VForce 1700 V1.0
Security Target

Version: 1.2
Update Date: July 20, 2006

NexG Co., LTD

<Revisions>

Version	Date	Revision	Prepared by	Approved by
1.1	June 30, 2006	First prepared.	Hwang Seong-hun	Ju Gap-su
1.2	July 20, 2006	Augmentation “Requirements for IT environment” prepared.	Hwang Seong-hun	Ju Gap-su

Table of Contents

1 Security Target Introduction

This chapter aims to identify Security Target and accurately describe typographic conventions and terms. The Target of Evaluation (TOE) is VForce 1700 V1.0 S/W of NexG, which controls information flow between networks and encrypts traffic transmitted to/from trusted networks. VForce 1700 V1.0 is a hardware device with a firewall and a Virtual Private Network built in. VForce 1700 V1.0 is a gateway-type machine that configures a firewall that controls network access using packet filtering and a VPN through IP Security (IPSec.) The VPN gateway encrypts/decrypts traffic through the Security Association (SA) with its counterpart (VPN gateway.) The TOE refers to a series of functions including major functions of the firewall and the VPN system built into VForce 1700 V1.0 S/W and supplementary network functions such as security management, audit recording, identification and authentication, routing, and DHCP.

The TOE decides whether to allow, drop, or reject networks specified by the security administrator and unencrypted traffic using the firewall or packet filtering, and processes encrypted traffic in compliance with the pre-defined VPN security policy. To execute these functions, the TOE is installed and operated at the endpoint of the network.

This Security Target for the TOE consists as follows:

- Chapter 1 introduces the Security Target and defines terms.
- Chapter 2 describes the TOE and defines scope and boundary of the TOE.
- Chapter 3 describes the TOE security environment.
- Chapter 4 describes the TOE security objectives.
- Chapter 5 describes IT security requirements.
- Chapter 6 describes the TOE summary specification.
- Chapter 7 describes protection profile claims.
- Chapter 8 provides the rationale for the Security Target.

1.1 Security Target Identification

The Security Target, TOE, and the Common Criteria for the information protection system shall be identified as follows:

Label	Description
Security Target Title	VForce 1700 V1.0 Security Target V1.1
Common Criteria Identification	Common Criteria for Information Protection System (Announcement No. 2005-25 by Ministry of Information and Communication)
Prepared by	Security and Authentication Team of NexG
Creation Date	March 30, 2006
Related Protection Profile	VPN Protection Profile V 1.1 for Government Agency (April 30, 2003) Firewall Protection Profile V1.1 for Government Agency (April 30, 2003)
TOE Identification	VForce 1700 V1.0
Terms	VPN, Integrity, Confidentiality, Identification and Authentication, Encryption, IKE, IPSec, VPN, Access Control, Information Flow Control, Firewall
Criteria	Common Criteria (CC) V2.3

1.2 Identifying Security Target and TOE

TOE provides a security function which controls information flow for secure information transmission between trusted networks connected to a public network in a physically safe environment. The security function provided by the TOE has an SOF-medium as defined in the protection profile.

1.3 Typographic Conventions

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

1.3.1 Iteration

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

1.3.2 Selection

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

1.3.3 Refinement

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

1.3.4 Assignment

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

1.3.5 Security Target Author

The Security Target author is used to indicate that final decisions related to attributes have been made by the Security Target author. The Security Target author is indicated by braces, {Decided by Security Target Author}. All security functional requirements not completely executed in the protection profile shall be completed by the Security Target Author.

1.3.6 Application Note

Application note clarifies the meaning of a requirement, provides information on options upon implementation, and warns of items that require special attention when "conformity/non-conformity" of the requirement is defined. Application note may be provided with the corresponding requirement, if necessary.

1.4 Terms and Definitions

Terms included in this Security Target and overlapping those in the Common Criteria for information protection systems and protection profiles for the government agencies shall supersede the others.

1.4.1 Object

An entity within the TSF Scope of Control (TSC) that contains or receives information and upon which subjects perform operations

1.4.2 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

1.4.3 SOF(Strength of Function)-of-Function (SOF)

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

1.4.4 SOF-medium

A level of the TOE SOF(Strength of Function)-of-function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security function by attackers possessing a moderate attack potential

1.4.5 Iteration

One of the operations defined in the Common Criteria for the information protection system. A component is used more than once in a variety of operations.

1.4.6 Security Target (ST)

A set of security requirements and functional specifications to be used as a basis for TOE evaluation

1.4.7 Protection Profile (PP)

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

1.4.8 Human User

Any person who interacts with the TOE

1.4.9 User

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

1.4.10 Selection

One of the operations defined in the Common Criteria for the information protection system. One or more items are specified from a list in a component.

1.4.11 Identity

A representation uniquely identifying an authorized user

1.4.12 Element

An indivisible security requirement

1.4.13 Role

A predefined set of rules establishing allowed interactions between a user and the TOE. (Example: User, Administrator)

1.4.14 Operation

An operation ensures that a component can respond to a certain threat in the Common Criteria for the information protection system or to satisfy a certain security policy. (Example: Iteration, Assignment, Selection, or Refinement)

1.4.15 Threat Agent

Any unauthorized user or external IT entity which threatens to access, alter, or delete assets

1.4.16 External IT Entity

Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE

1.4.17 Authorized Administrator

An authorized user who securely operates and manages the Firewall and the VPN system according to the TOE security Policy (TSP)

1.4.18 Authorized User

A user who can execute TSP functions according to the TSP

1.4.19 Authorized General User

A user who is not an authorized user who can execute TSP functions according to the TSP

1.4.20 Authentication Data

Information used to verify the claimed identity of a user.

1.4.21 Assets

Information or resources to be protected by TOE countermeasures

1.4.22 Refinement

One of the operations defined in the Common Criteria for the information protection system whereby additional details are added to a requirement. The addition of details to a component.

1.4.23 Common Criteria for Information Protection System

It is the Common Criteria published on May 21, 2005 by the Minister of Information and Communication. It is the Korean translation of Common Criteria (CC) version 2.3 which is based on the criteria of many countries and has been developed based on a common language and common understanding.

1.4.24 Organization Security Policies

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

1.4.25 Dependency

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

1.4.26 Subject

An entity within the TSC that causes operations to be performed

1.4.27 Augmentation

The addition of one or more assurance components to an EAL or assurance package

1.4.28 Component

The smallest selectable set of elements that may be included in a protection profile or Security Target.

1.4.29 Class

A grouping of families that share a common focus in the Common Criteria for the information protection system

1.4.30 Target of Evaluation (TOE)

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

1.4.31 EAL

A package consisting of assurance components that represents a point on the predefined assurance scale in the Common Criteria for the information protection system

1.4.32 Family

A group of components that share security objectives but may differ in emphasis or rigor

1.4.33 Assignment

The specification of an identified parameter in a component

1.4.34 Extension

The addition of functional requirements to an ST or PP not contained in Part 2 of the Common Criteria for the information protection system or security assurance requirements not contained in Part 3 of the Common Criteria for the information protection system.

1.4.35 Perfect Forward Security (PFS)

When a security tunnel is created between networks to form a VPN, the Diffie-Hellman algorithm is used. At this time, IKE, a key exchange protocol, supports PFS and reuses created keys instead of generating additional keys. PSF selects the Diffie-Hellman algorithm and generates keys that cannot be reused.

1.4.36 TCP Maximum Segment Size (TCPMSS)

The largest segment size in the first SYN packet of the TCP session is determined and the packet sizes for the next sessions are determined later

1.4.37 TOE security function (TSF)

A set of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP

1.4.38 TOE security Policy (TSP)

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

1.4.39 TSF Data

Data created by and for the TOE that might affect the operation of the TOE

1.4.40 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

1.4.41 VPN_PP_V1.1 (Virtual Private Network Protection Profile for Government V1.1)

VPN Protection Profile V1.1 for the government agency

1.4.42 FW_PP_V1. (1Firewall Protection Profile for Government V1.1)

Firewall Protection Profile for Government V1.1

1.5 Common Criteria Conformance

This Security Target complies with the following:

- VPN Protection Profile for Government Agency V1.1 April 30 2003 [VPN_PP_V1.1]
- Firewall Protection Profile for Government Agency V1.1 April 30 2003 [FW_PP_V1.1]
- Common Criteria for the information protection system (Notice 2005-25 by Ministry of Information and Communication, May 21 2005) [1]
- Common Criteria (CC) V2.3

The TOE that contains this Security Target fully complies with the functional requirements and the security assurance requirements specified in Parts 2 and 3 of the Common Criteria for the information protection system, VPN Protection Profile for Government Agency V1.1 [VPN_PP_V1.1] which defines minimum requirements for an information protection system for a government agency, and Firewall Protection Profile V1.1 [FW_PP_V1.1] for Government Agency. The assurance level of the TOE is EAL 3+ approved by the certificate authority (in Korea). The following is an extended security function component of Part 2 of the Common Criteria to which the TOE complies:

- FPT_TST.2 Response to the TSF Data integrity error

The following security function components have been added to VPN Protection Profile for Government Agency V1.1 [VPN_PP_V1.1] and Firewall Protection Profile for Government Agency V1.1 [FW_PP_V1.1] with which the TOE complies:

- FPR_PSE.1 Pseudonymity
- FPR_UNO.4 Authorized user observability

The following security function components have been added from Common Criteria (CC) V2.3 with which the TOE complies:

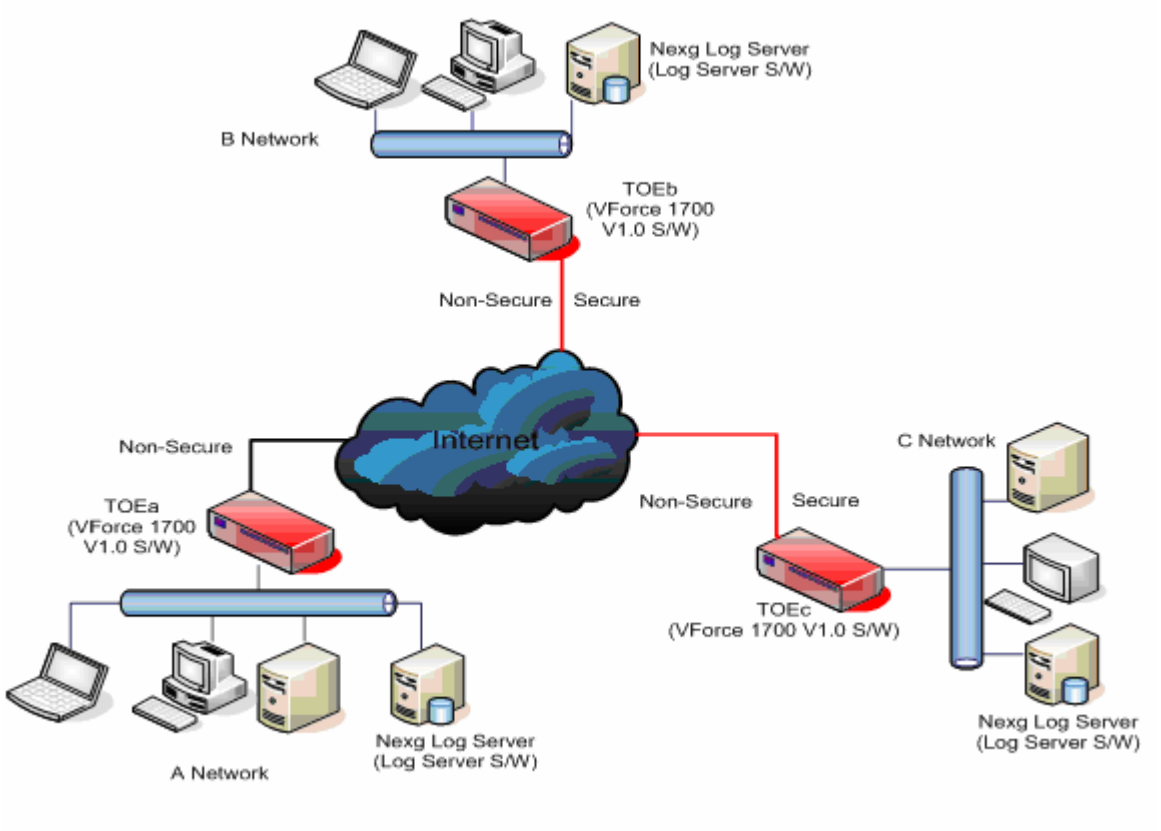
- FMT_SMF.1 Specification of Management Functions

The following assurance level components have been added to EAL3 in Part 3 of Common Criteria with which the TOE complies:

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

2 TOE Description

The TOE is VForce 1700 V1.0 S/W running in VForce 1700 hardware, and external log server S/W (Nexg Log Server). VForce 1700 V1.0 S/W provides both Firewalls with a strong access control function using packet filtering and a proxy to protect the underlying structure of the boundary and core networks of the user and a VPN which secures connection between two networks. The TOE is a security product which is equipped with a core engine integrating a kernel and security software and is configured using its own operating system.



[Figure2-1] TOE Operating Environment

As shown in [Figure2-1], the TOE can operate as a VPN or Firewall. The security policy of TOEa protects Network A from a non-secure Internet Network B establishes a trusted communication channel between TOEb and TOEc of Network C and imposes an encryption policy for the transmitted data. To allow non-secure communication (without data encryption), Network B and Network C can implement a security policy that allows only authorized users or authorized network traffic. In other words, Network B and Network C may conduct secure communication (using encryption) but they can also conduct non-secure communication (without encryption) by allowing transmission of only

authorized data. A user in the internet may need to be authorized by the gateway policy before being allowed to access the network through HTTP, TELNET, FTP, or other applications and only during certain times.

The TOE is an access control system that controls network access based on the header data of the TCP/IP v4 packet. To control access to the network, the TOE is installed at the endpoint of the network as shown in [Figure 2-1] and becomes the only access point to the Internet which the TOE protects. Each packet passing through the TOE or coming to the TOE in compliance with the packet-filtering security policy defined by the administrator is subject to the security policy of the TOE. Security policies of the TOE include Accept, Drop, and Reject. For the allowed packets, the TOE may apply an NAT (Network Address Translation) policy or use a proxy. The TOE has a trusted external DBMS to store, maintain, and manage audit records occurring during the execution of the TSF in a secure way.

2.1 Summary of Security Functions

The TOE (VForce 1700 V1.0) integrates a Firewall and a VPN—both run on the machine and the OS (VOS v3.0) developed by NexG. The TOE supports packet filtering, Network Address Translation (NAT), and proxy, and ensures secure communication by transmitting encrypted data through an IPSec-based virtual tunnel. The TOE provides the following security functions:

- Security management
- Packet filtering access control
- VPN
- NAT
- Support service
- Proxy (User authentication and mandatory access control)
- Audit records
- Identification and authentication

2.1.1 Security Management

The security management function allows the authorized administrators to manage security conditions through web or console interfaces. When the administrator manages security through the console, the TOE provides administrator commands using the Wizard so that the administrator can set up the network with an IP address that is the same as the one used when the TOE was first installed in the network. For security management through console and web interfaces, the TOE first identifies and authenticates the administrator. The authorized administrator can communicate with the TOE using a web browser in the form of SSL communication through the HTTPS protocol.

2.1.2 Packet-filtering Access Control

The packet-filtering access control function controls packet traffic according to the security policy predefined by the administrator. Based on the packet-filtering security policy, the TOE accepts, drops, or rejects packet traffic at the layer 3.

2.1.3 VPN (IPSec)

The TOE supports the VPN using IPSec. The TOE and the counterparty generate a Security Association (SA) using IKE and encrypt packet traffic between the networks of the two VPNs equipped with the TOE for data integrity.

2.1.4 Support Service

When the TOE supports VPN, the support service function encrypts the data transmitted between trusted networks by IPSec tunneling. To establish a tunnel, the TOE provides functions to create, distribute, or destroy keys based on pre-shared and RSA certificates. The TOE can issue a certificate using a built-in CA or request an external CA to issue a certificate, and can upload a certificate. To ensure integrity of execution files that provide security functions and of the security function configuration data, the TOE can conduct an abstract machine test and a file integrity test, and monitor the security function execution status. In addition, the TOE provides a time management function and network services such as DHCP, static routing, and ARP table.

2.1.5 Proxy

The proxy identifies and authenticates users for popular Internet applications such as HTTP, TELNET, and FTP so that only authorized users can access the services. The proxy uses HTTP authentication or SOCKS5 authentication. When a user accesses a proxy network defined by the administrator, a Strength of Function will be given to the user and the user's access to the network will be controlled according to that Strength of Function.

2.1.6 Audit Records

The audit record function stores audit records on a storage media upon event occurrence. Audit records are divided into real-time and non real-time audit records. Non real-time audit records are stored on separate external storage media and the administrator can check the records and calculate statistics using a separate external log server.

2.1.7 Identification and Authentication

The identification and authentication function authenticates administrators and general users using the internal user management database of the TOE. Authentication mechanisms include the password mechanism and One-Time Password (OTP) mechanism.

2.1.8 TOE Access and Privacy

All user and administrator sessions accessing the TOE are controlled by session locking and termination.

To protect privacy of the data passing through the TOE, the TOE translates source and destination IP addresses.

2.2 TOE Scope and Boundary

2.2.1 Physical Boundary

The TOE (VForce1700 V1.0) consists of the S/W (VForce 1700 V1.0 S/W) and the external log server software. The S/W of the TOE includes the firewall and the VPN functions, and the external log server software (Nexg Log Server) stores and manages audit logs. The software of the TOE runs on VForce-series hardware, and the external log server functions in an external machine.

The software of VForce 1700 is controlled by VOS, it owns operating system which is stored in flash memory and interacts with the hardware system. For availability and functional performance, VForce 1700 operates only with VOS. Basic components of the hardware where the software of the TOE operates include CPU, memory, network port, serial port, LED, and a case. The serial port connects to an external terminal. The administrator can manage the TOE through the administrator console CLI. Five network interfaces are provided to connect external networks and internal networks, and these network interfaces are physically separated so that packets not allowed by the TSP cannot pass through these interfaces. The LED helps the operator quickly check the operational status of VForce 1700 and the status of each network interface. VOS and Hardware are excluded from TOE.

The following table shows the hardware and software platform of the TOE.

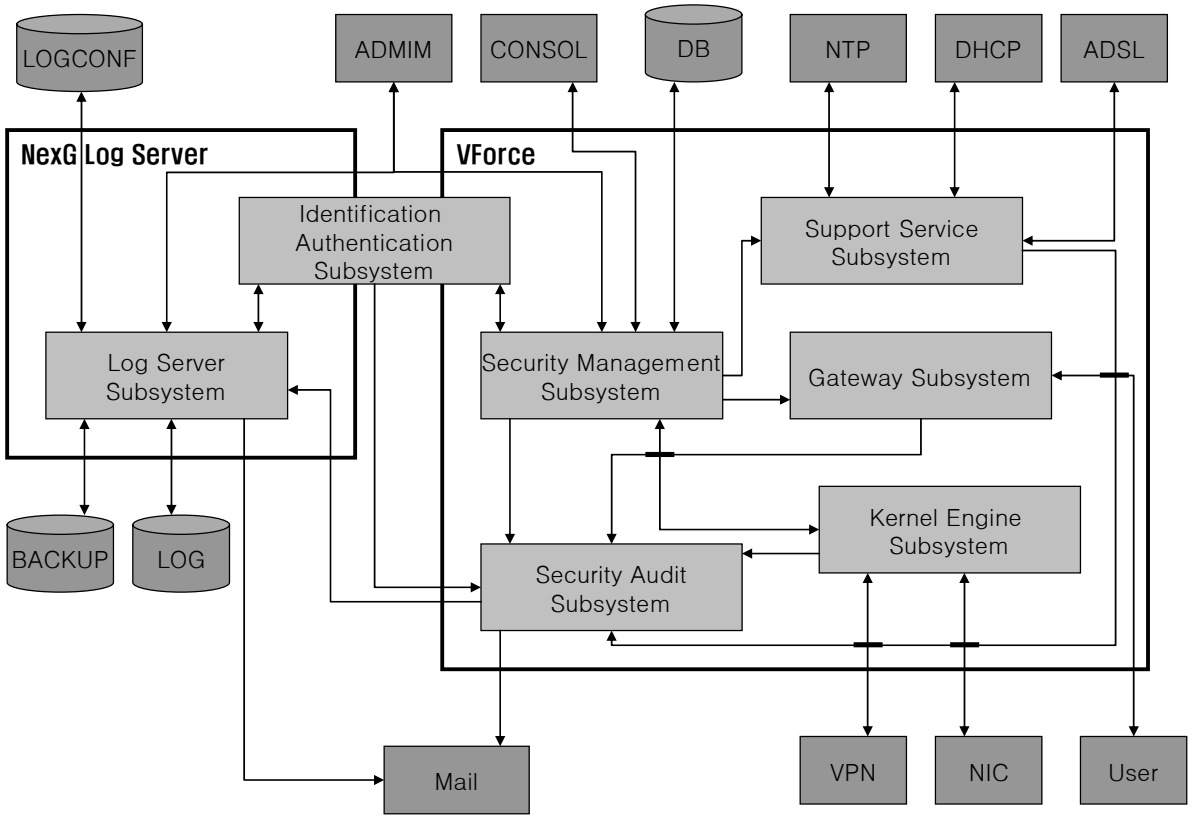
[Table 2-1] Hardware/Software Platform

Product	VForce 1700 v1.0 S/W	NexG Log Server
Hardware	CPU: VIA C3 1.2 GHz RAM: 128 MB Flash Memory: 64 MB Firmware, Configuration DB. Port: Network interface – 5 Port (10/100 Base T) Management interface – 1 Serial, 1 AUX Port	CPU: P4 2.0 GHz or higher RAM: 256 MB or more HDD: 18 GB or more Port : 2 Local NIC
Security Management	Microsoft Windows 2000 Professional/XP – Internet Explorer 6.0 SP2 or higher	

Console	- Pentium 3, 128 MB memory or more	
Operating System	VOS v3.0	RedHat 7.0 or higher

2.2.2 Logical Boundary

The TOE consists of the logical structure as shown in [Figure 2-2].



