Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper SRX Series and vSRX for Junos OS 24.4R1

Version 1.0, 30 March 2026

Document reference: AISEP-CC-CR-2026-EFT-T057-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 SRX Series and vSRX for Junos OS 24.4R1 developed by Juniper Networks against Common Criteria approved *Protection Profiles (PPs).*

The Target of Evaluation (TOE) is a network device with a complex security functionality. There are two variants of the TOE. The SRX variant of the TOE is a network device which is neither a distributed nor a virtual network device. The vSRX variant of the TOE is a virtual, non-distributed software-only network device.

This report concludes that the TOE has complied with the following *PPs [4]:*

- *collaborative Protection Profile for Network Devices, Version: 3.0e, Date: 06 December 2023 (CPP_ND_V3.0E)*
- *Functional Package for Secure Shell (SSH) Version 1.0, 13 May 2021 (PKG_SSH_V1.0)*
- *PP-Module for Intrusion Prevention Systems (IPS) Version: 1.0, 11 May 2021 (MOD_IPS_v1.0)*
- *PP-Module for Stateful Traffic Filter Firewalls Version 1.4+Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E)*
- *PP-Module for VPN Gateways Version: 1.3, 16 August 2023 (MOD_VPNGW_v1.3)*

Additionally, the above PP and modules are grouped together using 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 20 February 2026.

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 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
- Security administrators should ensure that the correct firmware image is used according to what platform is used as follows:
    - vSRX: Junos OS 24.4R1-S3.7
    - All other platforms: Junos OS 24.4R1.9

- 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 platform:
    - SRX4300

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 [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 [9]* which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is the Juniper SRX Series and vSRX for Junos OS 24.4R1 by Juniper Networks, Inc.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Juniper SRX Series and vSRX for Junos OS 24.4R1
Software version	Junos OS 24.4R1
Hardware platforms	SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, and SRX5800

Security Target	Security Target Juniper SRX Series and vSRX for Junos OS 24.4R1, Version 1.0, 15 January 2026
Evaluation Technical Report	Evaluation Technical Report Juniper SRX Series and vSRX for Junos OS 24.4R1, Version 1.0, dated 20 February 2026 Document reference EFT-T057-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, 6 December 2023 (CPP_ND_V3.0E) Functional Package for SSH Version 1.0, 13 May 2021 (PKG_SSH_v1.0) PP-Module for Intrusion Protection Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS_v1.0) PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e, 25 June 2020 (MOD_CPP_ FW_v1.4e) PP-Module for VPN Gateways, Version 1.3 16 August 2023 (MOD_VPNGW_v1.3) PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network, version 2.0, 25 April 2024. (CFG_NDcPP-IPS-FW-VPNGW_V2.0)
Developer	Juniper Networks, Inc.
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 network device with a complex security functionality. There are two variants of the TOE:

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

- The vSRX variant of the TOE is a virtual, non-distributed network device. It is a software-only TOE intended to be executed on specific hardware platforms. When executed on an authorized hardware platform, the combination of the TOE and the platform is an appliance meeting the security requirements stated in Base-PP, the Functional Package, and the PP-Modules.

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 virtual or 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) and 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 are connected and configured to operate like a single device to provide high availability. Each device executes the same TOE software. When configured as a Multinode HA mode, the two nodes back up each other. The Active node is the primary device, and the other is the backup device, ensuring stateful failover of processes and services in the event of software 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. Stateful inspection is applied on each packet that traverses the network and 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. 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 also provides tools to manage all security functions.

The composition of the TOE depends on the variant of the TOE:

- The SRX variant of 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 vSRX variant of the TOE is composed of the Junos OS Operating System. The Chassis on which the operating system is executed is one of the authorized platforms. The operating system and the platform implement the routing and management plane functions for a complete network appliance.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.4 of the *Security Target [9].*

TOE Physical Boundary

The SRX Variants of the TOE include the TOE Hardware, TOE Software and TOE Security Guidance. The vSRX variants of the TOE include the TOE Software and TOE Security Guidance only.

The TOE Hardware on the SRX5000-Series models also includes the linecards. The linecards include the Service Processing Cards (SPC), Modular Port Concentrators (MPC), Interface Cards (IOC), the Switch Control Boards (SCB), and the Routing Engine (RE). They are common to each SRX5000-Series variant of the TOE unless otherwise stated in the identification of the part.

The parts of the TOE included in the physical boundary of the TOE for both variants are identified and described in the below table.

Part Of the TOE	Identification	Description
TOE Hardware (SRX Variants only)	SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, and SRX5800	The hardware platform and the casing of the TOE. Includes the processor, the memories, the physical ports, network cards, and the persistent storage.
Services Processing Cards	SRX5K-SPC3 Services Processing Card	Contains two Services Processing Units (SPUs), which provide the processing power to run integrated services such as firewall, IPsec, and Intrusion Detection and Prevention.
Module Port Concentrators and Interface Cards	SRX5K-MPC3-40G10G	Provides 10 Gigabit Ethernet and 40 Gigabit Ethernet ports, with a Packet Forwarding Engine that provides a 240 Gbps line rate.
	SRX5K-MPC3-100G10G	Provides 100 Gigabit Ethernet and 10 Gigabit Ethernet ports, with a Packet Forwarding Engine that provides a 240 Gbps line rate.
	SRX5K-IOC4-10G	Provides 10 Gigabit Ethernet ports, with at Packet Forwarding Engine that provides 400-Gbps line rate.
	SRX5K-IOC4-MRAT	Provides 10 Gigabit Ethernet, 40 Gigabit Ethernet and 100 Gigabit Ethernet ports, with a Packet Forwarding Engine that provides a 480 Gbps line rate.
	SRX5K-SCB3 Switch Control Board	Provides a Gigabit Ethernet switch that is connected to the embedded CPU complex on all components,

Switch Control Boards		Switch fabric to provide the switching functions for the MPCs, and a slot for the Routing Engine.
	SRX5K-SCB4 Switch Control Board (SRX5600 and SRX5800 models only)	Provides improved fabric performance and bandwidth capabilities for high-capacity line cards, and a slot for the RE.
Routing Engine	SRX5K-RE3-128G	Software processes that run on the Routing Engine maintain the routing tables, manage the routing protocols used on the device, control the device interfaces, control some chassis components, and provide the interface for system management and user access to the device.
TOE Software	Juniper Junos OS 24.4R1 for SRX and vSRX	The Junos OS included in the TOE is Juniper Junos OS 24.4R1 for SRX and vSRX. The software for the SRX Variants includes the KVM Hypervisor. TOE software is distributed as an installation package. The following installation packages are used for different SRX variants of the TOE: ▪ SRX1500: junos-srxentedge-x86-64-24.4R1.9.tgz ▪ SRX1600, SRX2300 and SRX4300: junos-vmhost-install-srxmr2-x86-64-24.4R1.9.tgz ▪ SRX4100 and SRX4200: junos-srxmr-x86-64-24.4R1.9.tgz ▪ SRX4600: junos-srxhe-x86-64-24.4R1.9.tgz ▪ SRX5400, SRX5600 and SRX5800: junos-vmhost-install-srx-x86-64-24.4R1.9.tgz The KVM Hypervisor included in the software distribution for the vSRX variants of the TOE is the following: ▪ Linux KVM on Ubuntu 22.04.3 TOE software for the vSRX variant does not include the KVM Hypervisor. The TOE Software for the vSRX variant is distributed as an install package and a deployment package: ▪ The install package is junos-install-vsrx3-x86-64-24.4R1-S3.7.tgz ▪ The deployment package is junos-vsrx3-x86-64-24.4R1-S3.7.qcow2

Security Guidance	Juniper SRX Series and vSRX for Junos OS 24.4R1 Common Criteria Guidance Supplement	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.

Architecture

SRX variant of the TOE architecture

The SRX variants of the TOE are a suite of network devices with an architecture illustrated in Figure 1. The TOE includes the hardware, i.e., 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. The software includes 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 SRX 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.

