Samsung OfficeServ 7400 GWIMC Security Target

Document Type
Language Code /
Total page
Create /
Exam /
Approve /
Registered
Date
Item Code

Revision History

Date	Purpose	Description	Author	Approved By	Ver
2007-02-25	Initial draft		Dong Yoon, Jang	Tae Yong, Park	1.0
2008-02-13	First revision	Revised in accordance with EOR-01	Dong Yoon, Jang	Tae Yong, Park	1.1
2008-04-08	Second revision	Additional changes	Dong Yoon, Jang	Tae Yong, Park	1.2
2008-04-28	Third revision	changed the TOE configuration identifier	Dong Yoon, Jang	Tae Yong, Park	1.3
2008-06-13	Partial revision	Revised with respect to file integrity	Dong Yoon, Jang	Tae Yong, Park	1.4
2008-06-25	SSL version modification	Revised in accordance with the SSL version modification	Dong Yoon, Jang	Tae Yong, Park	1.5
2008-07-18	Corrected typographical errors	Corrected typographical errors	DY. Jang, HW. Cha, TY. Park	PB.Lim	1.6

Table of Contents

1. Introduction

This document is the Security Target (ST) for GWIMC V1.0 (hereinafter, GWIMC), which is security firmware, and SysLogStore V1.0 (hereinafter, SysLogStore), which is a software program for installation in an administrator PC. Both comprise the security function of Samsung OfficeServ 7400 GWIMC and are components of the Target of Evaluation (TOE) referenced in this ST. OfficeServ 7400 GWIMC (hereinafter, the TOE) designates both TOE components referenced in this ST. The purpose of this ST is to describe the security environment, security objectives, security function, and assurance requirements for the TOE.

The purpose of this chapter is to clearly describe the designations, conventions, and terminologies used in this ST. The TOE controls information flows among networks and encrypts traffics exchanged among reliable networks. The TOE supports the virtual private network (VPN) function using IPSec and the firewall system that performs network access control based on packet filtering. It is installed on GWIMC hardware equipment. In addition to the firewall and VPN functions, the TOE contains the security management, audit log, identification and authentication, and other security support functions for those two functions.

1.1. Security Target and TOE Identification

This section provides the information needed to identify and control the TOE and this ST as follows:

Item	Description
ST Title	OfficeServ 7400 GWIMC Security Target
ST Version	1.6
Date	July 15, 2008
Author	Dong Yoon, Jang
TOE Identification	OfficeServ 7400 GWIMC
TOE Component Identification	Security function firmware: GWIMC V1.0
	Security function software: SysLogStore V1.0
Common Criteria (CC) Identification	Common Criteria V2.3
Protection Profile (PP) Identification	Firewall Protection Profile for Government V1.2 (2006. 5.17) Virtual Private Network Protection Profile for Government V1.2

	(2006. 5.17)
Assurance Level	EAL3+

1.2. Security Target Overview

This ST contains the following chapters:

- **Chapter 1: Introduction**

  This chapter provides a brief summary of the identification information for this ST, including TOE identification information, terminology and conventions used in this ST, Evaluation Assurance Level (EAL), and compliance claims.

- **Chapter 2: TOE Description**

  This chapter describes the boundaries for the TOE and provides a brief summary of the information and features of the TOE.

- **Chapter 3: TOE Security Environment**

  This chapter describes the threats against the assets protected by the TOE, TOE environment, TOE usage, organizational security policies, and assumptions.

- **Chapter 4: Security Objectives**

  This chapter describes the TOE security objectives and the environmental security objectives to meet the level required by the threat identification, organizational security policies, and assumptions mentioned in the TOE Security Environment.

- **Chapter 5: IT Security Requirements**

  This chapter describes the Security Functional Requirements (SFRs) required to achieve the TOE Security Objectives, the IT environment requirements and the Security Assurance Requirements (SARs) that prove the TOE's implementation of those security functions.

- **Chapter 6: TOE Summary Specification**

  This chapter describes the actual security functions linked to the SFRs presented in the IT Security Requirements and the evaluation evidence for SARs.

- **Chapter 7: Protection Profile Claims**

This chapter provides the identification of the Protection Profiles (PPs) claims as well as a justification to support such claims.

- **Chapter 8: Rationale**

  This chapter presents the rationale for the security objectives, security requirements, security assurance requirements, and TOE summary specifications.

1.3. Common Criteria (CC) Compliance Claims

This ST conforms to the following evaluation criteria and protection profiles.

- Firewall Protection Profile for Government V1.2, May 17, 2006 (hereinafter, FWPP)
- Virtual Private Network Protection Profile for Government V1.2, May 17, 2006 (hereinafter, VPNPP)
- Common Criteria V2.3
- Common Criteria V2.3 Part 2
- Common Criteria V2.3 Part 3
- Evaluation Assurance Level: EAL3+

Since this ST conforms to FWPP and VPNPP, which have assurance level EAL3+, the following assurance components required by a higher assurance level than EAL3 are added in addition to the assurance components required by EAL3.

Assurance component		Required Assurance Level
ADV_IMP.2	Implementation of the TSF	EAL5
ADV_LLD.1	Descriptive low-level design	EAL4
ALC_TAT.1	Well-defined development tools	EAL4
ATE_DPT.2	Testing: low-level design	EAL5
AVA_VLA.2	Independent vulnerability analysis	EAL4

1.4. Conventions and Terminology

This document is a translation of the ST written in Korean and uses a number of acronyms. This section identifies the terms used in this ST.

1.4.1. Conventions

This ST uses a number of acronyms. The conventions used in this ST are consistent with those in the Common Criteria (hereinafter, CC). The CC allows four operations to be performed on security requirements: refinement, selection, assignment, and iteration. Each of these operations is used in this ST.

- **Refinement**
  The refinement operation is used to add detail to a requirement of the CC or Protection Profiles (PPs) to which the TOE claims compliance, and thus further restricts a requirement. The results of the refinement operations are denoted by **bold text**.

- **Selection**
  The selection operation is used to select one or more options provided by the CC or PPs to which the TOE claims compliance in stating a requirement. The results of the selection operations are denoted by *underlined italicized text*.

- **Assignment**
  The assignment operation is used to assign a specific value to an unspecified parameter such as the length of a password in the CC or PPs to which the TOE claims compliance,. The results of the assignment operations are denoted by showing the value in square brackets, [assignment_value].

- **Iteration**
  The iteration operation is used when a component is repeated with varying operations. The results of the iteration operations are denoted by showing the iteration number in parentheses (iteration_number) following the component identifier.

- **ST Author**
  This operation is used to indicate the final decision of an attribute is made by the ST author. The ST author operation is denoted by the specific text in braces, { Decided by the ST author }. The results of the ST author operations are denoted by the specific text in braces { written texts by the ST author }.

- **PP Reference**

  When a part of the component for a security function requirement is contained in both FWPP and VPNPP, the text **(FWPP)** or **(VPNPP)** follows the component identifier to indicate which PP it belongs to.

1.4.2. Terminology

The terms and acronyms used in the ST are defined below.

- **Mandatory Access Control (MAC)**

  An access control method that assigns security labels to networks or system resources and allows equipment or processes to access them only if they have the corresponding security labels.

- **Object**

  An entity within the TSC that contains or receives information and upon which subjects perform operations.

- **Attack potential**

  The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources, and motivation.

- **Strength of Function (SOF)**

  A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

- **SOF-medium**

  A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

- **Integrity**

  The property indicating that information or a resource has not been modified or altered in an unauthorized manner.

- **Iteration**

One of the operations defined in the CC. The use of a component more than once with varying operations.

- **Security Label**

  A security level assigned to networks, system resources, or users who use them with mandatory access control. It is used as the base for mandatory access control decisions that allow or deny access among networks, system resources and users who utilize them.

- **Security Target (ST)**

  A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

- **Protection Profile (PP)**

  An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

- **Decryption**

  The reverse process of encryption. The conversion of encrypted data into plain text by an encryption algorithm.

- **Confidentiality**

  A security feature that keeps the data on a computer or the data exchanged between computers through communication lines from being disclosed to any user not authorized to access it.

- **Human User**

  Any person who interacts with the TOE.

- **User**

  Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

- **Selection**

  One of the operations defined in the CC. The specification of one or more items from a list in a component.

- **Identity**

  A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

- **Encryption**

  Transformation of data (called "plain text") into a form (called "cipher text") that prevents the data's original meaning from being disclosed. Storing information on a storage device or transmitting it through communication lines in the form of cipher text can protect it.

- **Element**

  An indivisible security requirement.

- **Role**

  A predefined set of rules establishing the allowed interactions between a user and the TOE.

- **Operation**

  Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

- **Operating System**

  The basic software or integrated control program that, by operating and managing a computer in a dedicated manner, provides user applications with an environment in which they can run efficiently. It is usually called OS. When a computer starts, it loads its OS first. And its core part (kernel) resides in the main memory.

- **Threat Agent**

  An unauthorized user or external IT entity that brings assets under such threats as illegal access, modification, and deletion.

- **Authorized Administrator**

  An authorized user who operates and manages Firewall and VPN securely in accordance with the TSP.

- **Authorized User**

  The authorized user who can perform an operation in accordance with the TSP.

- **Authorized General User**

  The authorized user other than authorized administrator who can perform an operation in accordance with the TSP.

- **Authentication Data**

  Information used to verify the claimed identity of a user.

- **Assets**

  Information or resources to be protected by the countermeasures of a TOE.

- **Refinement**

  One of the operations defined in the CC. The addition of details to a component.

- **Organizational security policies**

  One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

- **Dependency**

  A relationship between requirements such that the requirement depended upon shall normally be satisfied for the other requirements to be able to meet their objectives.

- **Network Address Translation**

  An IETF standard that supports the sharing of public IP addresses to allow multiple users on an internal network to connect to the Internet with one public address. The users on an internal network use private IP addresses and when they communicate with an IT entity on an external network, the NAT translates their private IP address into a public IP address.

- **Subject**

  An entity within the TSF Scope of Control (TSC) that causes operations to be performed.

- **Local Access**

  Connecting to a system directly from an administrator PC through a console cable,

without using general IP networks. Local access is available only if an authorized administrator is allowed to enter where the system is physically installed.

- **Augmentation**

  The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

- **Component**

  The smallest selectable set of elements that may be included in a PP, ST or package.

- **Communication Peer**

  An external IT entity that is mutually authenticated for secure communications with the TOE.

- **Packet**

  A block of data used in data transmission.

- **Packet Filtering**

  An information flow control mechanism that determines whether to allow or deny information of the sender or recipient to flow through the TOE, based on the header information of IP packets. The security attributes and TSF data that determine it include source IP addresses, destination IP addresses, and port addresses.

- **Target of Evaluation (TOE)**

  An IT product or system and its associated guidance documentation that is the subject of an evaluation.

- **Evaluation Assurance Level (EAL)**

  A package consisting of assurance components from CC Part 3 that represents a point on the CC predefined assurance scale.

- **Port Forwarding**

  A process used to allow an external user to access a specific server or host on an internal private network by opening a port of a router or firewall installed at the gateway area of the internal private network. For example, if the router opens port 8000, an external user can connect to the service being operated with an internal private IP

address corresponding to port 8000, in accordance with the port forwarding table.

- **Assignment**

  One of the operations defined in the CC. a specification of an identified parameter in a component.

- **AES(Advanced Encryption Standard)**

  An encryption algorithm which replaced the DES algorithm. It supports the key length of 128, 192, and 256 bits and is more secure than 3DES.

- **Alarm Free Space**

  The ratio of the free audit record space to the total audit record storage space used by the TOE to determine whether to send “1st warning” reporting that most of the storage space is exhausted.

- **ARP(Address Resolution Protocol)**

  A protocol that associates the IP address of a network entity connected to a network with its Media Access Control (MAC) address. For example, if computer A wants to communicate with computer B, computer A sends a query with the IP address of computer B to obtain B’s MAC address. Computer B looks into the IP address requested by computer A and sends its MAC address information to computer A. After that, computers A and B use the mapping information (IP address and MAC address) for the data transmission between them.

- **DNS(Domain Name System)**

  A network system that translates IP addresses into readable domain names, therefore provides the convenient Internet services. The request with a domain name is replied by the correspondent IP address.

- **HSSI(High-Speed Serial Interface)**

  HSSI provides maximum speed of 52 Mbps and is usually used to connect T3/E3 leased lines to a network equipment such as a router.

- **ICMP(Internet Control Message Protocol)**

  A protocol used to exchange error messages between a gateway and a host, which use the IP protocol that does not guarantee its reliability.

- **IETF(Internet Engineering Task Force)**

  Main standard organization for the Internet established in 1996. It is international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet and its smooth operation. The major objectives of the IETF are to provide solutions for Internet management and related technical issues, develop and use Internet related projects, and suggest short-term Internet architectures to solve technical problems.

- **IKE(Internet Key Exchange)**

  A standard that exchanges secret key materials and negotiates the encryption method between two VPN communicating peers and creates security associations for the VPN peer authentication.

- **IPSec**

  A VPN protocol suggested by the IETF. It consists of data encryption at the IP layer, encryption and integrity-guaranteeing key management by AH/ESP protocols.

- **ISAKMP(Internet Security Association and Key Management Protocol)**

  The key management protocol developed by Cisco. It specifies the format in which the data for SA management and negotiation is stored, therefore can establish multiple key exchange algorithm and encryption negotiation sessions without any key management protocol.

- **IT Entity (External IT Entity)**

  Any untrusted or trusted IT product or system located outside the TOE interacting with the TOE.

- **Iteration**

  A value indicating how many times the hash function is applied to the secret key in S/Key.

- **L2TP(Layer 2 Tunneling Protocol)**

  One of the VPN tunneling protocol suggested by IETF. It is created by combining Cisco's L2F and Microsoft's PPTP. It can create multiple tunnels between endpoints and support non-IP protocols such as IPSec, AppleTalk and IPX.

- **NTP(Network Time Protocol)**

  A network protocol used to get reliable and correct international standard time information from Internet and synchronize the system time of the TOE with it.

- **OpenSSL**

  An open source implementation of the SSL protocol. The TOE uses SSL protocol implemented by the OpenSSL. In this ST, OpenSSL refers to the SSL v3 and the OpenSSL with 1024-bit RSA encryption.

- **Point-to-Point Tunneling Protocol (PPTP)**

  A VPN tunneling protocol developed by Microsoft and 3COM. It is supported by Microsoft Windows NT series severs by default, and supports various types of packet transmissions such as IP, IPX, and NetBEUI, etc.

- **RFC(Request for Comments)**

  A document that describes the standard procedures and specifications needed for implementation of a network protocol or service written by IETF.

- **RSA**

  A public-key based encryption algorithm developed by RSA Security. RSA is a highly secure encryption algorithm that supports message encryption and digital signature and authentication. RSA uses a pair of public and private key instead of a single key for encryption and decryption between the sender and recipient. Since the sender sends a message encrypted with the public key of the recipient and the recipient can only decrypt it with the private key of the sender, it guarantees the non-repudiation, integrity, and encryption processing. In this ST, RSA refers to the RSA with 1024-bit key.

- **SA(Security Association)**

  A security session established between VPN communication peers. SA includes the exchange of secret keys, negotiation of encryption method and mutual authentication of communication peers.

- **Seed**

  In S/Key, a value used to generate a one-time password. A one-time password is

generated by applying a hash function to the result obtained by concatenating the secret key with this value.

- **SEED**

  A 128-bit symmetric block cipher algorithm developed by the Korea Information Security Agency (KISA). SEED is a national standard which the Ministry of Information and Communication mandates to apply to the private security systems used in Korea.

- **SHA(Secure Hash Algorithm)**

  A hash algorithm developed by NIST in the United States; SHA-1 is a revision of SHA. It produces a 160-bit hash value from an message of any length less than 64 bits.
  SHA-2 reinforces its security more than SHA-1 and produces a 256-bit hash value.

- **SMTP(Simple Mail Transfer Protocol)**

  A TCP/IP based standard electronic mail protocol specified in the IETF RFC2821.

- **SNMP(Simple Network Management Protocol)**

  A network monitoring and control protocol. SNMP collects the status information of devices sent from SNMP agents and manages them in integrated manner.

- **SSL(Secure Socket Layer)**

  A standard protocol used to exchange data between Web browser and web server. Encrypted data cannot be decrypted even if an unauthorized user intercepts its authentication information or exchange information ion due to the authentication encryption function. The SSL described in this ST is SSL v3 and refers to the one implemented with OpenSSL on the basis of 1024-bit RSA encryption.

- **Stop Free Space**

  In SysLogStore which stores audit logs, the ratio of free space to total storage space, used by the TOE to determine whether all the storage space has been exhausted.

- **S/Key**

  A standard for one-time passwords defined in IETF RFC 1760 and 2289. In this ST, S/Key refers to the one using 160-bit SHA-1 as its hash function.

- **TOE Security Functions (TSF)**

A set consisting of all hardware, software, and firmware of the TOE that correct enforcement of the TSP shall be relied upon.

- **TOE Security Policy (TSP)**

A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

- **TSF Data**

Data created by and for the TOE, which might affect the operation of the TOE.

- **TSF Scope of Control (TSC)**

The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

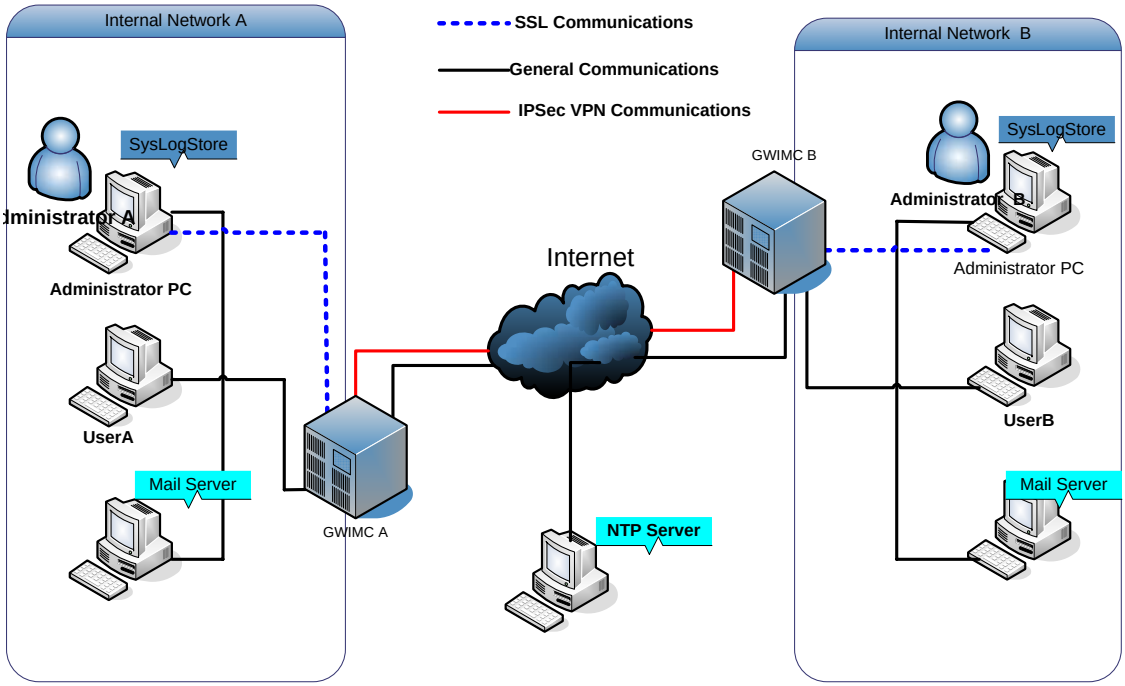
- **V.35**

A standard for high-speed synchronous data transmission of the ITU. V.35 is a de-facto leased line interface standard used by most of the routers and DSUs that provide T1 leased line service.

