WINS Technet

SNIPER IPS V5.0 (E4000)

Security Target

Version 1.4

2006/03/20

WINS Technet. CO., Ltd

Summary

This document is the security target of a network intrusion prevention system. (TOE : SNIPER IPS, Version : V5.0, Model : E4000, Platform : Self OS (SNIPER OS v1.0)).

Revision History

Version	Date	Reason
Version 1.4	2006/03/20	The final security target version from the observation report

Table of Contents

Intrusion Prevention System SNIPER IPS V.5.0 (E4000) will be described as ‘SNIPER’ from this page.

1. Security Target Introduction

This document is the security target of a network prevention system (Product name: SNIPER IPS, Version: V5.0, Model: E4000, Platform: Self OS (SNIPER OS v1.0)). 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: SNIPER IPS V5.0 (E4000) Security Target V1.4

2) Author: WINS Technet CO., Ltd

3) Common Criteria (CC) version: The Common Criteria for IT Security Evaluation (2005-25, the Ministry of Information and Communication)

4) Evaluation Assurance Level (EAL): EAL 4

5) Protection Profile claimed: Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005, KISA)

6) TOE identifier: SNIPER IPS V5.0 (E4000)

7) TOE description: Based on the IDS (Intrusion Detection System) developed at WINS Technet, and with an additional intrusion prevention engine, **SNIPER** thoroughly detects/blocks attacks toward the IT entity at the network base level. SNIPER is an Intrusion Protection System (IPS) that is installed in an In-line mode at the connection point of the external and internal network, detecting/blocking in realtime intrusions and attacks of the network traffic that flows into internal server.

8) Keyword : SNIPER IPS, Network-based Intrusion Detection, Intrusion Analysis, Intrusion countermeasure, Network Intrusion Prevention System, Information Flow Control

1.2 Security Target (ST) Overview

SNIPER is an Intrusion Protection System (IPS) that is installed in an In-line mode at the connection point of the external and internal network, detecting/blocking in realtime intrusions and attacks of the network traffic that flows into internal server. SNIPER provides intrusion detection function that collects, analyzes, and countermeasures the information generated by the user. It also provides intrusion protection function that blocks harmful packets, security management function, maintenance management function, live update function, user identification and authentication function, and lastly audit function that audit records activities of the administrator.

Prepared for CC certification of SNIPER, 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 SNIPER Scope and Boundary.

3) “TOE Security Environment” provides assumptions on environments where TOE is or will be used, explains threats that may exploit vulnerabilities either willingly or by chance, and describes security policies that are enforced by an organization and that TOE should adhere to, such as rules, procedures, practices, and guidelines.

4) “Security Objectives” describes the security objectives for the TOE and the environment required for reacting to threats and for satisfying assumptions and organizational security policies.

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

1.3 Common Criteria (CC) Conformance

TOE conforms to the Common Criteria for Information Technology Security Evaluation, Version 2.3 below and applies Final Interpretation (Oct. 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.

1.4 Glossary

- Audit Trail

A set of disk records that indicates information of users and their conducts.

- 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.

- SOF, Strength-of –Function

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.

- ST, Security Target

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

- Security violation events list

Detects intrusions by comparing the audit list or network packet with the intrusion detection events list that was predefined at Intrusion Detection System. In this case, the predefined intrusion events list stored at IDS is security violation events list.

- PP, Protection Profile

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

- Blackhole

A blocking policy list defining packets that needs to be blocked among the incoming traffics to SNIPER IPS. Since the blocking policy is set to its each time-out, it automatically deletes if it passed the expiration time.

- Anomaly Detection

Anomaly Detection is a detection method that has its basis on statistical means. It first creates profiles of normal actions of users, and then detects anomalies that deviate from those profiles.

- Human User

Any person who interacts with the TOE

- User

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

- Selection

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

- Identity

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

- Element

An indivisible security requirement.

- Role

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

- Operation

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

- Threat Agent

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

- External IT Entity

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

- Authorized Administrator

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

- In-line Mode

It configured as it enables the analysis and blocking operation for packets.

In case when IPS didn’t operate normally at the In-line Mode and when system keeps crashing, since they immediately cause network barriers, it configures Keep-alive Timer to send periodical signal.

- OPIE: One-time Passwords in Everything

Embodying RFC 1938, OPIE (One-time Passwords in Everything) is a one-time Passwords system developed at the US NRL (Naval Research Laboratory) and has its basis on S/Key, one of the One Time Password systems developed at Bellcore. Each password used in OPIE alters everytime it receives authentication, and therefore even with the stolen passwords, it is impossible to obtain access rights to the system. It is mentioned as OTP (One-Time Password).

- Authentication Data

Information used to verify the claimed identity of a user.

- 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)

It refers to common criteria for IT security evaluation proclaimed by the minister of information and communication on May 21st 2005. The Common Criteria for IT security evaluation is a Korean version of the International Common Criteria (CC) version 2.3 that was developed to attain 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.

- Final Interpretations

An officially released document by CCIB with additional interpretations or correction of errors to the official CC

- Augmentation

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

- 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.

- TOE, Target of Evaluation

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

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

- Packet

A set of data that is used in transmitting data on the network. Instead of transmitting data continually between the two points, packet transmission includes the method that divides transmitting data into adequate pieces to consist packet forms and transmit them one by one. Each packet contains not only a consistent size of data but also contains receiving place, address or even control information such as control code.

- Abstract machine

  It may be a hardware/firmware platform or a combination of hardware/software known as or assessed operating like an abstract machine. As underlying abstract machine used in this function package becomes OS when the TOE is application program and refers to firmware or hardware when the TOE is OS.

- 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.

- Challenge (Challenge Value)

  A value used at OPIE. Obtains result value that can access to the server with passwords that the users remember or with a combination of Key and Seed.

- DOM (Disk on Module)

  Disk on Module(DOM) is a high-performance embedded flash memory data storage system.

- HA (High Availability)

  HA indicates systems or components that can be constantly operated for an adequate length of time. SNIPER, in order to maintain everything available so that the entire network remains stable, consists two system pieces. When one of the two fails, send traffics to the other co-system and therefore maintain the normal network service.

- GUI (Graphical User Interface)

  A graphic user interface. It implemented interface between the user and computer into a ahpic.

- QoS (Quality of Service)

  An idea of attributes that can be somewhat guaranteed beforehand. QoS is also capable of transfer rate, error rate, estimation, and improvement on the internet or other networks. It refers to a function that insures consistent traffic processing load and therefore provides trusted service on the network device.

- Seed (Seed Value)

  A part of identifier that is generated from the system or specified by the user. It is composed of the combination of characters and numbers. (example, sn12345).

- 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.

- TSP, TOE Security Policy

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

- TSF Data

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

- TSC, TSF Scope of Control

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

- TTL (Time-To-Live)

  TTL is a value that exists inside the IP packet. TTL notifies the router whether a packet should be discarded since it stays too long inside the network. Packets may not be delivered to the designated place in time due to many reasons. For instance, the combination of incorrect routing tables may cause endless circulation of packet. When a certain period of time goes by, TTL is used as a solution in order to notify a sender so that the sender may decide whether to discard the packet and retransmit. Initial value of the TTL is normally set to 8 bit long packet heather by the system.

- Common abbreviations of CC

CC	Common Criteria
CCIMB	Common Criteria Interpretation Management Board
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
FI	Final Interpretation
IP	Internet Protocol
IT	Information Technology
PP	Protection Profile
RFC	Request for Comments
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.5 References

[1] Common Criteria for Information Technology Security Evaluation v2.3, the Ministry of Information and Communication (2005-25)

[2] Network Intrusion Prevention System Protection Profile for a state organ use V1.2, May. 17, 2006, KISA

[3] Network Intrusion Prevention System Protection Profile for a state organ use V1.2, May. 17, 2006, KISA

[4] Protection Profile and Security Target writing guide, Information and communication standards TTAR-0011, Dec. 11, 2002, KISA

[5] Network Intrusion Prevention System Protection Profile V1.1, Dec. 21, 2005, KISA

2. TOE Description

2.1 Product Type

서식 있음: 글머리 기호 및 번호 매기기

1) TOE is a network-based intrusion prevention system equipped with a function that can safely protect the internal assets, protect and prevent the intrusions

2) TOE is located at the connection point between an external network and internal network where it detects intrusions of network traffic in real time and performs prevention function.

3) TOE provides the following functions: an intrusion detection function that collects, analyzes, and reacts to, the activity data; a function to control unauthorized traffic; live update function; 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.

2.2 TOE Environment

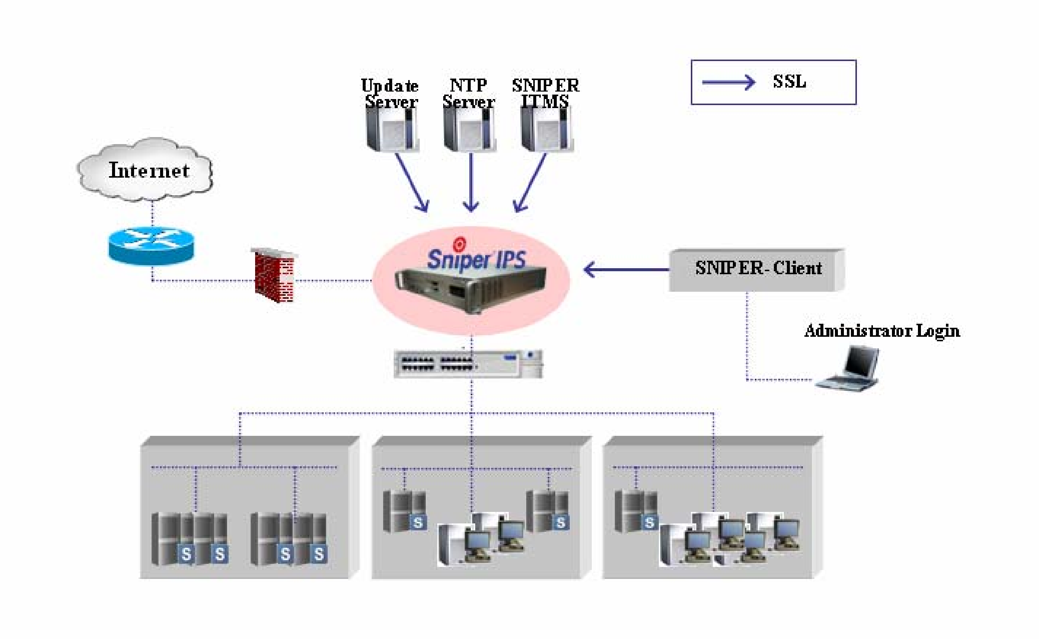
2.2.1 IT Environment

TOE IT Environment includes Update Server, NTP (Network Time Protocol) Server, and ESM/SNIPER ITMS etc...

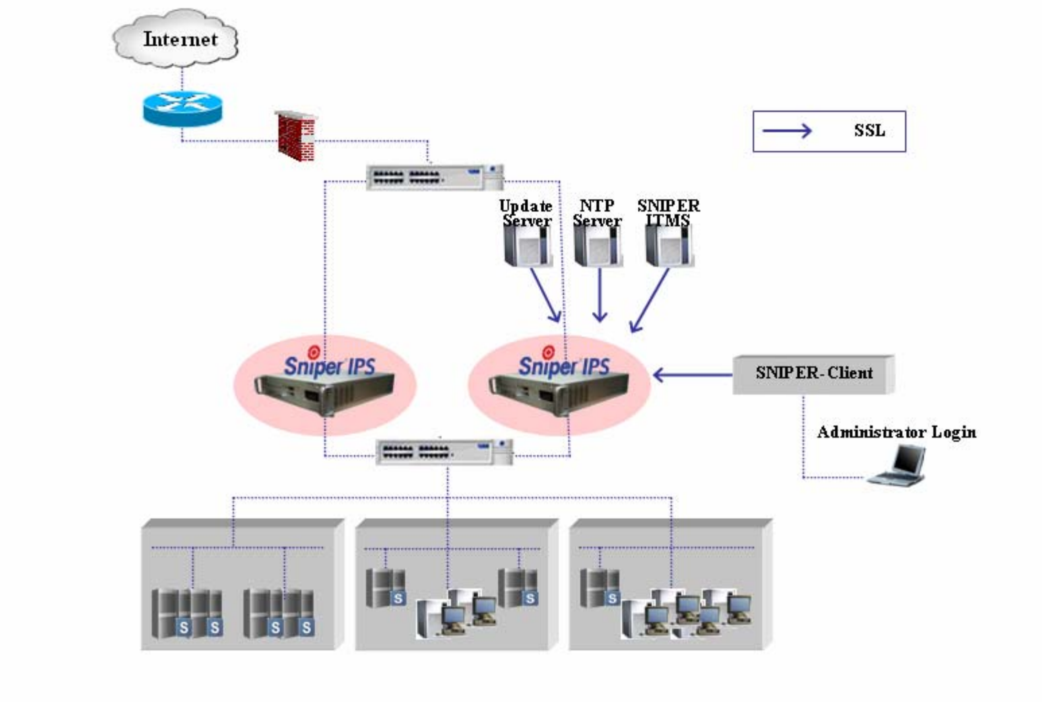
SNIPER and NTP Server communicate using Network Time protocol. For a secure communication, SNIPER communicates using identification and authentication data, internally transmitted data and area or SNIPER Client of the distant place and SSL protocol.

2.2.2 Network Environment

An objective for the main functions of TOE is a dynamic countermeasure towards network attacks and an identification of the attacks. .



[Image 1] TOE Network Environment



[Image 2] TOE Network Environment (High availability)

According to the two following methods, the TOE can be installed and operated either at the connection point of the internet and internal network or at the point where the network is divided into the external and internal network and then operated through the following methods.

As it appears in (Image 1), the TOE is independently installed and operated in an In-line mode at the point where the network is divided into the external and internal network

As it appears in (Image 2), the TOE is installed in duplicate either at the connection point of the internet and internal network or at the point where the network is divided into the external and internal network.

