

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

AhnLab TrusGuard V2.2

Security Target



673, Sampyeong-dong, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-400, South Korea www.ahnlab.com

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Revision History

Version	Date	Author	Description
1.0	2012-10-04	Jae-Hoon Hwang	Initial Version
1.1	2013-01-23	Jae-Hoon Hwang	Updated with additional scopes - VPN, Contents Filtering, IPv6, Anti-Virus
1.2	2013-03-31	Jae-Hoon Hwang	Updated with modification requests - Review comments: Chapters 1 ~ 4
1.3	2013-04-30	Jae-Hoon Hwang	Updated with EOR-01 and EOR-04
1.4	2013-05-09	Jae-Hoon Hwang	Updated with modification requests - Review comments: 6. Security requirements
1.5	2013-05-27	Jae-Hoon Hwang	Updated with modification requests - Review comments: 7. TOE summary specifications
1.6	2013-06-13	Jae-Hoon Hwang	Updated with modification requests - Additional review comments
1.7	2013-07-05	Jae-Hoon Hwang	Updated interoperable server - Removed LDAP server interoperation
1.8	2013-07-30	Jae-Hoon Hwang	Updated with function name changes (IPS > DPI)

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Table of Contents

1.	Security Target Introduction	7
1.1.	ST Reference	7
1.2.	TOE Reference	8
1.3.	TOE Overview	9
1.4.	TOE descriptions	25
1.5.	Conventions	35
1.6.	Terms and Definitions	36
2.	Conformance Claims	41
2.1.	Common Criteria Conformance	41
2.2.	Protection Profile Conformance	41
2.3.	Package Conformance	41
2.4.	Supporting rationale for conformance claim	42
3.	Security Problem Definitions	43
3.1.	Threats	43
3.2.	Organizational Security Policies	45
3.3.	Assumptions	46
4.	Security objectives	48
4.1.	TOE Security objectives	48
4.2.	Security Objectives for the Operational Environment	50
5.	Extended component definition	58
6.	Security requirements	59
6.1.	Security functional requirements	59
6.2.	TOE Security Assurance Requirements	105
6.3.	Rationale for Security Requirements	123
7.	TOE summary specification	136
7.1.	TOE Security Functionality	136

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

List of Tables

[Table 1-1]	TOE hardware models	20
[Table 1-2]	Specifications for administrator systems	20
[Table 1-3]	Installation specifications for SSL VPN Client and Authentication Client.....	21
[Table 4-1]	Security issue definitions and security objective countermeasures	51
[Table 6-1]	Security functional requirements for Security Target.....	59
[Table 6-2]	Countermeasures upon detection of a potential security violation.....	61
[Table 6-3]	Auditable events	62
[Table 6-4]	Audit data type and searching/sorting criteria by audit data type - TrusGuard Gateway	64
[Table 6-5]	Audit data Type and searching/sorting criteria by audit data type – TrusAnalyzer	66
[Table 6-6]	User security attributes list	85
[Table 6-7]	VPN User security attributes list	85
[Table 6-8]	Secret acceptance criteria.....	86
[Table 6-9]	Security functions and allowed capabilities - TrusGuard Gateway	88
[Table 6-10]	Security functions and allowed capabilities - TrusAnalyzer.....	89
[Table 6-11]	Security attributes list and allowed capabilities for authorized administrators ..	93
[Table 6-12]	TSF data created in the TOE(TrusGuard Gateway) and management capabilities for authorized TG top-level administrators and TG general administrators	95
[Table 6-13]	TSF data list created in the TOEs (TrusGuard Auth and SSL VPN client) and management capabilities for authorized general users	96
[Table 6-14]	TSF data created in the TOE (TrusAnalyzer) and management capabilities.....	97
[Table 6-15]	Security role types for authorized users	100
[Table 6-16]	User inactive periods for user session termination	102
[Table 6-17]	Security Assurance Requirements.....	105
[Table 6-18]	TOE Security objectives and a map between security objects and corresponding security functional requirements	123
[Table 6-19]	Dependencies of the functional components	133
[Table 7-1]	Functional components to trigger security alerts, auditable events and countermeasures	137
[Table 7-2]	Cryptographic algorithms used by the TOE	139
[Table 7-3]	Information flow control methods for Access control at Network Level policies	

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

143

[Table 7-4]	Information flow control methods for Signature-based blocking rules	146
[Table 7-5]	Information flow control methods for behavior-based blocking rules.....	147
[Table 7-6]	Users to be identified for TOE access	150
[Table 7-7]	Security attributes of authorized administrators	152
[Table 7-8]	Authorized general users / Security attributes of IT entities	152
[Table 7-9]	Password convention rules to authorize administrators	153
[Table 7-10]	VPN SFP security attributes.....	157
[Table 7-11]	Traffic filtering SPF Security attributes	158
[Table 7-12]	Content filtering SFP Security attributes.....	158

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

List of Figure

[Figure 1-1]	TOE operating environment examples (Dedicated IPv4 network)	14
[Figure 1-2]	TOE operating environment examples (Dedicated IPv6 network)	15
[Figure 1-3]	TOE operating environment examples (Mixed IPv4/IPv6 network).....	16
[Figure 1-4]	TOE operating environment examples (IPv4 VPN network)	17
[Figure 1-5]	TOE operating environment examples (IPv4 HA network).....	18
[Figure 1-6]	TOE logical scope.....	28

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1. Security Target Introduction

- 1 This chapter consists of references to the Security Target ("ST") and Target of Evaluation ("TOE"), as well as an overview on TOE and its descriptions. To help users to understand the TOE in phases, the ST reference and the TOE reference sections will outline identifiable materials for ST and TOE; the TOE overview section briefly describes the TOE; the TOE descriptions section explains it in more detail.

1.1. ST Reference

- 2 This section will provide information that identifies the particular ST in configuration to titles, versions, authors and publication dates.

Title

AhnLab TrusGuard V2.2 Security Target

ST Version

1.8

Author

Security Policy team at AhnLab Inc.

Publication date

2013. 7. 30

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.2. TOE Reference

- 3 The ST also provides a TOE **reference** that identifies the particular TOE. A typical TOE reference consists of TOE titles, versions and developer.

TOE Title

AhnLab TrusGuard V2.2

TOE Identifier

2.2.0.8

Developer

Network Development Division at AhnLab Inc.

Components of TOE

- ✓ TOE(TrusGuard Gateway): AhnLab TrusGuard Gateway 2.2.0.5
- ✓ TOE(SSL VPN client): AhnLab TrusGuard SSL VPN Client 1.0.3.2
- ✓ TOE(Authentication Client): AhnLab TrusGuard Auth 1.0.0.33
- ✓ TOE(TrusAnalyzer): AhnLab TrusAnalyzer 1.0.2.12

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.3. TOE Overview

- 4 The TOE overview is aimed at potential TOE consumers who are reading this ST in search of a TOE that may meet their security needs and supports their hardware, software and firmware.

1.3.1. Usage and major security features of a TOE

- 5 AhnLab TrusGuard V2.2 is an packet filtering system that performs access control for information that is transferred from the internal network to external network or from an untrusted external network to the internal network. It is also a VPN product that protects data through encrypted communication when the IT entity located at the remote site accesses a specific internal network through a public internet network.
- 6 AhnLab TrusGuard V2.2.0.8 ("TOE") consists of AhnLab TrusGuard Gateway, AhnLab TrusGuard SSL VPN Client, AhnLab TrusGuard Auth, and AhnLab TrusAnalyzer. These components are installed and distributed as firmware and software products, embedded in hardware equipment.
- 7 The major capabilities of TOE are access control at network level functions, VPN functions, and additional security functions as detailed below.

Access Control at Network Level

- 8 TrusGurd Gateway can handle abnormal traffic by interoperating with the packet filtering function based on the Access Control List, Virtual Private Network (VPN), and signature/behavior-based functions.
- Packet filtering: When access is requested from the external network to the internal network or from the internal network to the external network, the TOE controls information flows in accordance with authorized administrators' security policies with security attributes based on source/destination IPv4 or IPv6 addresses, services (protocols and ports), and time information.
 - Interoperation with VPN and abnormal traffic detection function: The access control at network level function can be set to interoperate with VPN functions and signature/behavior-based abnormal packet detection functions when administrators set

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

information flow control policies. In this way, information flows for abnormal network packets are controlled and transmission packets between communication targets are handled during VPN connection.

Virtual Private Network (VPN)

9 The TOE protects transmission data by providing encrypted communication during the use of IPsec VPN functions and SSL VPN functions to securely send and receive data from public networks to internal networks.

- IPsec VPN: This function protects user data transferred through encrypted communication via the IPsec protocol between the internal network gateway and the communication target gateway at the remote site.
- SSL VPN: This function protects user data transferred through encrypted communication via the SSL protocol between the VPN gateway and the SSL VPN Client installed in user PCs from the external location.

Network address translation

10 The TOE provides a network address translation function for modifying IP address information into the authenticated IP address specified by the authorized administrator. This hides the internal IP address information when hosts with the internal network address access external networks or external hosts access internal networks.

Deep Packet Inspection

11 The TOE proactively detects and blocks abnormal traffic (e.g. DoS and Scan attacks), hacking packets that exploited application vulnerabilities and traffic/network protocols that spread malware (e.g. Worm, Trojan horse, etc.).

- Signature-based abnormal traffic detection and block: It examines specific information (possibly the header or payload) of an incoming packet by comparing signature patterns and consistency provided by AhnLab Inc. It also handles abnormal packets in accordance with the DPI policies set by the authorized administrator.
- Behavior-based detection and block: If packets coming into internal networks contain traffic that causes DoS attacks or abnormal behaviors and exceeds the allowed threshold

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

in comparison with base data (BPS/PPS values) provided by AnhLab Inc., then they can be detected as abnormal packets and handled in accordance with the DPI policies set by the authorized administrator.

Contents filtering

12 The TOE blocks harmful information received from external networks at the application level and controls general user information flows through the user authentication client.

- Application Proxy: The TOE that works as an application proxy server can proactively examine and block harmful information received from attachments, unauthorized FTP commands, http documents, and e-mails requested from internal network hosts.
- User authentication: The TOE only allows information flows of users that are authorized through the Authentication Client when general users are accessing external FTP and HTTP servers.

High Availability (HA)

13 In an environment with a pair formed of two sets of identical hardware equipment, the TOE can maintain uninterrupted service operation despite the failure of one set by synchronizing security policies and distributing traffic processing to the functioning equipment. Depending on the system configuration, it can be operated in Active-Standby mode or Active-Active mode.

- Active-Standby mode: In this mode, master equipment and slave equipment are paired together, but the master equipment usually handles all traffic. When the master equipment fails, the slave equipment works as the master equipment to handle all incoming/outgoing traffic and apply security policies.
- Active-Active mode: In this mode, a pair of master equipment and a back-up work together to distribute and handle all traffic separately in more than two devices. In the event of equipment failure, the master equipment and the back-up work as hot spares for each other to take over the functionalities of the failed unit to handle all traffic and apply security policies.

Audit Data Management

14 The TOE creates audit data to record audit events specified by the authorized administrator, and

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

also saves and manages the created audit data. Audit data look up and review functions are provided, and security alerts are sent to administrators to check for potential security violations. The audit data is protected in the audit data storage, and the TOE proactively performs countermeasures predicting audit data loss.

Security management

- 15 The TOE provides authorized administrators with administration functions such as: TSF data management functions, TOE security function setup, or security functional commands. The allocated security management functions can vary, depending on the usage rights of authorized administrators. To securely perform security function setup, the authorized administrators should use operation systems and web browsers supporting SSH 2.0, TLS V1.0, V1.1, and V1.2 protocols.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.3.2.TOE Type

16 The TOE type is Packet Filtering Firewall and VPN.

1.3.2.1. TOE Operating Environments

17 The TOE(AhnLab TrusGuard V2.2.0.8) components consist of TrusGuard Gateway, TrusAnalyzer, SSL VPN Client, and Authorized Client. These TOE components are separately installed and operated on the network.

18 The TOE for TrusGuard Gateway is a firmware-type product embedded in hardware models and installed in the inline mode at the network boundary. It performs Packet filtering and VPN functions against all traffic passing through the TOE.

19 The TOE for TrusAnalyzer is firmware-type software for audit data management, which is installed and operated in the hardware along with the TOE for TrusGuard Gateway.

20 The TOE for SSL VPN Client, which provides SSL/TLS VPN client function, and the TOE for Authentication Client, which provides a user authentication function, are installed and operated in general user PCs.

21 The authorized administrator connects to the TOE security management screen via web browsers or SSH/Console programs to look up or set up security policies. The web browsers and SSH consoles support both IPv4 and IPv6 protocols.

22 The TOE for TrusAnalyzer can save, manage, and look up the audit data coming from the TOE for TrusGuard Gateway. The TOE for TrusAnalyzer generates reports based on the saved audit.

23 The TOE for TrusGuard Gateway performs security functions and operates the TOE by interoperating with external servers such as update servers (AST), anti-spam servers (RPD/RBL), NTP servers, user authentication servers (Radius/Active-Directory), and mail servers.

24 The TOE operating environments are explained from [Figure 1-1] through [Figure 1-5]. The TOE can be operated in the IPv4 network and the IPv6 network, which is configured as a VPN environment and an HA environment depending on the network configuration.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

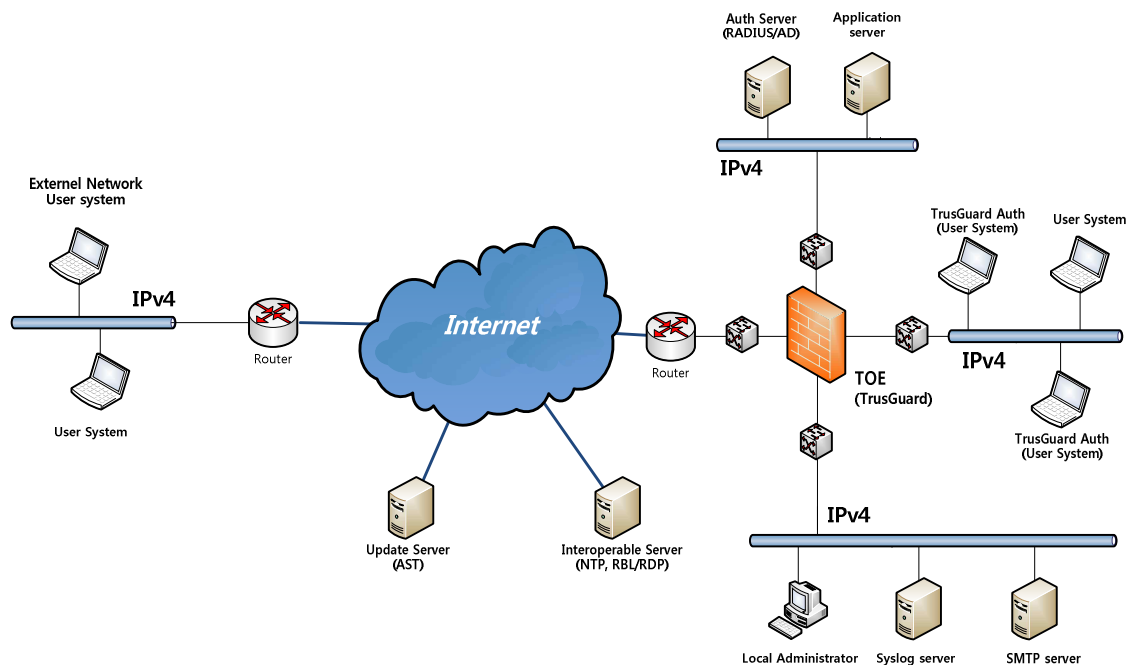
TOE on a dedicated IPv4 network

25

The TOE for TrusGuard Gateway is operated in a dedicated IPv4 protocol-based network environment as shown in [Figure 1-1], providing the following security functions.

- Access control at Network Level: Firewall, Exceptions, Access block by blacklist
- VPN: IPSec VPN, SSL VPN
- Other security functions: Network address translation, Deep Packet Inspection, content filtering, HA, audit data management and security management

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



TOE on a dedicated IPv6 network

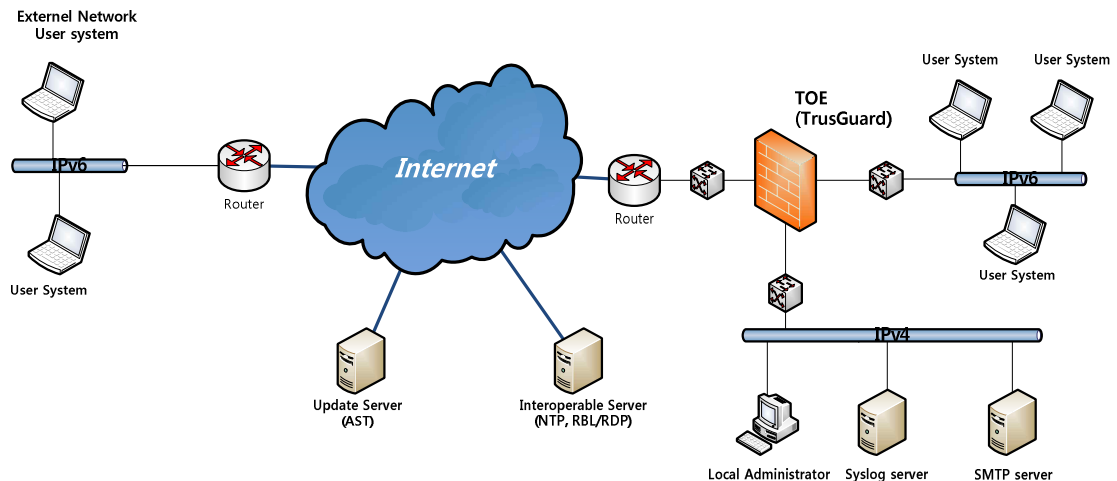
26

The TOE for TrusGuard Gateway is operated in a dedicated IPv6 protocol-based network environment as shown in [Figure 1-2], providing the following security functions.

- Access control at network level: Firewall
- Other security functions: Network address translation, audit data management and security management

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

[Figure 1-2] TOE operating environment examples (Dedicated IPv6 network)



TOE on a mixed IPv4/IPv6 network

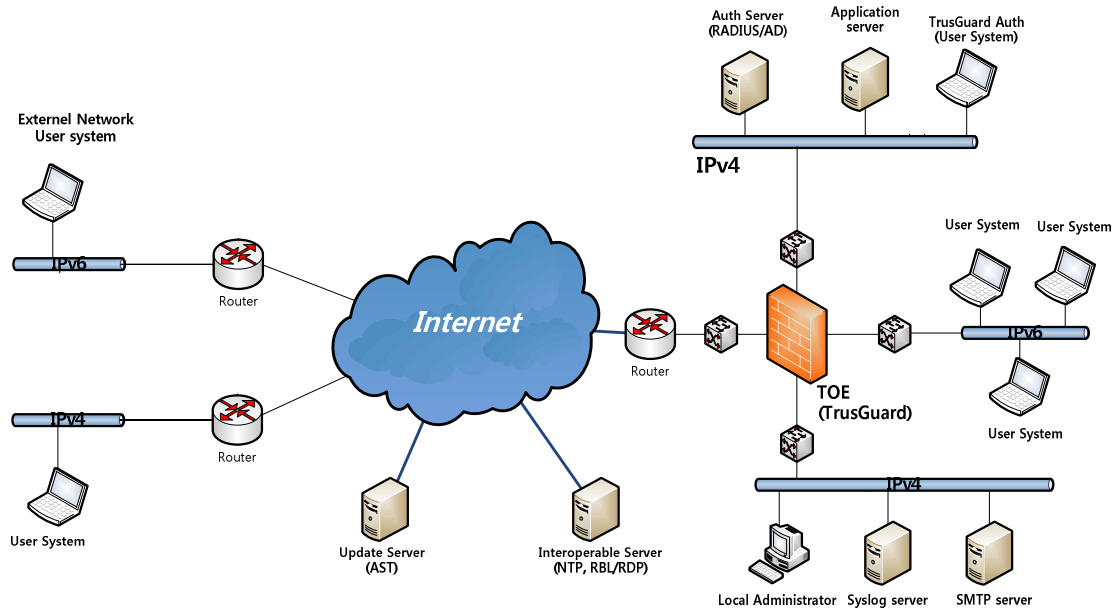
27

When the TOE for TrusGuard Gateway is installed on mixed IPv4/IPv6 protocol-based network environments, it can support only IPv4 to transmit resource operating status information and audit data created upon the application of security policies. In a dedicated IPv6 network, the network ports, SNMP servers and SYSLOG servers should use IPv4 addresses to send the audit data and resource operating status information of the TOE (TrusGuard Gateway). The TOE is operated in mixed IPv4/IPv6 protocol-based network environments as shown in [Figure 1-3], providing limited security functions depending on its IP protocol.

