WAPPLES

제품소개서

2016년
펜타시큐리티시스템㈜

SL2 CONFIDENTIAL Internal Only

목차

I. 웹방화벽(WAF) 개요
1. 웹방화벽(WAF) 이란?
2. 웹방화벽(WAF) 도입의 필요성

II. WAPPLES 소개
1. 제품소개
2. 제품구성도
3. 주요기능
4. 제품특장점
5. 제품라인업

III. WAPPLES 제품군 소개
1. WAPPLES V-Series
2. WAPPLES MS (Management System)

IV. 참고자료
1. 주요 레퍼런스
2. 인증 현황/ 수상 현황/ 특허 현황
3. 도입사례:증권사/ 금융권/ 사설교육기관

I. 웹방화벽(WAF) 개요

1. 웹방화벽(WAF) 이란?
2. 웹방화벽(WAF) 도입의 필요성

1. 웹방화벽(WAF) 이란?

웹방화벽 = Web Application Firewall (WAF)

- 일반적인 네트워크 방화벽 (Firewall)과는 달리 웹 애플리케이션 보안에 특화되어 개발된 제품입니다.

- 기본 역할은 SQL Injection, XSS등이라 불리는 웹공격들을 차단하는 것입니다.
  - 웹공격은 외부에서 웹을 통해 웹사이트나 웹서버를 타켓으로 하는 공격을 의미합니다.

- 기존의 웹방화벽은 웹공격 대응 기능만을 제공하였습니다만,
  최근에는 정보유출방지, 부정접근방지, 위변조 방지 등의 기능까지 제공하는 웹방화벽도 등장하였습니다.

1. 웹방화벽(WAF) 이란?

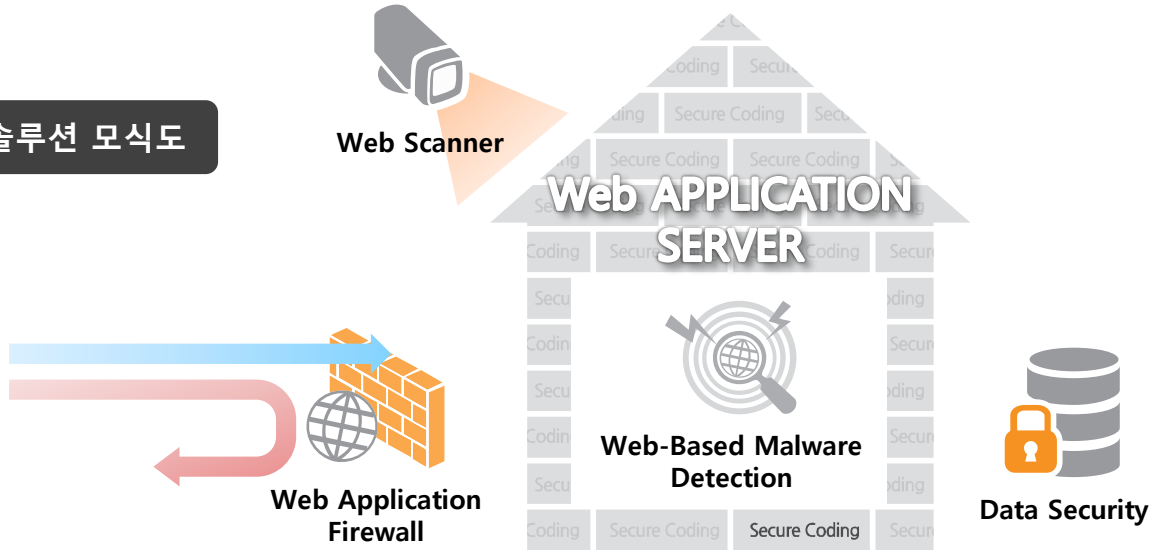
웹방화벽의 역할 = "집(애플리케이션)을 지키는 울타리"

- 웹방화벽은 웹을 통한 외부의 침입이나 웹 공격을 탐지하고 대응하는 역할을 수행합니다.

- 시큐어코딩, 웹 스캐너가 담당하는 웹 보안 취약점을 외부에 노출되지 않도록 보완해 줄 뿐만 아니라,
  외부 공격을 사전에 차단하는 역할을 수행하며, 웹서버 악성코드가 웹서버로 업로드되는 것 역시 막아 줍니다.
  - 일반적인 방화벽(Firewall)과 다르게 웹방화벽이 웹 애플리케이션에 특화되어 개발되어 있기에 가능

- 다른 솔루션과 달리 서버에 구축/적용하는 비용이 들지 않고, 외부에 편리하게 설치가 가능합니다.

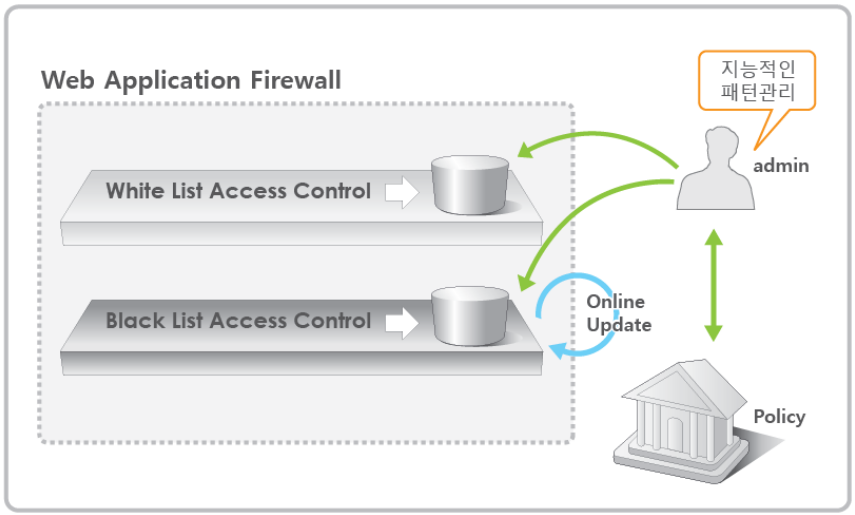
웹 애플리케이션 보안 솔루션 모식도



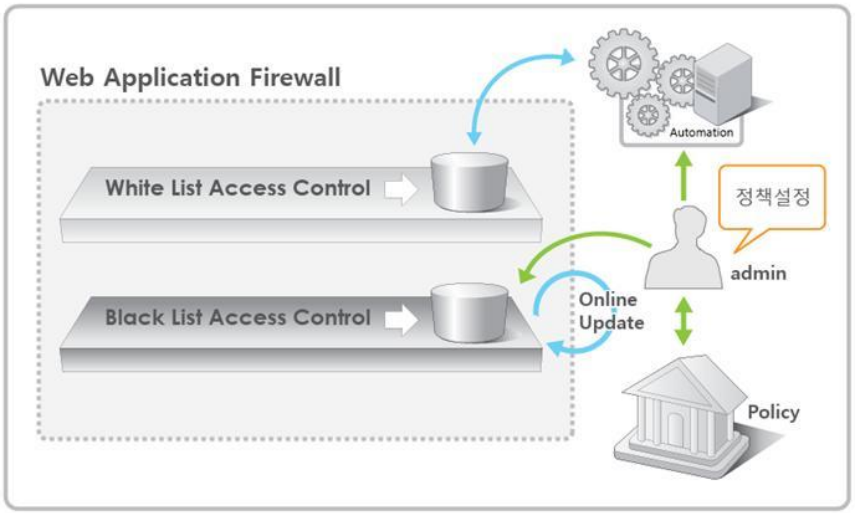
1. 웹방화벽(WAF) 이란?

1세대, 2세대 웹방화벽 = 블랙리스트 (Black List) + 화이트리스트 (White List) 병행 방식 사용

- 1세대: 자동으로 온라인 업데이트 되는 블랙리스트와 관리자가 직접 생성 및 관리하는 화이트리스트
- 2세대: 자동으로 온라인 업데이트 되는 블랙리스트와 몇 주간의 모니터링 결과를 기반으로 자동으로 생성되는 화이트리스트
- 문제점
  - 웹 공격 유형과 무관하게 통으로 블랙리스트와 화이트리스트를 관리 => 다양한 공격에 대한 분석 없이 대응하여 다량의 오탐 발생
  - 공격 유형의 다양화에 따른 등록된 시그니처 수 증가 => 성능 저하 발생
  - 고객 환경에 따라 다른 적용이 필요한 화이트리스트와 블랙리스트의 검토가 필수적으로 필요 => 관리자의 관리 부담 발생



< 1세대 웹방화벽 개념도 >

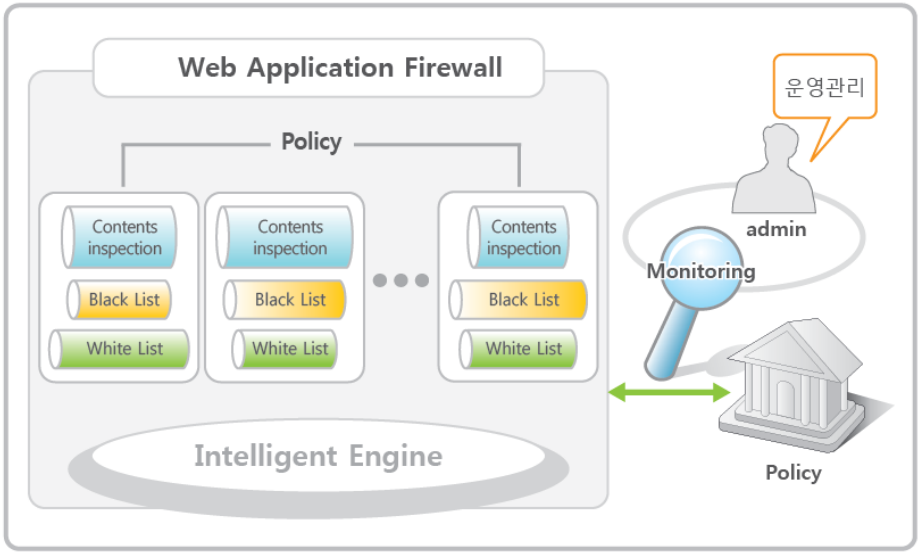


< 2세대 웹방화벽 개념도 >

1. 웹방화벽(WAF) 이란?

3세대 지능형 웹방화벽 = 논리 분석 기반 공격 탐지

- 웹 공격 유형별로 블랙리스트/ 화이트리스트 탐지 ,웹 트래픽 컨텐츠 분석 등의 기법들을 로지컬하게 결합하여 공격을 탐지합니다.
- 웹 공격 유형별 로직에 따라 웹 트래픽 컨텐츠를 검사하여 공격 진위 여부까지 판단하기 때문에 1, 2세대 웹방화벽 대비 오탐률이 낮습니다.
- 시그니처 기반 탐지가 아닌 공격 로직 분석을 통한 탐지를 수행하기 때문에 신종 변종 공격에 대해서도 즉각적 대응이 가능합니다.
- 최소한의 신규 시그니처 추가만으로도 변종 공격 방어가 가능하여 성능 저하 이슈 발생률도 적습니다.
- 관리자의 시그니처 관리 부담이 사라져 효율적인 보안 관리가 가능해졌습니다.



< 3세대 웹방화벽 개념도 >

1. 웹방화벽(WAF) 이란?

보안 장비 별 탐지현황 비교 – OWASP TOP 10

OWASP Top 10 (2013)	Network Firewall	IDS / IPS	WAF
A1: Injection	X	△	○
A2: Broken Authentication and Session Management	X	△	○
A3: Cross Site Scripting (XSS)	X	△	○
A4: Insecure Direct Object References	X	X	○
A5: Security Misconfiguration	X	X	○
A6: Sensitive Data Exposure	X	X	○
A7: Missing Function Level Access Control	X	X	○
A8: Cross Site Request Forgery (CSRF)	X	X	○
A9: Using Components with Known Vulnerabilities	X	○	○
A10: Unvalidated Redirects and Forwards	X	X	○

*** OWASP Top Ten Web Application Security Vulnerabilities(2013)**

1. 웹방화벽(WAF) 이란?

보안 장비 별 탐지현황 비교 – GARTNER REPORT

- WAF, IPS 및 NGFW의 주요 기능 비교
  - L7 계층에 대한 보안 확보는 WAF를 통해서만 가능합니다.

Figure 2. Main Differences Between WAF, IPS and NGFW

	Web Application Firewall	Intrusion Prevention System	Next-Generation Firewall
Multiprotocol Security	○	●	●
IP Reputation	◑	◑	◑
Web Attack Signatures	●	◑	○
Web Vulnerabilities Signatures	●	◑	◑
Automatic Policy Learning	●	○	○
URL, Parameter, Cookie, and Form Protection	●	○	○
Leverage Vulnerability Scan Results	●	◑	○

L4 계층

L7 계층

● = good to very good ◑ = average or fair ○ = below average

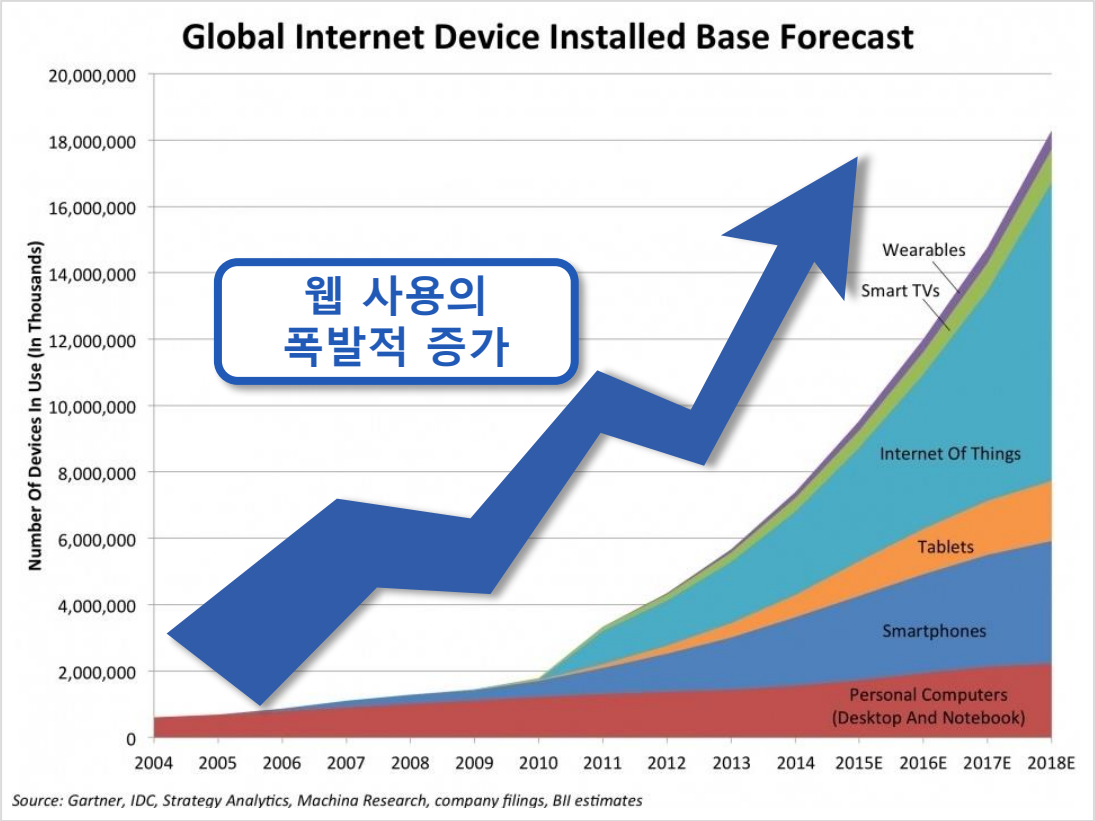
IP = Internet Protocol

* Source: Gartner Report (February 2014)