2. TOE Description

2.1. TOE Product Type

The TOE consists of the GWIMC installed in GWIMC hardware and the SysLogStore which is the software for audit log management and installed in the administrator PC located in the internal network where the GWIMC is installed. The TOE operates in the network configuration as shown in the figure below.



As shown in the figure above, the GWIMC A, which is operated in the internal network A, is installed in the boundary of the external network and the internal network A and performs the firewall functions to protect the internal network A from unauthorized access and network attacks. The firewall function of the GWIMC controls IP packets' access to the assets of the internal network, which are the protection targets of the TOE in accordance with the information flow control policy set, based on information contained in the IP packet headers. The purpose of the GWIMC A is to protect the internal network A from malicious information or intrusion attempts that flow in from the external network and keep network communications available by allowing authorized access.

Also, so that the GWIMC A, which is on the internal network A, performs secure

communications with the GWIMC B on the remote internal network B, both GWIMCs create a secure channel through the VPN between the internal networks and perform communications through it. When a security channel is created through the VPN between the internal networks, User A of the internal network A and User B of the internal network B can perform information communications between themselves through a secure IPSec-based channel. At this time, all traffic is encrypted. While the GWIMC is performing secure communications through a VPN, it can also contact with the external network user without secure communications.

The management of the TOE is performed through an administrator PC located in the internal network where a GWIMC is installed. The SysLogStore is also installed on the administrator PC. The SysLogStore stores and manages the audit logs transmitted from the GWIMC.

When the audit records which denote a potential security breach, or alarms on the lack of free log storage space are detected, SysLogStore sends an alert message to the authorized administrator. A mail server is need for the alarm mail operation.

The GWIMC supports the system time setting function. It can set the system time manually, or can be configured to receive reliable and exact time information from an external NTP server. With the NTP mode, an external NTP server which can operate and communicate with GWIMC correctly is needed.

The operation modes of the TOE are classified as shown in the table below for the GWIMC and SysLogStore.

	Initial Mode	Normal Mode	Emergency Mode
Occurrence Conditions	At startup and initial configuration	During normal operation	● When the system is stopped by the SysLogStore or configuration change ● system function fault
Access Method	Serial interface through the terminal program	Web browser-based GWIMC management interface	Serial interface through the terminal program
Available Functions	● Audit related configurations	All functions provided through the web	● Network interface configuration

	● Network interface configurations	browser-based interface	● Audit related configuration

<GWIMC>

	Initial Mode	Normal Mode	Emergency Mode
Occurrence Conditions	At initial installation and configuration	During normal operation	When the audit log storage space of the SysLogStore is fully used
Access Method	SysLogStore setup wizard	Management interface of the SysLogStore	Indirect access through the operating system interfaces of the administrator PC where the SysLogStore is installed
Available Functions	Initial configuration provided by the setup wizard	All functions provided by the management interface of the SysLogStore	None (No direct control is provided. Only provides indirect start and stop of the SysLogStore through the operating system interfaces of the administrator PC and audit log deletion)

<SysLogStore>

2.2. TOE Environment

2.2.1. IT Environment

The IT environment of the TOE includes the GWIMC hardware where the GWIMC is installed, operating system, the administrator PC where the SysLogStore is installed, which is used by an authorized administrator to control the TOE, an NTP server, a remote VPN gateway, and a mail server. Below are the roles and details on them.

- NTP Server

An IP address of an NTP server which is located outside the TOE is registered to the TOE by NTP server configuration function provided by the web management interface of the TOE. The NTP server periodically sends time information to the TOE when an NTP daemon is running.

- Remote VPN Gateway

Located outside the TOE and creates an IPSec protocol-based VPN at a remote location through the VPN function provided by the TOE, or creates a VPN after the negotiation to generate a secure channel requested by the TOE. The VPN gateway might be another TOE at a remote location or an application or equipment supporting the IPSec.

- Administrator PC

A PC located on the internal network where the GWIMC is installed. The administrator PC connects to the GWIMC web management interface and configures and controls the TOE through an SSL-based web browser connection. The SysLogStore is also installed in the administrator PC. It also communicates with the GWIMC through a secure SSL-based channel. The SysLogStore is installed in the administrator PC of an internal network where the GWIMC is installed. Therefore, the administrator PC must exist on the internal network.

Below are the minimum hardware, operating system, and software requirements.

Item	Description
CPU	Pentium 4 (1.0GHz)
RAM	512MByte
HDD (Audit log storage)	40GByte

Network Interface	100/10Base-T Ethernet 1 port
OS	Microsoft Windows XP SP2
Software	Microsoft Internet Explorer (Version 5.5, Encryption Level: 128 bits, JavaScript support version)

- Mail Server

If an audit log entry indicating a potential security breach occurs in the TOE-generated audit logs, or a security threat, such as full audit log storage space, arises, the SysLogStore can send an alert message to the authorized administrator via the mail server. The mail server is SMTP based. Once the IP address of this SMTP-based mail server and the e-mail addresses of the sender and recipient are registered to the TOE, when a potential security breach event occurs, an alert e-mail message containing the audit log message generated for that event is sent to the e-mail address of the authorized administrator via the mail server.

2.2.2. Operation Environment

The TOE is installed and operated at the boundary of the internal and external networks. The TOE is used in the environment where threat agents that have low-level knowledge may exist. That is, a threat agent may obtain the explicit vulnerability information and attack tools that can be used maliciously over the Internet to attack the operating system and applications. Then it may cause damage to targeted computer resources and illegally gain access to targeted information using them. The TOE is used to protect assets from threats to those explicit vulnerabilities.

2.3 TOE Scope

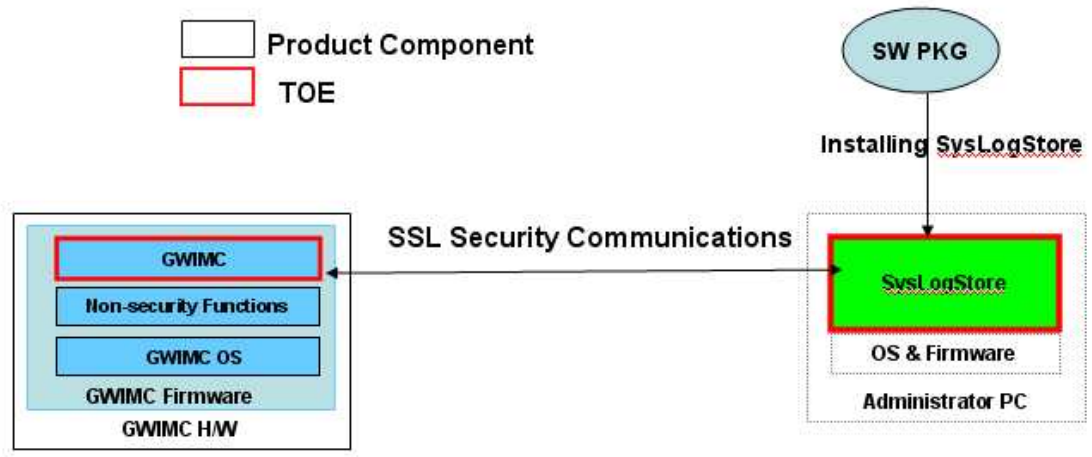
2.3.1 Physical Scope and Boundaries

Below are the components of the product that contains the TOE.

Component	Description
GWIMC Hardware	The hardware equipped with the GWIMC firmware
SysLogStore Setup File	The setup file of the SysLogStore to install on the administrator PC
Other	Communication or management, power cable, GWIMC hardware cabinet, and user manual

GWIMC hardware includes GWIMC firmware and the preinstalled TOE. The SysLogStore, which is the audit log management software, should be downloaded from the S/W license server operated by the company that developed it and should be installed and used on the administrator PC.

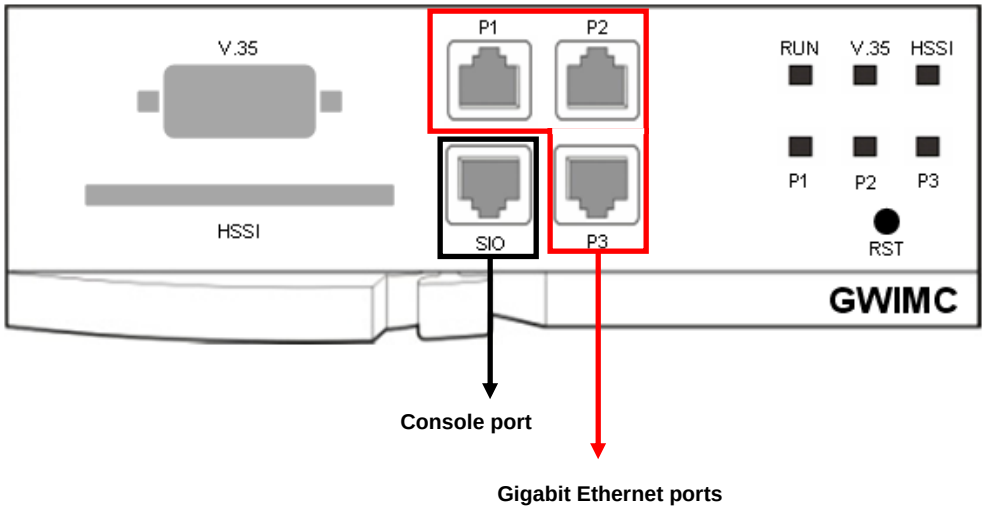
The hardware environment for TOE in a normal operational state consists of the GWIMC hardware and an administrator PC where SysLogStore are installed. It is configured as shown in the figure below.



Below are the configuration environment and the physical scope and boundaries of the TOE, which are in the operation state described above.

■ GWIMC Hardware

The hardware where TOE security functions except the SysLogStore are preinstalled. The GWIMC hardware is equipped with a Gigabit Ethernet interface for WAN or LAN. It is also equipped with the V.35 and HSSI interfaces for a leased line service and can interoperate with other vendors' switches depending on the site environment. The GWIMC hardware itself is excluded from the physical scope of the TOE. Below are the brief information on its hardware specifications, operating system, and appearance.



<Front of the GWIMC Hardware>

Item	Description
CPU	IBM750GX(1GHz)
Flash memory	32MB
DRAM	512MB
WAN	V.35 1 port, HSSI 1 port
LAN	10/100/1000 Base-T 3 ports
Console	1 port
OS	GWIMC OS V1.0

<GWIMC Hardware Specifications and Operating System>

■ GWIMC Firmware

The firmware installed in the GWIMC hardware. It is preinstalled on the GWIMC hardware. The GWIMC firmware consists of the following three components.

a) GWIMC OS – The underlying OS necessary for operating the GWIMC

b) Non-security function – A set of functions of the GWIMC firmware that have no relationship to security or are excluded from the scope of evaluation

c) GWIMC - A set of the security functions installed on the GWIMC hardware. The GWIMC is included in the TOE. It is equipped with a packet filtering firewall that controls traffic between the internal and external networks based on the IP addresses and port information of packets and the IPSec VPN functions. (L2TP and PPTP VPN functions are excluded from the TOE). Beside these functions, the GWIMC includes the security functions such as the audit function and integrity check function required by the FWPP and VPNPP.

- SysLogStore

The audit log management software. The SysLogStore is included in the TOE. It receives the audit logs generated in and sent by the GWIMC and provides the audit log collection, analysis, and retrieval functions. The SysLogStore should be downloaded from the S/W license server operated by the company that developed it and should be installed and used on the administrator PC.

2.3.2 Logical Scope and Boundaries

2.3.2.1 TOE Security Functions

- Security Audit

  The TOE generates audit logs for the security events and system events for all traffic that connect to or pass through the TOE and provides the function that flags potential security breaches. The security audit data recorded by type is sent from the GWIMC to the SysLogStore through a secure SSL-based channel and stored in the audit log storage space by the SysLogStore. An authorized administrator can view, backup, reset, and manage the storage space, as well as generate statistics for the stored audit logs using the management interface provided by the SysLogStore.

- Encryption Support

  The TOE supports an IPSec VPN configuration function. For this, generation, distribution, disposal and encryption operation of the private keys or certificates functions related to encryption are supported. Confidentiality and integrity of the sending and receiving packets are guaranteed through encryption algorithms and hash functions, such as 3DES, AES, SEED, and SHA-1. Also, the integrity and confidentiality of the IPSec VPN packets are implemented through an application of the AH and ESP. Usage is supported with a combination of the AH and ESP to guarantee integrity and confidentiality. For the mutual authentication method for communication parties, the Preshared key, X.509-based certificate, and RSA asymmetric key methods are supported. The L2TP and PPTP VPN functions are excluded from the TOE.

- User Data Protection

  An information flow control policy based on the security policy defined by the authorized administrator is applied to the information flow between the internal and external networks connected to the TOE as a connection point. Moreover, access to the TOE is only allowed for authorized administrators under its own permitted conditions only. Access to the TOE is controlled by checking ICMP packets access and registering a remote access system allowed. The TOE blocks unauthorized access to the TOE user data through the control policy for access to the TOE and controls information flow between the internal and external networks, and prevents the user data from being modified, altered, lost, or damaged by controlling the access rights of

IT entities through security attributes.

- Identification and Authentication

  The TOE performs identification and authentication functions to ensure that only authorized administrators or IT entities gain access to it. For the administrator authentication, the S/Key-based one time password and general password authentication methods are provided. The identification and authentication of the remote VPN user is performed by examining relevant security attributes, such as the IP address and authentication key. When a user fails to be authenticated or reaches the authentication failure limit, a management procedure such as imposing delay time for -authentication is performed. The TOE also checks the required secret information (password) generation and authentication condition.

- Security Management

  The TOE allows only an authorized administrator to manage and perform the TOE security functions. The authorized administrator can securely perform TSF functions, the generation, modification, deletion of TSF data and system management functions. The authorized administrator connects to the TOE through a secure SSL-based channel using the web browser of the administrator PC. The SysLogStore is installed and managed in the administrator PC. Moreover, the TOE supports the system management functions with a direct access to the GWIMC through the console interface.

- TSF Protection

  The TOE consists of a minimum set of interfaces needed to perform the TSF in the hardware, firmware, and software. It includes a mechanism that maintains a separate area that is not violated by non-TOE areas. The TOE provides diagnosis functions for the hardware where it is installed and an integrity check function for the important files required for the TOE operation.

- Secure Route/Channel

  The TOE, through the SSL protocol, provides an authorized administrator with a management channel with which to connect to it securely from an external location and provides an SSL-based secure transmission channel between the GWIMC and the SysLogStore.

- Access to the TOE

  If a specific idle time is passed for a generated SysLogStore administration session, the TOE locks the session and recovers it when re-authentication is performed successfully. For an authorized administrator allowed to connect to the TOE via the GWIMC web management interface, the session is terminated when a specific predefined idle time is passed.

2.3.2.2 Nonsecurity Functions and Features Excluded from TOE

- Network Interface Configuration

  The TOE provides the configuration and operation test functions for connecting the GWIMC hardware to the V.35, HSSI, and Gigabit Ethernet interfaces.

- Routing and Multicasting

  Through the routing function, the TOE selects an optimal route on the routing table to send packets from an internal network IP address to a destination IP address either in the external or the internal network. Moreover, if there are multiple packet destinations, rather than a single destination, the TOE provides the multicasting function that allows packets to be sent to them simultaneously.

- Network Load Distribution

  When two or more Internet lines are connected to the TOE hardware, the TOE equally distributes packet traffic between Internet lines by sending packets distributed to multiple Internet lines in accordance with the attributes (TCP port, IP address of the destination or source) of the packet-based connection sessions and enhances the service availability by automatically distributing load to other lines if a line does not operate.

- QoS

  To guarantee the quality of IP-based voice call service, the TOE supports a function that sets a minimum guaranteed transmission bandwidth, minimizing the transmission delay and loss of Internet Protocol (IP)-based voice traffic.

- DHCP

  The TOE supports assigning available IP addresses to IP devices, such as PCs, on the

internal network of the TOE through the DHCP protocol.

- Voice Communication Management

  When IP-based voice communication traffic is sent and received through a network where private IP addresses are used, the TOE provides the function recognizing this and transmitting them to the voice traffic processing system smoothly. It also supports the configuration of IP addresses and others for the voice communication service and viewing the operational status of the service.

- Firmware Management

  The TOE supports receiving a new GWIMC firmware version from the upgrade server based on the HTTP and FTP protocols; it also upgrades the GWIMC firmware currently installed in the GWIMC hardware.

- System Monitoring and Management

  The TOE allows you to boot and restart the system and the serial access function through a terminal access protocol and supports viewing the status of the IP devices on the internal network of the TOE through the SNMP.

- 2-Layer Security Protocol

  The TOE performs security communications by generating a secure channel from the external network to the internal network using the PPTP and L2TP-based security protocols.

- Interoperation with an Authentication Server

  The TOE allows interoperation with a RADIUS and TACACS authentication server.

3 TOE Security Environment

The TOE security environment consists of the assumptions that describe the security nature of the TOE environment, the threats that threat agents may pose to the TOE environment and assets, and the organizational security policies which are the security rules, procedures, practices, or guidelines that the TOE must keep. The assumptions, threats, and organizational security policies for the TOE include all the assumptions, threats, and organizational security policies of the FWPP and VPNPP. They also include some additional items to be applied to the TOE.

3.1 Assumptions

This chapter provides the assumptions that must be enforced or maintained in the TOE operating environment.

3.1.1 Assumptions From PPs

Below are the assumptions that must be applied to the TOE operating environment that claims compliance with the PPs.

Name	Description
A. Physical Security	The TOE shall be located in a physically secure environment that can be accessed only by the authorized administrator.
A. Security Maintenance	When the internal network environment changes due to change in the network configuration, host increase/decrease and service increase/decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.
A. Trusted Administrator	The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.
A. Operating System Reinforcement	Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.
A. Single Point	All communications between the external and internal networks are carried

of Connection	out only through the TOE.
A. Security Policy	The peer TOE communicating with the TOE shall be managed so that security policy is compatible. Compatible security policy implies that important security policies are the same and the differences are very limited.

3.1.2 Additional Assumptions

Below are the assumptions added to the ST.

Name	Description
A.SECURE_SERVER	The servers located outside of the TOE including the NTP server used to maintain a reliable system time in the TOE, the mail server used to send e-mail alert and the remote VPN gateway are secure.
A.SECURE_CHANNEL	For the communication data between the TOE and an authorized administrator, a secure communication channel is established using the SSL, and the certificates used in the SSL are managed securely.
A.SECURE_STORAGE	The hardware and underlying OS where the SysLogStore is installed and are used as the administrator PC have no programs installed in themselves other than the OS, and the functions that support the administrator PC and SysLogStore directly or indirectly. Therefore they are secure.

3.2 Threats

This chapter provides the threats to the TOE and the threats to the TOE operating environment. The major assets that the TOE is intended to protect are the computer resources and network services in the internal network operated by an organization.

