

**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**



**Validation Report
for the
Junos OS 24.2R2 for EX4400**

Report Number: CCEVS-VR-VID11622-2026
Dated: 6/1/2026
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 Meade, MD 20755-6982**

ACKNOWLEDGEMENTS

Validation Team

Swapna Katikaneni

Meredith Martinez

Deron Graves

The Aerospace Corporation

Common Criteria Testing Laboratory

Sean Bennett

Lightship Security USA, Inc.

Table of Contents

1.	Executive Summary	1
2.	Identification	2
3.	Architectural Information	4
3.1.	TOE Evaluated Configuration	4
3.2.	Physical Boundary	4
3.3.	Required Non-TOE Hardware, Software, and Firmware	5
4.	Security Policy	7
4.1.	Security Audit	7
4.2.	Cryptographic Support.....	7
4.3.	Identification and Authentication	7
4.4.	Security Management	7
4.5.	Protection of the TSF	7
4.6.	TOE Access	7
4.7.	Trusted Path/Channels	7
5.	Assumptions.....	8
6.	Clarification of Scope	10
7.	Documentation	11
8.	IT Product Testing	12
8.1.	Developer Testing.....	12
8.2.	Evaluation Team Independent Testing	12
8.3.	Test Bed Configuration.....	12
9.	Results of the Evaluation	14
9.1.	Evaluation of Security Target (ASE).....	14
9.2.	Evaluation of Development Documentation (ADV)	14
9.3.	Evaluation of Guidance Documents (AGD).....	14
9.4.	Evaluation of Life Cycle Support Activities (ALC).....	15
9.5.	Evaluation of Test Documentation and the Test Activity (ATE).....	15
9.6.	Vulnerability Assessment Activity (VAN).....	15
9.7.	Summary of Evaluation Results.....	16
10.	Validator Comments	17
11.	Annexes.....	18

12. Security Target.....	19
13. Glossary	20
14. Acronym List	21
15. Bibliography	22

List of Tables

Table 1: Evaluation Identifiers.....	2
Table 2: TOE Models.....	4
Table 3: Assumptions (CPP_ND_V3.0E).....	8
Table 4: Tools Used for Testing	13

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Junos OS 24.2R2 for EX4400 provided by Juniper Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in June 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). 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.

The TOE is Junos OS 24.2R2 for EX4400. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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). 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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.

The technical information included in this report was obtained from the Security Target and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Validated Products List.

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

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile 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
Evaluated Product	Junos OS 24.2R2 for EX4400
Sponsor and Developer	Juniper Networks, Inc. 1133 Innovation Way Sunnyvale, CA 94089
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 2.0 (CFG_NDcPP-MACsec_V2.0): Base PP: collaborative Protection Profile for Network Devices, Version 3.0e (CPP_ND_V3.0E) PP-Module: PP-Module for MACsec Ethernet Encryption, Version 1.0 (MOD_MACSEC_V1.0) Functional Package for Secure Shell (SSH), Version 1.0 (PKG_SSH_V1.0) conformant
ST	Junos OS 24.2R2 for EX4400 Security Target, v1.1
Evaluation Technical Report	Juniper Networks, Inc. Junos OS 24.2R2 for EX4400 Evaluation Technical Report, v1.1
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Sean Bennett
CCEVS Validators	Swapna Katikaneni, Meredith Martinez, Deron Graves

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Juniper Networks EX4400 series comprises high-performance Ethernet switches that support MACsec encryption and offer Gigabit/10-gigabit Ethernet connectivity.

3.1. TOE Evaluated Configuration

The TOE is the Juniper Networks EX4400-24X, EX4400-24T, EX4400-24P, EX4400-24MP, EX4400-48T, EX4400-48P, EX4400-48F, EX4400-48MP platforms executing the Junos OS 24.2R2 software.

The TOE contains the following logical interfaces:

- Local CLI. Direct serial connection to the local CLI.
- Remote CLI. Remote connection to the CLI via SSHv2.
- Syslog. Logging to syslog via SSHv2.
- MACsec. Point-to-point connections with MACsec peers.
- NTP. The TOE synchronizes time via NTP.

3.2. Physical Boundary

The physical boundary of the TOE includes all software and hardware shown in Table 2. The TOE is delivered via commercial courier.

