Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper Junos OS 23.4R1 for SRX1600

Version 1.0 18 March 2025

Document reference: AISEP-CC-CR-2025-EFT-T046-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary

This report describes the findings of the IT security evaluation of Juniper Junos OS 23.4R1 for SRX1600 appliance against Common Criteria approved Protection Profile (PP).

The TOE is an appliance that enforces information flow policies among network nodes. It is a purpose built platform that does not provide any general-purpose computing capabilities.

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

- collaborative Protection Profile for Network Devices Version: 2.2e, Date: 23-March-2020 (CPP_ND_V2.2E)
- PP-Module for VPN Gateways, Version: 1.3, 2023-08-16 (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, 2021-05-11 (MOD_IPS_V1.0).

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: 1.2, 2023-08-18 (CFG_NDcPP-IPS-FW-VPNGW_V1.2).

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) [8] submitted on 17 February 2025.

With regard to the secure operation of the TOE, the Australian 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
- 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 Juniper website
- the system auditor should review the audit trail generated and exported by the TOE periodically.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

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

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refers 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 [7] 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 Junos OS 23.4R1 for SRX1600.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Juniper Junos OS 23.4R1 for SRX1600
Software version	23.4R1
Hardware platforms	SRX1600
Security Target	Security Target Juniper Junos OS 23.4R1 for SRX1600 , Version 1.0.1, 12 March 2025
Evaluation Technical Report	Evaluation Technical Report - Junos OS 23.4R1 for SRX1600, Version 1.3, 17 February 2025 Document reference EFT-T046-ETR 1.3
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: 2.2e, Date: 23-March-2020 (CPP_ND_V2.2E) PP-Module for VPN Gateways, Version: 1.3, 2023-08-16 (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, 2021-05-11 (MOD_IPS_V1.0)
Developer	Juniper Networks
Evaluation facility	Teron Labs Unit 3, 10 Geils Court Deakin 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 TOE is the Juniper Networks SRX1600 Universal Routing Platform. The device is non-virtual and non-distributed, with no other variants. The TOE is an instance of the Juniper Networks portfolio of the software-defined networking (SDN)-enabled routing platforms.

The TOE provides security in a compact, scalable 1U form factor purpose-built to protect network environments. It provides Internet Mix (IMIX) firewall throughput of up to 12 Gbps, incorporates multiple security services and networking functions on top of the Junos OS. This allows the TOE to provide customisable threat protection, automation, and integration capabilities. The SRX1600 offers 19 Gbps of Next-Generation Firewall (NGFW), 19 Gbps of Intrusion Prevention System (IPS), and up to 8 Gbps of 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 are connected and configured to operate like a single device to provide high availability. When configured as a Multinode HA mode, the two nodes back up each other. The active node is the primary device and the other as the backup device, ensuring stateful failover of processes and services in the event of system or hardware failure. 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. The TOE implements stateful inspection of every packet that traverses the network and 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. Information flows are controlled 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 provides tools to manage all security functions.

The TOE implements multi-site VPN gateway and an Intrusion Prevention System (IPS). The IPS is capable of monitoring information flows to detect potential attacks based on pre-defined attack signature and anomaly characteristics in the traffic.

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 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) or IPsec.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.3 of the Security Target [7].

TOE Physical Boundary

The TOE is the complete appliance consisting of the Junos OS 23.4R1 firmware running on the SRX1600. The TOE is contained within the physical boundary of the SRX1600.

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 install image provided for the TOE is:

- junos-vmhost-install-srxmr2-x86-64-23.4R1.9.tgz

The scope of the TOE includes all hardware and software parts and the security guidance of the TOE as described in Table 1 below:

Part of the TOE	Identification	Description
Chassis	SRX1600	The hardware platform and the casing of the TOE. Includes the processor, the memories, and the persistent storage.
Junos OS	Junos OS 23.4R1	The Junos OS included in the TOE is Junos OS 23.4R1. The Junos OS includes the KVM Hypervisor.
Security Guidance	Junos OS Common Criteria Guide for SRX1600 Devices, Release 23.4R1, Pub. 2024-08-30	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.

Table 1

The physical boundary of the TOE is illustrated in Figure 1 below.

