TR7 ASP – Application Security Platform Software

Security Target Lite

Version No: 1.0

VERSION HISTORY

Version No	Reason for Change	Author	Release Date
1.0	ST Lite released	TR7	09.10.2025

GLOSSARY

ASP: This abbreviation refers to Application Security Platform, which is the entirety of the software developed by TR7. It is also the TOE of this document.

GTM: Refers to Global Traffic Management which is a feature of TR7 ASP Software.

Administrator: In this document, Administrator refers to the first user that comes with the TOE. This user has every authorization.

CLI: Refers to Command Line Interface.

Frontend Services: IP addresses or DNS records accessible over the internet whose traffic pass through TR7 ASP Software. These IP addresses/DNS records usually belong to firewalls or other network elements which redirect traffic to TR7 ASP Software before allowing them into the backend servers.

Web GUI: Graphical user interface of the TOE that is accessible over the management ip from a web browser.

Management IP: IP address used to access the TOE over GUI or SSH.

CONTENTS

List of Tables

List of Figures

1. ST Introduction

1.1. Security Target Lite & TOE Reference

ST Title: TR7 ASP Software - Application Security Platform Software Security Target Lite

ST Reference: v1.0

TOE Identification: TR7 Application Security Platform Software

TOE Version: v1.8

1.2. TOE Overview

TR7 Application Security Platform (ASP) Software is a security software which provides load balancing (LB), web application firewall (WAF) services. With such services, the TOE provides comprehensive network traffic management and multilayer security of web applications. TR7 ASP software can be located as a hardware or virtual appliance. However, TR7 ASP software cannot be offered as a Software as a Service (SaaS) appliance on cloud. It is deployed into the infrastructure of the customers and can be used by those customers only.

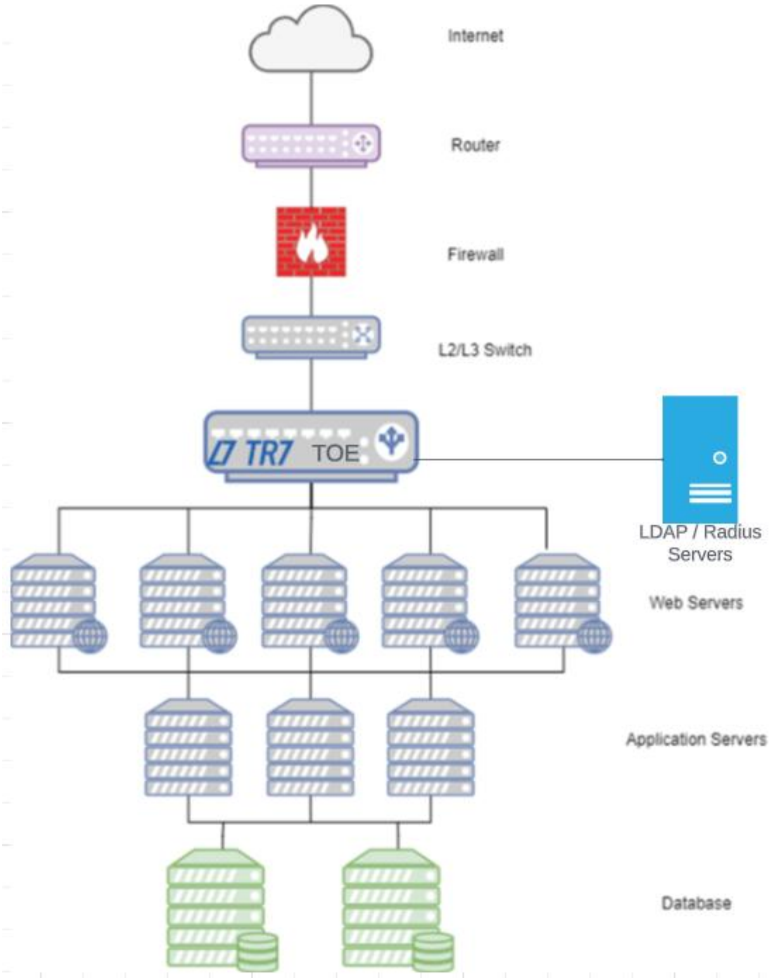

Figure 1. An example network topology where the TOE can be deployed to.

TR7 ASP software functionality is summarized below, detailed information is provided in TR7 ASP Software User Guide:

Load Balancer

- Layer 4 (TCP/UDP) and layer 7 (HTTP) load balancing,
- Network traffic manipulation with conditions and actions,
- Layer 7 caching and compression,
- SSL bridging and offloading,
- SSL certificate management,
- IPv4 and IPv6 support,

- Dashboard for live traffic monitoring and report generation in different formats (PDF, Excel, HTML),
- Application monitoring with health check profiles of TCP, Ping, HTTP, HTTPS, DNS, FTP, FTPS,
- All HTTP requests or specific requests can be redirected to HTTPS,
- Supports layer 2 mode switching and layer 3 mode routing,
- Supports static and dynamic routing protocols,
- One or more web GUI and SSH connections are supported across multiple networks,
- Daily backups,

Web Application Firewall

- Application security against common web application vulnerabilities:
- Learning, Monitor and Block modes with protection levels,
- Rule exceptions for optimized security,
- Virtual host groups for specialized WAF rules,
- Traffic filtering based on HTTP request parameter format (path, query, header, body),
- Whitelist condition and Whitelist/Blacklist IP filtering support,
- Path-based rule support,
- Collective learning support,
- One or more web GUI and SSH connections are supported across multiple networks,
- Daily backups,

1.2.1. Major Security Features of the TOE

The following features are the major security functionality of the TOE;

- **Security Audit:** TOE generates audit logs regarding all user activity: login attempts, login blocks, configuration changes (except LDAP configuration changes), configuration additions, configuration deletions and logouts. Logs can be viewed by administrators, and users can view logs related to their own user groups. Authorized users have right to read all the recorded logs related to their own user groups, whereas unauthorized users do not have access to these functions. Logs cannot be deleted or manipulated. The TOE can perform security violation analysis by monitoring the audited events and detecting access configuration changes. When a violation analysis is detected, the TOE notifies the admins via sending emails regarding the changed acccess configuration.

