PAS-K V2.2
Security Target Lite

Version 1.2

PIOLINK, Inc.
TEL 02-2025-6900
FAX 02-2525-6901
SITE www.piolink.com

History of the Document

Version	Date	Modification	Author
V1.0	2017-05-18	the first version	Ok Jeong
V1.1	2017-09-14	adding more details of new models	Ok Jeong
V1.2	2019-02-13	adding more details of new models	Ok Jeong

Table of Contents

Tables

Figures

1 Security Target Introduction

1.1 ST Reference

To identify this Security Target (ST), the terms are defined as follows.

Category	Description
ST Title	PAS-K V2.2 Security Target Lite
ST Version	V1.2
Author	PIOLINK, Inc.
Publication Date	February 13, 2019

1.2 TOE Reference

To identify the Target of Evaluation (TOE), the terms are defined as follows.

Category	Description
TOE Title	PAS-K V2.2
Firmware Version	PLOS-PASK-v2.2.4
Build Date	February 11, 2019
TOE Hardware Models	AS-K1716, PAS-K2424, PAS-K2824, PAS-K4024, PAS-K4224, PAS-K4424, PAS-K4824, PAS-K8220, PAS-K8620, PAS-K1800, PAS-K3200, PAS-K3600, PAS-K4300, PAS-K3200X, PAS-K5200, PAS-K5400, PAS-K5600
Developer	PIOLINK, Inc.
Keywords	network device, switch, router

1.3 TOE Overview

In this section, the major security properties of the TOE are explained, and the TOE operating environment as well as the non-TOE operating environment are identified.

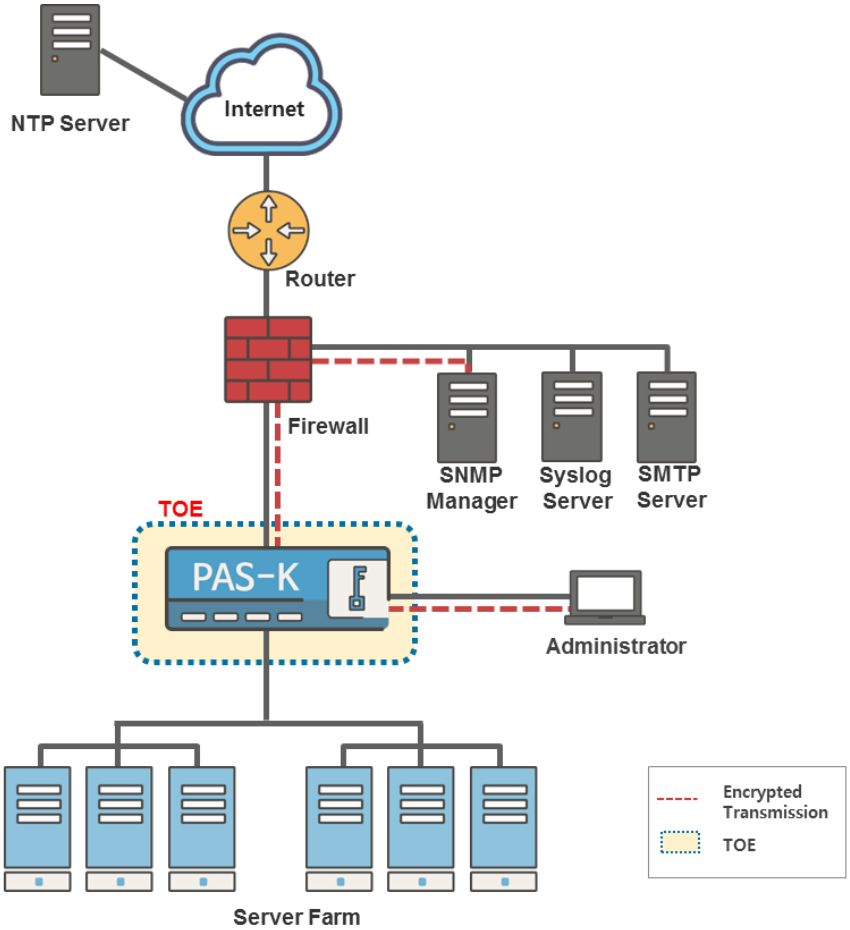
1.3.1 TOE Type

PAS-K V2.2 (hereafter referred to as “TOE”) is the network appliance as known as the L4/L7 switch for transmitting and controlling network packets from the source IT entity to the target IT entities. The TOE controls the traffic and transmits packets in front of IT products such as application servers which are linked to the internal network.

1.3.2 TOE Major Security Features

The TOE controls Layer 4/Layer 7 traffic and transmits packets according to the rules which the administrator has configured. As the security attributes which are used while processing the network traffic on the TOE, there are the protocol type of packets, source IP address, source port number, destination IP address, destination port number, packet contents, and TCP flag. The TOE allows or blocks IPv4 and IPv6 packets toward its network ports according to the control policy of the data flow which have been configured by the administrator.

This is an example of the TOE deployment.



[Figure 1-1] Example of the TOE Deployment

The TOE can be operated after deploying the network in the in-line structure at the point where the internal server farm is linked to the external network toward the Internet. The administrator can monitor and control the security features of the TOE on the security management CLI. The TOE controls the flow of unauthorized data and blocks anomalous packets after analyzing the details of all packets through the TOE, according to the user-defined security policies. Moreover, the network resource can be protected from SYN flood attacks as the SYN cookie feature is supported for the packets which are transmitted to the TOE interface. The TOE supports: the “security management” feature for the authorized administrators to handle the TOE more safely, the “identification and authentication” feature for controlling the access of unauthorized administrators, and the “security audit” feature for tracking violations of the security rules.

1.3.3 Non-TOE Hardware/Software/Firmware required by the TOE

The details of the hardware, software, and firmware for running the TOE are as follows.

[Table 1-1] Non-TOE Hardware/Software/Firmware

<table>
<tr><th></th><th>Description</th></tr>
<tr><td>Administrator's PC</td><td>This is the IT entity for the administrator to manage the TOE on the TOE security management interface.

<table>
<tr><th colspan="2">Category</th><th>Description</th></tr>
<tr><td colspan="2">OS</td><td>Microsoft Windows 7 Professional (32bit/64bit)</td></tr>
<tr><td colspan="2">S/W</td><td>supporting the protocols RS-232C and SSHv2</td></tr>
<tr><td rowspan="4">H/W</td><td>CPU</td><td>Intel Pentium 1.0 GHz or higher</td></tr>
<tr><td>Memory</td><td>2 GB or higher</td></tr>
<tr><td>HDD</td><td>20 GB or higher</td></tr>
<tr><td>NIC</td><td>1 or more units of 10/100 Mbps or higher</td></tr>
</table>
</td></tr>
<tr><td>NTP Server</td><td>This is the server which maintains the exact clock of the TOE by synchronizing the time through the NTP (Network Time Protocol).</td></tr>
<tr><td>SNMP Manager</td><td>This is the server which remotely checks the current status or configurations of the TOE through the SNMP (Simple Network Management Protocol). SNMPv3 shall be supported to communicate with the TOE.</td></tr>
<tr><td>SMTP Server</td><td>This is the server which sends alarm emails to the administrator through the SMTP(Simple Mail Transfer Protocol) if there are any violations of the security rules of the TOE.</td></tr>
<tr><td>Syslog Server</td><td>This is the server which remotely collects and manages the logs from the TOE. The TOE supports the feature which sends audit data (which is generated while running the TOE) to an external syslog server according to the security policy that the authorized administrator has specified.</td></tr>
<tr><td>Installer's PC at the Development Company</td><td>While upgrading the TOE firmware, the files are downloaded after connecting to the HTTPS server of the installer's PC at the development company.</td></tr>
</table>

1.4 TOE Description

In this section, there are the details on the operational environment, physical scope, and logical scope of the TOE.

1.4.1 Physical Scope of the TOE

The physical scope of the TOE includes: the network appliance, PLOS-PASK-v2.2.4 (which is stored as firmware), and the user guide and installation guide.

PLOS-PASK-v2.2.4

As the firmware which includes the software module with the security features (e.g. the firewall, SYN cookies, checking anomalous packets), operating system, and bootloader, this is distributed as the network appliance.

PAS-K V2.2 User Guide V1.4

As the document which describes the features of the TOE along with the details on how to use them, this document is distributed as the printed version or PDF file.

PAS-K V2.2 Installation Guide V1.3

As the document which describes all parts of the TOE's hardware along with the details on how to install them, this document is distributed as the printed version or PDF file.

Hardware

For the TOE, the 17 types of the hardware are: PAS-K1716, PAS-K2424, PAS-K2824, PAS-K4024, PAS-K4224, PAS-K4424, PAS-K4824, PAS-K8220, PAS-K8620, PAS-K1800, PAS-K3200, PAS-K3600, PAS-K4300, PAS-K 3200X, PAS-K5200, PAS-K5400, and PAS-K5600. The details are as follows

[Table 1-2] TOE Models

Hardware	Category		Description
PAS-K1716	CPU		1 x Intel Core Processor (dual-core, 3.70 GHz)
	RAM		4 GB
	SSD		40 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• copper port: 8 x 10/100/1000BASE-T, RJ-45 connectors • fiber port: 8 x 1000BASE-X SFP slots
	USB Port		1 x USB 2.0
	Acceleration Mode		N/A
PAS-K2424	CPU		1 x Intel Xeon Processor (quad-core, 3.10 GHz)
	RAM		16 GB
	SSD		40 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector

			• Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 16 x 1000BASE-X SFP slot
	USB Port		1 x USB 2.0
	Acceleration Mode		M04-L1
PAS-K2824	CPU		1 x Intel Xeon Processor (quad-core, 3.10 GHz)
	RAM		16 GB
	SSD		40 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• copper port: 8 x 10/100/1000BASE-T, RJ-45 connectors • fiber port: 16 x 1000BASE-X SFP slots
	USB Port		1 x USB 2.0
	Acceleration Mode		M08-L2
PAS-K4024	CPU		1 x Intel Xeon Processor (hexa-core, 2.20 GHz)
	RAM		12 GB
	SSD		40 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	----- Basic • fiber port: 16 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of 8 copper ports or 8 fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slot ----- Maximum • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 16 x 10GBASE-SR/LR SFP+ slot or • fiber port: 8 x 1000BASE-X SFP slot • fiber port: 16 x 10GBASE-SR/LR SFP+ slot
	USB Port		1 x USB 2.0
	Acceleration Mode		H06-L1
PAS-K4224	CPU		1 x Intel Xeon Processor (hexa-core, 2.20 GHz)
	RAM		12 GB

