MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C121 Certification Report

NC2.VPN+ version 2.1.9

File name: ISCB-5-RPT-C121-CR-v1
Version: v1
Date of document: 7 September 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

C121 Certification Report

NC2.VPN+ version 2.1.9

7 September 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:	C121 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C121-CR-v1
ISSUE:	v1
DATE:	7 September 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 13 September 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	23 August 2021	All	Initial draft
v1	7 Sep 2021	Front page, Page i, Page ii, Page 18, Page 19	i) Updated on date & version ii) Updated on recommendation information

Executive Summary

The Target of Evaluation (TOE) is hardware and software and is used as a high-security gateway solution that provides Captive Portal (e.g. Forward Caching Proxy, Traffic Shaper etc.), ClamAV, VPN, Dnsmasq DNS & Dynamic DNS, Stateful Traffic Filter Firewall, Load Balancer, Intrusion Detection and Inline Prevention, and Reporting capabilities. Physical/logical features and functions of the TOE that are not included in the TOE Evaluation are Load balancer, Captive Portal, ClamAV, Dnsmasq DNS & Dynamic DNS Operation, VPN(IPsec), Intrusion Detection and Inline Prevention operation and Web/Cache proxy operation.

The TOE provides security functionality such as Stateful Traffic Filter Firewall, Virtual Private Network (VPN), Cryptographic Support, Security Audit, Identification and Authentication, Security Management, Secure Communication.

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 CyberSecurity Malaysia MySEF and the evaluation was completed on 13 August 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 NC2.VPN+ v2.1.9 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 a self-contained box (security appliance) called NC2.VPN+ v2.1.9 which provides comprehensive high-security gateway solution with seamless communication features providing reliable, robust, fully customizable tools capable of handling any known security threat with software-defined security resiliency.

2 From the stateful inspection firewall to the inline intrusion detection & prevention system, various features are built-in to enhance network performance and protect your network from numerous cyber security threats.

3 The TOE provides a high level of security by using HardenedBSD that employs the TOE patented security technology and removes the inherent security risks often found in a network application running on non-security focused commercial operating systems, resulting in superior network security. It also includes a high-security gateway capabilities such as Captive Portal (e.g. Forward Caching Proxy, Traffic Shaper etc.), ClamAV, VPN, Dnsmasq DNS & Dynamic DNS, Stateful Traffic Filter Firewall, Load Balancer, Intrusion Detection and Inline Prevention and Reporting.

4 Physical/logical features and functions of the TOE that are not included in the TOE Evaluation are Load Balancer, Captive Portal, ClamAV, Dnsmasq DNS & Dynamic DNS Operation, VPN(IPsec), Intrusion Detection and Inline Prevention operation, OpenDNS & Unbound DNS Operation and Web/Cache proxy operation.

1.2 TOE Identification

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

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C121
TOE Name	NC2.VPN+
TOE Version	V2.1.9
Security Target Title	SCS NC2.VPN+ Security Target
Security Target Version	V1.0
Security Target Date	28 July 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	System Consultancy Services No.36, Jalan Wangsa Delima 6, Wangsa Maju, 53300 Kuala Lumpur
Developer	System Consultancy Services No.36, Jalan Wangsa Delima 6, Wangsa Maju, 53300 Kuala Lumpur
Evaluation Facility	CyberSecurity Malaysia MySEF (CSM MySEF)

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 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 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.

- Virtual Private Network (VPN)
    - The TOE can initiate and/or accept OpenVPN connections for traffic that needs authenticity, confidentiality and integrity protection. OpenVPN is a VPN connection that is used to secure data communication and extend private network services

- Cryptographic Support
    - The TOE implements encryption algorithm that utilizes AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB cryptographic algorithms with 128, 192 and 256 bits cryptographic key sizes for OpenVPN connections.

- Security Audit

  The TOE generates audit records for security events. Types of audit logs are:
    - System Log Files
    - Interface (Wireless Log File)
    - Interface (Point-to-Point Log File)
    - Firewall Log Files
    - VPN (OpenVPN & Self-Test 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, password and CAPTCHA code in order to access the TOE. There are two types of users; System Administrator and Normal User. System Administrator is a user that has the privilege to perform all operation. Normal user is a user that has the privilege (assigned by System Administrator) to perform only selected operations (it can be one operation or more) Normal User does not has the privilege to perform all operation as System Administrator.

- 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 The TOE resides between one or more internal networks (that the TOE is protecting) and an external network such as the Internet.