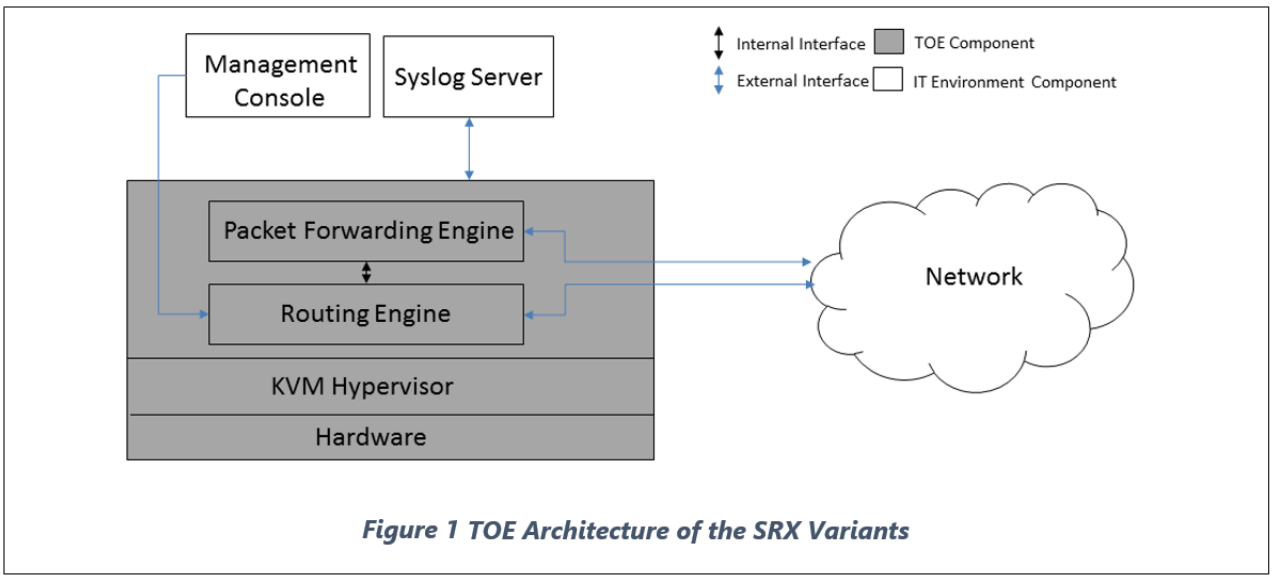

Figure 1 TOE Architecture of the SRX Variants

The TOE implements the following distinct sets of interfaces:

- The operationally required interfaces. These include the 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. They are the interfaces for the ingress and egress network traffic and 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 Configuration.
- 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 or IPsec. The management interface implements a CLI which is the only means of administering the TOE.

vSRX variant of the TOE architecture

The vSRX variant of the TOE is a virtual network device with an architecture illustrated in Figure 2. The vSRX TOE only includes the software of a complete appliance. The software must be executed on an authorized platform. The hypervisor is not part of the vSRX TOE. Only a single Virtual Machine (VM) created by the hypervisor may be used in the evaluated configuration.

The authorized platforms are the following:

- HPE ProLiant DL380 Gen10 Plus Smart Choice - Xeon Gold 6326 2.9 GHz

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 platform.

