Juniper Networks NFX150 Network Services Platform

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.0

Date: August 03, 2020

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

List of Tables

List of Figures

1 Introduction

NFX150 Network Services Platform are Juniper Network's secure, automated, software-driven customer premises equipment (CPE) devices that deliver virtualized network and security services on demand. Leveraging Network Functions Virtualization (NFV) and built on the Juniper Cloud CPE solution, NFX150 enables service providers to deploy and service chain multiple, secure, high-performance virtualized network functions (VNFs) as a single device. This automated, software-driven solution dynamically provisions new services on demand. The Juniper Networks NFX150 Network Services Platform cryptographic module, hereafter referred to as the NFX150 or the module, runs Juniper's Junos firmware Junos OS 19.2R1.

This Security Policy covers the NFX150-C-S1, NFX150-S1, and NFX150-S1E models. The cryptographic module is defined as multiple-chip standalone module that executes Junos firmware on the Juniper Networks NFX150 listed in the table below. The cryptographic module provides for an encrypted connection, using SSH, between the management station and the NFX150. The cryptographic modules also provide for an encrypted connection, using IPSec protocol, between the modules and other IPSec peers. All other data input or output from the NFX150 is considered plaintext for this FIPS 140-2 validation.

Table 1 – Cryptographic Module Configurations

Model	Hardware Versions	Firmware	Routing Engine (RE)	Power	Distinguishing Features
NFX150	NFX150-C-S1	Junos OS 19.2R1	Built-in RE (RE-NFX150-C-S1)	75 W AC-DC Power Adapter	8 GB of memory and 100 GB of solid-state drive (SSD) storage; 4 x 10/100/1000BASE-T RJ-45 LAN ports; 2 x 1GbE/10GbE SFP+ WAN ports; 1 x 10/100/1000BASE-T RJ-45 management port
NFX150	NFX150-S1	Junos OS 19.2R1	Built-in RE (RE-NFX150-S1)	150W AC-DC open frame power	16 GB of memory and 200 GB of solid-state drive (SSD) storage; 4 x 10/100/1000BASE-T RJ-45 LAN ports; 2 x 1GbE/10GbE SFP+ WAN ports; 1 x 10/100/1000BASE-T RJ-45 management port
NFX150	NFX150-S1E	Junos OS 19.2R1			32 GB of memory and 200 GB of solid-state drive (SSD)

Model	Hardware Versions	Firmware	Routing Engine (RE)	Power	Distinguishing Features
			Built-in RE (RE-NFX150-S1E)	150W AC-DC open frame power	storage; 4 x 10/100/1000BASE-T RJ-45 LAN ports; 2 x 1GbE/10GbE SFP+ WAN ports; 1 x 10/100/1000BASE-T RJ-45 management port

The module is designed to meet FIPS 140-2 Level 1 overall:

Table 2 – Security Level of Security Requirements

Area	Description	Level
1	Module Specification	1
2	Ports and Interfaces	1
3	Roles and Services	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Key Management	1
8	EMI/EMC	1
9	Self-test	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall	1

The module has a limited operational environment as per the FIPS 140-2 definitions. It includes a firmware load service to support necessary updates. Any firmware versions other than Junos OS 19.2R1, loaded into the modules are out of the scope of this validation and require a separate FIPS 140-2 validation.

The module does not implement any mitigations of other attacks as defined by FIPS 140-2.

1.1 Cryptographic Boundary

The physical form of the module is depicted in Figures 1,2, 3 and 4 below. The cryptographic boundary is defined as the outer edge of the chassis containing the Routing Engine and Junos firmware image defined in section 1. The module excludes the Junos Device Manager component of the firmware and non-Junos OS User Space applications. The modules also exclude the power supplies from the requirements of FIPS 140-2. The power supplies do not contain any security relevant components and cannot affect the security of the module.

