

Safezone IPS V1.0(SZ5XU)

Security Target_20070314_V1.00.04

LG N-Sys





LG N-Sys

Document Identification No.

SafezoneIPS V1.0(SZ5XU)

Security Target_20070314_V1.00.04

Product Name + Version + (Model)

SafezoneIPS V1.0(SZ5XU)

Document Type

Security Target

Revision History

Version	Date	Reason	Author
V1.00.01	2006.08.11.	Initial official registration	J.H. Park
V1.00.02	2006.11.06.	Recommendations from the observation report	J.H. Park
V1.00.03	2007.01.18.	Recommendations from the observation report	J.H. Park
V1.00.04	2007.03.14.	Recommendations from the observation report	J.H. Park


Although this document is a public version to allow reference, no part of this document may be copied, distributed, eliminated, or used otherwise without prior consent of LG N-Sys

CONFIDENTIAL

Table of Contents

1. Security Target (ST) Introduction.....	5
1.1 ST Identification.....	5
1.2 Security Target(ST) Overview.....	6
1.3 Common Criteria(CC) Conformance.....	8
1.4 Glossary.....	9
1.5 References.....	14
2. TOE Description.....	15
2.1 Product Type.....	15
2.2 TOE Environment.....	16
2.2.1 TOE Network Environment.....	16
2.2.2 TOE Product Configuration.....	19
2.3 TOE Scope and Boundary.....	21
2.3.1 Physical Scope and Boundary.....	21
2.3.2 Logical Scope and Boundary.....	22
3. TOE Security Environment.....	25
3.1 Assumption.....	25
3.2 Threats.....	27
3.2.1 Threats to the TOE.....	27
3.2.2 Threats to the TOE Operational Environment.....	29
3.3 Organizational Security Policy.....	30
4. TOE Security Objectives.....	31
4.1 Security Objectives for the TOE.....	31
4.2 Security Objectives for the Environment.....	32
5. IT Security Requirements.....	34
5.1 TOE Security Functional Requirements.....	35
5.1.1 Security Audit.....	37
5.1.2 User Data Protection.....	42
5.1.3 Identification and Authentication.....	46
5.1.4 Security Management.....	48

5.1.5	Protection of the TSF	54
5.1.6	Resource Utilization	56
5.1.7	TOE Access	57
5.1.8	Trusted Path/Channels	58
5.2	TOE Security Assurance Requirements.....	59
5.2.1	Configuration Management	59
5.2.2	Delivery and Operation	61
5.2.3	Development	62
5.2.4	Guidance Documents	66
5.2.5	Life Cycle Support	67
5.2.6	Tests	69
5.2.7	Vulnerability assessment	71
5.3	Security requirement for the IT environment	73
6.	TOE Summary Specification.....	74
6.1	TOE Security Functions	74
6.1.1	Security Audit	74
6.1.2	User Data Protection	79
6.1.3	Identification and authentication	81
6.1.4	Security Management	84
6.1.5	TSF Protection	89
6.1.6	TOE Access	92
6.2	Assurance Measures	93
7.	Protection Profile Claims.....	95
7.1	Protection Profile Reference.....	95
7.2	Protection profile tailoring.....	95
7.3	Protection Profile Additions.....	96
7.3.1	Protection Profile Modifications	103
8.	Rationale	104
8.1	Security Objectives Rationale.....	104
8.1.1	Rationale for the security objectives for the TOE.....	106
8.1.2	Rational for the security objectives for the environment.....	108
8.2	Security Requirements Rationale.....	111
8.2.1	TOE Security Functional Requirements Rationale.....	112

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

8.2.2	TOE assurance Requirements Rationale	118
8.3	Dependencies Rationale.....	119
8.3.1	TOE Security Functional Requirements Dependencies	119
8.3.2	TOE Assurance Requirements Dependencies	120
8.4	TOE Summary Sepcification Rationale	121
8.4.1	Correlations of Security Functional Requirements and TOE Security Functions	121
8.4.2	TOE Summary Specification Rationale	125
8.4.3	Correlations of Assurance Requirements and Assurance Measures	131
8.5	PP Claims Rationale.....	132
8.6	SOF Claim Rationale.....	133

List of Figures/Tables

[Figure 2-1] Bridge mode Network configuration-1.....	16
[Figure 2-2] Bridge mode Network configuration-2.....	17
[Figure 2-3] Gateway mode Network Configuration.....	18
[Figure 2-4] TOE Basic Configuration.....	19
[Table 2-1] SafezoneIPS Hardware specification.....	21
[Table 3-1] Identification of assumptions.....	25
[Table 3-2] Identification of threats.....	27
[Table 3-3] Identification of organizational security policies	30
[Table 4-1] Identification of TOE security objectives	31
[Table 5-1] Security functional requirements.....	36
[Table 5-2] Assurance components.....	59
[Table 6-1] Assurance measures.....	94
[Table 7-1] Protection profile additions and modifications	103
[Table 8-1] Correlation of security environment and security objectives ..	105
[Table 8-2] Correlation of security objectives and security functional requirements	111
[Table 8-3] Functional components Dependencies.....	120
[Table 8-4] Correlations of security functional requirements and TOE security functions	124
[Table 8-5] Assurance measures.....	132


1. Security Target (ST) Introduction

This document is the security target of a network prevention system based on the Network Intrusion Prevention System Protection Profile V1.1 (2005.12.21, KISA). This ST defines the security functions and assurance measures, describes the security requirements used for evaluation and general information such as implementation methods and technical information.

1.1 ST Identification

All information to identify ST and to control SafezoneIPS V1.0(SZ5XU)(hereinafter referred to as "SafezoneIPS ") are provided.

Divison	Description
Title	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04
Version	V1.00.04
Written date	Mar. 14, 2007
Author	LG N-Sys Security Gr.
Common Criteria(CC) version	The Common Criteria for IT Security Evaluation(2005-25, the Ministry of Information and Communication)
Evaluation Assurance Level(EAL)	EAL4
Protection Profile claimed	Network Intrusion Prevention System Protection Profile V1.1(Network Intrusion Prevention System Protection Profile), Dec. 21, 2005
TOE identifier	SafezoneIPS V1.0(SZ5XU) - TOE : V1.0
TOE Description	SafezoneIPS is a unified network security solution, which provides IPS, Firewall, QoS, Mail Filtering function.
Security Target evaluator	KISA
Keyword	Network Prevention System(IPS), Access Control, Information Flow Control, Identification and Authentication

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

1.2 Security Target(ST) Overview


SafezoneIPS is a unified network security solution(hardware-type) which provides IPS, Firewall, QoS, Mail Filtering function. That is, SafezoneIPS is a unified security system which enables efficient network resource usage by protecting the internal IT asset of the target network not only from direct attacks that exploit vulnerabilities but also from any illegal attacks that can shut down the network by increasing network traffic load using DOS attack, and by controlling network bandwidth.

- 1) TOE performs intrusion prevention function and protects internal resources and information, by preventing illegal access from external side.
- 2) TOE detects any illegal events in real time by collecting and analyzing data on user activities on the assets through the network. Based on the result of the analysis, TOE performs intrusion prevention function, which is attained by taking countermeasures to protect system.
- 3) TOE provides the following functions: an intrusion detection function that collects, analyzes, and reacts to, the activity data; a blocking function that blocks packets; a function to maintain and manage up-to-date TSF data such as the configuration of the network intrusion prevention system and security violation events list; a function to identify and authenticate users attempting to access the TOE; and an audit function to record an administrator's activities within the TOE.

TOE is operated for the purpose of protecting the resource of computer networks defined in the security policy. TOE is located at the connection point between an external network such as internet and an organizational internal network in inline mode. TOE performs detection and prevention function of network traffic intrusion and attacks according to security policy. TOE communicates with online update server for updating up-to-date rule and with NTP(Network Time Protocol) server for time synchronization.

ST includes ST introduction, TOE description, TOE security environment, TOE Security objective, IT security requirements, TOE summary specification, PP claims and the rationale.

- 1) "ST introduction" describes identification information about ST and general explanation.
- 2) "TOE Description" gives broad information about the product type, general TOE function, SafezoneIPS Scope and Boundary.
- 3) "TOE Security Environment" provides assumptions on environments where TOE is or will be used, explains threats that may exploit vulnerabilities either willingly or by chance, and describes security policies that are enforced by an organization and that TOE should adhere to, such as rules, procedures, practices, and guidelines.
- 4) "Security Objectives" describes the security objectives for the TOE and the environment required for reacting to threats and for satisfying assumptions and organizational security policies.
- 5) "IT Security Requirements" describes the security requirements for the TOE and IT environment required to meet the security objectives.
- 6) "TOE Summary Specification" defines IT security functions that satisfy identified security functional requirements and describes assurance measures that satisfy the identified security assurance requirements.
- 7) "PP claims" identifies referred protection profiles, refines requirements of the protection profile, and describes PP tailoring that identifies the IT security requirements.
- 8) "Rationale" proves that the security objectives are appropriately defined and are addressing all security problems (stated through threats, assumptions, and organizational security policies), that the security requirements are adequate, and that the dependency of unsatisfied security requirements is unnecessary.

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

1.3 Common Criteria(CC) Conformance

TOE follows Common Criteria and Protection Profile described below.

1) Common Criteria

TOE conforms to Information Protection System Common Criteria(CC) V2.3 (2005-25, the Ministry of Information and Communication).

2) CC Part 2 conformant

The security functional requirements of the TOE conform to the functional components in Part 2.

3) CC Part 3 conformant

The security assurance requirements of the TOE conform to the assurance components in Part 3.

4) Evaluation Assurance Level


Evaluation Assurance Level of the TOE is EAL4.

5) Protection Profile Conformance

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

6) SOF claim

The SOF targeted by the TOE is SOF-medium. The reason is that TOE provides security function to protect Computer resource and information of organization from external threats, and we suppose that attack success possibility of attacker who has lower information, resources is more than lowness.

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

1.4 Glossary

- Object

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

- Attack potential

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

- Administrator Console(SafezoneIPS Security Manager System)

The administrator console provides a Graphical User Interface (GUI) for the TOE administrators and general users to manage the engine, configuration, security policy, and the audit log.

- Strength-of-Function(SOF)

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

- SOF-medium

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

- Iteration

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

- Protected Systems


Asset protected by the security policy of an intrusion prevention system. For example, the protected system of a network-based intrusion prevention system is the network service or resource, and the protected system of a host-based intrusion prevention system is the resource or information saved in the host.

- Security Target(ST)

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

- Protection Profile(PP)

An implementation-independent set of security requirements for a category

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

of TOEs that meet specific consumer needs.

- Human User

Any person who interacts with the TOE.

- User

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

- Selection

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

- Identity

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

- Element

An indivisible security requirement.

- Role

A predefined set of rules establishing the allowed interactions between a user and the TOE(e.g. user, administrator).

- Operation

Making a component react to specific threats or satisfy specific security policy(e.g. iteration, assignment, selection, refinement).

- Threat Agent

An unauthorized user or external IT entity that poses threats to assets such as illegal access, modification, or deletion.

- External IT Entity

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

- Authorized Administrator

A manager who may, in accordance with the TOE security policy(TSP), execute functions of the TOE.

- Authorized User

A user who may, in accordance with the TOE security policy(TSP), perform an operation.

- Authentication Data

Information used to verify the claimed identity of a user.

- Mid-level administrator

A user who is authorized to use all functions provided by the TOE except user info-management, Engine info-management, and audit log deletion



function.

- Low-level administrator

A user who is authorized to use only reference functions and not allowed to use administrative functions. Among the reference functions, he/she can only refer to the engine assigned by the top administrator.

- Assets

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

- Refinement

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

- The Common Criteria for IT security evaluation(CC)

The Common Criteria for IT security evaluation is a Korean version of the International Common Criteria (CC) version 2.3 that was developed to attain a common language and mutual understanding based on the criteria of various countries.

- Organizational Security Policies

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

- Dependency

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

- Subject

An entity within TSC that causes operations to be performed.

- Augmentation

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

- Top Administrator

A user who is authorized to use all functions provided by TOE.

- Component


The smallest selectable set of elements that may be included in a PP and a ST.

- Class

A grouping of families that share a common security objective.

- Target of Evaluation(TOE)

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

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

- Evaluation Assurance Level(EAL)

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

- Assignment

One of the CC operations. The specification of an identical parameter in a component.

- Extension

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

- Dual-Homed Type

Type of installing a firewall that has two interfaces between external and internal network but does not have a routing function.

- NTP(Network Time Protocol)

NTP is a protocol which is used to synchronize a clock time among computers connected to networks.

- TOE Security Functions(TSF)

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

- TOE Security Policy(TSP)

A set of rules that regulate the administration, protection, and distribution of assets within a TOE.

- TSF Data

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

- TSF Scope of Control(TSC)

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

- Gateway

connection between computer networks.

- PCI(Peripheral Component Interconnect)

PCI is an interconnect system among devices attached to extended-slot located closely with micro-processor for high speed operation.

- PICS(platform for Internet content selection)

PICS is a standard in HTML which enables web developer to insert a HTML tag that represents information of their own web site 's contents. This is mainly used for keeping away children from accessing to contents for



adults. Web browsers and filtering software read PICS tag, then decide to show the site or not according to predefined content level configured by parent(or manager, teacher, the director of a library, etc)

- Public Time Server

In case that many computers are connected with networks in office, school, company, public time server is a time server to provide time information for time synchronization from reliable organization, not from own time server.

- SEED


Standardized in 1999 (TTA.K0-12.0004, '99. 9), SEED is a symmetric encryption algorithm of 128 bits key size that was developed by Korea Information Security Agency and ETRI to protect information and privacy in the private sector.

SEED has the following characteristics:

- DES-like(Feistel) structure
- The size of input/output bit is fixed 128-bit
- The size of key bit is fixed 128-bit
- Adapting a strong round function against known attacks
- Four 8X8 S-boxes
- Mixed Xor and Modular addition operations
- The number of rounds is fixed 16

- SHA-1

Developed by NIST, SHA is an algorithm defined in Secure Hash Standard (SHS). SHA-1 is the revision of the original SHA published in 1994 with corrected errors left in SHA. This architecture is very similar to the MD4 hash functions developed by Rivest. Also defined in ANSI X9.30, SHA-1 converts messages shorter than 264bits to abbreviated messages of 160bits. Although somewhat slower than MD5, this algorithm provides more protection when mass message abbreviations are attacked by violent collisions and inversions.

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

1.5 References

- [1] Network Intrusion Prevention System Protection Profile V1.1, Dec. 21, 2005, KISA
- [2] Software Process Standard, Apr. 1999, LG Electronics Information Division, R&D Center
- [3] Common Criteria for Information Technology Security Evaluation, Aug. 2005, (Korean, Version 2.3)
- [4] Common Methodology for Information Technology Security Evaluation, Aug. 2005, (Korean, Version 2.3)
- [5] SafezoneIPS V1.0(SZ5XU) Functional Specification_20070314_V1.00.04
- [6] SafezoneIPS V1.0(SZ5XU) Basic Design_20070205_V1.00.02
- [7] SafezoneIPS V1.0(SZ5XU) Detailed Design_20070314_V1.00.02
- [8] SafezoneIPS V1.0(SZ5XU) Installation Guide_20060811_V1.00.01
- [9] SafezoneIPS V1.0(SZ5XU) Administrative Guide_20060811_V1.00.01

2. TOE Description

Product Type and environment are described for helping to understand security requirements here.

2.1 Product Type

SafezoneIPS is a unified network seecurity solution(hardware-type) which provides IPS, Firewall, QoS, Mail Filtering function. That is, SafezoneIPS is a unified security system which enables efficient network resource usage by protecting the internal IT asset of the target network not only from direct attacks that exploit vulnerabilities but also from any illegal attacks that can shut down the network by increasing network traffic load using DOS attack, and by controlling network bandwidth.

- 1) TOE performs intrusion prevention function and protects internal resources and information, by preventing illegal access from external side.
- 2) TOE detects any illegal events in real time by collecting and analyzing data on user activities on the assets through the network. Based on the result of the analysis, TOE perfoms intrusion prevention function, which is attained by taking countermeasures to protect system.
- 3) TOE provides the following functions: an intrusion detection function that collects, analyzes, and reacts to, the activity data; a blocking function that blocks packets; a function to maintain and manage up-to-date TSF data such as the configuration of the network intrusion prevention system and security violation events list; a function to identify and authenticate users attempting to access the TOE; and an audit function to record an administrator 's activities within the TOE.

TOE is operated for the purpose of protecting the resource of computer networks defined in the security policy. TOE is located at the connection point between an external network such as internat and an organizational internal network in inline mode. TOE performs detection and prevention function of network traffic intrusion and attacks according to security policy. TOE communicates with online update server for updateing up-to-date rule and with NTP(Network Time Protocol) server for time synchronization.

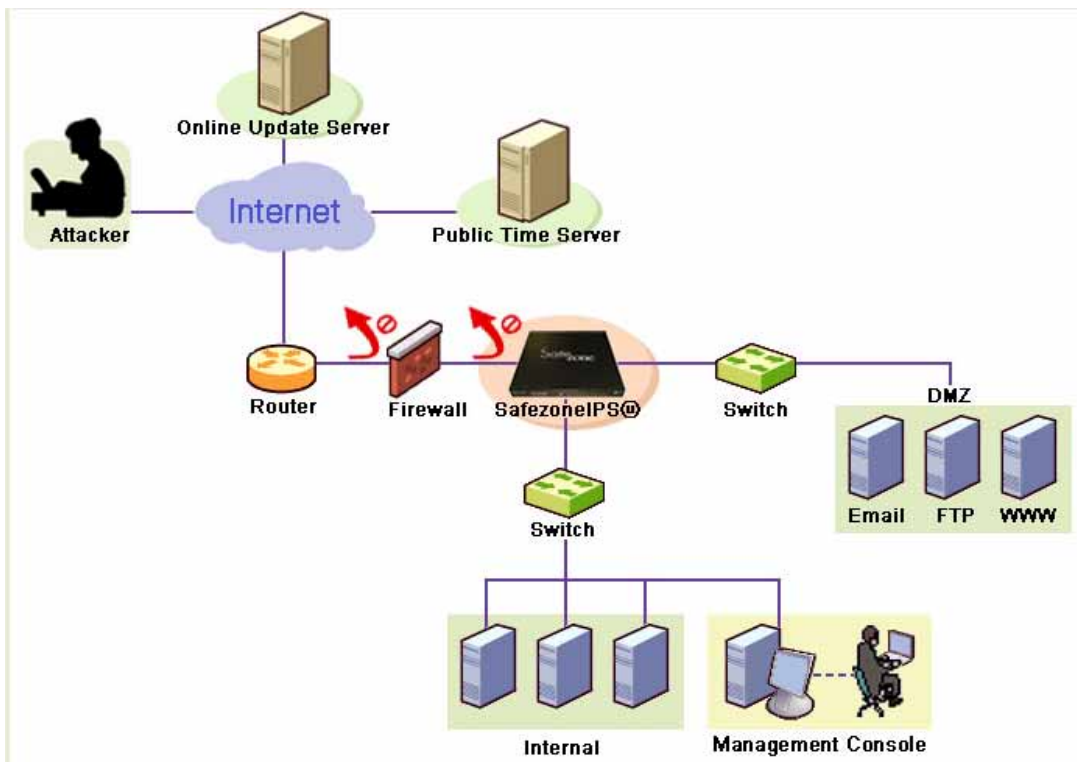
2.2 TOE Environment

2.2.1 TOE Network Environment

SafezoneIPS is located at the connection point between an external network such as internet and an organizational internal network in inline mode. And Administrator can manage SafezoneIPS in local or remote area with Management Console. SafezoneIPS is a unified network seecurity solution(hardware-type) which provides IPS, Firewall, QoS, Mail Filtering function.