SNIPER Client manages the TOE locally or remotely.

2.3 TOE Boundary

2.3.1 Physical Scope

SNIPER, where the TOE is included, consists of a dedicated hardware system (SNIPER engine) and SNIPER Client. The following table summarizes the hardware specifications of them.

	SNIPER Server (H/W type)			**SNIPER Client**
Operation System	SNIPER OS V1.0			MS Windows XP professional (Install IE 5.0 or more)
Options	CPU	Intel Xeon DP CPU 3.6GHz*2		Intel Pentium Ⅱ 400Mhz or subsequent compatible versions
	Memory	2G DDR-II		128MB or more
	HDD(LOG)	3.5” 73GB (SCSI) * 2		2GB or more
	DOM	512MB		Monitors supporting 1280 x 1024 pixels or more, sound card and speaker
Number of Port	Administration Port	10 / 100/ 1000 Mbps	2 port	More than one 10/100 NIC
	Packet gathering port	1000 Mbps	6port	
Features	■ SNIPER Client installs automatically after downloading OCXs from SNIPER Server.			

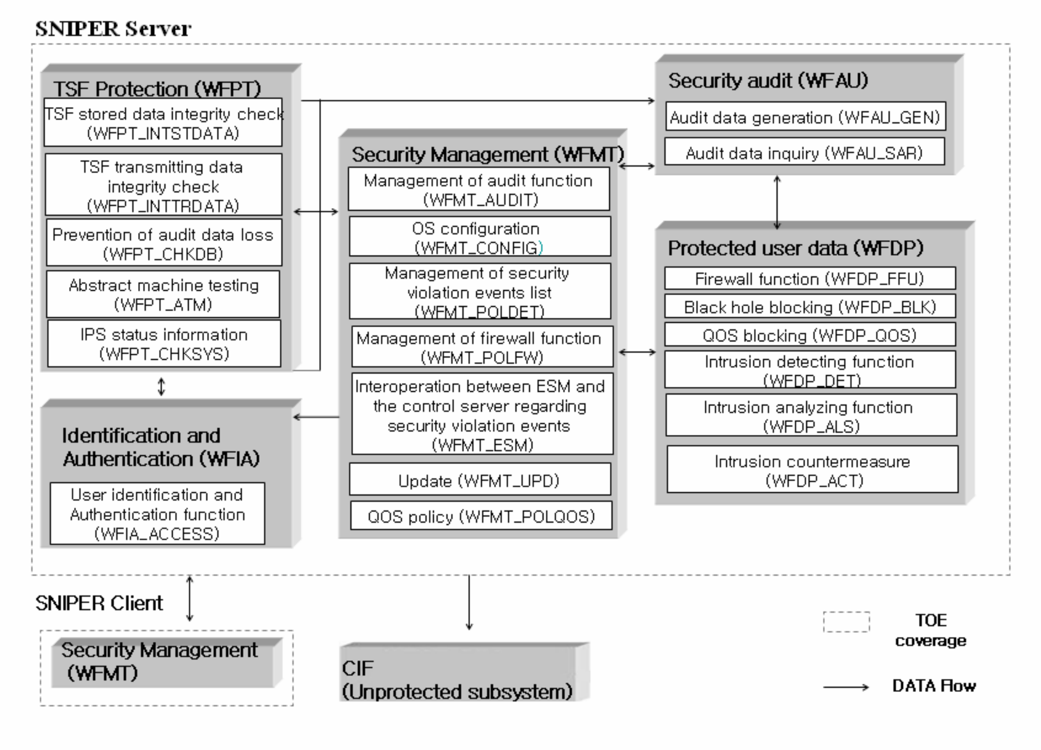
[Table 1] SNIPER performance and Hardware options

DOM (Disk on Module) is a high-performance embedded flash memory data storing system installed with SNIPER OS and SNIPER IPS.

HDD is used for storing Log.

SNIPER IPS V5.0 E4000 provides 8 ports in all, of which 6 of them support 1000Mbps that is purposed for the packet collection and 2 of them support 10/100/1000 Mbps that is purposed for the administration.

2.3.2 Logical Scope


SNIPER Server
TSF Protection (WFPT)
TSF stored data integrity check (WFPT_INTSTDATA)
TSF transmitting data integrity check (WFPT_INTTRDATA)
Prevention of audit data loss (WFPT_CHKDB)
Abstract machine testing (WFPT_ATM)
IPS status information (WFPT_CHKSYS)
Identification and Authentication (WFIA)
User identification and Authentication function (WFIA_ACCESS)
Security Management (WFMT)
Management of audit function (WFMT_AUDIT)
OS configuration (WFMT_CONFIG)
Management of security violation events list (WFMT_POLDET)
Management of firewall function (WFMT_POLFW)
Interoperation between ESM and the control server regarding security violation events (WFMT_ESM)
Update (WFMT_UPD)
QOS policy (WFMT_POLQOS)
Security audit (WFAU)
Audit data generation (WFAU_GEN)
Audit data inquiry (WFAU_SAR)
Protected user data (WFDP)
Firewall function (WFDP_FFU)
Black hole blocking (WFDP_BLK)
QOS blocking (WFDP_QOS)
Intrusion detecting function (WFDP_DET)
Intrusion analyzing function (WFDP_ALS)
Intrusion countermeasure (WFDP_ACT)
SNIPER Client
Security Management (WFMT)
CIF (Unprotected subsystem)
TOE coverage
DATA Flow

[Image 3] Logical Scope of the TOE

The following are logical scopes of the SNIPER.

- Security audit (WFAU)

Security audit sub-system operates a function of Audit data generation (WFAU_GEN) and Audit data inquiry (WFAU_SAR). This function collects and analyzes record history of the system use to check whether the system is operating consistently and efficiently. The audit result is used for detecting or blocking intrusions on the computer system and for detecting misuse of the system.

- User Data Protection (WFDP)

User Data Protection sub-system operates Firewall function (WFDP_FFU), Blackhole block (WFDP_BLK), QoS block (WFDP_QOS), Intrusion Detection function (WFDP_DET), Intrusion Analyzing function (WFDP_ALS), and Intrusion Countermeasure function (WFDP_ACT). 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 (WFIA)

Identification and Authentication sub-system operates user identification and authentication process (WFIA_ACCESS). Only authorized administrators are allowed to access key functions that are essential to the regular operation of SNIPER such as changing, deleting and adding policies and retrieving log files. In order to control the access to SNIPER perfectly, every access attempt through an administrator interface are examined to identify and authenticate an appropriate administrator. The communication between SNIPER Client and the engine is encrypted using SSL and its integrity is verified through SHA-1 to prevent any modification or exposure of the data.

Even with the access of an authorized administrator, if not operate for a certain period of time; protect the TOE during the inactive terms of an authorized administrator by locking up the interacting sessions.

• Security Management (WFMT)

Security Management sub-system operates Audit Management(WFMT_AUDIT), OS Configuration(WFMT_CONFIG), Management of Security Violation List (WFMT_POLDET), Firewall function Management(WFMT_POLFW), Management of Interoperation between ESM and the Control Server regarding security violation events (WFMT_ESM), Update(WFMT_UPD), and QoS Policy(WFMT_POLQOS). Security Management function provides the rules for detection/prevention SNIPER performs and the managerial actions retrieving and modifying information related to the state and configuration of SNIPER.

• TSF Protection (WFPT)

TSF Protection sub-system operates TSF stored data integrity check (WFPT_INTSTDATA), TSF transmitting data integrity check (WFPT_INTTRDATA), Prevention of audit data loss (WFPT_CHKDB), and Abstract machine testing (WFPT_ATM), IPS state information(WFPT_CHKSYS). TSF Protection subsystem 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 periodical monitoring.

In cases where components of the TOE interact remotely through internal communication channels, Server and Client identify and authenticate the nodes of the other side to ensure safe channels between TSFs.

3. TOE Security Environment

3.1 Assumption

서식 있음: 글머리 기호 및 번호 매기기

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

.Category	Item	Remark
Assumptions	A.Physical Security	
	A.Security Maintenance	
	A.Trusted Administrator	
	A.Hardened OS	
	A.Single Connection Point	
	A.Secure TOE external server	Added to ST
	A.TIME	Added to ST
	A.SSL Certificate of TOE	Added to ST

[Table 2] Identification of assumptions

- A. Physical Security

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

- A. Security Maintenance

When the internal network environment is changed due to network configuration changes, an increase or decrease of hosts, or an increase or decrease of services, the new changes are immediately noted and security policies are configured in accordance with the TOE operational policy to maintain the same level of security as before.

- A. Trusted Administrator

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

- A. Hardened OS

The underlying OS of the TOE ensures the reliability and stability by both eliminating the unnecessary services or means not required by the TOE and installing the OS patches.

- A. Single Connection Point

The TOE is installed and operated on a network and separates the network into external and internal network. Information can not flow between the two without passing through the TOE.

- A. Secure TOE External Sever

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.

- A. TOE SSL Certificate

The TOE, when installing the certificate that will be used for SSL authentication, generates in advance and stores at the TOE. SSL Certificate of the TOE is safely generated and managed.

3.2 Threats

서식 있음: 글머리 기호 및 번호 매기기

Threats are categorized into threats to the TOE and threats about the TOE operational environment.

Category	Items
Threat to the TOE (Threat)	T.Masquerade
	T.Failure
	T.Audit Failure
	T.Inbound Illegal Information
	T.Unauthorized sevice 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] Identification of Threats

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 Attack

  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 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.

2) Threats to the TOE Operational Environment

- TE. Poor Administration

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

- TE. Distribution and Installation

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

3.3 Organizational Security Policy

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

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

[Table 4] 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.

- P.SSL Certificate Administration

SNIPER must store and manage when safely creating SSL Certificate.

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 non technical/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
	OE.SSL Protocol	Added to ST

[Table 5] 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.

- 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.

- O. O.Information Flow Control

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

- O.TSF Data Protection

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

4.2 Security Objectives for the Environment

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

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.

- OE.SSL Protocol

The TOE mutually certificates through SSL Certificate, Administrator ID and Password using SSL protocol, and therefore protects the transmitting TSF data.

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 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 SNIPER Functional Requirements

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

Security functional class	Security functional component
FAU (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(1) Simple security attributes(1)
	FDP_IFF.1(2) Simple security attributes(2)
	FDP_IFF.1(3) Simple security attributes(3)
	FDP_IFF.1(4) Simple security attributes(4)
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.4 Reuse Prevention authentication mechanism
	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(1) Management of TSF data(1)
	FMT_MTD.1(2) Management of TSF data(2)
	FMT_MTD.1(3) Management of TSF data(3)
	FMT_MTD.1(4) Management of TSF data(4)
	FMT_MTD.2(1) Management of limits on TSF data(1)
	FMT_MTD.2(2) Management of limits on TSF data(2)
	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 6] Security functional requirements

5.1.1 Audit

5.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components

FAU_ARP.1.1 The TSF, when detects potential security violation, shall take [List of actions to minimize the following problems {Sending mails to the authorized administrator, warning screen, session termination]

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.

Component	Auditable event	Additional audit record
FAU.ARP.1	Actions taken due to an urgent security violation	Alarmed or not
FAU.SAA.1	Auto intrusion countermeasure by an initiation and abeyance of the analysis mechanism, and tools.	Alarmed or not
FAU.SEL.1	Modified items of the audit configuration occurred while the audit gathering function was operating.	Identity of an authorized Administrator (User ID)
FDP_IFF.1	All decisions on requests for information flow	Identification information of subject and object
FIA_AFL.1	Reaching limits of the unsuccessful authentication attempts and actions taken, If proper, recover to the normal state occurring subsequently.	User identity provided to the TOE (User ID)

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_SMF.1	The use of administration function	Identity of an authorized administrator
FRU_FLT.1	All failures detected by the TSF	-
FRU_RSA.1	Denial of assigned operation due to resource limitation.	-
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	-
FTA_SSL.1	Interacting session locking by the session locking mechanism	-
FTA_SSL.3	Interacting session termination by the session locking mechanism	-
FTP_ITC.1	Failure of secure channel functions, identification of the inaugurator and the target on the secure channel where the failure occurred.	Identification of the inaugurator and the target on the secure channel where the failure occurred.

[Table 7] Auditable events

c) [[Table-7] Refer to auditable events, Auditable events determined by the ST author: None]

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

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),

Auditable events information based on the definition [[Table-7] determined by the ST author: None]

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 violation of the TSP.

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

a) Accumulation or combination of the followings known as indicating potential security violation [

- Insufficient capacity of the stored medium warning
- Excess of the access attempt limits configured by an administrator
- Integrity errors warning
- Packet Drop due to an excessive traffic
- An overload reaching more than 90% on CPU remains more than 3 minutes
- Problems occurred at NIC]

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, ordering* of audit data based on [Type of events, time, results]

Dependencies: FAU_SAR.1 Audit review

5.1.1.7 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

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

a) *Victim identity, user identity, subject identity, host identity, event type*

b) [Classify the internal and external network hosts according to network sections]

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 generation

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 [actions to alert the authorized administrator, suspend Logging towards the descriptive DB, send E-mails to the authorized administrator, indicate warning messages in case of possible audit storage failure] if the audit trail exceeds [90% of the stored medium usage limit configured by the authorized administrator].

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.1.10 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized user with special rights* and [Modify Firewall policy to DROP when the capacity of the stored medium is less than 100MB] 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 [**Blocking Policy**] on list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP.

a) [subjects: unauthenticated external IT entities that send information;

b) Information: 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

Application notes: The term ‘Policy to reject all’ of the Intrusion Prevention System Protect Profile is substituted with ‘Blocking policy’ in this document.

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

Hierarchical to: FDP_IFC.1

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

a) [subjects: unauthenticated external IT entities that send information;

b) Information: 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

Application notes: The term ‘Policy to allow all’ of the Intrusion Prevention System Protect Profile is substituted with ‘Blackhole policy’ in this document.

