antiKor Next Generation Firewall Management v2

v2.0.1188

Security Target

Version 0.25

Mar 17, 2023

Document History

Version	***Date***	***Author***	***Description***
0.1	Jan 31, 2022	Berke Temel ATAK Ali Galip ÇAMLI	First Draft
0.2	Mar 7, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.3	July 26, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.4	July 26, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.5	July 26,2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.6	Oct 6, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.7	Oct 10, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.8	Nov 16, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.9	Nov 21, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.10	Nov 23, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.11	Nov 29, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates

Version	***Date***	***Author***	***Description***
0.12	Dec 6, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.13	Dec 12, 2022	Berke Temel ATAK Ali Galip ÇAMLI	Certification Updates
0.14	Dec 14, 2022	Ali Galip ÇAMLI	Certification Updates
0.15	Dec 16, 2022	Ali Galip ÇAMLI	Certification Updates
0.16	Jan 3, 2023	Ali Galip ÇAMLI	TOE Patch Version Update
0.17	Jan 3, 2023	Ali Galip ÇAMLI	Certification Update
0.18	Jan 5, 2023	Ali Galip ÇAMLI	TOE Patch Version Update
0.19	Jan 6, 2023	Ali Galip ÇAMLI	Certification Update
0.20	Jan 13, 2023	Ali Galip ÇAMLI	Certification Update
0.21	Feb 14, 2023	Ali Galip ÇAMLI	Certification Update
0.22	Feb 28, 2023	Ali Galip ÇAMLI	TOE Patch Version Update
0.23	Mar 3, 2023	Ali Galip ÇAMLI	TOE Patch Version Update
0.24	Mar 10, 2023	Ali Galip ÇAMLI	Certification Update
0.25	Mar 17, 2023	Ali Galip ÇAMLI	Certification Update

Contents

List of Figures

List of Tables

1 Introduction

This ST describes the objectives, requirements and rationale for the Antikor Next Generation Firewall Management v2.

TOE is a Next-Generation Unified Threat Management (UTM) firewall management software solution. By offering a simplified interface and workflow to the security capabilities of its environment, the program creates a security suite on top of the operating system facilities and networking applications.

TOE provides:

- constituents which accomplish analyzing the network traffic and react accordingly through the TOE modules that are *Firewall Settings, Security Rules, QoS Bandwidth Management, QoS Rules, Application Security / IPS Settings, Application Security Rules, Intrusion Detection and Prevention (IPS), SSH Inspection, DoS Flood Mitigation, Web Server Security, Service Filtering Rules, Web (HTTP and HTTPS) Filtering*.
- logging and auditing capabilities of the facilities it manages and internal configuration data through the TOE modules that are *Antispoof Reports, Dynamic Reports, Firewall Reports, System Management Reports, Traffic Statistics, Notification History*
- an access control facility to secure configuration data and audit logs through the TOE modules that are *Session Settings*, *Management Panel Settings*

The TOE also provides configuration management for the TOE modules that are *Client Definitions, Identity Definitions*, *Network Definitions*, *Client Groups, Hotspot Clients, Service Definitions*, *DNS Settings*, *SNMP Settings*, *Cluster Settings*, *Syslog Settings*, *IP Pools*, *IP Alias*, *Ethernet Assignment*, *Virtual Ethernet VLAN Interface with Link Aggregation and Loopback*, *Static Routing*, *Routing Table*, *CPU Utilization*, *Memory Utilization*, *Disc Utilization*, *Ethernet Bandwidths*, *Date and Time Settings*, *Power Management*, *User Roles* and *Management Panel Users*.

Management Console and Secure Web GUI are available parts of the TOE for management purposes.

Management Console features are:

- Advanced diagnostics such as real-time port usage, real-time network interface workload, real-time band-width usage
- Authorization settings for management console and Web GUI
- Backup and Recovery
- Basic diagnostics such as connection troubleshooting, interface status check-up, live packet inspection
- Basic network setup
- Management console, in addition to management console features
- Network configuration tools such as interface setup, routing setup
- Network debugging tools including text based web browser, ping and trace-route

TOE provides a web interface for all configuration purposes. The administrator panel may be used to enable and disable services. The server's LAN and WAN settings may be updated remotely, and the server can be shut down if necessary. The system status of CPU, RAM, and disk use may be viewed via the administrator panel.

Features of the Secure Web GUI are:

- Client and host management
- Client quarantine management

- Hotspot management
- HTTP authentication proxy management
- Logs, real-time statistics and reports
- HTTP and HTTPS filtering and caching management
- Firewall rule set and policy management
- Anti-spoof and IPS/IDS configuration and management
- DMZ management
- NAT configuration
- IPSec and VPN configuration
- Traffic shaping management
- Netflow export configuration
- Network configuration management
- VLAN management
- Virtual network interface configuration
- DHCP management
- Routing management
- Resource monitoring
- Web GUI access control management
- Backup and restore
- Basic network debugging tools
- Eduroam configuration
- Announcement module management
- BOTNET mitigation management
- SMS module configuration

1.1 References

ST Title	Antikor Next Generation Firewall Management v2 Security Target
ST Version	0.25
TOE Title	Antikor Next Generation Firewall Management v2
TOE Version	2.0.1188
TOE Type	Next Generation Firewall Management
Assurance Level	EAL4+ ALC_FLR.1
CC Identification	● Common Criteria Part 1 Version 3.1 Revision 5 ● Common Criteria Part 2 Version 3.1 Revision 5 ● Common Criteria Part 3 Version 3.1 Revision 5 ● Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 5

Table 1.1: TOE and ST references

1.2 TOE Overview

Main security features are summarized as follows:

- **Security audit:** TOE has the capability of generating audit logs which are signed by reliable time stamps, and are only accessible to authorized users.
- **Identification and authentication**: The TOE users should be identified and authenticated to access functions or resources inherited from their roles. There are security limits and metrics for unsuccessful authentications and password intricacies.
- **User data protection**: TOE sustains the access control SFP for its users and protected resources.
- **Security management**: The administrator has full access rights to manage the TOE and all other users are associated with the *moderator* role which is assigned by the administrator.
- **TOE access**: Interactive sessions are terminated when the TOE users reach the specified period of user inactivity or terminate their own sessions by themselves.
- **Trusted Path/Channels:** It provides a reliable TSFs path. It maintains interactive communication with administrators to protect both integrity and privacy.

