KECS-CR-17-28

PAS-K V2.2

Certification Report

Certification No.: KECS-NISS-0792-2017

2017. 5. 31

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2017.5.31	-	Certification report for PAS-K V2.2 - First documentation

This document is the certification report for PAS-K V2.2 of PIOLINK, Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary

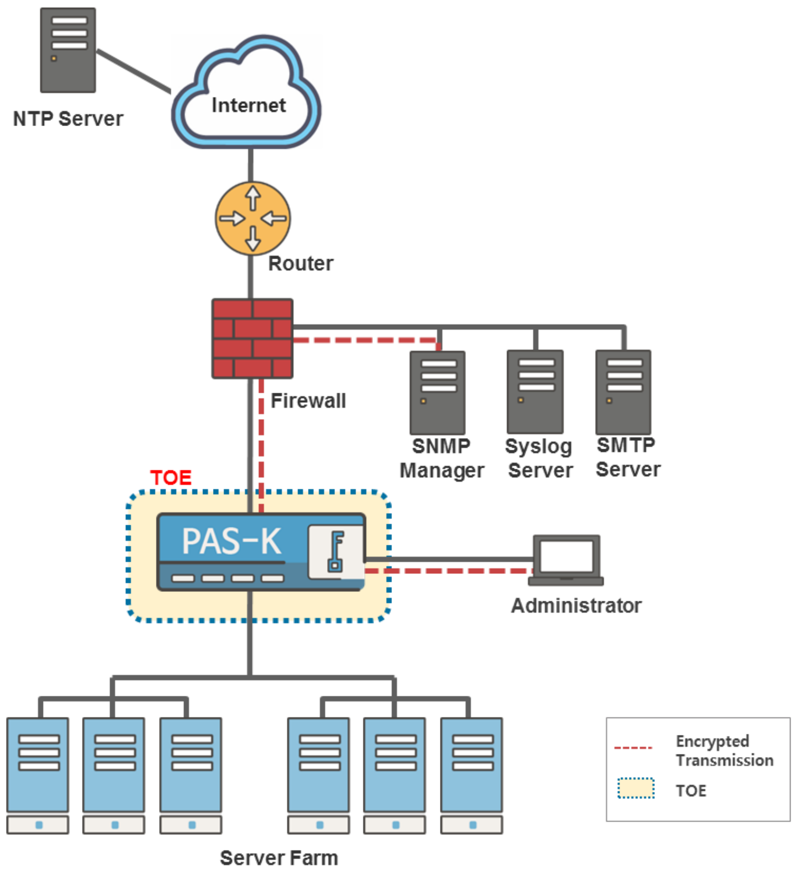
This report describes the certification result drawn by the certification body on the results of the PAS-K V2.2 developed by PIOLINK, Inc. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation ("TOE" hereinafter) is a network appliance known as a layer 4/7 switch for transmitting and controlling network packets from source IT entities to 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.

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on April 28th, 2017. This report grounds on the evaluation technical report (ETR) [4] TTA had submitted and the Security Target (ST) [5].

The ST claims conformance to the Korean National Protection Profile for Network Device V1.1 [3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3. The ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the PP, therefor the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE. 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.



[Figure 1] Operational environment of the TOE

The hardware models are detailed in [Table 1] below:

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

[Table 1] TOE Hardware Detailed Specifications

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE reference is identified as follows.

TOE	PAS-K V2.2
Firmware	PLOS-PASK-v2.2.2
Hardware Models	PAS-K1716, PAS-K2424, PAS-K2824, PAS-K4024, PAS-K4224, PAS-K4424, PAS-K4824, PAS-K8220, PAS-K8620
Document	PAS-K V2.2 User Guide V1.2
	PAS-K V2.2 Installation Guide V1.1

[Table 2] TOE identification

[Table 3] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (June 27, 2016) Korea Evaluation and Certification Regulation for IT Security (November 1, 2012)
TOE	PAS-K V2.2
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
Protection Profile	Korean National Protection Profile for Network Device V1.1, KECS-PP-0714a-2016
Developer	PIOLINK, Inc.
Sponsor	PIOLINK, Inc.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	April 28th, 2017
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The TOE Security Functions in [Table 4] are supported by the TOE. For more details refer to the ST.

TSF	Explanation
Security Audit	The TOE provides audit log creation and query execution functions to the subject that require audit.
Cryptographic Support	The TOE provides cryptographic functions to encrypt stored data, to check the integrity of the TOE and a firmware update and to encrypt transmitted data between the TOE and an administrator PC as well as the TOE and a SNMP manager.
User Data Protection	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) • SYN Cookie (IPv4) • Blocking Anomalous Packets (IPv4)
Identification and Authentication	The TOE provides authorization and authentication functions to control administrator who accesses the management.
Security Management	The TOE provides functions for system configuration, security policy planning and security function management with the local connection and the management connection.
Protection of the TSF	The TOE provides self-test functions for the TOE itself.
TOE Access	The TOE provides functions that constrains duplicated sessions from establishing for a superuser account or the highest authority level and destroys the authenticated session after the defined idle time.
Trusted Path/Channels	The TOE provides secure paths and channels for data transmission between the TOE and an administrator PC as well as the TOE and a SNMP manager.