2. 웹방화벽(WAF) 도입의 필요성

웹 대중화 시대의 도래

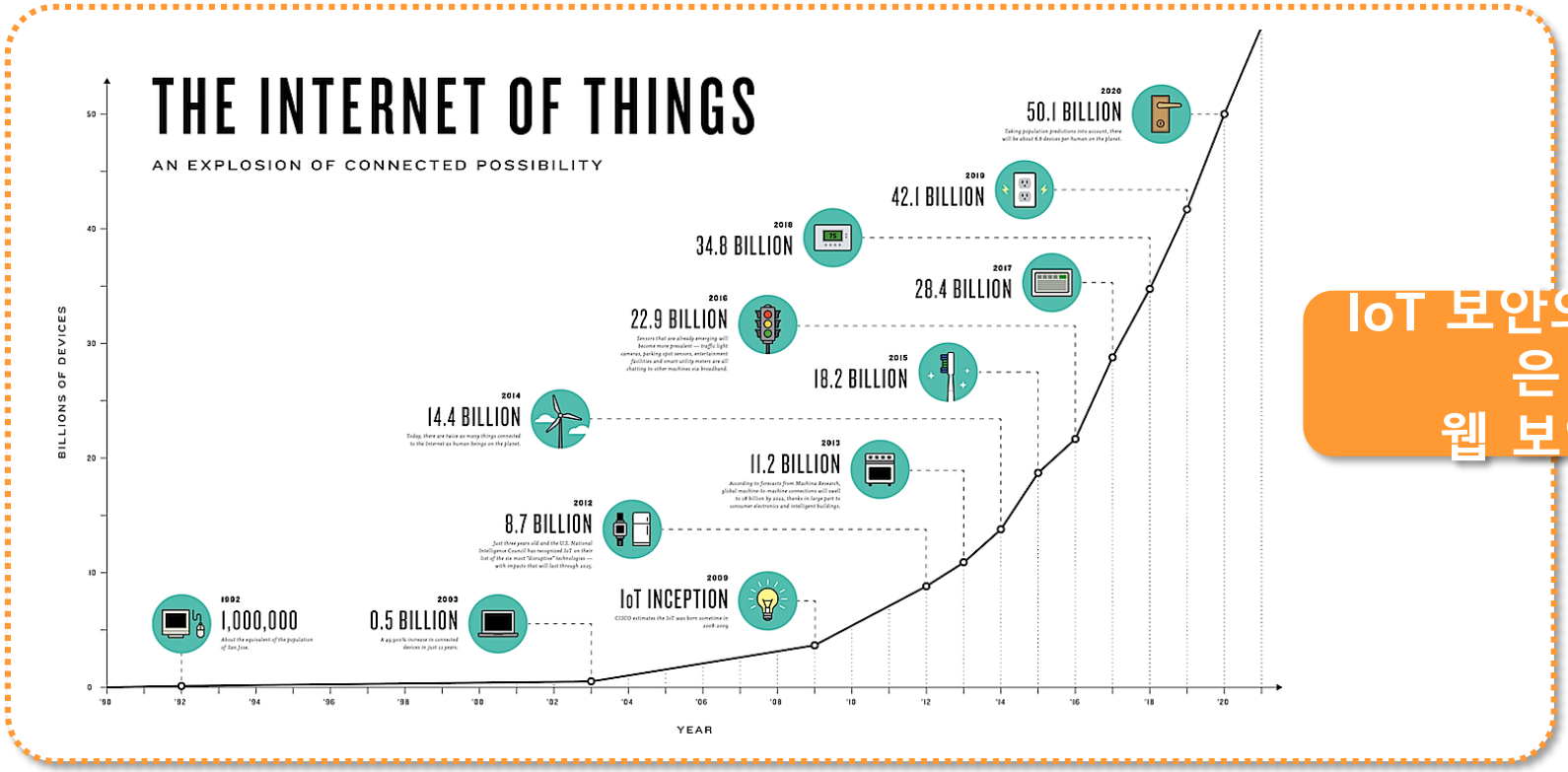
- 스마트폰, 태블릿 PC등의 사용이 급증하면서 기존의 웹 개념을 초월한 웹 대중화 시대가 도래하였습니다.
- 웹의 대중화와 더불어 웹 위협에 대한 노출 가능성도 폭발적으로 증가하였지만 많은 사용자들이 보안의 필요성에 대해서 인식하지 못하고 있는 것이 현실입니다.



2. 웹방화벽(WAF) 도입의 필요성

IoT 보안의 핵심은 [웹]

- IoT(The Internet of Things, 사물 인터넷)란 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미합니다.
- IoT 시대에는 모든 사물(가전제품, 모바일 장비, 웨어러블 컴퓨터 등)이 웹 해킹의 대상이 될 수 있어 IoT를 위한 웹보안이 반드시 필요합니다.

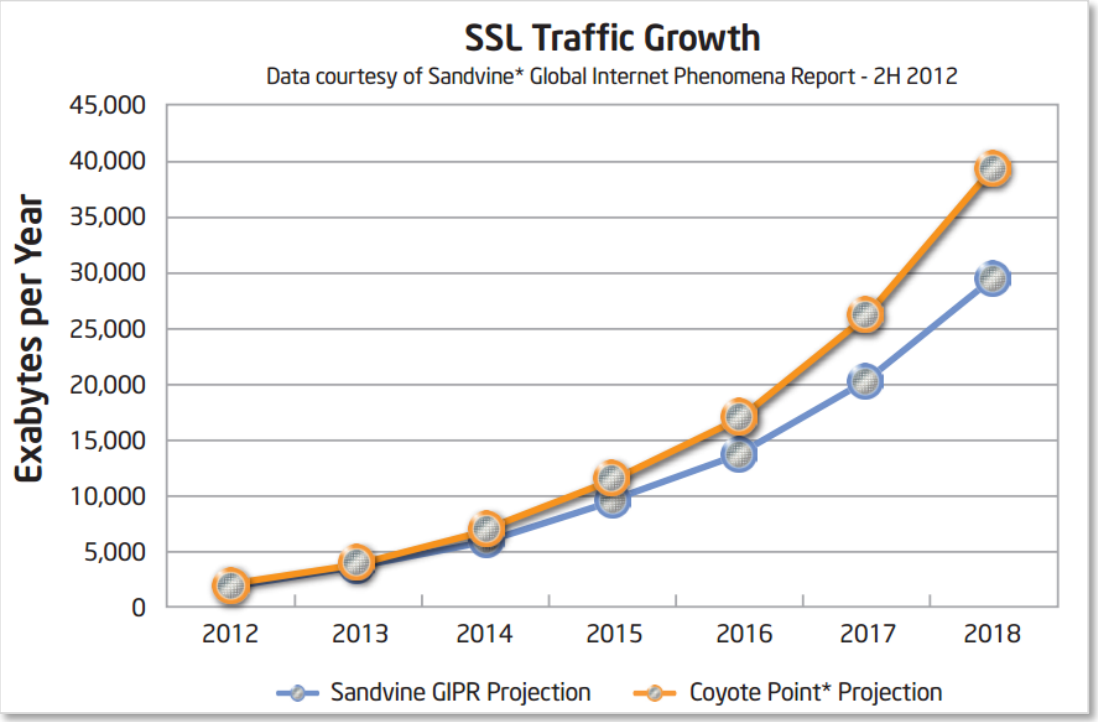


IoT 보안의 핵심은 웹 보안!

2. 웹방화벽(WAF) 도입의 필요성

안전한 웹 통신을 위해 SSL (Secure Socket Layer) 사용률 급증

- 웹 사용률 증가와 더불어 웹을 통해 이루어지는 통신을 암호화하여 보호하는 SSL의 사용이 빠르게 증가하고 있습니다.
  - ❖ SSL (Secure Socket Layer)란, Netscape 사에서 웹서버와 브라우저 사이의 보안의 위해 개발한 것으로, Certificate Authority (CA)라 불리는 서드 파티로부터 서버와 클라이언트 인증을 하는데 사용됩니다.
- 하지만 SSL 트래픽을 이용하여 웹공격을 시도하는 것 역시 가능하기 때문에 이는 임시방편에 불과 합니다.
- => SSL트래픽에 담긴 Web Attack 을 탐지하고 방어할 수 있는 유일한 솔루션은 [웹 방화벽] 입니다!



2. 웹방화벽(WAF) 도입의 필요성

최근 이슈가 되었던 사이버 공격들의 경우 모두 웹을 통한 공격

- 옥션 해킹 사건 (2008년 02월)
  - 피해 규모: 1,000만 건 이상의 개인 정보 유출
  - 웹을 통해 웹 서버 해킹 후 DB 서버에 접속하여 개인 정보 유출

- 네이트 (SK컴즈) 해킹 사건 (2011년 07월)
  - 피해 규모: 3,500만 건 이상의 개인 정보 유출
  - 알집 업데이트 서버 해킹으로 해당 웹을 통해 내부 PC가 감염
    -> 감염된 내부 PC로부터 DB 서버 접속이 이루어져 개인 정보 유출

- EBS 해킹 사건 (2012년 05월)
  - 피해 규모: 200만 건 이상의 개인 정보 유출
  - 웹사이트 게시판 취약점을 통한 웹 서버 해킹 (웹을 통한 웹쉘 업로드)을 통한 공격으로 밝혀짐

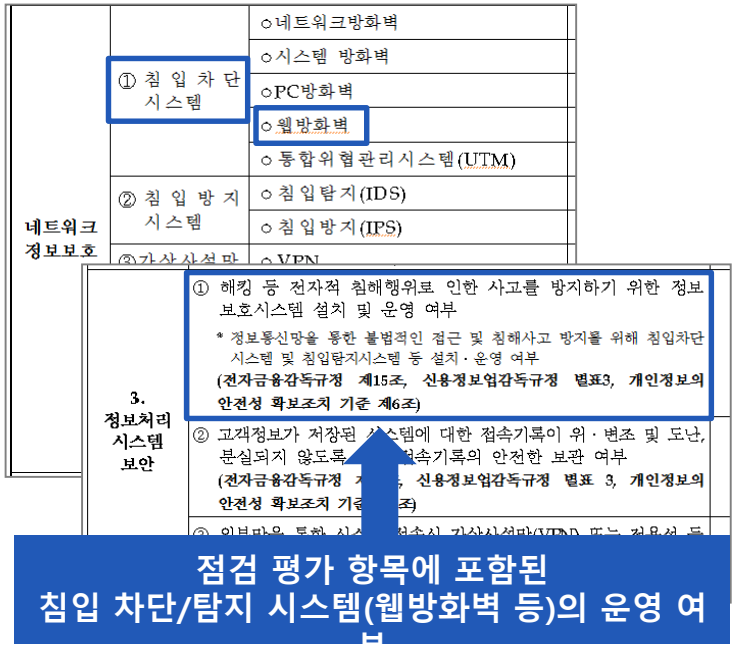
- 3.20 사이버 테러 (2013년 03월)
  - 피해 규모: 악성 코드에 의한 주요 금융/언론사의 기업 내부 시스템 파괴
  - 웹사이트 게시판 취약성을 이용한 웹 서버 해킹으로 1차 및 2차 C&C(명령제어) 서버를 확보
    -> 동시에 악성코드를 통해 목표 기업의 내부 PC를 감염 시킴
    -> C&C 서버를 통해 감염시킨 내부 PC에 내부 정보 수집을 위한 추가 악성코드를 배포
    -> 업데이트 관리서버를 감염시켜 파괴 악성코드를 배포하여 기업 내부 시스템을 파괴함

- => 대규모 피해를 막기 위해선 안전한 웹보안 구축이 필수!

2. 웹방화벽(WAF) 도입의 필요성

금융 감독원, 접근 제어와 침해사고 방지를 위한 침입 차단/탐지 시스템 (웹방화벽) 운영을 권고

- 금융감독원에서 금년 초의 대량 개인정보 유출 사고 관련하여 동일 사건 재발생 방지를 위한 목적으로 2014년 1월 27일 [고객 정보 보호 실태 점검 요청] 공문을 시행, 주요 금융 회사에 고객 정보 보호 관련 향후 추진 계획 및 점검 리스트를 전달하여 금융 회사의 정보 유출 방지 대책 및 정보 관리의 적정성에 대한 평가를 진행하였습니다.
- => 해당 자료에서 웹방화벽을 언급하며 침입 차단 시스템으로서의 운용 필요성을 언급하고 있습니다.



2. 웹방화벽(WAF) 도입의 필요성

(정보통신망법) 개인 정보의 보호 조치 기준 해설서에서 접근 제어와 침입 차단 시스템 운영 강조

- 금융감독원에서 [고객 정보 보호 실태 점검 요청] 에 체크 항목으로 포함시켰던 접근 제어와 침입 차단 시스템 운영은 이미 정보 통신망법에서 의무 사항으로 명기되어 있는 항목입니다.
- 정보통신망법의 개인 정보의 보호 조치 기준은 권고가 아닌 법률에 의해서 반드시 준수해야 하는 의무사항을 구체화 한 것으로, 기준 위반 시 법률에 따른 형사처벌이나 행정 처분이 부과될 수 있습니다.
- 2012년에 고지된 개정판 해설서에서 웹방화벽을 직접적으로 언급, 침입 차단/탐지 시스템 도입의 필요성을 강조하고 있습니다.
  - 2012년 9월 해설서 제4조 (접근통제) 제5항

⑤정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

▶ 침입차단 및 침입탐지 기능을 갖춘 설비의 설치 방법

- 일정 규모 이상의 개인정보처리시스템을 운영하고 있는 사업자는 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치·운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS : Intrusion Prevention System), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다.

