KECS-CR-08-22

eXshield V1.0.1.R Certification Report

Certification No : KECS-NISS-0105-2008

June 2008

National Intelligence Service

IT Security Certification Center

This document is the certification report on eXshield V1.0.1R of Samsung Networks Inc.

Certification Committee Members

J. W. Park (ETRI)

J. Y. Choi (Korea university)

D. S. Seo (Sungshin women's university)

I. Y. Lee (Soonchunhyang university)

S. W. Kim (Hansei university)

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Facility

Korea System Assurance, Inc.

Table of Contents

1. Overview ····· 1
2. TOE Identification ····· 2
3. Security Policy ····· 3
4. Assumptions and Scope ····· 4
4.1 Assumptions ····· 4
4.2 Scope to Counter a Threat ····· 4
5. TOE Information ····· 5
6. Guidance ····· 7
7. TOE Test ····· 7
7.1 Developer's Test ····· 7
7.2 Evaluator's Test ····· 8
8. Evaluation Configuration ····· 9
9. Evaluation Result ····· 11
10. Recommendations ····· 15
11. Acronyms and Glossary ····· 16
12. Reference ····· 17

1. Overview

This report describes the certification result drawn by the certification body on the results of the EAL4 evaluation of eXshield V1.0.1.R with reference to the Common Criteria for Information Technology Security Evaluation (notified 21 May 2005, "CC" hereinafter). It describes the evaluation result and its soundness and confirmity.

The evaluation of eXshield V1.0.1.R has been carried out by Korea System Assurance Inc. and completed on 22 May 2008. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted, in which the evaluation has confirmed that the product had satisfied the CC Part 2 and EAL4 of the CC Part 3 and had been "suitable" according to the CC Part 1, paragraph 191.

Developed by Secui.com Corp. and sponsored by Samsung Networks Inc., eXshield V1.0.1.R is an intrusion prevention system that detects and blocks an intrusion to protect the assets in the internal network.

The CB 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 CB has confirmed that the evaluation results had ensured that the TOE had satisfied all security functional requirements and assurance requirements specified in the ST, thus the observations and evaluation results made by the evaluator had been correct and reasonable, and the verdicts assigned by the evaluator on the product had been correct.

Certification validity: Information in this certification report does not guarantee that eXshield V1.0.1.R 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 (Notification No.2007-31 by the MIC, 22 Aug. 2007) Korea IT Security Evaluation and Certification Scheme (NIS, 1 Dec. 2007)
TOE	eXshield V1.0.1.R
Protection profile	Network Intrusion Prevention System Protection Profile V1.1
Security target	eXshield V1.0.1.R Security Target V1.10 (9 May 2008)
ETR	eXshield V1.0.1.R Evaluation Technical Report V1.00 (22 May 2008)
Evaluation result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation criteria	Common criteria for information technology security evaluation V2.3 (Notification No.2005-25 by the MIC, 21 May 2005)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)
Sponsor	Samsung Networks Inc.
Developer	Secui.com Corp.
Evaluator	Yeowung Yun, Mikyoung Kim, Yongjoon Choi Korea System Assurance
Certification body	National Intelligence Service

eXshield Security Switch V1.0 is a network intrusion prevention system that detects and blocks an intrusion to protect the assets in the internal network. Being located on the point that connects the Internet and the internal network or the point that separates the internal network and external network in a router or in-line type, eXshield Security Switch V1.0 performs detection and blocking of the network traffic flow between the internal and external networks in real time.

The TOE comprises TOE_Gateway to perform network intrusion prevention functions and TOE_LServer to store audit data.

The hardware, OS, and administrator console with which eXshield V1.0.1.R is installed are not covered in the evaluation. [Table 2] shows the necessary specifications of S/W and H/W for the operation of the TOE.

[Table 2] Specifications for the TOE operation

Category	TOE_Gateway	TOE_LServer	Administrator console
CPU	XLR 732 1.2 GHz XLR 532 1.2 Ghz	Intel Pentium III 1 GHz or above	Intel Pentium III 133 MHz or above
RAM	8 GB	256 MB and above	256 MB or above
CF Memory	2 GB	-	-
HDD	None	20 GB or above	20 GB or above
NIC	26 Ports (1Gbps*24, 10/100/1000 Mbps * 2)	2 Ports (1010/100/1000 Mbps * 2)	1 Port
Console	1 Port	-	-
OS	SecuiOS V1.2	RedHat Enterprise Linux 4 Update 4	Windows XP
S/W	-	-	- JRE V1.5.0_14 or above - Internet Explorer 6.0 or above

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 manage the TOE in a secure manner.

