SNIPER IPS-G V8.0

Security Target

Version 1.07

2013-06-03

WINS Technet Co., Ltd.

Summary

This document is a security target of Network Intrusion Prevention System (TOE: SNIPER IPS-G V8.0, Product Version: V8.0 2011.07.01R, Product Name: SNIPER IPS 10G)

Revision History

Version	Date	Revised Reason
Version 1.00	2011-12-08	First Document was enrolled.
Version 1.01	2012-05-30	Observation Report V1.00 Reflected -6.1.1 FAU_GEN.1.1: Audit target description based on the minimum audit level was added. -6.1.3 FIA_ATD.1.1: Objective and operation description based on operation functions of each administrator was added. -6.1.4 FMT_MOF.1.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MTD.1(1): Administrator's operation authority description on security policy and security functions was added.
Version 1.02	2012-06-20	Observation Report V1.10 Reflected -Description about Subject, Objective, Security Properties, and Operation used in SFR was added. - SFR and related content on 7. TOE Specification was added.
Version 1.03	2012-07-20	Observation Report V1.20 Reflected - Security properties description of subject and object that were used on SFR was supplemented. Certification authority requirements reflected
Version 1.04	2012-12-18	Certification authority requirements reflected - TOE Identifier changed - TOE Scope on 1.4 TOE Overview and 1.5 TOE Description were modified - 6.1.8 Cryptographic Support related SFR was added
Version 1.05	2013-01-15	TOE Client Build Version changed
Version 1.06	2013-03-06	Certification authority requirements reflected - 6.1.8 Cryptographic Support related SFR description was supplemented
Version 1.07	2013-06-03	Certification authority requirements reflected - 6.1.7 TOE Access related SFR was deleted

Table of Contents

1. SECURITY TARGET INTRODUCTION 5

1.1 REFERENCE FOR SECURITY TARGET 5
1.2 OVERVIEW FOR SECURITY TARGET 6
1.3 TOE REFERENCES 7
1.4 TOE OVERVIEW 7
1.4.1 Usage and Major Security Features of the TOE 7
1.4.2 TOE Type 8
1.4.3 None-TOE Hardware and Software for TOE Operation 11
1.5 TOE DESCRIPTION 12
1.5.1 Physical Scope 12
1.5.2 Logical Scope 15
1.6 TERMS AND DEFINITIONS 17
1.7 CONVENTIONS 21
1.8 REFERENCES 21

2. CONFORMANCE CLAIMS 23

2.1 CC CONFORMANCE 23
2.2 PP CONFORMANCE 23
2.3 PACKAGE CONFORMANCE 23
2.4 CONFORMANCE CLAIM RATIONALE 23

3. SECURITY PROBLEM DEFINITION 24

3.1 THREAT 24
3.2 SECURITY POLICY OF ORGANIZATION 25
3.3 ASSUMPTIONS OF TOE OPERATIONAL ENVIRONMENT 25

4. SECURITY OBJECTIVES 27

4.1 TOE SECURITY OBJECTIVE 27
4.2 SECURITY OBJECTIVE FOR THE OPERATIONAL ENVIRONMENT 28
4.3 SECURITY OBJECTIVES RATIONALE 29
4.3.1 TOE Security Objectives Rationale 30
4.3.2 Security Objectives Rationale of the Operational Environment 32

5. EXTENDED COMPONENTS DEFINITION 34

6. SECURITY REQUIREMENTS 35

6.1 SECURITY FUNCTIONAL REQUIREMENTS 35

6.1.1 Security Audit *38*
6.1.2 User Data Protection *41*
6.1.3 Identification and Authentication *43*
6.1.4 Security Management *46*
6.1.5 Protection of the TSF *51*
6.1.6 Resource Allocation *52*
6.1.7 TOE Access *52*
6.1.8 Cryptographic Support *52*
6.2 TOE SECURITY ASSURANCE COMPONENTS 54
6.2.1 Development *54*
6.2.2 Guidance Documents *57*
6.2.3 Life-Cycle Support *58*
6.2.4 Security Target Evaluation *61*
6.2.5 Tests *66*
6.2.6 Vulnerability Assessment *68*
6.3 SECURITY REQUIREMENTS RATIONALE 70
6.3.1 TOE Security Functional Requirements Rationale *71*
6.3.2 TOE Assurance Requirements Rationale *75*
6.4 DEPENDENCY RATIONALE 77
6.4.1 Security Functional Requirements Dependencies *77*
6.4.2 Assurance Required Components Dependencies *78*

7. TOE SUMMERY SPECIFICATION 79

7.1. SECURITY FUNCTION 79
7.1.1. Security Audit (WFAU) *79*
7.1.2 User Data Protection (WFDP) *82*
7.1.3 Identification and Authentication (WFIA) *87*
7.1.4 Security Management (WFMT) *89*
7.1.5 TSF Protection (WFPT) *98*
7.2 SECURITY FUNCTION RATIONALE 101

1. Security Target Introduction

This is a Security Target of Network Intrusion Prevention System (TOE: SNIPER IPS-G V8.0). It defines security function and security method and describes security requirements for evaluation grounds and general information such as designation process and technical information.

1.1 Reference for Security Target

Security Target Title	SNIPER IPS-G V8.0 Security Target
Security Target Version	Version 1.06
Security Target Written Date	Mar 6, 2013
Security Target Written by	WINS Technet Co., Ltd.
Common Criteria Standard	Common Criteria for Information Technology Security Evaluation (Public Administration and Security notification No. 2009-52) CC V3.1r3(Common Criteria for Information Technology Security Evaluation)
Evaluation Assurance Level	EAL4
Accepted Protection Profile	N/A
Tag	SNIPER IPS, Network based intrusion detection, intrusion analysis, intrusion response, intrusion prevention system, information flow control, IPv4, IPv6

1.2 Overview for Security Target

TOE is the Intrusion Prevention System (IPS : Intrusion Protection System), which is installed on the linkage location between external and internal network with in-line form, detects and prevents the real-time IPv4/IPv6 network traffic intrusion or attack from the external and internal network. It provides intrusion detection function that the user gathers, analyzes, and responses the information, which is generated by interworking with protected audit, intrusion prevent function that blocks malicious packet, security management function, user identification for who tries to access to TOE, certification function, and audit function that make audit record for user's activities within TOE.

In this security target, security target introduction, conformance claims, security problem definition, security objectives, security requirements, TOE summery specification, accepted protection profile, and theoretical basis are described.

1) In TOE Description, general information about physical and theoretical scope of TOE is described.

2) In Security Problem Definition, the assumption of the circumstance where TOE is applied or will be applied, the threats that the source intentionally or accidentally makes unjustified vulnerability uses, and security policy such as rules, processes, practices, or guidelines that forced by organization and TOE must follows are described.

3) In Security Objectives, TOE security objectives for corresponding threats, satisfying assumption or organization's policy, or operational circumstances are described.

4) In Security Requirements, security function requirements for satisfying the security objectives are described.

5) In TOE Summery Specifications, TOE security function that satisfies identified security functional requirement is described.

1.3 TOE References

Product Name		SNIPER IPS 10G
TOE Identification		SNIPER IPS-G V8.0
TOE Version		V8.0 2011.07.01R
Version Information	Product Version	V8.0
	Distributed Version	2011.07.01R
Developer		WINS Technet Co., Ltd.

1.4 TOE Overview

It describes usage and major security features of the TOE, product type and scope, and identifies none-TOE hardware/software/firmware that is required on TOE.

1.4.1 Usage and Major Security Features of the TOE

TOE is SNIPER IPS-G V8.0 (called "SNIPER IPS") that WINS Technet Co., Ltd. developed. TOE is network based intrusion prevention system that safely secures protected network assets and primarily detects and blocks intrusion from the external network.

TOE is supplied on hardware integrated product, and uses the OS (called "SNIPER OS V2.0 (Kernel 2.6.37)") that upgrades internal kernel version that is applied on Fedora 14, which is provided by Fedora, with Kernel 2.6.37, which is provided by kernel.org, eliminates unnecessary service, and adds necessary configurations for TOE.

TOE is installed on entrance of security target network with In-line form so that all the traffic inflows to security target network cannot bypass the TOE, and only-one or mixed installation for IPv4 address system network and IPv6 address system network.

TOE provides intrusion detection function against network attacks, intrusion response function against detected attack, security management function, user identification and certification function, audit function that records user activities within TOE, various statistics and reports providing, and update function.

Major features of TOE are:

- Behavior based intrusion detection function and signature based intrusion detection function

TOE multiply applies behavior based intrusion detection function and signature based intrusion detection function, so it can detect and prevent the typical Denial of Service attack such as TCP flooding with Syn, Ack, Fin, Push, or UDP flooding, or DoS attack with web based HTTP Get, Post Flood, or Half-Open Flood attacks

- L3, L5~L7 fragmentation attack detection and prevention

TOE performs Reassemble and Normalization process on gathered packets, and it performs detection and prevention function on L3, L5~L7 fragmentation attack headed to security target assets with those processes.

- Real-time network traffic inquiry and management

It provides normal or anomaly traffic blocking status, real-time attack detection status, and effective inquiry function for real-time attack blocking event by real-time network traffic monitoring, major target server traffic concentrated management function, and simultaneous monitoring function with independent window realization of each function based.

- IPv4 / IPv6 network analysis and detection/prevention

TOE is installed on the IPv6 system network, which is alternative system for currently exhausting IPv4 system, and detects/prevents the threat agents that inflow to security target network. TOE configurations are available for both IPv4 and IPv6, and the functions such as detection/prevention, or audit records are classified into each address system.

1.4.2 TOE Type

TOE is the intrusion detection system that performs effective defense the attacks using anomaly or normal traffic by analyzing traffic that inflow from external network.

TOE is composed of SNIPER IPS-G V8.0 Server (called “IPS Server”) and SNIPER IPS-G V8.0 Client (called “IPS Client”). And also, 3rd products that are built with TOE such as OpenSSL, SNIPER Crypto, TeeChart, Fast Report, and SNIPER OS V2.0 that includes SQLite V3 are also included in TOE.

- IPS Server: It performs intrusion prevention function and analysis function from the external threat agent by packet gathering, security audit function, user data protection function, identification and certification function, and TSF protection function.

- IPS Client: Graphical User Interface (GUI) that the administrator uses to operate management function. It sends the requests from the administrator to IPS Server.

For the safe communication between IPS Server and IPS Client, TOE uses OpenSSL v1.0.1c, and downloads the data through the Update Server, which is installed on WINS Technet Co., Ltd., to update the latest intrusion pattern. Communication between TOE and Update Server is operated safely with SSL protocol.

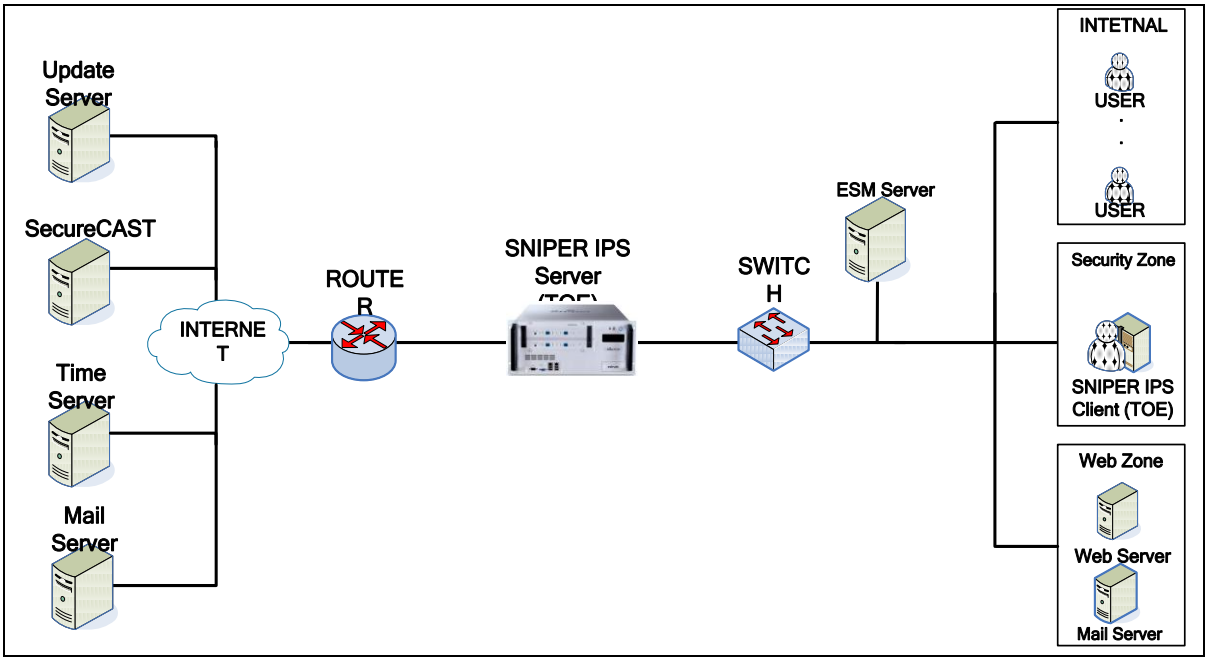
TOE maintain trustful Time Stamp, TOE performs time synchronization with time server on IPS Client, and synchronize this time stamp with IPS server. It uses NTP(Network Time Protocol, for example:

time.ntp.kornet.net) for communication with time server.

IPS server should be located in physically safe environment, only the trusted administrator is enable to access, and the administrator must access and perform the security management through the permitted IP that is configured when the administrator installed it, and access authority can be classified into two types – Super-administrator and general-administrator.

Since TOE must analyze and detect whole traffic inflows from the external network to security target network regarding to the rule set by the administrator, TOE should be installed on the above layer with In-line form so that whole traffic inflows to the security target network passes TOE.
At this moment, firewall for the security target network should be installed between TOE and security target network.

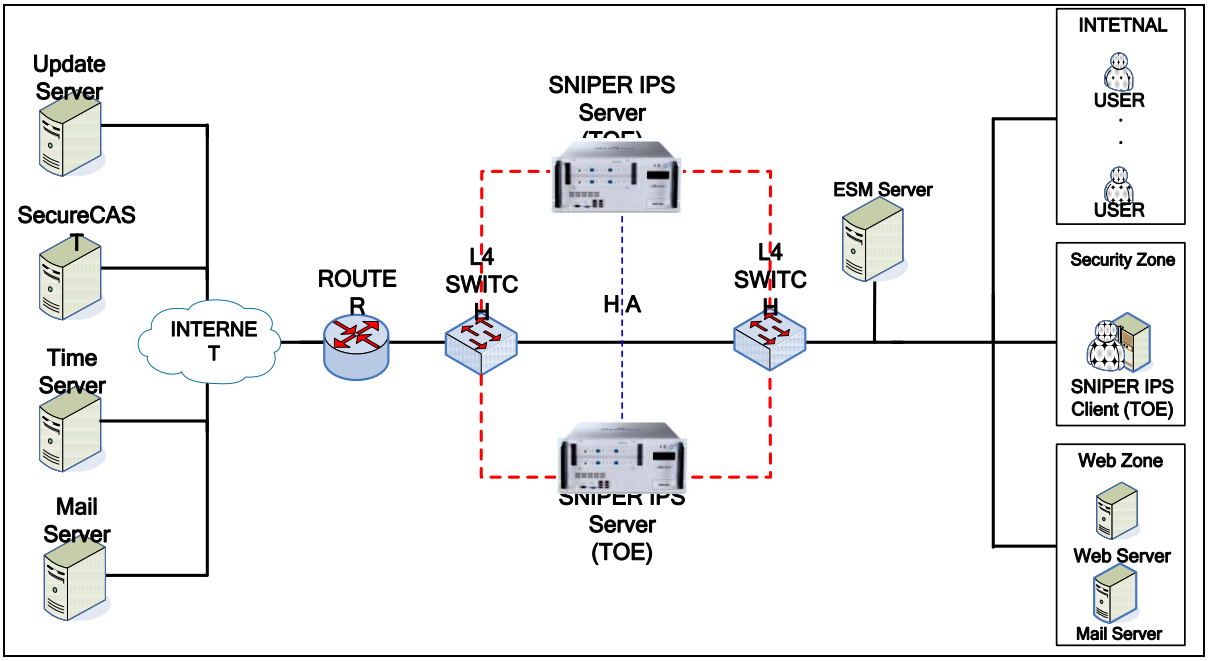
This is an example of single configuration with one TOE to protect the security target network.