The threat agent is generally IT entities and human users who exert damage to the TOE and internal assets in abnormal methods or attempt illegal access to the TOE and internal assets from outside. The threat agent also includes a user or IT entity that attempts to compromise the confidentiality and integrity of the assets being transmitted.
The threat agent has low level of expertise, resources and motivation.

Name	Description
T. Impersonation	The threat agent can access the TOE by masquerading as authorized user and the peer TOE.
T. Flaw Implementation	The developer can make the TOE vulnerable including codes with security-related flaws or not executed according to specifications.
T. Recording Failure	The threat agent can disable recording of security-related events of the TOE by exhausting storage capacity.
T. Illegal Information Inflow	The threat agent can violate the internal network with inflow of not allowed information from outside.
T. Illegal Information Outflow	The internal user can have illegal information exposed to the outside through the network.
T. New Attack	The threat agent can attack the TOE with newly known vulnerability of the TOE or the TOE operation environment.
T. Continuous Authentication Attempt	The threat agent can access the TOE by continuously attempting authentication.
T. Bypassing	The threat agent can access the TOE by bypassing the TOE security functions.
T. Replay Attack	The threat agent can access the TOE by replaying the authentication data of an authorized user.
T. Stored Data Damage	The threat agent can expose, modify and delete TSF data stored in the TOE in an unauthorized method.
T. Address Spoofing	The threat agent of the external network may try to access the

	internal network by spoofing the source IP addresses as the internal IP address.
T. Abuse	An authorized user of the TOE can damage the TOE security function deliberately or for other reasons.
T. Decrypt	The threat agent can access the unauthorized transferred data by using cryptanalysis attack.
T. Transmission Integrity	The threat agent can illegally modify data transferred by the TOE in the network.
TE. Poor Management	The TOE can be configured, managed and used in a non-secure manner by the authorized administrator.
TE. Delivery and Installation	The delivery and installation officer can damage security of the TOE in the process of the TOE delivery and installation.

3.3 Organizational Security Policies

An organization that operates the TOE implemented in accordance with this ST has its own security policies. Below are the organizational security policies that must be applied to the TOE operating environment that claims compliance with the FWPP and VPNPP.

Name	Description
P. Audit	To trace responsibilities on all security-related acts, security-related events shall be recorded and maintained and reviewed.
P. Secure Management	The authorized administrator shall manage the TOE in a secure manner.
P. Confidentiality	The network traffic transferred to/from the peer TOE communicating with the TOE is encrypted/decrypted by the TOE if specified in the TOE security policy.
P. Cryptographic	The cryptographic algorithm and module used in the TOE shall be approved by the National Intelligence Service.
P. Plain Text Transmission	All network traffic not transmitted to/from the peer TOE communicating with the TOE are allowed to be transmitted without encryption/decryption according to the TOE security policy.

4 Security Objectives

The security objectives are classified into the security objectives for the TOE and the security objectives for the environment. The security objectives for the TOE are the security objectives directly handled by the TOE. The security objectives for the environment are the security objectives handled by an IT area or non-technical/procedural means.

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE. Below is a list of the security objectives for which the TOE claims compliance with the FWPP and VPNPP.

Name	Description
O. Audit	The TOE shall record and maintain security-related events in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.
O. Flaw Implementation Inspection	It shall be inspected whether code created by developers has flaws and whether code with flaw is affecting internal components of the TOE.
O. Management	The TOE shall provide means for the authorized administrator of the TOE to efficiently manage the TOE in a secure manner.
O. Data Protection	The TOE shall protect TSF data stored in the TOE and data transmitted by the TOE in the network from unauthorized exposure, modify and deletion.
O. Identification and Authentication	The TOE shall uniquely identify user and authenticate identity of user before allowing the TOE access. Also, the TOE shall mutually authenticate before tunneling with the peer TOE.
O. Self-protection	The TOE shall protect itself from tempering, de-activation and bypassing attempt, etc. of the TOE security function from the first start-up.
O. Access Control	The TOE shall control access to the TOE according to the security policy rules.
O. Information Flow Control	The TOE shall control outflow and inflow of unauthorized information from inside to outside or from outside to inside.
O. Information Flow Mediation	The TOE shall mediate information flow between the TOE and the peer TOE according to security policy.
O. Confidentiality	The TOE shall ensure confidentiality of data transmitted by the TOE in th network.

O. Key Security	The TOE shall ensure confidentiality and integrity of cryptographic key-related data and secure key exchange.

4.2 Security Objectives for the Environment

The following security objectives for the environment are the security objectives to be handled by an IT domain or by non-technical/procedural methods. Below is a list of the security objectives under which the TOE claims comply with the FWPP and VPNPP.

Name	Description
OE. Physical Security	The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.
OE. Security Maintenance	When the internal network environment changes due to change in the network configuration, host increase/decrease and service increase/decrease, etc., the changed environment and security policy shall immediately be reflected in the Toe operation policy so that security level can be maintained to be the same as before.
OE. Security Policy	The peer TOE communicating with the TOE shall be managed so that security policy is compatible. Compatible security policy implies that important security policies are the same and the differences are very limited.
OE. Trusted Administrator	The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.
OE. Secure Management	The TOE shall be delivered and installed in a secure manner and be configured, managed and used in secure manner by the authorized administrator.
OE.Operation System Reinforcement	Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.
OE. Single Point of Connection	All communications between the external and internal networks are carried out only through the TOE.

4.2.1 Additional Security Objectives for the Environment

The security objectives for the environment added to this ST are listed below.

Name	Description
OE.SECURE_SERVER	The servers located outside of the TOE including the NTP server used to maintain a reliable system time in the TOE, the mail server used to send e-mail alert and the remote VPN gateway must be managed securely.
OE.SECURE_CHANNEL	For communications between the TOE and an authorized administrator, a secure channel and certificate management function must be provided. The channel and the certificate management method must be provided using the SSL protocol.
OE.TRUSTED_STORAGE	The hardware and underlying OS where the SysLogStore is installed and are used as the administrator PC must have no programs installed in themselves other than the OS, and the functions that support the administrator PC and SysLogStore directly or indirectly. And it has to be secure.
OE. TRUSTED_NTP_SERVER	An NTP server located outside the TOE must provide the TOE with trusted and reliable time information.

5 IT Security Requirements

This chapter describes the functions that must be met by the TOE, IT environment requirements and the assurance requirements. The functional requirements and assurance requirements in this ST include those described in the FWPP and VPNPP with some additional items added to them.

5.1 TOE Security Functional Requirements

The TOE Security Functional Requirements (SFRs) in this ST consist of the functional components of CC Part 2 claiming conformance on the FWPP and VPNPP. The table below shows a summary of the functional components.

This ST aims at an SOF-medium.

Because FIA_UAU.1 which is one of the SFRs of the FWPP is hierarchical to FIA_UAU.2 of the VPNPP, FIA_UAU.1 is replaced by FIA_UAU.2.

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support (FCS)	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)	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	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)	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_AMT.1	Abstract machine testing
	FPT_RPL.1	Replay detection
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing

TOE Access (FTA)	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated session termination
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel

5.1.1 Security Audit (FAU)

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 [{sending warning mails to the authorized administrator } list of actions] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) [Refer to “Auditable Events of [Table 5-1], { None } auditable events].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [Refer to “Additional audit record content” of [Table 5-1], { None } other audit relevant information].

Functional	Auditable Events	Additional audit

Component		record content
FAU_ARP.1	Actions taken due to imminent security violations.	Recipient identity of actions
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool.	-
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	-
FCS_CKM.1	Success and failure of the activity	-
FCS_CKM.2	Success and failure of the activity	Presumed identity of destination
FCS_CKM.4	Success and failure of the activity.	-
FCS_COP.1	Success and failure, and type of cryptographic operation	-
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.	Identification information of Object
FDP_IFF.1	Decisions to permit requested information flows.	Identification information of Object
FIA_AFL.1	The reaching the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	-
FIA_SOS.1	Rejection by the TSF of any tested secret	-
FIA_UAU.2	All use of the authentication mechanism	-
FIA_UAU.4	Attempts to reuse authentication data	-
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	-
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.	-
FMT_MSA.1	All modifications of the values of security attributes.	Modified values of the security attributes
FMT_MSA.2	All offered and rejected values for a security attribute	-

FMT_MTD.1	All modifications to the values of TSF data.	Modified values of TSF data
FMT_MTD.2	All modifications to the limits on TSF data.	Modified limit of TSF data
FMT_MTD.3	All rejected values of TSF data	-
FMT_SMF.1	Use of the management functions	-
FMT_SMR.1	Modifications to the group of users that are part of a role	-
FPT_STM.1	Changes to the time.	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests.	In case of violation of integrity, Modified TSF data of executable code
FTA_SSL.1	Locking an interactive session by the session locking mechanism, Successful unlocking of an interactive session.	-
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	
FTP_ITC.1	Failure of the trusted channel functions, Identification of the initiator and target of failed trusted channel functions.	-

[Table 5-1] Auditable events

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules when monitoring the audited events and based on these rules indicate a potential violation of the TSP.

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

a) Accumulation or combination of [Authentication unsuccessful audit events in auditable events of FIA_UAU.2, Violation of control rule audit events in auditable events of FDP_ACF.1 and FDP_IFF, Violation of integrity audit events in auditable events of

FPT_TST.1, failure of cryptographic operation audit events in auditable events of FCS_COP.1] known to indicate a potential security violation;

b) [{ None } any other rules].

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 [the authorized administrator] with the capability to read [all audit data] from the audit records.

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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches, sorting* of audit data based on [the following criteria with logical relations]:

a) Searches – System log, VPN log, Traffic log, audit log index., event type, a range of date and time, subject (prefix, for the traffic log), search word, and the AND logical relationship among these items

b) Sorting – Ascending or descending sort by date and time

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 include or exclude auditable events from the set of audited events based on the following attributes:

a) *event type*

b) [Whether audit log settings are configured in accordance with the packet filtering security policy and the administrator security policy]

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 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.

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 [notify to the authorized administrator, { None } actions to be taken in case of possible audit storage failure] if the audit trail exceeds [the ratio of free space to the total storage space for the audit log (from 10% to 5%, the range of values that can be set by an authorized administrator)]**.**

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *"prevent auditable events, except those taken by the authorized user with special rights"* and [{ sending mails to the authorized administrator, stop of all TSFs except the functions needed to recover the storage space } other actions to be taken in case of audit storage failure] if the audit trail is full.

5.1.2 Cryptographic Support (FCS)

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
FMT_MSA.2 Secure security attributes

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [block cipher algorithm Korean Standards] and specified cryptographic key sizes [128 bits or more] that meet the following: [list of block cipher algorithm Korean Standards].

FCS_CKM.2 Cryptographic key distribution

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 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [IKE] that meets the following: [IETF RFC2409].

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]
FMT_MSA.2 Secure security attributes

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [the cryptographic key storage area assigned in the TOE main memory is initialized to '0' and is freed] 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 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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1 TSF must execute [the method defined in “The ESP CBC-mode Cryptographic Algorithms” (RFC2451) and the method, such as using of HMAC-SHA-1-96 holding the key with the length of 160-bit in IPsec AH and ESP (RFC2404)] according to the specified cryptographic algorithm [Standard block cryptographic algorithm for government agencies, Hash function algorithm standard(HAS-160)] and the specified cryptographic key length [128 bits or more, 160 bits] that conform to [list of block cipher algorithm Korean Standards, organizational standard of TTAS.KO-12.0011/R1 “Hash FUNCTION STANDARD – PART 2 : Hash FUNCTION ALGORITHM STANDARD(HAS-160)”].

5.1.3 User Data Protection (FDP)

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.2.1 The TSF shall enforce the [administrator security policy specified in FDP_ACF.1] on [the following list of subjects and objects] and all operations among subjects and objects covered by the SFP.

a) Subject: Administrators authenticated by the authentication mechanism described in FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, and FIA_UAU.4, external IT entities that are allowed to gain remote access to the TOE, external IT entities that send ICMP packets.

b) Object: GWIMC web management interface, GWIMC system console interface, SysLogStore management interface, the TOE network interfaces

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [administrator security policy] to objects based on the following: [subject and object lists that are controlled under the following SFP, security

attributes or named security attribute groups suitable for the SFP for each subject and object].

a) Subject: Subjects described in FDP_ACC.2.1

b) Object: Objects described in FDP_ACC.2.1

c) Security attributes of subjects: Administrator ID, normal password, one-time password, authentication failure count, IP address

d) Security attributes of objects: Management interface type, system operating mode, network interface identifier, connection time, port number

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

a) Access to the GWIMC web management interface is allowed if an administrator's IT entity attempts to access it using a web browser via a secure SSL-based channel and is successfully authenticated by the authentication mechanism described in FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4.

b) Access to the GWIMC web management interface and SysLogStore management interface is denied if an administrator attempts to access them when the TOE is in the emergency mode because the audit log storage space is full as described in FAU_STG.4 or because of the initial configuration or reconfiguration.

c) Access to the SysLogStore management interface is allowed if an administrator attempts to access it through authentication by the SysLogStore when the TOE is in normal mode.

d) Access to the TOE is allowed if an external IT entity with a IP address for which remote access is allowed attempts to access the TOE based on a protocol, port number, and access time (day of the week/hour/minute) for which access is allowed.

e) An ICMP packet reply is allowed if an external IT entity sends an ICMP packet to TOE network interfaces for which an ICMP packet reply is allowed.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [When an authorized administrator accesses the GWIMC directly through the GWIMC system console interface in the internal network; when IKE communications are performed between the TOE and a remote VPN gateway or between TOEs].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the

[following rules, based on security attributes, that explicitly deny access of subjects to objects].

a) If an unauthorized user attempts to access the GWIMC web management interface through an internal/external network IT entity.

b) If an administrator attempts to access the GWIMC web management interface or SysLogStore management interface when the TOE is in initial or emergency mode.

c) If an external IT entity attempts to access the TOE with no IP address is registered in the remote access-allowed list.

d) If an external IT entity sends an ICMP packet to the TOE when there is no network interface to which ICMP packet reply is allowed.

FDP_IFC.1 Subset information flow control (VPNPP)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(1) Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [VPN Security Policy] on [the following list of subjects, information, and operations].

a) Subject list: External IT entities that send and receive information through the TOE.
b) Information list: Data transmitted through the TOE
c) Operation list
- Encryption and hash of information transmitted to the peer TOE
- Decryption, integrity check of the information, transmission to the subject
- Pass information

Application Note: The TOE can make secure or non-secure communication according to the TOE security policy.

FDP_IFF.1(1) Simple security attributes (VPNPP)

Hierarchical to: No other components.

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

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

a) Subject security attributes: IP address of external IT entities that send and receive information through the TOE, {an identifier of the subject} subject security attributes

b) Information security attributes: Source and destination IP addresses for information data packet transmission, { an identifier of the subject, IPSec pass-through interface, encryption and integrity assurance protocol, key exchange mode, mutual authentication method and security attribute based on it, encryption and hash algorithm, key life time, security method, connection management attribute } information security attributes

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Following rules].

a) Communication with the peer TOE: For inbound/outbound traffic from/to the peer TOE, the TOE shall do the following according to security policy.

- Establish secure channel or use existing secure channel in communicating with the peer TOE
- Not invoke security mechanism and not establish secure channel in communicating with the peer TOE

b) Communication with Not the Peer Toe: For not inbound/outbound traffic from/to the peer TOE, the TOE does not invoke security mechanism and establish secure channel.

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall provide the following [None].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [None].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [None].

Application Note: The TOE can make secure or non-secure communications according to the TOE security policy.

FDP_IFC.2(1) Complete information flow control (FWPP)

Hierarchical to: FDP_IFC.1

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [packet filtering security policy] on [the following list of subject and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

a) Subject : Any external IT entity sending and receiving information through the TOE.

b) Information : Any information transmitted through the TOE.

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

FDP_IFC.2(2) Complete information flow control (FWPP)

Hierarchical to: FDP_IFC.1

Dependencies: FDP_IFF.1 Simple security attributes

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

a) Subject: Any external IT entity sending and receiving information through the TOE after its IP address is translated.

b) Information: Any information transmitted through the TOE.

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

FDP_IFF.1(2) Simple security attributes (FWPP)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

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

a) Subject: Subjects described in FDP_IFC.2(1).

b) Information: Information described in FDP_IFC.2(1).

c) Subject security attributes: IP address of an external IT entity sending and receiving information through the TOE, security label.
d) Information security attributes: Protocol type (UDP, TCP, ICMP), port number, access time (day of the week/hour/minute), IP address of the external IT entity sending and receiving information, security label, URL.

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: [If the information flow conforms to the conditions allowed by the packet filtering security policy set in accordance with the security attributes described in FDP_IFF.1.1].

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall provide the following [None].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [None].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [If the IP addresses of two IT entities sending and receiving information to and from each other through the TOE are identical].

FDP_IFF.1(3) Simple security attributes (FWPP)
Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

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

a) Subject: Subjects described in FDP_IFC.2(2).
b) Information : Information described in FDP_IFC.2(2).
c) Subject security attributes: IP address of an external IT entity sending and receiving information through the TOE.

d) Information security attributes: Protocol type (UDP, TCP), translated port number of an external IT entity sending and receiving information, network interface, translated IP address of an external IT entity sending and receiving information.

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: [If the information flow conforms to the conditions allowed by the address translation policy set in accordance with the security attributes described in FDP_IFF.1.1].

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall provide the following [None].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [None].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [None].

5.1.4 Identification and Authentication (FIA)

FIA_AFL.1(1) Authentication failure handling (FWPP)
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *[five]* unsuccessful authentication attempts occur related to [Administrator authentication through the GWIMC web management interface and SysLogStore management interface].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent users from being authenticated till the authorized administrator takes proper action, { user authentication is prevented for five minutes } list of actions].

Application Note: The unsuccessful authentication attempt count for the GWIMC web

management interface and the SysLogStore management interface is accumulated respectively. That is, after five authentication failures, user authentication is prevented in each interface for five minutes.

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

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *"an administrator-configurable positive integer within [1, 2, 3]"* unsuccessful authentication attempts occur related to [VPN counterpart authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent users from being authenticated till the authorized administrator takes proper action, { None } list of actions].

FIA_ATD.1(1) User attribute definition (FWPP)

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: [the following list of security attributes].

a) Security label

b) { ID, normal password, one-time password, accumulated password authentication failure count } user security attributes

FIA_ATD.1(2) User attribute definition (VPNPP)

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: [IP address, ID, authentication mechanism and the security attributes (RSA key, X.509-based certificate, Preshared key)].

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 following defined quality metric].

a) A normal administrator password shall be 7 to 16 characters long.
b) Characters and digits that can be used in a normal administrator password − Case sensitive English letters (A to Z, a to z), digits (0 to 9)
c) For a normal administrator password, a combination of English letters and digits shall be used.
d) For a normal administrator password, the same English letter or digit shall not be used more than four times continuously.

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1
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 shall prevent reuse of authentication data related to [one-time password administrator authentication].

Application Note: This requirement is assumed to be applied only to the administrator authentication authorized by the same FWPP and VPNPP requirement.

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Authentication

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

a) Displays '*' as many times as the number of characters entered as the password.

b) Displays a reference value needed to enter a one-time password.

