Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500

Version 1.0, 26 September 2024

Document reference: AISEP-CC-CR-2024-EFT-T036-CR-V1.0
(Certification expires five years from certification report date)

cyber.gov.au

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Juniper Networks Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500 against Common Criteria approved Protection Profiles (PPs).

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, 23-March-2020 (CPP_ND_V2.2E)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25-June-2020 (MOD_CPP_FW_V1.4e)

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 23 August 2024.

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 https://www.juniper.net website
- the system auditor should review the audit trail generated and exported by the TOE periodically
- if data protection over the Router and Conductor instances is required, it will need to be secured by using external mechanisms (for example, either the link between Conductor and Router instances is physically protected, or logically protected via an out-of-band isolated network using a certified VPN solution).

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

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

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

Introduction

Overview

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

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria [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 SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500
Software version	v6.2.5-5r2
Hardware platforms	SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500
Security Target	Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500 version 2.1, 01 August 2024
Evaluation Technical Report	Evaluation Technical Report 1.0, dated 23 August 2024 Document reference EFT-T036-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 2.2e, 23-March-2020 (CPP_ND_V2.2E)

	PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25-June-2020 (MOD_CPP_FW_V1.4e)
Developer	Juniper Networks, Inc. 1133 Innovation Way, Sunnyvale California 94089 United States of America
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 Target of Evaluation (TOE) is the Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500, which are Session Smart Routing (SSR) appliances, allowing the development of agile, secure, and resilient applications and solutions with Wide Area Network (WAN) connections.

Each TOE variant includes the same software. Each variant may be provisioned and configured by the user to be a Session Smart Router (in short: Router) or a Session Smart Conductor (in short: Conductor). The TOE configured as a Router implements the data plane and control plane functions of the TOE and performs most functions. The TOE configured as a Conductor implements a centralized management and policy engine allowing provisioning and management of several Routers. A Conductor also acts as an information aggregation repository.

Each TOE configured as a Router may be administered individually. The Administrator connects to the TOE locally from console or remotely from a remote management station and issues commands to the TOE through a Command Line Interface (CLI). The remote connection is protected via SSH.

The TOE implements all security functions of a network device. It also implements a stateful traffic filtering firewall to guard access to the protected network. Instances of the TOE configured as Routers are deployed in various data centres, branches, and other facilities to protect the network connection. The Routers are associated to one or more instances of TOE configured as Conductors for information aggregation, life-cycle management, and configuration management. The Conductor may additionally be connected to other services to utilize the collected information.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.2 of the Security Target [8].

TOE physical boundary

The TOE for the Juniper Session Smart Routing (SSR) solution is a network device appliance that includes specific Juniper SSR hardware platforms and associated software. The TOE encompasses the physical hardware, the software running on these platforms, and the security guidance that governs their operation. The TOE excludes non-Juniper hardware, virtual platforms, and certain network security protocols and functionalities. The physical boundary of the TOE, defined by its hardware, software, and documentation, ensures a secure environment for network management and data protection. The hardware consists of various Juniper SSR platforms (SSR120, SSR130, SSR1200, SSR1300, SSR1400, and SSR1500), each with distinct CPU, microprocessor, and networking configurations. The software is standardised across these platforms, featuring Juniper SSR software version v6.2.5-5r2, delivered as an ISO package that includes Oracle Linux 7.9 operating system with kernel version 4.18.0, OpenSSL and OpenSSH.

The following table summarise the physical boundary of the TOE:

TOE Physical Boundary	Details
TOE Hardware	Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500
TOE Software	Juniper SSR software v6.2.5-5r2
TOE Security Guidance	Juniper SSR120, SSR130, SSR1200, SSR1300, SSR 1400 and SSR1500 Common Criteria Installation and User Guide v1.0

The TOE is contained within the physical boundary of the specified SSR platforms:

PLATFORM	CPU	MICROPROCESSOR	NETWORKING
SSR120	4-core Intel Atom	Denverton	2 x 1GbE combo RJ45/SFP 4 x 1GbE RJ45
SSR130	8-core Intel Atom	Denverton	2 x 1GbE combo RJ45/SFP 6 x 1GbE RJ45
SSR1200	8-core AMD	Snowy Owl	4 x 1/10 GbE SFP+ 8 x 1 GbE RJ45
SSR1300	16-core Intel Xeon	Cascade Lake	4 x 10 GbE SFP+ 4 x 1/10 GbE SFP+ 5 x 1 GbE RJ45
SSR1400	24-core Intel Xeon	Cascade Lake	4 x 10 GbE SFP+ 4 x 1/10 GbE SFP+ 5 x 1 GbE RJ45
SSR1500	64-core AMD	Milan	12 x 1/10/25 GbE SFP28 5 x 1 GbE RJ45

Architecture

Each instance of the TOE consists of the following major architectural components:

- The Session Smart Router (SSR) is the core component of the TOE responsible for handling both the data plane and control plane operations. It provides advanced routing services that include secure communication across Wide Area Networks (WANs), network address translation (NAT), and the encryption/decryption of data. The SSR is designed to optimize service-centric networking, ensuring that network traffic is efficiently managed and securely routed between connected systems. It implements a stateful traffic filtering firewall, providing robust protection against unauthorized access to the protected network. The Packet Forwarding Engine (PFE) provides all operations necessary for transit packet forwarding.
- The Session Smart Conductor (aka the Conductor) acts as a centralised management and policy engine within the TOE architecture. It enables the provisioning, configuration, and life-cycle management of multiple SSR instances. The Conductor also aggregates information from the SSRs, facilitating coordinated management and policy enforcement across the network. The Conductor communicates with the SSRs through a secure, dedicated out-of-band network, ensuring that management commands are reliably transmitted and executed.

