



# Australasian Information Security Evaluation Program

## Certification Report

Juniper Junos OS 19.2R1-S2 for SRX5400,  
SRX5600 and SRX5800

Version 1.0, 20 May 2020

# Table of contents

<b>Executive summary</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>Overview</b>	<b>2</b>
<b>Purpose</b>	<b>2</b>
<b>Identification</b>	<b>2</b>
<b>Target of Evaluation</b>	<b>4</b>
<b>Overview</b>	<b>4</b>
<b>Description of the TOE</b>	<b>4</b>
<b>TOE Functionality</b>	<b>4</b>
<b>TOE physical boundary</b>	<b>4</b>
<b>Architecture</b>	<b>7</b>
<b>Clarification of scope</b>	<b>9</b>
Evaluated functionality	9
Non-TOE hardware/software/firmware	9
Non-evaluated functionality and services	9
<b>Security</b>	<b>9</b>
<b>Usage</b>	<b>10</b>
Evaluated configuration	10
<b>Secure delivery</b>	<b>10</b>
Installation of the TOE	11
<b>Version verification</b>	<b>11</b>
<b>Documentation and guidance</b>	<b>11</b>
<b>Secure usage</b>	<b>11</b>

<b>Evaluation</b>	<b>13</b>
<b>Overview</b>	<b>13</b>
<b>Evaluation procedures</b>	<b>13</b>
<b>Functional testing</b>	<b>13</b>
<b>Entropy testing</b>	<b>13</b>
<b>Penetration testing</b>	<b>13</b>
<b>Certification</b>	<b>14</b>
<b>Overview</b>	<b>14</b>
<b>Assurance</b>	<b>14</b>
<b>Certification result</b>	<b>14</b>
<b>Recommendations</b>	<b>14</b>
<b>Annex A – References and abbreviations</b>	<b>16</b>
<b>References</b>	<b>16</b>
<b>Abbreviations</b>	<b>17</b>

# Executive summary

This report describes the findings of the IT security evaluation of Junos OS 19.2R1-S2 for SRX5400, SRX5600 and SRX5800 appliances against Common Criteria approved Protection Profiles.

Each Juniper Networks SRX Services Gateway appliance is a security system that supports a variety of high-speed interfaces (up to 40 Gbps for firewall and 20 Gbps for IPS) for medium/large networks and network applications. Juniper Networks routers share common Junos firmware, features, and technology for compatibility across platforms.

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

- collaborative Protection Profile for Network Devices (NDcPP), version 2.1 dated 24 September 2018
- collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 2.0+Errata 20180314, dated 14 March 2018
- collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for VPN Gateway, version 2.1, dated 08 March 2017 (VPN EP)
- 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, dated 15 June 2017 (IPS EP).

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 29 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
- After configuration changes relating to IKE/IPsec are made on the TOE, the user should restart the IKE key-management process using the command:

*restart ike-key-management*

This will ensure that the configuration parameters are available for immediate use.

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 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 OS 19.2R1-S2 for SRX5400, SRX5600 and SRX5800 appliances

Description	Version
Evaluation scheme	Australasian Information Security Evaluation Program
TOE	OS 19.2R1-S2 for SRX5400, SRX5600 and SRX5800
Software version	19.2R1-S2
Hardware platforms	SRX5400, SRX5600 and SRX5800 appliances
Security Target	<i>Security Target Junos OS 19.2R1-S2 for SRX5400, SRX5600 and SRX5800 Series, Version 1.1, 20-Apr-20</i>
Evaluation Technical Report	<i>Evaluation Technical Report v1.0, dated 29 April 2020</i> Document reference EFT-T011-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

collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 2.0+Errata 20180314, dated 14 March 2018

collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for VPN Gateway, version 2.1, dated 08 March 2017

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, dated 15 June 2017.

---

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 19.2R1-S2 Services Gateway appliances:

- SRX5400
- SRX5600
- 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.

All the SRX Services Gateway appliance models run the same Juniper Networks Junos operating system (Junos OS), Junos OS 19.2R1-S2.

The appliances are physically self-contained, housing the software, firmware and hardware necessary to perform all router functions. The hardware has two components: the Services Gateway appliance itself and various PIC/PIMs, which allow the appliances to communicate with the different types of networks that may be required within the environment where the Services Gateway appliances are used.

## 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 19.2R1-S2 firmware running on the appliance chassis listed in the table below. The TOE is contained within the physical boundary of the specified appliance chassis.

