Web Application Firewall

Valari Security Target

Document Version: 0.5
Document Date: 25-Sep-17

Company
Kaapagam Technologies Sdn. Bhd. (1015448-T)
A-5-10 Empire Tower SS16/1, Subang Jaya 47500,
Selangor, Malaysia.
Tel : +603 5021 8290 Fax : +603 5021 8291
Email : sales@kaapagamtech.com
Website: http://www.kaapagamtech.com

Prepared by:

Document Revision History

Version	Date	Description	Author
0.1	06 Feb 2017	Initial release	
0.2	19 May 2017	Updates based on EOR001	
0.3	17 July 2017	Updates based on CAR-001	
0.4	22 Aug 2017	1. Remove FPT_STM.2 2. Update FAU_GEN.3 and relevant sections	
0.5	25 Sep 2017	Update Section 7.2.2, 8.2 and 8.4	

Table of Contents

1 Document Overview

This document is the Security Target (ST) for the Valari Web Application Firewall. The ST is designed to meet the requirements of the CC ASE evaluation, and provides a baseline for the subsequent phases of Target of Evaluation (TOE) evaluation works.

2 Security Target Introduction

2.1 Security Target Reference

Security Target Title : Valari Security Target

Security Target Version : 0.5

Security Target Date : 25-Sep-17

2.2 TOE Reference

TOE Name : Valari Web Application Firewall

Software Version : 10.3.11

TOE Initial : VALARI

2.3 Terminology and Acronyms

CC	Common Criteria
Command Injection	A technique that execute arbitrary commands on host OS via vulnerable web application
Cross-site scripting	A technique that enables attacker to inject client side scripting into webpage to bypass access control
EAL	Evaluation Assurance Level
Event	Actions executed by user or TOE itself
HTTP Protocol violation	A request that is violates the standards http protocols
HTTP request	An HTTP client sends an HTTP request to a server in the form of a request message
HTTP response	After receiving and interpreting a request message, a server responds with an HTTP response message
IP	Internet Protocol
KTSB	Kaapagam Technologies Sdn. Bhd.
NTP	Network Time Protocol

OSP	Organizational Security Policy
PP	Protection Profile
Presumed address of destination subject	IP address of the destination subject
Presumed address of source subject	IP address of the source subject
Presumed port of destination subject	Port number of the destination subject
Presumed signature	A unique string that represents a information to identify specific information
Remote File Inclusion Attack	An attack technique used to exploit "dynamic file include" mechanisms in web applications
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
Source IP	IP address of the client connecting to the server
SQL injection	Code injection technic normally used in to attack data-driven application
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
Username	An identification used by a person with access to a computer, network, or online service.
Vulnerability Scanning	An inspection of any potentials points of exploit

2.4 Reference

CCPart1 Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 4, September 2012, CCMB

CCPart2 Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB

CCPart3	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB
CEM	Common Methodology for Information Technology Security Evaluation (CEM): Version 3.1 Revision 4, September 2012, CCMB

2.5 TOE Overview

2.5.1 Usage and major security features of the TOE

VALARI is a Web Application Firewall & Security Management System designed to secure web applications from attacks and provide a layer of security by proxy-ing all HTTP(S) traffic and shield web servers and databases from direct access of the attackers irrespective of the underlying application vulnerabilities.

VALARI has the following functionalities as following:

a) **Detect and block vulnerabilities and Web application threats**: HTTP Distributed Denial of Service (DDoS), HTTP Flooding and Slow HTTP DoS Attacks, Brute Force Login, OS Command Injection, Parameter / Form Field Tampering, Data Disclosure, Phishing Attacks, SQL Injection, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS), Drive-by-Downloads, Directory Traversal, Buffer Overflow, Cookie Injection, Cookie Poisoning, Site Reconnaissance, Data Destruction, Remote File Inclusion Attacks, Google Hacking, Anonymous Proxy Vulnerabilities, HTTP Response Splitting, HTTP Verb Tampering, HTTP Parameter Pollution Attack, Malicious Encoding, Malicious Robots, Known Worms, Web Services (XML) attacks, Session Hijacking, Site Scraping, Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI), Web server software and operating system attacks, Zero Day Web Worms, Forceful Browsing of Website Content, Automated Botnet Attacks and Manipulation of Query String Parameters.

b) **Full Web Traffic Logging** : contents in the web Request bodies are not logged by the web servers and hence attackers use POST requests to delivery exploits and it goes completely blind on the web server logs. With full HTTP transaction logging in VALARI, it is possible to log all requests and responses. This Logging feature can be controlled on what and when a log is created. VALARI can be configured to mask the sensitive data in the request and/or response fields before they are written to the audit log.