II. WAPPLES 소개

1. 제품소개
2. 제품구성도
3. 주요기능
4. 제품특장점
5. 제품라인업

SL2 CONFIDENTIAL Internal Only

1. 제품 소개 (1/6) – Why WAPPLES?

새로운 웹 공격에 대응하기 위해 빠르게 진화하는 지능형 웹방화벽(WAF), WAPPLES!!

- WAPPLES는 웹 공격 유형 별로 공격을 분석하여 탐지하는 로직 분석 기반의 지능형 웹방화벽입니다.
  - 웹공격 대응 뿐만 아니라 정보 유출 방지, 부정접근방지, 웹위변조 방지 솔루션으로써의 역할도 수행
- OWASP Top 10 취약점에 대해 모두 대응이 가능한 수준 높은 보안성을 제공합니다.
- 웹쉘 탐지 기능 고도화를 통해 웹방화벽을 우회하여 업로드 된 웹쉘에 대해서도 차단합니다.

클라우드 환경에 최적화된 WAPPLES Cloud

- Virtual Image 형식의 웹방화벽인 WAPPLES V-Series를 제공

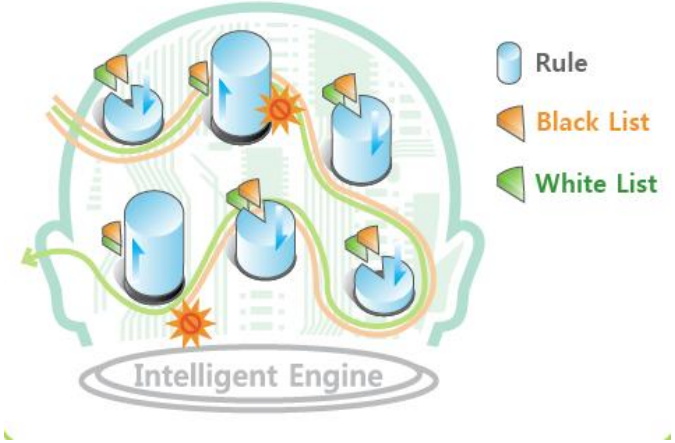
최신 웹 공격 동향 정보 제공 및 실시간 모니터링 서비스

- 신뢰할 수 있는 통계 자료 기반의 Web Application Threat Report
- WAPPLES에 대한 실시간 모니터링 및 원격 관리를 할 수 있는 WMP 서비스

1. 제품 소개 (2/6)

3세대 지능형 웹방화벽, WAPPLES

- 독창적인 지능형 논리 분석 엔진을 탑재하여 알려지지 않은 공격을 차단
  - 웹 공격을 유형 별로 분석 및 탐지하기 위한 총 26개의 룰과 IP Block 기능을 탑재
  - 다양한 형태로 시도되는 웹 공격으로부터 서버를 안전하게 보호
  - 정확한 탐지를 통하여 오탐률이 낮음
- 쉬운 보안 설정과 운영 편리성



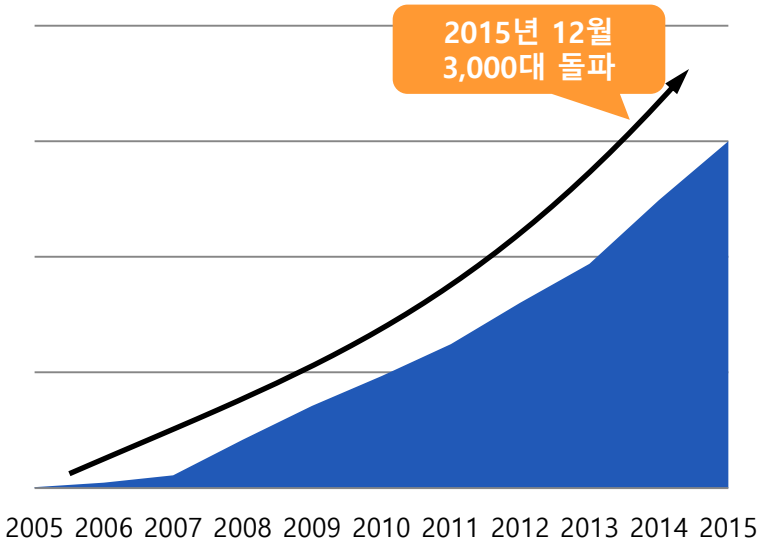
< 인간의 지능을 닮은 Intelligent COCEP Engine >
(COCEP: Contents Classification and Evaluation Processing)

< 3세대 지능형 웹방화벽 WAPPLES >

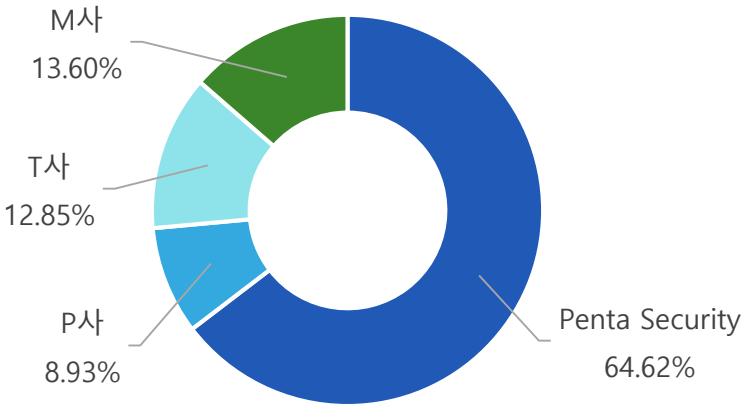
1. 제품 소개 (3/6) - 국내 시장 점유율

8년 연속 시장 점유율 1위 기록, 가장 많은 고객이 선택한 웹방화벽 WAPPLES

- 한국에서 2008년 이후 8년 연속 시장점유율 1위를 유지하고 있는 가장 많은 고객이 선택한 웹방화벽(WAF) 입니다. (출처: 나라장터 조달 통합 정보 시스템)



< WAPPLES 판매 대수 (출시 이후) >



< Percentage of the WAF market>
(*2012년 ~ 2015년 4Q까지의 조달 판매 점유율 정보를 기준으로 작성)

1. 제품 소개 (4/6) - 국내 시장에서의 평가

3년 연속 조달청 계약 이행 실적 평가에서 최우수 등급을 획득한 제품, WAPPLES

- 2013년~2015년 3년 연속으로 납기, 품질, 수요기관 만족도, 서비스, 계약 이행 성실도 등을 평가하는 조달청 계약 이행 실적 평가에서 총점 100점으로 최우수 등급을 획득한 우수한 제품입니다.

계약이행실적평가결과 안내

평가결과 상세보기

지표				지표 배점	평가결과		
분류	평가지표	평가기준	평가방법		평점	점수 환산	등급
납기	납기 준수율	납품기한 내에 납기된 비율	(납품기한 내로 납품한 건수..	13	13	100.0	최우수
	평균 납기지체일수	납품기한을 넘겨 지체된 평균일수	납품 지체된 건의 지체일수의..	12	12		
품질	품질 만족도	수요기관 만족도 조사 중 품..	품질 만족도 점수의 합/품질..	12	12	100.0	최우수
	조달품질신문고 ..	해당업체에 대한 조달품질신문..	해당업체 하자조치 요구 총 ..	9	9		
수요기관 만족도	서비스 만족도	수요기관 만족도 조사 중 서..	서비스 만족도 점수의 합/서..	6	6	100.0	최우수
	종합 만족도	수요기관 만족도 조사 중 종..	종합 만족도 점수의 합/종합..	6	6		
	가격 만족도	수요기관 만족도 조사 중 가..	가격 만족도 점수의 합/가격..	6	6		
서비스	납품 품목 비율	해당업체의 등록 품목수 대비..	(납품이 이루어진 해당업체의..	8	8	100.0	최우수
	조달품질신문고 ..	수요기관의 하자조치 요구시점..	하자조치 요구 후 경과 일수..	8	8		
계약이행 성실도	부정당업자 제재..	최근 1년 이내 부정당업자 ..	부정당업자 제재 기간	10	10	100.0	최우수
	쇼핑몰 거래정지..	최근 1년 이내 다수공급자계..	쇼핑몰 거래정지 기간	10	10		
가점	가점	가점	가점	2	0		
				총점 : 100.0		등급 : 최우수	

< 조달청 3자단가계약 계약이행실적 평가 결과 >

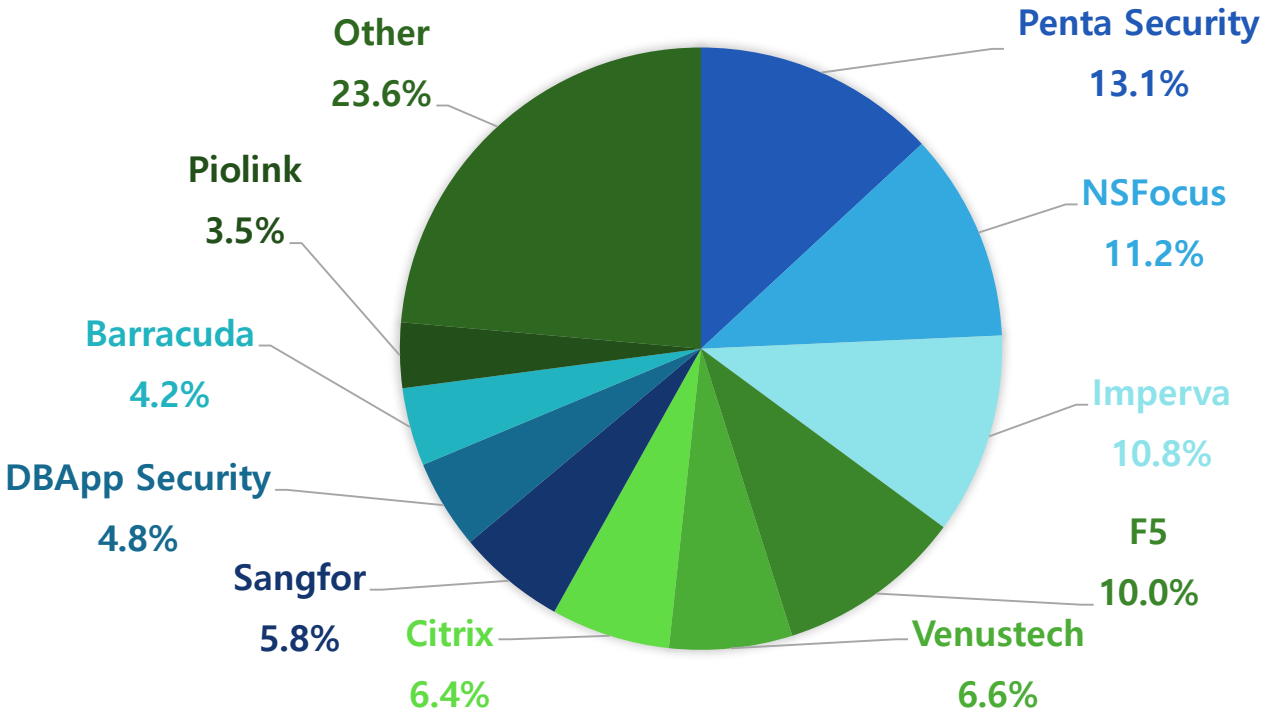
1. 제품 소개 (5/6) - 국내 시장에서의 평가

- 삼성그룹 국내 전사 표준
- LG전자
- KT
- 포스코건설
- LOTTE
- 대우인터내셔널
- 아모레퍼시픽
- KBS 한국방송공사
- MBC 문화방송
- SBS 콘텐츠 허브
- 이베이코리아
- 배달통
- 티켓몬스터
- 홈앤쇼핑
- 한국도미노피자
- 한국맥도날드
- 법무법인 율촌
- 녹십자
- KT&G
- 한국야쿠르트
- NH농협은행
- KB국민은행
- 한국은행
- IBK자산운용
- 현대증권
- 하나SK카드
- 삼성생명
- HMC투자증권
- 서울신용평가정보
- 나이스평가정보
- 국방부
- 국세청
- KRX 한국거래소
- 국회
- 국토해양부
- 대법원
- 안전행정부
- 한국전력공사
- 금융감독원
- 정부통합전산센터

1. 제품 소개 (6/6) - 해외 시장 점유율

APAC (Asia Pacific) 지역 시장 점유율 3년 연속 1위를 기록한 자랑스런 국내 기술 웹방화벽, WAPPLES

- WAPPLES은 제품의 우수성을 인정 받으면서 APAC 지역을 선두로 서서히 해외에서의 입지를 넓혀가고 있습니다.
  (출처: Asia Pacific Web Application Firewall Vendors 2015 by Frost & Sullivan)

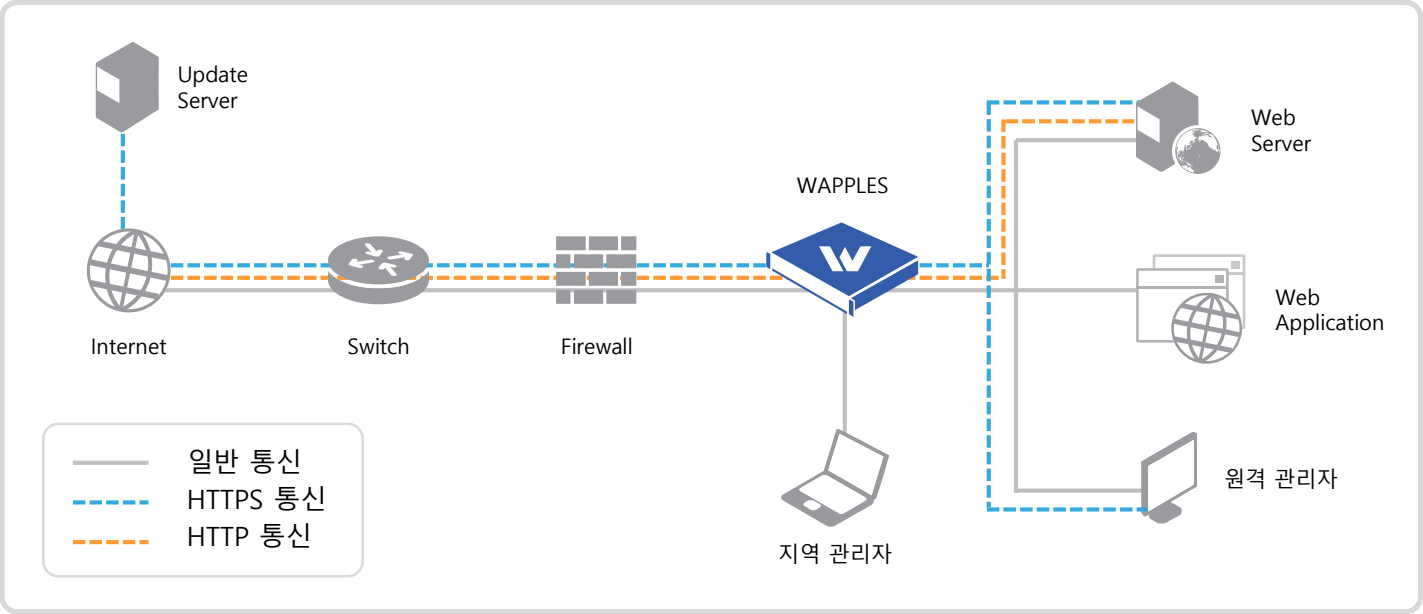


Source: Frost & Sullivan 2015 Frost Industry Quotient

2. 제품 구성도 (1/2)

