

C145 Certification Report

NC2.vpn+ V2.2.1

File name: ISCB-5-RPT-C145-CR-v1a

Version: v1a

Date of document: 2 Oct 2026

Document classification : PUBLIC



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

C145 Certification Report

NC2.vpn+ V2.2.1

2 Oct 2026

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: C145 Certification Report

DOCUMENT REFERENCE: ISCB-5-RPT-C145-CR-v1a

ISSUE: v1a

DATE: 2 Oct 2026

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND
DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2026

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 200601006881 (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.

The Certification Report, Certificate of the evaluated product, and the Security Target (Ref [5]) have been published on the MyCC Scheme Certified Product Register (MyCPR) at <https://iscb.cybersecurity.my> and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

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 2022 revision 1 (Ref[3]), for conformance to the Common Criteria for IT Security Evaluation, version 2022 revision 1 (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	17 Sept 2026	All	Initial draft
d2	24 Sept 2026	4,5,14,28	Updated based on comments from reviewer
v1	25 Sept 2026	All	Final Version
V1a	2 Oct 2026	4	Remove typographic error - duplicate "The TOE" as per SCC's Comment.

Executive Summary

The project is C145 NC2.vpn+ V2.2.1, referred to as the Target of Evaluation (TOE) which developed by System Consultancy Services Sdn. Bhd. The TOE is a network security solution designed to protect communications between trusted and untrusted networks through the enforcement of security policies and the monitoring of network traffic. The TOE comprises the NC2.vpn+ V2.2.1 software, including the TOE application software, the configured HardenedBSD operating system, and the TOE configuration necessary to provide the evaluated security functionality described in the Security Target. The TOE executes on a dedicated hardware platform; however, the hardware platform is outside the scope of this evaluation and serves solely as the execution environment for the TOE software. Accordingly, no security claims are made for the hardware platform.

The TOE provides security functions such as Stateful Traffic Filter Firewall, Virtual Private Network (VPN), Cryptographic Support, Security Audit, Identification and Authentication, Security Management and 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 4. 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 Sdn Bhd (Securelytics SEF) and the evaluation was completed on 15 Sept 2026.

This Certification Report is associated with the Certificate of Product Evaluation (2026-00#-C1##) dated DD MMM YYYY and the Security Target (Ref[6]). The certification is valid for a period of five (5) years from the date of the Certificate of Product Evaluation, after which it will expire.

It is the responsibility of the user to ensure that NC2.vpn+ V2.2.1 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

Document Authorisation	ii
Copyright Statement	iii
Foreword	iv
Disclaimer	v
Document Change Log.....	vi
Executive Summary.....	vii
Index of Tables	x
Index of Figures	x
1 Target of Evaluation	1
1.1 TOE Description	1
1.2 TOE Identification	2
1.3 Security Policy	3
1.4 TOE Architecture	3
1.4.1 Logical Boundaries	3
1.4.2 Physical Boundaries	5
1.5 Clarification of Scope	7
1.6 Assumptions	7
1.6.1 Operational Environmental assumptions	7
1.8 Evaluated Configuration	9
1.8.1 Evaluated Hardware Configuration.....	9
1.8.2 Evaluated Client-Side Configuration	9
1.8.3 Evaluated Cryptographic Configuration	10
1.9 Delivery Procedures	10
1.9.1 TOE Delivery Procedures	10
1.9.2 Documentation Delivery	11
2 Evaluation	12
2.1 Evaluation Analysis Activities	12

2.1.1	Life-cycle support	12
2.1.2	Development	13
2.1.3	Guidance documents	14
2.1.4	IT Product Testing	14
3	Result of the Evaluation	26
3.1	Assurance Level Information	26
3.2	Recommendation	27
Annex A	References	28
A.1	References	28
A.2	Terminology.....	28
A.2.1	Acronyms	28
A.2.2	Glossary of Terms	29

Index of Tables

Table 1: TOE List of Security Functions	2
Table 2: TOE Identification.....	3
Table 3: Assumptions for the TOE Environment	8
Table 4 : Threats for the TOE.....	9
Table 5 : Independent Functional Test	23
Table 6 : List of Acronyms	28
Table 7 : Glossary of Terms	29