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

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [blocking policy] based on at least the following types of subjects and information security attributes: [list of subjects and information]

a) Subject security attribute: IP address of the external IT entities that send/receive information, Administrator

b) Information security attributes:

- Departure address
- Destination address
- Protocol
- Port

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

- Session registered on a Whitehole table
- Session registered on a CPList by the Stateful inspection
- Session allowed to access by the ACCEPT rule at Firewall rule.

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

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

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on [the simple directed information flow when the departing point is TOE]

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

- Rules mentioned in FDP_IFF.1.2 do not exist.

- Information flow security policy generated by the authorized administrator [none].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

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

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [blackhole policy] based on at least the following types of subject and information security attributes: [list of subjects and information]

a) Subject security attribute: IP address of external IT entities that send/receive information, Administrator

b) Information security attributes:

- Departure address
- Destination address
- Protocol
- Destination Port

FDP_IFF.1.2 The TSF shall allow information flow between controlled subject and information through controlled operation if the following rules were maintained: [Following rules]

- In case rules mentioned in FDP_IFF.1.3 do not correspond to any rules

FDP_IFF.1.3 The TSF shall enforce [Allow information flow when the following rules exist].

- When the session reaching the attack accepted count was generated during the attack accepted time that was defined by an administrator authorized at a single departing address (terminate the corresponding session)
- TCP/UDP Time Out: 1 Hour, Session Full: When exceeded 150,000 session (DROP exceeded session)
- History registered by an administrator at the Realtime block list.
- When exceeded TCP/UDP session termination time set by an authorized administrator

FDP_IFF.1.4 The TSF shall provide [None].

FDP_IFF.1.5 The TSF shall explicitly authorize the information flow based on [One-way information flow where its departing point is TOE]

FDP_IFF1.6 The TSF shall explicitly deny the information flow according to the following rules.

a) [The TOE must block access request of the information transmitted from the external network IT entity including internal subject IP address.

b) The TOE must block access request of the information transmitted from the internal network IT entity including external subject IP address.

C) The TOE must block access request of the information transmitted from the external network IT entity that includes broadcasting subject IP address.

C) The TOE must block access request of the information transmitted from the external network IT entity that includes broadcasting loofing subject IP address.

e) The TOE must block access request of the information transmitted from the external network IT entity that includes abnormal packet structure.

f) [Block access network when internet use of the IT entity was set to ‘Banned’.
Block access network when it was classified to harmful site and set to ‘block’
Block access network when the session was blocked by the administrator.]

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

5.1.2.5 FDP_IFF.1 (3) Simple security attributes (3)

Hierarchical to: No other components

FDP_IFF.1.1 The TSF shall enforce the [QoS policy] based on at least the following types of subject and information security attributes: [list of subjects and information]

a) Subject security attribute: IP addresses of external IT entities that send/receive information,
Administrator

b) Information security attributes:

- Departure address
- Destination address
- Protocol
- Destination Port
- Blocking Method

FDP_IFF.1.2 The TSF shall allow information flow between the controlled subject and information through the controlled operation if the following rules were maintained: [Following rules]

- If the authorized number of session of IT entity is less than the limit value set by QoS policy of FMT_SMF.1

FDP_IFF.1.3 The TSF shall enforce [none]

FDP_IFF.1.4 The TSF shall provide [none]

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

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

- Rules mentioned in FDP_IFF.1.2 do not exist
- The information flow security policy generated by an authorized administrator does not exist

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

5.1.2.6 FDP_IFF.1 (4) Simple security attributes (4)

Hierarchical to: No other components

FDP_IFF.1.1 The TSF shall enforce the [Intrusion analyzing policy] based on at least the following types of subject and information security attributes: [list of subjects and information]

a) Subject security attribute: IP address of the external IT entities that send/receive information, Administrator

b) Information security attributes:

- Protocol
- Destination Port
- Attack accepted count
- Attack accepted time
- Access time limit
- Detection String pattern

FDP_IFF.1.2 The TSF shall allow the information flow between controlled subject and information by the controlled operation if the following rules were maintained: [Following rules]

- When authorized to access after comparing security violation events list with Pattern Block list.
- When the incoming attack was defined upon its attack accepted count and time, but did not correspond to any of those.
- When the traffic is not abnormally exceeding
- Detectable security violation events types are shown below.
  - Denial of Service Attack
  - Information gathering Attack
  - Protocol Vulnerability
  - Service Attack
  - Web CGI Attack
  - Backdoor Attack
  - User definition Attack
  - Service Statistic Analysis
  - Protocol Statistic Analysis
  - IP Statistic Analysis
  - Pattern Block

FDP_IFF.1.3 The TSF shall enforce [none]

FDP_IFF.1.4 The TSF shall provide [none]

FDP_IFF.1.5 The TSF shall explicitly authorize the information flow based on [One-way information flow where the departing point is TOE]

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

a) [The TOE shall block a request for network access of the information from external network IT entities has internal subject IP addresses.

b) The TOE shall block a request for network access of the information from internal network IT entities has external subject IP addresses.

c) The TOE shall block a request for network access of the information from external network IT entities have broadcasting subject IP addresses.

d) The TOE shall block a request for network access of the information from external network IT entities have loofing subject IP addresses.

e) The TOE shall block a request for network access of the information from external network IT entities have abnormal packet structures.

5.1.3 Identification and Authentication

5.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when [1~3] unsuccessful authentication attempts related to [the authentication of TOE use for the administrator] occur.

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 until an action is taken by the authorized administrator, Access limit to the user ID for 30 seconds to the SNIPER server, report to the administrator mail]

Dependencies: FIA_UAU.1 Authentication

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

Hierarchical to: No other components

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

a) IP Address

b) {Authorized} Administrator security attributes

Dependencies: no dependencies

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.
- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu.

Cannot use configuration function. Can only inquire essential search history during the audit.

- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

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 IT entity: [the following security attributes].

a) Identifier

b) User security attribute that includes {User ID, Password, Term of Validity, Authority and Information on the other administrators, number of unsuccessful authentication}.

Dependencies: no dependencies

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.
- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu. Cannot use configuration function. Can only inquire essential search history during the audit.
- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

5.1.3.4 FIA_UAU.1 Authentication

Hierarchical to: No other components

FIA_UAU.1.1 The TSF shall allow [Administrator's IP that may access beforehand must be registered and must acquire the certificate. A login screen in which ID and password are entered is operated. Access ID and password provided as default must be modified by the administrator.] 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 administrator.

Dependencies: FIA_UID.1 Identification

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.
- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu.

Cannot use configuration function. Can only inquire essential search history during the audit.

- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

5.1.3.6 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 Authentication

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.
- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu. Cannot use configuration function. Can only inquire essential search history during the audit.
- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

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

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

5.1.3.8 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

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.

- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu. Cannot use configuration function. Can only inquire essential search history during the audit.
- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

5.1.4 Security Management

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 following] ability to [the authorized administrator].

Security Function		Super Administrator	Security Administrator	Administrator
Security audit	Security audit history	Configuration, Inquiry, Modification	-	-
	SNIPER Executable history	Inquiry	-	-
	Access history inquiry	Inquiry	-	-
	Essential information search history inquiry	Inquiry	Modification	-
	Connection Failure Management	Configuration, Inquiry, Modification	-	-
	Integrity Verification	Configuration, Inquiry, Modification	-	-
	Process	Inquiry	-	-
	X-Driver	Configuration, Inquiry, Modification	-	-
	IPS state information	Configuration, Inquiry, Modification		
	Stored medium Management	Configuration, Inquiry, Modification	-	-
	DB Backup	Configuration, Inquiry, Modification	-	-
	DB Restore	Configuration, Inquiry, Modification	-	-
	Time Synchronization	Configuration, Inquiry, Modification	-	-

Configuration	Administrator Management	Configuration, Inquiry, Modification	-	-
	Detection Policy Set up	Configuration, Inquiry, Modification	-	-
	Blocking Policy Set up	Configuration, Inquiry, Modification	-	-
	QoS Policy	Configuration, Inquiry, Modification	-	-
	Host Management	Configuration, Inquiry, Modification	-	-
	Log Management	Configuration, Inquiry, Modification	-	-
	Harmful Information	Configuration, Inquiry, Modification	-	-
	Network	Configuration, Inquiry, Modification	-	-
	Realtime Monitoring	Configuration, Inquiry, Modification	-	-
	Statistic Information	Configuration, Inquiry, Modification	-	-
	Engine/GUI Update	Configuration, Inquiry, Modification	-	-
	Pattern Update	Configuration, Inquiry, Modification	-	-
Menu	Configuration	Configuration, Inquiry, Modification	-	-
	Icon Setting	Configuration, Inquiry, Modification	Configuration, Inquiry, Modification	Configuration, Inquiry, Modification
	User Definition	Configuration, Inquiry, Modification	Configuration, Inquiry, Modification	Configuration, Inquiry, Modification
	Packet Gathering Device	Configuration, Inquiry, Modification	Configuration, Inquiry, Modification	Configuration, Inquiry, Modification

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

5.1.4.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1 The TSF shall enforce [Blocking policy, Blackhole policy, and QoS policy, Intrusion Analyzing policy] to restrict the ability to *change_default, query, modify[create]* [the following] security attributes to [the authorize administrator].

Security Attribute	Action	Remark
Management of Administrator	Query, Modify, Delete, Create	Administrator ID, Password, Term of Validity, Mobile number, Electronic mail, IP setting
Denial of Service	Query, Modify	RCLS(External user-Internal server), LCRS(Internal server- External server), LCLS(Internal user- Internal server), Detection, Defense, Exceptional IP, Attack Accepted Count, Attack Accepted Time, Blocking Time, Risk Level, Alarm, E-mail, Mobile
Information Gathering	Query, Modify	RCLS(External user - Internal server), LCRS(Internal user - External server), LCLS(Internal user - Internal server), Detection, Defense, Exceptional IP, Attack Accepted Count, Attack Accepted Time, Blocking Time, Risk Level, Alarm, E-mail, Mobile
Protocol Vulnerability	Query, Modify	RCLS(External user - Internal server), LCRS(Internal user - External server), LCLS(Internal user - Internal server), Detection, Defense, Exceptional IP, Attack Accepted Count, Attack Accepted Time, Blocking Time, Risk Level, Alarm, E-mail, Mobile
Service Attack	Query, Modify	RCLS(External user - Internal server), LCRS(Internal user - External server), LCLS(Internal user - Internal server), Detection, Defense, Exceptional IP, Attack Accepted Count, Attack Accepted Time, Buffer Size, Blocking Time, Risk Level, Alarm, E-mail, Mobile
WebCGI Attack	Query, Modify, Delete, Create	Attack name, Detection, Defense, Blocking Time, RCLS(External user - Internal server), LCRS(Internal user - External server), LCLS(Internal user - Internal server), Detection, Defense, Exceptional IP, Blocking Time, Risk Level, Alarm, E-mail, Mobile
Backdoor	Query, Modify, Delete, Create	Attack name, Detection, Defense, Attack Accepted Count, Attack Accepted Time, Blocking Time RCLS(External user - Internal server), LCRS(Internal user - External server), LCLS(Internal user - Internal server), Risk Level, Alarm, E-mail, Mobile, Protocol, Server Port
User Definition	Query, Modify, Delete, Create	Attack name, Detection, Defense, Attack Accepted Count, Attack Accepted Time, Blocking Time, RCLS(External user - Internal server), LCRS(Internal user - External server), LCLS(Internal user - Internal server), Risk Level, Alarm, E-mail, Mobile, Protocol, Server Port, Detection String, Type, FLOW, Offset value,

		Offset compare
Protocol Statistic Analysis	Query, Modify	Detection, Detection Method, Manual Threshold, Risk Level, Alarm, E-mail, Mobile
Service Statistic Analysis	Query, Modify, Delete, Create	Attack name, Risk Level, Alarm, E-mail, Mobile, Protocol, Server Port, Detection Method, Manual Threshold, Detection
IP Statistic Analysis	Query, Modify	Detection, Detection Method, Exceptional IP, Manual Threshold, Risk Level, E-mail, Mobile
PATTERN BLOCK	Query, Modify, Delete, Create	Attack name, Detection, Defense, Blocking Time, RCLS(External user-Internal server), LCRS(Internal user-External server), LCLS(Internal user-Internal server), Risk Level, Alarm, E-mail, Mobile, Protocol, Server Port, Detection String, Type, Capital letter and small letter distinction, Blocking Method, Attacker Contraction, Target Contraction, FLOW, Offset Value, Offset Compare
Blocking Policy	Query, Modify, Delete, Create	Application, Interface, Source IP/Security Level, Destination IP/ Security Level, Service, Protocol, Port, Security Level, Policy(ACCECPT/DROP), Log
QoS Policy	Query, Modify, Delete, Create	Interface, Application, QoS Type, Protocol, Port, Limiting value
Host Management	Query, Modify, Delete, Create	Basic policy on internet use, Individual policy on internet use (MAC Address/ IP Address/Host name/Internet use/Routing function)
Log Management	Query, Modify, Delete, Create	External user-Internal server, Internal user-External server, Internal user-Internal server, (Port, Protocol, Time setting)
Harmful data	Query, Modify, Delete, Create	Policy, Tine setting, IP address, Search Key
Network	Query, Modify, Delete, Create	Internal IP Address, Audit IP Address, Audit Exceptional IP Address, Interface, Interface name
Engine/GUI Update	Query, Modify	Release History Confirm, Execute Update
Pattern Update	Query, Modify	Release History Confirm, Execute Update, Alarm setting (period/time)

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.
- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu. Cannot use configuration function. Can only inquire essential search history during the audit.
- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

5.1.4.5 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components

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

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

Dependencies: FMT_MSA.1 Security attributes management
FMT_SMR.1 Security roles

Application notes: Only Super administrator can operate.