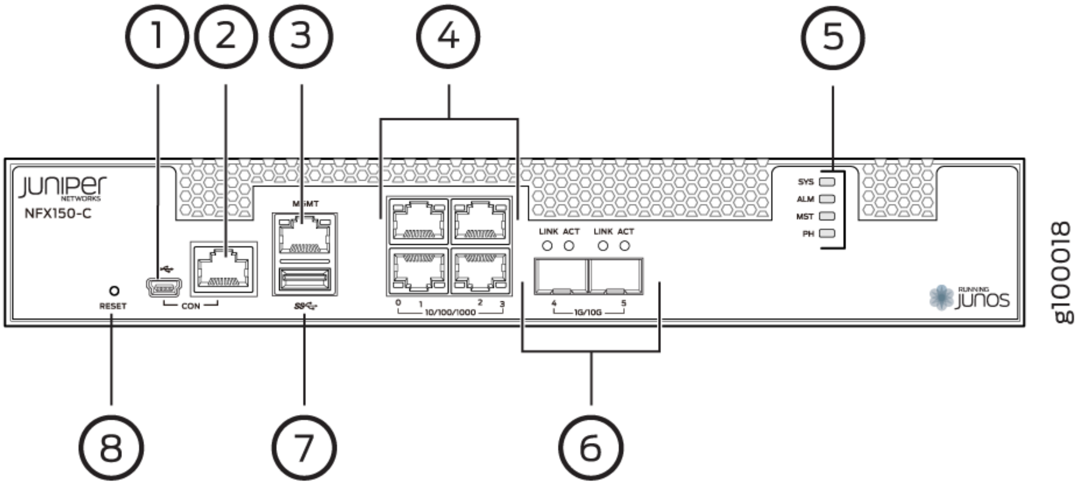

Figure 1 – NFX150-C-S1 Front View

1- Mini-USB console port	5- System status LEDs
2- RJ-45 console port	6- Two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports
3- One 10/100/ 1000BASE-T RJ-45 management port	7- USB 3.0 port
4- Four 10/100/ 1000BASE-T RJ-45 LAN ports	8- Reset button

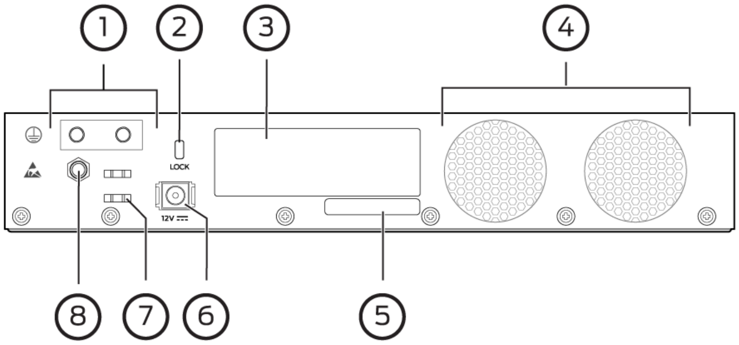

Figure 2 – NFX150-C-S1 Back View

1 - Grounding point	5 - CLEI code
2 - Lock	6 - Power supply input
3 - Serial number	7 - Cable tie holder
4 - Fans	8 - Electrostatic discharge (ESD) point