2.2.1.1 Bridge mode network configuration

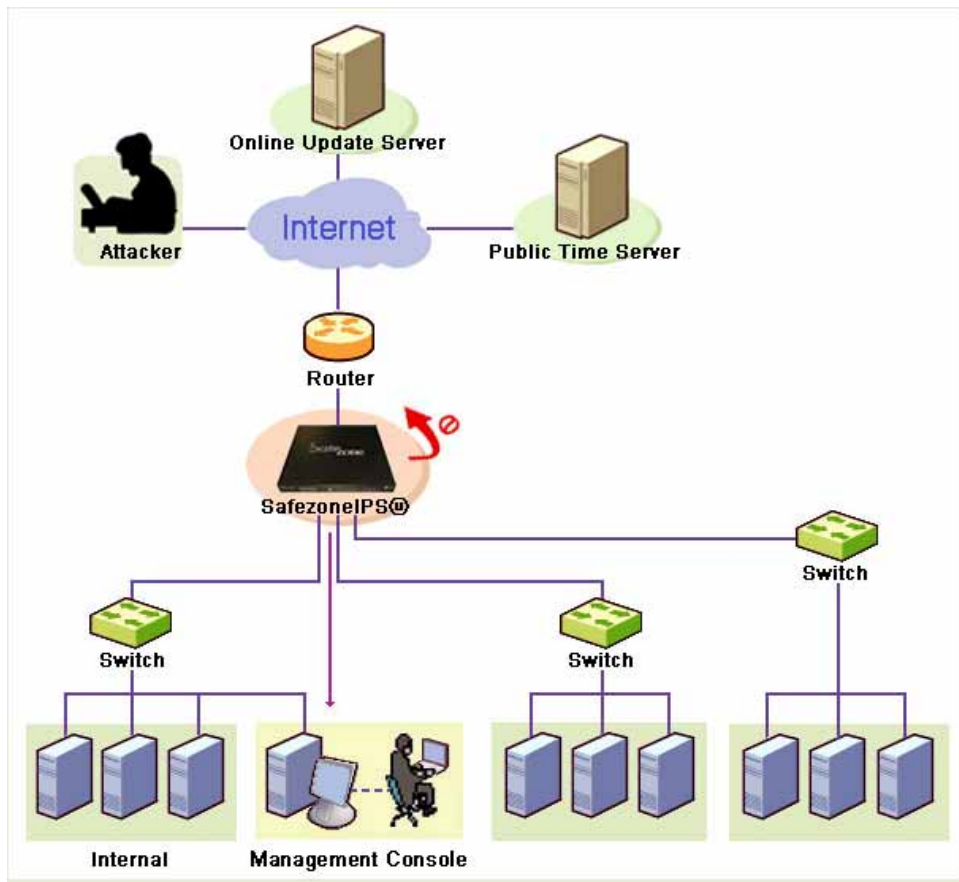
▶ Network configuration when Firewall function is not used.



[Figure 2-1] Bridge mode Network configuration-1

SafezoneIPS is installed behind firewall in Bridge Mode Network Configuration. Only using IPS function, SafezoneIPS can protect interal assets by preventing intrusion from hacker which is not filtered in Firewall.

▶ Network configuration when Firewall function is used.

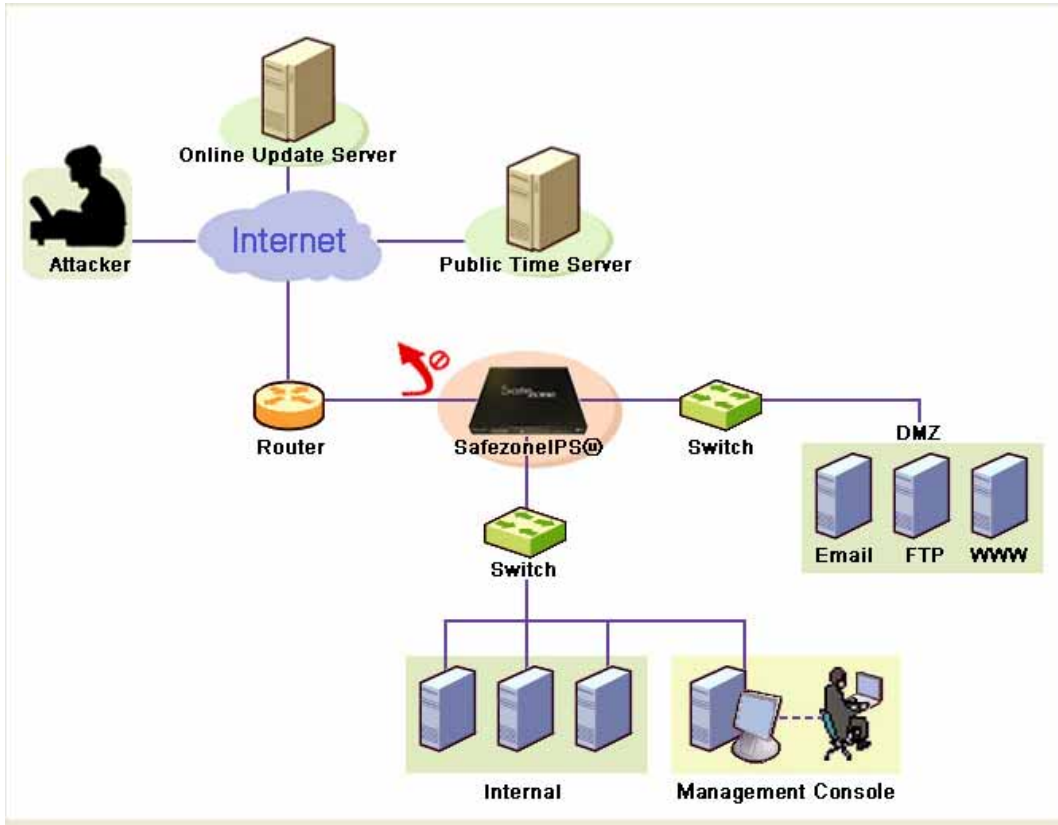


[Figure 2-2] Bridge mode Network configuration-2

Using several(2, 4, 6, 8) ports provided by SafezoneIPS , internal network can be divided several band. Firewall function can be performed with IPS function and SafezoneIPS blocks harmful traffic occurred in internal network.

2.2.1.2 Gateway mode Network Configuration

▶ Network configuration when Firewall function is used.

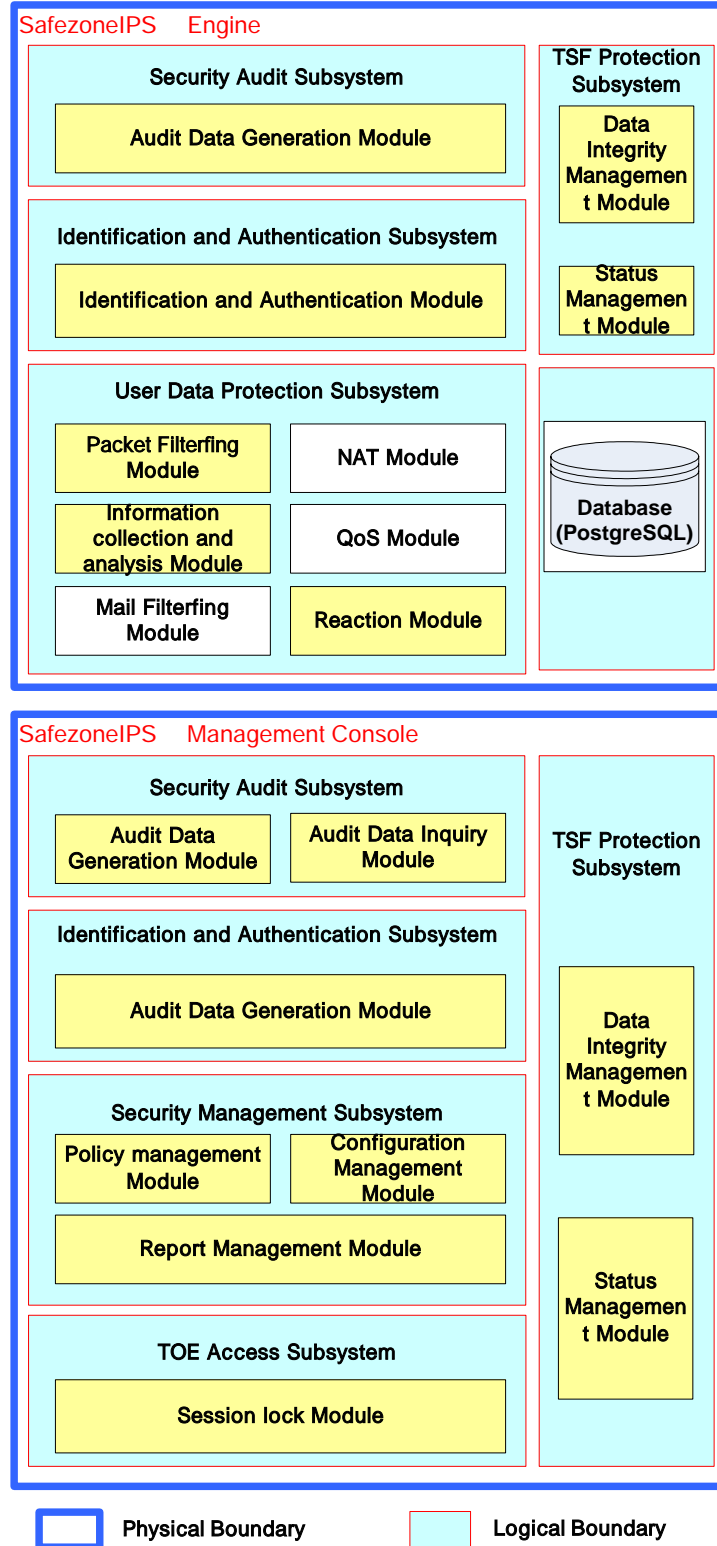


[Figure 2-3] Gateway mode Network Configuration


SafezoneIPS is installed in Gateway mode performing both IPS function and Firewall function without separate firewall in above configuration. SafezoneIPS performs Gateway function instead of firewall and blocks harmful traffic occurred in network.

2.2.2 TOE Product Configuration

TOE consists of Engine and Management Console like below figure.



[Figure 2-4] TOE Basic Configuration

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

SafezoneIPS Engine consists of Security Audit Subsystem, User Data Protection Subsystem, Identification and Authentication Subsystem, TSF Protection Subsystem, logically.

Management Console consists of Security Audit Subsystem, Identification and Authentication Subsystem, Security Management Subsystem, TOE Access Subsystem, TSF Protection Subsystem.

2.3 TOE Scope and Boundary

2.3.1 Physical Scope and Boundary

SafezoneIPS consists of a dedicated hardware system which provides Unified Network Security function(IPS, Firewall, NAT, QoS) and Management Console. The [Table 2-1] below summarizes the hardware specification of them:

Category		Item	Specification
SafezoneIPS Engine	H/W	CPU	M-Celeron 1.6G or more M-Centrino 1.66G or more Pentium 4 3.0 or more
		MEM	512 MB * 1 or more
		HDD	S-ATA 80 GB or more
		OS	Self OS(SZOS V1.1)
		Data management	PostgreSQL Server
		Ethernet Port (N/W I/F)	2/4/6/8 Ports (10/100/1000)
Management Console	H/W Recommendation	CPU	2.4Ghz 1 or more
		MEM	1GB or more
		HDD	72GB * 1 or more
		OS	Windows XP Profesional
		N/W Interface	1 Port or more

[Table 2-1] SafezoneIPS Hardware specification

If H/W bought from LG N-Sys, specification of H/W is as follows.

Division		Specification	
SafezoneIPS Engine	52U H/W	CPU	M-Celeron 1.6G
		MEM	512 MB
		HDD	S-ATA 80 GB
		OS	Self OS(SZOS V1.1)
		Data management	PostgreSQL Server
		Ethernet Port	Using 2 Ports (10/100/1000)
	54U H/W	CPU	M-Centrino 1.66G
		MEM	1GB
		HDD	S-ATA 80 GB
		OS	Self OS(SZOS V1.1)
		Data management	PostgreSQL Server
		Ethernet Port	Using 4 Ports (10/100/1000)
	56U H/W	CPU	M-Centrino 1.66G
		MEM	1GB
		HDD	S-ATA 80 GB
		OS	Self OS(SZOS V1.1)

		Data management	PostgreSQL Server
		Ethernet Port	6 Ports 4 ports (10/100/1000) 2 ports(Giga Fiber)
	58U H/W	CPU	Pentium 4 3.0
		MEM	1GB
		HDD	S-ATA 80 GB
		OS	Self OS(SZOS V1.1)
		Data management	PostgreSQL Server
		Ethernet Port	8 Ports (10/100/1000)
Management Console	H/W Recommendation	CPU	2.4Ghz 1 or more
		MEM	1GB or more
		HDD	72GB * 1 or more
		OS	Windows XP Profesional or more
		N/W Interface	1 Port or more

2.3.2 Logical Scope and Boundary

The followings are the security functions of TOE and descriptions:

- Security Audit

This function collects and analyzes the system usage record to check whether the system is operating stably and efficiently. The audit result is used for detecting or blocking intrusions on the computer system and for detecting misuse of the system.

- User Data Protection

This function controls the flow of network data according to the permission or blocking rule to protect the target network that is to be protected from internal or external attackers. Also it collects information to detect intrusion and react to an intrusion in case it is identified, and stores the analysis result so that the administrator can check.

- Identification and Authentication

Identification and authentication of SafezoneIPS provides the function that only authorized external IT entity and administrator can access to TOE. In order to control the access to SafezoneIPS perfectly, every access attempt through an administrator interface are examined to identify and authenticate an appropriate administrator. Only authorized administrators are allowed to access key functions that are essential to the regular



operation of SafezoneIPS such as changing, deleting and adding policies and retrieving log files.

- Security Management

Security Management refers to managerial functions such as retrieving or setting the attributes and information of various functions SafezoneIPS provides and checking the status of such data. Security Management provides various managerial functions such as starting or ending a security audit, retrieving and changing detection policies, retrieving and setting a security violation list, retrieving and setting rules for reacting to security violation events, setting the capacity of audit data, and setting and changing conditions required for preventing the loss of audit data.

- TSF Protection

TSF Protection provides a regular check function to assure that the TSF is properly operating. It performs checking the main component running on the TOE system when initially started, periodically during normal operation. In case of abnormal operation, it executes the function of a component again. And it protects the TOE data and functions by checking the integrity of TOE data and programs.

- Resource Utilization

This function ensures safe operation of the TOE by periodically monitoring H/W failures such as CPU, memory.

- TOE Access

If the TOE is accessed by an authorized administrator but remains inactive for a certain period of time, the interacting session will be locked on the basis of the identification and authentication in order to protect the TOE during the time.

- Trusted Path/Channels

In cases where components of the TOE interact remotely through internal communication channels, the nodes of the other side are identified and authenticated to ensure safe channels between TSFs.

The following function can be performed excluded from the scope of TOE.

- 1) NAT(Network Address Translation) function in Firewall Configuration
- 2) QoS function

- 3) Application gateway related to SMTP.
 - Mail Decoding function
 - Attached file decompress function
 - Content Filtering against tile, contents
 - Anti-Virus function
 - Spam Mail Filtering function
- 4) Configuration function related to network.
 - Routing configuration function
 - Static ARP configuration function
 - Network Interface Card address configuration function
 - Network Interface Card environment configuration (Auto Nego, Speed, Duplex) function
 - VLAN function supporting 802.1q
 - Secondary IP configuration function
- 5) Network service function
 - DHCP server functon to assign IP addresses dynamically to user.
 - Routing function to give and to receive routing information with other network devices
- 6) Integrated console configuration function
 - Alarm function to check the status of a device
 - Monitoring function to check the resource status of a device.
 - Binary update function to update engine binaries synchronously in remote.
 - Function to apply a security policy classified by group.
 - Alert function with e-mail or SMS to administrator when an error occurred.
- 7) Smart update function
 - harmful sites DB update function
 - Anti-Virus DB update function
 - Binary Update function
- 8) Audit Log storage
 - PostgreSQL DBMS to store audit log.
- 9) NTM(Network Traffic Monitoring) function

3. TOE Security Environment

This chapter describes the TOE security environment.

3.1 Assumption

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.Reliable TIMESTAMP	Added
	A.Secure Update Server	Added
	A.Secure Database	Added

[Table 3-1] Identification of assumptions

- A.Physical Security

The TOE is located in physically secure 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 decrease of services, the new changes are immediately noted and security policies are configured in accordance with the TOE operational policy to maintain the same level of security as before.

- A.Trusted Administrator


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

- A.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 Connection Point

The TOE is installed and operated on a network and separates the network into external and internal network. Information can not flow between the

 LGN-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
--	---	---

two without passing through the TOE.

- A.Reliable TIMESTAMP

To keep reliable TIMESTAMP function, NTP Server(Public Time Server) provides TOE with reliable TIMESTAMP. If TOE cannot get time information from Public Time Server, TOE get time information from system.

- A.Secure Update Server

Secure Update Server provides TOE with the latest attack rule, so TOE can keep the latest attack rule.

- A.Secure Database

TOE can save, search and keep audit log through secure database.

3.2 Threats

Threats are categorized into threats to the TOE and threats about the TOE operational environment. Main assets to be protected by TOE is computer resources and network services of internal networks or DMZ. External threat agents access to computer resources of the organization illegally and attack to exhaust availability. Threat agent is generally computer user or IT entity access to internal computer in external area. We suppose that threat agent has low level of technical knowledge, resource, motive and it has low success possibility to find malicious vulnerability. Using apparent vulnerability information, attacker can get attack tools and malicious vulnerability information about Operation system and applications through internet, get information illegally and damage computer resources. TOE preserve assets from threat against these apparent vulnerability.

Category	Item
Threat to the TOE	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.Unauthorized TSF Data Modification	
Threat to the TOE operational environment	TE.Poor Administration
	TE.Distribution and Installation


[Table 3-2] Identification of threats

3.2.1 Threats to the TOE

The assets to be protected by the intrusion prevention system include the TOE itself and the assets protected by the TOE.

The threats to the TOE are described below.

- T.Masquerade

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

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

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

- T.Spoofing IP Address

A threat agent may illegitimately gain access to the internal network by spoofing source IP address as an internal IP address.

- T.Unauthorized TSF Data Modification

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

A threat agent may attack by launching a buffer overflow attack, thus resulting in unauthorized modification of the TSF data.

3.2.2 Threats 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
Security Policy	P.Audit
	P.Secure Administration

[Table 3-3] Identification of organizational security policies

- P.Audit

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

- P.Secure Administration

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

4. TOE 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 nontechnical/procedural means.

Category	Item	Remark
Security objectives for the TOE	0.Availability	
	0.Audit	
	0.Administration	
	0.Abnormal Packet Screening	
	0.DoS Attack Blocking	
	0.Identification	
	0.Authentication	
	0.Information Flow control	
	0.TSF Data Protection	
Security objectives for the environment (Object about 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.Reliable TIMESTAMP	Added
	OE.Secure Update Server	Added
OE.Secure Database	Added	

[Table 4-1] Identification of TOE security objectives


4.1 Security Objectives for the TOE

The followings are the security objectives that must be directly managed by the TOE.

- 0.Availability

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

- 0.Audit

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

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

- 0.Administration

The TOE must provide administrative tools to enable authorized administrators to effectively manage and maintain the TOE.

- 0.Abnormal Packet Screening

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

- 0.DoS Attack Blocking

When an attacker abnormally uses service assets of a computer, the TOE must block the use to protect the network service of the protecting computer for normal users.

- 0.Identification

The TOE must identify all external IT entities subject to information flow control of the TOE and the users who want to access to the TOE.

- 0. Authentication

The TOE, after identifying an administrator, must authenticate the administrator 's identity before granting an access to the TOE.

- 0.Information Flow Control

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

- 0.TSF Data Protection

The TOE must 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 nontechnical/procedural means:

- OE.Physical Security

The TOE must 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 must be immediately noted and security policies configured in accordance with the TOE operational policy to maintain the same level of security as before.

- OE. Trusted Administrator

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

- OE. Secure Administration

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

- OE. 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.

- 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 is done through the TOE.

- OE. Vulnerability List Update

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

- OE. Reliable TIMESTAMP


The IT environment of the TOE should be provided with a reliable Timestamp from the NTP(Network Time Protocol) Public Time Server which conforms to RFC 1305 or from the OS(When receiving time information from Public Time Server, OS system time information is used).

- OE. Secure Update Server

Update Server locates in External area of the TOE and must be secure to maintain the latest attack rule.

- OE. Secure Database

Database is used to store and to search audit log, and must be configured, managed, used in secure manner by authenticated administrator.

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

5. IT Security Requirements

The security functional requirements defined in this document have selected related functional components drawn from CC Part 2 to satisfy the security objective identified in the previous chapter.

The intended level of the TOE strength of function (SOF) is SOF-medium.

Supposing that the function is to provide adequate protection for organizational computer resources and information from external threats, and that the expected attack potential of the threat agent is to be medium, the required strength of function (SOF) is defined as SOF-medium.

The targets of SOF requirements are “ FIA_UAU.1 Timing of authentication ” that uses general password mechanism and “ FPT_TST.1 TSF Testing ” that uses SHA-1 as a hash algorithm for integrity authentication, both from the security functional classes in Part 2.

The conventions used in this document are consistent with the Common Criteria for IT Security Evaluation.

Operations permitted to be performed on security functional requirements are iteration, selection, refinement, and assignment.

- **Iteration**

Allows a component to be used more than once with varying operations. The result of iteration operation is indicated by appending the repeated number in parenthesis, (repeated number), following the component identifier.

- **Selection**

Used to select one or more items provided by the Common Criteria for IT Security Evaluation when stating a requirement. The result of selection operation is indicated in *underlined italics*.

- **Refinement**

Used to add details to and thus further restricts a requirement. The result of refinement operation is indicated by **bold text**.


- **Assignment**

Used to assign a specific value to an unspecified parameter (e.g. password length). The result of assignment operation is indicated by putting the value in square brackets, [assignment_value].

5.1 TOE Security Functional Requirements

The TOE security functional components addressed in this document are summarized in the following table.

Security functional class	Security functional component
Security Audit	FAU_ARP.1 Security alarms
	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAA.1 Potential violation analysis
	FAU_SAR.1 Audit review
	FAU_SAR.3 Selectable audit review
	FAU_SEL.1 Selective audit
	FAU_STG.1 Protected audit trail storage
	FAU_STG.3 Action in case of possible audit data loss
	FAU_STG.4 Prevention of audit data loss
User data protection	FDP_IFC.1(1) Subset information flow control(1)
	FDP_IFC.1(2) Subset information flow control (2)
	FDP_IFF.1(1) Simple security attributes(1)
	FDP_IFF.1(2) Simple security attributes (2)
Identification and authentication	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1(1) User attribute definition(1)
	FIA_ATD.1(2) User attribute definition (2)
	FIA_UAU.1 Authentication
	FIA_UAU.7 Protected authentication feedback
	FIA_UID.2(1) User identification before any action(1)
FIA_UID.2(2) User identification before any action (2)	
Security Management	FMT_MOF.1(1) Management of security functions behavior(1)
	FMT_MOF.1(2) Management of security functions behavior (2)
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_MTD.2 Management of limits on TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Protection of the TSF	FPT_AMT.1 Abstract machine testing
	FPT_FLS.1 Failure with preservation of secure state
	FPT_ITT.1 Basic protection of TSF data for internal transmission
	FPT_RVM.1 Non-bypassability of the TSP
	FPT_SEP.1 TSF domain separation
	FPT_STM.1 Reliable time stamps
	FPT_TST.1 TSF testing
Resource utilization	FRU_FLT.1 Degraded fault tolerance
	FRU_RSA.1 Maximum quotas
TOE access	FTA_SSL.1 TSF-initiated session locking
	FTA_SSL.3 TSF-initiated termination

 LG N-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

Trusted path/channel	FTP_ITC.1 Inter-TSF trusted channel
----------------------	-------------------------------------

[Table 5-1] Security functional requirements

5.1.1 Security Audit

5.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [audit log generation and the action to alert the authorized Administrator : E-Mail, To display audit log on Management Console] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis


5.1.1.2 FAU_GEN.1 Audit data generation

Hierarchical to : No other components

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

- a) Start-up and shut-down of the audit functions
- b) All auditable events for the *minimum* level of audit

Component	Auditable event	Additional audit record
FUA_ARP.1	Reaction by imminent security violation	Alarmed or not
FAU_SAA.1	Automatic reaction by start-up and shutdown of analysis mechanism	Alarmed or not
FAU_SEL.1	Change of audit configuration occurred during audit collection function is performing.	Administrator identification ID
FDP_IFF.1(1)	All decisions on requests for information flow	Identification information of subject and object
FDP_IFF.1(2)	All decisions on requests for information flow	Identification information of subject and object
FIA_AFL.1	The number of authentication trial failure reached to limits and taken reaction, if appropriate, recover to normal state.	User identity provided to the TOE
FIA_UAU.1	Unsuccessful use of the authentication mechanism	User identity provided to the TOE
FIA_UID.2(1)	Unsuccessful use of the user identification mechanism, including the user identity provided.	User identity provided to the TOE

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

FIA_UID.2(2)	Unsuccessful use of the user identification mechanism, including the user identity provided.	User identity provided to the TOE
FMT_SMF.1	Use of management function	User identity provided to the TOE
FMT_SMR.1	Modification to the group of users that are part of a role	Identity of an authorized administrator
FPT_STM.1	Changes to the time	Identity of an authorized administrator who performs operation
FRU_FLT.1	All errors detected by TSF	-
FRU_RSA.1	Rejection of assignment operation by resource limit	-
FTA_SSL.1	Locking of an interactive session by the session locking mechanism, Successful unlocking of interactive session	-
FTA_SSL.3	Locking of an interactive session by the session locking mechanism	-
FTP_ITC.1	Failure of the trusted channel functions, Identification of the initiator and target of failed trusted channel functions	Identification of the initiator and target of failed trusted channel functions: Source IP, Port of Subject

c) Added audit data

Component	Auditable event	Additional audit record
FMT_MSA.1	All modifications of the values of security attributes	Security attribute value
FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data value
FMT_MTD.2	All modifications to the limits on TSF data	Modified TSF data limit
FPT_TST.1	Integrity errors, the action taken when an integrity error is identified and its result	Target and result of integrity check

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

- a) Date and time of the event, type of event, subject identity, and the result of the event(success or failure)
- b) For each audit event type, [the following information related to audit event] based of the auditable vent definitions of the functional components included in the Protection Profile(PP)/Security Target(ST)

Division	Auditable event information
General audit data	Audit log Data and time Audit Object Audit Subject Audit Contents Audit Type Console Type Audit record IP
Audit data about Intrusion detection/prevention	Name of intrusion Detection time Saved time Source IP Source Port Source MAC Address Target IP Target Port Target MAC Address Protocol Engine Reaction Attack times Attack direction Network name Saving type File name Risk level Attack Code

Dependencies : FPT_STM.1 Reliable TIMESTAMPS

5.1.1.3 FAU_GEN.2 User identity association


Hierarchical to : No other components

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

Dependencies : FAU_GEN.1 Audit data generation

FIA_UID.1 Identification

5.1.1.4 FAU_SAA.1 Potential violation analysis

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

Hierarchical to : No other components

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

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

a) Accumulation or combination of [analysis of abnormal protocol packets, trial of network DoS, and anomaly detection based on time and traffic loads] known to indicate a potential security violation;

b) [no additional rules]

Dependencies : FAU_GEN.1 Audit data generation

5.1.1.5 FAU_SAR.1 Audit review

Hierarchical to : No other components

FAU_SAR.1.1 The TSF shall provide [authorized administrator] with the capability to read [all audit data] from the audit records.


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

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.6 FAU_SAR.3 Selectable audit review

Hierarchical to : No other components

FAU_SAR.3.1 The TSF shall provide the ability to perform searching, sorting, ordering of audit data based on [in case of audit log, create date and time, subject and object, type; incase of attack detection/prevention log, create date and time, saving date and time,

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

subject and object, log content, reaction].

Dependencies : FAU_SAR.1 Audit review

5.1.1.7 FAU_SEL.1 Selective audit

Hierarchical to : No other components

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes;

- a) event type
- b) [No attributes]

Notice: The top Administrator and the middle administrator decide to create audit log by security policy or not, and auditable event is included or excluded according to decided policy.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 TSF Management of data

5.1.1.8 FAU_STG.1 Protected audit trail storage

Hierarchical to : No other components


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

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

Dependencies : FAU_GEN.1 Audit data generation

5.1.1.9 FAU_STG.3 Reaction in case of possible audit data loss

Hierarchical to : No other components

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

FAU_STG.3.1 The TSF shall take [action to generate and store audit data and to send an email to address configured by an authorized administrator] if the audit trail exceeds [% capacity configured by an authorized administrator(pre-defined limit : 80%)]

Dependencies : FAU_STG.1 Protected audit trail storage

5.1.1.10 FAU_STG.4 Prevention of audit data loss

Hierarchical to : FAU_STG.3

FAU_STG.4.1 The TSF shall overwrite the oldest audit record and [achieve the space for audit storage by deleting the oldest backup log, send an E-mail to address configured by authorized administrator].

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.2 User Data Protection

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


Hierarchical to : FDP_IFC.1

FDP_IFC.1.1 The TSF shall enforce [**Packet filtering policy**] on list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP.

- a) [subjects : unauthenticated external IT entities that send information;
- b) information : Network packet sent through the TOE from one subject to another;
- c) operation : pass information when allowing rules exist].

Dependencies : FDP_IFF.1 Simple security attributes

notice : 'policy to deny all' is transcribed as 'packet filtering policy' in ST.

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

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

Hierarchical to : FDP_IFC.1

FDP_IFC.1.1 The TSF shall enforce the [**Intrusion prevention policy**] on list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP.

- a) [subjects : unauthenticated external IT entities that send information;
- b) information : Network packet sent through the TOE from one subject to another;
- c) operation : block information when blocking rules exist].

Dependencies : FDP_IFF.1 Simple security attributes

notice : 'policy to allow all' is transcribed as 'intrusion prevention policy' in ST.

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

Hierarchical to : No other components

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

- a)subject list : unauthenticated external IT entities that send/receive information;
- b)information list : network packet sent through the TOE from one subject to another
- c) security attributes : Subject identifier(IP address information, port information, MAC information), object identifier(TCP/IP header information including protocol, IP information, port information)

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled

subject and controlled information via controlled operation if the following rules hold; [Information flow of network packet is blocked basically by defined packet filtering policy, but the network packet consistent with the security attributes of TCP/IP header information including protocol, IP information, port information is to be allowed.]

FDP_IFF.1.3 The TSF shall enforce the [none]

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

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on [audit log transmission occurred in TOE, network packet for TSF execution like sending rules].

FDP_IFF1.6 The TSF shall explicitly deny an information flow based on [the following rules].

- a) Rules does not exist described in FDP_IFF.1.2
- b) Information flow security policy generated by authorized administrator does not exist


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

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

Hierarchical to : No other components

FDP_IFF.1.1 The TSF shall enforce the [intrusion prevention policy] based on at least the following types of subject attributes and information security attributes; [list of subjects and information controlled under the indicated SFP, and for each security attributes].

- a)subject list : unauthenticated external IT entities that send/receive information;
- b)information list : network packet sent through the TOE from one subject to another
- c) security attributes : Subject identifier(IP address information, port

 LG N-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

information), object identifier(TCP/IP header information including protocol, IP information, port information, Fragmentation), not encrypted contents information included in network packet.

FDP_IFF.1.2 The TSF shall block an information flow between a controlled subject and controlled information via controlled operation if the following rules hold; [Information flow of network packet is blocked basically by defined intrusion prevention policy, but the network packet consistent with the security attributes of TCP/IP header information (including protocol, IP information, port information, fragmentation), and that of contents information(which is not encrypted) included in network packet is to be blocked.]

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


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

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

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

- a)[The TOE shall block a request for network access when the information from external IT entities has internal subject IP addresses.
- b) The TOE shall block a request for network access when the information from internal IT entities has external subject IP addresses
- c) The TOE shall block a request for network access when the information from external IT entities has broadcasting subject IP addresses.
- d) The TOE shall block a request for network access when the information from external IT entities has looping subject IP addresses.
- e) The TOE shall block a request for network access when the information from external IT entities has abnormal packet structures.
- f) [no additional rules]]

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

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

5.1.3 Identification and Authentication

5.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components

FIA_AFL.1.1 The TSF shall detect when *[1 to 10(initial value : 3)] times (configured by authentication administrator)* unsuccessful authentication attempts occur related to [the authentication of TOE use for the administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, The TSF shall perform [the termination of administrator console, the generation of audit log, the prevention of the user authentication during the time(1 hour to 24 hours, initial value : 1 hour) defined by authorized administrator, disconnection when engine and management console fail to authenticate each other].

Dependencies : FIA_UAU.1 Authentication

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

Hierarchical to : No other components

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

- a) IP address
- b) { port information, MAC address } user security attribute

Dependencies : No dependencies

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

Hierarchical to : No other components

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

a) identifier

b) { password, user level, user name, cell phone number, e-mail address }
use security attribute

Dependencies : No dependencies

5.1.3.4 FIA_UAU.1 Authentication

Hierarchical to : No other components

FIA_UAU.1.1 The TSF shall allow [the request for login procedure(the request for login screen for authentication), and authentication procedure for connection between engine and management console] to be performed by **the administrator** before the **administraor** is authenticated.

FIA_UAU.1.2 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions than those specified in FIA_UAU.1.1 on behalf of that **administrator**.


Dependencies : FIA_UID.1 Identification

5.1.3.5 FIA_UAU.7 Protected authentication feedback

Hierarchical to : No other components

FIA_UAU.7.1 The TSF shall provide only [the result of authentication (success/failure), and asterisks, for each password character to be displayed through the GUI, not the original character] to the **administrator** while the authentication is in progress.

Dependencies : FIA_UAU.1 Authentication

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

5.1.3.6 FIA_UID.2(1) User identification before all action (1)

Hierarchical to : FIA_UID.1

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

Dependencies : No dependencies

5.1.3.7 FIA_UID.2(2) User identification before all action (2)

Hierarchical to : FIA_UID.1

FIA_UID.2.1 The TSF shall require **each administrator** to identify himself/herself before allowing any other TSF-mediated actions on behalf of that **administrator**.

Dependencies : No dependencies

5.1.4 Security Management


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

Hierarchical to : No other components

FMT_MOF.1.1 The TSF shall restrict the ability to stop and to start [the following function list] to [authorized administrator].

- a) User management function
- b) Security management access function
- c) Auto online update function
- d) Connect to engine, disconnect to engine, stop engine functions
- e) Auto integrity check function
- f) Auto time synchronization function
- g) Auto backup management function

Dependencies : FMT_SMF.1 Specification of management functions

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

FMT_SMR.1 Security roles

notice: Top administrator and middle level administrator can perform.

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

Hierarchical to : No other components

FMT_MOF.1.1 The TSF shall restrict the ability to determine and to change an action on [the following function list] to [authorized administrator].

- a) Selective generation of audit log
- b) Manual online update function
- c) Management function of security configuration information
- d) Report generation function on audit result
- e) Manual integrity check function
- f) Manual time synchronization function
- g) Management function of manual backup
- h) Management function of security violated event list

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

notice: Top administrator and middle level administrator can perform. But report generation function on audit result can be performed by all administrators

5.1.4.3 FMT_MSA.1 Management of security attributes

Hierarchical to : No other components

FMT_MSA.1.1 The TSF shall enforce the [packet filtering policy, intrusion prevention policy] to restrict the ability to query, modify, delete, [create] [the following] security attributes to the [authorized administrator].

- a) Security attributes management of packet filtering policy

Security attributes	explanation	action
priority	Priority of packet filtering policy	modify, query
Access policy	Code name of attack	modify, query
Source IP	Source IP of packet	modify, query, delete, create
Source port	Source port of packet.	modify, query
Target IP	Target IP of packet	modify, query, delete, create
Target port	Target port of packet.	modify, query
protocol	Network protocol	modify, query
interface	Network interface	modify, query
Use time	Applied time of packet filtering policy	modify, query, delete, create
log	To generate a log or not	modify, query

b) Security attributes management of intrusion prevention policy

Security attributes	explanation	action
Attack name	Define attack name which presents the attribute of attack	modify, query, delete, create
Attack code	Code name of attack.	query
Detection contents	Character set which presents the attribute of attack in Payload part except header of packet.	modify, query, delete, create
Protocol	Protocol of packet	modify, query
Risk level	Risk level of attack.	modify, query
Type of saving	Type of saving in case of reaction is log. (MSG / FULL)	modify, query
Attack direction	Defines a flow of a packet	modify, query
Source IP	Source IP of attack packet	modify, query, delete, create
Target IP	Target IP of attack packet	modify, query, delete, create
Source port	Source port of attack packet. Range can be configured	modify, query, delete, create
Target port	Target port of attack packet. Range can be configured	modify, query, delete, create
Filter type of Duplicated log	Generated log can be judged as a same duplicated log. Administrator can select one of 4 conditions; same source IP, same target IP, same attack name, or all of them is the same.	modify, query
The number of times of duplication	Before judged as duplication, minimum number to store database and to print in screen.	modify, query
Duplication time	Based on selected filter type, period to judge as same log	modify, query
reaction	When judged as an attack, reaction can be configured. <ul style="list-style-type: none"> - Log - Sound - Syslog - PacketDrop - E-Mail - SNMP Trap 	modify, query

RateLimit	An inflow of packet per second for dynamic attack policy	modify, query
TTL	TTL value for packet integrity	modify, query
IP status	Source/Target IP for RateLimit policy is changed or not	modify, query
Base number of attacks	Base number of attacks by 10 seconds for RateLimit policy	modify, query
Base number of packets	Base number of packets for RateLimit policy	modify, query

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

notice: security violated event list which is provided by default can not be modified.