- **Trusted Path:** Web GUI and SSH access are protected with encrypted traffic, over TLS and SSH respectively.
- **Data Protection:** The access control function permits a user to access a protected resource only if a user ID or role of the user is given permission to perform the requested action on the resource by Administrator. Exported and imported data flow only through configured ports and are controlled by the authenticated user only. Data export can also take place manually via the user. Web interface and CLI access are provided via secure methods by default. The TOE permits the rollback of all operations on all objects committed by all subjects. Rollbacks can take place on a daily basis. This is enabled by taking regular daily backups of the TOE and allowing administrators to manually switch back to a snapshot of the TOE in case of failure or service discontinuity.
- **User Identification and Authentication:** When a user issues a request to the TOE for access to any functionality, the TOE requires that the user identifies and authenticates themselves before performing any action. Unsuccessful login attempts are blocked after an admin configured number of attempts.
- **TOE Access:** TOE imposes rate limiting to requests from every IP based connection. Connections accepted from a single IP is limited to a certain number configured by admins. This enables the TOE to protect itself from massive connection requests. When the session inactivity of users exceeds an administrator defined duration within 0-1440 minutes, the session is terminated and users are returned to the login page. The users are also able to terminate their own sessions by logging out of the TOE. The TOE enforces maximum quotas for IP based new connections that individual users can use over an admin configured time interval.
- **Role Based Access Control:** TOE has predefined user roles with different security attributes that can be associated with users. The TOE maintains the roles users, managers and

administrators. Administrators can generate new users with different roles with desired access rights. The access control function permits a user to access a protected resource only if the role of the user is given permission to perform the requested action on the resource by an Administrator. Administrators can add/delete users, change the roles of the existing users and manipulate the information of the existing users.

1.2.2. TOE TYPE

This TOE falls under the category "Network and Network-Related Devices and Systems". TOE is a load balancer and web application firewall software.

1.2.3. NON TOE HARDWARE/ SOFTWARE/ FIRMWARE

The TOE can operate both as a hardware appliance or as a virtual machine in a virtualization environment. Regardless of its operating environment, the minimum hardware requirements for the TOE are given below.

TR7 ASP Software Hardware Requirements

Hardware	Requirement
Processor	Minimum 4 64-bit Cores with 2 GHz +
RAM	4096 MB +
Disk space	130 GB +

Other Components Used by the TOE (Minimum Versions Supported):

- Debian GNU/Linux 10 (buster)
- Linux Kernel 4
- Docker Engine version 20.10.17
- JSON Database (in-memory)

1.3. TOE Description

1.3.1. TOE Physical Scope

The Physical Scope of the TOE is the blue area in the figure below. The TOE is limited to the software that provides the Load Balancing and Web Application Firewall functionality. The hardware and the operating system that the TOE runs on is excluded in the scope of the TOE. In addition, backend services and other network elements that can communicate with the TOE are also excluded from the scope.

The TOE is delivered to the customer as a single ISO file that contains the virtual image of the TOE. This ISO file delivered to the customer environment by TR7 Support Team. Hence, only delivered part of the TOE includes TR7 Application Secuirty Platform Software in the format ".iso".

"TR7 ASP Software- AGD - User Guide" and "TR7 ASP Software - AGD – Kurulum" documents are presented to the customers when the support team visit the customers face to face.

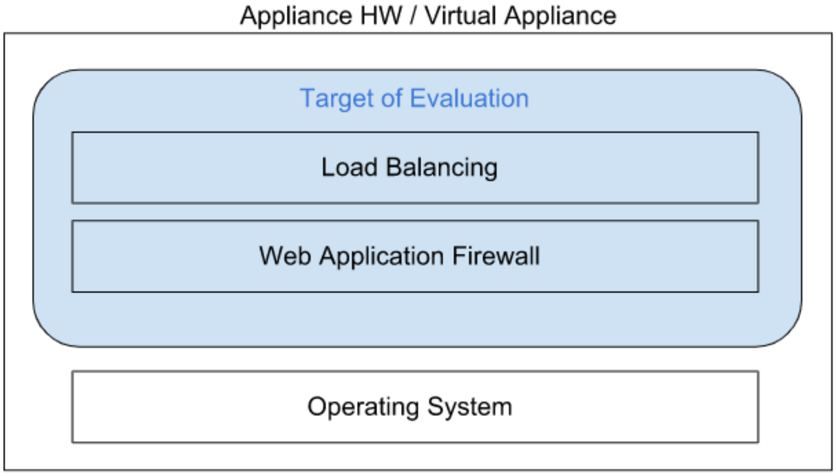

Figure 2. Typical Software/Firmware Environment of TOE

1.3.2. TOE Logical Scope

Security Audit:

The TSF generates audit logs that consist of various auditable events regarding all user activity: login attempts, login blocks, configuration changes (except LDAP configuration changes), configuration additions, configuration deletions and logouts. Authorized administrators have right to read all the recorded logs stated above. Audit logs are protected from unauthorized deletion or modification, and provisions are provided against audit data loss due to storage area excession. Authorized users have right to read all the recorded logs related to their own role group, whereas unauthorized users do not have access to these functions. Admins can view all logs. The TOE can perform security violation analysis by monitoring the audited events and detecting access configuration changes. When a violation analysis is detected, the TOE notifies the admins via sending emails regarding the changed acccess configuration.

User Identification and Authentication:

When a user issues a request to the TOE web interface or CLI, the TOE requires that the user identify and authenticate themselves before performing any action. Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. roles, and authorizations). LDAP and Radius users can be added to the TOE. In this case, The TOE ignores any security attributes associated with the user data when imported from outside the TOE. . Once the user attempts a configured number (by administrators) of unsuccessful authentications, his/her further login attempts are disabled and his/her IP will be blocked for a configured (by administrators) duration.

Data Protection:

The access control function permits a user to access a protected resource only if a user ID or role of the user is given permission to perform the requested action on the resource by Administrator. Exported and imported data flow only through configured ports and are controlled by the authenticated user only. Data export can also take place manually via the user. Web interface and CLI access are provided via secure methods by default. The TOE permits the rollback of all operations on all objects committed by all subjects. Rollbacks can take place on a daily basis. This is enabled by taking regular daily backups of the TOE and allowing administrators to manually switch back to a snapshot of the TOE in case of failure or service discontinuity.

Role Based Access Control:

Predefined roles are maintained and can be assigned to users. The TOE maintains the roles users, managers and administrators. User priviledges are based on subject security attributes, and each user has different priviledges on different objects. Access control SFP is enforced on all objects based on their security attributes which are determined by their associated roles.

Trusted Path:

Users’ sessions are established through trusted path using TLS or SSH for web GUI and remote CLI connections respectively. The TOE provides these communication paths between itself and 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. Users can initiate communication via the trusted path, and are required to use these paths for initial authentication.

The TOE also provides a communication channel between itself and a another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. The TOE permits another trusted IT product to initiate communication via the trusted channel. Trusted channels are initiated for handling connections from the frontend/backend services of the TOE.

TOE Access:

TOE imposes rate limiting to requests from every IP based connection. Connections accepted from a single IP is limited to a certain number configured by admins. This enables the TOE to protect itself from massive connection requests. When the session inactivity of users exceeds an administrator defined duration within 0-1440 minutes, the session is terminated and users are returned to the login page. The users are also able to terminate their own sessions by logging out of the TOE. The TOE enforces maximum quotas for IP based new connections that individual users can use over an admin configured time interval.

2. Conformance Claims

2.1. CC Conformance Claim

This Security Target Lite claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, CCMB-2017-04-001, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5, CCMB-2017-04-002, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5, CCMB-2017-04-003, [3]

referenced hereafter as [CC].

This Security Target Lite claims the following CC conformance:

- part 2 conformant
- part 3 conformant

- evaluation assurance level EAL4+ ALC_FLR.1

2.2. PP Claim

This ST does not claim conformance to any protection profile.

2.3. Package Claim

This PP is conforming to assurance package EAL4 augmented with ALC_FLR.1 defined in CC part 3 (CC Part 3).

3. Security Problem Definition

This part of the ST defines the security problem that is to be addressed by the TOE. It consists of Threat Agents, Threats, Assumptions and Organizational Security Policies.

3.1. Threat Agents

This section lists threat agents that can access and potentially harm the TOE. Threat agents are divided into two groups for clarity. Agents whose name ends with "**Client**", are unauthorized agents who are not authenticated by the TOE, i.e these agents can harm the TOE without being logged in. "**User**" agents are agents who are either successfully authenticated by the TOE or bypassed the authentication mechanisms.

TA.PHYSICAL_CLIENT: Physical clients have access to the TOE console via the VGA or serial port of the device. In virtual environments, such clients have access to the virtualization environment GUI.

TA.INTRANET_CLIENT: Intranet clients are the clients who are in the same local network as the TOE. Such clients have web GUI and SSH access to the TOE.

TA.INTERNET_CLIENT: This threat agent can be anybody in the internet. Even though the TOE is not accessible over the internet unless configured by the admin users, such threat agents can have access to the TOE as a result of misconfiguration.

TA.CONSOLE_USER: Console users are the users who are authenticated through the physical console interface or SSH of the TOE.

TA.MANAGER_USER: These are the TOE users with the "Manager" role who were authenticated in the web GUI. Such users can manage configurations and can manipulate access to the TOE. Admin role and this role are the only roles that can manage access to the TOE.

TA.USER_USER: These are the TOE users with the "User" role who were authenticated in the web GUI. Such users cannot manage configurations, but can view information on the TOE.

3.2. Threats

T.DDOS: This threat refers to denial of service (DoS) or distributed denial of service (DDoS) attacks. Such attacks can disable access to the web GUI and can be executed by TA.INTRANET_CLIENT or TA.INTERNET_CLIENT threat agents.

T.BRUTEFORCE: Bruteforce attacks can be executed against the TOE. As a result of such attacks, non-TOE users can be granted access to the TOE as being authenticated as a TOE user. Can be executed by TA.INTRANET_CLIENT, TA.PHYSICAL_CLIENT or TA.INTERNET_CLIENT.

T.MISCONFIG: After being authenticated as a TOE user, threat agents might change the access configurations of the TOE. TA.MANAGER_USER threat agents can manipulate access configurations. As a result of this threat, access to the TOE can be affected.

