**National Information Assurance Partnership**

**Common Criteria Evaluation and Validation Scheme**


TM

# Validation Report

**for the**

**Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS**

| | |
|---|---|
| **Report Number:** | **CCEVS-VR-VID10988-2019** |
| **Dated:** | **October 1, 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 6940**
**Fort Meade, MD 20755-6940**

**ACKNOWLEDGEMENTS**

**Validation Team**

Kenneth Stutterheim
Meredith M Hennan
*The Aerospace Corporation*

**Common Criteria Testing Laboratory**

Danielle Canoles
Heather Hazelhoff
Dayanandini Pathmanathan

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 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS 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 September 2019. The information in this report was largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the Collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and the Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACSECEP), Version 1.2.

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. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the NDcPP and MACsec EP. 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, evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the 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), which describes 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 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS |
| **Protection Profile** | Collaborative Protection Profile for Network Devices (NDcPP), Version 2.1<br>Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACSECEP), Version 1.2 |
| **Security Target** | Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS Security Target v1.6 |
| **Evaluation Technical Report** | Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS ETR Version 1.5 |
| **CC Version** | Version 3.1 Revision 5 |
| **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<br>2400 Research Blvd Suite 395<br>Rockville, MD 20850 |
| **CCEVS Validators** | Meredith M Hennan, Kenneth Stutterheim |

## 3 Architectural Information

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 18.3R1-S1 executing on MX-Series 3D Universal Edge Routers and EX9200-Series Ethernet Switches when equipped with MACsec Line Cards. The supported chassis are:

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

The supported next generation Routing Engines employed by the MX-Series Router and EX9200-Series Ethernet Switch are:

- **RE-S-X6-64G and RE-S-X6-128G** for MX240, MX480 andMX960
- **EX9200-RE2** for EX9204, EX9208 and EX9214
- **REMX2K-X8-64G and REMX2K-X8-128G** for MX2010 and MX2020

The line cards containing the MACsec module, which are required for deployment in the TOE, are

- MPC7E-10G in the MX-Series Router
- EX9200-40XS in the EX-Series Router

Each of the MX-Series/EX9200-Series appliances is a secure network device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. All MX-Series/EX9200-Series platforms are powered by the Junos OS firmware: Junos OS 18.3R1-S1, 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.

The MX-Series/EX9200-Series appliances primarily support the definition of, and enforce, 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 on the basis of 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 all of the security functions.

## 4 Security Policy

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

| Security Functionality | Description |
|---|---|
| Security Audit | Junos auditable events are stored in the syslog files on the appliance, and can be sent to an external log server (via Netconf over SSH). Auditable events include start-up and shutdown of the audit functions, authentication events, as well as the events listed in 10. 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 storage limits being reached the oldest logs will be overwritten. |
| Cryptographic Support | The TOE provides an SSH server to support protected communications for administrators to establish secure sessions and to connect to external syslog servers.<br><br>The TOE requires that applications exchanging information with it are successfully authenticated prior to any exchange (i.e. applications connecting over SSH).<br><br>Communication over point-to-point links between Juniper appliances can be secured using MACsec.<br><br>The TOE includes cryptographic modules that provide the underlying cryptographic services, including key management and protection of stored keys, algorithms, random bit generation and crypto-administration. The cryptographic modules provide confidentiality and integrity services for authentication and for protecting communications with connecting applications. |
| Identification and Authentication | The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password based authentication and public key based authentication. Based on the assigned role, a user is granted a set of privileges to access the system.<br><br>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. |
| Security 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<br>• the regular review of all audit data;<br>• initiation of trusted update function;<br>• administration of MACsec functionality;<br>• all administrative tasks (e.g., creating the security policy).<br>The devices are managed through a Command Line Interface (CLI). The CLI is accessible through local (serial) console connection or remote administrative (SSH) session. |
| Protection of the TSF | The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored in encrypted format. Passwords are stored using sha256 or sha512. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE internally maintains the date and time. |
| TOE Access | Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after a period of inactivity. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt. |
| Trusted Path/Trusted Channel | The TOE supports SSH v2 for secure communication to Syslog server. The TOE supports SSH v2 (remote CLI) for secure remote administration. |

# 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 | Assumption Definition |
|---|---|
| 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 cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP 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 computing platform for general purpose applications (unrelated to networking functionality). |
| 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 computing platform for general purpose applications (unrelated to networking functionality). |
| 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. 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). |

| Assumption | Assumption Definition |
|---|---|
| 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 | Threat Definition |
|---|---|
| T.DATA_INTEGRITY | An attacker may modify data transmitted over the MACsec channel in a way that is not detected by the recipient. |
| T. NETWORK_ACCESS | An attacker may send traffic through the TOE that enables them to access devices in the TOE's Operational Environment without authorization. |
| T.UNTRUSTED_COMMUNICATION_CHANNELS | An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit. |

| Threat | Threat Definition |
|---|---|
| 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. |

| Threat | Threat Definition |
|---|---|
| T.WEAK_AUTHENTICATION_ENDPOINTS | Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., 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 include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker. |

| Threat | Threat Definition |
|---|---|
| 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 | An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device. |

### 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 NDcPPv2.1 and MACsecEPv1.2.
- 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 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS Security Target v1.6
- Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS Common Criteria and FIPS Evaluated Configuration Guide v1.0

Any additional customer documentation provided with the product, or that may be 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. Consumers are encouraged to download the configuration documentation from the NIAP website to ensure that the TOE platforms are configured as evaluated.

