


SafezoneIPS V3.0

Security Target_20051205_V1.00.02

LG N-Sys Security Gr. R&D Division



	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	
	Product Name + Version + (Model) SafezoneIPS V3.0(SZ-4000)	Document Type Security Target

Summary

This document is the security target of a network intrusion prevention system (Product name: SafezoneIPS; Version: V3.0; Model: SZ-4000; Platform: Self OS(SZOS V1.0)).

Revision History


Version	Date	Reason	Author	Revision Request
V1.00.00	Jun. 27, 2005	Initial official registration	J.H. Park	
V1.00.01	Aug. 15, 2005	Recommendations from the observation report - Correct types - Delete redundant sentences	J.H. Park	
V1.00.02	Dec. 5, 2005	Modifications discussed at the follow-up meeting after the CCRA examination	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.




Table of Contents

1. SECURITY TARGET (ST) INTRODUCTION.....	5
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 NETWORK ENVIRONMENT	18
2.3 TOE SCOPE AND BOUNDARY	20
2.3.1 <i>Physical Scope and Boundary</i>	22
2.3.2 <i>Logical Scope and Boundary</i>	23
3. TOE SECURITY ENVIRONMENT	26
3.1 ASSUMPTION.....	26
3.2 THREAT	28
3.2.1 <i>Threats to the TOE</i>	28
3.2.2 <i>Threats to the TOE Operational Environment</i>	29
3.3 ORGANIZATIONAL SECURITY POLICY	31
4. TOE SECURITY OBJECTIVES.....	32
4.1 SECURITY OBJECTIVES FOR THE TOE.....	32
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT	34
5. IT SECURITY REQUIREMENTS	36
5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS	37
5.1.1 <i>Security Audit</i>	38
5.1.2 <i>User Data Protection</i>	42
5.1.3 <i>Identification and Authentication</i>	44
5.1.4 <i>Security Management</i>	46
5.1.5 <i>Protection of the TSF</i>	49
5.1.6 <i>Resource Utilization</i>	51

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0	Security Target
	Security Target_20051205_V1.00.02	


5.1.7	<i>TOE Access</i>	52
5.1.8	<i>Trusted Path/Channels</i>	53
5.2	TOE SECURITY ASSURANCE REQUIREMENTS	55
5.2.1	<i>Configuration Management</i>	55
5.2.2	<i>Delivery and Operation</i>	57
5.2.3	<i>Development</i>	58
5.2.4	<i>Guidance Documents</i>	62
5.2.5	<i>Life Cycle Support</i>	64
5.2.6	<i>Tests</i>	66
5.2.7	<i>Vulnerability assessment</i>	68
5.3	SECURITY REQUIREMENT FOR THE IT ENVIRONMENT.....	70
5.3.1	<i>Protection of the TSF</i>	70
6.	TOE SUMMARY SPECIFICATION	72
6.1	TOE SECURITY FUNCTIONS	72
6.1.1	<i>Security Audit (SFAU)</i>	72
6.1.2	<i>User Data Protection (SFDP)</i>	76
6.1.3	<i>Identification and Authentication (SFIA)</i>	81
6.1.4	<i>Security Management (SFMT)</i>	84
6.1.5	<i>TSF Protection (SFPT)</i>	92
6.1.6	<i>TOE access (SFTA)</i>	94
6.2	ASSURANCE MEASURES.....	95
7.	PROTECTION PROFILE CLAIMS	97
7.1	PROTECTION PROFILE REFERENCE.....	97
7.2	PROTECTION PROFILE TAILORING	97
7.3	PROTECTION PROFILE ADDITIONS.....	98
7.3.1	<i>Protection Profile Modifications</i>	105
8.	RATIONALE	106
8.1	SECURITY OBJECTIVES RATIONALE.....	106
8.1.1	<i>Rationale for the security objectives for the TOE</i>	108
8.1.2	<i>Rational for the security objectives for the environment</i>	110
8.2	SECURITY REQUIREMENTS RATIONALE	112
8.2.1	<i>TOE Security Functional Requirements Rationale</i>	114
8.2.2	<i>TOE assurance Requirements Rationale</i>	119
8.3	DEPENDENCY RATIONALE.....	120

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

8.3.1	<i>TOE Security Functional Requirements Dependencies</i>	120
8.3.2	<i>TOE Assurance Requirements Dependencies</i>	121
8.4	TOE SUMMARY SPECIFICATION RATIONALE.....	122
8.4.1	<i>Correlations of Security Functional Requirements and TOE Security Functions</i>	122
8.4.2	<i>TOE Summary Specification Rationale</i>	126
8.4.3	<i>Correlations of Assurance Requirements and Assurance Measures</i>	132
	<i>Guidance documents</i>	132
8.5	PP CLAIMS RATIONALE	133
8.6	SOF CLAIM RATIONALE	134

List of Figures/Tables

[Figure 2-1] SafezoneIPS(SZ-4000) network configuration.....	18
[Figure 2-2] SafezoneIPS(SZ-4000) network configuration (Dual configuration) ...	19
[Table 2-1] SafezoneIPS performance and hardware specification.....	20
[Figure 2-3] TOE architectural diagram	22
[Table 3-1] Identification of assumptions	26
[Table 3-2] Identification of threats	28
[Table 3-3] Identification of organizational security policies	31
[Table 4-1] Identification of TOE security objectives	32
[Table 5-1] Security functional requirements	37
[Table 5-3] Assurance components	55
[Table 6-1] Assurance measures	96
[Table 7-1] Protection profile additions and modifications.....	105
[Table 8-1] Correlation of security environment and security objectives	107
[Table 8-2] Correlation of security objectives and security functional requirements ..	113
[Table 8-3] Functional components dependencies.....	121
[Table 8-4] Correlations of security functional requirements and TOE security functions ..	125
[Table 8-5] Assurance measures	133


	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

1. Security Target (ST) Introduction

This document is the security target of a network prevention system (Product name: SafezoneIPS; Version: V3.0; Model: SZ-4000; Platform: Self OS(SZOS V1.0), hereinafter referred to as “ SafezoneIPS”). Based on the Network Intrusion Prevention System Protection Profile (Dec. 21, 2005, KISA), this ST defines the security functions and assurance measures and describes the security requirements used for evaluation and general information such as implementation methods and technical information.

1.1 ST Identification

- 1) Title : SafezoneIPS V3.0 Security Target_20051205_V1.00.02
Version : V1.00.02
Written date : Dec. 5, 2005
- 2) Author : LG N-Sys
- 3) Common Criteria(CC) version : The Common Criteria for IT Security Evaluation (2005-25, the Ministry of Information and Communication) and Final Interpretation(FI) that CCIMB recognized by Jun. 2005.
- 4) Evaluation Assurance Level(EAL) : EAL4
- 5) Protection Profile claimed : Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005, KISA)
 - TOE identifier : SafezoneIPS
 - TOE Version : V3.0
- 6) TOE description : SafezoneIPS is a network intrusion prevention system that is installed in an inLine mode by switching the in-bound and out-bound lines of a target network section to monitor all network traffic that flow through the system. SafezoneIPS blocks the abnormal traffic detected and notifies the operator of the attack.
- 7) Keyword : Network Intrusion Prevention System, Access Control, Information Flow Control

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

1.2 Security Target(ST) Overview

SafezoneIPS is a network prevention system that is installed in an InLine mode by switching the in-bound and out-bound lines of a target network section to monitor all traffic that flow through the system. SafezoneIPS blocks the abnormal traffic detected and notifies the operator of the attack. That is, SafezoneIPS protects 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 the network traffic load. In addition, SafezoneIPS is a hardware-type intrusion prevention system equipped with a dedicated ASIC-based packet processor (dedicated board) that can process every passing network traffic without any loss in real time regardless of the characteristic of the packet.


Prepared for CC certification of SafezoneIPS, this ST provides ST introduction, TOE description, TOE security environment, TOE security objectives, IT security requirements, and TOE summary specification, and describes the protection profile claimed and the rationale.

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

2) “ TOE Description” gives broad information about the product type, general TOE function, and 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.


 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

5) “ IT Security Requirements” describes the security requirements for the TOE and the 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.

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

1.3 Common Criteria(CC) Conformance

TOE conforms to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) V2.2 below and applies Final Interpretation (Jun. 2005).

1) Part 2 conformant

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

2) Part 3 conformant

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

3) Evaluation Assurance Level


Evaluation Assurance Level of the TOE is EAL4.

4) Protection Profile Conformance

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

5) SOF claim

The SOF targeted by the TOE is SOF-medium.

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type 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 of TOEs that meet specific consumer needs.

- Human User

Any person who interacts with the TOE

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	---	---

- 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, SSS/SCA 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 2.2 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) from Part 3 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 an 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.

- Evaluation Assurance Level (EAL)

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

- Family

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

A grouping of components from CC that share common security objectives but may differ in emphasis or rigor.

- 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.

- 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.

- Direct Memory Access (DMA)

A computer bus function that directly transfers data from a peripheral device (e.g. HDD) to the mother board memory.

- Peripheral Component Interconnect (PCI)

An interconnection system between devices equipped in extension slots located close to a microprocessor for high-speed operation.

- SEED

Standardized in 1999 (TTA.KO-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.


- Common abbreviations of CC

- CC : Common Criteria
- EAL : Evaluation Assurance Level
- IT : Information Technology
- PP : Protection Profile
- SFP : Security Function Policy
- SOF : Strength of Function
- ST : Security Target
- TOE : Target of Evaluation
- TSC : TSF Scope of Control
- TSF : TOE Security Functions
- TSFI : TSF Interface
- TSP : TOE Security Policy

	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type 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 (ISO/IEC 15408) V2.2, Parts 1,2,3
- [4] Common Criteria for Information Technology Security Evaluation (May 21, 2005), the Ministry of Information and Communication, KISA

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

2. TOE Description

2.1 Product Type


1) SafezoneIPS is a network intrusion prevention system that is installed in an InLine mode by switching the in-bound and out-bound lines of a target network section to monitor all network traffic that flow through the system. On detecting abnormal traffic, SafezoneIPS blocks the traffic out of the network and notifies the operator of the attack. That is, SafezoneIPS protects the internal IT asset of the target network not only from direct attacks that exploit vulnerabilities, but also from any illegal attacks such as a DoS attack that can shut down the network by increasing the network traffic load. In addition, SafezoneIPS is a hardware-type intrusion prevention system equipped with a dedicated ASIC packet processor (dedicated board) that can process all network traffic without any loss in real time regardless of the characteristic of the packet.

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 having abnormal structure and DoS attacks; a function to control unauthorized traffic; 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.

4) TOE is implemented as a network intrusion prevention system, and is operated for the purpose of protecting the resource of computer networks defined in the security policy.

5) TOE is located at the connection point between an external network, such as the Internet, and an organizational internal network, where it controls the flow of

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

information according to the security objectives.

6) TOE detects illegal events in real time and performs as a reaction the intrusion prevention function defined by the administrator based on the analysis result.

The following are the security functions of the TOE:

- 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. Security Audit also provides audit data protection function. In case the capacity of the memory is full, this function notifies the manager to prevent any loss of audit data that may occur due to lack of memory.

- 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

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. 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.

In addition, in cases where components of TOE interact remotely through internal communication channels, one identifies and authenticates the node of the other side to ensure trusted path and channel between TSFs. The communication between the administrator console and the engine is encrypted using SEED and its integrity is verified through SHA-1 to prevent any



modification or exposure of the data.

- 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. Security Management function provides the rules for detection/prevention SafezoneIPS performs and the managerial actions retrieving and modifying information related to the status and configuration of SafezoneIPS.

- TSF Protection

TSF Protection provides a regular check function to assure that the security assumptions related to the underlying abstract machine are properly operating. It performs checking when initially started, periodically during normal operation, and upon request of an authorized user to decide whether the main components running on the TOE system are normally operating in order. It also preserves a secure state when failure occurred and ensures safe operation of the TOE by periodically monitoring H/W failures related to the CPU and memory, S/W failures such as OS errors, and other failures caused by attacks.

- Resource Utilization

This function ensures safe operation of the TOE by periodically monitoring H/W failures related to the CPU and memory, S/W failures such as OS errors, and other failures caused by attacks.

- TOE Access

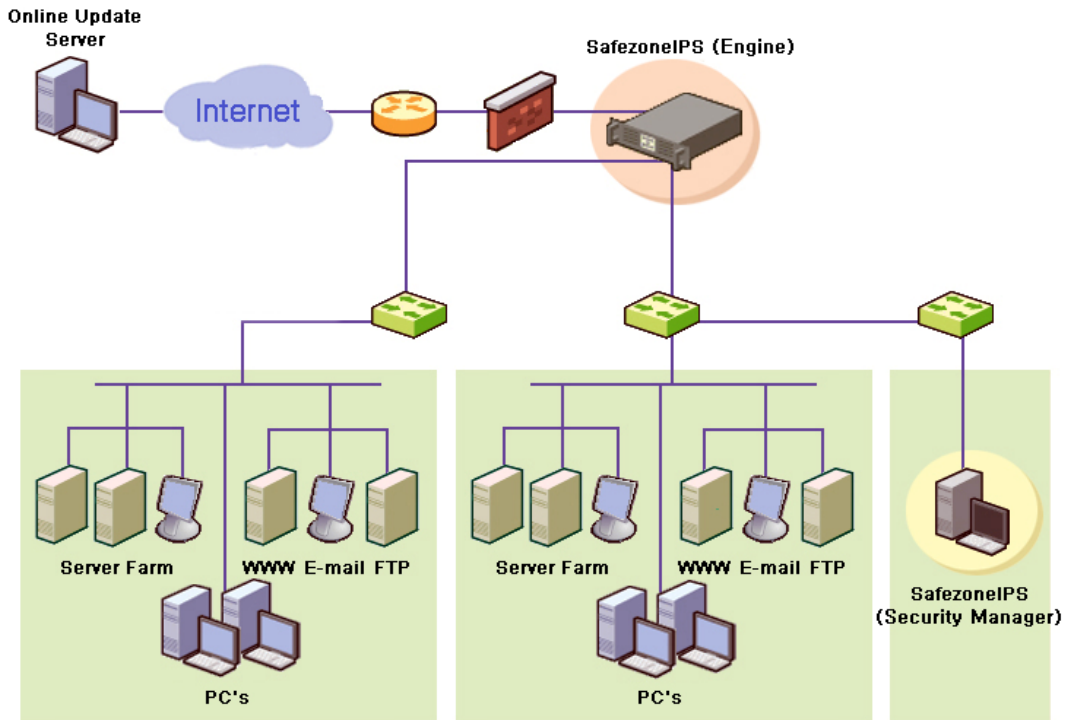
If the TOE is accessed by an authorized administrator but remains inactive for a certain period of time, the interacting session will be locked on the basis of the identification and authentication in order to protect the TOE during the time. The session locking is performed on the administrator console, which is the entry point of the interaction between the TOE function and the administrator.

- Trusted Path/Channels

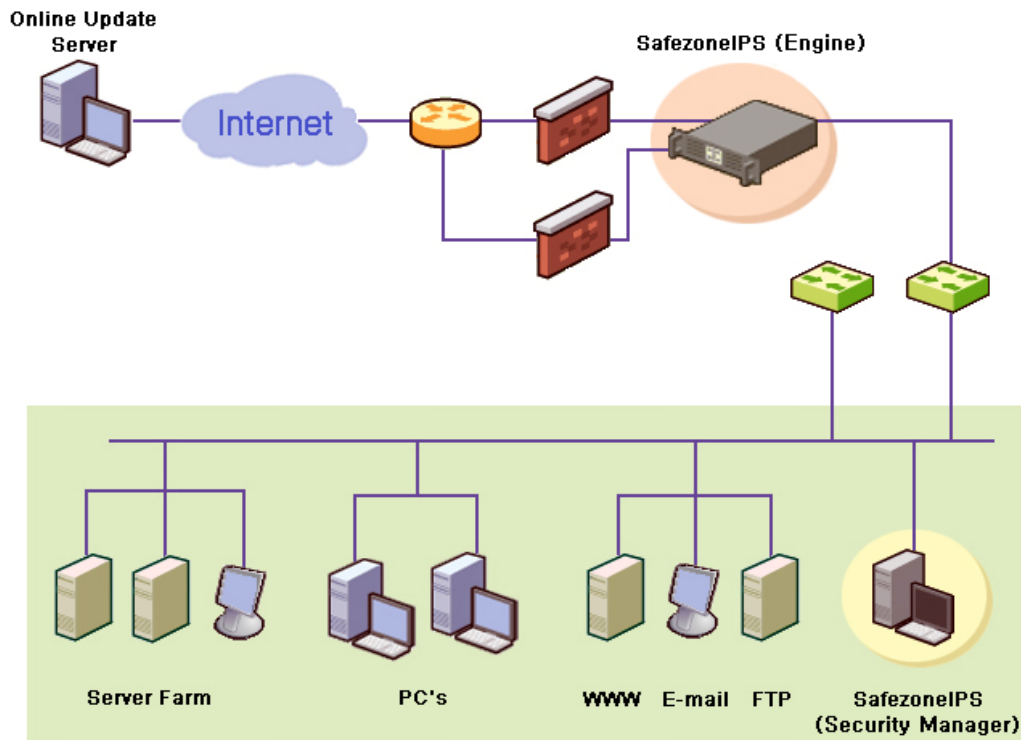
In cases where components of TOE interact remotely through internal communication channels, the nodes of the other side are identified and authenticated to ensure safe channels between TSFs.

2.2 TOE Network Environment

The primary purpose of SafezoneIPS function is an identification of network attack and an active reaction to it.



[Figure 2-1] SafezoneIPS(SZ-4000) network configuration



[Figure 2-2] SafezoneIPS(SZ-4000) network configuration (Dual configuration)

All network packets that flow through the SafezoneIPS engine are protected by the predefined TOE security policy. Equipped with a dedicated packet processor for processing mass traffic, SafezoneIPS can process in real time up to 2Gbps two-way traffic in Inline mode regardless of the packet size. An additional blocking policy makes concurrent process on the two separate networks possible with one equipment. ([Figure 2-1]) Especially, SafezoneIPS provides maximum 4 gigabit port, which results in the dual configuration. ([Figure 2-2])

2.3 TOE Scope and Boundary

SafezoneIPS, where the TOE is included, consists of a dedicated hardware system (SafezoneIPS engine) equipped with a dedicated packet processor and an administrator console. The [Table 2-1] below summarizes the hardware specifications of them:

Category		Performance & Specification	Remark	
SafezoneIPS Engine	Performance	Max 2 * 2Gbps Full Duplex	Throughput	
	Blocking Board (SR5000)	2 ports (for Giga) * 2	Service Port(In/Out)	Included in the TOE
	H/W	2.8Ghz * 2	CPU	
		4GB	MEM	
		73GB	HDD	
		Self OS(SZOS V1.0)	OS	
	2 Ports	Management Port (N/W I/F)		
Administrator Console	H/W Recommendation	2.4Ghz *1 or more	CPU	
		1GB or more	MEM	
		72GB * 2 or more	HDD	
		Version of or later than MS Windows 2000	OS	
		2 Ports or more	N/W Interface	
OS	Version of or later than MS SQL Server 2000	Data Management		

