KECS-CR-08-52

SECUI NXG W V1.0.1
Certification Report

Certification No. : KECS-NISS-0135-2008

December 2008

National Intelligence Service
IT Security Certification Center

Revision history			
No.	Date	Page	Revision
00	22 Dec. 2008	-	First draft

This document is the certification report on SECUI NXG W V1.0.1 of SECUI.COM Corporation.

Certification Committee Members

Y. H. Jang (MOPAS), I. J. Yoon (NSRI),

H. J. Lee (Korea university), H. B. Yoo (Kwangwoon university) ,

D. H. Won (Sungkyunkwan university), K. S. Lee (Soongsil university),

J. H. Song (Hanyang university), S. W. Son (ETRI), H. S. Lee (KIISC)

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Facility

Korea System Assurance, Inc.

Table of Contents

1. Overview ··· 1

2. TOE Identification ··· 3

3. Security Policy ··· 5

4. Assumptions and Scope ··· 6

4.1 Assumptions ··· 6

4.2 Scope to Counter a Threat ··· 6

5. TOE Information ··· 7

6. Guidance ··· 15

7. TOE Test ··· 16

7.1 Developer's Test ··· 16

7.2 Evaluator's Test ··· 17

8. Evaluation Configuration ··· 18

9. Evaluation Result ··· 19

10. Recommendations ··· 23

11. Acronyms and Glossary ··· 24

12. Reference ··· 27

1. Overview

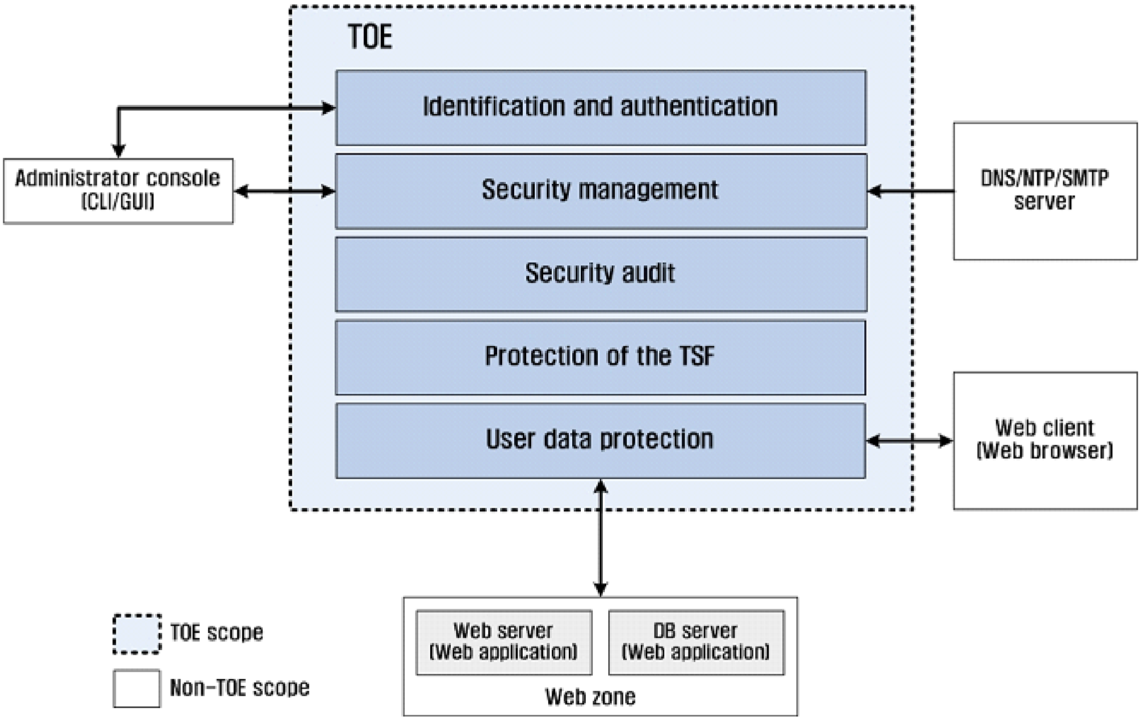
This report describes the certification result drawn by the certification body on the results of the EAL4 evaluation of SECUI NXG W V1.0.1 with reference to the Common Criteria for Information Technology Security Evaluation (notified on 16 July 2008, "CC" hereinafter). It describes the evaluation result and its soundness and conformity.

The evaluation of SECUI NXG W V1.0.1("TOE" hereinafter) has been carried out by Korea System Assurance Inc. and completed on 5 Dec. 2008. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted, according to which the TOE has been confirmed to satisfy the CC Part 2 and Part 3 requirements and hence to be "suitable."

The TOE is a software-based Web application firewall that locates on the connection point of external and internal of the Web zone connected to the Internet, detecting and preventing malicious Web traffic flowing 'from outside to inside of the Web zone' or 'from inside to outside of the Web zone' in real time, consequently protecting the Web application and Web server data.

The TOE provides the following security functions, which are shown in [Figure 1] Logical scope and boundaries of the TOE.