1.2.1 Firmware / Hardware / Software Required by the TOE

Minimum requirements of the TOE for hardware, software, and firmware are summarized as follows:

Component	***Required***	***Description***
Hardware required for TOE	Yes	● 8 Core Xeon CPU ● 32 GB DDR4 2133 Mhz RAM ● Multi-queue ethernet card (Intel i210 2 port 1GBit/s, Intel i350 4 port 1GBit/s, Intel x540 2 port 10 GBit/s or Intel x710T 4 port 10 GBit/s recommended) ● 256GB SSD disk
Hardware required for management console	Yes	A typical workstation with a modern web browser and a local console client installed
Software required for TOE	Yes	● Operating System: FreeBSD 13.1 ● Database: PostgreSQL 14.5

Table 1.2: Hardware and Software required by the TOE

1.3 TOE Description

A high level schema of the TOE is as follows:

The TOE's users communicate with the backend through the frontend, which is a web application. The frontend sends the backend configuration changes and operational orders, and the backend sends the frontend results and notifications. The backend saves configuration information, audit logs, and operational data to a database and updates the firewall system accordingly. It also communicates with the licensing management on a regular basis to verify the license's validity. The backend's other regular responsibility is to pull data from ACL providers. In this context, only the blue coloured part of the backend is covered by the TOE.

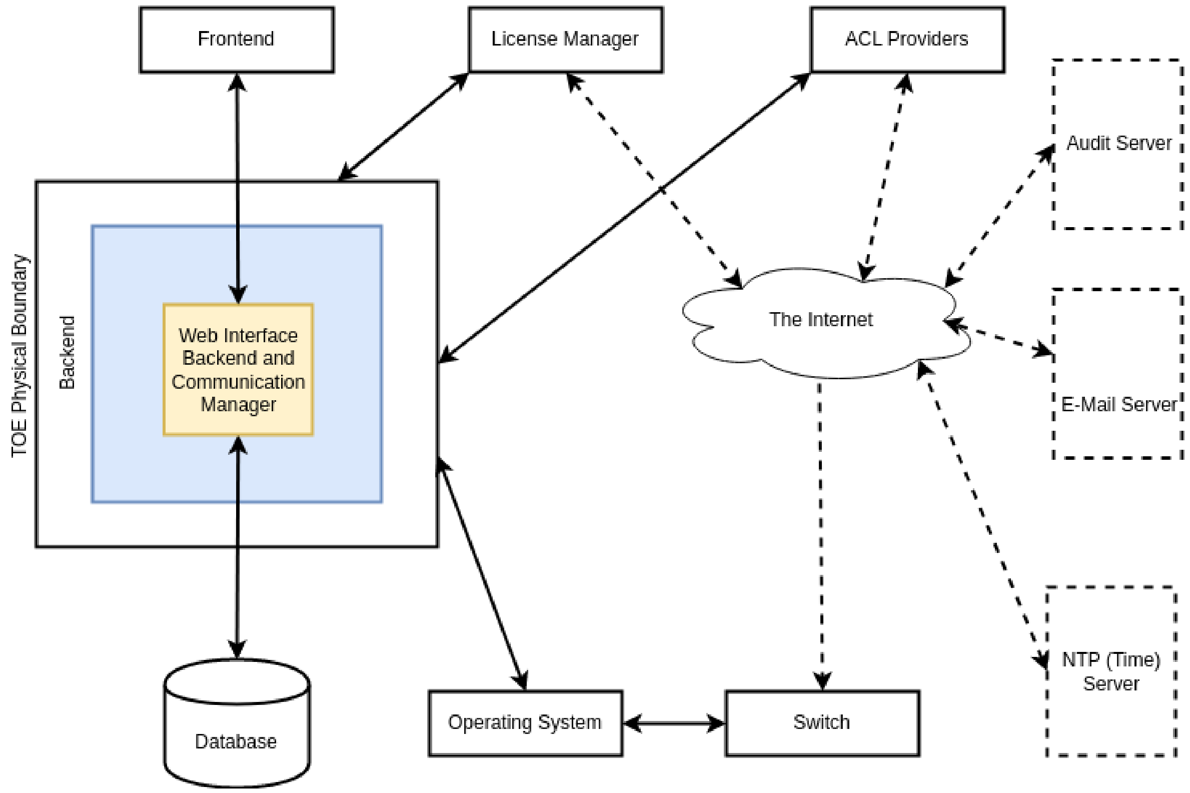

Figure 1.1: The high level schema of TOE

1.3.1 Physical Scope of the TOE

The physical boundaries of the TOE are described in this section, which sets the stage for the TOE examination. The TOE runs on a NanoBSD distribution of FreeBSD. The operating system and hardware addressed by the IT environment descriptions. The operating system, hardware and connected network devices (switch, hub, access point) are not part of the TOE. License Manager and ACL providers are operated by the vendor and are also not part of the TOE.

Physical scope for the TOE are depicted in Figure 1.2.

License manager, ACL providers, the underlying operating system, connected network devices and clients are out of the scope of the evaluation.

