National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214, Version 1.0

Report Number:	**CCEVS-VR-VID10939-2018**
Dated:	**February 21, 2019**
Version:	**1.0**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Meredith Hennan

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user 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 OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 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 February 2019. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test report, as summarized in the publicly Assurance Activities Report (AAR) for this evaluation; all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314 (NDcPPv2.0e).

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

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

2 Identification

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

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214
Protection Profile	Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018 (NDcPPv2.0e)
Security Target	Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Security Target
Evaluation Technical Report	Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 ETR
CC Version	Version 3.1 Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Juniper Networks, Inc.
Developer	Juniper Networks, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Rockville, MD 20850
CCEVS Validators	Meredith Hennan, Kenneth Stutterheim

3 Architectural Information

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 18.1R3 executing on MX-Series 3D Universal Edge Routers and EX9200 Ethernet Switch. The supported chassis are:

- MX240
- MX480
- MX960
- MX2008
- MX2010
- MX2020
- EX9204
- EX9208
- EX9214

The supported Routing Engines employed by the MX-Series Router and EX9200-Series switches are:

- MX-Series Routers
  - RE1800 generation Routing Engines:
    - RE-S-1800x4-YYG[1] for MX240, MX480 and MX960
    - RE-MX2000-1800X4 and REMX2K-1800-32G-S for MX2010 and MX2020
  - Next Generation Routing Engines (RE-NG):
    - RE-S-X6-64G for MX240, MX480 and MX960
    - REMX2K-X8-64G for MX2008, MX2010 and MX2020
- EX9200-Series Ethernet Switches
  - EX9200-RE (RE1800)
  - EX9200-RE2 (RE-NG)

Each of the MX-Series/EX9200 appliances is a secure network device that protects itself by offering only a minimal logical interface to the network and attached nodes. All MX-Series/EX9200-Series appliances are powered by the Junos OS software, Junos OS 18.1R3, which is a special purpose OS that provides no general-purpose computing capability. Junos OS provides both management and control functions as well as all IP routing.

[1] YY = 8, 16or 32 GB memory)

The MX-Series/EX9200-Series appliances primarily support the definition and enforcement of information flow policies among network nodes. All information flow from one network node to another passes through an instance of the TOE. Information flow is controlled based on network node addresses and protocol. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited and provides the security tools to manage the security functions.

4 Security Policy

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

Protected Communications
The TOE provides an SSH server to support protected communications which allow administrators and external syslog servers to establish secure sessions to the TOE. The TOE requires that applications exchanging information with it are successfully authenticated prior to any exchange (i.e. applications connecting over SSH). The TOE includes cryptographic modules that provide the underlying cryptographic services, including key management, 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.

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

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

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

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

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

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

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

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

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

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

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

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

5.2 Threats

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

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

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

	Failures could result in a compromise to the security functionality of the device. A network device self-testing its security critical components at both start-up and during run-time ensures the reliability of the device's security functionality.

5.3 Clarification of Scope

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

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

6 Documentation

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

- Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Security Target
- Junos OS Common Criteria and FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Series Devices

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

To use the product in the evaluated configuration, the product must be configured as specified in the Junos OS Common Criteria and FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Series Devices.

Consumers are encouraged to download that guidance document from the NIAP website to ensure the device is configured using the same instructions used by the evaluation team.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE consists of one or more of the physical devices listed in section 3, running Junos OS 18.1 R3 firmware, in an environment consisting of an administrative workstation with an SSH client and a syslog server with a SSH client with NETCONF support configured to receive streamed syslog messages from the TOE. Also part of the TOE is the Junos OS Common Criteria and FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Series Devices.

Physical Boundary:

The TOE is the Junos OS 18.1R3 firmware running on the appliance chassis listed in Table 1. Hence the TOE is contained within the physical boundary of the specified appliance chassis**,** as shown in Figures 1 and 2.

The physical boundary of the TOE is the entire chassis of the appliance (defined in Table 1.)

