AhnLab Suhoshin Absolute v3.0

Security Target

Version 001
Revision 6

Ahnlab Inc.
6th FL, CCMM Bldg, 12 Yeouido-dong, Yeongdeungpo-gu, Seoul, Korea
http://www.ahnlab.com

CONTENTS

List of Tables

List of Figures

1 Security Target introduction

1 This document serves as the AhnLab Suhoshin Absolute v3.0 Security Target for the Common Criteria) EAL4.

1.1 ST reference

2 The Security Target is for:

- Title: AhnLab Suhoshin Absolute v3.0 Security Target
- Version/Revision No.: 001-06
- Author: Ahnlab, Inc.
- Publication Date: 2009-01-09
- Identification No.: Absolute-STD-001-06
- File name: Absolute-STD-001.doc

1.2 TOE reference

3 The TOE consists of:

- Developer: AhnLab, Inc.
- TOE/Version: AhnLab Suhoshin Absolute v3.0
  - UTM Daemon Package
    - pkg 1.0.6.0-60[1]
  - AhnLab Suhoshin Absolute Log Server 1.0.1.3 (build21)
    - Log Server 1.0.1.3 (build21), Log Viewer 1.0.1.3 (build21), Log Reporter 1.0.1.3 (build21)

[Reference] The TOE is identified as below, according to the used hardware platform.

- AhnLab Suhoshin Absolute 1000 R(0) v3.0
- AhnLab Suhoshin Absolute 1000 R(1) v3.0
- AhnLab Suhoshin Absolute 400 R(0) v3.0
- AhnLab Suhoshin Absolute 400 R(1) v3.0
- AhnLab Suhoshin Absolute 400 R(2) v3.0
- AhnLab Suhoshin Absolute 400 R(3) v3.0
- AhnLab Suhoshin Absolute 400 R(4) v3.0
- AhnLab Suhoshin Absolute 100 R(0) v3.0
- AhnLab Suhoshin Absolute 100 R(1) v3.0
- AhnLab Suhoshin Absolute 100 R(2) v3.0

[1] Firmware image: AhnLab-UTM-NOS-1.0.6.0-60

1.3 TOE overview

4 This section describes the use and major security characteristics of the TOE. It also identifies the hardware, software and firmware that are not TOE but required by the TOE, as well as the type of TOE.

5 The TOE is a UTM (Unified Threat Management) system that performs network security features. The firewall and IPS in the TOE detects and blocks harmful contents, including viruses and spam, in various levels through intrusion prevention technology. It also prevents DDoS attacks. These features are provided through its exclusive hardware device.

- The TOE provides firewall and IPS features.
- The TOE provides traffic control and system quarantine features.
- The TOE not only provides each security feature independently, but also integratedly.
- The TOE provides continuous and immediate intrusion detection rules update to re-inforce content security.
- The TOE provides convenient setting and management of the exclusive device with various security features, as well as immediate detection and protection through various statistics and monitoring.
- The TOE provides virus protection through interoperation with the anti-virus engine of TOE operating environment, to manage complex and diverse security threats.

1.3.1 Use and Security Characteristics of TOE

6 The TOE is a UTM system that performs network security features, such as firewall, intrusion prevention, anti-spam, traffic control and system quarantine. It also blocks viruses by interoperating with the anti-virus engine of TOE operating environment.

7 The TOE 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 the information transmitted between the internal and external network.

8 The TOE could be in the form of network host (dual-homed), bastion host, screened-subnet or screen host, and provides various installation and management methods to protect the information of an organization.

- The TOE is installed in-line, so it performs access control, information flow control, data protection, security auditing and secutiy management features, such as user identification and authentication, firewall, intrusion prevention, anti-spam, traffic control and system quarantine, according to the defined security policies.
- The TOE provides security audit data management feature through the TOE-exclusive

security audit data management program (MS-Windows application), as when as the security management interface of the TOE-exclusive device, and it also provides basic security audit data management feature through the security management interface of the TOE (exclusive device).

9 The TOEs can run as part of a cluster to provide high availability of services. This enables the authorized administrator to manage multiple TOEs. When a problem occurs in a TOE, network services are provided through another TOE.

Firewall

10 The TOE blocks unauthorized access by controlling request for services on the network. In general, firewalls fall into three categories- packet filtering, application level gateway and comprehensive firewall- according to the network level applied to the firewall. The TOE falls under comprehensive firewall. It can be used as network host (dual-home), bastion host, screened-subnet and screen-host gateway firewall.

- Packet Filter
- Application Filter
- Network Address Translation

IPS

11 The TOE inspects and controls network traffic according to the TOE security policies to block harmful Internet traffic from external network to internal network.

12 The TOE detects and blocks harmful traffic from the Internet network to the internal network to protect information and resources in the internal network. In other words, proactively blocks hacking that exploits system and service vulnerabilities, attacks via email, and virus and worm attacks.

13 The TOE detects system vulnerabilities by renewing information on vulnerabilities on the database to prevent exploitation of vulnerabilities. With this, it promptly responds to new virus, worm or variant attacks.

- Intrusion Prevention

Contents Filter

14 The TOE protects the network through malicious code detection and prevention.

- Anti-Virus, Anti-Spam

Traffic Control

15 The TOE provides auto-throttling feature, which is a QoS feature that restricts the entire

traffic and the traffic by IP and port.

Quarantine

16 The TOE provides system quarantine that prevents proliferation of additional malicious ocdes by quarantining IP addresses detected by IPS.

1.3.2 TOE type

17 The TOE is a Unified Threat Management (UTM) system. It provides the following features: Firewall, IPS, Anti-Spam, Traffic Control, and Quarantine. It also interoperates with the anti-virus engine of its operating environment to block viruses, and is classified as follows:

- Unified Security System / Unified Threat Management (UTM) System
- Firewall
- Network Intrusion Prevention System (IPS) / Traffic Control

1.3.3 Non-TOE Hardware/Software/Firmware required by the TOE

18 The TOE runs on AhnLab Network Operating System (hereinafter referred to as 'ANOS') on its exclusive hardware. The hardware, firmware and software not required for evaluation are identified as follows:

1.3.3.1 Non-TOE Hardware

19 The hardware not required for evaluation are as follows:

- TOE exclusive hardware platform
- Administrator system (GUI/CLI)
- Audit data management system
- Update server and TOE-interoperable server (system)
- System on which the TOE user authentication program

TOE exclusive hardware platform

20 The TOE runs on an exclusive hardware platform. The hardware platform platform it self is excluded from evaluation.

21 In general, a product with TOE is identified according to the exclusive hardware platform. The detailed specification of the exclusive hardware platform for each product is as Table 1-1 below.

Table **1-1** _____ TOE exclusive hardware platform

Category	AhnLab Suhoshin Absolute 1000 R(0) v3.0	AhnLab Suhoshin Absolute 1000 R(1) v3.0

Category	AhnLab Suhoshin Absolute 1000 R(0) v3.0	AhnLab Suhoshin Absolute 1000 R(1) v3.0
CPU	Intel Pentium IV Xeon 2.8GHz Dual	Intel Pentium IV Xeon 3.4GHz Dual
RAM	2GB	4GB
CF Memory	2GB	2GB
NIC	▪ Gigabit Ethernet x 4 Ports(Filter) ▪ 10/100 Ethernet x 4 Ports	[Basic] ▪ Gigabit Ethernet x 4 Ports (Fiber) ▪ Gigabit x 4 Ports (Copper)* ▪ Gigabit Ethernet x 4 Ports (Fiber) (option)** [Selective] ▪ Gigabit Ethernet x 4 Ports (Fiber) ▪ Gigabit Ethernet x 4 Ports (Fiber)* ▪ Gigabit Ethernet x 4 Ports (Fiber) (option)** ※ Reference (*) Removable hardware module type selected on request by customer. (**) Removable hardware module type selected on request by customer.
Management Port	RS-232 x 1 Port	RJ45 x 1 Port
USB Port	-	1 Port* ※ Reference (*) Disable(N/A)
Chassis design	19"Rack-Mount(2U)	19"Rack-Mount(2U)
Status Display	4-line LCD panel	4-line LCD panel
Size	440 x 370 x 87 mm (W x D x H)	426 x 550 x 88.8 mm (W * D * H)
Power	Dual 100-240 VAC, 460W	Dual 100-240 VAC, 460W
Operating Environment	Temperature: 0 ~ 40 ˚C Storage: -20 ~ 70 ˚C Relative humidity: 10 ~ 90 % non-condensing	Temperature: 0 ~ 40 ˚C Storage: -20 ~ 70 ˚C Relative humidity: 5 ~ 95 % non-condensing

Category	AhnLab Suhoshin Absolute 400 R(0) v3.0	AhnLab Suhoshin Absolute 400 R(1) v3.0	AhnLab Suhoshin Absolute 400 R(2) v3.0

Category	AhnLab Suhoshin Absolute 400 R(0) v3.0	AhnLab Suhoshin Absolute 400 R(1) v3.0	AhnLab Suhoshin Absolute 400 R(2) v3.0
CPU	Intel Pentium IV Xeon 2.4GHz	Intel Pentium IV Xeon 2.8GHz	Intel core 2 duo 2.13GHz
RAM	1GB	1GB	2GB
CF Memory	2GB	2GB	2GB
NIC	▪ Gigabit Ethernet x 4ports (Copper)	▪ Gigabit Ethernet x 6 Ports (Copper) ▪ Gigabit Ethernet x 2 Ports (Fiber)(option)	▪ Gigabit Ethernet x 4 Ports ▪ Gigabit Ethernet x 2 Ports (Fiber)(option)
Management Port	RS-232 x 1 Port	RS-232 x 1 Port	RJ45 x 1 Port
USB Port	-	1 Port* ※ Reference (*) Disable(N/A)	2 Ports* ※ Reference (*) Disable(N/A)
Chassis design	19" Rack-Mount(1U)	19" Rack-Mount(1U)	19" Rack-Mount(1U)
Status Display	2-line LCD panel	2-line LCD panel	2-line LCD panel
Size	440 x 370 x 43 mm (W x D x H)	426 x 500 x 44.4 mm (W x D x H)	443 x 406 x 44.5 mm (W x D x H)
Power	Single 100-240 VAC, 350W	Single 100-240 VAC, 300W	Single 100-240 VAC, 220W
Operating Environment	Temperature: 0~40 ˚C Storage: -20~70 ˚C Relative humidity: 10 ~ 90 % non-condensing	Temperature: 0~40 ˚C Storage: -20~70 ˚C Relative humidity: 10 ~ 90 % non-condensing	Temperature: 5~40 ˚C Storage: 0~70 ˚C Relative humidity: 5 ~ 95 % non-condensing

Category	AhnLab Suhoshin Absolute 400 R(3) v3.0	AhnLab Suhoshin Absolute 400 R(4) v3.0
CPU	Intel Pentium IV Xeon 2.4GHz	Intel Pentium IV Xeon 2.8GHz
RAM	2GB	2GB
CF Memory	2GB	2GB
NIC	Gigabit Ethernet x 4 Ports (Copper)	Gigabit Ethernet x 6 Ports (Copper) Gigabit Ethernet x 2 Ports (Fiber) (option)

Category	AhnLab Suhoshin Absolute 400 R(3) v3.0	AhnLab Suhoshin Absolute 400 R(4) v3.0
Management Port	RS-232 x 1 Port	RS-232 x 1 Port
USB Port	-	1 Port* ※ Reference (*) Disable(N/A)
Chassis design	19" Rack-Mount(1U)	19" Rack-Mount(1U)
Status Display	2-line LCD panel	2-line LCD panel
Size	440 x 370 x 43 mm (W x D x H)	426 x 500 x 44.4 mm (W x D x H)
Power	Single 100-240 VAC, 350W	Single 100-240 VAC, 300W
Operating Envi-ronment	Temperature: 0~40 ° C Storage: -20~70 ° C Relative humidity: 10 ~ 90 % non-condensing	Temperature: 0~40 ° C Storage: -20~70 ° C Relative humidity: 10 ~ 90 % non-condensing

Category	AhnLab Suhoshin Absolute 100 R(0) v3.0	AhnLab Suhoshin Absolute 100 R(1) v3.0	AhnLab Suhoshin Absolute 100 R(2) v3.0
CPU	Intel Pentium 4 1.8GHz	Intel Mobile Celeron 1.2GHz	Intel Core Duo 1.8GHz
RAM	1GB	1GB	2GB
CF Memory	2GB	2GB	2GB
NIC	10/100 Ethernet x 4 Ports (Copper)	Gigabit Ethernet x 4 Ports (Copper)	Gigabit Ethernet x 6 Ports (Copper)
Management Port	RS-232 x 1 Port	RS-232 x 1 Port	RS-232 x 1 Port
USB Port	-	2 Ports* ※ Reference (*) Disable(N/A)	2 Ports* ※ Reference (*) Disable(N/A)
Chassis design	19"Rack-Mount(1U)	19"Rack-Mount(1U)	19"Rack-Mount(1U)
Status Display	2-line LCD panel	2-line LCD panel	2-line LCD panel
Size	440 x 370 x 43 mm (W x D x H)	426 x 270 x 44.4 mm (W x D x H)	443 x 381 x 44 mm (W x D x H)
Power	Single 100-240 VAC, 200W	Single 100-240 VAC, 220W	Single 100-240 VAC, 220W
Operating Envi-ronment	Temperature: 0 ~ 40 °C Storage: -20 ~ 70 °C Relative humidity: 10 ~ 90 %	Temperature: 0 ~ 40 °C Storage: -20 ~ 70 °C Relative humidity: 5 ~ 95 %	Temperature: 0 ~ 40 °C Storage: -20 ~ 70 °C Relative humidity: 5 ~ 95 %

Category	AhnLab Suhoshin Absolute 100 R(0) v3.0	AhnLab Suhoshin Absolute 100 R(1) v3.0	AhnLab Suhoshin Absolute 100 R(2) v3.0
	non-condensing	non-condensing	non-condensing

Administrator system (GUI/CLI)

22 An administrator system that supports web browser or SSH client program is needed to use the security management feature of the TOE. The administrator system used for the security management of the TOE is excluded from the evaluation.

23 The recommended specification of the administrator system is as Table 1-2 below. Ingeneral, the TOE data management program is installed and run on the administrator system. In this case, this administrator system must also satisfy the recommended specification of the audit data management system. Refer to Table 1-4.

Table **1-2** _____ Administrator system's recommended specification (※HTTPS, SSH communication)

Category		Recommended Specification
Hardware specification	CPU	Pentium II (or compatible) 300MHz or higher
	RAM	128MB or higher
	HDD	2GB or more
	Network Interface	TCP/IP based network (※ at least 1 NIC)
OS	▪ MS Windows XP Service Pack 2 or higher	
Required Soft-ware	▪ Software that supports SSH1/SSH2 communication protocol (e.g.: Putty v0.58 or higher) ▪ Web browser that supports HTTPS communication protocol (※ 128bit encryption supported, e.g.: Microsoft Internet Explorer 6.0 SP1 or higher)	

24 In addition, the TOE also provides security management feature through serial data communication. When using this feature, the recommended specification is as Table 1-3 below.

Table **1-3** _____ Administrator system's recommended specification (※ Serial data communication)

Category		Recommended Specification
Hardware specification	CPU	Pentium II (or compatible) 300MHz or higher
	RAM	128MB or higher
	HDD	2GB or more
	Serial communi-cation port	RS-232C

OS	▪ MS Windows XP Service Pack 2 or higher
Required Soft–ware	▪ Sofware that supports RS-232C communication protocol (e.g.: Microsoft hyperterminal v5.1 or higher)

Audit data management system

25 The TOE can separately run the audit data management system selectively according to the method of the authorized user (※ the administrator system used in security management is generally used).

26 AhnLab Suhoshin Absolute LogSever (hereinafter referred to as 'AhnLab LogServer' or 'Log Server'), an audit data management program of the TOE is installed on the audit data management system. The hardware itself is excluded from evaluation.

27 The recommneded specification for the audit data management system is as Table 1-4 below.

Table 1-4 Audit data management system's recommended specification

Category		Recommended Specification
Hardware specification	CPU	Pentium IV 2.66GHz or higher
	RAM	2GB or higher
	HDD	100GB or higher (※ RAID recommended)
	Network Interface	TCP/IP based network (※ at least 1 NIC)
OS	MS Windows Server 2003	
Required Soft–ware	MS SQL Server 2005	

Update server and TOE-interoperable server

28 The TOE provides the following features: update and interoperation with other server. Accordingly, the following system is additionally needed in the TOE operating environment according to the security policies defined by the authorized administrator. The hardware (system) on which the update server and TOE-interoperable server run is excluded from evaluation.

- Update Server: AST Server and CDN Server used by Anti-Virus Engine, TOE patch and pattern update
- TOE-Interoperable Server: Syslog Server, SNMP Manager Server, Korea Internet Safety Commission DB Server, NTP Server, RADIUS Server

System on which the TOE user authentication program operates

29 The TOE provides user identification and authentication feature based on ID and

password or OTP according to the policies defined by the authorized administrator. So, the TOE installs AhnLab Suhoshin Absolute Auth (hereinafter referred to as 'AhnLab Auth'), a user authentication program, on the user PC that request network communication by force.

30 The hardware (system) on which AhnLab Auth is installed and run is excluded from evaluation. The recommended specification is as Table 1.–5 below.

Table **1–5** User authentication program operating system's recommended specification

Category		Recommended Specification
Hardware specification	CPU	Pentium II (or compatible) 300MHz or higher
	RAM	128MB or higher
	HDD	2GB or more
	Network Interface	TCP/IP based network (※ at least 1 NIC)
OS	MS Windows 2000 Service Pack 2 or higher	
Required Soft–ware	Microsoft Internet Explorer 6.0 SP1 or higher	

1.3.3.2 Non–TOE Software

31 The TOE allows interoperation with various external systems according to the detailed options of the security policies (features) defined by the authorized administrator. The following software is excluded from evaluation.

- Anti-Virus Engine, Harmful Web Site DB
- AST (AhnLab Service Tower), CDN Server
- Syslog Server, SNMP Manager
- SSL communication, SSH/Serial communication supporting software
- MS SQL Server
- NTP (Network Time Protocol) Server
- RADIUS Server

Anti–Virus Engine

32 The TOE provides anti–viirus feature by interoperating with Anti–Virus Engine (V3 Engine). The anti–virus feature is used selectively according to the options defined by the authorized administrator in the TOE Application Filtering (Proxy). If the anti–virus feature is forced in the TOE, virus scan is requested through the anti–virus engine of the TOE operating environment. The TOE controls requested information flow according to the returned value. The anti–virus engine to scan virus is excluded from evaluation.

Harmful Website DB (Korea Internet Safety Commission)

33 The Harmful Web Site DB of the Korea Internet Safety Commission provides website database. This database is provided to block various harmful sites, including sites containing adult or violent content. The TOE blocks harmful sites through the database provided by the database server of the Korea Internet Safety Commission (downloaded) in the Application Filtering (Proxy). This database is excluded from evaluation.

AST (AhnLab Service Tower)

34 The TOE provides interoperation with AhnLab, Inc.'s AST. It uses AST along with CDN Server for updates. AST is a system that manages and distributes rules provided by ASEC of AhnLab, Inc. It is excluded from evaluation.

CDN Server

35 The TOE provides interoperation with AhnLab, Inc.'s CDN Server. It uses the CDN Server for updates. The CDN Server duplicates the same contents on the entire network, like a cache, and distributes them over the Intranet or Internet. It provides security policy pattern and patch files and content rating DB files for TOE updates. It is excluded from evaluation.

Syslog Server

36 The TOE transmits audit data generated during TOE operation according to the security policies defined by the authorized administrator to the external Syslog Server. The Syslog Server is excluded from evaluation.

SNMP Manager

37 The TOE can transmit SNMP Trap during TOE operation according to the the security policies defined by the authorized administrator. It gathers or changes information through the SNMP Manager. SNMP Manager is excluded from evaluation.

SSL communication supporting web browser

38 The TOE provides security management interface (GUI) through a web browser that supports SSL communication (HTTPS). The web browser must support 128bit encryption or higher (OpenSSL 0.9.8j). The web browser used to access the TOE security management interface (GUI) is excluded from evaluation.

SSH/Serial communication supporting software

39 The TOE provides security management interface (CLI) through SSH/Serial commu-

nication software. The communication software (OpenSSH v5.1p1) used to access the TOE security management interface (CLI) is excluded from evaluation..

MS SQL Server

40 The TOE uses MS SQL Server to save audit data from TOE operation. In general, MS SQL Server is installed and managed on the administrator system, but it gets installed and managed on a separate audit data management system according to the security policies defined by the authorized administrator. The MS SQL Server is excluded from evaluation. For reference, the audit data of the TOE is managed through the AhnLab LogServer.

NTP (Network Time Protocol) Server

41 The TOE uses NTP server selectively according to the time synchronization method specified by the authorized administrator. NTP is a protocol used to synchronize clock times of computers linked through a network. It is excluded from evaluation.

RADIUS Server

42 In general, the TOE provides ID and password based user identification and authentication feature through the authentication daemon of the TOE. Additionally, in the case it is specified by the authorized administrator, in other words, if an administrator authorized in the TOE Application Filtering (Proxy) forces user identification and authentication by interoperating with the external authentication server, RADIUS Server is used selectively. If the authorized administrator forces user identification and authentication through the RADIUS Server, the TOE delivers the ID and password entered by the user to the designated RADIUS Server and requests for authentication. The TOE decides whether to authenticate the user according to the result returned by the RADIUS Server. The RADIUS Server is excluded from evaluation.

1.3.3.3 Non-TOE Firmware

43 ANOS v2.0, the operating system of the TOE is excluded from evaluation. ANOS v2.0 is the abbreviation of 'AhnLab Network Operating System' and is a network security applicance exclusive operating system of AhnLab, Inc. ANOS v2.0 is in the form of firmware in the CF memory on the exclusive hardware platform.

1.4 TOE description

44 The TOE is a Unified Threat Management (UTM) system that performs network security features, such as firewall, intrusion prevention, anti-spam, traffic control and system quarantine. These security features are performed on an exclusive hardware platform (network security appliance). It also blocks viruses by interoperating with the anti-virus engine of TOE operating environment.

45 The TOE can run as part of a cluster to provide high availability of services. This enables the authorized administrator to manage multiple TOEs. When a problem occurs in a TOE, network services are provided through another TOE.

46 The TOE provides web based security management interface (GUI) and SSH/Serial communication based security management interface (CLI) to manage the security features on the exclusive hardware platform. In addition, it provides security auditing data management feature through a TOE exclusive security audit data management program (AhnLab LogServer).

1.4.1 TOE operating environment

47 The TOE 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. It can run as part of a cluster to provide high availability of services according to the management method of the authorized administrator. [Fig. 1-1], [Fig. 1-2]

48 The TOE performs network security features, such as firewall, intrusion prevention, anti-spam, traffic control and system quarantine, and also user identification and authentication, access and information flow control, data protection, security auditing and security management.

- The TOE audits and controls network traffic according to the TOE security policies to block harmful Internet traffic that enters from an external network to an internal network.
- The TOE protects information and resources of an internal network by proactively defending and blocking harmful traffic from the Internet network to the internal network. In other words, it proactively blocks hacking caused by exploitation of computer system and service vulnerabilities, attacks via email, and virus and worm attacks.
- The TOE performs system quarantine that prevents proliferation of additional malicious codes by quarantining the IP addresses that need to be quarantined based on IPS detection and worm/virus infected host.

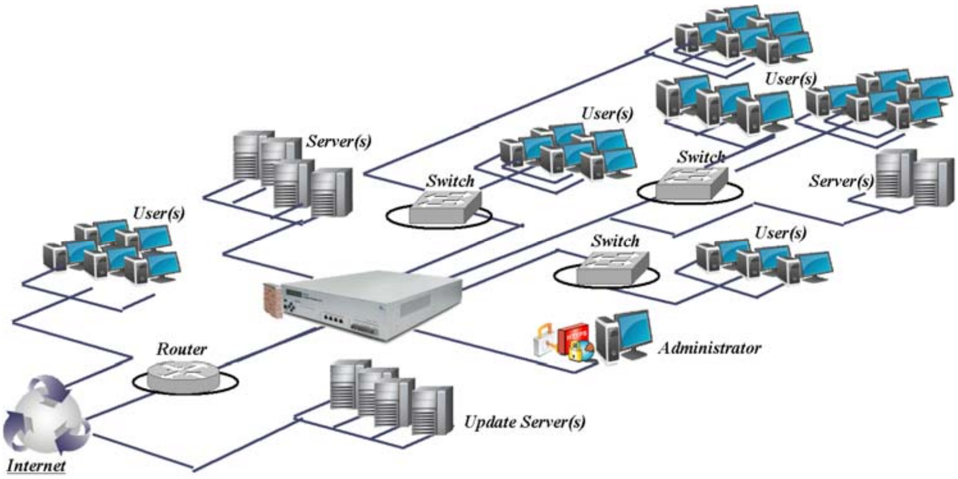
49 The TOE can be arranged and managed as the following [Fig. 1-1] and [Fig. 1-2]. The

authorized administrator can use TOE security management features through the web based security management interface (HTTPS) of the TOE operating environment. In addition, the authorized administrator can use CLI (Command Line Interface) through the SSH/Serial communication program.

In-line Mode

50 The TOE 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. In other words, security policies defined by the authorized administrator are applied to all network traffic sent/received through the TOE. [Fig. 1-1]

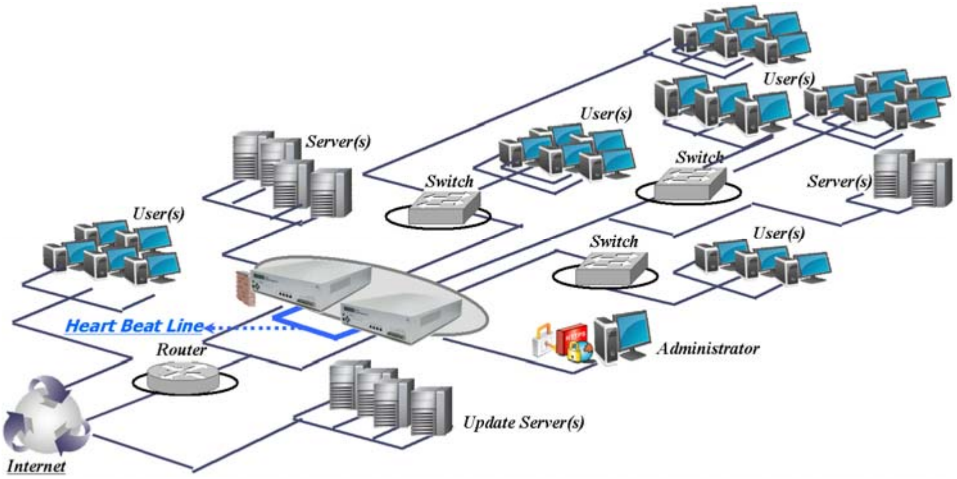
Fig. 1-1 _____ Example of TOE operating environment (In-line Mode)



HA (High Availability) Mode

51 HA Mode is almost similar to the In-line Mode above in [Fig. 1-1]. The only difference is there being multiple TOEs in a network, and when there is a problem in a TOE, the availability of the network is assured. The security policies defined by the authorized administrator are also applied to all network traffic sent/received through the TOE. [Fig. 1-2]

Fig. 1-2 ______ Example of TOE operating environment (HA Mode)



1.4.2 Physical Boundary

52 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 and AhnLab Suhoshin Absolute Log Server (hereinafter referred to as AhnLab LogServer or LogServer) which is a TOE audit data management software in a CD.

53 Also, User Guide and Preparation Guide are also included in the form of e–document (CD) to end–users (customers) for safe operation of the TOE.

[Ref.] The TOE is physically divided into an exclusive hardware platform (network security appliance) and administrator system. The hardware itself is exluded from the physical boundary. (※ Refer to 1.3.3 Non-TOE Hardware/Software/Firmware required by the TOE)

- Exclusive Hardware Platform
  - The UTM daemon package includes a software module that performs features such as packet filtering, application filtering, NAT, intrusion prevention, malicious Email filtering and virus detection through interoperation with the anti–virus engine of the TOE operating environment.
- Administrator System
  - The administrator system is used to manage the security features of the TOE that is managed on the exclusive hardware platform. In general, AhnLab LogServer, which is an audit data management system, is installed together on the administrator system, but it can be installed and managed on a separate exclusive audit management system.

1.4.2.1 UTM Daemon Package and AhnLab LogServer

UTM Daemon Package

54 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. When the authorized administrator turns on the hardware device, the UTM daemon package checks the integrity of the operating environment such as the hardware according to the booting procedure of the TOE operating environment, and if the the result is normal, it gets loaded onto the RAM by the operating system. After that, if the TOE initialization process ends normally, the security features provided by the TOE are performed.

55 The UTM daemon package that is saved in the CF memory on the exclusive hardware platform in the form of a firmware is distributed to the end–users (customers) along with

ANOS, and is identified as below.

- pkg 1.0.6.0-60

[Ref.] The UTM daemon package is included in the firmware image and distributed with ANOS. Accordingly, the version of the package is identified through the ANOS version. The 'pkg-1.0.6.0-60' above signifies the UTM daemon package saved in the firmware image, 'AhnLab-UTM-NOS-1.0.6.0-60'.

AhnLab LogServer

56 AhnLab LogServer is a TOE audit data management software. AhnLab LogServer has three installation files. They are provided to end-users (customers) in a CD and the three files are identified as follows.

- AhnLab Suhoshin Absolute Log Server 1.0.1.3(build21)

[Ref.] AhnLab LogServer has three installation files. The 'AhnLab Suhoshin Absolute Log Server 1.0.1.3(build21)' above consists of Log Server 1.0.1.3(build21), Log Viewer 1.0.1.3(build21) and Log Reporter 1.0.1.3(build21).

57 Also, AhnLab Auth software that is used when the authorized administrator forces authentication policy as a specific policy of the security policies of application filtering is included. It is distributed in the form of firmware image along with ANOS and it is not separatrely identified.

[Ref.] In general, when the authorized administrator forces authentication policy as a specific policy of the security policies of application filtering, AhnLab Auth is installed by making the end-user (customer) download it from the web page provided by the TOE.

1.4.2.2 User Guide

58 For safe management of the TOE, a guidebook and e-document (CD) is provided to the end-user (customer). The user guide distributed to the end-user (customer) is also included in the physical boundary of the TOE and is identified as follows.

- AhnLab Suhoshin Absolute Help: Absolute-OPE_UTM-001-01
- AhnLab Suhoshin Absolute Log Server Help: Absolute-OPE_LOGSERVER-001-01
- User Guide: Absolute-OPE_USER-001-01
- AhnLab Suhoshin Absolute 400 Installation Guide: Absolute-PRE_UTM-001-01
- AhnLab Suhoshin Absolute Log Server Installation Guide : Absolute-PRE_LOGSERVER-001-01

1.4.3 Logical Boundary

59 The TOE is a Unified Threat Management (UTM) system that provides firewall, IPS, anti–spam, traffic control and quarantine features. The TOE 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. It performs access control, information flow control, data protection, security auditing and secutiy management features, such as user identification and authentication, firewall and intrusion prevention, anti–spam, traffic control and system quarantine, according to the defined security policies.These security features are included in the logical boundary of the TOE.

