KECS-CR-13-24

SNIPER IPS-G V8.0

Certification Report

Certification No.: KECS-NISS-0455-2013

2013. 6. 21

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2013.06.21	-	Certification report for SNIPER IPS-G V8.0 - First documentation

This document is the certification report for SNIPER IPS-G V8.0 of Wins Technet Co., Ltd..

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Laboratory (KTL)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL4 evaluation of SNIPER IPS-G V8.0 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) is network intrusion prevention system (IPS) which protects the internal network assets by detecting and blocking intrusions from the external network. The TOE provides security features such as network intrusion detection and response, security management, security audit, user identification and authentication and updates to the IPS signature.

The TOE SNIPER IPS-G V8.0 is composed of the following components:

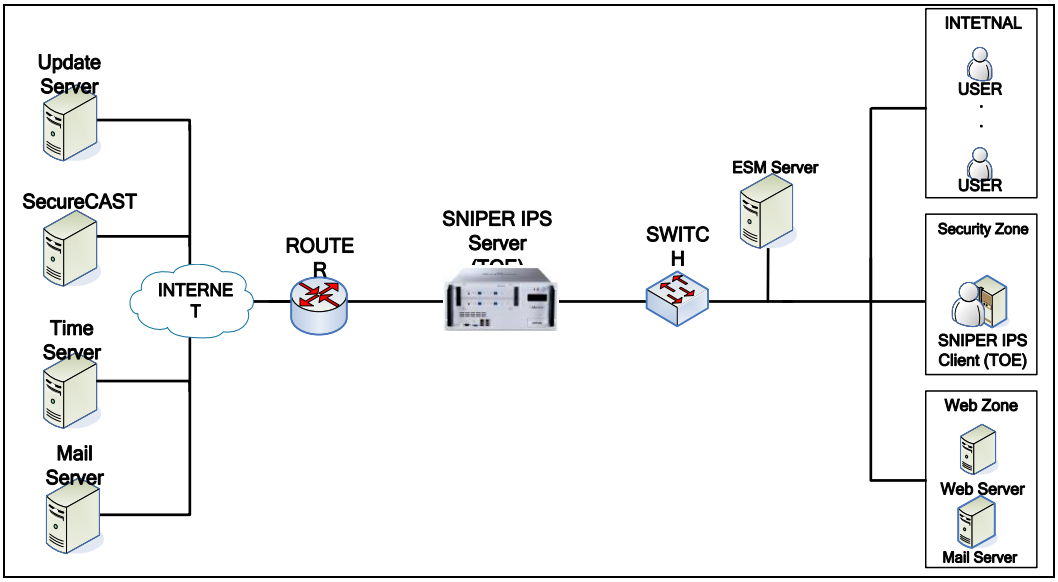
- SNIPER IPS-G V8.0 Server ("IPS Server" hereinafter) with SNIPER OS V2.0, and
- SNIPER IPS-G V8.0 Client ("IPS Client" hereinafter).

The IPS Server provides major security features including network intrusion prevention, and the IPS Client provides user interfaces to the authorized administrators to securely manage the TOE.

