KECS-CR-07-06

Certification Report on
SafezoneIPSⓤ V1.0(SZ5XU) of LG N-Sys

Certification No. : KECS-NISS-0065-2007

Apr. 2007

National Intelligence Service

IT Security Certification Center

This document is the certification report on SafezoneIPS ⓤ V1.0(SZ5XU) of LG N-Sys..

Certification Body

National Intelligence Service IT Security Certification Center

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Overview

This report is for the certification body to describe the certification result, which inspects the results of the EAL4 evaluation of SafezoneIPSⓤ V1.0(SZ5XU) with regard to the Common Criteria for Information Technology Security Evaluation (Notification No. 2005-25 of the Ministry of Information and Communication; "CC" hereinafter).

The Korea Information Security Agency(KISA) has finished the evaluation of the SafezoneIPSⓤ V1.0(SZ5XU) on Mar. 19, 2007. This report is written based on the Evaluation Technical Report(ETR) produced and provided by KISA. The evaluation concludes that the TOE satisfies the CC part 2 and EAL4 of the CC part 3 assurance requirements; thus, it is assigned the verdict "pass" on the basis of the paragraph 191 of the CC part 1. In addition, the TOE satisfies the Network Intrusion Prevention System Protection Profile V1.1 (Dec.21, 2005).

SafezoneIPSⓤ V1.0(SZ5XU) is an intrusion prevention system which performs intrusion detection and intrusion prevention function. It is installed in In-Line mode, and can be managed by CLI and GUI. It provides security functions such as:

- Intrusion detection and reaction
- Identification and authentication of the administrator
- Identification and authentication of node in case of internal communication
- Integrity check on executable files and configuration files
- Security management and audit log
- New policy online update
- Time synchronization
- Report on intrusion detection result

The certification body has examined the evaluation activities and testing procedures, provided the guidance regarding the technical problems and evaluation procedures, and reviewed each evaluation work package and evaluation technical report. In conclusion, the certification body has confirmed that the evaluation results gave assurance that the TOE meets all security functional requirements and assurance requirements described in the

Security Target(ST). As a result, the certification body has certified that the evaluator's observations and evaluation results were accurate and reasonable, and his verdict on each work package was correct.

Certification Validity : The information contained in this certification report does not mean that the use of SafezoneIPSⓤ V1.0(SZ5XU) is approved or its quality is guaranteed by governmental agency of the Republic of Korea.

2. TOE Identification

The [Table 1] summarizes the information of the TOE identification.

[Table 1] TOE Identification

Evaluation Guidance	Korea IT Security Evaluation and Certification Guidance (May 21, 2005) Korea IT Security Evaluation and Certification Scheme (Jan. 1, 2007)
Evaluation product	SafezoneIPSⓤ V1.0(SZ5XU)
TOE	SafezoneIPSⓤ V1.0(SZ5XU)
Protection Profile	Network Intrusion Prevention System PP V1.1 (2005. 12. 21)
Security Target	SafezoneIPSⓤ V1.0(SZ5XU) ST V1.00.03 (2007. 3. 14)
ETR	SafezoneIPSⓤ V1.0(SZ5XU) ETR V1.0 (2007. 3. 19)
Evaluation Result	Satisfies the CC part 2 Satisfies the EAL4 of the CC part3 assurance requirements
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V2.3 (Aug. 2005)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)
Sponsor	LG N-Sys
Developer	LG N-Sys
Evaluation Team	KISA IT Security Evaluation Center, Evaluation Team I NamGyun Baek, Eunjoo La
Certification Body	National Intelligence Service

Specification of system is like as [Table 2].