Application Note: Since the authentication of a counterpart connected through a VPN is performed through the unique VPN mechanism with the related pre-existing security attributes, it provides no feedback to the user while the authentication is in progress. Therefore, it is excluded from this rule.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

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

5.1.5 Security Management (FMT)

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, start, and modify the behavior of* the functions [the following list of functions] to [the authorized administrator].

a) Initialization, backup and recovery of the TOE configuration environment

b) Address translation policy management

c) Packet filtering policy management (including the IT entity mandatory access control policy setting)

d) VPN policy management (including the X.509 certificate management and RSA key creation functions)

e) Administrator authentication management

f) Audit logging configuration and management

g) System integrity check

h) System time setting

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 [administrator security policy] to restrict the ability to *change default, query, modify, delete* the security attributes [security label, access control rules, information flow control rules, { VPN counterpart } list of security attributes] to [the authorized administrator].

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

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 [administrator security policy, address translation policy, packet filtering security policy, and VPN security policy] 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 administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(1) Management of TSF data (FWPP)

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 *[statistics processing]* the [audit data] to [the authorized administrator].

FMT_MTD.1(2) Management of TSF data (FWPP)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *[backup and recover to semipermanent secondary storage]* the [major files composing the TOE] to [the authorized administrator].

FMT_MTD.1(3) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MTD.1.1 The TSF shall restrict the ability to *modify and delete* the [identification and authentication data] to [the authorized administrator].

Application Note: This component corresponds to both the FMT_MTD.1(3) of the FWPP and the FMT_MTD.1(2) of the VPNPP, jointly.

FMT_MTD.1(4) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MTD.1.1 The TSF shall restrict the ability to *modify* the [time] to [the authorized administrator].

Application Note: The TOE provides two methods for changing the system time. One is manual setting by an authorized administrator; the other is an authorized administrator configuring the NTP server environment so that time information is automatically received from an NTP server outside the TOE and is automatically applied to update the system time to the correct time. Both methods can only be configured and modified by authorized administrators.

Application Note: This component corresponds to both the FMT_MTD.1(4) of the FWPP and the FMT_MTD.1(3) of the VPNPP, jointly.

FMT_MTD.1(5) Management of TSF data (VPNPP)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *modify* the [cryptographic key attribute] to [the authorized administrator].

Application Note: This component corresponds to FMT_MTD.1(1) of the VPNPP.

FMT_MTD.1(6) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, modify, delete, clear, [generate]* the [{ TSF data used to set the VPN security policy, TSF data used to set the packet filtering security policy, TSF data used to set the address translation policy, TSF data used to configure the audit logging settings } list of other TSF data] to [the authorized administrator].

Application Note: This component corresponds to both the FMT_MTD.1(5) of the FWPP and the FMT_MTD.1(4) of the VPNPP, jointly.

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 specification of the limits for [audit storage capacity, some number of unsuccessful authentication attempts, time interval which self test occurs] to [the authorized administrator].

Application Note: The authentication failure count is fixed at five (5) times. This setting is not configurable by an authorized administrator.

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [specified in FAU_STG.3 and FIA_AFL.1, specified self-tests in FPT_TST.1].

Application Note: In case of the peer TOE authentication failure, it is possible to apply other metric rather than number of unsuccessful authentication attempt.

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model

FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF 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 security management functions: [the following list of security management functions to be provided by the TSF].

a) Initialization, backup and recovery of the TOE configuration environment

b) Address translation policy management

c) Packet filtering policy management (including the IT entity mandatory access control policy setting)

d) VPN policy management (including the X.509 certificate management and RSA key creation functions)

e) Administrator authentication management

f) Audit logging configuration and management

g) System integrity check

h) System time setting

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 [the authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with **the authorized administrator** roles.

5.1.6 Protection of the TSF (FPT)

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_AMT.1.1 The TSF shall run a series of tests *during initial start-up, periodically during normal operation, at the request of an authorized user, [at the conditions { None }]* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_RPL.1 Replay detection (VPNPP)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [mutual authentication data between VPN counterparts].

FPT_RPL.1.2 The TSF shall perform [blocking transmission data inflow between VPN communication counterparts and recording audit log].

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions should be invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in TSC.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Application Note: The TOE provides two methods for changing the system time. One is manual setting by an authorized administrator; the other is the NTP server configuration where time information is automatically received from an NTP server outside the TOE and applied to the system time correctly.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: FPT_AMT.1 Abstract machine testing

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the request of the authorized user, [at the conditions { None } conditions under which self test should occur]* to demonstrate the correct operation of *the TSF*.

FPT_TST.1.2 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of *[the following parts of TSF data]*.

a) The files and directories contained in the /bin/ directory of the TOE file system
b) The files and directories contained in the /lib/ directory of the TOE file system (except for the /lib/modules/ directory)
c) The files and directories contained in the /sbin/ directory of the TOE file system
d) The files and directories contained in the /usr/ directory of the TOE file system (except for the common.js file in the /usr/local/www/script/ and the rsakey.crt, certdown files in the /usr/local/www/ directory)

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

5.1.7 TOE Access (FTA)

FTA_SSL.1 TSF-initiated session locking
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an interactive session after [10 minutes idle time in the SysLogStore management interface] by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity on the **authorized administrator**'s data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the [administrator re-authentication] prior to unlocking the session.

Application Note: As the VPNPP Application Note says, a user is defined as an authorized

administrator, and this component is regarded complies with the FTA_SSL.1 of the VPNPP and FWPP simultaneously.

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive **authorized administrator** session after a [idle access limit time set by an authorized administrator using the GWIMC web management interface].

Application Note: As the TOE has no normal users other than authorized administrators, "user' as described in FTA_SSL.3.1 is modified and tailored to "administrator".

5.1.8 Trusted path/channels (FTP)

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 a remote 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 *the TSF* to initialize communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [remote management function, { communication between the GWIMC and SysLogStore} list of functions].

5.2 IT Environment Security Functional Requirements

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Application Note: This function, in which an authorized administrator configures an NTP server located outside the TOE, automatically gets correct time information from the NTP server and provides the TOE with a trusted time stamp.

5.3 Security Function Requirements Removed by Requirements with a Higher Hierarchical Relationship

Since this ST conforms to both the FWPP and VPNPP at the same time, and the FIA_UAU.1 contained in the FWPP is lower than FIA_UAU.2 contained in the VPNPP, only the FIA_UAU.2 is selected.

The FIA_UAU.1 hierarchical relationship and dependencies are regarded as being replaced by those of the FIA_UAU.2.

5.4 TOE Security Assurance Requirement

The security assurance requirements for this ST consist of the assurance components of the CC Part 3, which has an evaluation assurance level of EAL3+. The table below shows a summary of the assurance components and added components.

- ADV_IMP.2 Implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- ALC_TAT.1 Well-defined development tools
- ATE_DPT.2 Testing: low-level design
- AVA_VLA.2 Independent vulnerability analysis

Assurance class	Assurance component	
Configuration management	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.4.1 Configuration management (ACM)

ACM_CAP.3 Authorization controls

Dependencies: ALC_DVS.1 Identification of security measures

- Developer action elements:

  ACM_CAP.3.1D The developer shall provide a reference for the TOE.

  ACM_CAP.3.2D The developer shall use a CM system.

  ACM_CAP.3.3D The developer shall provide CM documentation.

- Content and presentation of evidence elements :

  ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE

  ACM_CAP.3.2C The TOE shall be labeled with its reference.

  ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

  ACM_CAP.3.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

  ACM_CAP.3.5C The configuration list shall describe the configuration items that comprise the TOE.

  ACM_CAP.3.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

  ACM_CAP.3.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

  ACM_CAP.3.8C The CM plan shall describe how the CM system is used.

  ACM_CAP.3.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

  ACM_CAP.3.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

  ACM_CAP.3.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.

- Evaluator action elements :

  ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.1 TOE CM coverage

Dependencies: ACM_CAP.3 Authorization controls

- Developer action elements :
  ACM_SCP.1.1D The developer shall provide a list of TOE configuration items for the TOE.

- Content and presentation of evidence elements :
  ACM_SCP.1.1C The list of configuration items shall include the following: implementation representation and the evaluation required by the assurance components in the ST.

- Evaluator action elements :
  ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 Delivery and operation (ADO)

ADO_DEL.1 Delivery procedures

Dependencies: No dependencies.

- Developer action elements :
  ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.
  ADO_DEL.1.2D The developer shall use the delivery procedures.

- Content and presentation of evidence elements :
  ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

- Evaluator action elements :
  ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation and start-up procedures

Dependencies: AGD_ADM.1 Administrator guidance

- Developer action elements :

  ADO_IGS.1.1D The developer shall document the procedures necessary for the secure installation, generation and start-up of the TOE.

- Content and presentation of evidence elements :

  ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

- Evaluator action elements :

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

  ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.3 Development (ADV)

ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

- Developer action elements :

  ADV_FSP.1.1D The developer shall provide a functional specification.

- Content and presentation of evidence elements :

  ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

  ADV_FSP.1.2C The functional specification shall be internally consistent.

  ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

  ADV_FSP.1.4C The functional specification shall completely represent the TSF.

- Evaluator action elements :

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies: ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

- Developer action elements :

  ADV_HLD.2.1D The developer shall provide the high-level TSF design of the TSF

- Content and presentation of evidence elements :

  ADV_HLD.2.1C The presentation of the high-level design shall be informal.

  ADV_HLD.2.2C The high-level design shall be internally consistent.

  ADV_HLD.2.3C The high-level design shall describe the structure of the TSF, in terms of sub-systems.

  ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

  ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

  ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

  ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

  ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

  ADV_HLD.2.9C The high-level design shall describe separation of the TOE into TSP-enforcing and other subsystems.

- Evaluator action elements :

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

  ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.2 Implementation of the TSF

Dependencies: ADV_LLD.1 Descriptive low-level design
ADV_RCR.1 Informal correspondence demonstration
ALC_TAT.1 Well-defined development tools

- Developer action elements :

  ADV_IMP.2.1D The developer shall provide implementation representation for the entire TSF.

- Content and presentation of evidence elements :

  ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

  ADV_IMP.2.2C The implementation representation shall be internally consistent.

  ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

- Evaluator action elements :

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

  ADV_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

Dependencies: ADV_HLD.2 Security enforcing high-level design
ADV_RCR.1 Informal correspondence demonstration

- Developer action elements :

  ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

- Content and presentation of evidence elements :

  ADV_LLD.1.1C The presentation of the low-level design shall be informal.

  ADV_LLD.1.2C The low-level design shall be internally consistent.

  ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

  ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

  ADV_LLD.1.5C The low-level design shall define the interrelationships between the

modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

- Evaluator action elements :

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

  ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies.

- Developer action elements :

  ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

- Content and presentation of evidence elements :

  ADV_RCR.1.1C For each adjacent pair of TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely reflected in the less abstract TSF representation.

- Evaluator action elements :

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

5.4.4 Guidance documents (AGD)

AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

- Developer action elements :

  AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administration personnel.

- Content and presentation of evidence elements :

  AGD_ADM.1.1C This administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

  AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

  AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

  AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

  AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

  AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event related to administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

  AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

  AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

- Evaluator action elements :

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

5.4.5 Life cycle support (ALC)

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

- Developer action elements :

  ALC_DVS1.1D The developer shall produce development security documentation.

- Content and presentation of evidence elements :

  ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

  ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

- Evaluator action elements :

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

  ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

- Developer action elements :

  ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

  ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

- Content and presentation of evidence elements :

  ALC_TAT.1.1C All development tools used for the implementation shall be well-defined.

  ALC_TAT.1.2C The documentation of development tools shall unambiguously define the meaning of all statements used in the implementation.

  ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

- Evaluator action elements :

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

5.4.6 Tests (ATE)

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

- Developer action elements :

  ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

- Content and presentation of evidence elements :

  ATE_COV.2.1C The analysis of the test shall demonstrate the correspondence between the tests identified in the test documentation and the TSF, as described in the functional specification.

  ATE_COV.2.2C The analysis of the test shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

- Evaluator action elements :

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

ATE_DPT.2 Testing: low-level design

Dependencies: ADV_HLD.2 Security enforcing high-level design
ADV_LLD.1 Descriptive low-level design
ATE_FUN.1 Functional testing

- Developer action elements :

  ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

- Content and presentation of evidence elements :

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level and low-level design.

- Evaluator Requirements

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

ATE_FUN.1 Functional testing

Dependencies: No dependencies.

- Developer action elements :

  ATE_FUN.1.1D The developer shall test the TSF, and document the results.

  ATE_FUN.1.2D The developer shall provide test documentation.

- Content and presentation of evidence elements :

  ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

  ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

  ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

  ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

  ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

- 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_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

- Developer action elements :

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

- Content and presentation of evidence elements :

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

  ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

- Evaluator action elements :

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

  ATE_IND.2.2E The evaluator shall test a subset of TSF as appropriate to confirm that the TOE operates as specified.

  ATE_IND.2.3E The evaluator shall execute a sample of the tests in the test documentation to verify the developer test results.

5.4.7 Vulnerability assessment (AVA)

AVA_MSU.1 Examination of guidance

Dependencies: ADO_IGS.1 Installation, generation and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

- Developer action elements :

  AVA_MSU.1.1D The developer shall provide guidance documentation.

- Content and presentation of evidence elements :

  AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operating of the TOE (including operations following failure or operational error), their consequences and the implications for maintaining secure operation.

  AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

- Evaluator action elements :

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

  AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

  AVA_MSU.1.3E The evaluator shall determine that use of the guidance documentation allows all insecure states to be detected.

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive low-level design

- Developer action elements :

  AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

- Content and presentation of evidence elements :

  AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

  AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

- Evaluator action elements :

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

  AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.2 Independent vulnerability analysis

Dependencies: ADV_FSP.1 Informal functional specification

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the Implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

- Developer action elements :

  AVA_VLA.2.1D The developer shall perform a vulnerability analysis.

  AVA_VLA.2.2D The developer shall provide vulnerability analysis documentation.

- Content and presentation of evidence elements :

  AVA_VLA.2.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

  AVA_VLA.2.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

  AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

  AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

- Evaluator action elements :

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

  AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

  AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

  AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

  AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

6 TOE Summary Specification

This chapter provides a summary of how the TOE provides its security functions and assurance measures.

6.1 TOE Security Functions

This section provides the rationale through which the TOE security function specification is actually implemented, using which functions.

The strength of a security function required for this Security Target is defined as SOF-medium. The following shows the security strength and the TOE security function on the TOE Summary Specification to which the security strength is applied.

- **IA_Password** – SOF-medium

The function above meets the SOF-medium by the combination of the restriction inspection function for general password creation provided by MT_Interface and the authentication delay invoked by the five continuous authentication failure provided by IA_Failure.

All the Identifying values of “Table 3 – Calculation of attack potential” in the “A.8 Strength of function and vulnerability analysis” section of the “Common Methodology for Information Technology Security Evaluation Version 2.3” are 0 under the combination of the restrictions for the identification and authentication above. And all the Exploiting values are unrealistic for both Elapsed Time and Access to TOE. Therefore, the value of a rating for the vulnerability given by the SOF analysis from “Table 4 – Rating of vulnerabilities” is higher than 24. As a result, the strength of the security function to which SOF is applied satisfies the SOF-medium.

6.1.1 Security Audit (AU)

6.1.1.1 Security Alarm (AU_Alarm)

The TOE inspects the audit record created, and notifies the authorized administrator by e-mail if an audit record classified as a potential security violation event is detected.

For an audit record showing a potential violation as above, a “!SecureAlert!” is inserted in it and an alert email is sent to the authorized administrator when such audit records classified as potential security violation events are detected. The formal alarm email is sent using the pre-configured mail server’s IP address and e-mail addresses of sender/receiver. The audit record content is attached to the alert mail, and the audit record for the activity of sending the alert mail is performed by AU_AuditRecord.

6.1.1.2 Audit Record Generation (AU_AuditRecord)

The TOE provides the authorized administrator with a function to create an audit record for a target event and transmit it to the SysLogStore according to the audit record configuration based on the packet filtering audit policy and Facility/Severity that is specified in IETF RFC 3164. It also provides a function to detect and classify the audit records denoting dangerous events.

The TOE only creates selectable audit records for the auditable events defined by event type as follows:

<Types of Auditable Events>

Auditable Event		Description
Event Type	Facility	The event classified by the sub-system that causes it.
	Severity	The event classified by its severity of security. The configured severity level to record includes its higher severity level (more severe) as well as its severity level
The auditable events set by the administrator security and packet filtering policies.		The event generated by the specific traffic flow that is set to be blocked and audited by the administrator security and packet filtering policies

Among these, the values set for Facility and Severity use the classification specified in IETF RFC 3164

The GWIMC creates an audit record based on the settings by the audit record policy and transmits it to the SysLogStore. All the audit record has detailed messages that consists of the date of event, identity of the subject causing the event, event type and event result. The audit record message consists of the following fields:

<Audit Record Message format>

Message Field	Description
Index	The index number to be assigned in order of audit record creation
Facility	The subsystem identifier generating the audit record (Event type)
Severity	The Identifier representing the security severity of the audit record (Event type)
Date Time	Date and time when audit record is created
Subject	Subject of the event that generated an audit record. Traffic Log (the audit set to be recorded by the ICMP and remote access control policy settings from the packet filtering and administrator security policies) displays “Prefix” instead of “Subject”.
Message	The body of an audit message in which the detailed information on the event is recorded (including the result of the event)

Regardless of the authorized administrator’s configuration, the events described in the table below are regarded as potential security violation events and “!SecureAlert!” is inserted in their audit message.

<Audit record for potential security violation events in which "!SecureAlert!” is inserted>

Auditable Event	Description
User authentication failure	■ When administrator authentication through the GWIMC web management interface or SysLogStore management interface fails ■ When VPN counterpart authentication fails
Access control policy violation	■ Access from an IT entity that does not have permission for TOE access (with its audit record settings) ■ When an ICMP pack is transmitted to the TOE network interface where ICMP packet access is not permitted (with its audit record settings) An event that occurs in an operation mode where the SysLogStore is not connected to the GWIMC is handled as an exception as below. ■ When an authorized administrator accesses the GWIMC web

	management interface or SysLogStore management interface when the TOE is in its emergency or initial mode
Information flow control policy violation	■ Information transmission between internal and external networks, complying with the denying rule among the packet filtering rules set by the authorized administrator, except for default packet filtering security policy settings. (The explicit denying policy such as information flow control by security label and a default policy are not applicable. Address translation policy is not applicable, either.) ■ When a VPN counterpart does not communicate through a legal security channel created by the VPN security policy
Cryptographic operation failure	The encrypted packet transmitted through IPSec VPN is not valid or the encryption procedure has not been carried out correctly.
TOE integrity violation audit event	When an integrity violation is detected by changing, deleting, creating executable files or configuration files of TOE

6.1.1.3 Audit Record View (AU_View)

The security function provides the functions for viewing all audit records stored via the SysLogStore management interface.

The items that relate to audit record searches/views are as follows.