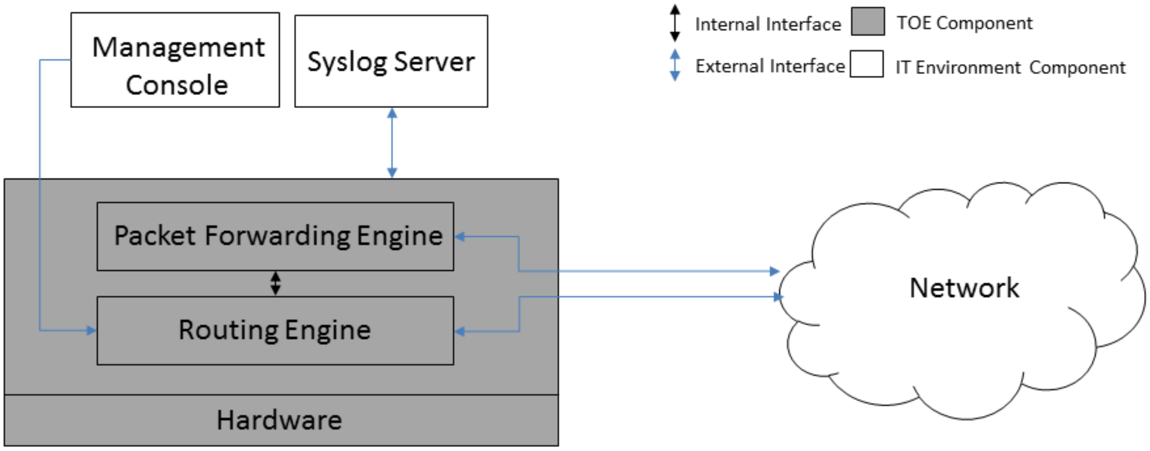

Figure 1 TOE Boundary with RE1800

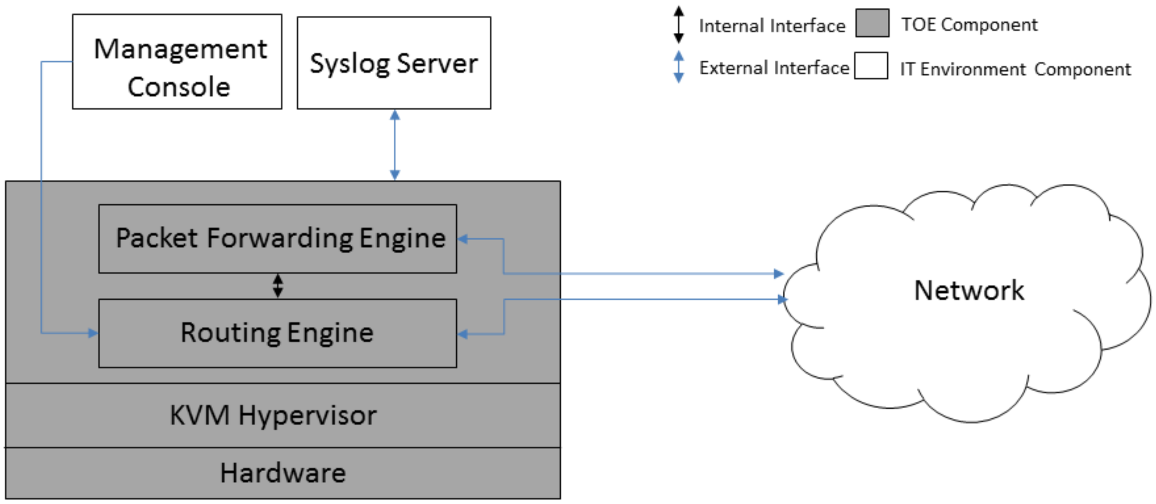

Figure 2 TOE Boundary with Next Generation RE (RE-NG)

The TOE interfaces are comprised of the following:

i. Network interfaces which pass traffic
ii. Management interface through which handle administrative actions.

Chassis Model	Routing Engine	Network Ports	Firmware
MX240	RE-S-1800X4-YYG (YY = 8, 16 or 32 GB memory) **or** RE-S-X6-64G	3 x (MPCs and DPCs)	Junos OS 18.1R3
MX480		6 x (MPCs and DPCs)	
MX960		12 x (MPCs and DPCs)	
MX2010	RE-MX2000-1800X4 **or** REMX2K-1800-32G-S **or** REMX2K-X8-64G	10 x MPCs	
MX2020		20 x MPCs	
MX2008	REMX2K-X8-64G	8 X MPCs	
EX9204 EX9208 EX9214	EX9200-RE **or** EX9200-RE2	EX9200-2C-8XS EX9200-4QS EX9200-6QS EX9200-MPC EX9200-12QS EX9200-32XS EX9200—40T EX9200-40F EX9200-40F-M EX9200-40XS	

Table 1 TOE Chassis Details

Separate jinstall images are provided for MX-Series and EX9200-Series chassis, for each RE1800 and RE-NG Routing Engine, namely:

- MX with RE1800 (RE-S-1800X4-YYG, RE-MX2000-1800X4 and REMX2K-1800-32G-S):
    - junos-install-mx-x86-64-18.1R3.3.tgz
- MX with RE-NG (RE-S-X6-64G and REMX2K-x8-64G):
    - junos-vmhost-install-mx-x86-64-18.1R3.3.tgz
- EX9200 with RE 1800 (EX9200-RE):
    - junos-install-ex92xx-x86-64-18.1R3-S3.4.tgz
- EX9200 with RE-NG (EX9200-RE2):
    - junos-vmhost-install-ex92xx-x86-64-18.1R3-S3.4.tgz

7.2 Excluded Functionality

- Use of telnet
- Use of FTP
- Use of SNMP
- Use of SSL, including management via J-Web, JUNOScript and JUNOScope
- Use of CLI account super-user and shell root account.
- Multi-Service MPCs (which provide IPsec and VPN functionality for these platforms)
- Routing, switching, inline services, subscriber management and advanced hierarchical quality of service (HQoS) functionality of the PFE/MPCs is not evaluated
- Network and Security Manager (NSM) and Junos Space; CLI is included
- Network Time Protocol (NTP)

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary Evaluation Test Report for Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

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

9 Results of the Evaluation

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

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP and SD.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP and SD.

