



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre

Australian Information Security Evaluation Program

Certification Report

Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1

Version 1.0, 14 August 2026

Document reference: AISEP-CC-CR-2026-EFT-T065-CR-v1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary	1
Introduction	2
Overview	2
Purpose	2
Identification	2
Target of Evaluation	4
Overview	4
Description of the TOE	4
TOE Functionality	5
TOE Physical Boundary	5
Architecture	6
Clarification of Scope	8
Security Policy	9
Secure Delivery	9
Version Verification	10
Documentation and Guidance	10
Secure Usage	10
Evaluation	12
Overview	12
Evaluation Procedures	12
Functional Testing	12
Entropy Testing	12
Penetration Testing	12
Certification	14
Overview	14
Assurance	14
Certification Result	14

Recommendations	14
Annex – References and Abbreviations	16
References	16
Abbreviations	17

Executive Summary

This report describes the findings of the IT security evaluation of Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1 appliances against Common Criteria approved *Protection Profiles (PPs)*.

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

- *Collaborative Protection Profile for Network Devices, Version, 3.0e, 06 December 2023 (CPP_ND_V3.0E)*
- *PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (MOD_VPNGW_v1.3)*
- *PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E)*
- *PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS_V1.0)*
- *Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (PKG_SSH_V1.0).*

Additionally, the above PPs can be grouped together using a certified PP-Configuration. This evaluation used the following *PP-Configuration [4]*:

- *PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 2.0, 25 April 2024 (CFG_NDcPP-IPS-FW-VPNGW_V2.0).*

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs with the final Evaluation Technical Report (ETR) submitted on 24 July 2026.

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

- Potential users 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
- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- The system auditor should review the audit trail generated and exported by the TOE periodically
- Security administrators should ensure that an IDP security licence and package is installed and kept up to date to correctly use and enforce [MOD_IPS_v1.0] requirements for the following platforms: SRX4700
- Security administrators shall follow the hardening and configuration instructions described in the *guidance [6]* to mitigate any security relevant issues associated with the TOE.

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

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

Introduction

Overview

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

Purpose

The purpose of this Certification Report is to:

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

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

Identification

The TOE is Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1
Software version	Junos OS 25.2R1
Hardware platforms	SRX4700, SRX4120 and SRX2300
Security Target	Security Target Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1, Version 1.0, 18 July 2026
Evaluation Technical Report	Evaluation Technical Report 1.0, Dated 24 July 2026 Document reference EFT-T065-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, Version 3.0e, 06 December 2023 (CPP_ND_V3.0E) ▪ PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (MOD_VPNGW_v1.3) ▪ PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E) ▪ PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS_V1.0) ▪ Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (PKG_SSH_V1.0) ▪ PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 2.0, 25 April 2024 (CFG_NDcPP-IPS-FW-VPNGW_V2.0).
-------------	---

Developer	HPE Juniper Networking 1133 Innovation Way Sunnyvale 94089 CA USA
-----------	--

Evaluation facility	Teron Labs Level 2, 14 Moore St Canberra ACT 2601 Australia
---------------------	--

Target of Evaluation

Overview

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

Description of the TOE

The TOE is a non-virtual and non-distributed network device with complex security functionality. It is a suite of appliances meeting the security requirements stated in Base-PP, the Functional Package, and the PP-Modules. The TOE is a suite of Juniper Networks SRX-series Universal Routing Platforms illustrated in *Figure 1*. The TOE is an instance of the Juniper Networks portfolio of the software-defined networking (SDN)-enabled routing platforms.



SRX4700



SRX4120



SRX2300

Figure 1 – TOE Variants

The TOE is purpose-built to protect network environments and provide Internet Mix (IMIX) firewall with high throughput. The TOE incorporates multiple security services and networking functions for a non-virtual appliance. This allows the TOE to provide highly customizable threat protection, automation, and integration capabilities. Advanced security capabilities on the TOE are offered as high throughput Next-Generation Firewall (NGFW), an Intrusion Prevention System (IPS), and a high-speed IPsec Virtual Private Network (VPN) in the data centre, enterprise campus, and regional headquarters deployments with IMIX traffic patterns.

The TOE can operate in a single mode or in a Multinode High Availability (HA) Mode. In Multinode HA Mode, a pair of devices, called nodes, executing the same software, is connected and configured to operate like a single device to

provide high availability. The two nodes back up each other. The Active node is the primary device, and the other is the backup device. If the primary device fails, the secondary device takes over processing of traffic. The interconnection of the two nodes is protected with IPsec. The configuration of the nodes is with Netconf over SSH.

