지능형 WAAP

WAPPLES

Penta SECURITY

WHY WAPPLES ?

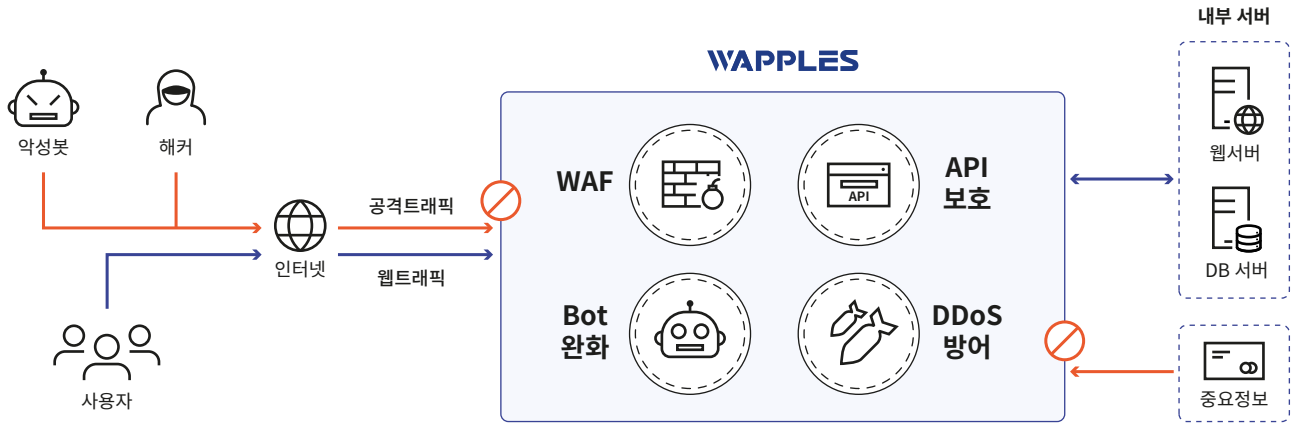
성능	• **세계 최고 수준의 성능을 발휘하는 웹방화벽 WAPPLES** - 650,000 TPS (이전 모델 대비 144% 성능, 12000모델 기준)
보안성	• **세계 최저 오탐률, [1]COCEP™ 엔진 v3** - 오탐률 4% 미만의 지능형 논리연산 탐지 엔진
자가점검	• **머신러닝 기반의 자가점검 제공** - 관리자의 부담을 최소화하고 보안성을 향상
고객 소통	• **24/365 온라인 고객 소통 시스템 [2]IMS, [3]IDS 운영** - 고객과 제조사 간의 정확한 정보 전달과 완벽한 기술지원 보장
빅데이터	• **세계 70만개 사이트 기반 빅데이터 보유** - 세계 70만개 이상의 웹사이트로부터의 데이터를 분석, 고객의 효과적인 보안 정책 수립을 지원하는 [4]ICS 운영
클라우드	• **Cloud-Ready and Cloud-Native** - 모든 클라우드 환경에서 완벽하게 동작, 국내외 7,000여 고객 대상 SaaS 운영
글로벌서비스	• **세계 56개국 서비스, 국제적으로 높은 평가**
API 보호	• **국내 최초 지능형 탐지 엔진 기반의 API Schema Validation** - 37개의 고도화된 탐지 룰을 기반으로 API 형식 및 공격 유형을 다각도로 검증
Bot 완화	• **고도화된 악성 봇 탐지 및 악성 트래픽 차단** - 20년 업력의 웹 공격 기술 노하우를 바탕으로 한 WAPPLES 만의 이상 탐지 기술지원

1) **COCEP™** : 논리연산탐지엔진 Contents Classification and Evaluation Processing
2) **IMS** : 고객 대응관리 시스템 Incident Management System
3) **IDS** : 정보 전달 시스템 Information Delivery System
4) **ICS** : WAPPLES 정보 수집 및 분석시스템 Intelligent Customer Support

202302

WAPPLES

WAPPLES은 웹 애플리케이션 보호 뿐만 아니라 API 보호, Bot 완화, DDoS 방어에 특화된 **지능형 WAAP 솔루션**입니다.
특허 받은 지능형 탐지 엔진 COCEP™을 바탕으로 웹공격에 대응하며, API 형식 위변조, Bot 부정행위, L7 기반의 DDoS를 방어하는 다기능 웹보안 솔루션입니다.

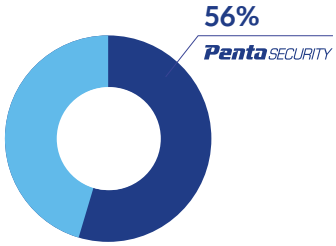


WAAP이란?

WAAP(Web Application and API Protection)은 기존의 웹 공격을 막아주는 역할을 하던 웹방화벽 기능 뿐만 아니라 API 보호, Bot 완화, DDoS 방어 등 웹 환경에서 추가로 발생할 수 있는 고도화된 공격을 막을 수 있는 기능을 가진 웹 보안 솔루션입니다.

국내 최고의 탐지 성능, COCEP 엔진v3

WAPPLES는 자체 개발한 지능형 탐지 엔진인 **COCEP 엔진 v3**을 통해 웹상에서의 복잡한 공격 패턴을 논리적으로 분석하고 탐지하여 일정한 보안성을 유지합니다.
COCEP 엔진 v3은 단순 패턴 분석을 통한 탐지 뿐만 논리분석을 바탕으로 실제 공격 여부를 탐지하고 공격을 예방합니다.



