National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

JUNOS 24.4R2 FOR MX240/480/960 ROUTERS AND EX9204/9208/9214 SWITCHES

Report Number: CCEVS-VR-VID11700 -2026

Dated: June 25, 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

Jaemond Reyes

Jenn Dotson

Lisa Mitchell

Lori Sarem

Randy Heimann

Sheldon Durrant

The MITRE Corporation

Common Criteria Testing Laboratory

Pratheek Menon

Manohar Negi

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 Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches 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 June 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 (CFG_NDcPP-MACsec_V2.0) which includes the following components:
    - *collaborative Protection Profile for Network Devices,* Version 3.0e, 6 December 2023 [CPP_ND_V3.0E]
    - *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 [MOD_MACSEC_V1.0]
- *Functional Package for SSH,* Version 1.0, 13 May 2021, [PKG_SSH_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 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	Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches
Protection Profile	*PP-Configuration for Network Devices and MACsec Ethernet Encryption*, Version 2.0 (CFG_NDcPP-MACsec_V2.0) which includes the following components: • *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 [CPP_ND_V3.0E] • *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 [MOD_MACSEC_V1.0] *Functional Package for SSH*, Version 1.0, 13 May 2021, [PKG_SSH_V1.0]
Security Target	*Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches Security Target*, Version 0.6, June 18, 2026
Evaluation Technical Report	*Evaluation Technical Report for MX240/480/960 and EX9204/9208/9214 Switches on JUNOS 24.4R2*, Version 0.4, June 3, 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)	Acumen Security Rockville, MD

Item	Identifier
CCEVS Validators	The MITRE Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the ST. See the ST for a complete description of the TOE and capabilities.

The TOE is the HPE Juniper Networking Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches with MACsec on the MPC10E/EX9200/MPC3E Series Line Cards.

3.1 TOE Description

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 24.4R2, 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.

3.2 TOE Evaluated Platforms

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

3.3 TOE Architecture

The architecture components of the MX240, MX480, and MX960 are:

- **Modular Control Plane:** The platforms utilize a redundant Routing Engine (RE) for the control plane, with available models including the RE-S-X6-64G and RE-S-X6-128G, both featuring a 6-core 2.0 GHz CPU with 64 GB and 128 GB of memory, respectively.
- **Unified Operating System:** The architecture runs on the modular Junos OS, which provides routing, switching, security, and service features, as well as supporting automation tools and telemetry.
- **Programmable Forwarding:** At the core of the hardware is the programmable Trio chipset, which enables wire-rate forwarding, service agility, and allows for the implementation of inline services and telemetry.
- **Inline MACsec Technology:** The platforms support robust data plane security through features like integrated Layer 2 MACsec, with line cards such as the MPC-10E providing inline AES-256 MACsec line-side encryption.

The architecture components of the EX9204, EX9208, EX9214 are:

- **Modular Chassis Design:** The EX9204 (4-slot), EX9208 (8-slot), and EX9214 (14-slot) are modular chassis that share a common set of line cards, Routing Engines, and Switch Fabric modules.

- **Centralized Control Plane:** The architecture is built for high availability with support for redundant EX9200-RE2 Routing Engines. The RE2 features a six-core, 2 GHz Intel processor with 64 GB of DRAM to run the Junos OS and manage all control plane functions.
- **Programmable Forwarding ASIC:** The platforms are based on "Juniper One," a custom-designed ASIC that provides a programmable Packet Forwarding Engine (PFE), allowing new networking protocols and features to be added via software updates.
- **High-Density Cryptographic-Capable Line Cards:** The chassis support various line cards, including the EX9200-15C, which provides 15 ports of 100GbE/40GbE with Media Access Control Security (MACsec) capability, each of which can house 10-gigabit small form-factor pluggable plus (SFP+) transceivers and includes hardware support for cryptographic functions.
- **Integrated MACsec Technology:** These cryptographic capabilities are exposed via MACsec technology (IEEE 802.1ae) with AES-256-bit encryption, supported online cards like the EX9200-15C to provide link-layer data confidentiality, integrity, and authentication.
- **Secure OS and Logging:** The EX9200-RE2 runs the carrier-class Junos OS, which stores its images and system logs on dual 64 GB SSDs. For secure management, the OS provides secure access protocols, including SSHv2.
- **Separated Management and Control:** The EX9200-RE2 modules communicate with the line cards over a dedicated internal out-of-band Gigabit Ethernet control interface, separating management traffic from the data plane.

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.

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).

