C039 Certification Report

Juniper Networks Junos Pulse Access Control Service 4.2 R4

File name: ISCB-5-RPT-C039-CR-v1a

Version: v1a

Date of document: 5 August 2013

Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C039 Certification Report

Juniper Networks Junos Pulse Access Control Service 4.2 R4

5 August 2013

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines, No 7 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8992 6888 Fax: +603 8992 6841

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C039 Certification Report – Juniper Networks Junos Pulse Access Control Service 4.2 R4
DOCUMENT REFERENCE:	ISCB-5-RPT-C039-CR-v1a
ISSUE:	v1a
DATE:	5 August 2013

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 5, Sapura@Mines,

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 5 August 2013, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	24 July 2013	All	Final Released
v1a	5 August 2013	Page iv	Add the date of the certificate.

Executive Summary

The Juniper Networks Junos Pulse Access Control Service 4.2 R4 (hereafter referred as Unified Access Control (UAC)) from Juniper Networks is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented with ALC_FLR.2 evaluation.

Juniper Networks Junos Pulse Access Control Service 4.2 R4 or the TOE is the central control point for Juniper Network's Unified Access Control (UAC) solution. Users will contact the TOE using 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.

It 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 or deny access based on the TOE's result of authentication and policy compliance.

The functions of the TOE that are within the scope of evaluation covering the secure audit, cryptographic support (including cryptographic operations), information flow control, identification and authentication, security management.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 3 (EAL3) Augmented with ALC_FLR.2. The report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the BAE Systems Detica evaluation facility (the 'BAE Systems Detica MySEF') and completed on 31 May 2013.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangement on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that the UAC meets their requirements. It is recommended that a potential user of the UAC to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), Juniper Networks Junos Pulse Access Control Service 4.2 R4 (hereafter referred as Unified Access Control (UAC)) is an appliance and software client running on a remote IT system. The TOE provides central control point for Juniper Network's Unified Access Control (UAC) solution.

2 Users will contact the TOE using 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.

3 Authorised users can communicate 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 or deny access based on the TOE's result of authentication and policy compliance.

4 In the context of the evaluation, the TOE provides the following major security features; which will be discussed further in Section 1.4.1 of this document:

a) Generates audit records of security events.

b) Cryptographic support for secure communications between TOE and other IT entities in order to authenticate users and to transmit authorisations to enforcement points.

c) Information flow control to 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) All users are required to perform identification and authentication before any information flows are permitted. For administrators, they must also be authenticated before performing any administrative functions.

e) Security management functions for the administrators to configure the TOE, manage users, manage information flow policy and auditing activities.

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C039
TOE Name	Juniper Networks Junos Pulse Access Control Service

TOE Version	Version 4.2 R4
Security Target Title	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2 R4
Security Target Version	v1.3
Security Target Date	30 May 2013
Assurance Level	Evaluation Assurance Level 3 augmented (EAL3+) with ALC_FLR.2.
Criteria	Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL3 augmented with ALC_FLR.2 (EAL3+ ALC_FLR.2)
Sponsor and Developer	Juniper Networks, Inc. 1194 North Matilda Avenue, Sunnyvale, California 94089-1206 Unites States
Evaluation Facility	BAE Systems Detica MySEF

1.3 Security Policy

6 The TOE enforces an information flow control policy between authenticated users and protected resources logically behind the appliance based on user roles and resource types. Administrators have the ability to establish rules that permit or deny information flows based on the combination of attributes.

7 Users will request for information access (such as reading, writing, or deleting a file or accessing an internal Web server) to a network in the IT environment. They are granted access if they successfully authenticate to the TOE and the endpoint is compliant to the Host Checker Policy or the endpoint MAC address is contained within an exception list. If the authentication is successful but the endpoint is not compliant to a Host Checker Policy, the endpoint may be remediated in an isolated area of the network to attain compliance with the Host Checker Policy then gain access.

8 The details of the security policy are described in Sections 6 and 7 of the Security Target (Ref [6]).

1.4 TOE Architecture

9 The TOE includes both logical and physical boundaries which are described in detail Section 1.7 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

10 The TOE implements and controls the security features listed below:

a) **Security audit**

The TOE generates audit records for security events. These logs are stored locally, and the system can also send them to an external SYSLOG server for alternative storage. The logs are divided into the following categories and are maintained separately:

i. Event logs – used to track system related events such as start-up and shutdown,

ii. Admin access logs – used to record administrator generated events, and

iii. User access logs – record user access events such as retrieving a file.

The log details and list of events where the TOE will generate the logs are listed in Section 6.1.1.1 and Section 7.2 of the Security Target (Ref [6]).

The logs are only accessible through the web-based administrative interface, in which only authenticated administrators are authorised to access. Administrators can view, clear, save the logs. When logs are saved from the TOE, they are transferred to the PC connected to the web-based administrative interface. The administrator also has the ability to change the log settings.

b) **Cryptographic support**

The TOE provides an encrypted path between users and itself. The secure connection ensures that user password and data are protected from modification and disclosure. The TOE use TDES and AES encryption algorithms with 128 bit, 192 bit or 256 bit key sizes to provide the secure communication. AES and TDES keys are generated with an ANSI X9.31 pseudo-random number generator and are used as session keys for TLS sessions. Cryptographic key distribution is implemented via the TLS protocol.

c) **Information flow control**

The TOE enforces an information flow policy between authenticated users and protected resources logically behind the appliance. Users will request for information access (such as reading, writing, or deleting a file or accessing an internal Web server) to a network in the IT environment. They are granted access if they successfully authenticate to the TOE and the endpoint is compliant to the Host Checker Policy or the endpoint MAC address is contained within an exception list. If the authentication is successful but the endpoint is not compliant to a Host Checker Policy, the endpoint may be remediated in an

isolated area of the network to attain compliance with the Host Checker Policy then gain access.

The TOE supports predefined rules that check for antivirus software and up-to-date virus signatures, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. Additionally, the TOE supports custom rules that use integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs) to perform customised client-side checks. Custom rules also allow the TOE to check for third party DLLs that perform customised client side checks. Finally, custom rules can check for ports, processes, files, registry key settings, and the NetBIOS name, MAC addresses or certificate of the client machine.

The examples above apply to Windows-based machines. For Mac OS, Linux, and Solaris the TOE can check for ports, processes, and files only.

d) **Identification and authentication**

All users, including administrators, are required to perform identification and authentication before any information flows are permitted. The TOE has the ability to authenticate users locally using a password or can integrate with a remote authentication server. In the evaluated configuration, the TOE will perform the authentication locally. The users will enter a username and password which will be validated by the TOE against the information stored by the TOE. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

The TOE ensures authentication parameters to meet the following:

i. Minimum of eight (8) characters,

ii. Minimum of three (3) numeric characters,

iii. Minimum of three (3) alphabetic characters,

iv. Combination of both uppercase and lowercase alphabetic characters,

v. Different from the username, and

vi. Different from the previously used password

The TOE associates an operator to a role by associating the username with the proper role once successful authentication occurs. Successful authentication is required prior to giving a user access to the system. These mechanisms are used for administration of the routing functions as well as the administration of the operator accounts used for management.

e) **Security management**

The TOE provides a wide range of security management functions. The Administrator logs onto the TOE from a protected network and performs all management functions through the browser interface. The administrator has the ability to control all aspects of the TOE configuration including: user management, information flow policy management, audit management, and system start-up and shutdown.

The TOE also provides a console port for certain management capabilities, such as configuring the network relevant information pertaining to the internal and external network interfaces. However, the console port does not provide the management capabilities necessary to utilise the security management functionalities claimed within this ST.

Administrators set the information flow policy rules on a per user basis. When the administrator adds a new user, the administrator defines the user access. Although users are grouped into roles, administrators can create rules that except specific users from the constraints of their role. By default, user access is restrictive but the administrator may override the default upon rule creation.

The TOE provides a timestamp for its own use. The timestamp is generated from the clock provided in the hardware. Communications between TOE components (client and appliance) are encrypted via a secure connection in order to protect the traffic from disclosure and modification.

1.4.2 The Physical Boundaries

11 The TOE includes the appliance and software client running on a remote IT system. The appliance TOE component is completely self-contained, housing the software and hardware necessary to perform all functions. The TOE boundary is shown in Figure 1 below.

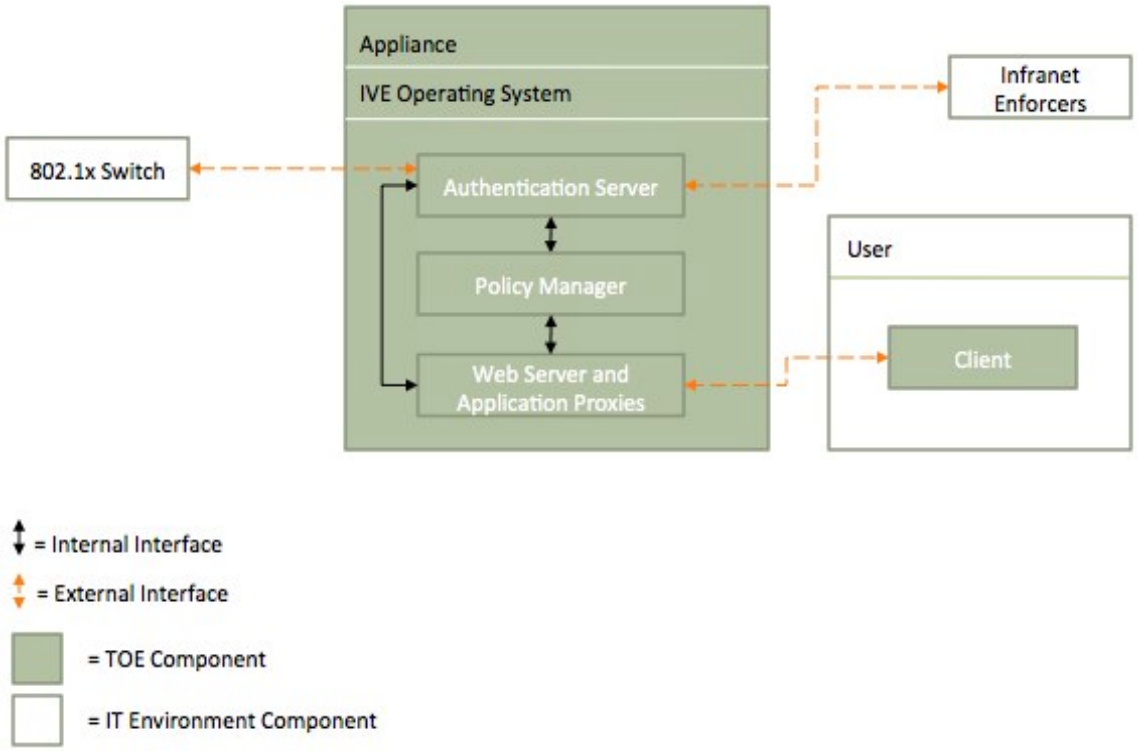

Figure 1: TOE Boundry

12 The TOE is composed of the following components:

a) Authentication Server – verifies the credentials presented by the user (or presented by the Authenticator on behalf of the user) and associates the user

with an access policy. The Authentication Server may use its integrated database, or it may consult an external authentication server. The interface to an external database may be RADIUS, or it may be a more generic database interface (e.g., LDAP).

b) Policy Manager – interfaces with external enforcement points like Juniper firewalls. It uses proprietary interfaces to set the access privileges of users that connect through those enforcement points.

c) Web Server and Application Proxies – provides the main interface for both users and administrators of the TOE. The web server provides users an interface to submit connection requests via an HTTPS encrypted tunnel. The web server provides administrators an interface to administrate the TOE using a web browser. The web server component is included as part of the TOE and this includes application proxies to govern the use of and access to applications on the protected network.

d) Software clients – open and manage a secure connection to the appliance in order to request network access.

13 The details of TOE physical scope are described in Section 1.7.1 of the Security Target (Ref [6]).

1.5 Clarification of Scope

14 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures such as physical access protection, non-hostile and well-managed user community in accordance with administrator guidance that is supplied with the product.

15 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]). The operating systems and the hardware running the software clients are outside the scope of the evaluation.

16 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

17 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE as defined in subsequent sections and in the Security Target Ref ([6]).

1.6.1 Usage assumptions

18 Assumptions for the TOE usage listed in the Security Target are:

a) 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.

1.6.2 Environmental assumptions

19 Assumptions for the TOE environment listed in the Security Target are:

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

1.7 Evaluated Configuration

20 The TOE is the appliance and software client running on a remote IT system, as described in Section 1.7.1 of the Security Target (Ref [6]). The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 31).

21 The evaluated configuration for the TOE encompasses three components:

a) Appliance software: Juniper Networks Junos Pulse Access Control Service 4.2 R4,

b) Appliance hardware: as per listed in Table 3 of the Security Target (Ref [6]), and

c) Client software: as per listed in Table 3 of the Security Target (Ref [6]).

1.8 Delivery Procedures

22 UAC is delivered to the customers using the delivery procedure (Ref 31a)), which ensures that the TOE is securely transferred from the development environment into the responsibility of the customer. The delivery procedures are outlined below.

23 Upon receipt by Juniper, customer orders are processed by Juniper Order Management where all subsequent processing (shipment transaction, package slip generation, and invoice generation) will take place.

24 UAC will be produced by authorised contract manufacturers. The appliances are uniquely labelled using an adhesive-backed thermal label that contains unit model number, unit serial number and in some instances the MAC address. These labels are printed during the manufacturing process by the contract manufacturers and affixed to the unit during final packaging of the box.

25 Juniper packages and labels the product in accordance with the current bill of material (BOM) and any applicable package specification for the product to be shipped.

26 Each hardware appliance is wrapped in a plastic bag to provide resistance against moisture. Then the appliance is enclosed in cardboard shipping boxes and sealed with tape that does not contain a Juniper logo. 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.

27 Juniper employs 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.

28 The recipient can verify 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. It is assumed that the trusted carriers provide reasonable measures to protect the products from tampering during shipping.

29 There are several mechanisms provided in the above process for a customer to ensure that they are receiving a box sent by Juniper that has not been masqueraded by another company or entity:

a) 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:

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.

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

b) 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.

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.

1.9 Documentation

30 To ensure continued secure usage of the product, it is important that the TOE is used in accordance with the guidance documentation.

31 The following documentation is provided by the developer to the end user as guidance to ensure secure installation and operation of the product:

a) Secure Delivery Processes and Procedures : Juniper Networks Junos Pulse Access Control Service 4.2R4, v1.1, 30 October 2012

b) Operational User Guidance and Preparative Procedures Supplement : Juniper Networks Junos Pulse Access Control Service 4.2 R4, v1.2, 30 October 2012

c) Quick Start Guide: Juniper Networks Junos Pulse Access Control Service 4.2R4, v4.0, 27 January 2011

d) Administrator Guide: Juniper Networks Junos Pulse Access Control Service 4.2R4, v4.1, 30 January 2011

e) Juniper Networks Unified Access Control Installation Guide (IC4500/IC6500), 530-029910-01 Rev 01, 2009

f) Troubleshooting Guide: Juniper Networks Junos Pulse Access Control Service 4.2R4, v4.0, 25 January 2011

2 Evaluation

32 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 3 augmented with ALC_FLR.2 (EAL3+ ALC_FLR.2). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

33 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

34 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be consistent with the provided evidence.

35 It is evaluated that the implemented configuration management system can control changes to those items that have been placed under configuration management system. The developer's configuration management system was also observed during the site visit, and it was found security flaws under configuration management ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution. This is evaluated to be consistent with the provided evidence.

36 During the site visit the evaluators examined the development security documentation and determined that it detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the TOE design and implementation. The evaluators confirmed that the developer used a documented life-cycle model which provides necessary control over the development and maintenance of the TOE by using the procedures, tools and techniques described by the life-cycle model.

37 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

38 The evaluators analysed the TOE functional specification and design documentation; they determined that the design completely and accurately describes the TOE

security functionality (TSF) interfaces, and the TSF subsystems. The design described the TOE subsystems to sufficiently determine the TSF boundary. It provides a detailed description of the SFR-enforcing subsystems and enough information about the SFR supporting and SFR-non-interfering subsystems for the evaluator to determine that the SFRs are completely and accurately implemented.

39 The evaluators analysed the TOE security architectural description and determined that the delivery and installation process was secure and the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

2.1.3 Guidance documents

40 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

41 Testing at EAL3 consists of assessing developer tests, performing independent function test, and performing penetration tests. The TOE testing was conducted by evaluator from BAE Systems Detica MySEF at BAE Systems Detica MySEF Lab, Kuala Lumpur and at the developer's site where it was subjected to comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

42 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

43 The evaluators analysed the developer's test coverage and depth analysis, and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the implementation representative, functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

44 Independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentations, executing a sample of the developer's test plan, and creating test cases that augmented the developer test.

45 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
To test that TSF shall be able to generate an audit record for the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [*not specified*] level of audit; and To test that TSF shall record within each audit record at least the following information. a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST.	FAU_GEN.1, FMT_SMT.1, FIA_UID.2, FIA_UAU.2, FDP_IFF.1, FPT_STM.1, FMT_MOF.1, FIA_ATD.1	Administrator Interface	**PASS.** The TOE does generate an audit record as claimed.
To test that the TSF shall provide an Administrator with the capability to read all audit information from the audit records in a manner suitable for the user to interpret the information.	FAU_SAR.1, FIA_ATD.1	Administrator Interface	**PASS.** The administrator and Read-Only Administrator are able to read and interpret audit record.
To test that the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [ANSI X9.31] and specified cryptographic key sizes	FCS_CKM.1, FCS_COP.1	Administrator Interface and End user interface	**PASS.** The TOE is able to configure using cryptographic key length of at least 128 bits.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
[128-, 192-, or 256-bit AES key and 168-bit TDES key] that meet the following: [FIPS 197 for AES and FIPS 46-3 for TDES].			
To test that TOE can be configured to only accept a cryptographic key length of at least 168 bits.	FCS_CKM.2	End user interface	**PASS**. The TOE is able to configure using AES/3DES cipher suites with the use of cryptographic key lengths of at least 168 bits.
To test that the TSF shall enforce the [NAC Information Flow Control SFP] based on the following types of subject and information security attributes. To test the TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation.	FDP_IFF.1	End user interface	**PASS**. Non-compliant end user was unable to authenticate to TOE due to access restriction defined in policy.
To test that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	FAU_UAU.2	Administrator Interface and End user interface	**PASS.** The end user can only access resources upon successfully authentication.
To test that read-only admin cannot create, delete, modify, or view resource policy rules that permit or deny resource requests.	FMT_MOF.1	Administrator Interface	**PASS.** Read-Only admin is not able to create/ modify/ delete Host Checker policies.
To test that user without proper authorisation cannot manage security attributes.	FMT_MSA.2	Administrator Interface	**PASS.** User without proper authorisation cannot manage security attributes.
To test that user with default TOE settings cannot telnet/ssh to backend servers.	FDP.IFF.1 and FMT_MSA.3	Administrator Interface and Network Interface	**PASS.** Unable to telnet/ssh to backend servers.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
To test that admin user can create, delete, modify, and view resource policy rules that permit or deny resource requests.	FMT_SMF.1.1	Administrator Interface	**PASS.** The TOE administrator can create, delete, modify, and view resource policy rules that permit or deny resource requests.
To test the default user/admin realm and roles.	FMT_SMR.1	Administrator Interface	**PASS.** The TOE does have default user/admin realm and roles.
To test that the basic Internal TSF data transfer is protected.	FPT_ITT.1.1	End user and network interface	**PASS.** Data transferred between the TOE and Client is encrypted.

46 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

47 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE and to determine whether these were exploitable in the intended operating environment of the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, security architecture description, and implementation representation.

48 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE, in its operational environment, is resistant to attack performed by an attacker possessing a Basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

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

49 The penetration tests focused on:

a) Man in the middle attack;

b) Input manipulation;

c) Fuzzing; and

d) Injection.

50 The results of the penetration testing note that there is no exploitable vulnerability and/or residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.4 Testing Results

51 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

52 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing a Basic attack potential.

3 Result of the Evaluation

53 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Juniper Networks Junos Pulse Access Control Service 4.2 R4 performed by the BAE Systems Detica MySEF.

54 The BAE Systems Detica MySEF found that Juniper Networks Junos Pulse Access Control Service upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL3+ ALC_FLR.2.

55 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

56 EAL3 provides assurance by a full Security Target (ST) and an analysis of the security functions in the ST, using a functional and complete interface specification, guidance documentation, and an architectural description of the TOE design to understand the security behaviour.

57 The analysis is supported by independent testing of the TOE security functions, 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. However, in this evaluation, the lifecycle support evaluation is performed by the evaluator assuming a flaw reporting procedures of High based on ALC_FLR.2 requirements.

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

59 EAL3 represents a meaningful increase in assurance 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.

3.2 Recommendation

60 In addition to ensure secure usage of the product, below are additional recommendations for Juniper Networks Junos Pulse Access Control Service 4.2 R4 consumers:

a) The users and administrators of the TOE should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

b) Appropriate network layer protection; the network on which the TOE is installed must be both physically and logically protected.

c) System Administrator ensures that the TOE is correctly configured and performs annual testing to confirm that all vulnerabilities have been suitably addressed.

Annex A References

A.1 References

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

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] Security Target: Juniper Networks Junos Pulse Access Control Service 4.2 R4, v1.3, 30 May 2013.

[7] Evaluation Technical Report: EAL3+ ALC_FLR.2 Evaluation of Juniper Networks Junos Pulse Access Control Service Version 4.2 R4, v1.1, 31 May 2013.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
AES	Advanced Encryption Standard
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
ISCB	Information Security Certification Body
ISO	International Standards Organisation
LDAP	Lightweight Directory Access Protocol
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
NAC	Network Access Control
PP	Protection Profile
RADIUS	Remote Authentication Dial-in User Service
SFP	Security Function Policy
SSH	Secure Shell
ST	Security Target
Syslog	System logging as specified in Request for Comment 5424
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UAC	Unified Access Control

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Certificate	An electronic attestation which links the SVD to a person and confirms the identity of that person.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA.
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65.

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.

--- END OF DOCUMENT ---