- VPN Log – Searching for VPN related audit records
- Traffic Log – Searching for the audit records of the events configured in the ICMP and the remote access user access control policy setting among the packet filtering and administrator security policies
- System Log – Searching for audit records except for the VPN Log and Traffic Log
- Audit record Index – Searching by the index numbers of the audit records
- Event type – Searching by Facility (25 types can be selected, including All types)
  Searching by Severity (9 types can be selected, including All types)
- Date and time range – Searching by the ascending or descending order within a time range including year/month/day/hour/minute/second units
- Subject – Searching for audit records by their subject identifier. With the Traffic Log, the "Prefix" is displayed instead of "Subject" and the audit records are searched by the prefix configured in the packet filtering security policy settings

- Key word − Searching for an audit record in which the specified key word is inserted in the message of the audit record.
- Searching by an AND operation of the items above

6.1.1.4 Audit Data Protection (AU_Protect)

The security function provides the protection for audit record messages created by the GWIMC.

The audit records that are created and temporarily stored on the GWIMC are protected from deletion or modification, because the direct access to the file system of the GWIMC is blocked, even by an authorized administrator.

The audit records transmitted and stored on the SysLogStore can only be deleted by the SysLogStore management interface by an authorized administrator who is authenticated by the SysLogStore administrator authentication function. A direct access from an external network to the SysLogStore and access and changes to audit records are blocked.

The security function checks the ratio of the consumed audit storage size against the maximum storage size set by the SysLogStore management interface. The TOE checks the remaining free space regularly while accumulating audit records. If the remaining free storage space falls to the “Alarm Free Space” (almost consumed) set by the GWIMC web management interface, the TOE warns an authorized administrator by email that there is insufficient free space for audit records.

If the storage condition reaches the “Stop Free Space” (completely consumed) after the “Alarm Free Space” by doing nothing, the TOE warns an authorized administrator by e-mail and stops all functions which can cause the events that may generate audit records. The Activities include the disabling of network interfaces, system demons, etc.

For the restart of the audit record function, an authorized administrator has to stop SysLogStore by the service control interface of the OS operating on the administrator PC where the SysLogStore is installed. Then change the name of the “SysLogDB.mdb” file for backup. And copy the empty “Empty.mdb” file with the name “SysLogDB.mdb”.

After doing them, restart the SysLogStore by OS service control interface.

6.1.2 User Data Protection (DP)

6.1.2.1 IP Filtering (DP_Filter)

The TOE applies the packet filtering and address translation policies to the network traffic which flows between IT entities via a TOE network interfaces. These policies have the following security attributes:

- attribute of subject that transmits packets − IP address, security label
- Information security attribute of the transmission packet − protocol type (UDP, TCP, ICMP), port number, passed network interface, access time (day of week/hour/minute), IP address, URL address, range of IP address and port address to be translated by NAT.

Packet Filtering

The packet filtering security policy analyzes the information in the transmission data to pass through the TOE according to the security attributes set by the GWIMC web management interface. For permitted transmission data, the transmission is allowed while the other is blocked and discarded.

In addition to the function above, the TOE provides the complementary function based on security label based MAC (Mandatory Access Control).

This function provides the security label based access control for an IT entity that has an IP address. It blocks access from the IT entity with low security level to the IT entity with high security level, giving the security label denoted by numbers to a single IP address or subnet based on IP address and netmask.

For example, if IT entity A has the IP address 192.168.0.1 with its security level 3 and IT entity B has the IP address 192.168.0.100 with its security level 6 are connected to each other on a network through TOE, access from A to B will be allowed, while access from B to A be blocked.

However, an authorized administrator can easily add and adjust exceptional rules to mandatory access control by providing a matrix-type correspondence table that can add

exceptional rules for service efficiency and flexibility.

For IPSec VPN traffic, communication is allowed within the VPN tunneling block among the peer TOEs in accordance with the packet filtering policy, and VPN traffic is controlled through the VPN security policy based on IPSec VPN's own TSF data and security attribute values.

Network Address Translation

With the address translation policy, TOE analysis the transmission data through the TOE according to the IP address and port number, protocol type that are the target of NAT.

If the transmission data has an IP address and port number that are target of address translation, they are translated to the configured IP address and port number for NAT and transmitted to the destination

6.1.2.2 VPN Access Control (DP_VPN_Filter)

VPN Security Policy

The TOE applies the VPN security policy to the VPN traffic transmitted through the TOE network interface. The TOE establishes an IPSec protocol based VPN with trusted external VPN counterpart and provides a security communication function. The data is encrypted at the sender side and then transmitted to the receiver. And the transmitted data is decrypted at the receiver side.

The TOE provides the following algorithms and key exchange environment for the encryption and decryption, hash, and mutual communication authentication. Key lengths are shown inside the parentheses in the bits.

- Encryption algorithm - 3DES(168bit), AES(128/192/256bit), SEED(128bit)
- Hash algorithm - SHA-1(160bit)
- Key exchange algorithm - IKE, ISAKMP
- Encryption and integrity protocol - ESP, AH
- Public key algorithm - RSA (1024 bit)

The general packets going through the same network interface with VPN packets are controlled by the packet filtering policy instead of the VPN security policy if their destination

is not the VPN counterpart. Therefore, the secure communication and non-secure communication can be performed simultaneously.

In the VPN security policy, access control is performed based on the following security attributes:

- Identifier of a VPN communication subject
- IP address
- Ethernet interface through which IPSec packets pass
- Encryption and integrity assurance protocols: AH, ESP
- Key exchange mode
- Mutual authentication type and related security attributes: Public key, X.509 certificate, RSA public key
- Encryption and Hash algorithm
- Key life time
- Security type: PFS group
- Connection management attributes: Detailed settings on a connection management

The TOE performs the access control based on security attributes above and carries out identification and authentication for the VPN counterpart simultaneously.

Authentication and Failure management of VPN Counterparts

The negotiation count, one of the connection management attributes, is the limitation value of authentication trial count for the VPN counterpart, and an authorized administrator can set it with 1,2 or 3. If the authentication failure reaches the value, the authentication is stopped unless the authorized administrator performs an action such as changing the related VPN settings.

VPN Replay Attack Detection and Measures

The TOE prevents reuse of unauthorized packets by ESP and AH protocols that are used for encryption processing and integrity assurance. The TOE checks the sequence number of the ESP or AH packet headers. If the sequence number has an invalid value under the protocol rules, the TOE regards it as an unauthorized replay attack and stops the related VPN sessions.

6.1.2.3 TOE Access Control (DP_Admin_Mode)

TOE applies the administrator security policy to itself by controlling the access to the TOE using the following methods.

TOE access control based on administrator operating mode

The TOE operating modes are divided into initial, normal and emergency modes for GWIMC and SysLogStore respectively. The TOE operating modes are described in 2.1. TOE Product Type.

An authorized administrator can access TOE by the GWIMC web management interface, the GWIMC system console interface and the SysLogStore management interface in its normal mode. The TOE allows the administrator to access the TOE after the administrator authentication is successful with the registered ID and correct password of the ID using its log-in interface. If the authentication fails, the access to the TOE is denied and related audit recording is performed. And then, the authentication failure count value maintained by the TOE is increased by one.

In emergency mode, access by the GWIMC web management interface and SysLogStore management interface are blocked, because the all the SSL access sessions are disabled. A direct access through the GWIMC system console interface is allowed.

Direct access to the system and TOE management interface by the unauthorized/unauthenticated user are blocked. Therefore, the security functions' own execution area is protected.

The initial mode is the operating mode required for the TOE initial installation. As for the GWIMC, it performs the default configuration for GWIMC and SysLogStore with which the console cable is connected directly to the GWIMC hardware and terminal program is used for the initial configuration. The initial mode is invoked during GWIMC's booting. In the initial mode, an access through the GWIMC web management interface or SysLogStore management interface is unavailable.

The initial mode for SysLogStore executes the initial configuration wizard similar to MS windows' installation wizard. Since the initial TOE installation has to be started with SysLogStore installation first and the GWIMC installation next, the access through the

GWIMC web management and system console interfaces is blocked in the initial mode.

Remote access control

The TOE checks and allows the access of any external IT entity only if its IP address, protocol type, access time and port number are registered as “allowed remote access” by the Remote Access configuration provided by the GWIMC web management interface.

Remote access control is performed through the following security attributes:

- IP address of external IT entity
- Protocol (TCP, UDP)
- Port number
- Access time (day of week/hour/minute)

ICMP Packet Access Control (Ping Packet Control)

When an external IT entity sends an ICMP packet to the TOE network interface through ping, the TOE allows the access of the ICMP packet and sending reply ICMP packet to the IT entity the network interface is configured to receive and reply it ing and answering ICMP packets are allowed in the setting of the ICMP Filtering menu of the GWIMC web management interface, the TOE allows access and permits the answering ICMP packet to be sent to the external IT entity.

Access control for ICMP packets is performed through the following security attributes:

- TOE network interface to allow the ICMP packet access (Ethernet0, Ethernet1, Ethernet2)

6.1.3 Cryptographic Support (CS)

6.1.3.1 Key Deletion Management (CS_KeyDeletion)

if the key life time is expired during VPN communication using the created cryptographic key, the key is deleted completely by initializing the portion of the TOE's memory assigned to store the cryptographic key to '0' and freeing it. The IPSec VPN session established using the cryptographic key becomes no longer valid.

6.1.3.2 Key Exchange Management (CS_KeyMgmt)

The TOE performs an IKE-based key exchange, using ISAKMP. In IKE, the key exchange is performed by the following two steps:

- Phase 1: SA establishment for communication initialization
- Phase 2: Establishes an IPSec SA using SA from Phase 1 and creates a cryptographic key for IPSec communication

The TOE transmits VPN packets after determining the protocol to use by negotiating with VPN counterpart using SA that is the security policy for their VPN communication. Other than a normal packet, a VPN packet is encrypted by the encryption algorithm determined by the SA negotiated by the TOE and its VPN counterparts. After the encryption, VPN packet is transmitted among them.

The TOE generates and uses the cryptographic key in symmetric and asymmetric types.

The symmetric key creates a secret key using the pre-shared key set by an authorized administrator and the selected encryption algorithm like 3DES, AES, SEED.

For the asymmetric key creation, A 1024-bit RSA key is used. The TOE provides the RSA key creation function. The TOE also provides the X.509 certificate creation function. It can create the TOE's own certificate and import the certificate created by the VPN counterpart and register it as an external certificate. All the certificates created by the TOE are based on X.509 standard.

When a VPN packet passes through the TOE, SA is applied to the packet. If there is no SA on the initial VPN packet, key exchange is performed for SA negotiation among the VPN

counterparts. The TOE exchanges the key regularly with its counterpart by IKE, and updates a new key. With the IKE, TOE creates its secret keys and SA parameters used for the VPN communication.

6.1.3.3 Encryption/Integrity Operation (CS_ESP_AH)

The TOE uses the ESP and AH protocols to ensure the integrity and confidentiality of a VPN packet containing user data.

The TOE supports the encryption operations through the following algorithms supporting 128-bit or longer key length for ESP protocol:

- 3DES: The encryption algorithm that applies DES operation 3 times to the plain text. It supports 168-bit keys and reinforces DES security in simple manner.
- AES: The new encryption algorithm that uses 128/192/256 bit keys.
- SEED: This encryption algorithm designed for Korean government agencies. It has a 128-bit block size.

The TOE assures the integrity of user data by the AH protocol. AH protocol uses the following hash functions for the user data integrity.

- HMAC-SHA-1-96: Hash function supporting 160-bit key

The TOE doesn't allow ESP only or AH only configuration for encryption and integrity operations. Only the combination of ESP and AH is allowed.

6.1.4 Identification & Authentication (IA)

6.1.4.1 Administrator Authentication (IA_Password)

The administrator authentication function (log-in) for gaining the access to the TOE is provided by the following interfaces.

- GWIMC Web Management Interface – Provides general password and one-time password (OTP) authentication
- SysLogStore Management Interface – Provides general password authentication only

Administrator authentication is performed by the administrator ID and password that are pre-configured and stored in TOE. The Web Management Interface and the SysLogStore management interface use the same general password.

When administrators try to access the TOE management interface, the TOE displays the login windows on the PC screen and waits for the administrator ID and password inputs. If the correct administrator ID and password are entered, the authentication would be successful and the authenticated administrator is allowed to access the TOE management interface pages.

The administrator authentication fails whether the tried password is correct or not if a user tries with wrong administrator ID and then fails the user identification process.

If the correct ID is entered and identified, password authentication would be conducted. The password letter typed by the administrator are display as the letter “*” during the authentication process. It lets the user know that each letter or number is being entered, and prevents the exposure of the password. As for the one-time password authentication, the iteration value, which is used for searching correct one-time password from OTP list is displayed on the login window.

If the authentication fails, the access to any the security functions of the TOE is blocked except the login window.

6.1.4.2 One-Time Password (IA_SKEY)

TOE provides the generation function of one-time password based on IETF RFC 1760. A one-time password list is created based on the related configuration parameters provided by the GWIMC web management interface.

The following parameters are used for creating one-time password based on RFC 1760.

- Seed: a value used for creating various one-time passwords by being concatenated with secret keys
- Secret key: keys that are confidential and owned by the OTP users
- Iteration: The frequency of the hash function application to the value created by the combination of seed and secret key to generate one-time passwords.

The S/Key-based one-time password generation using the above value is performed as follows:

- Creation Process

  (1) Concatenate seed with secret key.

  (2) Create a password list by repeatedly applying the hash function (Iteration+1) times to the value created from (1). For example, if the iteration value is 99, a list containing 99 one-time passwords is created. They are ranging from the first one hashed once to the last one hashed 99 times

  (3) The 99th OTP that is hashed 99 times is stored in the TOE, and the list containing the 99 OTPs including the 99th one is created as a file.

The contents of the password list file consist of the created passwords like the following:

```
1: MOST LUCY HYMN BEAT YOU SAN
2: ALAN VIEW KNEW VAST RATE CHOW
3: KNEW RUSK KIND AJAR LORE HEAR
4: DAD GALA WAS NOT REP MELT
5: SKID SAIL LIFE REED YARD WARM
6: CUTS LORE HEAR TOP ARMY DENY
7: WARN WAGE LIME DADE CARE HOC
8: ONE CREW CARD DOME GALA WAR
9: WHOA TOG CAL HOVE SHOE SANK
10: ARK GENE BEAK BAM DADE DIET
11: KONG LORE HEAT RAIN JAVA AX
```

(omitted)

```
93: DOVE WELT RIME FACE WAGE LIND
94: GOAL ICY TELL CHAD KURT WET
95: SLUG SUB TWIN CARL AMMO CAKE
96: HURD BABE FLEW AMOK USE HER
97: RATE OBEY RAM ROSE LUCY HYDE
98: JOBS FINE ATE FLEW FIR JEFF
99: NOUN MEN TOM VICE RAM LOGE
```

This one-time password list should be maintained only by an authorized administrator and protected from being exposed to unauthorized users. Each time an administrator logs in, the iteration value is automatically decreased by 1 and the valid one-time password is changed. The administrator should find the valid password from the list by searching the correspondent iteration value displayed on the login windows. From the above screenshot, the numbers on the left indicate the iteration values.

6.1.4.3 Administrator Authentication Failures Management (IA_Failure)

This function is applied to the following management interfaces:

- GWIMC web management interface
- SysLogStore management interface

The administrator's authentication failure management through the GWIMC web management interface and SysLogStore management interface depends on the frequency of authentication failures. The frequency of consecutive failures is recorded respectively for each management interface. If the failure frequency reaches 5, the authentication function is suspended for 5 minutes, disabling the administrator's login. The authentication function is reactivated after the 5-minute suspension has elapsed.

6.1.5 Security Management (MT)

6.1.5.1 Security Management Interface (MT_Interface)

The TOE provides the function management authority for storing, modifying, creating, deleting, querying configuration values and setting related functions to operate the TOE security functions via the security management interface.

The TOE is designed so that accessing and operating the security functions is allowed only through administrator security management interfaces and that administrator authentication must be conducted to access security management interfaces. Therefore, users other than authorized administrators cannot obtain the authority to access or manage the security functions.

TOE administrator's security management interfaces are provided by the following three types:

- GWIMC web management interface: Accessing by a web browser installed on the administrator PC using SSL session to guarantee the confidentiality of the management traffic.

- The SysLogStore management interface is provided by the SysLogStore installed on the administrator PC. The interface doesn't provide the direct access to the GWIMC.

- The GWIMC system console interface is a management interface that allows direct access to the GWIMC by connecting a serial console cable to the GWIMC directly in the area where the GWIMC hardware is physically located.

The following provides details on the security management functions controlled by authorized administrators in each management interface:

Security Management Function	Sub-function	Specific Functions Embodied by Management Interfaces
Firewall	NAT configuration	- NAT enable/disable - Private IP address configuration

		- Port forwarding configuration - Static NAT configuration
	Packet filter policy configuration	- Packet filter enable/disable - Packet filter rule configuration - Remote access rule configuration - Blocked IP address rule configuration - URL filter rule configuration - ICMP packet filter rule configuration
	Security label based access control	-Security label based mandatory access control enable/disable -Mandatory access control rule configuration
VPN	IPSec VPN policy configuration	- IPSec VPN user configuration - X.509 certificate backup/import/configuration - IPsec VPN enable/disable - RSA public key creation/download - IPSec status monitoring
System Management	System configuration file management	TOE system configuration file backup / restoration / initialization
	Admin authentication configuration	- General password configuration - One-time password configuration - Administrator session termination time configuration
	Audit record policy configuration	- SysLogStore IP address configuration - Warning e-mail server configuration - Audit record storage management - Audit event type configuration
	System time management	- NTP server configuration (getting trusted time information from the NTP server registered in the TOE) - Manual time configuration (setting system time by an administrator) - Local time zone configuration
	System integrity check	- File integrity check policy configuration and report - H/W test policy configuration and report

<Functions of GWIMC web management interface>

Security Management Function	Specific Functions Embodied by Management Interfaces
Audit record management	- SysLogStore audit record storage Initialization - SysLogStore audit record backup - Audit record file viewer - SysLogStore audit record storage configuration - SysLogStore management interface disabling
Audit record statistics report	Creates the report file extracted from accumulated audit records. The file contains the following and can be downloaded to the administrator PC: - Frequency of the 10 Subject items that have the highest frequency in the cumulative audit record - Frequency of the 10 Severity items that have the highest frequency in the cumulative “System Log” audit record - Frequency of the 10 Facility items that have the highest frequency in the cumulative “System Log” audit record - Frequency of audit record occurrence of 10 times where the highest number of audit records occurred within one time unit in the cumulative “System Log” audit record messages - Frequency of 10 prefix items that are recorded most often in the cumulative “Traffic Log” audit record messages.

<Functions of SysLogStore management interface>

Security Management Function	Specific Functions Embodied by Management Interfaces
Configuration in the initial and emergency operation mode	- GWIMC audit record policy configuration and query - SysLogStore connectivity test

<Functions of GWIMC system console interface>

The TOE provides the function checking validity and limitation of input values like TSF data, security attributes set via the management interfaces. If invalid values are entered, they are prevented from being stored and applied to the TOE.

And the TOE also provides an authorized administrator with the authority of configuring the functions with valid values by the interface composed of restrictive default values and

selectable options. Therefore, the TOE guarantees the validity of the management functions and only safe TSF data is applied to the TOE.