[Table 2] SafezoneIPSⓤ V1.0(SZ5XU) System Specification

Category		Specification
SafezoneIPSⓤ Engine	CPU	Pentium IV 3.0Ghz or more
	Memory	512MB or more
	Interface	NIC 1 Port(for 10/100/1000M) or more Serial 1 port
	HDD	80GB or more
	OS	Dedicated OS(SZOS V1.1)
SafezoneIPSⓤ Management Console	CPU	2.4Ghz 1 or more
	Memory	1GB or more
	Interface	NIC 1 Port 1 or more
	HDD	72GB * 1 or more
	OS	Windows XP Professional

3. Security Policy

The TOE operation conforms to the security policies stated below:

Name	Description
Audit Record	Every security-relevant event should be recorded and saved to make it possible to trace the responsibility of every action; the recorded data should be reviewed.
Security Management	Only an authorized administrator who accesses through trusted communication can use the security management function.

4. TOE Assumptions and Scope

4.1 Assumptions

The TOE installation and operation should conform to the assumptions stated below:

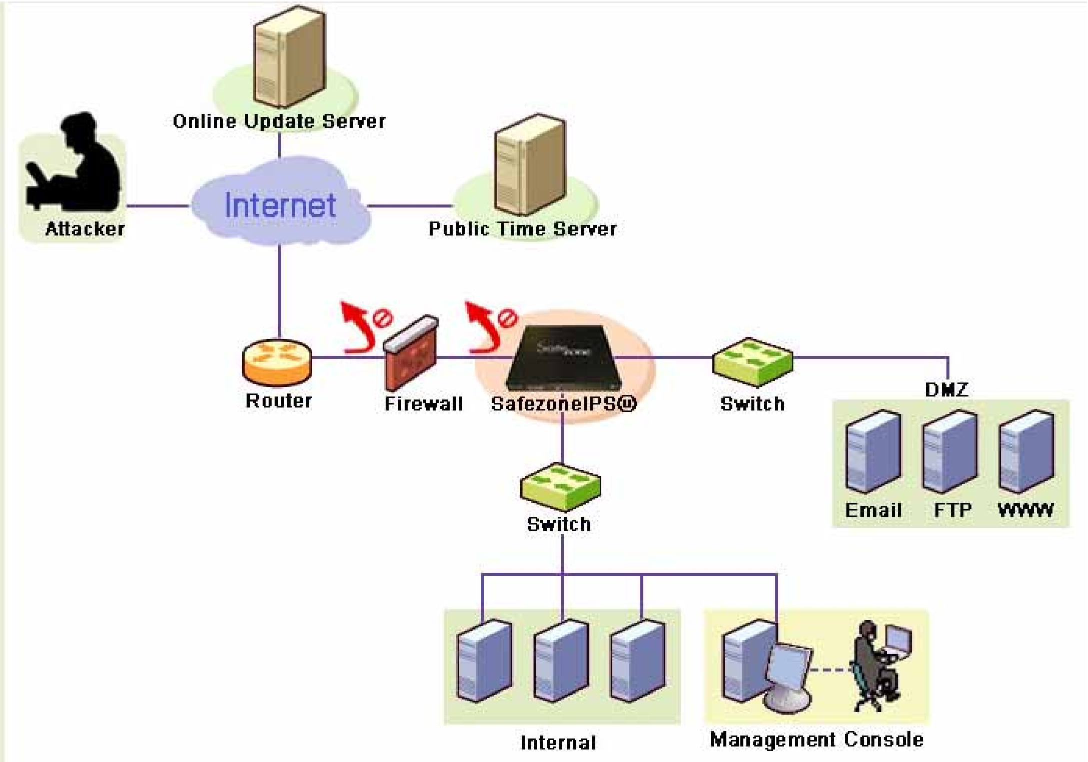
Name	Description
A.Physical Security	The TOE is located in physically secure environment where only authorized administrators are allowed the access.
A.Security Maintenance	When the internal network environment is changed due to network configuration changes, an increase or decrease of hosts, or an increase or decrease of services, the new changes are immediately noted and security policies are configured in accordance with the TOE operational policy to maintain the same level of security as before.
A.Trusted Administrator	An authorized administrator of the TOE possesses no malicious intention, is adequately educated, and performs his/her duties in accordance with the administrative guideline.
A.Hardened OS	The underlying OS of the TOE ensures the reliability and stability by both eliminating the unnecessary services or means not required by the TOE and installing the OS patches.
A.Single Connection Point	The TOE is installed and operated on a network and separates the network into external and internal network. Information can not flow between the two without passing through the TOE.
A.Reliable TIMESTAMP	To keep reliable TIMESTAMP function, NTP Server(Public Time Server) provides TOE with reliable TIMESTAMP. If TOE cannot get time information from Public Time Server, TOE get time information from system
A.Secure Update Server	Secure Update Server provides TOE with the latest attack rule, so TOE can keep the latest attack rule.
A.Secure Database	TOE can save, search and keep audit log through secure database.

