TESS TMS v4.5
Security Target v6

Summary

This document is the ST (Security Target) of the network intrusion prevention system (TOE: TESS TAS v4.5, Product Version: v4.5)

Summary of Change History

Version	Date	Reason of Change	Written by
STR-1	**March 20, 2006**	**First Formal Registration**	**Byung Uk Park**
STR-2	**May 24, 2006**	**Readjustment of Errors & Terms**	**Byung Uk Park**
STR-3	**May 26, 2006**	**TSF Complement**	**Yun Kyung Kim**
STR-4	**June 1, 2006**	**-Readjustment of Errors & Terms -TSF Complement -TOE Configuration Diagram Revision -Chapter 5 FDP_IFF Revision -Chapter 5 FMT_MTD.2 Revision -Chapter 6 Health Check Function Revision -Document Identification Info. Update & Error Revision**	**Byung Uk Park**
STR-5	**July 22, 2006**	**Additional Description of Threat-Level Policy**	**Byung Uk Park**
STR-6	**July 28, 2006**	**-Additional Description of Threat-Level Policy -Description of Changing to AES from DES3 from Cryptographic Method - FAU_SAA.1 Potential Violation Analysis. Description of Adding the Item of the Potential Violation Analysis**	**Byung Uk Park**

Table of Contents

1 Overview

This chapter introduces the ST of the TESS TMS v4.5, the intrusion prevention system, made by INFOSEC Technologies.

1.1 Objectives

This document is about the ST of the TESS TMS v4.5, defining the security function & assurance measures by claiming the network intrusion prevention system protection profile V1.1 (Dec. 21, 2005. KISA) and describing general items of security requirements, implementation method & technical information used for the basis of the evaluation.

This chapter provides the identification information on the ST and explains it. The ST written by INFOSEC Technologies, defines the product type, the TOE scope, the TOE threats & assumptions, describes the security objectives & requirements, and explains the security functional requirements provided by the TOE.

1.2 Document Identification

Document Name	TESS TMS v4.5 ST
Document Version	STR-6
Date	July 28, 2006
Product Name	TESS TMS v4.5
TOE Identification	TESS TAS v4.5(TESS TAS Sensor v4.5, TESS TAS Manager v4.5, TESS TAS Console v4.5)
Common Evaluation Criteria Identification	Common Criteria for Information Technology Security Evaluation V2.3(Aug. 2005)
Protection Profile Claims	Network Intrusion Prevention System Protection Profile V1.1 Dec. 21, 2005 (hereinafter IPSPP)
Assurance Level	EAL4
Written by	Byung wook Park, INFOSEC Technologies Co,. Ltd
Key Words	Access Control, Intrusion Target Event Info. Collection, Intrusion Correspondence, IPS

[Table 1-1] Document Identification

1.3 ST Overview (ST Introduction)

The TESS TMS v4.5 (hereinafter TESS TMS) is the intrusion prevention system consisting of TESS TAS v4.5 (hereinafter TESS TAS), TESS TMS Web, & TESS TMS Report, installs TESS TAS between the networks to be protected to judge the possible harmful traffic by checking the entire network traffic passing through the TOE and provides various functions of the prevention, logging, notification in accordance with the existing correspondence policies when harmful traffic is found.

TESS TMS easily detects any anomalous symptoms by analyzing changes for the packet, traffic and intrusion detection, and provides functions of minimizing the expansion of damage through the circumstantial judgment & decision making using the information on the attacker, victim and measure while taking steps for the damage recovery within a short notice.

TESS TES Web shall provide the information on the attacker, victim and measure through the intrusion detection & traffic change, bringing the information on the internal or external circumstances necessary for the advance preparation by knowing the internal threats and external trends.

The evaluation scope is restricted to TESS TAS v4.5,

The ST consists of the description of the TOE and definition of threats, assumptions & organizational security policies which the TOE has to manage while explaining the security objectives, IT security requirements, the TOE summary specification, and protection profile claims,

1.4 Configuration

Chapter 1 provides and generally describes the identification information on the ST.

Chapter 2 defines the TOE and describes the TOE environment with the explanation of the TOE.

Chapter 3 is about the TOE security environment, describing the security problems in the TOE & TOE environment from the perspective of assumptions, threats, and organizational security policies.

Chapter 4 is for the security objectives and describes the TOE security objectives & security objectives for the environment to respond to the identified threats in the

security environment as well as support the assumptions & organizational security policies.

Chapter 5 is about the IT security requirements and describes the security functional requirements and assurance requirements to meet the security objectives.

Chapter 6 is the TOE summary specification and describes the TSF & assurance requirements meeting the IT security requirements.

Chapter 7 is about the PP clams, telling the PP claimed by the ST.

Chapter 8 is for the rationales to prove that the TOE provides the effective IT security measures within the TOE security environment, including the description of the security objectives rationale, security requirements rationale, the TOE summary specification rationale, PP claims rationale & SOF rationale.

1.5 CC Conformance

This ST is now conforming to the following evaluation criteria and PP.

Part 2 conformant

The security functional requirements of the TOE conform to the functional components in Part 2. (MOIC Notification No. 2005-25) (CC V2.3)

Part 3 conformant

The security assurance requirements of the TOE conform to the assurance components in Part3 (MOIC Notification No. 2005-25) (CC V2.3)

EAL (Evaluation Assurance Level)

Evaluation Assurance Level of the TOE is EAL4

Protection Profile Conformance

The TOE conforms to Network Prevention System Protection Profile V1.1((Dec. 21, 2005, KISA).

1.6 Acronyms & Glossary

The terms defined in the ST are restricted to the intrusion prevention system. Those that are the same as the terms used in CC are not defined but conform to the CC.

Object

It is the target of the subject's operation and the entity within TSC (TSF Scope of Control) including or receiving the information.

SOF (Strength of Function)

It is the capacity of the TSF that shows the minimum efforts needed to incapacitate the expected security activities by directly attacking the security mechanism.

Iteration

It is one of CC operations and is something to use the same component just once in various operations.

ST (Security Target)

It is the collection of security requirements and functional specifications used as a basis of the TOE evaluation.

Security Level

It is the combination of the hierarchical Category & non-hierarchical Category that indicate the significance level of the user or information.

PP (Protection Profile)

It is the collection of the security requirements that are independent from the implementation meeting the demands of specific consumers for the TOE category

Human User

It is all people who mutually operate with the TOE

User

It is all entities, users, external IT entity, etc. which are mutually operating with the TOE outside the TOE

Selection

It is one of CC operations and is something to choose over a item from the list of a component.

Identity

It is only the expression to identify the authorized user.

Element

It is the minimum unit of the security requirements that can't be split

Operation[1]

It is make components to respond to a certain threat in CC or to meet the specific security policy (Iteration, assignment, selection, & refinement)

Operation[2]

It is the operation that is defined by computer commands or pseudo-instructions

Threat Agent

It is the unauthorized user or external IT entity causing threats like illegal access, modification, or deletion of assets

Authorized Administrator

It is the authorized user who is allowed to have the authority to manage the TOE

Authorized User

It is the user who can perform the function in accordance with TSP

Authentication Data

It is the information used to prove the identity of a user

DAC, Discretionary Access Control

It is the access control method based on the identities of users or groups

Assets

It is the protected information & resource as TSP

Refinement

It is one of CC operations and is something that is specified by adding details to a component

Information Protection System CC

It is the information protection system CC that was revised and notified by the Minister of Information and Communication on May 21, 2005. CC is the localized version of the International Common Criteria developed by the common language & understanding that everyone can accept based on the evaluation criteria existed in every nation across the world

Organizational Security Policies

It is the security rules, procedures, practices, guidance, etc. that are forced in the organization

Dependency

It is the relation between requirements enabling the dependent requirements to meet one another so as to the objective of a general requirement

Subject

It is the entity within the TSC generating the operation to perform

Sensitivity Label

It is the security attribute that indicates the security level of the subject or object.

Intrusion

It is the set of a series of activities hindering the integrity, confidentiality and availability of resources used by the computer, and the act to destroy the security policy of the computer system

Augmentation

It shall add over an assurance component to EAL or assurance package.

Abstract Machine

It is a corporate organization of hardware/software known or evaluated to operate like the hardware/firmware, platform or virtual machine. The underlying abstract machine becomes the OS when the TOE is the application program while becoming the firmware or hardware when the TOE is the OS.

Component

It is the set of elements in CC and is the smallest selection unit to be included in the PP, ST.

Class

It is the set of families with the same security objective in CC

TOE (Target of Evaluation)

It is IT products or systems that are the TOE, and the administrator & administrator guidance related to the IT products or systems

Family

It is the set of components that have the same objective but different precision or highlight in CC.

Assignment

It is one of CC operations and concretely specifies parameters identified within the component.

Extension

It shall add the security functional requirements that are not included in the CC part 2 or the assurance requirements that are not included in the CC part 3 to PP, ST

TSF (TOE Security Function)

It is the set of all-dependent hardware, software & firmware of the TOE to exactly perform the TOE

TSP (TOE Security Policy)

It is the set of rules to regulate the administration, protection and distribution of assets in the TOE

TSF Data

It is the data created by the TOE that can have an effect on the TOE operation for the TOE.

TSC (TSF Scope of Control)

It is the set of interaction that can be took place and controlled by the TSF rules

VLAN (Virtual LAN)

It is the LAN that divides the scope of broadcast packets without regard to the physical racing using the LAN switch with the virtual function or ATM switch in a discretionary manner. It is the product when the virtual LAN is assembled using port unit, MAC address, IP address unit and protocol unit. But a router is needed in the communication between terminals belonging to other virtual LANs. The compliant called IEEE 802.1Q is standardized to configure the virtual LAN through multiple LAN switches.

MPLS (Multi Protocol Label Switching)

It is the layer 3 label switching of the cut and through-mode packet dispatch that is being standardized by the Internet engineering test force (IETF).In the connection mode network like ATM, the high speed dispatch of packets can be possilbe by dividng the packet dispatch process from the path comutation process. MPLS has to use the far-end linker between nodes, the connection set between the nodes is related to the path information of the network layer.

The related connection shall be identified by adding a label or tag, the switch receiving the packet with the label transmits the packet based on the label.

As the label is assigned according to the path information, the dispatch process of the packet comes to have nothing to do with the path computation process. A new label becomes assigned when the path information changes. The technology related to this is the tag exchange of Cisco Systems, INC. or ARIS of IBM.

L/B (Load Balancing)

It shall balance the degree of the load of each processor in the multiple processor system where many processors are processing tasks in parallel. It shall properly distribute tasks in order to prevent too little or many loads. Sometimes, it moves the task to other processors from one processor in necessary.

HA (High Availability)

It is the abbreviation of high availability and is the system or component which desirably continue to operate for a long time.

2 TOE Description

This chapter consists of the 2.1 TESS TMS Description that describes the evaluation request product and the 2.2 TOE Description that narrates the evaluation scope of that request product

2.1 TESS TMS Description

TESS TMS is the intrusion prevention system to provide the function of preventing such cyber attacks as Internet worms, hacking, etc. It also provides functions of intrusion detection, packet filtering, comprehensive threat analysis through the traffic & correlation analysis, global threat information & vulnerability information, early prediction-alarm transmission & real-time correspondence.

TESS TMS consists of TESS TAS, TESS TMS Web, and TESS TMS Report providing the function of the intrusion prevention. TESS TAS provides the function of controlling the flow of the network packet using the intrusion detection & packet filtering function by the real-time network packet analysis.

TESS TMS Web is using the intrusion detection, screening & traffic information generated by TESS TAS to provide the analysis of traffic anomalous symptoms, vulnerabilities, and spyware as well as the comprehensive correlation analysis between events by the linkage of the network condition in the local and external global network condition. TESS TMS Report provides the function of creating the report enabling you to check the network condition based on every kind of log stored in DBMS.

2.2 TOE Description

Of components configuring TESS TMS, the TOE is confined to TESS TAS

2.2.1 TOE Overview

TESS TAS (TAS: Threat & Traffic Analysis System) is the intrusion prevention system which is installed as a in-line mode in the network section to be monitored and check the entire network traffic to decide the possibility of the harmful traffic. When the harmful traffic is found, TESS TAS provides the administrator with functions of the

screening, logging, user notification, etc. in accordance with the already set correspondent policy.

TESS TAS consists of 3Tier Architecture with more stability – intrusion, event detection/screening & traffic statistics generation (TESS TAS Sensor), event collection & anomalous symptom, correlation analysis (TESS TAS Manager), and GUI (TESS TAS Console) for the presentation.
With a help of the functional separation between Tiers, there is no delay of the presentation even when overload occurs in the detection & analysis owing to the traffic runaway. Also there is no delay of the detection & analysis during the presentation.
All security functions of TESS TAS are operating in the form of daemon or service. In addition, TESS TAS provides the automatic recovery function in case of emergency like the system error & failure through the monitor process that monitors each component. When the recovery is impossible, TESS TAS provides the mechanism in which it notifies the administrator of failures through SMS & e-mail to minimize the recovery period.
TESS TAS supports virtualization of sensor & network that can be applied in the various environments as well.
The sensor virtualization means the function of generating detection/screening & traffic statistics by logically integrating several physical convolutions including L/B (Load Balancing) or HA (High Availability).
The network virtualization is the function of generating the detection/screening traffic statistics by logical convolution like IP block, VLAN (Virtual LAN), MPLS (Multi Protocol Label Switching), etc.
In the form of in-line, TESS TAS Sensor is installed and operated in the points of connecting the Internet and internal network or branching off the network into the internal network & external network. It provides the function of effectively detecting & cutting off attacks of information collection, DoS, protocol vulnerability, WEB CGI, Backdoor, and virus/worm.
TESS TAS Manager plays a role of providing the function of detecting the storage & statistics generation & profile-based/absolute threshold-based anomalous symptoms. It also provides the function of managing every kind of security policy that is applied to TESS TAS Sensor.
TESS TAS Console provides every kind of intrusion detection/screening, event

inquiry & retrieval, and policy set the GUI for the administrator. The contents stored by the GUI are stored and managed by TESS TAS Manager.

Major functions of TESS TAS are as follows.

- Real-Time Detection/Screening & Alarm
  - It provides the function of more upgrade detection & real-time alarm like intrusion detection/screening & network anomalous symptom detection.
  - It provides the upgrade function of detecting attacks of information collection, denial of service, protocol vulnerability, virus, worm, etc.
  - It provides the function of detecting the anomalous symptoms according to profile-based (Adaptive Threshold), absolute threshold & delta.
  - It provides the function of the real-time visible & audible alarm, e-mail, and SMS alarm in TESS TAS Console.
- Threat Analysis.
  - It provides the function of the transitive analysis of event anomalous symptoms & traffic anomalous symptoms.
  - It provides the analysis function along with the profile for the result of detecting the anomalous symptoms in the whole systems or by sensor & network.
- Event Analysis
  - It provides the function of the rank, distribution & transitive analysis of the event occurred based on the statistics for the intrusion detection/prevention event.
  - It provides the function of the statistics analysis & correlation analysis by the event type, attacker IP, and victim IP.
  - It provides the distribution & transition of output by event & IP.
- Traffic Analysis
  - It provides the function of analyzing not only effective IP protocol but also non-IP protocol traffic usage.
  - It provides the distribution & transition of the traffic usage by the whole,

protocol, service, and frame size.

- It provides the distribution & transition of Ingress/Egress traffic category usage by sensor & virtual network.

➢ Traffic Logging

- It provides the function of the traffic logging-the entire traffic logging & part of traffic logging- needed for the augmentative packet analysis.
- It provides various filter options for the traffic logging.
- Traffic logging file compatibility with Sniffer, Ethereal, etc.

➢ Security Audit Inquiry & Correspondence

- It provides the function of generating and storing the audit log for all security events happening in the system.

➢ Identification & Authentication

- Access to all security functions provided by TESS TAS is possible by the authorized administrator. For this, TESS TAS provides the identification & authentication function through the two phases of administrator account.

➢ Integrity Check

- It periodically monitors the system usage for the trusted operation of TESS TAS and provides the integrity check function for TSF data & executable files used in the system.

➢ Screen Lock

- Access to TESS TAS is possible by TESS TAS Console alone. When the authorized administrator doesn't use it for a certain period of time, TESS TAS provides the screen lock function by locking the session through TESS TAS Console to prevent the unauthorized access to it.

➢ Encryption Communications

- TESS TAS has a 3-tier architecture. The communications between tiers implements mutual authentication & data transmission through the SSL encryption communication.

2.2.2 TOE Environment

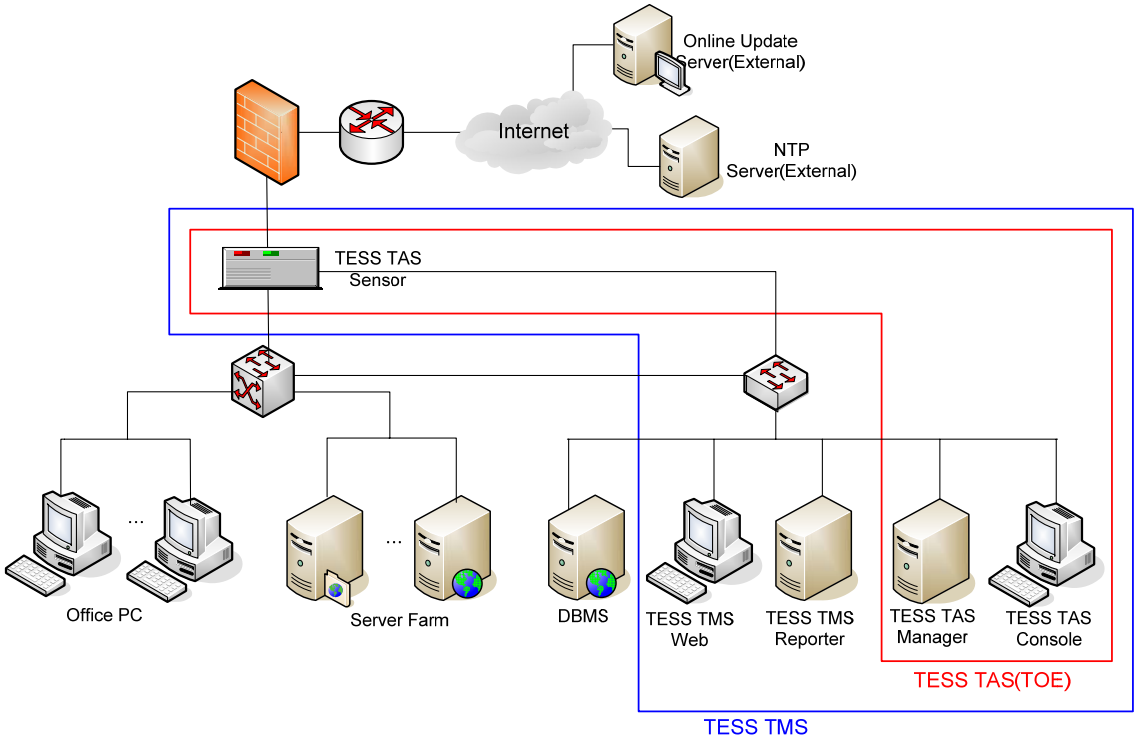
2.2.2.1 IT Environment

The IT environment of the TOE includes live update server, NTP (Network Time Protocol) server, and DBMS. For the sequential audit record, TESS TMS synchronizes the system time from the NTP server and implements the communications with the live update server to update the recent violation event list. The communications with the live update server uses the SSL protocol to implement the encryption communications while every kind of security audit log is stored by using DBMS.

2.2.2.2 Operational Environment

In the form of in-line, TESS TAS Senor shall be installed in the point of linking the internal network to the external network that are connected to the Internet. TESS TAS Manager, TESS TAS Console, DBMS, TESS TMS Web, and TESS TMS Report shall be installed in the internal network. The communications between TESS TAS Sensor & TESS TAS Manager and TESS TAS Manager & TESS TAS Console shall be encrypted as SSL. The communications for DBMS & TESS TAS Manager and DBMS & TESS TAS Console shall be protected by the SSL communication.
Updating the signature list for the intrusion prevention is performed between TESS TAS Manager and the Update Server. TESS TAS Manager shall access to the update server using the SSL encryption communication to update the signature list. All network packets are protected by the already defined TSP.

The following Figure shall schematize the configuration diagram of TESS TMS



[Figure 2-1] TOE Configuration Diagram

TESS TMS consists of TESS TAS, TESS TMS Web and Tss Tms Report while TESS TAS consists of TESS TAS Sensor, TESS TAS Manager and TESS TAS Console. TESS TMS Report can be installed in the form of the extra equipment and operate by being installed in the TESS TAS Manager or TESS TMS Web equipment. Normally, it can operate by being installed in the TESS TAS Manager or TESS TAS Web equipment.

2.2.3 TOE Configuration Component

The Five components of TESS TMS are as follows.

- TESS TAS Sensor
- TESS TAS Manager
- TESS TAS Console
- TESS TMS Report
- TESS TMS Web

TESS TAS Sensor is the component monitoring the network to directly prevent the harmful traffic and operates by being installed in the point of branching off the network into the external network & internal network or of linking the Internet to the internal network in the form of in line.
TESS TAS Manager is the component restoring every kind of detection & prevention information received from TESS TAS Sensor in DBMS and applying the contents set in the console to TESS TAS Sensor.
TESS TAS Console performs the function of the inquiry of the information on every kind of setting, detection & screening for the manager & sensor by accessing to TESS TAS Manager.
TESS TMS Report performs the function of generating the report checking the network status based on every kind of log stored in TESS TAS Manager.
TESS TMS Report doesn't belong to the scope of the evaluation.
TESS TMS Web provides the web-based service that can analyze the comprehensive status of the current network based on every kind of detection & screening log stored in DBMS.
IIS is used for the Web server to provide the Web service. TESS TMS Web doesn't belong to the scope of evaluation.
DBMS, the IT environment, stores every kind of information including the detection & screening information and is configured as the Oracle 9i version, which doesn't belong to the scope of the evaluation.

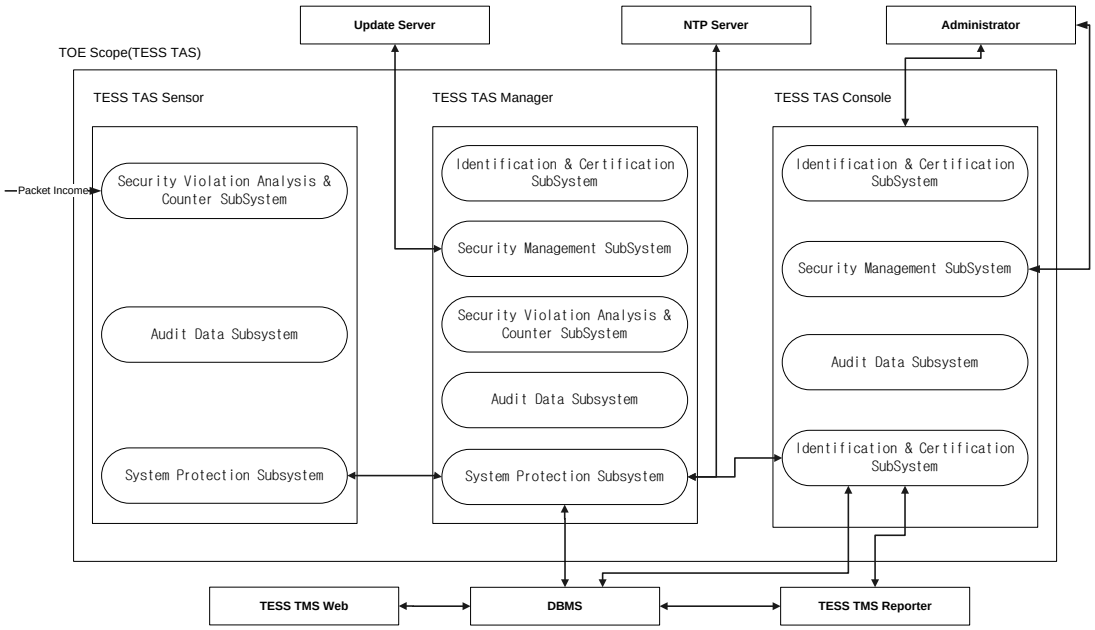
2.2.4 Scope & Boundary of Evaluated Environment

This paragraph generally describes the physical/logical scope & boundary of the TOE.

2.2.4.1 Physical Scope & Boundary

TESS TMS consists of TESS TAS Sensor, TESS TAS Manager, TESS TAS Console, TESS TMS Web, and TESS TMS Report. Every kind of security log generated in TESS TAS Sensor & TESS TAS Manager is stored in DBMS while TESS TAS Console shows the administrator the stored log by accessing to DBMS. The scope of the evaluation is confined to TESS TAS Sensor, TESS TAS Manager, and TESS TAS Console.

The following Figure shall schematize the physical scope of TOE.



[Figure 2-2] Physical Scope of the TOE

In the Figure above, the parts with dotted lines are the scope of the evaluation. Network packet, DBMS, NTP server, live update server, administrator, TESS TMS Report, and TESS TMS Web are exceptional in the evaluation.

The following [Table 2-1] shows the hardware specifications of TESS TAS. The software of TESS TAS is applied to the evaluation while the hardware & OS are not for the evaluation.

Component	Environment	
	Hardware	OS
TESS TAS Sensor	Board: Intel server board SR2400 CPU: Intel Xeon 3.0G stepping 3 Dual Memory: DDR 2G or more SCSI: LSI53C1030 Ethernet Port: 1Intel pro 10/100 Fast Ethernet (For Security Administration) Ethernet Port: 2 100 Fast Ethernet (For Packet collection) HDD: 64G or more	InfosecOS V1.0 (Self-OS)
TESS TAS	CPU: Intel Xeon 3.0G stepping 3 Dual	Windows Server

Manager	Memory: DDR 2G or more Ethernet Port: 1 10/100 Fast Ethernet or more HDD: 36G or more	2003
TESS TAS Console	CPU: Pentium4 2.4G Memory: DDR 1G or more Ethernet Port:1 10/100 Fast Ethernet or more HDD: 36G or more	Windows Server 2003

[Table 2-1] the TOE Component Hardware Specifications

Component Hardware Specifications except for the TOE are as follows.