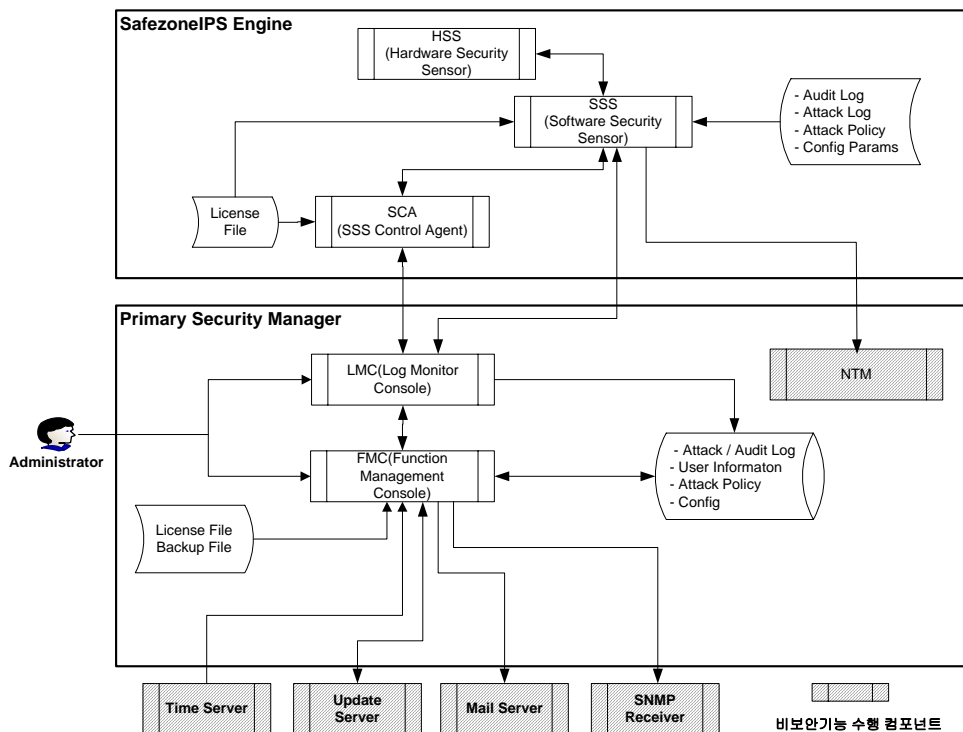
[Table 2-1] SafezoneIPS performance and hardware specification



The SafezoneIPS constituents that are excluded from the target of evaluation are listed in the following table.

Category		Excluded item	Description
Engine	OS	SZOS	OS of the dedicated hardware system of SafezoneIPS
	Hardware and other parts	H/W System	Dedicated equipment with SR5000 board and engine
Administrator Console	OS	MS Windows	OS of the computer with an administrator console installed
	Hardware and other parts	H/W System	A computer with an administrator console installed
		MS SQL Server	Database of the log and associated information
Others		Update Server	An external system for the delivery of updated security violation list
		Mail Server	A system for mail transfer
		SNMP Receiver	An external system for managing SNMP receipt
		Time Server	Public Timer Server, which is an external system, for time synchronization

2.3.1 Physical Scope and Boundary




[Figure 2-3] TOE architectural diagram

The engine is a dedicated hardware system of SafezoneIPS that comprises three components: Hardware Security Sensor (HSS), a board-type component with a PCI interface which identifies and reacts to an attack by collecting network packet; Software Security Sensor (SSS), which is a software application to check network packet through the second filtering; and Software Security Sensor Control Agent (SCA), which controls the operations of the SSS at the request of PSM, the administrator console, executing the commands of start-up, stop, and status check of SSS.

Primary Security Manager (PSM) is the administrator console which is a MS Windows-based GUI application for the remote control of SSS via SCA and the management of all relevant data. It consists of Log Monitor Console (LMC) for displaying intrusion logs received from engine, interface, and SSS and Function Management Console (FMC) for managing configuration and security policy and providing utility.

The shaded parts in the [Figure 2-4] above are excluded from the target of

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

evaluation, since they are constituents of hardware or additional system.

2.3.2 Logical Scope and Boundary

Security function of the TOE is the target of evaluation, including the security requirements of the Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005, KISA) and additional blocking functions. The following are the security functions of the 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. Security Audit also provides audit data protection function. In case the capacity of the memory is full, this function notifies the manager to prevent any loss of audit data that may occur due to lack of memory.

- 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

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. 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.

In addition, in cases where components of TOE interact remotely through internal communication channels, one identifies and authenticates the node of the other side to ensure trusted path and channel between TSFs. The communication between the administrator console and the engine is encrypted using SEED and its integrity is verified through SHA-1 to prevent any modification or exposure of the data.

- Security Management

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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. Security Management function provides the rules for detection/prevention SafezoneIPS performs and the managerial actions retrieving and modifying information related to the status and configuration of SafezoneIPS.

- TSF Protection

TSF Protection provides a regular check function to assure that the security assumptions related to the underlying abstract machine are properly operating. It performs checking when initially started, periodically during normal operation, and upon request of an authorized user to decide whether the main components running on the TOE system are normally operating in order. It also preserves a secure state when failure occurred and ensures safe operation of the TOE by periodically monitoring H/W failures such as CPU and memory, S/W failures such as OS errors, and buffer overflow failures caused by attacks.

- Resource Utilization


This function ensures safe operation of the TOE by periodically monitoring H/W failures such as CPU and memory, S/W failures such as OS errors, and buffer overflow failures caused by attacks.

- 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. The session locking is performed on the administrator console, which is the entry point of the interaction between the TOE function and the administrator.

- 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 administrator console and engine retrieve the secret keys (16byte SEED encryption key) distributed respectively and create authentication keys for the authentication

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

data to be used. Then they authenticate the right to open channel to the other node using the authentication key.

Note that Network Traffic Monitoring (NTM), which is a function of the TOE to monitor network traffic, is excluded from the scope of evaluation.

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
Assumption	A.Physical Security	
	A.Security Maintenance	
	A.Trusted Administrator	
	A.Hardened OS	
	A.Single Connection Point	
	A.Secure TOE external server	Added to ST
	A.TIME	Added to ST

[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. 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 two without passing through the TOE.

- A.Secure TOE External Server

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

- A.TIME

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

3.2 Threats

Threats are categorized into threats to the TOE and threats about the TOE operational environment, which are labeled as below:

Category	Item
Threat to the TOE (Threat)	T.Masquerade
	T.Failure
	T.Audit Failure
	T.Inbound Illegal Information
	T.Unauthorized Service Access
	T.Anomaly Packet Transfer
	T.New Vulnerability Attack
	T.DoS Attack
	T.Replay Attack
	T.Bypassing
	T.Spoofing IP Address
	T.Unauthorized TSF Data Modification
Threat to the TOE operational environment (Threat about 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. It is assumed that threat agent possesses a low level of expertise, resources and motivation and its attack potential for an exploitable vulnerability is low.

- T.Masquerade

A threat agent may masquerade as an authenticated administrator and therefore can obtain access to the TOE.

- T.Failure

Due to a failure or an attack, the TOE, while in operation, may not be able to provide proper services to users.

- T.Audit Failure



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

- T.Inbound Illegal Information

A computer in the internal network may be tampered or attacked by incoming a malicious packet from an external network containing unauthorized information.

- T.Unauthorized Service Access

A threat agent may gain access to a service unauthorized to internal network hosts, and disturb the proper offering of its service.

- T.Anomaly Packet Transfer

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

- T.New Vulnerability Attack

A threat agent may attack by exploiting a new vulnerability of a computer system in the internal network of the TOE or the TOE operational environment.

- T.DoS Attack

A threat agent may exhaust service resources of a computer in the internal network in the TOE operational environment and disturb authorized users' use of services.

- T.Replay Attack

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

- T.Bypassing

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

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.

	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

- 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 the 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	O.Availability	
	O.Audit	
	O.Administration	
	O.Abnormal Packet Screening	
	O.DoS Attack Blocking	
	O.Identification	
	O.Authentication	
	O.Information Flow control	
	O.TSF Data Protection	
Security 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.Secure TOE External Server	Added to ST
	OE.TIME	Added to ST

[Table 4-1] Identification of TOE security objectives

4.1 Security Objectives for the TOE

The following are the security objectives that must be directly managed by the TOE:

- O.Availability

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

- O.Audit



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

- O.Administration

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

- O.Abnormal Packet Screening

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

Application Notes : An abnormal packet is a packet that is not TCP/IP packet defined by an Internet standard protocol such as RFC 791 (internet protocol), RFC 792 (internet control message protocol), or RFC 793 (transfer control protocol), a packet with IP spoofing, broadcasting packet, or looping packet.

- O.DoS Attack Blocking

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

- O.Identification

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

- O.Authentication

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

Application Note : When a threat agent repeatedly tries authentication using the administrator's identity, there is a chance the agent may obtain authentication data. The TOE must implement an adequate authentication mechanism to defend these replay attacks.


- O.Information Flow Control

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

Application Note : This security objective implements the deny-all policy and the allow-all policy executed by TSF. Deny-all policy means screening all packets except for the ones specified to be allowed, and allow-all policy means allowing all packets except for the ones specified to be denied.