Chassis Model	Network Ports	Firmware (Operating System)
SRX5400	Four card cage slots: <ul style="list-style-type: none"> <li>• Slot 0: SCB</li> <li>• Slot1/0: SPC or MPC</li> </ul>	Junos OS 19.2R1-S2

- Slot 1: SPC or MPC

- Slot 2: SPC or MPC

SPC contains 2 SPUs

MPC contains two MIC slots

SRX5600	<p>Eight card cage slots:</p> <ul style="list-style-type: none"> <li>• Slots 0 &amp; 1: SCB</li> <li>• Slots 0 - 5: SPC or MPC or IOC or Flex IOC</li> </ul> <p>SPC contains 2 SPUs</p> <p>MPC contains two MIC slots IOCs have fixed interfaces</p> <ul style="list-style-type: none"> <li>• Flex IOC</li> </ul>	Junos OS 19.2R1-S2
SRX5800	<p>Fourteen card cage slots:</p> <ul style="list-style-type: none"> <li>• Slot 0: SPC or IOC/Flex IOC/ MPC</li> <li>• Slots 1-5: SPC or IOC/Flex IOC/ MPC or IOC3</li> <li>• Slots 0 &amp; 1: SCB or IOC3</li> <li>• Slots 2/6-10: SBC or SPC or IOC/Flex IOC/ MPC or IOC3</li> <li>• Slot 11: SPC or IOC/Flex IOC/ MPC</li> </ul>	Junos OS 19.2R1-S2

**Abbreviations:**

PIC – Physical Interface Card

PIM – Physical Interface Module

SCB – System Control Board

SPC – Services Processing Card

MPC – Modular Port Concentrator

SPU – Services Processing Unit

MIC – Modular Interface Card

IOC – Input Output Cards

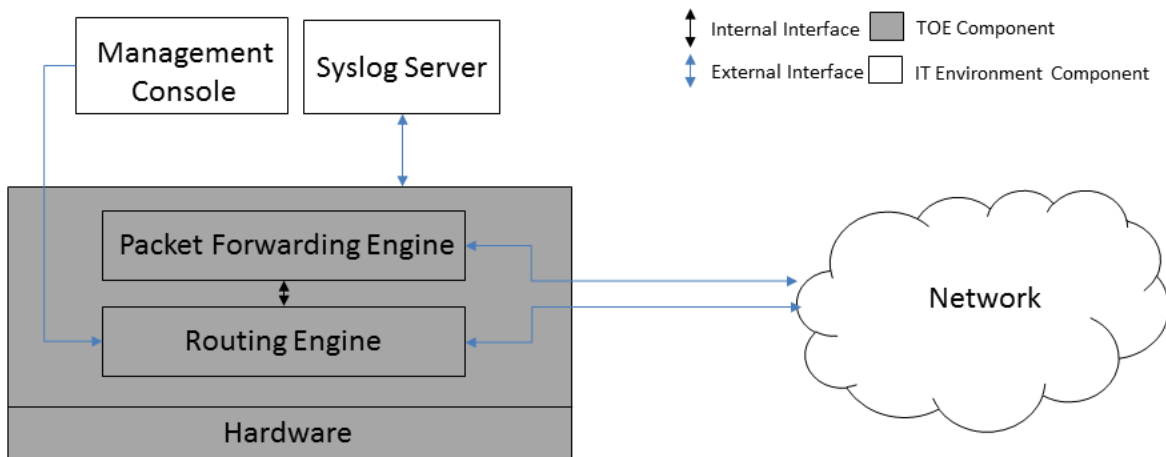
IOC3 – Input Output Card 3rd generation

ASIC – Application Specific Integrated Circuit



The physical boundary of the TOE is the entire chassis of the Services Gateway appliance, and includes both the hardware and firmware of the network device. The TOE is the Junos OS 19.2R1-S2 firmware running on the appliance chassis listed in the table above. This includes the firmware implementing the Routing Engine and the ASICs implementing the Packet Forwarding Engine. Hence the TOE is contained within the physical boundary of the specified appliance chassis. The install package for all SRX5xxx appliances is identical, namely junos-install-srx5000-x86-64-19.2R1-S2.tgz.

This physical boundary is shown in the 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 Guide for SRX5400, SRX5600 and SRX5800 Series Devices, Release 19.2R1-S2, Date 2019-12-01* [7]

## 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.

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 Services Gateway appliances support numerous routing standards for flexibility and scalability as well as IETF IPsec protocols. These functions can all be managed through the Junos firmware, either from a connected terminal console or via a network connection. Network management can be secured using IPsec and SSH protocols. All management, whether from a user connecting to a terminal or from the network, requires successful authentication. In the evaluated deployment Network management is secured using the SSH protocol, which can be tunnelled over IPsec.

