Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms

Certification Report
2015/91

8 July 2015
Version 1.0

Amendment Record

Version	Date	Description
1.0	8 July 2015	Final

Executive Summary

This report describes the findings of the IT security evaluation of Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms. The TOE is a product that is designed to provide for the support of the definition and enforcement of information flow policies among network nodes. Routers provide for stateful packet inspection of every packet that traverses the network and provides centralised management functions to manage and administer the network security policy. All information flowing from one network node to another will pass through an instance of the TOE.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit –** JUNOS auditable events are stored in Syslog files, which can be sent securely to an external server
- **Cryptological Support –** baseline cryptological module is included to provide confidentiality and integrity services for authentication
- **User Data Protection –** TOE is designed to forward packets (i.e. “information flows”) to source and destination entries as provided by TOE users
- **Identification and Authentication –** TOE requires users to provide unique identification and authentication data before any administration access to the system is granted
- **Security Management –** TOE provides for an authorised Administrator role
- **Protection of the TSF –** TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords
- **TOE Access –** TOE can be configured to terminate inactive sessions
- **Trusted Path / Channels –** TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator
- **Stateful Traffic Filtering** (FWEP & VPNGWEP) – TOE provides stateful network traffic filtering and
- **Virtual Private Network** (VPNGWEP) – TOE provides virtual private network (VPN) gateway functions.

The report concludes that the product has complied with the Security Requirements for Network Devices, version 1.1 (NDPP), Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall version 1.0 (FWEP), and Network Device Protection Profile Extended Package VPN Gateway version 1.1 (VPNGWEP) and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Systems Applied Intelligence and was completed on 12 June 2015.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled

b) Configure and Operate the TOE according to the vendor's product administrator guidance

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved

d) The evaluators note that in the evaluated configuration, the TOE does not permit the "Neighbour Discovery Protocol". This behaviour is consistent with the SFR FFW_RUL_EXT.1.8 from FWEP. The TOE administrator must configure the local link addresses manually in both the TOE and neighbouring devices

e) The evaluators also recommend that the administrator verify the hash of the downloaded software, as present on the Juniper Website.

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.

Table of Contents

Chapter 1 – Introduction

1.1 Overview

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

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms against the requirements of the Common Criteria (CC), the NDPP v1.1, and FWEP v1.0; and VPNGWEP v 1.1

b) 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 (Ref 9) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms
Software Version	Junos FIPS Version 12.1 X46 D20.6
Hardware Platforms	SRX100, SRX110, SRX210, SRX220, SRX240, SRX550 and SRX650; LN1000, LN2600 (same CPU and crypto processor as SRX650); SRX5400, SRX5600 and SRX5800 with SPC-4-15-320
Security Target	Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms v1.9 June 10,

	2015
Evaluation Technical Report	Evaluation Technical Report JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms, dated 12 June 2015, Version 1.0, Document reference EFS-T039-ETR.
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Extended, July 2009, Version 3.1.Rev3
Methodology	Common Methodology for Information Technology Security
Conformance	NDPP v1.1 FWEP v1.0 VPNGWEP v1.1 Security Requirements for Network Devices Errata #2
Sponsor	Juniper Networks, Inc 1194 North Mathilda Avenue Sunnyvale CA 94089
Developer	Juniper Networks, Inc 1194 Mathilda Avenue Sunnyvale CA 94089
Evaluation Facility	BAE Systems Applied Intelligence Level 1 / 14 Childers Street Canberra ACT 2601 Australia

Chapter 2 – Target of Evaluation

2.1 Overview

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

2.2 Description of the TOE

The TOE is Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms developed by Juniper Networks Inc.

The TOE is a product that is designed to provide for the support of the definition and enforcement of information flow policies among network nodes. Routers provide for stateful packet inspection of every packet that traverses the network and provides centralised management functions to manage and administer the network security policy. All information flowing from one network node to another will pass through an instance of the TOE.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit –** JUNOS auditable events are stored in Syslog files, which can be sent securely to an external server
- **Cryptological Support –** baseline cryptological module is included to provide confidentiality and integrity services for authentication
- **User Data Protection / Information Flow Control –** TOE is designed to forward packets (i.e. "information flows") to source and destination entries as provided by TOE users
- **Identification and Authentication –** TOE requires users to provide unique identification and authentication data before any administration access to the system is granted
- **Security Management –** TOE provides for an authorised Administrator role
- **Protection of the TSF –** TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords
- **TOE Access –** TOE can be configured to terminate inactive sessions
- **Trusted Path / Channels –** TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator and
- **Stateful Traffic Filtering –** TOE provides stateful network traffic filtering. (FWEP & VPNGWEP)
- **Virtual Private Network** (VPNGWEP) – TOE provides virtual private network (VPN) gateway functions. Tunnel mode is facilitated.

