KECS-CR-13-28

AhnLab TrusGuard V2.2

Certification Report

Certification No.: KECS-NISS-0459-2013

2013. 8. 12

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2013.8.12	-	Certification report for AhnLab TrusGuard V2.2 - First documentation

This document is the certification report for AhnLab TrusGuard V2.2 of AhnLab Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance, Inc. (KoSyAs)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL2 evaluation of AhnLab TrusGuard V2.2 developed by AhnLab Inc.. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

AhnLab TrusGuard V2.2 (hereinafter TOE) is a type of firewall and VPN. The TOE is a software type that is delivered to the final user as loaded on a dedicated hardware model of AhnLab TrusGuard 10000P R(2)(see Table 1).

Type	Description
CPU	Intel® Xeon® E5645 Six-Core 2.4 GHz * 2
Memory	4 GB DDR3 Memory * 4
CF	2 GB CF Memory
HDD	2 TB S-ATA2
NIC	10/100/1000 BASE-TX * 14 1 Gbps SFP * 8 10 Gbps SFP+ * 2
Console	RJ45 * 1
Size	431.8 mm * 580 mm * 88 mm (W*D*H)
PSU	Redundant, 500W, 5V/30A, 12V/32A, 3.3V/24A

[Table 1] TOE hardware model(AhnLab TrusGuard 10000P R(2))

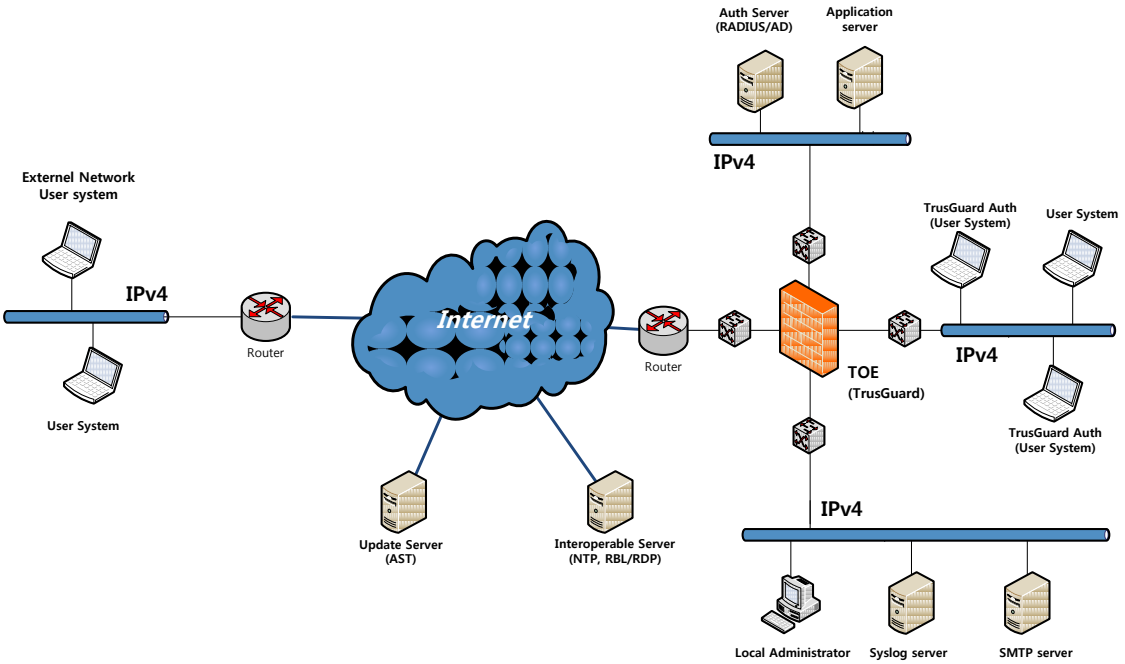
The TOE components consist of TrusGuard Gateway, TrusAnalyzer and SSL VPN Client, and Authorized Client. These TOE components are separately installed and managed on the network.

The evaluation of the TOE has been carried out by KoSyAs and completed on July. 12, 2013. This report grounds on the evaluation technical report (ETR)[2] that KoSyAs had submitted and the Security Target (ST)[3].

