



SCS NC2.vpn+ V2.2.1 Security Target



For more information visit us at
www.scs.my

Document management

Document identification

Document Title	SCS NC2.vpn+ V2.2.1 Security Target
Document Version	1.1.1
Document Date	19 AUG 2026
Release Authority	System Consultancy Services Sdn Bhd

Document history

Version	Date	Description
0.1.0	23 MAY 2025	Initial Released.
0.2.0	02 JUN 2025	Feedback review by SCS (Revision).
0.3.0	27 JUN 2025	Feedback review by SCS (Revision).
0.4.0	01 OCT 2025	Updated based on EOR and CAR feedback.
0.5.0	07 OCT 2025	Feedback review by SCS (Revision).
0.6.0	15 OCT 2025	Minor updates.
0.7.0	24 JAN 2026	Updated based on EOR and CAR feedback.
0.8.0	06 APR 2026	Updated based on EOR and CAR feedback.
0.9.0	08 MAY 2026	Updated based on EOR and CAR feedback.
0.10.0	19 JUN 2026	Updated based on EOR and CAR feedback.
1.0.0	20 JUL 2026	Final.
1.1.0	31 JUL 2026	Final – Minor Changes.
1.1.1	19 AUG 2026	Document update

Table of Contents

1	Security Target Introduction	5
1.1	ST Reference	5
1.2	TOE Reference	5
1.3	Defined Terms	5
1.4	TOE Overview	7
1.4.1	<i>TOE Usage and Major Security Functions</i>	<i>7</i>
1.4.2	<i>TOE Type</i>	<i>8</i>
1.4.3	<i>Non-TOE Supporting Hardware, Software and/or Firmware.</i>	<i>9</i>
1.4.4	<i>Non-TOE Hardware, Firmware, and Software Supplied by the IT Environment.....</i>	<i>9</i>
1.4.5	<i>Non-TOE Product Physical/Logical Features and Functions.....</i>	<i>10</i>
1.5	TOE Description	11
1.5.1	<i>Physical Scope of the TOE</i>	<i>11</i>
1.5.2	<i>Logical Scope of the TOE</i>	<i>13</i>
2	Conformance Claim	15
3	Security Problem Definition.....	16
3.1	Overview	16
3.2	Threats.....	16
3.3	Organisational Security Policies.....	17
3.4	Assumptions	17
4	Security Objectives.....	18
4.1	Overview	18
4.2	Security Objectives for the TOE.....	18
4.3	Security Objectives for the TOE Operational Environment	19
4.4	Security objectives rationale	20
4.4.1	<i>TOE security objectives rationale</i>	<i>21</i>
4.4.2	<i>Environment security objectives rationale</i>	<i>22</i>
5	Security Requirements	23
5.1	Overview	23
5.2	Extended Components Definition	23
5.2.1	<i>FFW_RUL_EXT Stateful Traffic Filter Firewall.....</i>	<i>23</i>
5.3	Security Functional Requirements	26
5.3.1	<i>Overview</i>	<i>26</i>
5.3.2	<i>FFW_RUL_EXT.1 Stateful Traffic Filtering</i>	<i>27</i>
5.3.3	<i>FAU_GEN.1 Audit data generation</i>	<i>28</i>

5.3.4	<i>FAU_SAR.1 Audit review</i>	29
5.3.5	<i>FCS_CKM.1 Cryptographic key generation</i>	29
5.3.6	<i>FCS_CKM.2 Cryptographic key distribution</i>	30
5.3.7	<i>FCS_CKM.3 Cryptographic key access</i>	30
5.3.8	<i>FCS_RNG.1 Random number generation</i>	30
5.3.9	<i>FCS_CKM.6 Timing and event of cryptographic key destruction</i>	31
5.3.10	<i>FCS_COP.1 Cryptographic operation</i>	31
5.3.11	<i>FDP_ACC.1 Subset access control</i>	32
5.3.12	<i>FDP_ACF.1 Security attribute-based access control</i>	32
5.3.13	<i>FIA_ATD.1 User attribute definition</i>	33
5.3.14	<i>FIA_UAU.2 User authentication before any action</i>	33
5.3.15	<i>FIA_UID.2 User identification before any action</i>	34
5.3.16	<i>FMT_MSA.1 Management of security attributes</i>	34
5.3.17	<i>FMT_MSA.3 Static attribute initialization</i>	34
5.3.18	<i>FMT_MTD.1 Management of TSF data</i>	35
5.3.19	<i>FMT_MOF.1 Management of security functions behaviour</i>	35
5.3.20	<i>FMT_SMF.1 Specification of Management Functions</i>	35
5.3.21	<i>FMT_SMR.1 Security roles</i>	36
5.3.22	<i>FTP_ITC.1 Inter-TSF trusted channel</i>	36
5.3.23	<i>FTP_TRP.1 Trusted path</i>	36
5.3.24	<i>FPT_STM.1 Reliable time stamps</i>	37
5.4	TOE Security Assurance Requirements	38
5.4.1	<i>Explanation for Selecting the SARs</i>	39
5.5	TOE Security Requirements Rationale	40
5.5.1	<i>Dependency Rationale</i>	40
5.5.2	<i>Mapping of SFRs to Security Objectives for the TOE</i>	42
6	TOE Summary Specification (ASE_TSS.1)	46
6.1	Overview	46
6.2	Stateful Traffic Filter Firewall	46
6.3	Virtual Private Network (VPN)	47
6.4	Cryptographic Support	47
6.5	Security Audit	48
6.6	Identification and Authentication	48
6.7	Security Management	49
6.8	Secure Communication	54

1 Security Target Introduction

1.1 ST Reference

ST Title	SCS NC2.vpn+ V2.2.1 Security Target
ST Version	1.1.1
ST Date	19 AUG 2026

1.2 TOE Reference

TOE Title	NC2.vpn+
TOE Version	V2.2.1

1.3 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term	Description
System Administrator	User that has the privilege to perform all operations related to the TOE.
Normal User	User has the privilege (created and assigned with limited access by System Administrator) to perform only selected operations (it can be one operation or more). Normal User does not have the privilege to perform all operations as System Administrator.
TOE User	Consist of System Administrator and Normal User. Both of them are user of the TOE with different privileges and access rights. The term “TOE User” will be used throughout the document that reflect the operation of the TOE that are applicable of both account type without the limitation set specifically on the access rights and privileges setting.
HTTPS	Hypertext Transfer Protocol Secure

Term	Description
ICMP	Internet Control Message Protocol
SSH	Secure Shell
SCS	System Consultancy Services Sdn. Bhd.
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TOE	Target of Evaluation
User data	Data created by and for the user, which does not affect the operation of the TSF.
LAN	Local Area Network

1.4 TOE Overview

1.4.1 TOE Usage and Major Security Functions

The NC2.vpn+ V2.2.1 product 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 Target of Evaluation (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 this 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 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.

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 this Security Target as part of the evaluated TOE security functionality.

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

Table 1: TOE List of Security Functions

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 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.

Security Functions	Descriptions
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.

1.4.2 TOE Type

The NC2.vpn+ V2.2.1 product is a security appliance designed to provide network security services for enterprise network environments. The product integrates multiple networking and security capabilities within a dedicated hardware platform.

The Target of Evaluation (TOE) is the NC2.vpn+ V2.2.1 software, comprising the TOE application software, the configured HardenedBSD operating system, and the associated configuration data necessary to provide the evaluated security functionality described in this Security Target. The TOE executes on a dedicated hardware platform, which provides the operational environment for the TOE software and is outside the scope of this evaluation. Accordingly, no security claims are made for the hardware platform.

The NC2.vpn+ V2.2.1 product also provides 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 explicitly identified elsewhere in this Security Target as part of the evaluated TOE security functionality.

The TOE is categorized as Network and Network-Related Devices and Systems, in accordance with the product categories defined by the Common Criteria Portal (www.commoncriteriaportal.org).

1.4.3 Non-TOE Supporting Hardware, Software and/or Firmware.

The following are the list of supporting hardware, software and/or firmware required by the TOE to operate, which are not part of TOE scope of evaluation.

Table 2: Non-TOE Specifications

Minimum System Requirements	
Appliance	
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.
Web-based GUI User	
Web Browser	• Mozilla Firefox: version 135.0 and above. • Google Chrome: version of 135.0 and above.

1.4.4 Non-TOE Hardware, Firmware, and Software Supplied by the IT Environment

The following are the list of non-TOE hardware, firmware and software, which are supplied by the IT environment, are excluded from the TOE boundary of its operations, as follows.

The components defined in this section are meant for the Local Management components covers the following.

- i. Local Console Software (Serial Console client).
- ii. Web Browser.

- iii. Command Line Interface (CLI) over the Console Port.
- iv. Command Line Interface (CLI) over SSH.
- v. USB Port.
- vi. Display Port.

1.4.5 Non-TOE Product Physical/Logical Features and Functions

The following are the list of non-TOE components specifically related to physical and/or logical features and functions are excluded from the TOE boundary of its operations, as follows.

- i. Hardware of the TOE including appliance case, cables and accessories of the TOE as security appliance as provided by SCS.
- ii. Load Balancer.
- iii. Captive Portal.
- iv. ClamAV.
- v. Dnsmasq DNS.
- vi. Dynamic DNS.
- vii. Intrusion Detection and Inline Prevention Operation.
- viii. OpenDNS & Unbound DNS Operation.
- ix. Web/Cache Proxy Operation.

1.5 TOE Description

1.5.1 Physical Scope of the TOE

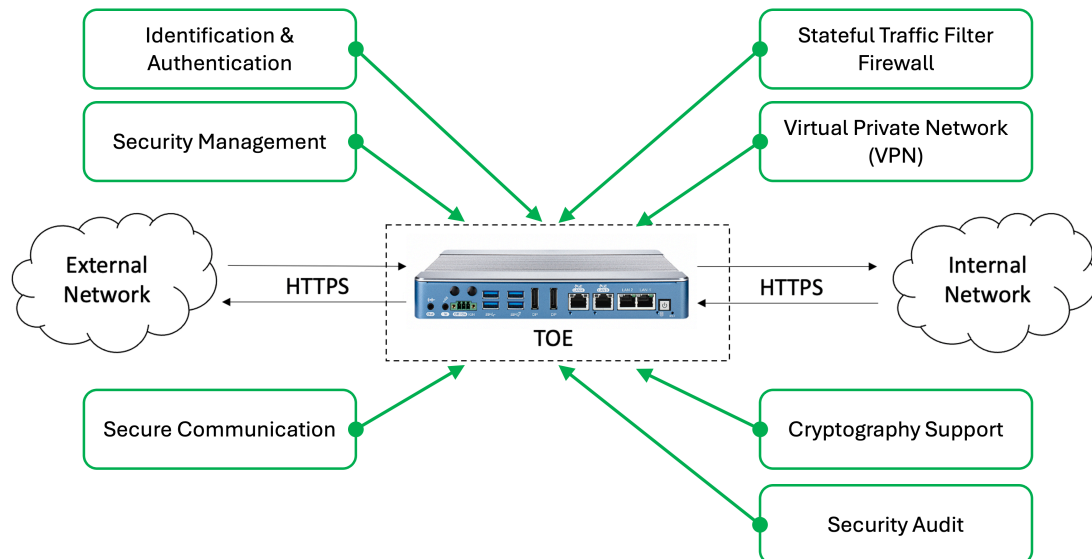


Figure 1 - TOE Physical Scope

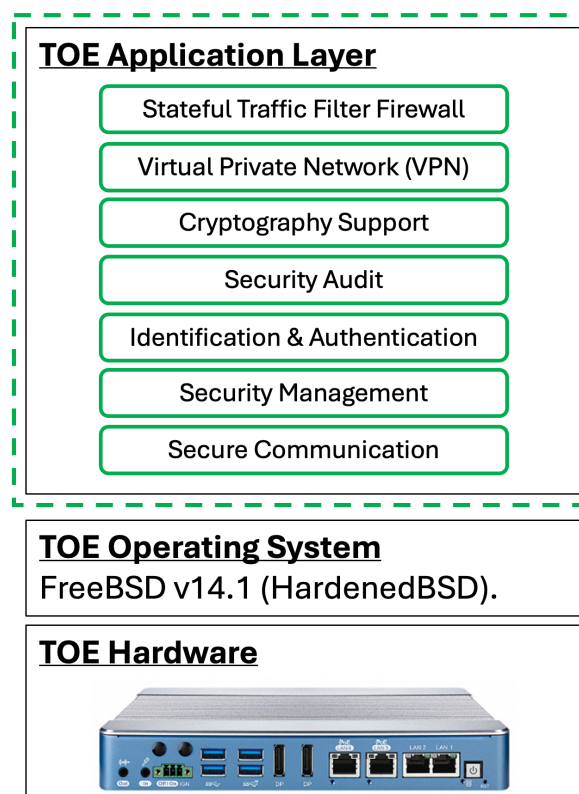


Figure 2 – TOE Boundary Scope

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).

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.

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.

The TOE provides evaluated security functionality including firewall policy enforcement, Virtual Private Network (VPN) services, cryptographic support, identification and authentication, security management, security audit, and secure communication. The TOE also provides additional networking and system management capabilities that are outside the scope of this evaluation unless explicitly identified elsewhere in this Security Target.

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.

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. Components identified in Sections 1.4.3, 1.4.4, and 1.4.5, 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.

The TOE is delivered by **System Consultancy Services Sdn. Bhd. (SCS)** to the customer in accordance with the secure delivery procedure described in Section 3.3. Upon delivery, the customer receives the TOE together with the applicable guidance documentation required for secure installation, configuration, operation, and administration. SCS remains the authorized point of contact for product support and the provision of updated guidance documentation throughout the TOE operational lifecycle.

The contact information for the support centre is:

System Consultancy Services Sdn. Bhd.
No. 36, Jalan Wangsa Delima 6
Wangsa Maju, 53300 Kuala Lumpur
Phone: +603 4149 1919

The TOE operates within the operational environment defined in **Section 1.4.3**, which specifies the minimum hardware and software requirements necessary to support the evaluated configuration.

1.5.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below.

- A. **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.
- B. **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.
- C. **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.
- D. **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).

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

- E. **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. 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. Normal User does not have the privilege to perform all operations similar to System Administrator.

- F. **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.
- G. **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.

2 Conformance Claim

The ST and TOE are conformant to version 2022, Revision 1, November 2022 of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the ST:

- **Part 2 extended.** Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 2022, Revision 1, November 2022.
- **Part 3 conformant, EAL4.** Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, version 2022, Revision 1, November 2022.
- **Part 5 conformant, EAL4.** Conformant with Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, version 2022, Revision 1, November 2022.
- No conformance to a Protection Profile is claimed.

3 Security Problem Definition

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

- a) a series of **threats** that the TOE has been designed to mitigate,
- b) specific **assumptions** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and
- c) any relevant **organisational security policies** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The TOE addresses the following threats.

Table 3: Threats

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.

Identifier	Threat statement
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.

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 4: Assumptions

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.

4 Security Objectives

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in following sections. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

The following are the TOE security objectives.

Table 5: Security Objectives of the TOE

Identifier	Objective statements
O.DATA_FLOW_CONTROL	The TOE shall ensure that only authorized traffic is permitted to flow through the TOE to its destination.
O.ENCRYPT	The TOE is able to protect the authenticity, confidentiality and integrity of traffic from, to or through the TOE by using OpenVPN-based encryption.
O.PROTECTED_MANAGEMENT	The TOE shall allow authorized TOE User to manage the TOE across protected communication channels.
O.LOGGING	The TOE shall log all forms of security-relevant actions recorded by the TOE, whilst only allow System administrators and Normal User to view and export them.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.

4.3 Security Objectives for the TOE Operational Environment

The following are the security objectives for the operational environment of the TOE.

Table 6: Security Objectives of the TOE Operational Environment

Identifier	Objective statements
OE.PHYSICAL	Physical security measures appropriate for the TOE, and its data are assumed to be implemented by the customer organization as part of its IT environment. All local IT management activities must be conducted exclusively within this physically secured environment. Similarly, any RADIUS and/or Syslog servers integrated with the TOE must be housed within a protected infrastructure, and all communications between these servers and the TOE must be safeguarded against unauthorized access or interception.
OE.SINGLE_CONNECTION	The networks connected to the TOE shall be configured so that information cannot flow outside or bypass the TOE.
OE.TRUSTED_ADMIN	The TOE System Administrator are expected to follow all administrator guidance.

4.4 Security objectives rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

Table 7: Security Objective Rational Mapping

THREATS/ ASSUMPTIONS OBJECTIVES	T.UNAUTHORIZED_DATA	T.READ_MODIFY_DATA	T.UNAUTHORIZED_ACCESS	T.UNDETECTED_ACTIONS	T.TOECOM	A.PHYSICAL	A.SINGLE_CONNECTION	A.TRUSTED_ADMIN
O.DATA_FLOW_CONTROL	✓							
O.ENCRYPT		✓						
O.PROTECTED_MANAGEMENT			✓					
O.LOGGING				✓				
O.TOECOM					✓			
OE.PHYSICAL			✓			✓		
OE.SINGLE_CONNECTION							✓	
OE.TRUSTED_ADMIN			✓	✓				✓

4.4.1 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE trace back to the threats in the security problem definition.

Table 8: Security Objective Rationale Justification

Threats	Objectives	Rationale
T.UNAUTHORIZED_DATA	O.DATA_FLOW_CONTROL	This security objective counter threat by ensuring all data and network packet traffic flow through the TOE from any source of the network (internal or external).
T.READ_MODIFY_DATA	O.ENCRYPT	This security objective counter threat by stating that the TOE can use OpenVPN-based encryption to protect the authenticity, confidentiality and integrity of the traffic flows.
T.UNAUTHORIZED_ACCESS	O.PROTECTED_MANAGEMENT	This security objective counter threat by specifying that only authorized TOE User can remotely access the TOE, and only through protected channels.
	OE.PHYSICAL	This security objective counter threat by specifying that the TOE itself is physically protected, as is local management.
	OE.TRUSTED_ADMIN	This security objective counter threat by specifying that only System Administrator and Normal User are trusted.
T.UNDETECTED_ACTIONS	O.LOGGING	This security objective counter threat by specifying that actions are logged and only System administrators and Normal User can view and export them.