- Access control at network level
 - IPv4: Firewall, Exceptions, Access Block by blacklist
 - IPv6: Firewall
- VPN
 - IPv4: IPSec VPN, SSL VPN
- Other security functions
 - IPv4: Network address translation, Deep Packet Inspection, content filtering, HA, audit data management and security management
 - IPv6: Network address translation, audit data management and security management

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

[Figure 1-3] TOE operating environment examples (Mixed IPv4/IPv6 network)



IPv4 VPN operating environments

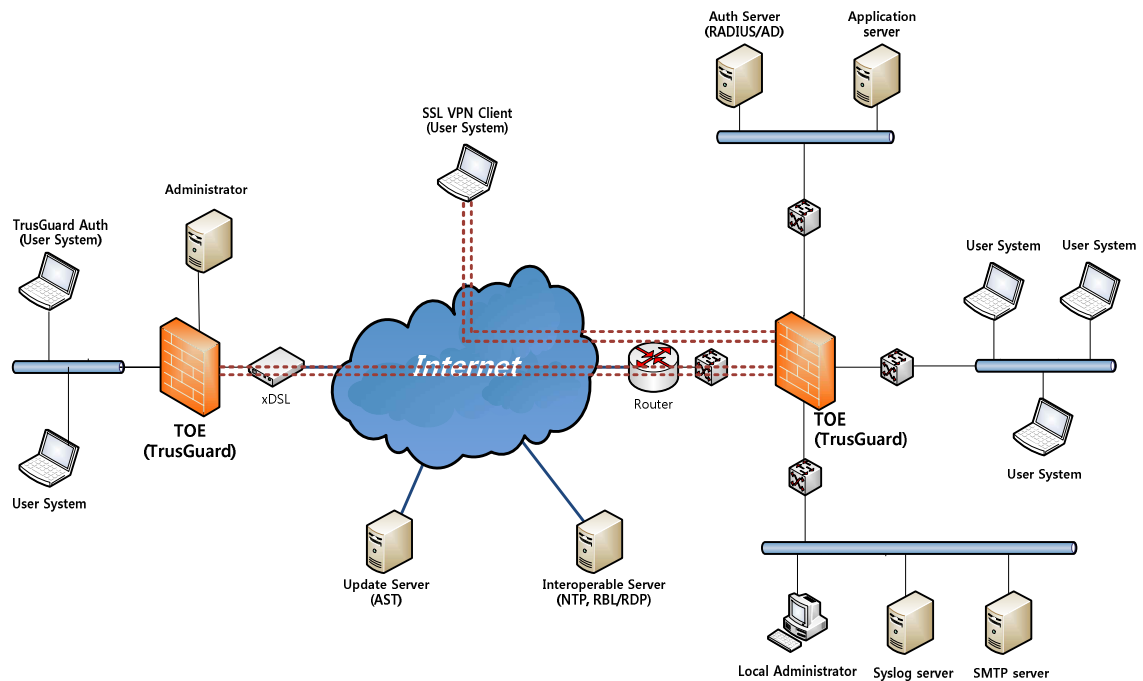
28

The TOE for TrusGuard Gateway is operated on the IPv4 VPN protocol-based operating environment as shown in [Figure 1-4], providing the following security functions.

- VPN
 - IPv4: IPSec VPN, SSL VPN

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	


[Figure 1-4] TOE operating environment examples (IPv4 VPN network)



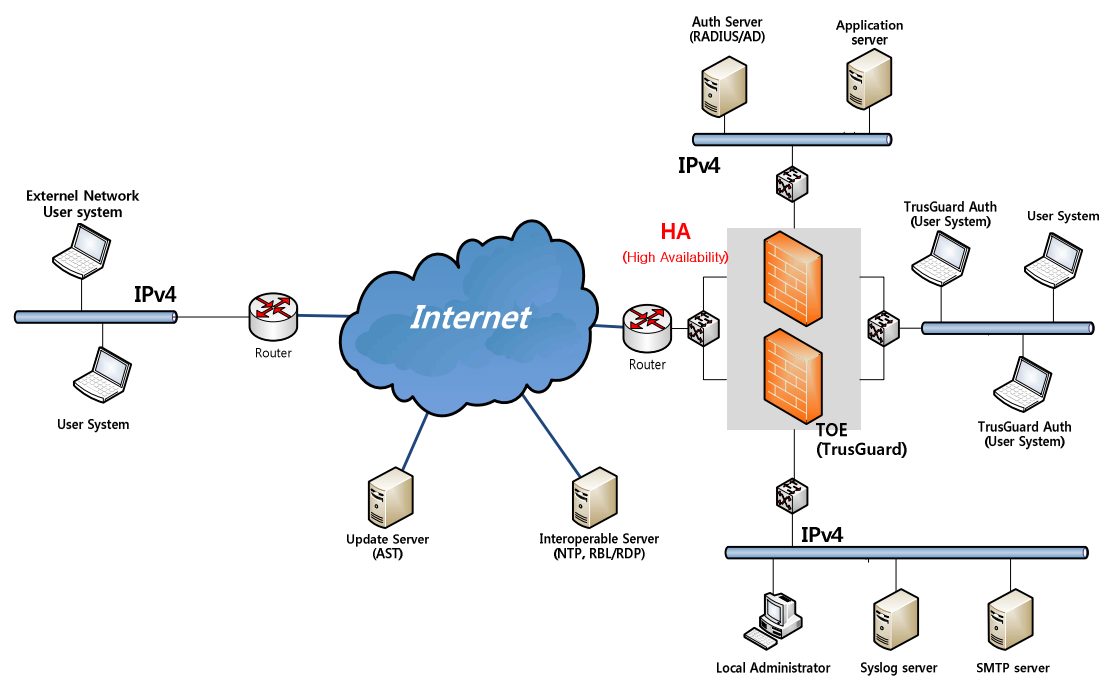
IPv4 HA operating environments

29 The TOE for TrusGuard Gateway is operated in the IPv4 protocol-based HA operating environment as shown in [Figure 1-5], providing the following security functions.

- Access control at network level
 - IPv4: Firewall, Exceptions, Access Block by blacklist
- VPN
 - IPv4: IPSec VPN, SSL VPN
- Other security functions
 - IPv4: Network address translation, Deep Packet Inspection, content filtering, HA, audit data management and security management

	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

[Figure 1-5] TOE operating environment examples (IPv4 HA network)



- 30 The general TOE operating environment example is shown in [Figure 1 1]. The TOE is installed on the network boundary and operated as a single device. To save, manage, and look up audit data, the TOE for TrusAnalyzer is installed and operated in the hardware along with the TOE for TrusGuard Gateway.
- 31 The audit data created upon the TOE operation is managed by TOE for TrusAnalyzer, while the resource operating status information is transferred and managed in the TOE for TrusAnalyzer or the SNMP server. In addition, the audit data managed by the TOE for TrusAnalyzer can be transferred and managed in the SYSLOG server.
- 32 The TOE for TrusGuard Gateway uses only the IPv4 protocol to transfer audit data and resource operating status information. In the dedicated IPv6 network, it is necessary for network ports, the SNMP server, and the SYSLOG server to use IPv4 protocols for transmitting audit data and resource operating status information. In the mixed IPv4/IPv6 protocol-based network, only the IPv4 protocol can support data transmission across the TOEs for TrusGuard Gateway, Authentication Client, and SSL VPN Client.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- 33 [Figure 1-4] shows examples of VPN operating environments. The red line shows that the encrypted secure channels are established by using VPN functions. The TOE supports both IPsec and SSL-based VPN functions. The VPN, however, only can be configured on an IPv4 network.
- 34 The HA operating environment example is shown in [Figure 1-5]. HA supports Active-Active and Active-Standby mode functions depending on configurations. The IPv6 network does not support HA configurations.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.3.3.Non-TOEs required by the TOE

- 35 To operate the TOE in a safe status, the following hardware, firmware and software are required in addition to the evaluation targets.

Hardware for TOE (TrusGuard)

- 36 The TOE for TrusGuard Gateway and the TOE for TrusAnalyzer need to be installed and operated in TOE hardware models. Products containing TOEs can be identified based on the hardware models. The detailed specifications of hardware products are shown in [Table 1-1].

[Table 1-1] TOE hardware models

Type	AhnLab TrusGuard 10000P R(2)
CPU	Intel® Xeon® E5645 Six-Core 2.4 GHz * 2
Memory	4 GB DDR3 Memory * 4
CF	2 GB CF Memory
HDD	2 TB S-ATA2
NIC	<ul style="list-style-type: none"> ● 10/100/1000 BASE-TX * 14 ● 1 Gbps SFP * 8 ● 10 Gbps SFP+ * 2
Console	RJ45 * 1
Size	431.8 mm * 580 mm * 88 mm (W*D*H)
PSU	Redundant, 500W, 5V/30A, 12V/32A, 3.3V/24A

Administrator system

- 37 Authorized administrators use an administrator system in which web browsers or SSH client programs are run to remotely use the security management functions of the TOEs (TrusGuard Gateway and TrusAnalyzer). Serial port-based communication programs should be running to use TOE security management functions via serial ports in the local systems. The specifications for administrator systems (based on Windows XP) are shown in [Table 1-2].

[Table 1-2] Specifications for administrator systems

Category	Type	Description
Hardware	CPU	Pentium 233 MHz processor or faster (300 MHz recommended)

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Memory	64 MB or above (128 MB recommended)
HDD	1.5 GB of free space or above
Network Interface	1 or more TCP/IP-based network ports
Serial Port	RS-232C
Operating system	Microsoft Windows XP or later
Required software	[TOE for TrusGuard Gateway] Terminal software supporting SSH2 or Serial communication Web browsers supporting SSL/TLS: Internet Explorer 7/8/9, Chrome 18.0/19.0 and Firefox 10/11/12 Adobe Flash Player 10
	[TOE for TrusAnalyzer] Web browsers supporting SSL/TLS: Internet Explorer 7/8/9 and Chrome 18.0/19.0 Adobe Flash Player 10

SSL VPN Client and Authentication client installation environments

38 The SSL VPN Client and User Authentication Client of TOE components are installed in general PCs. The specifications for general user PCs are shown in [Table 1-3].

[Table 1-3] Installation specifications for SSL VPN Client and Authentication Client

Category	Type	Description
Hardware	CPU	Pentium 233 MHz processor or faster (300 MHz recommended)
	Memory	64 MB or above
	HDD	1.5 GB of free space or above
	Network Interface	1 or more TCP/IP-based network ports
	Operating system	Windows XP(32/64-bit), Windows Vista(32/64-bit), Windows 7(32/64-bit)
	Required software	Internet Explorer 7/8/9

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Web browser

- 39 Administrators for TOEs (TrusGuard Gateway and TrusAnalyzer) use web browsers for security management. Administrators use SSL/TLS-based security communication options provided by web browsers to securely perform security management. The supported web browsers are the same as the required software products listed in [Table 1-2].

AhnLab Online Security (AOS) - Personal information protection program

- 40 Based upon the SSL VPN security policies set by the authorized administrator, the TOE can force general user PCs to use AhnLab Online Security (AOS) 2.1.26.1, a personal information protection program provided by AhnLab Inc. AOS is supported in the Internet Explorer environment, which is updated and operated in real-time through the AhnLab update server whenever authorized users use the SSL VPN. AOS provides PC Firewall, secure browser, and anti-virus functions.

Flash Player

- 41 The TOEs for TrusGuard Gateway and TrusAnalyzer offer certain functions in Flash Player formats (.swf) when security management graphic user interfaces (GUIs) are provided via web browsers. The latest Flash Player version should be installed and used in the administrator system.

SSH/Serial communication software

- 42 To use the command security management interfaces of the TOE (TrusGuard Gateway), the terminal client software for SSH/Serial communication needs to be installed in the administrator system.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.3.4.Non-TOE external IT entities

43 The TOE for TrusGuard Gateway interoperates with external servers to update its signature and perform TOE security functions. Based upon security policies specified by the authorized administrator, the following systems are additionally required for the TOE operating environment.

- Update server: AST server
- TOE interoperable server: NTP server, anti-spam server (RPD server and RBL server), Syslog server, SNMP Manager server and user authentication server (RADIUS, Active-Directory)

AhnLab Service Tower (AST) server

44 The TOE for TrusGuard Gateway downloads update files from the Content Delivery Network (CDN) through the AST server to update the V3 engine, signature/behavior-based policies, DB files for content classes, and Anti-MalSite files. The AST server is a system that verifies AhnLab TOE customer information and product information and provides update services according to the update requests.

Network Time Protocol (NTP) server

45 The TOE for TrusGuard Gateway selectively uses the NTP server according to the time synchronization method set by the authorized administrator. The NTP server is a networking protocol for clock synchronization between computer systems.

Anti-spam server (RPD server and RBL server)

46 By interoperating with the anti-spam servers (RPD server and RBL server), the TOE for TrusGuard Gateway verifies spam e-mails. The TOE for TrusGuard Gateway sends inspection requests to the interoperable anti-spam server to determine whether incoming e-mails are spam e-mails, checks the inspection results, and handles malicious spam e-mails in accordance with the security policies set by the authorized administrator.

SYSLOG server

47 The TOE for TrusAnalyzer transfers audit data by third parties to the SYSLOG server for audit data management.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Simple Network Management Protocol (SNMP) server

- 48 The TOE for TrusGuard Gateway transfers system status information and network status information by third parties to the SNMP servers or the TOE for TrusAnalyzer according to the SNMP protocol standards.

User authentication server (RADIUS server and AD server)

- 49 If the authorized administrator forces user identification and authentication by interoperating with the external authentication server, then the TOE for TrusGuard Gateway communicates with the RADIUS server or the Active Directory (AD) server for user identification and authentication.

Mail server

- 50 The TOEs for TrusGuard Gateway and TrusAnalyzer send alert e-mails to authorized administrators through the external mail server.

Short Message Service (SMS) server

- 51 The TOE for TrusGuard Gateway sends text messages to authorized administrators through the external SMS server according to the alert settings.

ATM server

- 52 The AhnLab TrusManager (ATM) is an integrated security management program for various AhnLab Inc. network security products. By enabling the environment settings, the TOE for TrusGuard Gateway can use interoperable ATM functions.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.4. TOE descriptions

53 This section provides the physical and logical scopes of the TOE to describe TOE application environments.

1.4.1. Physical scope

54 The TOE is installed and operated in the physical hardware or separate general PCs.

TrusGuard Gateway (TrusGuard Gateway package)

55 Along with the customized operating system (ANOS V2.1) based on Linux Kernel version 2.6.24.7, the TOE for TrusGuard Gateway is installed in a firmware format on the CF memory of the TOE hardware platform to be distributed to end users. The version of TrusGuard Gateway can be identified as below.

- AhnLab TrusGuard Gateway 2.2.0.5

56 The following components are also included in the TOE for TrusGuard Gateway.

- ANOS V2.1: A customized operating system based on Linux Kernel 2.6.24.7, embedded with the AhnLab Inc. Firewall, IPS and Anti-DDoS attack products.
- VPN communication cryptography module: The cryptography module for VPN communication uses the Magic Crypto V1.1.1, OpenSSL 1.0.1e, AhnLab Inc. cryptography library versions. The cryptography algorithms for each cryptography module are listed below.

Library	Type Key exchange (Key length)	Block cryptography (Key length)	Hash function (Key length)
Magic Crypto (IPsec, SSL VPN)	None	SEED (128) ARIA (128, 192, 256)	SHA (160)
AhnLab cryptography library	Diffie-Hellman (1024)	3DES (168) AES (128, 192, 256)	SHA2 (384, 512) HAS160 (160)
Openssl	RSA (1024)	3DES(168)	SHA2 (224)

AhnLab TrusGuard V2.2

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

(SSL VPN)	AES (128, 192, 256)	HAS160 (160)
	Blowfish (128, 448)	

- OpenSSL V1.0.1e: A cryptography module that performs secure encrypted communication between the TOE for TrusGuard Gateway and web browsers during security management
- OpenSSH 6.2p2: A cryptography module that performs secure encrypted communication between the TOE for TrusGuard Gateway and SSH terminal programs during security management
- OPIE 2.32: A module that performs user identification and authentication via one-time password (OTP) authentication between the TOE for TrusGuard Gateway and the TOE for Authentication Client
- Apache 2.2.23: A module that provides web services via administrator or user system browsers for the TOE (TrusGuard Gateway) security management and SSL VPN connection

TrusAnalyzer (AhnLab TrusAnalyzer Package)

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

- AhnLab TrusAnalyzer 1.0.2.12

58 The following components are also included in the TOE for TrusAnalyzer.

- PostgreSQL 9.0.4: DBMS for saving TrusAnalyzer reports and statistics data
- Tomcat 7.0.32: A module that provides web services via administrator system browsers for TrusAnalyzer security management
- OpenSSL V1.0.1e: A cryptography module that performs encrypted secure communication between the TOE for TrusAnalyzer and web browsers during security management

Authentication Client & SSL VPN Client

59 The TOEs for Authentication Client and SSL VPN clients perform user identification and authentication through content filtering functions. The TOE for SSL VPN Client is a software

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

product that performs VPN user client functions. The installations of the TOEs for Authentication Client and SSL VPN Client are packaged with the TOE for TrusGuard Gateway firmware, which are installed and distributed in the user PCs via web browsers upon the use of specific functions. These two software products are identified as below.

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

60 The following components are also included in the TOEs for Authentication Client and SSL VPN Client.

- OpenSSL V1.0.1e: A cryptography module that establishes a secure communication channel between Authentication Client/SSL VPN Client and user systems/TrusGuard Gateway
- OPIE 2.32: A module that performs user identification and authentication via one-time password (OTP) authentication between the TOE for Authentication Client and the TOE for TrusGuard Gateway

User guides

61 To safely manage the TOE, AhnLab provides printed guides to end users. The printed guides distributed to the end users are included in the Physical scope of the TOE and identified as below:

- AhnLab TrusGuard V2.2 Administrator Guide (2013.07.30.01)
- AhnLab TrusGuard V2.2 Command Guide (2013.07.30.01)
- AhnLab TrusGuard V2.2 Product Installation Guide (2013.07.30.01)

62 The AhnLab TrusGuard product installation guide contains installation guidelines for TOE components. The AhnLab TrusGuard Gateway Administrator Guide and the AhnLab TrusGuard Gateway Command Guide contains operation guidelines for the TOE.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

the free space reaches or exceeds a certain threshold to protect the audit data storage.

CS.Cryptographic Support

- 67 The TOE for TrusGuard Gateway safely creates and distributes cryptographic keys and algorithms used between two gateways (IPsec VPN) or between the gateway and the client (SSL VPN). The end-to-end nodes use the distributed session keys to perform cryptographic and integrity checks for transmission data.

DP.User Data Protection

- 68 The TOE for TrusGuard Gateway performs secure communication in accordance with security functional policies to protect data transferred through the public network. IPsec VPN and SSL VPN are provided. IPsec VPN is provided in the tunnel mode to establish a secure IPsec tunnel between gateways, while SSL VPN establishes secure SSL communication channels between the gateway and the host to ensure the user data cryptography and integrity.
- 69 Traffic filtering security functional policies verify IP addresses, service protocols and ports, security classes, and time of all incoming/passing/outgoing packets of TrusGuard Gateway, and control them in accordance with security policies set by the authorized administrator. It interoperates with policy exceptions, network address translation, signature/behavior-based block, abnormal packet detection/block, and traffic filtering functions to block abnormal packets or handle packets transferred between communication targets.
- 70 The TOE for TrusGuard Gateway examines application-level information received from external networks according to content filtering security functional policies to perform malicious code scans, spam e-mail scans, http content/URL scans, and command blocking functions. If user authentication is needed for HTTP, FTP and TCP general proxies, then it only allows information flows for users identified and authorized with IDs, passwords, or one-time passwords (OTP).

IA.Identification and Authentication

- 71 The TOE for TrusGuard Gateway should identify and authorize users wishing to use security management functions before performing any actions. It protects authentication feedback when users enter authentication data and provides safe identification and authentication functions when authentication fails consecutively.
- 72 It also handles user identification and authentication requests received from the TOEs for

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Authentication Client and SSL Client, allowing for information flow control of user systems. The TOE for Authentication Client performs user identification and authentication using IDs, passwords, or one-time passwords (OTP) of general users, while the TOE for SSL Client performs user identification and authentication uses IDs, passwords, and certificates. The TOE for TrusGuard Gateway provides user identification and authentication functions by interoperating with external authentication servers such as RADIUS and Active Directory for user identification and authentication for the TOE for Authentication Client.

MT.Security Management

- 73 The TOE classifies security management functions as "security functional management", "security attribute management", and "TSF data management".

✓ Security Functional Management

- 74 The TOE for TrusGuard Gateway provides the authorized administrator with functions to change, stop, and resume behavior settings of each TOE security function. The authorized administrators can be classified into two groups: TG top-level administrators and TG general administrators. The assigned security functional management differs, depending on the role.

✓ Security Attribute Management

- 75 To partially control information flows of passing TOE packets, the TOE (TrusGuard Gateway) limits query, change, and deletion capabilities of subjects and information security attributes based upon security roles specified by the authorized administrators. The subjects and information security attributes are source IP addresses, destination IP addresses, IDs, passwords, services (protocols and ports), packet data (headers and payloads), and time. The TG top-level administrators have full permissions (query, change and deletion) and the TG general administrators have query-only permission.

✓ TSF Data Management

- 76 The TOE provides authorized TG top-level administrators and TG general administrators with functions to query, change, delete, and change audit data and TSF data list managed by the TOE based upon their permissions.

PT.TSF Protection

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- 77 The TOE for TrusGuard Gateway periodically perform self-testing to check the process status during regular operation to ensure the normal and safe operation of security functions when the system restarts. It also performs integrity check for TSF data and TSF execution codes.

TA.TOE Access

- 78 The TOE for TrusGuard Gateway terminates the interactive administrator sessions that are idle for the specified inactive period.

TP.Trusted Path/Channel

- 79 The TOE for TrusGuard Gateway establishes secure paths and channels between trusted IT entities or TSFs to protect channel data from unauthorized changes or disclosure. IPsec VPN communication creates an IPsec tunnel between two TOEs for TrusGuard Gateways to establish VPN connection, whereas SSL VPN communication creates an SSL tunnel to establish a safe channel. Secure path/channels is used for TLS connection, between the administrator system web browser and TrusGuard Gateway, and SSH/console connection, between SSH (Secure Shell) terminal programs and TrusGuard Gateway, to provide safe paths.