2.3 TOE Functionality

Each Juniper Networks routing platform is a complete routing system that supports a variety of high-speed interfaces (up to 10 Gbps) for medium to large networks and network applications.

The TOE is a component of Juniper Networks routing platforms and provide components that manage and process authentication and authorisation claims across trusted organisational network boundaries and also across heterogeneous environments. The TOE provides the necessary infrastructure for implementing users from trusted partner organisations.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- The Routing Engine
- The Packet Forwarding Engine.

The Routing Engine (RE) runs the Junos software and provides Layer 3 routing and network management services, including the control of the flow of information through the TOE, applying Network Address Translation (NAT) where applicable and encryption/decryption operations of packets to provide for secure communication using the IPSec protocol.

The Packet Forwarding Engine (PFE) provides all operations necessary for transitory packet forwarding.

2.6 Clarification of Scope

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

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the JUNOS Secure Configuration Guide (Ref 8).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 9).

2.6.1 Evaluated Functionality

All tests performed during the evaluation were taken from NDPP (Ref 3), FWEP (Ref 4) and VPNGWEP (Ref 5) and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

2.6.2 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 Australian Government Information Security Manual (ISM) (Ref 6) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

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

- External Syslog server
- Use of telnet (note the use of telnet violates the Trusted Path Requirement Set)
- Use of file transfer protocol (FTP) (note the use of FTP violates the Trusted Path Requirement Set)
- Use of Simple Network Management Protocol (SNMP) (note the use of SNMP violates the Trusted Path Requirement Set)
- Management via “J-Web” (note the use of J-Web violates the Trusted Path Requirement Set)
- Use of media (other than the media required during the installation process)
- Network Address Translation (NAT)
- Virtual Routers
- SSL

2.7 Security

2.7.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref 9) contains a summary of the functionality to be evaluated:

- Security Audit
- Cryptographic Support
- User Data Protection / Information Flow Control
- Identification and Authentication – note that Telnet and FTP are considered to be out of scope
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel
- Stateful Traffic Filtering.
- VPN Gateway

2.8 Usage

2.8.1 Evaluated Configuration

The TOE consists of the Software version JUNOS 12.1 X46 D20.6. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the JUNOS Secure Configuration Guide (Ref 8).

2.8.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE:

- The shipping label should correctly identify the customer's name and address as well as the product
- The outside packaging should not appear to be tampered with so as to allow access to the contents, packing tape cut or the packaging resealed
- The inside packaging should be sealed and the seal itself should be intact
- Shipment of the device included a confirmation of the order number
- Verify that a shipment notification has been sent via email to the customer point of contact regarding the shipment of the order. The email should include details such as the purchase order number, Juniper Networks order number (which is used to track a shipment), list of items that have been shipped (including any serial numbers), and address/point of contact details for both the supplier and customer
- Verify that the shipment was initiated by Juniper Networks by comparison of shipment tracking numbers (Juniper's shipping notification email and tracking number of the package received)
- View/Check the delivery/shipment status of the order by logging into **https://www.juniper.net/customers/csc/management** and
- View/Check the carrier tracking number (or Juniper Networks order number) against the information provided to the customer by Juniper.

2.8.3 Installation of the TOE

The Configuration Guide (Ref 8) contains all relevant information for the secure configuration of the TOE. It should be noted that some well-known protocols are prevented from operating as per the FWEP (in particular the IPv6 Neighbourhood Discovery Protocol (NDP)). Network design should take this into account.

2.9 Version Verification

The verification of the TOE is largely automatic, including the verification using digital signatures. This was demonstrated during testing. The TOE cannot load a modified image. The software image can be downloaded from **https://juniper.net**.

2.10 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. All guidance material is available for download at **www.juniper.com.** All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.11 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.

No assumptions were noted in the testing documentation or the resultant reports.