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

Hierarchical to: No other components

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, query, modify, delete, erase, [null]* the [blocking policy, Alarm rules] to [the authorized administrator].

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

Application notes: The firewall policy and blackhole policy shall only be configured by 'Super administrator', an administrator with full authorities. The alarm rules may only be configured by 'Super administrator', 'Security administrator', and 'Administrator'.

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

Hierarchical to: No other components

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, query, modify, delete, erase, [create]* the [Attack pattern among blocking policies] to [the authorized administrator].

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

Application notes: The firewall policy and blackhole policy shall only be configured by 'Super administrator', an administrator with full authorities. The alarm rules may only be configured by 'Super administrator', 'Security administrator', and 'Administrator'.

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

Hierarchical to: No other components

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, query* [the followings] to [the super administrator].

- The TOE Timestamp used when tracing the Audit list.
- Session Time-out value of the authorized administrator
- Audit list related configuration value
- Auto Update cycle

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

5.1.4.9 FMT_MTD.1 (4) Management of TSF data (4)

Hierarchical to: No other components

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

- TCP/UDP Session Time out

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

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.
- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu. Cannot use configuration function. Can only inquire essential search history during the audit.
- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

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

Hierarchical to: No other components

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

FMT_MTD.2.2 The TSF shall perform [the actions specified at FAU_STG.3, FAU_STG.4] if the TSF data are at, or exceed, the designated limits:

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

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

Hierarchical to: No other components

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for the [Number of unsuccessful authentication attempts] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall perform [the actions specified at FIA_AFL.1] if the TSF data are at, or exceed, the designated limits:

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

5.1.4.12 FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

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

. [

a) Management of TSF function

- Item indicated at FMT_MOF.1

b) Management of TSF security attributes

- Item indicated at FMT_MSA.1

c) Management of TSF data

- Item indicated at FMT_MTD.1

d) Management of TSF data limit

- Item indicated at FMT_MTD.2

e) Management of security role

- Item indicated at FMT_SMR.1]

Dependencies: No dependencies

5.1.4.13 FMT_SMR.1 Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the roles [Super administrator, Security administrator, Administrator].

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

Dependencies: FIA_UID.1 Identification

Application notes: Administrator classifies into Super administrator, security administrator, and administrator. Each administrator has unique authority.

- Super administrator: Consist of 1 person. Performs overall functions of SNIPER.
- Security administrator: Capable of managing Realtime monitoring, Recent monitoring, Detection/Defense/Alarm, Realtime block list, General report, Help menu. Cannot use configuration function. Can only inquire essential search history during the audit.
- Administrator: Capable of managing Monitoring, Recent monitoring, detection/defense/alarm, and help menu. Cannot use Configuration, security, and audit function.

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, and during the integrity test on the TSF* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

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.

[Types of failures list described in **FRU_FLT.1**].

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

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 able to maintain reliable time stamp by the help of NTP server provided for the IT environment. The TOE, in order to obtain time information, accesses to NTP server, functioning as NTP client. The TOE is also capable of obtaining time information of the system provided by the proprietary OS. The way the TOE obtains time information follows administrator’s decision.

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 the 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

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: [transmitting layer demonstration] that *the group of defined IT entities* 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 According to the following rules, the TSF shall lock the session that interacts after when [the client screen of SNIPER does not activate for a certain period of time designated by **the authorized administrator** or there are no inputs from the keyboard and mouse.]

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 Authentication

5.1.7.2 FTA_SSL.3 TSF-initiated session termination

Hierarchical to: No other components

FTA_SSL.3.1 The TSF shall terminate the session that interacts after [the following inactive period of **the authorized IT entity**, {Excess session maximum quotas}].

- When the TCP/UDP session time-out of an authorized IT enitity has exceeded the TCP/UDP session termination time designated by an authorized administrator at FMT_MTD.1.
- When the number of sessions of an authorized IT entity exceeds the blocking method that was set after comparing with the blocking method of QoS policy interface, all traffic, protocol, service port at

FMT_MSA.1.

- When the number of an authorized IT entity exceeds the blocking method that was set at the QoS policy of FMT_SMF.1.

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, A trusted remote IT product* 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].

Dependencies: No dependencies

Application notes: The TOE forms SSL protocol by invoking SSL function provided to IT environment, and therefore provides the trusted channel.

5.2 Additional Security Functional Requirements

The following components were added on this document, in addition to the Network Intrusion Prevention System PP history.

Security Functional Class	Security functional components
Identification and Authentication	FIA_UAU.4(Additional) Reuse prevention authentication mechanism

FIA_UAU.4) Reuse prevention authentication mechanism

Hierarchical to: No other components

FIA_UAU.4.1 The TSF shall prevent the reuse of authentication data that is related to the [Encrypted communication between the SNIPER server and SNIPER user through SSL, one-time password].

Dependencies: No dependencies

5.3 SNIPER 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 8] Assurance components

5.3.1 Configuration Management

1) ACM_AUT.1 Partial CM Automation

- Dependencies:

  - ACM_CAP.3 Authorization controls

- Developer action elements

  - ACM_AUT.1.1D The developer shall use a CM system.
  - ACM_AUT.1.2D The developer shall provide a CM plan.

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

2) ACM_CAP.4 Generation support and acceptance procedures

- Dependencies:

- ALC_DVS.1 Identification of security measures

- Developer action elements

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

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

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

- Content and presentation of evidence elements

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

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

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

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

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

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

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

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

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

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

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

- ACM_CAP.4.12C The CM system shall support the generation of the TOE.
- ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

• Evaluator action elements

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

3) ACM_SCP.2 Problem tracking CM coverage

• Dependencies:

- ACM_CAP.3 Authorization controls

• Developer action elements

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

• Content and presentation of evidence elements

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

• Evaluator action elements

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

5.3.2 Delivery and Operation

1) ADO_DEL.2 Detection of modification

• Dependencies:

- ACM_CAP.3 Authorization controls

• Developer action elements

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

• Content and presentation of evidence elements

- ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
- ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of 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.

5.3.3 Development

1) ADV_FSP.2 fully defined external interfaces

• Dependencies:

- ADV_RCR.1 Informal correspondence demonstration

• Developer action elements

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

• Content and presentation of evidence elements

- ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
- ADV_FSP.2.2C The functional specification shall be internally consistent.
- ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
- ADV_FSP.2.4C The functional specification shall completely represent the TSF.

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

• Evaluator action elements

- ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

2) ADV_HLD.2 Security enforcing high-level design

• Dependencies:

- ADV_FSP.1 Informal functional specification
- ADV_RCR.1 Informal correspondence demonstration

• Developer action elements

- ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

• Content and presentation of evidence elements

- ADV_HLD.2.1C The presentation of the high-level design shall be informal.
- ADV_HLD.2.2C The high-level design shall be internally consistent.
- ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
- ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.
- ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
- ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.
- ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
- ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
- ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

• Evaluator action elements

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

- ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

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

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

4) ADV_LLD.1 Descriptive low-level design

- Dependencies:
  - ADV_HLD.2 Security enforcing high-level design
  - ADV_RCR.1 Informal correspondence demonstration
- Developer action elements
  - ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.
- Content and presentation of evidence elements
  - ADV_LLD.1.1C The presentation of the low-level design shall be informal.
  - ADV_LLD.1.2C The low-level design shall be internally consistent.
  - ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.
  - ADV_LLD.1.4C The low-level design shall describe the purpose of each module.
  - ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.
  - ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.
  - ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the

TSF.

- ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
- ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.
- ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

• Evaluator action elements

- ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5) ADV_RCR.1 Informal correspondence demonstration

• Dependencies: No dependencies

• Developer action elements

- ADV_RCR1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

• Content and presentation of evidence elements

- ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

• Evaluator action elements

- ADV_RCR.1.1E The evaluator shall confirm that the information provided 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.

5.3.4 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 behavior 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 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 behavior 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.

5.3.5 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

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

5.3.6 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 high-level design

• Dependencies:

- ADV_HLD.2 Security enforcing high-level design
- ADV_LLD.1 Security enforcing high-level design
- ATE_FUN.1 Functional testing

• Developer action elements

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

• Content and presentation of evidence elements

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

• Evaluator action elements

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

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 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.

5.3.7 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 TOE Strength of TOE security function evaluation

• Dependencies:

- ADV_FSP.1 Informal functional specification

- ADV_HLD.1 Descriptive high-level design

• Developer action elements

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

• Content and presentation of evidence elements

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

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

• Evaluator action elements

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

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

3) AVA_VLA.2 Independent vulnerability analysis

• Dependencies:

- ADV_FSP.1 Informal functional specification

- ADV_HLD.2 Security enforcing high-level design

- ADV_IMP.1 Subset of the implementation of the TSF

- ADV_LLD.1 Descriptive low-level design

- AGD_ADM.1 Administrator guidance

- AGD_USR.1 User guidance

• Developer action elements

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

- AVA_VLA.2.2D The developer shall provide vulnerability analysis documentation.

• Content and presentation of evidence elements

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

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

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

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

• Evaluator action elements

- AVA_VLA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
- AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.
- AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.
- AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

5.4 IT Security requirement for the IT environment

The following is the security requirement for the IT environment:

5.4.1 Protection of the TSF

5.4.1.1 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 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.

5.4.1.2 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP. ITC.1.1 The TSF is logically distinguished from other communication channels between the TSF and trusted IT remote products. The TSF shall also provide an assured identification of the unit and communication channel that protects the channel data from any modification or exposure.

FTP_ITC.1.2 The TSF shall allow initializing communication through the trusted channel.

FTP_ITC.1.3 The TSF shall initialize communication through the trusted channel regarding [remote management function].

Dependencies: No dependencies

Application notes: The TOE forms SSL protocol by invoking SSL function provided to IT environment, and therefore provides trusted channel.

6. TOE Summary Specification

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

6.1. Security Functions

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

- Security Audit (WFAU)
- User Data Protection (WFDP)
- Identification and Authentication (WFIA)
- Security Management (WFMT)
- TSF Protection (WFPT)
- TOE Access (WFTA)

The strength of function (SOF) targeted by the TOE is SOF-medium. Required SOF when the threat agent is assumed to possess a moderate attack potential is defined SOF-medium.

6.1.1. Security Audit (WFAU)

The security audit performs the following functions:

- Audit data generation (WFAU_GEN)
- Audit data search and retrieval (WFAU_SAR)

6.1.1.1 Audit data generation (WFAU_GEN)

(1) Security Audit events gathering (WFAU_GEN_EVENT)

If the following security management related events occurred, an identifier for the subject and entity, event types and results, date and time of the events are stored at DB as audit lists.

- SNIPER start-up
- Continual attempts of exceeding authentication failure limits
- Failure of the authentication mechanism use
- Failure of the user identification mechanism use
- All modifications on TSF data value
- All modifications on limits on TSF data

- Modification of the user group
- Time modification according to the time synchronization
- Contents and results of the actions taken on the Integrity errors history and integrity errors
- Auto session locking function when the user is inactive for a certain period of time.
- All modifications on the security attribute
- Results on permitted policy

6.1.1.2 Audit data search and retrieval (WFAU_SAR)

(1) Audit review (WFAU_SAR_SAR)

If an administrator requires audit records, transmit audit records to the Client, make them viewable on the Client screen so that they may be sorted and searched by the event types, time, and results. Print them in report forms.

(2) Audit data (LOG) View (WFAU_SAR_LOG)

Convert the audit log generated at the gathered packet into a viewable format and view contents of the audit log stored at Log DB and that the administrator is viewing in realtime.

Make the security violation events audit data viewable on the Client screen so that they may be sorted and searched by the event types, time, and the results, and to accommodate administrator's analysis, provide a separate interface so that the data may be printed in the composition of picture and chart, graph, report forms.

6.1.1.3 SFR Mapping

TSF	SFR Mapping
Audit data generation (WFAU_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 (WFAU_SAR)	FAU_SAR.1 Audit review
	FAU_SAR.3 Selectable audit review
	FAU_SEL.1 Selective audit

6.1.2 User Data Protection (WFDP)

User Data Protection operates the following functions.

- Blocking function (WFDP_FFU)
- Blackhole blocking (WFDP_BLK)
- QoS blocking (WFDP_QOS)
- Intrusion detection function (WFDP_DET)
- Intrusion analyzing function (WFDP_ALS)

- Intrusion countermeasure (WFDP_ACT)

6.1.2.1 Blocking function (WFDP_FFU)

(1) Blocking function (WFDP_FFU_FFU)

SNIPER allows or denies the packet after comparing with the blocking policy.

SNIPER classifies into target and group, domain and registers and registers service to configure blocking and permitting policy.

Also each target configured at the firewall has security level of 1 to 10. 1 refers that the security level is high and 10 refers that the security level is low. According to the security level, a target with low security level cannot access to the target with high security level.

6.1.2.2 Blackhole blocking (WFDP_BLK)

(1) Blackhole blocking (WFDP_BLK_BLK)

Based on an each classified blocking method registered on the blackhole list, compare communication between the attacker and the protected system with the attacker IP, victim IP, protocol, or victim port whether it corresponds to each other. If it corresponds, block, otherwise permit.

Blocking history registers on the blackhole list is shown below.

-Session locking on a realtime monitoring: Session on a realtime monitoring is indicated as it classified into active and inactive session and the administrator may shut-down the connection. Sessions blocked at the realtime monitoring are registered on the Blackhole list, and there fore access denied for 60 seconds.

-Defense configuration of security violation events list:

According to the rule that was set to 'defense' at the security violation events list, targets are blocked for a certain period of limited time set by the administrator.

-History registered by the administrator on a Realtime blocking list:

May register IT entities that the administrator attempts to block at the realtime blocking list, and blocked for a certain period of limited time set by the administrator.

-Harmful information:

When designated to harmful information and set to 'block', it shall be blocked for a certain period of time set by the administrator.