c) **Web Intrusion Detection with Just-In Time Monitoring and Detection** : Web Traffics are monitored real time to detect attacks and react on suspicious events / data that hit your web applications.

d) **Built-in Anti-evasion and Encoding validation mechanisms**. : To normalize inputs so as to prevent anti-evasion techniques (eg HexCoding, urlEncode, Nulls) that hackers typically use to get around web security defences.

e) **Protected protocols:** HTTP, HTTPS (SSL), XML, Web services, SOAP and AJAX. Basically anything that you use anticipate an enduser to use a browser for connecting to your web servers and more.

f) **Attack Prevention and External Patching / Virtual Patching** : VALARI acts immediately to prevent attacks from reaching the web applications. With more than 20,000 specific rules, VALARI is an ideal external patching tool. External patching (referred to as Virtual Patching) is about reducing the window of opportunity as the time needed to fix / patch application vulnerabilities often take weeks to months. With VALARI, application vulnerabilities can be patched from the WAF Layer without patching the application source code making your applications secure until a proper patch is applied to the application by your development team or vendors.

g) **Flexible Rule Engine** : The Heart of VALARI is made up of our flexible rule engine with more than 20,000 specific rules covering all sorts of application vulnerabilities, signature patterns and evasion patterns. Our Rule engine is implemented with hardening, protocol validation and detection of web application security issues and is kept updated on regular basis as and when vulnerabilities and attack vectors evolve.

h) **Geo-location Blocking** : VALARI allows Geo-location blocking to block request originated from specific countries

i) **Integrated Security Rules** from various public vulnerability data signature sources and VALARI correlates data from all these numerous sources to generate the Flexible – Scalable – Reliable rules, automatically updating daily and as needed. Various vulnerability data signature sources include :

   a. Kaapagam Tech Rule Set
   b. Public vulnerability data such as the Open Source Vulnerability Database (OSVDB)
   c. Honeypot systems

Not part of the scope of evaluation:

- The key generation, distribution and operation
- VALARI configurations modification
- All hardware appliance and operating system
- Administrator role by KSTB service personnel

The major security features of the TOE included in the evaluation are Identification and Authentication, User Data Protection, Security Audit and Security Management.

2.5.2 TOE Type

The TOE is a web application firewall.

2.5.3 Non-TOE hardware/software/firmware required by the TOE

The TOE comes with a hardware appliance and operating system that is required to run the TOE as following:

Table 1: Non-TOE Hardware and Software Specification

Specification	Details
CPU Speed	Base Model: Intel Quadcore Xeon (4 cores) with no redundant PSU Datacentre Model: Octa core Xeon (8 cores) with dual redundant PSU
Interface	4x Intel Gigabit interfaces with iKVM management capability
Form Factor	1U
Operating System	VALARI OS

2.6 TOE Description

2.6.1 Physical Scope of TOE

The TOE consists of the following components:

- Hardware appliance includes the physical port connections. Refer Table 1 for more details. Refer Figure 1 and Figure 2 for the physical presentation of hardware appliance.
- VALARI OS
- VALARI User Guide

Figure 1: VALARI hardware appliance

All hardware appliance and operating system are not part of the scope of evaluation.

The TOE must be placed in a secure physical area where only authorized users are granted physical access to the TOE.

TOE user could view configurations and logs TOE through the command-line interface by using SSH client (Win32 – putty, Unix – built-in). VALARI does not use SSH password but using PKI with mandatory SSH key.

