Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper Networks' Junos OS 23.4R1 for MX10004, MX10008 and MX10016

Version 1.0, 23 December2024

Document reference: AISEP-CC-CR-2024-EFT-T044-CR-V1.0
(Certification expires five years from certification report date)

cyber.gov.au

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Juniper Networks Junos OS 23.4R1 for MX10004, MX10008 and MX10016 against Common Criteria approved Protection Profiles (PPs).

The Target of Evaluation (TOE) is the Universal Routing Platforms that are non-virtual and non-distributed network devices. A purpose built appliance that does not provide any general-purpose computing capabilities. The TOE implements both management and control functions along with MACsec protocol connectivity to networked TOEs.

This report concludes that the Target of Evaluation (TOE) has complied with the following PPs [4]:

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP)
- PP-Module for MACsec Ethernet Encryption Version: 1.0, 02 March 2023 (MOD_MACSEC)

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs with the final Evaluation Technical Report (ETR) submitted on 19 December 2024.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends that administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the hash of any downloaded software, as present on the https://www.juniper.net website
- the system auditor should review the audit trail generated and exported by the TOE periodically

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target [8] and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria [1,2,3] and Protection Profiles [4]
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [8] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Juniper Junos OS 23.4R1 for MX10004, MX10008 and MX10016.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Junos OS 23.4R1 for MX10004, MX10008 and MX10016
Software version	23.4R1
Hardware platforms	MX10004, MX10008 and MX10016
Security Target	Security Target Juniper Junos OS 23.4R1 for MX10004, MX10008 and MX10016, Version 1.0, 16 December 2024
Evaluation Technical Report	Evaluation Technical Report 1.1, dated 19 December 2024 Document reference EFT-T044-ETR 1.1
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020

	PP-Module for MACsec Ethernet Encryption Version: 1.0, 02 March 2023 PP-Configuration for Network Devices and MACsec Ethernet Encryption, version 1.0, 29 March 2023
Developer	Juniper Networks, Inc. 1133 Innovation Way, Sunnyvale California 94089 United States of America
Evaluation facility	Teron Labs Unit 3, 10 Geils Court Deakin ACT 2600 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is the Juniper Networks Junos OS 23.4R1 for MX10004, MX10008, and MX10016. It consists of both hardware and software components that provide secure interconnection and traffic management for two network environments. The TOE includes the chassis MX10004, MX10008, and MX10016, line cards LC480 and LC9600, the Routing Engine and the Junos OS operating system. These components collectively implement the routing and management functions required for secure operation. The TOE features software-defined networking architecture supporting up to 76.8 Tbps of system capacity in four, eight and sixteen slot chassis supporting dense interfaces of 100GbE to 400GbE. The TOE implements MACsec in accordance with IEEE 802.1AE for link-layer encryption between two instances of the TOE.

The intended deployment of the appliances is at the edge to optimise Internet of Things (IoT), enterprise and cable environments in addition to multiservice edge and converged core architectures. The TOE can support label-switching router (LSR), provider edge, Internet peering and backbone applications for large-scale deployments.

TOE Functionality

The TOE functionality evaluated is described in section 1.3 of the Security Target [8]

TOE physical boundary

The TOE is the complete appliance consisting of the Junos OS 23.4R1 firmware running on the MX10004, MX10008, and MX10016. The TOE is contained within the physical boundary of the MX10004, MX10008, and MX10016. The MX10004 and MX10008 may be fitted with either LC480 or LC9600 linecard. The MX10016 may only be fitted with LC480.

LC480 uses Marvell Alaska C PHYs (X7121P/M C0 EVB) to achieve up to 480Gbps throughput. LC9600 utilises Juniper Trio 6 chipset for up to 9.6 Tbps total throughput.