[Figure-1] TOE Single Configuration

The administrator access to IPS server and performs security management through IPS client. IPS server and IPS client should use the same network bandwidth.

This is a HA (High Availability) duplex configuration with two TOEs.



[Figure-2] HA Configuration of TOE

For the HA configuration, two L4 switches that support Load Balancing function should be installed on up and down location of TOE.

Two IPS Servers check each other with Heart Bit, and let the traffic passes the other appliance and maintain the network service in normal when one IPS server operation is stopped.

Detection pattern is updated by downloading update file when any update breakdown exists on release issues by checking update server with SSL communication on IPS Server. The update file is encrypted via SHA-256 algorithm. At this moment, it makes the detection policy on two IPS server would be operated in a same rule by providing function that applies all the detection policy setup on Primary IPS Server to Peer IPS Server and function that applies any detection policy modification on Primary IPS Server to Peer IPS Server.
For the communication between Primary IPS Server and Peer IPS Server, the authentication process by the configured information with each IP and Port information, and it protects the transmitted data as the direct connection is used on HA configuration.

1.4.3 None-TOE Hardware and Software for TOE Operation

Hardware/Software that is required for TOE operation in none-TOE, and the requirements for them is:

TOE	Hardware and Software Environments	
	None-TOE Hardware	None-TOE Software
IPS Server	CPU: Intel Xeon Quad 2.66 * 2 Memory: 12GB HDD: 1TB * 2 Compact Flash(CF): 2GB 10/100/1000Mbps Ethernet Port * 2 RS232C Serial Port * 1 10Gbps Ethernet Port * 2(Default) or 4(Extend)	is4021g (10GB NIC Driver)
IPS Client	CPU: Intel Pentium IV 2.4GHz or higher Memory: 512 MB or higher HDD: 40GB or higher 10/100 Mbps Ethernet Port * 1 Monitor: 1024 x 768 or higher Sound Card and Speaker	OS : (Support these four OS types) - Microsoft Windows XP Professional (32bit) Service Pack 3 - Microsoft Windows Vista (32bit, 64bit) Service Pack 2 - Microsoft Windows 7 (32bit, 64bit) Service Pack 1 - Microsoft Windows Server 2008 (32bit, 64bit) Service Pack 2 Web Browser : Internet Explorer 7.0

[Table-1] Hardware/Software for TOE Operation

SNIPER OS V2.0 (Kernel 2.6.37) is installed on IPS server memory storage device, Compact Flash (CF).
And also, IPS server is installed on HDD, and it is used for log data and backup data storage.
IPS server provides one 10/100/1000Mbps Ethernet Port for monitoring and one 10/100/1000Mbps Ethernet Port for HA configuration as a management ports.
And two 10Gbps Ethernet Ports are provided for packet gathering as a default option, and four ports are provided when expansion.

IPS client automatically install OCXs from IPS server to administrator PC through the Internet Explorer.

None-TOE object that is not belonging to TOE scope is:

Classification	None-Evaluated Object	Description
External Server	Update Server	External system for new security violation event distribution

		When TOE updates the detection pattern by sending request to Update Server, it uses SSL communication for operation. TOE updates detection policy by sending GET request to Update Server. Electronic Signature used at this moment is RSA (2048bits). And also, all the algorithm used for update is provided by SNIPER Crypto.
	Time Server	Public Timer Server for time synchronization
	Mail Server	Mail Server for sending e-mail
	ESM(Enterprise Security Management) Server	External system that controls and gathers events from various network security appliances. Transmits Real-time intrusion detection, System information event, and Raw data by using IAP 0.3 and TLS 1.0.
	SecureCAST	Security forecasting and alerting web service that is operated by Security Incident Response Center of WINS Technet Co., Ltd., and it provides detailed attack help of detected attack. Provides this service through the vulnerability help link that TOE provides.

[Table-2] None-TOE Object List

1.5 TOE Description

TOE is the Intrusion Protection System(IPS), which detects and blocks the attacks to security target network on network based with installation on the linkage location between external and internal network with In-line form, detects and prevents the real-time IPv4/IPv6 network traffic intrusion or attack from the external and internal network.

Physical scope and logical scope of TOE is:

1.5.1 Physical Scope

Physical scope that composes TOE is listed down below, and installation package of TOE that includes IPS Server and IPS Client is created in compressed file form. Among the installation package, Teechart V8 and Fast Report V4 are included in IPS Client.

Each module that composes TOE performs roles are:

1) SNIPER IPS-G V8.0

The build version of SNIPER IPS-G V8.0 Server is 2011.07.01R.

IPS server performs TOE identification and certification, User data protection, Security audit, Security management, and TSF protection. User data protection engine of TOE detects, blocks, and responses intrusion by packet inspection, which inflows through NIC, and the inspected safe packet is transmitted to the destination through NIC.

2) SNIPER IPS-G V8.0 Client

The build version of SNIPER IPS-G V8.0 Client is GLOBAL-20130115.

The administrator who manages the product accesses management interface of server by using http, and accesses to TOE user interface by downloading and installing IPS client program on administrator's PC with ActiveX function of the Internet Explorer.

IPS client provides interface for identification and certification, audit data inquiry, security management (Configuration, Policy setup, Login failure management, Storage device management, Live update, and Tiem synchronization.) configuration.

3) OpenSSL V1.0.1c

It is SSL Library for safe communication between server and client, which are TOE components.

4) SNIPER Crypto V1.3

It is the cryptography algorithm for TOE that WINS Technet Co., Ltd. developed and verified module based on KCMVP standard.

It supports the encryption for Security Management and TSF Protection function operation.

Algorithm used in each encryption is:

Category	Protection Function	Length (bits)
Hash Function	SHA-256	-
Block Code	AES	256
	3DES	168
Electronic Signature	RSASSA-PKCS1-V1.5	2048

[Table-3] SNIPER Crypto Encryption module

5) Teechart V8

It is a module that outputs detection and log statistics chart on IPS client.

6) Fast Report V4

It is a module that generates and outputs detection and log statistics report on IPS client.

7) SNIPER OS V2.0 (Kernel 2.6.37)

It is the operation system that is used on TOE. WINS Technet Co., Ltd upgraded the internal kernel version from

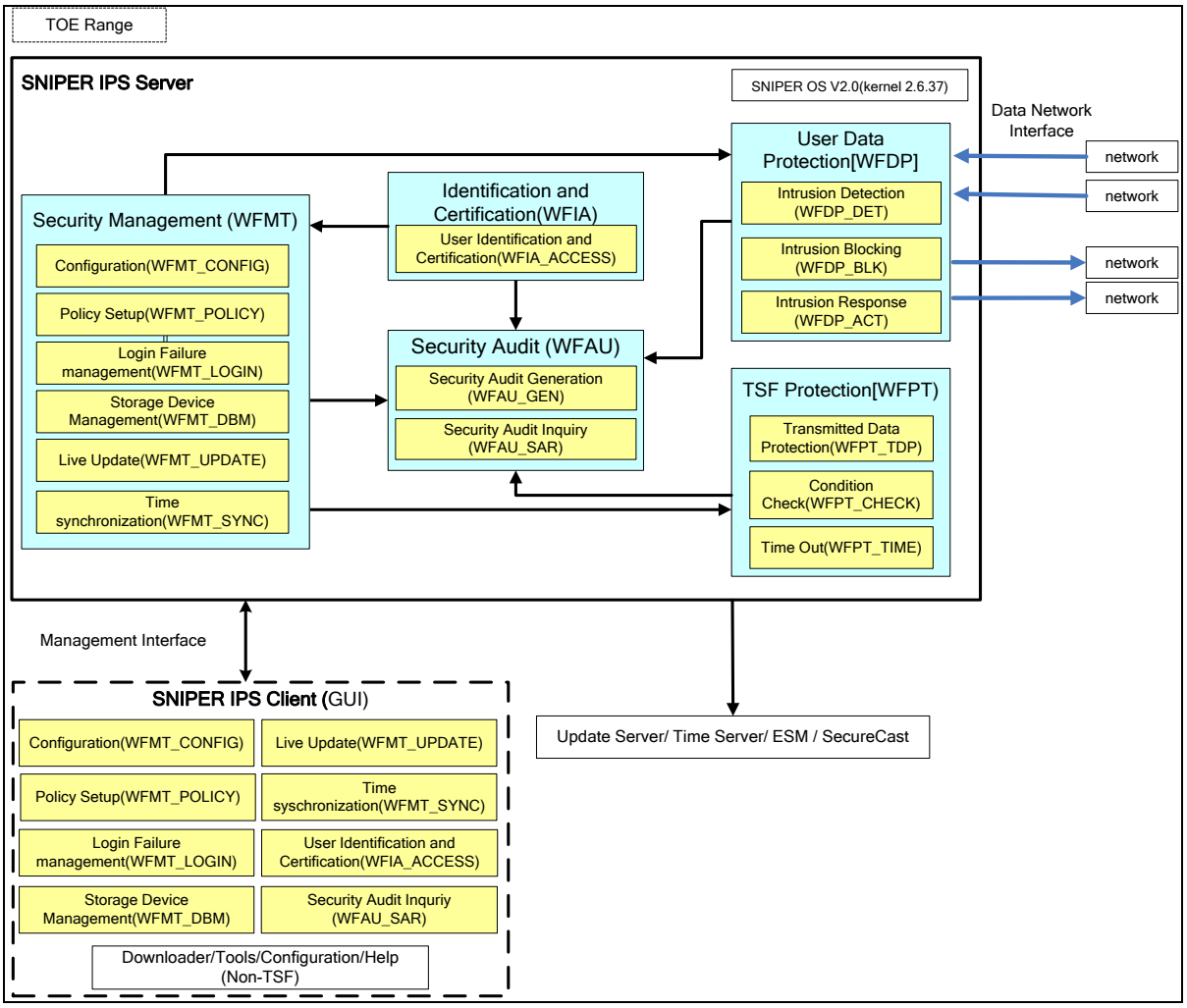
Fedora 14, which is provided from Fedora, into Kernel 2.6.37, which is provided from Kernel.org, and made additional process for removing unnecessary services and adding required configurations.

8) SQLite V3

It is DBMS that is included in SNIPER OS V2.0, the database that saves the data such as detection and blocking log, and administrator configuration information of TOE.

1.5.2 Logical Scope

Logical scope of TOE is:



[Figure-3] Logical scope of TOE

• Security Audit (WFAU)

Security Audit performs Security Audit Generation (WFAU_GEN) and Security Audit Inquiry (WFAU_SAR) functions.

Audit record, which is generated by system usage record gathering and analyzing function for checking whether the system is stably and effectively operated, detects or blocks the intrusion to TOE, and used for system misuse detection.

• User Data Protection (WFDP)

User Data Protection performs Intrusion Detection (WFDP_DET), Intrusion Blocking (WFDP_BLK), and Intrusion Response (WFDP_ACT) functions.

User Data Protection controls network data flows based on the usage or blocking rules to protect security target

network against the internal/external attacks. And also, it gathers information for intrusion detection, responses the intrusion based on the intrusion definition rule, and saves analysis result so that the administrator can review them.

• Identification and Certification (WFIA)
Identification and certification performs User Identification and Certification (WFIA_ACCESS) function.
To perfectly perform access control to TOE, it identifies and certificates administrators whether they are legitimate when they try to access to TOE.
Inter-communication between IPS server and IPS client is encrypted with SSL, and protected from the data modification and exposure by checking integrity through SHA-2.
When it is not operated for the scheduled time, it terminates interworking session to protect TOE for the authorized administrator's none-activity term no matter the access was made by the authorized administrator.

• Security Management (WFMT)
Security Management performs Configuration (WFMT_CONFIG), Policy Setup (WFMT_POLICY), Login Failure Management (WFMT_LOGIN), Storage Device Management (WFMT_DBM), Live Update (WFMT_UPDATE), and Time Synchronization (WFMT_SYNC) functions.

Security management subsystem is a management function for inquiring properties and information about each function that TOE provides, configuring, or inspecting the status. It provides various information inquiring and modifying function such as the rule for TOE detection and blocking activities and TOE status and configuration.

• TSF Protection (WFPT)
TSF Protection performs Transmitted Data Protection (WFPT_TDP), Status Check (WFPT_CHECK), and Time Out (WFPT_TIME) functions.
TOE protection provides checking function whether TOE major components related to integrity of transmitted or being transmitted data are operated normally, and secure the safe status when TOE failure by monitoring it periodically.

IPS Client provides user interface for Identification and Certification (WFIA_ACCESS), Security Audit Inquiry (WFAU_SAR), Configuration (WFMT_CONFIG), Policy Setup (WFMT_POLICY), Login Failure Management (WFMT_LOGIN), Storage Device Management (WFMT_DBM), Live Update (WFMT_UPDATE), and Time Synchronization (WFMT_SYNC) functions.

And also, Non-TSF among TOE functions is:

• Downloader: It installs the required files for IPS client by comparing file list on PC and server, and run IPS client.

• Tools: TOE provides interface that runs network tool of the OS for attacker or victim's IP checking. The administrator can check tracert, whois, ping, route, nbtstat, nslookup, arp, and netstat OS command by inputting IP address. And also, it provides the packet gathering function and report inquiry of the saved traffic and intrusion/detection/drop information function.

• Configuration: It sets the display of GUI.

• Help: TOE provides help to support the authorized administrator's security functions. It provides .chm form help that is installed together when TOE installation, and online help that is linked to SecureCAST service, which is provided by WINS Technet Co., Ltd.

1.6 Terms and Definitions

• 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

• Iteration

One of the CC operations. The use of a component more than once among various operations

• Protected Systems

The asset protected by intrusion detection system security policy. For example, protected systems of network based intrusion detection system are network service or resource, and the protected systems of host based intrusion detection system are resource or information saved in host

• ST, Security Target

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

• PP, Protection Profile

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

• Black hole

The blocking policy list for the packet that should be blocked among the traffic inflows to SNIPER IPS. Each of

black hole policy has time out setting, so it is automatically deleted after expiring period

• User

An 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 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 component to response to specific threat or to satisfy specific security policy on Common Criteria (e.g. Iteration, Assignment, Selection, and Refinement)

• Threat Agent

An unauthorized user or external IT entity that brings assets under such threats as illegal access, modification or deletion

• External IT Entity

Any IT product or system, un-trusted or trusted, outside of the TOE that interacts with the TOE

• Authorized Administrator

A authorized user, in accordance with the TSP(TOE Security Policy), operation and manage the intrusion prevention system

• In line Mode

It performs analysis and blocking against packets. If the IPS is not operated normally in In-line Mode and failure such as system down is occurred, it is led to the network failure, so it checks the system with periodical keep-alive signal.

• Authentication Data

The information used to verify the claimed idemfity of a user

• Assets

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

• Refinement

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

• Information Protection System Common Criteria

It means Information Protection System Common Criteria notified by Minister of Public Administration and Security on September 1, 2009. Common Criteria is Korean translated version of Global Common Criteria (CC) version 3.1 based on common language and understanding and all the evaluation standards that are exist on all over the countries

• Organisational Security Policies

One or more security rule, prosedure, custom, guidelines imposed by an organization upon its operations

• Dependency

A relationship between requirements shch that the requirements that is depended upon shall normally be satisfied for the other requirements to be able to meet their objectives

• Augmentation

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

• Component

The smallest selectable set of elements on CC that may be included in a PP, an ST

• Class

A grouping of families that share a common focus on CC

• TOE, Target of Evaluation

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

• Evaluation Assurance Level (EAL)

A package consisting of assurance components that represents a point ont the CC predefined assurance scale.

• Family

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

• Packet

A group of data for data used for data transmission in internet network. For packet transmission, data between two points are not continuously transmitted. After dividing data to be transmitted into appropriate size to form separate packets, each of the packets is individually transmitted. Each packet contains not only data of the prescribed size, but also control information, such as data destination, address or control code, etc.