인라인 (Inline) 모드, 프록시 (Proxy) 모드 도입 가능

- 기존 네트워크 환경에 변경 없이 도입이 가능합니다.
- 인라인(Inline)모드, 리버스 프록시(Reverse Proxy)모드, T.프록시(Transparent Proxy)모드
- 고가용성(HA)을 위한 이중화 구성 등 고객 니즈에 최적화 된 다양한 네트워크 환경 지원

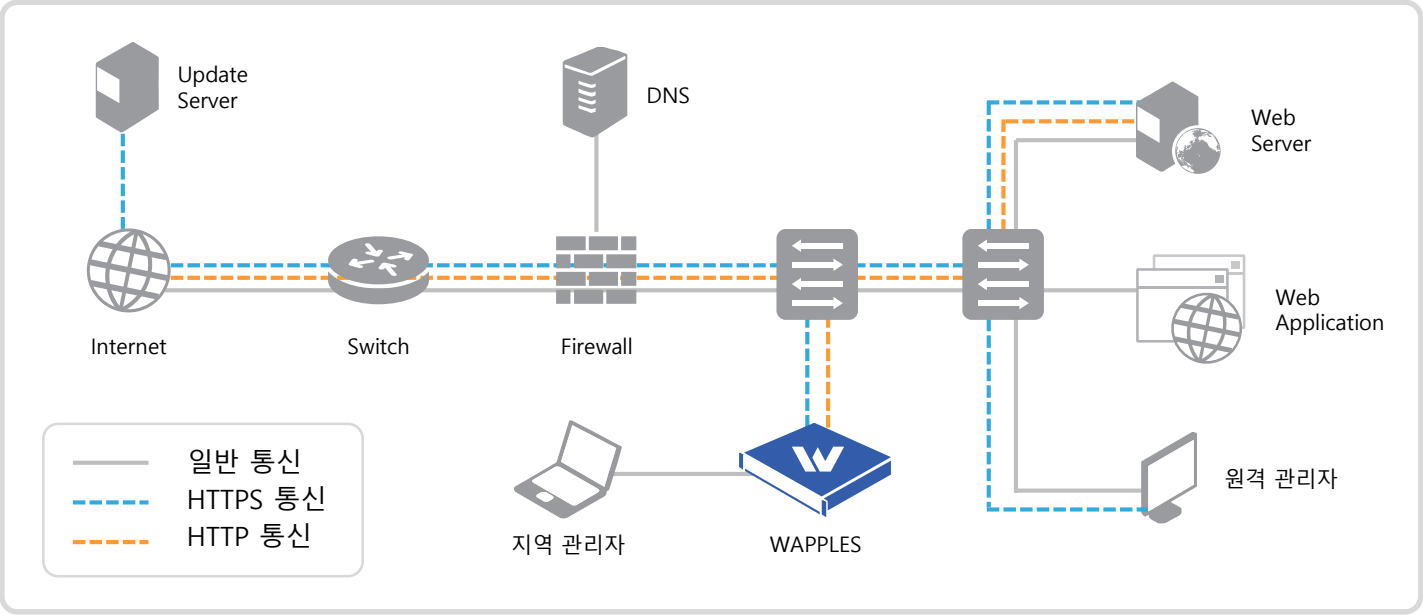


< 인라인(Inline)모드 구성 방식 >

2. 제품 구성도 (2/2)

인라인 (Inline) 모드, 프록시 (Proxy) 모드 도입 가능

- 기존 네트워크 환경에 변경 없이 도입이 가능합니다.
- 인라인(Inline)모드, 리버스 프록시(Reverse Proxy)모드, T.프록시(Transparent Proxy)모드
- 고가용성(HA)을 위한 이중화 구성 등 고객 니즈에 최적화 된 다양한 네트워크 환경 지원

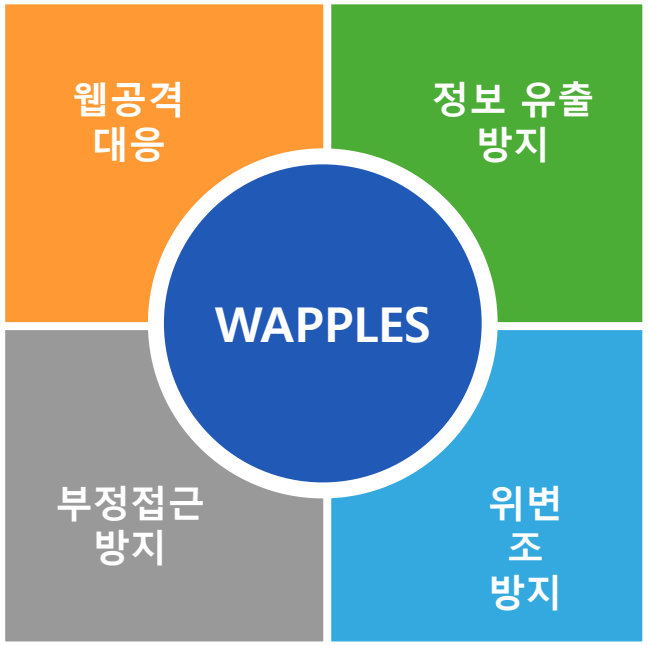


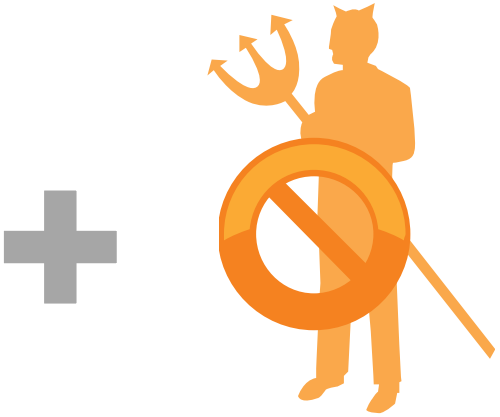
<리버스 프록시 (Reverse Proxy)모드 구성 방식 >

3. 주요 기능

WAPPLES에서 제공하는 4가지 솔루션 (4 in 1)

- WAPPLES은 웹공격 대응부터 정보 유출 방지, 부정 접근 방지, 위변조 방지 기능까지 제공합니다.
- 정부 또는 특정 회사의 중요 정보 획득, 정치적 목적, 사이버 테러 등을 목적으로 하는 범죄 그룹에 의한 사이트, 기업, 개인을 상대로 지속적으로 해킹 공격을 하는 지능적 지속 위협인 APT(Advanced Persistent Threat)에 대한 대응이 가능합니다.





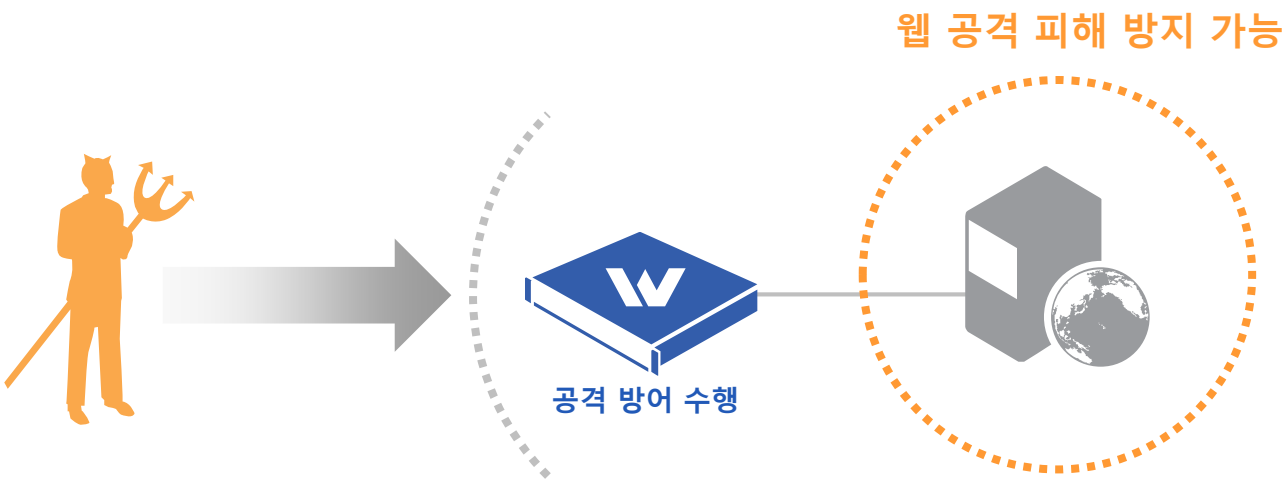
APT 공격을 포함하는
신종 공격에 대응

3. 주요 기능 - 웹공격대응솔루션

WAPPLES은, 직접적인 웹 공격에 대해 탐지 및 차단을 수행합니다

- 아래와 같이 잘 알려진 웹 공격 및 2차 공격 수행을 위한 정보 수집 목적의 1차 공격에 대해 대응이 가능합니다.

  - SQL 쿼리를 통해 DB 시스템 명령어를 활용하여 DB 시스템 조작 및 위변조가 가능한 공격에 대해 대응합니다.
  - 고객이 실행할 가능성이 있는 악성코드를 이용한 공격에 대해 대응합니다.
  - 변형된 악성 파라미터를 웹사이트로 보내는 공격에 대해 대응합니다.
  - 웹 서버에서 실행될 수 있는 파일을 업로드하여 하는 공격에 대해 대응합니다.
  - 신뢰할 수 없는 파일과 외부 URI의 삽입을 이용한 공격에 대응합니다.
  - 웹사이트의 디렉터리와 파일 유출을 목적으로 하는 공격에 대해 대응합니다.
  - 공격으로 정의된 패턴을 등록하여 해당 공격에 대응합니다.

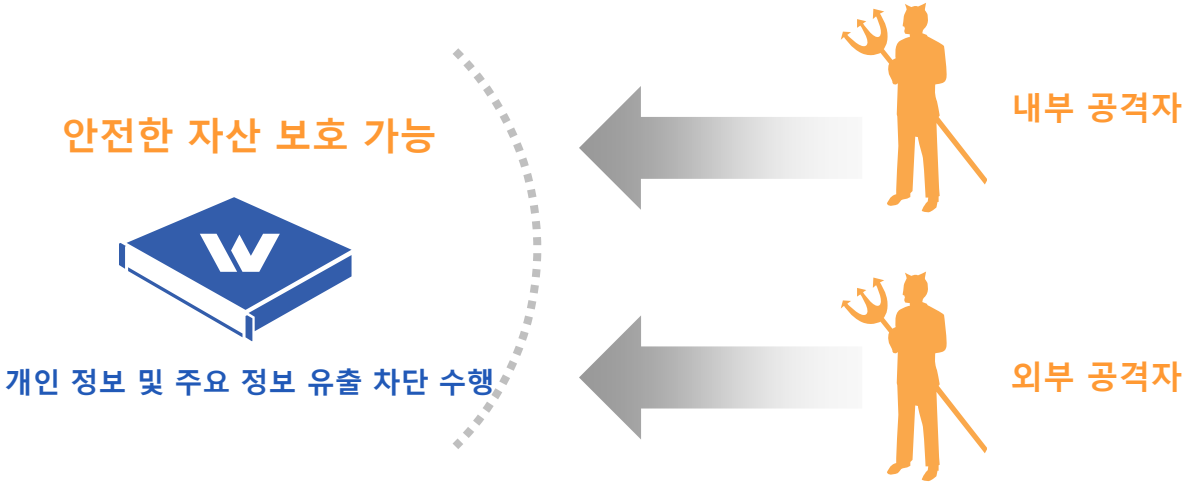


3. 주요 기능 - 정보유출방지솔루션

WAPPLES은, 개인 정보의 외부 유출을 목적으로 하는 공격에 대해 탐지 및 차단을 수행합니다.

- 개인정보가 웹 게시판에 게시되거나 개인 정보가 포함된 파일 등이 웹을 통해 업로드/다운로드 되는 경우에 대해서 탐지 및 대응이 가능합니다.

  - 검증 메커니즘을 통한 개인정보 유출을 방지합니다.
  - 300여 종의 업로드 파일 내의 개인정보 포함 여부를 검사하여 유출을 방지합니다.
  - 웹 서버, WAS, DBMS 서버 등에 대한 에러 메시지를 관리함으로써 정보의 유출을 방지합니다.
  - 내부 주요 정보를 포함하는 파일 관련 정보 및 파일의 유출을 방지합니다.

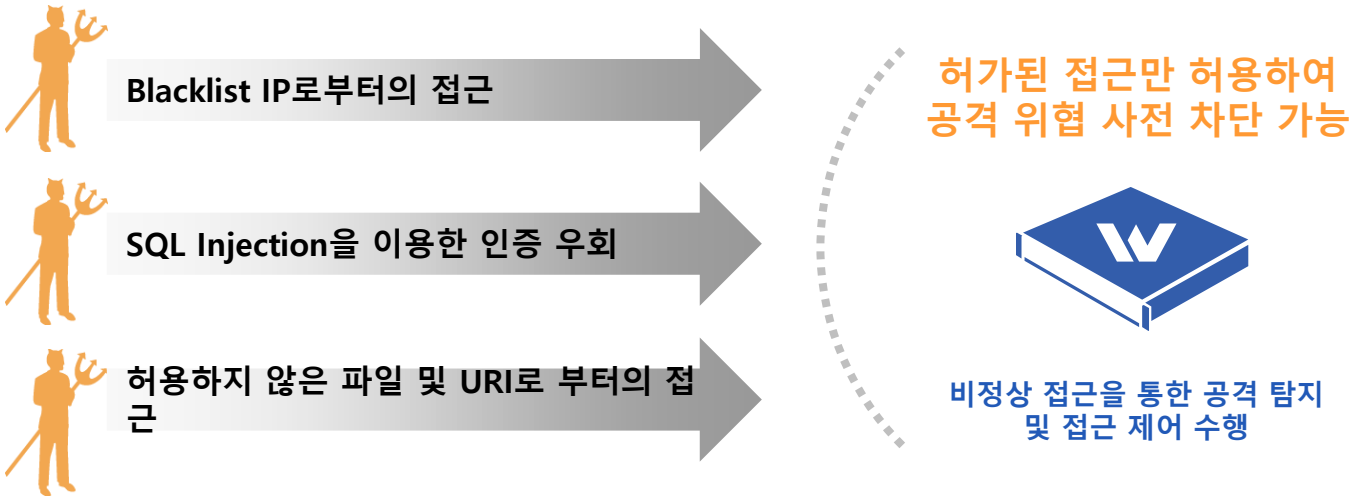


3. 주요 기능 - 부정접근방지솔루션

WAPPLES은, Brute Force Attack 등과 같은 비정상적인 접근에 대해 탐지 및 차단을 수행합니다.

