



**Australian Government**  
**Department of Defence**

# **Australasian Information Security Evaluation Program**

**Junos OS 17.4R1 for SRX300, SRX320,  
SRX340, SRX345, SRX550M, SRX5400,  
SRX5600 and SRX5800 Series**

**Certification Report  
2018/115**

**04-07-2018  
Version 1.0**

Commonwealth of Australia 2018  
Reproduction is authorised provided  
that the report is copied in its entirety.

## Amendment Record

Version	Date	Description
0.1	05 - 06 - 2018	Internal
1.0	04 - 07 - 2018	Public Release

## Executive Summary

This report describes the findings of the IT security evaluation of Junos OS 17.4R1 for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800 Series against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Junos OS 17.4R1 for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800 Series. The Services Gateway appliances primarily support the definition of, and enforce, information flow policies among network nodes. The Services Gateway appliances provide for stateful inspection of every packet that traverses the network and provide central management to manage the network security policy. 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, protocol, type of access requested, and services requested. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited, that their own functions are protected from potential attacks, and provides the security tools to manage all of the security functions. The TOE provides multi-site virtual private network (VPN) gateway functionality. The TOE also implements Intrusion Prevention System functionality, capable of monitoring information flows to detect potential attacks based on pre-defined attack signature and anomaly characteristics in the traffic.

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

Security Functionality	Description
Protected Communications	<p>The TOE provides an SSH server to support protected communications for administrators to establish secure sessions and to connect to external syslog servers.</p> <p>The TOE also supports IPsec connections to provide multi-site virtual private network (VPN) gateway functionality and also as a tunnel for remote administrate SSH connections. The TOE requires that applications exchanging information with it are successfully authenticated prior to any exchange (i.e. applications connecting over SSH and IPsec).</p> <p>Telnet, File Transfer Protocol (FTP), and Secure Socket Layer (SSL) are out of scope.</p> <p>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 adjacent systems.</p>
Administrator Authentication	<p>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.</p>

Security Functionality	Description
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, service requests and IPS events. 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	<p>The TOE provides a Security Administrator role that is responsible for:</p> <ul style="list-style-type: none"> <li>• the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product</li> <li>• the regular review of all audit data;</li> <li>• initiation of trusted update function;</li> <li>• administration of VPN, IPS and Firewall functionality;</li> <li>• all administrative tasks (e.g., creating the security policy).</li> </ul> <p>The devices are managed through a Command Line Interface (CLI). The CLI is accessible through local (serial) console connection or remote administrative (SSH) session.</p>
Packet Filtering/Stateful Traffic Filtering	The TOE provides stateful network traffic filtering based on examination of network packets and the application of information flow rules.
Intrusion Prevention	The TOE can be configured to analyse IP-based network traffic forwarded to the TOE's interfaces, and detect violations of administratively-defined IPS policies. The TOE is capable of initiating a proactive response to terminate/interrupt an active potential threat, and to initiate a response in real time that would cause interruption of the suspicious traffic flow.
User Data Protection/Information Flow Control	The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users. The TOE has the capability to regulate the information flow across its interfaces; traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, the transport layer protocol, the source service identifier, and the destination service identifier (TCP or UDP port number).

The report concludes that the product has complied with the following:

- Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314
- collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314
- collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11
- Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1

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-May-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

<b>Chapter 1 – Introduction .....</b>	<b>1</b>
1.1 Overview .....	1
1.2 Purpose .....	1
1.3 Identification .....	1
<b>Chapter 2 – Target of Evaluation .....</b>	<b>3</b>
2.1 Overview .....	3
2.2 Description of the TOE .....	3
2.3 TOE Functionality .....	4
2.4 TOE Architecture .....	5
2.5 Clarification of Scope .....	5
2.5.1 Evaluated Functionality .....	6
2.5.2 Non-evaluated Functionality and Services .....	6
2.6 Security .....	6
2.6.1 Security Policy .....	6
2.7 Usage .....	6
2.7.1 Evaluated Configuration .....	6
2.7.2 Secure Delivery .....	7
2.7.3 Installation of the TOE .....	8
2.8 Version Verification .....	8
2.9 Documentation and Guidance .....	8
2.10 Secure Usage .....	9
<b>Chapter 3 – Evaluation .....</b>	<b>10</b>
3.1 Overview .....	10
3.2 Evaluation Procedures .....	10
3.3 Functional Testing .....	10
3.3.1 Testing Coverage .....	10
3.4 Entropy Testing .....	10
3.5 Penetration Testing .....	11
<b>Chapter 4 – Certification .....</b>	<b>12</b>
4.1 Overview .....	12
4.2 Assurance .....	12
4.3 Certification Result .....	12
4.4 Recommendations .....	12
<b>Annex A – References and Abbreviations .....</b>	<b>14</b>
A.1 References .....	14

