National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

QFX5120-48YM switch on JUNOS 23.4R2

Report Number: CCEVS-VR-VID11650-2026
Dated: April 08, 2026
Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant

Jenn Dotson

Lisa Mitchell

Jaemond Reyes

Randy Heimann

Lori Sarem

Charles Schmidt

The MITRE Corporation

Common Criteria Testing Laboratory

Furukh Siddique

Yogita Kore

Alex Fannin

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 in determining 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 QFX5120-48YM switch on JUNOS 23.4R2 Series 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 April 2026. 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 of the *PP-Configuration for Network Devices and MACsec Ethernet Encryption*, Version 2.0, 2024-04-25 [CFG_NDcPP-MACsec_V2.0] and *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [PKG_SSH_V1.0]. The PP-Configuration includes the following components: *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (CPP_ND_V3.0E) and *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 2023-03-02 (MOD_MACsec_V1.0).

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev. 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR 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 ETR 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 of the functional requirements and assurance requirements stated in the 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 ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT 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 Compliant 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	QFX5120-48YM switch on JUNOS 23.4R2
Protection Profile	*PP-Configuration for Network Devices and MACsec Ethernet Encryption*, Version 2.0, 2024-04-25 [CFG_NDcPP-MACsec_v2.0]. This PP-Configuration includes the following: • *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] • *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 2023-03-02 [MOD_MACsec_V1.0] Additional Package is claimed as follows: • *Functional Package for Secure Shell (SSH)*, Version 1.0, May 13, 2021[PKG_SSH_V1.0].
Security Target	*QFX5120-48YM switch on JUNOS 23.4R2 Security Target*, v1.0, March 27, 2026
Evaluation Technical Report	*Evaluation Technical Report for QFX5120-48YM switch on JUNOS 23.4R2,* version 0.5, March 27, 2026
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	HPE Juniper Networking
Developer	HPE Juniper Networking
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security, 2400 Research Blvd Suite 395 Rockville, MD 20850

Item	Identifier
CCEVS Validators	Sheldon Durrant Jenn Dotson Lisa Mitchell Jaemond Reyes Randy Heimann Lori Sarem Charles Schmidt

3 Architectural Information

Note: The following description is based on the information presented in Section 1 of the ST.

3.1 TOE Overview

The TOE is the Juniper Networks Inc QFX5120-48YM switch on JUNOS 23.4R2 with MACsec and is comprised of both hardware and software. The following appliance models constitute the variations of the TOE:

- QFX5120 with Junos OS 23.4R2 software, offering 48 25GbE (SFP28)/10GbE (SFP+)/1GbE (SFP) ports.
- AES ECB 128bit & 256bit Encryption/Decryption Engine (BCM82391)

The TOE is a secure network device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. It includes the Junos OS firmware, JUNOS OS 23.4R2, which is a special purpose OS offering no general-purpose computing capabilities. Junos OS implements both management and control functions as well as all IP routing.

The appliance's primary function is to support the definition and enforcement of information flow policies among network nodes. Each information flow from one network node to other passes through an instance of the TOE. Information flow is controlled based on network node addresses and protocol. The TOE also ensures that security-relevant activity is audited and implements the necessary tools to manage all security functions.

The TOE implements MACsec between adjacent devices. All traffic communicated between the devices including frames for LLDP (Link Layer Discovery Protocol), DHCP (Dynamic Host Configuration Protocol), ARP (Address Resolution Protocol), STP (Spanning Tree Protocol), Ethernet Control frames, etc. (the exceptions to this protection are Destination MAC and Source MAC addresses in MACsec and MKA frames).

3.2 TOE Architecture

The TOE implements a variety of high-speed interfaces (only Ethernet is in the scope of the evaluation) for enterprise branch, campus, and data center networks. The appliance is physically self-contained, housing the firmware and hardware necessary to perform all routing functions. The architecture components of the TOE are:

- Switch fabric – the switch fabric boards/modules provide a highly scalable, non-blocking, centralized switch fabric matrix through which all network data passes.
- Routing Engine (Control Board) – the Routing Engine (RE) runs the Junos firmware and implements Layer 3 routing services and Layer 2 switching services. The RE also implements the management functions for configuration and operation of the TOE and controls the flow of information through the TOE, including support for appliance interface control and control plane functions such as chassis component, system management and user access to the appliance.
- Layer 2 switching services, Layer 3 switching/routing services and network management for all operations necessary for the configuration and operation of the TOE and controls the flow of information through the TOE.