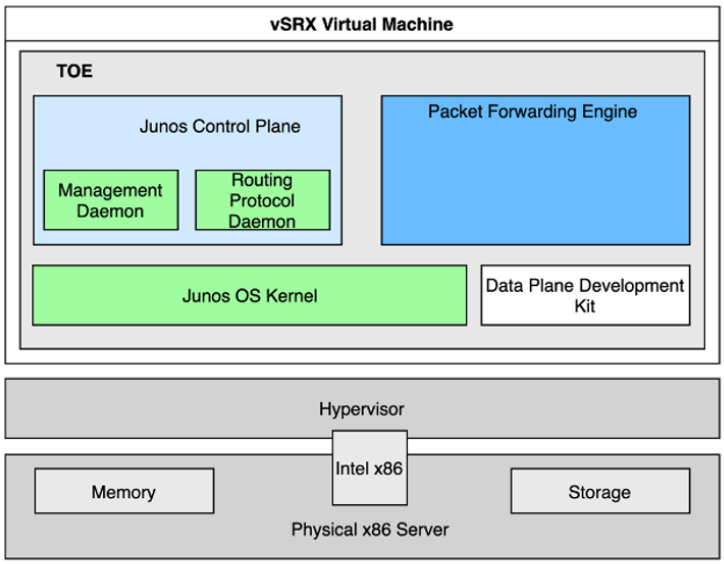

Figure 2 TOE Architecture of the vSRX Variants

The TOE is configured with virtual Network Interface Cards (vNIC). Connection of the TOE to the external devices is through the vNICs. Each vNIC is mapped to a different physical Network Interface Card (NIC) of the platform on which the TOE is executed. The platform must have at least the same number of physical NICs as there are vNICs configured to the TOE.

The TOE implements the following distinct sets of interfaces using the vNICs:

- Network interfaces used for connecting the TOE to the interconnected networks. They are the interfaces for the ingress and egress network traffic and 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 Configuration.
- 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 or IPsec. The management interface implements a CLI, which is the only means of administering the TOE.

The operationally required interfaces are implemented by the platform. These include the 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.

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 [9].*

Evaluated Functionality

Functional tests performed during the evaluation were taken from the *Protection Profiles [4]* and *Supporting Documents [13*] 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 requires external IT devices to be properly operated. Both variants of the TOE require the following items for operation:

- 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
- NTP server for synchronizing TOE time when so configured
- IPsec peer
- A management station with a serial connection client for local administration of the TOE.

Additionally, the vSRX variants of the TOE require the following:

- The chassis on which the TOE is executed. The chassis must be one of the authorized platforms.
- A hypervisor which implements the virtualization infrastructure on which the TOE runs on the chassis.

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:

- 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 and Transport Layer Security (TLS), 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 Junos root account.

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 [9]* 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 Guides [6] and [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. The evaluated configuration guides (System Admin Guide) document for the Juniper SRX Series and vSRX for Junos OS 24.4R1 is available for download at *https://www.juniper.net/documentation*. The title is:

- *Junos OS Common Criteria Guide for SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, and vSRX Devices, Release 24.4R1, 25 July 2025 [6]*
- *Junos® OS Common Criteria Guide for SRX5400, SRX5600, and SRX5800 Devices, Release 24.4R1, 25 July 2025 [7]*

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 [13].*

The evaluation was carried out in accordance with the operational procedures of the *Australian 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 [10]* and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs [14]* were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the *Protection Profiles [4]* and *Supporting Documents [13].* 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 separate *reports [12]*.

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the *NDcPP Supporting Document [13]* that follow a flaw hypothesis methodology. Accordingly, four types of flaw hypotheses have been considered:

- Type 1 - public vulnerabilities
- Type 2 - iTC (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 November 2025** 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 [13]*

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, Functional Package for SSH and intrusion prevention functions. 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 [1*3] 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. 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) [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 [9]* and **has met** the requirements of the *Protection Profiles CPP_ND_V3.0E [4.a], PKG_SSH_v1.0 [4.b], MOD_IPS_v1.0 [4.c], MOD_CPP_FW_v1.4e [4.d], MOD_VPNGW_v1.3 [4.e]* and *PP configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network, [4.f].*

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 SRX Series and vSRX for Junos OS 24.4R1 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the *Security Target [9]* 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:

- 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
- Security administrators should ensure that the correct firmware image is used according to what platform is used as follows:
  - vSRX: Junos OS 24.4R1-S3.7
  - All other platforms: Junos OS 24.4R1.9
- 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 platform:
  - SRX4300

