WAPPLES v4.0
Security Target

v4.0

Penta SECURITY

Revision History

Version	Date	Author	Summary
v1.0	Jan 20, 2012	PENTA SECURITY SYSTEMS INC.	· Initial version
v2.0	Feb 20, 2012	PENTA SECURITY SYSTEMS INC.	· Update according to EOR-01
v3.0	Mar 23, 2012	PENTA SECURITY SYSTEMS INC.	· Update according to EOR-02
v4.0	Sep 28, 2012	PENTA SECURITY SYSTEMS INC.	· Partial modification to the security function requirements. · Update according to the new item configuration identification system

TABLE OF CONTENTS

1. Security Target Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 TOE Overview 7
1.4 TOE Description 13
1.5 Terms and Definitions 18
1.6 Conventions 20
2. Conformance Claims 21
2.1 Conformance to the CC, PP, and Package 21
2.2 Conformance Rationale 21
3. Security Problem Definitions 22
3.1 Assets 22
3.2 Threats 22
3.3 Organizational Security Policy 23
3.4 Assumptions 24
4. Security Objectives 25
4.1 Security Objectives for the TOE 25
4.2 Security Objectives for the Operational Environment 26
4.3 Security Objectives Rationale 27
5. Extended Components Definition 34
6. Security Requirements 35
6.1 TOE Security Functional Requirements 35
6.2 TOE Assurance Requirements 52
6.3 Rationale for security requirements 72
6.4 Rationale for Dependencies 80
6.5 Rationale for Mutually Supportive Relationship and Internal Consistency 82
7. TOE Specifications Summary 84
7.1 Security Audit Functions 84
7.2 User Data Protection Functions 90
7.3 Identification and Authentication Functions 96
7.4 Security Management Functions 99
7.5 TSF Protection Functions 103
7.6 Session Locking Functions 103

LIST OF FIGURES

[Figure 1] Inline Mode 10
[Figure 2] Reverse Proxy Mode 10
[Figure 3] Logical Scope of the TOE 15

LIST OF TABLES

[Table 1] Security Target Reference 6
[Table 2] TOE Reference 6
[Table 3] Non-TOE Components Required by the TOE 12
[Table 4] Physical Scope of the TOE 13
[Table 5] Specifications of Detection Engine Operating Hardware 14
[Table 6] Specifications of Management Console Operating Hardware 14
[Table 7] Conformance to CC, PP, and Assurances 21
[Table 8] Threats to the TOE 23
[Table 9] Organizational Security Policy 24
[Table 10] Assumptions 24
[Table 11] Security Objectives for the TOE 25
[Table 12] Security Objectives for the Operational Environment 27
[Table 13] Tracing between the Security Objectives for the TOE and the Security Problem Definition 28
[Table 14] Tracing between the Security Objectives for the Operational Environment and the Security Problem Definition 31
[Table 15] Security Function Requirements 36
[Table 16] Security Alarm Countermeasures by Potential Security Violation Events 36
[Table 17] Auditable Events 39
[Table 18] Selectable Detection Log Review 41
[Table 19] Auditable Events by the Group of Event Types 41
[Table 20] Security Function Management List 47
[Table 21] Security Attributes Related to Security Policy 48
[Table 22] TSF Data List 49
[Table 23] Administrator Classification 50
[Table 24] TOE Assurance Requirements 52
[Table 25] Response to Security Objectives and Security Functional Requirements 73

[Table 26] The Dependencies of Functional Components 81
[Table 27] Audit Log Generation Events..... 86
[Table 28] Auditable Events by Group of Event Types 87
[Table 29] Auditable Events by Types of Audit Log 88
[Table 30] Detection Log Search and Sort Functions..... 89
[Table 31] Detailed Rules of Web Security Functions..... 94
[Table 32] OWASP Top 10 Security Function Responses 96
[Table 33] Security Function Descriptions..... 100
[Table 34] Security Attributes of Web Security Policy..... 101
[Table 35] Management Authority by TSF data 102

1. Security Target Introduction

This document is the Security Target (ST) of web application firewall 'WAPPLES v4.0,' and explains the security requirements of the web application firewall (WAF) and the grounds for its evaluation.

1.1 ST References

Category	Description
Title	WAPPLES v4.0 Security Target
ST Version	v4.0
Author	PENTA SECURITY SYSTEMS INC.
Date of Creation	Sep 28, 2012
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Public Administration and Security Notice No.2009-52)
Common Criteria Version	V3.1 R3
Evaluation Assurance Level	EAL 4
Keywords	Web Application Firewall, Access Control, Information Flow Control

[Table 1] Security Target References

1.2 TOE References

Category	Description
TOE Title	WAPPLES v4.0
TOE Scope	WAPPLES v4.0.5 - Detection Engine 4.0.2 - Management Console 4.0.3
User Guidance	WAPPLES v4.0 Operation and Installation Guidance v4.0
Developer	PENTA SECURITY SYSTEMS INC.
Sponsor	PENTA SECURITY SYSTEMS INC.
Final Release Date	Sep 28, 2012

[Table 2] TOE References

1.3 TOE Overview

1.3.1 Product and TOE Introduction

WAPPLES is a web application firewall (WAF) that securely protects a web server and its web applications by detecting and blocking attacks in advance through the identification of abnormal web traffic. WAPPLES v4.0 (“TOE” hereinafter) is a software type delivered to the end-user loaded on a dedicated hardware device (see Section 1.4.1).

The TOE protects web servers and web applications from attacks seeking to exploit web application vulnerabilities. In order to enable more secure web operations, it detects web attacks (such as SQL Injection and XSS), and prevents unnecessary information leakage by only allowing trusted access. In addition, it provides various visualized informational data related to web operations, along with audit records, and user convenience through customization options.

1.3.2 TOE Security Features

The TOE contains the following features as a web application firewall:

Web request and response analysis for web security

The TOE analyzes the HTTP/HTTPS request messages and response messages at an application level. If a character string that matches a specified pattern is found, or if a certain parameter’s integrity is violated, the TOE protects the web server and web application by taking appropriate measures such as blocking the relevant messages.

The method of web request and response security analysis is as follows:

- HTTP standard check: The TOE checks if the HTTP request complies with the predefined protocols and grammar rules, as many types of worms and buffer overflow attacks intentionally violate these protocols in an attempt to cause a malfunction of the web server. By thoroughly inspecting for compliance with the HTTP standard protocols, the TOE may detect many attacks.

- Analysis of attack methods: The TOE performs an analysis of the underlying method of each type of attack in order to detect a web attack that may not be countered via general pattern matching.
  For example, in the case of an SQL injection, the TOE identifies an SQL injection not

only by checking if the SQL query contains special characters but by checking whether the input values are a part of the SQL query by using an SQL Validator.

- Regular expression pattern matching: The TOE detects and blocks attacks that apply a regular expression by using the pattern matching method.
- URL access control: The TOE blocks the request for a URL that is not registered on the access allowance list.
- Protection of web security elements: The TOE detects web forgeries by verifying the integrity of Cookies and Hidden fields included within the HTTP requests and responses.

If the web server or web application protected by the TOE provides web services using HTTPS protocol, the TOE decrypts and analyzes the encrypted HTTPS request and response messages by acting as an intermediary between the web server and the web client.

Access control at the network level

The TOE detects and blocks access at the network level from web clients that have a source IP address which is not permitted. The prohibited IP addresses are managed in the form of a blacklist, which is either manually set by the authorized administrator or automatically added when an IP address meets the conditions of HTTP traffic which match that of a DoS attack, or exceed the accumulated risk level set by the administrator.

Security management function

The TOE provides security management functionality for an authorized administrator by requiring identification and authentication of all who attempt to access the management features. By using the security management functions, the administrator sets the web security policies and access controls, manages information related to the TOE operation, and prevents unauthorized access by locking an administrator session after a predefined period of inactivity.

Traceability in case of security-relevant events

In the case of a security-relevant event, the TOE generates audit data to ensure traceability and provides a means for the authorized administrator to search the logged data. The audit data is saved in a Detection log in which the web security and access

control results are recorded, and an Audit log in which the events related to the TOE operation are recorded. The TOE performs a statistical analysis on the audit data (Detection log) and provides a report on the result for the authorized administrator. In the case of a critical audit security event, through the analysis of potential violations, a security alarm is sent to the appointed administrator so that the stored audit data can be secured.

TSF and TSF data protection

The TOE guarantees secure operation of the TSF through integrated monitoring of the TSF executable files and the TSF configuration files. Additionally, the TOE enables the TSF to always maintain security by periodically inspecting the condition of the network interface and the Detection Engine's operational status.

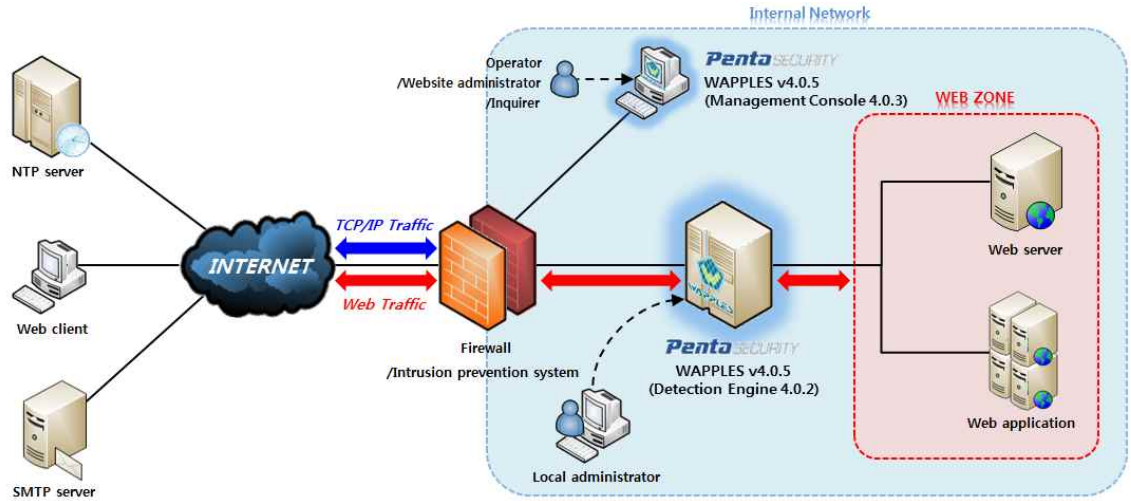
1.3.3 TOE Operational Environment

The TOE is composed of a "Detection Engine," which analyzes incoming web traffic and protects the web server and its web applications from external web attacks; a "Management Console," which provides the security management functions used for setting security policies and the TOE operational environment for the Remote administrator.

The TOE shall be installed and operated in an internal network where it is securely protected from external attacks by a firewall and intrusion prevention system. The firewall and intrusion prevention system should be set to forward the incoming web traffic from outside to the TOE.

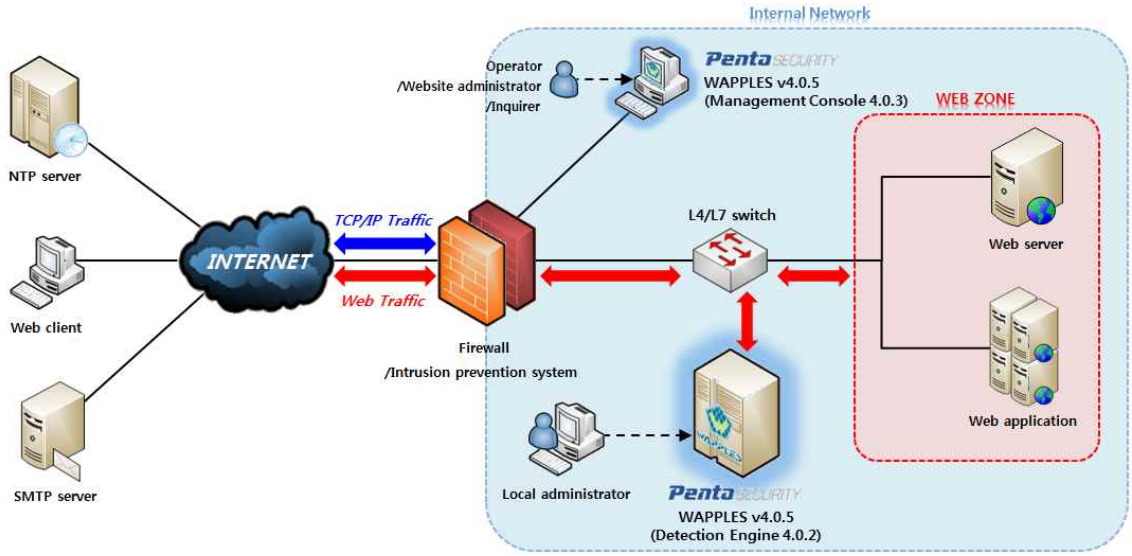
The TOE operational environment is configured in "inline mode" or "reverse proxy mode" depending on its network location.