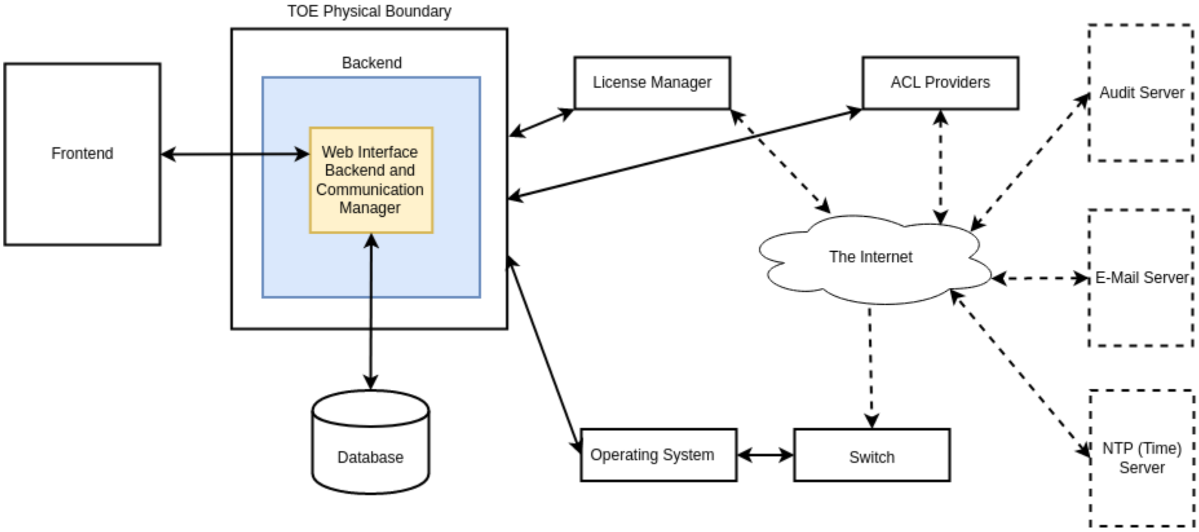

Figure 1.2: Physical boundaries of the TOE

In this context, only the blue coloured part of the backend is covered by the TOE.

TOE will be positioned as an Antikor Next Generation Firewall Management v2 appliance in front of the worldwide network in large institutions (throughput value greater than 10 Gbps). In small businesses (throughput value less than 1 Gbps), DNS requests will be forwarded to the Antikor Next Generation Firewall Management v2 server, and thus a clean traffic will be provided to the customer. The Antikor Next Generation Firewall Management v2 appliance placed in front of WAN will work in Bridge mode, rather than in Routing mode. Therefore, TOE in front of WAN, and even in front of Firewall will not cause any changes on the network. IP access will be assigned just for the management. Traffic cleaned by passing through the filter will be forwarded to the Firewall.

The TOE is supplied to the customer in ISO format, which may be downloaded from the vendor's website. The customer then burns the file on a DVD and starts the installation procedure by booting the PC from the DVD. The computer reboots when the installation is complete, and the TOE is configured for the first time. After that, the licensing manager is utilized to ensure that the installation is legal and valid.

TOE includes the guidance components. Guides are available at http://kitaplik.epati.com.tr/.

1.3.2 Logical Scope of the TOE

The logical TOE boundaries are defined by the security functions provided by the TOE and are described as follows:

1. **Security audit**: The TSF generates audit logs for various auditable events. Date and time, usernames and originating address of the events are recorded. Changes in TSF data related to configuration changes, the underlying system's start-up and shut-down, users who log in and log out, if datagrams received or delivered over network interfaces fit customizable patterns, they are sent or received, resetting passwords, and starting/stopping services. These logs are produced with a reliable time stamp provided by the operational environment. For each auditable event, TOE records the date and time of the event, the subject ID (identity), the type of event, and the success or failure of the event. Authorized administrators have the right to read and view all the recorded logs. Audit data includes the following:

    a. Startup and shutdown of the audit functions
    b. Startup and shutdown of the underlying system
    c. Datagrams received or sent through network interfaces if they match configurable pattern
    d. Login and logout of users.
    e. Log records defined in Table 7.1.

2. **Identification and authentication**: Any operations related to configuration editing and viewing, and operations about audit inspection are subject to identification and authentication. Identification and authorization are required to ensure that the user has administrative privileges. It encounters captcha verification when the number of failed authentication attempts exceeds 15. Unsuccessful authentication events lead to blocking of

the accessing user for a configurable duration. Before allowing access, TOE requires that the TOE user be identified requiring username and password. Passwords are applied to satisfy a sufficient amount of complexity. Before the security function completes successfully, an administrator cannot perform any of the related functions except user identification through login page, and user authentication following user identification. Once defined and verified, users can access functions or resources that are inherited from their roles.

3. **User data protection**: The access control function permits a user to access a protected resource only if administrative credentials are supplied. The administrator can read, delete, modify and create TOE modules and secrets within the scope of the access control SFP.

4. **Security management**: There are two roles: the *administrator* and the *moderator*. Only the administrator has full access rights to manage the TOE. All other users are associated with the moderator role. Administratrator and moderators are restricted by an access control SFP to be able to manage subject identity, metrics for verification of secrets and maximum number of failed login attempts in order to change the defaults, query, modify and delete security attributes. The authorized administrator can alter TSF data by several configuration operations, however a moderator without given permissions cannot change default values for security attributes. Creating, querying, modifying, deleting the security attributes and auditing configuration are available management functions.

5. **Protection of TSF**: When creating or updating a password, the password is encrypted and saved in the internal database using Blowfish-based crypt. Any communication channel does not have access to the password hashes. On hash construction, the salt of Blowfish-based crypt hashing is created at random.

6. **TOE access**: The session inactivity of users exceeds a configurable duration, the authorized users are returned to the login page. The authorized users can terminate their own interactive sessions. The maximum number of concurrent sessions for a single user must be limited by the TSF.
7. **Trusted Path/Channels:** It provides a reliable route of TSFs. To protect both integrity and privacy; it uses TLS1.2 for GUI access to maintain interactive communication with administrators. It also uses HTTPS, TLS1.2 connections to encrypt interactions with network peers, such as an external control server or identity provider.

1.3.3 User Description

TOE provides tools for organizing user groups at different levels of permitted system access. There are predefined permissions and permission sets as roles. When a user account is created, permissions and roles must be assigned to the user. The owner of this account inherits the assigned access levels of the assigned permissions and roles once the owner is successfully identified and verified.