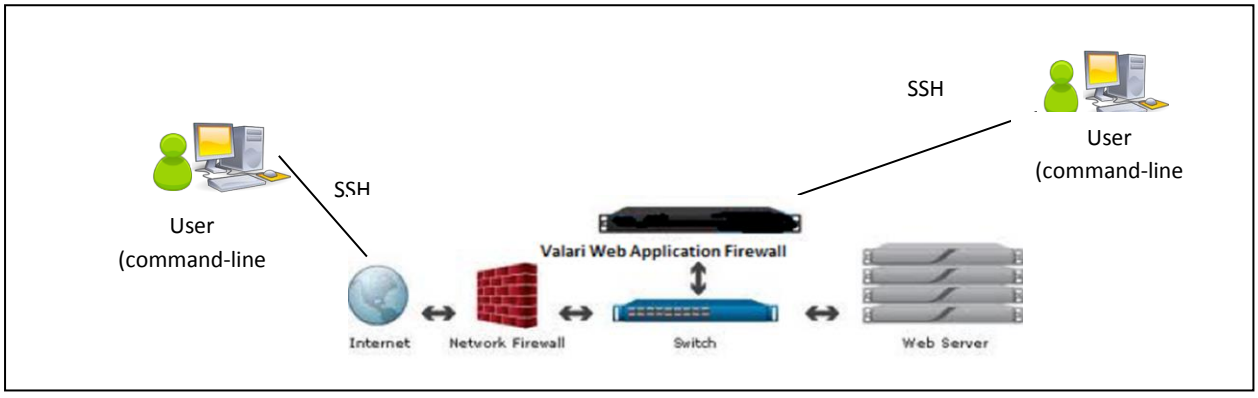

Figure 2: Typical TOE deployment

2.6.2 Logical Scope of TOE

The logical scope of TOE is described based on several security functional requirements.

2.6.2.1 Identification and Authentication

TOE user can access TOE by providing username and public key in the command-line interface. KTSB will create a user account for the given user using their public key for authentication.

2.6.2.2 User Data Protection

TOE protects the web application from external network intrusions by using information flow control between internal and external network. The TOE will log all HTTP requests and responses before allowing or rejecting the HTTP requests. KTSB service personnel could configure HTTP filter rules and policies based on the subject and information security attributes. By default, all external (Internet) traffic will be blocked. KTSB service personnel can configure rules for application vulnerabilities, signature patterns, evasion patterns and Geo-location blocking. However, the modification or changes to rules are not part of the scope of evaluation.

2.6.2.3 Security Management

TOE functions can be managed through command-line interface. The TOE only allows limited user access to run a limited set of commands. These do not affect the running mode of the TOE. User can view settings and logs but cannot modify configuration. Only KTSB service personnel are able to modify configurations upon request (eg whitelisting/blacklisting). However, the modification or changes to rules are not part of the scope of evaluation. KTSB service personnel role is not part of the scope.

2.6.2.4 Security Audit

The TOE will generate audit records for HTTP Request and responses. Each audited events will be recorded along with date and time of event, source IP, account user who performed the event, event name, system filename related to event and other event details. Audit records can be viewed by user and cannot be edited. Users are not able to delete or otherwise modify said audit log. User could select for viewing. Full audit reports are emailed every night to the designated email address together with an executive summary. TOE will create a new log file to store the audit records if the size limit is reached for a log file. The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. TOE prevents modification of date and time manually. The user has not ability to change date/time/time-zone. All these are set by KTSB service personnel, and the TOE is continuously clock-synchronized with a pool of NTP servers. However, the setting of date/time/time-zone by KTSB personnel are not part of the scope of evaluation.

3 Conformance Claims

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

CCv3.1 conformant	The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 4.
Part 2 conformant	The ST is Common Criteria Part 2 extended
Part 3 conformant	The ST is Common Criteria Part 3 conformant
Package conformant	The ST is package conformant to the package Evaluation Assurance Level EAL2.
Protection Profile conformance	None

4 TOE Security Problem Definition

4.1 Assumption

The assumptions are to ensure the security of the TOE and its deployed environment.

Table 2: Assumptions

A.PHY	The TOE and its environment are physically secure.
A.FLOW	HTTP traffic cannot flow through internal and external networks unless it passes through the TOE.
A.CONFIGRULE	TOE environment and TOE configurations and rules are pre-configured securely.
A.KEY	User's public and private keys are generated, distributed and used securely for SSH client.
A.TIME	The TOE environment will provide reliable time stamps.
A.CONN	The TOE environment will provide a secure connection between TOE and users.
A.ADMIN	The TOE Administrator (KTSB Service personnel) will be non-hostile and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.

4.2 Threats

Assets that are protected by the TOE are sensitive data stored in the TOE and internal network including critical TOE configuration data (configuration files and others), audit records, admin credentials, TOE data and TOE security functions.

Threat agents are entities that can adversely act on the assets. The threat agents identified are an unauthorized person.

Threats may be addressed either by the TOE or by its intended environment.

Table 3: Threats

T.ACCESSLOG	An unauthorized person successfully accesses the TOE data or security functions without being detected.
T.AUDIT	An unauthorized person may intentionally or unintentionally delete audit records to destroy evidence of adverse events executed.
T.EXPLOIT	An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.
T.REMOTE	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator (KTSB Service personnel) or user and the TOE.
T.CONFIG	An unauthorized person may read and modify security TOE functions and configuration data.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to assess and use security functions and/or non-security functions provided by the TOE.

4.3 Organizational Security Policies

The Organizational Security Policies (OSP) is imposed by an organization to secure the TOE and its environment.

Table 4: Organizational Security Policy

P.ROLE	Only authorized persons assigned by the organization have access to the TOE.
P.PASSPHRASE	Authorized user shall use complex passphrase to generate private and public key.

5 Security Objectives

Security objectives are formed to address the security problem definition defined in earlier section. The security implementation in TOE and its environment will meet these objectives.

5.1 Security Objectives for the TOE

The security objectives for the TOE as following:

Table 5: Security Objectives for the TOE

O.ACCESSLOG	TOE shall record a readable log of security events.
O.AUDIT	TOE shall prevent an unauthorized person to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.EXPLOIT	TOE shall mediate the information flow in internal network and between internal and external network.
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data.
O.NOAUTH	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.

5.2 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

Table 6: Security Objectives for the Operational Environment

OE.PHY	The TOE and its environment shall be physically secure.
OE.FLOW	The TOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.
OE.CONFIGRULE	The TOE environment and TOE configurations and rules shall be pre-configured securely.
OE.KEY	The TOE environment and user shall generate, distribute and use user's public and private keys securely for SSH client.
OE.TIMEBACK	The TOE environment shall provide reliable time stamps.
OE.CONN	Authorized user shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.
OE.ADMIN	The TOE Administrator (KTSB Service personnel) is non-hostile and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.

6 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE. These requirements are presented following the conventions identified in Section 7.1 Conventions.

6.1 Extended Security Functional Requirement (SFR)

Table 7: Extended SFR Component

Extended Component	Extended Component Name	Rationale
Class FAU : Security Audit		
FAU_GEN.3	Simplified Audit Data Generation	FAU class contains families of functional requirements that are related to monitor security-relevant events, and act as a deterrent against security violations. This component is a member of FAU_GEN, an existing CC Part 2 family. This extended requirement for the FAU class has been included in this ST because TSF audit function does not log start and stop of auditing function; hence FAU_GEN.1.1 (a) is not applicable. This component is also created to simplify the requirement of FAU_GEN.1.
Class FMT: Security Management		
FMT_MSA.5	Static attribute initialisation without overriding default values	FMT class contains families of functional requirements that relate to management of several aspects of the TSF: security attributes, TSF data and functions. The different management roles and their interaction, such as separation of capability, can be specified. This component is a member of FMT_MSA, an existing CC Part 2 family. This extended requirement for the FMT class has been included in in this ST because the authorized user for the TOE is not able to specify alternative initial values to override the default values when an object or information is created. The user only able to view configurations and logs in TOE. This component is used to replace FMT_MSA.3.

6.1.1 Class FAU: Security Audit

Family Behaviour: Same with FAU_GEN

Component levelling: Same with FAU_GEN

Management: FAU_GEN.3

There are no management activities foreseen

Audit: FAU_GEN.3

There are no auditable events foreseen

FAU_GEN.3 Simplified Audit Data Generation

Hierarchical	No other components
Dependencies	FPT_STM.1 Reliable time stamps
FAU_GEN.3.1	The TSF shall be able to generate an audit record of the following auditable events: [**assignment: defined auditable events**].
FAU_GEN.3.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event b) [**assignment: other information about the event**].

6.1.2 Class FMT: Security Management

Family Behaviour: Same with FMT_MSA

Component levelling: Same with FMT_MSA

Management: FMT_MSA.5

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

a) managing the group of roles that can specify initial values;

b) managing the permissive or restrictive setting of default values for a given access

control SFP;

a) management of rules by which security attributes inherit specified values.

Audit: FMT_MSA.5

There are no auditable events foreseen

FMT_MSA.5 Static attribute initialisation without overriding default values

Hierarchical	No other componentss
Dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.5.1	The TSF shall enforce the [**assignment: access control SFP, information flow control SFP**] to provide [***selection, choose one of: restrictive, permissive***, [**assignment: other property**]] default values for security attributes that are used to enforce the SFP.

6.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

7 TOE Security Requirements

This section provides the security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

7.1 Conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to the statement of security functional requirements. Following are the operations and the document conventions as used within this ST to depict their application:

Assignment	The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].
Selection	The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].
Refinement	The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
Iteration	The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing an acronym at the end of the component identifier as follows: FCS_COP.1(SWP).

7.2 Security Functional Requirements

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Table 8: Security Functional Requirements

Component	Component Name
Class FAU : Security Audit	
FAU_GEN.3	Simplified Audit Data Generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
Class FDP : User Data Protection	
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
Class FIA : Identification and Authentication	
FIA_ATD.1	User attributes definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FMT : Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MSA.1	Management of security attributes
FMT_MSA.5	Static attribute initialisation without overriding default values

7.2.1 Class FAU: Security Audit

7.2.1.1 FAU_GEN.3 Simplified Audit Data Generation

Hierarchical No other components

Dependencies FPT_STM.1 Reliable time stamps

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events: [

a) **HTTP Request and responses].**

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:

a)Date and time of the event

b)[**Source IP**

c) Account user who performed the event

d) Event name

e) System Filename

f) Event details].

Application The TOE does not have a feature to generate time stamps independently. The date

notes	and time stamp is provided by the environment, which is NTP server.

7.2.1.2 FAU_SAR.1 Audit review

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [**user**] 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.
Application notes	All audit logs are emailed nightly to the pre-configured email address which is typically the user's email address

7.2.1.3 FAU_SAR.3 Selectable audit review

Hierarchical	No other components
Dependencies	FAU_SAR.1 Audit review
FAU_SAR.3.1	The TSF shall provide the ability to apply [**select log file and/or filter**] of audit data based on [**log file related to event**].
Application notes	None

7.2.1.4 FAU_STG.1 Protected audit trail storage

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.
Application notes	None

7.2.2 Class FDP: User Data Protection

7.2.2.1 FDP_IFC.1 Subset Information Flow Control

Hierarchical	No other components
Dependencies	FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] on [

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another;

c) operation: allow/reject information].

Application notes None

7.2.2.2 FDP_IFF.1 Simple Security Attributes

Hierarchical No other components

Dependencies FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] based on the following types of subject and information security attributes: [

a) subject security attributes:
- **Presumed signature**

b) information security attributes:
- **Presumed address of source subject (whitelist/blacklist);**
- **Presumed address of source subject for geoblocked**
- **Presumed address of destination subject;**
- **Presumed port of destination subject;**]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a**) Subject on an internal network can cause information to flow through the TOE to another connected network if:**

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created based on cyber-attack below:**
  - **web application attack**

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- **all the information security attribute values are unambiguously permitted by the information flow security**

policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created based on cyber-attack below:
- **web application attack**
]

FDP_IFF.1.3 The TSF shall enforce the [**none**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [

- **Reject requests for access or services where the information arrives on an internal or external TOE interface, and the presumed signature is defined in on cyber-attack below:**
- **web application attack**
]

Application notes Destination is the webserver which has static IP address and port which is pre-configured.

7.2.3 Class FIA: Identification and Authentication

7.2.3.1 FIA_ATD.1 Subset Information Flow Control

Hierarchical No other components

Dependencies No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) Username
b) PKI Key].

Application notes None

7.2.3.2 FIA_UAU.2 User authentication before any action

Hierarchical FIA_UAU.1 Timing of authentication

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application notes None

7.2.3.3 FIA_UID.2 User identification before any action

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

7.2.4 Class FMT: Security Management

7.2.4.1 FMT_MOF.1 Management of security functions behavior

Hierarchical	No other components
Dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to [***determine the behaviour of***] the functions [**a) uptime : shows how long the unit has been powered up since last reboot/shutdown. Also shows load average over 1 minute, 5 minutes and 15 minutes. For minute by minute load, the first load avg is relevant. For longer term load, the 15 minute average is more useful.** **b) show-array: shows the status of the ZFS flash mirrored array** **c) show-network: shows network capture over the active WAN interface** **d) show-realtime: show a continuously rolling capture of realtime attacks** **e) show-realtimeall: show a continuously rolling capture of realtime WAF messages** **f) show-sqli: show all sql injection attacks in pagination mode** **g) show-rfi: show all remote file inclusion attacks in pagination mode** **h) show-xss: show all cross-site scripting attacks in pagination mode** **i) find-string: displays blocks by string or FQDN**] to [**user**].
Application Note	None

7.2.4.2 FMT_MTD.1 Management of TSF data

Hierarchical	No other components
Dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [***query,*** [**view**]] the [**logs**] to [**user**].
Application Note	None

7.2.4.3 FMT_SMF.1 Specification of Management Functions

Hierarchical	No other components
Dependencies	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**functions as in FMT_MOF.1.1**].
Application Note	None

7.2.4.4 FMT_SMR.1 Security roles

Hierarchical	No other components
Dependencies	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles [**user**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Application Note	User is defined as non-privileged user. Multiple non-privileged user accounts can be created by KTSB service personnel. Non-privileged user accounts cannot be used to create other accounts, or modify their own, or any other account. KTSB service personnel role is not part of the scope.

7.2.4.5 FMT_MSA.1 Management of security attributes

Hierarchical	No other components
Dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] to restrict the ability to [***change_default, modify,***

delete, [**and add**]] the security attributes [**as in FDP_IFF.1.1**] to [**user**].

Application Note None

7.2.4.6 FMT_MSA.5 Static attribute initialisation

Hierarchical No other components

Dependencies FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.5.1 The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] to provide [***restrictive, [none]***] default values for security attributes that are used to enforce the SFP.

Application Note By default, HTTP request and responses will be allowed or rejected based on pre-configured rules in TOE.

7.3 Security Assurance Requirements

This ST claims compliance to the assurance requirements from the CC EAL2 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat environment.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

Table 9: Security Assurance Requirements for EAL2

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design

AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

8 TOE Summary Specifications

TOE addressed the security functional requirements as following:

8.1 Identification and Authentication

TOE user can access TOE by providing username and public key in the command-line interface via SSH client. User is not allowed to perform any actions on TOE before being identified and authenticated successfully. KTSB service personnel will create a user account for the given user using their public key for authentication.

Relevant SFR: FIA_ATD.1, FIA_UID.2, FIA_UAU.2

8.2 User Data Protection

TOE protects the web application from external network intrusions by using information flow control between internal and external network. The TOE will log all HTTP requests and responses before allowing or rejecting the HTTP requests. KTSB service personnel could configure HTTP filter rules and policies based on the subject and information security attributes. The following are subject and information that used to allow or rejecting HTTP requests:

a) subject security attributes:
   - Presumed signature

b) information security attributes:
   - Presumed address of source subject (whitelist/blacklist);
   - Presumed address of source subject for geoblocked
   - Presumed address of destination subject;
   - Presumed port of destination subject;

Destination is the webserver which has static IP address and port which is pre-configured.

Following are the rules pre-configured in TOE to permit a HTTP requests and responses:

a) Subject on an internal network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created based on cyber-attack below:
  - web application attack

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created based on cyber-attack below:
  - web application attack

Following are the rules pre-configured in TOE to deny a HTTP requests and responses:

- Reject requests for access or services where the information arrives on an internal or external TOE interface, and the presumed signature is defined in on cyber-attack below:
  - web application attack

By default, all external (Internet) traffic will be blocked. KTSB service personnel can configure rules for application vulnerabilities, signature patterns, evasion patterns and Geo-location blocking. However, the modification or changes to rules are not part of the scope of evaluation.

Relevant SFR: FDP_IFC.1, FDP_IFF.1

8.3 Security Management

TOE functions can be managed through command-line interface. The TOE only allows limited user access to run a limited set of commands. User is defined as non-privileged user. Multiple non-privileged user accounts can be created by KTSB service personnel. Non-privileged user accounts cannot be used to create other accounts, or modify their own, or any other account. These do not affect the running mode of the TOE.

User can view settings and logs but cannot modify configuration. Following are the functions or logs that can be query or viewed by user:

a) uptime : shows how long the unit has been powered up since last reboot/shutdown. Also shows load average over 1 minute, 5 minutes and 15 minutes. For minute by minute load, the first load avg is relevant. For longer term load, the 15 minute average is more useful.
b) show-array: shows the status of the ZFS flash mirrored array
c) show-network: shows network capture over the active WAN interface
d) show-realtime: show a continuously rolling capture of realtime attacks
e) show-realtimeall: show a continuously rolling capture of realtime WAF messages
f) show-sqli: show all sql injection attacks in pagination mode
g) show-rfi: show all remote file inclusion attacks in pagination mode
h) show-xss: show all cross-site scripting attacks in pagination mode
i) find-string: displays blocks by string or FQDN

User could not change the default value, modify, delete and add the:

- signature
- address of source subject (whitelist/blacklist);
- address of source subject for geoblocked
- address of destination subject;
- port of destination subject;

By default, HTTP request and responses will be allowed or rejected based on pre-configured rules in TOE. Only KTSB service personnel are able to modify configurations upon request (eg whitelisting/blacklisting). However, the modification or changes to rules are not part of the scope of evaluation. KTSB service personnel role is not part of the scope.

Relevant SFR: FMT_MTD.1, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.5

8.4 Security Audit

The TOE will generate audit records for selected security events in several log files. The events that will be logged is HTTP Request and responses. Each audited events will be recorded along with date and time of event, source IP, event and event details. Audit records can be viewed by user and cannot be edited. Users are not able to delete or otherwise modify said audit log. User could select for viewing. Full audit reports are emailed every night to the designated email address together with an executive summary. TOE will create a new log file to store the audit records if the size limit is reached for a log file. The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. TOE prevents modification of date and time manually. The user has not ability to change date/time/time-zone. All these are set by KTSB service personnel,

and the TOE is continuously clock-synchronized with a pool of NTP servers. However, the setting of date/time/time-zone by KTSB personnel are not part of the scope of evaluation.

Relevant SFR: FAU_GEN.3, FAU_SAR.1, FAU_SAR.3, FAU_STG.1

9 Rationale

9.1 Protection Profile Conformance Claim Rationale

ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

9.2 Security Objectives Rationale

This section explains how threat, assumptions and OSP are related to each other. The following tables show threat, assumptions and organizational policy being mapped to security objectives.

9.2.1 Rationale for Security Objectives Mapped to Threats

Table 10: Rationale for Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.ACCESSLOG An unauthorized person successfully accesses the TOE data or security functions without being detected.	**O.ACCESSLOG** TOE shall record a readable log of security events.	This security objectives counter threat because any success or failure of authentication events will be recorded in a readable log of security events. Each security events will be logged along with the source IP address.
T.AUDIT An unauthorized person may intentionally or unintentionally delete audit records to destroy evidence of adverse events	**O.AUDIT** TOE shall prevent an unauthorized person to modify or deletes audit records of security events	This security objective counter threat because it will prevent an unauthorized person to modify or deletes audit records of security events

executed.	executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	executed. The objective also ensures the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
T.EXPLOIT An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.	**O.EXPLOIT** TOE shall mediate the information flow in internal network and between internal and external network.	This security objective counters threat because TOE will mediate the information flow in internal network and between internal and external network to decide whether to allow or drop information send by unauthorized person.
T.REMOTE An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator (KTSB Service personnel) or user and the TOE.	**OE.CONN** Authorized administrators (KTSB Service personnel) or user shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.	This security objective counters threat because the environment will provide a secure and encrypted connection to prevent unauthorized person or external IT entity sniff the data and modify it.
T.CONFIG An unauthorized person may read and modify security TOE functions and configuration data.	**O.CONFIG** TOE shall prevent unauthorized person to access TOE functions and configuration data.	This security objective counters threat because TOE will prevent unauthorized person to access TOE functions and configuration data.
T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to assess and use security functions and/or non-security functions provided by the TOE.	**O.NOAUTH** TOE shall protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective counters threat because security events are being audited and recorded in log file. Each security event will be recorded along with date and time of event, source IP address and other event details. The audit records cannot be modified by user in order to preserve its integrity. Access control shall be enforced to ensure only the permitted user role have privilege to TOE functions that is relevant to their role.

9.2.2 Rationale Security Objectives Mapped to OSP

Table 11: Rationale Security Objectives Mapped to OSP

OSP	Security Objectives	Rationale
P.ROLE Only authorized persons assigned by the organization have access to the TOE.	**O.CONFIG** TOE shall prevent unauthorized person to access TOE functions and configuration data.	This security objective counters OSP because TOE will prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized user shall have access to TOE.
P.PASSPHRASE Authorized user shall use complex passphrase to generate private and public key.	**OE.KEY** The TOE environment shall generate, distribute and use user's public and private keys securely for SSH client.	This security objective counters OSP because authorized user use complex passphrase to generate private and public key for SSH client during identification and authentication process in TOE.

9.2.3 Rationale Security Objectives Mapped to Assumptions

Table 12: Rationale Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.PHY The TOE and its environment are physically secure.	**OE.PHY** The TOE and its environment shall be physically secure.	This security objective counters assumption because the TOE and its environment shall be physically secure.
A.FLOW Information cannot flow through internal and external networks unless it passes through the TOE.	**OE.FLOW** The TOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.	This security objective counters assumption because TOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.
A.CONFIGRULE TOE environment and TOE configurations and rules are pre-configured securely.	**OE.CONFIGRULE** The TOE environment and TOE configurations and rules shall be pre-configured securely.	This security objective counters assumption because TOE environment and TOE configurations and rules are pre-configured securely.
A.TIMEBACK The TOE environment will provide	**OE.TIMEBACK** The TOE environment shall	This security objective counters assumption because TOE environment shall

reliable time stamps.	provide reliable time stamps.	provide reliable time stamps.
A.KEY User's public and private keys are generated, distributed and used securely for SSH client.	**OE.KEY** The TOE environment and user shall generate, distribute and use user's public and private keys securely for SSH client.	This security objective counters assumption because TOE environment and user shall generate, distribute and use user's public and private keys securely for SSH client.
A.CONN The TOE environment will provide a secure connection between TOE and authorized administrator (KTSB Service personnel) or users.	**OE.CONN** Authorized administrator (KTSB Service personnel) or user shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.	This security objective counters assumption because authorized administrator (KTSB Service personnel) or user shall access the TOE using a secure connection (SSH) provided by the environment to prevent eavesdropping.
A.ADMIN The TOE Administrator (KTSB Service personnel) will be non-hostile and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.	**OE.ADMIN** The TOE Administrator (KTSB Service personnel) is non-hostile and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.	This security objective counters assumption because authorized administrator (KTSB Service personnel) or user shall be non-hostile and follow guidance documentation accordingly to ensure a secure configuration being deployed for TOE.

9.3 Extended Security Functional Requirement Rationale

Refer to Section 8.1 Extended Security Functional Requirement (SFR) for rationale.

9.4 Extended Security Assurance Requirement Rationale

Not applicable since there is no extended Security Assurance Requirement declared in ST.

9.5 Security Functional Requirements Rationale

This section provides the rationale of using SFRs to meet the security objectives for the TOE and justify the SFRs dependencies that have been satisfied or not satisfied.

9.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Table 13: Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale

O.ACCESSLOG TOE shall record a readable log of security events.	FAU_GEN.3	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, source IP address and event details. It traces back to this objective.
	FAU_SAR.1	This SFR specify that user will have the capability to view the audit trail data in log form. It traces back to this objective.
	FAU_SAR.3	This SFR specify that user can select log file and/or filter it related to event. It traces back to this objective.
O.AUDIT TOE shall prevent an unauthorized person to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by user or unauthorized person. It traces back to this objective.
O.EXPLOIT TOE shall mediate the information flow in internal network and between internal and external network.	FDP_IFC.1	This SFR identify the external IT entities in the Unauthenticated Information Flow Control SFP that send information to other entity. The SFP will either reject or allow the information flow. It traces back to this objective.
	FDP_IFF.1	This SFR identify the external IT entity and its security attributes as part of the information flow control SFP. TOE will permit or deny the information flow based on rules pre-configured in TOE. It traces back to this objective.
O.CONFIG TOE shall prevent unauthorized person to access TOE functions and configuration data.	FIA_ATD.1	This SFR provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. It traces back to this objective.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data. It traces back to this objective.
	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.

	FMT_MOF.1	This SFR restrict the ability to view TOE functions to user. It traces back to this objective.
	FMT_MTD.1	This SFR restrict the ability to query and view the logs to in TOE. It traces back to this objective.
	FMT_SMF.1	This SFR identify management functions that are available in TOE, that are able to viewed by user. It traces back to this objective.
	FMT_SMR.1	This SFR identify the user role that exist in TOE. It traces back to this objective.
	FMT_MSA.1	This SFR restrict the ability to change default value, modify, delete and add security attributes to roles in TOE. It traces back to this objective.
	FMT_MSA.5	This SFR enforce default TOE behaviour which is to allow or reject HTTP request and responses based on pre-configured rules in TOE. It traces back to this objective.
O.NOAUTH The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	FAU_GEN.3	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, source IP address and event details. It traces back to this objective.
	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by user or unauthorized person. It traces back to this objective.
	FDP_IFF.1	This SFR identify the external IT entity and its security attributes as part of the information flow control SFP. TOE will permit or deny the information flow based on rules pre-configured in TOE. It traces back to this objective.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data. It traces back to this objective.
	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data. It traces back to this objective.

9.5.2 SFR Dependency Rationale

The following table provides a demonstration that all SFRs dependencies included in the ST have been satisfied.

Table 14: SFR Dependencies

SFR	Dependency	Dependency Met?	Justification
FAU_GEN.3	FPT_STM.1	No	The TOE does not have a feature to generate time stamps independently. The date and time stamp is provided by the environment, which is NTP server.
FAU_SAR.1	FAU_GEN.1	No	Met with FAU_GEN.3. Refer Section 6.1 for more details.
FAU_SAR.3	FAU_SAR.1	Yes	-
FAU_STG.1	FAU_GEN.1	No	Met with FAU_GEN.3. Refer Section 6.1 for more details.
FDP_IFC.1	FDP_IFF.1	Yes	-
FDP_IFF.1	FDP_IFC.1	Yes	-
	FMT_MSA.3	No	Met with FMT_MSA.5. Refer Section 6.1 for more details.
FIA_ATD.1	-	-	-
FIA_UAU.2	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FIA_UID.2	-	-	-
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_SMF.1	-	-	-
FMT_SMR.1	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MSA.5	FMT_MSA.1 FMT_SMR.1	Yes	-