C083 Certification Report

Valari Web Application Firewall v10.3.11

File name: ISCB-3-RPT-C083-CR-v1
Version: v1
Date of document: 24 November 2017
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

C083 Certification Report

Valari Web Application Firewall v10.3.11

24 November 2017

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:	C083 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C083-CR-v1
ISSUE:	v1
DATE:	24 November 2017

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

Foreword

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 24 November 2017, 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).

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 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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
d1	3rd November 2017	All	Initial draft
v1	13TH November 2017	vii, 1, 17	Change typing error and name of TOE.

Executive Summary

VALARI Web Application Firewall & Security Management System v10.3.11 is the TOE which designed to secure web applications from the attacks and provide a security layer by proxy-ing all HTTP(S) traffic and shield web servers and databases from direct access of the attackers irrespective of the underlying application vulnerabilities.

Valari has the following functionalities as following:

a) Detect and Block Vulnerabilities and Web Application Threats.

b) Full Web Traffic Logging

c) Web Intrusion Detection with Just-In Time Monitoring and Detection

d) Built-in Anti-evasion and Encoding validation mechanisms

e) Protected protocols

f) Attack Prevention and External Patching / Virtual Patching

g) Flexible Rule Engine

h) Geo-location Blocking and;

i) Integrated Security Rules.

However, there are some functionalities which are not part of the scope as below:

a) The key generation, distribution and operation

b) VALARI configurations modification

c) All hardware appliance and operating system

d) Administrator role by KTSB service personnel.

The TOE scope of evaluation covers various major security functions described as below:

a) Identification and Authentication

b) User Data Protection

c) Security Management

d) Security Audit

Table of Contents

Executive Summary vii

Table of Contents viii

Index of Tables ix

Index of Figures ix

1 Target of Evaluation 1

1.1 TOE Description 1

1.2 TOE Identification 3

1.3 Security Policy 4

1.4 TOE Architecture 5

1.4.1Logical Boundaries *5*

1.4.2 Physical Boundaries *6*

1.5 Clarification of Scope 7

1.6 Assumptions 8

1.6.1 Usage assumptions *8*

1.6.2 Environment assumptions *8*

1.7.1 Domain Separation *9*

1.7.2 Initialisation *9*

1.8 Delivery Procedures 11

1.8.1Procurement by customer *11*

1.8.2 Preparing the delivery package *11*

1.8.3 Receipt and Verification *11*

2 Evaluation 12

2.1 Evaluation Analysis Activities 12

2.1.1 Life-cycle support 12

2.1.2 Development 12

2.1.3 Guidance documents 13

2.1.4 IT Product Testing *13*

2.1.4.3 Penetration Testing *16*

2.1.4.4 Testing Results *17*

3 Result of the Evaluation 18

3.1 Assurance Level Information 18

3.2 Recommendation 18

Annex A References 20

A.1 References 20

A.2 Terminology 20

A.2.1 Acronyms 20

Table 4: List of Acronyms 20

A.2.2 Glossary of Terms 21

Table 4: Glossary of Terms 21

Index of Tables

Table 1: TOE identification 3

Table 2: Organisational Security Policies 4

Table 3: Independent Functional Test 14

Table 4: List of Acronyms 20

Index of Figures

Figure 1: VALARI Hardware Appliance 7

Figure 2: Typical TOE deployment 7

1 Target of Evaluation

1.1 TOE Description

1 VALARI Web Application Firewall & Security Management System v10.3.11 is the TOE which designed to secure web applications from the attacks and provide a security layer by proxy-ing all HTTP(S) traffic and shield web servers and databases from direct access of the attackers irrespective of the underlying application vulnerabilities.

2 VALARI consist of functionalities such as:

a) **Detect and Block Vulnerabilities and Web Application Threats:** TTP Distributed Denial of Service (DDoS), HTTP Flooding and Slow HTTP DoS Attacks, Brute Force Login, OS Command Injection, Parameter / Form Field Tampering, Data Disclosure, Phishing Attacks, SQL Injection, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS), Drive-by-Downloads, Directory Traversal, Buffer Overflow, Cookie Injection, Cookie Poisoning, Site Reconnaissance, Data Destruction, Remote File Inclusion Attacks, Google Hacking, Anonymous Proxy Vulnerabilities, HTTP Response Splitting, HTTP Verb Tampering, HTTP Parameter Pollution Attack, Malicious Encoding, Malicious Robots, Known Worms, Web Services (XML) attacks, Session Hijacking, Site Scraping, Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI), Web server software and operating system attacks, Zero Day Web Worms, Forceful Browsing of Website Content, Automated Botnet Attacks and Manipulation of Query String Parameters.

b) **Full Web Traffic Logging:** contents in the web Request bodies are not logged by the web servers and hence attackers use POST requests to delivery exploits and it goes completely blind on the web server logs. With full HTTP transaction logging in VALARI, it is possible to log all requests and responses. This Logging feature can be controlled on what and when a log is created. VALARI can be configured to mask the sensitive data in the request and/or response fields before they are written to the audit log.

c) **Web Intrusion Detection with Just-In Time Monitoring and Detection:** Web Traffics are monitored real time to detect attacks and react on suspicious events / data that hit your web applications.

d) **Built-in Anti-evasion and Encoding validation mechanisms:** To normalize inputs so as to prevent anti-evasion techniques (eg HexCoding, urlEncode, Nulls)

that hackers typically use to get around web security defences.

e) **Protected protocols:** HTTP, HTTPS (SSL), XML, Web services, SOAP and AJAX. Basically anything that you use anticipate an enduser to use a browser for connecting to your web servers and more.

f) **Attack Prevention and External Patching / Virtual Patching:** VALARI acts immediately to prevent attacks from reaching the web applications. With more than 20,000 specific rules, VALARI is an ideal external patching tool. External patching (referred to as Virtual Patching) is about reducing the window of opportunity as the time needed to fix / patch application vulnerabilities often take weeks to months. With VALARI, application vulnerabilities can be patched from the WAF Layer without patching the application source code making your applications secure until a proper patch is applied to the application by your development team or vendors.

g) **Integrated Security Rules:** from various public vulnerability data signature sources and VALARI correlates data from all these numerous sources to generate the Flexible – Scalable – Reliable rules, automatically updating daily and as needed. Various vulnerability data signature sources include:

3 However, some of the functionalities in VALARI Web Application Firewall v10.3.11 are excluded from the evaluation scope such as:

- The key generation, distribution and operation
- VALARI configurations modification
- All hardware appliance and operating system
- Administrator role by KSTB service personnel

4 The TOE scope of evaluation covers various major security functions described as below:

- **Identification and Authentication:** The TOE enables audit functionality to tracks all activities within the TOE boundary network inclusive of its own operations as TOE Application Server.
- **User Data Protection:** The TOE protects the web application from external network intrusions by using information flow control between internal and external network. The TOE will log all HTTP requests and responses before allowing or rejecting the HTTP requests. KTSB service personnel could configure

HTTP filter rules and policies based on the subject and information security attributes. By default, all external (Internet) traffic will be blocked. KTSB service personnel can configure rules for application vulnerabilities, signature patterns, evasion patterns and Geo-location blocking. However, the modification or changes to rules are not part of the scope of evaluation.

- **Security Management:** TOE functions can be managed through command-line interface. The TOE only allows limited user access to run a limited set of commands. These do not affect the running mode of the TOE. User can view settings and logs but cannot modify configuration. Only KTSB service personnel are able to modify configurations upon request (eg whitelisting/blacklisting). However, the modification or changes to rules are not part of the scope of evaluation. KTSB service personnel role is not part of the scope.
- **Security Audit:** The TOE will generate audit records for HTTP Request and responses. Each audited events will be recorded along with date and time of event, source IP, account user who performed the event, event name, system filename related to event and other event details. Audit records can be viewed by user and cannot be edited. Users are not able to delete or otherwise modify said audit log. User could select for viewing. Full audit reports are emailed every night to the designated email address together with an executive summary. TOE will create a new log file to store the audit records if the size limit is reached for a log file. The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. TOE prevents modification of date and time manually. The user has not ability to change date/time/time-zone. All these are set by KTSB service personnel, and the TOE is continuously clock-synchronized with a pool of NTP servers. However, the setting of date/time/time-zone by KTSB personnel are not part of the scope of evaluation.

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	C083
TOE Name	VALARI Web Application Firewall

TOE Version	V10.3.11
Security Target Title	Valari Security Target
Security Target Version	v0.5
Security Target Date	25 September 2017
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor and Developer	Kaapagam Technologies Sdn Bhd. B15-15, I-SOVO@I-City No. 6, Persiaran Multimedia, Section 7 40000 Shah Alam, Selangor Darul Ehsan
Evaluation Facility	Across Verticals – MySEF

1.3 Security Policy

6 The Organisational Security Policies (OSP) is imposed by an organisation to secure the TOE and its environment.

7 The details of the OSP are identified in Table 2 below.

Table 2: Organisational Security Policies

P.ROLE	Only authorized person assigned by the organisation have access to the TOE.
P.PASSPHRASE	Authorized user shall use complex passphrase to generate private and public key.

1.4 TOE Architecture

8 The TOE includes both logical and physical boundaries which are described in Section 1.5 of the Security Target (Ref [6])

1.4.1 Logical Boundaries

9 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality in Table 3:

Table 3: Logical Boundaries

Security function	Description
Identification and Authentication	TOE user can access TOE by providing username and public key in the command-line interface. KTSB will create a user account for the given user using their public key for authentication.
User Data Protection	TOE protects the web application from external network intrusions by using information flow control between internal and external network. The TOE will log all HTTP requests and responses before allowing or rejecting the HTTP requests. KTSB service personnel could configure HTTP filter rules and policies based on the subject and information security attributes. By default, all external (Internet) traffic will be blocked. KTSB service personnel can configure rules for application vulnerabilities, signature patterns, evasion patterns and Geo-location blocking. However, the modification or changes to rules are not part of the scope of evaluation.
Security Management	TOE functions can be managed through command-line interface. The TOE only allows limited user access to run a limited set of commands. These do not affect the running mode of the TOE. User can view settings and logs but cannot modify configuration. Only KTSB service personnel are able to modify configurations upon request (eg whitelisting/blacklisting). However, the

	modification or changes to rules are not part of the scope of evaluation. KTSB service personnel role is not part of the scope.
Security Audit	The TOE will generate audit records for HTTP Request and responses. Each audited events will be recorded along with date and time of event, source IP, account user who performed the event, event name, system filename related to event and other event details. Audit records can be viewed by user and cannot be edited. Users are not able to delete or otherwise modify said audit log. User could select for viewing. Full audit reports are emailed every night to the designated email address together with an executive summary. TOE will create a new log file to store the audit records if the size limit is reached for a log file. The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. TOE prevents modification of date and time manually. The user has not ability to change date/time/time-zone. All these are set by KTSB service personnel, and the TOE is continuously clock-synchronized with a pool of NTP servers. However, the setting of date/time/time-zone by KTSB personnel are not part of the scope of evaluation.

1.4.2 Physical Boundaries

10 The TOE consist of the following components which are:

- Hardware appliance includes the physical port connection. Refer Table 1 for more details. Refer Figure 1 and Figure 2 for the physical presentation of hardware appliance.

- VALARI OS
- VALARI User Guide

Figure 1: VALARI Hardware Appliance

11 However, all the hardware appliance and operating system are not part of the scope in evaluation.

12 The TOE must be placed in a secure physical area where only authorized users are granted physical access to the TOE. TOE user could view configurations and logs TOE through the command-line interface by using SSH client (Win32 – putty, Unix – built-in). VALARI does not use SSH password but using PKI with mandatory SSH key.

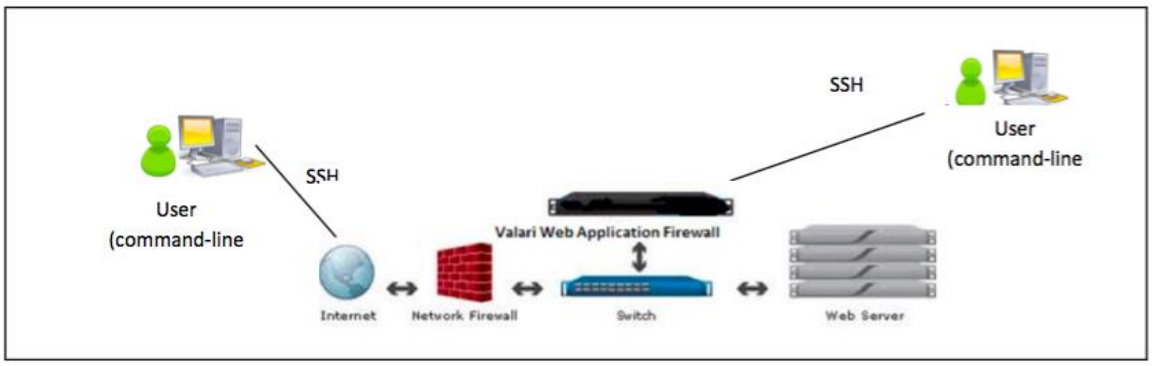

Figure 2: Typical TOE deployment

1.5 Clarification of Scope

13 The TOE is designed in order to secure the web applications from any attacks and provide a layer of security by proxy-ing all HTTP(s) traffic and shield web servers and databases from direct access of the attackers irrespective of the underlying application vulnerabilities.

14 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]). The TOE is an endpoint

management system that enables consumer to manage their assets such as desktops, laptops and servers in the organization and; perform management of assets, maintenance of assets, security perimeters protections and secure access controls of the assets through secure communications within the internet networks.

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

1.6 Assumptions

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

1.6.1 Usage assumptions

17 Assumption for the TOE usage as listed in Security Target:

a) HTTP traffic cannot flow through internal and external network unless it passes through the TOE.

b) User's public and private keys are generated, distributed and used securely for SSH client.

c) The TOE Administrator (KTSB Service personnel) will be non-hostile and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.

1.6.2 Environment assumptions

18 Assumption for the TOE environment listed in Security Target are:

a) The TOE and its environment are physically secure.

b) TOE environment and TOE configurations and rules are pre-configured securely.

c) The TOE environment will provide reliable time stamps.

d) The TOE environment will provide a secure connection between TOE and users.

1.7 Evaluated Configuration

19 There are three main components of the TOE to be evaluated which are:

1.7.1 Domain Separation

20 The TOE does not provide security domains to potentially-harmful entities. The TOE management functionality described does not provide security domains, but is a direct implementation of the security requirements. In short, security domains are not applicable for this TOE.

1.7.2 Initialisation

21 After the TOE securely delivered to the customer, the TOE will be in inactive state where it configurations are not yet configured. User needs to determine the relevant IP, Subnet and Gateway address for TOE, the PKI key and list of web application servers that will be mediated by TOE. However, all the configurations will be configuring in the TOE by KTSB service personnel.

22 SSH PKI key is generated for establishing secure communication with TOE. User will need to provide a secure passphrase in generating the private and public key. The public key shall then be submitted to KTSB service personnel to be embedded in the TOE configurations.

23 Once KTSB service personnel obtain the required information for the configurations, configured the TOE, only then the TOE will be in its initial secure state.

24 User shall access the TOE using SSH client, Putty by configured IP address with the default port. User shall produce their username to access the TOE.

1.7.3 Protection from Tampering

1.7.3.1 Physical Protection

25 TOE appliance sealed with a security tape at the casing to avoid product being tampered during distribution to the customer. If the security tape is broken, unauthorized person may have tampered the TOE.

26 TOE appliance shall be located in a physically secure facility to ensure unauthorized access prevented.

1.7.3.2 Logical

27 The TOE is administered through a command-line interface (CLI). By not using GUI as medium for TOE administration, it will reduce the attack surface for the TOE, hence reduce the risk for TOE from being tampered.

28 The communication from TOE to the user is an encrypted communication using SSH. If someone sniffed the network, the attacker could only obtain the ciphertext of the communication.

29 User's username and PKI is enforced by the TOE to protect unauthorized user from accessing the TOE from SSH connection.

30 User is only allowed to invoke certain commands from the CLI. This control reduces the risk of user from changing unnecessary TOE configurations which is pre-configured by KSTB service personnel.

1.7.4 Protection from Bypassing

31 TSF ensures that the security functionality is always invoked and hence, with the self-protection (as described earlier in this document) and correct functional behaviour (as described in the FSP/TDS/ATE evaluation evidence), the SFRs are always enforced.

32 TOE is not by passable dependent on trusted path SSH for remote access. The communication is encrypted throughout the session establishment.

1.8 Delivery Procedures

33 Delivery process of the TOE to the customer for installation and use is as follows:

34 The following procedures will be performed by Kaapagam personnel in maintaining security when distributing Valari to the customer:

1.8.1 Procurement by customer

35 The customer will purchase the product and complete the payment. Once payment is confirmed and legal documentations have been completed, Kaapagam personnel can proceed with preparing and delivering the product.

1.8.2 Preparing the delivery package

36 Kaapagam personnel will make the necessary preparation:

a) Prepare the User Guide document for Valari

b) Label the Valari appliance with Valari identification and serial number.

c) Apply security tape at the Valari casing to avoid the product being tampered during distribution to customer.

d) The product will be hand-delivered to customer

1.8.3 Receipt and Verification

37 Once the package is delivered, the customer is expected to perform the following measures:

a) Receive the package.

b) Acknowledge received items receipt.

38 Kaapagam personnel will keep the Acknowledge received items as proof of product receipt. Customer is expected to fill in the Valari Setup Sheet document and return back to Kaapagam personnel for Valari deployment. Customer is also expected to use the Valari Web Application Firewall User Training for operating Valari. Customer acceptance of product will be based on passing the metrics in Valari Web Application Firewall - User Acceptance Testing.

2 Evaluation

39 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). 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

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

2.1.1 Life-cycle support

41 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items 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 evaluated, and it was found to be consistent with the provided evidence.

42 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

43 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

44 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

45 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

46 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

47 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from Across Verticals-MySEF. 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

48 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).

49 The evaluators analysed the developer's test coverage 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 functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

50 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

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

Table 3: Independent Functional Test

Identifier	Description	Results
AVCC002 -F001	This test aims to verify that the TOE able to generate an audit record of the auditable events (HTTP request and response). In additional, the TOE able to record within each audit record at least the following information: a) Date and time of the event b) Source IP c) Event d) d) Event details	PASS. Result as expected.
AVCC002 -F002	This test aims to verify that the TOE provide user with the capability to read all audit trail data from the audit records in a manner suitable for the user to interpret the information.	PASS. Result as expected.
AVCC002 -F003	This test aims to verify that the web attack logs are selectable or filterable.	PASS. Result as expected.
AVCC002 -F004	The test aims to verify the TOE able to protect the stored audit records in the audit trail from unauthorised deletion.	PASS. Result as expected.
AVCC002 -F005	This test aims to verify that TOE can enforce the Unauthenticated Information Flow Control SFP on a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another; b) information: traffic sent through the TOE from one subject to another; c) c) operation: allow/reject information.	PASS. Result as expected.

Identifier	Description	Results
AVCC002 -F006	This test aims to verify the following items: TOE able to enforce the Unauthenticated Information Flow Control SFP based on the following types of subject and information security attributes: a) subject security attributes: • Presumed signature b) information security attributes: • Presumed address of source subject (whitelist/blacklist); TOE shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: a) Subject on an internal network can cause information to flow through the TOE to another connected network if: • all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created based on: - web application attack b) Subjects on the external network can cause information to flow through the TOE to another connected network if: • all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created based on: - web application attack TOE able to deny an information flow based on the following rules: • Reject requests for access or services where the information arrives on an internal or external TOE interface, and the presumed signature is defined based on: - web application attack	PASS. Result as expected.
AVCC002 -F007	The test aims to verify the security attributes stored belonging to valid users.	PASS. Result as expected.

Identifier	Description	Results
AVCC002 -F008	This test aims to verify that TOE requires each user to be successfully authenticated before allowing the user to perform any other TSF-mediated actions (command) such as below: • uptime: shows how long the unit has been powered up since last reboot/shutdown. Also shows load average over 1 minute, 5 minutes and 15 minutes. For minute by minute load, the first load avg is relevant. For longer term load, the 15 minutes average is more useful. • show-array: shows the status of the ZFS flash mirrored array • show-network: shows network capture over the active WAN interface • show-realtime: show a continuously rolling capture of realtime attacks • show-realtimeall: show a continuously rolling capture of realtime WAF messages • show-sqli: show all sql injection attacks in pagination mode • show-rfi: show all remote file inclusion attacks in pagination mode • show-xss: show all cross-site scripting attacks in pagination mode find-string: displays blocks by string or FQDN	PASS. Result as expected.
AVCC002 -F009	This test aims to verify that TOE able to restrict the ability to view the logs to user	PASS. Result as expected.
AVCC002 -F010	The test aims to ensure that TSF able to maintain and associate the user roles.	PASS. Result as expected.
AVCC002 -F011	This test aims to verify that TOE will enforce the access control policy to provide permissive default values for security attributes that are used to enforce the SFP and TOE administrator is allowed to specify alternative initial values to override the default values when an object or information is created.	PASS. Result as expected.
AVCC002 -F012	This test aims to verify that TOE able to provide reliable time stamps for the TSF functions.	PASS. Result as expected.

2.1.4.3 Penetration Testing

52 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public

domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

53 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE 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 (elapse 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 for exploitation.

54 The penetration tests focused on:

a) SSH Authentication Attack

b) WAF Bypass

55 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in Section 4 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

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

3 Result of the Evaluation

57 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 Valari Web Application Firewall v10.3.11 performed by Across Verticals – MySEF.

58 Across Verticals – MySEF, found that Valari Web Application Firewall v10.3.11 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL2).

59 Certification is not 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. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

60 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

61 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, 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.

62 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

63 In addition to ensure secure usage of the product, below are additional recommendations for TOE users:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The user should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

c) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE.

d) The TOE User keeps updated the administrator (external) to review the audit trail generated and exported by the TOE periodically.

e) The users must ensure appropriate network protection and firmware is maintained, the network on which the TOE is installed must be both physically and logically protected, commensurate with the sensitivity of the TOE keys.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1e, CyberSecurity Malaysia, August 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1d, August 2016.

[6] Valari Security Target, Version 0.5, 25 September 2017.

[7] Valari Evaluation Technical Report, Version 1.1, 31 October 2017.

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
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
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. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.

Term	Definition and Source
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.

--- END OF DOCUMENT ---