[Figure2-2] TOE Logical Boundary

2.2.2.1 Security Audit

The TOE provides access control audit records and system audit records. The access control audit records are related to access control and information flow control defined by the administrator while system audit records are related to changes in configuration, administrator's login, network connection status, or other events outside of access control. Both types of audit records include priorities. When an event crossing the threshold set by the administrator occurs, an alarm will notify the administrator. The TOE has a separate space to store both types of audit records in memory so that the administrator can search audit records in real time. The TOE also sends all audit records to an external audit record server where the administrator can check all accumulated audit records although the search is not in real time.

2.2.2.2 Cryptographic Support

For data encryption and secure communication, the TOE provides functions to generate, distribute, or revoke secret keys as well as functions related to cryptographic operations. The TOE ensures confidentiality and integrity of the packets transmitted at IP protocol layer using the IPSec tunnel-based cryptographic function. The TOE also performs both authentication and encryption in the key exchange stage to protect transmitted data using the highly reliable IPSec encryption method.

2.2.2.3 User Data Protection

The TOE basically denies traffic flow in all directions. Only traffic that passes through the TOE is controlled by the security policy predefined by the administrator. The access control and information flow control policy defines the information flow between two nodes in different sub networks connected through certain interfaces. For example, an internal user would be authenticated and allowed to access a network. In this case, the user is subject to the network access control and information flow policy. The TOE protects the user data by controlling random user access as well as imposes a mandatory access control based on the user's Strength of Function and the Strength of Function of the network object that the user tries to access.

2.2.2.4 Security Management

The TOE allows only the authorized administrator to generate, modify, or delete security attributes or TSF data and to start-up, terminate, or restart the TSF. The TOE provides CLI and web user interfaces for the administrator. The TOE does not include the web browser that supports the SSL used by the administrator to access the interface.

2.2.2.5 Identification and Authentication

In the TOE, the administrator, proxy user, and ADSL connection account users are divided into administrator and users. Every administrator or user is created and managed as a user object, and is mapped as a user group object with a Strength of Function and proxy information being registered. All administrators and users are identified and authenticated using IDs and passwords, which are stored in the user management database of the TOE.

2.2.2.6 TSF Protection

The TOE includes minimum interfaces required for execution of the TSF in hardware and software, and no other interfaces that may hinder execution of the TSF are provided. To execute the TSF, the TOE monitors the status of the security function daemons and conducts an integrity test on every file.

2.2.2.7 Trusted Path/Channel

The TOE provides a trusted path for the administrator to access the network using the SSL protocol. For secured access, the SSL protocol generates a secret key and maintains an encrypted connection.

2.2.2.8 TOE Access

The TOE manages access sessions of administrators and users. If the administrator or user remains idle for a given period of time, the TOE will perform session locking.

2.2.2.9 Privacy

The TOE translates source and destination IP addresses of the data passing through the TOE to protect user and server information.

3 TOE security Environment

This chapter defines security threats and organizational security policies related to the TOE. The TOE provides a proper level of protection for an IT environment that requires strong control of information flow on the network. The TOE does not respond to a physical attack that may damage the TOE or violate a security function (including suspension of and bypass security functions). Rather, the TOE is installed in the single point of connection of the network in a physically safe condition as specified in the assumptions, and provides security functions to protect a network connected to the TOE from all attacks. The TOE has been designed to be most suitable for the security environment defined in the Firewall for the government agency [FW_PP_V1.1] and VPN system protection profile [VPN_PP_V1.1].

3.1 Assumptions

3.1.1 Assumptions Same as Those for Protection Profile

The following describes assumptions same as those for [FW_PP_V1.1] and [VPN_PP_V1.1]:

3.1.1.1 A. Physical Security ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE is installed in a physically safe environment accessible only by authorized administrators.

Application Notes: The security policy for government agency computing equipment allows only the VPN client administrator (or authorized user) to access the VPN client.*

* - This Security Target does not support any VPN client.

3.1.1.2 A. Security Maintenance ([FW_PP_V1.1])

Upon changes in the network such as configuration changes, increase or decrease of hosts, and service increase/decrease, the new environment and the new security policy shall be immediately reflected in the TOE operation policy to provide a consistent level of security.

3.1.1.3 A. Trusted Administrator ([FW_PP_V1.1] / [VPN_PP_V1.1])

The authorized administrator of the TOE shall not have any malicious intention, receive proper training on TOE management, and follow the administrator guidelines.

3.1.1.4 A. Operating System Reinforcement ([FW_PP_V1.1] / [VPN_PP_V1.1])

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. ([VPN_PP_V1.1] – In case of a VPN client, the sub operating system of the TOE is secure and reliable. *)

* This Security Target does not support a VPN client.

3.1.1.5 A. Single Point of Connection ([FW_PP_V1.1])

All external networks and internal networks communicate with each other only through the TOE.

3.1.1.6 A. Security Policy ([VPN_PP_V1.1])

The TOE and its counterpart must use interchangeable security policies that share the same security policy and minor differences.

3.1.2 Assumptions for Author-augmented TOE

3.1.2.1 A. Trusted Server

Trusted servers are installed outside the TOE for maximum TOE performance. Such servers include the Network Time Protocol (NTP) server for reliable time management and the remote security management system.

3.1.2.2 A. Trusted Channel

The communication data between the TOE and the administrator is transmitted through a secure channel established by OpenSSL and the certificate for the OpenSSL is managed in a secure manner.

3.1.2.3 A. Trusted Storage

Audit records related to the TOE are stored, and the storage is maintained and operated in a secure manner.

3.2 Threats

This security target classifies and defines security threats that an external threat agent may impose against the assets protected by the TOE.

Major assets that the TOE protects include computer resources of the internal network and network services. External threat sources illegally access computer resources of the organization or undermine the availability of resources.

The threat agent is usually a computer user or an external IT entity accessing the internal computer. The threat agent usually possesses a low level of knowledge, resources, and motivations, and the threat agent is assumed to have a low possibility to attack vulnerabilities. The threat agent can attack clear vulnerabilities and easily gain information about vulnerabilities in the operating system and applications and the attack tools through the Internet to damage computer resources and acquire information without authorization. The TOE protects assets against these clear vulnerabilities from threat.

3.2.1 Threats Same as Those In Protection Profile

The followings are threats against the TOE augmented by the author and in [FW_PP_V1.1],, and [VPN_PP_V1.1].

3.2.1.1 T. Impersonation (Firewall System / [FW_PP_V1.1])

The threat agent may pretend as if it is an authorized user or counterpart in order to access the TOE.

3.2.1.2 T. Flaw Code ([FW_PP_V1.1] / [VPN_PP_V1.1])

The developer may include code that is not executed in some specifications and may have security flaws.

3.2.1.3 T. Storing Failure ([FW_PP_V1.1] / [VPN_PP_V1.1])

When storage is full, security-related events of the TOE may not be stored.

3.2.1.4 T. Unauthorized Information Inflow ([FW_PP_V1.1])

Unauthorized information may flow into the internal network.

3.2.1.5 T. Unauthorized Information Outflow ([FW_PP_V1.1])

An internal user can send information out of the network without authorization.

3.2.1.6 T. New Attack ([FW_PP_V1.1])

The threat agent can launch attacks against the TOE operating environment or newly found vulnerabilities of the TOE.

3.2.1.7 T. Continued Authentication Attempts ([FW_PP_V1.1] / [VPN_PP_V1.1])

The threat agent can access the TOE after continued access attempts.

3.2.1.8 T. Bypassing ([FW_PP_V1.1] / [VPN_PP_V1.1])

The threat agent can access the TOE by bypassing the TOE security functions.

3.2.1.9 T. Replay Attack ([FW_PP_V1.1] / [VPN_PP_V1.1])

The threat agent can access the TOE by replaying the authentication data of an authorized user.

3.2.1.10 T. Stored Data Damage ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TSF data stored in the TOE may be exposed, changed, or deleted without authorization.

3.2.1.11 T. IP Address Spoofing ([FW_PP_V1.1])

A threat agent in an external network may try to access the internal network by spoofing the source IP address as an internal IP address.

3.2.1.12 T. Abuse ([VPN_PP_V1.1])

An authorized user of the TOE may damage the TSF intentionally or for other reasons.

3.2.1.13 T. Decoding ([VPN_PP_V1.1])

The threat agent may decode the data and access data without authorization.

3.2.1.14 T. Transmission Integrity ([VPN_PP_V1.1])

The threat agent may convert the data transmitted on the network without authorization.

3.2.2 Threats against Author-augmented TOE

3.2.2.1 T. Privacy

When the IP address of the internal network is known as an IP address of a non-secure network, an attacker may access the internal network without authorization.

3.2.3 Threats against TOE Operating Environment Same as Protection Profile

The followings are threats against the TOE operating system that is the same as [FW_PP_V1.1] and [VPN_PP_V1.1]:

3.2.3.1 TE. Poor Management ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE may be configured, operated, and used by an authorized administrator in a non-secure way.

3.2.3.2 TE. Delivery and Installation ([FW_PP_V1.1] / [VPN_PP_V1.1])

Security breaches may occur in the TOE during delivery and installation.

3.3 Organizational Security Policies

3.3.1 Organizational Security Policies Same as Those in Protection Profile

The following shows the organizational security policies that are the same as those in [FW_PP_V1.1] and [VPN_PP_V1.1]:

3.3.1.1 P. Audit ([FW_PP_V1.1] / [VPN_PP_V1.1])

To trace responsibilities of all security-related behaviors, all security-related events shall be stored, maintained, and reviewed.

3.3.1.2 P. Trusted Management ([FW_PP_V1.1] / [VPN_PP_V1.1])

The authorized administrator shall manage the TOE in a secure manner.

3.3.1.3 P. Confidentiality ([VPN_PP_V1.1])

If the network traffic transmitted to/from the counterpart of the TOE is specified on the TOE security policy, the traffic shall be encrypted or decrypted by the TOE.

3.3.1.4 P. Cryptographic ([VPN_PP_V1.1])

The cryptographic algorithm and module used in the TOE must be approved by the Director of National Intelligence Service.

3.3.1.5 P. Plain Text Transmission ([VPN_PP_V1.1])

All network traffic other than those transmitted to/from the counterpart of the TOE are allowed to be transmitted without encryption/decryption according to the TOE security policy.

4 Security Objectives

4.1 TOE security Objectives

4.1.1 TOE security Objectives Same as Those for Protection Profile

The following describes the TOE security objectives augmented by the author and in [FW_PP_V1.1] and [VPN_PP_V1.1].

4.1.1.1 O. Audit ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE shall store and maintain security-related events to trace responsibilities of security-related behaviors, and shall provide a means for the administrator to review the stored data.

4.1.1.2 O. Flow Code Inspection ([FW_PP_V1.1] / [VPN_PP_V1.1])

All code created by the developer shall be inspected for flaws, and code with flow shall be inspected for its affect on internal elements of the TOE.

4.1.1.3 O. Management ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE shall provide a means for an authorized administrator of the TOE to efficiently manage the TOE.

4.1.1.4 O. Data Protection ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE shall protect the TSF data stored in the TOE and data transmitted on the network from unauthorized exposure, change, or deletion.

4.1.1.5 O. Identification and Authentication ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE shall identify and authenticate the user before allowing the user to access the TOE. Before tunneling with the counterpart, the TOE shall authenticate the counterpart.

4.1.1.6 O. Self Function Protection ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE shall protect itself from changes, deactivation, and bypassing of the security functions.

4.1.1.7 O. Access Control ([FW_PP_V1.1])

The TOE shall control access to internal and external networks according to the security policy.

4.1.1.8 O. Information Flow Control ([FW_PP_V1.1])

The TOE shall control unauthorized information inflow and outflow.

4.1.1.9 O. Confidentiality ([VPN_PP_V1.1])

The TOE shall guarantee the confidentiality of the data transmitted on the network.

4.1.1.10 O. Information Flow Mediation ([VPN_PP_V1.1])

The TOE shall mediate information flows between the TOE and its counterpart according to the security policy.

4.1.1.11 O. Key Security ([VPN_PP_V1.1])

The TOE shall guarantee confidentiality and integrity of the cryptographic key data and secure key exchanges.

4.1.2 Security Objectives for Author-augmented TOE

4.1.2.1 O. Privacy

The TOE shall prevent external users from predicting the IP addresses of internal users.

4.2 Security Objectives for the Environment

4.2.1 Security Objective for Environment Same as Those in Protection Profile

The following describes the security objectives for an environment the same as [FW_PP_V1.1] and [VPN_PP_V1.1]:

4.2.1.1 OE. Physical Security ([FW_PP_V1.1] / [FW_PP_V1.1])

The TOE shall be located in a physically safe environment whereby only an authorized administrator can access it.

4.2.1.2 OE. Security Maintenance ([FW_PP_V1.1])

Upon changes in the network such as configuration changes, increase or decrease of hosts, and service increase/decrease, the new environment and the new security policy shall be immediately reflected in the TOE operation policy to provide a consistent level of security.

4.2.1.3 OE. Trusted Administrator ([FW_PP_V1.1] / [VPN_PP_V1.1])

The authorized administrator of the TOE shall not have any malicious intentions, receive proper training on the TOE management, and follow the administrator guidelines.

4.2.1.4 OE. Trusted Management ([FW_PP_V1.1] / [VPN_PP_V1.1])

The TOE shall be distributed and installed in a secure manner, and must be configured, managed, and used by an authorized user in a secure manner.

4.2.1.5 OE. Operating System Reinforcement ([FW_PP_V1.1] / [VPN_PP_V1.1])

Unnecessary services or means are removed from the operating system, and security is enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.

4.2.1.6 OE. Single Point of Connection ([FW_PP_V1.1])

All communication between an external network and an internal network shall be established through the TOE.

4.2.1.7 OE. Security Policy ([VPN_PP_V1.1])

The TOE and its counterpart must use interchangeable security policies which share main security policies and minor differences.

4.2.2 Security Objectives for Author-augmented Environment

4.2.2.1 OE. Trusted Server

All servers that communicate with the TOE are installed outside the TOE and shall be secure. The Network Time Protocol (NTP) and the remote security management system maintain secure time.

4.2.2.2 OE. Trusted Channel

For secure communication between the TOE and the administrator, secure channels and certificate management functions are provided through the open SSL standard protocol.

4.2.2.3 OE. Trusted Storage

TOE-related audit records are stored, and the storage is maintained and operated in a secure manner. The storage provides a relational database SQL-Lite.

5 IT Security Requirements

This chapter specifically describes security functions and assurance requirements for the TOE. All requirements are same as those in the protection profile upon which this Security Target was created. The author added some security functions that the TOE provides but are not included in the protection profile by referring to the Common Criteria for the information protection system.

5.1 TSF Requirements

This paragraph describes the Security functional requirements (SFR):

- Security functional requirements same as those in the protection profile: This Security Target integrated and tailored SFRs of two protection profiles ([VPN_PP_V1.1] and [FW_PP_V1.1]) and includes all SFRs of these two protection profiles.

- Security functional requirements added by the author: The author added some security functions that are not included in the protection profile but provided by the TOE by referring to the Common Criteria for the information protection system.

- The SOF of the TOE is SOF-medium according to the SOF of [VPN_PP_1.1] and [FW_PP_1.1] with which this Security Target complies. FIA_UAU.2 and FIA_UAU.4 satisfy with SOF-medium specified in the Common Criteria for the information protection system (Notice 2005-25 by Ministry of Information and Communication) [1]. Moreover, FTP_TST.1 and FTP_TST.2 Hash functions have SOF-high.

5.1.1 Reused Security functional requirements (SFR) in Protection Profile

The Security functional requirements (SFR) to which this Security Target refers consists of SFR components of two protection profiles. The author added some SFRs that the TOE provides but are not included in the two protection profiles by referring to the Common Criteria for the information protection system.

[Table 5-1] Security functional requirements (SFR)

Security Function Class	Security Function Component		PP Identification*
Security Audit	FAU_ARP.1	Security alarms	F / V
	FAU_GEN.1	Audit data generation	F / V
	FAU_SAA.1	Potential violation analysis	F / V
	FAU_SAR.1	Audit review	F / V
	FAU_SAR.3	Selectable audit review	F / V
	FAU_SEL.1	Selective audit	F / V
	FAU_STG.1	Protected audit trail storage	F / V
	FAU_STG.3	Action in case of possible audit data loss	F / V
	FAU_STG.4	Prevention of audit data loss	F / V
Cryptographic Support	FCS_CKM.1	Cryptographic key generation	V
	FCS_CKM.2	Cryptographic key distribution	V
	FCS_CKM.4	Cryptographic key destruction	V
	FCS_COP.1	Cryptographic operation	V
User Data Protection	FDP_ACC.2	Complete access control	F
	FDP_ACF.1	security attribute based access control	F
	FDP_DAU.1	Basic data authentication	V
	FDP_IFC.1	Subset information flow control – VPN SFP	V
	FDP_IFC.2(1)	Complete information flow control – PacketFiltering SFP	F
	FDP_IFC.2(2)	Complete information flow control – Proxy SFP	F
	FDP_IFF.1(1)	Simple security attributes – VPN SFP	V
	FDP_IFF.1(2)	Simple security attributes – PacketFiltering SFP	F

	FDP_IFF.1(3)	Simple security attributes – Proxy SFP	F
Identification and Authentication	FIA_AFL.1	Authentication failure handling	F / V
	FIA_ATD.1	User attribute definition	F / V
	FIA_SOS.1	Verification of secrets	F / V
	FIA_UAU.1**	Timing of authentication	F
	FIA_UAU.2	User Authentication before any action	V
	FIA_UAU.4	Single-use authentication mechanisms	F / V
	FIA_UAU.7	Protected authentication feedback	F / V
	FIA_UID.2	User identification before any action	F / V
Security Management	FMT_MOF.1	Management of security functions behavior	F / V
	FMT_MSA.1	Management of security attributes	F / V
	FMT_MSA.2	Secure security attributes	V
	FMT_MSA.3	Static attribute initialisation	F / V
	FMT_MTD.1(1)	Management of TSF Data	F
	FMT_MTD.1(2)	Management of TSF Data	F
	FMT_MTD.1(3)	Management of TSF Data	F
	FMT_MTD.1(4)	Management of TSF Data	V
	FMT_MTD.1(5)	Management of TSF Data	F / V
	FMT_MTD.1(6)	Management of TSF Data	F / V
	FMT_MTD.2	Management of limits on TSF data	F / V
	FMT_MTD.3	Secure TSF Data	V
	FMT_SMR.1	Security roles	F / V
TSF Protection	FPT_AMT.1	Abstract machine testing	F / V
	FPT_RPL.1	Replay detection	V
	FPT_RVM.1	Non-bypassability of the TSP	F / V
	FPT_SEP.1	TSF domain separation	F / V
	FPT_STM.1	Reliable time stamps	F / V
	FPT_TST.1	TSF testing	F / V
	FPT_TST.2 (Extension)	TSF Data integrity error handling	F / V
TOE Access	FTA_SSL.1	TSF-initiated session locking	F / V
	FTA_SSL.3	TSF-initiated termination	F
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel	V

* - F: [FW_PP_V1.1], V: [VPN_PP_V1.1]

** - FIA_UAU.1 of [FW_PP_V1.1] has a hierarchical relationship with FIA_UAU.2 of [VPN_PP_V1.1]. This Security Target adopted FIA_UAU.2, and FIA_UAU.1 is not explained here.

5.1.1.1 Security Audit (FAU)

FAU_ARP.1 Security Alarm

Hierarchical to: No other components
Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [{Notification to the administrator via warning mail, warning message popup}] 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 shut-down of the audit function.
b) All events subject to auditing according to the ***minimum*** audit level.
c) [See [Table 5-2] Audit Target Events. {None}]

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

a) Event date, event type, subject identity, and event result (Success or failure)
b) Audit data type based on the audit target event definition of the functional component included in the protection profile or Security Target. [[Table 5-2] Audit Target Events, Information related to the audit target events of {Next}]

- System audit – Event priority, Process name, Message contents (Open/Close, Details)
- Access control audit – Processing result (ACCEPT/DROP/REJECT), prefix (Audit record prefix to identify packet audit records), Interface name (Direction – In/Out), Source/Destination IP address, Protocol, Source/Destination port, ICMP type/code
- IPSec packet audit – Event priority, Message contents (Details)

[Table 5-2] Audit Target Event

Functional Component	Audit Target Event	Augmented Audit Records
FAU_ARP.1	Actions against sudden security breaches	Estimated source/destination addresses.
FAU_SAA.1	Operation initiation and stoppage of analysis mechanism, automatic response by the tool.	Authorized administrator's identity.
FAU_SEL.1	Changes in audit environment occurring while audit collection function is executed.	-
FCS_CKM.1	Success and failure of the behavior.	Estimated source/destination addresses.
FCS_CKM.2	Success and failure of the behavior.	Estimated source/destination addresses.
FCS_CKM.4	Success and failure of the behavior.	Estimated source/destination addresses.
FCS_COP.1	Success and failure of cryptographic operation, cryptographic operation type.	Estimated source/destination addresses.
FDP_DAU.1	Successful creation of valid evidence.	Estimated source/destination addresses.
FDP_ACF.1	Successful request for operation in relation to the object handled by the SFP.	Subject and object identifiers.
FDP_IFF.1	Decision to allow the requested information flow.	Subject and object identifiers, estimated source/destination addresses.
FIA_AFL.1	Reaching the threshold of failed authentication attempts and responses including recovery to normal state, if proper.	Identification of unauthorized users and authorized administrators.
FIA_SOS.1	Rejection of all tested secret by the TSF.	-
FIA_UAU.2	Failure of the authentication mechanism.	User identity provided for the TOE.
FIA_UID.2	Failure of user identification mechanism including provided user identity.	User identity provided for the TOE.
FMT_MSA.1	Changes in all security attributes.	Security attributes.
FMT_MSA.2	All proposed security attributes and denied security attributes.	Estimated source/destination addresses.
FMT_MTD.1	Changes in the TSF data.	Changed TSF data.