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

9.2 Evaluation of Development Documentation

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

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

9.3 Evaluation of Guidance Documents

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

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

9.4 Evaluation of Life Cycle Support Activities

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

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

9.5 Evaluation of Test Documentation and the Test Activity

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

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP, and 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 evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

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

- http://www.securityfocus.com/

The evaluator performed the public domain vulnerability searches using the following key words. The search was originally performed on January 4, 2019 and was updated on January 30, 2019.

- JunOS 18.1R3
- MX240
- MX480
- MX960
- MX2008
- MX2010
- MX2020
- EX9204
- EX9208
- EX9214
- RE-S-1800x4-YYG
- RE-MX2000-1800X4
- REMX2K-1800-32G-S
- RE-S-X6-64G
- REMX2K-X8-64G
- EX9200-RE
- EX9200-RE2
- SSH
- RE1800 – OpenSSL
- OpenSSL

The evaluator selected the search key words based upon the following criteria.

- The vendor name was searched,
- The software running on the TOE devices were searched. Further, the version the TOE software in evaluation was searched,
- The name of the hardware devices within the TOE,
- The secure protocols supported by the TOE,
- The type of TOE device.

In accordance with NIAP policy Letter #17, the vulnerability analysis conducted on January 30, 2019 revealed a security vulnerability that was addressed by the vendor resulting in a firmware revision change. The security related change was regression tested by the CCTL. The security related change and non-security related bug fixes were acceptability tested by the vendor.

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

9.7 Summary of Evaluation Results

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

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

10 Validator Comments & Recommendations

Administrators of the devices are cautioned to pay careful attention to the instructions provided in the Common Criteria and FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Series Devices Release 18.1 R2, 2018-12-14; especially to note that the FIPS mode configuration is NOT equivalent to Common Criteria evaluated configuration. FIPS mode compliance was not evaluated as part of this evaluation. In particular; although approved for FIPS mode, 3DES-CBC, AES192-CBC and AES192-CTR are not to be used in the evaluated configuration.

SSHV2 is the only permitted remote management protocol that can be used in the evaluated configuration.

Administrators should note that the TOE does not automatically reestablish broken netconf sessions with an audit server; to reestablish a session the administrator must establish a new session from the audit server to the TOE.

11 Annexes

Not applicable.

12 Security Target

Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Security Target

13 Glossary

The following definitions are used throughout this document:

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

14 Bibliography

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

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. collaborative Protection Profile for Network Devices, Version 2.0 + Errata, 14 March 2018
6. Supporting Document, Mandatory Technical Document, Evaluation Activities for Network Device cPP, March 2018, Version 2.0 + Errata 20180314 [SD]
7. Security Target Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214, Version 1.4, February 7, 2019. [ST]
8. Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Common Criteria NDcPP Assurance Activity Report, Version 3.2, February 2019. [AAR]
9. Common Criteria and FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Series Devices Release 18.1 R3, 2019-02-12. [AGD]
10. Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Security Target Evaluation Technical Report, Version 2.0 February 2019. <Evaluation Sensitive> [ASE-ETR]
11. Vulnerability Assessment for Junos OS 18.1R2 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214, Version 1.1, January 2019. <Evaluation Sensitive> [AVA]
12. Junos OS 18.1R2 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Equivalency Analysis, Version 1.0 September 2018, <Evaluation Sensitive>
13. Junos OS 18.1R3 for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208 and EX9214 Evaluation Technical Report, Version 1.2, February 2019. <Evaluation Sensitive> [TOE-ETR]
14. Test Plan for a Target of Evaluation, (Appliance EX9208, Routing Engine EX9200-RE), Version 1.2, February 2019. <Evaluation Sensitive>
15. Test Plan for a Target of Evaluation, (Appliance EX9208, Routing Engine EX9200-RE2), Version 1.2, February 2019. <Evaluation Sensitive>
16. Test Plan for a Target of Evaluation, (Appliance MX240/Routing Engine: RE-S-1800x4-YYG), Version 1.2, February 2019. <Evaluation Sensitive>

17. Test Plan for a Target of Evaluation, (Appliance MX240/Routing Engine: RE-S-X6-64G), Version 1.2, February 2019. <Evaluation Sensitive>
18. National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme, NIAP Policy Letter #17, Effects of Vulnerabilities in Evaluated Products, 29 August, 2014.