Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australasian Information Security Evaluation Program

Certification Report

Juniper Junos OS 19.4R1 for EX4300-48MP

Version 1.0, 20 May 2020

cyber.gov.au

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Junos OS 19.4R1 executing on the EX4300-48MP Ethernet switch against Common Criteria approved Protection Profile.

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 19.4R1 for EX4300-48MP Ethernet switch.

The Ethernet switch is a secure network device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. All switching platforms are powered by the Junos OS software, Junos OS 19.4R1, 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 switching.

This report concludes that the TOE has complied with the following Protection Profile [4]:

- collaborative Protection Profile for Network Devices (NDcPP), version 2.1 dated 24 September 2018

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program. The evaluation was performed by Teron Labs with the final Evaluation Technical Report (ETR) submitted on 27 April 2020.

With regard to the secure operation of the TOE, the Australasian 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
- verify the hash of any downloaded software, as present on the Juniper 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 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 and Protection Profile [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 Junos OS 19.4R1 for EX4300-48MP

Description	Version
Evaluation scheme	Australasian Information Security Evaluation Program
TOE	Junos OS 19.4R1 for EX4300-48MP
Software version	19.4R1
Hardware platforms	EX4300-48MP Ethernet switch
Security Target	*Security Target Junos OS 19.4R1 for EX4300-48MP, Version 1.0, 21-April-2020*
Evaluation Technical Report	*Evaluation Technical Report v1.0, dated 27 April 2020* Document reference EFT-T012-ETR 1.0
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 (NDcPP), version 2.1 dated 24 September 2018

Developer	Juniper Networks, Inc. 1133 Innovation Way, Sunnyvale California 94089 United States of America
Evaluation facility	Teron Labs, Unit 3, 10 Geils Court, Canberra, 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 Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 19.4R1 executing on EX4300-48MP Ethernet switch.

The Ethernet switch is a secure network device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. All switching platforms are powered by the Junos OS software, Junos OS 19.4R1, 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 switching.

The Ethernet switch 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.

The appliance is physically self-contained, housing the software, firmware and hardware necessary to perform all switching functions. The appliance is a fixed chassis configuration switch.

TOE Functionality

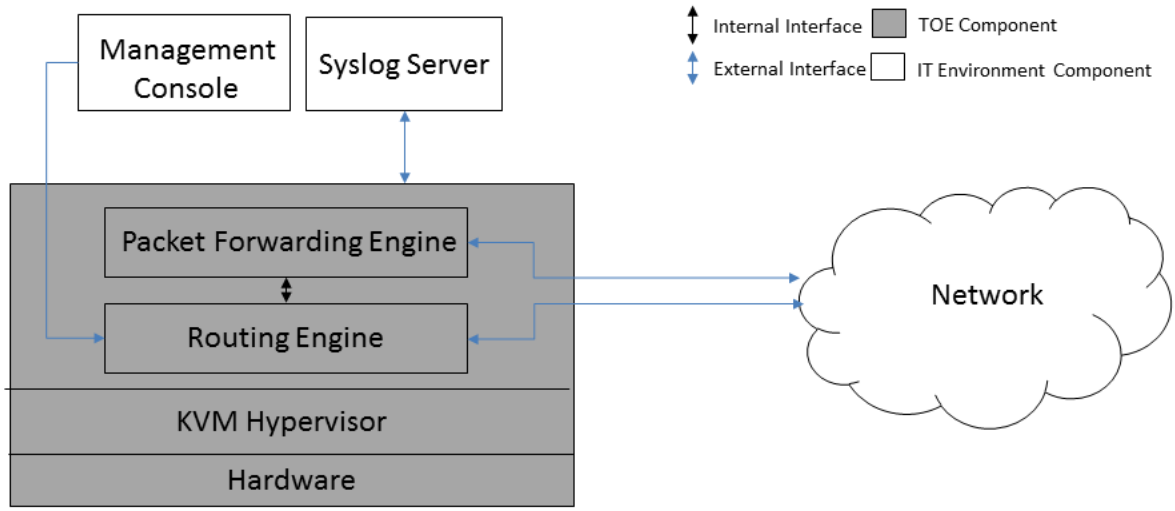
The TOE functionality that was evaluated is described in section 1.6 of the Security Target [8].

TOE physical boundary

The TOE is the Junos OS 19.4R1 firmware running on the Ethernet switch chassis listed in the table below. The TOE is contained within the physical boundary of the specified chassis.

Chassis Model	Network Ports	Firmware (Operating System)
	EX4300-48MP:	
EX4300	24 10/100/1000BASE-T Ethernet network ports o 24 100/1000/2500/5000/10000BASE-T Ethernet network ports, and four built-in QSFP+ ports that can house 40-Gigabit QSFP+ transceivers	Junos OS 19.4R1

The physical boundary of the EX4300-48M switch instance of the TOE includes the KVM Hypervisor, which provides the virtualisation layer in which Junos OS VM executes, as shown in figure below.