- 추정 가능한 모든 경우의 수를 대입하여 웹사이트에 로그인을 시도하는 경우와 같은 비정상적인 접근에 대한 대응 및 사용자가 공격으로 정의한 행위에 대해 접근 제어를 통한 탐지 및 대응이 가능합니다.

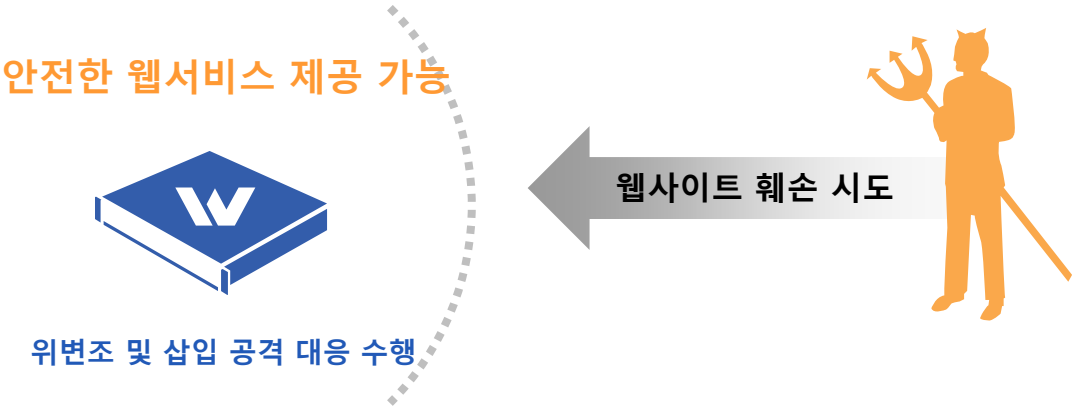
  - 관리자 권한 없이도 특정 서버에 처리할 수 없을 정도로 대량의 접속 신호를 한꺼번에 보내 해당 서버가 마비 되도록 하는 서비스 거부 공격에 대응합니다.
  - 특정 기간 동안 같은 출발지 IP로부터 설정 값 보다 많은 접근 시도가 이루어지는 것에 대한 제어 및 대응합니다.
  - SQL Injection을 이용한 인증 우회에 대응합니다.
  - 공격으로 확인된 특정 IP 범위나 특정 국가로 부터의 접근을 탐지하고 차단합니다.
  - 파일의 확장자가 사용자가 허용한 확장자가 아닐 경우에 대해서 접근 제어를 수행합니다.
  - 특정 URI와 파일로 부터의 접근 요청을 제어합니다.



3. 주요 기능 - 웹위변조방지솔루션

WAPPLES은, 웹 위변조에 대해 탐지 및 차단을 수행합니다.

- 해커가 사이트를 해킹한 후에 자신의 행동을 과시하는 목적으로 주로 사용하는 웹사이트 변조에 대해서 탐지 및 대응 가능합니다.
- 삽입 (Injection) 기술을 이용한 공격에 대해서 탐지 및 대응이 가능합니다.
  - 웹사이트의 훼손(위변조)을 탐지하고 이에 대해 웹 페이지를 복구를 수행합니다.
  - 인증정보를 담고 있는 쿠키의 변조에 대응합니다.
  - DB에 저장된 데이터 값을 조회, 열람, 삭제, 추가가 가능한 공격 (내부 DB 변조 목적의 공격)에 대응합니다.
  - 공격자가 피해자의 브라우저 내에서 스크립트의 실행하여 사용자의 웹사이트가 변조 가능한 공격에 대응합니다.
  - WAPPLES의 웹구간(웹브라우저-웹서버) 에서의 데이터 암호화를 통해 파라미터 변조 공격에 대응합니다.



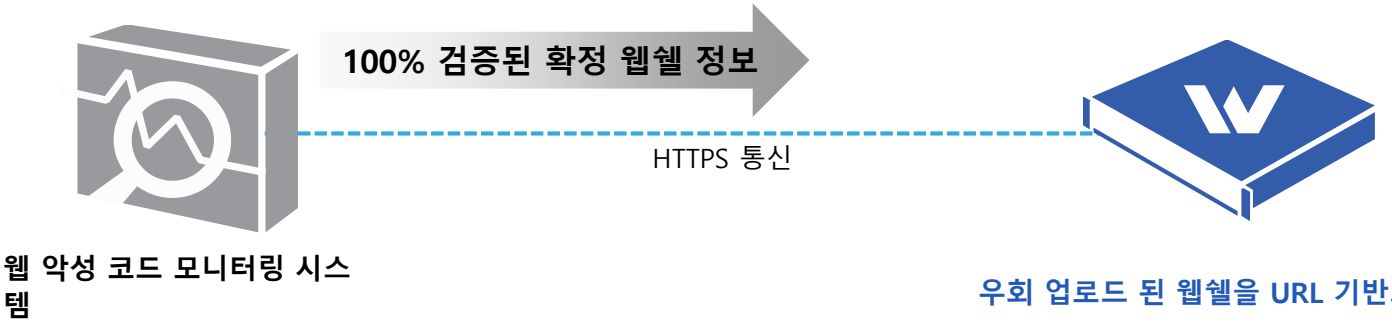
3. 주요 기능 – 고도화된 웹쉘 탐지 기능

WAPPLES는 웹쉘 공격을 탐지하는 기능을 제공합니다.

- 오탐률이 낮은 고도화된 웹쉘 공격 탐지
  - 웹 악성 코드 모니터링 시스템에서 수집된 웹쉘 공격 리스트를 전달 받아 보안 정책에 적용

- 웹쉘 공격이 웹방화벽을 우회하여 업로드 된 경우에 대해서도 공격 탐지 및 차단이 가능
  - 웹 악성 코드 모니터링 시스템에서 HASH 값 검증을 통해 100% 웹쉘로 판명된 URL 리스트를 WAPPLES에 전달 합니다. (오탐 가능성이 거의 없음)
  - 우회하여 업로드 된 웹쉘의 URL 리스트를 전달 받은 후 WAPPLES의 차단 리스트에 등록하여 탐지 시 차단합니다.

고도화된 웹쉘 탐지/차단 기능 제공



3. 주요 기능 – Gartner에서 정의한 WAF 기능

WAPPLES은, Gartner에서 정의한 웹방화벽(WAF)의 주요 기능을 모두 만족합니다.

	Web Application Firewall	논리 분석 기반 지능형 웹방화벽 WAPPLES
Multiprotocol Security	○	-
IP Reputation	◑	IP Block 및 IP Filtering 룰을 통한 접근 제어 (Blacklist/Whitelist)
Web Attack Signatures	●	SQL Injection, XSS 등과 같은 주요 공격에 대해서는 논리 분석 기반으로 공격 탐지/대응
Web Vulnerabilities Signatures	●	특정 애플리케이션이나 S/W의 알려진 취약점에 대해서는 User Defined Pattern 룰을 통해 탐지 및 대응
Automatic Policy Learning	●	(시그니처 기반 웹방화벽 제품에 필요한 기능)
URL, Parameter, Cookie, and Form Protection	●	Parameter Tampering, Cookie Poisoning, Website Defacement 룰 등을 이용하여 탐지 및 대응
Leverage Vulnerability Scan Results	●	취약점 분석 후 대응이 필요한 패턴에 대해 User Defined Pattern 등록을 통해 탐지 및 대응

● = good to very good ◑ = average or fair ○ = below average

IP = Internet Protocol

4. 제품특장점

오탐 없는 높은 보안성 보장 (기능성)

- 지능형 엔진 COCEP 탑재로 변형 공격 및 새로운 공격에 대한 즉각적 탐지가 가능합니다.
- 애플리케이션 레벨의 웹서비스 거부 공격(DDoS공격) 차단이 가능합니다.
- 검증 메커니즘(Luhn algorithm : ISO/IEC7812 등)을 이용한 정확한 개인정보 검사 및 차단이 가능합니다.

쉽고 편리한 보안 관리 (사용성)

- 기존 네트워크 환경의 변경 없이 설치가 가능합니다.
- GUI 기반 관리 콘솔을 이용하여 간편하게 보안 설정이 가능합니다.
- 웹서버, 도메인 등록만으로 보안기능 적용이 가능합니다.

안정적인 고성능 제공 (효율성)

- 공격 탐지 정책 최적화를 통해 고성능을 제공합니다.
- 인메모리 컴퓨팅 (In-Memory Computing) 기술 채용을 통한 고성능 처리가 가능합니다.
  - 인메모리 컴퓨팅이란 어플리케이션을 구동하는 컴퓨터의 메인 메모리에서 데이터를 저장/처리하는 컴퓨팅 기술
- therChannel, Multi-Segment, VLAN 등과 같은 다양한 네트워크 환경에서도 안정적으로 고성능을 제공합니다.

다양한 웹 환경 지원 (이식성)

- 인라인(Inline)모드, 프록시 (Reverse Proxy)모드, T.프록시 (Transparent Proxy)모드, 이중화(HA) 구성 등 다양한 네트워크 환경을 지원합니다.
- 소/중/대규모 웹 서비스 환경을 위한 다양한 제품 라인업을 제공합니다.
- 국내 최초로 Virtual Appliance 형태의 클라우드 웹방화벽(Virtual WAF)를 제공합니다.
  - 다양한 하이퍼바이저(가상화 환경)를 지원하며, 클라우드 웹방화벽 중 국내 최초로 국제 CC 인증 획득 (2014년 7월)

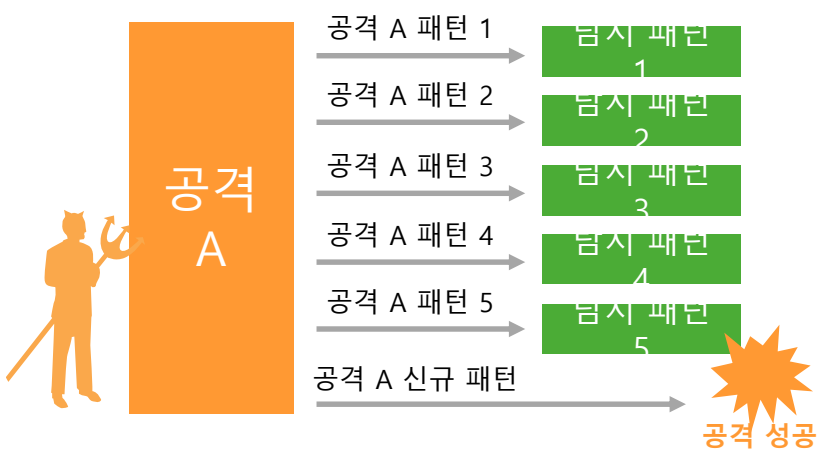
4. 제품특장점 - 오탐 없는 높은 보안성 보장

논리 분석형 탐지엔진 (COCEP) 탑재를 통한 로직 기반 공격 분석

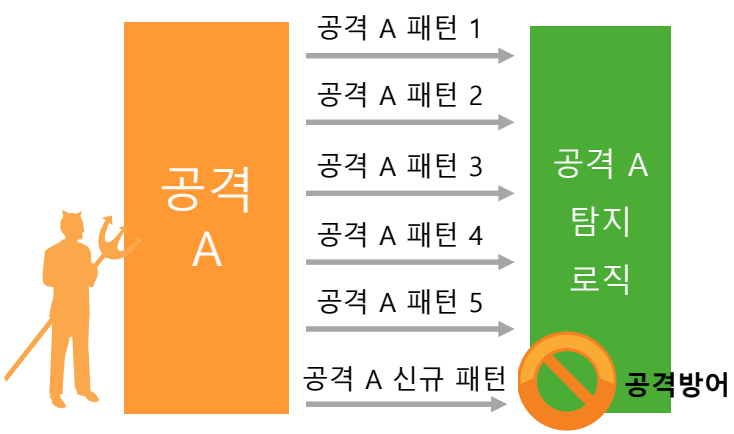
- 자체 개발한 논리연산 탐지 엔진인 COCEP (Contents Classification and Evaluation Processing)엔진을 탑재하여 개별 시그니처 비교를 통한 탐지뿐만 아니라, 공격 자체의 특성을 파악하여 공격 탐지 로직 기반으로 방어할 수 있습니다.
- 공격으로 정의되어 있는 형태부터 실제 공격인지까지 분석하여 공격 여부를 판단하여 오탐이 거의 없습니다.

기존 1,2세대 웹방화벽 탐지 엔진 vs WAPPLES의 COCEP 엔진

- 공격A의 신규 패턴에 대해
  => 1,2세대 웹방화벽 탐지 엔진에서는 공격으로 탐지되지 않고 공격 시도가 성공합니다.
  => WAPPLES의 COCEP 엔진에서는 동일한 공격 A로 인식되어 탐지 및 차단이 이루어 집니다!!



< 1, 2 세대 웹방화벽 탐지엔진 >

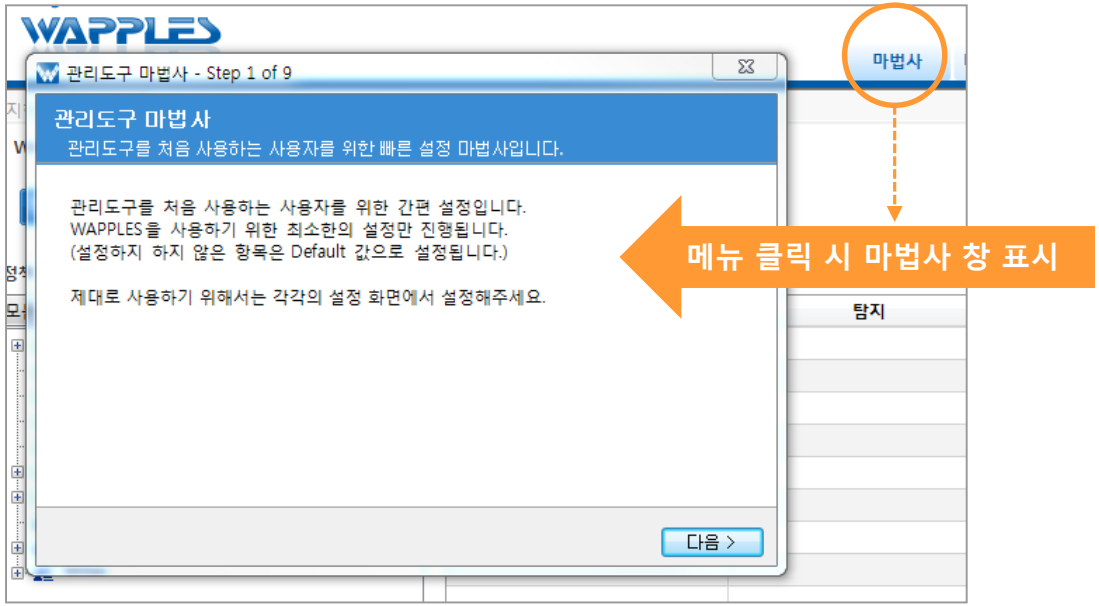


< WAPPLES COCEP 엔진 >

4. 제품특장점 - 쉽고 편리한 보안 관리 (GUI 기반 관리콘솔 지원)

WAPPLES 관리도구를 처음 사용하는 사용자를 위한 간편 설정 기능

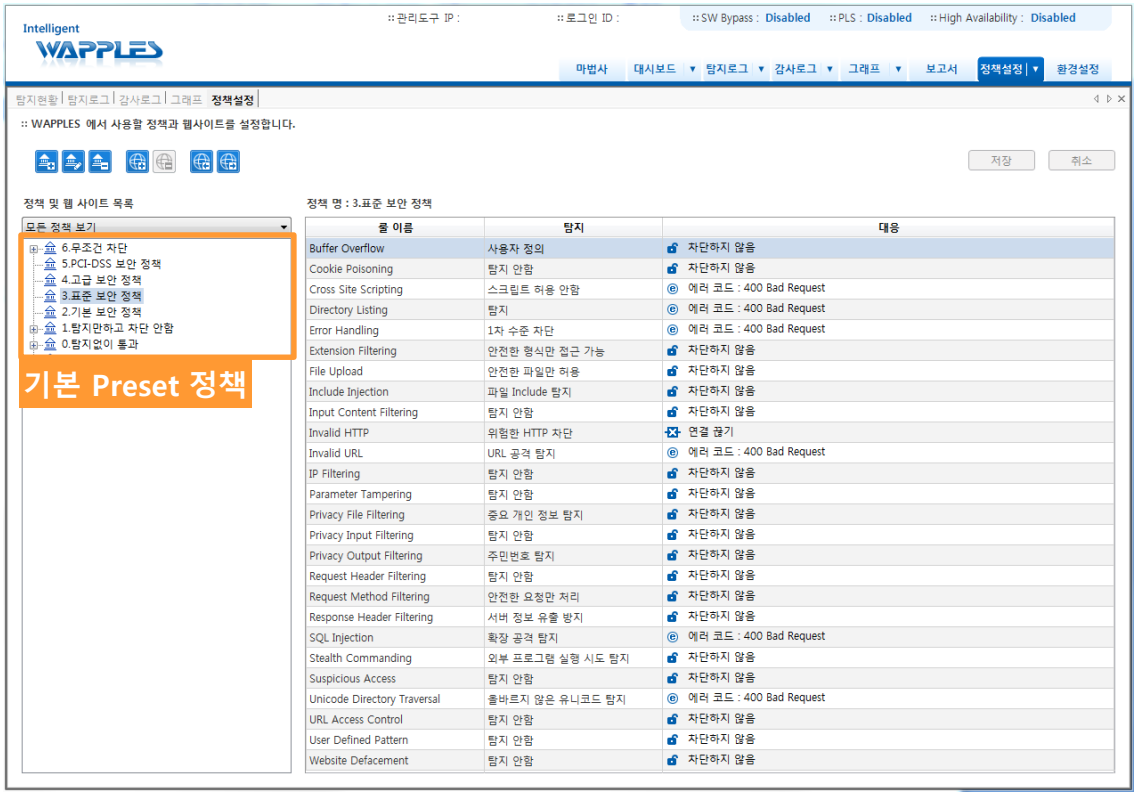
- 9가지 Step으로 구성된 마법사 형식의 설정 기능을 이용하여
  WAPPLES을 처음 사용하는 사용자도 간편하게 WAPPLES을 사용하기 위한 설정이 가능합니다.
  - 라이선스 설정, 웹서버 추가, 웹서버 운영모드 설정, 웹사이트 설정 등
- WAPPLES 사용을 위한 최소한의 설정만 진행되며 설정하지 않은 항목은 Default 값으로 설정됩니다.



4. 제품특장점 - 쉽고 편리한 보안 관리 (GUI 기반 관리콘솔 지원)

기본 Preset 정책 바탕으로 자유로운 설정 지원

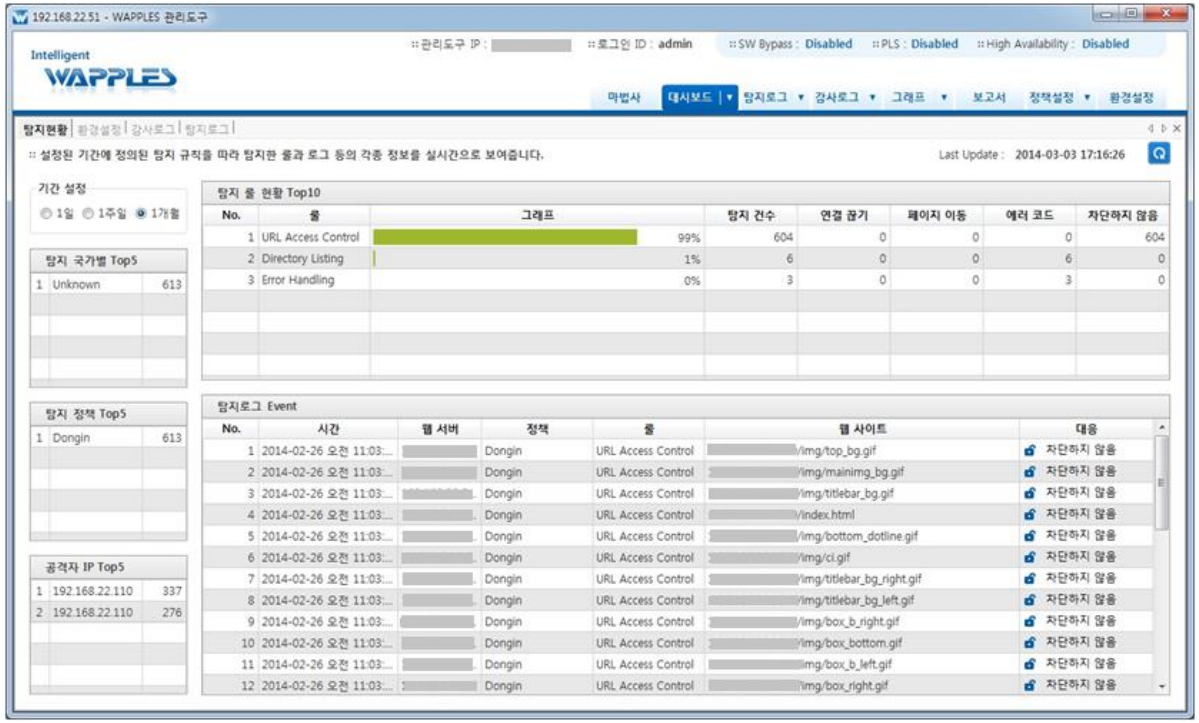
- 기본으로 제공되는 7 가지 Preset 정책을 바탕으로 고객 환경에 최적화 되도록 자유롭게 설정할 수 있습니다.
- 정책 편집은 물론, 정책 내보내기, 불러오기 기능도 제공됩니다.



4. 제품특장점 - 쉽고 편리한 보안 관리 (GUI 기반 관리콘솔 지원)

고도화된 대시보드 기능 제공

- 탐지현황/ 시스템현황/ 서비스 현황에 대해 한 눈에 파악이 가능한 고도화된 대시보드 기능을 제공합니다.
  - 탐지현황: 탐지 룰 현황 Top10/ 탐지로그 Event/ 탐지국가별 Top5/ 탐지정책 Top5/ 공격자IP Top 5
  - 시스템 현황: CPU 사용 현황/ RAM 사용 현황/ 네트워크 인터페이스 현황/ 시스템 현황/ 기타 현황 (PLS 연동 및 HA 등)
  - 서비스 현황: 웹사이트 서비스 현황 (정책 이름, 웹사이트, 트래픽, 페이지히트, 응답코드)/ Throughput 현황/ CPS 현황/ TPS 현황

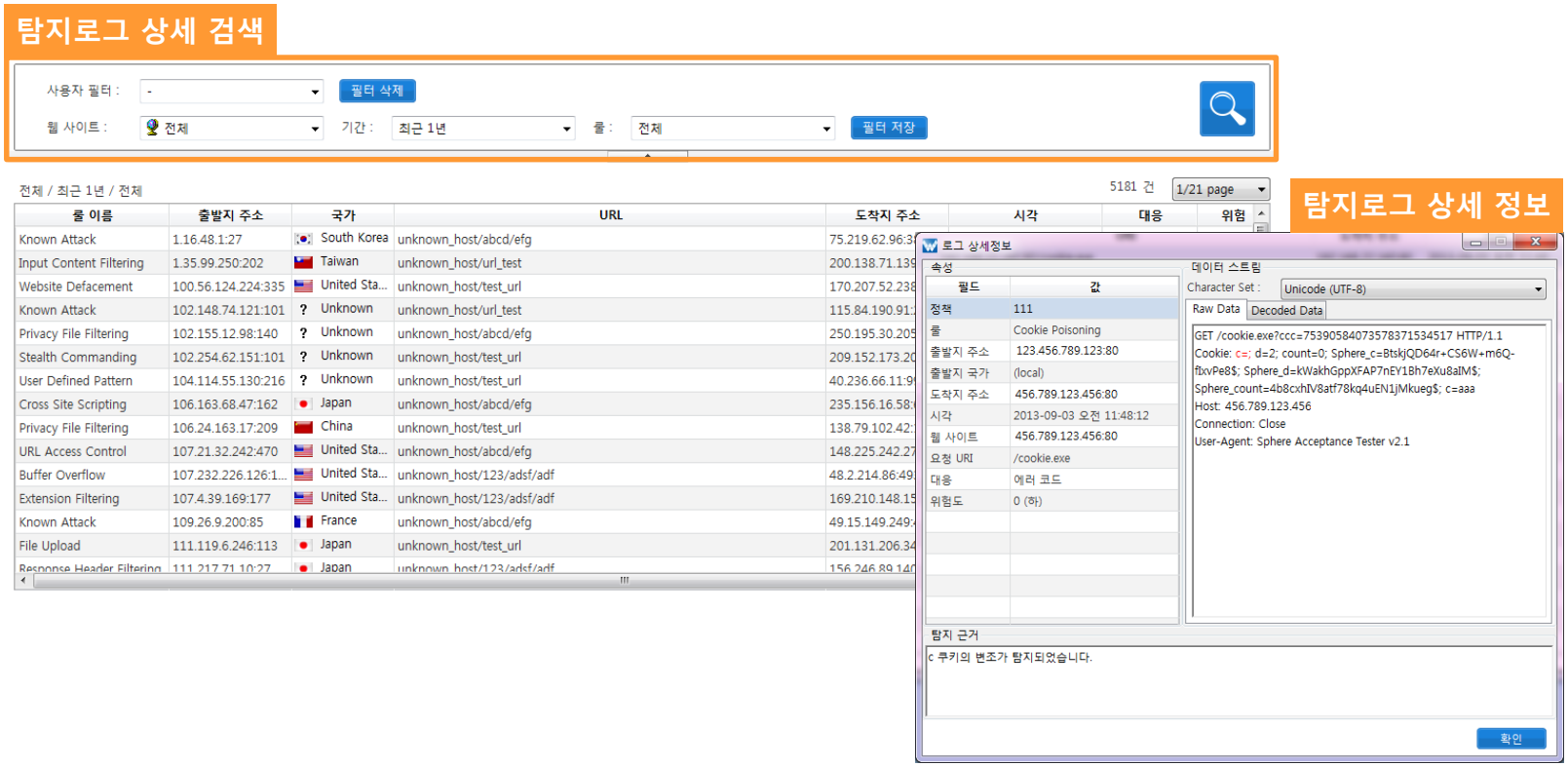


< 대시보드 --> 탐지 현황 이미지 >

4. 제품특장점 - 쉽고 편리한 보안 관리 (GUI 기반 관리콘솔 지원)

탐지 로그의 상세 내용 확인 기능 및 상세 검색 기능 제공을 통해 공격자 분석이 가능하도록 지원

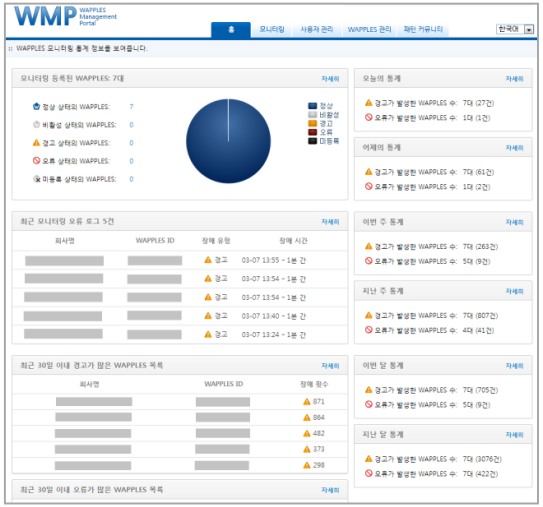
- 웹사이트 별/ 기간 별/ 룰 별/ 사용자 정의 필터 기준으로 탐지 로그 상세 검색이 가능합니다.
- 상세 로그 화면에서 실제 공격이 어떻게 이루어 졌는지에 대해서 확인이 가능합니다. (Raw data 및 탐지 근거 등 제공)



4. 제품특장점 – 웹 기반의 WAPPLES Management Portal (WMP) 서비스 제공

웹 GUI 기반으로 제공되는 쉽고 간단한 WAPPLES 모니터링 및 관리 서비스 (wm.pentasecurity.com)

