**National Information Assurance Partnership**

**Common Criteria Evaluation and Validation Scheme**


TM

# Validation Report

**for the**

**Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016, Version 1.1**

| | |
|---|---|
| **Report Number:** | **CCEVS-VR-VID10930-2019** |
| **Dated:** | **January 28, 2019** |
| **Version:** | **1.1** |

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6940**
**Fort George G. Meade, MD 20755-6940**

**ACKNOWLEDGEMENTS**

**Validation Team**

Meredith Hennan

Kenneth Stutterheim

*The Aerospace Corporation*

**Common Criteria Testing Laboratory**

Acumen Security, LLC

## Table of Contents

## 1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user to determine the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in January 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314 (NDcPPv2.0e).

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

## 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| **Evaluation Scheme** | United States NIAP Common Criteria Evaluation and Validation Scheme |
| **TOE** | Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 |
| **Protection Profile** | Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018 (NDcPPv2.0e) |
| **Security Target** | Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 Security Target, Version 1.5, January 2019 |
| **Evaluation Technical Report** | Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 ETR, Version 1.2 January 2019 |
| **CC Version** | Version 3.1 Revision 4 |
| **Conformance Result** | CC Part 2 Extended and CC Part 3 Conformant |
| **Sponsor** | Juniper Networks, Inc. |
| **Developer** | Juniper Networks, Inc. |
| **Common Criteria Testing Lab (CCTL)** | Acumen Security<br>2400 Research Blvd<br>Rockville, MD 20850 |
| **CCEVS Validators** | Meredith Hennan, Kenneth Stutterheim |

## 3 Architectural Information

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 18.1R2 executing on QFX10K-Series Ethernet Switches. The supported QFX10K-Series chassis are:

- QFX10002
- QFX10008
- QFX10016

Each of the Ethernet Switches is a secure network device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. All switching platforms are powered by the Junos OS firmware, Junos OS 18.1R2 for QFX10K Series, which is a special purpose OS that provides no general-purpose computing capability. Junos OS provides both management and control functions as well as all IP switching.

The Ethernet Switches primarily support the definition and enforcement of information flow policies among network nodes. All information flow from one network node to another passes through an instance of the TOE. Information flow is controlled based on network node addresses and protocol. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited and provides the security tools to manage the security functions.

## 4 Security Policy

The logical boundary of the TOE includes those security functions implemented exclusively by the TOE.

**Protected Communications**

The TOE provides an SSH server to support protected communications for administrators to establish secure sessions and to support connections from external syslog servers. The TOE requires that applications exchanging information with it are successfully authenticated prior to any exchange (i.e. applications connecting over SSH). The TOE includes cryptographic modules that provide the underlying cryptographic services, including key management and protection of stored keys, algorithms, random bit generation and crypto-administration. The cryptographic modules provide confidentiality and integrity services for authentication and protecting communications with connecting applications.

**Administrator Authentication**

Administrative users must provide unique identification and authentication data before any administrative access to the system is granted. Authentication data entered and stored on the TOE is protected. The TOE can be configured to terminate interactive user sessions and to present an access banner with warning messages prior to authentication.

**Correct Operation**

The TOE provides for both cryptographic and non-cryptographic self-tests, and is capable of automated recovery from failure states.

**Trusted Update**

The administrator can initiate update of the TOE firmware. The integrity of any firmware updates is verified prior to installation of the updated firmware.

**Audit**

Junos auditable events are stored in the syslog files on the appliance, and can be sent to an external log server (via Netconf over SSH). Auditable events include start-up and shutdown of the audit functions, authentication events, as well as the events listed in Table 4. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). Local syslog storage limits are configurable and are monitored. In the event of storage limits being reached the oldest logs will be overwritten.

**Management**

The TOE provides a Security Administrator role that is responsible for:

- the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product

- the regular review of all audit data;
- initiation of trusted update function;
- all administrative tasks (e.g., creating the security policy).

The devices are managed through a Command Line Interface (CLI). The CLI is accessible through local (serial) console connection or remote administrative (SSHv2) session.

