National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report for

Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2

Report Number:	CCEVS-VR-VID11626-2026
Dated:	January 21, 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

Jenn Dotson

Lisa Mitchell

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Joachim Vandersmissen

Parker Collier

Alex Gong

atsec information security corporation

Austin, TX

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2 (the Target of Evaluation, or 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.

The evaluation was performed by atsec Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed in January 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by atsec. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant and meets the assurance requirements of the:

- *Collaborative Protection Profile for Network Devices*, Version 3.0E, 6 December 2023 [NDcPP] with
    - Optional Security Assurance Requirements ALC_FLR.3
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG].

The TOE is the Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2. 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 the functional requirements and assurance requirements stated in the Security Target (ST). 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 *Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2 Security Target*, Version 1.4, 2025-11-05, 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 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 (PCL).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PPs/PP-Modules/Packages to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Validation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2
Security Target	*Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2 Security Target*, Version 1.4, 2025-11-05
Sponsor & Developer	Juniper Networks, Inc.
Completion Date	January 2026
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Release 5, April 2017
CEM Version	*Common Methodology for Information Technology Security Evaluation*, Version 3.1, Release 5, April 2017
PP	*Collaborative Protection Profile for Network Devices*, Version 3.0E, 6 December 2023 [NDcPP] *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG].
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant
CCTL	atsec information security corporation 4516 Seton Center Parkway Suite 250 Austin, TX 78759

Validation Personnel	Jenn Dotson, Lisa Mitchell, Lori Sarem
Evaluation Personnel	Joachim Vandersmissen, Parker Collier, Alex Gong

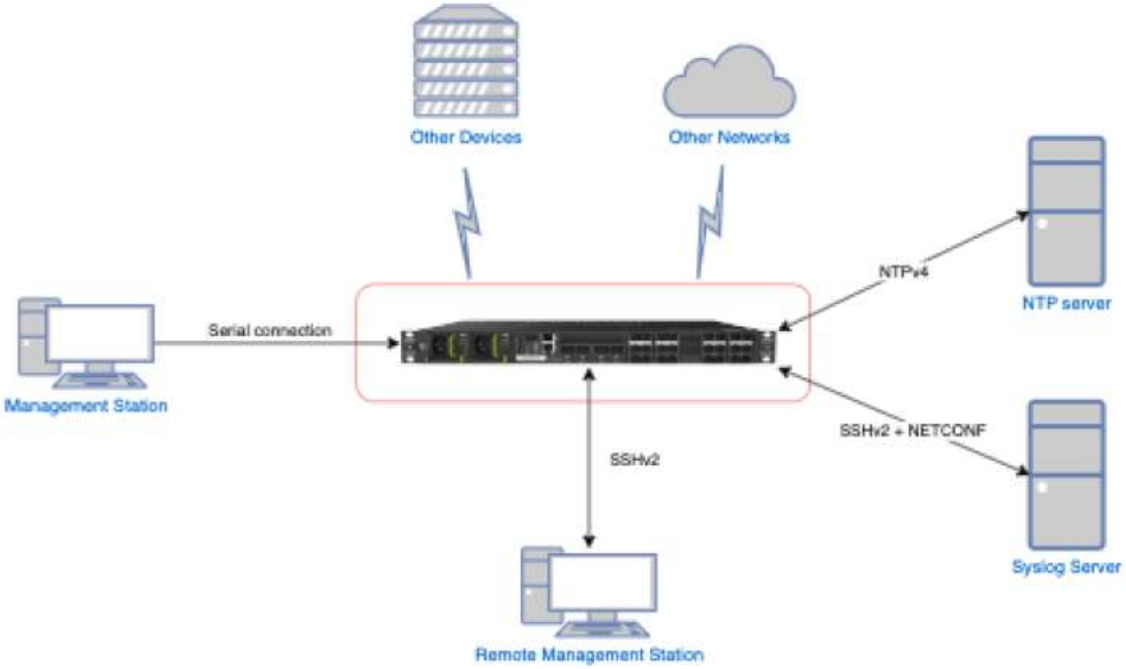
3 TOE Architecture

The TOE is comprised of the Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved version 24.4R2. The TOE is a network router composed of hardware and software. The software is named Junos® OS Evolved which is the single purpose operating system that operates the management functions of all the Juniper Networks® routers. The evaluation covers Junos® OS Evolved 24.4R2.