TrusAnalyzer

AU.Security Audit

- 80 The TOE for TrusAnalyzer generates audit data for security management actions by authorized administrators and receives audit data from the TOE for TrusGuard Gateway. Authorized administrators search and query audit data managed by the TOE for TrusAnalyzer.
- 81 The TOE for TrusAnalyzer provides protection functions for audit data storage to prevent audit data loss. To protect audit data against unauthorized deletion, modification, or loss, the TOE for TrusAnalyzer deletes the oldest data if the free space reaches or exceeds a certain threshold to protect the audit data storage.

IA.Identification and Authentication

- 82 The TOE for TrusAnalyzer identifies and authenticate administrators based on IDs and passwords. The TOE delays user authentication for a specified time period (default value: 5 minutes) after the specified number of failed authentication attempts (default value: 5 times) to block malicious accesses.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

MT.Security Management

- 83 The TOE for TrusAnalyzer classifies security management functions as "security functional management" and "TSF data management".

✓ Security Functional Management

- 84 The TOE for TrusAnalyzer provides authorized administrators with functions to change, stop, and resume behavior settings for each security function. Authorized administrators are classified as TrusAnalyzer top-level administrators and TrusAnalyzer general administrators. TrusAnalyzer top-level administrators have full permissions such as security function setup, while TrusAnalyzer general administrators have query-only permission for managing equipment.

✓ TSF Data Management

- 85 The TrusAnalyzer provides authorized users (TrusAnalyzer top-level administrators and TrusAnalyzer general administrators) with limited capabilities to query, change, delete, and create audit data and TSF data list based on their permissions. TrusAnalyzer top-level administrators have full permissions for all actions, while TrusAnalyzer general administrators have partial permissions to change settings for selected equipment, create, change and delete integrated reports, and query logs and reports.

TA.TOE Access

- 86 The TOE for TrusAnalyzer terminates administrator sessions that are idled for the specified inactive time period (10 minutes) to restrict and protect administrator sessions.

TP.Trusted Path/Channel

- 87 The TOE for TrusGuard Gateway establishes a secure path for TLS communication between the administrator system web browser and the TOE to protect data from unauthorized changes or disclosure while administrators perform security management.

Authentication Client

IA.Identification and Authentication

- 88 The TOE for Authentication Client provide authentication data protection functions for user

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

identification and authentication, and it creates authentication data by computing response values for identification and authentication challenges through one-time-passwords (OTP).

MT.Security management

- 89 The TOE for Authentication Client allows TrusGuard Auth users that are authorized by using TSF data management functions to change passwords.

TA.TOE Access

- 90 The TOE for Authentication Client terminates user sessions if TrusGuard Auth users do not perform any action for the specified inactive period (default value: 30 minutes).

TP.Trusted Path/Channel

- 91 The TOE for Authentication Client establishes a secure channel for TLS communication between TOEs for TrusGuard Gateway to protect channel data from unauthorized change or disclosure.

SSL VPN Client

CS.Cryptographic Support

- 92 The TOE for SSL VPN safely creates and distributes cryptographic keys and algorithms used in sessions to provide SSL VPN functions through user PCs. The end-to-end nodes use the distributed cryptographic keys to perform cryptographic and integrity checks for transmission data and destroy expired keys.

DP.User Data Protection

- 93 The TOE for SSL VPN Client performs secure communication to protect transmission data when communicating with the TOE for TrusGuard Gateway. Based upon the VPN security functional policies set by authorized administrators for incoming/outgoing data, it provides user data cryptography and integrity.

IA.Identification and Authentication

- 94 The TOE for SSL VPN Client provides authentication data protection functions for user identification and authentication.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

MT.Security Management

- 95 The TOE for SSL VPN Client provides authorized SSL VPN users with capabilities to change passwords or change/query TSF setting values.

TA.TOE Access

- 96 The TOE for SSL VPN Client terminates sessions if the authorized users do not perform any security management action for the specified inactive period (default value: 5 minutes).

IA.Identification and Authentication

- 97 The TOE for SSL VPN Client establishes a secure channel for TLS communication between TrusGuard Gateway and SSL VPN to protect channel data from unauthorized changes or disclosure.

non-TSF. Non-security functions

- 98 Multi-language support, a packet analysis utility, network port settings, network connection settings and DHCP are included in the non-security functions.
- Multi-language support: The TOE for TrusGuard Gateway supports multi-language environments including Korean, English and Chinese environments.
 - Packet analysis utility: The packet analysis utility exists as firmware in the hardware along with the TOE (TrusGuard Gateway). It captures images of information flow passing through network ports.
 - DHCPv4/DHCPv6: DHCPv4/DHCPv6 exists as firmware in the hardware along with the TOE (TrusGuard Gateway). The DHCPv4/DHCPv6 function dynamically distributes or arbitrates IP addresses in the IPv4 network or IPv6 network environments. DHCPv6 can be used with RA.
 - RA: The RA function exists as firmware in the hardware along with the TOE (TrusGuard Gateway). It also supports network configurations which enable it to send RA messages for network hosts/nodes to automatically generate IPv6 addresses in the IPv6 network environment. RA can be installed separately or together with DHCPv6.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.5. Conventions

99 The notation, forms and writing conventions conform with the Common Criteria for Information Technology Security Evaluation. To clearly distinguish carried-out operations from the Protection Profile that this ST has referred to, additional writing conventions can be defined and utilized.

100 The Common Criteria allows operations to be selected, allocated, refined and repeated to meet Security Functional Requirements.

101 Each operation can be used in this Security Target as below:

Iteration

102 Used when the same components are repeated in various operations. The repeated operations outputs are displayed as a specific number of times enclosed within brackets (Number of times repeated) after the component identifier.

Selection

103 Used to select more than one item from selections provided by the Common Criteria for Information Technology Security Evaluation when you write down requirements. Select operation outputs are displayed in underline and italics.

Refinement

104 Used to limit requirements by adding details in the requirements. **Refine** operation outputs are displayed in **bold**.

Assignment

105 Used to allocate specified values to unclaimed parameters (ex: Password length). Allocation operation outputs are displayed with angle brackets. Example: [Assignment_value].

106 The Protection Profile that this ST complies to clearly identifies security requirements, provides selection information for implementation and provides application notes to define "Fit/Unfit" criteria for such requirements. The application notes are described with the requirement, if necessary.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

1.6. Terms and Definitions

107 If terms used for this Security Target are the same as the ones for the Common Criteria and Protection Profile, then those term definitions also comply with the Common Criteria terminology and will not be described herein.

Administrator system

108 An administrator system that accesses the TOE to remotely control security management functions to set and monitor TOE security policies. Web browsers and SSH/Serial connection programs are installed in the administrator system to support security management functions, and only authorized administrator systems can access the TOE, as administrator IPs are restricted.

Network Address Translation (NAT)

109 A function that translates internal IP addresses into public IP addresses to protect the internal network. With this function, a node without assigned addresses is able to access the Internet. Based upon the administrator's settings, NAT translates internal network IP addresses and services into external IP addresses or services with dynamic and static NAT commands. The TOE provides the Network Address Conversion function to both IPv4 environments and IPv6 environments.

Quarantine

110 This system quarantine function restricts network service usage of hosts that cause abnormal traffic.

Network hosts

111 The network host is a computer capable of bi-directional communication with other computers through the Internet. Unique IP addresses can be formed by combining specific host numbers with network numbers. The host is a single network node. Specifically, user computers accessing or participating in the Internet network are called Internet hosts.

Web Browsers

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

112 Web browsers are client application programs that can search information on websites (WWW, Worldwide Web). They search, save and transfer materials between Internet users and web servers. Internet Explorer, Firefox and Google Chrome are currently the most popular Internet browsers.

External Entity

113 External entities are external users or IT entities who can interact with the TOE. In this document, if the external entities are 'IT entities', then those entities are written as 'IT entities'.

Authorized users

114 Authorized administrators, authorized log administrators and authorized general users are included as authorized users.

Authorized Administrator

115 An authorized user who safely operates and manages the TOE according to Security Functional Requirements (SFR). In addition, authorized users who safely operate and manage the TOE for TrusGuard Gateway are also called authorized administrators. In this case, the TOE classifies authorized administrators as TG top-level administrators and TG general administrators based upon their permissions. TG top-level administrators have full permission (Read/Write) to use all security management functions. TG general administrators who have read-only permissions can run some critical commands like update or query TOE operation policies.

Authorized log administrator

116 Authorized administrators who safely operate and manage the TOE for TrusAnalyzer (one of TOE components) where audit data is stored separately. TOE administrators for TrusAnalyzer are categorized into TrusAnalyzer top-level administrators and TrusAnalyzer general administrators. TrusAnalyzer top-level administrators have full permission to use all security management functions, while TrusAnalyzer general administrators can have a read-only permission for audit and statistics data and device management permission to manage selected devices.

Authorized general user

117 Authorized general users can be classified into SSL VPN users and TrusGuard Auth users. SSL VPN users are those who go through identification and authentication processes to use SSL

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

VPN, while TrusGuard Auth users are users who pass identification and authentication processes based on IDs and passwords when the content filtering function forces user authentication.

Access control at Network Level (Firewall system)

- 118 A software/hardware-based network security system (called a firewall) implemented on network gateways in in-line mode to protect internal networks connected to the Internet against malicious intrusions. Based upon IP addresses and port numbers, the Firewall system blocks all traffic that does not match rules allowed by authorized administrators. It allows connections from the internal network to the external network but blocks connections from the external network to the internal network to protect internal network resources from security threats.

HA (High Availability)

- 119 High Availability is a system or a component that can be operated continuously during a contractual measurement period. Availability can be used as "100% available" or "Never out of order ". Currently 99.999% (often called "Five 9s") refers to a desirable percentage of availability of given systems or products, which cannot be easily achieved. The TOE introduces HA to ensure high availability of networks and operates in Active-Standby or Active-Active mechanism, according to its configuration.

IT Entity

- 120 IT entities that receive/send information through the TOE. TOE security policies for information flow control are applied. External IT entities that can interact with the TOE are called 'IT entities'.

Serial communication

- 121 Serial communication is the process of sequentially transferring data one bit at a time over communication channels or computer buses. The TOE provides a serial communication based on RS-232 standards. RS-232 is a serial port interface used for sound coupler or modem connections.

Spam

- 122 Spam (called spam mails) is advertising bulk e-mails that are sent to numerous recipients by e-mail. Unsolicited bulk e-mails are named "junk e-mails" because they are randomly sent to a great number of users on computer networks. Junk e-mails burden recipients with time and

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

effort needed to eliminate annoying unwanted messages.

Deep Packet Inspection (DPI)

- 123 The Deep Packet Inspection (DPI) is a technology for verifying not only packet headers and payloads but also internal contents to detect and block the following: packets with abnormal traffic violating the availability of internal computing resources and network resources, packets spreading worm/Trojan Horse malware, and network packets with abnormal structures based on protocols. Using signature/behavior-based deep packet inspection functions, the TOE can handle abnormal traffic based on security policies set by the authorized administrator.

DoS (Denial of Service)

- 124 *Denial of Service* (DoS) is a malicious attack to paralyze a system and make its resources unavailable. Dos attacks generally interrupt or suspend services by creating excessive connections to a specific server or using up all its TCP connections. Also, when an attacker uses multiple systems to simultaneously launch attacks against other systems, it is classified as Distributed DoS (DDoS) and is also included in Dos attacks.

Recurrent Pattern Detection (RPD)

- 125 An anti-spam technology developed in consideration of the fact that spam mails might be distributed widely. It collects e-mail traffic information worldwide to detect bulk mails with spam patterns. Furthermore, the RPD classifies risk of e-mails with distribution patterns and filters 98% of spam mails, including intelligent spam mails with attachments (ex. GIF images). This technology is pioneered by Commtouch.

Real-time Black List (RBL)

- 126 Real-time Black List is a system that sends RBL results to requested systems after checking incoming server IP addresses against its own real-time black list. The system collects and registers in its RBL server IP addresses of specific organizations or companies which send spam mails.

Secure Socket Layer (SSL)

- 127 Secure socket layer is a standard protocol to safely send and receive data between world-wide web browsers and web servers. Netscape Communications pioneered this technology and major

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

web product providers including Microsoft are adopting this technology. SSL can be applied to not only web-based products but also to File Transfer Port (FTP) and other application services, which provide channel cryptographic functions such as mutual authentication, data cryptographic and integrity check. The authentication is a function to verify identity of web browsers and web servers. The identification of the virtual store using web browsers and web server can be verified through authentication processes. With the cryptographic function, the risk of data disclosure is minimized and unintentional change of data can be prevented through integrity check.

VPN SFP

- 128 VPN SFP are security functional policies to handle incoming and outgoing TOE VPN traffic based upon security rules set by authorized administrators, which can be classified into IPsec VPN functions and SSL VPN functions. VPN SFP establishes secure communication channels between TOE components (TrusGuard Gateway, SSL VPN Client). It identifies communication targets and perform authentication, replaces cryptographic keys and sends/receives packets after establishing secure channels. VPN SFP ensures confidentiality and integrity of data through cryptographic and hashing.

Traffic filtering SFP

- 129 The traffic filtering SFP are security functional policies to handle incoming/passing/outgoing TOE traffic in accordance with security rules specified by the authorized administrator, which can be classified as Access control at Network Level functions and deep packet inspection functions. Access control at Network Level functions consist of IPv4/IPv6 firewall, network address translation, policy exceptions, access blocking, IPv4/IPv6 conversion, traffic control (QoS), signature/behavior-based blocking functions, and each rule can be defined as a Access control at Network Level rule.

Content filtering SFP

- 130 Content filtering SFP are security functional policies to handle TOE passing-through traffic via application proxy function based upon content filtering rules set by the administrator. Ant-virus, anti-spam, website filtering and anti-malsite filtering functions are provided for DNS, FTP, General, HTTP, POP3, SMTP, SQL*Net and UDP proxies.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

2. Conformance Claims

- 131 The chapter will describe conformance claims for the Common Criteria, Protection Profile and Package that this Security Target complies to.

2.1. Common Criteria Conformance

- 132 This Security Target conforms to the following Common Criteria for Information Technology Security Evaluation V3.1 revision 4.

Common Criteria

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general models, Version 3.1r4, 2012. 9, CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements Version 3.1r4, 2012. 9, CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Assurance requirements Version 3.1r4, 2012. 9, CCMB-2012-09-003

Common Criteria Conformance

- Common Criteria for Information Technology Security Evaluation part 2
- Common Criteria for Information Technology Security Evaluation part 3

2.2. Protection Profile Conformance

- 133 This Security Target does not conform to the requirements of other Protection Profiles.

2.3. Package Conformance

- 134 This Security Target conforms to the following assurance requirements package.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- Assurance package: EAL2 conformance

2.4. Supporting rationale for conformance claim

135 This Security Target does not claim the conformance of other Protection Profiles, so a supporting rationale for conformance claim is not required.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

3. Security Problem Definitions

136 This chapter will define security threats, assumptions and organizational security policies to be addressed by the TOE and TOE operating environments.

3.1. Threats

137 The term Threat Agent is used to indicate an individual or IT entity that attempts to damage confidentiality and integrity of outgoing data, or illegally access and exploit TOEs and internal assets from outside. The threat agent is fundamental to identify who has professional knowledge, assets and motivations.

T.Disguise

138 The threat agent can approach the TOE disguised as an authorized user or communication target.

T.Recording failure

139 The threat agent can prevent the recording of TOE security-related events by completely exhausting storage capacity.

T.Illicit information import

140 The threat agent has the ability to infiltrate into internal networks by inserting prohibited harmful information from outside.

T.Illicit information export

141 Internal users can illicitly send confidential information via networks.

T.Decoding

142 The threat agent can access to outgoing data through decoding attacks.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

T.Consecutive authentication attempts

- 143 The threat agent can acquire authorized user permission by consecutively attempting user authentication for TOE access.

T.Damage to saved TSF data

- 144 The threat agent can disclose, modify and delete TSF data saved in the TOE using unauthorized methods.

T.Damage to transferred TSF data

- 145 The threat agent can illegally disclose and modify TSF data that the TOE is transferring via networks.

T.Transfer integrity

- 146 The threat agent can illegally modify user data that the TOE is transferring via networks.

T.Address disguising

- 147 The threat agent on an external network can attempt to acquire internal network access permission by disguising external source addresses with internal addresses.

T.Abnormal packet dispatch

- 148 The threat agent can cause system failures on internal networks by transferring network packets with abnormal structures.

T.Denial of Services (DoS) attacks

- 149 The threat agent can interrupt users and services by excessively consuming service resources of internal computer networks in the TOE operating environments.

T.User session hijacking

- 150 The threat agent can illegally access to the TOE by hijacking idle sessions of authorized users.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

3.2. Organizational Security Policies

151 Organizational Security Policies imposed by an organization in TOE operating environment will be explained in the following section.

P.Audit

152 To trace down all security-related behaviors and responsibilities, security-related events or incidents should be recorded, retained and reviewed.

P.Secure Management

153 It is required to provide effective management tools and methods, so authorized administrators can safely manage the TOE.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

3.3. Assumptions

154 In the section below, assumptions required for TOE operating environments are described to provide appropriate security functionality.

A.Physical security

155 The TOE and administrator systems are placed in physically safe environments where only authorized administrators can access them.

A.Constant security

156 The security level should be maintained steadily even when internal network environments are changed (ex. network configuration changes, host increase and service increase/decrease) by immediately applying environmental changes and security policy changes to TOE operating policies.

A.Trusted administrator

157 Authorized TOE administrators who are properly trained to use TOE management functions with good intentions can perform their roles and responsibilities in accordance to the administrators' guidelines.

A.Enhance operating systems

158 The operating systems for the TOEs (TrusGuard Gateway and TrusAnalyzer) provide reliability and high availability by addressing OS vulnerabilities and removing unnecessary services. The operating sub-systems of the TOEs (Authentication Client and SSL Client) are safe and reliable.

A.Safe TOE external server

159 AST servers for update and customer license verification, NTP servers for trusted timestamps, user authentication server for user authentications, anti-spam servers for proxy functions, mail servers for alarm messages and SMS server are safely managed to provide reliability.

A.Sole Connection Point

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

160 All communications between external networks and internal networks are possible only via the TOE.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

4. Security objectives

161 This Security Target classifies and defines security objectives as two types: the TOE security objectives and the operating environment security objectives. TOE Security objectives are directly addressed in the TOE, while operating environment security objectives address technical/procedural methods supported by operating environments to accurately provide TOE security functionality.

4.1. TOE Security objectives

162 The following section describes security objectives that should be addressed by the TOE.

O.Audit

163 The TOE should provide tools or methods to review audit data, as well as to record and keep security-related events in order to trace security-related behaviors and responsibilities.

O.Management

164 The TOE should provide authorized administrators with management methods to effectively manage the TOE.

O.Data protection

165 The TOE protects TSF data saved in TOE from disclosure, modification and deletion. Furthermore, the TOE should guarantee confidentiality and integrity of TSF data and user data on networks.

O.Identification and authentication

166 The TOE should identify users and perform authentication before allowing user accesses to the TOE, and perform mutual authentication before establishing a tunnel with communication targets.

O.Information flow control

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

167 The TOE should control the unauthorized incoming and outgoing data between internal and external networks.

O.Key security

168 The TOE should guarantee confidentiality and integrity of cryptographic key related data and ensure safe key exchanges.

O.Block abnormal packets

169 The TOE should block TOE packets with abnormal structures.

Application Notes: Abnormal packets means packets disguised with internal IP addresses, broadcasting packets, looping packets or packets that are not TCP/IP packets defined in Internet standard protocols such as RFC 791 (Internet protocol), RFC 792 (Internet control message protocol), and RFC (Transmission control protocol).

O.Block Denial of Services (DoS) attacks

170 To ensure safe access to computer network services protected by the TOE, malicious DoS attacks that exploit computer service resources excessively or abnormally should be blocked by the TOE.

O.Protect user sessions

171 The TOE should terminate inactive user sessions which are idle for the specific session timeout period.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

4.2. Security Objectives for the Operational Environment

172 This section will explain operating environment security objectives that address technical/procedural methods supported by operating environments to accurately provide TOE security functions.

OE.Physical security

173 The TOE and administrator system should be located in physically safe environments where only authorized administrators can access them.

Application notes: The VPN client should be safely managed by VPN client administrators (authorized general users) based upon security policies of network devices.

OE.Constant security

174 The security level should be maintained steadily even when internal network environments are changed (ex. Network configuration change, host increase and service increase/decrease) by immediately applying environmental changes and security policy changes to TOE operating policies.

OE.Security policy

TOE communication targets should maintain their security policies interoperable with TOEs. Interoperable security policies mean security policies that are identical but limited.

OE.Trusted administrator

175 Authorized TOE administrators who are properly trained to use TOE management functions with good intentions can perform their roles and responsibilities in accordance to the administrators' guidelines.

OE.Enhance operating systems

176 The operating sub-systems of the TOEs for Authentication Client and SSL Client should be safe and reliable through OS enhancement.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

OE.Sole Connection Points

- 177 All communications between external networks and internal networks are possible only via the TOE.

OE.Timestamp

- 178 The TOE should accurately record security-related events with timestamps provided by TOE operating environments.

OE.DBMS

- 179 To save audit data, the TOE should safely manage DBMS interoperating with the TOE for TrusAnalyzer.

OE.Safe TOE external server


- 180 AST servers for update and customer license verification, NTP servers for trusted timestamps, user authentication server for user authentications, anti-spam servers for proxy functions, mail servers for alarm messages and SMS server are safely managed to provide reliability.

4.2.1.Security Objectives Rationale

- 181 The supporting rationale for security objectives justifies that the described security objectives are not excessive but suitable and sufficient enough to handle security issues. Supporting rationale of security objectives proves the following facts.

- Each assumption, threat and Organizational Security Policies (OSP) is addressed by at least one security objective.
- Each security objective addresses at least one assumption, threat and Organizational Security Policies (OSP).