	SSD		40 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	----- Basic • fiber port: 16 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of 8 copper ports or 8 fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slot ----- Maximum • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 16 x 10GBASE-SR/LR SFP+ slot or • fiber port: 8 x 1000BASE-X SFP slot • fiber port: 16 x 10GBASE-SR/LR SFP+ slot
	USB Port		1 x USB 2.0
	Acceleration Mode		H12-L2
PAS-K4424	CPU		1 x Intel Xeon Processor (hexa-core, 2.20 GHz)
	RAM		24 GB
	SSD		40 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	----- Basic • fiber port: 16 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of 8 copper ports or 8 fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slot ----- Maximum • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 16 x 10GBASE-SR/LR SFP+ slot or • fiber port: 8 x 1000BASE-X SFP slot • fiber port: 16 x 10GBASE-SR/LR SFP+ slot
	USB Port		1 x USB 2.0
	Acceleration Mode		N/A
PAS-K4824	CPU		1 x Intel Xeon Processor (octa-core, 2.30 GHz)
	RAM		48 GB

	SSD		60 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	----- Basic • fiber port: 16 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of 8 copper ports or 8 fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slot ----- Maximum • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 16 x 10GBASE-SR/LR SFP+ slot or • fiber port: 8 x 1000BASE-X SFP slot • fiber port: 16 x 10GBASE-SR/LR SFP+ slot
	USB Port		1 x USB 2.0
	Acceleration Mode		N/A
PAS-K8220	CPU		2 x Intel Xeon Processor (octa-core, 2.00 GHz)
	RAM		64 GB
	SSD		160 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• fiber port: 4 x 40GBASE-SR4 QSFP+ slot • fiber port: 16 x 10GBASE-SR/LR SFP+ slot
	USB Port		1 x USB 2.0
	Acceleration Mode		N/A
PAS-K8620	CPU		2 x Intel Xeon Processor (dodeca-core, 2.70 GHz)
	RAM		128 GB
	SSD		160 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• fiber port: 4 x 40GBASE-SR4 QSFP+ slot • fiber port: 16 x 10GBASE-SR/LR SFP+ slot
	USB Port		1 x USB 2.0
	Acceleration Mode		N/A
PAS-K1800	CPU		1 x Intel Pentium Processor (dual-core, 2.20 GHz)
	RAM		----- Basic

			• Type 1: 1 x 4 GB • Type 2: 1 x 8 GB ----- Extended • Type 1: 1 x 4 GB • Type 2: 1 x 8 GB ----- Maximum • Type1: 8GB (2 x 4 GB) • Type2: 16GB (2 x 8 GB)
	SSD		• Type 1: 120 GB • Type 2: 256 GB • Type 3: 480 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• copper port: 12 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slot • fiber port: 2 x 10GBASE-SR/LR SFP+ slot
	USB Port		1 x USB 3.0
	Acceleration Mode		N/A
PAS-K3200	CPU		1 x Intel Xeon Processor (quad-core, 2.20 GHz)
	RAM		• Type 1: 16 GB (2 x 8 GB) • Type 2: 32 GB (2 x 16 GB)
	SSD		• Type 1: 120 GB • Type 2: 256 GB • Type 3: 480 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• copper port: 12 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slots • fiber port: 2 x 10GBASE-SR/LR SFP+ slots
	USB Port		• 1 x USB 3.0
	Acceleration Mode		• K3M01ADC-L1
PAS-K3600	CPU		• Intel Xeon Processor (quad-core, 2.20GHz)
	RAM		• Type 1: 16 GB (2 x 8 GB) • Type 2: 32 GB (2 x 16 GB)
	SSD		• Type 1: 120 GB • Type 2: 256 GB • Type 3: 480 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• copper port: 12 x 10/100/1000BASE-T, RJ-45 connector

			• fiber port: 8 x 1000BASE-X SFP slots • fiber port: 2 x 10GBASE-SR/LR SFP+ slots
	USB Port		1 x USB 3.0
	Acceleration Mode		K3M02ADC-L2
PAS-K4300	CPU		1 x Intel Xeon Processor (octa-core, 1.70 GHz)
	RAM		• Type 1: 16 GB (2 x 8 GB) • Type 2: 32 GB (2 x 16 GB)
	SSD		• Type 1: 120 GB • Type 2: 256 GB • Type 3: 480 GB
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	• copper port: 12 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slots • fiber port: 2 x 10GBASE-SR/LR SFP+ slots
	USB Port		1 x USB 3.0
	Acceleration Mode		N/A
PAS-K3200X	CPU		1 x Intel Xeon Processor (quad-core, 2.20 GHz)
	RAM		----- Basic • Type 1: 16 GB (2 x 8 GB) • Type 2: 32 GB (2 x 16 GB) ----- Extended: N/A ----- Maximum: N/A
	SSD		----- Basic • Type 1: 120 GB • Type 2: 256 GB • Type 3: 512 GB ----- Extended: N/A ----- Maximum: N/A
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	----- Basic • fiber port: 12 x 1000BASE-X SFP slot • fiber port: 4 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of 8 copper ports or 8 fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 1000BASE-X SFP slot ----- Maximum • fiber port: 12 x 1000BASE-X SFP slot • fiber port: 4 x 10GBASE-SR/LR SFP+ slot

			• copper port: 8 x 10/100/1000BASE-T, RJ-45 connector or • fiber port: 12 x 1000BASE-X SFP slot • fiber port: 4 x 10GBASE-SR/LR SFP+ slot • fiber port: 8 x 1000BASE-X SFP slot
	USB Port		1 x USB 3.0
	Acceleration Mode		N/A
PAS-K5200	CPU		1 x Intel Xeon Processor (hexa-core, 1.90 GHz)
	RAM		----- Basic • Type 1: 16 GB (2 x 8 GB) • Type 2: 32 GB (2 x 16 GB) ----- Extended: N/A ----- Maximum: N/A
	SSD		----- Basic • Type 1: 120 GB • Type 2: 256 GB • Type 3: 512 GB ----- Extended: N/A ----- Maximum: N/A
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	----- Basic • fiber port: 16 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of copper ports or fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 10GBASE-SR/LR SFP+ slot • fiber port: 2 x 40GBASE-SR4 QSFP+ slot ----- Maximum • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector or • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • fiber port: 8 x 10GBASE-SR/LR SFP+ slot or • fiber port: 16 x 10GBASE-SR/LR SFP+ slot fiber port: 2 x 40GBASE-SR4 QSFP+ slot
	USB Port		1 x USB 3.0
	Acceleration Mode		N/A
PAS-K5400	CPU		1 x Intel Xeon Processor (octa-core, 1.70 GHz)

	RAM		----- Basic 32 GB (2 x 16 GB) ----- Extended: N/A ----- Maximum: N/A
	SSD		• Type 1: 120 GB • Type 2: 256 GB • Type 3: 512 GB ----- Extended: N/A ----- Maximum: N/A
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector
		Ethernet Port	----- Basic • fiber port: 16 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of copper ports or fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 10GBASE-SR/LR SFP+ slot • fiber port: 2 x 40GBASE-SR4 QSFP+ slot ----- Maximum • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector or • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • fiber port: 8 x 10GBASE-SR/LR SFP+ slot or • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • fiber port: 2 x 40GBASE-SR4 QSFP+ slot
	USB Port		• 1 x USB 3.0
	Acceleration Mode		• N/A
PAS-K5600	CPU		• 1 x Intel Xeon Processor (dodeca-core, 1.50 GHz)
	RAM		----- Basic • 64 GB (2 x 32 GB) ----- Extended: N/A ----- Maximum: N/A
	SSD		----- Basic • Type 1: 120 GB • Type 2: 256 GB • Type 3: 512 GB ----- Extended: N/A ----- Maximum: N/A
	NIC	Management Port	• console port: 1 x RJ-45 connector • Ethernet port: 1 x RJ-45 connector

		Ethernet Port	----- Basic • fiber port: 16 x 10GBASE-SR/LR SFP+ slot ----- Extended *You may select an additional set of copper ports or fiber ports. • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector • fiber port: 8 x 10GBASE-SR/LR SFP+ slot • fiber port: 2 x 40GBASE-SR4 QSFP+ slot ----- Maximum • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • copper port: 8 x 10/100/1000BASE-T, RJ-45 connector or • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • fiber port: 8 x 10GBASE-SR/LR SFP+ slot or • fiber port: 16 x 10GBASE-SR/LR SFP+ slot • fiber port: 2 x 40GBASE-SR4 QSFP+ slot
	USB Port		• 1 x USB 3.0
	Acceleration Mode		• N/A

※ Acceleration Mode: As the value for processing packets, this is composed of the “product identifier code” part and “level” part. The details are as follows.

- M04-L1: PAS-K2424’s acceleration mode of packet forwarding is supported as Level 1 (4 Gbps).
- M08-L2: PAS-K2824’s acceleration mode of packet forwarding is supported as Level 2 (8 Gbps).
- H06-L1: PAS-K4024’s acceleration mode of packet forwarding is supported as Level 1 (6 Gbps).
- H12-L2: PAS-K4224’s acceleration mode of packet forwarding is supported as Level 2 (12 Gbps).
- K3M01ADC-L1: PAS-K3200’s acceleration mode of packet forwarding is supported as Level 1 (6 Gbps).
- K3M02ADC-L2: PAS-K3600’s acceleration mode of packet forwarding is supported as Level 2 (12 Gbps).

1.4.2 Logical Scope of the TOE

Security Audit (FAU)

When there is an event about one of the currently defined audit target, the TOE generates audit data which includes the date and time of the event as well as the information on who it was from (based on the reliable timestamp). In addition, the TOE supports the feature for the authorized administrator to search and check audit data. Moreover, the loss of audit data is prevented by overwriting data from the oldest after checking the space of the audit file storage when the storage reaches its threshold.

Cryptographic Support (FCS)

The TOE prevents leaking and falsifying important data of the TSF and supports the encryption feature to guarantee the integrity.

- **encryption of stored data**: SNMP setting (AES-CBC-256), administrator's password (SHA2-512)
- **encryption of transmitted data**: SSHv2 management access(AES-CBC-256, HMAC-SHA2), SNMPv3(AES-CFB-128, HMAC-SHA1)
- **checking the integrity:** TSF test (SHA2-512), firmware update (SHA2-512)

User Data Protection (FDP)

The TOE supports the following security policies to protect the TOE and the network resources (which are connected to the TOE) from the attacks and threats from the network.

- **Firewall Policy (IPv4/IPv6)**:
  The network resource can be protected by blocking the transmission of unauthorized traffic with filters of various options. When packets are transmitted to the TCP/IP kernel through the network interface card, the TOE allows packets if the value of the firewall policy is "allow" and drops packets if the value is "drop", after comparing security properties such as the protocol type, source IP address, source port number, destination IP address, destination port number, contents of packets, and TCP flags according to the firewall policies on the list.

- **SYN Cookies (IPv4)**:
  This is for protecting the network resource by blocking DoS attacks such as the SYN flood. When the client sends TCP SYN packets to the TOE interface, these packets are stored in the queues which have been allowed on the firewall policy. The firewall policies allocate up to 65535 queues on each destination port. When the queues are full, the TOE includes cookie values in the TCP SYN/ACK packets toward the client. Meanwhile, instead of maintaining the half-open status, SYN flood attacks are blocked while allowing normal accesses by opening sessions only (when TCP ACK responses are transmitted by allocating memories for receiving TCP ACK packets from the clients).