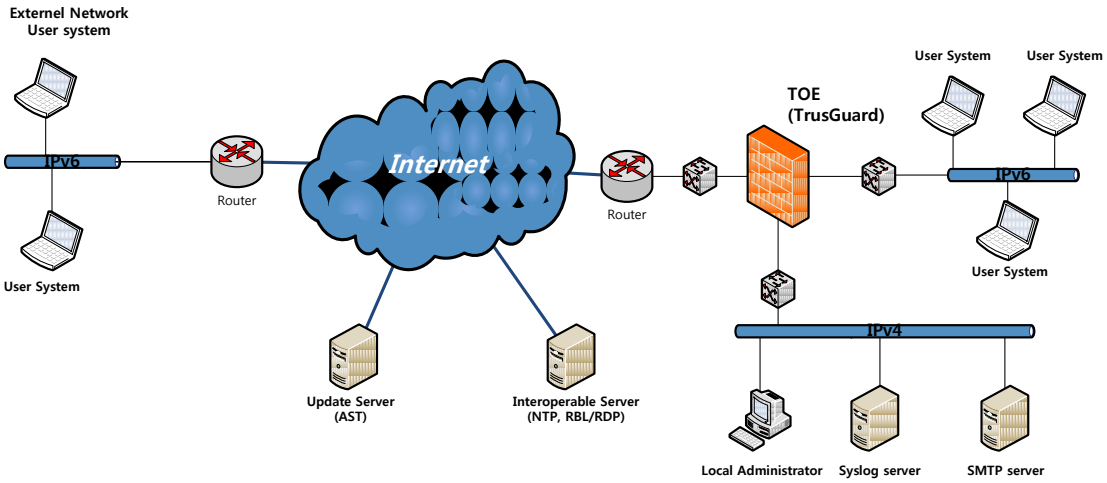
The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL2. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and

the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

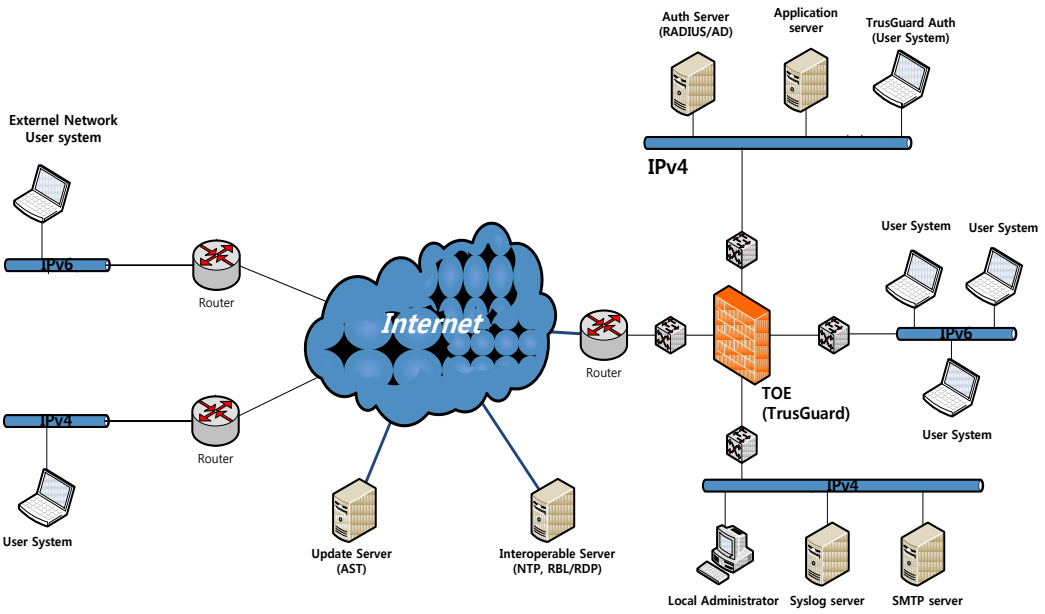
The TOE operating environments are shown from [Figure 1] through [Figure 5]. The TOE can be operated in the IPv4 and IPv6 networks by configuring VPN or HA environments. The TOE for TrusGuard Gateway is operated in the router mode or in the bridge mode on the network boundary. In the router mode, the TOE is operated on the network boundary in different IP address ranges. In the bridge mode, the TOE is operated in the network environment in same IP address ranges.



