KECS-CR-05-23

Certification Report V1.0 on SafezoneIPS V3.0(SZ-4000) of LG N-Sys

Certification No. : KECS-NISS-0050-2006

Aug. 2006

National Intelligence Service
IT Security Certification Center

This document is the certification report on SafezoneIPS V3.0(SZ-4000) 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 V3.0(SZ-4000) 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 V3.0(SZ-4000) on Dec. 9, 2005. 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 V2.2 part 2 and EAL4 of the CC V2.2 part 3 assurance requirements; thus, it is assigned the verdict "pass" on the basis of the paragraph 175 of the CC V2.2 part 1. In addition, the TOE satisfies the Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005).

SafezoneIPS V3.0(SZ-4000) is an intrusion prevention system that is installed on the single connection point on which the internal and external network are separated and detects and prevents any attack from every passing network traffic and notifies the administrator about the attack. It provides security functions such as:

- Intrusion detection and solution
- Identification and authentication of the administrator
- Integrity check on executable files and configuration files
- Security management functions: Establishment, inquiry, and modification of the security attributes
- Audit record and availability function

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 V3.0(SZ-4000) 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 (May 7, 2005)
TOE	SafezoneIPS V3.0(SZ-4000)
Protection Profile	Network Intrusion Prevention System PP V1.1 (Dec. 21, 2005)
Security Target	SafezoneIPS V3.0(SZ-4000) ST V1.00.02 (Dec. 5, 2005)
ETR	SafezoneIPS V3.0(SZ-4000) ETR, V1.01 (Dec. 9, 2005)
Evaluation Result	Satisfies the CC V2.2 part 2 Satisfies the EAL4 of the CC V2.2 part 3 assurance requirements
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (May 21, 2005) Final Interpretation (Jun. 2005)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.2 Final Interpretation (Jun. 2005)
Sponsor	LG N-Sys
Developer	LG N-Sys
Evaluation Team	KISA IT Security Evaluation Center, Evaluation Team II Soontai Park, Sungsoo Ahn, Seunghwan Lee, Kyuchul Song, Sungjae Lee(Evaluation Team I)
Certification Body	National Intelligence Service

SafezoneIPS V3.0(SZ-4000) is an appliance that requires the system specification as stated in the [Table 2].

[Table 2] SafezoneIPS V3.0(SZ-4000) System Specification

Category		Specification
SafezoneIPS Engine	CPU	Intel 2.8GHz * 2
	Memory	4GB
	Interface	2 Service ports (for Giga) * 2 2 Administration ports (one for 10/100, the other for 1000)
	HDD	73 GB
	OS	SZOS V1.0 (Dedicated OS)
Administrator Console	CPU	2.4GHz * 1 or more
	Memory	1 GB or more
	Interface	2 ports or more
	HDD	72GB * 2 or more
	OS	Version of or later than MS Windows 2000
	Data Management	Version of or later than MS SQL Server 2000

3. Security Policy

The TOE operation conforms to the security policies stated below:

Intrusion Prevention

The TOE should block the access of a host which attempts to intrude.

Identification & Authentication

The administrator should pass through the process of identification and authentication before using the security functions of the TOE.

Integrity Check

Principal TOE files such as an executable file or configuration file should checked regularly by the integrity check function to detect any unauthorized modification.

Security Management

Only an authorized administrator who accesses through trusted communication can use the security management function.

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.

4. TOE Assumptions and Scope

4.1 Assumptions

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

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.Secure TOE External Server

The network time protocol (NTP) server which maintains a trusted time outside the TOE for security functions of the TOE and the update server which provides the latest attack pattern rules are secure.

A.TIME

The IT environment of the TOE is provided with a reliable Timestamp from the NTP server which conforms to RFC 1305 or from the OS.