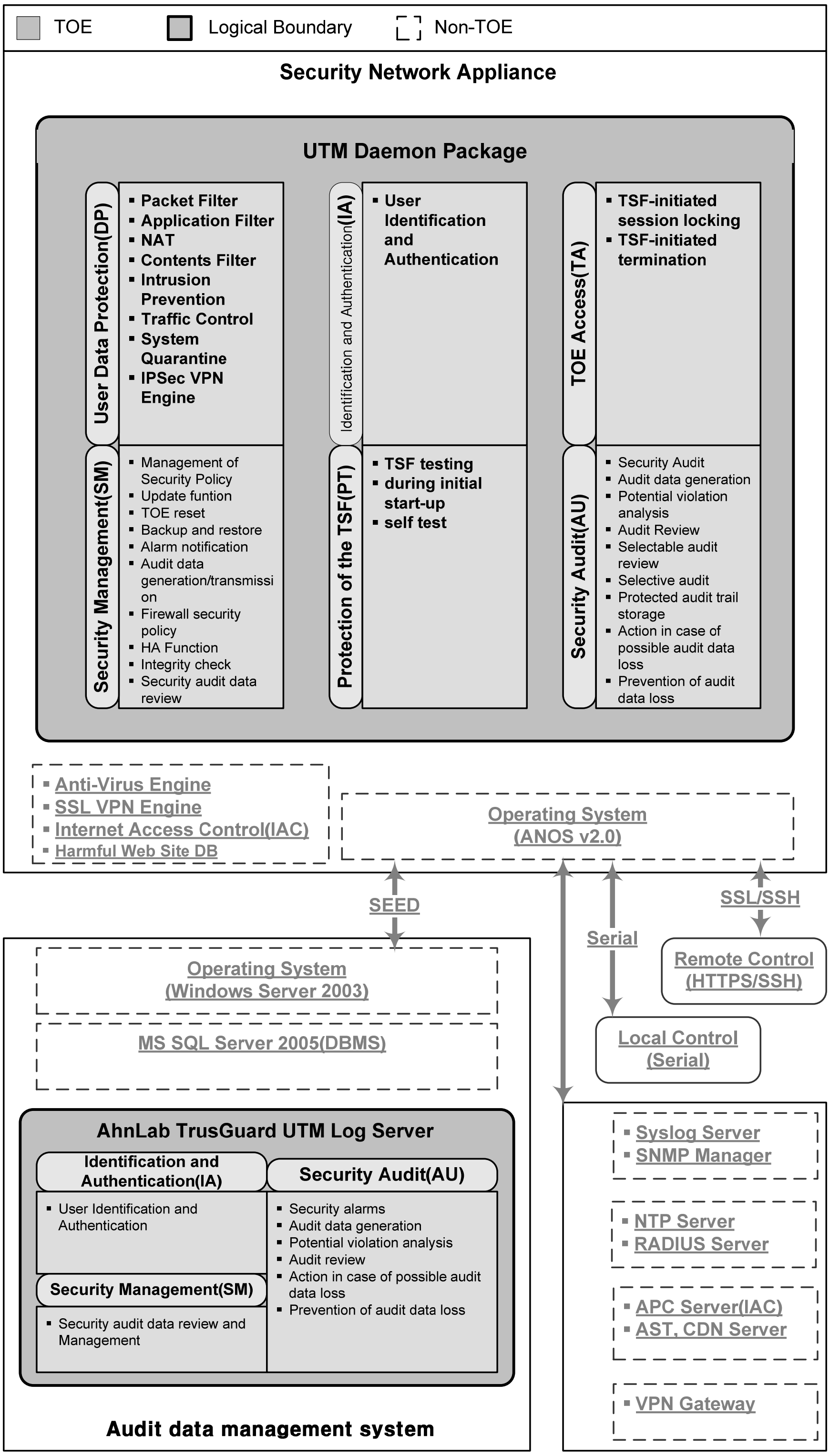
60 The TOE provides security audit review and management through AhnLab LogServer, which is a physically separated (run remotely) TOE and not an exclusive device. Accordingly, the security features provided by AhnLab LogServer are also included in the logical boundary of the TOE. For reference, the TOE provides basic security audit data management feature through the security management interface of the TOE (exclusive device).

61 The logical boundary of the TOE is summarized as follows.

- Identification and authentication
- Access control and information flow control
- Security Management
- Security Audit
- TSF Protection
- TOE

62 The logical boundary of the TOE is as [Fig. 1-3] below.

Fig. 1-3 ______ Logical boundary of TOE


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 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
Security Management(SM)
▪ Security audit data review and Management
Audit data management system
▪ Syslog Server
▪ SNMP Manager
▪ NTP Server
▪ RADIUS Server
▪ APC Server(IAC)
▪ AST, CDN Server
▪ VPN Gateway

[Ref.] As it can be observed in [Fig. 1-3], it is not included in the logical boundary of the TOE, but SSL VPN Engine and IPSec VPN Engine are loaded on the TOE operating environment. In addition, the TOE interoperates with the anti–virus engine of the TOE operating environment to block viruses. Likewise, the anti–virus engine itself is also not included in the logical boundary of the TOE.

1.4.3.1 Identification and authentication

63 The TOE identifies all users that attempts to access itself. All users that attempts to access before being identified cannot use any of the TOE features. The TOE provides the following identification and authentication features.

- IP address based identification
- ID and password based user identification and authentication
- One–time Password based user identification and authentication

64 The TOE may lock a user account if the specified number of failed login authentication is exceeded (default: 3 times) to protect the TOE from login attempts by malicious users. The authorized administrator can unlock the locked account through the TOE security management interface.

1.4.3.2 Access control and information flow control

65 The TOE provides Packet Filter (Dynamic & Stateful Packet Filtering), Application Filter (Proxy), Network Address Translation (NAT), Anti–Virus, Intrusion Prevention, andQuarantine to control access and information flow.

1.4.3.2.1 Firewall

66 The TOE blocks unauthorized access by controlling thes request for service on the network to protect. It can be divided into packet–filtering, application level gateway and comprehensive firewall according to the network level. In addition, these can be used as network host, bastion host, screened–subnet and screen–host gateway firewall, according to the TOE and management method.

Packet Filter (Dynamic & Stateful Packet Filtering)

67 When packets enter the TCP/IP kernel through the Network Interface Card (NIC), the TOE determines the security policies of the packets based on the access control list. The source IP address and port, and destination IP address and port place an important role in determining the security policy. If the security policies are allowed, the TOE allows the packets to pass, and if not allowed, they are dropped.

68 If the security policies of packets are the security level, the TOE compares the security level of the source network and destination network, and if the security policy of the source network is the same as that of the destination network, or higher, the packets are allowed to pass. If the security level of the source network is lower than that of the destination network, the packets are dropped. Also, packets are delivered to the NAT module if there exists NAT rules for packet control rules.

69 If the security policy of a packet is redirection (Redirection, ※ Packets to which the Application Filter must be applied), the packet gets delivered to the application program. The TOE processes the packets delivered to the application program level through the application filter (proxy). The proxy determines the security policy by referring to the shared memory according to the source IP address and port, and destination IP address and port. If the security policy is allowed, the packets are allowed to passed, and if not allowed, they are dropped. If the security policy has to be authenticated, the packets are allowed only if the user is authenticated. The features provided by the application proxy are described in detail below.

Application Filter (Proxy)

70 If the security policy of a packet is redirection (Redirection, ※ Packets to which the Application Filter must be applied), the TOE processes the packets through the application filter. The authorized administrator manages the application filtering security policy list by service type. If there is a security policy list that matches the security characteristics of the packet deivered from the packet filter, the TOE either allows of disallows passing of packets based on the security policy. The types of application filtering and additional features provided by the TOE are as follows.

- General TCP Proxy: Performs delivery host, session timeout and authentication (ID and password, or one-time password) features according to the administrator defined security policies.
- FTP Proxy: Performs delivery host, session timeout, anti-virus (blocking virus by interoperating with the anti-virus engine of the TOE operating environment), command block and authentication (ID and password, or one-time password) features according to the administrator defined security policies.
- SMTP Proxy: Performs delivery host, session timeout, relay block, anti-virus (blocking virus by interoperating with the anti-virus engine of the TOE operating environment), anti-spam and command block features according to the administrator defined security policies.
- HTTP Proxy: Performs delivery host, session timeout, anti-virus (blocking virus by interoperating with the anti-virus engine of the TOE operating environment), and authentication (ID and password, or one-time password) features according to the

administrator defined security policies.

- POP3 Proxy: Performs delivery host, session timeout, anti-virus (blocking virus by interoperating with the anti-virus engine of the TOE operating environment), and anti-spam features according to the administrator defined security policies.
- Oracle Proxy: Performs delivery host and session timeout features according to the administrator defined security policies.
- UDP Proxy: Performs delivery host and session timeout features according to the administrator defined security policies.
- DNS Proxy: Performs delivery host, session timeout, DNS response test and split DNS features according to the administrator defined security policies.
- URL Filtering: The HTTP proxy allows/drops services requested by the user selectively based on the standard of harmful URL (harmful URL DB provided by Korea Internet Safety Commission) according to the administrator defined security policies.

Network Address Translation (NAT)

71 The TOE provides masquerade features that apply SNAT on dynamic IP addresses, such as Source NAT (SNAT) that changes the source address, Destination NAT (DNAT) that changes the destination address, Redirection that changes the destination address to the local host (TOE itself) and PPP/DHCP.

72 The NAT feature of TOE changes the private IP address to public IP address- the TOE allots a public IP address for external user from private IP address to access from an external public network, or specifies a public IP address for the internal server. Accordingly, when there is not enough IP addresses of the internal network, the IP addresses can be added by using the private IP address through the TOE. Also, as the internal IP address is not disclosed, the network will be safe from external attacks.

1.4.3.2.2 Network Intrusion Prevention System

73 The TOE detects and blocks harmful traffic from the Internet network to the internal network to protect the information and resouces of the internal network. In other words, the TOE proactively blocks malicious hacking that exploits the computer system and service vulnerabilities, attacks via Email, and virus and worm attacks.

74 In addition, the TOE renews vulnerability information on the vulnerability database to detect vulnerabilities in the computer system and block attacks that exploits the vulnerabilities. With this, it promptly responds to new virus, worm or variant attacks.

75 The TOE prevents malicious codes to protect the network.

Intrusion Prevention

76 The TOE provides signature based intrusion prevention feature which blocks known

harmful traffic through pattern (rule) matching. Also, the authorized administrator can also add new rules, apart from the rules provided by AhnLab as default.

77 The TOE provides algorithm based intrusion prevention features that analyze the behavorial patterns or statistical values on abnormal behaviors and undetectable attackst through simple rule and pattern matching.

- DoS Protection: Blocks action that can cause a problem in the network service provided by TOE caused bya malicious user or worm requesting excessive number of network services.
- DDoS Protection: Detects and blocks DDoS attacks on the network or specific service to provide normal service.
- Anti-Scanning: Detects and blocks scanning attacks from worm or hackers by analyzing the traffic of specific IPs.
- Anomaly Detection: Detects and blocks abnormal traffic that cannot be detected by pattern matching, DoS/DDoS protection or anti-scanning. (E.g.: attempt of access from abnormal IP address (reserved IP address, multicast IP address)).
- Behavior based user defined rules: The TOE provides exclusive macro rule for the authorized user to add behavior based detection as well as simple signature based user defined rules. It counters new attacks that can only be detected through statistical processing without changing the process by adding macro rules.

[Ref.] 'Anomaly Detetion' means detection of attacks such as packet storming, tcp flag spoofing and tcp redirect.

- packet storming: Network error caused by infinite loop, such as wrong network connection caused by mistake of user or same packets repeated by hacker in short period of time
- tcp flag spoofing: Fabricated paths of packets
- tcp redirect: Changed packet transmission paths

1.4.3.2.3 Contents Filter

78 The TOE safely protects the network by detecting and preventing malicious codes by interoperating with the anti-virus engine (V3 Engine) of the TOE operating environment. But, the anti-virus engine is excluded from evaluation.

Anti-Virus

79 The TOE provides anti-virus features by interoperating with the application filter (proxy). The types of proxy include SMTP Proxy, HTTP Proxy, POP3 Proxy and FTP Proxy.

80 The TOE uses AhnLab anti-virus engine as the virus detection engine, and supports engine updates. The virus prevention features provided are as follows.

- Email scan: Message and attached file sent via email
- Web scan: Files sent via web sites
- FTP scan: Files sent via FTP

Anti-Spam

81 The TOE blocks spam mail (SMTP/POP3) by means of filtering the subject and message.

1.4.3.2.4 Traffic Control

82 The TOE provides auto-throttling feature, which is a QoW feature that restricts entire traffic or traffic by IP and port. Accordingly, it can secure or restrict the bandwidth specified by each user of security policy.

1.4.3.2.5 Quarantine

83 The TOE provides system quarantine that prevents proliferation of additional malicious ocdes by quarantining IP addresses detected by IPS.

1.4.3.3 Security Management

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

85 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 environment settings file get loaded on the shared memory when running the TOE and the changes settings are saved.

86 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. Also, it also provides CLI (Command Line Interface) used to fix the TOE error. The security management features provided by the TOE are as follows.

- Restart/Stop TOE , System: TOE operating environment Information Management, Network Environment Management, Security Policy Management, Update, Integrity Check

87 Also, the security audit data is managed and checked through the AhnLab LogServer, a physically separated TOE. The security management features provided through the

AhnLab LogServer is as follows.

- TOE (AhnLab LogServer) Start/Stop, Configuration (Security Audit), Backup Settings (Security Audit Data), Backup and Restore, Trend Analysis, Log Search

Restart/Stop TOE

88 The authorized administrator can restart or stop the TOE. When the TOE gets restarted or stopped, all the features will restart or stop.

System: TOE operating environment Information Management

89 When the authorized administrator logs in to the security management interface through a web browser (HTTPS), the TOE provides TOE resource status, settings information, security policy status, management information and event log. Also, it also provides administrator, update, log, SNMP, TOE time, session and alert mail settings, backup and restore, and integrity check features to the authorized administrator.

Network Environment Management

90 The TOE provides network port, routing, network connection, DHCP and HA setting features to the authorized administrator.

Security Policy Management

91 The TOE provides security policy management features to the authorized administrator. The features include security policy target management, firewall security policy management, network intrusion prevention policy management and contents filter security policy management.

Update

92 The TOE provides features to update signature, patch and content rating DB (harmful information DB)[1], regularly or manually. Through this, the latest signatures can be used to safely protect the network environment.

Integrity Check

93 The TOE provides integrity check feature to maintain accuracy, stability and consistency of file system information. The authorized administrator can use the integrity check feature to check identification, generate checksum database on access control files and audit record files, and compare the status with the current database. Data that includes TOE configuration files, identification, authentication, access control rules and

[1] Korea Internet Safety Commission

security label information is protected from all unpermitted changes by applying integrity (HAS-160).

TOE (AhnLab LogServer) Start/Stop

94 The authorized administrator can restart or stop the TOE (AhnLab LogServer). When the TOE (AhnLab LogServer) gets restarted or stopped, all the features will restart or stop.

Configuration (Security Audit)

95 The TOE (AhnLab LogServer) provides security management features for the authorized administrator to configure the device, alert level and account settings to manage the TOE.

Backup Settings (Security Audit Data), Backup and Restore

96 The TOE provides management features for the authorized administrator to directly or regularly back up security audit data.

Trend Analysis

97 The TOE provides features for the authorized administrator to perform analysis for system and network status, attacker, attack target, attack type, risk and country of attack by each TOE (exclusive device) and date through the TOE (AhnLab LogServer).

Log Search

98 The TOE provides features for the authorized administrator to monitor audit data-operation logs, firewall logs, IPS logs, quarantine logs, contents filter logs, website filtering logs, anti-virus logs and anti-spam logs- in real time or manage (search/delete) existing audit data through the TOE (AhnLab LogServer).

1.4.3.4 Security Audit

99 The TOE uses the system time maintained by the TOE operating environment to secure successive generation of audit data when the data is generated. The TOE operating environmnet regularly compares the value saved in the Real-time Clock (RTC) where the TOE is managed to provide time stamps. Also, it automatically synchronizes the time with the NTP Server in the TOE operating environment according to the security policy defined by the authorized administrator.

100 The TOE saves all logs (operationg log, packet filtering log, IPS log and contents filtering log) onto storage (exlcusive device) for saving audit data. At the same time, they get sent to AhnLab LogSever, which is a physically separated TOE (but remotely connected

through a network) specified by the authorized administrator. If the authorized administrator forces security transmission, the TSF data gets encrypted with a SEED and sent to prevent exposure of TSF data between the TOE and Log Server. AhnLab LogServer saves the received logs in the DB file system (e.g.: MS-SQL) and provides search, statistics and management features.

Security Alert

101 The TOE generates audit data when security violation occurs when a security feature is running and then alerts through the real time event window of the security management interface and records it. Also, the TOE transmits audit data to remote AhnLab LogServer specified by the authorized administrator. The authorized administrator can check security violations through the real time event window of the Log Server. Also, if the authorized administrator has specified security alert when the CPU, memory and HDD of the TOE operating environment has exceeded the limit, the authorized administrator will be alerted according to the specified rule.

Audit Data Generation and Violation Analysis

102 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 the generate the audit data selectively according to the event type and also by individual audit target event (security violation). The TOE generates audit data according to value specified by the authorized administrator, in other words whether audit data has been specified for the event type and individual event.

103 If a potential security violation is detected, the TOE reports it to the authorized administrator in real time and responds according to the specified method according to the type of violation.

Audit Review

104 The TOE provides feature to review audit records by type for all audit data. It manages audit data through the TOE operating environment file system (DB). When requested by the authorized administrator, the TOE reads the file from the TOE operating environment and provides it in a form that can be interpreted by the administrator. An authorized adminsitrator can review the audit data through the AhnLab LogServer.

Audit Evidence Protection

105 The TOE only allows the authorized administrator to access the audit record of audit

evidence (DB) saved on the TOE operating environment. Accordingly, it can protect audit record from unauthorized deletion or modification. The TOE provides audit record to the authorized administrator when:

- identification and authentication of the security management interface (web UI) has succeeded, and
- authentication of AhnLab LogServer has succeeded after identification and authentication of the audit data management system OS (Windows Server 2003).

Audit Data Loss Response and Prevention

106 The TOE checks the space available in the audit evidence storage in intervals (every 1 minute) to protect lodd of audit data. If the space available falls to less to 10%, the authorized administrator will be alerted through email or popup window. It can be used as normal after it has been restored by the administrator.

107 The authorized administrator can specify the limit of the audit evidence storage space in the form of [total capacity of audit evidence storage space – available space specified by the authorized administrator (%)] (default: 10%). If the specified limit is reached, the authorized administrator will be alerted through email or popup window.

1.4.3.5 TSF Protection

Maintaining security when error occurs

108 The TOE maintains and manages list for important daemon and operation status (e.g. start, stop, restart, reload) which need to be restarted when error occurs. It regulary checks the status of the daemon to manage to secure normal security operation by restarting the dameon when an abnormally terminated daemon is detected.

Self test

109 TheTOE 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. The administrator can ignore or initialize it.

1.4.3.6 TOE Access

Administrator session lock and user session termination

110 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.

111 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 (30 minutes) 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.

1.5 Typographic Convention

112 This Security Target uses English words for clearer meaning of abbreviations and terms. Notations, forms, and typographic conventions conform to the Common Criteria for information protection systems and protection profiles for government agencies

113 The Common Criteria allows selection, iteration, refinement and assignment operations to apply to functional requirements.

114 The operations used in this document are as follows.

Iteration

115 Iteration is used when the same component is used repeatedly for multiple operations. The esult of the Iteration operation is indicated by the iteration number within parentheses, (repeat number), following the component identifier.

Selection

116 Selection is used to select one or more options provided by the Common Criteria for the information protection system. The result of the *Selection* operation is indicated in *underlined italicized characters*.

Refinement

117 Refinement is used to further restrict any requirement by adding details to the requirement. The result of the **Refinement** operation is indicated in **bold characters**.

Assignment

118 Assignment is used to allocate a specific value to an unspecified parameter. (Example: Password length). The result of the Assignment operation is indicated by square brackets, [Assignment_Value].

Security Target Author

119 The security target author makes the final decisions. The author's operation is indicated by braces {Decision made by Security Target}.

120 Application notes clarify the meaning of a requirement, provide information on options upon implementation, and define the "suitable/non-suitable" standard for the re-quirement. It may be provided with the corresponding requirement, if necessary. In order to further clarify the meaning of a requirement, the requirement was indicated with'Ref.' when necessary.

1.6 Terms and Definitions

121 Terms and definitions in this Security Target and overlapping those in the Common Criteria for information protection systems shall follow the Common Criteria. They will not be additionally escribed in this document.

Virus

A virus is a computer program that can copy itself. It infects computer programs by copying itself or its variant.

Spam Mail

Spam mail is junk mail sent to numerous recipients by email or PC communication users. It is also known as junk email, with the aspect that email is unsolicited and sent. Spam mail wastes the time and money of people.

Secure Shell

Secure Shell is a protocol that allows data exchange or remote access over a network. There are three types of protocol- transport layer protocol, user authentication protocol and connection protocol. The transport layer protocol is on the upper layer of TCP/IP, and involves ecryption data transmission or server authentication. Various cryptographic procedures can be used and the exchange of password key or negotiation procedure is set. The user authentication protocol is on the upper layer on the transport layer protocol.

External Entity

An external entity is an entity (person or IT) outside the TOE that interacts (or may interact) with the TOE. If the external entity is IT, it will be indicated as 'IT entity'.

Authorized Administrator

The authorized administrator is a user authorized to operate and manage the TOE safely according to the SFR (Security Functional Requirement). In this document, it represents the authorized user who operates and manages the TOE (exclusive device). In this case, the TOE identifies the authorized administrator as a super administrator or just an administrator according to the 'permission'. A super administrator is the authorized administrator with all permissions (read/write) and can use all security management features provided by the TOE. An administrator is the authorized administrator with only read-only permission to check policies on TOE management.

Authorized Log Administrator

An authorized log administrator is a user authorized to operate and maange the TOE (AhnLab Server) physically separated and implemented according to the SFR on the security audit data of the TOE. An authorized log administrators are divided into super log administrator and just log administrator. A super log administrator can use all the security management features provided by the TOE (AhnLab LogServer), whereas a log administrator can only check the aduit data.

Authorized User

If the authorized administrator forces authentication for [Application Filter] information flow control policy, he or she can change his or her own password, as a user who has been authenticated based on ID and password.

IT Entity

An IT entity is a user who sends/receives information through the TOE. The TOE ifnormoation flow control security policy is applied. It is an entity (external entity) outside the TOE that interacts (or may interact) with the TOE.

Harmful Traffic

Harmful traffic is disallowed access of service, all network packets with abnormal packet structure, packets with computer virus and worm, and packets that performs service denial attack that damages the availability of the internal computer resources.

Firewall System

A firewall is an access control system installed on the gateway to prevent a network connected through an IP from illegal intrusion. As two-way connection is possible when one-way connection has been made on the Internet, the network connected through an IP can be accessed from outside the network. Security can be maintained by restricting access, but there are also methods such as blocking IP packet transmission between networks or allowing transmission of packets by/from specific application.

Ttraffic Control

It controls information flow or signals of the communication system.

Administration System

It is a system where the authorized administrator sets, monitors and controls the TOE from the host and on which the AhnLab LogServer and web browser to remotely operate all administrator features are installed.

AhnLab LogServer

It is an abbreviated form of AhnLab Suhoshin Absolute LogServer. It is an audit data management software of the TOE.

ASEC

It is a security response center of AhnLab where malicious codes such as the virus are analyzed and responded to.

AST (AhnLab Service Tower)

AST is a server that is used for pattern and patch updates. It is a system that manages and distributes the rules provided by ASEC.

Browser

As a client application program, it is a tool to search www information. It searches, saves and transmits data between the Internet user and www server. The type of browsers inlcude Netscape, Mosaic and Internet Explorer.

CDN Server

CDN Server is a system that copies the same contents from the entire network and distributes them on a large intranet or the Internet, as a type of cache. AhnLab's CDN server provides pattern and patch files for TOE updates.

Content

It is generally used to imply digital information provided through a wired/wireless communication network.

Database

It is a group of related data saved on a medium which a computer can access to provide application programs or documents to an unspecific organization or for a specific organization to jointly use application programs or documents.

DNS (Domain Name System)

DNS is a server that finds IP addresses corresponding to the host name. The form of host name used on the Internet at present is called domain name.

DoS (Denial of Service)

It obstructs a user from using data or resources of information system within a period of waiting time. As an attacking host, it causes large amount of network traffic for hacking attack that temporarily or completely stops the network service of the host.

Dynamic PacketFilter

It monitors the status of active connection, and decides whether to allow network packets to pass the firewall. It records session information such as IP address and port for stricter security status than passive packet filter.

HA (High Availability)

HA is a system or component that can be continuously operated for a long period of time. Availability is measured relatively and often described as "100% available" or "never breaks down". There is also 99.999%, called "five 9s", which is hard to accomplish but often used in availability standard for systems and products.

(IPS) Intrusion Prevention System

IPS is a network security technology used to immediately respond to potential threats that have been recognized. Like IDS, it monitors network traffic. If an attacker acquires access permission, the system could be used maliciously, so IPS must be able to immediately act based on the rules set by the network administrator. If IPS checks a packet and decides it is harmful, all traffic will not be allowed to the IP address or port, but legal traffic will be allowed without any obstruction.

IP Scan

It scans unspecific IPaddresses for specific service port.

NAT (Network Address Translation)

In a computer network, Network Address Translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for remapping a given address space into another. NAT enables computers on small to medium sized organizations with private networks to access resources on the Internet or a public network. The computers on a private network are configured with reusable private Internet Protocol version 4 (IPv4) addresses; the computers on a public network are configured with globally unique IPv4 (or, rarely at present, Internet Protocol version 6 [IPv6]) addresses).

NTP (Network Time Protocol)

NTP is a protocol used to synchronize clocks of computers over a network. It was originally developed by Dave Mills of the University of Delaware, and now is the standard Internet protocol. It synchronizes computer clocks to UTC (Coordinated Universal Time) and maintains time within 1/1000 seconds.

Port Scan

It scans a specific IP address for its service port.

Quarantine

It quarantines the system to restrict the network service use of host that causes harmful traffic.

Registered Jack (RJ-11, RJ-14, RJ-45, and others)

It is usually called RJ or at times, RJ-XX. They are a series of telephone connection interfaces that are registered with the FCC (Federal Communications Commission). They derive from interfaces that were part of the Universal Service Order Codes (USOC) and were adopted as part of FCC regulations (Part 68, Subpart F. Section 68.502). The term ‘jack’ means both receptacle and plug, or just the receptacle.

The RJ-45 is a single-line jack for digital transmission. The interface has eight pins. Untwisted wire can be used to connect a modem, printer, or a data PBX at a data rate up to 19.2 Kbps. For faster transmissions like Ethernet 10BASET network, a twisted wire is needed. (Untwisted is usually a flat like common household phone extension wire. Twisted is round.) There are two types of RJ-45: keyed and unkeyed. Keyed has a small bump on its end and the female complements it. Both jack and plug must match.

RSA (Rivest, Shamir, Adleman, Cryptosystem)

RSA is the intitial of R. Rivest (R), A. Shamir (S) and L. Adleman (A) at MIT. It is a algorithm for public key cryptography.

Serial

Serial means one event at one time. It is an opposite concept from parallel, which means multiple events happening at one time. In data transmission, time division and space division techniques are used, where time division separates the transmission of individual bits of information sent serially, and space division is used to have multiple bits sent in parallel.

SNMP (Simple Network Management Protocol)

SNMP govens network management and monitors network devices and their functions. It is not limited to TCP/IP networks.

SQL Server

SQL (Structured Query Language) Server is a relational database management system that implements the SQL, a database computer language developed at IBM in the 1970s. There are the following servers: Windows based Oracle 9i, IBM's DB2 and MS SQL Server.

SSL VPN

SSL VPN is SSL based VPN (Virtual Private Network). VPN is an enterprise communication service that cuts costs of circuits by using the Internet network of public network like a virtual network.

SSL (Secure Socket Layer)

SSL is a protocol for transmitting data between the WWW browser and web server. It was developed by Netscape, but also adopted by major companies, such as Microsoft. It can be applied not only to web browsers, but also TPC/IP applications such as the FTP. These applications use key certificate to verify the identity of endpoints. Using the encryption feature can reduce the risk of data transmission from being wiretapped over the Internet.

Stateful Inspection

Stateful inspection is also called dynamic packet filtering, as an industrial standard of network firewall that substitutes for static packet filtering.

UTM (Unified Threat Management)

UTM is a comprehensive security product that provides protection against multiple threats. It usually includes a firewall, anti-virus software, content filitering and spam filter in an intergrated package. IDC, a market data provider, first started using the term, UTM. The main advantages of UTM are simplicity, efficient installation and use and the ability to update all security features or programs at the same time. UTM products must keep up with the nature and diviersity of Internet threats as they are evolving and growing more complex. This enables system administrators to maintain multiple security programs.

Worm

Worm is a type of virus or self replicating code residing in a place that could compromise the computer system. There are viruses like Melissa that replicates itself in computers through email. An example of a worm is Worm.ExploreZip. Like most computer viruses, the worm gets embedded in a Trojan horse.

1.7 Security Target Composition

122 Chapter 1 introduces the Security Target and includes the security target reference, TOE reference, TOE overview, TOE description, typographical conventions, terms and definitions and security target composition.

123 Chapter 2 includes comformance claims on the common criteria, protection profile and package, and provides a rationale on the claims.

124 Chapter 3 defines security problems based on the TOE, security threats in the TOE operating environment, security policies of the organization and assumptions.

125 Chapter 4 identifies the security objectives for the TOE and operating environment to support the security policies of the organization and assumptions, and addresses the threats ideintified in the previous chapter.

126 Chapter 5 describes the extended components defined by the security target author without basis on the components in Parts 2 or 3 of the Common Criteria.

127 Chapter 6 describes security functional components and security assurance components that satisfy the security components.

128 Chapter 7 summarized the TOE and describes the method to satisfy the security functional components.

129 Chapter 8 is the reference used when writing this Security Target.

2 Conformance claims

130 This chapter how the Security Target conforms to the Common Criteria, Protection Profile and Package.

2.1 Common Criteria Conformance Claims

131 This Security Target conforms to the following Common Criteria.

- CC Identification
  - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1r1, 2006. 9, CCMB-2006-09-001
  - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1r2, 2007. 9, CCMB-2007-09-002
  - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1r2, 2007. 9, CCMB-2007-09-003
- CC Conformance
  - Part 2 conformant
  - Part 3 conformant

2.2 Protection Profile claims

132 This Security Target conforms to the following Protection Profile.

- Protection Profile Identification
  - Firewall Protection Profile V2.0 (KECS-PP-0093-2008, April 24, 2008)
- Protection Profile Conformance
  - Firewall Protection Profile v2.0 "Verifiable PP conformance"

2.3 Package claims

133 This Security Target conforms to the following Package.

- Assurance Package: EAL4 conformant

2.4 Conformance claim rationale

134 The Protection Profile conforms to Firewall Protection Profile V2.0 (hereinafter referred to as 'FW-PP', without the version).

- Protection Profile conformance method: "Verifiable Protection Profile Conformance" rationale

[Ref.] As the most basic rule of the verifiablePP conformance that can be verified in the Common Criteria, the ST must be equal to or more restrictive than the PP. The concept of 'equal to' means using "A", the SFR in the PP, as is in the ST, or substituting with another SFR, "B", of equal standard. For instance, it is like substituting FTA_SSL.1 (lock session) of the PP with FTA_SSL.3 (end session) in the ST, for managing session after user inactivity period. Also, the concept of 'more restrictive' means adding details such as detailed operation or applying strong requirements so that the TOE that satisfies the ST also satisfies the original PP requirements. .

135 The PP conformance claim rationale is as follows.

2.4.1 Security problem related conformance claim rationale

136 The security problem related conformance claim rationale is as Table 2.1 below. Table 2.1 shows that the security problems of this security target is equal to (or more restrictive than) those of FW-PP.

Table **2-1** ____ Security problem related conformance claim rationale-Threats

Cate-gory	Threat	Rationale
From FW-PP	T.Disguise	※ Equal to FW-PP. ▪ The threats in the left column in this ST are defined the same as the FW-PP.
	T.Failed recording	
	T.Illegal information flow	
	T.Illegal information leakage	
	T.Repeated authentica-tion attempt	
	T.Replay attack	
	T.Saved data damage	
	T.Address disguise	
	T.Damage	
	T.Abnormal packet transmission	

	T.Denial of service attack	the TOE and TOE operating environment to counter additional threats, so it is more re–strictive than FW–PP.
	T.Unauthorized TSF data change	

Table **2–2** _____ Security problem related conformation claim rationale–Organizational security policies

Cate–gory	Security Policy	Rationale
From FW–PP	P.Audit	※ Same as FW–PP. ▪ The security policies in the left column in this ST are defined the same as the FW–PP.
	P.Safe management	

Table **2–3** _____ Security problem related conformation claim rationale–Assumptions

Cate–gory	Assumption	Rationale
From FW–PP	A.Physical security	※ Same as FW–PP. ▪ The assumptions in the left column in this ST are defined the same as the FW–PP.
	A.Security maintenance	
	A.Trusted administrator	
	A.OS reinforcement	
	A.Sole connection point	
Addi–tion	A.Trusted_security man–agement_UI	※ More restrictive than FW–PP. ▪ The assumptions in the left colum are addi–tionally defined in this ST. Accordingly, this ST defines the TOE and TOE operating environ–ment to support the additional assumptions, so it is more restrictive than FW–PP.
	A.Trusted_update_server	
	A.Trusted_SSH_communication	
	A.Trusted_SSL_communication	
	A.Trusted_TOE_interoperable_server	
	A.Trusted_TOE_interoperable_engine	

2.4.2 Security objective related conformance claim rationale

137 The security objective related conformance claim rationale is as Table 2.4 below. Table 2.4 shows that the security objectives of this security target is equal to (or more re–strictive than) those of FW–PP.

Table **2–4** ____ Security objective related conformance claim rationale–Security objectives for TOE

Cate–gory	Security Objective for TOE	Rationale
From FW–PP	O.Audit	※ Same as FW–PP. ▪ The security objectives for TOE in the left
	O.Management	

Cate-gory	Security Objective for TOE	Rationale
	O.Data protection	column in this ST are defined the same as the FW-PP.
	O.Indetification and au-thentication	
	O.Information flow control	
Addi-tion	O.Abnormal packet filter	※ More restrictive than FW-PP. ▪ The security objectives for TOE in the left column are additionally defined in this ST as security objectives directly addresses the TOE. Accordingly, this ST defines the TOE to address additional security objectives, so it is more restrictive than FW-PP.
	O.DDoS protection	
	O.Safe state maintenance	

Table **2-5** _____ Security objective related conformance claim rationale-Security objectives on operating environment

Cate-gory	Security objective for op-erating environment	Rationale
From FW-PP	OE.Physical security	※ Same as FW-PP. ▪ The TOE security objectives for operating en-vironment in the left column in this ST are defined the same as the FW-PP.
	OE.Security maintenance	
	OE.Trusted administrator	
	OE.OS reinforcement	
	OE.Sole connection point	
	OE.Time stamp	
Addi-tion	OE.Trusted_security management_UI	※ More restrictive than FW-PP. ▪ The TOE security objectives for operating en-vironment in the left column are additionally defined in this ST as security objectives that need to be addressed based on techni-cal/procedural means supported by the op-erating environment for the TOE to provide security features. Accordingly, this ST defines the TOE operating environment to address additional security objectives, so it is more restrictive than FW-PP.
	OE.Trusted_update_serv er	
	OE.Trusted_SSH_commu nication	
	OE.Trusted_SSL_commu nication	
	OE.Trusted_TOE_interope rable_server	
	OE.Trusted_TOE_interope rable_engine	

2.4.3 Security components related conformance claim rationale

138 The security components related conformance claim rationale is as Table 2.6 below. Table 2.6 shows that the security components of this security target is equal to (or more restrictive than) those of FW-PP.

