OULLIM Information Technology Inc.

SECUREWORKS IPSWall 1000 V4.0

Security Target

Version 1.18

Contents

Table Contents

1 ST Introduction

Chapter 1 provides identification information and a general summary of the ST. This ST describes the product type, scope and boundaries of the TOE (chapter 2), defines threats and assumptions of the TOE (chapter 3), describes security objectives and security requirements (chapter 4, 5), explains the security functions which the TOE provides (chapter 6), identifies the protection profile claimed (chapter 7) and lastly, provides rationale (chapter 8).

1.1 Security Target and TOE Identification

This section provides the necessary information to identify and control this ST and the TOE.

ST Title:	OULLIM IT, Inc. SECUREWORKS IPSWall 1000 V4.0 Security Target Version 1.18
ST Version:	V1.18
Written Date :	AUG/19/2005
Written by	OULLIM IT, Inc. Mi-kyung Kim, Soo-yeon Lee
TOE Identification:	SECUREWORKS IPSWall 1000 V4.0 S/W
CC Identification:	Common Criteria for Information Technology Security Evaluation V2.2 Final Interpretation published until JUNE 2005
Relevant PP:	Network Intrusion Prevention System Protection Profile V1.0 , May/24/2005
Assurance Level	EAL4
Evaluator:	Korea Information Security Agency (KISA)
Key Words:	Intrusion Prevention System(IPS), Identification and Authentication, Firewall, Information Flow Control

[Table 1-1] ST and TOE Identification

1.2 Conventions and Terminology

This ST was initially written in Korean with abbreviations and terminology in English for clear understanding of the meaning. This section identifies the terms used in this ST.

1.2.1 Conventions

The notation, format, and conventions used herein conform to the Common Criteria for Information Technology Security Evaluation (hereinafter Common Criteria or CC).

The Common Criteria defines four operations used in the security functional requirements.

- Refinement : The refinement operation is used to further restrict a requirement by adding detail to the CC or the claimed PP. The result of the refinement operation is denoted by **bold text**.

- Selection : The selection operation is used to select one or more options provided by the CC or the claimed PP in stating a requirement. Selections are denoted by *underlined italicized text*.

- Assignment : The assignment operation is used to assign a specific value to a parameter unspecified by the CC or the claimed PP, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

- Iteration : The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

- Security Target Writer : The security target writer operation is used to denote points in which the final determination of attributes is left to the security target writer. Security target writer operations are indicated by the words {determined by the security target writers} in braces.

Application notes are provided to help the developer clarify the intent of a requirement, identify implementation choices and define “pass/fail” criteria for a requirement. For those components where application notes are appropriate, the application notes will follow the requirement component.

1.2.2 Terminology

Many terms are defined in section 2.3 of the CC part 1. The following terms are a part of those definitions listed here to aid the users of this ST.

Audit Trail - A set of disc record that recorded the user accessed to the system and the user's behavior.

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

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

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

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

Log Server – The name of a service in charge of security audit management in the TOE.

Log Administrator – An administrator that possesses log related configuration authorities only.

Iteration - The use of a component more than once with varying operations.

Security Management Server – The daemon (service) name of a TOE that identifies and authenticates an administrator and provides security management service to an authorized administrator through a web interface. The administrator establishes the security policy by connecting to this security management server.

Security Target (ST) - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Protection Profile (PP) - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Anomaly Detection - Anomaly detection is a detection technique based on a statistical method. This technique draws up a profile about user's normal behaviors, and then detects any abnormal behavior that conflicts with the profile.

Human User – Any person who interacts with the TOE

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

Selection - The specification of one or more items from a list in a component.

Identity - A representation (e.g. a string) uniquely identifying an authorized user.

Element - An indivisible security requirement.

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

Operation1 – Allowing components of the CC to counter specific threats or to meet specific security policy. (e.g. iteration, assignment, selection, refinement)

Operation2 – calculation or activation defined by command or pseudo command.

Threat Agent - An unauthorized user or external IT entity that imposes threats like illegal access, modification, or deletion of assets.

External IT Entity - Any IT product or system, trusted or untrusted, outside of the TOE that interacts with the TOE.

Authorized Administrator - Administrators of the TOE are categorized by authority into root administrator, log administrator, and policy administrator. With no further explanation, an authorized administrator mentioned in the ST refers to the root administrator with full authority. Log and policy administrators are configured by root administrator, and the authorized administrator possessing authority may not perform administrative functions that exceed the authority.

Authentication Data - Information used to verify the claimed identity of a user.

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

Refinement - The addition of details to a component.

Policy Administrator – An administrator that possesses policy related configuration authorities only.

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

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

Subject - An entity within the TSC that causes operations to be performed.

Final Interpretation – An official document published by CCIMB with additional interpretation or correction of errors in the official CC.

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

Abstract Machine – The abstract machine could be a hardware/firmware platform, or it could be some known and assessed hardware/software combination acting as a virtual machine. The underlying abstract machine used in this functional package refers to an operation system in case the TOE is an application program, a firmware/hardware in case the TOE is an operation system.

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

Class - A grouping of families that share a common focus.

Target of Evaluation (TOE) - An IT product or system and its associated guidance documentation that is the subject of an evaluation.

Evaluation Assurance Level (EAL) - A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Family - A grouping of components that share security objectives but may differ in emphasis or rigour.

Packet – The unit of data using the data transmission on the Internet. The packet transmission doesn't sequentially transmit to data between the places, the form of the packet that transmitting data divided into appropriate size, then the packets transmit packet by packet. Each packet includes data source, address or control information of control code as well as data of a regular size.

Assignment - The specification of an identified parameter in a component.

Extension - The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

Deep Inspection (DI) – The rules that define pattern, level, service, data size, IP datagram and details of Transport datagram that define an attack to reject abnormal packets and DoS attacks.

DI Rule Update Server – A server that updates the HOTLIST, which is the latest list of DI rules of the TOE.

HOTLIST – A database to maintain the latest list of DI rules. HOTLIST, downloaded from the DI Rule Update Server in SECUREWORKS, is not subject to deletion or modification even by an authorized administrator.

Intrusion Prevention System (IPS) – A system that detects any illegal intrusion attempt, the Worm on the network, and the interception of traffic.

SECUREWORKS IP (SWIP) – As a virtual IP driver of the SECUREWORKS, it is core engine that performs major functions of IPS.

TOE Security Functions (TSF) - A set of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF data - Data created by and for the TOE, that might affect the operation of the TOE.

TSF Scope of Control (TSC) - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

1.3 ST Overview

This ST defines the IT security requirements of the SECUREWORKS IPSWall 1000 V4.0 S/W. SECUREWORKS IPSWall 1000 V4.0 (hereinafter SECUREWORKS) is an appliance IT product system, installed the SECUREWORKS S/W which provides intrusion prevention system (IPS) on the SWOS (dedicated OS). SECUREWORKS, as a network boundary protection type network security solution, provides Firewall, VPN, IPS, and QoS functions. The evaluation scope of SECUREWORKS covers the S/W that provides intrusion prevention system which is able to actively cope with any attack using the worm on the Internet or the application layer.

SECUREWORKS, connected in-line at the connection point of the internal network and the external network connected to the Internet, detects and rejects in real-time the intrusion or attack of any network traffic that flows in from outside.

1.4 CC Conformance

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

- Network Intrusion Prevention System Protection Profile V1.0 May/24/2005 (hereafter [IPSPP])
- Common Criteria V2.2 Part 1
- Common Criteria V2.2 Part 2 conformant
- Common Criteria V2.2 Part 3 conformant
- Evaluation Assurance Level 4(EAL4) conformant
- SOF-medium Claim

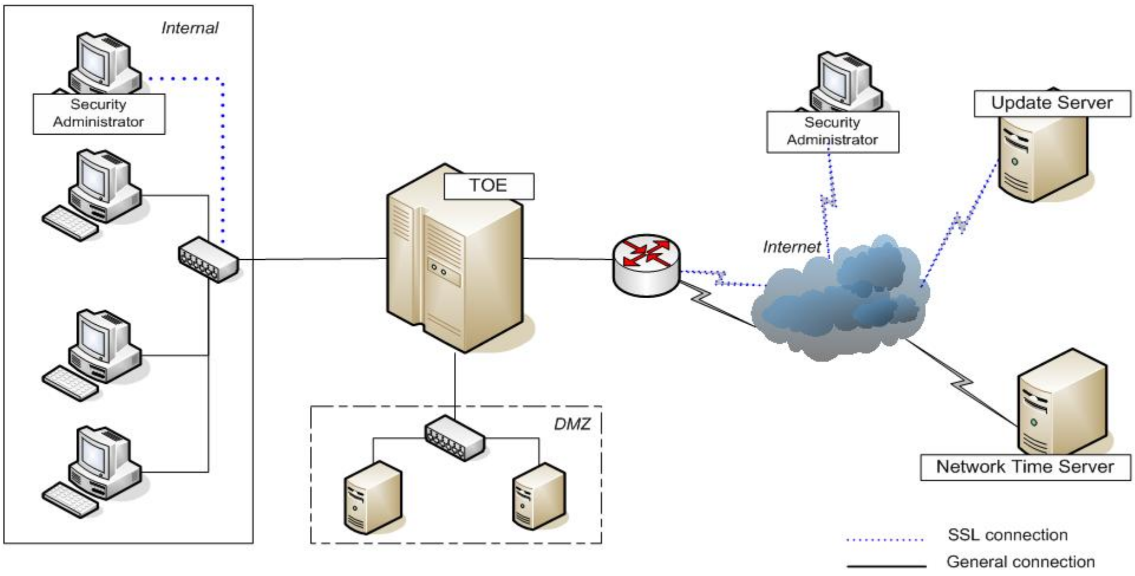
2 TOE Description

This chapter briefly describes the product type and configuration of the TOE, and provides the background knowledge for an evaluation of the TOE.

The TOE meets EAL4 of the CC V2.2 Part 3, assurance requirements.

2.1 Product Type

2.1.1 TOE configuration



[Figure 2-1] General TOE Network configuration

SECUREWORKS, as shown in [Figure 2-1], operates in-line at the connection between the internal network and the Internet, or the junction between the internal and external network. The administrator controls SECUREWORKS through local or remote IT entities. Internal hosts of the center site and the DMZ system send data in accordance with the security policy when communicating with an unreliable external entity on a public network.

SECUREWORKS, a network integrated security solution, is an appliance equipment providing network security functions such as the IPS, VPN, and Firewall. The evaluation scope of SECUREWORKS covers the S/W that provides the IPS function.

The TOE is a network intrusion prevention system based on existing Firewall technology, is implemented to detect and cope with the worm on the Internet or application layer attacks. The detailed functions of the IPS that SECUREWORKS S/W provides are as follows:

- Packet Filtering
- Deep Inspection
- Attack Pattern Detection Using HOTLIST
    - Protocol Anomaly Detection
    - Traffic Anomaly Detection (DDoS Traffic Control)

The TOE protects internal network assets from any known or unknown attacks. The Deep Inspection function detects and rejects malicious traffic by examining L3~L7 packets. The Protocol Anomaly Detection function examines protocols between L4~L7 and promptly rejects any traffic that does not meet protocol standards. Traffic Anomaly Detection function detects DDoS or traffic surge of normal traffic using statistical method, and provides network shared asset protection function by restricting or rejecting the traffic.

Malicious traffic includes accessing unauthorized services, any network packet with abnormal packet structure, packets with computer worms/viruses, and packets that launch DoS attacks which damage the availability of internal computer assets.

The TOE defines the information flow rules based on the security policy and controls the traffic between an internal network and an external network in accordance with the defined rules. The TOE enforces the packet filtering security policy or the intrusion prevention security policy (in other words, the DI policy). Packets passing (incoming and outgoing) through the TOE are enforced the packet filtering policy on a network layer, then pass through the DI policy. The DI policy allows the access to any packet other than attack patterns, Worms, or anomaly packets.

The TOE, in order to maintain rules of the attack patterns about the latest attacks, updates and applies the latest attack rules from a trusted update server(i.e. DI Rule Update Sever). This can maximize avoiding the attacks that find and exploit new vulnerabilities.

User of the TOE can be only the authorized administrator. The three roles of the authorized administrators are the Root administrator, the Log administrator, and the Policy administrator. Generally an authorized administrator means the Root, Log, and Policy administrators. The roles of the Log administrator and the Policy administrator are mentioned when necessary.

2.1.2 TOE Environment

2.1.2.1 IT Environment

The IT environment of the TOE includes DI rule update server, NTP (Network Time Protocol) server, and remote administrator PC. The TOE saves audit records using the time information received from the NTP server for a sequential audit recording. The TOE and the NTP server communicate through the Network Time protocol implemented by RFC 1305. The TOE communicates with the remote administrator console or the DI rule update server using SSL protocol for secure communication.

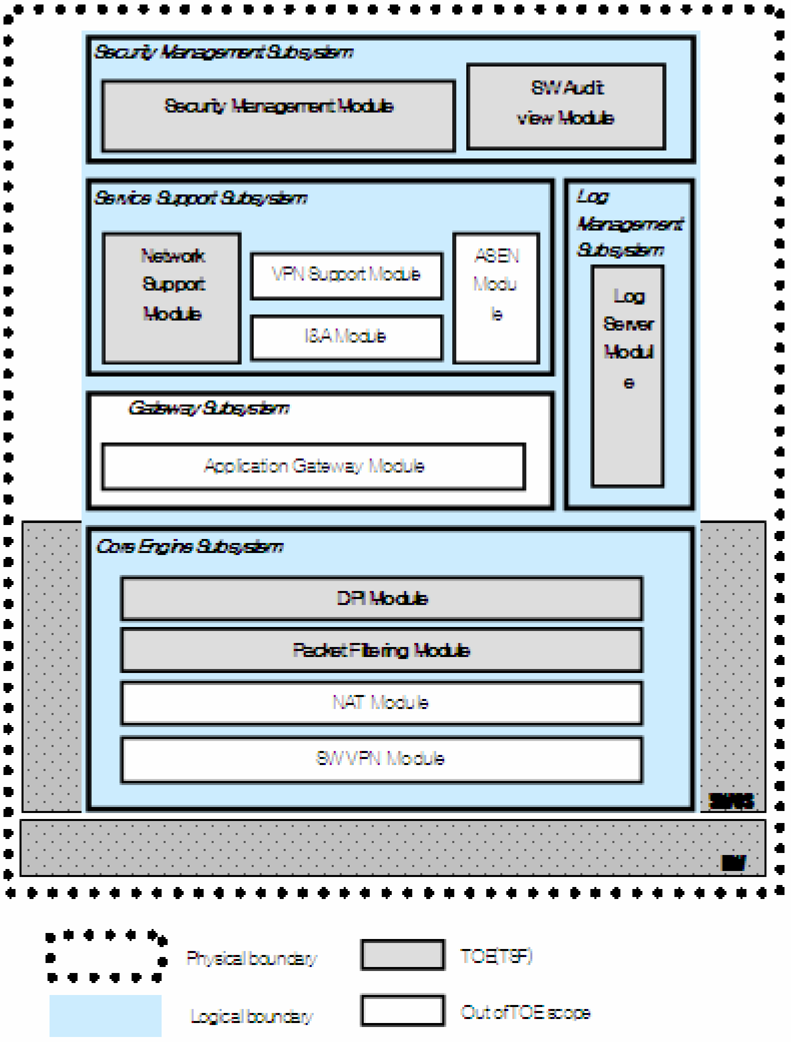
2.1.2.2 Operational Environment

The SECUREWORKS is installed in-line at the connection point between the internal network and the external network connected to the Internet. SECUREWORKS is appliance equipment operating on dedicated OS (SWOS V4.0). The TOE is used in an environment where threat agents with a moderate level of expertise may exist. Threat agents with a moderate level of expertise can easily obtain exploitable vulnerability information and tools with which they may damage or obtain their target assets. The TOE is used to protect internal assets from these threat agents with a moderate level of expertise.

2.2 Product Component

The TOE is composed of the following four components:

- Security Management
- Core Engine
- Service Support
- Log Management



[Figure 2-2] TOE Internal Logic Diagram

Security management component, in forms of daemon, performs various operations and management functions (security policy configuration, deletion, review function and security data protection function) for managing TSF and TSF data. Access right to the security management component is granted only an authorized administrators who success administrator identification and authentication to ensure that only authorized administrators access the TOE. The TSF data transferred from a trusted external IT entity to the security management component of the TOE is protected by SSL protocol.

Core engine component performs the user data protection function based on the security policies established in the security management. The core engine component, unlike the other components, is attached to Kernel of OS and performs security functions. The security functions provided by the core engine component are as follows.

- Packet filtering – selectively controls user data (packet) flow between internal network and external network at network layer level in conformance with security policies. Results of the control are expressed as Allow or Deny, and basically the Deny rule is applied.

- DI (Deep Inspection) – defines attack pattern in terms of an attack type and an attack rule which composed of risk level, network service, data size information and so on. Check whether matching or not the defined attack pattern and disconnect the associated session matching the attack pattern. Check and block the packet access to the TOE based on the protocol anomaly rule and the traffic anomaly rule.

Service support component performs network related functions of the TOE such as network interface state testing.

Log management stores and maintains audit records of security related events occurred while enforcing security functions. And it monitors and analyzes the audited events and alarms in case a potential violation of the TSP

2.3 Scope and Boundaries of the Evaluated Environment

This section generally explains physical/logical scope and boundaries of the TOE.

2.3.1 Physical Scope and Boundaries

The SECUREWORKS composed of hardware and software is shown in [Table 2-1].

Software	Environment	
	Hardware	OS
SECUREWORKS IPSWall 1000 V4.0 S/W	CPU – Celeron 2.6GHz Chipset – 845 GV+Winbond 83627 HF Memory - DDR 512MB Ethernet Ports – 10/100 Fast Ethernet 4EA PCI Slot - 32-Bit/33 Mhz PCI Slot(Accelerator) IPsec Accelerator - Cavium Nitrox CN1005i Serial Interface - DB9 + 1cDB9(for modem) Storage - 3.5 inch HDD PATA type + Compact Flash HDD – 80 GByte or more Power Supply - Single Free Voltage	SWOS V4.0 (dedicated OS)

[Table 2-1] Software/Hardware Platform

The TOE is SECUREWORKS V4.0 software which implements the security functions for packet filtering and intrusion detection. Hardware parts and dedicated OS (SWOS V4.0) are excluded from the evaluation. IPSec accelerator is also excluded since VPN function is not included in the scope of the TOE.

2.3.2 Logical Scope and Boundaries

2.3.2.1 TOE Security Functions

The TOE generally provides the following security functions.