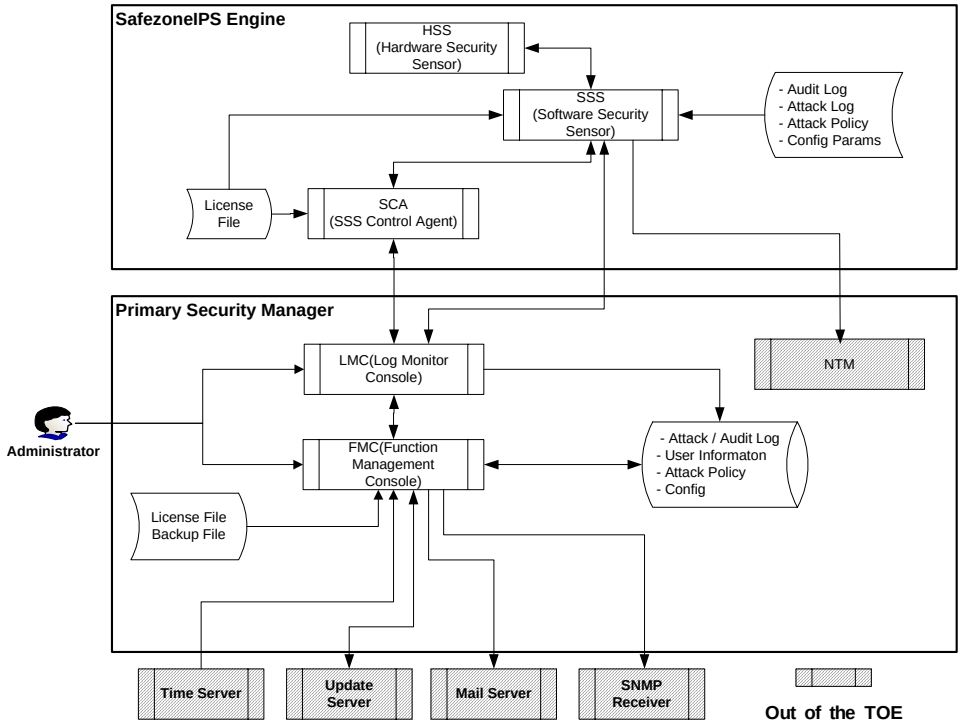
4.2 Scope to Counter a Threat

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 structure of the TOE.



The TOE consists of the major subsystems stated below:

- Hardware Security Sensor (SY_HSS)

Checks every incoming packet and blocks or transfers it according to the security policy set by the administrator; performs functions such as collecting information on the intrusion detection events, integrity attack detection, static attack detection, detailed prevention, and applying prevention exception.

- Software Security Sensor (SY_SSS)

Operates and controls HSS and transmits data from HSS to console; performs the second filtering; detects a dynamic attack(e.g. DoS) and an abnormal traffic RateLimit attack; generates an intrusion detection log and HSS operational log.

- Software Security Sensor Control Agent (SY_SCA)

Controls the operations of the SSS including start-up, stop, and status check; checks SSS periodically and restarts it in case of an abnormal termination.

- Log Management Console (LMC)

A MS Windows-based GUI application which displays on screen an intrusion log received from an engine interface and SSS.

- **Function Management Console (FMC)**

Manages security attributes such as audit log, users, and security policy; performs identification and authentication of an administrator, integrity check, and backup.

6. Guidance

The TOE provides the following guidances:

- SafezoneIPS V3.0(SZ-4000) Installation Manual Version 1.00.01, Dec. 5, 2005
- SafezoneIPS V2.0(SZ-4000) Administrator Guidance Version 1.00.02, Dec. 5, 2005

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 the application sever(e.g. web server, mail server, etc.) and 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 : 6 sets (for internal · external computer and for the administrator console)

- CPU : More than 1.5GHz
- RAM : More than 512MB
- Hard disk : More than 10GB

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

- SUSE Linux 8.2
- Windows 2000 server, XP

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 V2.2, and the Final Interpretation (Jun. 2005). It concludes that the TOE satisfies the CC V2.2 part 2 and EAL4 of the CC V2.2 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 V2.2 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 V2.2 to the evaluation of the configuration management of the TOE.