- O.TSF Data Protection

The TOE must protect stored TSF data from unauthorized disclosure, modification, or

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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.Secure TOE External Server

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

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

- OE.TIME

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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	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
FAU (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
FDP (User data protection)	FDP_IFC.1(1) Subset information flow control(1)
	FDP_IFC.1(2) Subset information flow control(2)
	FDP_IFF.1 Simple security attributes
FIA (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 Timing of authentication
	FIA_UAU.7 Protected authentication feedback
	FIA_UID.2(1) User identification before any action(1)
	FIA_UID.2(2) User identification before any action(2)
FMT (Security management)	FMT_MOF.1 Management of security functions behavior
	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 (Protection of the TSF)	FPT_AMT.1 Abstract machine testing
	FPT_FLS.1 Failure with preservation of secure state
	FPT_RVM.1 Non-bypassability of the TSP
	FPT_SEP.1 TSF domain separation
	FPT_STM.1 Reliable time stamps
	FPT_TST.1 TSF testing
FRU (Resource utilization)	FRU_FLT.1 Degraded fault tolerance
	FRU_RSA.1 Maximum quotas
FTA (TOE access)	FTA_SSL.1 TSF-initiated session locking
	FTA_SSL.3 TSF-initiated termination
FTP (Trusted path/channels)	FTP_ITC.1 Inter-TSF trusted channel

[Table 5-1] Security functional requirements

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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 [the action to alert the authorized administrator] 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 shutdown of the audit functions;
- b) All auditable events for the minimum level of audit; and

Component	Auditable event	Additional audit record
FDP_IFF.1	All decisions on requests for information flow	Identification information of subject and object
FIA_UAU.1	Unsuccessful use of the authentication mechanism	User identity provided to the TOE
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	User identity provided to the TOE
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
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
FPT_TST.1	Integrity errors, The action taken when an integrity error is identified and its result	Target and result of integrity monitoring

Component	Auditable event	Additional audit record
FTA_SSL.1	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

[Table 5–2 Auditable events]

c) [no additional rules]

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

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the Protection Profile (PP) / Security Target (ST), [audit object, audit content]

Dependencies: FPT_STM.1 Reliable time stamps

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 Timing of identification

5.1.1.4 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

violation of the TSP.

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 searches, sorting, ordering of audit data based on [date and time, audit object, audit subject, audit content, audit type, and audit code].

Dependencies: FAU_SAR.1 Audit review

5.1.1.7 FAU_SEL.1 Selective audit

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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) Object identity, subject identity, event type

b) [audit code]

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


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

Hierarchical to: No other components.

FAU_STG.3.1 The TSF shall take [action to alert the authorized administrator in case of possible audit storage failure] if the audit trail exceeds [80% capacity(pre-defined limit)].

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.1.10 FAU_STG.4 Prevention of audit data loss

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the authorized user with special rights and [alert the authorized administrator] if the audit trail is full.

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 the [policy to reject all] 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: traffic sent through the TOE from one subject to another;
- c) operation: pass information when allowing rules exist].

Dependencies: FDP_IFF.1 Simple security attributes

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 [policy to allow all] [list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

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

Dependencies: FDP_IFF.1 Simple security attributes

5.1.2.3 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.


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

- a) subjects: unauthenticated external IT entities that send/receive information;
- b) information: traffic sent through the TOE from one subject to another
- c) security attributes: subject identifier(MAC address, IP information, and port information), object identifier(MAC address, IP information, and port information).

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [the network packet consistent with the source MAC address, objective MAC address, source IP address, objective IP address, source port number, objective port number, total IP packet length, and the protocol' s configured value is to be blocked, otherwise the traffic 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].

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [The TOE shall block a request for network access when:

- a) the information from external IT entities has internal subject IP addresses
- b) the information from internal IT entities has external subject IP addresses
- c) the information from external IT entities has broadcasting subject IP addresses
- d) the information from external IT entities has looping subject IP addresses
- e) 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

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 [three] 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 prevention of the user authentication, the termination of administrator console, and the generation of audit log until an action is taken by the authorized administrator].

Dependencies: FIA_UAU.1 Timing of authentication

	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

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) IT identifier

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 name, user level, cell phone number, e-mail address


Dependencies: No dependencies

5.1.3.4 FIA_UAU.1 Timing of 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)] to be performed **by the administrator** before the **administrator** is authenticated.

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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

administrator.

Dependencies: FIA_UID.1 Timing of 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, not the original character, 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 Timing of authentication

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

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

5.1.4.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behavior of, disable, enable, modify the behavior of the functions [management of user information, management of configuration information, management of security violation events, configuration of new policy online update, reports on audit results, prevention of audit data loss, configuration of time synchrony functions] to [the authorized administrator].

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

5.1.4.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.


FMT_MSA.1.1 The TSF shall enforce the [blocking policies] to restrict the ability to change default, query, modify, delete, [create] the security attributes [security function, security violation events list] to [the authorized administrator].

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

5.1.4.3 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [blocking policies] to provide restrictive default values for security attributes that are used to

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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

5.1.4.4 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to change_default, query, modify, [create] the [current time, audit trail, identification and authentication data, security violation events, configuration data, automatic backup information, automatic integrity check information, online update information, communication-related information] to [the authorized administrator].


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

5.1.4.5 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, the number of logged-in super administrators] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [the generation of audit record, the action to alert the authorized administrator].

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

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

5.1.4.6 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: [management of security attributes, management of TSF data, management of security function].

Dependencies: No dependencies

5.1.4.7 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [an authorized administrator].

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


Dependencies: FIA_UID.1 Timing of 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, at the request of an authorized user to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

Dependencies: No dependencies

5.1.5.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [detection and blocking failures due to hardware functional failures, audit data storage failures due to software failures].

Dependencies: ADV_SPM.1 Informal TOE security policy model

5.1.5.3 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

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

Dependencies: No dependencies


5.1.5.4 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

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

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

Dependencies: No dependencies

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

5.1.5.5 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

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

Dependencies: No dependencies

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.

5.1.5.6 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

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

Hierarchical to: No other components.

FRU_FLT.1.1 The TSF shall ensure the operation of [the administrator' s management using the console or security management screen] when the following failures occur: [failure of network interface, error of major process].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

Application notes: The main purpose of this function is to ensure that users can use network service even in case of failure. Thus, the developer should implement the TOE as it can take action to a failure so minimum services can be provided for the users, and specify it in the ST.

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-authentication].

Dependencies: FIA_UAU.1 Timing of 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 a [IT entity inactivity period: 10 minutes].

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].

	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

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	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Analysis	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

[Table 5-3] 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.

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

- Content and presentation of evidence elements
 - ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.
 - ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.
 - ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.
 - ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.
- Evaluator action elements
 - ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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 CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
 - ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.
 - ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.
 - ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items.
 - ACM_CAP.4.7C The CM system shall uniquely identify all configuration items.
 - ACM_CAP.4.8C The CM plan shall describe how the CM system is used.
 - ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.



- ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
- ACM_CAP.4.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.
- ACM_CAP.4.12C The CM system shall support the generation of the TOE.
- ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- Evaluator action elements
- ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.


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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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

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.

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

- ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.
- ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
- ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
- ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.
- Evaluator action elements
 - ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
 - ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.


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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

between all adjacent pairs of TSF representations that are provided.

- Content and presentation of evidence elements
 - ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
- Evaluator action elements
 - ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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

- Dependencies:
 - ADV_FSP.1 Informal functional specification
- Developer action elements
 - AGD_USR.1.1D The developer shall provide user guidance.
- Content and presentation of evidence elements
 - AGD_USR.1.1C The user guidance shall describe the functions and interfaces

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

available to the non-administrative users of the TOE.

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

5.2.5 Life Cycle Support

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
 - 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 well-defined.

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

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

- Evaluator action elements

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

- 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.2 Security enforcing high-level design
 - ADV_LLD.1 Descriptive low-level design
- 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

- 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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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 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 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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target


- 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

The following is the security requirement for the IT environment:

5.3.1 Protection of the TSF

5.3.1.1 FPT_STM.1 Reliable time stamps


 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	----------------------------------

Hierarchical to: No other components.

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

Dependencies: No dependencies

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.

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

6. TOE Summary Specification

This chapter provides a description of the security functions and assurance measures of the SafezoneIPS. It shows that SafezoneIPS meets the security functional requirements and assurance requirements for the network intrusion 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 (SFAU)
- User Data Protection (SFDP)
- Identification and Authentication (SFIA)
- Security Management (SFMT)
- TSF Protection(SFPT)
- TOE Access (SFTA)

The strength of function (SOF) targeted by the TOE is SOF–medium, since the threat agent is assumed to possess a moderate attack potential.

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.


6.1.1 Security Audit (SFAU)

The 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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0	Security Target
	Security Target_20051205_V1.00.02	


functions of the system and intrusion detection/prevention logs. Audit log on the event is generated by the audit log generation module of SSS(Software Security Sensor) and PSM(Primary Security Manager), collected by the audit log module of PSM, and finally managed by PSM. Intrusion detection/prevention log is about the audit data detected and prevented by HSS(Hardware Security Sensor) and SSS, which is collected by the audit log module of PSM and managed by PSM.

Audit data generated by each main TOE component shall include the following items:

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
Console type	Classification of the types of console that generated an audit log; either an administrator console(PSM) or web console(SSM)
Audit code	A code to identify the event
IP	IP address of the system that generated the audit log

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 collected by the audit log module of PSM and managed by PSM. They will be reviewed through GUI interface of PSM, but only on the basis of the authority level defined by the TOE system.

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target


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, SSS/SCA 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.

- 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) 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 PSM 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:

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

- 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

6.1.1.3 SFR Mapping

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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

6.1.2 User Data Protection (SFDP)

In order to protect the target network, the TOE collects information for the detection/prevention of an attack, takes a counter action to potential security violations, and stores the results of analysis so the administrator can check them later.

- Detection/prevention event information collection and analysis (SFDP_CHK)
- Counter attack activity (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.