The TOE supports definition and enforcement of information flow policies among network nodes. Stateful inspection is applied on each packet that traverses the network. The TOE provides a central point of control to manage the network security policy. The network topology enforces that each information flow from one network node and subnetwork to another passes through an instance of the TOE. The TOE then controls the information flows between the nodes and subnetworks based on network node addresses, protocol, type of access requested, and services requested. The TOE ensures that each security-relevant activity is audited and that the TOE functions are protected from potential attacks. The TOE also provides tools to manage all security functions.

The TOE is composed of the chassis and the Junos OS Operating System. In concert, they implement the routing and management plane functions for a complete network appliance. The chassis variants are illustrated in *Figure 1*. The TOE implements all security functions required for controlling access to the management functions. The management functions of the TOE are only accessible to legitimate administrators through a Command Line Interface (CLI). No other means but the CLI are available for administering the TOE. The TOE may be managed locally or remotely. Remote management sessions are protected with Secure Shell (SSH).

The TOE implements a set of security functions and security mechanisms required for conformance with the *Base-PP [4.a]* enhanced with *VPN Gateway [4.b]*, *Stateful traffic filtering firewall [4.c]*, *Intrusion Prevention System (IPS) [4.d]* and *SSH [4.e]*.

TOE Functionality

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

TOE Physical Boundary

The physical boundary of the TOE includes all hardware and software parts and the security guidance of the TOE. The parts of the TOE included in the physical boundary are detailed in *Table 1* below:

Part of the TOE	Identification	Description
TOE Hardware	SRX4700, SRX4120 and SRX2300	The hardware platform and the casing of the TOE. Includes the processor, the memories, the physical ports, network cards, and the persistent storage.
TOE Software	Juniper Junos OS 25.2R1	The Junos OS included in the TOE is Juniper Junos OS 25.2R1. TOE software is distributed as an installation package. The following installation packages are used for different variants of the TOE: ▪ SRX4700: junos-vmhost-install-srxhe2-x86-64-25.2R1.9.tgz

- **SRX4120:** junos-vmhost-install-srxmr2-x86-64-25.2R1.9.tgz
- **SRX2300:** junos-vmhost-install-srxmr2-x86-64-25.2R1.9.tgz

Security Guidance	Juniper SRX4700, SRX4120, SRX2300 for Junos OS 25.2R1 Common Criteria Guidance Supplement	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.
-------------------	---	--

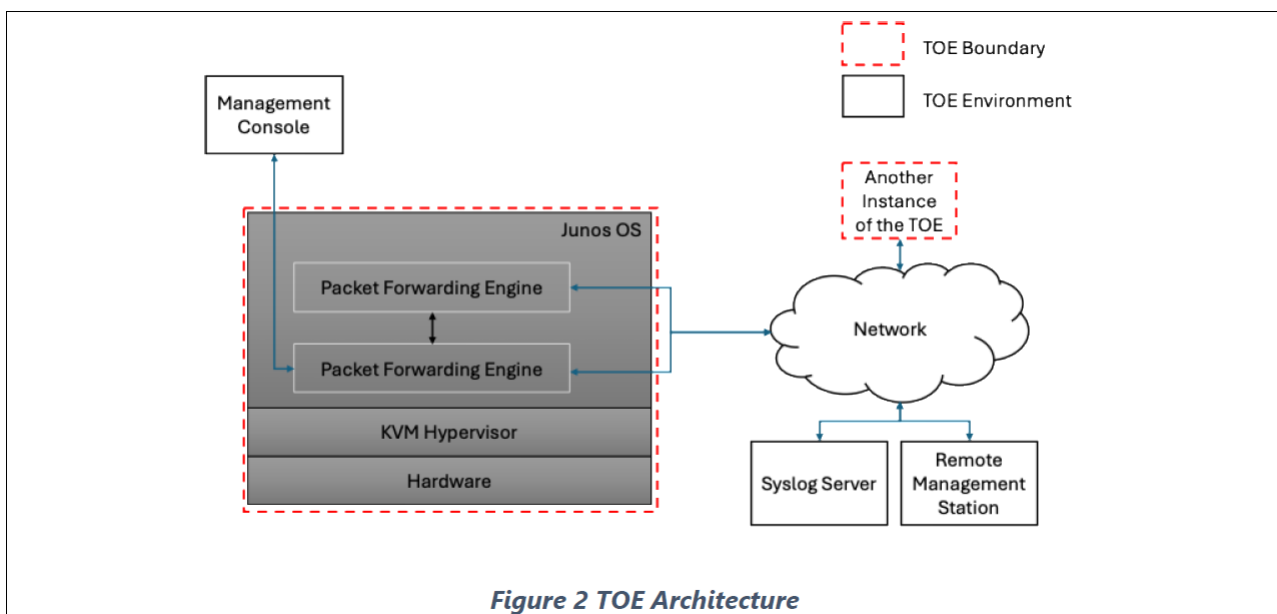
Table 1 - Parts Included in the Physical Scope of the TOE

