Juniper Networks QFX10002, QFX10008 and QFX10016

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.3

Date: December 8, 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

The Juniper Networks QFX series switches are high performance, high density data center switches. The QFX switches provide high performance, wire speed switching with low latency and jitter. The QFX series switches provide the universal building blocks for multiple data center fabric architectures. This Security Policy covers the following models – the QFX10002, QFX10008 and QFX10016.

All models run Juniper's JUNOS firmware. The JUNOS firmware is FIPS-compliant, when configured in FIPS-MODE called JUNOS-FIPS-MODE, version 18.1R1. The firmware image file for the QFX10002 unit is *jinstall-host-qfx-10-f-x86-64-18.1R1.9-secure-signed.tgz*, and for the QFX10008/QFX10016 units it is *jinstall-host-qfx-10-m-x86-64-18.1R1.9-secure-signed.tgz*. The firmware status service on each model identifies itself as "Junos 18.1R1".

The cryptographic modules are defined as multiple-chip standalone modules that execute Junos OS firmware on the Juniper Networks QFX Series switches listed in Table 1. Section 1.1 describes the cryptographic boundaries for each QFX model.

The cryptographic module provides for an encrypted connection, using SSH, between the management station and the QFX switch. All other data input or output from the QFX switch is considered plaintext for this FIPS 140-2 validation.

Table 1 – Cryptographic Module Configurations

Model	Hardware	Power Supply	Boundary/Chassis Type
QFX10002	QFX10002 -36Q QFX10002-72Q	JPSU-1600W-AC-AFO JPSU-1600W-DC-AFO	Switch Case/ Fixed configuration
QFX10008	QFX10008 with QFX10000 Control board	QFX10000-PWR-AC QFX10000-PWR-DC	Chassis/Modular Configuration (Line card slots 0-7)
QFX10016	QFX10016 with QFX10000 Control board	QFX10000-PWR-AC QFX10000-PWR-DC	Chassis/Modular Configuration (Line card slots 0-15)

The modules are 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 modules have a limited operational environment as per the FIPS 140-2 definitions. They include a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into these modules is out of the scope of this validation and require a separate FIPS 140-2 validation.

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

1.1 Hardware and Physical Cryptographic Boundary

The physical forms of the module's various models are depicted in Figures 1-3 below. For all models, the cryptographic boundary is defined as the outer edge of the chassis/switch. The modules 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. The modules do not rely on external devices for input and output.

The cryptographic boundaries for each of the QFX Series models validated are:

- QFX10002: The outer edge of the switch is the crypto-graphic boundary
- QFX10008: 2 QFX10000 Control Boards, 8 slots with all empty module bays containing a slot cover installed for proper cooling air circulation.
  - includes the inverse three-dimensional space where non-crypto-relevant line cards fit, with the backplane port serving as the physical interface.
- QFX10016: 2 QFX10000 Control Boards, 16 slots with all empty module bays containing a slot cover installed for proper cooling air circulation.
  - includes the inverse three-dimensional space where non-crypto-relevant line cards fit, with the backplane port serving as the physical interface.