[Table 4-1] Security issue definitions and security objective countermeasures

	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

<div>Security objectives</div> <div>Security environments</div>	TOE Security objectives										Security Objectives for the Operational Environment					
	O.Audit	O.Management	O.Data protection	O.Identification and authentication	O.CONTROL INFORMATION FLOW	O.Key security	O.Block abnormal packets	O.Block Denial of Services (Dos) attacks	O.Protect user sessions	OE.Physical security	OE.Constant security	OE.Trusted administrator	OE.Enhance operating systems	OE.SOLE CONNECTION POINTS	OE.TIMESTAMP	OE.Safe TOE external server
T.Disguise				X												
T.Recording failure	X															
T.Illicit information import					X											
T.Illicit information export					X											
T.Decoding						X										
T.Consecutive authentication attempts				X												
T.Damage to saved TSF data			X													
T.Damage to transferred TSF data			X													
T.Transfer integrity			X													
T.Address disguising							X									
T.Abnormal packet dispatch							X									

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Security objectives	TOE Security objectives										Security Objectives for the Operational Environment				
T.Denial of Services (DoS) attacks								X							
T.Administrator Session hijacking									X						
P.Audit	X													X	
P.Safe management		X									X				
A.Physical security										X					
A.Constant security											X				
A.Trusted administrator												X			
A.Enhance operating systems													X		
A.Safe TOE external server															X
A.Sole Connection Point														X	

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

4.2.2.TOE Security Objectives Rationale

182 The supporting rationale and the details for TOE security objectives will be described in the following section.

O.Audit

183 As the TOE provides methods to accurately record, retain and review TOE security-related events, this TOE security objective is required to rapidly handle Threats T.Recording failure and perform Organizational Security Policies (OSP) P.Audit.

O.Management

184 As the TOE provides TOE authorized administrators with safe TOE management methods, this TOE security objective is required to perform Organizational Security Policies (OSP) P.Safe management.

O.Data protection

185 As the TOE prevents unauthorized disclosure, modification and deletion of TSF data saved in the TOE, this TOE security objective is required to rapidly handle situations of T.Damage. It is also required to handle Threats T.Damage transferred TSF data and T.Transfer integrity since the TOE ensures the confidentiality and integrity of TSF data and user data on networks.

O.Identification and authentication

186 As the TOE ensures identification and authorization of authorized administrators and other TOEs that are communicating with itself, this TOE security objective is required to rapidly handle Threats T.Disguise.

O.Information flow control

187 As the TOE controls information flow based on its security policies, this TOE security objective is required to handle Threats T.Illicit information import, T.Illicit information export and T.Address disguising.

O.Key security

188 As the TOE provides confidentiality and integrity of cryptographic keys and ensures appropriate

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

key exchanges, this TOE security objective is required to handle Threats T.Decoding.

O.Block abnormal packets

- 189 This TOE security objective ensures blocking of abnormal packets such as: packets disguised with internal IP addresses, broadcasting packets, looping packets and packets that are not TCP/IP packets among numerous incoming packets from external networks. This TOE Security objective is required to handle Threats T.Abnormal packet dispatch and T.Address disguising.

O.Block Denial of Services (DoS) attacks

- 190 The TOE prevents a particular user from dominating computer resources to ensure use of the computer by normal users. This TOE security objective is required to handle Threats T.Denial of Services (DoS) attacks.

O.Protect administrator sessions

- 191 The TOE terminates inactive administrator sessions that are idle for the specified timeout period to prevent threat agents from hijacking sessions illegally. This TOE security objective is required to handle Threats T.Hijacking administrator sessions.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

4.2.3.Security Objectives for the Operational Environment

192 This section will introduce the supporting rationale and details for operating environment security objectives.

OE.Physical security

193 As the TOE ensures physical safety, this operating environment security objective is required to support Assumptions A.Physical security.

OE.Constant security

194 As this operating environment security objective ensures security level to be maintained steadily even when internal network environments are changed (ex. Network configuration changes, host increase and service increase/decrease) by immediately applying the environmental changes and security policy changes to TOE operating policies, it is required to support Assumptions A.Constant security.

OE.Trusted administrator

195 As this operating environment security objective guarantees authenticity of TOE authorized administrators, it is required to perform management actions for Organizational Security Policies (OSP) P.Secure Management and support Assumptions A.Trusted administrator.

OE.Enhance operating systems

196 As this operating environment security objective offers guaranteed stability and reliability of operating systems by addressing OS vulnerabilities and removing all unnecessary services or methods, it is required to support Assumptions A.Enhance operating systems.

OE.Sole Connection Point

197 As this operating environment security objective ensures all communications between internal networks and external networks can be made only through the TOE, it is required to support Assumptions A.Sole Connection Point.

OE.TIMESTAMP

198 As this operating environment security objective ensures the TOE to accurately recode security-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

related events using timestamps provided by the TOE operating environment, it is required to perform Organizational Security Policies (OSP) P.Audit.

OE.Safe TOE external server

- 199 As this operating environment security objective ensures the TOE to accurately operate security functions using trusted safe TOE external servers provided by TOE operating environments, it is required to support Assumptions A.Safe TOE external server.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

5. Extended component definition

200 This Security Target does not include components that are extended in the Common Criteria for Information Technology Security Evaluation part 2 and part 3.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6. Security requirements

201 This chapter describes the functions and the assurance requirements to be satisfied by the TOE.

6.1. Security functional requirements

202 In order to meet all security objectives identified in chapter 4, the security functional requirements defined in this ST selected and represented the related functional components from the extended components of chapter 5 and CC Part 2. The following table shows a summary of the security functional components used in this ST:

[Table 6-1] Security functional requirements for Security Target

Class	Component ID	Name
Security audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
Cryptographic operation	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User data protection	FDP_IFC.1(1)	Subset information flow control (1)
	FDP_IFC.1(2)	Subset information flow control (2)
	FDP_IFC.1(3)	Subset information flow control (3)
	FDP_IFF.1(1)	Simple security attributes (1)
	FDP_IFF.1(2)	Simple security attributes (2)
	FDP_IFF.1(3)	Simple security attributes (3)

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Identification and authentication	FIA_AFL.1(1)	Authentication failure handling (1)
	FIA_AFL.1(2)	Authentication failure handling (2)
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (1)
	FMT_MTD.1(2)	Management of TSF data (2)
	FMT_MTD.2	Management of limits on TSF data
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_TST.1	TSF testing
TOE access	FTA_SSL.3	TSF-initiated termination
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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 the [countermeasures specified in [Table 6-2]] upon detection of a potential security violation.

[Table 6-2] Countermeasures upon detection of a potential security violation.

Functional component	Auditable events	Countermeasures
FAU_SAA.1	- CPU usage is higher than the alert level.	Send alert e-mail /alert SMS
	- Memory usage is higher than the alert level.	
	- Disk usage is higher than the alert level.	
	- HA status is changed.	
	- Log level is higher than the selected value.	
	- Power supply equipments have failed.	
	- The alert network port's connection is disconnected.	
FDP_IFF.1(3)	- The number of sessions is higher than the alert level.	Alert e-mail
	- Detect spam mail blocking in the log file.	

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.

- Start-up and shutdown of the audit functions;
- All auditable events for the *Not specified* level of audit; and
- ["Auditable events" in [Table 6-3]].

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

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- 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 ST, please refer ["Additional Audit data" in [Table 6-3]].

[Table 6-3] Auditable events

Functional component	Auditable events	Additional Audit data
FAU_ARP.1	Countermeasures taken as the result of critical security violation	Recipient identification of countermeasures
FAU_SAA.1	Analysis mechanism start and finish, and automatic countermeasures by tools	-
FAU_SEL.1	Audit environments setting changes during audit data collection	-
FCS_CKM.1	Action results (success or failure)	-
FCS_CKM.2	Action results (success or failure)	Assume recipients' identification
FCS_CKM.4	Action results (success or failure)	-
FCS_COP.1	Cryptographic operation results (success or failure), cryptographic operation types	-
FDP_IFF.1(1)~(3)	Determination of information flow requests	Object identification information
FIA_AFL.1(1)~(2)	Countermeasures taken after a specific number of unsuccessful user authentication attempts, service delay and resume if required.	-
FIA_SOS.1	Deny all passwords tested by TSF	-
FIA_UAU.2	Usage all of authentication mechanisms	-
FIA_UAU.4	Authentication data re-usage attempts	-
FIA_UID.2	User identification and usage of all user identification mechanisms	-
FMT_MOF.1	All TSF function changes	-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Functional component	Auditable events	Additional Audit data
FMT_MSA.1	All changes of security attributes values	Changed security attributes values
FMT_MTD.1(1)~(2)	All changes of TSF data values	Changed TSF data values
FMT_MTD.2	All changes of TSF data thresholds	Changed TSF data thresholds
FMT_MTD.3	All values denied as TSF data	-
FMT_SMF.1	Management function usage	-
FMT_SMR.1	Changes of user groups for role assignment	-
FPT_TST.1	TSF self-test execution and test results	Changed TSF data or execution codes upon violation of integrity
FTA_SSL.3	Disconnection of interacting sessions according to session locking mechanism	-

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

- a) Accumulation or combination of [audit events violating control rules among auditable events in FDP_IFF.1(3)] known to indicate a potential security violation;
- b) [
 - CPU usage is higher than the alert level.
 - Memory usage is higher than the alert level.
 - Disk usage is higher than the alert level.
 - HA status is changed.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- Log level is higher than the selected values
- Power supply equipments have failed.
- The alert network port's connection is disconnected.
- The number of sessions is higher than the alert level.]

Application notes: As for control-rule violation events applied by these security functional requirements, a) TrusAnalyzer sends alert e-mails with the Anti-Spam log of TrusGuard Gateway to alert security violation.

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 [authorized administrators and authorized log administrators] with the capability to read [all audit data] from 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 ["Allowed capabilities" in [Table 6-4], [Table 6-5]] of audit data based on ["Selection criteria by type" of [Table 6-4], [Table 6-5]].

- [Table 6-4] Audit data Type and searching/sorting criteria by audit data type
 - TrusGuard Gateway
- [Table 6-5] Audit data Type and searching/sorting criteria by audit data type
 - TrusAnalyzer

[Table 6-4] Audit data type and searching/sorting criteria by audit data type - TrusGuard Gateway

Type	Selection criteria by type	Allowed capabilities
------	----------------------------	----------------------

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
Event log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Period ● Log level ● Log Type ● Users ● Description 	Search
Security Log	<p>All items selected from the following search conditions are included.</p> <ul style="list-style-type: none"> ● Period ● Risk level/Action ● Protocol ● Log Type ● Source IP address/port ● Destination IP address/port ● Description 	Search
Firewall log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Period ● Type/Log ID ● Protocol ● Source IP address/port ● Destination IP address/port ● Description 	Search
VPN log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Period ● Log Type ● Results 	Search

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
	<ul style="list-style-type: none"> ● Type ● Remote site ID ● Remote site IP 	

[Table 6-5] Audit data Type and searching/sorting criteria by audit data type – TrusAnalyzer

Type	Selection criteria by type	Allowed capabilities
System log (Operating log)	<p>The items selected in the following search</p> <p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Description ● Log numbers per page 	Search
	Log Delivered Time: Sort from the latest log	Sort
System status log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Log numbers per page 	Search
	Log Delivered Time: Sort from the latest log	Sort
Firewall log	<p>1) The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Session status ● Log numbers per page 	Search

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
	<p>2) The items selected in the following search conditions combined with the logical operators AND, OR and NOT.</p> <ul style="list-style-type: none"> ● Protocol ● Log ID ● NAT Type ● Source IP/port ● Destination IP/port ● Translated IP/ports 	
	Log Delivered Time: Sort from the latest log	Sort
Signature/behavior-based blocking log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Risk Score ● Source IPv4 address ● Source port ● Destination IPv4 address ● Destination port ● Action ● Intrusion Type ● Rule ID ● Log numbers per page 	Search
	Log Delivered Time: Sort from the latest log	Sort
System quarantine log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Action ● Log numbers per page 	Search

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
SSL VPN log	<ul style="list-style-type: none"> ● Source IPv4 address ● Description 	
	Log Delivered Time: Sort from the latest log	Sort
	1) The items selected in the following search conditions combined with the logical operator AND. <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Maximum number of Searches 2) The items selected in the following search conditions combined with the logical operators AND, OR and NOT. <ul style="list-style-type: none"> ● Type ● Results ● Users ● IP address ● Description 	Search
IPSec VPN Log	Log Delivered Time: Sort from the latest log	Sort
	The items selected in the following search conditions combined with the logical operator AND. <ul style="list-style-type: none"> ● Group/Device ● Log Type ● Log Delivered Time ● Protocol ● Source address ● Source port ● Destination address ● Maximum number of Searches 	Search
	Log Delivered Time: Sort from the latest log	Sort

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
QoS log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Action ● Source IPv4 address ● Source port ● Destination IPv4 address ● Destination port ● Description ● Maximum number of Searches 	Search
	Log Delivered Time: Sort from the latest log	Sort
Contents filtering log	<p>1) The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Log numbers per page <p>2) The items selected in the following search conditions combined with the logical operators AND, OR and NOT.</p> <ul style="list-style-type: none"> ● Description ● Filtering 	Search
	Log Delivered Time: Sort from the latest log	Sort
Website filtering log	<p>1) The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Log numbers per page <p>2) The items selected in the following search</p>	Search

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
	<p>conditions combined with the logical operators AND, OR and NOT.</p> <ul style="list-style-type: none"> ● Action ● URL ● Source IP/port ● Destination IP/port 	
	Log Delivered Time: Sort from the latest log	Sort
Anti-Virus log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Action ● Source IPv4 address ● Source port ● Destination IPv4 address ● Destination port ● Description ● Maximum number of Searches 	Search
	Log Delivered Time: Sort from the latest log	Sort
Anti-Spam log	<p>1) The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Log numbers per page <p>2) The items selected in the following search conditions combined with the logical operators AND, OR and NOT.</p> <ul style="list-style-type: none"> ● Action ● E-mail sender address ● E-mail recipient address 	Search

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
	<ul style="list-style-type: none"> ● Source IP/port ● Destination IP/port 	
	Log Delivered Time: Sort from the latest log	Sort
DNS filtering log	<p>1) The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Log numbers per page <p>2) The items selected in the following search conditions combined with the logical operators AND, OR and NOT.</p> <ul style="list-style-type: none"> ● Action ● Protocol ● Source IP/port ● Destination IP/port ● Description 	Search
	Log Delivered Time: Sort from the latest log	Sort
QoS log	<p>1) The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Group/Device ● Log Delivered Time ● Log numbers per page <p>2) The items selected in the following search conditions combined with the logical operators AND, OR and NOT.</p> <ul style="list-style-type: none"> ● QoS Name ● Network port ● Bandwidth (bps) ● Bandwidth (pps) 	Search

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Selection criteria by type	Allowed capabilities
	Log Delivered Time: Sort from the latest log	Sort
TrusAnalyzer operating log	<p>The items selected in the following search conditions combined with the logical operator AND.</p> <ul style="list-style-type: none"> ● Log generated Time ● Keywords (ID, type, content keywords) 	Search

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 events to be audited from the set of all auditable events based on the following attributes:

- [Event type]
- [None]

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 unauthorized deletion.

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

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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 delete the [oldest audit trail] if the audit trail exceeds the [specified audit data capacity].

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.1.2.Cryptographic support

FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [3DES, AES, SEED, ARIA, SHA1, SHA2, Blowfish, RSA, Diffie-Hellman] and specified cryptographic key sizes [168-bit (3DES), 128-bit or higher (AES, 192-bit, 256-bit), 128-bit (SEED), 160-bit (HAS160), 256-bit or higher (SHA2, 384-bit, 512-bit), 128-bit or higher (Blowfish, 128~448-bit), 1024-bit (RSA and Diffie-Hellman)], which meet [FIPS PUB 46-3¹, FIPS PUB 197², TTAS.KO-12.0004/R1³, KS * 1213:2004⁴, FIPS PUB 180-2⁵, Blowfish⁶, RFC3447⁷, RFC2631⁸].

Application notes: These security functional requirements define cryptographic support required for IPSec VPN and SSL VPN. The cryptographic key generation algorithm may vary depending on available protocols.

FCS_CKM.2 Cryptographic Key Distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

¹ FIPS PUB 46-3, "Data Encryption Standard: specifies the use of Triple DES(3DES)"

² FIPS PUB 197, "Advanced Encryption Standard(AES)"

³ TTAS.KO-12.0004/R1, "128-BIT SYMMETRIC BLOCK CIPHER(SEED)"

⁴ KS X 1213:2004, "128 bit block encryption algorithm ARIA"

⁵ FIPS PUB 180-2, "Secure Hash Standard(SHS)"

⁶ The Blowfish Encryption Algorithm, <http://www.schneier.com/blowfish.html>

⁷ RFC3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"

⁸ RFC2631, "Diffie-Hellman Key Agreement Method"

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [IKE, IKEv2, SSLv3/TLSv1] that that meets the following: [RFC2409⁹, RFC4306¹⁰, RFC2246¹¹].

Application notes: These security functional requirements define cryptographic key distribution required for IPsec VPN and SSL VPN. IPsec VPN distributes cryptographic keys via IKE/IKEv2 protocol, while SSL VPN distributes cryptographic keys via SSLv3/TLSv1 protocol.

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [by replacing all important security parameters and all plain-text cryptographic keys in cryptographic key-related devices into '0'] that meets the following: [None].

FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security

⁹ RFC2409, "The Internet Key Exchange (IKE)"

¹⁰ RFC4306, "Internet Key Exchange (IKEv2) Protocol"

¹¹ RFC2246, "The TLS Protocol Version 1.0"

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

attributes, or

FDP_ITC.2 Import of user data with security

attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [encryption/decryption, cryptographic key distribution, message authentication, integrity check] in accordance with a specified cryptographic algorithm [3DES, AES, SEED, ARIA, SHA1, SHA2, Blowfish, HAS-160, RSA, Diffie-Hellman] and cryptographic key sizes [168-bit (3DES), 128-bit or higher (AES, 192-bit, 256-bit), 128-bit(SEED), 160-bit (HAS160), 256-bit or higher (SHA2, 384-bit, 512-bit), 128-bit or higher (Blowfish, 128~448-bit), 1024-bit (RSA and Diffie-Hellman)] that meet the following: [FIPS PUB 46-3¹², FIPS PUB 197¹³, TTAS.KO-12.0004¹⁴, KS * 1213:2004¹⁵, FIPS PUB 180-2¹⁶, Blowfish¹⁷, RFC3447¹⁸, RFC2631¹⁹].

Application notes: These security functional requirements define the cryptographic operation required for IPsec VPN and SSL VPN. The cryptographic key creation algorithm may vary depending on available protocols.

¹² FIPS PUB 46-3, "Data Encryption Standard(DES)"

¹³ FIPS PUB 197, "Advanced Encryption Standard(AES)"

¹⁴ TTAS.KO-12.0004, "128-BIT SYMMETRIC BLOCK CIPHER(SEED)"

¹⁵ KS X 1213:2004, "128 bit block encryption algorithm ARIA"

¹⁶ FIPS PUB 180-2, "Secure Hash Standard(SHS)"

¹⁷ The Blowfish Encryption Algorithm, <http://www.schneier.com/blowfish.html>

¹⁸ RFC3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"

¹⁹ RFC2631, "Diffie-Hellman Key Agreement Method"

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.1.3. User data protection

FDP_IFC.1(1) Subset Information Flow Control (1)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(1) Simple security attributes(1)

FDP_IFC.1.1 The TSF shall enforce the [VPN SFP] on [following subjects, information and operation list]:

- a) Subject:
 - External IT entities sending/receiving data through the TOE
 - TOE components (TrusGuard Gateway, SSL VPN client) communicating via VPN
- b) Information: Data transferred via TOEs
- c) Operation
 - Encrypt and hash data transferred to communication targets
 - Decode encrypted data, perform integrity check and send data to the subjects
 - Pass information

Application notes: These security functional requirements define information flow controls required for IPSec VPN and SSL VPN to communicate between TOE components.

FDP_IFC.1(2) Subset Information Flow Control (2)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(2) Simple security attributes(2)

FDP_IFC.1.1 The TSF shall enforce the [traffic filtering SFP] on [following subjects, information and operation list].

- a) Subject: External IT entities sending/receiving data through the TOE
- b) Information: Traffic passing through the TOE
- c) Operation: Pass information

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

FDP_IFC.1(3) Subset Information Flow Control(3)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(3) Simple security attributes(3)

FDP_IFC.1.1 The TSF shall enforce the [contents filtering SFP] on [following subjects, information and operation list].

- a) Subject:
 - External IT entities sending/receiving data through the TOE
 - Authorized users who send/receive data through the TOE
- b) Information: Traffic passing through the TOE
- c) Operation:
 - Pass information

FDP_IFF.1(1) Simple Security Attributes (1)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(1) Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [VPN SFP] based on the following types of subject and information security attributes: [following subjects, information and security attributes].

- a) Subject security attributes:
 - Source IPv4 address
 - Destination IPv4 address
- b) Information security attributes:
 - Source IPv4 address
 - Destination IPv4 address
 - Service (protocol and 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: [Following rules]

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- a) The TOE should apply decryption and integrity check operations before data is handled by traffic filtering SFP, if subject security attributes match VPN packets coming from communication targets (external entities) through TOE components (TrusGuard Gateway and SSL VPN client), and secure communication channels are established according to FPT_ITC.1.
- b) The TOE should apply cryptographic and hash operations, if security attributes of VPN rules match VPN packets going out to communication targets (external entities) and allowed by traffic filtering SFP.
- c) The TOE should allow information flow when allowed by traffic filtering SFP, and operations a) or b) are performed for packets going out to communication targets (external IT entities and TOE components).