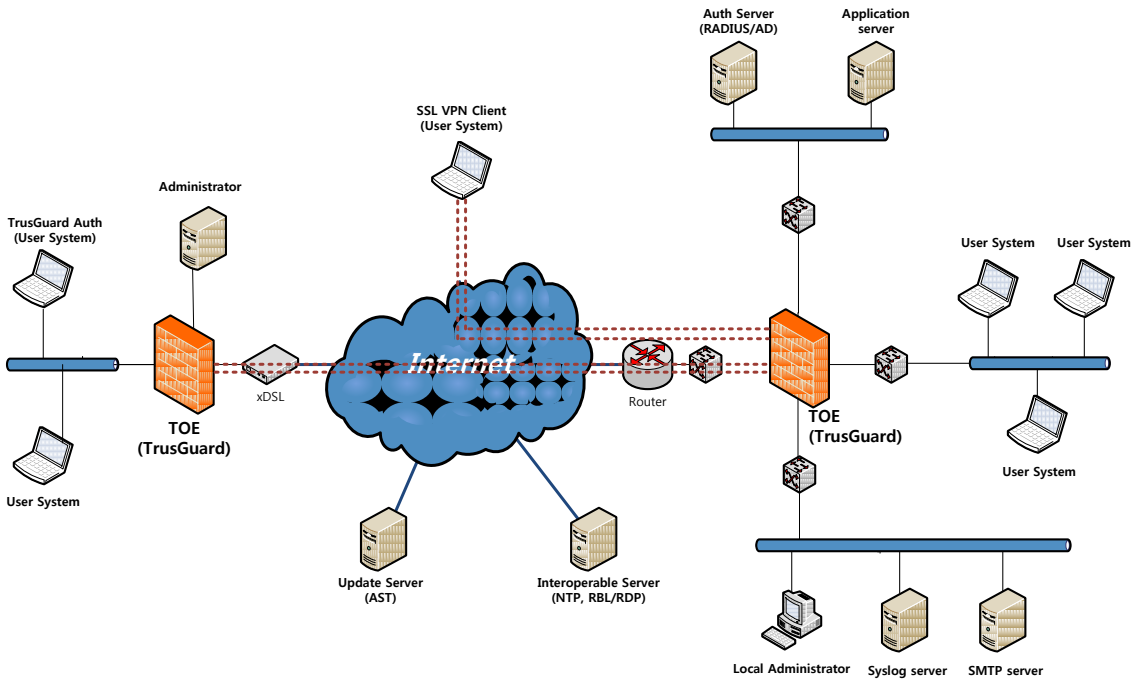
[Figure 1] TOE operating environment examples (Dedicated IPv4 network)



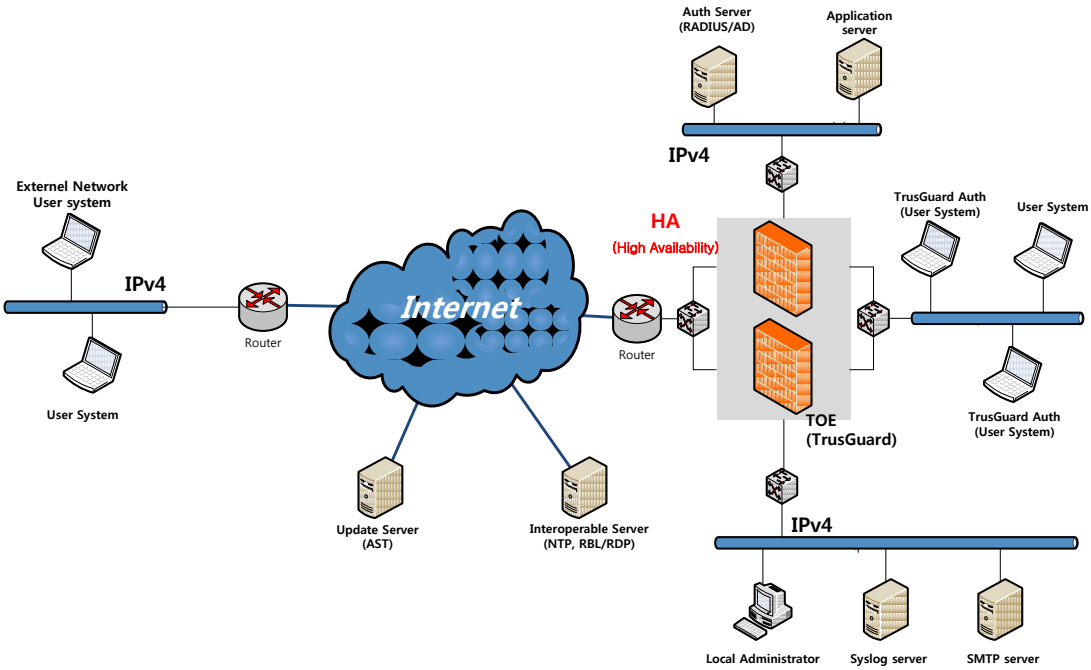
[Figure 2] TOE operating environment examples (Dedicated IPv6 network)