4.2 Scope to Counter a Threat

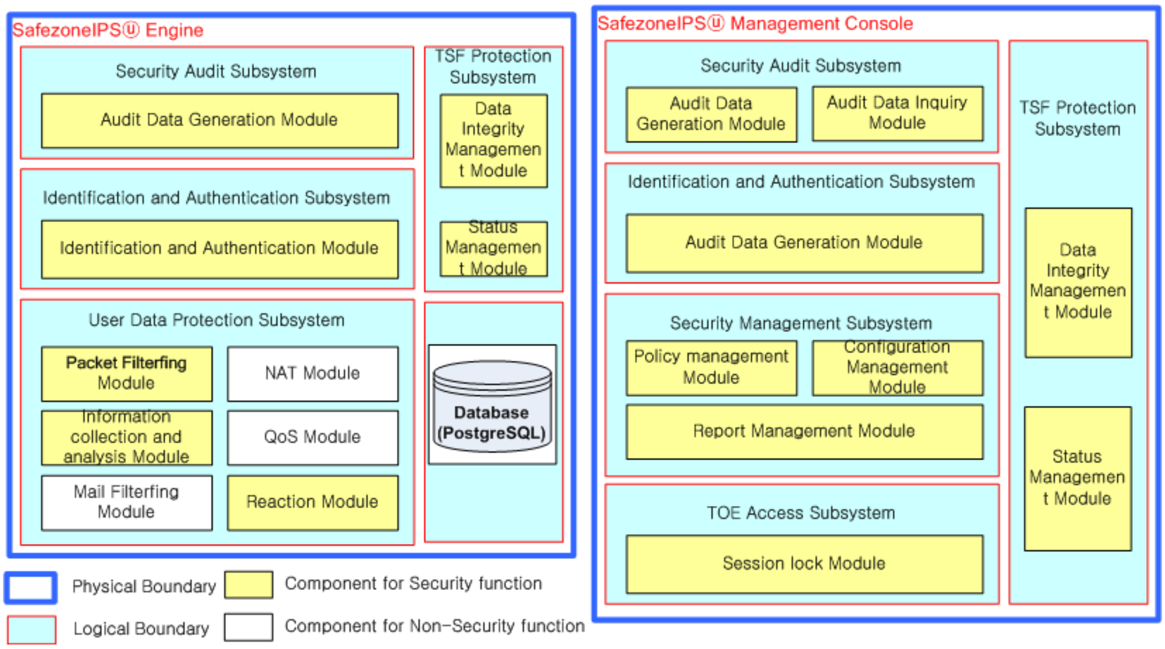
The TOE provides a means to counter a threat that is appropriate for the IT environment which requires rigorous control on the network traffic. Although the TOE does not have a countermeasure for a direct physical attack which disables or bypasses security functions, it provides a countermeasure for a logical attack occurred within its network by threat agents possessing medium-level expertise, resources, and motivation. It also provides a countermeasure for an attack by an entity which disguises itself as an authorized administrator, an attack to exhaust the audit storage, or a service attack, abnormal packet attack. In addition, the TOE provides a countermeasure to counter a consecutive authentication attempt, a bypass attack, and unauthorized modification of the TSF data.
All security objectives and security policies are described to provide a means to counter an identified security threat.