- **Blocking Anomalous Packets (IPv4)**:
  By checking the validity of TCP headers, the checksum of TCP packets, TCP flags, and the validity of IP headers, the network is protected against malicious traffic by blocking/allowing anomalous ones and allowing normal ones among the packets which have been transmitted to the TOE.
  - checking the validity of the TCP header: If the header of a packet is smaller than 20 bytes or if the actual length is different from the length information on the header, this packet is considered as anomalous and blocked/allowed according to the administrator's setting.

- checking the checksum of the TCP packet: If the checksum value (which is indicated on the TCP header) is different from the actual checksum value, this packet is considered as anomalous and blocked/allowed according to the administrator's setting.
- checking the TCP flag: If the combination of the TCP header flag is incorrect or if there are no settings, this packet is considered as anomalous and blocked/allowed according to the administrator's setting.
- checking the validity of the IP header: If the header length (which is indicated on the IP header) is bigger than the total packet length or if the indicated total packet length is bigger than the actual packet length, this packet is considered as anomalous and blocked.

Identification and Authentication (FIA)

The TOE performs the distinguishing and authenticating steps with the password-based authentication mechanism to guarantee the authorized administrators to access to the login interface with the local connection (through the console port) and management connection (through SSH). The TOE and sessions are maintained for the administrator who has been authorized with the identifying/authenticating features. If there are no inputs or activities, the authentication step is started again after closing the current session. Moreover, another administrator with the same ID or authority level is restricted from logging in to the system at the same time. While logging in to the TOE remotely through SSH, the access is restricted by allowing specific IP addresses.

Security Management (FMT)

The TOE supports the security management features with the local connection (through the console port) and management connection (through SSH). For the management connection from a remote place, the encrypted interface is provided with the SSH. Only the authorized administrators can configure security policies, and only the superuser can manage all of the administrators' accounts. The authorized administrators can use the management features such as configuring the details and descriptions on the security features of the TOE, according to their authority levels.

Protection of the TSF (FPT)

To guarantee the correct operation, the TOE runs the self-test on its main processes (while starting the system or when the authorized administrator requests) and tests the integrity (while starting the system, according to the period value while running the system, or when the authorized administrator requests).

The TOE tests the statuses of the fans, memories, LCD, and power supply units to check the running status of the main parts on the system (while starting the system or when the authorized administrator requests), and displays the current status on the LED at the front panel for the authorized administrators to respond to the troubles. The TOE send notification emails as the alarm feature if there are any troubles on these parts.

The TOE supports firmware updates to improve the security features and fix security vulnerabilities. Only the authorized administrators can update the firmware, and the update files are verified by checking hash values before the updating process. The TOE encrypts and stores the administrators' passwords along with the passwords for the SNMP authentication and encryption, before storing them on the storage which is controlled by the TSF.

TOE Access (FTA)

For more safety of the management, The TOE supports the feature of automatically terminating sessions after the configured time interval of the administrator's inactivity after logging in to the TOE management interface. Moreover, if there is an attempt of logging in with the superuser's ID or authority level while the superuser is logged in to the TOE management interface, this attempt is blocked.

Trusted Path/Channels (FTP)

The TOE prevents the disclosure and modification of the data/information by unauthorized users, with secure channels which use the encryption protocol of SSH. Moreover, the TOE supports secure channels with the SNMPv3 for the interoperation feature for the SNMP managers.

.

1.5 Conventions

The notation, formatting and conventions used in this ST are consistent with the Common Criteria(CC) for Information Technology Security Evaluation.

The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this ST

Iteration
Iteration is used when a component is repeated with varying operations. The result of iteration is marked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.).

Assignment
This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection
This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized*.

Refinement
This is used to add details and thus further restrict a requirement. The result of refinement is shown in **bold text**.

1.6 Terms and Definitions

The overlapping terms and definitions in this Security Target follow the Common Criteria for Information Technology Security Evaluation.

Administrator PC
a personal computer of the administrator to control the TOE with the local access or management access

Accept
processing packets (which are received on the device) according to the access rules

Assets
entities that the owner of the TOE presumably places value upon

Assignment
the specification of an identified parameter in a component (of the CC) or requirement

Augmentation
addition of one or more requirement(s) to a package

Authentication Data
information used to verify a user's claimed identity

Authorized Administrator
authorized user to securely operate and manage the TOE

Authorized User
TOE user who may, in accordance with the SFRs, perform an operation

Attack Potential
measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources and motivation

Class
set of CC families that share a common focus

Content
a firewall rule which refers to the strings in the payload of packets

Component
smallest selectable set of elements on which requirements may be based

Dependency
relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Drop
discarding packets (which are received on the device) according to the access rules

Element
indivisible statement of a security need

Evaluation Assurance Level (EAL)
set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

External Entity
human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Family
set of components that share a similar goal but differ in emphasis or rigor

Filter
a condition for accepting or dropping packets while the firewall feature is enabled

Identity
representation uniquely identifying entities (e.g. user, process, or disk) within the context of the TOE

Installer's PC of the Developers

a personal computer of an installer (from one of the developers) for updating the TOE firmware

Iteration
use of the same component to express two or more distinct requirements

Local Access
the access to the TOE by using the console port to manage the TOE by administrator, directly

Management Access
the access to the TOE by using the HTTPS, SSH, TLS, IPSec, etc. to manage the TOE by administrator, remotely

Monitoring User
the administrator who is granted the authority of checking the security feature settings and audit logs of the TOE

NTP Server
the server (which provides the data of the current time on the network) for maintaining the accuracy of the system time

Object
passive entity in the TOE containing or receiving information and on which subjects perform operations

Operation (on a component of the CC)
modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation (on an object)
specific type of action performed by a subject on an object

Organizational Security Policies
set of security rules, procedures, or guidelines for an organization wherein the set is currently given by actual or virtual organizations, or is going to be given

Packet Rate
the amount of packets which can be transmitted during a specific period of time

Port
physical connection port on the outside of network device

Protection Profile (PP)
implementation-independent statement of security needs for a TOE type

Queue
As the queue for waiting for the requests of the network connection, this is a memory where the details of the connections with the TOE.

Rate
processing packets (which are received on the device) according to the access rules, up to the configured value

Refinement
addition of details to a component

Role
predefined set of rules on permissible interactions between a user and the TOE

Security Target (ST)
implementation-dependent statement of security needs for a specific identified TOE

Selection
specification of one or more items from a list in a component

SMTP Server
the server which transmits emails through the SMTP (Simple Mail Transfer Protocol)

SNMP Manager
a server for monitoring devices (e.g. switches, routers) through the SNMP (Simple Network Management Protocol)

Subject
active entity in the TOE that performs operations on objects

Superuser
the administrator who is granted the authority of managing all security features of the TOE

SYN Cookies
As the feature for blocking SYN floods, this transmits TCP SYN/ACK response packets for the TCP SYN from the client after inserting the SYN cookie values. After this, the transmission is allowed for the clients who have replied with normal TCP ACK packets.

Syslog Server
a server which collects and manages system logs which are generated on the device

Target of Evaluation (TOE)
set of software, firmware and/or hardware possibly accompanied by guidance

Threat Agent
entity that can adversely act on assets

TOE Security Functionality (TSF)
combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data
data for the operation of the TOE upon which the enforcement of the SFR relies

User
administrator in network device

2 Conformance Claims

In this chapter, there are the details on this Security Target's conformance to the Common Criteria for Information Technology Security Evaluation, Protection Profiles, and Package.

2.1 Conformance to Common Criteria

This Security Target conforms to the following Common Criteria.

Common Criteria Identification

- Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
  - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
  - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
  - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.

Common Criteria Conformance

- Common Criteria for Information Technology Security Evaluation, Part 2 Extended (FMT_PWD.1, FPT_PST.1, FPT_TUD.1, FTA_SSL.5)
- Common Criteria for Information Technology Security Evaluation, Part 3 Conformant

2.2 Conformance to Protection Profiles

This Security Target conforms to the following protection profile.

Identification of the Protection Profile

- Korean National Protection Profile for Network Device V1.1 (Certification Number: KECS-PP-0714a-2016)

Protection Profile Conformance

- Korean National Protection Profile for Network Device V1.1: "**strict** Protection Profile conformance"

2.3 Conformance to Packages

This Security Target conforms to the following package.

- Assurance Package: EAL1 augmented by ATE_FUN.1

2.4 Conformance Claim Rationale

This Security Target conforms to the following Protection Profiles, according to the requirements on Korean National Protection Profile for Network Device V1.1 (hereafter also referred to as “K-NDPP” without the version).

- Protection Profile conformance method: “**strict** Protection Profile conformance”
- TOE type conformance: The TOE type is in conformance with the TOE type described in the Protection Profile. For more information on this point, please refer to chapter 1.3 of this Security Target

The PP conformance claim rationale is as follows.

2.4.1 Security Objectives Related Conformance Claim

[Table 2-1] indicates that the security objectives of this Security Target is equal to those of K-NDPP.

[Table 2-1] Security Objectives Related to Conformance Claim Rationale

Security Objectives for Operational Environment	Rationale
OE.PHYSICAL_CONTROL	Equivalent to the PP: The security objectives in this ST are defined as same as the PP.
OE.SECURITY_MAINTENANCE	
OE.TRUSTED_ADMIN	
OE.PATCH_MANAGEMENT	
OE.LOG_BACKUP	

2.4.2 SFR related Conformance Claim Rationale

The following table indicates that the SFRs of this Security Target are equivalent to or more restrictive than the SFRs of the K-NDPP.