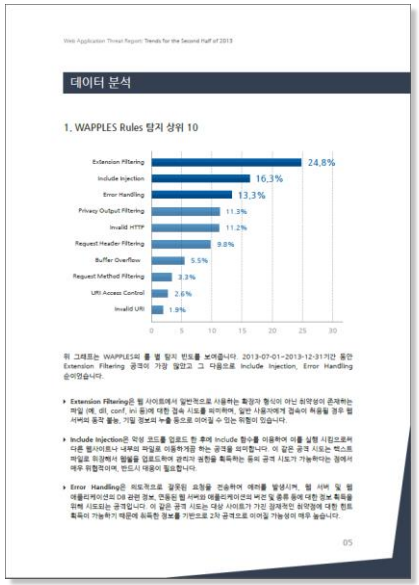
- 고객이 자신의 위치와 상관없이 실시간으로 WAPPLES 상태 파악 가능
- WMP를 이용함으로써 고객 WAPPLES 실시간 모니터링을 통한 신속한 대응이 가능
- WAPPLES의 정상 서비스 여부 체크 및 WAPPLES 장애 발생에 따른 SMS/ 메일 알람 기능 제공
  - 다수의 고객을 보유하고 있을 경우 한 화면에서 WAPPLES 서비스 상태 확인 가능
- WAPPLES의 시스템 현황 모니터링, 주기 별 탐지로그 건 수 체크, 장애 발생 빈도 체크 등
- 커뮤니티를 통한 유효한 User Defined Pattern 파일 및 Blacklist IP 리스트 공유
  - 전세계 WAPPLES에서 수집된 정보를 바탕으로 작성된 패턴 및 Blacklist IP 정보를 본인의 WAPPLES에서 이용가능

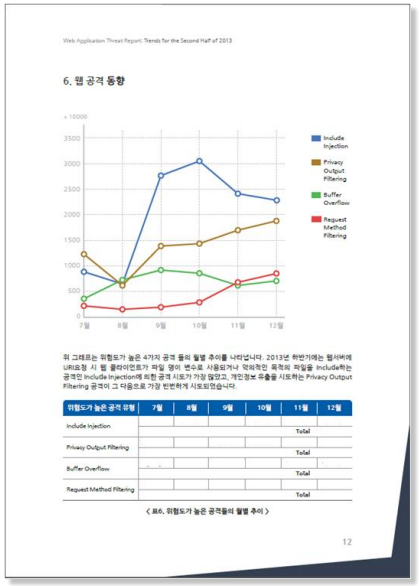


4. 제품특장점 - ICS (Intelligent Customer Support) 서비스 제공

WAPPLES 고객에게 제공되는 Web Application Threat Report

- 중앙센터에서 탐지 통계 취합하여 해킹유형 및 공격자 IP 등 전반적인 웹 공격 동향을 분석
- 경쟁제품과 차별화된 서비스 제공
  - 평판(Reputation) 기반 Black List IP 제공 가능
  - 전국적인 보안 이상 동향 파악 및 중앙 관리를 통한 신속한 대응 가능





4. 제품특장점 – 간단한 구축 절차

간단한 3 Step 프로세스 : 고객 환경 분석 ⇒ 설치 및 설정 ⇒ 정책 보완

- 다양한 고객 환경에 맞춰 최적화된 정책 설정이 중요하기 때문에,
  WAPPLES 설치 후 모니터링 기간을 통해 탐지로그 분석 후 정책 최적화를 통해 최종적으로 구축을 완료하게 됩니다.

사전 조사	설치 및 설정	정책 보완
사전 설치 조사서 전달 및 검토	WAPPLES 설치 WAPPLES 설정 운영 테스트 및 시연	탐지 로그 분석 분석 보고서 작성 보완 정책 수립

5. 제품라인업 (1/2)

Class	Value		
Model	**WAPPLES-50**	**WAPPLES-100**	**WAPPLES-500**
Appearance			
Capacity			
Maximum Throughput	100 Mbps	300 Mbps	500 Mbps
HTTP Transaction/sec	10,000	20,000	30,000
HTTP Connection/sec	9,000	18,000	25,000
Hardware			
Type	1 U	1 U	1 U
Memory	4 Gb	4 Gb	8 Gb
HDD	160 Gb	500 Gb	500 Gb
NIC	2 x 1G Copper port 4 x 1G Copper bypass port	2 x 1G Copper port 4 x 1G Copper bypass port **Optional** 4 x 1G Copper bypass port	2 x 1G Copper port 8 x 1G Copper bypass port or 2 x 1G Copper port 4 x 1G Copper bypass port 2 x 1G Fiber bypass port
Power Supply	AC100~240V 50/60Hz 250W	AC100~240V 50/60Hz 250W	AC100~240V 50/60Hz 250W

5. 제품라인업 (2/2)

Class	Performance		High End	
Model	**WAPPLES-1200**	**WAPPLES-2200**	**WAPPLES-5200**	**WAPPLES-10000**
Appearance				
Capacity				
Maximum Throughput	2 Gbps	4 Gbps	10 Gbps	14 Gbps
HTTP Transaction/sec	50,000	70,000	140,000	180,000
HTTP Connection/sec	35,000	45,000	90,000	130,000
Hardware				
Type	2 U	2 U	2 U	2 U
Memory	8 Gb	16 Gb	24 Gb	32 Gb
HDD	1 Tb	1 Tb	1 Tb	1 Tb
SSD	128 GB	128 GB	128 GB	128 GB
NIC	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port **Optional** 4 x 1G Copper bypass port 8 x 1G Copper port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port or 2 x 1G Copper port 2 x 10G Fiber bypass port **Optional** 4 x 1G Copper bypass port 8 x 1G Copper port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port 2 x 10G Fiber module port 2 x 10G Fiber bypass port	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port or 2 x 1G Copper port 2 x 10G Fiber bypass port **(Optional)** 4 x 1G Copper bypass port 8 x 1G Copper bypass port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port 2 x 10G Fiber module port 2 x 10G Fiber bypass port	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port or 2 x 1G Copper port 2 x 10G Fiber bypass port **(Optional)** 4 x 1G Copper bypass port 8 x 1G Copper bypass port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port 2 x 10G Fiber module port 2 x 10G Fiber bypass port
Power Supply	AC100~240V 50/60Hz 400W Redundant Power Supply	AC100~240V 50/60Hz 400W Redundant Power Supply	AC100~240V 50/60Hz 600W Redundant Power Supply	AC100~240V 50/60Hz 600W Redundant Power Supply

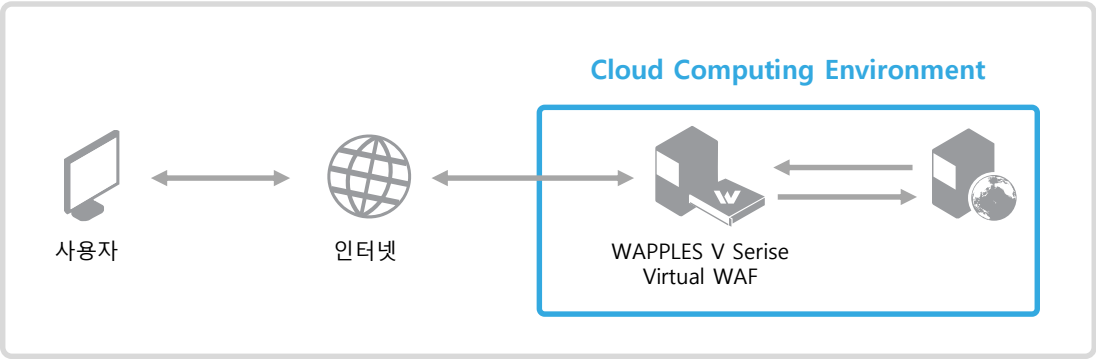
III. WAPPLES 제품군 소개

1. WAPPLES V-Series 소개
2. WAPPLES MS (Management System) 소개

1. WAPPLES V-Series 소개

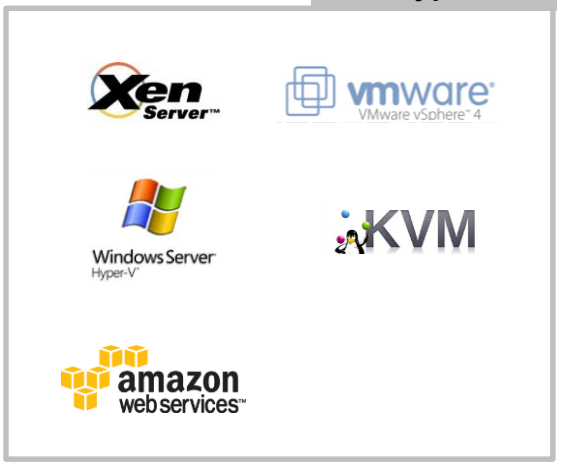
국내 최초 클라우드 웹방화벽(WAF)

- WAPPLES V-Series는, 클라우드 컴퓨팅 제공업자와 사용자를 위해 Virtual Appliance 형태로 제공되는 WAPPLES
- WAPPLES V-Series의 기본적인 기능은 H/W Appliance 형태로 제공하는 WAPPLES과 동일
- Citrix XenServer 과 VMWare vSphere, Redhat의 KVM, Hyper-V, Amazon의 AMI 를 지원
- WAPPLES V-Series는 반드시 프록시 (Reverse proxy) 로 구성
  (*인라인(Inline)구성의 경우는 고객의 Hypervisor 환경에 따라 가능 여부 판단)
- 가상 어플라이언스를 클라우드 환경에서 동작 가능하게 하려면, 가상의 네트워크 인터페이스 카드 한 쌍이 필요



<클라우드 환경에 최적화된 웹방화벽>

지원 Hypervisor

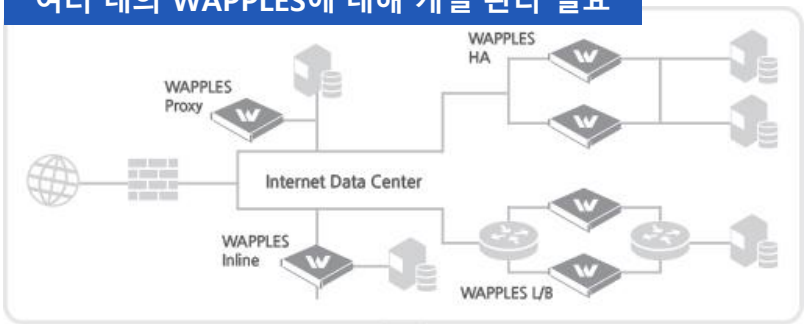


2. WAPPLES MS (Management System) 소개

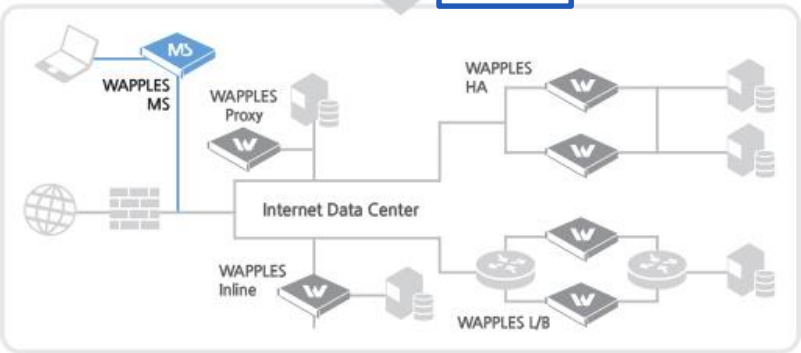
여러 대의 WAPPLES을 간편하게 관리하는 통합 관리 전용 시스템

- WAPPLES-MS는 다양한 네트워크대역에 걸쳐 설치되어 있는 여러 대의 WAPPLES (H/W Appliance & V-Series) 을 하나의 관리 콘솔을 이용하여 원격 제어 가능
- 관리 환경에 의해 동일한 관리 영역에 종속되거나, HA와 같은 특수한 설치 환경으로 인하여 동일한 관리 범주에 속한 WAPPLES을 그룹화하여 관리함으로써 보다 효율적인 업무 환경을 제공

여러 대의 WAPPLES에 대해 개별 관리 필요



Solution



- ✓ 쉽고 간편한 UI 제공
- ✓ WAPPLES-MS를 이용한 원격 제어와 편리한 통합 관리 기능, 실시간 동기화
- ✓ WAPPLES-MS를 이용한 WAPPLES 통합 로그 관리
- ✓ 대시보드 통합 관리
- ✓ 등록된 WAPPLES의 시스템 현황 실시간 감사

여러 대의 WAPPLES을 WAPPLES MS를 통해 통합 관리 가능

- ✓ One-click 설정으로 정책 일괄 동기화
- ✓ 웹 공격 동향과 WAPPLES에 의한 보호 현황에 대한 종합 보고서 기능 제공 (예정)
- ✓ 네트워크 설정/계정 관리 (Multi tenant) 등 설정 마법사를 통한 편리한 운영 및 관리
- ✓ 운영 데이터 저장 이중화 지원

IV. 참고 자료

1. 주요 레퍼런스
2. 인증 현황/ 수상 현황/ 특허 현황
3. PCI-DSS v3.1 준수 테스트
4. 도입 사례:증권사/ 금융권/ 사설교육기관

SL2 CONFIDENTIAL Internal Only

1. 주요 레퍼런스

NLB National Library Board Singapore
ING LIFE INSURANCE
NISSAY ASSET MANAGEMENT
SHIBUYA 109 NET SHOP
SAMSUNG
BMW
MINISTRY OF FINANCE MALAYSIA
AEON MALL
TOT
NIKE SPORTSWEAR
LG
DEP Department of Export Promotion Ministry of Commerce Royal Thai Government
SoftBank
Marriott
MINISTRY OF HOME AFFAIRS
MetLife

2-(1). 인증 현황

- 2015. 12 ICSA labs WAF 인증
  PCI-DSS v3.1 준수 테스트 보증
- 2014. 07 WAPPLES V-Series 국제 CC 인증
- 2013. 06 WAPPLES v4.0 GS 인증
- 2013. 04 녹색기술 및 녹색기술제품 인증
- 2012. 11 국제 CC(Common Criteria) EAL4 인증
- 2011. 12 VMware Solution Provider 자격 획득
- 2010. 06 WAPPLES 국정원 CC 인증
- 2009. 12 PCI-DSS 준수 인증 획득
- 2008. 07 암호모듈(CIS-CC) 국가 정보원 검증 필
- 2007. 05 전자파 적합 등록 인증

< CC 인증 >

< ICSA labs WAF 인증 >

< GS 인증 >

< 녹색 기술 인증 >

2-(2). 수상 현황

- 2014. 06 프로스트 앤 설리반 선정 "올해의 웹방화벽" 수상
- 2013. 11 2013 대한민국 IT Innovation 대상 "미래창조과학부장관 표창" 수상
- 2013. 06 프로스트 앤 설리반 선정 "올해의 웹방화벽" 수상
- 2013. 02 제 12회 대한민국 SW 기업경쟁력 최우수상 수상
- 2012. 11 지식정보보안산업 유공자 '지식경제부장관 표창'
- 2012. 05 특허스타기업 선정
- 2010. 02 제9회 대한민국 SW 기업경쟁력 최우수상 수상
- 2009. 11 2009신기술 실용화 국무총리 표창 수상
- 2009. 04 지식경제부 신소프트웨어 상품 대상 수상
- 2008. 11 한국지능정보시스템학회 인텔리전스 대상 수상

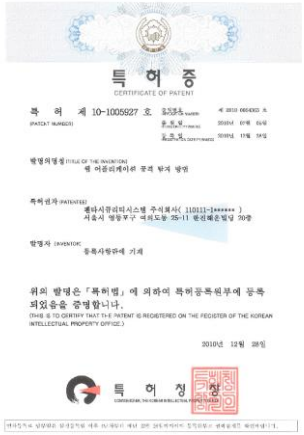
< 대한민국 SW 기업경쟁격 최우수상 >

< 인텔리전스 대상 >

< 국무총리 표창 수상 >

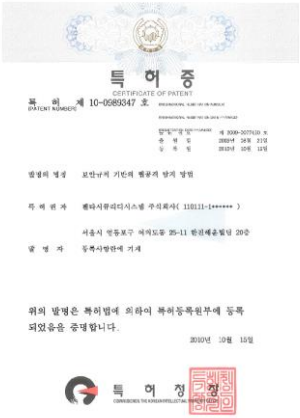
2-(3). 특허 현황

- 보안 규칙 기반의 웹공격 탐지방법 (METHOD FOR DETECTING A WEB ATTACK BASED ON A SECURITY RULE)
- 웹 어플리케이션 공격 탐지 방법 (METHOD FOR DETECTING A WEB APPLICATION ATTACK)
- 웹방화벽과 웹소스 취약점 분석툴의 연동 방법 및 그를 이용한 보안 시스템
- 이벤트 분석에 기반한 사이버 공격 탐지 장치 및 방법


특 허 증
CERTIFICATE OF PATENT
특 허 청

특 허 증
CERTIFICATE OF PATENT
특허청장 김 영

특 허 증
CERTIFICATE OF PATENT
특 허 청


특 허 증
CERTIFICATE OF PATENT
특 허 청

2-(4) PCI-DSS v3.1 준수 테스트 보증 (1/3)

번호	요건	준수 여부
2.2.2	시스템 기능에 필요한 서비스, 프로토콜, 데몬 등만을 활성화 합니다.	Y
2.3	강력한 암호화를 사용하여 콘솔 외의 관리적인 접근을 암호화 합니다.. 웹 기반 관리 및 기타 콘솔 외의 관리적인 접근을 위하여 SSH, VPN 혹은 TLS 등의 기술을 사용합니다.	Y
3.3	PAN이 표시되는 경우 마스킹하고 (처음 6자리와 마지막 4자리가 최대 표시 자릿수), 업무상 타당한 요구가 있는 직원만 전체 PAN을 볼 수 있도록 합니다.	Y
3.4.1	디스크 암호화(파일 또는 컬럼 수준의 데이터베이스 암호화가 아닌)를 사용하는 경우, 논리적 액세스는 기본 운영 체제(OS)의 인증 및 액세스 제어 매커니즘과는 별도로 관리할 필요가 있습니다. (예를 들어 로컬 사용자 계정 데이터베이스 또는 전반적인 네트워크 로그인 자격 증명을 사용하지 않는 등의 방법). 복호화 키는 반드시 사용자 계정과 연결되어 있지 않아야 합니다.	Y
6.5.1	Injection 결합(flaws), 특히 SQL Injection. 또한 LDAP과 Xpath Injection 결함(flaws)뿐만 아니라 다른 Injection 결함(flaws)들도 고려해야 합니다.	Y
6.5.2	Buffer overflow	Y
6.5.3	안전하지 않은 암호화 저장	Y
6.5.4	안전하지 않은 통신	Y
6.5.5	부적절한 error handling	Y
6.5.7	Cross-site scripting (XSS)	Y
6.5.8	부적절한 접근 제어 (안전하지 않은 직접 객체 참조, URL 접근 제한 실패, 디렉토리 탐색 (traversal), 기능에 대한 사용자 접근 제한 실패 등)	Y

2-(4) PCI-DSS v3.1 준수 테스트 보증 (2/3)

번호	요건	준수 여부
6.5.9	Cross-site 요청 변조	Y
6.5.10	취약한 인증과 세션 관리	Y
6.6	공개된 웹 어플리케이션에 대해 지속적으로 새로운 위협 및 취약성이 대응하고, 다음 내용과 같은 방법에 의해 알려진 공격으로부터 이러한 어플리케이션이 보호되도록 합니다.. : • 최소한 1년에 한 번 그리고 모든 변경 후 수동 또는 자동화된 어플리케이션 취약성 보안 평가 도구나 방법을 통해 공개된 웹 어플리케이션을 검토합니다. • 지속적으로 모든 트래픽 확인을 위해 공개된 웹 어플리케이션 앞에 웹 기반의 공격을 탐지 및 방어하는(예를 들어, 웹 어플리케이션 방화벽) 자동화된 기술적 솔루션을 설치합니다.	Y
10.2	다음 사건을 재구성하기 위해 모든 시스템 구성 요소에 대한 자동 감사 추적 기능을 실행합니다 :	
10.2.1	카드 소유자 데이터의 모든 사용자 접근	Y
10.2.2	루트 또는 관리자 권한으로 개인에 의해 취해진 행동	Y
10.2.3	모든 감사 추적에 대한 접근	Y
10.2.4	유효하지 않은 접근 시도	Y
10.2.5	식별 및 인증 메커니즘의 사용 및 변경 (새로운 계정 생성, 권한 상승을 포함하지만 이에 한정하지 않음) 및 루트 또는 관리자 권한이 있는 계정의 모든 변경, 추가, 삭제	Y
10.2.6	감사 로그 초기화, 중지, 일시 중지	Y

2-(4) PCI-DSS v3.1 준수 테스트 보증 (3/3)

번호	요건	준수 여부
10.2.7	시스템 레벨의 객체 생성 및 삭제	Y
10.3	최소한 모든 시스템 구성 요소에 대해 다음과 같은 감사 추적 기입 사항을 기록 :	
10.3.1	사용자 식별	Y
10.3.2	이벤트 유형	Y
10.3.3	날짜 및 시간	Y
10.3.4	성공 혹은 실패 표시	Y
10.3.5	이벤트의 발생원	Y
10.3.6	영향을 받는 데이터, 시스템 구성 요소 또는 리소스의 ID 혹은 이름	Y
10.5.2	승인되지 않은 수정으로부터 감사 추적 파일을 보호합니다.	Y

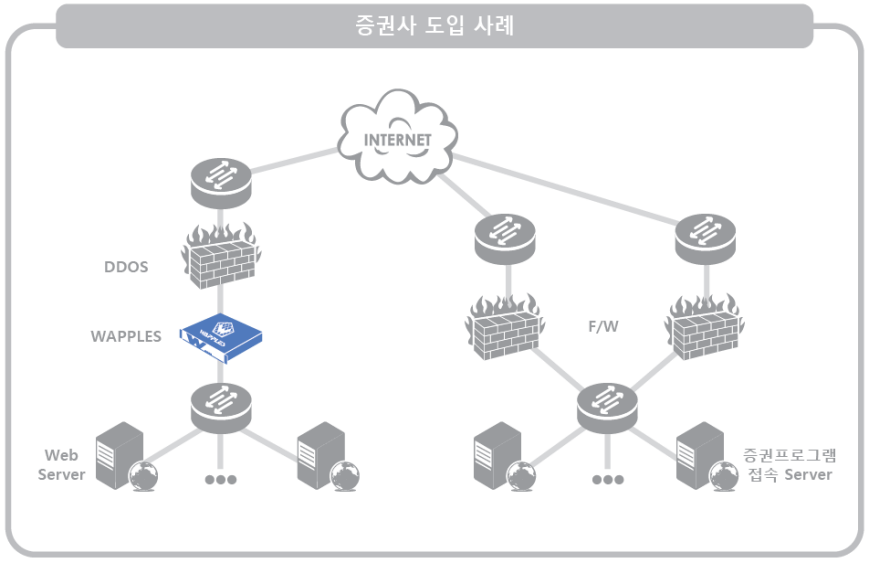
3. 도입 사례 - 증권 회사

도입 목적

- 신규 장비 교체 프로젝트 때, 신규 보안 장비로서 도입 – 웹방화벽(WAF), DDoS 장비
- 지속적인 웹 보안점검을 받았으며,
  보안 강화를 위해 웹방화벽(WAF) 도입

적용 내역

- 웹방화벽(WAF)을 DDoS 장비와
  DMZ Zone사이에 인라인(Inline) 방식으로 설치
- 3개 네트워크에 동일하게 구성
- 로그 분석을 통해 주민번호 노출 확인
- 설치 후 Mass SQL Injection 공격이 탐지
- Mass SQL Injection 공격 등을
  웹방화벽(WAF)을 통해 차단



도입 효과

- 지속적으로 취약성 점검을 받아 왔으나, 웹방화벽(WAF) 도입을 통해서 새로운 취약점 및 공격을 사전에 차단
- 네트워크 방화벽 없이 웹방화벽(WAF) 만으로 웹 서버 보호
- 상시 모니터링을 통한 공격 시도 탐지
- 공격 차단을 통해 웹 서버의 가용성 확보

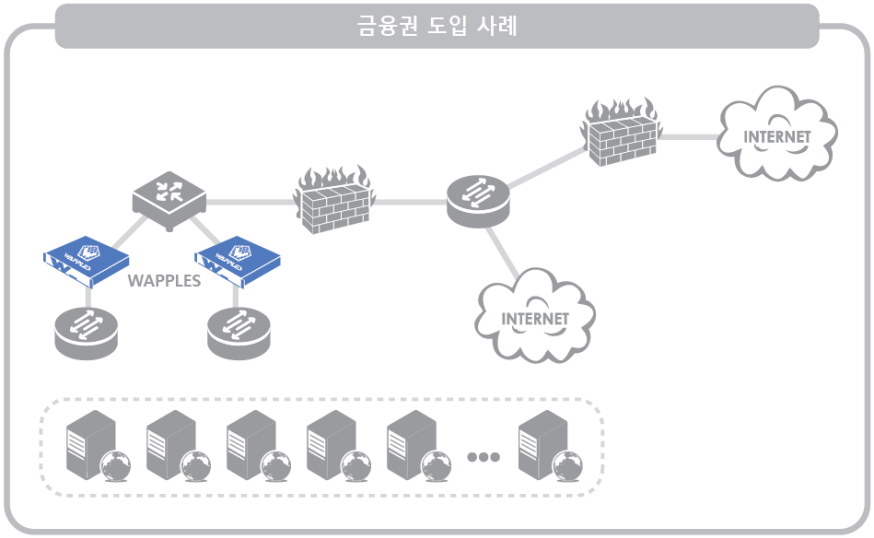
3. 도입 사례 - 금융권

도입 목적

- 외부에 노출된 그룹웨어 및 내부 중요 서버에 대한 보안 필요
- 개인정보 유출 및 지속적인 자동화된 공격 보호 필요

적용 내역

- 이중화된 네트워크 지원을 위해
  복수의 웹방화벽(WAF) 도입
- Active/Standby 구성 및 인라인 방식 구축
- 업무 처리시 발생되는 웹 애플리케이션 오류 확인
- 개인정보 유출 경로 파악 조치
- 자동화된 공격 발생시,
  자동으로 블랙리스트 IP관리 기능 활용
- URL 접근제어 기능 반영



도입 효과

- 개인정보 유출 / 웹 애플리케이션 오류 URL보호를 통한 신뢰성 제공
- 자동화된 공격 차단으로 가용성 증가
- 내부 보안 감사 시 소스코드 수정 등에 비해 TCO 절감
- 내부 중요서버 애플리케이션에 대해, 인가된 운영자만 접근 가능하여 내부정보 유출 방지

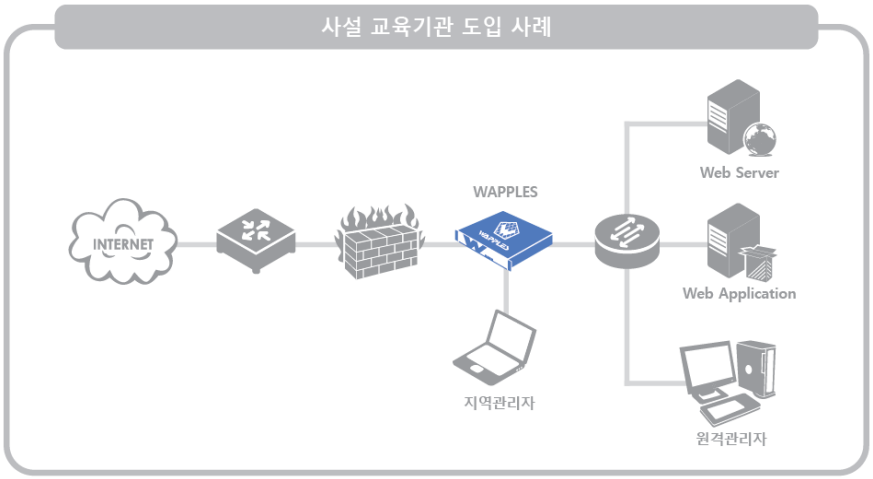
3. 도입 사례 - 사설교육기관

도입 목적

- 온라인 교육 사이트를 운영하는 웹 서버가 홈페이지 해킹 후 악성코드가 대량으로 배포되어 과도한 부하 발생
- 컨텐츠를 노린 웹 공격이 중국으로부터 수시로 발생하여 정상적인 서비스 제공에 어려움을 겪음

적용 내역

- 웹방화벽(WAF)을 웹 서버 앞에 인라인 방식으로 설치
- 로그 분석을 통해 다양한 백도어 발견
- 로그 분석 후 해당 백도어 제거
- 공격자가 설치한 다양한 악성 코드 설치 확인 및 제거
- 중국으로부터의 SQL Injection 공격 등을 웹방화벽(WAF)을 통해 차단
- 웹방화벽(WAF) 운영을 통해 컨텐츠 복사 시도 차단



도입 효과

- 악성코드의 대량 유포로 인한 웹 서버 부하 증가로 서비스 장애가 발생되었으나 웹방화벽(WAF) 운영 후 부하 증가 현상이 소멸됨
- 악성코드 차단 및 삭제를 통해 서비스를 위한 네트워크 대역폭 확보
- 온라인 교육 사이트의 주요 자산인 컨텐츠 복사 근절

감사합니다.

Bell I&S
Bell Information&Solutions

Tel) 02-6925-1131 / Fax) 02-2664-1575

[본사]서울시 서대문구 충정로 8
(종근당빌딩 8층)
E-Mail : shlee@bellins.net