5. TOE Information

The TOE provides an intrusion prevention function. The figure below shows the operational environment of the TOE.



[Figure 1] TOE operational environment


SafezoneIPS® Engine
Security Audit Subsystem
Audit Data Generation Module
Identification and Authentication Subsystem
Identification and Authentication Module
User Data Protection Subsystem
Packet Filterfing Module
NAT Module
Information collection and analysis Module
QoS Module
Mail Filterfing Module
Reaction Module
TSF Protection Subsystem
Data Integrity Management Module
Status Management Module
Database (PostgreSQL)
SafezoneIPS® Management Console
Security Audit Subsystem
Audit Data Generation Module
Audit Data Inquiry Module
Identification and Authentication Subsystem
Audit Data Generation Module
Security Management Subsystem
Policy management Module
Configuration Management Module
Report Management Module
TOE Access Subsystem
Session lock Module
TSF Protection Subsystem
Data Integrity Management Module
Status Management Module
Physical Boundary
Component for Security function
Logical Boundary
Component for Non-Security function

[Figure 2] Structure of TOE

The TOE consists of 6 subsystems stated below:

•Security Audit Subsystem

Security Audit Subsystem generates audit data, and provides search function of detection/prevention log and audit log.

•User data protection Subsystem

User data protection Subsystem performs access control against packet based on header to protect network from external attacker. And if needed, it performs harmful site blocking, collecting information for detection/prevention, reacting against potential security violation, storing analysis result so that the administrator can check.

•Identification and authentication Subsystem

Only the authorized users may use the TOE system. Identification and authentication of a user are carried out by the following two methods.

- User Identification and authentication function
- Mutual identification and authentication between TOE components during remote connection through the communication channel (Management console ↔ Engine)

•Security Management Subsystem

The security management function of the TOE system is provided through the Management Console GUI interface. The authorized administrator can perform the function through GUI to ensure continuous operation of the TOE.

•TSF protection Subsystem

TSF Protection provides a regular check function to assure that the TSF is properly operating. It performs checking the main component running on the TOE system when initially started, periodically during normal operation. In case of abnormal operation, it executes the function of a component again. And it protects the TOE data and functions by checking the integrity of TOE data and programs.

•TOE Access Subsystem

If the TOE is accessed by an authorized administrator but remains inactive for a certain period of time, the interacting session will be locked on the basis of the identification and authentication in order to protect the TOE during the time.

6. Guidance

The TOE provides the following guidances:

- afezoneIPS V1.0(SZ5XU) Administrator Guidance_20060811_V1.00.01
- afezoneIPS V1.0(SZ5XU) Delivery Document_20070130_V1.00.03
- afezoneIPS V1.0(SZ5XU) Installation Manual_200600811_V1.00.01

7. TOE Test

7.1 Developer's Test

- Test Method

The developer produced the test considering the security function of the TOE. Each test is described in test documentation including the following items in detail:

- Test No./Tester : The identifier of the test and the developer who participated in testing
- Purpose of the test : Describes the purpose of the test including security function and security module to be tested
- Test configuration : Detailed environment where the test is carried out
- Detailed test procedure : Detailed procedure to test security functions
- Expected result : Test result expected when performing the test procedure
- Actual result : Test result acquired when the test is performed
- Comparison of the expected result and the actual result : Result of comparison of the expected result and the actual result

The evaluator performed an evaluation of the validity such as the test configuration, test procedure, test scope analysis, and the low-level design test. The evaluator verified that the developer's test and its results were adequate for the evaluation configuration.

- Test configuration

The test configuration described in the test documentation includes the detailed configuration such as the organization of network for the test, the TOE, PC and the server. In addition, it describes detailed test configuration such as test tools required to perform each test.

- Test Scope Analysis/Low-Level Design Test

The detailed evaluation results are described in the ATE_COV and ATE_DPT evaluation result.

- Test Result

The test documentation describes the expected result and actual result of each test. The actual result is confirmed through the audit record as well as the GUI of the TOE..