FMT_MTD.2	Changes in the TSF data thresholds.	Changed TSF data threshold.
FMT_MTD.3	All rejected TSF data.	Estimated source/destination addresses.
FPT_SEP.1	Change in the user group sharing the role.	Authorized administrator's identity.
FPT_STM.1	Time change.	Authorized administrator's identity.
FPT_TST.2	Description of integrity error, actions against the integrity error, and result of actions taken.	-
FTA_SSL.1	Locking of the interactive session by the session locking mechanism.	-
FTA_SSL.3	Termination of the interactive session by the session locking mechanism.	-
FTP_ITC.1	Faults in the secure channel function, identification of a secure channel where a fault occurred from an initiator.	Initiator of a secure channel where a fault occurred and the target identity.
FMT_MOF.1	Use of related functions belonging to the audit records.	Authorized administrator's identity.
FMT_SMF.1	Use of management functions.	Authorized administrator's identity.
FPR_PSE.1	Subject/User who requested an answer to user identity.	Estimated source/destination addresses.
FPR_UNO.4	Observation of resources or services by user or subject.	User identity provided for the TOE. Estimated source/destination addresses.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

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

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

a) Accumulation or combination of [Identification and authentication security policy violation, Access control rule violation, Cryptographic operation failure] known to indicate a potential security violation.
b) [{None}]

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [Authorized 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 interrupt 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 the audit data based on [{standards for the following logical relations}].

a) Audit record types – System log, firewall log, session log, proxy session log
b) System log – Time, host IP address, priority, process, message contents (Details: Keyword)
c) Firewall/Session log – Time, host, source/destination IP address, protocol, source/destination port, ICMP type, service, size, operation (ACCEPT/DROP/REJECT/OPEN/CLOSE)
d) proxy session log – Time, host IP Address, source/destination IP address, user, service, operation (open, close)

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) [{Packet-filtering 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 [send notification to authorized administrator, {None}] if audit trail exceeds [{The default remaining space of the storage media where the audit records are stored is 10% and the administrator's setting (0~99%)}]

FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *prevents audit target events except actions taken by an authorized user with special authority* and [{When the default remaining space of the storage media is 5% and the administrator's setting (0~99%) is crossed, a notification will be sent to the authorized administrator and action will be taken to stop the TSF of the TOE.}], if the audit trail is full.

Application Notes: If audit storage is full, only the authorized administrator shall be allowed to perform operations. Only after the authorized administrator restores storage can audit records be generated.

5.1.1.2 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 [standard block cryptographic algorithm for government agencies] and specified cryptographic key sizes [128 bits or more] that meet the following: [standard block cryptographic algorithm list for government agencies].

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 access

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 [**All plain text cryptographic key in the device and important security-related parameters will be changed into 0.**].

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 The TSF shall perform [Method defined in "The ESP CBC-Mode Cipher Algorithms" (RFC2451), Using HMAC-SHA-1-96 (RFC2404) with IPSec AH and a 160-bit key in the ESP] in accordance with a specified cryptographic algorithm [Standard block cryptographic algorithm for government agency, Hash function algorithm standard (HAS-160)]and cryptographic key sizes [128 bits or higher, 160 bits] that meet the following: [Standard block cryptographic algorithm for government agencies, IT industry standard TTAS.KO-12.0011/R1 "Hash function standard – Part 2: Hash function algorithm standard (HAS-160)"].

5.1.1.3 User Data Protection (FDP)

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

Dependencies to: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [{administrator security policy}] on [{the following subject list and object list}]and all operations among subjects and objects covered by the SFP.

a) Subject list: IT entity of the administrator authenticated by FIA_UAU.2 or FIA_UAU.4.

b) Object list:

- TOE security management (Control Center)
- TOE system console

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 initialisation

FDP_ACF.1.1 The TSF shall enforce the [{administrator security policy}] to objects based on the following: [{following security attribute, Named security attribute group}]

a) Administrator group
b) Administrator Network

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[{

a) Allow if the user belongs to the administrator group. Otherwise, deny.

b) Allow if the user belongs to the administrator group and the source network IP address is set in the administrator network. Otherwise, deny.

}]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [{Administrator's access to TOE console }]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [{None}].

FDP_DAU.1 Basic data authentication

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [data transmitted through the TOE]

FDP_DAU.1.2 The TSF shall provide [authorized administrator] with the ability to verify evidence of the validity of the indicated information.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [{VPN security policy}] on [the following subjects, information, operations].

a) Subject list: External IT entities transmitting data through the TOE

b) Information list: Data transmitted through the TOE

c) Operation list:

- Encryption and hash of the information transmitted to the counterpart.
- Decryption and integrity check of the information, transmission to the subject.
- Information passing.

Application Notes: The TOE can establish secure or non-secure communication depending on the TSP.

FDP_IFF.1(1) Subset Information Flow Control

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFC.1.1 The TSF shall enforce the [{VPN security policy}] on [the following] security attributes of subjects and information.

a) Subject security attribute: IP addresses of external IT entities transmitting data through the TOE, {Certificate subject (Certificate country, Organization, Organization Unit, Common Name, Email Address)}

b) Information security attribute: Source and destination IP address to/from which the data packets are transmitted, {Following security attributes}

- IPSec-bound interface
- Shared key
- Security protocol
- Key exchange mode
- Authentication method (Shared key/Certificate)
- Subject security attribute – local and remote VPN gateway information (IP address and certificate subject)
- ISAKMP policy – Encryption type (algorithm) and key length, hash algorithm, Diffie-Hellman group (Numbers 2 and 5), valid period
- IPSec policy – Authentication method (authentication algorithm), encryption method (encryption algorithm) and key length, valid time
- VPN Network IP Address

- PFS group - Diffie-Hellman group (Numbers 2 and 5)

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 counterpart: For traffic coming from or going to the counterpart, the TOE shall perform the following according to the security policy:

- establish a trusted channel with the counterpart, or use an existing trusted channel, or
- not call a security mechanism for the communication nor establish a secure channel.

b) Communication with other than the counterpart: For traffic not coming from or going to the counterpart, the TOE does not call a security mechanism nor establish a security channel.

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

FDP_IFF.1.4 The TSF shall provide the [{following}].

a) Create the corresponding tunnel upon a request for tunnel connection or tunnel creation.
b) Use Dead Peer Detection (DPD.)

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}].

FDP_IFC.2 (1) Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

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

a) Subject list: Internal/External IT entities exchanged through the TOE and the TOE itself.
b) Information list: All traffic (packet) passing 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

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

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

a) Subject list: Internal/External IT entities exchanged through the TOE.
b) Information list: Protocol (FTP, TELNET traffic) using HTTP and SOCK5 passing 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 (3) Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

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

a) Subject list: Internal/External IT entities exchanged through the TOE.
b) Information list: All traffic (packet) passing 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

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [{packet-filtering security policy}] based on the types of subject and information security attributes: [{as shown below}].

a) Subject security attribute: IP addresses of internal and external IT entities transmitting data through the TOE.

b) Information security attribute:

- Interface policy mapping
- Source/destination IP Address, Security label
- Service (port)
- Time
- Number of packets per second (Minimum 1~10,000)
- Packet size (Minimum 1~65535)
- MAC address
- TCPMSS (Minimum 0~65495)

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: [as shown below].

a) [{If the information security attribute of the corresponding traffic is proven to be subject to information flow according to the packet-filtering security policy set by the administrator, information flow will be allowed.}]

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

a) The port scan for the traffic subject to the packet-filtering security policy will be detected, and the audit records or mail will be sent to the administrator.
b) A fragment packet for the traffic subject to the packet-filtering security policy will be detected, and the audit records or mail will be sent to the administrator.

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: [as shown below].

a) Basic packet-filtering policy – If there is no packet-filtering security policy met.
b) When the Source security label is lower than the destination security label.

FDP_IFF.1(3) Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [{proxy security policy}] based on the types of subject and information security attributes: [{as shown below}].

a) Subject security attribute: User and network addresses of internal/external IT entities, user ID, and user Strength of Function

b) Information security attribute:

- Security attribute – Maximum access count (5~65535), Session time-out (5~65535)
- Proxy time group
- Proxy network group
- HTTP authentication control
- SOCKS5-type authentication control

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: [as shown below].

a) [{If the information security attribute of the corresponding traffic is proven to be subject to information flow according to the proxy security policy set by the administrator, information flow will be allowed.}]

FDP_IFF.1.3 The TSF shall enforce the [{reauthentication for the following cases}].

a) After idle status between the user and the proxy within the session time-out limit set by the administrator
b) After the administrator forcibly logs out a user

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: [{basic proxy policy – traffic of an unauthenticated user passing through HTTP or SOCKS5 }].

FDP_IFF.1(4) Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [{network address translation policy}] based on the types of subject and information security attributes: [{as shown below}].

a) Subject security attribute: source and destination network addresses of internal/external IT entities

c) Information security attribute:

- Network address translation – IP address range for Network Address translation
- Port binding – port range for port binding
- Service

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: [as shown below].

a) [{The network address shall be translated according to the network address translation policy set by the administrator, and then, information flow shall be allowed.}]

FDP_IFF.1.3 The TSF shall enforce [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].

5.1.1.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication*
* - [VPN_PP_V1.1] selected FIA_UAU.2 which has hierarchical relationship with FIA_UAU.1 so this Security Target adopted FIA_UAU.2.

FIA_AFL.1.1 The TSF shall detect when [{an administrator configurable positive integer other than 0}] unsuccessful authentication attempts occur related to [{user authentication attempt}]

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.].

Application Notes: A user is an authorized administrator or a counterpart. For a counterpart, other measures than the user authentication attempt count can be used.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users[the list of the following security attributes].

a) Security label
{

b) User Object - User ID (ID), group, use status (by the current user), password type, password, PAP, CHAP, log-in failure count, allowed log-in, last log-in, use time
c) User group - User Object group ID, attempt limit, proxy status (proxy time selection), administrator mode status, user ID
d) VPN gateway - X.509-type certificate subject, IP Address
}

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1(1) The TSF shall provide a mechanism to verify that secrets meet [the following limit].

a) Minimum length of the password set by the administrator
- General password: 7~16 characters
- One-time password: 8 characters

b) Combination rule – Alphanumeric (alphabetic + numeric, or alphabetic + special symbols)

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [one-time password].
Application Notes: The single-use authentication mechanism can be applied to both authorized administrators and user. single-use authentication mechanism may not be used as long as the provided services conform to the security policy.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication*
* - [VPN_PP_V1.1] selected FIA_UAU.2 which has a hierarchical relationship with FIA_UAU.1 so this Security Target adopted FIA_UAU.2.

FIA_UAU.7.1 The TSF shall provide only [counterfeited password (Example: *)] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID Timing of identification
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.

5.1.1.4 Security Management (FMT)

FMT_MOF.1 Management of security functions behaviors

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security Role

FMT_MOF.1.1 The TSF shall restrict the ability to *activate, stop, start, change* the functions [{listed as below}]] to [the authorized administrator].

a) Object definition – Certificate, CA management, Network, Service, Time, IPSec, User
b) Status checking – Traffic per interface, Session list, IPSec security tunnel, Log-in user, Integrity, System (firmware version, start-up time, CPU load), Process
c) Interface management – Ethernet and PPP (PPPoE for ADSL authentication) setup and management
d) Static routing management
e) ARP address list management
f) DHCP server management
g) Network Address Translation policy management – Network Address Translation, port forwarding, redirect policy
h) Basic proxy setting management
i) Administrator password change
j) SNMP configuration management
k) Date and time management
l) Firmware upgrade
m) System restart/stop
n) Audit records backup
o) Audit records setup management

Application Notes: These security functional requirements are for the management of security functions. For example, when the audit record storage is full, the security functional requirements describe what measures the authorized administrator shall take and under which circumstances the administrator can conduct a self-test.

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_SMF.1 Speciation of Management functions
FMT_SMR.1 Security role

FMT_MSA.1.1 The TSF shall enforce [{administrator security policy}] to restrict the ability to *change, inquire, and delete default, {None* security attributes {Security label, FDP_IFF.1-packet-filtering security policy rule audit records

status and limit, Port scanning packet, Audit recording status for abnormal packets, TCPMSS setup, VPN security policy, Proxy security policy}] to [the authorized administrator]].

Application Notes: The authorized administrator shall support execution of the information flow control SFP by managing security attributes.

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 initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [{packet-filtering security policy, proxy security policy, 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

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 *handle the statistic of* the [audit data] to the [authorized administrator]

FMT_MTD.1(2) Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *recover, backup* the [major files composing the TOE] *in a permanent auxiliary storage device* 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 *query, modify, and delete* the [access control security policy, information flow control security policy] to the [authorized administrator].

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 [cryptographic key attribute] to the [authorized administrator].

FMT_MTD.1(5) 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].

FMT_MTD.1(6) 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].

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.
Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [audit storage capacity, authentication failure count, self-test interval] to [authorized administrator].

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

Application Notes: If the counterpart is not authenticated, another standard can be used rather than the authentication failure count.

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_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 [of authorized administrator].

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

5.1.1.6 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 suite of tests *during initial start-up, periodically during normal operation, at the request of an authorised user, {None}* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_RPL.1 Reply detection

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [{Authentication of the counterpart}]

FPT_RPL.1.2 The TSF shall perform [{prevention of reattempts and generation of audit records }] when replay is detected.

Application Notes: The entity may be a message, service request, service response, or session. As a response to the entity, the entity may be ignored.

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 are 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 the 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 Notes: The security functional requirements shall provide a time stamp that guarantees that audit data is generated in order and in relation to the security audit function.

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 authorised user,* [None] to demonstrate the correct operation of the TSF. operation of *the TSF*.

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

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

FPT_TST.2 TSF Data integrity error handling

Hierarchical to: No other components.
Dependencies: FPT_TST.1 TSF testing

FPT_TST.2.1 If an TSF data integrity error is detected, TSF shall handle it as follows.

a) Notification to Authorized Administrator
b) [{Audit Record}]

5.1.1.7 TOE access (FTA)

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication*
* - [VPN_PP_V1.1] selected FIA_UAU.2 which has a hierarchical relationship with FIA_UAU.1 so that this Security Target adopted FIA_UAU.2.

FTA_SSL.1.1 The TSF shall lock the session of **the authorized administrator** after [{authorized administrator idle time (default: 1 minute)}] by:

a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 .The TSF shall require the following events to occur prior to unlocking the session: [{re-identification and authentication}].

Application Notes: In the security functional requirements, a user means an authorized administrator.

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive **authorized general users** session after a [{the following Idle time of **authorized general users** set by the administrator (default: None)}].

a) When an authorized general user using a proxy crosses the threshold of the corresponding proxy

5.1.1.8 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 initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [remote management function, {None}].

5.1.2 Author-augmented Security functional requirements (SFR)

The Security functional requirements referred to by this Security Target consists of the SFR components specified in Protection Profile Type 2. For the security functions provided by the TOE but not included in the protection profile, the author can add them by referring to the Common Criteria for the information protection system.

[Table 5-3] Augmented Security Functional Requirements

Security Function Class	Security Function Component	
Security Management	FMT_SMF.1*	Specification of management functions
Privacy	FPR_UNO.4	Authorized user observability

* FMT_SMF.1 is based on 'Common Criteria (CC) V2.2 Final Interpretation, October 2005.'

5.1.2.1 Security Management (FMT)

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 security management functions [as follows]:

a) TSF function management and security attribute management – Specified in FMT_MOF.1.
b) TSF data management – Specified in FMT_MTD.1.
c) TSF Data (Configuration Data) backup and recovery
d) Upgrading of the TOE

5.1.2.2 Privacy (FPR)

FPR_UNO.4 Authorized user observability

Hierarchical to: No other components.
Dependencies: No dependencies.

FPR_UNO.4.1 The TSF shall provide the [authorized administrator] with the capability to observe the usage of [traffic at each interface of the TOE, packet filtering, network address translation, and VPN tunnel, logged-in user].

5.1.3 Deleted Security functional requirements(SFR)

The deleted security functional requirements shown below use components with a hierarchical relationship so they are not used again: FIA_UAU.1 Authentication – FIA_UAU.2 with a hierarchical relationship was selected in the VPN protection profile.

5.2 TOE security Assurance Requirements

This paragraph selectively provides augmented assurance requirements (in bold characters) which conform to the EAL 3 grade of the Common Criteria for the information protection system and EAL 3+ grade defined by a local (Korean) certificate agency. The augmented assurance 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

[Table 5-4] EAL 3+ Grade Assurance Requirements List

Assurance Class	Assurance Component	
Configuration management	ACM_CAP.3	Authorisation 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
	AGD_USR.1	User 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**

5.2.1 Configuration Management

ACM_CAP.3 Authorisation 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 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 authorised changes are made to the configuration items.

<Evaluator action elements>
ACM_CAP.3.1.E 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 Authorisation controls

<Developer action elements>
ACM_SCP.1.1D The developer shall provide a list of 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 evidence 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.

5.2.2 Delivery and Operation

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 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 procedures necessary for the secure installation, generation, and start-up of the TOE.

<Content and presentation 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.

5.2.3 Development

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 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 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 subsystems.
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 the 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
ADV_TAT.1 Well-defined development tools

<Developer action elements>
ADV_IMP.2.1D The developer shall provide the 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 provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined 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.

5.2.4 Guidance documents

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 administrative personnel.
Content and presentation of evidence elements:

<Content and presentation of evidence elements>
AGD_ADM.1.1C The 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 behaviour 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 relative to the 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.

AGD_USR.1 User guidance

Dependencies: ADV_FSP.1 Informal functional specification

<Developer action elements>
AGD_USR.1.1D The developer shall provide user guidance.

<Content and presentation of evidence elements>
AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

<Evaluator action elements>
AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Life Cycle Support

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

<Developer action elements>
ALC_DVS.1.1D The developer shall produce development security documentation.

<Content and presentation 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 evidence.
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 TSF Subset of the implementation 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 implementation shall be well-defined.
ALC_TAT.1.2C The documentation of the 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.

5.2.6 Tests

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.1 Informal functional specification
ATA_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 coverage 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 coverage 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 design and low-level design.

<Evaluator action elements>

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

ATE_FUN.1 Functional testing

Dependencies: 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 evidence.
ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.7 Vulnerability Assessment

AVA_MSU.1 Examination of guidance

Dependencies: ADO_IGS.1 Installation, generation, 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 operation of the TOE (including operation following failure or operational error), their consequences and 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 the use of the guidance documentation allows all insecure states to be detected.

AVA_SOF.1 Strength of TOE function evaluation

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD1 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.

5.3 Requirements for IT Environments

Requirements for IT Environments are as follows:

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 initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [remote control, {None}].

Application Notes: The TOE calls the SSL function in the IT environment and provides a secure channel through the SSL protocol.

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 Notes: The TOE calls the time stamp server in the IT environment and manages the time sources in a secure manner.

FAU_SAR.3 Selective 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 and sorting* of audit data based on[{standard for following logical relations}].

e) Audit record type – System logs, firewall logs, session logs, proxy session logs
f) System log – Time, host IP Address, priority, process, message content (Detailed information: keyword)
g) Firewall/session log – Time, host, source/destination IP Address, protocol, source/destination port, ICMP type, service, size, operation (ACCEPT/DROP/REJECT/OPEN/CLOSE))
h) Proxy session log – Time, host IP Address, source/destination IP Address, User, service, operation (OPEN, CLOSE)

Application Notes: The TOE calls SQL-Life, an external DBMS, in the IT environment and manages the audit record storage in a secure manner.

6 TOE Summary Specification

This chapter describes how the TOE provides security functions and assurance measures to meet the assurance and security requirements of the TOE.

6.1 Assurance Measures

The assurance measures for the assurance requirements specified in this Security Target comply with the assurance requirements specified in Part 3 of the Common Criteria for the Information Protection System. [Table 6-1] shows the list of documents that can verify compliance with the assurance requirements.

[Table 6-1] Assurance Requirements and Assurance Documents

Assurance component	Assurance Component	Assurance Document
ACM_CAP.3	Authorisation controls	Configuration Management Document
ACM_SCP.1	TOE CM coverage	Configuration Management Document
ADO_DEL.1	Delivery procedures	Delivery documents
ADO_IGS.1	Installation, generation, and start-up procedures	Installation Guide
ADV_FSP.1 ADV_RCR.1	Informal functional specification Informal correspondence demonstration	Functional Specification
ADV_HLD.2 ADV_RCR.1	Security enforcing high-level design Informal correspondence demonstration	High-level Design
ADV_IMP.2 ADV_RCR.1	Implementation of the TSF Informal correspondence demonstration	Implementation Specification
ADV_LLD.1 ADV_RCR.1	Descriptive low-level design Informal correspondence demonstration	Low-level Design
AGD_ADM.1	Administrator guidance	Administrator Guidance documentation
AGD_USR.1	User guidance	User Guidance documentation

ALC_DVS.1	Identification of security measures	Development Security Document
ALC_TAT.1	Well-defined development tools	Development Tool 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	Test Document
AVA_MSU.1	Examination of guidance	Administrator and User Guidance Documentation
AVA_SOF.1	Strength of TOE security function evaluation	Vulnerability Analysis Report
AVA_VLA.2	Independent vulnerability analysis	Vulnerability Analysis Report

6.2 TOE Security Function

Description of TOE Security Function (TSF) includes how each TSF conforms to the corresponding security functional requirements. This paragraph includes descriptions of each security function and explains how each security function meets the corresponding requirements.