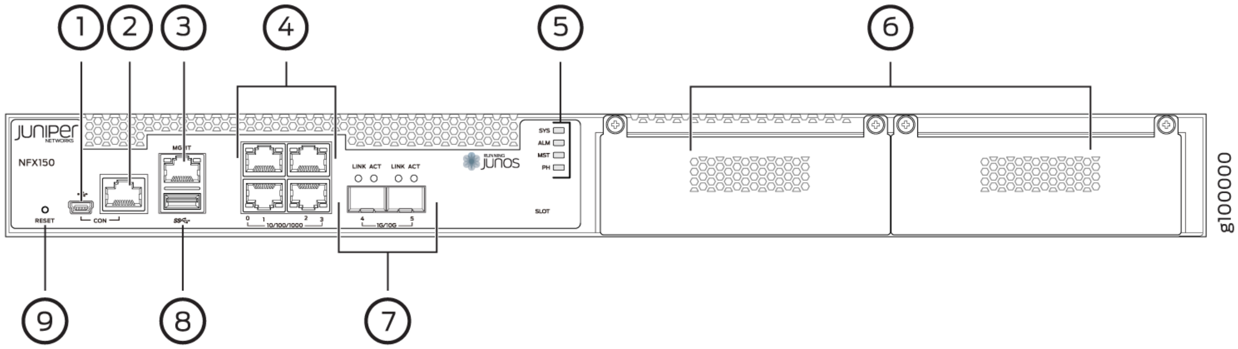

Figure 3 – NFX150-S1/NFX150-S1E Front View

1 - Mini USB console Port

2 - RJ-45 console port

3 - One 10/100/1000BASE-T RJ-45 management port

4 - Four 10/100/1000BASE-T RJ-45 LAN ports

5 - System status LEDs

6 - Expansion module slots

7 - Two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports

8 - USB 3.0 port

9 - Reset button

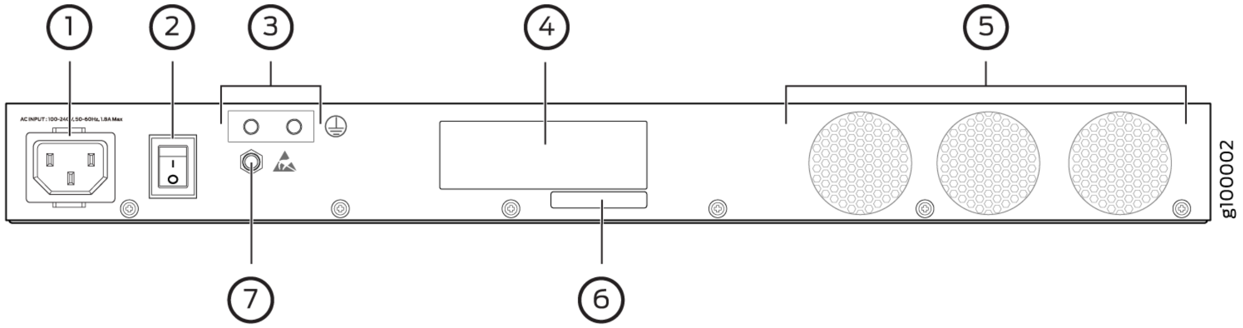

Figure 4 – NFX150-S1/NFX150-S1E Back View

1 - AC power cord inlet

2 - Power switch

3 - Grounding point

4 - Serial number

5 - Fans

6 - CLEI code

7 - Electrostatic discharge (ESD) point

Table 3 – Ports and Interfaces

Port	Device (# of ports)	Description	Logical Interface Type
Ethernet	NFX150-C-S1 (4), NFX150-S1 (4), NFX150-S1E (4)	RJ - 45 LAN Communications	Control in, Data in, Data out, Status out
Ethernet	NFX150-C-S1 (2), NFX150-S1 (2), NFX150-S1E (2)	SFP+ WAN ports	
Ethernet	NFX150-C-S1 (1), NFX150-S1 (1), NFX150-S1E (1)	Management port	Control in, Status out
Serial	NFX150-C-S1 (1), NFX150-S1 (1), NFX150-S1E (1)	Console serial port	Control in, Status out
Mini-USB	NFX150-C-S1 (1), NFX150-S1 (1), NFX150-S1E (1)	Console mini-USB port	Control in, Status out
USB	NFX150-C-S1 (1), NFX150-S1 (1), NFX150-S1E (1)	Firmware load port	Control in, Data in
Power	NFX150-C-S1 (1), NFX150-S1 (1), NFX150-S1E (1)	Power connector	Power
Reset	NFX150-C-S1(1), NFX150-S1 (1), NFX150-S1E (1)	Reset	Control in
LED	NFX150-C-S1 (8), NFX150-S1 (8), NFX150-S1E (8)	Status indicator lighting	Status out

1.2 Mode of Operation

The NFX150 has both a FIPS Approved mode of operation and a non-Approved mode of operation. The NFX150 is in a non-FIPS Approved mode by default. The Crypto-Officer enables the FIPS-Approved mode of operation and sets up keys and passwords for the system and other FIPS users. The Crypto-Officer must put the NFX150 into a FIPS Approved mode by following the steps listed in Section 6.1.2.

1.3 Zeroization

The cryptographic module provides a non-Approved mode of operation in which non-approved cryptographic algorithms are supported. When transitioning between the Approved mode of operation and the non-Approved mode of operation, the Cryptographic Officer must run the following commands to zeroize the Approved mode CSPs:

```
crypto-officer:fips> request system zeroize
```

Once the NFX150 is put into a FIPS Approved mode it remains in the FIPS Approved mode. The only way the module can leave the FIPS mode is to perform “request system zeroize” which will zeroize the system to include any configuration detail.

Note: The Cryptographic Officer must retain control of the module while zeroization is in process.

2 Cryptographic Functionality

The module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Tables 4, 5,6,7, 8 and 9 below. The Allowed Protocols in Table 11 summarizes the high-level protocol algorithm support. There maybe some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this/these table(s).

2.1 Approved Algorithms

There is a limit of 2^20 encryptions with the same Triple-DES key. The user is responsible for ensuring the module does not surpass this limit. References to standards are given in square bracket [ ]; see the References table.

Table 4 – Data Plane Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C946	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		SP 800-38D	GCM	Key Sizes: 128, 192, 256	Encrypt, Decrypt, AEAD
C946	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication
			SHA-256	Key size: 256 bits, λ = 128	
C946	SHS	PUB 180-4	SHA-1 SHA-256		Message Digest Generation
C946	Triple-DES	SP 800-67	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

Table 5 – Control Plane QuickSec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C947	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		SP 800-38D	GCM	Key Sizes: 128, 256	Encrypt, Decrypt, AEAD
N/A[1]	CKG	SP 800 - 133rev2	Section 4		Asymmetric seed generation (for use in asymmetric key generation) using unmodified DRBG output
			Section 6.2.1		Derivation of symmetric keys
C947	CVL	SP 800-135	IKEv1	SHA 256, 384	Key Derivation
			IKEv2	SHA 256, 384	

[1] Vendor Affirmed.