• Assignment

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

• Extension

An adding of SFR(Security Functional Requirements) in part 2 or SAR(Security Assurance Requirements) in part 3 of CC on PP, ST

• GUI (Graphical User Interface)

Graphical User Interface that realizes the interface between user and computer in graphic

• HA (High Availability)

HA indicates a system or component that provides continuous operation for a disirably long period. SNIPER configures two system for maintaining all the appliances are available for whole network operation, and keep service in normal status by sending traffic to the other appliance when a failure occured on one system.

• TSF, TOE Security Function

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 regulate how assets are managed, protected and distributed within a TOE

• TSF Data

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

• CC Common Abbreviation

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

1.7 Conventions

This Security Target mix uses English for some abbreviation and clear understanding. Notation, form, conventions in this document follows "Information Protection System Common Criteria" (called "Common Criteria"). Common Criteria allows Selection, Assignment, Iteration, and Refinement operations that can be performed in Security Functional Requirements. Each operation is used in this Security Target.

(1) Iteration

It is used when the operation is multiply applied and one component is repeated many times. The result of Iteration operation is marked as the iteration number in parenthesis after component identifier, i.e., (Iteration No.).

(2) Selection

It is used when more than one selectable option among Information Protection System Common Criteria while requirement writing. The result of Selection operation is marked as underlined and *italicized*.

(3) Refinement

It is used for requirement limitation by adding specification on requirements. The result of Refinement operation is marked as **bold text**.

(4) Assignment

It is used for parameter assignment that is not specified. (e.g. : Password length). The result of Assignment operation is marked as squared parenthesis, i.e., [assignment_Value].

1.8 References

[1] Information Protection System Common Criteria, Public Administration and Security notification No. 2009-

52

[2] Network Intrusion Prevention System Protection Profile V2.1(KECS-PP-0100a-2008), 2010.6.10, KISA (Korea Internet & Security Agency)

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1 : Introduction and general model , Revision 3, July 2009, CCMB-2009-07-001

[4] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 2 : Security functional components , Revision 3, July 2009, CCMB-2009-07-002

[5] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 3 : Security assurance components, Revision 3, July 2009, CCMB-2009-07-003

2. Conformance Claims

2.1 CC Conformance

This Security Target is in conformance with following Common Criteria listed.

- Common Criteria
  - Information Protection System Common Criteria (Public Administration and Security notification No. 2009-52)
  - Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1 : Introduction and general model , Revision 3, July 2009, CCMB-2009-07-001
  - Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 2 : Security functional components , Revision 3, July 2009, CCMB-2009-07-002
  - Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 3 : Security assurance components, Revision 3, July 2009, CCMB-2009-07-003

- Common Criteria Conformance
  - This Security Target is in conformance with Information Protection System Common Criteria, Version 3.1, Part 2: Security functional components and Part 3 : Security assurance components, Revision 3.

2.2 PP Conformance

This Security Target is not in conformance with Protection Profile.

2.3 Package Conformance

This Security Target is in conformance with following Security Assurance Components listed.

- Assurance Package
  - EAL4 Conformance

2.4 Conformance claim rationale

Not applicable.

3. Security Problem Definition

3.1 Threat

Threats are classified into Threat against TOE and Threat against TOE Operational Circumstances.

1) Threats on the TOE

Assets that TOE protects become the internal network that TOE and TOE protects.

Threat agents in general are unauthorized IT entity and user who tries illegal access to TOE or internal assets from external, or harms the TOE or internal assets with anomaly method. Threat agents have strengthened basic level of expert knowledge, resource, and motivation.

Threat	Description
T. Masquerade	Threat agents may access TOE by masquerading as the authorized administrator.
T. Breakdown	When TOE cannot provide normal service to user because of the breakdown caused by the external attacks while it is being operated, threat agents may abuse this failure.
T. Record Failure	Threat agents may disable TOE security incident record by exhausting storage volume.
T. Illegal Information Inflow	Threat agents may intrude the computer of internal network from the external network by sending the packet that includes unauthorized information.
T. Illegal Service Access	Threat agents may interrupt normal service providing of the host by accessing unauthorized service of internal network.
T. Denial of Service Attack	Threat agents may interrupt normal users' operation by abnormal overusing the service resources in internal computer within TOE operating environment.
T. Consecutive Authentication Attempt	Threat agents may acquire authority of authorized user by consecutive authentication attempts for TOE access.
T. Address Spoofing	Threat agents may illegally accesses internal network by spoofing source address as internal address.
T. Save Data Exposure and Damage	Threat agents may exposure, modify, and deletes TSF data that is saved in TOE with unauthorized method.
T. Transmitted Data Exposure and Damage	Threat agents may illegally expose or change the data that transmitted between TOE configuration modules or the data transmits to / transmitted from the trustful external network.

[Table-4] Threat on the TOE

3.2 Security Policy of Organization

Security Policy of Organization described in this paragraph should be observed by TOE.

Policy	Description
P. Audit	To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained. Also, the recorded data shall be reviewed.
P. Safe Management	TOE shall provide management method so that the authorized administrator shall manage the TOE in a secure way.

[Table-5] Security Policy of Organization

3.3 Assumptions of TOE Operational Environment

It is assumed that these conditions exist in TOE operational environment.

Assumption	Description
A. Physical Security	The TOE (IPS Server) shall be located in physically secure environment that can be accessed only by the authorized users.
A. Security Maintenance	When internal network environment changes due to change in the network configuration, host increase/decrease and service increase/decrease, etc. the changed environment and security policy shall immediately be reflected in TOE operation policy so that security level can be maintained to be the same as before.
A. Trusted Administrator	Authorized administrator of TOE shall be non-malicious, have completed appropriate training on TOE administration functions and fulfill obligations according to administrator guidelines.
A. Operating System Reinforcement	Reliability and security of an operating system shall be ensured by administering operations to remove services or means in operating system not required and reinforcement on vulnerabilities in the operating system.
A. Sole Connection Point	The TOE branches off network into external and internal networks and all communications between external and internal networks are carried out only through the TOE.
A. Trusted External Server	Mail Server and SMS Server for e-mail and Short Message Service (SMS) transmission function that TOE provides, Time Server for providing trustful Time-stamp are located in physically safe environment of external professional institute who provides the services. And also, WINS Technet Co., Ltd. provides the service of Update Server, ESM Server, SecureCAST Server, and TOE for HA are located in internal/external safe environment where the servers are operated, and the data transmitted from these servers to TOE assure reliability and stability.

[Table-6] Assumptions

4. Security Objectives

Security objectives are defined and classified into TOE Security Objective and Operational Environment Security Objective.

TOE Security Objective is directly controlled Security Objective by TOE, and Operational Environment Security Objective should be controlled by technically/procedurally method, which is provided in operational environment, so that TOE can correctly provide Security function.

4.1 TOE Security Objective

Security objective that should be directly controlled by TOE is:

Security Objectives	Description
O. Audit	The TOE shall record and maintain security-related incidents in order to enable tracing of responsibility for security-related acts and must provide means to review the recorded data.
O. Management	The TOE shall provide means for authorized administrator of TOE to efficiently manage TOE in secure method and maintains TSF data with the latest status.
O. Denial of Service Cut-off	In order to enable network service of the protected computer to be used by normal users, the TOE shall cut off using of abnormal computer service resources by attackers.
O. Identification	The TOE shall identify users intending to access TOE and all external IT entities that are subject to information flow control by the TOE.
O. Secure State Maintenance	The TOE shall maintain secure state when any failure occurred on TSF.
O. Authentication	The TOE shall authorize identity of administrator before permitting TOE access after administrator identification.
O. Information Flow Control	The TOE shall control unauthorized flow of information from external network to internal network according to the security policy.
O. TSF Data Protection	The TOE shall protect saved TSF data from unauthorized exposure, change and deletion.
O. Transmitted Data Protection	The TOE shall protect transmitted TSF data and updated TSF data between separated locations of TOE from the unauthorized exposure or change.

[Table-7] Security Objective of TOE

4.2 Security Objective for the Operational Environment

This is the Security Objective for the Operational Environment should be controlled by technically/procedurally method, which is provided in operational environment, so that TOE can correctly provide Security Function.

Security Objectives	Description
OE. Physical Security	The TOE (IPS Server) shall be located in physically secure environment to which access is possible only by the authorized administrator.
OE. Security Maintenance	When internal network environment changes due to change in network configuration, increase/decrease of host and increase/decrease of service, etc., the changed environment and security policy must be immediately reflected to TOE operation policy in order to maintain security in the same level as before.
OE. Trusted Administrator	Authorized administrator has no malice, well-educated about TOE management function, and performs duty based on administrator guidelines.
OE. Operating System Reinforcement	Reliability and security of operating system must be assured by administering operations to remove services or means in operating system not required and reinforcement on vulnerabilities in the system.
OE. Sole Connection	The TOE branches off network into external and internal networks and all communications between external and internal networks are carried out only through TOE.
OE. Time Stamp	The TOE shall correctly record security incidents by using trustful time stamp, which is provided in external time server.
OE. Trusted External Server	Mail Server and SMS Server for e-mail and Short Message Service (SMS) transmission function that TOE provides, Time Server for providing trustful Time-stamp are located in physically safe environment of external professional institute who provides the services. And also, WINS Technet Co., Ltd. provides the service of Update Server, ESM Server, SecureCAST Server, and TOE for HA are located in internal/external safe environment where the servers are operated, and the data transmitted from these servers to TOE assure reliability and stability.

[Table-8] Operational Environment Security Objective

4.3 Security Objectives Rationale

Rationale of Security Objectives demonstrates that the specified security objectives are appropriate, sufficient to handle security problems and ar essential, rather than excessive. Rationale of Security objectives demonstrates following items.

- Each assumption, threat, and security policy of the organization is handled by at least one security objective.
- Each security objective handles at least one assumption, threat, and security policy of organization.

This table describes the correspondence between Security Environment and Security Objectives.

Security Environment \ Security Objectives	TOE Security Objectives								
	O. Audit	O. Management	O. Denial of Service Cut-off	O. Identification	O. Secure State Maintenance	O. Authentication	O. Information Flow Control	O.TSF Data Protection	O. Transmitted Data Protection
T. Masquerade	●			●		●			
T. Breakdown					●				
T. Recording Failure	●								
T. Illegal Information Inflow	●	●		●			●		
T. Illegal Service Access		●					●		
T. Denial of Service Attack	●		●	●					
T. Continuous Authentication Attempt	●			●		●			
T. Address Spoofing	●		●	●					
T. Save Data Exposure and Damage								●	
T. Transmitted Data Exposure and Damage									●
T. Cryptography									
P. Audit	●			●					
P. Secure Management		●							

Security Objectives / Security Environment	Operational Environment Security Objective							
	OE. Physical Security	OE. Security Maintenance	OE. Trusted Administrator	OE. Operating System Reinforcement	OE. Sole Connection	OE. Time Stamp	OE. Trusted External Server	OE. Trusted Repository
P. Audit						●		
P. Secure Management								
A. Physical Security	●							
A. Security Maintenance		●						
A. Trusted Administrator			●					
A. Operating System Reinforcement				●				
A. Sole Connection Point					●			
A. Trusted Repository								●
A. Trusted External Server							●	

[Table-9] Theoretical basis of Security Objective

4.3.1 TOE Security Objectives Rationale

Security Objective	Description
O. Audit	As for this TOE security objective, TOE records audit event per user according to audit record policy when user is using security function. Also, the TOE assures to provide the means of safely maintaining and reviewing the recorded audit events. In other words, the TOE provides handling function when audit data reaches saturation state. Audit record creation assures to detect identity of attacker through audit record in case continuous attempts for authentication are made. Spoofing attack, service denial attack and attack to produce and transmit abnormal packet can also be traced through audit record. Therefore, this security objective handles T.Masquerade, T.Recording Failure, T.Illegal Information Inflow, T.Denial of Service Attack, T.Continuous Authentication Attempt, and T. Address Spoofing through audit record and required to execute P. Audit on security policy of organization.
O. Management	In order to execute security policy, TOE sets rules of information flow control, therefore controls illegal access to internal network. For this, the TOE shall provide means to safely manage TOE and TSF data, such as on TOE configuration data creation and management

	as well as the newest vulnerability signature management, etc. Therefore, this security objective handles T. Illegal Information Inflow, T. Illegal Service Access, and required to execute security policy of organization P.Secure Management since it provides safe TOE management method to the authorized administrator.
O. Denial of Service Attack Cut-off	Attacker can execute network service denial attack to internal network computer by passing through the TOE. The representative network service denial attack is for a remote user to exhaust computer resources by making abnormally large service requests to internal computer. In this case, internal computer allocates a large amount of resources to attacker, therefore interrupts normal user from using computer. In preparation to this case, TOE prevents specific user from holding exclusive ownership of specific computer resources, therefore assures computer use by normal user. Therefore, this security objective is required to handles to threat of T.Denial of Service Attack, T.Address Spoofing.
O. Identification	Users to use TOE are divided into administrator who manages TOE by connecting to TOE with authentication and external user (IT entity) passing through the TOE without authentication simply to use computer of internal network. Two of the above cases require the function of identification to process security-related events. Administrator identification function is required because responsibilities are given to all acts used by administrator. External IT identification is necessary for abnormal packet transmission, avoiding service denial attack, avoiding address spoofing attack and creating audit record on attempts of connection to external IT. Therefore, this security objective handles T.Masquerade, T.Address Spoofing, T.Illegal Information Inflow, T.Denial of Service Attack, and T.Continuous Authentication Attempt, and required to execute Security Policy of Organization P.Audit.
O. Secure State Maintenance	TOE may not provide normal service to user when unexpected attack from the external causes TOE failure. TOE on this Security Objective assures its preservation of secure state when TOE malfunction occurred due to any failure. Therefore, this security objective is required to handle threat of T. Breakdown.
O. Authentication	Users who want to access to TOE must get the certification. However, the certification required when TOE access may be vulnerable on consecutive certification attempts by the external attacker. Therefore, TOE should assure the certification mechanism that endures consecutive certification attempt attacks regarding to the external attacker's level. Therefore, this security objective is required to handle threat of T. Masquerade, T. Continuous Authentication Attempt.
O. Information Flow Control	TOE controls information flow according to security policy by being installed at the point where internal and external networks are separated. This security objective assures identifying and avoiding diverse attacks possible to occur in network according to deny

	and allow policies. Diverse attacks in network refer to virus attack, e-mail or web service including illegal information and access to service that is not allowed. The TOE ensures security of internal network by controlling these attacks and preventing them from being flown into internal network according to the set rules. Therefore, this security objective is required to handle threat of T.Illegal Information Inflow, T.Illegal Service Access.
O. TSF Data Protection	Due to unexpected attack from the outside or occurrence of breakdown in TOE, TSF data can be changed beyond recognition by administrator. Therefore it may be impossible to appropriately execute security policy. For this, normal functioning of TSF shall be assured by ensuring integrity of TSF data after inspecting whether TOE, TSF data changes occurred intentionally or unintentionally. Therefore, this security objective is required to handle threat of T.Save Data Exposure and Damage.
O. Transmitted Data Protection	This security objective is required to handle threat of T.Transmitted Data Exposure and Damage since it guarantees that transmitted user data or TSF data are protected from unauthorized exposure and modification.

[Table-10] Description of Theoretical Basis of Security Objective

4.3.2 Security Objectives Rationale of the Operational Environment

Security Objective	Description
OE. Physical Security	This security objective is required to support assumption of A.Physical Security since it guarantees that TOE (IPS Server) is located and operated in physically safe environment.
OE. Security Maintenance	This security objective is required to support assumption of A.Security Maintaining since it guarantees that it reflects modified environment and security policy on TOE operation policy immediately when internal network environment is modified such as Internal network configuration changing, Host increase/decrease, or Service increase/decrease so that it maintains the same security level.
OE. Trusted Administrator	This security objective is required to support assumption of A.Trusted Administrator since it guarantees that authorized administrator of TOE can be trusted.
OE. Operating System Reinforcement	This security objective is required to support assumption of A.Operating System Reinforcement since it guarantees that the Operation System is safe and trusted by eliminating the service and method on unnecessary OS and operating reinforcement task on OS vulnerability.
OE. Sole Connection	This security objective is required to support assumption of A.Sole Connection since it guarantees that all the communications between external and internal is processed through TOE.

OE. Time Stamp	This security objective is required to execute security policy of organization of P.Audit since it guarantees that TOE correctly records security related incidents by using trustful Time Stamp that is provided in external time server.
OE. Trusted Repository	This security objective handles assumption of A.Trusted Repository since it provides trusted Repository to save audit data for TOE function.
OE. Trusted External Server	This security objective handles assumption of A.Trusted External Server since it guarantees that Mail server and SMS server for e-mail and Short Message Service (SMS) Server, External Server, and additional TOE for HA function are located in physically safe environment.

[Table-11] Description of Theoretical Basis of Operational Environment

5. Extended Components Definition

Security requirements on this ST are based on Part 2 or Part 3 components of Common Criteria. So, there is no requirement, which is not based on the Common Criteria, on this ST, and no Extend Components are required for additional definition.

6. Security Requirements

The Security requirements defined in this document is based on related functional components from General Evaluation Standard Part 2 for satisfy the security objectives distinguished in the former chapter.

6.1 Security Functional Requirements

This table summarizes and describes TOE security functional requirements

Security Functional class	Security functional components
Security Audit	FAU_ARP.1 Security Alarm
	FAU_GEN.1 Audit Data Generation
	FAU_GEN.2 User Identity Association
	FAU_SAA.1 Potential Violation Analysis
	FAU_SAR.1 Audit Review
	FAU_SAR.3 Selectable Audit Review
	FAU_SEL.1 Selectable Audit
	FAU_STG.1 Protected Audit Protection
	FAU_STG.3 Action in case of Possible Audit Data loss
	FAU_STG.4 Prevention of Audit Data Loss
User Data Protection	FDP_IFC.1(1) Subset Information Flow control (1)
	FDP_IFC.1(2) Subset Information Flow control (2)
	FDP_IFF.1(1) Simple Security Attributes (1)
	FDP_IFF.1(2) Simple Security Attributes (2)
Identification and Authentication	FIA_AFL.1 Authentication Failure Handling
	FIA_ATD.1(1) User Attribute Definition (1)
	FIA_ATD.1(2) User Attribute Definition (2)
	FIA_UAU.2 User Authentication Before Any Action
	FIA_UAU.7 Protected Authentication Feedback
	FIA_UID.2(1) User Identification Before Any Action (1)
	FIA_UID.2(2) User Identification Before Any Action (2)
Security Management	FMT_MOF.1 Management of Security Functions Behaviour
	FMT_MSA.1 Management of Security Attributes
	FMT_MSA.3 Static Attribute Initilalisation
	FMT_MTD.1(1) Management of TSF Data (1)
	FMT_MTD.1(2) Management of TSF Data (2)
	FMT_MTD.2 Management of Limits on TSF Data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles
Protection of the TSF	FPT_ITT.1 Basic internal TSF data transfer protection
	FPT_ITI.1 Inter-TSF detection of modification
	FPT_TDC.1 Inter-TSF basic TSF data consistency
	FPT_TST.1 TSF Testing
Resource Allocation	FRU_RSA.1 Maximum Quotas
TOE Access	FTA_SSL.3 TSF-initiated termination
Cryptographic Support	FCS_CKM.1 Cryptographic key generation

	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1 Cryptographic operation

[Table-12] Security Functional Requirements

Subject	Security Properties of Subject	Object	Security Properties of Object	Operation
Unauthorized External IT Entity from Information Transmitter	IP Address Port	Traffic Transmitted from the Subject to Others through TOE	Source Address Destination Address Protocol Port Flag Information URI(Uniform Resource Identifier) Attack recognition Count Attack recognition Time Access Time limit bps / pps	determine, enable, disable, modify
Authorized Administrator (Super-administrator)	Identifier, ID, Password, Valid Period, Usage Authority, Certification Failure count	All the TOE Functions	Configuration Tracing Tool Packet Gathering Automatic Report WINS Technet Vulnerability DB Help Version Information Appliance Information Traffic Detection / Defense / Alarm Blocking Traffic Intrusion / Detection Blocking System Management Record Status Check DB Management	determine, enable, disable, modify

Subject	Security Properties of Subject	Object	Security Properties of Object	Operation
			Administrator Management Network Setting Control Center Update Detection Policy Setting Firewall Setting	
Authorized Administrator (General-administrator)	Identifier, ID, Password, Valid Period, Usage Authority, Certification Failure count	All the TOE Functions except Security Audit, Configuration, Security policy	Configuration Tracing Tool Packet Gathering Automatic Report WINS Technet Vulnerability DB Help Version Information Appliance Information Traffic Detection / Defense / Alarm Blocking Traffic Intrusion / Detection Blocking System	determine, enable, disable, modify

6.1.1 Security Audit

6.1.1.1 FAU_ARP.1 Security Alarm

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [sending E-mails selectively to authorized administrators, showing warning windows] upon detection of a potential security violation.

6.1.1.2 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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 *not specified* level of audit; and

c) [none].

Application notes: Auditable events for the not specified level of auditable events.

Functional Components	Authentication Events
FAU.ARP.1	Security alarms, the TSF shall take actions in case a potential security violation is detected
FAU_SAA.1	Operational start and stop of analysis mechanism
FAU_SEL.1	Authentication configuration modification while collecting function is processed.
FDP_IFF.1(1)	Decisions to permit requested information flows
FDP_IFF.1(2)	Decisions to permit requested information flows
FIA_AFL.1	Threshold and counter action of failed authorization trial
FIA_UAU.2	Authentication mechanism usage failure
FIA_UID.2(1)	User identification mechanism usage failure include provided user identity
FIA_UID.2(2)	User identification mechanism usage failure include provided user identity
FMT_SMF.1	Management function usage
FMT_SMR.1	User group changing related to the security roles
FPT_ITI.1	Inter-TSF detection of modification
FRU_RSA.1	Rejection of allocation operation due to resource limits
FTA_SSL.3	Interwork session termination by session termination mechanism

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 (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [none].

6.1.1.3 FAU_GEN.2 User Identity Association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.4 FAU_SAA.1 Potential Violation Analysis
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

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 TSPs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [none] known to indicate a potential security violation;
b) [

- Lack of storage device space warning,
- Surpassing the access limit set by administrator,
- Integrity error warning,
- Packet drop caused by too much traffic,
- More than 90% of the CPU overload continues for more than three minutes,
- Problem on NIC].

6.1.1.5 FAU_SAR.1 Audit Review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [authorized users] with the capability to read [the following audit data] from the audit records.
a) Super Administrator: Available to inquire the all the audit data
b) General Administrator: Available to inquire the audit data related to detection details and drop details only

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

6.1.1.6 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [subject and Object of the event, event type, event date, outcome of the event] of audit data based on [sort].

6.1.1.7 FAU_SEL.1 Selective Audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) subject identity

b) [none]

6.1.1.8 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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 stored audit records.

6.1.1.9 FAU_STG.3 Action in case of Possible Audit Data Loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [send e-mail to authorized administrator] if the audit trail surpasses [when audit data storage device usage of security target system is more than 90% of limitation (5~90%) set by authorized administrator].

6.1.1.10 FAU_STG.4 Prevention of Audit Data Loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *prevent audited events, except those taken by the super administrator with special rights* and [overwrite the DB logging when free space on device is lower than 1GB, notify the super administrator by e-mail] if the audit trail is full.

6.1.2 User Data Protection

6.1.2.1 FDP_IFC.1(1) Subset Information Flow Control (1)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Firewall Policy] on [The following 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 at information sender's side

b) Information: traffic sent by TOE from the subject to others

c) Operation: pass when allowed rule is exist

Application notes: This security policy prevents all the accesses except explicitly permitted rules. So, TOE is network traffic access control policy which allows the service access by defining the rules, and blocks the rest.

6.1.2.2 FDP_IFC.1(2) Subset Information Flow Control (2)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Intrusion Analysis Policy] on [The following 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 at information sender's side

b) Information: traffic sent by TOE from the subject to others

c) Operation: block when prevention rule is exist

Application notes: This security policy prevents malicious traffic based on the signature included in vulnerability list data, and allows all the accesses except the prevention rule is exist.

6.1.2.3 FDP_IFF.1(1) Simple Security Attributes (1)

Hierarchical to: No other components.

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

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

a) Subjects: unauthenticated external IT entities at information sender's side

b) Security attribute of subjects

- IP address

c) Information: traffic sent by TOE from the subject to others

d) Security attribute of information

- Source 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: [When subject IP is registered as ACCEPT on Firewall policy]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [the source is one-way flow of TOE].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [The following list of rules]

a) TOE should block access request for the information that has subject IP address of external network from the internal IT entities.

b) TOE should block access request for the information that has broadcasting subject IP address from the external network.

c) TOE should block access request for the information that has looping subject IP address from the external IT entities.

d) TOE should block access request for the information that has anomaly packet structure from the external IT entities.

6.1.2.4 FDP_IFF.1(2) Simple Security Attributes (2)

Hierarchical to: No other components.

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

FDP_IFF.1.1 The TSF shall enforce the [Intrusion Analysis Policy] based on the following types of subject and information security attributes: [The following list of subjects and information controlled under the indicated SFP, and for each, the security attributes].
a) Subjects: unauthenticated external IT entities at information sender's side
b) Security attribute of subjects
- IP address
- Port

b) Information: traffic sent by TOE from the subject to others
d) Security attribute of information
- Source 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: [Allow when Intrusion Analysis Policy is set as Accept]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [The following list of rules]
a) Deny when intrusion analysis policy is set as drop.

6.1.3 Identification and Authentication

6.1.3.1 FIA_AFL.1 Authentication Failure Handling
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [1~5]* unsuccessful authentication attempts occur related to [authorized administrator's authentication trial].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met or surpassed*, the

TSF shall [general administrator authorization prevention until entire administrators make a counter action, general administrator ID access blocking for five minutes on IPS Server, sending notification e-mail to super-administrator].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual IT entity: [IP Address, Port]

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) IP address

b) {validation, permissions, other administrator's information, or the number of certification failure}

Application notes: Authorized administrators are divided into Super-administrator and General-administrator, and each of them has different permissions.

- Super administrator: Defined as only one user, and enable to perform all the TOE functions.
- General administrator: Enable to perform All the TOE Functions except Security Audit, Configuration, and Security policy.

Security Function		Super-administrator	General-administrator
Setup Menu	Configuration Setting	determine, enable, disable, modify	enable, modify
	Tracking Tool	determine, enable, disable	determine, enable, disable
	Packet Collection	determine, enable, disable, modify	determine, enable, disable, modify
	Auto Report	determine, enable, disable	determine, enable, disable
	WINS Technet Vulnerability DB	enable, disable	enable, disable
	Help	enable, disable	enable, disable
	Version Information	enable, disable	enable, disable
Real-time	Appliance Information	enable, disable	enable, disable

Monitor	Traffic	enable, disable	enable, disable
	Detection/Prevention/ Alert	enable, disable	enable, disable
	Prevention	enable, disable	enable, disable
Comprehensive Report	Traffic	enable, disable	enable, disable
	Intrusion/Detection	enable, disable	enable, disable
	Prevention	enable, disable	enable, disable
	System	enable, disable	enable, disable
Security Audit	Management History	determine, enable, disable, modify	-
	Status Check	determine, enable, disable, modify	-
	DB management	determine, enable, disable, modify	-
Configuration	Administrator Management	determine, enable, disable, modify	determine, enable, modify
	Network Setting	determine, enable, disable, modify	-
	Control Center	determine, enable, disable, modify	-
	Update	determine, enable, disable	-
Security Policy	Detection Policy Setup	determine, enable, disable, modify	-
	Firewall Setup	determine, enable, disable, modify	-

6.1.3.4 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each authorized administrators to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrators.

6.1.3.5 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [showing password conversion into "*" on monitor, succeed and failure message] to the authorized administrator while the authentication is in progress.

6.1.3.6 FIA_UID.2(1) User Identification Before Any Action (1)
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each IT entity to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.7 FIA_UID.2(2) User Identification Before Any Action (2)
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each authorized administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of the authorized administrator.

6.1.4 Security Management

6.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of, disable, enable, modify the behaviour of* the functions [The following the table] to [super-administrator or General administrator].

Security Functions	Super-administrator	General-administrator
Timeout Setting	determine, enable, disable, modify	-
Sending Mail	determine, enable, disable, modify	-
Integrity Check	determine, enable	-
IPS Status Information	determine, enable	-
Administrator Management	determine, disable, enable, modify	determine, modify
Network	determine, disable, enable, modify	-
Control Center Setting	determine, disable, enable, modify	-
Mode Setting	determine, disable, enable, modify	-
Packet Gathering Setting	determine, disable, enable, modify	determine, disable, enable, modify
Detection Policy setting	determine, disable, enable, modify	-

Firewall Setting	determine, disable, enable, modify	-
Access Failure Management	determine, enable	-
Storage Limitation Setting	determine, enable	-
DB Backup/Restore	determine, enable, disable	-
Live Update	determine, enable	-
Time Synchronization	determine, enable	-

[Table-13] Security function management

6.1.4.2 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

Dependencies: [FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [Intrusion Analysis Policy, Firewall Policy] to restrict the ability to *query*, *modify*, *delete*, *(generate)* the security attributes [The following the table] to [super-administrator].

Security attribute		Action
Intrusion Analysis Policy	Denial of Service	query, modify
	Information Gathering	query, modify
	Protocol Vulnerability	query, modify
	Service Attack	query, modify
	WebCGI Attack	query, modify, delete, generate
	User Defined	query, modify, delete, generate
	Protocol Statistics Analysis	query, modify
	Service Statistics Analysis	query, modify, delete, generate
	IP Statistics Analysis	query, modify
	PATTERN BLOCK	query, modify, delete, generate
	Packet Header Detection	query, modify, delete, generate
Firewall Policy	Interface (Inbound/Outbound/Any)	query, modify
	Source IP	query, modify
	Destination IP	query, modify
	Service (Port, Protocol)	query, modify
	Policy (ACCECPT/DROP)	query, modify

[Table-14] Security Attribute Management

6.1.4.3 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the [Intrusion Analysis Policy, Firewall Policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

Application notes: Firewall policy should be limited as Super administrator to block the illegal access to the protected assets.

6.1.4.5 FMT_MTD.1(1) Management of TSF Data (1)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *change default, query, modify, delete, clear, [generate, updated with the latest data]* the [The following table of TSF data] to [authorized administrator].

Application notes: Limit to the Super-administrator, which is the highest administrator.

Security Function	TSF Data	Super-administrator	General-administrator
Timeout setting	Timeout Time	query, modify	-
Sending Mail	Mail Address related Mail Sending	query, modify	-
Integrity check	Integrity period setting, integrity file setting	query, modify, generate	-
IPS Status Information	HA setting	modify the default value, query, modify	-
Administrator Management	Administrator information	query, modify, delete, clear, generate	query, modify, clear
Network	Internal IP, Security audit IP, Exceptional IP	query, modify, delete, generate	-
	Interface Name Setting	query, modify	
Control Center Setting	Server IP, Port, SNIPER identifier, Control interworking, Applying check	query, modify, delete, clear, generate	-
Mode Setting	IPS mode, IDS mode, Firewall usage	modify the default value,	-

	mode, SNIPER mode, BW mode	query, modify	
Packet Gathering Setting	Interface, Protocol, Filter type, Filter, Explanation, Termination condition, Packet count	modify the default value, query, modify, delete, generate, updated with the latest data	modify the default value, query, modify, delete, generate, updated with the latest data
Detection Policy Setting	Intrusion detection policy	modify the default value, query, modify, delete, generate, updated with the latest data	-
Firewall Setting	Firewall policy	modify the default value, query, modify, delete, generate	-
Access Failure Management	Access count limitation	modify the default value, query, modify	-
Storage Limitation Setting	Storage device threshold setting, log storage period	modify the default value, query, modify	-
DB Backup/Restore Management	Backup period, Backup device, Restore device	query, modify	-
	DB Backup reserving setting	query, modify, delete, generate	-
Live update	Pattern update data	updated with the latest data	-
	Reserve setting	query, modify, delete, generate	-
Time Synchronization	SNIPER Client current time, SNIPER Server current time	query, modify, updated with the latest data	-
	Time server setting	updated with the latest data	

6.1.4.5 FMT_MTD.1(2) Management of TSF Data (2)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *query* the [The following lists of TSF data] to [super administrator].

- TOE time stamp used when audit record trail
- Authorized administrator session timeout value
- Audit record setting value

• Auto update cycle

6.1.4.6 FMT_MTD.2 Management of Limits on TSF Data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [audit data storage volume] to [super administrator].

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

6.1.4.7 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[

a) TSF function management:

- Authorizing function on each authorized administrator related to security function management

b) Security attributes management:

- Security properties management functions on intrusion analysis policy and firewall policy, etc.

c) TSF data management:

- Authorizing function on each authorized administrator related to TSF data management and question

d) TSF data threshold management:

- Threshold management function on audit data storage volume

e) Security role management:

- Security roles management functions on super administrator and general administrator].

6.1.4.8 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [super administrator, general administrator].

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

6.1.5 Protection of the TSF

6.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

6.1.5.2 FPT_ITI.1 Inter-TSF Detection of Modification

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [limited on trusted external server sated on ST].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [Stopping Data Transmission] if modifications are detected.

6.1.5.3 FPT_ TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [All TSF data] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [none] when interpreting the TSF data from another trusted IT product.

6.1.5.4 FPT_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [*TSF execution code*].

6.1.6 Resource Allocation

6.1.6.1 FRU_RSA.1 Maximum Quotas
Hierarchical to: No other components.
Dependencies: No dependencies.

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

6.1.7 TOE Access

6.1.7.1 FTA_SSL.3 TSF-Initiated Termination
Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [timeout value set by Super-administrator (default: 10 minutes)].

6.1.8 Cryptographic Support

6.1.8.1 FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [SEED encryption algorithm, ARIA encryption algorithm, 4SHA-2 algorithm, RSASSA-PKCS1-V1_5 algorithm, RSAES-OAEP algorithm] and specified cryptographic key sizes [above 128bit, above 256bit for SHA-2 algorithm] that meet the following: [KS X ISO/IEC 19790].

6.1.8.2 FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key

destruction method [change all the cryptographically related cryptographic keys and important parameters into '0'] that meets the following: [IETF FIPS PUB 140-2].

6.1.8.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Electronic signature verification, data encryption and decryption, hash code generation] in accordance with a specified cryptographic algorithm [SEED encryption algorithm, ARIA encryption algorithm, SHA-2 algorithm, RSASSA-PKCS1-V1_5 algorithm, RSAES-OAEP algorithm] and cryptographic key sizes [above 128bit, above 256bit for SHA-2 algorithm] that meet the following: [KS X ISO/IEC 19790].

6.2 TOE Security Assurance Components

TOE Security Assurance Components configured by Assurance Components of CC Part.3, and evaluation assurance level is EAL4. [Table-15] Assurance Components shows brief description of each category.

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete Functional Specification
	ADV_IMP.1	Implementation Representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and Automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle model
	ALC_TAT.1	Well-Defined Development Tools
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.2	Testing : Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing – Sample
Vulnerability Assessment	AVA_VAN.3	Focused Vulnerability Analysis

[Table-15] Assurance Components

6.2.1 Development

6.2.1.1 ADV_ARC.1 Security Architecture Description

Dependencies: ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:
ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.
ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

6.2.1.2 ADV_FSP.4 Complete Functional Specification
Dependencies: ADV_TDS.1 Basic design

Developer action elements:
ADV_FSP.4.1D The developer shall provide a functional specification.
ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:
ADV_FSP.4.1C The functional specification shall completely represent the TSF.
ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.
ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.
ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:
ADV_FSP.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content

and presentation of evidence.

ADV_FSP.4.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.1.3 ADV_IMP.1 Implementation Representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:

ADV_IMP.1.1C The implementation representation shall 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 in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

6.2.1.4 ADV_TDS.3 Basic Modular Design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.
ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose.
ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces.
ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.
ADV_TDS.3.10C The mapping shall demonstrate to the behaviour described in the TOE design that they invoke.

Evaluator action elements:
ADV_TDS.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

6.2.2 Guidance Documents

6.2.2.1 AGD_OPE.1 Operational User Guidance
Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:
AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:
AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C The operational user guidance 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.
AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

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

6.2.2.2 AGD_PRE.1 Preparative Procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.3 Life-Cycle Support

6.2.3.1 ALC_CMC.4 Production Support, Acceptance Procedures and Automation

Dependencies: ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.
ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.
ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.
ALC_CMC.4.6C The CM documentation shall include a CM plan.
ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:
ALC_CMC.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

6.2.3.2 ALC_CMS.4 Problem Tracking CM Coverage
Dependencies: No dependencies.

Developer action elements:
ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:
ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.
ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:
ALC_CMS.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

6.2.3.3 ALC_DEL.1 Delivery Procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

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

6.2.3.4 ALC_DVS.1 Identification of Security Measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce security documentation.

Content and presentation 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.

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.

6.2.3.5 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 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.

6.2.3.6 ALC_TAT.1 Well-Defined Development Tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall indentify the documentation each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

Content and presentation elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool 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.

6.2.4 Security Target Evaluation

6.2.4.1 ASE_CCL.1 Conformance Claims

Dependencies: APE_INT.1 PP introduction

APE_ECD.1 Extended components definition

APE_REQ.1 Stated security requirements

Developer action elements:

APE_CCL.1.1D The developer shall provide a conformance claim.

APE_CCL.1.2D The developer shall provide a conformance claim rationale.

APE_CCL.1.3D The developer shall provide a conformance statement.

Content and presentation elements:

APE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the PP claims conformance.

APE_CCL.1.2C The CC conformance claim shall describe the conformance of the PP to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

APE_CCL.1.3C The CC conformance claim shall describe the conformance of the PP to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

APE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

APE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the PP claims conformance.

APE_CCL.1.6C The conformance claim shall describe any conformance of the PP to a package as either package-conformant or package-augmented.

APE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

APE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

APE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

APE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

APE_CCL.1.11C The conformance statement shall describe the conformance required of any PPs/STs to the PP as strict-PP or demonstrable-PP conformance.

Evaluator action elements:

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

6.2.4.2 ASE_ECD.1 Extended Components Definition

Dependencies: No dependencies.

Developer action elements:

APE_ECD.1.1D The developer shall provide a statement of security requirements.

APE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

APE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

APE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

APE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

APE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

APE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

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

APE_ECD.1.2E The evaluator *shall confirm* that no extended component may be clearly expressed using existing components.

6.2.4.3 ASE_INT.1 ST Introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E The evaluator *shall confirm* that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

6.2.4.4 ASE_OBJ.2 Security Objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

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

6.2.4.5 ASE_REQ.2 Derived Security Requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.
ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

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

6.2.4.6 ASE_SPD.1 Security Problem Definition

Dependencies: No dependencies.

Developer action elements:

APE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

APE_SPD.1.1C The security problem definition shall describe the threats.

APE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

APE_SPD.1.3C The security problem definition shall describe the OSPs.

APE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

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

6.2.4.7 ASE_TSS.1 TOE Summary Specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

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

ASE_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.5 Tests

6.2.5.1 ATE_COV.2 Analysis of Coverage

Dependencies: ADV_FSP.2 Security-enforcing 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 elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

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

6.2.5.2 ATE_DPT.1 Testing: Basic Design

Dependencies: ADV_ARC.1 Security architecture description
ADV_TDS.2 Architectural 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 elements:

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements:

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

6.2.5.3 ATE_FUN.1 Functional Testing

Dependencies: ATE_COV.1 Evidence of coverage

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 elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

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

6.2.5.4 ATE_IND.2 Independent Testing - Sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation 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 execute* a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator *shall test* a subset of the TSF interface to confirm that the TSF operates as specified.

6.2.6 Vulnerability Assessment

6.2.6.1 AVA_VAN.3 Enforced Vulnerability Analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.4 Complete functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_DPT.1 Testing: basic design

Developer action elements:

AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.3.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content

and presentation of evidence.

AVA_VAN.3.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator *shall perform* an independent, focused vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6.3 Security Requirements Rationale

Security requirements rationale demonstrates that described IT security functional required components are suitable for Security objectives, and they are appropriate for treating security risks.

Objectives / SFR	O.Audit	O.Management	O.TSF Data Protection	O.Denial of Service Cut-off	O. Identification	O. Secure State Maintenance	O.Authentication	O. Information Flow Control	O.Transmitted Data Protection
FAU_ARP.1	●								
FAU_GEN.1	●								
FAU_GEN.2	●								
FAU_SAA.1	●								
FAU_SAR.1	●								
FAU_SAR.3	●								
FAU_SEL.1	●								
FAU_STG.1	●								
FAU_STG.3	●								
FAU_STG.4	●								
FDP_IFC.1(1)								●	
FDP_IFC.1(2)								●	
FDP_IFF.1(1)								●	
FDP_IFF.1(2)								●	
FIA_AFL.1							●		
FIA_ATD.1(1)				●	●			●	
FIA_ATD.1(2)					●				
FIA_UAU.2		●	●				●		
FIA_UAU.7							●		
FIA_UID.2(1)				●	●			●	
FIA_UID.2(2)		●	●		●				
FMT_MOF.1		●							
FMT_MSA.1		●							
FMT_MSA.3		●							
FMT_MTD.1(1)		●							
FMT_MTD.1(2)		●							
FMT_MTD.2		●							

Objectives / SFR	O.Audit	O.Management	O.TSF Data Protection	O.Denial of Service Cut-off	O. Identification	O. Secure State Maintenance	O.Authentication	O. Information Flow Control	O.Transmitted Data Protection
FMT_SMF.1		●							
FMT_SMR.1		●							
FPT_ITT.1									●
FPT_ITI.1									●
FPT_TDC.1						●			
FPT_TST.1			●						
FRU_RSA.1				●					
FTA_SSL.3		●	●	●					
FCS_CKM.1									●
FCS_CKM.4									●
FCS_COP.1									●

[Table-16] Cross of Security Objectives and Requirement Components

6.3.1 TOE Security Functional Requirements Rationale

TOE security functional requirements Rationale proofs the list down below.

- Each of TOE security objectives is treated by at least one TOE security functional requirement.
- Each of TOE security functional requirements treats at least one TOE security objective.

Security Functional Requirements	Rationale
FAU_ARP.1 Security Alarm	This component meets TOE security objective of O. Audit because it assures the counter action ability when security violation detection.
FAU_GEN.1 Audit Data Generation	This component meets TOE security objective of O. Audit because it defines audit target events and assures audit record generation ability.
FAU_GEN.2 User Identity Association	This component meets TOE security objective of O. Audit because it defines audit target events and audit record requires user identification for user relevance tracking.
FAU_SAA.1 Potential Violation Analysis	This component meets TOE security objective of O. Audit because it assures security violation inspection by examining audited events.
FAU_SAR.1 Audit Review	This component meets TOE security objective of O. Audit because it assures authorized user's ability to examine audit record.

FAU_SAR3 Selectable Audit Review	This component meets TOE security objective of O. Audit because it assures audit data searching and sorting ability by logical connection standard.
FAU_SEL.1 Selective Audit	This component meets TOE security objective of O. Audit because it assures audit target event inclusion /exclusion ability by security attributes basis.
FAU_STG.1 Protected Audit Trail Storage	This component meets TOE security objective of O. Audit because it assures audit record protection ability against inappropriate modify and delete.
FAU_STG.3 Action in case of Possible Audit Data Loss	This component meets TOE security objective of O. Audit because it assures counter action ability when audit trail is surpassed defined threshold.
FAU_STG.4 Prevention of Audit Data Loss	This component meets TOE security objective of O. Audit because it assures counter action ability when audit storage is saturated.
FDP_IFC.1(1) Subset Information Flow Control (1)	This component meets TOE security objective of O. Information Flow Control because it defines security policy for information flow control and assures security policy boundary.
FDP_IFC.1(2) Subset Information Flow Control (2)	This component meets TOE security objective of O. Information Flow Control because it defines security policy for information flow control and assures security policy boundary.
FDP_IFF.1(1) Simple Security Attributes (1)	This component meets TOE security objective of O. Information Flow Control because it describes confront function against explicit attacks.
FDP_IFF.1(2) Simple Security Attributes (2)	This component meets TOE security objective of O. Information Flow Control because it describes confront function against explicit attacks.
FIA_AFL.1 Authentication Failure Handling	This component meets TOE security objective of O. Certification because it defines user authentication failure counts and assures counter action ability when authentication is reached or surpassed defined threshold.
FIA_ATD.1(1) User Attribute Definition (1)	This component requires detecting external IT substance identifier as computer IP address. It meets O. Denial of Service Blocking, O. Detection, and O. Information Flow control because IP address generates audit record, judges whether the address is forged, or can be used as grounds for DDoS Attack detection/Information flow blocking by identifying external IT substance.
FIA_ATD.1(2) User Attribute Definition (2)	This component meets TOE security objective of O. Detection because it is about administrator identifications.
FIA_UAU.2 User authentication before any action	This component meets TOE security objective of O. Management, O. TSF Data Protection because it assures the authentication capability before all the TOE actions are processed.
FIA_UAU.7 Protected Authentication Feedback	This component meets TOE security objective of O. Certification because it assures only specified certification feedback is provided for administrator during certification process.

FIA_UID.2(1) User Identification Before Any Actions (1)	This component requires detecting external IT substance identifier as computer IP address. It meets O. Denial of Service Blocking, O. Detection, and O. Information Flow control because IP address generates audit record, judges whether the address is forged, or can be used as grounds for DDoS Attack detection/Information flow blocking by identifying external IT substance.
FIA_UID.2(2) User Identification Before Any Actions (2)	This component meets TOE security objective of O. Management, O. TSF Data Protection, O. Detection because it requires identification of the administrator.
FMT_MOF.1 Management of Security Functions Behaviour	This component meets TOE security objective of O. Preservation of Secure State, O. Management because it assures its secure state when TOE malfunctions, and the administrator's security functions management ability.
FMT_MSA.1 Management of Security Attributes	This component meets TOE security objective of O. Management, O.TSF Data protection, and O. Information Flow Control because it assures only the administrator's access to TSF security attributes data, which is essential for TOE security functional operation.
FMT_MSA.3 Static Attribute Initialisation	This component meets TOE security objective of O. Management, O.TSF Data protection, and O. Information Flow Control because it assures only the administrator's access when initialise TSF security attributes data, which is essential for TOE security functional operation.
FMT_MTD.1(1) Management of TSF Data	This component meets TOE security objective of O. Management, O. Preservation of Secure State because it requires authorized administrator's functions for updating the latest vulnerability database.
FMT_MTD.1(2) Management of TSF Data (2)	This component meets TOE security objective of O. Management, O. TSF Data Protection because it requires the administrator's TSF data management functions.
FMT_MTD.2 Management of Limits on TSF Data	This component meets TOE security objective of O. Management, O. Preservation of Secure State because it assures authorized administrator's TSF data threshold management and TOE's important availability when data is reached or surpassed threshold.
FMT_SMF.1 Specification of Management Functions	This component meets TOE security objective of O. Management because it requires specifying the management functions that should be provided by TSF, such as security objectives, TSF data, and Security functions.
FMT_SMR.1 Security Roles	This component meets TOE security objective of O. Management because it assures user association into authorized administrator role.

FPT_ITT.1 Basic internal TSF data transfer protection	This component meets TOE security objective of O. Transmitted data Protection because it assures when TSF data is transmitted between separated locations of TOE.
FPT_ITI.1 Inter-TSF detection of modification	This component meets TOE security objective of O. Transmitted data Protection because it assures that TSF data is protected when it is transmitted to the trusted external server.
FPT_TDC.1 Inter-TSF basic TSF data consistency	This component meets O. Preservation of Secure State because it guarantees the consistency of the entire TSF data between the trusted IT products that substitutes the entire TSF function when any failure occurred on TSF and TOE.
FPT_TST.1 TSF Testing	This component meets TOE Security objective of O. TSF Data Protection because it assures TSF testing for its effective operation and the authorized administrator verifies TSF data and its integrity of operational code so that it prevents TOE malfunction, or its instant detection when malfunctions.
FRU_RSA.1 Maximum Quotas	This component meets TOE Security objective of O. Denial of Service Blocking because it blocks denial of service attack by resource usage quotas limitation for TOE protected assets of each user.
FRU_RSA.1 Limited fault tolerance (Apply all)	This component meets TOE Security objective of O. Preservation of Secure State because it assures continuous TOE security functions when TOE has malfunction problem.
FTA_SSL.3 TSF-initiated Termination	This component meets TOE security objective of O. Denial of Service Blocking because it requires securing network service availability by session termination between external IT substance and internal computers after specified time.
FCS_CKM.1 Cryptographic key generation	This component meets TOE Security objective of O. Transmitted Data Protection because it protects the internal and external transmitted data on TOE related to cryptographic operation.
FCS_CKM.4 Cryptographic key destruction	This component meets TOE Security objective of O. Transmitted Data Protection because it protects the internal and external transmitted data on TOE related to cryptographic operation.
FCS_COP.1 Cryptographic operation	This component meets TOE Security objective of O. Transmitted Data Protection because it protects the internal and external transmitted data on TOE related to cryptographic operation.