# 5 Assumptions, Threats & Clarification of Scope

## 5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

| Assumption | Description |
|---|---|
| A.PHYSICAL_PROTECTION | The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the [NDcPP] will not include any requirements on physical tamper protection or other physical attack mitigations. The [NDcPP] will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. |
| A.LIMITED_FUNCTIONALITY | The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). |
| A.NO_THRU_TRAFFIC_PROTECTION | A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall). |
| A.TRUSTED_ADMINISTRATOR | The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength |

| | |
|---|---|
| | and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. |
| A.REGULAR_UPDATES | The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities. |
| A.ADMIN_CREDENTIALS_SECURE | The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside. |
| A.RESIDUAL_INFORMATION | The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. |

### 5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

| Threat | Description |
|---|---|
| T.UNAUTHORIZED_ADMINISTRATOR_ACCESS | Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides. |
| T.WEAK_CRYPTOGRAPHY | Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort. |

| | |
|---|---|
| T.UNTRUSTED_COMMUNICATION_CHANNELS | Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself. |
| T.WEAK_AUTHENTICATION_ENDPOINTS | Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised. |
| T.UPDATE_COMPROMISE | Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration. |
| T.UNDETECTED_ACTIVITY | Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised. |
| T.SECURITY_FUNCTIONALITY_COMPROMISE | Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. |
| T.PASSWORD_CRACKING | Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices. |
| T.SECURITY_FUNCTIONALITY_FAILURE | An external, unauthorized entity could make use of failed or compromised security functionality and might therefore |

| | |
|---|---|
| | subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device. |

### 5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPPv2.0e.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

### 5.4 Excluded Functionality

The following security capabilities of the device were not tested as part of the evaluation although they are represented in the administrative guide; therefore, no claims can be made regarding their proper operation or effectiveness:

- Access Control Lists as part of stateless firewall filtering capability
- Reverse Path Forwarding
- Routing Engine IPSec

The following capabilities are Out-of-Scope for this evaluation:

- Use of telnet, since it violates the Trusted Path requirement
- Use of FTP, since it violates the Trusted Path requirement
- Use of SNMP, since it violates the Trusted Path requirement
- Use of SSL, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement
- Use of CLI account super-user and Linux root account.

## 6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 Security Target
- Junos OS Common Criteria and FIPS Evaluated Configuration Guide for QFX10K Ethernet Switches Release 18.1R2

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The TOE is the Junos OS 18.1R2-S3 firmware running on the appliance chassis listed in table 2 of ST. Hence the **TOE is contained within the physical boundary of the specified appliance chassis** as shown in figure 1 below.

The **physical boundary of the TOE is:**

- QFX10002 Ethernet Switches – the entirety of the Fixed Ethernet Switch appliance (either QFX10002-72Q or QFX10002-36Q switch)
- QFX10008 and QFX10016 Modular Ethernet Switches – the chassis populated with at least one instance of the QFX10000 Control Board and one or more or the line cards listed in Table .

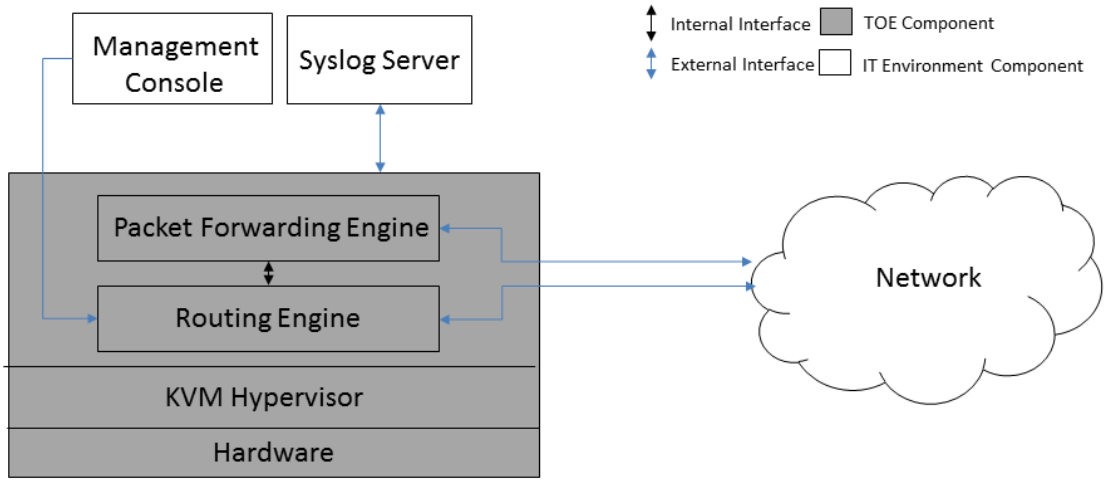


**Figure 1 TOE Boundary**

Separate install images are provided for QFX10002 and QFX10008/QFX10016, namely:

- **QFX10002**: jinstall-host-qfx-10-f-x86-64-18.1R2-S3.3-secure-signed.tgz
- **QFX10008/QFX10016**: jinstall-host-qfx-10-m-x86-64-18.1R2-S3.3-secure-signed.tgz

The TOE interfaces comprise the following:

i. Network interfaces which pass traffic

ii. Local and Remote Management interfaces used for administrative actions.