- Identification and authentication
- Security management
- Security audit
- Protection of the TSF
- User data protection



[Figure 1] Logical scope and boundaries of the TOE

The Certification Body has examined the evaluation activities and test procedures, provided the guidance for the technical problems and evaluation procedures, and reviewed each evaluation work package report and evaluation technical report.

Consequently, the Certification Body has confirmed that the TOE had satisfied all security functional requirements and assurance requirements specified in the ST.

Thus the Certification Body has certified that the evaluation, including the observations of the evaluators, had been performed correctly and appropriately.

Certification validity: Information in this certification report does not guarantee that TOE is permitted use or that its quality is assured by the government of Republic of Korea.

2. TOE Identification

[Table 1] identifies the TOE.

[Table 1] TOE identification

Evaluation guidance	Korea IT Security Evaluation and Certification Guidance (16 Jul. 2008) Korea IT Security Evaluation and Certification Scheme (1 Sep. 2008)
Evaluated Product	SECUI NXG W V1.0.1
Protection Profile	N/A
Security Target	SECUI NXG W V1.0.1 Security Target V1.2 (1 Sep. 2008), Secui.com Corp.
Evaluation Technical Report	SECUI NXG W V1.0.1 Evaluation Technical Report, issued V1.0 (5 Dec. 2008)
Evaluation result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation criteria	Common criteria for information technology security evaluation V3.1(No.2008-26 notified by the MOPAS, 16 Jul. 2008)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1 Revision 2, Sep. 2007
Sponsor	Secui.com Corp.
Developer	Secui.com Corp.
Evaluator	Yongjoon Choi, Sui Yim, Jiyeon Lee Korea System Assurance, Inc.
Certification body	IT Security Certification Center, National Intelligence Service

The TOE is a software loaded on the CF memory of its exclusive hardware platform that is identified depending on the platform.

[Table 2] shows the operational environment of the TOE.

[Table 2] Specifications for the TOE operation

Compo-nent	SECUI NXG 4000W			SECUI NXG 2000W			
	4C	12C	12F	4C	12C	12F	
CPU	XLR 732 1.2 Ghz XLR 532 1.2 Ghz			XLR 532 1.2 Ghz			
RAM	8 GB			4 GB			TOE
CF Card	2 GB *2			2 GB			LOG
HDD	500 GB			500 GB			
NIC	10/100/1000 BASE-T *4 (Copper)	10/100/1000 BASE-T *12 (Copper)	1000 BASE-SX *12 (Fiber)	10/100/1000 BASE-T *4 (Copper)	10/100/1000 BASE-T *12 (Copper)	1000 BASE-SX *12 (Fiber)	
Mgmt	10/100/1000 BASE-TX			10/100/1000 BASE-TX			Manage-ment port
Console	RJ-45			RJ-45			

3. Security Policy

The TOE operates in conformance with the following security policies:

P.Audit To ensure the accountability of all security-relevant actions, the security-relevant events shall be recorded and maintained, and the data be reviewed.

P.Administration The authorized administrator shall be able to manage the TOE in a secure manner and keep the TSF data up to date.

4. Assumptions and Scope

4.1 Assumptions

The TOE shall be installed and operated with the following assumptions in consideration:

A.Locate The TOE is located in a physically secure environment that only authorized personnel can access.

A.Security When the internal Web zone environment changes due to a network configuration change, increase or decrease of Web server, Web application, and Web service, the changed environment and security policies are reflected immediately to the TOE operational policy to maintain the same security as before.

A.Administrator The authorized TOE administrator is not malicious, well trained of the TOE management functions, and performs duties as specified in the administrator's guideline.

A.OSpatch Any services or measures not required on the OS are eliminated and the vulnerabilities are patched to ensure confidence and stability of the OS.

A.Connection The TOE divides the network of Web zone into internal and external; all Web traffic between which are transferred through the TOE.

A.Transfer The TOE protects the TSF data transferred between a remote administrator and the TOE from unauthorized disclosure and modification.

