KECS-CR-2005-04

Network Intrusion Prevention System Protection Profile V1.1 Certification Report

Certification No. : CC-20-2005.12

12, 2005

National Intelligence Service

This document is the certification report for Network Intrusion Prevention System Protection Profile V1.1.

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Summary

This report describes the certification results by the certification body on the evaluation results applied with requirements of APE(Protection Profile Evaluation) Class of Common Criteria for Information Security Evaluation (‘CC’ hereinafter) in relation to [Network Intrusion Prevention System Protection Profile V1.1]. This report describes the evaluation result and its soundness and confirmity.

The evaluation on [Network Intrusion Prevention System Protection Profile V1.1] was conducted by Korea Information Security Agency and completed on April 30, 2005. Contents of this report have been prepared on the basis of the contents of the ETR submitted by Korea Information Security Agency. The evaluation was conducted by applying CEM. This PP satisfies all APE requirements of the CC, therefore the evaluation results were decided to be ‘suitable’.

[Network Intrusion Prevention System Protection Profile V1.1] is installed and operated in the form of In-line at the point of connection between Internet and internal network in order to securely protect information assets and resources of internal network. Also, it provides the functions to detect and block the intrusion and attack by abnormal traffic. Major functions of the TOE are as follows:

• Detects and blocks off abnormal traffic flowed from Internet network into internal network, therefore securely protects information assets and resources of internal network.

Information Flow Control Policies
- Deny policy(FDP_IFC.1(1)): Deny all access with the exception of explicitly allowed rules - Allow policy(FDP_IFC.1(2)) : Allow all access with the exception of explicitly block off rules

• The TOE blocks off attacks that exploit computer system vulnerabilities as much as possible and handles new/transformed attacks by updating vulnerability information.

Network DoS Attack Blocking
- Define maximum quotas per user of the protected resources (FRU_RSA.1)

• The TOE monitors and processes all traffics flowed from the outside to the inside. Therefore, the TOE shall be ensured of high-performance processing and high availability to withstand fault occurrence.

TOE Availability Ensure
- Maintain secure state at breakdown occurrence (FPT_FLS.1) - Maintain core security functions at breakdown occurrence (FRU_FLT.1)

The CB(Certification Body) has examined the evaluation activities, provided the guidance for the technical problems and evaluation procedures, and reviewed each WPR(Work Package Report), OR(Observation Report) and ETR(Evaluation Technical Report). The CB confirmed that this PP is complete, consistent and technically sound through the evaluation results. Therefore, the CB certified that observation and evaluation results by evaluator are accurate and reasonable.

Certification validity: Information in this certification report does not guarantee that [Network Intrusion Prevention System Protection Profile V1.1] is permitted use or that its quality is assured by the government of Republic of Korea.

2. Information for Identification

[Table 1] shows information for the PP identification.

[Table 1] Shows Information for the PP Identification

Scheme	Korea evaluation and certification guidelines for IT security (MIC, May. 2005) Korea Evaluation and Certification Scheme for IT Security(NIS, Jan. 2005)
TOE	Network Intrusion Prevention System Protection Profile V1.1
ETR	IPS-ETR-V1.00
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25, 2005. 5.)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation v2.3
Sponsor	Korea Information Security Agency
Developer	Korea Information Security Agency
Evaluator	IT Security Evaluation Division, CC Evaluation Lab, Korea Information Security Agency W. S. Hong, Y. J. Yu
Certification body	National Intelligence Service

3. Security Policies

The TOE of [Network Intrusion Prevention System Protection Profile V1.1] shall comply with the following Organizational Security Policies.

P. Audit	To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained. Also, the recorded data shall be reviewed.
P. Secure Management	The Authorized administrator shall manage the TOE in a secure way.

4. Assumptions and Scope

4.1 Assumptions

The TOE of [Network Intrusion Prevention System Protection Profile V1.1] shall be installed and operated with the following assumptions in consideration.

