KECS-CR-08-10

Firewall Protection Profile V2.0 Certification Report

Certification No. : KECS-PP-0093-2008

Apr, 2008

National Intelligence Service
IT Security Certification Center

This document is the certification report for Firewall Protection Profile V2.0.

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Summary

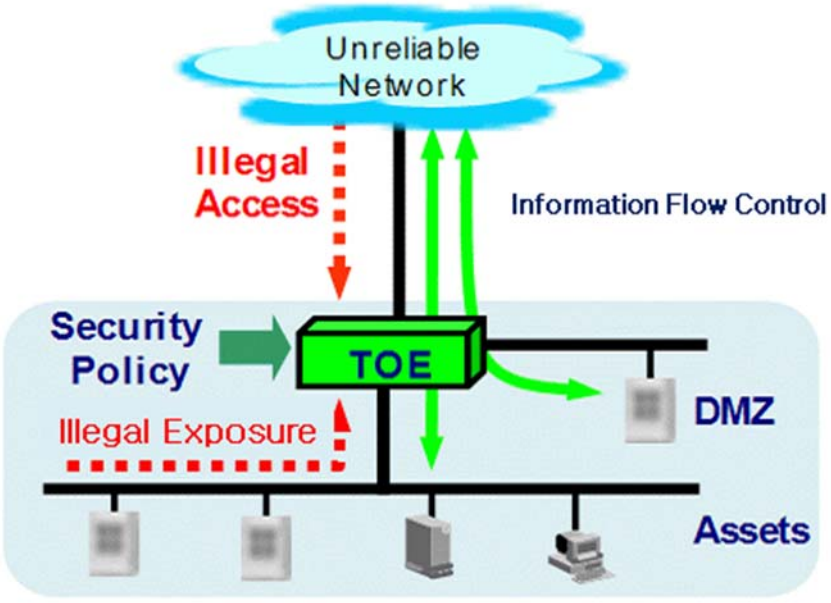
This report describes the certification results by the certification body on the evaluation results applied with requirements of APE(Protection Profile Evaluation) Class of Common Criteria for Information Security Evaluation (‘CC’ hereinafter) in relation to Firewall Protection Profile V2.0. This report describes the evaluation result and its soundness and confirmity.

The evaluation on Firewall Protection Profile V2.0 was conducted by Korea Information Security Agency and completed on April 1, 2008. Contents of this report have been prepared on the basis of the contents of the ETR submitted by Korea Information Security Agency. The evaluation was conducted by applying CEM. This PP satisfies all APE requirements of the CC, therefore the evaluation results were decided to be ‘suitable’.

The TOE is located where the external network, such as the Internet, and the internal network of Organization are connected and executes security functions, all information transferred between the internal and external networks shall pass through the TOE. A firewall can be configured in the forms of dual-homed, screened-host and screened-subnet, etc. Diverse installation types and operation methods of a firewall can be used.

(Figure 1) shows the operational environment and the key security functions of the TOE.

Assets to be protected by the TOE are the protected target system (network services and resources, etc., protected by the security policies of the firewall) that exist in the internal network of organization. Also, the TOE itself and the important data of the inside of the TOE (security attributes and TSF data, etc.) are assets to be protected by the TOE.



(Figure 1) TOE operational environment

The TOE executes the functions of security audit, information flow control, user identification and authentication, security management and other TSF protection, etc.

■ Security Audit

The TOE generates, records and reviews audit record of the security-related events in order to trace responsibilities for the security-related activities. Also, the TOE detects potential security violation of the audited events and takes the response actions

■ Information flow control

The TOE ensures that the related security policies are executed in order to mediate information flow.

■ Identification and Authentication

The TOE identifies and authenticates the user identity and defines TSF actions in cases of authentication failures.

■ Security Management

The TOE manages security functions, security attributes, TSF data and security roles, etc.

■ Other TSF Protection

The TOE executes self tests in order to verify integrity of TSF data and executable code. The TOE provides session management functions after time interval of user inactivity.

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

Certification validity: Information in this certification report does not guarantee that Firewall Protection Profile V2.0 is permitted use or that its quality is assured by the government of Republic of Korea.

2. Information for Identification

[Table 1] shows information for the PP identification.

[Table 1] Shows Information for the PP Identification.

Scheme	Korea evaluation and certification guidelines for IT security (Notification No.2007-31 by the MIC, 22 Aug. 2007) Korea Evaluation and Certification Scheme for IT Security(NIS, 1 Dec. 2007)
TOE	Firewall Protection Profile V2.0
ETR	Firewall Protection Profile ETR V1.0 (Apr. 1, 2008)
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation v2.3
Sponsor	Korea Information Security Agency
Developer	Korea Information Security Agency
Evaluator	IT Security Evaluation Division, CC Evaluation Lab, Korea Information Security Agency H. J. Jang
Certification body	National Intelligence Service

3. Security Policies

The TOE of Firewall Protection Profile V2.0 shall comply with the following Organizational Security Policies.

P. Audit	To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained 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 of Firewall Protection Profile V2.0 shall be installed and operated with the following assumptions in consideration.