The requirements for such values are categorized by the following types:

- Simple set value entered by keyboard
  IP address – 0 or positive integer ranging from 0 to 255 for each of 4 input fields
  Port address – 0 or positive integer ranging from 1 to 65535
  Netmask – Same as IP address above if the input field is 4 input field type.
  0 or positive integer ranging from 1 to 32 if the input field is single input field type.
  E-mail – Character string with special character "@" in its middle, or combined character/number string starts with a character

  The paths of file upload/download and audit record storage are some of the same types

- Set values by using a mouse
  Usually, it has a form of check box or selection list. Selected by a mouse click on the selectable value or range. The time interval of the system integrity check, protocol (UDP, TCP) are included in the type.

- Single set values that are pre-defined by the TOE. They are fixed and cannot be modified.
  Such as the maximum number of authentication failure in the GWIMC web management interface (5 times), the elapsed idle time with which an active administrator session of SysLogStore is converted to locked session (10 minutes), the administrator's ID (admin) and so on.

- Others
  No duplicated IP address is allowed for some functions.

Other than simple set values, there is a more restrictive and complex condition to create an administrator password and the TOE provides corresponding inspection and generation functions.

The general password for the administrator authentication can be created and stored

through the administrator interface only if the password satisfies the following restrictive conditions, in order to meet the condition of AVA_SOF.1.

- The general password should be 7~16 characters in length
- Allowed characters and numbers for the general password creation - case sensitive letters (A~Z, a~z), numbers (0~9)
- The general password must combine letters and numbers.
- The general password should not contain four or more of the same letters/numbers in a row.

The setup value “seed” used for one-time password is automatically and randomly created. The iteration value is set to 99 when new one time password is created. Only the secret key can be entered manually by the authorized administrator. The detailed information on the values used for the one time password is described in IA_SKEY.

6.1.6 TSF Protection (PT)

6.1.6.1 Hardware Test (PT_Sys_Diag)

The TOE conducts a test to check whether each GWIMC hardware element is normally operable upon initial start, configured regular test time, or upon the request of the administrator. The following tests are performed for checking the normality of GWIMC:

- Flash Memory Test

  This test checks the flash memory operation by comparing the data which is randomly written on the unused portion of flash memory and the data which is read from the potion.

- SDRAM Test

  This test checks the SDRAM operation by comparing the data which is randomly written on the unused portion of SDRAM and the data which is read from the potion.

- EEPROM Test

  This test checks the EEPROM operation by trying to write to EEPROM and checking nothing is written to EEPROM.

- Real Time Clock Test

  This test checks whether the system clock keeps working properly when the GWIMC hardware is turned off. It checks whether the time just before turning off and the time just after turning on are different.

- VPN Accelerator Test

  This test checks the VPN accelerator chip is working properly on the H/W based encryption processing using the test data.

- Network Interface Test

  This test checks the operation and accessibility of the network Interfaces

The tests above can be performed based on the following conditions.

- In the middle of the system booting.

- Just after the administrator request
- Daily
- Weekly
- Monthly

By the conditions above, the TOE performs self-diagnostics upon the initial operation, configured regular test time and the request of an administrator. The test result is displayed on the GWIMC web management interface.

6.1.6.2 File Integrity Test (PT_File_Integrity)

The TOE creates and stores hash values for its important files, such as the executives, configuration files and so on. The TOE performs the integrity test by creating the new hash values for the same files and comparing the hash values created before. The hash function used for it is SHA-2. This function inspects the following files and paths of the TOE file systems.

- Files and subdirectories in the following system directories of GWIMC

/bin/
/lib/ (/lib/modules/ is excluded)
/sbin/
/usr/ (common.js of /usr/local/www/script/ and rsakey.crt, certdown of /usr/local/www/ are excluded)

- The following execution file located on the paths of the SysLogStore installation folder (Default path)

\[Hard disk drive identifier]\Program Files\OS7400\SysLogStore\SysLogStore.exe
\[Hard disk drive identifier]\Program Files\OS7400\SysLogStoreSvc\SysLogStore.Svc.exe

The test result contains file name, modification status, modified time, and modified file size. The modified time information is maintained reliable by NTP protocol or the manual time set up by an authorized administrator.

The tests above can be performed based on following conditions.

- In the middle of the system booting.
- Just after the administrator request
- Daily
- Weekly
- Monthly

By the conditions above, the TOE performs its file integrity test upon the initial operation, configured regular test time and the request of an administrator.

Since all the modifications are recorded regardless of its authorization, the authorized administrator must check whether the reported modification is authorized or not and renew the hash values of the files as the standard hash value database of the files.

The test result is displayed on the GWIMC web management interface.

6.1.7 TOE Access (TA)

6.1.7.1 Session Lock Function (TA_Session_Lock)

The session locking function is applied to the session of an authorized administrator's TOE access via the SysLogStore management interface.

The session is automatically locked by the TOE if the administrator's session remains idle for 10 minutes. On the locked condition, if any input is attempted, the TOE requests the re-authentication requiring administrator's ID and password. If re-authentication is successful, the administrator can access the management interface page again.

6.1.7.2 Session Termination Function (TA_Session_Term)

The session termination function is applied to the session of an authorized administrator's TOE access via the GWIMC web management interface.

This session is automatically terminated by the TOE if the administrator's session remains idle for the configured time interval by an authorized administrator. The administrator session created via the GWIMC system console interface is excluded since it allows only a direct connection physically.

6.1.8 Trusted Path/Channel (TP)

6.1.8.1 Security Channel Function (TP_SecChannel)

The TOE provides the following security communication with the secure channels that identify the terminal during communication among trusted TSFs and prevent the transmission data from the unauthorized modification and exposure.

- The communication for transmitting audit record and management data between GWIMC and SysLogStore, which are the components of the TOE
- The communication for the remote management by an authorized administrator using an IT entity located in a non-trusted external network.

If the administrator remotely accesses the GWIMC web management interface through an allowed remote IP address, the GWIMC creates a SSL-based secure channel for the access session. With the SSL session, the authorized administrator in remote location can obtain the authority equivalent to that of the authorized administrator in the internal network.

The GWIMC and SysLogStore, which are components of the TOE, communicate with each other by the SSL maintaining the security of the internal communication of the TOE.

6.2 Assurance Measures

In this chapter, the assurance measures satisfying the assurance requirements are described. For convenience, the general names of documents for the assurance measures are used instead of their full name including TOE product name, version, documented date, document identifier. And 2 documents such as “OfficeServ 7400 GWIMC Security Function Low-Level Design” and “OfficeServ 7400 GWIMC OS Low-Level Design” is described as a single document name “OfficeServ 7400 GWIMC Low-Level Design” omitting “Security Function” and “OS”. “Security Function” means the security functions belong to the TOE and “OS” means the underlying OS for supporting the TOE operation.

Also, “Low-Level Design test document” and “Function test document” are marked as “Test document”.

Assurance Component Identifiers (Name)	Assurance Measures
ACM_CAP.3 (Authorization controls)	Configuration Management document
ACM_SCP.1 (TOE CM coverage)	Configuration Management document
ADO_DEL.1 (Delivery procedures)	Delivery procedure document
ADO_IGS.1 (Installation, generation, and start-up procedures)	Life Cycle Support document Installation Guideline
ADV_FSP.1 (Informal functional specification)	Functional Specification
ADV_HLD.2 (Security enforcing high-level design)	High-level Design
ADV_IMP.2 (Implementation of the TSF)	Implementation Specification, source code
ADV_LLD.1 (Descriptive low-level design)	Low-level Design
ADV_RCR.1 (Informal correspondence demonstration)	Inserted to the Function Specification, Low-level Design, High-level Design, Implementation Specification

AGD_ADM.1 (Administrator guidance)	Administrator Security Manual
ALC_DVS.1 (Identification of security measures)	Life Cycle Support document
ALC_TAT.1 (Well-defined development tools)	Life Cycle Support document
ATE_COV.2 (Analysis of coverage)	Test Document
ATE_DPT.2 (Testing: low-level design)	Test Document
ATE_FUN.1 (Functional testing)	Test Document
ATE_IND.2 (Independent testing - sample)	TOE Product
AVA_MSU.1 (Examination of guidance)	Administrator Security Manual
AVA_SOF.1 (Strength of TOE security function evaluation)	Vulnerability Analysis Report
AVA_VLA.2 (Independent vulnerability analysis)	Vulnerability Analysis Report

7 Protection Profile Claims

This chapter describes the Protection Profiles claimed in the Security Target and the IT Security Requirements processed by the CC operation. And ST author-added Security Environments, Security Objectives, IT Security Requirements are described, too.

7.1 Protection Profile References

The following Protection Profiles are claimed in the ST and TOE satisfies all the requirements of the Protection Profiles.

- Firewall Protection Profile for Government V1.2 (May 17, 2006)
- Virtual Private Network Protection Profile for Government V1.2 (May 17, 2006)

7.2 Protection Profile Tailoring

A. Operation System Reinforcement in Assumption and OE.Operation System Reinforcement in Security Objectives for the Environment of VPNPP are tailored to exclude the description portion on VPN client, because the TOE doesn't include VPN clients. The ST selected A. Operation System Reinforcement and OE.Operation System Reinforcement of FWPP which cover those of VPNPP.

The ST selected T. Impersonation in Threats of VPNPP which covers that of FWPP.

The ST selected O. Identification and Authentication and O. Data Protection in Security Objectives for the TOE of VPNPP which cover those of FWPP.

Tailored Assumptions, Threats, Security Objectives for the TOE, Security Objectives for the Environment	
Identifier	**Tailored Contents**
A.Operation System Reinforcement	■ "In case of VPN client, operation system that underlies the TOE is reliable and stable." is deleted. ■ The assumption of FWPP which is covering that of VPNPP is selected.
T. Impersonation	The threat of VPNPP which is covering that of FWPP is selected.
O. Data Protection	The VPNPP component which is covering that of FWPP is selected.

O. Identification and Authentication	The VPNPP component which is covering that of FWPP is selected.
OE.Operation System Reinforcement	■ "In case of VPN client, operation system that underlies the TOE is reliable and stable" is deleted. ■ The FWPP component which is covering that of VPNPP is selected.

The Security Target performed the operations (Assignment, Selection, Iteration, Refinement, etc.) allowed by the Protection Profiles, and the operated security functional requirements are as follows:

Security Functional Component	
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_CKM.4	Cryptographic key destruction
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFC.2(1)	Complete information flow control
FDP_IFC.2(2)	Complete information flow control
FDP_IFF.1(1)	Single security attributes
FDP_IFF.1(2)	Single security attributes
FDP_IFF.1(3)	Single Security Attributes
FIA_AFL.1(1)	Authentication failure handling
FIA_AFL.1(2)	Authentication failure handling
FIA_ATD.1(1)	User attribute definition
FIA_ATD.1(2)	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.4	Single-use authentication mechanisms

FIA_UAU.7	Protected authentication feedback
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
FMT_MTD.1(2)	Management of TSF data
FMT_MTD.1(3)	Management of TSF data
FMT_MTD.1(4)	Management of TSF data
FMT_MTD.1(5)	Management of TSF data
FMT_MTD.1(6)	Management of TSF data
FMT_SMF.1	Specification of management functions
FPT_AMT.1	Abstract machine testing
FPT_RPL.1	Replay detection
FPT_TST.1	TSF testing
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1	Inter-TSF trusted channel

The ST claims FWPP and VPNPP conformance. The same requirements in both Protection Profiles described as a single requirement and different requirements with the same identifiers are described using the CC operation “Iteration”. With the components which have a hierarchical relationship among them within their family, higher components which are covering those of lower components are selected.

7.3 Protection Profiles Augmentation

The following table describes the components of the Assumptions, Organizational Security Policies, and Security Objectives for the environments, IT Environment Security Functional Requirements which are added to the Protection Profiles claimed in the ST.

Name	Description
A.SECURE_SERVER	The servers located outside of the TOE including the NTP server used to maintain a reliable system time in the TOE, the mail server used to send e-mail alert and the remote VPN gateway are secure.
A.SECURE_CHAN	For the communication data between the TOE and an authorized

NEL	administrator, a secure communication channel is established using the SSL, and the certificates used in the SSL are managed securely.
A.SECURE_STORAGE	The hardware and underlying OS where the SysLogStore is installed and are used as the administrator PC have no programs installed in themselves other than the OS, and the functions that support the administrator PC and SysLogStore directly or indirectly. Therefore they are secure.
OE.SECURE_SERVER	The servers located outside of the TOE including the NTP server used to maintain a reliable system time in the TOE, the mail server used to send e-mail alert and the remote VPN gateway must be managed securely.
OE.SECURE_CHANNEL	For communications between the TOE and an authorized administrator, a secure channel and certificate management function must be provided. The channel and the certificate management method must be provided using the SSL protocol.
OE.TRUSTED_STORAGE	The hardware and underlying OS where the SysLogStore is installed and are used as the administrator PC must have no programs installed in themselves other than the OS, and the functions that support the administrator PC and SysLogStore directly or indirectly. And it has to be secure.
OE.TRUSTED_NTP_SERVER	The NTP server located outside the TOE must provide the TOE with trusted and reliable time information.
FPT_STM.1	**FPT_STM.1 Reliable time stamps** Hierarchical to: No other components. Dependencies: No dependencies. FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

7.4 Protect Profile Deletion

FIA_UAU.1 of FWPP is replaced by FIA_UAU.2, which is in the higher hierarchy described in VPNPP. Therefore, the following security function components are deleted from the TOE security requirements.

Security Functional Component	
FIA_UAU.1	Authentication

Authorized general users may exist inside the logical boundary of the TOE. However, they are the users of IT entities passing through the TOE and no TOE function is provided for them to control. Therefore, there is no requirement on the authorized general user in FMT of the TOE security functional requirement and no user guidance for general users.

The following item is deleted from the TOE assurance requirements.

Assurance class	Assurance component	
Guidance Documents (AGD)	AGD_USR.1	User guidance

8 Rationale

This chapter provides rationale demonstrating the completeness and consistency of the ST.

The following sections are describing the completeness and consistency of the ST.

8.1 Rationale of Security Objectives

8.1.1 Rationale of TOE Security Objective

O. Audit

This TOE security objective ensures for the TOE to provide means to accurately record, maintain and review security-related events in details, therefore is required to counter threat of T. Recording Failure and T. Abuse and to support organizational security policy of P. Audit.

O. Flaw Implementation Inspection

This TOE security objective ensures to inspect flaw implementation possible to exist in code created by developer therefore is required to counter threat of T. Flaw Implementation.

O. Management

This TOE security objective provides means for the authorized administrator to manage the Toe in a secure manner, therefore is required to support organizational security policy of P. Secure Management.

O. Data Protection

This TOE security objective ensures for the TOE to provide integrity of transmission data and TSF data stored in the TOE therefore is required to counter threats of T. Stored Data Damage and T. Transmission Integrity and to support organizational security policy of P. Confidentiality and P. Cryptographic.

O. Confidentiality

This TOE security objective ensures for the TOE to provide confidentiality of data transmitted in the network therefore is required to counter threat of T. Decrypt and to support organizational security policy of P. Confidentiality and P. Cryptographic.

O. Identification and Authentication

This TOE security objective ensures for the TOE to uniquely identify and authorize authorized administrator and other TOE that communicates with the TOE, therefore is required to counter threats of T. Abuse, T. Impersonation, T. Continuous Authentication Attempt, T. Bypassing, T. Stored Data Damage and T. Replay Attack.

O. Self-protection

This TOE security objective ensures for the TOE to provide self-protection therefore is required to counter threats of T. Abuse, T. Bypassing, T. Stored Data Damage, T New Attack.

O. Access Control

This TOE security objective ensures access to the TOE, therefore is required to counter threat of T. Bypassing.

O. Information Flow Control

This TOE security objective ensures for the TOE to mediate information flow according to security policy, therefore is required to counter threats of T. Illegal Information Inflow, T. Illegal Information outflow and T. Address Spoofing.

O. Information Flow Mediation

This TOE security objective ensures for the TOE to mediate information flow according to security policy, therefore is required to support organizational security policy of P. Confidentiality and P. Plain Text Transmission.

O. Key Security

This TOE security objective ensures for the TOE to provide confidentiality and integrity of cryptographic key and that appropriate key exchange is provided therefore is required to counter threats of T. Decrypt and T. Transmission Integrity and to support organizational security policy of P. Confidentiality and P. Cryptographic.

Security Objective / Security Environments	O. Audit	O. Flaw Implementation Inspection	O. Management	O. Data Protection	O. Identification and Authentication	O. Self-protection	O. Access Control	O. Information Flow Control	O. Confidentiality	O. Key Security	O. Information Flow Mediation
T. Impersonation					X						
T. Flaw Implementation		X									
T. Recording Failure	X										
T. Abuse	X				X	X					
T. Decrypt									X	X	
T. Continuous Authentication Attempt					X						
T. Bypassing					X	X	X				
T. Replay Attack					X						
T. Storage Data Damage				X	X	X					
T. Transmission Integrity				X						X	
T. Illegal Information Inflow								X			
T. Illegal Information Outflow								X			
T. New Attack						X					
T. Address Spoofing								X			
P. Audit	X										
P. Confidentiality				X					X	X	X
P. Secure Management			X								
P. Cryptographic				X					X	X	
P. Plain Text Transmission											X
A. Physical Security											
A. Security Policy											
A. Security Maintenance											
A. Trusted Administrator											
A. Operation System Reinforcement											
A. Single Point of Connection											
A.SECURE_SERVER											

Security Objective / Security Environments	O. Audit	O. Flaw Implementation Inspection	O. Management	O. Data Protection	O. Identification and Authentication	O. Self-protection	O. Access Control	O. Information Flow Control	O. Confidentiality	O. Key Security	O. Information Flow Mediation
A.SECURE_CHANNEL											
A.SECURE_STORAGE											
TE. Poor Management											
TE. Delivery and Installation											

<Security Environment and the Response to the TOE Security Objective>

8.1.2 Rationale of Security Objective for the Environments

OE. Physical Security

This security objective for the environments ensures physically secure environment of the TOE, therefore is required to support assumption of A. Physical Security.

OE. Security Maintenance

When the internal network environment changes due to change in the internal network configuration, increase/decrease of host and increase/decrease of service, etc., this security objective for the environments ensures to immediately reflect the changed environment and security policy to operation policy, therefore to maintain security in the same level as before. Therefore, this security objective is required to support assumption of A. Security Maintenance and to counter threat of T. New Attack.

OE. Security Policy

This security objective for the environments ensures that the peer TOE communicating with the TOE is managed to enforce compatible security policy, therefore is required to support assumption of A. Security Policy.

OE. Trusted Administrator

This security objective for the environments ensures that the authorized administrator of the TOE can be trusted. Therefore, this is required to support assumption of A. Trusted administrator and to counter threats of T. Abuse, TE. Poor Management and TE. Delivery and Installation.

OE. Secure Management

This security objective for the environments ensures for the TOE to be delivery and installed in the secure manner and to be configured, managed and used in the secure manner by the authorized administrator. Therefore, this security objective counters threats of T. New Attack, TE. Poor Management and TE. Delivery and Installation and supports organizational security policy of P. Secure Management.

OE. Operation System Reinforcement

This security objective for the environments ensures for operation system to be reliability and stability by executing operation to remove all services or means in operation system not required by the TOE and reinforcement on vulnerabilities of operation system. Therefore this security objective is required to support A. Operation System Reinforcement and to counter threat of T. New Attack. The content mentioned in VPNPP regarding VPN clients are excluded, since it doesn't belong to the types and scope of the TOE.

OE. Single Point of Connection

This security objective for the environment ensures that all communications between the external and internal networks are carried out through the TOE, therefore is required to support assumption of A. Single Point of Connection.