[Table 2-2] Security Functional Requirements Related to Conformance Claim Rationale

Class	PP SFR	ST SFR	Rationale
FAU	FAU_GEN.1	FAU_GEN.1	Equivalent to the PP.
	FAU_SEL.1	FAU_SEL.1	
	FAU_STG.1	FAU_STG.1	
	FAU_STG.3	FAU_STG.3	
	-	FAU_SAR.1	More restrictive than the PP. This ST shall define the additional SFR to review audit data based on the log type, level, and keyword.
	-	FAU_SAR.3	

Class	PP SFR	ST SFR	Rationale
FCS	FCS_CKM.1	FCS_CKM.1(1)	Equivalent to the PP. The ST added this SFR using Iteration Operation defined in the PP.
		FCS_CKM.1(2)	
		FCS_CKM.1(3)	
	FCS_CKM.2	-	This does not need to be implemented as it is optional SFR in the PP.
	FCS_CKM.4	FCS_CKM.4	Equivalent to the PP.
	FCS_COP.1	FCS_COP.1(1)	Equivalent to the PP. The ST added this SFR using Iteration Operation defined in the PP.
		FCS_COP.1(2)	
		FCS_COP.1(3)	
		FCS_COP.1(4)	
		FCS_COP.1(5)	
		FCS_COP.1(6)	
		FCS_COP.1(7)	
FDP	FDP_IFC.2	FDP_IFC.2(1)	Equivalent to the PP.
		FDP_IFC.2(2)	
		FDP_IFC.2(3)	
	FDP_IFF.1	FDP_IFF.1(1)	
		FDP_IFF.1(2)	
		FDP_IFF.1(3)	
FIA	FIA_AFL.1	FIA_AFL.1	Equivalent to the PP.
	FIA_SOS.1	FIA_SOS.1	
	FIA_UAU.1	FIA_UAU.1	
	FIA_UAU.7	FIA_UAU.7	
	FIA_UID.1	FIA_UID.1	
	-	FIA_ATD.1	More restrictive than the PP. This ST shall define the additional SFR to maintain the security attribute lists for individual users.
FMT	FMT_MOF.1	FMT_MOF.1	Equivalent to the PP.
	FMT_MSA.1	FMT_MSA.1	
	FMT_MSA.3	FMT_MSA.3	
	FMT_MTD.1	FMT_MTD.1	
	FMT_PWD.1(Extended)	FMT_PWD.1(Extended)	
	FMT_SMF.1	FMT_SMF.1	

Class	PP SFR	ST SFR	Rationale
	FMT_SMR.1	FMT_SMR.1	
FPT	FPT_PST.1(Extended)	FPT_PST.1(Extended)	Equivalent to the PP.
	FPT_STM.1	FPT_STM.1	
	FPT_TEE.1	FPT_TEE.1(1)	
		FPT_TEE.1(2)	
	FPT_TST.1	FPT_TST.1	
	FPT_TUD.1(Extended)	FPT_TUD.1(Extended)	
FTA	FTA_MCS.2	FTA_MCS.2	Equivalent to the PP.
	FTA_SSL.5 (Extended)	FTA_SSL.5(Extended)	
	FTA_TSE.1	FTA_TSE.1	
FTP	FTP_ITC.1	FTP_ITC.1	Equivalent to the PP.
	FTP_TRP.1	FTP_TRP.1	

3 Security Objectives

3.1 Security Objectives for the Operational Environment

[Table 3-1] Security Objectives

Security Objective	Description
OE.PHYSICAL_CONTROL	The TOE shall be located in physically secure environment to which only the authorized administrator is allowed to access and the protective facilities are provided.
OE.SECURITY_MAINTENANCE	When the internal network environment changes due to the change in network configuration, increase/decrease of host and increase/decrease of service, etc., the changed environment and security policies shall be immediately reflected to the TOE operational policies in order to maintain the same level of security as before.
OE.TRUSTED_ADMIN	The authorized administrator of TOE shall be non-malicious users, have appropriately trained for TOE management functions and accurately fulfill the duties in accordance with administrator guidance.
OE.PATCH_MANAGEMENT	The authorized administrator regularly applies the latest patches for the firmware of network device and software used in the device. If the source of patch files cannot be verified, the installation of patch files shall be restricted. After updates, the authorized administrator checks that disused or unnecessary services are disabled and blocks the interfaces connected to the disused port.
OE.LOG_BACKUP	The authorized administrator periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (on an external log server, separate storage device, etc.) to prevent audit data loss.

4 Extended Components Definition

4.1 Security Management

4.1.1 ID and Password

Family Behavior

This family defines the capability that is required to control ID and password management used in the TOE, and set or modify ID and/or password by authorized users.

Component levelling

FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.

Management: FMT_PWD.1

The following actions could be considered for the management functions in FMT:
a) Management of the ID and password configuration rules

Audit: FMT_PWD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimal: all changes of the password

FMT_PWD.1 Management of ID and password

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].
1. [assignment: *password combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].
1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

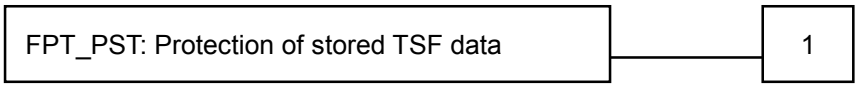
4.2 Protection of the TSF

4.2.1 Protection of Stored TSF Data

Family Behavior

This family defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component levelling



FPT_PST.1 Basic protection of stored TSF data, requires the protection of TSF data stored in containers controlled by the TSF.

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

FPT_PST.1 Basic protection of stored TSF data

Hierarchical to: No other components
Dependencies: No dependencies

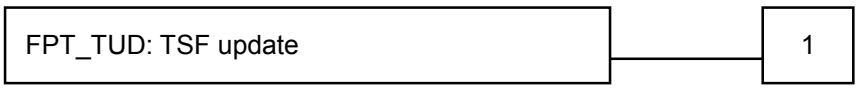
FPT_PST.1.1 The TSF shall protect [assignment: *TSF data*] stored in containers controlled by the TSF from the unauthorized [selection: *disclosure, modification*].

4.2.2 TSF Update

Family Behavior

This family defines TOE firmware/software update requirements.

Component levelling



FPT_TUD.1 TSF security patch update, requires trusted update of the TOE firmware/software including the capability to verify the validity on the update file before installing updates.

Management: FPT_TUD.1

The following actions could be considered for the management functions in FMT:
a) Management of update file verification mechanism

Audit: FPT_TUD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the

PP/ST:
a) Minimal: Update file verification result (success, failure)

FPT_TUD.1 TSF security patch update

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TUD.1.1 The TSF shall provide the capability to view the TOE versions to [assignment: *the authorized identified roles*].

FPT_TUD.1.2 The TSF shall verify validity of the update files using [selection: *hash value comparison, digital signature verification*] before installing updates.

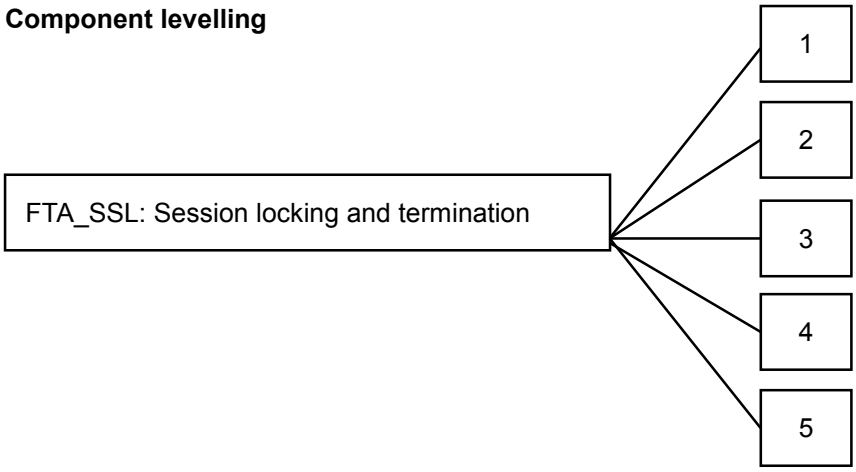
4.3 TOE Access

4.3.1 Session Locking and Termination

Family Behaviour

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

Component levelling



In CC Part 2, the session locking and termination family consists of four components. In this PP, it consists of five components by extending one additional component as follows.

※ The relevant description for four components contained in CC Part 2 is omitted.

FTA_SSL.5 The management of TSF-initiated sessions, provides requirements that the TSF locks or terminates the session after a specified time interval of user inactivity.

Management: FTA_SSL.5

The following actions could be considered for the management functions in FMT:

a) Specification for the time interval of user inactivity that is occurred the session locking and termination for each user

b) Specification for the time interval of default user inactivity that is occurred the session locking and termination

Audit: FTA_SSL.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive session

FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to: No other components.

Dependencies: [FIA_UAU.1 authentication or No dependencies.]

FTA_SSL.5.1 The TSF shall [selection:

- *lock the session and re-authenitcate the user before unlocking the session*,
- *terminate*] an interactive session after a [assignment: time interval of user inactivity].

5 Security Requirements

This chapter describes security functional requirements and security assurance requirements which should be satisfied in the TOE.

The security requirements of this Security Target are composed while “conforming to the following protection profile strictly”.

- Korean National Protection Profile for Network Device V1.1 (KECS-PP-0714a-2016)

5.1 Security Functional Requirements

The security functional requirements of this Security Target are composed while conforming to the PP. The summary on the security functional components is as follows.

[Table 5-1] Security Functional Requirements

Security Functional Class	Security Functional Component	
FAU	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
FCS	FCS_CKM.1(1)	Cryptographic key generation (SSH)
	FCS_CKM.1(2)	Cryptographic key generation (for storing SNMP settings)
	FCS_CKM.1(3)	Cryptographic key generation (SNMPv3)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (SSH-AES)
	FCS_COP.1(2)	Cryptographic operation (SSH-HMAC)
	FCS_COP.1(3)	Cryptographic operation (for storing SNMP settings)
	FCS_COP.1(4)	Cryptographic operation (SNMPv3-AES)
	FCS_COP.1(5)	Cryptographic operation (SNMPv3-HMAC)
	FCS_COP.1(6)	Cryptographic operation (for storing the administrator’s password)
	FCS_COP.1(7)	Cryptographic operation (for checking the integrity)
FDP	FDP_IFC.2(1)	Complete information flow control (1)
	FDP_IFC.2(2)	Complete information flow control (2)
	FDP_IFC.2(3)	Complete information flow control (3)

	FDP_IFF.1(1)	Simple security attributes (1)
	FDP_IFF.1(2)	Simple security attributes (2)
	FDP_IFF.1(3)	Simple security attributes (3)
FIA	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1 (extended)	Management of the ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_PST.1 (extended)	Basic protection of stored TSF data
	FPT_STM.1	Reliable time stamps
	FPT_TEE.1(1)	Testing of external entities (1)
	FPT_TEE.1(2)	Testing of external entities (2)
	FPT_TST.1	TSF testing
	FPT_TUD.1 (extended)	TSF security patch update
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5 (extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment
FTP	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

5.1.1 Security audit (FAU)

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-ups and shutdowns of the audit functions;
b) all auditable events for the *not specified* level of audit; and
c) [Refer to the “auditable event” in [Table 5-2] Audit Events, [none]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (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 [Refer to the contents of ″additional audit record″ in [Table 5-2] Audit Events, [none]].

[Table 5-2] Audit Events

Security Functional Component	Auditable Event	Additional Audit Record
FAU_STG.3	Actions taken due to exceeding of a threshold	-
FDP_IFF.1(2)	All decisions on requests for information flow	-
FDP_IFF.1(3)	All decisions on requests for information flow	-
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	
FIA_UAU.1	All use of the authentication mechanism	-
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	-
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	-
FMT_MSA.1	All modifications of the values of security attributes	-
MFT_MSA.3	Modifications of the default setting of permissive or restrictive rules, All modifications of the initial values of security attributes	-
FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data
FMT_SMR.1	Modifications to the group of users that are part of a role	-
FMT_PWD.1	All changes of the password	-

FPT_TUD.1	Update file verification result (success, failure)	Cause of verification failure
FPT_TST.1	Execution of the TSF self tests and the results of the tests(failure)	-
FPT_TEE.1(1)	Execution of the tests of the external entities and the results of the tests.	-
FPT_TEE.1(2)	Result of the tests of the external entities	-
FTA_SSL.5	Termination of an interactive session by the session locking mechanism.	
FTA_MCS.2	Rejection of a new session based on the limitation of multiple concurrent sessions.	

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 [the authorized administrator] with the capability to read [all audit data] from the audit records.