[Figure 3] TOE operating environment examples (IPv4 VPN network)



[Figure 4] TOE operating environment examples (Dedicated IPv6 network)



[Figure 5] TOE operating environment examples (IPv4 HA network)

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to the certificate, and no warranty of the IT Product by the government of Republic of Korea or by any other organization that recognizes or gives effect to the certificate, is either expressed or implied

2. Identification

The TOE title is AhnLab TrusGuard V2.2, consisting of the following components and related guidance documents and they are identified as described in [Table 2].

Type	Identifier		Delivery Form
SW	AhnLab TrusGuard V2.2.0.8	AhnLab TrusGuard Gateway 2.2.0.5	Firmware loaded on a Hardware
		AhnLab TrusAnalyzer 1.0.2.12	Software
		AhnLab TrusGuard Auth 1.0.0.33	Software
		AhnLab TrusGuard SSL VPN Client 1.0.3.2	Software
DOC	AhnLab TrusGuard V2.2 Administrator Guide (2013.07.30.01)		Booklet
	AhnLab TrusGuard V2.2 Command Guide (2013.07.30.01)		Booklet
	AhnLab TrusGuard V2.2 Product Installation Guide (2013.07.30.01)		Booklet

[Table 2] TOE identification

[Table 3] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009)[4] Korea Evaluation and Certification Regulation for IT Security (November 1, 2012)[5]
TOE	AhnLab TrusGuard V2.2
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL 2
Developer	AhnLab Inc.

Sponsor	AhnLab Inc.
Evaluation Facility	Korea System Assurance, Inc. (KoSyAs)
Completion Date of Evaluation	July 12, 2013
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The TOE complies with security policies defined in the ST [3] by security objectives and security requirements. The TOE provides the security functions to protect web server and web application by detecting and blocking web attack based on main security features as follows :

The TOE complies with security polices defined in the ST[3] by security objectives and security requirements. The TOE provides the security functions as follows.

- Access Control at Network Level(Firewall)
- VPN (IPSec VPN, SSL VPN)
- Translate network addresses
- Abnormal Traffic Blocking
- Contents filtering
- High Availability (HA)
- Audit Data Management
- Security management

In addition, the TOE provides security features to identify and authenticate authorized users, to generate audit records of the auditable events including start-up and shut-down of audit functions, and to securely manage the TOE including setting of detection rules.
For more details refer to the ST [3].