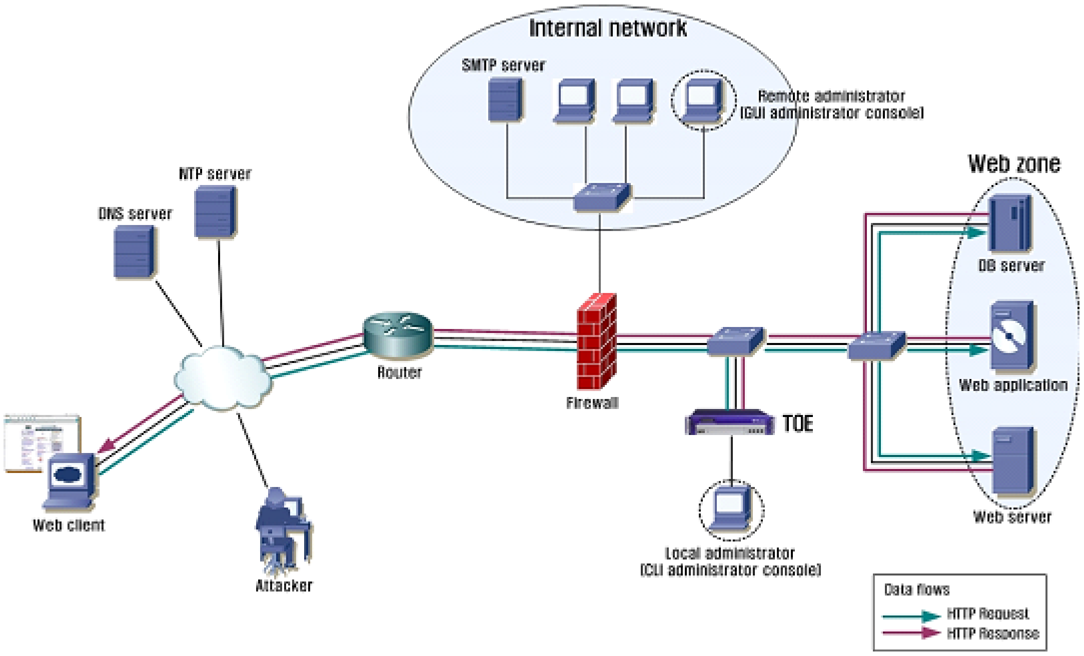
4.2 Scope to Counter a Threat

The TOE provides a means appropriate for the IT environment of the TOE to counter a security threat but not a means to counter a direct physical attack that causes malfunction of the TOE. The TOE also provides a means to take actions on any logical attacks launched by a threat agent possessing extended-basic expertise, resources, and motivation in the networks of the TOE.

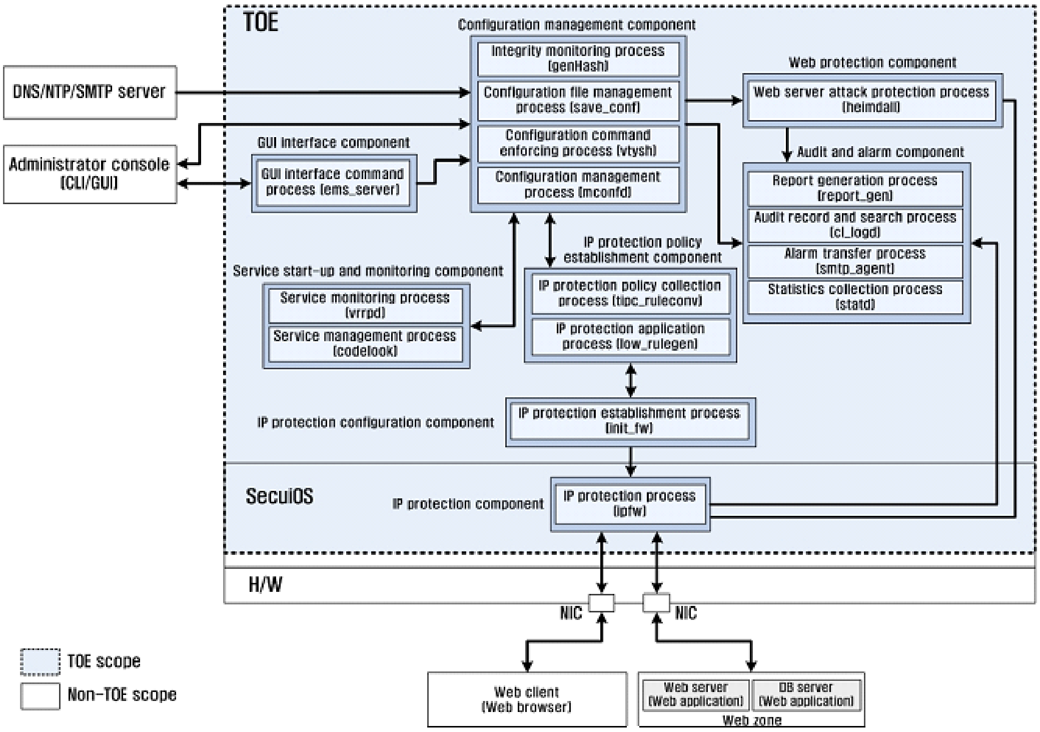
All security objectives and security policies are described such that a means to counter identified security threats can be provided.

5. TOE Information

The TOE is a Web application firewall that locates on the connection point of external and internal of the Web zone connected to the Internet, detecting and preventing malicious Web traffic flowing from outside[inside] to inside[outside] of the Web zone in real time. Its operational environment is shown in [Figure 2], which can be configured depending on the network environment as: 'Gateway mode' (similar to a general router mode) where the TOE that is assigned the Web server IP analyzes and processes all Web traffic before transmitting it to the Web server, which is not accessible from outside; 'Transparent-bridge mode' (similar to a firewall) where the TOE is not assigned an IP so that it is not seen to the external; or 'Transparent-gateway mode,' which is a combination of the above-mentioned modes.



