KECS-CR-06-15

WINS Technet. SNIPER IPS V5.0 E4000 Certification Report

Certification No. : KECS-NISS-0055-2006

Oct. 2006

National Intelligence Service
IT Security Certification Center

This document is the certification report on SNIPER IPS V5.0 (E4000) of the WINS Technet CO., Ltd.

Certification Body

National Intelligence Service IT Security Certification Center

Evaluation Body

Korean Information Security Agency

Table of Contents

1. Overview

This report is for the certification body to describe the certification result, which inspects the result and the conformance of the EAL4 evaluation of SNIPER IPS V5.0 (E4000) with regard to the Common Criteria for Information and Technology Security Evaluation.

The Korea Information Security Agency(KISA) has finished the evaluation of the SNIPER IPS V5.0 (E4000) on Sept. 28, 2006. 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 191 of the CC V2.2 part 1. In addition, the TOE satisfies the Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21,2005).

SNIPER IPS V5.0 (E4000) is a hardware integrated product developed by WINS Technet CO., Ltd that provides intrusion detecting/blocking functions. It is installed in an In-line mode at the network section that is to be protected, and can be managed through GUI (Graphic User Interface). Also, all security functions provided are included in the evaluation scope.

The TOE provides the following security functions:

- Control access according to the security policy. Intrusion detection and blocking according to the security violation events list.
- In order to operate detection and prevention function regarding the intrusion and harmful traffic, operate Blackhole and Firewall functions for all incoming packets.
- In order to communicate with the Client, SERVER ensures the trusted path through integrity and encryption using SSL protocol.
- Provided with the latest attack pattern through Live Update function, and provides security audit function so as to search the history conducted by the administrator.
- In case of failure, the TOE provides HA(High Availability) function to minimize the service interruption.
- Client operates security management function to manage Server efficiently.

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 package was correct.

Certification Validity: The information contained in this certification report does not mean that the use of SNIPER IPS V.0 (E4000) is approved or its quality is guaranteed by government agency of the Republic of Korea.

2. TOE Identification

The following [Table 1] indicates the information of the TOE identification.

[Table 1] TOE Identification

Evaluation Guide	Korea IT Security Evaluation and Certification Guidance (May 21, 2005) Korea IT Security Evaluation and Certification Scheme (Dec. 26 2005)
TOE	SNIPER IPS V5.0 (E4000)
Protection Profile	Network Intrusion Prevention System PP V1.1(Dec. 21 2005)
Security Target	Security Target V1.4 (Mar. 20 2006), WINS Technet CO., Ltd
ETR	SNIPER IPS V5.0 (E4000) ETR, V1.10 (Sept. 28 2006)
Evaluation Result	Satisfies the CC part 2 Satisfies the EAL4 of the CC part 3 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)
Sponser	WINS Technet CO., Ltd
Developer	WINS Technet CO., Ltd
Evaluation Team	KISA Evaluation Center, Evaluation Team II Seunghwan Lee, Byungki Jeon
Certification Body	National Intelligence Service

Underlying Hardware specification are stated in the [Table 2].

[Table 2] SNIPER IPS V5.0 (E4000) Server and Client Specification

Category			Specification
Server	Hardware	CPU	Intel Xeon DP CPU 3.6GHz*2
		Memory	2G DDR-II
		Interface	Packet gathering ports (for Giga)*6 Management ports (for 10/ 100/ 1000 Mbps)*2
		HDD	SATA-3.5"(SCSI) 73GB*2
	Software	OS	SNIPER OS V1.0 (Dedicated OS)
Client	Hardware	CPU	Intel Pentium II 400Mhz or more
		Memory	128MB or more
		Interface	10/100 NIC (1 or more)
		HDD	2GB or more
	Software	OS	MS Windows XP professional

3. Security Policy

The TOE operation conforms to the security policies stated below.

Name	Description
Audit	In order to trace responsibilities regarding all actions related to the security, security related events shall be recorded and maintained, and the recorded data shall be examined.
Secure manage	An authorized administrator shall manage the TOE in a secure manner.
SSL (Certificate management)	SNIPER shall securely generate the SSL Certificate and therefore store, manage it.

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	As it operates removal of the OS service or means that are not essential and enhancement regarding the OS vulnerability, it ensures reliability and stability of the OS.
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 seperates the network into external and internal network. Information cannot flow between the two without passing through the TOE.
A.Secure TOE External Server	The network time protocol (NPT) 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.
A.TOE SSL Certificate	The TOE, when installing certificate that is to be used for SSL authentication, generates in advance and stores at the TOE. SSL Certificate of the TOE is safely generated and managed,

4.2 Scope to Counter a Threat

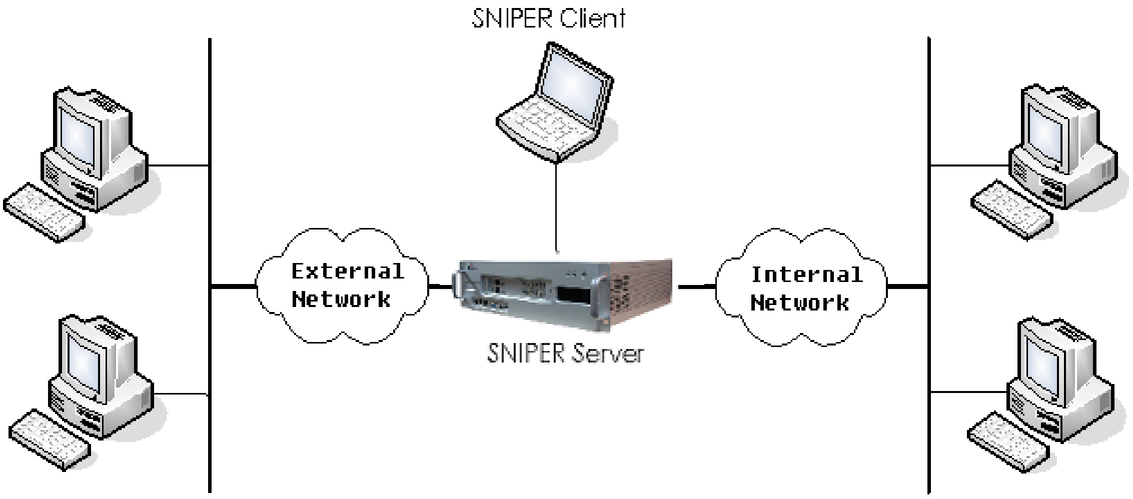
The TOE provides a means to counter a security threat including asset violation attempts of the TOE itself that is under protection. The TOE provides countermeasures against the vulnerability attack that is new or bypasses the security function. The TOE provides a countermeasure for the logical/physical attacks caused by the malicious user possessing low-level expertise, resources, and motivation.

All security objectives and security policies are described to provide a means to counter an identified security threat.

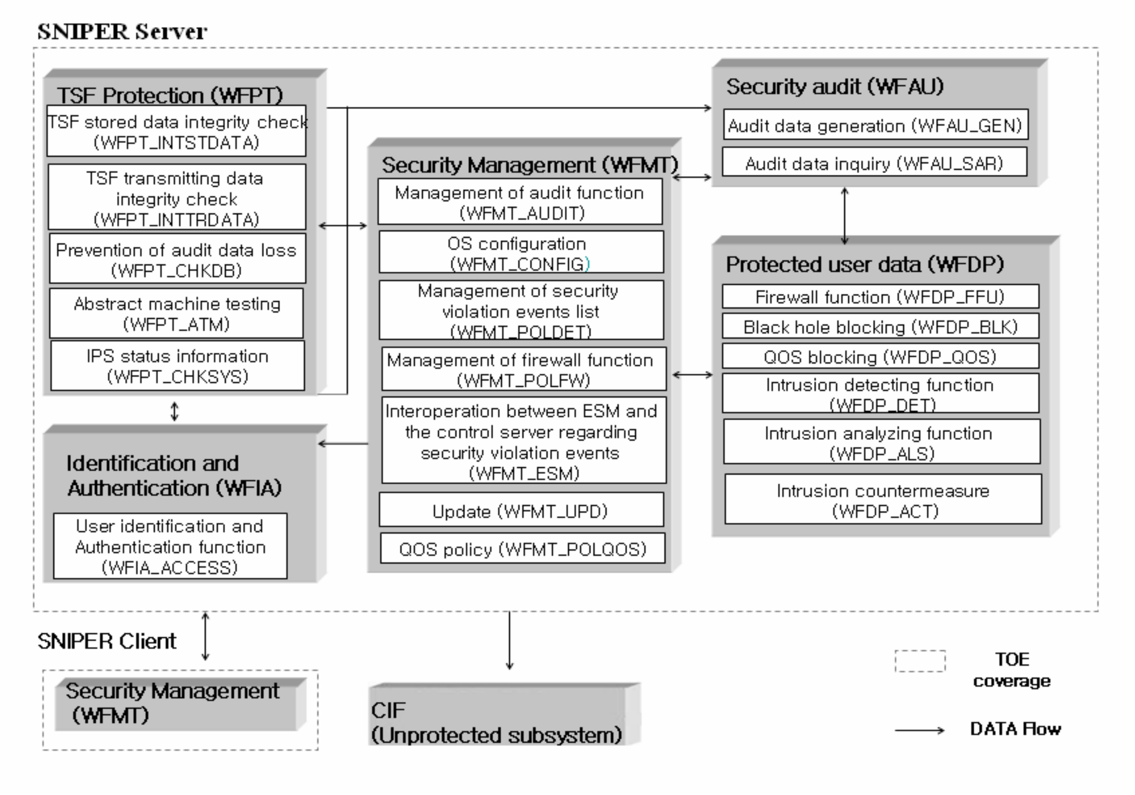
5. TOE Information

The TOE supports the security function of intrusion detection and firewall.

Operation environment is illustrated in the [Image 1], and the basic structure follows the [Image 2].



[Image 1] SNIPER IPS V5.0 (E4000) Operation network environment


SNIPER Server
TSF Protection (WFPT)
TSF stored data integrity check (WFPT_INTSTDATA)
TSF transmitting data integrity check (WFPT_INTTRDATA)
Prevention of audit data loss (WFPT_CHKDB)
Abstract machine testing (WFPT_ATM)
IPS status information (WFPT_CHKSYS)
Identification and Authentication (WFIA)
User identification and Authentication function (WFIA_ACCESS)
Security Management (WFMT)
Management of audit function (WFMT_AUDIT)
OS configuration (WFMT_CONFIG)
Management of security violation events list (WFMT_POLDET)
Management of firewall function (WFMT_POLFW)
Interoperation between ESM and the control server regarding security violation events (WFMT_ESM)
Update (WFMT_UPD)
QOS policy (WFMT_POLQOS)
Security audit (WFAU)
Audit data generation (WFAU_GEN)
Audit data inquiry (WFAU_SAR)
Protected user data (WFDP)
Firewall function (WFDP_FFU)
Black hole blocking (WFDP_BLK)
QOS blocking (WFDP_QOS)
Intrusion detecting function (WFDP_DET)
Intrusion analyzing function (WFDP_ALS)
Intrusion countermeasure (WFDP_ACT)
SNIPER Client
Security Management (WFMT)
CIF (Unprotected subsystem)
TOE coverage
DATA Flow

[Image 2] SNIPER IPS V5.0 (E4000) Basic structure

The TOE consists of the following main subsystems.

- Audit (WFAU)

Security audit subsystem operates the function of audit data generation(WFAU_GEN) and audit data inquiry(WFAU_SAR). In order to check whether a system operates efficiently, by gathering, analyzing the record history, audit records generated through the audit detect/block intrusions to the computer system and are used for detecting the misuse for the system.

- User Data Protection (WFDP)

User Data Protection sub-system operates Firewall function (WFDP_FFU), Blackhole blocking (WFDP_BLK), QoS blocking (WFDP_QOS), Intrusion Detecting function (WFDP_DET), Intrusion Analyzing function (WFDP_ALS), and Intrusion Countermeasure function (WFDP_ACT). This function controls the flow of network data according to the permission or blocking rule to protect the target network that is to be protected from internal or external attackers. Also it collects information to detect intrusion and react to an intrusion in case it is identified, and stores the analysis result so that the administrator can check.

- Identication and Authentication (WFIA)

Identification and Authentication sub-system operates user identification and authentication process (WFIA_ACCESS). Only authorized administrators are allowed to access key functions that are essential to the regular operation of SNIPER such as changing, deleting and adding policies and retrieving log files. In order to control the access to SNIPER perfectly, every access attempt through an administrator interface are examined to identify and authentication appropriate administrator. The communication between SNIPER Client and the engine is encrypted using SSL and its integrity is verified through SHA-1 to prevent any modification or exposure of the data. Even with the access of an authorized administrator, if not operate for a certain period of time; protect the TOE during the inactive terms of an authorized administrator by locking up the interacting sessions.

- Security Management (WFMT)

Security Management sub-system operates Security Audit Management(WFMT_AUDIT), OS Configuration(WFMT_CONFIG), Management of Security Violation List (WFMT_POLDET), Firewall function Management(WFMT_POLFW), Management of Interoperation between ESM and the Control Server regarding security violation events (WFMT_ESM), Update(WFMT_UPD), and QoS Policy(WFMT_POLQOS). Security Management function provides the rules for detection/prevention SNIPER performs and the managerial actions retrieving and modifying information related to the state and configuration of SNIPER.

- TSF Protection (WFPT)

TSF Protection sub-system operates TSF stored data Integrity check (WFPT_INTSTDATA), TSF transmitting data Integrity check (WFPT_INTTRDATA), Prevention of audit data loss (WFPT_CHKDB), Abstract machine testing (WFPT_ATM), and IPS status information (WFPT_CHKSYS). TSF Protection provides a regular check function to assure that the security assumptions related to the underlying abstract machine are properly operating. It performs checking when initially started, periodically during normal operation, and upon request of an authorized user to decide whether the main components running on the TOE system are normally operating in order. It also preserves a secure state when failure occurred and ensures safe operation of the TOE by periodical monitoring. In cases where components of the TOE interact remotely through internal communication channels, Server and Client identify and authenticate the nodes of the other side to ensure safe channels between TSFs.

6. Guidance

The TOE provides the following guidances.

- SNIPER IPS V5.0 (E2000) Administrator Guidance V1.2 , 2006. 7. 2
- SNIPER IPS V5.0 (E2000) Delivery documentation V1.1 , 2006. 1. 24
- SNIPER IPS V5.0 (E2000) Installation Manual V1.1 , 2006. 1. 24

7. TOE Test

7.1 Developer's Test

- **Testing 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 :

  Detail 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 :

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, the internal/external network. 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 and the 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.

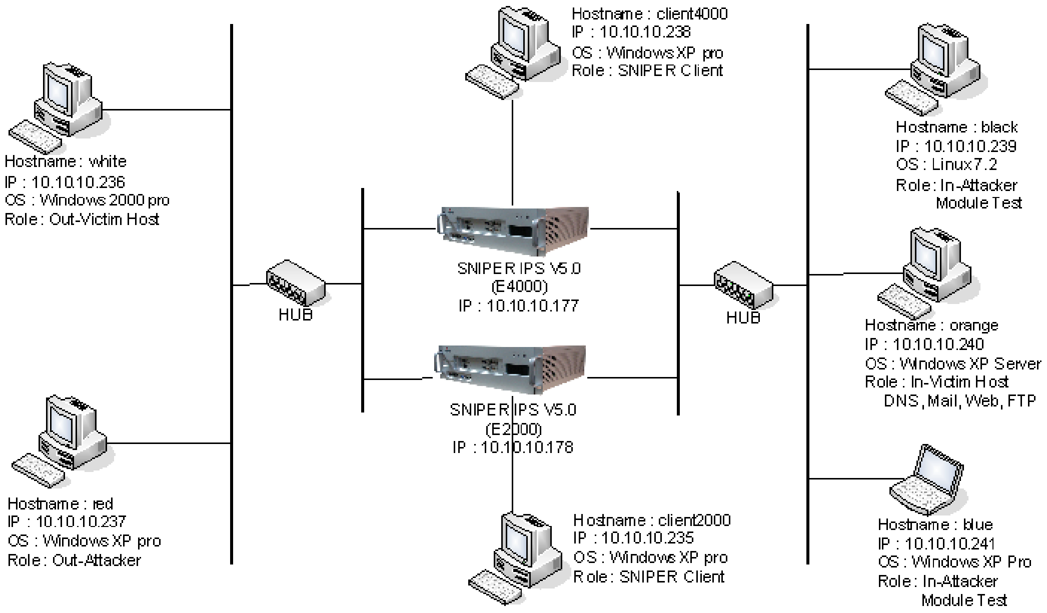
Moreover, the evaluator devised and performed additional evaluator's tests on the basis of the developer's test, and confirmed that the actual test result was consistent with the expected test result.

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.

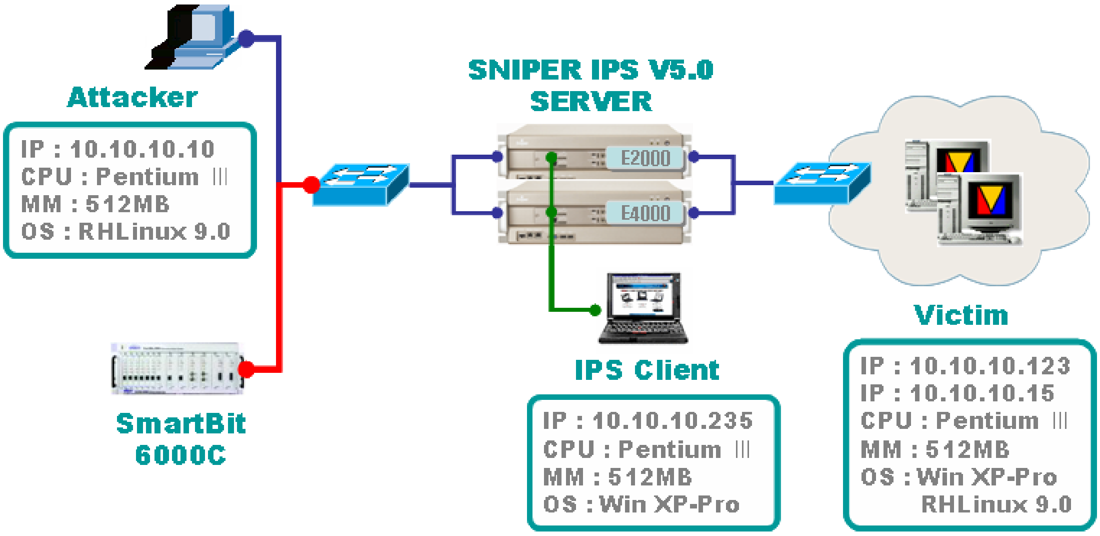
8. Evaluation Configuration

For testing, the evaluator composed the following test configuration that corresponds to the environment structure specified on the Security Target.



[Image 3] TOE test configuration

For testing, after constructing the test configuration that is identical to the network structure, the TOE, via the security management, prepares the preliminary items in advance to the test after installing the engine and the monitoring console.



[Image 3] Penetration test configuration

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 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 provides a logical description of the TOE; that it is internally consistent and consistent with other parts of the ST. The TOE security environment provides definition of the consistent, complete security issues that are induced from the TOE and the TOE security environment. The security objectives are also described completely and consistently. The security objectives counter the identified threats, achieve the organizational security policies, and satisfy the stated assumptions. The TOE security 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.

TOE summary specification provides security function and assurance standard with an accurate and consistent superior level definition, satisfies described TOE security requirements. Also, it accurately substantialize Protection Profile that the Security Target accepts.

- 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 verified that the configuration management specifies the configuration list, configuration identification, version endowment, configuration modification control and that all development documentations and source files were developed applying the configuration management system. He also confirmed that the generation and modification of the configuration items are achieved through the configuration management organization and the configuration management system.

- Delivery and Operation Evaluation (ADO)

The evaluator applied the ACM sub-activities described in the CEM V2.2 to the evaluation of the delivery and operation of the TOE. The Delivery and Operation describes measures and procedures of the secure delivery, installation, and operation. Thus, it ensures that the security is not being damaged while the TOE is transmitted, installed, operated, and it verifies that the contents of the document are being actually applied according to the results of inspections.

- 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.

Development evaluation defines as it specifies the TOE security functional requirements from the TOE summary specification to the actual implementation stage, using functional specification, high-level design, low-level design, implementation representation.

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 in the CEM V2.2 to the evaluation of the guidance of the TOE. The administrator guidance describes the method of how the administrator may access to the security management interface. It also describes the guidelines and rules regarding the each provided menu by giving examples. The administrator guidance has verified that the contents described are being accurately operated. Also, as the TOE does not request the user guidance for security requirements, it is impossible to apply user guidance evaluation.

- 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 life cycle support evaluation clearly describes that it protects the development environment using security measures, such as procedures, policies, tools and methods regarding the every stage of the TOE development. Through the actual inspection process of the institutions, It verified that the above statements were actually being applied.

- 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 test documentation predicts the result and describes the objectives of the test, progressive test procedures, and the test results regarding the security functions specified on the ST. By performing module test and the provided development functional test repeatedly, the evaluator verified that the contents of the test described in the test documentation was accurate and that the security functional actions implemented during the development were consistent. Also, by performing independent testing, the evaluator confirmed accuracy of the developer's test.

- 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. The vulnerability analysis document reasonably and specifically describes the identified vulnerabilities of the TOE and appropriate countermeasures, analysis and countermeasures of the misuse. Also, by conducting independent vulnerability analysis, the evaluator confirmed the accuracy of the vulnerability analysis. Also, the strength of TOE security function analysis describes that the strength of TOE security function satisfies the functional strength permit level defined at the PP/ST.

10. Recommendations

- In order to ensure the secure path when registering, modifying the administrator, it is necessary to register additional administrator's IP address. If the additional IP address was not added, it prints the message saying 'Register one or more administrator's IP address'. Thus, all administrators shall remember input IP address when register.
- When checking the integrity, Master.dat files stored with ID and password, modify whenever the administrator login/logout. For an accurate integrity check the administrator has to setup automatic integrity check which automatically check the latest status of signature and date modified, since they change everytime.
- The TOE supports a function to block the access by registering the external attacker's address on the blackhole list. Since even the normal packet may be blocked its access by the blackhole list, administrators shall constantly manage the list so that it won't block the normal packet.
- Update is classified into pattern update and engine/GUI update. When operating the pattern update, it is not necessary to restart the engine, but when operating engine/GUI update, since the engine has to be updated, the security function does not operate. Thus, when operating engine/GUI update, it is efficient to block other network services and set time when the network traffic is relatively small (e.g. weekend, late hour).
- In case when the device itself or the network environment fails, the TOE provides HA function to immediately recover the network service. Therefore, the administrator shall maintain and manage the TOE that provides the main service and the backup in a highly available status so as to recover network failure.

11. Acronyms and Glossary

The following acronyms are used in this certification report.

(1) Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

(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

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

NTP
Protocol used for synchronizing time

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)
[5] Korea IT Security Evaluation and Certification Guidance (May 21, 2005)
[6] Korea IT Security Evaluation and Certification scheme (Dec 26, 2005)
[7] SNIPER IPS V5.0(E2000) Security Target V1.4 (Mar. 20, 2006), WINS Technet.
[8] SNIPER IPS V5.0(E2000) Evaluation Technical Report V1.10 (Sept 28, 2006)