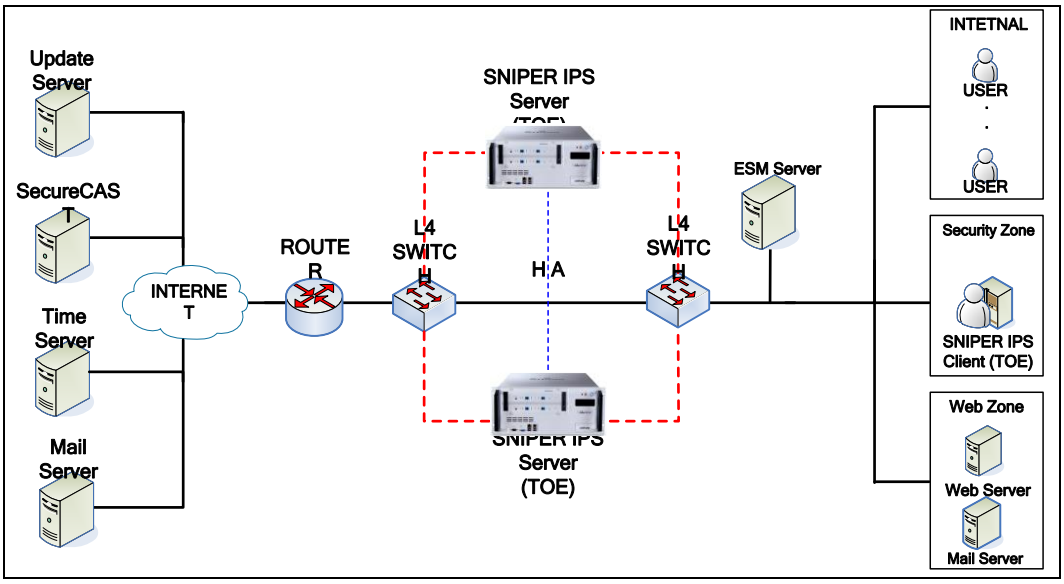
The evaluation of the TOE has been carried out by Korea Testing Laboratory (KTL) and completed on June 4, 2013. This report grounds on the evaluation technical report (ETR) KTL had submitted [5] and the Security Target (ST) [6][7].

The ST claims no conformance to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL4. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

[Figure 1] and [Figure 2] show the operational environment of the TOE. The TOE should be installed and operated in the in-line mode (see [Figure 1].) so that all traffic between external and internal networks passes the TOE. The organization who deploy can choose HA (High Availability) mode (see [Figure 2].) in accordance with the organizational policies in case of hardware failures.



[Figure 1] Operational environment of the TOE – In-line configuration



[Figure 2] Operational environment of the TOE – HA configuration

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 is software consisting of the following components and related guidance documents.

Type	Identifier	Version	Delivery Form
SW	SNIPER IPS-G V8.0 Server	2011.07.01R	Installed on the appliance device
	- SNIPER OS	V2.0 (Kernel 2.6.37)	
SW	SNIPER IPS-G V8.0 Client	GLOBAL_20130115 (20130115_1428)	Downloaded from the IPS Server to administrator's PC when it access to the IPS Server for the first time
DOC	SNIPER IPS-G V8.0 Installation Guidance	V1.02	Hardcopy
	SNIPER IPS-G V8.0 Administrator Manual	V1.02	

[Table 1] TOE identification

The SNIPER OS is customized version of Fedora 14 by upgrading its kernel with Kernel 2.6.37 provided by Kernel.org, removing unnecessary services, and applying configurations necessary for the TOE.

[Table 2] shows underlying platform specifications for the IPS Server.

Model	Contents	
SNIPER IPS 10G	CPU	Intel Xeon Quad 2.66 * 2
	Memory	12GB
	HDD	1TB * 2
	Compact Flash (CF)	2GB
	NIC	10/100/1000Mbps Ethernet Port * 2
	Serial Port	RS232C Serial Port * 1
	Basic Configuration	NIC: 10Gbps Ethernet Port * 2

Model	Contents	
	Expansion Slot Option	1 NIC expansion slot - 10Gbps Ethernet Port * 2
	Max Configuration	Basic + Expansion configuration - 10Gbps Ethernet Port * 2 - 10Gbps Ethernet Port * 2

[Table 2] Underlying platform specifications for the IPS Server

The SNIPER OS is installed on memory storage device, Compact Flash (CF) of IPS server platform, and the IPS server is installed on HDD, and it is used for log data and backup data storage. The IPS Server utilize SQLite V3 to store audit records and the TSF data.

The IPS server provides one 10/100/1000Mbps Ethernet Port for monitoring and the other 10/100/1000Mbps Ethernet Port for HA configuration as a management ports. And another two 10Gbps Ethernet Ports are provided for packet gathering as a default option, and therefore four ports are provided in case of expansion.

[Table 3] shows underlying platform specifications for the IPS Client.