The TOE contains the following user groups:

User Groups	***Access Levels***
Administrator	These users have full read and write access on all pages of the Web UI and can run all of the command line interface (CLI) commands.
Moderator	Users in this group can log on to the Web UI. By default, moderators do not have read and write access to the TOE. If authorized, they can log on to the CLI. In addition, all or specified permissions can be granted or revoked by administrators to view, add, delete, and update on a menu basis. For CLI, they can only run commands authorized by administrators.

Table 1.3: Users access

2 Conformance Claims

2.1 CC Version Conformance Claim

This ST claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- The Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 has to be taken into account.

This ST is Common Criteria for Information Security Evaluation, Part 2, Version 3.1, Revision 5 extended conformant and Common Criteria Part 3, Version 3.1, Revision 5 conformant.

2.2 PP Conformance Claims

This Security Target does not claim conformance to a Protection Profile.

2.3 Package Claim

This Security Target claims augmented conformance to the assurance package EAL4, by adding the Security Assurance Requirement of ALC_FLR.1.

3 Security Problem Definition

3.1 Assets

- **TOE configuration data** by which the TOE users supply to operate the system. TOE configurations are:
  - filters for all traffic, namely Security Settings: *Firewall Settings, Security Rules, QoS Bandwidth Management, QoS Rules, Application Security / IPS Settings, Application Security Rules, Intrusion Detection and Prevention (IPS), SSH Inspection, DoS Flood Mitigation, Web Server Security, Service Filtering Rules*
  - settings for all the system services
  - system settings: *System Information, DNS Settings, Campus Settings, RADIUS Settings, Proxy Settings, Syslog Settings, Log Settings, SSL Certificate Management, HTTP(s) Server Forwarding, DHCP Settings, Cluster Settings, SNMP Configurations, Session Settings, Language Settings*
- **TOE sensitive user data** which is username, password and user identity information: *name*, *surname*, *gender, date of birth*, *nationality*, *national identity number*, *telephone number* and *e-mail address*.

3.2 The Threat Agents

- **Attackers** who have basic knowledge about TOE. The Attacker is assumed to have a basic skill level in how the TOE works and aims to change the settings and operation of the TOE configuration.
- **TOE users** who have extensive knowledge about the TOE operations and are assumed to have a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE.

3.3 Threats

Applicable threats for the TOE are listed in Table 3.1.

Threat	***Description***	
T.UNAUTH	*Assets*	TOE configuration data
	Threat Agents	Attackers
	Threat Definition	Gain unauthorized access to the TOE data.
T.DOS	*Assets*	TOE configuration data
	Threat Agents	Attackers
	Threat Definition	Make the service provided by the TOE or the TOE itself unusable or inaccessible for a period of time to a specific user or all users.
T.CHANNEL	*Assets*	TOE sensitive user data
	Threat Agents	TOE users
	Threat Definition	Gain the valuable information (passwords and enterprise data) of authorized administrators.

Threat	***Description***
T.BRUTE	*Assets* TOE sensitive user data *Threat Agents* Attackers *Threat Definition* Repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.WEAKNESS	*Assets* TOE configuration data *Threat Agents* Attackers *Threat Definition* Exploit a weakness of the protocol used and gain access to the TOE in order to read, modify or destroy TSF data.

Table 3.1: Threats

3.4 Organizational Security Policies

Organizational security policies are listed in Table 3.2.

Policy	***Description***
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.PW_CONFIDENTIALITY	The TOE shouldn't store any plain-text passwords, but only the hashes, and must use the hashes of the passwords to authenticate, which are not available to the TOE users by any means.

Table 3.2: Organizational policies

3.5 Assumptions

Assumptions regarding the environment in which the TOE will reside are listed in Table 3.3.

Assumption	***Description***
A.ADMIN	It is assumed that authorized administrator who is responsible to install, configure and operate the TOE and the IT entities in the operational environment of the TOE are experienced, trained and meet the security conditions.
A.PROTECT	Each appliance configuration is securely managed by authorized people to provide protection of secured data in terms of its confidentiality and integrity.
A.CONFW	The management interface can be accessed through a browser or console port. Physical access to the console port should be restricted.
A.TSP	The IT environment provides reliable time stamps.

Assumption	*Description*
A.PROT	The connections between the network components (*) around the TOE are protected by cryptographic transforms. (Mostly asymmetric encryption is used.) The IT environment provides a hashing function algorithm, whose vulnerability is unknown, for passwords.
A.AUDIT	The IT environment provides a logging server where logs are kept and a means to present a readable view of the audit data.

Table 3.3: Assumptions

(*) The network components stated below in Section 4.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment.

4.1 Security Objectives for the TOE

Security objectives for the TOE are listed in Table 4.1.

Security Objective	***Description***
O.MANAGEMENT	The TOE must provide security management functions in order to modify its configuration and endorse and ensure a secure TOE environment.
O.AUDIT	The TOE must provide an audit trail of security-related events.
O.PASSWORD	Passwords used to authenticate the TOE will be strong enough to resist brute force attacks. The TOE shouldn't store the passwords as clear text, but only the hashes of the passwords, which are not available to anyone by any means.
O.IDENT & AUTH	The TOE must identify and authenticate all users before they access protected resources or functions. In addition, login attempts must be limited and when these limits are passed necessary actions must be taken.
O.SECURE_CONNECTION	The TOE must provide a trusted path/channel between itself and the following entities; another trusted IT product and remote administrators.

Table 4.1: Security objectives for the TOE

4.2 Security Objectives for the Operational Environment

Security objectives for the operational environment are listed in Table 4.2.