[Table 4] The TOE Security Functions

4. Assumptions and Clarification of Scope

The followings are procedural method supported from operational environment in order to provide the TOE security functionality accurately (for the detailed and precise definition of the assumption refer to the ST, chapter 3.1):

- 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.

- 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 must be immediately reflected to the TOE operational policies in order to maintain the same level of security as before.
- The authorized administrator of TOE shall be non-malicious, have appropriately trained for TOE management functions and accurately fulfill the duties in accordance with administrator guidance.
- 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 necessary services are disabled and blocks the interfaces connected to the disused port.
- 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 (external log server or separate storage device, etc.) to prevent audit data loss.

5. Architectural Information

The physical scope of the TOE includes: the network appliance, PLOS-PASK-v2.2.2 (which is stored as firmware), and the user guide and installation guide (which are distributed as the printed versions or PDF files). The logical scope of the TOE described in the ST.

- PLOS-PASK-v2.2.2

As the firmware which includes the software module with the security features (e.g. the firewall and protection against SYN floods and illegal packets), operating system and boot loader, this is distributed as the network appliance.

- PAS-K V2.2 User Guide V1.2

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 V1.1

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 nine types of the hardware are: PAS-K1716, PAS-K2424, PAS-K2824, PAS-K4024, PAS-K4224, PAS-K4424, PAS-K4824, PAS-K8220 and PAS-K8620.

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
PAS-K V2.2 User Guide	V1.2	April 6th, 2017
PAS-K V2.2 Installation Guide	V1.1	February 17th, 2017

[Table 5] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor
- Test Purpose: Includes the security functions and modules to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR.

8. Evaluated Configuration

The TOE is PAS-K V2.2. The TOE is product consisting of the following components:

- Hardware Device : PAS-K1716, PAS-K2424, PAS-K2824, PAS-K4024, PAS-K4224, PAS-K4424, PAS-K4824, PAS-K8220 and PAS-K8620
- Firmware : PLOS-PASK-v2.2.2

The Administrator can identify the product name, the firmware version and the hardware model information in the screen of the management system after executing the "show system" command. The hardware model information also displayed on the label attached on the product box and the rear side of hardware equipment itself.

And the guidance documents listed in this report chapter 5, [Table 5] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC and CEM [2].
As a result of the evaluation, the verdict PASS is assigned to all assurance components

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Objectives for the operational environment are clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and they are internally consistent. Therefore the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore the verdict PASS is assigned to ALC_CMS.1.

Also the evaluator confirmed that the correct version of the firmware is installed in the correct model of the hardware device.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable.

Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The functional specifications specifies a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore the verdict PASS is assigned to ADV_FSP.1.

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore the verdict PASS is assigned to ATE_IND.1.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don’t allow attackers possessing basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE administrator must maintain the safe condition of the product, such as changing the password of the administrator periodically.
- The TOE administrator must register the e-mail address of the administrator with the product after product installation so that alert e-mail can be normally sent out in the event of a potential security breach.

- The TOE administrator shall block unauthorized access to the TOE through information protection products such as firewalls.
- The TOE administrator must recognize that the security features provided by the product are different for each network environment (IPv4, IPv6) and properly deploy and operate it.

11. Security Target

PAS-K V2.2 Security Target V1.6 is included in this report for reference. For the purpose of publication, it is provided as sanitized version [6] according to the CCRA supporting document ST sanitizing for publication [7].

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

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

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: The acceleration mode of packet forwarding is supported as Level 1 (4 GBPS).
- M08-L2: The acceleration mode of packet forwarding is supported as Level 2 (8 GBPS).
- H06-L1: The acceleration mode of packet forwarding is supported as Level 1 (6 GBPS).
- H12-L2: The acceleration mode of packet forwarding is supported as Level 2 (12 GBPS).

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

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

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

Installer's PC of the Developers	A personal computer of an installer (from one of the developers) for updating the TOE firmware
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 SSH 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
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
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
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)
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	The server which collects and manages system logs which are generated on the device

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012

[3] Korean National Protection Profile for Network Device V1.1, KECS-PP-0714a-2016

[4] TTA-CCE-16-017 PAS-K V2.2 Evaluation Technical Report V1.3, April 28th, 2017

[5] PAS-K V2.2 Security Target V1.6, April 26th, 2017 (Confidential Version)

[6] PAS-K V2.2 Security Target Lite V1.0, May 18th, 2017 (Sanitized Version)

[7] ST sanitizing for publication, CCDB-2006-04-004, April 2006