The TOE is the entire network appliance. The TOE is connected to management workstations, to one or more NTP servers, and to a syslog server. The management workstations can be local or remote. The TOE is also connected to the networks which it interconnects. Neither the management console, the NTP servers, the syslog server, nor the interconnected networks are part of the TOE.

The TOE software is Junos® OS Evolved, which is the Juniper Linux-based operating system for network devices. It implements a flexible Software Defined Networking (SDN) allowing the tailoring of the software to several applications. Junos® OS Evolved is a horizontal software layer that decouples the application processes from the hardware on which the processes run. Effectively, this decoupling creates a general-purpose software infrastructure spanning all different computing resources on the system. Application processes (protocols, services, and so on) run on top of this infrastructure and communicate with each other by publishing and consuming (that is, subscribing to) the state. Junos® OS Evolved implements the routing, filtering, management, and platform functions.

The figure below shows the TOE in a sample deployment in its operational environment.



4 Security Policy

The TOE enforces the following security functions as described in the ST.

4.1 Security Audit

The TOE implements an audit function. A rich set of audit data is collected and stored as audit records. Each audit record includes a time stamp stating the exact time at which the audit record was generated. Each audit record also includes sufficient information to allow administrators of the TOE to examine the events and investigate possible security violations and attempts thereof.

Audit records are stored in log files within the TOE. The administrator also configures the TOE to forward the audit records to an external syslog server. The syslog server is not part of the TOE. Forwarding the audit records to a syslog server takes place over a trusted channel protected with the SSHv2 protocol.

4.2 Cryptographic Support

The TOE implements cryptographic functionality for the following purposes:

- protection of user passwords;
- establishment of trusted channels and trusted paths using the SSHv2 protocol;
- symmetric key authentication for the NTP protocol; and
- digital signature verification for TOE trusted updates.

The TOE includes several cryptographic libraries for providing this functionality:

- The Junos® OS Evolved Kernel Cryptographic Module provides a Deterministic Random Bit Generation (DRBG), compliant with SP800-90A, for the creation of random data and cryptographic keys; and hashing algorithms for the protection of user's passwords.
- The Junos® OS Evolved OpenSSL Cryptographic Module, based on the open source OpenSSL library version 3.0.16, provides the rest of the cryptographic algorithms.

The TOE also includes a physical, SP800-90B compliant Entropy Source implemented in the TOE hardware for seeding the DRBG with full entropy. In the evaluated configuration, the DRBG is only seeded by the entropy source claimed in FCS_RBG_EXT.1.

All cryptographic algorithms implemented in the Junos® OS Evolved OpenSSL Cryptographic Module and the Junos® OS Evolved Kernel Cryptographic Module are validated by the Cryptographic Algorithm Validation Program (CAVP). This fulfills the requirements of NIAP Policy Letter #5. In addition, the SP800-90B compliant Entropy Source is validated by the Entropy Source Validation (ESV).

4.3 Identification and Authentication

The TOE ensures that access to administrative functions is only granted to successfully identified and authenticated users. Illegitimate users are deterred and prevented from gaining access.

The TOE implements password-based authentication to local and remote users. Remote authentication, which is implemented over a trusted path using SSHv2, can be also performed using public-key authentication.

The external syslog server establishes an SSHv2 session under NETCONF with the TOE so the TOE can send audit records. The TOE identifies and authenticates the external server using SSHv2 public-key authentication.

4.4 Security Management

Authorized administrators may use a Command Line Interface (CLI) for performing a wide range of security management tasks on the TOE. The CLI may be accessed locally from the console or remotely over a SSH connection. There are no alternative methods of administering the TOE.