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

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 [log type, log levels, and keywords] of audit data based on [searching].

Application notes: The log type can be selected and searched between “system” and “audit”, and the audit data can be searched from a specifically selected level or higher by selecting the level among “debug”, “info”, “notice”, “warning”, “err”, “crit”, “alert”, and “emerg”. A keyword can be used while searching audit data

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) *event type*
b) [none]

Application note: The event type can generate audit data of a selected log level and higher among “debug”, “info”, “notice”, “warning”, “err”, “crit”, “alert”, and “emerg”. In case of transmission toward the syslog server, a log facility (among “auth”, “authpriv”, “cron”, “daemon”, “ftp”, “kern”, “local0-7”, “lpr”, “mail”, “news”, “syslog”, “user”, and “uucp”) can be selected in addition to the log level.

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 in the audit trail from unauthorized deletion.

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

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 [notification to the authorized administrator, [overwrite the oldest stored audit records] if the audit trail exceeds [the number of 21 audit log files, with the size of 50 MB for each].

5.1.2 Cryptographic support (FCS)

FCS_CKM.1(1) Cryptographic key generation (SSH)

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
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 [diffie-hellman-group-exchange-sha256] and specified cryptographic key sizes [256 Bit] that meet the following: [RFC4419].

FCS_CKM.1(2) Cryptographic key generation (for storing SNMP Settings)

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
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 [HMAC_DRBG(SHA-256)] and specified cryptographic key sizes [256 Bit] that meet the following: [NIST SP 800-90A].

FCS_CKM.1(3) Cryptographic key generation (SNMPv3)

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
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 [Key Localization Algorithm] and specified cryptographic key sizes [128 Bit, 160 Bit] that meet the following: [RFC3414, RFC3826].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
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 [overwriting the memory with zeros] that meets the following: [none].

FCS_COP.1(1) Cryptographic operation (SSH-AES)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [data encryption and decryption] in accordance with a specified cryptographic algorithm [AES-CBC] and cryptographic key sizes [256 Bit] that meet the following: [FIPS PUB 197, NIST SP 800-38A].

FCS_COP.1(2) Cryptographic operation (SSH-HMAC)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [message authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA2-256] and cryptographic key sizes [256 Bit] that meet the following: [RFC6668].

FCS_COP.1(3) Cryptographic operation (for storing SNMP settings)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [data encryption and decryption] in accordance with a specified cryptographic algorithm [AES-CBC] and cryptographic key sizes [256 Bit] that meet the following: [FIPS PUB 197, NIST SP 800-38A].

FCS_COP.1(4) Cryptographic operation (SNMPv3-AES)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [data encryption and decryption] in accordance with a specified cryptographic algorithm [CFB128-AES-128] and cryptographic key sizes [128 Bit] that meet the following: [FIPS PUB 197, NIST SP 800-38A].

FCS_COP.1(5) Cryptographic operation (SNMPv3-HMAC)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [message authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA-96] and cryptographic key sizes [160 Bit] that meet the following: [RFC3414].

FCS_COP.1(6) Cryptographic operation (for storing the administrator's password)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA2] and **message digest sizes** [512 Bit] that meet the following: [FIPS PUB 180-2].

FCS_COP.1(7) Cryptographic operation (for checking the integrity)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [SHA2] and **message digest sizes** [512 Bit] that meet the following: [FIPS PUB 180-2].

5.1.3 User data protection (FDP)

FDP_IFC.2(1) Complete information flow control(1)

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [blocking anomalous packets] on [the following lists of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

[

- Subjects: IT entities that transmit and receive the information through the TOE
- Information: **IPv4** Packets transmitted through the TOE

]

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFC.2(2) Complete information flow control(2)

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [firewall policy] on [the following lists of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

[

- Subjects: IT entities that transmit and receive the information through the TOE
- Information: **IPv4/IPv6** Packets transmitted through the TOE

]

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFC.2(3) Complete information flow control(3)

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [SYN cookies] on [the following lists of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

[

- Subjects: IT entities that transmit and receive the information **toward** the TOE

- Information: **IPv4 SYN Packets** and **IPv4 ACK Packets** transmitted **toward** the TOE

]

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

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 initialization

FDP_IFF.1.1 The TSF shall enforce the [blocking anomalous packets] based on the following types of subject and information security attributes: [The following list of subjects and information presented in FDP_IFC.2(1), and for each following security attributes].

[

- Subject: IT entities that transmit and receive data through the TOE, [IPv4 address]
- Information: **IPv4** Packets transmitted through the TOE, [field values of the IP header lengths, IP total lengths, TCP header lengths, TCP checksums, and TCP flags as well as actual values of the IP packet lengths, TCP header lengths, and TCP checksums]

]

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

[

a) The requested flow shall be permitted if the result of checking the security attributes of IPv4 packets (which the subject has sent) is “normal”.
b) The requested flow shall be permitted if the result of checking the security attributes of IPv4 packets (which the subject has sent) is “anomalous” and the invalid packet forwarding method is “allowed”.

]

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

FDP_IFF.1.4 The TSF shall explicitly authorize 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 rules].

[

a) If the actual length of the TCP headers (of IPv4 packets which the subject sent) is smaller than 20 bytes and the invalid packet forwarding method is selected as “block”, the requested information flow is blocked.
b) If the actual length of the TCP headers is different from the header length value of the TCP headers (of IPv4 packets which the subject sent) and the invalid packet forwarding method is selected as “block”, the requested information flow is blocked.
c) If the actual checksum value of the TCP headers is different from the checksum value of the TCP headers (of IPv4 packets which the subject sent) and the invalid packet forwarding method is selected as “block”, the requested information flow is blocked.
d) If the TCP header flag (of IPv4 packets which the subject sent) is invalid and the invalid packet forwarding method is selected as “block”, the requested information flow is blocked.
e) If the length value of the IP header (of IPv4 packets which the subject sent) is bigger than the total packet length, the requested information flow is blocked.
f) If the total packet length of the IP headers (of IPv4 packets which the subject sent) is bigger than the actual packet length, the requested information flow is blocked.

]

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 initialization

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 presented in FDP_IFC.2(2), and for each following security attributes].

[

- Subject: IT entities that transmit and receive data through the TOE, [IPv4 address, IPv6 address]
- Information: **IPv4 and IPv6** Packets transmitted through the TOE, [protocol, TCP flag, ICMP type, source IP address, source port number, destination IP address, destination port number, packet contents, packet length]

]

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

[

a) By comparing the information security attribute of packets (which the subject has sent) and the firewall policy attributes, the requested flow shall be permitted if the filtering rule is “allowed”.
b) By comparing the information security attribute of packets (which the subject has sent) and the firewall policy attributes, the requested flow shall be permitted if the filtering rule is “rate” and the rate of packets (which the subject has sent) is smaller than the current “packet rate” value.

]

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

FDP_IFF.1.4 The TSF shall explicitly authorize 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 rules].

[

a) If the filtering rule is selected as “block” by comparing the information security attributes of IP packets and the attributes of the firewall policies, the requested information flow is blocked.

b) If the filtering rule is selected as “rate” by comparing the information security attributes of IP packets as well as the attributes of the firewall policies and the rate of the packets that the subject sent is more than the “packet rate”, the requested information flow is blocked.

]

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

Hierarchical to: No other components.

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

FDP_IFF.1.1 The TSF shall enforce the [SYN cookies] based on the following types of subject and information security attributes: [The following list of subjects and information presented in FDP_IFC.2(3), and for each following security attributes].

[

- Subject: IT entities that transmit and receive data **toward** the TOE, [IPv4 address, IPv6 address]
- Information: **IPv4 SYN packets and IPv4 ACK packets** transmitted **toward** the TOE, [TCP flag]

]

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

[

a) The requested flow shall be permitted if the number of connection request SYN packets from the subject is equal or less than 65535, the number of the assigned queues for each port.

b) If the number of connection request SYN packets from the subject is more than 65535, the TOE includes cookie values in the response packets (SYN+ACK) and sends the packets. And then, the requested flow shall be permitted if the response packets (ACK) are received.

]

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

FDP_IFF.1.4 The TSF shall explicitly authorize 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 rules].

[

a) If the number of connection request SYN packets from the subject is more than 65535, the TOE includes cookie values in the response packets (SYN+ACK) and sends the packets. And then, the requested flow shall be blocked if the response packets (ACK) are not received.

]

5.1.4 Identification and authentication (FIA)

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 [*5*] unsuccessful authentication attempts occur related to [the administrator's authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*surpassed*], the TSF shall [lock out the administrator's logging in for 5 minutes].

FIA_ATD.1 User attribute definition

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 users: [user ID, password, level, authority to access to logs].

Application note: The administrator types and the authorities are as follows:

- Superuser: This user has the authority to monitor, check, and modify all configurations of the TOE.
- Monitoring User: This user has the authority only to monitor the system, but cannot modify any configurations of the TOE.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following defined quality metric].

a) Target: administrator's password, SNMP authentication/encryption password
b) Quality metric:
- The password shall be a combination of all of English upper case/lower case/number/special characters,
- The length shall be within 9 and 20 characters,
- The available special characters are as follows.

Category	Special Character
Administrator's password	~!@#$%^&*()_+{}|:"<>?`-=[]\;',./
SNMP authentication/encryption password	~!@#$%^&*()_+{}|:<>?`-=[];,./ (except for " (quotation mark), '(apostrophe), and \ (backslash))

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [requesting identification/authentication (login screen), displaying login banner] on behalf of **the administrator** to be performed before **the administrator** is authenticated.

FIA_UAU.1.2 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of **the administrator**.

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 [masked password input, [*No feedback about the failure reason when unsuccessful authentication attempts*] to **the administrator** while the authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [requesting identification/authentication (login screen), displaying login banner] on behalf of **the administrator** to be performed before **the administrator** is identified.

FIA_UID.1.2 The TSF shall require each administrator to be successfully identified before allowing any other TSF-mediated actions on behalf of **the administrator**.

5.1.5 Security management (FMT)

FMT_MOF.1 Management of security functions behavior

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 ***conduct management actions*** of the functions [the following list of functions] to [**the authorized superuser**].

[
[Table 5-3] Management Ability for each Security Feature

Security feature	Management Action
Syslog setting	determine the behavior, modify the behavior
Log level setting	determine the behavior, modify the behavior
Firewall policies	determine the behavior, disable, enable
Blocking anomalous packets	determine the behavior, disable, enable
SYN cookies	determine the behavior, disable, enable
Administrator account management	determine the behavior, modify the behavior
System clock setting	determine the behavior, enable
Restarting / shutting down the system	enable
TOE configuration file management	determine the behavior, enable
Running the security management service	disable, enable
Email alarm setting	disable, enable
Firmware update	determine the behavior, enable
TOE session termination time setting	determine the behavior, modify the behavior
Security management access control setting	determine the behavior, modify the behavior
Administrator concurrent session limitation	disable, enable
Interface setting	disable, enable
Testing of External Entities	enable
TSF Testing	enable

]

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
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 [firewall policies, SYN cookies, blocking anomalous packets] to restrict the ability to [*query, modify, delete, [create]*] the security attributes [the following list of security attributes] to [the authorized administrator].

