Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2010/66

10 Mar 2010

Version 1.0

Amendment Record

Version	Date	Description
1.0	10/03/2010	Public release

Executive Summary

1 The Target of Evaluation (TOE) is the Juniper Networks Secure Access Family Version 6.4R2 which is designed to act as an application gateway that mediates all requests between remote computers and internal network resources.

2 This report describes the findings of the IT security evaluation of Juniper Networks Secure Access Family Version 6.4R2, to the Common Criteria (CC) evaluation assurance level EAL3 augmented with ALC.FLR.2. 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 24 December 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) 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;

c) 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;

d) Ensure that the SSL configuration is set to Advanced Encryption Standard (AES) using key lengths of 128, 192 or 256 bits or Triple Data Encryption Standard (3DES) using key length 168 by going to **System > Configuration > Security**, otherwise the default cipher would use RC4 with a 256 bit key length;

e) Consumers must be aware of the residual vulnerability in the TOE (VU#261869 at http://www.kb.cert.org/vuls/id/261869 and Juniper JTAC Bulletin PSN-2009-11-580). The ACA recommends that the guidance provided in Juniper KB15799 to work around this vulnerability be applied to the TOE; and

f) Ensure strict adherence to the delivery procedures.

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 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 Secure Access Family Version 6.4R2, 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 Secure Access Family Version 6.4R2
Software Version	Version 6.4R2
Hardware	Secure Access 700, 2000, 2500, 4000, 4500, 4500 FIPS, 6000, 6000SP, 6500, 6500 FIPS
Security Target	Juniper Networks Secure Access Family Version 6.4 Document Version 1.9, February 26, 2010
Evaluation Level	EAL3+
Evaluation Technical Report	Evaluation Technical Report for Juniper Networks Secure Access Family Version 6.4R2, 2 March 2010
Criteria	Common Criteria July 2009, Version 3.1, Revision 3, with

	interpretations as of 8 July 2009.
Methodology	Common Criteria, Common Methodology for Information Technology Security Evaluation, Evaluation methodology July 2009, Version 3.1 Revision 3 with interpretations as of 8 July 2009.
Conformance	CC Part 2 CC Part 3 augmented
Sponsor and 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 Secure Access Family Version 6.4R2 developed by Juniper. The TOE is a secure application layer gateway that intermediates all requests between remote computers and internal corporate resources. All requests from remote computers to a Secure Access (SA) appliance and from a SA appliance to remote computers are encrypted. All unencrypted requests (e.g. HTTP) are redirected to HTTPS which ensures the connection is encrypted. In summary, the TOE provides a secure remote access to internal network resources, including:

i) Web based traffic including web pages and web-based applications;

ii) Java applets, including Web applications that use Java applets;

iii) File traffic including file servers and directories;

iv) The routers client/server applications;

v) Telnet and SSH terminal emulation services;

vi) Windows terminal servers and Citrix server terminal emulation sessions;

vii) Email clients based on the IMAP4, POP3 and SMTP protocols; and

viii) All network traffic.

2.3 Security Policy

12 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

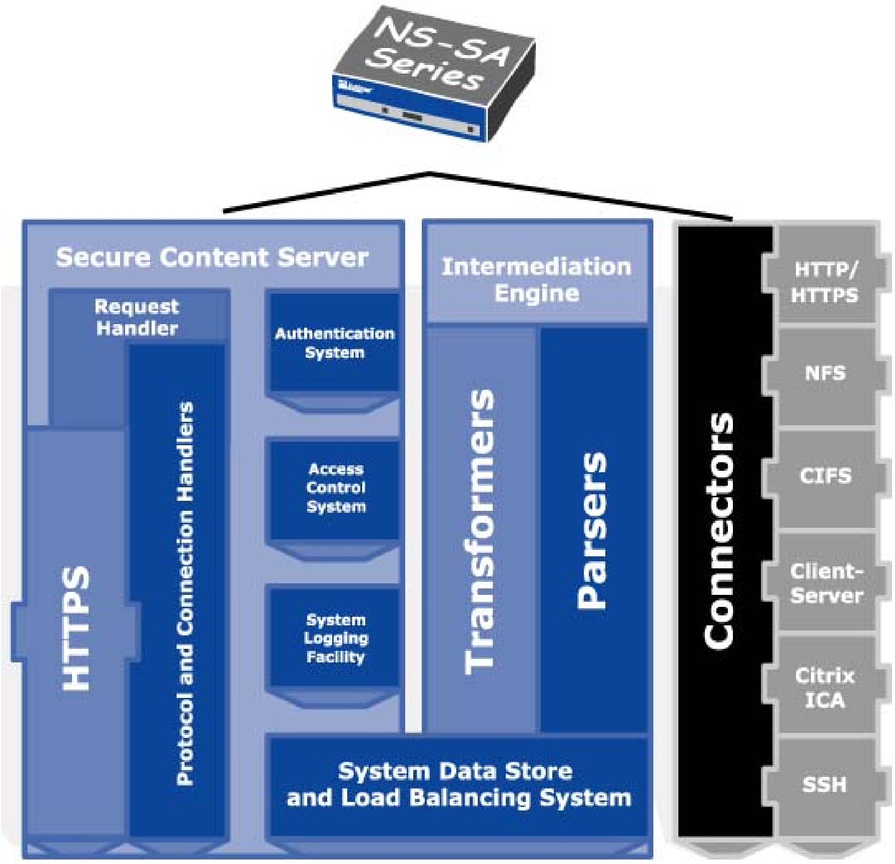

Figure 1: TOE Architecture Diagram

13 The TOE consists of the following major architectural components:

a) Secure content server which consists of the following components:

i) Access Control System;

ii) Authentication System;

iii) Protocol and Connection Handlers;

iv) Request Handler;

v) System logging facility; and

vi) Web server.