-Restriction configuration of the internet use of the host management:

Block when the Internet use on a specific IT entity or network at the host management was set to restrict. Keep blocking until the administrator modifies to 'Accept'.

6.1.2.3 QoS blocking QoS (WFDP_QOS)

(1) QoS Blocking (WFDP_QOS_QOS)

QoS, a function that ensures or restricts the bandwidth of traffic, may set blocking methods on incoming traffics from the interface configured by the administrator by the network, protocol, and service. When it exceeds the configuration value, traffic is blocked.

6.1.2.4 Intrusion detection function (WFDP_DET)

(1) Intrusion detection target events information gathering (WFDP_DET_EVENT)

When security violation events occur on the protected system, in order to detect and block, collect information on the intrusion detection target events of an event via the protected system and the activity on the network of the user who used the system in advance, and therefore store identifier and information on the subject and entity, event type, date and time of the event to DB.

(2) Contract audit DB selection/contraction/modification (WFDP_DET_CON)

Reads contents of the packet stored in the packet memory and analyzes at each stage of Data link layer, Network layer, Transport layer, and Application layer, then selects security associated information, and therefore generates contract audit through contraction and modification.

(3) Stored audit log DB (WFDP_DET_DBSTG)

Stores the audit log generated at the gathered packet to DB.

(4) Stored security violation events information (WFDP_DET_INFOSTG)

When security violation attempts to attack the protected system, it compares the gathered data on a stored security violation events list with audit events of the intrusion detection system, and provides Client screen so as to inquire all intrusion detection results that are considered to be potential or attacking security violation.

Intrusion detection result is suitable for the authorized administrator to interpret information since it stores information of the attacker and victim server, type of attack, attack initiation time, attack termination time, security violation items, number of attempts, in addition to the information of the domain and attacker obtained from the external DNS server during the process of analyzing the packet. When it’s an internal user, by storing detail information (such as Mac Address of the LAN card etc.) on DB, also make it suitable for the authorized administrator to interpret information.

6.1.2.5 Intrusion Analyzing Function (WFDP_ALS)

(1) Intrusion Analysis (WFDP_ALS_POLDET)

SNIPER is consisted as an In-line mode on the network and compares all packets that attempt to pass through the SNIPER with Blackhole list. Authorized packets during this process are again compared with pattern Block according to protocol, victim port, and packet data. If the corresponding rules were found on the Pattern Block list and they were set to ‘Defense’, SNIPER discards those packets and registers on the BlackHole to defend for a registered time.

Analyzes IP of the accessed Packets, then at IP, TCP, UDP are analyzed, and at TCP, analyzes TCP

Services (telnet, ftp etc.) and then stores security violation items after comparing with contents of the security violation events list by each analyzing stage of Link, Network, Transport, Application Layer during the process of generating audit log.

Security violation events lists are shown below.

- DoS attack:

  An attack that prevents the victim server from providing a normal service by sending counterfeited or falsified packet. It lowers system performance by having it waste system resources (SPU, Memory etc.) and increase network traffic.

- Information gathering attack:

  An attack capable of probing information that includes server vulnerability, system vulnerability, network path, presence of firewall installation of the attack target, before the attacker attacks the specific server or system.

- Protocol vulnerability:

  An attack that exploits defects of the protocol regulation. It may create an overload on the network and system or prevent normal service by killing the server.

- Service attack:

  An attack that gains authority or operates commands through illegal access to a server. It accesses to a server using vulnerability of the various service and overflow bugs (occurs due to a software variable managing).

- Web CGI attack:

  An attack that gains authority or operates commands illegally by exploiting CGI (supported by the Web) Bug.

- Backdoor attack Backdoor:

  An attack that installs program on the target system on a malicious purpose. Using installed program, it destroys system or gain information.

- User definition attack: Administrators may register at discretion.

- Service Statistic analysis:

  Detects abnormal behavior or computer resource use. Analyzes traffic transition of each service port on the network, and by using this, detects abnormal symptoms on the network.

- Protocol statistic analysis:

  Detects abnormal behavior or computer resource use. Analyzes traffic transition of each protocol on the network, and by using this, detects abnormal symptoms on the network.

- IP Statistic analysis:

  Detects abnormal behavior or computer resource use. Analyzes traffic transition on a usual network, and by using this, detects abnormal symptoms on the network.

- Pattern Block:

  'Drop' harmful packets such as Worm virus or the One Way Attack detected at the Pattern Block, preventing harmful packets transmitting to the target system. Also by registering detected information and settings on the Black Hole list, blocks consecutive attacks effectively.

6.1.2.6 Intrusion Countermeasure (WFDP_ACT)

(1) Administrator report (WFDP_ACT_ALARM)
Reads security violation items on the memory and sends content message of the detected violation items to the administrator making alarm ring according to the levels of security violation items. Dispatch E-mail in a form designated at the configuration by each security violation item.

(2) Response regarding system protection (WFDP_ACT_KILL)
Response regarding security violation items verifies whether to block or not at the SNIPER configuration. If it indicates 'defense', block the connection, if it indicates 'detection', do not block the connection. When it indicates to block, control the access for a certain period of time by registering attacker's IP and Port on the Blackhole List.

(3) Interoperation between ESM and the control server (WFDP_ACT_LINK)
In response to the security violation events, it verifies whether ESM interlocks to the control server or not, and then transmits security violation events information to the interlocked ESM and control server.

For the security of transmitting data, SNIPER supports interoperation by using the trusted network communication and the encryption protocol that is supported by the each security product.

6.1.2.2 SFR Mapping

TSF	SFR Mapping
Firewall function (WFDP_FFU)	FDP_IFC.1 Subset information flow control FPT_RVM.1 Non-bypassability of the TSP FDP_IFF.1(1) Simple security attributes (1)
Blackhole blocking (WFDP_BLK)	FDP_IFC.1 Subset information flow control FDP_IFF.1(2) Simple security attributes (2) FPT_RVM.1 Non-bypassability of the TSP FTA_SSL.3 TSF-initiated termination
QoS blocking (WFDP_QOS)	FDP_IFC.1 Subset information flow control FDP_IFF.1(3) Simple security attributes (3)
Intrusion Detecting function (WFDP_DET)	FDP_IFC.1 Subset information flow control
Intrusion Analyzing function (WFDP_ALS)	FDP_IFC.1 Subset information flow control FDP_IFF.1(4) Simple security attributes (4)
Intrusion countermeasure (WFDP_ACT)	FDP_IFC.1 Subset information flow control

6.1.3 Identification and Authentication (WFIA)

Identification and authentication operates the following functions.

- User identification and authentication function (WFIA_ACCESS)

6.1.3.1 User identification and authentication function (WFIA_ACCESS)

(1) Identification and authentication (WFIA_ACCESS_LOGIN)

All users shall register an accessing IP address when registering the user ID so that if the administrator enters ID and Password at the designated IP Client screen, it is encrypted by SSL method and transmitted.

It prevents identification and authentication data from draining and being reused by encrypt communicating through SSL between SNIPER server and SNIPER user.

Transmitted encryption data reads/compares the identification and authentication information to DB at the SNIPER Server, and therefore identifies/authenticates the user.

Passwords shall be created with more than 6 or less than 10 letters including alphabets, numbers and special characters. It shall include at least 1 or more special characters. Also, passwords cannot be identical to IDs, and once password is used, it shall be used at least 10 or more times to be reused. It shall configure 1 to 99 days of validation time of the administrator’s password.

When an administrator enters his ID on a login screen, make it appear as “ID: *******” in order to protect password from draining.

Identification and authentication using disposable passwords generates different password every time it uses, and therefore prevents the access of unauthorized users.

When users attempt to log on, server issues the Challenge value that corresponds to n-1, and then the user enters the password that he remembers and sends the result obtained from applying hash function (SHA-1) for n-1 times to the server.

Server applies hash function 1 to the result transmitted by the user and if it corresponds to the stored value, authentication proceeds.

When authenticate, if the network administrator failed to Login within a certain count of the authentication attempts, count the number of attempts whether it exceeds the configured count. If it exceeds, print the error message and report to the user and administrator. User identification and authentication is strength of function (SOF) related security function. SOF-medium.

6.1.3.2 SFR Mapping

TSF	SFR Mapping
User identification and Authentication function (WFIA_ACCESS)	FAU_ARP.1 Security alarms FAU_SAA.1 Potential violation analysis FIA_AFL.1 Authentication failure handling FIA_UAU.1 Authentication FIA_UAU.4 Reuse prevention authentication mechanism FIA_UAU.7 Protected authentication feedback FIA_UID.2 User identification before any action FMT_MTD.1 Management of TSF data FPT_TST.1 TSF testing FTP_ITC.1 Inter-TSF trusted channel

6.1.4 Security management (WFMT)

Security management operates the following functions.

- Management of audit function (WFMT_AUDIT)
- OS Configuration (WFMT_CONFIG)
- Management of security violation events list (WFMT_POLDET)
- Management of blocking policy (WFMT_POLFW)
- Management of interoperation between ESM and control server regarding the security violation events (WFMT_ESM)
- Update (WFMT_UPD)
- QoS Policy (WFMT_POLQOS)

6.1.4.1 Management of audit function (WFMT_AUDIT)

(1) Management of audit function (WFMT_AUDIT_MAN)

Provides interface for the authorized network administrator in order to set up IPS mode, IDS mode, Firewall mode, QoS so as to operate harmful traffic detection and blocking through audit.

Configure audit mode whether to operate an audit function over SNIPER activation and shutdown, audit start-up and shutdown, access history, access failure etc...

(Status check)

Check integrity of the data that are necessary for starting up the SNIPER operation and provide interface so as to check the integrity according to the administrator’s request.

Indicates the system memory information and verifies SNIPER process that is currently running. When the process is abnormal, it reboots after storing audit records.

Check on the Client screen to examine whether the network driver of SNIPER IPS is activating normally. Provides state of packets transmitted from the each interface of NIC and that will be delivered.

(Management of the stored medium)

SNIPER provides interface to an authorized network administrator in order to configure the usage of audit data stored medium of the protected system.

(Backup and Repair)

SNIPER backup data files generated by SNIPER, using HDD or other devices in order to cope with file damage, safekeeping of the stored data, insuring capacity of the stored medium. And then ‘Restore’ the previously ‘Backup’ data to inquire.

Using the DB backup schedule, auto backup according to the cycle configured by the administrator.

(Time Synchronization)

Time modification of the SNIPER is only possible through the authorized administrator.

Information recorded on the SNIPER is recorded based on the SNIPER server time. If the SNIPER server time was not set correctly, information that SNIPER records cannot be trusted. Therefore, provides the time synchronization interface that configures the SNIPER Server time to GMT standard time.

6.1.4.2 OS Configuration (WFMT_CONFIG)

(1) OS Configuration (WFMT_CONFIG_OPERATION)

Administrators that are capable of security functions are classified into network administrator, security administrator, and system administrator.

Each administrator’s authority and roles are determined by the network administrator and it provides the interface over administrator configuration.

An authorized network administrator may define administrators that use SNIPER according to security roles. He may also operate registration, modification, and deletion of identification and authentication data.

Register administrator ID, password, the term of validity, authority, call reference, E-Mail Address, Clients (PC) IP address, and reference information.

Count the number of access attempts by configuring the number of access attempt limit. If it exceeds, print the warning screen, terminate the session, and block access for 30 seconds.

(Host management)

SNIPER may register, modify, and delete information of the examining target host. SNIPER generates data, based on configured host information and uses the data for operating. Configure MAC address, IP address, host name, internet use, routing functions.

(Log management)

SNIPER provides log management configuration, inquiry, and modification so as to leave administrators a detail history on a communication history between the user and the server regarding protocol and service that SNIPER handles.

(Management of harmful information blocking)

Harmful information blocking function is a function that blocks, modifies, and deletes harmful information. Harmful information blocking analyzes <Title></Title> Tag and URL at the audit log generation-TCP Session-Http session data.

Harmful information terms may be included in <Title></Title> Tag and harmful information site may be included in URL.

If set to 'block' by the administrator, SNIPER shutdowns the corresponding TCP session.

(Network management)

Configures internal IP, audit IP, audit exceptional IP. Inputs network IP Address, Net mask and therefore configures available address. Regarding the registered IP, SNIPER detects intrusion and handles IP related information.

Let the configured network verify whether to use DHCP, DNS, and therefore prevents intrusion detection errors due to IP SPOOFING.

If not configured separately, configure the IP bands installed with SNIPER as observing targets.

(Management of security audit countermeasure)

SNIPER provides the authorized administrator a function that sends stored medium check, login failure, integrity check, packet loss due to an excessive traffic, overload of CPU, NIC failure by mail.

(Session locking function of the Security Function)

An authorized network administrator may set time-out to enhance security of the account.

When the Client screen of SNIPER does not activate by the authorized administrator for a certain period of time, or when there are no inputs from the keyboard or mouse, SNIPER Client logs out automatically. Standard time is set to 30minutes.

(Environment variable)

Configures a screen for GUI. Configure Hide Login ID, SNIPER information title bar setting, risk level ICON setting, risk level string setting, OTP, Connection program setting, Display setting, Alarm setting.

6.1.4.3 Management of security violation events list (WFMT_POLDET)

(1) Management of security violation events list (WFMT_POLDET_MAN)

When SNIPER initiates the operation, it reads list files on the security violation events and manages in the memory. When modification on the security violation events list occurs, the content shall be maintained by storing at list file.

Type of security violation events that may be detected by the SNIPER is listed below.

- DoS attack
- Information gathering attack
- Protocol vulnerability
- Service attack
- Web CGI attack
- Backdoor attack
- User definition attack
- Statistic Analysis (Protocol, Service, IP)
- Pattern Block

Provides configurations of detection and detection policy, defense configuration function on each security violation event.