6.2.1 Security Audit (FAU)

6.2.1.1 Security Alarm (FAU_Alarm)

FAU_Alarm.1 When an audit record of the corresponding priority set by the administrator occurs, the TOE will send a warning message to the administrator. If an audit record crossing the priority set by the administrator occurs, details of the corresponding audit record will be sent to the administrator's e-mail address and display the "Unconfirmed important audit records" message will be displayed on the security management screen of the authorized administrator's PC.

FAU_Alarm.2 The TOE includes a potential violation analysis based on the priority of the audit record. If an event such as "identification and authentication security policy violation", "cryptographic operation failure," or "access control rule violation", which can be considered as potential threats, occurs, the priority level of the warning or error will be sent to the authorized administrator with the corresponding audit record. In case of a user authentication failure in the TOE, an alarm will be sent to the administrator as the identification and authentication security policy violation. In case of a

cryptographic operation failure when the cryptographic packet sent by the user through the IPSec protocol is not valid, an alarm will be sent to the administrator. To send an alarm (an e-mail to the administrator) for a packet dropped (by rule violation, not the rejection policy), set "log" in the packet-filtering policy so that the "dropped" packets and the corresponding audit records will be informed to the administrator. This process can be summarized as follows:

- Identification and authentication security policy violation – Audit records failed in authentication and identification. Audit records crossing the priority.
- Cryptographic operation failure – When the cryptographic packet sent by the user through the IPSec protocol is not valid.
- Access control rule violation – When a packet dropped by the packet-filtering policy selects an audit record.

6.2.1.2 Audit Records Generation (FAU_Audit)

FAU_Audit.1 The TOE stores audit records generated in VForce 1700 V1.0 S/W and VForce 1700 V1.0 S/W where the security function operate to protect user data on the network. The TOE can also search the stored audit records, generate statistical data, and report these items to the administrator. VForce 1700 V1.0 generates audit records for operations of all security functions. When the TOE generates audit records, the event occurrence time, audit record data, and the subject identity (user, source IP address, or the process that generated the audit record) will be also generated. Each audit record contains similar information depending on the audit record type. For consistency of the event occurrence time, the TOE can use trusted time through the NTP protocol.

- System Log – Time (month, day, hh:mm:ss), priority, program, contents
- Access Control Log – Time (month, day, hh:mm:ss), processing (accept/drop/reject), prefix (audit records prefix to identify packet audit records, IN (inbound), OUT (outbound), source, destination, protocol, SPORT, DPORT, TYPE (ICMP), CODE (ICMP)
- IPSec packet Log – Time (month, day, hh:mm:ss), priority, contents

FAU_Audit.2 Audit records created by TOE are categorized as shown below:

[Table 6-2] Audit Record Types and Description

Audit Record Type	Audit Record Result and Contents	Included Functional Components Required by FAU_GEN
System	Audit records are classified into audit records	FAU_ARP.1, FAU_SAA.1,

Log	generated in the system, session opening/closing information, and proxy-related audit records. Then, audit records related to starting and stopping of the process responsible for the audit function are created. The system Log identifies the security breach type according to the definition in FAU_Alarm.2 and, audits and records the responses (mail sending.) All of the administrator's security management activities and new security attributes are audited and recorded. If a security setting fails due to an internal security problem, this event will be included in the important audit records so that the event is audited and stored. Audit records related to identification and authentication are classified as system Log which include success or failure of identification and authentication in the TOE.	FAU_SEL.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2, FMT_MSA.1, FMT_MSA.2, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FPT_SMR.1, FPT_STM.1, FPT_TST.2, FTA_SSL.1, FTA_SSL.3, FTP_ITC.1, FMT_MOF.1,FMT_SMF.1,FPR_UNO.4
Access Control Log	Audit records created by the packet-filtering security policy rules. These audit records contain the processing result of the packet data and the audit records generated in the IKE process that is executed to connect the VPN. The audit records for success and failure in each phase or key generation phase of the IKE process are included. Details about processing result (accept, drop, or reject) generated by the packet-filtering policy are also included.	FDP_ACF.1, FDP_IFF.1,FPR_PSE.1
IPSec Packet Log	Encoding/decoding packets through the VPN IPSec interface and event priority and message contents (details) are recoded. The IPSec Packet Log includes the audit records related to the success/failure of encryption.	FCS_COP.1, FDP_DAU.1

FAU_Audit.3 The above audit records have the following priorities:

- Emergency: Audit record that has critical influence on the TOE.
- Alert: Audit records that must be immediately modified.

- Critical: Audit records that must warn of a dangerous situation related to storage media.
- Error: Audit records that may produce an unexpected result
- Warning: Audit records subject to warning
- Notice: Audit records that do not produce an unexpected result but may need special action.
- Information: Audit records for general activities made in the TOE.
- Debug: Audit records concerning debugging messages in the subsystem (or process) that is responsible for the security functions in the TOE.

FAU_Audit.4 VForce 1700 V1.0 S/W can select whether to create an audit record for each packet-filtering policy set by the administrator. (The selection choices include None, New Connection, and All.) In particular, to prevent overload caused by multiple audit records for the same event, the TOE can limit the number of audit records for the corresponding policy created per time unit. If the administrator selects "New Connection" or "All," the administrator will be required to select the average and the maximum number of audit records created by the corresponding security policy per second.

6.2.1.3 Prevention of Loss of Audit Records (FAU_Prevent)

FAU_Prevent.1 Only the authorized administrator can access and manage audit records generated and managed by the TOE so that a general user or an unauthorized user including a third party cannot search, change, or delete audit records. Even the authorized administrator cannot access the file system of the TOE. The console shell supports only basic installation commands so that even an authorized administrator cannot access the file system that stores audit record data. Only the corresponding process executing the security function can access the audit record data files. There are no accounts that can access the TOE through a network. The administrator can manage the file system only by accessing the console.

FAU_Prevent.2 The TOE checks the available storage media space of the file system every hour. VForce 1700 V1.0 manages free space in two ways – "Warning" and "Suspension." If the free space is less than 10% (changeable by the administrator) of the total file system space and audit records may be lost, the following warnings will be generated for the administrator as primary measures:

- Corresponding audit records
- Notification of occurrence of important audit records through a warning e-mail or a message box

FAU_Prevent.3 When the free space is 5% (changeable by the administrator) of the total file system space which is subject to "Suspension", an alarm mail will be sent to the administrator and all services of the TOE will be suspended to prevent events subject to audit records as secondary measures. In other words, the authorized administrator will be allowed only to access the security management functions of the TOE and all packet-filtering operations will be suspended.

6.2.1.4 Viewing Audit Records (FAU_View)

FAU_View.1 The TOE allows the authorized administrator to view audit records generated in the TOE on the security management screen. (through web UIs.) Before the audit records generated in VForce1700 are sent to the NexG log server, they are stored in memory as long as memory space allows so that administrators can view stored audit records. VForce1700 provides a security management screen so that the authorized administrator can view audit records by audit record types shown in [Table 6-1]. The authorized administrator can check the audit records according to the creation time of the audit records on the security management screen.

FAU_View.2 The audit records created in VForce1700 are transmitted to and stored on the NexG log server in real time so that an authorized administrator can view the audit records on the security management screen in real time. In other words, in VForce1700, the administrator can search audit records that are stored in the available memory space based on FIFO. However, if audit records created in VForce1700 are transmitted to the NexG log server in real time, the administrator can view real-time audit records and search audit records in the log server's disk by specifying the search conditions.

FAU_View.3 After receiving audit records from VForce1700, for easier search, the NexG log server classifies these records into several types including those classified by VForce 1700:

[Table 6-3] Audit Record Types

NexG Log Server Classification	VForce1700 Classification
System log	System Log IPSec packet Log
Firewall log	Access Control Log
Session log	System Log
Proxy session log	System Log

FAU_View.4 The NexG log server can search and sort audit records according to the "log server classification" Upon the administrator's request, the NexG log server can search the audit records based one of the following conditions and display the search result on the security management screen of the log server. Upon the search request of the administrator, the log server sends queries to the DB where the audit records are stored and displays the query result:

- System Log – Audit record creation time, IP address of the host which generated the audit records, Process which generated the audit records, contents of the audit record (Details: keyword)
- Firewall/Session Log – Audit records creation time, IP address of the host which generated the audit records, Source/Destination IP address, Protocol, Source/Destination port, ICMP type, Service, Packet size, Processing result (accept, drop, reject, open, and close)
- Proxy Session Log – Audit records creation time, IP address of the host which generated the audit records, Source/Destination IP address, User ID, Service, Processing result (open, and close)

6.2.1.5 Security Functional Requirements (SFR) Mapping:

- FAU_APR.1
- FAU_GEN.1
- FAU_SAA.1
- FAU_SAR.1
- FAU_SAR.3
- FAU_SEL.1
- FAU_STG.1
- FAU_STG.3
- FAU_STG.4

6.2.2 Cryptographic Support (FCS)

6.2.2.1 Cryptographic Key Management (FCS_IKE)

FCS_IKE.1 Key exchange is made through the use of the IKE. IKE uses ISAKMP which defines how to establish a service for key exchanges. The IKE of the TOE consists of two phases for secure key exchange. In the first phase, the SA is established, and in the second phase, the IPSec SA is established and a secret key is generated for IPSec communication using the SA established in the first phase.

FCS_IKE.2 The TOE generates, installs, and manages cryptographic keys for cryptographic support. Cryptographic keys supported by the TOE are divided into symmetric keys created by the Digital Signature Algorithm (DSA) algorithm and asymmetric keys created by the Rivest-Shamir-Adieman (RSA) algorithm. Symmetric keys create an algorithm and a secret key as defined based on the pre-shared key defined by the administrator. RSA keys are directly created through the CA or a certificate can be issued by a trusted CA after a certificate issuance request is made. At this time, the RSA authentication key creation function supports 1024 bits and 2048 bits as the key length.

FCS_IKE.3 The IPSec that processes the IP packets uses the SA. When an outbound or inbound packet occurs, an SA will be established to apply the cryptographic policy to the corresponding packet. If there is no SA, key exchange will be made to establish a secure SA with the TOE. The TOE automatically exchanges keys with the gateway on a regular basis to use new secret keys. The IKE of the TOE uses the ISAKMP that defines how to establish a key exchange-based security service. Authenticated keys as a result of the IKE and the authentication keys with the security parameters of the IPSec SA will be created. The key exchange policy will support main and aggressive modes.

6.2.2.2 Key Destruction Management (FCS_KEYDEST)

FCS_KEYDEST.1 If the key is expired during encrypted communication after the key exchange process, the IKE daemon will destruct the cryptographic keys of the TOE and the counterpart gateway, register the certificate revocated in the key exchange process in the Certificate Revocation List (CRL) of the TOE, and update keys. When a cryptographic key used in the security tunnel is destructed, the TOE will set the data (file) with the corresponding cryptographic key stored as “0” and delete data related to all cryptographic keys to prevent the old cryptographic key from remaining in resources (such as memory.)

6.2.2.3 ESP Support (FCS_ESP)

FCS_ESP.1 The TOE generates, distributes, and destruct secret keys related to encryption for safe transmission of the user data through the IPSec ESP protocol. The TOE also supports functions related to the cryptographic operations. The TOE provides the following encryption algorithms:

- **AES:** AES is being recognized as the new encryption algorithm standard. It is being widely applied to the Internet backbone structure and is highly interoperable. Key lengths include 128, 192, and 256 bits.
- **3DES:** An alternative to supplement the short key length of 56 bits of DES. 3DES iterates DES three times using three keys. Although 3DES is three times slower than DES, it has been adopted by various standards because it can be easily implemented and provides higher reliability. The key length is 168 bits.
- **SEED:** An encryption algorithm that has a block size of 128 bits and supports 128-bit key size. SEED is an encryption algorithm for Korea developed by the Korea Information Security Agency (KISA).

FCS_ESP.2 The encryption key length created by the TOE is minimum 128 bits. Depending on the selected encryption algorithm, the key length is determined (AES: 128, 192, or 256 bits; 3DES: 192 bits; SEED: 128 bits).

FCS_ESP.3 When the TOE establishes encrypted communication with its counterpart using ESP, the TOE supports both encryption and integrity of the data (packets.) For this purpose, the TOE provides the following integrity algorithm:

- **HMAC-SHA-1-96**: The SHA-1 algorithm is based on the HMAC algorithm. The HMAC algorithm provides a framework for using a hash algorithm like SHA-1. The HMAC-SHA-1-96 algorithm has a block size of 64 bits. This algorithm supports a key length of 160 bits, or stores only the first 96 bits in the ESP. Upon verification of the data, this algorithm generates 160 bits and verifies the first 96 bits.
- **HMAC-HAS-160**: The HAS-160 algorithm is based on the HMAC algorithm. The HMAC algorithm provides a framework for using a hash algorithm like HAS-160. HAS-160 uses a dedicated hash algorithm. It can perform paste, division, and iteration operations. It handles message input in 512-bit blocks and displays data as 160 bits.

FCS_ESP.4 The TOE provides functions which can authenticate the counterpart and detect replay of the authenticated account in order to prevent packet hijacking by using an SA, authentication, and a sequence number when the TOE is connected to a VPN gateway.

6.2.2.4 AH Support (FCS_AH)

FCS_AH.1 The TOE verifies the integrity of the data (packets) for secure data transmission using the IPSec AH protocol. To establish secured communication using the AH, the TOE provides an integrity algorithm as follows:

- **HMAC-SHA-1-96**: The SHA-1 algorithm is based on the HMAC algorithm.. The HMAC algorithm provides a framework for using a hash algorithm like SHA-1. HMAC-SHA-1-96 algorithm has a block size of 64 bits. This algorithm supports a key length of 160 bits, or stores only first 96 bits in the ESP. Upon verification of the data, this algorithm generates 160 bits and verifies the first 96 bits.
- **HMAC-HAS-160**: The HAS-160 algorithm is based on the HMAC algorithm.. The HMAC algorithm provides a framework for using a hash algorithm like HAS-160. HAS-160 uses a dedicated hash algorithm. It can perform paste, division, and iteration operations. It handles message input in 512-bit blocks and displays data in 160 bits.

6.2.2.5 Security Functional Requirements (SFR) Mapping:

- FCS_COP.1
- FCS_CKM.1
- FCS_CKM.2
- FCS_CKM.4

6.2.3 User Data Protection (FDP)

The packet-filtering engine and the proxy engine of the TOE control all traffic accessing the network according to the security policy predefined by the administrator. The packet-filtering engine and the proxy of the TOE firstly filters the packets at Layer 3 and decides whether to allow, reject, or forward the packets based on information included in the packet header. The access control methods of the TOE include Mandatory Access Control (MAC) that uses the security labeling information of each object added by the administrator as well as Discretionary Access Control (DAC) described earlier.

6.2.3.1 Packet-filtering (FDP_PacketFiltering)

FDP_PacketFiltering.1 Packets that do not go through the VPN of the TOE shall pass the packet-filtering policy of the TOE. The packet-filtering security policy of the TOE decides whether to accept, reject, or drop the packet based on the security object and information contained in the IP header. If the security attribute is proper, the packet will be forwarded or accepted. If a packet is rejected, a reply will be sent using an ICMP error message and the packet not conforming to the corresponding policy will be dropped. If a packet is dropped, no message reply will be generated.

- Source and destination IP Address – Network object and group, source/destination network IP address of the IP header
- Port no. – Service object, IP header port address
- Time (Time object)

FDP_PacketFiltering.2 If the administrator has not set any packet-filtering security policy, the default policy will be used and drop all packets. If none of the security policies set by the administrator is proper for a packet passing through the TOE, the packet will be dropped. In other words, all packets not specified in the policy will be dropped.

FDP_PacketFiltering.3 The TOE shall map each interface where the packet comes or goes with the corresponding policy to apply the packet-filtering policy. When mapping them, the TOE can determine the order of the policies. When the packet comes in or goes out through the interface, the TOE matches the packets in order of packet-filtering security policies mapped with the interface and decides whether to accept, reject, or drop the packet.

FPT_Packetfiltering.4 To protect from interference and intrusion of an unreliable subject during packet filtering, network address translation, and access control, the TOE separates TSF data and code from external entities and separates the subjects in the TSC. This function is executed by the OS function of the sub-abstract machine.

6.2.3.2 Proxy (FDP_Proxy)

FDP_Proxy.1 The TSF that the TOE executes requires an entity which uses HTTP or SOCKS5 protocols for information exchange through the TOE. The TSF controls access and information flow by filtering packets at the network layer level, and determines the maximum connection count and the session time-out for HTTP and SOCKS5 sessions.

FDP_Proxy.2 The proxy of the TOE provides user authentication and session limit functions together through a single integrated daemon. Therefore, the proxy can apply the user authentication function for the HTTP and the SOCKS5 protocols that support user authentication. To use the user authentication function in the TOE, the administrator shall connect the proxy time object to each user group that the administrator sets in the security management. Only connected users can be authenticated by the unique (HTTP, SOCKS5 (TELNET, FTP)) proxy security policy of the proxy.

FDP_Proxy.3 When HTTP or SOCKS5 (TELNET or FTP) proxy is used as the default policy of the proxy in the TOE, the policy can be decided by the following common security attributes:

- Proxy operation status
- Input interface: Determines the interface to bind the corresponding port of the proxy.
- DNS cache: Caches DNS names used in the proxy as many as set by the administrator and reduces repetitively occurring DNS traffic to maintain the proxy rate consistent.
- Proxy protocol: Sets HTTP and SOCKS5 protocols. Uses HTTP protocol for the HTTP and SOCKS5 for FPT and TELNET. According to the characteristics of the protocol, only the HTTP protocol and SOCKS5 protocol supports user authentication.
- Maximum connection count (1~65535): Determines the number of sessions to pass through the proxy.
- Session time-out (1~65535): Determines session time-out. If no data exchange occurs during the determined time, the corresponding session will be disconnected.
- Proxy time group: Same concept as “time object” in the packet-filtering security policy. The time group can be set only in the proxy.

FDP_Proxy.4 The TOE allows the administrator to disconnect a user if the user was forcibly authenticated in the proxy session through HTTP or SOCKS5. If the disconnected user wants to establish communication through HTTP or SOCKS5, the user shall be authenticated in the TOE. FPD_Proxy.3 can automatically disconnect users by “session time-out.” In other words, if there is no traffic passing through the proxy after the user was authenticated, the user will be disconnected after the defined time set by the administrator.

FDP_Proxy.5 The TOE performs security-level based mandatory access control for users through the proxy. If the user passes through the proxy using an application which uses HTTP or SOCKS5 protocol, the TOE will perform mandatory access control. If the user tries to access an external network through an application, the TOE will compare the security level of the authenticated user with the security level of the network object that the user tries to access. Only when user security level is the same as or higher than the security level of the network object, the user will be allowed to access. Otherwise, user access request will be denied by security level. For this purpose, the administrator shall define the proxy network object and give it a security level. The administrator is also required to map the proxy network group with the corresponding user group and allow the user to access the proxy network.

6.2.3.3 Encrypted Data Transmission (FDP_VPN)

FDP_VPN.1 To establish a secure connection between two or more networks using a public network (for example, the Internet), the TOE creates an IPSec-based virtual tunnel and establishes encrypted communication between two or more trusted sub-networks. All data transmitted through the TOE is encoded, decoded, and hashed, and for this purpose, the TOE supports confidentiality algorithms such as 3DES, SEED, and AES, and the integrity algorithms of HAS-160 and SHA-1. For the IKE, the TOE supports the aggressive and main mode.

FDP_VPN.2 The TOE selects the IPSec protocol for encrypted communication with the gateway using the SA determined by the VPN security policy. If a packet is altered by a third party during IKE procedure or encrypted communication by the ESP protocol, the TOE drops the packet to guarantee integrity for data transmission and authentication. At this time, the TOE provides SHA-1 and HAS-160 algorithms on ESP.

FDP_VPN.3 Packets destined for the encryption policy network defined in the VPN policy among the packets passing through the TOE are encrypted according to the VPN policy set by the administrator before being transmitted. If the packing going through the VPN interface is not part of the network communication defined in the VPN security policy, the packet will be handled according to the packet-filtering policy. Even after the packet passes through the IPSec interface, the TOE applies a normal packet-filtering policy instead of the encryption policy. The administrator defines the security policy of the VPN on the security management screen using the following attributes:

- IPSec binding interface: Applies the VPN security policy only to the packets passing through the corresponding interface.
- Shared key: Used to exchanges keys with the counterpart and create cryptographic keys. The shared key is the string seed that both communication parties share.
- Security protocol: Determines ESP protocol or AH protocol during IPSec communication.
- Key exchange mode: Determines the main mode or aggressive mode for IKE key exchange.
- Authentication method: Determines whether to use the shared key or a predefined certificate for the key exchange for the security tunnel (SA).

- Subject security attribute: IP addresses of the communication subject and the counterpart. Certificate subject.
- ISAKMP policy: Determines the encryption method. Determines the cryptographic algorithm, the key length, and the valid period for phase-1 cryptographic key (SA) of the IKE.
- IPSec policy: Determines the encryption and the authentication methods. Determines encryption and authentication algorithms, the key length, and the valid period for phase-2 cryptographic key (SA) of the IKE.
- VPN network IP address: Determines the IP addresses of the internal networks of the encrypted communication counterpart and the local VPN gateway. Packets are encoded and decoded through the IPSec binding interface according to the predefined policy only for the communication between the defined IP addresses.
- PFS group – Determines how to generate the VPN security tunnel (SA) and regularly create cryptographic keys of the security tunnel. PSF group number 2 or 5 is selected here, and the group numbers are Deffie-Hellman group numbers.