- This function uses the following mechanisms:
 - Static rule based attack analysis: Static policy basis (SFDP_CHK_STAT)
 - Hard-wired based attack analysis: Packet integrity policy basis (SFDP_CHK_INT)
 - DoS/Scan traffic attack analysis: Dynamic attack policy analysis (SFDP_CHK_DYN)
 - Protocol header based access control: Detailed blocking policy basis (SFDP_CHK_BLK)
 - Abnormal traffic attack analysis: Abnormal traffic RateLimit policy basis (SFDP_CHK_ABN)
 - Detection/prevention exception: Detection/prevention exception policy basis (SFDP_CHK_EXP)

1) Classification of attack types

- Static attack (Signature-based attack)

This is an attack with a specific pattern. All packets coming from the networks are identified by matching their pattern on the basis of security policies.

- Network protocol integrity attack

This is an attack of the packet which is not the standard TCP/IP protocol or cannot be generated logically. This type of attack is to be detected and



processed from another attack analysis mechanism before **other types**.

- DoS / Scan type dynamic attack

This is an attack which is composed of a set of multiple packets and remains as it is for a specific period. It is identified by analyzing a packet stream that lasts for a certain period of time.

- Protocol header based access control

This is an attack with specific conditions by which a network administrator can identify it as an attack. It can be prevented at a certain time for a certain period through a detailed definition rule of the protocol header information. If a packet that matches the specific condition occurs, it is interpreted as an attack.

- Unspecific patterned abnormal traffic attack

This is an attack that shuts down the network service by causing traffic overload on the network with an unspecific pattern, which is distinguished from the flooding DoS attack or scan type attack. It is identified by analyzing a packet stream that lasts for a certain period of time. The type of packet stream change is defined by the administrator.

2) Analysis subject information collection


The traffic of both directions entering the HSS Ethernet controller should be analyzed in a packet unit. All collected network traffic and data are used for the attack analysis. They are also used as a statistical data of abnormal protocol packet, network DoS attack attempt, abnormal activities concerning the time and packet volume can be used to identify an attack. The collected time information, identify information of the subject and object, security attributes, data type, and other information are added to the data for an attack analysis.

- Subject: Source IP/port information
- Object: Destination 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

Detection mechanism identifies attack using the packet information input by packet collection module.

- Static rule based attack analysis: Static policy basis (SFDP_CHK_STAT)

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

- Static rule based attack analysis detects an attack based on the security policy defined by the security management function that manages security violation events list.
- Static rule based attack analysis detects an attack by comparing the characteristics of collected packet with the static rule predefined by HSS hardware components.
- Collected packet is divided into header and content, which go through the rule based test under the header test module and content test module respectively. The result of the test by each module is used to identify an attack.
- Static policy is downloaded from PSM/SSS, divided into header rule and content rule, and loaded to each module.
- If the result of packet analysis proves an attack, the counter attack activity is carried out as defined.
- Regarding the modification of attributes of static policy, the administrator should be able to define the counter attack policy, activation of detection function, and the information of security violation events list, such as IP address/port/attack direction.
- An attack with a specific pattern can be analyzed on the basis of static rule when a fragmented packet is reassembled. A fragmented packet is transmitted from HSS to SSS, then SSS reassembles it and performs an attack analysis based on the static rule.
 - Hard-wired based attack analysis: Packet integrity policy basis (SFDP_CHK_INT)
 - Packet integrity policy analyzes the attack of the packet which is not the standard TCP/IP protocol or cannot be generated logically.
 - DoS / Scan traffic attack analysis: Dynamic attack policy basis (SFDP_CHK_DYN)
 - Dynamic attack analysis identifies an attack by analyzing a packet stream that lasts for a certain period of time.
 - After analyzing the packet stream based on the data sent from the packet collection module of HSS, it carries out the counter attack policy when the attack is at the predefined dynamic attack limit.
 - Protocol header based access control: Detailed blocking policy basis (SFDP_CHK_BLK)
 - This concerns the attack with specific conditions by which a network administrator can identify it as an attack. The administrator applies a detailed



definition rule of the protocol header information through which an attack is prevented at a certain time for a certain period.

– Blocking policy carries out counter attack activity when a predefined blocking rule is satisfied.

- Abnormal traffic attack analysis: Abnormal traffic RateLimit policy basis (SFDP_CHK_ABN)

– The RateLimit of TCP/UDP/ICMP dynamic attack should be reinforced for an analysis of various types of packets possessing no specific pattern in content.

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

Even if an attack is identified by the criteria regarding static attack, dynamic attack, detailed blocking policy, and abnormal traffic attack, the traffic generated legally from the host or network with predefined protocol, source IP, destination IP, source port, and destination port should be processed before all the other attack filtering. exempted from the attack filtering.

6.1.2.2 Counter attack activity (SFDP_ACT)

If a collected packet is detected as an attack, the TOE automatically counters the attack according to the counter attack policy defined by the administrator.

The counter attack policy is configured for each attack type through the security violation management function and applied after being updated in SSS.

1) Prevention and passage of the network packet (Packet Drop, IP Block)

Installed in-line on the network, it drops only those packets identified as the attack in order to prevent the suspicious packets from coming in the network and to prevent connection with the harmful session. If the packet drop is not configured in the counter attack policy, even the attack packets can pass through. Packet drop is divided into two types: one is to prevent only the identified attack packets, and the other is to prevent all packets generated from the attack source for a certain period, which is called “ IP Block.”

2) Real-time warning (Log transfer, e-mail transfer, SMS transfer)

When an attack packet is detected and prevented, the detection/prevention log information is sent to PSM in real time. The method of warning includes sending detection/prevention log to PSM and sending e-mail or SMS to the

authorized administrator.


3) Integration with other system: Syslog and SNMP Trap transfer
 Detection/prevention log is transmitted to Syslog and SNMP Trap.

4) Additional network information

Tools using Whois, Traceroute, and Ping information of attack IP or attack target IP in the detection/prevention log shall be provided so the administrator can trace back the attack path.

6.1.2.3 SFR Mapping

TSF	SFR
Detection/prevention event information collection and analysis (SFDP_CHK)	FDP_IFC.1 Subset information flow control FDP_IFF.1 Simple security attributes FIA_ATD.1(1) User attribute definition (1) FIA_UID.2(1) User identification before any action (1)
Counter attack activity (SFDP_ACT)	FAU_ARP.1 Security alarms FDP_IFF.1 Simple security attributes FIA_ATD.1(1) User attribute definition (1) FIA_UID.2(1) User identification before any action (1)

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

6.1.3 Identification and Authentication (SFIA)

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

- 1) Identification and authentication of GUI user of PSM/SSM
- 2) Mutual identification and authentication between TOE components during remote connection through the communication channel (PSM ↔ SCA, PSM ↔ SSS)

Identification and authentication of the TOE user perform the following functions:

- User identification and authentication (SFIA_LOGON)
- Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)

6.1.3.1 User identification and authentication (SFIA_LOGON)

User identification and authentication (SFIA_LOGON) is required as a part of the SOF level targeted by the TOE. (The SOF targeted by the TOE is SOF–medium, since the threat agent is assumed to possess a moderate attack potential. “ FIA_UAU.1 Timing of authentication” , which uses general password mechanism, is required in accordance with the SOF claim.)

PSM 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.

The authorized administrator confirmed through user identification and authentication can access the TSF data and can generate, delete, and modify the configuration data for the operation. Confirmed user identification and authentication ensure the authority to control and modify the security attributes for operating TSF. The authority to execute TSF and access the TSF data is determined by each user group.

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 PSM:

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, SSS/SCA 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.


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 (default value: 3), the PSM 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.

Mutual identification and authentication for remote connection through the communication channel (SFIA_UID) is required as a part of the SOF level targeted by the TOE. (The SOF targeted by the TOE is SOF-medium, since the threat agent is assumed to possess a moderate attack potential. " FIA_UAU.1 Timing of authentication" and " FIA_UID.2(1) User identification before any

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

action” , which uses general IT identification mechanism, are required in accordance with the SOF claim.)

1) Mutual identification and authentication between PSM and SCA or between PSM and SSS

- Identification: When PSM requests opening of the communication channel with SCA/SSS, each component identifies the node of other side.
- Authentication: Once identification is completed, PSM and SCA/SSS secure distributed secret keys (16byte SEED encryption key) and create the authentication key as the encryption key of the authentication data. The authentication key is then used to authenticate the authority to open the channel.

2) Mutual identification and authentication between PSM and online update server

The interface between PSM and online update server also identifies and authenticates each other before connection, using TCP/IP socket interface.


3) Prevention of reusing authentication data for remote connection through the communication channel

The authentication key should be periodically changed to prevent its drain and reuse.

Data is encrypted using SEED and its integrity is verified through SHA-1 to prevent any modification or exposure of the data.

6.1.3.3 SFR Mapping

TSF	SFR
User identification and authentication (SFIA_LOGON)	FIA_AFL.1 Authentication failure handling FIA_UAU.1 Timing of authentication FIA_UAU.7 Protected authentication feedback FIA_UID.2 User identification before any action
Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)	FIA_UAU.1 Timing of authentication FIA_UAU.7 Protected authentication feedback FTP_ITC.1 Inter-TSF trusted channel FIA_UID.2(1) User identification before any action (1)

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

6.1.4 Security Management (SFMT)

The security management function of the TOE system is provided through the PSM 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
- PSM configuration information management (Console management)
- SCA/SSS configuration information management (Engine management)
- Security violation events management
- Intrusion detection/prevention result report
- Prevention of audit data loss
- PSM/SSS time synchronization

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. (Ref. “ 6.1.4.3 SCA/SSS configuration management (SFMT_SSS)”)

3) Identification and authentication management

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

A. User information creation

- New user information can only be created by the top administrator.
- When storing the security attribute value, the password should be encrypted to protect it from exposure.

