KECS-CR-13-24

SNIPER IPS-G V8.0
인증보고서

인증번호 : KECS-NISS-0455-2013

2013년 6월

IT보안인증사무국

1. 제품 개요

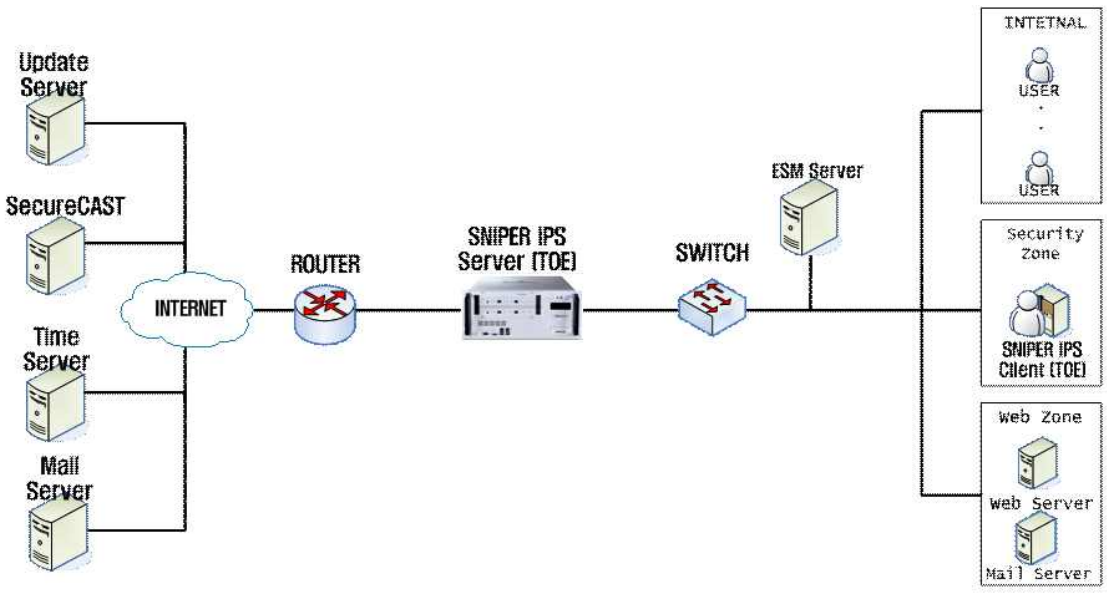
SNIPER IPS-G V8.0(이하 "TOE"라 한다)은 외부 네트워크로부터 유입되는 유해 트래픽을 탐지하고 차단하여 내부 네트워크의 자산을 보호하는 침입방지시스템이다. TOE는 네트워크 공격에 대한 침입탐지 및 침입대응 기능, 보안관리 기능, 사용자에 대한 식별 및 인증 기능, 보안관련 사건을 감사 기록하는 감사 기능, 다양한 통계 및 보고서 제공, 업데이트 기능 등을 제공한다.

TOE는 다음 구성요소 및 관련 설명서로 구성된다.

구 분	식별자	버 전	배포 및 운영 형태
SW	SNIPER IPS-G V8.0 Server (이하 "IPS Server"라 한다)	2011.07.01R	하드웨어 전용장비에 설치되어 배포 및 운영
	- SNIPER OS	V2.0(Kernel 2.6.37)	
SW	SNIPER IPS-G V8.0 Client (이하 "IPS Client"라 한다)	GLOBAL_20130115 (20130115_1428)	IPS Server에 최초 접속 시 관리자 PC로 다운로드, 윈도우 기반 운영체제에 설치 및 운영
문서	SNIPER IPS-G V8.0 설치지침서	V1.02	하드카피
	SNIPER IPS-G V8.0 관리자 설명서	V1.02	

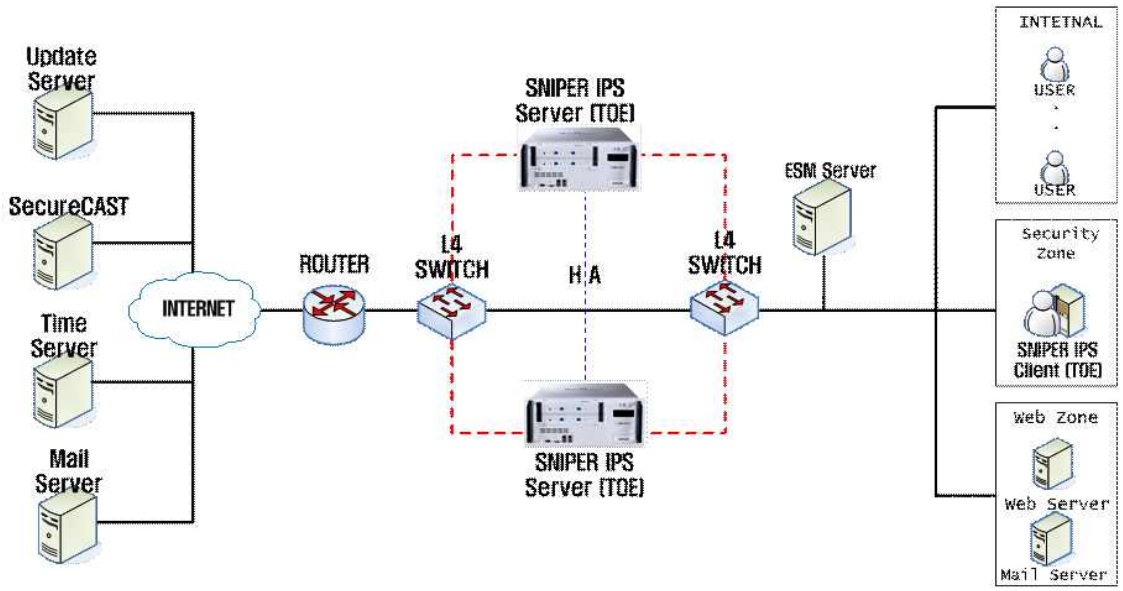
[표 1] TOE 식별정보

IPS Server는 침입방지 기능을 포함한 주요 보안기능성을 제공하며, IPS Client는 인가된 관리자가 TOE를 안전하게 관리하기 위한 UI를 제공한다.



[그림 1] TOE 운영환경 - 단일구성

TOE는 [그림 1]에서와 같이 외부망과 내부망을 연결하는 경계선에 인라인으로 설치되어 운영되어야 하며, TOE를 운영하는 조직의 정책에 의해 [그림 2]에서와 같이 TOE 운영 중에 하드웨어 장애가 발생한 경우 보안정책이 지속적으로 적용될 수 있도록 HA(High Availability) 방식으로 구성하여 운영할 수 있다.



[그림 2] TOE 운영환경 - HA 구성

IPS Server의 전용 하드웨어 모델 요구사항은 다음과 같다.

모델명	내 용	
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
	기본 구성	NIC: 10Gbps Ethernet Port * 2
	확장 구성	NIC 확장 슬롯 1개 - 10Gbps Ethernet Port * 2
	최대 구성	기본 + 확장 구성 - 10Gbps Ethernet Port * 2 - 10Gbps Ethernet Port * 2

[표 2] IPS Server 전용 하드웨어 모델 요구사항

SNIPER OS는 CF 메모리에 탑재되며, IPS Server는 HDD에 탑재된다. IPS Server는 감사 기록 및 TSF 데이터 등을 저장하기 위해 SQLite V3를 사용한다.

IPS Client에 요구되는 시스템 최소 요구사항은 다음과 같다.

항 목		내 용
하드웨어	CPU	Intel Pentium IV 2.4 Ghz 이상
	Memory	512 MB 이상
	HDD	40 GB 이상
	NIC	10/100 Mbps Ethernet Port * 1
운영체제		Microsoft Windows 7 (32bit/64bit) SP1 Microsoft Windows Server 2008 (32bit/64bit) SP2
웹 브라우저		Internet Explorer 8.0, 9.0

[표 3] IPS Client가 설치되는 PC 시스템 최소 요구사항

IPS Client에는 탐지 및 차단 감사기록 통계 차트 및 보고서 생성을 위해 Teechart V8와 Fast Report V4가 포함되어 설치 패키지가 생성된다. IPS Client와 Server간의 통신은 OpenSSL V1.0.1C를 사용하여 보호되며, 업데이트 서버와 TOE간에 전송되는 침입탐지 패턴은 검증필 암호모듈인 SNIPER Crypto V1.3을 사용한 전자서명을 통해 보호된다.

인증 효력에 관한 고지: 상기 제품의 인증서는 IT보안인증사무국 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

2. 주요 기능

TOE가 제공하는 일반적인 보안 특성은 다음과 같다.

■ 보안감사

TOE는 감사대상 사건 발생 시 감사기록을 생성하고 조회할 수 있는 기능을 제공한다. 시스템이 안정적이며 효율적으로 동작하고 있는 지를 확인하기 위하여 시스템 사용에 대한 기록내역을 수집하고 분석하는 기능으로, 생성된 감사기록은 TOE에 대한 침입을 탐지 또는 차단하고, 시스템에 대한 오용을 탐지하기 위하여 사용된다.

■ 식별 및 인증

TOE는 TOE에 접근을 시도하는 관리자를 IP 주소, ID/패스워드를 사용하여 식별 및 인증한다. 관리자 인증 실패 회수가 정의된 회수에 도달하는 경우 일정시간 동안 TOE에 접속을 금지하며, 인가된 관리자가 로그인 후 일정시간 동안 동작하지 않는 경우 TOE와 상호작용하는 세션을 종료한다. 또한, TOE는 TOE를 통해 서비스를 사용하는 외부 IT 실체를 IP, 포트 번호를 사용하여 식별하며, 외부 IT 실체가 일정시간 동안 동작하지 않는 경우 외부 IT 실체의 세션을 종료한다.

■ 사용자 데이터 보호

TOE는 방화벽 기능, 블랙홀 차단 기능, 침입탐지 기능, 침입분석 기능, 침입대응 기능을 수행함으로써 내·외부 공격자로부터 보호하고자 하는 감시 대상 네트워크를 보호한다. 침입탐지를 위한 정보를 수집하고 정의된 규칙에 의하여 침입이라고 판단되면 정의된 대로 침입에 대응하고 분석된 결과를 저장하여 관리자가 검토할 수 있도록 한다.

■ 보안관리

TOE는 보안감사 기능관리, 운영환경 설정, 보안위반 사건 목록관리, 방화벽 기능관리, 보안위반 사건에 대한 ESM 및 관제서버와의 연동기능 관리, IP POOL 관리, 업데이트 수행 등 보안관리 기능을 제공한다.

TOE는 보안관리 기능을 통해 TOE가 제공하는 각종 기능들에 대한 속성과 정보를 조회하거나 설정하고 상태를 검사하며, TOE의 탐지 및 차단 활동을 위한 규칙과 TOE의 상태 및 구성에 관련된 여러 가지 정보를 조회하고 수정하는 관리 기능을 제공한다.

■ TSF 보호

TOE는 저장된 TSF 데이터의 무결성 보호, 전송된 TSF 데이터의 보호, 감사데이터 손실방지, IPS 실행코드 무결성 보호 기능을 제공한다. TOE는 시동 시, 정규 운영 동안 주기적으로, 인가된 관리자 요구 시 실행에 필요한 파일들에 대한 무결성을 검증한다. TOE 시스템의 주요 프로세스들이 정상적으로 운영 중인지 주기적으로 확인하여 장애 발생 시 안전한 상태를 유지하도록 한다.

IPS Server와 Client는 통신 시 전송되는 데이터의 비밀성 및 무결성을 보장하기 위해 SSL 통신을 사용한다. 업데이트 서버와 IPS Server간에 업데이트 되는 침입탐지 패턴은 암호화, 해시값 검증, 전자서명 검증을 통해 보호된다.

3. 평가결과 요약

TOE에 대한 평가는 한국산업기술시험원에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL4 평가보증등급을 만족하여, 공통평가기준 1부 305항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2009. 9. 1) 정보보호제품 평가인증 수행규정 (2012. 11. 1)
평가제품	SNIPER IPS-G V8.0
보호프로파일	없음
보안요구사항	없음
보안목표명세서	SNIPER IPS-G V8.0 보안목표명세서 V1.07 (2013.06.03)
평가보고서	SNIPER IPS-G V8.0 평가결과보고서 V1.30 (2013.06.04)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R3
평가방법론	정보보호시스템 공통평가방법론 V3.1 R3
평가신청인	㈜윈스테크넷
개발업체	㈜윈스테크넷
평가기관	한국산업기술시험원