[Figure 2] Operational environment of the TOE


TOE
Configuration management component
Integrity monitoring process (genHash)
Configuration file management process (save_conf)
Configuration command enforcing process (vtysh)
Configuration management process (mconfd)
DNS/NTP/SMTP server
Administrator console (CLI/GUI)
GUI interface component
GUI interface command process (ems_server)
Web protection component
Web server attack protection process (heimdall)
Audit and alarm component
Report generation process (report_gen)
Audit record and search process (cl_logd)
Alarm transfer process (smtp_agent)
Statistics collection process (statd)
IP protection policy establishment component
IP protection policy collection process (tipc_ruleconv)
IP protection application process (low_rulegen)
Service start-up and monitoring component
Service monitoring process (vrrpd)
Service management process (codelook)
IP protection configuration component
IP protection establishment process (init_fw)
SecuiOS
IP protection component
IP protection process (ipfw)
H/W
NIC
NIC
Web client (Web browser)
Web server (Web application)
DB server (Web application)
Web zone
TOE scope
Non-TOE scope

[Figure 3] Architecture of the TOE

The TOE comprises the following 8 subsystems:

- IP protection subsystem

Comprised of a IP protection process(ipfw) that performs packet filtering. It exists as a module in the kernel domain to provide information flow control of all packets coming into or out of the network at the network layer. Packet filtering is based on the policy registered on the IP protection policy set subsystem with conditions of a packet such as source/destination IP address/port number, protocol, and packet direction (from Web client to Web server, from Web server to Web client). It also provides a function to send a packet filtering log generated by the IP protection process(ipfw) to the audit and alarm subsystem in the application domain.

- IP protection set subsystem

Comprised of an IP protection establishment process(init_fw), which supports packet filtering. When the TOE starts the services, IP protection establishment process(init_fw) will be enabled and it accesses the configuration management subsystem. After checking the operation mode and zone information of the network, it refers to the load balance information and board type information in the configuration file to apply them to the IP protection process(ipfw). It can bring a network operation mode information applied to the enabled Web protection subsystem and apply to the IP protection subsystem to perform the re-direct function.

- IP protection policy set subsystem

Comprised of an IP protection policy collecting process(tipc_ruleconv), which accesses the configuration management subsystem to obtain and transform an activated packet filtering policy; and an IP protection policy application process(low_rulegen), which applies a packet filtering policy on the IP protection process(ipfw).

- Web protection subsystem

Comprised of a Web server attack protection process(heimdall), performing Web protection on the packets that passed through the IP protection subsystem and mediating communication between the Web server and client. It is based on multi thread considering confirmation delays according to the information flow control policy; the thread includes one that performs Web protection and another that processes a client access in order to ensure fast handling of client accesses.

(1) Web server data learning

Web server attack protection process(heimdall) monitors the requests of Web client sent to the Web server for a specific period of time categorizing them into cookie domain, cookie, Web server, and URL and blocks attack based on the collected Web traffic data.

Cookie domain, in which the cookie information is managed, is necessary for management at each domain when maintaining session information at the request for a cookie of a Web client.

'Cookie' means a session cookie, in which ID information of a session allowed access to the Web server is included. Functions to protect a cookie include SQL phrase/syntax injection protection, Cross-site scripting protection, and Command injection protection.

The TOE will collect Web traffic data about a virtual Web server in case that it is configured as a virtual domain in the protected Web server.

URL information is collected as a part of heuristics about URLs in the Web server at the request of a Web client and under application of information flow functions.

(2) Web server data protection

Web traffic check performs an analysis of a source IP address, destination IP address, and HTTP protocol. It checks attack patterns in accordance with the policies set by each module composed as a countermeasure against the top 10 vulnerabilities defined by OWASP as the following:

- URL check: Checks if a URL is allowed
- Query phrase check: Checks if a query is allowed
- Cross site scripting(XSS) protection: Blocks an attack using XSS
- Hidden field manipulation protection: Checks if a hidden form component is manipulated
- Header method check: Checks if an HTTP method is allowed
- SQL syntax injection protection: Checks if an SQL syntax is included and replaces it
- Command injection protection: Checks if a system command is injected
- URL-based access control: Controls access using IP addresses and port numbers allowed for each URL
- Base64 encoding check: Checks a query encoded using base64 encoding method
- Header buffer overflow check: Checks the header size
- URL extension check: Checks the extension of a file used in a URL
- Password check: Checks if a vulnerable password is used
- SSL application protection: Protects a Web page by applying SSL
- X-Forwarded-For header support: Adds a client IP to a standard HTTP header

If one of the traffics passing through the TOE maintains a Web session using a cookie, the TOE stores the issued contents of that Web session cookie to compare it with one sent from a Web client and checks the Web session according to the information flow control policy. The administrator can define the valid time of a Web session cookie.

- Cookie corruption protection: Blocks an unauthorized access manipulating cookies.

It protects data transferred between a Web client and the Web server using SSL protocol by applying the information flow control policy for each URL of that Web server.

- SSL application protection: Protects a Web page on which policies have been set by automatically applying SSL

(3) Service contents protection

A response packet from the Web server may contain critical information such as personal information that requires protection. Web server attack protection process(heimdall) reassembles the packets sent from the Web server, performs data protection by the policies, and transfers only the Web traffic that passed the Web contents protection policy to the client.

The following functions are provided to protect personal credit information like an SSN or credit card number included in a Web page serviced by the Web server:

- Social security number protection: Checks the numbers and replace them
- Credit card number protection: Checks the numbers and replace them

Response from the Web server may include information about the Web server or Web page itself such as types of server and application, different error values, or footnote, which will be protected by the following functions:

- Error page handling: Prevents information from being leaked through an error page on the Web server
- Footnote deletion: Prevents analyzing the Web page information by deleting a footnote from that Web page

A Web page may have risk of having corruption of contents by an attacker. In this case, the following functions prevent a corrupted Web page from being exposed:

- Checksum protection: Performs a checksum operation on a Web page to detect corruption
- Forbidden word check: Checks if a Web page contains any forbidden word

- Audit and alarm subsystem

Comprised of an audit record and search process(cl_logd) that procides a function to generate and search all security audit records by the TSF; alarm transfer process(smtp_agent) that sends an email to an administrator when a potential violation is detected; statistics collection process(statd) that provides statistical material for each type of allow/deny transaction and Web intrusion attack; and report generation process(report_gen) that generates a report out of the statistics.

(1) Audit record and search

Performed by an audit record and search process(cl_logd), which receives the audit events occurred in the configuration management subsystem, service start-up and monitoring subsystem, Web protection subsystem, and IP protection subsystem and categorizes them into an allow transaction log, deny transaction log, L3 firewall log, audit(configuration change) log, and system log to generate audit data.

Audit record and search process(cl_logd) also searches the audit data by audit review criteria (e.g. level, time, subject ID, object ID, event result, etc.) and transforms them into a format readily understandable by the administrator.

(2) Report generation

Performed by the report generation process(report_gen); provides an administrator with a function to produce graphs out of reports(daily/weekly/monthly/yearly statistics and store them in a report file format(Excel, PDF).

(3) System monitoring and audit storage monitoring

Performed by a statistics collection process(statd), which provides information about CPU, memory, file system, network interface, and process status in the system. It generates audit data upon detection of a failure such as a network interface error and informs the administrator.

It also monitors the HDD usage in the system to protect the audit data in the storage. If it reaches 95%, it sends an alarm email about audit data loss to the administrator and overwrites the oldest audit data in case of storage exhaustion.

(4) Alarm transfer

Performed by an alarm transfer process(smtp_agent). It sends an email to an administrator when a potential violation such as a consecutive authentication failures, audit event of information flow control rule violation, or audit event of integrity violation is detected.

• Service start-up and monitoring subsystem

Comprised of a service monitoring process(vrrpd) that enables the processes of each component in the TOE and monitors operation of each process to restart it if service stops due to malfunction and a service management process(codelook) that processes command sent from configuration management process(mconfd) and controls start/stop/restart of each process.

(1) Command process and service operation

Performed by a service management process(codelook). While the TOE is providing its services, any TSF process can be enabled or disabled, and a TSF process in question can be enforced or stopped by the commands related to the TOE operation such as start, stop, and restart.

(2) Service monitoring

Service monitoring is performed by the service monitoring process(vrrpd). It monitors TSF processes and re-starts a service upon detection of a process not operating.

- Configuration management subsystem

Comprised of a configuration management process(mconfd), a configuration command enforcing process(vtysh), a configuration file management process(save_config), and an integrity monitoring process(genHash).

Configuration management process(mconfd) interprets an administrator command sent from GUI interface command handling process(ems_server) of GUI interface subsystem to send it to the related subsystems or provides the current setup(command interpretation related to the Web protection policy setup, Web server attack protection function setup, and addition/deletion/application of the packet filtering policy) to the administrator. It also provides a function to set general network information such as Interface IP, Gateway IP, DNS, SMTP IP, etc; a function to add/delete/modify an administrator (group); an administrator identification and authentication function(authentication failure handling); and a function to manage the time limit of an administrator session. Configuration command enforcing process(vtysh) processes the interpreted command and performs the functions. Configuration file management process(save_config) stores what is set by an administrator in a configuration file in HDD or applies what is set in the stored configuration files. Integrity monitoring process(genHash) monitors whether integrity of the TSF data(TOE configuration file, TOE executable file, administrator identification and authentication data, etc.) is damaged and, when it is, restores it..

- GUI interface subsystem

Comprised of a GUI interface command process(ems_server), which categorizes an administrator's command into log-related, file-related, and configuration-related and sends it to the configuration management subsystem.

6. Guidance

The TOE provides the following guidance documents:

1) SECUI NXG W V1.0.1 Operational user guidance Version 1.1, 31 Oct. 2008
2) SECUI NXG W V1.0.1 Preparative procedures Version 1.1, 1 Sep. 2008

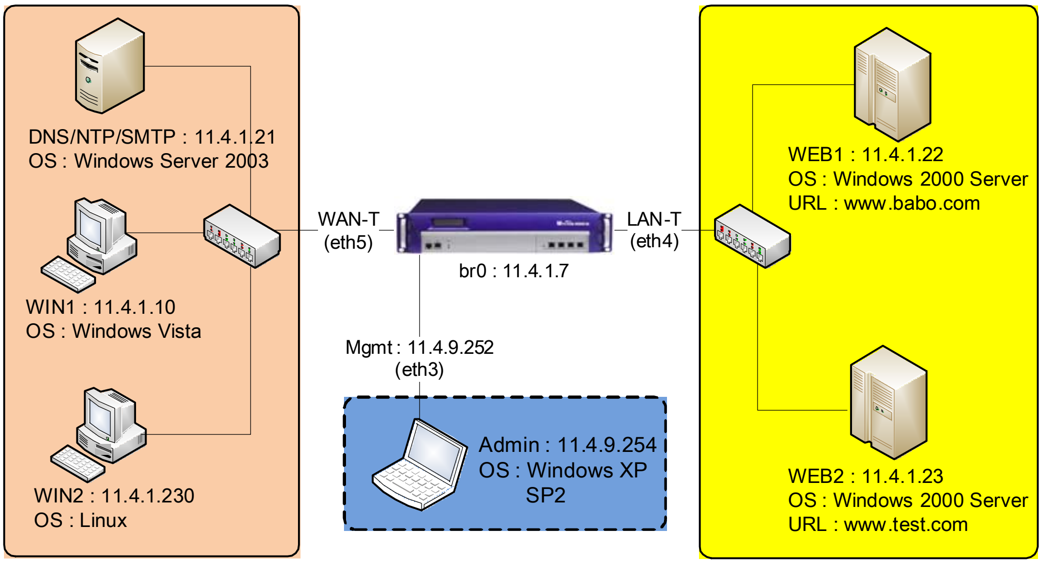
7. TOE Test

7.1 Developer's Test

Developer's testing is detailed in the test documents. The next clauses describe the categorization of tests according to the security function features and the evaluation results of the developer's test.

- TOE test configuration

The developer has configured the test as specified in the ST as the following:



[Figure 4] Developer's test configuration

- Test method

The developer has configured the test environment, installed the TOE and Web server, and tested the security functionality through its TSFIs and internal interfaces of the SFR-enforcing modules.

- Analysis of test coverage / Testing

Details are given in the ETR.

- Test results

The evaluator has assessed the appropriateness of the developer's test configuration, test cases, functional testing and module testing and verified that the test and its results had been suitable for the evaluation environment. Detailed information can be found in the Independent Testing, which describes the evaluation results of ATE_IND.2.

7.2 Evaluator's Test

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.

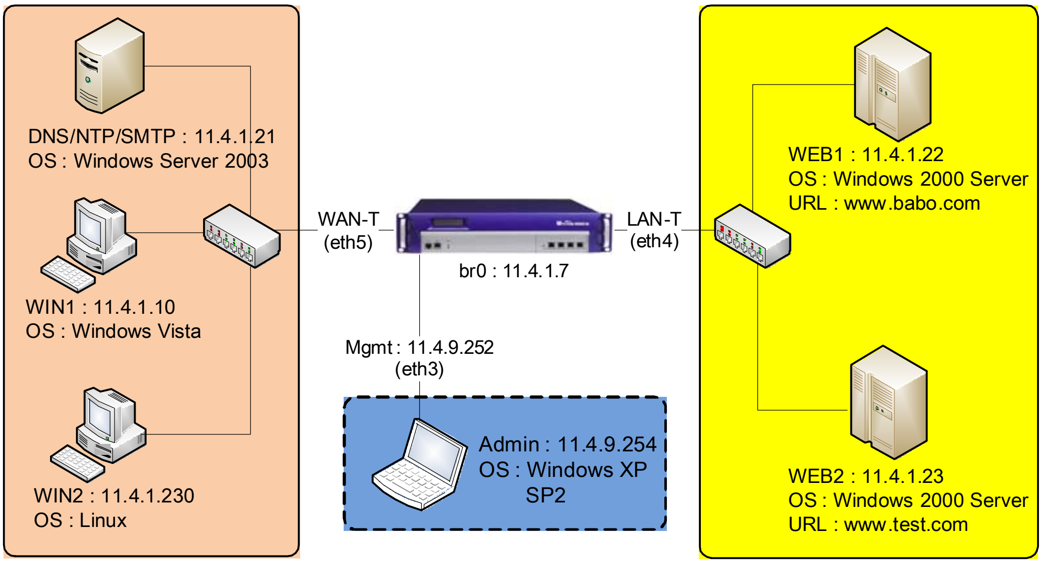
The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

The evaluator's test result has ensured that the product had normally operated as described in the design documents.

8. Evaluation Configuration

The evaluator has configured the environment for the independent testing as consistent with that specified in the ST as [Figure 5] below.



[Figure 5] Evaluator's test configuration

9. Evaluation result

The evaluation is performed with reference to the CC V3.1 and CEM V3.1. The result claims that the evaluated product satisfies the requirements from the CC Part 2 and EAL4 in the CC Part 3. Refer to the evaluation technical report for more details.

- Security Target evaluation (ASE)

ASE work units of the CEM are employed to evaluate the ST.

The ST introduction uniquely and correctly identifies the ST and TOE reference and describes the type, usage, major security features, physical and logical scope of the TOE to the extent of providing a reader general understanding.

Conformance claim includes the version of CC to which the TOE conforms, PP claim, and package claim and is described in consistent with the TOE type, security problem definition, and security objectives.

Security problem definition clearly describes the security problems that should be addressed by the TOE and its operational environment, that is, threats, organizational security policies(OSPs), and assumtions.

Security objectives counter the identified threats, achieve the OSPs, and address the assumptions properly and completely. The security problems are defined and categorized obviously into those for the TOE and for the operational environment.

The security requirements are described completely and consistently, and provide an appropriate basis for the development of the TOE to achieve the security objectives.

The TOE summary specification addresses all security functional requirements and defines them consistently with other parts of the ST.

Therefore, the ST is complete, consistent, and technically sound, and hence suitable for use as the basis for the TOE evaluation.

Satisfies the CC requirements.

- Development evaluation (ADV)

ADV work units of the CEM are employed to evaluate the development.

The security architecture description gives a sufficient description about the architectural properties of the TSF regarding how the security enforcement of the TSF cannot be compromised or bypassed and how the security domain provided by the TSF is separated from other domains.

The functional specification adequately describes all security functions of the TOE and that the functions are sufficient to satisfy the security functional requirements of the ST. It also adequately describes the TSFIs(TSF interfaces) to the extent that a reader can understand how the TSF satisfies the TSP.

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It also describes that the SFRs are completely and accurately implemented in terms of the SFR-enforcing, SFR-supporting, and SFR-non-interfering modules.

The implementation representation is sufficient to satisfy the security functional requirements in the ST and accurately implements the TOE design.

Therefore, the development documentation is adequate to give understanding about how the TSFs are provided, as it consists of a functional specification (which describes the interfaces of the TSF), a TOE design (which describes the architecture of the TOE in terms of subsystems and modules), an implementation representation (a source code level description), and a security architecture description (which describes how the TSF enforcement cannot be compromised or bypassed).

Satisfies the CC requirements.

- Guidance documents evaluation (AGD)

The preparative procedures documentation describes the procedures to progress the delivered TOE to the evaluated configuration as the operational environment described in the ST. Consequently, the evaluator has confirmed that the TOE had been securely configured.

The operational user guidance describes how to administer the TOE in a secure manner.

Therefore, the guidance documents give a suitable description of how the personnel who install, manage, and operate the TOE can administer the TOE in a secure way. Hence, the evaluator has confirmed that what is in the documents had been under a correct operation.

Satisfies the CC requirements.

- Life cycle support evaluation (ALC)

The configuration management documentation describes that the changes to the implementation representation are controlled with the support of automated tools. It also clearly identifies the TOE and its associated configuration items and describes that the ability to modify these items is properly controlled.

The evaluator has confirmed by the CM documentation that the developer had performed configuration management on the TOE implementation representation, evaluation evidence required by the assurance components in the ST, and security flaws.

Therefore, the evaluation of configuration management assists the consumer in identifying the evaluated TOE, ensures that the configuration items are uniquely identified, and ensures the adequacy of the procedures that are used by the developer to control and track changes that are made to the TOE.

The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site. Therefore, the delivery documentation is adequate to ensure that the TOE is delivered in the same way the developer intended without modification.

The evaluator confirmed in the life cycle support that the developer's control of the development environment had been suitable to provide the confidentiality and integrity of the TOE design and implementation required for the secure operation of the TOE and that the developer had used a systematic life-cycle model.

The evaluator has also confirmed the developer had used well-defined development tools with which one can get consistent and predictable results. Therefore, the life-cycle support provides an adequate description of the security procedures and tools used in the whole development process and the procedures of the development and maintenance of the TOE.

Satisfies the CC requirements.

- Tests evaluation (ATE)

The tests have been sufficient to establish that the TSF had been systematically tested against the functional specification. The evaluator has confirmed that the developer had tested the security functions of the TOE and the developer's test documents had been sufficient to show the security functions had behaved as specified.

The evaluator has determined, by independently testing a subset of the TSF, that the TOE had behaved as specified and gained confidence in the test results by performing all of the developer's tests.

Therefore, the tests have proved that the TSF had satisfied the TOE security functional requirements specified in the ST and behaved as specified in the design documentation.

Satisfies the CC requirements.

- Vulnerability assessment evaluation (AVA)

The vulnerability analysis adequately describes the obvious security vulnerabilities of the TOE and the countermeasures such as the functions implemented or recommended configuration specified in the guidance documentation. The evaluator has confirmed by independent vulnerability analysis that the developer's analysis had been correct. The evaluator has determined by performing vulnerability analysis that there had not been any vulnerabilities exploitable by an attacker possessing an enhanced-basic attack potential in the intended TOE environment.

Therefore, based on the evaluator's vulnerability analysis and penetration testing, the evaluator has confirmed that there had been no flaws or vulnerabilities exploitable in the intended environment for the TOE.

Satisfies the CC requirements.

10. Recommendations

- This product is a Web application firewall that detects and prevents an attack using HTTP/HTTPS protocol; which means it may be vulnerable to attacks using protocols other than HTTP/HTTPS protocol. Therefore, it is recommended that a network security product such as firewall, IPS, or IDS be installed in front of the network to enhance its security.
- Since this product allows multiple accesses of one admin ID on the GUI administrator console, it is recommended that the ID be distributed to the user in question according to the security manager's authority.
- The TOE overwrites the oldest audit data in case of the storage exhaustion; therefore, the security manager should check the capacity regularly and backup before the data is deleted.
- The security policies changed by the security manager during operation of the TOE will not be stored in the configuration files in real-time but stay in the memory; therefore, regular backup of the configuration files is recommended using the backup functions(Web firewall, administrator PC, etc.) provided by the TOE in order to prepare for any kinds of error.
- The TOE will be distributed with an administrator ID/password set tentatively. If one keeps using them, identification and authentication might be compromised. So, the security manager should delete them before installing and operating the TOE. Regular change of the administrator password is also recommended.
- The TOE controls access from external network to internal only with the functional security activated; when the power is off, all packets can pass by the properties of NIC. So the security manager should make sure that the power is on throughout the operation of the TOE.

11. Acronyms and Glossary

The following terms are used in this report:

(1) Acronyms

CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SF	Security Function
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

(2) Glossary

TOE
Target of evaluation; a set of IT product or system accompanied by guidance

Web application firewall
An IT security product that monitors HTTP/HTTPS packets and controls packet flow to detect and prevent attacks using vulnerability of Web server or Web application.

Gateway Mode
Gateway mode is operated in a proxy mode. Proxy was originally used in a firewall for Internet protection, but now for the access to a Proxy server on a Web browser. When a Web browser specifies a Proxy, URL required by a Web client will be connected to the Proxy server, not a server indicated by the URL. A Proxy server will send the request to the server indicated by the URL, then receive a response instead of the client and deliver it to the client.

Administrator console
Helps administer the TOE; Includes a GUI administrator that can access the TOE through a JAVA virtual machine on the Internet explorer and a CLI administrator console that can directly connect with the TOE through a serial port.

Forbidden word check
Checks if the contents from the Web server or query value delivered to the Web server include a forbidden word and, if they do, protects the contents from being leaked.

Command injection protection
Checks if any forbidden system command is being used.

Base64 encoding
Checks if a query used base64 encoding method.

File-upload attack
An attack where a user uploads to the Web server .exe, .jsp, and .php files applicable on it and enforces malicious commands.

Error Message Handling
Server script error messages the Web server displays such as JSP, ASP, and PHP, and a DB error message may give an attacker information that might threaten the security of the Web server. Error message handling stops the messages from being transferred to a user from the Web server.

Web application
Software developed since Web for the Internet/Intranet using various languages to search database or process general business logic. Script and service like Java script or JSP access database to search for the latest data and provide the result to a user through a browser or client program.

Web zone
Contrary concept to an Intranet; a domain protected by the TOE, where assets like a system that provides Web application are placed.

Web client
A user that receives Web services from a Web server.

Checksum protection
Checks the length or hash value of a Web page that the protected Web server sends as a respond to a Web client and protects modified contents from being leaked.

Cookie
Recorded information of access to the Internet Web site, which mediates between a user and the Web site.

Cookie corruption check
Checks the cookie made by the Web server; performs cookie encryption, cookie forge/corruption protection, and domain cookie management.

Cross Site Scripting (XSS)
An attack where an attacker uploads a client side script to a Web server to enforce a malicious code on someone else's browser.

Cross site scripting protection
Checks whether the query or cookie data sent to the Web server includes an enforceable script or HTML tag.

Header method check
Checks if the header method of each URL is allowed.

Header buffer overflow check
Specifies the maximum size of an HTTP header to prevent buffer overflow.

Hidden field
A hidden field in an HTML is used, though not being seen on a Web browser, to transmit data.

Hidden field manipulation protection
Checks if each URL includes a hidden field.

SQL Injection
An attack to manipulate an SQL syntax and send it to a Web server in order to manipulate the DB of the Web server.

SQL syntax injection protection
Blocks an attack where a user forges query and cookie value sent to the Web server so they have an SQL syntax error and enforces SQL command randomly.

12. Reference

The certification body has used the following documents to produce this certification report:

1) Common Criteria for Information Technology Security Evaluation (Notification no.2008-26 of the MOPAS, 16 Jul. 2008)
2) Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2006-09-001, Version 3.1 Revision 1, Sep. 2006
3) Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2007-09-002, Version 3.1 Revision 2, Sep. 2007
4) Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2007-09-003, Version 3.1 Revision 2, Sep. 2007
5) Common Methodology for Information Technology Security Evaluation, CCMB-2007-09-004, Version 3.1 Revision 2, Sep. 2007
6) Korea IT Security Evaluation and Certification Guidance, Jul. 2008
7) Korea IT Security Evaluation and Certification Scheme, Sep. 2008
8) SECUI NXG W V1.0.1 Security Target V1.2, Sep. 2008
9) SECUI NXG W V1.0.1 Evaluation Technical Report, issued V1.0, Dec. 2008