The install image provided for the TOE is:

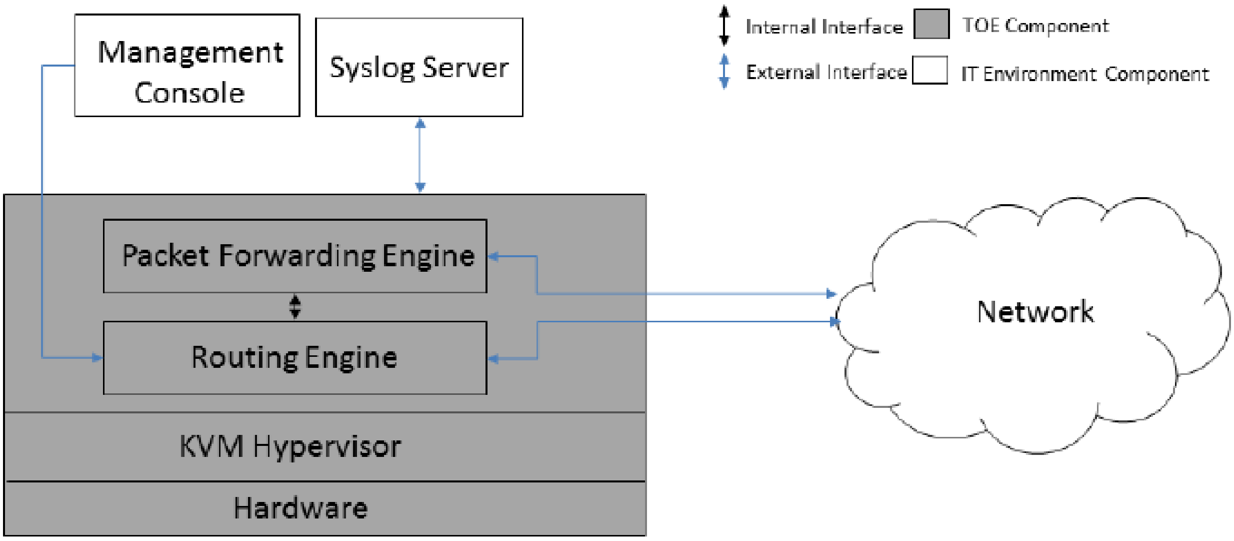
- junos-vmhost-install-mx-x86-64-23.4R1.9.tgz

The firmware version reflects the detail reported for the components of the Junos OS when the “show version” command is executed on the device.

The TOE is contained within the physical boundary of the specified SSR platforms:

PLATFORM	TYPE	ROUTING ENGINE	LINE CARD
MX10004	Chassis	JNP10K-RE1	LC480 LC9600
MX10008	Chassis	JNP10K-RE1	LC480 LC9600
MX10016	Chassis	JNP10K-RE1	LC480

The physical boundary for the MX10004, MX10008 and MX10016 model is shown in the figure below.



Architecture

Each instance of the TOE consists of the following major architectural components:

- The Routing Engine is embedded in a Routing and Control Board (RCB) and performs all routing-process functions. Up to two RCB can be installed on the TOE for increased redundancy.
- The Packet Forwarding Engine is incorporated in the TOE software to perform packet forwarding functons on top of hardware-based link layer and routing engine capabilities.
- The KVM Hypervisor is packaged with the Junos OS to virtualise hardware components for the software of the TOE. The software combined with linecards and routing engine implement all management and routing functions of the TOE.

- The distinct interfaces of the TOE include mechanical, defining the hardware used for cooling and ventilation, LEDs for user status of the TOE. Network interfaces for connecting the TOE to operational network environments. The interfaces ingress and egress traffic from physically seperated from other network interfaces. The TOE does not enforce data processing of network traffic. Management interfaces for administrators to manage the TOE locally from console or remotely via a SSH connection. A Command Line Interface (CLI) is the only method of administering the TOE.
- MACsec is implemented on the linecards for encrypted communcation of adjacent devices via an Ethernet point-to-point link of MACsec capable devices. The protected traffic includes Link Layer Discovery Protocol (LLDP), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), Spanning Tree Protocol (STP) and Ethernet Control Frames.

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [8].

Evaluated functionality

Functional tests performed during the evaluation were taken from the Protection Profiles [4] and Supporting Documents [12] and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

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

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [5] for policy relating to using an evaluated product in an unevaluated configuration.