5.1.4.4 FMT_MSA.3 Static attribute initialization

Hierarchical to : No other components

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

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

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

5.1.4.5 FMT_MTD.1 Management of TSF data

Hierarchical to : No other components

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, [create] [the following function] to [the authorized administrator].

Division	Configuration information	Action
User authentication	The admitted number of continuous fail of authentication	modify, query
	Management console lock time	modify, query
	Inactive time for locking of management console session	modify, query
Mail information	Mail server IP address	modify, query, delete, create
	Sender mail address	modify, query, delete, create
	Receiver mail address	modify, query, delete, create
Auto log backup	Limit of disk usage	modify, query
	Reservation of auto log backup	modify, query, delete, create
	Auto log backup disk	modify, query, delete, create
	Send a mail when DB capacity exceeds	modify, query, delete, create
Integrity check	Reservation of auto integrity check	modify, query
	Send a mail about integrity check result	modify, query, delete, create
Online Update	Server IP/Port	modify, query
	Reservation of update	modify, query, delete, create
	The number of connection trial	modify, query
	To apply new policy automatically to engine	modify, query
	When policy is applied automatically, calculate optimized attack rule	modify, query
	To apply port attack name or not	modify, query
	The latest update time	query
	The latest update rule version	query
Communication	Reaction	modify, query
	Log encryption	modify, query
Reaction	Interactive authentication of authentication key	modify, query
	Alarm	modify, query
Time synchronization	SNMP Trap	modify, query
	Time synchronization of management console and engine	modify, query
Engine connection information	Engine name	modify, query, delete, create
	Engine IP address	modify, query, delete, create
	Engine service Port	modify, query, delete, create
	Engine MAC address	modify, query, delete, create
	Engine model name / the number of port	modify, query
Detection related information	Product serial	modify, query
	Observed network information	modify, query, delete, create
Engine operation information	Console MAC address	modify, query, delete, create
	Duration of session block	modify, query
Reaction related	Duration of session block	modify, query
	Filter type of Duplicated log	modify, query

	The number of times of duplication	modify, query
	Duplication time	modify, query
Packet filtering policy Intrusion prevention policy	Information about security attributes which is defined in 'FMT_MSA.1 security attributes management	Each action about security attributes which is defined in 'FMT_MSA.1 security attributes management

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

5.1.4.6 FMT_MTD.2 Management of limits on TSF data

Hierarchical to : No other components

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [audit trail capacity, the number of failed authentication trials] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall take [specified reaction in FAU_STG.3 or in FAU_STG.4 when audit trail capacity is at or exceed the indicated limits; specified reaction in FIA_AFL.1 when the number of authentication trial exceeds the indicated limits], if the TSF data is at or exceed the indicated limits.


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

5.1.4.7 FMT_SMF.1 Specification of management functions

Hierarchical to : No other components

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

- a) Specified item in "FMT_MOF.1(1) Management of security functions behavior(1)" of chapter 5.1.4.1
- b) Specified item in "FMT_MOF.1(2) Management of security functions behavior(1)" of chapter 5.1.4.2
- c) Specified item in "FMT_MSA.1 Management of security attributes" of

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

chapter 5.1.4.3

d) Specified item in “FMT_MTD.1 Management of TSF data” of chapter 5.1.4.5

e) Specified item in “FMT_MTD.2 Management of limits on TSF data” of chapter 5.1.4.6

Dependencies : No dependencies

5.1.4.8 FMT_SMR.1 Security roles

Hierarchical to : No other components

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

- a) Top administrator
- b) Middle level administrator
- c) Low level administrator

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

Dependencies : FIA_UID.1 Identification

5.1.5 Protection of the TSF


5.1.5.1 FPT_AMT.1 Abstract machine testing

Hierarchical to : No other components

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies theTSF.

Dependencies : No dependencies

5.1.5.2 FPT_FLS.1 Failure with preservation of secure state

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

Hierarchical to : No other components

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur : [Hareware failure including CPU, memory, Operating system, software failure of TOE, buffer overflow due to attack].

Dependencies : ADV_SPM.1 Informal TOE security policy model

5.1.5.3 FPT_ITT.1 Basic protection of internal transmission of TSF data

Hierarchical to : No other components

FPT_ITT.1.1 The TSF shall protect TSF data from modification when TSF data is transmitted among separated parts of TOE

Dependencies : No dependencies

5.1.5.4 FPT_RVM.1 TSP Non-bypassability of the TSP

Hierarchical to : No other components

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


Dependencies : No dependencies

5.1.5.5 FPT_SEP.1 TSF domain separation

Hierarchical to : No other components

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

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

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

Dependencies : No dependencies

5.1.5.6 FPT_STM.1 Reliable timestamps

Hierarchical to : No other components

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

Dependencies : No dependencies

Application notes : A possible way to maintain reliable time stamps for the TOE is to retrieve the time from the NTP server or underlying OS of the TOE. That is, the TOE may be able to maintain reliable time stamp either by the help of NTP server provided for the IT environment or by the system time information provided by the OS.

5.1.5.7 FPT_TST.1 TSF testing

Hierarchical to : No other components

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


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

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

Dependencies : FPT_AMT.1 Abstract machine testing

5.1.6 Resource Utilization

5.1.6.1 FRU_FLT.1 Degraded fault tolerance : subset

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

Hierarchical to : No other components

FRU_FLT.1.1 The TSF shall ensure the operation of [the administrator's management using console] when the following failures occur; [Hardware failure including CPU, memory, Operating system, software failure of TOE, buffer overflow due to attack].

Dependencies : FPT_FLS.1 Failure with preservation of secure state

5.1.6.2 FRU_RSA.1 Maximum quotas

Hierarchical to : No other components

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources:[transport layer representation] that subjects can use over a specified period of time.

Dependencies : No dependencies

5.1.7 TOE Access


5.1.7.1 FTA_SSL.1 TSF-initiated session locking

Hierarchical to : No other components

FTA_SSL.1.1 The TSF shall lock an interactive session of the authorized administrator after [authorized administrator inactivity period: 10 minutes(default value)] by:

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

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

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

Dependencies : FIA_UAU.1 Authentication

5.1.7.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to : No other components

FTA_SSL.3.1 The TSF shall terminate an interactive session after [inactivity period for management console action : 10 minutes(default), inactivity period for TCP data flow specified by administrator : 10 minutes(default)].

Dependencies : No dependencies

5.1.8 Trusted Path/Channels

5.1.8.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to : No other components

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

FTP_ITC.1.2 The TSF shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [the update of security violation events list, remote management function].

Dependencies : No dependencies

5.2 TOE Security Assurance Requirements

Security assurance requirements of the TOE are composed of assurance components in Part 3 and meet EAL4 assurance level. The assurance components addressed in this document are summarized in the following table.

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

[Table 5-2] Assurance components

5.2.1 Configuration Management

1) ACM_AUT.1 Partial CM automation

- Dependencies :

- ACM_CAP.3 Authorization controls


- Developer action elements

- ACM_AUT.1.1D The developer shall use a CM system.

- ACM_AUT.1.2D The developer shall provide a CM plan.

- Content and presentation of evidence elements

- ACM_AUT.1.1C The CM system shall provide an automated means by which

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

only authorized changes are made to the TOE implementation representation.

- ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

- ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

- ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

- Evaluator action elements

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

2) ACM_CAP.4 Generation support and acceptance procedures

- Dependencies :

- ALC_DVS.1 Identification of security measures

- Developer action elements

- ACM_CAP.4.1D The developer shall provide a reference for the TOE.

- ACM_CAP.4.2D The developer shall use a CM system.

- ACM_CAP.4.3D The developer shall provide CM documentation.

- Content and presentation of evidence elements

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

- ACM_CAP.4.2C The TOE shall be labeled with its reference.

- ACM_CAP.4.3C The configuration list shall uniquely identify all configuration items that comprise the TOE.

- ACM_CAP.4.4C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

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

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

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

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

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

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



the CM system.

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

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

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

- Evaluator action elements

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

3) ACM_SCP.2 Problem tracking CM coverage

- Dependencies :

- ACM_CAP.3 Authorization controls

- Developer action elements

- ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

- Content and presentation of evidence elements

- ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

- Evaluator action elements

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

5.2.2 Delivery and Operation

1) ADO_DEL.2 Detection of modification

- Dependencies :

- ACM_CAP.3 Authorization controls

- Developer action elements


- ADO_DEL.2.1D developer shall document procedures for delivery of the TOE or parts of it to the user.

- ADO_DEL.2.2D The developer shall use the delivery procedures.

- Content and presentation of evidence elements

- ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

- ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

modifications, or any discrepancy between the developer's master copy and the version received at the user site.

- ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

- Evaluator action elements

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

2) ADO_IGS.1 Installation, generation, and start-up procedures

- Dependencies :

- AGD_ADM.1 Administrator guidance

- Developer action elements

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

- Content and presentation of evidence elements

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

- Evaluator action elements

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

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

5.2.3 Development

1) ADV_FSP.2 Fully defined external interfaces

- Dependencies :

- ADV_RCR.1 Informal correspondence demonstration

- Developer action elements

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

- Content and presentation of evidence elements


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

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

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



- ADV_FSP.2.4C The functional specification shall completely represent the TSF.
- ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.
- Evaluator action elements
- ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.
- 2) ADV_HLD.2 Security enforcing high-level design
- Dependencies :
- ADV_FSP.1 Informal functional specification
- ADV_RCR.1 Informal correspondence demonstration
- Developer action elements
- ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.
- Content and presentation of evidence elements
- ADV_HLD.2.1C The presentation of the high-level design shall be informal.
- ADV_HLD.2.2C The high-level design shall be internally consistent.
- ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
- ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.
- ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
- ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.
- ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
- ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
- ADV_HLD.2.9C The high-level design shall describe the separation of the

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

TOE into TSP enforcing and other subsystems.

- Evaluator action elements
 - ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
 - ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.


3) ADV_IMP.1 Subset of the implementation of the TSF

- Dependencies :
 - ADV_LLD.1 Descriptive low-level design
 - ADV_RCR.1 Informal correspondence demonstration
 - ALC_TAT.1 Well-defined development tools
- Developer action elements
 - ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.
- Content and presentation of evidence elements
 - ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.
 - ADV_IMP.1.2C The implementation representation shall be internally consistent.
- Evaluator action elements
 - ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
 - ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

4) ADV_LLD.1 Descriptive low-level design

- Dependencies :
 - ADV_HLD.2 Security enforcing high-level design
 - ADV_RCR.1 Informal correspondence demonstration
- Developer action elements
 - ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.
- Content and presentation of evidence elements
 - ADV_LLD.1.1C The presentation of the low-level design shall be informal.
 - ADV_LLD.1.2C The low-level design shall be internally consistent.

- ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.
- ADV_LLD.1.4C The low-level design shall describe the purpose of each module.
- ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.
- ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.
- ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.
- ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
- ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.
- ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.
- Evaluator action elements
 - ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
 - ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.
- 5) ADV_RCR.1 Informal correspondence demonstration
 - Dependencies : No dependencies
 - Developer action elements
 - ADV_RCR1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
 - Content and presentation of evidence elements
 - ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
 - Evaluator action elements
 - ADV_RCR.1.1E The evaluator shall confirm that the information provided

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

meets all requirements for content and presentation of evidence.

6) ADV_SPM.1 Informal TOE security policy model

- Dependencies :
 - ADV_FSP.1 Informal functional specification
- Developer action elements
 - ADV_SPM.1.1D The developer shall provide a TSP model.
 - ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.
- Content and presentation of evidence elements
 - ADV_SPM.1.1C The TSP model shall be informal.
 - ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
 - ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
 - ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.
- Evaluator action elements
 - ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Guidance Documents

1) AGD_ADM.1 Administrator guidance

- Dependencies :
 - ADV_FSP.1 Informal functional specification
- Developer action elements
 - AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.
- Content and presentation of evidence elements
 - AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
 - AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.
 - AGD_ADM.1.3C The administrator guidance shall contain warnings about



functions and privileges that should be controlled in a secure processing environment.

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

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

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

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

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

- Evaluator action elements

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

2) AGD_USR.1 User guidance

- User is excluded in logical area of the TOE, so user guidance is not provided.

5.2.5 Life Cycle Support

1) ALC_DVS.1 Identification of security measures

- Dependencies : No dependencies

- Developer action elements


- ALC_DVS.1.1D The developer shall produce development security documentation.

- Content and presentation of evidence elements

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

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

- Evaluator action elements

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

- ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.
- 2) ALC_LCD.1 Developer defined life-cycle model
 - Dependencies : No dependencies
 - Developer action elements
 - ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.
 - ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.
 - Content and presentation of evidence elements
 - ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
 - ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
 - Evaluator action elements
 - ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 3) ALC_TAT.1 Well-defined development tools
 - Dependencies :
 - ADV_IMP.1 Subset of the implementation of the TSF
 - Developer action elements
 - ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.
 - ALC_TAT.1.2D The developer shall document the selected implementation dependent options of the development tools.
 - Content and presentation of evidence elements
 - ALC_TAT.1.1C All development tools used for implementation shall be welldefined.
 - ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.
 - ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.
 - Evaluator action elements

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

5.2.6 Tests

1) ATE_COV.2 Analysis of coverage

- Dependencies :

- ADV_FSP.1 Informal functional specification

- ATE_FUN.1 Functional testing

- Developer action elements

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

- Content and presentation of evidence elements

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

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

- Evaluator action elements

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

2) ATE_DPT.1 Testing: high-level design

- Dependencies :

- ADV_HLD.1 descriptive high-level design

- ATE_FUN.1 Functional test

- Developer action elements

- ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing


- Content and presentation of evidence elements

- ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

- Evaluator action elements

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

3) ATE_FUN.1 Functional testing

 LGN-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
--	---	---

- Dependencies : No dependencies
 - Developer action elements
 - ATE_FUN.1.1D The developer shall test the TSF and document the results.
 - ATE_FUN.1.2D The developer shall provide test documentation.
 - Content and presentation of evidence elements
 - ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
 - ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
 - ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
 - ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.
 - ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
 - Evaluator action elements
 - ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 4) ATE_IND.2 Independent testing – sample
- Dependencies :
 - ADV_FSP.1 Informal functional specification
 - AGD_ADM.1 Administrator guidance
 - AGD_USR.1 User guidance
 - ATE_FUN.1 Functional testing
 - Developer action elements
 - ATE_IND.2.1D The developer shall provide the TOE for testing.
 - Content and presentation of evidence elements
 - ATE_IND.2.1C The TOE shall be suitable for testing.
 - ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
 - Evaluator action elements
 - ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
 - ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate

to confirm that the TOE operates as specified.

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

5.2.7 Vulnerability assessment

1) AVA_MSU.2 Validation of analysis

- Dependencies :

- ADO_IGS.1 Installation, generation, and start-up procedures

- ADV_FSP.1 Informal functional specification

- AGD_ADM.1 Administrator guidance

- AGD_USR.1 User guidance

- Developer action elements

- AVA_MSU.2.1D The developer shall provide guidance documentation.

- AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

- Content and presentation of evidence elements

- AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

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

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

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


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

- Evaluator action elements

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

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

- AVA_MSU.2.3E The evaluator shall determine that the use of the guidance

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

documentation allows all insecure states to be detected.

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

2) AVA_SOF.1 TOE Strength of TOE security function evaluation

- Dependencies :

- ADV_FSP.1 Informal functional specification
- ADV_HLD.1 Descriptive high-level design

- Developer action elements

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

- Content and presentation of evidence elements

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

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

- Evaluator action elements

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

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

3) AVA_VLA.2 Independent vulnerability analysis

- Dependencies :

- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF
- ADV_LLD.1 Descriptive low-level design

- AGD_ADM.1 Administrator guidance

- AGD_USR.1 User guidance

- Developer action elements

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

- AVA_VLA.2.2D The developer shall provide vulnerability analysis



documentation.

- Content and presentation of evidence elements

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

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

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

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

- Evaluator action elements

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

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

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

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

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

5.3 Security requirement for the IT environment

no security requirements.

6. TOE Summary Specification

This chapter provides a description of assurance measures related to the security functions of SafezoneIPS . It shows that SafezoneIPS meets the security functional requirements and assurance requirements for the network prevention system protection profile claimed.

6.1 TOE Security Functions

This section describes the summary specification of TOE security functions(TSF) based on the TOE security functional requirements

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TSF Protection
- TOE Access

6.1.1 Security Audit

Security audit performs the following functions

- Audit data generation(SFAU_GEN)
- Audit data search and retrieval (SFAU_SAR)

6.1.1.1 Audit data generation(SFAU_GEN)

The TOE generates security audit logs on the events occurred from the security functions of the system and intrusion detection/prevention logs.

Audit log for security management function is generated by Audit log generation module of engine and management console, and generated audit log is stored in Database of Engine.

Item	Description
Audit log	The system that generated the audit log, which is divided into an administrator console and engine.
Date and time	The date and time when the audit log is generated

Audit object	The object of the activity defined by the audit log (i.e. target of generation)
Audit subject	The subject of the activity defined by the audit log (i.e. subject of generation)
Audit activity	Description of the audit log including success or failure of the security functional activities.
Audit type	Type of the audit log as either Information, Warning, or Error - Information: Audit of the event that describes success of the service of the TOE security function - Warning: Audit of the event that warns the potential, though not important, problem when performing the service of the TOE security function - Error: Audit of the event that causes data loss, functional loss, or failure/error in performing the function provided by the TOE
Audit code	A code to identify the event
IP	IP address of system in which audit log is generated.

Intrusion/Prevention log is stored in Database. Audit log for intrusion/prevention log contains the following items.

Item	Division
Audit log	Attack name
Date and Time	Detection time
	Store time
Audit Subject	Source IP
	Source Port
	Source MAC Address
Audit Object	Target IP
	Target Port
	Target MAC Address
Audit Content	Protocol
	Engine
	Reaction
	The number of times for attack
	Attack direction
	Network Name
	Type of Content
File name	
Audit Type	Risk level
Audit code	Attack code

When attack packet is detected and prevented from engine, audit log is displayed in Management console. Management console gives notice to administrator about audit log.

- Selective audit log generation

Event generated from security management function can include or exclude audit event selectively by the following defined event type.

Event Type
[Console]Backup management
[Console]Engine management
[Console]Configuration management
[Console]DB management
[Console]Log management
[Console]User management
[Console]Monitor management
[Console]Web console management
[Console]SNMP management
[Console]Time management
[Console]Update management
[Console]Mail management
[Console]Traffice management
[Console]Session management
[Console]Offline update management
[Console]Statistics module management
[Engine]Agent management
[Engine]Engine management
[Engine]Configuration management
[Engine]Policy file management
[Engine]Data management
[Engine]Connection management
[Engine]CLI tool management
[Engine]Traffic management
[Engine]License management
[Engine]Detection log management
[Engine]Thread management
[Engine]Online update management
[Engine]Firewall management

6.1.1.2 Audit data search and retrieval (SFAU_SAR)

All audit logs and intrusion detection/prevention results generated in the TOE system are managed by engine. They will be reviewed through GUI interface of Management console, but only on the basis of the authority level defined by the TOE system.

The user groups classified by authority defined by the TOE system are as the following.


Category	Description
Top administrator	A user who is authorized to use all functions provided by the TOE

Mid-level administrator	A user who is authorized to use all functions provided by the TOE except user info-management, Engine info-management, audit log deletion function
Mid-level administrator	A user who is authorized to use only reference functions and not allowed to use administrative functions. Among the reference functions, he/she can only refer to the engine assigned by the top administrator.

- 1) Top administrator is authorized to refer to all audit logs.
- 2) Stored audit data is provided in a list format so that a user can interpret the content of audit log items.
- 3) Each field of audit log can be re-arranged.
- 4) Audit logs can be retrieved only through search by one of or combination of the following conditions:
 - Date and time of the generation of an audit log
 - Subject and object of an audit log
 - Type of an audit log

The reference function for the intrusion detection/prevention result managed by Management Console has the following features:.


- 1) A registered user is authorized to refer to an intrusion detection/prevention log.
- 2) Stored intrusion detection logs are provided in a list format so that a user can interpret the content of intrusion detection items including the following information:.
 - Date and time of the generation of an intrusion detection/prevention log
 - Date and time of the storage of an intrusion detection/prevention log
 - Subject and object of an intrusion detection/prevention log: protocol, source IP, source port, destination IP, destination port
 - Content of an intrusion detection/prevention
 - Result of counter action to an intrusion
- 3) Intrusion detection/prevention logs can be retrieved only through search by one of or combination of the following conditions:
 - Date and time of the generation of an intrusion detection/prevention log
 - Date and time of the storage of an intrusion detection/prevention log
 - Subject and object of an intrusion detection/prevention log: protocol, source IP, source port, destination IP, destination port

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

- Content of an intrusion detection/prevention
- Result of counter action to an intrusion

6.1.1.3 SFR Mapping

TSF	SFR Mapping
Audit data generation(SFAU_GEN)	FAU_ARP.1 Security alarms FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association FAU_SEL.1 Selective audit
Audit data search and retrieval(SFAU_SAR)	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

6.1.2 User Data Protection

In order to protect the target network, first, TOE performs access control function based on packet header, if needed, second, TOE performs to block harmful site and collect information for detection/prevention, reaction, and stores the analysis result. So administrator can review that information.

- Detection/prevention event information collection and analysis (SFDP_CHK)
- Reaction(SFDP_ACT)

6.1.2.1 Detection/prevention event information collection and analysis (SFDP_CHK)

All network traffic passing through the system and data incoming to the system are collected for the purpose of network analysis. Collected network traffic and data will be used in analyzing intrusion.

Information flow control policy for SafezoneIPS is packet filtering and intrusion prevention policy and they protect user data. If packet is sent to TOE, it is checked by packet filtering policy first, and then checked for intrusion prevention policy.

1) Type of intrusion

- Static Attack
- Attack of network protocol integrity
- Dynamic Attack
- Abnormal traffic attack

2) Information collection for analysis

- Subject : Source IP / Port information
- Object : Target IP / Port information
- Collection time : Date and time of the inflow of a packet
- Type and other information
 - Protocol information and header information of each protocol
 - Content field information of each packet

3) Detection mechanism for each attack type

- Static rule based attack analysis : Static policy based(SFDP_CHK_STAT)
- Packet integrity based attack analysis : Packet integrity based policy

(SFDP_CHK_INT)

- Dynamic attack policy based(SFDP_CHK_DYN)
- Abnormal traffic attack analysis : Abnormal traffic RateLimit policy based (SFDP_CHK_ABN)

4) Application of detection/prevention exception policy (SFDP_CHK_EXP)

5) Packet filtering(SFDP_CHK_PKF)

Using protocol header information, packet header is compared with packet filtering policy. According to this result, packet is controlled(PASS or DROP)

6) Harmful site block(SFDP_CHK_URL)

Payload of packet is checked, then if that packet is HTTP request or HTTP reply, it is compared with DB and PICS(Platform for Internet Content Selection) level information in HTML tag. So TOE provides URL blocking function based on PICS, and user-defined URL can be blocked, too.


6.1.2.2 Reaction(SFDP_ACT)

TOE can react automatically according to reaction policy defined by administrator if collected packet is judged as attack packet.

- 1) Packet Drop, IP Block, Session Kill
- 2) Audit log generation
- 3) Real-time warning(log, E-Mail)
- 4) Integration with other system : Syslog, SNMP Trap
- 5) Additional network information

6.1.2.5 SFR Mapping

TSF	SFR Mapping
Detection/prevention event information collection and analysis (SFDP_CHK)	FDP_IFC.1(1) Subset information flow control FDP_IFC.1(2) Subset information flow control FDP_IFF.1(1) Simple security attributes FDP_IFF.1(2) Simple security attributes FAU_SAA.1 Analysis of potential violation FPT_RVM.1 NON-BYPASSABILITY OF THE TSP FRU_RSA.1 Maximum quotas
Reaction(SFDP_ACT)	FAU_GEN.1 Audit data generation FAU_ARP.1 Security alarms FDP_IFF.1(2) Simple security attributes

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

6.1.3 Identification and authentication

Only the authorized users may use the TOE system. Identification and authentication of a user are carried out by the following two methods:

- User Identification and authentication function(SFIA_LOGON)
- Mutual identification and authentication between TOE components during remote connection through the communication channel (SFIA_UID)

6.1.3.1 User Identification and authentication function (SFIA_LOGON)

User identification and authentication (SFIA_LOGON) is required as a part of the SOF level(SOF-medium) targeted by the TOE.

Management Console displays the user entry browser for authentication as soon as the operation is initiated, and then receives the keyboard entry from the user. All password entries through GUI are displayed as asterisk(“ * ”) instead of the typed-in characters to prevent revealing the value. The PSM authentication module identifies the user with the ID and authenticates the user authority with the password.

1) Qualification of authority for administrative function

The authority to access the security management function and operational function is classified into the following three groups according to the user authority of Management Console:

Category	Description
Top administrator	A user who is authorized to use all functions provided by the TOE
Mid-level administrator	A user who is authorized to use all functions provided by the TOE except user info-management, Engine info-management, audit log deletion function
Mid-level administrator	A user who is authorized to use only reference functions and not allowed to use administrative functions. Among the reference functions, he/she can only refer to the engine assigned by the top administrator.

2) User authentication failure processing

If the PSM authentication process fails due to the entry of the invalid user ID or password, the number of continuous failures is recorded; if the number exceeds the predefined limit (1 to 10, default value: 3), the Management console operation for user authentication is locked(i.e. terminated) and the audit log of the event is recorded.

6.1.3.2 Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)

To ensure inter-TSF trusted channel, the components interacting remotely through the communication channel should identify and authenticate each other ' s node to initialize the communication channel and secure trusted channel.

- 1) Mutual identification and authentication between management console and engine
- 2) Mutual identification and authentication between engine and online update server

6.1.3.3 SFR Mapping


TSF	SFR Mapping
User identification and authentication(SFIA_LOG ON)	FIA_AFL.1 Authentication failure handling FIA_ATD.1(2) Definition of user attributes(2) FIA_UAU.1 Authentication FIA_UAU.7 Authentication feedback protection FIA_UID.2(2) User identification before any



Document Identification No.
SafezoneIPS V1.0(SZ5XU)
Security Target_20070314_V1.00.04

Document Type
Security Target

	action(2) FMT_SMR.1 Security role
Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)	FIA_AFL.1 Authentication failure handling FIA_UAU.1 Authentication FTP_ITC.1 INTER-TSF TRUSTED CHANNEL FPT_ITT.1 BASIC PROTECTION OF TSF DATA FOR INTERNAL TRANSMISSION FIA_UID.2(1) User identification before any action(1) FIA_ATD.1(1) Definition of user attributes(1)

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

6.1.4 Security Management

The security management function of the TOE system is provided through the Management Console GUI interface. The authorized administrator can perform the function through GUI to ensure continuous operation of the TOE. The management functions include the following:

- User information management
- Configuration information management for Management Console operation
- Configuration information management for Engine operation
- Packet control list management
- Security violation events management
- Harmful site block management
- Intrusion detection/prevention result report
- Prevention of audit data loss
- Management Console/Engine time synchronization
- Activation of security policy

6.1.4.1 User information management(SFMT_USR)

1) GUI user information management

Creation, modification and deletion of the user for each PSM GUI user group is performed by the user information management function.

2) User identification and authentication between TSFs

The user information to identify the other party during inter-TSF operation is managed by the configuration management function.

3) Identification and authentication management

PSM user identification and authentication management function for management console is provided through the GUI interface.

6.1.4.2 Configuration information management for Management Console operation (SFMT_PSM)

Management Console configuration information management function manages the information needed for Management Console operation through the GUI interface

1) Management Console configuration information search and retrieval

2) Management Console configuration information modification

6.1.4.3 Configuration information management for Engine operation (SFMT_SSS)

Engine configuration information management function manages the information related to engine connection and operation

- 1) Registration of engine information
- 2) Search and retrieval of Engine configuration information
- 3) Modification of Engine configuration information
- 4) Deletion of Engine configuration information

6.1.4.4 Security violation events management (SFMT_POL)

Security policy of TOE is divided into packet filtering and intrusion prevention policy. Security attributes can be determined by security violation events management function(SFMT_POL).

Packet filtering policy is managed by

- Packet filtering(SFMT_POL_PKF)


Intrusion prevention policy is managed by

- Static policy(SFMT_POL_STAT)
- Dynamic attack policy(SFMT_POL_DYN)
- Packet integrity policy(SFMT_POL_INT)
- Abnormal traffic RateLimit policy(SFMT_POL_ABN)
- Prevention exception policy(SFMT_POL_EXP)
- Harmful site block(SFMT_POL_URL).

Authorized administrator(top administrator, mid-level administrator) can use, activate and inactivate rules for each policy. If rule is created for the first time by authorized administrator(top administrator, mid-level administrator), that rule is in inactivate state.

The system-provided intrusion prevention policy itself cannot be applied to engine. A user can select one from the system-provided security policies during the TOE installation and derive from it a new user defined security policy keeping the existing attributes. Users can also search and retrieve the user-defined policies.

- 1) Static policy management(SFMT_POL_STAT)
- 2) Dynamic attack policy management (SFMT_POL_DYN)

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

- 3) Packet integrity policy management (SFMT_POL_INT)
- 4) Abnormal traffic RateLimit policy management (SFMT_POL_ABN)
- 5) Prevention exception policy management (SFMT_POL_EXP)
- 6) Packet filtering policy management(SFMT_POL_PKF)
- 7) Harmful site block policy management (SFMT_POL_URL)

6.1.4.5 Online update of new policy(SFMT_POLUP)

A new list of security violation events, processed by the static attack detection mechanism, is provided through online update.

- 1) This function is provided through the connection to the online update server, which is the new security violation events distribution server provided by the supplier. This should be executed only after the mutual authentication between Management console and the online update server.
- 2) The function to compare the static policy of the security violation event list registered in Management console with the security violation events list version registered in the online update server is provided.
- 3) The new version of online update server policies can be downloaded.
- 4) The online update function periodically connects to the online update server to inspect if there are new security violation events registered in the server.
- 5) The online update function can automatically register the newly updated security violation events list in policy database and apply it to engine. Then engine can immediately perform detection based on the updated policy.

6.1.4.6 Intrusion detection/prevention result report (SFMT_RPT)

Management console provides a report of the intrusion detection/prevention result through the GUI interface. The intrusion detection/prevention results searched by administrator-specified conditions are displayed in a predefined format of report.

6.1.4.7 Prevention of the loss of intrusion detection/prevention and audit data (SFMT_BKUP)

- 1) Criteria for deleting and modifying the stored data of intrusion detection/prevention log and audit log
- 2) Reaction according to audit trail limit
 - The disk usage is periodically monitored by checking the hard disk of



the system where the intrusion detection/prevention log and audit log databases are installed.

3) Prevention of data loss due to insufficient data storage capacity

- Backup audit log automatically against predicted audit data loss
- Check disk usage by periodical monitoring of hard disk usage.


6.1.4.8 Management/Engine time synchronization(SFMT_TIME)

The main components of the TOE system are provided with a secure time stamp to perform time synchronization so that they can operate with same time value.

Management console and engine are the subjects of time synchronization.

It is basic presumption that the TOE system receives an accurate time from the time server, which is an external interface to the TOE system.

- The TOE should be able to perform time synchronization by collecting current timestamp at the start-up and every period.
- Time synchronization should be performed any time if the administrator requests, even during the operation. Only the top administrator can perform time synchronization.
- The following are provided as an administrator interface through the GUI interface.
 - Time Server IP address input interface
 - Automatic time synchronization period (select one from 1, 2, 3, ... ,10 days) input interface
 - Time synchronization activation input interface

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

6.1.4.9 SFR Mapping

TSF	SFR Mapping
User information management (SFMT_USR)	FIA_ATD.1(1) Definition of user attributes(1) FIA_ATD.1(2) Definition of user attributes(2) FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_SMF.1 Specification of Management Functions
Configuration information management for Management Console operation (SFMT_PSM)	FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_MTD.1 Management of TSF data FMT_MTD.2 Management of limits on TSF data FMT_SMF.1 Specification of Management Functions
Configuration information management for Engine(SFMT_SSS)	FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of Management Functions
Security violation events management(SFMT_POL)	FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of Management Functions
New policy online update (SFMT_POLUP)	FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of Management Functions
Intrusion detection/prevention result report(SFMT_RPT)	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_SMF.1 Specification of Management Functions
Prevention of the loss of the intrusion detection and audit data(SFMT_BKUP)	FAU_STG.1 Protected audit trail storage FAU_STG.3 Action in case of possible audit data loss FAU_STG.4 Prevention of audit data loss FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_SMF.1 Specification of Management Functions FMT_MTD.2 Management of limits on TSF data
Management console/engine time synchronization (SFMT_TIME)	FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_SMF.1 Specification of Management Functions FPT_STM.1 Reliable time stamps

6.1.5 TSF Protection

The TOE system ensures safe TSF operations.

- Management Console/Engine Health Checking(SFPT_CHKSYS)
- TSF stored data integrity check(SFPT_CHKINT)

6.1.5.1 Management Console/Engine Health Checking (SFPT_CHKSYS)

This function periodically checks if th main components of the TOE system are normally operating.

1) Management Console checklist

- Management Console process
- Connection state of Management Console and engine
- Disk resource usage of the Management Console system
- Memory usage of each process of Management Console system

2) Engine checklist


- Engine processes
- Link status of Engine
- Memory, CPU, and disk usage of engine

Engine generates memory areas for packet filtering and intrusion prevention policy, and performs access control. Engine protects TSF domain for SFP from interference and violation by unreliable subject related to TSF.

SafezoneIPS provides the following function to keep operation though error occurs.

a) Hardware error : Status information about CPU and memory can be monitored using Management console. When hardware error(CPU, exhaust of memory) occurred, secure status can be maintained by engine restart-up and modification of security management configuration

b) Software error of TOE, Buffer overflow error by some attack : When engine daemon is stopped, that daemon is re-executed. When communication with TOE is impossible, administrator can manage network configuration using management console.

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

6.1.5.2 TSF stored data integrity check(SFPT_CHKINT)

TOE can check integrity of data generated by TSF and reacts against it. Integrity check function is a component of management console, so it is provided through GUI interface. TOE detects and counters the corruption of the TSF-generated data.

Integrity check is performed at the initial start-up by the executable files and configuration files in TSC that execute each TSF. TSF is executed only after the successful data integrity check. Hash values of the executable files and configuration files are generated at the initial start-up and updated at every start-up or upon the administrator ' s request. SHA-1 hash algorithm is used to generate the hash value.

6.1.5.3 SFR Mapping

TSF	SFR Mapping
Management console/Engine Health Checking (SFPT_CHKSYS)	FPT_AMT.1 Abstract machine testing FPT_SEP.1 TSF domain separation FPT_FLS.1 Failure with preservation of secure state FRU_FLT.1 Degraded fault tolerance : subset
TSF Stored data integrity checking (SFPT_CHKINT)	FPT_TST.1 TSF testing

6.1.6 TOE Access

If the TOE is accessed by an authorized administrator but remains inactive for a certain period of time, the interacting session will be locked to protect the TOE during the time of inactivity.

The session locking is performed on the Management Console interface, which is the entry point of the interaction between the TOE function and the administrator.

1) Criteria for session locking function configuration

- When there is no key entry for a certain period of time (default value: 10 min.) after the administrator logged on Management Console, all visible attributes on Management Console interface are deactivated to hide them from display.
- The period of inactivity before the session locking may be configured only by the top administrator.
- The session locking function can be activated or deactivated through the security management function, also by the top administrator.

2) Criteria for session unlocking

When the icon showing deactivation of Management Console GUI interface is clicked on, the initial logon process is carried out again to confirm whether it is an access of the authorized administrator.

3) Criteria for session termination

- The period of inactivity before the session termination may be configured only by the top administrator.
- The session termination function can be activated or deactivated through the security management, also by the top administrator.


6.1.6.1 SFR Mapping

TSF	SFR Mapping
TSF-initiated session locking (SFTA_SSL)	FTA_SSL.1 TSF-initiated session locking FTA_SSL.3 TSF-initiated termination

6.2 Assurance Measures

This section describes the TOE assurance measures. The assurance measures are used to satisfy the assurance requirements, which are listed in the [Table 6-1].

assurance class	assurance component		assurance measures
Configuration Management	ACM_AUT.1	Partial CM automation	Configuration Management Document
	ACM_CAP.4	Generation support and acceptanc procedures	Configuration Management Document
	ACM_SCP.2	Problem tracking CM coverage	Configuration Management Document
Delivery and operation	ADO_DEL.2	Detection of modification	Delivery Procedure
	ADO_IGS.1	Installation, generation, and start-up procedures	Installation Manual
Development	ADV_FSP.2	Fully defined external interfaces	Functional specification
	ADV_HLD.2	Security enforcing high-level design	High-level Design
	ADV_IMP.1	Subset of the implementation of the TSF	Validation specification
	ADV_LLD.1	Descriptive low-level design	Low-level Design
	ADV_RCR.1	Informal correspondence demonstration	Validation Specification
	ADV_SPM.1	Informal TOE security policy model	Security Policy Modeling
Guidance Documents	AGD_ADM.1	Administrator guidance	Administrator Guidance Document
	AGD_USR.1	User guidance	N/A
Life Cycle Support	ALC_DVS.1	Identification of security measures	Life Cycle Support
	ALC_LCD.1	Developer defined life-cycle model	Life Cycle Support
	ALC_TAT.1	Well-defined development tools	Life Cycle Support
Tests	ATE_COV.2	Analysis of coverage	Testing

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

	ATE_DPT.1	Testing: high-level design	Testing
	ATE_FUN.1	Functional testing	Testing
	ATE_IND.2	Independent testing - sample	-
Vulnerability assessment	AVA_MSU.2	Validation of analysis	Misuse Analysis
	AVA_SOF.1	Strength of TOE security function evaluation	Vulnerability Analysis
	AVA_VLA.2	Independent vulnerability analysis	Vulnerability Analysis

[Table 6-1] Assurance measures

The configuration management document will provide the assurance of the components concerning Configuration Management such as ACM_AUT.1 Partial configuration management automation, ACM_CAP.4 Generation support and acceptance procedures, and ACM_SCP.2 Problem tracking CM coverage).

Assurance of the components concerning Delivery and Operation are provided by the delivery procedure for ADO_DEL.2 Detection of modification and the installation manual for ADO_IGS.1 installation, generation, and operation procedures.

Assurance of the components concerning Development is provided by the functional specification for ADV_FSP.2 Fully defined external interface, highlevel design for ADV_HLD.2 Security enforcing high-level design, low-level design for ADV_LLD.1 Descriptive low-level design, and validation specification for both ADV_IMP.1 Subset of the implementation of the TSF and ADV_RCR.1 Informal correspondence demonstration.

For the components concerning Guidance Documents, AGD_ADM.1 Administrator guidance is assured by administrator guidance while AGD_USR.1 User guidance doesn't require assurance since there are no users other than the administrator.

For the components concerning Life Cycle Support, the life cycle support assures ALC_DVS.1 Identification of security measures, ALC_LCD.1 Developer defined life cycle model, and ALC_TAT.1 Well-defined development tools.

For the components dealing with Tests, the testing assures ATE_COV.2 Analysis of coverage, ATE_DPT.1 Testing: high-level design, ATE_FUN.1 Functional testing, and ATE_IND.2 Independent testing - sample.

The misuse analysis assures AVA_MSU.2 Validation of analysis, and the vulnerability analysis assures AVA_SOF.1 Strength of TOE security function evaluation and AVA_VLA.2 Independent vulnerability analysis.

7. Protection Profile Claims

This chapter explains claimed protection profile and identifies objectives and requirements that are not included in the PP.

7.1 Protection Profile Reference

This ST claims conformance to the Network Intrusion Prevention System Protection Profile V1.1 (Dec.21, 2005, KISA)

7.2 Protection profile tailoring

The following table shows the security functional requirements that are tailored in this ST.

Operation	Security functional components
Iteration	FDP_IFC.1(1) Subset information flow control(1) FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1(1) User attribute definition(1) FDP_IFF.1(2) User attribute definition(2) FIA_ATD.1(1) Definition of user attributes(1) FIA_ATD.1(2) Definition of user attributes(2) FIA_UID.2(1) User identification before any action(1) FIA_UID.2(2) User identification before any action(2) FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_MOF.1(2) Management of Security Functions Behavior(2)
Selection	FAU_GEN.1 Audit data generation FAU_SAR.3 Selectable audit review FAU_SEL.1 Selectvie audit FAU_STG.1 Protected audit trail storage FAU_STG.4 Prevention of audit data loss FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_MSA.1 Management of security attributes FMT_MTD.1 Management of TSF data FPT_AMT.1 Abstract machine testing FPT_TST.1 TSF testing FRU_RSA.1 Maximum quotas FPT_ITT.1 Basic protection of TSF Data for internal transmission

Refinement	FAU_GEN.1 Audit data generation FIA_ATD.1(1) Definition of user attributes(1) FIA_ATD.1(2) Definition of user attributes(2) FIA_UAU.1 Authentication FIA_UAU.7 Protected authentication feedback FIA_UID.2(1) User identification before any action(1) FIA_UID.2(2) User identification before any action(2) FMT_SMR.1 Security roles FPT_TST.1 TSF testing FTA_SSL.1 TSF-initiated session locking
Assignment	FAU_ARP.1 Security alarms FAU_GEN.1 Audit data generation FAU_SAA.1 Potential violation analysis FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FAU_SEL.1 Selective audit FAU_STG.3 Reaction in case of possible audit data loss FAU_STG.4 Prevention of audit data loss FDP_IFC.1(1) Subset information flow control (1) FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1(1) User attribute definition FDP_IFF.1(2) User attribute definition FIA_AFL.1 Authentication failure handling FIA_ATD.1(2) Definition of user attributes(2) FIA_UAU.1 Authentication FIA_UAU.7 Protected authentication feedback FMT_MOF.1(1) Management of Security Functions Behavior(1) FMT_MOF.1(2) Management of Security Functions Behavior(2) FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FMT_MTD.1 Management of TSF data FMT_MTD.2 Management of limits on TSF data FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles FPT_FLS.1 Failure with preservation of secure state FRU_FLT.1 Degraded fault tolerance : subset FRU_RSA.1 Maximum quotas FTA_SSL.1 TSF-initiated session locking FTA_SSL.3 TSF-initiated termination FTP_ITC.1 Inter-TSF trusted channel

7.3 Protection Profile Additions

This section describes claimed protection profile (Network Intrusion Prevention System Protection Profile V1.1, Dec. 21, 2005, KISA) and

added/modified items.

Category	Item	Reference
Assumption	A.Physical security	Intrusion prevention system PP
	A.Security maintenance	Intrusion prevention system PP
	A.Trusted administrator	Intrusion prevention system PP
	A.Hardened OS	Intrusion prevention system PP
	A.Single connection point	Intrusion prevention system PP
	A.Reliable TIMESTAMP	Added to ST
	A.Secure Update Server	Added to ST
	A.Secure Database	Added to ST

Category	Item	Reference	Remark
Threat	T.Masquerade	Intrusion prevention system PP	Threats to the TOE
	T.Failure	Intrusion prevention system PP	
	T.Audit failure	Intrusion prevention system PP	
	T.Inbound illegal information	Intrusion prevention system PP	
	T.Unauthorized service access	Intrusion prevention system PP	
	T.Anomaly packet transfer	Intrusion prevention system PP	
	T.New vulnerability attack	Intrusion prevention system PP	
	T.DoS Attack	Intrusion prevention system PP	
	T.Replay attack	Intrusion prevention system PP	
	T.Bypassing	Intrusion prevention system PP	
	T.Spoofing IP address	Intrusion prevention system PP	
	T.Unauthorized TSF data modification	Intrusion prevention system PP	
	Threat	TE.Poor administration	
TE.Distribution and installation		Intrusion prevention system PP	
Security Policy	P.Audit	Intrusion prevention system PP	Organizational security policy
	P.Secure administration	Intrusion prevention system PP	
Security Objective	O.Availability	Intrusion prevention system PP	Security objectives for the TOE
	O.Audit	Intrusion prevention system PP	
	O.Administration	Intrusion prevention system PP	
	O.Abnormal packet screening	Intrusion prevention system PP	
	O.DoS attack blocking	Intrusion prevention system PP	
	O.Identification	Intrusion prevention system PP	
	O.Authentication	Intrusion prevention system PP	



	0.Information flow control	Intrusion prevention system PP	
	0.TSF data protection	Intrusion prevention system PP	
Security objectives for the environment	0E.Physical security	Intrusion prevention system PP	Security objectives for the environment
	0E.Security maintenance	Intrusion prevention system PP	
	0E.Trusted administrator	Intrusion prevention system PP	
	0E. Secure administration	Intrusion prevention system PP	
	0E.Hardened OS	Intrusion prevention system PP	
	0E.Single Connection point	Intrusion prevention system PP	
	0E.Vulnerability list update	Intrusion prevention system PP	
	0E.Trusted TIMESTAMP	Added to ST	
	0E.Secure Update Server	Added to ST	
	0E.Secure Database	Added to ST	

Category	Item	Reference	Remark
SAR	FAU_ARP.1 Security alarms	Intrusion prevention system PP	Security audit
	FAU_GEN.1 Audit data generation	Intrusion prevention system PP	
	FAU_GEN.2 User identity association	Intrusion prevention system PP	
	FAU_SAA.1 Potential violation analysis	Intrusion prevention system PP	
	FAU_SAR.1 Audit review	Intrusion prevention system PP	
	FAU_SAR.3 Selectable audit review	Intrusion prevention system PP	
	FAU_SEL.1 Selective audit	Intrusion prevention system PP	
	FAU_STG.1 Protected audit trail storage	Intrusion prevention system PP	
	FAU_STG.3 reaction in case of possible audit data loss	Intrusion prevention system PP	
	FAU_STG.4 Prevention of audit data loss	Intrusion prevention system PP	
FDP	FDP_IFC.1(1) Subset information flow control(1)	Intrusion prevention system PP	User data protection
	FDP_IFC.1(2) Subset information flow control(2)	Intrusion prevention system PP	
	FDP_IFF.1(1) Simple security attributes(1)	Intrusion prevention system PP	
	FDP_IFF.1(2) Simple security attributes(2)	Intrusion prevention system PP	
FIA	FIA_AFL.1 Authentication failure handling	Intrusion prevention system PP	Identification and Authentication
	FIA_ATD.1(1) Definition of user attributes(1)	Intrusion prevention system PP	
	FIA_ATD.1(2) Definition of user attributes(2)	Intrusion prevention system PP	
	FIA_UAU.1 Authentication	Intrusion prevention system PP	
	FIA_UAU.7 Protected authentication feedback	Intrusion prevention system PP	
	FIA_UID.2(1) User identification before any action(1)	Intrusion prevention system PP	
	FIA_UID.2(2) User identification before any action(2)	Intrusion prevention system PP	
FMT_MOF.1(1) Management of Security Functions Behavior(1)	Intrusion prevention system PP	Security Management	

FMT_MOF.1(2) Management of Security Functions Behavior(2)	Intrusion prevention system PP	
FMT_MSA.1 Management of security attributes	Intrusion prevention system PP	
FMT_MSA.3 Static attribute initialization	Intrusion prevention system PP	
FMT_MTD.1 Management of TSF data	Intrusion prevention system PP	
FMT_MTD.2 Management of limits on TSF data	Intrusion prevention system PP	
FMT_SMF.1 Specification of Management Functions	Intrusion prevention system PP	
FMT_SMR.1 Security roles	Intrusion prevention system PP	
FPT_AMT.1 Abstract machine testing	Intrusion prevention system PP	TSF Protection
FPT_FLS.1 Failure with preservation of secure state	Intrusion prevention system PP	
FPT_ITT.1 Basic protection of TSF data for internal transmission	Added to ST	
FPT_RVM.1 Non-bypassability of the TSP	Intrusion prevention system PP	
FPT_SEP.1 TSF domain separation	Intrusion prevention system PP	
FPT_STM.1 Reliable time stamps	Intrusion prevention system PP	
FPT_TST.1 TSF testing	Intrusion prevention system PP	
FRU_FLT.1 Degraded fault tolerance : subset	Intrusion prevention system PP	Resource utilization
FRU_RSA.1 Maximum quotas	Intrusion prevention system PP	
FTA_SSL.1 TSF-initiated session locking	Intrusion prevention system PP	TOE access
FTA_SSL.3 TSF-initiated termination	Intrusion prevention system PP	
FTP_ITC.1 INTER-TSF TRUSTED CHANNEL	Intrusion prevention system PP	Trusted path/channels


Category	Item	Reference	Remark
SAR	ACM_AUT.1 Partial CM automation	Intrusion prevention system PP	Configuration Management Document
	ACM_CAP.4 Generation support and acceptance procedures	Intrusion prevention system PP	Configuration Management Document
	ACM_SCP.2 Problem tracking CM coverage	Intrusion prevention system PP	Configuration Management Document
	ADO_DEL.2 Detection of modification	Intrusion prevention system PP	Delivery Procedure
	ADO_IGS.1 Installation, generation, and start-up procedures	Intrusion prevention system PP	Installation Manual
	ADV_FSP.2 Fully defined external interfaces	Intrusion prevention system PP	Functional specification
	ADV_HLD.2 Security enforcing high-highlevel	Intrusion prevention system PP	High-level Design
	ADV_IMP.1 Subset of the implementation of the TSF	Intrusion prevention system PP	Validation Specification
	ADV_LLD.1 Descriptive low-level design	Intrusion prevention system PP	Low-level Design
	ADV_RCR.1 Informal correspondence demonstration	Intrusion prevention system PP	Validation Specification
	ADV_SPM.1 Informal TOE security policy model	Intrusion prevention system PP	Security Policy Modeling
	AGD_ADM.1 Administrator guidance	Intrusion prevention system PP	Administrator Administrator
	AGD_USR.1 User guidance	Intrusion prevention system PP	-
	ALC_DVS.1 Identification of security measures	Intrusion prevention system PP	Life Cycle Support
ALC_LCD.1 Developer defined life-cycle model	Intrusion prevention system PP	Life Cycle Support	

ALC_TAT.1 Well-defined development tools	Intrusion prevention system PP	Life Cycle Support
ATE_COV.2 Analysis of coverage	Intrusion prevention system PP	Testing
ATE_DPT.1 Testing: high-level design	Intrusion prevention system PP	Testing
ATE_FUN.1 Functional testing	Intrusion prevention system PP	Testing
ATE_IND.2 Independent testing sample	Intrusion prevention system PP	-
AVA_MSU.2 Validation of analysis	Intrusion prevention system PP	Misuse Analysis
AVA_SOF.1 Strength of TOE security function evaluation	Intrusion prevention system PP	Vulnerability Analysis
AVA_VLA.2 Independent vulnerability analysis	Intrusion prevention system PP	Vulnerability Analysis

[Table 7-1] Protection profile additions and modifications

7.3.1 Protection Profile Modifications

The requirements of the PP (Network Intrusion Prevention System Protection Profile) are all included in this document(ST). Added or modified requirements are the following: for assumptions - A.Reliable TIMESTAMP, A.Secure Update Server, A. Secure Database, for Security Objectives for environment - OE. Reliable TIMESTAMP, OE. Secure Update Server, OE. Secure Database

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

8. Rationale

This chapter describes the security objectives defined on the basis of the security environments (threats, assumptions, and organizational security policies) and the rationale for the security requirements that satisfy the security objectives. The rationale shows that the TOE provides efficient IT security measures in its security environments.

Correlations and rationales for the following items are described.

- Correlation of the security objectives with assumptions, threats, and security policies
- Correlation of security functional requirements and security objectives
- Correlation of TOE summary specification, IT security requirements, and assurance requirements
- Rationale for protection profile claims

8.1 Security Objectives Rationale


The rationale for security objectives shows that the specified security objectives are suitable, not too much but sufficient enough to deal with security problems, and requisite. The security objectives rationale shows the following statements:

- Each assumption, threat, organizational security policy will be addressed by at least one security objective.
- Each security objective will address at least one assumption, threat, and organizational security policy.

[Table 8-1] shows the correlation of security environment and security objectives.

Security environment	Security Objectives																			
	O.Availability	O.Audit	O.Administration	O.TSF data protection	O.Abnormal packet screening	O.DoS Attack blocking	O.Identification	O.Authentication	O.Information 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.Reliable TIMESTAMP	OE.Secure Update Server	OE.Secure Database	
A.Physical security																				
A.Security maintenance																				
A.Trusted administrator																				
A.Hardened OS																				
A.Single connection point																				
A.Reliable TIMESTAMP																				
A.Secure Update Server																				
A. Secure Database																				
T.Masquerade																				
T.Failure																				
T.Audit Failure																				
T.Inbound illegal informion																				
T.Unauthorized service access																				
T.Anomaly packet transfer																				
T.New vulnerability attack																				
T.DoS attack																				
T.Replay Attck																				
T.Bypassing																				
T.Spoofing IP Address																				
T. Unauthorized TSF Data Modification																				
TE.Poor Administration																				
TE.Distribution and Installation																				
P.Audit																				
P.Secure Administration																				

[Table 8-1] Correlation of security environment and security objectives

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

8.1.1 Rationale for the security objectives for the TOE

1) O.Availability

This TOE security objective ensures the TOE availability for providing minimum network service when the TOE is in failure or overloaded from attacks.

Therefore, this security objective is to guarantee the TOE availability to counter the threats of T.Failure, T.Unauthorized TSF data modification, T.Bypassing, and T.Audit failure, which means an audit trail storage exhaustion attack.

2) O. Audit

This TOE security objective is to record the audit events for each user according to TOE audit record policy when a user uses security functions. The TOE guarantees to provide the means to keep the logged audit events safe and review them. That is, the TOE takes actions when the audit trail storage is full.

The generation of audit record ensures that the identification of an attacker should be detected through the audit record in case continuous authentication attempts occur. Spoofing attacks, DoS attacks, and attacks of generating and sending abnormal packets can be traced through the audit record. Therefore, this security objective is to counter the threats like T.Masquerade, T.Audit failure, T.Anomaly Packet Transfer, T.DoS attack, T.Replay attack, T.Spoofing IP address, and T.Unauthorized TSF data modification, and is to support the organizational security policy of P.Audit.

3) O. Administration

The TOE controls the illegal access to internal network by establishing information flow control rules to enforce security policy. To do that, the TOE should provide the means to manage the TOE and TSF data safely for the generation and management of TOE configuration data, and the management of the latest vulnerability signature etc. Therefore, this TOE security objective counters the threats like T.Inbound Illegal Information, T.Unauthorized service access, T.New vulnerability attack, and TE.Poor administration. It also supports the organizational security policy of P.Secure administration by providing the means for the authorized administrator to manage the TOE securely.



4) 0. TSF data protection

When TSF data is modified without administrator ' s notice due to unexpected external attacks or TOE malfunctions, it may not be able to perform proper security policy. To prevent this event from occurring, the TOE ensures the proper operation of TSF by monitoring the TSF data for intentional or unintentional data changes and checking the integrity of TSF data. Therefore, this TOE security objective counters the threats like T.Failure and T.Unauthorized TSF data modification.

5) 0. Abnormal packet screening


This security objective ensures that of a large amount of packets coming from the external to the internal network, the packets which are not suitable for the TCP/IP standard, the packets with an internal network address, broadcasting packets and looping packets will not be allowed to come in. Therefore, this TOE security objective is intended to counter the threats such as T.Anomaly packet transfer and T.Spoofing IP address.

6) 0. DoS attack blocking

The attacker can make network DoS attacks on Intranet computers through the TOE. A typical network DoS attack is to exhaust the computer resources by sending too many service requests from a remote attacker. Then the Intranet computer, under the attacks, would prevent legitimate users from using the computer by allocating much of resource for the DoS attacker. To counter this attack, the TOE prevents a specific user from monopolizing the resources of a specific computer so that other legitimate users can use the resources without traffic. Therefore, this security objective is intended to counter the threats like T.DoS attack and T.Spoofing IP address.

7) 0. Identification

The TOE users are either logged-on administrators who manage the TOE with the TOE authentication or external users (IT entities) who just use Intranet computer without the TOE authentication. All the cases of two need the identification function to deal with security events. The identification of administrators is necessary to grant the full responsibility to them and the identification of external entities is necessary to generate the audit record for abnormal packet transmission, prevention of DoS attacks and address disguise attacks and connection trials by external entities. Therefore, this security objective counters

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

the threats like T.Masquerade, T.DoS attack, T.Spoofing IP address, T.Anomaly packet transfer, T.Replay attack, and T.Unauthorized TSF data modification. It also assists P.Audit.

8) O.Authentication

The user who wants to access the TOE should acquire the authentication. The authentication required in the TOE access may be vulnerable to the replay attack made by external entities. The TOE should provide the authentication mechanism, which can endure the replay attack according to the level of external entities. Therefore, this TOE security objective counters the threats like T.Masquerade and T.Replay attack.

9) O. Information flow control

The TOE is installed at the connection point between internal and external networks in order to control the information flow according to the security policy. According to allow/deny policy, this security objective ensure identifying and blocking various attacks on the network which mean virus attacks, e-mail or web services including illegal information and access to the unauthorized service. The TOE ensures the security of internal network by controlling the attacks based on the pre-defined rules and blocking the illegal access to the internal network. Therefore, this TOE security objective counters the threats like T.Inbound illegal information, T.Unauthorized service access and T.Bypassing.

8.1.2 Rational for the security objectives for the environment

1) OE. Physical security

The security objective for this environment is to ensure that the TOE is installed and operated at a physically secured place so that the TOE is protected from external physical attacks and TOE modification attempts. Therefore, the security objective for this environment is necessary to assist the assumption of A.Physical security and to counter the threat of T.Bypassing.

2) OE. Security maintenance

The security objective for this environment is to maintain the same level of security as the previous one by adopting changed environments and security policy to the TOE operation policy when the internal network environments is changed by configuration changes in internal network, the increase or decrease in host (or in service) and so on. Therefore, the



security objective for this environment is necessary to assist the assumption of A.Security maintenance and to counter the threat of T.New vulnerability attack.

3) OE. Trusted administrator

The security objective for this environment is to ensure the trustworthiness of an authorized administrator of the TOE. Therefore, the security objective for this environment is necessary to assist the assumptions of A.Trusted administrator and the security policy of P.Secure administration, and to counter the threats of TE.Poor administration and TE.Distribution and installation.

4) OE. Secure administration

The security objective for this environment is to ensure that the TOE is distributed and installed in a secure way and is configured, managed, and used securely by the authorized administrator. Therefore, the security objective for this environment is necessary to assist the assumption of A.Physical security and the security policy of P.Secure administration, and to counter the threats of T.Failure, T.New vulnerability attack, TE.Poor administration, and TE.Distribution and installation.

5) OE. Hardened OS


The security objective for this environment is to eliminate unnecessary OS services or measures and to harden the weak points in the OS so that the operation system is secure and reliable. Therefore, the security objective for this environment is necessary to assist the assumption of A.Hardened OS, and to counter the threats of T.Failure and T.New vulnerability attack.

6) OE. Single connection Point

The security objective for this environment is to ensure that all communications between internal and external networks are made through the TOE. Therefore, the security objective for this environment is necessary to assist the assumption of A.Single connection point, and to counter the threat of T.Bypassing.

7) OE. Vulnerability list update

The security objective for this environment is to protect the TOE and the internal network protected by the TOE from external attacks that are exploiting new vulnerability in them by renewing and managing the vulnerability database managed by the TOE. Therefore, the security objective for this environment is necessary to counter the threat of T.New

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

vulnerability attack.

8) OE.Reliable TIMESTAMP

The security objective for this environment is to provide the trusted NTP server and OS to maintain the reliable Timestamp for the TOE security function. Therefore, the security objective for this environment is necessary to assist the assumption A.Reliable TIMESTAMP.

9) OE. Secure Update Server

The security objective for this environment is to ensure that Update server to communicate with TOE is secure. Therefore, the security objective for this environment is necessary to assist the assumption A.Secure Update Server.

10) OE. Secure Database


The security objective for this environment is to ensure that TOE is secure for maintaining the function to store data and to search. Therefore, the security objective for this environment is necessary to assist the assumption A. Secure Database.

8.2 Security Requirements Rationale

This rationale demonstrates that the IT security functional requirements are suitable to meet the security objectives and hence address the security problems.

SFR	Security objectives									
	0.Availability	0.Audit	0.Administration	0.TSF data protection	0.Abnormal packet screening	0.DoS Attack blocking	0.Identification	0.Authentication	0.Information flow control	
FAU_ARP.1 Security alarms										
FAU_GEN.1 Audit data generation										
FAU_GEN.2 User identity association										
FAU_SAA.1 Potential violation analysis										
FAU_SAR.1 Audit review										
FAU_SAR.3 Selectable audit review										
FAU_SEL.1 Selective audit										
FAU_STG.1 Protected audit trail storage										
FAU_STG.3 reaction in case of possible audit data loss										
FAU_STG.4 Prevention of audit data loss										
FDP_IFC.1(1) Subset information flow control(1)										
FDP_IFC.1(2) Subset information flow control(2)										
FDP_IFF.1(1) Simple security attributes(1)										
FDP_IFF.1(2) Simple security attributes(2)										
FIA_AFL.1 Authentication failure handling										
FIA_ATD.1(1) Definition of user attributes(1)										
FIA_ATD.1(2) Definition of user attributes(2)										
FIA_UAU.1 Authentication										
FIA_UAU.7 Protected authentication feedback										
FIA_UID.2(1) User identification before any action(1)										
FIA_UID.2(2) User identification before any action(2)										
FMT_MOF.1(1) Management of Security Functions Behavior(1)										
FMT_MOF.1(2) Management of Security Functions Behavior(2)										
FMT_MSA.1 Management of security attributes										
FMT_MSA.3 Static attribute initialization										
FMT_MTD.1 Management of TSF data										
FMT_MTD.2 Management of limits on TSF data										
FMT_SMF.1 Specification of Management Functions										
FMT_SMR.1 Security roles										
FPT_AMT.1 Abstract machine testing										
FPT_FLS.1 Failure with preservation of secure state										
FPT_ITT.1 Basic protection of TSF data for internal transmission										
FPT_RVM.1 Non-Bypassability of the TSP										
FPT_SEP.1 TSF domain separation										
FPT_STM.1 Reliable time stamps										
FPT_TST.1 TSF testing										
FRU_FLT.1 Degraded fault tolerance : subset										
FRU_RSA.1 Maximum quotas										
FTA_SSL.1 TSF-initiated session locking										
FTA_SSL.3 TSF-initiated termination										
FTP_ITC.1 INTER-TSF TRUSTED CHANNEL										

[Table 8-2] Correlation of security objectives and security functional requirements

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

8.2.1 TOE Security Functional Requirements Rationale

This rationale demonstrates the following:

- Each TOE security objective is addressed by at least one TOE security functional requirement.
- Each TOE security functional requirement addresses at least one TOE security objective.

1) FAU_ARP.1 Security alarms

As this component ensures the ability to take reactions in case a potential security violation is detected, it meets TOE security objective: 0.Audit.

2) FAU_GEN.1 Audit data generation

As this component ensures that the TOE defines auditable events and generates the audit records, it meets TOE security objective: 0. Audit.

3) FAU_GEN.2 User identity association

As this component requires user identification to define auditable events and to trace the association of audit records with users, it meets TOE security objective: 0. Audit.

4) FAU_SAA.1 Potential violation analysis

As this component ensures the ability to monitor the audited events to indicate a potential violation of the TSP, it meets TOE security objective: 0. Audit.

5) FAU_SAR.1 Audit review

As this component ensures the capability for authorized administrators to review information from the audit records, it meets TOE security objective: 0. Audit.

6) FAU_SAR.3 Selectable audit review

As this component ensures the ability to perform searches of audit data based on criteria with logical relations, it meets TOE security objective: 0. Audit.

7) FAU_SEL.1 Selective audit

As this component ensures the ability to include or exclude auditable events from the set of audited events based on attributes, it meets security objective: 0. Audit.

8) FAU_STG.1 Protected audit trail storage

As this component ensures that TSF provides the ability to protect audit



record from unauthorized modification and/or deletion, it meets security objective: 0.Audit.

9) FAU_STG.3 reaction in case of possible audit data loss

As this component ensures that actions are taken if a threshold on the audit trail is exceeded, it meets TOE security objective: 0. Audit.

10) FAU_STG.4 Prevention of audit data loss

As this component ensures that actions are taken in case the audit trail is full, it meets TOE security objective: 0. Audit.

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

As this component ensures that the packet filtering security policy for TOE information flow control and its scope are defined, it meets TOE security objective: 0.Information flow control.

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

As this component ensures that the intrusion prevention security policy for TOE information flow control and its scope are defined, it meets TOE security objective: 0.Information flow control.

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

As this component describes the countermeasures for explicit attacks, it meets TOE security objective: 0.Abnormal packet screening, 0.Information flow control.

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


As this component describes the countermeasures for explicit attacks, it meets TOE security objective: 0.Abnormal packet screening, 0.Information flow control.

15) FIA_AFL.1 Authentication failure handling

As this component defines the number of unsuccessful administrator authentication attempts and ensures ability to take actions when the defined number has been met or surpassed, it meets TOE security objective: 0.Identification and 0.Authentication.

16) FIA_ATD.1(1) Definition of user attributes(1)

This component requires maintaining IP address as security attribute for external IT entity. As IP address identifies external IT entities and creates audit history serving as the criteria for illegal addresses, DoS attacks, and information flow control, this component meets TOE security objectives: 0.Audit, 0.Abnormal packet screening, 0.DoS attack blocking, 0.Identification, and 0.Information flow control.

 LG N-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

17) FIA_ATD.1(2) Definition of user attributes(2)

As this component requires identifying an administrator, it meets TOE security objective: 0.Audit and 0.Identification.

18) FIA_UAU.1 Authentication

As this component ensures the ability to authenticate administrators successfully, it meets TOE security objectives: 0.Administration, 0.TSF Data protection, and 0.Authentication.

19) FIA_UAU.7 Protected authentication feedback

As this component ensures that only limited authentication feedback is provided to the administrator while the authentication is in progress, it meets TOE security objective: 0. Authentication.

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

As this component requires that the identifier for external IT entity be identified as a computer IP address, which identifies external IT entities and creates audit history serving as the criteria for illegal addresses, DoS attacks, and information flow control, it meets TOE security objectives: 0. Audit, 0.Abnormal packet screening, 0.DoS attack blocking, 0.Identification, and 0.Information flow control.

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

As this component requires identification of the administrator, it meets TOE security objectives: 0.Audit, 0.Administration, 0.TSF data protection, and 0.Identification

22) FMT_MOF.1(1) Management of Security Functions Behavior(1)


As this component provides the authorized administrator with the ability to manage the security functions and ensures the availability when TOE failures occur, it meets TOE security objectives: 0.Availability and 0.Administration.

23) FMT_MOF.1(2) Management of Security Functions Behavior(2)

As this component provides the authorized administrator with the ability to manage the security functions and ensures the availability when TOE failures occur, it meets TOE security objectives: 0.Availability and 0.Administration.

24) FMT_MSA.1 Management of security attributes

As this component ensures that only authorized administrators are allowed to access TSF data, or security attribute data, which is necessary for the performance of TOE security functions, it meets TOE security objectives:

 LG N-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

0.Administration, 0.TSF data protection, 0.Information flow control.

25) FMT_MSA.3 Static attribute initialization

As this component ensures that only authorized administrators are allowed to access at the initialization of TSF data, or security attribute data, which is necessary for the performance of TOE security functions, it meets TOE security objectives: 0.Administration, 0.TSF data protection, 0.Information flow control.

26) FMT_MTD.1 Management of TSF data

As this component requires that only the authorized administrator should be able to manage the TSF data, it meets TOE security objectives: 0.Administration and 0.TSF data protection.

27) FMT_MTD.2 Management of limits on TSF data

As this component allows the authorized administrator to manage the limits of TSF data, and take countermeasures if the TSF data are at, or exceed the pre-defined limits, it meets TOE security objectives: 0.Availability and 0.Administration.

28) FMT_SMF.1 Specification of Management Functions

As this component requires specification of management functions such as security attributes, TSF data and security functions to be provided by the TSF, it meets TOE security objective: 0.Administration.

29) FMT_SMR.1 Security roles

As this component restricts the role of the TOE security administrator to authorized administrator roles, it meets TOE security objectives: 0.Administration, 0.Identification and 0.Authentication.

30) FPT_AMT.1 Abstract machine testing


As this component run a suite of tests to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF, it meets TOE security objectives:, 0. Availability, 0.TSF data protection.

31) FPT_FLS.1 Failure with preservation of secure state

As this component ensures that the TOE, in failure, preserves a secure state and performs the function of information flow control for the operation of core security functions, it meets TOE security objectives: 0.Availability, 0.Information flow control.

32) FPT_ITT.1 Basic protection of TSF data for internal transmission

As this component ensures the protection of TSF data for internal

 LG N-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

transmission through Management Console/Engine encryption, it meets TOE security objectives: 0.TSF data protection.

33) FPT_RVM.1 Non-bypassability of the TSP

As this component ensures that the TSP enforcement functions are invoked and succeeded and prevents bypassing of information flow control, it meets TOE security objective: 0. Information flow control.

34) FPT_SEP.1 TSF domain separation

As this component ensures that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects, it meets TOE security objective: 0.TSF data protection
0. Information flow control.

35) FPT_STM.1 Reliable time stamps

This component requires that the TSF maintains reliable time stamps. As the generated time stamps ensure the serial logging of security audit events in the event of creating the audit history, it meets TOE security objective: 0.Audit.

36) FPT_TST.1 TSF testing

This component ensures self-tests for the correct operation of TSF and requires the function to prevent or detect TOE ' s failure by verifying the integrity of TSF data and TSF executable code, it meets TOE security objectives: 0.Availability, 0.TSF data protection.

37) FRU_FLT.1 Degraded fault tolerance : subset

As this component ensures management activities through console or security management screen when TOE failures – such as hardware failure of network interfaces or software failure of a daemon (except the main daemon) – occur, and guarantees the performance of information flow control function, it meets the TOE security objectives: 0.Availability, 0.Information flow control.

38) FRU_RSA.1 Maximum quotas

As this component blocks the DoS attacks by requiring maximum quotas of the TOE assets for each user, it meets the TOE security objective: 0.DoS attack blocking.

39) FTA_SSL.1 TSF-initiated session locking

As this component requires the function for the TOE to lock the authorized session after a specified period of administrator inactivity, it meets TOE security objectives: 0.TSF data protection.




40) FTA_SSL.3 TSF-initiated termination

As this component secures the availability of network service by requiring the external IT entity to terminate the session with the internal computer after a certain period of time, it meets TOE security objectives: 0. DoS attack blocking.

41) FTP_ITC.1 Inter-TSF trusted channel

As this component requires the creation of the trusted channel when the authorized administrator manages the TOE locally or remotely, or when the TOE external vulnerability data servers communicate each other, it meets TOE security objectives: 0.Administration, 0.Authentication and 0.TSF data protection.

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

8.2.2 TOE assurance Requirements Rationale

The evaluation assurance level targeted by the TOE is EAL4, which requires the reinforcement of development document and vulnerability analysis, and automated configuration management in the process of development. The assurance documents necessary to satisfy the TOE assurance requirements are sufficient to satisfy the assurance requirements needed in EAL4 assurance level.

1) Rationale for the TOE assurance level of EAL4


- The TOE assurance level is determined as EAL4 to satisfy the claimed protection profile (Network Intrusion Prevention System Protection Profile V1.1, Dec. 21, 2005, KISA).

8.3 Dependencies Rationale

8.3.1 TOE Security Functional Requirements Dependencies

The following [Table 8-3] shows the dependencies among the functional components.

NO	Functional component	Dependency	Ref. No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	29
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 17
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 21
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_IFC.1(2)	FDP_IFF.1	12
12	FDP_IFF.1(1), FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	11 20
13	FIA_AFL.1	FIA_UAU.1	15
14	FIA_ATD.1(1), FIA_ATD.1(2)	-	-
15	FIA_UAU.1	FIA_UID.1	17
16	FIA_UAU.7	FIA_UAU.1	15
17	FIA_UID.2(1), FIA_UID.2(2)	-	-
18	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	23 24
19	FMT_MSA.1	[FDP_ACC.1 FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	11 23 24
20	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	19 24
21	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	23 24
22	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	21 24
23	FMT_SMF.1	-	-
24	FMT_SMR.1	FIA_UID.1	17
25	FPT_AMT.1	-	-
26	FPT_FLS.1	ADV_SPM.1	Assurance requirement
27	FPT_ITT.1	-	-
28	FPT_RVM.1	-	-
29	FPT_SEP.1	-	-
30	FPT_STM.1	-	-
31	FPT_TST.1	FPT_AMT.1	25
32	FRU_FLT.1	FPT_FLS.1	26
33	FRU_RSA.1	-	-
34	FTA_SSL.1	FIA_UAU.1	15
35	FTA_SSL.3	-	-
36	FTP_ITC.1	-	-

 LGN-Sys	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
--	---	---

[Table 8-3] Functional components Dependencies

- FAU_GEN.2, FIA_UAU.1, FMT_SMR.1 have dependencies on FIA_UID.1, which is satisfied by FIA_UID.2 that is Hierarchical to FIA_UID.1.

8.3.2 TOE Assurance Requirements Dependencies

This rationale can be omitted, because the dependencies for each assurance package provided by the Common Criteria for IT Security Evaluation are completely fulfilled.

8.4 TOE Summary Specification Rationale

The TOE summary specification rationale shall demonstrate that the IT security functions and assurance requirements are suitable to meet the TOE security functions and assurance measures, so that they are suitable to address security problems.


8.4.1 Correlations of Security Functional Requirements and TOE Security Functions

[Table 8-5] shows the correlation between IT security functional requirements and TOE security functions.