4. Assumptions and Clarification of Scope

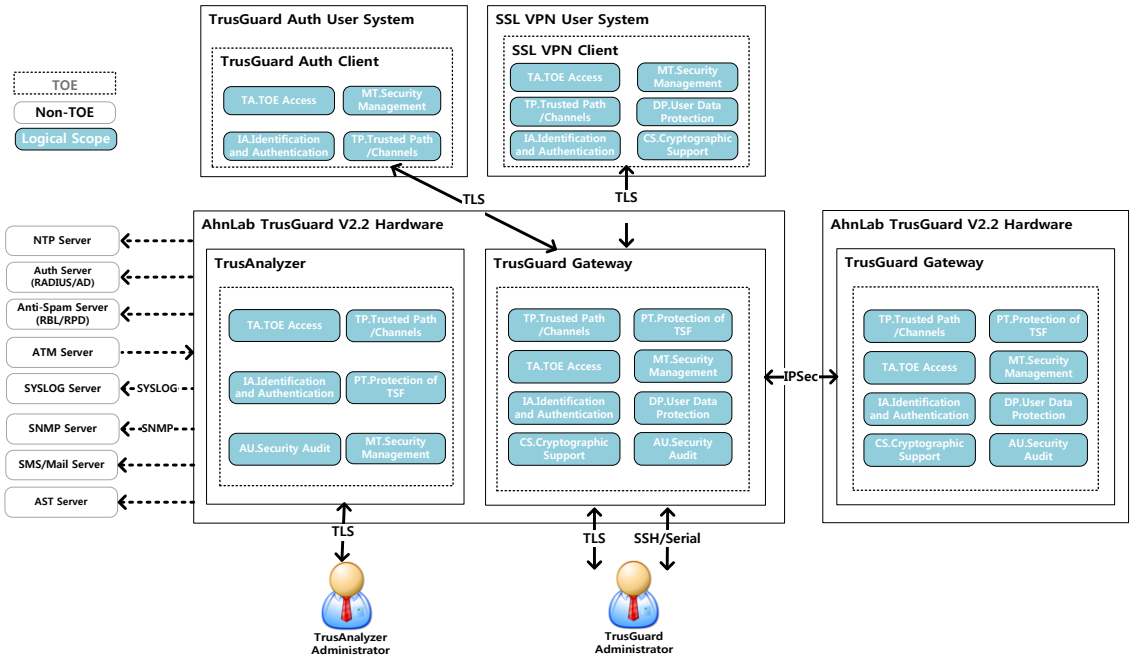
The following assumptions describe the security aspects of of the environment in which the TOE will be used or is intended to be used in order to limit the scope of security consideration(for the detailed and precise definition of the assumption refer to the ST [3], chapter 3.3) :

- The TOE and administrator systems are placed in physically safe environments where only authorized administrators can access them.
- The security level should be maintained steadily even when internal network environments are changed (ex. network configuration changes, host increase and service increase/decrease) by immediately applying environmental changes and security policy changes to TOE operating policies.
- Authorized TOE administrators who are properly trained to use TOE management functions with good intentions can perform their roles and responsibilities in accordance to the administrators' guidelines.
- The operating systems for the TOEs (TrusGuard Gateway and TrusAnalyzer) provide reliability and high availability by addressing OS vulnerabilities and removing unnecessary services. The operating sub-systems of the TOEs (Authentication Client and SSL Client) are safe and reliable.
- AST(AhnLab Service Tower) servers for update and customer license verification, NTP servers for trusted timestamps, user authentication server for user authentications, anti-spam servers for proxy functions, mail servers for alarm messages and SMS server are safely managed to provide reliability.
- All communications between external networks and internal networks are possible only via the TOE.

For the detailed information on the lists of threats, refer to the ST [3], chapter 3.2. For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

5. Architectural Information

This chapter explains the logical scope of the TOE and the main components as shown in [Figure 6].



[Figure 6] TOE logical scope

The TOE for TrusGuard Gateway is installed in a firmware format on the CF memory of the dedicated hardware platform to be distributed to end users. The version of the TOE for TrusGuard Gateway can be verified using SSL/TLS-based web interfaces or SSH/Serial-based command interfaces (CLIs). The version is identified as below:

- AhnLab TrusGuard Gateway 2.2.0.5

The TOE for TrusAnalyzer is a software product that saves and manages audit data. The TOE for TrusAnalyzer is installed in the ANOS operating system and deployed along with the TOE as part of the TrusGuard hardware model. The version is identified as below.

- AhnLab **TrusAnalyzer** 1.0.2.12

The TOE Authentication Client and the TOE SSL VPN Client are installed in general PCs. The TOE for Authentication Client performs user identification and authentication

when the TOE for TrusGuard Gateway requests them using the content filtering function before arbitrating user information flows. The TOE for SSL VPN Client performs security functions through VPN along with the TOE for TrusGuard Gateway to protect user information flows.

Two software products are included in the TOE for TrusGuard Gateway firmware. Both can be downloaded and installed from the TOE for TrusGuard Gateway when general users leverage the proxy function and the SSL VPN function. Deployment and installation of two software products proceed through web browsers when the security policies are initially applied to the users. Two software products are identified as below:

- AhnLab TrusGuard Auth 1.0.0.33
- AhnLab TrusGuard SSL VPN Client 1.0.3.2

For detailed information on security functions, please refer to chapters 1.3, 1.4.2 and 7 of ST [3].