Security Management – The TOE allows only authorized administrators to administer and operate the information flow security policy. This is done through an encrypted web interface using the SSL. Only authorized administrators may view or manage the TSF data related to the TSF, security attributes, and authentication data.

Security Audit – The TOE allows only authorized administrators to view audit records. Any important security event that occurs in the TOE, all the information of network packet and the success or failure for information flow of the packet are stored in audit storage in an order of time with a time-stamp. Saved audit records can be review and searched on various conditions.

User Data Protection – The TOE performs user data protection through the packet filtering security policy and the intrusion prevention security policy of network layers. The TOE enforces security policies by performing a core security function that implement the information flow control for all the packets passing through the TOE. The TOE identifies an external IT entity and a remote PC of administrators to grant only legitimate external IT entities and authorized administrators the access right to the TOE. In this case, the TOE creates a trusted channel using SSL protocol.

Identification and Authentication (I&A) – The TOE provides passwords mechanism as an authentication mechanism for authenticating administrators. The TOE communicates with the remote PC of administrator using SSL protocol in order to encrypt the authentication data for protection against discloser by attacker. Also, the TOE, when there is no activity in a session to which an authorized administrator is connected, locks the session and authenticates the administrator again.

TSF Protection - The TOE tests the correct operation of TSF periodically, and resets abnormal operations to allow it to operate normally. The TOE protects TSF data and

TSF by verifying the integrity for TSF data and execution programs. Also, the TOE changes its NIC state to Link Down when a failure occurs and the super daemon restarts the dead daemons by checking other daemons periodically.

2.3.2.2 Out of TOE Scope

The following are the functions that are not included in the TOE scope:

a) QoS policy function of the packet filtering security policy and enable/disable function of corresponding rules in case of Frame Relay network down

b) NAT which changes the source or destination address

c) Application Gateway function that can control various L7 protocols (HTTP, FTP, TELNET, RLOGIN, SMTP, POP3, IMPA4, NNTP, H.323, FTP Kernel).

d) VPN Function : the method for encryption key exchange to create a virtual private network, generation of cryptographic key for VPN communication, additional registration of certificate, security methods, CA configuration function

e) Statistics or Audit Record Back-up and Transfer related function
   - Log Client/Server function to store audit records of SECUREWORKS in other SECUREWORKS
   - Deletion or Compressed Storage function of audit records, statistics data, and session data
   - Back-up function of audit records on separate devices
   - Interoperability with WebTrends Firewall Suite
   - Statistics Generation and Viewing function of audit records
   - Addition, Deletion, and Modification function of SNMP to transfer audit records

f) Status Viewing Function – current application state viewing function of NAT, VPN, QoS

g) Backup and restoration function of important configuration information of SECUREWORKS

h) Virus engine and malicious information DB update configuration function

i) Network related configuration functions
   - Interface connection configuration, interface status test, interface load balancing configuration, location configuration functions
   - Addition, deletion, review functions of static routing information

- RIP configuration function is provided.
- Addition and deletion function of ARP information
- Addition/Deletion of SNMP access list table – this is configured to receive replies from the systems that receive network information or host information using SNMP protocol.

j) Country and language selection, user name establishment, license request and registration functions

k) Automatic version (image) update function of SECUREWORKS IPSWall 1000 v4.0

l) Product information and system information display function of SECUREWORKS

m) SecureDNS function which provides separated external and internal DNS service

n) Automatically assign the IP address to internal user

o) Local Console Management Function

p) Identification and authentication function
- General user authentication function used in gateway and packet filtering
- The function that discontinues or delays when a general user fails the authentication more than the established number of times
- Termination of the user session
- Identification and authentication method (general user and administrator) using OTP
- Other authentication methods – authentication function using LDAP server for unregistered users.
- Identification and authentication of an administrator who possesses user control rights

q) Recovery
- HA
- Clustering
- Router backup function using VRRP
- Execution of backup for circuit or interface. The function that allows VPN circuit backup using PPP circuit and Frame Relay Backup network

r) ASEN Frame Work – Communication function using trusted products and ASEN API

s) Load Balancing

- Line Load Balancing function for VPN tunnel
- Load Balancing function which balances loads in accordance with predefined maximum bandwidth of each interface.
- QoS function which sets maximum bandwidth for each security policy and balances loads.

3 TOE Security Environments

The TOE, configured as a multi-homed network, protects user information that passes though the TOE by mediating and controlling information flow. This chapter provides assumptions about the TOE usage to define and ensure the TOE security environments.

3.1 Assumptions

The following shows the assumptions to be initiated or maintained in the TOE operational environment. The following assumptions consist of two parts. The first part consists of the assumptions identical to those of the IPSPP, and the second part consists of additional assumptions. Respective sections contain adequate explanation.

3.1.1 Assumptions Identical to IPSPP

The following is a list of assumptions which apply to the TOE operational environment that conforms to the IPSPP.

Name	Description
A.AttackLevel	The attacker possesses a medium level of expertise, resources, and motivation. Chances of the attacker finding an exploitable vulnerability are moderate. Application Notes: The attacker can easily obtain exploitable vulnerability information or attack tools against OS or application program from the Internet. The attacker possesses a medium level of expertise and may damage the target computer or obtain information using the vulnerability information or tools obtained from general computers or the Internet.
A.PhysicalSecurity	The TOE is located in physically secure environment where only authorized administrators are allowed the access.
A.SecurityMain	When the internal network environment is changed due to network

tenance	configuration changes, an increase or decrease of hosts, or an increase or decrease of services, the new changes are immediately noted and security policies are configured in accordance with the TOE operational policy to maintain the same level of security as before.
A.TrustedAdministrator	An authorized administrator of the TOE possesses no malicious intention, is adequately educated, and performs his/her duties in accordance with the administrative guideline.
A.HardenedOS	The underlying OS of the TOE ensures the reliability and stability by both eliminating the unnecessary services or means not required by the TOE and installing the OS patches.
A.SingleConnectionPoint	The TOE is installed and operated on a network and separates the network into external and internal network. Information can not flow between the two without passing through the TOE. .

[Table 3-1] Assumptions Identical to IPSPP

3.1.2 Additional Assumptions of the TOE

[Table 3-2] shows the assumptions added on this ST.

Name	Description
A.SecureTOEExternalServer	The network time protocol (NTP) server which provide a trusted time stamp to the TOE and the DI rule update server which updates HOTLIST by uploading the latest DI rules to the TOE are secure. The TOE uses the SSL protocol to establish a secure channel with the remote administrator PC and the DI rule update server.
A.SSLCertificateoftheTOE	SECUREWORKS issues the certificate to be used for an SSL authentication in advance at installation and store it in the TOE. The SSL certificate for the TOE is issued and controlled in a secure manner.

[Table 3-2] Additional Assumptions

3.2 Threats

This section introduces the threats to the assets against which specific protection within the TOE or its environment is required.

The assets that the TOE intends to protect are the internal network operated by the organization or the computer assets of the DMZ, and network services. External threat agents attack the computer to disrupt its normal use, so as to exhaust the availability of organizational assets.

3.2.1 Threats countered by the TOE

This chapter lists the threats to the TOE. The following threats are induced by the TOE or the operational environment. The threat agent that creates these threats is an unauthorized user of the TOE or an external IT entity.

The following table lists the threats to the TOE taken straight from the IPSPP.

Name	Description
T.Masquerade	A threat agent may masquerade as an authenticated administrator and therefore can obtain access to the TOE.
T.Failure	Due to a failure or an attack, the TOE, while in operation, may not be able to provide proper services to users.
T.AuditFailure	Auditable events of the TOE may not be logged due to audit storage capacity exhaustion.
T.InboundIllegal Information	A computer in the internal network may be tampered or attacked by incoming a malicious packet from an external network containing unauthorized information.
T.Unauthorized Service Access	A threat agent may gain access to a service unauthorized to internal network hosts, and disturb the proper offering of its service.
T.AnomalyPacket Transfer	A threat agent may transfer network packets of anomaly structure to cause abnormal operations.

Name	Description
T.NewVulnerabilityAttack	A threat agent may attack by exploiting a new vulnerability of a computer system in the internal network of the TOE or the TOE operational environment.
T.DoSAttack	A threat agent may exhaust service resources of a computer in the internal network in the TOE operational environment and disturb authorized users' use of services.
T.ReplayAttack	A threat agent may gain access to the TOE by attempting authentication repeatedly.
T.Bypassing	A threat agent may gain access to the TOE by bypassing security functions of the TOE.
T.SpoofingIPAddress	A threat agent may illegitimately gain access to the internal network by spoofing source IP address as an internal IP address.
T.UnauthorizedTSFDataModification	A threat agent may attack by launching a buffer overflow attack, thus resulting in unauthorized modification of the TSF data.

[Table 3-3] Threats countered by the TOE

3.2.2 Threats countered by the TOE Environment

The following are the threats to the TOE operational environment.

The following table lists the threats to the TOE environment taken from the IPSPP. These are the threats applicable to the TOE.

Name	Description
TE.PoorAdministration	The TOE may be configured, administered, or operated in an insecure manner by an authorized administrator.
TE.DistributionandInstallation	The TOE may be damaged during its distribution or installation process.

[Table 3-4] Threats countered by the TOE Environment

3.3 Organizational Security Policies

The organization which operates the TOE implemented by this ST has its own security policies, and authorized administrators enforce the security policies using the TOE. The security objectives for this environment are divided into two parts as the assumptions in section 3.1.

3.3.1 Organizational Security Policies

The following organizational policies are to be applied to a TOE operational environment which conforms [IPSPP].

Name	Description
P.Audit	Auditable events must be recorded and maintained to trace the responsibility of all security related actions, and the recorded data must be reviewed.
P.SecureManagement	An authorized administrator must manage the TOE in a secure manner.

[Table 3-5] Organizational Security Policies

3.3.2 Additional Organizational Security Policies

The following is an organizational security policy added on this ST.

Name	Description
P.SSLCertificatemanagement	SECUREWORKS must issue, store, and control an SSL certificate in a secure manner.

[Table 3-6] Additional Organizational Security Policy

4 Security Objectives

Security objectives are defined and categorized into TOE security objectives and security objectives for its the environment. The first part defines the security objectives that are to be addressed directly by the TOE, and the second part defines the security objectives to be addressed by the IT domain or by non-technical or procedural means.

4.1 TOE Security Objectives

This section describes the security objectives that are to be addressed by the TOE. The following table is the list of TOE security objectives taken straight from the IPSPP.

Name	Description
O.Availability	In the case of an accidental breakdown or a failure caused by an external attack, the TOE must be able to maintain minimum security functions and provide regular services.
O.Audit	The TOE must provide a means to record, store and review security-relevant events in audit records to trace the responsibility of all actions regarding security.
O.Administration	The TOE must provide administrative tools to enable authorized administrators to effectively manage and maintain the TOE.
O.AbnormalPacketScreening	The TOE must screen out packets with an abnormal structure from all the packets that pass through the TOE. Application Notes : An abnormal packet is a packet that is not TCP/IP packet defined by an Internet standard protocol such as RFC 791 (internet protocol), RFC 792 (internet control message protocol), or RFC 793 (transfer control protocol), a packet with IP spoofing, broadcasting packet, or looping packet.
O.DoSAttackBlocking	The TOE, when an attacker abnormally uses service assets of a computer, must block the use to protect the network service of the protecting computer for normal users.

Name	Description
O.Identification	The TOE must identify all external IT entities subject to information flow control of the TOE and the users who want to access to the TOE.
O.Authentication	The TOE, after identifying an administrator, must authenticate the administrator's identity before granting an access to the TOE. Application Note : When a threat agent repeatedly tries authentication using the administrator's identity, there is a chance the agent may obtain authentication data. The TOE must implement an adequate authentication mechanism to defend these replay attacks.
O.InformationFlowControl	The TOE must control unauthorized information flow from the external network to the internal network based on security policies. Application Note : This security objective implements the deny-all policy and the allow-all policy executed by TSF. Deny-all policy means screening all packets except for the ones specified to be allowed, and allow-all policy means allowing all packets except for the ones specified to be denied.
O.TSFDataProtection	The TOE must protect stored TSF data from unauthorized disclosure, modification, or deletion.

[Table 4-1] TOE Security Objectives

4.2 Security Objectives for the Environment

Security objectives for the environment are solved or countered by the organizational security policies and assumptions. This section describes the security objectives for the environment. These security objectives for the environment are divided into two parts as the assumptions in section 3.1.

4.2.1 Security Objectives for the Environment Identical to IPSPP

The following table is the list of security objectives for the environment taken straight from the IPSPP.

Name	Description
OE.AttackerLevel	The attacker possesses a medium level of expertise, resources, and motivation. Chances of the attacker finding an exploitable vulnerability are moderate.
OE.PhysicalSecurity	The TOE must be located in physically secure environment where only authorized administrators are allowed to access.
OE.SecurityMaintenance	When the internal network environment is changed due to network configuration changes, an increase or decrease of hosts, or an increase or decrease of services, the new changes must be immediately noted and security policies configured in accordance with the TOE operational policy to maintain the same level of security as before.
OE.TrustedAdministrator	An authorized administrator of the TOE possesses no malicious intention, is adequately educated, and performs his/her duties in accordance with the administrative guideline.
OE.SecureAdministration	The TOE must be distributed and installed securely, and must be configured, administered, and used in a secure manner.
OE.HardenedOS	The underlying OS of the TOE ensures the reliability and stability by both eliminating the unnecessary services or means not required by the TOE and installing the OS patches.

Name	Description
OE.SingleConnectionPoint	The TOE, when installed and operated on a network, separates the network into the internal and external network. All communication between the two is done through the TOE.
OE.VulnerabilityListUpdate	The administrator must update and control the vulnerability data managed by the TOE to defend external attacks exploiting new vulnerabilities of an internal computer.

[Table 4-2] Security Objectives for the Environment Identical to IPSPP

4.2.2 Additional Security Objectives for the Environment

[Table 4-3] lists additional environments other than the security objectives for the environment in the IPSPP.

Name	Description
OE.TrustedTOEExternalServer	Both the Network Time Protocol (NTP) server that provides trusted time source outside the TOE and the DI rule update server that updates the latest DI rules must be secure. The TOE uses the SSL protocol to create trusted channels with remote administrator console, DI Rule Update Server.
OE. SSL Protocol	The TOE calls the SSL function to create trusted communication channels with remote administrator console and the DI rule update server. The TOE, using the SSL protocol, mutually authenticates with an SSL certificate of the TOE or administrator's ID & password, and protects the TSF data.

[Table 4-3] Additional Security Objectives for the Environment

5 IT Security Requirements

These requirements are composed of the security functional components of the CC V2.2 part 2 and the assurance components related to assurance level in part 3. The CC is divided into the following two categories.

- Security Functional Requirements: provide security functions such as access control, information flow, audit record, identification, and authentication.

- Assurance Requirements: provide reliable basis on which the TOE may or may not meet security objectives.

5.1 TOE Security Functional Requirements

This section provides the security functional requirements (SFR) for the TOE and explains in two parts.

- Security Functional Requirements (SFRs): This ST meets SFR of the claimed IPSPP. There are additional operations in need of protection profile and also operations added by the author of this ST.

- Strength of Function (SOF) for the TOE SFRs: This ST describes SOF used in the claimed protection profile in 5.1.2.

5.1.1 Security Functional Requirements (SFRs)

The SFRs listed in [Table 5-1] are the names of SFR components used in the claimed IPSPP. The SFRs described in this section are taken straight from IPSPP, and the author of this ST completed incomplete operations of IPSPP. Further details of this are explained in chapter 7.

Security Function Class	Functional Component ID	Functional Component Name
Security Audit Class	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User Data Protection Class	FDP_IFC.1(1)	Subset information flow control (1)
	FDP_IFC.1(2)	Subset information flow control (2)
	FDP_IFF.1(1)	Simple security attributes (1)
	FDP_IFF.1(2)	Simple security attributes (2)
Identification & Authentication Class	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition (1)
	FIA_ATD.1(2)	User attribute definition (2)
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	User identification before any action (1)
	FIA_UID.2(2)	User identification before any action (2)
Security Management Class	FMT_MOF.1(1)	Management of security functions behaviour (1)

Security Function Class	Functional Component ID	Functional Component Name
	FMT_MOF.1(2)	Management of security functions behaviour (2)
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(1)	Management of TSF data (1)
	FMT_MTD.1(2)	Management of TSF data (2)
	FMT_MTD.1(3)	Management of TSF data (3)
	FMT_MTD.2(1)	Management of limits on TSF data (1)
	FMT_MTD.2(2)	Management of limits on TSF data (2)
	FMT_MTD.2(3)	Management of limits on TSF data (3)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF Class	FPT_AMT.1	Abstract machine testing
	FPT_FLS.1	Failure with preservation of secure state
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF Testing
Resource Utilisation Class	FRU_FLT.1	Degraded fault tolerance : partial application
	FRU_RSA.1	Maximum quotas
TOE Access Class	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination
Trusted Path/ Channels Class	FTP_ITC.1	Inter-TSF trusted channel

[Table 5-1] SFRs Reused in IPSPP

FAU_ARP.1 Security alarms

Hierarchical to : No other components.

FAU_ARP.1.1 The TSF shall take [{following actions: alarm an authorized administrator – e-mail or SMS messages, generate and log audit records}] upon detection of a potential security violation.