T.EAVESDROP: HTTP/HTTPS/SSH traffic between the TOE and clients can be intercepted by threat agents. Data transfer between the TOE and clients may carry sensitive information in plain text depending on the access configurations of the TOE. Login credentials of TOE users can be acquired as a result of sniffing. Can be executed by TA.INTRANET_CLIENT or TA.INTERNET_CLIENT threat agents.

T.PRIVILEDGE_ESCALATION: Malicious TOE users can gain further priviledges determined by their role groups through the exploitation of the TOE's vulnerabilities. Can be executed by TA.CONSOLE_USER or TA.MANAGER_USER threat agents.

T.LOG_DISCLOSURE: Audit logs kept on the TOE can be reached by unauthorized users. A user can see logs he/she should not have access to, or an unauthorized user can reach the audit logs. Can be executed by TA.INTRANET_CLIENT, TA.PHYSICAL_CLIENT, TA.CONSOLE_USER, TA.MANAGER_USER, TA.USER_USER or TA.INTERNET_CLIENT.

T.LOG_STORAGE: Audit log storage of the TOE can get full after a while. This may result in service discontinuity and/or disfunctionalities. This threat can be executed by anyone who can take actions on the TOE GUI: TA.INTRANET_CLIENT, TA.PHYSICAL_CLIENT, TA.MANAGER_USER, TA.CONSOLE_USER, TA.USER_USER or TA.INTERNET_CLIENT.

T.AUTH_BYPASS: Unauthenticated clients of the TOE can bypass the login process via different methods. This can result in unauthenticated clients accessing sensitive data on the TOE. Can be executed by: TA.INTRANET_CLIENT, TA.PHYSICAL_CLIENT or TA.INTERNET_CLIENT.

T.SERVICE_FAULT: This threat relates to the disfunctionalities that can take place after version updates or hardware changes of the TOE initiated by the users of the TOE. This disfunctionalities include service discontinuity, misconfigurtions and disfunctional features of the TOE. This threat can be executed by: TA.MANAGER_USER or TA.CONSOLE_USER.

3.3. Organizational Security Policies

The organizational security policies are described in below.

P.PASSWORD_POLICY: Users of TOE shall use passwords that obey TR7's password policy ,that is defined in FIA_SOS.1 ,in order to ensure the security of TOE.

3.4. Assumptions

The assumptions are described below;

A.NO_GENERAL_PURPOSE It is assumed that there are no general-purpose computing capabilities (e.g.,compilers or user applications) available on the TOE, other than those installed initially during the setup of the TOE.

A.PHYSICAL Physical security is assumed to be provided by the environment such that the device cannot be physically harmed.

A.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

A.TIME_SERVER It is assumed that a trustworthy computing platform is provided for the TOE and that the trusted time server provides reliable time information.**A.BACKUP_SAFETY** It is assumed that the backups of the TOE are stored in a safe environment.

A.LOG_SAFETY It is assumed that the logged audit trail of the TOE is stored in a safe environment, and that enough storage is present to accommodate for the stored logs of the TOE. It is also assumed that the log storage is increased when necessary.

A.STRICT_BRUTEFORCE_CONFIG It is assumed that anti-bruteforce settings "Max. failed login per IP" and "Max. failed login per IP & username" are not intentionally configured above 15 by the admin users to allow bruteforce attacks.

4. Security Objectives

In this section part-wise solutions are given against the security problem defined in Part 3.

4.1. Security Objectives for the TOE

The security objectives for the TOE are described in below;

O.RATE_LIMIT: Connections from any IP:Port pairs are rate limited by a default number.

O.AUTHENTICATION: Username-password based authentication is enforced on all users on all interfaces before they can access the TOE.

O.SECURE_ACCESS: Web interface access is done over HTTPS with secure cipher and TLS 1.2. SSH access is achieved via secure cipher. TOE establishes communication channels between itself and other trusted IT products that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

O.AUTH_BLOCK: After a configured number of failed login attempts, user authentication is blocked.

O.AUDIT : The TOE generates audit logs for all user activity, which can be viewed by the administrators and users with related roles.

O.AUDIT_PROTECTION: The TOE protects its saved audit logs by preventing their unauthorized deletion or modification. Unauthorized access to audit logs are prevented by allowing role groups to view only the logs of their role group. The TOE ignores audited events if the audit trail is full.

O.TOE_RBAC: The TOE allows administrators to create new users and assign them pre-defined roles with specific access rights and authorizations.

O.NOTIFICATIONS: The TOE keeps the logs of access configuration changes, and sends notifications to admins when these configuratios are changed.

O.BACKUPS: The TOE takes regular daily backups which can be used to recover from attacks.

O.KILL_SESSION: Users can terminate their own sessions. Inactive sessions of users are terminated after an administrator defined time.

4.2. Security Objectives for the Operational Environment

OE.PHYSICAL: Physical security is provided by the environment.

OE.TRUSTED_ADMIN: The administrator of the application software is not careless, willingly negligent or malicious.

OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.PLATFORM: The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.BACKUP_SAFETY: The TOE relies upon an environment in which a safe storge of backup files can be ensured.

OE.LOG_SAFETY: The audit trail storage is monitored, and in case there is low space, audit trail storage is increased.

OE.STRICT_BRUTEFORCE_CONFIG Configurations for access do not intentionally allow bruteforce attacks.