The SSR and Conductor components operate independently but are closely integrated through secure communication channels. The Conductor manages the policies and configurations that the SSRs enforce, while the SSRs perform the real-time data routing and firewall functions necessary to protect the network. This architecture allows the TOE to scale efficiently, supporting complex and distributed network environments with high levels of security and performance.

All management operations within the TOE are conducted through a Command Line Interface (CLI), which can be accessed locally via a console or remotely through a Secure Shell (SSH) connection. SSH is used to secure remote management sessions, ensuring that all configuration and operational commands are transmitted securely. The TOE's architecture supports real-time monitoring and intrusion detection, allowing it to identify and respond to potential threats based on predefined attack signatures or anomaly detection methods.

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 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 relies on the provision of the following items in the network environment:

- Syslog server supporting SSHv2 connections to send audit logs
- SSHv2 client for remote administration
- serial connection client for local administration
- NTP Server is not part of the TOE
- Audit server is mandatory but not part of TOE

- Non-Juniper branded hardware platforms and Juniper branded hardware platforms not explicitly included in the physical scope of the TOE
- Security of the communication between the instances of TOE configured as Routers and Conductors
- Juniper SSR Software for virtual platforms
- Protocol (HTTPS/TLS, IPSec, SNMP, RADIUS) is not part of TOE
- X.509 certificate management, validation or verification is excluded to the TOE
- VPN, IPS functions and GUI and Juniper MIST are not part 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.

Please refer to the Security Target [8] for additional information on non-evaluated functions and services.

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. Hence, the Security Target [8] contains the functionality that is to be evaluated.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per model specific guidance instructions [6].

Secure delivery

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

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

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

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

- verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order
- when a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received and contains the following information:
  - purchase order number
  - Juniper Networks order number used to track the shipment
  - carrier tracking number used to track the shipment
  - list of items shipped including serial numbers
  - address and contacts of both the supplier and the customer
- verify that the shipment was initiated by Juniper Networks, by 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 document for the Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130,SSR1200, SSR1300, SSR1400 and SSR1500 is available for download at https://www.juniper.net/documentation. The title is:

- *SSR Common Criteria Installation and User Guide, Version v1.0, Date 6 June 2024* [6]

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org. [1, 2, 3, 9, 13].

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [5].

Secure usage

The evaluation of the TOE considered specific assumptions about its operational environment. These assumptions are essential to ensure that the security objectives of the TOE are achieved.

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.

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 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] and 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.a].

Penetration testing

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

- public vulnerabilities
- NDFW-iTC (Network international Technical Community) sourced
- evaluation team generated
- tool generated.

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. 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 activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profiles (PPs). PPs provide assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that Security Target, guidance documentation, and a basic description of the architecture of the TOE.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [8] and **has met** the requirements of the Protection Profiles NDcPP V2.2e [4.a] and MOD_CPP_FW_V1.4e [4.b].

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 SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [8] may claim to have met the requirements of the Network Device Protection Profile and Protection Profile Module for Stateful Traffic Filter Firewalls [4].

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
- if data protection over the Router and Conductor instances is required, it will need to be secured by using external mechanisms (for example, either the link between Conductor and Router instances is physically protected, or logically protected via an out-of-band isolated network using a certified VPN solution).

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. Protection Profiles:
    a) *collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23 March 2020 (CPP_ND_V2.2E)*
    b) *PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25-June-2020 (MOD_CPP_FW_V1.4e)*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. Guidance documentation: *SSR Common Criteria Installation and User Guide v1.0 dated 06 June 2024*
7. *Evaluation Technical Report - Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500 Version 1.0, dated 23 August 2024* (Document reference EFT-T036-ETR 1.0)
8. *Security Target for Juniper SSR Software v6.2.5-5r2 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400 and SSR1500 Version 2.1, dated 1 August 2024*
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. Description and analysis of TOE random bit generation
    a) *Entropy Report, Juniper SSR software v6.2.5-5r2 on Juniper SSR120,SSR130, SSR1200, SSR1300, SSR1400 and SSR1500, Version 1.0, dated 5 April 2024 (Document reference T036-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) *Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, June 2020, Version 1.4e (FW_MOD-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
ASIC	Application Specific Integrated Circuit
CCRA	Common Criteria Recognition Arrangement
CLI	Command Line Interface
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IPsec	Internet Protocol Security
MOD_CPP_FW	collaborative Protection Profile Module for Stateful Traffic Filter Firewalls
NAT	Network Address Translation
NDcPP	collaborative Protection Profile for Network Devices
NDFW iTC	Network Device Fundamentals and Firewalls international Technical Community
PFE	Packet Forwarding Engine
PP	Protection Profile
RE	Routing Engine
RJ-45	8-pin copper connection
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSR	Session Smart Router
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form factor Pluggable
TOE	Target of Evaluation
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Networks