The evaluator confirmed the following through an examination of the configuration management documentation:

- The developer controls changes of the implementation representation with the support of automated tools.

- The developer has clearly identified the TOE and its associated configuration items; the ability to modify these items is properly controlled.

- The developer performs configuration management on, at a minimum, the TOE implementation representation, the evaluation evidence required by the assurance components in the ST, and security flaws.

Thus, the configuration management documentation assists the consumer in identifying the evaluated TOE, and ensures that the configuration items are uniquely identified and that the procedures used by the developer to control and track changes of the TOE are adequate.

- Delivery and Operation Evaluation (ADO)

The evaluator applied the ADO sub-activities described in the CEM V2.2 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 V2.2 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.

The high-level design describes the TSF in terms of subsystems, major TOE structural units, and adequately explains the interfaces to the subsystems. It is a correct realization of the functional specification.

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

The implementation representation is sufficient to satisfy the functional requirements in 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 in the ST into the functional specification, high-level design, low-level design, and implementation representation.

Thus, the following design documentations are adequate to aid understanding how the TSFs are provided: the functional specification which describes the external interfaces to the TOE; the high-level design which describes the architecture of the TOE in terms of internal subsystems; the low-level design which describes the architecture of the TOE in terms of internal modules; the implementation representation in the form of source code-level description; and the representation correspondence which maps representations of the TOE to one another in order to ensure consistency.

- Guidance Evaluation (AGD)

The evaluator applied the AGD sub-activities described in the CEM V2.2 to the evaluation of the guidance of the TOE.

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

Thus, the guidance documentation adequately describes how to use the TOE in a secure manner.

- **Life Cycle Support Evaluation (ALC)**

The evaluator applied the ALC sub-activities described in the CEM V2.2 to the evaluation of the life cycle support of the TOE.

The evaluator confirmed that the developer's control on the security of the development environment was adequate to provide the confidentiality and integrity of the TOE design and implementation that are necessary to ensure secure operation of the TOE; that the developer had used a documented life-cycle model of the TOE; and that the developer had used well-defined development tools that yield consistent and predictable results.

Thus, 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.

- **Tests Evaluation (ATE)**

The evaluator applied the ATE sub-activities described in the CEM V2.2 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 V2.2 to the evaluation of the vulnerability assessment of the TOE.

From the misuse analysis, it is confirmed that the guidance is not misleading, unreasonable, or conflicting; that secure procedures for all modes of operation have been addressed; and that the use of the guidance will facilitate prevention and detection of insecure TOE state.

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.

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.

From the vulnerability analysis, it is confirmed that the TOE, in its intended environment, has no vulnerability exploitable by attackers possessing low attack potential.

Thus, based upon the developer/evaluator's vulnerability analysis and the evaluator's penetration testing, it is confirmed that there are no flaws or weaknesses of the TOE that are exploitable in its intended environment.

10. Recommendations

- SafezoneIPS V3.0(SZ-4000) has a certain administrator password, which must be changed after the installation has finished.
- 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.
- Live update function is available to ensure the latest security violation event list. It is efficient to set time where the network traffic is relatively small (e.g. weekend, late hour, etc.) as the update time.
- SafezoneIPS V3.0(SZ-4000) 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.

11. Acronyms and Glossary

The following acronyms are used in this certification report.

CR	Certification Report
EAL	Evaluation Assurance Level
IT	Information Technology
KECS	Korea IT security Evaluation and Certification Scheme
TOE	Target of Evaluation

The following terms are used in this certification report.

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

Intrusion prevention system
IT product to detect and block an attack from outside so the network to be protected (i.e. internal network) can be safe from attack

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 V2.2
[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 (May 7, 2005)
[6] SafezoneIPS V3.0(SZ-4000) Security Target V1.00.02 (Dec. 5, 2005), LG N-Sys
[7] SafezoneIPS V3.0(SZ-4000) Evaluation Technical Report V1.01 (Dec 9, 2005)