10 All information transferred between the internal and external networks shall pass through the TOE.

11 Network packets are inspected in real-time as they pass through the TOE (inbound and outbound protection).

12 Malicious network packets are filtered before they have a chance to reach inside the protected network.

13 The table below identifies the hardware specification and components of the TOE:

Components	Specification
Processor	8th Generation Intel Core I U-series processor
Chassis	Ultra-slim and cables design support wide range temperature of -40 Celsius to 75 Celsius with fanless operation
Memory (RAM)	2 DDR4 2400MHz memory up to 64GB
Port/Interfaces	Dual independent DisplayPort displays support up to 4K resolution 4-port USB 3.1 support up to 10Gbps data transfer 4 Independent GigE Lan with 2 IEEE 802.3at PoE SIM Socket for 5G/WIFI/4G/3G/LTE/GPRS/UMTS 4 COM RS-232/422/482, 16 Isolated DIO 9v to 50v dc Wide Range Power Input Ignition Power Control, TPM 2.0 Mini PCIe Comms Module with pre-installed
Storage	256GB 2.5" SATA SSD
Power Adapter	PWA-120WM4P (120W, 24V, 90V AC to 264V AC Power Adapter with 4-pin Mini-DIN Connector with UK power cord)

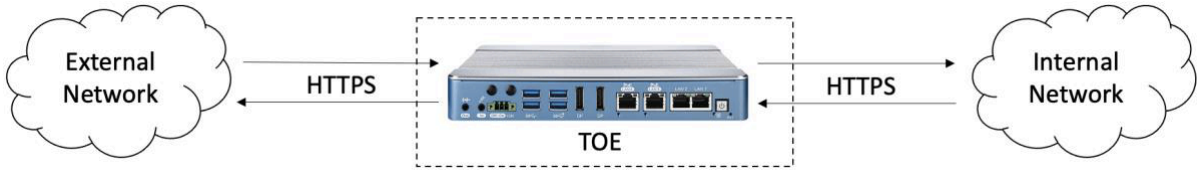

Figure 1: TOE Physical Scope

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 2: Assumptions for the TOE Environment

Environment	Statement
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. Local management shall only take place within this physically secured environment. Any RADIUS and/or Syslog servers shall be similarly protected and their connections with the TOE shall be protected against access by attackers.
A.SINGLE_CONNECTION	Information cannot flow among the networks connected to the TOE unless it passes through the TOE.

A.TRUSTED_ADMIN	TOE System Administrators and Normal Users are trusted to follow and apply all administrator guidance in a trusted manner.

1.7 Evaluated Configuration

19 This section describes the configurations of the TOE is to be configured according to the Preparative Guidance.

20 The TOE is delivered as an appliance by the developer, and the system administrator must then make the following configuration changes:

1) The appliance/hardware on which the TOE has been installed must be free from viruses and other malware which may compromise the security and functionality of the software, and users must conscientiously take steps to use the computer in a secure manner.

2) Users must keep their passwords secret, not share them with other persons and not write them down; and

3) The appliance/hardware on which the TOE has been installed must be placed in a reasonably secure physical environment (e.g., within a locked and/or guarded premises) so that the threat of the computer or its hard disk/memory being stolen is reduced.

4) The TOE should be installed and configured in accordance with the administration guide provided by the developer to ensure secure installation and configuration;

5) The physical environment in which the TOE is installed should be physical secure to prevent unauthorized physical access to the TOE, have logical and physical access control policies in place and have well-documented configuration and change management systems;

6) Staff assigned to handle, configure and operate the TOE shall be appropriately trained to prevent accidental misuse or misconfiguration of the TOE; and

7) TOE updates shall be installed whenever released by the developer to ensure continuing secure operation of the TOE.

1.8 Delivery Procedures

21 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.

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

1.8.1 TOE Delivery Procedures

23 The TOE is delivered by SCS's authorizes 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 SCS 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 SCS 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 SCS
- The TOE configuration will be performed by the Authorized Representative from SCS. 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 SCS

24 The following is the customer's order and delivery process handling for TOE from manufacturing until the TOE is delivered to customer for installation:

a) Receiving Customer Order

Responsibilities: Sales

- Received with official written Purchase Order from Customers through fax/email.

b) Evaluate Customer's Order

Responsibilities: Sales Dept. Head

- To evaluate with customer the exact product requirements, quantity and pricing.

c) Planning Stock Delivery

Responsibilities: Sales Dept. Head/Production Manager

- To determine the stock delivery schedule and executive

d) Product Requisition

Responsibilities: Sales/ Sales Coordinator

- To determine the stock delivery schedule and executive to raise Sales Requisition to Production / Stock Controller. To inform Product delivery schedule to Production and Store Personnel.

e) Product Delivery Arrangement

Responsibilities: Sales/ Store Personnel

- Store Personnel to prepare product model and quantity required.

f) Product Delivery

Responsibilities: Sales/ Sales Coordinator

- To execute the product delivery to customer based on the quantity required and schedule agreed

g) Invoicing

Responsibilities: Sales/ Sales Coordinator/Store Personnel

- To ensure the product model and quantity are correct and deliver according to the agreed delivery schedule. Proceed to Invoice when product being delivered

h) End

- If any issues occur during the delivery process, the customer and SCS's authorized 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.

