28 JULY 2021
Document Version 1.0

SCS NC2.VPN+ SECURITY TARGET

For more information visit us at

www.scs.my

Document management

Document identification

Document Title	SCS NC2.vpn+ Security Target
Document Version	1.0
Document Date	28-JULY-2021
Release Authority	System Consultancy Services Sdn Bhd

Document history

Version	Date	Description
0.1	30-SEPT-2020	Initial Released
0.2	16-OCT-2020	Updated Section 1.6.1, Section 5.3.9, Section 6.2.1 and Section 6.7 based on evaluator's comments
0.3	25-NOV-2020	Updated Section 1.5, Section 1.6.1, Section 1.6.2, Section 3.4, Section 4.2, Section 4.3, Section 4.4.1, Section 5.2.1, Section 5.3.1, Section 5.3.17, Section 5.3.21, Section 5.5.2 and Section 6 based on evaluator's comments in MySEF-3-EXE-E050-EOR1-d1
0.4	02-DEC-2020	Updated Section 1.5.1, Section 1.5.2, Section 1.6.1, Section 3.4 and Section 5.2.1 based on evaluator's comments in MySEF-3-EXE-E050-EOR1-d2
0.5	26-JAN-2021	Updated Section 1 and Section 5 based on evaluator's comments in MySEF-3-EXE-E050-EOR4-d1
0.6	11-FEB-2021	Updated Section 1 until Section 6 based on evaluator's comments in MySEF-3-EXE-E050-EOR4-d2 Removed VPN IPsec from the evaluation scope
0.7	01-APR-2021	Updated Section 1 until Section 6 based on evaluator's comments in MySEF-3-EXE-E050-EOR3-d3 and MySEF-3-EXE-E050-EOR5-d1
0.8	16-APR-2021	Removed AES GCM in Section 1.5.1, Section 1.6.2, Section 5.3.5, Section 5.3.8 and Section 6.4
0.9	28-JUNE-2021	Updated the TOE version to v2.1.9 in Section 1.2, Section 1.5.1 and Section 1.5.3 Updated Guidance documentation reference in Section 1.6.2

		Added CAPTCHA description in Section 1.4, Section 1.6.2 and Section 6.6 Added ‘Self Test’ in Section 5.3.9 and Section 6.7 Added 'Self Test log files' in Section 1.6.2, Section 5.3.3 and Section 6.5
1.0	28-JULY-2021	Added AES CFB term in Section 1.4 Final Released

Table of Contents

1 Security Target Introduction (ASE_INT.1)

1.1 ST Reference

ST Title	SCS NC2.vpn+ Security Target
ST Version	1.0
ST Date	28-JULY-2021

1.2 TOE Reference

TOE Title	NC2.vpn+
TOE Version	2.1.9

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 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
Authentication Data	It is information used to verify the claimed identity of a user.
AES CFB	AES CFB will refer to AES CFB128
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
System Administrator	User that has the privilege to perform all operation stated in Table 1 & Table 2.
Normal User	User that has the privilege (assigned by System Administrator) to perform only selected operations (it can be one operation or more) stated in Table 1 & Table 2. Normal User does not has the privilege to perform all operation as System Administrator.
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
RAM	Random Access Memory
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.
Users	System Administrator and Normal User

1.5 TOE Overview

1.5.1 TOE Usage and Major Security Functions

The TOE is NC2.vpn+ version 2.1.9. The TOE is a self-contained box (security appliance) consisting of hardware and software that provides comprehensive high-security gateway solution with seamless communication features providing reliable, robust, fully customizable tools capable of handling any known security threat with software-defined security resiliency. From the stateful inspection firewall to the inline intrusion detection & prevention system, various features are built-in to enhance network performance and protect your network from numerous cyber security threats.

The TOE provides a high level of security by using HardenedBSD that employs the TOE patented security technology and removes the inherent security risks often found in a network application running on non-security focused commercial operating systems, resulting in superior network security. It also includes a high-security gateway capabilities such as Captive Portal (e.g. Forward Caching Proxy, Traffic Shaper etc.), ClamAV, VPN, Dnsmasq DNS & Dynamic DNS, Stateful Traffic Filter Firewall, Load Balancer, Intrusion Detection and Inline Prevention and Reporting (Refer to Table 2 for more details on Reporting operation). Refer to Section 1.6.4 for physical/logical features and functions of the TOE that are not included in the TOE Evaluation.

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

Security Features	Descriptions
Stateful Traffic Filter Firewall	System Administrator and Normal User can provide rules to be used by the TOE to restrict the flow of traffic between the various networks connected to the TOE. Rules can be based on various traffic properties such as source and/or destination address, source and destination ports
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 algorithm that utilizes AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB cryptographic algorithms
Security Audit	The TOE generates audit records for security events. System Administrator and Normal User have the ability to view and export the audit and transaction logs.
Identification and Authentication	System Administrator and Normal User are required to identify and authenticate with the TOE prior to any user action or information flow being permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

Security Features	Descriptions
Secure Communication	The TOE can protect the user data from disclosure and modification by using HTTPS (TLS v1.2 & TLS v1.3) as a secure communication

1.5.2 TOE Type

The TOE is a hardware and software and is used as a high-security gateway solution that provides Captive Portal (e.g. Forward Caching Proxy, Traffic Shaper etc.), ClamAV, VPN, Dnsmasq DNS & Dynamic DNS, Stateful Traffic Filter Firewall, Load Balancer, Intrusion Detection and Inline Prevention, and Reporting (Refer to Table 2 for more details on Reporting operation) capabilities. Refer to Section 1.6.4 for physical/logical features and functions of the TOE that are not included in the TOE Evaluation. The TOE provides security functionality such as Stateful Traffic Filter Firewall, Virtual Private Network (VPN), Cryptographic Support, Security Audit, Identification and Authentication, Security Management, Secure Communication. The TOE can be categorised as *Network and Network-Related Devices and Systems* in accordance with the categories identified in the Common Criteria Portal (www.commoncriteriaportal.org).

1.5.3 Supporting Hardware, Software and/or Firmware

Minimum System Requirements	
Appliance	
Software	NC2.vpn+ v2.1.9
Hardware	ABP-3000-8665U16
Operating System	FreeBSD v12.1 (HardenedBSD)
Web-based GUI User	
Web Browser	Microsoft Edge 44 and later Mozilla Firefox 64 and later Google Chrome 71 and later

1.6 TOE Description

1.6.1 Physical Scope of the TOE

The TOE resides between one or more internal networks (that the TOE is protecting) and an external network such as the Internet. All information transferred between the internal and external networks shall pass through the TOE. Network packets are inspected in real-time as they pass through the TOE (inbound and outbound protection). Malicious network packets are filtered before they have a chance to reach inside the protected network.

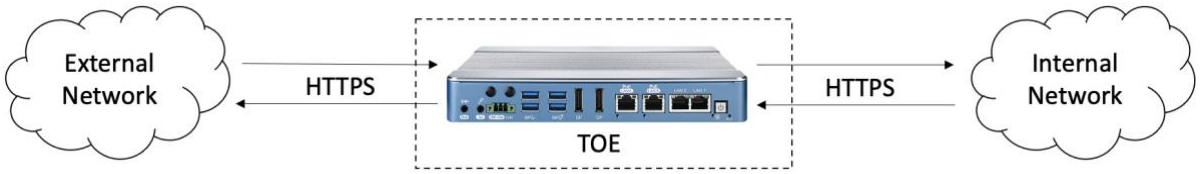

Figure 1 - TOE Physical Scope

The table below identifies the hardware specification and component of the TOE:

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

The TOE is delivered by SCS's authorized representative to the customer. The TOE is wrapped in a plastic bag to provide resistance against moisture. Each TOE is then enclosed in cardboard shipping boxes and sealed with tape that contains SCS logo. A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the box. If any issues occur during the delivery process, the customer or appointed account manager can communicate via a phone call or face-to-face to resolve the issue via contact information provided below. The TOE includes the following guidance documentation; NC2.vpn+ Administration Guide Version 1.0.4.pdf (PDF Document).

The contact information for the support center is:

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

1.6.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below.

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

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

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

- **Security Audit.** The TOE generates audit records for security events. Types of audit logs are:

  - System Log Files
  - Interface (Wireless Log File)
  - Interface (Point-to-Point Log File)
  - Firewall Log Files
  - VPN (OpenVPN & Self Test Log Files)

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

- **Identification & Authentication.** All users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to key in a valid username, password and CAPTCHA code in order to access the TOE. There are two types of users; System Administrator and Normal User. System Administrator is a user that has the privilege to perform all operation stated in Table 1 & Table 2. 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) stated in Table 1 & Table 2. Normal User does not has the privilege to perform all operation as System Administrator.

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

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

1.6.3 Hardware, Firmware, and Software Supplied by the IT Environment

The following hardware, firmware and software, which are supplied by the IT environment, are excluded from the TOE boundary:

- Local management including:
    - Local Console Software (Serial Console client)
    - Web Browser
    - Command Line Interface (CLI) over the Serial/ Console Port
    - Command Line Interface (CLI) over SSH
    - USB Port
    - Display Port

1.6.4 Product Physical/Logical Features and Functions not included in the TOE Evaluation

The TOE is capable of this functionality however the following features have not been examined as part of this evaluation:

- Load Balancer

- Captive Portal
- ClamAV
- Dnsmasq DNS & Dynamic DNS Operation
- VPN (IPsec)
- Intrusion Detection and Inline Prevention Operation
- OpenDNS & Unbound DNS Operation
- Web/Cache Proxy Operation

2 Conformance Claim (ASE_CCL.1)

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2

3 Security Problem Definition (ASE_SPD.1)

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 following are threats identified for the TOE and the IT System the TOE monitors:

Identifier	Threat statement
T.UNAUTHORIZED_DATA	An attacker: - sends data from one network to another network - accesses services on one network from another network while not authorised to do so
T.READ_MODIFY_DATA	An attacker on a network reads traffic or modifies traffic on that network that comes from or through the TOE, or goes to or through the TOE and this is not desired
T.UNAUTHORIZED_ACCESS	An attacker gains unauthorised access to the TOE itself
T.UNDETECTED_ACTIONS	An attacker may take actions that adversely affect the security of the TOE or the networks it is 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.

3.3 Organisational Security Policies

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

3.4 Assumptions

This section contains assumptions regarding the operational environment and the intended usage of the TOE:

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 environment. Local management shall only take place within this physically secured environment. Any RADIUS and/or Syslog servers shall be similarly protected and their connections with the TOE shall be protected against access by attackers.
A.SINGLE_CONNECTION	Information cannot flow among the networks connected to the TOE unless it passes through the TOE.
A.TRUSTED_ADMIN	TOE System Administrators and Normal Users are trusted to follow and apply all administrator guidance in a trusted manner.

4 Security Objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. 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:

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 users to manage the TOE across protected communication channels
O.LOGGING	The TOE shall log security-relevant actions and allow only System administrators and Normal User to review and export them
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.

4.3 Security Objectives for the Environment

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

Identifier	Objective statements
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. Local management shall only take place within this physically secured environment. Any RADIUS and/or Syslog servers shall be similarly protected and their connections with the TOE shall be protected against access by attackers
OE.SINGLE_CONNECTION	The networks connected to the TOE shall be configured so that information cannot flow among them unless it passes through the TOE

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

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.

OBJECTIVES / THREATS/ ASSUMPTIONS	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.

Threats	Rationale
T.UNAUTHORIZED_DATA	This threat is countered by O.DATA_FLOW_CONTROL, which directly restates the threat.

Threats	Rationale
T.READ_MODIFY_DATA	This threat is countered by O.ENCRYPT stating that the TOE can use OpenVPN-based encryption to protect the authenticity, confidentiality and integrity of the traffic flows
T.UNAUTHORIZED_ACCESS	This threat is countered by: • O.PROTECTED_MANAGEMENT specifying that only authorized users can remotely access the TOE, and only through protected channels • OE.PHYSICAL specifying that the TOE itself is physically protected, as is local management • OE.TRUSTED_ADMIN specifying that all System Administrator and Normal User are trusted
T.UNDETECTED_ACTIONS	This threat is countered by: • O.LOGGING specifying that actions are logged and only System administrators and Normal User can review and export them • OE.TRUSTED_ADMIN specifying that System Administrators and Normal Users will follow the guidance on checking the log
T.TOECOM	This threat is countered by O.TOECOM requiring 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.

Assumptions	Rationale
A.PHYSICAL	This assumption is upheld by OE.PHYSICAL, which restates the assumption
A.SINGLE_CONNECTION	This assumption is upheld by OE.SINGLE_CONNECTION, which restates the assumption
A.TRUSTED_ADMIN	This assumption is upheld by OE.TRUSTED_ADMIN, which restates the assumption

5 Security Requirements (ASE_REQ.2)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) 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 (ASE_ECD.1)

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 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: None

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 following network protocol fields:

- ICMP
- IPv4
- IPv6
- TCP
- UDP

FFW_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules:

- Pass
- Block
- 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:

a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: TCP, UDP based on the following network packet attributes:
   - TCP: source and destination addresses, source and destination ports;
   - 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
   - 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.

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.

Identifier	Title
FFW_RUL_EXT.1	Stateful Traffic Filtering
FAU_GEN.1	Audit data generation

Identifier	Title
FAU_SAR.1	Audit review
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	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 initialisation
FMT_MTD.1	Management of TSF data
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTP_ITC.1	Inter-TSF trusted channel (VPN)
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.
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 following network protocol fields:

	a) ICMP b) IPv4 c) IPv6 d) TCP e) UDP
FFW_RUL_EXT.1.3	The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: a) Pass b) Block c) 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: 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 • 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
Dependencies:	No dependencies.
Notes:	None

5.3.3 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit report 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; and **c)** [**Specifically defined auditable events listed in the Notes section below**]**.**
FAU_GEN1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].
Dependencies:	FPT.STM.1 Reliable time stamps
Notes:	Auditable events within the TOE: • System Log Files • Interface (Wireless Log File) • Interface (Point-to-Point Log File) • Firewall Log Files • VPN (OpenVPN and Self Test Log Files)

5.3.4 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**System Administrator and Normal User**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.3.5 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
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**] and specified cryptographic key sizes [**128, 192, 256 bits**] that meet the following: [**ISO 18033-3**]**.**
Dependencies	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	None

5.3.6 FCS_CKM.2 Cryptographic key distribution

Hierarchical to:	No other components.
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**]
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.4 Cryptographic key destruction
Notes:	None

5.3.7 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**key zeroization**] that meets the following: [**none**].
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]
Notes:	None

5.3.8 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB**] and cryptographic key sizes [**128, 192, 256 bits**] that meet the following: [**ISO 18033-3**]
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.4 Cryptographic key destruction
Notes:	None

5.3.9 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**access control SFP**] on [**objects listed in the table 1 below**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	Refer to Section 1.4 for user description.

Table 1 - Subject, Object and Operations for FDP_ACC.1

Subject	Object	Operation
System Administrator / Normal User (only	Lobby	Dashboard (View/ Add Widget)
		License (View)

	able to perform selected operation assigned by System Administrator)		Password (Update)
			Logout (Logout)
		Reporting	Health (View)
			Insight (View/ Export)
			Netflow (View/ Edit)
			Settings (View/ Edit/ Delete)
			Traffic (View)
		System	Access (View/ Add/ Edit, Delete)
			Configuration: • Backup (Edit/ Download/ Restore) • Defaults (Edit) • History (View/ Download/ Revert/ Delete)
			Gateways: • Single (View/ Add/ Edit/ Delete) • Group (View/ Add/ Edit/ Delete) • Log File (View, Export)
			High Availability: • Settings (View/ Edit) • Status (View)
			Routes: • Configuration (View/ Add/ Edit) • Status (View) • Log File (View, Export)
			Settings: • Administration (View/ Edit) • Cron (View/ Edit/ Delete) • General (View/ Edit) • Logging (View/ Edit)

			• Logging/ Targets (View/ Add/ Edit/ Delete) • Miscellaneous (View/ Edit) • Tunables (View/ Add/ Edit/ Delete)
			Trust: • Authorities (View/ Add/ Edit/ Delete/ Export) • Certificates (View/ Add/ Export) • Revocation (Add/ Import)
			Wizard (View/ Add)
			Log Files: • Backend (View, Export) • General (View, Export) • Web GUI (View, Export)
			Diagnostics: • Activity (View) • Services (Start/ Refresh/ Stop)
		Interfaces	LAN (View/ Edit)
			WAN (View/ Edit)
			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)
			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)
		Firewall	Shaper (View/ Add/ Edit/ Delete)
			Aliases (View/ Add/ Edit/ Delete)
			Rules (View/ Add/ Edit/ Delete)
			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)
		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) • Self Test (View, Export) • Log File (View, Export)
		Services	DHCPv4 (View/ Add/ Edit)
			DHCPv6 (View/ Add/ Edit)
			Monit (View/ Add/ Edit/ Delete)

			Network Time (View/ Add/ Edit/ Delete)
		Power	Power (Reboot/ Power Off)

5.3.10 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**access control SFP**] to objects based on the following: [**as listed in the Table 1**].
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 authorise 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**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.3.11 FIA_ATD.1 User attribute definition

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

5.3.12 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication

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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.3.13 FIA_UID.2 User identification before any action

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

5.3.14 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify, delete]*** the security attributes [**TOE Configuration, Users Account**] to [**System Administrator and Normal User**].
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
Notes:	None.

5.3.15 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
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.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.3.16 FMT_MTD.1 Management of TSF data

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

5.3.17 FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
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**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.18 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**Refer to Table 2**]
Dependencies:	No dependencies.
Notes:	None.

5.3.19 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.3.20 FTP_ITC.1 Inter-TSF trusted channel (VPN)

Hierarchical to:	No other components.
FTP_ITC.1.1	The TSF shall provide a**n 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 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**].
Dependencies:	No dependencies.
Notes:	None.

5.3.21 FTP_TRP.1 Trusted path

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

5.3.22 FPT_STM.1 Reliable time stamps

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

5.4 TOE Security Assurance Requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to attackers with basic attack potential.

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

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
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

Assurance class	Assurance components
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4.1 Explanation for Selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

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 EAL2, 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.

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_COP.1] FCS_CKM.4	FCS_CKM.2 FCS_COP.1 FCS_CKM.4
FCS_CKM.2	[FDP_ITC.1, or	FCS_CKM.1

Identifier	Dependency	Inclusion
	FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[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.4	FCS_CKM.1 FCS_CKM.4
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
FTP_ITC.1	No dependencies	N/A

Identifier	Dependency	Inclusion
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

Objective	Rationale
O.DATA_FLOW_CONTROL	This objective is met by: • FFW_RUL_EXT.1 which specifies a stateful firewall that is able to mediate traffic based on rules defined by System Administrator or Normal User
O.ENCRYPT	This objective is met by: • FTP_ITC.1 which specifies that the TOE can setup OpenVPN channels with other OpenVPN clients or servers. • FCS_CKM.1 which generates cryptographic keys in accordance with a specified cryptographic key generation algorithm for OpenVPN • FCS_CKM.4 which destroys cryptographic keys in accordance with a specified cryptographic key destruction method. • FCS_COP.1 which performs cryptographic operation in accordance with a specified cryptographic algorithm for OpenVPN

Objective	Rationale
O.PROTECTED_MANAGEMENT	This objective is met by: • FMT_MOF.1 restricting this management to System Administrator and Normal User • FMT_MSA.1 which restricts the ability to change default, modify and delete the security attributes such as TOE Configuration and Users (System Administrator and Normal User) Account to System Administrator and Normal User. • FMT_MSA.3 which ensures that there are permissive default values for security attributes that are used to enforce the SFP. • FMT_MTD.1 which restricts the ability to modify the user (System Administrator and Normal User) accounts to System Administrator and Normal User • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based. • FIA_UID.2 and FIA_UAU.2 specifying that users must be identified and authenticated before allowing access • FIA_ATD.1 ensures user security attributes are maintained. • FDP_ACC.1 provides an access control functionality to ensure that access to security functionality is controlled. • FDP_ACF.1 ensures that access to security functionality is controlled.
O.LOGGING	This objective is met by: • FAU_GEN.1 specifying which events to log • FAU_SAR.1 allowing System Administrator and Normal User to read the log • FPT_STM.1 providing reliable time stamps, so that it is known when events happened.
O.TOECOM	This objective is met by: • FTP_TRP.1 which ensures that traffic transmitted between TOE components is protected from disclosure and modification • FCS_CKM.2 which 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:

- 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 to define a set of filtering rules.

The stateful traffic filter firewall operations include (**FFW_RUL_EXT.1)** :

- Allow the definition of stateful traffic filtering rules on various network protocol fields; ICMP, IPv4, IPv6, TCP, UDP

- The packet matches the rule, and the rule says “Pass”. No further rules are applied and the packet is passed through the TOE.

- The packet matches the rule, and the rule says “Block/Reject”. No further rules are applied and the packet is not passed through (deleted). 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.

- The packet does not match the rule, in which case the packet is moved to the next rule.

- Accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: TCP (source and destination addresses, source and destination ports), UDP (source and destination addresses, source and destination ports)

- Drop packets which are invalid fragments

- Drop fragmented packets which cannot be re-assembled completely;
- Drop packets where the source address of the network packet is:
  - on a broadcast network
  - on a multicast network
  - a loopback addresses
- Drop network packets where the source or destination address of the packet is unspecified
- Drop network packets where:
  - the source address of the network packet is equal to 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.
- Deny packet flow if a matching rule is not identified

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 (**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 cryptographic algorithm with 128, 192 and 256 bits cryptographic key sizes (**FCS_CKM.1, FCS_COP.1**). The TOE also able to destroy cryptographic keys by performing key zeroization (**FCS_CKM.4**). System Administrator and Normal User have to login to the TOE WebGUI and delete the certificate and the cryptographic keys will be deleted automatically after certificate deletion.

AES cryptographic keys (AES CBC, AES CFB, AES CFB1, AES CFB8, AES OFB with 128, 192 and 256 bits cryptographic key sizes) are used by the TOE for VPN (OpenVPN) connections to encrypt and decrypt the OpenVPN tunnel data **(FCS_COP.1)**. The TOE provides web-based GUI interface that permit the System Administrator or Normal User to configure and manage OpenVPN.

The TOE distributes the session keys using TLS (**FCS_CKM.2**). Distribution of session keys occurred during the TLS handshake when OpenVPN connection is initiated. The OpenVPN server/client perform authentication of TLS packets and shared the TLS authentication key.

6.5 Security Audit

The TOE generates a fine-grained set of audit log. These 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 (**FAU_GEN.1**):

- System Log Files
- Interface (Wireless Log File)
- Interface (Point-to-Point Log File)
- Firewall Log Files
- VPN (OpenVPN and Self Test Log Files)

The TOE's System Administrator and Normal User have the capability to view and export these audit records via a web-based GUI interface (**FAU_SAR.1**). Timestamps are generated by TOE for audit logs. It is s generated from the clock provided in the TOE hardware (**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 (**FMT_SMR.1**). System Administrator is a user that has the privilege to perform all operation stated in Table 1 & Table 2. 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) stated in Table 1 & Table 2. Normal User does not has the privilege to perform all operation as System Administrator. These users are able to interact with the TOE via a web-based GUI interface. When a user issues a request to the TOE to access protected resources, the TOE requires that the user to identify and authenticate themselves before performing any TSF mediated action (**FIA_UAU.2, FIA_UID.2**). In order for the users to access the TOE, users have to enter the management port IP address in the browser. At the login page, users need to key in a valid username, password (**FIA_ATD.1**). Users also need to enter a valid CAPTCHA code in order to access the TOE. The TOE checks the credentials presented by the user against the authentication information stored in the database and grant access if they are match based on privilege allocated and access permission is denied if they are not authenticated successfully (**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 (**FDP_ACC.1**, **FDP_ACF.1**, **FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MOF.1**):

Table 2 - Management Function

User Roles	Menu	Operation
System Administrator / Normal User (only able to perform selected operation assigned by System Administrator)	Lobby	Dashboard (View/ Add Widget)
		License (View)
		Password (Update)
		Logout (Logout)
	Reporting	Health (View)
		Insight (View/ Export)
		Netflow (View/ Edit)
		Settings (View/ Edit/ Delete)
		Traffic (View)
	System	Access (View/ Add/ Edit, Delete)
		Configuration: • Backup (Edit/ Download/ Restore) • Defaults (Edit) • History (View/ Download/ Revert/ Delete)
		Gateways: • Single (View/ Add/ Edit/ Delete) • Group (View/ Add/ Edit/ Delete) • Log File (View, Export)
		High Availability: • Settings (View/ Edit) • Status (View)
		Routes: • Configuration (View/ Add/ Edit) • Status (View) • Log File (View, Export)

		Settings: • Administration (View/ Edit) • Cron (View/ Edit/ Delete) • General (View/ Edit) • Logging (View/ Edit) • Logging/ Targets (View/ Add/ Edit/ Delete) • Miscellaneous (View/ Edit) • Tunables (View/ Add/ Edit/ Delete)
		Trust: • Authorities (View/ Add/ Edit/ Delete/ Export) • Certificates (View/ Add/ Export) • Revocation (Add/ Import)
		Wizard (View/ Add)
		Log Files: • Backend (View, Export) • General (View, Export) • Web GUI (View, Export)
		Diagnostics: • Activity (View) • Services (Start/ Refresh/ Stop)
	Interfaces	LAN (View/ Edit)
		WAN (View/ Edit)
		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)
		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)
	Firewall	Shaper (View/ Add/ Edit/ Delete)
		Aliases (View/ Add/ Edit/ Delete)
		Rules (View/ Add/ Edit/ Delete)
		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)
	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) • Self Test (View, Export) • Log File (View, Export)

	Services	DHCPv4 (View/ Add/ Edit)
		DHCPv6 (View/ Add/ Edit)
		Monit (View/ Add/ Edit/ Delete)
		Network Time (View/ Add/ Edit/ Delete)
	Power	Power (Reboot/ Power Off)

Refer to Section 1.4 for user description.

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 (**FTP_TRP.1**).