FDP_IFF.1.3 The TSF shall enforce the [following specified rules].

- a) Reassemble fragmented packets: The TOE should reassemble the fragmented packets before data is handled by VPN SFP.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [None].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [Configured using suggested security attributes as below].

- a) The TOE denies service requests or connections in plain text formats based on the following information security attributes.
 - Source IPv4 addresses are IPsec VPN gateway addresses or included in SSL VPN network lists.
 - Destination IPv4 addresses are IPsec VPN gateway addresses or SSL VPN gateway addresses
- b) The TOE denies services or connection requests for cryptographic and authentication requests if VPN tunnels cannot be established.
- c) The TOE denies service and connection requests with decryption and integrity check errors.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

FDP_IFF.1(2) Simple Security Attributes (2)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(2) Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce [traffic filtering SFP] based on the following types of subject and information security attributes: [Following subject and information security attributes].

- a) Subject security attributes:
 - Source IPv4/IPv6 address
 - Destination IPv4/IPv6 address
- b) Information security attributes:
 - Source IPv4/IPv6 address
 - Destination IPv4/IPv6 address
 - Service (protocol and port)
 - Security level
 - Packet data (header and 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: [Following rules]

- a) By comparing information security attributes passing through the TOE with Access control at Network Level rules set by authorized administrators with security attributes (source IP address, destination IP address, services and security level) defined in FDP_IFF.1.1:
 - If the information security attributes match, the TOE allows information flow requested by subjects.
 - If information security attributes (IPv4/IPv6 addresses and services) match and are connected to adjacent networks based upon network address translation rules, the TOE allows information flow.
- b) If information security attributes passing through the TOE do not match signature/behavior-based rules combined by the authorized administrators with security attributes (source IP address, destination IP address and packet

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

data (header and payload)) defined in FDP_IFF.1.1, the TOE allows information flow.

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

- a) Reassemble fragmented packets: The TOE should reassemble the fragmented packets before data is handled by traffic filtering SFP.
- b) Session restriction: If the traffic passing through the TOE is higher than the session number set by the authorized administrator, the TOE does not allow information flow for the exceeded sessions.
- c) Traffic control: The traffic passing through the TOE is using the same bandwidth as the bandwidth (bps/pps) set by the authorized administrator, the TOE restricts information flow traffic based upon information handling methods.
- d) Content filtering interoperation: If the contents filtering is interoperating with traffic passing through the TOE based on Access control at Network Level SFP, the TOE controls information flow according to FDP_IFF.1(3).

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [None].

FDP_IFF1.5 The TSF shall explicitly deny an information flow based on the following rules: [Following information flow denial rules according to security attributes].

- a) The TOE must block access requests if the information coming from external IT entities has internal network IPv4/IPv6 address.
- b) The TOE should block access requests if inbound information of internal network of IT entities has IPv4/IPv6 network addresses of external subjects.
- c) The TOE must block access requests if the information coming from external IT entities has IPv4 addresses of broadcasting entities.²⁰
- d) The TOE must block access requests if the information coming from external IT entities has IPv4/IPv6 addresses of looping subjects.
- e) The TOE must block access requests if the information coming from external IT entities has abnormal packet structures.

²⁰ IPv6 does not support broadcasting.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

FDP_IFF.1(3) Simple Security Attributes (3)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(3) Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [Contents filtering SFP] based on the following types of subject and information security attributes: [Following subjects, information and information security attributes].

- a) Subject security attributes:
 - Source IPv4 address
 - Identifier
 - Password
- b) Information security attributes:
 - Source IPv4 address
 - Destination IPv4 address
 - Service (protocol and port)
 - Packet data (header and payload)
 - 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: [Following rules]

- a) By comparing the TOE traffic security attributes (source IPv4 address, destination IPv4 address, services (protocol and port), packet data (header and payload), time) with information security attributes defined in FDP_IFF1.1, if the information security attributes do not match content filtering rules combined by the authorized administrator, the TOE allows information flow.
- b) If the TOE traffic subjects are authorized users and its attributes match content filtering rules, the TOE allows the connection requests to general, HTTP and FTP proxies.

FDP_IFF.1.3 The TSF shall enforce the [Detailed acceptance rules against information flow allowed by FDP_IFF.1.2].

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- a) Network address translation: As for traffic passing through TOE, destination IP addresses and service ports are translated into the TOE addresses and the proxy port number to be handled with application proxy functions.
- b) Session restriction: The TOE blocks information flow for exceeded sessions if the traffic passing through TOE is higher than the concurrent connections per service.
- c) If information security attributes match anti-virus and anti-spam mail rules, the TOE allows information flow by changing information security attributes of mail content and attachments.
- d) The TOE allows information flow by changing traffic information security attributes (destination IP address and port if the traffic passing through the TOE has specified transfer hosts.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules:
[none].

FDP_IFF1.5 The TSF shall explicitly deny an information flow based on the following rules:
[none].

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.1.4. Identification and authentication

FIA_AFL.1(1) Authentication Failure Handling (1)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [5], unsuccessful authentication attempts occur related to [following authentication events].

- a) Consecutive authentication attempts for TOE security management interfaces
 - TG administrator authentication – Web browsers (SSL/TLS) and SSH/Serial-based CLI
 - TrusAnalyzer administrator authentication – Web browsers (SSL/TLS)

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [be delayed for 5 minutes].

FIA_AFL.1(2) Authentication Failure Handling (2)


Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when "the configurable number [1~5] set by administrators", unsuccessful authentication attempts occur related to [following authentication events].

- a) User authentication attempts forced by SSL VPN policies of FDP_IFC.1(1) and FDP_IFF.1(1).
- b) User authentication attempts forced by Contents filtering policies of FDP_IFC.1(3) and FDP_IFF.1(3).
 - General proxy (General TCP)
 - FTP proxy
 - HTTP proxy

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall perform [countermeasures in the following list].

	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- a) Locking of Identified general user accounts

FIA_ATD.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: [See security attributes list in [Table 6-6] and [Table 6-7]]

[Table 6-6] User security attributes list

User type	Security attributes
TG top-level administrator	Authentication information (Password)
TG general administrator	Access permissions
TrusAnalyzer top-level administrator	Authentication information (Password)
TrusAnalyzer general administrator	Access permissions
TrusGuard Auth user	Authentication information (Password) Security level

[Table 6-7] VPN User security attributes list

User type	Security attributes
IPSec VPN Peer	IP address Shared key
SSL VPN user	Authentication information (Password) Security level

Application notes: These security requirements define VPN users as SSL VPN users and TrusGuard Gateway (IPSec VPN Peer).

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 [The secret

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

acceptance criteria in [Table 6-8]].

[Table 6-8] Secret acceptance criteria

Type	Criteria
Accepted characters	52 alphabets (Upper cases + lower cases: A~Z, a~z)
	Number (Decimal: 0~9)
	Special characters (25: ``~!@#%^*()_+ -=,./:;[]{}'`~`)
Combination rules	Exclude dictionary words
	Include at least one alphanumeric character or number
	More than 5 consecutive characters/number strings (Example: abcd1234 cannot be used as a password because 6 character sets ('ab', 'bc', 'cd', '12', '23', '34') are consecutive.)
	Prohibit using the same character more than 3 times
Minimum/Maximum length	9~15 alphanumeric + special characters (9~15 byte)

FIA_UAU.2 User Authentication Before any Action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.4 Single-use Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF should prevent re-utilization of authentication data related with [TG administrators, TrusAnalyzer administrators and TrusGuard Auth users].

Application notes: These security functional requirements prevent authentication data re-utilization of TG administrators and TrusAnalyzer administrators with timestamps, while it prevents authentication data re-utilization of TrusGuard Auth users for

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

GENERAL-Proxy, HTTP-Proxy and FTP-Proxy with one-time password.

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 [following feedback list] to the user while the authentication is in progress.

- a) Output passwords as masked characters

FIA_UID.2 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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.1.5.Security management

FMT_MOF.1 Management of Security Functions Behavior

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 determine, stop and resume behaviors of security functions described in [Table 6-9] and [Table 6-10] to [authorized administrators].

[Table 6-9] Security functions and allowed capabilities - TrusGuard Gateway

Security function	Authorized users	Capability		
		Determine	Stop	Resume
Backup	TG top-level administrator TG general administrator	O	-	-
Recover	TG top-level administrator	O	-	-
Security alert setting	TG top-level administrator	O	-	-
Audit data creation setting	TG top-level administrator	O	-	-
Log server interoperation setting	TG top-level administrator	O	-	-
SNMP setting	TG top-level administrator	O	O	O
TrusGuard Manager interoperation setting	TG top-level administrator	O	O	O
Integrity check	TG top-level administrator	O	-	-
Update	TG top-level administrator	O	-	-
System Restart	TG top-level administrator	O	-	-
Signature/behavior-based rule update	TG general administrator	O	-	-
Session timeout	TG top-level administrator	O	-	-
HA setting	TG top-level administrator	O	O	O
Access control at Network Level policy (function)	TG top-level administrator	O	-	-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Security function	Authorized users	Capability		
		Determine	Stop	Resume
Restrictions on session number	TG top-level administrator	O	-	-
Restrictions on large web traffic	TG top-level administrator	O	O	O
Signature/behavior-based blocking policy setting	TG top-level administrator	O	O	O
DDoS blocking setting	TG top-level administrator	O	-	-
System quarantine setting	TG top-level administrator	O	-	-
IPSec VPN setting	TG top-level administrator	O	O	O
SSL VPN setting	TG top-level administrator	O	O	O
CRL list management	TG top-level administrator	O		
Contents filtering security policy (function)	TG top-level administrator	O	-	-

[Table 6-10]Security functions and allowed capabilities - TrusAnalyzer

Security function	Authorized users	Capability		
		Determine	Stop	Resume
Log forward setting	TrusAnalyzer top-level administrator	O	O	O
Disk cleanup setting	TrusAnalyzer top-level administrator	O	O	O
Auto backup setting	TrusAnalyzer top-level administrator	O	O	O
Mail server notification setting	TrusAnalyzer top-level administrator	O	-	-
Spam and statistics information transmission setting	TrusAnalyzer top-level administrator	O	-	-
Alert setting	TrusAnalyzer top-level	O		

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Security function	Authorized users	Capability		
		Determine	Stop	Resume
	administrator			
TrusAnalyzer integrity check	TrusAnalyzer top-level administrator	O	-	-
TrusAnalyzer data recovery	TrusAnalyzer top-level administrator	O	-	-
TrusAnalyzer manual backup	TrusAnalyzer top-level administrator	O	-	-
Firmware Upgrade	TrusAnalyzer top-level administrator	O	-	-
System Restart	TrusAnalyzer top-level administrator	O	-	-
System Status Report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Network Status Report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Source-specific traffic report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Service-specific traffic report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Website analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Security function	Authorized users	Capability		
		Determine	Stop	Resume
	administrator			
Main service report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Attack analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Risk level analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Worm analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Spyware analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Correlation analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Virus analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Website filtering report	TrusAnalyzer top-level administrator	O	-	-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Security function	Authorized users	Capability		
		Determine	Stop	Resume
	TrusAnalyzer general administrator			
Spam mail analysis report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
SSL VPN report	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Virus analysis	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Website filtering analysis	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Spam mail analysis	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
SSL VPN analysis	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			
Integrated report creation	TrusAnalyzer top-level administrator	O	-	-
	TrusAnalyzer general administrator			

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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 [VPN SFP, traffic filtering SFP and contents filtering SFP] to restrict the ability to query, change and delete the security attributes described in] to [authorized TG top-level administrators and TG general administrators]

Application notes: According to these security functional requirements, TG top-level administrators have full permission, but TG general administrators have a query-only permission. The details of TOE user roles can be referred to 'FMT_SMR.1 Security roles'. TG top-level administrators have full permission for all capabilities (Default value change, query, change and deletion) described in security functional requirements, while TG general administrators have a query-only permission.

[Table 6-11]Security attributes list and allowed capabilities for authorized administrators

Type	Security attributes		Capability		
			Query	Change	Delete
VPN SFP	Subject	Source IPv4 address	O	O	O
		Destination IPv4 address	O	O	O
	information	Source IPv4 address	O	O	O
		Destination IPv4 address	O	O	O
		Service	O	O	O
		(protocol and port)			
Traffic filtering SFP	Subject	Source IPv4/IPv6 address	O	O	O
		Destination IPv4/IPv6 address	O	O	O
	information	Source IPv4/IPv6 address	O	O	O

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Security attributes		Capability		
			Query	Change	Delete
		Destination IPv4/IPv6 address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Service (protocol and port)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Security level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Packet data (header and payload)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Content filtering SFP	Subject	Source IPv4 address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Identifier	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Password	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	information	Source IPv4 address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Destination IPv4 address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Service (protocol and port)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Packet data (header and payload)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Time	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

FMT_MSA.3 Static attribute Initialization

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 [Traffic filtering SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Authorized TG top-level administrators] to specify alternative initial values to override the default values when an object or information is created.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

FMT_MTD.1(1) Management of TSF Data(1)

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 query, modify, delete, add the [TSF data listed in [Table 6-12]] to [authorized TG top-level administrators, TG general administrators and authorized general users].

[Table 6-12]TSF data created in the TOE(TrusGuard Gateway) and management capabilities for authorized TG top-level administrators and TG general administrators

TSF data	Capability			
	Query	Modify	Delete	Add
Administrator account, IP setting value	O	O	O	O
Update setting value	O	O	-	-
Selective audit data creation setting value	O	O	O	O
Audit data transmission setting value	O	O	O	O
SNMP setting value	O	O	O	O
Security alert setting value	O	O	-	-
Security alert mail/SMS setting	O	O	-	-
TOE identification (host) name	O	O	-	-
Time setting value	O	O	-	-
License information	O	O	-	-
Authentication certificate usage setting value	O	O	-	-
HA setting information: Audit port (physical port, local/remote device, virtual IPv4 address, Ping enable/disable) list information	O	O	O	O
HA setting information: HA setting (enable/disable, priority, connection	O	O	-	-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

TSF data	Capability			
	Query	Modify	Delete	Add
NIC, remote device IPv4 address, heart beat status)				
Signature/behavior-based blocking policy setting value	O	O	O	O
System quarantine setting value	O	O	-	-
IPSec VPN network setting value	O	O	O	O
Auto key setting value	O	O	O	O
Manual key setting value	O	O	O	O
IPSec VPN setting value	O	O	-	-
SSL VPN network setting value	O	O	O	O
SSL VPN user setting value	O	O	O	O
SSL VPN connection website setting value	O	O	-	-
SSL VPN setting value	O	O	-	-
Local certificate setting value	O	O	O	O
CA certificate setting value	O	O	O	O
Certificate profile	O	O	O	O
Proxy service object list: Proxy setting value	O	O	O	O
Proxy service object list: Proxy group setting value	O	O	O	O
Proxy concurrent connections/proxy process setting value	O	O	-	-

Application Notes: TG top-level administrators have full permission, but TG general administrators have a query-only permission.

[Table 6-13]TSF data list created in the TOEs (TrusGuard Auth and SSL VPN client) and management capabilities for authorized general users

TSF data	Capability			
	Query	Modify	Delete	Other

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

TSF data	Capability			
	Query	Modify	Delete	Other
TrusGuard Auth password	-	O	-	
SSL VPN Client user password	-	O	-	
SSL VPN Client setting value	O	O	-	-

FMT_MTD.1(2) Management of TSF Data(2)

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 query, modify, delete, add the [TSF data list specified in [Table 6-14]] to [authorized TrusAnalyzer top-level administrators and TrusAnalyzer general administrator].

[Table 6-14]TSF data created in the TOE (TrusAnalyzer) and management capabilities

TSF data	Capability			
	Query	Modify	Delete	Add
TOE (TrusAnalyzer) administrator account setting value	O	O	O	O
TOE (TrusAnalyzer) log forward setting value	O	O	O	O
TOE (TrusAnalyzer) disk cleanup setting value	O	O	-	-
TOE (TrusAnalyzer) auto backup setting value	O	O	-	-
TOE (TrusAnalyzer) mail server notification setting value	O	O	-	-
TOE (TrusAnalyzer) spam and statistics transmission setting value	O	O	-	-
TOE (TrusAnalyzer) alarm setting value	O	O	-	-
TOE (TrusGuard Gateway) device connection setting value	O	O	O	O
Connected TOE (TrusGuard Gateway) resource status	O	-	-	-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

TSF data	Capability			
	Query	Modify	Delete	Add
information				
Connected TOE (TrusGuard Gateway) network status information	O	-	-	-
TOE (TrusGuard Gateway) system log	O	-	-	-
TOE (TrusGuard Gateway) system status log	O	-	-	-
TOE (TrusGuard Gateway) firewall log	O	-	-	-
TOE (TrusGuard Gateway) signature/behavior-based blocking log	O	-	-	-
TOE (TrusGuard Gateway) system quarantine log	O	-	-	-
TOE (TrusGuard Gateway) content filtering log	O	-	-	-
TOE (TrusGuard Gateway) website filtering log	O	-	-	-
TOE (TrusGuard Gateway) virus blocking log	O	-	-	-
TOE (TrusGuard Gateway) Anti-Spamlog	O	-	-	-
TOE (TrusGuard Gateway) SSL VPN log	O	-	-	-
TOE (TrusGuard Gateway) DNS proxy log	O	-	-	-
TOE (TrusGuard Gateway) QoS log	O	-	-	-
TOE (TrusGuard Gateway) Anti-malsite log	O	-	-	-
TOE (TrusGuard Gateway) QoS log	O	-	-	-
TOE (TrusAnalyzer) system log	O	-	-	-

Application Notes: TrusAnalyzer top-level administrators have full permission, while TrusAnalyzer general administrators has only limited permission, such as: selected device setting change, integrated reports creation, change and deletion and log and report query.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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 [audit data storage capacity] to [TrusAnalyzer top-level administrators].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed the indicated limits: [Countermeasures described in FAU_STG.3].

Application notes: In these security functional requirements, 'authorized administrators' mean TrusAnalyzer top-level administrators. They can specify physical audit data storage capacity described in FMT_MTD.2.1.

FMT_MTD.3 Secure TSF Data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1(1)~(2) Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [identification and authentication data].

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: [the security function lists].

- a) Security function list described in FMT_MOF.1
- b) Security function list described FMT_MSA.1
- c) Static attributes initialization list described FMT_MSA.3
- d) TSF data management list described in FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.2

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

FMT_SMR.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 [authorized user roles described in [Table 6-15]].

[Table 6-15]Security role types for authorized users

Types	Contents
TG top-level administrator	Administrator with full permissions for all TOE (TrusGuard Gateway) functions
TG general administrator	Administrator with limited permission such as signature/behavior-based blocking rule update, environment setup and query for TOE (TrusGuard Gateway)
TrusAnalyzer top-level administrator	Administrator with full permission for all TOE (TrusAnalyzer) functions
TrusAnalyzer general administrator	Administrator with limited permission such as TOE (TrusGuard Gateway) setting change, integrated report creation and audit data query
SSL VPN user	General user authorized based upon SSL VPN policies defined in FDP_IFF.1(1)
TrusGuard Auth user	General user authorized based upon content filtering policies defined in FDP_IFF.1(3)

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

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.1.6. 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 during initial start-up, periodically during normal operation to demonstrate the correct operation of [*TrusGuard Gateway and TrusAnalyzer processes*].

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 **authorized administrators** with the capability to verify the integrity of [*TSF execution code*].

Application Notes: In security functional requirements, 'authorized administrators' mean TG top-level administrators and TrusAnalyzer top-level administrators. The details of TOE user roles can be referred to 'FMT_SMR.1 Security roles'.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.1.7.TOE access

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 [user inactive periods described in [Table 6-16]]

[Table 6-16]User inactive periods for user session termination

Type	User inactive period
TG top-level administrator TG general administrator	Inactive period for authorized TG top-level administrators and TG general administrators specified by TG top-level administrators - Web-based security management interface (SSL/TLS) : 10~600 sec. (Default: 600 sec.) - Local/remote CLI (SSH, Serial): 10~600 sec. (Default: 600 sec.)
TrusAnalyzer top-level administrator TrusAnalyzer general administrator	Inactive period for authorized TrusAnalyzer top-level administrators and general administrators specified by TrusAnalyzer top-level administrators - Web-based security management interface (SSL/TLS): 10 min.
SSL VPN user	Inactive period (5 min.) for authorized general users that allow information flow based upon rules with SSL VPN security attributes among information flow control policies allowed by FDP_IFF.1(1).
TrusGuard Auth user	Inactive period (30 min.) for authorized general users that allow information flow based upon rules with proxy security attributes among information flow control policies allowed by FDP_IFF.1(3).

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.1.8.Trusted path/channels

FTP_ITC.1 Inter-TSF trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit trusted IT entities or TSFs to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [IPSec/SSL VPN communication and SSL/TLS, SSH communication software and communication functions between TOEs]

Application Notes: These security functional requirements are used for IPSec/SSL VPN communication channel.

FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote, local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit local users, remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, [SSL/TLS, SSH communication software and the TOE].

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Application Notes: These security functional requirements can be applied for SSL/TLS communication between the web browser and TOE and SSH communication between the SSH (Secure Shell) terminal program and the TOE.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.2. TOE Security Assurance Requirements

203 Security assurance components, as defined in Common Criteria for Information Technology Security Evaluation part 3, are the basis for the security assurance requirements expressed in this Security Target. The evaluation assurance level is EAL2. Security assurance components are summarized in [Table 6-17].