The following components are considered outside of the scope of the TOE:

- use of telnet, since it violates the Trusted Path requirement set
- use of File Transfer Protocol, since it violates the Trusted Path requirement set
- use of Simple Network Management Protocol, since it violates the Trusted Path requirement set
- use of Secure Sockets Layer, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement set
- use of Command Line Interface account super-user and Linux root account.
- Use of NTP is not included in the certified configuration. Only a local clock of the TOE is used.

Security

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The Security Target [8] contains a summary of the functionality that is evaluated.

Secure delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform:

- shipping label - Ensure that the shipping label correctly identifies the correct customer name and address as well as the device
- outside packaging - Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device
- inside packaging - Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, they should immediately contact the supplier providing the order number, tracking number and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Juniper Networks and not a different company masquerading as Juniper Networks. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:

- verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order
- when a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received and contains the following information:
  - purchase order number
  - Juniper Networks order number used to track the shipment
  - carrier tracking number used to track the shipment
  - list of items shipped including serial numbers
  - address and contacts of both the supplier and the customer
- verify that the shipment was initiated by Juniper Network, by performing the following tasks:
  - compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received
  - log on to the Juniper Networks online customer support portal at https://www.juniper.net/customers/csc/management to view the order status
  - compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

Installation of the TOE

The Configuration Guide [6] contains all relevant information for the secure configuration of the TOE.

Version verification

The verification of the TOE is largely automatic, including the verification using hashes. The TOE cannot load a modified image. Valid software images can be downloaded from https://www.juniper.net. In addition to the automated verification, the site includes individual hashes for each image. The administrator should verify the hash of the software before installing it into the hardware platform.

Security Administrators are able to query the current version of the TOE firmware using the CLI command 'show version'.

Documentation and guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. The evaluated configuration guide (System Admin Guide) document for the Juniper Junos OS 23.4R1 for MX10004, MX10008 and MX10016 is available for download at https://www.juniper.net/documentation. The title is:

- *Junos® OS Common Criteria Evaluated Common Criteria Evaluated Configuration Guide for MX10004, MX10008, and MX10016 Devices with JNP10K-LC9600 and JNP10K-LC480 Line Cards, Release 23.4R1, Published 15 July 2024.*

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org. [1, 2, 3, 9, 13].

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [5].

Secure usage

The evaluation of the TOE considered specific assumptions about its operational environment. These assumptions are essential to ensure that the security objectives of the TOE are achieved.

The network device is assumed to be physically secured within its operational environment, protected from physical attacks that could compromise its security or interfere with its physical connections and correct operation. This level of protection is expected to be sufficient to safeguard the device and the sensitive data it handles.

The TOE is expected to provide networking functionality as its primary purpose and should not offer any general-purpose computing capabilities, such as running compilers or user applications unrelated to its networking functions. This ensures that the device remains focused solely on its intended security and networking roles.

The network device's administrator(s) are assumed to be trustworthy, acting in the best interests of the organization's security. This includes being well-trained, adhering to established policies, and following all guidance documentation. Administrators are responsible for ensuring that passwords and credentials used within the TOE are strong and secure. The TOE is not expected to protect against a malicious administrator who deliberately seeks to bypass or compromise its security features.

The TOE's firmware and software are assumed to be regularly updated by an administrator, particularly in response to newly discovered vulnerabilities. This ensures that the TOE remains protected against emerging threats.

The credentials (such as private keys) used by administrators to access the TOE must be securely protected on any platform where they are stored. Administrators must also ensure that sensitive residual information, including cryptographic keys, keying material, PINs, and passwords, is not accessible to unauthorized individuals when networking equipment is discarded or removed from service.

The TOE is assumed to be connected to distinct networks in a way that ensures its security policies are enforced on all relevant network traffic flowing between these networks.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant Protection Profiles [4] and Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].

Testing methodology was drawn from Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3] and relevant Supporting Documents [12].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [10].

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9] and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs* [13] were also upheld.

Functional testing

All functional tests performed by the evaluators were taken from the Protection Profiles [4] and Supporting Documents [12]. The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Entropy testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report [11].