[
[Table 5-4] Management Ability for each Security Attribute

Security policy	Security attribute	Authorized administrator	Ability
Firewall policies	content (packet payload string, packet payload checking range)	Superuser	query, modify, delete, create
		Monitoring user	query
	filter (protocol, TCP flag, ICMP type, source IP address, destination IP address, source port number, destination port number, logging, packet length, action)	Superuser	query, modify, delete, create
		Monitoring user	query
	interface, priority, status	Superuser	query, modify
		Monitoring user	query
SYN cookies	SYN cookies using option	Superuser	query, modify
		Monitoring user	query
Blocking anomalous packets	Checksum checking option TCP flag validity checking option Anomalous packet processing option	Superuser	query, modify
		Monitoring user	query

]

FMT_MSA.3 Static attribute initialization

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 [firewall policies, SYN cookies, blocking anomalous packets] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

FMT_MTD.1 Management of TSF data

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 ***manage*** the [following list of TSF data] to [the authorized administrator].

[Table 5-5] TSF Data List and the Management Ability

TSF data		Authorized administrator	Ability
Audit log setting	log level, syslog server IP address, port number, log type, and server status	Superuser	query, modify
		Monitoring user	query
Administrator account setting	ID, password, description, level, and log-checking authority	Superuser	query, modify, delete, create
		Monitoring user	query
System time setting	current date and time, NTP client status / server IP address, time zone	Superuser	query, modify
		Monitoring user	query
System information	Product Name, Serial Number, BL version, OS version, PLD version, Mgmt IP Address, Mgmt MAC Address, SDRAM Size, Storage Size, System Uptime	Superuser, Monitoring user	query
Login banner	Login banner information	Superuser	query, modify, delete, create
		Monitoring user	query
TSF testing	Result of TSF testing	Superuser, Monitoring user	query
Email alarm	Sender, receiver, SMTP server IP address, alarm type, transmission interval, and status information	Superuser	query, modify, delete, create
		Monitoring user	query
SNMP setting		Superuser	query, modify, delete, create

	Username, password(aes/sha), status, system information, and load-timeout	Monitoring user	query
Administrator's management connection IP setting	ID, IP address	Superuser	query, modify, delete, create
		Monitoring user	query
Security management service setting	Port number, status(enable/disable)	Superuser	query, modify
		Monitoring user	query
TOE session termination time setting	Time (in minutes)	Superuser	query, modify
		Monitoring user	query
Interface setting	VLAN: VLAN ID, VLAN name, port number, and tagged/untagged option IP address: interface name, IP address, and overlapping IP address setting option Default gateway: IP address Interface status (enable/disable)	Superuser	query, modify
		Monitoring user	query

FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [administrator's account setting] to [the authorized administrator].
1. [none]
2. [none]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [administrator's account setting] to [the authorized administrator].
1. [none]
2. [none]

FMT_PWD.1.3 The TSF shall provide the capability for [*changing the password when the authorized **superuser** accesses for the first time*].

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:
[
1. enable/disable [SSH v2] (default value:disable)
2. Supporting SNMP v3
3. Designating IP address for management access service
4. Setting access privileges per administrator account
5. Checking details and results of the testing by FPT_TST.1 and FPT_TEE.1
6. [Performing the security management features that are indicated in FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1, and FMT_SMR.1.]

]

Application note: The management function list from FMT_SMF.1.1 is applied on both the local access and management access.

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 [superuser, monitoring user].
FMT_SMR.1.2 The TSF shall be able to associate users with **roles defined in FMT_SMR.1.1**.

Application note: The level of administrators are divided into the “superuser” and “monitoring user”. The details are as follows:

- Superuser: This user has the authority to monitor and modify all configurations of the TOE.
- Monitoring User: This user can only monitor the system, but cannot modify any configurations of the TOE.

5.1.6 Protection of the TSF (FPT)

FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_PST.1.1 The TSF shall protect [the administrator password, SNMP authentication/encryption password] stored in the containers controlled by the TSF from the unauthorized *disclosure*.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TEE.1(1) Testing of external entities(1)

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests *during the initial start-up, at the request of* ***the authorized administrator*** to check the fulfillment of [operating status of memory, LCD, voltage].

FPT_TEE.1.2 If the test fails, the TSF shall [none].

FPT_TEE.1(2) Testing of external entities(2)

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests *during the initial start-up, periodically during normal operation* to check the fulfillment of [the following tests].

- CPU: Checking the CPU usage rate if it exceeds 90%
- Memory: Checking the memory usage rate if it exceeds 90%
- Temperature: Checking the temperature if it exceeds the standard range
- Power: Checking the power if it is turned off and the power supply if there are any problems
- Fans: Checking the operation status of fans
- Link: Detecting the link statuses of the interface (UP/DOWN)

FPT_TEE.1.2 If the test fails, the TSF shall [turn on the LED, send an alarming email].

Application note: Each LED is turned on only when there is a trouble on the temperature, power supply, and fans.

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 *after loading firmware during the initial start-up, at the request of* ***the authorized administrator*** to demonstrate the correct operation of [*main parts of the TOE*].

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

FPT_TST.1.3 The TSF shall provide ***the authorized administrator*** with the capability to verify the integrity of *TSF execution files*

FPT_TUD.1 TSF security patch update (Extended)

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TUD.1.1 The TSF shall provide the capability to view the TOE versions to [the authorized administrator].

FPT_TUD.1.2 The TSF shall verify validity of the update files using *hash value comparison* before installing updates.

5.1.7 TOE access (FTA)

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same **administrator** according to the rules [following rules/ assignment: rules for the number of maximum concurrent sessions].

[

- Only one concurrent session is allowed for the superuser ID.
- Only one concurrent session is allowed for the administrator who has the superuser's authority

]

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [1] sessions per **administrator**.

FTA_SSL.5 Management of TSF-initiated sessions (Extended)

Hierarchical to: No other components.
Dependencies: [FIA_UAU.1 Timing of authentication or no dependencies]

FTA_SSL.5.1 The TSF shall *terminate* **the administrator's** interactive session after a [time interval of **the administrator** inactivity (1–60 minutes, default: 10 minutes)].

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **administrator's management access session** establishment based on [connection IP, *whether or not to activate the management access session of the same account, whether or not to activate the management access session of administrator account with the **superuser** privilege*]

5.1.8 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

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

FTP_ITC.1.2 The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [interoperating with SNMP Manager].

FTP_TRP.1 Trusted path

Hierarchical to: No other components.
Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***the management access*** **administrator** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure, [none]*.

FTP_TRP.1.2 The TSF shall permit *the TSF,* ***the management access administrator*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***the authentication of management access administrator***.

5.2 Security Assurance Requirements

Security assurance requirements (SAR) defined in this document consists of assurance component in Common Criteria for Information Technology Security Evaluation, Part 3. The Evaluation Assurance Levels (EALs) is EAL1+. [[Table 5-6] shows the summary of assurance components.

[Table 5-6] Security Assurance Requirements

Security Assurance Class	Security Assurance Components	
Security Target evaluation (ASE)	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic functional specification
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life cycle support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing – conformance
Vulnerability assessment (AVA)	AVA_VAN.1	Vulnerability survey

5.2.1 Security target evaluation

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.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:

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

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

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

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

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

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

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

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

ASE_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.

ASE_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.

ASE_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.

ASE_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.

Evaluator action elements:

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

ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

Developer action elements:

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements:

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

ASE_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:

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

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements:

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

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C 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.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

Evaluator action elements:

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

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

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.

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3 Guidance documents

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.

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

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.

5.2.4 Life-cycle support

ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Evaluator action elements:

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

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

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

5.2.5 Tests

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.

ATE_IND.1 Independent testing - conformance

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified..

5.2.6 .Vulnerability assessment

AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E 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 Basic attack potential.

5.3 Security Requirements Rationale

5.3.1 Security Assurance Requirements Rationale

The Evaluation Assurance Level of this Security Target is “EAL1+ (ATE_FUN.1)”

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. For EAL1, the developer is not required to add more effort if a company has developed a product according to commonly applied development practices. In other words, it should not require an increased investment of cost or time.

EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

For EAL1, the developer is not required to provide the evidence of developer testing, based on the functional specification. However, ATE_FUN.1 is included for the documentation process based on the results of constructing TSFs correctly and conducting tests internally to check for flaws.

Evaluation assurance level of this Security Target is EAL1+(ATE_FUN.1).

5.3.2 Dependency of TOE Security Functional Requirements

The following table shows dependency of security functional requirements.

[Table 5-7] Rationale for the Dependency of Security Functional Requirements

NO.	Security Functional Components	Dependencies	Ref. No.
1	FAU_GEN.1	FPT_STM.1	38
2	FAU_SAR.1	FAU_GEN.1	1
3	FAU_SAR.3	FAU_SAR.1	2
4	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	1 33
5	FAU_STG.1	FAU_GEN.1	1
6	FAU_STG.3	FAU_STG.1	5
7	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[- or 11, 12] 10
8	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[- or 13] 10
9	FCS_CKM.1(3)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[- or 14, 15] 10
10	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	[- or – or 7, 8, 9]
11	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[- or - or 7] 10
12	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[- or - or 7] 10
13	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[- or - or 8] 10
14	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[- or - or 9] 10
15	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[- or - or 9] 10
16	FCS_COP.1(6)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- -
17	FCS_COP.1(7)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- -
18	FDP_IFC.2(1)	FDP_IFF.1	21
19	FDP_IFC.2(2)	FDP_IFF.1	22
20	FDP_IFC.2(3)	FDP_IFF.1	23
21	FDP_IFF.1(1)	FDP_IFC.1	18

		FMT_MSA.3	32
22	FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	19 32
23	FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	20 32
24	FIA_AFL.1	FIA_UAU.1	27
25	FIA_ATD.1	-	-
26	FIA_SOS.1	-	-
27	FIA_UAU.1	FIA_UID.1	29
28	FIA_UAU.7	FIA_UAU.1	27
29	FIA_UID.1	-	-
30	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	35 36
31	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	[- or 18, 19, 20] 35 36
32	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	32 37
33	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	35 36
34	FMT_PWD.1(Extended)	FMT_SMF.1 FMT_SMR.1	35 36
35	FMT_SMF.1	-	-
36	FMT_SMR.1	FIA_UID.1	29
37	FPT_PST.1(Extended)	-	-
38	FPT_STM.1	-	-
39	FPT_TEE.1(1)	-	-
40	FPT_TEE.1(2)	-	-
41	FPT_TST.1	-	-
42	FPT_TUD.1(Extended)	-	-
43	FTA_SSL.5(Extended)	[FIA_UAU.1 or No dependencies]	27
44	FTA_TSE.1	-	-
45	FTA_MCS.2	FIA_UID.1	29
46	FTP_ITC.1	-	-
47	FTP_TRP.1	-	-

The dependency of some functional components is not satisfied, and the description for the justification of such is as follows.