[Table 6-17]Security Assurance Requirements

Class	Assurance Components	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objective
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Guidance documents	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.2.1.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 summarize 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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

6.2.2.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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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 initialization 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.2 Security-Enforcing Functional Specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

- ADV_FSP.2.1D The developer shall provide a functional specification.
- ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

- ADV_FSP.2.1C The functional specification shall completely represent the TSF.
- ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 Basic Design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D 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.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3.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.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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 fulfill 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

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

6.2.4.Life-cycle Support

ALC_CMC.2 Use of a CM System

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Evaluator action elements:

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 Parts of the TOE CM Coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E 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 and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

6.2.5.Tests

ATE_COV.1 Evidence of Coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

ATE_COV.1.1E 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:

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.1.1E 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_FSP2 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:

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

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.

6.2.6.Vulnerability Assessment

AVA_VAN.2 Vulnerability Analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E 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 Basic attack potential.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.3. Rationale for Security Requirements

204 This chapter will demonstrate that the security requirements of the ST meet the security objectives and appropriately control the security issues. It also describes why the group of specific assurance requirements are suitable based on the supporting rationale of the SARs.

6.3.1. Security Functional Requirements Rational

205 The supporting rationale of security functional requirements demonstrate the following facts.

- Each security objective traces back to at least one security functional requirement.
- Each security functional requirement addresses at least one security objective.


206 The table below shows that the security objective itself and the fact that none of security objectives are missing and each security objective must trace back to at least one security functional requirement.

[Table 6-18] TOE Security objectives and a map between security objects and corresponding security functional requirements

TOE Security objectives Security functional requirements	O.Audit	O.Management	O.Data protection	O.Identification and authentication	O.Information flow control	O.Key security	O.Block abnormal packets	O.Block Denial of Services (DoS) attacks	O.Protect user sessions
FAU_ARP.1	X								
FAU_GEN.1	X								

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

TOE Security objectives Security functional requirements	O.Audit	O.Management	O.Data protection	O.Identification and authentication	O.Information flow control	O.Key security	O.Block abnormal packets	O.Block Denial of Services (DoS) attacks	O.Protect user sessions
FAU_SAA.1	X								
FAU_SAR.1	X								
FAU_SAR.3	X								
FAU_SEL.1	X								
FAU_STG.1	X								
FAU_STG.3	X								
FCS_CKM.1			X			X			
FCS_CKM.2			X			X			
FCS_CKM.4			X			X			
FCS_COP.1			X						
FDP_IFC.1(1)			X						
FDP_IFC.1(2)					X		X	X	
FDP_IFC.1(3)					X				
FDP_IFF.1(1)			X						
FDP_IFF.1(2)					X		X	X	
FDP_IFF.1(3)					X				
FIA_AFL.1(1)				X					
FIA_AFL.1(2)				X					
FIA_AFL.1(3)				X					
FIA_ATD.1				X					

	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

<div>TOE Security objectives</div> <div>Security functional requirements</div>	O.Audit	O.Management	O.Data protection	O.Identification and authentication	O.Information flow control	O.Key security	O.Block abnormal packets	O.Block Denial of Services (DoS) attacks	O.Protect user sessions
FIA_SOS.1				X					
FIA_UAU.2		X		X					
FIA_UAU.4				X					
FIA_UAU.7				X					
FIA_UID.2		X		X					
FMT_MOF.1		X							
FMT_MSA.1		X							
FMT_MSA.3		X							
FMT_MTD.1(1)		X							
FMT_MTD.1(2)		X							
FMT_MTD.2		X							
FMT_MTD.3		X							
FMT_SMF.1		X							
FMT_SMR.1		X							
FPT_TST.1			X						
FTA_SSL.3		X							X
FTP_ITC.1			X						
FTP_TRP.1			X						

FAU_ARP.1 Security alarms

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

207 As this component ensures the capability of performing appropriate countermeasures in case of detecting potential security violations, it satisfies the TOE security objectives O.Audit.

FAU_GEN.1 Audit data generation

208 As this component ensures the capability of defining auditable events and creating audit records, it satisfies the TOE security objectives O.Audit.

FAU_SAA.1 Potential violation analysis

209 As this component ensures the capability of inspecting audited events to point out security violations, it satisfies the TOE security objectives O.Audit.

FAU_SAR.1 Audit review

210 As this component ensures the authorized log administrator to review audit records, it satisfies the TOE security objectives O.Audit.

FAU_SAR.3 Selective audit review

211 As this component ensures the capability of searching audit data based on the criteria with logical relationship, it satisfies the TOE security objectives O.Audit.

FAU_SEL.1 Selective audit

212 As this component ensures the capability to including/excluding auditable events based on event types, it satisfies TOE security objectives O.Audit.

FAU_STG.1 Audit trail storage protection

213 As this component ensures the capability of protecting audit trails from unauthorized changes and deletions, it satisfies TOE security objectives O.Audit.

FAU_STG.3 Countermeasure for possible audit data loss

214 As this component ensures the capability of performing countermeasures when the audit trail exceeds the pre-defined threshold, it satisfies TOE security objectives O.Audit.

FCS_CKM.1 Cryptographic key creation

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

215 As this component ensures the capability of creating cryptographic keys in accordance with the specified cryptographic key algorithm and cryptographic key length, it satisfies the TOE security objectives O.Data protection and O.Key security.

FCS_CKM.2 Cryptographic key distribution

216 As this component ensures the capability of distributing cryptographic keys in accordance with the specified cryptographic key distribution method, it satisfies the TOE security objectives O.Data protection and O.Key security.

FCS_CKM.4 Cryptographic key destruction

217 As this component ensures the capability of destroying cryptographic keys in accordance with the specified cryptographic key destruction method, it satisfies the TOE security objectives O.Data protection and O.Key security.

FCS_COP.1 Cryptographic operation

218 As this component ensures the capability of performing cryptographic operation in accordance with the specified cryptographic algorithm and cryptographic key length, it satisfies the TOE security objectives O.Data protection.

FDP_IFC.1(1) Partial information flow control (1)

219 As this component ensures the capability of controlling information flows of incoming/outgoing TOE data in accordance with the TOE information flow control policies, it satisfies the TOE security objectives O.Data protection.

FDP_IFC.1(2), Partial information flow control (2)

220 As this component ensures the capability of controlling information flows of incoming/outgoing TOE data in accordance of TOE information flow control policies, it satisfies the TOE security objectives O.Information flow control, O.Abnormal packet blocking and O.Denial of Service (DoS) attack blocking.

FDP_IFC.1(3) Partial information flow control (3)

221 As this component ensures the capability of controlling information flows of incoming/outgoing TOE data in accordance of TOE information flow control policies, it satisfies the TOE security

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

objectives O.Information flow control.

FDP_IFF.1(1), Single-layer Security attribute (1)

222 As this component provides IPSec VPN rules to control information flows in accordance of security attributes, it satisfies the TOE security objectives O.Data protection.

FDP_IFF.1(2) Single-layer Security attribute (2)

223 As this component provides SSL VPN rules to control information flows in accordance with security attributes, it satisfies the TOE security objectives O.Information flow control, O.Abnormal packet blocking and O.Denial of service (DoS) attack blocking.

FDP_IFF.1(3) Single-layer Security attribute (3)

224 As this component provides signature/behavior-based blocking rules to control information flows in accordance with security attributes, it satisfies the TOE security objectives O.information flow control.

FIA_AFL.1(1) Authentication failure handling (1)

225 As this component ensures the capability of defining values for some number of unsuccessful authentication attempts of TG top-level administrators, TG general administrators and TrusAnalyzer administrators to perform countermeasures in case of authentication attempt failure, it satisfies the TOE security objectives O.Identification and authentication.

FIA_AFL.1(2) Authentication failure handling (2)

226 As this component ensures the capability of defining values for some number of unsuccessful general user authentication attempts to perform countermeasures after the specified number of failed authentication attempts, it satisfies the TOE security objectives O.Identification and authentication.

FIA_ATD.1 User attribute definition

227 As this component defines a security attribute list for each user, it satisfies the TOE security objectives O.Identification and authentication.

FIA_SOS.1 Password verification

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

228 As this component provides a verification mechanism to check if the password meets the defined acceptance criteria, it satisfies the TOE security objectives O.Deification and authentication.

FIA_UAU.2 User authentication before performing any actions

229 As this component ensures the capability of authorizing users successfully, it satisfies the TOE security objectives O.Management and O.Identification and authentication.

FIA_UAU.4 Authentication mechanism to prevent re-utilization

230 As this component ensures the capability of preventing re-utilization of authentication data, it satisfies the TOE security objectives O.Identification and authentication.

FIA_UAU.7 Authentication feedback protection

231 As this component ensures the capability of providing only limited authentication feedback to the user during authentication process, it satisfies the TOE security objectives O.Identification and authentication.

FIA_UID.2 User identification before any action

232 As this component ensures the capability of successfully identifying users, it satisfies the TOE security objectives O.Management and O.Identification and authentication.

FMT_MOF.1 Security functional management

233 As this component ensures the authorized administrator to manage security functions, it satisfies the TOE security objectives O.Management.

FMT_MSA.1 Security attribute management

234 As this component ensures the authorized administrator to manage security attributes that apply to information flow control policies, it satisfies the TOE security objectives O.Management.

FMT_MSA.3 Static attribute initialization

235 As this component provides the default values of security attributes that apply to information flow control policies, it satisfies the TOE security objectives O.Management.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

FMT_MTD.1(1) TSF data management (1)

236 As this component ensures TG top-level administrators and TG general administrators to manage TSF data, it satisfies the TOE security objectives O.Management.

FMT_MTD.1(2) TSF data management (2)

237 As this component ensures TrusAnalyzer top-level administrators and TrusAnalyzer general administrators to manage TSF data, it satisfies the TOE security objectives O.Management.

FMT_MTD.2 TSF data threshold management

238 As this component ensures the authorized top-level administrators or top-level log administrators to manage TSF data thresholds and perform countermeasures if the specific threshold is reached or exceeded, it satisfies the TOE security objectives O.Management.

FMT_MTD.3 Secure TSF data

239 As this component ensures that only safe and valid values are assigned to TSF data, it satisfies the TOE security objectives O.Management.

FMT_SMF.1 Specification of management functions

240 As this component requires to specify management functions including security attributes, TSF data and security functions that the TSF shall perform, it satisfies the TOE security objectives O.Management.

FMT_SMR.1 Security Roles

241 As this component ensures the capability of associating users to the roles of authorized administrators, it satisfies the TOE security objectives O.Management.

FPT_TST.1 TSF Self-Test

242 As this component provides the ability to perform self-testing to ensure the accurate TSF operation and check the integrity of TSF data and executable code, it satisfies the TOE security objectives O.Data protection.

FTA_SSL.3 TSF-initiated Session Termination

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

243 As this component terminates interactive user sessions after general users, authorized general users, authorized TG top-level administrators and TG general administrators do not perform any action for the specified user inactive period, it satisfies the TOE security objectives O.Management and O.User session protection.

FTP_ITC.1 Inter-TSF trusted channel

244 As this component establishes a secure channel between the general user system and the authorized general user system or between TOEs through SSL and SSH protocols, it satisfies O.Data protection.

FTP_TRP.1 Trusted path

245 As this component provides trusted paths via SSL/SSH protocols across (general) user and authorized general user systems and TOEs, it satisfies the TOE security objective O.Data protection.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.3.2.Security Assurance Requirements Rational

- 246 The assurance level for this Security Target is EAL2.
- 247 EAL2 is a assurance package that requires a structural test and the cooperation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.
- 248 EAL2 can be applied in situations when developers of users require a low to moderate level of independently assured security in the absence of availability of the complete development records. Such a situation may arise when securing existing systems, or where access to the developer may be limited.
- 249 EAL2 provides assurance with the functional and interface specification, operational user guides, testing results, a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guide evidence provided) demonstrating resistance to penetration attackers with a basic attack potential, and a basic description of the architecture of the TOE, to understand security behaviors. EAL2 also provides assurance with the evidence of the CM system and the secure distribution procedures.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

6.3.3.Dependency Rational

Dependencies of TOE security functional requirements

250

[Table 6-19] below shows dependencies of the functional components.

[Table 6-19]Dependencies of the functional components

Number	Functional component	Dependencies	Reference number
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE Time Stamps
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1(1)	2, 31
7	FAU_STG.1	-	-
8	FAU_STG.3	FAU_STG.1	7
9	FCS_CKM.1	[FCS_CKM.2, FCS_COP.1], FCS_CKM.4	10, 11, 12
10	FCS_CKM.2	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FCS_CKM.4	9, 11
11	FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1]	9
12	FCS_COP.1	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1], FCS_CKM.4	9, 11
13	FDP_IFC.1(1)	FDP_IFF.1(1)	16
14	FDP_IFC.1(2)	FDP_IFF.1(2)	17
15	FDP_IFC.1(3)	FDP_IFF.1(3)	18
16	FDP_IFF.1(1)	FDP_IFC.1(1), FMT_MSA.3	13, 30
17	FDP_IFF.1(2)	FDP_IFC.1(2), FMT_MSA.3	14, 30
18	FDP_IFF.1(3)	FDP_IFC.1(3), FMT_MSA.3	15, 30
19	FIA_AFL.1(1)	-	*24
20	FIA_AFL.1(2)	-	*24

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Number	Functional component	Dependencies	Reference number
21	FIA_AFL.1(3)	-	*24
22	FIA_ATD.1	-	-
23	FIA_SOS.1	-	-
24	FIA_UAU.2	FIA_UID.1	*27
25	FIA_UAU.4	-	-
26	FIA_UAU.7	-	*24
27	FIA_UID.2	-	-
28	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	35, 36
29	FMT_MSA.1	[FDP_ACC.1, FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	13, 14, 15, 35, 36
30	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	29, 36
31	FMT_MTD.1(1)	FMT_SMF.1, FMT_SMR.1	35, 36
32	FMT_MTD.1(2)	FMT_SMF.1, FMT_SMR.1	35, 36
33	FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	31, 32, 36
34	FMT_MTD.3	FMT_MTD.1	31, 32
35	FMT_SMF.1	-	-
36	FMT_SMR.1	FIA_UID.1	*27
37	FPT_TST.1	-	-
38	FTA_SSL.3	-	-
39	FPT_ITC.1	-	-
40	FTP_TRP.1	-	-

FAU_GEN.1

251 These form dependencies on FPT_STM.1, but the dependencies of FAU_GEN.1 are satisfied with security objectives for operating environments OE.Timestamps instead of FPT_STM.1 because security-related events are accurately recorded with the trusted timestamps provided by the TOE operating environment.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

****FIA_UAU.2, FMT_SMR.1***

252 These form dependencies on FIA_UID.1, but the dependencies are satisfied with FIA_UID.2 that is hierarchical to them.

****FIA_AFL.1, FIA_UAU.7, FTA_SSL.1***

253 These form dependencies on FIA_UAU.1, but the dependencies are satisfied with FIA_UAU.2 that is hierarchical to them.

Dependencies of TOE assurance requirements

254 The dependencies of each assurance package provided by the Common Criteria for Information Technology Security Evaluation are already satisfied, so the supporting rationale can be omitted.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

7. TOE summary specification

255 This chapter will explain TOE security functionalities that satisfy security functional requirements.

7.1. TOE Security Functionality

256 TOE Security functionality can be categorized into the security audit, the user data protection, the identification and authentication, the security management, the TSF protection, the TOE access and the trust path/channels. This chapter will describe how the TOE satisfies security functional requirements.

7.1.1. Security Audit

Potential security violation analysis and alert

257 When the potential security violations are detected, the TOE (TrusGuard Gateway) notifies them to administrators and performs corresponding countermeasures. **(FAU_ARP.1, FAU_SAA.1)**

258 When the TOE for TrusAnalyzer receives Anti-Spam logs from the TOE for TrusGuard Gateway, it checks potential security violations and sends alert e-mails with spam mail blocking lists to administrators.

259 Further, the TOE for TrusAnalyzer applies the following rules when it inspects events with additional potential violation analysis for SFR enforcement.

- CPU usage is higher than the alert level.
- Memory usage is higher than the alert level.
- Disk usage is higher than the alert level
- HA status is changed.
- Log level is higher than the selected value
- Power supply equipments are failed
- Alterable network port connection is disconnected.
- The number of sessions is higher than the alert level.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

260 The TOE (TrusGuard Gateway) monitors potential security violation events for each function and performs countermeasures to alert administrators to take appropriate actions against security violation events. It sends alert e-mails or alert SMS.

[Table 7-1] Functional components to trigger security alerts, auditable events and countermeasures

Functional component	Auditable events	Countermeasures
FPT_SAA.1	CPU usage is higher than the alert level.	Send alert e-mail /alert SMS
	Memory usage is higher than the alert level.	
	Disk usage is higher than the alert level	
	HA status is changed.	
	Log level is higher than the selected value	
	Power supply equipments are failed	
	Alterable network port connection is disconnected.	
	The number of sessions is higher than the alert level.	
FDP_IFF.1(3)	Detect spam mail blocking in the log file	Alert e-mail

Audit data creation

261 The TOEs (TrusGuard Gateway and TrusAnalyzer) create audit data to record security events or security management function enforcement during operation.

262 The TOEs (TrusGuard Gateway and TrusAnalyzer) use the system time provided by the TOE operating environment to ensure the audit data to be created in sequence of time. The TOE for TrusGuard Gateway automatically synchronizes the system time with the NTP server specified by the authorized administrator or allows the administrator to manually specify the system time. The TOE for TrusAnalyzer uses timestamps provided by the TOE for TrusGuard Gateway. The user who is in charge of managing the TOEs for TrusGuard Gateway and TrusAnalyzer shall always maintain accurate timestamps.

263 The TOE creates records for audit function start-up and shut-down or all auditable events defined in [Table 6-3] during operation. The audit data that the TOE for TrusGuard Gateway creates contains items such as event date, event type, subject identification and event results (success or failure). The created audit data is saved in the TOE for TrusGuard Gateway and transferred to the TOE for TrusAnalyzer which is the interoperated audit data management

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

server to manage audit data. **(FAU_GEN.1)**

- 264 The TOE for TrusGuard Gateway provides authorized administrators with functions to determine audit data creation. The authorized administrator can select all auditable event groups in accordance with event types (Event log, Security log, Firewall log and VPN log). **(FAU_SEL.1)**

Audit review

- 265 The TOEs for TrusGuard Gateway and TrusAnalyzer provide authorized administrators and authorized log administrators with functions to query all TOE audit data, and the TSF outputs audit records in an easy-to-interpret format for administrators. Further, the TSF provide functions to search and sort audit data based on selection criteria for each audit data type. **(FAU_SAR.1, FAU_SAR.3)**

- The TOE for TrusGuard Gateway provides the authorized administrator with functions to query the audit data of the VPN log, the firewall log, the Security log and the event log from the monitor center. For each log type, search functions are provided based on selection criteria such as period, protocol, user, IP address and description. For each selected item, selective search functions are provided based on the logical operator AND.
- The TOE for TrusAnalyzer allows the authorized administrator to search the audit data system log (operation log), the system status log, the firewall log, the signature/behavior-based blocking log, the system quarantine log, the content filtering log, the website filtering log, the virus blocking log, the Anti-Spam log, the IPSec VPN log, the SSL VPN log, the DNS filtering log, the QoS log, the anti-malsite filtering log, the QoS log received from the TOE for TrusGuard Gateway and the TrusAnalyzer operation log. For each log type, search functions are provided based on selected criteria such as period, protocol, user, IP address and description. For each selected item, selective search, sort functions are provided based on the logical operators AND, OR and NOT.

Audit trail protection

- 266 The TOEs for TrusGuard Gateway and TrusAnalyzer protect saved audit data from unauthorized deletion. The TOE audit data is protected from unauthorized changes. The TOE protects audit data from unauthorized deletion or changes, except in case of deleting the oldest audit data as a countermeasure in respect of possible data loss defined in FAU_STG.3. **(FAU_STG.1)**

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Audit data loss handling and prevention

- 267 The TOEs (TrusGuard Gateway, TrusAnalyzer) prevent audit data loss as it deletes the oldest audit data as a countermeasure in respect of possible data loss when the audit trail exceeds the threshold. To prevent audit data loss, the TOE for TrusGuard Gateway deletes the oldest file and backs up the current file when the file size of the audit record saved in the local disk exceeds the specified size. To handle audit data loss, the TOE for TrusAnalyzer sequentially delete from the oldest data file when the threshold specified by the authorized administrator is exceeded. (FAU_STG.3)

7.1.2.Cryptographic Support

- 268 The TOEs for TrusGuard Gateway and SSL VPN client provide the IPSec/SSL-based VPN functions to provide confidentiality and integrity of transmission data. The VPN function leverages cryptographic algorithms provided by the certified cryptographic module Magic Crypto V1.1.1 and the latest Openssl library for the algorithms that are not provided by the certified cryptographic module.