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. 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. Single Point of Connection	All communications between the external and internal networks are carried out only through the TOE.
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.

4.2 Scope to Counter Threats

The Threat agent is generally IT entities and human users who exert damage to the TOE and internal assets in abnormal methods or attempt illegal access to the TOE and internal assets from outside. The Threat agent has enhanced-basic level of expertise, resources and motivation.

T. Address Spoofing	The threat agent of the external network may try to access the internal network by spoofing the source IP address as an the internal IP address.
T. Continuous Authentication Attempt	The threat agent can acquire the authorized user rights by attempting continuous authentication to access the TOE.
T. Illegal Information Inflow	The threat agent can violate the internal network with inflow of not allowed information from outside.
T. Illegal Information Outflow	The Internal user can have illegal information exposed to the outside through the network.
T. Impersonation	The threat agent can access the TOE by masquerading as an authorized user.
T. Recording Failure	The threat agent can disable recording of security-related events of the TOE by exhausting storage capacity.
T. Replay Attack	The threat agent can access the TOE by replaying the authentication data of an authorized user.
T. Stored Data Damage	The threat agent can expose, modify and delete TSF data stored in the TOE in an unauthorized method.

5. PP Information

5.1 Security Functional Requirements

The TOE of Firewall Protection Profile V2.0 defines security functional requirements as of the following.

[Table 2] Security Functional Requirements

Security Functional Class	**Security Functional Components**	
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination

5.2 Assurance Packages

Assurance requirements of [Firewall Protection Profile V2.0] consist with assurance components in the CC Part 3 and evaluation assurance level is “EAL4.”

6. Evaluation Results

The evaluation is performed with reference to the CC V3.1r2 and CEM V3.1r2. The verdict of Firewall Protection Profile V2.0 is the pass as it satisfies all requirements of APE(Protection Profile Evaluation) Class of CC. Therefore, the evaluation results were decided to be suitable. Refer to the ETR for more details.

The PP introduction demonstrates that the PP is correctly identified, that the PP reference and TOE overview are consistent with each other. Therefore, the verdict of APE_INT.1 is the Pass.

The conformance claim determines the validity of the conformance claim that indentifies the CC and Package which the PP claims conformance. Therefore, the verdict of APE_CCL.1 is the Pass.

The security problem definition defines the security problem to be addressed by the TOE and its operational environment. The security problem definitions shall describe the threats, OSP(organizational security policy)s and assumptions. Therefore, the verdict of APE_SPD.1 is the Pass.

The security objectives demonstrate that the security objectives adequately and completely address the security problem definition and that the division of this problem between the TOE and its operational environment is clearly defined. Therefore, the verdict of APE_OBJ.2 is the Pass.

The Extended components definition is only applicable if the PP contains IT security requirements that are explicitly stated without reference to either CC Part 2 or CC Part 3. If this is not the case, all work units in this section are not applicable, and considered to be satisfied. Therefore the verdict of APE_ECD.1 is the Pass.

The SFRs form a clear, unambiguous and well-defined descriptions in relation to the expected security behaviors of the TOE. Also, SARs form a clear, unambiguous and well-defined descriptions of the expected activities that will be undertaken to gain assurance in the TOE. Therefore, the verdict of APE_REQ.2 is the Pass.

The Evaluator reached the final conclusions on evaluation of Firewall Protection Profile V2.0 as of the following. ‘Firewall Protection Profile V2.0’ is complete, consistent and technically sound, therefore is suitable to lead to the development of the ST.

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

Assurance Class	Assurance Components	Evaluator action elements	verdict		
			Evaluator action elements	Assurance Components	Assurance Class
APE	APE_INT.1	APE_INT.1.1E	Pass	Pass	Pass
	APE_CCL.1	APE_CCL.1.1E	Pass	Pass	
	APE_SPD.1	APE_SPD.1.1E	Pass	Pass	
	APE_OBJ.2	APE_OBJ.2.1E	Pass	Pass	
	APE_ECD.1	APE_ECD.1.1E	Pass	Pass	
		APE_ECD.1.2E	Pass		
	APE_REQ.2	APE_REQ.2.1E	Pass	Pass	

7. Recommendations

This PP includes the minimum security requirements and does not make definition on implementation model of the TOE. In relation to security-related considerations possible to occur according to the model of the TOE implemented(or to be implemented), the ST author shall define additional security problems, security objectives and security requirements.

8. Acronyms

The following acronyms have been used in this report.

EAL Evaluation Assurance Level
ETR Evaluation Technical Report
OR Observation Report
PP Protection Profile
TOE Target of Evaluation
WPR Work Package Report

9. References

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

[1] Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25)

[2] Common Methodology for Information Technology Security Evaluation V2.3

[3] Korea evaluation and certification guidelines for IT security (Notification No.2007-31 by the MIC, 22 Aug. 2007)

[4] Korea Evaluation and Certification Scheme for IT Security(NIS, 1 Dec. 2007)

[5] Firewall Protection Profile ETR V1.0(Apr. 1, 2008)