7.2 Evaluator's Test

The evaluator installed the TOE using the evaluation configuration and evaluation tools identical to those of the developer test and performed testing for the overall tests provided by the developer. The evaluator confirmed that the actual result of every test was consistent with the expected result.

Moreover, the evaluator devised and performed additional evaluator's tests on the basis of the developer's test, and confirmed that the actual test result was consistent with the expected test result.

The evaluator carried out the vulnerability test and confirmed that there was no exploitable vulnerability in the evaluation configuration.

The evaluator's test result assured that the TOE worked normally as described in the design documentation.

8. Evaluation Configuration

The network configuration for the evaluation is separated into the internal and external network. The following information is about the hardware used for the evaluation configuration:

- Computer : 9 sets(PC : 5, Server : 4)
- CPU : More than Intel Pentium 3 1.8GHz
- RAM : More than 512MB
- HDD : More than 80GB

The following information is about the software used for the evaluation configuration:

- Linux 7.0
- Windows 2003 Server
- Windows XP Professional
- Windows 2000 Professional

All security functions provided by the TOE are included in the scope of evaluation. The evaluation configuration is based on the detailed security attributes and configuration of each security function.

9. Evaluation Result

The evaluation is on the basis of the Common Criteria for Information Technology Security Evaluation, Common Methodology for Information Technology Security Evaluation. It concludes that the TOE satisfies the CC part 2 and EAL4 of the CC part 3 assurance requirements. The detailed information regarding the evaluation is described in the ETR.

- ST Evaluation (ASE)

The evaluator applied the ASE sub-activities described in the CEM to the evaluation of the ST of the TOE. The ST introduction is complete and consistent with other parts of the ST, and correctly identifies the ST.
The TOE description contains relevant information to aid the understanding of the purpose of the TOE and its functionality, and is complete, internally consistent, and consistent with other parts of the ST.
The TOE security environment in the ST clearly and consistently defines the assumptions, threats, and organizational security policies related to the security problem that the TOE and its environment are intended to address, and is described completely and consistently. The security objectives counter the identified threats, achieve the organizational security policies, and satisfy the stated assumptions.
The IT security requirements (both the TOE security functional requirements and the TOE security assurance requirements) and the security requirements for the IT environment are described completely and consistently and provide an adequate basis for the development of a TOE that will achieve its security objectives. The TOE summary specification provides a clear and consistent definition of the security functions and assurance measures and satisfies the specified TOE security requirements. The ST is a correct instantiation of any PP for which compliance is being claimed.
Thus, the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

- Configuration Management Evaluation (ACM)

The evaluator applied the ACM sub-activities described in the CEM to the evaluation of the configuration management of the TOE.

The configuration management documentation includes configuration list, how to identify configuration, how to give a version, how to control configuration modification. All development document and source files are developed with configuration management method, and generation and modification of configuration items are controlled by configuration management organization and configuration management system.

- Delivery and Operation Evaluation (ADO)

The evaluator applied the ADO sub-activities described in the CEM to the evaluation of the delivery and operation of the TOE. The delivery documentation describes all procedures used to maintain the security of the TOE and detect modification or substitution of the TOE when distributing the TOE to the user's site. The procedures and steps for the secure installation, generation, and start-up of the TOE have been documented, which ensures a secure configuration of the TOE.
Thus, 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 and that it is delivered without modification.

- Development Evaluation (ADV)

The evaluator applied the ADV sub-activities described in the CEM to the evaluation of the development of the TOE. The functional specification adequately describes all security functions of the TOE and explains that the security functions of the TOE are sufficient to satisfy the security functional requirements in the ST.
The security policy modeling clearly and consistently describes the rules and characteristics of the security policies; this description corresponds with the security functions described in the functional specification.

- Guidance Evaluation (AGD)

The evaluator applied the AGD sub-activities described in the CEM to the evaluation of the guidance of the TOE. The administrator guidance describes how to access to security management interface and how to administer the TOE in a secure manner. Thus, the guidance documentation adequately describes how to use the TOE in a secure manner. And TOE does not require user guidance as assurance requirements, so user guidance is not evaluated.