Index of Figures

Figure 1: TOE Physical Scope	5
Figure 2: TOE Boundary Scope.....	6

1 Target of Evaluation

1.1 TOE Description

- 1 The NC2.vpn+ V2.2.1(TOE) comprises the NC2.vpn+ V2.2.1 software, including the TOE application software, the configured HardenedBSD operating system, and the TOE configuration necessary to provide the evaluated security functionality described in the Security Target. The TOE executes on a dedicated hardware platform; however, the hardware platform is outside the scope of this evaluation and serves solely as the execution environment for the TOE software. Accordingly, no security claims are made for the hardware platform.
- 2 The TOE provides the security functions necessary to control network communications, enforce access control policies, protect administrative access, establish secure communication channels, detect unauthorized network activities, and generate audit records for security-relevant events. These evaluated security functions are described in detail in the TOE Summary Specification.
- 3 The NC2.vpn+ V2.2.1 product also includes additional networking and system management capabilities, such as Captive Portal, Forward Caching Proxy, Traffic Shaper, ClamAV integration, Dnsmasq DNS, Dynamic DNS, Load Balancing, and Reporting. These capabilities are outside the scope of this evaluation unless they are explicitly identified elsewhere in the Security Target as part of the evaluated TOE security functionality.
- 4 The following table highlights the range of security functions implemented by the TOE.

Security Functions	Descriptions
Stateful Traffic Filter Firewall	TOE User can configure rules to be enabled by the TOE in its operations, in which 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
Virtual Private Network (VPN)	The TOE can initiate and/or accept OpenVPN connections for traffic that needs authenticity, confidentiality and integrity protection.
Cryptographic Support	The TOE implements encryption algorithms that utilizes AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB, Camellia and SHA cryptographic algorithms.

Security Functions	Descriptions
Security Audit	The TOE generates audit records for security events for security auditing and record purposes. TOE User have the ability to view and export the audit logs and transaction logs.
Identification and Authentication	TOE User are required to identify and authenticate with the TOE prior to any user action or information flow being permitted.
Security Management	The TOE provides functionality that allows management of the TOE and all 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 enabling the HTTPS (TLS v1.2 & TLS v1.3) for secure communication.

Table 1: TOE List of Security Functions

- 5 The TOE can be categorised as Network and Network-Related Devices and Systems in accordance with the categories identified in the Common Criteria Portal.

1.2 TOE Identification

- 6 The details of the TOE are identified in table below.

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C145
TOE Name	NC2.vpn+
TOE Version	V2.2.1
Security Target Title	SCS NC2.vpn+ V2.2.1 Security Target
Security Target Version	v1.1.1
Security Target Date	19 Aug 2026
Assurance Level	Evaluation Assurance Level 4
Criteria	Common Criteria for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref[2])

Methodology	Common Methodology for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref[3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor	System Consultancy Services Sdn. Bhd. 36 Jalan Wangsa Delima 6, Pusat Bandar Wangsa Maju, 53300 Kuala Lumpur
Developer	System Consultancy Services Sdn. Bhd. 36 Jalan Wangsa Delima 6, Pusat Bandar Wangsa Maju, 53300 Kuala Lumpur
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya, Selangor, Malaysia

Table 2: TOE Identification

1.3 Security Policy

- 7 No Organisational Security Policy (OSP) declared for the TOE.

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

- 9 The logical boundary of the TOE is summarized below:

- **Stateful Traffic Filter Firewall**

System Administrator and Normal User with limited access provided as defined by System Administrator able to configure rules in the TOE and enforce it within the TOE operations, to restrict the flow of traffic between the various networks connected to the TOE. The configured rules will restrict the flow of network traffics between protected networks and other attached networks (e.g., Internet) based on network addresses and ports of the network nodes originating (source) and/or receiving (destination) of applicable network traffics 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 provides Virtual Private Network (VPN) services using OpenVPN to establish secure communication channels between trusted endpoints. The TOE can initiate and accept VPN connections to provide confidentiality, integrity, and authenticity for data transmitted over untrusted networks. Secure communication channels are established using the TOE's evaluated cryptographic mechanisms.

- **Cryptographic Support**

The TOE implements cryptographic operations through the usage of encryption algorithm that utilizes AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB, Camellia and SHA cryptographic algorithms with 128, 192, 256 and 512 bits cryptographic key sizes for OpenVPN connections.