Cryptographic key creation, distribution and operation

- 269 The TOEs (TrusGuard Gateway and SSL VPN Client) provide encrypted communication in the use of the SSH connection and HTTPS connection for IPSec VPN, SSL VPN and administrator connections.
- 270 The cryptographic algorithms for cryptographic key creation, distribution and operation are SEED, 3DES, AES, ARIA and Blowfish, the hash algorithms are SHA1, SHA2 and HAS160, and the key distribution algorithms are IKE, IKEv2 and SSLv3/TLSv1. The cryptographic key creation algorithms, the hash algorithms and the key distribution algorithms provided by the TOE are listed in [Table 7-2]. (FCS_CKM.1, FCS_CKM.2, FCS_COP.1)

[Table 7-2] Cryptographic algorithms used by the TOE

Type	Description
Cryptographic algorithm (CBC mode)	SEED (128 bits), 3DES(168 bits), AES (128 bits or higher: 192 bits and 256 bits), ARIA (128 bits, 192 bits and 256 bits), Blowfish
	SEED encrypts and decrypts data in a 128-bit block size with a

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Description
	<p>128-bit input key length. SEED is used to encrypt the entire IPv4 packet (IP header + IP Payload) as well as authentication information and packet sequence number for IPv4 packets.</p> <p>3DES encrypts and decrypts data in 64-bit block size with a 192-bit input key length. 3DES is used to encrypt the entire IPv4 packet (IP header + IP Payload) as well as authentication information and packet sequence number for IPv4 packets.</p> <p>AES encrypts and decrypts data in a 128-bit block size with a variable input key length. AES is used to encrypt the entire IPv4 packet (IP header + IP Payload) as well as authentication information and packet sequence number for IPv4 packets.</p> <p>ARIA encrypts and decrypts data in a 128-bit block size with a variable input key length. ARIA is used to encrypt the entire IPv4 packet (IP header + IP Payload) as well as authentication information and packet sequence number for IPv4.</p> <p>Blowfish encrypt data in a 64-bit block size with a variable input key length from 32 bits to 448 bits. Blowfish is used to encrypt packets in SSL/TLS.</p>
Hash algorithm (HMAC mode)	<p>SHA1(160 bits), SHA2(256 bits or higher: 384 bits, 512 bits), HAS160(160 bits)</p> <p>SHA1 and SHA2 are hash algorithms to generate MAC (Message Authentication Code) and the authentication information for IPv4 packets. SHA1 and SHA2 are used with SEED, 3DES, AES and ARIA to provide data integrity and data source authentication services.</p> <p>HAS160 is a hash algorithm to generate MAC (Message Authentication Code) and the authentication information for IPv4 packets. HAS160 is used with SEED, 3DES, AES and ARIA to provide data integrity and data source authentication services.</p>
Key distribution algorithm	<p>IKEv2 (IETF RFC4306), IKE (IETF RFC2409), SSLv3/TLSv1 (RFC 2246)</p> <p>The TOE exchanges keys with the assigned IKE (Internet Key Exchange) standards in accordance with IETF RFC2409 or the assigned IKEv2 standards in accordance with IETF RFC4306 between the local gateway and the remote gateway.</p>

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Description
	The TOE for TrusGuard Gateway exchange keys with the assigned SSLv3/TLSv1 standards in accordance with IETF RFC2246 and the TOE for SSL VPN Client.

Cryptographic key destruction

- 271 To prevent cryptographic key re-utilization and permanently destroy cryptographic keys, the TOEs (TrusGuard Gateway and SSL VPN client) overwrite all plaintext keys in the devices related with cryptographic keys and memory spaces containing important security parameters with '0'. (FCS_CKM.4)

7.1.3. User Data Protection

- 272 The TOE (TrusGuard Gateway) provides user data protection function through VPN SFP, traffic filtering SFP and content filtering SFP to protect user data.
- The VPN SFP is security functional policies for the authorized administrator to handle VPN traffic passing through the TOE, which can be classified as IPsec VPN functions and SSL VPN functions.
 - The traffic filtering SFP are security functional policies to handle incoming/passing/outgoing TOE traffic in accordance with security rules specified by the authorized administrator, which can be classified as Access control at Network Level functions and deep packet inspection functions.
 - The content filtering SFP performs security functions to handle traffic passing through the TOE in accordance with content filtering rules specified by the authorized administrator through application proxy functions.

VPN SFP

- 273 The TOEs (TrusGuard Gateway and SSL VPN Client) provide VPN functions to extend a private network across a public network like Internet. The TOEs (TrusGuard Gateway and SSL VPN Client) provide secure communication channels through IPsec VPN and SSL VPN functions to protect transmission data between communication targets.
- 274 If attribute information of VPN packets coming from communication targets is matching with

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

VPN rules specified by the authorized administrator, the TOE (TrusGuard Gateway) shall perform integrity check and decrypt data before the traffic filtering SFP handles the packets. The VPN packet going out to the communication target uses the encrypted communication through cryptographic and hash algorithms if the traffic filtering SFP allows it.

- 275 The TOE (TrusGuard Gateway) reassembles encapsulated and fragmented packets before handling any packet data. And it also blocks connections and service requests in a plaintext format even if the packet IP address is identical with the network IP address of VPN rules. If decryption errors or integrity check errors occur for incoming VPN packets, it blocks services and connection requests.

IPSec VPN

- 276 The TOE (TrusGuard Gateway) performs IPSec VPN information flow control functions against packets coming from the TOE (TrusGuard Gateway) based on source IP address, destination IP address, protocol and port information.
- 277 The TOE (TrusGuard Gateway) establishes a secure channel between the traffic coming to the IPSec VPN gateway and the traffic going out to the communication target based on IPSec VPN rules specified by the authorized administrator.
- 278 The TOE (TrusGuard Gateway) performs cryptographic based on security policies specified by the authorized administrator while the security mechanism for IPSec VPN information flow control functions and secure channels are generated. The related details can be found in the "Cryptographic support". (FDP_IFC.1(1), FDP_IFF.1(1))

SSL VPN

- 279 The TOEs (TrusGuard Gateway and SSL VPN Client) establish SSL/TLS-based virtual tunnels between public networks to safely protect incoming/outgoing data when the authorized administrator enforces SSL VPN functions on incoming traffic. The SSL/TLS protocols are socket libraries of the transfer layer to encrypt the entire communication channels, being independent with application programs. Through SSL/TLS protocols, the TOEs (TrusGuard Gateway and SSL VPN Client) can perform encryption/decryption and hash integrity check for the external IT entities that receive/send information through the TOE, traffic that sends to other places through the TOE components (TrusGuard Gateway and SSL VPN Client) from subjects, and information that sends to communication targets. (FDP_IFC.1(1), FDP_IFF.1(1))

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Traffic filtering SFP

- 280 The TOE (TrusGuard Gateway) protects internal network resources from external Internet users through the traffic filtering SFP, and controls external resources that internal users shall access by blocking access to the non-disclosed external resources of the public Internet.
- 281 The Access control at Network Level functions of the traffic filtering SFP consist of the packet filtering function, the network address translation function, policy exceptions, the traffic control (QoS) function and signature/behavior-based blocking functions. The traffic filtering SFP supports the packet filtering function and the network address translation function on the IPv4 and IPv6 networks.
- 282 The traffic filtering SFP is the first function to handle incoming and outgoing TOE packets. It reassembles the fragmented packets, so the packets are handled based on each security function. When the administrator sets policies to interoperate the content filtering function, the IPSec VPN function, the signature/behavior-based blocking function and the network traffic control function, the TOE handles packets based on the packet filtering rules and then forwards packets to the interoperated functions.

Packet filtering

- 283 The TOE (TrusGuard Gateway) performs the information flow control based on actions specified in the matching rules by comparing incoming traffic information security attributes (source IP address, destination IP address, services (protocols and ports), physical network ports of the TOE (TrusGuard Gateway) sending and receiving traffic and time) with information flow control security policy attributes. **(FDP_IFC.1(2), FDP_IFF.1(2))**
- 284 The packet filtering rules for the TOE (TrusGuard Gateway) are configured with source IP addresses, destination IP addresses, services (protocol and port), actions, schedule, remaining logs after cleanup, enabling/disabling proxy and QoS. The control rules that are applied for TOE packet filtering functions are listed in [Table 7-3]. The related security management functions are described in the security policy target (object) management and Access control at Network Level policy management.

[Table 7-3] Information flow control methods for Access control at Network Level policies

Action	Information flow/access control contents
--------	--

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Allow	If the information security attributes (source IP addresses, destination IP addresses, services (protocol and port)) are matching with the packet filtering rules, those information flows are 'allowed'.
Block	The TOE (TrusGuard Gateway) blocks all information flows that do not match with 'allowed' packet filtering rules. It blocks all information flows whose actions of security policies are explicitly set as 'blocked'.
Security level	By comparing the security level (High, moderate and low) specified in the security attributes with the security level of the subject and the communication target, the TOE 'allows' information flows if the security level of the subject is equal or higher than the security level of the communication target.

285 Further, the TOE (TrusGuard Gateway) blocks the excessive sessions if the network connection number of the TOE traffic exceeds the session number specified by the authorized administrator. In addition, the TOE (TrusGuard Gateway) denies the abnormal information flows as below.

- If the information coming from the external network IT entities has internal network subject IP addresses
- If the information coming from the internal network IT entities has external network subject IP addresses
- If the information coming from the external network IT entities has the broadcasting subject IP addresses
- If the information coming from the internal network IT entities has looping subject IP addresses
- If the information coming from the external network IT entities has abnormal packet structures

Translate network addresses

286 The Network Address Translation (NAT) is a function to translate and forward IP addresses and service ports between adjacent networks for packet passing through the TOE. The NAT assigns public IP addresses for internal users to access to the external public networks or public IP addresses for the internal server. In the mixed IPv4 and IPv6 network environment, it provides translation function between IPv4 addresses and IPv6 addresses. **(FDP_IFF.1(2))**

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

287 The NAT functions are classified as network port-based NAT functions and policy-based NAT functions. The network port-based NAT function can be configured with Dynamic NAT, Static NAT, non-translation and LSNAT(Load-Sharing NAT) in respect of the purpose. The policy-based NAT has higher priority than the network port-based NAT.

Policy exceptions

288 The TOE (TrusGuard Gateway) performs policy exception functions based on security attributes (source IP addresses, destination IP addresses/service ports and protocols when the traffic is coming from the internal network or the external network). The TOE (TrusGuard Gateway) allows traffic information flows that match with the policy exception rules registered by the authorized administrator through security management interfaces. **(FDP_IFC.1(2), FDP_IFF.1(2))**

289 The details of adding/changing/deleting policy exception rules can be found in the policy exception management section. Among TOE user data protection functions, the information flow control function with policy exceptions has the highest priority.

Traffic control (QoS)

290 Even when information flows of incoming traffic are allowed by the packet filtering function, the TOE (TrusGuard Gateway) provides traffic control functions to enforce traffic control functions on the session that interrupts other information flows by generating excessive traffic. When the traffic bandwidth is bigger than the threshold value specified by the authorized administrator, the TOE controls the traffic bandwidth in case that the packet filtering function is interoperated, the large web traffic setting is applied, or address-specific traffic control policies of the signature/behavior-based blocking functions are applied. **(FDP_IFF.1(2))**

Abnormal Traffic blocking (Signature-based blocking)

291 The abnormal Traffic blocking (Signature-based blocking) function is an additional Access control at Network Level function to control information flows based on countermeasures specified by the authorized administrator. When the traffic is coming from the internal network or the external network of the TOE (TrusGuard Gateway), it controls information flows if their security attributes such as source IPv4 addresses, destination IPv4 addresses, services (protocol and port) and packet data (header and payload) are matching with the rules of the TOE (TrusGuard Gateway). In other words, it allows the information flow if the incoming information does not match with the rules. If it matches with the rules, the information flow is controlled by

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

the specified actions. (FDP_IFC.1(2), FDP_IFF.1(2))

- 292 The TOE can control detected attacks in accordance with rules specified by the authorized administrator through blocking, session termination, system quarantine and usage restriction methods. Actions for each rule are listed in [Table 7-4].

[Table 7-4] Information flow control methods for Signature-based blocking rules

Rules	Actions
Allow	Allow the information flow request if the action specified on that information (source IPv4 addresses, destination IPv4 addresses, services (protocol and port) and packet data (header and payload)) is set to 'Allow'.
Block	Deny or block the information (packet) transmission.
Session termination	Terminate the session related with the information (packet).
System quarantine	Deny the information (packet) transmission and quarantine the IP addresses that cause excessive traffic. The information quarantine is continuously maintained or automatically dismissed after a certain period set by the authorized administrator.
Usage restriction	Restrict the bandwidth of the traffic. Deny the transmission of the information that exceeds the allowed capacity usage.

Abnormal Traffic blocking (Behavior-based blocking)

- 293 The abnormal Traffic blocking (Behavior-based blocking) function is an additional access control at Network Level to perform behavior-based information flow control functions such as Dos blocking, DDoS blocking, scanning blocking and abnormal traffic blocking based on the specified information flow control policies when the network traffic is coming to the TOE (TrusGuard Gateway).
- 294 The TOE (TrusGuard Gateway) provides the DoS/DDoS attack to prevent behaviors causing network service interruptions of the TOE (TrusGuard Gateway) as malicious users or worm virus generate excessive network service requests that cannot be handled normally. The TOE (TrusGuard Gateway) determines the method to detect network traffic attacks with statistical methods (ex: flooding attacks). In other words, the TOE detects attacks based on the traffic bandwidth and handles them in accordance with rules specified by the authorized administrator.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

The authorized administrator can set up the TOE to handle attacks with blocking, system quarantine and usage restriction methods through behavior-based blocking functions.

(FDP_IFC.1(2), FDP_IFF.1(2))

295 The TOE (TrusGuard Gateway) ensures the normal service by effectively detecting and handling DoS attacks that might incapacitate the network or specific services. In short, it detects and handles social engineering DoS attacks against random users or IP spoofed DoS attacks. Further, the TOE (TrusGuard Gateway) provides detection/blocking functions against scanning attacks. The TOE detects and blocks scanning attacks by analyzing traffic with the specific IP address. It provides the protocol or port-centric anti-scanning functions in accordance with the pattern matching-based rules. As the TOE can detect/block unknown scanning attacks, various behaviors like pre-information collections (photo scan and IP scan) can be detected and blocked.

296 The TOE (TrusGuard Gateway) can detect/block abnormal traffic that the DoS/DDoS and anti-scanning cannot detect such as: connection attempts from the abnormal IP addresses, connection to the IP segments that are not used in the internal network, connections to the ports that are no longer serviced, a large number of TCP connections without 3-way handshaking, abnormal combinations of packet levels (IPv4 header verification, TCP, UDP, ICMP header verification) and traffic occupying more than the specified threshold. Actions for each rule are listed in [Table 7-5].

[Table 7-5] Information flow control methods for behavior-based blocking rules

Rules	Actions
Allow	Allow the information flow request if the action specified on that information (source IPv4 addresses, destination IPv4 addresses, services (protocol and port), packet data and time) is set to 'Allow'.
Block	Deny or block the information (packet) transmission.
System quarantine	Deny the information (packet) transmission and isolate IP addresses that cause excessive traffic. The information quarantine is continuously maintained or automatically dismissed after certain period set by the authorized administrator.
Usage restriction	Deny the transmission of the information that exceeds the allowed capacity usage by restricting the bandwidth of the traffic.
DDoS attack blocking	Block or deny the information (packet) that exceeds the accepted

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Rules	Actions
	values. For example, it detects packets or traffic that is higher than the specific values for a certain period of time.

Content filtering SFP

- 297 The content filtering SFP function is a TOE additional function to control information flows of TOE traffic for each service through application proxy functions. The content filtering functions are classified as DNS, FTP, General, HTTP, POP3, SMTP, SQLNet and UDP proxies to handle information flows in accordance with administrators' policies for each protocol. In addition, it performs filtering functions by interoperating with virus blocking, spam mail blocking, website filtering and anti-malsite filtering functions.
- 298 The content filtering function controls information flows if the security attributes of source IPv4 addresses, destination IPv4 addresses, services (protocol and port), packet data (header and payload) match with contents filtering rules. It allows information flows if the security attributes does not match with content filtering rules.
- 299 If the user authentication is set for general, HTTP and FTP proxies, the user identification and authentication are performed through the TOE (Authentication Client) and the connection requests are allowed for the authorized users.
- 300 As the content filtering function handles information flows through the proxy for each service, it leverages the network address translation functions that can change packet destination IP addresses and the service port number into TOE IP addresses and its proxy port number, handles the changed information flows and then changes them back to the original destination IP addresses and the port numbers.
- 301 If the number of TOE traffic sessions exceeds the concurrent connection number specified for each service, the session restriction function blocks the excessive sessions. If the 'redirection host' is specified, it changes traffic destination IP addresses and port numbers to redirect the traffic to that host.

Malicious code blocking

- 302 The TOE (TrusGuard Gateway) provides malicious code detection and blocking functions against malicious codes (ex. virus or worm) by interoperating with malicious code engines. The TOE

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

(TrusGuard Gateway) provides malicious code blocking functions for the SMTP proxy, the POP3 proxy, the HTTP proxy and the FTP proxy.

- 303 If the malicious code blocking function is enabled, the TOE (TrusGuard Gateway) requests virus scans for packet data (file) among security attributes of incoming traffic by calling malicious code engines. If the malicious codes are not detected, the TOE allows the information flow by modifying attached files. If malicious codes are detected, the TOE applies malicious code actions specified by the authorized administrator.²¹

Spam mail blocking

- 304 The TOE (TrusGuard Gateway) provide anti-spam functions for the SMTP proxy and the POP3 proxy. For the SMTP proxy, if the authorized administrator sets control rules as Block, the TOE transfers the blocked e-mail list to the IT entities (log servers) specified by the authorized administrator by changing e-mail body or sending out a blocked sender reply to the sender. If the authorized administrator sets the control rules as 'Allow', the TOE sends the e-mail by adding the header specified by the authorized administrator into the e-mail subject. For the POP3 proxy, the TOE sends the e-mail by adding the header specified by the authorized administrator into the e-mail subject. The authorized administrator can specify and manage the start-up and shut-down of anti-spam functions and detailed attributes of rules.
- 305 If the Anti-Spam function is enabled and the administrator interoperates with the anti-spam servers (RBL server and RPD server) through "Spam mail policy management", the TOE (TrusGuard Gateway) sends scan requests to the anti-spam server based upon source IP addresses, destination IP addresses, services (protocol and port) and packet data (payload) among security attributes of incoming traffic. According to the scan results from the anti-spam server, the TOE allows information flows that are not detected as spam mails, and blocks information flows that are detected as spam mails with actions specified with the administrator.

Website filtering

- 306 The TOE (TrusGuard Gateway) blocks connections to the harmful malsites (ex. pornography,

²¹ The malicious code blocking function used by the content filtering and the signature used by the signature-based blocking function uses are applied to the different targets. The malicious code blocking function applies to the file data parts that are attached to the SMTP, POP3, FTP and HTTP proxies, while the signature-based blocking function applies to the packet payload.

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

violence and gambling) by comparing contents with content rating DB file provided by the communications commission. In addition, it blocks website connections based upon the Platform for Internet Content Selection (PICS), a content rating specification for websites.

307 By interoperating with the Anti-MalSite file, the TOE blocks connections to phishing sites or websites inserted with malicious codes. The website filtering function can be called directly from the packet filtering or through the HTTP proxy.

7.1.4. Identification and Authentication

User identification and authentication

308 The TOEs (TrusGuard Gateway and TrusAnalyzer) perform identification and authentication for all accessing users. The TSF shall successfully identify and authorize users before allowing any action that the TSF arbitrates in lei of users. The users of the TOEs (TrusGuard Gateway, Authentication Client, SSL VPN Client and TrusAnalyzer) are classified as [Table 7-6] (**FIA_UAU.2, FIA_UID.2**)

[Table 7-6] Users to be identified for TOE access

Type	Description
TG top-level administrator	This user accesses security management interfaces (GUIs and CLIs) of the TOE (TrusGuard Gateway) and successfully completes identification and authentication enforced by the TOE. This user can use security management functions of the TOE (TrusGuard Gateway). The authorized administrators are classified as TG top-level administrators and TG general administrators based upon their 'roles'.
TrusAnalyzer top-level administrator	Thus user accesses security management interfaces of the TOE (TrusAnalyzer) and successfully completes identification and authentication enforced by the TOE. This user can use security management functions of the TOE (TrusAnalyzer). The authorized administrators are classified as TrusAnalyzer top-level administrators and TrusAnalyzer general administrators based upon their 'roles'.
TrusAnalyzer general administrator	
SSL VPN user	The user successfully completes identification and authentication to

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Description
	use the SSL VPN through the SSL VPN Client. This use can use the VPN communication through SSL VPN.
TrusGuard Auth user	The user successfully completes identification and authentication through the Authentication Client when the TOE is interoperated with the user identification and authentication among content filtering functions. The use can access the TOE through the proxy service after user verification.

309 The TOE (TrusGuard Gateway) performs the user identification and authentication when the authorized administrator attempts to access security management interfaces through web browsers (HTTPS), SSH (Secure Shell) or serial ports for security management. The TOE for TrusGuard Gateway performs the user identification and authentication through the TOE for Authentication Client if the authorized administrator set proxy and user authentication in the "Access control at Network Level policy management". The TOE for TrusGuard Gateway enforces 'authentication' against the general proxy, the FTP proxy and the HTTP proxy. The password is displayed as masking values (ex: Replace the typed values with '*'). If the authentication fails, the TOE does not provide reasons for the authentication mechanism failure to ensure the safe identification and authentication. **(FIA_UAU.2, FIA_UAU.7, FIA_UID.2)**

310 If the authorized user attempts to access for security management and security audit, the TOE uses the re-utilization prevention mechanism to prevent users from re-using the authentication information. The TOEs for TrusGuard Gateway, TrusAnalyzer and SSL VPN Client prevents re-utilization of authentication information through session timestamps provided by the SSL/TLS, while the TOE for Authentication Client prevents re-utilization of authentication information through one-time password (OTP) authentication. **(FIA_UAU.4)**

User authentication failure handling

311 The TOE protects the TOE from malicious authentication attempts of unsolicited users through the authentication delay and user account locking after the specified number of failed authentication attempts.