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C947	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
C947	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384)	KeyGen, SigGen, SigVer
C947	HMAC	PUB 198	SHA-256	Key size: 256 bits, Λ = 256	Message Authentication, KDF Primitive
				Key size: 384 bits, λ = 384	
N/A	KTS		AES Cert. #C947 and HMAC Cert. #C947		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. #C947 and HMAC Cert. #C947		key establishment methodology provides 112 bits of encryption strength
C947	RSA	PUB 186-4	PKCS1_V1_5	n=2048 (SHA 256) n=4096 (SHA 256)	SigGen, SigVer[2]
C947	SHS	PUB 180-4	SHA-256 SHA-384		Message Digest Generation
C947	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 6 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C970	AES	PUB 197-38A	CBC CTR	Key Sizes: 128, 192, 256	Encrypt, Decrypt
C970	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
N/A[3]	CKG	SP 800 - 133rev2	Section 4		Asymmetric seed generation (for use in asymmetric key generation) using unmodified DRBG output
			Section 6.2.1		Derivation of symmetric keys
C970	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer, PKV

[2] RSA 4096 SigVer was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 SigVer was tested and testing for RSA 4096 SigVer is not available.

[3] Vendor Affirmed.

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C970	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 160	Message Authentication
			SHA-512	Key size: 512 bits, λ = 512	
			SHA-256	Key size: 256, λ = 256	Message Authentication DRBG Primitive
N/A[4]	KAS-SSC	SP 800-56Arev3	ECDH	SSHD, PKID, IKED P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	Key Agreement Scheme - Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135 (CVL Cert. #C947)
			DH	IKED SHA 256 (Group 24)	
N/A	KTS		AES Cert. #C970 and HMAC Cert. #C970		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. #C970 and HMAC Cert. #C970		key establishment methodology provides 112 bits of encryption strength
C970	RSA	PUB 186-4		n=2048 (SHA 256, 512) n=4096 (SHA 256, 512)	KeyGen[5] , SigGen, SigVer[6]
C970	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384		Message Digest Generation, KDF Primitive
			SHA-512		Message Digest Generation
C970	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

[4] Vendor Affirmed per IG D.1rev3 (per IG D.8 Scenario X1)

[5] RSA 4096 KeyGen was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 KeyGen was tested and testing for RSA 4096 KeyGen is not available.

[6] RSA 4096 SigVer was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 SigVer was tested and testing for RSA 4096 SigVer is not available.

Table 7 – OpenSSH Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C945	CVL	SP 800-135	SSH	SHA 1, 256, 384	Key Derivation

Table 8 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C943	HMAC	PUB 198	SHA-1 SHA-256	Key size: 160 bits, λ = 160 Key size: 256 bits, λ = 256	Password Hashing
C943	SHS	PUB 180-4	SHA-1 SHA-256 SHA-512		Message Digest Generation

Table 9 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C942	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
C942	HMAC	PUB 198	SHA-256	Key size: 256, λ = 256	DRBG Primitive
C942	SHS	PUB 180-4	SHA-1 SHA-256		Message Authentication DRBG Primitive

2.2 Allowed Algorithms

Table 10 – Allowed Cryptographic Functions

Algorithm	Caveat	Use
NDRNG [IG] 7.14 Scenario 1a	The module generates a minimum of 256 bits of entropy for key generation.	Seeding the DBRG

2.3 Allowed Protocols

Table 11 – Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1[7]	Diffie-Hellman (L = 2048, N = 256) EC Diffie-Hellman P-256, P-384	RSA 2048 RSA 4096 Pre-Shared Secret ECDSA P-256 ECDSA P-384	Triple-DES CBC AES CBC 128/192/256	SHA-256 SHA-384

[7] RFC 2409 governs the generation of the Triple-DES encryption key for use with the IKEv1 protocol.

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv2[8]	Diffie-Hellman (L = 2048, N =256) EC Diffie-Hellman P-256, P-384	RSA 2048 RSA 4096 Pre-Shared Secret ECDSA P-256 ECDSA P-384	Triple-DES CBC AES CBC 128/192/256 AES GCM[9] 128/256	SHA-256 SHA-384
IPsec ESP	IKEv1 with optional: • Diffie-Hellman (L = 2048, N = 256) EC Diffie-Hellman P-256, P-384	IKEv1	3 Key Triple-DES CBC AES CBC 128/192/256 AES GCM[10] 128/192/256	HMAC-SHA-1-96 HMAC-SHA-256-128
	IKEv2 with optional: • Diffie-Hellman (L = 2048, N = 256) EC Diffie-Hellman P-256, P-384	IKEv2	3 Key Triple-DES CBC AES CBC 128/192/256 AES GCM[11] 128/192/256	
SSHv2[12]	EC Diffie-Hellman P-256, P-384, P-521	RSA 2048 ECDSA P-256	Triple-DES CBC AES CBC 128/192/256 AES CTR 128/192/256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

No part of these protocols, other than the KDF, has been tested by the CAVP and CMVP. The IKE and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In reference to the Allowed Protocols in Table 11 above, each column of options for a given protocol is independent and may be used in any viable combination. These security functions are also available in the SSH connect (non-compliant) and IPSec connect (non-compliant) service.

2.4 Disallowed Algorithms and Protocols

These algorithms are non-Approved algorithms that are disabled when the module is operated in an Approved mode of operation.

[8] IKEv2 generates the SKEYSEED according to RFC7296, from which all keys are derived to include Triple-DES keys.