- **Security Audit**

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

- I. System Log Files
- II. Interface (Wireless Log File).
- III. Interface (Point-to-Point Log File).
- IV. Firewall Log Files.
- V. VPN (OpenVPN Log Files).

- **Identification & Authentication**

System Administrator and Normal User are required to be identified and authenticated before any information flows are permitted. At the login page, TOE User are needed to key in a valid username, password, certificate and certificate password to access the TOE.

System Administrator is an organisation appointed and TOE User that has the privilege to perform all operations stated in Table 11, Security Target (Ref[6]). Aside of that, Normal user is a user that has the privilege (created and assigned with limited access by System Administrator) to perform only selected operations

(it can be one operation or more) stated in Table 11, Security Target (Ref[6]). Normal User does not have the privilege to perform all operations similar to 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 all TOE functions are restricted to those who have the privilege to access the TOE functionalities. The TOE provides a web-based GUI interface that permits 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 TOE User. It also provides assured identification of its end points and protection of the communicated data from modification or disclosure.

1.4.2 Physical Boundaries

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

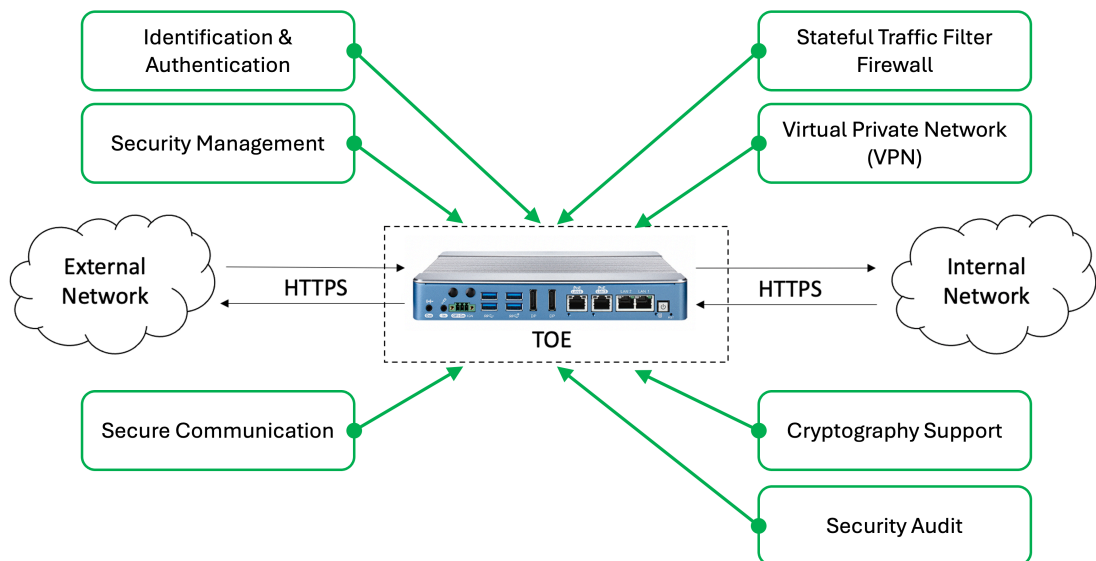


Figure 1: TOE Physical Scope

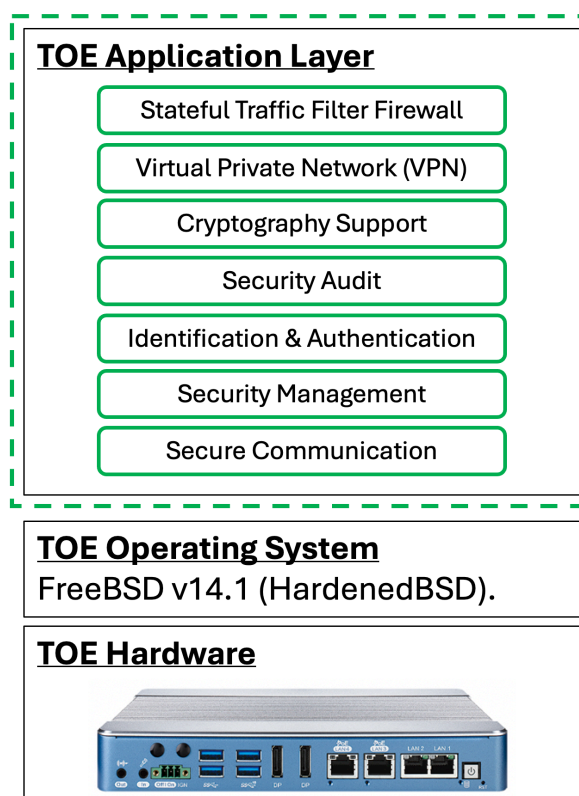


Figure 2: TOE Boundary Scope

- 11 Figure 1 illustrates the overall deployment environment of the TOE. Figure 2 identifies the TOE boundary, highlighted by the **green dotted line**, showing the components included within the scope of the Target of Evaluation (TOE).
- 12 The TOE comprises the **NC2.vpn+ V2.2.1 application software**, the **configured HardenedBSD operating system**, and the **TOE configuration** required to provide the evaluated security functionality described in this Security Target. The TOE executes on a dedicated hardware platform that provides the execution environment for the TOE software. The hardware platform is **outside the scope of this evaluation**, and no security claims are made for the hardware platform.
- 13 The TOE is deployed between one or more trusted internal networks and an untrusted external network (for example, the Internet) to enforce the organization's network security policy. All network traffic exchanged between the trusted and untrusted networks passes through the TOE, where it is processed in accordance with the security policies configured by System Administrator. The TOE inspects network traffic in real time and applies the configured security policies before permitting or denying communication between connected networks.