Penetration testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the NDcPP Supporting Document [12] that follow a flaw hypothesis methodology. Accordingly, four types of flaw hypotheses have been considered:

- public vulnerabilities
- NDFW-iTC (Network international Technical Community) sourced
- evaluation team generated
- tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to **16 September 2024** coinciding with the conclusion of the evaluation. There was no identifiable Type 2 hypotheses for this evaluation.

The evaluation team devised one test to check a potential vulnerability within the TOE's boot process. The evaluation team also conducted tool-generated vulnerability testing of the TOE as per the Supporting Document [12]

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification is focused on the evaluation of product compliance with Protection Profiles that cover the technology area of network devices. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profiles cover the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the PP Supporting Document and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profiles (PP). PP provides assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that Security Target, guidance documentation, and a basic description of the architecture of the TOE.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [8] and **has met** the requirements of the Protection Profiles CPP_ND_V2.2E [4.a], MOD_MACSEC_V1.0 [4.b] and PP configuration for NDcPP and MACsec [4.c].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of the Juniper Junos OS 23.4R1 for MX10004, MX10008 and MX10016 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [8] have met the requirements of the Network Device Protection Profiles [4].

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the Australian Government Information Security Manual [5].

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends that users and administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings

- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the hash of any downloaded software, as present on the https://www.juniper.net website
- the system auditor should review the audit trail generated and exported by the TOE periodically.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*

2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*

3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*

4. Protection Profiles:

   a) *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (CPP_ND_V2.2E)*
   b) *PP-Module for MACsec Ethernet Encryption Version: 1.0, 02 March 2023 (MOD_MACSEC_V1.0)*
   c) *PP-Configuration for Network Devices and MACsec Ethernet Encryption, version 1.0, 29 March 2023*

5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism

6. Junos® OS Common Criteria Evaluated Common Criteria Evaluated Configuration Guide for MX10004, MX10008, and MX10016 Devices with JNP10K-LC9600 and JNP10K-LC480 Line Cards, Release 23.4R1, Published 15 July 2024.

7. *Evaluation Technical Report Juniper Junos OS 23.4R1 for MX10004, MX10008 and MX10016 Version 1.1, dated 19 December 2024* (Document reference EFT-T044-ETR 1.1)

8. *Security Target Junos OS 23.4R1 for Juniper MX10004, MX10008 and MX10016, Version 1.0, 16 December 2024.*

9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*

10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf

11. Entropy Documentation:

    a) *Entropy Report, Intel® Digital Random Number Generator SP800-90B Entropy Assessment Report for Intel® Xeon® CPUs Based on the Intel® Xeon® E5 v4 Processor Family and Intel® Core™ i7 (Formerly Broadwell EP) 10-Core Die with FCLGA2011 Package, Revision 12, dated May 2023*

12. Protection Profile Supporting Documents

    a) *Supporting document, Evaluation Activities for Network Device cPP, version 2.2e, December 2019 (NDcPP-SD)*
    b) *Supporting document, PP-Module for MACsec Ethernet Encryption, version 1.0, 02 March 2023 (MOD_MACSEC-SD)*

13. CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0

Abbreviations

AISEP	Australian Information Security Evaluation Program
ARP	Address Resolution Protocol
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
CEM	Common Criteria Evaluation Methodology
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GbE	Gigabit Ethernet
Gbps	Gigabit per second
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers standards
IoT	Internet of Things
IPsec	Internet Protocol Security
KVM	Kernel-based Virtual Machine
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
LSR	Label-Switching Router
MACsec	Media Access Control Security
MOD_MACSEC	NIAP Protection Profile Module for MACsec
MOD_MACSEC-SD	Supporting Document for MACsec Module Protection Profile
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
NDcPP-SD	Supporting Document for Network Device collaborative Protection Profile
NTP	Network Time Protocol
PP	Protection Profile
RCB	Routing Control Board
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
Tbps	Terabits Per Second
TOE	Target of Evaluation
TLS	Transport Layer Security