TESS TMS Web	CPU: Intel Xeon 3.0G stepping 3 Dual or more Memory: DDR 1G or more Ethernet Port: 1 10/100 Fast Ethernet or more HDD: 36G or more	Windows Server 2003
DBMS	CPU: Intel Xeon 3.0G stepping 3 Dual or more Memory: DDR 1G or more Ethernet Port: 1 10/100 Fast Ethernet or more HDD: 72G or more	Windows Server 2003
TESS TMS Report	CPU: Intel Xeon 2.4G stepping 3 Dual or more Memory: DDR 1G or more Ethernet Port: 1 10/100 Fast Ethernet or more HDD: 36G or more	Windows Server 2003

[Table 2-2] Non-TOE Component Hardware Specifications

2.2.4.2 Logical Scope & Boundary

Security functions of the TOE are as follows.

- Security Audit

  The security audit function shall generate every kind of security-related audit data occurring in the system and counter it according to the policy that is already set. The security audit function includes the stored inquiry & retrieval function. The audit data consists of the detection/screening log generated by the intrusion detection/prevention, the system resource audit data generated by the system resource monitoring, the traffic statistics data generated by the traffic category,

and the system audit data generated in the security administration & internal system. The retrieval of the audit data is allowed for the administrator alone.

- Security Violation Analysis & Correspondence

  The function of the security violation analysis & correspondence performs the protection the monitoring target network to be protected from the internal & external attackers through the packet filtering security policy & intrusion prevention policy. This function is likely to collect the information on the intrusion & prevention, counter the attacks as there is intrusion according to the defined rules (signature list & packet filtering rule), and make the administrator to check the correspondence & intrusion results in the future by storing them. This function broadly consists of the packet data contraction & identification, packet filtering policy, protocol vulnerability analysis, session administration, signature violation analysis, statistical analysis, correspondence by violated event, traffic category, and anomalous symptom analysis. The packet filtering policy & signature violation policy are dealt in the security administrative function.

- Identification & Authentication

  An authorized administrator alone provides all security functions of this evaluation product. Functions like inquiry can be provided by the authorized administrator through every kind of security-related policy setting & inquiry and audit. The function of identifying this authorized administrator is the identification & authentication function. For these functions, TESS TAS identifies and authorizes the administrator accessing to it to check whether he or she is authorized through the administrative interface. The password for the authentication of the administrator is using SEED MAC encryption algorithm to encrypt while the encryption key of SEED MAC is using the value of hashing the administrator password into SHA-256. The encryption key is not internally stored. The identification & authentication function consists of the identification & authentication and authentication failure administration.

- Security Administration

A security function means the administrative function that can inquire or set the attribute and information on every kind of function provided by the TOE. A security function consists of the administrator account administration, security administration, audit data correspondence setting, signature list administration, security audit administration, security violation event correspondence administration, packet filtering policy administration, integrity administration, manager environment administration, sensor administration, and anomalous symptom administration.

- TSF Protection.

  The TSP protection function provides the function of checking whether major components are normally operating in the TOE system operating in the system when there is a request made by the authorized administrator. The TSP protection function also periodically shows whether the TOE is operating correctly at the time of the initial start-up. For this, the TOE provides the functions of health check, integrity checkup, synchronization of time.

- TOE Access

  In case of no operation for a certain period of time even when the authorized administrator accesses to it, the TOE system shall protect the TOE during its inactive period by locking the sessions that are mutually operating. For this, the TOE provides the screen lock function. When TESS TAS Console has been inactive for a certain period of time, locking the screen during the inactive period of the authorized administrator can protect the TOE's access.

- Trusted Path/Channel

  The trusted path/channel provides the function of protecting the authentication & data for the communication between TESS TAS Manager, TESS TAS Sensor and TESS TAS Console.

  TESS TAS has a 3-tier architecture consisting of TESS TAS Manager, TESS TAS Console and TESS TAS Sensor.

  Among these, TESS TAS Manager plays a role of a server while TESS TAS

Console and TESS TAS Sensor become the client for the communication.. The data encryption of authentication & communication between tiers uses SSL protocol, SSLv3 (Secure Socket Layer version 3).

In the process of the SSL communication, the authentication between server and client is the mutual authentication method using the public key/private key of 1024 bits generated by the RSA public key algorithm.

In other words, exchanging and authenticating the public key certificate generated by the RSA algorithm in a mutual way can certificate the counterpart. The certificate can pass through the message digest to assure the integrity after the signature with the Private Root CA certificate of TESS TAS. And the certificate is configured in the form of X509v3.

In the data communication between TESS TAS Sensor, TESS TAS Manger, and TESS TAS Console after the mutual authentication, the data encryption is using the AES method whereas the message digest for the integrity is using the SHA-256 hash message authentication code (HMAC) method. As the SSL protocol encrypts the data by generating the set of random session key by session, it can prevent the reuse of the data.

The following is the description of the function provided by TESS TMS Web, the scope of non-evaluation.

- General Diagram

  It provides the general diagram & global threat information enabling you to grasp the network threat situation. For this, it provides the global/local network threats, 7-day transition of the entire traffic & harmful traffic, 5-min. attack type/service usage top5, new global threat information.

- Comprehensive Correlation Analysis

  When undefined anomalous symptoms are found through the correlative analysis of global anomalous symptoms, local traffic anomalous symptoms, vulnerabilities, and inter-malicious code, the support function is provided for the cause analysis and correspondent decision.

- Prediction/Alarm Transmission

It provides administrators with the prediction/alarm function through e-mail & SMS. For this, it also provides the prediction/alarm setting & administrative function, while supplying the function of the transmitted prediction/alarm history administration & prediction/alarm target setting administration by the type of prediction/alarm.

The function of TESS TMS Report, the scope of non-evaluation is as follows as well.

- Report

  It supplies the daily/weekly/monthly trend analysis report & various reports using the detected traffic and log.

3 TOE Security Environment

The TSE security environment consists of the assumption describing the security for the TOE environment, possible threats posed on the TOE assets & environment by the threat agent, the security policy including the rule, procedure, principle and guidance that TOE shall observe.

3.1 Assumptions

The following conditions are assumed to exist in the TOE operational environment.

Category	Item	Remark
Assumptions	A. Physical Security	
	A. Security Maintenance	
	A. Trusted Administrator	
	A. Hardened OS	
	A. Single Connection Point	
	A. Secure TOE External Server	Added to IPSPP
	A.SSL Certificate	Added to IPSPP
	A.TIME	Added to IPSPP
	A.DBMS	Added to IPSPP

[Table 3-1] Assumptions

A. Physical Security

The TOE is located in the physically trusted environment where only authorized administrators are allowed the access.

A. Security Maintenance

When the internal network environment is changed due to network configuration changes, an increase or decrease of hosts, or an increase or decreases 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. Trusted Administrator

An authorized administrator of the TOE has no malicious intent, is well educated about the TOE administrative function, performs his/her duty in accordance with the administrative guidance.

A. Hardened OS

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. Single Defect

When the TOE is installed and operated in the network, it branches off the network into the internal network and external network. At this time, the communications between the external network and internal network can be implemented by the TOE alone.

A. Secure TOE External Server

The network time protocol (NTP) server which maintains a trusted time outside the TOE for security functions of the TOE and the update server which provides the latest attack pattern rules are secure.

A. SSL Certificate

When installed, the certificate used in the SSL protocol for the trusted communication is generated and managed in a safe manner. The TOE, when installing the certificate that will be used for SSL authentication, generates in advance and stores at the TOE, SSL Certificate of the TOE is safely generated and managed.

A.TIME

The IT environment where the TOE operates receives the Timestamp information trusted by the NTP server or OS conforming to RFC 1305. The IT environment of the TOE is provided with a reliable Timestamp from the NTP server which conforms to RFC 1305 or from the OS.

A.DBMS

The intrusion detection & traffic data generated in the TOE are stored in DBMS. The

stored data is safely managed in accordance with the identification & authentication method defined in DBMS. DBMS provides the function of the retrieval & inquiry of stored intrusion prevention & traffic data at the request of the administrator. DMBS applies the up-to-date security & vulnerability –related patch for the secure administration.

3.2 Threats

The ST defines the security threats which external threat agents can pose on the protected assets of the TOE by classifying those threats into the threat for the TOE and threat for the TOE operational environment.

Major assets that TOE is likely to protect are the computer resources and network services of the internal network or DMZ being operated by the organization. The external threat agent launches an attack to illegally access to or deplete the availability of the organization's computer resources.

Generally, threat agents are computer users or IT entities accessing to the internal computer from outside. The agent has a low level of expertise, resources, and motivation. There is an assumption that the chance for the agent to find any vulnerability that can be malignantly used is minimal.
The agent is using clear vulnerable information while attackers easily acquire vulnerable information & attack tools that can be used in a malignant way through the Internet to destroy the computer resources or illegally obtain the information. TOE protects the assets from those threats to such clear vulnerabilities.

Category	Items
Threats to the TOE (Threat)	T. Masquerade
	T. Failure
	T. Audit Failure
	T. Inbound Illegal Information
	T. Unauthorized Service Access
	T. Anomaly Packet Transfer
	T. New Vulnerability Attack
	T. DoS Attack
	T. Replay Attack
	T. Bypassing

	T. Spoofing IP Address
	T.TSF Data Modification
Threats to the TOE Operational Environment	TE. Poor Administration
	TE. Distribution and Installation

[Table 3-2] Threats

3.2.1 Threats to TOE

The protected assets of the intrusion prevention system are classified into TOE itself and those assets protected by TOE. The threats to TOE and the assets protected by TOE are as follows.

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. Audit Failure

Auditable events of the TOE may not be logged due to audit storage capacity exhaustion.

T. Inbound Illegal 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. Anomaly Packet Transfer

A threat agent may transfer network packets of anomaly structure to cause abnormal operations.

T. New Vulnerability Attack

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. DoS Attack

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. Replay Attack

A threat agent may gain access to the TOE by attempting authentication repeatedly.

T. Bypassing Attack

A threat agent can access to TOE by bypassing the security functions of the TOE.

T. Spoofing

A threat agent can illegally access to the internal network by spoofing source IP address as an internal address

T. TSF Data Modification

A threat agent can launch the buffer overflow attack on the TOE, thus resulting in unauthorized modification of the TSF data.

3.2.2 Threat to the TOE Operational Environment

TE. Poor Administration

The TOE may be configured, administered, or operated in an insecure manner by an authorized administrator.

TE. Distribution and Installation

The TOE may be damaged during its distribution or installation process.

3.3 Organizational Security Policy

This chapter addresses the organizational security policies managed by the TOE.

Category	Item	Remark
Security Policy of	P. Audit	
	P. Secure Administration	
	P. SSL Certificate Administration	Added to IPSPP

[Table 3-3] Identification of Organizational Security Policies

P. Audit

Auditable events shall be recorded and maintained to trace the responsibility of all security related actions, and the recorded data shall be reviewed.

P. Secure Administration

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

P. SSL Certificate Administration

At the time of the installation, SSL Certificate shall be generated, recorded and managed in a secure manner.

4 Security Objectives

Security objectives are categorized into objectives for the TOE and objectives for the environment. Security objectives for the TOE are managed by the TOE and security objectives for the environment by IT sector or non technical/procedural means.

Category	Item	Remark
Security Objective for the TOE	O. Availability	
	O. Audit	
	O. Administration	
	O. Abnormal Packet Screening	
	O. DoS Attack Blocking	
	O. Identification	
	O. Authentication	
	O. Information Flow Control	

	O. TSF Data Protection	
Security Objective for the Environment	OE. Physical Security	
	OE. Security Maintenance	
	OE. Trusted Administrator	
	OE. Secure Administration	
	OE. Hardened OS	
	OE. Single Connection Point	
	OE. Vulnerability List Update	
	OE. Secure TOE External Server	Added to IPSPP
	OE. SSL Protocol	Added to IPSPP
	OE. TIME	Added to IPSPP
	OE. DBMS	Added to IPSPP

[Table 4-1] Security Objective

4.1 Security Objective for the TOE

The following are the security objective that shall be directly managed by the TOE.

O. Availability

In the case of an accidental failure or a failure caused by an external attack, the TOE shall be able to maintain minimum security functions and provide regular services.

O. Audit

The TOE shall provide a means to record, store and review security-relevant events in audit record to trace the responsibility of all actions regarding security.

O. Administration

The TOE shall provide the administration tools to enable authorized administrators to effectively manage and maintain the TOE.

O. Abnormal Packet Screening

The TOE shall screen out packets with an abnormal structure from all the packets that pass through the TOE.

O. DoS Attack Blocking

The TOE, when an attacker abnormally uses services assets of a computer, shall block the use to protect the network service of the protecting computer for normal users.

O. Identification

The TOE shall 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, shall authenticate the administrator's identity before granting an access to the TOE.

O. Information Flow Control

The TOE shall control unauthorized information flow from the external network to the internal network based on security policies.

O. TSF Data Protection

The TOE shall protect stored TSF data from unauthorized disclosure, modification, or deletion.

4.2 Security Objectives for the Environment

The following are the security objectives that are managed by IT sector or non technical/procedural means.

OE. Physical Security

The TOE shall be located in physically secure environment where only authorized administrators are allowed to access.

OE. Security Maintenance

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 shall be immediately noted and security policies configured in

accordance with the TOE operational policy to maintain the same level of security as before.

OE. Trusted Administrator

An authorized administrator of the TOE possesses no malicious intention, is adequately educated, and perform his/her duties in accordance with the administrative guideline.

OE. Secure Administration

The TOE shall be distributed and installed securely, and shall be configured, administered, and used in a secure manner.

OE. Hardened OS

It performs the job of ridding the unnecessary services or means by the TOE while reinforcing the vulnerability in the OS to assure the trust and safety for the OS. 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.

OE. Single Connection Point

The TOE, when installed and operated on a network, separates the network into the internal and external network. All communication between the two id done through the TOE.

OE. Vulnerability List Update

The administrator shall update and control the vulnerability data managed by the TOE to defend external attacks exploiting new vulnerabilities of an internal computer.

OE. Secure TOE External Server

The network time protocol (NTP) server which maintains a trusted time outside the TOE for security functions of the TOE and the update server which provides the latest attack pattern rules shall be secure.

OE. SSL Protocol

The TOE mutually certificates through SSL Certificate, Administrator ID and

Password using SSL protocol, and therefore protects the transmitting TSF data..

OE.TIME

The IT environment of the TOE shall be provided with a reliable Timestamp from the NTP server which conforms to RFC 1305 or from the OS.

OE.DBMS

The intrusion detection & traffic data generated in the TOE are stored in DBMS. The stored data is safely managed in accordance with the identification & authentication method defined in DBMS. DBMS provides the function of the retrieval & inquiry of stored intrusion prevention & traffic data at the request of the administrator. DMBS applies the up-to-date security & vulnerability –related patch for the secure administration.

5 IT Security Requirements

IT security requirements describe both the security functional requirements & assurance requirements that shall be satisfied in the TOE. The requirements consists of the security functional component of the information protection system CC (CC V2.3) part 2 and assurance component related to the assurance level of part 3.

The strength of function, the objective of the ST, is somewhere in the middle of the strength of function of the network intrusion prevention system PP. The chance for the threat agent to succeed in the attack is defined to be low and the strength of function is defined to be intermediate to counter the agent. FIA_UAU.2 that has probability & permutation mechanism is also somewhere in the middle.

The framing rule follows the information protection system CC.

Iteration, selection, sophistication, assignment and operation that can be performed in the security functional requirements are allowed.

- Iteration

It is used when the same component iterates in various operations. The result of iterated operations is displayed as (Iterative number), the iterative number in a parenthesis behind the component identifier.

- Selection

When describing the requirements, it is used to select over one of options provided in the information protection system CC. The result of selection operation is displayed in underlined italics

- Sophistication

By adding details to the requirements, it is used to confine the requirements more. The result of sophistication operation is displayed in bold.

➢ Assignment

It is used to assign the specific value to unspecified parameter.(Ex: password length) The result of the assigned operation is displayed as assignment value in a bracket.

5.1 TSF Requirements

The TSF requirements components used in this document are summarized and explained in the following table. SFRs described in the following table are the name of SFR component used in claiming IPSPP. SFRs described hear are not untouched as they came from IPSPP, while “the basic protection of FPT_ITT.1 internal transmission TSF data” is added to protect the TSF data between the internal TOEs. The writer of this ST completes the operation for whose operation is not completed in IPSPP.

Security Functional Class	Security Functional Component		Remark
Security Audit	FAU_ARP.1	Security Alarm	
	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	Selectable Audit	
	FAU_STG.1	Audit Trace Protection	
	FAU_STG.3	Correspondence When Predicting Audit Data Loss	
	FAU_STG.4	Audit Data Loss Prevention	
User Data Protection	FDP_IFC.1 (1)	Partial Info. Flow Control (1)	
	FDP_IFC.1 (2)	Partial Info. Flow Control (2)	
	FDP_IFF.1 (1)	Single Layer Security Attribute (1)	
	FDP_IFF.1 (2)	Single Layer Security Attribute (2)	
Identification & Authentication	FIA_AFL.1	Authentication Failure Process	
	FIA_ATD.1 (1)	User Attribute Definition (1)	
	FIA_ATD.1 (2)	User Attribute Definition (2)	
	FIA_UAU.2	User Authentication Before All Actions	

	FIA_UAU.7	Authentication Feedback Protection	
	FIA_UID.2 (1)	User Authentication Before All Actions (1)	
	FIA_UID.2 (2)	User Authentication Before All Actions (2)	
Security Administration	FMT_MOF.1 (1)	Security Functional Administration (1)	
	FMT_MOF.1 (2)	Security Functional Administration (2)	
	FMT_MSA.1	Security Attribute Administration	
	FMT_MSA.3	Static Attribute Initialization	
	FMT_MTD.1 (1)	TSF Data Administration (1)	
	FMT_MTD.1 (2)	TSF Data Administration (2)	
	FMT_MTD.1 (3)	TSF Data Administration (3)	
	FMT_MTD.2	Administration of TSF Data Threshold	
	FMT_SMF.1	Administration Functional Specification	
	FMT_SMR.1	Security Role	
TSF Protection	FPT_AMT.1	Abstract Machine Test	
	FPT_FLS.1	Trusted Status Maintenance during Failure	
	FPT_ITT.1	Basic Protection of Internal Transmission TSF Data	Security Functional Requirements Added to IPSPP
	FPT_RVM.1	Non TSP Bypass	
	FPT_SEP.1	Security Function Region Isolation	
	FPT_STM.1	Trusted Timestamp	
	FPT_TST.1	Self-TSF Test	
Resource Utilization	FRU_FLT.1	Immunity for Errors: Partial Application	
	FRU_RSA.1	Maximum Assignment	
TOE Access	FTA_SSL.1	Session Locking by TSF	
	FTA_SSL.3	Session Shut-down by TSF	
Trusted Path/Channel	FTP_ITC.1	Trusted Channel between TSFs	

[Table 5-1] Security Functional Requirements

FIA_UAU.1 An authentication of IPSPP is replaced by the user authentication before FIA_UAU.2 All actions in this evaluation. “Basic Protection of FPT_ITT.1 internal transfer TSF data” is added to protect the TSF data between internal TOEs.

5.1.1 Security Audit

FAU_ARP.1 Security Alarm

Hierarchical To: None

FAU_ARP.1.1 The TSF shall provide [functions of SMS transference to authorized administrators, e-mail transmission, visible aural notification, program execution] when detecting the potential security violation while taking a SNMP action when violating anomalous detection & intrusion detection policy,

Dependencies: FAU_SAA.1 Potential Violation Analysis

FAU_GEN.1 Audit Data Generation

Hierarchical To: None

FAU_GEN.1.1 The TSF shall generate audit records of auditable events as follows;

a) Start-up & shut-down of the audit function

b) All auditable events according to the ***minimal*** audit ([Table 5-2] Refer to Auditable Events

c) [[Table 5-3] Additional Auditable Event]

Functional Component	Auditable Event
FAU_ARP.1	Counter action taken by urgent security violation
FAU_SAA.1	Action of the analysis mechanism initiation & halt
FAU_SEL.1	Change in the audit environment setting during the execution of audit collection function
FDP_IFF.1	Decision of allowing the requested information flow
FIA_AFL.1	Recovery to the normal status after reaching to the threshold of failed authentication attempts and its counter action
FIA_UAU.2	Failure of using the authentication mechanism
FIA_UID.2	Failure of using the administrator identification mechanism including the provided administrator's identity
FMT_SMF.1	Use of administration function
FMT_SMR.1	Change in the administrator groups sharing roles
FRU_FLT.1	All errors detected by TSF
FRU_RSA.1	Denial of the assigned operation by the resource limit
FTP_ITC.1	Failure of trusted channel function Initiator of trusted channel with failures & identification by object
FPT_STM.1	Change of time
FTA_SSL.1	Mutual operation session locking by the session locking mechanism
FTA_SSL.3	Mutual operation session shutdown by the session locking mechanism

[Table 5-2] Minimum Auditable Event

Functional Component	Auditable Event	Additional Audit Record Content
FAU_STG.3	Shortage of audit record storage	-
FMT_MTD. 1	All modifications for TSF data value	-
FMT_MTD.2	All modifications for the threshold of TSF data	-
FDP_IFF.1	Decision of denying the requested information flow-intrusion detection	-
FPT_TST.1	Integrity error occurrence & integrity check & generation	-
FAU_GEN.1	Traffic statistics data generation	Traffic volume (bps, pps)
	Intrusion detection statistics data generation	Attack count & damage count, identity of object, attacker No. & victim No.
	Intrusion prevention statistics data generation	Attack count & damage count, identity of object, attacker No. & victim No.

[Table 5-3] Additional Auditable Event

FAU_GEN.1.2 The TSF shall record the following information in each audit record.

a) Event date, event type, identity of subject, event result (success or failure)

b) [Table 5-3] auditable event based on the definition of functional components that are included in the PP/ST for the type of each audit event.

- Traffic Volume (bps, pps)
- Attack Count & Damage Count
- Object Identity (Destination IP address, port)
- Number of attackers & victims

Dependencies: FPT_STM.1 trusted Timestamp

Application Notes: The audit record of the traffic volume (bps, pps) described above is one for the traffic statistics data generation auditable event alone, and the audit records of attack counts & damage counts, object identity (Destination IP Address, Port), and number of attackers & victims are done in the intrusion detection statistics data generation & intrusion prevention statistics data generation auditable event.

FAU_GEN.2 User Identity Association

Hierarchical To: None

FAU_GEN.2.1 The TSF shall associate the identity of the user causing the event with the auditable event.

Dependencies: FAU_GEN.1 Audit Data Generation
FIA_UID.1 Identification

FAU_SAA.1 Potential Violation Analysis

Hierarchical To: None

FAU_SAA.1.1 The TSF shall apply the set of rules and point out the potential violation based on these rules when checking the audited event.

FAU_SAA.1.1 TSF shall apply rules as follows when checking the audited event.

a) The potential security violation are the accumulation or combination of []
[
- Identification & authentication security policy violation
- Anomalous symptom detection policy violation
- Intrusion detection policy violation
- Threat level policy violation
- All faults detected by TSF
- Integrity generation check
- Start & end the security audit function
- Modification to security policy setting
- Communication access & release
- DB backup & recovery
- Signature live update
- Modification to the manager environment setting

]

b) [None]

Dependencies: FAU_GEN.1 Audit Data Generation

Application Notes: The anomalous symptom detection is the function of detecting changes in the auditable events to be checked, providing the function of analyzing the increase or decrease of the network traffic & intrusion detection event. The threat level means the value of quantitatively calculating the network threat level based on

the detection event.

FAU_SAR.1 Audit Review

Hierarchical To: None

FAU_SAR.1.1 The TSF shall provide [authorized administrators] with the function enabling them to read [all audit data] from the audit record.

FAU_SAR.1.2 The TSF shall provide the audit record for user to interpret the information in a proper way.

Dependency: FAU_GEN.1 Audit Data Generation

FAU_SAR.3 Selectable Audit Review

Hierarchical To: None

FAU_SAR.3.1 TSF shall provide the ability to perform the function of ***retrieving*** the audit data based on [the following criteria with logical relations].

- Identity of Subject
- Identity of Object-Selective Provision
- Event Date
- Event Type
- Keyword (Contents of Audit Data)
- Traffic Display Criteria (bps, pps)-Selective Provision

Dependencies: FAU_SAR.1 Audit Review

Application Notes: Among the auditable events, the retrieval function using the identity of object is provided for “the decision allowing the requested information flow”, “decision-intrusion detection denying the requested information flow”, “intrusion detection statistics data generation”, and “intrusion prevention statistics data generation”. The retrieval function using the traffic display criteria is provided for “traffic statistics data generation” auditable events as well.

FAU_SEL.1 Selective Audit

Hierarchical To: None

FAU_SEL.1.1 The TSF shall include or exclude the auditable event from the audited event groups based on the following attributes.

a) *Event Type*

b) [None]

Dependencies: FAU_GEN.1 Audit Data Generation
FMT_MTD.1 TSF Data Administration

FAU_STG.1 Audit Evidence Protection

Hierarchical To: None

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

FAU_STG.1.2 The TSF shall ***prevent*** the unauthorized modification to the audit record of the audit history

Dependencies: FAU_GEN.1 audit data generation

FAU_STG.3 Correspondence When Predicting Audit Data Loss

Hierarchical To: None

FAU_STG.3.1 The TSF shall let the authorized administrator perform the SMS transmission, e-mail transmission, visible aural notice, alarm, real-time notice, and custom program when the audit evidence exceeds [80% of the rest room of the audit storage] (whenever exceeding 5%),

Dependencies: FAU_STG.1 Audit Evidence Protection

FAU_STG.4 Loss Prevention of Audit Data

Hierarchical To: FAU_STG.3

FAU_STG.4.1 The TSF shall *ignore the auditable events* when there is no room for the storage while letting [the authorized administrator perform SMS transfer, e-mail transmission, visible aural notice, real-time notice, custom program, and rid old tables selectively].