The TOE supports intrusion detection and prevention functionality, which allows it to detect and react to potential attacks in real time. The detection component of the IPS can be based on attack signatures which specify the characteristics of the potentially malicious traffic based on a variety of packet headers payload data attributes. Anomaly detection based on deviation of the monitored traffic from expected values is also supported.

Services Gateway appliances accomplish routing through a process called a Virtual Router (VR). A security device divides its routing component into two or more VRs with each VR maintaining its own list of known networks in the form of a routing table, routing logic, and associated security zones.

## 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 Profiles 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 SRX5400, SRX5600 and SRX5800 series models require SFPs/PIMs/SPCs/IOCs/MPCs/SCBs/RE to operate and communicate with the connected network. These are detailed for each TOE appliance in Section 10 of the Security Target [8].

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
- IPsec peer.

### 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 Guide for SRX5400, SRX5600 and SRX5800 Series Devices, Release 19.2R1-S2, Date 2019-12-01* [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 Guide for SRX5400, SRX5600 and SRX5800 Series Devices, Release 19.2R1-S2, Date 2019-12-01*
- *Junos OS Intrusion Detection and Prevention Feature Guide for Security Devices, 13-Oct-19*
- *Junos OS VPN Feature Guide for Security Devices, 01-Oct-19*
- *Junos OS CLI User Guide, 25-Sep-19*
- *Junos OS Installation and Upgrade Guide, 05-Aug-19*
- *Junos OS Routing Policies, Firewall Filters, and Traffic Policers Feature Guide, 11-Oct-19*

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.
- 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 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. 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 security vulnerabilities.
- The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
- The assumptions A.RESIDUAL\_INFORMATION and A.NO\_THRU\_TRAFFIC\_PROTECTION defined in NDcPP are not relevant to this TOE as they are addressed by additional requirements introduced through conformance to FWcPP.
- The following assumption A.CONNECTIONS is introduced through compliance to [VPN\_EP] and [IPS\_EP]. It is typically understood that an ST claiming exact compliance to a Protection Profile cannot introduce assumptions. However, that is on the understanding this limits applicability of the security functional requirements for the TOE, whereas this assumption is a clarification of how the manner in which the TOE is to be connected to distinct networks.
- 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.

# 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 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].

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 Profiles [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 Profiles 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 Profiles 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 Profiles. More details can be found in the Protection profiles and their supporting documents.

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 Profiles that covers the technology area of network devices. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile 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 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 Profiles (PPs). PPs provide 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 [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 19.2R1-S2 for SRX5400, SRX5600 and SRX5800 appliances 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
- After configuration changes relating to IKE/IPsec are made on the TOE, the user should restart the IKE key-management process using the command:

**restart i ke- key- management**

This will ensure that the configuration parameters are available for immediate use.

# 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 (NDcPP), Version 2.1, 24 September 2018*
  - b) *collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 2.0+Errata 20180314, dated 14 March 2018*
  - c) *collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for VPN Gateway, version 2.1, dated 08 March 2017 (VPN EP)*
  - d) *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, dated 15 June 2017 (IPS EP).*
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 Guide for SRX5400, SRX5600, and SRX5800 Series Devices, Release 19.2R1-S2, Date 2019-12-01*
  - *Junos OS Intrusion Detection and Prevention Feature Guide for Security Devices, 13-Oct-19*
  - *Junos OS VPN Feature Guide for Security Devices, 01-Oct-19*
  - *Junos OS CLI User Guide, 25-Sep-19*
  - *Junos OS Installation and Upgrade Guide, 05-Aug-19*
  - *Junos OS Routing Policies, Firewall Filters, and Traffic Policers Feature Guide, 11-Oct-19*
8. *Security Target Junos OS 19.2R1-S2 for SRX5400, SRX5600 and SRX5800 Series, Version 1.1, 20-Apr-20*
9. *Evaluation Technical Report - Junos OS 19.2R1-S2 for SRX5400, SRX5600 and SRX5800 Series v1.0, dated 29 April 2020 (Document reference EFT-T011-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](https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf)*
12. *Seeding of the Kernel RBG in SRX5K Appliances running Junos 19.2R1-S2, Version 1.0, 26-Nov-19.*

## 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
FWcPP	CCRA-approved collaborative Protection Profile for Stateful Traffic Filter Firewalls
VPNEP	Virtual Private network (Gateway) Extended package
IPSEP	Intrusion Prevention Systems Extended package
TOE	Target of Evaluation