FDP_VPN.4 The TOE and the counterpart start to exchange keys when both sides determine all VPN policies. The TOE determines the VPN policy later and becomes the initiator and starts to exchange keys for the security tunnel (SA). An SA automatically expires when there is no inbound/outbound packet through the SA, Dead Peer Detection (DPD) or . an error occurs in the network environment (disconnection in the network.).

6.2.3.4 Network Intrusion Detection (FDP_NID)

FDP_NID.1 The TOE inspects traffic passing through the packet-filtering security policy, and stores audit records for the abnormal packets. The administrator identifies abnormal packets by the access control audit record prefix (delimiter that identifies audit records):

- Detects the port scan for the traffic applied to the packet-filtering security policy, and generates audit records and mail to the administrator.
- Detects fragmented packets for packets applied to the packet-filtering security policy, and generates audit records and mail to the administrator.

6.2.3.5 Administrator Access Control (FDP_AdminNetwork)

FDP_AdminNetwork.1 When an administrator with identification and authentication data (for example, ID and password) or with a trusted administrator network address tries to access the TOE from a remote place, the TOE explicitly allows information flow. When an authorized administrator tries to access the security management screen, the TOE checks whether the source IP address belongs to the administrator network. If the administrator is from an allowed administrator network, the TOE will display the security management login screen for the administrator. Then, the administrator shall input the ID and the password to be authenticated in order to log in to the security management screen. At this time, the TOE authenticates and identifies the user based on the administrator accounts and passwords of the administrator group. If a user tries to log in with an account not in the administrator group, the TOE will consider the user is not an authorized administrator, deny the login attempt, and generate the audit records.

FDP_AdminNetwork.2 The administrator can directly access the console using the RS-232 console cable other than the Internet browser. When the machine is first installed in the network or the machine is initialized, the user shall access the console to set the network IP. Like when using the web interface, the administrator shall input the ID and the password to access the console. After the machine is first installed, the network will be set up and the administrator account (admin) will be added. The administrator account becomes the default account.

6.2.3.6 Security Functional Requirements (SFR) Mapping:

- FDP_ACC.2
- FDP_ACF.1
- FDP_DAU.1
- FDP_IFC.1
- FDP_IFC.2(1)
- FDP_IFC.2(2)
- FDP_IFF.1(1)
- FDP_IFF.1(2)
- FDP_IFF.1(3)
- FPT_RVM.1
- FPT_SEP.1
- FPT_RPL.1

6.2.4 Identification and Authentication (FIA)

Identification and authentication is made in the TOE at these points:

- Before the administrator allows the user to access the security management interface (on the web) for security management.
- Before a general user uses a protocol (FTP, TELNET), that uses the web (HTTP), or SOCKS5 through the proxy.

The TOE performs identification and authentication as follows:

6.2.4.1 General Cryptographic Authentication (FIA_PwdAuth)

FIA_PwdAuth.1 When the administrator generates or changes a security policy related to user identification or authentication, the TOE will inspect the cryptographic verification mechanism. The following policy is provided to meet AVA_SOF.1 assurance requirements. A general password authentication mechanism is used to authenticate users and performs authentication based on the following collation rules:

- The password shall be of 7~16 digits.
- A total of 94 characters including special symbols (including a-z (26), A-Z (26), and 0-9 (10)) can be used. (Special Symbols: ! @ # $ % ^ & * ( ) _ + | ` - = \ { } : " < > ? [ ] ; ' , . / ")
- Collation rule: Alphanumeric or alphabetic characters with special symbols. (Alphabetic and numeric characters, or alphabetic and special symbols)

FIA_PwdAuth.2 A normal user's password automatically expires on a date predefined by the administrator. When the user accesses the network again, the user will be required to change the password.

FIA_PwdAuth.3 The TOE identifies and authenticates IT entities through the internal user management database and verifies general users and administrators. The TOE supports general passwords and one-time passwords. The authorized administrator can allow users to select a general password or a one-time password.

FIA_PwdAuth.4 After the user (all users in the TOE including administrators) is successfully authenticated, the user can use the security functions of the TOE. However, only the administrator can access the Security Management screen and use security management functions. General users are authenticated by the proxy and can use HTTP or SOCKS5 using the proxy defined in each proxy security policy. The TOE provides the authentication-feedback protection

function during the operation of authentication by hiding the password entered by the user (for example, using the "*" symbol.)

6.2.4.2 One-time Password Authentication (FIA_OTPAuth)

FIA_OTPAuth.1 The onetime password is used. There is a list of one-time passwords for the authorized administrator and users. When a user attempts to access the network using a one-time password, the user must input the ID and password corresponding to the sequence number displayed on the screen. However, if the user inputs an incorrect password three times, an additional process is required to allow the user to try to access. If an administrator or a general user loses the list of one-time passwords, the administrator shall be immediately informed and another list of one-time passwords shall be re-issued.

FIA_OTPAuth.2 The one-time password mechanism authenticates human users using characters. If created numeric (280) passwords are used up, the administrator shall be informed and new passwords shall be created. To create a one-time password, the TOE uses a prefix as a password. A prefix can be of 1~ 255 digits, and both the prefix and the one-time password shall be used together to authenticate a user.

6.2.4.3 Authentication Failure Handling (FIA_IAFailure)

FIA_IAFailure.1 Each user's authentication failure can be processed, and the failure record is stored with the user profile in the user DB. If the user authentication failure count exceeds the threshold set by the administrator, the session will be locked. In this case, until the authorized administrator restores the setting, the user status cannot be changed. The administrator can set the maximum authentication failure count. If the default is none, there will be no limit to the user's authentication failure count. If the user authentication failure count crosses the threshold, the TOE will reject the user's login. In this case, the user can log in only after the administrator changes the login setting.

FIA_IAFailure.2 Other counterparts than the user are also subject to the authentication failure count threshold. If a VPN gateway with a constant certificate subject (country, organization, organization unit, common name, or e-mail address) or a shared key tries to exchange cryptographic keys for the VPN security tunnel (SA), the authentication failure count applied to the IP address of counterpart. If the count exceeds the threshold, the VPN gateway will not able to exchange keys till the administrator modifies the gateway. The related audit records will be stored.

6.2.4.4 User Password Change (FIA_UPWDSet)

The TOE allows general users using a proxy service to access the TOE using HTTPS and to change passwords in their accounts.

6.2.4.5 Identification and Authentication Security Strength (FIA_SoF)

FIA_SOF.1, FIA_UAU.2, and FIA_UAU.4 conform to SOF-medium specified in the Common Criteria for the Information Protection System (Notice 2005-25 by the Ministry of Information and Communication) [1].

6.2.4.6 Security Functional Requirements (SFR) Mapping:

- FIA_AFL.1
- FIA_UAU.2
- FIA_UAU.4
- FIA_UAU.7
- FIA_UID.2
- FIA_SOS.1

6.2.5 Security Management (FMT)

6.2.5.1 Overview

Only authorized administrators can access the security management functions of the TOE through the identification and authentication processes, and only administrators can access TSF to restart or stop the TOE and change the security policy. The TOE verifies the password in addition to the login password using the management password to allow the user to access the Security Management screen.

Using the security management functions, the authorized administrator can set the TSF and define the TSP. To use a security management function, the administrator must be identified and authenticated and verified to determine if he has proper authority. Only the authorized administrator can add, change, or delete security policies using the security management functions after passing the identification and authentication processes. The authorized administrator can use TSF to restart and stop the TOE and operate the TOE.

For efficient security management the TOE provides web interfaces for the administrator and allows the administrator to access the network through Internet Explorer. The administrator browser accesses the TOE through SSL using the HTTPS protocol. The Security Management screen is implemented by HTML or CGI to set or receive security attributes by the administrator.. The TOE provides categorized security management functions as shown below and allows the administrator to efficiently manage security:

[Table 6-4] Security Function Management Interfaces

Higher Menu	Menu 1	Menu 2	Description
Object Definition	Certificate	CA Management	Manages the CA certificate and certificate requests when the TOE functions as a CA.
		Certificate Management	Manages own certificates.
	Network		Manages the network object.
	Service		Manages the service object.
	Time		Manages the time object.
	IPSec		Manages the IPSec object (ISAKMP policy, IPSec, and gateway policy.)
	User		Manages the user object.
Network	Overall Status	Traffic at Each	Shows traffic amount of the interface in

		Interface	Kbytes/second or packet/ second unit.
		Session	Shows the list of sessions passing the TOE.
	Interface	Overall Status	Shows interface information.
		Ethernet Interface	Sets Ethernet interfaces.
		PPP Interface	Sets the PPP interfaces.
	Routing	Overall Status	Shows current routing table of the TOE.
		Static Routing	Manages routing table.
	ARP		Shows and adds ARP.
	DHCP		Shows and sets the DHCP.
Access Control	Overall Status		Shows status of packet filtering, address translation, port forwarding policy, and redirect.
	Default Setup		Sets the default setting of the packet-filtering policy and the TCPMSS.
	Packet Filtering		Manages packet-filtering policy.
	NAT		Manages NAT policy.
	Port Forwarding		Manages port-forwarding policy.
	Redirect		Manages redirect policy.
	Proxy	Default Setup	Sets and manages proxy use status and protocol.
		Proxy Time Object	Manages proxy time object.
VPN	IPSec	Status	Shows the currently established SAs.
		Connection Setup	Manages the IPSec connection setting.
system	Cryptographic Change		Changes and manages the cryptograph in security management access.
	Login User		Shows login user in the TOE or the administrator.
	Host/Name Server		Manages host name of the TOE and the DNS name.
	Date/Time		Manages date/time of the TOE.
	SNMP		Sets the SNMP.
	Audit Records	Real-time system log	Shows system audit records in real time.
		Real-time firewall log	Shows firewall audit records in real time.
		Real-time session log	Shows session audit records in real time.
		Real-time proxy session log	Shows proxy session audit records in real time.

		Log search	Shows audit records.
		Log statistics	Shows audit record statistics.
		Backup	Backs up audit records.
		Policy	Sets environment for the audit records.
		Service setup	Sets service.
	System Management	Access control	Manages administrator policy.
		Firmware upgrade	Upgrades software of the TOE.
		System setup management	Changes and initializes security management, and backs up and restore TOE configuration.
		System restart/stop	Restarts or ends TOE.
	System Status	Integrity	Inspects and manages integrity.
		Status	Shows software version of TOE, operation time, and CPU load.

The TOE allows the administrator to add, change, delete, or search alarms. When the administrator inputs the alarm security policy attribute, the TOE will check whether the attribute already exists. If the attribute is not overlapping with an existing one, the TOE will create an alarm security policy using the security policy attribute entered by the administrator and add the alarm policy to the configuration data. The alarm security policy is activated as soon as it is added. If the administrator requests the TOE to change or delete a particular alarm policy, the TOE will change or delete the policy in the configuration data.

The TOE provides security management functions whereby the administrator can create, delete, or search cryptographic keys. The TOE provides the root CA creation function and the certificate request and management functions. The TOE reads the current authentication key and certificate list from the configuration data, displays them on the Security Management screen, and shows the downloading option. When the administrator inputs a command to delete the authentication key, the TOE will check whether the key is used in other VPN policies. If the key is not in use by the VPN policy, the TOE will delete the key and store the record in the certificate revocation list (CRL.) The authorized administrator can search or download this certificate drop list. The TOE can recreate and change cryptographic keys. After the TOE checks that the certificate created by the old cryptographic key is not valid, the TOE changes the cryptographic key.

The TOE selectively creates audit records for each event security level. The TOE can store generated audit record files or statistical data in the audit record management database and delete them or extract them as a file. The TOE reads the current audit record setting from the configuration data and displays it for the administrator. The selective audit record setting interface is Event Type—Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug—and the administrator can change the setting. After the administrator successfully inputs data, the TOE stores the security

attributes set by the administrator in the configuration data. The TOE reads the audit record setting option from the configuration data and stores the audit record data or statistical data in the audit record management database. The administrator can also extract the data as a file for secondary backup.

The TOE displays interfaces for the administrator to back up the configuration file. After selecting the configuration data to back up, the administrator at a remote PC can download the selected data using the HTTP protocol. The TOE launches a browser for the administrator to search a configuration file on the remote PC. When the administrator selects a configuration file, it will be overwritten in the configuration file stored in the TOE.

6.2.5.2 Security Object Management (FMT_Object)

The TOE provides security functions that can add, change, delete, and search security objects necessary for the security policy. The security objects (network, user, service, time, IPSec object) are used to establish all security policies of the TOE. Network, user, and IPSec include data that can be identified by network address, user ID, and IPSec certificate subject and the corresponding authentication data. The administrator can add, delete, or modify the identification and authentication data.

The administrator creates network objects that are required to perform mandatory access control for network groups and user groups and check the encryption status and integrity of the transmitted data. Service objects are used by the packet-filtering security policy and the proxy security policy to apply a certain service. The time object is used by the packet-filtering security policy and the proxy security policy, and the corresponding security policy is activated or deactivated according to the time object. The IPSec object is used by the VPN security policy.

Network Object Management (FMT_NetworkObj)
The TOE allows the authorized administrator to manage network object information (source and destination network addresses) required for setting the packet-filtering security policy used to control accesses and information flows. The authorized administrator can search, add, modify, or delete network object information (source and destination network addresses) using the network object management functions.

Service Object Management (FMT_ServiceObj)
The TOE allows the authorized administrator to manage service object information (such as protocol and port) necessary for setting the packet-filtering policy used to control accesses and information flows. The authorized administrator can search, add, modify, or delete service object information (such as protocol or port) using the service object management functions.

Time Object Management (FMT_TimeObj)

The TOE allows the authorized administrator to manage time object information (time and date) required for setting the packet-filtering security policy used to control accesses and information flows. The authorized administrator can search, add, modify, or delete time object information (time and date) using the time object management function.

IPSec Object Management (FMT_IPsecObj)

The TOE allows the administrator to define and manage objects required for IPSec tunnel establishment to set the VPN security policy for functions such as access control, information control flow, and cryptographic support. The IPSec objects that the TOE provides include "ISAKMP policy object" in the key exchange phase such as authentication of the counterpart and key exchange before the establishment of a tunnel, "IPSec policy object" that defines encryption and integrity protocols that the ESP protocol uses for the establishment of the tunnel, and the "gateway object" that defines the gateway which will use IPSec. The administrator can search, add, modify, or delete IPSec objects using IPSec object management functions.

User Object Management (FMT_UserObj)

The TOE provides functions which define and manage user object information (ID, password, authentication method, and other) to set the administrator and user security authentication policy used for user identification and authentication. The authorized administrator can search, add, modify, or delete user object information (ID, password, authentication method, and other) using the user object management functions.

TOE users include administrators, general users, and counterpart VPN gateways. When defining a user attribute of the administrator, the TOE generates a general user, which is included in the default administrator group (admin group.) Therefore, the user attribute of the administrator is same as the security attribute of the administrator group. The administrator group refers to a group of general users in the administrator mode. Therefore, users in the TOE have the following security attributes:

- Security label: All users in the TOE have a security label.
- User: User ID, Group, Use status (by the current user), Password type (normal or one time), password, and Password Authentication Protocol (PAP) which is used for the authentication in the PPP server through the PPP interface that TOE supports; Challenge Handshake Authentication Protocol (CHAP) which prevents disclosure of the user name and password through challenge and reply process; Login failure count; Login permission; Last login time; and Duration.
- User group: User group ID, Maximum attempt limit, Proxy use status (Proxy time object per user group), Administrator mode status (The administrator group is in administrator mode, and in the default state, only the admin group has the admin user ID, which can be changed by the administrator), and associated user IDs.
- VPN gateway – X.509-type certificate subject, and gateway network IP address

Certificate Object Management (FMT_CertObj)

The TOE provides functions which can define and manage certificate objects required for using RSA-based keys. The authorized administrator can add, modify, or delete the certificate issuance request using the certificate object management function.

CA Object Management (FMT_CAObj)

The TOE provides the CA management function as a CA by issuing a certificate with local keys and managing issued certificates. The authorized administrator can create (drop, recreate) and view the root CA certificates using the CA management function, and can download the certificate file (cacert.crt).

Proxy Time Object Management (FMT_ProxyTimeObj)

The TOE defines proxy time objects besides time objects. The administrator can set the proxy time objects in the same way as defining the time objects. The proxy time objects are mapped with the user group for the authentication of a special proxy.

Proxy Network Object Management (FMT_ProxyNetObj)

The TOE defines proxy network objects separately from network objects. The administrator can set proxy network objects in the same way as defining network objects. The proxy network object is mapped with the user group for the authentication of a special proxy.

6.2.5.3 Security Policy Management (FMT_Policy)

Access Control Setting Management (FMT_ACDefaultPolicy)

Access control policies of the TOE include the packet-filtering security policy, network address translation policy, port forwarding policy, redirect policy, and proxy security policy. The TOE provides a default for each of these policies. The administrator can set a default policy for access control and apply the default policy to all access control activities. The default access control policy usually covers basic policies related to packet-filtering security and audit records.

Packet-filtering Policy Management (FMT_PacketFilterPolicy)

The TOE allows the administrator to add, change, delete, or search packet-filtering security policies using the security management functions. The TOE checks whether the attribute of the packet-filtering security policy entered by the administrator overlaps with an attribute of an existing policy. If it does not overlap with an existing one, the TOE will create a packet-filtering security policy based on the attribute of the security policy entered by the administrator. The new security policy is not directly applied to the TOE. Instead, it is mapped with the interface before being applied. When an existing packet-filtering policy is deleted or changed, the deletion will be applied immediately but the change will be applied after the administrator saves the new setting.

Network Address Translation Policy Management (FMT_SourceNATPolicy)

The TOE provides security management functions to add, change, delete or search network address translation security policies. The TOE allows the administrator to create a network address translation policy. The TOE checks whether the network address translation policy inputted by the administrator overlaps with an existing one. If the policy does not overlap with an existing one, the TOE will add the network address translation policy to the security policy. A new policy is immediately applied but not stored till the administrator saves it. When the administrator changes or deletes a certain network address translation policy, the TOE will immediately change or delete the corresponding policy in the configuration data.

Port-forwarding Policy Management (FMT_DestNATPolicy)

To control accesses and information flow, the TOE provides a function for setting the port-forwarding (DNAT) security policy. The administrator can search, add, modify, or delete the port-forwarding security policies using the port-forwarding policy management functions. Based on created object information, the TOE creates a security policy. If information overlaps with existing information and a validity error occur, the administrator will be immediately informed through a message box. Otherwise, the policy will be immediately added.

Redirect Policy Management (FMT_RedirectPolicy)

The TOE provides functions to establish a redirect security policy to control accesses and information flow. The administrator can search, add, modify, or delete redirect security policies using the redirect policy functions. Based on created network and service object information, the TOE creates a security policy. If information overlaps with existing information and a validity error occur, the administrator will be immediately informed through a message box. Otherwise, the policy will be immediately added. The added policy is applied to the network only after the administrator maps the policy with the corresponding network interface. The administrator can modify or delete existing policies. When the administrator modifies or delete a policy, the change will be immediately applied to the network.

Default Proxy Policy Management (FMT_ProxyDefault)

The TOE provides the default values for the security policy that the proxy provides. The administrator can set a default policy that will be applied to the proxy as follows:

- Default server setting: Information related to the proxy operation
- Proxy protocol setting: Protocol to be used in the proxy and the authentication protocol

IPSec policy Management (FMT_IPsecPolicy)

The TOE provides functions to add, modify, delete, or search VPN security policies. The TOE checks whether the attribute of the VPN security policy entered by the administrator overlaps with an attribute of an existing policy. If it does not overlap with an attribute of an existing policy, the TOE will add the VPN security policy. The new VPN security policy is immediately applied but not stored until the administrator stores the setting. When the administrator requests to

modify or delete a certain VPN security policy, the VOE will immediately modify or delete the corresponding security policy.

6.2.5.4 Network Interface Management (FMT_NICManage)

The TOE provides various network configuration functions for its interfaces. The TOE can set interface status search, connection method, backup, interface activation status, media type, and line fault detection, and view the status. The TOE can set both physical and tunnel interfaces.

6.2.5.5 PPP Interface Management (FMT_PPPManage)

The TOE provides functions to create, modify, delete, or search PPP interfaces necessary for PPP connection. The TOE checks whether the attribute of the PPP connection inputted by the administrator overlaps with an attribute of an existing interface. If the attribute does not overlap, the TOE will create a new PPP interface based on the attribute inputted by the administrator and will add PPP interface information set by the administrator to the configuration data. If the administrator requests to modify or delete a certain PPP interface, the TOE will modify or delete the corresponding interfaces in the configuration data.

6.2.5.6 Static Routing Management (FMT_RoutingManage)

The TOE provides functions for the administrator to add, modify, delete or search the current routing table, network address, gateway, interface, and device information. To add a static routing table, the administrator inputs address (network/host) and gateway information and this information is applied to the TOE system. The TOE can search and delete the static routing tables added by the administrator.

6.2.5.7 ARP Management (FMT_ARP)

The TOE provides functions to add, modify, or delete ARP address information cached in the ARP memory address table through the administrator interface.

6.2.5.8 DHCP Management (FMT_DHCP)

The TOE provides functions to add, modify, or delete attributes of the DHCP server such as IP lease duration, IP assignment scope, and subnet through the administrator interface to provide automatic IP assignment (DHCP) function for an internal user.

