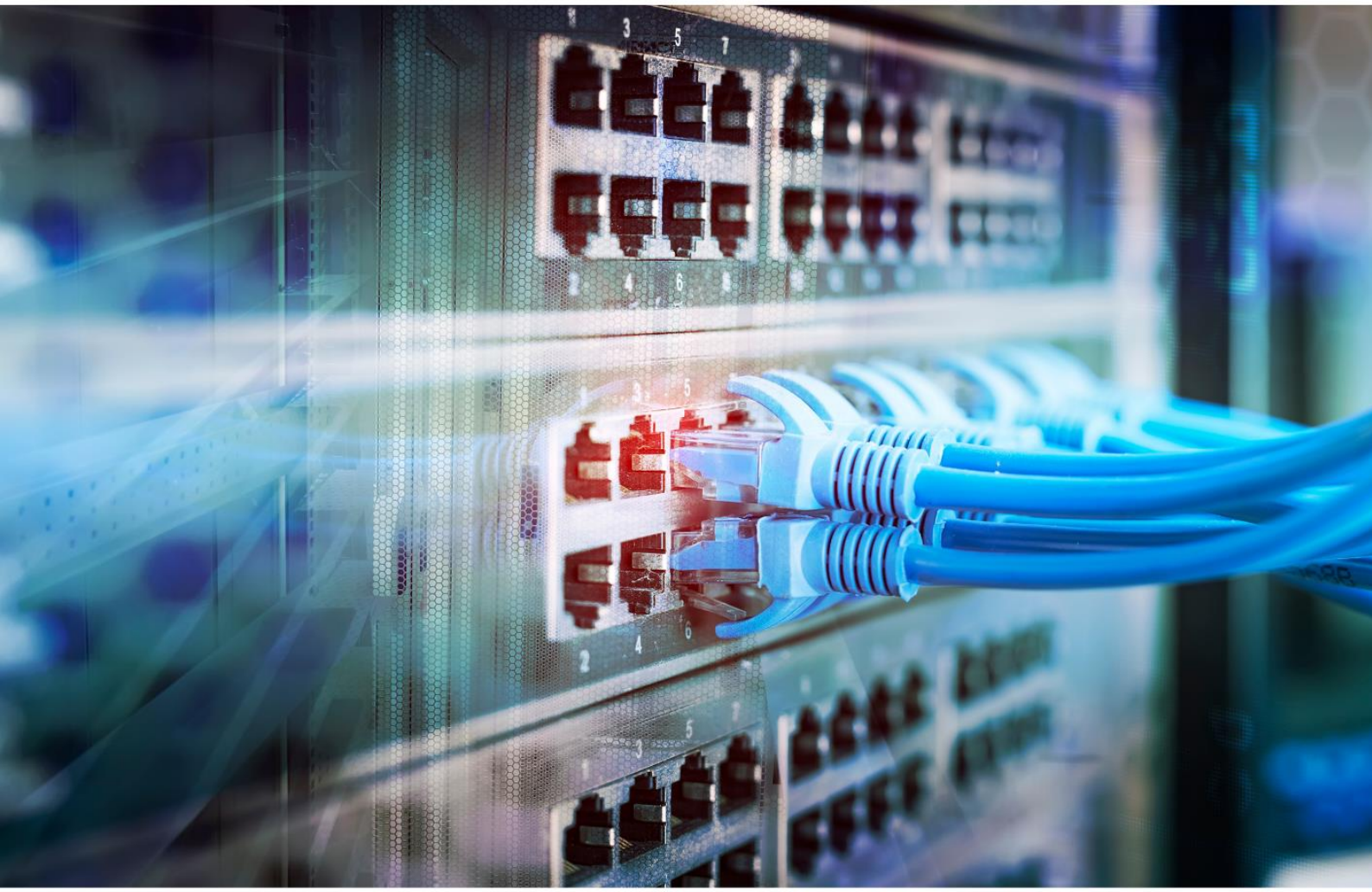
19 MAY 2021
Document Version 1.0



GARCINIA SECURITY TARGET

GARCINIA™
FIREWALL ROUTERS

For more information visit us at

https://sigmarectrix.com

Document management

Document identification

Document Title	Garcinia Security Target
Document Version	1.0
Document Date	19-MAY-2021
Release Authority	Sigma Rectrix Systems (M) Sdn Bhd

Document history

Version	Date	Description
0.1	27-JULY-2020	Initial Released
0.2	07-OCT-2020	Added Section 6 – TOE Summary Specification
1.0	19-MAY-2021	Updated Section 1 until Section 6 to address comments in T2002-4-EOR001 Final Released

Table of Contents

1 Security Target Introduction (ASE_INT.1)

1.1 ST Reference

ST Title	Garcinia Security Target
ST Version	1.0
ST Date	19-MAY-2021

1.2 TOE Reference

TOE Title	Garcinia Firewall Router
TOE Version	v21.1.0

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.
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 Target of Evaluation (TOE) is Garcinia Firewall Router v21.1.0. The TOE is a firewall and routing platform which is a self-contained appliance consisting of hardware and firmware. The TOE is a product that manages the network from any congestion and harm. The TOE analyse the incoming and outgoing network traffic, loss and manipulation of data, business secrets and confidential of data leaks. Lost of time due to the down time is loss of money to the business. Firewall are indeed important and everyone who is online must strive to have a firewall protection before it's vulnerable to external and internal. The TOE core features include Traffic Shaper, Captive portal, Forward Caching Proxy, Virtual Private Network, High Availability & Hardware Failover, Intrusion Detection and Inline Prevention, Build-in reporting and monitoring tools, Support for plugins, DNS Server & DNS Forwarder, DHCP Server and Relay, Dynamic DNS, Backup & Restore, Stateful inspection firewall, Granular control over state table, 802.1Q VLAN support and many more. 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 functions implemented by the TOE:

Security Function	Description
Stateful Traffic Filter Firewall	System Administrator and Normal User can provide rules to be used by the TOE to restrict the flow of traffic between the various networks connected to the TOE. Rules can be based on various traffic properties such as source and/or destination address, source and destination ports
Security Audit	The TOE generates audit records for security events. System Administrator and Normal User have the ability to view and export the audit and transaction 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.
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 firewall and routing platform and is used to analyse the incoming and outgoing network traffic, loss and manipulation of data, business secrets and confidential of data leak. The TOE provides security functionality such as Stateful Traffic Filter Firewall, Security Audit, Identification and

Authentication, Security Management and 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	Garcinia Firewall Router v21.1.0
Hardware Appliance	Garcinia V4, Garcinia V6, Garcinia V8
Web-based GUI User	
Web Browser	Microsoft Edge 44 and later Mozilla Firefox 64 and later Google Chrome 71 and later

Refer to Section 1.6.1 – Physical Scope for more detail on hardware appliance specification

1.6 TOE Description

1.6.1 Physical Scope of the TOE

Figure 1 - TOE Physical Scope

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.

There are three (3) types of hardware appliance model namely Garcinia V4, Garcinia V6 and Garcinia V8. Each appliance model operates using an identical software image with identical functionality. Below is the hardware specification:

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

The TOE is delivered by Sigma Rectrix's authorized representative to the customer. The TOE is wrapped in a plastic bag to provide resistance against moisture. Each TOE is then enclosed in cardboard shipping boxes and sealed with tape that contains Sigma Rectrix logo. A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the box. 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 comes with a user guidance and accessible at https://garcinia.sigmarectrix.com.

The contact information for the support center is:

- Sigma Rectrix Systems (M) Sdn Bhd
  Suite 3-05 ,4805 CBD Perdana 2,
  Jalan Perdana Cyber 12,
  Cyberjaya 63000, Selangor Malaysia

1.6.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below.

- **Stateful Firewall Filtering.** System Administrator and Normal User can provide rules to be used by the TOE to restrict the flow of traffic between the various networks connected to the TOE. Rules will restrict the flow of network traffic between protected networks and other attached networks based on network addresses and ports of the network nodes originating

(source) and/or receiving (destination) applicable network traffic as well as on established connection information. The rules action can be either Pass, Block or Reject. The difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

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

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
- Virtual Private Network (VPN)
- Captive Portal
- ClamAV Operation
- Dnsmasq DNS & Dynamic DNS Operation
- 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.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to modify the behaviour of TSF data without being detected.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.OLDINF	An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
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.

Identifier	Threat statement
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

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

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.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for System Administrator and Normal User use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.MEDIAT	The TOE must mediate the flow of all information from users on an external network to resources on an internal network and must ensure that residual information from a previous information flow is protected and not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables System Administrator and Normal User to use the TOE security functions and must ensure that only System Administrator and Normal User are able to access such functionality.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.
O.DATA_FLOW	The TOE shall ensure that only authorized traffic is permitted to flow through the TOE to its destination.

4.3 Security Objectives for the Environment

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

Identifier	Objective statements
OE.ADMTRA	System Administrator and Normal User are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.PHYSEC	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

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.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.AUDACC	T.AUDFUL	T.MEDIAT	T.NOAUTH	T.OLDINF	T.PROCOM	T.SELPRO	T.TUSAGE	T.TOECOM	T.MISUSE	A.NOEVIL	A.PHYSEC	A.SINGEN
O.ACCOUN	✓												
O.AUDREC	✓												
O.IDAUTH				✓									
O.MEDIAT			✓		✓								
O.SECFUN		✓											
O.SECSTA							✓						
O.TOECOM									✓				
O.DATA_FLOW										✓			
OE.ADMTRA								✓			✓		

OE.GUIDAN								✓					
OE.PHYSEC												✓	
OE.SINGEN													✓

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
O.ACCOUN	This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that System Administrator and Normal User are accountable for the use of security functions related to audit.
O.AUDREC	This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search the information contained in the audit trail.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
O.MEDIAT	This security objective is necessary to counter the threats: T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
O.SECFUN	This security objective is necessary to counter the threat T.AUDFUL by requiring that the TOE provides functionality that ensures that only the System Administrator and Normal User has access to the TOE security functions.
O.SECSTA	This security objective ensures that no information is comprised by the TOE upon startup or recovery and thus counters the threat T.SELPRO.
O.TOECOM	This security objective is necessary to counter the threat T.TOECOM by requiring the TOE to protect the confidentiality of communications between distributed TOE components.
O.DATA_FLOW	This security objective is necessary to counter the threat T.MISUSE by ensuring the TOE is able to collect all network packets flowing between network segments to which it is connected

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
OE.ADMTRA	This non-IT security objective is necessary to counter the threat T.TUSAGE and support the assumption A.NOEVIL because it ensures that System Administrator and Normal User receive the proper training in the correct configuration, installation and usage of the TOE.
OE.GUIDAN	This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.
OE.PHYSEC	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.PHYSEC).
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE (A.SINGEN)

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

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 Filter Firewall
FAU_GEN.1	Audit data generation

Identifier	Title
FAU_SAR.1	Audit review
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control
FIA_ATD.1	User attribute definition
FIA_AFL.1	Authentication failure handling
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_SOS.1	Verification of secrets
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_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 • Firewall 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 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.

<table>
<tr><td>FDP_ACC.1.1</td><td>The TSF shall enforce the [access control SFP] on [objects listed in the table 1 below].</td></tr>
<tr><td>Dependencies:</td><td>FDP_ACF.1 Security attribute based access control</td></tr>
<tr><td>Notes:</td><td>
Table 1 - Subject, Object and Operations for FDP_ACC.1
<table>
<tr><th>Subject</th><th>Object</th><th>Operation</th></tr>
<tr><td rowspan="13">System Administrator / Normal User</td><td rowspan="4">Lobby</td><td>Dashboard (View/ Add Widget)</td></tr>
<tr><td>License (View)</td></tr>
<tr><td>Password (Update)</td></tr>
<tr><td>Logout (Logout)</td></tr>
<tr><td rowspan="5">Reporting</td><td>Health (View)</td></tr>
<tr><td>Insight (View/ Export)</td></tr>
<tr><td>Netflow (View/ Edit)</td></tr>
<tr><td>Settings (View/ Edit/ Delete)</td></tr>
<tr><td>Traffic (View)</td></tr>
<tr><td rowspan="6">System</td><td>Access (View/ Add/ Edit, Delete)</td></tr>
<tr><td>Configuration:
• Backup (Edit/ Download/ Restore)
• Defaults (Edit)
• History (View/ Download/ Revert/ Delete)</td></tr>
<tr><td>Gateways:
• Single (View/ Add/ Edit/ Delete)
• Group (View/ Add/ Edit/ Delete)
• Log File (View, Export)</td></tr>
<tr><td>High Availability:
• Settings (View/ Edit)
• Status (View)</td></tr>
<tr><td>Routes:
• Configuration (View/ Add/ Edit)</td></tr>
</table>
</td></tr>
</table>

			• 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)
		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)

5.3.6 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.

5.3.7 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.

5.3.8 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.

FIA_AFL.1.1	The TSF shall detect when [***a positive integer*** [**3**]] unsuccessful authentication attempts occur related to [**user entering their password for authentication to the TOE**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**block usage of the TOE**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	None.

5.3.9 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.

5.3.10 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.

5.3.11 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**minimum eight (8) characters**]
Dependencies:	No dependencies.
Notes:	None.

5.3.12 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 [**Admin Account, 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.

5.3.13 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.

5.3.14 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.

5.3.15 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.

5.3.16 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: [**as stated in Table 2**]
Dependencies:	No dependencies.
Notes:	None.

5.3.17 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**System Administrator and 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.

5.3.18 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.

5.3.19 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

Assurance class	Assurance components
	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_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 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.

SFR	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

SFR	Dependency	Inclusion
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_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UID.2	FIA_UID.1	FIA_UID.2
FIA_UAU.2	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.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_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.ACCOUN	This objective is completely satisfied by: • FAU_GEN.1 which outlines what events must be audited • FIA_UID.2 ensures that users are identified to the TOE

OBJECTIVE	RATIONALE
O.AUDREC	This objective is completely satisfied by: • FAU_GEN.1 which outlines what events must be audited • FAU_SAR.1 which requires that the audit trail can be read • FPT_STM.1 ensures that reliable time stamps are provided for audit records
O.IDAUTH	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE • FIA_UID.2 which ensures that users are identified to the TOE • FMT_MTD.1 which restricts the ability to modify the user accounts to System Administrator and Normal User • FIA_AFL.1 which detects unsuccessful authentication attempts when user entering their password • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users
O.MEDIAT	This objective is completely satisfied by • FMT_MSA.1 which restricts the ability to change default, modify and delete the security attributes 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 accounts to System Administrator and Normal User

OBJECTIVE	RATIONALE
O.SECFUN	This objective is completely satisfied by • FMT_MOF.1 which ensures the ability to disable, enable and modify the behaviour of the TOE Configurations are restricted to System Administrator and Normal User • FMT_MSA.1 which restricts the ability to change default, modify and delete the security attributes 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 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.
O.SECSTA	This objective is completely satisfied by • FMT_MOF.1 which ensures the ability to disable, enable and modify the behaviour of the TOE Configurations are restricted to System Administrator and Normal User • FMT_MSA.1 which restricts the ability to change default, modify and delete the security attributes 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 accounts to System Administrator and Normal User
O.TOECOM	This objective is completely satisfied by • FTP_TRP.1 which ensures that traffic transmitted between TOE components (client and appliance) is protected from disclosure and modification
O.DATA_FLOW	This objective is completely satisfied by • FFW_RUL_EXT.1 which ensures that only authorized traffic is permitted to flow through the TOE to its destination.

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
- 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 or 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 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
- Firewall 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**)

6.4 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 and password in order to access the TOE (**FIA_ATD.1**). The TOE detects three (3) unsuccessful authentication attempts when user entering their password for authentication to the TOE (**FIA_AFL.1**). 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)**

6.5 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 under the Configuration application privilege. These functions allow for the configuration of the TOE to suit the organization in which it is deployed. The following tasks are the 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	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)
	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)

6.6 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**).