Chapter 3 – Evaluation

3.1 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.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the NDPP (Ref 3), FWEP (Ref 4), VPNGWEP (Ref 5), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3, Parts 2 and 3 (Ref 1 and 2).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (Ref 19).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from JUNOS configuration guide (Ref 8).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the evaluators were taken from the NDPP, FWEP and VPNGWEP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile packages were exercised during testing.

3.3.2 Test phases

Testing is determined in the assurance activities in the Protection Profiles. The evaluation was conducted in two phases.

a) **Phase 1**: The TOE was in its default configuration. The first phase of testing was between 12 June 2014 and 24 June 2014.

b) **Phase 2**: The developer updated the TOE to resolve any possible vulnerability caused by the disclosure of CVE-2014-0160 (SSL HeartBleed). Retesting of the TOE was performed during 31 July 2014 to 30 September 2014.

Cryptographic Algorithm Validation Systems (CAVS) testing was completed on 10-Jun-2015

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 17).

3.5 Penetration Testing

The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

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

4.2 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of network devices. Agencies 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 security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles (PPs). PPs provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by testing as outlined in the NDPP, FWEP and VPNGWEP assurance activities, and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

4.3 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref 10) the Australasian Certification Authority **certifies** the evaluation of the Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms product performed by the Australasian Information Security Evaluation Facility, BAE Systems Applied Intelligence.

BAE Systems Applied Intelligence **has determined** that Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms uphold the claims made in the Security Target (Ref 9) and **has met** the requirements of NDPP, FWEP and VPNGWEP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles.

The analysis is supported by testing as outlined in the NDPP assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 6) and New Zealand Government users should consult the GCSB.

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled

b) Configure and operate the TOE according to the vendor’s product administrator guidance

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.

d) The evaluators note that in the evaluated configuration, the TOE does not permit the “Neighbour Discovery Protocol”. This behaviour is consistent with the SFR FFW_RUL_EXT.1.8 from FWEP. The TOE administrator must configure the local link addresses manually in both the TOE and neighbouring devices

e) The evaluators also recommend that the administrator verify the hash of the downloaded software, as present on the Juniper Website.

Annex A – References and Abbreviations

A.1 References

1. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009, Version 3.1 Revision 3

2. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009, Version 3.1 Revision 3

3. US Government approved Protection Profile – Protection Profile for Network Devices (NDPP) version 1.1 June 8, 2012

4. US Government approved Network Devices Protection Profile – Protection Profile Stateful Traffic Filter Firewall Extended Package (FWEP) Version 1.0 December 2011

5. US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 (VPNGWEP)

6. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

7. Test Report for JUNOS 12.1 X46 D20.6 for SRX and LN Platforms, version 0.2, 4 November 2014, Document reference EFS-T039-TR

8. Guidance Documentation:

    - Junos® Common Criteria Evaluated Configuration Guide for LN Series Rugged Secure Routers and SRX Series Security Devices 1 Release 12.1 X46-D20 2-June-2015

    - Annex for AGD – Juniper Networks SRX Series Service Gateways Running Junos 12.1X46-D20, Version 1.1, 08-Oct-14

    - Junos® OS CLI User Guide, Release 12.1X46, 07-Oct-13

    - Junos® OS Getting Started Guide for the Branch SRX Series, Release 12.1X46, 15-Nov-13

    - Junos® OS Installation and Upgrade Guide for Security Devices, Release 12.1X46, 18-Nov-13

9. Juniper: Security Target – Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms version 1.9 June 10, 2015

10. Evaluation Technical Report JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms, dated 12 June 2015, Version 1.0, Document reference EFS-T039-ETR.

11. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms AGD Workbook, EFS-T039-AGD-EWB version 1.0, 12 June 2015

12. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms AVA Workbook, EFS-T039-EWB-AVA 1.0 version 1.0, 12 June 2015,

13. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms ALC Workbook 1.0 EFS-T039-EWB-ALC version 1.0, 12 June 2015

14. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms ASE Workbook 1.0-EFS-T039-EWB-ASE version 1.0, 12 June 2015

15. JUNOS 12.1 X46 D20.6 for SRX and LN Series Platforms ATE Workbook 1.0 EFS-T039-EWB-ATE version 1.0, 12 June 2015

16. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

17. Seeding of the Kernel RBG in SRX Series Appliances Running Junos 12.1 version 1.10, June 10, 2015

18. NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2012.

19. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CAVS	Cryptographic Algorithm Validation System
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
IDM	IPS Device Manager
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy