KECS-CR-12-70

WAPPLES v4.0
인증보고서

인증번호 : KECS-NISS-0426-2012

2012년 11월

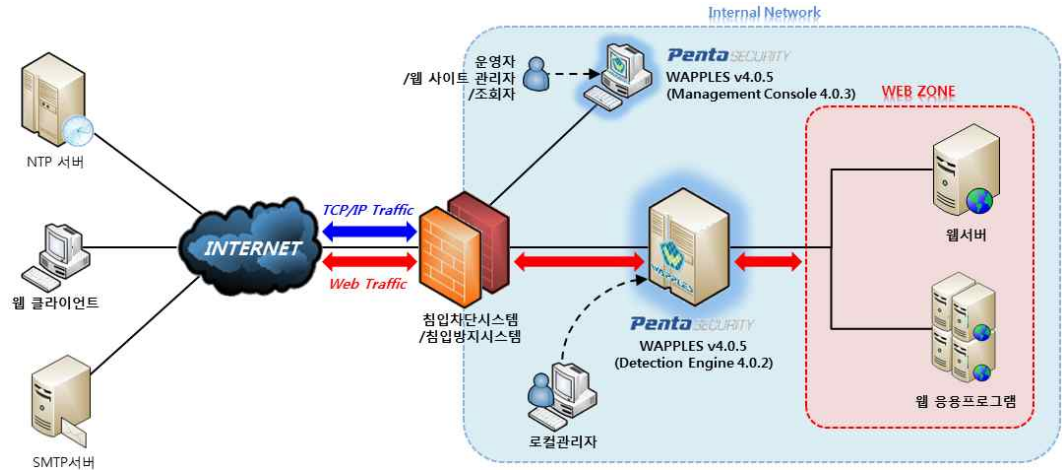
IT보안인증사무국

1. 제품 개요

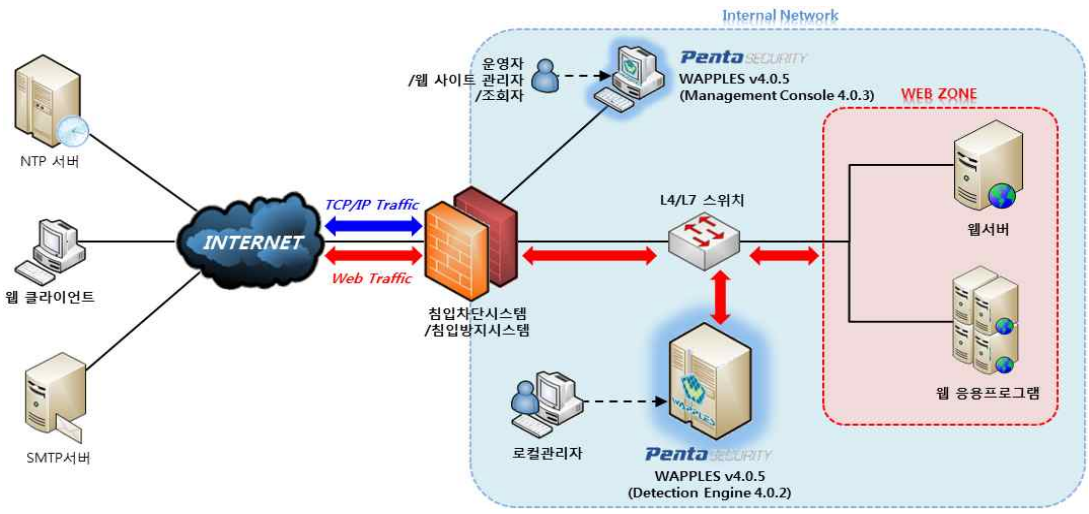
TOE는(WAPPLES v4.0) 웹 트래픽에 대한 정상 여부를 판단하여 사전에 공격을 탐지 및 차단함으로써 웹 서버 및 웹 응용프로그램을 안전하게 보호하는 웹 응용프로그램 침입차단시스템(웹방화벽)이다. TOE는 웹 보안을 위한 웹 요청 및 응답 분석(HTTP 표준 검사, 정규표현식 기반 패턴매칭, URL 접근제어 등), 네트워크 접근제어(IP 접근차단 등), 보안관리, 보안사건 추적, 자체보호 등의 보안기능을 제공한다.

TOE는 외부로부터 유입되는 웹 트래픽을 분석하여 내부 웹 존에 위치한 웹 응용프로그램 및 웹 서버를 외부의 웹 공격으로부터 보호하는 'Detection Engine'과 원격 관리자에게 보안정책 및 TOE 운영환경 설정 등의 보안관리 기능을 제공하는 'Management Console'로 구성된다.

TOE의 운영환경은 설치 및 운영되는 위치에 따라 인라인 모드(Inline mode)와 리버스 프락시 모드(Reverse proxy mode)로 구분된다([그림 1] 및 [그림 2] 참조)



[그림 1] 인라인 모드(Inline Mode)



[그림 2] 리버스 프락시 모드(Reverse Proxy Mode)

TOE는 전용 하드웨어에 탑재되어 사용자에게 배포되는 소프트웨어 형태의 Detection Engine, 관리자PC에 설치되는 소프트웨어 형태의 Management Console 및 책자로 배포되는 설명서로 구성된다. Detection Engine 설치 이미지에는 Management Console이 포함되어 배포되며 관리자가 관리자PC에서 Detection Engine에 접속하여 Management Console를 다운로드 받아 설치한다.

구분	내용	배포형태
WAPPLES v4.0.5	Detection Engine 4.0.2	하드웨어에 탑재되는 소프트웨어
	Management Console 4.0.3	소프트웨어
사용자 설명서	WAPPLES v4.0 운영 및 설치 설명서 v4.0	책자

[표 1] TOE 물리적 범위

Detection Engine을 운영하는 TOE 하드웨어는 100 eco, 1000 Type2, 1000 Type2 Plus 이며 하드웨어 사양은 다음과 같다.

하드웨어 모델	구분	내용
WAPPLES-100 eco	CPU	Intel Core2 Quad 2.66 GHz
	하드디스크	500 GB
	메모리	4 GB
	네트워크 인터페이스	▪ Management port : 10/100/1000 BaseTX * 2 ▪ Service port : 10/100/1000 BaseTX * 8
WAPPLES-1000 Type2	CPU	Intel Xeon Quad Core 2.33 GHz * 2
	하드디스크	500 GB
	메모리	8 GB
	네트워크 인터페이스	▪ Management port : 10/100/1000 BaseTX *2 ▪ Service port: - 10/100/1000 BaseTX * 8 - 1000 BaseSFP * 2 ▪ Optional Service port: - 1000 Base Optical * 2
WAPPLES-1000 Type2 Plus	CPU	Intel Xeon Quad Core 2.50 GHz * 2
	HDD	500 GB
	Memory	8 GB
	Network interface	▪ Management port : 10/100/1000 BaseTX *2 ▪ Service port: - 10/100/1000 BaseTX * 8 - 1000 BaseSFP * 2 ▪ Optional Service port: - 1000 Base Optical * 2

[표 2] Detection Engine 운영 하드웨어 사양

Management Console이 설치 및 운영되는 관리자PC의 하드웨어 최소사양은 다음과 같다.

구분	내용
CPU	Intel Pentium4 1.6 GHz 이상
하드디스크	100 GB 이상
메모리	1 GB 이상
네트워크 인터페이스	100/1000 Mbps

[표 3] Management Console 운영 하드웨어 사양

2. 주요기능

Management Console을 통해 제공되는 주요 보안기능은 다음과 같다.

■ 원격관리자 로그인

Management Console은 인가된 사용자에게만 보안관리 기능을 제공하기 위해 원격관리자 로그인 기능을 제공한다. 로그인에 성공한 원격관리자는 역할에 따라 운영자, 웹사이트관리자, 조회자 권한을 부여받는다. Management Console은 원격관리자의 연속 인증 실패 시 해당 원격관리자 계정을 일시 잠금하고 원격관리자의 비 활동 시간이 일정시간을 초과하는 경우 보안관리 화면을 잠금하여 비 인가된 관리자의 접근을 방지한다.

■ 보안관리

Management Console은 관리자 계정 관리, 운영환경 및 네트워크 설정, WEB SFP 및 WEBCLIENT SFP 설정을 수행할 수 있는 능력을 원격관리자로 제한한다.

■ 모니터링

Management Console은 감사데이터 조회 및 검색, 웹 공격 탐지 통계정보 조회, TOE 시스템 현황 조회 능력을 원격관리자로 제한한다.

Detection Engine을 통해 제공되는 주요 보안기능은 다음과 같다.

■ WEB SFP에 기반한 웹 공격 차단, 웹 컨텐츠 및 웹 보안요소 보호

Detection Engine은 원격관리자가 설정한 WEB SFP에 기반하여 외부로부터 보호대상 웹 서버로 시도되는 다양한 공격들을 탐지 및 대응하고 쿠키(Cookie) 값과 Hidden field 값에 대한 보호와 웹 컨텐츠에 대한 유출을 방지한다. 다음과 같은 공격 탐지 및 분석 기법에 따라 보안기능을 수행한다.

① HTTP 표준검사를 통한 비정상적인 웹 트래픽 차단
② 공격 기법별 분석을 통해 다양한 공격 패턴 탐지 및 차단
③ 정규표현식을 이용한 패턴 매칭
④ 접근이 허용된 URL로의 접속 허용
⑤ Cookie 및 히든필드 등의 웹 보안요소 보호

■ WEBCLIENT SFP에 기반한 비인가된 접근 차단

Detection Engine은 접근 차단 목록에 등록된 IP를 가진 웹 클라이언트에서의 HTTP 요청을 우선적으로 차단한다. 또한 HTTP DoS공격 및 탐지 규칙 누적위험도 조건에 따라 공격자라 의심되는 IP를 자동으로 차단목록에 등록하여 차단한다.

■ 자체보호 및 감사데이터 보호 기능

Detection Engine은 주기적으로 실행파일 및 설정데이터 등에 대한 무결성 위·변조 여부와 프로세스의 상태 점검을 통해 보안기능의 가용성을 보장한다. 또한, PostgreSQL DB 및 CouchDB의 가용 용량을 주기적으로 점검하여 지정된 임계치를 초과하는 경우 적절한 조치를 취할 수 있도록 지정된 관리자에게 경고한다.

■ CLI 보안관리 기능

Detection Engine은 로그인을 통해 로컬관리자에게만 네트워크 환경 등을 설정할 수 있는 CLI 보안관리 인터페이스를 제공한다.

3. 평가결과 요약

TOE에 대한 평가는 한국시스템보증에서 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. 1. 1)
평가제품	WAPPLES v4.0
보호프로파일	없음
보안요구사항	없음
보안목표명세서	WAPPLES v4.0 보안목표명세서 v4.0
평가보고서	WAPPLES v4.0 평가결과보고서 V1.00 (KOSYAS-2011-20-ETR V1.00)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R3
평가방법론	정보보호시스템 공통평가방법론 V3.1 R3
평가신청인	펜타시큐리티시스템(주)
개발업체	펜타시큐리티시스템(주)
평가자	한국시스템보증(주) 최태경, 정재구