| Ethernet Switch Model | Network Ports | Routing Engine | Firmware |
|---|---|---|---|
| QFX10002 | QSFP+ for 40GbE speeds<br>QSFP28 ports for 100GbE speeds | Fixed in QFX10002 chassis | Junos OS 18.1R2 |
| QFX10008 | • QFX10000-36Q, a 36-port 40GbE quad small form-factor pluggable plus transceiver (QSFP+) or 12-port 100GbE QSFP28 line card<br>• QFX10000-30C, a 30-port 100GbE QSFP28/40GbE QSFP+ line card<br>• QFX10000-60S-6Q, a 60-port 1GbE/10GbE SFP/SFP+ line card with six-port 40GbE QSFP+ / two-port 100GbE QSFP28<br>• QFX10008 Switch Fabric | QFX10000 Control Board | |
| QFX10016 | • QFX10000-36Q, a 36-port 40GbE quad small form-factor pluggable plus transceiver (QSFP+) or 12-port 100GbE QSFP28 line card<br>• QFX10000-30C, a 30-port 100GbE QSFP28/40GbE QSFP+ line card<br>• QFX10000-60S-6Q, a 60-port 1GbE/10GbE SFP/SFP+ line card with six-port 40GbE QSFP+ / two-port 100GbE QSFP28<br>• QFX10016 Switch Fabric | QFX10000 Control Board | |

**Table 2 TOE Chassis Details**

The firmware version reflects the detail reported for the components of the Junos OS when the "show version" command is executed on the appliance.

The guidance documents included as part of the TOE are:

[ECG] Junos OS Common Criteria and FIPS Evaluated Configuration Guide for QFX10K Ethernet Switches Release 18.1R2

To use the product in the evaluated configuration, the product must be configured as specified in the Junos OS Common Criteria and FIPS Evaluated Configuration Guide for QFX10K Ethernet Switches Release 18.1R2. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

# 8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016, which is not publicly available. The publicly available Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

## 8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

## 8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

## 9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR) and summarized in the publicly available Assurance Activity Report (AAR) for this evaluation. The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the NDPP and Supporting Document (SD).

### 9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

### 9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

### 9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP and the Supporting Document Evaluation Activities for Network Device cPP, and that the conclusion reached by the evaluation team was justified.

### 9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities performed vulnerability testing and did not discover any issues with the TOE. A search of publicly available sources was performed on November 19, 2018. A follow up search was performed on January 2, 2019 using the following search terms:

- JunOS 18.1R2
- QFX10K
- QFX10000

- QFX10002
- QFX10008
- QFX10016
- WindRiver
- WindRiver 7
- QFX10K-Kernel
- WRL7
- SSH
- QFX10K-OpenSSL

The sources of the publicly available information search are provided below.

- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the NDcPPv2.0e, and that the conclusion reached by the evaluation team was justified.

### 9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the NDcPPv2.0e, and correctly verified that the product meets the claims in the ST.

## 10 Validator Comments & Recommendations

Administrators of the devices should note that if the audit storage space on the TOE is exhausted, the TOE continues to operate.

The AGD points out that the devices must be configured into FIPS mode to meet the requirements of the Common Criteria evaluated mode. Note that FIPS mode sets AES192-CBC and AES192-CTR which are not allowed in the Common Criteria evaluated configuration. Therefore, administrators should follow the configuration as set forth in the section titled "Configuring SSH on the Evaluated Configuration for NDcPP"

NIST CAVP algorithms were tested on JunOS 18.1r1. The vendor asserts this version of the JunOS is identical to the tested version with the exception of bug fixes, and that there were no changes to the implementation of the cryptographic functionality.

## 11 Annexes

Not applicable.

## 12 Security Target

Junos OS 18.1R2 for QFX10002, QFX10008 and QFX100016 Security Target

## 13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

## 14 Bibliography

The Validation Team used the following documents to produce this Validation Report:


1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Security Target Junos OS 18.1R2 for QFX10002, QFX 10008, and QFX10016 Series Devices, Version 1.5, January 2019.
6. Common Criteria and FIPS Evaluated Configuration Guide for QFX10002, QFX 10008, and QFX10016 Series Devices Release 18.1R2, 2018-12-31.
7. Junos OS 18.1R2 for QFX10002, QFX 10008, and QFX10016 Common Criteria NDcPP Assurance Activity Report, Version 1.4, January 2019.
8. Vulnerability Assessment for Junos OS 18.1R2 for QFX10002, QFX 10008, and QFX10016, Version 1.1, January 2019. (evaluation sensitive)
9. Junos OS 18.1R2 for QFX10002, QFX 10008, and QFX10016 Evaluation Technical Report, Version 1.2, January 2019. (evaluation sensitive)
10. Test Plan for a Target of Evaluation, Version 1.2, January 22, 2019. (evaluation sensitive)