FCS_CKM1, FCS_CKM4 (Dependencies: FCS_COP.1(6)):
FCS_CKM.1 and FCS_CKM4 in dependency with FCS_COP.1(6) are not satisfied. Administrator Password Encryption function uses SHA-512 hash algorithm. So, the cryptographic key generation/destruction processes are not required.

FCS_CKM1, FCS_CKM4 (Dependencies: FCS_COP.1(7)):
FCS_CKM.1 and FCS_CKM4 in dependency with FCS_COP.1(7) are not satisfied. TOE integrity checking uses SHA-512 hash algorithm. So, the cryptographic key generation/destruction processes are not required.

FDP_IFF.1(Dependencies: FDP_IFC.1)
FDP_IFF.1 has a dependency to FDP_IFC.1, and this is satisfied by FDP_IFC.2 that is in a hierarchical relationship with FDP_IFC.1.

FDP_MSA.1(Dependencies: FDP_IFC.1)
FDP_MSA.1 has a dependency to FDP_IFC.1, and this is satisfied by FDP_IFC.2 that is in a hierarchical relationship with FDP_IFC.1.

5.3.3 Dependency Rationale of Security Assurance Requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.

The augmented SAR ATE_FUN.1 has dependency on ATE_COV.1. but, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation, ATE_COV.1 is not included in this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6 TOE summary Specification

6.1 Security Audit

The TOE supports the features of generating, checking, and searching audit logs on actions which occur during the operation for the security, as these actions are controlled by the TSF. With the audit logs, the authorized administrators can check the details of when and how each event has occurred, in real time or at any other time.

FAU_GEN.1
FAU_SEL.1

6.1.1 Security Audit Data Generation

The TOE generates audit logs on the management activities of the authorized administrators and on the operation of the TOE security features. The TOE includes the details such as the system time (e.g. date, time) and the identity (e.g. user ID, source IP address, etc.) while generating audit logs. Audit logs are categorized according to the type, level, and category of the event. Among the generated security audit logs, only the ones with the levels, which the authorized superuser has selected or higher, are stored on the disk.

The audit logs of the TOE are classified into eight levels as follows, according to the priorities. Only the audit logs with the levels, which the authorized superuser has selected or higher, are stored on the disk.

[Table 6-1] Levels of Audit Logs

Level	Description
emergency	an event which is critical to the system
alert	an event which needs an immediate response
critical	an event which is important
error	an error message
warning	a warning message
notice	an event which is general and unimportant
information	an event which includes information
debug	an event which is related to debugging

As the type of audit logs, there are “system” and “audit”. Data is recorded as follows.

[Table 6-2] Types of Audit Logs

Type	Description
System	security audit data on the events which are generated by the TOE’s hardware or the system daemon
Audit	security audit data on the setting of the authorized administrators’ security features and on the events of authenticating the administrators’ logins

[Table 6-3] Records of Audit Logs

Category	Description
System/Audit	• Time: the date and time of generating a log • System Name: the name of the PAS-K system where the log was generated • Event Level: the level of the log event • Subject: the information on the subject that generated the log (e.g. the name of the user or daemon) • Class: the class of the log • Message: the details on the log

6.1.2 Security Audit Review

FAU_SAR.1
FAU_SAR.3

The TOE supports the checking and searching feature on audit logs. The authorized administrators can check all audit logs in the ascending order of the date, or search specific ones with the search options as follows.

[Table 6-1] Audit Log Search Option

Search Option	Description
Audit Log Type	This is used for search a selected type of audit logs. (e.g. system, audit)
Audit Log Level	• fix-level: This is used for search audit logs for a selected level only. • imply-level: This is used for search audit logs for a selected level and higher.
Keyword	This is used for search audit data with a keyword.

6.1.3 Protected Audit Trail Storage

FAU_STG.1
FAU_STG.3

The TOE prevents all users (including the authorized users) from stored log files to protect these files from any deletions and modifications. Moreover, audit logs cannot be deleted or modified as these logs can be checked only, on the security management screen.

By checking the total size of audit data files every five minutes, audit data is prevent from the loss due to overflowing the storage. If there are 21 audit log files and the size of each file is bigger than 50 megabytes, the logs are deleted from the oldest ones to prevent any losses. An audit log is generated when one or more oldest files are overwritten, and a syslog is sent to the administrators as a notification.

6.2 Cryptographic Support

FCS_CKM.1(1)
FCS_CKM.1(2)
FCS_CKM.1(3)
FCS_CKM.4
FCS_COP.1(1)
FCS_COP.1(2)
FCS_COP.1(3)
FCS_COP.1(4)
FCS_COP.1(5)
FCS_COP.1(6)
FCS_COP.1(7)

The TOE stores data after the encryption to prevent unauthorized disclosures of the important data stored in the storage controlled by the TSF. Moreover, The TOE uses the encrypted communication channels between the TOE and the administrator's PC and between the TOE and the SNMP manager. The details are as follows.

[Table 6-2] TOE Cryptographic Algorithms

Category		Cryptographic key generation	Algorithm	Cryptographic key destruction
Encryption of stored data	SNMP setting	HMAC_DRBG (SHA-256)	AES-CBC(256-bit key)	zeroization after the AES encryption and decryption
Encryption of transmitted data	SSH	diffie-hellman-group-exchange-sha256	AES-CBC(256-bit key), HMAC-SHA2-256(256-bit key)	zeroization after the AES encryption and decryption
	SNMPv3	key localization algorithm of RFC 3414 and RFC 3826 (128-bit/160-bit)	CFB128-AES-128(128-bit key), HMAC-SHA-96(160-bit key)	• zeroization after the AES encryption and decryption • zeroization after the messages authentication
Checking the integrity		-	SHA-2(512-bit hash)	-
Storing the administrators' passwords		-	SHA-2(512-bit hash)	-

6.3 User Data Protection

The TOE supports security policies to protect the network resources (which are connected to the TOE) from online attacks and threats. The details are as follows.

6.3.1 Firewall Policy

FDP_IFC.1(2)
FDP_IFF.1(2)

To protect the internal network, the firewall policies allow the authorized users and transmission from the authorized networks while blocking the access from unauthorized external networks.

The TOE monitors packets transmitted between the internal network and external network, and filters the packets based on the filtering options. Each filter is composed of an “option” and “action”. The condition is used to categorize packets and the action is used to decide whether to accept or drop categorized packets. If firewall policy is enabled, it is possible to restrict internal network to be exposed to external network(by blocking a certain port) as well as to block unnecessary traffic sent from the internal to the external, and unauthorized accesses.

The firewall filtering options are as follows. Both the IPv4 and IPv6 are supported.

- protocol types of packets
- source/destination IP addresses of packets
- source/destination port numbers of packets
- content of packets
- TCP flags
- lengths of packets
- ICMP types

The firewall filtering actions are as follows

- **accept:** Packets are allowed if they match the details of the option.
- **drop:** Packets are dropped if they match the details of the option.
- **reject:** The reset packets (for the IPv4) or ICMP port-unreachable packets (for the IPv6) are sent to the source IP address of the packets which match the details of the condition. This can be used only when the protocol type is configured as “TCP” or “ICMP”.
- **rate:** The packets (which match the details of the option) are allowed up to the configured value.

A firewall policy consists of an ordered list of rules with options and actions. The administrator can select the priority of each rule to apply the one with the highest priority first.

6.3.2 SYN Cookies (IPv4)

FDP_IFC.1(3)
FDP_IFF.1(3)

The TOE supports the “SYN cookies” feature for blocking the SYN flood attack which is a type of DoS attacks. If the clients send TCP SYN packets to the TOE, these packets are stored in the queue up to 65535. The information flow is allowed until all of these allocated queues are used. When the queues are full, the TOE includes cookie values in the TCP SYN/ACK packets toward the clients. At this point, the TOE allocates memory for receiving TCP ACK packets from the clients, instead of maintaining the “half-open” status. With this, it is possible to block SYN flood attacks on the TOE while allowing the normal access. With SYN cookies, the TOE resource can be prevented from being wasted due to the TCP SYN packets. For the normal clients, TOE provide seamless service even while there are SYN flood attacks.

6.3.3 Anomalous Packet Prevention (IPv4)

The TOE supports the detection and analysis features, based on IPv4 packets, to maintain the stability of the service even when there are inflows of anomalous traffic. The network is protected from malicious traffic by allowing normal packets and blocking anomalous packets.

FDP_IFC.1(1)
FDP_IFF.1(1)

The details are as follows.

- checking the validity of the TCP header
  If the header of a packet is smaller than 20 bytes or if the actual length is different from the length information on the header, this packet is considered as anomalous and blocked/allowed according to the administrator's setting.
- checking the checksum of the TCP packet
  If the checksum value (which is indicated on the TCP header) is different from the actual checksum value, this packet is considered as anomalous and blocked/allowed according to the administrator's setting.
- checking the TCP flag
  If the combination of the TCP header flag is incorrect or if there are no settings, this packet is considered as anomalous and blocked/allowed according to the administrator's setting.
- checking the validity of the IP header
  If the header length (which is indicated on the IP header) is bigger than the total packet length or if the indicated total packet length is bigger than the actual packet length, this packet is considered as anomalous and blocked.

6.4 Identification and Authentication

6.4.1 User Identification and Authentication

FIA_AFL.1
FIA_ATD.1
FIA_SOS.1
FIA_UAU.1
FIA_UAU.7
FIA_UID.1

The TOE supports the security features with the local access and management access. For the security management features, it is required to identify and authenticate the administrator.

The combination rules for the administrator ID and password are as follows.

[Table 6-3] Administrator ID / Password Combination Rules

Category	Combination rule
Administrator ID	• This shall be between 1 to 8 characters. • The first character shall be an alphabet. • This part is case sensitive.
Password	• This shall be a combination of each of uppercase letters, lowercase letters, numbers, and special characters. • This shall be between 9 to 20 characters. • The supported special characters are as follows. (e.g. ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ? ` - = [ ] \ ; ' , . /)

The TOE supports the protected authentication feedback feature by not displaying the characters that the administrators type in as the passwords and by not providing a feedback in case of failing to log in.

The TOE locks an account for five minutes when five times of unsuccessful authentication attempts has been attempted consecutively.

6.5 Security Management

6.5.1 Audit Log Management

The TOE supports the interface of the audit log management for the authorized administrators to create audit logs selectively. The TOE generates audit data based on the values that the authorized administrators have specified. Moreover, the TOE sends the logs (with the types which have been enabled for the transmission in the configuration) to a syslog server which has been physically separated. If the authorized administrators add, modify, or delete any security attributes which are related to the audit log management features, audit data is generated for each case.

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1

[Table 6-4] Log Setting Items

Feature	Description
Log Level Setting	The audit log level is configured for storing on the TOE. Audit logs are generated for the events with this level or higher.
Server Setting for Log Transmission	The syslog server information is configured for sending audit logs by selecting aydit log types and audit log levels.

6.5.2 Firewall Policy Management

The TOE supports querying, adding, modifying, deleting, enabling, and disabling the firewall policy lists. The TOE generates audit data during the operation when the authorized administrators add/modify/delete firewall policy lists or modify the security attributes of the policies.