Inline mode is illustrated in [Figure 1]. The TOE operates in the form of a Bridge, where the TOE is not externally exposed as it is located on the sole connection point between the outside and inside of the web zone. Using an inline mode has the advantage of accurately tracing the subject of a web attack, as the TOE sends the web traffic to the web server without changing its source IP address.



[Figure 1] Inline Mode

Reverse proxy mode is illustrated in [Figure 2]. This mode changes the DNS setting of the web application or the web server and uses a L4/L7 switch to hide the IP address of the web server and distribute services for each URL, which brings forth enhanced security.



[Figure 2] Reverse Proxy Mode

The hardware and software required by the TOE are as follows:

Category		Non-TOE components required by the TOE	
External Entity		Web server	A web service provider located in the web zone that responds to HTTP request messages sent from a web client
		Web client	An entity that sends HTTP request messages to the web server to receive web services
		Remote administrator	An administrator who uses the TOE security management interface through the Management Console. It includes an Operator who can set and operate all TOE security management functions, a Website administrator who can manage and operate the policies applied on the assigned website, and an Inquirer who can look up the audit data
		Local administrator	An administrator who can set up a network for the TOE operation through a CLI-based console
		NTP server	An external time stamp server from which the TOE receives a reliable time value that is used to generate an accurate audit record (Detection log, Audit log) in regards to security-relevant events
		SMTP server	An email delivery server used to send security alarm emails to the Remote administrator
Detection Engine	H/W	TOE-dedicated hardware platform	Hardware on which the Detection Engine is installed and operated (refer to [Table 5] for a detailed specification of each hardware model)
	S/W	Gentoo Linux OS 2008.0	A Linux (Kernel 2.6.29.3)-based operating system used for operation of the Detection Engine
		OpenSSL 0.9.8x	A cryptographic library used for SSL communication to prevent disclosure and forgery of the data sent from Management Console (OpenSSL Library in Gentoo Linux OS is invoked by modSSL of the Apache HTTP Server)

Category		Non-TOE components required by the TOE	
		Apache HTTP Server 2.2.22	A web server that provides a web page through which the administrator can request or operate the Management Console installation file and the WebAPI for communication with the Management Console
		PostgreSQL 8.0.15	A DBMS used to securely store the TOE audit data (Detection log, Audit log)
		CouchDB 1.1.0	A DBMS used to securely store the settings information such as the security policies set by the authorized administrator
Management Console	H/W	Administrator PC	A hardware on which the Management Console is installed and operated (refer to [Table 6] for a detailed specification of the hardware)
	S/W	Microsoft Windows XP Professional SP3 (32 bit)	A Windows operating system used for the operation of the Management Console
		.NET Framework 4.0	A framework that performs SSL communication to operate the Management Console and to prevent disclosure and forgery of transferred data
		Windows Internet Explorer 8.0	A web browser used to access the start-up page for the operation of the Management Console

[Table 3] Non-TOE Components Required by the TOE

1.4 TOE Description

1.4.1 Physical Scope

The TOE is composed of the Detection Engine software that is delivered to the user loaded on a dedicated hardware device, the Management Console software that is installed on the Administrator PC, and a guidance document that is delivered in the form of a booklet. The Management Console is included in the delivered Detection Engine installation image, thus the administrator accesses the Detection Engine and downloads and installs the Management Console on the Administrator PC.

Category	Description	Distribution Form
WAPPLES v4.0.5	Detection Engine 4.0.2	Software loaded on a hardware
	Management Console 4.0.3	Software
User Guidance	WAPPLES v4.0 Operation and Installation Guidance v4.0	Booklet

[Table 4] Physical Scope of the TOE

The TOE hardware that operates the Detection Engine includes 100 eco, 1000 Type2, and 1000 Type2 Plus. Their specifications are as follows.

Non-TOE Components		Description
WAPPLES-100 eco	CPU	Intel Core2 Quad 2.66 GHz
	HDD	500 GB
	Memory	4 GB
	Network Interface	▪ Management port: 10/100/1000 BaseTX * 2 ▪ Service port: 10/100/1000 BaseTX * 8
WAPPLES-1000 Type2	CPU	Intel Xeon Quad Core 2.33 GHz * 2
	HDD	500 GB
	Memory	8 GB
	Network Interface	▪ Management port : 10/100/1000 BaseTX *2 ▪ Service port: - 10/100/1000 BaseTX * 8 - 1000 BaseSFP * 2 ▪ Optional Service port: - 1000 Base Optical * 2

Non-TOE Components		Description
WAPPLES-1000 Type2 Plus	CPU	Intel Xeon Quad Core 2.50 GHz * 2
	HDD	500 GB
	Memory	8 GB
	Network Interface	▪ Management port : 10/100/1000 BaseTX *2 ▪ Service port: - 10/100/1000 BaseTX * 8 - 1000 BaseSFP * 2 ▪ Optional Service port: - 1000 Base Optical * 2

[Table 5] Specifications of Detection Engine Operating Hardware

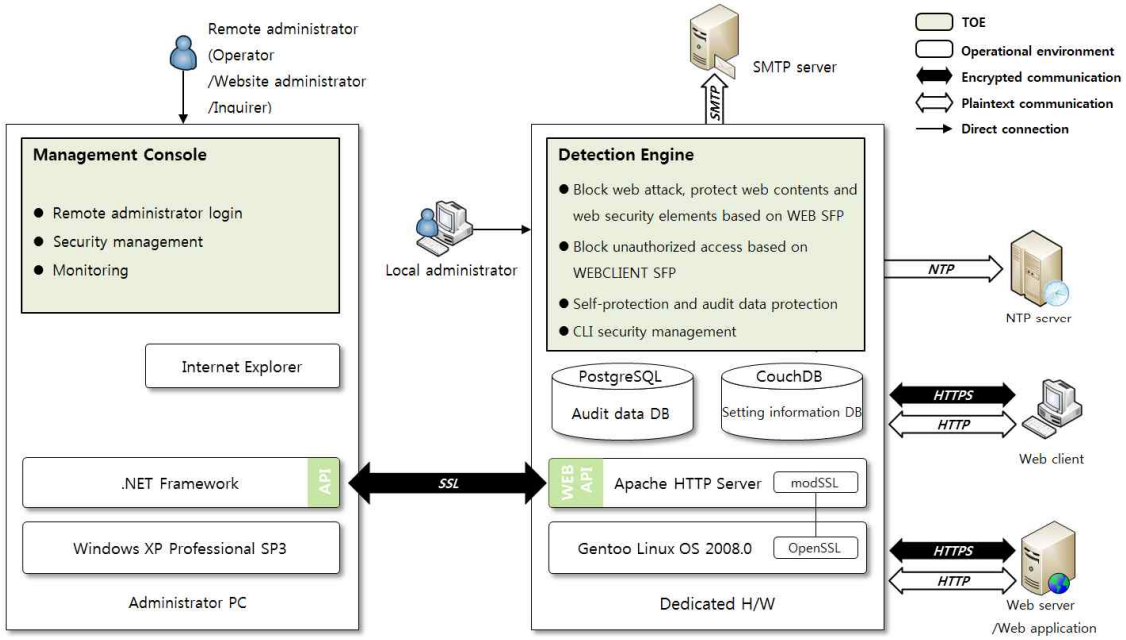
The minimum specifications for the Administrator PC (on which the Management Console is installed and operated) are as follows:

Non-TOE Components	Description
CPU	Intel Pentium4 1.6 GHz or above
HDD	100 GB or above
Memory	1 GB or above
Network Interface	100/1000 Mbps

[Table 6] Specifications of the Management Console Operating Hardware

1.4.2 Logical Scope

The logical scope of the TOE is as illustrated in [Figure 3].



[Figure 3] Logical Scope of the TOE

- Management Console

The Management Console is operated in the .NET Framework environment of the Administrator PC. To operate the Management Console, the administrator shall connect to the start-up web page of the Detection Engine through Internet Explorer and install the Management Console on the Administrator PC.

The Management Console enables an authorized administrator to operate the TOE by using the security management functions via GUI. In order to securely transmit and receive the TSF data requested or configured through the Management Console by the authorized administrator, an SSL communication channel formed between the .NET Framework and the Apache HTTP Server is used.

The security functions provided through the Management Console are as follows:

Remote administrator login

The Management Console provides the Remote administrator with a login function to ensure that only authorized users have access to the security management functions. Once the Remote administrator successfully logs in, the privileges of an Operator, a

Website administrator, or an Inquirer in accordance with his/her role are granted.

To prevent unauthorized access, the Management Console temporarily locks the Remote administrator's account in the event of consecutive authentication failures and locks the security management screen if the Remote administrator is inactive for a time exceeding the predefined period.

Refer to Section 6.1 for additional information on the identification and authentication and the TOE access.

Security management

The Management Console only allows the Remote administrator to manage the administrator accounts and set up the operational environment, network configuration, WEB SFP, and WEBCLIENT SFP.

Refer to Section 6.1 for additional information on security management.

Monitoring

The Management Console only allows the Remote administrator to look up and search audit data, look up web attack detection statistics, and look up the TOE system status.

Refer to Section 6.1 for additional information on security auditing and security management.

- Detection Engine

The Detection Engine protects the web server and web applications based on WEBCLIENT SFP and WEB SFP, and is stored in PostgreSQL. In addition, it provides the Local administrator with an interface for security management such as configuring the network, and performs self-protection and audit data protection for the secure operation of the TOE security functions.

If the web server that needs protection provides HTTPS web services, the Detection Engine relays the HTTPS web traffic between the web server and the web client by using an OpenSSL library.

The security functions provided by the Detection Engine are as follows:

Blocking web attack and protecting web contents and web security elements based on WEB SFP

The Detection Engine detects and counters various external attack attempts on the web server based on the WEB SFP set by the Remote administrator, protects the Cookie and Hidden field values, and prevents leakage of the web contents. The security functions are performed by using the following methods for attack detection and analysis:

① Blocking of abnormal web traffic through an HTTP standards check.
② Detecting and blocking various attack patterns through an analysis of attack methods.
③ Pattern matching using a regular expression.
④ Selectively allowing access to only the URLs that are permitted for web clients.
⑤ Protecting web elements such as Cookies and Hidden fields.

Refer to Section 6.1 for additional information on user data protection.

Blocking unauthorized access based on WEBCLIENT SFP

The Detection Engine preferentially blocks the HTTP requests of a web client with an IP address that is registered on the access block list.

Additionally, depending on the configured HTTP DoS attack settings and accumulated risk values for each detection rule, the IP address of a potential threat is automatically updated on the access block list.

Refer to Section 6.1 for additional information on user data protection.

Self-protection and audit data protection

The Detection Engine assures the availability of security functions by periodically checking for modulation or forgery of the integrity of executable files, the settings data, and inspecting the status of processes. In addition, by periodically checking the available capacity of PostgreSQL DB and CouchDB, the Detection Engine sends an alarm mail to the appointed administrator to take appropriate action when the predefined threshold is exceeded.

Refer to Section 6.1 for additional information on protection of the TSF and security audit.

CLI security management

The Detection Engine provides a CLI security management interface for only the Local administrator, after logging in he/she can configure the network environment.

Refer to Section 6.1 for additional information on security management.

1.5 Terms and Definitions

Administrator refers to the user who accesses the TOE to securely operate and manage the TOE. The administrators are authorized through identification authentication from the TOE and are classified as a "Remote administrator" who remotely operates the TOE security management functions through the Management Console; and a "Local administrator," who directly connects via a serial port of the hardware on which the Detection Engine is installed and operated.

Management Console refers to a component of the TOE used by the Remote administrator for the operation of security management functions such as setting security policies and checking audit data.

Detection Engine refers to a component of the TOE that protects the web application and web server by analyzing and detecting the incoming web traffic and blocking harmful web traffic in accordance with the security policies and operational information set by the Remote administrator sent from the Management Console.

Remote administrator refers to the authorized administrator who can operate the security management functions through the Management Console and is classified as an Operator, a Website administrator, and an Inquirer according to the privileges. The term of the administrator is also used to refer to the role.

Local administrator refers to the authorized administrator who can operate part of security management functions such as setting the management IP and network bandwidth via serial port of the hardware where the Detection Engine is installed and operated. The term of the administrator is also used to refer to the role.

Hidden field refers to the field hidden inside the HTML that is not visible on the web browsers but is used to deliver data.

URL(Uniform Resource Locator) refers to the standard that locates servers that provide the services of web documents and is expressed with standard protocols such as HTTP

and FTP. The URL is used to locate the files of each server that exists on the web.

HTTP 1.1 standard refers to the standard format of HTTP (HyperText Transfer Protocol) 1.1, a protocol that is used to exchange information on the WWW. It has enhanced speed, added methods, and added Host request-header data compared to HTTP 1.0.

HTTP Request message refers to the message sent by the web client user to the web server in order to request resources. The Request message is composed of the URL containing resources, the method, the header field information, and the body information.

HTTP Response message refers to the response message of the web server in order to confirm the request of the web client user. The Response message is composed of the web server's status code, the Header information, and the body information of the request.

SQL Syntax validator refers to a syntax analyzer that is used to detect and protect against SQL Injection attacks by analyzing SQL query syntax which may exist in an HTTP request message.

Cookie refers to the temporary file automatically generated when a web client accesses an Internet website. It contains sensitive records such as the browsing history of the user, product purchases, credit card information, ID, password, and IP address.

HTTP DoS attack refers to an attack method where a web client requests more HTTP connections than a web server can respond to, rendering the web server unable to offer normal services.

Personal information refers to the information used to identifiy each person, such as social security number, identification card number, coporate registration number, business registration number, email, credit card number, passport number, etc.

Accumulated risk refers to the degree of risk calculated by considering the weighted risk values, the number of attacks, and the time over which the attacks progressed according to each detection rule. It is used to automatically register an IP on the access block list of the TOE if the IP exceeds the threshold set by the administrator.

Detection log refers to the audit data that records the detection results (e.g. abnormal web traffic) according to the detection rules set by the Remote administrator.

Audit log refers to the audit data that records the security-relevant events of the TOE

operation such as the start-up and shut-down of the TOE, the setting of detection rules, and the identification and authentication of a Remote administrator.

IP block time refers to the effective time frame for blocking the IP addresses and the IP address ranges that are registered in the access block list.

Delayed traffic time refers to the time period over which the sessions are delayed without being established normally, due to abnormal traffic occuring from the same source.

Import time of delayed traffic refers to the time over which the abnormal traffic occurring from the same source is continually being imported to the web server.

Import frequency of delayed traffic refers to the number of the import attempts of the abnormal traffic occurring from the same source to the web server.

Web application refers to the web-based (either Internet or intranet) computer application that is developed so that a user can utilize various services of the web server . The programming languages to develop a web application include Java, XML, PHP, ASP, JSP, etc.

Web contents refers to all auditory and visual representations that are delivered through the web. These are provided to the user in the form of documentation, data, application, image, audio, video file, web page, mail message, etc.

Access block list refers to the list of HTTP DoS attacker IP addresses, the IP addresses that have exceeded the acculmuated risk, and the IP address and IP address ranges that have been set by the administrator to be blocked.

1.6 Conventions

This ST uses the selection, the assignment, the refinement, and the iteration operation as identical to those of the CC.

2. Conformance Claims

2.1 Conformance to CC, PP, and Assurances

Category	Description
CC	• Common Criteria for Information Technology Security Evaluation(Ministry of Public Administration and Security Notice No.2009-52) • Common Criteria for Information Technology Security Evaluation Part 1 (CCMB-2009-07-001) Version 3.1 Revision 3 • Common Criteria for Information Technology Security Evaluation Part 2 (CCMB-2009-07-002) Version 3.1 Revision 3 • Common Criteria for Information Technology Security Evaluation Part 3 (CCMB-2009-07-003) Version 3.1 Revision 3
CC Part 2	Conformance
CC Part 3	Conformance
PP	None
Assurance Package	EAL 4

[Table 7] Conformance to CC, PP, and Assurances

2.2 Conformance Rationale

This ST does not conform to any PP.

3. Security Problem Definitions

The TOE security problem definitions are composed of the assumptions that describe the security of the TOE environment, the threats to the TOE assets and environment by a threat agent, and the organizational security policies, which includes the rules, procedures, practices, and the compliance guidelines for the TOE to maintain security.

3.1 Assets

The primary assets protected by the TOE are as follows.

- The web server, or the website in the web zone, and important contents stored in the web server
- The TOE itself, including the TSF data, executable files, and configuration files that support secure operation of the TOE.

3.2 Threats

An external threat agent is an unauthorized user of the TOE or a web client that causes a threat to the website and the web application. The threat agent has enhanced-basic level of expertise, resources, and motivation. By easily obtaining attack tools and exploitable vulnerability information of a website, operating system, or application through the Internet, it can damage the assets of the targeted website, illicitly obtain information, or damage the TOE assets by an unauthorized method. The TOE protects its asset from these threats as below.

Label	Threats to the TOE
T. Abnormal data import	The web client that sends HTTP request message may export or damage the data stored in the web server by importing abnormal data to the web server
T. Web server access control bypass	A threat agent may attempt to bypass the access control policy of the web server to access a URL that it is not allowed
T. CSRF attacks	A threat agent may export or corrupt important information of the web server by intercepting and corrupting the HTTP request messages that include session information and the authentication information of the web client, and then

Label	Threats to the TOE
	sending it to a vulnerable web application
T. Administrator masquerade	A threat agent may masquerade as an authorized administrator by reusing or guessing the authentication data and change the TOE information flow control policy
T. TSF data export and damage during transmission	A threat agent may export, modify, or delete the TSF data transmitted between the components of the TOE through unauthorized methods
T. Stored TSF data damage	A threat agent may modify or delete the important data related to operations saved in the TOE through unauthorized methods
T. Record failure	A threat agent may prevent audit records from being recorded by taking actions to exhaust audit storage capacity
T. DoS attacks	A threat agent may interfere with normal web services of the web server by excessively using its service resources
T. Consecutive authentication attempts	A threat agent may try to access the TOE by continuously attempting to be authenticated
T. Personal information import and export	A threat agent may cause unauthorized import/export of personal information to/from the web server through HTTP requests/responses or file uploads
T. Web client's sensitive data export and corruption	A threat agent may export or corrupt the sensitive data sent by the web client or stored in the web server

[Table 8] Threats to the TOE

3.3 Organizational Security Policy

The following conditions are included in the organizational security policy (OSP):

Label	Organizational Security Policy
P. Audit	Security-relevant events shall be recorded and maintained to trace accountability for the security related actions and the recorded data shall be reviewed
P. Secure management	The authorized administrator shall manage the TOE in a secure manner

Label	Organizational Security Policy
P. Blocking of external remote access	The authorized administrator shall block remote access to the TOE from the external network

[Table 9] Organizational Security Policy

3.4 Assumptions

The following conditions are assumed to exist in the TOE operational environment:

Label	Assumptions
A. Physical	It is assumed that the TOE is located in a physically secure environment where only authorized administrator can access
A. Manage	It is assumed that the authorized administrator performs the latest security updates of the TOE S/W platform (e.g. operating system, web browser) and, when changing the network configuration, keeps the TOE operational environment consistent with the security policy
A. No-evil	It is assumed that administrators who manage the TOE have no malicious intentions and are appropriately trained and follow all administrator guidance practices
A. Secure database	It is assumed that the database used by the TOE operates stably and is securely configured and managed
A. Sole connection point	It is assumed that the authorized administrator shall operate the firewall in a manner which only the web traffic among all imported traffics are sent to the web server by passing through the TOE.
A. Direct	It is assumed that the TOE and the CLI console are connected directly

[Table 10] Assumptions

4. Security Objectives

4.1 Security Objectives for the TOE

The following are the security objectives that shall be directly dealt with by the TOE:

Label	Security Objectives for the TOE
O. Blocking of abnormal data transfer	The TOE shall block importation of abnormal or corrupted data to the web server by analyzing the HTTP/HTTPS request messages sent by the web client as well as the HTTP/HTTPS response messages sent by the web server
O. Prevention of web server access control bypass	The TOE shall prevent the bypassing of the web server access control policy by blocking a web client's access to URLs that are not allowed
O. Identification and authentication	The TOE shall give access only to the authorized administrators by prompting identification and authentication of all who access the TOE
O. Prevention of stored TSF data damage	The TOE shall protect the stored TSF data from unauthorized modification or deletion
O. Restriction of excessive resource usage	The TOE shall keep the attackers from abnormally overusing the resources of the web application in order to ensure they will be available to normal users
O. Prevention of personal information import and export	The TOE shall control the HTTP requests/responses or file uploads to prevent unintentional import/export of personal information to/from the web server
O. Audit	The TOE shall record and maintain the security-relevant events to trace accountability for the security related responses, provide a means for the authorized administrator to review the recorded data, and prevent the loss of said audit data
O. Management	The TOE shall provide a means for the authorized administrator to manage the TOE effectively

[Table 11] Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

Below are the security objectives to be dealt with by the technical/procedural measures that are implemented by the operational environment in order for the TOE to correctly provide security functionality:

Label	Security Objectives for the Operational Environment
OE. Physical	The TOE shall be located in a physically secure environment where only authorized administrators can access
OE. Manage	The authorized administrator shall perform the latest security updates of the TOE S/W platform (e.g. operating system, web browser) and, when changing the network configuration, keep the TOE operational environment consistent with the security policy
OE. No-evil	Administrators who manage the TOE shall have no malicious intentions, be appropriately trained, and follow all administrator guidance practices
OE. Secure management	The TOE shall be delivered and installed in a secure way and be configured, managed, and used by the authorized administrator in a secure manner
OE. Secure database	The database used by the TOE shall operate stably and be securely configured and managed
OE. Sole connection point	It is assumed that the authorized administrator shall operate the firewall in a manner which only the web traffic among all imported traffics are sent to the web server by passing through the TOE.
OE. Time synchronization via NTP server	In order to record the security-relevant events accurately, the TOE shall receive reliable time stamp information from an external NTP server
OE. Prevention of TSF data export and damage during transmission	The TOE shall protect the data being transmitted between the components of the TOE from being exported, modified, or deleted by using an SSL VPN provided by the .NET Framework and the Apache HTTP Server in its operational environment
OE. Protection of web	The TOE shall protect the sensitive data sent by the web

client's sensitive data	client or stored in the web server from being exported or corrupted by using the HTTPS web service provided by the web server
OE. Blocking of external remote access	In order to block remote access to the TOE from the external network, the authorized administrator shall establish an access control policy of the firewall and the intrusion prevention system that protect the network in which the TOE is installed and operated
OE. Direct	The TOE and the CLI console shall be connected directly through a serial port

[Table 12] Security Objectives for the Operational Environment

4.3 Security Objectives Rationale

The following is the rationale for the security objectives:

1) Rationale for the security objectives for the TOE

Security objectives for the TOE / Security problem	O. Blocking abnormal data transfer	O. Prevention of web server access control bypass	O. Identification and authentication	O. Prevention of stored TSF data damage	O. Restriction of excessive resource usage	O. Prevention of personal information import and export	O. Audit	O. Management
T. Abnormal data import	X							
T. Web server access control bypass		X						
T. CSRF attacks	X							
T. Administrator masquerade			X					
T. Stored TSF data damage				X				
T. Record failure							X	

Security objectives for the TOE / Security problem	O. Blocking abnormal data transfer	O. Prevention of web server access control bypass	O. Identification and authentication	O. Prevention of stored TSF data damage	O. Restriction of excessive resource usage	O. Prevention of personal information import and export	O. Audit	O. Management
T. DoS attacks					X			
T. Consecutive authentication attempts			X					
T. Personal information import and export						X		
P. Audit							X	
P. Secure management								X

[Table 13] Tracing between the Security Objectives for the TOE and the Security Problem Definition

O. Blocking abnormal data transfer

This security objective ensures that the TOE analyzes the HTTP/HTTPS request messages sent by the web client and the HTTP/HTTPS response messages sent by the web server and blocks abnormal data importation to the web server, thereby preventing export or damage of the data stored in the web server. Therefore, this security objective counters the threat “T. Abnormal data import.”

Furthermore, it ensures that the TOE detects intercepted and corrupted HTTP request messages through the anlyasis of the HTTP/HTTPS messages, thereby preventing export or damage of the important information of the web server. Therefore, this security objective counters the threat “T. CSRF attacks.”

O. Prevention of web server access control bypass

This security objective ensures that the TOE blocks a web client’s access to URLs that are not allowed, which makes it impossible for an unauthorized user to bypass the web server access control policy and access its services or resources. Therefore, this security objective counters the threat “T. Webserver access control bypass.”

O. Identification and authentication

This security objective ensures that the TOE gives access only to the authorized administrators through the identification and authentication process, which blocks attempts to masquerade as an authorized administrator attempting to reuse authentication data and modify the information flow control policy of the TOE. Therefore, this security objective counters the threat “T. Administrator masquerade.”

Furthermore, as the identification and authentication function provided by the TOE can handle the case of consecutive authentication failures of an administrator, this security objective ensures that the threat agent cannot access the TOE through consecutive authentication attempts. Therefore, this security objective counters the threat “T. Consecutive authentication attempts.”

O. Prevention of stored TSF data damage

This security objective ensures that the integrity of the TSF data will be checked during initial start-up of the Detection Engine or periodically during its normal operation to make sure that TSF data is not modulated, forged, or deleted. Therefore, this security objective counters the threat “T. Stored TSF data damage.”

O. Restriction of excessive resource usage

This security objective ensures that the TOE supports a normal service of the web server by blocking web server access of users who excessively overuses the network resources. Therefore, this security objective counters the threat “T. DoS attacks.”

O. Prevention of personal information import and export

This security objective ensures that the TOE prevents unintended import/export of personal information to/from the web server by either blocking information flow or masking the personal information. Therefore, this security objective counters the threat “T. Personal information import and export.”

O. Audit

This security objective ensures that the TOE generates an audit record of the security-relevant events, securely stores the records, and provides a means for the authorized administrator to review the recorded data. Therefore, this security objective enforces the OSP “P. Audit.”

Furthermore, this security objective ensures that the TOE prevents audit data storage

exhaustion that may impede the generation of audit data and ensures accountability for security related actions. Therefore, this security objective counters the threat “T. Record failure.”

O. Management

This security objective ensures that the TOE provides the authorized administrator with a means to manage the TOE effectively. Therefore, this security objective contributes to the enforcement of the OSP “P. Secure management.”

2) Rationale for the security objectives for the operational environment

Security objectives for the operational environment / Security problem	OE. Physical	OE. Manage	OE. Noevil	OE. Secure management	OE. Secure database	OE. Sole connection point	OE. Time synchronization via NTP server	OE. Prevention of TSF data export and damage during transmission	OE. Protection of web client's sensitive data	OE. Blocking of external remote access	OE. Direct
T. TSF data export and damage during transmission								X			
T. Stored TSF data damage					X						
T. Web client's sensitive data export and corruption									X		
A. Physical	X			X							
A. Manage		X									
A. Noevil			X								
A. Secure database					X						
A. Sole connection point						X					
A. Direct											X
P. Audit							X				
P. Secure management			X	X							

Security objectives for the operational environment / Security problem	OE. Physical	OE. Manage	OE. Noevil	OE. Secure management	OE. Secure database	OE. Sole connection point	OE. Time synchronization via NTP server	OE. Prevention of TSF data export and damage during transmission	OE. Protection of web client's sensitive data	OE. Blocking of external remote access	OE. Direct
P. Blocking of external remote access										X	

[Table 14] Tracing between the Security Objectives for the Operational Environment and the Security Problem Definition

OE. Physical

This security objective assures that the TOE is installed and operated in a physically secure place and protected against external attacks and attempts to modify the TOE. Therefore, this security objective upholds the assumption "A. Physical."

OE. Manage

This security objective ensures that the authorized administrator performs the latest security update of the TOE S/W platform (e.g. operating system, web browser) and, when changing the network configuration, keeps the TOE operational environment to be consistent with the security policy. Therefore, this security objective upholds the assumption "A. Management."

OE. Noevil

This security objective ensures that the TOE is managed in a secure manner by an authorized administrator that is appropriately trained and follows the administrator guidance. Therefore, this security objective upholds the assumption "A. No-evil" and contributes to the enforcement of the OSP "P. Secure management."

OE. Secure management

This security objective ensures that the TOE is delivered and installed in a secure way

and is configured, managed, and used by the authorized administrator in a secure manner. Therefore, this security objective upholds the assumption “A. Physical” and enforces the OSP “P. Secure management.”

OE. Secure database

This security objective ensures that the database of the TOE operates stably and is securely configured and managed, thereby assuring the security of the data stored in it. Therefore, this security objective upholds the assumption “A. Secure database” and counters the threat “T. Stored TSF data damage.”

OE. Sole connection point

This security objective ensures that the TOE is set and operated in an internal network with a firewall and intrusion prevention system. It is securely protected from external intrusion, and the firewall and intrusion prevention system send sorted web traffic within imported traffic from an external network to the TOE. Therefore, this security objective upholds the assumption “A. Sole connection point.”

OE. Time synchronization via NTP server

This security objective ensures that the TOE receives reliable time stamps from the external NTP server in order to accurately record the security-relevant events. Therefore, this security objective contributes to the enforcement of the OSP “P. Audit.”

OE. Prevention of TSF data export and damage during transmission

This security objective ensures that the important data being transmitted between the components of the TOE are not exported, modified, or deleted by malicious attackers as the transmission is processed through the encryption library provided by the operational environment of the TOE. Therefore, this security objective counters the threat “T. TSF data export and damage during transmission.”

OE. Protection of web client’s sensitive data

This security objective ensures that the sensitive data sent by the web client or stored in the web server is not exported or corrupted as the HTTPS web service is provided by the web server. Therefore, this security objective counters the threat “T. Web client’s sensitive data export and corruption.”

OE. Blocking of external remote access

This security objective ensures that the authorized administrator establishes an access control policy of the firewall and the intrusion prevention system to protect the network in which the TOE is installed and operated so that remote access to the TOE from the external network can be blocked. Therefore, this security objective enforces the OSP “P. Blocking of external remote access.”

OE. Direct

This security object ensures that the TOE and the CLI console are connected directly via a serial port. Therefore, this security objective upholds the assumption “A. Direct.”

5. Extended Components Definition

This ST does not need to define extended components as there are no extended requirements in it.

6. Security Requirements

This chapter describes the functions and the assuarance requriments to be satisfied by the TOE.

6.1 TOE Security Function Requirements

In order to meet all security objectives identified in chapter 4, the security functional requirements defined in this ST selected and represented the related functional components from the extended components of chapter 5 and CC Part 2. The following [Table 15] shows a summary of the security functional components used in this ST:

Class	Security Function Components	
Security audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3(1)	Selectable audit review (1)
	FAU_SAR.3(2)	Selectable audit review (2)
	FAU_SEL.1	Selective audit
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition (1)
	FIA_ATD.1(2)	User attribute definition (2)
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action

Class	Security Function Components	
Security management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TSF protection	FPT_TST.1	TSF testing
TOE access	FTP_SSL.1	TSF-initiated session locking

[Table 15] Security Function Requirements

1) Security audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 TSF shall take [the counteractions of Table 16] upon detection of a potential security violation.

Potential Security Violation Events	Security Alert Countermeasures
If the availability of the audit trail storage reached the threshold	• Outputs a warning page to the Remote administrator • Sends an alarm mail to the appointed email address
If the audit trail storage has reached saturation	• Outputs a warning page to the Remote administrator • Sends an alarm mail to the appointed email address
If the web client's IP address is updated onto the access block list according to the WEBCLIENT SFP	Outputs a warning page to the Remote administrator

[Table 16] Security Alarms Counteractions by Potential Security Violation Events

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *minimum* level of audit; and

c) [Successful identification and authentication of Remote administrator, remote administrator logout, successful identification and authentication of local administrator, local administrator logout, successful audit data query, and automatic update of access block list through WEBCLIENT SFP].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Data and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [Additional Information in audit record of Table 17].

Requirements	Audit Events Prompted by Requirements	Additional Information in Audit Records
FAU_ARP.1	Counteractions taken due to potential security violations	(none)
FAU_GEN.1	(none)	(none)
FAU_GEN.2	(none)	(none)
FAU_SAA.1	Automatic response to the operation start and stop of the analysis mechanism	(none)
FAU_SAR.1	(none)	(none)
FAU_SAR.3(1)	(none)	(none)
FAU_SAR.3(2)	(none)	(none)
FAU_SEL.1	Audit configuration changes that occur during the operation of audit collection function	(none)
FAU_STG.3	Counteractions taken when the	(none)

Requirements	Audit Events Prompted by Requirements	Additional Information in Audit Records
	threshold is exceeded	
FAU_STG.4	Counteractions taken when the audit saving fails	(none)
FDP_ACC.1	(none)	(none)
FDP_ACF.1	Successful requests of the operation in regards to the object handled by SFP	(none)
FDP_IFC.1	(none)	(none)
FDP_IFF.1	Decision to permit the requested information flow	- URI: Detected URI information - Risk: Risk of each detection rule - Detection rule ID: Identifier of detected rule
FIA_AFL.1	Reaching of the limit of failed authentication attempts and the counteractions taken	(none)
FIA_ATD.1(1)	(none)	(none)
FIA_ATD.1(2)	(none)	(none)
FIA_SOS.1	Refusal of all tested confidential information by the TSF	(none)
FIA_UAU.2	Authentication mechanism usage failure	(none)
FIA_UAU.7	(none)	(none)
FIA_UID.2	User identification mechanism usage failure including the provided user identity	(none)
FMT_MOF.1	(none)	(none)
FMT_MSA.1	All changes to the security attribute value	(none)
FMT_MSA.3	(none)	(none)
FMT_MTD.1	All changes to the TSF data value	(none)
FMT_SMF.1	Use of management functions	(none)
FMT_SMR.1	Changes to the user group that divides roles	(none)
FPT_ITT.1	(none)	(none)
FPT_TST.1	Fulfillment of the TSF self-test and the test results	(none)
FTA_SSL.1	Locking of an interactive session due	(none)

Requirements	Audit Events Prompted by Requirements	Additional Information in Audit Records
	to the session lock mechanism	

[Table 17] Auditable Events

FAU_GEN.2 User identify association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.2 User identification before any action

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.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

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 [FAU_STG.3 Counteractions taken when the threshold is exceeded, and FAU_STG.4 Counteractions taken when the audit saving fails] known to indicate a potential security violation;

b) [In a case the HTTP/HTTPS connection of a web client exceeds the threshold set by the Remote administrator due to WEBCLIENT SFP, and thereby registering the IP address of the web client on the access block list].

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [Remote administrator] with the capability to read [all audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for **Remote administrator** to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

FAU_SAR.3 (1) Selectable audit review (1)

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [search] of **Audit log** based on [AND of following clauses].

a) Processing time for Audit log

b) Type of Audit log

Application Note: The events for audit by the type of audit data are the criteria for search of an Audit log as shown in [Table 29].

FAU_SAR.3 (2) Selectable audit review (2)

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [search, sort] of **Detection log** based on [AND of the criteria for Search in Table 18 and OR of the criteria for Sort in Table 18].

Criteria	Ability
Time (user-defined), source IP address, URL, nationality, website	Search
Time (Last 5 minutes, 1 hour, 1 day, 1 week, 1 month, or 1 year), rule name (25 detection rules including buffer overflow), log state	Sort

[Table 18] Selectable Detection Log Review

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) *event type*

b) [None]

Application Notes: The group of event types used in this security functional requirement is defined in [Table 19].

Event Type	Auditable Events
Basic	- Start-up and shut-down of the audit functions - Actions taken due to exceeding of a threshold - Actions taken due to the audit storage failure - Modifications to the values of TSF data (e.g. website information, protected web server information, Management Console connection IP, Remote administrator ID/password, and time synchronization server information) - All modifications of the values of security attributes - Actions taken due to potential security violations - Execution of TSF self tests and the results of the tests (fail) - Unsuccessful use of the authentication mechanism - Unsuccessful use of the user identification mechanism, including the user identity provided - Locking of an interactive session by the session locking mechanism

[Table 19] Auditable Events by the Group of Event Types

FAU_STG.3 Actions in case of possible audit data loss

Hierarchical to: No other components.
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [output a warning page to the Remote administrator and notifies an alarm mail to the appointed email] if the audit trail exceeds [90% of the overall audit trail storage].

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Actions in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [output a warning page to the administrator and notify an alarm mail to appointed email address] if the audit trail is full.

2) User data protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 TSF shall enforce the [WEBCLIENT SFP] on [

a) Subject : Web client

b) Object : Webserver

c) Operation: HTTP/HTTPS connection request].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

a) Subject : Web client

b) Subject attributes :
   - IP address
   - IP address range
   - Traffic delay time
   - Import time of delayed traffic
   - Import frequency of delayed traffic

c) Object : Webserver

d) Object attributes:
   - IP address
   - Port].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Allow if all of the following rules are satisfied

a) If the web client's IP address or the IP address range that requested the HTTP/HTTPS connection to webserver is not included in the access block list.

b) If the IP address and port of the requested webserver included the HTTP/HTTPS connection to the target of protection webserver].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no explicit authorization rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [About the web client's HTTP/HTTPS connection request that is allowed by FDP_ACF.1.2

a) If the traffic delay time, the import time of delayed traffic, and the import frequency of delayed traffic exceeds the administrator set threshold, the TSF updates the web client's IP address on the access block list and blocks access].

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [WEB SFP] on [

a) Subject:
- A web client requesting the services of a webserver
- A webserver responding to the requests of a web client

b) Information: HTTP request message or HTTP response message

c) Operation: request/response HTTP/HTTPS pass information].

FDP_IFF.1 Simple security attributes

Hierarchical to: 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 [WEB SFP] based on the following types of subject and information security attributes: [

a) Subject: Web client or webserver

b) Subject properties: Web client's IP address

c) Information: HTTP request message or HTTP response message

d) Information properties :
- HTTP request message
  - ✓ URL
  - ✓ Cookie
  - ✓ Method
  - ✓ User Agent
  - ✓ From
  - ✓ Accept
  - ✓ HOST
  - ✓ Contents-type
- HTTP response message
  - ✓ Response status code
  - ✓ Web directory information].

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) The TSF shall allow when the security attribute value that is defined in FDP_IFF.1.1 within the HTTP request/response message does not match the character string information set by the Remote administrator.

b) The TSF shall allow when the URL value within the HTTP request message and the web client's IP address match the URL access allow list set by the Remote administrator].

FDP_IFF.1.3 The TSF shall enforce the [

a) Blockage if the URL length, the key length, and the header length within the HTTP request messages exceeds the Remote administrator set values.

b) Blockage if the field information within the HTTP request/response messages does not match the standard field information of HTTP 1.1 protocol.

c) Blockage if the information within the HTTP request/response messages matches the information (character string or personal information) set by the Remote administrator.

d) Updating the IP address onto the access block list and block if the accumulated risk of the identical IP address exceeds the threshold within the time set by the Remote administrator].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [no explicit authorization rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [no explicit deny rules].

3) Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.2 User authentication before any actions

FIA_AFL.1.1 The TSF shall detect when *[5]* unsuccessful authentication attempts occur related to [authentication of an administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*,

the TSF shall [lock the administrator account for 10 minutes].

FIA_ATD.1 (1) User attribute definition (1)

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to Remote administrator : [Password, security-relevant roles (see FMT_SMR.1)].

FIA_ATD.1 (2) User attribute definition (2)

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to Local administrator : [Password, security-relevant roles (see FMT_SMR.1)].

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following allowed criteria].

- Include 1 or more alphabet letters, numbers, and special characters (*~!@#$%()-=+;|₩.,<>/?), each;
- More than 9 letters but less than 15 letters;
- No more than 3 letters in an ascending or a descending pattern; and
- No repeating characters of 3 or more letters.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.2 User authentication before any action

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.
Dependencies: FIA_UAU.2 User authentication before any action

FIA_UAU.7.1 The TSF shall provide only [the authentication success or failure message and the passwords indicated by '*' or "" mark (blank) instead of the original characters] to the administrator while the authentication is in progress.

FIA_UID.2 User identification before any actions

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of that administrator.

4) Security management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: 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 [such as the following list of functions] to [the following roles].

Security Functions	Actions	Authorized Roles
Session lock setting	Determine the behaviour	Operator
Audit level setting	Determine the behaviour	Operator
Detection level setting of each WEB SFP	Determine the behaviour	Operator Website administrator
Setting of access block list management method (automatic or manual)	Determine the behaviour	Operator

[Table 20] Security Function Management List

FMT_MSA.1 Management of security attributes

Hierarchical to: 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 [WEBCLIENT SFP, WEB SFP] to restrict the ability to *query, modify, delete, [create]* the security attributes [of the following Table 22] to [the Operator and Website administrator].

SFP	Security Features	Authorized Roles	Operations
WEBCLIENT SFP access block list	· IP address · IP address range · Traffic delay time · Import time of delayed traffic · Import frequency of delayed traffic	Operator, Website-administrator	Query, modify, delete, create
WEBCLIENT SFP's target of protection webserver list	· IP address · Port	Operator	Query, modify, delete, create
Information flow block or allow list of WEB SFP	· URI, Cookie, Method, User Agent, From, Accept, HOST, Contents-type, Response status code, Web directory information	Operator, Website-administrator	Query, modify, delete, create

[Table 21] Security Attributes Related to Security Policy

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [WEBCLIENT SFP, WEB SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Operator and Website administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: 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, modify, delete, [create]* the [TSF data of Table 23] to [the authorized administrators of each TSF data of Table 23].

TSF Data	Actions	Authorized Roles
Remote administrator ID and password	Query, modify, delete, create	Operator
	Query, modify	Website administrator
Management Console connection IP	Query, modify, create	Local administrator
Security alert email address	Query, modify, delete	Operator
Local administrator password	Modify	Local administrator
Personal information	Query, modify, delete, create	Operator Website administrator
Statistic data	Query	Operator Website administrator Inquirer
Website information	Query, modify, delete, create	Operator
Information of the target of protection webserver	Query, modify, delete, create	Operator
Information of the time initialisation server	Query, modify, delete, create	Operator
Information of the current state of the system (Network port, traffic, resources, webserver and other current state information)	Query	Operator

[Table 22] TSF Data List

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [accumulated risk] to [the Operator].

FMT_MTD.2.2 The TSF shall take the following actions, if the accumulated risk is at, or exceed, the indicated limits: [registration of the web client's IP address on the access block list].

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 TSF shall be capable of performing the following management functions: [management of security functions behavior, management of security attributes, and management of TSF data].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.2 User Identification before any actions

FMT_SMR.1.1 The TSF shall maintain the roles [such as the following authorized identified roles].

Classifications		Roles
Remote administrator	Operator	The authorized administrator with all the authorities
	Website administrator	The administrator for the assigned website operation and management
	Inquirer	The administrator who is able to modify his/her own password, and view the Detection log and the audit data
Local administrator		The administrator for CLI network configuration setting

[Table 23] Administrator Classification

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

5) TSF Protection

FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of *[TSF provided by the Detection Engine]*.

FPT_TST.1.2 The TSF shall provide Operator with the capability to verify the integrity of *[Detection Engine configuration file]*.

FPT_TST.1.3 The TSF shall provide Operator with the capability to verify the integrity of *[Detection Engine execution file]*.

6) TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components.
Dependencies: FIA_UAU.2 User authentication before any actions

FTA_SSL.1.1 The TSF shall lock an interactive session after [inactive time period set by a Remote administrator] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [re-authentication of a Remote administrator].

6.2 TOE Assurance Requirements

The assurance requirements of this ST are composed of the assurance components of the CC, Part 3 of, the assurance level being EAL4. The table below shows a summary of assurance components:

Assurance Class	Assurance Components	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objective
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representations of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operation user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independence testing - sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

[Table 24] TOE Assurance Requirements

1) Security target

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summaries the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide the conformance claims.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security

requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives. ASE_OBJ.2.2D The developer shall provide a security objective rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives

for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirement rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

2) Development

ADV_ARC.1 Security architecture guidance

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_IMP.1 Implementation representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design
ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification.

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all

subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

3) Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies: No Dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

4) Life cycle support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies: ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce and provide development security documentation.

Content and presentation elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all

requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

Content and presentation elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5) Tests

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Basic design test

Dependencies: ADV_ARC.1 Security architecture guidance
ADV_TDS.2 Architectural design

ATE_FUN.1 Functional test

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independence test - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6) Vulnerability assessment

AVA_VAN.3 Focused vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.4 Complete functional specification

ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_DPT.1 Testing: basic design

Developer action elements:

AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.3.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator shall perform an independent, focused vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6.3 Rationale for Security Requirements

1) The rationale for security functional requirements

TOE Security Objectives / Security Functional Requirements	O. Audit	O. Management	O. Identification and authentication	O. Blocking of abnormal data transfer	O. Prevention of web server access control bypass	O. Restriction of excessive resource usage	O. Prevention of stored TSF data damage	O. Prevention of personal information import and export
FAU_ARP.1	X							
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_SAA.1	X							
FAU_SAR.1	X							
FAU_SAR.2								
FAU_SAR.3(1)	X							
FAU_SAR.3(2)	X							
FAU_SEL.1	X							
FAU_STG.3	X							
FAU_STG.4	X							
FDP_ACC.1				X		X		
FDP_ACF.1				X		X		
FDP_IFC.1				X	X			X
FDP_IFF.1				X	X			X
FIA_AFL.1			X					
FIA_ATD.1(1)			X					
FIA_ATD.1(2)			X					
FIA_SOS.1			X					
FIA_UAU.2			X					
FIA_UAU.7			X					
FIA_UID.2			X					
FMT_MOF.1		X						

TOE Security Objectives / Security Functional Requirements	O. Audit	O. Management	O. Identification and authentication	O. Blocking of abnormal data transfer	O. Prevention of web server access control bypass	O. Restriction of excessive resource usage	O. Prevention of stored TSF data damage	O. Prevention of personal information import and export
FMT_MSA.1		X						
FMT_MSA.3		X						
FMT_MTD.1		X						
FMT_MTD.2		X						
FMT_SMF.1		X						
FMT_SMR.1		X	X					
FPT_TST.1							X	
FTP_SSL.1			X					

[Table 25] Response to Security Objectives and Security Functional Requirements

FAU_ARP.1 Security alarms

This component enables the tracing of the accountability of security related actions as it outputs a warning page to the authorized administrator or notifies an alarm mail to the appointed email address when potential security violations are detected by the FAU_SAA.1. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_GEN.1 Audit data generation

This component enables the tracing of the accountability of security related actions as it records the audit function start-up and shut-down, the Remote administrator logout, and all events for audit by the minimum audit level with the information such as date and time of the event and the subject identity in the audit record. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_GEN.2 User identity association

This component enables the tracing of the accountability of security related actions as it generates an audit data in terms that the audit event that occurred from the user’s actions is able to associate with the identity of the user who caused the audit event and the event for audit. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_SAA.1 Potential violation analysis

This component enables the tracing of the accountability of security related actions as it is able to indicate the potential security violations by applying the rules on the basis of the audited events by the FAU_GEN.1. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_SAR.1 Audit review

This component provides the authorized administrator with the measures to review the recorded audit data as it provides the Remote administrator with all audited events by the FAU_GEN.1 in a form that it may be easily interpreted. Therefore, this component satisfies the security objective, “O. Audit.”

FAU_SAR.2 Restricted audit review

This component provides the authorized administrator with the measures to review the recorded audit data as it assures the ability to review audit records only to the Remote administrator. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_SAR.3 (1) Selectable audit review (1)

This component provides the authorized administrator with the measures to review the recorded audit data as it assures the ability to search an Audit log through the association of its processing period and the type of AND. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_SAR.3 (2) Selectable audit review (2)

This component provides the authorized administrator with the measures to review the recorded audit data as it assures the ability to search a Detection log through the association of date and time of the event and AND of the subject’s identity and the ability to sort a Detection log through the association of the type of event or OR of the subject’s identity. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_SEL.1 Selective audit

This component assures the ability to record the security-relevant events as it is able to select a set of events that shall be audited among the events for audit defined by the FAU_GEN.1 according to the group of event types that is classified into a whole audit and a basic audit. Therefore, this component satisfies the security objective, “O. Audit”.

FAU_STG.3 Action in case of possible audit data loss

This component prevents the audit data loss as it outputs a warning page to the

administrator and notifies an alarm mail to the appointed email address if the audit trail storage in which an Audit log and a Detection log are saved is reaches 90% of the whole capacity. Therefore, this component satisfies the security objective, “O. Audit.”

FAU_STG.4 Prevention of audit data loss

This component prevents the audit data loss as it overwrites the oldest audit record to secure the available capacity if the audit trail storage is saturated in which an Audit log and a Detection log are saved. Therefore, this component satisfies the security objective, “O. Audit”.

FDP_ACC.1 Subset access control

This component blocks the import of abnormal data to the webserver through the sectional access control between the web client and the webserver as it compels WEBCLIENT SFP when requesting the HTTP/HTTPS connection from web client to webserver. Therefore, this component satisfies the security objective, “O. Blocking of abnormal data transfer”.

Furthermore, this component satisfies the security objective, “O. Restriction of excessive resource usage” as the compelled WEBCLIENT SFP, when requesting the HTTP/HTTPS connection from web client to webserver, controls the access of a web client that abnormally overuse the resources of webserver.

FDP_ACF.1 Security attribute based access control

This component blocks the import of abnormal data to the webserver through the access control rule based on the security attributes between the web client and the webserver as it compels WEBCLIENT SFP by using the web client and webserver’s security attributes such as the IP address and IP block time when requesting the HTTP/HTTPS connection from web client to webserver. Therefore, this component satisfies the security objective, “O. Blocking of abnormal data transfer”.

Furthermore, when the access allowed HTTP/HTTPS connection request from the web client to the webserver exceeds the Remote administrator set threshold of traffic delay time, the import time of delayed traffic, and the import frequency of delayed traffic, this component enlists the corresponding web client’s IP address on the access block list to control the access of a web client that abnormally overuses the webserver’s resources. Therefore, this component satisfies the security objective, “O. Restriction of excessive resource usage”.

FDP_IFC.1 Subset information flow control

This component blocks the import of abnormal data to the webserver through the

sectional information flow control between the web client and the webserver as it compels WEBCLIENT SFP when sending the HTTP request message of which the web client has the pass information or the HTTP response message of which the webserver has the pass information. Therefore, this component satisfies the security objective, “O. Blocking of abnormal data transfer”.

Furthermore, this component satisfies the security objective “O. Prevention of web server access control bypass” as it only allows web client’s access to authorized URL when compelling WEB SFP.

Moreover, this component satisfies the security objective “O. Prevention of personal information import and export” as it controls the HTTP request/response or the file upload to prevent the import or export of unintended personal information into the webserver when compelling WEB SFP.

FDP_IFF.1 Simple security attributes

This component blocks the import of abnormal data to the webserver through the access control rule based on the security attributes between the web client and the webserver as it compels WEBCLIENT SFP by using the web client’s IP address security attributes, the security attributes such as URL, cookie, method, etc. of the HTTP request message, and the security attributes such as response status code, web directory information, etc. of the HTTP response message. Therefore, this component satisfies the security objective, “O. Blocking of abnormal data transfer”.

Furthermore, this component prevents the web client from bypassing the access control policy of the webserver by allowing the information flow of the corresponding HTTP request message in case the web client’s IP address and the URL value within the HTTP request message matches the access allow list. Therefore, this component satisfies the security objective, “O. Prevention of web server access control bypass”.

Moreover, this component prevents the import into or the export from the webserver when Remote administrator-set personal information is included in security attributes within the HTTP request/response messages by interpreting it as the unintended personal information. Therefore, this component satisfies the security objective, “O. Prevention of personal information import and export”.

FIA_AFL.1 Authentication failure handling

When the authentication fails for 5 times consecutively, this component locks the corresponding administrator’s account for 10 minutes to block the consecutive authentication attempts of a exploit attacker and only allows authorized administrator to access TOE. Therefore, this component satisfies the security objective, “O. Identification

and authentication".

FIA_ATD.1 (1) User attribute definition (1)

As this component assures the ability to maintain the security attribute list of a Remote administrator, the TOE allows only the authorized administrator to access the TOE through the identification and authentication. Therefore, this component satisfies the security objective, "O. Identification and authentication".

FIA_ATD.1 (2) User attribute definition (2)

As this component assures the ability to maintain the security attribute list of a Local administrator, the TOE allows only the authorized administrator to access the TOE through the identification and authentication. Therefore, this component satisfies the security objective, "O. Identification and authentication".

FIA_SOS.1 Verification of secrets

This component mitigates the unauthorized access attempts of a exploit attacker and only allows the authorized administrator to access the TOE as it provides a mechanism that satisfies a password (confidential information) used as security attributes of the Remote administrator and the Local administrator. Therefore, this component satisfies the security objective, "O. Identification and authentication".

FIA_UAU.2 User authentication before any action

Only the administrator authorized by the identification and authentication is able to access the TOE as this component assures the prohibition of any sort of TSF arbitrated actions until the successful authentication of administrator. Therefore, this component satisfies the security objective, "O. Identification and authentication".

FIA_UAU.7 Protected authentication feedback

The authentication feedback information may not be exploited by attacks such as the authentication data reuse, as this component assures only the provision of authentication success or failure messages or masking-done password to the administrator during the authentication process. Therefore, this component satisfies the security objective, "O. Identification and authentication".

FIA_UID.2 User identification before any action

Only the authorized administrator may access the TOE as this component assures no provision of any action on behalf of a Remote administrator and a Local administrator before an identification of the authorized users. Therefore, this component satisfies the security objective, "O. Identification and authentication".

FMT_MOF.1 Management of security functions behaviour

This component provides a way the authorized administrator to effectively manage the TOE as it assures that an Operator may determine the actions of security functions such as the session lock setting, the audit level setting, and the detect level setting according to each web security policy and assures that the Website administrator may determine the detection level setting and the actions of security function by the web security policy. Therefore, this component satisfies the security objective, “O. Management”.

FMT_MSA.1 Management of security attributes

This component is necessary to provide a means to the authorized administrator to effectively manage the TOE as it assures that necessary security attribute data for WEBCLIENT SFP and WEB SFP are queried, corrupted and deleted by the Operator or the Website administrator. Therefore, this component satisfies the security objective, “O. Management”.

FMT_MSA.3 Static attribute initialisation

This component is necessary to provide a means to the authorized administrator to effectively manage the TOE as it assures a default value of the negative model-based security attribute that is used by WEBCLIENT SFP and WEB SFP and the authorized administrator may changeover to the optional initial value. Therefore, this component satisfies the security objective, “O. Management”.

FMT_MTD.1 Management of TSF data

This component is necessary to provide a means to the authorized administrator to effectively manage the TOE as it assures that the TSF data is queried, modified, deleted and created by the authorized administrator. Therefore, this component satisfies the security objective, “O. Management”.

FMT_MTD.2 Management of limits on TSF data

This component is necessary to provide a means to effectively manage the TOE as it assures the restriction of an Operator to specify the limits to accumulated risk within the TSF data, and once the set limit is reached or exceeded, automatically updates web client’s IP address onto the access block list. Therefore, this component satisfies the security objective, “O. Management”.

FMT_SMF.1 Specification of management functions

This component is necessary to provide a means to effectively manage the TOE as it assures that the TSF may perform the management functions such as the management of security functions behavior, the management of security attributes, and the

management of TSF data. Therefore, this component satisfies the security objective, “O. Management”.

FMT_SMR.1 Security roles

This component assures that only the authorized administrator may access the TOE by classifying the security roles into a Remote administrator (Operator, Website administrator, and Inquirer) and a Local administrator. Therefore this component satisfies a security objective “O. Identification and authentication”.

Furthermore, by classifying the authorities of security management that may be operated by each security role, this component provides a means to effectively manage the TOE. Therefore, this component satisfies the security objective, “O. Management”

FPT_TST.1 TSF testing

This component assures that the TSF data are not changed or deleted without permission by periodically checking for normality of the Detection Engine’s process, forgery of the configuration file and the execution file during the start-up and the normal operation period. Therefore, this component satisfies the security objective, “O. Prevention of stored TSF data damage”.

FTA_SSL.1 TSF-initiated session locking

This component guarantees that only the authorized administrator may access the TOE as it locks the administrator session when the non-active Remote administrator desires to reuse the locked session and demands a re-authentication of the identical Remote administrator. Therefore, this component satisfies the security objective, “O. Identification and authentication”.

2) Rationale for security assurance requirements

This security target’s evaluation assurance level was selected as EAL4 with a consideration of the asset value protected by the TOE and the threat level.

The TOE is set and operated in the following environments where assurance at EAL4 level can be sufficiently provided; physically safe (OE. Physical), where latest security update of TOE S/W platform and TOE operational environment/security policy is maintained consistently (OE. Manage), can trust administrators (OE. No-evil), TOE is securely managed (OE. Secure management), the database that TOE use is securely configured and managed (OE. Secure database), firewall is operated to allow the imported web traffics to be sent to a web server by passing through TOE (OE. Sole connection point), receive a trusted time stamp through external NTP server (OE. Time synchronization via NTP server),

prevents export and damage to data transmitted within TOE elements (OE. Prevention of TSF data export and damage during transmission), protects export and modification of sensitive data of web client (OE. Protection of web client's sensitive data), the internal network where TOE is set and operated is securely protected by a firewall and intrusion prevention system (OE. Blocking of external remote access), and TOE and CLI console is connected directly (OE. Direct). These operations assume that they imply the attackers with Enhanced-Basic level of attack potential.

Therefore selecting EAL4 which provides an assurance necessary for responding to Enhanced-Basic level of attack potential as an evaluation assurance level is appropriate for this ST.

6.4 Rationale for Dependencies

1) The functional components deigned in this security target are as shown in [Table 26].

Number	Functional Components	Dependency	Reference Number
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	-
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.2	2 22
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.2	FAU_SAR.1	5
7	FAU_SAR.3(1)	FAU_SAR.1	5
8	FAU_SAR.3(2)	FAU_SAR.1	5
9	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	2 26
10	FAU_STG.3	FAU_STG.1	-
11	FAU_STG.4	FAU_STG.1	-
12	FDP_ACC.1	FDP_ACF.1	13
13	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	12 25
14	FDP_IFC.1	FDP_IFF.1	15
15	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	14 27

Number	Functional Components	Dependency	Reference Number
16	FIA_AFL.1	FIA_UAU.2	20
17	FIA_ATD.1(1)	-	-
18	FIA_ATD.1(2)	-	-
19	FIA_SOS.1	-	-
20	FIA_UAU.2	FIA_UID.2	22
21	FIA_UAU.7	FIA_UAU.2	20
22	FIA_UID.2	-	-
23	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	28 29
24	FMT_MSA.1	FDP_ACC.1 FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	12 14 28 29
25	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	24 29
26	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	28 29
27	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	26 29
28	FMT_SMF.1	-	-
29	FMT_SMR.1	FIA_UID.2	22
30	FPT_TST.1	-	-
31	FTA_SSL.1	FIA_UAU2	20

[Table 26] The Dependencies of Functional Components

- As the FAU_GEN.1 has the FPT_STM.1 as a dependency, the FPT_STM.1 shall be considered as the security function requirements, but due to the security objectives of operational environment, “OE. Time synchronization,” it receives the trusted time stamp from an external NTP server, the requirements of FPT_STM.1 are satisfied by the operational environment. Therefore, this security target does not define the requirements of FPT_STM.1.

- The FAU_GEN.2, the FIA_UAU.2, the FMT_SMR.1 should include the FIA_UID.1 as a dependency, but by an elaboration operation, the dependency has changed to the

FIA_UID.2. As this security target has derived the FIA_UID.2 which is a hierarchical to the FIA_UID.1 as a security functional requirement, the rationale for the FIA_UID.1's dependency is satisfied by the FIA_UID.2. Therefore this security target does not define the requirements of FIA_UID.1.

- The FIA_AFL.1, the FIA_UAU.7, the FTA_SSL.1 should include the FIA_UAU.1 as a dependency, but by an elaboration operation, the dependency has changed to FIA_UAU.2. As this security target has derived FIA_UAU.2 which is in hierarchical to FIA_UID.1 as a security function requirement, the rationale for FIA_UAU.1's dependency is satisfied by FIA_UAU.2. Therefore this security target does not define FIA_UAU.1's requirement.

- As the FAU_STG.3, the FAU_STG.4 has the FAU.STG.1 as a dependency, the FAU_STG.1 shall be considered as the security function requirement, but it acts stably and receives a safe composition/management support by the operational environment's security objective "OE. Secure database," FAU.STG.1's requirement is satisfied by operational environment. Therefore this security target does not define FAU_STG.1's requirement.

2) Dependency of Assurance Requirements

As the CC provided EAL4 level assurance package dependencies are satisfied, its rationale is omitted.

6.5 Rationale for Mutually Supportive Relationship and Internal Consistency

This rationale shows that a series of security requirements is mutually supportive and internally consistent.

In the "6.4.1) Dependencies of security functional requirements" and "6.4.2) Dependencies of security assurance requirements", the TOE analyzes the dependencies that rely on other security requirements in order to achieve a certain security objective as it is insufficient to just rely on one security requirement and provides an additional rationale if the dependencies are not satisfied for the support relationships between the security requirements.

In addition, the security functional requirements are mutually supportive to the TSF and internally consistent as follows, even if they do not have a dependency:

The limits to accumulated risk are specified by the Operator (FMT_MTD.2), and the TOE

enforces WEB SFP after automatically registering the web client's IP address that caused web traffic by exceeding the accumulated risk on the access block list (FDP_IFF.1). In case the IP address is automatically registered on the access control list by WEB SFP, the TOE indicates this as a potential violation (FAU_SAA.1). Thus, these security requirements are mutually supportive and internally consistent.

The personal information list protected by an Operator or a Website administrator is managed (FMT_MTD.1), and if the personal information managed by an Operator or a Website administrator is included in the HTTP request/response message delivered by a webserver or a web client is present, the information flow is blocked (FDP_IFF.1). Thus, these security requirements are mutually supportive and internally consistent.

The TOE shall maintain the list of security attributes of the Remote administrator and the Local administrator (FIA_ATD.1), and the ID and password which are the security attributes of the Remote administrator and the Local administrator are managed by the Operator, the website manager, and the Local administrator (FMT_MTD.1); the password shall be able to satisfy the formally defined mechanisms (FIA_SOS.1). Thus, these security requirements are mutually supportive and internally consistent.

7. TOE Summary Specification

This chapter summarizes how the security functional requirements operate as the security functions of the TOE.

7.1 Security Audit Functions

The TOE generates and stores audit data of the detection results of abnormal web traffic and the security-relevant events related to the TOE operation and provides the authorized Remote administrator with the option to query this audit data.

1) Audit data generation function

The audit data is generated either as a "Detection log," which stores the detection results of abnormal web traffic according to the detection rules set by the Operator and Website administrator, or an "Audit log," which stores the security management activities of an authorized administrator or security-relevant events of the TOE.

The detection engine detects a web attack among incoming web traffic, and generates and stores a Detection log of the results.

The Management Console collects the security management activities of the Remote administrator and the security-relevant events related to the TOE operation and sends them to the Detection Engine. Then the Detection Engine generates and stores an Audit log on the collections of audit events sent from the management console and the security-relevant events caused in the detection engine.

When storing the audit data, the Detection log and Audit log records information such as date and time of the event, event type, identity of the subject (an administrator ID and IP address of the Administrator PC for an Audit log, and a source IP address for a Detection log), and the outcome (success or failure) of the event within each audit record. The Detection log additionally records the URL and the accumulated risk.

Auditable Events	Function and Time of Generation
Start-up and shutdown of the audit function	- During start-up of the detection engine - During shutdown of the detection engine
Logout of a Remote administrator	During shut-down of Management Console
Actions taken due to potential security violations	- Audit trail protection function - 5 consecutive authentication failures of a

Auditable Events	Function and Time of Generation
	Remote administrator - When a particular IP is updated on the access block list by the network access control security function
Enabling and disabling any of the analysis mechanisms	During start-up and shutdown of the detection engine
All modifications to the audit configuration that occur while the audit collection functions are operating	When a modification to audit level occurs through the audit setting function
Actions taken due to exceeding a threshold	When the available capacity of the audit trail storage exceeds the threshold
Actions taken due to the audit storage failure	When the audit trail storage is saturated
Successful requests to perform an operation on an object covered by the SFP	The result of the operation performed according to the WEBCLIENT SFP
Decisions to permit requested information flows	The result of the operation performed according to the WEBCLIENT SFP
Reaching the threshold for the number of unsuccessful authentication attempts and the following actions	When 5 consecutive authentication failures of a Remote administrator (Operator, Website administrator, or Inquirer) and a Local administrator occur
Rejection by the TSF of any tested secret	When a password does not correspond to the generation rule
Unsuccessful use of the authentication mechanism	- In the case of a Remote administrator (Operator, Website administrator, or Inquirer) authentication failure - In the case of a Local administrator authentication failure
Unsuccessful use of the user identification mechanism, including the user identity provided	- In the case of a Remote administrator (Operator, Website administrator, or Inquirer) identification failure - In the case of a Local administrator identification failure
All modifications to the values of	When the values of security attributes or TSF

Auditable Events	Function and Time of Generation
security attributes	data are modified by the Remote administrator (Operator, Website administrator, or Inquirer) or the Local administrator
All modifications to the values of TSF data	When the TSF data is modified by the Remote administrator while performing the security management functions
Use of the management functions by the Remote administrator or the Local administrator	When the Remote administrator performs security management functions
Modifications to the group of Remote administrators that are part of a role	When the ID of an Operator, a Website administrator, or an Inquirer is added or deleted
Execution of the TSF self tests and the results of the tests	In the event of an integrity failure of the TSF executable files or setting files
Locking of an inactive session by the session locking mechanism	When the Remote administrator(Operator) is inactive during the specified period of time

[Table 27] Audit Log Generation Events

- FAU_GEN.1.1
- FAU_GEN.1.2
- FAU_GEN.2.1

The TOE can either audit all auditable events defined in FAU_GEN.1 or selectively audit the following auditable events according to the settings of the Operator.

Event Type	Auditable Events
Basic	- Start-up and shut-down of the audit functions - Actions taken due to exceeding a threshold - Actions taken due to the audit storage failure - Modifications to the values of TSF data (e.g. website information, protected web server information, Management Console connection IP, Remote administrator ID/password, and time synchronization server information) - All modifications of the values of security attributes - Actions taken due to potential security violations - Execution of TSF self tests and the results of the tests (fail)

Event Type	Auditable Events
	- Unsuccessful use of the authentication mechanism - Unsuccessful use of the user identification mechanism, including the user identity provided - Locking of an inactive session by the session locking mechanism

[Table 28] Auditable Events by Group of Event Types

- FAU_SEL.1.1

2) Security alarm function

When the storage capacity of the audit trail storage exceeds the threshold of possible auditing data loss or reaches the state of saturation, the detection engine identifies it as a potential security violation, then sends an alarm mail to the appointed email and generates a warning page through the Management Console.

- FAU_ARP.1.1
- FAU_SAA.1.1
- FAU_SAA.1.2(a)
- FAU_STG.3.1
- FAU_STG.4.1

When the access block list is automatically updated according to the WEBCLIENT SFP, the detection engine identifies it as a potential security violation and outputs a warning page through the Management Console.

- FAU_ARP.1.1
- FAU_SAA.1.1
- FAU_SAA.1.2(b)
- FDP_ACF.1.4
- FDP_IFF.1.3(d)

3) Audit data query function

The Remote administrator may query a Detection log and an Audit log through the management console.

An Audit log is provided as a list for each item and can be reviewed by the following query conditions:

- Time of generation of Audit log: Last 5 minutes, 1 hour, 1 day, 1 week, 1 month, 1

year, or user-defined

- Type of Audit log: Refer to the following table for the auditable events of each type

Type of Audit Log	Auditable Events
Login-related	Reaching a threshold of unsuccessful authentication attempts and the response action taken
	Rejection by the TSF of any tested secret
	Unsuccessful use of the authentication mechanism
	Unsuccessful use of the user identification mechanism, including the user identity provided
	Locking of an inactive session by the session locking mechanism
Modification of setting	All modifications to the audit configurations that occur while the audit collection functions are operating
	Use of the management functions
	Modifications to the group of users that are part of a role
WAPPLES system	Actions taken due to potential security violations
	Enabling and disabling of any of the analysis mechanisms or automated responses performed by the tool
	Failure of the TSF
Data-related	Actions taken due to exceeding of a threshold
	Actions taken due to the audit storage failure
Network interface	Failure of the TSF

[Table 29] Auditable Events by Types of Audit Log

The query conditions of a Detection log generated according to the WEBCLIENT SFP and WEB SFP are as follows:

- Website
- Time of generation of Detection log
- Other (source IP address, rule name, nationality, URL, whether to include a hidden log)

The Remote administrator is provided with a function to search or sort the Detection logs according to the query conditions as shown in the following table:

Condition	Function
Time (user-defined), source IP address, URL, nationality, website	Search
Time (Last 5 minutes, 1 hour, 1 day, 1 week, 1 month, or 1 year), rule name (25 detection rules including buffer overflow), log state	Sort

[Table 30] Detection Log Search and Sort Functions

The Audit log is provided through the command line interface (CLI) when the Local administrator wants to make a request for the audit data of network settings, or the authentication results for the TOE operation.

- FAU_SAR.1.1
- FAU_SAR.1.2
- FAU_SAR.2.1
- FAU_SAR.3(1)
- FAU_SAR.3(2)

4) Audit data protection function

Detection Engine prevents the loss of audit data by checking the capacity of the audit trail storage.

If the audit trail of the Detection log and Audit log reaches 90% of overall capacity, the management console notifies the Remote administrator through a warning page and the detection engine sends an alarm mail to the appointed email address.

- FAU_STG.3.1

The audit trail saturation refers to a status where the audit trail of the Detection log and Audit log have reached 95% of the overall capacity of the audit trail storage. If the storage is saturated, the management console notifies the Remote administrator through a warning page and the detection engine sends an alarm mail to the appointed email address and secures available memory capacity of theaudit trail storage by deleting the oldest audit data in 10% increments of the whole audit data.

- FAU_STG.4.1

7.2 User Data Protection Functions

The detection engine applies a network access control security function (WEBCLIENT SFP) and a web security function (WEB SFP) to the HTTP request and response messages transferred between the web client and web server.

It first applies the WEBCLIENT SFP to a connection request to the web server sent by a web client from the external network. At this stage, the Detection Engine blocks the connection request if the web client's IP address is registered on the access block list.. If it is not registered on the list, the detection engine checks whether or not the IP address and port of the web server are included on the list of web servers to be protected. Consequently if they are included on the list, the Detection Engine applies WEB SFP to the connection request, and if they are not included on the list, the Detection Engine sends the connection request to a destination (web server) without applying WEB SFP.

Among the WEB SFPs, the Invalid HTTP rule and URL Access Control rule, which are both based on a positive security model, are the first ones to be applied to a request that after applying the WEBCLIENT SFP. The Invalid HTTP rule performs a blocking action (set by the Remote administrator) if the request does not comply with HTTP standards; and the URL Access Control rule allows the request only when the requested URL is on the permitted list.

To a request that is allowed after applying Invalid HTTP rule and URL Access Control rule, the Detection Engine applies the following WEB SFP rules, which analyze a request message and perform detection and response actions: Buffer overflow, Cross Site Scripting, Cookie Poisoning, Extension Filtering, File Upload, Input Content Filtering, Include Injection, Invalid HTTP, Invalid URL, IP Filtering, Parameter Tampering, Privacy Input Filtering, Privacy File Filtering, Request Method Filtering, Request Header Filtering, SQL Injection, Stealth Commanding, Suspicious Access, URL Access Control, User Defined Pattern, and Unicode Directory Traversal.

The HTTP requests that pass through all SFPs are sent to the web server, which then sends a response to the external network. WEB SFPs such as Directory Listing, Error Message Handling, Invalid HTTP, Privacy File Filtering, Privacy Output Filtering, Response Header Filtering, User Defined Pattern, and Website Defacement are applied to these HTTP responses as well. The SFPs that are not applied to an HTTP response are as follows:

- WEBCLIENT SFP
- URL Access Control rule among WEB SFPs (only performs URL heuristics function)

1) WEBCLIENT SFP

The WEBCLIENT SFP can be applied either automatically or manually.

If the WEBCLIENT SFP is manual, the Remote administrator sets the access block list manually on the management console. When an HTTP request is sent to the TOE, the Detection Engine examines whether or not the identified web client is on the access block list, and if the web client's IP address and port are on the list, the detection engine blocks the request.

If the WEBCLIENT SFP is automatic, the detection engine automatically registers an IP address that meets the conditions of HTTP DoS attack and accumulated risk values for each detection rule on the access block list and performs a block function. The automatically updated access block list can also be managed by the Remote administrator. Once the IP block time is expired, the IP address is deleted from the list.

- FDP_ACC.1.1
- FDP_ACF.1.1
- FDP_ACF.1.2 a)
- FDP_ACF.1.2 b)
- FDP_ACF.1.4 a)
- FDP_IFF.1.3 d)

2) WEB SFP

The detection engine checks if an HTTP request or response matches the attack pattern by using a pattern matching function. The web-targeted attack has a fixed pattern (like a fingerprint) that distinguishes itself from normal web usage. By checking if there are any HTTP requests that match such attack patterns, the Detection Engine detects an attack from the external network. In addition, the pattern matching method is used to prevent the web server from unintentionally exporting information that may be a threat to the security by checking the HTTP responses. The detection rules that operate an attack pattern check are as follows:

Rule	Description	Request	Response
Buffer Overflow	Detects and blocks a buffer overflow attack, which executes a malicious attacker's command intended to cause an overflow of the internal buffer when the executable code of the web server is running	O	
Cookie Poisoning	Detects the unauthorized manipulation of cookie information and blocks it from being delivered to the web server	O	
Cross Site Scripting	Detects and blocks/disables the upload of client side script on the web server that intends to run a malicious code in other users' browsers	O	
Directory Listing	Automatically blocks the complete showing of directory contents of a web server when it does not have a main page (index.html, default.asp, etc.)		O
Error Handling	Blocks error messages of a web server from being delivered to a user, as the DB error messages or the server script error messages such as JSP, ASP, and PHP may provide the attacker with the information that may be a threat to the security of web server		O
Extension Filtering	Restricts queries of file extensions on the web server that are not allowed by the administrator	O	
File Upload	Blocks files such as .exe, .jsp, and .php from being uploaded to the web server as they may be executed by the web server	O	
Input Content Filtering	Blocks input from a user if a prohibited word is included, or automatically transforms the word into another listed word	O	
Include Injection	Defends against various injection vulnerabilities, including the injection of a dangerous script, file, malicious code, etc.	O	
Invalid HTTP	Identifies an HTTP request or response message sent to or from a web server as a potential web attack and operates a function of detection and response when it does not conform to HTTP standards	O	O

Rule	Description	Request	Response
Invalid URL	Blocks an invalid URL to prevent malfunctioning of a web server	O	
Parameter Tampering	Detects and blocks manipulation of a user input domain such as the hidden field or unauthorized adding of a debug option	O	
Privacy File Filtering	Blocks various files containing important personal information such as social security number, credit card number, email address, and phone number from being uploaded or downloaded on the web service	O	O
Privacy Input Filtering	Detects and blocks input of important personal information such as social security number and card number according to the administrator's settings	O	
Privacy Output Filtering	Prevents the disclosure of important personal information such as social security number and card number through web service		O
Request Method Filtering	Blocks web request methods that are unnecessary for the web server operation	O	
Request Header Filtering	Analyzes the header of a request message from a web client, and blocks the request upon detecting a possible attack pattern	O	
Response Header Filtering	Filters the fields from the header of a web server's response message that provide more information than is necessary to the user		O
SQL Injection	Detects an attack to attempting manipulate an SQL string on the web server DB, and blocks it's delivery to the web server	O	
Stealth Commanding	Detects and blocks an attack to attach server side script in an input and send it to the web server attempting to implement malicious commands or obtain information	O	
Suspicious Access	Detects or blocks a web client's access through an abnormal web browser	O	

Rule	Description	Request	Response
User Defined Pattern	Compares the string in the request message of a web client with the patterns defined by a user when there is a match, blocks the request.	O	O
Unicode Directory Traversal	Detects and blocks an access to the directory file that is not allowed by the web server by using a Unicode	O	
Website Defacement	Detects unauthorized alteration of a web page and blocks it from being disclosed		O
URL Access Control	Detects and blocks an access request to a URL that is not included in the permitted access list	O	

[Table 31] Detailed Rules of Web Security Functions

- Even when access is identified as an intrusion, the TOE does not record a Detection log when the source IP and the destination URL are in the predefined list of exceptions. In addition, when a detected case matches the exception handling pattern (Regular Expression), it does not record a Detection log.

- The TOE takes predefined response actions to the rejected HTTP requests and responses. The applicable actions include "disconnect," "error code," "page redirection" and "do not block."

  - FDP_IFF.1.1
  - FDP_IFF.1.2
  - FDP_IFF.1.3 a)
  - FDP_IFF.1.3 b)
  - FDP_IFF.1.3 c)

3) Protection against OWASP Top 10 web vulnerabilities

The OWASP (Open Web Application Security Project) regularly releases the top 10 most important security risks of a web application. The TOE provides the following functions to counter the OWASP Top 10:

OWASP TOP10[1]	WAPPLES v4.0 Response Functions (Rules)
A1.Injection	Parameter Tampering
	SQL Injection
	Stealth Commanding
	Include Injection
A2.Cross-Site Scripting (XSS)	XSS
A3.Broken Authentication and Session Management	Cookie Poisoning
A4.Insecure Direct Object References	Invalid URL
	Unicode Directory Traversal
	Directory Listing
	Error Handling
A5.Cross-Site Request Forgery (CSRF)	XSS
	Stealth Commanding
A6.Security Misconfiguration	This vulnerability cannot be blocked by a WAF product. An administrator should constantly maintain proper security of the web server.
A7.Insecure Cryptographic Storage	Privacy Input Filtering
	File Filtering
	Input Contents Filtering
	Extension Filtering
	Privacy Output Filtering
A8.Failure to Restrict URL Access	URL Access Control

[1] OWASP Top 10 - 2010

OWASP TOP10[1]	WAPPLES v4.0 Response Functions (Rules)
A9.Insufficient Transport Layer Protection	This vulnerability cannot be blocked by a WAF product. However, use of an encryption function provided by the operational environment may prevent export, corruption, or deletion of the TSF data during transmission.
A10.Unvalidated Redirects and Forwards	URL Access Control

[Table 32] OWASP Top 10 Security Function Responses

- FDP_IFC.1.1
- FDP_IFF.1.1
- FDP_IFF.1.2
- FDP_IFF.1.3 a)
- FDP_IFF.1.3 b)
- FDP_IFF.1.3 c)

7.3 Identification and Authentication Functions

The TOE provides functions for identification and authentication, and authentication failure handling responses for a Remote administrator or Local administrator.

1) Remote administrator and Local administrator login

A Remote administrator (Operator, Website administrator, or Inquirer) or a Local administrator can access the security management functions by entering the correct administrator identification and authentication information.

A user attempting to obtain the authority of a Remote administrator enters an ID and a password on the login page provided by the management console. Then the management console sends the input ID and password to the detection engine to determine whether or not the user is appropriate for the Remote administrator role, and returns the authentication result to the user. In the case of a succssful authentication, the authenticated user is given the Remote administrator role and access to the operation screen of the management console. However, in the case of an unsuccessful authentication, the management console notifies the result to a Remote administrator. If the number of accumulated consecutive authentication failures reaches or exceeds 5, it is seen as malicious attack attempt and thus the Remote administrator account is

locked for 10 minutes.

A user attempting to obtain the authority of a Local administrator enters a password by access through a serial port of the hardware device on which the Detection Engine is installed and operates. The input password is sent to the Detection Engine and the authentication result is returned to the user. In the case of a successful authentication, the authenticated user is given the Local administrator role and access to the operation screen of the CLI. However, in the case of an unsuccessful authentication,the user is notified. If the number of accumulated consecutive authentication failures reaches or exceeds 5, it is seen as a malicious attack attempt, and thus the Local administrator account is locked for 10 minutes.

The identification and authentication information used are as follows:

- Identification information: Remote administrator ID or Local administrator ID
- Authentication information: Remote administrator password or Local administrator password

The Remote administrator is enforced to change the default password after initial authentication. Also the Remote administrator can change the password on the login page any time after an authentication. The password of a Remote administrator and a Local administrator is composed of 9-15 characters including one or more letters, numbers, or special characters. To counter dictionary and brute-force attacks, the use of 3 or more consecutive alphabetic/numeric characters in ascending/descending order and use of identical letters are prohibited. .

- FIA_AFL.1.1

When authenticating a Remote administrator or a Local administrator, the password is shown as "*" or " " (blank) to be proteced from disclosure.

To ensure that only a Remote administrator (opreator, Website administrator, or Inquirer) can access the TOE by using the management console, the Remote administrator identification is done prior to allowing access to the TOE function. The identification and authentification is performed through a trusted communication channel between the TOE components genetrated during the Remote administrator identification process.

The Remote administrator and Local administrator access through the management console and the CLI are as follows:

- Management Console

  · A remote administrator (Operator, Website administrator, or Inquirer) PC that has an IP address that is in the permitted IP address range

  · Remote administrator (Operator, Website administrator, or Inquirer)

- CLI console

  · Connection through a serial port that is directly connected to the TOE hardware

  · Local administrator

If the identification and authentication information entered by a Remote administrator (Operator, Website administrator, or Inquirer) and a Local administrator matches the information stored in CouchDB, the Remote administrator and Local administrator are allowed to access the TSF data and use the security mangement functions.

- FIA_ATD.1.1(1)
- FIA_ATD.1.1(2)
- FIA_UAU.2.1
- FIA_UAU.7.1
- FIA_UID.2.1
- FIA_SOS.1.1

2) Authentication failure handling

The TOE provides a function to manage authentication failures so as to prevent unauthroized access. When this function detects 5 unsuccessful authentication attempts, it takes the following actions:

- In the case of 5 or more authentication failures, sends an account locking message to a Remote administrator and a Local administrator

- Shuts down the login page of the management console of the Remote administrator and disconnects the CLI connection of the Local administrator

- Disables authentication of the Remote administrator and Local administrator account for 10 minutes

- FIA_AFL.1.1
- FIA_AFL.1.2

7.4 Security Management Functions

The TOE provides the Remote administrator and the Local administrator with the ability to manage security functions, security attributes of WEBCLIENT SFP, security attributes of WEB SFP, and TSF data.

The Detection Engine analyzes the commands of a Remote administrator sent through the Management Console and those of a Local administrator sent through the CLI and stores the setting values in CouchDB. Then it applies them to other security functions in real time according to the results of command analysis.

A Remote administrator is provided with the security management functions with the authorities of the Operator, Website administrator, or Inquirer; and a Local administrator is provided with the management functions for a part of the TSF data and security attributes.

1) Security function management

The TOE grants the ability to delegate the behavior of the following security functions to the Operator and the Website administrator:

Security Functions	Description	Authority
Session lock setting	A function to decide the threshold of inactivity time before locking an authorized administrator session. The time threshold may be set to 5 min, 15 min, and 30 min.	Operator
Setting of audit record event types	A function to decide the level of the audit record, classified into basic audit and whole audit	Operator
Detection level setting of each WEB SFP	A function to determine the detection level of detailed rules of WEB SFP. The detection level is generally classified into “not detected” and “detected”, and for some WEB SFPs, “detected” is subdivided according to the characteristics of rules. In the case of some detailed rules, it can be “user-defined” or “heuristics.”	Operator, Website administrator
Management setting of	A function to decide how to manage the	

Security Functions	Description	Authority
access block list method (automatic or manual)	access block list. When using a manual method, the Operator registers the IP address and port information to be blocked on the access block list. When using the automatic method, the Operator sets the degree of risk associated with each rule. Additionally, the HTTP DoS detection conditions which automatically update the IP address block list can be set.	

[Table 33] Security Function Descriptions

- FMT_MOF.1.1
- FMT_SMF.1.1

2) Security attribute management of WEBCLIENT SFP

The TOE provides the Operator with the functions to manage the security attributes of the subjects and objects that are used for the WEBCLIENT SFP. Also, the initial values of the security attributes used for the WEBCLIENT SFP can only be set by the Operator.

- FMT_MSA.1.1
- FMT_MSA.3.1
- FMT_MSA.3.2
- FMT_MTD.2.1
- FMT_MTD.2.2
- FMT_SMF.1.1

3) Security attribute management of WEB SFP

The TOE provides the Operator and the Website administrator with the functions to manage the security attributes of the subjects and objects that are used for the WEB SFP. The security attribtues used for the WEB SFP are as shown in [Table 34]. Also, the initial values of the security attributes used for the WEB SFP can only be set by the Remote administrator (Operator and Website administrator).

SFP	Security Attributes	Authorized Roles	Management Functions
Information	URL, Cookie, Method, User	Operator,	Query

SFP	Security Attributes	Authorized Roles	Management Functions
flow block list or allow list of the WEB SFP	Agent, From, Accept, HOST, Contents-type, Response status code, Web directory information	Website administrator	Modify Delete Generate

[Table 34] Security Attributes of Web Security Policies

- FMT_MSA.1.1
- FMT_MSA.3.1
- FMT_MSA.3.2
- FMT_SMF.1.1

4) TSF data management

The TOE provides the Remote administrator and the Local administrator with the functions to manage the following TSF data:

TSF Data	Detailed Information	Authority
Remote administrator account	Authority, ID, password, other information	Operator, Website administrator
Remote administrator access IP	IP address of IPv4 type, IP address of IPv6 type	Local administrator
Security alarm email address	-	Operator
Local administrator password	-	Local administrator
Personal information	-	Operator, Website administrator
Statistical data	Statistical information of traffic, page hits, Detection log, distribution by each rule, system status, network status	Operator, Website administrator, Inquirer
Website information	Website name, port, trusted IP, other information	Operator
Protected web server information	Web server IP address/port, operation mode, SSL usage	Operator
Time synchronization	Sending email address, SMTP server	Operator

TSF Data	Detailed Information	Authority
server information	IP address	
Information of the current state of the system	Network port, traffic, resources, web server, other information of the current state	Operator

[Table 35] Management Authority by TSF data

- FMT_MTD.1.1
- FMT_SMF.1.1

5) Administrator-specific security roles

The administrator role of the TOE is classified into a Remote administrator and a Local administrator according to the access methods and authorities of security management functions. A Remote administrator is classified into an Operator, a Website administrator, and an Inquirer according to the detailed authorities.

An Operator is the root administrator who can perform all security management functions and manage the accounts of Website administrator and Inquirer. A Website administrator can make changes to the given website but cannot generate or delete the website or the security attributes. An Inquirer cannot change security attributes other than his/her own password, and can search/review the Detection log and Audit log, and review the dashboard.

A Local administrator has access to the CLI for security management via a serial port and can only operate part of security management functions such as network configuration.

- FMT_SMR.1.1
- FMT_SMR.1.2

7.5 TSF Protection Functions

The TOE checks the status of the major processes of the detection engine and verifies the integrity of its setting files and executable files to allow the secure enforcement of the TSF.

1) Integrity monitoring

The detection engine detects any corruption by comparing the hash value of the settings files and executable files necessary for the TSF enforcement. If the hash values do not match, it recovers the file to its original state to guarantee integrity. The comparison of the hash values is performed during initial start-up, periodically during normal operation, and at the request of the Operator.

- FPT_TST.1.2
- FPT_TST.1.3

2) Status checkup for major process of Detection Engine

To ensure the secure enforcement of the TSF, the detection engine checks the status of its detection and blocking processes during initial start-up and periodically during normal operation, and then restarts upon detecting an error.

The detection and blocking process checkup is performed by the management process. It sends a check message to the detection and blocking processes and if no response messages were sent from the processes, it is seen as an abnormal state and the processes are restarted.

- FPT_TST.1.1

7.6 Session Locking Functions

1) Locking of a Remote administrator session due to inactivity timeout

If there is no activity (i.e. input) from the Remote administrator during the predefined time period, to prevent an unauthorized user's access, the management console clears the security management screen and locks the Remote administrator's session to disable any security management activities through the management console. The Remote administrator shall perform re-authentication to unlock the session.

To perform the session locking function, the TOE examines all actions of the keyboard

and mouse of the Management Console every minute and, if no actions were detected during the predefined time period, locks the Remote administrator's session. In addition, the TOE clears the security management screen of the management console and outputs a re-authentication screen for session unlocking, thereby making sure that no security management activities can be performed through the management console before re-authentication.

- FTA_SSA.1.1
- FTA_SSL.1.2