Each security violation event includes following attributes: Type of attack, Attack accepted time/ Attack accepted count, Blocking time, Filter, Detection, Defense, Exceptional IP, and Risk level. According to type of attack, one may define whether an attack occurred or not based on the attack accepted time/attack accepted count. Detects and defines aggression level of the abnormally overloading traffic and therefore blocks the detected IT entity for a blocking time.

6.1.4.4 Management of blocking policy (WFMT_POLFW)

(1) Management of blocking policy (WFMT_POLFW_MAN)

SNIPER shall configure whether to allow or block the policy, host needed for the policy setting, network, registration, modification and deletion of the group, and the registration, modification and deletion of service.

Entities configured at the firewall have security levels from 1 to 10. Security level of 1 represents high level of security while 10 represents the low level.

6.1.4.5 Management of interoperation between ESM and the control server regarding security violation events (WFMT_ESM)

(1) Interoperation setting between ESM and the control server (WFMT_ESM_LINK)

SNIPER provides the authorized network administrator a control center interface in order to send security violation events information to ESM and control server that operate to cope with the security violation events.

6.1.4.6 Update (WFMT_UPD)

(1) Update (WFMT_UPD_CON)

Authorized network administrators are provided with Live Update interfaces so as to renew the data. They may access to Update Server through the SNIPER Client receiving newly updated security violation events list and therefore, update on the SNIPER Server. By using scheduling function, authorized network administrator also provides the interface that enables SNIPER Server to access Update Server receiving newly updated security violation events list, and then updates on the SNIPER Server.

6.1.4.7 QoS Policy QoS (WFMT_POLQOS_QOS)

(1) QoS Policy QOS (WFMT_POLQOS_QOS)

SNIPER provides QoS policy setting interface that ensures or limits bandwidth of the traffic generated by a group of specific network.

6.1.4.8 SFR Mapping

TSF	SFR Mapping
Management of audit function (WFMT_AUDIT)	FAU_GEN.2 User Identity association FMT_MOF.1 Management of security functions behavior FMT_MTD.2(1) Management of limits on TSF data(1) FMT_SMF.1 Specification of management functions FPT_STM.1 Trusted Timestamp FRU_FLT.1 Degraded fault tolerance FMT_MTD.1(3) Management of TSF data(3)
OS Configuration (WFMT_CONFIG)	FAU_APR.1 Security alarms FAU_SEL.1 Selective audit FAU_SAA.1 Potential violation analysis FAU_STG.3 Action in case of possible audit data loss FIA_AFL.1 Authentication failure handling FIA_ATD.1 User attribute definition FMT_MTD.1(3) Management of TSF data (3) FMT_MTD.1(4) Management of TSF data (4) FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles FPT_SEP.1 TSF domain separation FPT_FLS.1 Failure with preservation of secure state FPT_TST.1 TSF testing FRU_FLT.1 Degraded fault tolerance FTA_SSL.1 TSF-initiated session locking FMT_MTD.2(2) Management of limits on TSF data (2)
Management of Security violation events list (WFMT_POLDET)	FMT_MSA.3 Static attribute initialization FMT_SMF.1 Specification of management functions FRU_FLT.1 Degraded fault tolerance FRU_RSA.1 Maximum quotas FMT_MTD.1(2) Management of TSF data (2)
Management of blocking function (WFMT_POLFW)	FMT_MSA.1 Management of security attributes FMT_SMF.1 Specification of management functions FMT_MTD.1(1) Management of TSF data (1)
Management of the interoperation function between ESM and the control server regarding security violation events (WFMT_ESM)	FMT_MTD.1(3) Management of TSF data (3) FMT_SMF.1 Specification of management functions FRU_FLT.1 Degraded fault tolerance
Update (WFMT_UPD)	FMT_MTD.1(3) Management of TSF data (3) FMT_SMF.1 Specification of management functions
QoS Policy (WFMT_POLQOS)	FMT_MTD.1(3) Management of TSF data (3) FMT_SMF.1 Specification of management functions

6.1.5 TSF Protection (WFPT)

The TSF protection operates the following functions.

- TSF stored data integrity check (WFPT_INTSTDATA)
- TSF transmitting data integrity check (WFPT_INTTRDATA)
- Prevention of audit data loss (WFPT_CHKDB)
- Abstract machine testing (WFPT_ATM)

6.1.5.1 TSF stored data integrity check (WFPT_INTSTDATA)

(1) TSF stored data integrity check (WFPT_INTSTDATA_INT)

TSF stored data integrity check is verified by identity of HMAC-SHA-1 encryption method and authority of file, owner, group, modified date.

Check integrity of the data that are necessary for starting up the SNIPER operation. Also check the standard network configuration information and provide interface so as to check the integrity according to the administrator's request. If integrity errors of the stored files were found, send warning mail and warning message to the administrator.

6.1.5.2 TSF transmitting data integrity check (WFPT_INTTRDATA)

(1) TSF transmitting data integrity check (WFPT_INTTRDATA_INT)

In order to assure the integrity and the confidentiality of the data transmitted from SNIPER server and Client communication, use SSL protocol.

Encrypt and transmit using SSL encryption method at the sending point where the data is being transmitted, decode using SSL encryption method at the receiving point, and therefore ensures integrity.

If integrity errors were found during the decoding process, drop transmitted data so as to not affect the security function, and prevent contents of the transmitting data from draining by using SSL encryption method.

6.1.5.3 Prevention of audit data loss (WFPT_CHKDB)

(1) Prevention of audit data loss (WFPT_CHKDB_PRE)

When reaches a critical value of the stored medium, it deletes the oldest Traffic Dump data, detail information on each service, in order to insure the capacity of stored medium. Also if the capacity is less than 100MB, it modifies firewall policy to DROP.

Check every 5 minute whether the usage for the audit data stored medium of the system under protection exceeds 90 % or 100MB of the usage limit set by an authorized administrator. If it exceeds 90% of the usage limit, warn administrator by sending messages or e-mails..

6.1.5.4 Abstract machine testing (WFPT_ATM)

(1) Abstract machine testing (WFPT_ATM_ATM)

SNIPER, when running, operates Integrity of executable files of process, Integrity of administrator's information file, Verification of the stored medium, Confirmation of license.

Periodically or when requested, the Abstract machine testing verifies normalcy of the process and NIC status. It reboots when the state of the process is abnormal.

6.1.5.5 IPS state information (WFPT_CHKSYS)

(1) IPS state information (WFPT_CHKSYS_INFO)

SNIPER, when the active master system causes hardware related problems, transfers traffic to the Slave system. An authorized administrator, as by configuring whether or not to use L7 HA, either synchronizes the state information table of SNIPER or verifies the port state, line state of NIC and the HA control state of SNIPER IPS.

6.1.5.6 SFR Mapping

TSF	SFR Mapping
TSF stored data integrity check (WFPT_INTSTDATA)	FAU_STG.1 Protected audit trail storage FMT_MTD.1 Management of TSF data FPT_TST.1 TSF testing
TSF transmitting data integrity check (WFPT_INTTRDATA)	FPT_TST.1 TSF testing
Prevention of audit data loss (WFPT_CHKDB)	FAU_STG.3 Action in case of possible audit data loss FAU_STG.4 Prevention of audit data loss
Abstract machine testing (WFPT_ATM)	FPT_AMT.1 Abstract machine testing
IPS state information (WFPT CHSYS)	FPT FLS.1 Failure with preservation of secure state FRU FLT.1 Degraded fault tolerance

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-9].

Assurance class	Assurance component		Assurance measures
Configuration management	ACM_AUT.1	Partial CM automation	Configuration Management Document_v1.2
	ACM_CAP.4	Generation support and acceptance procedures	
	ACM_SCP.2	Problem tracking CM coverage	
Delivery and operation	ADO_DEL.2	Detection of modification	Delivery Procedure_v1.2
	ADO_IGS.1	Installation, generation, and start-up procedures	Installation Manual_v1.1
Development	ADV_FSP.2	Fully defined external interfaces	Functional specification_v1.3
	ADV_HLD.2	Security enforcing high-level design	High-level Design_v1.5
	ADV_IMP.1	Subset of the implementation of the TSF	Validation Specification_v1.3
	ADV_LLD.1	Descriptive low-level design	Low-level Design_v1.3
	ADV_RCR.1	Informal correspondence demonstration	Functional specification_v1.3 High-level Design _v1.3 Validation Specification_v1.3 Low-level Design _v1.3 Tests _v1.2
	ADV_SPM.1	Informal TOE security policy model	Security Policy Modeling_v1.3
Guidance documents	AGD_ADM.1	Administrator guidance	Administrator Guidance_v1.3
	AGD_USR.1	User guidance	
Life cycle support	ALC_DVS.1	Identification of security measures	Life Cycle Support_v1.2
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.1	Well-defined development tools	
Tests	ATE_COV.2	Analysis of coverage	Testing_v1.2
	ATE_DPT.1	Testing: high-level design	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing – sample	
Vulnerability assessment	AVA_MSU.2	Validation of analysis	Misuse Analysis_v1.2
	AVA_SOF.1	Strength of TOE security function evaluation	Vulnerability Analysis_v1.1
	AVA_VLA.2	Independent vulnerability analysis	

[Table 9] Assurance measures

6.2.1 Configuration Management

- ACM_AUT.1 (Subset CM automation):

Assures by Configuration Management system automated by the subset CM automation for the TOE.

- ACM_CAP.4 (Generation support and Acceptance procedures):

The TOE is managed by Configuration Management system. Assured by CM document regarding CM procedures of the TOE and the CM system.

- ACM_SCP.2 (Problem tracking CM coverage):

Assures configuration items list of the TOE by configuration management document (configuration management log).

6.2.2 Delivery and Operation

- ADO_DEL.2 (Detection of modification):

Assures to provide delivery document on delivering the TOE or part of it.

- ADO_IGS.1 (Installation, Generation, Start-up procedures):

Assures by an installation quide regarding installations, generation, and start-up procedures.

6.2.3 Development

- ADV_FSP.2 (Fully defined external interfaces):

Function specification of the TOE is assured by the function specification document.

- ADV_HLD.2 (Security enforcing high-level design):

High-level design of the TOE is assured by the high-level design document.

- ADV_IMP.2 (Subset of the implementation of the TSF):

Implementation of the TOE security function is assured by the validation specification.

- ADV_LLD.1 (Descriptive low-level design):

Low-level design for the TOE security function is assured by the low-level design document.

- ADV_RCR.1 (Informal correspondence demonstration):

Correspondence between the TSF demonstrations is assured via function specification, high-level design, validation specification, low-level design, and tests.

- ADV_SPM.1 (Informal TOE security policy model):

Assures by the security policy model regarding the TSP model.

6.2.3 Guidance

- AGD_ADM.1 (Administrator guidance):

Administrator guidance for those who manage systems is assured by administrator guidance.

- AGD_USR.1 (User guidance):

Users that are capable of using TOE are trusted administrators and assured by administrator guidance.

6.2.4 Life Cycle Support

- ALC_DVS.1 (Security measure):

A security document, related to the TOE development, is assured by life-cycle support.

- ALC_LCD.1 (Developer defined life-cycle model):

Assures life-cycle model used for the TOE development and maintenance by life-cycle support.

- ALC_TAT.1 (Well-defined development tool):

A development tool used for the TOE development. Assured by the life cycle support.

6.2.5 Tests

- ATE_COV.2 (Analysis of coverage):

An analysis document regarding the coverage. Assured by the test paper.

- ATE_DPT.1 (Testing: high-level design):

An analysis document of a high-level design standard of the test. Assured by the test paper.

- ATE_FUN.1 (Functional testing):

A testing document of the TSF result. Assured by the test paper.

- ATE_IND.2 (Independent testing: sample):

Provides SNIPER IPS V5.0 for the TOE testing.

6.2.6 Vulnerability assessment

- AVA_MSU.2 (Validation of analysis):

Assures analysis of the guidance documents by the misuse analysis.

- AVA_SOF.1 (Strength of TOE security function evaluation):

An analysis document regarding the strength of TOE security function. Assured by the vulnerability analysis.

- AVA_VLA.2 (Independent vulnerability analysis):

A document that analyzes the vulnerability so as to not be exploited at the intended environment of the TOE. Assured by the vulnerability analysis document.

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

서식 있음: 글머리 기호 및 번호 매기기

The TOE satisfies all requirements as by referring to the following PP.

Registration number: PP-009

Title: Network Intrusion Prevention System PP.

Version: V1.1, Dec.21 2005

Assessment Assurance Level: EAL4

Assessment Standard: Information Protection System Common Criteria (The Ministry of Information and Communication 2005-25)

Information Protection System Common Criteria (The Ministry of Information and Communication 2005-25)

7.2 Protection Profile tailoring

서식 있음: 글머리 기호 및 번호 매기기

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

Functional Component	Name
FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User Identification association
FAU_SAA.1	Potential violation analysis
FAU_SAR.3	Selectable audit
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FDP_IFC.1(1)	Subset information flow control (1)
FDP_IFC.1(2)	Subset information flow control (2)
FDP_IFF.1(1)	Simple security attributes (1)
FDP_IFF.1(2)	Simple security attributes (2)
FDP_IFF.1(3)	Simple security attributes (3)
FDP_IFF.1(4)	Simple security attributes (4)
FIA_AFL.1	Authentication failure handling
FIA_ATD.1(1)	User attribute Definition (1)
FIA_ATD.1(2)	User attribute Definition (2)
FIA_UAU.1	Authentication

FIA_UAU.4	Reuse prevention authentication mechanism
FIA_UAU.7	Protected Authentication feedback
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Security attributes management
FMT_MSA.3	Static attribute initialization
FMT_MTD.1(1)	Management of TSF data (1)
FMT_MTD.1(2)	Management of TSF data (2)
FMT_MTD.1(3)	Management of TSF data (3)
FMT_MTD.1(4)	Management of TSF data (4)
FMT_MTD.2(1)	Management of limits on TSF data (1)
FMT_MTD.2(2)	Management of limits on TSF data (2)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ATM.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	Trusted Timestamp
FPT_TST.1	TSF testing
FRT_FLT.1	Degraded fault tolerance
FRT_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

서식 있음: 글머리 기호 및 번호 매기기

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. Secure TOE external server	Added to ST	
	A.TIME	Added to ST	
	A.TOE SSL Certificate	Added to ST	
Security policy	P.SSL Certificate management	Added to ST	Organizational security policy
Security objectives	OE.Secure TOE external server	Added to ST	TOE security objectives
	OE.TIME	Added to ST	
	OE.SSL Protocol	Added to ST	
Security functional Requirements	FIA_UAU.4 Reuse prevention authentication mechanism	Added to ST	Identification and Authentication

[Table 10] Additional security components

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, A.TOE SSL Certificate is added. Also OE.Secure TOE external server, OE.TIME, OE.SSL Protocol, P.SSL Certificate is added.