Dependencies : FAU_SAA.1 Potential violation analysis

FAU_GEN.1 Audit data generation

Hierarchical to : No other components

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 functions;
b) All auditable events for the *minimum* level of audit(refer to the [Table 5-2] Auditable events); and
c) [Auditable events in **[Table 5-3]**]

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in **[Table 5-2], [Table 5-3]** and following information]
   - Importance of the event (Log type)
   - Sequence number
   - Protocol
   - Object identity (Destination IP address, Port)
   - Number of overlaps for the audited event
   - Reason and information of failed event

Dependencies : FPT_STM.1 Reliable time stamps

Component ID	**Minimal Auditable Events**	**Additional Information of Audit Record**
FAU_ARP.1	Actions taken due to an imminent security violation	Generation of an alarm
FAU_SAA.1	Enabling and disabling of any of the analysis mechanism, automatically	Generation of an alarm

Component ID	Minimal Auditable Events	Additional Information of Audit Record
	responses by the tool	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection function is operating.	Authorized administrator's identity (administrator ID)
FDP_IFF.1	Decision to permit requested information flows	Information of the packet
FIA_AFL.1	Reaching the threshold of unsuccessful authentication attempts, the counteraction taken, and the subsequent, if appropriate, restoration to normal state	User identity presented to the TOE (administrator ID)
FIA_UAU.1	Unsuccessful authentication attempt	User identity presented to the TOE (administrator ID)
FIA_UID.2	Unsuccessful user identification	User identity presented to the TOE (administrator ID)
FMT_SMF.1	Use of The security management functions	Authorized administrator's identity (administrator ID)
FMT_SMR.1	Modifications to the group of administrator that are part of a role	Authorized administrator's identity (administrator ID)
FRU_FLT.1	All failure detected by the TSF	
FRU_RSA.1	Rejection of assignment operation due to resource limits	
FTP_ITC.1	Failure of the trusted channel function. Identification of the initiator of a failed trusted channel and of the subject.	Identity of the subject (Source IP, Port)
FPT_STM.1	Changes to the time	Authorized administrator's identity (administrator ID)
FTA_SSL.1	Locking of an interactive session by the session locking mechanism	-
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	-

[Table 5-2] Minimal Auditable Events

Component ID	Additional Auditable Event	Additional Information of Audit Record
FAU_STG.3	Audit record storage deficiency alarm	-
FDP_IFF.1	Decision to deny a requested information flow Intrusion detection	Information of the packet
FIA_UAU.1	Timing of authentication	Authorized administrator's identity (administrator ID)
FMT_MSA.1	All modifications to security attributes	Modified security attribute values
FMT_MSA.3	Modifications to the basic setup of allowing rules or restriction rules All modifications to the default value of security attributes	Modified security attribute values
FMT_MTD.1	All modifications to the TSF data	Modified TSF data
FMT_MTD.2	All modifications to limits on the TSF data	Modified TSF data limits
FPT_TST.1	TSF self-test results	
others	Local system host name acquisition failure	
	Audit record generation error	
	Database HASH calculation error	

[Table 5-3] Additional Auditable Events

FAU_GEN.2 User identity association

Hierarchical to : No other components

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies : FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAA.1 Potential violation analysis

Hierarchical to : No other components

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 [
    - Audit record storage shortage warning
    - Intrusion detection
    - All failures detected by the TSF
    - Failure of getting the host name of a local system
    - Integrity error
    - Log generation error
    - Database HASH calculation error
    - Alarm rules for the events defined in FAU_GEN.1, added by an authorized administrator] known to indicate a potential security violation;

b) [none]

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit review

Hierarchical to : No other component

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 interpret the information.

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to : No other components

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

- Subject identity
- Object identity
- Date and time of the event
- Type of event (service)
- Importance of the event (log type)
- Keyword (The result (success or failure) of the event)

Dependencies : FAU_SAR.1 Audit review

Application Note: The root administrator and the log administrator can perform this component, and the policy administrator can perform simple review functions.

FAU_SEL.1 Selective audit

Hierarchical to : No other components

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) [importance of the event, protocol]

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

Application Note: The root administrator and the log administrator can determine auditable events. However, the root administrator and the policy administrator determines the generation of audit records for each packet filtering security policy.

FAU_STG.1 Protected audit trail storage

Hierarchical to : No other components

FAU_STG.1.1 The TSF shall protect the stored records from unauthorized deletion.

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

Dependencies : FAU_GEN.1 Audit data generation

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to : No other components

FAU_STG.3.1 The TSF shall take [actions to inform the authorized administrator and to {generate and log audit records}] if the audit trail exceeds [{% value (default is 5%) of the remaining audit trail storage space which an authorized administrator can define, that % value must be higher than “1”}].

Dependencies : FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

Hierarchical to : FAU_STG.3

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized user with special rights* and [{send e-mail or SMS message to the authorized administrator and stop all the TSF services of the TOE except the authorized administrator’s connection}] if the audit trail is full.

Dependencies : FAU_STG.1 Protected audit trail storage

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

Hierarchical to : No other components

FDP_IFC.1.1 The TSF shall enforce the **[packet filtering SFP]** on [operation that cause controlled information to flow to and from controlled subjects covered by the SFP].

a) [Subject : IT entities which send packets to the internal network host, external IT entities or the TOE,
b) Information : network packet sent through the TOE from the subject to another
c) Operation : pass if allowing rules exist]

Dependencies : FDP_IFF.1 Simple security attributes

Application Note : The 'deny all policy' of the IPSPP is denoted as the 'packet filtering security function policy' in this ST.

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

Hierarchical to : FDP_IFC.1

FDP_IFC.1.1 The TSF shall enforce the **[intrusion prevention SFP]** on [operation that cause controlled information to flow to and from controlled subjects covered by the SFP].

a) [Subject : IT entities which send packets to the internal network host, external IT entities or the TOE
b) Information : network packet sent through the TOE from the subject to another

c) Operation : deny if denying rules exist]

Dependencies : FDP_IFF.1 Simple security attributes

Application Note : The ‘allow all policy’ of the IPSPP is denoted as the ‘intrusion prevention security policy’ in this ST.

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

Hierarchical to : No other components.

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

a) Subject security attributes: the IP address of IT entities transmitting and receiving information through the TOE, user ID
b) Information security attributes:
   - Source address
   - Destination address
   - Protocol
   - Allow/Deny Fragmentation

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: [the following rules]

a) The information(Network packet) security attributes values are correspondent to or included in the packet filtering SFP rules security attributes values and unambiguously permitted by the packet filtering SFP rules, where such rules may be composed from all possible combinations of the values of its security attributes
b) If the source address of a network packet is included in the administrator IP designated to the TOE, the destination address is the IP of TOE, and the destination port is 443.
c) If response packet against the request packet of which the source

address is the IP of TOE is registered on the session table.

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

FDP_IFF.1.4 The TSF shall provide the [none].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [{unidirectional information flow where the source is the TOE}].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on [the following rules]:

- The rules described in FDP_IFF.1.2 do not exist.
- Information flow security policy generated by the authorized administrator does not exist.

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

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

Hierarchical to : No other components

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

a) Subject security attributes: The IP address of external IT entities interchanging information through the TOE, {User ID}

b) Information security attributes:
   - Source address
   - Destination address
   - Protocol
   - Packet header information

- Packet data information

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

[Subject can cause information (network packets) to flow through the TOE only if that packet is not denied based on Traffic anomaly check and Attack pattern matching rules, these rules are as follows

Traffic anomaly check

- If sessions per second from a source address are generated more than the value specified by the authorized administrator
- If the source address is on the Black list
- If SYN packets are created more than the number set by the authorized administrator during the period of time set by the authorized administrator for a destination address
- When the packets sent from a source address are ICMP and UDP packets, if the number of packets are more than the number set by the authorized administrator

Attack pattern matching

- Data information of the packet corresponds to or is included in the attack rules of the attack patterns by the Intrusion Prevention SFP.]

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

FDP_IFF.1.4 The TSF shall provide the [none].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the [none].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules.

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network.

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loop back network.

e) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and has an abnormal packet structure.

f) [{the following} other rules]

IP

- Source route: reject packets with source routing information at the header.
- IP Spoof: reject IP spoofing attack packets with a deceptive source IP address.
- Martian address: reject packets with abnormally set value of source IP address.
- Non-existent address: reject packets from an IP address not assigned by the INNA.

TCP

- Poisoned Reversed Flag: reject packets which the TCP reserved flag is not set up at 0. (Fingerprint Scan)
- Illegal Control Flags: reject packets if abnormal TCP control flag is set up.
- Illegal Header Length: reject packets with abnormal TCP header length.

UDP

- Echo Loop: reject UDP echo loop attack packets.
- Illegal Header Length: reject packets with abnormal TCP UDP length.

ICMP

- Bad Echo Request: reject packets when the checksum of ICMP Echo Request packet is incorrect or the code is abnormal.
- Bad Echo Reply: reject packets when the checksum of ICMP Echo Reply packet is incorrect or the code is abnormal.

Others

- Post scanning detection: reject any access attempt using the packet log as statistics from the same source to more ports than the number of ports specified by the authorized administrator during the time specified by the authorized administrator.
- Address scanning detection: reject any access attempt using the packet log as statistics from the same source to more addresses than the number of addresses specified by the authorized administrator during the time specified by the authorized administrator.
- Trap Ports scanning: using the packet log as statistics, if traps are created more than the number specified by the authorized administrator to the service specified by the authorized administrator during the time specified by the authorized administrator, they are shut down.

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

Application Note: Generation methods of attack patterns by the intrusion prevention SFP are divided into three categories which are being included as default at installation, being defined by the administrator, and downloading from the DI rule update server. Security attributes of attack patterns vary by how an attack pattern is created. However, security attributes of the rules included as default and the ones downloaded from the DI rule update server are identical.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when "*an authorized administrator configurable positive integer within [the range from 1 to 9999]*" unsuccessful authentication attempts occur related to [administrator authentication attempt].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent authentication {or delay authentication} until an action is taken by the authorized administrator].

Dependencies: FIA_UAU.1 Timing of authentication

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

Hierarchical to: No other components

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

a) IP address
b) {none} user security attributes

Dependencies: No dependencies

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

Hierarchical to: No other components

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

a) Identifier

b) User security attributes {of the following additional items}

- Password
- Authentication method
- Authentication status – normal, disabling account, delay
- The limit number of unsuccessful authentication attempts
- Authority(security role)

Dependencies: No dependencies

Application Note: Administrators include the root administrator, the policy administrator, and the log administrator.

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [none] on behalf of the **administrator** to be performed before the **administrator** is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification

Application Note: Administrators include the root administrator, the policy administrator, and the log administrator.

FIA_UAU.7 Protected authentication feedback

Hierarchical to : No other components

FIA_UAU.7.1 The TSF shall provide only [user ID, success or deny message] to the administrator while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

Application Note: Administrators include the root administrator, the policy administrator, and the log administrator.

FIA_UID.2(1) User identification before any action(1)

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1 The TSF shall require each **IT entity** to identify itself before allowing any other TSF mediated actions on behalf of the user.

Dependencies: No dependencies

FIA_UID.2(2) User identification before any action(2)

Hierarchical to : FIA_UID.1 Timing of identification

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

Dependencies: No dependencies

Application Note: Administrators include the root administrator, the policy administrator, and the log administrator.

FMT_MOF.1(1) Management of security functions behaviour(1)

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable* the functions [{the following list of functions}] to [an authorized administrator].

- The management function for managing the group of administrator that are part of a role
- The administrator management function for authorized administrator's multiple access to TOE
- NIC link status check function
- HOTLIST automatic update function

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

Application Note: The root administrator and the policy administrator can perform this component.

FMT_MOF.1(2) Management of security functions behaviour(2)

Hierarchical to : No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour* of the functions [the following list of functions] to [an authorized administrator].

- Enable and apply TOE security policy
- Perform self-test at authorized administrator's request
- Whether or not to generate audit records for each security policy
- Manual HOTLIST update at authorized administrator's request

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

Application Note: Generation of audit records is performed by the root administrator and the log administrator. However, generation of audit records for each packet filtering security policy is determined by the root administrator and the policy administrator.

FMT_MSA.1 Management of security attributes

Hierarchical to : No other components

FMT_MSA.1.1 The TSF shall enforce the [packet filtering SFP, intrusion prevention SFP] to restrict the ability to *query, modify, delete, [{generate}]* the security attributes [of the following list] to [an authorized administrator].

[Table 5-4]

Security Attributes	Action	Remarks
Sequence number in the Packet Filtering SFP rule	Query, Modify, Delete, Generate	
Network Interface	Query, Modify	
Network Group	Query, Modify, Delete, Generate	-Possess group name, location, IP information. -Used for packet filtering security management access group.
Applicable Service	Query, Modify, Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
(Allow/Deny) Policy in the Packet Filtering SFP rule	Query, Modify	Attack patterns that downloaded from DI rule update server : Query
Whether or not to Allow Fragmentation Packet	Query, Modify	Attack patterns that downloaded from DI rule update server : Query
Attack Type ID of Attack pattern	Query, Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
Attack Type Description of Attack pattern	Query, Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
Attack Rule Name of Attack pattern	Query, Modify	Attack patterns that

Security Attributes	Action	Remarks
	Delete, Generate	downloaded from DI rule update server : Query
Attack Rule Description of Attack pattern	Query, Modify Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
Signature Character String of Attack pattern (pattern)	Query, Modify Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
Start Point of Attack pattern (data size)	Query, Modify Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
End Point of Attack pattern (data size)	Query, Modify Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
Maximum Data Size of Attack pattern (data size)	Query, Modify Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
Minimum Data Size of Attack pattern (data size)	Query, Modify Delete, Generate	Attack patterns that downloaded from DI rule update server : Query
Context of Attack pattern	Query, Modify	Attack patterns that downloaded from DI rule update server : Query
Upper/Lowercase Distinction of Attack pattern	Query, Modify	Attack patterns that downloaded from DI rule update server : Query
Direction	Query, Modify	Attack patterns that downloaded from DI rule update server : Query
Risk Level of Attack pattern (Level 1-High, Level 2-Moderate, Level 3-Low, Level 4-Minimal)	Query, Modify	Attack patterns that downloaded from DI rule update server : Query
Policy of Attack pattern - Reject/Warning	Query, Modify	Attack patterns that downloaded from DI rule

Security Attributes	Action	Remarks
		update server : Query
CVE Code	Query	Attack patterns that downloaded from DI rule update server : Query
Source route	Query, Modify	
IP Spoof	Query, Modify	
Martian address	Query, Modify	
Non-existent address	Query, Modify	
Poisoned Reversed Flag	Query, Modify	
Illegal Control Flags	Query, Modify	
Illegal TCP Header Length	Query, Modify	
Echo Loop	Query, Modify	
Illegal UDP Header Length	Query, Modify	
Bad Echo Request	Query, Modify	
Bad Echo Reply	Query, Modify	
Post Scanning detection	Query, Modify	
Address Scanning detection	Query, Modify	
Trap Ports Scanning detection	Query, Modify	
Session Restriction	Query, Modify	
SYN Attack Defense	Query, Modify	
Packet Restriction	Query, Modify	
Disk(Audit storage) Capacity Shortage Warning	Query, Modify	
Security Management Multiple Access	Query, Modify	
Security Management Time-Out	Query, Modify	
Alarm Rule	Query, Modify, Delete, Generate	
Administrator Account	Query, Modify, Delete, Generate	The account for root administrator is unable to delete or generate. It is default.
HOTLIST Update Setup	Query, Modify	
Network Interface State Check	Query, Modify	
Enable/Disable of Log Generation (per	Query, Modify	

Security Attributes	Action	Remarks
Type, Service, Protocol)		
Overlapping Log Setup	Query, Modify	
TOE Time Setup	Query, Modify	
Integrity Check Function	Query, Modify	
Self-test Function	Query, Modify	

[Table 5-4] Management of Security Attributes

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

Application Note: The root administrator and the policy administrator can perform management of security attributes. All the security attributes of the attack patterns downloaded from the DI rule update server and the default attack patterns provided at TOE installation allows Query only. However, only the policy information of the security attributes may be modified.

FMT_MSA.3 Static attribute initialisation

Hierarchical to : No other components.

FMT_MSA.3.1 The TSF shall enforce the [packet filtering SFP, intrusion prevention SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

Dependencies : FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

Application Note: The root administrator and the policy administrator can perform this component.

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

Hierarchical to: No other components

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify, delete, [{generate}]* the [packet filtering SFP rules, intrusion prevention SFP rule (only attack patterns of), alarm rule] to [authorized administrator].

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

Application Note: The root administrator and the policy administrator can set the packet filtering security policy and the intrusion prevention security policy, while the root administrator and the log administrator can set alarm rules. The policies downloaded from the DI rule update server among attack patterns cannot be modified or deleted.

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

Hierarchical to: No other components

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

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

FMT_MTD.1(3) Management of TSF data(3)

Hierarchical to: No other components

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

- TOE time stamp used for audit trail at generating audit record
- Session time-out value of authorized administrator
- Authorized administrator's configurable value associated security audit
- HOTLIST automatic update cycle
- Authorized administrator's configurable value for setting up NIC status check condition

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

FMT_MTD.2(1) Management of limits on TSF data(1)

Hierarchical to : No other components

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [audit storage capacity] to [an authorized administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FAU_STG.3 or actions specified in FAU_STG.4].

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

FMT_MTD.2(2) Management of limits on TSF data (2)

Hierarchical to : No other components

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [the number of failed authentication attempts] 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: [{actions specified in FIA_AFL.1}].

Dependencies : FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

FMT_MTD.2(3) Management of limits on TSF data (3)

Hierarchical to : No other components

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [the time interval between occurrences of self-tests] to [an authorized administrator].

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to : No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Management of security function behaviour
   - Items specified in section 5.1.1.1 of FMT_MOF.1
b) Management of security attributes
   - Items specified in section 5.1.1.1 of FMT_MSA.1
c) Management of TSF data
   - Items specified in section 5.1.1.1 of FMT_MTD.1
d) Management of the limits on TSF data
   - Items specified in section 5.1.1.1 of FMT_MTD.2

e) Management of security roles
   - Items specified in section 5.1.1.1 of FMT_SMR.1

f) Management of current state information of session and traffic anomaly check functions
   - Viewing current state of a session generated by the packet filtering security policy
   - Viewing the information of a source IP restricted by the traffic anomaly check function

g) Management of self-test setup
   - Integrity check results inquiry
   - Integrity initialization of the subject of Integrity check (HASH data re-generation)]

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the roles of [the following authorized administrators].

a) Root administrator
b) Log administrator
c) Policy administrator

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

Dependencies: FIA_UID.1 Timing of identification

Application Note: Administrators can be classified into the root administrator, the policy administrator, and the log administrator by authority. Only the root administrator can establish privileges of the administrators.

- Root administrator: an authorized administrator with all privilege.

- Log administrator: an authorized administrator who has the privilege to view audit records.
- Policy administrator: an authorized administrator who has the privilege to establish the packet filtering security policy and intrusion prevention security policy.

FPT_AMT.1 Abstract machine testing

Hierarchical to : No other components

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 authorized administrator* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies: No dependencies

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to : No other components

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [list of types of failures specified in FRU_FLT.1.1]

Dependencies: ADV_SPM.1 Informal TOE security policy model

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to : No other components

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.

Dependencies: No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to : No other components

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.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components

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

Dependencies: No dependencies

FPT_TST.1 TSF testing

Hierarchical to: No other components

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the request of the authorized administrator* to demonstrate the correct operation of TSF data.

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

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

Dependencies: FPT_AMT.1 Abstract machine testing

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components

FRU_FLT.1.1 The TSF shall ensure the operation of [management activities by the administrator using a console or security management screen] when the following failures occur [hardware failure (CPU, memory etc.), software failure (OS, TOE etc.), buffer overflow failure due to other types of attack].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_RSA.1 Maximum quotas

Hierarchical to: No other components.

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [transport layer expression] that *defined group of **IT entities*** can use over *a specified period of time*.

