Australian Government
Department of Defence

Australasian Information Security Evaluation Program

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

Certification Report
2015/90

3 July 2015
Version 1.0

Amendment Record

Version	Date	Description
1.0	3 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 Series against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX 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. The routers provide for stateful packet inspection of every packet that traverses the network and provides central 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. Information flow is controlled on the basis of network node addresses, protocol, type of access requested, and services requested. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited, that their own functions are protected from potential attacks, and provides the security tools to manage all of the security functions.

The report concludes that the product has complied with the Security Requirements for Network Devices (NDPP) Version 1.1, Security Requirements for Network Devices Errata #2, 13 January 2013, the Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0 (FWEP) 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 and was completed on 11 June 2015.

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

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) 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 TOE administrator should 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 Series Platforms against the requirements of the Common Criteria (CC), the NDPP v1.1 FWEP v1.0

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-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 Series Platforms
Software Version	JUNOS Version 12.1 X46 D20.6 for SRX Series Platforms
Hardware Platforms	SRX1400, SRX3400 and SRX3600; SRX5400, SRX5600 and SRX5800 with SPC-2-10-40
Security Target	Juniper Networks, Inc. JUNOS 12.1 X46 D20.6 for SRX-Series Platforms v1.11, 20 June 2015
Evaluation Technical Report	Evaluation Technical Report JUNOS 12.1 X46 D20.6 for SRX-Series Platforms, Version 1.0, dated 11 June 2015

Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Conformant, July 2009, Version 3.1, Rev 3
Methodology	Common Methodology for Information Technology Security , July 2009, Version 3.1, Revision 3
Conformance	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (NDPP) Security Requirements for Network Devices Errata #2, 13 January 2013 Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 (FWEP)
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, Civic, ACT 2601

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 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 as follows:

- **Security Audit:** JUNOS auditable events are stored in the syslog files, and can be sent to an external log server (via IPsec). Auditable events include start-up and shutdown of the audit functions, authentication events, service requests, as well as other event types. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). Local Syslog storage limits are configurable and are monitored. In the event of storage limits being reached the oldest logs will be overwritten.

- **Cryptographic Support:** The TOE includes a baseline cryptographic module that provides confidentiality and integrity services for authentication and for protecting communications with adjacent systems.

- **User Data Protection/Information Flow Control:** The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by the users or indirectly from other network entities (outside the TOE) configured by the users. The TOE has the capability to regulate the information flow across its interfaces; traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, the transport layer protocol, the source service identifier, and the destination service identifier (TCP or UDP port number).

- **Identification and Authentication:** The TOE requires the users to provide unique identification and authentication data before any administrative access to the system is granted. The devices also require that applications exchanging information with them successfully authenticate prior to any exchange.

- **Security Management:** The TOE provides an Administrator role that is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product, the regular review of all audit data and all administrative tasks (e.g., creating the security policy). The devices are managed through a Command Line Interface (CLI).

- **Protection of the TSF:** The TOE provides protection mechanisms for TSF data (e.g. cryptographic keys, administrator passwords). Another protection mechanism is to ensure the integrity of any software/firmware updates are can be verified prior to installation. The TOE provides for both cryptographic and non-cryptographic self-tests, and is capable of automated recovery from failure states. Also, reliable timestamps are made available by the TOE.

- **TOE Access:** The TOE can be configured to terminate interactive user sessions, and to present an access banner with warning messages prior to authentication.

- **Trusted Path/Channels:** The TOE creates trusted channels between itself and remote trusted authorized IT product (e.g. syslog server) entities that protect the confidentiality and integrity of communications. The TOE creates trusted paths between itself and remote administrators and users that protect the confidentiality and integrity of communications.

- **Stateful Traffic Filtering:** The TOE provides stateful network traffic filtering based on examination of network packets and the application of information flow rules.

2.3 TOE Functionality

Each Juniper Networks routing platform is a complete routing system that supports a variety of high-speed interfaces for medium/large networks and network applications. Juniper Networks routers share common JUNOS software, features, and technology for compatibility across platforms.

