Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2011/75

15 July 2011

Version 1.3

Amendment Record

Version	Date	Description
0.1	26/05/2011	Internal release.
0.2	01/06/2011	Extended review.
1.3	15/07/2011	Public release.

Executive Summary

1 Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms is a product that is designed to primarily support the definition of and enforce information flow policies among network nodes. The routers provide stateful inspection of every packet that traverses the network and provide central management for the network security policy. All the information flows from one network node to another, passing through an instance of the Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms. Information flow is controlled on the basis of network node addresses, protocol, type of access requested, and services requested.

2 Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms is the Target of Evaluation (TOE).

3 This report describes the findings of the IT security evaluation of Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms, to the Common Criteria (CC) evaluation assurance level EAL 3. The report concludes that the product has met the target assurance level of EAL 3 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 stratsec and was completed in 23 May 2011.

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

a) The administrator should check the operational requirements and compatibility with deployed infrastructure;

b) The administrators must ensure that the TOE is physically secured; and

c) The administrator should have a thorough understanding of how the environment must be set up. The administrator should be familiar with requirements, integration into existing architectures and the application of certificate authorities.

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

6 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 at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

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

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 3; and

b) provide a source of detailed security information about the TOE for any interested parties.

9 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

10 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms
Software Version	JUNOS US/Canada Version 10.0 R4 JUNOS-FIPS Version 10.0 R4
Security Target	Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms, V2.0, 13 July 11
Evaluation Level	EAL 3
Evaluation Technical Report	Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms Evaluation Technical Report 1.0 23 May 11
Criteria	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 3.1 Revision 3, July 2009.
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1

Item	Identifier
	Revision 3, CCMB-2009-07-004.
Conformance	Common Criteria Part 2 conformant Part 2 Extended with FCS_CKM_SYM_EXP.1 Common Criteria Part 3 conformant
Developer	Juniper Networks 1194 North Mathilda Avenue Sunnyvale, California 94089, USA
Evaluation Facility	stratsec Suite 1/50 Geils Crt DEAKIN ACT 2600

Chapter 2 - Target of Evaluation

2.1 Overview

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

2.2 Description of the TOE

12 The Target of Evaluation (TOE), Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms, is the firmware running on Juniper's high-end and branch enterprise routing platforms. The primary function of the TOE is to support the definition of; and enforce; information flow policies among network nodes. The TOE provides stateful inspection of every packet that transverses the network and provides a central location to manage the network security policy. All information flow from one network node to another passes 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 provide the security tools to manage all of the security functions. The J-series Services routers are deployed at branch and remote locations in the network to provide all-in-one secure wide area network connectivity, IP telephony, and connection to local PCs and servers via integrated Ethernet switching.

13 The functionality defined in the Security Target that has been evaluated is:

a) **Security Audit**: the TOE generates audit records for security events. The administrator and the read-only administrator are the only roles with access to the audit trail and have the ability to view the audit trail.

b) **Cryptographic Support** the TOE supports secure communications between the TOE and other IT entities in order to authenticate users and to transmit authorisations to enforcement points. Encryption prevents modification and disclosure of this information.

c) **Information Flow Control**: the TOE is designed to help prevent unwanted and non-compliant endpoints from gaining access to the local area network. The TOE compares endpoint configuration with defined security policies; a non-compliant endpoint is not allowed full access to the network.

d) **Identification and Authentication**: the TOE requires all users to be identified and authenticated before any information flows are permitted. Additionally, administrators must be authenticated before performing any administrative functions.

e) **Security Management**: the TOE provides a wide range of security management functions. Administrators can configure the TOE, manage users, the information flow policy, and audit among other routine maintenance activities.

2.3 Security Policy

The Security Target (Ref [1]) contains no explicit security policy statements.