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 network environment changes due to a network configuration change, increase or decrease of host or services, the changed environment and security policies are reflected 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
Eliminates services or measures not required by the TOE and patches the vulnerabilities to ensure confidence and stability of the OS.
A.Connection
The TOE on a network divides it into internal and external, such that all communications between which are mediated by the TOE.
A.Server(*)
The NTP server and SECUI Update server that locate outside the TOE for the secure operation of the TOE functions are secure.

4.2 Scope to Counter a Threat

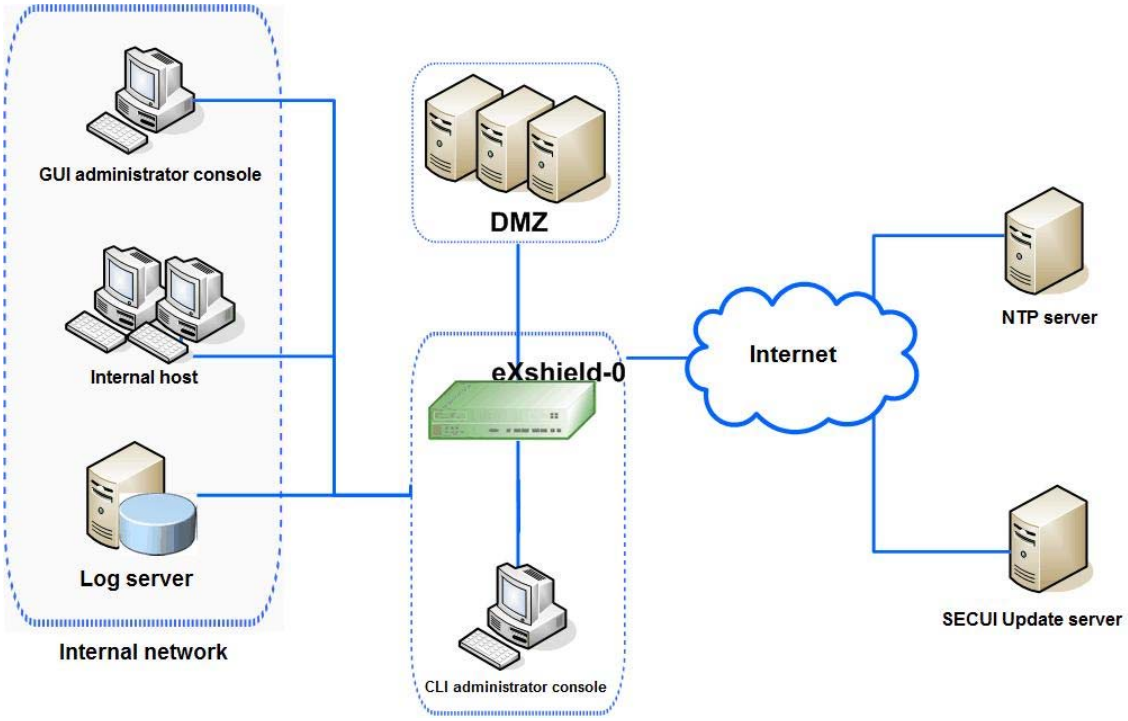
The TOE provides a means appropriate for the IT environment of the TOE to counter a security threat but not a means to counter a direct physical attack that causes malfunction of the TOE. The TOE also provides a means to take actions on any logical attacks launched by a threat agent possessing low-level 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

eXshield Security Switch V1.0 is a network intrusion prevention system that detects and blocks an intrusion to protect the assets in the internal network. Being located on the point that connects the Internet and the internal network or the point that separates the internal network and external network in a router or in-line type, eXshield Security Switch V1.0 performs detection and blocking of the network traffic flow between the internal and external networks in real time.

As the figure below shows, installation of eXshield Security Switch V1.0 on the contact of external untrusted network ensures the intrusion prevention function for the illicit intrusion and attack from outside.



(Figure 1) Configuration of eXshield Security Switch V1.0

eXshield Security Switch V1.0 uses its intrusion prevention function to prevent, detect, and block illicit access or hacking attack that makes resources of host and network exhausted or causes problem in the accessibility by exploiting vulnerabilities.

The authorized administrator is able to perform the security management of eXshield Security Switch V1.0 by using GUI administrator console, which accesses through the Internet explorer or eXshield Manager, and CLI administrator console,

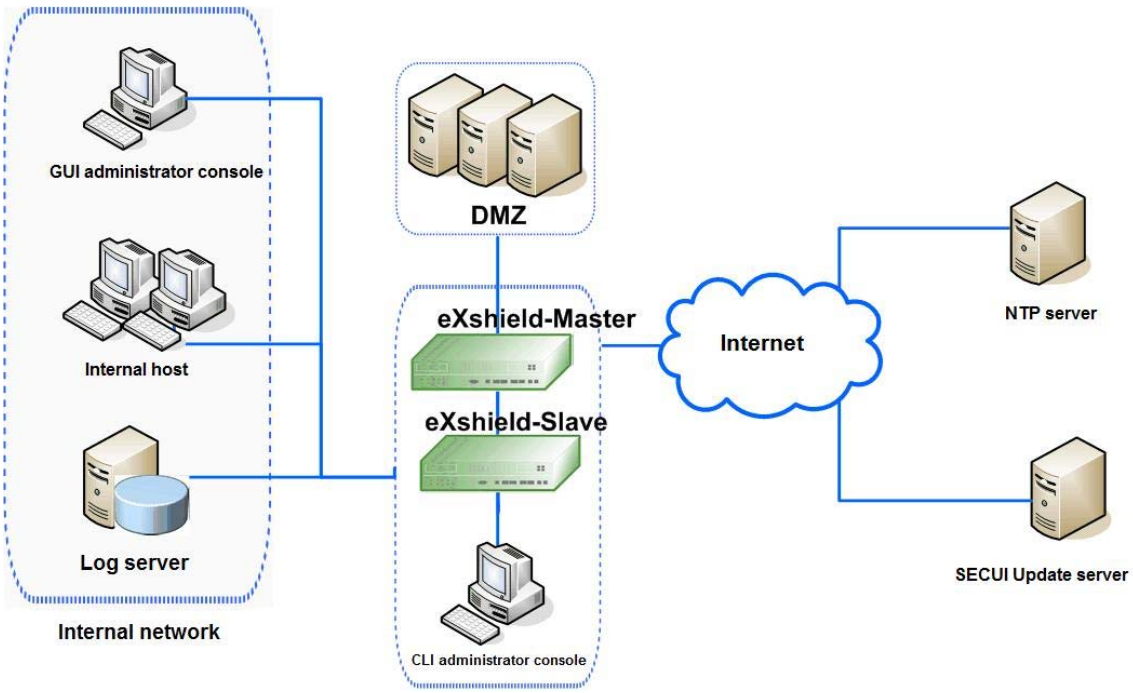
which connects directly to the serial port. The administrator can also manage the log server of eXshield Security Switch V1.0 by establishing an IP for connection to the log server through the CLI administrator console. The log server manager can perform the security management functions after accessing the log server that stores audit data of eXshield Security Switch V1.0.

eXshield Security Switch V1.0 is a distributed product, comprising one to perform network intrusion prevention and a log server to store audit data. Since the former does not have a hard disk in it, a log server accessible from an authorized administrator should be provided in the internal network to store all audit data created.

Intranet servers, DNS server, SMTP server, Web server, or FTP server will be in the DMZ, the network of which will be separated to protect the internal network.

For the protection against external attacks exploiting new vulnerabilities of the internal network, the administrator of eXshield Security Switch V1.0 updates and manages the Signature list on the vulnerabilities of the product using the update server.

The administrator ensures a sequential generation of audit data using time source provided by the NTP server or OS, which helps regular Signature update.



(Figure 2) Configuration of eXshield Security Switch V1.0: 2

eXshield Security Switch V1.0 is an intrusion prevention system that performs an access control and information flow control.

eXshield Security Switch V1.0 performs the access control function based on the packet filtering rule, which checks whether there is any policy that allows a subject to access information and whether a subject has the security level necessary to access information.

eXshield Security Switch V1.0 comprises of Master and Slave in HA mode, where kernels synchronize the session information and check operational state and roles to realize distributed load and HA. Master and Slave regularly check each other in operation through HA link. Slave synchronizes with Master every 1 minute and works on behalf of Master if necessary.

eXshield Security Switch V1.0 is comprised of hardware, OS, image(software). The OS is SecuiOS V1.2 developed by Secui.

6. Guidance

The TOE provides the following guidance documents.

- eXshield V1.0.1.R Administrator Guidance V1.5, 12 May 2008
- eXshield V1.0.1.R Installation Guidance V1.0, 8 Apr. 2008

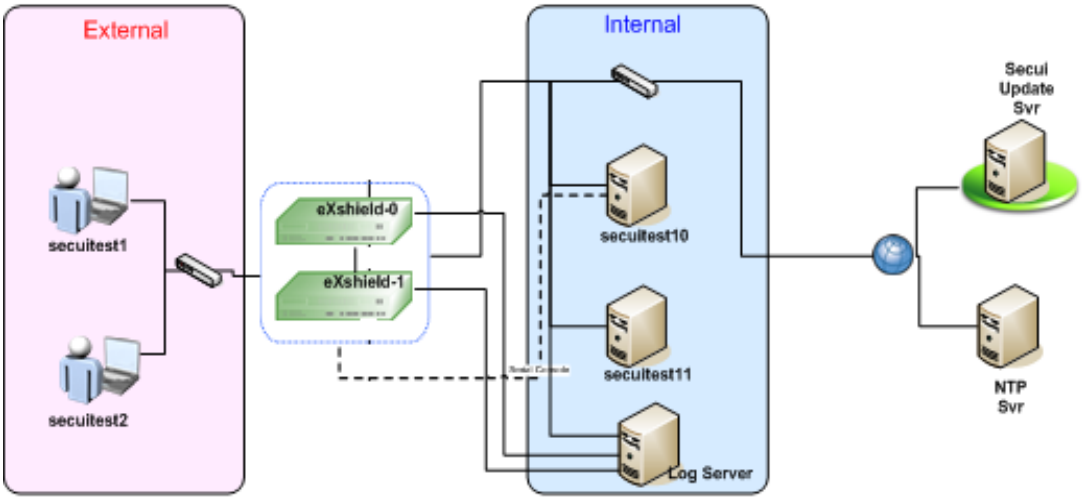
7. TOE Test

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.

(1) TOE test configuration

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



(Figure 3) Developer's test configuration

(2) Test method

The developer has configured the Master and Slave for testing and used an automated packet generation tool for the IPS Signature detection test.

(3) Analysis of test coverage / Low-level design test

Details regarding the coverage and low-level design test are given in the ETR.

(4) Test results

The test document describes expected result and actual result of each test. The actual results can be confirmed both on the screen of the TOE and by audit records.

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.

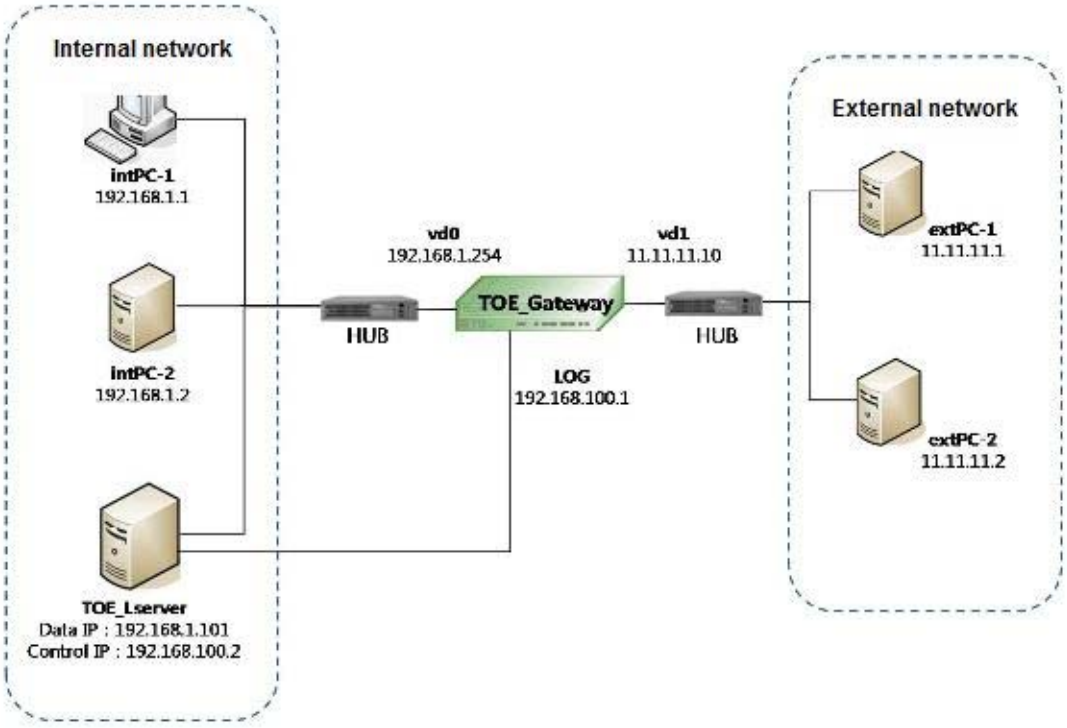
The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

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 4) below.



(Figure 4) Evaluator's test configuration

Evaluator's test tools

TOE_Gateway	CPU	XLR 732 1.2 GHz XLR 532 1.2 Ghz	-
	RAM	8 GB	
	CF Memory	2 GB	
	NIC	26 Ports (1 Gbps *24, 10/100/1000 Mbps *2)	
	OS	SecuiOS V1.2	

TOE_LServer	OS	RedHat Linux 4 Update 4	-
	CPU	1.0 GHz	
	RAM	1 GB	
	NIC	10/100 Mbps *2	
intPC-1	OS	Windows XP	-
	S/W	eXshield Manager	
	CPU	2.0 GHz	
	RAM	1 GB	
	NIC	10/100 Mbps	
intPC-2	OS	RedHat Linux 4 Update 4	-
	CPU	2.0 GHz	
	RAM	1 GB	
	NIC	10/100 Mbps	
extPC-1	OS	Windows Vista Home	-
	CPU	1.8 GHz	
	RAM	1 GB	
	NIC	10/100 Mbps	
extPC-2	OS	RedHat Linux 4 Update 4	-
	S/W	VMWare-workstation-6.0.3	
	CPU	1.8 GHz	
	RAM	1 GB	
	NIC	10/100 Mbps	
	S/W	VMWare-workstation-6.0.3	
	CPU	1.8 GHz	
	RAM	1 GB	
	NIC	10/100 Mbps	
Hub	Intel 24 Port *2		-

9. Evaluation result

The evaluation is performed with reference to the CC V2.3 and CEM V2.3. 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.

1) Security Target evaluation (ASE)

The ST introduction is complete and consistent with all other parts of the ST and gives a correct identification of the ST.

The TOE description describes the objectives and functionality of the TOE sufficiently to be understandable and is coherent, complete, internally consistent, and consistent with all other parts of the ST.

The TOE security environment provides a clear and consistent definition of the security problems that are induced in the TOE and its environment in terms of assumptions, threats, and OSP(organizational security policy)s.

The security objectives are categorized into those for the TOE and those for the environment. They counter the identified threats, achieve the identified OSPs, and are consistent with the identified assumptions.

The IT security requirements describe the security functional and assurance requirements completely and consistently, and provide an adequate basis for development of a TOE that will achieve its security objectives.

TOE summary specification defines correctly and consistently the security functions and assurance measures that satisfy the described TOE security functional requirements.

The PP claims correctly identify the PP to which the ST claims conformance and ensure that the operations uncompleted in the PP are completed in the ST.

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

2) Configuration management evaluation (ACM)

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.

3) Delivery and operation evaluation (ADO)

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.

The evaluator has confirmed that the procedures and steps for the secure installation, generation, and start-up of the TOE had been documented and resulted in a secure configuration.

Therefore, the delivery and operation documentation is adequate to ensure that the TOE is installed, generated, and started in the same way the developer intended it to be and that it is delivered without modification.

4) Development evaluation (ADV)

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 external interfaces to the TOE.

The high-level design describes the TSF in terms of subsystems, describes the interfaces to the subsystems, and correctly realizes the functional specification.

The low-level design describes the internal operation of the TSF in terms of internal modules. It describes the interrelationships and dependencies between the modules. It is sufficient to satisfy the functional requirements of the ST, and is a correct and effective refinement of the high-level design.

The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realization of the low-level design.

The representation correspondence shows that the developer has correctly and completely implemented the requirements of the ST in the functional specification, high-level design, low-level design, and implementation representation.

The security policy model clearly and consistently describes the rules and characteristics of the security policies and describes their correspondence to the security functions in the functional specification and the security functional requirements in the ST.

Therefore, the development documentation is determined adequate to understand how the TSF provides the security functions of the TOE, as it consists of a functional specification (which describes the external interfaces of the TOE), a high-level design (which describes the architecture of the TOE in terms of internal subsystems), a low-level design (which describes the architecture of the TOE in terms of internal modules), an implementation description (a source code level description), a representation correspondence (which maps representations of the TOE to one another in order to ensure consistency), and a security policy model (which describes the rules and characteristics of the security policies enforced by the TOE).

5) Guidance documents evaluation (AGD)

The administrator guidance describes how the TOE is securely administered by the administrator. Therefore, it gives a suitable description of how to administer the TOE.

6) Life cycle support evaluation (ALC)

The evaluator has confirmed:

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;

the developer had used a documented life-cycle model; and

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.

7) 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 functional specification and design documentation.

8) Vulnerability assessment evaluation (AVA)

The misuse analysis has confirmed that the guidance documentation had not been misleading, unreasonable, and conflicting, that secure procedures for all modes of operation had been addressed, and that the use of the guidance documentation had allowed insecure states of the TOE to be prevented and detected.

The evaluator has confirmed that the strength of TOE security function had been claimed for all probabilistic and permutational mechanism in the ST and the developer's SOF analysis had been correct.

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 performing penetration testing based on the evaluator's 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 a low attack potential in the intended TOE environment.

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

10. Recommendations

• The TOE may be administered through the Internet Explorer and eXshield Manager. For a safe security management of the TOE, the administrator is recommended to use the Internel Explorer V6.0 (or above) and install JRE V1.5.0_14 (or above).

• The configuration of the TOE that separates Master and Slave guarantees HA in case of a network circuit error. Therefore, it is recommended that the administrator operates the TOE in a distributed mode to provide HA.

• The TOE may not be able to generate an audit record in case that one of TOE_Gateway and TOE_LServer is reactivated until a new session will be established. Therefore, both TOE_Gateway and TOE_LServer need to be reactivated if reactivation is required to generate audit records.

• The TOE shall maintain the session between TOE_Gateway and TOE_LServer for a regular audit record generation, otherwise the audit record will not be transmitted to TOE_LServer. The administrator is therefore recommended to monitor on a regular basis the communication between TOE_Gateway and TOE_LServer to prevent audit data loss.

• The TOE provides a password method and OTP mechanism using S-Key method as a means for the I&A of administrator. For a secure I&A, OTP is recommended that changes PIN at every single access.

11. Acronyms and Glossary

The following acronyms and glossary are used in this report:

(1) Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OR	Observation Report
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

(2) Glossary

HA(High Availability)

To protect an application from any failure on the components of CPU, HDD, and network and ensure continuous services in the operational environment

KLSM

A subsystem implemented on the IP Layer among the Network Stacks, which performs the validity check of a packet, access control, and intrusion detection

NAT(Network Address Translation)

A technique of exchanging a specific IP address in an internal network and a public IP address

Secui Update server

This server under the in-house management of SECUI does update of IPS Signature list and ICEC list

Administrator console

Helps administer the TOE; Includes a GUI administrator console that can access the TOE through the Internet explorer or eXshield Manager and a CLI administrator console that can directly connect with the TOE through a serial port.

Static access control

Applied based on the access control rules generated by an authorized administrator on the GUI administrator console when a subject accesses an object

MAC

A subject is allowed to access an object only when its security level is same as or higher than that of the object

12. Reference

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

[1] Common Criteria for Information Technology Security Evaluation (21 May 2005)
[2] Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)
[3] Korea IT Security Evaluation and Certification Guidance (21 May 2005)
[4] Korea IT Security Evaluation and Certification Scheme (1 Dec. 2007)
[5] eXshield V1.0.1.R Security Target V1.10 (19 May 2008)
[6] eXshield V1.0.1.R Evaluation Technical Report, V1.00 (22 May 2008)