[Table-17] Security Objectives and Security Functional Requirements Components

6.3.2 TOE Assurance Requirements Rationale

TOE evaluation assurance level is EAL4, which requires enforcing development documentation and vulnerability analysis, automated configuration management of development process. This table describes TOE assurance means. Assurance means, methods for satisfying assurance requirements, are listed in [Table-18].

Assurance Class	Assurance Components		Assurance Measures
Development	ADV_ARC.1	Security architecture description	SNIPER IPS-G V8.0 Security Architecture Guidance
	ADV_FSP.4	Complete functional specification	SNIPER IPS-G V8.0 Unit Plan
	ADV_IMP.1	Implementation representation of the TSF	SNIPER IPS-G V8.0 Verification Specifications
	ADV_TDS.3	Basic modular design	SNIPER IPS-G V8.0 Basic Unit Plan SNIPER IPS-G V8.0 Specific Unit Plan
Guidance Documents	AGD_OPE.1	Operational user guidance	SNIPER IPS-G V8.0 Administrator Guidance
	AGD_PRE.1	Preparative procedures	SNIPER IPS-G V8.0 Installation Manual
Life-Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	SNIPER IPS-G V8.0 Configuration Management Documents
	ALC_CMS.4	Problem tracking CM coverage	
	ALC_DEL.1	Delivery procedures	SNIPER IPS-G V8.0 Deploy Documents
	ALC_DVS.1	Identification of security measures	SNIPER IPS-G V8.0 Life-cycle Support Documents
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.1	Well-defined development tools	
Security Target Evaluation	ASE_CCL.1	Conformance claims	SNIPER IPS-G V8.0 Security Target
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security Objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
Tests	ATE_COV.2	Analysis of coverage	SNIPER IPS-G V8.0 Test Documents
	ATE_DPT.1	Testing: basic design	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing – sample	
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis	TOE Offer

[Table-18] Assurance Measure List

6.3.2.1 Development

ADV_ARC.1(Security architecture description) : TOE security architecture TOE description is assured by security unit plan.

ADV_FSP.4(Complete functional specification): It is assured by complete basic unit plan.

ADV_IMP.1(Implementation representation of the TSF): Implementation representation of the TSF is assured by verification specification.

ADV_TDS.3(Basic modular design): Basic modular design is assured by unit plan.

6.3.2.2 Guidance Documents

AGD_OPE.1(Operational user guidance) : Operational user guidance, for administrators, is assured by administrator guidance.

AGD_PRE.1 (Preparative procedures) : Trusted administrators are enable to use TOE, and they are assured by administrator guidance.

6.3.2.3 Life-Cycle Support

ALC_CMC.4 (Production support, acceptance procedures and automation) : Production support, acceptance procedures and automation of TOE are assured by configuration management documents.

ALC_CMS.4 (Problem tracking CM coverage): Problem tracking CM coverage of TOE are assured by configuration management documents.

ALC_DEL.1 (Delivery procedures): Delivery procedures of TOE are assured by configuration management documents.

ALC_DVS.1 (Identification of security measures): It is a security document related to TOE, and assured by configuration management documents.

ALC_LCD.1 (Developer defined life-cycle model) : It is used for development and maintenance of TOE, and assured by configuration management documents.

ALC_TAT.1 (Well-defined development tools) : It is development tool for TOE, and assured by configuration management documents.

6.3.2.4 Security Target Evaluation

ASE_CCL.1 (Conformance claims) : Conformance claims are assured by the security target.

ASE_ECD.1 (Extended components definition): Extended components definition is assured by the security target.

ASE_INT.1 (ST introduction): ST introduction is assured by the security target.

ASE_OBJ.2 (Security objectives): Security objectives are assured by the security target.

ASE_REQ.2 (Derived security requirements): Derived security requirements are assured by the security target.

ASE_SPD.1 (Security problem definition): Security problem definition is assured by the security target.

ASE_TSS.1 (TOE summary specification): TOE summary specification is assured by the security target.

6.3.2.5 Tests

ATE_COV.2 (Analysis of coverage): Analysis of coverage is assured by the test document.

ATE_DPT.1 (Testing: basic design): Testing: sub-system is assured by the test document.

ATE_FUN.1 (Functional testing): Functional testing is assured by the test document.

ATE_IND.2 (Independent testing - sample): Independent testing - sample is assured by the test document.

6.3.2.6 Vulnerability Assessment

AVA_VAN.3(Focused vulnerability analysis): TOE is offered for Focused vulnerability analysis of TOE.

6.4 Dependency Rationale

6.4.1 Security Functional Requirements Dependencies

[Table-19] shows the dependencies of TOE functional component.

No	Functional Component	Dependencies	Reference No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	OE.Time Stamp
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 20, 21
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 25, 26
8	FAU_STG.1	FAU.GEN.1	2
9	FAU_STG.3	FAU_STG.1	8
10	FAU_STG.4	FAU_STG.1	8
11	FDP_IFC.1(1)	FDP_IFF.1	13,14
12	FDP_IFC.1(2)	FDP_IFF.1	13,14
13	FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	11,12 24
14	FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	11,12 24
15	FIA_AFL.1	FIA_UAU.1	18
16	FIA_ATD.1(1)	None	-
17	FIA_ATD.1(2)	None	-
18	FIA_UAU.2	FIA_UID.1	20,21
19	FIA_UAU.7	FIA_UAU.1	18
20	FIA_UID.2(1)	None	-

21	FIA_UID.2(2)	None	-
22	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	28 29
23	FMT_MSA.1	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	11,12 28 29
24	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	23 29
25	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	28 29
26	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	28 29
27	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	25,26 29
28	FMT_SMF.1	None	-
29	FMT_SMR.1	FIA_UID.1	20, 21
30	FPT_ITT.1	None	-
31	FPT_TDC.1	None	-
32	FPT_TST.1	None	-
33	FRU_RSA.1	None	-
34	FTA_SSL.3	None	-
35	FPT_ITI.1	None	-
36	FCS_CKM.1	FCS_COP.1 FCS_CKM.4	37, 38
37	FCS_CKM.4	FCS_CKM.1	36
38	FCS_COP.1	FCS_CKM.1 FCS_CKM.4	36, 37

[Table-19] Functional Component Dependencies

6.4.2 Assurance Required Components Dependencies

Rationale for Common Criteria for Information Technology Security Evaluation is omitted since its dependencies of each assurance package is already satisfied.

7. TOE Summery Specification

In this chapter, the security requirement that TOE provides is described. And it proves that security functions of TOE are satisfied by the security functional requirements.

7.1. Security Function

In this paragraph, Security Functions (TSF) of TOE is described based on TOE security functional requirement components. Security functions that TOE provides are:

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

Targeted TOE strength of function is SOF-Medium. Since the possibility of successful attack of threat agent is assumed as low, required SOF is defined as medium.

7.1.1. Security Audit (WFAU)

Security audit performs these functions.

- Security Audit Generation (WFAU_GEN)
- Security Audit Inquiry (WFAU_SAR)

7.1.1.1 Security Audit Generation (WFAU_GEN)

Security audit generation is classified into Intrusion Event Data Gathering (WFAU_GEN_EVENT) and Security Audit Data Gathering (WFAU_GEN_AUDIT).

(1) Intrusion Event Data Gathering (WFAU_GEN_EVENT)

When intrusion event to protected server is occurred, it gathers these intrusion event data for detection / blocking / prevention against the attack.

Audit targeted incidents are:

- Event occurred time: Start time, End time
- Attacker information: Source IP, Port, User information of Source IP
- Subject information: Destination IP, Port information
- Attack detection: Attack name, Attack code, (identification of security violation event), Attack classification, and Risk level of the attack
- Attack status information: Finish, in progress check
- Attempt count
- Traffic information: PPS/ BPS of normal traffic and anomaly traffic, Data size, Use of data, TTL,

Protocol, and Service Information

TOE stores the gathered data on permanent buffer, and saves analyzed detection/prevention/alert log and statistics data and traffic data and blocking list log and statistics data on each DB.

(2) Security Audit Data Gathering (WFAU_GEN_AUDIT)

Security Audit Data Gathering gathers audit data regarding to security management function operated by authorized administrator and in case when security audit function, which is controlled by TSF, is violated. In case when security audit IP is configured by the super administrator, the audit data gathering is available for the case the security audit function that is arbitrated by TSF is violated.

Audit targeted incidents are:

- Usage of management function
- Start-up and shut-down of the TOE
- Usage failure of authentication mechanism
- Reaching of the threshold and actions to be taken for failed authentication attemption
- Result of verify the integrity of TSF data
- Changing TSF data
- Testing result
- Log Data deletion
- Changing TSF data threshold
- Actions to be taken caused by Security violations
- Authorized administrator role registration, changing, and deletion
- Time changing caused by time synchronization
- Denial of allocation operation due to resource limits
- Interworking session termination due to session termination mechanism
- DB backup, restoration, and backup reservation

For the events above, save these information on audit record at least.

- Event date
- Event type
- Identification of subject and object
- Event result

7.1.1.2 Security Audit Inquiry (WFAU_SAR)

Security audit inquiry is classified into Intrusion Event Inquiry (WFAU_SAR_EVENT) and Security Audit Inquiry (WFAU_SAR_AUDIT).

(1) Intrusion Event Inquiry (WFAU_SAR_EVENT)

Intrusion event inquiry function is:

① Authorized administrator makes inquiries for the all audit log.

② Saved audit log about intrusion event is provided in a various form so that the user can interpret the information, such as table, graph, or chart.

③ The contents of intrusion event audit log is printed as time, event type, or result based regarding to standard down below. Printed search result can be sorted and inquired by each objective based. And also inquiry by internal user and external user based, such as internal-internal, internal-external, external-external, or external-internal is available.

- By time based: Audit log generated date and time
- By event type based: Subject and object of audit log (Server IP address, Server port, User(Operator)ID, configuration details, etc.), Intrusion Detection/Prevention substances (The number of intrusion detection, attackers, victims, attempts, attack types, traffic, blocks, attacker IP, victim IP, packet, etc.)
- By result based: Intrusion response result (Alert, Blocking, Data transmission to control center)

(2) Security Audit Inquiry (WFAU_SAR_AUDIT)

Security audit inquiry function is:

① Authorized administrator makes inquiries for the entire audit log event.

- Super Administrator: Inquires all the gathered audit data.
- General Administrator: Inquires the audit data related to detection details and drop details only.

② Saved audit log about security audit event is provided in a table form so that the user can interpret the information.

③ The contents of security audit log is printed as time, event type, or result based regarding to standard down below.

- By time based: Audit event generated date and time
- By event type based: Subject and object of audit event (User(Operator) ID, Operator IP Address, Configuration, etc.)
- By result based: Audit event result

7.1.1.3 SFR Mapping

Functions		SFR Mapping
Security Audit Generation (WFAU_GEN)	Intrusion Event Data Gathering (WFAU_GEN_EVENT)	FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association
	Security Audit Data Gathering (WFAU_GEN_AUDIT)	FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association
Security Audit Inquiry (WFAU_SAR)	Intrusion Event Inquiry (WFAU_SAR_EVENT)	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FAU_SEL.1 Selective audit
	Security Audit Inquiry (WFAU_SAR_AUDIT)	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FAU_SEL.1 Selective audit

[Table-20] Security Audit SFR Mapping

7.1.2 User Data Protection (WFDP)

User data protection performs these functions.

- Intrusion detection (WFDP_DET)
- Intrusion Prevention (WFDP_BLK)
- Intrusion Response (WFDP_ACT)

7.1.2.1 Intrusion Detection (WFDP_DET)

Intrusion detection is intrusion analysis policy, and classified into Anomaly protocol detection (WFDP_DET_PROTOCOL), Signature based detection (WFDP_DET_SIGNATURE), Statistics analysis based detection (WFDP_DET_STATISTIC), and Application layer stare analysis detection (WFDP_DET_ALSI).

Intrusion Analysis Policy is basically configured with Detection, Blocking, Risk Level, RCLS, LCRS, LCLS, Attack Recognition Count, Attack Recognition Time, and Time limitation.

Intrusion analysis policies detect the intrusion events by analyzing the traffic that inflows from the external, and take measures as the response process of the detected policy.

- Event Occurred Time: Start Time, End Time
- Attack Information: Source IP, Protocol, Port, User information of Source IP
- Victim Information: Destination IP, Protocol, Port information
- Attack Detection: Attack Name, Attack Code(Identification of Security Violated Event), Attack Categorization, Risk Level of Attack, Attack Recognition Count, Attack Recognition Time, Limitation Time
- Attack State Information: Finished, On Progress
- Information: Data size of the traffic detected as intrusion event, TTL, Protocol, Service Information

(1) Anomaly Protocol Detection (WFDP_DET_PROTOCOL)

It analyzes traffics from the external network, and detects invalid packets, which are against to protocol regulations such as TCP/UDP/ICMP/IP, as intrusion.

Detection policy category for anomaly protocol detection is described down below, and it includes Detection method, Attacker Summary, Victim Summary, Attacker Summary (IPv6), and Victim Summary (IPv6) beside default configuration.

- Protocol Vulnerability: It detects attacks that cause network or system overload by ill using protocol regulation problem, or attacks that down the server for interrupting normal services.

TOE make Data-link layer analysis first, and send it to Network layer protocol to analyze protocol in gathered packets.

Anomaly protocol detection function detects whether or not the protocol is normal, and protocol vulnerability attack type of security violation event lists.

(2) Signature Based Detection (WFDP_DET_SIGNATURE)

It analyzes traffics from the external network and compares them with SNIPER IPS signature list, and detects them as intrusion if analysis result is same.

Detection policy category for signature based detection is described down below, and includes Blocking method, Attacker Summary, Victim Summary, Attacker Summary (IPv6), and Victim Summary (IPv6) beside default configuration..

- Pattern block: It analyzes malicious traffics, such as Worm virus or One-way Attack, and detects the attacks with the unique attack pattern, which is extracted for accurate detection. It includes Protocol, Server port, Flow, and Detected character string as the additional properties.
- Web CGI: It detects the attacks that operate illegal command operation or authority acquisition by using CGI bug that Web provides. It includes Detected character string, type as the additional properties.
- Packet Header Detection: It detects administrator defined pattern by inspecting packet header. It includes Direction, Packet header, and Packet header mask as the additional properties.

Security violation event list defines whether attack or not with attack recognition count and time, and allows the session if the traffic is not an attack.

It detects the One way attack among network based system threaten attacks. Packets, which the protocol inspection is done, are compared with Web-CGI list with protocol, port, and packet data based. If the same rule is detected in Pattern block, Web-CGI, and Packet header detection list, and 'Protection' is set on the rule, TOE dumps the packet, and register it on the BlackHole list to protect for the registered time. If the 'protection' is not set on the rule, the packet passes the system.

(3) Statistics Analysis Based Detection (WFDP_DET_STATISTIC)

It statistically analyzes traffics from the external network and compares them with SNIPER IPS IPS, Service, Protocol threshold that is set on the SNIPER IPS by manually, and detects them as intrusion if the traffic excesses the threshold.

Detection policy category for Statistics analysis based detection is described down below, and it includes Detection method with threshold setting and manual threshold beside default configuration.

- Service Statistics Analysis: It detects the anomaly behavior and computer resource usage, analyzes traffic progress of each service port, and detects anomaly symptoms on network when the network is normally operated.
- Protocol Statistics Analysis: It detects the anomaly behavior and computer resource usage, analyzes traffic progress of each protocol, and detects anomaly symptoms on network when the network is normally operated.

TOE statistically analyzes the traffic progress in normal network status, and checks anomaly symptoms on network.