Threats	Objectives	Rationale
	OE.TRUSTED_ADMIN	This security objective counter threat by specifying that System Administrators and Normal Users will follow the guidance on checking the TOE audit logs.
T.TOECOM	O.TOECOM	This security objective counter threat by O.TOECOM requires the TOE to protect the confidentiality of communications between distributed TOE components.

4.4.2 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions in the security problem definition.

Table 9: Environment Security Objective Rationale Justification

Assumptions	Objectives	Rationale
A.PHYSICAL	OE.PHYSICAL	This security objective counters assumptions by providing the relevant mechanism that protects the TOE physically and logically throughout the TOE operations within the customer organisation IT environment.
A.SINGLE_CONNECTION	OE.SINGLE_CONNECTION	This security objective counters assumption by ensuring all forms of connections shall be configured flow through the TOE.
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	This security objective counters assumption by defining all TOE User are trusted by the customer organisation as appointed System Administrator.

5 Security Requirements

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from CC2022R1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application.

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows **[assignment]**.
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows ***[selection]***.
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows: FDP_IFF.1a and FDP_IFF.1b.

5.2 Extended Components Definition

This section defines the list of Security Functional Requirements (SFRs) Extended for the TOE. The formatting and original definitions of the TOE Extended SFRs are based on CC Part 2.

5.2.1 FFW_RUL_EXT Stateful Traffic Filter Firewall

Family Behaviour

This ST defines a new functional class for use within this ST: Stateful Traffic Filter Firewall (FFW). This family of FFW requirements was created to specify the behaviour of a Stateful Traffic Filter Firewall. The network protocols that the TOE can filter, as well as the attributes that can be used by a System Administrator and Normal User (with limited access provided as defined by System Administrator) to construct a ruleset are identified in this component. How the ruleset is processed (i.e., ordering) is specified, as well as any expected default behaviour on the part of the TOE.

Component levelling

There is only one component

Management: FFW_RUL_EXT.1

The following actions could be considered for the management functions in FMT:

- a) enable/disable a ruleset on a network interface
- b) configure a ruleset

Audit: FFW_RUL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

- a) Minimal.
 - Result (i.e., Pass, Block, Reject) of applying a rule in the ruleset to a network packet.
 - Configuration of the ruleset.

FFW_RUL_EXT.1 Stateful Traffic Filtering

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FFW_RUL_EXT.1.1	The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.
FFW_RUL_EXT.1.2	The TSF shall allow the definition of Stateful Traffic Filtering rules using the network protocol fields: ICMP, IPv4, IPv6, TCP and UDP.
FFW_RUL_EXT.1.3	The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: Pass, Block and Reject.
FFW_RUL_EXT.1.4	The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.
FFW_RUL_EXT.1.5	The TSF shall accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols, which are TCP, UDP based on the following network packet attributes: a) TCP: source and destination addresses, source and destination ports. b) UDP: source and destination addresses, source and destination ports.
FFW_RUL_EXT.1.6	The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic: a) The TSF shall drop packets which are invalid fragments; b) The TSF shall drop fragmented packets which cannot be re-assembled completely; c) The TSF shall drop packets where the source address of the network packet is on a broadcast network, on a multicast network, and/or a loopback address.

	d) The TSF shall drop network packets where the source or destination address of the packet is: unspecified.
FFW_RUL_EXT.1.7	The TSF shall drop network packets where: a) the source address of the network packet is equal to the address of the network interface where the network packet was received; b) the source or destination address of the network packet is a link-local address; c) the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.
FFW_RUL_EXT.1.8	The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.
FFW_RUL_EXT.1.9	The TSF shall deny packet flow if a matching rule is not identified.
Notes:	None.

5.3 Security Functional Requirements

5.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Table 10: SFRs

Identifier	Title
FFW_RUL_EXT.1	Stateful Traffic Filtering
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.3	Cryptographic key access
FCS_RNG.1	Generation of random numbers
FCS_CKM.6	Timing and event of cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions

Identifier	Title
FMT_SMR.1	Security roles
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path
FPT_STM.1	Reliable time stamps

5.3.2 FFW_RUL_EXT.1 Stateful Traffic Filtering

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FFW_RUL_EXT.1.1	The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.
FFW_RUL_EXT.1.2	The TSF shall allow the definition of Stateful Traffic Filtering rules using the network protocol fields: ICMP, IPv4, IPv6, TCP and UDP.
FFW_RUL_EXT.1.3	The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: Pass, Block and Reject.
FFW_RUL_EXT.1.4	The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.
FFW_RUL_EXT.1.5	The TSF shall accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols, which are TCP, UDP based on the following network packet attributes: a) TCP: source and destination addresses, source and destination ports. b) UDP: source and destination addresses, source and destination ports.
FFW_RUL_EXT.1.6	The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic: a) The TSF shall drop packets which are invalid fragments; b) The TSF shall drop fragmented packets which cannot be re-assembled completely; c) The TSF shall drop packets where the source address of the network packet is on a broadcast network, on a multicast network, and/or a loopback addresses.

	d) The TSF shall drop network packets where the source or destination address of the packet is: unspecified.
FFW_RUL_EXT.1.7	The TSF shall drop network packets where: a) the source address of the network packet is equal to the address of the network interface where the network packet was received; b) the source or destination address of the network packet is a link-local address; c) the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.
FFW_RUL_EXT.1.8	The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.
FFW_RUL_EXT.1.9	The TSF shall deny packet flow if a matching rule is not identified.
Notes:	None.

5.3.3 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
Dependencies:	FPT.STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate audit data of the following auditable events: a) ~~Start up and shutdown of the audit functions;~~ b) All auditable events for the [not specified] level of audit; c) [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.1.2	The TSF shall record within the audit data at least the following information: a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

	b) 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] .
Notes:	None.

5.3.4 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [System Administrator and Normal User] with the capability to read [Auditable events within the TOE, as defined in FAU_GEN.1.1] from the audit data.
FAU_SAR.1.2	The TSF shall provide the audit data in a manner suitable for the user to interpret the information.
Notes:	None.