- Packet Forwarding Engine (PFE) – The PFE implements all operations necessary for transit packet forwarding. The PFE implements an extensive set of Layer 2 and Layer 3 services that can be deployed in any combination of L2- L3 applications.
- Power – The TOE includes non-PoE ports. Power supply bays allow flexibility for provisioning and redundancy. The power supplies connect to the midplane, which distributes the different output voltages produced by the power supplies to the appliance components, depending on their voltage requirements.

The appliance supports numerous routing and switching standards for flexibility and scalability. Juniper's Virtual Chassis technology allows multiple interconnected switches to operate as a single, logical unit, enabling users to manage all platforms as one virtual device. The functions of the appliances can all be managed through the Junos firmware, either from a connected terminal console or via a network connection. Network management is secured using the SSH protocol. All management, whether from a user connecting to a terminal or from the network, requires successful authentication. In the evaluated deployment the TOE is managed and configured via Command Line Interface, either via a directly connected console or over the network secured using the SSH protocol.

3.3 TOE Evaluated Platforms

Detail regarding the evaluated configuration and any excluded functionality is provided in Section 8.

3.4 Physical Boundaries

The following figure provides a visual depiction of an example TOE deployment, including physical boundaries and other components in the operational environment.

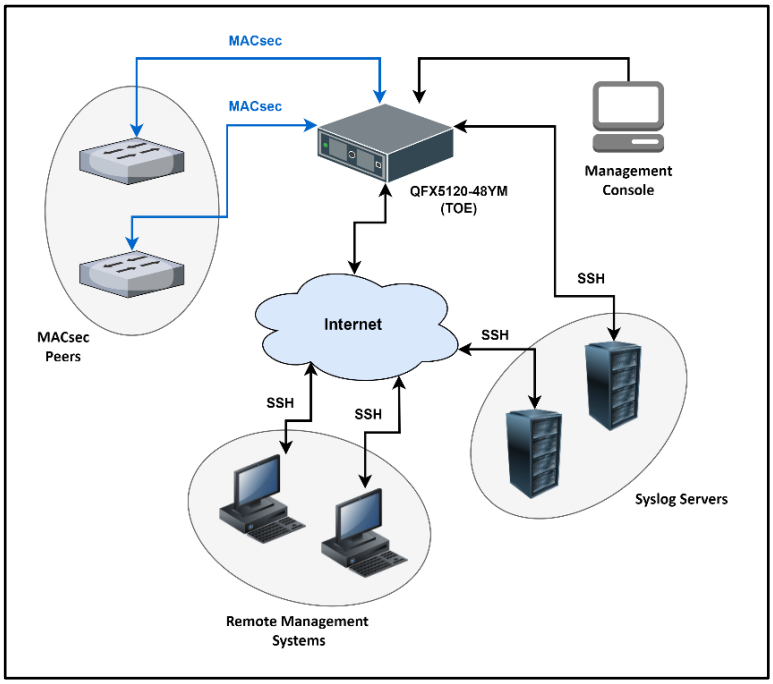

Figure 1 Representative TOE Deployment

4 Security Policy

The TOE provides the security functions required by the CFG_NDcPP-MACsec_v2.0 and PKG_SSH_V1.0.

4.1 Security Audit

The TOE generates audit events for all start-up and shutdown functions as well as all auditable events specified in **Error! Reference source not found.**. 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, and all SFR-specific events required by the applicable Protection Profiles. 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. If the storage limit is reached the oldest logs will be overwritten.

4.2 Cryptographic Support

The TOE implements an SSH server to support protected communications for administrators to establish secure sessions and to connect to 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). Communication over point-to-point links between Juniper appliances can be secured using MACsec. The TOE includes cryptographic modules that implement 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 for protecting communications with connecting applications. Details on cryptographic implementations by the TOE are documented in the ST.

4.3 Identification and Authentication

The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to being granted access to any management actions. The TOE supports password-based authentication and public key based authentication. Based on the assigned role, a user is granted a set of privileges to access the system. 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.

4.4 Security Management

The TOE provides a Security Administrator role that is responsible for

- configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product;
- regular review of all audit data;
- initiation of trusted update function;
- administration of MACsec functionality;
- 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 (SSH) session.

4.5 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored using sha256 or sha512. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE internally maintains the date and time.

4.6 TOE Access

The TOE displays a customizable banner before any administrative session can be established with it. The TOE will terminate local or remote interactive sessions after a specified period of session inactivity configured by an administrator. An administrator can terminate their own interactive local or remote sessions.