Architecture

The variants of the TOE are a suite of network devices with an architecture illustrated in *Figure 2*. The TOE includes the chassis of the TOE. The Chassis implements the casing, the physical ports, and the hardware foundation for all those functions of the TOE which require hardware.

The KVM Hypervisor virtualizes the hardware for access by the software parts of the TOE. The software implements the routing engine and the packet forwarding engine of the TOE. Together, the two implement all routing plane and management plane functions of the TOE. Jointly, all software constitutes the Juniper Junos operating system.

The TOE is connected to the management console and to a syslog server. The management console may be local or remote. The TOE is also connected to the networks which it interconnects. Only the routing plane functions are implemented on the network traffic to and from the interconnected networks. All management plane functions are implemented on the devices connected to the dedicated management ports of the TOE.



The TOE implements the following distinct sets of interfaces:

- The operationally required interfaces, including power management, and the mechanical interfaces used for the cooling and ventilation of the TOE as well as the LEDs informing the user of the status of the TOE.
- Network interfaces used for connecting the TOE to the interconnected networks. Network interfaces are the interfaces for the ingress and egress network traffic. They are physically separate from all other network interfaces. The TOE implements the networking functionality for the network traffic to traverse through it.
- High Availability interfaces for the Multinode HA Mode.
- Management interfaces are used by the administrators to manage the TOE. Management interface is through dedicated network ports and may be accessed locally from console or remotely over SSH. The management interface implements a CLI which is the only means of administering the TOE.

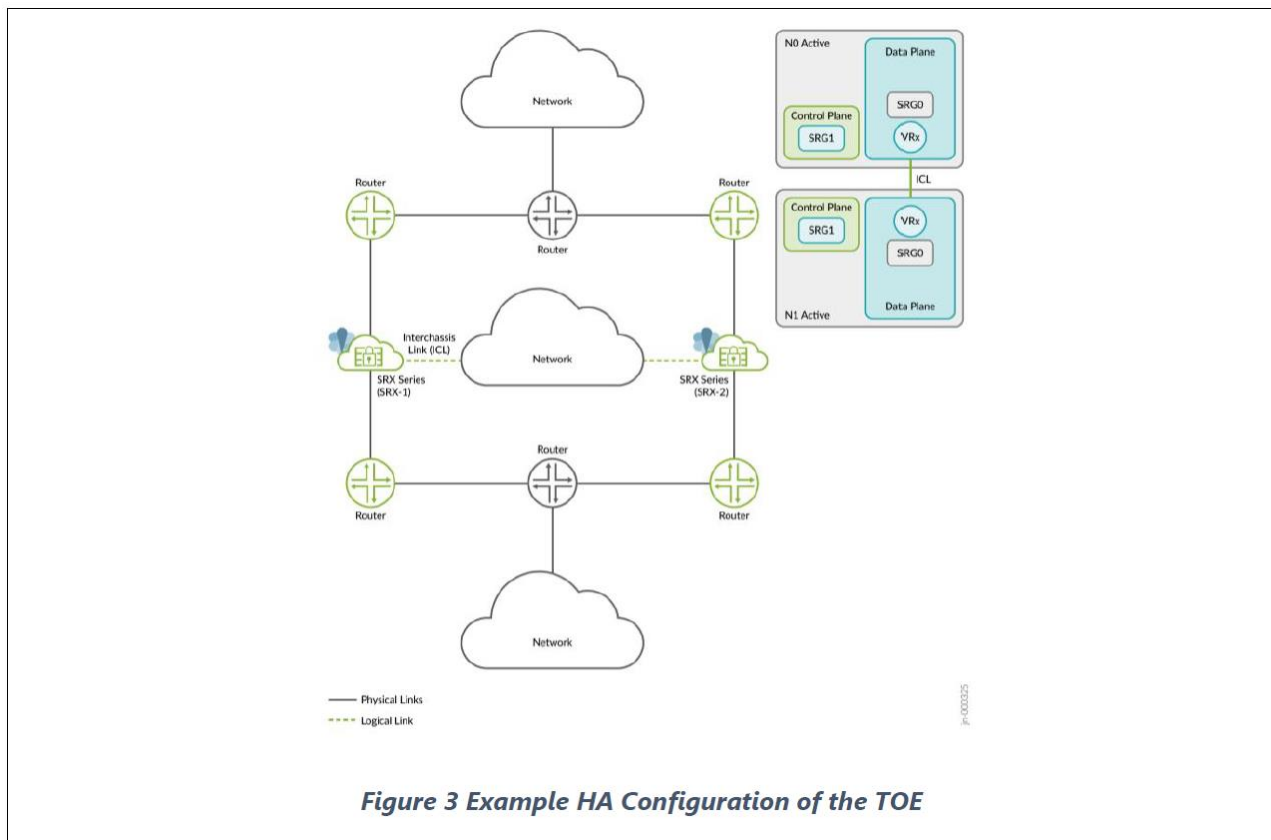
While offering identical functionality, the variants of the TOE offer different capabilities for different applications. The capabilities of different variants of the TOE are fully detailed in their datasheets given in *Table 2*.