25 SCS maintains one support center which is located in Kuala Lumpur. The contact information for the support center is:

System Consultancy Services

No.36, Jalan Wangsa Delima 6

Wangsa Maju, 53300 Kuala Lumpur

Phone:+603 4149 1919

26 Note that a new software release will be updated by authorized representative from SCS manually at the customer's facility. End users will be notified via email about the available update.

2 Evaluation

27 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

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

2.1.1 Life-cycle support

29 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.

30 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

31 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).

32 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.

33 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.

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

2.1.3 Guidance documents

35 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.

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

2.1.4 IT Product Testing

37 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by CyberSecurity Malaysia MySEF). 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

38 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

39 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.

40 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 3: Independent Functional Test

No	Test Title	Description	Security Function	Results
Test Group A Administration for System Administrator and Normal User				
1	A.1. System Administrator Login	To test that each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of the user.	Identification and Authentication	Passed
2	A.2. Security Management (System Administrator)	To test that the System Administrator able to perform security management functions such as change password, user and group access, firewall rules management and VPN IPsec management.	Security Management	Passed

No	Test Title	Description	Security Function	Results
3	A.3.Normal User Login	To test that each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user.	Identification and Authentication	Passed
4	A.4 Security management by Normal User	To test that the User can perform security management functions such as change password, user and group access, firewall rules management and VPN IPsec management.	Identification and Authentication Security Management	Passed
5	A.5 Firewall: Stateful traffic filtering (System Administrator and Normal User)	To test that System Administrator and Normal User can provide rules to be used and the TOE able to restrict the traffic flow between the various networks connected to the TOE	Stateful traffic filter firewall Security Management	Passed

No	Test Title	Description	Security Function	Results
6	A.6 Manage audit log for System Administrator and Normal User	To test that the System Administrator and Normal user can perform security management functions such as viewing the audit log for System Log, Firewall log and OpenVPN log.	Security Audit	Passed
7	A.7 Cryptographic Operation [System Administrator and Normal User]	To test that TOE able to perform encryption and decryption with specified Cryptographic Algorithm AES CBC, CFB, CFB1, CFB8, OFB. with 128, 192 and 256 bits cryptographic key sizes and meet ISO 18033-3.	Cryptographic support	Passed
8	A.8 Trusted Channel [System Administrator and Normal user]	To test that TOE able to initiates communication via OpenVPN channel	Virtual Private Network	Passed
Test Group B Trusted channel				
9	B.1 Encrypted Communication (System Administrator)	Verify the encrypted communication between the System Administrator and the TOE.	Secure Communication	Passed

No	Test Title	Description	Security Function	Results
10	B.2 Encrypted Communication (Normal User)	Verify the encrypted communication between the Normal User and the TOE.	Secure Communication	Passed
Test Group C Cryptographic algorithm validation				
11	C.1 Generate cryptographic keys	Verify the TOE can generate cryptographic keys using algorithm AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB 128,192, and 256 bits by following ISO-18033-3 standard.	Cryptographic support	Passed
12	C.2 Distribute cryptographic key	Verify the TOE can distribute cryptographic key during the distribution of session key using TLS.	Secure communication	Passed
13	C.3 Destroy cryptographic key	Verify the TOE can destroy cryptographic key using destruction method which is key zeroization.	Cryptographic support	Passed

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

2.1.4.3 Vulnerability Analysis

42 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.

43 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

44 The penetration tests focused on:

a) Authentication bypass

b) Broken access control

c) Sniffing

d) Cross site scripting

e) Insufficient Logging and Monitoring

f) Denial of Service

g) Insecure Deserialization

45 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

46 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

47 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 NC2.VPN+ version 2.1.9 which is performed by CyberSecurity Malaysia MySEF.

48 CyberSecurity Malaysia MySEF found that NC2.VPN+ version 2.1.9 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.

49 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

50 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.

51 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.

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

3.2 Recommendation

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

1) Consumer/Client are advised to make sure that all assumptions regarding the TOE security environment are fulfilled.

2) Consumer/Client are advised to make sure that the operation of the TOE is in its evaluated configuration.

3) Consumer/Client are advised to seek help, assistance, or guidance from the developer of the TOE if any cases of specific requirements shall be configured onto the TOE to meet certain policies, procedures and security enforcement within the consumer/client organization. Therefore, there should not be any misconfiguration or malfunctions, or insecure operations of the TOE that may affect consumer/client assets that is protected by the TOE.

4) Developer is recommended to keep on updating the TOE user guide and relevant documentations based on updated features of the TOE.

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] SCS NC2.VPN+ Security Target, Version 1.0, 28 July 2021.

[7] E050 Evaluation Technical Report NC2.VPN v2.19 v1.1, 23 August 2021.

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

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 5: 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 ---