Juniper Networks NFX250 Network Services Platform

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.4

Date: September 6, 2018

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

NFX250 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, NFX250 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 NFX250 Network Services Platform cryptographic module, hereafter referred to as the NFX250 or the module, runs Juniper's Junos firmware Junos OS 17.3R2.

This Security Policy covers the NFX250-S1 and NFX250-S2 models. The cryptographic module is defined as multiple-chip standalone module that executes Junos firmware on the Juniper Networks NFX250 listed in the table below. The cryptographic module provides for an encrypted connection, using SSH, between the management station and the NFX250. All other data input or output from the NFX250 is considered plaintext for this FIPS 140-2 validation.

Table 1 – Cryptographic Module Configurations

Model	Hardware Versions	Firmware	Distinguishing Features
NFX250	NFX250-S1	Junos OS 17.3R2	16 GB of memory and 100 GB of solid-state drive (SSD) storage; 8 x 1GbE ports; 2 x 1GbE RJ-45 ports; 2 SFP and 2 SFP+
NFX250	NFX250-S2	Junos OS 17.3R2	32 GB of memory and 400 GB of solid-state drive (SSD) storage; 8 x 1GbE ports; 2 x 1GbE RJ-45 ports; 2 SFP and 2 SFP+

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. New firmware version within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is 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 and Figure 2 below. The cryptographic boundary is defined as the outer edge of the chassis containing the 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 module does not rely on external devices for input and output.

Figure 1 - NFX250 Front View

Figure 2 - NFX250 Back View

Table 3 - Ports and Interfaces

Port (# of ports)	Description	Logical Interface Type
Ethernet (8)	RJ - 45 LAN Communications	Control in, Data in, Data out, Status out
Ethernet (2)	RJ - 45 LAN/WAN Communications	
Ethernet (4)	2 – SFP WAN ports 2 – SFP+ WAN ports	
Ethernet (1)	Management port	Control in, Status out
Serial (1)	Console serial port	Control in, Status out
Mini-USB (1)	Console mini-USB port	Control in, Status out
USB (1)	Firmware load port	Control in, Data in
Power (1)	Power connector	Power
Reset (1)	Reset	Control in
LED (15)	Status indicator lighting	Status out

1.2 Mode of Operation

The NFX250 has both a FIPS Approved mode of operation and a non-Approved mode of operation. The NFX250 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 NFX250 into a FIPS Approved mode by following the steps below.

1.2.1 Placing the NFX250 in FIPS Approved mode of operation

The Crypto-Officer starts the process of putting the module into FIPS mode by following the steps provided below

1. Set a plain-text root-authentication password for NFX250.
2. Enter into CLI mode on NFX250 (still in non-fips mode) and establish a SSH connection to "ssh jdm-sysuser@vjunos0".
3. Set a plain-text root-authentication password for root.
4. Exit
5. Execute the following commands:
    a. root@jdm> start shell
    b. ssh jdm-sysuser@vjunos0 request system software add optional://fips-mode.tgz
    c. exit

6. From the CLI, enter

    root@jdm> ***request system zeroize to-fips***
    warning: System will be rebooted and current installation will be zeroized.
    warning: This will stop all VNFs and remove all user configuration and data.

7. Type **yes** at the prompt, to reboot the system:

    Reboot system to switch device to FIPS mode? [yes,no] (no)
    Yes

8. The device reboots multiple times and after the series of reboots occurs the module is in FIPS Level 1 mode.

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).

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:

root:fips> ***request system zeroize***

Once the NFX250 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 and 6 below. The Allowed Protocols in Table 8 summarizes the high-level protocol algorithm support.

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.

Table 4 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Functions
5320	AES	PUB 197-38A	CBC, CTR	Key Sizes: 128, 192, 256	Encrypt, Decrypt
N/A[1]	CKG	SSH-PUB 133	Section 6.2 Section 6.3		Asymmetric key generation using unmodified DRBG output
			Section 7.3		Derivation of symmetric keys
1601	CVL	SP 800-135	SSH KDF	SHA 1, 256, 384[2], 512	Key Derivation
1867	DRBG	SP 800-90A	HMAC	SHA 1, SHA 224, SHA 256, SHA 384, SHA 512	Random Bit Generation
1301	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen
				P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	KeyGen, SigVer
3367	HMAC	PUB 198	SHA-1	Key Sizes: 112 bits, 160 bits, λ = 160	Message Authentication DRBG Primitive
			SHA-224	Key Sizes: 160 bits, 256 bits, λ = 224	
			SHA-256	Key Sizes: 160 bits, 256 bits, λ = 256	
			SHA-384	Key Sizes: 160 bits, 512 bits, λ = 384	
			SHA-512	Key Sizes: 160 bits, 512 bits, λ = 512	
N/A	KTS		AES Cert. #5320 and HMAC Cert. #3367		key establishment methodology provides between 128 and 256 bits of encryption strength

[1] Vendor Affirmed.

[2] SSH KDF with SHA 384 was validated; however, it is not used by any service.