B. User information search and retrieval

- User information search and retrieval can be performed only by the top and mid-level administrator.
- Stored user information is read from the database and displayed through the GUI viewer. The password is displayed in a string of “ *” to protect it from



exposure.

C. User information deletion

- Like user information creation, its deletion also can only be performed by the top administrator.
- The top administrator can delete any user information except his/hers, but cannot delete the information of a user who is logged on currently.

D. User information modification

- Only the top administrator can modify the user information. However, the logon status and the final logon time cannot be modified and the user password is enforcedly modified at the initial start-up. The mid-level administrator and low-level administrator can only modify their own passwords.

6.1.4.2 PSM configuration information management (SFMT_PSM)

PSM configuration management function manages the information needed for PSM operation through the GUI interface.

1) PSM configuration information search and retrieval

- PSM configuration search and retrieval can be performed only by the top administrator and mid-level administrator.


2) PSM configuration information modification

- The retrieved configuration information can be modified by the top and mid-level administrators.
- Regarding the online update function, “ Last update time” and “ Last updated rule version” can only be retrieved and cannot be changed.
- The values changed by PSM should be reflected immediately for the operation of PSM. However, the reflection of “ Intrusion detection/prevention log encryption” should be possible only after the re-startup of PSM.
- The period of time synchronization of an administrator console and engine can be modified only by the top administrator. Time synchronization occurs at the initial startup and every period.

6.1.4.3 SCA/SSS configuration information management (SFMT_SSS)

SCA/SSS configuration management function manages the information related to SCA/SSS connection and operation.

1) SCA/SSS configuration information registration

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target


- SCA/SSS configuration information can be registered only by the top and mid-level administrators. The new information can be registered only by the top administrator.
 - The security attributes necessary for the connection, such as SSS name, SSS IP address/service port, SSS communication MAC address, SSS model name/number of ports should be input to generate a new record.
- 2) SCA/SSS configuration information search and retrieval
- Only the top and mid-level administrator can search and retrieve the SCA/SSS configuration information.
- 3) SCA/SSS configuration information modification
- Only the top and mid-level administrators can modify the SCA/SSS configuration information. However, SSS connection information can be modified only by the top administrator.
 - The SSS connection information cannot be changed even by the top administrator if the SSS is currently in communication with PSM.
 - Excepting the connection information, the SCA/SSS operation information can be modified and synchronized with the engine.
- 4) SCA/SSS configuration information deletion
- SCA/SSS configuration information can be deleted by the top and mid-level administrators. However, the authority to delete SCA/SSS information is granted only to the top administrator.
 - When there is an attempt to delete the information of SSS currently in communication with PSM, a warning message is displayed and the information is not deleted.

6.1.4.4 Security violation events management (SFMT_POL)

All attack information processed by the TOE can be managed through the GUI interface.

Attack information is classified according to the mechanism to detect the attack as the following:

- Static policy (SFMT_POL_STAT)
- Dynamic attack policy (SFMT_POL_DYN)
- Packet integrity policy (SFMT_POL_INT)
- Detailed blocking policy (SFMT_POL_BLK)
- Abnormal traffic RateLimit policy (SFMT_POL_ABN)

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

- Prevention exception policy (SFMT_POL_EXP)

When a security policy is modified, it is applied to the detection engine(SSS/HSS) so that the detection and counter action can be initiated in accordance with the changed information. The system-provided policy itself cannot be applied to SSS. 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. (However, there is no security violation events included in the dummy policy of the system-provided security policies for the detailed prevention, abnormal traffic RateLimit, prevention exception policies, unlike the static/dynamic attack policies.) Furthermore, the user-defined security policies derived from the system-provided security policies can be deleted and modified.

1) Static policy management (SFMT_POL_STAT)


: Defines and manages the detection and counter action policy to an attack with a specific pattern. The contents of the security violation events detection of the system-provided security policy may not be searched and retrieved. The contents of the security violation events detection derived from the system-provided security policy may not either. However, the contents of the security violation events of the user-defined security policy can be searched and retrieved. The function to activate or deactivate the detection of the security violation event is provided.

2) Dynamic attack policy management (SFMT_POL_DYN)

: Defines and manages the detection and counter action policy to an attack which is identified by analyzing a packet stream that lasts for a certain period of time. Dynamic attack must be detected and analyzed, so the function to activate or deactivate the detection is not provided.

3) Packet integrity policy management (SFMT_POL_INT)

: Defines and manages the detection and counter action policy to an attack of the packet which is not the standard TCP/IP protocol or cannot be generated logically. The function to activate or deactivate the detection is provided.

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

4) Detailed blocking policy management (SFMT_POL_BLK)

: Defines and manages the detailed blocking policy used to detect an attack with specific conditions by which the network administrator can identify it as an attack. The policy is defined so that the attack can be prevented at a certain time for a certain period through a detailed definition rule of the protocol header information. The function to activate or deactivate the detection is provided.

5) Abnormal traffic RateLimit policy management (SFMT_POL_ABN)

: Defines and manages the policy to detect an attack that shuts down the network service by causing network overload with an unspecific pattern, which is distinguished from the flooding DoS attack or scan type attack. Even for the user-defined security violation events, the attack code once assigned may not be modified. The function to activate or deactivate the detection is provided.

6) Prevention exception policy management (SFMT_POL_EXP)

: This policy defines the packets that will be exempted from the detection/prevention policy (i.e. that can be passed through without the network packet detection/prevention), except for the integrity policy. This management function concerns the information having the characteristics under the application of the exception rule. Even for the user-defined exception rule, however, the exception code once assigned may not be modified. The function to activate or deactivate the application of the exception rule is provided.

6.1.4.5 New policy online update (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 PSM and the online update server.

2) The function to compare the static policy of the security violation event list registered in PSM 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 PSM policy database and apply it to SSS. Then SSS/HSS can immediately perform detection based on the updated policy.

6.1.4.6 Intrusion detection/prevention result report (SFMT_RPT)

PSM 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.

There are two types of the report: one is “detailed report” that shows the intrusion detection/prevention results in a text-based list form; the other is “statistical report” that shows the statistical analysis of the results by a certain condition. The statistical report should include the following:


- Top 10 distribution of the intrusion detection/prevention result for each field
- Distribution of the intrusion detection/prevention result for each field against all data

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

All intrusion detection/prevention logs and audit logs generated in the TOE system are integrated, collected, managed, and protected by PSM(Primary Security Manager).

1) Criteria for deleting and modifying the stored data of intrusion detection/prevention log and audit log

- Only authorized administrators can delete the stored intrusion detection/prevention log and audit log records through the intrusion log backup manager and audit log backup manager of PSM.
- The intrusion detection/prevention log and audit log generated by the TOE system may not be modified. The PSM audit log search manager does not

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

provide any modification function except “ deletion.”

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

- 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.
- In case failure of log storage occurs due to insufficient storage space, the new intrusion detection/prevention logs and audit logs are neglected in order to prevent the audit data loss and the following actions are initiated.
 - Notify the administrator to perform backup
 - Terminate PSM

6.1.4.8 PSM / SSS 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.


PSM, SCA, and SSS 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. When it is impossible, the TOE system synchronizes time with the administrator console.

- 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

6.1.4.9 SFR Mapping

TSF	SFR
User information management (SFMT_USR)	FMT_MOF.1 Management of security functions behavior FMT_MSA.1 Management of security attributes FMT_MTD.1 Management of TSF data FIA_ATD.1 User attribute definition FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
PSM configuration information management (SFMT_PSM)	FMT_MOF.1 Management of security functions behavior 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
SCA/SSS configuration information management (SFMT_SSS)	FMT_MOF.1 Management of security functions behavior 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
Security violation events management (SFMT_POL)	FMT_MOF.1 Management of security functions behavior 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 FDP_IFC.1 Subset information flow control FDP_IFF.1 Simple security attributes FPT_RVM.1 Non-bypassability of the TSP FMT_SMF.1 Specification of management functions FRU_RSA.1 Maximum quotas FIA_ATD.1(1) User attribute definition (1) FTA_SSL.3 TSF-initiated termination FIA_UID.2(1) User identification before any action (1)
New policy online update (SFMT_POLUP)	FMT_MOF.1 Management of security functions behavior FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of management functions
Intrusion detection/prevention result report (SFMT_RPT)	FMT_MOF.1 Management of security functions behavior FMT_SMF.1 Specification of management functions
Prevention of the loss of the intrusion detection and audit data (SFMT_BKUP)	FMT_MOF.1 Management of security functions behavior 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_SMF.1 Specification of management functions
PSM / SSS time synchronization (SFMT_TIME)	FMT_MOF.1 Management of security functions behavior FPT_STM.1 Reliable timestamps FMT_SMF.1 Specification of management functions

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

6.1.5 TSF Protection (SFPT)

The TOE system ensures safe TSF operations.

[TSF protection functions]

- PSM / SSS Health Checking (SFPT_CHKSYS)
- TSF stored data integrity check (SFPT_CHKINT)
- TOE failure with preservation of secure state (SFPT_CHKTOE)

6.1.5.1 PSM / SSS Health Checking (SFPT_CHKSYS)

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

1) PSM checklist

- PSM processes
- Disk resource usage of the PSM system
- Memory usage of each PSM system process

2) SSS checklist

- SSS processes
- Memory, CPU, and disk usage of SSS

6.1.5.2 TSF stored data integrity check (SFPT_CHKINT)

TSF stored data integrity check (SFPT_CHKINT) is required as a part of the SOF level targeted by the TOE. (The SOF targeted by the TOE is SOF-medium, since the threat agent is assumed to possess a moderate attack potential. “FPT_TST.1 TSF testing”, which uses SHA-1 as a hash algorithm for integrity authentication, is required in accordance with the SOF claim.)

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 TOE failure with preservation of secure state (SFPT_CHKTOE)

This function checks if the main components of the TOE system are preserving secure state.

