Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2010/70

23 November 2010

Version 1.0

Amendment Record

Version	Date	Description
1.0	23/11/2010	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is Juniper Networks IC Series UAC Appliances Version 3.0R2 which is a product that is designed to mediate access to a network. The TOE authenticates users and retrieves the access policies for those users. It is able to utilise both internal authentication tables and access external authentication servers. The TOE also assesses the health of a user's host machine and compares it to the policies in order to determine the allowed network access. It then communicates with a variety of enforcement points to enforce the network access constraints. Enforcement points include Juniper packet filters configured on the endpoints, Juniper firewalls and any vendor's 802.1X enabled switches or wireless access points.

2 This report describes the findings of the IT security evaluation of Juniper Networks' Juniper Networks IC Series UAC Appliances Version 3.0R2, to the Common Criteria (CC) evaluation assurance level EAL3+ (augmented with ALC_FLR.2)

3 The report concludes that the product has met the target assurance level of EAL3+ 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 10 September 2010.

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 the deployed Infranet enforcers;

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 IC Series UAC Appliances Version 3.0R2, 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.

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 IC Series UAC Appliances Version 3.0R2
Security Target	Juniper Networks IC Series UAC Appliances Version 3.0R2 ST version: 2.0, August 12, 2010
Evaluation Level	EAL3+ (augmented with ALC_FLR.2)
Evaluation Technical Report	Evaluation Technical Report, Juniper Networks IC Series UAC Appliances Version 3.0R2. Version: 1.0, 10 September 2010
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2007

Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2007, Version 3.1 Revision 2, CCMB-2007-09-004
Conformance	Common Criteria Part 2 conformant Common Criteria Part 3 augmented.
Sponsor/Developer	Juniper Networks 1194 North Mathilda Avenue Sunnyvale, California 94089, USA
Evaluation Facility	stratsec Suite 1/50 Geils Court, 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 TOE is the Juniper Networks IC Series UAC Appliances version 3.0R2 developed by Juniper Networks. It's primary role is to provide a network access decision to network controllers based on information about the client.

13 The TOE is the central control point for Juniper Network's Unified Access Control (UAC) solution. Users can contact the TOE with a variety of clients in order to request network access. The TOE authenticates users and retrieves the access policies for those users. The TOE also assesses the health of a user's host machine and compares it to the policies in order to determine whether network access is allowed.

14 The TOE then communicates with a variety of enforcement points (including Juniper endpoint clients filters, Juniper firewalls, and standard 802.1X enabled switches or wireless access points) to communicate the network access constraints based on the TOE's decision. The enforcement points will allow/deny access based on the TOE's result of authentication and policy compliance. The following figure shows the TOE (Infranet Controller) in a typical environment:

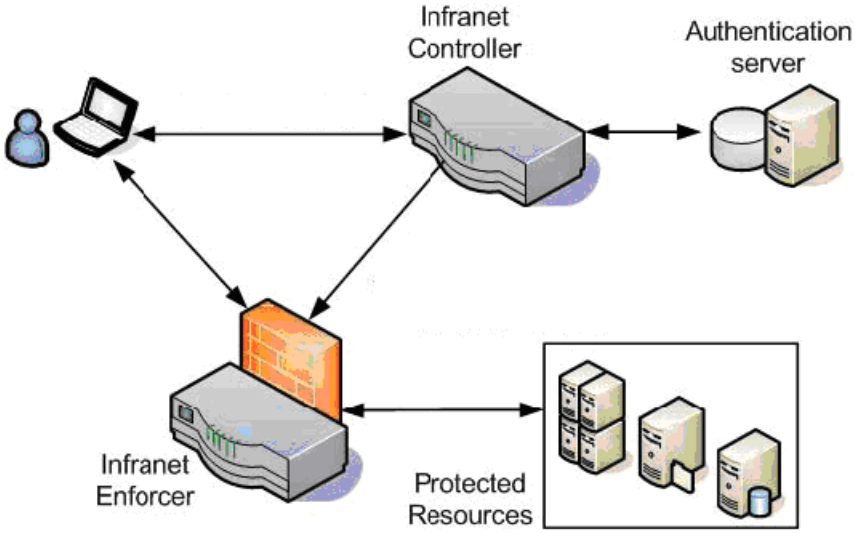

Figure 1: The TOE in a Typical Environment

2.3 Security Policy

15 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, the following TSPs are implied:

a) **Audit** – a user's actions should be auditable;

b) **Information Flow Control –** the ability to make data flow on the network should be able to be controlled where that information is sensitive;

c) **Authentication –** users accessing a monitored resource should be identified and authenticated; and

d) **Security Management –** the TOE must be able to be managed and have access to those functions restricted.