6.2.5.9 Host DNS Setting (FMT_HostDNSSet)

The TOE provides functions to set, modify, delete, or search host names on the network. The administrator can define a unique name (less than 255 alphanumeric digits) on the network, and the administrator can initialize domain information with a new host name and host information.
The TOE provides functions to set, modify, delete, or search the name servers (DNS) that are used by the security policy and audit record functions to search network address information. The administrator can add three name servers (DNS) as IP addresses, and the new information is immediately applied.

6.2.5.10 System Time Setting (FMT_TimeSet)

The TOE provides a function to set the time of the TOE. In the default status, the TOE synchronizes with a reliable external NTP server for time setting. At this time, instead of an internal TOE function, an external time stamp server is used to securely manage time sources. The TOE also allows the administrator to set and modify the time.
. .

6.2.5.11 Audit Records Setting (FMT_AuditSetup)

To manage all audit records which occur during the operation of the TOE, the TOE sets the audit record management policy. The administrator can set the audit record and confirm and cancel the audit record setting using provided functions. The following is inputted for the management of the audit records:

- TOE real-time audit records storage size
- Log priority
- Warning priority
- SMTP server address
- Administrator mail
- Mail queue

6.2.5.12 Security Management Setting (FMT_AdminSetup)

The TOE can set the time-out limit of the administrator session in the security management environment. The time-out limit is in minute or second units, and the default time-out limit is 10 minutes. The TOE can run each server from the basic port or a port randomly set by the administrator. A trusted administrator network is registered in advance to prevent the administrator from accessing the TOE due to a mistake in security policy. An administrator network can be set based on the existing network object and groups.

6.2.5.13 Firmware Upgrade (FMT_FirmUp)

The TOE provides a firmware upgrade function for enhanced capacity of the security functions and operating system. The administrator can move the firmware to the administrator PC, and upload the corresponding image to the TOE through the security management connection (HTTPS.) The TOE checks the integrity of the uploaded image, and updates the firmware stored in flash memory. For this purpose, the administrator must receive the corresponding firmware image from the TOE provider (NexG) in a secure manner, and move it to the administrator's PC. When uploading the image, the TOE can use the SSL protocol for security management.

6.2.5.14 System Setting (FMT_SysSetup)

The TOE provides functions to store, initialize, back up, and restore system settings such as policies and functional items for operation and execution of the security functions. Therefore, the administrator can set, modify, delete, or search system setting data. The administrator can set, modify, delete, or search the system setting necessary for TOE operation.

If a change is made in the operation of the TOE by the authorized administrator or in the policy and functional setting, the change will be immediately applied in memory and saved in flash memory. The TOE can be also initialized to the factory setting. The administrator can initialize only the setting while the TOE is operating or can select the Initialize and Restart option. The TOE also allows the administrator to back up all policies and settings in a single file and restore the system using the backup file. In this way, the TOE can restore the settings damaged by unexpected faults.

The TOE provides functions for the authorized administrator to stop and restart the software in the Security Management environment. The administrator can decide whether to restart or stop the system using these functions. When the administrator executes a command to restart or stop the system, the TOE displays the confirmation message. After the administrator's approval, the TOE will restart or stop the system.

6.2.5.15 System Status Management (FMT_SysStatus)

The TOE provides functions to display the versions of the security function and the operating system. The TOE provides the following version information:

- Dedicated operating system version and firmware version

The TOE provides functions to search the running time of the system and system load (with the CPU idle time being displayed in %) among system status information.

6.2.5.16 Audit Records Backup (FMT_AUBackup)

The TOE allows only the authorized administrator to store and back up audit record data in permanent storage to protect the audit record trail. The audit records are stored in a dedicated database so that the audit records can be backed up and extracted into a file using the standard database management interface, SQL.

The TOE provides a function to restore backed up audit record data.

6.2.5.17 Configuration Saving (FMT_SaveConfig)

"Security environment attributes" set during operation are saved in the operating system and applied to the running TOE. However, if the TOE is restarted, all security environment attributes will be deleted. Therefore, the administrator must save the security environment attributes in flash memory. The TOE can save security environment attributes entered during operation in the DB.

6.2.5.18 Statistics (FMT_Statistics)

The TOE creates a statistical report by processing audit record data accumulated on audit record storage media and provides a report to the administrator for efficient analysis. Only the authorized administrator can search the statistical data, and the TOE provides the following types of audit record statistics:

- Packet information by date (Daily, Weekly, Monthly, and Yearly)
- Total packets, Allowed packets, Rejected packets, Data traffic, By service (Port, Protocol, Type)
- Sessions, packets, and data by packet source or destination

6.2.5.19 Administrator Password Change (FMT_AdminPass)

The TOE provides functions to change the password of the authorized administrator. The TOE also can set whether to use the administrator password provided with the password or to newly set an administrator password.

6.2.5.20 Installation Wizard Launch (FMT_Wizard)

When the TOE is installed, the TOE is initialized and the administrator must be allowed to access the TOE through the security management screen. For this purpose, the TOE provides a minimum level security management setting through the console (RS-232C) port.

6.2.5.21 Audit Records Policy Setting (FMT_LogServerPolicy)

The TOE provides functions to selectively include or exclude the audit target events based on the audit record event type and the level in compliance with the audit record management security policy set by the administrator. All security function-related operations and processing of VForce 1700 V1.0 S/W have a few options in relation to the generation of audit records. Most of all, VForce 1700 V1.0 S/W generates audit records based on the selective audit record priority. The priorities of the audit records are as follows:

- Eight stages: Emergency > Alert > Critical > Error> Warning > Notice > Information > Debugging
- Higher audit record priority level includes lower levels.
- Audit records only for audit target events higher than the priority selected by the administrator. will be created.

6.2.5.22 Security Functional Requirements (SFR) Mapping:

- 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_SMR.1
- FMT_SMF.1
- FIA_ATD.1
- FPT_STM.1

6.2.6 TSF Protection (FPT)

6.2.6.1 Abstract Machine Test (FPT_ABTest)

FPT_ABTest.1 The TOE conducts a test to check whether each hardware element of the TSF implementation are normally operable upon initial start, every 24 hours during operation, or upon the request of the administrator. The TOE checks the gateway status of the interface it uses. If the gateway is down, the TOE will update the corresponding routing table. In other words, if the gateway of an interface is down, the TOE will immediately delete the corresponding routing table. When the TOE detects a message in the kernel while checking interfaces, it will immediately update the corresponding routing table. The DPD test described earlier is included in the abstract machine test.

6.2.6.2 Integrity Checking (FPT_Integrity)

FPT_Integrity.1 The TOE tests processes that use security functions. If a process is terminated without authorization, the TOE will create audit records (and will send mail to the administration, if necessary) and restart the corresponding process. To monitor whether an unauthorized user forges or alters files, the TOE provides an integrity function. The integrity function targets the TSF data and the TSF execution codes. For the TSF data, the TOE compares the result of the integrity test with the result of the previous test. The TSF execution codes are not changeable. The TOE conducts integrity tests on the (execution) files composing processes and important files of the OS. If an integrity error is found, the TOE will take measures as in the abstract machine test describe above to inform the authorized administrator and to store audit records. The TOE conducts an integrity test for the following:

- At startup
- Upon the request of the authorized administrator through security management functions
- Every cycle defined by the administrator

FPT_Integrity conforms to SOF-high for the hash function specified in the Common Criteria for the Information Protection System (Notice 2005-25 by the Ministry of Information and Communication) [1].

6.2.6.3 Security Functional Requirements (SFR) Mapping:

- FPT_AMT.1
- FPT_TST.1
- FPT_TST.2
- FPT_RPL.1

6.2.7 TOE Access (FTA)

6.2.7.1 Session Kill (FTA_SessionKill)

FTA_SessionKill.1 A general user is authenticated by the corresponding protocol (HTTP or SOCKS 5) through the proxy and accesses the final destination server. If no traffic data is created after the user accesses the server, the corresponding session will be terminated. After the session is terminated, the TOE informs the server and the client of this and deletes the session from the session list. If the user requests server to access again, the TOE will authenticate the user through the HTTP or SOCKS5 and recognize the user's access to the destination server as a new session.

6.2.7.2 Session Locking (FTA_SessionLock)

FTA_SessionLock.1 All administrators and general users who are accessing the TSF of the TOE shall prove that they have proper authority through the identification and authentication processes. If no data is transmitted between the administrator's browser and the TOE, the TOE will lock the session. In other words, the session will be maintained (with the SSL authentication token and the security management page being saved,) and the administrator will be required to input an ID and password (with the SSL authentication token maintained) to access the previous page.

6.2.7.3 Security Functional Requirements (SFR) Mapping:

- FTA_SSL.1
- FTA_SSL.3

6.2.8 Trusted Path/Channel (FTP)

6.2.8.1 Trusted Channel (FTP_AdminTrusted)

FTP_AdminTrusted.1 This is for secure information transmission. When the administrator directly accesses the TOE for security management, the TOE provides an HTTPS (GUI)-based secure communication path for the protection of the console and the network. HTTPS is a Netscape web protocol installed in the browser that encodes and decodes the user page request at the SSL sub layer under the HTTP. The TOE uses the Open SSL cryptographic toolkit to support SSL protocol network communication.

6.2.8.2 Security Functional Requirements (SFR) Mapping:

- FTP_ITC.1

6.2.9 Privacy (FPR)

6.2.9.1 TOE Status View (FPR_Status)

Upon the request of the authorized user who successfully logged in using the security management screen, the TOE will display the following:

- Traffic at Each Interface: Displays inbound/outbound packets, packets in Kbytes per second, and packet count per second at each Ethernet interface including any virtual IPSec interface as well as activation/deactivation status of each interface.
- Session: Displays the list of sessions having passed the security policy of the TOE. The list includes protocol, valid time (in second), source/destination port, ICMP type, code, TCP status, and establishment status of each session.
- Access Control Status: Displays the number of packets and bytes that use packet-filtering, network address translation, port-forwarding, and redirect security policies of the TOE.
- IPSec Status: Displays security tunnel (SA) information between the TOE and the communication counterpart. Security tunnel information includes local and remote VPN networks of each security tunnel, gateway address of the communication counterpart, and the number of packets having passed the corresponding security tunnel.
- Login User: List of authorized administrators currently connected to the TOE. Displays user IDs, TTY types, standby time, login time, and host IP addresses.
- System Information: Displays overall TOE system information including the software version, operation time, and CPU load.

6.2.9.2 Source Address Translation (FPR_SNAT)

FPR_SNAT.1 To overcome the lack of IP address resources of IPv4 and to protect internal users, the TOE provides an network address translation function which can create private addresses. With this function, an internal user can disclose only public IP addresses to the external IT entity and hide the private IP addresses during the communication with an external IT entity.

6.2.9.3 Destination Network Address Translation (FPR_DNAT)

FPR_DNAT.1 The TOE can also redirect a session from an public IP address to a certain internal host. When an external IT accesses an internal private host, the TOE hides the network information of the private host to the outside and

connects the network IP accessible from the outside. Then, an external It entity can access the network through a shared IP without direct connection to the network.

6.2.9.4 Redirecting (FPR_Redirect)

FPR_Redirect.1 The TOE changes destination network information (IP and port) and redirects to a destination set by the administrator. The TOE can redirect some incoming and outgoing packets using the protocols (HTTP, FTP, and TELNET) that the proxy supports and require them to pass the proxy. The TOE can also redirect access to the destination without changing the network information of the host that the TOE protects.

6.2.9.5 Security Functional Requirements (SFR) Mapping:

- FDP_IFC.2(3)
- FDP_IFF.1(4)
- FPR_UNO.4

7 Protection Profile Claims

This chapter provides correspondence between the TOE and [FW_PP_V1.1] and between the Security Target and [VPN_PP_V1.1].

7.1 Protection Profile Reference

The TOE and the Security Target have been prepared based on [FW_PP_V1.1] and [VPN_PP_V1.1] , and the product has been designed to meet all Security Functional Requirements and assurance requirements specified in the protection profile.

7.2 Protection Profile Tailoring

7.2.1 [FW_PP_V1.1] Tailoring

The following shows the Security Functional Requirements of the Common Criteria for the Information Protection System tailored by [FW_PP_V1.1]:

[Table 7-1] Security Functional Requirements Tailored in [FW_PP_V1.1]

Functional Component	Description
FAU_ARP.1	Security alarm
FAU_GEN.1	Audit data creation
FAU_SAA.1	Potential violation analysis
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.3	Response to predicted audit data loss
FAU_STG.4	Prevention of loss of audit data
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute-based access

	control
FDP_IFC.2	complete information flow control
FDP_IFF.1	Single-layer security attribute
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute management
FIA_SOS.1	Secret verification
FIA_UAU.1	Authentication
FIA_UAU.4	Replay prevention authentication mechanism
FIA_UAU.7	Authentication feedback protection
FMT_MOF.1	Security function management
FMT_MSA.1	Security attribute management
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	TSF data management
FMT_AMT.1	Abstract machine test
FTP_TST.1	TSF self-test
FPT_TST.2(Extension)	Response to TSF data integrity fault (Extension)
FTA_SSL.1	Session locking by TSF
FTA_SSL.3	Session termination by TSF

7.2.2 [VPN_PP_V1.1] Tailoring

The following shows the Security Functional Requirements tailored to the Common Criteria for the Information Protection System by [VPN_PP_V1.1]:

[Table 7-2] Security Functional Requirements Tailored by [VPN_PP_V1.1]

Functional Component	Description
FAU_ARP.1	Security Alarm
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	Response expected loss of audit data
FAU_STG.4	Prevention of loss of audit data
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Single-layer security attribute
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of confidential information
FIA_UAU.4	Replay prevention authentication mechanism
FIA_UAU.7	Authentication feedback protection
FMT_MOF.1	Security function management
FMT_MSA.1	Security attribute management
FMT_MSA.3	Static attribute initialization
FPT_AMT.1	Abstract machine test
FPT_PRL.1	Replay attack detection and measure
FPT_TST.1	TSF self-test
FPT_TST.2(Extension)	Response to TSF data integrity fault
FTA_SSL.1	Session locking by TSF
FTP_ITC.1	Trusted channel between TSFs

7.3 Protection Profile Augmentation

7.3.1 Security Requirements Augmentation for Protection Profile

To support additional security functions of the TOE besides the requirements specified in the protection profile, the author added the following security functional requirements:

[Table 7-3] Author-augmented SFR

Functional Component	Description
FMT_SMF.1	Management function specification
FPT_UNO.4	Authorized user observability

7.3.2 Protection Profile Threats and Purpose Augmentation

Besides the security threats and objectives specified in the security target, the author added the following security threats and security objectives:

[Table 7-4] Author-augmented Threats and Security Objectives

Functional Component	Description
T. Privacy	If an internal network IP address is disclosed to a non-trusted network IP address, an unauthorized attacker may predict the internal network and access the network without permission.
O. Privacy	The TOE shall prevent an external user from predicting the IP of an internal user.
OE. Trusted Server	For the functions of the TOE, the following servers located outside the TOE shall be protected: Network Time Protocol (NTP) and the remote security management system.
OE. Trusted Channel	For secure communication between the TOE and the administrator, the TOE shall provide a function that will protect channels and certificates using the OpenSSL protocol.

OE. Trusted Storage	To ensure safe maintenance and management of the storage where the TOE-audit records are stored, trusted storage shall be provided and this storage shall provide SQL-Lite, a database management system.

8 Rationale

This chapter provides the rationale for proving the completeness and the consistency of the security target. The rationale covers the following:

- Security objectives
- Security requirements
- TOE summary specification
- Security functional requirements dependency
- Internal consistency of the security target

8.1 Security Objectives Rationale

8.1.1 Security Objectives Rationale for TOE Security Function Purpose Same as Those in Protection Profile

[Table 8-1] Security Objective Rationale Same as [FW_PP_V1.1] and [VPN_PP_V1.1]

Security Objective	Description
O. Audit	This security objective provides means for the TOE to store, maintain, and review the security-related events in a detailed and accurate manner. This security objective is necessary for handling T. Misuse and T. Recording Failure and supporting P. Audit in the organizational security policies.
O. Flaw Code Inspection	The security objective ensures that flaw codes that might exist in the code by the developer are detected. This security objective is necessary for responding to T. Flaw Code.
O. Management	This security objective provides means for the authorized administrator to securely manage the TOE. This security objective is necessary for supporting P. Trusted Management.
O. Data Protection	This security objective ensures the integrity of TSF data. This security objective is necessary for ensuring T. Transmission Integrity, handling T. Stored Data Damage, and supporting P. Confidentiality and P. Cryptograph.

O. Confidentiality	This security objective ensures confidentially of data transmitted by the TOE on the network. This security objective is necessary for supporting T. Cryptograph Decoding, P. Confidentiality and P. Cryptograph.
O. Identification and Authentication	This security objective ensures that the TOE can identify and authenticate users. This security objective is necessary for responding to T. Impersonation, T. Continued Authentication Attempt, T. Bypassing, T. Replay attack, T. Stored Data Damage, T. IP Address Spoofing and T. Misuse.
O. Self-protection	Because the TOE has a self-protection function, this security objective is necessary for responding to T. New Attack, T. Bypassing, T. Misuse, and T. Stored Data Damage.
O. Access control	Because the TOE controls access to the network, this security objective is necessary for responding to T. Unauthorized Information Outflow, T. Bypassing, T. IP Address Spoofing and T. Unauthorized Information Inflow.
O. Information Flow Control	Because the TOE ensures mediation of information flow based on the security policy, this security objective is necessary for responding to T. Unauthorized Information Inflow and T. Unauthorized Information Outflow.
O. Information Flow Mediation	Because the TOE ensures mediation of information flow based on the security policy, this security objective is necessary for supporting P. Confidentiality and P. Plain Text Transmission.
O. Key Security	Because the TOE provides confidentiality and integrity of the cryptographic keys and ensures proper key exchanges, this security objective is necessary for supporting T. Cryptographic Decoding, T. Transmission Integrity, P. Confidentiality, and P. Cryptograph.

8.1.2 Security Objectives Rationale for Environment Same as Protection Profile

[Table 8-3] Security Objective Rationale for Environment Same as Protection Profile

Security Objective	Description
OE. Physical Security	OE. Physical Security ensures physical security of the TOE so it is necessary for supporting A. Physical Security.
OE. Security Maintenance	When there is a change in network environment due to a network configuration change or increase/decrease of hosts or services, OE. Maintenance ensures that the new environment and the new security policy are immediately applied to the TOE operation policy for consistent security levels. Therefore, OE. Maintenance is necessary for supporting A. Security Maintenance and responding to T. New Attack.
OE. Trusted Administrator	OE. Trusted Administrator ensures that the authorized administrator of the TOE is reliable so it is necessary for supporting A. Trusted Administrator and responding to T. Misuse, TE. Poor Management and TE. Delivery and Installation.
OE. Trusted Management	OE. Trusted Management ensures that the TOE is delivered and installed in a secure way and configured and managed by the authorized administrator so it is necessary for responding to T. New Attack, TE. Poor Management, and TE. Delivery and Installation and supporting P. Trusted Management.
OE. Security Policy	This security objective ensures that the TOE and an authenticated TOE that communicates with the TOE execute compatible security policies so it is necessary for supporting Assumptions A. Security Policy.
OE. Operating System Reinforcement	This security objective eliminates unnecessary services or means for the operation of the TOE, reinforces the vulnerabilities in the operating system, and support safety and reliability of the operating system. It is necessary for supporting Assumption A. Operating System Reinforcement and responding to T. New Attack.
OE. Single Point of Connection	This security objective ensures that all external networks communicate with the internal network through the TOE so it is necessary for supporting Assumption A. Single Point of Connection.

※ OE. Attacker Level has been changed to Threat in Assumptions and not included in this table.

[Table 8-4] Relation between the Security Environment and Security Objective

Security Objective / Security Environment	TOE Security Objective											Security Objective for Environment						
	O. Impersonation	O. Flaw Code Inspection	O. Management	O. Data Protection	O. Identification and Authentication	O. Self-protection of Functions	O. Access Control	O. Information Flow Control	O. Confidentiality	O. Key Protection	O. Information Flow Mediation	OE. Physical Security	OE. Security Management	OE. Trusted Administrator	OE. Safe Management	OE.Operating System Reinforcement	OE. Single Point of Connection	OE. security policy
T. Impersonation					X													
T. Flaw Code		X																
T. Record Flaw	X																	
T. Abuse	X				X	X								X				
T. Decoding									X	X								
T. Continued Authentication Attempts					X													
T. Bypassing					X	X	X											
T. Replay Attack					X													
T. Stored Data Damage				X	X	X												
T. Transmission Integrity				X						X								
T. Unauthorized Information Inflow							X	X										
T. Unauthorized Information Disclosure							X	X										
T. New Attack						X							X		X	X		X
T. IP Address Spoofing					X		X											
P. Audit	X																	
P. Confidentiality				X					X	X	X							
P. Trusted Management			X												X			
P. Cryptographic				X					X	X								
P. Plain Test Transmission											X							
A. Physical Security												X						
A. security policy																		X
A. Security Maintenance													X					X
A. Trusted Administrator														X				
A. Operating System Reinforcement																X		
A. Single Point of Connection																	X	
TE. Poor Management														X	X			
TE. Delivery and Installation														X	X			

※ A. Attacker's level and OE. Attacker Level has been changed to Threat in Assumptions and not included in this table.

8.1.3 Author Augmented Security Objectives Rationale

[Table 8-4] Author-augmented Security Objective Rationale

Security Target	Description
O. Privacy	This security objective shall prevent an external user from predicting the IP of an internal user. This security objective responds to Threat T. Privacy.
OE. Trusted Server	This security objective ensures that external servers interacting with the TOE are reliable so it is necessary for supporting Assumption A. Trusted Server.
OE. Trusted Channel	This security objective ensures a trusted channel for the communication between the TOE and the administrator so it is necessary for supporting A. Trusted Channel. For safe channel provision and certificate management, OpenSSL protocol is used.
OE. Trusted Storage	This security objective ensures that the storage where TOE-related audit records are stored is maintained and managed in a secure way. This security objective is necessary for supporting A. Trusted Storage. The storage provides a relational database, SQL-Lite.

[Table 8-5] Relations between Augmented Security Objective Rationale and Security Environment

Security Objective / Security Environment	TOE Security Objective			
	O. Privacy	OE. Trusted Server	OE. Trusted Channel	OE. Trusted Storage
T. Privacy	X			
A. Trusted Server		X		
A. Trusted Channel			X	
A. Trusted Storage				X

8.2 Rationale for Security functional requirements

8.2.1 Rationale for Security functional requirements Same as Those in Protection Profile

O. Flaw Code Inspection is covered by the assurance requirements.

8.2.1.1 FAU_ARP.1 Security Alarm

The TOE provides functions that take measures against identified security breaches. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.2 FAU_GEN.1 Audit Data Generation

The TOE provides functions to define audit target events and generate audit records. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.3 FAU_SAA.1 Potential Violation Analysis

The TOE provides functions to inspect audited events and identify security breaches. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.4 FAU_SAR.1 Audit Review

The TOE provides functions for the authorized administrator to review the audit records. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.5 FAU_SAR.3 Selectable Audit Review

The TOE provides functions to search and sort audit record data. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.6 FAU_SEL.1 Selective Audit

The TOE provides functions for the authorized administrator to include or selectively apply the audit target events based on the security attribute. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.7 FAU_STG.1 Audit Trail Protection

The TOE provides functions to protect audit records from being changed or deleted by an unauthorized user. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.8 FAU_STG.3 Response to Predicted Audit Data Loss

The TOE provides functions for the administrator to take predefined actions when the audit trail crosses the threshold. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.9 FAU_STG.4 Prevention of Loss of Audit Data

The TOE provides functions for the administrator to take predefined actions when audit record storage is full. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.10 FCS_CKM.1 Cryptographic Key Creation

The TOE provides functions to create cryptographic keys based on the cryptographic key creation algorithm and the defined cryptographic key length. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Confidentiality, O. Data Protection, and O. Key Security of [VPN_PP_V1.1].

8.2.1.11 FCS_CKM.2 Cryptographic Key Distribution

The TOE provides functions to distribute cryptographic keys according to the cryptographic key distribution method. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Confidentiality, O. Data Protection, and O. Key Security of [VPN_PP_V1.1].

8.2.1.12 FCS_CKM.4 Cryptographic Key Destruction

The TOE provides functions to destroy the cryptographic keys according to the cryptographic key destruction method. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Confidentiality, O. Data Protection, and O. Key Security of [VPN_PP_V1.1].

8.2.1.13 FCS_COP.1 Cryptographic Operation

The TOE provides functions to perform cryptographic operations according to the cryptographic algorithm and the predefined cryptographic key length. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Confidentiality and O. Data Protection of [VPN_PP_V1.1].

8.2.1.14 FDP_ACC.2 Complete Access Control

The TOE provides functions to secure complete access control for all traffic passing the TOE in compliance with the administrator-set security policy. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Data Protection and O. Access Control of [FW_PP_V1.1].

8.2.1.15 FDP_ACF.1 Security Attribute-based Access Control

The TOE provides functions to allow access control based on the security attribute in compliance with the administrator-defined access control security policy. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Data Protection and O. Access Control of [FW_PP_V1.1].

8.2.1.16 FDP_DAU.1 Basic Data Authentication

The TOE provides subjects to verify evidence creation capacity and evidence to guarantee the integrity of the data transmitted to/from the TOE. Therefore, the TOE conforms to the requirements specified in Security Objective O. Data Protection of [VPN_PP_V1.1].

8.2.1.17 FDP_IFC.1 Subset Information Flow Control

The TOE ensures that the information flow of the data transmitted to/from the TOE is controlled according to the VPN security policy. Therefore, the TOE conforms to the requirements specified in Security Objective O. Information Flow Mediation of [VPN_PP_V1.1].

8.2.1.18 FDP_IFC.2(1) Complete Information Flow Control

The TOE provides functions to completely control information flow of all traffic passing through the TOE based on the packet-filtering security policy defined by the administrator. Therefore, the TOE conforms to the requirements specified in Security Objective O. Information flow Control of [FW_PP_V1.1].

8.2.1.19 FDP_IFC.2(2) Complete Information Flow Control

The TOE provides functions to completely control information flow of all traffic passing through the TOE based on the proxy security policy defined by the administrator. Therefore, the TOE conforms to the requirements specified in Security Objective O. Information Flow Control of [FW_PP_V1.1].

8.2.1.20 FDP_IFF.1(1) Single-layer Security Attribute

The TOE provides functions to define and apply the VPN security policy which controls information flow based on the security attribute. Therefore, the TOE conforms to the requirements specified in Security Objective O. Information Flow Mediation of [VPN_PP_V1.1].

8.2.1.21 FDP_IFF.1(2) Single-layer Security Attribute

The TOE provides functions to define and apply the packet-filtering security policy which controls information flow based on the security attribute. Therefore, the TOE conforms to the requirements specified in Security Objective O. Information Flow Control of [FW_PP_V1.1].

8.2.1.22 FDP_IFF.1(3) Single-layer Security Attribute

The TOE provides functions to define and apply the proxy security policy which controls information flow based on the security attribute. Therefore, the TOE conforms to the requirements specified in Security Objective O. Information Flow Control of [FW_PP_V1.1].

8.2.1.23 FIA_AFL.1 Authentication Failure Handling

The TOE provides functions to define the user authentication failure threshold and takes predefined actions when the threshold is crossed. Therefore, the TOE conforms to the requirements specified in Security Objective O. Identification and Authentication of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.24 FIA_ATD.1 User Attribute Definition

The TOE provides functions to define the security attribute list for each user. Therefore, the TOE conforms to the requirements specified in Security Objective O. Identification and Authentication of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.25 FIA_SOS.1 Verification of Confidential Information

The TOE provides functions to impose compliance with the password collation rule set by the password. Therefore, the TOE conforms to the requirements specified in Security Objective O. Identification and Authentication of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.26 FIA_UAU.2 User Authentication Prior to Every Behavior

The TOE provides functions to successfully authenticate authorized administrator and users. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Management, O. Data Protection, O. Identification and Authentication of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.27 FIA_UAU.4 Replay Prevention Authentication mechanism

The TOE provides functions to prevent replay of the authentication data. Therefore, the TOE conforms to the requirements specified in Security Objective O. Identification and Authentication of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.28 FIA_UAU.7 Authentication Feedback Protection

The TOE provides a response that contains minimum information for the user before or during the authentication process. Therefore, the TOE conforms to the requirements specified in Security Objective O. Identification and Authentication of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.29 FIA_UID.2 User Identification Prior to Every Behavior

The TOE guarantees successful identification of the authorized administrator and the user. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Management, O. Data Protection, O. Identification and Authentication of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.30 FMT_MOF.1 Security Function Management

The TOE provides functions that allow only the authorized administrator to manage security functions. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.31 FMT_MSA.1 Security Attribute Management

The TOE provides functions that allow only the authorized administrator to manage security attributes. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.32 FMT_MSA.2 Trusted Security Attribute

The TOE allows only values within the defined range to be inputted as security attributes. Therefore, the TOE conforms to the requirements specified in Security Objective O. Self-protection of [VPN_PP_V1.1].

8.2.1.33 FMT_MSA.3 Static Attribute Initialization

The TOE guarantees management of the security attributes which are applied to the administrator security policy, the VPN security policy, the packet-filtering security policy, and the proxy security policy. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1] and [VPN_PP_V1.1] and Security Objective O. Information Flow Mediation of [VPN_PP_V1.1].

8.2.1.34 FMT_MTD.1(1) TSF Data Management

The TOE provides functions for the authorized administrator to create statistics from the audit data. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1].

8.2.1.35 FMT_MTD.1(2) TSF Data Management

The TOE provides functions to back up and restore important files composing the TOE. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1].

8.2.1.36 FMT_MTD.1(3) TSF Data Management

The TOE provides functions for the authorized administrator to manage the administrator security policy, VPN security policy, packet-filtering security policy, and proxy security policy. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1].

8.2.1.37 FMT_MTD.1(4) TSF Data Management

The TOE provides functions for the authorized administrator to manage cryptographic key attributes. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [VPN_PP_V1.1].

8.2.1.38 FMT_MTD.1(5) TSF Data Management

The TOE provides functions for the authorized administrator to manage identification and authentication data. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.39 FMT_MTD.1(6) TSF Data Management

The TOE provides functions for the authorized administrator to manage TOE time data. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.40 FMT_MTD.2 TSF Data Threshold Management

The TOE provides functions for the authorized administrator to manage TSF data thresholds and to take actions predefined by the administrator when the threshold is crossed. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.41 FMT_MTD.3 Trusted TSF Data

The TOE allows only values within the defined range to be inputted as security attributes. Therefore, the TOE conforms to the requirements specified in Security Objective O. Self-protection of [VPN_PP_V1.1].

8.2.1.42 FMT_SMR.1 Security Role

The TOE provides functions to define and apply security roles of all users including the administrators. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.43 FPT_AMT.1 Abstract Machine Test

The TOE provides the abstract machine test function to check whether all functions of the TOE including the TSF are normally operating. Therefore, the TOE conforms to the requirements specified in Security Objective O. Data Protection of [VPN_PP_V1.1] and Security Objective O. Self-protection of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.44 FPT_RPL.1 Replay Attack Detection and Measures

The TOE provides functions to detect and audit replay of user or VPN gateway authentication data. Therefore, the TOE conforms to the requirements specified in Security Objective O. Identification and Authentication of [VPN_PP_V1.1].

8.2.1.45 FPT_RVM.1 Non-bypassability of the TSP

The TOE provides a single point of connection through which the TSP is called. Therefore, the TOE conforms to the requirements specified in Security Objective O. Self-protection of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.46 FPT_SEP.1 Security Function Fragmentation

The TOE provides functions to maintain security for the execution of the TSF. Therefore, the TOE conforms to the requirements specified in Security Objective O. Self-protection [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.47 FPT_STM.1 Reliable Time Stamp

The TOE provides a reliable time stamp function for the TSF. Therefore, the TOE conforms to the requirements specified in Security Objective O. Audit of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.48 FPT_TST.1 TSF Self-test

The TOE provides self-test and integrity test functions. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Data Protection and O. Self-protection of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.49 FPT_TST.2 Response to TSF Data Integrity Fault

The TOE provides functions to take actions predefined by the administration upon occurrence of a TSF data integrity fault. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Data Protection and O. Self-protection of [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.1.50 FPT_SSL.1 Session Locking by TSF

After a certain period of idle time by the authorized administrator, the TOE locks the corresponding session and requires an event before unlocking the session. Therefore, the TOE conforms to the requirements specified in Security Objectives O. Self-protection of [FW_PP_V1.1] and [VPN_PP_V1.1], Security Objective O. Identification and Authentication of [FW_PP_V1.1], and Security Objective O. Data Protection of [VPN_PP_V1.1].

8.2.1.51 FPT_SSL.3 Session Termination by TSF

The TOE provides functions to terminate the session after a general user remains idle for a certain period of time. Therefore, the TOE conforms to the requirements specified in Security Objective O. Self-protection of [FW_PP_V1.1].

8.2.1.52 FTP_ITC.1 Trusted Channel between TSFs

The TOE provides functions to securely manage the channel while the authorized administrator is accessing the security management environment of the TOE. Therefore, the TOE conforms to the requirements specified in Security Objective O. Management of [VPN_PP_V1.1].

[Table 8-6] Mapping between TOE Security Functions and Security Objectives

PP	[FW_PP_V1.1]							[VPN_PP_V1.1]							
Security Target / Security Function Requirements	O· Audit	O· Management	O· Data Protection	O· Identification and Authentication	O· Self-protection of Functions	O· Access Control	O· Information Flow Control	O· Audit	O· Management	O· Data Protection	O· Confidentiality	O· Identification and Authentication	O· Self-protection of Functions	O· Information Flow Mediation	O· Key Security
FAU_ARP.1	X							X							
FAU_GEN.1	X							X							
FAU_SAA.1	X							X							
FAU_SAR.1	X							X							
FAU_SAR.3	X							X							
FAU_SEL.1	X							X							
FAU_STG.1	X							X							
FAU_STG.3	X							X							
FAU_STG.4	X							X							
FCS_CKM.1										X	X				X
FCS_CKM.2										X	X				X
FCS_CKM.4										X	X				X
FCS_COP.1										X	X				
FDP_ACC.1			X			X									
FDP_ACF.1			X			X									
FDP_DAU.1										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								X			
FIA_ATD.1				X								X			
FIA_SOS.1				X								X			
FIA_UAU.2		X	X	X					X	X		X			
FIA_UAU.4				X								X			
FIA_UAU.7				X								X			
FIA_UID.2		X	X	X					X	X		X			
FMT_MOF.1		X							X						
FMT_MSA.1		X							X						
FMT_MSA.2		X							X				X		
FMT_MSA.3		X							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							X						
FMT_MTD.1(6)		X							X						
FMT_MTD.2		X							X						
FMT_MTD.3									X				X		
FMT_SMR.1		X							X						
FPT_AMT.1					X					X			X		
FPT_RPL.1												X			
FPT_RVM.1					X								X		
FPT_SEP.1					X								X		
FPT_STM.1	X							X							
FPT_TST.1			X		X					X			X		
FPT_TST.2			X		X					X			X		
FTA_SSL.1				X	X					X			X		
FTA_SSL.3					X										
FTP_ITC.1									X						

8.2.2 Author-augmented Rationale for Security functional requirements

8.2.2.1 FMT_SMF.1 Management Function Specification

The TOE ensures that it provides all required security management functions, and meets the requirements specified in O. Management of Security Objective in [FW_PP_V1.1] and [VPN_PP_V1.1].

8.2.2.2 FPR_UNO.4 Authorized User Observability

The TOE ensures that the authorized administrator can check TOE resources and process status for the purpose of managing the TOE. The TOE meets the requirements specified in O. Management in Security Objective in [FW_PP_V1.1] and [VPN_PP_V1.1].

[Table 8-7] Rationale for Author-augmented Security functional requirements

Security Target / Security Function Requirements	O. Management *
FMT_SMF.1	X
FPR_PSE.1(1)	
FPR_PSE.1(2)	
FPR_UNO.4	X

* - [FW_PP_V1.1], [VPN_PP_V1.1]

8.2.3 Rationale for IT Environment Requirements

8.2.3.1 FTP_ITC.1 Trusted Channel between TSFs

The TOE secures the channel while the authorized administrator accesses the TOE from a remote place. The TOE meets the requirements specified in OE. Trusted Channel of TOE Security Objective.

8.2.3.2 FPT_STM.1 Reliable time stamp

The TOE provides a reliable time stamp using a reliable external time stamp synchronization function. Therefore, the TOE conforms to the requirements specified in OE. Trusted Server of the TOE Security Objective OE.

8.2.3.3 FAU_SAR.3 Selectable Audit Review

For secured management and maintenance of the audit records, the TOE provides a reliable DBMS. The TOE meets the requirements specified in OE. Trusted Storage of TOE Security Objective.

[Table 8-8] Rationale for Author-augmented Security functional requirements

Security Target for Environment / Security Function Requirements	OE. Trusted Channel	OE. Trusted Server	OE. Trusted Storage
FTP_ITC.1	X		
FPT_STM.1		X	
FAU_SAR.3			X

8.3 Rationale for security assurance Requirements

This Security Target conforms to protection profiles for government agency [FW_PP_V1.1] and [VPN_PP_V1.1]. Therefore, an assurance requirements package which satisfies EAL3+ specified in the above protection profiles has been selected, and EAL3 of the Common Criteria for the Information Protection System includes augmentation components as follows:

- ADV_IMP.2 Expression of TSF implementations
- ADV_LLD.1 Declarative low-level design
- ALC_TAT.1 Well-defined development tool
- ATE_DPT.2 Low-level design Test
- AVA_VLA.2 Independent Vulnerability Analysis

Security Objective O. Collated Code Inspection checks whether the code written by the developer has any flaw, and if so, whether the flaw code affects internal components of the TOE. This security objective adds the assurance component ADV_IMP.2 (expression of TSF implementation) and ATE_DTP.2 (low-level design test).

Due to the dependency of ADV_IMP.2 (expression of TSF implementation), ADV_LLD.1 (declarative low-level design) and ALC_TAT.1 (well-defined development tool) have been augmented. AVA_VLA.2 (independent vulnerability analysis) has been also added because the protection profile requires the developer to carry out the vulnerability analysis and the evaluator the independent vulnerability analysis.

8.4 Rationale for Functional Requirements SOF(Strength of Function)

The TOE of this Security Target shall protect general information of a government agency and the asset value is medium level. A threat agent is considered to possess low-level expertise, resources, and motivations. Therefore, to respond to a threat agent with low-level attack potential, the TOE should provide security functions for SOF-medium. This Security target has been designed and prepared based on SOF-medium declared in the intrusion prevention system for government agency [FW_PP_V1.1] and the VPN protection profile [VPN_PP_V1.1].

The identifying value of FIA_UAU.2 and FIA_UAU.4 is 0 and the exploiting value is 21 when the security strength of FIA_UAU.2 and FIA_UAU.4 is calculated according to Table A.3 in Annex A of CEM V2.3. This mechanism can respond to low-level attackers and conforms to the SOF-medium requirement declared in the Security Target.

From the analysis of the SHA1 algorithm hash function SOF which is used to protect the integrity of the stored data and to create the OTP, the exploiting value has been found impractical. This mechanism conforms to the declared SOF-high requirement.

8.5 Rationale for TOE Summary

Some security function of the TOE shall operate together to satisfy TOE security functional requirements. The following table shows that all security functions are mapped with all SFRs:

[Table 8-9] Mapping between SFRs and Security Functions

Security Function Summary	Security functional requirements
Security alarm (FAU_Alarm)	FAU_ARP.1 FAU_SAA.1
Audit records generation (FAU_Audit)	FAU_GEN.1 FAU_SEL.1
Audit records search (FAU_View)	FAU_SAR.1 FAU_SAR.3
Prevention of loss of audit records (FAU_Prevent)	FAU_STG.1 FAU_STG.3 FAU_STG.4
ESP support (FCS_ESP)	FCS_COP.1
AH support (FCS_AH)	
Cryptographic key management (FCS_IKE)	FCS_CKM.1 FCS_CKM.2 , FPT_RPL.1
Key drop management (FCS_KEYDEST)	FCS_CKM.4
Administrator access control (FDP_AdminNetwork)	FDP_ACC.2 FDP_ACF.1 , FPT_RVM.1 , FPT_SEP.1
Encrypted data transmission (FDP_VPN)	FDP_DAU.1 FDP_IFC.1,FDP_IFF.1(1) , FPT_RVM.1 , FPT_SEP.1
Packet-filtering (FDP_PacketFiltering) Network intrusion detection (FDP_NID)	FDP_IFC.2(1) FDP_IFF.1(2), FPT_RVM.1 , FPT_SEP.1
Proxy (FDP_Proxy)	FDP_IFC.2(2), FDP_IFF.1(3),FPT_RVM.1 , FPT_SEP.1
Authentication failure handling (FIA_IAFailure)	FIA_AFL.1
General cryptographic authentication (FIA_PwdAuth)	FIA_UAU.2 FIA_UAU.7 FIA_UID.2 FIA_SOS.1

One-time password authentication (FIA_OTPAuth)	FIA_UAU.4
User password change (FIA_UPWDSet)	FIA_UAU.2 , FIA_SOS.1, FIA_UAU.7
Strength of identification and authentication security (FIA_SoF)	FIA_SOS.1
Security object management (FMT_Object)	FMT_MTD.1(4),FMT_MTD.1(5), FMT_MTD.3,FIA_ATD.1
Security policy management (FMT_Policy)	FMT_MTD.1(3),FMT_MSA.3, FMT_MTD.3
Network interface management (FMT_NICManage)	FMT_MOF.1 FMT_MSA.1 , FMT_MSA.2 FMT_MTD.1(3)
PPP interface management (FMT_PPPManage)	FMT_MOF.1 FMT_MSA.1, FMT_MSA.2 FMT_MTD.1(3)
Static routing management (FMT_RoutingManage)	FMT_MOF.1 FMT_MSA.1, FMT_MSA.2 FMT_MTD.1(3)
ARP management (FMT_ARP)	FMT_MOF.1 FMT_MSA.1, FMT_MSA.2
DHCP management (FMT_DHCP)	FMT_MOF.1 FMT_MSA.1, FMT_MSA.2
Host name DNS setting (FMT_HostDNSSet)	FMT_MOF.1 FMT_MSA.1
System time setup (FMT_TimeSet)	FMT_MOF.1 FMT_MSA.1 FMT_MTD.1(6), FPT_STM.1
Audit record setup (FMT_AuditSetup)	FMT_MOF.1 FMT_MSA.1
Security management Setup (FMT_AdminSetup)	FMT_MOF.1 FMT_MSA.1,FMT_SMR.1
firmware upgrade (FMT_Firmup)	FMT_MOF.1 FMT_MSA.1
System setup management (FMT_SysSetup)	FMT_SMF.1
System status management (FMT_SysStatus)	FMT_MOF.1 FMT_MSA.1

Audit records backup (FMT_AuBackup)	FMT_MTD.1(2), FMT_MTD.2
Setup storing (FMT_SaveConfig)	FMT_MOF.1 FMT_MSA.1
Statistics (FMT_Statistics)	FMT_MTD.1(1)
Administrator password change (FMT_AdminPass)	FMT_MTD.1(5)
Installation Wizard launch (FMT_Wizard)	FMT_MOF.1
Audit record policy setting (FMT_LogServerPolicy)	FMT_MTD.1(3), FMT_MTD.2
Abstract machine test (FPT_ABTest)	FPT_AMT.1
Integrity check (FPT_Integrity)	FPT_TST.1 FPT_TST.2
Session locking (FTA_SessionLock)	FTA_SSL.1
Session termination (FTA_SessionKill)	FTA_SSL.3
Trusted channel (FTP_AdminTrusted)	FTP_ITC.1
Source address conversion (FPR_SNAT)	FDP_IFC.2(3), FDP_IFF.1(4)
Destination address conversion (FPR_DNAT)	FDP_IFC.2(3), FDP_IFF.1(4)
Path redirection (FPR_Redirect)	
TOE status Checking (FPR_Status)	FPR_UNO.4

8.5.1 FAU_ARP.1 – FAU_Alarm

The TOE sends alarms to an administrator through e-mail or message box when it detects an event.

8.5.2 FAU_GEN.1 – FAU_Audit

The TOE generates audit data for all events occurring in the TOE. The audit data has eight phases: Emergency > Alert > Critical > Error> Warning > Notice > Information > Debugging.

8.5.3 FAU_SAA.1 - FAU_Alarm

When an event predefined by the administrator or an event that requires audit records, occurs, the TOE will warn the administrator by sending an e-mail or displaying a message box.

8.5.4 FAU_SEL.1 – FAU_Audit

Depending on the security policy set by the administrator, the TOE can selectively generate audit records.

8.5.5 FAU_SAR.1 – FAU_View

The TOE allows the administrator to analyze audit records for traffic in real time and search the security accumulated security audit records in the extended audit record analysis environment.

8.5.6 FAU_SAR.3 - FAU_View

The TOE allows the administrator to selectively search audit records by defining search conditions.

8.5.7 FAU_STG.1 - FAU_Prevent

The TOE allows the administrator to store audit records by system, date, and type.

8.5.8 FAU_STG.3 - FAU_Prevent

The TOE checks the remaining audit data space. When the remaining space crosses the threshold, the TOE generates alarms, stops security functions, or takes other measures to prevent the loss of audit records.

8.5.9 FAU_STG.4 - FAU_Prevent

When the audit storage becomes full, the TOE informs the administrator by sending an e-mail or opening a message box.

8.5.10 FCS_COP.1 – FCS_ESP, FCS_AH

When the TOE establishes encrypted communication with the VPN gateway, the TOE uses the cryptographic hash algorithm specified by the government agency or a standard algorithm defined by the RFC.

8.5.11 FCS_CKM.1 – FCS_IKE

The TOE generates cryptographic keys using one of the algorithms specified by the government agency.

8.5.12 FCS_CKM.2 - FCS_ IKE

The TOE implements an IKE daemon at the application layer and distributes cryptographic keys in a standardized way specified in the IETF.

8.5.13 FCS_CKM.4 -FCS_KEYDEST

The TOE destroys cryptographic keys in a secure way by setting parameters important for security as 0.

8.5.14 FDP_ACC.2 – FDP_AdminNetwork

The TOE controls administrator access by packet source or destination through the use of the administrator security policy.

8.5.15 FDP_ACF.1 - FDP_AdminNetwork

The TOE provides an access control function according to the administrator access control security that the administrator predefined based on the security attribute.

8.5.16 FDP_DAU.1 – FDP_VPN

When the TOE establishes encrypted communication with the VPN gateway, the TOE applies the integrity algorithm to all packets carrying data. For the communication channels with the administrator's security management interface, the TOE applies the integrity algorithm.

8.5.17 FDP_IFC.1 Subset Information Flow Control – FDP_VPN

The TOE controls the flow of information transmitted to/from the TOE according to the VPN security policy.

8.5.18 FDP_IFC.2(1) Complete Information Flow Control - FDP_PacketFiltering

The TOE can completely control information flow according to the packet-filtering security policy predefined by the administrator to control information flow in relation to all traffic passing through the TOE.

8.5.19 FDP_IFC.2(2) Complete Information Flow Control – FDP_Proxy

The TOE can completely control information flow according to the proxy security policy predefined by the administrator to control information flow in relation to all traffic passing through the TOE.

8.5.20 FDP_IFC.2(3) Complete Information Flow Control - FPR_SNAT, FPR_DNAT, FPR_Redirect

The TOE can completely control information flow according to the address translation security policy predefined by the administrator to control information flow in relation to all traffic passing through the TOE.

8.5.21 FDP_IFF.1(1) Single-layer Security Attribute - FDP_VPN

The TOE provides a function that can control and apply the VPN security policy to control information flow based on the security attribute.

8.5.22 FDP_IFF.1(2) Single-layer Security Attribute - FDP_PacketFiltering

The TOE provides a function that can control and apply the packet-filtering policy to control information flow based on the security attribute.

8.5.23 FDP_IFF.1(3) Single-layer security attribute - FDP_Proxy

The TOE provides a function that can control and apply the proxy security policy to control information flow based on the security attribute.

8.5.24 FDP_ IFF.1(4) Single-layer security attribute - FPR_SNAT, FPR_DNAT, FPR_Redirect

The TOE provides a function that can control and apply the address translation security policy to control information flow based on the security attribute.

8.5.25 FIA_AFL.1 – FIA_IAFailure

When the administrator authentication failure count crosses the threshold, the TOE will inform the administrator by generating an alarm.

8.5.26 FIA_ATD.1 – FMT_Object

When a security policy is executed based on the user object, the TOE allows the administrator to define and apply the security attributes.

8.5.27 FIA_UAU.2 – FIA_PwdAuth , FIA_UPWDSet

After authenticating an administrator who can access the TOE, the TOE applies the security policy.

8.5.28 FIA_UAU.4 - FIA_OTPAuth

The TOE authenticates the administrator using a one-time password.

8.5.29 FIA_UAU.7 - FIA_PwdAuth , FIA_UPWDSet

When authenticating an administrator user, the TOE hides cryptographic data using special characters.

8.5.30 FIA_UID.2 - FDP_PwdAuth

Before the administrator or user uses a security function of the TOE, the administrator shall enter the ID so that the TOE can judge the administrator's or user's authority (such as backup or policy change)

8.5.31 FIA_SOS.1 - FIA_PwdAuth , FIA_UPWDSet

The TOE applies a mechanism to the minimum length, collation rule, and change cycle.

8.5.32 FMT_MOF.1 – FMT_NICManage, FMT_PPPManage, FMT_RoutingManage, FMT_ARP , FMT_DHCP, FMT_HostDNSSet, FMT_TimeSet, FMT_AuditSetup, FMT_AdminSetup, FMT_Firmup, FMT_SysStatus, FMT_SaveConfig, FMT_Wizard

Only the authorized administrator can access security and management functions after passing the identification and authentication processes. Only the administrator can use TSF functions such as starting or stopping the TOE and change security policies.

8.5.33 FMT_MSA.1 - FMT_NICManage, FMT_PPPManage, FMT_RoutingManage, FMT_ARP , FMT_DHCP , FMT_HostDNSSet, FMT_TimeSet, FMT_AuditSetup, FMT_AdminSetup, FMT_Firmup ,FMT_SysStatus, FMT_SaveConfig

The TOE provides a security management environment where only authorized administrators can manage networks, time, users, IPSec objects, and security levels.

8.5.34 FMT_MSA.2 - FMT_NICManage, FMT_PPPManage, FMT_RoutingManage, FMT_ARP , FMT_DHCP

The TOE validates the setup data used in the TOE and all user security attributes.

8.5.35 FMT_MSA.3 – FMT_Policy

In the default case, the packet-filtering security policy is not used. Instead, the proxy security policy is used.

8.5.36 FMT_MTD.1(1) – FMT_Statistics

The TOE generates various types of statistical data using stored audit data.

8.5.37 FMT_MTD.1(2) – FMT_AuBackup

The TOE backs up or recovers important files composing the TOE.

8.5.38 FMT_MTD.1(3) - FMT_Policy

The TOE allows the authorized administrator to manage administrator security policy, the VPN security policy, the packet-filtering security policy, and the proxy security policy.

8.5.39 FMT_MTD.1(4) - FMT_Object

The TOE allows the authorized administrator to manage cryptographic key attributes.

8.5.40 FMT_MTD.1(5) – FMT_Object

The TOE allows the authorized administrator to manage identification and authentication data.

8.5.41 FMT_MTD.1(6) - FMT_TimeSet

The TOE allows the authorized administrator to manage TOE time.

8.5.42 FMT_MTD.2 - FMT_AuBackup, FMT_LogServerPolicy

The TOE can define the maximum authentication failure count, time interval, maximum number of users per proxy, and the storage capacity through the security management interfaces of the console or web provided by the TOE.

8.5.43 FMT_MTD.3 - FMT_Object, FMT_Policy

The TOE validates the security policy and the objects of the security policy set by the administrator.

8.5.44 FMT_SMR.1 - FMT_AdminSetup

The TOE can give administrator authority to the authorized user and augment authorities.

8.5.45 FMT_SMF.1 - FM_SysSetup

The TOE allows the administrator to set up the back up procedure and the network environment by providing web interfaces.

8.5.46 FPR_UNO.4 –F PR_Status

The TOE assures that the authorized administrator can check the TOE resources and process status in order to manage the TOE.

8.5.47 FPT_AMT.1 – FPT_ABTest

The TOE detects interface-related errors upon start and during operation to maintain communication with the VPN and operation of the VPN gateway.

8.5.48 FPT_RPL.1 – FDP_VPN

When the IKE daemon establishes tunnels with the VPN gateway and during communication with the VPN gateway, the TOE detects and rejects the replay attacks.

8.5.49 FPT_RVM.1 - FDP_PacketFiltering, FDP_VPN

The TOE filters all packets passing the TOE.

8.5.50 FPT_STM.1 - FMT_TimeSet

The TOE can obtain reliable time information from the NTP server or allows a trusted administrator to change the TOE time.

8.5.51 FPT_TST.1 – FPT_Integrity

The TOE checks the integrity of the TSF data (configuration and binary files) and shows the result to the administrator.

8.5.52 FPT_TST.2 - FPT_Integrity

When an integrity error is found in the TSF data (configuration and binary files), the TOE informs this to the administrator and generates audit records.

8.5.53 FPT_SEP.1 - FMT_UserObj, FDP_Proxy

When executing the security function, the TSF divides the area into reliable and unreliable.

8.5.54 FTP_ITC.1 – FPT_AdminTrusted

The TOE establishes encrypted communication with a trusted product. To establish encrypted communication, the TOE supports the SSL protocol. The SSL protocol is created by the library that the Open SSL encryption toolkit provides.

8.5.55 FTA_SSL.1 – FTA_SessionLock

When an authorized administrator logs in to the security management server and remains idle for more than the specified time, the TOE will lock the session.

8.5.56 FTA_SSL.3 - FTA_SessionLock , FTA_SessionKill

If the authorized administrator remains idle for a certain time set by the administrator or general user, the corresponding communication session will automatically disconnect. The administrator and general users can access the TOE when a communications session is established again.

8.6 Compliance with TSF SOF(Strength of Function)

The TOE confirms to the SOF-medium specified in [FW_PP_V1.1] and [VPN_PP_V1.1] to which this Security Target conforms. General cryptographic operation and the one-time password method provided by the TOE all satisfy the cryptographic grades defined in the protection profile.

8.7 Compliance with TOE security Assurance Requirements

The rationale for the assurance requirements of EAL 3+ is as follows:

[Table 8-9] Assurance Measures Mapping

Assurance Measures / Assurance Component ID	Configuration Management	Delivery Documents	Installation Guide	Function specifications서	Basic Design	Implementation Verification Specification	Low-level design서	Administrator Guidance document	User documentation Guidance	Development Document Security	Development Document Tool	Function Test Document	Module Test Document	Vulnerability분석서
ACM_CAP.3	X													
ACM_SCP.1	X													
ADO_DEL.1		X												
ADO_IGS.1			X											
ADV_FSP.1				X										
ADV_HLD.2					X									
ADV_IMP.2						X								
ADV_LLD.1							X							
ADV_RCR.1				X	X	X	X					X		
AGD_ADM.1								X						
AGD_USR.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	X	
AVA_MSU.1								X						
AVA_SOF.1														X
AVA_VLA.2														X

8.7.1 ACM_CAP.3 (Approval Control)

To assure all changes are approved and to guarantee proper functionality and use of the configuration management system, configuration management documents are provided.

8.7.2 ACM_SCP.1 (TOE Configuration Management Scope)

Configuration management documents are provided to assure that all changes are approved and controlled in the configuration.

8.7.3 ADO_DEL.1 (Delivery Procedure)

Delivery documents are provided to assure facilities and procedures that can deliver and control the TOE without any change.

8.7.4 ADO_IGS.1 (Installation, Generation, and Start Procedures)

To assure that the TOE is installed, generated, and started in a safe manner that the developer intended, installation guide documents are provided.

8.7.5 ADV_FSP.1 (informal function specifications)

Functional specification documents are provided to describe user interfaces, TSF operations, and the TOE security functional requirements.

8.7.6 ADV_HLD.2 (Basic Design Separating Security Functions from Non-security Functions)

The basic design document describes major elements (sub-systems) of the TSF and the relations between the sub-system and the functions it provides. To assure that the TOE provides a proper structure to implement the TSF requirements, the basic design document is provided.

8.7.7 ADV_IMP.2 (The subset of the Implementation Representation)

To help operators understand and analyze operations of the TSF in detail, the implementation verification specification documents are provided.

8.7.8 ADV_LLD.1 (Declarative low-level design)

Low-level design documents are provided to describe internal operations of the TSF and interactions and dependency between modules and to ensure the low-level design of the TSF sub-system is accurate and effective.

8.7.9 ADV_RCR.1 (Informal Correspondence Verification)

To ensure correspondence among various expressions of the TSF (TOE summary specification, function specification, basic design, low-level design, and implementation expression), the correspondence analysis is included in the function specification, the basic design, the low-level design, and the implementation representations.

8.7.10 AGD_ADM.1 (Administrator Guidance documentation)

The administrator guidance documents are provided for the operation personnel so they can configure, maintain, and manage the TOE in a secure manner.

8.7.11 AGD_USR.1 (User Guidance documentation)

The user guidance documents are provided for TOE users and others who will use the external interfaces besides the administrator.

8.7.12 ALC_DVS.1 (Security Countermeasure Identification)

The development security documents are provided to protect the TOE with physical resources, procedures, human resources, and other security users in the development environment.

8.7.13 ALC_TAT.1 (Well-defined Development Tool)

To ensure that the TOE is correctly defined and correct and accurate development tools are used for the development of the TOE, development tool documents are provided.

8.7.14 ATE_COV.2 (Test Coverage Analysis)

To assure that the TSF is systematically tested according to the functional specifications, the function test documents are provided.

8.7.15 ATE_DPT.2 (Low-level Design Test)

To ensure that the TSF sub-system and the TSF module are correctly implemented in the TSF sub-system phase and the module phase, the module test documents are provided.

8.7.16 ATE_FUN.1 (Functional Test)

To ensure that all security functions are executed as specified, the functional test documents are provided.

8.7.17 ATE_IND.2 (Independent Test)

To ensure that the security functions are executed as specified, the functional test documents are provided.

8.7.18 AVA_MSU.1 (Guidance Documentation Examination)

The fault analysis is included in the administrator guidance and user guidance documents to describe all functions of the guidance documents and to ensure that guidance documents have internal consistence and safety procedures are included in the operation.

8.7.19 AVA_SOF.1 (Evaluation of TSF Strength)

A vulnerability analysis report is provided to describe quantitative or statistical result for the security behaviors of the lower security mechanism and to determine the strength of the security behavior to adapt to the result.

8.7.20 AVA_VLA.2 (Independent Vulnerability Analysis)

The TOE identifies security vulnerabilities and provides a vulnerability analysis report to ensure that these vulnerabilities will not be intentionally misused.

8.8 Rationale for Satisfaction with Dependencies

8.8.1 Dependency of Security Functional Requirements

The security functional requirements and the assurance requirements used for the preparation of the TOE and the Security Target have the following dependency relationship. There is no independent component.

[Table 8-10] SFR Satisfaction with Dependency

Component	Dependency	Inclusion Status
FAU_ARP.1	FAU_SAA.1	Included.
FAU_GEN.1	FPT_STM.1	Included.
FAU_SAA.1	FAU_GEN.1	Included.
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Included.
FAU_SAR.1	FAU_GEN.1	Included.
FAU_SAR.3	FAU_SAR.1	None.
FAU_STG.1	FAU_GEN.1	Included.
FAU_STG.3	FAU_STG.1	Included.
FAU_STG.4	FAU_STG.1	Included.
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4, FMT_MSA.2	Included.
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Included.
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Included.
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2	Included.
FDP_ACC.2(1)	FDP_ACF.1	Included.
FDP_ACC.2(2)	FDP_ACF.1	Included.
FDP_ACC.2(3)	FDP_ACF.1	Included.
FDP_ACF.1(1)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.2 Selection
FDP_ACF.1(2)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.2 Selection
FDP_ACF.1(3)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.2 Selection
FDP_DAU.1	None.	None.
FDP_IFC.1	FDP_IFF.1	Included.
FDP_IFC.2(1)	FDP_IFF.1	Included.

FDP_IFC.2(2)	FDP_IFF.1	Included.
FDP_IFC.2(3)	FDP_IFF.1	Included.
FDP_IFC.2(4)	FDP_IFF.1	Included.
FDP_IFC.2(5)	FDP_IFF.1	Included.
FDP_IFF.1(1)	FDP_IFC.1, FMT_MSA.3	Included.
FDP_IFF.1(2)	FDP_IFC.1, FMT_MSA.3	Included.
FDP_IFF.1(3)	FDP_IFC.1, FMT_MSA.3	Included.
FDP_IFF.1(4)	FDP_IFC.1, FMT_MSA.3	Included.
FDP_IFF.1(5)	FDP_IFC.1, FMT_MSA.3	Included.
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.2*
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.2*
FIA_ATD.1	None.	None.
FIA_SOS.1	None.	None.
FIA_UAU.2	FIA_UID.1	FIA_UID.2**
FIA_UAU.4	None.	None.
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2*
FIA_UID.2	None.	None.
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	Included.
FMT_MSA.1	[FDP_ACC1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	Included.
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	Included.
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Included.
FMT_MTD.1(1)	FMT_SMR.1, FMT_SMF.1	Included.
FMT_MTD.1(2)	FMT_SMR.1, FMT_SMF.1	Included.
FMT_MTD.1(3)	FMT_SMR.1, FMT_SMF.1	Included.
FMT_MTD.1(4)	FMT_SMR.1, FMT_SMF.1	Included.
FMT_MTD.1(5)	FMT_SMR.1, FMT_SMF.1	Included.
FMT_MTD.1(6)	FMT_SMR.1, FMT_SMF.1	Included.
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	Included.
FMT_MTD.3	ADV_SPM.1, FMT_MTD.1	Included.
FMT_SMR.1	FIA_UID.1	FIA_UID.2**
FPT_AMT.1	None.	None.
FPT_RPL.1	None.	None.
FPT_RVM.1	None.	None.

FPT_SEP.1	None.	None.
FPT_STM.1	None.	None.
FPT_TST.1	FPT_AMT.1	Included.
FPT_TST.2	FPT_TST.1	Included.
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2*
FTA_SSL.3	None.	None.
FTP_ITC.1	None.	None.

* - FIA_UAU.1 selected FIA_UAU.2 which is in a hierarchical relationship to conform to the dependency requirement.
** - FIA_UID.1 selected FIA_UID.2 which is in a hierarchical relationship to confirm to the dependency requirement.

8.8.2 Dependency of SFR Requirements in Hierarchical Relationship

All functional components specified in this Security Target except FMT_MSA.2 and FMT_MTD.3 meet the dependency requirement. The assurance requirements EAL3+ according to the government agency profile which complies with this Security Target is considered acceptable for the TOE for the government agency. ADV_SPM.1 informal TSP model has not been selected.

FIA_AFL.1, FIA_UAU.7, and FTA_SSL.1 having a dependent relationship with FIA_UAU.1 and FIA_UAU.2 having a hierarchical relationship with FIA_UAU.1 conform to the dependency requirement. FIA_UAU.2 and FMT_SMR.1 having a dependent relationship with FIA_UID.1 and FIA_UID.2 having a hierarchical relationship with FIA_UID.1 conform to the dependency requirement.

Each assurance package specified in the Common Criteria for the Information Protection System conforms to the dependency requirement so the rationale for this is not included in this document. [Table 8-11] shows dependency conformation status of the augmented assurance requirements, and this Security Target specification conforms to the dependency requirement of all assurance requirements.

[Table 8-11] Satisfaction with Dependency of Assurance Requirements Augmented to EAL3

Component	Dependency	Inclusion Status
ADV_IMP.2	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1	Included.
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1	Included.
ALC_TAT.1	ADV_IMP.1	Included.
ATE_DPT.2	ADV_HLD.2, ADV_LLD.1, ATE_FUN.1	Included.
AVA_VLA.2	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	Included.

Bibliography

- Announcement 2005-25 by Ministry of Information and Communication, Common Criteria for the Information Protection System
- VPN Protection Profile for Government Agency V1.1 [VPN_PP_V1.1]
- Firewall Protection Profile for Government Agency V1.1 [FW_PP_V1.1]
- Common Criteria (CC) V2.2 Final Interpretation, October 2005
- Common Evaluation Methodology for Information Technology Security