[9] The AES GCM IV is generated according to RFC5282 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.

[10] The AES GCM IV is generated according to RFC4106 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.

[11] The AES GCM IV is generated according to RFC4106 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.

[12] RFC 4253 governs the generation of the Triple-DES encryption key for use with the SSHv2 protocol.

Algorithms:

- ARCFOUR
- Blowfish
- CAST
- DSA (SigGen, SigVer; non-compliant)
- HMAC-MD5
- HMAC-RIPEMD160
- UMAC

Protocols:

- Finger
- ftp
- rlogin
- telnet
- tftp
- xnm-clear-text

2.5 Critical Security Parameters

All CSPs and public keys used by the module are described in this section.

Table 12 – Critical Security Parameters (CSPs)

Name	Description and usage
DRBG_Seed	Seed material used to seed or reseed the DRBG
DRBG_State	V and Key values for the HMAC_DRBG
Entropy Input String	256 bits entropy (min) input used to instantiate the DRBG
ECDH Shared Secret	The Diffie-Hellman shared secret used in EC Diffie-Hellman (ECDH) exchange. Created per the EC Diffie-Hellman protocol. Provides between 128-256 bits of security.
DH Shared Secret	The shared secret used in Diffie Hellman (DH) key exchange. 128 bits. Established per the Diffie-Hellman key agreement.
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. RSA 2048, ECDSA P-256. Used to identify the host.
SSH ECDH	SSH Elliptic Curve Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in SSH. ECDH P-256, ECDH P-384 or ECDH P-521
SSH-SEKs	SSH Session Keys; SSH Session Encryption Key: TDES (3key) or AES; SSH Session Integrity Key: HMAC
ESP-SEKs	IPSec ESP Session Keys: IKE Session Encryption Key: TDES (3key) or AES; IKE Session Integrity Key: HMAC.
IKE-PSK	Pre-Shared Key used to authenticate IKE connections.
IKE-Priv	IKE Private Key. RSA 2048, RSA 4096, ECDSA P-256, or ECDSA P-384
IKE-SKEYID	IKE SKEYID. IKE secret used to derive IKE and IPsec ESP session keys.
IKE-SEKs	IKE Session Keys: IKE Session Encryption Key: TDES (3key) or AES; IKE Session Integrity Key: HMAC

Name	Description and usage
IKE-DH-PRI	IKE Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in IKE. DH (L=2048, N = 256), ECDH P-256, or ECDH P-384
HMAC Key	The LibMD HMAC keys: message digest for hashing password and critical function test.
CO-PW	ASCII Text used to authenticate the CO.
User-PW	ASCII Text used to authenticate the User.

Table 13 – Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. RSA 2048, ECDSA P-256.
SSH-ECDH-PUB	SSH EC Diffie-Hellman public component. EC Diffie-Hellman public key used in SSH key establishment. ECDH P-256, ECDH P-384 or ECDH P-521
IKE-PUB	IKE Public Key RSA 2048, RSA 4096, ECDSA P-256, or ECDSA P-384
IKE-DH-PUB/IKE-ECDH-PUB	IKE Ephemeral Diffie-Hellman or EC Diffie-Hellman public key used in IKE key establishment. DH (L = 2048, N = 256), ECDH P-256, or ECDH P-384
Auth-UPub	User Authentication Public Keys. Used to authenticate users to the module. RSA 2048, 4096 or ECDSA P-256, P-384 and P-521
Auth-COPub	CO Authentication Public Keys. Used to authenticate CO to the module. RSA 2048, 4096 or ECDSA P-256, P-384 and P-521
Root-CA	JuniperRootCA. ECDSA P-256 or P-384 X.509 Certificate; Used to verify the validity of the Juniper Package-CA at software load.
Package-CA	PackageCA. ECDSA P-256 X.509 Certificate; Used to verify the validity of Juniper Images at software load and also at runtime integrity.

3 Roles, Authentication and Services

3.1 Roles and Authentication of Operators to Roles

The module supports two roles: Cryptographic Officer (CO) and User. The module supports concurrent operators but does not support a maintenance role and/or bypass capability. The module enforces the separation of roles using either of the identity-based operator authentication methods in section 3.2.

The Cryptographic Officer role configures and monitors the module via a console or SSH connection. As root or super-user, the Cryptographic Officer has permission to view and edit secrets within the module.

The User role monitors the module via the console or SSH. The user role may not change the configuration.

3.2 Authentication Methods

The module implements two forms of Identity-Based authentication, Username and password over the Console and SSH as well as Username and public key over SSH.

Password authentication: The module enforces 10-character passwords (at minimum) chosen from the 96 human readable ASCII characters. The maximum password length is 20-characters. Thus, the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million.