Set the threshold by manually, and detects the traffic as intrusion if the traffic excesses the threshold.

(4) Application Layer State Analysis Detection (WFDP_DET_ALSI)

It Reassemble/Normalizes traffics from the external network and detects the fragmentation attacks on Layer3, Layer5~7 of OSI 7 layers.

Detection policy category for Application layer stare analysis detection is described down below, and it includes Blocking method, Attacker Summary, Victim Summary, Attacker Summary (IPv6), and Victim Summary (IPv6) beside default configuration. In case of User defined category, Protocol, Port, Flow, and Detected character string are included.

- Denial of Service attack: Attackers transmit the fake/false packets to victims to not operating normal service, it detects the attacks that lower the system performance and interrupt normal service by increasing network traffic or exhausting system resources (CPU, Memory, etc.).
- Information gathering: It detects the attacks that the attackers check the victim information such as server vulnerability, system vulnerability, or whether or not the firewall is installed before they attack specific server or system.
- Service Attack: It detects the attacks that operate the command or acquire authority by illegally access to server with the vulnerability of Overflow Bug or each service, which is the software parameter management problem.
- User Defined: The administrator sets up the detection policy as wanted, and detects the attack by the policy based.

7.1.2.2 Intrusion Blocking (WFDP_BLK)

Intrusion Prevention is classified into Firewall policy based blocking (WFDP_BLK_FW) and Dynamic block list based blocking (WFDP_BLK_DYNAMIC).

(1) Firewall Policy Based Blocking (WFDP_BLK_FW)

TOE allows or blocks packets by comparing with firewall policy.

TOE firewall classifies and registers packets by object (by Host/Network), group, or domain based, registers the service so that it can set blocking and allowing policy.

Default setting for firewall policy is set to drop the entire packets, and the administrator can set the Accept or Drop policy to allow or block the packets.

TOE compares and take measures based on the policy (Accept/Drop) for the Interface applied on Firewall Policy, Source Address (IP Address), Destination Address (IP Address), Service (Protocol/Port), Policy (Accept/Drop), Flow Information (Request/Response), and Objective information (IP bandwidth policy information registered on IP POOL) when unauthorized external IT entity of Information Senders are transmitted from subject to the others through TOE. At this moment, it the traffic accepts rule exists, that session passes TOE.

Session content that is allowed to passes the firewall is:

- Allowed session by ACCEPT rule on firewall policy.

(2) Dynamic Block List Based Blocking (WFDP_BLK_DYNAMIC)

Dynamic Block List Based Blocking (WFDP_BLK_DYNAMIC) is classified as Intrusion Drop Policy.

It blocks the intrusion if the traffic from the external network is same as the real-time blocking listed attacker address, destination address, protocol, and port information. Real-time blocking listed policy is dynamically controlled by timeout value based, and the case blocking policy is registered on real-time blocking list is:

- Blocking setting of Intrusion detection policy: It detects the security violated events by the attack types beside protocol statistical analysis and service statistical analysis among attack types of detection policy setting that the TOE basically provides. Attack types of detection policy setting are consist of behavior basis and signature basis, it blocks the intrusion of relevant attacks and registers them on the real-time drop list in case when each detected attack is set as 'Blocking' on the detection policy setting, and executes drop policy by maintaining the drop list on the relevant rule for the limitation time that the administrator configured.

- Blocking by real-time blocking list set by the administrator: The administrator can register the user IP to block, maintains blocking list as set, and operates blocking policy.

7.1.2.3 Intrusion Response (WFDP_ACT)

(1) Intrusion Alarm (WFDP_ACT_ALARM)

Read the security violations on memory, send the message of the detected contents to the administrator, and make alarms depending on the security violation level. Send the e-mail as set on the configuration for each security violation.

(2) Defense Policy Operation (WFDP_ACT_POLICY)

Defense the attack if the detection policy of the detected event is set as 'Defense'. And also, register the defense policy on the real-time blocking list with the gathered data for the detected attacks, maintain the policy for the set time limit by detection policy, and block the repeated attacks. Default time limit is 60 seconds.

In case when the traffic inflows to TOE over the performance limitation (Throughput) that TOE provides, it guarantees the bandwidth of the traffic and normal operation of TOE by not reading it but dropping.

In case when the traffic inflows over the performance limitation(Throughput) that the TOE provides, it guarantees the bandwidth of the traffic and normal operation of TOE by not reading the traffic but drop it.

(3) Control Center Data Transmission (WFDP_ACT_LINK)

Response for the security violated event, check the link status with ESM, control center, and send the security violation information to the ESM, control center.

SNIPER IPS supports the encryption protocol, which each security appliances supports, and interworking for the safe network connection for the transmitted data protection.

7.1.2.4 SFR Mapping

Functions		SFR Mapping
Intrusion Detection (WFDP_DET)	Anomaly Protocol Detection (WFDP_DET_PROTOCOL)	FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1(2) Simple security attributes (2) FIA_ATD.1(1) User attribute definition (1)
	Signature Based Detection (WFDP_DET_SIGNATURE)	FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1(2) Simple security attributes (2) FIA_ATD.1(1) User attribute definition (1)
	Statistics Analysis Based Detection (WFDP_DET_STATISTIC)	FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1(2) Simple security attributes (2) FIA_ATD.1(1) User attribute definition (1)
	Application Layer State Analysis Detection (WFDP_DET_ALSI)	FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1(2) Simple security attributes (2) FIA_ATD.1(1) User attribute definition (1)
Intrusion Blocking (WFDP_BLK)	Dynamic Block List Based Blocking (WFDP_BLK_DYNAMIC)	FDP_IFC.1(1) Subset information flow control (1) FDP_IFF.1(1) Simple security attributes (1) FIA_ATD.1(1) User attribute definition (1)
	Firewall Policy Based Blocking (WFDP_BLK_FW)	FDP_IFC.1(1) Subset information flow control (1) FDP_IFF.1(1) Simple security attributes (1) FIA_ATD.1(1) User attribute definition (1)
Intrusion Response (WFDP_ACT)	Intrusion Alarm (WFDP_ACT_ALARM)	FAU_ARP.1 Security alarms
	Defense Policy Operation (WFDP_ACT_POLICY)	FDP_IFC.1(1) Subset information flow control (1) FDP_IFF.1(1) Simple security attributes (1) FDP_IFC.1(2) Subset information flow control (2) FDP_IFF.1(2) Simple security attributes (2)
	Control Center Data Transmission (WFDP_ACT_LINK)	FAU_ARP.1 Security alarms

[Table-21] User Data Protection SFR Mapping

7.1.3 Identification and Authentication (WFIA)

Identification and Authentication performs the functions down below.

• User Identification and Authentication (WFIA_ACCESS)

7.1.3.1 User Identification and Authentication Function (WFIA_ACCESS)

(1) Identification and Authentication (WFIA_ACCESS_LOGIN)

Identification and Authentication (WFIA_ACCESS_LOGIN) provides identification method using password by SSL communication. All the users should register the accessed IP address when user ID registration, so the contents are transmitted with encrypted form by SLL method if the administrator enters ID and Password on the designated IP's client screen.

It blocks the identification and authentication leakage or re-usage between SNIPER IPS server and users by SSL encryption communication.

Transmitted data with encrypted form identifies and certificates the user by reading authentication and identification information DB on SNIPER IPS Server.

When the administrator enters the ID on the login window, it displays the information like "ID'*******'" to protect the account and password leakage. When identification, it only shows the message that indicates whether or not the success or fail, but the specific reason for success or fail does not displayed. And also if the normal login attempt is failed under the count the super-administrator set and the attempt exceeds the limitation, the system shows the error message, prohibits the access for five minutes, and sends the notification e-mail to the user and the administrator. TOE functions are operated normally only when the identification and authentication process is successfully finished, and TOE functions are not available before the identification and authentication process is done.

Password is done with the access to the local console by the administrator, and the strength of authentication mechanism is decided by probability and permutation mechanism.

ID and Password generation rule for user identification and authentication is:

a) ID Generation Rule

- The length of ID should be between 6~10 characters.
- ID cannot be made with one character.
- Numeric characters 0~9, small English letter a~z, capital English letter A~Z, and all the special characters on the keyboard are available for the ID.
- Capital letter and small letters can be combined for ID.

b) Password Generation Rule

- The length of Password shall be between 6~10 characters.
- ID and Password cannot be generated with same characters.
- Same numbers and characters cannot be used for password.
- Capital letter and small letters can be combined for password.

- Valid period for password is at least 1 to 99 days.
- Three types of characters, numbers and special characters, etc. shall be combined for password.
- Stored and encrypted with HMAC-SHA-256.

User Identification and Authentication Function (WFIA_ACCESS) strength of function related security function, SOF-Medium.

7.1.3.2 SFR Mapping

Functions		SFR Mapping
User Identification and Authentication Function (WFIA_ACCESS)	Identification and Authentication (WFIA_ACCESS_LOGIN)	FIA_AFL.1 Authentication failure handling FIA_UAU.2 User authentication before any action 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)

[Table-22] User Identification and Authentication Function SRF Mapping

7.1.4 Security Management (WFMT)

The administrator who can operate the security function is classified into super-administrator, security-administrator, and general-administrator.

The authority and role of each administrator is decided by the super-administrator, and the interface for the administrator setup is provided. Security management performs the functions down below.

- Configuration (WFMT_CONFIG)
- Policy Set-up (WFMT_POLICY)
- Login Failure Management (WFMT_LOGIN)
- Storage Device Management (WFMT_DBM)
- Live Update (WFMT_UPDATE)
- Time Synchronization (WFMT_SYNC)

7.1.4.1 Configuration (WFMT_CONFIG)

(1) Configuration (WFMT_CONFIG)

Configuration (WFMT_CONFIG) is classified into Timeout setup, Sending mail, Administrator management, Network, Control center setup, Mode setup, Packet gathering setup, and Status check setup.

- Timeout setup (WFMT_CONFIG_TIMEOUT)
- Sending mail (WFMT_CONFIG_MAIL)
- Administrator management (WFMT_CONFIG_ADMIN)
- Network (WFMT_CONFIG_NETWORK)
- Control center setup (WFMT_CONFIG_LINK)
- Mode setup (WFMT_CONFIG_MODE)
- Status check setup (WFMT_CONFIG_STATUS)
- IP Pool setup (WFMT_CONFIG_IPPOOL)

(1) Timeout setup (WFMT_CONFIG_TIMEOUT)

The super-administrator can set timeout to strengthen the security of the account.

The super-administrator can determine, enable, disable, or modify the action for the timeout function.

Select ‘Use’ to use the timeout function or ‘not-use’ for not using it.

When the super-administrator selects ‘Use’, the window for the timeout period setup is activated, and the default period is set as one minute.

Timeout period can be set between 1 to 60 minutes.

(2) Sending mail (WFMT_CONFIG_MAIL)

Super-administrator sets or modifies the mail sending details to notify the administrator when potential security violation event occurred.

TOE sends the e-mail to the administrator’s account when these potential violation events occurred.

- Storage Device Check: When the storage usage exceeds the threshold that the super-administrator set
- Login Failure: When login attempt failure occurred
- Integrity Check: When integrity error occurred on saved TSF data integrity inspection
- Packet Loss: When packet loss occurred on gathering port
- CPU Overload: When CPU overload exceeds 90%
- NIC Failure: When packet gathering interface downed

(3) Administrator management (WFMT_CONFIG_ADMIN)

Authorized administrator who uses SNIPER IPS operates registration, modification, or deletion of identification and authentication data regarding to the security roles.

Authority for TOE is:

- Super-administrator: Enable to operate the entire SNIPER IPS functions, and limited to only one person.
  Enable to operate the entire TOE functions, and have authority to use the entire functions such as real-time monitor, Summary report, Security audit, Configuration, Security policy, and other settings (Configurations, Timeout, Sending mail, Packet gathering, WINS Technet vulnerability DB, Help, Version information, Close, and Display setting).

- General-administrator: Enable to operate partial TOE functions.
  Real-time monitor and Summary report are available, but Security audit and Security policy are not.
  Personal information modification function on Configuration is available.
  Other settings (Configurations, Packet gathering, WINS Technet vulnerability DB, Help, Version information, Close, and Display setting) are available.

The authorized administrator sets the administrator ID, Password, Password check, Valid-period, Authority, Mobile phone number, E-mail address, and Note.

The super-administrator is enables to inquire, modify, delete, clear, and generate the entire administrator data, and the general-administrators are only enable to inquire, modify, and clear its own administrator data.

ID and Password generation rule for user identification and authentication is described down below.

a) ID Generation Rule
- The length of ID should be between 6~10 characters.
- ID cannot be made with one character.
- Numeric characters 0~9, small English letter a~z, capital English letter A~Z, and all the special characters on the keyboard are available for the ID.
- Capital letter and small letters can be combined for ID.

b) Password Generation Rule
- The length of Password should be between 6~10 characters.
- ID and Password cannot be generated with same characters.

- Same numbers and characters cannot be used for password.
- Capital letter and small letters can be combined for password.

• Valid period for password is at least 1 to 99 days.

(4) Network (WFMT_CONFIG_NETWORK)

The super-administrator configures Internal IP address, Security audit IP address, Security audit exception IP address, and Interface name setting of Network management function.

In internal IP address setting defines where SNIPER IPS protects, adds, modifies, or deletes the IP, Netmask, or Valid Address range. SNIPER IPS should be restarted after internal IP address setup.

Security audit address defined the IT objective that security audit is operated, adds, modifies, or deletes the IP, Netmask, or Valid Address range

Security audit exception address defined the IT objective that security audit is not operated, adds, modifies, or deletes the IP, Netmask, or Valid Address range

Interface name setting sets the input and output interface name of SNIPER IPS, modifies and applies the name.

(5) Control center setup (WFMT_CONFIG_LINK)

Super-administrator inquires, modifies, deletes, clears, or generates the communication method or detection information of ESM server, control server, or other IPS server where the interworking is set on control center setup.

Each interworking object has different IP, interworking port, and control interworking (interworking method).

To interwork with the objectives, SNIPER IPS sets server IP, Port, SNIPER identifier, control interworking, and applying.

(6) Mode setup (WFMT_CONFIG_MODE)

Super-administrator sets firewall mode and SNIPER mode for malicious traffic detection and blocking.

Mode setup is defined as Use and None use, and setup result is saved as security log.

Super-administrator inquires audit start time, audit end time, server IP address, server port, start ID, end ID, and configurations.

(7) Status check setup (WFMT_CONFIG_STATUS)

TOE provides integrity check and IPS status information management functions through the status check setup.

The administrator can verify the integrity on the IPS client screen.

Super-administrator sets, inquires, or modifies the integrity check period and automatic integrity inspection to check the saved audit record and whether or not configuration setup file has damaged.

By setting integrity check period, integrity inspection could be operated periodically.

IPS Server status information checks whether packet gathering interface is operated on the client screen. It provides the received and transmitted packet status on each packet gathering NIC interface.

Super-administrator sets failure control category of packet gathering interface (Line0, Line1) and heartbit. The

default value is 5 seconds.

Inquires CPU, Memory, Driver status of IPS server. Super-administrator can set driver information renewal cycle as manual or automatic – none, 5 seconds, 10 seconds, 15 seconds, or 30 seconds.

(8) IP Pool setup (WFMT_CONFIG_IPPOOL)

IP pool setup is the function that manages intrusion detection event or traffic information when IP bandwidth is controlled by group category by logical division of network bandwidth.

IP pool management provides the function that user can manage traffic information, which inflows through SNIPER IPS, by interface based.

The super-administrator can register, modify, or delete the IP bandwidth information through the IP pool management interface. IP pool management interface restricts the behavior determining and modifying functions to super-administrator.

7.1.4.2 Policy Set-up (WFMT_POLICY)

Policy setup is classified into detection policy setup (WFMT_POLICY_RULE) and blocking policy setup (WFMT_POLICY_BLK).

(1) Detection Policy Setup (WFMT_POLICY_RULE)

Super-administrator can inquire, modify, delete, generate, or renew with the latest data about security violation policy for intrusion detection.