4.7 Trusted Path/Channels

The TOE supports SSH for secure communications with authorized IT entities such as syslog servers. The TOE supports SSHv2 (remote CLI) for secure remote administration. The TOE also supports MACsec for securing data at Layer 2 between TOE and MACsec supporting peer device.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 (NDcPP30E)
- *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MOD_MACsec_V1.0)
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 (PKG_SSH_V1.0)

That information has not been reproduced here. The NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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:

- 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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0.
- Apart from the Admin Guide, additional customer documentation for the specific TOE models was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device in the evaluated configuration.
- Consistent with the expectations of the PP, 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.

6 Documentation

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

- *QFX5120-48YM switch on JUNOS 23.4R2 Security Target*, v1.0, March 27, 2026
- *Common Criteria Evaluated Configuration Guide for QFX5120-48YM Device*, 2026-03-27

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

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 be relied upon when configuring or operating the device as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the following proprietary document:

- *Evaluation Technical Report for QFX5120-48YM switch on JUNOS 23.4R2,* version 0.5, March 27, 2026

The AAR provides an overview of testing and the prescribed assurance activities.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the QFX5120-48YM switch with the JUNOS 23.4R2 operating system and the AES ECB 128bit & 256bit Encryption/Decryption Engine.

8.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- Telnet
- FTP
- SNMP
- HTTPS and SSL, including management via J-Web, JUNOScript and JUNOScope
- NTP
- CLI account with super-user privileges, and
- Linux root account(s)

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 ETR. The reader of this document can assume that all 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. 5 and CEM version 3.1 Rev. 5. The evaluation determined the QFX5120-48YM switch on JUNOS 23.4R2 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0 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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0.

The validation team 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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0 related to the examination of the information contained in the TOE Summary Specification.

The validation team 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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0 related to the examination of the information contained in the operational guidance documents.

The validation team 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 validation team 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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0 and recorded the results in a Test Report, summarized in the ETR and AAR.

The validation team 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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0, 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.

The evaluation team performed a public search against the following sources to ensure there are no publicly known and exploitable vulnerabilities in the TOE:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog),
- CVE Database (https://www.cve.org/),
- Security Advisories (https://kb.juniper.net)

The initial vulnerability searches were performed in March 2025, January 2026, February 2026. A final search was carried out on March 27th, 2026, to ensure no additional vulnerabilities were found. No open vulnerabilities applicable to the TOE were identified. The search was conducted with the following terms:

- JunOS 23.4R2 (cpe:2.3:o:juniper:junos:23.4:r2:*:*:*:*:*:*:*)
- Juniper QFX5120 (cpe:2.3:h:juniper:qfx5120:-:*:*:*:*:*:*:*:*)
- Openssl 1.1.1zb
- Openssh 9.7p1 (cpe:2.3:a:openbsd:openssh:9.7:p1:*:*:*:*:*:*:*)
- Intel Xeon D-1627

- Junos libMD
- Broadcom BCM82391

The validation team 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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0, 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 NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Common Criteria Evaluated Configuration Guide for QFX5120-48YM Device*, Release 23.4R2, March 27, 2026. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described NDcPP30E/ MOD_MACsec_V1.0/ PKG_SSH_V1.0 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is the *QFX5120-48YM switch on JUNOS 23.4R2 Security Target*, v1.0, March 27, 2026.

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 5.
2. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5.
3. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
5. *PP-Configuration for Network Devices and MACsec Ethernet Encryption*, Version 2.0, 2024-04-25 [CFG_NDcPP-MACsec_v2.0].
6. *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E].
7. *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 [MOD_MACsec_V1.0].
8. *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [PKG_SSH_V1.0].
9. *QFX5120-48YM switch on JUNOS 23.4R2 Security Target*, v1.0, March 27, 2026.
10. *Common Criteria Evaluated Configuration Guide for QFX5120-48YM Device*, 2026-03-27.
11. *Assurance Activity Report for QFX5120-48YM switch on JUNOS 23.4R2*, V0.5, April 2026.
12. *Evaluation Technical Report for QFX5120-48YM switch on JUNOS 23.4R2*, Version 0.5, March 27, 2026.*Vulnerability Assessment for QFX5120-48YM switch on JUNOS 23.4R2*, Version 0.4, March 27, 2026.
13. *Test Plan for QFX5120-48YM SWITCH on JUNOS 23.4R2*, Version 1.1, March 27, 2026.