- 14 The TOE shall only be administered by System Administrator through the TOE management interfaces. Administrative functions are protected by identification and authentication mechanisms, and all TOE configuration activities are performed in accordance with the privileges assigned to the System Administrator. Secure administrative access to the TOE is provided using HTTPS (TLS v1.2 and TLS v1.3) or other supported secure communication mechanisms provided by the TOE.
- 15 The TOE scope of evaluation includes only the TOE software, configured operating system, and TOE configuration identified in Section 1.4.1 and Section 1.4.2 of the Security Target (Ref[6]). Components identified in Sections 1.4.3, 1.4.4, and 1.4.5 of the Security Target (Ref[6]), including the dedicated hardware platform, external networks, connected network devices, customer-defined firewall policies, user accounts, certificates, and other operational configuration data, are outside the scope of this evaluation unless explicitly stated otherwise.

1.5 Clarification of Scope

- 16 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.
- 17 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]).
- 18 Potential consumers of the TOE are advised that some functions and services of the overall product have not 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

- 19 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. Operational Environmental assumptions

- 20 Assumptions for the TOE environment as described in the Security Target (Ref [5]):

Identifier	Assumption statement
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the customer organisation IT environment. IT 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 Administrator is trusted to follow and apply all administrator guidance in a trusted manner.

Table 3: Assumptions for the TOE Environment

1.7 Threats

21 Threats for the TOE as address in the Security Target (Ref[6]):

Identifier	Threat Statement
T.UNAUTHORIZED_DATA	An attacker with intentions to perform the following actions: i. Sends data from one network to another network; and/or ii. Accesses services on one network from another network; while not authorised to do so, that may compromise the TOE operations through bypassing the filtering mechanism configured in the TOE.
T.READ_MODIFY_DATA	An attacker on a network may read the network packet traffic or modify network packet traffic in that network that comes from or through the TOE, or goes to or through the TOE, in which this action is not allowed to be performed.
T.UNAUTHORIZED_ACCESS	An attacker gains unauthorised access to the TOE itself and performs unauthorised actions on the TOE.
T.UNDETECTED_ACTIONS	An attacker may take actions that adversely affect the security of the TOE or the networks protected by the TOE, whereas connected to and these actions remain undetected and thus their effects cannot be effectively mitigated.

T.TOECOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.
----------	---

Table 4 : Threats for the TOE

1.8 Evaluated Configuration

- 22 The TOE was evaluated in a defined and controlled configuration. The evaluation results presented in this report apply only to the TOE when installed, configured, and operated in accordance with this evaluated configuration. Any other configurations are outside the scope of this evaluation.

1.8.1 Evaluated Hardware Configuration

- 23 During evaluation, the TOE was operated on the following hardware/appliance requirement (minimum requirement):
- **Hardware:** FWS-7840
 - **Operating System:** FreeBSD v14.1 (HardenedBSD)
 - **Processor:** 10th Generation Intel Core/Xeon processor
 - **Chassis:** Operational up to 40 degrees Celsius
 - **Memory (RAM):** 2 DDR4 2666MHz, minimum 16GB, maximum 64GB
 - **Port/Interfaces:** 1 port of HDMI displays support up to 4K resolution, 2 ports of USB 3.2 support up to 10Gbps data transfer, 8 ports of 1-GigabitE with RJ-45 connectors, 240V AC Power Input
 - **Storage:** 256GB 2.5" SATA SSD
 - **Power Adapter:** Standard PC power cord with UK type connector

1.8.2 Evaluated Client-Side Configuration

- 24 The TOE was accessed by users using the following client configuration (minimum requirement):
- **Web Browsers:**
 - Mozilla Firefox: version 135.0 and above.
 - Google Chrome: version of 135.0 and above.

1.8.3 Evaluated Cryptographic Configuration

- 25 The TOE was evaluated with the following cryptographic mechanism enabled:
- TLS v1.2 and TLS v1.3 to provide trusted communication paths between the TOE and TOE users
- 26 These cryptographic mechanisms support the security functional requirements defined in the ST which is secure communication.

1.9 Delivery Procedures

- 27 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.
- 28 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.9.1 TOE Delivery Procedures

- 29 The TOE is delivered only by SCS or an authorized representative to ensure that the integrity and authenticity of the TOE are maintained throughout the delivery process.
- 30 Prior to delivery, the TOE is verified to ensure that the correct product model, serial number, software version, and associated configuration correspond to the customer's order. The TOE is then packaged in protective materials to prevent damage during transportation. Each TOE is enclosed in a sealed cardboard shipping box bearing the SCS identification label. The shipping label includes the product model, serial number, and customer information for identification and traceability.
- 31 Where applicable, the TOE may undergo factory configuration before shipment. The configuration activities include TOE initialization, network configuration, administrator account creation, IP address configuration, zone upload, and license generation.
- 32 Site-specific security configuration is performed by authorized SCS personnel during installation at the customer site.
- 33 The authorized representative shall notify the customer of the expected delivery schedule via email or telephone prior to shipment.
- 34 Upon receipt of the TOE, the customer is required to verify that:
- The shipping package is received in good condition without evidence of tampering.

- The product model and serial number match the accompanying delivery documents.
- The delivered TOE corresponds to the purchased product.
- The packaging seal remains intact prior to installation.

35 Any discrepancies, damage, or suspected tampering shall be reported immediately to SCS before the TOE is installed or operated.

1.9.2 Documentation Delivery

36 The TOE is supplied together with the relevant guidance documentation required for installation, administration, operation, and maintenance.

37 The documentation may be delivered using one of the following methods:

- a) **Softcopy.** Provided via email, secure download, or USB storage device; or
- b) **Hardcopy.** Provided upon customer request or where required by contractual or regulatory obligations.

38 Both softcopy and hardcopy documents are controlled documents and correspond to the released TOE version. The document version is verified before delivery to ensure consistency with the delivered TOE.

2 Evaluation

39 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2022 Revision 1 (Ref[2]) and the Common Methodology for IT Security Evaluation (CEM), version 2022 Revision 1 (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 automated and 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 and determine that the delivery procedures are used.

31 The evaluators examined the development security documentation and determine that it described details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation, including sufficiency of the security measures employed, and development security documentation and associated evidence was performed to determine that the security measures are being applied.

32 The evaluators examined the documented life-cycle model to verify that it covers the development and maintenance processes and that the procedures, tools, and techniques used support the development and maintenance of the TOE.

- 33 The evaluators examined the development tool documentation and verified that the tools are clearly defined, including the statements, conventions, directives, and implementation-dependent options used.
- 34 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.2 Development

- 35 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), how it completely and accurately describes all errors messages and its meanings resulting from an invocation of each TSFI, and how the TOE security function (TSF) implements complete and accurate instantiation of the security functional requirements (SFRs).
- 36 The evaluators analyzed the TOE Implementation representation; they determined that the implementation representation defines the TSF to a level of detail such that the TSF can be generated without further design decisions and verified that mapping between the TOE design description and the sample of the implementation representation to determine that it is accurate.
- 37 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 and accurate descriptions of the SFR-enforcing behavior of the SFR-enforcing subsystems; verified that TOE design has description and purpose of a SFR-supporting or SFR-non-interfering module's interaction with other modules is complete and accurate; it contains a complete and accurate mapping from the TSFI described in the functional specification to the modules of the TSF described in the TOE design; and examined TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered and accurate by the TOE design.
- 38 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.
- 39 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

- 40 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.
- 41 The documents for TOE users to refer as guidance are as per listed:
- SCS NC2.vpn+ V2.2.1 Guidance Document, V1.1.1, 19 Aug 2026
 - SCS NC2.vpn+ V2.2.1 Programmer Guide, V1.0.1, 19 Aug 2026
 - SCS NC2.vpn+ V2.2.1 Administration Guide, V1.1.1, 19 Aug 2026
 - SCS NC2.vpn+ V2.2.1 Installation and Troubleshooting Guide, V1.1.1, 19 Aug 2026
- 42 The evaluators confirmed that the TOE guidance has fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

- 43 Testing at EAL 4 consists of coverage analysis, testing depth, 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

- 44 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

- 45 At EAL 4, 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.

- 46 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.

Test ID	Description	Security Function	Results
F001 – Stateful Traffic Filter Firewall	- To test that the TOE perform Stateful Traffic Filtering on network packets processed by the TOE. - To test that the TOE allow the definition of Stateful Traffic Filtering rules using the network protocol fields: - ICMP - IPv4 - IPv6 - TCP - UDP - To test that the TOE allow the following operations to be associated with Stateful Traffic Filtering rules: - Pass - Block - Reject - To test that the TOE allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface. - To test that the TOE accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an	FFW_RUL_EXT.1.1 FFW_RUL_EXT.1.2 FFW_RUL_EXT.1.3 FFW_RUL_EXT.1.4 FFW_RUL_EXT.1.5 FFW_RUL_EXT.1.6 FFW_RUL_EXT.1.7 FFW_RUL_EXT.1.8 FFW_RUL_EXT.1.9	Passed

Test ID	Description	Security Function	Results
	allowed established session for the following protocols, which are TCP, UDP based on the following network packet attributes: • TCP: source and destination addresses, source and destination ports. • UDP: source and destination addresses, source 6. To test that the TOE enforce the following default Stateful Traffic Filtering rules on all network traffic: • To test that the TOE drop packets which are invalid fragments; • To test that the TOE drop fragmented packets which cannot be re-assembled completely; • To test that the TOE drop packets where the source address of the network packet is on a broadcast network, on a multicast network, and/or a loopback addresses. • To test that the TOE drop network packets where the source or destination address of the packet is: unspecified. 7. To test that the TOE drop network packets where: • The source address of the network packet is equal to		

Test ID	Description	Security Function	Results
	the address of the network interface where the network packet was received; - The source or destination address of the network packet is a link-local address; - The source address of the network packet does not belong to the networks associated with the network interface where the network packet was received. 8. To test that the TOE process the applicable Stateful Traffic Filtering rules in an administratively defined order. 9. To test that the TOE deny packet flow if a matching rule is not identified.		
F002 -Security Audit	1. To test that the TOE be able to generate audit data of the following auditable events: - All auditable events for the [not specified] level of audit; - Auditable events within the TOE as follows: i. System Log Files; ii. Interface (Wireless Log File); iii. Interface (Point-to-Point Log File); iv. Firewall Log Files; and v. VPN (OpenVPN Log Files). vi. IP Lockout	FAU_GEN.1.1 FAU_GEN.1.2	Passed.

Test ID	Description	Security Function	Results
	2. To test that the TOE record within the audit data at least the following information: • Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; • For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [none].		
F003 – Security Audit	1. To test that the TOE provide [System Administrator and Normal User] with the capability to read and export [Auditable events within the TOE, as defined in FAU_GEN.1.1] from the audit data. 2. To test that the TOE provide the audit data in a manner suitable for the user to interpret the information.	FAU_SAR.1.1 FAU_SAR.1.2	Passed.
F004 – Cryptographic Support	To test that the TOE generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB, Camellia, SHA] and specified cryptographic key sizes [128, 192,	FCS_CKM.1.1	Passed.

Test ID	Description	Security Function	Results
	256, 512 bits] that meet the following: [ISO/IEC18033-3].		
F005 – Cryptographic Support	To test that the TOE distribute cryptographic keys in accordance with a specified cryptographic key distribution method [distribution of session keys using TLS] that meets the following: [none].	FCS_CKM.2.1	Passed.
F006 – Cryptographic Support	To test that the TOE perform [cryptographic key access while generating and exporting certificates] in accordance with a specified cryptographic key access method [username, password, certificate, certificate password] that meets the following: [ISO/IEC 18033-3].	FCS_CKM.3.1	Passed.
F007 – Cryptographic Support	1. To test that the TOE provide a [nonphysical true] random number generator that implements: [TRNG (True Random Number Generator)]. 2. To test that the TOE provide [bits] that meet [NIST SP800-22].	FCS_RNG.1.1 FCS_RNG.1.2	Passed.
F008 – Cryptographic Support	1. To test that the TOE destroy [AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB, Camellia, SHA] when [[key zeroization]]. 2. To test that the TOE destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [key	FCS_CKM.6.1 FCS_CKM.6.2	Passed.

Test ID	Description	Security Function	Results
	zeroization] that meets the following: [none].		
F009 – Cryptographic Support	To test that the TOE perform [encryption and decryption] in accordance with a specified cryptographic algorithm [Camellia, AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB, SHA] and cryptographic key sizes [128, 192, 256, 512 bits] that meet the following: [ISO/IEC 18033-3].	FCS_COP.1.1	Passed.
F010 – Identification and Authentication	To test that the TOE enforce the [access control SFP] on [subjects, objects and operations as listed in Table 11 in the ST.	FDP_ACC.1.1	Passed.
F011 – Identification and Authentication	- To test that the TOE enforce the [access control SFP] to objects based on the following: [subject, objects and attributes in Table 11 in the ST. - To test that the TOE enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: - If the System Administrator and Normal User are successfully authenticated accordingly, then access is granted based on privilege allocated; - If the System Administrator and Normal User are not authenticated successfully,	FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4	Passed.

Test ID	Description	Security Function	Results
	therefore, access permission is denied]. 3. To test that the TOE explicitly authorize access of subjects to objects based on the following additional rules: [none]. 4. To test that the TOE explicitly deny access of subjects to objects based on the following additional rules: [none].		
F012 - Identification and Authentication	To test that the TOE maintain the following list of security attributes belonging to individual users: [username, password, certificate and certificate password].	FIA_ATD.1.1	Passed.
F013 - Identification and Authentication	1. To test that the TOE require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. 2. To test that the TOE require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.	FIA_UAU.2.1 FIA_UID.2.1	Passed.
F014 - Security Management	To test that the TOE enforce the [access control SFP(s)] to restrict the ability to [change_default, modify, delete] the security attributes [TOE Configuration, Users Account] to [System Administrator and Normal User].	FMT_MSA.1.1	Passed.
F015 - Security Management	1. To test that the TOE enforce the [access control SFP] to provide [permissive] default values for	FMT_MSA.3.1 FMT_MSA.3.2	Passed.

Test ID	Description	Security Function	Results
	security attributes that are used to enforce the SFP. 2. To test that the TOE allow the [none] to specify alternative initial values to override the default values when an object or information is created.		
F016 – Security Management	To test that the TOE restrict the ability to [modify] the [System Administrator Account and Normal User Account] to [System Administrator and Normal User].	FMT_MTD.1.1	Passed.
F017 – Security Management	To test that the TOE restrict the ability to [disable, enable and modify the behaviour of] the functions [TOE Configurations] to [System Administrator and Normal User].	FMT_MOF.1.1	Passed.
F018 – Security Management	To test that the TOE be capable of performing the following management functions: [refer to Table 11 in the ST.	FMT_SMF.1.1	Passed.
F019 – Security Management	1. To test that the TOE maintain the roles [System Administrator, Normal User]. 2. To test that the TOE be able to associate users with roles.	FMT_SMR.1.1 FMT_SMR.1.2	Passed.
F020 – Virtual Private Network (VPN)	1. To test that the TOE provide an OpenVPN communication channel between itself and OpenVPN clients and/or servers that is logically distinct from other communication channels and provides assured identification of its end points and protection of	FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3	Passed.

Test ID	Description	Security Function	Results
	the channel data from modification or disclosure. 2. To test that the TOE permit [the TSF and OpenVPN clients and/or servers] to initiate communication via the OpenVPN channel. 3. To test that the TOE initiate communication via the OpenVPN channel for [ingoing/outgoing sessions that require OpenVPN].		
F021 – Secure Communication	1. To test that the TOE provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure] 2. To test that the TOE permit [remote users] to initiate communication via the trusted path. 3. To test that the TOE require the use of the trusted path for [initial user authentication, [all further communication after authentication]].	FTP_TRP.1.1 FTP_TRP.1.2 FTP_TRP.1.3	Passed.
F022 – Secure Communication	To test that the TOE be able to provide reliable time stamps.	FPT_STM.1.1	Passed.

Table 5 : Independent Functional Test

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

2.1.4.3 Vulnerability Analysis

- 48 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, implementation representation and security architecture description.
- 49 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a **Enhanced-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

- 50 The penetration tests focused on:
- a) Broken Access Control
 - b) Cryptographic Failures
 - c) Injection
 - d) Insecure Design
 - e) Security Misconfiguration
 - f) Vulnerable and Outdated Components
 - g) Identification and Authentications Failures
 - h) Software and Data Integrity Failures
 - i) Security Logging and Monitoring Features
 - j) Server-Side Request Forgery (SSRF)
- 51 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

- 52 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

- 53 After due consideration during the oversight of the execution of the evaluation by the certifiers and review of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies that the evaluation of NC2.vpn+ V2.2.1, performed by Securelytics SEF has been completed with a **PASS** verdict.
- 54 Securelytics SEF found that NC2.vpn+ V2.2.1 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 4.
- 55 Certification does not guarantee that a TOE is completely free from exploitable vulnerabilities. A residual level of risk remains that previously undiscovered exploitable vulnerabilities may exist within its claimed security functionality. However, this risk is reduced as the assurance level achieved by the TOE increases.

3.1 Assurance Level Information

- 56 EAL4 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE and a subset of the implementation, to understand the security behaviour.
- 57 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results and a vulnerability analysis (based on the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.
- 58 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation and evidence of secure delivery procedures.
- 59 This EAL represents a meaningful increase in assurance by requiring more design description, the implementation representation for the entire TSF and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

3.2 Recommendation

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

- a) The TOE users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.
- b) The TOE users must ensure that the TOE and its supporting operational environment are physically protected against unauthorized access, and that local management activities are performed only within a physically secured environment.
- c) The TOE users must ensure that the network environment is configured so that network traffic cannot bypass the TOE and that applicable traffic is processed through the TOE in accordance with the configured security policies.
- d) The TOE users must protect TOE user accounts, passwords and certificates from unauthorized access and ensure that access privileges are assigned only to authorized personnel.
- e) The TOE users should regularly review the TOE audit logs and investigate any unexpected or suspicious security-relevant activities.

(Disclaimer: Opinion and interpretations expressed herein are outside the scope of certification)

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 2022, Revision 1, November 2022.
- [3] The Common Methodology for Information Technology Security Evaluation, Version 2022, Revision 1, November 2022.
- [4] MyCC Scheme Requirement (MYCC_REQ), V2, April 2025.
- [5] ISCB Evaluation Facility Manual (ISCB_EFM), v4, April 2025.
- [6] SCS NC2.vpn+ V2.2.1 Security Target, v1.1.1, 19 Aug 2026.
- [7] Evaluation Technical Report (T2504-2-ETR 1.0) – NC2.vpn+ V2.2.1, V1.0, 15 Sept 2026.

A.2 Terminology

A.2.1 Acronyms

Table 6 : 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

Acronym	Expanded Term
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
SCS	System Consultancy Services Sdn. Bhd.

A.2.2 Glossary of Terms

Table 7 : 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-to-day 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 ---