A.2 Abbreviations ..... 16

# 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), the NDcPP v2.0E, and FWcPP v2.0E; IPSEP v2.11 and VPNEP v 2.1
- 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 [11] 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 17.4R1-S1 for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800.

**Table 1 Identification Information**

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Juniper SRX-Metal Appliances running Junos OS
Software Version	17.4R1-S1
Hardware Platforms	SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800
Security Target	Security Target Junos OS 17.4R1 for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800 Series, v2.2, dated 22-06-2018

Evaluation Technical Report	Evaluation Technical Report v1.0, dated 22-June-18, Document reference EFS-T050-ETR
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extend 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	NDcPP v2.0E FWcPP v2.0E VPNEP v2.1 IPSEP v2.11
Developer	Juniper Networks, Inc. 1133 Innovation Way, Sunnyvale California 94089 United States
Evaluation Facility	BAE Applied Intelligence Level 1 14 Childers Street 2600

## **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 TOE is Junos OS 17.4R1-S1 for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800.

The Services Gateway appliances primarily support the definition of, and enforce, information flow policies among network nodes. The Services Gateway appliances provide for stateful inspection of every packet that traverses the network and provide central management to manage the network security policy. 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, protocol, type of access requested, and services requested. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited, that their own functions are protected from potential attacks, and provides the security tools to manage all of the security functions. The TOE provides multi-site virtual private network (VPN) gateway functionality. The TOE also implements Intrusion Prevention System functionality, capable of monitoring information flows to detect potential attacks based on pre-defined attack signature and anomaly characteristics in the traffic.

## 2.3 TOE Functionality

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

Security Functionality	Description
Protected Communications	<p>The TOE provides an SSH server to support protected communications for administrators to establish secure sessions and to connect to external syslog servers.</p> <p>The TOE also supports IPsec connections to provide multi-site virtual private network (VPN) gateway functionality and also as a tunnel for remote administrate SSH connections. The TOE requires that applications exchanging information with it are successfully authenticated prior to any exchange (i.e. applications connecting over SSH and IPsec).</p> <p>Telnet, File Transfer Protocol (FTP), and Secure Socket Layer (SSL) are out of scope.</p> <p>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 adjacent systems.</p>
Administrator Authentication	<p>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.</p>
Correct Operation	<p>The TOE provides for both cryptographic and non-cryptographic self-tests, and is capable of automated recovery from failure states.</p>
Trusted Update	<p>The administrator can initiate update of the TOE firmware. The integrity of any firmware updates is verified prior to installation of the updated firmware.</p>
Audit	<p>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, service requests and IPS events. 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.</p>

Security Functionality	Description
Management	<p>The TOE provides a Security Administrator role that is responsible for:</p> <ul style="list-style-type: none"> <li>• the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product</li> <li>• the regular review of all audit data;</li> <li>• initiation of trusted update function;</li> <li>• administration of VPN, IPS and Firewall functionality;</li> <li>• all administrative tasks (e.g., creating the security policy).</li> </ul> <p>The devices are managed through a Command Line Interface (CLI). The CLI is accessible through local (serial) console connection or remote administrative (SSH) session.</p>
Packet Filtering/Stateful Traffic Filtering	<p>The TOE provides stateful network traffic filtering based on examination of network packets and the application of information flow rules.</p>
Intrusion Prevention	<p>The TOE can be configured to analyze IP-based network traffic forwarded to the TOE's interfaces, and detect violations of administratively-defined IPS policies. The TOE is capable of initiating a proactive response to terminate/interrupt an active potential threat, and to initiate a response in real time that would cause interruption of the suspicious traffic flow.</p>
User Data Protection/Information Flow Control	<p>The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users. The TOE has the capability to regulate the information flow across its interfaces; traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, the transport layer protocol, the source service identifier, and the destination service identifier (TCP or UDP port number).</p>

## 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 3 routing 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, including Network Address Translation (NAT) and all operations necessary for the encryption/decryption of packets for secure communication via the IPSec protocol.
- The Packet Forwarding Engine (PFE) provides all operations necessary for transit 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 and FIPS Evaluated Configuration Guide for SRX Series Devices [10].