4.3. Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Threat, Assumption, or OSP	Security Objectives	Rationale
T.DDOS	**O.RATE_LIMIT**	O.RATE_LIMIT decreases the magnitude of D/DoS attacks as only a limited number of connections are accepted from a single source.
T.BRUTEFORCE	**O.AUTHENTICATION** **O.AUTH_BLOCK**	O.AUTHENTICATION enforces secure username-password based authentication which is difficult to bruteforce. O.AUTH_BLOCK blocks login attempts after a configured number of failed login attempts.
T.MISCONFIG	**O.AUDIT** **O.AUDIT_PROTECTION** **O.TOE_RBAC** **O.NOTIFICATIONS** **O.BACKUPS**	To prevent misconfigurations by threat agents, the TOE offers O.AUDIT, which logs every action taken by users. O.AUDIT_PROTECTION ensures that these logs cannot be deleted by anyone. O.TOE_RBAC allows a role based acces so that if threat agents authenticate as a user, they can only manage configurations of their role. With O.NOTIFICATIONS, the TOE sends immediate notifications via e-mail to inform admins about manipulation of access configurations. Finally, O.BACKUPS automatically take backups of the TOE so

		that quick recovery is possible after a misconfiguration attack.
T.EAVESDROP	**O.SECURE_ACCESS**	O.SECURE_ACCESS allows communication from secure channels established with the client and the TOE. This enables the TOE users to securely communicate sensitive information like login credentials without the risk of man-in-the-middle attacks. For communication with the web GUI, secure cipher and TLS 1.2 is supported. Similarly for SSH, secure cipher is present to prevent eavesdropping attacks.
T.PRIVILEDGE_ESCALATION	**O.TOE_RBAC** **O.KILL_SESSION**	O.TOE_RBAC enforces all users to be created with roles that have predefined priviledges. Users with attached roles other than admins cannot access other resources than the resources allowed for their role group. O.KILL_SESSION prevents priviledge escalation via session hijack.
T.LOG_DISCLOSURE	**O.AUDIT_PROTECTION**	O.AUDIT_PROTECTION prevents log disclosure by preventing the role groups to view the logs of other role groups. Logs are also protected from unauthorized deletion and modification to protect their integrity.
T.LOG_STORAGE	**O.AUDIT_PROTECTION**	O.AUDIT_PROTECTION ignores auditable events when the log storage is full. Hence, any service disfunctionality due to this

		reason is prevented.
T.AUTH_BYPASS	**O.AUTHENTICATION** **O.AUTH_BLOCK** **O.KILL_SESSION**	O.AUTHENTICATION enforces that secure authentication tokens are used by the admins to generate login credentials which are hard to brute force. O.AUTH_BLOCK blocks clients after certain number of unsuccessful login attempts to prevent bypass via brute force or other methods. O.KILL_SESSION prevents the stealing of other users' sessions by third parties to bypass authentication.
T.SERVICE_FAULT	**O.BACKUPS**	O.BACKUPS ensure that if a service fault occurs after a version update or a hardware change, TOE can be brought back to a snapshot to recover to a functional state.
A.NO_GENERAL_PURPOSE	**OE.NO_GENERAL_PURPOSE**	The operational environment objective OE.NO_GENERAL_PURPOSE is realized through A.NO_GENERAL_PURPOSE. Since A.NO_GENERAL_PURPOSE indicates that there are no general purpose computing capabilities on the TOE other than those services necessary for the operation, administration and support of the TOE, the assumption that computing capabilities are limited to the initial setup is guaranteed.
A.PHYSICAL	**OE.PHYSICAL**	The operational environment objective OE. PHYSICAL is realized through A.PHYSICAL because the assumption that the physical hardware hosting the TOE is safe implies

		that the TOE cannot be harmed by any threat agents.
A.TRUSTED_ADMIN	**OE.TRUSTED_ADMIN**	The operational environment objective OE. TRUSTED_ADMIN is realized through A.TRUSTED_ADMIN. The assumption guarantees that the admins follow and apply all administrator guidance in a trusted manner. Hence they cannot willingly harm or neglect the TOE.
A.TIME_SERVER	**OE.PLATFORM**	The operational environment objective OE.PLATFORM is realized through A. TIME_SERVER. As reliable time information is assumed to be provided, the TOE can trust the underlying operating system to execute with accurate timestamps.
A.BACKUP_SAFETY	**OE.BACKUP_SAFETY**	The operational environment objective OE.BACKUP_SAFETY is realized through A.BACKUP_SERVER. As a safe environment is assumed for backups, the TOE can store backups in this provided storage.
A.LOG_SAFETY	**OE.LOG_SAFETY**	The operational environment objective OE.LOG_SAFETY is realized through A.LOG_SERVER. As a safe environment and adequate storage is assumed, TOE can store logs in this storage. When necessary in case of inadequate storage, log storage is increased.
A.STRICT_BRUTEFORCE_CONFIG	**OE.STRICT_BRUTEFORCE_CONFIG**	The operational environment objective **OE.STRICT_BRUTEFORCE_CONFIG** is realized through **A.STRICT_BRUTEFORCE_CONFIG.** As incorrect login limitations are assumed to be maximum 15, bruteforce configurations cannot intentionally allow attacks.

P.PASSWORD_POLICY	**O.AUTHENTICATION**	To allow secure username-password based authentication defined in O.AUTHENTICATION, P.PASSWORD_POLICY ensures that defined passwords meet the complexity requirements.

Table 1. Security Objectives Rationale

5. Extended Components Definition

There is not any extended components definition within this Security Target Lite.