OE. SECURE_SERVER

This security objective for the environment is needed for supporting the assumption A. SECURE_SERVER because it requires that external servers are secure for the TOE functionality.

OE. SECURE_CHANNEL

This security objective for environment is needed for supporting the assumption A. SECURE_CHANNEL because it requires ensuring secure communication channels while the TOE and an authorized administrator are communicating.

OE. TRUSTED_NTP_SERVER

This security objective for environment is needed for supporting organization security policy P. Audit because it requires the TOE to provide reliable time information for recording and reviewing security related events accurately and in detail.

OE. TRUSTED_STORAGE

This security objective for environment is needed for supporting the assumption A. SECURE_STORAGE because, for the secure management, it requires that only the OS and functions that directly or indirectly support SysLogStore functions are installed on the server.

Security Objective / Security Environments	OE. Physical Security	OE. Security Maintenance	OE. Truted Administrator	OE. Secure Management	OE. Operating System Reinforcement	OE. Single Point of Connection	OE. Security Policy	OE. SECURE_SERVER	OE. SECURE_CHENNEL	OE SECURE_NTP_SERVER	OE. TRUSTED_STORAGE
T. Impersonation											
T. Flaw Implementation											
T. Recording Failure											
T. Abuse			X								
T. Decrypt											
T. Continuous Authentication Attempt											
T. Bypassing											
T. Replay Attack											
T. Storage Data Damage											
T. Transmission Integrity											
T. Illegal Information Inflow											
T. Illegal Information Outflow											
T. New Attack		X		X	X						
T. Address Spoofing											
P. Audit										X	

Security Objective / Security Environments	OE. Physical Security	OE. Security Maintenance	OE. Truted Administrator	OE. Secure Management	OE. Operating System Reinforcement	OE. Single Point of Connection	OE. Security Policy	OE. SECURE_SERVER	OE. SECURE_CHENNEL	OE SECURE_NTP_SERVER	OE. TRUSTED_STORAGE
P. Confidentiality											
P. Secure Management				X							
P. Cryptographic											
P. Plain Text Transmission											
A. Physical Security	X										
A. Security Policy							X				
A. Security Maintenance		X									
A. Trusted Administrator			X								
A. Operating System Reinforcement					X						
A. Single Point of Connection						X					
A. SECURE_SERVER								X			
A. SECURE_CHANNEL									X		
A. SECURE_STORAGE											X
TE. Poor Management			X	X							
TE. Delivery and Installation			X	X							

<Security Environment and the Counter Plan for the Environmental Security Objective>

8.2 Rationale of Security Requirements

Rationale of security requirements demonstrates that the described IT security requirements are suitable to satisfy security objectives and, as a result, appropriate to address security problems.

8.2.1 Rationale of TOE Security Functional Requirements

Rationale of TOE security functional requirements demonstrates the followings.

- Each TOE security objective has at least one TOE security function requirement tracing to it. However, O. Flaw Implementation Inspection has security assurance requirement tracing to it.
- Each TOE security functional requirement traces back to at least one TOE security objectives.

Some components of the security functional requirements which performed Iteration operation newly in this ST while they are not iterated in FWPP or VPNPP respectively are not described in their iterated form in this chapter unless they have to be described in their iterated form for some unavoidable reason.

FAU_ARP.1 Security alarms

This component provides the ability in the event of detecting security violation, therefore satisfies the TOE security objective of O. Audit.

FAU_GEN.1 Audit data generation

This component provides the ability to define events for audit and to generate audit record, therefore satisfies the TOE security objective of O. Audit.

FAU_SAA.1 Potential violation analysis

This component ensures the ability to point out security violation by inspecting the audited events, therefore satisfies the TOE security objective of O. Audit.

FAU_SAR.1 Audit review

This component ensures the ability of the authorized administrator to review audit record, therefore satisfies the TOE security objective of O. Audit.

FAU_SAR.3 Selectable audit review

This component ensures the ability to search and sort audit data by bases to hold logical relations, therefore satisfies the TOE security objective of O. Audit.

FAU_SEL.1 Selective audit

This component ensures the ability to include or exclude events for audit on the basis of attributes, therefore satisfies the TOE security objective of O. Audit.

FAU_STG.1 Protected audit trail storage

This component ensures the ability to protect audit record from unauthorized modification and deletion, therefore satisfies the TOE security objective of O. Audit.

FAU_STG.3 Action in case of possible audit data loss

This component ensures handling ability in the audit trail exceeds the pre-defined limit, therefore satisfies the TOE security objective of O. Audit.

FAU_STG.4 Prevention of audit data loss

This component ensures handling ability in the audit storage is full, therefore satisfies the TOE security objective of O. Audit.

FCS_CKM.1 Cryptographic key generation

This component ensures the ability to generation cryptographic key according to the specified cryptographic key generation algorithm and cryptographic key length, therefore satisfies the TOE security objectives of O. Confidentiality, O. Data Protection and O. Key Security.

FCS_CKM.2 Cryptographic key distribution

This component ensures the ability to distribute cryptographic key according to the specified cryptographic key distribution method, therefore satisfies the TOE security objectives of O. Confidentiality, O. Data Protection and O. Key Security.

FCS_CKM.4 Cryptographic key destruction

This component ensures the ability to destroy cryptographic key according to the specified cryptographic key destruction method, therefore satisfies the TOE security objectives of O. Confidentiality, O. Data Protection and O. Key Security.

FCS_COP.1 Cryptographic Operation

This component ensures the ability to perform cryptographic operation according to the specified cryptographic algorithm and cryptographic key length, therefore satisfies the Toe security objectives of O. Confidentiality and O. Data Protection

FDP_ACC.2 Complete access control

This component ensures that security policy for the TOE access control is defined and that scope of security policy is defined therefore satisfies the TOE security objectives of O. Data Protection and O. Access Control.

FDP_ACF.1 Security attribute based access control

This component ensures that the defined security policy of access control is executed on the basis of attributes, therefore satisfies the TOE security objectives of O. Data Protection and O. Access Control.

FDP_IFC.1 Subset information flow control

This component ensures the ability to control the information flow of data transsmitted to or from the TOE according to the TOE information flow control policy, therefore satisfies the TOE security objective of O. Information Flow Mediation.

FDP_IFC.2(1) Complete information flow control

This component ensures that security policy for the TOE information flow control is defined and that scope of security policy is defined therefore satisfies the TOE security objective of O. Information Flow Control.

FDP_IFC.2(2) Complete information flow control

This component ensures that security policy for the TOE information flow control is defined and that scope of security policy is defined therefore satisfies the TOE security objective of O. Information Flow Control.

FDP_IFF.1(1) Simple security attributes

This component provides the rules to control information flow on the basis of security attributes, therefore satisfies the TOE security objective of O. Information Flow Control.

FDP_IFF.1(2) Simple security attributes

This component provides the rules to control information flow on the basis of security attributes, therefore satisfies the TOE security objective of O. Information Flow Control.

FDP_IFF.1(3) Simple security attributes

This component provides the rules to control information flow on the basis of security attributes, therefore satisfies the TOE security objective of O. Information Flow Control.

FIA_AFL.1 Authentication failure handling

This component ensures the ability to define the count of authentication failure attempt by user and to take handling actions when the defined count is reached or exceeded therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_ATD.1 User attribute definition

This component defines security attribute list for each user, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_SOS.1 Verification of secrets

This component provides the mechanism to verify whether password satisfies the defined quality metric, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_UAU.2 User authentication before any action

This component ensures the ability to successfully authenticate the authorized administrator, therefore satisfies the TOE security objectives of O. Management, O. Data Protection and O. Identification and Authentication.

FIA_UAU.4 Single-use authentication mechanisms

This component ensures the ability to prevent reusing of authentication data, therefore satisfies the TOE security objectives of O. Identification and Authentication.

FIA_UAU.7 Protected authentication feedback

This component ensures that only the designated authentication feedback is provided to user while authentication is in progress, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_UID.2 User identification before any action

This component ensures the ability to successfully identify user, therefore satisfies the TOE security objectives of O. Management, O. Data Protection and O. Identification and Authentication.

FMT_MOF.1 Management of security functions behavior

This component ensures the ability for the authorized administrator to manage security function, therefore satisfies the TOE security objective of O. Management.

FMT_MSA.1 Management of security attributes

This component ensures that the authorized administrator manages security attributes applied to access control and information flow control policies, therefore satisfies the TOE security objective of O. Management.

FMT_MSA.2 Secure security attributes

This component ensures that only safe values are accepted for security attributes, therefore satisfies the TOE security objectives of O. Management and O. Self-protection.

FMT_MSA.3 Static attribute initialization

This component provides default values of security attributes applied to access control and information flow control policies, therefore satisfies the TOE security objective of O. Management and O. Information Flow Mediation.

FMT_MTD.1(1) Management of TSF Data

This component provides the ability for the authorized administrator to handle statistical processing of audit data, therefore satisfies the TOE security objectives of O. Audit and O. Management.

FMT_MTD.1(2) Management of TSF Data

This component provides the ability for the authorized administrator to backup and recover major files composing the TOE, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.1(3) Management of TSF data

This component provides the ability for the authorized administrator to manage identification and authentication data, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.1(4) Management of TSF data

This component provides the ability for the authorized administrator to manage time, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.1(5) Management of TSF Data

This component provides the ability for the authorized administrator to manage cryptographic key attributes, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.1(6) Management of TSF data

This component provides the ability for the authorized administrator to manage TSF data determined by the Security Target author, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.2 Management of limits on TSF data

This component ensures that the authorized administrator manages limits of TSF data and takes handling actions when the indicated limits are reached or exceeded, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.3 Secure TSF data

This component ensures that only secure values are accepted for TSF data, therefore satisfies the TOE security objectives of O. Management and O. Self-protection.

FMT_SMF.1 Specification of management functions

This component requires to specify management functions, such as security attributes, TSF data and security functions, etc., to be executed by TSF, therefore satisfies the TOE security objective of O. Management.

FMT_SMR.1 Security roles

This component ensures the ability to associate user with the administrator role, therefore satisfies the TOE security objective of O. Management.

FPT_AMT.1 Abstract machine testing

This component ensures to run a suite of tests to demonstrate the correct operation of the abstract machine that underlies the TSF, therefore satisfies the TOE security objective of O. Data Protection and O. Self-protection.

FPT_RPL.1 Replay detection

This component ensures to detect replay at user authentication and that actions are taken when replay is detected, therefore satisfies the TOE security objective of O. Identification and Authentication.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that TSP enforcement functions are invoked and successful, therefore satisfies the TOE security objective of O. Self-protection.

FPT_SEP.1 TSF domain separation

This component ensures to maintain security domain for TSF's own execution, therefore satisfies the TOE security objective of O. Self-protection.

FPT_STM.1 Reliable time stamps

This component provides reliable time stamp used by the TSF. Component FAU_GEN requires accurate time and date. This is required by dependency to this component. This satisfies the TOE security objective of O. Audit

FPT_TST.1 TSF testing

This component ensures to run a suite of self tests to demonstrate the correct operation of the TSF and provides the authorized user with the capability to verify the integrity of the TSF data and the TSF executable code, therefore satisfies the TOE security objectives of O. Data Protection and O. Self-protection.

FTA_SSL.1 TSF-initiated session locking

This component requires to lock an interactive session after time interval of user inactivity and events to occur prior to unlocking the session, therefore satisfies the TOE security objectives of O. Identification and Authentication and O. Self-protection.

FTA_SSL.3 TSF-initiated termination

This component requires to terminate an interactive session after time interval of the authorized administrator inactivity, therefore satisfies the TOE security objective of O. Self-protection.

Application Note: As the TOE has no normal users other than authorized administrators,

"general user" described in FTA_SSL.3.1 is modified and tailored to "administrator"

FTP_ITC.1 Inter-TSF trusted channel

This component ensures that trusted channel is established when the authorized administrator manages the TOE locally or a remote location, therefore satisfies the TOE security objective of O. Management.

The mapping relationship between the security functional requirements and the security objective is as follows.

Security Objective / TOE Security Function Requirements	O. Audit	O. Management	O. Information Flow Control	O. Data Protection	O. Confidentiality	O. Identification and Authentication	O. Self-protection	O. Information Flow Mediation	O. Key Security	O. Access Control
FAU_ARP.1	X									
FAU_GEN.1	X									
FAU_SAA.1	X									
FAU_SAR.1	X									
FAU_SAR.3	X									
FAU_SEL.1	X									
FAU_STG.1	X									
FAU_STG.3	X									
FAU_STG.4	X									
FCS_CKM.1				X	X				X	
FCS_CKM.2				X	X				X	
FCS_CKM.4				X	X				X	
FCS_COP.1				X	X					

Security Objective / TOE Security Function Requirements	O. Audit	O. Management	O. Information Flow Control	O. Data Protection	O. Confidentiality	O. Identification and Authentication	O. Self-protection	O. Information Flow Mediation	O. Key Security	O. Access Control
FDP_ACC.2				X						X
FDP_ACF.1				X						X
FDP_IFC.1								X		
FDP_IFC.2(1)			X							
FDP_IFC.2(2)			X							
FDP_IFF.1(1)								X		
FDP_IFF.1(2)			X							
FDP_IFF.1(3)			X							
FIA_AFL.1						X				
FIA_ATD.1						X				
FIA_SOS.1						X				
FIA_UAU.2		X		X		X				
FIA_UAU.4						X				
FIA_UAU.7						X				
FIA_UID.2		X		X		X				
FMT_MOF.1		X								
FMT_MSA.1		X								
FMT_MSA.2		X					X			
FMT_MSA.3		X						X		
FMT_MTD.1(1)	X	X								
FMT_MTD.1(2)		X								
FMT_MTD.1(3)		X								
FMT_MTD.1(4)		X								
FMT_MTD.1(5)		X								

Security Objective / TOE Security Function Requirements	O. Audit	O. Management	O. Information Flow Control	O. Data Protection	O. Confidentiality	O. Identification and Authentication	O. Self-protection	O. Information Flow Mediation	O. Key Security	O. Access Control
FMT_MTD.1(6)		X								
FMT_MTD.2		X								
FMT_MTD.3		X					X			
FMT_SMF.1		X								
FMT_SMR.1		X								
FPT_AMT.1				X			X			
FPT_RPL.1						X				
FPT_RVM.1							X			
FPT_SEP.1							X			
FPT_STM.1	X									
FPT_TST.1				X			X			
FTA_SSL.1						X	X			
FTA_SSL.3							X			
FTP_ITC.1		X								

8.2.2 Rationale of IT Environment Security Functional Requirements

FPT_STM.1 Reliable time stamps

This component provides reliable time stamp used by the TSF. component FAU_GEN requires accurate time and date. This is required by dependency to this component. This satisfies the security objective for the Environment of OE. TRUSTED_NTP_SERVER.

Application Note: This means that the reliable time stamp will be received in order to

provide reliable time stamps, by setting up the environment on the external NTP server.

Security Objective / IT Environment Security Functional Requirements	OE. TRUSTED_NTP_SERVER
FPT_STM.1	X

8.2.3 Rationale of TOE Security Assurance Requirements

This ST accepted the FWPP and VPNPP of EAL3+. Therefore, the rationale is the same as the rationale provided by FWPP and VPNPP with the assurance level of EAL3+. And the augmented with components are as follows.

- ADV_IMP.2 Implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- ALC_TAT.1 Well-defined development tools
- ATE_DPT.2 Testing: low-level design
- AVA_VLA.2 Independent vulnerability analysis

The TOE security objective of the TOE O. Flaw Implementation inspection requires inspecting whether code drawn up by developers has defects and whether the Flaw Implementation affects the TOE internal components. Therefore, in accordance with this security objective, security assurance components ADV_IMP.2 (Implementation of the TSF) and ATE_DPT.2 (Testing: low-level design) have been augmented.

In accordance with dependency to ADV_IMP.2 (Implementation of the TSF), ADV_LLD.1 (Descriptive low-level design) and ALC_TAT.1 (Well Defined development tools) have been augmented. FWPP and VPNPP require not only vulnerability analysis by developers, but also independent vulnerability analysis by evaluators. Therefore, AVA_VLA.2 (Independent vulnerability analysis) has been augmented.

Authorized general users may exist in the logical scope of the TOE, however, they are IT entity users going through the TOE and no TOE function is managed by them. So there is no management requirement for authorized general users in the FMT class of the TOE security functional requirements. Therefore, no general user guidance is provided for the TOE and the assurance measure for AGD_USR.1 (User guidance) can't be applied. So AGD_USR.1 has been deleted from the TOE security assurance requirements.

8.3 Rationale of Dependency

8.3.1 Dependency of TOE Security Functional Requirements

The following table shows dependency of security functional components.

Since this ST accepted FWPP and VPNPP with EAL3+, ADV_SPM.1 is not required for them. Therefore, the dependency of ADV_SPM.1 is not described here.

In the dependency of functional components included in this ST, FDP_ACF.1, FMT_MSA.1, FMT_MSA.2 depend on FDP_ACC.1 and this is satisfied by FDP_ACC.2 that is in hierarchical relationship with FDP_ACC.1.

FIA_UAU.2 and FMT_SMR.1 depend on FIA_UID.1 and this is satisfied by FIA_UID.2 that is in hierarchical relationship with FIA_UID.1.

FIA_AFL.1, FIA_UAU.7 and FTA_SSL.1 depend on FIA_UAU.1 and this is satisfied by FIA_UAU.2 that is in hierarchical relationship with FIA_UAU.1.

Number	Components	Subordinate Relationship	Reference Number
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	39
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	2, 30
7	FAU_STG.1	FAU_GEN.1	2
8	FAU_STG.3	FAU_STG.1	7
9	FAU_STG.4	FAU_STG.1	7
10	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4, FMT_MSA.2	[11 or 13] 12, 28
11	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4, FMT_MSA.2	[- or – or 10] 12, 28
12	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or	[- or – or 10]

Number	Components	Subordinate Relationship	Reference Number
		FCS_CKM.1] FMT_MSA.2	28
13	FCS_COP.1	[FDF_ITC.1 or FDF_ITC.2 or FCS_CKM.1] FCS_CKM.4, FMT_MSA.2	[- or – or 10] 12, 28
14	FDP_ACC.2	FDP_ACF.1	15
15	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	14 29
16	FDP_IFC.1	FDP_IFF.1	18
17	FDP_IFC.2	FDP_IFF.1	18
18	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	16, 29
19	FIA_AFL.1	FIA_UAU.1	22
20	FIA_ATD.1	-	-
21	FIA_SOS.1	-	-
22	FIA_UAU.2	FIA_UID.1	25
23	FIA_UAU.4	-	-
24	FIA_UAU.7	FIA_UAU.1	22
25	FIA_UID.2	-	-
26	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	33, 34
27	FMT_MSA.1	[FDF_ACC.1 or FDF_IFC.1] FMT_SMF.1, FMT_SMR.1	[14 or 16] 33, 34
28	FMT_MSA.2	ADV_SPM.1 [FDF_ACC.1 or FDF_IFC.1] FMT_MSA.1, FMT_SMR.1	EAL.4 [14 or 16] 27, 34
29	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	27, 34
30	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	33, 34
31	FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	30, 34
32	FMT_MTD.3	ADV_SPM.1 FMT_MTD.1	EAL4 30
33	FMT_SMF.1	-	-
34	FMT_SMR.1	FIA_UID.1	25
35	FPT_AMT.1	-	-
36	FPT_RPL.1	-	-
37	FPT_RVM.1	-	-

Number	Components	Subordinate Relationship	Reference Number
38	FPT_SEP.1	-	-
39	FPT_STM.1	-	-
40	FPT_TST.1	FPT_AMT.1	35
41	FTA_SSL.1	FIA_UAU.1	22
42	FTA_SSL.3	-	-
43	FTP_ITC.1	-	-

8.3.2 Dependency of IT Environment Security Functional Requirements

Number	Components	Subordinate Relationship	Reference Number
1	FPT_STM.1	-	-

8.3.3 Dependency of TOE Security Assurance Requirements

The dependency of each security assurance package in the CC has already been satisfied. Therefore rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in the following table. This ST satisfies dependencies of all security assurance requirements.