Table 2–6 Security components related conformance claim rationale

Cate-gory	Component	Rationale
From FW-PP	FAU_ARP.1	※ Equal to FW-PP. (But, excluding FAU_SAA.1.) ▪ Among the components in the left column, the operations allowed in the FW-PP on FAU_ARP.1, FAU_GEN.1, FAU_SAR.1, FAU_SAR_3, FAU_SEL.1, FAU_STG.1, FAU_STG.3 and FAU_ST.4 SFR were performed in this ST.
	FAU_GEN.1	
	FAU_SAA.1	
	FAU_SAR.1	
	FAU_SAR.3	
	FAU_SEL.1	
	FAU_STG.1	
	FAU_STG.3	
	FAU_STG.4	
From FW-PP	FDP_IFC.2	※ Equal to FW-PP. ▪ In this ST, the operations allowed in the FW-PP on SFR in the left column were performed.
	FDP_IFF.1	
Addi-tion	FDP_ACC.2(1)	※ More restrictive than FW-PP. ▪ In this ST, FDP_IFC.2, FDP_IFF.1 information flow control of FW-PP were added, and FDP_ACC.2(1) ~ (2), FDP_ACF.1(1) ~ (2), FDP_IFC.1(1) ~ (8), FDP_IFF.1(1) ~ (8) function components in the left column were additionally defined. It defines additional user data protection requirements, so it is more restrictive than FW-PP.
	FDP_ACF.1(1)	
	FDP_ACC.2(2)	
	FDP_ACF.1(2)	
	FDP_IFC.1(1)	
	FDP_IFF.1(1)	
	FDP_IFC.1(2)	
	FDP_IFF.1(2)	
	FDP_IFC.1(3)	
	FDP_IFF.1(3)	
	FDP_IFC.1(4)	
	FDP_IFF.1(4)	
	FDP_IFC.1(5)	
	FDP_IFF.1(5)	
	FDP_IFC.1(6)	
	FDP_IFF.1(6)	
	FDP_IFC.1(7)	
	FDP_IFF.1(7)	
	FDP_IFC.1(8)	
	FDP_IFF.1(8)	
From FW-PP	FIA_AFL.1	※ Equal to FW-PP. (FIA_AFL.1, FIA_SOS.1, FIA_UAU.4, FIA_UAU.7) ▪ Among the components in the left column, the opera–
	FIA_ATD.1(1)	
	FIA_ATD.1(2)	

Cate-gory	Component	Rationale
	FIA_ATD.1(3)	tions allowed in the FW-PP on FIA_AFL.1, FIA_SOS.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.2 function components were performed in this ST. ※ More restrictive than FW-PP. (FIA_ATD.1(1) ~ (4), FIA_UAU.1(1) ~ (3), FIA_UID.2(1) ~ (4)) ▪ In this ST, FIA_ATD.1, FIA_UAU.1, FIA_UID.2 function components specified in FW-PP in the left colum SFR, performed repeated operation and fine operation allowed by the CC to specify the additional user attributes and authentication, identification requirements, so it is more restrictive than FW-PP.
	FIA_ATD.1(4)	
	FIA_SOS.1	
	FIA_UAU.1(1)	
	FIA_UAU.1(2)	
	FIA_UAU.1(3)	
	FIA_UAU.4	
	FIA_UAU.7	
	FIA_UID.2(1)	
	FIA_UID.2(2)	
	FIA_UID.2(3)	
	FIA_UID.2(4)	
From FW-PP	FMT_MOF.1	※ Equal to FW-PP. ▪ In this ST, the operations allowed in the FW-PP on SFR in the left column were performed. ※ More restrictive than FW-PP. (FMT_MTD.1(3) FMT_SMR.1(1)~(2)) ▪ In this ST, repeated operation was conducted on FMT_MTD.1(3). This is requirement additional SFR on TSFdata management, so it is more restrictive than FW-PP. ▪ In this ST, repeated operation and fine operation were conducted on FMT_SMR.1. This is detailed classification of the roles of authorized users (super administrator, administrator, super log administrator and log administrator) and designation of rights for each role. Also, it additionally specifies the role of authorized user, so it is more restrictive than FW-PP.
	FMT_MSA.1	
	FMT_MSA.3	
	FMT_MTD.1(1)	
	FMT_MTD.1(2)	
	FMT_MTD.1(3)	
	FMT_MTD.2	
	FMT_SMF.1	
	FMT_SMR.1(1)	
	FMT_SMR.1(2)	
From FW-PP	FPT_TST.1	※ Equal to FW-PP. ▪ In this ST, the operations allowed in the FW-PP on SFR in the left column were performed.
Addition	FPT_FLS.1	※ More restrictive than FW-PP. ▪ In this ST, SFR for maintaining safe state when there is error, protecting TSF data during inter-transmission and external protection that interacts with the TOE was additionally defined. It defines additional security components for TSF protection, so it is more restrictive than FW-PP.
	FPT_ITT.1	
	FPT_TEE.1	
Addition	FRU_FLT.1	※ More restrictive than FW-PP. ▪ In this ST, SFR to force maximum allotted value to respond to attack that could use up the TOE resources and management of some TOE features when an error
	FRU_RSA.1	

Cate-gory	Component	Rationale
		occurs is defined. It defines additional security com-ponents to additionally use of TOE resource, so it is more restrictive than FW-PP.
From FW-PP	FTA_SSL.1 FTA_SSL.3	※ Equal to FW-PP. ▪ In this ST, the operations allowed in the FW-PP on SFR in the left column were performed.

2.4.4 Assurance components related conformance claim rationale

139 The assurance components related conformance claim rationale is as Table 2.7 below. Table 2.7 shows that the assurance components of this security target is equal to (or more restrictive than) those of FW-PP

Table 2-7 Assurance components related conformance claim rationale

FW-PP/Security Target		Rationale
Assurance Class	Assurance Component	
Security Target evaluation	ASE_INT.1 ST Introduction	This ST provides assurance components conforming to EAL4. ▪ This ST includes completely equal assurance components to FW-PP, and ▪ does not add to the FW-PP or specify stronger components.
	ASE_ECD.1 Extended components definition	
	ASE_CCL.1 Conformance claims	
	ASE_OBJ.2 Security objectives	
	ASE_REQ.2 Derived security requirements	
	ASE_SPD.1 Security problem definition	
	ASE_TSS.1 TOE summary specification	
Development	ADV_ARC.1 Security architecture description	
	ADV_FSP.4 Complete functional specification	
	ADV_IMP.1 Implementation representation of the TSF	
	ADV_TDS.3 Basic modular design	
Guidance documents	AGD_OPE.1 User guide	
	AGD_PRE.1 Preparative procedures	
Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	
	ALC_CMS.4 Problem tracing management scope	
	ALC_DEL.1 Delivery procedures	
	ALC_DVS.1 Identification of security measures	
	ALC_LCD.1 Developer defined life-cycle model	
	ALC_TAT.1 Well-defined development tools	
Tests	ATE_COV.2 Analysis of coverage	
	ATE_DPT.2 Testing: security enforcing modules	
	ATE_FUN.1 Functional testing	
	ATE_IND.2 Independent testing - sample	
Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	

3 Security problem definition

140 Security problem definition defines assumptions that need to be supported, organizational security policies and threats intended for the TOE and TOE operating environment to manage.

141 This ST conforms to all security problem definitions of the FW-PP. The security problems (threats, organizational security policies and assumptions) additionally defined in this ST is as Table 3.-1 below.

Table **3-1** _____ Security problem definition-Added from Security Target

Category	Security problem definition added from Security Target
Threats to secuirity	▪ T.Damage ▪ T.Abnormal packet transfer ▪ T.DoS attack ▪ T.Illegal access
Organizational security policies	▪ N/A
Assumptions	▪ A.Trusted_security management_UI ▪ A.Trusted_update_server ▪ A.Trusted_SSH_communication ▪ A.Trusted_SSL_ ▪ A.Trusted_TOE_interoperable_server ▪ A.Trusted_TOE_interoperable_engine

3.1 Threats to secuirity

142 The threat agent is IT entity or user that harms the internal and TOE assets in an abnormal way or attempts to make illegal acces to the internal and TOE assets from outside. The threats have reinforced special knowledge, resource and motive.

143 This Security Target confoms to all threats stated in the FW-PP. The threats that are additionally defined are as below.

- T.Damage
- T.Abnormal packet transfer
- T.DoS attack
- T.Illegal access

3.1.1 Threats to secuirity

144 The threats taken from the FW-PP to which this Security Target conforms are as follows. They are completely the same as the FW-PP.

T.Disguise

145 The threat agent may attempt to access the TOE, disguising as the authorized user.

T.Failed recording

146 The threat agent may use up the storage space, causing security related events of the TOE not to be recorded.

T.Illegal information flow

147 The threat agent may break into the internal network by bringing in unauthorized information from outside.

T.Illegal information leakage

148 An internal user may leak information in an illegal way through the network.

T.Repeated authentication attempt

149 The threat agent may gain authorized user permissions by attempting authentication repeatedly to access the TOE.

T.Replay attack

150 The threat agent may access the TOE by replaying the authentication data of the authorized user.

T.Saved data damage

151 The threat agent may expose, change and delete TSF data saved on the TOE in an unauthorized way.

T.Address disguise

152 The external network threat agent may gain internal network access permission by disguising its source address as an internal address.

3.1.2 Threats to secuirity (addition)

153 The threats that are additionally defined in the Security Target are as below.

T.Damage

154 Normal service cannot be provided due to damage cuased by external attack while the TOE or external entity that interacts with the TOE (DBMS) is being used.

T.Abnormal packet transfer

155 The threat agent may cause system error in the internal network by sending network

packets with abnormal structure.

T.DoS attack

156 The threat agent may obstruct normal users through abnormal excessive use of the service resources of the computer system on the internal network of the TOE operating environment.

T.Illegal access

157 The threat agent may access an unauthorized IT entity or the TOE through the network.

3.2 Organizational security policies

158 The organizational security policies in this section are addressed by the TOE.

159 This Security Target confoms to all organizational security policies in stated in the FW–PP. There are no additionally defined organizational security policies in this Se–curity Target.

3.2.1 Organizational security policies

160 The organizational security policies taken from the FW–PP to which this Security Target conforms are as follows. They are completely the same as the FW–PP.

P.Audit

161 Security related events shall be recorded and maintained to trace the responsibility towards all security related behaviors, and the recorded data shall be reviewed.

P.Safe management

162 The TOE shall provide management means for the authorized administrator to manage the TOE safely.

3.3 Assumptions

163 It is assumed that the following conditions exist in the TOE operating environment.

164 This Security Target conforms to all assumptions in the FW-PP. In addition, the following assumptions are additionally defined.

- A.Trusted_security management_UI
- A.Trusted_update_server
- A.Trusted_SSH_communication
- A.Trusted_SSL_
- A.Trusted_TOE_interoperable_server
- A.Trusted_TOE_interoperable_engine

3.3.1 Assumptions

165 The assumptions taken from the FW-PP to which this Security Target conforms are as follows. They are completely the same as the FW-PP.

A.Physical security

166 The TOE is located in a physically safe environment only the authorized administrator can access.

A.Security maintenance

167 When the internal network environment changes due to change in network configuration and increase/decrease of hosts and services, the changed environment and security policies shall be immediately reflected in the TOE management policies, to maintain the same security standard as before..

A.Trusted administrator

168 An authorized TOE administrator shall not be malicious and be properly trained on the TOE management features, and perform his/her duties according to the administrator guide.

A.OS reinforcement

169 Stability of OS is assured by reinforcing OS vulnerabilities and removing all unnecessary OS services or means.

A.Sole connection point

170 All communications between the external network and internet network shall be made

through the TOE only.

3.3.2 Assumptions (addition)

171 The assumptions that are additionally defined in the Security Target are as below.

A.Trusted_security management_UI

172 The TOE provides security management interface (GUI) through a web browser and security management interface (CLII) through through SSH/Serial communication supporting software. In general, MS Internet Explorer is used as the web browser. The administrator system OS (e.g. Windows XP Pro) where the TOE security management interface is operated, web browser, and the SSH/Serial communication softwareare distributed and installed in a safe way. The authorized administrator assures reliability and stability on the security management interface by safe management and conforming to the administrator guide.

A.Trusted_update_server

173 The TOE operating environment provides CDN server and AST server which is a trusted server to update the list of vulnerabilities and firmware (patch), and the anti-virus engine.

A.Trusted_SSH_communication

174 The TOE operating environment provides a trusted SSH based communication mechanism that can be used for IT entity (user) authentication and password communication during communication between the TOE and trusted external IT product of the TOE. Through this, reliability and stability are assured during SSH communication.

A.Trusted_SSL_communication

175 The TOE operating environment creates the certificate to use for SSL certification every time the TOE (exclusive device) is running, and saves it on the TOE and manages the certificate safely. The TOE operating environment provides a trusted SSL based communication mechanism that can be used for IT entity (user) authentication and password communication during communication between the TOE and trusted external IT product of the TOE. Through this, reliability and stability are assured during SSL communication.

[Ref.] A trusted external IT entity means an ‘administrator system’ that accesses the security management features provided by the TOE and update server stated in 'A.Trusted_update_server'.

A.Trusted_TOE_interoperable_server

176 The TOE operating environment provides a trusted server that interoperates with the TOE. The TOE provides features that are interoperable with Syslog Server, SNMP Manager Server, Korea Internet Safety Commission DB Server, NTP Server, and RADIUS Server. These servers are managed safely, and reliability and stability are assured.

A.Trusted_TOE_interoperable_engine

177 The TOE operating environment provides a filtering engine (V3 Engine) used in the anti-virus feature of the TOE. The safety of this engine has been verified through wide use, and its reliability and stability are assured.

4 Security objectives

178 This Security Target defines the security policies in two categories– security policies for the TOE and security policies for the operating environment. The security objectives for the TOE are directly addresses the TOE and the security objectives for the environment must be addressed based on technical/procedural measure supported by the operating environment for the TOE to provide the security technicalities.

179 This Security Target conforms to all the security objectives of FW–PP. The security objectives (for the TOE and operating environment) additionally defined in this Security Target are as Table 4–1 below.

Table **4–1** _____ Security objectives–Added to Security Target

Category	Security objectives added to the Security Target
Security objectives for the TOE	▪ O.Abnormal packet filter ▪ O.DDoS protection ▪ O.Safe state maintenance ▪ O.Access control
Security objectives for the environment	▪ OE.Trusted_security managemen_UI ▪ OE.Trusted_update_server ▪ OE.Trusted_SSH_communication ▪ OE.Trusted_SSL_communication ▪ OE.Trusted_TOE_interoperable_server ▪ OE.Trustede_TOE_interoperable_engine

4.1 Security objectives for the TOE

180 The security objectives to be directly addressed by the TOE are as below.

181 This Security Target takes all the TOE security objectives from the FW–PP. In addition, it defines the following TOE security objectives.

- O.Abnormal packet filter
- O.DDoS protection
- O.Safe state maintenance
- O.Access control

4.1.1 Security objectives for the TOE

182 The security objectives for the TOE taken from the FW–PP to which this Security Target conforms are as follows. They are completely the same as the FW–PP.

O.Audit

183 The TOE shall maintain a record of security related events tha can be traced for security related behavorial responsibility, and provide a means to review the recorded data.

O.Management

184 The TOE shall provide a management measure for the authorized administrator to manage the TOE efficiently in a save way.

O.Data protection

185 The TOE shall protect the saved TSF data from unauthorized exposure, modification and deletion.

O.Identification and authentication

186 The TOE shall identify the user solely and authentication the user identity.

O.Information flow control

187 The TOE shall control unauthorized internal to/from external information flow.

4.1.2 Security objectives for the TOE (addition)

188 The TOE security objectives additionally defined in this Security Target are as below.

O.Abnormal packet filter

189 The TOE shall filter packets with abnormal structure amongs normal packets that pass the TOE.

[Ref.] Abnormal packets mean rooting packets, broadcasting packets, packets with disguise IP address, or packets that are not TCP/IP defined in the Internet standard protocol, such as RFC 791 (Internet protocol), RFC 792 (Internet control message protocol) and RFC 793 (transmission control protocol).

O.DDoS protection

190 When attackers use up the computer service resources abnormally, the TOE shall block them to enable users with normal network service to use.

O.Safe state maintenance

191 The TOE shall maintain safe state when an error occurs in the external entity (DBMS) that interacts with the TSF and TOE.

O.Access control

192 The TOE shall control access by an unauthorized IT entity and external or internal access to the TOE.

4.2 Security objectives for the environment

193 The security objectives for operating environment shall be addressed based on technical/procedural means supported by the operating environment for the TOE to provide security features.

194 This Security Target conforms to the security objectives for the environment included in the FW-PP. Also, it additionally defines security objectives for the following operating environment.

- OE.Trusted_security managemen_UI
- OE.Trusted_update_server
- OE.Trusted_SSH_communication
- OE.Trusted_SSL_communication
- OE.Trusted_TOE_interoperable_server
- OE.Trustede_TOE_interoperable_engine

4.2.1 Security objectives for the environment

195 The security objectives for the operating environment taken from the FW-PP to which this Security Target conforms are as follows. They are completely the same as the FW-PP.

OE.Physical security

196 The TOE shall be located in a physically safe environment only the authorized administrator can access.

OE.Security maintenance

197 When the internal network environment changes due to change in network configuration and increase/decrease of hosts and services, the changed environment and security policies shall be immediately reflected in the TOE management policies, to maintain the same security standard as before.

OE.Trusted administrator

198 An authorized TOE administrator shall not be malicious and be properly trained on the TOE management features, and perform his/her duties according to the administrator guide.

OE.OS reinforcement

199 Stability and reliability of the OS shall be assured by reinforcing OS vulnerabilities and

removing all unnecessary OS services or means.

OE.Sole connection point

200 All communications between the external network and internet network shall be made through the TOE only.

OE.Time stamp

201 The TOE shall accurately record security related events, using a reliable time stamp provided on the TOE operating environment.

4.2.2 Security objectives for the environment (addition)

202 The security objectives for the environment additionally defined in this Security Target are as below.

OE.Trusted_security managemen_UI

203 The TOE shall provide security management interface (GUI) through a web browser and security management interface (CLII) through through SSH/Serial communication supporting software. In general, MS Internet Explorer is used as the web browser. The administrator system OS (e.g. Windows XP Pro) where the TOE security management interface is operated, web browser, and the SSH/Serial communication software are distributed and installed in a safe way. The authorized administrator assures reliability and stability on the security management interface by safe management and con-forming to the administrator guide.

OE.Trusted_update_server

204 The TOE operating environment shall provide CDN server and AST server which is a trusted server to update the list of vulnerabilities and firmware (patch), and the anti-virus engine.

OE.Trusted_SSH_communication

205 The TOE operating environment shall assure reliability and safety by using SSH protocol based communication mechanism provided by the TOE operating environment when forming communication channel for safe communication with a remote management console (system that access CLI through SSH communication program). It shall protect the TSF data by verifying the user any encrypting communication using SSH protocol.

OE.Trusted_SSL_communication

206 The TOE operating environment shall assure reliability and safety by using SSL protocol

based communication mechanism provided by the TOE operating environment when forming communication channel for safe communication with the administrator system and TOE and update server.

OE.Trusted_TOE_interoperable_server

207 The TOE operating environment shall assure reliability and safety by safely managing the Syslog Server, SNMP Manager Server, Korea Internet Safety Commission DB Server, NTP Server, and RADIUS Server that interoperates with the TOE.

OE.Trustede_TOE_interoperable_engine

208 The TOE operating environment shall assure reliability and safety by safely managing the engine used for anti-virus interoperation of the TOE. Also, it shall maintain the engine to the latest version to protect the TOE and TOE operating environment from new malicious attacks.

4.3 Security objectives rationale

209 The security objectives rationale corresponds to the security objectives, sufficiently address security problems, and verify that athey are not excessive, but essential.

210 The security objectives rationale verifies the following.

- Each assumption, threat and organizational security policy are addressed by at least one security objective.
- Each security objective addresses at least one assumption, threat and organizational security policy.

Table 4–2 _____ Security problem definition and security objective

Security Objectives / Threats to secuirity	TOE Security Objectives									Security objectives for the environment											
	O.Audit	O.Management	O.Data Protection	O.Identification and	O.Information	O.Abnormal	O.DDoS protection	O.Safe State	O.Access Control	OE.Physical Security	OE.Security maintenance	OE.Trusted administrator	OE.OS reinforcement	OE.Sole connection point	OE.Time Stamp	OE.Trusted_security managemen_U	OE.Trusted_update_server	GE.Trusted_SSH_commun cal on	GE.Trusted_SSL_commun cal on	OE.OE.Trusted_TOE_interoperable_server	OE.Trustede_TOE_interoperable_engine
T.Disguise				x																	
T.Failed recording	x																				
T.Illegal information flow					x																
T.Illegal information leakage					x																
T.Repeated Authentication Attempt	x			x																	
T.Replay attack				x																	
T.Saved data damage			x	x																	
T.Address disguise					x	x	x														
T.Damage								x													
T.Abnormal Packet Transfer	x			x		x															
T.DoS attack	x			x			x														
T.Illegal access									x												
P.Audit	x														x						
P.Safe management		x										x									
A.Trusted_security management_UI										x											
A.Trusted_update_server											x										
A.Trusted_SSH_ Communication												x									
A.Trusted_SSL_													x								
A.Trusted_TOE_ Interoperable_Server														x							
A.Trusted_Security Management_UI																x					
A.Trusted_update_server																	x				
A.Trusted_SSH_ Communication																		x			
A.Trusted_SSL_ Communication																			x		
A.Trusted_TOE_ Interoperable_Server																				x	
A.Trusted_TOE_ Interoperable_Engine																					x

4.3.1 TOE security objectives rationale

O.Audit

211 The TOE assures providing means to record, maintain and review security related cases in detail and accurately. When repeated attempt of authentication is made through generated audit record, the identity of the attacker shall be identified. Also, attacks that creates and sends abnormal packets and denial or service attacks shall be traced through the audit record. It is needed to counter T.Abnormal packet transmission and T.Denial of service attack, and perform P.Audit, an organizational security policy.

O.Management

212 The TOE provides measure for the authorized administrator to safely manage the TOE. It is needed to perform P.Safe management, an organizational security policy.

O.Data protection

213 The TOE assures TSF data integrity, so it is needed to counter T.Saved data damage threat.

O.Identification and authentication

214 The TOE assures sole identification and authentication of user. In particular, identification of user is needed when generating audit record on abnormal packet transmission and DDoS protection. It is needed to counter T.Assumption, T.Repeated authentication attempt, T.Replay attack, T. Saved data damage, T.Abnormal packet transmission and T.Denial of service attack threats.

O.Information flow control

215 The TOE assures control of information flow according to the security policy so it is needed to counter T.Illegal information flow, T.Illegal information leakage and T.Address disguise threats.

O.Abnormal packet filter

216 This security objective assures filtering of packets that does not conform to the TCP/IP standard among packets transmitted from external to internal network, packets with internal address among packets from external network, broadcasting packets and rooting packets. So this security policy is needed to counter T.Abnormal packet transmission and T.Address disguise threats.

O.DDoS protection

217 An attacker may launch denial of service attack against computers on the internal network by passing through the TOE. One of the major denial of service attacks is a remote user using up the computer resources by flooding the network with useless traffic. The internal computer then prevents a normal user from using the computer by allotting lots of resources to the attacker. As a proactive measure, the TOE assures normal usage of computer by preventing a specific user from exclusively using the resources of a specific computer. So, this security objective is needed to counter T.Denial of service attack and T.Address disguise threats.

O.Safe state maintenance

218 The TOE may not be able to provide normal service to users caused by damage in TOE and unexpected attacks from outside. This security objective assures maintaining safe status when an error occurs due to damage in the TOE. Also, in order to prove that the external entity (DBMS) that interacts with the TOE is accurately managed, it conducts tests regularly on start up as well as during operation. When the test has failed, a warning window is displayed for the authorized administrator to restore the state to maintain a safe status. So, this security objective is needed to counter T.Damage threat.

O.Access control

219 This security objective assures control access to an unauthorized IT entity and TOE access according to the security policy, so it is needed to counter T.Illegal access threat.

4.3.2 Operating environment security objectives rationale

OE.Physical security

220 The security objective for this operating environment assures physical safety of the TOE, so it is needed to support A.Physical security assumption.

OE.Security maintenance

221 The security objective for this operating environment assures the same security standnard as before by reflecting the changed environment and security policy to the TOE operating environment immediately when the internal network environment changes due to increase/decrease of services and hosts and change in internal network configuration, so it is needed to support A.Security maintenance assumption.

OE.Trusted administrator

222 The security objective for this operating environment assures trusted authorized TOE administrator, so it is needed to conduct P.Safe management organizational security policy and support A.Trusted administrator assumption.

OE.OS reinforcement

223 The security objective for this operating environment assures safe and reliable OS by reinforcing OS vulnerabilities and removing all unnecessary OS services or means, so it is needed to support A.OS reinforcement assumption.

OE.Sole connection point

224 The security objective for this operating environment assures all communications between the external network and internet network tol be made through the TOE only, so it is needed to support A.Sole connection point assumption.

OE.Time stamp

225 The security objective for this operating environment assures accurate record of security related events, using a reliable time stamp provided on the TOE operating environment, so it is needed to support A.Time stamp assumption.

OE.Trusted_security management_UI

226 The security objective for this operating environment assures safe distribution and installation of software and sub-OS used to access the security management interface (GUI and CLI) provided by the TOE and reliability and stability of the software used for

security management by the authorized administrator in a safe way, so it is needed to support A.Trusted_security management_UI assumption.

OE.Trusted_update_server

227 The security objective for this operating environment assures renewal and management of Korea Internet Safety Commission DB and Anti-virus Engine, and renewal (patch) of the firmware, database on vulnerabilities managed by the TOE, so it is needed to support A.Trusted_update_server assumption.

OE.Trusted_SSH_communication

228 The security objective for this operating environment assures provision of trusted SSH based communication mechanism for safe communication between the TOE and system that access the security management (CLI) provided by the TOE, so it is needed to support A.Trusted_SSH_communication assumption.

OE.Trusted_SSL_communication

229 The security objective for this operating environment assures provision of trusted SSL based communication mechanism for forming communication channel and mutual authentication for safe communication for communication between the TOE and update server and administrator system, so it is needed to support A.Trusted_SSL_communication assumption.

OE.Trusted_TOE_interoperable_server

230 The security objective for this operating environment assures safe management of Syslog Server, SNMP Manager Server, Korea Internet Safety Commission DB Server, NTP Server, and RADIUS Server that interoperates with the TOE, so it is needed to support A.Trusted_TOE_interoperable_server assumption.

OE.Trusted_TOE_interoperable_engine

231 The security objective for this operating environment assures safe management of TOE and TOE against new malicious attacks by assuring safe management of the TOE operating environment engine that calls from the anti-virus provided/managed by the TOE, so it is needed to support A.Trusted_TOE_interoperable_engine assumption.

5 Extended components definfition

232 This chapter describes the extended components described in Parts 2 or 3 of the Common Criteria in this Security Target.

5.1 Extended components definfition

233 There are no extended components in Parts 2 or 3 of the Common Criteria in this Security Target.

6 Security requirement

234 This chapter describes the features and assurance requirements that need to be satisfied by the TOE.

235 The security requirements of this Security Target were written, conforming in a verifiable manner to the following Protection Profile.

- Firewall Protection Profile V2.0 (KECS-PP-0093-2008, April 24, 2008) (Hereinafter referred to as 'FW-PP')

236 This Security Target defines the subject, object, operation, security attributes, external entity and other conditions used in the security requirements as follows (※ Note- there are no entity, object, operation, security attributes, external entity and other conditions used in the assurance requirements).

a) Subject, object, related security attributes, and operation: Refer to Table 6-1 below

b) External entity: Refer to Table 6-2 below

Table **6-1** Definition of subject, object, related security attributes and operation

※ (*) Only 'query' operation allowed for administrator and log administrator

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
Authorized administrator (super log administrator)	▪ Identifier ▪ Password ▪ Max. allowed login attempts ▪ Lock time ▪ Locked/ Unlocked ▪ Name ▪ Permission	Audit data	File	Statistics, Backup and restore in semipermanenet sub-memory	FMT_MTD.1(2)
Authorized administrator (Super administrator, * Administrator)	▪ Identifier ▪ Password ▪ Access permission ▪ Locked/ Unlocked	Audit data backup settings (Scheduled backup, backup path, backup	File	Query, modify	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		target, latest backup list)			
		Important file that configures TOE (Configuration file)	File	Backup and restore in semipermanenet sub-memory, Restore to initial settings	FMT_MTD.1(2)
		Integrity check data	File	Query, modify	FMT_MTD.1(2)
		Update settings (Automatic update status, update interval)	File	Query, modify	FMT_MTD.1(2)
		List of vulnerabilities (intrusion prevention rules)	File	Query, modify, renew to latest data, create new vulnerability, delete vulnerability created and added by authorized administrator	FMT_MTD.1(2)
		Options: Log settings (log type, log transfer method, Log Server)	File	Query, modify, delete, create and delete Log Server (IP address) list to get audit data	FMT_MTD.1(2)
		Settings to generate selective audit data	File	Query, modify	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		Configuration: TOE identification (host) name	File	Query, modify	FMT_MTD.1(2)
		Configuration: Time	File	Query, modify	FMT_MTD.1(2)
		Configuration: Session time limit setting (TCP, UDP, ICMP session maintenance time, TCP MSS status and size, TCP validity test)	File	Query, modify	FMT_MTD.1(2)
		HA settings information: Monitoring port (physical port, local/remote device's virtual IP, Ping allow status) list	File	Query, modify, create and delete monitoring port	FMT_MTD.1(2)
		HA settings information: HA settings	File	Query, modify	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		(Status, priority, connection NIC, remote device IP address, Heart beat status)			
		Policy applied list: IP address (name, type, IP address, network port, security level) and IP address group (name, network port, IP address object included in group) list	File	Query, modify, delete, create and delete IP address and IP address group	FMT_MTD.1(2)
		Policy applied list: Service (name, protocol, source/destination port) and service group (name, service object	File	Query, modify, delete, create and delete service and service group	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		included in group) list			
		Policy applied list: Schedule (name, interval, time) list	File	Query, modify, (create and delete schedule)	FMT_MTD.1(2)
		Policy applied list: QoS application (name, min. bandwidth, max. bandwidth, priority) list	File	Query, modify, create and delete QoS application list	FMT_MTD.1(2)
		Proxy service object list: Proxy (name, proxy type (Single selection among general proxy, HTTP Proxy, FTP Proxy, SMTP Proxy, POP3 Proxy, Oracle Proxy,	File	Query, modify, delete, create and delete proxy service object	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security at-tribute	List	Security at-tribute		
		UDP Proxy, DNS Proxy), port, time limit, transfer host) and proxy group (name, proxy object included in group) list			
		Proxy ad-vanced rules settings (Ant-virus status, website filtering status, anti-spam status, command block status, list of com-mands to block, DNS re-sponse scan status, status of IP addres block during DNS re-sponse)	File	Query, modify	FMT_MTD.1(2)
		Proxy authenti-cation	File	Query, modify	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		user list (User ID, Proxy type, connected IP address, connection time)			
		No. of simultaneous proxy connection (Specified by General, HTTP, FTP, SMTP, POP3, Oracle, UDP, DNS Proxy)	File	Query, modify	FMT_MTD.1(2)
		Anti-virus status (Email message scan status, mail size, POP3 scan settings, SMTP scan settings, list of file extensions to filter)	File	Query, modify, create and delete file extension	FMT_MTD.1(2)
		Anti-spam settings (Outgoing mail scan	File	Query, modify, create and delete mail to be applied as	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		status, mail size, POP3 scan settings, SMTP scan settings, mail to apply as spam/allowed mail and action list, RBL status and RBL Server list)		spam mail/allowed mail and action, create and delete RBL Server	
		Anti-spam settings: Keyword filtering list (Group name, keyword, target, keyword type)	File	Query, modify, create and delete keyword filter	FMT_MTD.1(2)
		Website filtering settings (Internet content rating DB status, content rating tag scan status and filtering tag, attachment filtering	File	Query, modify	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		status and action, block message and redirection URL, website content filtering)			
		Website filtering settings: URL filtering list (group name, URL)	File	Query, modify, delete, create and delete website filter	FMT_MTD.1(2)
		Website filtering settings: URL filtering exceptions list (Status, target, source/destination)	File	Query, modify, delete, create and delete URL filter exceptions	FMT_MTD.1(2)
		DDoS protection settings	File	Query, modify	FMT_MTD.1(2)

※ (*) Only 'query' operation allowed for administrator and log administrator

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
Authorized administrator (Super administrator, *	▪ Identifier ▪ Password ▪ Max. allowed login attempts	Connection between physically separated	File	Query	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
Administrator)	▪ Lock time ▪ Locked/Unlocked ▪ Name ▪ Permission	TOEs (Log Server and exclusive device)			
		Information on user logged in to TOE	File	Query	FMT_MTD.1(2)
		Infomration of log server to connect and connection settings, automatic logout status	File	Query, modify	FMT_MTD.1(2)
		Alert mail settings Spam mail list transfer status, list sending time, email address, alert method, recipient's email address, Mail Server information (IP address, port, ID, password)	File	Query, modify	FMT_MTD.1(2)

Subject (User)		Object (Information)		Operation	SFR
List	Security attribute	List	Security attribute		
		Account settings (AhnLab LogServer) (ID, password, name, permission, login, no. of allowed failed login attempts, lock time)	File	Query, modify, create and delete user list	FMT_MTD.1(2)
		Information on TOE (exclusive device) to manage (TOE (exclusive device) name, IP address, Firmware version, continuous usage time, status)	File	Query	FMT_MTD.1(2)

Table **6-2** _____ Definition of external entity

External entity	Description	SFR
Update Server	Called by TOE when performing update through AST Server and CDN Server used in Anti-Virus Engine, TOE patch and pattern updates.	FMT_MTD.1(2)
TOE interoperable server	TOE interoperates with SNMP Manager Server, Korea Internet Safety Commission DB Server, MS SQL Server, NTP Server and RADIUS Server according to the security policies specified by the authorized administrator.	FAU_ARP.1, FDP_IFF.1(1) FPT_TEE.1, FMT_MTD.1(2), FIA_ATD.1(2)

External entity	Description	SFR
TOE interoper–able engine	The TOE calls Anti–Virus Engine that interoperates with the TOE according to the security policies specified by the authorized administrator.	FDP_IFF.1(8)
Administration system	System used by authorized administrator to manage the security of TOE with administrator system directly connected to the TOE and direct data cable when using security managemetn feature through direct data communication, ad–ministrator system with software that supports SSH communication or web browser that supports SSL communication (128bit encryption).	FMT_MOF.1
Audit data man–agement system	System on which AhnLab LogServer, an MS SQL Server and TOE audit data management program, is installed. The above web browser or adminis–trator with software that supports SSH communi–cation is used. TOE audit data is saved.	FMT_MOF.1, FPT_ITT.1

6.1 Security functional requirements

237 The security function requirements defined in this Security Target conforms to the FW–PP. Additional security functional requirements in this ST not defined in the FW–PP are based on the functional components in Part 2 of the Common Criteria. For reference, this Security Target conforms to the FW–PP in a verifiable manner.

[Ref.] Table 6–3 below summarizes the functional components additionally defined in FW–PP. For further details, refer to "6.2 Security functional requirements (addition)".

Table **6–3** Security functional requirements added to FW–PP

Class name	Assurance component	
User data protection	FDP_ACC.2(1) ~ (2)	Complete access control
	FDP_ACF.1(1) ~ (2)	Security attribute based access control
	FDP_IFC.1(1) ~ (10)	Subset information flow control
	FDP_IFF.1(1) ~ (10)	Simple security attributes
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_TEE.1	Testing of external entities
Resource utilisation	FRU_FLT.1	Degraded fault tolerance
	FRU_RSA.1	Maximum quotas

238 The operations not completed in Part 2 of the Common Criteria or security functional requirements for operations incomplete in the FW–PP to which the ST conforms have been completed by the author of this ST.

239 Table 6–4 below summarizes the functional components defined by this ST.

Table **6-4** ____ Security functional requirements

Class name	Assurance component		Note
Security audit	FAU_ARP.1	Security alarms	FW-PP
	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	FW-PP
	FDP_IFF.1	Simple security attributes	
	FDP_ACC.2(1)	Complete access control	Addition
	FDP_ACF.1(1)	Security attribute based access control	
	FDP_ACC.2(2)	Complete access control	
	FDP_ACF.1(2)	Security attribute based access control	
	FDP_IFC.1(1)	Subset information flow control	
	FDP_IFF.1(1)	Simple security attributes	
	FDP_IFC.1(2)	Subset information flow control	
	FDP_IFF.1(2)	Simple security attributes	
	FDP_IFC.1(3)	Subset information flow control	
	FDP_IFF.1(3)	Simple security attributes	
	FDP_IFC.1(4)	Subset information flow control	
	FDP_IFF.1(4)	Simple security attributes	
	FDP_IFC.1(5)	Subset information flow control	
	FDP_IFF.1(5)	Simple security attributes	
	FDP_IFC.1(6)	Subset information flow control	
	FDP_IFF.1(6)	Simple security attributes	
	FDP_IFC.1(7)	Subset information flow control	
	FDP_IFF.1(7)	Simple security attributes	
	FDP_IFC.1(8)	Subset information flow control	

Class name	Assurance component		Note
	FDP_IFF.1(8)	Simple security attributes	
Identification and authentication	FIA_AFL.1	Authentication failure handling	FW-PP
	FIA_ATD.1(1)	User attribute definition	
	FIA_ATD.1(2)	User attribute definition	Addition (repeated)
	FIA_ATD.1(3)	User attribute definition	
	FIA_ATD.1(4)	User attribute definition	
	FIA_SOS.1	Verification of secrets	FW-PP
	FIA_UAU.1(1)	Timing of authentication	
	FIA_UAU.1(2)	Timing of authentication	Addition (repeated))
	FIA_UAU.1(3)	Timing of authentication	
	FIA_UAU.4	Single-use authentication mechanisms	FW-PP
	FIA_UAU.7	Protected authentication feedback	
	FIA_UID.2(1)	User identification before any action	
	FIA_UID.2(2)	User identification before any action	Addition (repeated)
	FIA_UID.2(3)	User identification before any action	
	FIA_UID.2(4)	User identification before any action	
Security management	FMT_MOF.1	Management of security functions behaviour	FW-PP
	FMT_MSA.1	Management of security attributes	
	FMT_MSA.3	Static attribute initialisation	
	FMT_MTD.1(1)	Management of TSF data	
	FMT_MTD.1(2)	Management of TSF data	
	FMT_MTD.1(3)	Management of TSF data	Addition (repeated)
	FMT_MTD.2	Management of limits on TSF data	FW-PP
	FMT_SMF.1	Specification of Management Functions	
	FMT_SMR.1(1)	Security roles	
	FMT_SMR.1(2)	Security roles	Addition (repeated)
Protection of the TSF	FPT_TST.1	TSF testing	FW-PP
	FPT_FLS.1	Failure with preservation of secure state	Addition
	FPT_ITT.1	Basic internal TSF data transfer protection	
	FPT_TEE.1	Testing of external entities	

Class name	Assurance component		Note
Resource utilisa-tion	FRU_FLT.1	Degraded fault tolerance	Addition
	FRU_RSA.1	Maximum quotas	
TOE access	FTA_SSL.1	TSF-initiated session locking	FW-PP
	FTA_SSL.3	TSF-initiated termination	
(※ The 'FW-PP' means SFR take from the PP, where as 'Addition' means SFR added from the ST.)			

6.1.1 Security audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [assignment: list of actions] upon detection of a potential security violation.

{

a) Failed authentication audit events in FIA_UAU.1(1) ~ (3):

- Notify, Logging

b) Control rules violation events in FDP_IFF.1, FDP_ACF.1(1) ~ (2), FDP_IFF.1(1) ~ (4), FDP_IFF.1(6) ~ (8):

- Notify, Drop, Logging

c) Control rules violation events in FDP_IFF.1(5):

- Notify, Prevention, Quarantine, Session Drop, Logging

d) Integrity violation events in FPT_TST.1:

- Notify, Logging

e) Audit events reaching specified limit for capacity (%) and period (minutes) of auditable events on CPU, memory, disk usage (%):

- Notify, Logging

}

FAU_ARP.1.1 The TSF shall take [{The following} list of the least disruptive actions] upon detection of a potential security violation.

{

a) Failed authentication audit events in FIA_UAU.1(1) ~ (3):

- Notify, Logging

b) Control rules violation events in FDP_IFF.1, FDP_ACF.1(1) ~ (2), FDP_IFF.1(1) ~ (4), FDP_IFF.1(6) ~ (8):

- Notify, Drop, Logging

c) Control rules violation events in FDP_IFF.1(5):

- Notify, Prevention, Quarantine, Session Drop, Logging

d) Integrity violation events in FPT_TST.1:

- Notify, Logging

e) Audit events reaching specified limit for capacity (%) and period (minutes) of auditable events on CPU, memory, disk usage (%):

- Notify, Logging

}

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and

c) [assignment: other specifically defined auditable events].

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events.

a) Start-up and shutdown of the audit functions

b) All auditable events for *not specified* level of audit

c) [assignment: "Auditable events" of Table 6-5 Auditable events]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the Security Target, [assignment: "other audit relevant information" of Table 6-5 Auditable events].

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation;

b) [assignment: any other rules].

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: failed audit events of defined auditable events in FIA_UAU.1, control rules violation events of defined auditable events in FDP_IFF.1, integrity violation audit events of defined auditable events in FPT_TST.1] known to indicate a potential security violation;

b) [assignment: any other rules {below}]

{

- Accumulation or combination of control rules violation events under defined auditable events in FDP_ACF.1
  - Audit events reaching specified limit for capacity (%) and period (minutes) of auditable events on CPU, memory, disk usage (%)

}

Table **6-5** ____ Auditable events

SFR	Auditable events	Other audit relevant information
FAU_ARP.1	Actions taken due to potential security violations	Identity of recipient of action
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms	-
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	-
FDP_IFF.1	Decisions to permit requested information flows.	Identification information of object
FIA_AFL.1	the reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	-
FIA_SOS.1	Rejection by the TSF of any tested secret	-
FIA_UAU.1	Unsuccessful use of the authentication mechanism	-

SFR	Auditable events	Other audit relevant information
FIA_UAU.4	Attempts to reuse authentication data	–
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	–
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	–
FMT_MSA.1	All modifications of the values of security attributes	Modified security attribute value
FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data
FMT_MTD.2	All modifications to the limits on TSF data	Modified TSF data limit
FMT_SMF.1	Use of the management functions	–
FMT_SMR.1	modifications to the group of users that are part of a role	–
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code when integrity is violated
FTA_SSL.1	Locking of an interactive session by the session locking mechanism.	–
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	–
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	Identification information of object
FRU_FLT.1	Any failure detected by the TSF	–
FRU_RSA.1	Rejection of allocation operation due to resource limits.	–

FAU_SAR.1 **Audit review**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: authorised users] with the capability to read [assignment: list of audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1.1 The TSF shall provide [assignment: authorised users] with the capability to read [assignment: all audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: methods of selection and/or ordering] of audit data based on [assignment: criteria with logical relations].

[

- Criteria with logical relations: Selection criteria based on Audit data types in **Table 6-6** Audit data types
  - Methods of selection and/or ordering: Descending order based on time of event according to Selection criteria based on audit data type in **Table 6-6** Audit data types

]

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: the following methods of selection and/or ordering] of audit data based on [assignment: the following criteria with logical relations].

[

- Criteria with logical relations: Selection criteria based on Audit data types in **Table 6-6** Audit data types
  - Methods of selection and/or ordering: Descending order based on time of event according to Selection criteria based on audit data type in **Table 6-6** Audit data types

]

[Ref.] The types of audit data include operation logs, firewall logs, IPS logs, quarantine logs, contents filter logs, website filtering logs, anti-virus logs and anti-spam logs.

Table **6–6** _____ Audit data types and criteria (search, sorting)

Audit data type	Selection criteria based on audit data type	Allowed ca-pacity
Operation logs	▪ Group/Device: Single selection of registered TOE (group, exclusive device) ∩ ▪ Search period: Single selection (Today, 1 week) ∪ ▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000,	Search, sort according to time

	50000) ∪ ▪ Specific period (Start date – end date) ∪ ▪ Content: Keyword to search	
Firewall log	▪ Group/Device: Single selection of registered TOE (group) ∩ ▪ Log type: Single selection (Allow, block, end) ∪ ▪ Search period: Single selection (Today, ※ specific period: start date – end date) ∪ ▪ Protocol: Single selection (All, TCP, UDP, ICMP, IGMP, ESP, AH, OSPF, VRRP, Others: Port no.) ∪ ▪ Source IP address ∪ ▪ Source port ∪ ▪ Destination IP address ∪ ▪ Destination port ∪ ▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000, 50000)	Search, sort according to time
IPS log	▪ Group/Device: Single selection of registered TOE (group) ∩ ▪ Search period: Single selection (Today, ※ specific period: start date– end date) ∪ ▪ Risk level: Single selection (All, critical, high, medium, low, N/A) ∪ ▪ Source IP address ∪ ▪ Source port ∪ ▪ Destination IP address ∪ ▪ Destination port ∪ ▪ Action: Single selection (All, block, quarantine, allow, replace, redirection, drop session, limit bandwidth, DDoS protection, unknown) ∪ ▪ Attack type ∪ ▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000, 50000)	Search, sort according to time
Quarantine log	Group/Device: Single selection of registered TOE (group) ∩ ▪ Search period: Single selection (Today, 1 week, ※ specific period: start date– end date) ∪ ▪ Action: Single selection (All, quarantine, release) ∪ ▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000, 50000) ∪ ▪ Source IP address ∪ ▪ Content	Search, sort according to time
Content filter log	▪ Group/Device: Single selection of registered TOE (group) ∩ ▪ Search period: Single selection (Today, ※ specific period: start date– end date) ∪ ▪ Log type: Single selection (All, error, operation log) ∪	Search, sort according to time

	▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000, 50000) ∪ ▪ Content	
Website filter log	▪ Group/Device: Single selection of registered TOE (group) ∩ ▪ Search period: Single selection (Today, ※ specific period: start date– end date) ∪ ▪ Action: Single selection (All, allow, block) ∪ ▪ Source IP address ∪ ▪ Source port ∪ ▪ Destination IP address ∪ ▪ Destination port∪ ▪ URL ∪ ▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000, 50000)	Search, sort according to time
Anti–virus log	Group/Device: Single selection of registered TOE (group) ∩ ▪ Log type: Single selection (Allow, block, end) ∪ ▪ Search period: Single selection (Today, ※ specific period: start date– end date) ∪ ▪ Action: Single selection (All, allow, block) ∪ ▪ Source IP address ∪ ▪ Source port ∪ ▪ Destination IP address ∪ ▪ Destination port∪ ▪ Description ▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000, 50000)	Search, sort according to time
Anti–spam log	▪ Group/Device: Single selection of registered TOE (group) ∩ ▪ Search period: Single selection (Today, ※ specific period: start date– end date) ∪ ▪ Action: Single selection (All, allow, block) ∪ ▪ Source IP address ∪ ▪ Source port ∪ ▪ Destination IP address ∪ ▪ Destination port∪ ▪ Sender ∪ ▪ Receiver ∪ ▪ Subject ∪ ▪ Max. search (no.): Single selection (1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000, 40000, 50000)	Search, sort according to time
(※ Note: ∩ means 'and' and ∪ means 'or')		

FAU_SEL.1 **Selective audit**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a) [selection: object identity, user identity, subject identity, host identity, event type]

b) [assignment: list of additional attributes that audit selectivity is based upon]

FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a) *Event type*

b) [N/A]

FAU_STG.1 **Protected audit trail storage**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: prevent, detect] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.1.2 The TSF shall be able prevent unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 **Action in case of possible audit data loss**

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].

{

a) Backup audit trails in saved location or delete oldest audit trails first

}

FAU_STG.3.1 The TSF shall [take {the following} actions in case of possible audit storage failure] if the audit trail exceeds [the pre-defined limit (total audit trail storage capacity – space (%) ※ Default space: 10%].

{

a) Backup audit trails in saved location or delete oldest audit trails first

}

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: "ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

{

a) Notify authorized user with following method to take restore audit record storage

- Send mail to email address specified by the authorized administrator

}

FAU_STG.4.1 The TSF shall *prevent audited events, except those taken by the authorised user with special rights* and [{the following} other actions to be taken in case of audit storage failure] if the audit trail is full.

{

a) Notify authorized user with following method to take restore audit record storage

- Send mail to email address specified by the authorized administrator

}

6.1.2 User data protection

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

[

a) Subject: User sending/receiving information through the TOE

b) Information: Network traffic passing the TOE

]

FDP_IFC.2.1 The TSF shall enforce the [Packet Filtering SFP] on [the following list of subjects and information] and all operations that cause the information to flow to and from subjects covered by the SFP.

[

a) Subject: User sending/receiving information through the TOE

b) Information: Network traffic passing the TOE

]

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes
   - IP address

b) Information security attributes
   - Source IP address
   - Destination IP address
   - Protocol (service)
   - Time

]

[Ref.] Packet Filtering SFP is based on priority, and the first rule (the top-most rule) among those specified by the authorized administrator shall be applied.

FDP_IFF.1.1 The TSF shall enforce the [Packet Filtering SFP] based on the following types of subject and information security attributes: [the following list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes
   - IP address

b) Information security attributes
   - Source IP address
   - Destination IP address
   - Protocol (service)
   - Time

]

[Ref.] Packet Filtering SFP is based on priority, and the first rule (the top-most rule) among those specified by the authorized administrator shall be applied.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

a) According to the information flow control security policies, the traffic sent from a subject through the TOE shall
   - compare the information security attributes ((Source IP address, Destination IP address, protocol (service), time) requested by the subject (IP address) to send and the information flow control security policy attributes defined by the authorized user, and if the action on the information flow is 'allowed', the requested information flow must be allowed.

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each following operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

a) According to the information flow control security policies, the traffic sent from a subject through the TOE shall

- compare the information security attributes ((Source IP address, Destination IP address, protocol (service), time) requested by the subject (IP address) to send and the information flow control security policy attributes defined by the authorized user, and if the action on the information flow is 'allowed', the requested information flow must be allowed.

]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

[

The TOE shall block request for information from the IT entity of the external network with the entity IP address of the internal network.

b) The TOE shall block request for information from the IT entity of the internal network with the entity IP address of the external network.

c) The TOE shall block request for information from the IT entity of the external network with the broadcasing entity IP address.

d) The TOE shall block request for information from the IT entity of the external network with looping entity IP address.

e) The TOE shall block request for information from the IT entity of the external network with abnormal packet structure.

]

FDP_IFF1.5 The TSF shall explicitly deny an information flow based on the following rules: [rules, based on security attributes, that explicitly deny information flows].

[

a) The TOE shall block request for information from the IT entity of the external network with the entity IP address of the internal network.

b) The TOE shall block request for information from the IT entity of the internal network with the entity IP address of the external network.

c) The TOE shall block request for information from the IT entity of the external network with the broadcasing entity IP address.

d) The TOE shall block request for information from the IT entity of the external network with looping entity IP address.

e) The TOE shall block request for information from the IT entity of the external network with abnormal packet structure.

]

6.1.3 Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

[

a) Unsuccessful authentication attempt after the last successful authentication when attempting to access the the following TOE security management interface

- Web User Interface (HTTPS): 10 times
- Command Line Interface (SSH): 10 times
- AhnLab LogServer (Win32 application): Administrator configurable positive integer (Default: 6 times, Range: 1 - 99)

b) Unsuccessful authentication attempt after the last successful authentication requesting following serviec in which user authentication is forced in FDP_IFC.1(1), FDP_IFF.1(1) Application Filtering SFP

- (General TCP) Proxy: Administrator configurable positive integer (Default: N/A, Range: 1 - 9)
- FTP Proxy: Administrator configurable positive integer (Default: N/A, Range: 1 - 9)
- HTTP Proxy: Administrator configurable positive integer (Default: N/A, Range: 1 - 9)

]

[Ref.] The SFR stated in AhnLab LogServer under part a) of FIA_AFL.1.1 의 is provided based on LogViewer.

FIA_AFL.1.1 The TSF shall detect when [*the following [positive integer number], an administrator configurable positive integer within [range of acceptable values]*] unsuccessful authentication attempts occur related to [list of authentication events].

[

a) Unsuccessful authentication attempt after the last successful authentication when attempting to access the the following TOE security management interface
   - Web User Interface (HTTPS): 10 times
   - Command Line Interface (SSH): 10 times
   - AhnLab LogServer (Win32 application): Administrator configurable positive integer (Default: 6 times, Range: 1 - 99)

b) Unsuccessful authentication attempt after the last successful authentication requesting following serviec in which user authentication is forced in FDP_IFC.1(1), FDP_IFF.1(1) Application Filtering SFP
   - (General TCP) Proxy: Administrator configurable positive integer (Default: N/A, Range: 1 - 9)
   - FTP Proxy: Administrator configurable positive integer (Default: N/A, Range: 1 - 9)
   - HTTP Proxy: Administrator configurable positive integer (Default: N/A, Range: 1 - 9)

]

[Ref.] The SFR stated in AhnLab LogServer under part a) of FIA_AFL.1.1 is provided based on LogViewer.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].

{

a) When the defined number of unsuccessful authentication attempts has been surpassed when attempting to access the TOE security management interface
   - Web User Interface (HTTPS): Authentication of user prevented until the authorized administrator takes action after getting notified via email
   - Command Line Interface (SSH): Authentication of user prevented until the authorized administrator takes action after getting notified via email
   - AhnLab LogServer (Win32 application): Authentication of user delayed (default: 10 minutes) until the time specified by the authorized administrator

b) When the defined number of unsuccessful authentication attempts has been surpassed when requesting service that forces user authentication in the next FDP_IFC.1(1), FDP_IFF.1(1) Application Filtering SFP
   - (General TCP) Proxy: Authentication of user prevented until the authorized administrator takes action

- FTP Proxy: Authentication of user prevented until the authorized administrator takes action
- HTTP Proxy: Authentication of user prevented until the authorized administrator takes action

}

[Ref.] The SFR stated in AhnLab LogServer under part a) of FIA_AFL.1.1 is provided based on LogViewer.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [prevent user authentication until the authorized administrator takes action, {the following} list of actions].

{

a) When the defined number of unsuccessful authentication attempts has been surpassed when attempting to access the TOE security management interface
   - Web User Interface (HTTPS): Authentication of user prevented until the authorized administrator takes action after getting notified via email
   - Command Line Interface (SSH): Authentication of user prevented until the authorized administrator takes action after getting notified via email
   - AhnLab LogServer (Win32 application): Authentication of user delayed (default: 10 minutes) until the time specified by the authorized administrator

b) When the defined number of unsuccessful authentication attempts has been surpassed when requesting service that forces user authentication in the next FDP_IFC.1(1), FDP_IFF.1(1) Application Filtering SFP
   - (General TCP) Proxy: Authentication of user prevented until the authorized administrator takes action
   - FTP Proxy: Authentication of user prevented until the authorized administrator takes action
   - HTTP Proxy: Authentication of user prevented until the authorized administrator takes action

}

[Ref.] The SFR stated in AhnLab LogServer under part a) of FIA_AFL.1.2 is provided based on LogViewer.

FIA_ATD.1(1) User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[assignment: list of security attributes].

[

a) Identifier

b) Secret (password)

c) Access permission

d) Lock status

]

[Ref.] This SFR is user attributes used to identify administrators (super administrator, administrator) to manage through interaction with the TOE. Through this, the TOE identifies allowed admnistrators and then request for identification. The administrators include super administrator and administrator identified by the UTM daemon package. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual authorized administrators: [the following list of security attributes].

[

a) Identifier

b) Secret (password)

c) Access permission

d) Lock status

]

[Ref.] This SFR is user attributes used to identify administrators (super administrator, administrator) to manage through interaction with the TOE. Through this, the TOE identifies allowed admnistrators and then request for identification. The administrators include super administrator and administrator identified by the UTM daemon package. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_ATD.1(2) User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

[

a) ID

b) Secret (password)

c) User authentication server

d) Authentication method

e) Security level

f) Login retry limit

g) Password validity

h) Expiry date

i) Lock

]

[Ref.] This SFR is user attributes used to identify users (who are force-authenticated) sending/receiving information through the TOE. Through this, the TOE identifies allowed admnistrators and then request for identification.

- User authentication server: A TOE self-authentication module or server (RADIUS) in the TOE operating environment can be used according to the rules specified by the authorized administrator.
- Authentication method: Selectively used according to rules specified by by the authorized administrator: password or one-time password.
- Security level: Critical, medium or low

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **authorized users:** [the following list of security attributes].

[

a) ID

b) Secret (password)

c) User authentication server

d) Authentication method

e) Security level

f) Login retry limit

g) Password validity

h) Expiry date

i) Lock

]

[Ref.] This SFR is user attributes used to identify users (who are force-authenticated) sending/receiving information through the TOE. Through this, the TOE identifies allowed admnistrators and then request for identification.

- User authentication server: A TOE self-authentication module or server (RADIUS) in the TOE operating environment can be used according to the rules specified by the authorized administrator.
- Authentication method: Selectively used according to rules specified by by the authorized administrator: password or one-time password.

- Security level: Critical, medium or low

FIA_ATD.1(3) **User attribute definition**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

[

a) Name

b) Type: Single, range or CIDR

c) IP address: ※ The following, according to selected type in b)

    - Single: IP address
    - Range: IP address range (Starting IP address - ending IP address)
    - CIDR: IP address, subnet mask

d) Network port

e) Security level

]

[Ref.] This SFR is user attributes used to identify unauthorized external user (IT entity) that is communicating with an internal computer to protect via the TOE. Through this, the TOE identifies the external IT entity, and audits and records the security events of the IT entitty to trace responsibility in the future.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual IT entities: [the following list of security attributes].

[

a) Name

b) Type: Single, range or CIDR

c) IP address: ※ The following, according to selected type in b)

    - Single: IP address
    - Range: IP address range (Starting IP address - ending IP address)
    - CIDR: IP address, subnet mask

d) Network port

e) Security level

]

[Ref.] This SFR is user attributes used to identify unauthorized external user (IT entity) that is communicating with an internal computer to protect via the TOE. Through this, the TOE identifies the external IT entity, and audits and records the security events of the IT entitty to trace responsibility in the future.

FIA_ATD.1(4) User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

[

a) Identifier

b) Secret (password)

c) Login retry limit: (Default: 6 times)

d) Lock time: (Default: 10 minutes)

e) Lock: On/Off

f) Name: Description of user

g) Permission: Manageable list of TOE (exclusive device)

]

[Ref.] This SFR is user attributes used to identify administrators (super log administrator, log administrator) to manage through interaction with the TOE. Through this, the TOE identifies allowed admnistrators and then request for identification. The administrators mean log administrators identified by the AhnLab LogServer. FIA_ATD.1.1 interacts with the TOE through LogViewer and/or LogReporteri and is forced to log administrators to manage. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **authorized log administrators**: [the following list of security attributes].

[

a) Identifier

b) Secret (password)

c) Login retry limit: (Default: 6 times)

d) Lock time: (Default: 10 minutes)

e) Lock: On/Off

f) Name: Description of user

g) Permission: Manageable list of TOE (exclusive device)

]

[Ref.] This SFR is user attributes used to identify administrators (super log administrator, log administrator) to manage through interaction with the TOE. Through this, the TOE identifies allowed admnistrators and then request for identification. The administrators mean log administrators identified by the AhnLab LogServer. FIA_ATD.1.1 is forced to log adminis-trators to manage by interacting with the TOE through LogViewer and/or LogReporter. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_SOS.1 **Verification of secrets**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].

[

a) Allowed characters
   - Alphabets upper/lower case (52 letters: a ~ z, A ~ Z), numbers (0 - 9), special characters (26 characters: special characters on keyboard, except $)

b) Combination rule
   - Words in dictionary not allowed
   - At least one alphabet or number required
   - More than five consecutive or reverse-consecutive letters or numbers not allowed (e.g.: abcd123, dcba123)
   - More than five consecutive letters or numbers not allowed (e.g.: 123xxx)

c) Min./Max. length
   - 6 - 15 characters (6 - 15 byte)

d) Reset interval (Password validity)
   - 0 - 9999days

]

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following defined quality metric].

[

a) Allowed characters
   - Alphabets upper/lower case (52 letters: a ~ z, A ~ Z), numbers (0 - 9), special characters (26 characters: special characters on keyboard, except $)

b) Combination rule
   - Words in dictionary not allowed
   - At least one alphabet or number required
   - More than five consecutive or reverse-consecutive letters or numbers not allowed (e.g.: abcd123, dcba123)
   - More than five consecutive letters or numbers not allowed (e.g.: 123xxx)

c) Min./Max. length

- 6 - 15 characters (6 - 15 byte)

d) Reset interval (Password validity)

- 0 - 9999days

]

FIA_UAU.1(1) Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

[

a) Security management mode access control SFP of FDP_ACC.2(1), FDP_ACF.1(1)

b) Identification and authentication process request (login window)

]

FIA_UAU.1.1 The TSF shall allow [the following list of TSF mediated actions] on behalf of the authorized administrator to be performed before the authorized administrator is authenticated.

[

a) Security management mode access control SFP of FDP_ACC.2(1), FDP_ACF.1(1)

b) Identification and authentication process request (login window)

]

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF–mediated actions on behalf of that user.

[Ref.] This SFR applies when authenticating identified administrators (super administrator administrator), but does not apply to identified IT entity. Administrators include super administrator administrator. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UAU.1.2 The TSF shall require each authorized administrator to be successfully authenticated before allowing any other TSF–mediated actions on behalf of that authorized administrator.

[Ref.] This SFR applies when authentication identified administrators (super administrator administrator), but not identified IT entity. Administrators include super administrator administrator. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UAU.1(2) Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

[

a) Application Filtering SFP of FDP_IFC.1(1), FDP_IFF.1(1)

b) Identification and authentication process request (login window)

]

FIA_UAU.1.1 The TSF shall allow [the following list of TSF mediated actions] on behalf of the **authorized administrator** to be performed before the **authorized administrator** is authenticated.

[

a) Application Filtering SFP of FDP_IFC.1(1), FDP_IFF.1(1)

b) Identification and authentication process request (login window)

]

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] This SFR applies when authenticating used of identified Application Filtering (Proxy) SFP, but does not apply to identified external IT entity.

FIA_UAU.1.2 The TSF shall require each **authorized administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **authorized administrator**, apart from actions in FIA_UAU.1.1.

[Ref.] This SFR applies when authenticating used of identified Application Filtering (Proxy) SFP, but does not apply to identified external IT entity.

FIA_UAU.1(3) Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

[

a) Identification and authentication process request (login window)

b) Connection settings

- (LogServer) server address, server port, search port, security transfer status
- Language (Korean), auto-logout (time (minutes), status)

]

FIA_UAU.1.1 The TSF shall allow [the following list of TSF mediated actions] on behalf of the **authorized log administrator** to be performed before the **authorized log administrator** is authenticated.

[

a) Identification and authentication process request (login window)

b) Connection settings

- (LogServer) server address, server port, search port, security transfer status
- Language (Korean), auto-logout (time (minutes), status)

]

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] This SFR is applied when authenticating log administrators (super log administrator, log administrator), but does not apply to identified IT entity. The administrators mean log administrators identified by the AhnLab LogServer. FIA_UAU.1.1 interacts with TOE through LogViewer and LogReporter and is forced to log administrators to manage. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UAU.1.2 The TSF shall require each **authorized log administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **authorized log administrator**, apart from actions in FIA_UAU.1.1.

[Ref.] This SFR is applied when authenticating log administrators (super log administrator, log administrator), but does not apply to identified IT entity. The administrators mean log administrators identified by the AhnLab LogServer. FIA_UAU.1.1 interacts with TOE through LogViewer and LogReporter and is forced to log administrators to manage. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)].

[

a) User authentication

]

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [the following: identified authentication mechanism(s)].

[

a) User authentication

]

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress.

[

a) When entering secret information (password), each character is changed to '*'

b) 'Cause of unsuccessful authentication mechanism' when authentication is unsuccessful

]

FIA_UAU.7.1 The TSF shall provide only [the following list of feedback] to the user while the authentication is in progress.

[

a) When entering secret information (password), each character is changed to '*'

b) 'Cause of unsuccessful authentication mechanism' when authentication is unsuccessful

]

FIA_UID.2(1) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requesting identification of authorized user (super administrator, administrator). The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UID.2.1 The TSF shall require each **authorized administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requesting identification of authorized user (super administrator, administrator). The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UID.2(2) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requesting identification of authorized user (super administrator, administrator). The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UID.2.1 The TSF shall require each **authorized user** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requesting identification of authorized user. The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UID.2(3) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requires identification of authorized user.

FIA_UID.2.1 The TSF shall require each **IT entity** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requires identification of authorized user.

FIA_UID.2(4) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requires identification of authorized log administrator (super log administrator, log administrator). The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

FIA_UID.2.1 The TSF shall require each authorized log administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[Ref.] The TOE user includes authorized administrator, authorized log administrator, authorized user, and IT entity. This SFR is for requires identification of authorized log administrator (super log administrator, log administrator). The details of TOE users can be found in 'FMT_SMR.1 Security Role'.