5.3.5 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_CKM.1.1	The TSF shall 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, 256, 512 bits] that meet the following: [ISO/IEC18033-3] .
Notes:	None

5.3.6 FCS_CKM.2 Cryptographic key distribution

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [distribution of session keys using TLS] that meets the following: [none] .
Notes:	None

5.3.7 FCS_CKM.3 Cryptographic key access

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.3.1	The TSF shall perform [cryptographic key access while generating and exporting certificates] in accordance with a specified cryptographic key access method [username, password, certificate and certification password] that meets the following: [ISO/IEC18033-3] .
Notes:	The TOE able to generate its own self-signed certificate as key access for secure communications using cryptographic functions such as VPN access. Aside of that, the TOE also accept external certificate signed by approved CA for cryptographic operations of TOE. Details can be refer to AGD documentations and TOE Administration Guide.

5.3.8 FCS_RNG.1 Random number generation

Hierarchical to:	No other components.
------------------	----------------------

Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [non-physical true] random number generator that implements: [TRNG (True Random Number Generator)] .
FCS_RNG.1.2	The TSF shall provide [bits] that meet [NIST SP800-22] .
Notes:	All random numbers used in the system are TRNG type. The source of the data is audio noise from a microphone. The data is then evaluated using NIST SP800-22 Statistical Test Suite standard. No intervention from the user is needed or allowed. This is done automatically and not visible to the users.

5.3.9 FCS_CKM.6 Timing and event of cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.6.1	The TSF shall destroy [AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB, Camellia, SHA] when [key zeroization] .
FCS_CKM.6.2	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [key zeroization] that meets the following: [none] .
Notes:	In the event of the TOE being compromised physically or logically, upon opening the casing, upon temperature range exceeding 40 degrees Celsius, upon over-voltage(5v) of key storage device. Note that, key zeroization is performed by overwriting the storage space with random values for 7 times.

5.3.10 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or

	FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access
FCS_COP.1.1	The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [Camellia, AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB, Camellia, SHA] and cryptographic key sizes [128, 192, 256, 512 bits] that meet the following: [ISO/IEC18033-3] .
Notes:	For Auth Digest Algorithm, the TOE using: SHA512.

5.3.11 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.			
Dependencies:	FDP_ACF.1 Security attribute-based access control			
FDP_ACC.1.1	The TSF shall enforce the [access control SFP] on [subjects, objects and operations as listed in the Table 11 below] .			
Notes:	Table 11: TOE Management Functions based on Subject and Object			
	No.	Subject	Object	Function
	1	TOE User	Password Function	Password change with password complexity enforcement.
	2		Audit Log Function	Reporting - health, settings, traffic, IP Lockout.
	3		Management Function	System backup, restore viewing history.
	4		Network Function	System gateway and routing.
	5		Certificate Management Function	Trusted Authorities and Certificates
	6		Network Function	Network interfaces settings.
	7		VPN Function and Firewall Function	VPN and Firewall settings

5.3.12 FDP_ACF.1 Security attribute-based access control

Hierarchical to:	No other components.
------------------	----------------------

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the [access control SFP] to objects based on the following: [subject, objects and attributes in Table 11] .
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [a) If the System Administrator and Normal User are successfully authenticated accordingly, then access is granted based on privilege allocated; b) If the System Administrator and Normal User are not authenticated successfully, therefore, access permission is denied].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none] .
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none] .
Notes:	None.

5.3.13 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [username, password, certificate and certificate password] .
Notes:	None.

5.3.14 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Notes:	None.

5.3.15 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.
Notes:	None.

5.3.16 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	The TSF shall 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] .
Notes:	None.

5.3.17 FMT_MSA.3 Static attribute initialization

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [access control SFP] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2	The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.
Notes:	None.

5.3.18 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [modify] the [System Administrator Account and Normal User Account] to [System Administrator and Normal User] .
Notes:	None.

5.3.19 FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to [disable, enable and modify the behaviour of] the functions [TOE Configurations] to [System Administrator and Normal User] .
Notes:	None.

5.3.20 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [refer to Table 11] .
Notes:	None.

5.3.21 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles [System Administrator, Normal User] .
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Notes:	None.

5.3.22 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide an OpenVPN communication channel between itself and ~~another trusted IT product~~ OpenVPN clients and/or servers that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit ~~[the TSF, another trusted IT product]~~ the TSF and OpenVPN clients and/or servers to initiate communication via the ~~trusted~~ OpenVPN channel.
FTP_ITC.1.3	The TSF shall initiate communication via the ~~trusted~~ OpenVPN channel for [ingoing/outgoing sessions that require OpenVPN] .
Notes:	None.

5.3.23 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_TRP.1.1	The TSF shall 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 <i>[modification, disclosure]</i> .
FTP_TRP.1.2	The TSF shall permit <i>[remote users]</i> to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for <i>[initial user authentication, all further communication after authentication]</i> .
Notes:	None.

5.3.24 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Notes:	None.

5.4 TOE Security Assurance Requirements

Evaluation Assurance Level 4 (EAL4) offers assurance through a comprehensive Security Target (ST) and a thorough analysis of the Security Functional Requirements (SFRs) defined within it. This analysis is based on a complete and functional interface specification, guidance documentation, a description of the TOE's basic modular design, and a partial implementation, enabling an understanding of the TOE's security behaviour.

The assurance is further reinforced by independent testing of the Target of Evaluation's Security Functions (TSF), supported by developer testing evidence derived from the functional specification and TOE design. Additionally, there is selective independent confirmation of the developer's test results and a vulnerability analysis. This analysis—based on the functional specification, TOE design, implementation representation, security architecture, and provided guidance, in which led to demonstrate resistance to attackers with an Enhanced-Basic attack potential.

EAL4 also includes assurance through the use of development environment controls, enhanced configuration management of the TOE (including automation), and evidence of secure delivery procedures.

Compared to EAL3, EAL4 provides a significant increase in assurance by requiring a more detailed design description, a complete implementation representation of the TSF, and improved procedures and mechanisms that ensure the TOE remains free from tampering during development.