ALC_TAT.1, AVA_VLA.2 depend on ADV_IMP.1, and this is satisfied by ADV_IMP.2 that is in hierarchical relationship with ADV_IMP.1

Authorized general users may exist in the logical scope of the TOE, however, they are IT entity users going through the TOE and no TOE function is managed by them. So there is no management requirement for authorized general users in the FMT class of the TOE security functional requirements. Therefore, no general user guidance is provided for the TOE. And AGD_USR.1 (User guidance) on which AVA_VLA.2 depends has been deleted in the dependencies of the TOE security assurance requirements.

Number	Assurance component	Dependency	Reference Number

1	ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	2 EAL3 3
2	ADV_LLD.1	ADV_HLD.2 ADV_RCR.1	EAL3 EAL3
3	ALC_TAT.1	ADV_IMP.1	1
4	ATE_DPT.2	ADV_HLD.2 ADV_LLD.1 ATE_FUN.1	EAL3 2 EAL3
5	AVA_VLA.2	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1	EAL3 EAL3 1 2 EAL3

8.4 Rationale for the TOE Summary Specification

8.4.1 Rationale for the TOE Security Functions

The following table shows that all the security functions described in the TOE summary specification meet the SFRs of the TOE. Some of the TOE security functions have to cooperate with other functions to satisfy the TOE security functional requirements.

Summary Specification	Security Functional Requirement
AU_Alarm	FAU_ARP.1
AU_AuditRecord	FAU_GEN.1 FAU_SAA.1 FAU_SEL.1
AU_View	FAU_SAR.1 FAU_SAR.3
AU_Protect	FAU_STG.1 FAU_STG.3 FAU_STG.4
DP_Filter	FDP_IFC.2(1) FDP_IFC.2(2) FDP_IFF.1(2) FDP_IFF.1(3)
DP_VPN_Filter	FDP_IFC.1 FDP_IFF.1(1) FIA_AFL.1(2) FIA_UAU.2 FIA_UID.2 FPT_RPL.1
DP_Admin_Mode	FDP_ACC.2 FDP_ACF.1
CS_KeyDeletion	FCS_CKM.4
CS_KeyMgmt	FCS_CKM.1 FCS_CKM.2

CS_ESP_AH	FCS_COP.1
IA_Password	FIA_UAU.2 FIA_UAU.7 FIA_UID.2
IA_SKEY	FIA_UAU.4
IA_Failure	FIA_AFL.1(1)
MT_Interface	FIA_ATD.1(1) FIA_ATD.1(2) FIA_SOS.1 FMT_MOF.1 FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_MTD.1(4) FMT_MTD.1(5) FMT_MTD.1(6) FMT_MTD.2 FMT_MTD.3 FMT_SMF.1 FMT_SMR.1 FPT_STM.1
PT_Sys_Diag	FPT_AMT.1
PT_File_Integrity	FPT_TST.1
TA_Session_Lock	FTA_SSL.1
TA_Session_Term	FTA_SSL.3
TP_SecChannel	FTP_ITC.1
All functions	FPT_SEP.1 FPT_RVM.1

- **AU_Alarm – FAU_ARP.1**

  The TOE notifies the authorized administrator by e-mail if any potential violation is detected.

- **AU_AuditRecord – FAU_GEN.1**

  The TOE generates audit record messages caused by all events occurred in the TOE with required information elements varied by the event types.

- **AU_AuditRecord – FAU_SAA.1**

  The TOE detects potential violation events and generates audit records on them.

- **AU_AuditRecord – FAU_SEL.1**

  The TOE provides the functions to generate audit records selectively based on event types and security levels, etc. that are configured according to the audit record policy by an authorized administrator.

- **AU_View – FAU_SAR.1**

  The TOE provides the authorized administrator with the ability to search the stored audit records in readable manner.

- **AU_View – FAU_SAR.3**

  The TOE provides the authorized administrator with the ability to search the audit records selectively based on various conditions like specified event types, key words, etc.

- **AU_Protect – FAU_STG.1**

  The TOE allows only an authorized administrator to access the generated audit records.

- **AU_Protect – FAU_STG.3**

  The TOE notifies an authorized administrator by e-mail if audit record storage is close to full.

- **AU_Protect – FAU_STG.4**

  If audit record storage is full, the TOE stops all the security functions that can generate audit record except the storage recovery function and interface, and notifies an authorized administrator by e-mail.

- **DP_Filter – FDP_IFC.2(1)**

  The TOE controls the information flow among the IT entity objects and subjects by the packet filtering security policy.

- **DP_Filter – FDP_IFC.2(2)**

  The TOE controls the information flow among the IT entity objects and subjects by the address translation policy.

- **DP_Filter – FDP_IFF.1(2)**

  The TOE controls the information flow among the IT entity objects and subjects by the packet filtering security policy.

- **DP_Filter – FDP_IFF.1(3)**

  The TOE controls the information flow among the IT entity objects and subjects by the address translation policy.

- **DP_VPN_Filter – FDP_IFC.1**

  The TOE controls the information flow among the IT entity objects and subjects by the VPN security policy.

- **DP_VPN_Filter – FDP_IFF.1(1)**

  The TOE controls the information flow among the IT entity objects and subjects by the VPN security policy.

- **DP_VPN_Filter – FIA_AFL.1(2)**

  The TOE blocks the authentication attempts of the VPN peer if it exceeds the maximum count of authentication failure configured.

- **DP_VPN_Filter – FIA_UAU.2**

  The TOE allows the action mediated by TSF if a VPN peer is successfully authenticated.

- **DP_VPN_Filter – FIA_UID.2**

  The TOE allows the action mediated by TSF if a VPN peer is successfully identified.

- **DP_VPN_Filter – FPT_RPL.1**

  The TOE checks the sequence number of the VPN packets to which AH and ESP have been applied to prevent the replay attack against the VPN packet transmission.

- **DP_Admin_Mode – FDP_ACC.2**

  The TOE performs the access control for administration interfaces varied by the TOE operation mode and management interface type, and the access control for TOE through the remote access and ICMP packet request from outside according to the administrator security policy.

- **DP_Admin_Mode – FDP_ACF.1**

  The TOE performs the access control for administration interfaces varied by the TOE operation mode and management interface type, and the access control for TOE through the remote access and ICMP packet request from outside according to the administrator security policy.

- **CS_KeyDeletion – FCS_CKM.4**

  The TOE destroys the cryptographic key by deleting the files in which the cryptographic keys are stored for the security purpose.

- **CS_KeyMgmt – FCS_CKM.1**

  For an encrypted communication with a VPN peer, the TOE creates a 128-bit cryptographic key using algorithms that meet one from the encryption algorithm list confirmed by the government organization.

- **CS_KeyMgmt – FCS_CKM.2**

  The TOE distributes cryptographic keys through the method specified in IETF RFC2409 by implementing the IKE.

- **CS_ESP_AH – FCS_COP.1**

  The TOE uses the cryptographic methods, hash algorithms, and protocols that are confirmed by the government organization for an encryption processing for the VPN communication.

- **IA_Password – FIA_UAU.2, FIA_UAU.7**

  The TOE allows the ability only for a successfully authorized administrator to access and manage the TSF. And the TOE provides limited feedbacks used for identifying reference values used for entering passwords and checking the input action is working during its authentication process.

- **IA_Password − FIA_UID.2**

  The TOE allows the identified administrator to perform the TSF-mediated actions like an authentication.

- **IA_SKEY − FIA_UAU.4**

  The TOE prevents the unauthorized reuse of the administrator authentication data by providing the mechanism for one-time password generation and management.

- **IA_Failure − FIA_AFL.1(1)**

  The TOE provides the ability to deactivate the authentication function for 5 minutes in case that the count of the administrator's password authentication failure reaches 5 applying the limits on the authentication failure count.

- **MT_Interface − FIA_ATD.1(1), FIA_ATD.1(2)**

  The TOE provides the ability to configure, store and maintain the security attributes of users like administrator and VPN peers.

- **MT_Interface − FIA_SOS.1**

  The TOE applies the quality metric like required length, combination, acceptable data types, etc. to the creation of the secrets.

- **MT_Interface − FMT_MOF.1**

  The TOE provides various security management functions controlled only by an authorized administrator.

- **MT_Interface − FMT_MSA.1**

  The TOE provides the security attribute management functions controlled only by an authorized administrator.

- **MT_Interface − FMT_MSA.2**

  The TOE ensures that only secure values are accepted for security attributes by performing validity check on the security attributes tried in the TOE.

- **MT_Interface − FMT_MSA.3**

  The TOE provides default values for the TSF data and security attributes used in the TOE and functions for an authorized administrator to se up the default value.

- **MT_Interface – FMT_MTD.1(1)**

  The TOE provides an authorized administrator with the statistics processing function for the stored audit data.

- **MT_Interface – FMT_MTD.1(2)**

  The TOE provides an authorized administrator with the backup and recovery functions for the important TOE files such as a system configuration file.

- **MT_Interface – FMT_MTD.1(3)**

  The TOE provides an authorized administrator with functions to modify or delete the identification and authentication data, such as VPN related parameters and passwords.

- **MT_Interface – FMT_MTD.1(4)**

  The TOE provides an authorized administrator with the functions to configure the time automatically or manually.

- **MT_Interface – FMT_MTD.1(5)**

  The TOE provides an authorized administrator with functions to configure the cryptographic keys used for communicating with VPN peers.

- **MT_Interface – FMT_MTD.1(6)**

  The TOE provides an authorized administrator with functions to operate the set values used for configuring various security policies.

- **MT_Interface – FMT_MTD.2**

  The TOE provides an authorized administrator with functions to set the limits for the audit storage capacity, count of authentication failure. And the TOE provides the ability to counter and test them.

- **MT_Interface – FMT_MTD.3**

  The TOE ensures only the secure values are allowed for the TSF data by performing validity test for the TSF data used in the TOE.

- **MT_Interface – FMT_SMF.1**

  The TOE provides various security management functions through the administration

interfaces.

- **MT_Interface − FMT_SMR.1**

  The TOE allows its management functions only for an authorized administrator and maintains the role of an authorized administrator.

- **MT_Interface − FPT_STM.1**

  The TOE provides the function to maintain the reliable system time and uses it to the timestamp of the audit record.

- **PT_Sys_Diag − FPT_AMT.1**

  The TOE provides the function to test the operation of the hardware elements and report the result.

- **PT_File_Integrity − FPT_TST.1**

  The TOE provides the functions to generate and maintain the integrity database of TSF data and executable files by creating their hash values, and check the integrity of the TSF data and executable files on the basis of the integrity database and report the result.

- **TA_Session_Lock − FTA_SSL.1**

  The TOE provides the function to lock the administrator session if the session connected to SysLogStore is keeping its idle condition for more than the configured time interval of the inactivity.

- **TA_Session_Term − FTA_SSL.3**

  The TOE provides the function to terminate the administrator session if the session connected to the GWIMC web management interface is keeping its idle condition for more than the configured time interval of the inactivity.

- **TP_SecChannel − FTP_ITC.1**

  The TOE invokes the SSL-based secure channel to communicate with a trusted administrator or for the communication between the GWIMC and SysLogStore.

- **All Security Functions − FPT_SEP.1**

  The TOE maintains its own security domain which is protected from access or

infringement from untrusted subjects or functions on the basis of its software and firmware design.

- **All Security Functions – FPT_RVM.1**

  The TOE prevents the bypassing access by necessarily invoking the functions enforcing the TOE security policy implemented on the basis of the identification and authentication of subject/administrator, the internal separation of the security function domain by the TOE software and firmware design.

8.4.2 Rationale for the Assurance Measures

In this chapter, for convenience, the general names of assurance documents are used omitting the TOE product name, version, documented date.

And 2 documents such as “OfficeServ 7400 GWIMC Security Function Low-Level Design” and “OfficeServ 7400 GWIMC OS Low-Level Design” is described as a single document name “OfficeServ 7400 GWIMC Low-Level Design” omitting “Security Function” and “OS”. “Security Function” means the security functions belong to the TOE and “OS” means the underlying OS for supporting the TOE operation.

Assurance Measures / Assurance Components	Configuration Management document	Delivery procedure document	Installation Guideline	Functional Specification	High-level Design	Implementation Specification, Source code	Low-level Design	Administrator Security Manual	Life Cycle Support document	Test Document	TOE Product	Vulnerability Analysis Report
ACM_CAP.3	X											
ACM_SCP.1	X											
ADO_DEL.1		X										
ADO_IGS.1			X						X			
ADV_FSP.1				X								
ADV_HLD.2					X							
ADV_IMP.2						X						
ADV_LLD.1							X					
ADV_RCR.1				X	X	X	X					
AGD_ADM.1								X				

ALC_DVS.1									**X**			
ALC_TAT.1									**X**			
ATE_COV.2										**X**		
ATE_DPT.2										**X**		
ATE_FUN.1										**X**		
ATE_IND.2											**X**	
AVA_MSU.1								**X**				
AVA_SOF.1												**X**
AVA_VLA.2												**X**

ACM_CAP.3 (Authorization controls)

The TOE provides the configuration management document to ensure the authenticated modification, and the proper functionality and usability of the configuration management system.

ACM_SCP.1 (The TOE CM coverage)

The TOE provides the configuration management document to ensure the modification is controlled according to the proper authorization for configuration items under the configuration management.

ADO_DEL.1 (Delivery procedures)

The TOE provides the delivery procedure document to ensure that the TOE receiver receives the TOE without unauthorized modification and the reliability of the delivery facilities and procedures.

ADO_IGS.1 (Installation, generation, and start-up procedures)

The TOE provides the installation guideline to ensure that the TOE is installed and used in secure manner as the developer intended. And the TOE provides the Life Cycle Support document to ensure the proper generation procedure of the TOE, because the GWIMC is delivered with itself preinstalled on the hardware.

ADV_FSP.1 (Informal functional specification)

The TOE provides the Functional Specification for the basic description on the visible interfaces and operation of TSF and for the embodiment of the TOE security functional requirements.

ADV_HLD.2 (Security enforcing high-level design)

The TOE provides the high-level design to describe the TSF's major subsystems and their relation with TOE functions implemented by them ensuring the proper TOE structure for implementing the TOE security functional requirements.

ADV_IMP.2 (Implementation of the TSF)

The TOE provides the Implementation Specification and source codes to ensure analysis on the detailed internal operation of the TSF.

ADV_LLD.1 (Descriptive low-level design)

The TOE provides the Low-level Design to describe the internal operation of the TSF with respect to the dependency and relation among the modules and ensure that the TSF subsystems are accurately and effectively specified.

ADV_RCR.1 (Informal correspondence demonstration)

The TOE provides a correspondence demonstration in the Functional Specification, High-level Design, and Low-level Design, Implementation Specification to ensure correspondence among the various representation of the TSF (TOE Summery Specification, Functional Specification, High-level Design, and Low-level Design, and Implementation Specification).

AGD_ADM.1 (Administrator guidance)

The TOE provides the officer who shall configure, maintain, and manage the TOE in accurate manner to maximize its security with Administrator Security Manual.

ALC_DVS.1 (Identification of security measures)

The TOE provides the Life Cycle Support document to protect the TOE using security policies using physical, procedural, personnel and other factors used in the development environment.

ALC_TAT.1 (Well-defined development tools)

The TOE provides the Life Cycle Support document to ensure that poorly defined, unreliable or inconsistent development tools are not used in the TOE development.

ATE_COV.2 (Analysis of coverage)

The TOE provides a Functional Test document and Low-level design Test document ensuring the TSF has been tested in systematic manner on the basis of the Function Specification.

ATE_DPT.2 (Testing: low-level design)

The TOE provides the Low-level Test document ensuring the correct implementation of the TSF subsystems and modules.

ATE_FUN.1 (Functional testing)

The TOE provides the Functional Test document ensuring the correct operation of all the security functions.

ATE_IND.2 (Independent testing - sample)

The TOE provides the TOE product (OfficeServ 7400 GWIMC) ensuring evaluator's independent testing of the security functions.

AVA_MSU.1 (Examination of guidance)

The TOE provides the Administrator Security manual ensuring that all the functions are specified well, internally consistent, and describing secure operation procedures. And the Administrator Security manual is also provided for the misuse analysis on it.

Authorized general users may exist in the logical scope of the TOE, however, they are IT entity users going through the TOE and no TOE function is managed by them. So there is no management requirement for authorized general users in the FMT class of the TOE security functional requirements. Therefore, no general user guidance is provided for the TOE. Therefore AGD_USR.1 (User guidance) has been deleted from the TOE security assurance requirements.

AVA_SOF.1 (Strength of TOE security function evaluation)

The TOE provides the Vulnerability Analysis Report to obtain the quantitative or statistical analysis report on the security actions performed by the underlying security mechanisms, and determine the strength of the security action by the effort required to defeat them.

AVA_VLA.2 (Independent vulnerability analysis)

The TOE provides the Vulnerability Analysis Report to recognize the vulnerabilities and ensure that the vulnerabilities are not exploited in the specific environment required for the

TOE.

8.5 Rationale of the Strength of Function (SOF)

Since this ST accepts FWPP and VPNPP, the information that the TOE shall protect is unclassified information and the asset value is medium level. The threat agent is considered to have low level of expertise, resources and motivation. The Common Methodology for Information Technology Security Evaluation (CEM V2.3) recommends at least providing the medium strength of function in order to handle the threat agent with low level of attack potential. In this ST, strength of function for probabilistic or permutational mechanism is decided to be SOF–medium by considering of attack potential and asset value, etc.

The security functions of the TOE Security Functional Requirements to which the SOF applied are as follows.

- FIA_UAU.2 (Replacement of FIA_UAU.1 by the Hierarchical Relationship)

The above function is implemented and described as “IA_Password” in the TOE Summary Specification section. The IA_Password satisfies SOF–medium by the quality metric applied to generate a general password provided by the “MT_Interface” and by the authentication suspension function invoked by the 5 authentication failures provided by the “IA_Failure”.

All the Identifying value of “Table 3 – Calculation of attack potential” in the “A.8 Strength of function and vulnerability analysis” section of the “Common Methodology for Information Technology Security Evaluation Version 2.3” are 0 under the combination of the restrictions for the identification and authentication above. And all the Exploiting values are unrealistic for both Elapsed Time and Access to TOE. Therefore, the value of a rating for the vulnerability given by the SOF analysis from “Table 4 – Rating of vulnerabilities” is higher than 24. As a result, the strength of the security function to which SOF is applied satisfies the SOF-medium.