Dependencies: No dependencies

FTA_SSL.1 TSF-initiated session locking

Hierarchical to : No other components

FTA_SSL.1.1 The TSF shall lock an interactive **authorized administrator** session after [surpassing **authorized administrator's** session timeout value(1-60 minutes, default value 1 minute) defined by **the root administrator**] by:

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

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

Dependencies: FIA_UAU.1 Timing of authentication

Application Note: Authorized administrators include the root administrator, the log administrator, and the policy administrator.

FTA_SSL.3 TSF-initiated termination

Hierarchical to : No other components.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [the following idle periods of an authorized **IT entity**, {excess of the maximum session quota}].

- When the number of sessions or packets that occurred by an authorized IT entity exceeds the limit number of sessions or packets defined by the authorized administrator in FMT_MSA.1.
- When SYN Flooding is determined by the value set by SYN attack defense in FMT_MSA.1.
- When the authorized administrator requests termination of a packet filtering session searched by section f) of FMT_SMF.1.

Dependencies: No Dependencies

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

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].

Dependencies: No dependencies

Application Note: The TOE initiates a trusted channel by invoking the SSL function which is provided by an IT environment in order to create the SSL protocol.

5.1.2 SOF Claim

This ST accepts SOF-medium defined in the IPSPP. The attacker is presumed to have a moderate level of expertise, resources, and motivation. The IPSPP advises to provide, at least, SOF-medium security functions to provide adequate protection against attackers possessing a moderate attack potential. This ST conforms to [IPSPP] which SOF claim is SOF-Medium .Therefore, the SOF of ST should at least claim SOF-medium for security mechanism required in relevant SFR(FIA_UAU.1, FTP_TST.1). The security functions SW_INA and SW_PT specified in ST satisfied SOF-high.

5.2 TOE Security Assurance Requirements

[Table 5-5] shows security assurance components of the TOE. These are composed of Security Assurance Requirements in common criteria part 3 V2.2 and meets EAL4 assurance level.

Assurance Class	Assurance Component ID	Assurance Component Name
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	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
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Evaluation	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

[Table 5-5] EAL4 Assurance Requirements

*Assurance component AGD_USR.1 is not applicable since there is no general user of the TOE but the administrator.

5.2.1 Configuration Management

ACM_AUT.1 Partial CM automation

Dependencies : ACM_CAP.3 Authorization controls

Developer action elements
ACM_AUT.1.1D The developer shall use a CM system.
ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements
ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.
ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

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

ACM_CAP.4 Generation support and acceptance procedure

Dependencies:
ALC_DVS.1 Identification of security measures

Developer action elements
ACM_CAP.4.1D The developer shall provide a reference for the TOE.
ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.7C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.8C The CM plan shall describe how the CM system is used.

ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.12C The CM system shall support the generation of the TOE.

ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

Dependencies :

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.
Content and presentation of evidence elements:
ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:
ACM_SCP.2.1E 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.2 Detection of modification

Dependencies : ACM_CAP.3 Authorization controls

Developer action elements:
ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:
ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.
ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:
ADO_DEL.2.1E 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 of evidence elements:

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

Evaluator action elements:

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

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

5.2.3 Development

ADV_FSP.2 Fully defined external interface

Dependencies : ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

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

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the 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.1 Subset of the implementation of the TSF

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

Developer action elements:
ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:
ADV_IMP.1.1C 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.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:
ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided 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.

ADV_SPM.1 Informal TOE security model

Dependencies : ADV_FSP.1 Informal functional specification

Developer action elements

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model..

Content and presentation of evidence elements

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements

ADV_SPM.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
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

General users are excluded from the logical scope of the TOE. User guidance is not provided because the FMT class of the TOE security functional requirements does not include the description about general users. Therefore, an assurance measure for AGD_USR.1 is not applicable.

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_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies

Developer action elements

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements

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

ALC_TAT.1 Well-defined development tools

Dependencies : ADV_IMP.1 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
ATE_FUN.1 Functional testing

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

Content and presentation of evidence elements
ATE_COV.2.1C The analysis of the test 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.1 Testing: high-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.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements
ATE_DPT.1.1C 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.

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

ATE_FUN.1 Functional testing

Dependencies: 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 test

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 Evaluation

AVA_MSU.2 Validation of analysis

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

Developer action elements
AVA_MSU.2.1D The developer shall provide guidance documentation.
AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements

AVA_MSU.2.1C 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.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements

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

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies : ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-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.

Application note: Evident vulnerability refers to the vulnerability of firewall or Intrusion Prevention System (IPS) disclosed externally or to the Internet. The developer should test the safeguarding measures against these vulnerabilities. The evaluator should examine that the analysis on the evident vulnerabilities performed by the developer is done well, and perform a penetration test based on the results of the analysis to determine whether the TOE is resistant or not.

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.

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].

Dependencies: No dependencies

Application Note : The TOE initiates a trusted channel by invoking the SSL function which is provided by an IT environment in order to create the SSL protocol.

6 TOE Summary Specification

This chapter simply and clearly describes how the security functions of the TOE are implemented and how the assurance requirements are satisfied.

6.1 TOE Security Functions

This section describes the security functions of the TOE and how the security functions satisfy all the security functional requirements.

6.1.1 Security Management (SW_ADMIN)

Each administrator has his/her own ID (the default value of root administrator's ID is 'admin'), and is able to perform the following functions that manage the security functions behaviors and the TSF data after successfully logging in the TOE. When entering the authorized administrator configurable values of security attributes for the following security managements, SW_ADMIN checks input value whether or not to be within the range of valid. If not valid, SW_ADMIN display error message on a remote administrator's PC.

Security Management Role

The root administrator which is created at the TOE installation has basically all privileges and he/she performs the management of security role by generating, deleting, or modifying the administrator's authentication data of which composed privilege (policy administrator, log administrator), limits number of unsuccessful authentication attempts, authentication status and so on.

- An administrator assigned the role of log privilege can set and manage log viewing, log search, alarm, and log generation.
- An administrator assigned the role of policy privilege can establish necessary policies for the packet filtering security policy and intrusion prevention security policy. Also, the administrator can create objects such as the network or

service for policy establishment, and can perform log viewing function. The policy administrator can determine whether or not to generate logs for each security policy.

Generation of log depending on the type and importance of an event is determined by the log administrator, while the function which determines the generation of log per security policy, regardless of the type and importance, is set by the policy administrator.

Access Control for Security Management Function

An administrator is able to log on the TOE providing security management function only when the IP of the administrator's PC is registered in the MANAGER group among network groups. For two or more administrators to log on the TOE at the same time, in accordance with FMT_MOF.1(1), the security management multiple access allow option must be set. The MANAGER network group can be searched, modified, generated, or deleted by FMT_MSA.1.

An authorized administrator, by FMT_MSA.1, can set the security management multiple access allow option. If two or more administrators log on to the security management screen while the security management multiple access allow option is not setup, only the administrator that logged on first and accessed the session is able to perform the function. The administrator that logged on later is not able to perform any security management function or confirm the error message that says 'in use'.

An authorized administrator, by FMT_MSA.1 and FMT_MTD.1(3), can define the session time-out value of an authorized administrator. The administrator session is locked when there is no security management activity of the authorized administrator during the time of defined session time-out value.

In accordance with FMT_MSA.3, an administrator may modify the initial value of security attributes for the security management session time-out value and for whether or not to allow security management multiple access.

The TOE grants access only to administrators authorized by the TOE manages a security object called MANAGER, and the object is used to allow an authorized administrator to access the TOE. the TOE can allow network groups other than the MANAGER network group as security management access group. For the network groups assigned as the security management access group, the packet filtering security policy which allows the security management access of the TOE is internally established.

Except the security management role and the security management access control described above, the security management function (SW_ADMIN) of the TOE consists of the following 6 detailed functions. The description for these functions are as follows ; Management Function of the Packet Filtering SFP, Management Function of the Intrusion prevention SFP, Management Function of Security objectives, Management Function of audit function, Management Function of I&A, Management Function of TOE security configuration.

Management Function of the Packet Filtering SFP

a) Based of FMT_MSA.1 and FMT_SFM.1, the following security attributes of the packet filtering SFP rules can be determined. Two operation specified in the packet filtering security policy rules are Allow and Deny. SW_ADMIN configures the sequence number of the packet filtering SFP rules and the network interface that handles the inbound traffic in accordance with the value specified by authorized administrator. When determining the interface for a traffic flowing from a source outside the TOE to a destination inside, the external interface handled at the initial inbound must be determined to allow the information flow. Otherwise, the information flow is denied by rules. Also, SW_ADMIN manages the packet filtering SFP rules to allow information flow in case the service of network packet is included in the security attributes of the packet filtering SFP rules. SW_ADMIN manages the packet filtering SFP rules to select audit record generation by the root/policy administrator's determination. SW_ADMIN can configure the security attribute to allow bidirectional information flow and fragmentation of the network packet based on the values defined by the root/policy administrator's. When the root/policy administrator defines security attributes of the packet filtering SFP rules, SW_ADMIN can make the intrusion prevention SFP rule by selecting the value of the risk level security attribute in accordance with the root/policy administrator's determination

b) Based on FMT_MOF.1(2), an authorized administrator can activate or deactivate each rule of the packet filtering SFP. A deactivated security policy exists but amounts to nothing for it does not handle the traffic. The authorized administrator (including policy administrator) creates rules in the first place. The rules, yet deactivated, must be activated to enforce them by applying to the TOE, and again the rules can be applied to the SWIP of the TOE by requesting 'application' for all of the rules. SWIP(the TOE IP), a virtual IP driver of the TOE, operates attached to the IP driver of the kernel in the form of a kernel loadable module, and transmits packets by allowing or denying according to the security policy.

c) Based on FMT_MSA.1, an authorized administrator may change the applying sequence of the packet filtering SFP rules. The packet filtering SFP rules are applied to information flow when checking an inbound or outbound packet according to the order defined by root/policy administrator.

d) Because the default value of the security attributes of "Policy in the packet filtering SFP rules" is 'Deny', all accesses and flows except for the authorized administrator (including specific privileged administrators) are impossible if there exist no rules.

e) Based on FMT_SMF.1, an authorized administrator is able to review the current state applied of packet filtering through the TOE. This can be searched by destination, source, protocol, or port, and currently applied session can be confirmed by reviewing the whole.

Management Function of the Intrusion Prevention SFP

a) The intrusion prevention SFP rules applied to the TOE consists of attack pattern matching, protocol anomaly check, and traffic anomaly check. Based on FMT_MSA.1, FMT_MTD.1(1), and FMT_SFM.1, an authorized administrator may query/modify/delete/generate security attributes included in the intrusion prevention SFP rules. Attack pattern manages attack rules by grouping them by services. ’Attack pattern’ is managed as ‘attack type’ and ‘attack rule’. Managing ‘attack rules’ by grouping is ‘attack type’, and these two are ‘attack patterns’. The rules of an actual attack are defined in attack rules, and attack types are selected when the attack rules are defined. The attack rules are written in pattern characters and they are established by an authorized administrator to be able to check the attributes of the attack packet. Traffic anomaly detection function consists of session restriction, SYN Flooding attack defense, and packet restriction. Session restriction is that the number of sessions to allow per second can be set to reject the session beyond the limit number of session. The session will be set to list on the Black List If it exceed to the limit number of the session. SYN Flooding attack defense allows to set the time and quantity limit to regard as an attack if SYN packets occur beyond the set limit. To restrict packets, the number of UDP, ICMP packets to allow per second can be set to reject the packets beyond the limit.

b) Attack patterns can be categorized into signatures added by the administrator, signatures downloaded from the DI rule update server, and signatures included as default. Addition, deletion, or modification of an attack pattern can only be done for attack patterns added by the administrator. For attack patterns downloaded from the DI rule update server and attack patterns included as default at the installation, authorized administrator is allowed only to review or modify the policy (warning, rejection), in order for the authorized administrator to maintain the attack patterns.

Regarding the risk level of each attack rule, all attack rules corresponding to the risk level of attack rules mentioned here are applied if the intrusion prevention security policy for the source and destination is selected, and the risk level of attack rules is selected from the TOE packet filtering SFP management described above.

c) Based on FMT_MSA.3, an administrator can modify the initial value of security attributes used in the traffic anomaly check or protocol anomaly check.

d) Based on FMT_SMF.1, an authorized administrator can confirm the IP and information of a host who is blocked its packets for being registered on the black list by the traffic anomaly check function of the intrusion prevention security policy.

Management Function of security Objects

The TOE provides the following security objects for an authorized administrator to achieve simple management of the security policy for a large-scale system. Once the objects are defined, they are used in the SFP rules. Based on FMT_MSA.1 and FMT_SFM.1, the security management function may review, add, modify, or delete the following objects.

- Service Group Object : composed of protocol or port number and groups several ports under one service name.
- Network Group Object : composed of IP address and may be IP address of a host or a network (IP class).

Among network group objects, the MANAGER group is generated at installation of the TOE, and only the administrator who has an IP address registered on the MANAGER group may log on the TOE to perform security management.

Management Function of Audit Function

a) Based on FMT_MSA.1, SW_ADMIN establishes whether or not to generate audit records in security audit function configuration, and provides the function that sets the time for the TOE. SW_ADMIN enable

b) For providing time stamps, SW_ADMIN enables the authorized administrator to set manually the time or to synchronize automatically the time of the TOE with NTP server by downloading time resource from NTP server.

c) Based on FMT_MSA.1, FMT_MTD.1(1), and FMT_SMF.1, SW_ADMIN provides the function that generates, deletes, modifies, or reviews the alarm rules for security related events. If an audit record is generated from a source/destination which corresponds to the type of security related event which the authorized administrator selected, this security management function performs the methods (E-mail, SMS message) established in this alarm rule.

d) Based on FMT_MSA.1, FMT_MTD.1(3), and FMT_SMF.1, SW_ADMIN can set the limit on the number of overlapping audit records. Among audit record fields, if particular items specified by the administrator generate the same audit records more than the number specified, they are considered duplicated logs.

e) Based on FMT_MSA.1, FMT_MTD.2(1) and FMT_SMF.1, SW_ADMIN sends an alarm to the administrator or stops operation of the TSF service, and provides to an authorized administrator the function that maintains the threshold for indicating the audit trail exceeds pre-defined limit or is full , and that maintains actions to be taken in case the audit storage capacity is smaller than the threshold.
When the audit storage capacity exceeds the threshold (alarm % value) defined by the authorized administrator (default value 5%: the audit storage's remaining space is 5% or smaller), SW_ADMIN sends a warning message to the specified E-mail address of the administrator or an SMS message.
When the audit storage capacity reaches the overall service halt % meaning the audit trail full (default value 3%), the TOE stops all services other than the access of the authorized administrator who belongs to the security management access group (MANAGER network group) in order to prevent any further generation of audit records.

f) Based on FMT_MSA.3, an administrator can modify the default value for the security attributes of the number of audit record overlaps, threshold for preventing of audit data loss, and generation of audit records.

Management Function of I&A Function

SW_ADMIN allows an authorized administrator to establish authentication data for each administrator based on FMT_MSA.1, FMT_MTD.1(2) and FMT_SMF.1.

An administrator's ID should be composed of 3~30 characters of alphabet/number/special characters beginning with an English alphabet. SW_ADMIN verifies if a password is a combination of English alphabets and numbers, or special characters consisting of 7 or more and 40 or less characters. If not, SW_ADMIN displays an error message to the administrator in order to establish a secure password.

Based on FMT_MTD.2(2) and FMT_SMF.1, if an authorized administrator exceeds the specified limits number of failed authentication attempts, actions specified by the authorized administrator such as disabling that administrator's account or authentication delay are performed. The disabling administrator's account action block account and allows no more to authenticate with the same ID, and the authentication delay action delays the screen in which the administrator's account is to be entered for 10 seconds then displays it.

In order to lock an interactive authorized administrator session after surpassing authorized administrator's session timeout value, SW_ADMIN can set that session timeout value defined by an authorized root administrator.

Management Function of TOE Security configuration Setup Function

a) Based on FMT_MSA.1 and FMT_SMF.1, SW_ADMIN provides integrity check results review function to an authorized administrator. It also provides initialization function and integrity check time setup function to perform integrity check and allows an authorized administrator to confirm the results of the latest integrity check.

b) Based on FMT_MSA.1, FMT_MTD.2(3) and FMT_SMF.1, SW_ADMIN performs a self-test between the time intervals specified by an authorized administrator. It checks the operation of the TOE's major daemons and restarts the ones terminated abnormally.

c) SW_ADMIN is able to perform the following setups for the environment setup:

- Based on FMT_MSA.1, FMT_MOF.1(1), FMT_MTD.1(2), FMT_MTD.1(3) and FMT_SMF.1, set the environment for HOT LIST.
  Set the automatic update time, download the latest update information and display it on the screen. After confirming this, authorized administrator applies the latest HOTLIST, or it can be applied without the administrator's confirmation.
  Upon an administrator's request, manually check whether there is information to be updated, and mark it on the latest update list if there is a HOTLIST to be updated. The authorized administrator applies this after confirming.
- Based on FMT_MSA.1, FMT_MTD.1(3) and FMT_SMF.1, TOE system time setup function is provided.
- Based on FMT_MSA.1, FMT_MTD.1(3), and FMT_MOF.1(1), criteria determining a network failure (Physical link state check, Link state check using ICMP (check subject's address, time, response failure or number of success)) setup function is provided.

d) Based on FMT_MSA.1, network interface's IP can be configured.

e) Based on FMT_MSA.3, TCP/UDP session time-out, an administrator can modify the initial value of security attributes for TOE system time setup, network state check function, HOTLIST update environment setup, integrity check setup and self-test check cycle.

Security Management of TSF through Console

When network failure (H/W failure) occurs, the administrator can access the TOE only through the console. In that case, the administrator can use the following security management functions through the console.

- Network IP Setup – allows current IP set-up. IP setup is only possible if the TOE uses a static IP.
- Add, Delete, Review, or Apply the SFP rules– Though it performs the same functions with the 'TOE packet filtering security policy management function' of SW_ADMIN, there is no function which modifies the security policy already generated.
- Review, Add, or Delete Security Object – Though it performs the same functions with the 'TOE audit record related management function', there is no function which modifies the security object already generated. And only network groups can be deleted.
- Time Setup – An administrator can set the OS time.
- Review Audit Record Information – review the real time audit record and the audit record stored in DB
- Delete Audit record stored in audit trail storage – Deletes audit record to increase audit trail storage capacity.

Functional Requirements Satisfied: FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.2(1), FMT_MTD.2(2), FMT_MTD.2(3), FMT_SMR.1, FMT_SMF.1

6.1.2 Security Audit (SW_AUDIT)

Requirements of the security audit function described in this section include generation of audit record, audit record review, protection of audit trail storage, and selectable audit record review.