2.4 TOE Architecture

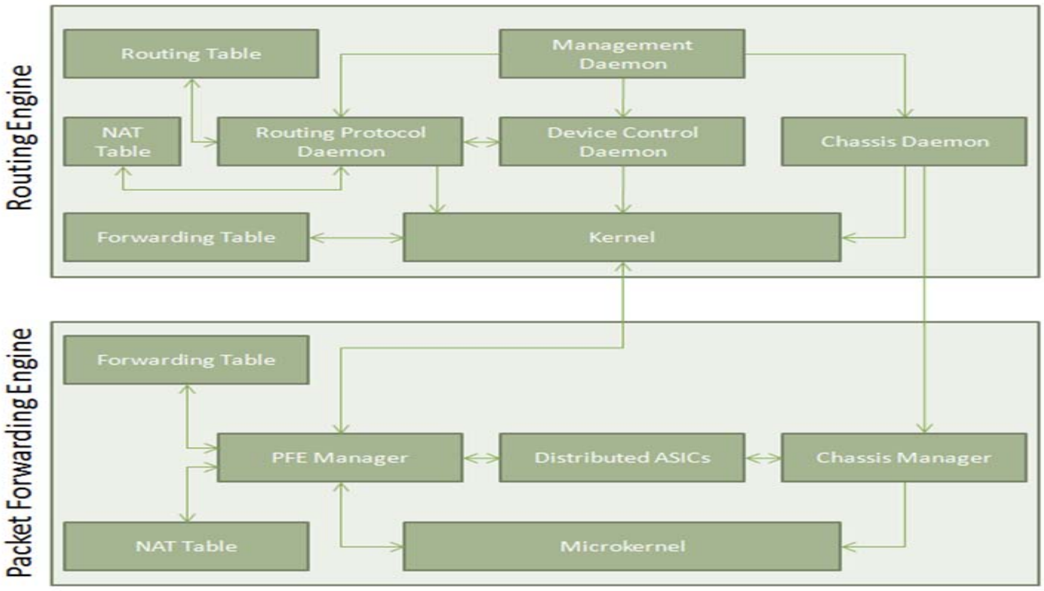
14 The TOE consists of the following major architectural components:

a) **The Routing Engine** receives exception packets and anything else that is specifically destined for it. As much traffic as possible is handled by the Packet Forwarding Engine so that the routing engine can do its job: managing JUNOS and the routing tables. The routing engine handles routing protocol processes and other processes that control the router's interfaces and user access. This engine maintains the routing table and the primary copy of forwarding table; and

b) **The Packet Forwarding Engine** pushes packets through the router and performs route lookups; most of the traffic on the router, especially the services traffic, is handled by the packet forwarding engine.

15 The TOE architecture inherently enforces separation of control and forwarding, meaning those two activities (control and forwarding) are handled by two separate engines: routing engine handles TOE control functions and the packet forwarding engine handles packet forwarding processes. For the SRX series, the routing engine and packet forwarding engine reside on physically separate hardware planes. For the J-Series, the control and forwarding are still logically separate processes, but they run on the same hardware plane.

16 This illustration shows the architectural separation of the main security domains of the TOE:



TOE Architecture Diagram

2.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]). The TOE includes a hardware cryptographic accelerator module. While the developer did not develop this part of the TOE, it was included for the evaluation. During testing, it was not possible to verify the deletion of keys in accordance with FCS_CKM.4.

18 The requirement's dependency on FCS_CKM.4 is not met and excluded from the Security Target because key destruction is implemented in hardware, as specified in the ADV_ARC.1 evidence. The architecture addresses this by not providing any commands to retrieve keys and not providing any functions pertaining to a general-purpose operating system. Additionally, the operational environment helps counter this by not providing unauthorised physical access to the TOE. (See OE.PHYSICAL in the Security Target (Ref [1]) for more information).

2.5.1 Evaluated Functionality

19 The TOE provides the following evaluated security functionality as described in the table below:

Security Function	Description
Audit	JUNOS auditable events are stored in the syslog files, and although they can be sent to an external log server, the requirements for auditing are met by local storage. Audit events cover authentication activity and configuration changes. Audit records include the date and time, event category, event type, username. An accurate time is gained by the router NTP daemon, acting as a client, from an NTP server in the IT environment. (The NTP server is considered outside the scope of the TOE.) This external time source allows synchronization of the TOE audit logs with external audit log servers in the environment. The audit log can be viewed only by a super-user and custom-user with appropriate privileges.
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 TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users. The TOE also implements Internet Protocol Security (IPSec) support including confidentiality, integrity, and authenticity of data transmitted from and to the TOE in a VPN-configured state.
Identification and Authentication	The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides three levels of authority for users, providing administrative flexibility (additional flexibility is provided in JUNOS, but is outside the scope of the evaluation). Super-users and custom-users with appropriate privileges have the ability to define groups and their authority and they have complete control over the TOE. The routers also require that applications exchanging information with them successfully authenticate prior to any exchange. This covers all services used to exchange information, including telnet (out of scope), SSH, SSL, and FTP. Authentication services can be handled either internally (fixed user selected passwords) or through a RADIUS or TACACS+ authentication server in the IT environment (the external authentication server is considered outside the scope of the TOE).