b) Intermediation engine which consists of

   i) Parsers – event-driven components that process resource data streams and decompose them into ‘chunks’ that are manipulated by associated transformers.

   ii) Transformers – components that receive the ‘chunks’. The transformers have the opportunity to modify each chunk in the data stream before writing it out to the Request Handler.

c) Connectors which are components that use protocol adapters to retrieve resource and application data streams, such as documents on file servers, HTML pages on the intranet servers or messages from an MS Exchange server

d) System Data Store. All data stored on the device is encrypted using AES, however access to the encrypted data is outside the scope of the TOE. Only SA system software can read the encrypted data store. Users and administrators cannot replace executable files and they do not have system-level accounts. Potential attackers cannot employ privilege-elevation attacks against the appliance.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

15 The TOE provides the following evaluated security functionality:

a) Security Audit;

b) Cryptographic operations;

c) User data protection ;

d) Identification and authentication;

e) Security Management; and

f) Protection afforded to the TOE security functions.

2.5.2 Non-evaluated Functionality

16 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).

2.6 Usage

2.6.1 Evaluated Configuration

17 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.

18 The TOE is comprised of the following software components:

a) Revision 6.4R2.

19 The TOE relies on the following hardware:

a) Secure Access 700, 2000, 2500, 4000, 4500, 4500 FIPS, 6000, 6000SP, 6500, 6500 FIPS.

2.6.2 Delivery procedures

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

21 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.

22 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; and

c) Juniper packages and labels the product in accordance with the current bill of material (BOM).Verify that the tamper evident seal is intact upon receipt.

23 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

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

25 The appliances are labelled using an adhesive-backed thermal label. This label contains the unit model number, unit serial number and in some instances the MAC Address.

26 This label also contains product certification statements and markings in regards to Electromatic Compatability (EMC), Safety and Network Equipment Building System (NEBS).

27 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: SA 6.4R2. The download website provides both an MD5 and a SHA-1 hash of the file for integrity checking.

2.6.4 Documentation

28 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following

29 documentation is available for download from the developer to ensure secure installation of the product.

a) Guidance Documentation (Ref [3]).

2.6.5 Secure Usage

30 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.

31 The following assumptions were made:

a) there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE;

b) authorised administrators are non-hostile and follow all administrator guidance. They are capable of error;

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

d) the TOE does not host public data; and

e) information cannot flow among the internal and external networks unless it passes through the TOE.

Chapter 3 - Evaluation

3.1 Overview

32 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

33 The criteria against which the 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

34 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; 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 audit, cryptographic key management, user data protection, identification and authentication, security management, TOE access and trusted path.

3.4 Penetration Testing

35 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.

36 The evaluators were able to discover one vulnerability specific to the TOE from publicly available sources. This vulnerability relates to SSL-VPN devices that may affect the web browser's domain based security models. The evaluators determined that the attack potential required to undermine the SFRs exceeds the assurance components claimed in this evaluation. Therefore the evaluators determined this vulnerability is not exploitable in the context of this evaluation. Juniper has provided several solutions which include constraining the web servers for content rewriting.

37 The web interface was subjected to common penetration attacks which failed to have effect.

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 ACA.

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 Secure Access Family Version 6.4R2 performed by the Australasian Information Security Evaluation Facility, stratsec.

40 stratsec has found that Juniper Networks Secure Access Family Version 6.4R2 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL3 augmented with ALC_FLR.2.

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

4.3 Assurance Level Information

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

43 The analysis is supported by independent testing of the TOE security functions (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.

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) 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

c) 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.

d) Ensure that the SSL configuration is set to Advanced Encryption Standard (AES) using key lengths of 128, 192 or 256 bits or Triple Data Encryption Standard (3DES) using key length 168 by going to **System** > **Configuration** > **Security**, otherwise the default cipher would use RC4 with a 256 bit key length;

e) Consumers must be aware of the residual vulnerability in the TOE (VU#261869 at http://www.kb.cert.org/vuls/id/261869 and Juniper JTAC Bulletin PSN-2009-11-580). The ACA recommends that the guidance provided in Juniper KB15799 to work around this vulnerability be applied to the TOE; and

f) Ensure strict adherence to the delivery procedures.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for Juniper Networks Secure Access Family Version 6.4. Document Version 1.9 February 26 2010

[2] Australian Government Information Security Manual (ISM), 2009, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] User Documentation.

a) Juniper Networks Secure Access, Quick Start Guide, 093-1692-000 Rev 02

b) Juniper Networks Secure Access, Quick Start Guide for Secure Access 2500, 4500 and 6500, 530-023034 Rev 02

c) Juniper Networks Secure Access, Administration Guide Release 6.4, 530-029892-01

d) IVE Quick Startup Guide – OS 4.0

e) Juniper Networks NetScreen-Secure Access Release Notes, IVE Platform version 6.4R2 Build #14343

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), July 2009 Version 3.1, Revision 3, , CCMB-2009-07-001, Incorporated with interpretations as of 2009-07-08

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components (CC), July 2009 Version 3.1, Revision 3 , , CCMB-2009-07-002, Incorporated with interpretations as of 2009-07-08

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components (CC), July 2009, Version 3.1, Revision 3, CCMB-2009-07-003, Incorporated with interpretations as of 2009-07-08

[7] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 3, July 2009, CCMB-2009-07-004, Incorporated with interpretations as of 2009-07-08

[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 Networks Secure Access Family Version 6.4, 2 March 2010.

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
IMAP4	Internet Message Access Protocol version 4
POP3	Post Office Protocol version 3
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SMPT	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VLAN	Virtual local area network