The audit record generated from each module is transferred to the log server module, and the log server module checks the audit record and if it is a subject of alarming, generates an alarm and stores it in the audit record DB.

Audit Record Generation

a) Audit record generation activates or deactivates the rules that are selected the audit record option among the security attributes of packet filtering security policy, and determines whether or not to allow the rule to generate audit records. SW_AUDIT generates audit records only for the rules established to generate audit records. The SWIP (the TOE virtual IP driver) which actually handles packets generates audit records according to this setup and transfers them to the log server module which stores audit records. For all other auditable events occurring in the TOE, each TSF transfer the information need in audit record generation to the log server and the log server generate and store an audit record for the auditable event based on information received.

b) For auditable events described in [Table 5-2], at least the following information should be stored in the audit record data record:
   - Date and time of event
   - Type of event (service)
   - Importance of event (ERROR, WARNING, NOTICE, ACCOUNT, MANAGE, DPI)
   - Sequence number
   - Protocol
   - Object identity (destination address, port)
   - Subject identity (source address, port)

- Number of overlaps – the number of overlaps for each packet is marked as the authorized administrator established in SW_ADMIN.
- Reason and information of a failed event – success or failure, rejection and its reason of an event.

c) SW_AUDIT audit records for each administrator all series of actions which an authorized administrator manages security policies specified in SW_ADMIN.

d) SW_AUDIT monitors generated audit records and sends an e-mail or SMS message to the authorized administrator when audit records which correspond to the alarm rules that the authorized administrator established in SW_ADMIN.

e) However, when an auditable event categorized by the importance established for each auditable event as important audit record occurs, the TOE informs the authorized administrator of potential security violations by sending alarms about the following events although they are not established in the alarm rules.

- Audit record storage shortage warning
- Intrusion detection
- All failures detected by the TSF
  (process shortage, socket bind error, file opening failure, service error, SWIP device opening error, system error, memory shortage, program execution error, kernel image opening failure, kernel image damage)
- Failure in getting a local system host name
- Integrity error
- Audit record generation error
- Database HASH calculation error

f) SW_AUDIT generates audit records for the log types that indicate the importance of the event (ACCOUNT, WARNING, NOTICE, ERROR, MANAGE, DPI) and enable to include or exclude auditable events from the set of audited event based on the services that indicate the type of event (security management, authentication server, PACKET, IP Broadcast) and the protocol of the event (TCP, UDP, ICMP, OSPF, others).according to administrator's audit setup

g) Audit records which occurred within the time and as many as the number set by the authorized administrator are considered duplicates. Determine overlapping of audit records and for exact duplicates, generate one overlapping audit record for each indicating number established by the authorized administrator instead of generating as many audit records as they occurred. The option that enables determining duplication are source address and port, destination address and port, protocol, and the attack rule ID of intrusion prevention security policy. Among these options, if the ones specified by the administrator are the same, the audit records are considered to overlap each other and the audit record is not generated.
The TOE determines whether to audit record every packet of ICMP packets and DENY packets, or to audit record ICMP packets only in sessions but not DENY packets.

Audit Review

a) SW_AUDIT provides conditional review, search and monitoring functions for all audit records only to the authorized administrator (root administrator and log administrator). Especially, the policy administrator who is not entitled to the log privilege can only use the audit record review function. An authorized administrator can review audit records by type or specific date and time.

b) An authorized administrator (root administrator, log administrator) reviews desired audit records with the stored TOE audit records by the following conditions. Results of the search can be viewed by the authorized administrator (including the log administrator) through a web browser.

- Date and time of the event
- Importance of the event (log type)
- Event type (service)
- Subject identity (source IP, port)
- Object identity (destination IP, port)
- Keyword
- Output type (display or file)

- Direction of search (from previous time, from the most recent time)

c) An authorized administrator (root administrator, log administrator) of the TOE can view audit records in real-time as soon as they are generated. IF the authorized administrator wishes to see a current audit record, he/she can obtain the information of the desired audit record in real-time by entering the suitable value for its condition.

- Importance of the event (log type)
- Event type (service)
- Subject identity (source IP, port)
- Object identity (destination IP, port)
- Keyword

Audit Trail

SW_AUDIT prevents audit records from being lost due to storage exhaustion with the following method.

Send a warning message (e-mail or SMS service) to the administrator when a loss of audit data is expected (if audit storage's remaining space is less than 5%).

Send a warning message to the administrator and stop all services of the TOE by deactivating all packet filtering security policies when the audit storage is exhausted (if audit storage's remaining space is less than 3%). When services are stopped due to audit storage exhaustion, only the authorized administrator can access security management of the TOE and perform the security management function.

The audit storage's remaining space mentioned above is the default value, and can be set at an administrator's discretion.

The TOE checks automatically the audit storage's remaining space every minute.

TOE Time Stamp

a) SW_AUDIT uses a reliable time stamp for the consistency of audit records (SW_AUDIT). SW_AUDIT brings ever consistent time source from the external NTP server and applies it to the TOE. An authorized administrator sets the NTP.

b) Other TSF use TOE Time Stamp to periodically perform HOTLIST automatic update and TOE self-test

Functional Requirements Satisfied: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG.3, FAU_STG.4, FPT_STM.1

6.1.3 User Data Protection (SW_UDP)

SW_UDP provides security policies of such mechanisms as the packet filtering or the deep inspection. SW_UDP performs the function of protecting a user's data (network packet) by, using SWIP, applying the information flow control policy to the packet received through the network interface.

The information flow control SFP is implemented in two ways. One is the packet filtering SFP and the other is the intrusion prevention SFP. The two SFPs are mutually complementary and not exclusive of each other. A packet which came into the TOE is first checked the packet filtering security policy basically, and then only the one allowed is applied the detailed intrusion prevention security policy. Packets that come inbound to the TOE are applied to the intrusion prevention SFP rules. The packet allowed by the packet filtering is checked only the rules that correspond to the attack pattern level selected from the security attributes of the packet filtering security policy when applying the intrusion prevention security policy.

The intrusion prevention SFP implements security policies in three mechanisms. They are attack pattern matching and protocol anomaly detection, and traffic anomaly detection.

The packet that passed through the packet filtering security policy is applied the traffic anomaly check and the protocol anomaly check one by one, and lastly the attack pattern check.

The sequence of information flow control for packet filtering and intrusion prevention is as fallows;

① In first, traffic anomaly detection mechanism examine whether a packet register on black list table

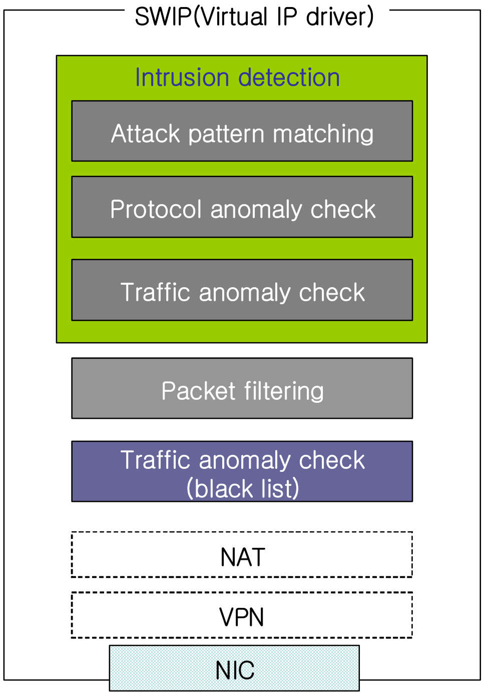
② And then perform packet filtering mechanism

③ Perform traffic anomaly detection excluding examination of the black list

④ Perform protocol anomaly detection

⑤ Perform attack pattern matching

⑥ Lastly perform scanning detection based on audit record generated



[Figure 6-1] Application of Information Flow Control Policy

The Packet Filtering SFP

a) When a packet is sent into the TOE, only the packet that does not register in black list flows based on the packet filtering SFP rules. SW_UDP blocks the packet in case it registers in black list. The packet filtering rules define the overall information flow control policy of the TOE. The packet filtering policy enforces the following policies depending on the source, the destination, and the service of the packet.

- Allow
- Deny

b) The user data protection function of the TOE performs on the adequate information – source address, destination address, protocol, and port number - of the packets that pass through the TOE. With this information, the TOE decides whether to allow or deny the packet. Moreover, access control is performed upon the abundant information included in the IP header of the packet. The following is the list of items by which the packet filtering security policy allows or denies a packet passing through the TOE.

- Sequence Number
- Network Interface
- Presumable Source Network Group (IP)
- Presumable Destination Network Group (IP)
- Applied Service (the Name Mapped as the Port of Use) Group
- Bi-directional Policy
- Allow or Deny of Fragmentation Packet

c) SW_UDP makes the packet filtering SFP rules allowing response packets based on the information above. SW_UDP always checks the current session's stage by keeping the session information of TCP and rejects any illegal packet, any that does not conform to the rules, or any that does not have the packet filtering security policy.

d) SW_UDP confirms that the session is 443 port using SSL before performing administrator (including administrators with specific privilege) identification and authentication. When the session is confirmed SSL communication of 443 ports, create an SSL channel using the SSL function supported as an IT environment, and identify the IT identity of the administrator. Administrator's IT identity identification is allowed at the packet filtering if the administrator is confirmed the IP to belong to the security management access group. An allowed administrator is performed an authentication by confirming the administrator's ID and password according to SW_INA.

e) The packet filtering SFP always allow information flow from TOE to external IT entity (i.e. outbound packet). All external IT entities except a remote administrator PC connect to TOE by sending a response packet against a TOE packet. The packet filtering SFP also allow the response packet. Therefore for identification of external IT entities, SW_UDP registers firstly an outbound packet on a session table and then response packet to be a pair of outbound packet. The value for the security attributes of external IT entities for Identifying is stored in DB of TOE, the information stored are as fallows;

- DI rule Update Server : IP address defined by authorized administrator and 9999
- NTP Server : IP address defined by authorized administrator and 123 port

The Intrusion Prevention SFP

a) SW_UDP performs successively traffic anomaly check, protocol anomaly check, and attack pattern check on the packets allowed by the packet filtering SFP. If the traffic anomaly check or the attack pattern check is not to be performed by administrator's setup, skip the one and perform the other two one by one. For example, if the administrator set not to perform the traffic anomaly check, the packet is applied the protocol anomaly check and the attack pattern check after performing the packet filtering security policy.

b) Intrusion prevention security policy rules are applied in two ways. One is for an authorized administrator to create the rules him/herself, and the other is to apply urgent rules by updating them from a trusted external IT entity, the DI rule update server. The rules received from the DI rule update server are guaranteed their confidentiality and integrity by using SSL protocol. The rules are stored in the environment setting file and applied. This is to apply the important security rules updated at any time to the site which the TOE is installed. The rules downloaded from the DI rule update server can be applied immediately to the TOE in accordance with the administrator's setting or after the administrator's confirmation.

c) The intrusion prevention security policy is divided into the 'attack pattern check' function which rejects specific signature and worm virus, the 'protocol anomaly check' function which checks and rejects any abnormal protocol, and the 'traffic anomaly check' function which controls traffic.

   The intrusion prevention security policy performs traffic anomaly check on the session applied by the packet filtering security policy.

   The intrusion prevention security policy monitors the sessions allowed by the packet filtering security policy and restricts sessions if sessions generated per second at one source are more than the value set by the authorized administrator. This is to prevent a sudden increase in the traffic because a sudden increase in the traffic is related to the increase of worms. Furthermore, the intrusion prevention security policy function controls as Black List the source addresses where sessions increase as many as the number set by the authorized administrator during the time set by the authorized administrator, and rejects all traffic from those source addresses.

The intrusion prevention security policy function also controls SYN Flooding. A SYN session is terminated if there is no ACK for the SYN packet sent from a source address during the time (second) set by the authorized administrator.

Also, the number of ICMP and UDP packets that can be created from a source is restricted by rejecting the packets created more than the number of packets per second set by the authorized administrator.

d) The intrusion prevention security policy checks the packets allowed by traffic anomaly check whether they are normal packets by a proper protocol. Protocol anomaly check items provided by the TOE are as follows.

IP

- Source route: reject packets with source routing information on the IP header.
- IP Spoof : reject IP spoofing attack packets which send spoofed source IP address.
- Martian address: reject packets with abnormal source IP address.
- Non-existent address: reject packets from an IP address which is not assigned by the INNA.

TCP

- Poisoned Reversed flag: rejects packets which the TCP reserved flag is set at a value other than 0. (Fingerprint Scan)
- Illegal Control Flags: reject packets with an abnormal TCP control flag.
- Illegal header length: reject packets with abnormal TCP header length.

UDP

- Echo Loop: reject UDP echo loop attack packets.
- Illegal length: reject packets with abnormal UDP header length.

ICMP

- Bad Echo Request: reject packets which the checksum of ICMP Echo Request is incorrect or the code is abnormal.
- Bad Echo Reply: reject packets which the checksum of ICMP Echo Reply packet is incorrect or the code is abnormal.
- Scanning Detection
- Port scanning, Address Scanning, Trap Ports Scanning detection: reject by detecting port scanning using packet log as statistics data.

e) Attack pattern check is performed after protocol anomaly check. The attack pattern check consists of two parts which are the attack type and the attack rule. The attack rule includes all elements that define an attack. It consists of signature, destination port L3/L4 protocol, and level. The attack rules downloaded from the rule server are registered here and cannot be deleted by the authorized administrator. Among these attack rules, the ones that attack application programs of the same subject can be grouped by service. These are attack types. Attack rules of the intrusion prevention security policy have risk levels. Risk level (level 1-High, level 2-Moderate, level 3-Low, level 4-Minimal) determines the importance of a rule and allows the authorized administrator to select as it is categorized. This distinguishes attack rules. Attack types consist of minimum, regular, maximum, and all. This allows the authorized administrator to determine the level of Deep Inspection when defining the policies of packet filtering.

Session Termination

a) The TOE forcibly terminates sessions generated beyond the restricted number of sessions per second during the traffic anomaly check of the intrusion prevention security policy set by the authorized administrator for sessions that pass the TOE.

b) The TOE forcibly terminates sessions if SYN packets are generated more than the limited number of SYN packets per second from the same source during the traffic anomaly check of the intrusion prevention security policy set by the authorized administrator for sessions that pass the TOE.

c) The TOE forcibly terminates sessions if the authorized administrator requests session termination of reviewed sessions using the ‘TOE packet filtering security policy management function’ of SW_ADMIN.

Functional Requirements Satisfied: FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2), FIA_ATD.1(1), FPT_RVM.1, FPT_SEP.1, FIA_UID.2(1), FTA_SSL.3, FRU_RSA.1. FTP_ITC.1

6.1.4 Identification and Authentication (SW_INA)

The TOE implements the identification function in the packet filtering SFP to allow all actions after identifying an IT entity or an administrator IT entity. When an information flow which corresponds to the source-destination determined in the packet filtering security policy of the TOE occurs, the IT entity that requested the information flow is not allowed the flow of the information before being identified since the IT entity is able to use the rules of the packet filtering security policy after it is identified. Administrator's identification and authentication enforces packet filtering so an administrator would request authentication to the TOE and use the security management only when allowed after authentication.

I&A Mechanism for authenticating Administrator

a) SW_INA has an authentication mechanism for administrators. The authentication method is password mechanism which uses IDs and passwords which are general passwords. The root administrator, log administrator, and policy administrator all use the same authentication mechanism.

b) An administrator (including administrators with specific privilege), in accordance with SW_UDP, is identified and authenticated by confirming his/her ID and password after the administrator IT entity is identified.

c) SW_INA authenticates an administrator in remote location based on the administrator's ID &PWD transferred using SSL protocol. SW_UDP initiate secure communication channel (SSL channel) and SW_INA utilize the established secure channel by SW_UDP.

d) When an administrator enters an administrator's ID and password to be authenticated, the security management server brings the administrator's authentication data (password, authentication method, administrator's state, number of fails, privilege) using identifier as it's ID. If the password entered by the user corresponds with the password attribute value and the administrator's state is normal, the administrator is granted the functions befitting to the administrator's privilege.

e) the TOE Password authentication mechanism is used to authenticate administrators and performs authentications with the following password characters.

- A password must consist of more than 7 and less than 40 characters.
- There are 93 possible characters except the special character '&' including the following: "a-z(26), A-Z(26), 0-9(10), ! @ # $ % ^ * ( ) _ + | ` - = \ { } : " < > ? [ ] ; ' , . / "
- A password identical with the administrator's ID is not allowed.

While an administrator performs an authentication, the TOE shows the administrator only his/her ID and echoes the password with '*' which the administrator cannot see either.

The administrator identification and authentication function is implemented by permutational mechanism (password mechanism). Its SOF is SOF-high.

Authentication Failure Handling Method

When an administrator fails to be authenticated, determine whether the administrator's ID failed more than the number of authentication failures established (basic 0), and execute user break or authentication delay if the administrator failed more than the number established.

a) Disabling of administrator account : If an ID's action in authentication failure is set as user break and fails to be authenticated more than the authentication failure number, the ID cannot be authenticated any more.

b) Authentication Delay : If an ID's action in authentication failure is set as user delay and fails to be authenticated more than the authentication failure number, the screen to enter the administrator's account is displayed after being delayed for 10 seconds.

Session Locking

An authorized administrator's session logged on through the TOE is locked if there is no action beyond the time set by the authorized administrator. If the authorized administrator tries to make any changes through the locked security management session, the TOE unconditionally displays the re-identification and authentication screen to allow re-authentication through the security management session. This is a function which protects the TOE's security management screen by locking it when the time limit is surpassed while maintaining the SSL session.

Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1(2), FIA_UAU.1, FIA_UAU.7, FIA_UID.2(2) , FTA_SSL.1

6.1.5 TSF Protection (SW_PT)

SW_PT protects the TSF domain from unreliable subjects and stores the hash values of the TSF environment data and TSF execution data. When an administrator logs on to the TOE for managing, periodically, and at the authorized administrator's request, the TOE verifies the integrity by comparing with the stored hash values. Also, it checks the link status of its network interface.

TOE Abstract Machine Check

the TOE checks the link status of its own network interface, and using the ICMP ping checks the link status of correspondent the TOE.

TOE Domain Separation and Non-bypassability

The TOE core engine (virtual IP driver) protects the TSF domain where the SFP is applied from any interference or infringement of TSF related unreliable subjects when applying access control by creating an accounting device to generate packet filtering rules and audit records. (Audit records are stored in the SWIP buffer before they are transferred and stored in the log server module. The device created in the SWIP for generation of audit records and temporary storage is the accounting device.)