6.1.4 Security management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorised identified roles].

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of, disable, enable, modify the behaviour of* the functions [in the following list of functions in Table 6-7] to [the authorised administrator].

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

Table **6-7** _____ Security functions list and security function management ability

Security function	Ability			
	Determine behavior	Disable	Enable	Modify behav-ior
TOE reset	-	-	O	-
Identification and authentication	O	-	-	O
Backup and restore	-	-	O	-
Alarm notification	O	O	O	-
Audit data generation/transmission	O	O	O	O
Security audit data review	-	O	O	-
Firewall security policy (function)	O	O	O	O
Intrusion Prevention security policy (function)	O	O	O	O
Application Filter security policy (function)	O	O	O	O
QoS security policy (function)	O	O	O	O
Integrity check	-	-	O	-
Update function	O	O	O	-
HA (High Availiability) function	O	O	O	-
(※ Note: - Not supported, O Supported)				

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

[

a) Access control SFP

- Security management mode access control SFP

- Security label based access control SFP

b) Information flow control SFP

- Packet Filtering SFP
- Application Filtering SFP
- Network Address Translation (NAT) SFP
- White List SFP
- Anti-Spam SFP
- Intrusion Prevention SFP
- Traffic Control SFP
- Quarantine SFP
- Anti-Virus SFP

]

[Ref.] The 'authorized administrator' in this SFR means super administrator and administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'. A super administrator has all the abilities (change default, query, modify, delete, clear) included in this SFR, and an administrator only has query ability.

FMT_MSA.1.1 The TSF shall enforce the [following access control SFP(s), information flow control SFP(s)] to restrict the ability to *change default, query, modify, delete, clear* security attributes [in the following list of security attributes in Table 6-8] to [the authorised administrator].

[

a) Access control SFP

- Security management mode access control SFP
- Security label based access control SFP

b) Information flow control SFP

- Packet Filtering SFP
- Application Filtering SFP
- Network Address Translation (NAT) SFP
- White List SFP
- Anti-Spam SFP
- Intrusion Prevention SFP
- Traffic Control SFP
- Quarantine SFP
- Anti-Virus SFP

]

[Ref.] The 'authorized administrator' in this SFR means super administrator and administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'. A super administrator has all the abilities (change default, query, modify, delete, clear) included in this SFR, and an administrator only has query ability.

Table **6–8** _____ Security attribute list and management ability

Category	Security attribute		Ability				
			Change default	Query	Modify	De–lete	Clear
Packet Filter–ing SFP	Subject	IP address	O	O	O	O	O
	Infor–mation	Source IP address	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Protocol (service)	O	O	O	O	O
		Physical network port of TOE where network traffic passes	O	O	O	O	O
		Time	O	O	O	O	O
Security management mode access control SFP	Subject	IP address	–	O	O	O	–
	Object	IP address	–	O	O	–	O
		Service port	–	O	O	–	O
Security label based access control SFP	Subject	IP address	O	O	O	O	O
		Security label	–	O	O	O	O
	Object	IP address	O	O	O	O	O
		Security label	–	O	O	O	O
Application Filtering SFP	Subject	IP address	O	O	O	O	O
	Infor–mation	Source IP address	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Protocol	O	O	O	O	O
		Service port	O	O	O	O	O
		Packet data	–	–	–	–	–
		Time	O	O	O	O	O
Network Ad–dress Trans–lation (NAT) SFP	Subject	IP address	O	O	O	O	O
	Infor–mation	Source IP address	O	O	O	O	O
		Source (internal) port	–	O	O	O	O
		Destination IP address	O	O	O	O	O
		Destination (external) port	–	O	O	O	O
		Protocol	–	O	O	–	O

Category	Security attribute		Ability				
			Change default	Query	Modify	Delete	Clear
White List SFP	Subject	IP address	O	O	O	O	O
	Information	Source IP address	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Service port	O	O	O	O	O
Anti-Spam SFP	Subject	IP address	O	O	O	O	O
	Information	Source IP address	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Protocol (service)	O	O	O	O	O
		Packet data (payload)	O	O	O	O	O
Intrusion Prevention SFP	Subject	IP address	O	O	O	O	O
	Information	Source IP address	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Protocol (service)	O	O	O	O	O
		Packet data	O	O	O	O	O
		Time	O	O	O	O	O
Traffic Control SFP	Subject	IP address	O	O	O	O	O
	Information	Source IP address	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Protocol (service)	O	O	O	O	O
		Packet data	O	O	O	O	O
		Time	O	O	O	O	O
Quarantine SFP	Subject	IP address	O	O	O	O	O
	Information	Source IP address	O	O	O	O	O
		Service port	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Service port	O	O	O	O	O
Anti-Virus SFP	Subject	IP address	O	O	O	O	O
	Information	Source IP address	O	O	O	O	O
		Destination IP address	O	O	O	O	O
		Protocol (service)	O	O	O	O	O

Category	Security attribute		Ability				
			Change default	Query	Modify	De-lete	Clear
		Packet data	O	O	O	O	O
(※ Note: – Not supported, O Supported)							

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.1 The TSF shall enforce the [access control SFP, information flow control SFP in the following Table 6-9] to *restrictive*, default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MSA.3.2 The TSF shall allow the [authorised administrator] to specify alternative initial values to override the default values when an object or information is created.

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

Table **6-9** _____ Access control SFP and information flow control SFP

Category	Access control/information flow control SFP
Access control SFP	Security management mode access control SFP
	Security label based access control SFP
	Packet Filtering SFP
	Application Filtering SFP
	Network Address Translation (NAT) SFP

Category	Access control/information flow control SFP
	White List SFP:
	Anti-Spam SFP
	Intrusion Prevention SFP
	Traffic Control SFP
	Quarantine SFP
	Anti-Virus SFP

FMT_MTD.1(1) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MTD.1.1 The TSF shall restrict the ability to *change, delete* the [identification and authentication data] to [the authorised administrator].

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MTD.1(2) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].

[Ref.] The 'authorized administrator' in this SFR means super administrator and log administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify, delete, clear, [assignment: other opera-*

tions] the [audit data, list of TSF data {in the following Table 6-10}] to [the authorised administrator].

[Ref.] The 'authorized administrator' in this SFR means super administrator and log administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

Table **6–10** ____ TSF data list and management ability

TSF data	Ability					
	Change default	Query	Modify	Delete	Clear	Other operations
Audit data	–	–	–	–	–	Statistics, backup and restore in a semipermanent secondary memory device
Audit data backup settings (Scheduled backup, backup path, backup target, latest backup list)	–	O	O	–	–	–
Important TOE configuration files	–	O	O	–	–	Backup and restore in a semipermanent secondary memory device, roll back to initial settings
Integrity check data	–	O	O	–	–	–
Update settings (Auto update status, update interval)	–	O	O	–	–	–
Vulnerability list (Firewall rules)	–	O	O	–	O	Renew to latest data, (Create new vulnerability list and delete vulnerabilities created and added by authorized administrator only)
Options: Log settings (log type, log transmission method, log server)	–	O	O	–	O	Create and delete log server (IP address) to receive audit data
Settings for generating selective audit data	–	O	O	–	–	–
Configuration: TOE idetification (host) name	–	O	O	–	–	–
Configuration: Time	–	O	O	–	–	–
Configuration: Session drop settings (TCP, UDP, ICMP session time, TCP MSS	–	O	O	–	–	–

TSF data	Ability					
	Change default	Query	Modify	Delete	Clear	Other operations
status and size, TCP validity check status)						
Network information: Network port (name, status, type, physical port, IP address, control, MTU), router information	–	O	O	O	O	Create and delete (logical) network port list
HA settings information: onitoring port (physical port, local/remote device virtual IP, Ping status) list	–	O	O	–	–	Create and delete monitoring port list
HA settings information: HA settings (status, priority, connection NIC, remote device IP address, Heart beat state)	–	O	O	–	–	–
Profile list: IP address (name, type, IP address, network port, security level) and IP address group (name, network port, IP address object included in group) list	–	O	O	O	–	Create and delete IP address and IP address group list
Profile list: Service (name, protocol, source/destination port) and service group (name, object included in group) list	–	O	O	O	–	Create and delete service and service group list
Profile list: Schedule (name, interval, time) list	–	O	O	–	–	(Create and delete schedule list)
Profile list: QoS application (name, minimum and maximum bandwidth, priority) list	–	O	O	–	–	Create and delete QoS application list
Proxy service object list: Proxy name, Proxy type (Single selection from General Proxy, HTTP Proxy, FTP Proxy, SMTP Proxy, POP3 Proxy, Oracle Proxy, UDP Proxy, DNS Proxy), port, time limit, delivery host) and Proxy group (name, proxy	–	O	O	O	–	Create and delete proxy service object list

TSF data	Ability					
	Change default	Query	Modify	De-lete	Clear	Other operations
object included in group) list						
Advanced proxy rules settings (anti-virus status, website filtering status, anti-spam status, command block status, list of commands to block, DNS response test status, Status of private IP address block during DNS response)	-	O	O	-	-	-
Proxy authentication user list (user ID, Proxy type, connected IP address, connection time)	-	O	-	-	-	-
No. of simultaneous proxy connection (Specified General, HTTP, FTP, SMTP, POP3, Oracle, UDP, DNS Proxy)	-	O	O	-	-	-
Anti-virus settings (Mail message scan status, mail size, POP3 scan settings, SMTP scan settings, file extensions to filter list)	-	O	O	-	-	Create and delete file extension list
Anti-spam settings (Outgoing mail scan status, mail size, POP3 scan settings, SMTP scan settings, spam/allowed mail status and action list, RBL status and RBL Server list)	-	O	O	-	-	Create and delete spam/allowed mail status and action list, create and delete RBL Server list
Anti-spam settings: Keyword filtering list (group name, keyword, target, keyword type)	-	O	O	-	-	Create and delete keyword filtering list
Website filtering settings (Internet content rating DB status, content rating tag scan status and tags to filter, file attachment filtering status and action, blocked message and redirection URL, website configuration block	-	O	O	-	-	-

TSF data	Ability					
	Change default	Query	Modify	Delete	Clear	Other operations
settings)						
Website filtering settings: URL filtering list (group name, URL)	–	O	O	–	O	Create and delete website filtering list
Website filtering settings: URL filtering exceptions list (Status, target, Source/destination)	–	O	O	–	O	Create and delete URL filtering exceptions list
DDoS protection settings (profile time, network port (WAN), bandwidth block standard, web load attack block (enable/disable, HTTP port)	–	O	O	–	O	–
Connection information between physically separated TOE (Log Server and exclusive device)	–	O	O	O	–	–
Information on user logged in to the TOE	–	O	–	–	–	–
Information on log server to connect and connection settings, auto logout status	–	O	O	–	–	–
Alert mail settings (Spam mail list transmission status, list transmission time, mail address, alert method, recipient mail address, mail server information (IP address, port, ID, password)	–	O	O	–	–	–
Account settings (AhnLab LogServer) (ID, password, name, permission, login, login retry limit, lock period)	–	O	O	–	–	Create and delete user list
Information on TOE to manage (exclusive device) (TOE (exclusive device) name, IP address, firmware version, continuous usage time, state)	–	O	–	–	–	–
(※ Note: – Not supported, O Supported)						

FMT_MTD.1(3) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].

[Ref.] This SFR is forced (provided) to 'authorized users' to perform security related features of the TOE. The authorized user of the TOE can change his/her own password from the security attribute list in 'FIA_ATD.1(2) Definition of user attributes'. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MTD.1.1 The TSF shall restrict the ability to *change* the [authentication data (own secret (password) of authorized user] to [the authorized user].

[Ref.] This SFR is forced (provided) to 'authorized users' to perform security related features of the TOE. The authorized user of the TOE can change his/her own password from the security attribute list in 'FIA_ATD.1(2) Definition of user attributes'. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment: list of TSF data] to [assignment: the authorised identified roles].

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [aduit storage capacity, login retry limit, time interval for self test] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: actions to be taken]

[Ref.] The 'authorized administrator' in this SFR means super administrator and log administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits:

[actions to be taken stated in FAU_STG.3, FIA_AFL.1, self test stated in FPT_TST.1].

[Ref.] The 'authorized administrator' in this SFR means super administrator and log administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

[

a) Security feature list in FMT_MOF.1

b) Security feature list in FMT_MSA.1

c) Static attribute initialization list in FMT_MSA.3

d) TSF data management list in FMT_MTD.1(1) ~ (3), FMT_MTD.2

]

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [the following list of management functions to be provided by the TSF].

[

a) Security feature list in FMT_MOF.1

b) Security feature list in FMT_MSA.1

c) Static attribute initialization list in FMT_MSA.3

d) TSF data management list in FMT_MTD.1(1) ~ (3), FMT_MTD.2

]

FMT_SMR.1(1) Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles].

FMT_SMR.1.1 The TSF shall maintain the roles [the authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

[Ref.] The roles recognized by the TOE, in other words, the roles that can be taken by users regarding security are divided into four authorized administrator roles: super administrator,

administrator, super log administrator and log administrator, and authorized e user role. A super authorized administrator can only add an administrator or user. In the case of log administrator, there exists a separate TOE operating environment administrator. The details on each role can be found in [Security roles].

FMT_SMR.1.1 The TSF shall maintain the roles [the authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate authorized administrators and users with roles.

[Ref.] The roles recognized by the TOE, in other words, the roles that can be taken by users regarding security are divided into four authorized administrator roles: super administrator, administrator, super log administrator and log administrator, and authorized user role. A super authorized administrator can only add an administrator or user. In the case of log administrator, there exists a separate TOE operating environment administrator. The details on each role can be found in [Security roles].

Table 6-11 ____ Security roles (1)

Role		Description
Authorized admin-istrator	Super adminis-trato	Authorized administrator with all permissions (Read/Write)
	Administrato	Authorized administrator with permission to inquiry policies related to TOE management only (Read-Only permission)
	Super log ad-ministrato	Authorized administrator with all permissions of physically separated TOE (AhnLab LogServer)
	Log administrato	Authorized administrator with audit data inquiry permission in physically separated TOE (AhnLab LogServer)

FMT_SMR.1(2) Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles].

FMT_SMR.1.1 The TSF shall maintain the roles the authorized administrator.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

[Ref.] The roles recognized by the TOE are divided into authorized administrator and authorized user. In the case of log administrator, there exists a separate TOE operating environment administrator. The details on each role can be found in [Security roles]. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'. Only an authorized super administrator can add the authorized user. The roles of the authorized user is as below.

FMT_SMR.1.2 The TSF shall be able to associate users with authorized user roles.

[Ref.] The roles recognized by the TOE are divided into authorized administrator and authorized user. In the case of log administrator, there exists a separate TOE operating environment administrator. The details on each role can be found in [Security roles]. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'. Only an authorized super administrator can add the authorized user. The roles of the authorized user is as below.

Table **6–12** ____ Security roles (2)

Role	Description
Authorized user	As stated in 'FIA_UAU.1(2)', the authorized user is a user that has successfully completed the identification and authentication mechanism forced by the TSF. But, the authorized user can change his/her own password only.

6.1.5 Protection of the TSF

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]] to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF].

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the request of the authorised user, to demonstrate the correct operation of [the TSF, excluding TOE process management daemon].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF data].

FPT_TST.1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

FPT_TST.1.3 The TSF shall provide **authorized administrators** with the capability to verify the integrity of stored TSF executable code.

[Ref.] The 'authorized administrator' in this SFR means super administrator. The details of TOE users' roles can be found in 'FMT_SMR.1 Security Role'.

6.1.6 TOE access

FTA_SSL.1 TSF–initiated session locking

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: time interval of user inactivity] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.1 The TSF shall lock an interactive session of **authorized administrator** after [10 minutes of inactivity of authorized user] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the **authorized administrator**'s data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: events to occur].

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [reauthentication of administrator].

FTA_SSL.3 TSF–initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: time interval of user inactivity].

[Ref.] A 'user' stated in the SFR means a user that has not been forced 'user authentication' according to the TOE security policies (※ access control and information flow control rules).

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [time interval of user inactivity in the following Table 6-13].

Table **6–13** ____ User inactivity period

Category	Inactivity period
User	▪ User inactivity period specified by the authorized administrator ▪ UDP (Default: 30 sec.) ▪ ICMP (Default: 30 sec.) ▪ TCP (Default: 432000 sec.) ▪ User inactivity period specified by the authorized administrator by each service type in the advanced rules of information flow control policy of FDP_IFF.1(1) (Default: 120 sec.) ▪ Time limit specified in General TCP Proxy, SMTP Proxy, POP3 Proxy, FTP Proxy, HTTP Proxy, Oracle Proxy, UDP Proxy, DNS Proxy
Authorized user	▪ Authorized user inactivity period specified by the authorized administrator ▪ In the case session is formed based on 'user authentication' policy in information flow control policy of FDP_IFF.1(1) (Default: 30 min.)

[Ref.] A 'user' stated in the SFR means a user that has not been forced 'user authentication' according to the TOE security policies (※ access control and information flow control rules).

6.2 Security functional requirements (addition)

240 The security functional requirements in this section have been additionally defined in the Protection Profile on which this ST conforms. It is based on the functional components in Part 2 of the Common Criteria. The security functional requirements with operations that have not been completed in Part 2 of the Common Criteria have been completed by the author of this Security Target.

241 The functional components added to this ST are as the following Table 6-14.

Table 6-14 Security functional requirements (addition)

Security functional class	Security functional component	
User data protection	FDP_ACC.2(1) ~ (2)	Complete access control
	FDP_ACF.1(1) ~ (2)	Security attribute based access control
	FDP_IFC.1(1) ~ (10)	Subset information flow control
	FDP_IFF.1(1) ~ (10)	Simple security attributes
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_TEE.1	Testing of external entities
Resource utilisation	FRU_FLT.1	Degraded fault tolerance
	FRU_RSA.1	Maximum quotas

6.2.1 User data protection

FDP_ACC.2(1) Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

[

a) Subject: User sending/receiving information through the TOE

b) Object: TOE

]

FDP_ACC.2.1 The TSF shall enforce the [security management mode access control SFP] on [the following list of subjects and objects] and all operations among subjects and objects covered by the SFP.

[

a) Subject: User sending/receiving information through the TOE

b) Object: TOE

]

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

[Ref.] This SFR is required to govern access to the TOE security management interface by a user not authorized through an access control SFP on TOE security management interface.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

[Ref.] This SFR is required to govern access to the TOE security management interface by a user not authorized through an access control SFP on TOE security management interface.

FDP_ACF.1(1) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[

a) Subject secrity attribute: IP address

b) Object secrity attribute: IP address, service port

]

FDP_ACF.1.1 The TSF shall enforce the [security management mode access control SFP] to objects based on the following: [list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[

a) Subject secrity attribute: IP address

b) Object secrity attribute: IP address, service port

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[

a) According to the TOE security policy on the request by the subject to access the object:

- access of object by the subject shall be allowed only if access of object (IP address, service port) by security attribute (IP address) that has arrived from the subject is explicitly allowed.
- access of object by the subject shall be denied if access of object (IP address, service port) by security attribute (IP address) that has arrived from the subject is explicitly denied.

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[

a) According to the TOE security policy on the request by the subject to access the object:

- access of object by the subject shall be allowed only if access of object (IP address, service port) by security attribute (IP address) that has arrived from the subject is explicitly allowed.
- access of object by the subject shall be denied if access of object (IP address, service port) by security attribute (IP address) that has arrived from the subject is explicitly denied.

]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [N/A].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [N/A].

FDP_ACC.2(2) Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

[

a) Subject: User sending/receiving infromation through the TOE

b) Object: User sending/receiving infromation through the TOE

]

FDP_ACC.2.1 The TSF shall enforce the [security label based access control SFP] on [the following list of subjects and objects] and all operations among subjects and objects covered by the SFP.

[

a) Subject: User sending/receiving infromation through the TOE

b) Object: User sending/receiving infromation through the TOE

]

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1(2) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[

a) Subject secrity attribute: IP address, security label

b) Object secrity attribute: IP address, security label

]

[Ref.] The security label provided by the TOE is divided into high, medium and low level. 'High' level security label is higher than 'low' level security label.

FDP_ACF.1.1 The TSF shall enforce the [security label based access control SFP] to objects based on the following: [list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[

a) Subject secrity attribute: IP address, security label

b) Object secrity attribute: IP address, security label

]

[Ref.] The security label provided by th TOE is divided into high, medium and low level. 'High' level security label is higher than 'low' level security label.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[

a) According to the TOE security policy on the request by the subject to access the object:

- access from the subject to the object shall be allowed when after comparing the security labels of both the subject (IP address) and object (IP address), the security label of the subject is higher than or same as the security label of the object.
- access from the subject to the object shall be decined if the security label of the subject is lower than that of the object.

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[

a) According to the TOE security policy on the request by the subject to access the object:

- access from the subject to the object shall be allowed when after comparing the security labels of both the subject (IP address) and object (IP address), the security label of the subject is higher than or same as the security label of the object.
- access from the subject to the object shall be decined if the security label of the subject is lower than that of the object.

]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [N/A].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [N/A].

FDP_IFC.1(1) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFC.1.1 The TSF shall enforce the [Application Filtering SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFF.1(1) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address
- Protocol
- Service port
- Packet data
- Time

]

FDP_IFF.1.1 The TSF shall enforce the [Application Filtering SFP] based on the following types of subject and information security attributes: [list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address
- Protocol
- Service port
- Packet data
- Time

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute–based relationship that must hold between subject and information security attributes].

[

a) The TOE compares the information flow control security policy attributes defined by the authorized administrator with the security attributes (source IP address, destination IP address, protocol, service port, packet data, time) of the information requested by the subject (IP address) according to the information flow control security policy shallfrom the traffic from the subject, and

- if the action for the requested information flow is specified to 'allow', information flow shall be allowed (※ But, the following 'b)' must be enforced)
- if the action for the requested information flow is specified to 'authenticate',

information flow shall be allowed only when authentication is successful.

For the information flow allowed from 'a)' above, according to the information flow security policy, the TOE

- shall allow information flow by forcing the allow rules in the following Table 6-15 if the rules for the action to take on the requested information flow is additionally specified.

]

[Ref.] Authentication policy applies only if the service attributes (service port) conforms to the proxy defined by the authorized administrator.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

a) The TOE compares the information flow control security policy attributes defined by the authorized administrator with the security attributes (source IP address, destination IP address, protocol, service port, packet data, time) of the information requested by the subject (IP address) according to the information flow control security policy shallfrom the traffic from the subject, and

- if the action for the requested information flow is specified to 'allow', information flow shall be allowed (※ But, the following 'b)' must be enforced)
- if the action for the requested information flow is specified to 'authenticate', information flow shall be allowed only when authentication is successful.

For the information flow allowed from 'a)' above, according to the information flow security policy, the TOE

- shall allow information flow by forcing the allow rules in the following Table 6-15 if the rules for the action to take on the requested information flow is additionally specified.

]

[Ref.] Authentication policy applies only if the service attributes (service port) conforms to the proxy defined by the authorized administrator.

Table **6-15** ____ Allowed rules according to Application Filtering SFP rules

Category	Allowed rules
General TCP Proxy	The TOE shall allow the following in the information flow security policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'.

Category	Allowed rules
	▪ If a delivery host (Destination IP address, protocol, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host).
SMTP Proxy	The TOE shall allow the following in the information flow security policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'. ▪ If a delivery host (Destination IP address, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host). ▪ If mail relay block is specified, information flow (mail relay block) shall be allowed only if the internal mail service is the destination IP address. ▪ If Anti-Virus is specified, the information (packet data) shall be delivered from the requested information flow to the TOE operating environment Anti-Virus Engine. In other words, the TOE shall determine whether to allow information flow according to the result of delivering information to the Anti-Virus SFP stated in 'FDP_IFC.1(8), FDP_IFF.1(8)'. ▪ If Anti-Spam is specified, the information (packet data) shall be delivered to the Anti-Spam SFP. In other words, the TOE shall determine whether to allow information flow according to the result of delivering information to the Anti-Spam SFP stated in 'FDP_IFC.1(4), FDP_IFF.1(4)'. ▪ If 'Block Commands' is specified, information flow shall be allowed only if the command is not blocked (※ e.g. vrfy, debug, expn) in the requested information (packet data).
POP3 Proxy	The TOE shall allow the following in the information flow security policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'. ▪ If a delivery host (Destination IP address, protocol, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host). ▪ If Anti-Virus is specified, the information (packet data) shall be delivered from the requested information flow to the TOE operating environment Anti-Virus Engine. In other words, the TOE shall determine whether to allow information flow according to the result of delivering information to the Anti-Virus SFP stated in 'FDP_IFC.1(8), FDP_IFF.1(8)'. ▪ If Anti-Spam is specified, the information (packet data) shall be delivered to the Anti-Spam SFP. In other words, the TOE shall determine whether to allow information flow according to the result of delivering information to the Anti-Spam SFP stated in 'FDP_IFC.1(4), FDP_IFF.1(4)'.
FTP Proxy	The TOE shall allow the following in the information flow security

Category	Allowed rules
	policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'. ▪ If a delivery host (Destination IP address, protocol, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host). ▪ If Anti-Virus is specified, the information (packet data) shall be delivered from the requested information flow to the TOE operating environment Anti-Virus Engine. In other words, the TOE shall determine whether to allow information flow according to the result of delivering information to the Anti-Virus SFP stated in 'FDP_IFC.1(8), FDP_IFF.1(8)'. ▪ 'If 'Block Commands' is specified, information flow shall be allowed only if the command is not blocked (※ e.g. put, get, chmod, delete, mdelete, rename, rmdir, dir, ls) in the requested information (packet data).
HTTP Proxy	The TOE shall allow the following in the information flow security policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'. ▪ If a delivery host (Destination IP address, protocol, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host). ▪ If Anti-Virus is specified, the information (packet data) shall be delivered from the requested information flow to the TOE operating environment Anti-Virus Engine. In other words, the TOE shall determine whether to allow information flow according to the result of delivering information to the Anti-Virus SFP stated in 'FDP_IFC.1(8), FDP_IFF.1(8)'. ▪ If 'website filtering' is specified, the following rules shall be enforced for the requested information (packet data). ▪ If Internet content rating DB is specified, the Korea Internet Safety Commission DB of the TOE operating environment and requested information (packet data) are compared, and if it does not match the list, the information flow shall be allowed. ▪ If content rating tag filtering is specified, the content rating tag (PICS) and requested information (packet data) are compared, and if it does not match the list, the information flow shall be allowed. ▪ If file attachment filtering is specified and the file does not exceed the specified file size, the information flow shall be allowed. ▪ If ActiveX block, Applet block, Javascript block, VB script block, Textarea tag block are not specified, and if it does not match the tag specified by the authorized administrator, information flow (packet data, ※ e.g. website configuration) shall be allowed.

Category	Allowed rules
	▪ If URL filtering is specified, the registered URL list and requested information (packet data) are compared, and if it does not match the list, the information flow shall be allowed. Also, if it matches the filtering exceptions list, information flow shall be allowed.
Oracle Proxy	The TOE shall allow the following in the information flow security policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'. ▪ If a delivery host (Destination IP address, protocol, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host).
UDP Proxy	The TOE shall allow the following in the information flow security policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'. ▪ If a delivery host (Destination IP address, protocol, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host).
DNS Proxy	The TOE shall allow the following in the information flow security policy rules: ▪ If 'time limit' is specified, the information flow (session timeout) shall be allowed if there is request for information flow that does not exceed the specified 'session idle time'. ▪ If a delivery host (Destination IP address, protocol, service port) is specified, it shall be convertede to the specified delivery host to allow information flow (delivery host). ▪ If Check DNS response is specified, the information flow is allowed only if the DNS response from the requested information is not private IP address. ▪ If split DNS is specified, information flow shall be allowed for request to DNS response.

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

FDP_IFC.1(2) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFC.1.1 The TSF shall enforce the [Network Address Translation (NAT) SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFF.1(2) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes
   - IP address

b) Information security attributes
   - Source IP address, source (internal) port
   - Destination IP address, destination (external) port
   - Protocol

]

FDP_IFF.1.1 The TSF shall enforce the [Network Address Translation (NAT) SFP] based on the following types of subject and information security attributes: [list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address, source (internal) port
- Destination IP address, destination (external) port
- Protocol

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute–based relationship that must hold between subject and information security attributes].

[

The TOE compares the information flow control security policy attributes defined by the authorized administrator with the security attributes (Source IP address, source (internal) port, destination IP address, destination (external) port, protocol) of the information requested by the subject (IP address) according to the information flow control security policy shallfrom the traffic from the subject, and

- if address translation rules for the requested information flow is specified, it shall allow the requested information flow by translating the network address according to the source IP address based NAT in the information (requested from the IT entity of internal network) in following the Table 6-16〉 (SNAT).
  - Along with translated address, 1:1 port translation or M:N translation shall be enforced according to the rules specified by the authorized administrator .
- As a response to the allowed information flow, network address is converted according to the address conversion rules based on destination IP address of the information requested from the IT entity of the external network to allow information flow (DNAT).
  - Along with translated address, 1:1 port translation or M:N translation shall be enforced according to the rules specified by the authorized administrator .

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute–based relationship that must hold between subject and information security attributes].

[

a) The TOE compares the information flow control security policy attributes defined by the authorized administrator with the security attributes (Source IP address, source (internal) port, destination IP address, destination (external) port, protocol) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

- if address translation rules for the requested information flow is specified, it shall allow the requested information flow by translating the network address according to the source IP address based NAT in the information (requested from the IT entity of internal network) in following the **Table 6-16**〉 (SNAT).
    - Along with translated address, 1:1 port translation or M:N translation shall be enforced according to the rules specified by the authorized administrator .
- As a response to the allowed information flow, network address is converted according to the address conversion rules based on destination IP address of the information requested from the IT entity of the external network to allow information flow (DNAT).
    - Along with translated address, 1:1 port translation or M:N translation shall be enforced according to the rules specified by the authorized administrator .

]

Table **6–16** ____ Address translation rules of Network Address Translation(NAT) SFP

Category	Address translation rule
Dynamic NAT	▪ If the action for the information flow policy on the requested information is 'Dynamic NAT', M (more than one) internal network private IP addresses shall be enforced translation to N (more than one) public IP addresses. ▪ Along with translated address, 1:1 port translation or M:N translation shall be enforced according to the rules specified by the authorized administrator (Dynamic NAT(M:N)).
Static NAT	▪ If the action for the information flow policy on the requested information is 'Static NAT', an internal network private IP address shall be enforced translation to a public IP addresses. ▪ Along with translated address, 1:1 port translation or M:N translation shall be enforced according to the rules specified by the authorized administrator (Static NAT(1:1)).
Disable NAT	▪ If the action for the information flow policy on the requested information is 'Disable NAT', the above Dynamic NAT, Static NAT rules shall be disabled by force.

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

FDP_IFC.1(3) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFC.1.1 The TSF shall enforce the [White List SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFF.1(3) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address, service port

]

FDP_IFF.1.1 The TSF shall enforce the [White List SFP] based on the following types of subject and information security attributes: [the following list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address, service port

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute–based relationship that must hold between subject and information security attributes].

[

For the traffic sent from the subject (IP address) through the TOE, the TOE shall compare the information flow control security policy attributes defined by the authorized user and security attributes of the information requested by the subject (Source IP address, destination IP address/service port), according to the information flow control security policy, and

- allow the requested information flow if information flow is allowed for the subject and information security attributes.

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute–based relationship that must hold between subject and information security attributes].

[

a) For the traffic sent from the subject (IP address) through the TOE, the TOE shall compare the information flow control security policy attributes defined by the authorized user and security attributes of the information requested by the subject (Source IP address, destination IP address/service port), according to the information flow control security policy, and

- allow the requested information flow if information flow is allowed for the subject and information security attributes.

]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

FDP_IFC.1(4) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFC.1.1 The TSF shall enforce the [Anti-Spam SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

FDP_IFF.1(4) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address
- Protocol (service)
- Packet data (payload)

]

FDP_IFF.1.1 The TSF shall enforce the [Anti-Spam SFP] based on the following types of subject and information security attributes: [the following list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address
- Protocol (service)
- Packet data (payload)

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

a) The TOE compares the information flow control security policies (sender's IP address, sender's email address, recipient's email address) defined by the authorized administrator with the security attributes (Source IP address, destination IP address, protocol (service), packet data) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

  - if the action for the requested information flow is 'allowed mail, the information flow shall be allowed.
    - If 'Spam tagging' is specified, tag must be added to allow the information flow (POP3, SMTP).
  - If the action for the requested information flow is 'block', the information flow shall be allowed only if it does not match after comparing with the registered keyword filtering list (subject, message).
    - Even if it matches the keyword filtering list, and information flow is denied, 'Send a reject message' to the subject shall be allowed if 'Send a reject message' is specified (SMTP).
    - Even if the information flow is denied as it matches the keyword filtering list, 'Send a blocked e-mail list' to an IT entity shall be allowed if 'Send a blocked e-mail list' is specified (SMTP).

b) The TOE compares the information flow control security policies (RBL (Real-time Blackhole List) Server spam list) defined by the authorized administrator with the security attributes (Source IP address, destination IP address, protocol (service), packet data) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

    - if it matches, the information flow shall be allowed.