Table 12: EAL4 List of SARs

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model

Assurance class	Assurance components
	ALC_TAT.1 Well defined developer tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

5.4.1 Explanation for Selecting the SARs

Evaluation Assurance Level 4 (EAL4) strikes an ideal balance between assurance and practicality, making it well-suited for products developed using sound commercial engineering practices. It allows developers to achieve a high level of assurance through structured security engineering without the need for highly specialized expertise or excessive resource investment.

EAL4 is the highest assurance level that remains economically viable for retrofitting into existing product lines, offering a realistic path to certification for mature or widely deployed solutions. It is particularly appropriate when there is a need for moderate to high assurance of security that is independently validated, within conventional, commercially available Targets of Evaluation (TOEs).

By selecting EAL4, we demonstrate a commitment to robust security backed by independent verification, while maintaining alignment with practical development constraints and cost considerations. This makes EAL4 the optimal choice for products requiring trustworthy security assurance in real-world operational environments.

5.5 TOE Security Requirements Rationale

5.5.1 Dependency Rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL4, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

Table 13: Rationale of SFRs

Identifier	Dependency	Inclusion
FFW_RUL_EXT.1	No dependencies	N/A
FAU_GEN.1	FPT.STM.1	FPT_STM.1
FAU_SAR.1	FAU.GEN.1	FAU.GEN.1
FCS_CKM.1	[FCS_CKM.2 or, FCS_CKM.5 or, FCS_COP.1] FCS_CKM.3 [FCS_RBG.1 or, FCS_RNG.1] FCS_CKM.6	FCS_CKM.2 FCS_CKM.3 FCS_RNG.1 FCS_CKM.6 FCS_COP.1
FCS_CKM.2	[FDP_ITC.1 or, FDP_ITC.2 or, FCS_CKM.1 or, FCS_CKM.5] FCS_CKM.3	FCS_CKM.1 FCS_CKM.3
FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FCS_CKM.1
FCS_RNG.1	No dependencies	N/A

Identifier	Dependency	Inclusion
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1 FCS_CKM.5] FCS_CKM.3	FCS_CKM.1 FCS_CKM.3
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_UID.2	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FMT_MSA.1	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_SMR.1 FMT_MSA.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2

Identifier	Dependency	Inclusion
FTP_ITC.1	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A

5.5.2 Mapping of SFRs to Security Objectives for the TOE

Table 14: Mapping SFRs towards Security Objective of the TOE

Objective	Mapped SFRs	Rationale
O.DATA_FLOW_CONTROL	FFW_RUL_EXT.1	This objective is met by specifying a stateful firewall that is able to mediate traffic based on rules defined by System Administrator or Normal User.
O.ENCRYPT	FTP_ITC.1	This objective is met by specifying the TOE can setup OpenVPN channels with other OpenVPN clients or servers.
	FCS_CKM.1	This objective is met by the TOE generates cryptographic keys in accordance with a specified cryptographic key generation algorithm for OpenVPN.
	FCS_CKM.2	This objective is met by the TOE, in which the TOE perform cryptographic key distribution through method defined by the session keys distribution using TLS.
	FCS_CKM.3	This objective is met by the TOE, in which the TOE perform cryptographic key access through method defined in the SFR declarations with reference to the TOE AGD documentations.
	FCS_RNG.1	This objective is met by the TOE, in which the TOE shall provide method of generating random number using the method defined in the SFR declarations with reference to the TOE AGD documentations.

Objective	Mapped SFRs	Rationale
	FCS_CKM.6	This objective is met by the TOE, in which the TOE perform cryptographic key destruction based on timing and/or event using the method defined in the SFR declarations with reference to the TOE AGD documentations.
	FCS_COP.1	This objective is met by the TOE, in which performs cryptographic operation in accordance with a specified cryptographic algorithm for OpenVPN.
O.PROTECTED_MANAGEMENT	FMT_MOF.1	This objective is met by the TOE, by restricting this management to System Administrator and Normal User.
	FMT_MSA.1	This objective is met by the TOE, in which restricts the ability to change default, modify and delete the security attributes such as TOE Configuration and TOE User Account to System Administrator and Normal User.
	FMT_MSA.3	This objective is met by the TOE, in which ensures that there are permissive default values for security attributes that are used to enforce the SFP.
	FMT_MTD.1	This objective is met by the TOE, in which restricts the ability to modify the TOE User accounts to System Administrator and Normal User.
	FMT_SMF.1	This objective is met by the TOE, by allowing access to the lists the security management functions that must be controlled only for System Administrator and Normal User.
	FMT_SMR.1	This objective is met by the TOE, by defining the roles on which access decisions are based.

Objective	Mapped SFRs	Rationale
	FIA_UID.2 FIA_UAU.2	This objective is met by the TOE, by specifying that users must be identified and authenticated before allowing access to the TOE.
	FIA_ATD.1	This objective is met by the TOE, by ensuring the TOE User security attributes are maintained.
	FDP_ACC.1	This objective is met by the TOE, by providing an access control functionality to ensure that access to security functionality is controlled.
	FDP_ACF.1	This objective is met by the TOE, by ensuring that the access to security functionality is controlled.
O.PROTECTED_MANAGEMENT	FMT_MOF.1	This objective is met by the TOE, by restricting this management to System Administrator and Normal User.
	FMT_MSA.1	This objective is met by the TOE, in which restricts the ability to change default, modify and delete the security attributes such as TOE Configuration and TOE User Account to System Administrator and Normal User.
	FMT_MSA.3	This objective is met by the TOE, in which ensures that there are permissive default values for security attributes that are used to enforce the SFP.
	FMT_MTD.1	This objective is met by the TOE, in which restricts the ability to modify the TOE User accounts to System Administrator and Normal User.
	FMT_SMF.1	This objective is met by the TOE, by allowing access to the lists the security management functions that must be controlled only for System Administrator and Normal User.