2.4 TOE Architecture

16 The TOE consists of the following major architectural components:

a) **Authentication Server –** provides the capability to manage users, roles, user password restrictions, sessions and enforce authentication.

b) **Policy Manager –** provides the capability to manage and enforce the network access policies.

c) **Web Server and Application Proxies –** provides the capability to archive event logs, user access logs and admin access logs, restart and shut down the appliance, manage session encryption, create or modify policies and manage the time and date.

d) **Operating System –** provides the capability to view and apply settings to the event logs, user access logs and admin access logs.

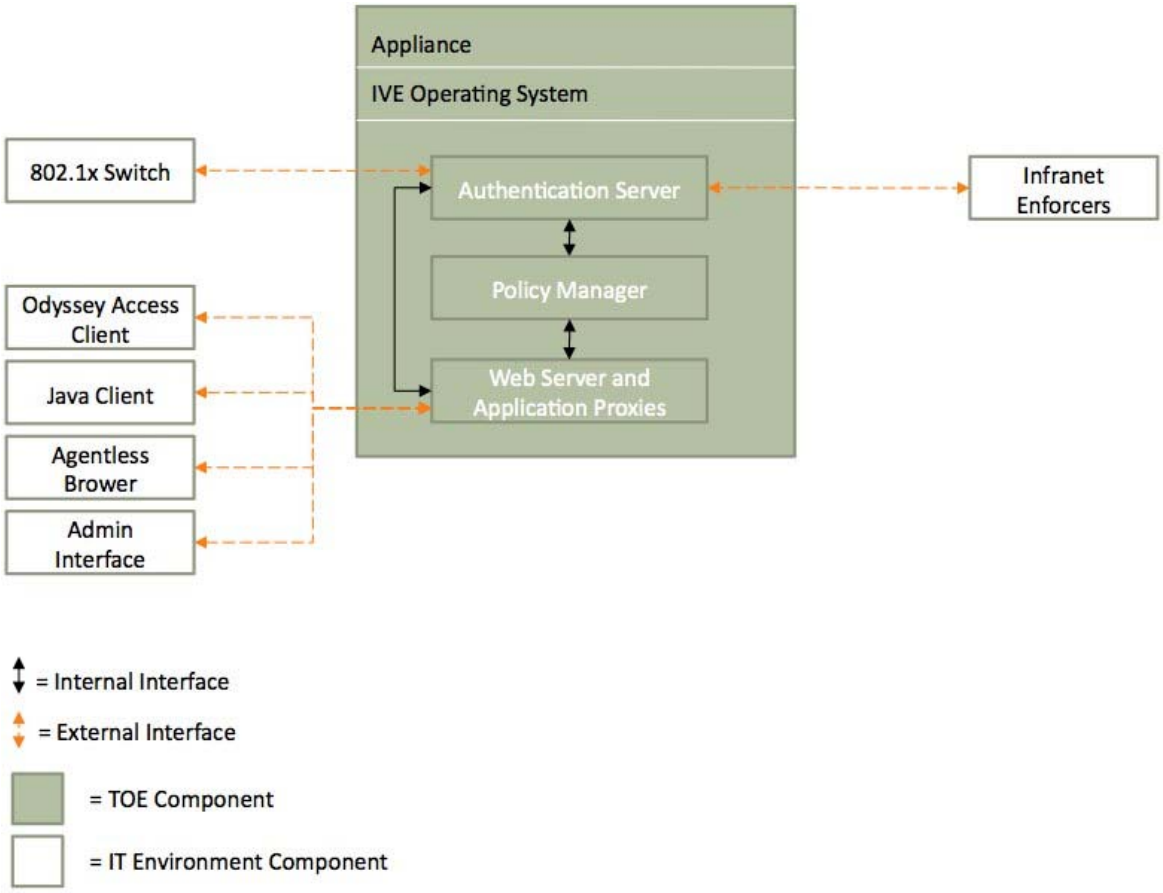

Figure 2: TOE Architecture Diagram

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

18 The TOE provides the following evaluated security functionality:

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 –** All users are required to perform identification and authentication 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:

i) configure the TOE;

ii) manage users;

iii) manage the information flow policy;

iv) audit; and

v) perform routine maintenance activities.

2.5.2 Non-evaluated Functionality and Services.

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 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 GCSB.

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

a) Cryptographic key destruction was excluded from the scope of the TOE. Owners of the TOE must ensure that the TOE is used from a secure room.