4.5 Protection of the TSF

The TOE implements a set of security measures for protecting its TSF and the corresponding configuration parameters. The TOE implements integrity tests of the TOE and cryptographic algorithm self-tests at start-up and takes protective measures if the tests indicate that the TOE software has been tampered or there is a failure in the self-tests.

The TOE protects passwords by hashing their values and not allowing direct access to where they are stored. The TOE also protects cryptographic keys by enforcing access control to the key containers.

TOE access is restricted to authorized administrators and all administrator access goes through a CLI. Administrators have no root access to the underlying Linux operating system.

The TOE also allows upgrading the software in case of vulnerabilities being discovered in the implementation. The integrity of the TOE software is ensured by using a digital signature that is verified before the TOE update.

The TOE maintains a system clock that is used for generating time stamps used in the enforcement of security functions.

4.6 TOE Access

The TOE allows the display of a banner before and after a user logs in. The TOE also controls idle remote sessions and terminates the session after a period of time.

4.7 Trusted Path/Channel

The TOE implements a secure channel for administrators to manage the TOE remotely. Administrators can connect to the TOE from a remote management station using the SSHv2 protocol. Once successfully identified and authenticated, the administrator has access to the Command Line Interface (CLI).

The TOE also establishes a secure channel using SSHv2 for sending audit records to an external syslog server.

The TOE includes the OpenSSH library version 9.8p1 to implement the SSHv2 protocol. The TOE allows both password-based and public-key-based authentication. The underlying cryptographic algorithms needed for the protocol are provided by the Junos® OS Evolved OpenSSL Cryptographic Module.

5 Assumptions and 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 [NDcPP]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG].

That information has not been reproduced here and the NDcPP/SSHPKG 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 NDcPP/SSHPKG 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 clarification. 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 assurance activities specified in the NDcPP with the SSHPKG and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, 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 as evaluated.
- 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 NDcPP/SSHPKG and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The vendor provides guidance documents describing the installation process for Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2, as well as guidance for subsequent administration and use of the applicable security features.

The following guidance documentation was examined during the evaluation:

- *Common Criteria Evaluated Configuration Guide for ACX7024 and ACX7024X Devices*, Release 24.4R2, dated 2026-01-14

To use the TOE in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above. Consumers are encouraged to download this documentation from the NIAP website.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated.

7 IT Product Testing

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

Detailed Test Report Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2, Version 1.1, 2025-11-07 [DTR]

A non-proprietary description of the tests performed, and their results are provided in the following document:

Assurance Activities Report Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2, Version 1.2, 2026-01-14 [AAR]

7.1 Developer Testing

No evidence of developer testing is required by the assurance activities for this TOE.

7.2 Evaluation Team Testing

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to NDcPP and SSHPKG.

The Evaluation team established a test configuration comprising Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2. Section 2.3.5 of the AAR provides a description of the test configuration the CCTL used to test the TOE, including a description of the test environment and a list of tools used.

The Evaluation team devised a Test Plan based on the Test Activities specified in NDcPP and SSHPKG. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The Evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the atsec CCTL facility in Austin, TX between September 2025 and November 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the following hardware and software when configured in accordance with the documentation specified in Section 6.

The TOE software is provided as an ISO image, as well as necessary TOE updates, running on the following hardware platforms:

- ACX7024: industrial-rated (I-Temp) multiservice router
- ACX7024X: commercial-rated (C-Temp), highscale multiservice router

8.2 Excluded Functionality

The following protocols and services must not be used in association with the TOE.

- Telnet, FTP, SNMP for trusted path and channels
- TLS and protocols not covered by the evaluation
- Other methods of TOE management including and JUNOScript
- Linux root account is only used for initial TOE configuration
- Third-party applications and tools allowed by Junos® OS Evolved architecture
- The TOE as an SSHv2 client

Section 1.5.5 of the ST should be consulted for additional information on the excluded functionality provided above.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary *Evaluation Technical Report for Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2*, Version 1.2, dated 2026-01-14 ([ETR]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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 ([CCPART1], [CCPART2], [CCPART3]) and CEM version 3.1, revision 5 ([CEM]), and the specific evaluation activities specified in the NDcPP and SSHPKG. The Evaluation team determined the Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2 to be Part 2 extended and Part 3 conformant and to meet the SARs contained in the NDcPP and SSHPKG.

9.1 Evaluation of the Security Target (ST) (ASE)

The Evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description (also referred as the TOE Architecture), security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved Version 24.4R2 that are consistent with the claimed Protection Profile, and security function descriptions that satisfy 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 the Development Activities (ADV)

The Evaluation team performed each assurance activity and 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 Evaluation team performed the assurance activities specified in the NDcPP/SSHPKG related to the examination of the information contained in the TSS.

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.

9.3 Evaluation of the Guidance Activities (AGD)

The Evaluation team performed each guidance assurance activity and applied each AGD CEM work unit. The Evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The Evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was 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 the Life Cycle Support Activities (ALC)

The Evaluation team performed each ALC assurance activity and applied each ALC CEM work unit. The Evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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 the Test Documentation and the Test Activities (ATE)

The Evaluation team performed each test activity and applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the claimed PP and recorded the results in the 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 Evaluation of the Vulnerability Assessment Activity (AVA)

The evaluation team performed a search of the following online sources:

- MITRE Common Vulnerabilities and Exposures (CVE) List (https://cve.mitre.org/cve/)
- National Vulnerability Database (https://nvd.nist.gov/)
- CISA Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- US-CERT (https://www.kb.cert.org/vuls/html/search)
- Tenable Network Security (https://www.tenable.com/plugins)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/?type=nexpose)
- OpenSSL Vulnerabilities (https://openssl-library.org/news/vulnerabilities-3.0/)

The searches were performed several times, most recently January 12, 2026, using the following search terms:

- OpenSSL
- OpenSSH
- Junos OS
- ACX7024
- ACX7024X
- C3508
- C3758R
- ntpd
- Linux
- Intel Atom
- Broadcom

The results of these searches identified one vulnerability that is applicable to the TOE. The vulnerability is mitigated by TOE configuration, which is documented in the AGD. The Evaluation team conclusion drawn from the vulnerability analysis was that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

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 testing 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 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 instructions in the Guidance documents defined in Section 6. No versions of the TOE and software, either earlier or later, were evaluated.

Please note that 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. All other functionality provided by devices in the operational environment should be assessed separately and no further conclusions can be drawn about their effectiveness.

Per NIAP/CCEVS Scheme Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Security Target

The ST for this product's evaluation *is Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved version 24.4R2 Security Target*, Version 1.4, 2025-11-05 [ST].

A Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

B Bibliography

The validation team used the following documents to produce this VR:

[CCPART1] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model*, Version 3.1, Revision 5, April 2017.

[CCPART2] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[CCPART3] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements*, Version 3.1, Revision 5, April 2017.

[CEM] *Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, April 2017.

[NDcPP] *collaborative Protection Profile for Network Devices*, Version 3.0e, 2023-12-06.

[SSHPKG] *Functional Package for SSH*, Version 1.0, 2021-05-13.

[ST] *Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved version 24.4R2 Security Target*, Version 1.4, 2025-11-05.

[AGD] *Common Criteria Evaluated Configuration Guide for ACX7024 and ACX7024X Devices,* Release 24.4R2, 2026-01-14.

[ETR] *Evaluation Technical Report Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved version 24.4R2*, Version 1.2, 2026-01-14.

[AAR] *Assurance Activity Report Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved version 24.4R2*, Version 1.2, 2026-01-14.

[DTR] *Detailed Test Report Juniper Networks® ACX7024 and ACX7024X routers with Junos® OS Evolved version 24.4R2,* Version 1.1, 2025-11-07.