15년 연속 국내 시장점유율 1위
2008-2022년 나라장터 기준 웹방화벽 평균 점유율

지능형 탐지 엔진 관련 특허 현황

- 보안규칙 기반의 웹 공격 탐지방법
- 웹 애플리케이션 공격 탐지 방법
- 웹방화벽과 웹 소스 취약점 분석툴의 연동방법 및 그를 이용한 보안시스템
- 이벤트 분석에 기반한 사이버 공격 탐지 장치 및 방법

WAPPLES 주요 기능

WAF

- 논리분석엔진 COCEP™ 탑재로 오탐 없는 웹 공격 탐지
- OWASP Web Security TOP 10 취약점 유형 대응
- 신유형 공격에 빠른 대응을 위한 Custom Rule 기능 제공
- 신규 취약점 보안 패치 제공
  (TOR IP, GEO IP, Threat Protection Profile 등)

Bot 완화

- 악성 봇 트래픽 검사
- mTLS 모드 제공으로 보안성 강화
- CAPTCHA 지원
- Browser Fingerprinting
- 계정탈취(Account Take-over)공격 방지

API 보호

- OWASP API Security TOP 10 취약점 유형 대응
- API 형식 검사를 통한 고도화된 API 공격 방어
- JSON/XML 요청 필드 검사

DDoS 방어

- L7 DoS 탐지 및 트래픽 차단

관리

- 제품 운영 중 이상 발생 시 자동으로 서비스를 복구하거나 알림을 주는 자가점검 기능 제공
- GUI 기반 관리 콘솔을 이용하여 간편하게 보안 설정 가능
- 실시간 운영 현황 대시보드 기능 제공
- 탐지/감사 로그 관리, 백업/복구 기능 제공
- 웹 서비스에 필요한 인증 처리 및 2차 인증 제공
- 엔지니어의 체계적인 유지보수를 위한 정기점검 툴 제공

수상 및 인증

Gartner
Magic Quadrant
WAF 부문 4년 연속 등재

FROST & SULLIVAN
Frost&Sullivan
최고 보안기업 선정

Global Infosec Awards
웹 애플리케이션 최우수 혁신상

CyberSecurity Breakthrough Award
올해의 웹보안상

FORRESTER®
Forrester
Now Tech, WAF 등재

CC 인증

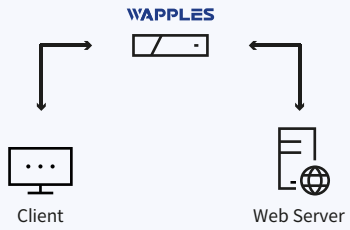
GS 인증

ISO 9001 인증

IPv6 Ready Logo

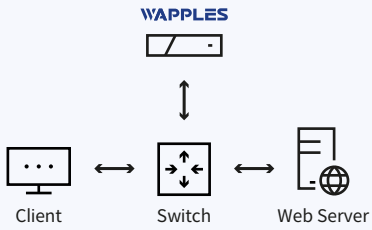
녹색인증

WAPPLES 구성도



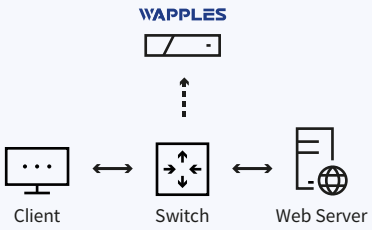
WAPPLES의 존재가 노출되지 않고, 웹 서버로 가는 모든 패킷을 WAPPLES에서 탐지 및 차단 할 수 있도록 하고 싶은 경우

인라인모드 Inline



외부 클라이언트로부터 전송되는 모든 패킷이 WAPPLES의 서비스 IP로 전송되도록 운영하고 싶은 경우

리버스프록시모드 Reverse Proxy



외부 클라이언트로부터 전송되는 모든 패킷을 변조하지 않고 모니터링 뿐만 아니라 차단까지 하고 싶은 경우

미러링모드 Mirroring

WAPPLES 사양

Class	Economy	Value	Performance
Model	**160**	**1600**	**2600**
Max Throughput	600Mbps	1Gbps	5Gbps
Form Factor	1 U	1 U	2 U
Size (mm)	432 x 292 x 44	438 x 292 x 44	438 x 500 x 88
Memory	8 GB	16 GB	32 GB
SSD	1 TB	1 TB	256 GB + 1 TB
Management port	2 x 1G Copper	2 x 1G Copper	2 x 1G Copper
NIC Bypass Service Port	4 x 1G Copper	4 x 1G Copper	4 x 1G Copper / 2 x 1G Fiber
Optional NIC	-	-	10G Fiber

Class	High-end		
Model	**4600**	**5600**	**12000**
Max Throughput	10Gbps	18Gbps	20Gbps
Form Factor	2 U	2 U	2 U
Size (mm)	438 x 550 x 88	465 x 594 x 89	465 x 594 x 89
Memory	48 GB	96 GB	192 GB
SSD	256 GB + 1 TB	256 GB + 1 TB	256 GB + 1 TB
Management port	2 x 1G Copper	2 x 1G Copper	2 x 1G Copper
NIC Bypass Service Port	4 x 1G Copper / 2 x 1G Fiber	4 x 1G Copper / 2 x 1G Fiber	4 x 1G Copper / 2 x 1G Fiber
Optional NIC	10G Fiber	10G Fiber	10G Fiber

Penta SECURITY

펜타시큐리티시스템(주)
서울시 영등포구 여의공원로 115 세우빌딩 9층, 07241

TEL. +82-2-780-7728 / TECH 365(기술지원). 1661-4020
E-MAIL. waf@pentasecurity.com
www.pentasecurity.co.kr

USA SAN JOSE
JAPAN TOKYO
SINGAPORE
CHINA SHANGHAI