Table 2: TOE Models

Model	Port Configuration	MACsec FPGA	CPU	Software
EX4400-24X	24-Port 1/10GbE SFP+	PHY1 BCM82756 PHY2 BCM82399 PHY3 BCM82398	Intel Atom C3558R (Denverton)	Junos OS 24.2R2
EX4400-24T	24-port 10/100/1000BASE-T	PHY1 BCM54192 PHY2 BCM82399		
EX4400-24P	24-port 10/100/1000BASE-T (PoE)	PHY1 BCM54192		

Model	Port Configuration	MACsec FPGA	CPU	Software
		PHY2 BCM82399		
EX4400-24MP	24x-port 100M/1/2.5/5/10GbE (PoE)	PHY1 BCM84894M PHY2 BCM82399		
EX4400-48T	48-port 10/100/1000BASE-T	PHY1 BCM54192 PHY2 BCM82399		
EX4400-48P	48-port 10/100/1000BASE-T (PoE)	PHY1 BCM54192 PHY2 BCM82399		
EX4400-48F	12-port 1000/10000BASE-X + 36-port 100/1000BASE-X	PHY1 BCM54195 PHY2 BCM82399 PHY3 BCM82756		
EX4400-48MP	12x100M/1/2.5/5/10GbE + 36x100M/1/2.5GbE (PoE)	PHY1 BCM54998EM PHY2 BCM82399 PHY3 BCM84894M		

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- **Audit Server.** The TOE sends audit events to an external syslog server via SSHv2.
- **NTP Server.** The TOE synchronizes time via NTP.

- **MACsec Peer(s).** TOE MACsec peers supporting 802.1ae.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates audit records of user and administrator actions. The TOE includes the user identity in audit events resulting from actions of identified users. The TOE is capable of sending logs in real-time to an external syslog server via SSHv2

4.2. Cryptographic Support

The TOE implements a cryptographic module. The cryptographic module has the ability to generate and destroy cryptographic keys. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4 in the ST.

4.3. Identification and Authentication

The TOE ensures that all users must be identified and authenticated before accessing its functions and data.

4.4. Security Management

The TOE provides a suite of security management functions that is available to authorized administrators in support of configuring and maintaining the TOE.

4.5. Protection of the TSF

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions including software integrity verification using digital signatures. The TOE also supports the use of NTP or its own manually configurable time source to support the execution of reliable and time sensitive operations.

4.6. TOE Access

The TOE can be accessed physically via direct serial connection or remotely via SSH connection. When a user account has reached the configured number of failed authentication attempts, the account will be locked for a Security Administrator defined time period.

4.7. Trusted Path/Channels

The TOE protects the integrity and confidentiality of communications between itself and local/remote administrators as noted in the Security Target section 2.2.2.

5. Assumptions

Table 3: Assumptions (CPP_ND_V3.0E)

Identifier	Description
A.PHYSICAL_PROTECTION	<p>The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security 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 cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.</p>
A.LIMITED_FUNCTIONALITY	<p>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).</p> <p>If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.</p>
A.NO_THRU_TRAFFIC_PROTECTION	<p>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 ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).</p>

Identifier	Description
A.TRUSTED_ADMINISTRATOR	<p>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 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.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
A.REGULAR_UPDATES	<p>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.</p>
A.ADMIN_CREDENTIALS_SECURE	<p>The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.</p>
A.RESIDUAL_INFORMATION	<p>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.</p>

NOTE: MOD_MACSEC_V1.0 does not define additional assumptions.

6. 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 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the evaluation activities specified in CPP_ND_V3.0E-SD, MOD_MACSEC_V1.0-SD and PKG_SSH_V1.0 and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V3.0E, MOD_MACSEC_V1.0 and PKG_SSH_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.
- **Excluded Functionality:**
 - The following functions are excluded from the evaluation and should not be used in the evaluated configuration:
 - Telnet
 - FTP
 - SNMP
 - TLS/SSL including management via J-Web, JUNOScript and JUNOScope

-

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Juniper Networks Junos OS Common Criteria Evaluated Configuration Guide for EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T Devices, Release 24.2R2, Published 2026-03-27*

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.

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.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Juniper Networks, Inc. Junos OS 24.2R2 for EX4400 Assurance Activity Report, v1.1* provides an overview of testing and the prescribed evaluation activities.

8.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

8.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from June 2025 until March 2026. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.3. Test Bed Configuration

The TOE testing environment components are identified in Figure 1 and Table 4 below.