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

a) The TOE compares the information flow control security policies (sender's IP address, sender's email address, recipient's email address) defined by the authorized administrator with the security attributes (Source IP address, destination IP address, protocol (service), packet data) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

- if the action for the requested information flow is 'allowed mail, the information flow shall be allowed.
  - If 'Spam tagging' is specified, tag must be added to allow the information flow (POP3, SMTP).
- If the action for the requested information flow is 'block', the information flow shall be allowed only if it does not match after comparing with the registered keyword filtering list (subject, message).
  - Even if it matches the keyword filtering list, and information flow is denied, 'Send a reject message' to the subject shall be allowed if 'Send a reject message' is specified (SMTP).
  - Even if the information flow is denied as it matches the keyword filtering list, 'Send a blocked e–mail list' to an IT entity shall be allowed if 'Send a blocked e–mail list' is specified (SMTP).

b) The TOE compares the information flow control security policies (RBL (Real–time Blackhole List) Server spam list) defined by the authorized administrator with the security attributes (Source IP address, destination IP address, protocol (service), packet data) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

  - if it matches, the information flow shall be allowed.

]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

FDP_IFC.1(5) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] This security policy applies after Packet Filtering SFP. In other words, the TOE defines the rules for the service to allow after applying Packet Filtering SFP through this network traffic access control policy to allow access, and blocks the rest.

FDP_IFC.1.1 The TSF shall enforce the [Intrusion Prevention SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] This security policy applies after Packet Filtering SFP. In other words, the TOE defines the rules for the service to allow after applying Packet Filtering SFP through this network traffic access control policy to allow access, and blocks the rest.

FDP_IFF.1(5) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

FDP_IFF.1.1 The TSF shall enforce the [Intrusion Prevention SFP] based on the following types of subject and information security attributes: [the following list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address
- Protocol (service)
- Packet data
- Time

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

The TOE compares the vulnerabilities list data (signature) with the security attributes (Source IP address, destination IP address, protocol, packet data, time) of the information requested by the subject according to the information flow control security policy from the traffic from the subject, and

- shall allow the requested information flow if it does not matches.
- shall allow the requested information flow if it matches, and the action is specified to ‘allow’.
- shall allow the requested information flow to the Traffic Control SFP in FDP_IFC.1(6), FDP_IFF.1(6) if it matches, and the action is specified to ‘limit bandwidth’.
- shall allow the requested information flow to the Quarantine SFP in 'FDP_IFC.1(7), FDP_IFF.1(7) if it matches, and the action is specified to ‘quarantine’.
- shall allow the requested information flow if it matches, and the action is specified to ‘exceptions’.

]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

FDP_IFC.1(6) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] Traffic Control SFP is applied as Packet Filtering SFP, Intrusion Prevention SFP action rules only when specified by the authorized administrator.

FDP_IFC.1.1 The TSF shall enforce the [Traffic Control SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] Traffic Control SFP is applied as Packet Filtering SFP, Intrusion Prevention SFP action rules only when specified by the authorized administrator.

FDP_IFF.1(6) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address
- Protocol (service)
- Packet data
- Time

]

FDP_IFF.1.1 The TSF shall enforce the [Traffic Control SFP] based on the following types of subject and information security attributes: [list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address
- Destination IP address
- Protocol (service)
- Packet data
- Time

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

The TOE compares the information flow control security policies attributes defined by the authorized administrator with the security attributes (Source IP address, destination IP address, protocol (service), packet data, time) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

- if the maximum threshold for information flow is specified, only information flow that does not exceed the threshold shall be allowed (maximum bandwidth).

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute–based relationship that must hold between subject and information security attributes].

[

a) The TOE compares the information flow control security policies attributes defined by the authorized administrator with the security attributes (Source IP address, destination IP address, protocol (service), packet data, time) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

- if the maximum threshold for information flow is specified, only information flow that does not exceed the threshold shall be allowed (maximum bandwidth).

]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

FDP_IFC.1(7) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] The quarantine list used in this SFP is generated/registered when quarantine is specified as the action for information flow in Intrusion Prevention SFP.

FDP_IFC.1.1 The TSF shall enforce the [Quarantine SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] The quarantine list used in this SFP is generated/registered when quarantine is specified as the action for information flow in Intrusion Prevention SFP.

FDP_IFF.1(7) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address/service port
- Destination IP address/service port

]

FDP_IFF.1.1 The TSF shall enforce the [Quarantine SFP] based on the following types of subject and information security attributes: [the following list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes

- IP address

b) Information security attributes

- Source IP address/service port
- Destination IP address/service port

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

The TOE compares the quarantine list (IP address) with the security attributes (Source IP address, service port) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

- if it does not matches, the requested information flow shall be allowed.

b) If the authorized administrator specify 'auto release time' as a security attribute of the information flow control policy for the subject (IP address) registered in the quarantine list, the TOE shall delete it from the quarantine list after the specified time and allow information flow.

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

a) The TOE compares the quarantine list (IP address) with the security attributes (Source IP address, service port) of the information requested by the subject (IP address) according to the information flow control security policy from the traffic from the subject, and

- if it does not matches, the requested information flow shall be allowed.

b) If the authorized administrator specify 'auto release time' as a security attribute of the information flow control policy for the subject (IP address) registered in the quarantine list, the TOE shall delete it from the quarantine list after the specified time and allow information flow.

]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A]

FDP_IFC.1(8) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] The TOE uses Anti-Virus Engine (V3 Engine) provided by the TOE operating environment to detect viruses. Anti-Virus Engine shall be excluded from evaluation. This SFP is selectively applied according to the action specified by the authorized administrator according to the TOE security policy in POP3, SMTP, HTTP, FTP Proxy of the Application Filtering SFP.

FDP_IFC.1.1 The TSF shall enforce the [Anti-Virus SFP] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) Subject: User sending/receiving information through the TOE

b) Information: Traffic sent from subject through the TOE

c) Operation: Pass/Deny when there is allowed rules

]

[Ref.] The TOE uses Anti-Virus Engine (V3 Engine) provided by the TOE operating environment to detect viruses. Anti-Virus Engine shall be excluded from evaluation. This SFP is selectively applied according to the action specified by the authorized administrator according to the TOE security policy in POP3, SMTP, HTTP, FTP Proxy of the Application Filtering SFP.

FDP_IFF.1(8) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes
   - IP address

b) Information security attributes
   - Source IP address
   - Destination IP address
   - Protocol (service)
   - Packet data (payload)

]

FDP_IFF.1.1 The TSF shall enforce the [Anti-Virus SFP] based on the following types of subject and information security attributes: [the following list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

[

a) Subject security attributes
   - IP address

b) Information security attributes
   - Source IP address
   - Destination IP address
   - Protocol (service)
   - Packet data (payload)

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

[

For the traffic sent from the subject (IP address) through the TOE, the TOE shall do the following according to the information flow control

- The TSF shall allow the requested information flow only when virus scan result show that the packet data has not been infected, based on the information security attributes (Source IP address, destination IP address, protocol, packet data), through the anti–virus engine of the TOE operating environment called by the TOE.

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute–based relationship that must hold between subject and information security attributes].

[

a) For the traffic sent from the subject (IP address) through the TOE, the TOE shall do the following according to the information flow control

- The TSF shall allow the requested information flow only when virus scan result show that the packet data has not been infected, based on the information security attributes (Source IP address, destination IP address, protocol, packet data), through the anti–virus engine of the TOE operating environment called by the TOE.

]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.3 The TSF shall enforce the [N/A].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

6.2.2 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF].

[

a) Software error

- Error in other daemon, except TOE process management daemon
- Operation error of physically separated TOE (AhnLab LogServer)

b) Hardware error

- Error in some TOE when multiple TOEs are managed

]

[Ref.] The TOE process management daemon checks the state of other daemons of TOE, excluding itself, and restores it to be safe, if an error occurs. The TOE process management daemon maintains safe status through the TOE operating environment (OS).

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [the following list of types of failures in the TSF].

[

a) Software error

- Error in other daemon, except TOE process management daemon
- Operation error of physically separated TOE (AhnLab LogServer)

b) Hardware error

- Error in some TOE when multiple TOEs are managed

]

[Ref.] The TOE process management daemon checks the state of other daemons of TOE, excluding itself, and restores it to be safe, if an error occurs. The TOE process management daemon maintains safe status through the TOE operating environment (OS).

FPT_ITT.1 Basic protection of internal transmission TSF data

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_ITT.1.1 The TSF shall protect the TSF data from *exposure* when it gets sent from parts separated from the TOE.

[Ref.] The TOE is implemented separately as TOE (exclusive device) that physically performs firewall and intrusion prevention and security audit exclusive management program (AhnLab LogServer). This SFR implements safe internal channel when sending TSF data to prevent TSF data exposure between the AhnLab LogServer and TOE (exclusive device) sent through the network. Safe internal channel is provided through TSF data encryption (SEED) during communication between the TOE (exclusive device) and AhnLab LogServer.

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]] to check the fulfillment of [assignment: list of properties of the external entities] .

a) Attributes list of external entity

- DBMS that interoperates with the TOE: IP address, service port

]

FPT_TEE.1.1 The TSF shall run a suite of tests during *initial start-up, periodically during normal operation* to check the fulfillment of [the following list of properties of the external entities].

[

a) Attributes list of external entity

- DBMS that interoperates with the TOE: IP address, service port

]

FPT_TEE.1.2 If the test fails, the TSF shall [assignment: action(s)] .

[

a) When DBMS test fails,

- a warning window will be displayed for the authorized administrator to restore.

]

FPT_TEE.1.2 If the test fails, the TSF shall take the [following action].

[

a) When DBMS test fails,

- a warning window will be displayed for the authorized administrator to restore.

]

6.2.3 Resource utilisation

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

[Ref.] This function is to assure utilization of network service for users even in the case an error occurs in the TOE.

FRU_FLT.1.1 The TSF shall ensure the operation of [assignment: list of TOE capabilities] when the following failures occur: [assignment: list of type of failures].

FRU_FLT.1.1 The TSF shall ensure the operation of [the following list of TOE capabilities in Table 6-17] when the following failures occur: [the following list of type of failures in Table 6-17].

Table 6–17 ____ Type of failure and TOE capacibilty

Type of failure		TOE capability
Software error	▪ Other daemon error that performs TSF, except TOE process management daemon	▪ The TOE shall process management daemon that regularly checks the state of other daemons that perform TSF, and when an abnormality is detected, it shall reset the daemon to manage the TSF that is provided.
	▪ Operation error of physically separated TOE (AhnLab LogServer)	▪ Even when operational error occurs caused by the TOE operating environment where the TOE (AhLab LogServer) is managed, all TSF provided through the TOE (exclusive device) shall be managed.
Hardware error	▪ Error in some TOE when multiple TOEs are managed	▪ If the authorized administrator manages multiple TOEs and an error occurs in some TOEs, all TSF from the other TOEs shall be managed.

[Ref.] This function is to assure utilization of network service for users even in the case an error occurs in the TOE.

FRU_RSA.1 Maximum quotas

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment: controlled resources] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time].

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [SYN packet connection of TCP] *that individual user, defined group of users* can use *simultaneously*.

6.3 Security assurance requirements

242 The security assurance requirements of this Security Target are based on the assurance components defined in Part 3 of the Common Criteria. The assurance requirements are assurance level EAL4. The following Table 6-18 shows the augmented assurance components.

Table **6-18** ____ Assurance requirements

Assurance Class	Assurance components
Security Target evaluation	ASE_INT.1 ST introduction
	ASE_ECD.1 Extended components definition
	ASE_CCL.1 Conformance claims
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6.3.1 Security Target

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package–conformant or package–augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.3.2 Development

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_IMP.1 Implementation representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design
ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

ADV_TDS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.3.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.3.4 Life-cycle support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies: ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

Content and presentation elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5 Tests

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.2 Testing: security enforcing modules

Dependencies: ADV_ARC.1 Security architecture description
ADV_TDS.3 Basic modular design
ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR–enforcing modules in the TOE design.

ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR–enforcing modules in the TOE design have been tested.

Evaluator action elements:

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing – sample

Dependencies: ADV_FSP.2 Security–enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.3.6 Vulnerability assessment

AVA_VAN.3 Focused vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.3.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6.4 Security requirements rationale

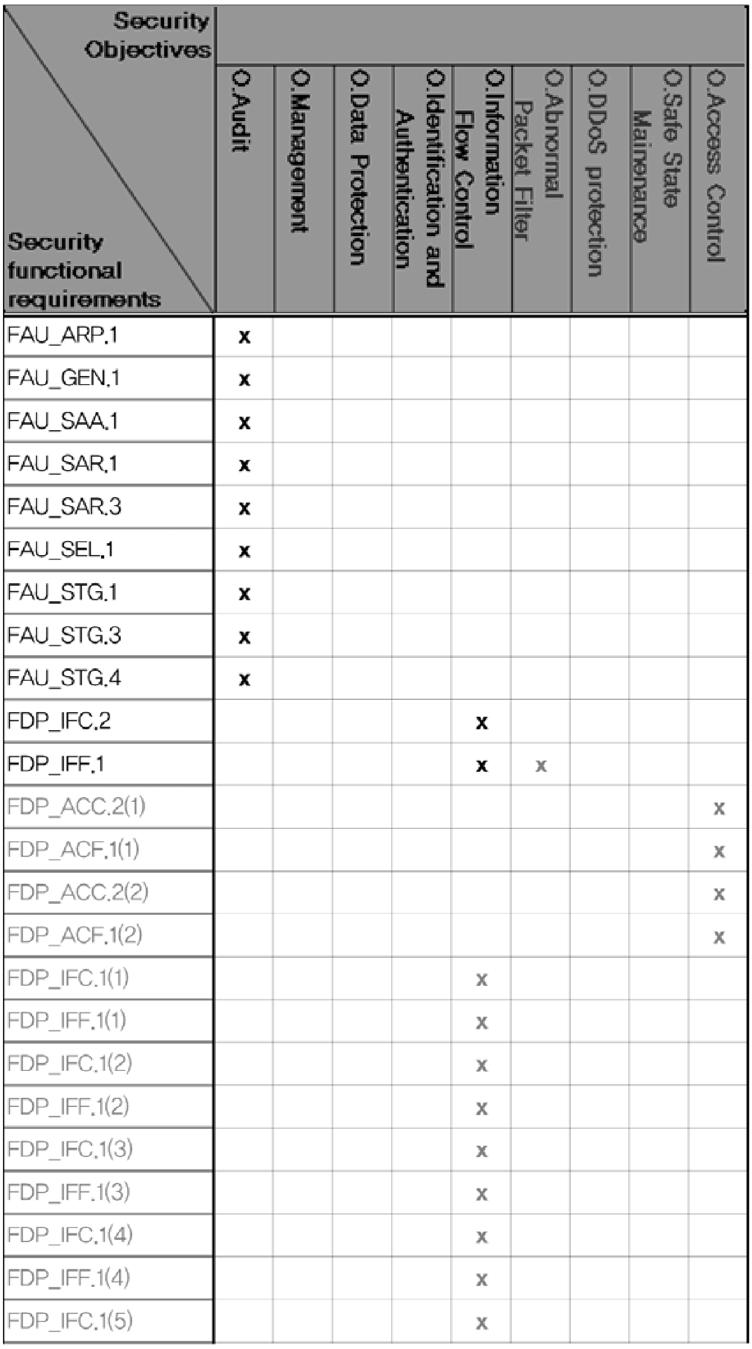
243 The security requirements must satisfy the security objectives, and as a result, verify that it is appropriate for dealing with security problems.

6.4.1 Security requirements rationale

244 The security requirements rationale shall verify the following:

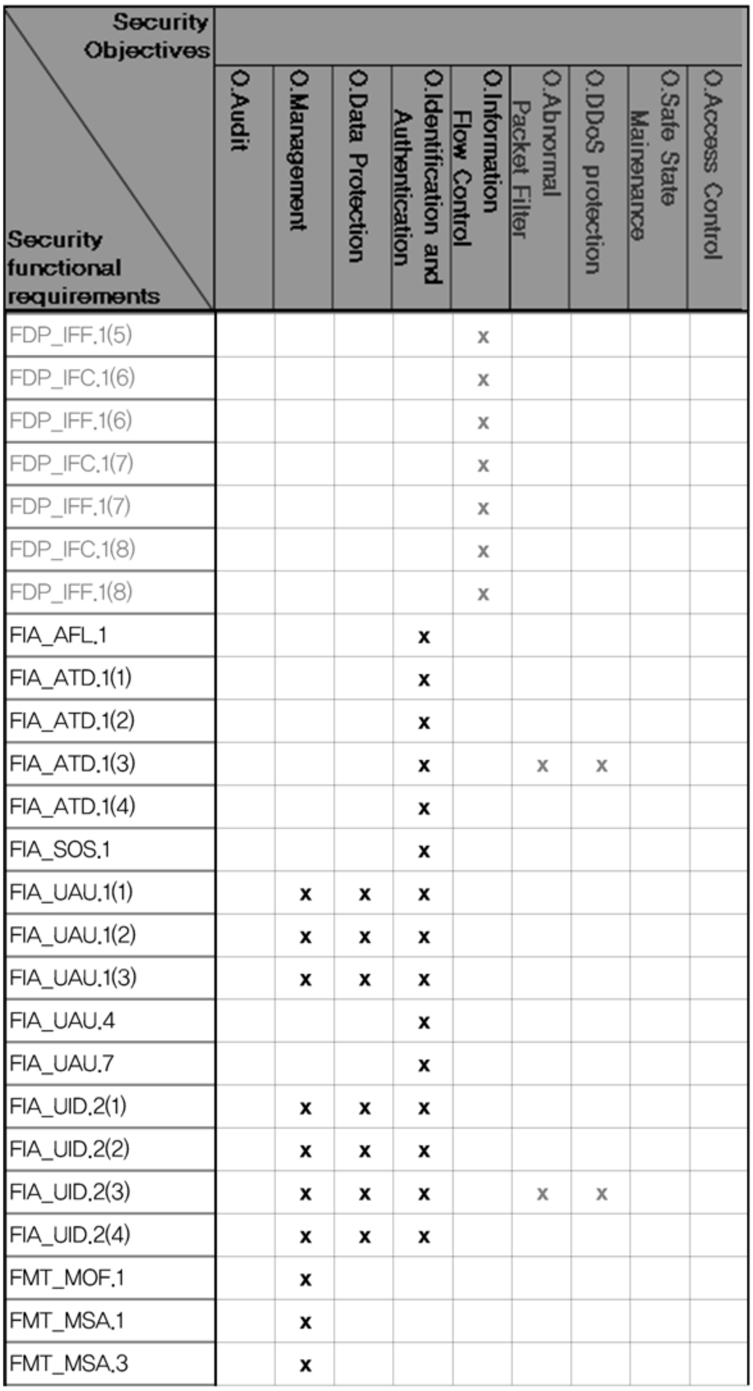
- Each security objective is addresses based on at least one security requirement.
- Each security requreiment addresses at least one security objective.

Table **6–19** ____ Security objectives and security functional requirements



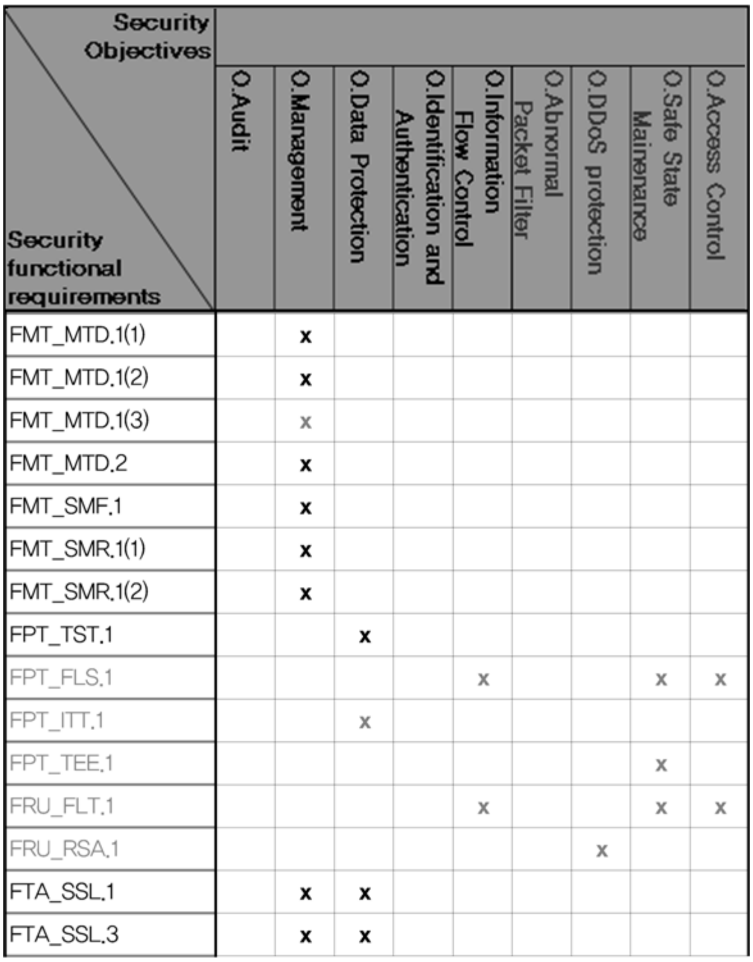
Security Objectives / Security functional requirements	O.Audit	O.Management	O.Data Protection	O.Identification and Authentication	O.Information Flow Control	O.Abnormal Packet Filter	O.DDoS protection	O.Safe State Mainenance	O.Access Control
FAU_ARP.1	x								
FAU_GEN.1	x								
FAU_SAA.1	x								
FAU_SAR.1	x								
FAU_SAR.3	x								
FAU_SEL.1	x								
FAU_STG.1	x								
FAU_STG.3	x								
FAU_STG.4	x								
FDP_IFC.2					x				
FDP_IFF.1					x	x			
FDP_ACC.2(1)									x
FDP_ACF.1(1)									x
FDP_ACC.2(2)									x
FDP_ACF.1(2)									x
FDP_IFC.1(1)					x				
FDP_IFF.1(1)					x				
FDP_IFC.1(2)					x				
FDP_IFF.1(2)					x				
FDP_IFC.1(3)					x				
FDP_IFF.1(3)					x				
FDP_IFC.1(4)					x				
FDP_IFF.1(4)					x				
FDP_IFC.1(5)					x				

Table **6–20** ____ Security objectives and security functional requirements (continued)



Security Objectives / Security functional requirements	O.Audit	O.Management	O.Data Protection	O.Identification and Authentication	O.Information Flow Control	O.Abnormal Packet Filter	O.DDoS protection	O.Safe State Mainenance	O.Access Control
FDP_IFF.1(5)					x				
FDP_IFC.1(6)					x				
FDP_IFF.1(6)					x				
FDP_IFC.1(7)					x				
FDP_IFF.1(7)					x				
FDP_IFC.1(8)					x				
FDP_IFF.1(8)					x				
FIA_AFL.1				x					
FIA_ATD.1(1)				x					
FIA_ATD.1(2)				x					
FIA_ATD.1(3)				x		x	x		
FIA_ATD.1(4)				x					
FIA_SOS.1				x					
FIA_UAU.1(1)		x	x	x					
FIA_UAU.1(2)		x	x	x					
FIA_UAU.1(3)		x	x	x					
FIA_UAU.4				x					
FIA_UAU.7				x					
FIA_UID.2(1)		x	x	x					
FIA_UID.2(2)		x	x	x					
FIA_UID.2(3)		x	x	x		x	x		
FIA_UID.2(4)		x	x	x					
FMT_MOF.1		x							
FMT_MSA.1		x							
FMT_MSA.3		x							

Table **6–21** ____ Security objectives and security functional requirements (continued)



Security Objectives / Security functional requirements	O.Audit	O.Management	O.Data Protection	O.Identification and Authentication	O.Information Flow Control	O.Abnormal Packet Filter	O.DDoS protection	O.Safe State Mainenance	O.Access Control
FMT_MTD.1(1)		x							
FMT_MTD.1(2)		x							
FMT_MTD.1(3)		x							
FMT_MTD.2		x							
FMT_SMF.1		x							
FMT_SMR.1(1)		x							
FMT_SMR.1(2)		x							
FPT_TST.1			x						
FPT_FLS.1					x			x	x
FPT_ITT.1			x						
FPT_TEE.1								x	
FRU_FLT.1					x			x	x
FRU_RSA.1							x		
FTA_SSL.1		x	x						
FTA_SSL.3		x	x						

FAU_ARP.1 Security alarms

245 This component assures action against detected security violattion, so it satisfies the TOE security objective O.Audit.

FAU_GEN.1 Audit data generation

246 This component defines auditable events and assures generation of audit record, so it satisfies the TOE security objective O.Audit.

FAU_SAA.1 Potential violation analysis

247 This component assures detection of security violation by checking audited events, so it satisfies the TOE security objective O.Audit.

FAU_SAR.1 Audit review

248 This component assures the ability of an authorized administrator to review audit records, so it satisfies the TOE security objective O.Audit.

FAU_SAR.3 Selectable audit review

249 This component assures ability to search and sort audit data based on logical relation, so it satisfies the TOE security objective O.Audit.

FAU_SEL.1 Selective audit

250 This component assures the ability to include or exclude auditable events based on attributes, so it satisfies the TOE security objective O.Audit.

FAU_STG.1 Audit trace storage protection

251 This component assures the ability to protect audit records from unauthorized modification and deletion, so it satisfies the TOE security objective O.Audit.

FAU_STG.3 Action againts audit data loss prediction

252 This component assures action taken when the audit data exceeds the defined limit, so it satisfies the TOE security objective O.Audit.

FAU_STG.4 Audit data loss prevention

253 This component assures action taken when the audit storage is full, so it satisfies the TOE security objective O.Audit.

FDP_IFC.2 Complete information flow control

254 This component assures definition of security policy scope and security policy for TOE ifnormation control, so it satisfies the TOE security objective O.Information flow control.

FDP_IFF.1 Single layer security attribute

255 This component provides rules to control information flow based on security attributes, so it satisfies the TOE security objective O.Information flow control. In addition, FDP_IFF.1 includes action against explicit attacks, so it satisfies O.Abnormal packet filter.

FIA_AFL.1 Failed authentication

256 This component defines the allowed number of failed login attempts, and assures ability of taking action when the number has been reached or exceeded, so it satisfies the TOE security objective O.Identification and authentication.

FIA_ATD.1(1) ~ (4) User attribute definition

257 This component defines security attribute list for each user. FIA_ATD.1(1) defines the security attributes of the administrator (exclusive device: super administrator, administrator) to manage by interacting with the TOE by accessing the TOE; FIA_ATD.1(2) defines the security attributes of the user (ID and password based) sending/receiving information through the TOE; FIA_ATD.1(3) defines the security attributes of the user (IP address based) sending/receiving information through the TOE; and FIA_ATD.1(4) defines the security attributes of log administrator (Log Server: super log administrator, log administrator) to manage by interacting with the TOE by accessing the TOE. So, they satisfy the TOE security objective O.Identification and authentication. In addition, FIA_ATD.1(3) requires the identifier for the IT entity to identify with the computer IP address. IP address identifies IT entity to generate audit record and is the basis to determine whether the address is disguised, and also to determine DDoS for information flow control, so it satisfies the TOE security objective O.Abnormal packet filter and O.DoS protection.

FIA_SOS.1 Verification of secret

258 This component provides a mechanism that verifies whether the secret satisfies the defined allowed criteria, so it satisfies the TOE security objective O.Identification and authentication.

FIA_UAU.1(1) ~ (3) Authentication

259 This component assures the ability to successfully authentication users. FIA_UAU.1(1) assures the ability to successfully authenticate the administrator (exclusive device) to manage by interacting with the TOE by accessing the TOE; FIA_UAU.1(2) assures the

ability to successfully authenticate users who have been forced to be authenticated by the authorized administrator in Application Filtering SFP of FDP_IFF.1(1); and FIA_UAU.1(3) assures the ability to successfully authenticate administrator (Log Server) to manage by interacting with the TOE by accessing the TOE. So, it satisfies the TOE security objective O.Management, O.Data protection, O.Identification and authentication.

FIA_UAU.4 Replay attack prevention authentication mechanism

260 This component assures the ability to prevent reuse to authentication data, so it satisfies the TOE security objective O.Identification and authentication.

FIA_UAU.7 Authentication feedback protection

261 This component assures provision of only authentication feedback that has been specified to the user during authentication, so it satisfies the TOE security objective O.Identification and authentication.

FIA_UID.2(1) ~ (4) User identification before all behaviors

262 This component assures the ability to successfully identity users. In other words, FIA_UID.2(1) assures the ability to successful identify authorized administrator to manage by interacting with the TOE by accessing the TOE; FIA_UID.2(2) assures the ability to successful identify authorized user (ID and password based) sending/receiving information through the TOE; FIA_UID.2(3) assures the ability to successful identify the user (IP entity, IP address based) sending/receiving information through the TOE; and FIA_UID.1(4) assures the ability to successful identify authorized log administrator to manage by interacting with the TOE by accessing the TOE. Accordingly, they satisfy the TOE security objective O.Management, O.Data protection, O.Identification and authentication. In addition, the IP address identified in FIA_UID.2(3) identifies the IT entity and generates audit record to determine whether the address is disguised, and also determines DoS for information flow control, so it satisfies the TOE security objective O.Abnormal packet filter and O.DDoS protection.

FMT_MOF.1 Security functional management

263 This component assures the ability for the authorized administrator to manage security functions, so it satisfies the TOE security objective O.Management.

FMT_MSA.1 Security attribute management

264 This component assures the authorized administrator to manage the security attributes applied in the access control, information flow control policy, so it satisfies the TOE

security objective O.Management.

FMT_MSA.3 Static attribute initialization

265 This component provides intial value of security attributes applied to the access control, information flow control policy, so it satisfies the TOE security objective O.Management.

FMT_MTD.1(1) TSF data management

266 This component provides the ability for the authorized administrator to manage identification and authentication data, so it satisfies the TOE security objective O.Management.

FMT_MTD.1(2) TSF data management

267 This component provides the ability for the authorized administrator to manage audit data and TSF data (important TOE configuration files, time, vulnerability list, ※ Refer to Table 6-10 for TSF data list), so it satisfies the TOE security objective O.Management.

FMT_MTD.1(3) TSF data management

268 This component provides the ability for user to manage his/her own authentication data, so it satisfies the TOE security objective O.Management.

FMT_MTD.2 TSF data threshold management

269 This component assures the authorized administrator to manage TSF data threshold and action when it reaches or exceeds the specified limit, so it satisfies the TOE security objective O.Management.

FMT_SMF.1 Management functions

270 This component requires stating of management functions, such as security functions, security attributes and TSF data, so it satisfies the TOE security objective O.Management.

FMT_SMR.1(1) ~ (2) Security roles

271 This component assures association of each user role. In other words, it assures association of authorized administrator role with the FMT_SMR.1(1) user, and authorized user role with the FMT_SMR.1(2) user, so it satisfies the TOE security objective O.Management.

FPT_TST.1 TSF self test

272 This component assures self test for accurate management of TSF, and assures the

authorized administrator to verify the TSF data and TSF execution code integrity, so it satisfies the TOE security objective O.Data protection.

FTA_SSL.1 Session lock based on TSF

273 This component requires events before the authorized administrator locks the interactive session after the inactivity time and unlocks it, so it satisfies the TOE security objective O.Management, O.Data protection.

FTA_SSL.3 End session based on TSF

274 This component terminates interactive session after the user inactivity time, so it satisfies the TOE security objective O.Management, O.Data protection.

FDP_ACC.2(1) ~ (2) Complete access control

275 This component defines the security policies for TOE accses control and assures definition of security policy scope, so it satisfies the TOE security objective O.Access control.

FDP_ACF.1(1) ~ (2) Access control based on security attributes

276 This component provides rules to control access based on security attributes, so it satisfies the TOE security objective O.Access control.

FDP_IFC.1(1) ~ (8) Partial information flow control

277 This component defines the security policies for TOE information flow control assures definition of security policy scope, so it satisfies the TOE security objective O.Information flow control.

FDP_IFF.1(1) ~ (8) Single layer security attributes

278 This component provides rules to control information flow based on security attributes, so it satisfies the TOE security objective O.Information flow control.

FPT_FLS.1 Maintenance of safe state during error

279 This component assures safe state to operate core security functions (e.g. process management daemon, terminal daemon (CLI) log transmission daemon, security management interface processing daemon, LCD (LCD of exclusive device), security management daemon) including information flow control and access control when the TOE breaks down, and assures performance of core security functions including information flow control and access control of the TOE when multiple TOEs are managed and a few breaks down, so it satisfies the TOE security objective O.Information flow

control. O.Safe state maintenance, O.Access control.

FPT_ITT.1 Basic protection of internally transmitted TSF data

280 This component provides TSF data encryption to protect TSF data from exposure when transmitting TSF data between separated parts of the TOE, so it satisfies the TOE security objective O.Data protection.

FPT_TEE.1 Test of external entity that interoperates with the TOE

281 This component performs a series of tests for accurate management of TOE external entity, so it satisfies the TOE security objective O.Safe state maintenance.