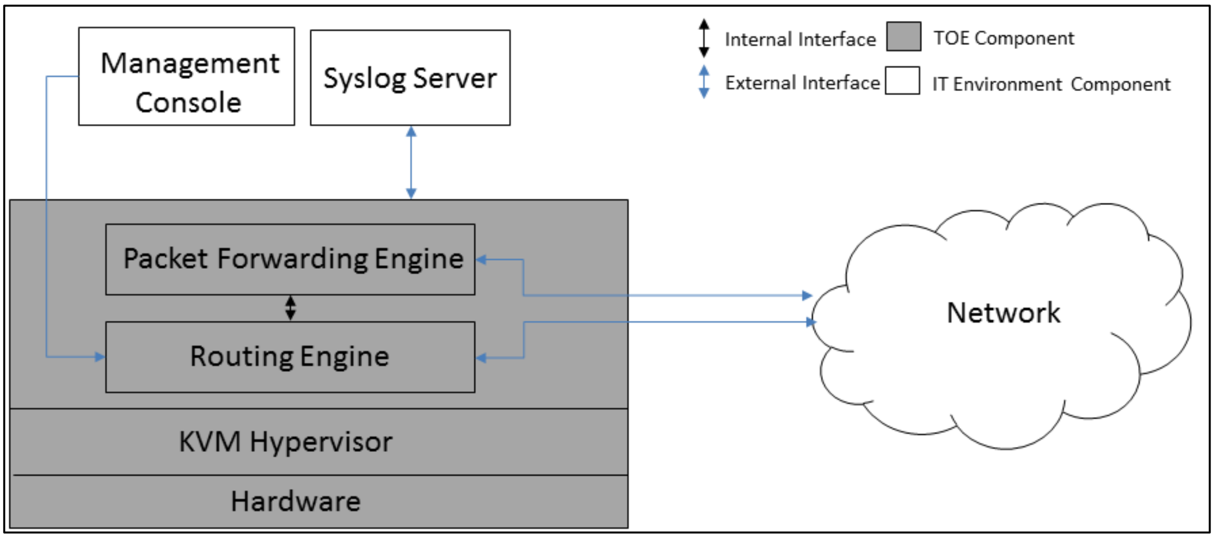

Figure 1

Architecture

The TOE consists of the following major architectural components:

- The Routing Engine is embedded in a Routing and Control Board (RCB) and performs all routing-process functions. Up to two RCB can be installed on the TOE for increased redundancy.

- The packet forwarding engine is incorporated in the TOE software to perform packet forwarding functions on top of hardware based link layer and routing engine capabilities

- 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. The software includes the Juniper Junos operating system. The distinct interfaces of the TOE include mechanical, defining the hardware used for cooling and ventilation, LEDs for user status of the TOE. Network interfaces for connecting the TOE to operational network environments. The interfaces ingress and egress traffic and physically separated from other network interfaces. The TOE enforces data processing of network traffic. Management interfaces for administrators to manage the TOE locally from console or remotely via a SSH connection.

- High Availability interfaces for the Multinode HA Mode configuration that supports two SRX Series Firewalls 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.

- The TOE implements a VPN gateway with IPsec. IPsec is used for protecting the state sharing between the Active Node and the Backup Node. when the TOE is configured in Multinode HA mode. IPsec may also be used for protecting the connection between the TOE and the remote management station. The VPN is implemented with IPsec.

- The administrator may configure the TOE to analyse IP-based network traffic forwarded to the TOE’s interfaces and detect violations of administrator defined IPS policies. The TOE is capable of a proactive response to terminate/interrupt an active potential threat and of a response in real time to interrupt a suspicious traffic flow. As the TOE is a standalone network device, the entire functionality of the IPS is contained within the standalone TOE.

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 [7].

Evaluated Functionality

Functional tests performed during the evaluation were taken from the Protection Profiles and Supporting Documents 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; however, it does require external IT devices to be properly operated. Specifically, the TOE requires the following items in the network environment:

- 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
- High Availability peer when in Multinode HA Mode
- IPsec peer
- A management station with a serial connection client for local administration of the TOE.

Disallowed Protocols and Services

The following protocols and services must not be used in association with the TOE:

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

Security

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 [7] 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, 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.