The module enforces a timed access mechanism as follows: For the first two failed attempts (assuming 0 time to process), no timed access is enforced. Upon the third attempt, the module enforces a 5-second delay. Each failed attempt thereafter results in an additional 5-second delay above the previous (e.g. 4th failed attempt = 10-second delay, 5th failed attempt = 15-second delay, 6th failed attempt = 20-second delay, 7th failed attempt = 25-second delay).

This leads to a maximum of 7 possible attempts in a one-minute period for each getty. The best approach for the attacker would be to disconnect after 4 failed attempts and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour/60 mins); this would be rounded down to 9 per minute, because there is no such thing as 0.6 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $9/(96^{10})$, which is less than 1/100,000.

ECDSA signature verification: SSH public-key authentication. The module supports ECDSA (P-256, P-384, and P-521), which has a minimum equivalent computational resistance to attack of either 2^128 , 2^192 or 2^256 depending on the curve. Thus, the probability of a successful random attempt is 1/ (2^128), which is less than 1/1,000,000. Configurable SSH connection establishment rate limits the number of connection attempts, and thus failed authentication attempts in a one-minute period to a maximum of 15,000 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is 15,000/(2^128), which is less than 1/100,000.

RSA signature verification: SSH public-key authentication. The module supports RSA (2048, 4096), which has a minimum equivalent computational resistance to attack of 2^112 (2048). Thus, the probability of a successful random attempt is 1/ (2^112), which is less than 1/1,000,000. Configurable SSH connection establishment rate limits the number of connection attempts, and thus failed authentication attempts in a one-minute period to a maximum of 15,000 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is 15,000/ (2^112), which is less than 1/100,000.

3.3 Services

All services implemented by the module are listed in the tables below. Table 16 lists the access to CSPs by each service.

Table 14 – Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Secure Traffic	IPsec protected connection (ESP)	X	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
IPsec connect	Initiate IPsec connection (IKE)	X	
Console access	Console monitoring and control (CLI)	x	x
Remote reset	Software initiated reset conducted over SSH connection to the management port. The remote reset service is used to perform self-tests on demand.	x	
Load Image	Verification and loading of a validated firmware image onto the module	x	

Table 15 – Unauthenticated traffic

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services

Table 16 – CSP Access Rights within Services

Service	CSPs																
	DRBG_Seed	DRBG_State	Entropy Input String	DH Shared Secret	ECDH Shared Secret	SSH PHK	SSH DH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYID	IKE-SEK	IKE-DH-PRI	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	GWR	GWR	GWR	--	--	--	WR	GWR	--	--	--	G	W	W

Service	CSPs																
	DRBG_Seed	DRBG_State	Entropy Input String	DH Shared Secret	ECDH Shared Secret	SSH PHK	SSH DH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYID	IKE-SEK	IKE-DH-PRI	HMAC Key	CO-PW	User-PW
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure traffic	--	--	--	--	--	--	--	--	E	--	--	--	E	--	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	--	--	--	Z	Z	Z
SSH connect	--	E	--	E	E	E	G E	G E	--	--	--	--	--	--	--	E	E
IPsec connect	--	E	--	--	--	--	--	--	G	E	E	G E	G	G E	--	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E
Remote reset	GE Z	G Z	G Z	Z	Z	--	Z	Z	Z	--	--	Z	Z	Z	--	Z	Z
Load Image	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Local reset	GE Z	G Z	G Z	Z	Z	--	Z	Z	Z	--	--	Z	Z	Z	--	Z	Z
Traffic	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

G = Generate: The module generates the CSP
R = Read: The CSP is read from the module (e.g. the CSP is output)
E = Execute: The module executes using the CSP
W = Write: The CSP is updated or written to the module
Z = Zeroize: The module zeroizes the CSP.

3.4 Non-Approved Services

The following services are available in the non-Approved mode of operation. The security functions provided by the non-Approved services are identical to the Approved counterparts with the exception of SSH Connect (non-compliant) and IPSec Connect (non-compliant). SSH Connect (non-compliant) supports the security functions identified in Section 2.4 and the SSHv2 row of Table 11. The IPsec (non-compliant) supports the DSA in Section 2.4 and the IKEv1, IKEv2 and IPSec rows of Table 11.

Table 17 – Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	x	
Configure (non-compliant)	Non-security relevant configuration	x	
Secure Traffic (non-compliant)	IPsec protected connection (ESP)	X	
Status (non-compliant)	Show status	x	x
Zeroize (non-compliant)	Destroy all CSPs	x	
SSH connect (non-compliant)	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
IPsec connect (non-compliant)	Initiate IPsec connection (IKE)	X	
Console access (non-compliant)	Console monitoring and control (CLI)	x	x
Remote reset (non-compliant)	Software initiated reset	x	
Load Image (non-compliant)	Verification and loading of a validated firmware image into the switch.	x	

Table 18 – Unauthenticated traffic

Service	Description
Local reset (non-compliant)	Hardware reset or power cycle
Traffic (non-compliant)	Traffic requiring no cryptographic services

4 Self-tests

Each time the module is powered up, it tests that the cryptographic algorithms still operate correctly, and that sensitive data has not been damaged. Power-up self–tests are available on demand by power cycling the module (Remote reset service).