FRU_FLT.1 Resistance towards error: partial application

282 This component requires core security functions (e.g. process management daemon, terminal daemon (CLI) log transmission daemon, security management interface processing daemon, LCD (LCD of exclusive device), security management daemon) including information flow control and access control when the TOE breaks down, and assures performance of core security functions including information flow control and access control of the TOE when multiple TOEs are managed and a few breaks down, so it satisfies the TOE security objective O.Information flow control. O.Safe state maintenance, O.Access control.

FRU_RSA.1 Maximum quota

283 This component requires function that limits the resource usage (SYN packet of TCP) for TOE protection asset by each defined user group and individual user based on the security policy defined by the authorized administrator to block DoS attack, so it satisfies the TOE security objective O.DDoS protection.

6.4.2 Assurance requirements rationale

284 The assurance level of this security target is EAL4.

- This Security Target conforms to the Firewall Protection Profile with assurance level of EAL4. (※ Please refer to 2.2 PP Claims.)

285 EAL4 is an assurance package that requires methodical design, test and review. It permits a developer to gain maximum assurance from practical security engineering based on good commercial development practices. Good commercial development practices do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

286 EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security–specific engineering costs.

287 EAL4 provides assurance by analyzing the SFR included in a complete ST, using the expressions of implementation on parts of TSF, basic module design description of TOE, description and functional and complete interface statement. Based on TSF independent test, functional statement and TOE design, this analysis supports the analysis of vulnerabilities that verifies the tests conducted by the developer, independence of the test result and sample, and resistence of attack by attacker with possibility to succeed in reinforced attacks (based on provided functional statement, TOE design, expression of implementation, description of security structure, guide).

6.5 Dependency rationale

6.5.1 Dependency of security functional requirements

288 The following Table 6-22 shows the dependency of function components.

289 FDP_IFF.1 is dependent to FDP_IFC.1, and this is satisfied based on FDP_IFC.2 that has a hierarchical relation with FDP_IFC.1.

290 FIA_UAU.1, FMT_SMR.1 is dependent to FIA_UID.1, and this is satisfied based on FIA_UID.2 that has a hierarchical relation with FIA_UID.1.

291 FMT_MSA.1 is dependent to FDP_ACC.1 or FDP_IFC.1, and this is satisfied based on FDP_IFC.2 that has a hierarchical relation with FDP_IFC.1.

292 FAU_GEN.1 is dependent to FPT_STM.1, but the TOE accurately records security related events using trustable timestamp provided by the TOE operating environment, so the dependency of FAU_GEN.1 is satisfied based on operating environment security objective OE.Timestamp instead of FPT_STM.1.

293 FDP_ACF.1 is dependent to FDP_ACC.1, and this is satisfied based on FDP_ACC.2 that has a hierarchical relation with FDP_ACC.1.

6.5.2 Dependency of assurance requirements

294 The dependency of each assurance package provided by the CC is already satisfied.

Table **6–22** ___ Functional component dependancy

No.	Functional component	Dependancy	Note
1	FAU_ARP.1	FAU_SAA.1	
2	FAU_GEN.1	FPT_STM.1	OE. Timestamp
3	FAU_SAA.1	FAU_GEN.1	
4	FAU_SAR.1	FAU_GEN.1	
5	FAU_SAR.3	FAU_SAR.1	
6	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	
7	FAU_STG.1	FAU_GEN.1	
8	FAU_STG.3	FAU_STG.1	
9	FAU_STG.4	FAU_STG.1	
10	FDP_IFC.2	FDP_IFF.1	
11	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	
12	FIA_AFL.1	FIA_UAU.1	
13	FIA_ATD.1	–	
14	FIA_SOS.1	–	
15	FIA_UAU.1	FIA_UID.1	
16	FIA_UAU.4	–	
17	FIA_UAU.7	FIA_UAU.1	
18	FIA_UID.2	–	
19	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	
20	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1, FMT_SMR.1	
21	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	
22	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	
23	FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	
24	FMT_SMF.1	–	
25	FMT_SMR.1	FIA_UID.1	
26	FPT_TST.1	–	
27	FTA_SSL.1	FIA_UAU.1	
28	FTA_SSL.3	–	
29	FDP_ACC.2	FDP_ACF.1	
30	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	
31	FDP_IFC.1	FDP_IFF.1	
32	FPT_FLS.1	–	
33	FPT_ITT.1	–	

No.	Functional component	Dependancy	Note
34	FPT_TEE.1	–	
35	FRU_FLT.1	FPT_FLS.1	
36	FRU_RSA.1	–	

7 TOE summary specification

295 This chapter describes the security functions of TOE that satisfy the SFR.

7.1 TOE security functionality

296 TOE security functionalities include: [Security audit, User data protection, Identification and authentication, Security management, Security audit data management/review, TSF protection, TOE access]. This chapter describes the method of TOE satisfying the [Security functional requirements] above.

7.1.1 Security audit

297 The TOE uses a trustable timestamp provided by the TOE operating environment at the event occurrence time to assure sequential generation of audit. The TOE operating environment (OS) periodically compares the value saved in the Real-time Clock (RTC) on which the TOE is operated, and provides the value as timestamp value. Also, the TOE can automatically synchronize the time with the NTP Server specified by the authorized administrator.

298 All the logs from TOE operation (e.g. operation log, packet filtering log, IPS log, contents filter log) are saved storage allotted for audit data storage. In addition, they are sent to the physically separated TOE (AhnLab LogSever, or 'Log Server'), which is connected remotely. The Log Server saves the received logs in the DB file system (MS-SQL), and provides search, statistics and management functions. The details on the TOE security audit review and management functions are described in [Security audit data management/review].

7.1.1.1 Security alarm, audit data generation, potential violation analysis

Security alarm

FAU_ARP.1 When an event is determined by the [Potential violation analysis] to violate security, the TOE generates audit data on this event, and warns the authorized administrator through the real-time event window of the security management interface, and records the audit data.

Audit data generation

FAU_GEN.1 The TOE saves audit data during operation.

Potential violation analysis

FAU_SAA.1 When a potential security violating event is detected, the TOE notifies the authorized administrator in real–time, and take the specified action according to the event type. The TOE provides the function to specify individual action for each security violation detectable event through the security management interface.

7.1.1.2 Audit review

FAU_SAR.1, FAU_SAR.3

The TOE provides the function to distinguish and review all audit data of the TOE by event type. The TOE manages the audit data through the file system (DBMS) of the TOE operating environment. When requested by the authorized administrator, it reads file from the TOE operating environment and provides it in a form that can be interpreted by the authorized administrator. The details on the TOE [Audit review] function are described in [Security audit data management/review].

7.1.1.3 Selective audit data generation, audit evidence protection, audit data loss prevention

Selective audit data generation

FAU_SEL.1

The TOE enables the authorized administrator to determine whether to generate audit data selectively from all auditable events according to the audit type. Also, it provides the function to determine whether to generate audit data by individual auditable event (advanced rules of the security policy).

Audit evidence protection

FAU_STG.1

The TOE uses the TOE operating environment storage (RAM and CF memory for exclusive device, and hard disk for Log Server) as the audit evidence storage. It saves audit evidence (DB) based on the file system provided by the TOE operating environment. It only allows the authorized administrator to access the audit record of the audit evidence (DB) saved in the Operating Environment. Accordingly, the TOE protects the TOE audit record from unauthorized deletion or modification.

Audit data loss action and prevention

FAU_STG.3, FMT_MTD.2

The TOE provides audit data loss action and prevention function. The authorized administrator can specify the capacity of the audit evidence storage based on [total capacity of audit evidence storage – space specified by authorized administrator (%)].

FAU_STG.4

When the space of the audit evidence storage reaches the specified limit, the TOE sends an alarm to the email address specified by the authorized administrator or displays the alarm on a popup window.

FMT_MTD.1(2)

The TOE automatically backs up the audit data at every specified interval just in case of audit data loss.

7.1.2 User data protection

299 To protect the user data, the TOE performs [Packet Filtering, Application Filter, Network Address Translation, System White List, Anti-Virus, Anti-Spam, Signature-based Intrusion Prevention, Algorithm-based Intrusion Prevention, Traffic Control, Quarantine] functions.

300 Logically, the TOE performs information flow control on the incoming network traffic based on the [System White List]. And then, it controls the information flow based on [Application Filter], [Network Address Translation], [Packet Filtering], and [Quarantine]. After that, it controls the information flow based on [Anti-Virus, Anti-Spam, Signature-based Intrusion Prevention, Algorithm-based Intrusion Prevention, Traffic Control] according to the interoperable rules specified by the authorized administrator. For reference, [Quarantine] list is generated as a result of the information flow control based on the [Signature-based Intrusion Prevention, Algorithm-based Intrusion Prevention] according to the rules specified by the authorized administrator.

7.1.2.1 Firewall

301 The TOE protects the internal network resources from Internet users through the firewall. It also blocks access to resources hidden from the external Internet, and controls the resources of the external network to which an internal user has to connect. The TOE [Packet Filtering], [Application Filter], [Network Address Translation], [System White List] are described below.

7.1.2.1.1 Packet Filtering

FDP_IFC.2, FDP_IFF.1

When there is network traffic from the external network to the internal network, the TOE performs [Packet Filtering] information flow control based on the source IP address, destination IP address, protocol (service), and time security attributes. In other words, the TOE compares the source IP address, destination IP address, protocol (service) and time that are security attributes of network traffic information with the information flow control security policy attributes specified by the authorized administrator, and controls the information flow and access according to the 'Action' specified in the first rule.

FDP_ACC.2(2), FDP_ACF.1(2)

If the authorized administrator specifies access control policy with 'security level' for the user (IT entity) that will be accessed and the user (IT entity) that attempts to access from the internal/external network, the following action will be taked based on the P address of each IT entity and security label. The security label provided by th TOE is divided into high, medium and low level. 'High' level security label is higher than 'low' level security label.

FDP_ACC.2(1), FDP_ACF.1(1)

The TOE addresses the request to access the security management interface provided by the TOE itself of the user (IT entity) that tries to access from the internal or external nework based on the IP address of the IT entity that attempts access.

7.1.2.1.2 Application Filter

FDP_IFC.1(1), FDP_IFF.1(1)

The TOE controls [Application Filter] information flow if there is network traffic from the internal or external network based on the source IP address, destination IP address, protocol (service), service port, packet data, and time security attributes. The TOE Application Filter mediates between the Internet and user if there is request for network (application layer). When there is request for network service (application layer) by the user, instead of directly connecting the client with the server, it mediates communication between the client and the server for itself (TOE) and the client, and the server and itself (TOE).

The TOE [Application Filter] rules is formed of source IP address, destination IP address, proxy type, action, and schedule. The details on [Application Filter] policy management provided by the authorized administrator are described in [Profile (object) management], [Contents filter policy management].

The TOE provides application filter (proxy) information flow control according to the security policy specified by the authorized administrator on services, such as General TCP, FTP, SMTP, POP3, HTTP, Oracle, UDP and DNS. In other words, the TOE provides functions such as delivery host, session timeout, anti-virus, anti-spam, relay block, block command, check DNS response and check split DNS for the [Application Filter].

7.1.2.1.3 Network Address Translation

FDP_IFC.1(2), FDP_IFF.1(2)

The TOE controls [Network Address Translation] information flow if there is network traffic from the internal or external network based on the source IP address, source port (internal) destination IP address, destination port (external) and protocol security attributes. The TOE provides the following functions: Source NAT (SNAT) that changes the source address, Destination NAT (DNAT) that changes the destination address, redirection that changes the destination address to the TOE's address itself, and Masquerade that applies SNAT for dynamic IP address such as PPP/DHCP.

The NAT feature of TOE changes the private IP address to public IP address- the TOE allots a public IP address for external user from private IP address to access from an external public network, or specifies a public IP address for the internal server. Accordingly, when there is not enough IP addresses of the internal network, the IP addresses can be added by using the private IP address through the TOE. Also, as the internal IP address is not disclosed, the network will be safe from external attacks

7.1.2.1.4 System White List

FDP_IFC.1(3), FDP_IFF.1(3)

When network traffic enters through the internal or external network, the TOE controls information flow based on [System White List] based on source IP address, destination IP address/service port security attributes. The TOE allows information flow only when the network traffic completely matches the exceptions registered in the [System White List] through the security management interface by the authorized administrator. The TOE [System White List] is formed of service, source IP address and destination IP address. The details on adding, modifying and deleting exceptions in the [System White List] are described in [Exceptions management]. For reference, in the user data protection function of the TOE, information flow control based on [System White List] has the highest priority.

7.1.2.2 Contents Filter

302 The TOE safely protects the network by detecting and preventing malicious codes by interoperating with the [Anti-Virus] engine of the TOE operating environment, as well as provide [Anti-Spam] function.

7.1.2.2.1 Anti-Virus

FDP_IFC.1(8), FDP_IFF.1(8)

The TOE controls [Network Address Translation] information flow if there is network traffic from the internal or external network based on the source IP address, destination IP address, protocol (service), packet data (payload) security attributes. It TOE provides anti-virus features by interoperating with the [Application Filter]. The types of proxy include SMTP Proxy, HTTP Proxy, POP3 Proxy and FTP Proxy.

7.1.2.2.2 Anti-Spam

FDP_IFC.1(4), FDP_IFF.1(4)

The TOE controls [Anti-Spam] information flow if there is network traffic from the internal or external network based on the source IP address, destination IP address, protocol (service), packet data (payload) security attributes. It checks the packet data (payload) of the traffic on whether the keyword specified by the authorized user is included in the mail and whether it matches the source IP address or email address of the sender, and receiver's email address, and applies the specified information flow control accordingly. The TOE blocks spam mail beforehand by comparing it to the website that sends spam mail in bulk, in other words the URLs registered in the RBL (Real-time Blackhole List). In other words, when spam mail or phishing mail is detected, it maintains the black list that is based on sender's IP address or email address, and blocks any mail from the sender in the list. The TOE provides [Anti-Spam] function by interoperating with [Application Filter], and proxies that provide [Anti-Spam] function are SMTP Proxy and POP3 Proxy. In the case of SMTP Proxy, is the authorized administrator specified to block the control rules, the blocked mail list is sent to the IT entity (Log Server) specified by the authorized administrator, or a reject message is sent to the sender. If the authorized administrator specified the control rules as 'allow', the tag specified by the authorized administrator shall be added to the mail subject and sent. In the case of POP3 Proxy, the tag specified by the authorized administrator shall be added to the mail subject and sent. The authorized administrator can disable/enable [Anti-Spam], and specify/manage the advanced attributes of the rules.

7.1.2.3 Intrusion Prevention

303 The TOE detects and blocks harmful traffic from the Internet network to the internal network to protect the information and resouces of the internal network. With this, the TOE provides [Signature-based Intrusion Prevention, and Algorithm-based Intrusion Prevention].

7.1.2.3.1 Signature-based Intrusion Prevention

FDP_IFC.1(5), FDP_IFF.1(5)

The TOE controls information flow if there is network traffic from the internal or external network based on action specified by the authorized administrator when after comparing the the rule patterns it owns with the source IP address, destination IP address, protocol (service), packet data (payload) security attributes, and they match. This is [Signature-based Intrusion Prevention] that blocks (known) harmful traffic through signature matching. In other words, it compares the information and the rule patterns, and if they do not match, it allows the information flow. If it matches, the requested information flow is allowed if the action is 'allowed' or 'exceptions'.

An authorized user can enable/disable [Signature-based Intrusion Prevention] or specify/manage advanced attributes of the function through [Network intrusion prevention policy management]. Apart from the signatures initially provided as default, the TOE provides a function where the authorized administrator can add new rules (signatures).

7.1.2.3.2 Algorithm-based Intrusion Prevention

FDP_IFC.1(5), FDP_IFF.1(5), FRU_RSA.1

The TOE controls information flow if there is network traffic from the internal or external network based on action specified by the authorized administrator when after comparing the the rule patterns it owns with the source IP address, destination IP address, protocol (service), packet data (payload) and time security attributes, and they match. This is an [Algorithm-based Intrusion Prevention] information flow control function that analyzes and blocks the behavorial patterns or statistical values for attacks that cannot be detected through rule pattern matching. An authorized user can enable/disable [Algorithm-based Intrusion Prevention] or specify/manage advanced attributes of the function. Apart from the algorithm-based rule patterns initially provided as default, the TOE provides a function where the authorized administrator can add new rules (signatures).

FRU_RSA.1

The TOE provides DoS Protection feature that blocks attacks by malicious users such as hackers and worm that request excessive amount of network service and cause network service error. The TOE blocks attacks that exploit the system (application) vulnerabilities (e.g. buffer overflow attack) among Dos/DDoS attacks through Signature-based Intrusion Prevention (rule pattern matching). The TOE takes action according to the rules specified by the authorized user (tcp syn flooding, icmp echo request flooding, udp flooding, ping of death, tear drop attack, land attack, F5 attack) by judging whether the attack is based on quantity/distribution/time of the traffic from attacks that can be found based on statistical method (e.g.: flooding attack). The authorized administrator can specify whether to block, end session, quarantine or limit bandwidth of the attack through [Network intrusion prevention policy management].

The TOE assures continuous normal service by effectively detecting/taking action on the DDoS attack to deactivate specific network or service. In other words, it detects/takes action on DDoS attack that uses IP Spoofing or social engineering DDoS based on unspecified individuals. The authorized administrator can specify to block, end session, quarantine, limit bandwidth and block DDoS attack (judged as network attack if more packets or traffics than the specified default is detected in the specified period) through [Network intrusion prevention policy management].

The TOE provides Anti-Scanning feature that detects/blocks scanning attacks from worm or hackers. It detects/blocks (rule pattern matching based protocol or port anti-scanning) scanning by analyzing traffic in specific IP address. Accordingly, as TOE can detect/block unknown scans, it can detect/block various scans (port scan, IP scan, Stealth scan, X-mas scan, Full-xmas scan, Fin scan, Spau scan, Syn/Fin scan, Vecna scan, NmapID scan) in hacking attempts. The authorized administrator can specify to block, end session, quarantine or limit bandwidth when an attack is detected through [Network intrusion prevention policy management].

The TOE detects and blocks abnormal traffic that cannot be detected through patterns or DoS/DDoS Protection and Anti-Scanning, in other words, attempt of connection from abnormal IP address (reserved IP address, multicast IP address); connection to IP segment that is not used internally; connection to port that is not in service; attempt of multiple connections at day break when there is almost no connection; multiple TCP connection (DRDOS protection) without 3-way handshaking; unauthorized connection of security system; abnormal combination of packet levels (IP header verification, TCP, UDP, ICMP header verification); and traffic exceeding the threshold. The authorized administrator can specify to block, end session, quarantine or limit bandwidth when an attack is detected through [Network intrusion prevention policy management].

7.1.2.4 Traffic Control

FDP_IFC.1(6), FDP_IFF.1(6)

The TOE controls [Traffic Control] information flow if there is network traffic from the internal or external network based on the source IP address, destination IP address, protocol (service), packet data (payload) and time security attributes. The [Traffic Control] information flow control that limits the traffic by the entire network traffic or IP address and protocol (service), is performed based on the rules specified by the authorized administrator.

7.1.2.5 Quarantine

FDP_IFC.1(7), FDP_IFF.1(7)

The TOE controls [Quarantine] information flow if there is network traffic from the internal or external network based on the source IP address/service port, destination IP address/service port security attributes. The TOE [Quarantine] information flow control is performend through interoperation with [Signature-based Intrusion Prevention] and [Algorithm-based Intrusion Prevention]. In other words, if the authorized administrator specifies the action for the TOE [Signature-based Intrusion Prevention] and [Algorithm-based Intrusion Prevention] as 'Quarantine', the TOE adds the IP address of the user (IT entity) where the information flow as detected to the Quarantine list. Information flow requested by the user (IP address) listed to the list subsequently shall be rejected for the specified period or until the authorized administrator manually disables it from the list. Through this, the TOE controls traffic that passes the TOE to prevent spreading of additional malicious codes. If the authorized administrator specifies 'Auto Release' from [Quarantine policy management] and the time, the TOE deletes the IP address of the user from the Quarantine list after the specified time. The authorized administrator can delete a user from the list or specify the quarantine period through [Quarantine policy management].

7.1.3 Identification and authentication

304 The TOE identifies all users that sends/receives network traffic to/from the TOE or through the TOE. In addition, if the event forces authentication, TOE authentication will be forced.

7.1.3.1 User identification and authentication

User identification and authentication

FIA_UID.2(1), FIA_UID.2(2), FIA_UID.2(3), FIA_UID.2(4)

The TOE identifies all users that attempts to access itself. All users that attempts to access before being identified cannot use any of the TOE features.

FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.1(3)

The TOE forces authentication of user in the following cases: if the authorized administrator attempts to connect to the security management interface (managemenet daemon) through a web browser (HTTPS), SSH (Secure SHell), serial port for security management; if the authorized administrator attempts to connect to the Log Server (AhnLab LogServer); and if the authorized administrator specifies authentication as the advanced rule for information flow control in the [Application Filter] security policy, in other words General TCP Proxy, FTP

Proxy, HTTP Proxy forced to user in [Application Filter]information flow control .

FIA_UAU.4 The TOE provides authentication through a general password or one-time password.

FIA_AFL.1, FIA_UAU.1(1) Before the user attempts to access the TOE security management interface before getting authenticated, access control will be forced through [Packet Filtering], and then, if it the access if determined to be rightful, it shall be verified through an ID and password through the identification and authentication procedure request window (login window).

FIA_AFL.1, FIA_UAU.1(2) Also, if the authorized administrator is a forcefully authenticater user by the advanced security policy of the General TCP Proxy, FTP Proxy and HTTP Proxy based on the [Application Filter], [Application Filter] will be forced first, and verified through an ID and password through the identification and authentication procedure request window (login window).

FIA_AFL.1, FIA_UAU.1(3) Lastly, if a user attempts to connect to a physically separated TOE, in other words, Log Server, the user shall be verified through an ID and password through the identification and authentication procedure request window (login window).

FIA_UAU.4 The TOE prevents reuse of authentication data through an authentication mechanism through a one-time password.

FIA_UAU.7 When password is entered during the authentication process, each character will be displayed as '*' on the window. If the authentication has failed, an audit data on the cause of failure shall be generated and displayed.

Failed authentication handling

FIA_AFL.1 The TOE protects authentication attempts by malicious users by providing account lock function in [Packet Filtering]. If the authentication has failed, an audit data on the cause of failure shall be generated and displayed. The TOE may lock a user account if the specified number of failed login authentication is exceeded (e.g. 10 times) to protect the TOE from login attempts by malicious users. But, in the case of an authorized administrator account, the locked account can be unlocked after the specified time (e.g. 10 mins.). The TOE notifies the user that the account has been locked or displays a window showing the cause of the failure and creates an audit data. An authorized administrator can unlock the locked account through the [Profile (object) management-User object management] function. If [User identification and authentication] is successful for an unlocked account, all the TOE functions can be used.

User security attribute: authorized administrator/log administrator

FIA_ATD.1(1), FIA_SOS.1 The TOE (exclusive device) maintains a security attribute list on the ID, password, access permission and lock status of the administrator. An authorized administrator can inquire, add to or delete from the account list, or inquire or modify the security attributes. But, user with the role of an authorized administrator is only allowed to modify ID and password.

FIA_ATD.1(4), FIA_SOS.1 The TOE (Log Server) maintains security attributes like identifier, password, login retry limit, lock time, lock status, name and permission. An authorized administrator can inquire, add to or delete from the account list, or inquire or modify the security attributes. The role of an authorized log administrator regarding [Security audit data management/review] of the Log Server is divided into super log administrator and log administrator.

FIA_SOS.1 Each verification standard of the characters allowed, combination rules, minimum/maximum length and reset interval for the password is forced.

User security attribute: authorized user/IT entity

FIA_ATD.1(2), FIA_SOS.1 The TOE maintains security attributes like ID, password, user authentication server, security level, login retry limit, password validity, expiry date and and lock account for user that has been forced authentication. An authorized administrator can inquire, add to or delete from the account list, or inquire or modify the security attributes through TOE [User object management].

FIA_ATD.1(3) The TOE maintains security attributes like name, type, IP address, network port and securtiy level for user sending/receiving information through the TOE. An authorized administrator can inquire, add to or delete from the account list, or inquire or modify the security attributes through TOE [IP address (object) management].

7.1.4 Security management

305 An authorized administrator can access the TOE security management interface (CLI) through the serial communication program operated on the system (IT entity) directly connected through a serial port during initial operation after successfully installing the TOE. The authorized administrator may specify a system (IT entity, remote management system) to allow connection to the TOE security management interface (GUI) through the web browser (e.g.: Internet Explorer 6.0). Accordingly, the TOE allows connection to the security management interface (HTTPS, SSH) only if the forced identification and authentication of the user that tries to access through the explicitly allowed remote management system (IT entity) is successful.

Security roles

FMT_SMR.1(1) The roles of TOE authorized administrators are divided into super administrator, administrator, super log administrator and log administrator. In addition, there is also an administrator of the TOE operating environment, the OS operated on the IT entity, used to connect to the security management interface. The permissions of each administrator are as below.

- Super administrator: Administrator with all permissions (read/write) to use all security management functions in [Security management].
- Administrator: Administrator with all read-only permission to TOE operation related policies only. Only a super administrator is able to add/modify/delete administrators through [Administrator settings]. An administrator can use all the security management functions in [Security management] in read-mode only.
- Super log administrator: Administrator with all permissions on the physically separated TOE (Log Server) that provides search and management features of security audit data of the TOE. Only a super log administrator can use the security audit data review/management feature by receiving security audit data through the system which the TOE super administrator granted permission through [Security management-Log settings, SNMP settings]. A super log administrator can use all the functions in [Security audit data management/review] only if the identification and authentication process forced by the Log Server itself has been successful.
- Log administrator: Permission is graneted by the super log administrator only. A log administrator has the permission to inquire audit data through the Log Server.
- TOE operating environment administrator: To access the security management interface (GUI, CLI, AhnLab LogServer) provided by the TOE, the identification and authentication process forced by the OS of the TOE operating system must be successful. An authorized administrator will grant permission only if , the identification and authentication has been successful.

FMT_SMR.1(2)

In addition, there is also the role of authorized user in the TOE. An authorized user is a user that has been forced by [Application Filter] function and successfully completed the identification and authentication process based on ID and password. An authorized user can change its password through the AhnLab Auth (Win32 application). But first, must successfully complete the identification and authentication process forced by the by [Application Filter] through the AhnLab Auth.

7.1.4.1 TOE Restart/Stop

FMT_MOF.1, FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1

The authorized administrator (super administrator) can restart or stop the TOE. When the TOE gets restarted or stopped, all the features will restart or stop. When an authorized administrator starts or stops the TOE, the TOE creates audit data.

7.1.4.2 System: TOE operating environment information management

The TOE provides [System: TOE operating environment] functions, such as [TOE operating environment and status monitoring], [Administrator settings], [Update settings], [Log settings], [SNMP settings], [Mail alert settings], [Backup and restore], [Integrity check], [TOE identification (host) name settings], [TOE time and language settings], [License update], [Session settings] for an authorized adminisrator to specify the settings needed for operating the TOE and monitor the status.

TOE operating environment and status monitoring

FMT_SMF.1, FMT_SMR.1(1), FAU_SAR.1

The TOE provides TOE support status, TOE settings information, TOE profile result, TOE operation information and event log when an authorized administrator successfully logs in to the TOE security management interface through the web browser (HTTPS).

Administrator settings

The TOE defines the administrator role to for the authorized administrator (super administrator), and provides the function to management the administrator ID and password and user IP address to allow access to the TOE security management interface (HTTPS, SSH). The TOE only allows connection to the TOE security management interface (HTTPS, SSH), only if an authorized administrator who accesses through the remote management system (IT entity), which has been explicitly allowed access, succeeds in getting authenticated. The TOE provides a default administrator ID. The password must be from 6 characters to 15 characters long.

FIA_ATD.1(1)

For reference, there will be restriction rules for the security attributes of the administrator account that has been forced by the TOE, such as ID, password, access permission and lock status.

FIA_SOS.1

The restriction rules on the password security attributes consist of allowed characters, combination rules, and minimum/maximum length.

FMT_MTD.1(1), FMT_MSA.1, FMT_SMR.1(1), FMT_SMF.1

An authorized administrator can search for, add, modify and delete administrator ID and password, and IP address to allow acess to the TOE security management interface. The TOE performs [User identification and authentication, in other words, identifies and authenticates the administrator based on the value defined by the authorized administrator.

FAU_GEN.1

When an authorized administrator adds, modifies or deletes an administrator IP address and ID, or modifies the security attributes of the object, the TOE creates an audit data on this.

Update settings

FMT_MOF.1, FMT_MTD.1(2), FMT_SMR.1(1), FMT_SMF.1

The authorized administrator can manage the security attributes of [Update], in other words, detection rules update, engine update and contents rating DB (harmful information engine) update. The TOE performs [Update] automatically or manually by an authorized administrator, every interval specified by an authorized administrator, based on the value specified by an authorized administrator. But, Firmware can only be updated manually by an authorized administrator.

FAU_GEN.1

The TOE performs TOE [Update] according to the value specified by an authorized administrator, and creates audit data on the result. Also, the TOE creates audit data when the authorized administrator modifies the following security attributes related to [Update].

Log settings

FMT_MOF.1,
FMT_MTD.1(2),
FMT_SMR.1(1),
FMT_SMF.1,
FAU_SEL.1,
FPT_ITT.1

The TOE provides management interface on the security attributes of [**Selective audit data generation, audit evidence protection, audit data loss prevention**] functions. It performs [**Selective audit data generation, audit evidence protection, audit data loss prevention**] functions based on the the value specified by an authorized administrator. The TOE sends only log types with activated log transfer to the physically separated TOE (Log Server) specified by the authorized administrator. In addition, if an authorized administrator specifies the log transfer method as 'secure transfer', the TOE (exclusive edvice) encrypts the audit data to SEED and sends it to the Log Server. In other words, the TOE encrypts and sends the TSF data to prevent exposure of TSF data.

FAU_GEN.1

When an authorized administrator adds, modifies or deltes the following security attributes related to [Selective audit data generation, audit evidence protection, audit data loss prevention] functions, the TOE creates audit data on this

SNMP settings

FMT_MOF.1,
FMT_MTD.1(2),
FMT_SMR.1(1),
FMT_SMF.1

The TOE provides the function to management the network through SNMP (Simple Network Management Protocol). The TOE sends status information of TOE to the SNMP manager specified by the authorized administrator. The information specified is also used in communication with the Log Server. In other words, the TOE uses SNMP to communicate with the Log Server for audit data transmission, and provides normal [**Security audit data management/review**] functions to the authorized administrator through it. The TOE interoperates with the SNMP according to the enable/disable status of SNMP, SNMP community name used for SNMP interoperation, IP address and CIDR (IP address/subnet mast) specified by the authorized administrator. An authorized administrator can add, modify and delete SNMP object, and start and stop transmission through the SNMP.

FAU_GEN.1

When the authorized administrator adds or deletes SNMP interoperable object, or modify the object security attributes, the TOE creates audit data on this.

Mail alert settings

FMT_MOF.1,
FMT_SMR.1(1),
FMT_SMF.1,
FAU_ARP.1,
FAU_SAA.1

The TOE provides the authorized administrator with the function to set the alert level and method when security violation event that reaches the CPU, memory and disk usage limit of the TOE operating environment occurs. In other words, the TOE alerts based on the value specified by an authorized administrator. The TOE sends the mail alert to the email address specified by an authorized administrator when the limit has been reached/exceeded.

FAU_GEN.1 When the authorized administrator modifies the security attributes of the alert function for the TOE operating environment, such as alert level and mail information, the TOE creates audit data on this.

Backup and restore

FMT_MOF.1, FMT_MTD.1(2), FMT_SMR.1(1), FMT_SMF.1 The TOE provides the authorized administrator with the management interface to [Backup and restore] the TOE operating environment files (important files that configures the TOE) in a semipermanent secondary memory device. TOE operating environment files are managed wby the TOE operating environment file system. The TOE sets a password according to the value specified by the authorized administrator during TOE operating environment file backup and then saves it in the specified location. The password for backing up the TOE operating environment must contain from 6 to 15 alphanumeric characters. When an authorized administrator attempts to restore the TOE operating environment settings through the backer up file, the TOE checks whether the password matches the password specified by the authorized administrator during backup. If the password matches, the TOE checks the integrity of the files requested by the authorized administrator for backup, and it is applied to the TOE only if it is not violated. When the authorized administrator restores the backed up environment files, the TOE renews (overwrites) the TOE operating environment configuration files, and performs the functions based on the changes settings.

FAU_GEN.1 When the authorized administrator backs up or restores the configuration files through the [Backup and Restore] function, the TOE creates audit data on this.

Integrity check

FMT_MOF.1, FMT_MTD.1(2), FMT_MTD.2, FMT_SMR.1(1), FMT_SMF.1 The TOE provides the authorized administrator with the function to renew or check the integrity. If the authorized administrator renews or checks the integrity, it performs [Self-test] pm the TSF data amd TSF execution code, and then notifies the result to the security management interface. If the integrity has been violated, the authorized administrator may ignore the event or take actions, such as initialization. An authorized administrator can specify the time interval for the self-test.