Detection policy that SNIPER IPS detects is:

Attack type	Description	Action
Denial of Service	Attacker transmits the fake/false packets to victims to not operating normal service, it detects the attacks that lower the system performance and interrupt normal service by increasing network traffic or exhausting system resources (CPU, Memory, etc.).	query, modify
Information Gathering	It detects the attacks that the attackers check the victim information such as server vulnerability, system vulnerability, or whether or not the firewall is installed before they attack specific server or system.	query, modify
Protocol Vulnerability	It detects attacks that cause network or system overload by ill using protocol regulation problem, or attacks that down the server for interrupting normal services	query, modify
Service Attack	Attacker transmits the fake/false packets to victims to not operating normal service, it detects the attacks that lower the system performance and interrupt normal service by increasing network traffic or exhausting system resources (CPU, Memory, etc.).	query, modify

Web-CGI Attack	It detects attacks that illegal command operation or authority acquisition with the bug of CGI the web provides.	query, modify, delete, generate
User Defined	When the administrator finds the symptoms for the zero-day attack, registration for the arbitrary detection policy is available, and this policy detects the attacks.	query, modify, delete, generate
Protocol Statistical Analysis	It detects anomaly behavior or computer resource usage, analyzes each protocol's traffic progress when network is operated in normal, and detects the anomaly symptoms on network.	query, modify
Service Statistical Analysis	It detects anomaly behavior or computer resource usage, analyzes each protocol's traffic progress when network is operated in normal, and detects the anomaly symptoms on network.	query, modify, delete, generate
Pattern Block	It analyzes malicious traffic such as worm virus or one-way attack, and detects attacks with unique attack patterns that is extracted for accurate detection.	query, modify, delete, generate
Packet Header Detection	It detects pattern that the administrator defined by inspecting packet header.	query, modify, delete, generate

Intrusion detection policy is classified into each attack type category, and includes default properties such as detection, risk level, alarm, E-mail, Mobile phone, RCLS, LCRS, LCLS, attack count, attack time, time limitation, and RAW, and also attacker summary, victim summary, attacker summary (IPv6), and victim summary (IPv6). Each property value may be modified by the super-administrator.

Detection policy that is set by the super-administrator is saved with AES-256 Encryption Algorithm, and the administrator opens and applies the saved file in a proper time.

Detection policy setup for by each IPS is available when interworking with other IPS through control center interworking.

Detection policy update with the latest policy is available by using pattern update.

(2) Blocking Policy Setup (WFMT_POLICY_BLK)

Super-administrator can determine the behavior of, enable, disable, and modify the action on TOE blocking policy setup.

Blocking policy setting blocks the traffic by setting the drop details on the real-time drop list and by firewall policy setting.

It registers blocking setting on dynamic blocking list with real-time blocking list.

Super-administrator inputs the attacker IP that should be blocked, and sets the blocking method and time limitation.

Blocking method could be selected among Source IP based blocking (SN_SRC_IP), Destination IP based blocking, (SN_DST_IP), Source and Destination IP of packet, Blocking when Protocol is coincidence (SN_AND_IP), Blocking by the Source IP Port based (SN_SRC_SERV), and Blocking by the Destination IP Port based (SN_DST_SERV).
Default time limitation is 30 seconds.

Firewall policy can set firewall policy allowing/blocking, host, network, or group registration, modification, or deletion, which is essential for policy setup, service registration, modification, or deletion.
Super administrator sets the blocking policy by using the priority of policy, interface, source, destination, service, policy (Accept, Drop), log, and flow (Request, Response).
Default firewall policy is set as 'DROP' to block whole traffic. Default policy cannot be deleted, but the super-administrator can change it to 'ACCEPT' to allow whole traffic regarding to the policy.
Allowing rule will be added when default policy is set as 'block whole traffic (DROP)', and blocking rule will be added when 'allow whole traffic(ACCEPT)' is set.
The administrator opens the saved policy backup file on server and applies the policy on appropriate timing.
Firewall policy restricts determine the behavior of, enable, disable, and modify functions to super-administrator only.

7.1.4.3 Login Failure Management (WFMT_LOGIN)
Login failure management sets or modifies the login failure count when the user login attempts.
Super-administrator sets the login failure limitation between 1 and 3. Default setting is 3.

7.1.4.4 Storage Device Management (WFMT_DBM)
Storage device management is classified into Storage volume limitation setup (WFMT_DBM_LIMIT), DB backup/restoration management (WFMT_DBM_BAK).

(1) Storage volume limitation setup (WFMT_DBM_LIMIT)
To prevent the system down caused by the limitation of storage device threshold, the super-administrator secures a certain limitation, and sets the threshold and log preservation period for audit data loss prevention.
Threshold is the usage limitation, and the default option is 70%.
This audit data storage device usage limitation value (5~90%) is set by the super-administrator, and warning mail that the oldest log is being deleted automatically is sent to the super-administrator when usage limitation is exceeded.

(2) DB backup/restoration management (WFMT_DBM_BAK)
DB backup/restoration management sets the configuration for log data backup and restoration of storage device.
DB backup/restoration management is classified into DB backup, DB restoration, and DB backup reservation.

- DB Backup: SNIPER IPS provides data file backup function that is generated by TOE on HDD or

another storage device for securing the storage device volume, safe storage of saved data, and treating file damage. Super-administrator determines whether or not delete the data after backup for the availability of storage device after check whole volume size, used volume and enable volume, and setting backup period and backup route. Operation result of backup function is marked as task classification, start date, end date, operator ID, equipment name, period, whether or not the data deletion, and result.

- DB Restoration: Super-administrator performs the restoration of already saved data by selecting restore location and restore equipment. Define the backup data restoration location after checking whole volume, used volume, and enable volume. When DB restoration is done, restored result will be marked on the table by task classification, start date, end date, operator ID, equipment name, and result.
- DB Backup Reservation: Automatic backup is process as the super-administrator set by using DB backup reservation function. Super-administrator configures period, time, and whether or not the data deletion. Automatic backup is periodically operated by the period setting based. Period is selected by daily, weekly, monthly, or yearly, and set the backup operation time. Check whether or not delete data file after backup, set the file location and backup file name, and register it as reserved task.

7.1.4.5 Live Update (WFMT_UPDATE)

Live update performs the live update function for detection pattern update (WFMT_UPDATE_SNIPER).
It supports simple pattern type signature among Detection policy such as Web-CGI and Pattern Block.
Update file is encrypted with SHA-256 algorithm.
For the latest detection pattern update, it provides these two methods.

- Download the latest detection pattern update file from the Update Server by IPS Client and apply it on IPS Server.
- With the reservation function, downloading the latest detection pattern update file from the Update Server by IPS Client and apply it on IPS Server is also available. Update is operated on the date and time as the super-administrator configured, such as once a day / week / month.

Update interface restricts determine and modify functions to super-administrator only.

7.1.4.6 Time Synchronization (WFMT_SYNC)

TOE operates time Synchronization (WFMT_ SYNC_TIME) function to provide trusted time stamp of security audit.
Time Synchronization interface restricts determination and modification functions to super-administrator only.
Information, which is recorded on SNIPER IPS, follows the SNIPER IPS server time. If the SNIPER IPS server time is incorrect, the user cannot trust the information that TOE records. So, time Synchronization interface is provided to set IPS server time to GMT standard time.

7.1.4.7 SFR Mapping

Functions		SFR Mapping
Configuration	Timeout Setup	FMT_MOF.1 Management of security

(WFMT_CONFIG)	(WFMT_CONFIG_TIMEOUT)	functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_MTD.1(2) Management of TSF data (2) FMT_SMF.1 Specification of Management Functions
	Sending Mail (WFMT_CONFIG_MAIL)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions
	Administrator management (WFMT_CONFIG_ADMIN)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles FIA_ATD.1(2) User attribute definition(2)
	Network (WFMT_CONFIG_NETWORK)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions
	Control Center Setup (WFMT_CONFIG_LINK)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions
	Mode Setup (WFMT_CONFIG_MODE)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions
	Packet Gathering Setup (WFMT_CONFIG_PACKET)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions
	Status Check Setup (WFMT_CONFIG_STATUS)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions
	IP Pool setup (WFMT_CONFIG_IPPOOL)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(1) Management of TSF data (1) FMT_SMF.1 Specification of Management Functions
Policy Set-up	Detection Policy Setup	FMT_MOF.1 Management of security

(WFMT_POLICY)	(WFMT_CONFIG_RULE)	functions behaviour FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialisation FMT_SMF.1 Specification of Management Functions
	Blocking Policy Setup (WFMT_CONFIG_BLK)	FMT_MOF.1 Management of security functions behaviour FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialisation FMT_SMF.1 Specification of Management Functions
Login Failure Management (WFMT_LOGIN)	Login Failure Management (WFMT_LOGIN_FAIL)	FMT_MOF.1 Management of security functions behaviour FMT_SMF.1 Specification of Management Functions FAU_SAA.1 Potential violation analysis
Storage Device Management (WFMT_DBM)	Storage Volume Limitation Setup (WFMT_DBM_LIMIT)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(2) Management of TSF data (2) FMT_MTD.2 Management of limits on TSF data FMT_SMF.1 Specification of Management Functions FAU_SAA.1 Potential violation analysis
	DB Backup/Restoration Management (WFMT_DBM_BAK)	FMT_MOF.1 Management of security functions behaviour FMT_SMF.1 Specification of Management Functions
Live Update (WFMT_UPDATE)	Live Update (WFMT_UPDATE_SNIPER)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(2) Management of TSF data (2) FMT_SMF.1 Specification of Management Functions FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FCS_COP.1 Cryptographic operation
Time Synchronization (WFMT_SYNC)	Time Synchronization (WFMT_SYNC_TIME)	FMT_MOF.1 Management of security functions behaviour FMT_MTD.1(2) Management of TSF data (2) FMT_SMF.1 Specification of Management Functions

[Table-23] Security Audit SFR Mapping

7.1.5 TSF Protection (WFPT)

TSF Protection performs the operation down below.

- Transmitted Data Protection (WFPT_TDP)
- Status Check (WFPT_CHECK)
- Time Out (WFPT_TIME)

7.1.5.1 Transmitted Data Protection (WFPT_TDP)

(1) Transmitted Data Integrity Assurance (WFPT_TDP_HA)

It uses SSL Protocol to assure the confidentiality and integrity of the transmitted data for the communication between IPS Server and Client. Transmitted Data Integrity Assurance (WFPT_TDP_INT) provides the authentication methods such as Password via SSL communication or OTP (One Time Password). The segment where to transmit the data encodes the data by SSL Encryption, and the segment where to receive the data decodes the data by SSL Encryption to assure the integrity.

If an integrity error occurs while decoding process, it prevents leakage of the transmitted data by dropping the transmitted data so that it does not effect on the security function and by using SSL encryption. Integrity algorithm HMAC-SHA-2 of Transmitted Data Integrity Assurance satisfies Security Strength – Medium since it has low possibility that the low leveled attacker creates the same hash value. The strength of authentication mechanism is decided by probability and permutation mechanism.

Update Server and TOE communicates via SSL Protocol, and it assures the integrity through the SHA-256 algorithm hash value. The updated detection pattern data is encrypted by AES (256bits) and transmitted, and the Digital signature Algorithm is RSA (2048 bits). If the integrity is violated, IPS Client does not perform the update.

In case when the real-time detection and system information event, Raw data are transmitted to ESM Server, it assures the encrypted communication domain by using TLS 1.0.

(2) High Availability Function (WFPT_TDP_HA)

Transmitted Data Protection performs High Availability Function (WFPT_TDP_HA), which transmits the data to the assistant communication channel when SNIPER IPS failure occurred. When SNIPER IPS is installed with HA configuration, each SNIPER IPS checks the other SNIPER IPS operation status periodically as the administrator set, and shares transmitted data session table connection information.

When a failure occurred on IPS Server, the other installed IPS Server shares session table information and blacklist, which is serviced, so blocks the IP that the service is provided normally.

7.1.5.2 Status Check (WFPT_CHECK)

Status Check is classified into IPS Status Check (WFPT_CHECK_SYSTEM), Storage Data Integrity Assurance (WFPT_CHECK_INTEGRITY), and Storage Data Loss Protection (WFPT_CHECK_PROTECT).

(1) IPS Status Check (WFPT_CHECK_SYSTEM)

When TOE is being start-up, it first checks the safety by checking packet gathering interface and then gathers the packet. It does not read the packet before the safe status is checked, and no packet is passed the packet gathering interface before the TOE is safely start-up and becomes the operation mode.

When TOE is safely start-up and operation mode, it periodically checks the status of packet gathering interface (Line0, Line1).

When any failure occurred on packet gathering interface, it performs the function that follows failure control configuration of packet gathering interface.

IPS Server checks packet gathering interface every 3 seconds.

Based on the status check result, it displays green icon when packet gathering interface status is normal, and displays red icon when anomaly case. And also, it stops packet transmission by packet gathering interface link down, or transmits the data to assistant communication channel when HA function is available. When packet gathering information inspection result is Fail, it sends e-mail to super-administrator based on the configuration.

It checks CPU, Memory, Driver status of IPS Server. For CPU, the warning mail is sent to the configured administrator e-mail address in case more than 90% of total CPU usage rates last for more than 3 minutes. IPS server is not booted if CPU or Memory usage becomes 100%.

(2) Storage Data Integrity Assurance (WFPT_CHECK_INTEGRITY)

TOE should protect the saved file from the unauthorized deletion, and prevent unauthorized modification on audit record.

Storage data integrity can be checked by data identity such as SHA-256(160bits) encryption techniques, file authority, possessor, group, and modified data. When IPS Server operation, check the default network configuration information by checking integrity of files that is needed for operating. And also, integrity inspection interface is provided when administrator's request while operating or on the configured integrity inspection period, and the integrity inspection period can be set by super-administrator. Storage data that assure the integrity are made up with 5 types.

- Log storage execution file for execution file and log storage
- Security violation event list file
- Identification and authentication file
- Configuration file
- Administrator defined file

Warning mail and warning message is sent to the administrator when integrity error in storage file is detected.

(3) Storage Data Loss Protection (WFPT_CHECK_PROTECT)

To retain the storage device volume when its threshold is reached, it deletes the oldest traffic dump data, specific information of each service.

It periodically checks weather the audit data storage device usage exceeds 90%(maximum value) of the administrator configured threshold on every minute while TOE is being operated. And also, it periodically checks whether the entire available capacity of storage device is 1GB on every minute. If more than 90%(maximum value) of usage limitation is over or less than 1GB of the entire available capacity left, the warning mail that the oldest log is automatically deleted is sent to the administrator.
The administrator saves the important log data on another storage device by checking the warning mail.

7.1.5.3 Time Out (WFPT_TIME)

When any command is not inputted on the IPS client through the input media such as keyboard or mouse, etc. more than timeout value(default: 10minute) set by the administrator, it automatically close the IPS client to session termination between IPS server and IPS client.
TOE checks access time when the authorized user logins, and closes session when access time exceeds timeout, that is set by the administrator. Terminated session information is recorded as audit record.
If the access time is not exceeds the timeout value, it keep performs the security function.

7.1.5.4 SFR Mapping

Functions		SFR Mapping
Transmitted Data Protection (WFPT_TDP)	Transmitted Data Integrity Assurance (WFPT_TDP_INT)	FPT_ITT.1 Basic internal TSF data transfer protection FPT_ITI.1 Inter-TSF detection of modification FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FCS_COP.1 Cryptographic operation
	High Availability Function (WFPT_TDP_HA)	FPT_TDC.1 Inter-TSF basic TSF data consistency
Status Check (WFPT_CHECK)	IPS Status Check (WFPT_CHECK_SYSTEM)	FPT_TST.1 TSF Testing FAU_SAA.1 Potential violation analysis
	Storage Data Integrity Assurance (WFPT_CHECK_INTEGRITY)	FAU_STG.1 Protected audit trail storage FPT_TST.1 TSF Testing FAU_SAA.1 Potential violation analysis FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FCS_COP.1 Cryptographic operation
	Storage Data Loss Protection (WFPT_CHECK_PROTECT)	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 FPT_TST.1 TSF Testing

Time Out (WFPT_TIME)	Session Termination (WFPT_TIME_SESSION)	FTA_SSL.3 TSF-initiated termination

[Table-24] TSF Protection SFR Mapping

7.2 Security Function Rationale

Rationale of Security Function that TOE provides is suggested rationale by mapping the TOE security function and security functions requirements through SFR Mapping table on each paragraph of Chapter 7.1 Security Function.