MACsec can be deployed in point-to-point mode or shared mode with multiple stations. In the evaluated configuration MACsec must be configured individually on each point-to-point Ethernet link, such that a pair of MACsec devices (connected by a physical medium) protect Ethernet frames switched or routed from one device to the other. The two MACsec devices are provided with a Connectivity Association Key (CAK) and utilize the MACsec Key Agreement

(MKA) protocol to create a secure tunnel. MKA is used by the two MACsec devices to agree upon MACsec keys. MACsec must be configured to protect all traffic between the devices, with the exception of the MKA or Ethernet control traffic such as EAP over LAN (EAPOL) frames. The devices will first exchange MKA frames, which serve to determine if the peer is an authorized peer and agree upon a shared key and MACsec cipher suite used to set up a transmit (Tx) Security Association (SA) and a receive (Rx) SA. Once the SAs are set up, MACsec-protected frames traverse the unprotected link.

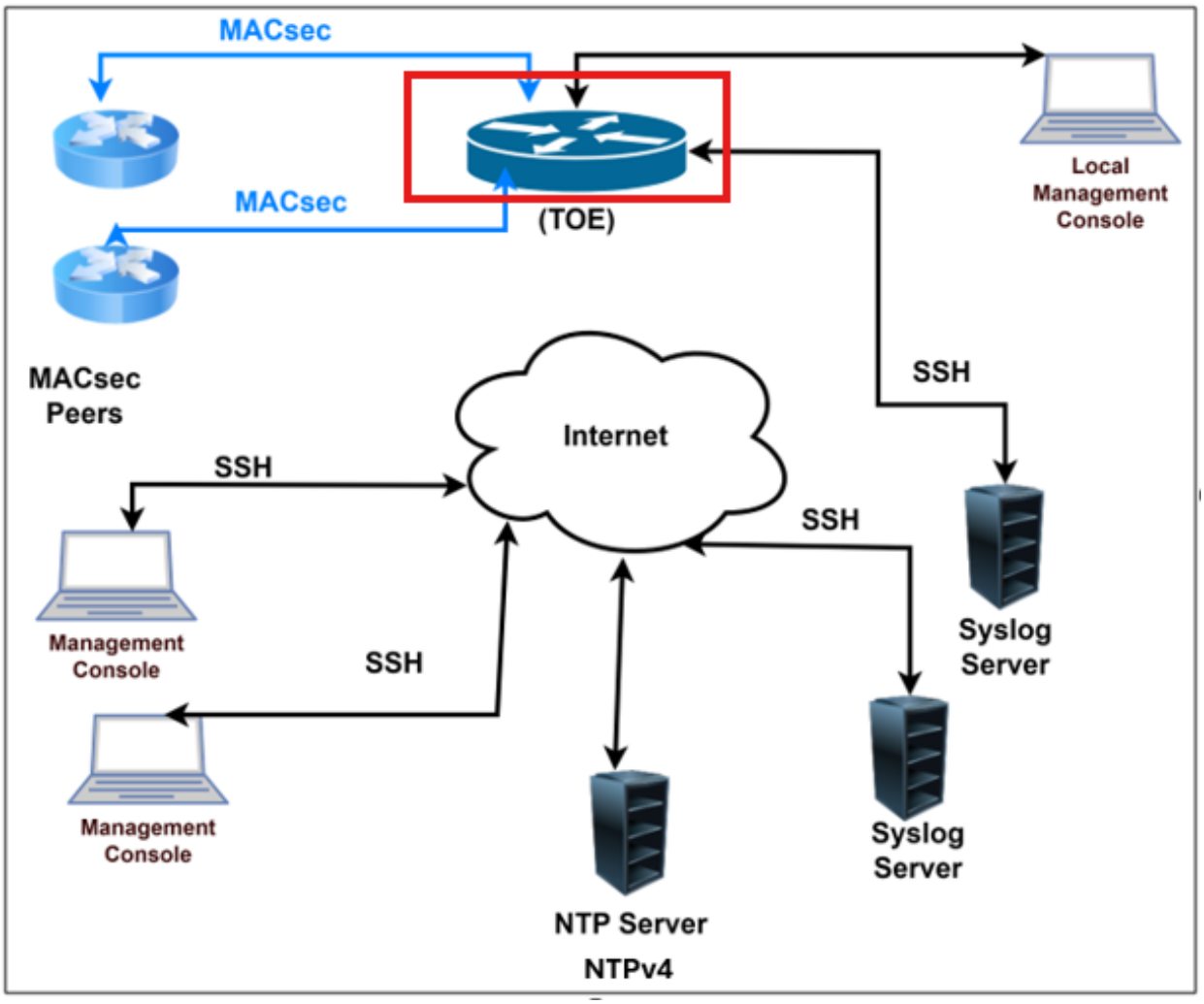
The following appliance models constitute the variations of the TOE:

Model	Routing Engine (RE)	RE-CPU	MACsec Line card	MIC-3D-10GE-SFP-E within MPC3E-3D-NG
MX240	RE-S-X6-128G RE-S-X6-64G	HASWELL-EP, Intel Xeon E5-2608L V3	MPC10E-10C and MPC10E-15C, with JNPR Penta Silicon MACsec ASIC	BCM82756 MACsec ASIC with CAVP num AES4550
MX480				
MX960				
EX9204	EX9200-RE2	HASWELL-EP, Intel Xeon E5-2608L V3	EX9200-15C with JNPR Penta Silicon MACsec ASIC	Not supported
EX9208				
EX9214				

Note that the RE-S-X6 and EX9200-RE2 routing engines have identical hardware and are simply marketed with different names.

3.4 Physical Boundaries

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded by a red line.


MACsec
MACsec
(TOE)
Local
Management
Console
MACsec
Peers
Internet
SSH
SSH
SSH
SSH
Management
Console
Management
Console
Syslog
Server
Syslog
Server
NTP Server
NTPv4

4 Security Policy

The TOE provides the security functions required by the CPP_ND_V3.0E, MOD_MACSEC_V1.0, and PKG_SSH_V1.0. These security functionalities are listed in more detail in the sections below.

4.1 Security Audit

The TOE generates audit events for all start-up and shutdown functions as well as all auditable events specified in Tables 12 and 13 of the ST. 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, Packages and Modules. 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). Layer 2 communication over point-to-point Ethernet links between the TOE and compliant peers 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 available 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:

- Ability to administer the TOE remotely
- Ability to configure the access banner
- Ability to configure the remote session inactivity time before session termination

- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Ability to start and stop services
- Ability to configure local audit behaviour
- Ability to modify the behaviour of the transmission of audit data to an external IT entity
- Ability to manage the cryptographic keys
- Ability to configure the cryptographic functionality
- Ability to configure thresholds for SSH rekeying
- Ability to re-enable an Administrator account
- Ability to configure the local session inactivity time before session termination or locking
- Ability to configure the authentication failure parameters for FIA_AFL.1
- Ability to set the time which is used for timestamps
- Ability to configure NTP
- Ability to administer the TOE locally
- Ability to manage the trusted public keys database
- Ability to manage a PSK-based CAK and install it in the device
- Ability to manage the Key Server to create, delete, and activate MKA participants using the CLI commands
- Ability to specify the lifetime of a CAK
- Ability to enable, disable, or delete a PSK-based CAK using CLI commands

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 allows manual setting of time by the administrator and is also capable of syncing time to an NTP server.

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 SSHv2 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
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021

That information has not been reproduced here and the CPP_ND_V3.0E, MOD_MACSEC_V1.0, and 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 CPP_ND_V3.0E, MOD_MACSEC_V1.0, and PKG_SSH_V1.0 as described for this TOE in the ST. 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:

- 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 claimed PP/PP-Modules/Package listed below.
    - *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 [CPP_ND_V3.0E]
    - *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 [MOD_MACSEC_V1.0]
    - *Functional Package for SSH*, Version 1.0, 13 May 2021, [PKG_SSH_V1.0].
- 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 this evaluation:

- *Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches Security Target*, Version 0.6, June 18, 2026
- *Junos® OS Common Criteria Evaluated Configuration Guide for MX240, MX480, MX960, EX9204, EX9208 and EX9214 Devices*, Release 24.4R2, June 18, 2026.

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

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 guides from the NIAP website to ensure the device is configured 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 *Evaluation Technical Report for MX240/480/960 and EX9204/9208/9214 Switches on JUNOS 24.4R2*, Version 0.4, 03 June 2026 [ETR], which is not publicly available. 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 claimed PP/PP-Modules/Package listed below:

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 [CPP_ND_V3.0E]
- *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 [MOD_MACSEC_V1.0]
- *Functional Package for SSH*, Version 1.0, 13 May 2021, [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 following models:

Model	Routing Engine (RE)	RE-CPU	MACsec Line card	MIC-3D-10GE-SFP-E within MPC3E-3D-NG
MX240 MX480 MX960	RE-S-X6-128G RE-S-X6-64G	HASWELL-EP, Intel Xeon E5-2608L V3	MPC10E-10C and MPC10E-15C, with JNPR Penta Silicon MACsec ASIC	BCM82756 MACsec ASIC with CAVP num AES4550
EX9204 EX9208 EX9214	EX9200-RE2	HASWELL-EP, Intel Xeon E5-2608L V3	EX9200-15C with JNPR Penta Silicon MACsec ASIC	Not supported

The following environmental components are required to operate the TOE in the evaluated configuration:

Components	Description
Local Management Console	Any management workstation (computer) that is directly (serially) connected to the TOE's console port may be used by the TOE administrator for local administration of the TOE.
Remote Management Workstation	Any management workstation (computer) with a SSHv2 client installed that may be used by the TOE administrator for remote administration of the TOE through SSH protected channel.
Syslog Server	A syslog server, used for remote storage of audit records that have been generated by and transmitted from the TOE securely using SSH tunnel (SSHv2).
NTP Server	A NTPv4 server, used to provide reliable timestamps to the TOE.
MACsec Peer	A MACsec Peer, used for establishing MACsec communication for securing Layer 2 data using MACsec functionality.

8.2 Excluded Functionality

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

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

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 TOE 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, PP-module, and Functional Package.

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 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches** 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 claimed PP/PP-Modules/Package.

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 the claimed PP/PP-Modules/Package 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 the claimed PP/PP-Modules/Package 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 the claimed PP/PP-Modules/Package 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 the claimed PP/PP-Modules/Package, 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 were no publicly known and exploitable vulnerabilities in the TOE:

- https://nvd.nist.gov/vuln/search#/nvd/home?resultType=records
- https://www.cve.org/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://supportportal.juniper.net/s/global-search/%40uri#f-sf_primarysourcename=Knowledge&f-sf_articletype=Security%20Advisories&f-sflevel3=MX-Series,EX-Series&f-sflevel4=MX960,MX240,MX480,EX9204,EX9208,EX9214

The vulnerability searches were performed on Sep 26, 2025, Nov 24, 2025, April 30, 2026 and June 18, 2026. The search was conducted with the following terms:

- Juniper MX240 (cpe:2.3:h:juniper:mx240:-:*:*:*:*:*:*:*)
- Juniper MX480 (cpe:2.3:h:juniper:mx480:-:*:*:*:*:*:*:*)
- Juniper MX960 (cpe:2.3:h:juniper:mx960:-:*:*:*:*:*:*:*)
- Juniper EX9204 (cpe:2.3:h:juniper:ex9204-:*:*:*:*:*:*:*)
- Juniper EX9208 (cpe:2.3:h:juniper:ex9208:-:*:*:*:*:*:*:*)
- Juniper EX9214 (cpe:2.3:h:juniper:ex9214:-:*:*:*:*:*:*:*)
- JUNOS OS 24.4R2
- Intel Xeon E5-2608L V3 (cpe:2.3:h:intel:xeon_e5-2608l_v3:-:*:*:*:*:*:*:*)
- Juniper Penta Silicon
- Broadcom BCM82756
- OpenSSL 1.1.1zb
- OpenSSH 9.7p1 (cpe:2.3:a:openbsd:openssh:9.7:p1:*:*:*:*:*:*)
- Junos libMD
- Junos libquicksec 7.0

No open vulnerabilities applicable to the TOE were 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 addressed the vulnerability analysis Assurance Activities in the claimed PP/PP-Modules/Package, 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 claimed PP/PP-Modules/Package, 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 *Junos® OS Common Criteria Evaluated Configuration Guide for MX240, MX480, MX960, EX9204, EX9208 and EX9214 Devices*, Release 24.4R2. 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 in the claimed PP/PP-Module/Package listed in Section 2 and their 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

Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches Security Target, Version 0.6, June 18, 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. *Evaluation Technical Report for MX240/480/960 AND EX9204/9208/9214 Switches on JUNOS 24.4R2*, Version 0.4, 03 June 2026.
6. *Junos® OS Common Criteria Evaluated Configuration Guide for MX240, MX480, MX960, EX9204, EX9208 and EX9214 Devices* Release 24.4R2, June 18, 2026.
7. *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 [CPP_ND_V3.0E].
8. *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 [MOD_MACSEC_V1.0].
9. *Functional Package for SSH Version 1.0*, 13 May 2021, [PKG_SSH_V1.0]
10. *Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches Security Target*, Version 0.6, June 18, 2026.
11. *Assurance Activity Report for JUNOS 24.4R2 for MX240/480/960 and EX9204/9208/9214 Switches*, Version 0.5.
12. *Vulnerability Assessment for Junos 24.4R2 for MX240/480/960 Routers and EX9204/9208/9214 Switches*, Version 0.5, June 18, 2026.
13. *HPE Juniper Networking Flaw Remediation Procedures*, Version 0.1, 10 March 2026.