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, version 3.0e, 06 December 2023 (CPP_ND_V3.0E)*

    b) *Functional Package for SSH Version 1.0, 13 May 2021 (PKG_SSH_v1.0)*

    c) *PP-Module for Intrusion Protection Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS_v1.0)*

    d) *PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e, 25 June 2020 (MOD_CPP_ FW_v1.4e)*

    e) *PP-Module for VPN Gateways, Version 1.3 16 August 2023 (MOD_VPNGW_v1.3)*

    f) *PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network, version 2.0, 25 April 2024*

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

6. *Junos OS Common Criteria Guide for SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, and vSRX Devices, Release 24.4R1, 24 February 2026.*

7. *Junos® OS Common Criteria Guide for SRX5400, SRX5600, and SRX5800 Devices, Release 24.4R1, 24 February 2026.*

8. *Evaluation Technical Report Juniper SRX Series and vSRX for Junos OS 24.4R1 Version 1.0, dated 20 February 2026* (Document reference EFT-T057-ETR 1.0)

9. *Security Target Juniper SRX Series and vSRX for Junos OS 24.4R1, Version 1.0, 15 January 2026.*

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/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf

12. 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, 20 February 2024 (SRX1600 &SRX2300)*
    b) *Entropy Assessment Report, Intel® Digital Random Number Generator SP800-90B Entropy Assessment Report for Intel® Xeon® CPUs Based on the Intel® Xeon® E5 v4 Processor Family and Intel® Core™ i7 (Formerly Broadwell EP) 10-Core Die with FCLGA2011 Package, Revision v12, May 2023 (SRX4100 & SRX4200)*
    c) *Entropy Assessment Report, Junos OS Physical Entropy Source – Intel Xeon D-22 Series (Ice Lake-D-22) Die with FCBGA2579 Package 1.0, 24 May 2024 (SRX4300)*

d) *Entropy Assessment Report, Junos OS Physical Entropy Source – Intel Xeon AWS-1000 v4 and E5 v4 (Broadwell EP) 15 Core Die with FCLGA2011 Package 1.0, 27 May 2024 (SRX4600)*
e) *Entropy Assessment Report, Junos OS Entropy Source version 24.4 Entropy Assessment and SP 800-90B Compliance Report, version 1.2, 14 May 2025 (SRX5400, SRX5600 & SRX5800)*
f) *Entropy Assessment Report, Junos OS Physical Entropy Source – Intel Xeon Silver, Gold, W Series (Ice Lake-28) with FCLGA4189 Package 1.0, 23 September 2025 (vSRX HPE server: HPE ProLiant DL380 Gen10 Plus Smart Choice - Intel Xeon Gold 6326)*
g) *Entropy Assessment Report, Entropy Source Analysis and Validation per SP 800-90B Requirements for Junos OS™ Kernel CPU Time Jitter RNG Version 3.4.1, version 1.0, 23 September 2025 (SRX1500)*

13. 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, PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (MOD_VPNGW_V1.3_SD)*

c) *Supporting Document Mandatory Technical Document, Evaluation Activities for Stateful Traffic Filter Firewalls, Version 1.4e, 25 June 2020, (MOD_CPP_FW_V1.4E_SD)*

d) *Supporting Document Mandatory Technical Document, PP-Module for Intrusion Prevention Systems (IPS), 11 May 2021, (MOD_IPS_V1.0_SD)*

14. *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
ASIC	Application Specific Integrated Circuit
CA	Certificate Authority
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
IOC	Interface Cards
IPsec	Internet Protocol Security
IPSEP	Intrusion Prevention Systems Extended Package
LED	Light-emitting diode
MPC	Modular Port Concentrators
NAT	Network Address Translation
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
NDFW iTC	Network Device Fundamentals and Firewalls international Technical Community
NIC	Network Interface Card
PFE	Packet Forwarding Engine
PIN	Personal Identification Number
PP	Protection Profile
RE	Routing Engine
SCB	Switch Control Boards
SDN	Software-Defined Networking

SPC	Services Processing Card
SPU	Services Processing Unit
SSH	Secure Shell
TLS	Transport Layer Security
TOE	Target of Evaluation
vNIC	virtual Network Interface Card
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.

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