Items		Contents
Hardware	CPU	Intel Xecon Quad 2.66 * 2
	Memory	12GB
	HDD	1TB * 2
	NIC	10/100/1000Mbps Ethernet Port * 2
OS		Microsoft Windows 7 (32bit/64bit) SP1 Microsoft Windows Server 2008 (32bit/64bit) SP2
Web Browser		Internet Explorer 8.0, 9.0

[Table 3] Underlying platform specifications for the IPS Client

The IPS Client is automatically installed by downloading OCXs from IPS server to administrator PC through the Internet Explorer. When generating the IPS Client installation package, Techchart V8 and Fast Report V4 which are 3rd party software are included to provide features such as statistics and reports resulting from audit records.

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation

facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009) Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)
TOE	SNIPER IPS-G V8.0 - SNIPER IPS-G V8.0 Server 2011.07.01R with SNIPER OS V2.0 (Kernel 2.6.37) - SNIPER IPS-G V8.0 Client GLOBAL_20130115 (20130115_1428)
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
EAL	EAL4
Developer	Wins Technet Co., Ltd.
Sponsor	Wins Technet Co., Ltd.
Evaluation Facility	Korea Testing Laboratory (KTL)
Completion Date of Evaluation	June 4, 2013
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [6], [7] as follows:

- Intrusion prevention, protects protected network by ensuring network intrusion detection, analysis, and response functionality. The TOE gathers information for network intrusion detection, determines intrusion based on the detection rules and take response actions in accordance with predefined policies. And the TOE provides ability to review results to the authorized administrators by storing them.
- Security audit, ensures ability to generate and review audit records related to

security events.

- Identification and authentication, ensures ability to identify and authenticate administrators based on the IP address, ID, and password. The TOE also identifies external IT entities which requests services passing through the TOE based on the IP address and port number.
- Security management, ensures ability to securely manage the TOE itself and the TSF data including security attributes.
- TSF protection, ensures ability to protect stored TSF data and TSF executable codes, TSF data transmitted between the IPS Server and the IPS Client, and IPS signatures transmitted from update server to the IPS Server.

4. Assumptions and Clarification of Scope

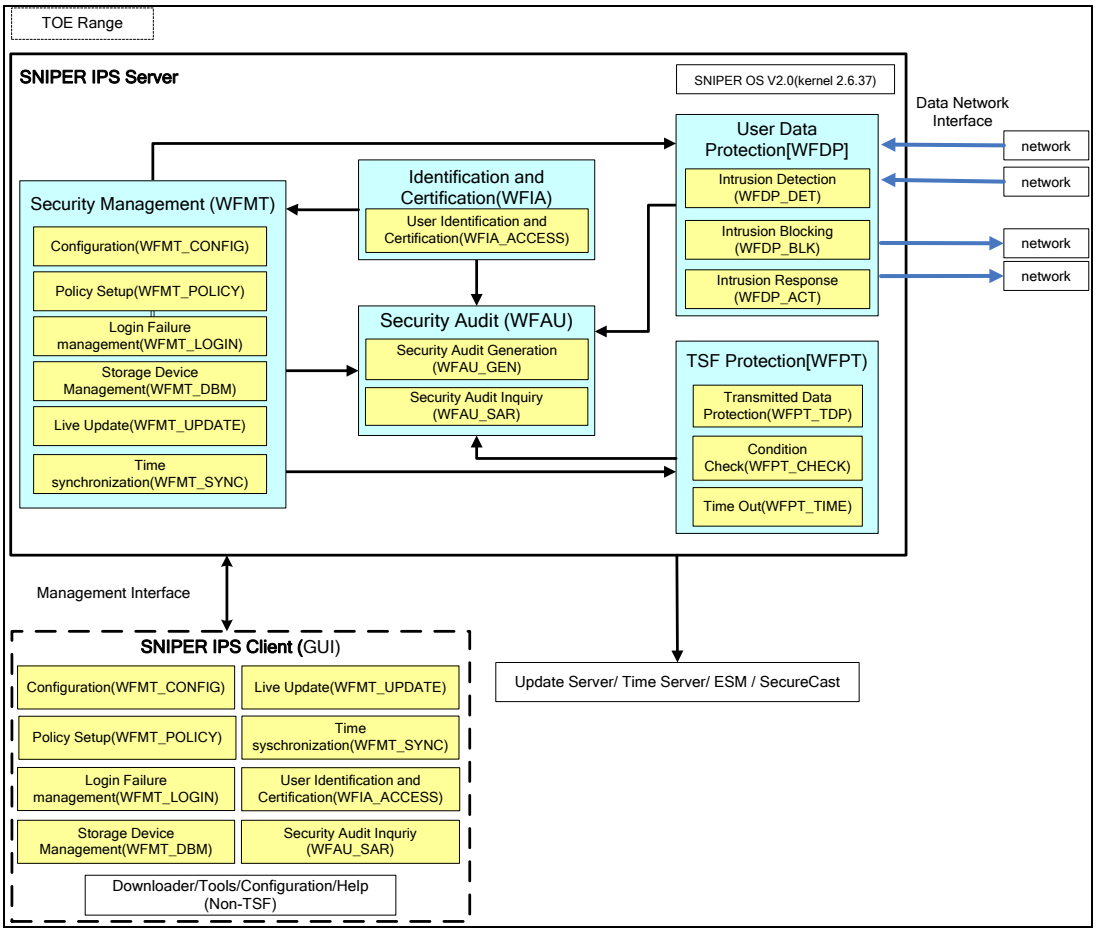
The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [6][7], chapter 3.3):