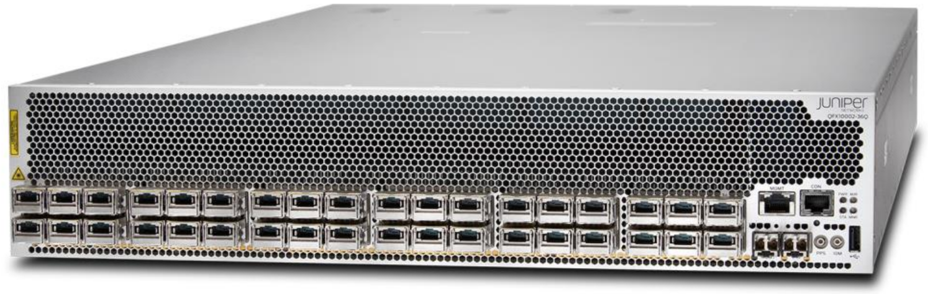

Figure 1 – QFX10002

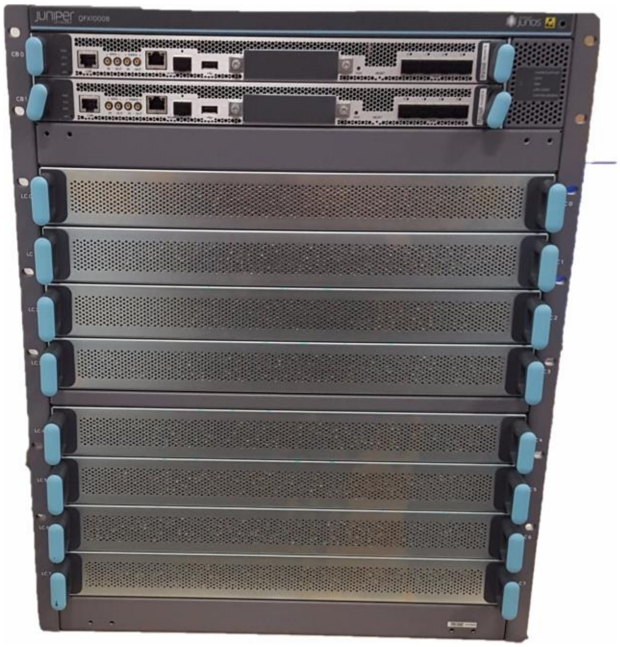

Figure 2 – QFX10008

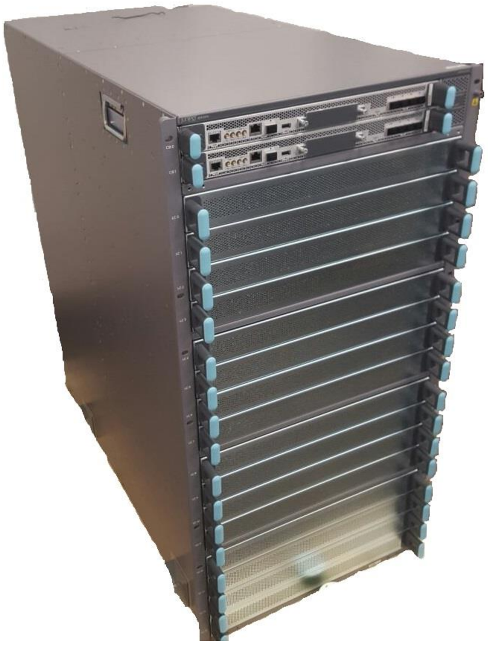

Figure 3 – QFX10016

Table 3 – Ports and Interfaces

Port	Device (# of ports)	Description	Logical Interface Type

Ethernet	QFX10002-36Q(39: 1 MGMT, 36 QSFP+, 2 SFP)
	QFX10002-72Q(79: 1 MGMT, 72 QSFP+, 2 SFP)
	QFX10008(12: 4 MGMT, 8 SFP+)
	QFX10016(12: 4 MGMT, 8 SFP+)
		LAN Communications	Control in, Data in, Data out, Status out

Serial	QFX10002(1)
	QFX10008(2)
	QFX10016(2)
		Serial Console Port	Control in, Status out

SMB	QFX10002(2)
	QFX10008(8)
	QFX10016(8)
		PTP Connectors	Control in, status out

Power	QFX10002-36Q(2)
	QFX10002-72Q(4)
	QFX10008(8)
	QFX10016(10)
		Power connector	Power

Reset	QFX10002(1)
	QFX10008(2)
	QFX10016(2)
		Reset	Control in

LED	QFX10002(4)
	QFX10008(13)
	QFX10016(13)
		Status indicator lighting	Status out

USB	QFX10002(1)
	QFX10008(2)
	QFX10016(2)
		Load Junos OS image/configuration	Data in, Data out

Backplane Line Card Interface	QFX10002-72Q(12)
	QFX10008(8)
	QFX10016(16)
		Line card interface	Control in, Data in, Data out, Status out

1.2 Mode of Operation

The QFX switches support a FIPS Approved mode of operation and a non-approved mode. The cryptographic officer can configure the module to run in a FIPS Approved mode of operation by following the instructions in the crypto-officer guidance. When running in FIPS Approved mode of operation, the CLI interface will suffix the user name shown on the command prompt with the text ":fips".

1.2.1 Non-Approved Mode

The cryptographic module supports a non-Approved mode of operation. When operated in the non-Approved mode of operation, the module supports the algorithms identified in Section 2.4 as well as the algorithms supported in the Approved mode of operation.

If the module has been in a FIPS- Approved mode of operation, the cryptographic officer can configure the module to run in a non-Approved mode by following the instruction in the cryptographic officer guidance.

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 non-Approved mode of operation and the Approved mode of operation, the Cryptographic Officer must run the following commands to zeroize the Approved mode CSPs:

```
user@host> request system zeroize
```

This command wipes clean all the CSPs/configs. Perform system zeroization with care. After the zeroization process is complete, no data is left on the Routing Engine. The QFX device is returned to the factory default state.

Use of the zeroize command is restricted to the Cryptographic Officer. The cryptographic officer shall perform zeroization in the following situations:

1. Before FIPS Operation: To prepare the device for operation as a FIPS cryptographic module by erasing all CSPs and other user-created data on a device before its operation as a FIPS cryptographic module.
2. Before non-FIPS Operation: To conduct erasure of all CSPs and other user-created data on a device in preparation for repurposing the device for non-FIPS operation.

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. Allowed Protocols summarizes the high-level protocol algorithm support.

2.1 Approved Algorithms

Table 4 - OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
5459	AES	PUB 197-38A	CBC CTR ECB	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		SP 800-38D	GCM[1]	Key Sizes: 128, 192, 256	Encrypt, Decrypt, AEAD
N/A[2]	CKG	SP 800-133	Section 6.1 Section 6.2		Asymmetric key generation using unmodified DRBG output
2142	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
1458	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer, KeyVer
3617	HMAC	PUB 198	SHA-1	Key size: 512, λ = 80,160	Message Authentication
			SHA-224	Key size: 512, λ = 112	
			SHA-256	Key size: 512, λ = 128,256	Message Authentication; DRBG Primitive
			SHA-384	Key size: 1024, λ = 192,384	Message Authentication
			SHA-512	Key size: 1024 bits, λ = 256,512	
2931	RSA	PUB 186-4		n=2048,3072,4096 (SHA 256, 384, 512)	KeyGen[3] , SigGen, SigVer[4]
4381	SHS	PUB 180-4	SHA-1 SHA-224 SHA-256		Message Digest Generation, KDF Primitive

[1] AES GCM was validated, however it is not used by any service in the module

[2] Vendor Affirmed

[3] 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.

[4] 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.

			SHA-384 SHA-512		
2746	Triple-DES	SP 800-67	CBC	Key Size: 192	Encrypt, Decrypt
1909	CVL	SP 800-135	SSH	SHA 1, 256, 384, 512	Key Derivation
N/A[5]	KAS ECC	SP 800-56Arev3	ECCDH	P256 SHA-256 P384 SHA-384 P521 SHA-512	Key Agreement Scheme - Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135 (SSH KDF CVL Cert. #1909)

Table 5 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
3616	HMAC	PUB 198-1	SHA-1	Key size: 512, λ = 80,160	
			SHA-256	Key size: 512, λ = 128,256	
4380	SHS	PUB 180-4	SHA-1 SHA-256 SHA-512		Message Digest Generation

Table 6 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
2141	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
3615[6]	HMAC	PUB 198-1	SHA-1	Key size: 512, λ = 80,160	DRBG Primitive
			SHA-256	Key size: 512, λ = 128,256	
4379[7]	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Authentication DRBG Primitive

[5] Vendor Affirmed per IG D.1-rev3

[6] HMAC SHA1 was validated, however it is not used by any service in the module

[7] SHA-384 and SHA-512 were validated, however neither are used by any service in the module

2.2 Allowed Algorithms

Table 7 – 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 DRBG

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, RSA	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, have been tested by the CAVP and CMVP. The SSH algorithm allows independent selection of key exchange, authentication, cipher and integrity. In reference to the Allowed Protocols in Table 10 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 Disallowed Algorithms

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

- RSA with keys less than 2048 bits
- ARCFOUR
- Blowfish
- CAST
- DSA (SigGen, SigVer; non-compliant)
- HMAC-MD5
- HMAC-RIPEMD160
- UMAC
- AES GCM

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 or RSA. 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
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 10 – Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256 or RSA.
SSH-ECDH-PUB	Elliptic Curve Diffie-Hellman public component. Ephemeral Diffie-Hellman public key used in SSH key establishment. ECDH P-256, or ECDH P-384, ECDH-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

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.

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 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.

RSA signature verification: SSH public-key authentication. Processing constraints allow for a maximum of 5.6e7 RSA attempts per minute. The module supports RSA (2048, 3072, 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. 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 $5.6e7/(2^{112})$, which is less than 1/100,000.

3.3 Services

All services implemented by the module are listed in the tables below. Table 15 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
Load Image	Verification and loading of validated firmware image into the switch	X	
Remote reset	Software initiated reset (used to perform self-tests on demand).	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

	CSPs								
Service	DRBG_Seed	DRBG_State	Entropy Input String	SSH PHK	SSH DH	SSH-SEK	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	GWR	--	--	G	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	-	-
Load Image	-	-	-	-	-	-	--	-	-
Local reset	GEZ	GZ	GZ	--	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) which supports the security functions identified in Section 2.4 and the SSHv2 row of 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
Load Image (non-compliant)	Verification and loading of validated firmware image into the switch	X	
Remote reset (non-compliant)	Software initiated reset (used to perform self-tests on demand).	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 have 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**
    - 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-224 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - AES-CBC (128/192/256) Encrypt KAT
    - AES-CBC (128/192/256) Decrypt KAT
    - KDF SSH KAT
- **LibMD KATs**
    - HMAC-SHA-1 KAT
    - HMAC-SHA2-256 KAT
    - SHA-2-512 KAT
- **Kernel KATs**
    - SP 800-90A HMAC DRBG KAT
        - Health-tests initialize, re-seed, and generate
    - Triple DES CBC KAT
    - HMAC-SHA2-256 KAT
    - SHA-2-384 KAT
    - SHA-2-512 KAT
    - AES-CBC 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 NDRNG and OpenSSL DRBG
- 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 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 determine whether firmware being loaded is a legacy use of the firmware load service.
12. The cryptographic officer must retain control of the module while zeroization is in process.
13. The cryptographic officer must configure the module to ensure the module does not encrypt more than 2^20 blocks with a single Triple-DES key when Triple-DES is the encryption-algorithm.
14. Virtualized Network Functions (VNFs) shall not be configured in FIPS-mode of operation.
15. RSA host keys generated for SSHv2 must be 2048 bits or greater.

6.1 Crypto-Officer Guidance

6.1.1 Enabling FIPS-Approved Mode of Operation

The crypto-officer is responsible for initializing the module in a FIPS Approved mode of operation. The FIPS-Approved mode of operation is not automatically enabled. The Crypto-officer should execute the following steps:

1. Zeroize the QFX switch according to the instructions in the section 1.3.

2. To enable FIPS mode in Junos OS on the switch:

   a. Enter configuration mode:

      ```
      root@switch> configure
      Entering configuration mode
      [edit]
      root@switch#
      ```

   b. Enable FIPS mode on the switch by setting the FIPS level to 1, and verify the level:

      ```
      [edit]
      root@switch# set system fips level 1
      [edit]
      root@switch# show system fips level level 1;
      ```

c. Commit the configuration:

```
{master:0}[edit security]
root@switch# commit
configuration check succeeds
[edit]
'system'
reboot is required to transition to FIPS level 1
commit complete
```

d. Reboot the Switch:

```
[edit]
root@switch# run request system reboot
Reboot the system ? [yes,no] (no) yes
```

6.1.2 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 switch to return it to a non-Approved mode of operation. To disable FIPS-Approved mode on the switch, 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 switch. If the string ":fips" is present then the switch 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 switches and documentation in a secure area.
- Deploy 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

Table 16 – Acronyms and Definitions

Acronym	Definition
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
ICV	Integrity Check Value (i.e. Tag)
IOC	Input/Output Card
MD5	Message Digest 5
NPC	Network Processing Card
RE	Routing Engine
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SHA	Secure Hash Algorithms
SMB	Server Message Block
SPC	Services Processing Card
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 17 – Datasheets

Model	Title	URL
QFX10002 QFX10008 QFX10016	QFX10000 Modular Ethernet Switches	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000529-en.pdf