On power up or reset, the module performs the self-tests described below. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fails, the module enters the Critical Failure error state.

The module performs the following power-up self-tests:

- Firmware Integrity check using ECDSA P-256 with SHA-256
- **Data Plane KATs**
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - AES-GCM (128/192/256) Encrypt KAT
  - AES-GCM (128/192/256) Decrypt KAT
- **Control Plane QuickSec KATs**
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - RSA 2048 w/ SHA-256 Sign KAT
  - RSA 2048 w/ SHA-256 Verify KAT
  - ECDSA P-256 w/ SHA-256 Sign/Verify PCT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
  - HMAC-SHA-256 KAT
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - AES-GCM (128/256) Encrypt KAT
  - AES-GCM (128/256) Decrypt KAT
  - KDF-IKE-V1 KAT
  - KDF-IKE-V2 KAT
- **OpenSSL KATs**
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate.
  - ECDSA P-256 Sign/Verify PCT
  - ECDH P-256 KAT
    - Derivation of the expected shared secret.
  - RSA 2048 w/ SHA-256 Sign KAT
  - RSA 2048 w/ SHA-256 Verify KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
  - HMAC-SHA-1 KAT

    - HMAC-SHA-256 KAT
    - HMAC-SHA-512 KAT
    - AES-CBC (128/192/256) Encrypt KAT
    - AES-CBC (128/192/256) Decrypt KAT
    - KAS-ECC-EPHEM-UNIFIED-NOKC KAT
    - KAS-FFC-EPHEM-NOKC KAT
- **OpenSSH KATs**
    - KDF-SSH-SHA256 KAT
- **LibMD KATs**
    - HMAC SHA-1
    - HMAC SHA-256
    - SHA-512
- **Kernel KATs**
    - SP 800-90A HMAC DRBG KAT
        - Health-tests initialize, re-seed, and generate
    - HMAC-SHA-256 KAT
    - SHA-1

- **Critical Function Test**
    - The cryptographic module performs a verification of a limited operational environment, and verification of optional non-critical packages.

The module also performs the following conditional self-tests:

- Continuous RNG Test on the OpenSSL SP 800-90A HMAC-DRBG
- Continuous RNG test on the NDRNG
- Pairwise consistency test when generating ECDSA and RSA key pairs.
- Firmware Load Test (ECDSA signature verification)

5 Physical Security Policy

The module's physical embodiment is that of a multi-chip standalone device that meets Level 1 Physical Security requirements. The module is composed of production grade materials. The module is completely enclosed in a rectangular nickel or clear zinc coated, cold rolled steel, plated steel and brushed aluminum enclosure. There are no ventilation holes, gaps, slits, cracks, slots, or crevices that would allow for any sort of observation of any component contained within the cryptographic boundary.

6 Security Rules and Guidance

The module design corresponds to the security rules below. The term *must* in this context specifically refers to a requirement for correct usage of the module in the Approved mode; all other statements indicate a security rule implemented by the module.

1. The module clears previous authentications on power cycle.
2. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. Power up self-tests do not require any operator action.
4. Data output is inhibited during key generation, self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not support manual key entry.
9. The module does not output intermediate key values.
10. The module requires two independent internal actions to be performed prior to outputting plaintext CSPs.
11. The cryptographic officer must verify that the firmware image to be loaded on the NFX150 is a FIPS validated image. If any other non-validated image is loaded the module will no longer be a FIPS validated module.
12. The cryptographic officer must retain control of the module while zeroization is in process.
13. Virtualized Network Functions (VNFs) shall not be configured in FIPS-mode of operation.
14. The Triple-DES encryption key is generated as part of recognized IETF protocols (RFC 2409 IKEv1, RFC 4251 SSH, RFC 7296 IKEv2, and RFC 6071 IPSec). The operator is required to ensure that Triple-DES keys used in the SSH protocol do not perform more than 2^20 encryptions.
15. If the module loses power and then it is restored, then a new key shall be established for use with the AES GCM encryption/decryption processes.
16. When the IV in RFC 5282 exhausts the maximum number of possible values for a given security association, either party to the security association that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key for the security association per RFC 7296.
17. 3-key Triple-DES has been implemented in the module and is FIPS approved until December 31, 2023. Should the CMVP disallow the usage of Triple-DES post December 31, 2023, then users must not configure Triple-DES.

6.1 Cryptographic-Officer Guidance

The cryptographic officer must check to verify the firmware image on the module is the FIPS 140-2 validated image. If the image is the FIPS 140-2 validated image, then proceed to section 6.1.2.

6.1.1 Installing the FIPS-Approved firmware image

Download the validated firmware image from the https://www.juniper.net/support/downloads/junos.html. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives. Select the validated firmware image. Download the firmware image to a local host or to an internal software distribution site.