Objective	Mapped SFRs	Rationale
	FMT_SMR.1	This objective is met by the TOE, by defining the roles on which access decisions are based.
	FIA_UID.2 FIA_UAU.2	This objective is met by the TOE, by specifying that users must be identified and authenticated before allowing access to the TOE.
	FIA_ATD.1	This objective is met by the TOE, by ensuring the TOE User security attributes are maintained.
	FDP_ACC.1	This objective is met by the TOE, by providing an access control functionality to ensure that access to security functionality is controlled.
	FDP_ACF.1	This objective is met by the TOE, by ensuring that the access to security functionality is controlled.
O.LOGGING	FAU_GEN.1	This objective is met by the TOE, FAU_GEN.1 specifying which all relevant events to be logged by TOE.
	FAU_SAR.1	This objective is met by the TOE, by allowing System Administrator and Normal User to view and export the audit logs.
	FPT_STM.1	This objective is met by the TOE, by providing reliable time stamps, so that it is known when events happened.
O.TOECOM	FTP_TRP.1	This objective is met by the TOE, in which ensuring that traffic transmitted between TOE components is protected from disclosure and modification.
	FCS_CKM.2	This objective is met by the TOE, which are distributes cryptographic keys in accordance with a specified cryptographic key distribution algorithm.

6 TOE Summary Specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions as stated below, with reference to the Logical scope of the TOE.

- Stateful Traffic Filter Firewall
- Virtual Private Network (VPN)
- Cryptographic Support
- Security Audit
- Identification and Authentication
- Security Management
- Secure Communication

6.2 Stateful Traffic Filter Firewall

The TOE performs Stateful Traffic Filtering on network packets processed by the TOE. The TOE allows System Administrator and Normal User (with limited access provided as defined by System Administrator) to define a set of filtering rules in ensuring the internal network(s) and external network communications are being processed by the TOE by all the network packets traffics passed through the filtering of the TOE capabilities.

The stateful traffic filter firewall operations include as follows.

- i. Allows the definition of stateful traffic filtering rules on various network protocol fields, defined as: ICMP, IPv4, IPv6, TCP, UDP.
- ii. The network packet(s) matches the rule, and the rule says “Pass”. No further rules are applied, and the packet is passed through the TOE.
- iii. The network packet(s) matches the rule, and the rule says “Block/Reject”. No further rules are applied, and the packet is not passed through (which is meant that the network packet will be dropped). The difference between block and reject is that with reject, the network packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender. Whereas, with block the network packet is dropped silently. In either case, the original packet is discarded.
- iv. The network packet(s) does not match the rule, in which case the packet is moved to the next rule.
- v. Acceptance of a network packet(s) without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for these protocols: TCP (source and destination addresses, source and destination ports), UDP (source and destination addresses, source and destination ports).
- vi. Network packet(s) will be dropped, in which are invalid fragments.

- vii. Network packet(s) will be dropped, in which are fragmented packets that cannot be re-assembled completely.
- viii. Network packet(s) will be dropped, in which network packets where the source address of the network packet(s) are as defined below.
 - a) on a broadcast network.
 - b) on a multicast network.
 - c) a loopback address.
- ix. Network packet(s) will be dropped, these network packets where the source or destination address of the packet is unspecified.
- x. Network packet(s) will be dropped, when it fulfils the condition as stated below.
 - a) The source address of the network packet is equal to the address of the network interface where the network packet was received.
 - b) The source or destination address of the network packet is a link-local address.
 - c) The source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.
- xi. Deny packet flow if a matching rule is not identified

Security Functional Requirements: FFW_RUL_EXT.1

6.3 Virtual Private Network (VPN)

The TOE permits OpenVPN clients to initiate communication via the trusted OpenVPN channel. The TOE can act as an OpenVPN server (allowing external entities to set up OpenVPN connections with the TOE) and as an Open VPN client (where the TOE sets up OpenVPN connections with external entities).

The TOE initiates communication via the trusted OpenVPN channel for ingoing/outgoing sessions that require OpenVPN.

Note that, all other 3rd parties' desktop clients or appliances that outside the operations of the TOE that initiates communication of OpenVPN with the TOE are not part of the scope of TOE.

Security Functional Requirements: FTP_ITC.1

6.4 Cryptographic Support

The TOE performs key generation, encryption and decryption using 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. The TOE is also able to destroy cryptographic keys by performing key zeroization. System Administrator and Normal User have to login to the TOE Web GUI and delete the certificate and the cryptographic keys will be deleted automatically after certificate deletion. Note that, the SHA512 only been used for Auth Digest Algorithm operation.

AES cryptographic keys (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 are used by the TOE for VPN (OpenVPN) connections to encrypt and decrypt the OpenVPN tunnel data. The TOE provides a web-based GUI interface that permits the System Administrator or Normal User to configure and manage OpenVPN.

The TOE distributes the session keys using TLS. Distribution of session keys occurred during the TLS handshake when OpenVPN connection is initiated. The OpenVPN server/client performs authentication of TLS packets and shares the TLS authentication key.

Aside from that, the cryptographic functionality of the TOE is supported by key generation of random numbers defined using the method **TRNG**. Furthermore, the process of key destruction based on timing and events are being managed by the TOE using the method **key zeroization**.

In the event of the TOE being compromised physically or logically, upon opening the casing, upon a temperature range exceeding 40 degrees Celsius, upon over-voltage(5v) of key storage device.

Note that, key zeroization is performed by overwriting the storage space with random values for 7 times.

Security Functional Requirements: FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_RNG.1, FCS_CKM.6 and FCS_COP.1.

6.5 Security Audit

The TOE generates a fine-grained set of audit log stored within the TOE in appliance mode. These audit logs are stored locally, and the TOE can also send them to an external SYSLOG server for alternative storage. The TOE will generate audit logs (which contain the date and time of the event, type of event, subject identity and outcome of the transaction event) for the following auditable events, as stated below.

- System Log Files.
- Interface (Wireless Log File).
- Interface (Point-to-Point Log File).
- Firewall Log Files.
- VPN (OpenVPN Log Files).
- IP Lockout.

The System Administrator and Normal User have the capability to view and export these audit records via a web-based GUI interface. Timestamps are generated by TOE for audit logs using the internal source of trusted timestamps. It is generated from the clock provided in the TOE hardware.

Security Functional Requirements: FAU_GEN.1, FAU_SAR.1 and FPT_STM.1.

6.6 Identification and Authentication

The TOE maintains two types of user roles which are the roles System Administrator and Normal User. System Administrator is a TOE User that has the privilege to perform all operations stated in Table 11.

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) as stated in Table 11.

Normal User does not have the privilege to perform all operations as System Administrator. These TOE Users are able to interact with the TOE via a web-based GUI interface. When a TOE User issues a request to the TOE to access protected resources, the TOE requires that the TOE User to identify and authenticate themselves before performing any TSF mediated action.

In order for the TOE User to access the TOE, the TOE User has to enter the management port IP address in the web browser, accessible by their own device. At the login page, TOE User needs to key in a valid username, password, certificate and certificate password for login in order to access the TOE. The TOE checks the credentials presented by the TOE User against the authentication information stored in the database and grants access if the credentials are matched based on privilege allocated and access permission is denied if they are not authenticated successfully.

Security Functional Requirements: FMT_SMR.1, FIA_UAU.2, FIA_UID.2, FIA_ATD.1 and FDP_ACF.1.

6.7 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE. TOE provides a suite of management functions to System Administrator and Normal User. The following tasks are the TOE's management functions as defined in the table below. Table 15 mapped back to Table 11 (FDP_ACC.1), in which Table 11 elaborate the mapped between TOE User (Subject) to the list of TOE Management Functions towards the Object and Function of each object, whilst for Table 15 further elaborate the Table 11 information on the mapping between subject to the TOE operation based on defined menu (accessible functions) stated in the TOE.

Security Functional Requirements: FDP_ACC.1, FDP_ACF.1, FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MOF.1

Table 15: TOE Management Functions based on Table 11 (FDP_ACC.1)

Subject	Menu	Operation	Object (Refer to Table 11, FDP_ACC.1)
TOE User	Lobby	Dashboard (View/ Add Widget)	
		License (View)	
		Password (Update)	Password Function
		Login (Login)	
		Logout (Logout)	
	Reporting	Health (View) – Insight and Netflow	Audit Log Function

Subject	Menu	Operation	Object (Refer to Table 11, FDP_ACC.1)
		Settings (View/ Edit/ Delete)	
		Traffic (View)	
		IP Lockout	
	System	Access (View/ Add/ Edit, Delete)	
		Configuration: • Backup (Edit/ Download/ Restore) • Defaults (Edit) • History (View/ Download/ Revert/ Delete)	Management Function
		Gateways: • Single (View/ Add/ Edit/ Delete) • Group (View/ Add/ Edit/ Delete) • Log File (View, Export)	Network Function
		High Availability: • Settings (View/ Edit) • Status (View)	
		Routes: • Configuration (View/ Add/ Edit) • Status (View) • Log File (View, Export)	Network Function
		Settings: • Administration (View/ Edit) • Cron (View/ Edit/ Delete) • General (View/ Edit) • Logging (View/ Edit)	Management Function

Subject	Menu	Operation	Object (Refer to Table 11, FDP_ACC.1)
		- Logging/ Targets (View/ Add/ Edit/ Delete) - Miscellaneous (View/ Edit) - Tunables (View/ Add/ Edit/ Delete)	
		Snapshot	Management Function
		Trust: - Authorities (View/ Add/ Edit/ Delete/ Export) - Certificates (View/ Add/ Export) - Revocation (Add/ Import) - Settings	Trusted Authorities and Certificates
		Wizard (View/ Add)	
		Log Files: - Backend (View, Export) - General (View, Export) - Web GUI (View, Export) - Audit - Boot	Management Function
		Server: Password Complexity Module	Management Function
		Diagnostics: - Activity (View) - Services (Start/ Refresh/ Stop)	
	Interfaces	LAN (View/ Edit)	Network Function
		WAN (View/ Edit)	

Subject	Menu	Operation	Object (Refer to Table 11, FDP_ACC.1)
		Assignments (View/ Add/ Edit/ Delete)	
		Overview (View)	
		Settings (View/ Edit)	
		Wireless: - Devices (View/ Add/ Edit/ Delete) - Log File (View, Export)	
		Point-to-Point: - Devices (View/ Add/ Edit/ Delete) - Log File (View, Export)	
		Other Types (View/ Add/ Edit/ Delete)	
	Firewall	Diagnostics: - ARP Table (View/ Flush/ Refresh) - DNS Lookup (Lookup) - NDP Table (View/ Refresh) - Netstat (View) - Packet Capture (View/ Edit/ Start) - Ping (Edit/ Ping) - Port Probe (Edit/ Test) - Traceroute (Edit/ Traceroute)	System gateway and routing
		Shaper (View/ Add/ Edit/ Delete)	
		Aliases (View/ Add/ Edit/ Delete)	
		Rules (View/ Add/ Edit/ Delete)	

Subject	Menu	Operation	Object (Refer to Table 11, FDP_ACC.1)
		NAT (View/ Add/ Edit)	
		Groups (View/ Add/ Edit/ Delete)	
		Virtual Ips (View/ Add/ Edit/ Delete)	
		Settings (View/ Edit)	
		Log Files (View, Export)	
		Diagnostics (View/ Delete)	
		Categories	
		Automation	
	VPN	OpenVPN: • Servers (View/ Add/ Edit/ Delete) • Clients (View/ Add/ Edit/ Delete) • Client Specific Overrides (View/ Add/ Edit/ Delete) • Client Export (View) • Connection Status (View) • Log File (View, Export)	VPN Function and Firewall Function
	Services	DHCPv4 (View/ Add/ Edit)	System gateway and routing.
		DHCPv6 (View/ Add/ Edit)	
		Monit (View/ Add/ Edit/ Delete)	
		Network Time (View/ Add/ Edit/ Delete)	
		Captive Portal	
		DCRelay	

Subject	Menu	Operation	Object (Refer to Table 11, FDP_ACC.1)
		Dnsmasq DNS	
		Intrusion Detection	
		Key DHCP	
		nginx	
		Opends	
		Unbound dns	
	Power	Power (Reboot/ Power Off)	

6.8 Secure Communication

The TOE provides trusted paths for communication with remote users that is logically distinct from other communication channels. These trusted paths protect transmitted data from disclosure and undetected modification. All remote communications take place over a secure encrypted session which is HTTPS (TLS v1.2 & TLS v1.3) connection.

Security Functional Requirements: FTP_TRP.1