			Triple-Des Cert. #2606 and HMAC Cert. #3367		key establishment methodology provides 112 bits of encryption strength
4112	SHS	PUB 180-4	SHA-1 SHA-224 SHA-256 SHA-384		Message Digest Generation, KDF Primitive
			SHA-512		Message Digest Generation
2606	Triple-DES	SP 800-67	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

Table 5 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Functions
3366	HMAC	PUB 198	SHA-1	Key Sizes: 112 bits, 160 bits, λ = 160	Password hashing
			SHA-256[3]	N/A	
4111	SHS	PUB 180-4	SHA-1		Message Digest Generation
			SHA-256		
			SHA-512		

Table 6 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Functions
2054	DRBG	SP 800-90A	HMAC	SHA 256	Random Bit Generation
3522	HMAC	PUB 198	SHA-256	Key Sizes: 256 bits, λ = 256	DRBG Primitive
4276	SHS	PUB 180-4	SHA-256		Hash for HMAC

2.2 Allowed Algorithms

Table 7 - Allowed Cryptographic Functions

Algorithm	Caveat	Use
Elliptic Curve Diffie-Hellman [IG] D.8	Provides between 128 and 256 bits of encryption strength.	key agreement; key establishment
NDRNG [IG] 7.14 Scenario 1a	The module generates a minimum of 256 bits of entropy for key generation.	Seeding the DBRG

[3] HMAC SHA-256 was validated; however, it is not used by any service.

2.3 Allowed Protocols

Table 8 - Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
SSHv2	EC Diffie-Hellman P-256, P-384, P-521	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 the SSH protocol, other than the KDF, has been tested by the CAVP and CMVP. The SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In reference to the Allowed Protocols in Table 8 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) service.

2.4 Disabled Algorithms

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

- ARCFOUR
- Blowfish
- CAST
- HMAC-MD5
- HMAC-RIPEMD160
- UMAC

2.5 Critical Security Parameters

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

Table 9 - 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
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. ECDSA P-256. Used to identify the host.
SSH DH	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
CO-PW	ASCII Text used to authenticate the CO.
User-PW	ASCII Text used to authenticate the User.

Table 10 - Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256.
SSH-DH-PUB	Diffie-Hellman public component. Ephemeral Diffie-Hellman public key used in SSH key establishment. ECDH P-256, ECDH P-384 or ECDH P-521
Auth-UPub	User Authentication Public Keys. Used to authenticate users to the module. ECDSA P256 or P-384
Auth-COPub	CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P256 or P-384
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 identity-based operator authentication.

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 router via the console or SSH. The user role may not change the configuration.

3.2 Authentication Methods

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.

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. 4^{th} failed attempt = 10-second delay, 5^{th} failed attempt = 15-second delay, 6^{th} failed attempt = 20-second delay, 7^{th} failed attempt = 25-second delay).

This leads to a maximum of nine (9) 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. Thus the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million. 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. Processing constraints allow for a maximum of 5.6e7 ECDSA attempts per minute. The module supports ECDSA (P-256, P-384 and P-521), which has a minimum equivalent computational resistance to attack of either 2^{128} depending on the curve. Thus, the probability of a successful random attempt is $1/ (2^{128})$, which is less than 1/1,000,000. Processing speed (partial establishment of an SSH session) limits the number of failed authentication attempts in a one-minute period to 5.6e7 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{128})$, which is less than 1/100,000.

3.3 Services

All services implemented by the module are listed in the tables below. Table 13 lists the access to CSPs by each service.

Table 11 - Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	

SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	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 into the switch.	x	

Table 12 - Unauthenticated traffic

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

Table 13 - CSP Access Rights within Services

Service	DRBG_Seed	DRBG_State	Entropy Input String	SSH PHK	SSH DH	SSH-SEK	CO-PW	User-PW
Configure security	--	E	--	GWR	--	--	W	W
Configure	--	--	--	--	--	--	--	--
Status	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z
SSH connect	--	E	--	E	GE	GE	E	E
Console access	--	--	--	--	--	--	E	E
Remote reset	GEZ	GZ	GZ	--	Z	Z	Z	Z
Load Image	--	--	--	--	--	--	--	--
Local reset	GEZ	GZ	GZ	--	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). SSH Connect (non-compliant) supports the security functions identified in Section 2.4 and the SSHv2 in Table 8.

Table 14 - Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	x	
Configure (non-compliant)	Non-security relevant configuration	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
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 15 - 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
- OpenSSL KATs
    - AES-CBC (128/192/256) Encrypt KAT
    - AES-CBC (128/192/256) Decrypt KAT
    - SP 800-90A HMAC DRBG KAT
    - ECDSA P-256 Sign/Verify
    - ECDH P-256 KAT
        - Derivation of the expected shared secret
    - Triple-DES-CBC Encrypt KAT
    - Triple-DES-CBC Decrypt KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-224 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - KDF-SSH KAT
- Libmd
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - SHA-512 KAT
- Kernel
    - SP 800-90A HMAC DRBG KAT
        - Health-tests initialize, re-seed, and generate
    - HMAC-SHA-256 KAT
- 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 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 completely enclosed in a rectangular nickel or clear zinc coated, cold rolled steel, plated steel and brushed aluminum enclosure.

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 NFX250 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 operator is required to ensure that Triple-DES keys used in the SSH protocol do not perform more than 2^{20} encryptions.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 16 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[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*
[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 17 – 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 18 – Datasheets

Model	Title	URL
NFX250	NFX250 Network Services Platform	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000563-en.pdf