The routers are physically self-contained, housing the software, firmware and hardware necessary to perform all router functions. The hardware has two components: the router itself and various PIC/PIMs, which allow the routers to communicate with the different types of networks that may be required within the environment where the routers are used.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- The Routing Engine; and
- 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 Configuration Guide (Ref 11).

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 5) and the FWEP (Ref 6) and sufficiently demonstrate through exercise the security functionality of the TOE.

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 8) 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 items are out of the scope of the evaluation:

- External syslog server
- Use of telnet
- Use of FTP
- Use of SNMP
- Management via J-Web
- Media use (other than during installation of the TOE)
- Network Address Translation (NAT)
- Virtual Routers
- SSL

In addition, the Web Authentication Policy Enforcement's web interface was not included in testing and evaluation when the active vulnerability assessments were conducted.

2.7 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected.

Since the NDPP and FWEP do not require it, the TOE does not support any Security Functional Policy.

2.8 Secure Usage

2.8.1 Evaluated Configuration

This section describes the configuration of the TOE that was included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to the ISM (Ref 8) to ensure that the configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

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 Configuration Guide (Ref 11).

2.8.2 Delivery Procedures

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

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

If the customer identifies a problem during the inspection, he or she should immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

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

- Verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order.
- When a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received.
- Verify that the e-mail contains the following information:

- Purchase order number
- Juniper Networks order number used to track the shipment
- Carrier tracking number used to track the shipment
- List of items shipped including serial numbers
- Address and contacts of both the supplier and the customer

- Verify that the shipment was initiated by Juniper Networks. To verify that a shipment was initiated by Juniper Networks, you should perform the following tasks:

    - Compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received.

    - Log on to the Juniper Networks online customer support portal at https://www.juniper.net/customers/csc/management to view the order status.

    - Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

2.8.3 Installation of the TOE

The Configuration Guide (Ref 11) and Installation and Upgrade Guide (Ref 14) contain 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)).

The verification of the TOE is largely automatic, including the verification using MD5 hashes. This was demonstrated during testing. The TOE cannot load a modified image. The software image can be downloaded from **https://juniper.net**.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. Guidance and installation documentation (Refs 11 and 14) will be available to the consumer when the TOE is purchased.

All guidance material is also 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**.

2.10 Assumptions

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 5), FWEP (Ref 6), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3, Parts 2 and 3 (Refs 1 and 2).

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

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 (Ref 4) 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 11).

3.3 Testing

All tests performed by the evaluators were taken from the NDPP and FWEP. 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 SFR listed in the Security Target and the Protection Profile packages were exercised during testing.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 15).

3.5 Penetration Testing

A vulnerability analysis was performed on 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.

In addition, the documentation supplied as evidence for the evaluation of the TOE was analysed to identify possible vulnerabilities.

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 and FWEP 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.

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 Series Platforms product performed by the Australasian Information Security Evaluation Facility, BAE Systems.

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

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.

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 8) 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) 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 the FWEP. The TOE administrator must configure the local link addresses manually in both the TOE and neighbouring devices
e) The TOE administrator should 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. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3

4. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

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

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

7. Security Requirements for Network Devices Errata #2, 13 January 2013

8. 2014 Australian Government Information Security Manual (ISM), Defence Signals Directorate

9. Security Target - Juniper Networks, Inc. Junos 12.1 X46 D20.6 for SRX Series Platforms, version 1.11, 20 June 2015

10. Evaluation Technical Report - Juniper Networks Junos 12.1 X46 D20.6 for SRX Series Platforms EFS-T038-ETR Version 1.11, 11 June 2015

11. Junos® OS Common Criteria Evaluated Configuration Guide for LN Series Rugged Routers and SRX Series Security Devices, Release 12.1X46-D20, 10-Oct-14

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

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

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

15. Seeding of the Kernel DRBG in SRX Series Appliances Running Junos 12.1X46-D20, Version 1.9, 06-May-14

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CC	Common Criteria
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
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