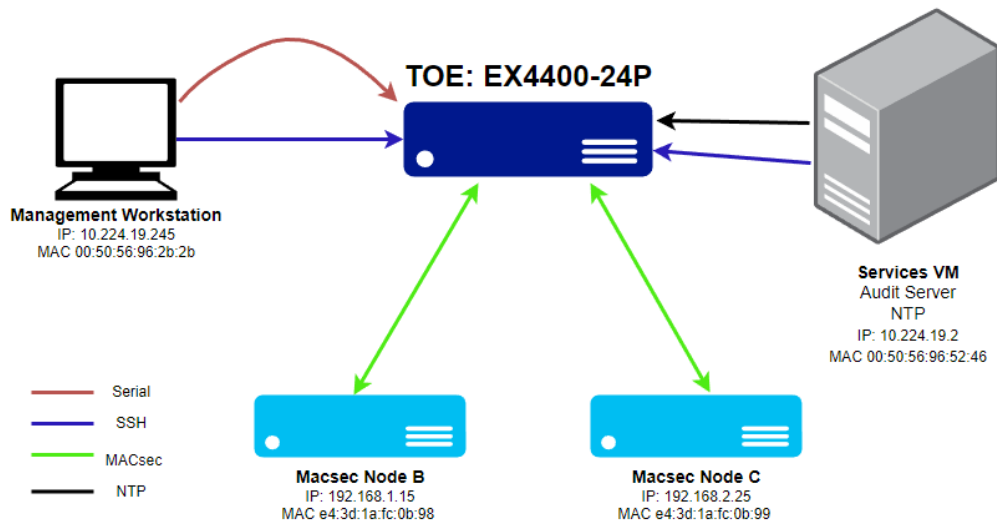


Figure 1: Testing Environment Overview

Table 4: Tools Used for Testing

Tool name	Version	Description
Lightship Greenlight	3.0.59	Tool used for SSH protocol modification testing
OpenSSH	8.8p1-Lightship	Component of Lightship Greenlight
OpenSSL	3.1.2	Component of Lightship Greenlight
Python	3.9	Component of Lightship Greenlight
OpenSSH	8.8p1	Tool for SSH protocol testing
OpenSSH (portable)	10.2p1	FCS_SSH_EXT.1.6 Test 4
OpenSSL	1.1.1m	OpenSSL built into OpenSSH
Wpa_supplicant	v2.10-lightship-1.0	Tool used for MACsec protocol testing
Wireshark	4.22	Used for packet analysis
Tcpdump	4.9.3	Used for packet capture on the Services VM
Tcpdump	4.99.3	Used for packet capture on the GL VM, NodeB and NodeC

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). 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined Junos OS 24.2R2 for EX4400 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_ND_V3.0E-SD, MOD_MACSEC_V1.0-SD and PKG_SSH_V1.0.

9.1. Evaluation of Security Target (ASE)

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 24.2R2 for EX4400 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 (ADV)

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 and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TSS.

The Validation 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.

9.3. Evaluation of Guidance Documents (AGD)

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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 procedures regarding systematic flaw remediation and requirements of the CEM, and that the conclusions reached by the Evaluation team were justified.

9.5. Evaluation of Test Documentation and the Test Activity (ATE)

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

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.

9.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Juniper Networks, Inc. Junos OS 24.2R2 Vulnerability Assessment, v1.1, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on May 27, 2026, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): <https://web.nvd.nist.gov/view/vuln/search>
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- Common Vulnerabilities and Exposures: <https://www.cvedetails.com/vulnerability-search.php>
- CISA - Known Exploited Vulnerabilities Catalog: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Juniper Networks, Inc. Security Advisories (<https://supportportal.juniper.net/s/global-search/>)

The Evaluation team performed a search using the following keywords:

- Junos 24.2R2;
- TOE Models;
- EX4400-24X
- EX4400-24T
- EX4400-24P
- EX4400-24MP
- EX4400-48T
- EX4400-48P
- EX4400-48F
- EX4400-48MP
- Processors and PHYs used by the TOE:
- Intel Atom C3558R
- BCM54192
- BCM54195
- BCM82398
- BCM82399
- BCM82756
- BCM84894M
- BCM54998EM
- OpenSSH;
- OpenSSL;
- FreeBSD
- Note: Additional proprietary search terms were also included.

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.

9.7. 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 followed the procedures defined in the CEM and performed the Evaluation Activities in CPP_ND_V3.0E-SD, MOD_MACSEC_V1.0-SD and PKG_SSH_V1.0, and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. 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.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11. Annexes

Not applicable.

12. Security Target

Junos OS 24.2R2 for EX4400 Security Target, v1.1

13. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model*, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements*, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements*, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
5. *PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 2.0*
6. *collaborative Protection Profile for Network Devices, Version 3.0e*
7. *Evaluation Activities for Network Device cPP, 06-December-2023, Version 3.0e*
8. *Functional Package for secure Shell (SSH), Version 1.0*
9. *PP-Module: PP-Module for MACsec Ethernet Encryption, Version 1.0*
10. *Supporting Document Mandatory Technical Document PP-Module for MACsec Ethernet Encryption, Version: 1.0*
11. *Junos OS 24.2R2 for EX4400 Security Target, v1.1*
12. *Juniper Networks Junos OS Common Criteria Evaluated Configuration Guide for EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T Devices, Release 24.2R2, Published 2026-03-27*
13. *Juniper Networks, Inc. Junos OS 24.2R2 for EX4400 Assurance Activity Report, v1.1*
14. *Juniper Networks, Inc. Junos OS 24.2R2 Vulnerability Assessment, v1.1*
15. *Juniper Networks, Inc. Junos OS 24.2R2 for EX4400 Evaluation Technical Report, v1.1*
16. *Juniper Networks, Inc. Junos OS 24.2R2 for EX4400 NDcPPv3.0e + PKG_SSH_V1.0 + MOD_MACSEC_V1.0 Test Plan, v1.1*
17. *Juniper Networks, Inc. Junos OS 24.2R2 for EX4400 EX4400-24P Test Evidence, v1.1*