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The Juniper Networks MX routing appliance is a complete routing system that supports a variety of high-speed interfaces (only Ethernet is within scope of the evaluation).

The EX9200-Series line of Ethernet core switches.

The appliances are physically self-contained, housing the firmware and hardware necessary to perform all routing functions. The architecture components of the appliances are:

- Switch fabric – the switch fabric boards/modules provide a highly scalable, non-blocking, centralized switch fabric matrix through which all network data passes.
- Routing Engine (Control Board) – the RE runs the Junos firmware and provides Layer 3 routing services and Layer 2 switching services. The RE also provides network management for all operations necessary for the configuration and operation of the TOE.
- Layer 2 switching services (EX9200-Series only), Layer 3 switching/routing services and network management for all operations necessary for the configuration and operation of the TOE.
- The Packet Forwarding Engine (PFE) – provides all operations necessary for transit packet forwarding.

In the evaluated deployment the TOE is managed and configured via Command Line Interface, either via a directly connected console or over the network secured using the SSH protocol.

The MACsec line cards support MACsec between adjacent devices, all traffic communicated between the devices including frames for LLDP, DHCP, ARP, STP, Ethernet Control frames, etc (the exceptions to this protection are Destination MAC and Source MAC addresses in MACsec and MKA frames).

In the evaluated configuration MACsec must be configured individually on each point-to-point Ethernet link, such that a pair of MACsec devices (connected by a physical medium) protect Ethernet frames switched or routed from one device to the other. The two MACsec devices are provided with a Connectivity Association Key (CAK) and utilize the MACsec Key Agreement (MKA) protocol to create a secure tunnel. MACsec must be configured to protect all traffic between the devices, with the exception of the MKA or Ethernet control traffic such as EAP over LAN (EAPOL) frames.

**Physical boundary**

The TOE is the Junos OS 18.3R1-S1 firmware running on the appliance chasses listed (below). Hence, the TOE is contained within the physical boundary of the specified appliance chassis**,** as shown in Figure 1 and Figure 2 below.

The physical boundary of the TOE is the entire chassis of the appliance (defined in Table 2 below). In the evaluated configuration, the MX series routers support the MPC7E MACsec line card and the EX series routers support the Ex9200-40XS line card.