Security Objective	***Description***
OE.SECENV	Operational environment of the TOE shall ensure physical and environmental security of the TOE. Unauthorized access shall be restricted and all components in the operational environment shall be secured. Only specifically authorized people shall be allowed to access critical components. In addition, the blocking of denial of service attacks by someone who is unauthorized will be blocked and secured with the expiration of the established limits. TLS1.2 and SSL are used in secure communication of TOE with the management interface.
OE.CREDENTIALS	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users.
OE.TSP	The IT environment provides reliable time stamps.

Security Objective	***Description***
OE.PROT	It is assumed that communication between the network components (*) around the TOE is encrypted. The IT environment provides a hashing function algorithm, whose vulnerability is unknown, for passwords.
OE.AUDIT	The IT environment provides a logging server and a means to present a readable view of the audit data.

Table 4.2: Operational security objectives

(*) The network components stated below in Section 4.3.

4.3 Security Objectives Rationale

		THREATS					OSPs		ASSUMPTIONS					
		T.UNAUTH	T.DOS	T.CHANNEL	T.BRUTE	T.WEAKNESS	P.ACCOUNTABILITY	P.PW_CONFIDENTIALITY	A.ADMIN	A.PROTECT	A.CONFW	A.TSP	A.PROT	A.AUDIT
Security objective for TOE	O.MANAGEMENT			X										
	O.AUDIT	X					X							
	O.PASSWORD	X			X			X						
	O.IDENT & AUTH	X												
	O.SECURE_CONNECTION			X										
Security objectives for operational environment	OE.SECENV		X	X	X	X				X	X		X	
	OE.CREDENTIALS	X		X					X					
	OE.TSP											X		
	OE.PROT	X		X									X	
	OE.AUDIT	X					X							X

Table 4.3: Security objectives rationale

Table 4.3 demonstrates that all security objectives trace back to threats, OSPs and assumptions in the security problem definition.

T.UNAUTH: O.AUDIT security objective is responsible for the TOE that generates audit reports to trace moderator and administrator access events and OE.AUDIT ensures that the audit reports are kept externally and easily analyzable. O.PASSWORD enables the TOE to provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources. O.IDENT&AUTH ensures that the TOE identifies and authenticates all users before they access protected resources or functions. OE.CREDENTIALS is an operational environment objective which ensures that all user credentials are protected appropriately by users and they are not negligent. Finally, OE.PROT aims to protect sensitive authentication data.

T.DOS: OE.SECENV enables necessary measures to facilitate access barriers for arbitrary access to management components.

T.CHANNEL: O.MANAGEMENT and OE.PROT are together responsible for securing communications during operation. O.SECURE_CONNECTION protects integrity and privacy with trusted path/channel. OE.SECENV complements O.MANAGEMENT externally. OE.CREDENTIALS provides protection from user negligence.

T.BRUTE: O.PASSWORD requires the passwords in the TOE to be complicated enough to resist brute force attacks. OE.SECENV is required for additional assurance to address attacks from the operational environment.

T.WEAKNESS: This threat is countered by configuration of the TOE accordingly and making sure that the operational environment is sufficiently secure to block attacks, provided by OE.SECENV.

P.ACCOUNTABILITY: This policy is ensured by operational and environmental auditing provided by O.AUDIT and OE.AUDIT.

P.PW_CONFIDENTIALITY: This policy is ensured by the TOE itself, satisfying the O.PASSWORD.

A.ADMIN: OE.CREDENTIALS ensures proper authentication protection for administrators.

A.PROTECT: Environmental security assumption is backed by OE.SECENV, making sure the physical system is secure.

A.CONFW: This assumption asserts that precautions for the environment have been taken by OE.SECENV.

A.TSP: Requirements for a consistent timestamping of audit logs are provided by OE.TSP.

A.PROT: Secure connections between the *Firewalls, Switches, Access Points, DNS Server, DHCP Server, Web Servers, NTP Servers, Network Servers, Application Servers, FTP Servers, Database Servers, Game Servers, Communication Servers, Virtual Servers, VPN Servers* around the TOE are provided by OE.SECENV and OE.PROT.

A.AUDIT: Making sure the logs are processed and kept secure is provided by OE.AUDIT.

5 Extended Components Definition

5.1 User Data Confidentiality in Retention (FDP_UCR_EXT)

5.1.1 User Data Confidentiality in Retention - FDP_UCR_EXT.1

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure. FDP_UCR_EXT has been added to the FDP class because it is a feature intended to protect TOE user passwords which is user data and the FDP class contains families of functional requirements that focuses on user data protection.

Component Leveling

User Data Confidentiality in Retention FDP_UCR_EXT
1

FDP_UCR_EXT.1 User Data Confidentiality in Retention requires that the TSF prevent

plaintext credential data from being read by any user or subject.

Management: FDP_UCR_EXT.1

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

a) No management functions.

Audit: FDP_UCR_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) No audit necessary.

User Data Confidentiality in Retention - FDP_UCR_EXT.1

Hierarchical to	No other components
Dependencies	No dependencies
FDP UCR_EXT.1.1	The TSF shall store passwords in non-plaintext form.
FDP_UCR_EXT.1.2	The TSF shall prevent the reading of plaintext passwords.

6 Security Requirements

In this section, functional and assurance requirements specific to the TOE and the trace between SFR and the security objectives for the TOE will be provided.

6.1 SFR Formatting

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 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 that are 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 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 an identifier at the end of the component identifier as follows FDP_ACC.1/IDENTIFIER

6.2 Security Functional Requirements

The TOE satisfies the SFRs listed in Table 6.1.

SFR class	***Requirement***	***Description***
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Provide Audit Records
User data protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_UCR_EXT.1	User data confidentiality in retention
User identification (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UID.1	Timing of identification
	FIA_UAU.1	Timing of authentication
Security management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE access (FTA)	FTA_MCS.1	Basic Limitation on Multiple Concurrent Sessions
	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Table 6.1: Security functional requirements

6.2.1 Audit Data Generation - FAU_GEN.1

Hierarchical to	No other components
Dependencies	FPT_STM.1 - Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record 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) **[start-up and shut-down of the underlying system** (d) **Login and logout users** (e) **Datagrams received or sent through network interfaces if they match configurable patterns** (f) **Changes in TSF data related to configuration changes** (g) **Log records defined in Table 7.1.]**,
FAU_GEN.1.2	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]**.

6.2.2 User Identity Association - FAU_GEN.2

Hierarchical to No other components

Dependencies FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.3 Audit Review - FAU_SAR.1

Hierarchical to No other components

Dependencies FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide **[administrator]** with the capability to read **[all audit trail data]** 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.

6.2.4 Subset Access Control - FDP_ACC.1

Hierarchical to	No other components
Dependencies	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the **[access control SFP]** on **[subjects: administrator, moderators with read, delete, modify and create privileges; objects: TOE modules, secrets; operations: read, delete, modify and create]**.

6.2.5 Security Attribute Based Access Control - FDP_ACF.1

Hierarchical to No other components

Dependencies FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the **[access control SFP]** to objects based on the following: **[subjects: administrator, moderators with read, delete, modify and create privileges; subject attributes: username, password; objects: TOE modules, secrets; operations: read, delete, modify and create; object attributes: each TOE module requires a different set of operation accesses in order to utilize them.]**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[administrators are granted access to all functions or resources, moderators provide access according to the permissions granted by administrators. This authorization is passed as read , write, delete, and update for each page separately]**.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

6.2.6 User Data Confidentiality in Retention - FDP_UCR_EXT.1

Hierarchical to No other components

Dependencies No dependencies

FDP_UCR_EXT.1.1 Passwords should also be stored in a non-plaintext format by the TSF.

FDP_UCR_EXT.1.2 Plaintext passwords shouldn't be read by the TSF.

6.2.7 Authentication Failure Handling - FIA_AFL.1

Hierarchical to No other components

Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***[an administrator configurable positive integer within 5-50]*** unsuccessful authentication attempts occur related to **[login attempts by administrator and moderators]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *[met]*, the TSF shall **[disable login functionality for a configurable amount of period between 1 minute and 12 hours]**.

Application Note: *The captcha screen appears [when the number of failed entries exceeds 15].*

6.2.8 Verification of Secrets - FIA_SOS.1

Hierarchical to	No other components
Dependencies	No dependencies
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet **[the following default metrics:** **1. at least 1 uppercase character (A-Z)** **2. at least 1 lowercase character (a-z)** **3. at least 1 digit (0-9)** **4. at least 1 special character (punctuation)** **5. at least 6 characters** **]**.

6.2.9 Timing of Identification - FIA_UID.1

Hierarchical to	No other components
Dependencies	No dependencies
FIA_UID.1.1	The TSF shall allow **[user identification through login page]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.10 Timing of Authentication - FIA_UAU.1

Hierarchical to No other components

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **[user identification through login page, user authentication following user identification]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.11 Management of Security Attributes - FMT_MSA.1

Hierarchical to No other components

Dependencies [FDP_ACC.1 Subset access control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **[access control SFP]** to restrict the ability to *[change_default, query, modify and delete]* the security attributes **[subject identity, metrics for verification of secrets and maximum number of failed login attempts]** to **[the administrator and the moderators]**.

6.2.12 Static Attribute Initialization - FMT_MSA.3

Hierarchical to	No other components
Dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the **[access control SFP]** to provide *[restrictive]* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the **[administrators]** to specify alternative initial values to override the default values when an object or information is created.

6.2.13 Specification of Management Functions - FMT_SMF.1

Hierarchical to	No other components
Dependencies	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[create, query, modify and delete the security attributes and audit configuration]**.

6.2.14 Security Roles - FMT_SMR.1

Hierarchical to	No other components
Dependencies	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles **[administrator, moderator]**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.2.15 Basic Limitation on Multiple Concurrent Sessions - FTA_MCS.1

Hierarchical to	No other components
Dependencies	FIA_UID.1 Timing of identification
FTA_MCS.1.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.
FTA_MCS.1.2	The TSF shall enforce, by default, a limit of **[1000]** sessions per user.

6.2.16 Per user attribute limitation on multiple concurrent sessions - FTA_MCS.2

Hierarchical to FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

Dependencies FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules **[within 5 seconds, 100]**.

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of **[1000]** sessions per user.

Note: TSF limits total connection number to 1000 sessions per user.

6.2.17 TSF Initiated Termination - FTA_SSL.3

Hierarchical to No other components

Dependencies No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[a configurable amount of time, with a default value of 10 minutes and minimum value of 1 minute]**.

6.2.18 User Initiated Termination - FTA_SSL.4

Hierarchical to	No other components
Dependencies	No dependencies
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user’s own interactive session.

6.2.19 Inter_TSF Trusted Channel - FTP_ITC.1

Hierarchical to	No other components
Dependencies	No dependencies
FTP_ITC.1.1	The TSF shall **be able to use HTTPS, TLS to** provide a **trusted** communication channel between itself and another trusted IT product that **supports the following capabilities: audit server, identity provider, email server and** is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [*the TSF, another trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [*logging of audit messages, forwarding authentication request for identity provider, sending notifications for email server*].

6.2.20 Trusted Path - FTP_TRP.1

Hierarchical to	No other components
Dependencies	No dependencies
FTP_TRP.1.1	The TSF ~~shall provide a~~ **should be able to use TLS, HTTPS to establish a logically independent** communication path between itself and **authorized** [*remote*] ~~users~~ **administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure*].
FTP_TRP.1.2	The TSF shall permit [*remote ~~users~~* **administrators**] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **[all remote administrator authentication and initial administrator authentication].**

6.3 Security Assurance Requirements

Security assurance requirements for the TOE constitute the evaluation assurance package EAL4+ (ALC_FLR.1) and are fully defined with reference to CC Part 3. The security assurance requirements constituting EAL4+ (ALC_FLR.1) are in Table 6.2.

Assurance Class	***Assurance Components***
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Lifecycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.1 Basic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools

Assurance Class	***Assurance Components***
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis

Table 6.2: Assurance requirements for the TOE

6.4 Security Assurance Requirements Rationale

The security assurance level of this Security Target was selected as EAL4+ augmented with ALC_FLR.1 in consideration of the value and threat level of the assets protected by the TOE. This level of assurance was chosen because it is based upon maximum assurance from positive security engineering based on good commercial development practices, and being the highest level which is both economically feasible and suitable on an existing product.

EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

EAL 4 provides:

1. a design description, the implementation representation for the entire TSF, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development; provided by ADV and ALC class assurances listed in Table 6.2.

2. assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behavior; provided by ADV and AGD class assurances listed in Table 6.2

3. independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an enhanced-basic attack potential; provided by ATE and AVA class assurances listed in Table 6.2

In addition, in order to identify responses to potential security flaws, ALC_FLR.1, basic flaw remediation is requested, so that the procedures used to provide flaw information, corrections and guidance on corrective actions are provided.

6.5 Security Requirements Rationale

Security requirements rationale is summarized in Table 6.3. The following is an explanation of each rationale.

	O.MANAGEMENT	O.AUDIT	O.PASSWORD	O.IDENT&AUTH	O.SECURE_ CONNECTION
FAU_GEN.1		X			
FAU_GEN.2		X			
FAU_SAR.1		X			
FDP_ACC.1			X		
FDP_ACF.1			X		
FIA_AFL.1				X	
FIA_SOS.1			X	X	
FIA_UID.1				X	
FIA_UAU.1				X	
FMT_MSA.1	X				
FMT_MSA.3	X				
FMT_SMF.1	X				
FMT_SMR.1	X				
FTA_MCS.1	X				
FTA_MCS.2	X				
FTA_SSL.3	X				
FTA_SSL.4	X				
FTP_ITC.1					X
FTP_TRP.1					X
FDP_UCR_EXT .1			X		

Table 6.3: Tracing of functional requirements to objective

O.MANAGEMENT	Security requirements are managed by FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1. Management of TOE access is addressed by FTA_SSL.3 and FTA_SSL.4. Excessive connection of TOE is addressed by FTA_MCS.1. Limitations on per-user attributes for numerous concurrent sessions are addressed by FTA_MCS.2
O.AUDIT	FAU_GEN.1 describes when and what kind of audit data is generated and FAU_GEN.2 ensures the relation between the audit data and the user. FAU_SAR1. provides an appropriate way to interpret audit records.
O.PASSWORD	is provided by enforcing access control on all operations on subjects. FDP_ACC.1 protects control roles and privileges. FDP_ACF.1 protects secret credentials and determines access. FIA_SOS.1 outlines a quality metric for passwords. FDP_UCR_EXT.1 stores passwords in non-plaintext form.
O.IDENT&AUTH	FIA_AFL.1 detects successive authentication failures. FIA_SOS.1 shall provide a mechanism that outlines a quality metric for passwords. FIA_UID.1 and FIA_UAU.1 manage the user related security requirements.
O.SECURE_CONNECTION	FTP_ITC.1 provides a trusted communication channel. FTP_TRP.1 establishes a logically independent communication path.

6.6 Rationale for IT Security Requirement Dependencies

Figure 6.1 depicts dependencies and Table 6.4 lists the claimed TOE and IT Environment security requirements and their dependencies.

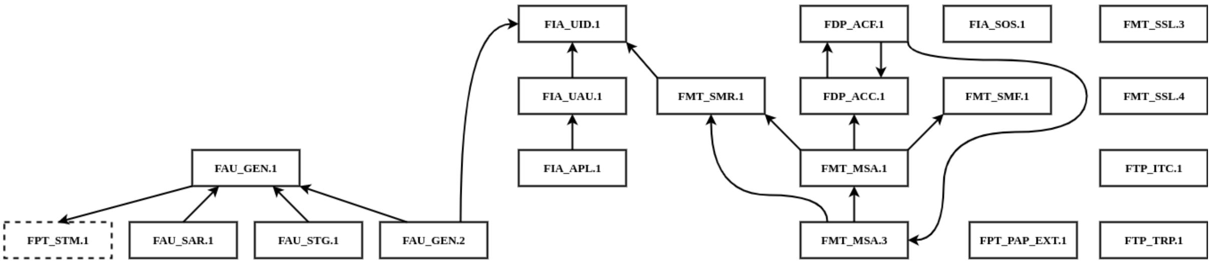

Figure 6.1: Security functional dependencies

Claim	***Hierarchical to***	***Dependencies***	***Dependency met?***
FAU_GEN.1	-	FPT_STM.1	Dependency exists with A.TSP and OE.TSP.
FAU_GEN.2	-	FAU_GEN.1 FIA_UID.1	Yes.
FAU_SAR.1	-	FAU_GEN.1	Yes.
FDP_ACC.1	-	FDP_ACF.1	Yes.
FDP_ACF.1	-	FDP_ACC.1 FMT_MSA.3	Yes.
FIA_AFL.1	-	FIA_UAU.1	Yes.

Claim	*Hierarchical to*	*Dependencies*	*Dependency met?*
FIA_SOS.1	-	-	Not applicable.
FIA_UID.1	-	-	Not applicable.
FIA_UAU.1	-	FIA_UID.1	Yes.
FMT_MSA.1	-	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Yes
FMT_MSA.3	-	FMT_MSA.1 FMT_SMR.1	Yes.
FMT_SMF.1	-	-	Not applicable.
FMT_SMR.1	-	FIA_UID.1	Yes.
FTA_MCS.1	-	FIA_UID.1	Yes.
FTA_MCS.2	FTA_MCS.1	FIA_UID.1	Yes.
FTA_SSL.3	-	-	Not applicable.
FTA_SSL.4	-	-	Not applicable.
FTP_ITC.1	-	-	Not applicable.
FTP_TRP.1	-	-	Not applicable.
FDP_UCR_EXT.1	-	-	Not applicable.