Category	SFR	TSF
Security audit	FAU_ARP.1 Security alarms	Audit data generation(SFAU_GEN) Reaction(SFDP_ACT)
	FAU_GEN.1 Audit data generation	Audit data generation(SFAU_GEN) Reaction(SFDP_ACT)
	FAU_GEN.2 User identity association	Audit data generation(SFAU_GEN)
	FAU_SAA.1 Potential violation analysis	Detection/prevention event information collection and analysis(SFDP_CHK)
	FAU_SAR.1 Audit review	Audit data search and retrieval(SFAU_SAR) Intrusion detection/prevention result report(SFMT_RPT)
	FAU_SAR.3 Selectable audit review	Audit data search and retrieval(SFAU_SAR) Intrusion detection/prevention result report(SFMT_RPT)
	FAU_SEL.1 Selective audit	Audit data generation(SFAU_GEN)
	FAU_STG.1 Protected audit trail storage	Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP)
	FAU_STG.3 reaction in case of possible audit data loss	Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP)
	FAU_STG.4 Prevention of audit data loss	Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP)
User data protection	FDP_IFC.1(1) Subset information flow control(1)	Detection/prevention event information collection and analysis(SFDP_CHK)
	FDP_IFC.1(2) Subset information flow control(2)	Detection/prevention event information collection and analysis(SFDP_CHK)
	FDP_IFF.1(1) Simple security attributes(1)	Detection/prevention event information collection and analysis(SFDP_CHK)
	FDP_IFF.1(2) Simple security attributes(2)	Detection/prevention event information collection and analysis(SFDP_CHK) Reaction(SFDP_ACT)
Identification and Authentication	FIA_AFL.1 Authentication failure handling	User identification and authentication (SFIA_LOGON) Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)
	FIA_ATD.1(1) Definition of user attributes(1)	User information management(SFMT_USR) Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)

FIA_ATD.1(2) Definition of user attributes(2)	of	User information management(SFMT_USR) User identification and authentication (SFIA_LOGON)
FIA_UAU.1 Authentication		User identification and authentication (SFIA_LOGON) Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)
FIA_UAU.7 Protected authentication feedback		User identification and authentication (SFIA_LOGON)
FIA_UID.2(1) User identification before any action(1)	any	Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)
FIA_UID.2(2) User identification before any action(2)	any	User identification and authentication(SFIA_LOGON)

Category	SFR	TSF
Security Management	FMT_MOF.1(1) Management of Security Functions Behavior(1)	User information management(SFMT_USR) Security violation events management(SFMT_POL) New policy online update(SFMT_POLUP) Management console/engine time synchronization(SFMT_TIME)
	FMT_MOF.1(2) Management of Security Functions Behavior(2)	Management Console configuration information management(SFMT_PSM) Engine configuration information management(SFMT_SSS) New policy online update(SFMT_POLUP) Intrusion detection/prevention result report(SFMT_RPT) Management console/engine time synchronization(SFMT_TIME)
	FMT_MSA.1 Management of security attributes	Security violation events management(SFMT_POL)
	FMT_MSA.3 Static attribute initialization	Security violation events management(SFMT_POL)
	FMT_MTD.1 Management of TSF data	Management Console configuration information management(SFMT_PSM) Engine configuration information management(SFMT_SSS) Security violation events management(SFMT_POL) New policy online update(SFMT_POLUP)
	FMT_MTD.2 Management of limits on TSF data	Management Console configuration information management(SFMT_PSM) Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP)
	FMT_SMF.1 Specification of Management Functions	User information management(SFMT_USR) Management Console configuration information management(SFMT_PSM) Engine configuration information management(SFMT_SSS) Security violation events management(SFMT_POL) New policy online update(SFMT_POLUP) Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP) Intrusion detection/prevention result report(SFMT_RPT) Management console/engine time synchronization(SFMT_TIME)
	FMT_SMR.1 Security roles	User identification and authentication (SFIA_LOGON)
TSF Protection	FPT_AMT.1 Abstract machine testing	Management Console/Engine Health Checking(SFPT_CHKSYS)
	FPT_FLS.1 Failure with preservation of secure state	Management Console/Engine Health Checking(SFPT_CHKSYS)
	FPT_ITT.1 Basic protection of TSF data for internal transmission	Mutual identification and authentication for remote connection through the communication channel(SFIA_UID)
	FPT_RVM.1 Non-bypassability of the TSP	Detection/prevention event information collection and analysis(SFDP_CHK)
	FPT_SEP.1 TSF domain separation	Management Console/Engine Health Checking(SFPT_CHKSYS)
	FPT_STM.1 Reliable time stamps	Management console/engine time synchronization(SFMT_TIME)
	FPT_TST.1 TSF testing	TSF stored data integrity check(SFPT_CHKINT)
Resource utilization	FRU_FLT.1 Degraded fault tolerance : subset	Management Console/Engine Health Checking(SFPT_CHKSYS)
	FRU_RSA.1 Maximum quotas	Detection/prevention event information collection and analysis(SFDP_CHK)

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

TOE access	FTA_SSL.1 TSF-initiated session locking	TSF-initiated session locking((SFTA_SSL)
	FTA_SSL.3 TSF-initiated termination	TSF-initiated session locking((SFTA_SSL)
Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel	Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)

[Table 8-4] Correlations of security functional requirements and TOE security functions

8.4.2 TOE Summary Specification Rationale

This rationale demonstrates the following:

- Each security functional requirement is addressed by at least one TOE summary specification.
- However, FAU_STG.1 Protected audit trail storage shall be countered by procedural measures through database, and supplemented by prevention of the loss of intrusion detection/prevention and audit data (SFMT_BKUP).

1) FAU_ARP.1 Security alarms

This component uses Audit Data Generation (SFAU_GEN) and Counter Attack Activity (SFDP_ACT) to ensure the ability to take action in case a potential security violation is detected.

2) FAU_GEN.1 Audit data generation

This component uses Audit Data Generation (SFAU_GEN) to ensure the ability to define auditable events and generate audit record.

3) FAU_GEN.2 User identity association

This component uses Audit Data Generation (SFAU_GEN) to ensure that the user identification is needed to define the auditable events and trace the audit record with the user.

4) FAU_SAA.1 Potential violation analysis

This component uses Detection/prevention event information collection and analysis(SFDP_CHK) to ensure the ability to scrutinize the audited events and based upon the results detect a potential violation.

5) FAU_SAR.1 Audit review

This component uses Audit data search and retrieval(SFAU_SAR), Intrusion detection/prevention result report(SFMT_RPT) to ensure the ability of the authorized administrator to review audit records.

6) FAU_SAR.3 Selectable audit review

This component uses Audit data search and retrieval(SFAU_SAR), Intrusion detection/prevention result report(SFMT_RPT) to ensure the ability to perform searches and sorting of audit data based on the standard with logical relations.

7) FAU_SEL.1 Selective audit

This component uses Audit data generation(SFAU_GEN) to ensure the ability to include or exclude auditable events from the set of audited events based on the attributes.

8) FAU_STG.1 Protected audit trail storage

This component uses Prevention of the Loss of Intrusion Detection/Prevention and Audit Data (SFMT_BKUP) to ensure the ability to protect the stored audit records from unauthorized modifications and/or deletion.

9) FAU_STG.3 reaction in case of possible audit data loss

This component uses Prevention of the Loss of Intrusion Detection/Prevention and Audit Data (SFMT_BKUP) to ensure the ability to take countermeasures when the audit trail exceeds the pre-defined limit.

10) FAU_STG.4 Prevention of audit data loss

This component uses Prevention of the Loss of Intrusion Detection/Prevention and Audit Data (SFMT_BKUP) to ensure the ability to take countermeasures when the audit trail storage is full.

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

This component uses Detection/prevention event information collection and analysis (SFDP_CHK) to ensure the policy which deny all access except allowed rules.

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

This component uses Detection/prevention event information collection and analysis (SFDP_CHK) to ensure the policy which block harmful traffic.

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

This component uses Detection/prevention event information collection and analysis(SFDP_CHK) to describe the reaction for explicit attacks.

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

This component uses Detection/prevention event information collection and analysis(SFDP_CHK), Reaction(SFDP_ACT) to describe the reaction for explicit attacks.

15) FIA_AFL.1 Authentication failure handling

This component uses User identification and authentication(SFIA_LOGON) to ensure the ability that defines the number of unsuccessful authentication attempts and takes countermeasures when the authentication attempts exceed the pre-defined number. This component uses Mutual identification and authentication for remote connection through the communication channel (SFIA_UID) to ensure the process by disconnecting management console and engine when authentication failure occurred.

16) FIA_ATD.1(1) Definition of user attributes(1)



This component uses User information management(SFMT_USR) to require that the identifier for the external IT entities be identified as a computer IP address, port information, Mac address add, which shall identify external IT entities and create the audit history serving as the criteria for illegal addresses, DoS attacks, and information flow control.

17) FIA_ATD.1(2) Definition of user attributes(2)

This component uses User information management(SFMT_USR) to require identification of administrator.

18) FIA_UAU.1 Authentication

This component uses User identification and authentication(SFIA_LOGON), Mutual identification and authentication for remote connection through the communication channel (SFIA_UID) to ensure the ability to authenticate the administrator and remote connector.

19) FIA_UAU.7 Protected authentication feedback

This component uses User identification and authentication(SFIA_LOGON) to ensure that only pre-defined feedbacks shall be provided to the administrator while the authentication is in progress.

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

This component uses Mutual identification and authentication for remote connection through the communication channel (SFIA_UID) to ensure that it requires that the identifier for the external IT entities be identified as a computer IP address, port information, MAC address, which shall identify external IT entities and create the audit history serving as the criteria for illegal addresses, DoS attacks, and information flow control.

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

This component uses User identification and authentication(SFIA_LOGON) to require identification of administrator.

22) FMT_MOF.1(1) Management of Security Functions Behavior(1)

This component uses User information management(SFMT_USR), Security violation events management(SFMT_POL), New policy online update(SFMT_POLUP), Management console/engine time synchronization(SFMT_TIME) to provide the authorized administrator with the ability to manage the security functions.

23) FMT_MOF.1(2) Management of Security Functions Behavior(2)

This component uses Management Console configuration information management(SFMT_PSM), Engine configuration information

management(SFMT_SSS), New policy online update(SFMT_POLUP), Intrusion detection/prevention result report(SFMT_RPT), Management console/engine time synchronization(SFMT_TIME) to provide the authorized administrator with the ability to manage the security functions.

24) FMT_MSA.1 Management of security attributes

This component uses Security violation events management(SFMT_POL) to ensure that only the authorized administrator is allowed to get access to the TSF data, or security attribute data, which is needed in performing the TOE security functions.

25) FMT_MSA.3 Static attribute initialization

This component uses Security violation events management(SFMT_POL) to ensure that default value is provided.

26) FMT_MTD.1 Management of TSF data

This component uses User information management(SFMT_USR), Management Console configuration information management(SFMT_PSM), Engine configuration information management(SFMT_SSS), Security violation events management(SFMT_POL), New policy online update(SFMT_POLUP), Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP), Intrusion detection/prevention result report(SFMT_RPT), Management console/engine time synchronization(SFMT_TIME) to require that only the authorized administrator should be able to manage the TSF data.

27) FMT_MTD.2 Management of limits on TSF data

This component uses Management Console configuration information management(SFMT_PSM), Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP) to secure the TOE availability by ensuring that the authorized administrator is allowed to manage the limits of TSF data and takes countermeasures if the TSF data are at, or exceed the predefined limits.

28) FMT_SMF.1 Specification of Management Functions

This component uses User information management(SFMT_USR), Management Console configuration information management(SFMT_PSM), Engine configuration information management(SFMT_SSS), Security violation events management(SFMT_POL), New policy online update(SFMT_POLUP), Prevention of the loss of intrusion detection/prevention and audit data(SFMT_BKUP), Intrusion detection/prevention result report(SFMT_RPT), Management console/engine time synchronization(SFMT_TIME) to ensure for the



specification of management functions such as security attributes, TSF data, and security function, which should be provided by TSF.

29) FMT_SMR.1 Security roles

This component uses User identification and authentication(SFIA_LOGON) to limit the role of a TOE security administrator to that of an administrator.

30) FPT_AMT.1 Abstract machine testing

This component uses Management Console/Engine Health Checking(SFPT_CHKSYS) to ensure that a suite of tests are performed to demonstrate the correct operation of the security assumptions provided by the underlying abstract machine of the TSF.

31) FPT_FLS.1 Failure with preservation of secure state

This component uses Management Console/Engine Health Checking(SFPT_CHKSYS) to ensure that a secure state is preserved and the function of information flow control is performed when TOE failures occur.

32) FPT_ITT.1 Basic protection of TSF data for internal transmission

This component uses Mutual identification and authentication for remote connection through the communication channel (SFIA_UID) to ensure the protection of TSF data.

33) FPT_RVM.1 Non-bypassability of the TSP

This component uses Detection/prevention event information collection and analysis(SFDP_CHK) to ensure that the bypass of information flow control is prevented by assuring TSP enforcement functions to be invoked and succeed.

34) FPT_SEP.1 TSF domain separation


This component uses Management Console/Engine Health Checking(SFPT_CHKSYS) to ensure that TSF maintains a security domain for its own execution which protects it from interference and tampering by untrusted subjects.

35) FPT_STM.1 Reliable time stamps

This component uses Management console/engine time synchronization(SFMT_TIME) to provide reliable Timestamps to be used by TSF. The generated time ensures the serial logging of security audit events in the event of creating the audit history.

36) FPT_TST.1 TSF testing

This component uses TSF stored data integrity check(SFPT_CHKINT) to ensure a suite of self tests to demonstrate the correct operation of TSF, and prevents or detects TOE failures by providing the authorized administrator

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

with the capability to verify the integrity of TSF data and TSF executable code.

37) FRU_FLT.1 Degraded fault tolerance : subset

This component uses Management Console/Engine Health Checking(SFPT_CHKSYS) to demand the core security functional actions when TOE failures occur, and to ensure the operation of information flow control.

38) FRU_RSA.1 Maximum quotas

This component uses Detection/prevention event information collection and analysis(SFDP_CHK) to block the DoS attacks by enforcing maximum quotas of the TOE assets that each user can use.

39) FTA_SSL.1 TSF-initiated session locking

This component uses TSF-initiated session locking((SFTA_SSL) to allow TOE to lock an interactive session after a specified period of user inactivity.

40) FTA_SSL.3 TSF-initiated termination

This component uses Detection/prevention event information collection and analysis(SFDP_CHK) to allow the external IT entities to terminate an interactive session after a period of time so that it can promote the availability of network service.


41) FTP_ITC.1 Inter-TSF trusted channel

This component uses Mutual identification and authentication for remote connection through the communication channel (SFIA_UID) to allow the administrator to manage TOE locally or remotely or to call for the creation of a trusted channel in communications between external vulnerability data servers.

8.4.3 Correlations of Assurance Requirements and Assurance Measures

The assurance measures for each assurance component are listed in the [Table 8-5].

Assurance class	Assurance component		Assurance measures
Configuration Management	ACM_AUT.1	Partial CM automation	Configuration Management Document
	ACM_CAP.4	Generation support and acceptance procedures	Configuration Management Document
	ACM_SCP.2	Problem tracking CM coverage	Configuration Management Document
Delivery and operation	ADO_DEL.2	Detection of modification	Delivery Procedure
	ADO_IGS.1	Installation, generation, and start-up procedures	Installation Manual
Development	ADV_FSP.2	Fully defined external interfaces	Functional specification
	ADV_HLD.2	Security enforcing high-highlevel	High-level Design
	ADV_IMP.1	Subset of the implementation of the TSF	Validation Specification
	ADV_LLD.1	Descriptive low-level design	Low-level Design
	ADV_RCR.1	Informal correspondence demonstration	Validation Specification
	ADV_SPM.1	Informal TOE security policy model	Security Policy Modeling
Guidance documents	AGD_ADM.1	Administrator guidance	Administrator Guidance document
	AGD_USR.1	User guidance	-
Life Cycle Support	ALC_DVS.1	Identification of security measures	Life Cycle Support
	ALC_LCD.1	Developer defined life-cycle model	Life Cycle Support
	ALC_TAT.1	Well-defined development tools	Life Cycle Support
Tests	ATE_COV.2	Analysis of coverage	Testing
	ATE_DPT.1	Testing: high-level design	Testing
	ATE_FUN.1	Functional testing	Testing
	ATE_IND.2	Independent testing - sample	-
Vulnerability	AVA_MSU.2	Validation of analysis	Misuse Analysis

	Document Identification No.		Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04		Security Target

assessment	AVA_SOF.1	Strength of TOE security function evaluation	Vulnerability Analysis
	AVA_VLA.2	Independent vulnerability analysis	Vulnerability Analysis

[Table 8-5] Assurance measures

The configuration management document will provide the assurance of the components concerning Configuration Management such as ACM_AUT.1 Partial configuration management automation, ACM_CAP.4 Generation support and acceptance procedures, and ACM_SCP.2 Problem tracking CM coverage).

Assurance of the components concerning Delivery and Operation are provided by the delivery procedure for ADO_DEL.2 Detection of modification and the installation manual for ADO_IGS.1 installation, generation, and operation procedures.

Assurance of the components concerning Development is provided by the functional specification for ADV_FSP.2 Fully defined external interface, highlevel design for ADV_HLD.2 Security enforcing high-level design, low-level design for ADV_LLD.1 Descriptive low-level design, and validation specification for both ADV_IMP.1 Subset of the implementation of the TSF and ADV_RCR.1 Informal correspondence demonstration.


For the components concerning Guidance Documents, AGD_ADM.1 Administrator guidance is assured by administrator guidance while AGD_USR.1 User guidance doesn't require assurance since there are no users other than the administrator.

For the components concerning Life Cycle Support, the life cycle support assures ALC_DVS.1 Identification of security measures, ALC_LCD.1 Developer defined life cycle model, and ALC_TAT.1 Well-defined development tools.

For the components dealing with Tests, the testing assures ATE_COV.2 Analysis of coverage, ATE_DPT.1 Testing: high-level design, ATE_FUN.1 Functional testing, and ATE_IND.2 Independent testing - sample.

The misuse analysis assures AVA_MSU.2 Validation of analysis, and the vulnerability analysis assures AVA_SOF.1 Strength of TOE security function evaluation and AVA_VLA.2 Independent vulnerability analysis.

8.5 PP Claims Rationale

	Document Identification No.	Document Type
	SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Security Target

This ST accepted all security functional requirements from Network Intrusion Prevention System Protection Profile V1.1, Dec. 21, 2005, KISA). The added or modified requirements are shown in the following table:

Category	Item	Remark
Assumption	A.Reliable TIMESTAMP	Addition
	A.Secure Update Server	
	A.Secure Database	
Security objectives for the environment	OE.Reliable TIMESTAMP	Addition
	OE.Secure Update Server	
	OE.Secure Database	
TOE Security function requirements	FPT_ITT.1 Basic protection of TSF data for internal transmission	Addition

The requirements for Network Intrusion Prevention System Protection Profile are all included in the ST. Added or modified requirements are as follows;

Assumption - A.Reliable TIMESTAMP, A.Secure Update Server, A.Secure Database


Security objectives for the environment - OE.Reliable TIMESTAMP, OE.Secure Update Server, OE.Secure Database.

TOE Security function requirements - FPT_ITT.1 Basic protection of TSF data for internal transmission.

8.6 SOF Claim Rationale

This ST conforms to the SOF level claimed in the Network Intrusion Prevention System Protection Profile. Since the threat agent is assumed to possess a moderate expertise, resources, and motivation, the PP should provide security functions of SOF-medium. Therefore this ST also requires SOF-medium in accordance with the SOF claim of the PP.

The general password mechanism used in “ FIA_UAU.1 Timing of Authentication ” satisfies SOF-medium as the probability of the attacker possessing a moderate attack potential to know the password is 1/18,514,312,960 according to the calculation system in CEM B.8.

	Document Identification No. SafezoneIPS V1.0(SZ5XU) Security Target_20070314_V1.00.04	Document Type Security Target
---	---	---

The TOE is used in an ordinary network environment where an attacker may attack the TOE with medium-level of expertise, resources, and equipment. Thus the SOF-medium is selected to disable the attacker.