Transferring TSF Data on a Secure Channel

SW_PT detects unauthorized modification of the TSF data because the SSL is used between the TOE and the web browser which is the administrator's interface. In case an unauthorized modification occurs, the modified content is not reflected on the TSF data. Data between the security management server and the web browser which is the administrator's interface are protected by using the confidentiality algorithm (3DES), the integrity algorithm (SHA-1). This is the same when performing an administrator authentication. An administrator authentication is performed using the trusted SSL channel created by using the SSL certificate issued at the installation of the TOE.

TOE Self-test

There are two ways in which the TOE guarantees a stable operation of security functions.

a) First, SW_PT always checks the status of the daemons which are the components of other the TOE. If a daemon operating in the TOE is dead, SW_PT always restarts the daemon. Also, SW_PT executes the programs that perform the TSF in order.

b) Second, the integrity check guarantees the security of the environment files and execution files that execute the TSF. To protect the TSF data, SW_PT stores the hash values of the TSF environment data and TSF execution data and verifies the integrity by comparing with the stored hash values when an administrator logs on to the security management server, periodically, and at the authorized administrator's request, and informs the authorized administrator of any changed information. Also, it checks the link status of its network interface. If an integrity error occurs by SW_PT when the authorized administrator accesses the TOE through the security server, the TOE displays the error on the security management screen for the error to be handled. The authorized administrator can regenerate hash for the files that integrity error occurred. The integrity check and the TOE process check are performed at the initial operation of the TOE, periodically, and at the time specified by the authorized administrator or at an immediate request.

Self tests are performed after each time interval determined in FMT_MTD.2(3), at the request of the administrator, or at the TOE operation. However, integrity checks are done periodically in addition to the time interval determined by FMT_MTD.2(3).

The TSF protection function is implemented by permutational mechanism (TSF data integrity check using SHA-1). The SOF is SOF-high.

Availability

SW_PT provides the following functions to maintain functional operation when the following failures occur.

a) H/W Failure : Using the ICMP ping for network interface, the connection with a specific gateway is checked. If there is no reply within time limit specified by the authorized administrator, a failure is assumed to have occurred and the network interface is changed to Link Down after the authorized administrator is reported an alarm.

b) S/W Failure, Buffer Overflow Failure : SW_PT always checks the state of daemons which are components of other the TOE, and restarts the daemon when it is discontinued while in operation in the TOE. When the daemons are discontinued due to a buffer overflow, SW_PT checks and restarts them.

When it is impossible to communicate with the TOE due to the failures described above, the administrator can conduct management activities such as network establishing using the system console.

Functional Requirements Satisfied: FPT_AMT.1, FPT_FLS.1, FPT_RVM.1, FPT_SEP.1, FPT_TST.1, FRU_FLT.1, FTP_ITC.1

6.2 Assurance Measures

The assurance requirements described in this ST conforms to the assurance requirements of the Common Criteria (1) part 3. The TOE provides documents in [Table 6-1] which verifies the assurance requirements satisfying SAR described in chapter 5.

Assurance Component ID	Assurance Component Name	Assurance Document
ACM_AUT.1	Partial CM automation	SECUREWORKS IPSWall 1000 V4.0 Configuration Management Documentation V1.9[ACM]
ACM_CAP.4	Generation support and acceptance procedures	SECUREWORKS IPSWall 1000 V4.0 Configuration Management Documentation V1.9[ACM]
ACM_SCP.2	Problem tracking CM coverage	SECUREWORKS IPSWall 1000 V4.0 Configuration Management Documentation V1.9[ACM]
ADO_DEL.2	Detection of modification	SECUREWORKS IPSWall 1000 V4.0 Delivery Documentation V1.3[DEL]
ADO_IGS.1	Installation, generation, and start-up procedures	SECUREWORKS IPSWall 1000 V4.0 Installation Guidance V1.21[IGS]
ADV_FSP.2	Fully defined external interfaces	SECUREWORKS IPSWall 1000 V4.0 Functional Specification V1.13[FSP]
ADV_HLD.2	Security enforcing high-level design	SECUREWORKS IPSWall 1000 V4.0 High-level Design V1.7[HLD]
ADV_IMP.1	Subset of the implementation of the TSF	SECUREWORKS IPSWall 1000 V4.0 Implementation Representation V1.2[IMP]
ADV_LLD.1	Descriptive low-level design	SECUREWORKS IPSWall 1000 V4.0 Low-level Design V1.5[LLD]
ADV_RCR.1	Informal correspondence	SECUREWORKS IPSWall 1000

Assurance Component ID	Assurance Component Name	Assurance Document
	demonstration	V4.0 Correspondence Analysis V1.5[RCR]
ADV_SPM.1	Informal TOE security policy model	SECUREWORKS IPSWall 1000 V4.0 Security Policy Modeling V1.6[SPM]
AGD_ADM.1	Administrator guidance	SECUREWORKS IPSWall 1000 V4.0 Administrator Guidance V1.23[ADM] SECUREWORKS IPSWall 1000 V4.0 Operation Guidance V1.14[OPR]
AGD_USR.1	User guidance	*N/A
ALC_DVS.1	Identification of security measures	SECUREWORKS IPSWall 1000 V4.0 Life Cycle Support V1.4[DVS]
ALC_LCD.1	Developer defined life-cycle model	SECUREWORKS IPSWall 1000 V4.0 Life Cycle Definition Documentation V1.5[LCD]
ALC_TAT.1	Well-defined development tools	SECUREWORKS IPSWall 1000 V4.0 Development Tool Documentation V1.3[TAT]
ATE_COV.2	Analysis of coverage	SECUREWORKS IPSWall 1000 V4.0 Test Documentation V1.6[TST]
ATE_DPT.1	Testing: high-level design	SECUREWORKS IPSWall 1000 V4.0 Test Documentation V1.6[TST]
ATE_FUN.1	Functional testing	SECUREWORKS IPSWall 1000 V4.0 Test Documentation V1.6[TST]
ATE_IND.2	Independent testing-sample	SECUREWORKS IPSWall 1000 V4.0 Test Documentation V1.6[TST]

Assurance Component ID	Assurance Component Name	Assurance Document
AVA_MSU.2	Validation of analysis	SECUREWORKS IPSWall 1000 V4.0 Misuse Analysis V1.5[MSU]
AVA_SOF.1	Strength of TOE security function evaluation	SECUREWORKS IPSWall 1000 V4.0 Strength of Function Analysis V1.4[SOF]
AVA_VLA.2	Independent vulnerability analysis	SECUREWORKS IPSWall 1000 V4.0 Vulnerability Analysis V1.2[VLA]

[Table 6-1] Assurance Requirements vs. Assurance measures

* User guidance is not provided because general users are precluded from the logical scope of the TOE and general user management is not described in class FMT of the TOE SFRs. Therefore, assurance measures for AGD_USR.1 are not applicable.

7 Protection Profile Claims

This chapter is documented to show this ST conforms to IPSPP.

7.1 IPSPP reference

The TOE satisfies all the requirements by referencing the following protection profile.

Network Intrusion Prevention System Protection Profile V1.0 5/24/2005 [IPSPP]

7.1.1 Redefined Protection Profile

The following security functional requirements (SFRs) of the protection profile are redefined for this ST.

Functional Component	Name
FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit Data Generation
FAU_SAA.1	Potential Violation Analysis
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FDP_IFC.1(1)	Subset information flow control(1)
FDP_IFC.1(2)	Subset information flow control(2)
FDP_IFF.1(1)	Simple security attributes(1)
FDP_IFF.1(2)	Simple security attributes(2)
FIA_AFL.1	Authentication failure handling
FIA_ATD.1(1)	User attribute definition(1)
FIA_ATD.1(2)	User attribute definition(2)

Functional Component	Name
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected authentication feedback
FMT_MOF.1(1)	Management of security functions behavior(1)
FMT_MOF.1(2)	Management of security functions behavior(2)
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1(1)	Management of TSF data(1)
FMT_MTD.1(2)	Management of TSF data(2)
FMT_MTD.1(3)	Management of TSF data(3)
FMT_MTD.2(1)	Management of limits on TSF data(1)
FMT_MTD.2(2)	Management of limits on TSF data(2)
FMT_MTD.2(3)	Management of limits on TSF data(3)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FMT_AMT.1	Abstract machine testing
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FRU_FLT.1	Failure with preservation of secure state
FRU_RSA.1	Maximum quotas
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1	Inter-TSF trusted channel

[Table 7-1] SFRs redefined from IPSPP

※ FDP_IFC.1(1) in IPSPP [all rejection policy] was refined into [packet filtering security policy], [all permission policy] of FDP_IFC.1(2) was refined into [Intrusion prevention security policy] by ST author.

7.1.2 Protection Profile Addition

The following is a list of assumptions, organizational security policies, security objectives and requirements for the IT environment outside of PP added for this ST.

Name	Description
A.SecureTOEExternalServer	Both the NTP(Network Time Protocol) Sever providing trusted external time source for functions of the TOE and the DI Rule Update Server updating the latest DI rules are secure. The TOE uses SSL protocol to create a trusted channel with the remote administrator PC and the DI rule update server.
A.SSLCertificateoftheTOE	The SECUREWORKS creates the certificate to be used for SSL authentication in advance at installation and stores it in the TOE. The SSL certificate of the TOE is securely generated and managed
OE.TrustedTOEExternal Server	Both the NTP Sever providing trusted external time source for functions of the TOE and the DI Rule Update Server updating the latest DI rules must be secure. The TOE uses SSL protocol to create a trusted channel with the remote administrator PC and the DI rule update server.
OE.SSLProtocol	The TOE calls SSL function to create trusted communication channels with remote administrator console and DI Rule Update Server. The TOE, using SSL protocol, mutually authenticates with SSL certificate of the TOE and administrator’s ID & password, and protects TSF data.
P.SSLCertificateManagement	The SECUREWORKS must securely generate, save, and manage a SSL certificate.
FTP_ITC.1	The TOE provides a trusted channel by calling SSL functions provided as an IT environment and creating SSL protocol.

[Table 7-2] Assumptions, OSPs, Security Objectives, SFR for the IT environment

8 Rationale

This chapter describes the rational why this ST can be used for evaluation. This rational supports the concept that this ST is a complete and dense set of requirements and it provides effective IT security measures. Further, the TOE summary specification addresses requirements. When describing evidence, rationale is individually described with the PP because this ST conforms to IPSPP.

8.1 Rationale for security objective

The following is rationale for security objectives.

Security Objectives(TOE) Security environments	O.Availability	O.Audit	O.Administration	O.TSFDataProtection	O.AbnormaPacketScree	O.DoSAttackBlocking	O.Identification	O.Authentication	O.InformationFlowContr
T.Masquerade		X					X	X	
T.Failure	X			X					
T.AuditFailure	X	X							
T.InboundIllegalInformation			X						X
T.UnauthorizedServiceAccess									X
T.AnomalyPacketTransfer		X			X	X			
T.NewVulnerabilityAttack			X						
T.DoSAttack		X				X	X		
T.ReplayAttack		X					X	X	
T.Bypassing	X								X
T.SnoofingIPAddress		X			X	X	X		
T.UnauthorizedTSFDataModification	X	X		X			X		

Security Objectives(TOE) Security environments	O.Availability	O.Audit	O.Administration	O.TSFDataProtection	O.AbnormaPacketScree	O.DoSAttackBlocking	O.Identification	O.Authentication	O.InformationFlowContr
TE.PoorAdministration			X						
P.Audit		X					X		
P.SecureAdministration			X						

[Table 8-1] Mapping of Rationale for Security Objectives

8.1.1 Rationale for security objective identical to IPSPP

The following is rationale for security objectives identical to IPSPP.

Security Objective	Description
O.Availability	This TOE security objective ensures the TOE availability for providing minimum network service when the TOE is in failure or overloaded from attacks. Therefore, this security objective is to guarantee the TOE availability to counter the threats of T.Failure, T.UnauthorizedTSFDataModification, T.Bypassing, and T.AuditFailure, which means an audit trail storage exhaustion attack.
O.Audit	This TOE security objective is to record the audit events for each user according to TOE audit record policy when a user uses security functions. The TOE guarantees to provide the means to keep the logged audit events safe and review them. That is, the TOE takes actions when the audit trail storage is full. The generation of audit record ensures that the identification of an attacker should be detected through the audit record in case continuous authentication attempts occur. Spoofing attacks, DoS attacks, and attacks of generating and sending abnormal packets can be traced through the audit record. Therefore, this security objective is to counter the threats like T.Masquerade, T.AuditFailure, T.AnomalyPacketTransfer, T.DoSAttack, T.ReplayAttack, T.SpoofingIPAddress, and T.UnauthorizedTSFDataModification, and is to support the organizational security policy of P.Audit.
O.Administration	The TOE controls the illegal access to internal network by establishing information flow control rules to enforce security policy. To do that, the TOE should provide the means to manage the TOE and TSF data safely for the generation and management of TOE configuration data, and the management of the latest vulnerability signature etc. Therefore, this TOE security objective counters the threats like T.InboundIllegalInformation, T.NewVulnerabilityAttack, and TE.PoorAdministration. It also supports the organizational security policy of P.SecureAdministration by providing the means for the

Security Objective	Description
	authorized administrator to manage the TOE securely.
O.TSFDataProtection	When TSF data is modified without administrator's notice due to unexpected external attacks or TOE malfunctions, it may not be able to perform proper security policy. To prevent this event from occurring, the TOE ensures the proper operation of TSF by monitoring the TSF data for intentional or unintentional data changes and checking the integrity of TSF data. Therefore, this TOE security objective counters the threats like T.Failure and T.UnauthorizedTSFDataModification.
O.AbnormalPacketScreening	This security objective ensures that of a large amount of packets coming from the external to the internal network, the packets which are not suitable for the TCP/IP standard, the packets with an internal network address, broadcasting packets and looping packets will not be allowed to come in. Therefore, this TOE security objective is intended to counter the threats such as T.AnomalyPacketTransfer and T.SpoofingIPAddress.
O.DoSAttackBlocking	The attacker can make network DoS attacks on Intranet computers through the TOE. A typical network DoS attack is to exhaust the computer resources by sending too many service requests from a remote attacker. Then the Intranet computer, under the attacks, would prevent legitimate users from using the computer by allocating much of resource for the DoS attacker. To counter this attack, the TOE prevents a specific user from monopolizing the resources of a specific computer so that other legitimate users can use the resources without traffic. Therefore, this security objective is intended to counter the threats like T.DoSAttack and T.SpoofingIPAddress.
O.Identification	The TOE users are either logged-on administrators who manage the TOE with the TOE authentication or external users (IT entities) who just use Intranet computer without the TOE authentication. All the cases of two need the identification function to deal with security events. The identification of administrators is necessary to grant the full responsibility to them and the identification of external entities is necessary to generate the audit record for abnormal packet transmission, prevention of DoS attacks and address disguise attacks and connection trials by external entities. Therefore, this security objective counters the threats like

Security Objective	Description
	T.Masquerade, T.DoSAttack, T.SpoofingIPAddress, T.AnomalyPacketTransfer, T.ReplayAttack, and T.UnauthorizedTSFDataModification. It also assists P.Audit.
O.Authentication	The user who wants to access the TOE should acquire the authentication. The authentication required in the TOE access may be vulnerable to the replay attack made by external entities. The TOE should provide the authentication mechanism, which can endure the replay attack according to the level of external entities. Therefore, this TOE security objective counters the threats like T.Masquerade and T.ReplayAttack.
O.InformationFlow Control	The TOE is installed at the connection point between internal and external networks in order to control the information flow according to the security policy. According to allow/deny policy, this security objective ensure identifying and blocking various attacks on the network which mean virus attacks, e-mail or web services including illegal information and access to the unauthorized service. The TOE ensures the security of internal network by controlling the attacks based on the pre-defined rules and blocking the illegal access to the internal network. Therefore, this TOE security objective counters the threats like T.InboundIllegalInformation, T.UnauthorizedServiceAccess and T.Bypassing.

[Table 8-2] Rationale for security objectives identical to IPSPP

8.2 Rationale for security objectives in TOE environment

The following rationale for TOE environment is classified into two sections. The first is rationale for TOE environment identical to one in IPSPP, the second is rationale for additional TOE environment to one in IPSPP. You can see adequate descriptions in each section.

Security objectives (TOE) Security environments		Security objective identical to IPSPP								Added security objectiv	
		OE.AttackLevel	OE.PhysicalSecurity	OE.SecurityMaintenance	OE.TrustedAdministrator	OE.SecureAdministration	OE.HardenedOS	OE.SingleConnetionPoint	OE.VulnerabililtyListUpdate	OE.SecureExternalITEntity	OE.SSLProtocol
Assumptins, Threats, Threats to the Environment, Security Policy Identical to IPSPP	A.AttackLevel	X									
	A.PhysicalSecurity		X			X					
	A.SecurityMaintenance			X							
	A.TrustedAdministrator				X						
	A.HardenedOS						X				
	A.SingleConnetionPoint							X			
	T.Failure					X	X				
	T.NewVulnerabilityAttack			X		X	X		X		
	T.Bypassing		X					X			
	TE.PoorAdministration				X	X					

Security objectives (TOE) / Security environments		Security objective identical to IPSPP								Added security objectiv	
		OE.AttackLevel	OE.PhysicalSecurity	OE.SecurityMaintenance	OE.TrustedAdministrator	OE.SecureAdministration	OE.HardenedOS	OE.SingleConnetionPoint	OE.VulnerabililtyListUpdate	OE.SecureExternalITEntity	OE.SSLProtocol
	TE.DistributionAndInstallation				X	X					
	P.SecureAdministration				X	X					
Added assumption	A.SecureExternalITEntity									X	
	A.SSLCertificateOfTOE										X
Added OSPs	P.SSLCertificateManagement										X

[Table 8-3] Rationale Mapping to Security Objectives for the Environment

8.2.1 Rationale for security objectives in TOE environment identical to IPSPP

The following is rationale for security objectives in TOE environment identical to IPSPP.