312 The TOEs (TrusGuard Gateway and TrusAnalyzer) will lock out the user account and delays the user authentication for the specified time period (default value: 5 minutes) after the specified number of failed authentication attempts (Default value: 5 times). **(FIA_AFL.1(1))**

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

313 The user account that tries to log in through the TOEs for Authentication Client and SSL VPN Client will be locked out after the specified number of failed authentication attempts. The number of failed authentication attempts is specified 5 times by default but the TG top-level administrator can specify the number from one to five. The user account will be locked out for the specified time period (default value: 30 minutes) after the specified number of failed authentication attempts. The TG top-level administrator can unlock the locked general user accounts. (FIA_AFL.1(2), FMT_MTD.2)

User security attributes: Authorized administrators/authorized log administrators

314 The TOEs (TrusGuard Gateway and TrusAnalyzer) maintain the security attribute list including passwords and access permissions of authorized administrators and authorized log administrators. The authorized administrators are classified as the TG top-level administrators and the TG general administrators, while the authorized log administrators are classified as the TrusAnalyzer top-level administrators and the TrusAnalyzer general administrators. The user security attributes are classified based upon password and access permissions. (FIA_ATD.1)

[Table 7-7] Security attributes of authorized administrators

Type	Description
Password	The attribute to authorize the identification information of the authorized users
Access permissions	The permission attributes given to the authorized administrators

User security attributes: Authorized general users /IT entities

315 The TOE (TrusGuard Gateway) maintains security attributes such as passwords and security levels for general users who are forced to go through the user authentication. The authorized users are classified as TrusGuard Auth users and SSL VPN users. The TOE maintains security attributes of IP addresses and shared keys between IT entities (The TOE components for IPSec VPN communication). (FIA_ATD.1)

[Table 7-8] Authorized general users / Security attributes of IT entities

Type	Description
Password	The attribute to authorize the identification information of the authorized users

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Description
Security level	Security levels (High, moderate and low) for user accounts
IP address	IPv4 addresses to identify IT entities
Shared key	Keys to encrypt and decrypt data between VPN communication targets

Password verification

- 316 The TOE (TrusGuard Gateway) enforces password verification criteria (accepted characters, combination rules, maximum/minimum lengths) to meet the defined password acceptance criteria. **(FIA_SOS.1)**

[Table 7-9] Password convention rules to authorize administrators

Type	Description
Accepted characters	- 52 alphabets (Upper cases + lower cases : a ~ z, A ~ Z), number (Decimal: 0 ~ 9), special characters
Combination rules	- Exclude dictionary words - Include at least one alphanumeric character or number - Passwords are invalid if more than 5 consecutive characters/number strings or vise versa are included (ex: abcd1234 cannot be used as a password because 6 character sets ('ab', 'bc', 'cd', '12', '23', '34') are consecutive.) - Passwords are invalid if the same character is used more than 3 times
Maximum/minimum lengths	- 9 ~ 15 characters (9 ~ 15 bytes)

7.1.5.Security Management

- 317 The authorized administrator accesses the TOE through security management interfaces (HTTPS, SSH or Serial) and performs security management functions after installing the TOE. The TOE allows user accesses to security management interfaces only when the administrators successfully complete identification and authentication of the TOE and attempt to access the TOE through explicitly allowed remote management systems (IT entities).

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

318 The security management functions of the TOE can be classified as 'security function management', 'security attribute management', 'TSF data management' and 'security roles'.

Security function management

319 The TOEs (TrusGuard Gateway and TrusAnalyzer) provide the authorized administrator with the functions to change, stop and resume behaviors of each TOE security function. The authorized administrator can change TOE security functions based upon administrators' permissions. The authorized administrators can be classified as two groups: full-control administrators and read-only administrators. The assigned security functional management is different depending on the role. **(FMT_MOF.1, FMT_SMF.1)**

320 The authorized administrator can perform the following security function management of the TOE (TrusGuard Gateway) described in [Table 6-9].

- Backup and restore: Provide the authorized administrators with management interfaces to backup or restore TOE operating files (important files to configure the TOE) in the second memory devices through the administrator system. According to the values specified by the authorized administrator, the TOE (TrusGuard Gateway) sets up passwords for the backup files, encrypts those files, and transfers them to the administrator system. The TG general administrators can perform only backup functions.
- Alert setting: The authorized administrators can analyze potential TOE security violation events and set up alert criteria and actions when potential security violation events (ex. a rising CPU, memory and disk usage thresholds) occur. The TOE transfers security alerts through e-mails and SMS in accordance with alert settings of the authorized administrator.
- Audit data creation setting: The authorized administrator can create specific audit data that are selected from the entire audit data created by the TOE (TrusGuard Gateway). Depending on the log type, the usage settings for created audit data can be changed.
- Log server interoperation setting: The authorized administrator can set up the log server interoperation to transfer audit data. The TOE for TrusGuard Gateway interoperates with the TOE for TrusAnalyzer installed in the same device to send audit data.
- SNMP setting: The SNMP (Simple Network Management Protocol) functions are supported to transfer system status information of the TOE TrusGuard Gateway through SNMP, the authorized administrator can set up SNMP communities, and the TOE for

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

TrusAnalyzer becomes a SNMP server to receive the system status information of the TOE TrusGuard Gateway.

- TrusGuard Manager inter-operation: The authorized administrator sets up interoperation with TrusGuard Manager and the security management server of the TOE for TrusGuard Gateway. The TOE for TrusGuard Gateway receives and applies update and security management commands from the TrusGuard Manager.
- Integrity check: The authorized administrator checks integrity of TSF data and TSF execution codes with integrity check functions, and initializes integrity values with update functions.
- Update: The TOE for TrusGuard Gateway provides the authorized administrator with functions for signature-based rule update, behavior-based rule update, malicious code engine update, content rating DB update, Anti-MalSite file update and firmware update. The TOE (TrusGuard Gateway) manually performs the updates in accordance with update commands of the authorized administrator, or automatically performs the updates within the period of time specified by the authorized administrator. The TG general administrator has the permission to perform signature/behavior-based rule updates.
- HA function: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to add/change/delete HA audit port objects, start/stop HA functions and query HA operating status and audit port lists. It also transfers security policies to the slave system and synchronizes them with the HA policy synchronization function.
- Access control at Network Level policy (function): The authorized administrator can set up and change security functions for the IPv4/IPv6 packet filtering.
- Restrictions on large web traffic: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change bandwidth thresholds of web traffic control and enable/disable functions.
- Signature/behavior-based blocking policy setting: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change settings for signature/behavior-based blocking functions and enable/disable signature/behavior-based blocking functions. The authorized administrator can enable/disable signature/behavior-based blocking functions and change other setting values (ex: sorting criteria for each applicable policy).
- DDoS blocking setting: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change DDOS function settings. The authorized administrator changes policy application times, DDoS monitoring port settings, TCP

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

SYN flooding response MSS value, Network Segment Protection, HTTP GET Flooding attack blocking and HTTP port settings.

- System quarantine setting: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change system quarantine function settings. The authorized administrator can change system isolate setting of auto removal of quarantine, quarantine time and messages.
- IPsec VPN setting: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change IPsec VPN function settings. The authorized administrator can change IPsec VPN settings (ex: enable/disable IPsec VPN, DPD and NAT connection duration).
- SSL VPN setting: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change SSL VPN function settings. The authorized administrator can change SSL VPN settings (ex: enable/disable SSL VPN and VPN gateway, client IP range).
- CRL list management: The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change certification revocation lists.
- Contents filtering security policy (function): The TOE (TrusGuard Gateway) provides the authorized administrator with functions to change content filtering security policies.

321 The authorized administrators can perform the following functions using security management functions of the TOE (TrusAnalyzer).

- TrusAnalyzer security function setting: The TOE (TrusAnalyzer) provides functions to enable/disable security functions and change usage setting by changing various security functional settings including The TOE (TrusAnalyzer) mail server settings, notification settings, alert settings and disk cleanup settings.
- TrusAnalyzer security function commands: Provide authorized administrators with security functions for integrity check, backup and recovery.
- Log forwarding setting: The TOE (TrusAnalyzer) provides the authorized administrator with functions to change the settings that transfer the retained audit data to the SysLog server.
- Disk cleanup setting: The TOE (TrusAnalyzer) provides the authorized administrator with functions to set up the threshold to avoid the full usage of the audit data storage and change the disk cleanup settings that delete the oldest audit data.
- Auto backup setting: The TOE (TrusAnalyzer) provides the authorized administrator with

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

functions to change auto backup settings for audit data and systems.

- Mail server notification setting: The TOE (TrusAnalyzer) provides the authorized administrator with functions to change alert mail settings to perform alert functions.
- Spam and statistics information transmission setting: The TOE (TrusAnalyzer) provides the authorized administrator with functions to change spam and statistics information settings that transfer Anti-Spam log lists received from the TOE (TrusGuard Gateway) in the alert e-mail format.
- Alert setting: The TOE (TrusAnalyzer) provide the authorized administrator with functions to change alert settings that check the resource information of the TOE (TrusGuard Gateway) and send out alert e-mails if the threshold specified by the authorized administrator is exceeded.
- TrusAnalyzer integrity check: The TOE (TrusAnalyzer) provides the authorized administrator with functions to perform integrity check and update integrity check results.
- TrusAnalyzer data restore: The TOE (TrusAnalyzer) provides the authorized administrator with functions to restore settings to the normal point-in-time.
- TrusAnalyzer manual backup: The TOE (TrusAnalyzer) provides the authorized administrator with functions to manually back up TOE settings.
- Report query: The TOE (TrusAnalyzer) provides functions to query each statistics report and create/change/delete integrate reports.
- Integrate report creation: The TOE (TrusAnalyzer) provides the authorized administrator with functions to change integrated report creation settings. TrusAnalyzer general administrators can change integrated report creation settings.

Security attribute management

322 To partially control information flows of incoming/passing/outgoing TOE traffic, the TOE (TrusGuard Gateway) enforces VPN SFP, traffic filtering SFP and content filtering SFP to limit query, change and deletion capabilities of subjects and information security attributes based upon security roles specified by the authorized administrators. **(FMT_MSA.1, FMT_SMF.1)**

323 The TG top-level administrator can query, change and delete VPN SFP security attributes listed in [Table 7-10], while the TG general administrator can only 'query' the security attributes.

[Table 7-10]VPN SFP security attributes

Type	Security attribute	Description
------	--------------------	-------------

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Security attribute	Description
Subject	Source IPv4 address	IP addresses of TOE components (VPN communication targets) or external IT entities (subjects)
	Destination IPv4 address	
information	Source IPv4 address	Source IP addresses and destination IP addresses of transmission data
	Destination IPv4 address	
	Service (protocol and port)	Protocols and port number of transmission data

324 TG top-level administrators can query, change and delete security attributes of traffic filtering SFP listed in [Table 7-11], while TG general administrators can only 'query' security attributes.

[Table 7-11]Traffic filtering SPF Security attributes

Type	Security attribute	Description
Subject	Source IPv4/IPv6 address	IPv4/IPv6 addresses of TOE components (VPN communication targets) or external IT entities (subjects)
	Destination IPv4/IPv6 address	
information	Source IPv4/IPv6 address	Source IPv4/IPv6 addresses and destination IPv4/IPv6 addresses of transmission data
	Destination IPv4/IPv6 address	
	Service (protocol and port)	Protocols and port number of transmission data
	Security level	Security levels of IP address objects of transmission data
	Packet data (header and payload)	Packet headers and payloads of transmission data

325 TG top-level administrators can query, change and delete security attributes of content filtering SFP list in [Table 7-12], while TG general administrators can only 'query' security attributes.

[Table 7-12]Content filtering SFP Security attributes

Type	Security attribute	Description
Subject	Source IPv4 address	IP addresses of TOE components (VPN communication targets) or external IT entities (subjects)

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

Type	Security attribute	Description
information	Identifier	TrusGuard Auth user ID
	Password	TrusGuard Auth user password
	Source IPv4 address	Source IP addresses and destination IP addresses of transmission data
	Destination IPv4 address	
	Service (protocol and port)	Protocols and port number of transmission data
	Packet data (header and payload)	Packet headers and payloads of transmission data
	Time	Timestamp information of transmission packets

- 326 The TSF not only provides limited default values of security attributes to enforce each SFP but also provides the authorized TG top-level administrator with permissions to specify the selective default values to replace the default values. **(FMT_MSA.3, FMT_SMF.1)**

TSF data management

- 327 The TOE provides the authorized administrator with functions to query, create, change and delete TSF data lists for audit data the TOE in [Table 6-12]. The following items are TSF data that the TOE (TrusGuard Gateway) manages. TG top-level administrators have full permissions, while TG general administrators have a query-only permission. **(FMT_MTD.1, FMT_SMF.1)**

- Administrator account setting value
- Update setting value
- Selective audit data creation setting value
- Audit data transmission setting value
- SNMP setting value
- Security alert setting value
- Security alert mail/SMS settings
- TOE identification (host) name
- Time setting value
- License information
- Authentication certificate setting value
- HA setting information:

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- Monitoring port (Physical ports, local/remote devices virtual IPv4 addresses, Ping enablement) list information
- HA setting information:
- HA settings (Usage enabled, priority, connection NIC, remote device IPv4 addresses, Heart beat status)
- Signature/behavior-based blocking policy setting value
- System quarantine setting value
- IPSec VPN network setting value
- Auto key setting value
- Manual key setting value
- IPSec VPN setting value
- SSL VPN network setting value
- SSL VPN user setting value
- SSL VPN connection website setting value
- SSL VPN setting value
- Local certificate setting value
- CA certificate setting value
- Certificate profile
- Proxy service object list: Proxy setting value
- Proxy service object list: Proxy group setting value
- Concurrent proxy connection number/Proxy process setting value

328 The following items are TSF data that the TOE (TrusAnalyzer) manages. TrusAnalyzer top-level administrators have full permissions to query, create, change and delete TSF data lists ([Table 6-14]), while TrusAnalyzer general administrators have a query-only permission.

- The TOE (TrusAnalyzer) administrator account setting value
- The TOE (TrusAnalyzer) log forward setting value
- The TOE (TrusAnalyzer) disk cleanup setting value
- The TOE (TrusAnalyzer) auto backup setting value
- The TOE (TrusAnalyzer) mail server and notification setting value
- The TOE (TrusAnalyzer) spam and statistics information transmission setting value
- The TOE (TrusAnalyzer) alert setting value
- The TOE (TrusGuard Gateway) device connection setting value
- Connected TOE (TrusGuard Gateway) resource status information

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

- Connected TOE (TrusGuard Gateway) network status information
- The TOE (TrusGuard Gateway) system log
- The TOE (TrusGuard Gateway) system status log
- The TOE (TrusGuard Gateway) firewall log
- The TOE (TrusGuard Gateway) signature/behavior-based blocking log
- The TOE (TrusGuard Gateway) system quarantine log
- The TOE (TrusGuard Gateway) content filtering log
- The TOE (TrusGuard Gateway) website filtering log
- The TOE (TrusGuard Gateway) virus blocking log
- The TOE (TrusGuard Gateway) Anti-Spam log
- The TOE (TrusGuard Gateway) SSL VPN log
- The TOE (TrusGuard Gateway) DNS proxy log
- The TOE (TrusGuard Gateway) QoS log
- The TOE (TrusGuard Gateway) Anti-malsite log
- The TOE (TrusGuard Gateway) QoS log
- The TOE (TrusAnalyzer) system log

329 The TOE for TrusGuard Auth allows the authorized TrusGuard Auth users to change TrusGuard Auth passwords (TSF data), while the TOE for SSL VPN Client allows the authorized SSL VPN users to change SSL VPN Client user passwords (TSF data), and query and change SSL VPN Client setting values.

330 The TOEs (TrusGuard Gateway and TrusAnalyzer allow the authorized administrators (TG top-level administrators and TrusAnalyzer top-level administrators) to specify audit storage capacity and the threshold for failed authentication attempts. When the TSF data reaches or exceeds the threshold, the TSF perform authentication failure handling as a countermeasure for the possible audit data loss and integrity check through TSF self-testing. **(FMT_MTD.2, FMT_SMF.1)**

331 Further, the TSF receives only verified safe values to prevent various vulnerabilities like SQL injection through functions to verify valid values and entry values. **(FMT_MTD.3, FMT_SMF.1)**

Security roles

332 The TOE provides users with security capabilities to perform security management functions based on the authorized user roles. The authorized administrators are classified as TG top-level administrators, TG general administrators, TrusAnalyzer top-level administrators, TrusAnalyzer

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

general administrators, SSL VPN users and TrusGuard Auth users and they can perform security functions of TOE components based on their permissions. **(FMT_SMR.1)**

- The security roles defined in the TOE (TrusGuard Gateway) are as below.
 - TG top-level administrator: The authorized administrators have full permissions (Read/Write) for security functions of the TOE (TrusGuard Gateway). For the TOE for TrusGuard Gateway, only one TG top-level administrator account can exist.
 - TG general administrator: The authorized administrators have a read-only permission for security functions of the TOE (TrusGuard Gateway), except signature/behavior-based rule update and integrity check.
 - SSL VPN user: The user successfully completes user identification and authentication based on ID and password through SSL VPN functions.
 - TrusGuard Auth user: The user successfully completes user identification and authentication based on ID and password among users who are required to go through proxy functions.
- The security roles defined to the TOE (TrusAnalyzer) are as below.
 - TrusAnalyzer top-level administrator: This administrator can use all security management and security audit functions of the TOE (TrusAnalyzer).
 - TrusAnalyzer general administrator: This administrator has a read-only permission for all audit data and statistics reports, read/change permissions for TrusGuard Gateway device management setting specified by the TOE (TrusAnalyzer) top-level administrator, and creation/ change permissions for integrated reports.

7.1.6.TSF Protection

333 The TOEs (TrusGuard Gateway and TrusAnalyzer) perform the self-testing to ensure accurate TOE operation and integrity of TSF data and TSF execution codes.

Self-tests

334 The TSF periodically performs the self-testing to ensure the accurate operation of the TOE (TrusGuard Gateway and TrusAnalyzer) processes during operation and startup. The TSF checks the status of main security functional processes and performs self-testing at the process restart

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

upon the detection of abnormally terminated processes. The TOE shall execute process management demons and CLI demons with initialization scripts of the operating system, and perform the self-testing against the processes specified by the administrator, security policy management demons, updates and log demons to accurately operate processes. **(FPT_TST.1)**

- 335 The TOE provides integrity check functions to the authorized administrators (TG top-level administrators and TrusAnalyzer top-level administrators) to protect TSF data integrity. The authorized administrator can perform integrity checks against environment setup files, TSF data rule files and execution files of TSF execution codes. The TOE creates hash values for integrity checking items and compares them with the latest hash values (baseline values). The TOE (TrusAnalyzer) creates and saves hash values for integrity checking items at the time of the TOE installation, while the administrator creates hash values for integrity checking items at the time of integrity check and compares them with the saved hash values. If the TOE (TrusGuard Gateway and TrusAnalyzer) detects the integrity violation, the results are displayed to authorized administrators through security management interfaces. The TOE provides the authorized administrator with integrity update functions as countermeasures. **(FPT_TST.1)**

7.1.7.TOE Access

- 336 The TOEs (TrusGuard Gateway and TrusAnalyzer) performs session termination functions of security management interfaces by checking TOE user inactive periods.

User session termination

- 337 The TOE (TrusGuard Gateway) terminates the interactive session of the connected administrator if the authorized administrator (TG top-level administrator or TG general administrator) who logs in through user identification and authentication does not perform any action for a specified inactive time period. The session timeout period is 10~600 seconds (default value: 600 seconds) for web-based SSL/TLS interfaces and 10~600 seconds (default value: 600 seconds) for CLI (SSH and Serial) connection. **(FTA_SSL.3)**
- 338 The TOE (TrusAnalyzer) terminates the interactive session of the connected administrator if the authorized administrator (TrusAnalyzer top-level administrator or TrusAnalyzer general administrator) who logs in through user identification and authentication does not perform any action for a specified inactive time period. The session timeout period is 10 minutes for web-

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

based SSL/TLS interfaces. **(FTA_SSL.3)**

- 339 The TOE terminates the interactive session of the connected SSL VPN users and TrusGuard Auth users if the authorized users do not perform any action for a specified inactive time period. SSL VPN user sessions are terminated if the authorized users do not perform any action for the specified inactive period (5 minutes) that allows information flows based on the rules specified with the 'SSL VPN' security attributes among the information flow control policies in accordance with FDP_IFF.1(1).
- 340 TrusGuard Auth user sessions are terminated if the authorized users do not perform any action for the specified inactive period (30 minutes) that allows information flows through 'user authentication' based on the proxy functions. The TOE (TrusGuard Gateway) creates audit data for this incident. **(FTA_SSL.3)**

7.1.8.Trusted Path/Channels

- 341 The TOEs (TrusGuard Gateway and TrusAnalyzer) establish secure communication channel to protect channel data from unauthorized changes or disclosures during communication channel establishment among the TOEs and other trusted IT products or during VPN communication.

Secure channel

- 342 The TOEs for TrusGuard Gateway and SSL VPN Client provide secure paths and channels that can be logically distinguished from other communication channels from among TOE components or trusted IT entities, uniquely identify terminals, and protect channel data from unwanted changes and disclosure.
- 343 The TOE initiates communication and connects through secure VPN communication channels between TOE components (TrusGuard Gateway and SSL VPN Client). As the TOE performs data cryptographic and integrity check through secure communication channels, the transmission data is protected from unauthorized changes or disclosure. **(FTP_ITC.1)**
- 344 When the authorized administrator attempts to connect through web browsers by using SSL/TLS protocols or terminal programs by using SSH protocols to perform security management of the TOEs (TrusGuard Gateway and TrusAnalyzer), the secure communication channels are established. **(FTP_TRP.1)**

AhnLab	AhnLab Inc.			CC Part3 V3.1r4
	Type	Version	Date	
	CC certification	1.8	2013-07-30	

AhnLab

Copyright © AhnLab, Inc. 2010. All rights reserved.

AhnLab, the AhnLab log, and V3 are trademarks or registered trademarks of AhnLab, Inc., in Korea and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.