Dependencies: FAU_STG.1 Audit Trail Protection

5.1.2 User Data Protection

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

Hierarchical To: None

FDP_IFC.1.1 The TSF shall force [**packet filtering security policy**] for the operation causing the information flow from controlled subjects/subjects dealt by the following subject, information list and SFP.

a) [Subject: Unauthorized External IT Entity of the Information transmitter

b) Information: Traffic transmitted to other places from the subject through the TOE

c) Operation: Pass when there is a rule of allowing it to pass]

Dependencies: FDP_IFF.1 Single Layer Security Attribute

Application Notes: 'All Denial Policies' of IPSPP shall be notated as 'packet filtering security policies' in ST

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

Hierarchical To: FDP_IFC.1

FDP_IFC.1.1 The TSF shall force [**intrusion prevention security policy**] for the operation causing the information flow from controlled subjects/subjects dealt by the following subject, information list and SFP.

a) [Subject: Unauthorized External IT Entity of the Information transmitter

b) Information: Traffic transmitted to other places from the subject through the TOE

c) Operation: Block when there is a rule of allowing it to block]

Dependencies: FDP_IFF.1 Single Layer Security Attribute

Application Notes: 'All allowed Policies' of IPSPP shall be notated as 'intrusion prevention security policies' in ST

FDP_IFF.1(1) Single Layer Security Attribute (1)

Hierarchical To: None

FDP_IFF.1.1 The TSF shall force [packet filtering security policy] based on [the following] subject security attribute and information security attribute type.

a) Subject Security Attribute: IP address of the external IT entity, port No., protocol No. transceiving the information through the TOE

b) Information Security Attribute: Departure (IP address, port), destination (IP address, port), and protocol

FDP_IFF.1.2 The TSF shall allow the information flow between the controlled subject and controlled information through the controlled operation when the following rules maintain: [When the security attribute value of the packet filtering security policy is permissible as IP address, port No, protocol No. of input traffic from the external IT

entity that is defined by the authorized administrator match or include IP address, port and protocol among security attributes of the packet filtering security policy]
FDP_IFF.1.3 The TSF shall force [none].
FDP_IFF.1.4 The TSF shall provide [none]
FDP_IFF.1.5 The TSF shall explicitly authorize the information flow based on [none].
FDP_IFF1.6 The TSF shall explicitly deny the information flow based on [when there are no packet filtering rules set by the authorized administrator beside rules with basic settings]
Dependencies: FDP_IFC.1 Partial Information Flow Control
FMT_MSA.3 Static Attribute Initialization

Application Notes: 'All Denial Policies' of IPSPP shall be notated as 'packet filtering security policies' in ST

FDP_IFF.1(2) Single Layer Security Attribute (2)
Hierarchical To: None
FDP_IFF.1.1 The TSF shall force [intrusion prevention security policy] based on [the following] subject security attribute and information security attribute type.

a) Subject Security Attribute: IP address of the external IT entity, port No., protocol No. transceiving the information through the TOE
b) Information Security Attribute: Departure address, destination address, protocol, packet header information, packet data information

FDP_IFF.1.2 The TSF shall **block** the information flow between the controlled subject and controlled information through the controlled operation when the following rules maintain [the following rules]

Traffic Check

- When the protocol of the traffic (network packet) input from the external IP entity is the TCP and the TCP control flag is the SYN (packet header information of information security attribute). And when over threshold set in the intrusion prevention policy that is made by the authorized administrator generates
- When the protocol of the traffic (network packet) generated in the

external IP entity is the UDP, and the ICMP while having the same destination address among the information security attribute and over threshold of the intrusion prevention policy set by the authorized administrator.

Attack Pattern Check

- When the packet data information of the information security attribute of the traffic (network packet) input from the external IP entity matches or is included in the packet data information rule of intrusion prevention security policy.

FDP_IFF.1.3 The TSF shall force [none].

FDP_IFF.1.4 The TSF shall provide [none].

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

FDP_IFF1.6 The TSF shall explicitly deny the information flow based on the rules below.

a) The TOE shall block the access request for the subject IP address in the information coming from the IT entity of the internal network.
b) The TOE shall block the access request for the subject IP address in the information coming from the IT entity of the external network.
c) The TOE shall block the access request for the subject IP address to broadcast the information coming from the IT entity of the external network.
d) The TOE shall block the access request for the subject IP address for looping the information coming from the IT entity of the external network.
e) The TOE shall block the access request for the abnormal packet architecture in the information coming from the IT entity of the external network.
f) [{The following} other rules]
IP

- Backdoor Q: When the departure IP is 255.255.255.0 and the action is set to block among the information security attributes

TCP

- Trace route: When the ttl field value is 1 and action is set to block among the information security attributes, packet is blocked.
- Land Attack: When IPs of the destination & departure are the same and action is set to block among the information security attributes, packet is blocked.
- Illegal Control flag: When abnormal TCP control flag is set and action is set to block among the information security attributes, packet is blocked.

UDP

- Trace route: When the ttl field value is 1 and action is set to block among the information security attributes, packet is blocked.

ICMP

- Trace route: When the ttl field value is 1 and action is set to block among the information security attributes, packet is blocked.

- Overflow: When the length of the packet is abnormally long and action is set to block among the information security attributes, packet is blocked.

Others

- Port scanning: When an authorized administrator attempts to access to more ports than designated (threshold of the information security attribute) for a set of time at the same departure based on the statistical packet log and the action is set to block among the information security attributes, packet is blocked.

Dependencies: FDP_IFC.1 Partial Information Flow Control
FMT_MSA.3 Static Attribute Initialization

Application Notes : ‘All allowed Policies’ of IPSPP shall be notated as ‘intrusion prevention security policies’ in ST

5.1.3 Identification & Authentication

FIA_AFL.1 Authentication Failure Process

Hierarchical To: None

FIA_AFL.1.1 The TSF shall detect the authentication attempts when the [authentication attempt of the administrator]-related authorized administrator fails to attempt to get the authentication *from 1 to 100 times that the administrator can configure*.

FIA_AFL.1.2 The TSF shall perform [the affected user authentication prevention, authentication delay until the authorized administrator takes a counteraction when the number of failed authentication attempts reaches or exceeds the defined number,

Dependencies: FIA_UAU.1 Authentication

FIA_ATD.1(1) User Attribute Definition (1)

Hierarchical To: None

FIA_ATD.1.1 The TSF shall maintain the following security attribute list belonging to each IT entity: [The following security attribute]

a) IP Address

b) {None}

Dependencies: None

FIA_ATD.1(2) User Attribute Definition (2)

Hierarchical To: None

FIA_ATD.1.1 The TSF shall maintain the following security attribute list belonging to each administrator: [The following security attribute]

a) Identifier

b) {For the following additional items} User Security Attribute

- Password
- State Set Point (Normal, Locking, Delay)
- Authentication Failure Count
- Authority

Dependencies: None

Application Notes: Administrators include the primary and secondary administrator.

FIA_UAU.2 User Authentication Before All Actions

Hierarchical To: FIA_UID.1

FIA_UAU.2.1 The TSF shall successfully certificate the administrator before allowing all actions mediated by the TSF on behalf of users.

Dependencies: FIA_UID.1 Identification

FIA_UAU.7 Authentication Feedback Protection

Hierarchical To: None

FIA_UAU.7.1 The TSF shall provide the administrator with [Success or denial message, password is displayed "*"] during the authentication.

Dependencies: FIA_UAU.1 Authentication

FIA_UID.2(1) User Identification Before All Actions (1)

Hierarchical To: FIA_UID.1

FIA_UID.2.1 The TSF shall successfully identify each IT entity before allowing all actions mediated by the TSF on behalf of users.

Dependencies: None

FIA_UID.2(2) User Identification Before All Actions (2)

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall successfully identify each administrator before allowing all actions mediated by the TSF on behalf of users

Dependencies: None

Application Notes: Administrators include the primary and secondary administrator.

5.1.4 Security Administration

FMT_MOF.1(1) Security Functional Administration (1)

Hierarchical to: None

FMT_MOF.1.1 The TSF shall confine the capability to stop or start the action for [the following function list] to [the authorized administrator].

- Setting of Possible Live Update Use
- Start or Stop of Sensor
- Setting of Possible Time Synchronization Use
- Setting of Possible DB Automatic Backup Use
- Setting of Automatic Integrity Check Use

Dependencies: FMT_SMF1 Administrative Functional Specification
FMT_SMR.1 Security Role

FMT_MOF.1(2) Security Functional Administration (2)

Hierarchical to: None

FMT_MOF.1.1 The TSF shall confine the capability of *deciding the action* for [the following function list] to [the authorized administrator].

- Live Update at the Request of the Authorized Administrator.
- Offline Signature Update at the Request of the Authorized Administrator
- Activation & Application by Intrusion Detection Signature
- Activation & Application by Item of the Packet Filtering Policy
- DB Backup at the Request of the Authorized Administrator
- Integrity Check at the Request of the Authorized Administrator

Dependencies: FMT_SMF1 Administrative Functional Specification
FMT_SMR.1 Security Role

FMT_MSA.1 Security Attribute Administration

Hierarchical to: None

FMT_MSA.1.1 The TSF shall force [packet filter security policy, intrusion prevention security policy] to confine the capability of *query, alteration, deletion, [generation]* of [the following] security attribute.

Security Attribute	Action
Packet Filtering Security Policy Order	Query, Modification
Policy of Packet Filtering Security Policy (Permission/Denial/Addition/Deletion)	Query, Modification, Generation, Deletion
Name of Attack Pattern	Query, Modification
Risk of Attack Pattern (High, Low, Medium)	Query, Modification
Protocol of Attack Pattern	Query
Service of Attack Pattern (Port)	Query
Application Protocol Command of Attack Pattern	Query
Character String of Attack Pattern	Query, Modification
Capitalization Separation of Attack Pattern	Query
Beginning Position of Attack Pattern (data size)	Query
End Position of Attack Pattern (data size)	Query

Packet Size of Attack Pattern (byte)	Query
Backdoor Q	Query
Trace route	Query
Land Attack	Query
Illegal Control flag	Query
Overflow	Query, Modification
Port scanning	Query, Modification
Attack Detection Threshold	Query, Modification
Correspondent Policy After the Attack Detection-Leave Log (Leave Log, Leave Detailed Log, Leave Session Log), Screening	Query, Modification
User Definition Attack Pattern	Query, Modification, Generation, Deletion
Detection Exception Policy	Query, Modification, Generation, Deletion

[Table 5-4] Administration of Security Attribute

Dependencies: [FDP_ACC.1 Partial Access Control or
FDP_IFC.1 Partial Information Flow Control]
FMT_SMR.1 Security Role
FMT_SMF.1 Security Administrative Function Specification

FMT_MSA.3 Static Attribute Initialization

Hierarchical to: None

FMT_MSA.3.1 The TSF shall force [packet filtering security policy, intrusion prevention security policy] to provide the ***limited*** default logic of the security attribute used to force SFP.

FMT_MSA.3.2 The TSF shall let [the authorized administrator] specify the selective entry value to replace the default logic when generating an object or information.

Dependencies: FMT_MSA.1 Security Attribute Administration
FMT_SMR.1 Security Role

FMT_MTD.1(1) TSF Data Administration (1)

Hierarchical to: None

FMT_MTD.1.1 The TSF shall confine the capability of ***query, modification, deletion,***

and [generation] of [the following] to [the authorized administrator]

- Packet Filtering Security Policy
- Intrusion Prevention Security Policy
- Detection Exception Policy
- Anomalous Symptom Policy
- Host Administration Policy
- Threat Level Policy
- Physical System Setting
  - Physical Sensor Setting
  - Firewall Setting
- Logical System Setting
  - Virtual Sensor Setting
  - Virtual Network Setting

Dependencies: FMT_SMR.1 Security Role
FMT_SMF.1 Security Administrative Functional Specification

Application Notes: The detection exception policy, the function of setting the exception policy of the intrusion prevention security policy, sets the intrusion detection exception policy to prevent the intrusion. The host administrative policy is the policy of detecting the harmful traffic flowing into or from the host by registering the harmful host or administrative host. The threat level policy provides the administrator with the correspondent means in accordance with changes in the threat level by estimating the network status where the evaluation product is installed as threat level. The physical system setting provides the functions of the addition, deletion and entry-information change of TESS TAS Sensor while providing the functions of the addition, deletion and entry-information change of the firewall information to counter the firewall. The logical system setting provides the functions of the addition, deletion and change of the virtual sensor as well as the functions of the logical grouping of the physical sensor.

FMT_MTD.1(2) TSF Data Administration (2)

Hierarchical to: None

FMT_MTD.1.1 The TSF shall confine the capability of *alteration & deletion* of

[identification & authentication data] to [the authorized administrator].

Dependencies: FMT_SMR.1 Security Role
FMT_SMF.1 Security Administrative Specification

FMT_MTD.1(3) TSF Data Administration (3)

Hierarchical to: None

FMT_MTD.1.1 The TSF shall confine the capability of changing [the following] to [the authorized administrator].

- Authorized Administrator Session Time Out Value (Screen Locking Time Out Value)
- TCP Session Time Out Value Automatic Signature List Update Cycle Value
- Automatic Backup Cycle Value & Item
- Administrator Account Locking Policy
- Time Synchronization Cycle & Server Address Change
- System Audit Log Policy Change
- Automatic Integrity Check Object Setting & Check Cycle Value.

Dependencies: FMT_SMR.1 Security Role
FMT_SMF.1 Security Administration Functional Specification

FMT_MTD.2 TSF Administration of Data Threshold

Hierarchical to: None

FMT_MTD.2.1 The TSF shall confine the specification of the threshold for [failed authentication attempt count] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall take a [counteraction specified in FIA_AFL.1] when the TSF data reaches or exceeds assigned threshold.

Dependencies: FMT_MTD.1 TSF Data Administration
FMT_SMR.1 Security Role

FMT_SMF.1 Administrative Functional Specification

Hierarchical to: None

FMT_SMF.1.1 The TSF shall be able to perform the security administrative function as follows:[The following security administrative function list]

- TSF Security Functional Administration
  - FMT_MOF.1 Items specified in (Clause 5.1.1.1)
- TSF Security Attribute Administration
  - FMT_MSA.1 Items specified in (Clause 5.1.1.1)
- TSF Data Administration
  - FMT_MTD.1(1), FMT_MTD.1(2)Items specified in (Clause 5.1.1.1)
- TSF Administration of Data Threshold
  - FMT_MTD.2 Items specified in (Clause 5.1.1.1)
- Administration of Security Role
  - FMT_SMR.1 Items specified in (Clause 5.1.1.1)
- Self-Test Setting Administration
  - Integrity Check Result Inquiry
  - Initialization for Integrity Check Target (HASH data regeneration)

Dependencies: None

FMT_SMR.1 Security Role

Hierarchical to: None

FMT_SMR.1.1 The TSF shall maintain the role of [the following authorized administrator].

- Primary Administrator
- Secondary Administrator

FMT_SMR.1.2 The TSF shall correlate the roles of users & authorized administrators.

Dependencies: FIA_UID.1 Identification

Application Notes: Administrators to be maintained can be classified into the primary administrator and secondary administrator by authority.

- Primary Administrator: It refers to the authorized administrator with all authorities.
- Secondary Administrator: It refers to the administrator with confined authorities of the following five.
  - Audit Data Inquiry: Authority for the inquiry & retrieval of the security audit data
  - Policy Setting: Authority of setting & changing every kind of security policy

- System Audit Data Inquiry: Of the security audit data, the authority for the inquiry & retrieval by accessing to the system security audit data
- Report: Authority for the generation & inquiry of the report
- Account Administration: Authority for the addition, deletion and alteration of the account administration

5.1.5 TSF Protection

FPT_AMT.1 Abstract Machine Test

Hierarchical to: None

FPT_AMT.1.1 The TSF shall periodically perform a series of tests *during the general operation* to show the accurate operation of the TSF subabstract machine-related security assumptions.

Dependencies: None

FPT_FLS.1 Status Maintenance at the Time of Failure

Hierarchical to: None

FPT_FLS.1.1 The TSF shall maintain the trusted status when the following patterns of failures.

[

Failure Pattern List Described in FRU_FLT.1

]

Dependencies: ADV_SPM.1 Non-standardized the TOE Security Policy Model

FPT_ITT.1 Basic Protection of Internal Transfer TSF Data

Hierarchical to: None

FPT_ITT.1.1 The TSF shall protect the TSF data from *the disclosure & modification* when the TSF data is transmitted between the separated TOEs.

Hierarchical to: None

Application Notes: The TOE configures the SSL protocol by calling the SSL function provided as the IT environment to provide the trusted channel.

FPT_RVM.1 TSP Non-Bypass

Hierarchical to: None

FPT_RVM.1.1 The TSF shall assure the success and calling of the function forcing the TSP before each function in the TSC is allowed to perform.
Hierarchical to: None

FPT_SEP.1 Security Function Region Separation
Hierarchical to: None
FPT_SEP.1.1 The TSF shall maintain the security region for the self-execution of protecting itself from the interference & breach made by the distrustful subject.
FPT_SEP.1.2 The TSF shall separate the security region of subjects in the TSC.
Hierarchical to: None

FPT_STM.1 Trustable Timestamp
Hierarchical to: None
FPT_STM.1.1 The TSF shall be able to provide the trustable Timestamp for the TSF to use.
Dependencies: None

Application Notes : The object of this TSF requirements shall provide the Timestamp function of assuring the sequential generation of the audit data relative to the security audit function. Thus, the requirements are not necessarily implemented as the TSF requirements. The TOE can use the time provided by the TOE environment.

FPT_TST.1 TSF Self-Test
Hierarchical to: None
FPT_TST.1.1 The TSF shall perform the self test at *the time of startup, regular operation and request of the authorized administrator* to prove the correct operation of *the TSF data*.
FPT_TST.1.2 The TSF shall provide **the authorized administrator** with the function of proving the integrity of *the TSF data*.
FPT_TST.1.3 The TSF shall provide the function of letting the authorized administrator verifying the integrity of the stored TSF executable code.
Dependencies: FPT_AMT.1 Abstract Machine

5.1.6 Resource Utilization

FRU_FLT.1 Immunity for Errors: Partial Application

Hierarchical to: None

FRU_FLT.1.1 The TSF shall assure the operation of [the administrator is using the system console for the administration] when the following failures of [software failure of daemon except for the main daemon, network connection failure between parts of the TOE]

Dependencies: Trusted Status Maintenance during FPT_FLS.1 failure

FRU_RSA.1 Maximum Assignment Value

Hierarchical to: None

FRU_RSA.1.1 The TSF shall force the maximum assignment value of the following resource [transport layer representation] used by *the defined **IT entity** groups during the specified period.*

Dependencies: None

Application Notes: The transport layer representation means the connection of the SYN packet of the TCP. The SYN packet connection can attack the SYN by making anti-connection status. This attack depletes the connected table resource and interferes the connection service of normal users. The subject of the attack is the IT entity while this function can block the DoS attack of the TCP protocol stack according to the identifier of the IT entity.

5.1.7 TOE Access

FTA_SSL.1 Session Locking by TSF

Hierarchical to: None

FTA_SSL.1.1 The TSF shall lock **the authorized administrator** sessions which are mutually operating after [excess session time out value (1-60 min. base value 1 min.)]

a) Clear or overwrite the screen display device in order no to read the current contents

b) Incapacitate all actions of the data access/screen display device of **the authorized administrator** rather than release the session locking

FTA_SSL.1.2 The TSF shall request the [reauthentication of the administrator] before

releasing the session locking.
Dependencies: FIA_UAU.1 Authentication

FTA_SSL.3 Session End by the **TSF**
Hierarchical to: None
FTA_SSL.3.1 The TSF shall end the mutually operational session after [excessive time out (sec.) set in the TCP session time out of FMT_MSA.1 by the authorized administrator].

Dependencies: None

5.1.8 Trusted Path/Channel

FTP_ITC.1 Trusted Path/Channel between the TSFs
Hierarchical to: None
FTP_ITC.1.1 The TSF is logically distinguished from other communication channels between IT products that are remotely trusted by the TSF itself while providing the communication channel of protecting the channel data from a change or disclosures and identifying the assured terminal.
FTP_ITC.1.2 The TSF shall allow the *TSF* to initialize the communication through the trusted channel.
FTP_ITC.1.3 The TSF shall initialize the communication for [signature list update, communication with DBMS] through the trusted channel.
Dependencies: None

Application Notes: The TOE configures the SSL protocol by calling the SSL function provided as the IT environment to provide the trusted channel.

5.2 TOE Assurance Requirements

The assurance requirements consists of the assurance component of the CC part 3 (CC V2.3) and its assurance level is EAL4. [Table 5-4] shows the assurance component by summarizing it.

Assurance Class	Assurance Component

Configuration Administration	ACM_AUT.1	Partial Automation of Configuration Administration
	ACM_CAP.4	Generation Support & Claim Procedure
	ACM_SCP.2	Scope of Problem Trace Configuration Administration
Delivery & Operation	ADO_DEL.2	Detection of Modification
	ADO_IGS.1	Installation, Generation, Start-up Procedure
Development	ADV_FSP.2	Completely Defined External Interface
	ADV_HLD.2	Basic Design of Separating Security Function from Non-Security Function
	ADV_IMP.1	Implementation Representation for Partial TSF
	ADV_LLD.1	Descriptive & Detailed Design
	ADV_RCR.1	Verification of Non-Standardized Conformity
	ADV_SPM.1	Non-Standardized TSF Model
Guidance	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Policy
	ALC_LCD.1	Life Cycle Model Defined by Developer
	ALC_TAT.1	Well Defined Development Tool
Test	ATE_COV.2	Analysis of Scope of Test
	ATE_DPT.1	Low-Level Design Test
	ATE_FUN.1	Functional Test
	ATE_IND.2	Independent Test: Sampling Test
Vulnerability Analysis	AVA_MSU.2	Verification of Guidance Analysis
	AVA_SOF.1	Evaluation on Strength of TSF
	AVA_VLA.2	Independent Vulnerability Analysis

[Table 5-4] Assurance Requirements

5.2.1 Configuration Administration

ACM_AUT.1 Partial Configuration Administrative Automation

Dependency:

ACM_CAP.3 Authentication Control

Developer Requirements

ACM_AUT.1.1D A developer shall use the configuration administrative system.

ACM_AUT.1.2D A developer shall provide the configuration administrative plan.

Evidence Requirements

ACM_AUT.1.1C The configuration administrative system shall provide the automatic means for the authorized modifications alone in the TOE implementation representation.

ACM_AUT.1.2C The configuration administrative system shall provide the automatic means to support the TOE generation.

ACM_AUT.1.3C The configuration administrative plan shall describe the automated tools used in the configuration administrative system.

ACM_AUT.1.4C The configuration administrative plan shall describe the way of using the automated tools in the configuration administrative system.

Evaluator Requirements

ACM_AUT.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

ACM_CAP.4 Generation Support & Claim Procedure

Dependency:

ALC_DVS.1 Identification of Security Policy

Developer Requirements

ACM_CAP.4.1D A developer shall provide reference to the TOE.

ACM_CAP.4.2D A developer shall use the configuration administrative system.

ACM_CAP.4.3D A developer shall provide the configuration administrative document.

Evidence Requirements

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

ACM_CAP.4.2C The label shall be placed for the TOE reference.

ACM_CAP.4.3C The configuration list shall identify all configuration items alone that are configuring the TOE.

ACM_CAP.4.4C The configuration documents shall include the configuration list, configuration administrative plan and claim plan.

ACM_CAP.4.5C The configuration list shall describe the configuration item configuring the TOE.

ACM_CAP.4.6C The configuration administrative document shall describe the way of uniquely identifying the configuration items.

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

ACM_CAP.4.8C The configuration administrative plan shall describe the way used by the configuration administrative system.

ACM_CAP.4.9C The evidence shall prove that the configuration administrative system is being operated according to the configuration administrative plan.

ACM_CAP.4.10C The configuration administrative document shall provide the evidence that all configuration items were effectively managed in the configuration administrative system and those are being managed even now.

ACM_CAP.4.11C The configuration system shall provide the means of allowing only the authorized modification to the configuration item.

ACM_CAP.4.12C The configuration administrative system shall support the TOE generation.

ACM_CAP.4.13C The claim plan shall describe the procedure used in claiming the configuration item that is modified or newly generated as part of the TOE.

Evaluator Requirements

ACM_CAP.4.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

ACM_SCP.2 Scope of Problem Trace Configuration Administration

Dependency:

ACM_CAP.3 Authentication Control

Developer Requirements

ACM_SCP.2.1D A developer shall provide the configuration item list for the TOE.

Evidence Requirements

ACM_SCP.2.1C The configuration item list shall include the evaluation evidence required by the assurance component of implementation representation, security bug and the ST.

Evaluator Requirements

ACM_SCP.2.1E An evaluator shall confirm whether the provided information meets the requirements for all evidences.

5.2.2 Delivery & Operation

ADO_DEL.2 Detection of Operation

Dependencies:

ACM_CAP.3 Authentication Control

Developer Requirements

ADO_DEL.2.1D A developer shall document the procedure for delivering the TOE or part of the TOE for users.

ADO_DEL.2.2D A developer shall use the procedure for the delivery.

Evidence Requirements

ADO_DEL.2.1C When the TOE is delivered to users, the delivered document shall describe all procedures needed for the security maintenance.

ADO_DEL.2.2C The delivered document shall describe various procedures and technological means to detect any modification or changes made by the original and inter-versions performed by users.

ADO_DEL.2..3C When a developer delivers nothing to users, the delivered document shall describe various procedures for the detection of the delivery attempts masqueraded as the developer.

Evaluator Requirements

ADO_DEL.2.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

ADO_IGS.1 Installation, Generation Start-up Procedure

Dependency:

AGD_ADM.1 User Guidance

Developer Requirements

ADO_IGS.1.1D A developer shall document the procedure needed for the trusted installation, generation, start-up of the TOE.

Evidence Requirements

ADO_IGS.1.1C The installation, generation, and start-up documents shall describe all stages needed for the trusted installation, generation, and start-up of the TOE.

Evaluator Requirements

ADO_IGS.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

ADO_IGS.1.2E An evaluator shall decide whether the TOE is configured in a trust way through the procedure of installation, generation, and start-up.

5.2.3 Development

ADV_FSP.2 Completely Defined External Interface

Dependency:

ADV_RCR.1 Non-Standardized Conformity Verification

Developer Requirements

ADV_FSP.2.1D A developer shall provide the functional specification.

Evidence Requirements

ADV_FSP.2.1C The functional specification shall describe the TSF & the TSF external interface in a non-standardized way.

ADV_FSP.2.2C The functional specification shall have internal consistency.

ADV_FSP.2.3C The functional specification shall properly provide the details for effect, exception & error message and describe the use objective & method of all TSF external interfaces.

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

ADV_FSP.1.5C The functional specification shall include the rationale for the complete representation of the TSF.

Evaluator Requirements

ADV_FSP.2.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

ADV_FSP.2.2E An evaluator shall decide whether the functional specification completely substantiates the TOE security functional requirements.

ADV_HLD.2 Basic Design Separating Security Function from Non-Security Function

Dependency:

ADV_FSP.1 Non-Standardized Functional Specification

ADV_RCR.1 Verification of Non-Standardized Conformity

Developer Requirements

ADV_HLD.2.1D A developer shall provide the basic design of the TSF.

Evidence Requirements

ADV_HLD.2.1C The basic design shall be represented in the non standardized way.

ADV_HLD.2.2C The basic design shall have internal consistency.

ADV_HLD.2.3C The basic design shall describe the TSF architecture with subsystems.

ADV_HLD.2.4C The basic design shall describe the security function provided by each subsystem.

ADV_HLD.2.5C The basic design shall identify subhardware, firmware, and software that the TSF request by representing the function provided by subsidiary protection mechanism implemented in subhardware, firmware, and software.

ADV_HLD.2.6C The basic design shall identify all interfaces of the TSF subsystem.

ADV_HLD.2.7C The basic design shall identify the external interface of the TSF subsystem.

ADV_HLD.2.8C The basic design shall describe the objective of use or method of all interfaces for the subsystem of the TSF by properly providing the details for effect, exception, error message, etc.

ADV_HLD.2.9C The basic design shall describe the TOE by separating the TSP

execution subsystem from other subsystems.

Evaluator Requirements

ADV_HLD.2.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

ADV_HLD.2.2E An evaluator shall decide whether the basic design completely substantiates the TOE security functional requirements.

ADV_IMP.1 Implementation Representation for Partial TSF

Dependency:

ADV_LLD.1 Descriptive & Detailed Design

ADV_RCR.1 Verification of Non-Standardized Conformity

ALC_TAT.1 Well Defined Development Tools

Developer Requirements

ADV_IMP.1.1D A developer shall provide the implementation representation for the selected TSF.

Evidence Requirements

ADV_IMP.1.1C The implementation representation shall clearly define the TSF in a detailed way to generate the TSF without more design processes

ADV_IMP.1.2C The implementation representation shall have internally consistency.

Evaluator Requirements

ADV_IMP.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements

ADV_IMP.1.2E An evaluator shall decide whether the most concrete the TSF representation completely substantiates the TOE security functional requirements

ADV_LLD.1 Descriptive & Detailed Design

Dependency:

ADV_HLD.2 The basic design separating the security function and non-security function

ADV_RCR.1 Verification of non-standardized conformity

Developer Requirements

ADV_LLD.1.1D A developer shall provide the detailed design.

Evidence Requirements

ADV_LLD.1.1C The detailed design shall be represented in the non-standardized way.

ADV_LLD.1.2C The detailed design shall have internal consistency.

ADV_LLD.1.3C The detailed design shall describe the TSF as module.

ADV_LLD.1.4C The detailed design shall describe objectives of each module.

ADV_LLD.1.5C The detailed design shall design the mutual relations between modules as the provided security function and dependency with other modules.

ADV_LLD.1.6C The detailed design shall describe the method of providing each TSP-execution.

ADV_LLD.1.7C The detailed design shall identify all interfaces of the TSF module.

ADV_LLD.1.8C The detailed design shall identify the external interface of the TSF module.

ADV_LLD.1.9C The detailed design shall describe the objective of use or method of all interfaces for the TSF module by properly providing the details for effect, exception, error message, etc.

ADV_LLD.1.10C The detailed design shall describe the TOE by separating TSP execution module and other modules.

Evaluator Requirements

ADV_LLD.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements

ADV_LLD.1.2E An evaluator shall decide whether the detailed design completely substantiates the TOE security functional requirements

ADV_RCR.1 Verification of Non-Standardized Conformity

Dependencies: None

Developer Requirements

ADV_RCR1.1D A developer shall provide the analysis of the conformity between representations of all neighboring TSFs.

Evidence Requirements

ADV_RCR.1.1C For each representation of neighboring TSFs, all related security functionalities of more abstract TSF representation is more clearly and completely refined in the concrete TSF representation through the analysis.

Evaluator Requirements

ADV_RCR.1. The evaluator shall confirm whether the provided information meets all evidence requirements.

ADV_SPM.1 Non-Standardized TOE Security Policy Model

Dependencies:

ADV_FSP.1 Non-Standardized Functional Specification

Developer Requirements

ADV_SPM.1.1D A developer shall provide the TSP model.

ADV_SPM.1.2D A developer shall provide the conformity between the functional specification and TSP model.

Evidence Requirements

ADV_SPM.1.1C The TSP model shall be non-standardized.

ADV_SPM.1.2C The TSP model shall describe the rules and traits of all policies of the TSP whose modeling is possible.

ADV_SPM.1.3C TSP The TSP model shall include the rationale for the perfection and conformity of all policies of the TSP whose modeling is possible.

ADV_SPM.1.4C TSP Where there is conformity between the TSP model and the functional specification, all security functions specified in the ST shall be proved to be consistent and perfect for the TSP model.

Evaluator Requirements

ADV_SPM.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements

5.2.4 Guidance

AGD_ADM.1 Administrator Guidance

Dependency:

ADV_FSP.1 Non-Standardized Functional Specification

Developer Requirements

AGD_ADM.1.1D A developer shall provide the administrator guidance for the person managing the system.

Evidence Requirements

AGD_ADM.1.1C The administrator guidance shall describe the administrative function & interface that the TOE administrator can use.

AGD_ADM.1.2C The administrator guidance shall describe the way of managing the TOE in a trusted way.

AGD_ADM.1.3C The administrator guidance shall include the warning for the function & privilege controlled in the trusted process environment

AGD_ADM.1.4C The administrator guidance shall describe all assumptions for user actions relative to the trusted operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator by properly representing the trusted value.

AGD_ADM.1.6C The administrator guidance shall describe each pattern of security-related events for the administrative function to be performed, including the security characteristic modification under the TSF control.

AGD_ADM.1.7C The administrator guidance shall has consistence along with other documents submitted for the evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements of the IT environment for the administrator.

Evaluator Requirements

AGD_ADM.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements

AGD_USR.1 User Guidance

Dependency:

ADV_FSP.1 Non-Standardized Functional Specification

Developer Requirements

AGD_USR.1.1D A developer shall provide the user guidance.

Evidence Requirements

AGD_USR.1.1C The user guidance shall describe the function and interface that the TOE user can use not the administrator.

AGD_USR.1.2C The user guidance shall describe the use of the TOE security function that the user can use.

AGD_USR.1.3C The user guidance shall include the warning for the function and privilege that can be used by the user who has to be controlled in the trusted process environment.

AGD_USR.1.4C The user guidance shall clearly indicate the user's accountabilities needed for the trusted operation of the TOE, including the responsibility for the assumptions relative the user action in the TOE security environment.

AGD_USR.1.5C The user guidance shall have consistence along with other documents submitted for the evaluation.

AGD_USR.1.6C The user guidance shall describe the security requirements in the IT environment for users.

Evaluator Requirements

AGD_USR.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

5.2.5 Life Cycle Support

ALC_DVS.1 Identification of Security Policy

Dependencies: None

Developer Requirements

ALC_DVS.1.1D A developer shall write the development security document.

Evidence Requirements

ALC_DVS.1.1C The development security document shall describe all necessary physical, procedural, human and other security policy to protect the confidentiality and integrity in the process of the TOE design and implementation in the development environment.

ALC_DVS.1.2C The development security document shall provide the evidence

that such a security policy is being observed during the development and maintenance of the TOE.

Evaluator Requirements

ALC_DVS.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements

ALC_DVS.1.2E An evaluator shall confirm whether the security policy is well applied.

ALC_LCD.1 Life Cycle Model Defined by Developer

Dependencies: None

Developer Requirements

ACL_LCD.1.1D A developer shall establish the life cycle model used for the development and maintenance of the TOE.

ACL_LCD.1.2D A developer shall provide the life cycle definition document.

Evidence Requirements

ALC_LCD.1.1C The life cycle definition document shall describe the model used for the development and maintenance of the TOE.

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

Evaluator Requirements

ALC_LCD.1.1E An evaluator shall confirm whether the security policy is well applied.

ALC_TAT.1 Well Defined Development Tool

Dependency:

ADV_IMP.1 Implementation Representation for the partial TSF.

Development Requirements

ALC_TAT.1.1D A developer shall identify the development tool used in the TOE.

ALC_TAT.1.2D A developer shall document the implemented-dependent selected record of the options in terms of the development tools.

Evidence Requirements

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

ALC_TAT.1.2C The development tool document shall define meanings of all commands in an unambiguous way.

ALC_TAT.1.3C The development tool document shall define the meanings of all implemented-dependent options in an unambiguous way.

Evaluator Requirements

ALC_TAT.1.1E An evaluator shall confirm whether the security policy is well applied.

5.2.6 Test

ATE_COV.2 Analysis of Scope of Test

Dependency:

ADV_FSP.1 Non-Standardized Functional Specification

ATE_FUN.1 Functional Test

Developer Requirements

ATE_COV.2.1D A developer shall provide the analysis of the scope of the test

Evidence Requirements

ATE_COV.2.1C The analysis of the scope of the test shall prove the conformity between TSFs described in the test item and functional specification identified in the test document.

ATE_COV.2.2C The analysis of the scope of the test shall prove the conformity between TSFs described in the functional specification and the test item identified in the test document.

Evaluator Requirements

ATE_COV.2.1E An evaluator shall confirm whether the security policy is well applied.

ATE_DPT.1 Low-Level Design Test

Dependency:

ADV_HLD.2 Basic Design Separating the Security Function and Non-Security Function

ADV_LLD.1 Describes & Detailed Design

Developer Requirements

ATE_DPT.1.1D A developer shall provide the detailed analysis of the test.

Evidence Requirements

ATE_DPT.1.1C The detailed analysis of the test shall prove that the test item identified in the test document is good enough to verify the operation of TSF in accordance with the basic design

Evaluator Requirements

ATE_DPT.1.1E An evaluator shall confirm whether the security policy is well applied.

ATE_FUN.1 Functional Test

Dependencies: None

Developer Requirements

ATE_FUN.1.1D A developer shall document the result by testing the TSF.

ATE_FUN.1.2D A developer shall provide the test document.

Evidence Requirements

ATE_FUN.1.1C The test document shall consist of the test plan, test procedural description, expected test result and real test result.

ATE_FUN.1.2C The test plan shall describe the test objectives which shall identify and perform the security function to be tested.

ATE_FUN.1.3C The test procedural description shall describe the scenario for the test on each security function and for the identification of the test items to be executed. Such a scenario shall include the order dependency for other test results.

ATE_FUN.1.4C The expected test result shall prove the expected results from the successful test execution.

ATE_FUN.1.5C The result of the test given by the administrator shall prove that each tested security function is operating in accordance with the specification.

Evaluator Requirements

ATE_FUN.1.1E An evaluator shall confirm whether the security policy is well applied.

ATE_IND.2 Independent Test: Sample Test

Dependency:

ADV_FSP.1 Non-Standardized Functional Specification

AGD_ADM.1 Administrator Guidance

AGD_USR.1 User Guidance

ATE_FUN.1 Functional Test

Developer Requirements

ATE_IND.2.1D A developer shall provide the TOE to be tested.

Evidence Requirements

ATE_IND.2.1C The TOE shall be good enough to be tested

ATE_IND.2.2C A developer shall provide the identical resources to those used in the TSF functional test of the developer.

Evaluator Requirements

ATE_IND.2.1E An evaluator shall confirm whether the provided information meets the evidence requirements

ATE_IND.2.2E An evaluator shall properly test part of the TSF to check the operation of the TOE according to the specification

ATE_IND.2.3E An evaluator shall perform the sample test on the test item in the test document to verify the developer test result.

5.2.7 Vulnerability Analysis

AVA_MSU.2 Verification of Guidance Analysis

Dependency:

ADO_IGS.1 Installation, Generation, Start-up Procedure

ADV_FSP.1 Non-Standardized Functional Specification

AGD_ADM.1 Administrator Guidance
AGD_USR.1 Guidance

Developer Requirements
AVA_MSU.2.1D A developer shall provide the guidance.

Evidence Requirements
AVA_MSU.2.1C The guidance (including post-failure operation & post-operative errors operation) shall identify related items for all possible operation mode, its effect and trusted operation maintenance of the TOE.
AVA_MSU.2.2C The guidance shall be perfect, clear, consistent and feasible.
AVA_MSU.2.3C The guidance shall enumerate all assumptions for the intended environment.
AVA_MSU.2.4C The guidance (including procedural, physical, human control) shall enumerate all requirements for the external security policy.

Evaluator Requirements
AVA_MSU.2.1E An evaluator shall confirm whether the provided information meets all evidence requirements.
AVA_MSU.2.2E An evaluator shall iterate all configuration & installation procedure as well as other procedures in a selective way to confirm that the TOE is configured and used in a trusted way by using the guidance alone.
AVA_MSU.2.3E An evaluator shall decide that all unsafe status can be detected using the guidance.
AVA_MSU.2.4E An evaluator shall confirm whether the guidance shows the provision of the trusted operation for all operation modes of the TOE.
AVA_SOF.1 Evaluation on Strength of the TSF
Dependency:
ADV_FSP.1 Non-Standardized Functional Specification
ADV_HLD.1 Described & Detailed Description

Developer Requirements
AVA_SOF.1.1D A developer shall perform the strength analysis of the TSF for each identified mechanism in the ST where the strength of the TSF is declared

Evidence Requirements

AVA_SOF.1.1C The strength analysis of the TSF shall prove that the strength of the TSF meets or exceeds the minimum the SOF level defined in the PP/ST for each mechanism where the strength of the TSF is declared.

AVA_SOF.1.2C The strength analysis of the TSF shall prove that the strength of the TSF meets or exceeds the minimum the SOF level defined in the PP/ST for each mechanism where the specific strength of the TSF is declared.

Evaluator Requirements

AVA_SOF.1.1E An evaluator shall confirm whether the provided information meets all evidence requirements.

AVA_SOF.1.2E An evaluator shall confirm whether the SOF declaration is correct.

AVA_VLA.2 Independent Vulnerability Analysis

Dependency:

ADV_FSP.1 Non-Standardized Functional Specification

ADV_HLD.2 Basic Design Separating the Security Function & Non-Security Function

ADV_IMP.1 Implementation Representation of the Partial TSF

ADV_LLD.1 Descriptive & Detailed Design

AGD_ADM.1 Administrator Guidance

AGD_USR.1 User Guidance

Developer Requirements

AVA_VLA.2.1D A developer shall perform the vulnerability analysis.

AVA_VLA.2.2D A developer shall provide the vulnerability analysis document.

Evidence Requirements

AVA_VLA.2.1C The vulnerability analysis document shall describe the analysis of the TOE submitted document performed to find the method of violating the TSP by the user.

AVA_VLA.2.2C The vulnerability analysis document shall enumerate identified vulnerabilities.

AVA_VLA.2.3C The vulnerability analysis document shall prove that the vulnerability can’t be used in a malignant way in the intended environment of the

TOE for all identified vulnerabilities.

AVA_VLA.2.4C The vulnerability analysis document shall justify that the TOE with some identified vulnerabilities has an immunity from clear penetration attacks

Evaluator Requirements

AVA_VLA.2.1E An evaluator shall confirm that the provided information meets all evidence requirements.

AVA_VLA.2.2E An evaluator shall perform the penetration test based on the vulnerability analysis of the developer for ensuring the handling of those identified vulnerabilities.

AVA_VLA.2.3E An evaluator shall perform the independent vulnerability analysis.

AVA_VLA.2.4E An evaluator shall perform the independent penetration test based on the independent vulnerability analysis for deciding the possibility of additionally identified vulnerabilities used in a malignant way in the intended environment.

AVA_VLA.2.5E An evaluator shall decide whether the TOE has an immunity from attackers with low-level of the possible success in the attack

5.3 Security Requirements for the Environment

Security requirements for the IT environment are as follows.

5.3.1 TSF Protection

FPT_STM.1 Trusted Timestamp

Hierarchical to: None

FPT_STM.1.1 The TSF shall provide the trusted Timestamp to be used by the TSF.

Dependencies: None

Application Notes: The method of the TOE maintaining the trusted Timestamp shall bring time from the NTP server or suboperating system of the TOE. The TOE can maintain the trusted Timestamp with a help of the NTP server provided in the IT environment and get the system time information provided by the OS.

5.3.2 Security Audit

FAU_SAR.3 Selectable Audit Review

Hierarchical to: None

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

- Identity of Subject
- Identity of Object-Selective Provision
- Event Date
- Event Type
- Keyword (Audit Data Contents)
- Traffic Display Criteria (bps, pps)-Selective Provision

Dependencies: FAU_SAR.1 Audit Review

Application Notes: Of auditable events, the retrieval function is provided for “the decision of allowing the requested information flow”, “decision of denying the requested information flow-intrusion detection”, “intrusion detection statistics data generation”, and “intrusion prevention statistics data generation“ through the identities of objects. The retrieval function is provided for “the traffic statistics data generation” and auditable events by using the traffic display criteria (bps, pps)

FAU_STG.1 Audit Evidence Protection

Hierarchical to: None

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

FAU_STG.1.2 The TSF shall ***prevent*** the unauthorized modification to the audit records in the audit history.

Dependencies: FAU_GEN.1 Audit Data Generation

5.3.3 TSF Protection

FPT_ITT.1 Basic Protection of Internal Transfer TSF Data

Hierarchical to: None

FPT_ITT.1.1 The TSF shall protect the TSF data from the disclosure & modification when the TSF data is transmitted between parts of the separated TOEs.
Dependencies: None

Application Notes: The TOE provides the trusted channel as it configures the SSL protocol by calling the SSL function provided by the IT environments.

5.3.4 Trusted Path/Channel

FTP_ITC.1 Trusted Channel between TSFs
Hierarchical to: None
FTP_ITC.1.1 The TSF shall provide the communication channel to protect the channel data from the disclosure or modification while providing the assured identification of the terminal and being logically separated from other communication channels between trusted IT products.
FTP_ITC.1.2 The TSF shall allow the *TSF* to initialize the communication through the trusted channel.
FTP_ITC.1.3 The TSF shall initialize the communication through the trusted channel for [signature list update, communication with DBMS]
Dependencies: None

Application Notes: The TOE provides the trusted channel as it configures the SSL protocol by calling the SSL function provided by the IT environments

6 TOE Summary Specification

This chapter briefly and clearly describe how the TSF is implemented. It also explains how the security requirements are satisfied.

Of the security functions implemented by this TOE, the security function which has probability & permutation mechanisms is “identification & authentication (IA_UID)”while the SOF has a high level of the security function meeting the satisfaction of the medium the SOF, the SOF of FIA_UAU.2. “Identification & authentication (IA_UID)”is implemented by the password authentication mechanism.

6.1 TSF

This paragraph describes the TSF. Security functions provided by the TOE are as follows;

- Security Audit (AT)
- Security Violation Analysis & Correspondent (DP)
- Identification & Authentication (IA)
- Security Administration (SM)
- TSF Protection (PT)
- TOE Access (TA)
- Trusted Path/Channel (SP)

6.1.1 Security Audit (AT) Function

The security audit function is broadly used to let users confirm that the TOE system is being operated in a trusted and effective way and that everything is being operated as planned.

- Audit Data Generation (AT_GEN)
- Audit Data Inquiry (AT_SAR)
- Audit Data Correspondence (AT_RES)

The audit data generated during the operations of TESS TAS Sensor, TESS TAS

Manager and TESS TAS Console is transmitted to TESS TAS Manager and TESS TAS Manager records these in the DB.

6.1.1.1 Audit Data Generation (AT_GEN) Function

The audit data generation let the security audit log be generated for every kind of event occurring from the security function in the system.

Of the security attributes of the packet filtering security policy, the audit record option activates or deactivates the selected rules to decide whether the affected rules generate the audit history or not. The TESS TAS generates the audit record for the rules set to generate the audit records alone.

Of the security attributes of the intrusion prevention security policy, the TESS TAS generates the audit records for only the rules selecting the audit record options.

The audit function starts at the same time of the beginning of the main processor of the TESS TAS Sensor & Manager while it ends along with the end of the main processor. In this evaluated product, information like the process name and time is recorded as the form of the audit data as well as the beginning and end are recorded at the time of beginning and end of the main daemon (main process sensor & monitor process of TESS TAS Sensor and main process & monitor process of TESS TAS Manager) configuring the product.

[Table 5-2], The auditable events described in [Table 5-3] store the following information in the audit history data record.

- Event Date
- Event Type
- Identity of Subject
- Event Result –Success or Failure

When the traffic statistics data is generated, the traffic volume (bps, pps) is additionally recorded in the audit record contents mentioned while information including the attack count, damage count, victim identity (IP, Port), number of attackers, number of victims is additionally recorded when the intrusion

prevention/intrusion screening statistics are generated.

When the audit record is generated for the correspondent rules set in the system audit data reaction administration (SM_ADT), the reaction is done through the audit data reaction (AT_RES) in accordance with the rules set in the security administration.

The intrusion detection statistics data & intrusion prevention statistics data are generated in the audit data generation based on the intrusion detection screening audit data generated in the security violation analysis & correspondence.

The audit data generated in this evaluated produce is as follows;

- Security audit data (system audit data) generated in the security administrative (SM) function
  - The modification to the correspondent setting of the detection policy with the security audit log generated by the security administrative (SM) function and to every kind of security administrative function of the packet filtering means the audit log generated. Hereinafter referred to as the system audit data.
- Intrusion detection/blocking audit data in the function of the security violation analysis & correspondence (DP)
  - Means the log for the intrusion detection or packet screening. Hereinafter referred to as the intrusion detection log intrusion screening audit data.
- Network traffic statistics audit data
  - Means the traffic statistics data by separating the network traffic in accordance with the criteria. That is called as the traffic statistics audit data.
- Audit data generated through the system monitoring
  - Means the log generated by the resource condition monitoring of the system. Hereinafter referred to as the system resource audit data.

This evaluated product can generate the audit data for the following potential security violation items and detect the potential violation by analyzing these items.

- Identification & Authentication Security Policy Violation
- Anomalous Symptom Detection Policy Violation

- Referring to the function of detecting the sudden rise & fall in traffic or intrusion detection event.
- Intrusion Detection Policy Violation
- Threat Level Policy Violation
- All Failures Detected by TSF
- Integrity Generation & Check
- Beginning & End of the Security Audit Function
- Security Policy Setting Modification
- Communication Access & Release
- DB Backup & Recovery
- Signature Live Update
- Manager Configuration Modification

This evaluated product provides the function of generating or not generating the audit data by the audit data type through the packet filtering policy administrative (SM_FLT), signature list administration (SM_SIG) and system audit data correspondence administration (SM_ADT).

Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN2, FAU_SAA.1, FAU_SEL.1

6.1.1.2 Audit Data Inquiry (AT_SAR) Function

All audit data generated in the TOE system can only be inquired and retrieved through the GUI interface of TESS TAS Console.

The inquiry of the audit data allows only the authorized administrator (the one with the authority of the inquiry & retrieval) to have the function of the inquiry & retrieval. Authorities by administrator can be described in the administrator account administration (SM_ACC).

An authorized administrator can retrieve the audit data according to the following the retrieval condition.

- Event Day & Time (Date & Time)
- Event Type

- Identity of Subject
- Keyword (Audit Data Contents)

The information on the identity of objects is additionally recorded (AT_GEN_ in the audit data for the packet allowed by the packet filtering (DP_FLT) and provides the function of the retrieval by using the identity of objects.

In the traffic statistics audit data generated in the traffic statistics generation (DP_TRA), the audit data can be retrieved on the retrieval condition of bps, pps. The intrusion screening statistics & intrusion detection statistics data (AT_GEN) provides the retrieval function by adding the object (IP, port) condition to the retrieval condition above.

The security log generated in the security administrative (SM) function out of the audit data allows only the authorized administrator to retrieve and inquire it. The administrator authority provided by this evaluated product consists of two phases. The administrator account is explained in the following the administrator account administration (SM_ACC).

Functional Requirements Satisfied: FAU_SAR.1, FAU_SAR.3

6.1.1.3 Audit Data Correspondence (AT_RES)

For the system audit data out of the audit data generated in the audit data generation (AT_GEN), the following administrator notice function is provided.

- Real-Time Notice
  - Rea-time notice function for all administrators connected to console. The contents of the audit data are displayed in notice window of TESS TAS.
- SMS Transmission
  - Transmission of SMS message to the cellular phone of the administrators registered in the administrator account.
- E-mail Transmission
  - Transmission of the e-mail to the e-mail account of the administrators registered in the administrator account

- Visible Audible Notice
  - Generation of the message box along with the siren for the visible audible notice to all administrators connected to console.
- Custom Program Execution
  - Program execution already registered by the administrator

The system audit data correspondent setting is done through the security administrative audit data administration (SM_ADT).

. For the intrusion detection audit data, this evaluated product provides the following functions.

- SNMP Interworking
  - Transmission of the SNMP message for the intrusion detection audit data to the external SNMP server.
- Firewall Interworking
  - Provides the function of interworking with the external firewall with the intrusion screening function.

Ways of preventing the audit record loss due to the saturation of the audit record stores are as follows;

- When the audit data loss is expected (with 80% or more of the storage capacity)
  - Take a correspondent action providing functions of real-time notice, visible audible notice, SMS transfer, e-mail transfer, custom program execution which are provided from the security data correspondence (AT_RES) for the administrator.
  - When the storage capacity is over 80%, notice it to the administrator whenever exceeding 5%.
  - The stores of the audit data are checked once a minute. (Health Check (PT_HCH))
- When the audit data is saturated
  - Generated audit data is not recorded but executes the notice function for the administrator.
- The administrator notice setting can be done through the system audit data reaction administration (SM_ADT).

Functional Requirements Satisfied: FAU_ARP.1, FAU_STG.3, FAU_STG.4

6.1.2 Security Violation Analysis & Correspondence (DP)

The security violation analysis & correspondence (DP) provides the functions of the packet filtering, intrusion detection, traffic statistics generation & anomalous symptom detection to protect the auditable network from the external/internal attackers. It provides the following functions.

- Packet Data Contraction & Identification (DP_GET)
- Packet Filtering (DP_FLT)
- Protocol Vulnerability Analysis (DP_ID1)
- Session Administration (DP_ID2)
- Signature Violation Analysis (DP_ID3)
- Statistics Analysis (DP_ID4)
- Correspondence by Violated Event (DP_RES)
- Traffic Statistics Generation (DP_TRA)
- Anomalous Symptom Detection (DP_ANM)

6.1.2.1 Packet Data Contraction & Identification (DP_GET)

The packet data contraction & identification (DP_GET) extracts the packet summary information for the collected packet by collecting the network packet. All network packets targeted for the audit get the flow control through the TEO. The packet data contraction & identification (DP_GET) input all network packets from the network device.

The network packet, the IP packet, analyzed in this evaluated product identifies the subject and object by using the IP address of the packet.
For the packet filtering & intrusion prevention function provided from this evaluated product, all network packets are initially input as the packet data contraction & identification (DP_GET). After that, the packet is analyzed for the packet filtering (DP_FLT) & intrusion prevention (DP_ID1, DP_ID2, DP_ID3, DP_ID4).
The summary information of the packet provided in this function consists of the following items.

- IP Address
- Protocol No.
- Port No.
- Network No.
- IP Header Size
- TCP Header Size
- Packet Length

This evaluated product is the analysis function of dividing the auditable network into several virtual networks. Such functions include the function of classifying the virtual network that the network packet belongs to. The category criteria of the virtual network is as follows.

- IP Scope
  - Virtual Network Configuration Using IP Scope
- VLAN
  - Virtual Network Configuration Using the VLAN Tag in the VLAN Environment
- HTTP URL Address
  - Virtual Network Configuration Using the URL Information of the HTTP Packet

The summary information of the packet is the foundation of the functions of packet filtering (DP_FLT) & protocol vulnerability (DP_ID1), session administration (DP_ID2), signature violation analysis (DP_ID3), statistical analysis (DP_ID4), correspondence by violated event (DP_RES), and traffic statistics generation (DP_TRA).

Functional Requirements Satisfied: FIA_ATD.1(1), FIA_UID.2(1), FPT_RVM.1

6.1.2.2 Packet Filtering (DP_FLT)

The packet passing through the packet data contraction & identification (DP_GET) is inputted as the packet filtering (DP_FLT) and checks the packet
filtering rules. Those rules define the information flow control policy of the entire TOE. The packet filtering policy executes the following policies by packet departure (IP address, port), destination (IP address, port) and protocol.

- Allow
- Deny

This function is executed with the proper information (departure address, destination address, protocol, port No.) passing through the evaluated product. It decides whether allowing the affected packet or not based on this information. The following is the items configuring the packet filtering security policy.

- Policy Identifier (ID)
- Departure (IP Address & Port)
- Destination (IP Address & Port)
- Protocol
- Policy (Deny or Allow)
- Existence & Nonexistence of Leave Audit Data (Leave, Not Leave)

This evaluated product can decide the existence & nonexistence of the audit data generation for the violated packet through the packet filtering security policy. When generating the audit data, the data can be generated by transferring the affected packet information to the correspondence by violated event (DP_RES).

The policy set in the packet filtering security policy operates in the top-down form. The top level policy has the most priority and the rest priorities go on sequentially

All basic packet filtering security policies are denial policies. Or, all network packets are blocked.

Functional Requirements Satisfied: FDP_IFF.1(1), FDP_IFC.1(1)

6.1.2.3 Protocol Vulnerability Analysis (DP_ID1)

The packet allowed by the packet filtering (DP_FLT) security policy is inputted in the protocol vulnerability analysis. The analysis provides the function of performing the vulnerability analysis through the protocol header analysis of the network packet.
The analysis provided this function is as follows.
IP

- Backdoor Q: When the departure IP is 255.255.255.0

TCP

- Trace route: When the value of ttl field is 1
- Land Attack: When the IP of the departure and destination is the same
- Illegal Control flag: When abnormal TCP control flag is set

UDP

- Trace route: When the value of ttl field is 1

ICMP

- Trace route: When the value of ttl field is 1
- Overflow: When the length of the packet is abnormally long

When detected as the policy violation, as mentioned above, transfer the affected packet & packet data contraction information to the correspondence by violated event (DP_RES). The correspondence by violated event executes works of blocking the packet and leave log according to the set point of the intrusion prevention policy.
This function also provides the function of reassembling the IP packet which is fragmented. The reassembled packet information is transferred to the session administration (DP_ID2) or signature violation analysis (DP_ID3)).

Functional Requirements Satisfied: FDP_IFC.1(2), FDP_IFF.1(2)

6.1.2.4 Session Administration (DP_ID2)

Of packets which are not violated through the protocol vulnerability analysis (DP_ID1), The TCP packet input the packet information as the session administration (DP_ID2). The rest UDP & ICMP packets are transferred to the signature violation analysis (DP_ID3).
When the inactive period lasts longer than the time set in the TCP session time out, the authorized administrator forcibly end the affected session for the TCP session passing through this evaluated product in this function.

The TCP session administration is done by using the HASH algorithm, the mass data administrative algorithm. This function includes the function of reassembling the TCP packet that is segmented. The following services are reassembly services.

- HTTP Service

- TELNET Service
- FTP Service
- SMTP Service
- POP Service

Functional Requirements Satisfied: FTA_SSL.3

6.1.2.5 Signature Violation Analysis (DP_ID3)

The TCP packet passing through the UDP, ICMP packet and session administration which are not violated in the protocol vulnerability analysis (DP_ID1) is inputted as the signature violation analysis (DP_ID3) for checking the attack pattern. This function checks whether the data information of the packet matches or includes the security attribute of the attack rules of the attack packets in the intrusion prevention security policy.

The signature violation analysis (DP_ID3) is processed by classifying the packet into TCP, UDP and ICMP by protocol.

The ICMP signature violation analysis executes the analysis of smurf, nmap ping, icmp id for the ICMP packet first and classifies the passed packet into ICMP PING & ICMP PING REPLY to check the signature pattern by affected category.

The TCP & UDP signature violation analysis executes the two phases of fragmenting according to the defined criteria in every protocol after classified into the service protocol based on the destination port of the TCP & UDP packet. After deciding the scope and characteristics of the signature to be analyzed in such a way, the signature pattern check and hardcode check are executed by affected group.

This evaluated product provides the custom signature function. The pattern checkup function is also provided for the detection signature defined by the administrator.

Functional Requirements Satisfied: FDP_IFC.1(2), FDP_IFF.1(2)

6.1.2.6 Statistical Analysis (DP_ID4)

The statistical analysis function is the function of detecting intrusions like DOS or

Scan and provides the function of deciding & detecting the existence and nonexistence of the intrusions with a help of the statistical mechanism.

The statistical analysis is carried out for the packet finishing the signature violation analysis (DP_ID3) while using the threshold to detect.

- SYN Flooding Check
  - When there are more SYN packets than those set by the administrator during the time set by the authorized administrator for a destination address
- UDP, ICMP Flooding Check
  - When there are more packets than set by the authorized administrator as packets (UDP, ICMP) from the same departure are inputted in the same destination address.
- Port scanning
  - There are more attempts of port access than set by the administrator during the time set by the authorized administrator at the same departure.

The threshold consists of number & time and contains the contents of detecting when exceeding the certain number for a certain period of time.

Functional Requirements Satisfied: FDP_IFC.1(2), FDP_IFF.1(2), FRU_RSA.1

6.1.2.7 Correspondence by Violated Event (DP_RES)

The function of correspondence by violated event (DP_RES) is in charge of the action for the case that the packet violating the intrusion prevention & packet filtering policy is detected.

The following functions are provided.

- Leave Audit Data
- Leave Detailed Log
  - Leave the entire affected packets as audit data
- Packet Blocking
  - Block the flow of the affected packet.

When generating the audit data, the following items are at least left.

- Generation Time
- Violated Event No.
- Departure IP
- Departure Port
- Destination IP
- Destination Port
- Protocol No.

Functional Requirements Satisfied: FAU_GEN.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2)

6.1.2.8 Traffic Statistics Generation (DP_TRA)

The network packet inputted as the evaluated product generates the traffic statistics data.

The traffic statistics data executes the packet in the network identified in the packet data contraction & identification (DP_GET)

The traffic statistics are collected as the following items.

- Network Protocol Type
- Network Service Type
- TCP/UDP by Session
- IP by Address
- TCP by Flag
- Frame by Size
  - The statistics are generated by length of the network packet.

The traffic statistics data is generated with an unit of 1 min., 5 min., 1 hour, and 1 day.

Functional Requirements Satisfied: FAU_GEN.1

6.1.2.9 Anomalous Symptom Detection (DP_ANM)

The threat condition for the network is very important in the security event. It is difficult to tell the threats for the network by looking at the intrusion event alone.

Thus, the anomalous symptom analysis function shall discriminate the anomalous symptoms by the 2nd analysis of the intrusion event trend or the analysis of the network traffic by using the traffic threshold.
The use of the anomalous symptom analysis can quickly detect the threats occurring in the network operation and allows you take an correspondent action based on the result of analyzing the relative contents.

Anomalous Detection Items are as follows

Category	Item	Description
Traffic Threshold	Permanent Threshold	Way of Users inputting the threshold directly Consistent setting without time
	Profile Threshold	Use of the threshold by making different thresholds by time slot as the profile.
Event Delta	Count Change	Setting of changed ranks by comparing the ranks with the 5-min. time frame.
	Rank Change	Setting of the changed counts by risk based on the comparison of the accounts with the time frame of 5 min.
		Setting of the increased traffic (bps) by risk based on the comparison of harmful traffic by even with the time frame of 5 min.

Functional Requirements Satisfied: FAU_SAA.1

6.1.2.10 Threat Level Evaluation (DP_THR)

TESS TAS Manager estimates the network threat level through the log generated by the protocol vulnerability analysis of TESS TAS Sensor, signature violation analysis, and statistical analysis. The estimated threat level notifies the administrator changes in the threat level through the corresponding threats like emergent alarm display, visible aural, e-mail transfer, and SMS transfer.

Functional Requirements Satisfied: FAU_SAA.1

6.1.3 Identification & Authentication (IA) Function

All security functions provided in this product are supplied by the authorized administrator. Functions like every kind of policy setting & inquiry, audit log inquiry, etc. are provided by the authorized administrator. The function which shall identify such an authorized administrator is the identification & authentication function. In order to execute such functions, the TOE identifies and certifies whether they are authorized through the administrative interface when there are attempts to access to the TOE. The crypto is encrypted through SEED. The identification & authentication function broadly consists of identification & authentication, authentication failure.

- Identification & Authentication (IA_UID)
- Authentication Correspondence (IA_RES)

6.1.3.1 Identification & Authentication (IA_UID)

The identification & authentication function executes the identification & authentication function based on the user identification information and authentication information inputted by the administrator. Only changed values are stored by using the SEED MAC (Message Authentication Code) without storing the secret authentication data.

The administrator of this evaluated product shall pass through the administrator identification & authentication by using the ID & password in the console to access to the security function provided by the evaluated product. When the administrator input the ID and password, the ID is compared with the one in the password file to identify the user and the inputted password is hashed by using the SEED MAC to compare it with the hashed authentication information stored in the password file.

The password of users encrypts the extracted hash value as the key of the SEED encryption algorithm after extracting the hash value by using the SHA-256 algorithm. Thus, the key used for the encryption is not internally stored.

When the user inputs the Administrator ID and Password to get the administrator authentication, this function regards the ID as the identifier and brings the attribute value (password, condition setting value, authentication failure count, authority) of the affected administrator.

The user shall pass through the process of the user identification & authentication before using all security functions provided in this evaluated product.
Only the authorized administrator who passes through the identification & authentication can access but the administrator can access to the audit data as he/she login TESS TAS Console which is correlated with the identification & authentication process of DBMS.
The function of deleting and modifying the stored audit record is not provided. The audit record is securely managed by DBMS and prevents the unauthorized deletion and modification.
The following shall enumerate the rules of ID & password used in this evaluated product.

- ID Input Rule
  - ID shall be the combination of minimum 6 letters of English and figure.
- Password Input Rule
  - Password shall be the combination of 6~15 letters of English and figure (including special characters)
  - Password is displayed as "*" to protect the data

The information on the authentication result displays only the authentication success or authentication failure. In case of the authentication failure, the detailed information on the authentication failure (ID or password failure) is not displayed.

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

6.1.3.2 Authentication Correspondence (IA_RES)

When the administrator authentication fails, the following actions are taken in case of more failures than set by judging the authentication failure account (Default 3. Scope:1~10).

- Prohibition of Permanent Use of the Affected ID
  - Permanently prohibit the use of the affected ID.
- Affected ID Authentication Delay

- Forbid the use of the affected ID for a min.

The locked account can be unlocked by only the administrator with the account administrative authority out of the primary or secondary administrators. The account lockout of the primary administrator can't be unlocked.

The authentication failure count can be set by only the administrator who has the policy setting administration out of the primary & secondary administrators.

Functional Requirements Satisfied: FIA_AFL.1, FMT_MTD.2

6.1.4 Security Administrative (SM) Function

The security administrative function of the TOE system is provided through the GUI of the console. It provides the following detailed functions.

- Administrator Account Administration (SM_ACC)
- System Audit Data Reaction Administration (SM_ADT)
- Signature List Administration (SM_SIG)
- Packet Filtering Policy Administration (SM_FLT)
- Integrity Administration (SM_INT)
- Manager Environment Setting Information Administration (SM_MAN)
- Anomalous Symptom Policy Administration (SM_ANM)
- Host Administrative Policy (SM_HST)

6.1.4.1 Administrator Account Administration (SM_ACC)

The administrator account administration manages the works like the addition, deletion, and alteration of accounts. The account addition can be done by the administrator who received the authority assignment by account. The administrator account can be managed by only the administrator with the account administrative authority out of the primary & secondary administrators.

The following shall enumerate the authorities given to the administrator of this evaluated product.

Authority	Description

Policy Setting	Refers to the authority which can all security policies of this evaluated product
Audit Data Inquiry	Refers to the authority of the inquiry & retrieval of the system audit data, and system resource audit data including the intrusion detection & blocking audit data
Report	Refers to the authority of the generation & inquiry of every kind of intrusion detection and blocking report
System Audit Data Inquiry	Refers to the inquiry & retrieval of the system audit data
Account Administration	Refers to the authority of the addition, deletion, and alteration of the administrator account

The evaluated product provides the administrators by classifying them into the primary & secondary administrator. The following shall enumerate authorities by administrator.

Item	Description
Primary Administrator	Impossible to delete the administrator account input at the time of the system installation. Possible to access to all security functions provided by the TOE. This administrator account is the primary administrator account and can add/delete the secondary administrator account after the login.
Secondary Administrator	The account added by the primary administrator. The account added by the secondary administrator with the account authority. The account can be duplicated for the 5 authorities described above

The administrator account configuration consists of the minimum items as follows

- User ID
- Password
- Name
- Cellular Phone No.
- Mail Account

- Authority Information

The setting of the authentication failure account for the account locking function for the failed authentication attempts is confined to the primary administrator or the second administrator with the policy setting authority.

The administrator account list is confined to the primary administrator or the second administrator with the account information authority. In the account list, the account configuration list described above is displayed and password here is protected as “*”.

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

6.1.4.2 System Audit Data Reaction Administration (SM_ADT)

The audit reaction administration manages the function of managing the reaction setting for the audit log. The setting items are as follows

- Reaction Generation Threshold
  - The setting unit of the threshold is set as the generation count per 1 min.
- Reaction Type Selection
  - Emergent Alarm
    - Generate the alarm message through TESS TAS Console
  - Visible Aural Message
    - Generate the message box with the siren in TESS TAS Console
  - Registered Program Execution
    - Execute the already registered program
  - Mail Transfer
    - When registering the administrator account, transfer the e-mail to the registered e-mail account.
  - SMS Transfer
    - When registering the administrator account, transfer the SMS message to the registered cellular phones

This function can be amended by only the administrator with the system audit data authority out of the primary or secondary administrators.

Functional Requirements Satisfied: FMT_SMF.1, FMT_MTD.1(3)

6.1.4.3 Signature List Administration (SM_SIG)

It manages the detection signature list which is the base of the intrusion detection and allows the user to take an effective counteraction for the network intrusion through the reaction setting administration after the detection. It consists of the reaction setting administration of the detection signature, custom signature administration, and detection exceptional policy administration in the intrusion violation event list.

The detection signature list administration can set the detection reaction by each detection signature list. The following is the enumeration of the setting items.

- Detection Threshold Setting Modification
  - Set it in the form of the generation count/min.
- Leave Log Setting Modification
  - Leave Audit Data
  - Leave Detailed Log (Packet Info.)
  - Session Log
    - TCP Session Data Logging
- Possible Screening Setting Modification
  - Packet Screening
- Possible Use Setting Modification
  - Possible Detection of Affected Signature

The following detection list is included in the detection signature list. The contents of the detection threshold setting can be changed as the contents are given to the administrator for such a detection list.

- All Intrusion Detection by Using Attack Patterns
- Backdoor Q(Query)
- Trace route(Query)
- Land Attack(Query)
- Illegal Control flag(Query)

- Overflow(Query or Threshold Change)
- Port scanning(Query or Threshold Change)

This function provides the item configuring the detection signature for the administrator in a detailed manner.

- Possible to Inquiry & Modification to the Name of Attack Patterns
- Possible to Inquiry & Modification to Risk (High, Low, Medium) of Attack Patterns
- Provide Only the Inquiry of the Protocol of Attack Patterns
- Provide Only the Inquiry of the Service (Port) of Attack Patterns
- Provide Only the Inquiry of the Application Protocol Command of Attack Patterns
- Possible to Inquiry & Modification to the Pattern Character String of Attack Patterns
- Provide Only the Inquiry of Capitalization Separation of Attack Patterns
- Provide Only the Inquiry of Start Point (Data Size) of Attack Patterns
- Provide Only the Inquiry of End Point (Data Size) of Attack Patterns
- Provide Only the Inquiry of the Packet Size (Byte) of Attack Patterns

This function provides the function of adding/deleting/modifying the custom signature defined by the administrator. To meet the various demands of the user, the setting rules are provided in the form of snort rule. The reaction to the set signature is applied in the same way of the detection signature list setting item defined above. The custom signature consists of the following items.

- Signature Name: Signature Name Inputted by the Administrator
- Risk: Select it among high, low, and medium. The default is medium.
- Signature ID: The Identifier automatically given in the evaluated product can not be changed
- Rule, Technology: Describe the detection pattern

This evaluated function can deny the generation of a specific detection event by applying the exception process polity for the security violation event detected by the detection signature. The detection exception policy is applied by the intrusion prevention policy for the detected events alone. The setting items of the detection exception policy are as follows.

- Signature Type (Default: Any)

- Destination (IP Address, Port) (Default: Any)
- Departure (IP Address, Port) (Default: Any)
- Protocol (Default: Any)
  - Select among TCP,UDP,ICMP,IP
- Virtual Network Identifier (Default: Any)
  - Refer to the virtual network that packets belong to

In this function, the function of updating the online/offline signature list is provided. The online signature list update supplies the function of applying the evaluated product through the download of the up-to-date intrusion detection pattern by accessing to the remote signature update server while the offline signature list update function is the function of letting the administrator choose the signature list provided in the form of a file.

Such technologies described above can be modified, amended and inquired by only the primary administrator or the secondary administrator with the policy setting authority.

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

6.1.4.4 Packet Filtering Policy Administration (SM_FLT)

It is the function of managing the policy to execute the packet filtering function and manages the policy as the following items.

- Departure (IP Address, Port) (Default: any)
- Destination (IP Address, Port) (Default: any)
- Protocol (Default: any)
  - Select among IP, TCP, UDP, ICMP
- Action (Default: Allow)
  - Select one of deny/allow
  - When choosing deny, the affected packet is blocked.
- Log (Default: Off)
  - When the affected policy violation is generated, select one of Leave

Log & Off as the filed deciding whether the audit data is left or not

When adding the new packet filtering policy, the TOE provides the default value presented above. The administrator can change it out of items above by the selection.

The packet filtering security policy has a top-down architecture, the policy on the top has the priority and the rest priorities go on sequentially. The administrator can change the priority by up/down the policy.

. When the packet filtering policy is not set, all denial policies are applied. In other words, all network packets are denied and blocked. At this time, the security audit data is not generated.

Those functions described above can be modified, amended and inquired by the primary administrator or the secondary administrator with the policy setting authority.

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

6.1.4.5 Integrity Administration (SM_INT)

The integrity administration (SM_INT) provides the administrative function for the integrity function, a way of ensuring that the evaluated product securely executes the security function. It provides the following the administrative items.

- Integrity Check Time Setting
  - When the system begins, check the integrity
  - Periodically check the integrity
    - ◆ The cycle of the integrity check can be set by the administrator per minutes.
- Integrity Check Item Setting
  - Integrity check list setting of TESS TAS Sensor
  - Integrity check list setting of TESS TAS Manager
  - Integrity check list setting of TESS TAS Console

This function can be modified, amended and inquired by the primary administrator or the secondary administrator with the policy setting authority.

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

6.1.4.6 Manager Environment Setting Information Administration (SM_MAN)

The manager environment setting information administration provides the GUI including the alteration & inquiry of the configuration value need for driving the manager system. The following settings are provided.

- Physical System Setting
  - Physical Sensor Setting
  - Firewall Reaction Information Setting for the Firewall Reaction
- Logical System Setting
  - Virtual Sensor Setting
  - Virtual Network Setting
- Locking Time Out Time Setting for the Screen Locking Function (1~60 min.)
- Update Server Registration & Automatic Signature List Update Cycle Setting for Automatic Signature List Update
- Automatic & Manual (Offline) Signature Update Execution
- NTP Server Registration & Possible Time Synchronization Function Size Setting for Time Synchronization
- DB Backup & Recovery
- Backup List & Backup Cycle Setting for DB Backup
- TCP Session Time Out Value Setting (Default 30 min.)
- E-mail Server Registration for E-mail Reaction

This function can be modified, amended and inquired by the primary administrator or the secondary administrator with the policy setting authority.

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

6.1.4.7 Anomalous Symptom Policy Administration (SM_ANM)

It provides the function of setting the policy for detecting the anomalous symptoms. The policy lets the administrator set the absolute threshold while providing the way of using the 1-hour-unit profile.

- Direct Setting by Administrator
- Setting by Using Profile

The setting by using the profile is the method of using the detection & traffic information used before and generates the profile based on the data generating the statistics per 1 hour.

This function can be modified, amended and inquired by the primary administrator or the secondary administrator with the policy setting authority.

Functional Requirements Satisfied: FMT_MTD.1(1), FMT_SMF.1

6.1.4.8 Host Administrative Policy (SM_HST)

The host administrative policy is the function of intensively managing the designated IT entity (host) and letting the administrator know the detection events generated in the affect host or the detection events flowing into the affected host when they happen.

The host administrative policy consists of the administrative host policy and harmful host policy.

- Administrative Host: It refers to the object that the network packet flows into and notices the administrator the intrusion detection in the affected IP by using the destination IP of the intrusion detection events when the intrusion actually happens.
- Harmful Host: It refers to the subject generating the network packet and lets the administrator know the intrusion detection in the affected IP by using the departure IP of the intrusion detection event when the intrusion actually happens.

There are following kinds of notices.

- Real-Time Notice
  - Real-time notice function for all administrators connected to the console. The content of the audit data is displayed in the window of TESS TAS.
- SMS Transfer
  - Transfer the SMS message to the cellular phone of the administrators registered in the administrator account
- E-mail Transfer
  - Transfer the e-mail to the e-mail account of the administrators registered in the administrator account.
- Visible Aural Notice
  - Generation of the message box along with the siren for the visible audible notice to all administrators connected to console

This function allows only the primary administrator & secondary administrator with the policy setting authority to change the setting and see the contents of it.

Functional Requirements Satisfied: FMT_MTD.1(1), FMT_SMF.1

6.1.5 TSF Protection (PT) Function

The TSF protection function provides the function of checking whether major components of the TOE system operated in the system are normally operating periodically to show the correct operation of the TOE at the time of the initial starting and at the request of the authorized users.
For this, the TOE provide the function of the health check and integrity check.

- Health Check (PT_HCH) Function
- Integrity Check (PT_INT) Function
- Time Synchronization (PT_TSN) Function

6.1.5.1 Health Check(PT_HCH) Function

It checks whether major components of the TOE system are normally operating. The

check lists are as follows.

- Process check configuring the sensor system
- Process check configuring the manager system
- CPU, HDD, Memory utilization of the sensor system
- CPU, HDD, Memory utilization of the manager system
- DB table space utilization
- Connection status check between sensor/manager
- Restart at the time of abnormal action of sensor/manager process

The TESS TAS provides the following functions so as to maintain the function in spite of the following failures

- Software Failure: The monitor process, the one of configuration components of TESS TAS Sensor reruns processes at the time of abnormal operation (halt) by periodically the status of other processes of TESS TAS Sensor. TESS TAS Manager also reruns and detects the abnormal operation (halt) of processes configuring TESS TAS Manager through the monitor process.
- Network Failure: The status check message is received and sent between TESS TAS Sensor and TESS TAS Manager periodically. When the message is not received or sent due to the network failure, the audit record is done and the authorized administrator can know this.
-

When the communications with the TOE is impossible due to the failures above, the administrator can use the system console to execute the administrative actions like the network settings.

TESS TAS Manager periodically (per 1 min.) generates the audit data by checking the DB table space. When the table space exceeds over maximum 80%, the audit data is generated whenever there is a 5% increase by generating the audit data noticing the shortage of the audit data stores. When the audit data is saturated, additional recording of the audit record is ignored while old audit table is getting removed according to the settings. The administrator can know about the status of the stores through the administrator alarm function of the audit data reactions (AT_RES) after generating the audit data.

This function provides the function of periodically checking TESS TAS Sensor, TESS TAS Manager and the communication status. At the time of the initial drive, TESS TAS Sensor automatically attempts to link the communication to TESS TAS Manager. When no connection is made, attempts to connect are made once a min. During the connected status, the message (alive message) is transferred to check the channel connection status once per 3 sec. When no message is arrived, TESS TAS Manager ends the affected communication channel and generates the security audit. When there is anomaly in the communication linkage between TESS TAS Sensor and TESS TAS Manager, the administrator can execute the check action of the network condition by using the system console of TESS TAS Sensor.

The TSF maintains the security zone to execute the TSF itself from the interference and breach of the unauthorized subject through the health check function.

Functional Requirements Satisfied: FAU_STG.3, FAU_STG.4, FPT_FLS.1, FRU_FLT.1, FPT_AMT.1, FPT_SEP.1

6.1.5.2 Integrity Check (PT_INT) Function

The integrity check function provides the function of checking and generating the integrity of every kind of TSF data configuring the TOE. The integrity check function proceeds with the integrity check of EXE files & configuration files needed for the execution of each TSF at the time of the TOE start-up while the TSF is executed when safety is found.

The integrity check criteria goes for the check at the time of the system drive or at the request of the administrator according to the schedule. The check results are stored in the form of the system audit data.

The integrity check goes for the implementation by using the SHA-256 hash algorithm. The hash value for the integrity check target is generated by using the SHA-256 and is managed. When there is a request for the check, judge the possible conformity by comparing the hash value being managed after generating the hash value for the check target. When the hash values are the same, the integrity is decided not to be

compromised. When they are not the same, the integrity is judged to be compromised.

The hash value generation time for the integrity check is generated at the time of the initial drive after the first installation. The hash value is automatically generated when the check items are changed by the administrator (changes in accordance with the policy change). Also, the administrator can directly generate the hash value.

Integrity check targets are as follows.

- TSF Data (Configuration File)
- TSF EXE Code

This function allows only the primary administrator & secondary administrator with the policy setting authority to change the setting and see the contents of it.

Functional Requirements Satisfied: FPT_TST.1, FMT_SMF.1, FMT_MOF.1(2)

6.1.5.3 Time Synchronization (PT_TSN) Function

Major components configuring the TOE system has the same time value as they are given the secure Timestamp while executing the security function and secure the audit record.

The TOE is given the Timestamp from the secure the NTP server. When no Timestamp is provided, the TOE synchronizes the time of the TOE system based on the OS time of the TESS TAS Manager system.

The TOE is the NTP client which is the secure external IT entity. The TOE is using RFC 1305 NTP to set the time of the TOE.

The administrator sets the NTP server registration and synchronization cycle.

Functional Requirements Satisfied: FPT_STM.1

6.1.6 TOE Access (TA) Function

The TOE system shall protect the TOE during the inactive period of the authorized administrator by locking the session as the system doesn't operate even the administrator access to it. For this, this evaluated product provides the screen locking function.

- Screen Locking Function (TA_SSN)

6.1.6.1 Screen Locking (TA_SSN) Function

The screen locking can be carried out through the console, the mutual entry point between the TOE and administrator. TESS TAS Console without the use of the administrator for a certain period of time halts all functions of the console.

- Policy Setting Function Halt
- Every Kind of Event Inquiry & Retrieval Function Halt

The time reference for the screen locking is set by the administrator with the unit of 1~60 min. This is provided in the manager configuration information administration (SM_MAN)

The administrator can access to the security function of the TOE after passing through the reauthentication process of the administrator after locking the screen. The functions provided after the screen locking are as follows

- Administrator Reauthentication
  - Provide the reauthentication function using the password of the affected administrator
- TESS TAS Console End
  - End Process

Functional Requirements Satisfied: FTA_SSL.1

6.1.7 Trusted Path/Channel (SP)

The trusted path provides the function of certifying the manager sensor & console as well as of protecting the data.

- Authentication between Tiers (SP_UID)

- Transfer Data Protection (SP_SSL)

6.1.7.1 Authentication between Tiers (SP_UID)

TESS TAS, the 3 tier architecture, consists of TESS TAS Manager, TESS TAS Console, and TESS TAS Sensor. Among these, TESS TAS Manager plays the role of the server while TESS TAS Console and TESS TAS Sensor become the client for the communication. The communications with the live update server is implemented in TESS TAS Manager and TESS TAS Manager plays the role of the client to implement the communications. The communications with DBMS is implemented in TESS TAS Console and TESS TAS Manager while DBMS plays the role of the server. The authentication & communication data encryption between each tier is using the SSL protocol, SSLv3(Secure Socket Layer version 3).
In the process of the SSL communications, the authentication between the server and client is the mutual authentication method using public key/ private key of 1024 bit generated by the RSA public key algorithm.
The authentication is implemented by certificating and exchanging the public key certificates generated by the RSA algorithm. The certificate digests (hash generation) the message with SHA-256 to assure the integrity after the signature with the Private Root CA private key of TESS TAS. The signed private key of Root CA is used once to sign the certificate when installing the product and is discarded to rid the risk of stealing. The other party can be confirmed by certifying the digital signature of the party's certificate. However, the communication channel is not established for the secure communication when either party fails to be certified.

Functional Requirements Satisfied: FTP_ITC.1, FPT_ITT.1

6.1.7.2 Transfer Data Protection (SP_SSL)

TESS TAS, the 3 tier architecture, consists of TESS TAS Manager, TESS TAS Console, and TESS TAS Sensor. Among these, TESS TAS Manager plays the role of the server while TESS TAS Console and TESS TAS Sensor become the client for the communication. The communications with the live update server is implemented in TESS TAS Manager and TESS TAS Manager plays the role of the client to implement the communications. The communications with DBMS is implemented in TESS TAS

Console and TESS TAS Manager while DBMS plays the role of the server. The authentication & communication data encryption between each tier is using the SSL protocol, SSLv3(Secure Socket Layer version 3).

In the SSL data communication, the data encryption is using the AES method and the message digest for the integrity is using the SHA-256 hash-based message authentication code (HMAC) method. The SSL proto치 can prevent the reuse of the data by encrypting the data through the generation of arbitrary session key set by session.
The sended side tier encrypts the data and HMAC key which are compressed as AES after generating the SHA-256 hash along with the HMAC key and compressing the data. When the SHA-256 hash and encrypted data are transferred, the sended side tier decodes the AES-encrypted data & HMAC key and generates the hash before comparing them with the transferred hash. After the check, the compressed data is recovered as plaintext to use.
Functional Requirements Satisfied: FTP_ITC.1, FPT_ITT.1

6.2 Assurance Measures

This paragraph describes the assurance measures of the TOE. The assurance measure which is the means to satisfy the assurance requirements is described in the assurance measures list.

Assurance Class	Assurance Component		Assurance Measures
Configuration Administration	ACM_AUT.1	Partial Configuration Administrative Automation	TESS TMS v4.5 Configuration Administrative Document
	ACM_CAP.4	Generation Support & Claim Procedure	
	ACM_SCP.2	Scope of Issue Tracking Configuration Administration	
Delivery & Operation	ADO_DEL.2	Detection of Modification	TESS TMS v4.5 IGS
	ADO_IGS.1	Installation, Generation, Start-up Procedure	TESS TMS v4.5 Installation Manual
Development	ADV_FSP.2	Completely Defined External Interface	TESS TMS v4.5 FSP
	ADV_HLD.2	Basic Design Separating Security Function & Non-Security Function	TESS TMS v4.5 HLD
	ADV_IMP.1	Implementation Representation for the Partial TSF	TESS TMS v4.5 IMP
	ADV_LLD.1	Described & Detailed Design	TESS TMS v4.5 LLD
	ADV_RCR.1	Non-Standardized Conformity Verification	TESS TMS v4.5 FSP, TESS TMS v4.5 HLD, TESS TMS v4.5 LLD, TESS TMS v4.5 IMP
	ADV_SPM.1	Non-Standardized TOE Security Policy Model	TESS TMS v4.5 SPM
Guidance	AGD_ADM.1	Administrator Guidance	TESS TMS v4.5 ADM
	AGD_USR.1	User Guidance	-
Life Cycle Support	ALC_DVS.1	Identification of Security Policy	TESS TMS v4.5 Life Cycle Support Document
	ALC_LCD.1	Life Cycle Model Defined by Developer	
	ALC_TAT.1	Well Defined Development Tools	
Test	ATE_COV.2	Analysis of Test Scope	TESS TMS v4.5 Functional Test
	ATE_DPT.1	Basic Design Test	
	ATE_FUN.1	Functional Test	
	ATE_IND.2	Independent Test: Sample Test	
	AVA_MSU.2	Verification of Guidance Analysis	TESS TMS v4.5 MSU

[Table 6-2] Assurance Measures

The assurance component for the configuration administration, ACM_AUT.1 partial configuration administrative automation, ACM_CAP.4 generation support & claim procedure, and ACM_SCP.2 issue tracking configuration administrative scope can be assured by the TESS TMS v4.5 configuration administrative document.
The detection of modification to ADO_DEL.2 of delivery & operation class is assured by the TESS TMS v4.5 IGS while ADO_IGS.1 installation, generation, start-up procedure are assured by the TESS TMS v4.5 installation manual.
ADV_FSP.2 completely defined external interface of the development class is assured by the TESS TMS v4.5 FSP. The basic design separating ADV_HLD.2 security function and non-security function is assured by the TESS TMS v4.5 HLD.
The implementation representation for the partial ADV_IMP.1 TSF is assured by the TESS TMS v4.5 IMP.
ADV_LLD.1 described & detailed design is assured by the TESS TMS v4.5 LLD. ADV_RCR.1 non-standardized conformity verification is assured by the TESS TMS v4.5 HLD, TESS TMS v4.5 LLD, TESS TMS v4.5 FSP and TESS TMS v4.5 IMP.
ADV_SPM.1 non-standardized TOE security policy model is assured by the TESS TMS v4.5 SPM. AGD_ADM.1 ADM of the guidance class can be assured by the TESS TMS v4.5 ADM. AGD_USR.1 USR is not applied here as extra users but administrators are not classified.
The identification of ALC_DVS.1 security policy of the life cycle support class, life cycle model defined by ALC_LCD.1 developer, and ALC_TAT.1 well defined development tools are assured by the TESS TMS v4.5 life cycle support document.
The analysis of ATE_COV.2 test scope of the test class, ATE_DPT.1 basic design test, ATE_FUN.1 functional test, ATE_IND.2 independent test: sample test are assured by the TESS TMS v4.5 FT.
The verification of AVA_MSU.2 guidance analysis of the vulnerability analysis class is assured by the TESS TMS v4.5 MSU. The evaluation on the AVA_SOF.1 TOE security functional strength and AVA_VLA.2 independent VLA are assured by the TESS TMS v4.5 VLA.

7 PP Claims

This chapter describes the claimed PP and identifies the objectives and requirements that PP doesn't not have.

7.1 PP Reference

The ST claims the Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005. Korea Information Security Agency)

7.2 PP Tailoring

The tailoring contents can be confirmed below.

Identification	Object	Tailoring Contents
FAU_ARP.1	[The list of correspondent action to minimize the confusion {caused by the writer of ST}]	[SMS transfer to the authorized administrator, E-mail transfer, visible aural notice, real-time notice, custom program execution]
FAU_GEN.1	[Assignment: *Specially defined auditable event*]	[[Table 5-3] Additional Auditable Events]
	[Assignment: Other Audit-related information]	[**[Table 5-3]** Reference to the auditable event, The following information on the auditable event] ● Traffic Volume (bps, pps) ● Attack Count & Damage Count ● Object Identity (Destination IP Address, Port) ● Number of Attackers & Victims

FAU_SAA.1	[Assignment: *Subset of defined auditable events*	[● Identification & Authentication Security Policy Violation ● Anomalous Symptom Detection Policy Violation ● Intrusion Detection Policy Violation ● Threat Level Policy Violation ● All Faults Detected by the TSF ● Integrity Generation, Check ● Beginning & End of the Security Audit Function ● Security Policy Setting Modification ● Communication Access & Release ● DB Backup & Recovery ● Signature Live Update ● Manager Environment Setting Modification]
	[Assignment: Other Rules]	[None]
FAU_SAR.3	[Assignment: *Criteria for Logical Relations*]	[Criteria for the Following Logical Relations] ● Identity of Subject ● Identity of Object-Selective Provision ● Event Date ● Event Type ● Keyword (Audit Data Contents) ● Traffic Display Criteria (bps, pps)-Selective Provision

	[Selection: *Retrieval, Arrangement, Sequencing*]	*Retrieval*
FAU_SEL.1	[Selection: Object Identity, User Identity, Subject Identity, Host Identity, Event Type]	*Event Type*
	[Assignment: Addition Attribute List for the Basis of the Audit Selection]	[None]
FAU_STG.1	[Selection: *Prevention, Detection*]	*Prevention*
FAU_STG.3	[Assignment: *Defined Limit in Advance*]	[The rest room for the audit store is 80& (Whenever exceeding 5%)]
	[Assignment: *Counteraction Taken When the Audit Storage Failure Is Expected*]	[SMS transfer to the authorized administrator, E-mail transfer, visible aural notice, real-time notice, custom program execution in Preparation for the Expected Audit Loss]
FAU_STG.4	[Selection: Select One of '*Ignoring Auditable Events', 'Prevention of Auditable Events Barring from Actions Taken by the Authorized Administrator with the Special Authority', and 'Oldest Audit Record Overwriting'*]	*Ignoring Auditable Events*
	[Assignment: Extra Actions Taken in Case of the Audit Storage Failure]	[SMS transfer to the authorized administrator, E-mail transfer, visible aural notice, real-time notice, custom program execution]
FDP_IFC.1(1)	[All Denial Policies]	[**Packet Filtering Security Policy**]
FDP_IFC.1(2)	[All Allowing Policies]	[**Intrusion Prevention Security Policy**]

FDP_IFF.1(1)	[Assignment: *List of the Subject & Information Controlled by the Following SF and Security Attribute for Each One*]	[Next] a) Subject Security Attribute: IP Address, Port No. & Protocol No. of the External IT Entity Transceiving the Information through the TOE b) Information Security Attribute: Departure (IP Address, Port), Destination (IP Address, Port), Protocol
	[Assignment: *Information Flow Control SFP*]	[Packet Filtering Security Policy]
	[Assignment: *Relations Based on the Security Attribute to be Maintained between the Subject & Information Security Attribute for Each Operation*]	[IP Address, Port No, & Protocol No of the Traffic (Network Packet) Inputted from the External IT Entity Match or are Included in IP Address, Port & Protocol out of the Security Attributes of the Packet Filtering Security Policy Defined by the Authorized Administrator When the Security Attribute Value of the Packet Filtering Security Policy Is the Permission]
	[Assignment: *Additional Information Flow Control SFP Rule*]	[None]
	[Assignment: *Additional SFP Capability List*]	[None]
	[Assignment: Rules to Explicitly Certify the Information Flow Based on the Security Attribute]	[None]

	a) The TOE shall block the request for the access in case that the information arriving in the external IT entity of the external network has the subject IP address of the internal network at any case. b) The TOE shall block the request for the access in case that the information arriving in the external IT entity of the internal network has the subject IP address of the external network at any case. c) The TOE shall block the access request in case that the information arriving in the IT entity of the external network has the subject IP address to broadcast at any cost. d) The TOE shall block the access request in case that the information arriving in the IT entity of the external network has the subject IP address to loop at any cost. e) The TOE shall block the access request in case that the information arriving in the IT entity of the external network has the abnormal packet architecture at any cost.	[When there is no packet filtering rules set by the authorized administrator barring from the rule basically set]
	f)[{다음과 같은}1개타 규칙]	

FDP_IFF.1(2)	[Assignment: *List of the Subject & Information Controlled by the Following SF and Security Attribute for Each One*]	[Next] a) Subject Security Attribute: IP Address, Port No. & Protocol No. of the External IT Entity Transceiving the Information through the TOE b) Information Security Attribute: Departure Address, Destination Address, Protocol, Packet Header information, Packet Data Information
	[Assignment: *Information Flow Control SFP*]	[Intrusion Prevention Security Policy]
	Allow	**Screening**

	[Assignment: *Relations Based on the Security Attribute to be Maintained between the Subject & Information Security Attribute for Each Operation*]	[The Following Rule] Traffic Check ● When the Protocol of the Traffic (Network Packet) Inputted from the External IP Entity Is TCP While TCP Control Flag Is SYN (Packet Header Information of Information Security Attribute). When the Traffic Is Generated Much More Than the Threshold Set in the Intrusion Prevention Security Policy Made by the Authorized Administrator ● When the Protocol of the Traffic (Network Packet) Generated in the External IP Entity Is UDP, ICMP While having the Same Destination Address among the Information Security Attributes. When the Traffic Is Generated Much More Than the Threshold Set in the Intrusion Prevention Security Policy Made by the Authorized Administrator Attack Pattern Check ● When the Protocol of the Traffic (Network Packet) Generated in the External IP Entity Matches or Is Included in the Packet Data Information Rule of the Intrusion Prevention Security Policy Set by the Authorized Administrator

	[Assignment: Additional Information Flow Control *SFP Rule*]	[None]
	[Assignment: *Additional SFP Capability List*]	[None]
	[Assignment: Rules to Explicitly Certify the Information Flow Based on the Security Attribute]	[None]

	[{Decided by the Writer of the ST}]	[{The Following} Other Rules] IP ● Backdoor Q: When the Departure IP Is 255.255.255.0, the Packet Is Blocked in Case That the Action Is Set to be Blocked among Information Security Attributes. TCP ● Trace route: When the Value of TTL Field Is 1, the Packet Is Blocked in Case That the Action Is Set to be Blocked among Information Security Attributes ● Land Attack: When the IP of the Destination & Departure Is the Same, the Packet Is Blocked in Case That the Action Is Set to be Blocked among Information Security Attributes ● Illegal Control flag: When the Abnormal TCP Control Flag Is Set, the Packet Is Blocked In Case That the Action Is Set to be Blocked among Information Security Attributes UDP ● Trace route: When the Value of TTL Field Is 1, the Packet Is Blocked in Case That the Action Is Set to be Blocked among Information Security Attributes ICMP ● Trace route: When the Value of TTL Field Is 1, the Packet Is
	119	Blocked in Case That the Action Is Set to be Blocked among Information Security Attributes Overflow: 비정상적으로 패킷의 길이 긴 경우이며 정보

FIA_AFL.1	[Assignment: List of Authentication Event]	[Authentication Attempt by Authorized Administrator]
	[Selection: [Assignment : Positive], "Positive in [Assignment: Scope of Allowable Number] That is Configurable by Administrator"	*Positive in [More Than 1 to Less Than 10] Where the Authorized Administrator Can Configure*
	[Assignment: Correspondent Action List]	[Affected User Authentication Prevention, Authentication Delay until the Authorized Administrator Takes a Correspondent Action]
FIA_ATD.1 (1)	{ Decision by the Writer of ST}	{None}
FIA_ATD.1 (2)	{ Decision by the Writer of ST }	{For the Additional Following Items} ● Password ● Status Setting Value (Normal, Locking, Delay) ● Authentication Failure Count ● Authority
FIA_UAU.7	[Assignment: *Feedback List*]	[Success or Denial Message, Password Are Displayed as"*"]
FMT_MOF. 1(1)	[Assignment: *Functional List*]	[The Following Functional List] ● Possible Live Update Use Setting ● Beginning & Halt of Sensor ● Possible Time Synchronization Use Setting ● Possible DB Automatic Backup Use Setting ● Possible Automatic Integrity Check Use Setting
	[Selection: *Decide Action, Modify Halt, Beginning & Action*]	*Halt & Beginning of Action*

FMT_MOF.1(2)	[Assignment : *Functional List*]	[The Following Functional List] ● Live Update at the Request of Authorized Administrator ● Offline Signature Update at the Request of Authorized Administrator ● Activation & Application by Intrusion Detection Signature ● Activation & Application of the Packet Filtering Policy by Item ● DB Backup at the Request of Authorized Administrator ● Integrity Check at the Request of Authorized Administrator
	[Selection: *Decide Action, Modify Halt, Beginning & Action*]	*Decide Action*
FMT_MSA.1	[Assignment: *List of Security Attributes*]	[Next] [Table 5-4] Administration of Security Attribute
	[Selection: *Default Value Modification, Query Modification, Deletion [Assignment: Other Operations]]*	*Query, Modification, Deletion, [Generation]*
	[Assignment: *Access Control SFP, Information Flow Control SFP*]	[Packet Filtering Security Policy, Intrusion Prevention Security Policy]
FMT_MSA.3	[Selection: Select One of *Confined, Allowable, [Assignment: Other Attributes]*]	*Confined*

	[Assignment: *Access Control SFP, Information Flow Control SFP*]	[Packet Filtering Security Policy, Intrusion Prevention Security Policy]
FMT_MTD.1(1)	[Assignment: *TSF Data List*]	[Next] ● Packet Filtering Security Policy ● Intrusion Prevention Security Policy ● Detection Exception Policy ● Anomalous Symptom Policy ● Host Administrative Policy ● Threat Level Policy ● Physical System Setting ■ Physical Sensor Setting ■ Firewall Setting ● Logical System Setting ■ Virtual Sensor Setting ■ Virtual Network Setting
	[Selection: *Default Value Modification, Query, Deletion, Clear, [Assignment: Other Operations]*]	*Query, Modification, Deletion, [{Generation}]*
FMT_MTD.1(2)	[Assignment: *TSF Data List*]	[Identification & Authentication Data]
	[Selection: *Default Value Modification, Query, Deletion, Clear, [Assignment: Other Operations]*]	*Modification, Deletion*

FMT_MTD.1(3)	[Assignment: *TSF Data List*] Authorized Administrator Session Time Out Value (Screen Locking Time Out Value)	[Next] ● Authorized Administrator Session Time Out Value (Screen Locking Time Out Value) ● TCP Session Time Out Value ● Automatic Signature List Update Cycle Value ● Automatic Backup Cycle Value & Item ● Administrator Account Locking Policy ● Time Synchronization Cycle & Server Address Modification ● System Audit Log Policy Modification ● Automatic Integrity Auditable Setting & Audit Cycle Value
	[Selection: *Default Value Modification, Query, Deletion, Clear, [Assignment: Other Operations]*]	*Modification*
FMT_MTD.2	[Assignment: *TSF Data List*]	[Failed Authentication Attempt Count]
	[Assignment: *Correspondent Action to be Taken*]	[Correspondent Action Specified in FIA_AFL.1]
FMT_SMF.1	[Assignment: *Security Administrative Functional List Provided by TSF*]	[The Following Security Administrative Functional List] ● TSF Security Functional Administration ■ Item Described in FMT_MOF.1(Clause 5.1.1.1) ● TSF Security Attribute

		Administration ■ Item Described FMT_MSA.1(Clause 5.1.1.1) ● TSF Data Administration ■ Item Described in FMT_MTD.1(1), FMT_MTD.1(2)(Clause 5.1.1.1) ● Administration of TSF Data Threshold ■ Item Described in FMT_MTD.2(Clause 5.1.1.1) ● Administration of Security Role ■ Item Described in FMT_SMR.1(Clause 5.1.1.1) ● Self Test Setting Administration ■ Integrity Check Result Inquiry ■ Initialization for Integrity Check Object (HASH Data Regeneration)
FMT_SMR.1	[Authorized Administrator]	[Authorized Administrator] ● Primary Administrator ● Secondary Administrator
FPT_AMT.1	[Selection: *Warm Start-up, Periodically during the General Operation, at the Request of Authorized Administrator, [Assignment: Other Conditions]*]	*Periodically during General Operation*

FPT_FLS.1	[Assignment: *TSF Failure Type List*]	[Failure Type List Described in FRU_FLT.1]
FPT_ITT.1	[Selection: Disclosure, Modification]	*Disclosure, Modification*
FPT_TST.1	[Selection: *[Assignment: Segments of TSF Data], TSF Data*]	*TSF Data*
	[Selection: *During Start-up, Periodically during General Operation, at the Time of Requests of Authorized Administrator, [Assignment: Condition of Generating Self-Test], Conditional*]	*During Start-up, Periodically during General Operation, at the Time of Requests of Authorized Administrator*
	[Selection: *[Assignment: Segments of TSF Data], TSF Data*]	*TSF Data*
FRU_FLT.1	[Assignment: *Failure Type List*]	[Software Failure of Daemon Except for Major Daemon, Network Connection Failure between the Partial TOEs]
	[Assignment: *List of the TOE Function*]	[Administrative Action of Using System Console by Administrator]
FRU_RSA.1	[Selection: *Individual IT Entity , Defined IT Entity Group, Subject*]	*Defined **IT Entity** Group*
	[Selection: *Simultaneously, during the Specified Period*]	*During the Specified Period*
FTA_SSL.1	[Assignment: *Inactive Period of **Authorized Administrator***]	[Exceed Administrator's Session Time Out Value Set by **Administrator** (1-60 min., Default 1 min)]
	[Assignment: *Event to Happen*]	[Reauthentication of Administrator]
FTA_SSL.3	[Assignment*: **IT Entity*	[Inactive Period of Authorized

	Inactive Period]	Administrator of the Following Authorized **IT Entities**, { Exceed Number of Session Maximum Assigned Number}] a) When the Authorized Administrator Exceeds Time Out (sec.) Set in the TCP Session Time Out of FMT_MSA.1 b) When the Number of Session of the Authorized IT Entity Exceeds the Number of Session Set by the Authorized Administrator in the Session Confinement of FMT_MSA.1
FTP_ITC.1	[Selection: *TSF, Remote Trusted IT Product*]	*TSF*
	[Assignment: *Functional List Requested for Secure Channels*]	[Signature List Update, Communications with DBMS]

[Table 7-1] PP Tailoring Trail

7.3 PP Additions

The following is the assumptions, body's security policy, and security objective & security requirements that add something else to the PP for this ST

Beside the security objective & security requirements described below, FIA_UAU.1 of the PP is replaced by FIA_UAU.2.

Name	Description
A. Secure TOE External Server	The NTP server and live update server which are the secure TOE external server for the security function provided by the TOE are secure. NTP is used to get the trusted visual information while the live update server is for updating the up-to-date intrusion pattern rules.
A.SSL Certificate	The certificate used in the SSL protocol for the secure communication is generated at the time of the installation and is securely managed.

A.TIME	The IT environment where the TOE is operating receives the trusted Timestamp information from the NTP server or OS directing RFC 1305
A.DBMS	The intrusion detection & traffic data generated in the TOE are stored in DBMS. The stored data is securely managed by the identification & authentication method defined by DBMS itself. DBMS provides the function of the retrieval & inquiry of the stored intrusion detection & traffic data at the request of the administrator. DBMS is securely managed and operated by applying the advanced security & vulnerability-related patch.
P.SSL Certificate Administration	SSL Certificate shall be generated during the installation and shall be securely stored and managed
OE. Secure TOE External Server	NTP designed to maintain the trusted time existing outside the TOE for the TOE function and the live update server whose role shall update the latest attack rules shall be secure.
OE.SSL Protocol	In case of the communication among DBMS, signature live update server, separated partial TOE, the TOE forms the secure communication channel through the SSL protocol based on the certificate provided in the IT environment.
OE.TIME	The IT environment shall provide the trusted Timestamp from the NTP server directing RFC 1305 or the OS.
OE.DBMS	The intrusion detection & traffic data generated in the TOE are stored in DBMS. The stored data shall be securely managed by the identification & authentication method defined by DBMS itself DBMS provides the function of the retrieval & inquiry of the stored intrusion detection & traffic data at the request of the administrator. DBMS is securely managed and operated by applying the advanced security & vulnerability-related patch.

[Table 7-2] Assumptions, Body's Security Policy & Security Objectives

Name	Description
FPT_ITT.1	During the transmissions between data of the TSF, the TOE shall prevent the disclosure & modification from outside by configuring the SSL protocol by calling the SSL function

[Table 7-3] Security Functional Requirements for the TOE Added to PP

Name	Description
FPT_STM.1	The TOE is given the trusted Timestamp from the OS based on the time information set by the administrator and from the NTP server by being operated as the NTP client to maintain the Timestamp.
FAU_SAR.3	The TOE shall be able to retrieve the audit record stored in DBMS by using the DBMS function provided in the IT environment based on the identity of subject, identity of object, event date, event type, audit data contents and traffic display criteria.
FAU_STG.1	The TOE shall protect the stored audit record the unauthorized deletion by using the DBMS function provided in the IT environment while preventing the unauthorized modification.
FPT_ITT.1	During the transmissions between data of the TSF, the TOE shall prevent the disclosure & modification from outside by configuring the SSL protocol by calling the SSL function
FTP_ITC.1	The TOE provides the secure channel by forming the SSL protocol by calling the SSL function provided in the IT environment.

[Table 7-4] Security Functional Requirements for the Environment Added to PP

8 Rationale

This chapter describes the rationale for the security requirements satisfying the security objectives defined by the security environment (threat, assumption, body's security policy).

8.1 Security Objectives Rationale

The security objectives rationale proves that the explicit security objectives are appropriate, good enough to deal with the security issue, and badly needed.

The security objectives rationale proves the following.

Each assumption, threat and body's and security policy are managed by at least one security objective.

Each security objective deals with at least one assumption, threat, and body's security policy.

Security Objectives / Security Environment	O. Availability	O. Audit	O. Administration	O.TSF Data Protection	O. Abnormal Packet Screening	O. DoS Attack Screening	O. Identification	O. Authentication	O. Info. Flow Control	OE. Physical Security	OE. Security Maintenance	OE. Trusted Administrator	OE. Secure Administration	OE. Hardened OS	OE. Single Connection Point	OE. Vulnerability List Update	OE. SSL Protocol	OE. Secure TOE External Server	OE.TIME	OE.DBMS
A. Physical Security										●			●							
A. Security Maintenance											●									
A. Trusted Administrator												●								
A. Hardened OS														●						
A. Single Connection Point															●					
A. Secure TOE External Server																		●		
A. SSL Certificate																	●			
A.TIME																			●	
A.DBMS																				●
T. Masquerade		●					●	●												
T. Down	●			●									●	●						
T. Record Failure	●	●																		
T. Illegal Info Inflow			●						●											
T. Illegal Service Access			●						●											
T. Abnormal Packet Transfer		●			●		●													
T. New Vulnerability Success			●								●		●	●		●				●
T. DoS Attack		●				●	●													
T. Consecutive Authentication Attempt		●					●	●												
T. Bypass Access	●								●	●					●					
T. Spoofing		●			●	●	●													
T.TSF Data Modification	●	●		●			●													

without Permission																			
TE. Poor Administration			●									●	●						
TE. Delivery Installation												●	●						
P. Audit		●					●												
P. Secure Administration			●									●	●						
P.SSL Certificate Administration																●			

[Table 8-1] Security Environment & Security Objective Correspondence

8.1.1 TOE Security Objectives Rationale

O. Availability

When the TOE breaks down or is overloaded by the attacker's attack, the TOE security objective provides the TOE availability for the provision of the minimum network service.

Thus, the security objective ensures the TOE availability to counter T. failure, T. TSF data modification without permission, threats for T. bypass access and T. record failure which is threatening the saturation of audit record storage capacity of the TOE.

O. Audit

When the user is using the security function, the TOE security objective shall record the audit events by user in accordance with the TOE audit record policy. The TOE ensures the provision of the function of securely maintaining and reviewing the recorded audit events. Or, the TOE provides the correspondent function when the audit data reaches the saturation. When there is a replay attack, the audit record generation ensures the detection of the identity of attackers through the audit records. The spoofing attack, DoS attack, and attacks that transfer the abnormal packet can be traced through the audit records.

Therefore, this security objective shall counter T. masquerade, T. record failure, T. abnormal packet transfer, T. DoS attack, T. consecutive authentication attempts, T. spoofing and T. TSF data modification without permission while supporting the security policy p. audit of the body.

O. Administration

The TOE controls the illegal access to the internal network by setting the information

flow control for the execution of the security policy. For this, The TOE shall provide the means of securely managing the TSF data & the TOE including the TOE configuration data generation & administration, latest vulnerability signature administration, etc. Thus, the TOE security objective shall counter T. illegal information flow, T. illegal service access, T. new vulnerability attack and threat of poor TE administration while supporting the security policy P. secure administration of the body by providing the means of securely managing the TOE.

O. TSF Data Protection

When the TSF data cannot identify the administrator due to the unexpected attack from outside or the TOE failure, the security policy can not be normally executed. For this, make sure that the TSF can normally operate by ensuring the integrity of the TSF data through checking whether intentional or unintentional modification to the TOE TSF data is generated.

So, the security objective counters the threat T. failure and T.TSF data modification without permission.

O. Abnormal Packet Screening

Of many packets flowing into the internal network from the external network, this security object ensures that packets not right for the TCP/IP standard, packets with the internal network address among those flowing from the external network, broadcasting packet and looping packet shall not flow into the internal network.

Thus, thshallE security objective shall counter the threat T. abnormal packet transfer and T spoofing.

O. DoS Attack Screening

The attacker can make an DoS attack on the internal computer by passing through the TOE. The representative DoS attack shall deplete the computer resource by abnormally making too many service requests to the internal computer by the remote user. At this time, the internal computer interferes the abnormal user not to use the computer by assigning too many resources to the attacker. In order to prepare for this, the TOE ensures that abnormal users can use the computer by blocking a specific user monopolizing the specific computer resources.

Thus, this security objective counters threat T. DoS attack, and T. spoofing.

O. Identification

There are some cases that the user using the TOE accesses to it by receiving the authentication and the administrator managing the TOE & outsiders (IT entity) pass through the TOE without the authentication to use the internal computer. The two cases need the identification function to manage the security event. The administrator identification function is needed for giving the accountability for all actions used by the administrator. The identification of the external IT is necessary for abnormal packet transfer, DoS attack screening, spoofing attack screening and audit records of the external IT access attempts.

Thus, this TOE security objective shall counter T. masquerade, T DoS attack, T spoofing, T. abnormal packet transfer, T. consecutive authentication attempts, and T. TSF data modification without permission while supporting the P. audit.

O. Authentication

Users who want to access to the TOE shall be certified. But the authentication required at the time of the access to the TOE can be vulnerable to a replay attack launched by outsiders. Thus, the TOE shall ensure the authentication mechanism which can endure the authentication attempt attacks meeting the standard of the outsiders. So, the security objective shall counter T. masquerade, and T. consecutive authentication attempts.

O. Information Flow Control

The TOE is the product of controlling the information flow in accordance with the security policy by being installed where the internal & external networks are separated. This security objective ensures the blocking of various attacks by identifying them which can be generated in the network. The various attacks in the network means the virus attack, e-mail or web service with illegal information and the access to the unallowable service. The TOE ensures the safety of the internal network by preventing it from flowing into the internal network by controlling this according to the rules set.

Thus, the security objective counters the T. illegal information flow, T. illegal service access and T. bypass access threat.

8.1.2 Security Objectives Rationale for the Environment

OE. Physical Security

The security objectives for this environment shall support A. physical security assumptions and counter T. bypass access threat by ensuring that the TOE is installed and operated at a safe place and by protecting the physical attacks from outside and the TOE modification attempts.

OE. Security Maintenance

The security objectives for this environment are necessary for supporting the assumption A. security maintenance and countering threat T. new vulnerability attack as the same level of the security is ensured to maintain as that of the security before by reflecting the changed environment and security policy in the TOE operation policy when the internal network environment is changed due to the internal network configuration change, rise & fall in host & service.

OE. Trusted Administrator

The security objectives for this environment is necessary for supporting assumption A. trusted administrator, and P. secure administrative security policy and countering poor TE administration, TE delivery & installation as it ensures the trusted authorized administrator of the TOE.

OE. Secure Administration

The security objectives for this environment ensures that the TOE is delivered, installed, configured, managed, and used by the administrator in a secure way so that it counters T. failure, T. new vulnerability attack, poor TE administration, threats of TE delivery & installation and supports the assumption A physical security, and body's security P. secure administration.

OE. Hardened OS

The security objectives for this environment gets rid of the service or means that the TOE doesn't need in the OS and executes the hardening work for vulnerabilities in the OS to show that the OS is secure and trusted, which enables it to support assumption A hardened OS and counters threat T. failure, and T. new vulnerability attack.

OE. Single Connection Point

The security objectives for this environment counters the threat T. bypass access and supports assumption A. single connection point by ensuring that the communications between the internal & external network is done through the TOE.

OE. Vulnerability List Update

The security objectives for this environment counters threat T. new vulnerability attack by ensuring the update & administration of the DB for the vulnerability managed by the TOE to protect the internal network resource protected by the TOE from the outsiders taking advantage of the vulnerability.

OE. Secure TOE External Server

The security objectives for this environment supports the Assumption A. secure TOE external server by ensuring that the mutually operated external server is secure for the functions of the TOE.

OE.SSL Protocol

The security objectives for this environment lets the TOE ensure the secure channel by executing the trusted IT entity authentication & cryptographic communication function through the SSL protocol. So, the assumption A. SSL Certificate and P. SSL Certificate are managed.

OE.TIME

The security objectives for this environment ensures the use of the trusted NTP sever for the trusted Timestamp needed for the function of the TOE, which provides the assumption A.TIME.

OE.DBMS

The security objectives for this environment supports the assumption A.DBMS by using the data administrative function in every kind of audit information administration generated by the TOE and counters T. new vulnerability attack as it updates the database for the new vulnerability.

8.2 Security Requirements Rationale

The security requirements rationale proves that the described IT security requirements is good enough to satisfy the security objectives and is proper to deal with the security issues as a result of that.

8.2.1 TOE Security Requirements Rationale

The TOE security requirement rationale proves the following.

Each TOE security objective is managed by at least one of the TOE security requirements.

. Each TOE security objective manages one of the TOE security requirements.

Security Objective / Security Functional Requirements	O. Availability	O. Audit	O. Administration	O.TSF Data Protection	O. Abnormal Packet Screening	O. DoS Attack Screening	O. Identification	O. Authentication	O. Info. Flow Control
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		●							
FDP_IFC.1(1)									●
FDP_IFC.1(2)									●
FDP_IFF.1(1)									●
FDP_IFF.1(2)					●	●			●
FIA_AFL.1								●	
FIA_ATD.1 (1)		●			●	●	●		●

FIA_ATD.1 (2)		●					●		
FIA_UAU.2			●	●				●	
FIA_UAU.7								●	
FIA_UID.2(1)		●			●	●	●		●
FIA_UID.2(2)		●	●	●			●		
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	●		●						
FMT_SMF.1			●						
FMT_SMR.1			●				●	●	
FPT_AMT.1	●			●					
FPT_FLS.1	●								●
FPT_RVM.1									●
FPT_SEP.1				●					●
FPT_STM.1		●							
FPT_TST.1	●			●					
FRU_FLT.1	●								●
FRU_RSA.1						●			
FTA_SSL.1				●					
FTA_SSL.3						●			
FTP_ITC.1				●					
FPT_ITT.1			●	●					

[Table 8-2] Security Objective & Security Functional Requirements Correspondence

FAU_ARP.1 Security Alarm

When detecting the security violation, this component satisfies the TOE security objectives 0 as it ensures the capability to take a correspondent action.

FAU_GEN.1 Audit Data Generation

As this component defines the auditable event and ensures the capability of generating the audit records, it satisfies the TOE security objective 0.

FAU_GEN.2 User Identity Association

As the audit record requires the user identification to trace the association with users, this component defines the events object to audited and satisfies the TOE security objective 0.

FAU_SAA.1 Potential Violation Analysis

This component satisfies the TOE security objective 0.by ensuring the capability of indicating the security violation by checking the audited events.

FAU_SAR.1 Audit Review

This component satisfies the TOE security objective 0. audit by ensuring the capability of the authorized administrator to review.

FAU_SAR.3 Selectable Audit Review

As the capability of the retrieve and arrangement of the audit data according to the criteria having the logical relations, this component satisfies the TOE security objective 0. audit.

FAU_SEL.1 Selectable Audit

As this component ensures the capability of including or excluding the auditable events based on attributes, this component satisfies the TOE security objective 0. audit.

FAU_STG.1 Audit Trail Protection

As ensuring the capability of protecting the audit record from the unauthorized changes & deletion, this component satisfies the TOE security objective 0. audit.

FAU_STG.3 Correspondent Action When Expecting Audit Data Loss

As ensuring the capability of taking a correspondent action when the audit trail exceeds the limits defined in advance, this component satisfies the TOE security objective 0. audit.

FAU_STG.4 Loss Prevention of Audit Data
As ensuring the capability of taking a correspondent action when the audit stores are saturated, this component satisfies the TOE security objective 0. audit.

FDP_IFC.1(1) Partial Information Flow Control (1)
As ensuring the definition of the security policy for the TOE information flow control and the scope of the security policy, this component satisfies the TOE security objective 0. information flow control.

FDP_IFC.1(2) Partial Information Flow Control (2)
As ensuring the definition of the security policy for the TOE information flow control and the scope of the security policy, this component satisfies the TOE security objective 0. information flow control.

FDP_IFF.1(1) Single Layer Security Attribute (1)
As providing the packet filtering security policy rules controlling the information flow based on the security attribute, this component satisfies the TOE security objective 0. information flow control.

FDP_IFF.1(2) Single Layer Security Attribute (2)
As describing the correspondent function for the explicit attacks including the DoS attack and abnormal packet transfer, this component satisfies the 0. information flow control, 0 abnormal packet screening and 0. DoS attack screening security objectives.

FIA_AFL.1 Authentication Failure Process
As defining the authentication attempt failure counts of users and ensuring the capability of taking an correspondent action when the failure counts exceed the defined counts, this component satisfies the TOE security objectives 0.

FIA_ATD.1(1) User Attribute Definition (1)
This component requires that the identifier for the external IT entity be identified as the compute IP address. The IP address generates the audit records by identifying the external IT entity, and becomes the rationale for judging the possible bogus address & DoS attack & information flow control so that it satisfies the 0. audit, 0.

abnormal packet screening, 0. DoS attack screening, 0. identification and 0. information flow control.

FIA_ATD.1(2) User Attribute Definition (2)
As this component is the requirements for the administrator to identify, it satisfies 0. audit and 0. identification.

FIA_UAU.2 Authentication
As this component ensures the capability of successfully identifying the administrator, it satisfies the TOE security objective 0. administration, 0. TSF data protection, (Addition: Administrator authentication shall be done to protect the TOE administration and TSF data protection) and 0. authentication.

FIA_UAU.7 Authentication Feedback Protection
As ensuring only the designated feedback provided to the administrator during the authentication process, this component satisfies the TEO security objective 0. authentication.

FIA_UID.2(1) User Identification before All Actions (1)
This component requires the identification of the identifier for the external IT entity as the computer IP address. The IP address generates the audit records by identifying the external IT entity, and becomes the rationale for judging the possible bogus address & DoS attack & information flow control so that it satisfies the 0. audit, 0. abnormal packet screening, 0. DoS attack screening, 0. identification and 0. information flow control.

FIA_UID.2(2) Identification before All Actions (2)
As requiring the identification for the administrator, this component satisfies 0. audit, 0. administration, 0. TSF data protection, and 0. identification.

FMT_MOF.1(1) Security Functional Administration (1)
As ensuring the capability of the authorized administrator to halt & start the security function and availability at the time of the TOE malfunction, this component satisfies the TOE security objective 0. availability, and 0. administration.

FMT_MOF.1(2) Security Functional Administration (2)
As ensuring the capability of the authorized administrator to decide the action of the security function and availability at the time of the TOE malfunction, this component satisfies the TOE security objective 0. availability, and 0. administration.

FMT_MSA.1 Security Attribute Administration
As the security attribute data, the TSF data needed for the execution of the TOE security function allows only the administrator to access, this component satisfies the TOE security objective 0. availability, and 0. administration.

FMT_MSA.3 Static Attribute Initialization
As ensuring that only the authorized administrator can assess at the time of initialization of the security attribute, the TSF data needed for the execution of the TOE security function, this component satisfies the TOE security objective 0. administration, 0. TSF data protection, and 0. information flow control.

FMT_MTD.1(1) TSF Data Administration (1)
As providing the function of checking the attack pattern among the packing filtering security policy & intrusion prevention security policy and of managing the alarm rules by the authorized administrator, this component satisfies the TOE security objective 0. administration and 0. TSF data protection.

FMT_MTD.1(2) TSF Data Administration (2)
As providing the administrator's capability of the identifying and managing the authentication data, this component satisfies the TOE security objective 0. administration, and 0. TSF data protection.

FMT_MTD.1(3) TSF Data Administration (3)
As ensuring that the authorized administrator sets the screen locking time out value, TCP session time out value, automatic live update cycle, automatic backup cycle & item, automatic integrity check object and check cycle, this component satisfies the TOE security objective 0. administration and 0. TSF data protection.

FMT_MTD.2 Administration of the TSF Data Threshold
As ensuring that the authorized administrator can manage the threshold of the

authentication attempt count when the authentication fails and take a correspondent action when the count reaches or exceeds the threshold to ensure the availability of the TOE, this component satisfies the TOE security objective 0. availability and 0. administration.

FMT_SMF.1 Administrative Function Specification
As requiring the specification of functions of the security attribute provided by the TSF, TSF data, and security function, this component satisfies 0. administration.

FMT_SMR.1 Security Role
As requiring restricting the role of the TOE security administrator to the role of the administrator, this component satisfies the TOE security objective 0. administration, 0. identification and 0. authentication.

FPT_AMT.1 Abstract Machine Test
As designed to execute a series of tests to show the exact operation of the TSF subabstract machine, this component satisfies the TOE security objective 0. availability and 0. TSF data protection objective.

FPT_FLS.1 Secure Status Maintenance during the Failure
As ensuring the secure status maintenance and information flow control function for the critical security functional operation during the TOE failure, this component satisfies the TOE security objective 0. availability, and 0. information flow control.

FPT_RVM.1 TSP Bypass Denial
As preventing the bypass of the information flow control by ensuring that the function of executing the TSP is called and succeeded, this component satisfies the TOE security objective 0. information flow control.

FPT_SEP.1 Security Functional Region Separation
As ensuring that the TSF maintains the security region for its execution from the distrusted subject, this component satisfies the TOE security objective 0. TSF data protection, 0. information flow control objective.

FPT_STM.1 Trusted Timestamp

This component provides the trusted Timestamp used by the TSF. As the generated time ensures recording the sequential security audit events at the time of the audit record generation, this component satisfies the Toe security objective 0. audit.

FPT_TST.1 TSF Self Test

As requiring the function of preventing & detecting the TOE failure by ensuring the self test for the exact operation of the TSF and verifying the integrity of the TSF data & TSF EXE code by the authorized administrator, this component satisfies the TOE security objective 0. availability, and 0. TSF data protection.

FRU_FLT.1 Immunity for Errors: Partial Application

As requiring the critical security functional operation at the time of the TOE failure and ensuring the execution of the information flow control function, this component satisfies the TOE security objective 0. availability and 0. information flow control.

FRU_RSA.1 Maximum Assigned Value

As preventing the DoS attack by requiring the function of confining the resource use assigned value for the TOE protection assets by user, this component satisfies the TOE security objective 0. DoS attack screening.

FTA_SSL.1 Session Locking by the TSF

As the TOE requires the function of locking the authorized session after the inactive period of the authorized administrator, this component satisfies 0. TSF data protection objective.

FTA_SSL.3 Session End by the TSF

As the external IT entity requiring the end of the internal computer and session after a certain period of time, which expands the availability of the network service, this component satisfies the 0. DoS attack screening objective.

FTP_ITC.1 Trusted Channel between TSFs

As the administrator requires the secure channel generation after the mutual authentication at the time of the communications between the TOE & TOE external vulnerability update server (signature update server) or the communication for the exchange of DBMS and data, this component satisfies the 0. TSF data protection.

FPT_ITT.1 Basic Protection of Internal Transfer TSF Data

As protecting the 0. authentication and TSF data requiring the TOE access prohibition of the unauthorized user while requiring the protection of the TSF data from disclosure and modification by generating the trusted channel after the mutual authentication execution when the TSF data is transferred between the separated parts of the TOE for the TOE administration.

8.2.2 IT Environment Security Requirements Rationale

The following shall describe the rationale for the security requirements for the environment.

Security Objective / Security Functional Requirements	OE.TIME	OE.DBMS	OE.SSL Protocol
FPT_STM.1	●		
FAU_SAR.3		●	
FAU_STG.1		●	
FTP_ITC.1			●
FPT_ITT.1			●

[Table 8-3] Rationale for Security Requirements for IT Environment

FPT_STM.1 Trusted Timestamp

As providing the Timestamp for the TSF to use in the IT environment, this component satisfies OE.TIME that shall provide the Timestamp through NTP or the OS where the IT environment complies with RFC 1305.

FAU_SAR.3 Selectable Audit Review

As retrieving & arranging the audit data of DBMS by the criteria with the logic relations, this component satisfies OE.DBMS.

FAU_STG.1 Audit Trail Protection
As DBMS which is the IT environment prevents the unauthorized modification and protects the audit record stored from the unauthorized deletion, this component satisfies OE. DBMS.

FTP_ITC.1 Trusted Channel between TSFs
As the TOE executes the secure communications between the signature list update server and DBMS through the SSL protocol, this component satisfies the OE. SSL protocol.

FPT_ITT.1 Basic Protection of Internal Transfer TSF Data
As ensuring the secure communications between the separated parts of the TOE through the SSL protocol, this component satisfies the OE.SSL protocol.

8.2.3 TOE Assurance Requirements Rationale

This ST claims the assurance package (EAL4) of IPSPP whose suitability is declared, and EAL4 can provide enough assurance in the environment where the TOE is used given the security environment of the TOE. The assurance measures that satisfy the requirements of the EAL 4 class package is described in 6.2 of the document while each document is good enough to satisfy the assurance requirements. The assurance measures which have a dependent relations with ADV_SPM.1 from FPT_FLS.1 and meets the satisfaction of ADV_SPM.1 requirements is described in 6.2 of the referred assurance document (TESS TMS v4.5 SPM). The TOE doesn't define users for the AGD_USR.1 user guidance assurance component so that the user guidance is not available. So, the assurance measures for this component is not provided.

8.3 Dependency Rationale

8.3.1 Dependency of TOE Security Functional Requirements

[Table 8-4] shows the dependency of the functional component.

No.	Functional Component	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	36
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 20,21(Dependency Upper FIA_UID.2 Selection)
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(Depedency Upper FIA_UAU.2 Selection)
16	FIA_ATD.1 (1)	-	-
17	FIA_ATD.1 (2)	-	-
18	FIA_UAU.2	FIA_UID.1	20,21(Dependency Upper FIA_UID.2 Selection)
19	FIA_UAU.7	FIA_UAU.1	18(Dependency Upper FIA_UAU.2 Selection)
20	FIA_UID.2(1)	-	-
21	FIA_UID.2(2)	-	-
22	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	30 31
23	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	30 31
24	FMT_MSA.1	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	- 11,12 31 30

25	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	24 31
26	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	30 31
27	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	30 31
28	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	30 31
29	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	26,27 31
30	FMT_SMF.1	-	-
31	FMT_SMR.1	FIA_UID.1	20,21(Dependency Upper FIA_UID.2 Selection)
32	FPT_AMT.1	-	-
33	FPT_FLS.1	ADV_SPM.1	Assurance Requirements
34	FPT_RVM.1	-	-
35	FPT_SEP.1	-	-
36	FPT_STM.1	-	-
37	FPT_TST.1	FPT_AMT.1	32
38	FRU_FLT.1	FPT_FLS.1	33
39	FRU_RSA.1	-	-
40	FTA_SSL.1	FIA_UAU.1	18(Dependency Upper FIA_UAU.2 Selection)
41	FTA_SSL.3	-	-
42	FTP_ITC.1	-	-
43	FPT_ITT.1	-	-

[Table 8-4] Functional Component Dependency

FAU_GEN.2, FIA_UAU.1, FMT_SMR.1 have dependency in FIA_UID.1 but are satisfied by FIA_UID.2 having a layer relations with FIA_UID.1.
FIA_AFL.1, FIA_UAU.7, FTA_SSL.1 have dependency in FIA_UAU.1 but are satisfied by FIA_UAU.2 having a layer relations with FIA_UAU.1.

8.3.2 Dependency of TOE Assurance Requirements

Dependency of each assurance package provided in the information protection system CC is already satisfied so that the rationale for this is omitted.

8.4 SOF Rationale

The SOF is applied to “FIA_UAU.2”, the security requirements with probability & permutation mechanism and “identification & authentication (IA_UID)” which implements FIA_UAU.2 through a function. The SOF of “FIA_UAU.2”is medium while the SOF of “identification & authentication (IA_UID)”is high. The rationale for the SOF of “identification & authentication (IA_UID)”is as follows.

What the time took for the treat agent to find the password is 4,507 days for the security function of satisfying “FIA_UAU.2” and password mechanism of “identification & authentication (IA_UID)”. However, that is unrealistic attack time so that its SOF is high according to the calculation method of CEMB.8.

The threat agent having the network intrusion prevention system PP of EAL4 class and consistently low level of expertise, resource, & motivation lets the TOE be specified to have the immunity from the vulnerability in the ST.
The function of “identification & authentication (IA_UID)”, what is earned by implementing the “FIA_UAU.2”security requirements whose SOF is medium , whose SOF is high is good enough to counter the threat agent with the low level of threat agents

8.5 TOE Summary Specification Rationale

The rationale TOE summary specification proves that the described IT security functional requirements & assurance requirements are good enough to satisfy the TOE security function & assurance measures while verifying that those requirements are proper to deal with the security issues as a result of that.

8.5.1 Association of Security Functional Requirements & TSF

[Table 8-5]is the association of the TOE security function for the IT security functional requirements.

TOE Security Functional Requirements		TOE Summary Specification Security Function
Class	Component	
Security Audit	FAU_ARP.1	Audit Data Correspondence (AT_RES)

	FAU_GEN.1	Audit Data Generation (AT_GEN) Traffic Statistics Generation (DP_TRA) Correspondence by Violated Event (DP_RES)
	FAU_GEN.2	Audit Data Generation (AT_GEN)
	FAU_SAA.1	Audit Data Generation (AT_GEN) Anomalous Symptom Detection (DP_ANM) Threat Level Evaluation(DP_THR)
	FAU_SAR.1	Audit Data Inquiry (AT_SAR)
	FAU_SAR.3	Audit Data Inquiry (AT_SAR)
	FAU_SEL.1	Audit Data Generation (AT_GEN)
	FAU_STG.1	Identification & Authentication (IA_UID)
	FAU_STG.3	Audit Data Correspondence (AT_RES) Health Check(PT_HCH) Function
	FAU_STG.4	Audit Data Correspondence (AT_RES) Health Check(PT_HCH) Function
User Data Protection	FDP_IFC.1(1)	Packet Filtering (DP_FLT) Correspondence by Violated Event (DP_RES)
	FDP_IFC.1(2)	Protocol Vulnerability Analysis (DP_ID1) Signature Violation Analysis (DP_ID3) Statistical Analysis (DP_ID4) Correspondence by Violated Event (DP_RES)
	FDP_IFF.1(1)	Packet Filtering (DP_FLT) Correspondence by Violated Event (DP_RES)
	FDP_IFF.1(2)	Signature Violation Analysis (DP_ID3) Statistical Analysis (DP_ID4) Protocol Vulnerability Analysis (DP_ID1) Correspondence by Violated Event (DP_RES)
Identification & Authentication	FIA_AFL.1	Authentication Correspondence (IA_RES)
	FIA_ATD.1 (1)	Packet Data Contraction & Identification (DP_GET)
	FIA_ATD.1 (2)	Identification & Authentication (IA_UID)
	FIA_UAU.2	Identification & Authentication (IA_UID)
	FIA_UAU.7	Identification & Authentication (IA_UID)
	FIA_UID.2(1)	Packet Data Contraction & Identification (DP_GET)

	FIA_UID.2(2)	Identification & Authentication (IA_UID)
Security Administration	FMT_MOF.1(1)	Manager Environment Setting Information Administration (SM_MAN) Integrity Administration (SM_INT)
	FMT_MOF.1(2)	Signature List Administration (SM_SIG) Packet Filtering Policy Administration (SM_FLT) Manager Environment Setting Information Administration (SM_MAN) Integrity Check (PT_INT) Function
	FMT_MSA.1	Signature List Administration (SM_SIG) Packet Filtering Policy Administration (SM_FLT)
	FMT_MSA.3	Signature List Administration (SM_SIG) Packet Filtering Policy Administration (SM_FLT)
	FMT_MTD.1(1)	Signature List Administration (SM_SIG) Packet Filtering Policy Administration (SM_FLT) Manager Environment Setting Information Administration (SM_MAN) Anomalous Symptom Policy Administration (SM_ANM) Host Administrative Policy (SM_HST)
	FMT_MTD.1(2)	Administrator Account Administration (SM_ACC)
	FMT_MTD.1(3)	System Audit Data Reaction Administration (SM_ADT) Integrity Administration (SM_INT) Manager Environment Setting Information Administration (SM_MAN)
	FMT_MTD.2	Authentication Correspondence (IA_RES) Administrator Account Administration (SM_ACC)

	FMT_SMF.1	Administrator Account Administration (SM_ACC) Signature List Administration (SM_SIG) Packet Filtering Policy Administration (SM_FLT) Integrity Administration (SM_INT) Manager Environment Setting Information Administration (SM_MAN) Anomalous Symptom Policy Administration (SM_ANM) Host Administrative Policy (SM_HST) Integrity Check (PT_INT) Function System Audit Data Reaction Administration (SM_ADT)
	FMT_SMR.1	Administrator Account Administration (SM_ACC)
TSF Protection	FPT_AMT.1	Health Check(PT_HCH) Function
	FPT_FLS.1	Health Check(PT_HCH) Function
	FPT_RVM.1	Packet Data Contraction & Identification (DP_GET)
	FPT_SEP.1	Health Check(PT_HCH) Function
	FPT_STM.1	Time Synchronization (PT_TSN) Function
	FPT_TST.1	Integrity Check (PT_INT) Function
	FPT_ITT.1	Authentication between Tiers (SP_UID) Transfer Data Protection (SP_SSL)
Resource Utilization	FRU_FLT.1	Health Check(PT_HCH) Function
	FRU_RSA.1	Statistical Analysis (DP_ID4)
TOE Access	FTA_SSL.1	Screen Locking (TA_SSN) Function
	FTA_SSL.3	Session Administration (DP_ID2)
Trusted Path/Channel	FTP_ITC.1	Authentication between Tiers (SP_UID) Transfer Data Protection (SP_SSL)

[Table 8-5] Association of the TOE Security Function for the IT Security Functional Requirements

[Table 8-6] is the association of the IT security functional requirements based on the TOE security function.

Security Function	Security Requirements
Audit Data Generation (AT_GEN)	FAU_GEN.1

	FAU_GEN.2
	FAU_SAA.1
	FAU_SEL.1
Audit Data Inquiry (AT_SAR)	FAU_SAR.1
	FAU_SAR.3
Audit Data Correspondence (AT_RES)	FAU_ARP.1
	FAU_STG.3
	FAU_STG.4
Packet Data Contraction & Identification (DP_GET)	FIA_ATD.1(1)
	FIA_UID.2(1)
	FPT_RVM.1
Packet Filtering (DP_FLT)	FDP_IFF.1(1),
	FDP_IFC.1(1)
Protocol Vulnerability Analysis (DP_ID1)	FDP_IFF.1(2) FDP_IFC.1(2)
Session Administration (DP_ID2)	FTA_SSL.3
Signature Violation Analysis (DP_ID3)	FDP_IFF.1(2) FDP_IFC.1(2)
Statistical Analysis (DP_ID4)	FDP_IFF.1(2) FDP_IFC.1(2) FRU_RSA.1
Correspondence by Violated Event (DP_RES)	FAU_GEN.1
	FDP_IFF.1(1)
	FDP_IFF.1(2)
	FDP_IFC.1(1)
	FDP_IFC.1(2)
Traffic Statistics Generation (DP_TRA)	FAU_GEN.1
Anomalous Symptom Detection (DP_ANM)	FAU_SAA.1
Threat Level Evaluation (DP_THR)	FAU_SAA.1
Identification & Authentication (IA_UID)	FAU_STG.1
	FIA_ATD.1(2)
	FIA_UAU.2
	FIA_UAU.7

	FIA_UID.2(2)
Authentication Correspondence (IA_RES)	FIA_AFL.1
	FMT_MTD.2
Administrator Account Administration (SM_ACC)	FMT_MTD.1(2)
	FMT_MTD.2
	FMT_SMF.1
	FMT_SMR.1
System Audit Data Reaction Administration (SM_ADT)	FMT_SMF.1 FMT_MTD.1(3)
Signature List Administration (SM_SIG)	FMT_MSA.1
	FMT_MOF.1(2)
	FMT_MSA.3
	FMT_MTD.1(1)
	FMT_SMF.1
Packet Filtering Policy Administration (SM_FLT)	FMT_MSA.1
	FMT_MOF.1(2)
	FMT_MSA.3
	FMT_MTD.1(1)
	FMT_SMF.1
Integrity Administration (SM_INT)	FMT_MOF.1(1)
	FMT_MTD.1(3)
	FMT_SMF.1
Manager Environment Setting Information Administration (SM_MAN)	FMT_MOF.1(1)
	FMT_MOF.1(2)
	FMT_MTD.1(1)
	FMT_MTD.1(3)
	FMT_SMF.1
Anomalous Symptom Policy Administration (SM_ANM)	FMT_MTD.1(1)
	FMT_SMF.1
Host Administrative Policy(SM_HST)	FMT_MTD.1(1)
	FMT_SMF.1
Health Check(PT_HCH) Function	FAU_STG.3
	FAU_STG.4
	FPT_AMT.1

	FPT_FLS.1
	FPT_SEP.1
	FRU_FLT.1
Integrity Check (PT_INT) Function	FPT_TST.1
	FMT_SMF.1
	FMT_MOF.1(2)
Time Synchronization (PT_TSN) Function	FPT_STM.1
Screen Locking (TA_SSN) Function	FTA_SSL.1
Authentication between Tiers (SP_UID)	FPT_ITT.1
	FTP_ITC.1
Transfer Data Protection (SP_SSL)	FPT_ITT.1
	FTP_ITC.1

[Table 8-6] Association of the IT Security Functional Requirements for the TOE Security Function

8.5.2 TOE Summary Specification Rationale

FAU_ARP.1:Security Alarm

When detecting the potential security violation of the TSF through the audit data correspondence (AT_RES), the TOE ensures this security requirements by providing the function of emergent alarm, visible aural notice, SMS transfer, e-mail transfer, and registered program execution to the authorized administrator.

FAU_GEN.1: Audit Data Generation

The TOE generates the system security audit data through the audit data generation (AT_GEN) function and statistics for the intrusion detection & blocking event. It also generates the traffic statistics data through the traffic statistics generation (DP_TRA) function. The audit data for the intrusion detection is generated through the correspondence by violated event (DP_RES).

FAU_GEN.2:User Identity Correlation

As correlating the user identity with the auditable events by recording the user identity when the audit records are generated through the audit data generation (AT_GEN) function, the TOE ensures this security requirements.

FAU_SAA.1:Potential Violation Analysis

The TOE ensures this security requirements by providing the administrator notice function based on the analysis of the security events indicating the potential security violation through the audit data generation (AT_GEN) function, anomalous symptom detection (DP_ANM) and threat level evaluation (DP_THR).

FAU_SAR.1:Audit Review

The TOE ensures this security items by providing the function of the inquiry & retrieval of the audit data through the audit data inquiry (AT_SAR) function.

FAU_SAR.3: Selectable Audit Review

The TOE ensures this security requirements by selectively providing the audit record review through the inquiry & retrieval function of the audit data inquiry (AT_SAR) function.

FAU_SEL.1: Selectable Audit

The TOE ensures this security requirements by selectively generating the audit data of the security event indicating the potential security violation through the audit data generation (AT_GEN) function.

FAU_STG.1: Audit Trail Protection

The TOE prevents the unauthorized modification by allowing only the authorized & identified administrators to access to the DB. Thus, it ensures this security requirements through the identification & authentication (IA_UID).

FAU_STG.3: Correspondent Action When Expecting Audit Data Loss

The TOE notices the administrator though the audit data correspondence (AT_RES) for the audit data generated by the excessive audit stores. The check on the store capacity can be done through Health Check(PT_HCH). Through this, this security requirements are ensured.

FAU_STG.4: Loss Prevention of Audit Data

The TOE notices the authorized administrator through the audit data correspondent (AT_RES) function for the audit data generated when the audit stores are saturated.

The check on the store capacity is carried out by Health Check(PT_HCH). Through this, this security requirements are ensured.

FDP_IFC.1(1): Partial Information Flow Control (1)
The TOE ensures this security requirements by controlling the information flow between the subject and object through the correspondent function by violated event (DP_RES) and packet filtering allowing or denying the packets in accordance with the packet filtering rules.

FDP_IFC.1(2): Partial Information Flow Control (2)
The TOE ensures this security requirements by controlling the information flow between the subject and object through the protocol vulnerability analysis (DP_ID1), signature violation analysis (DP_ID3), statistical analysis (DP_ID4) and correspondent function by violated event (DP_RES) when the packet violated in the intrusion prevention & packet filtering policy is detected.

FDP_IFF.1(1): Single Layer Security Attribute
The TOE controls the access by departure, destination and service of the packet through the packet filtering (DP_FLT) function. It also provides the function of the screening of the packet & audit data generation through the correspondence by violated event (DP_RES). Through this, this security requirements are ensured.
FDP_IFF.1(2): Single Layer Security Attribute
The TOE controls the information flow between the subject and object through the protocol vulnerability check by the protocol vulnerability analysis (DP_ID1), protocol & pattern check by the signature violation analysis (DP_ID3), and the DoS attack detection by the statistical analysis (DP_ID4) function. It also provides the function of blocking the packet and generating the audit data through the correspondence by violated event (DP_RES). Through this, this security requirements are ensured.

FIA_AFL.1: Authentication Failure Process
The TOE ensures the security requirements by providing the authentication prevention of users through authentication correspondence (1A_RES) when the number of the authentication failure exceeds the criteria that is set.
FIA_ATD.1(1): User Attribute Definition
The TOE ensures the security requirements by extracting the IP address of the

external IT entity through the extraction audit data generation (DP_GET) function.

FIA_ATD.1(2): User Attribute Definition
The TOE ensures the security requirements by maintaining & managing the security attributes of users through the identification & authentication (IA_UID) function.

FIA_UAU.2: User Authentication before All Actions
The TOE shall pass through the administrator log-in process when using all security functions. Identification & authentication (IA_UID) ensures this security requirements by providing the authentication function.

FIA_UAU.7: Authentication Feedback Protection
The TOE ensures this security requirements by providing the function of outputting only the success/fail messages for the administrator authentication process progress results.

FIA_UID.2(1): User Identification before All Actions
The TOE shall identify all IT entities to provide the intrusion detection & blocking function. The packet data contraction & identification (DP_GET) ensures this security requirements by providing the function of identifying the IT entity.

FIA_UID.2(2): User Identification before All Actions
The TOE shall pass through the administrator log-in process. Identification & authentication (IA_UID) ensures this security requirements by providing the authentication function

FMT_MOF.1(1):Security Function Administration (1)
The TOE ensures this security requirements by confining only the authorized administrator to the security function initiation and halt through the manager environment setting information administration (SM_MAN) & integrity administrative (SM_INT) function.

FMT_MOF.1(2): Security Function Administration (2)
The TOE ensures this security requirements by confining only the authorized administrator to the security function execution through the signature list

administration (SM_SIG), packet filtering policy administration (SM_FLT), manager environment setting information administration (SM_MAN) and integrity check (PT_INT).

FMT_MSA.1: Security Attribute Administration
The TOE ensures this security requirements by confining only the authorized administrator to the function of the modification, query, deletion, etc. for the security attributes through the function of signature list administration (SM_SIG), and packet filtering policy administration (SM_FLT).

FMT_MSA.3: Static Attribute Initiation
The TOE ensures this security requirements by providing the confined default value through the function of the packet filtering policy administration (SM_FLT) and signature list administration (SM_SIG).

FMT_MTD.1(1):TSF Data Administration
The TOE ensures this security requirements by confining only the authorized administrator to the function of the modification, deletion, generation and inquiry for the packet filtering policy administration (SM_FLT), anomalous list administration (SM_SIG), manager environment setting information administration (SM_MAN), anomalous symptom policy administration (SM_ANM) and host administration policy (SM_HST).

FMT_MTD.1(2):TSF Data Administration
The TOE ensures this security requirements by confining only the authorized administrator to the function of the modification & deletion of the identification & authentication data for the administrator account administration (SM_ACC).

FMT_MTD.1(3):TSF Data Administration
The TOE ensures this security requirements by confining only the authorized administrator to the modification to the security function for the integrity administration (SM_INT), manager environment setting information administration (SM_MAN), and system audit data reaction administration (SM_ADT).

FMT_MTD.2:TSF Data Threshold Administration

The TOE ensures this security requirements by confining only the authorized administrator to the specification of the authentication attempt failure counts for the function of the administrator account administration (SM_ACC) and authentication correspondence (IA_RES).

FMT_SMF.1: Administrative Function Specification
The TOE ensures this security requirements by providing the function of the administrator account administration (SM_ACC), system audit data reaction administration (SM_ADT), signature list administration (SM_SIG), packet filtering policy administration (SM_FLT), integrity administration (SM_INT), manager environment setting information administration (SM_MAN), anomalous symptom policy administration (SM_ANM), host administrative policy (SM_HST), and integrity check (PT_INT).

FMT_SMR.1:Security Role
The TOE provides the administrator account authority of the two phases, which is done in the administrator account administration (SM_ACC) to ensure this security requirements.

FPT_AMT.1: Abstract Machine Test
The TOE ensures this security requirements by checking the communication connection status between parts of the TOEs periodically through the Health Check(PT_HCH) function.

FPT_FLS.1: Secure Status Maintenance during Failure
The TOE maintains the secure status for the critical security functional operation through the Health Check(PT_HCH) function during the failure of the TOE, and ensures this security requirements by dealing with the communication faults through the system console when the communication linkage failure between parts of the TOEs is generated.

FPT_RVM.1:TSP Bypass Denial
As all network packets inputted in the TOE are collected through the packet data contraction & identification (DP_GET), the flow control is done.

FPT_SEP: Security Functional Region Separation
The TOE ensures this security requirements by protecting the TOE from the interference and breach made by the distrusted subject through the Health Check(PT_HCH) function.

FPT_STM.1: Trusted Timestamp
The TOE ensures this security requirements by providing the trusted time through the time synchronization (PT_TSN) function.

FPT_TST.1:Self TSF Test
The TOE ensures this security requirements by proving the exact operation of the TSF data through the integrity check (PT_INT) function and verifying the integrity of the TSF data.

FRU.FLT.1:Immunity for Errors: Partial Application
The TOE ensures this security requirements by maintaining the secure status for the critical security functional operation through the Health Check(PT_HCH) function during the TOE failure.

FRU_RSA.1: Maximum Threshold
The TOE provides the detection function for the DoS attack of the TCP protocol stack like Syn flooding through the statistical analysis (DP_ID4) function.

FTA_SSL.1: Session Locking by the TSF
The TOE ensures this security requirements by providing the screen locking function for the session where the administrator doesn't access through the screen locking (TA_SSN) function.

FTA.SSL.3: Session End by the TSF
The TOE ensures this security requirements by providing the function of ending the affected session in the session administration (DP_ID2) when the TCP session hasn't been operating for a certain period of time.

FTP_ITC.1: Trusted Channel between TSFs
The TOE ensures this security requirements by preventing the communications

between the TSF and remote trusted IT product from the disclosure and modification through the provision of identification & encryption communication through the transfer data protection (SP_SSL) & authentication between Tiers (SP_UID).

FPT_ITT.1: Basic Protection of Internal Transfer TSF Data
The TOE ensures this security requirements by the prevention of the disclosure & modification to the communication between parts of the TOEs through the provision of the transfer data protection (SP_SSL) & authentication between Tiers (SP_UID).

8.5.3 Association of Assurance Requirements & Assurance Measures

The assurance measures for each assurance component is satisfied through the following table.

Assurance Class	Assurance Component		Assurance Measures
Configuration Administration	ACM_AUT.1	Partial Configuration Administrative Automation	TESS TMS v4.5 Configuration Administrative Document
	ACM_CAP.4	Generation Support & Claim Procedure	
	ACM_SCP.2	Scope of Issue Tracking Configuration Administration	
Delivery & Operation	ADO_DEL.2	Detection of Modification	TESS TMS v4.5 IGS
	ADO_IGS.1	Installation, Generation, Start-up Procedure	TESS TMS v4.5 Installation Guide
Development	ADV_FSP.2	Completely Defined External Interface	TESS TMS v4.5 FSP
	ADV_HLD.2	Basic Design Separating the Security Function & Non-Security Function	TESS TMS v4.5 HLD
	ADV_IMP.1	Implementation Representation for the Partial TSF	TESS TMS v4.5 IMP
	ADV_LLD.1	Described & Detailed Design	TESS TMS v4.5 LLD

	ADV_RCR.1	Non-Standardized Conformity Verification	TESS TMS v4.5 FSP, TESS TMS v4.5 HLD, TESS TMS v4.5 LLD, TESS TMS v4.5 IMP
	ADV_SPM.1	Non-Standardized TOE Security Policy Model	TESS TMS v4.5 SPM
Guidance	AGD_ADM.1	Administrator Guidance	TESS TMS v4.5 ADM
	AGD_USR.1	User Guidance	-
Life Cycle Support	ALC_DVS.1	Identification of Security Policy	TESS TMS v4.5 Life Cycle Support Document
	ALC_LCD.1	Developer Defined Life Cycle Model	
	ALC_TAT.1	Well Defined Development Tools	
Test	ATE_COV.2	Analysis of Test Scope	TESS TMS v4.5 FT
	ATE_DPT.1	Basic Design Test	
	ATE_FUN.1	Functional Test	
	ATE_IND.2	Dependent Test : Sample Test	
Vulnerability Analysis	AVA_MSU.2	Verification of Guidance Analysis	TESS TMS v4.5 MSU

[Table 8-7] Association of Security Assurance Requirements & Non-Security Assurance Requirements

ACM_AUT.1: Partial Configuration Administrative Automation- The TOE provides the automatic means of generating only the authorized modification to the TOE implementation representation in the configuration administrative system, and provides the **TESS TMS v4.5 configuration administrative document** to ensure the use of the automatic means supporting the TOE generation.

ACM_CAP.4: Generation Support & Claim Procedure- The TOE provides the control for ensuring that the unauthorized modification doesn't happen and supplies the

TESS TMS v4.5 configuration administrative document to ensure the use of the configuration administrative system and the system's functionality.

ACM_SCP.2: Scope of Issue Tracking Configuration Administration- The TOE supplies **the TESS TMS v4.5 configuration administrative document** to ensure that the configuration items under the configuration administration are modified in a controlled way according to the proper authorization.

ADO_DEL.2:Detection of Modification- The TOE supplies **the TESS TMS v4.5 IGS** to ensure the system control & delivery facility & procedure assuring that the TOE sent by the sender is given to the receiver without the modification.

ADO_IGS.1: Installation, Generation, Start-up Procedure- The TOE supplies **the TESS TMS v4.5 installation guide** to ensure that the TOE is installed, generated and started up in the secure way as intended by the developer.

ADV_FSP.2: Completely Defined External Interface- The TOE supplies **the TESS TMS v4.5 FSP** to substantiate the basic description on the interface & action seen by the user of the TSF and the TOE security functional requirements while closely looking into all external interfaces.

ADV_HLD.2: Basic Design Separating Security Functions & Non-Security Functions- The TOE describes the TSF as major configuration units (subsystem) and relations of those units and the functions that those functions provide. As a result of this, supplies **the TESS TMS v4.5 HLD** to ensure the proper structure to implement the TOE security functional requirements.

ADV_LLD.1: Described & Detailed Design - The TOE describes the TSF internal operation from the perspective of the mutual & dependent relations between modules and supplies **the TESS TMS v4.5 LLD** to ensure that the TSF subsystem is getting correct and detailed effectively.

ADV_IMP.1: Implementation Representation for the Partial TSF- The TOE supplies **the TESS TMS v4.5 IMP** to ensure the analysis by letting the TSF detect the detailed internal operation.

ADV_RCR.1: Non-Standardized Conformity Verification- The TOE supplies **the TESS TMS v4.5 HLD FSP, TESS TMS v4.5 HLD, TESS TMS v4.5 LLD, and TESS TMS v4.5 IMP** to ensure the conformity between various representations of the TSF.

ADV_SPM.1: Non-Standardized TOE Security Policy Model - The TOE describes all rules & characteristics of all policies of the TSP and provides **the TESS TMS v4.5 SPM** to ensure the consistency and completeness.

AGD_ADM.1:Administrator Guidance- The TOE provides **the TESS TMS v4.5 ADM** for the documented material to be used by the responsible people for configuring, maintaining and managing the TOE in the exact way to maximize the security.

AGD_USR.1:User Guidance- The TOE doesn't provide the **user guidance** as extra users besides the administrator can't be distinguished.

ALC_DVS.1: Security Policy Identification- The TOE provides **the TESS TMS v4.5 life cycle support document** by using the physical, procedural, human, and other security policies that can be used for the development environment to protect the TOE.

ALC_LCD.1: Developer Defined Life Cycle Model- The TOE provides **the TESS TMS v4.5 life cycle support document** to ensure the control needed for the development and maintenance by the model used for the development and maintenance of the TOE.

ALC_TAT.1: Well Defined Development Tools- The TOE provides **the TESS TMS v4.5 life cycle support document** to ensure that the incorrect development tools with the wrong definition or inconsistency are not used for the development of the TOE.

ATE_COV.2: Analysis of Test Scope- The TOE provides **the TESS TMS v4.5 life FT** to verify whether the TSF is tested systematically according to the functional specification.

ATE_DPT.1: Detailed Design Test- The TOE provides **the TESS TMS v4.5 life FT** to ensure the correct implementation of the TSF subsystem.

ATE_FUN.1:Funtional Test- The TOE provides **the TESS TMS v4.5 life FT** to ensure that all security functions are executed as specified.

ATE_IND.2:Independent Test: Sample Test- The TOE provides **the TESS TMS v4.5 life FT** to ensure that security functions are executed as specified.

AVA_MSU.2: Verification of Guidance Analysis- The TOE provides **the TESS TMS v4.5 MSU** to ensure that there is no wrong description, irrationality, & conflicting guides and secure procedures for all operation modes are managed.

AVA_SOF.1: Evaluation on the TOE Security SOF - The TOE provides the **TESS TMS v4.5 VLA** to decide the strength of the security action through quantitative or statistical analysis results for the security action of subsecurity mechanism and efforts needed for overcoming this result.

AVA_VLA.2: Independent Vulnerability Analysis - The TOE provides the **TESS TMS v4.5 VLA** to confirm that there exists the security vulnerability and to ensure that vulnerabilities can be used malignantly in the intended environment.

8.6 PP Claims Rationale

This ST claimed all security functional requirements of the network intrusion prevention PP V1.1 (Network Intrusion Prevention System Protection Profile, Dec. 21, 2005, Korea Information Security Agency). Added or modified contents are as follows.

Category	Item	Contents
Security Objectives for the Environment	OE. Secure TOE External Server	For the function of the TOE, the NTP for maintaining the trusted time existing in the external TOE and the live update server updating the latest attack rules shall be secure

	OE.SSL Protocol	The TOE forms secure communication channel at the time of communications of DBMS, signature live update server and separated parts of the TOE through the SSL protocol based on the certificate that the IT environment provides.
	OE.TIME	The IT environment shall provide the trusted Timestamp from the NTP server or OS directing RFC 1305
	OE.DBMS	The intrusion detection & traffic-related data generated in the TOE shall be stored in DBMS, the stored data shall be securely managed by the identification & authentication method defined by DBMS itself. At the request of the administrator, DBMS provides the function of the inquiry & retrieval of the stored intrusion detection & traffic-related data. DBMS shall be securely managed and operated with the latest security & vulnerability-related patches.

[Table 8-8] Security Objectives Additions

Security Functional Class	Security Functional Component		Remark
Security Audit	FPT_ITT.1	Basic Protection of Internal Transfer TSF Data	Added
	FIA_UAU.2	User Authentication before All Actions	Replacement of FIA_UAU.1

[Table 8-9] TOE Security Functional Requirements Added & Modified Items

Security Functional	Security Functional Component	Remark

Class			
Security Audit	FAU_SAR.3	Selectable Audit Review	Added
	FAU_STG.1	Audit Trail Protection	Added
	FPT_ITT.1	Basic Protection of Internal Transfer TSF Data	Added
	FPT_STM.1	Trusted Timestamp	Added
	FTP_ITC.1	Trusted Channel between TSFs	Added

[Table 8-10] Security Requirements Additions for the Environment