Security objective	Description
OE.AttackLevel	The security objective for this environment is to define the threat agent as one with medium-level motivation, resource, and expertise and chances of the threat agent discovering an exploitable vulnerability are moderate. Therefore, the security objective for this environment is necessary to assist the assumption of A.AttackLevel.
OE.PhysicalSecurity	The security objective for this environment is to ensure that the TOE is installed and operated at a physically secured place so that the TOE is protected from external physical attacks and TOE modification attempts. Therefore, the security objective for this environment is necessary to assist the assumption of A.PhysicalSecurity and to counter the threat of T.Bypassing.
OE.SecurityMaintenance	The security objective for this environment is to maintain the same level of security as the previous one by adopting changed environments and security policy to the TOE operation policy when the internal network environments is changed by configuration changes in internal network, the increase or decrease in host (or in service) and so on. Therefore, the security objective for this environment is necessary to assist the assumption of A.SecurityMaintenance and to counter the threat of T.NewVulnerabilityAttack.
OE.Trustedadministrator	The security objective for this environment is to ensure the trustworthiness of an authorized administrator of the TOE. Therefore, the security objective for this environment is necessary to assist the assumptions of A.TrustedAdministrator and the security policy of P.SecureAdministration, and to counter the threats of TE.PoorAdministration and TE.DistributionAndInstallation.
OE.SecureAdministration	The security objective for this environment is to ensure that the TOE is distributed and installed in a secure way and is configured,

Security objective	Description
	managed, and used securely by the authorized administrator. Therefore, the security objective for this environment is necessary to assist the assumption of A.PhysicalSecurity and the security policy of P.SecureAdministration, and to counter the threats of T.Failure, T.NewVulnerabilityAttack, TE.PoorAdministration, and TE.DistributionAndInstallation.
OE.HardenedOS	The security objective for this environment is to eliminate unnecessary OS services or measures and to harden the weak points in the OS so that the operation system is secure and reliable. Therefore, the security objective for this environment is necessary to assist the assumption of A.HardenedOS, and to counter the threats of T.Failure and T.NewVulnerabilityAttack.
OE.SingleConnetionPoint	The security objective for this environment is to ensure that all communications between internal and external networks are made through the TOE. Therefore, the security objective for this environment is necessary to assist the assumption of A.SingleConnectionPoint, and to counter the threat of T.Bypassing.
OE.VulnerabilityListUpdate	The security objective for this environment is to protect the TOE and the internal network protected by the TOE from external attacks that are exploiting new vulnerability in them by renewing and managing the vulnerability database managed by the TOE. Therefore, the security objective for this environment is necessary to counter the threat of T.NewVulnerabilityAttack.

[Table 8-4] Rationale for security objectives in TOE environment identical to IPSPP

8.2.2 Rationale for security objectives in additional TOE environment

The following is additional items to security objectives in IPSPP.

Security objective	Description
OE.SecureExternallTEntity	This security objective for the environment ensures that the external server with which the TOE interacts for function is secure. Therefore, this security objective for the environment is necessary to support the assumptions: A.SecureExternalITEntity.
OE.SSLProtocol	The security objective for the environment ensures that the TOE creates trusted channels by supporting trusted IT entity authentication and encrypted communication function. Therefore, this security objective for the environment is necessary to assist the assumptions: A.SSLCertificateOfTOE, P.SSLCertificateManagement

[Table 8-5] Rationale for the security objective in added environment

8.3 Rationale for SFRs

Security objective	Security objectives identical to IPSPP								
SFRs	O. Availability	O. Audit	O. Administration	O. TSF Data Protection	O. Abnormal Packet	O. DoS Attack Blocking	O. Identification	O. Authenticatoin	O. Information Flow
FAU_ARP.1		X							
FAU_GEN.1		X							
FAU_GEN.2		X							
FAU_SAA.1		X							
FAU_SAR.1		X							
FAU_SAR.3		X							
FAU_SEL.1		X							
FAU_STG.1		X							
FAU_STG.3		X							
FAU_STG.4		X							
FDP_IFC.1(1)									X
FDP_IFC.1(2)									X
FDP_IFF.1(1)									X
FDP_IFF.1(2)					X	X			X
FIA_AFL.1							X	X	
FIA_ATD.1(1)		X			X	X	X		X
FIA_ATD.1(2)		X					X		
FIA_UAU.1			X	X				X	
FIA_UAU.7								X	
FIA_UID.2(1)		X			X	X	X		X
FIA_UID.2(2)		X	X	X			X		
FMT_MOF.1(1)	X		X						
FMT_MOF.1(2)	X		X						
FMT_MSA.1			X	X					X

Security objective SFRs	Security objectives identical to IPSPP								
	O. Availability	O. Audit	O. Administration	O. TSF Data Protection	O. Abnormal Packet	O. DoS Attack Blocking	O. Identification	O. Authenticatoin	O. Information Flow
FMT_MSA.3			X	X					X
FMT_MTD.1(1)			X	X					
FMT_MTD.1(2)			X	X					
FMT_MTD.1(3)			X	X					
FMT_MTD.2(1)	X		X						
FMT_MTD.2(2)	X		X						
FMT_MTD.2(3)	X		X						
FMT_SMF.1			X						
FMT_SMR.1			X				X	X	
FPT_AMT.1	X			X					
FPT_FLS.1	X								X
FPT_RVM.1									X
FPT_SEP.1				X					X
FPT_STM.1		X							
FPT_TST.1	X			X					
FRU_FLT.1	X								X
FRU_RSA.1						X			
FTA_SSL.1				X					
FTA_SSL.3						X			
FTP_ITC.1			X	X				X	

[Table 8-6] Mapping of Rationale for the SFRs

8.3.1 Rationale for SFRs identical to IPSPP

The following describes rationale for SFRs of the TOE conforming to IPSPP.

FAU_ARP.1 Security alarms

As this component ensures the ability to take reactions in case a potential security violation is detected, it meets TOE security objective: O.AUDIT.

FAU_GEN.1 Audit data generation

As this component ensures that the TOE defines auditable events and generates the audit records, it meets TOE security objective: O.AUDIT.

FAU_GEN.2 User identity association

As this component requires user identification to define auditable events and to trace the association of audit records with users, it meets TOE security objective: O.Audit.

FAU_SAA.1 Potential violation analysis

As this component ensures the ability to monitor the audited events to indicate a potential violation of the TSP, it meets TOE security objective: O.AUDIT.

FAU_SAR.1 Audit review

As this component ensures the capability for authorized administrators to review information from the audit records, it meets TOE security objective: O.AUDIT.

FAU_SAR.3 Selectable audit review

As this component ensures the ability to perform searches of audit data based on criteria with logical relations, it meets TOE security objective: O.AUDIT.

FAU_SEL.1 Selective audit

As this component ensures the ability to include or exclude auditable events from the set of audited events based on attributes, it meets security objective: O.AUDIT.

FAU_STG.1 Protected audit trail storage

As this component ensures that TSF provides the ability to protect audit record from unauthorized modification and/or deletion, it meets security objective: O.AUDIT.

FAU_STG.3 Action in case of possible audit data loss

As this component ensures that actions are taken if a threshold on the audit trail is exceeded, it meets TOE security objective: O.AUDIT.

FAU_STG.4 Prevention of audit data loss

As this component ensures that actions are taken in case the audit trail is full, it meets TOE security objective: O.AUDIT.

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

As this component ensures that the packet filtering security policy for TOE information flow control and its scope are defined, it meets TOE security objective: O.INFORMATION FLOW CONTROL.

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

As this component ensures that the intrusion prevention security policy for TOE information flow control and its scope are defined, it meets TOE security objective: O.INFORMATION FLOW CONTROL.

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

As this component provides the packet filtering security policy rules for information flow control based on the security attributes, it meets TOE security objective: O.INFORMATION FLOW CONTROL.

.

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

As this component describes countermeasures for explicit attacks such as Spoofing IP Address, DoS Attack, Anomaly Packet Transfer, it meets TOE security objective: O. INFORMATION FLOW CONTROL, O.ABNORMAL PACKET SCREENING, and O. DOS ATTACK BLOCKING.

FIA_AFL.1 Authentication failure handling

As this component defines the number of unsuccessful administrator authentication attempts and ensures ability to take actions when the defined number has been met or surpassed, it meets TOE security objective: O.IDENTIFICATION and O.AUTHENTICATION.

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

This component requires maintaining IP address as security attribute for external IT entity. As IP address identifies external IT entities and creates audit history serving as the criteria for illegal addresses, DoS attacks, and information flow control, this component meets TOE security objectives: O. AUDIT, O.ABNORMAL PACKET

SCREENING, O. PREVENTION OF DOS ATTACKS, O.IDENTIFICTION, and O.INFORMATION FLOW CONTROL.

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

As this component requires identifying an administrator, it meets TOE security objective: O.ADUIT and O.IDENTIFICATION.

FIA_UAU.1 Timing of Authentication

As this component ensures the ability to authenticate administrators successfully, it meets TOE security objectives: O.ADMINISTRATION, O.TSF DATA PROTECTION, and O.AUTHENTICATION

FIA_UAU.7 Protected authentication feedback

As this component ensures that only limited authentication feedback is provided to the administrator while the authentication is in progress, it meets TOE security objective: O. AUTHENTICATION.

FIA_UID.2(1) User identification before any action (1)

As this component requires that the identifier for external IT entity be identified as a computer IP address, which identifies external IT entities and creates audit history serving as the criteria for illegal addresses, DoS attacks, and information flow control, it meets TOE security objectives: O. AUDIT, O.ABNORMAL PACKET SCREENING, O. PREVENTION OF DOS ATTACKS, O.IDENTIFICTION, and O.INFORMATION FLOW CONTROL.

.

FIA_UID.2(2) User identification before any action (2)

As this component requires identification of the administrator, it meets TOE security objectives: O.ADUIT, O.ADMINISTRATION, O.TSF DATA PROTECTION and O.IDENTIFICATION

FMT_MOF.1(1) Management of security functions behavior(1)

As this component ensures the ability for authorized administrator to disable, enable the security functions and guarantees availability in case of TOE failures, it meets TOE security objectives: O. AVAILABILITY, O.ADMINISTRATION.

FMT_MOF.1 (2) Management of security functions behavior(2)

As this component ensures the ability for an authorized administrator to determine the behavior of security functions and guarantees availability in case of TOE failures, it meets TOE security objectives: O. AVAILABILITY, O.ADMINISTRATION.

FMT_MSA.1 Management of security attributes

As this component ensures that only authorized administrators are allowed to access TSF data, or security attribute data, which is necessary for the performance of TOE security functions, it meets TOE security objectives: O.ADMINISTRATION, O.TSF DATA PROTECTION, O.INFORMATION FLOW CONTROL.

FMT_MSA.3 Static attribute initialization

As this component ensures that only authorized administrators are allowed to access at the initialization of TSF data, or security attribute data, which is necessary for the performance of TOE security functions, it meets TOE security objectives: O.ADMINISTRATION, O.TSF DATA PROTECTION, O.INFORMATION FLOW CONTROL.

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

As this component provides the authorized administrator with the ability to manage the packet filtering SFP, attack pattern in intrusion prevention SFP, and alarm rules, it meets TOE security objectives: O.ADMINISTRATION, O.TSF DATA PROTECTION.

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

As this component provides the authorized administrator with the ability to manage the identification and authentication data, it meets TOE security objectives: O.ADMINISTRATION, O.TSF DATA PROTECTION.

FMT_MTD.1(3) Management of TSF data (3)

As this component provides an authorized administrator with the ability to manage time, session time-out value of authorized administrator, TCP/UDP session time-out, session time-out for each packet filtering security policy, audit record related setup value, HOTLIST update cycle, and network interface state check related setup value, it meets TOE security objectives: O.ADMINISTRATION, O.TSF DATA PROTECTION.

FMT_MTD.2(1) Management of TSF limits on TSF data (1)

As this component guarantees the important availability of the TOE by ensuring that the authorized administrator manages audit trail storage limit and takes actions if the limits are reached or exceeded, it meets TOE security objectives: O.AVAILABILITY, O.ADMINISTRATION.

FMT_MTD.2(2) Management of TSF limits on TSF data (2)

As this component guarantees the important availability of the TOE by ensuring that the authorized administrator manages the limits for the number of unsuccessful authentication attempts and takes actions if the limits are reached or exceeded, it meets TOE security objectives: O.AVAILABILITY, O.ADMINISTRATION.

FMT_MTD.2(3) Management of TSF limits on TSF data (3)

As this component guarantees the important availability of the TOE by ensuring that the authorized administrator manages the limits for time interval for self-testing and takes actions if the limits are reached or exceeded, it meets TOE security objectives: O.AVAILABILITY, O.ADMINISTRATION.
e: O.AVAILABILITY, O.ADMINISTRATION.

FMT_SMF.1 Specification of management functions

As this component requires specification of management functions such as security attributes, TSF data and security functions to be provided by the TSF, it meets TOE security objective: O.ADMINISTRATION.

FMT_SMR.1 Security roles

As this component restricts the role of the TOE security administrator to authorized administrator roles, it meets TOE security objectives: O.ADMINISTRATION, O.IDENTIFICATION and O.AUTHENTICATION

FPT_AMT.1 Abstract machine testing

As this component run a suite of tests to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF, it meets TOE security objectives:, O. AVAILABILITY , O.TSF DATA PROTECTION

FPT_FLS.1 Failure with preservation of secure state

As this component ensures that the TOE, in failure, preserves a secure state and performs the function of information flow control for the operation of core security functions, it meets TOE security objectives: O.AVAILABILITY, O.INFORMATION FLOW CONTROL.

FPT_RVM.1 TSP Non-bypassibility of the TSP

As this component ensures that the TSP enforcement functions are invoked and succeeded and prevents bypassing of information flow control, it meets TOE security objective: O. INFORMATION FLOW CONTROL.

FPT_SEP.1 TSF domain separation

As this component ensures that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects, it meets TOE security objective: O.TSF DATA PROTECTION O. INFORMATION FLOW CONTROL.

FPT_STM.1 Reliable time stamps

This component provides reliable time stamps which can be used by the TSF. As the generated time stamps ensure the serial logging of security audit events in the event of creating the audit history, it meets TOE security objective: O.AUDIT.

FPT_TST.1 TSF Self-testing

This component ensures self-tests for the correct operation of TSF and requires the function to prevent or detect TOE's failure by verifying the integrity of TSF data and TSF executable code, it meets TOE security objectives: O.AVAILABILITY, O.TSF DATA PROTECTION

FPT_FLT.1 Fault tolerance

As this component ensures management activities through console or security management screen when TOE failures occur and guarantees the performance of information flow control function, it meets TOE security objectives: O.AVAILABILITY, O.INFORMATION FLOW CONTROL.

FPT_RSA.1 Maximum quotas

As this component blocks the DoS attacks by requiring maximum quotas of the TOE assets for each user, it meets the TOE security objective: O.DoS ATTACK BLOCKING.

FPT_SSL.1 TSF-initiated session locking

As this component requires the function for the TOE to lock the authorized session after a specified period of administrator inactivity, it meets TOE security objectives: O.TSF DATA PROTECTION.

FPT_SSL.3 TSF-initiated termination

As this component secures the availability of network service by requiring the external IT entity to terminate the session with the internal computer after a certain period of time, it meets TOE security objectives: O. DoS ATTACK BLOCKING.

FTP_ITC.1 Inter-TSF trusted channel

As this component requires the creation of the trusted channel when the authorized administrator manages the TOE locally or remotely, or when the TOE external vulnerability data servers communicate each other, it meets TOE security objectives: O.ADMINISTRATION, O.AUTHENTICATION and O.TSF DATA PROTECTION.

8.3.2 Rationale for IT environment requirements

Security objective SFR	OE. SSL protocol
FTP_ITC.1	X

[Table 8-7] Rationale mapping of SFR for IT environment

FTP_ITC.1 Inter-TSF trusted channel

This component satisfies OE. SSL protocol that supports trusted IT entity authentication and encrypted communication function for the creation of trusted channel of the TOE.

8.4 Rationale for assurance requirements

This ST claims conformance to the assurance package of IPSPP (EAL4), which is able to provide sufficient assurance in the environment where the TOE operates in consideration of the TOE security environments. The assurance measures that satisfy requirements of EAL4 level package are described in the assurance documents referenced in section 6.2, and each document is sufficient to satisfy the assurance requirements. However, for AGD_USR.1 user guidance assurance component, the TOE does not define general users so that the user guidance is not available. Therefore, assurance measures for this component are not provided. FPT_FLS.1 has dependency to ADV_SPM.1, and assurance measure satisfied ADV_SPM.1 is identified by reference [SPM] in section 6.2.

8.5 Rationale for Strength-of-Function (SOF)

This ST selects "SOF–medium" claimed by Network intrusion prevention system protection profile (IPSPP). In SOF-medium, most attackers are considered to possess moderate level of expertise, resources and motivation. The IPSPP recommends providing security functions whose level is at least "SOF–medium" in order to counter threat agents possessing a moderate attack potential. Therefore, the strength of function required by this ST is "SOF– medium" which conforms to IPSPP.

The likelihood that an attacker possessing a moderate attack potential finds out passwords is less than 1/313,165,535,047 so that the password mechanism of security function SW_INA which satisfies FIA_UAU.1 meets "SOF-high".

SHA-1, the integrity algorithm of security function SW_PT which meets FPT_TST.1, satisfies "SOF-high" because it has low likelihood that an attacker possessing a moderate attack potential generates identical hash values.

The TOE is used in general network environments, in which a threat agent is able to attack the TOE using moderate level of expertise, resources and devices. Therefore, "SOF-medium" is selected as to disable the attacker.

8.6 Rationale for TOE summary specification

This chapter explains the TOE security functions and assurance measures are appropriate to TOE security requirements.

8.6.1 TOE security functions

Some specific TOE security functions should operate together to satisfy SFRs. [Table 8-8] shows that SFRs for the TOE are mapped to all security functions.