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.

.

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-11] shows the correlation of security environment and security objectives.

Security Objectives Security Environment	O. Availability	O. AUDIT	O. ADMINISTRATION	O. TSE DATA PROTECTION	O. ABNORMAL PACKETSCREENING	O. DOS ATTACK BLOCKING	O. IDENTIFICATION	O. AUTHENTICATION	O.IFORMATION FLOW CONTROL	OE. PHYSICAL SECURITY	OE.SECURITY MAINTENANCE	OE.TRUSTED ADMINISTRATOR	OE.SECURE ADMINISTRATION	OE. HARDENE DOS	OE. SINGLE CONNECTION POINT	OE. VULNERABILITY LIST UPDATE	OE.SECURE TOE EXTERNAL SERVER	OE.TIME	OE. SSL PROTOCOL
A. Physical Security										●			●						
A. Security Maintenance											●								
A. Trusted Administrator												●							
A. Hardened OS														●					
A. Single Connection point															●				
A. Secure TOE External server																	●		
A.TIME																		●	
A,TOE SSL Certificate																			●
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		●										●	●						
P.SSLCertificate management			●																●

[Table 11] security environment and security objectives

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 countermeasure the threats of T.Failure, T.Unauthorized TSF data modification, T.Bypassing, and T.Audit failure, which means 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.TSFdata 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 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.

10) OE SSL Protocol

The security objective for this environment is to ensure that the TOE builds up trusted channel by supporting trusted IT entity authentication and encryption communication function. Therefore, the security objective for this environment is necessary to assist assumptions of A.TOE SSL Certificate, P.SSL Certificate administration.

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.

Security Objectives SFR	O. AVAILABILITY	O. AUDIT	O. ADMINISTRATION	O. TSF DATA PROTECTION	O. ANORMAL 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_SEL.1 Selective audit		●							
FAU_STG.1 Protected audit trail storage		●							
FAU_STG.3 Action in case of possible audit data loss		●							
FAU_STG.4 Prevention of audit data loss		●							
FDP_IFC.1(1) Subset information flow control(1)									●
FDP_IFC.1(2) Subset information flow control(2)									●
FDP_IFF.1(1) Simple security attributes (1)					●				●
FDP_IFF.1(2) Simple security attributes (2)					●				●
FDP_IFF.1(3) Simple security attributes (3)					●				●
FDP_IFF.1(4) Simple security attributes (4)					●				●
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.4 Reuse prevention authentication mechanism							●	●	
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(1) Management of TSF data (1)			●	●					
FMT_MTD.1(2) Management of TSF data(2)			●	●					
FMT_MTD.1(3) Management of TSF data (3)			●	●					
FMT_MTD.1(4) Management of TSF data (4)			●	●					
FMT_MTD.2(1)TSF Management of limits on TSF data (1)	●		●						
FMT_MTD.2(2)TSF Management of limits on TSF data (2)	●		●						

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 12] Correlation of security objectives and security functional requirements

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 (1) Simple security attributes (1)

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

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

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

15) FDP_IFF.1 (3) Simple security attributes (3)

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

16) FDP_IFF.1 (4) Simple security attributes (4)

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

17) 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.

18) 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.Identifiction, and O.Information flow control.

19) 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.

20) 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, (Addition: This is because the TOE management and TSF Data protection function is possible only when administrator is authenticated.) and O.Authentication.

21) FIA_UAU.4 Reuse prevention authentication mechanism

As this component ensures the reuse prevention of authenticated data, it meets TOE security objectives: O.Identification, O.Authentication.

22) 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.

23) 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.

24) 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

25) 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.

26) 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.

27) 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.

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

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.

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

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.

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

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.

31) FMT_MTD.1 (4) Management of TSF data (4)

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.

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

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.

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

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.

34) 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.

35) 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.

36) 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.

37) 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.

38) FPT_RVM.1 TSP 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.

39) 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.

40) 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 audit events in the event of creating the audit history, it meets TOE security objective: O.Audit,O.Information gathering, O.Intrusion detection, O.Intrusion countermeasure.

41) 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: O.Availability, O.TSF data protection.

42) FRU_FLT.1 Degraded fault tolerance

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

43) 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.

44) 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.

45) 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.

46) FTP_ITC.1 Inter-TSF trusted channel

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

8.2.2 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).

8.2.3 Additional Security Requirements Rationale

Security Objectives **SFR**	**O. AVAILABILITY**	**O. AUDIT**	**O. ADMINISTRATION**	**O. TSF DATA PROTECTION**	**O. ANORMAL PACKET BLOCKING**	**O. DOS ATTACK BLOCKING**	**O. IDENTIFICATION**	**O. AUTHENTICATION**	**O. INFORMATION FLOW CONTROL**
FIA_UAU.4 Reuse Prevention authentication mechanism							●	●	

1) FIA_UAU.4 Reuse Prevention authentication mechanism

As this component ensures to prevent the reuse of the authenticated data, it meets TOE security objectives: O.Identification, O.Authentication.

8.3 Dependency Rationale

8.3.1 TOE Security Functional Requirements Dependencies

The following [Table-13] shows the dependencies among the functional components.

Number	Functional component	Dependency	Ref. No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	29
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 17
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.3	FAU_SAR.1	5
7	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	2 21
8	FAU_STG.1	FAU_GEN.1	2
9	FAU_STG.3	FAU_STG.1	8
10	FAU_STG.4	FAU_STG.1	8
11	FDP_IFC.1	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.4	-	-
17	FIA_UAU.7	FIA_UAU.1	15
18	FIA_UID.2	-	-
19	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	23 24
20	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	11 23 24
21	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	19 24
22	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	23 24
23	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	21 24
24	FMT_SMF.1	-	-
25	FMT_SMR.1	FIA_UID.1	17
26	FPT_AMT.1	-	-
27	FPT_FLS.1	ADV_SPM.1	Assurance Requirement
28	FPT_RVM.1	-	-
29	FPT_SEP.1	-	-
30	FPT_STM.1	-	-
31	FPT_TST.1	FPT_AMT.1	25
32	FRU_FLT.1	FPT_FLS.1	26
33	FRU_RSA.1	-	-
34	FTA_SSL.1	FIA_UAU.1	15
35	FTA_SSL.3	-	-
36	FTP_ITC.1	-	-

[Table 13] Functional components dependencies

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-14] shows the correlation between IT security functional requirements and TOE security functions.

TOE Security Functions	SFR
Security audit events gathering (WFAU_GEN_EVENT) Authentication and Identification (WFIA_ACCESS_LOGIN) OS Configuration (WFMT_CONFIG_OPERATION)	FAU_ARP.1 Security alarms
Security audit events gathering (WFAU_GEN_EVENT)	FAU_GEN.1 Audit data generation
Security audit events gathering (WFAU_GEN_EVENT) Management of the security audit function (WFMT_AUDIT_MAN)	FAU_GEN.2 User Identification association
Security events gathering (WFAU_GEN_EVENT) Authentication and Identification (WFIA_ACCESS_LOGIN) OS Configuration (WFMT_CONFIG_OPERATION)	FAU_SAA.1 Potential violation analysis
Audit review (WFAU_SAR_SAR) Audit log (Log)(WFAU_SAR_LOG)	FAU_SAR.1 Audit Examination
Audit review (WFAU_SAR_SAR) Audit log (Log)(WFAU_SAR_LOG)	FAU_SAR.3 Selectable Audit examination
Audit review (WFAU_SAR_SAR) Audit log (Log)(WFAU_SAR_LOG) OS Configuration (WFMT_CONFIG_OPERATION)	FAU_SEL.1 Selective Audit
TSF stored data integrity check (WFMT_INTSTDATA_INT)	FAU_STG.1 Protected audit trail storage
OS Configuration (WFMT_CONFIG_OPERATION) Prevention of audit data loss (WFPT_CHKDB_PRE)	FAU_STG.3 Action in case of possible audit data loss
Prevention of audit data loss (WFPT_CHKDB_PRE)	FAU_STG.4 Prevention of audit data loss
Firewall function WFDP_FFU_FFU) Blackhole blocking (WFDP_BLK_BLK) QoS blocking (WFDP_QOS_QOS) Intrusion detection target events information gathering (WFDP_DET_EVENT) Contract Audit DB selection/contraction/alteration (WFDP_DET_CON) Stored information of security violation events (WFDP_DET_INFOSTG) Intrusion analysis (WFDP_ALS_POLDET) Administrator alert (WFDP_ACT_ALARM) Actions taken for system protection (WFDP_ACT_KILL) Interoperation between ESM and the control server (WFDP_ACT_LINK)	FDP_IFC.1(1)Subset Information flow control (1)
Firewall function WFDP_FFU_FFU) Blackhole blocking (WFDP_BLK_BLK) QoS blocking (WFDP_QOS_QOS) Intrusion detection target events information gathering (WFDP_DET_EVENT) Contract Audit DB selection/contraction/alteration (WFDP_DET_CON) Stored information of security violation events (WFDP_DET_INFOSTG) Intrusion analysis (WFDP_ALS_POLDET) Administrator alert (WFDP_ACT_ALARM) Actions taken for system protection (WFDP_ACT_KILL) Interoperation between ESM and the control server (WFDP_ACT_LINK)	FDP_IFC.1(2) Subset Information flow control (2)

Firewall function WFDP_FFU_FFU)	FDP_IFF.1(1) Simple security Attributes (1)
Blackhole blocking (WFDP_BLK_BLK)	FDP_IFF.1(2) Simple security Attributes (2)
QoS blocking (WFDP_QOS_QOS)	FDP_IFF.1(3) Simple security Attributes (3)
Intrusion analysis (WFDP_ALS_POLDET)	FDP_IFF.1(4) Simple security Attributes (4)
Authentication and Identification (WFIA_ACCESS_LOGIN) OS Configuration (WFMT_CONFIG_OPERATION)	FIA_AFL.1 Authentication failure handling
OS Configuration (WFMT_CONFIG_OPERATION)	FIA_ATD.1(1) User attribute Definition (1)
OS Configuration (WFMT_CONFIG_OPERATION)	FIA_ATD.1(2) User attribute Definition (2)
Authentication and Identification (WFIA_ACCESS_LOGIN)	FIA_UAU.1 Timing of authentication
Authentication and Identification (WFIA_ACCESS_LOGIN)	FIA_UAU.4 Reuse prevention authentication mechanism
Authentication and Identification (WFIA_ACCESS_LOGIN)	FIA_UAU.7 Protected authentication feedback
Authentication and Identification (WFIA_ACCESS_LOGIN)	FIA_UID.2(1) User identification before any action(1)
Authentication and Identification (WFIA_ACCESS_LOGIN)	FIA_UID.2(2) User identification before any action (2)
Management of security audit functions (WFMT_AUDIT_MAN)	FMT_MOF.1 Management of security functions behaviors
Management of Firewall policy (WFMT_POLFW_MAN)	FMT_MSA.1 Security attributes management
Security violation events management (WFMT_POLDET_MAN)	FMT_MSA.3 Static attribute initialization
Management of Firewall policy (WFMT_POLFW_MAN)	FMT_MTD.1(1) Management of TSF data (1)
Security violation events management (WFMT_POLDET_MAN)	FMT_MTD.1(2) Management of TSF data (2)
Management of security audit functions (WFMT_AUDIT_MAN) OS Configuration (WFMT_CONFIG_OPERATION) Interlocking configuration between ESM and the control server (WFMT_ACT_LINK) Update (WFMT_UPD_CON) QoS Policy (WFMT_POLQOS_QOS) TSF stored data integrity check (WFMT_INTSTDATA_INT)	FMT_MTD.1(3) Management of TSF data (3)
OS Configuration (WFMT_CONFIG_OPERATION)	FMT_MTD.1(4) Management of TSF data (4)
Management of security audit functions (WFMT_AUDIT_MAN)	FMT_MTD.2(1) Management of limits on TSF data (1)
OS Configuration (WFMT_CONFIG_OPERATION)	FMT_MTD.2(2) Management of limits on TSF data (2)
Management of security audit functions (WFMT_AUDIT_MAN) OS Configuration (WFMT_CONFIG_OPERATION) Security violation events management (WFMT_POLDET_MAN) Management of Firewall policy (WFMT_POLFW_MAN) Interlocking configuration between ESM and the control server (WFMT_ESM_LINK) Update (WFMT_UPD_CON) QoS Policy(WFMT_POLQOS_QOS)	FMT_SMF.1 Specification of management functions
OS Configuration (WFMT_CONFIG_OPERATION)	FMT_SMR.1 Security roles
Abstract machine testing (WFPT_ATM_ATM)	FPT_AMT.1 Abstract machine testing

OS Configuration (WFMT_CONFIG_OPERATION) IPS state information(WFPT_CHKSYS_INFO)	FPT_FLS.1 Failure with preservation of secure state
Firewall function (WFDP_FFU_FFU) Blackhole blocking (WFDP_BLK_BLK)	FPT_RVM.1 Non-bypassability of the TSP
OS Configuration (WFMT_CONFIG_OPERATION)	FPT_SEP.1 TSF domain Separation
Management of security audit functions (WFMT_AUDIT_MAN)	FPT_STM.1 Reliable Timestamp
Authentication and Identification (WFIA_ACCESS_LOGIN) OS Configuration (WFMT_CONFIG_OPERATION) TSF stored data integrity check (WFPT_INTSTDATA_INT) TSF transmitting data integrity check (WFPT_INTTRDATA_INT)	FPT_TST.1 TSF testing
Management of security audit functions (WFMT_AUDIT_MAN) OS Configuration (WFMT_CONFIG_OPERATION) Security violation events management (WFMT_POLDET_MAN) Interlocking configuration between ESM and the control server (WFMT_ESM_LINK) IPS state information(WFPT_CHKSYS_INFO)	FRU_FLT.1 Degraded fault tolerance
Management of security violation events List (WFMT_POLDET_MAN)	FRU_RSA.1 Maximum quotas
Operation Configuration (WFMT_CONFIG_OPERATION)	FTA_SSL.1 TSF-initiated session locking
Blackhole blocking (WFMT_BLK_BLK)	FTA_SSL.3 RSF-initiated termination
Authentication and Identification (WFIA_ACCESS_LOGIN)	FTP_ITC.1 Inter-TSF trusted channel

[Table 14] Correlations of security functional requirements and TOE security functions

8.4.2 TOE Summary Specification Rationale

This rationale demonstrates the following.