A. Physical Security	The TOE shall be located in the physically secure environment that can be accessed only by the authorized users.
A. Security Maintenance	When internal network environment changes due to change in the network configuration, host increase/decrease and service increase/decrease, etc., the changed environment and security policy shall immediately be reflected in TOE operation policy so that security level can be maintained to be the same as before.
A. Trusted Administrator	Authorized administrator of TOE shall be non-malicious users, have completed appropriate training on TOE administration functions and fulfill obligations according to administrator guidelines.
A. Operating System Reinforcement	Reliability and security of an operating system shall be ensured by administering operations to remove services or means in operating system not required by TOE and reinforcement on vulnerabilities in the operating system.
A. Sole Connection Point	TOE, when installed and operated in network, branches off network into external and internal networks and all communications between external and internal networks are carried out only through the TOE.

4.2 Scope to Counter Threats

[Network Intrusion Prevention System Protection Profile V1.1] defines security threats exerted by external threat agents to protection assets of the TOE by categorizing them into threats to the TOE and threats to the TOE operational environment.
The Threat agent is generally IT entities and human users who exert damage to the TOE and internal assets in abnormal methods or attempt illegal access to the TOE and internal assets from outside. The Threat agent has low level of expertise, resources and motivation.

T. Abnormal Packet Transmission	Threat agent may cause erroneous operation in system of internal network by transmitting network packet that holds abnormal structure.
T. Address Spoofing	Threat agents may illegally access internal network by spoofing source address as internal address.
T. Breakdown	TOE may not provide normal services to user as it is in use or breakdown occurred due to external attacks, etc.
T. Bypass Access	Threat agents may access TOE through bypassing security function of TOE.
T. Continuous Authentication Attempt	Threat agents may access TOE by continuously attempting authentication.
T. Denial of Service Attack	. Threat agents may interrupt normal use through abnormally excessive using of computer service resources in internal network located in TOE operational environment.
T. Illegal Information Inflow	Computer of internal network may be violated due to inflow of packet that contains unapproved information from external network.
T. Illegal Service Access	Threat agent may interrupt normal service provision of host by accessing services not approved to the host of internal network.
T. Masquerade	Threat agents may access TOE by masquerading as authorized administrator.
T. New Vulnerability Attack	Threat agents may make attack by using new vulnerability in computer system of internal network located in the TOE or TOE operational environment
T. Recording Failure	As storage capacity is insufficient, security-related incidents of TOE may not be recorded.

T. Unauthorized TSF Data Change	TSF data may be changed without authentication as threat agent makes buffer overflow attack to TOE.
TE. Administration Deficiency	The TOE may be configured, managed and used in insecure method by authorized administrator.
TE. Distribution and Installation	The TOE may be impaired of security in the process of distribution or installation.

5. PP Information

5.1 Security Functional Requirements

The TOE of [Network Intrusion Prevention System Protection Profile V1.1] defines security functional requirements as of the following.

[Table 2] Security Functional Requirements

Security Functional Class	Security Functional Components	
Security Audit	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_IFC.1(1)	Subset information flow control(1)
	FDP_IFC.1(2)	Subset information flow control(2)
	FDP_IFF.1	Simple security attributes
Identification And Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition (1)
	FIA_ATD.1(2)	User attribute definition (2)
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	User identification before any action(1)
	FIA_UID.2(2)	User identification before any action(2)
Security Management	FMT_MOF.1	Management Of Security Functions Behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection Of The TSF	FPT_AMT.1	Abstract machine testing
	FPT_FLS.1	Failure with preservation of secure state
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation

	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
Resource Utilisation	FRU_FLT.1	Degraded fault tolerance
	FRU_RSA.1	Maximum quotas
TOE Access	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination
Trusted Path/Channel	FTP_ITC.1	Inter-TSF trusted channel

5.2 Assurance Package

Assurance requirements of [Network Intrusion Prevention Protection Profile V1.1] consist with assurance components in CC Part 3 and evaluation assurance level is “EAL4.”

5.3 Strength of Function(SOF)

The Strength of function in [Network Intrusion Prevention Protection Profile V1.1] is “SOF-Medium”

6. Evaluation Results

The evaluation is performed with reference to the CC V2.3 and CEM V2.3. The verdict of [Network Intrusion Prevention Protection Profile V1.1] is the pass as it satisfies all requirements of APE(Protection Profile Evaluation) Class of CC. Therefore, the evaluation results were decided to be suitable. Refer to the ETR for more details.

• Protection Profile Evaluation (APE)
Evaluators conducted evaluation by applying work units of each component included in APE of CEM. Accordingly, the evaluation results of [Network Intrusion Prevention Protection Profile V1.1] are as follows.

The PP introduction of [Network Intrusion Prevention Protection Profile V1.1] consistently provides information necessary in PP identification, therefore the verdict of APE_INT.1 is the Pass.

The TOE description of [Network Intrusion Prevention Protection Profile V1.1] describes the objectives and functionality of the TOE sufficiently to be understandable and is coherent, internally consistent, and consistent with all other parts of the PP. Therefore, the verdict of APE_DES.1 is the Pass.

The TOE security environment of [Network Intrusion Prevention Protection Profile V1.1] 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. Therefore, the verdict of APE_ENV.1 is the Pass.

The security objectives of [Network Intrusion Prevention Protection Profile V1.1] counter the identified threats, achieve the identified OSPs, and are consistent with the identified assumptions. Therefore, the verdict of APE_OBJ.1 is the Pass.

The IT security requirements of [Network Intrusion Prevention Protection Profile V1.1] completely satisfy all the TOE security objectives and IT security requirements applied with the CC operation do not conflict with each other. Therefore, the verdict of APE_REQ.1 is the Pass.

The explicitly stated IT security requirements of [Network Intrusion Prevention Protection Profile V1.1] are only applicable if the PP contains IT security requirements that are explicitly stated without reference to either CC Part 2 or CC Part 3. If this is not the case, all work units in this section are not applicable, and considered to be satisfied. Therefore, the verdict of APE_SRE.1 is the Pass.

[Network Intrusion Prevention Protection Profile V1.1] is complete, consistent and technically sound, therefore is suitable to lead to the development of the ST.

Therefore, the final verdict on the APE is the **Pass**.

<Summary of the evaluation results>

Assurance Components	Evaluation Results
APE_INT.1 PP Introduction	Pass
APE_DES.1 TOE Description	Pass
APE_ENV.1 Security environment	Pass
APE_OBJ.1 Security objectives	Pass
APE_REQ.1 IT security requirements	Pass
APE_SRE.1 Explicitly stated IT security requirements	Pass

7. Recommendations

- [Network Intrusion Prevention System Protection Profile V1.1] defines security requirements for network intrusion prevention system that protects internal network and computer resources of organization. The CB found no special recommendation after reviewing this PP.

- This PP can be utilized as of the following. Product developer or marketer can draw up the Security Target by conforming all contents defined in this protection profile and user can utilize them for selection, operation and management of the product intended for use.

- This PP includes the minimum security requirements and does not make definition on implementation model of the TOE. In relation to security problems possible to occur according to the TOE implementation model, developer shall define additional security problems, security objectives and security requirements. If the TOE is implemented by being physically distributed in the network, developer shall define additional security problems, security objectives and security requirements in the Security Target in order to protect data being transferred among each component from external threats.

8. Acronyms

The following acronyms have been used in this report.

DoS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IPS	Intrusion Prevention System
OR	Observation Report
PP	Protection Profile
TOE	Target of Evaluation
WPR	Work Package Report

9. References

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

[1] Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25)
[2] Common Methodology for Information Technology Security Evaluation V2.3
[3] Korea evaluation and certification guidelines for IT security (MIC, 2005)
[4] Korea Evaluation and Certification Scheme for IT Security(NIS, 2005)
[5] IPS-ETR-V1.00 (2005. 12)