1) PSM checklist

- Connection status between PSM and SSS

2) SSS checklist

- SSS link connection status and HSS status such as H/W flaw

6.1.5.4 SFR Mapping

TSF	SFR
PSM / SSS Health Checking (SFPT_CHKSYS)	FPT_AMT.1 Abstract machine testing FPT_TST.1 TSF testing FPT_SEP.1 TSF domain separation FPT_FLS.1 Failure with preservation of secure state FRU_FLT.1 Degraded fault tolerance
TSF stored data integrity check (SFPT_CHKINT)	FPT_TST.1 TSF testing
TOE failure with preservation of secure state (SFPT_CHKTOE)	FPT_FLS.1 Failure with preservation of secure state FRU_FLT.1 Degraded fault tolerance

6.1.6 TOE access (SFTA)

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 PSM GUI 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 PSM, all visible attributes on PSM 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 PSM 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

- When there is no key entry on the GUI interface for a certain period of time after the logon to SSM, the connection with SSM interface is terminated.
- 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
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 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-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	–
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

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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	Testing
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, high-level 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) FIA_ATD.1(1) User attribute definition (1) FIA_ATD.1(2) User attribute definition (2) FIA_UID.2(1) User identification before any action (1) FIA_UID.2(2) User identification before any action (2)
Selection	FAU_GEN.1 Audit data generation FAU_SAR.3 Selectable audit review FAU_SEL.1 Selective audit FAU_STG.1 Protected audit trail storage FAU_STG.4 Prevention of audit data loss FMT_MOF.1 Management of security functions behavior 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

Refinement	FAU_GEN.1 Audit data generation FIA_ATD.1(1) User attribute definition (1) FIA_ATD.1(2) User attribute definition (2) FIA_UAU.1 Timing of authentication FIA_UAU.7 Protected authentication feedback FIA_UID.2(1) User identification before any action (1) FIA_UID.2(2) User identification before any action (2) 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 Action in case of possible audit data loss FAU_STG.4 Prevention of audit data loss FDP_IFC.1(1) Subset information flow control (1) FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1 Simple security attributes FIA_AFL.1 Authentication failure handling FIA_ATD.1(2) User attribute definition (2) FIA_UAU.1 Timing of authentication FIA_UAU.7 Protected authentication feedback FMT_MOF.1 Management of security functions behavior FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FMT_MTD.1 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 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	Remark
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.Secure TOE external server	Added to ST	
	A.TIME	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	
	TE.Poor administration	Intrusion prevention system PP	
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	




O.Information flow control	Intrusion prevention system PP	Security objectives for the environment
O.TSF data protection	Intrusion prevention system PP	
OE.Physical security	Intrusion prevention system PP	
OE.Security maintenance	Intrusion prevention system PP	
OE.Trusted administrator	Intrusion prevention system PP	
OE.Secure administration	Intrusion prevention system PP	
OE.Hardened OS	Intrusion prevention system PP	
OE.Single connection point	Intrusion prevention system PP	
OE.Vulnerability list update	Intrusion prevention system PP	
OE.Secure TOE external server	Added to ST	
OE.TIME	Added to ST	


Category	Item	Reference	Remark
SFR	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 Action in case of possible audit data loss	Intrusion Prevention System PP	
	FAU_STG.4 Prevention of audit data loss	Intrusion Prevention System PP	
SFR	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	
SFR	FDP_IFF.1 Simple security attributes	Intrusion Prevention System PP	Identification and authentication
	FIA_AFL.1 Authentication failure handling	Intrusion Prevention System PP	
	FIA_ATD.1(1) User attribute definition(1)	Intrusion Prevention System PP	
	FIA_ATD.1(2) User attribute definition(2)	Intrusion Prevention System PP	
	FIA_UAU.1 Timing of 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	
SFR	FMT_MOF.1 Management of security functions behavior	Intrusion Prevention System PP	Security management
	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	Protection of the TSF
FPT_FLS.1 Failure with preservation of secure state	Intrusion Prevention System PP	
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	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

	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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-level design	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 Guidance document
	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	Testing


	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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: A.Secure TOE external server, A.TIME, OE.Secure TOE external server, and OE.TIME.

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type 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	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.Secure TOE external server	OE.TIME	
A.Physical security										●									
A.Security maintenance											●								
A.Trusted administrator												●							
A.Hardened OS															●				
A.Single connection point																●			
A.Secure TOE external server																		●	
A.TIME																			●
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	●	●		●			●												
TE.Poor Administration				●								●	●						
TE.Distribution and Installation												●	●						
P.Audit		●					●												
P.Secure Administration				●								●	●						

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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	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) O.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) O.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) O.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) O.Identification

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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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 vulnerability attack.

8) OE.Secure TOE external server

The security objective for this environment is to ensure that the external server interacting with the TOE is secure. Therefore, the security objective for this environment is necessary to assist the assumption of A.Secure TOE external server.

9) OE.TIME

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.TIME.


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								
	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
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		●							
FDP_IFC.1(1) Subset information flow control(1)									●
FDP_IFC.1(2) Subset information flow control(2)									●
FDP_IFF.1 Simple security attributes					●				●
FIA_AFL.1 Authentication failure handling							●	●	
FIA_ATD.1(1) User attribute definition(1)		●			●	●	●		●
FIA_ATD.1(2) User attribute definition(2)		●					●		
FIA_UAU.1 Timing of authentication			●	●				●	
FIA_UAU.7 Protected authentication feedback								●	
FIA_UID.2(1) User identification before any action(1)		●			●	●	●		●
FIA_UID.2(2) User identification before any action(2)		●	●	●			●		
FMT_MOF.1 Management of security functions behavior	●		●						
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_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	●									●
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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	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: O.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: O. 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: O. 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: O. 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: O. 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: O. 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: O. 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: O. Audit.



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

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

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: O. 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: O.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: O.Information flow control.

13) FDP_IFF.1 Simple security attributes

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

14) FIA_AFL.1 Authentication failure handling

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

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


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

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

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

17) FIA_UAU.1 Timing of authentication

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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

18) FIA_UAU.7 Protected authentication feedback

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

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

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

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

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

21) FMT_MOF.1 Management of security functions behavior

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: O.Availability and O.Administration.

22) FMT_MSA.1 Management of security attributes

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

23) FMT_MSA.3 Static attribute initialization

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

24) 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: O.Administration and O.TSF data protection.

25) 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: O.Availability and O.Administration.

26) FMT_SMF.1 Specification of Management Functions

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

27) FMT_SMR.1 Security roles

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

28) FPT_AMT.1 Abstract machine testing

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

29) FPT_FLS.1 Failure with preservation of secure state

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

30) 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: O. Information flow control.

31) FPT_SEP.1 TSF domain separation


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

32) 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: O.Audit.

33) 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:

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type Security Target
---	--	---

O.Availability, O.TSF data protection.

34) FRU_FLT.1 Degraded fault tolerance

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: O.Availability, O.Information flow control.

35) 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: O.DoS attack blocking.

36) 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: O.TSF data protection.

37) 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: O. DoS attack blocking.

38) FTP_ITC.1 Inter–TSF trusted channel

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

 LG N-Sys	Document Identification No. SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Document Type 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, described in 6.2, 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 Dependency 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	FPT_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	FDP_IFF.1	12
12	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	11 20
13	FIA_AFL.1	FIA_UAU.1	15
14	FIA_ATD.1	-	-
15	FIA_UAU.1	FIA_UID.1	17
16	FIA_UAU.7	FIA_UAU.1	15
17	FIA_UID.2	-	-
18	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	23 24
19	FMT_MSA.1	[FDP_ACC.1 or 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_RVM.1	-	-
28	FPT_SEP.1	-	-
29	FPT_STM.1	-	-
30	FPT_TST.1	FPT_AMT.1	25
31	FRU_FLT.1	FPT_FLS.1	26
32	FRU_RSA.1	-	-
33	FTA_SSL.1	FIA_UAU.1	15
34	FTA_SSL.3	-	-
35	FTP_ITC.1	-	-

[Table 8-3] Functional components dependencies

- FAU_GEN.2, FIA_UAU.1, and 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) Counter action activity (SFDP_ACT)
	FAU_GEN.1 Audit data generation	Audit data generation (SFAU_GEN)
	FAU_GEN.2 User identity association	Audit data generation (SFAU_GEN)
	FAU_SAA.1 Potential violation analysis	Audit data generation (SFAU_GEN)
	FAU_SAR.1 Audit review	Audit data search and retrieval (SFAU_SAR)
	FAU_SAR.3 Selectable audit review	Audit data search and retrieval (SFAU_SAR)
	FAU_SEL.1 Selective audit	Audit data search and retrieval (SFAU_SAR)
	FAU_STG.1 Protected audit trail storage	Prevention of the loss of intrusion detection/prevention and audit data (SFMT_BKUP)
	FAU_STG.3 Action 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) Security violation events management (SFMT_POL)
	FDP_IFC.1(2) Subset information flow control (2)	Detection/prevention event information collection and analysis (SFDP_CHK) Security violation events management (SFMT_POL)
	FDP_IFF.1 Simple security attributes	Detection/prevention event information collection and analysis (SFDP_CHK) Counter action activity (SFDP_ACT) Security violation events management (SFMT_POL)
Identification and authentication	FIA_AFL.1 Authentication failure handling	User identification and authentication (SFIA_LOGON)
	FIA_ATD.1(1) User attribute definition (1)	Security violation events management (SFMT_POL) Detection/prevention event information collection and analysis (SFDP_CHK) Counter action activity (SFDP_ACT)
	FIA_ATD.1(2) User attribute definition (2)	User information management (SFMT_USR)