FAU_GEN.1 When the authorized administrator checks the integrity, the TOE creates audit data on this.

TOE identification (host) name settings

FMT_MTD.1(2), FMT_SMR.1(1), FMT_SMF.1 The TOE provides the authorized administrator with the function to specify the TOE identification (host) name. The TOE identification name is included in the memor when starting the TOE, and used as TOE information when creating audit data. The name gest managed through the TOE operating environment file system.

FAU_GEN.1 When the authorized administrator modifies the TOE identification name, the TOE creates audit data on this.

TOE time and language settings

FMT_MOF.1, FMT_MTD.1(2), FMT_SMR.1(1), FMT_SMF.1 The TOE provides the authorized administrator with the function to inquire and change the TOE system time and security management interface language. The TOE system time is managed through entry of time by the authorized administratorand synchronization with the trusted NTP server of the TOE operating environment. If an authorized administrator enters the time, the system time will be reset and used based on the time that has been entered (date, time: hour/minutes/seconds). If an authorized administrator specifies synchronization with the trusted NTP server (time server address, auto update time: day/time), the TOE system time will be reset based on the NTP server time by communicating with the specified NTP server at every specified update interval. After that, the system time is managed through the TOE operating environment RTC, and the system time gest used as the TOE time.

FAU_GEN.1 When the authorized administrator modifies the TOE time and management method through [TOE time and language settings], the TOE creates audit data on this.

License update

FMT_MOF.1, FMT_SMR.1(1), FMT_SMF.1, FAU_GEN.1 The TOE provides the authorized administrator with the function to inquire or set the license. The authorized administrator can control the functions provided by the TOE also through the TOE license information. In other words, if the license on the security functionalities provided by TOE does not exist, the TSF may not work properly. When the authorized administrator modifies the license information during operation, the TOE creates audit data on this.

Session settings

FMT_MTD.1(2), FMT_SMR.1(1), FMT_SMF.1, FAU_GEN.1 The TOE provides the authorized administrator with the function to inquire and modify the security attributes of [End user session] that limits the time of session between IT entities formed through the TOE.

When the authorized administrator modifies the security attributes of [End user session], the TOE creates audit data on this.

7.1.4.3 Network environment management

306 The TOE provides the authorized administrator with [Network environment management] such as [Network port], [Router settings], [Network], [DHCP] and [HA], to add, modify, delete and clear (activate/deactivate) network related objects used in [Security policy management], or set the network environment, which is required in TOE operation.

Network port settings

FMT_MTD.1(2),
FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1)

The TOE provides the authorized administrator with the function to inquire, add, modify, delete and clear (activate/deactivate) the security attributes of the network port. It manages the network interface (object) by dividing it into logical interface and physical interface. The types of logical network interface provided by the TOE include Aggregation, Bridge, VLAN and secondary network port, and the physical network interface types include static), PPPoE and DHCP. An authorized administrator can add, delete or change the security attributes of the types of logical network interface, and physical network interface, mentioned above. Then, the TOE operates according to the network port settings specified by the authorized administrator.

FAU_GEN.1

When the authorized administrator adds, modifies or deletes the network interface object or modifies the security attributes of the object, the TOE creates audit data on this.

Router settings

FMT_MTD.1(2),
FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1)

The TOE provides the authorized administrator with the function to search for, add, modify and delete the latest routing of the TOE from the list. The TOE manages the routing objects by dividing it into source routing, destination routing and general rounting. The authorized administrator can add, modify or delete a routing, or modify the sercurity attributes according to the object type.

FAU_GEN.1

When the authorized administrator adds, modifies or deletes the rounting object or modifies the security attributes of the object, the TOE creates audit data on this.

Network connection settings

FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1)

The TOE provides the authorized administrator with the function to inquire, add, modify and delete the ARP settings information and DNS server settings (※ if the authorized administrator specifies TOE to be operated as a client) owned by the TOE. The authorized administrator can change the DNS server settings that are related to the network connection of TOE, or inquire, add, modify or delete the ARP object, or change the security attributes of the object.

FAU_GEN.1

When the authorized administrator modifies the DNS server information or adds, modifies or deletes the the ARP settings or changes the security attributes of the object, the TOE creates audit data on this.

DHCP settings

FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1)

The TOE provides the authorized administrator with the function to search for, add, modify and delete the DHCP settings of the TOE or start/stop the DHCP server. Accordingly, the authorized administrator can start/stop the DHCP functions provides by the TOE, or add, modify and delete the DHCP object, or change the security attributes of the object. The TOE operates according to the DHCP settings specified by the authorized administrator.

FAU_GEN.1 When the authorized administrator can start/stop the DHCP server functions, or add, modify and delete the DHCP server settings object, or changes the security attributes of the object, the TOE creates audit data on this.

HA settings

FMT_MOF.1, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1) The TOE provides the authorized administrator with the function to inquire the HA operation state and audit port, start/stop the HA function or add, modify and delete the HA audit port object. Accordingly, the authorized administrator can add, modify and delete the audit port, modify the port object and change the security attributes of the HA function. The TOE performs [**Maintaining safe state in error–Hardware error processing**] according to the specified HA settings.

FAU_GEN.1 When the authorized administrator can start/stop the HA function, or add, modify and delete the HA audit port object, or changes the security attributes of the object, the TOE creates audit data on this.

7.1.4.4 Security policy management

307 The TOE provides the authorized administrator with [Profile (object) management], [Firewall policy management], [Network intrusion prevention policy management], [Contents filter policy management], [Update] that manages the objects used in [Security audit], [User data protection], [Identification and authentication] and security policy list. Through these management functions, the authorized administrator can control [Packet Filtering], [Application Filter], [Network Address Translation], [System White List], [Anti–Virus], [Anti–Spam], [Intrusion Prevention], [Traffic Control], [Quarantine] functions performed by the TOE.

7.1.4.4.1 Profile (object) management

308 The TOE provides the authorized administrator with [IP address (object) management], [Service object management], [User object management], [Schedule object management], [QoS object management] functions to add, delete and modify the object used in the TOE security policy.

IP address (object) management

FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1), FIA_ATD.1(3), FAU_GEN.1 The TOE provides the authorized administrator with the function to search for, add, modify and delete the IP address or IP address group object used in the TOE security policy. When the authorized administrator adds, modifies and deletes the IP address or IP address group object, or changes the security attributes of the object, the TOE creates audit data on this.

Service object management

FMT_MSA.1,
FMT_MSA.3,
FMT_MTD.1(2),
FMT_SMF.1,
FMT_SMR.1(1),
FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify and delete the service or service group object used in the TOE security policy. When the authorized administrator adds, modifies and deletes the service or service group object, or changes the security attributes of the object, the TOE creates audit data on this.

User object management

FMT_MTD.1(1),
FMT_MTD.2
FMT_SMF.1,
FMT_SMR.1(1),
FIA_ATD.1(2),
FIA_SOS.1,
FIA_UAU.4,
FAU_GEN.1

The term, 'user' used here means the object with security attributes such as user ID and password management by the TOE. The TOE provides the authorized administrator with the function to search for, add, modify and delete the user or user group object used in the TOE security policy. When the authorized administrator adds, modifies and deletes the user or user group object, or changes the security attributes of the object, the TOE creates audit data on this.

FMT_MTD.1(3)

In addition, if the user forced authentication by the [Application Filter] successfully completes the identification and authentication process, the user can change the authentication data (password). When the authorized administrator modifies the authentication data, the TOE creates audit data on this.

Schedule object management

FMT_MSA.1,
FMT_MSA.3,
FMT_MTD.1(2),
FMT_SMF.1,
FMT_SMR.1(1),
FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify and delete the schedule object used in the TOE security policy. Through this management function, the schedule objects added, modified and deleted by the authorized administrator gets use by [Packet Filtering], [Application Filter] functions. When the authorized administrator adds, modifies and deletes the schedule object, or changes the security attributes of the object, the TOE creates audit data on this.

QoS object management

FMT_MSA.1,
FMT_MSA.3,
FMT_MTD.1(2),
FMT_SMF.1,
FMT_SMR.1(1),
FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify and delete the QoS object used in the TOE security policy. Through this management function, the QoS objects added, modified and deleted by the authorized administrator gets use by [Packet Filtering] function. When the authorized administrator adds, modifies and deletes the QoS object, or changes the security attributes of the object, the TOE creates audit data on this.

7.1.4.4.2 Firewall policy management

309 The TOE provides the authorized administrator with the [Firewall policy management], [NAT policy management], [Quarantine policy management], [Policy exceptions management] functions to manage the security policies of [Packet Filtering], [Network Address Translation], [Quarantine], [System White List].

Firewall policy management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1(1), FAU_SEL.1, FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify, delete and activate/deactivate (clear) the firewall policy. The firewall policy objects added, modified and deleted by the authorized administrator gets use by [Packet Filtering] function. When the authorized administrator adds, modifies and deletes the firewall policy object, or changes the security attributes of the object, the TOE creates audit data on this.

NAT policy management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify, delete and activate/deactivate (clear) the [Network Address Translation] policy. The TOE provides the following NAT function types: Dynamic (M:N), Static(1:1) and Excluded. The NAT policy objects added, modified and deleted by the authorized administrator gets use by [Network Address Translation] function. When the authorized administrator adds, modifies and deletes the NAT policy object, or changes the security attributes of the object, the TOE creates audit data on this.

Quarantine policy management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1

The TOE provides the authorized administrator with the function to search for and quarantined system (IP address), or modify the [Quarantine] policy. The quarantine policy object modified by the authorized administrator gets use by [Quarantine] function. When the authorized administrator adds, modifies and deletes the quarantine policy object, or changes the security attributes of the object, the TOE creates audit data on this.

Policy exceptions management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify, delete and activate/deactivate (clear) the exceptions policy. The quarantine policy object added, modified, deleted and cleared (activated/deactivated) by the authorized administrator gets use by [System White List] function.

7.1.4.4.3 Network intrusion prevention policy management

310 The TOE provides the authorized administrator with the [IPS policy management], [Signature-based policy management], [Signature-absed policy (customized) management], [Pattern-based policy management], [Pattern-based policy (customized)

management], [DDoS protection settings], [Limit bandwidth management] functions to manage the security attributes of [Signature-based Intrusion Prevention], [Algorithm-based Intrusion Prevention].

IPS policy management

FMT_MOF.1,
FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1),
FAU_SEL.1,
FAU_GEN.1

The TOE provides the authorized administrator with the function to start/stop [Signature-based Intrusion Prevention] and [Algorithm-based Intrusion Prevention], or change the security attributes of the functions. When the authorized administrator start/stop the Network Intrusion Prevention function, or changes the security attributes of the function, the TOE creates audit data on this. The TOE maintains the following security attributes on the [Signature-based Intrusion Prevention] and [Algorithm-based Intrusion Prevention] functions. Through this management function, the IPS policy specified by the authorized administrator is used in the [Signature-based Intrusion Prevention] and [Algorithm-based Intrusion Prevention] functions.

Signature-based policy management

FMT_MOF.1,
FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1),
FAU_SEL.1,
FAU_GEN.1

The TOE provides the authorized administrator with the function to check the security attributes and operation state of [Signature-based Intrusion Prevention] or search for/change the detection/block rules (by individual signature or signature group), or rollback the currently applied rules to the initial state (default). Through this management function, the signature based policy specified by the authorized administrator is used in the [Signature-based Intrusion Prevention] function.

Signature-absed policy (customized) management

FMT_MOF.1,
FMT_MSA.1,
FMT_MSA.3,
FMT_MTD.1(2),
FMT_SMF.1,
FMT_SMR.1(1),
FAU_SEL.1,
FAU_GEN.1

The TOE provides the authorized administrator with the function to check the security attributes and operation state of [Signature-based Intrusion Prevention], or search for, modify, add and delete the detection/block rules (by individual signature or signature group).The authorized administrator directly adds the detection/block rules, separate from the signatures provided by AhnLab. Through this management function, the signature based policy specified by the authorized administrator is used in the [Signature-based Intrusion Prevention] function. When the authorized administrator adds, modifies and deletes the security policy of the [Signature-based Intrusion Prevention] function, or changes the security attributes of the object, the TOE creates audit data on this.

Pattern-based policy management

FMT_MOF.1,
FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1),
FAU_SEL.1,
FAU_GEN.1

The TOE provides the authorized administrator with the function to check the security attributes and operation state of [Algorithm–based Intrusion Prevention] or search for/change the detection/block rules (by individual signature or signature group), or rollback the currently applied rules to the initial state (default). Through this management function, policy specified by the authorized administrator is used in the [Algorithm–based Intrusion Prevention] function.

Pattern–based policy (customized) management

FMT_MOF.1,
FMT_MSA.1,
FMT_MSA.3,
FMT_MTD.1(2),
FMT_SMF.1,
FMT_SMR.1(1),
FAU_SEL.1,
FAU_GEN.1

The TOE provides the authorized administrator with the function to check the security attributes and operation state of [Algorithm–based Intrusion Prevention], or search for, modify, add and delete the detection/block rules (by individual signature or signature group). The authorized administrator directly adds the detection/block rules, separate from the pattern based signatures provided by AhnLab. Through this management function, the policy specified by the authorized administrator is used in the [Algorithm–based Intrusion Prevention] function. When the authorized administrator adds, modifies and deletes the security policy of the [Algorithm–based Intrusion Prevention] function, or changes the security attributes of the object, the TOE creates audit data on this.

DDoS protection settings

FMT_MOF.1,
FMT_MSA.1,
FMT_MSA.3,
FMT_MTD.1(2),
FMT_SMF.1,
FMT_SMR.1(1),
FAU_GEN.1

The TOE provides the authorized administrator with the function to inquire and modify the standard to consider an attack as DDoS attack based on [Algorithm–based Intrusion Prevention]. The default value to consider an attack as DDoS can be found in [DDoS protection settings]. When the authorized administrator modified the default value to consider an attack as DDoS, the TOE creates audit data on this.

Limit bandwidth management

FMT_MSA.1,
FMT_MSA.3,
FMT_SMF.1,
FMT_SMR.1(1),
FAU_GEN.1

The TOE provides the authorized administrator with the function to inquire the user (IP address) with limited bandwidth based on [Traffic Control], and delete a limited bandwidth. The threshold forced for the bandwidth limit can be specified through [IPS policy management]. The authorized administrator can select the user (event) to force limited bandwidth by specifying the security attribute of each policy object from [Signature–based policy management], [Signature–absed policy (customized) management], [Pattern–based policy management], [Pattern–based policy (customized) management]. When the authorized administrator deletes the object that is forced of [Traffic Control], the TOE creates audit data on this.

7.1.4.4.4 Contents filter policy management

311 The TOE provides the authorized administrator with the [Proxy policy management],

[Proxy service object management], [Proxy security attributes management], [Anti-virus policy management], [Anti-spam policy management], [Website filtering policy management] functions to manage the security attributes of [Application Filter] and [Contents Filter].

Proxy policy management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1(1), FAU_SEL.1, FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify, delete and activate/deactivate (clear) the proxy policy. The policy specified by the authorized administrator gets used by [Application Filter] function. When the authorized administrator adds, modifies and deletes the proxy security policy, or changes the security attributes of the object, the TOE creates audit data on this.

Proxy service object management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1

The TOE provides the authorized administrator with the function to search for, add, modify and delete the proxy service (type) object and group used as security attributes of the proxy policy. The policy specified by the authorized administrator gets used by [Application Filter] function. When the authorized administrator adds, modifies and deletes the proxy service (type) or service group object used in the security policy of [Application Filter], or changes the security attributes of the object, the TOE creates audit data on this.

The TOE provides proxy service object on the FTP, General TCP, HTTP, Oracle, POP3, SMTP, UDP and DNS service. An authorized administrator can add the proxy service object by protocol type based on this. When the authorized administrator adds, modifies and deletes service group object or proxy service (type) used for the security policy of [Application Filter], or changes the security attributes of the object, the TOE creates audit data on this.

Proxy security attributes management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

The TOE provides the authorized administrator with the function to search for, and modify the number of simultaneous proxy connection used as security attribute of the proxy policy. When the authorized administrator specifies a limit for the number of simultaneous connections (General TCP (Default: 16384), HTTP, (Default: 16384) FTP (Default: 512), SMTP (Default: 16384), POP3 (Default: 1024), Oracle (Default: 512), UDP (Default: 16384), DNS Proxy (Default: 16384)) by type of proxy, the TOE performs [Application Filter] based on this.

FAU_GEN.1

When the authorized administrator specifies a limit for the number of simultaneous connections used in the [Application Filter], the TOE creates audit data on this.

Proxy authentication user information inquiry

FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

The TOE provides the authorized administrator with the function to inquire the information on each user (user ID, proxy type, IP address to connect, connection time) and list of users that transmits network traffic through the TOE after succeeding in getting identified and authenticated through the [Application Filter].

Anti–virus policy management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

The TOE provides the authorized administrator with the function to inquire and modify the security attributes and attachment scanning method based on service type (e–mail, website, FTP). The TOE performs [Anti-Virus] function according to virus mail detection and actions (status, mail size to scan, removal of infected file, send a reject mail, filtered file extension list) used in the SMTP and POP3 proxy specified by the authorized administrator, virus detection and actions during file up/download in FTP proxy (mail size to scan, action), and virus detection and actions during file up/download in HTTP proxy (mail size to scan, action, filtered file extension list).

FAU_GEN.1

When the authorized administrator changes the security attributes of [Anti–Virus], the TOE creates audit data on this.

Anti–spam policy management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1) ,

The TOE provides the authorized administrator with the function to search for and modify the security attributes of [Anti–Spam] function. It performs the [Anti–Spam] function based on the anti–spam policy specified by the authorized administrator (Scan outgoing mail, mail size to scan, action in POP3 and SMTP Proxy, anti–spam filtering method).

FAU_GEN.1

When the authorized administrator changes the security attributes of [Anti–Spam], the TOE creates audit data on this.

Website filtering policy management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1) ,

The TOE provides the authorized administrator with the function to search for and modify the security attributes used in the HTTP proxy in the [Application Filter]. It performs the [Application Filter–HTTP Proxy] function based on website filtering policy specified by the authorized administrator (action, URL filtering status, Internet contents rating DB status, contents rating tag scan status).

FAU_GEN.1

When the authorized administrator changes the security attributes of [Application Filter–HTTP Proxy], the TOE creates audit data on this.

7.1.4.5 Update

312 The TOE maintains the virus engine, harmful information DB, and IPS engine to the latest

version by renewing the intrusion detection rules, engine and contents rating DB (harmful information DB) after checking the update server manually according to the specification set by the authorized administrator, or automatically at the specified intervals through [Update settings] .

Update

FMT_MTD.1(2), FAU_GEN.1 After checking the update server manually according to the specification set by the authorized administrator, or automatically at the specified intervals through [Update settings], the Toe renews the intrusion detection rules, engine and contents rating DB (harmful information DB) to maintain the virus engine, harmful information DB, and IPS engine to the latest version. It checks the integrity of the update files through encrypted communication (SSL) provided by the TOE operating environment when communicating with the update server to prevent errors. When update is performed, the TOE creates audit data on it.

7.1.5 Security audit data management/review

313 An authorized administrator can perform [Security audit data management/review] through the physically separated TOE (AhnLab LogServer, also called, 'Log Server'). To use [Security audit data management/review], the identification and authentication process forced by the Log Server itself must be successfully completed. The Log Server receives audit data from the exclusive data where the UTM daemon package runs, and manages it through the TOE operating environment DBMS (e.g. MS-SQL). When requested by the authorized administrator, the Log Server reads DB file from the TOE operating environment, and provides it to the authorized administrator in an interpretable form.

314 The Log Server saves the logs ti received in the DB file system and provides search and statistics function.

FMT_SMR.1(1) The roles of TOE authorized administrators are divided into super administrator, administrator, super log administrator and log administrator. In addition, there is also an administrator of the TOE operating environment, the OS operated on the IT entity, used to connect to the security management.

7.1.5.1 TOE (AhnLab LogServer) start/stop

FMT_MOF.1 FMT_SMF.1 The authorized administrator can start, stop and restart the Log Server that provides security audit data review through [TOE (AhnLab LogServer) start/stop]. Also, Log Server can be run as a start service, automatically, when the OS of the TOE operating environment runs according to the security policy. To use [Security audit data management/review] provided by Log Server, the identification and authentication process forced by the Log Server must be completed successfully.

Configuration

FMT_MTD.1(2), FMT_SMR.1(1) An authorized administrator (super log administrator) can manage the information of connection to DBMS that runs in the TOE operating environment to safely manage Log Server.

FAU_STG.1 FAU_STG.3 FAU_STG.4 FMT_SMR.1(1) If the authorized administrator (super log administrator) specifies the DB saving location, DBMS login ID and password and DBMS Server's address/port of the TOE operating environment, the TOE performs [**Security audit data management/review**] based on it. Also, if there is insufficient disk space and the authorized administrator specifies the location to save the original log and backup log, and the database action, the Log Server prevents audit data loss based on it. In other words, Log Server notifies the authorized administrator (super log administrator) when there is insufficient space in the audit storage through an alert window, and backs up the audit data in a specified location or deletes from the oldest audit data. An authorized administrator shall specify the space in percentage (%). When the authorized administrator specifies an alert level and backup/delete standard, the Log Server prevents audit data loss based on it.

FMT_MTD.1(1), FMT_MTD.1(2), FMT_SMR.1(1), FTA_SSL.1 An authorized administrator (super log administrator) can change the password or modify other options through [Configuration]. When the authorized administrator changes the password, the Log Server identifies and authenticates the authorized administrator (super log administrator) based on it. When an authorized administrator specifies auto logout time, the authorized administrator will be automatically loggede out if there has not been any activity (such as keyboard entry of mouse-click) for the specified time. TO access the Log Server security management interface, reauthentication process must be completed successfully.

Connection information

FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1) An authorized administrator (super log administrator) can check information (ID, name, group, logged in program, login time) on user logged in to TOE through [Connection information].

7.1.5.2 Configuration

315 To use the security audit data management/review normally, an authorized administrator (super log administrator) must register the TOE to receive the audit data created while operating the TOE (exclusive device where UTM daemon package is running, hereinafter called, 'exclusive device'), using the TOE security management interface [Configuration]. Accordingly, the audit data management system, where the Log Server

is installed and operated through the TOE security management interface [SNMP settings], [Log settings], must be installed.

Connection settings

FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

An authorized administrator specifies the information on Log Server to access and connection information (Server address, Server port, search port, SSL status) to inquire the audit data with [Connection settings]. Then, the authorized administrator can inquire the audit data based on this information. In addition, auto logout status and time can be specified, and through this, session is locked and reauthentication is forced if the inactivity time of the an authorized administrator has been exceeded.

Alert mail

FMT_MOF.1, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

An authorized administrator specifies the spam mail list sending status, list sending time, mail address, alert method (mail, notification window), receiver's email address, mail server information (IP address, port) and ID, password through [Alert mail]. With this, the TOE sends the spam mail list based on this information.

Device settings

FMT_MOF.1, FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

An authorized administrator can add, modify and delete the TOE to manage audit data through [Device settings]. If the authorized administrator adds, modifies and deletes TOE rules (IP address, port, community name) to manage, the Log Server shall perform [Security audit data management/review], such as audit data statistics processing, based on this. For the TOE to gain permission to receive security audit data, the IP address, port and community name of the TOE (exclusive device) must be entered accurately. In addition, the audit data management system where the Log Server is installed and operated must be registered accurately through TOE security management interface [SNMP settings], [Log settings].

Alert level

FAU_SAR.1, FMT_MOF.1, FMT_SMF.1, FMT_SMR. 1

An authorized administrator can check the system resource usage state of the TOE by specifying the alert level and standard (safe, caution, warning, critical according to the risk level and alert level) according to the amount of system resources usage (CPU capacity, memory capacity, disk capacity, no. of network connections, network usage, no. of sent packets through) of the TOE (exclusive device) through [Alert level]. The specified alert level is used as the default for [Trend analysis], [Security alarm (system status alert)]. But, when setting the alert level, the risk level cannot be higher than the alern level.

Account settings

FIA_ATD.1(4), FMT_MTD.1(1), FMT_SMR.1(1)

An authorized administrator (super log administrator) can add, modify and delete the user account that can access the [Security audit data management/review] function provided by the Log Server through [Account settings]. An authorized administrator manages user account (identifier, password, maximum login retry limit, lock time, lock status, name, permission) through [Account settings]. The Log Server identifies and authenticates log administrators based on the user information registered by the authorized administrator. The roles of the authorized administrator related to [Security audit data management/review] is divided into super log administrator and log administrator.

7.1.5.3 Program settings

License

FMT_SMF.1,

An authorized administrator can check the Log Server license. For reference, the Log Server license is provided with the TOE, and when there is no license, the Log Server cannot be managed.

Backup settings

FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

An authorized administrator (super log administrator) can directly back up the security audit data or specify the backup interval through [Backup settings]. If the authorized administrator specifies schedule backup interval, backup path or target for backup, Log Server can back up the audit data based on this value. An authorized administrator can restore the saved backup data or create a backup list. But, restore is not provided in trend analysis and configuration data.

7.1.5.4 Device information

Device information

FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

An authorized administrator (super log administrator) can check the information of the TOE (exclusive device) to be managed by the Log Server through [Device information]. In other words, the authorized administrator can check the time information, the latest device in-formation, device name, IP address, firmware version, continuous use time and state.

7.1.5.5 Trend analysis

Trend analysis

FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1(1)

An authorized administrator (super log administrator) can analyze the trend by type of audit data, such as TOE (exclusive device비), system status trend by date, network status trend, attacker analysis, attack target analysis, attack type analysis, risk analysis, and attack country analysis through Log Server's [Trend analysis].

7.1.5.6 Log

FAU_SAR.1, FAU_SAR.3, FMT_SMF.1, FMT_SMR.1(1)

An authorized administrator (super log administrator) can read all audit data created/saved during TOE operation from the audit record through the Log Server. The authorized administrator can monitor the audit data in real-time or review the existing audit data according to the type of audit data (operation log, firewall log, IPS log, quarantine log, contents filter log, website filter log, anti-virus log, ant-spam log) through the security management interface [Log] provided by the TOE (Log Server). When the authorized administrator specifies a search value after selecting the type of audit data to review, the Log Server provides the audit data search result. Log Server provides audit data by ascending order of the time it occurred.

7.1.6 TSF protection

316 The TOE performs [Maintaining safe state in error], [Self-test], [External entity test] to protect the TSF.

7.1.6.1 Maintaining safe state in error

Software error processing

FPT_FLS.1, FRU_FLT.1, FAU_GEN.1

The TOE (exclusive device) maintains/manages the daemon that performs the main functions to deal with the errors as well as the list on the operation state (e.g. start, stop, restart, reload) of the daemon to deal with software errors. Then the TOE regularly checks the state of the daemon that has been specified to be managed based on the target list, and when an abnormally terminated daemon is detected, it restarts the daemon to sort out the software error. When the daemon gets restarted, audit data on the daemon gets created. Also, TOE assures safe performance of all the security functions provided through the TOE (exclusive device) even when the Log Server causes the error, in other words, even when the Log Server does not operate properly due to error in the TOE operating environment.

Hardware error processing

FPT_FLS.1, FRU_FLT.1, FAU_GEN.1

The TOE (exclusive device) can be managed based on HA. In other words, an authorized administrator can manage multiple TOEs, and when several of them are mangaged together, and an error occurs in a few of them, all the security functions provided by the TOE (exclusive device) will be provided normally through the other TOEs. When HA runs due to an error in a TOE, the TOE creates audit data on this.

7.1.6.2 Self-test

FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FPT_TST.1, FMT_MTD.2

The TOE conducts self test regularly (hourly) while the TOE is running to verify accurate management of all TSF, excluding the 'TOE process management daemon' which is the main management daemon of TOE. In addition, an authorized administrator can also perform integrity chck through the TOE security management interface. The TOE creates hash value on the target for integrity check every specified test interval and compares it to the default hash value saved at the initial startup. When violation of integrity is detected, the TOE notisfies it to the authorized administrator through the security management interface and creates audit data on this. An authorized administrator can ignore it or take action, such as initialization. Audit data for all these events are created. When an authorized administrator has been successfully identified and authenticated, and security attributes have been added, deleted or modified through the TOE security management interface, TOE will consider it as rightful, and renew the hash value. In addition, the TOE also updates the hash value even when [Update] has been performed successfully, and creates an audit data one this. Then, the TEO checks the integrity based on the updated hash value. The TOE checks the integrity of all executable files and configuration files, such as security policy files, that are needed in TOE operation. It audits and records the action of the authorized administrator and the [Self-test], [Integrity check] results.

FMT_MOF.1, FMT_SMF.1, FMT_SMR.1(1)

When an authorized administrator requests for integrity check through the TOE security management interface [Integrity check], the TOE checks the TSF data and TSF execution code. When violation of integrity is detected, the TOE notifies the authorized administrator through the security management interface. The authorized administrator can take action, such as ignore or initialize.

In other words, the TOE provides the function to check the integrity of the configuration data and execution codes through the TOE security management interface (GUI). Details on this can be found in [System: TOE operating environment –Integrity check].

7.1.6.3 External entity test

FPT_TEE.1

The TOE (Log Server) regularly checks whether the Microsoft SQL Server, a DBMS that interoperates with the TOE, is operating precisely at startup and during operation. If it is not operating properly, a warning window will be displayed for the authorized administrator to restore it. The authorized administrator can also check the DBMS operation state through the security management interface of the TOE (Log Server) in real-time.

7.1.7 TOE access

317 The TOE performs [Session lock of security management interface] and [End user session] functions to control TOE access.

7.1.7.1 Session lock of security management interface

When the TOE (exclusive device) gets properly distributed and installed, the authorized administrator usually connects to the TOE security management interface (CLI) through the serial communication program operated on the system (IT entity), which is directly connection with a serial console port, first. And then, the authorized administrator specifies the system (IT entity) to allow access to the TOE security management interface (HTTPS, SSH) remotely, for convenience. The TOE only allows connection to the TOE security management interface (HTTPS, SSH) only if the user that tries to connect through the remote management system (IT entity) that has been allowed access permission explicitly has been identified and authenticated.

FTA_SSL.1, FAU_GEN.1 When the authorized administrator logs in to the TOE security management interface (Web UI) successfully, and there has been no activity for the allowed inactivity period, the session will be locked. The specified default of the inactivity period that is allowed is 10 minutes, and it cannot be changed. When the session is locked, all functions in the session will be locked as well. The TOE creates new session and allows access to the security management interface only if the administrator has been successfully reauthenticated (User identification and authentication). The TOE creates audit data on such events, in other words the result of [Session lock of security management interface].

7.1.7.2 End user session

FTA_SSL.3 In general, the TOE ends a session created through the TOE if there is no network traffic transfer event through the TOE between IT entities based on inactivity (entry) of the user for the time specified for each service (TCP default: (432,000 sec.), UDP default: 30 sec.), ICMP default: 30 sec.).

FMT_MOF.1, FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1 Au authorized administrator can specify the session timeout for each protocol type, in other words the session maintenance time, through the TOE security management interface [System: TOE operating environment –Session settings]. If the authorized administrator does not specify a separate value, the default value will be used. Based on this value, the TOE will perform [End user session] function, and create audit data on it.

FTA_SSL.3 If the user gains permission to transmit network traffic through the TOE through 'user authentication' based on [Application Filter], and sends/receives traffic, the TOE will end the session created through the TOE if there is no network traffic transfer event through the TOE between IT entities based on inactivity (entry) of the user for the time specified (30 min.).

FMT_MOF.1, FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1 An authorized administrator can specify a target to force ending of session based on user authentication through the TOE security management interface [Contents filter policy management–Proxy policy management]. The services that provide user reauthentication function when the session ends due to exceeding the specified time include HTTP Proxy, General TCP Proxy and FTP Proxy services. The TOE performs [End user session] based

	on this value, and creates audit data on it.
FTA_SSL.3	The TOE ends the session of the user of which the information flow is controlled based on [Application Filter], if there has not been any network traffic transfer event through the TOE between IT entities based on inactivity (entry) of the user for the time specified (※ Refer to [Proxy service object management], Default: 120 sec.) for each service (Proxy services provided by the TOE: General TCP Proxy, SMTP Proxy, POP3 Proxy, FTP Proxy, HTTP Proxy, Oracle Proxy, UDP Proxy, DNS Proxy).
FMT_MOF.1, FMT_SMF.1, FMT_SMR.1(1), FAU_GEN.1	An authorized administrator can specify the session timeout value through the TOE security management interface [Contents filter policy management–Proxy service object management]. If the authorized administrator does not specify a time, the default time will be applied. The TOE will then perform [End user session] based on the value, and create audit data based on it.

8 Reference

[1] Ministry of Public Administration and Security Notification(Ministry of Public Administration and Security, 2008.07)

[2] Common Criteria (Ministry of Public Administration and Security Notification No. 2008-26), Ministry of Public Administration and Security, 2008.07

[3] Common Evaluation Methodology V3.1 r2, Korea Information Security Agency, 2007.09

[4] Firewall Protection Profile for Government V1.2, Korea Information Security Agency, 2006.05

[5] Network Prevention System Protection Profile V2.0, Korea Information Security Agency, 2008.04

[6] Firewall Protection Profile V2.0, Korea Information Security Agency, 2008.04