- Life Cycle Support Evaluation (ALC)

The evaluator applied the ALC sub-activities described in the CEM to the evaluation of the life cycle support of the TOE. The life cycle support adequately describes the procedures which the developer uses during the development and maintenance of the TOE, including the security procedures and tools used in the development of the TOE. Development environment is the same with already evaluated product, so result of previous actual inspection is applied.

- Test Evaluation (ATE)

The evaluator applied the ATE sub-activities described in the CEM to the evaluation of the test of the TOE. The testing is sufficient to establish that the TSF has been systematically tested against the functional specification.
The evaluator confirmed that the developer had tested the TSF against its high-level design. The developer's functional test documentation is sufficient to demonstrate that the security functions perform as specified.
The evaluator confirmed that the TOE behaved as specified by performing independent testing of a subset of the TSF and gained confidence in the developer's test results by performing entire developer's tests.
Thus, by performing independent testing of a subset of the TSF, the evaluator confirmed that the TSF behaved in accordance with the TOE security functional requirements stated in the ST and the design documentation.

- Vulnerability Assessment Evaluation (AVA)

The evaluator applied the AVA sub-activities described in the CEM to the evaluation of the vulnerability assessment of the TOE.
The vulnerability analysis document describes the identified vulnerabilities of the TOE and appropriate countermeasures, for example, by specifying operational environment in the functional specification or guidance documents. The evaluator confirmed the accuracy of the vulnerability analysis by conducting independent vulnerability analysis. It is confirmed that the SOF claims are made for all probabilistic or permutational mechanisms in the ST and that the analysis of the developer's SOF claims is correct.

10. Recommendations

- Dynamic attack policy, which detects attack in accordance with the threshold value setup, may require some time for the application of a rule, which in turn may cause the incoming of an attack packet into the internal network. Thus, an adequate threshold value needs to be set through a tuning process regarding the traffic property of the internal network.
- TOE provides the administrator alarm function which works when it reaches the threshold due to the audit record storage exhaustion. However, the administrator should not depend solely on the alarm function but continuously check the usage of storage space and secure enough audit record storage space.
- Traffic bottleneck can be generated by the limit of hardware specification in case of hundreds of traffic processing, administrator should assure operation of TOE security function through load balancing.
- TOE provides live update function to update intrusion detection pattern when new vulnerability is found. Administrator should maintain the latest security violation event list by periodical update.

11. Acronyms and Glossary

The following acronyms are used in this certification report..

(1) Acronyms

EAL	Evaluation Assurance Level
SOF	Strength of Function
TOE	Target of Evaluation
TSF	(TOE Security Functions

(2) Glossary

TOE
An IT product or system and its associated guidance documentation that are the subject of evaluation

Audit record
Audit data to save an auditable event relevant to the security of the TOE

User
Any entity (either human or external IT entity) outside the TOE that interacts with the TOE

Authorized administrator
Authorized user that can manage the TOE in accordance with the TSP

Authorized user
User that can run functions of the TOE in accordance with the TSP

Identity
A representation uniquely identifying an authorized user

Authentication data
Information used to verify the claimed identity of a user

External IT entity
Any IT product or system, either trusted or untrusted, outside the TOE that interacts with the TOE

Assets
Information and resources to be protected by the security measures of the TOE

12. Reference

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

[1] Common Criteria for Information Technology Security Evaluation (May 21, 2005)
[2] Common Methodology for Information Technology Security Evaluation V2.3
[3] Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005)
[4] Korea IT Security Evaluation and Certification Guidance (May 21, 2005)
[5] Korea IT Security Evaluation and Certification Scheme (Jan 1, 2007)
[6] SafezoneIPS⓾ V1.0(SZ5XU) Security Target_20070314_V1.00.04
[7] SafezoneIPS⓾ V1.0(SZ5XU) Evaluation Technical Report V1.0 (Mar,3, 2007)