- The IPS Server is located in a physically secure environment that only the authorized users can access.
- Network configuration changes, an increase or decrease of the host, and when the internal network environment changes such as an increase or decrease of service to reflect the changed environment and security policy the TOE operational policy to maintain the same level of security as before.
- Authorized administrator of the TOE possesses no malicious intention, and received proper training on the TOE management, and performs duties in accordance with the administrative guideline.
- To ensure the reliability and stability of the operating system. Remove unnecessary services on the operating system or by any means, and perform reinforcement on the vulnerabilities of the operating system.
- The TOE allows the separation of the external and internal network, and all communication between the external and internal network is done through the TOE.
- Server for the transmission of text messages, e-mail, and server to provide reliable time-stamp provided by the TOE are located at external professional organization’s physically secure environment.
- Service for update server used by the TOE is provided by WINS Technet Co.,

Ltd. And, to ensure the reliability and stability of the data that is transmitted to the TOE from these servers, the servers to operate ESM server, SecureCAST server, TOE for HA are located in internally / externally secure environment.

5. Architectural Information

[Figure 3] show the scope of the TOE.



[Figure 3] Scope of the TOE

The IPS Server provides major security features including network intrusion prevention, and the IPS Client provides user interfaces to the authorized administrators to securely manage the TOE.

For the detailed description is referred to the ST [6][7].

6. Documentation

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

Identifier	Release	Date
SNIPER IPS-G V8.0 Installation Guidance	V1.02	JAN 15, 2013
SNIPER IPS-G V8.0 Administrator Manual	V1.02	JAN 3, 2013

[Table 5] Documentation

7. TOE Testing

The developer's testing was performed on the final TOE. The developer tested 134 tests for basic functions of the TOE, 2,031 tests against rules based on IPS signatures, 131 module tests.

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.2. This means that the developer tested all the TSFI defined for each life cycle state of the TOE, and demonstrated that the TSFI behaves as described in the functional specification.

The developer tested subsystems (including their interactions), and analyzed testing results according to the assurance component ATE_DPT.1.

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

The evaluator performed all the developer's tests, and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. The tests cover preparative procedures, according to the guidance.

Also, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These test cases cover testing SQL injection, known network protocol attacks, source code weakness analysis, invalid input parameters, and so on. No exploitable vulnerabilities by attackers possessing Enhanced-Basic attack potential were found from penetration

testing.
The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is SNIPER IPS-G V8.0. The TOE is consisting of the following components:

- SNIPER IPS-G V8.0 Server 2011.07.01R with SNIPER OS V2.0 (Kernel 2.6.37)
- SNIPER IPS-G V8.0 Client GLOBAL_20130115 (20130115_1428)

The operational mode of the TOE is shown in [Figure 1] and [Figure 2] of this report.
And the guidance documents listed in this report chapter 6, [Table 5] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1] and CEM [2].
As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL4.

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 Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is

assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The Extended Components Definition has no extended components. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

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 used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.

