KECS-CR-07-10

NXG IPS 6000 V1.6 Certification Report

Certificate number: KECS-NISS-0069-2007

June 2007

National Intelligence Service

IT Security Certification Center

This document is the certificate report for NXG IPS 6000 V1.6 of SECUI.COM.

Certification Committee Members

Ministry of Information and Communication Official—GyuJoe Cho
National Security Research Institute—JongWook Park
Korea University—JongIn Im
Ewha WomansUniversity—KiJune Chae
SungKyunKwan University –SeungJue Kim
SoonChunHyang University - HeungRyul Yum
ChungNam University—JaeChul Ryu
HanNam University—KangSue Lee
ETRI—SeungWon Son

Certification Institute

National Intelligence Service IT Security Certification Center

Evaluation Institute

Korea Information Security Agency

Table of contents

1 Summary

This report describes the certification result by the certification institute about the Common Evaluation Criteria for Information Protection System (Noticed on May 21, 2005) (which will be referred to hereafter as 'Common Evaluation Criteria'), the EAL 4 evaluation result, for NXG IPS 6000 V1.6. This report describes the evaluation result and the validity and suitability for the evaluation result.

The evaluation for NXG IPS 6000 V1.6 is performed by Korea Information Security Agency and it is completed on June 4, 2007. This report is created based on the evaluation report that Korea Information Security Agency submitted. The evaluation is resulted as "valid" according to Part 1 of the Common Evaluation Criteria section 191 because the product satisfies the EAL 4 evaluation assurance level for Part 2 and 3 of the Common Evaluation Criteria.

NXG IPS 6000 V1.6, developed by SECUI.COM, is an Intrusion Protection System (IPS) that has been developed to protect the internal network, servers, and services as well as information and services between the internal and external networks.

The product consists of the SecuiOS that provides basic operating environment, the hardware that provides system resource, and the software that provides IPS security function. The evaluation product provides the main security functions as follows:

- Security auditing, and audit data generation and protection (Audit)
- Security management (SEC_MAN)
- Protection of internal property and information from illegal accesses (Firewall)
- Protection of illegal accesses and attacks (IPS)
- TOE user identification and authentication (UI&AD)
- TSF stability (TSF_SAFER)
- Process monitoring (Mon_Process)

The certification institute checked evaluation activities and test procedures of the evaluator, provided the guidelines for the technical problems and test evaluation procedures, and reviewed each evaluation unit and contents of the evaluation report. The certification institute confirmed that the evaluation products meet all of the requirements for described security functions and assurances and the evaluation result assures it. Accordingly the certification institute authenticated that the evaluations and the results of the evaluator are accurate and reasonable and the evaluation result on the validity test is correct.

Certificate Validity Range: The information included in this certificate report is not referred to the permission from the Korean government agency to use NXG IPS 6000 V1.6 or the quality assurance for NXG IPS 6000 V1.6.

2 Identification

[Table 1] shows the information used to identify the product to evaluate.

[Table1] Evaluation Identifiers

Evaluation Guidance	Evaluation & Assurance Scheme for Information Protection System (May 30, 2007, Ministry of Information and Communication Official Notice 2007-19) Evaluation Authentication Regulations for the Information Security Product (2007.4.15)
TOE	NXG IPS 6000 V1.6
Protection Profile	Network Intrusion Protection System Protection Profile V1.1
Security Target	NXG IPS 6000 V1.6 Security Target version 1.13, 2007-04-23
Evaluation Report	NXG IPS 6000 V1.6 Evaluation Report V1.0, 2007-06-04
Conformance Result	Common Evaluation Criteria Part 2—Valid Common Evaluation Criteria Part 3—Valid
Evaluation Standards	Common Evaluation Criteria for Information Protection System (May 21, 2005, Ministry of Information and Communication Official Notice 2005-25)
Evaluation Methodology	Common Evaluation Methodology for Information Protection System V2.3 (2005. 8)
Evaluation Requester	SECUI.COM
Developer	SECUI.COM
Evaluator	Korea Information Security Agency - Security Evaluation Team 2 GyuMin Cho, YongSeok Oh, HyunMi Park, YoungJu Noh
Certified by	National Intelligence Services

The evaluation range for this product does not contain the hardware and operating system but security function of the identified firmware version shown below.

o NXG IPS 6000 V1.6 firmware : V1.2.5.R
(On delivery of goods, it is provided to customers after installing the firmware in the following operating hardware)

o Hardware for installing and operating TOE:

Item	Specification	Remarks
CPU	MPC7447 X 7	
Main memory	3.5 GB	
HDD	72 GB	
NIC	8(1Gbps * 8) Ports + For console (DB9 type) 2 ports + For management tool connection RJ45 type 1 port	RJ-45 Type 4 ports Fiber Type 4 ports
Operating system	SecuiOS V1.1	

※ The ports for console are divided into AUX and Console. The Console manages CPU-X that is the management CPU among 7 CPUs. The AUX manages CPU-1 that is the first CPU among 6 CPUs managing other applications.

The management console is the PC that is in charge of operating and managing the TOE with the administrator program installed. For installing and operating the management console, it is recommended to use following physical hardware specifications:

o Environment for installing and operating TOE:

Management Console	Minimum Specification	Remarks
CPU	Pentium III 133 MHz or higher	
Main memory	256 MB or higher	
HDD	40 GB or higher	
NIC	One or more	
Serial	1 EA	DB9 type
Operating system	Windows XP Service Pack 2	
Web browser	Internet Explorer Version 5.5 or higher	Required for patch supporting 128 bit (pr longer) SSL

3 Security Policy

The evaluation product is operated by satisfying security policies as follows.

Security Audit To track the responsibility on all security-related activities, it is required to record and maintain security-related events, and to review the recorded data.
Secure Management The authorized administrator should manage the TOE using the secure way-.

4 Assumptions and Scope

4.1 Assumptions

The evaluation product should follow the assumptions as shown below for installation and operation.

A.Physical security	
The TOE is located in a physically secure environment that only the authorized users can access.	
A.Maintaining security	
When the internal network environment changes according to network configuration change, increase or decrease in host range, increase or decrease in service count, the changed environment and security policies are applied to maintain the same security level as the previous.	
A.Authorized administrator	
A TOE authorized administrator is not a malicious user, well trained for the TOE management functions, and performs the duty for manager guidelines.	
A.Operating system reinforcement	
To guarantee credibility and stability of the operating system, the TOE removes unnecessary services and means and reinforces the vulnerability of the operating system.	
A.Unique connection point	
When the TOE is installed on the network, it branches the network to external and internal ones so that all communications between internal and external networks are enabled only through the TOE.	
A.Operating system time	**Input by a ST author**
The TOE takes an input for time source from the underlying operating system and external NTP server.	
A.SSL certificate	**Input by a ST author**
The SSL certificate for access to the TOE uses the private certificate of the TOE itself for secure management.	
A.Secure TOE external server	**Input by a ST author**
The NTP server and SECUI update server for secure TOE operation outside of the TOE are secure.	

4.2 Threat Reaction Scope

The evaluation product does not provide ways to handle the security threats to the proper level for the IT environment that TOE requests and the direct physical attacks that cause the abnormal operation for the evaluation product. But the evaluation product provides ways to handle the logical attacks come from the threats that have low-level of expert knowledge, resources, and motivation on the connected network.

All the security objectives and security policies are described to provide the ways to handle the identified security threats.

5 Product Information

The TOE provides an intrusion protection system (IPS) to block any illegal external intrusions and attacks by installing the TOE on a vulnerable network point of contact as the following figure.
As in the following diagram, the TOE operates on the operating system described in the physical boundary and scope and it is installed on the hardware produced by SECUI.COM to use.

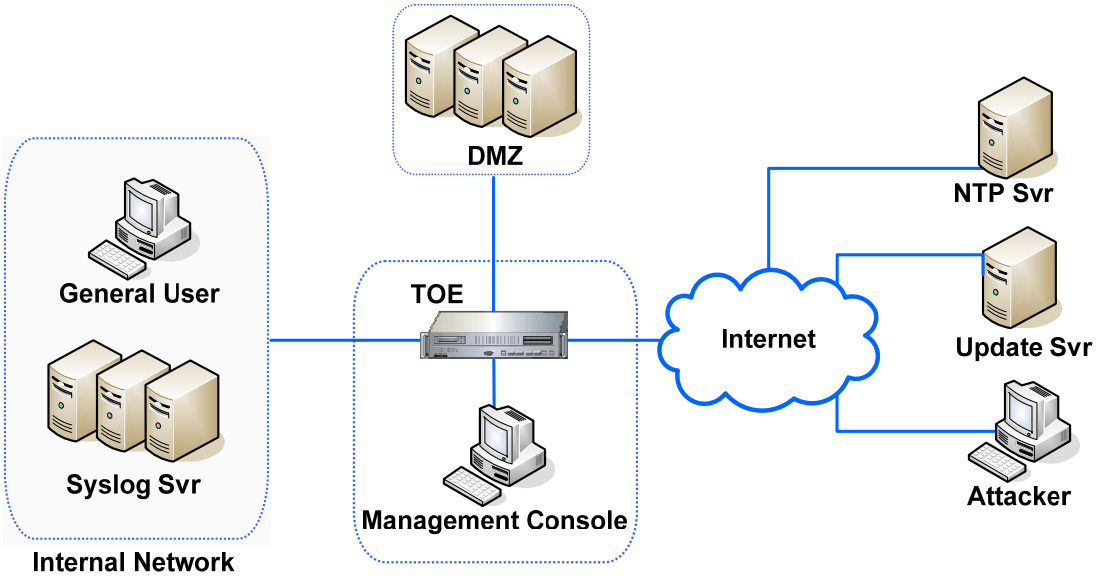


Figure 1 TOE Environment

The product consists of the SecuiOS that provides the basic operating environment, the hardware that provides system resources, and the software that provides IPS security functions. The TOE is the security software. The following figure shows the software architecture for the TOE and this security software can be divided into the kernel level subsystem and the application level subsystem.

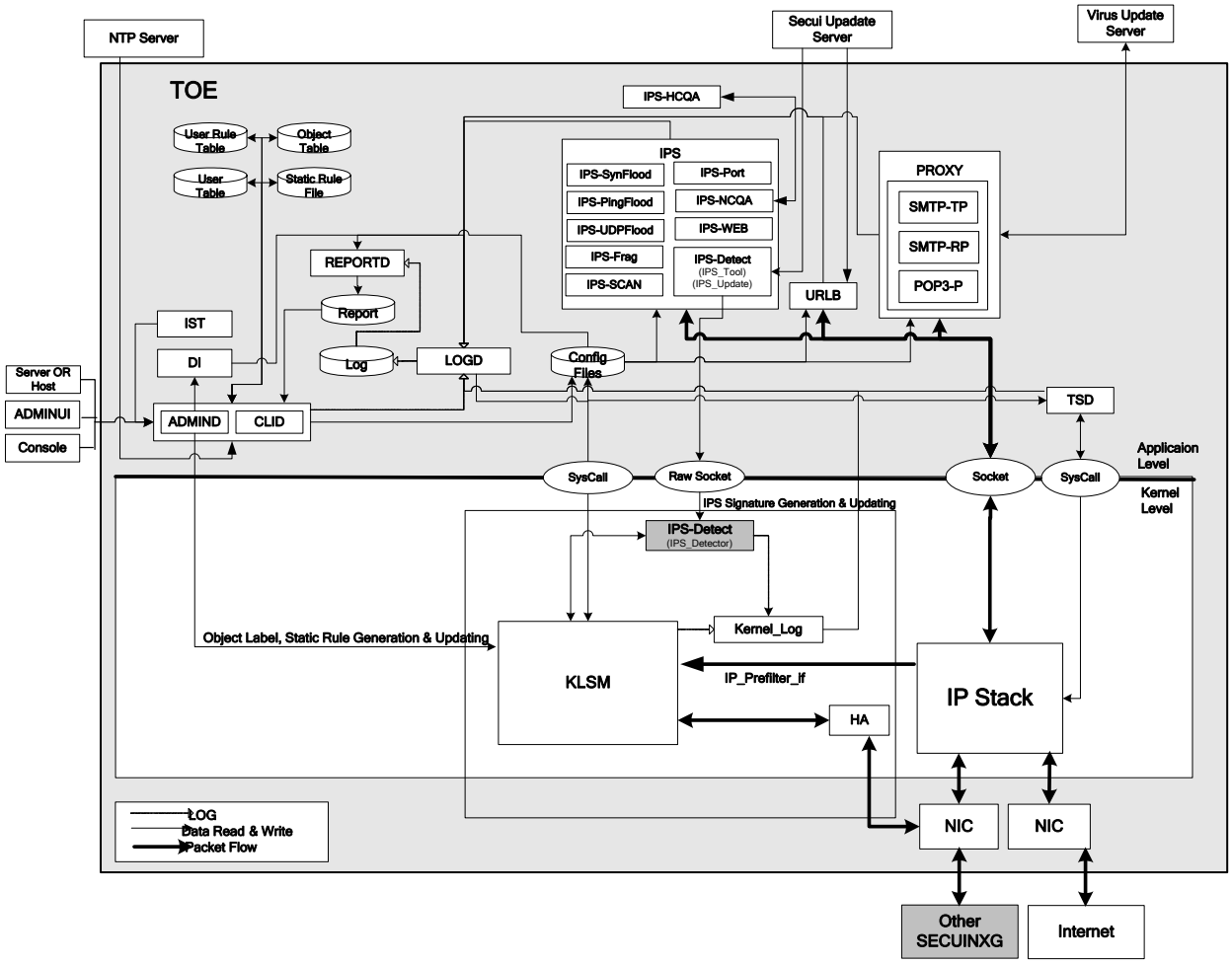


Figure 2 TOE Architecture

6 Administrator Guidance

The evaluation product provides the guidance as follows:

- NXG IPS 6000 V1.6 Administrator Guidance V1.5, May 29, 2007

7 Product Testing

7.1 Developer Testing

- **How to test**

  The developer created test items with the consideration of the product security function. Each test item is described in the test book. Each test item described in the test book contains following details:

  - Test number/tester: The test item identifier and the developer who applied for a test
  - Test purpose: Describes the purpose of the test including the security function for testing objective and the security module
  - Test environment: The detailed test environment to perform the test
  - Detailed test procedures: The detailed procedures to test the security function
  - Expected results: The expected test results after performing the test procedure
  - Actual results: The test results when actually performing the test procedure
  - Comparison between expected results and actual results: The results after comparing between expected results and actual results

  The evaluator evaluated the test validity such as test environment, test procedures, test range analysis, and high-level design test for the test book. The evaluator proved that the test of developer and the test result are suitable for evaluation environment.

- **Test environments**

  The test environments described on the test book contain detailed environments such as configuration for test, evaluation product, and TOE installed server. The detailed test environments to test each test items are also described.

- **Test range analysis /High-level design test**

  The detailed evaluation results are described on the ATE_COV and ATE_DTP evaluation results.

- **Test result**

  The test book describes expected results and actual results for each test items. The actual results can be checked through not only the actual product activation screen but also the audit log.

7.2 Evaluator Testing

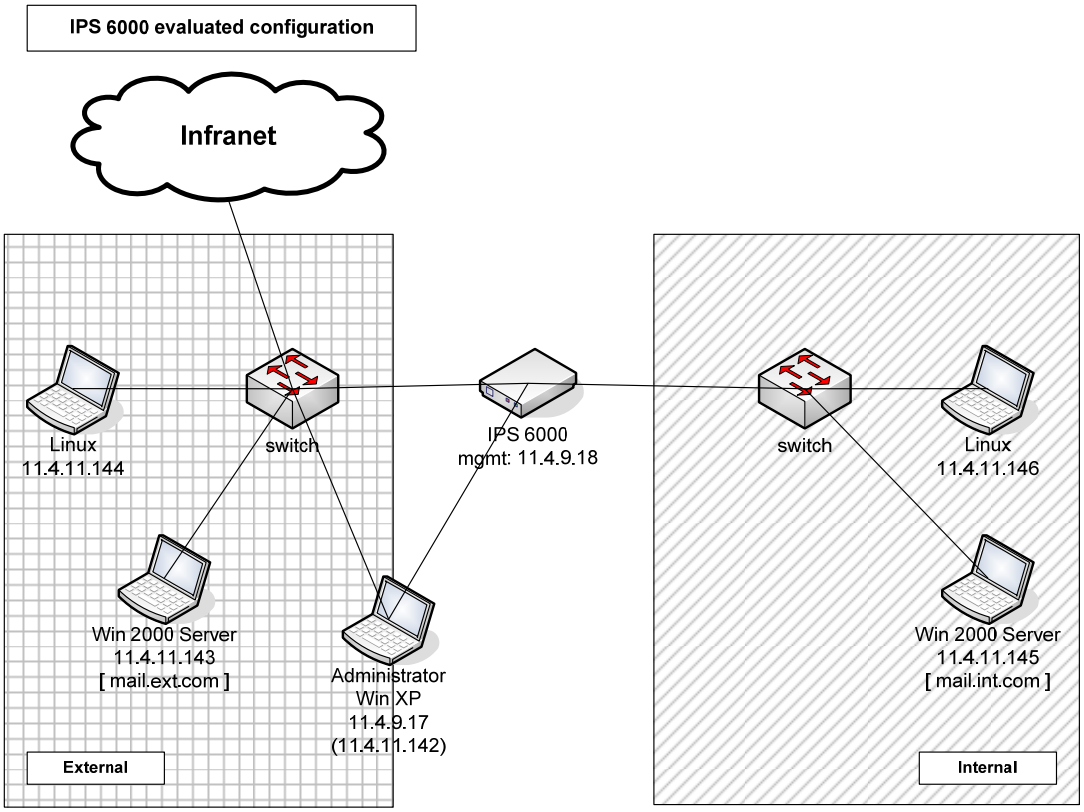
The evaluator installed the evaluation product by using the evaluation environment and evaluation tool same as for the developer test and evaluated all test items provided by the developer. The evaluator confirmed that actual results match with expected results for all test items.

The evaluator also tested by creating separate evaluator test items based on the developer test and checked that actual results and expected results match.

The evaluator confirmed that the any vulnerability cannot be exploited in the evaluation environment after performing the vulnerability test.

The evaluator test result assured that the evaluation product properly operates as described in the design documentation.

8 Evaluated Configuration



o Security function

The evaluator performed the test for security functions in the following table.

TSF	Description
Generation and protection for security audit and audit data (Audit)	It generates audit data on all packets passing through the TOE and all processes executed in the TOE for administrators to query, analyze, and integrate the generated audit data for management. It also manages the file system that stores audit data in order to protect audit data.
Security management (SEC_MAN)	The administrator can determine, disable, enable, and modify the behavior on the security functions only through the administrator program or the management console. In order to operate the administrator program and directly interoperate with the TOE, the administrator should take the administrator identification and authentication procedures first. Accordingly the right to perform the abovementioned functions is restricted to the authorized administrators.

Protection of internal property and information from illegal accesses (Firewall)	The TOE identifies and authenticates internal/external IT entities sending/transmitting information through TOE (access subject) and subsequently applies the access control rules based on the IP address and security attributes (e.g., security levels: 1 to 20) to determine whether each IT entity has access right. The subject allows operations to allow, deny, refuse (ICMP) and refuse (reset) security attributes of the network packets passing through the TOE. The security attributes are the destination URI (uniform resource identifier), time, and packet's header and data information. When there is no access right to access objects, the access control is executed by terminating the corresponding user connection. The TOE information flow control is divided into the discretionary access control and compulsory access control as well as the access control based on the additional rules.
Protection of illegal accesses and attacks (IPS)	There are hacking attacks that exhaust host and network resources and cause availability problems through the known vulnerabilities. In order to prevent those problems, it is necessary to have the intrusion protection system (IPS) that detects illegal accesses and attacks and protect the system from them.
TOE user identification and authentication (UI&AD)	There are authorized administrators who manage the system itself. The authorized administrator shall be registered in the TOE and pass the user identification and authentication procedure through the TOE.
TSF stability (TSF_SAFER)	It provides the TSF data integrity test and counteractions when the TSF data integrity constraints are breached and tests whether the TOE system works properly or not. Encrypted communication is also supported using the encoding algorithm to guarantee communication through safe routes between TSFs. This is the function for protecting communication data between TSFs.
Process monitoring (Mon_Process)	The process guard function watches whether the application process for each security function operates correctly or not. This function supports continuous services so that the security function defined by the administrator cannot be stopped due to any arbitrary error.

9 Results of the Evaluation

The evaluation applied the common evaluation criteria for information protection system V2.3 and the common evaluation methodology for information protection system V2.3. The result of evaluation says that the evaluation product meets the requirements of the evaluation assurance level (EAL4) in Part 2 and Part 3 of the Common Evaluation Criteria for the information protection system. Refer to the evaluation report for the detailed evaluation results.

- **Security target evaluation (ASE)**

  The evaluator applied the common evaluation methodology task unit to proceed on evaluation.
  The overview of security target evaluation is perfect, has the consistency with other parts of the security target, and accurately identifies the security target. The TOE description provides perfect and logical descriptions to fully understand the purpose and functions for the TOE with the internal consistency and it has the consistency with other parts of the security target.
  The security environment defines the complete, clear, and consistent security problems came from TOE and TOE security environment as assumptions, threats, and operational security policies and provides complete and consistent descriptions. The security objectives satisfy the identified threats, accomplish the identified organizational policies, and satisfy the described assumptions.
  The IT security requirements are completely and consistently described and it provides proper basis for the TOE development that helps to achieve the security objectives. The TOE summary specification defines the security function and assurance criteria completely and consistently and meets the requirements for the described TOE security requirements. The security target accurately describes accommodating security profiles.
  Accordingly, this security target specification is appropriate to use as the basic material (that is complete, consistent, technically reasonable, and corresponding to results) for TOE evaluation.

- **Configuration management evaluation (ACM)**

  The evaluator applied the ACM common evaluation methodology task unit to proceed on evaluation. It is confirmed that the configuration management documents helps the developer to use automation tools to modify implementation representation for controlling. It is confirmed that the configuration management document helps the developer to clearly identify the TOE and TOE related configuration items and moderately restricts the ability to change the items. It is confirmed that the configuration management documentation helps the developer to perform the configuration management for TOE implementation representation, evaluation evidences required by ST assurance components, and security flaws.
  Accordingly the configuration management documentation helps customers to identify the evaluated TOE and it guarantees that the configuration items are uniquely identified. It also guarantees that the developer used appropriate procedures to control and track the TOE change.

- **Delivery and operation (ADO)**

  The evaluator used the ADO common evaluation methodology to proceed on evaluation. The delivery documentation describes all procedures that are necessary to maintain security when distributing version of the TOE to a user's site. There is a document that describes the secure installation, generation, and start-up of the TOE and it is confirmed that the TOE has the secure environment configuration.
  Accordingly, the deployment and operation documentations are appropriate to assure that the TOE is installed, generated, and started as same as the developer intended method and deployed without a change.

- **Development evaluation (ADV)**

  The evaluator used the ADV common evaluation methodology task unit to proceed on evaluation. The functional specification describes the TOE security function well and explains that the TOE security function is enough to meet the security function requirements for the security target. It also gives enough descriptions to the TOE external interface. The security policy model describes the rules and characteristics of all policies accurately and consistently and the description corresponds to the security functions described on the functional specification.
  The high-level design describes the TSF as the subsystem that is main component and it gives descriptions to interface and detailed information to the functional specification. The low-level design describes the internal actions for TOE security functions in the interrelationships and dependencies between the models. The low-level design meets the security requirements for security target and it makes the high-level design to be precise and effectively refine.
  The implementation representation meets the requirements for the security target and follows the high-level design precisely. The correspondence of representation shows that the developer implemented the security target requirements precisely and perfectly with functional specification, low-level design, high-level design, and implementation representation.
  Accordingly, the representation correspondence documentation that assures consistency of the TOE representation methods (the functional specification that describes TOE external interface, the low-level design that explains the TOE architecture, the high-level design that explains the TOE architecture as an internal module, and the implementation representation that is explanation in the source code level) helps to understand the way to provide TOE security functions.

- **Guidance document evaluation (AGD)**

  The evaluator used the AGD common evaluation methodology task unit to proceed on evaluation. The administrator guidance describes how the administrator can connect to the security management interface and gives descriptions for each guidance provided for security management interfaces and safety information with examples. The contents described on the administrator guidance are perfectly followed.

- **Life-cycle support evaluation (ALC)**

  The evaluator used the ALC common evaluation methodology task unit to proceed on evaluation. The security control for the development environment by developer was appropriate to provide the required confidentiality and implementation for the TOE design and integrity to safely operate the TOE. The developer used the TOE life-cycle model in documentation. The developer used well-defined development tools for the consistent and predictable results.
  Accordingly, the life-cycle support describes the procedures that the developer uses to develop and maintain the TOE including the security procedures and tools used for the entire TOE development process.

- **Test evaluation (ATE)**

  The evaluator used the ATE common evaluation methodology task unit to proceed on evaluation. The test book describes test purpose, test procedures for each step, and test results for the security functions described on security target and gives examples for the results. By repeating the test procedure of functional test for each development step, the test contents described on the test book are confirmed to be precise and correspond to the security functions that are implemented during development process. Also the evaluator performed the separate test to assure the accuracy of developer test.

- **Vulnerability evaluation (AVA)**

  The evaluator used the AVA common evaluation methodology task unit to proceed on

evaluation. The guidance for misuse analysis was not misunderstood, irrational, or conflicted and it had contents about safety procedures for all safety modes. The unstable status for the TOE could be prevented or detected by using the guidance. The function strength was declared for all statistics and permutation mechanism on the security target and the developer made an accurate analysis for the function strength declaration.
The analysis of misuses has explanations about the known vulnerabilities for the TOE and the ways to handle these. And the evaluator performed the vulnerability analysis separately for the accuracy of vulnerability analysis. The TOE had no vulnerability that can be badly used by the attacker with the low level of expert knowledge in the intended environment..
Accordingly the TOE is confirmed to have no vulnerability that can be badly used in the intended environment based on the vulnerability analysis and penetration test by developers and evaluators.

10 Recommendations

- NXG IPS 6000 V1.6, the H/W in one product, is evaluated based on the H/W environment that is described on the security target and evaluation report; therefore, it should be installed on the H/W to use.
- The HDD capacity for this product is 72 GB and it is different from the HDD capacities applied to many other PCs and servers. Therefore it is recommended to send logs to the external log sever according to the product operating environment, frequently backup information, and monitor the keep checking the storage capacity.
- The TOE should be used with caution because it has no NAT function and any internal IP address can be exposed.
- The administrator notice function is provided when the audit log storage capacity exceeds and reaches to the critical value. However, the administrator should not depend on the notice function only but keep checking the storage capacity and use the audit log backup function.
- To minimize a waste of system resources caused by the Denial Of Service, the administrator should set the session number for simultaneous connection that is appropriate for the user number and system hardware capacity.
- The periodic signature updates should be performed to cope with the recent malicious codes and it should be considered that the signature for this TOE is limited to 100 and evaluated for the product evaluation.
- The updates for anti-virus engine and malicious information DB should be performed periodically.
- The latest security patch should be always applied for the strict security policy recommendation and operating system or application program on each internal network system because the security function for the evaluation product cannot protect all resources for internal network.

11 Acronyms and terminology

The following terminology and acronyms are used for this 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

(2) Terminology

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

Audit log
The audit data that stores audit logs for the TOE security related events

User
All entities such as users and external IT entities that interoperate with TOE from outside.

Authorize administrator
Authorized user that securely operates or manages TOE according to the TOE security policies.

External IT entity
All secure or insecure IT products or systems that correspond to the TOE from the outside of the TOE

SecuiOS
The SECUI.COM developed operating system, the operating system for appliance type network security Gateway, consists of the minimum specification to support the TOE security functions. It is implemented with four functions: process management, memory management, file system management, and network communication.

12 References

The certification institute used following documents to complete this certificate report:

[1] Common evaluation criteria for information protection system (2005. 5. 21)
[2] Common evaluation methodology for information protection system V2.3
[3] Evaluation ·Authentication Scheme for Information Protection System (2007. 5. 30)
[4] Evaluation Authentication Guidance for Information Protection Products (2007. 1. 1)
[5] NXG IPS 6000 V1.6 Security Target V1.13 (2007. 4. 23)
[6] NXG IPS 6000 V1.6 Evaluation Result Report, version 1.0 (2007. 6. 4)