6. Security Requirements

6.1. Security Functional Requirements Formatting

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part1 [17]. The following operations are used in the ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC instating a requirement. Selections having been made are denoted as underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, like the length of a password. Assignments are denoted by *italicized* text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.2. Security Functional Requirements

Requirement Class	Requirement Component
FAU: SECURITY AUDIT	FAU_GEN.1
	FAU_GEN.2
	FAU_SAR.1
	FAU_SAR.2
	FAU_STG.1
	FAU_STG.4
	FAU_SAA.1
	FAU_ARP.1
FDP: USER DATA PROTECTION	FDP_ACC.2
	FDP_ITC.1
	FDP_ROL.2
	FDP_ACF.1
FIA: IDENTIFICATION AND AUTHENTICATION	FIA_AFL.1
	FIA_SOS.1
	FIA_UAU.1
	FIA_UID.1
	FIA_ATD.1
FMT: SECURITY MANAGEMENT	FMT_MTD.1
	FMT_SMF.1
	FMT_SMR.1
FTP: TRUSTED PATH/CHANNELS	FTP_ITC.1
	FTP_TRP.1

FTA: TOE ACCESS	FTA_SSL.3
	FTA_SSL.4
FRU: PRIORITY OF SERVICE	FRU_RSA.1

6.2.1. Class FAU: Security Audit

6.2.1.1.FAU_GEN.1 Audit Data Generation

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) [

- *Success and failure of logins*
- *Log outs*
- *All user action logs (except password updates)*
- *All admin action logs (except LDAP configuration changes)*
- *TOE state changes*

].

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 the event, subject identity, and the outcome (success or failure) of the event.

b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP~~/ST [*user IP, log type, error message, log description*].

6.2.1.2.FAU_GEN.2 User Identity Association

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.

6.2.1.3.FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*administrators and other users groups*] with the capability to read [*respectively; all audit record, audit records of assigned user group*] 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.

6.2.1.4.FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.5.FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

6.2.1.6.FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [ignore audited events] and [*none*] if the audit trail is full.

6.2.1.7.FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*access configuration changes*] known to indicate a potential security violation;

b) [*none*].

6.2.1.8.FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take [*send email notifications to admins*] upon detection of a potential security violation.

6.2.2. Class FDP: User Data Protection

6.2.2.1.FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [*Access Control SFP*] to objects based on the following: [

Subjects:

- *Administrator*
- *Manager*
- *User Group*

Subject Attributes:

- *const CAN_SEE*
- *const CAN_MODIFY*
- *const FULL_AUTH*

Objects:

- *Audit Logs*
- *Device settings*
- *Interface settings*
- *Network settings*
- *Firewall settings*
- *WAF Settings*
- *Load balancer settings*
- *Dashboard*
- *Access Control*
- *Traffic Manipulation*
- *User role settings*

Object Attributes:

const TR7_USER_AREAS = ['zones', 'network', 'lb', 'waf', 'gtm', 'settings', 'users', 'certificate', 'certificatePool']

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*Allowed if the authorized user is admin; allowed else if the user group has the necessary priviledges for the requested operation; not allowed otherwise*].

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 [*none]*.

6.2.2.2.FDP_ACC.2 Complete Access Control

FDP_ACC.2.1 The TSF shall enforce the [*Access Control SFP*] on [

Subjects:

- *Administrator*
- *Manager*
- *User Group*

Objects:

- *Audit Logs*
- *Device settings*
- *Interface settings*
- *Network settings*
- *Firewall settings*
- *WAF Settings*
- *Load balancer settings*
- *Dashboard*
- *Access Control*

- *Traffic Manipulation*
- *User role settings*

] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.2.2.3.FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [*Access Control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*none*].

6.2.2.4.FDP_ROL.2 Advanced Rollback

FDP_ROL.2.1 The TSF shall enforce [*access control SFP*] to permit the rollback of all the operations on the [*all objects*].

FDP_ROL.2.2 The TSF shall permit operations to be rolled back within the [*daily backups*].

6.2.4. Class FIA: Identification and Authentication

6.2.4.1.FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [0-1000]] unsuccessful authentication attempts occur related to [*unsuccessful user login attempts*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block user authentication until it is unblocked after an administrator determined time*].

6.2.4.2.FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*user id, name, password, user role*].

6.2.4.3.FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

- *8-32 characters,*
- *at least 1 number,*
- *at least 1 uppercase letter,*
- *at least 1 lowercase letter,*
- *at least 1 special character.*

].

6.2.4.4.FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [*login*] 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.

6.2.4.5.FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [*login*] 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 succesfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5. CLASS FMT: SECURITY MANAGEMENT

6.2.5.1.FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [modify, delete] the [*users, admin passwords, user passwords, managers, manager passwords*] to [*Administrators*].

6.2.5.2.FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- *changing access control settings*
- *restricting connection of certain IP's*

].

6.2.5.3.FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*users, managers and administrators*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6. Class FTA: ToE Access

6.2.6.1.FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an inactive session after a [*10 minutes*] **by default, which can then be configured by admins to a duration of 1 to 1440 minutes**.

6.2.6.2.FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.7. Class FTP: Trusted Paths

6.2.7.1.FTP_TRP.1 Trusted Path

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].

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].

6.2.7.2.FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [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 [*handling connections from frontend/backend services of the TOE*].

6.2.8. Class FRU: Priority of service

6.2.8.1.FRU_RSA.1 Maximum Quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [*IP based new connections*] that [individual user] can use [over a specified period of time].

6.3. Security Assurance Requirements

Assurance Class	Assurance Component
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: Life-cycle Support	ALC_CMC.4 – Production support, acceptance procedures automation
	ALC_CMS.4– Problem tracking CM coverage

	ALC_DEL.1 – Delivery procedures
	ALC_DVS.1 – Identification of security measures
	ALC_LCD.1 – Developer defined life-cycle model
	ALC_TAT.1 – Well defined development tools
	ALC_FLR.1 – Flaw Remediation
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: Test	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 2. Security Assurance Requirements

6.4. Security Requirements Rationale

6.4.1. Security Functional Requirements Dependency Rationale

SFR	Dependency	Hierarchical To	Dependency Met?
FAU_GEN.1	FPT_STM.1 Reliable time stamps	No other components.	NO
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	No other components.	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1 Audit data generation	No other components	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1 Audit review	No other components	FAU_SAR.1
FAU_STG.1	FAU_GEN.1 Audit data generation	No other components	FAU_GEN.1
FAU_STG.4	FAU_STG.1 Protected audit trail storage	FAU_STG.3 Action in case of possible audit data loss	FAU_STG.1
FAU_SAA.1	FAU_GEN.1 Audit data generation	No other components.	FAU_GEN.1
FAU_ARP.1	FAU_SAA.1 Potential violation analysis	No other components.	FAU_SAA.1
FIA_AFL.1	FIA_UAU.1 Timing of authentication	No other components.	FIA_UAU.1
FIA_SOS.1	-	No other components.	-
FIA_UAU.1	FIA_UID.1 Timing of identification	No other components.	FIA_UID.1
FIA_UID.1	-	No other components.	-

FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	No other components.	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	-	No other components.	-
FMT_SMR.1	FIA_UID.1 Timing of identification	No other components.	FIA_UID.1
FTP_ITC.1	-	No other components.	-
FTP_TRP.1	-	No other components.	-
FTA_SSL.3	-	No other components.	-
FTA_SSL.4	-	No other components.	-
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	FDP_ACF.1
FDP_ACF.1	FDC_ACC.1 Complete Access Control FMT_MSA.3 Static attribute initialisation	No other components.	NO
FIA_ATD.1	-	No other components.	-
FDP_ROL.2	FDP_ACC.2 Complete Access Control	FDP_ROL.1 Basic rollback	NO
FRU_RSA.1	-	No other components.	-

Table 3. Security Functional Requirements Dependency Rationale

Unmet Dependency Rationale:

FAU_GEN.1: FPT_STM.1 dependency is not required as time zone is selected during initial configuration by the user. It is assumed that the trusted time server provides reliable time information.

FDP_ACF.1: The SFR FDP_ACC.1 is not necessary as FDC_ACC.2 is already present which is hierarchical to FDP_ACC.1. FMT_MSA.3 is not applicable to the TOE as default security attributes cannot be overriden.

FDP_ROL.2: The SFR FDC_ACC.1 is not necessary as FDC_ACC.2 is already present which is hierarchical to FDP_ACC.1.

6.4.2. Security Functional Requirements Rationale

Objectives	SFRs	Rationale
O.RATE_LIMIT	FRU_RSA.1	During authentication process, FRU_RSA.1 enforces maximum quotas for the IP based new connections that individual users can have over a specified period of time configured by admins.
O.AUTHENTICATION	FIA_UAU.1 FIA_UID.1 FIA_ATD.1 FIA_SOS.1 FDP_ITC.1	Before performing any action, FIA_UAU.1 forces TOE users to authenticate as well as identify provided by FIA_UID.1 before they perform any action on the TOE. FIA_ATD.1 provides maintaining of the following security attributes user id, name, password, user role. FIA_SOS.1 enforces that the generation of authentication tokens are generated based on a policy, which makes it harder for third parties to gain unauthorized access to the TOE. FDP_ITC.1 allows users from LDAP/Radius servers to be imported to the TOE without their security attributes. These users can authenticate themselves after an admin user adds them as a TOE user and appoints their security attributes.

O.SECURE_ACCESS	FTP_TRP.1 FTP_ITC.1	FTP_TRP.1 helps to establish a secure channel from the remote users to the TOE and enforces the use of this path, hence blocking third parties from eavesdropping the communication. FTP_ITC.1 allows another IT products to establish a secure connection to the TOE for access and ensures the integrity of this data.
O.AUTH_BLOCK	FIA_AFL.1	FIA_AFL.1 protects the TOE against brute-force attacks by introducing a protection mechanism that blocks login attempts after the client makes an administrator configured number of unsuccesful attempts between 0-1000.
O.AUDIT	FAU_GEN.1, FAU_GEN.2 FAU_SAR.1, FAU_SAR.2	Auditing requirements of the TOE are defined by FAU_GEN.1 and generated audit records are associated with users of TOE by FAU_GEN.2. FAU_SAR.1 provides the users of the TOE with a human-readable interface to the audit records while FAU_SAR.2 prohibits unauthorized users to review audit logs, only administrators are able to see all audit logs.
O.TOE_RBAC	FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 FDP_ACC.2 FDP_ACF.1	FMT_MTD.1 allows authorized users to manage TSF data within the specified rules, and allows only admins to manipulate user credentials. FMT_SMF.1 and FMT_SMR.1 determines the management functions and roles. FMT_SMR.1 associates users with role groups

		that include authorizations. FDP_ACC.2 enforces access control SFP on all user groups and admins before they can perform any operation covered by the SFP on the TOE, and checks if the role group of the user has the proper authorizations to perform such operation. The TSF ensures that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP. After authentication, FDP_ACF.1 determines the authorizations of the user and grants only the allowed operations based on the security attributes of the user.
O.NOTIFICATIONS	FAU_SAA.1 FAU_ARP.1	FAU_SAA.1 determines a set of rules in monitoring the audited events and based upon these rules indicates a potential violation of the enforcement of the SFRs. FAU_ARP.1 sends email notifications to admins upon detection of a change in access configurations.
O.BACKUPS	FDP_ROL.2	FDP_ROL.2 allows the recovery of the TSF functionality manually by using regularly taken backups of the TOE.
O.KILL_SESSION	FTA_SSL.3 FTA_SSL.4	FTA_SSL.3 ensures that the TSF terminates inactive sessions of the users after an administrator defined time has passed. FTA_SSL.4 allows each user to terminate their

		own session.
O.AUDIT_PROTECTION	FAU_STG.1 FAU_STG.4	FAU_STG.1 ensures that the TSF shall protect the stored audit records in the audit trail from unauthorized deletion or modification. FAU_STG.4 ignores the audited events when the audit log storage is full.