The scope of the evaluation was limited to those claims made in the Security Target [11].

### **2.5.1 Evaluated Functionality**

All tests performed during the evaluation were taken from NDcPP v2.0E [4], FWcPP v2.0E [5], VPNEP v2.1 [7], IPSEP v2.11 [6] 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) [8] 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) Information Security Manual (NZISM) [9].

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 [11] contains a summary of the functionality to be evaluated:

## **2.7 Usage**

### **2.7.1 Evaluated Configuration**

The TOE consists of the Junos OS 17.4R1-S1 for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Common Criteria and FIPS Evaluated Configuration Guide for SRX Series Devices [10].

## 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 [10] 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](http://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](http://www.juniper.net).

- Junos® OS Common Criteria and FIPS Evaluated Configuration Guide for SRX Series Devices, Release 17.4R1, 11 May 2018
- Junos® OS Intrusion Detection and Prevention Feature Guide for Security Devices, 17-Oct-17
- Junos® OS VPN Feature Guide for Security Devices, 31-Oct-17
- Junos® OS CLI User Guide, 19-Sep-17
- Junos® OS Installation and Upgrade Guide, 30-Oct-17
- Junos® OS Routing Policies, Firewall Filters and Traffic Policers Feature Guide, 22-Aug-17

All common criteria guidance material is available at [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org). The Information Security Manual (ISM) is available at [www.asd.gov.au](http://www.asd.gov.au) [8]. The NZISM is available at [www.gcsb.govt.nz](http://www.gcsb.govt.nz) [9].

## 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).
- 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).

- 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.
- It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

## **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], FWcPP [5], VPNEP [7], IPSEP [6] 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 Rev 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, FWcPP, IPSEP and VPNEP. 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 [14].

### **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 Protection Profiles 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 [12], the Australasian Certification Authority **certifies** the evaluation of the Juniper SRX-Metal Appliances running Junos OS 17.4R1-S1 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 [11] and **has met** the requirements of NDcPP, FWcPP, VPNEP, IPSEP.

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 [8] and New Zealand Government users should consult the GCSB's NZISM [9].

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 2107, Version 3.1, Revision 5
4. collaborative Protection Profile for Network Devices (NDcPP), Version 2.0E, 14-March-18
5. collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 2.0E, 14 March 2018
6. Network Device Collaborative Protection Profile/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package for Intrusion Prevention Systems, Version 2.11, 8-Mar-17
7. Network Device Collaborative Protection Profile/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, 8-Mar-17
8. 2017 Australian Government Information Security Manual (ISM), Australian Signals Directorate
9. NZ Information Security Manual (NZISM), Government Communications Security Bureau <https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/>
10. Guidance Documentation:
  - Junos® OS Common Criteria and FIPS Evaluated Configuration Guide for SRX Series Devices, Release 17.4R1, 11 May 2018
  - Junos® OS Intrusion Detection and Prevention Feature Guide for Security Devices, 17-Oct-17
  - Junos® OS VPN Feature Guide for Security Devices, 31-Oct-17
  - Junos® OS CLI User Guide, 19-Sep-17
  - Junos® OS Installation and Upgrade Guide, 30-Oct-17

- Junos® OS Routing Policies, Firewall Filters and Traffic Policers Feature Guide, 22-Aug-17
11. Security Target Junos OS 17.4R1 for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 and SRX5800 Series, v2.2, 22-June-2018
  12. Evaluation Technical Report, Junos OS 17.4R1-S1 FOR SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600 AND SRX5800 SERIES, v1.0 – 11-May-2018
  13. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014.
  14. Seeding of the Kernel RBG Junos 17.4R1-S1.9 for SRX300, SRX320, SRX340, SRX345,SRX345-DUAL, SRX550-M , 16-April-2018
  15. NIST publication SP800-90B Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2016.

## **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