The developer has used well-defined development tools (e.g. programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results. Therefore the verdict PASS is assigned to ALC_TAT.1.

The developer has clearly identified the TOE and its associated configuration items, and the ability to modify these items is properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence. Therefore the verdict PASS is assigned to ALC_CMC.4.

The configuration list includes the TOE, the parts that comprise the TOE, the TOE implementation representation, security flaws, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.4.

The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Therefore the verdict PASS is assigned to ALC_DVS.1.

The delivery documentation describes all procedures used to maintain security of the

TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, the tools used by the developer throughout the life-cycle of the TOE, the handling of security flaws, and the delivery activity.

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 TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing and SFR-supporting modules and enough information about the SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented; as such, the TOE design provides an explanation of the implementation representation. Therefore the verdict PASS is assigned to ADV_TDS.3.

The developer has completely described all of the TSFI in a manner such that the evaluator was able to determine whether the TSFI are completely and accurately

described, and appears to implement the security functional requirements of the ST. Therefore the verdict PASS is assigned to ADV_FSP.4.
The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.
The implementation representation made available by the developer is suitable for use in other analysis activities. Therefore the verdict PASS is assigned to ADV_IMP.1.
Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed), an implementation description (a source code level description). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.
The developer has tested all the TSF subsystems against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.1.
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 TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
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 Enhanced-Basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.3.

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 or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), don't allow attackers possessing Enhanced-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_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.1	ALC_TAT.1.1E	PASS	PASS	
	ALC_CMS.4	ALC_CMS.4.1E	PASS	PASS	
	ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.1	ALC_DVS.1.1E	PASS	PASS	
		ALC_DVS.1.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
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_TDS.3	ADV_TDS.3.1E	PASS	PASS	PASS
		ADV_TDS.3.2E	PASS	PASS	
	ADV_FSP.4	ADV_FSP.4.1E	PASS	PASS	
		ADV_FSP.4.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
	ADV_IMP.1	ADV_IMP.1.1E	PASS	PASS	
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.1	ATE_DPT.1.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.3	AVA_VAN.3.1E	PASS	PASS	PASS
		AVA_VAN.3.2E	PASS		
		AVA_VAN.3.3E	PASS		
		AVA_VAN.3.4E	PASS		

[Table 6] Evaluation Result Summary

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 administrator must ensure when operating any internal / external network communication it should be done via TOE. It is recommended to apply a security policy for the system accordingly to grasp the amount of normal traffic.

- The TOE is installed in the form of in-line mode between the outside Internet and the internal network or the main networking point for network intrusion prevention. It is recommended to operate with the network boundary protection devices such as DDOS protection device to protect the internal network.
- The TOE provides SSL communication for security management using web-based access, and HTTPS must be used for SSL communication. The certificate for SSL communication must be unique throughout the organization, it is recommended to securely manage that certificate.
- The TOE provides update feature to upgrade the maintenance of up-to-date list of signatures and a new type of intrusion detection. The administrator is recommended to check for updates periodically.
- The TOE is provided by time stamp from external NTP server for audit data generation. The TOE administrator must appropriately manage NTP service to use the TOE accurately.
- The administrator should set only the necessary IPS rules, and delete the unused rules to avoid introduction of potential vulnerabilities.

11. Security Target

SNIPER IPS-G V8.0 Security Target V1.07, JUN 3, 2013 [6][7] is included in this report by reference. For the purpose of publication, it can be provided as sanitized version [7] according to the CCRA supporting document ST sanitising for publication [8].

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

In-line mode	The TOE is configured like bridge, so that all network traffic is passing through the TOE.
HA (High Availability)	Two TOEs are configured, so that, if one of them is brought down, the second one assumes the workload of both of them.

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 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-004, July 2009

[3] Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009)

[4] Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)

[5] 12-402-002 SNIPER IPS-G V8.0 Evaluation Technical Report V1.30, June 4, 2013

[6] SNIPER IPS-G V8.0 Security Target V1.07, June 3, 2013 (Korean Version)

[7] SNIPER IPS-G V8.0 Security Target V1.07, June 3, 2013 (English Version, Sanitized)

[8] ST sanitising for publication, CCDB-2006-04-004, April 2006