KECS-CR-12-70

WAPPLES v4.0

Certification Report

Certification No.: KECS-NISS-0426-2012

2012. 11. 9

IT Security Certification Center

History of Creation and Revision

No.	Date	Revised Pages	Description
00	2012.10.12	-	Certification report for WAPPLES v4.0 - First documentation
01	2012.11.9	5, 7	evaluation completion date

This document is the certification report for WAPPLES v4.0 of PENTA SECURITY SYSTEMS INC.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance, Inc. (KoSyAs)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL4 evaluation of WAPPLES v4.0 developed by PENTA SECURITY SYSTEMS INC. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

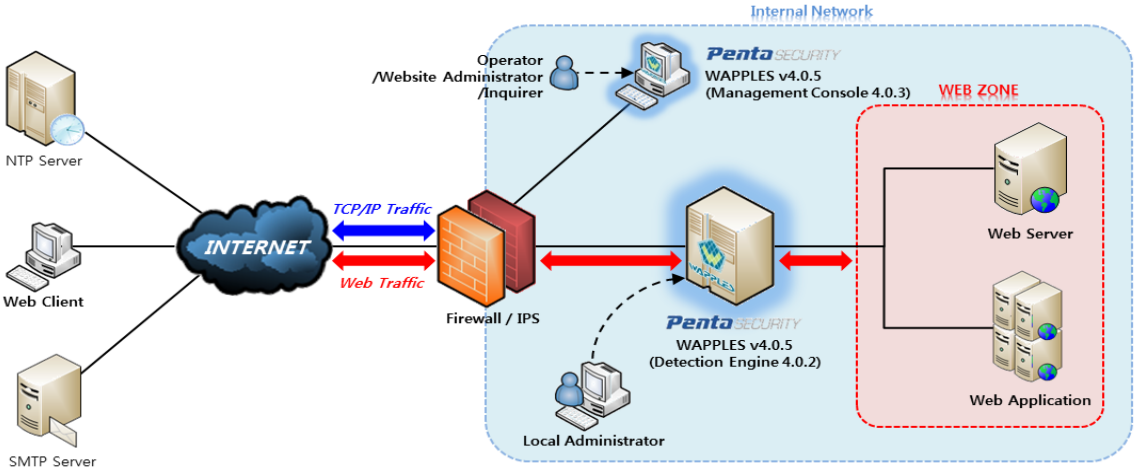
WAPPLES v4.0 (hereinafter TOE) is a Web Application Firewall (WAF) that securely protects the web server and web application by detecting and blocking attacks in advance by judging normality web traffics. The TOE is a software type that is delivered to the final user as loaded on a dedicated hardware model of WAPPLES-100 eco, WAPPLES-1000 Type2 and WAPPLES-1000 Type2 Plus.

The TOE is composed of a “detection engine” from external web attacks which protects the web application and the web server located in the web zone by analyzing the web traffic entering from outside and a “management console” which provides the security management functions such as security policies and the TOE operational environment setting to the remote administrator.

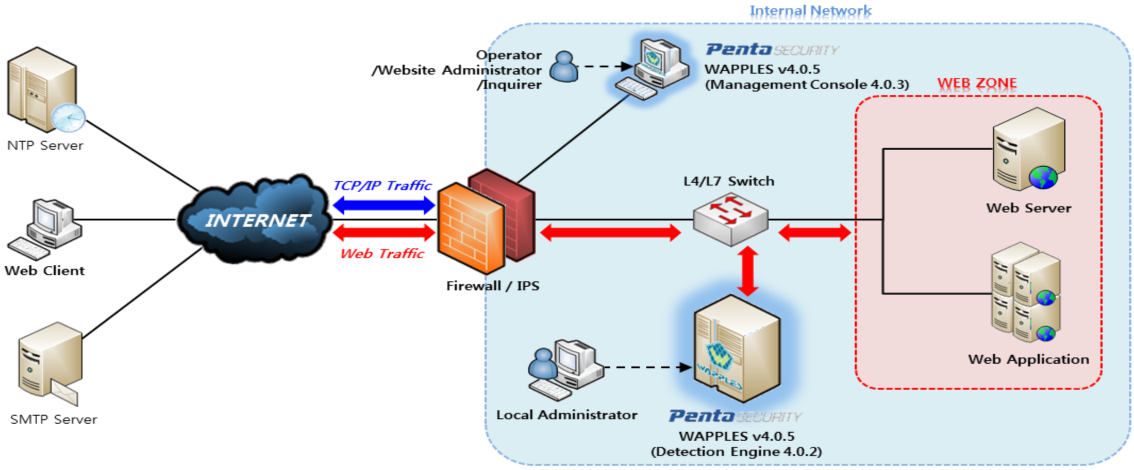
The evaluation of the TOE has been carried out by KoSyAs and completed on Oct. 19, 2012. This report grounds on the evaluation technical report (ETR)[2] that KoSyAs had submitted and the Security Target (ST)[3].

The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL4. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

The TOE operational environment is classified into an “Inline mode [Figure 1]” and a “Reverse proxy mode [Figure 2],” depending on the location of its installation and operation.



[Figure 1] Inline mode



[Figure 2] Reverse proxy mode

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to the certificate, and no warranty of the IT Product by the government of Republic of Korea or by any other organization that recognizes or gives effect to the certificate, is either expressed or implied

2. Identification

The TOE title is WAPPLES v4.0, consisting of the following components and related guidance documents and they are identified as described in [Table 1].

Type	Identifier		Delivery Form
SW	WAPPLES v4.0.5	Detection engine 4.0.2	Software loaded on a Hardware
		Management Console 4.0.3	Software
DOC	WAPPLES v4.0 Operation and Installation Guidance v4.0		Booklet

[Table 1] TOE identification

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (September. 1, 2009)[4] Korea Evaluation and Certification Regulation for IT Security (July 20, 01, 2011)[5]
TOE	WAPPLES v4.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
EAL	EAL 4
Developer	PENTA SECURITY SYSTEMS INC.
Sponsor	PENTA SECURITY SYSTEMS INC.
Evaluation Facility	Korea System Assurance, Inc. (KoSyAs)
Completion Date of Evaluation	October 19, 2012
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The TOE complies with security policies defined in the ST [3] by security objectives and security requirements. The TOE provides the security functions to protect web server and web application by detecting and blocking web attack based on main security features as follows :

- Web request and response analysis for web security
- Access control of the network level
- Provision of security management function
- Provision of traceability in case of security related events
- TSF and TSF data protection

In addition, the TOE provides security features to identify and authenticate authorized users, to generate audit records of the auditable events including start-up and shut-down of audit functions, and to securely manage the TOE including setting of detection rules.
For more details refer to the ST [3].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of of the environment in which the TOE will be used or is intended to be used in order to limit the scope of security consideration(for the detailed and precise definition of the assumption refer to the ST [3], chapter 3.4) :

- It is assumed that the TOE is located in a physically secure environment where only authorized administrator can access
- It is assumed 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
- It is assumed that administrators who manage the TOE have no malicious intentions are appropriately trained and follow all administrator guidance
- It is assumed that the database used by the TOE operates stably and is

securely configured and managed

- 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
- It is assumed that the TOE and the CLI console are connected directly

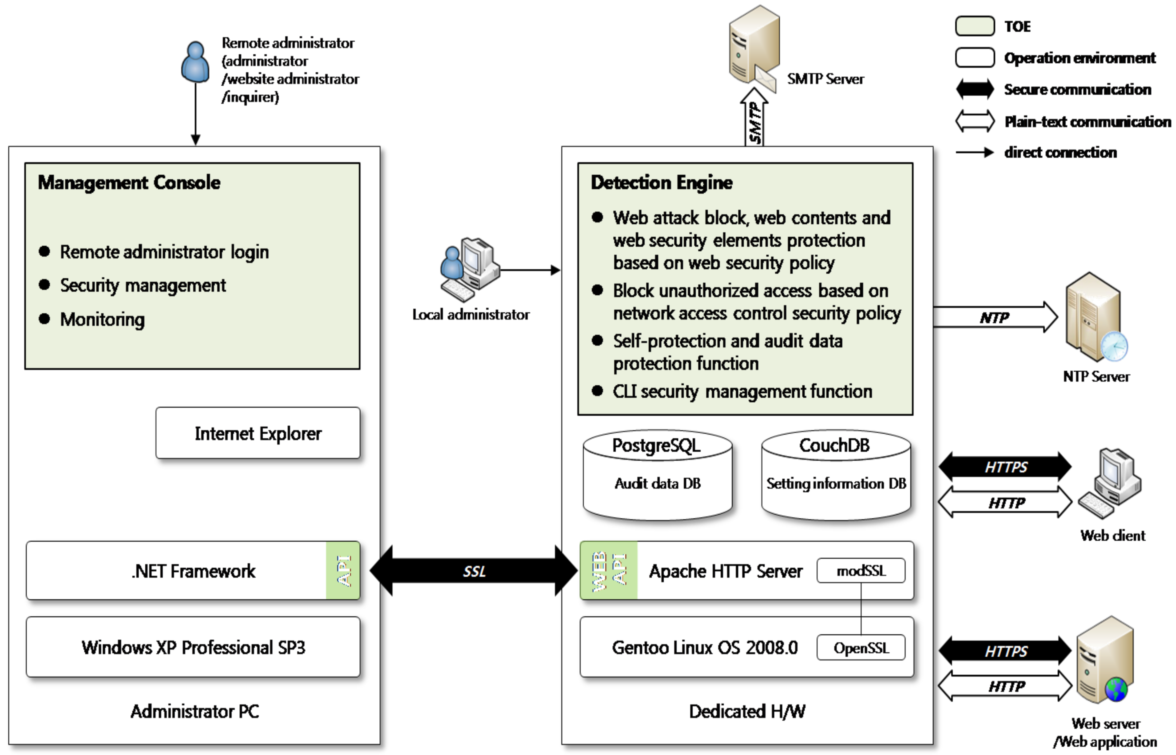
An external threatening agent is an unauthorized user of the TOE and the web client that causes a threat to the website and the application. The threatening agent has the enhanced-basic level of knowledge, resources, and motives. It may damage the resources of the target website by easily obtaining the vulnerability information and the attacking tools that may abuse the operational system and the application; it may also damage the TOE assets by using unauthorized methods. The TOE protects its asset from these obvious threats to vulnerabilities. For the detailed information on the lists of threats, refer to the ST [3], chapter 3.2:

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

5. Architectural Information

This chapter explains the logical scope of the TOE and the main components as shown in [Figure 3].

The TOE is composed of a software-form detection engine that is delivered to the user by being loaded on a dedicated hardware, a software-form management console that is installed on the administrator PC and a guidance document that is delivered as a form of a booklet. The management console is included in the detection engine installation image to be delivered and the administrator access the detection engine and downloads and installs the management console on the administrator PC.



[Figure 3] Logical scope of the TOE

The management console is operated in the .NET Framework environment of the administrator's PC. The TOE accesses the start-up web page of the security engine through the internet explorer in order to operate the management console and installs the management console on the administrator's PC through the web page and operates it.

The management console provides a security management function in the form of GUI to an authorized administrator enabling the TOE operation. The SSL cryptography channel that is developed in .NET Framework and Apache HTTP server is used when the authorized administrator requests through a management console or for the secure transmission of set TSF data.

The security functions provided by the management console are as follows :

- Remote Administrator Login
- Security management
- Monitoring

Detection engine protects the web server and web application based on WEBCLIENT SFP and WEB SFP saved in PostgreSQL. In addition, it provides the security management interface such as the network setting to the authorized local administrator, and operates self-protection and audit data protection for the security of TOE security functions,

The security functions provided by the security engine are as follows :

- WEB SFP-based Web Attack Block, Protection of Web Contents and Web Security Elements
- WEBCLIENT SFP-based Unauthorized Access Block
- Self-Protection and Audit Data Protection Function
- CLI Security Management Function

For detailed information on security functions, please refer to chapters 1.3, 1.4.2 and 7 of ST [3].

The minimum specifications for the administrator PC on which the management console is installed and operated are as follows :

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 3] HW specification for management console

The TOE hardware that operates the detection engine includes 100 eco, 1000 Type2, and 1000 Type2 Plus. Those specifications are as follows :

Hardware Model	**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
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 4] HW specification for detection engine

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
WAPPLES v4.0 Operation and Installation Guidance	v4.0	September 28, 2012

[Table 5] Documentation

7. TOE Testing

The developer took a testing approach deriving test cases regarding the TOE components and security functions including detection rules against web vulnerabilities, which are described in the tests. Each test case includes the following information :

- Test no. and conductor: Identifier of each test case and its conductor
- Test purpose: Includes the security functions and modules to be tested
- Test configuration: Details about the test configuration
- Test procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.2. This means that the developer tested all the TSFI defined for each life cycle state of the TOE, and demonstrated that the TSF behaves as described in the functional specification.

The developer tested both subsystems (including their interactions) and all the SFR-enforcing modules (including their interfaces), and analyzed testing results according to the assurance component ATE_DPT.1

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The penetration testing approach includes web vulnerabilities provided by the certification body and high-level techniques such as fuzzing and source code static analysis using Fortify tool. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [2].

8. Evaluated Configuration

The evaluated configuration of the TOE is identified by the name, major version and minor version as mentioned in [Table 2]. Especially, the detection engine will be delivered on three different types of hardware platform denoted by model names of WAPPLES-100 eco, WAPPLES-1000 Type2 and WAPPLES-1000 Type2 Plus.

For information about type names in relation to the hardware platform and software, please read chapters 1.3 and 1.4 of ST [3].

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [2] which references Single Evaluation Reports for each assurance requirement and Observation Reports.

The evaluation result was based on the CC [1] and CEM [6].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL 4.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The ST doesn't define any extended component. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be use as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.

The developer clearly identifies the TOE and its associated configuration items, that the ability to modify these items is properly controlled by automated tool, and that as a result, the errors caused by someone's mistake or negligence in the configuration management system decrease. Therefore the verdict PASS is assigned to ALC_CMC.4.

The configuration management document verifies that the configuration list includes the TOE, the TOE elements, the TOE implementation representation, security flaws, evaluation deliverables, and development tools. Therefore, the verdict of ALC_CMS.4 is the Pass.

The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Therefore the verdict PASS is assigned to ALC_DVS.1.

The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to

ALC_DEL.1.

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, and the delivery activity.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The security architecture document is structured to ensure that TSF cannot be compromised or bypassed, and appropriately describes that the TSF which provides the security domain separates these domains from each other. Therefore, the verdict of ADV_ARC.1 is the Pass.

The functional specifications specifies the objective, way of using, input parameter, operation, and error message to the TSFI(SFR-enforcing, SFR-supporting, and SFR-non-interfering) at equal detail level, and accurately and completely describes the TSFI. Therefore, the verdict of ADV_FSP.4 is the Pass.

The implementation representation is adequate to be used for other evaluators' analysis, and is sufficient to understand the detailed internal workings. Therefore, the verdict of ADV_IMP.1 is the Pass.

The TOE design description provides environment and overall TSF description to describe TSF, provides sufficient TOE description with respect to subsystem to determine the TSF boundary, and provides description about the TSF internals with respect to module. Also, it also provides detailed description of the SFR-enforcing module and sufficient information about the SFR-supporting, and SFR-non-interfering modules to determine that the SFRs are completely and accurately implemented. Hence the TOE design provides the description about the implementation representation. Therefore, the verdict of ADV_TDS.3 is the Pass.

Therefore, the security architecture document (the TSF architecture attribute which describes how to the TSF security enforcement is not compromised or bypassed), functional specification(TSF interface description), design description and implementation representation(architecture description about how the TSF behaves to execute the functions related to the claimed SFR), and implementation representation(description of source code level), which are included in the development documentation, are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged or bypassed.

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.

The developer has tested the TSF subsystems against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.1.

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing enhanced-basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.3.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing enhanced-basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_CMS.4	ALC_CMS.4.1E	PASS	PASS	
	ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.1	ALC_DVS.1.1E	PASS	PASS	
		ALC_DVS.1.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ADV	ADV_TDS.3	ADV_TDS.3.1E	PASS	PASS	PASS
		ADV_TDS.3.2E	PASS	PASS	
	ADV_FSP.4	ADV_FSP.4.1E	PASS	PASS	
		ADV_FSP.4.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.1	ATE_DPT.1.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.3	AVA_VAN.3.1E	PASS	PASS	PASS
		AVA_VAN.3.2E	PASS		
		AVA_VAN.3.3E	PASS		
		AVA_VAN.3.4E	PASS		

[Table 6] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE shall be set and operated within a controlled access facility physically available to authorized administrators only, and the detection engine shall not allow any other remote management from externals except for management console.
- The administrator shall be able to guarantee the reliability and stability for an operation system through periodical security updates of the TOE operation system.

- The administrator shall maintain and counter the security of web server against vulnerabilities of OWASP TOP 10 which cannot be countered by the TOE.

11. Security Target

The WAPPLES v4.0 Security Target v4.0, September. 28, 2012 [3] is included in this report by reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
SFP	Security Functional Policies
Management Console	TOE component used by a remote administrator for the operation of security management functions such as establishing of security policies and confirming of audit data
Detection Engine	TOE component that securely protects the web application and web server by analyzing and detecting the externally imported web traffics by receiving the remote administrator set security policies and operational environment information from Management Console, and blocking harmful web traffics
Bridge Mode	The operation mode in which a web client’s IP is preserved as the web application intrusion block system

is constructed as a firewall

Reverse proxy mode
The operation mode in which a web firewall operates as a type of web proxy and the communication between the web server and the web client passes through the web firewall via the changes of the DNS setting

Transparent proxy mode
The operation mode in which a web firewall operates as a type of web proxy but takes in the Proxy IP by selecting a physical composition mode similar to the bridge mode

Hidden field
The field hidden inside the HTML that is not visible in the web browsers but used to deliver the data

SQL syntax validator
The syntax analyzer, among the web attack detection rules that are provided by the TOE, which is used to detect the attack syntax by analyzing the SQL query that exists in HTTP request message in order to defend against the SQL injection attack

Accumulated risk
The degree of risk calculated by using the weighted values and the number of attacks of each detection rules and the time over which the attacks progressed that is used to automatically register the IP on the IP block list of the TOE if it satisfies the administrator-set threshold

Web application
Web-based computer application that is developed for the user client to receive various services of the web server based on a network such as the internet or the intranet. The representative programming languages include Java, XML, PHP, ASP and JSP for the development of this web application

Web contents
All auditory and visionary 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

Administrators
The user who accesses the TOE for purposes of secure operation and management of the TOE. The administrators are authorized through identification authentication of the TOE and are classified into a “remote administrator” who remotely operates the TOE

security management functions by using a management console and a “local administrator” who directly connects via a serial port of hardware in which the security engine is installed and operated.

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] KOSYAS-2011-20, WAPPLES v4.0 Evaluation Technical Report V1.00, October 5, 2012

[3] WAPPLES v4.0 Security Target v4.0, September 28, 2012

[4] Korea Evaluation and Certification Guidelines for IT Security(September 1, 2009)

[5] Korea Evaluation and Certification Regulation for IT Security (July 20, 2011)

[6] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-004, July 2009