The TOE interfaces comprise the following:

- network interfaces which pass traffic
- management interface through which handle administrative actions.

The firmware version reflects the detail reported for the components of the Junos OS when the 'show version local' command is executed on the appliance.

The guidance document included as part of the TOE is *Junos OS Common Criteria Evaluated Configuration Guide for EX4300 Devices, Release 19.4R1, Published 2020-03-04* [7]

Architecture

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

The Routing Engine (RE) runs the Junos firmware and provides Layer 2 and Layer 3 switching services and network management for all operations necessary for the configuration and operation of the TOE and controls the flow of information through the TOE.

The Packet Forwarding Engine (PFE) provides all operations necessary for packet forwarding.

The Routing Engine and Packet Forwarding Engine perform their primary tasks independently, while constantly communicating through a high-speed internal link. This arrangement provides streamlined forwarding and routing control and the capability to run Internet-scale networks at high speeds.

The Ethernet switches support numerous switching standards for flexibility and scalability.

The functions of the Ethernet switches can all be managed through the Junos firmware, either from a connected terminal console or via a network connection. Network management is secured using the SSH protocol. All management, whether from a user connecting to a terminal or from the network, requires successful authentication. 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 Junos RE functionality is running as a Guest in a Virtual Machine (VM) provided by Wind River Linux (WRL7). The WRL virtualisation is provided using an optimised Kernel-Based Virtual Machine (KVM).

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

All tests performed during the evaluation were taken from the Protection Profile listed in [4] 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 Ethernet switches require RJ-45, SFP/SFP+ and/or QSFP+ network interfaces to operate and communicate with the connected network.

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. New Zealand Government users should consult the *New Zealand Information Security Manual* [6].

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.

Security

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

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per guidance documentation Junos OS Common Criteria Evaluated Configuration Guide for EX4300 Devices, Release 19.4R1, Published 2020-03-04 [7]

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 Networks. To verify that a shipment was initiated by Juniper Networks, you should perform 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 [7] 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. All guidance material is available for download at https://www.juniper.net:

- *Junos OS Common Criteria Evaluated Configuration Guide for EX4300 Devices, Release 19.4R1, Published, 4 March 2020*
- *Junos OS CLI User Guide, 25 September 2019*
- *Junos OS Installation and Upgrade Guide, 9 January 2020*

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [5]. The *New Zealand Information Security Manual* is available at https://www.gcsb.govt.nz/ [6].

Secure usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met:

- 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 unauthorised entities to extract data, bypass other controls, or otherwise manipulate the device.
- 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 standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
- The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organisation. 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.

- 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.
- The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
- The Administrator must ensure that there is no unauthorised 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.

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 Protection Profile [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].

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program [11].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [10].

Functional testing

All tests performed by the evaluators were taken from the Protection Profile [4]. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All Security Functional Requirements listed in the Security Target and the Protection Profile were exercised during testing.

Entropy testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report [12].

Penetration testing

Vulnerability assessments made against the Protection Profile are performed using a set of modified evaluation activities drawn from the Common Criteria Evaluation Methodology [5] to provide standardised vulnerability testing for TOE-types evaluated against the Protection Profile. More details can be found in the Protection Profile and its supporting document.

The evaluator performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for the exploitation.

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 Profile that covers the technology area of network devices. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers 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 assurance activities, 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 Profile (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 Profile [4].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [9], the Australasian Certification Authority **certifies** the evaluation of the Juniper Junos OS 19.4R1 for EX4300-48MP Ethernet switch performed by the Australasian Information Security Evaluation Facility, Teron Labs.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [5] and New Zealand Government users should consult the *New Zealand Information Security Manual* [6].

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australasian 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 Profile:
   - *collaborative Protection Profile for Network Devices (NDcPP), Version 2.1, 24 September 2018*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. *New Zealand Information Security Manual:* https://www.nzism.gcsb.govt.nz/ism-document/
7. Guidance documentation:
   - *Junos OS Common Criteria Evaluated Configuration Guide for EX4300 Devices, Release 19.4R1, Published, 4 March 2020*
   - *Junos OS CLI User Guide, 25 September 2019*
   - *Junos OS Installation and Upgrade Guide, 9 January 2020*
8. *Security Target Junos OS 19.4R1 for EX4300-48MP, Version 1.0, 21-April-2020*
9. *Evaluation Technical Report - Junos OS 19.4R1 for EX4300-48MP v1.0, dated 27 April 2020* (Document reference EFT-T012-ETR 1.0)
10. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
11. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf
12. *Seeding of the Kernel RBG In EX4300-MP Appliances Running Junos 19.4R1, Version 1.0, 2 December 2019*

Abbreviations

AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
TOE	Target of Evaluation