TOE Variant	Datasheet URL
SRX4700	https://www.juniper.net/documentation/us/en/hardware/srx4700/index.html
SRX4120	https://www.juniper.net/documentation/us/en/hardware/srx4120/index.html
SRX2300	https://www.juniper.net/documentation/us/en/hardware/srx2300/index.html

Table 2 Hardware Capabilities of the Variants of the TOE

The TOE can set up the Multinode HA Mode for High Availability. Multinode HA Mode is common for both variants of the TOE. It supports two instances of the TOE presenting themselves as independent nodes to the rest of the network. The nodes are connected to adjacent infrastructure belonging to the same or different networks, all depending on the deployment mode. These nodes can either be collocated or separated across geographies. Participating nodes back up each other to ensure a fast synchronized failover in case of system or hardware failure.

Several models for network deployment of Multinode HA Mode are supported. Two instances of the TOE are connected through the vNICs mapped to the physical NICs of the platform. The connection is through an Interchassis Link (ICL) which connects the nodes over a routed part (instead of a dedicated Layer 2 network seen in some high availability implementations). The nodes are configured by the administrator of the TOE with Netconf over SSH. Once the nodes are configured, the ICL communication is protected with IPsec. An example configuration of the TOE in a Multinode HA Mode over the ICL is given in *Figure 3*.



Clarification of Scope

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

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

Evaluated Functionality

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

Non-TOE Hardware/Software/Firmware

The TOE is the entire network appliance. Yet, it does require external IT devices to operate properly. Specifically, the TOE requires the following items for operation:

- Network connectivity
- Syslog server including a SSHv2 client for connecting to the TOE for the TOE to send audit logs
- A management station with a SSHv2 client for remote administration of the TOE
- A Certification Authority to use in the validation of the X.509 public key certificates by the TOE
- NTP server for synchronizing TOE time when so configured

- A management station with a serial connection client for local administration of the TOE.

Non-evaluated Functionality and Services

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

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

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

- Telnet, FTP and SNMP are not considered secure. They violate the trusted path and trusted channel requirements and must not be used.
- SSL and TLS are not included in the certification and must not be used.
- The TOE must not be managed via J-Web, JUNOScript and JUNOScope. Neither is included in the certification. All administration of the TOE must be through the CLI.
- No user must be assigned super-user or FreeBSD root account privileges.

Security Policy

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

Secure Delivery

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

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

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

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

- Verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order

- When a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received and contains the following information:
 - Purchase order number
 - Juniper Networks order number used to track the shipment
 - Carrier tracking number used to track the shipment
 - List of items shipped including serial numbers
 - Address and contacts of both the supplier and the customer
- Verify that the shipment was initiated by Juniper Network, performing the following tasks:
 - compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received
 - Log on to the Juniper Networks online customer support portal at <https://www.juniper.net/customers/csc/management> to view the order status
 - Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

Installation of the TOE

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

Version Verification

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

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

Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. The evaluated configuration guide (System Admin Guide) document for the Juniper SRX4700, SRX4120, SRX2300 for Junos OS 25.2R1 is available for download at <https://www.juniper.net/documentation>. The title is:

- *Juniper SRX4700, SRX4120, SRX2300 for Junos OS 25.2R1 Common Criteria Guidance Supplement, version 1.0, 18 July 2026* [6].

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].