Table 6.4: Security functional requirements and dependencies

7 TOE Summary Specifications

This section provides the TOE summary specifications, a definition of the security functions claimed to meet the functional requirements.

7.1 Security Audit

TOE generates audit logs for administrative login and logout, changes to TSF data related to configuration changes, starting/stopping services, if datagrams received or delivered or delivered over network interfaces fit customizable patterns and log records defined in Table 7.1. The operating environment provides a valid time stamp, which is used to create these logs. Authorized moderators have access to all recorded logs and can read and view them. The TOE keeps track of the date and time of each auditable event, as well as the subject's identification, the kind of event, and (when appropriate) the event's success or failure.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2 and FAU_SAR.1

Requirement	***Auditable Events***
FAU_GEN.1	None.
FAU_GEN.2	None.
FAU_SAR.1	None.
FDP_ACC.1	None.
FDP_ACF.1	All requests to modify users' secrets, statuses, and configuration data with the origin of the attempt.
FDP_UCR_EXT.1	None.
FIA_AFL.1	Unsuccessful login attempts limit is met. If the unsuccessful login attempts exceed the limit, the user cannot log in for a certain period of time*[configurable amount of period between 1 minute and 12 hours]*. Logs of unsuccessful login attempts that exceed the limit are kept.
FIA_SOS.1	Identification of any changes to the defined quality metrics.
FIA_UID.1	All use of the user identification mechanism, including user identity provided.
FIA_UAU.1	None.
FMT_MSA.1	All modifications of the values of security attributes.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules.
FMT_SMF.1	All management activities of TSF data.
FMT_SMR.1	Modifications to the group of users that are part of a role.

Requirement	***Auditable Events***
FTA_MCS.1	Connection limits as the maximum number of connections per user.
FTA_MCS.2	Limitations on per-user attributes for numerous concurrent sessions
FTA_SSL.3	The termination of a remote session by the session locking mechanism.
FTA_SSL.4	The termination of an interactive session by the user.
FTP_ITC.1	Launching the trusted channel. Termination of the trusted channel. Failure of reliable channel functions.
FTP_TRP.1	Initialization of the reliable path. Termination of the trusted path. Failure of trusted path functions.

Table 7.1 Auditable Events

7.2 Identification and Authentication

The TOE's Identification and Authentication security feature allows the administrator and authorized moderators to limit access for users who have been established and assigned responsibilities. The administrator and authorized moderators can read, delete, modify and create TOE modules and secrets within the scope of the access control SFP. The TOE ensures that an administrator identity is established and verified before access to the TOE is allowed. Prior to allowing access, the TOE requires the administrator or authorized moderators to be identified using a username and password. Passwords are enforced to meet a sufficient amount of complexity. Before successful completion of the security function, administrator or moderators are unable to perform any of the relevant functions. Once identified and authenticated, the users are able to access the functions or resources available to their roles. Information flow on input and output is mediated by the TOE, making sure that accessing the configuration and secrets require administrative authentication. It encounters captcha verification when the number of failed authentication attempts exceeds 15. When a configurable amount of unsuccessful authentication attempts has been met, login functionality is disabled for a configurable amount of time. Without being identified and authorized through the login page, no additional activities are available.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FIA_AFL.1, FIA_SOS.1, FIA_UID.1 and FIA_UAU.1.

7.3 Security Management

The TOE provides mechanisms to govern which users can access with resources or functions. The administrator can setup this functionality effectively using the Security Management function. A moderator is assigned read, write, edit, and view permissions for each page by the administrator. In this context, any moderator can be authorized as an administrator. The administrators can change the defaults, query, modify and delete *subject identities*, *metrics for verification of secrets* and *maximum number of failed login attempts* within the context of the access control SFP that the TOE enforces to provide restrictive default values for the security attributes that are used for users. Administrators are allowed to specify alternative commencing values to override default values when an object or information is created. Besides creating, querying, modifying and deleting the security attributes, auditing configuration is also an available management function in the TOE.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1.

7.4 Protection of the TSF

Passwords belongs to administrator users for secure operation of the TOE are stored in an internal database. The internal database is listening only to unix sockets that are not possible to access out of TOE over the network. The user credentials belongs to the authorized administrators are entered through the Trusted Paths defined in FTP_TRP SFR such as local console, HTTPS GUI. The password is encrypted using Blowfish based crypt when creating administrator account or changing password and then stored to the internal database. The password hashes are not available through any communication channel. The salt of the Blowfish based crypt hashing is generated randomly on hash creation.

TOE Security Functional Requirements Satisfied: FDP_UCR_EXT.1, FTP_TRP.1.

7.5 TOE Access

The TSF has a way for regulating the formation of an administrator's session based on the session being terminated after a configurable time of inactivity, which is set to 10 minutes by default and 1 minute by default. Inactive sessions are logged out and returned to the login page automatically. The TOE also allows the user to end their own interactive session on their own terms. The administrator sets connection limits, such as the maximum number of connections per user and the number of connections per five seconds. When these limitations are exceeded, they are prohibited for the duration of the blocking window that the administrator has specified.

TOE Security Functional Requirements Satisfied: FTA_MCS.1, FTA_MCS.2, FTA_SSL.3 and FTA_SSL.4.

7.6 Trusted Path/Channels

The TOE provides an Inter-TSF trusted path/channel between itself and the following entities. To protect both integrity and privacy, the TOE uses TLS1.2 for GUI access to maintain interactive communication with administrators. The attempted connection will not be created if the negotiation of an encrypted session fails. The TOE uses HTTPS, TLS1.2 connections to encrypt interactions with network peers, such as an external audit server or an identity provider to avoid unintentional log disclosure or manipulation. Furthermore, TOE ends the interactive session after a specific duration of user inactivity, with a default time value of 10 minutes and a minimum value of 1 minute. TOE also allows the user to terminate his or her own interactive session.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_SSL.4 and FTP_ITC.1.