Connect to the console port on the module from your management device and log in to the Junos OS CLI. Copy the firmware package to the module to the /var/tmp/ directory. Install the new package on the NFX150 device:

```
root> request vmhost software add  /var/tmp/package.tgz.
```

NOTE: The NFX150 devices are shipped with a default username and password to be used when logging into the device for the first time. The default username and password can be found in the documentation. The password must be reset post the initial login.

NOTE: If you need to terminate the installation, do not reboot your device; instead, finish the installation and then issue the request system software delete *package*.tgz command, where *package*.tgz is, for example, jinstall-ppc-19.2R1-signed.tgz. This is your last chance to stop the installation.

Reboot the device to load the installation and start the new firmware image:

```
root > request vmhost reboot
```

6.1.2 Enabling FIPS-Approved Mode of Operation

The cryptographic officer shall follow the steps found in the *Junos OS FIPS Evaluated Configuration Guide for NFX150 Network Services Platform, Release 19.2R1* document Chapter 2 to place the module into a FIPS-Approved mode of operation. The steps from the aforementioned document are repeated below:

1. Zeroize the device by following instructions outlined in Section 1.3 to delete all CSPs before entering FIPS mode.
2. Login using username root:

   ```
   FreeBSD/amd64 (Amnesiac) (ttyu0)
   login: root
   --- JUNOS 19.2-20180131.0 Kernel 64-bit JNPR-11.0-20180123.155949_fbsdroot@:~
   # cli
   root>
   ```

3. Configure root authentication:

   ```
    root> edit
   Entering configuration mode
   [edit]
   root# set system root-authentication plain-text-password
   New password:
   Retype new password: [edit]
   root# commit
   commit complete
   ```

4. Load configuration onto device and commit new configuration.
5. Install fips-mode package needed Routing Engine KATS.

   ```
   root@hostname> request vmhost software add optional://fips-mode.tgz
   Verified fips-mode signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
   ```

6. Install jpfe-fips package.

   ```
   root@hostname> request vmhost software add optional://jpfe-fips.tgz

   Verified jpfe-fips signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
   ```

7. Configure the FIPS mode of operation by setting “set system fips chassis level 1”, and “set systems fips level 1” , followed by commit.

   Device might display the encrypted-password must be re-configured to use FIPS compliant hash warning to delete older CSP in loaded configuration.

8. After deleting and reconfiguring CSPs, commit will go through and device needs reboot to enter FIPS mode.

   ```
   [edit]
   root@hostname# commit
   Generating RSA key /etc/ssh/fips_ssh_host_key
   Generating RSA2 key /etc/ssh/fips_ssh_host_rsa_key
   Generating ECDSA key /etc/ssh/fips_ssh_host_ecdsa_key
   [edit]
   system
   reboot is required to transition to FIPS level 1
   commit complete
   root@hostname> request vmhost reboot
   ```

9. After rebooting the device, FIPS self-tests will run and device enters FIPS mode.

   ```
   root@hostname:fips>
   ```

10. After the reboot has completed, log in and use the show version command to verify.

    ```
    root @hostname:fips > show version
    ```

The module boots up in FIPS mode which allows only a restricted set of SSH Key algorithms. All Disallowed Algorithms listed in section 2.4 are disabled.

Direct access to Junos Device Manager (JDM), from external connections, is disabled in FIPS mode. All connections from external devices, to the module, are via the Junos Control Plane (JCP).

6.1.3 Placing the Module in a Non-Approved Mode of Operation

As cryptographic officer, the operator may need to disable the FIPS-Approved mode of operation on the module to return it to a non-Approved mode of operation. To disable FIPS-Approved mode on the module, the module must be zeroized. Follow the steps found in section 1.3 to zeroize the module.

6.2 User Guidance

The user should verify that the module is operating in the desired mode of operation (FIPS-Approved mode or non-Approved mode) by observing the command prompt when logged into the module. If the string ":fips" is present, then the module is operating in a FIPS-Approved mode. Otherwise it is operating in a non-Approved mode.

All FIPS users, including the Crypto Officer, must observe security guidelines at all times.

All FIPS users must:

- Keep all passwords confidential.
- Store routers or switches and documentation in a secure area.
- Deploy routers or switches in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
  - Users are trusted.
  - Users abide by all security guidelines.
  - Users do not deliberately compromise security.
  - Users behave responsibly at all times.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 19 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[133rev2]	*National Institute of Standards and Technology, Recommendation for Cryptographic Key Generation,* June 2020.
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC,* November 2007.
[56Arev3]	*National Institute of Standards and Technology, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography,* April 2018.
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004*
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.

Table 20 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
JCP	Junos Control Plane
JDM	Junos Device Manager
MD5	Message Digest 5
SHA	Secure Hash Algorithms
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 21 – Datasheets

Model	Title	URL
NFX150	NFX Series Network Services Platform	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000563-en.pdf