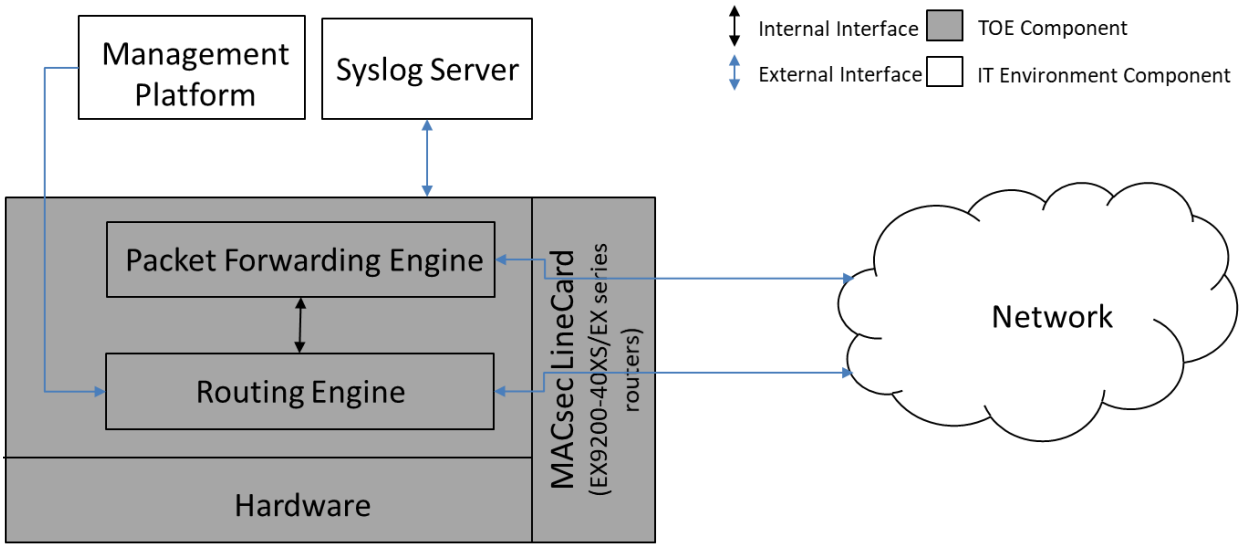


**Figure 1 EX-series TOE Boundary**

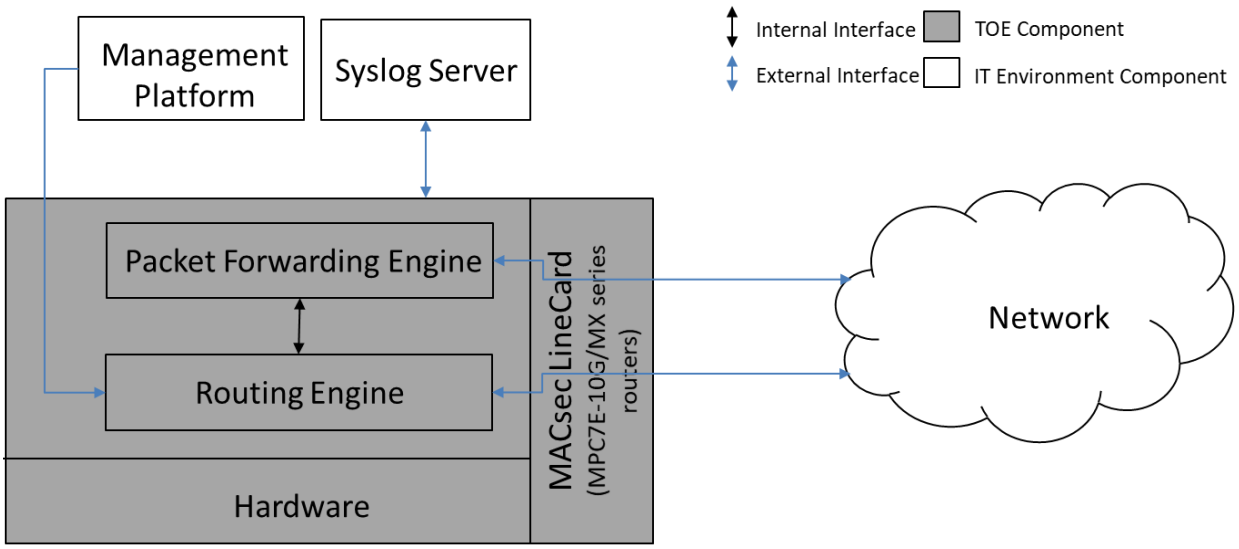


**Figure 2 MX-series TOE Boundary**

1. 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 | Processor | Firmware (Operating System) |
|---|---|---|---|
| MX240 | RE-S-X6-64G and RE-S-X6-128G | Intel Xeon E5-2608L | Junos OS 18.3R1-S1 |
| MX480 | | | |
| MX960 | | | |
| MX2010 | REMX2K-X8-64G and REMX2K-X8-128G | Intel Xeon E5-2618L | |
| MX2020 | | | |
| EX9204<br>EX9208<br>EX9214 | EX9200-RE2 | Intel Xeon E5-2608L | |

**Table 2 TOE Chassis Details**

### 7.1.1 Non-TOE hardware/software/firmware

The TOE relies on the provision of the following items in the network environment:

- Syslog server supporting SSHv2 connections to send audit logs;
- SSHv2 client for remote administration;
- Serial connection client for local administration.

### 7.1.2 Summary of out scope items

- Use of telnet, since it violates the Trusted Path requirement set (see Section 5.7.2)
- Use of FTP, since it violates the Trusted Path requirement set (see Section 5.7.2)
- Use of SNMP, since it violates the Trusted Path requirement set (see Section 5.7.2)
- Use of SSL, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement set (see Section 5.7.2)
- Use of CLI account super-user and linux root account.

## 8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS, 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 and MACsec EP. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, 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 5 and CEM version 3.1 rev 5. The evaluation determined the Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS to be Part 2 extended, and meets the SARs contained in the PP. In addition, the evaluator performed the Assurance Activities specified in the NDPP.

### 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 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS 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 MACsec EP.

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 and MACsec EP 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 and

MACsec EP 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 MACsec EP 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 MACsec EP, and that the conclusion reached by the evaluation team was justified.

### 9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. The vulnerability searches were conducted on July 11th, 2019, July 25th, 2019 , September 13th, 2019 and September 24th, 2019. 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 NDcPPv2.1 and MACsecEPv1.2, 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 NDcPPv2.1 and MACsecEPv1.2, and correctly verified that the product meets the claims in the ST.

## 10 Validator Comments & Recommendations

On MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208, and EX9214 devices, Junos OS Release 18.3R1 is certified for Common Criteria with FIPS mode enabled on the devices.

The evaluation was limited to those security functions contained in the Protection Profile and Extended Package in the as-evaluated configuration. Any other functionality provided by the devices was not assessed as part of this evaluation and therefore no claims nor conclusions can be drawn about their effectiveness or proper operation.

## 11 Annexes

Not applicable.

## 12 Security Target

Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS Security Target v1.6

## 13 Glossary

The following definitions are used throughout this document:

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

## 14 Bibliography

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


1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Security Target Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS, Version 1.6, September 4, 2019.
6. Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS NDcPP and MACSECEP Assurance Activity Report, Version 1.4, September 2019.
7. Junos OS 18.3R1-S1 for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with MPC7E-10G/Ex9200-40XS NDcPP and MACSECEP Evaluation Technical Report, Version 1.5, September 2019.