Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Juniper Networks, Inc. JUNOS 15.1 X49-D60 for SRX platforms

Certification Report
2017/105

06-Feb-2017
Version 1.0

Amendment Record

Version	Date	Description
1.0	07-02-2017	External

Executive Summary

This report describes the findings of the IT security evaluation of Juniper Networks, Inc. Junos 15.1 X49-D60 for SRX platforms against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos 15.1 X49-D60 for SRX 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. Juniper Networks security devices accomplish routing through a process called a Virtual Router (VR). A security device divides its routing component into two or more VRs with each VR maintaining its own list of known networks in the form of a routing table, routing logic, and associated security zones.

The functionality defined in the Security Target that was subsequently evaluated is summarised 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 numerous other security events. 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.
- **Cryptological Support** – baseline cryptological module is included to provide confidentiality and integrity services for authentication. Tests for cryptological support were performed using the CAVS tool. The CMVP certificates are listed in the Security Target.
- **User Data Protection** – 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 TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users.
- **Information Flow** - 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 users to provide unique identification and authentication data before any administration 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 authorised 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
    - all other administrative tasks (e.g., creating the security policy) and
    - the devices are managed through a Command Line Interface (CLI). The CLI is accessible through remote administrative session.
- **Protection of the TSF** – The TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords. The TOE provides for both cryptographic and non-cryptographic self-tests and is capable of automated recovery from failure states. Also, reliable timestamp is made available by the TOE
- **TOE Access** – The TOE can be configured to terminate inactive sessions.
- **Trusted Path / Channels** – The TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator
- **Stateful Traffic Filtering** – The TOE provides stateful network traffic filtering based on examination of network packets and the application of information flow rules.
- **Virtual Private Networks** --The TOE provides Virtual Private Network (VPN) support, allowing site-to-site, hub-and spoke and remote access VPNs.
- **Intrusion Prevention -** The TOE can be configured to analyse IP-based network traffic forwarded to the TOE's interfaces, and detect violations of administratively-defined IPS policies. The TOE is capable of initiating a proactive response to terminate/interrupt an active potential threat, and to initiate a response in real time that would cause interruption of the suspicious traffic flow.

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), Network Device Protection Profile Extended Package VPN Gateway version 1.1 (VPNGWEP) and Network Device Protection Profile (NDPP) Extended Package for Intrusion Prevention Systems version 1.0 (IPSEP**)** 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 30 November 2016.

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 recommend that the administrator verify the hash of the downloaded software, as present on the Juniper Website.
e) Note in the evaluated configuration of the TOE, remote SSH connections to the TOE must be encapsulated within an IPSec tunnel.

This report includes information about 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.

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 15.1 X49-D60 for SRX Platforms against the requirements of the Common Criteria (CC), the NDPP v1.1, FWEP v1.0; and VPNGWEP v 1.1 and the IPSEP 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 1) 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 15.1 X49-D60 for SRX Platforms.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Juniper Networks, Inc. Junos 15.1 X49-D60 for SRX Platforms
Software Version	Junos 15.1 X49-D60
Hardware Platforms	SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX5400E,SRX5400X, SRX5600E,SRX5600X SRX5800E and SRX5800X
Security Target	Junos 15.1 X49-D60 for SRX Series Platforms. Version 1.0, dated 24 January 2017
Evaluation Technical Report	Evaluation Technical Report Junos 15.1 X49-D60 for SRX Series Platforms, Version 1.0, dated 27 January 2017

Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, September 2012, Version 3.1.Rev 4
Methodology	Common Methodology for Information Technology Security September 2012, Version 3.1.Rev 4
Conformance	NDPP v1.1 FWEP v1.0 VPNGWEP v1.1 IPSEPv1.0 Security Requirements for Network Devices Errata #3
Developer	Juniper networks Inc 1133 Innovation Way, Sunnyvale, California, 94089, United States
Evaluation Facility	BAE Systems Applied Intelligence Level 1, 14 Childers Street Canberra ACT 2600

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 Junos 15.1 X49-D60 for SRX 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.

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 TOE provides Virtual Private Network (VPN) support, allowing site-to-site, hub- and spoke and remote access VPNs.

The TOE also implements Intrusion Prevention System functionality. It is able to monitor information flows to detect potential attacks based on both pre-defined attack signature and anomaly characteristics in the traffic.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised 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 numerous other security events. 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.
- **Cryptological Support** – baseline cryptological module is included to provide confidentiality and integrity services for authentication. Tests for cryptological support were performed using the CAVS tool. The CMVP certificates are listed in the Security Target.

- **User Data Protection** – 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 TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users.
- **Information Flow** - 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 users to provide unique identification and authentication data before any administration 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 authorised 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
    - all other administrative tasks (e.g., creating the security policy)
    - The devices are managed through a Command Line Interface (CLI) The CLI is accessible through remote administrative session.
- **Protection of the TSF** – The TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords. The TOE provides for both cryptographic and non-cryptographic self-tests and is capable of automated recovery from failure states. Also, reliable timestamp is made available by the TOE
- **TOE Access** – The TOE can be configured to terminate inactive sessions.
- **Trusted Path / Channels** – The TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator.
- **Stateful Traffic Filtering** – The TOE provides stateful network traffic filtering based on examination of network packets and the application of information flow rules.
- **Virtual Private Networks** – The TOE provides Virtual Private Network (VPN) support, allowing site-to-site, hub-and spoke and remote access VPNs.
- **Intrusion Prevention** – The TOE can be configured to analyse IP-based network traffic forwarded to the TOE's interfaces, and detect violations of administratively-defined IPS policies. The TOE is capable of initiating a proactive response to terminate/interrupt an active potential threat, and to initiate a response in real time that would cause interruption of the suspicious traffic flow.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- The Routing Engine (RE) runs the Junos software and provides Layer 3 routing services and network management for all operations necessary for the configuration and operation of the TOE and controls the flow of information through the TOE, including Network Address Translation (NAT) and all operations necessary for the encryption/decryption of packets for secure communication via the IPSec protocol.

- The Packet Forwarding Engine (PFE) provides all operations necessary for transit packet forwarding

Juniper Networks security devices accomplish routing through a process called a Virtual Router (VR). A security device divides its routing component into two or more VRs with each VR maintaining its own list of known networks in the form of a routing table, routing logic, and associated security zones.

The TOE is managed and configured via Command Line Interface, which can be access via a console port or remotely using SSH over IPsec encapsulated connections, and does not depend on FTP or SSL to operate correctly.

2.5 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 guidance documentation (Ref 2).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from NDDP (Ref 3), FWEP (Ref 4) and VPNGWEP (Ref 5) and IPSEP (Ref 6) and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

2.5.2 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 7) 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:

- Secure Socket Layer (SSL)
- External syslog server

- Use of telnet, since it violates the Trusted Path requirement set (see Security Requirements)
- Use of FTP, since it violates the Trusted Path requirement set (see Security Requirements)
- Use of SNMP, since it violates the Trusted Path requirement set (see Security Requirements)
- Management via J-Web, since it violates the Trusted Path requirement set (see Security Requirements)
- Media use (other than during installation of the TOE)
- SSH
- TLS

2.6 Security

2.6.1 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 1) contains a summary of the functionality to be evaluated.

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the Juniper Networks, Inc. Junos 15.1 X49-D60 for SRX platforms. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the configuration guidance (Ref 2).

2.7.2 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 verification of the TOE is largely automatic, as demonstrated in testing. The TOE cannot load a modified software image. Authentic software images can be downloaded from https://www.juniper.net. In addition to the automated verification, the site includes individual MD5 hashes for each image. The administrator should verify the hash of the software before installing it into the hardware platform.

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.

2.7.3 Installation of the TOE

The guidance documentation (Ref 2) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

The verification of the TOE is largely automatic. This was demonstrated in testing. The TOE cannot load a modified software image. Authentic software images can be downloaded from https://www.juniper.net. In addition to the automated verification, the site includes individual MD5 hashes for each image. The administrator should verify the hash of the software before installing it into the hardware platform.

2.9 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:

- Junos® OS Common Criteria Evaluated Configuration Guide for SRX Series Security Devices, Release 15.1X49-D60, 24-Oct-16
- Junos® OS Common Criteria and FIPS Evaluated Configuration Guide for SRX Series Security Devices, Release 15.1X49-D60, 24-Oct-16
- Junos® OS CLI User Guide, Release 15.1, 22-Jul-16
- Junos® OS Installation and Upgrade Guide, Release 15.1, 21-Sep-16
- Junos® OS Getting Started Guide for Branch SRX Series, Release 15.1 X49, 30-Aug-16
- Junos® OS Intrusion Protection and Prevention Feature Guide for Security Devices, Release 15.1X49-D60, 06-Sep-16
- Junos® 15.1 X49 for SRX Series Platforms – SRX Guidance Annex, Version 1.0, 18-Jan-17
- Junos® OS VPN Feature Guide for Security Devices, Release 15.1X 49, 07-Jul-16
- Junos® 15.1 X49 for SRX Series Platforms – SRX Running Processes, Version 1.0, 18-Jan-17

All guidance material is available for download at **www.juniper.net.** 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 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.

- **A.NO_GENERAL_PURPOSE**

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

- **A.PHYSICAL**

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

- **A.TRUSTED_ADMIN**

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

- **A.CONNECTIONS**

It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

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), IPSEPv1.0, (Ref 6) Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Refs 8 and 9).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 10).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Ref 11).

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 (Ref 14).

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from the guidance documentation (Ref 2).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the Evaluators were taken from the NDPP, FWEP and VPNGWEP and IPSEP. 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.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 12).

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.

Based on the results of this testing, the Evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

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 and the associated functional packages 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.

4.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the Certifiers and of the Evaluation Technical Report (Ref 13) the Australasian Certification Authority **certifies** the evaluation of the Juniper Networks, Inc. Junos 15.1 X49-D60 for SRX Platforms product performed by the Australasian Information Security Evaluation Facility, BAE Applied intelligence.

The AISEF BAE Systems Applied Intelligence **has determined** that Juniper Networks, Inc. Junos 15.1 X49-D60 for SRX Platforms uphold the claims made in the Security Target (Ref 1) and **has met** the requirements of NDPP (Ref 3), FWEP (Ref 4), VPNGWEP (Ref 5) and IPSEP (Ref 6).

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 (Ref 3), FWEP (Ref 4), VPNGWEP (Ref 5) and IPSEP (Ref 6) 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.

4.4 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 7) 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 recommend that the administrator verify the hash of the downloaded software, as present on the Juniper Website
e) Note in the evaluated configuration of the TOE, remote SSH connections to the TOE must be encapsulated within an IPSec tunnel.

Annex A – References and Abbreviations

A.1 References

1. Security Target - Junos 15.1 X49-D60 for SRX Series Platforms Version 1.0, 24 January 2017

2. Guidance Documentation:

   - Junos® OS Common Criteria Evaluated Configuration Guide for SRX Series Security Devices, Release 15.1X49-D60, 24-Oct-16
   - Junos® OS Common Criteria and FIPS Evaluated Configuration Guide for SRX Series Security Devices, Release 15.1X49-D60, 24-Oct-16
   - Junos® OS CLI User Guide, Release 15.1, 22-Jul-16
   - Junos® OS Installation and Upgrade Guide, Release 15.1, 21-Sep-16
   - Junos® OS Getting Started Guide for Branch SRX Series, Release 15.1 X49, 30-Aug-16
   - Junos® OS Intrusion Protection and Prevention Feature Guide for Security Devices, Release 15.1X49-D60, 06-Sep-16
   - Junos® 15.1 X49 for SRX Series Platforms – SRX Guidance Annex, Version 1.0, 18-Jan-17
   - Junos® OS VPN Feature Guide for Security Devices, Release 15.1X 49, 07-Jul-16
   - Junos® 15.1 X49 for SRX Series Platforms – SRX Running Processes, Version 1.0, 18-Jan-17

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 20

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

6. Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS) Version 1.0 26 June 2014 (IPSEP)

7. 2016 Australian Government Information Security Manual (ISM), Australian Signals Directorate

8. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012, Version 3.1 Revision 4

9. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012, Version 3.1 Revision 4

10. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1, Revision 4.

11. AISEP Policy Manual Release: 30 August 2011 Version 4.0

12. Seeding of the Kernel in SRX Series Appliances running Junos 15.1 X49-D60, Version 1.0, 29-Nov-16

13. Evaluation Technical Report JUNOS 15.1 X49-D60 for SRX Series Platforms Version 1.0 Ref EFS-T043-ETR 1.0, 27 January 2017

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

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CAVS	Crypto Algorithm Validation System
CC	Common Criteria
CEM	Common Evaluation Methodology
CMVP	Cryptographic Module Validation Program
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
FWEP	US Government approved Network Devices Protection Profile – Protection Profile Stateful Traffic Filter Firewall Extended Package
GCSB	Government Communications Security Bureau
IPsec	Internet Protocol security
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
IPSEP	Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS)
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VPNGWEP	US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway