14 APRIL 2020
Document Version 1.0

OPEN KOD DURIO SECURITY TARGET

OPEN KOD
GET IT DONE!

For more information visit us at

www.openkod.com

Document management

Document identification

Document title	Open Kod Durio Security Target
Document version	1.0
Document date	14-APR-2020
Release Authority	Open Kod Sdn Bhd

Document history

Version	Date	Description
0.1	10-SEPT-18	Released for internal review
0.2	04-DEC-18	Updated Section 6
0.3	07-APR-20	Updated Section 1, Section 4 and Section 6 based on evaluator's comments
0.4	08-APR-20	Updated Section 4
1.0	14-APR-20	Final Released

Table of Contents

1 Security Target Introduction

1.1 ST reference

ST Title	Open Kod Durio Security Target
ST Version	1.0
ST Publication Date	14-APR-2020

1.2 TOE reference

TOE Title	Durio Unified Threat Management (UTM)
TOE Version	3.2.5

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 TOE overview

1.4.1 TOE usage and major security functions

The Target of Evaluation (TOE) is Durio Unified Threat Management (UTM) version 3.2.5. The TOE is a comprehensive security product that includes protection against multiple threats. The TOE is a hardware appliance that includes several features such as firewall, antivirus software, content filtering and a spam filter in a single integrated package.

The TOE is designed to provide firewall services ensuring network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks. The TOE is capable of robust filtering based on information contained in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFC's. Additionally, the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols. The TOE has extensive logging capabilities. These audit logs are capable of being exported to an external syslog server over a protected channel for further analysis and inspection.

Refer to Section 1.5.1 for more detail explanations.

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

Security function	Description
Security Audit	The TOE generates audit records for security events. Only Admin has the ability to view/export the audit logs
Identification and authentication	The TOE requires that each user is successfully identified (user IDs) and authenticated before any interaction with protected resources is 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.
Trusted Path	The TOE can protect the user data from disclosure and modification by using Secure Socket Layer (SSL) as a secure communication.

1.4.2 TOE Type

The TOE is Durio Unified Threat Management (UTM) version 3.2.5 and provides security functionality such as Security Audit, Identification and Authentication, Security Management and Trusted Path. The TOE can be categorised as *Other Devices and Systems* in accordance with the categories identified on the Common Criteria Portal (www.commoncriteriaportal.org) that lists all the certified products.

1.4.3 Supporting Hardware, software and/or firmware

The underlying hardware and software that is used to support the TOE are:

Minimum System Requirements	
Durio UTM (Based on hardware model Durio 2H)	
Operating Systems	Linux kernel 4.1.35.e16
Processor	x86/x64 architecture
Memory (RAM)	4GB
Software	Durio Unified Threat Management (UTM) version 3.2.5
CPU Type	Dual Core
Storage	500 GB HDD
End-user	
Web Browser	• Chrome 35 • Safari 10 • Firefox 54 • Microsoft Internet Explorer 11

1.5 TOE description

1.5.1 Physical Boundary

The physical scope of the TOE includes the TOE hardware and software. A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

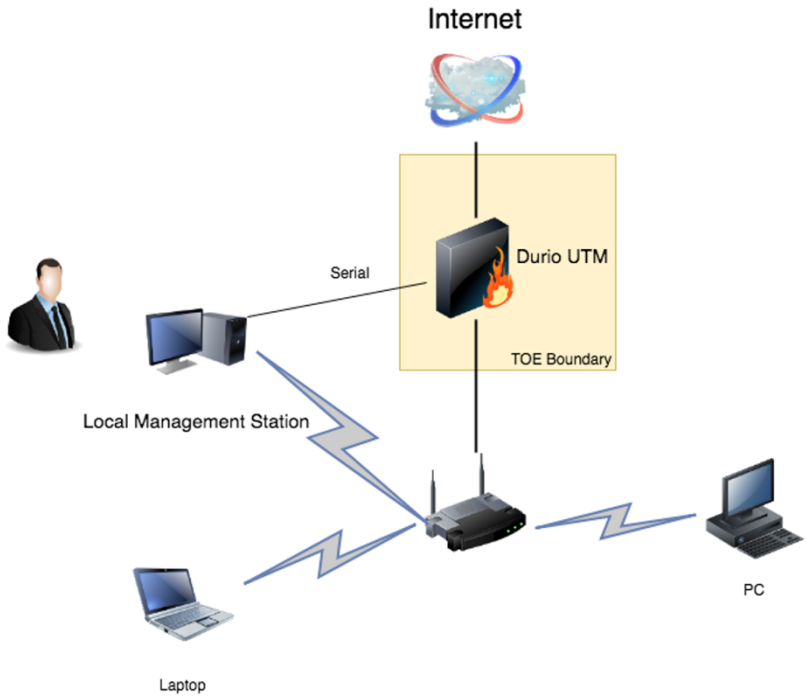

Figure 1 – TOE

The following hardware models are capable of running in the evaluated configuration:

1.5.2 1U Hardware Model

1U Hardware model is for one rack unit of height. To be precise, 1U equals 1.75-inches (44.45mm) of rack height. The TOE 1U models are:

- Durio 2H
- Durio 5H
- Durio 1K

1.5.3 2U Hardware Model

2U devices is 3.5 inches tall and takes up 2 units of rack space. The TOE 2U models are:

- Durio 2K
- Durio 5K

1.5.4 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

a) **Security Audit.** The TOE is capable of generating and securely transmitting Security Audit logs to a remote, external server for further processing and review. The TOE will generate auditable events which may help indicate a number of potential security concerns including login/Logout, Backup and local console and SSH session. For all auditable events the TOE will associate a user (either IP address or with administrative credentials) to the session and use this identifier for all logging to the audit server.

   The event will also be logged to the remote audit server. An authorized administrator may delete the local audit trail. An authorized administrator may configure these or additional auditable events, back-up audit data to an external source and manage audit data storage.

   The auditing function is supported by reliable timestamps provided by the TOE. In the evaluated configuration, the audit server consists of the server.

b) **Identification & Authentication.** All users are required to be identified and authenticated before any information flows are permitted. The TOE checks the credentials presented by the user at the login page against the authentication information stored in the database. All administration requires authentication by user identification and password mechanism. There are two types of users; Admin and Root. Admin is a user that is allowed to perform TOE configuration (except network configuration, turn off device and reboot device) and monitoring via Web-based GUI. Root is a user that has the privilege to perform all TOE configuration and monitoring via Web-based GUI and Command Line.

c) **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 remote and local administrative interfaces that permit the administrative to configure and manage the TOE. In the evaluated configuration the TOE is connected to two or more networks and remote administration request data flows from a Network to the TOE. On the TOE hardware model in each configuration there is also a Local Console, located within the physically secured area described and consists of a physical serial interface to the TOE.

d) **Trusted Path.** The TOE provides a secure SSL channel between the end-user and the TOE.

1.5.5 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

1.5.6 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:

- ClamAV Antivirus
- OpenVPN
- HTTP Proxy
- Spam Training
- Intrusion Prevention System
- Firewall Operations
- Network Uplink Editor
- Dashboard Settings
- Backup Settings and Operations

2 Conformance Claim

The ST and TOE are conformant to version 3.1 (REV 5) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 5), April 2017

- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 5). Evaluation is EAL2, April 2017.

3 Security Problem Definition

3.1 Overview

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

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The TOE addresses the following threats:

Identifier	Threat statement
T.MANAGEMENT	An unauthorized user modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.WEB_ATTACK	An unauthorized person may attempt to compromise the integrity, availability and confidentiality of enterprise information by performing web application attacks.
T.UNAUTHORISED_ACCESS	A user may gain unauthorized access to the TOE and residing data by sending impermissible information through the TOE (such as Brute Force Attacks) resulting the exploitation of protected resources
T.CONFIG	An unauthorized person may read, modify, or destroy 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.

3.3 Organisational security policies

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

3.4 Assumptions

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

Identifier	Assumption statement
A.PLATFORM	The TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities. The TOE relies on this platform to provide logon services via a local or network directory service, and to provide basic audit log management functions. The platform is expected to be configured specifically to provide TOE services, employing features such as a host-based firewall which limits its network role to providing TOE functionality.
A.ADMIN	One or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorized as the Admin, and do so using and abiding by guidance documentation.
A.USER	TOE users are not wilfully negligent or hostile and use the application within compliance of a reasonable enterprise security policy.
A.TIMESTAMP	The platforms on which the TOE operate shall be able to provide reliable time stamps.
A.PHYSICAL	The appliance hosting the firmware and database are in a secure operating facility with restricted physical access and non-shared hardware.

4 Security Objectives

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

Identifier	Objective statements
O.ACCESS	The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources or functions and to explicitly deny access to specific users when appropriate
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data. Only Admin shall have access to TOE management interface.
O.MANAGE	The TOE must allow Admin to effectively manage the TOE, while ensuring that appropriate controls are maintained over those functions.
O.USER	The TOE must ensure that all users are identified and authenticated before accessing protected resources or functions.
O.NOAUTH	The TOE shall protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.PLATFORM	The TOE relies upon the trustworthy platform and hardware to provide policy enforcement as well as cryptographic services and data protection.
OE.ADMIN	The owners of the TOE must ensure that the Admin who manages the TOE is not hostile, competent and apply all Admin guidance in a trusted manner.

OE.USER	Users of the systems are trained to securely use the systems and apply all guidance in a trusted manner.
OE.TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

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/ OSPs	T.MANAGEMENT	T.WEB_ATTACK	T.UNAUTHORISED_ACCESS	T.CONFIG	T.TOECOM	A.PLATFORM	A.ADMIN	A.USER	A.TIMESTAMP	A.PHYSICAL
O.ACCESS	✔	✔	✔							
O.CONFIG				✔						
O.MANAGE	✔									
O.USER	✔		✔							
O.TOECOM					✔					
O.NOAUTH			✔							
OE.PLATFORM						✔				
OE.ADMIN							✔			
OE.USER								✔		
OE. TIMESTAMP									✔	
OE. PHYSICAL										✔

4.4.1 TOE security objectives rationale

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

Threats/OSPs	Objectives	Rationale
T.WEB_ATTACK	O.NOAUTH	The objective ensures that the TOE protect the integrity, availability and confidentiality of enterprise information and itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality and perform web application attacks
T.MANAGEMENT	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O.MANAGE	This objective ensures that the TOE provides the tools necessary for the authorized system admin to manage the security-related functions and that those tools are usable only by users with appropriate authorizations.
	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and deny access to specific users when appropriate
T.UNAUTHORISED_ACCESS	O.NOAUTH	The objective ensures that the TOE protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality
	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and deny access to specific users when appropriate
	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
T.TOECOM	O.TOECOM	The objective ensures that the TOE protect the confidentiality of its dialogue between distributed components.
T.CONFIG	O.CONFIG	The objective ensures that the TOE only allowed authorized person such as Admin to access TOE functions and configuration data.

4.5 Environment security objectives rationale

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

Assumptions	Objective	Rationale
A.PLATFORM	OE.PLATFORM	This objective ensures that the underlying platforms are trustworthy and hardened to protect against known vulnerabilities and security configuration issues.
A.ADMIN	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.USER	OE.USER	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of operating the TOE and the security of the information it contains in a secure manner.
A.TIMESTAMP	OE.TIMESTAMP	This objective ensures that reliable timestamps are provided by the operational environment for the TOE.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that the appliance that hosts the operating system and database are hosted in a secure operating facility with restricted physical access with non-shared hardware.

5 Security Requirements

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 Security functional requirements

5.2.1 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
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control

Identifier	Title
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 (Password)
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

5.2.2 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: • Traffic monitoring - the ntopng graphic interface gives a real time overview of the network traffic using charts. • Summary - get daily summaries of all logs • Logs from the intrusion detection system (IDS), OpenVPN, and antivirus • Firewall - logs from iptables rules

	• Proxy - logs from the HTTP, SMTP, and content filter proxies

5.2.3 FAU_SAR.1 Audit Review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**admin, root**] 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.

5.2.4 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:	**Table 1 - Subject, Object and Operations for FDP_ACC.1**

Subject	Object	Operation
Admin	System	View Dashboard Update Interval time Enabled/Disabled Information
	Status	View TOE Status
	Services	Edit DHCP Enable DHCP Disable DHCP Edit DHCP Fixed Leases View Dynamic Leases Add host for Dynamic DNS Clie Edit ClamAV Setting TimeServer Setting Spam Training Setting IPS Setting (Enable/Disable)

			Edit IPS Rules Traffic Monitoring (Enable/Disable) SNMP Server Setting (Enable/Disable) QoS Settings NAT Port Forwarding	
		Firewall	Port Forwarding/NAT Settings Outgoing Traffic Settings Inter-Zone Traffic Settings VPN Traffic Settings System Access Settings Firewall Diagrams Settings	
		Proxy	Edit HTTP Configuration Settings POP3 Configuration Settings FTP Configuration Settings SMTP Configuration Settings DNS Configuration Settings	
		VPN	Edit Open VPN Settings Edit OpenVPN Client IPSEC Authentication, Ceri	
		Logs and Reports	View Live Logs	
	Root	All Access	-	
		Turn Off & Reboot Device	Turn Off Reboot Device	

5.2.5 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 Admin is successfully authenticated accordingly, then access is granted based on privilege allocated; **b) If the Admin is 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.

5.2.6 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.

5.2.7 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.

5.2.8 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.

5.2.9 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 [**Admin**].
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.

5.2.10 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.

5.2.11 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 [**Admin]**
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.12 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 [**Admin**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.13 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: [• **View/Add/Edit/Delete** • **View/Add/Edit/Delete Views** • **View/Add/Edit/Delete User Accounts** • **View/Export Audit Log**].
Dependencies:	No dependencies.
Notes:	None.

5.2.14 FMT_SMR.1 Security Roles

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

5.2.15 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 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 Security requirements rationale

5.4.1 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
FAU_GEN.1	FPT.STM.1 Reliable time stamps	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform. This has been addressed in Section 3.4 by A.TIMESTAMP.
FAU.SAR.1	FAU.GEN.1 Audit data generation	FAU.GEN.1
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3

SFR	Dependency	Inclusion
FIA_ATD.1	No dependencies	NA
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[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	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_SMR.1 FMT_MSA.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_TRP.1	No dependencies	N/A

5.4.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.USER	FIA_UAU.2	The requirement helps meet the objective by authenticating user before any TSF mediated actions.
	FIA_UID.2	The requirement helps meet the objective by identifying user before any TSF mediated actions
O.ACCESS	FAU_GEN.1	This SFR specifies security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.

Security objective	Mapped SFRs	Rationale
	FAU_SAR.1	This SFR specifies that admin will have the capability to view the audit trail data in log form. It traces back to this objective.
	FIA_ATD.1	The requirement helps meet the objective by ensuring user security attributes are maintained.
	FMT_SMF.1	The requirement helps meet the objective by providing management functions of the TOE for authenticated user.
	FMT_SMR.1	This SFR identifies the roles exist in TOE, which is Admin and Normal User. Each user account created must be associated to the roles. It traces back to this objective.
O.MANAGE	FMT_MTD.1	This SFR restricts the ability to modify the user accounts to Admin. It traces back to this objective.
	FMT_MSA.1	The requirement helps to meet the objective by restricting the ability to modify the security attributes for the Admin.
O.CONFIG	FMT_MTD.1	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MSA.1	The requirement helps meet the objective by restricting user access to security attributes.
	FMT_MSA.3	The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP.
	FMT_SMR.1	The requirement helps meet the objective by defining the security roles used within the TOE.
	FDP_ACC.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FDP_ACF.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FMT_MOF.1	This requirement helps meet the objective by restricting the modification of the TOE behaviour to Admin
O.TOECOM	FTP_TRP.1	The requirement ensures that data sent by users is protected from modification or disclosure.
O.NOAUTH	FIA_UAU.2	The requirement helps meet the objective by authenticating user before any TSF mediated actions.
	FIA_UID.2	The requirement helps meet the objective by identifying user before any TSF mediated actions

5.4.3 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.

6 TOE Summary Specification

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:

- Security Audit;
- Identification and Authentication;
- Security Management;
- Trusted Path

6.2 Security Audit

The TOE is capable of generating and securely transmitting Security Audit logs to a remote, external server for further processing and review. The TOE will generate auditable events which may help indicate a number of potential security concerns including login/Logout, Backup and local console and SSH session. For all auditable events the TOE will associate a user (either IP address or with administrative credentials) to the session and use this identifier for all logging to the audit server. (FAU_GEN.1)

The event will also be logged to the remote audit server. An authorized administrator may delete the local audit trail. An authorized administrator may configure these or additional auditable events, back-up audit data to an external source and manage audit data storage. (FAU_SAR.1)

The auditing function is supported by reliable timestamps provided by the TOE. In the evaluated configuration, the audit server consists of the server.

6.3 Identification and Authentication

The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1). All TOE users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces.

All users are required to be identified and authenticated before any information flows are permitted. The TOE checks the credentials presented by the user at the login page against the authentication information stored in the database. (FIA_UAU.2, FIA_UID.2)

All administration requires authentication by user identification and password mechanism (FIA_ATD.1). Administration may either be performed locally using the Local Console CLI or remotely using the Web-Based GUI. When authenticating to the TOE it supports complex configurable password rules and supports complex character sets. (FDP_ACC.1, FDP_ACF.1). There are two types of users; Admin and Root. Admin is a user that is allowed to perform TOE configuration (except network configuration, turn off device and reboot device) and monitoring via Web-based GUI. Root is a user that has the privilege to perform all TOE configuration and monitoring via Web-based GUI and Command Line.

Any individual attempting to log on for an interactive session will be shown a warning message that they must accept prior to being presented with a prompt to attempt their authentication.

6.4 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 remote and local administrative interfaces that permit the administrative to configure and manage the TOE. In the evaluated configuration the TOE is connected to two or more networks and remote administration request data flows from a Network to the TOE. On the TOE hardware model in each configuration there is also a Local Console, located within the physically secured area described and consists of a physical serial interface to the TOE.

Additionally, each TOE unit comes with a default administrator account with all permissions, which may not be deleted but may have its credentials changed. The term 'authorized administrator' is used throughout this ST to describe an administrator given the appropriate permission to perform tasks as required. Management roles may perform the following tasks (FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FMT_MTD.1, FMT_MSA.1 and FMT_MSA.3):

Subject	Object	Operation
Admin	System	View Dashboard Update Interval time Enabled/Disabled Information Plugin
	Status	View TOE Status
	Services	Edit DHCP Enable DHCP Disable DHCP Edit DHCP Fixed Leases View Dynamic Leases

		Add host for Dynamic DNS Client Edit ClamAV Setting TimeServer Setting Spam Training Setting IPS Setting (Enable/Disable) Edit IPS Rules Traffic Monitoring (Enable/Disable) SNMP Server Setting (Enable/Disable) QoS Settings NAT Port Forwarding
	Firewall	Port Forwarding/NAT Settings Outgoing Traffic Settings Inter-Zone Traffic Settings VPN Traffic Settings System Access Settings Firewall Diagrams Settings
	Proxy	Edit HTTP Configuration Settings POP3 Configuration Settings FTP Configuration Settings SMTP Configuration Settings DNS Configuration Settings
	VPN	Edit Open VPN Settings Edit OpenVPN Client IPSEC Authentication, Ceri
	Logs and Reports	View Live Logs
Root	All Access	-
	Turn Off & Reboot Device	Turn Off Reboot Device

6.5 Trusted Path

When a user accesses the TOE on their browser, by typing in the website address, the TOE will initiate SSL secure channel establishment with the user's browser (FTP_TRP.1). The TOE implements the Secure Sockets Layer (SSL v2/v3) protocol.