Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/55

7 July 2009

Version 1.0

Amendment Record

Version	Date	Description
1.0	07/07/2009	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the Juniper Networks JUNOS 9.3 for J-Series and SRX-Series Platforms which is designed to support the definition of and enforces information flow policies among network nodes.

2 This report describes the findings of the IT security evaluation of Juniper Networks JUNOS 9.3 for J-Series and SRX-Series Platforms, to the Common Criteria (CC) evaluation assurance level EAL3. The report concludes that the product has met the target assurance level of EAL3 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed 1 July 2009.

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

a) use it only in its evaluated configuration;

b) synchronise the TOE to an network time protocol (NTP) trusted and authenticated source with an eventual cascaded synchronisation to a primary NTP service when configured as an NTP server;

c) restrict remote management of the TOE via web or secure shell (SSH) to a dedicated virtual local area network (VLAN) or subnet. Security policies should be configured on the TOE to filter remote access to SSH and HTTP/S;

d) be aware that persistent storage on the TOE hardware is limited and event logs should be archived regularly. Alternatively, the TOE may be configured to log to an external syslog service; and

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

5 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 (Ref [1]) and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

CHAPTER 1 - INTRODUCTION 1

1.1 OVERVIEW 1
1.2 PURPOSE 1
1.3 IDENTIFICATION 1

CHAPTER 2 - TARGET OF EVALUATION 2

2.1 OVERVIEW 2
2.2 DESCRIPTION OF THE TOE 2
2.3 SECURITY POLICY 3
2.4 TOE ARCHITECTURE 3
2.5 CLARIFICATION OF SCOPE 4
2.5.1 Evaluated Functionality 4
2.5.2 Non-evaluated Functionality 4
2.6 USAGE 4
2.6.1 Evaluated Configuration 4
2.6.2 Delivery procedures 5
2.6.3 Determining the Evaluated Configuration 6
2.6.4 Documentation 6
2.6.5 Secure Usage 6

CHAPTER 3 - EVALUATION 7

3.1 OVERVIEW 7
3.2 EVALUATION PROCEDURES 7
3.3 FUNCTIONAL TESTING 7
3.4 PENETRATION TESTING 8

CHAPTER 4 - CERTIFICATION 8

4.1 OVERVIEW 8
4.2 CERTIFICATION RESULT 8
4.3 ASSURANCE LEVEL INFORMATION 8
4.4 RECOMMENDATIONS 9

ANNEX A - REFERENCES AND ABBREVIATIONS 10

A.1 REFERENCES 10
A.2 ABBREVIATIONS 15

Chapter 1 - Introduction

1.1 Overview

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

1.2 Purpose

7 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 9.3 for J-Series and SRX-Series Platforms, against the requirements of the Common Criteria (CC) evaluation assurance level EAL3; and

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

8 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

9 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 9.3 for J-Series and SRX-Series Platforms
Software Version	JunOS Version 9.3
Hardware	J-series: J2320, J2350, J4350 and J6350
	SRX-series: SRX 5600 and SRX 5800
Security Target	Juniper Networks JUNOS 9.3 for J-Series and SRX Series Platforms Version 1.6 Document Number 530-029019-01
Evaluation Level	EAL3
Evaluation Technical Report	Evaluation Technical Report for Juniper JunOS9.3 Version 1.0
Criteria	Common Criteria Version 3.1, Revision 2, September 2007,

	with interpretations as of 29 May 2008.
Methodology	Common Criteria, Common Methodology for Information Technology Security Evaluation, Evaluation methodology September 2007 Version 3.1 Revision 2 with interpretations as of 29 May 2008.
Conformance	CC Part 2 Extended
Sponsor	SAIC, 7125 Columbia Gateway Drive, Suite 300, M/S CM6-80, Columbia MD 21046, United States of America
Developer	Juniper, 1194 North Matilda Avenue Sunnyvale, California 94089, United States of America
Evaluation Facility	stratsec, Suite 1/50 Geils Court, Deakin, Australian Capital Territory 2600

Chapter 2 - Target of Evaluation

2.1 Overview

10 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

11 The TOE is the Juniper Networks JUNOS 9.3 for J-Series and SRX-Series Platforms developed by Juniper. Its primary role is to support the definitions of and enforces information flow policies among network nodes.

12 The routers provide for stateful inspection of every packet that traverses the network and provide central management of the network security policy. All information flow from one network 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.

13 The J-series Services Routers are deployed at branch and remote locations in the networks to provide an all in one secure WAN connectivity, IP telephony and connection to local PCs and servers via integrated Ethernet Switching.

2.3 Security Policy

14 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 no explicit security policy statements.

2.4 TOE Architecture

15 The TOE consists of the following major architectural components:

a) Routing engine

b) Packet forwarding engine

16 The Developer's Architectural Design identifies the following components of the TOE:

a) Routing engine

i) SNMP and Management processes.

ii) Routing table

iii) Routing processes

iv) Interface processes

v) Chassis process

vi) Forwarding table

vii) Kernel

viii) Switch fabric

ix) I/O Card

b) Packet Forwarding Engine

i) Internet processor II

ii) Forwarding table

iii) Switch fabric

iv) I/O Card

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

18 The TOE provides the following evaluated security functionality:

a) Security Audit;

b) Communication;

c) Cryptographic support;

d) User data Protection ;

e) Identification and authentication; and

f) Security Management.

2.5.2 Non-evaluated Functionality

19 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 and Technology 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).

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

a) External NTP Server;

b) External Management Platform; and

c) External Authentication server.

2.6 Usage

2.6.1 Evaluated Configuration

21 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 these defined evaluated configuration(s). Australian Government users should refer to the ISM (Ref [2]) to ensure that the configuration(s) meets the minimum Australian Government

policy requirements. New Zealand Government users should consult the GCSB.

22 The TOE is comprised of the following software components:

a) JunOS 9.3

23 The TOE relies on the following hardware:

a) J-Series and SRX series' platforms.

24 The routers are physically self contained containing the software, firmware, hardware and interfaces necessary to perform all router functions.

2.6.2 Delivery procedures

25 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product. They should then receive the correct product.

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

(a) Purchase order number;

(b) Juniper Order Number to be used to track the shipment ;

(c) Carrier tracking number to be used to track the shipment;

(d) List of Items shipped including serial numbers; and

(e) Address and contacts of the customer who ordered the product and the destination of the product.

27 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; and

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.

28 Software: The TOE software components are downloaded from the Juniper customer service website by registered users. This website provides both MD5 and SHA-1 hashes for each downloadable file.

2.6.3 Determining the Evaluated Configuration

29 All Juniper appliances are uniquely identified on the appliance itself and with a corresponding unique label on the outer packing carton. 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 and affixed to the unit during final packaging of the box. The unit model number in this instance should correspond with the model numbers identified in the security target. The recipient can also compare carrier tracking numbers and Juniper order numbers as described above. The downloaded TOE image should have the filename: junos-jsr-9.3R2.8-domestic.tgz or junos-srx5000-9.3R2.8-domestic.tgz. The download website provides both an MD5 and a SHA-1 hash of the file for integrity checking.

30 Once the TOE has been installed on the hardware platform, the software version may be verified from the command line interface (CLI) by executing the command: ‘show version’. The output of this command should show the device name, hardware platform and installed OS image e.g. Router1, jsr6350, JUNOS Software Release [9.3R2.8] Enhanced Services.

2.6.4 Documentation

31 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available from the developer to ensure secure installation of the product.

a) Guidance Documentation (Ref [3]).

2.6.5 Secure Usage

32 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.

33 The following assumptions were made:

a) the processing resources of the TOE will be located within controlled access facilities, which prevent unauthorised physical access;

b) the authorised users will be competent and not careless, wilfully negligent or hostile and will follow and abide by the instructions provided by the documentation;

c) if the TOE is configured for external authentication services then these will be available either by Radius, TACACS+ or both;

d) external Network Time Protocol (NTP) services will be available; and

e) in-band management traffic will be protected using Secure Sockets layer (SSL) or Secure Shell (SSH).

Chapter 3 - Evaluation

3.1 Overview

34 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

35 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [4],[5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [7]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8],[9],[10] and [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Functional Testing

36 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. The areas tested were security alarms, audit, management access, authentication, configuration and filtering.

3.4 Penetration Testing

37 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 web interface was subjected to common attacks and a TOE masquerade was also attempted.

Chapter 4 - Certification

4.1 Overview

38 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

39 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority certifies the evaluation of Juniper Networks JUNOS 9.3 for J-Series and SRX-Series Platforms performed by the Australasian Information Security Evaluation Facility, stratsec.

40 stratsec has found that Juniper Networks JUNOS 9.3 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 EAL3.

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

4.3 Assurance Level Information

42 EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE to understand the security behaviour.

43 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

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

4.4 Recommendations

45 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 the ISM (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

46 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that users and administrators:

a) use it only in its evaluated configuration;

b) synchronise the TOE to an network time protocol (NTP) trusted and authenticated source with an eventual cascaded synchronisation to a primary NTP service when configured as an NTP server;

c) restrict remote management of the TOE via web or secure shell (SSH) to a dedicated virtual local area network (VLAN) or subnet. Security policies should be configured on the TOE to filter remote access to SSH and HTTP/S; and

d) be aware that persistent storage on the TOE hardware is limited and event logs should be archived regularly. Alternatively, the TOE may be configured to log to an external syslog service.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for Juniper Networks JUNOS 9.3 for J-Series and SRX-Series platforms, version 1.6, Document number 530-029019-01, June 29, 2009.

[2] Australian Government Information and Communications Technology Security Manual (ISM), 2008, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] User Documentation.

a) JUNOScript API Guide Release 9.3 beta draft

b) JUNOS XML API Configuration Reference Release 9.2

c) JUNOS XML API Operational Reference Release 9.2

d) NETCONF API Guide Release 9.3

e) Configuration and Diagnostic Automation Guide Release 9.3

f) Administration Guide Release 9.3

g) Advanced WAN Access Configuration Guide Release 9.3

h) Basic LAN and WAN Access Configuration Guide Release 9.3

i) Getting Started Guide Release 8.5 (J2300, J4300, J6300 Service Router)

j) Getting Started Guide Release 9.3 (J2320, J2350, J4350, J6350 Service Router)

k) J-series Service Router Quick Start

l) J-series Service Router Release Notes for JUNOS 9.3 Software

m) Security Configuration Guide for Common Criteria and JUNOS-FIPS Release 8.1

n) Access Privilege Configuration Guide Release 9.3

o) User Guide Release 9.3

p) Class of Service Configuration Guide Release 9.3

q) High Availability Configuration Guide Release 9.3

r) Software Installation and Upgrade Guide Release 9.3

s) MPLS Applications Configuration Guide Release 9.3

t) Multicast Protocols Configuration Guide Release 9.3

u) Network Management Configuration Guide Release 9.3

v) Network Interfaces Configuration Guide Release 9.3.

w) Policy Framework Configuration Guide Release 9.3

x) Routing Protocols Configuration Guide Release 9.3

y) Services Interfaces Configuration Guide Release 9.3

z) System Basics Configuration Guide Release 9.3

aa) VPNs Configuration Guide Release 9.3

bb) System Basics and Services Command Reference Release 9.3

cc) Interfaces Command References Release 9.3

dd) Routing Protocols and Policies Command Reference Release 9.3

ee) Hierarchy and RFC Reference Release 9.3

ff) System Log Messages Reference Release 9.2

gg) Administration Guide for J-series Services Routers and SRX-series Services Gateways Release 9.3

hh) CLI Reference for J-series Services Routers and SRX-series Services Gateways Release 9.3

ii) Interfaces and Routing Configuration Guide for J-series Services Routers and SRX-series Services Gateways Release 9.3

jj) Security Configuration Guide for J-series Services Routers and SRX-series Services Gateways Release 9.3

kk) JUNOS 9.3 Software for SRX-series Services Gateways Release Notes

ll) JUNOS 9.3 EFT Software for SRX 210 Services Gateway Release Notes Release 9.3

mm) JUNOS 9.3 EFT Software for SRX 3400 and SRX 3600 Services Gateways Release Notes

nn) Hardware Guide EFT Draft (SRX 3400 Services Gateway)

oo) Hardware Guide EFT Draft (SRX 3600 Services Gateway)

pp) SRX 5600 and SRX 5800 Services Gateway Craft Interface Installation Instructions

qq) SRX 5600 and SRX 5800 Services Gateway I/O Card Installation Instructions

rr) SRX 5600 and SRX 5800 Services GatewayRouting Engine Installation Instructions

ss) SRX 5600 and SRX 5800 Services Gateway Switch Control Board Installation Instructions

tt) SRX 5800 and SRX 5600 Services Gateway Service Processing Card Installation Instructions

uu) SRX 5600 Services Gateway AC Power Supply Installation Instructions

vv) SRX 5600 Services Gateway Air Filter Installation Instructions

ww) SRX 5600 Services Gateway DC Power Supply Installation Instructions

xx) SRX 5600 Services Gateway Fan Tray Installation Instructions

yy) SRX 5600 Services Gateway Getting Started Guide

zz) Protected System Domain Configuration Guide Release 9.3

aaa) JUNOS 9.3 Software Release Notes

bbb) Feature Guide Release 9.3

ccc) JUNOS 9.3 Software Release Notes: Release 9.3R1

ddd) Administration Guide for J-series Services Routers and SRX-series Services Gateways Release 9.3

eee) Security Configuration Guide for J-series Services Routers and SRX-series Services Gateways Release 9.3

fff) CLI Reference for J-series Services Routers and SRX-series Services Gateways Release 9.3

ggg) JUNOS Software with Enhanced Services: Migration Guide for J-Series Services Routers

hhh) SSG 300M-series/J2320 and J2350 Services Router Read This First

iii) SSG 300M-series/J2320 and J2350 Services Router Conversion Kit Instructions

jjj) SSG 500M-series/J4350 and J6350 Services Router Read This First

kkk) SSG 500M-series/J4350 and J6350 Services Router Conversion Kit Instructions

lll) Converting SSG 300M-series and SSG 500M-series Security Devices to J-series Services Routers with a USB Storage Device Read This First

mmm) Converting SSG 300M-series and SSG 500M-series Security Devices to J-series Services Routers with a USB Storage Device Conversion Kit Instructions

nnn) JUNOS Software with Enhanced Services Hardware Guide for J-series Services Routers Release 9.3

ooo) JUNOS Software with Enhanced Services: Design and Implementation Guide for J-series Services Routers

ppp) Interfaces and Routing Configuration Guide for J-series Services Routers and SRX-series Services Gateways Release 9.3

qqq) WXC Integrated Services Module Installation and Configuration Guide Release 9.2

rrr) JUNOS Software with Enhanced Services Quick Start for J-Series Services Routers.

sss) Mapping for AGD documents

ttt) Operational User Guidance and Preparative Procedures Supplement, Juniper Networks JUNOS 9.3 for J-Series and SRX-Series Platforms, Document Number 530-026385-01, Version 1.3.

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 3.1, Revision 1, September 2006, CCMB-2006-09-001, Incorporated with interpretations as of 2008-05-29

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components (CC), Version 3.1, Revision 2 , September 2007, CCMB-2007-09-002, Incorporated with interpretations as of 2008-05-29

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-003, Incorporated with interpretations as of 2008-05-29

[7] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 2 September 2007, CCMB-2007-09-004 Incorporated with interpretations as of 2008-05-29

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

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1,29 September 2006, Defence Signals Directorate.

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

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

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

[13] Evaluation Technical Report for Juniper JunOS9.3, 1 July 2009.

A.2 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
HTTP/S	Hypertext Transfer Protocol Secure
NTP	Network Time Protocol
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VLAN	Virtual local area network