Table 4. Security Functional Requirements Rationale

6.4.3. Security Assurance Requirements Rationale

EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. 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. In addition, ALC_FLR.1 is chosen to provide additional quality assurance to the TOE.

7. TOE Summary Specification

7.1. TOE Security Functions

7.1.1. Security Audit

TOE generates audit logs in order to provide accountability for the administrators and system users. Administrators and related user groups have the capability to review the audit logs.

Audit data includes date, source, username, user IP, text and tags. When a log is created after a user's action, that log is associated with that user. All audit logs can be viewed by administrators. Users can view the logs of their own actions as well as the users who are hierarchically below them as a role. For example, a "WAF Manager" user can view the logs of the users who have the role "WAF User".

The TOE generates audit logs for the following events:

- Success and failure of logins

- Log outs
- All user action logs (except password updates)
- All admin action logs (except LDAP configuration changes)
- TOE state changes

All user and admin actions (except LDAP configuration changes) can be configuration changes, additions or deletions.

Authorized users have right to read all the recorded logs for their user groups, whereas unauthorized users do not have access to these functions. Logs are protected from unauthorized deletion or manipulation.

The TOE can perform security violation analysis by monitoring the audited events and detecting access configuration changes. When a violation analysis is detected, the TOE notifies the admins via sending emails regarding the changed acccess configuration.

Implemented SFR's: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FAU_SAA.1, FAU_ARP.1.

7.1.2. User Identification and Authentication

When a user issues a request to the TOE for access to any functionality, the TOE requires that the user identifies and authenticates themselves before performing any action. Users' passwords are controlled according to the following password quality requirements:

every password should have;

- 8-32 characters,
- at least 1 number
- at least 1 uppercase letter,
- at least 1 lowercase letter,
- at least 1 special character.

Once the user attempts a configured number of unsuccessful authentication attempts between 0-1000, his/her login access is disabled for a configured duration. The TSF maintains the following security attributes belonging to individual users: user id, name, password, user role.

The TOE terminates inactive sessions after an administrator defined time interval, and allows users to terminate their own sessions by logging out of the TOE.

Implemented SFR's: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FTA_SSL.3, FTA_SSL.4

7.1.3. Role Based Access Control

The access control function permits a user to access a protected resource only if the role of the user is given permission to perform the requested action on the resource by an Administrator. Administrators can add/delete users, change the roles of the existing users and manipulate the information of the existing users. The TOE allows administrators to associate users with predefined roles and enable the creation of new users with different roles. New roles cannot be created.

The TSF enforces access control SFP on the users, managers and administrators. Audit logs, device settings, interface settings, network settings, firewall settings, WAF settings, load balancer settings, dashboard, access control settings, traffic manipulation configurations and user role settings are the protected objects from all operations covered by the access control SFP.

The TSF allows to associate users with roles in three main categories: Users, managers and administrators. All user roles are subject to Access Control SFP and are listed below:

- Admin
- User
    - Read-only User
    - Monitor User
    - Network User
    - Traffic User
    - WAF User
    - Traffic + WAF User
- Manager

  - Network Manager
  - Traffic Manager
  - WAF Manager
  - Traffic + WAF Manager
  - Certificate Manager

The TSF restricts the ability to modify and delete the users, managers, manager passwords, admin passwords, user passwords to administrators only. Following actions are permitted as the management functions of the TOE:

- changing access control settings
- restricting connection of certain IP's

Implemented SFR's: FDP_ACC.2, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

7.1.4. TOE Access

The TOE web interface can be susceptible to DoS or DDoS attacks. To prevent these attacks, TOE enforces that the IP based connections accepted from an individual user over a specified period of time is limited to a specific number configured by admins. This does not prevent the attack surface altogether, but significantly reduces the magnitude of the attacks.

Implemented SFR's: FRU_RSA.1

7.1.5. Data Protection

The TSF enforces access control SFP on users, managers and administrators. Audit logs, device settings, interface settings, network settings, firewall settings, WAF settings, load balancer settings, dashboard, access control settings, traffic manipulation configurations and user role settings are the protected objects from query, insert, update, delete, import and export operations by the TSF.

The TSF enforces the Access Control SFP when importing user data without security attributes, controlled under the SFP, from outside of the TOE. The TSF ignores any security attributes associated with the user data when imported from outside the TOE.

All operations on all objects can be rolled back on the basis of daily backups. Regular backups of the TOE are taken automatically every day. If an unrecoverable attack or a misconfiguration takes place, the TOE can be restored back to its snapshot manually.

Implemented SFR’s: FDP_ROL.2, FDP_ACC.2, FDP_ITC.1

7.1.6. Trusted Paths

The TSF provides a communication path/channel between itself and remote users that is logically distinct from other communication paths/channels and provides assured identification of its end points and protection of the communicated data from modification. The TSF permits remote users to initiate communication via the trusted path and requires the use of it for initial user authentication. TSF initiates communication via the trusted channel for handling connections from frontend/backend services of the TOE.

Implemented SFR’s: FTP_ITC.1, FTP_TRP.1