KECS-CR-08-53

AhnLab Suhoshin Absolute v3.0
Certification Report

Certification No. : KECS-NISS-0136-2008

December 2008

National Intelligence Service
IT Security Certification Center

Revision history

No.	Date	Page	Revision
00	22 Dec. 2008	-	First draft

This document is the certification report on AhnLab Suhoshin Absolute v3.0 of AhnLab, Inc.

Certification Body

National Intelligence Service

Evaluation Facility

Korea System Assurance, Inc.

Table of Contents

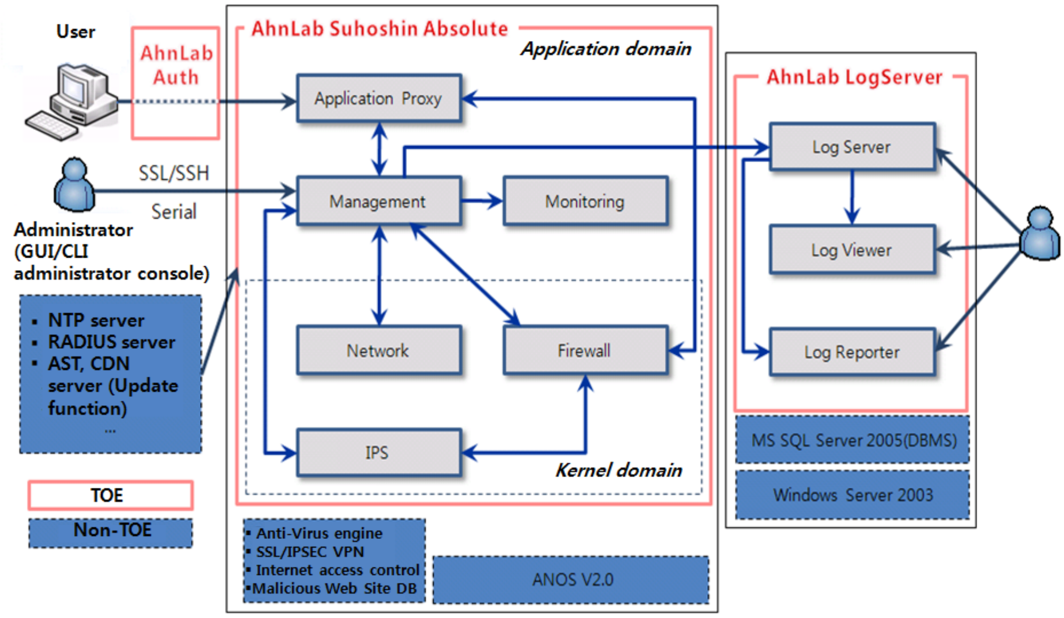
1. Overview

This report describes the certification result drawn by the certification body on the results of the EAL4 evaluation of AhnLab Suhoshin Absolute v3.0("TOE" hereinafter) with reference to the Common Criteria for Information Technology Security Evaluation (notified on 16 July 2008, "CC" hereinafter). It describes the evaluation result and its soundness and conformity.

The evaluation of the TOE has been carried out by Korea System Assurance, Inc. and completed on 5 Dec. 2008. This report grounds on the evaluation technical report(ETR) KOSYAS had submitted, in which the evaluation has confirmed that the product had satisfied the requirements of CC Part 2 and CC Part 3 and had been "suitable" according to the CC Part 1, paragraph 245.

The TOE is a UTM(unified threat management) system that performs network security features such as firewall(packet filtering and application filtering), IPS, anti spam, traffic control, system quarantine, and virus blocking by interoperating with an anti-virus engine. It is a network security device on an exclusive hardware platform that is connected in-line between an external network such as the Internet and the internal network of an organization. Accordingly, it processes all information transmitted between the internal and external network.

The TOE is comprised of AhnLab Suhoshin Absolute, which provides security functions such as packet filtering, application filtering, NAT, intrusion prevention, anti spam, and interoperation with an anti-virus engine; AhnLab LogServer, which gives management of audit data of the TOE; and AhnLab Auth, which authenticates a user.



[Figure 1] Architecture of the TOE

The CB has examined the evaluation activities and test procedures, provided the guidance for the technical problems and evaluation procedures, and reviewed each evaluation work package report and evaluation technical report.

Consequently, the CB has confirmed that the evaluation results had ensured that the TOE had satisfied all security functional requirements and assurance requirements specified in the ST.

Thus the CB has certified that observations and evaluation results made by the evaluator had been correct and reasonable, and the verdicts assigned by the evaluator on the product had been correct.

Certification validity: Information in this certification report does not guarantee that AhnLab Suhoshin Absolute v3.0 is permitted use or that its quality is assured by the government of Republic of Korea.

2. TOE identification

[Table 1] identifies the TOE.

[Table 1] TOE identification

Evaluation guidance	Korea IT Security Evaluation and Certification Guidance (16 Jul. 2008) Korea IT Security Evaluation and Certification Scheme (1 Sep. 2008)
TOE	AhnLab Suhoshin Absolute v3.0
Protection Profile	Firewall Protection Profile V2.0
Security Target	AhnLab Suhoshin Absolute v3.0 Security Target Version 001 Revision 5 (17 Oct. 2008)
ETR	AhnLab Suhoshin Absolute v3.0 Evaluation Technical Report V1.0
Evaluation result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation criteria	Common criteria for information technology security evaluation V3.1
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1
Sponsor	AhnLab, Inc.
Developer	AhnLab, Inc.
Evaluator	Hyunjung Lee, Taekyung Choi Korea System Assurance, Inc.
Certification body	National Intelligence Service

The TOE runs on an exclusive hardware platform, which is excluded from evaluation.

In general, a product with the TOE is identified according to the exclusive hardware platform. Detailed specification of the exclusive hardware platform for each product is as [Table 2] below.

[Table 2] Operational environment of the TOE system

TOE	Product	Specification
AhnLab Suhoshin Absolute	1000 R(0)	▪ CPU : Intel Pentium IV Xeon 2.8 GHz Dual ▪ RAM : 2 GB ▪ CF Memory : 2 GB ▪ NIC : 1000 Base-SX Gigabit Ethernet x 4 Ports 10/100 Ethernet x 4 Ports
	1000 R(1)	▪ CPU : Intel Pentium IV Xeon 3.4 GHz Dual ▪ RAM : 4 GB ▪ CF Memory : 2 GB ▪ NIC[Basic] : 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber) 10/100/1000 Ethernet x 4 Ports (Copper) 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber)(option) ▪ NIC[Selective] : 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber) 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber) 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber)(option)
	400 R(0)	▪ CPU : Intel Pentium IV Xeon 2.4 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100 Ethernet x 4 ports (Copper)
	400 R(1)	▪ CPU : Intel Pentium IV Xeon 2.8 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100/1000 Ethernet x 6 Ports (Copper) 1000 Base-SX Gigabit Ethernet x 2 Ports (Fiber)(option)
	400 R(2)	▪ CPU : Intel Pentium IV Xeon 2.8 GHz Dual ▪ RAM : 2 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100/1000 Ethernet x 4 Ports 1000 Base-SX Gigabit Ethernet x 2 Ports (Fiber)(option)
	100 R(0)	▪ CPU : Intel Pentium 4 1.8 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100 Ethernet x 4 Ports (Copper)
	100 R(1)	▪ CPU : Intel Mobile Celeron 1.2 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100 Ethernet x 4 Ports (Copper)

TOE	Item 항목	Specification
AhnLab Log Server	CPU	Pentium IV 2.66 GHz and above
	RAM	2 GB and above
	HDD	100 GB and above
	NIC	TCP/IP-based, 1 or more
	OS	MS Windows Server 2003
	Other S/W	MS SQL Server 2005
Administrator system	CPU	Pentium II 300 MHz and above
	RAM	128 MB and above
	HDD	2 GB and above
	Interface	TCP/IP-based, 1 or more; or RS-232C serial communication port
	OS	MS Windows XP Service Pack 2 and above

3. Security Policy

The TOE operates in conformance with the following security policies:

P.Audit To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained and reviewed.

P.Secure management The TOE shall provide management means for the authorized administrator to manage the TOE in a secure manner.

4. Assumptions and scope

4.1 Assumptions

The TOE shall be installed and operated with the following assumptions in consideration:

A.Physical security

The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.

A.Security maintenance

When the 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 the TOE operation policy so that security level can be maintained to be the same as before.

A.Trusted administrator

The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

A.Operating System reinforcement

Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.

A.Single connection point

All communications between the external and internal networks are carried out only through the TOE.

4.2 Scope to Counter a Threat

The TOE provides a means appropriate for the IT environment of the TOE to counter a security threat and a means to take actions on any logical/physical attacks launched by a threat agent possessing enhanced-basic expertise, resources, and motivation.

All security objectives and security policies are described such that a means to counter identified security threats can be provided.

5. TOE Information

The physical boundary of the TOE includes the UTM daemon package that is saved as a firmware in the CF memory on the exclusive TOE hardware platform, AhnLab Suhoshin Absolute Log Server, which is a TOE audit data management software in a CD, and AhnLab Auth S/W distributed during operation from the exclusive H/W.

- **UTM daemon package**

  The UTM daemon package includes a software module that performs features such as packet filtering, application filtering, NAT, intrusion prevention, malicious Email filtering and interoperation with the anti-virus engine.

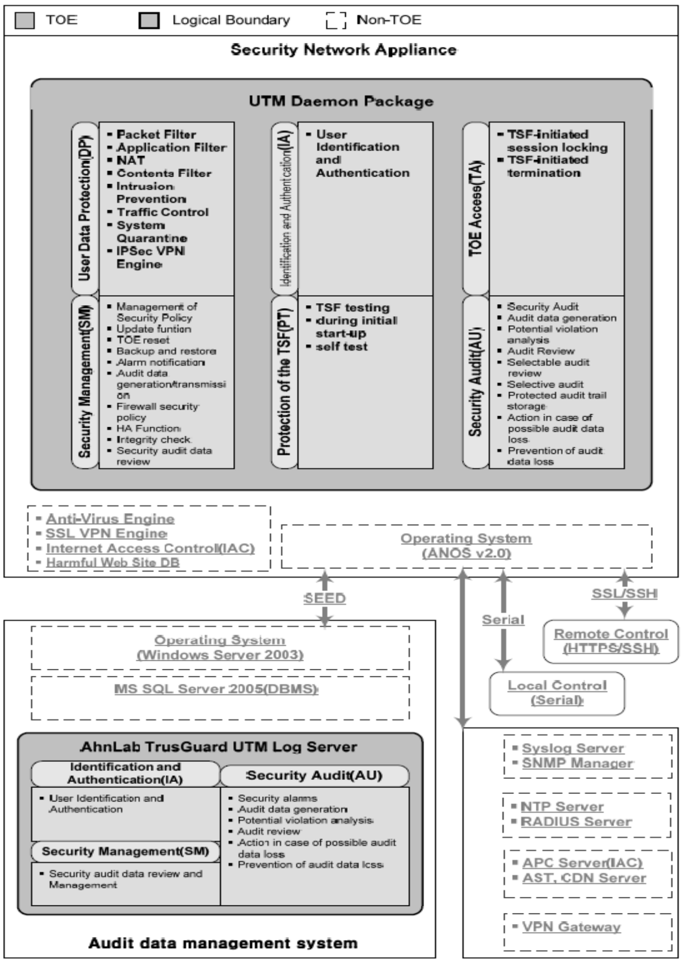
- **AhnLab LogServer**

  AhnLab LogServer is a TOE audit data management software, which has three installation files: Log Server 1.0.1.3(build21), Log Viewer 1.0.1.3(build21), and Log Reporter 1.0.1.3(build21).

- **AhnLab Auth S/W**

  AhnLab Auth software is used when the authorized administrator forces authentication policy as a specific policy of the security policies of application filtering. It is distributed in the form of firmware image along with ANOS. An end-user may download AhnLab Auth V1.0 S/W from the TOE to at the first authentication.

  The logical boundary of the TOE is as [Figure 2] shows, each security function of which is described below.


TOE
Logical Boundary
Non-TOE
Security Network Appliance
UTM Daemon Package
User Data Protection(DP)
▪ Packet Filter
▪ Application Filter
▪ NAT
▪ Contents Filter
▪ Intrusion Prevention
▪ Traffic Control
▪ System Quarantine
▪ IPSec VPN Engine
Identification and Authentication(IA)
▪ User Identification and Authentication
TOE Access(TA)
▪ TSF-initiated session locking
▪ TSF-initiated termination
Security Management(SM)
▪ Management of Security Policy
▪ Update funtion
▪ TOE reset
▪ Backup and restore
▪ Alarm notification
▪ Audit data generation/transmission
▪ Firewall security policy
▪ HA Function
▪ Integrity check
▪ Security audit data review
Protection of the TSF(PT)
▪ TSF testing
▪ during initial start-up
▪ self test
Security Audit(AU)
▪ Security Audit
▪ Audit data generation
▪ Potential violation analysis
▪ Audit Review
▪ Selectable audit review
▪ Selective audit
▪ Protected audit trail storage
▪ Action in case of possible audit data loss
▪ Prevention of audit data loss
▪ Anti-Virus Engine
▪ SSL VPN Engine
▪ Internet Access Control(IAC)
▪ Harmful Web Site DB
Operating System (ANOS v2.0)
SEED
Serial
SSL/SSH
Remote Control (HTTPS/SSH)
Local Control (Serial)
Operating System (Windows Server 2003)
MS SQL Server 2005(DBMS)
AhnLab TrusGuard UTM Log Server
Identification and Authentication(IA)
▪ User Identification and Authentication
Security Management(SM)
▪ Security audit data review and Management
Security Audit(AU)
▪ Security alarms
▪ Audit data generation
▪ Potential violation analysis
▪ Audit review
▪ Action in case of possible audit data loss
▪ Prevention of audit data loss
Audit data management system
▪ Syslog Server
▪ SNMP Manager
▪ NTP Server
▪ RADIUS Server
▪ APC Server(IAC)
▪ AST, CDN Server
▪ VPN Gateway

[Figure 2] Logical scope of the TOE

- Identification and authentication

The TOE identifies all users that attempts to access itself. Any user that attempts to access the TOE cannot use any of the TOE features before being identified. The TOE provides identification and authentication for a user, administrator, and log administrator.

The TOE may lock a user account if the specified number of failed login authentication is exceeded to protect the TOE from login attempts by malicious users. The authorized administrator can unlock the locked account through the TOE security management interface.

- Access control and information flow control

The TOE provides Packet Filter(Dynamic & Stateful Packet Filtering), Application Filter(Proxy), Network Address Translation(NAT), Contents Filter, Intrusion Prevention, and Quarantine to control access and information flow.

- Security management

The TOE provides features to manage its features and operation. It manages TSF data such as TOE operating configuration file and security features according to the security policies specified by the authorized administrator.

The TOE manages and saves network, service, user and security policy objects, and delivers the security policies to the firewall packet filter. All the contents of the shared memory are saved in the configuration file, and the file contents get encrypted. In other words, the contents of the configuration file get loaded on the shared memory when running the TOE and the changes settings are saved.

The TOE provides web based management interface through the HTTPS protocol. It runs security features according to the security policy specified by the administrator and manages TSF data such as TOE operating configuration file. It also provides the security functions through the CLI(Command Line Interface) used to manage the TOE and fix TOE errors.

Also, the security audit data is managed and checked through the AhnLab LogServer, a physically separated TOE.

- Security audit

The TOE saves the audit data during operation. It generates audit data when a security aduit event specified by the authorized administrator occurs. The audit data includes event date and time, type, subject identity, and event results (success or fail). Also, the authorized administrator can decide on whether to generate the audit data selectively according to the event type. If a potential security violation is detected, the TOE reports it to the authorized administrator in real time and only allows the authorized administrator to access the audit records of the DB saved in the TOE operating environment. Accordingly, it can protect the audit records from unauthorized deletion or modification.

- Protection of the TSF

Maintaining security when an error occurs: The TOE maintains and manages a list for operation status(e.g. start, stop, restart, reload) and important daemons which need to be restarted when an error occurs. It checks the status of the daemons to be managed regularly or at the authorized administrator's request and reloads an abnormally terminated daemon to secure normal services of the security functions.

Self test: The TOE generates hash values on the targets to check the integrity and compares them with the hash value (default value) saved during initial operation on every test interval. If integrity violation is detected, the TOE reports it to the authorized administrator through the TOE security management interface and generates audit data on it.

- TOE access

The TOE locks the session when the inactivity period of the authorized administrator has exceeded the specified period (10 minutes). The administrator must be reauthenticated to unlock the locked session.

The TOE terminates the session when an unauthenticated external entity starts a session through the TOE and the inactivity period has exceeded the session period specified by the authorized administrator. If the authorized administrator does not send/receive network traffic through the TOE for the specified session period for the service that forced user authentication (e.g., General TCP Proxy, HTTP Proxy, FTP Proxy), the session will be terminated. The administrator will be able to generate new session if the he or she requests for service again, and succeeds in getting reauthenticated.

6. Guidance

The TOE provides the following guidance documents:

- AhnLab Suhoshin Absolute v3.0 Operational User Guidance for UTM v1.0 Revision 33 (24 Oct. 2008)
- AhnLab Suhoshin Absolute v3.0 Operational User Guidance for LogServer v1.0 Revision 22 (1 Dec. 2008)
- AhnLab Suhoshin Absolute v3.0 Operational User Guidance v1.0 Revision 1 (26 Feb. 2008)
- AhnLab Suhoshin Absolute v3.0 Installation Guide v1.0 Revision 5 (24 Oct. 2008)

7. TOE Test

7.1 Developer's Test

- Test method

The developer had derived the test cases considering the TOE security functionality, which are explained in the test documents. Each test case includes the following information:

- Test No./Conductor: Identifier and test conductor of the test case
- Test purpose: Includes the security functions and modules to be tested
- Test configuration: Details about the test environment
- Test procedures detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator has assessed the appropriateness of the developer's test configuration, test procedures, analysis of coverage, and detail of testing and verified that the test and its results had been suitable for the evaluation configuration.

- Test configuration

The test configuration described in the tests includes details such as network configuration, evaluated product, PC, server, or evaluation tools required for each test case.

- Analysis of test coverage / Testing

Details of evaluation results are given in the ATE_COV and ATE_DPT WPRs.

- Test results

The test documents describe the expected and actual results of each test. The actual test result can be checked by the operating GUI menu and audit records.

7.2 Evaluator's Test

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results.

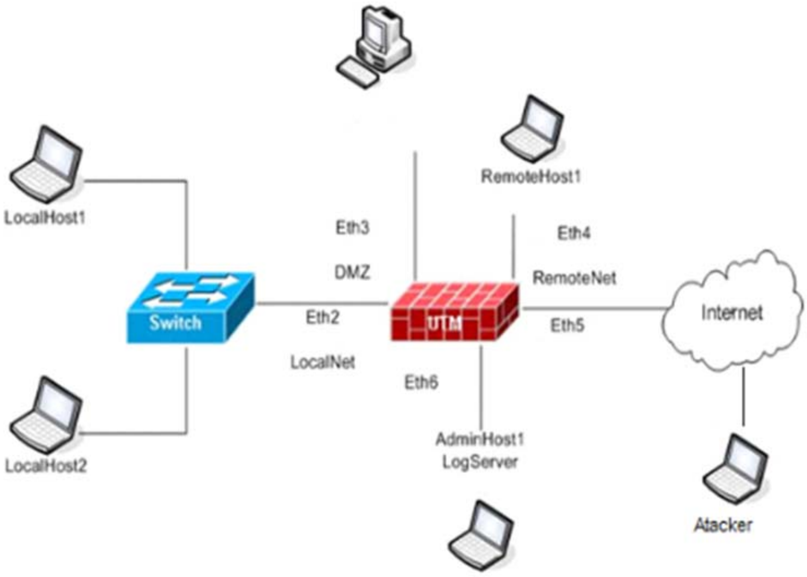
The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

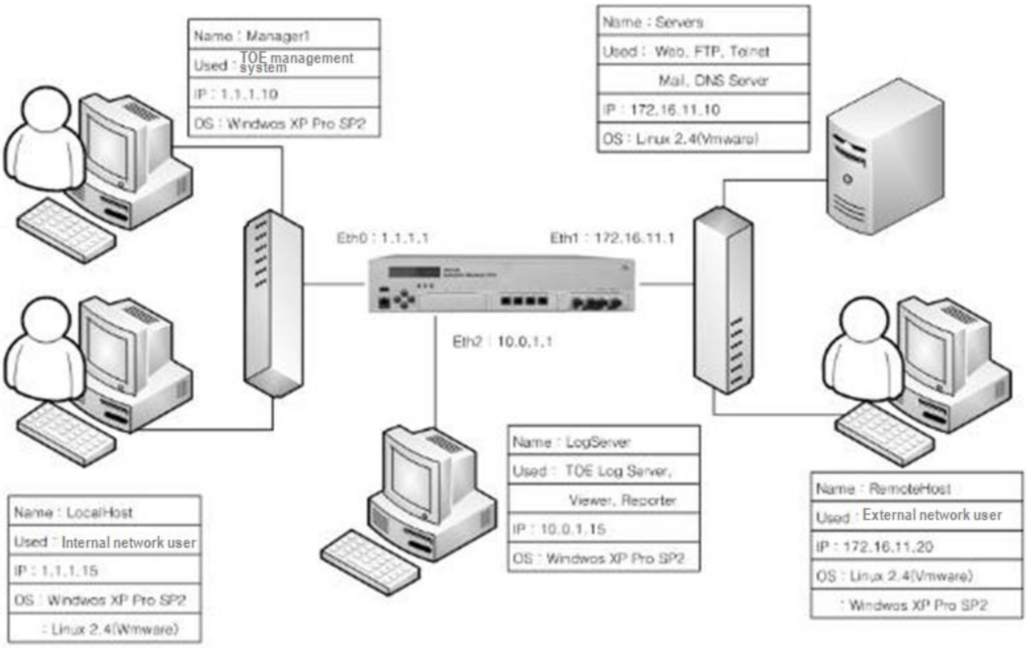
The evaluator's test result has ensured that the product had normally operated as described in the design documents.

8. Evaluation Configuration

The evaluator configured the test environment as shown in [Figure 3] to verify the developer's test and [Figure 4] for the evaluator's independent testing.



[Figure 3] Developer's test configuration



[Figure 4] Evaluator's test configuration

9. Evaluation Results

The evaluation is performed with reference to the CC V3.1 and CEM V3.1. The result claims that the evaluated product satisfies the requirements from the CC Part 2 and EAL4 in the CC Part 3. Refer to the evaluation technical report for more details.

- Security Target evaluation (ASE)

The ST introduction uniquely and correctly identifies the ST and TOE reference and describes the type, usage, major security features, physical and logical scope of the TOE to the extent of providing a reader general understanding.

Conformance claim includes the version of CC to which the TOE conforms, PP claim, and package claim and is described in consistent with the TOE type, security problem definition, and security objectives.

Security problem definition clearly describes the security problems that should be addressed by the TOE and its operational environment, that is, threats, organizational security policies(OSPs), and assumtions.

Security objectives counter the identified threats, achieve the OSPs, and address the assumptions properly and completely. The security problems are defined and categorized obviously into those for the TOE and for the operational environment.

The security requirements are described completely and consistently, and provides an appropriate basis for the development of the TOE to achieve the security objectives.

The TOE summary specification addresses all security functional requirements and defines them consistently with other parts of the ST.

Therefore, the ST is complete, consistent, and technically sound, and hence suitable for use as the basis for the TOE evaluation.

- Development evaluation (ADV)

The security architecture description gives a sufficient description about the architectural properties of the TSF regarding how the security enforcement of the TSF cannot be compromised or bypassed and how the security domain provided by the TSF is separated from another domains.

The functional specification adequately describes all security functions of the TOE and that the functions are sufficient to satisfy the security functional requirements of the ST. It also adequately describes the TSFIs(TSF interfaces) to the extent that a reader can understand how the TSF satisfies the TOE security policies.

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It also describes that the SFRs are completely and accurately implemented in terms of the SFR-enforcing, SFR-supporting, and SFR-non-interfering modules.

The implementation representation is sufficient to satisfy the security functional requirements in the ST and accurately implements the TOE design.

Therefore, the development documentation is adequate to give understanding about how the TSFs are provided, as it consists of a functional specification (which describes the interfaces of the TSF), a TOE design (which describes the architecture of the TOE in terms of subsystems and modules), an implementation representation (a source code level description), and a security architecture description (which describes how the TSF enforcement cannot be compromised or bypassed).

- Guidance documents evaluation (AGD)

The preparative procedures documentation describes the procedures to progress the delivered TOE to the evaluated configuration as the operational environment described in the ST. Consequently, the evaluator has confirmed that the TOE had been securely configured.

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

Therefore, the guidance documents give a suitable description of how a personnel who installs, manages, and operates can administer the TOE in a secure way.

- Life cycle support evaluation (ALC)

The configuration management documentation describes that the changes to the implementation representation are controlled with the support of automated tools. It also clearly identifies the TOE and its associated configuration items and describes that the ability to modify these items is properly controlled.

The evaluator has confirmed by the CM documentation that the developer had performed configuration management on the TOE implementation representation, evaluation evidence required by the assurance components in the ST, and security flaws.

Therefore, the evaluation of configuration management assists the consumer in identifying the evaluated TOE, ensures that the configuration items are uniquely identified, and ensures the adequacy of the procedures that are used by the developer to control and track changes that are made to the TOE.

The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site.

Therefore, the delivery documentation is adequate to ensure that the TOE is delivered in the same way the developer intended without modification.

The evaluator has confirmed that:

the developer's security controls on the development environment had been adequate to provide the confidentiality and integrity of the TOE design and implementation that are necessary to ensure secure operation of the TOE;

the developer had used a documented model of the TOE life-cycle; and

the developer had used well-defined development tools that yield consistent and predictable results.

Therefore, the life-cycle support provides an adequate description of the security procedures and tools used throughout TOE development and the procedures of the development and maintenance of the TOE.

- Tests evaluation (ATE)

The tests have been sufficient to establish that the TSF had been systematically tested against the functional specification.

The evaluator has confirmed that the developer had tested the security functions of the TOE in the TOE design.

The developer's test documents had been sufficient to show the security functions had behaved as specified.

The evaluator has determined, by independently testing a subset of the TSF, that the TOE had behaved as specified and gained confidence in the test results by performing all of the developer's tests.

Therefore, the tests have proved that the TSF had satisfied the TOE security functional requirements specified in the ST and behaved as specified in the design documentation.

- Vulnerability assessment evaluation (AVA)

The vulnerability analysis adequately describes the obvious security vulnerabilities of the TOE and the countermeasures such as the functions implemented or recommended configuration specified in the guidance documentation. The evaluator has confirmed by performing penetration testing based on the evaluator's independent vulnerability analysis that the developer's analysis had been correct.

The evaluator has determined by performing vulnerability analysis that there had not been any vulnerabilities exploitable by an attacker possessing an enhanced-basic attack potential in the intended TOE environment.

Therefore, based on the evaluator's vulnerability analysis and penetration testing, the evaluator has confirmed that there had been no flaws or vulnerabilities exploitable in the intended environment for the TOE.

10. Recommendations

The TOE is guaranteed security only in the evaluated operational environment. Therefore, one should take the following in consideration while operating the TOE:

① The TOE applies DAC, LBAC, intrusion prevention policy, application filter policy, and QoS policy in order. Therefore, the security administrator of the TOE should fully understand the access control features before applying policies.

② The security administrator can manage the audit data generated from more than one AhnLab Suhoshin Absolute using AhnLab Suhoshin Absolute LogServer. He should set the time of system in which AhnLab Suhoshin Absolute accurately because if the time information of each data does not match, the audit data is not reliable.

③ In case that a threshold of the storage is met, the TOE alarms the administrator by sending an email. When the threshold is exceeded, it either stops security functions or overwrites the oldest audit data. So in order to ensure traceability of security-relevant events, the security administrator should regularly check the audit storage of AhnLab Suhoshin Absolute and AhnLab Suhoshin Absolute LogServer and an email to back up the audit data before the storage is exhausted.

④ The TOE will be distributed with a default ID/PW established. To prevent threat to identification and authentication, the security administrator should change the ID/PW at initialization/operation before using the TOE. Also regular change of ID/PW is recommended during using the TOE because it does not provide an automatic PW change.

⑤ The TOE will be distributed with the session time limit, number of simultaneous proxy connection, and action in case of intrusion detection established without consideration of actual operating environment. So the security administrator should check the network and security status of the environment in which the TOE will be installed and change the values accordingly.

⑥ Since the TOE does not provide automatic backup for the configuration file, the security administrator should regularly back up the files when he changed the configuration in preparation for possible TOE errors.

11. Acronyms and Glossary

The following acronyms are used in this report:

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

The following terms are used in this report:

TOE	Target of evaluation; a set of IT product or system accompanied by guidance
Audit log	Data that stores events related to the security of the TOE
User	Any entity outside the TOE that interacts with the TOE: human user or external IT entity
Authorized administrator	A user who administers the TOE securely in accordance with the TOE security policy
Authorized user	A user who may, in accordance with the SFRs, perform an operation
External entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE

12. Reference

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

[1] Common Criteria for Information Technology Security Evaluation V3.1

[2] Common Methodology for Information Technology Security Evaluation V3.1

[3] Korea IT Security Evaluation and Certification Guidance (16 Jul. 2008)

[4] Korea IT Security Evaluation and Certification Scheme (1 Sep. 2008)

[5] AhnLab Suhoshin Absolute v3.0 Security Target Version 001 Revision 5 (17 Oct. 2008), AhnLab, Inc.

[6] AhnLab Suhoshin Absolute v3.0 Evaluation Technical Report V1.0 (5 Dec. 2008)