Security Function	SFRs
Security Administration (SW_ADMIN)	FMT_MOF.1(1)
	FMT_MOF.1(2)
	FMT_MSA.1
	FMT_MSA.3
	FMT_MTD.1(1)
	FMT_MTD.1(2)

Security Function	SFRs
	FMT_MTD.1(3)
	FMT_MTD.2(1)
	FMT_MTD.2(2)
	FMT_MTD.2(3)
	FMT_SMR.1
	FMT_SMF.1
Security Audit (SW_AUDIT)	FAU_ARP.1
	FAU_GEN.1
	FAU_GEN.2
	FAU_SAA.1
	FAU_SAR.1
	FAU_SAR.3
	FAU_SEL.1
	FAU_STG.1
	FAU_STG.3
	FAU_STG.4
	FPT_STM.1
User Date Protection (SW_UDP)	FDP_IFC.1(1)
	FDP_IFC.1(2)
	FDP_IFF.1(1)
	FDP_IFF.1(2)
	FIA_ATD.1(1)
	FPT_RVM.1
	FPT_SEP.1
	FIA_UID.2(1)
	FTA_SSL.3
	FRU_RSA.1
	FTP_ITC.1
Identification & Authentication (SW_INA)	FIA_AFL.1
	FIA_ATD.1(2)
	FIA_UAU.1
	FIA_UAU.7
	FIA_UID.2(2)

Security Function	SFRs
	FTA_SSL.1
TSF Protection (SW_PT)	FPT_AMT.1
	FPT_FLS.1
	FPT_RVM.1
	FPT_SEP.1
	FPT_TST.1
	FRU_FLT.1
	FTP_ITC.1

[Table 8-8] Mapping between SFRs and security functions

FMT_MOF.1(1) - Management of security functions behavior – The TOE satisfies this SFR as it provides the ability to disable or enable attack rule update functions, security management related functions and fault tolerance related functions. (SW_ADMIN)

FMT_MOF.1(2) - Management of security functions behavior – The TOE satisfies this SFR as it provides the ability to determine behaviors about TOE security policies, audit records and self-test related functions. (SW_ADMIN)

FMT_MSA.1- Management of Security attributes – The TOE satisfies this SFR as it provides the ability to manage security attributes for information flow control security policy. (SW_ADMIN)

FMT_MSA.3 - Static Attribute Initialization – The TOE satisfies this SFR as it provides administrators with the ability to modify the initial value of security attributes which are restrictive based on defined in FMT_MSA.1. (SW_ADMIN)

FMT_MTD.1(1) - Management of TSF data (1) – The TOE is able to generate, modify, delete, and review the rules of information flow control policy and alarm rules. (SW_ADMIN)

FMT_MTD.1(2) - Management of TSF data (2) – The TOE satisfies this SFR as it provides the authorized administrator with the ability to add, delete, modify the list of security attributes of IT entities and administrators. (SW_ADMIN)

FMT_MTD.1(3) - Management of TSF data (3) - The TOE satisfies this SFR as it provides the ability to modify TSF data such as TOE time stamp, session time-out value, audit record related setup value, DI rule automatic update cycle. (SW_ADMIN)

FMT_MTD.2(1) - Management of limits on TSF data (1) – The TOE is able to define audit trail storage limit through security management interface. (SW_AUDIT)

FMT_MTD.2(2) - Management of limits on TSF data (2) – The TOE is able to define the limits for the number of unsuccessful authentication attempts. (SW_ADMIN)

FMT_MTD.2(3) - Management of limits on TSF data (3) – The TOE is able to define the limits for time interval for self-testing through security management interface.

(SW_ADMIN)

FMT_SMR.1 - Security Roles – The TOE is able to give or add administrator authority for each policy or log. (SW_ADMIN)

FMT_SMF.1 - Specification of management functions - The TOE satisfies this SFR as it provides management functions for security functions, security attributes, TSF data and its limits, security roles, status information, and self-test . (SW_ADMIN)

FAU_ARP.1 - Security alarms – The TOE alarms the authorized administrator by sending e-mail and SMS message upon detection of a potential security violation. (SW_AUDIT)

FAU_GEN.1 - Audit data generation – The TOE generates audit data of all events occurring in the TOE by classifying it into ERROR, WARNING, NOTICE, ACCOUNT, MANAGE. (SW_AUDIT)

FAU_GEN.2- User identity association - The TOE is able to associate each auditable event occurring in the TOE with the identity of the user that caused the event. (SW_AUDIT)

FAU_SAA.1 - Potential violation analysis – The TOE alarms the authorized administrator by sending e-mail or SMS message for the list of potential alarm items predefined by the administrator. (SW_AUDIT)

FAU_SAR.1 - Audit review – The TOE allows the authorized administrator to read information from the audit records through web interface. (SW_AUDIT)

FAU_SAR.3 - Selectable audit review – The TOE is able to perform searches of stored audit data based on various criteria with logical relations so that the authorized administrator can review information he/she wants. The selected audit data can be stored in file format. (SW_AUDIT)

FAU_SEL.1 - Selective audit – The TOE can generate audit records selectively according to audit record fields and security rules. (SW_AUDIT)

FAU_STG.1 - Protected audit trail storage – The TOE stores generated audit records in a system file which restricts access rights only to the authorized administrator according to system, date, and types of audit data. (SW_AUDIT)

FAU_STG.3 – Action in case of possible audit data loss – The TOE informs the authorized administrator of the remaining capacity of the audit trail and issues an alarm. (SW_AUDIT)

FAU_STG.4 - Prevention of audit data loss – If the audit trail is full, the TOE denies any access except from the authorized administrator and alarms the administrator by sending e-mail or SMS message (SW_AUDIT)

FDP_IFC.1(1) - Subset information flow control (1) – The TOE controls information flow between subjects and objects by enforcing the packet filtering SFP. (SW_UDP)

FDP_IFC.1(2) - Subset information flow control (2) – The TOE controls information flow between subjects and objects by enforcing the intrusion prevention SFP. (SW_UDP)

FDP_IFF.1(1) - Simple security attribute (1) – The TOE performs access control according to the source, destination, service, time of packets by enforcing the packet filtering SFP. (SW_UDP)

FDP_IFF.1(2) - Simple security attribute (2) – The TOE performs access control on explicit attacks by enforcing the intrusion prevention SFP. (SW_UDP)

FIA_AFL.1 - Authentication failure handling – The TOE alarms the authorized administrator when the defined number of unsuccessful administrator authentication failure has been met by a certain administrator during the administrator authentication process. (SW_INA)

FIA_ATD.1(1) - User attribute definition (1) – When the TOE enforces SFP based on external IP entity, the authorized administrator defines and applies the security attributes of IT entity. (SW_UDP)

FIA_ATD.1(2) - User attribute definition (2) – When the TOE enforces SFP based on administrator, the authorized administrator defines and applies the security attributes of administrator. (SW_INA)

FIA_UAU.1 – Timing of authentication - For administrators who need administrator authentication, the TOE applies SFPs after they are authenticated. (SW_INA)

FIA_UAU.7 - Protected authentication feedback – The TOE uses special characters to prevent a password from being displayed on the administrator's interface while the authentication is in progress. (SW_INA)

FIA_UID.2(1) – User identification before any action (1) – The TOE identifies IP address of IT entities before allowing them to use security functions of the TOE. (SW_UDP)

FIA_UID.2(2)– User identification before any action (2) – The TOE requires administrators to input their ID before allowing them to use security functions of the TOE. (SW_INA)

FPT_AMT.1 - Abstract machine testing – The TOE sustains communication by detecting errors related to interfaces during its initial start-up and operation, and checks the Link Status of its own interfaces. (SW_PT)

FPT_FLS.1 - Failure with preservation of secure state – The TOE ensures administrator activities through console or security management screen to perform correct operation in a secure state when the failure of FRU_FLT.1 occurs. (SW_PT)

FPT_RVM.1 Non-bypassibility of the TSP - The TOE transfers all the packets passing through the TOE by using a virtual IP driver of the TOE .(SW_UDP, SW_PT)

FPT_SEP.1 - TSF domain separation – The TSF separates reliable domain from unreliable domain for each interface when establishing security policies to perform security functions. (SW_UDP, SW_PT)

FPT_STM.1 - Reliable time stamps – The TOE is able to provide reliable time stamps from external sources. (SW_AUDIT)

FPT_TST.1 - TSF testing – The TOE checks the integrity of its own TSF data and execution binary files during initial start-up or operation of the TOE, and shows the authorized administrator the check results. (SW_PT)

FRU_FLT.1 - Degraded fault tolerance : partial application – The TOE checks the link status of its own network interfaces. If there is no response, the TOE regards it as a failure and generates audit records to alarm the authorized administrator. Moreover, if the daemons are discontinued while operating in the TOE, the security management server re-starts them. (SW_PT)

FRU_RSA.1 - Maximum Quotas – The TOE sets the maximum quotas of SYN packets that can be sent by an IT entity over a certain period of time and ensures blocking the DoS attacks. (SW_UDP)

FTA_SSL.1 - TSF-initiated session locking – If an authorized administrator attempts to access the security management server after a specified period of administrator inactivity, the TOE locks the authorized session and displays security management log-in screen unconditionally. (SW_INA)

FTA_SSL.3 - TSF-initiated termination - In case occurring a session to exceed the number of session per second defined by administrator, detecting SYN Flooding attack, requesting session termination by authorized administrator, TOE disconnect the associated session.(SW_UDP)

FTP_ITC.1 – Inter-TSF trusted channel – The TOE calls SSL functions provided as an IT environment for authentication and encrypted communication in case the TOE communicates with trusted external IT entities and administrators. (SW_UDP, SW_PT)

8.6.2 TOE SOF compliance

The level of the TOE strength of function in this ST is “SOF-medium”, which is defined in CC Part 1 as the level to resist attackers possessing a moderate attack potential. The security functions under which SOF is applied are :

Identification and authentication (SW_INA) : used a probabilistic/permutational mechanism.
TSF protection (SW_PT) : used SHA-1 which is the 160 bit integrity algorithm.

The TOE is installed and operated in-line at the connection point between the internal and external network. In such an environment, the threat agents have mid-level expertise, resources, and motivation, and the likelihood of discovering exploitable vulnerability is moderate.

8.6.3 TOE assurance requirements compliance

The following [Table 8-9] provides assurance measures that was described as assurance requirements in section 5.1.2.

Assurance measures / Assurance Component ID	Configuration management	Delivery Document	Installation guidance	Functional specification	High-level design	Implementation representation	Low-level design	Correspondence	Security policy modeling	Administrator guidance	Life cycle support	Life cycle definition	Development tools	Test document	Misuse analysis	Vulnerability analysis	SOF analysis
ACM_AUT.1	X																
ACM_CAP.4	X																
ACM_SCP.2	X																
ADO_DEL.2		X															
ADO_IGS.1			X														
ADV_FSP.2				X													
ADV_HLD.2					X												
ADV_IMP.1						X											
ADV_LLD.1							X										
ADV_RCR.1								X									
ADV_SPM.1									X								
AGD_ADM.1										X							
ALC_DVS.1											X						
ALC_LCD.1												X					
ALC_TAT.1													X				
ATE_COV.2														X			
ATE_DPT.1														X			
ATE_FUN.1														X			
ATE_IND.2														X			
AVA_MSU.2															X		
AVA_SOF.1																	X
AVA_VLA.2																X	

[Table 8-9] Assurance measures mapping

ACM_AUT.1 - Partial CM automation – The TOE provides an automated means by which only authorized changes are made to the TOE implementation representation. The TOE also provides a Configuration Management Documentation to ensure using an automated means to support the generation of the TOE.

ACM_CAP.4 - Generation support and acceptance procedures - The TOE provides a Configuration Management documentation to provide controls to ensure that there is no unauthorized change to the TOE as well as to guarantee the proper functionality and use of the CM system.

ACM_SCP.2 - Problem tracking CM coverage – The TOE provides Configuration Management documentation to ensure that the configuration items under the CM are changed in a controlled manner in accordance with the adequate authorization.

ADO_DEL.2 - Detection of modification – The TOE provides a Delivery Document to ensure the system control, delivery facilities and procedures by which the TOE is distributed from the developer to a user’s site without any modification.

ADO_IGS.1 - Installation, generation, and start-up procedures – The TOE provides an Installation Guidance to ensure that the TOE is installed, generated, and initialized in a secure way the developer intended.

ADV_FSP.2- Fully defined external interface – The TOE provides a Functional Specification to examine all of the external interfaces as well as to give insanitation of the TOE SFRs and basic description of the operation and interfaces that TSF users can see.

ADV_HLD.2 - Security enforcing high-level design – The TOE provides a High-level Design to ensure that the TOE provides adequate structure to implement the TOE SFRs by describing the structure of the TSF in terms of subsystems and explaining the relationship between the subsystems and their functions.

ADV_IMP.1 - Subset of the implementation of the TSF – The TOE provides an Implementation representation to ensure analysis by making delicate internal operations of the TSF understood.

ADV_LLD.1 - Descriptive low-level Design – The TOE provides a Low-level design to describe the internal operation of the TSF in terms of mutual and dependent relationship between modules as well as to ensure that the TSF subsystems are accurately and effectively explained.

ADV_RCR.1 - Informal correspondence demonstration - The TOE provides Correspondence Analysis to ensure consistency with various expression of the TSF (i.e. TOE Summary Specification, Function Specification, High-level design, Low-level design, Implementation representation).

ADV_SPM.1 - Informal TOE security policy model – The TOE provides a Security policy modeling to describe all security policies and attributes of the TSP as well as to ensure the consistency and completeness of all security polices.

AGD_ADM.1 - Administrator guidance – The TOE provides Administrator Guidance/Operation Guidance as the documented materials that will be used by those responsible for configuring, maintaining, managing the TOE in a correct manner to maximize security.

ALC_DVS.1 - Identification of security measures – The TOE provides Life-cycle Support to protect the TOE by using physical, procedural, personnel and other security measures that can be used in the development environment.

ALC_LCD.1 - Developer-defined life-cycle model – The TOE provides Life-cycle Definition Documentation to ensure that the model used to develop and maintain the TOE provides necessary controls for the development and maintenance of the TOE.

ALC_TAT.1- Well-defined Development Tools - The TOE provides the Documentation of the Development Tools to ensure that inconsistent or incorrect tools are not used to develop the TOE.

ATE_COV.2- Analysis of Coverage – The TOE provides Test Documentation to demonstrate that the TSF has been systematically tested in accordance with the functional specification.

ATE_DPT.1 - Testing : High-level design - The TOE provides Test documentation to ensure that the TSF subsystem phase are correctly implemented.

ATE_FUN.1 - Functional testing – The TOE provides Test documentation to ensure that all the security functions are performed as specified.

ATE_IND.2 - Independent testing: sample test - The TOE provides Test Documentation to ensure that security functions are performed as specified.

AVA_MSU.2 - Validation of analysis - The TOE provides Misuse Analysis to ensure that its guidance has no misleading, unreasonable, conflicting guidelines and address secure procedures for all modes of operation of the TOE.

AVA_SOF.1-TOE Strength of TOE security function evaluation – The TOE provides SOF(Strength-of-Function) Analysis to determine the strength of security behavior based on the quantative or statistical analysis results of underlying security mechanisms.

AVA_VLA.2 - Independent vulnerability analysis – The TOE provides Vulnerability Analysis Documentation to confirm that vulnerabilities exist and to ensure that they cannot be exploited in the intended environment for the TOE.

8.7 Rationale for dependency

The SFRs used in this ST satisfy dependencies as shown in [Table 8-10], and there is no component that does not satisfy any dependency.

No.	Component	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	38
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 20, 21 (hierarchical to FAI_UID.2)
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.3	FAU_SAR.1	5
7	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	2 26, 27, 28
8	FAU_STG.1	FAU_GEN.1	2
9	FAU_STG.3	FAU_STG.1	8
10	FAU_STG.4	FAU_STG.1	8
11	FDP_IFC.1(1)	FDP_IFF.1	13
12	FDP_IFC.1(2)	FDP_IFF.1	14
13	FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	11 25
14	FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	12 25
15	FIA_AFL.1	FIA_UAU.1	18
16	FIA_ATD.1(1)	-	-
17	FIA_ATD.1(2)	-	-
18	FIA_UAU.1	FIA_UID.1	20, 21 (hierarchical to FAI_UID.2)
19	FIA_UAU.7	FIA_UAU.1	EAL4
20	FIA_UID.2(1)	-	-
21	FIA_UID.2(2)	-	-
22	FMT_MOF.1(1)	FMT_SMR.1 FMT_SMF.1	33 32

No.	Component	Dependency	Reference No.
23	FMT_MOF.1(2)	FMT_SMR.1 FMT_SMF.1	
24	FMT_MSA.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	11, 12 33 32
25	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	24 33
26	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	32 33
27	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	32 33
28	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	32 33
29	FMT_MTD.2(1)	FMT_MTD.1 FMT_SMR.1	26, 27, 28 33
30	FMT_MTD.2(2)	FMT_MTD.1 FMT_SMR.1	26, 27, 28 33
31	FMT_MTD.2(3)	FMT_MTD.1 FMT_SMR.1	26, 27, 28 33
32	FMT_SMF.1	-	-
33	FMT_SMR.1	FIA_UID.1	20, 21 (hierarchical to FAI_UID.2)
34	FPT_AMT.1	-	-
35	FPT_FLS.1	ADV_SPM.1	EAL4 (assurance requirements)
36	FPT_RVM.1	-	-
37	FPT_SEP.1	-	-
38	FPT_STM.1	-	-
39	FPT_TST.1	FPT_AMT.1	34
40	FRU_FLT.1	FPT_FLS.1	35
41	FRU_RSA.1	-	-
42	FTA_SSL.1	FIA_UAU.1	18
43	FTA_SSL.3	-	-
44	FTP_ITC.1	-	-

[Table 8-10] Satisfaction of Dependency among SFRs

9 References

[01] IPSPP (Network intrusion prevention system protection profile) v1.0 May 24, 2005

[02] CC V2.2 [CC]

[03] SECUREWORKS IPSWall 1000 V4.0 Configuration Management Documentation V1.9[ACM]

[04] SECUREWORKS IPSWall 1000 V4.0 Delivery Documentation V1.3[DEL]

[05] SECUREWORKS IPSWall 1000 V4.0 Installation Guidance V1.21[IGS]

[06] SECUREWORKS IPSWall 1000 V4.0 Functional Specification V1.13[FSP]

[07] SECUREWORKS IPSWall 1000 V4.0 High-level Design V1.7[HLD]

[08] SECUREWORKS IPSWall 1000 V4.0 Implementation Representation V1.2[IMP]

[09] SECUREWORKS IPSWall 1000 V4.0 Low-level Design V1.5[LLD]

[10] SECUREWORKS IPSWall 1000 V4.0 Correspondence Analysis V1.5[RCR]

[11] SECUREWORKS IPSWall 1000 V4.0 Security Policy Modeling V1.6[SPM]

[12] SECUREWORKS IPSWall 1000 V4.0 Administrator Guidance V1.23[ADM]

[13] SECUREWORKS IPSWall 1000 V4.0 Operation Guidance V1.14[OPR]

[14] SECUREWORKS IPSWall 1000 V4.0 Life Cycle Support V1.4[DVS]

[15] SECUREWORKS IPSWall 1000 V4.0 Life Cycle Definition Documentation V1.5[LCD]

[16] SECUREWORKS IPSWall 1000 V4.0 Development Tool Documentation V1.3[TAT]

[17] SECUREWORKS IPSWall 1000 V4.0 Test Documentation V1.6[TST]

[18] SECUREWORKS IPSWall 1000 V4.0 Misuse Analysis V1.5[MSU]

[19] SECUREWORKS IPSWall 1000 V4.0 Strength of Function Analysis V1.4[SOF]

[20] SECUREWORKS IPSWall 1000 V4.0 Vulnerability Analysis V1.2[VLA]