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Version	Date
AhnLab TrusGuard V2.2 Administrator Guide	V2.2	2013.07.30
AhnLab TrusGuard V2.2 Command Guide	V2.2	2013.07.30
AhnLab TrusGuard V2.2 Product Installation Guide	V2.2	2013.07.30

[Table 4] Documentation

7. TOE Testing

The developer took a testing approach deriving test cases regarding the TOE components and security functions including detection rules against web vulnerabilities,

which are described in the tests. Each test case includes the following information :

- Test no. and conductor: Identifier of each test case and its conductor
- Test purpose: Includes the security functions and modules to be tested
- Test configuration: Details about the test configuration
- Test procedure 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 developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.1. This means that the developer tested all the TSFI defined for each life cycle state of the TOE, and demonstrated that the TSF behaves as described in the functional specification.
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. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [2].

8. Evaluated Configuration

The evaluated configuration of the TOE is identified by the name, major version and minor version as mentioned in [Table 2]. For information about type names in relation to the hardware platform and software, please read chapters 1.3 and 1.4 of ST [3].

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [2] which references Single Evaluation Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1] and CEM [6].
As a result of the evaluation, the verdict PASS is assigned to all assurance

components of EAL 2.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The ST doesn't define any extended component. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be use as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer clearly identifies the TOE and its associated configuration items, that the ability to modify these items is properly controlled by automated tool, and that as a result, the errors caused by someone's mistake or negligence in the configuration management system decrease. Therefore the verdict PASS is assigned to ALC_CMC.2.

The configuration management document verifies that the configuration list includes

the TOE, the TOE elements, the TOE implementation representation, security flaws, evaluation deliverables, and development tools. Therefore, the verdict of ALC_CMS.2 is the Pass.

The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, and the delivery activity.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The security architecture document is structured to ensure that TSF cannot be compromised or bypassed, and appropriately describes that the TSF which provides the security domain separates these domains from each other. Therefore, the verdict of ADV_ARC.1 is the Pass.

The functional specifications specifies the objective, way of using, input parameter, operation, and error message to the TSFI at equal detail level, and accurately and completely describes the TSFI. Therefore, the verdict of ADV_FSP.2 is the Pass.

The TOE design description provides environment and overall TSF description to describe TSF, provides sufficient TOE description with respect to subsystem to determine the TSF boundary, and provides description about the TSF internals with respect to module. Hence the TOE design provides the description about the implementation representation. Therefore, the verdict of ADV_TDS.1 is the Pass.
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.1.
The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).
The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.2.
Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don’t allow attackers possessing basic attack potential to violate the SFRs.
The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	PASS
	ALC_CMC.2	ALC_CMC.2.1E	PASS	PASS	
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.1	ADV_TDS.1.1E	PASS	PASS	PASS
		ADV_TDS.1.2E	PASS		
	ADV_FSP.2	ADV_FSP.2.1E	PASS	PASS	
		ADV_FSP.2.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
	ATE_COV.1	ATE_COV.1.1E	PASS	PASS	
AVA	AVA_VAN.2	AVA_VAN.2.1E	PASS	PASS	PASS
		AVA_VAN.2.2E	PASS		
		AVA_VAN.2.3E	PASS		
		AVA_VAN.2.4E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- In the case of using IPv6 stateless address, its assign address could be change periodically, it is recommended to use static address method to enforce network access control rules efficiently.

11. Security Target

The AhnLab TrusGuard V2.2 Security Target V1.8, July 30, 2013 [3] is included in this report by reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
Access control at Network Level (Firewall system)	A software/hardware-based network security system (called a firewall) implemented on network gateways in in-line mode to protect internal networks connected to the Internet against malicious intrusions. Based upon IP addresses and port numbers, the Firewall system blocks all traffic that does not match rules allowed by authorized administrators. It allows connections from the internal

network to the external network but blocks connections from the external network to the internal network to protect internal network resources from security threats.

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] KOSYAS-2013-30, AhnLab TrusGuard V2.2 Evaluation Technical Report V2.00, July 31, 2013

[3] AhnLab TrusGuard V2.2 Security Target V1.8, July 30, 2013

[4] Korea Evaluation and Certification Guidelines for IT Security(September 1, 2009)

[5] Korea Evaluation and Certification Regulation for IT Security (November , 2012)

[6] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012