Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australasian Information Security Evaluation Program

Juniper Junos OS 18.1R1 for QFX5100 and EX4600

Certification Report 2018/119

11-10-2018
Version 1.0

Amendment Record

Version	Date	Description
0.1	04 - 10 - 2018	Internal
1.0	11 - 10 - 2018	Public Release

Executive Summary

This report describes the findings of the IT security evaluation of Junos OS 18.1R1 for QFX5100 and EX4600 against Common Criteria and a Protection Profile.

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 18.1R1 executing on QFX5100 and EX4600 Ethernet Switches.
Each of the Ethernet Switches 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 18.1R1, 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 Switches 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 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 optimized Kernel-Based Virtual Machine (KVM).

The report concludes that the product has complied with the Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314.

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Applied Intelligence and was completed on 10 August 2018.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) 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 and
d) Verify the hash of the downloaded software, as present on the Juniper website.

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.

Contents

Chapter 1 – Introduction

1.1 Overview

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

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria (CC) and the NDcPP v2.0E.

b) 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.

1.3 Identification

The TOE is Junos OS 18.1R1 for QFX5100 and EX4600.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Junos OS 18.1R1 for QFX5100 and EX4600
Software Version	18.1R1
Hardware Platforms	QFX5100 and EX4600
Security Target	Security Target Junos OS 18.1R1 for QFX5100 and EX4600, dated 10 October 2018
Evaluation Technical Report	Evaluation Technical Report v1.0, dated 11 October 18, Document reference EFS-T054-ETR

Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1.Rev5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	NDcPP v2.0E
Developer	Juniper Networks, Inc. 1133 Innovation Way, Sunnyvale California 94089 United States
Evaluation Facility	BAE Applied Intelligence Level 1 14 Childers Street, Canberra, ACT 2600 AUSTRALIA

Chapter 2 – Target of Evaluation

2.1 Overview

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

2.2 Description of the TOE

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 18.1R1 executing on QFX5100 and EX4600 Ethernet Switches. Each of the Ethernet Switches 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 18.1R1, 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 Switches 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 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 optimized Kernel-Based Virtual Machine (KVM).

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

Function	Description
Protected Communications	The TOE provides an SSH server to support protected communications for administrators to establish secure sessions and to connect to external syslog servers. 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 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.
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 with warning messages 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.
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 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 **Error! Reference source not found.** of the Security Target. 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.
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.

2.4 TOE Architecture

Each instance of the TOE consists of the following 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.

2.5 Clarification of Scope

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

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Common Criteria Evaluated Configuration Guide for EX4600, and QFX5100 Devices [7].

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

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from NDcPP v2.0E [4], and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

2.5.2 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 Australian Government Information Security Manual (ISM) [5] for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB)'s NZISM [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 FTP, since it violates the Trusted Path requirement set
- Use of SNMP, since it violates the Trusted Path requirement set
- Use of SSL, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement set
- Use of CLI account super-user and linux root account.

2.6 Security

2.6.1 Security Policy

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

2.7 Usage

2.7.1 Evaluated Configuration

The evaluated configuration is based on default installation of the TOE with additional configuration taken from the Evaluated Configuration Guide [7].

2.7.2 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, he or she should immediately contact the supplier. Provide 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.
- Verify that the e-mail 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.

2.7.3 Installation of the TOE

The Evaluated Configuration Guide [7] contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

The verification of the TOE is largely automatic, including the verification using MD5 hashes. The TOE cannot load a modified image. Valid software images can be downloaded from **www.juniper.net.**

2.9 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 **www.juniper.net.**

- Junos® OS Common Criteria Evaluated Configuration Guide for EX4300, EX4600, QFX5100, and QFX5200 Series Devices, Release 18.1R1, 16-Jul-18
- Junos® OS CLI User Guide, 27 June 2018
- Junos® OS Installation and Upgrade Guide, 18 July 2018
- Seeding of the Kernel RBG – Junos™ OS 18.1R1 QFX5100-24Q/EX4600-40F, Version 7.0, 07 October 2018

All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au** [5]. The NZISM is available at **www.gcsb.govt.nz** [6].

2.10 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.

- 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.

Chapter 3 – Evaluation

3.1 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.

3.2 Evaluation Procedures

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

Test 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 (AISEP).

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.

3.3 Functional Testing

3.3.1 Testing Coverage

All tests performed by the evaluators were taken from the NDcPP. 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 SFRs listed in the Security Target and the Protection Profiles were exercised during testing.

3.4 Entropy Testing

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

3.5 Penetration Testing

Vulnerability assessments made against the NDcPP are performed using a set of modified evaluation activities drawn from the Common Criteria Evaluation Methodology (CEM) to provide standardised vulnerability testing for TOE-types evaluated against this cPP. More details can be found in the NDcPP [4].

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

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

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

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

4.2 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of network devices. Agencies 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 security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles (PPs). PPs provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

4.3 Certification Result

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 18.1R1 for QFX5100 and EX4600 performed by the Australasian Information Security Evaluation Facility, BAE Applied Intelligence.

BAE Applied Intelligence **has determined** that the TOE upholds the claims made in the Security Target [8] and **has met** the requirements of NDcPP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles.

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.

4.4 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 ISM [5] and New Zealand Government users should consult the GCSB's NZISM [6].

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.
d) The Evaluators also recommend that the administrator verify the hash of the downloaded software, as present on the **www.juniper.net** website.

Annex A – References and Abbreviations

A.1 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. collaborative Protection Profile for Network Devices (NDcPP), Version 2.0E, 14-March-2018

5. 2017 Australian Government Information Security Manual (ISM), Australian Signals Directorate

6. NZ Information Security Manual (NZISM): https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

7. Guidance Documentation:

    - Junos® OS Common Criteria Evaluated Configuration Guide for EX4300, EX4600, and QFX5100 Devices, Release 17.4R1, 9 July 2018

    - Junos® OS Intrusion Detection and Prevention Feature Guide for Security Devices, 22 May 2018

    - Junos® OS VPN Feature Guide for Security Devices, 29 May 2018

    - Junos® OS CLI User Guide, 28 May 2018

    - Junos® OS Installation and Upgrade Guide, 20 June 2018

    - Junos® OS Routing Policies, Firewall Filters and Traffic Policers Feature Guide, 13 June 2018

8. Security Target Junos OS 18.1 R1 for QFX5100 and EX4600, v1.6, 10 October 2018

9. Evaluation Technical Report - Junos OS 18.1R1 for QFX5100 and EX4600, v1.0 – 11 October 2018

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

11. Seeding of the Kernel RBG – Junos™ OS 18.1R1 QFX5100-24Q/EX4600-40F, Version 6.0, 7 October 2018

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
FWcPP	CCRA approved collaborative Protection Profile for Firewalls
GCSB	Government Communications Security Bureau
IDM	IPS Device Manager
NTP	Network Time Protocol
NDcPP	CCRA approved collaborative Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy