MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C122 Certification Report

Garcinia Firewall Router v21.1.0

File name: ISCB-5-RPT-C122-CR-v1
Version: v1
Date of document: 21 June 2021
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C122 Certification Report

Garcinia Firewall Router v21.1.0

21 June 2021

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C122 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C122-CR-v1
ISSUE:	v1
DATE:	21 June 2021
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (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 29 June 2021 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 using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	11 June 2021	All	Initial draft
v1	21 June 2021	All	Final version

Executive Summary

The Target of Evaluation (TOE) is Garcinia Firewall Router v21.1.0. The TOE is a firewall and routing platform which is a self-contained appliance consisting of hardware and firmware. The TOE is a product that manages the network from any congestion and harm. The TOE analyse the incoming and outgoing network traffic, loss and manipulation of data, business secrets and confidential of data leaks.

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 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Securelytics SEF and the evaluation was completed on 2 June 2021.

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

It is the responsibility of the user to ensure that Garcinia Firewall Router v21.1.0 meets their requirements. It is recommended that a potential user of the TOE 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) is Garcinia Firewall Router v21.10. The TOE is a firewall and routing platform which is a self-contained appliance consisting of hardware and firmware.

2 The TOE is a product that manages the network from any congestion and harm. The TOE analyse the incoming and outgoing network traffic, loss and manipulation of data, business secrets and confidential of data leaks. Loss of time due to the down time is loss of money to the business.

3 Firewall are indeed important and everyone who is online must strive to have a firewall protection before it's vulnerable to external and internal. The TOE core features include Traffic Shaper, Captive portal, Forward Caching Proxy, Virtual Private Network, High Availability & Hardware Failover, Intrusion Detection and Inline Prevention, Build-in reporting and monitoring tools, Support for plugins, DNS Server & DNS Forwarder, DHCP Server and Relay, Dynamic DNS, Backup & Restore, Stateful inspection firewall, Granular control over state table, 802.1Q VLAN support and many more.

4 The following table highlights the range of security functions implemented by the TOE:

Table 1: Security Function

Security Function	Description
Stateful Traffic Filter Firewall	System Administrator and Normal User can provide rules to be used by the TOE to restrict the flow of traffic between the various networks connected to the TOE. Rules can be based on various traffic properties such as source and/or destination address, source and destination ports
Security Audit	The TOE generates audit records for security events. System Administrator and Normal User have the ability to view and export the audit and transaction log
Identification and Authentication	System Administrator and Normal User are required to identify and authenticate with the TOE prior to any user action or information flow being permitted.

Security Function	Description
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
Secure Communication	The TOE can protect the user data from disclosure and modification by using HTTPS (TLS v1.2 & TLS v1.3) as a secure communication.

1.2 TOE Identification

5 The details of the TOE are identified in Table 2: TOE Identification below.

Table 2: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C122
TOE Name	Garcinia Firewall Router
TOE Version	v21.1.0
Security Target Title	Garcinia Security Target
Security Target Version	V1.0
Security Target Date	19 May 2021
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2
Sponsor	Sigma Rectrix Systems (M) Sdn Bhd Suite 3-05 4805 CBD Perdana 2 Jalan Perdana Cyber 12 Cyberjaya 63000 Selangor

Developer	Sigma Rectrix Systems (M) Sdn Bhd Suite 3-05 4805 CBD Perdana 2 Jalan Perdana Cyber 12 Cyberjaya 63000 Selangor
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Petaling Jaya, Selangor Darul Ehsan

1.3 Security Policy

6 There is no organisational security policy defined regarding the use of TOE.

1.4 TOE Architecture

7 The TOE consist of logical and physical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

8 The logical boundary of the TOE is summarized below:

- Stateful Firewall Filtering
  System Administrator and Normal User can provide rules to be used by the TOE to restrict the flow of traffic between the various networks connected to the TOE. Rules will restrict the flow of network traffic between protected networks and other attached networks based on network addresses and ports of the network nodes originating (source) and/or receiving(destination) applicable network traffic as well as on established connection information. The rules action can be either Pass, Block or Reject. The difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
- Security Audit

  The TOE generates audit records for security events. Types of audit logs are:

  - System Log Files
  - Firewall Log Files

System Administrator and Normal User have the capability to view and export these audit and transaction logs via the web-based GUI interface.

- Identification & Authentication

  All users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to key in a valid username and password in order to access the TOE. The acceptable minimum password length is minimum eight (8) characters. The TOE checks the credentials presented by the user against the authentication information stored in the database. There are two types of users; System Administrator and Normal User.

- Security Management

  The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The TOE provides web-based GUI interface that permit the System Administrator and Normal User to configure and manage the TOE.

- Secure Communication

  The TOE provides a secure HTTPS (TLS v1.2 & TLS v1.3) between the TOE and remote users. It also provides assured identification of its end points and protection of the communicated data from modification or disclosure.

1.4.2 Physical Boundaries

9 A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

Figure 1 – TOE Physical Boundaries

10 The TOE resides between one or more internal networks (that the TOE is protecting) and an external network such as the Internet. All information transferred between the internal and external networks shall pass through the TOE.

11 There are three (3) types of hardware appliance model namely:

i) Garcinia V4

ii) Garcinia V6

iii) Garcinia V8

12 Each appliance model operates using an identical software image with identical functionality.

13 Below is the hardware specification:

Specifications \ Models	Garcinia V4	Garcinia V6	Garcinia V8
Throughput	4.5 Gbit/s	4.5 Gbit/s	20.0 Gbit/s
Concurrent Connection	7,000,000	10,000,000	12,000,000
CPU Type	Dual Core	Quad Core	Quad Core
Memory	8 GB	16 GB	32 GB
Storage	1TB HDD	1TB HDD	1TB HDD
Form Factor	Rack 1U	Rack 1U	Rack 2U
Front I/O	6 x Gigabit Ethernet 1 x Console 2 x USB2.0	6 x Gigabit Ethernet 1 x Console 2 x USB2.0	12 x Gigabit Ethernet 4 x SFP+ 1 x Console 2 x USB2.0
PCI Slot	YES	YES	YES
Dimension	450 mm x 430 mm x 44.5mm	450 mm x 430 mm x 44.5mm	550 mm x 440 mm x 88 mm
Power	220W ATX Single PSU	220W ATX Single PSU	250W ATX Single PSU
Cooling	2x Cooling Fans with Smart Fan	2x Cooling Fans with Smart Fan	2x Cooling Fans with Smart Fan
Weight	12.8 KG	12.8 KG	18.3 KG
Hardware Warranty	12 months *	12 months *	12 months *
License	Free Unlimited User	Free Unlimited User	Free Unlimited User
Certifications	RoHS, CE/FCC Class A, UL	RoHS, CE/FCC Class A, UL	RoHS, CE/FCC Class A, UL

1.5 Clarification of Scope

14 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

15 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

16 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

17 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand the requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Environmental assumptions

18 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 3: Assumptions for the TOE Environment

Environment	Statement
A.NOEVIL	System Administrator and Normal User are non-hostile and follow all administrator guidance.
A.PHYSEC	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

1.7 Evaluated Configuration

19 This section describes the configurations of the TOE that are included within the scope of the evaluation. The evaluated configuration for TOE is the firewall and routing platform which is a self-contained appliance consisting of hardware and firmware.

20 Figure 2 provides various of subsystems involved:

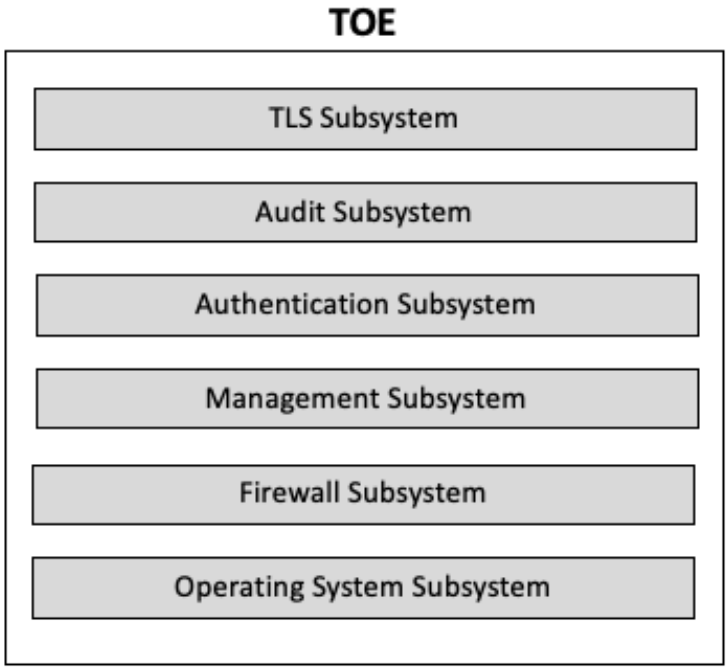
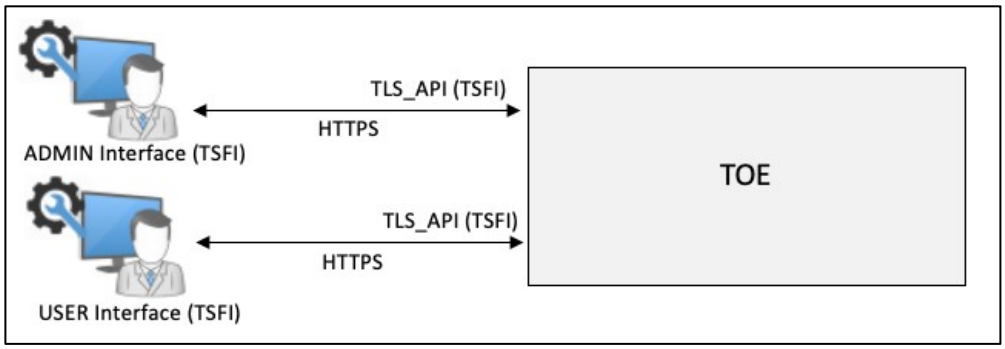


Figure 2 - TOE Subsystems

21 As depicted in Figure 3 below, the TOE has the following TSFI:

- **ADMIN Interface (SFR-enforcing).** The ADMIN interface provides a web-based interface for System Administrator to communicate with the TOE and perform security management functionality and operational functions.
- **USER Interface (SFR-enforcing).** The USER interface provides a web-based interface for Normal User to communicate with the TOE and perform security management functionality and operational functions assigned by the System Administrator.
- **SEC_API (SFR-enforcing).** The programming interface used to engage the TLS functionality of the TOE and provides secure communication channel between TOE users and the TOE .



Legend:

TSFI Interaction

Figure 3 - Evaluated Deployment Configuration of the TOE

1.8 Delivery Procedures

22 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

23 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

24 The TOE is delivered by Sigma Rectrix's authorized representative to the customer. The TOE is wrapped in a plastic bag to provide resistance against moisture. Each TOE is then enclosed in cardboard shipping boxes and sealed with tape that contains Sigma Rectrix 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 box. Before the TOE is delivered, the authorized representative from Sigma Rectrix will ensure that:

- Ensuring that the underlying software/hardware platforms meet the required specifications; A schedule is given to customers via email or phone call regarding the delivery of the TOE to allow customer to know when the TOE is expected to be delivered by the Authorized Representative from Sigma Rectrix

- The TOE configuration will be performed by the Authorized Representative from Sigma Rectrix. The configuration process include the TOE configuration, credentials configuration, IP address, zone upload and license generation.
- Default accounts and passwords are created by authorized representative from Sigma Rectrix
- The following is the customer's ordering and delivering process handling for TOE from manufacturing until the TOE is delivered to customer for installation:
    a) Receiving Customer Order
    b) Evaluate Customer's Order
    c) Planning Stock Delivery
    d) Product Requisition
    e) Product Delivery Arrangement
    f) Product Delivery
    g) Invoicing
- If any issues occur during the delivery process, the customer and Sigma Rectrix's unauthorized sales representative or appointed account manager can communicate via email, phone call or face-to-face to resolve the issue via contact information in website. Sigma Rectrix maintains one support center which is located in Cyberjaya, Selangor. The contact information for the support center is:
    Sigma Rectrix Systems (M) Sdn Bhd
    Suite 3-05 ,4805 CBD Perdana 2,
    Jalan Perdana Cyber 12,
    Cyberjaya 63000,
    Selangor Malaysia
    +603-83186696

2 Evaluation

25 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

27 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.

28 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

29 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).

30 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.

31 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.

32 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

33 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.

34 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

35 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

36 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, 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). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

37 At EAL 2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation,

examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

38 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 recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 4: Independent Functional Test

Test ID	Description	Security Function	Results
F001- Identification and Authentication	1. To test that the TOE requires each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user 2. To test that the TOE maintains username & password	FIA_UAU.2 FIA_UID.2 FIA_ATD.1	Passed.

F002- Security Management	1. To test that the TOE capable of performing the management function stated in Table 2 of ST 2. To test that the TOE enforces the access control SFP to restrict the ability to change, modify and delete the security attributes to System Administrator and Normal User 3. To test that the TOE restricts the ability to modify the User Accounts to System Administrator and Normal User 4. To test that the TOE enforces the access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. 5. To test that the TOE restricts the ability to disable, enable and modify the behaviour of the functions TOE Configurations to System Administrator and Normal User 6. To test that the TOE maintains the System Administrator and Normal User roles 7. To test that the TOE able to associate users with roles 8. To test that the TOE detects [3] unsuccessful authentication attempts occur related to user entering their password for authentication to the TOE and block usage of the TOE 9. To test that the TOE provides a mechanism to verify that secrets meet number of characters equal to or greater than 8	FMT_SMF.1 FMT_MSA.1 FMT_MTD.1 FMT_MSA.3 FMT_MOF.1 FMT_SMR.1 FDP_ACC.1 FDP_ACF.1 FIA_AFL.1 FIA_SOS.1	Passed.

Test ID	Description	Security Function	Results
F003 - Stateful Traffic Filtering	1. The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE	FFW_RUL_EXT.1	Passed.
F004 - Secure Communication	1. To test that the TOE provides a communication path between itself and remote users or IT Systems that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure 2. To test that the TOE permits remote users to initiate communication via the trusted path 3. To test that the TOE requires the use of the trusted path for initial user authentication and all further communication after authentication	FTP_TRP.1	Passed.
F005 - Security Audit	1. To test that the TOE able to generate an audit report and record within each audit record 2. To test that the TOE able to provide reliable time stamps.	FAU_GEN.1 FAU_SAR.1 FPT_STM.1	Passed.

39 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Vulnerability Analysis

40 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.

41 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 (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 equipment required for exploitation

2.1.4.4 Vulnerability testing

42 The penetration tests focused on:

a) SQL Injection

b) Cross site scripting

c) Accessing Higher Privilege Access

d) Accessing Restricted Page

e) Browser cache

f) Cookie management

g) Cookie misconfiguration

h) Sensitive Info in Cookie Local Storage

i) Http Response Header

j) SSL Configuration

43 The result of the penetration testing noted 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 the Security Target (Ref [6]).

2.1.4.5 Testing Results

44 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. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

45 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 Garcinia Firewall Router v21.1.0 which is performed by Securelytics SEF.

46 Securelytics SEF found that Garcinia Firewall Router v21.1.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

47 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. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

48 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

49 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.

50 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

51 The Malaysian Certification Body (MyCB) is strongly recommended that:

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

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

c) System Auditor should review the audit trail generated and exported by the TOE periodically.

d) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

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 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.

[6] Garcinia Security Target, Version 1.0, 19 May 2021.

[7] Evaluation Technical Report (T2002-4-ETR 1.0) Garcinia Firewall Router ,10 June 2021.

A.2 Terminology

A.2.1 Acronyms

Table 5: 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

Acronym	Expanded Term
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 6: 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

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. 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.
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 ---