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

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

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

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

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

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

Evaluation

Overview

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

Evaluation Procedures

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

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

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

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

Functional Testing

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

Entropy Testing

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

Penetration Testing

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

- Type 1 - public vulnerabilities
- Type 2 - ND-ITC (Network international Technical Community) sourced
- Type 3 - evaluation team generated
- Type 4 - tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the **14 May 2026** coinciding with the conclusion of the evaluation. There was no identifiable Type 2 hypotheses for this evaluation.

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

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

Certification

Overview

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

Assurance

This certification is focused on the evaluation of product compliance with Protection Profiles that cover the technology area of network devices with added security functionality including stateful traffic firewall functions, VPN gateway functions, intrusion prevention functions and functional package for SSH. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the *PP Supporting Documents* [12] and Protection Profile Module 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.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the *Protection Profiles (PPs)* [4]. 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 *CPP_ND_V3.0E* [4.a], *MOD_VPNGW_v1.3* [4.b], *MOD_CPP_FW_V1.4E* [4.c], *MOD_IPS_V1* [4.d], *PKG_SSH_V1.0* [4.e] and *PP configuration for NDcPP, IPS, FW and VPNGW* [4.f].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the *Evaluation Technical Report* [7], the Australian Certification Authority **certifies** the evaluation of the Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1 performed by the Australian Information Security Evaluation Facility, Teron Labs.

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

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

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

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

- Potential users 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

- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- The system auditor should review the audit trail generated and exported by the TOE periodically
- Security administrators should ensure that an IDP security licence and package is installed and kept up to date to correctly use and enforce [MOD_IPS_v1.0] requirements for the following platforms: SRX4700
- Security administrators shall follow the hardening and configuration instructions described in the *guidance [6]* to mitigate any security relevant issues associated with the TOE.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5, CCMB-2017-04-001*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5, CCMB-2017-04-002*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003*
4. Protection Profiles:
 - a) *Collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (CPP_ND_V3.0E).*
 - b) *PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (MOD_VPNGW_v1.3)*
 - c) *PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E)*
 - d) *PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS_V1.0)*
 - e) *Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (PKG_SSH_V1.0)*
 - f) *PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 2.0, 25 April 2024 (CFG_NDcPP-IPS-FW-VPNGW_V2.0).*
5. *Australian Government Information Security Manual: <https://www.cyber.gov.au/ism>*
6. *Juniper SRX4700, SRX4120, SRX2300 for Junos OS 25.2R1 Common Criteria Guidance Supplement, version 1.0, 18 July 2026*
7. *Evaluation Technical Report Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1, Version 1.0, dated 24 July 2026 (Document reference EFT-T065-ETR 1.0)*
8. *Security Target Juniper SRX4700, SRX4120 and SRX2300 for Junos OS 25.2R1, Version 1.0, 18 July 2026*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
10. *AISEP Policy Manual (APM): https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf*
11. Entropy Documentation:
 - a) *Entropy Assessment Report (SRX2300 & SRX4120), Junos OS Physical Entropy Source – Intel Xeon D-10 Series (Ice Lake-D-10) Die with FCBGA2227 Package 1.0, version 1.0, 20 February 2025*
 - b) *Entropy Assessment Report (SRX4700), Junos OS 25.2 for HPE Juniper Networking SRX4700 Series Products, Version 1.0, 03 March 2026*
12. Protection Profile Supporting Documents
 - a) *Supporting Document, Evaluation Activities for Network Device cPP, Version 3.0e, 06 December 2023 (CPP_ND_V3.0E_SD)*

- b) *Supporting Document, Mandatory Technical Document, Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 +Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E_SD)*
- c) *Supporting Document, Mandatory Technical Document, PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (MOD_VPNGW_V1.3_SD)*
- d) *Supporting Document, Mandatory Technical Document, PP-Module for Intrusion Protection Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS_V1.0_SD)*

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

Abbreviations

AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
CLI	Command Line Interface
Gbps	Gigabits per second
HA	High Availability
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMIX	Internet Mix
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPSEP	Intrusion Prevention Systems Extended Package
LED	Light-emitting diode
NAT	Network Address Translation
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
NDFW iTC	Network Device Fundamentals and Firewalls international Technical Community
Netconf	Network Configuration Protocol
NGFW	Next-Generation Firewall
NIC	Network Interface Card
Mbps	megabits per second

OS	Operating System
PFE	Packet Forwarding Engine
PP	Protection Profile
RE	Routing Engine
SDN	Software-Defined Networking
SPC	Services Processing Card
SPU	Services Processing Unit
SSH	Secure Shell
TLS	Transport Layer Security
TOE	Target of Evaluation
VPN	Virtual Private Network
WAN	Wide Area Network

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government

Australian Signals Directorate