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 this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that the configuration 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) IC OS Version 3.0R2

23 The TOE relies on the following hardware:

a) Infranet Controller 4500, 6500, or 6500 FIPS.

2.6.2 Delivery procedures

24 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 TOE.

25 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, tape, and tamper-evidence seals 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 is 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. It is assumed that the trusted carriers (FedEx and UPS) provide reasonable measures to protect the products from tampering during shipping; and

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

26 When an appliance is shipped, an Advanced 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;

e) Address and contacts of the customer who ordered the product and to whom the product will be shipped;

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

    i) 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

ii) 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.

2.6.3 Determining the Evaluated Configuration

27 The administrators and users can determine if they are in the evaluated configuration by checking the following:

a) **Verify Hardware –** In order to comply with the TOE configuration, only the appliance models listed in the evaluation's Security Target can be used.

b) **IC6500 FIPS Platform** – *Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules* specifies requirements for cryptographic products to be deployed in a sensitive but unclassified environment. More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html. The IC6500 FIPS platform is a standard IC6500 (respectively) appliances equipped with a FIPS-certified cryptographic module. In order to maintain FIPS-mode of operation, the administrator should read and follow the guidance in the *Using the IC6500 FIPS* section on page 40 of the *Juniper Networks Unified Access Control Administration Guide Release 3.0*.(Ref [3]).

c) **Verify Software –** In order to comply with the TOE configuration, the appliances must run software version 3.0. To verify the version, the Administrator can select **System > Status > Overview Page** from the Administrator Web Console. If the pre-loaded software version differs from the version required for the TOE configuration, the administrator should load version 3.0 by performing the following steps:

i) Select Maintenance > System > Upgrade/Downgrade from the Administrator Console;

ii) Click on **Browse…;**

iii) Locate the System Software Package Version 3.0 file ;

iv) Click on **Open;** and

v) Click on Install Now.

d) **Evaluated configuration –** The evaluated configuration is based on default installation of the TOE with the additional configuration:

i) Set default policies to 'Deny';

ii) Timeout of sessions;

i) Idle timeout: 10 minutes; and

ii) Max. session length: 60 minutes.

iii) Required Password;

i) Minimum length: (8) characters;

ii) Password must have at least (3) digits;

iii) Password must have at least (3) letters;

iv) Password must have mix of UPPERCASE and lowercase letters;

v) Password must be different from username; and

vi) New passwords must be different from previous password.

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 documentation is available upon request from the developer:

a) Guidance documentation (Ref [3]),

2.6.5 Secure Usage

29 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.

30 The following assumptions were made during the evaluation:

a) The processing resources of the TOE will be located within controlled access facilities, which will 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 TOE documentation.

Chapter 3 - Evaluation

3.1 Overview

31 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

32 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 [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2 (CEM) (Ref [7]). The evaluation was 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

33 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.

34 The areas tested were Security Audit, Cryptographic Support, Information Flow Control, Identification and Authentication and Security Management.

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 and developer documents submitted for the evaluation.

36 The evaluators considered numerous known vulnerabilities and developed tests to determine the TOEs susceptibility to the following types of attacks:

a) Brute force of authentication credentials;

b) Man in the middle attacks; and

c) Interface fuzzing and misuse of data fields in forms.

Chapter 4 - Certification

4.1 Overview

37 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

38 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 IC Series UAC Appliances Version 3.0R2 performed by the Australasian Information Security Evaluation Facility, stratsec.

39 stratsec has found that Juniper Networks IC Series UAC Appliances Version 3.0R2 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 + ALC_FLR.2.

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

4.3 Assurance Level Information

41 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.

42 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.

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

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

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 ISM (Ref [2]) and New Zealand Government users should consult the 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 administrators:

a) Check the operational requirements and compatibility with the deployed Infranet enforcers;

b) Ensure that the TOE is physically secured; and

c) 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, Abbreviations and Glossary of terms

A.1 References

[1] Juniper Networks IC Series UAC Appliances Version 3.0R2 Security Target Version 2.0

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

[3] Administrator and User Guidance

i) Juniper Networks IC Series UAC Appliances Version 3.0R2 Operational User Guidance and Preparative Procedures Supplement Version 1.0.

ii) Juniper Networks Unified Access Control Administration Guide Release 3.0.

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-003

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

[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 3.3, September 2007, 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 IC Series UAC Appliances Version 3.0R2, Version: 1.0, Released: 10 September 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
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
UAC	Unified Access Control
+	Augmented

A.3 Glossary of Terms

Infranet	An Enterprise Infranet is a framework that describes network infrastructure capable of coordinating delivery of applications to users, irrespective of location, in a secure and assured manner.