	FIA_UAU.1 Timing of 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) Mutual identification and authentication for remote connection through the communication channel (SFIA_UID)
	FIA_UID.2(1) User identification before any action (1)	User identification and authentication (SFIA_LOGON)
	FIA_UID.2(2) User identification before any action (2)	User identification and authentication (SFIA_LOGON)

Category	SFR	TSF
Security management	FMT_MOF.1 Management of security functions behavior	User information management (SFMT_USR) PSM configuration information management (SFMT_PSM) SCA/SSS configuration information management (SFMT_SSS) Security violation events management (SFMT_POL) New policy online update (SFMT_POLUP) Intrusion detection/prevention result report (SFMT_RPT) Prevention of the loss of intrusion detection/prevention and audit data (SFMT_BKUP) PSM / SSS time synchronization (SFMT_TIME)
	FMT_MSA.1 Management of security attributes	User information management (SFMT_USR) PSM configuration information management (SFMT_PSM) SCA/SSS configuration information management (SFMT_SSS) Security violation events management (SFMT_POL)
	FMT_MSA.3 Static attribute initialization	PSM configuration information management (SFMT_PSM) SCA/SSS configuration information management (SFMT_SSS) Security violation events management (SFMT_POL)
	FMT_MTD.1 Management of TSF data	User information management (SFMT_USR) PSM configuration information management (SFMT_PSM) SCA/SSS 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	PSM configuration information management (SFMT_PSM) SCA/SSS configuration information management (SFMT_SSS) Security violation events management (SFMT_POL)
	FMT_SMF.1 Specification of Management Functions	User information management (SFMT_USR) PSM configuration information management (SFMT_PSM) SCA/SSS configuration information management (SFMT_SSS) Security violation events management (SFMT_POL) New policy online update (SFMT_POLUP) Intrusion detection/prevention result report (SFMT_RPT) Prevention of the loss of intrusion detection/prevention and audit data (SFMT_BKUP) PSM / SSS time synchronization (SFMT_TIME)



	FMT_SMR.1 Security roles	User information management (SFMT_USR)
TSF protection	FPT_AMT.1 Abstract machine testing	PSM / SSS Health Checking (SFPT_CHKSYS)
	FPT_FLS.1 Failure with preservation of secure state	TOE failure with preservation of secure state (SFPT_CHKTOE)
	FPT_RVM.1 Non-bypassability of the TSP	Security violation events management (SFMT_POL)
	FPT_SEP.1 TSF domain separation	PSM / SSS Health Checking (SFPT_CHKSYS)
	FPT_STM.1 Reliable time stamps	PSM / SSS time synchronization (SFMT_TIME)
	FPT_TST.1 TSF testing	PSM / SSS Health Checking (SFPT_CHKSYS) TSF stored data integrity check (SFPT_CHKINT)
Resource utilization	FRU_FLT.1 Degraded fault tolerance	TOE failure with preservation of secure state (SFPT_CHKTOE)
	FRU_RSA.1 Maximum quotas	Security violation events management (SFMT_POL)
TOE access	FTA_SSL.1 TSF-initiated session locking	TSF-initiated session locking(SFTA_SSL)
	FTA_SSL.3 TSF-initiated termination	Security violation events management (SFMT_POL)
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

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

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 Audit Data Generation (SFAU_GEN) 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) 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) 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 Search and Retrieval (SFAU_SAR) 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 Action 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) and Security Violation Events Management (SFMT_POL) to define the security policy for the TOE information flow control and to define the scope of the security policies.

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

This component uses Detection/Prevention Event Information Collection and Analysis (SFDP_CHK) and Security Violation Events Management (SFMT_POL) to define the security policy for the TOE information flow control and also to define the scope of the security policies.

13) FDP_IFF.1 Simple security attributes


This component uses Detection/Prevention Event Information Collection and Analysis (SFDP_CHK) and Security Violation Events Management (SFMT_POL) to describe the countermeasures for explicit attacks.

14) 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.

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

This component uses Security Violation Events Management (SFMT_POL), Detection/Prevention Event Information Collection and Analysis (SFDP_CHK) (SFDP_CHK), and Counter Attack Activity (SFDP_ACT) to requires that the identifier for the external IT entities be identified as a computer IP address, which shall identify external IT entities and create the audit history serving as the

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

criteria for illegal addresses, DoS attacks, and information flow control.

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

This component uses User Information Management (SFMT_USR) to require the identification of the administrator.

17) FIA_UAU.1 Timing of 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.

18) FIA_UAU.7 Protected authentication feedback

This component uses User Identification and Authentication (SFIA_LOGON), Mutual Identification and Authentication for Remote Connection through the Communication Channel (SFIA_UID) to ensure that only pre-defined feedbacks shall be provided to the administrator while the authentication is in progress.

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

This component uses Security Violation Events Management (SFMT_POL) Detection/Prevention Event Information Collection and Analysis (SFDP_CHK), Counter Attack Activity (SFDP_ACT) to ensure that it requires that the identifier for the external IT entities be identified as a computer IP 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.

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

This component uses User Identification and Authentication (SFIA_LOGON) to require the identification of the administrator.

21) FMT_MOF.1 Management of security functions behavior

This component uses User Information Management (SFMT_USR), PSM Configuration Information Management (SFMT_PSM), SCA/SSS Configuration Information Management (SFMT_SSS), Security Violation Events Management (SFMT_POL), New Policy Online Update (SFMT_POLUP), Intrusion Detection/Prevention Result Report (SFMT_RPT), Prevention of the Loss of Intrusion Detection/Prevention and Audit Data (SFMT_BKUP), and PSM/SSS Time Synchronization (SFMT_TIME) to provide the authorized administrator with the ability to manage the security functions as well as to ensure the availability when TOE failures occur.

22) FMT_MSA.1 Management of security attributes

This component uses User Information Management (SFMT_USR), PSM



Configuration Information Management (SFMT_PSM), SCA/SSS Configuration Information Management (SFMT_SSS), and 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.

23) FMT_MSA.3 Static attribute initialization

This component uses PSM Configuration Information Management (SFMT_PSM), SCA/SSS Configuration Information Management (SFMT_SSS), and Security Violation Events Management (SFMT_POL) to ensure that only the authorized administrator is allowed to get access to the initialization of the TSF data, or security attribute data, which is needed in performing the TOE security functions.

24) FMT_MTD.1 Management of TSF data

This component uses User Information Management (SFMT_USR), PSM Configuration Information Management (SFMT_PSM), SCA/SSS Configuration Information Management (SFMT_SSS), Security Violation Events Management (SFMT_POL), and New Policy Online Update (SFMT_POLUP) to require that only the authorized administrator should be able to manage the TSF data.

25) FMT_MTD.2 Management of limits on TSF data


This component uses PSM Configuration Information Management (SFMT_PSM), SCA/SSS Configuration Information Management (SFMT_SSS), and Security Violation Events Management (SFMT_POL) 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 pre-defined limits.

26) FMT_SMF.1 Specification of Management Functions

This component uses User Information Management (SFMT_USR), PSM Configuration Information Management (SFMT_PSM), SCA/SSS Configuration Information Management (SFMT_SSS), Security Violation Events Management (SFMT_POL), New Policy Online Update (SFMT_POLUP), Intrusion Detection/Prevention Result Report (SFMT_RPT), Prevention of the Loss of Intrusion Detection/Prevention and Audit Data (SFMT_BKUP) and PSM/SSS Time Synchronization (SFMT_TIME) to call for the specification of management functions such as security attributes, TSF data, and security function, which should be provided by TSF.

27) FMT_SMR.1 Security roles

This component uses User Information Management (SFMT_USR) to limit the

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	Security Target

role of a TOE security administrator to that of an administrator.

28) FPT_AMT.1 Abstract machine testing

This component uses PSM / SSS 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.

29) FPT_FLS.1 Failure with preservation of secure state

This component uses TOE Failure with Preservation of Secure State (SFPT_CHKTOE) to ensure that a secure state is preserved and the function of information flow control is performed when TOE failures occur.

30) FPT_RVM.1 Non-bypassability of the TSP

This component uses Security Violation Events Management (SFMT_POL) to ensure that the bypass of information flow control is prevented by assuring TSP enforcement functions to be invoked and succeed.

31) FPT_SEP.1 TSF domain separation

This component uses PSM / SSS 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.

32) FPT_STM.1 Reliable time stamps

This component uses PSM/SSS 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.

33) FPT_TST.1 TSF testing

This component uses PSM / SSS Health Checking (SFPT_CHKSYS), 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 with the capability to verify the integrity of TSF data and TSF executable code.

34) FRU_FLT.1 Degraded fault tolerance

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

35) FRU_RSA.1 Maximum quotas

This component uses Security Violation Events Management (SFMT_POL) to block the DoS attacks by enforcing maximum quotas of the TOE assets that each user can use.

36) 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.

37) FTA_SSL.3 TSF-initiated termination

This component uses Security Violation Events Management (SFMT_POL) 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.


38) 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-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	–
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	Testing
Vulnerability	AVA_MSU.2	Validation of analysis	Misuse Analysis

 LG N-Sys	Document Identification No.	Document Type
	SafezoneIPS V3.0 Security Target_20051205_V1.00.02	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, high-level 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

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	Addition/Modification
Assumption	A.Secure TOE external server	Addition
	A.TIME	Addition
Security objectives for the environment	OE. Secure TOE external server	Addition
	OE.TIME	Addition

As shown in this table, A.Secure TOE external server, A.TIME, OE.Secure TOE external server, and OE.TIME. are added to this ST.

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.

The SHA–1, a hash algorithm used in “ FPT_TST.1 TSF testing” satisfies SOF–medium as the probability of the attacker possessing a moderate attack potential to generate identical hash value is considerably low.

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.