• Each security functional requirement is addressed by at least one TOE summary specification.

1) Audit data generation

When the security management related events occur, as the TOE ensures to generate audit data by subject and entity for the identifier, event type and result, date and time of events, it corresponds to FAU_GEN.1.

2) Audit data inquiry

As the TOE ensures to inquire Audit records through the GUI, it corresponds to FAU_SAR.1 and FAU_SAR.3.

3) User identification and authentication function

As it ensures to authenticate and identify whether he/she is a proper user to access and handle when it has failed to authenticate and identify, it corresponds to FAU_ARP.1, FAU_SAA.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.2, FPT_TST.1 FTP_ITC.1. As identification and authentication data, internally transferred data of the TOE is encoded to SSL ensuring trusted communication channels; it corresponds to FMT_MTD.1, FPT_TST.1, and FTP_ITC.1

4) Management of security audit functions

As it ensures to manage the security audit functions that include start-up and termination audit of the

TOE, audit start-up and termination audit, access history management, access failure management, it corresponds to FMT_MOF.1, FMT_SMF.1. Also, as information on the TOE is recorded by the standards of the TOE time and as it ensures the function that unifies the TOE time and GMT time, it corresponds to FMT_MTD.1 (3), FPT_STM.1.

As the TOE ensures to provide the back-up and repair function to cope with file damage, safekeeping of the stored medium usage setting and stored data, it corresponds to FMT_MTD.2(1).

When operating TOE, as it ensures integrity check configuration of the files that are essential for execution, it corresponds to FMT_MTD.1 (3). As it correlates audit subject events and the user identification that caused the events, it corresponds to FAU_GEN.2.

As it ensures the fault tolerance in case of the TOE failure, it corresponds to FRU_FLT.1

5) OS Configuration

As it ensures the configuration, inquiry by classifying roles of administrator who is capable of operating security functions of the TOE, it corresponds to FIA_ATD.1, FMT_MTD.1 (3), FMT_MTD.1 (4), and FMT_SMR.1 by the configuration of the number of access attempts limit.

As the TOE ensures to configure the information regarding the observing victim host, it corresponds to FMT_MTD.1 (3).

As the TOE ensures to provide log management setting and inquiry, alteration functions, in order to report the administrator a specified history of the user and server on protocol and service that the TOE handles, it corresponds to FMT_MTD.1(3).

If it was considered to be a harmful information after comparing words appointed as harmful information with harmful information site, since it ensures to provide configuration, modification, deletion functions in order to block TCP session, it corresponds to FMT_MTD.1(3).

As the TOE configures available internal network Address, and as the SNIPER detects intrusions over registered IP and ensures to handle the information related to IP, it corresponds to FAU_SEL.1, FMT_MTD.1, FPT_SEP.1

As the TOE ensures to provide the authorized administrator a function that transmits the verification of the stored medium, Login failure, Integrity check, packet loss due to an excessive traffic, overload state of the CPU, failure state of the NIC by mail, it corresponds to FAU_ARP.1, FAU_SAA.1, FAU_STG.3, FIA_AFL.1, FPT_TST.1, FPT_FLS.1, FRU_FLT.1, FMT_SMF.1.

As the TOE ensures to operate the session locking function of the security function, it corresponds to FTA_SSL.1.

6) Management of the security violation events list

As the TOE ensures to configure and manage detectable security violation events list, it corresponds to FMT_MSA.3, FRU_RSA.1, FMT_SMF.1, FMT_MTD.1 (2).

7) Management of Firewall policy

As the TOE ensures to configure and manage the firewall policy, it corresponds to FMT_MSA.1, FMT_SMF.1, FMT_MTD.1 (1).

8) Management of interoperation between ESM and the control server regarding the security violation

events

As the TOE ensures to provide control center interface to the authorized network administrator in order to transfer security violation events information to the control server and ESM which operates as it responses to the security violation events, it corresponds to FMT_MTD.1 (3).

As it transfers system log to the administrator in case of OS failure, it corresponds to FRU_FLT.1, FMT_SMF.1.

9) Update

As it ensures to provide the function to maintain the latest type of the TOE, it corresponds to FMT_MTD.1 (3), FMT_SMF.1.

10) QoS Policy

As it ensures to provide QoS Policy configuration function of the TOE, it corresponds to FMT_MTD.1 (3), FMT_SMF.1.

11) TSF stored data integrity check

As the TOE ensures integrity of the stored files, it corresponds to FAU_STG.1, FPT_TST.1, FMT_MTD.1 (3).

12) TSF transmitting data integrity check

As the TOE ensures integrity of the transmitting data, it corresponds to FPT_TST.1.

13) Prevention of audit data loss

As the TOE ensures to operate counter actions when it forecasts audit data loss, it corresponds to FAU_STG.3, FAU_STG.4

14) Abstract machine testing

As the OS itself, when operates, ensures to proceed tests on memory inspection, normalcy of the file system, Daemon verification, module test, it corresponds to FPT_AMT.1.

15) IPS state information (HA)

As it ensures to check NIC port state and line state of the IPS, HA configuration, it corresponds to FPT_FLS.1, FRU_FLT.1

16) Firewall function

As the TOE ensures whether to allow or deny packet after comparing with the firewall policy, it corresponds to FPT_RVM.1, FDP_IFC.1, FDP_IFF.1

17) Blackhole blocking

As the TOE ensures to block in accordance to block method for each rule that are registered on the blackhole list, it corresponds to FTA_SSL.3, FPT_RVM.1, FDP_IFC.1 FDP_IFF.1

18) Pattern block blocking

As the TOE ensures to block after comparing with pattern block and security violation events list, it corresponds to FDP_IFC.1.

19) QoS Function

As the TOE ensures to block according to the blocking method registered on the QoS Policy list, it corresponds to FDP_IFC.1.

8.4.3 Correlations of Assurance Requirements and Assurance Measures

The assurance measures for each assurance component are listed in the [Table 15].

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	
	ACM_SCP.2	Problem tracking CM coverage	
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	Functional specification High-level Design Validation Specification Low-level Design Testing
	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	
	ALC_TAT.1	Well-defined development tools	
Tests	ATE_COV.2	Analysis of coverage	Testing
	ATE_DPT.1	Testing: high-level design	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing – sample	
Vulnerability assessment	AVA_MSU.2	Validation of analysis	Misuse Analysis
	AVA_SOF.1	Strength of TOE security function evaluation	Vulnerability Analysis
	AVA_VLA.2	Independent vulnerability Analysis	

[Table 15] Assurance measures

- ACM_AUT.1 Partial configuration management automation
  - The TOE provides Configuration Management document on configuration managing.

- ACM_CAP.4 Generation support and acceptance procedures

  - The TOE provides Configuration Management document on configuration managing.
- ACM_SCP.2 Problem tracking CM coverage

  - The TOE provides Configuration Management document on configuration managing.
- ADO_DEL.2 Detection of modification

  - The TOE provides distribution document to guarantee system controls and distribution facilities, procedures to assure that the receiver has received the TOE sent by the sender with its figure remaining intact.
- ADO_IGS.1 installation, generation, and operation procedures

  - The TOE, in order to assure that it is being installed, generated, started on a secure manner as the developer intended, provides Installation quidance.
- ADV_FSP.2 Fully defined external interface

  - The TOE provides a functional specification on functional specification that describes the TSF.
- ADV_HLD.2– high-level design

  -The TOE provides a high-level design document of which the TSF functional specification is specified.
- ADV_IMP.1- the implementation of the TSF specification

  - The TOE provides validation specification, the most concrete description of the TSF.
- ADV_LLD.1 Descriptive low-level design,

  - The TOE provides descriptive low-level design document that is descriptive low-level design of the high-level design.
- ADV_RCR.1- correspondence of expression

  - Correspondence of expression is included in functional and high-level design, high-level and descriptive low-level design, validation specification, and test paper.
- ADV_SPM.1 – Informal TOE security policy model

  -A TSP model. Provides a security policy modeling.
- AGD_ADM.1– Administrator guidance

  - Provides administrator guidance, a guidance document for the TOE.
- AGD_USR.1– User guidance

  - As administrators, users of the TOE provide administrator guidance.
- ALC_DVS.1– Identification of security measures

  - Provides life-cycle support documents to physical, procedural, personal, and other security means of the TOE development environment.
- ALC_LCD.1- Developer defined life cycle model

  –Provides life-cycle support document.
- ALC_TAT.1- Well-defined development tools

  - Provides life-cycle support documents to tools used for developing, analyzing, implementing the TOE.
- ATE_COV.2- Analysis of coverage

  - Provides test papers regarding test requirements that prove the TSF satisfies security function requirements of TOE.

- ATE_DPT.1- Testing: high-level design
  - Provides test papers for the high-level design test of the TOE
- ATE_FUN.1- Functional testing
  - Provides test papers for the functional testing of the TOE.
- ATE_IND.2 - Independent testing - sample
  - Provides testing tools for an independent testing of the TOE.
- AVA_MSU.2 – Guidance analysis
  - Provides at the misuse analysis. .
- AVA_SOF.1 - Strength of TOE security function evaluation
  - Provides vulnerability analysis regarding the Strength of TOE security function.
- AVA_VLA.2 - Independent vulnerability analysis
  - Provides vulnerability analysis regarding the vulnerability of the TOE.

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
	A.TOE SSL Certificate	Addition
Security Objectives for the environment	OE. Secure TOE external server	Addition
	OE.TIME	Addition
	OE.SSL Protocol	Addition

Requirements of the Network Intrusion Prevention System PP are all included in this document (ST). A. Secure TOE external server, A.TIME, A.TOE SSL Certificate, OE.Secure TOE external server, and OE.TIME, OE.SSL protocol 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.

IT security function, a user identification and authentication function, maps with FIA_UAU.1, FIA_UAU.4, FIA_UAU.7 of the TSF, providing authentication methods that utilize password and disposable password.

Security Functional Class	Security Functional Component	
Identification and Authentication	FIA_UAU.1	Authentication
	FIA_UAU.4	Reuse prevention authentication mechanism
	FIA_UAU.7	Protected authentication feedback
TSF Protection	FPT_TST.1	TSF testing

[Table 16] Strength of function related security function and security functional requirements

CEM. According to Table A.3, calculations regarding the potential attack may be done as shown below. SNIPER assumes that the threat agent possesses moderate expertise, resources, and motivation.

Elapsed time for exploiting SNIPER is “>1 month” → Exploiting value is 8
Expertise is “Expert” → Exploiting value is 2.
Knowledge of TOE is “None” → Exploiting value is 0.
Access to TOE is “1 month” → Exploiting value is 9.
Equipment is “Standard” → Exploiting value is 2.

Elapsed time for identifying SNIPER is “<0.5 hour” → Identifying value is 0.
Expertise is “Layman” → Identifying value is 0.
Knowledge of TOE is “None” → Identifying value is 0.
Access to TOE is “<0.5 hour, or access undetectable” → Identifying value is 0.
Equipment is “None” → Identifying value is 0.

The total sum (Exploiting value 21 + Identifying value 0) is therefore 21.

According to CEM A.8, and since the rating of vulnerabilities of SNIPER falls into a range of 18-24, it satisfies SOF-medium.

Since the hash algorithm SHA-1 of “FPT_TST.1 self testing” function has small possibility for the low level attacker to generate identical hash value, it satisfies SOF-medium.

SNIPER proceeds integrity inspection on implementing files and configuration files in TSC. The TSF is being operated until it verifies the security. To operate integrity inspection, hash value of the implementing files and configuration files is generated at the initial start-up and renewed at every start-up and request from the administrator.. SHA-1 hash algorithm is used as an integrity algorithm for generating hash value.

SNIPER assumes that the threat agent possesses moderate expertise, resources, and motivation.

Elapsed time for exploiting SNIPER is “>1 month” → Exploiting value is 8

Expertise is “Expert” → Exploiting value is 2.

Knowledge of TOE is “None” → Exploiting value is 0.

Access to TOE is “1 month” → Exploiting value is 9.

Equipment is “Standard” → Exploiting value is 2.

Elapsed time for identifying SNIPER is “<0.5 hour” → Identifying value is 0.

Expertise is “Layman” → Identifying value is 0.

Knowledge of TOE is “None” → Identifying value is 0.

Access to TOE is “<0.5 hour, or access undetectable” → Identifying value is 0.

Equipment is “None” → Identifying value is 0.

The total sum (Exploiting value 21 + Identifying value 0) is therefore 21.

According to CEM A.8, and since the rating of vulnerabilities of SNIPER falls into a range of 18-24, it satisfies SOF-medium.