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 *SRX1600 Devices* product running Junos OS 23.4R1 is available for download at https://www.juniper.net/documentation. The title is:

- *Junos OS Common Criteria Guide for SRX1600 Devices, Release 23.4R1, Pub. 2024-08-30* [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 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 administrator must ensure that there is no unauthorised access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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 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], the 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]. Accordingly, the entropy source **has met** Entropy Source Validation requirements under NIST Cryptographic Module Validation Program (CMVP). Each cryptographic function of the TOE is CAVP validated. The CAVP certificate references, organised by the applicable Security Functional Component, are given in the Security Target [7].

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the NDcPP Supporting Document [12.a] which follow a flaw hypothesis methodology. The MOD_FW [12.b], MOD_VPNGW [12.c], and MOD_IPS [12.d], do not explicitly impose additional vulnerability assessment requirements. 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 **29 October 2024** coinciding with the conclusion of the evaluation. There were no identifiable Type 2 hypotheses for this evaluation.

The evaluation team devised four tests to check a potential vulnerability within CSP datatypes protected by IPSEC, HA Nodes maintaining independency, and race conditions within the TOE's boot process. The evaluation team also conducted tool-generated vulnerability testing of the TOE as per the Supporting Document [12.a]

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 and intrusion prevention functions. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profiles 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 PP Supporting Documents 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 [7] and **has met** the requirements of the Protection Profiles NDcPP V2.2E, MOD_VPNGW_v1.3, MOD_CPP_FW_V1.4E, MOD_IPS_V1.0 [4].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [8], the Australian Certification Authority **certifies** the evaluation of the Juniper Junos OS 23.4R1 for SRX1600 appliance, performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [7] claim to have met the requirements of the PP-Configuration CFG_NDcPP-FW-VPNGW_V1.0 [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:

- 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
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the hash of any downloaded software, as present on the https://www.juniper.net website
- the system auditor should review the audit trail generated and exported by the TOE periodically.

Annex – 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 2.2E, 23 March 2020*

   b) *PP-Module for VPN Gateways (MOD_VPNGW), Version 1.3, 16 August 2023*

   c) *PP-Module for Stateful Traffic Filter Firewalls (MOD_CPP_FW_V1.4E), Version 1.4, 25 June 2020*

   d) *PP Module for Intrusion Prevention Systems (IPS), Version 1.0, 11 May 2021*

   e) *PP-Configuration for Network Device, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways (CFGG_NDcPP-IPS-FW-VPNGW_V1.2, 18 August 2023*

5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism

6. Guidance documentation:

   a) *Junos OS Common Criteria Guide for SRX1600 Devices, Release 23.4R1, Pub. 2024-08-30*

7. *Security Target JuniperJunos OS 23.4R1 for SRX1600, Version 1.0.1, 12 March 2025*

8. *Evaluation Technical Report - Junos OS 23.4R1 for SRX1600 dated 17 February 2025* (Document reference EFT-T046-ETR 1.3)

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/2019-03/AISEP_Policy_Manual.pdf

11. Entropy Documentation:

    a) *Entropy Assessment Report, 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 2024 (Document Reference ESV-E008-EAR 1.0)*

12. Protection Profile Supporting Documents

    a) *Supporting Document, Evaluation Activities for Network Device cPP, December 2019, version 2.2 (NDcPP-SD)*

    b) *Supporting Document, PP-Module for VPN Gateways, 16 August 2023, version 1.3 (VPNGW-SD)*

    c) *Supporting Document, Evaluation Activities for Stateful traffic Filter Firewalls PP-Module, June 2020, version 1.4 (MOD_CPP_FW_V1.4E-SD)*

    d) *Supporting Document, PP-Module for Intrusion Prevention Systems (IPS), 11 May 2021, version 1.0 (MOD_IPS-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
CAVP	Cryptographic Algorithm Validation Program
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
FTP	File Transfer Protocol
FW	Firewall
HA	High Availability
IKE	Internet Key Exchange
IMIX	Internet Mix
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IT	Information technology
LED	Light Emitting Diode
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
OS	Operating System
PDF	Portable Document File
PP	Protection Profile
SD	Supporting Document
SDN	Software-Defined Networking
SNMP	Simple Network Management Protocol

SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
VPN	Virtual Private 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

Use of the Coat of 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