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1
FMT_MSA.3

The filter options of the firewall policies are applied by generating the objects of the “content” and “filter as well as forming multiple objects as either a “content group” or a “filter group”.

On the firewall policies, the TOE maintains the security attributes as follows.

[Table 6-5] Firewall Policy Security Attributes

Category	Security attributes
Firewall Policy	• filter: a filter object which will be used in the policy • filter group: a filter group object which will be used in the policy • interface: an interface where the firewall policy will be applied • priority: the priority of the firewall policy • using: enable/disable *Default: enable
Filter	• protocol *Default: all • TCP flag • ICMP type • source IP address *Default: all • destination IP address *Default: all • source port number • destination port number • content: content or a content group object which will be applied on the filter • packet length • processing method: accept/drop/reject/rate • recording as an audit log: enable/disable *Default: enable
Content	• string: a string which will be searched on the payload of the packet

	• offset: the part where a string search is started on the payload of the packet • depth: the part where a string search is finished on the payload of the packet • case sensitivity: enable/disable *Default: enable

6.5.3 SYN Cookies Management

The TOE supports querying, enabling, and disabling the SYN cookie feature for the authorized administrators. The TOE runs the “SYN cookies” feature and generates audit data according to the details that the authorized administrators have specified. The default value is “disabled”, and this feature shall be enabled before using it.

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1

6.5.4 Anomalous Packet Checking Management

The TOE supports querying, enabling, and disabling the anomalous packet blocking feature for the authorized administrators. The TOE blocks or allows anomalous packets based on the checking setting, and generates audit logs about the setting.

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1

- checking checksums of TCP packets *Default: enable
- checking TCP flags *Default: disable
- processing anomalous packets *Default: allow

The features of “checking the validity of TCP headers” and “checking the validity of IP headers” are supported as the default.

6.5.5 Administrator Account Management

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1
FMT_SMR.1
FMT_PWD.1

The TOE supports querying, adding, deleting, and modifying administrators' accounts for identifying and authenticating administrators. As the default, "root" is registered as the default administrator ID of the TOE. It is required to modify the password after logging in with this ID for the first time.

The admin security attributes are as follows.

[Table 6-6] Admin Security Attributes

Category	Description
Administrator ID	• This shall be between 1 to 8 characters. • The first character shall be an alphabet. • This part is case sensitive.
Password	• This shall be a combination of each of uppercase letters, lowercase letters, numbers, and special characters. • This shall be between 9 to 20 characters. • The supported special characters are as follows. (e.g. ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ? ` - = [ ] \ ; ' , . /)
Administrator Level	The level of administrators are divided into the "superuser" and "monitoring user". • Superuser: This user has the authority to monitor and modify all configurations of the TOE. • Monitoring User: This user can only monitor the system, but cannot modify any configurations of the TOE.
Accessibility on Logs	This is the authority to check audit logs.
Description	This is the description about an administrator.

6.5.6 System Management

System Information Querying

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1
FPT_STM.1

The TOE supports the features of displaying the system information, for the authenticated administrators. The details are as follows.

- device names, serial numbers, versions of the bootloaders, versions of the operating systems, versions of the PLDs, capacity of the memory, capacity of the hard disk, duration of the running the systems, acceleration mode

Login Banner Setting

The authorized administrators can configure and check the content of the login banner as this is the feature which displays notes and notifications on the system login screen for the administrators who log in to the CLI through the console port or SSH.

Network Connection Setting

The TOE supports querying, adding, modifying, and deleting IP addresses and routing information to

communicate with other network devices. The TOE supports both the IPv4 and IPv6. The TOE generates audit logs for the authorized administrators' adding, modifying, and deleting IP addresses.

System Time

The TOE records the system time whenever there are instances of various events, troubles, or commands (which the administrators type in). It is very important to maintain the system clock exact as these logs are crucial evidence of troubleshooting on the system. The TOE supports both methods of the customization of the time and the automatic synchronization by receiving accurate time values from an NTP server periodically.

Restarting or Shutting Down the System

The TOE supports the features of restarting or shutting down the TOE system. When the system is rebooted or shut down, all features are restarted or shut down as well. The TOE generates audit logs when any of the authorized administrators restart or shut down the TOE.

Configuration File Management

The TOE supports the feature of storing TSF data which is managed by the FMT of the system.

[Table 6-7] Configuration File Management

Feature	Description
Saving the Configuration as a File	The current configurations of the TOE are stored as a file on the "Startup-config" storage or "Config-slot".
Copying a Configuration File	A configuration file is copied from "Config-slot" to another section of the storage.
Uploading/Downloading a Configuration File	The configuration files from the "config-slot" storage are uploaded to or downloaded from the server.
Restoring the Previous Configuration	The current configurations of the TOE are rolled back to the previous status.
Initializing the Configuration	The current configurations of the TOE are rolled back to the factory settings.
Backing Up the Configuration	The current configurations of the TOE are backed up on a remote server periodically.

SNMPv3 Setting

The TOE supports the SNMP manager interoperation. The TOE sends its status to SNMP managers which have been selected by authorized administrators. The TOE supports querying, adding, deleting, enabling, and disabling the SNMP settings. The TOE generates audit logs when the authorized administrators add/delete SNMP setting lists or modify the security attributes.

Security Management Service

The administrators can configure the TOE through the security management access service. As a type of the management access service, there is the CLI such as SSH which supports both IPv4 addresses and IPv6 addresses. As the factory settings, all parts of service is disabled. The administrators can enable or disable the “security management access service” and query/modify the port number of each service. Moreover, these administrators can allow the TOE to gain the access toward specific IP addresses only.

6.5.7 Email Alarm Setting

The TOE supports the “email alarm” feature which sends security audit logs to the email addresses of the administrators if there are any events of: 1) troubles on the TOE’s CPU, memory, temperature, power supply, or fans or 2) events of modifying the configurations. The TOE sends email alarms and generate audit logs on the “email-alarm” setting.

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1

6.5.8 Firmware Update

The TOE supports the feature of updating the firmware to enhance the security features and respond to vulnerabilities. Only the authorized administrators can update the firmware through the HTTPS. The TOE checks the validity of the current firmware file by comparing the hash values (SHA2-512) for any modifications on the update file for the firmware. As this updating feature allows only the HTTPS for the encrypted transmission, the Installer’s PC at the Development Company should support the SSL protocol.

FMT_MOF.1
FMT_SMF.1
FPT_TUD.1

6.5.9 TOE Access Management

The TOE supports the “TOE access management” feature. The TOE generates audit logs when the authorized administrators modify the “TOE access management” setting.

FMT_MOF.1
FMT_MTD.1
FMT_SMF.1

[Table 6-8] TOE Access Setting

Feature	Description
TOE session termination time setting	After the authorized administrators specify the session timeout, the accounts are automatically logged out if the administrators do not do any activities, such as typing on the keyboard or clicking the mouse buttons. To gain the access toward the security-management interface, it is necessary to reauthenticate.
Administrator’s management connection IP setting	If the authorized administrators specify the IP addresses for the access toward the security management interface, it is possible to access to the system from the allowed IP addresses only.
Administrator concurrent session limitation	If the authorized administrators enable the “Administrator concurrent session limitation” feature, it is possible to prevent 2 or more administrators’ accounts from logging in at the same time.

6.6 Protection of the TSF

6.6.1 Protection of Stored TSF Data

The TOE encrypts important data before storing it in containers to protect it from unauthorized disclosures. FPT_PST.1

[Table 6-9] TSF Data Encryption Algorithm

Stored Data	Encryption Algorithm
SNMP Settings	AES-256
Administrator's Password	SHA2-512

6.6.2 Testing of External Entities

Checking the System

The TOE starts checking the system either while booting the system or when the authorized administrator requests. The details are as follows. FPT_TEE.1(1)

- checking the memory: The statuses of memory are checked for errors, and the sizes of memory are compared with the specifications of the TOE model.
- checking the status of the LCD: The status of the LCD module is checked for any troubles.
- checking the voltage: The voltage of the TOE system is checked whether it is maintained as the normal value.

Email Alarm

The TOE supports the feature of checking the statuses of the following parts while starting the TOE or periodically, and sending the details of the situations to the administrators' email addresses to respond to the troubles as soon as possible. FPT_TEE.1(2)

[Table 6-10] Email Alarm Checking Items

Category	Description
CPU	Checking the CPU usage rate if it exceeds 90%
Memory	Checking the memory usage rate if it exceeds 90%
Temperature	Checking the temperature if it exceeds the standard range
Power	Checking the power if it is turned off and the power supply if there are any problems
Fans	Checking the operation status of fans
Link	Detecting the link statuses of the interface (UP/DOWN)

6.6.3 TSF Testing

FPT_TST.1

The TOE supports the feature of checking the integrity of the main processes and configuration files which are necessary for running the security features. If any part of the main processes is terminated abnormally, the TOE generates an audit log and restart the specific process. The integrity is checked for modulations of important configuration files and TSF execution files by using the SHA-2 (512-Bit) algorithm. If there are any violations, the TOE sends a notification to the authorized administrators and generates audit logs.

The feature of checking the integrity is started on one of the following situations.

- while starting the TOE system
- when there is a request from an authorized administrator through the security management interface

[Table 6-11] TSF Testing Items

Type	Goal
Checking the Integrity of the Configuration Files	By maintaining the integrity of the configuration files, anomalous attempts of modulation are prevented.
Checking the Integrity of the Execution File	By maintaining the integrity of the binary numbers for the main execution, anomalous operations are prevented.
Checking the Status of Running Main Processes	By maintaining the integrity of the main daemons, troubles on the system are prevented. (e.g. malfunctioning due to an anomalous daemon, crashing of the system)

6.7 TOE Access

6.7.1 Session Termination

The administrator logs in to the security management interface of the TOE after the “identification and authentication” steps. If there is no data transmission after the period of login maintenance period the current session is finished automatically. (e.g. 1 minute to 60 minutes) The administrator must log in to the TOE again by going through the authentication process. FTA_SSL.5

6.7.2 Limitation on Multiple Concurrent Sessions

The TOE supports the feature of limiting the concurrent sessions to prevent more than one superuser (who has the full authority) to log in to the system. While the superuser is logged in, none of additional administrators who have either the same IDs or authority levels can log in to the system. FTA_TSE.1 FTA_MCS.2

For the security management interface of the TOE, up to eight IP addresses can be configured while allowing sessions from the terminals with these IP addresses.

6.8 Trusted Path/Channels

FTP_ITC.1
FTP_TRP.1

For the management connections of the administrators, the TOE prevents data from unauthorized disclosure and modification by supporting the secure channel which uses the encrypted protocol of SSHv2. Moreover, the TOE supports trusted channels with the SNMPv3 for the interoperation feature for the SNMP managers.

The TOE supports cryptographic protocols with the versions as follows.

[Table 6-12] Trusted Path/Channels Algorithms

Transmission path	Type and version of the cryptographic protocol
TOE <-> Administrator's PC (with the remote management access)	• SSHv2
TOE <-> SNMP manager	• SNMPv3


PIOLINK