Security Function	Description
Security Management	The router is managed using XML RPCs (JUNOScript), either through raw XML (API mode) as in the case of J-Web (over HTTP) and JUNOScope (over SSL) or through a Command Line Interface (CLI) protected by SSH. Both interfaces provide equivalent management functionality. Through these interfaces all management can be performed, including user management and the configuration of the router functions. The CLI is accessible through an SSH session, or via a local terminal console. Net conf is an IETF standardisation effort which is closely aligned to JUNOScript.

2.5.2 Non-evaluated Functionality and Services

20 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 [2]) 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).

21 The functions and services that have not been included as part of the evaluation are provided below:

a) FCS_CKM.4 is excluded from the Security Target because key destruction is implemented in hardware. However, as specified in the ADV_ARC.1 evidence, the architecture addresses this by not providing any commands to retrieve keys and not providing any functions pertaining to a general-purpose operating system. Additionally, the operational environment helps counter this by not providing unauthorised physical access to the TOE. Please refer to the Security Target (Ref [1]) for more detail.

b) The NTP server is considered outside the scope of the TOE as it is an external time source.

2.6 Usage

2.6.1 Evaluated Configuration

22 This section describes the configurations of the TOE that were 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 [2]) to ensure that their configuration meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

23 The TOE is comprised of the following software components:

TOE component	Version/Model Number
J-Series Hardware	J2320, J2350, J4350, J6350
SRX Series Hardware	SRX100, SRX210, SRX240, SRX650, SRX3400, SRX3600, SRX5600, SRX5800
Software	JUNOS US/Canada Version 10.0 R4 JUNOS-FIPS Version 10.0 R4

24 Each Juniper Networks J-Series and SRX-Series 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.

25 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 Physical Interface Cards / Modules (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.

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

a) The Routing Engine 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 and all operations necessary for the encryption/decryption of packets for secure communication via the IPSec protocol; and

b) The Packet Forwarding Engine provides all operations necessary for transit packet forwarding.

27 The Routing Engine and Packet Forwarding Engine perform their primary tasks independently, while constantly communicating through a high-speed internal link. This arrangement provides streamlined forwarding and routing control and the capability to run internet-scale networks at high speeds.

2.6.2 Delivery Procedures

28 When placing an order for the TOE, the purchaser should make it clear to their supplier that they wish to receive the evaluated product.

29 Upon receipt by Juniper, customer orders are processed by Juniper Order Management and entered into the Oracle database where all subsequent processing (shipment transaction, packing slip generation, and invoice generation) will take place. The TOE is produced by authorised contract manufacturers. Each of the contract manufacturer sites are secure and are only accessible through card key access.

2.6.3 Determining the Evaluated Configuration

30 All appliances are uniquely identified on the appliance itself and with a corresponding unique label on the outer packing carton.

31 The appliances are labelled using an adhesive-backed thermal label, silver in colour. This label contains the unit model number, unit serial number, and in some instances the MAC Address. This label also contains product certification statements and markings in regards to EMC, Safety, NEBS, etc. These labels are printed during the manufacturing process by the contract manufacturers and affixed to the unit during final packaging of the box.

32 Juniper ships its products in an outer carton/box. The shipping container is labelled using an adhesive-backed white paper label. The label contains a UPC code, unit model number(s) and unit serial number(s). The carton label information is taken directly from the unit label packed in the carton. The data on this white carton label is then used to confirm orders in the order fulfilment database, which is securely maintained by Juniper Networks.

2.6.4 Packaging

33 All shipping containers and their associated bill of landing are uniquely identified with the product serial number. Juniper packages and labels the product in accordance with the current bill of material and any applicable package specification for the product to be shipped.

34 All products are enclosed in cardboard shipping boxes and sealed with tape. A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the shipping box.

35 Each hardware device is wrapped in a plastic bag and sealed with a warning label that states *'Please read the license terms regarding the use of the product included inside this box. By using the product, you agree to be bound by these license terms. If you do not agree with these terms, promptly return the unused product, manual, related equipment and hardware (with proof of payment) to the place of purchase for a full refund'*. The device cannot be removed from the plastic bag without damaging either the bag or the label.

2.6.5 Shipping

36 Juniper employs the use of a commercial carrier for its shipment of goods. The commercial carrier provides a tracking service for both the sender (Juniper) and the receiver to track delivery and receipt of the package.

2.6.6 Assurance of Proper Delivery

37 There are several mechanisms provided in the above process for a customer to ensure that they have received a product that has not been tampered with.

a) Outside packaging: If the outside shipping box and tape have not been broken and the outside shipping label properly identifies the customer and the product, then the product has not been tampered with.

b) Inside packaging: If the plastic bag or seal on the plastic bag are damaged or removed, the device may have been tampered with.

c) Delivery times: if delivery times coincide with the tracking information from the carrier, it can be assumed that the package was not tampered.

d) It is assumed that the trusted carriers provide reasonable measures to protect the products from tampering during shipping.

38 There are several mechanisms provided in the above process for a customer to ensure that they are receiving a box sent by Juniper and not another entity.

a) Customers must request the shipment of a Juniper appliance. Orders are never shipped without being requested.

b) When an appliance is shipped, a shipment notification is sent to the email address provided by the customer when the order is taken. This email includes the following information:

i) Purchase order number;

ii) Juniper order number to be used to track the shipment;

iii) Carrier tracking number to be used to track the shipment;

iv) List of Items shipped including serial numbers; and

v) Address and contacts of the customer who ordered the product and who the product will be shipped to.

39 If a customer wants to verify that a box they have received was sent by Juniper they can do the following:

a) Compare the carrier tracking number or the Juniper order number listed in the Juniper shipment notification with the tracking number on the package received;

b) Log onto the Juniper 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 order number listed in the Juniper shipment notification with the tracking number on the package received.

40 To verify that the hardware has not been tampered with during delivery, the administrator should follow the guidance below:

a) Verify outside packaging. If the outside shipping box and tape have not been broken, and the outside shipping label properly identifies the customer and the product, then the product has not been tampered with;

b) Verify inside packaging. If the plastic bag or seal on the plastic bag are damaged or removed, the device may have been tampered with; and

c) Contact Juniper networks if there is any suspicion that tampering has occurred.

2.6.7 Verify Software and Hardware

41 The Juniper device ships with the latest image version available. To load a validated version of the image, you must download the image from the Juniper networks support web site.

42 All JUNOS software is delivered in signed packages that contain digital signatures, secure hash algorithm (SHA1) checksums, and message digest 5 (MD5) checksums.

43 In order to comply with the TOE configuration, only the appliance models listed in the Security Target can be used.

2.6.8 Product Installation

44 Prior to installation, the administrator should read and be familiar with the details of all documentation for Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms.

2.6.9 Documentation

45 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. For a full list of the documentation available to customers of the TOE for download see: Annex A - product documentation. This is available when the TOE is downloaded from the Juniper support website.

2.6.10 Secure Usage

46 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.

47 Section 4: Security Objectives in the Security Target (Ref [1]) provide a full description of the assumptions.

Chapter 3 - Evaluation

3.1 Overview

48 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

49 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [3], [4] and [5]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [6]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation

Program (AISEP) (Refs [7] and [9]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [11]) were also upheld.

3.3 Functional Testing

50 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

51 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. The evaluators performed these tests to determine if the TOE is resistant to attacks performed by an attacker possessing enhanced-basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit;

b) Specialist technical expertise required;

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

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

Chapter 4 - Certification

4.1 Overview

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

4.2 Certification Result

53 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [12]), the Australasian Certification Authority certifies the evaluation of Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms performed by the Australasian Information Security Evaluation Facility, stratsec.

54 stratsec has found that Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 3.

55 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

56 EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and an architectural description of the design of the TOE, to understand the security behaviour.

57 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

58 EAL3 also provides assurance through the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures.

59 This EAL represents a meaningful increase in assurance from EAL2 by requiring more complete testing coverage of the security functionality and mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development.

4.4 Recommendations

60 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 [2]) and New Zealand Government users should consult the GCSB.

61 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref A.1), the ACA also recommends:

- The administrator should check the operational requirements and compatibility with deployed Infrastructure;
- The administrators must ensure that the TOE is physically secured; and
- The administrator should have a thorough understanding of how the environment must be set up. The administrator should be familiar with requirements, integration into existing architectures and the application of certificate authorities.

Annex A - References and Abbreviations

A.1 Product Documentation

The documentation is available for download from the Juniper support website, http://www.juniper.net/techpubs/

- JUNOS Software Configuration and Diagnostic Automation Guide - Release 10.0 r4;
- JUNOS Software Class of Service Configuration Guide - Release 10.0 r4
- JUNOS Software MPLS Applications Configuration Guide - Release 10.0 r4
- JUNOS Software Multicast Protocols Configuration Guide - Release 10.0 r4
- JUNOS Software Network Interfaces Configuration Guide - Release 10.0 r4
- JUNOS Software Network Management Configuration Guide - Release 10.0 r4
- JUNOS Software Policy Framework Configuration Guide - Release 10.0 r4
- JUNOS Software Routing Protocols Configuration Guide - Release 10.0 r4
- JUNOS Software SDK Applications Configuration Guide and Command Reference - Release 10.0 r4
- JUNOS Software Feature Support Reference for SRX Series and J Series Devices - Release 10.0 r4
- JUNOS Software VPNs Configuration Guide – Release 10.0 r4
- JUNOS Software System Basics Configuration Guide – Release 10.0 r4
- JUNOS Software Integrated Convergence Services Configuration and Administration Guide for SRX210 and SRX240 Services Gateways - Release 10.0 r4
- JUNOS Software JUNOscript API Guide - Release 10.0 r4
- JUNOS Software Design and Implementation Guide for J-series Services Routers – Release 10.0 r4
- WXC Integrated Services Module Installation and Configuration Guide – Release 10.0 r4
- Juniper Networks JUNOS 10.0 Software Release Notes – Release 10.0 r4
- JUNOS Software Administration Guide – Release 10.0 r4
- JUNOS Software CLI Guide – Release 10.0 r4
- JUNOS Software Interfaces and Routing Configuration Guide – Release 10.0 r4
- JUNOS Software Security Configuration Guide – Release 10.0 r4
- JUNOS Software WLAN Configuration and Administration Guide for SRX210, SRX240 and SRX 650 Services Gateways – JUNOS 10.0 r4

- JUNOS Software Feature Support Reference for SRX Series and J Series Devices
- JUNOS Software J-Web Interface User Guide – Release 10.0 r4
- JUNOS Internet Software Baseline Operations Guide
- JUNOS Internet Software Interfaces Operations Guide
- JUNOS Internet Software MPLS Fats Reroute Network Operations Guide
- JUNOS Internet Software MPLS Network Operations Guide Log Reference
- JUNOS Internet Software MPLS Network Operations Guide
- JUNOS Software Hierarchy and Standards Reference – Release 10.0 r4
- JUNOS Software System Basics and Services Command Reference - Release 10.0 r4
- JUNOS Software Interfaces Command Reference – Release 10.0 r4
- JUNOS Software Routing Protocols and Policies Command Reference – Release 10.0 r4
- Juno OS Secure Configuration Guide for Common Criteria and Junos – FIPS – Release 10.0 r4
- JUNOS Software Access Privilege Configuration Guide – Release 10.0 r4
- JUNOS Software CLI User Guide – Release 10.0 r4
- JUNOS Software High Availability Configuration Guide – Release 10.0 r4
- JUNOS Software Installation and Upgrade Guide – Release 10.0 r4
- Juno OS Secure Configuration Guide for Common Criteria and Junos – FIPS – Release 10.0 r4
- Juniper Networks JUNOS Software System Log Messages Reference - Release 10.0 r4

A.2 References

[1] Security Target: Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms Security Target Version 1.7

[2] Australian Government Information Security Manual (ISM), Jun 2011, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 3.1 Revision 3, July 2009, CCMB-2009-07-002.

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004.

[7] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[8] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, September 2007, Defence Signals Directorate.

[9] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[10] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[12] Evaluation Technical Report for Juniper Networks JUNOS 10.0 r4 for J-Series and SRX-Series Platforms – EFS-T027 ETR 1.0

A.3 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
IPSec	Internet Protocol Security
PFE	Packet Forwarding Engine
PP	Protection Profile
RE	Routing Engine
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy