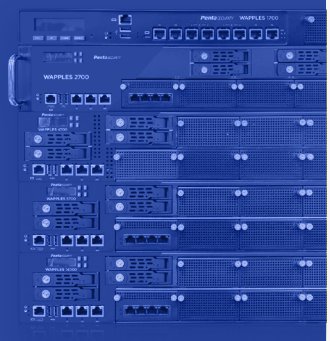
지능형 WAAP

# WAPPLES

Penta SECURITY

## WHY WAPPLES ?

대한민국 시장점유율 1위의
검증된 제품



**성능**

- **세계 최고 수준의 성능**
  - 특허받은 인메모리 컴퓨팅 기반의 멀티 프로세싱 기술로 고수준의 탐지 성능 보장
  - 웹 캐싱 기능을 통해 리소스 처리 효율 향상 및 응답속도 개선
  - SSE(Server-Sent Events)를 활용한 단방향 지속 연결로 실시간 데이터 처리 성능 최적화

**자가점검**

- **머신러닝 기반의 자가점검 기능 제공**
  - 위험상태 체크 및 실시간 알림 기능을 통한 관리자 부담 최소화

**고객 소통**

- **온라인 고객 소통 시스템 운영**
  - 업무시간 외 콜/원격지원 서비스 및 긴급 물류 지원 서비스 제공
  - 고객과의 정확한 정보전달 및 소통을 위한 [1]IMS, [2]IDS 운영

**클라우드**

- **Cloud-Ready and Cloud-Native**
  - 모든 클라우드 환경에서 완벽하게 동작, 국내외 9,000여 고객 대상 SaaS 운영

**신뢰성**

- **세계 70만 개 이상의 웹사이트 보호, 국제적으로 높은 평가**
  - 2년 연속 국가서비스 대상 사이버보안 솔루션 부문 수상(2024, 2025)
  - 3년 연속 Frost & Sullivan 선정 '올해의 웹방화벽' 수상(2023~2025)
  - Gartner WAAP Market Guide 언급(2023) 및 Forrester Now Tech(2022) 등재(국내유일)
  - Fortress Cyber Security Award 'Application Security' 부문 수상 (2020,2024)

**API 보안**

- **국내 최다 API 데이터 포맷 및 아키텍처 스타일 보호**
  - API 형식 검사를 통해 고도화된 공격을 방어하고 JSON/XML 요청필드 검사 및 mTLS모드 제공

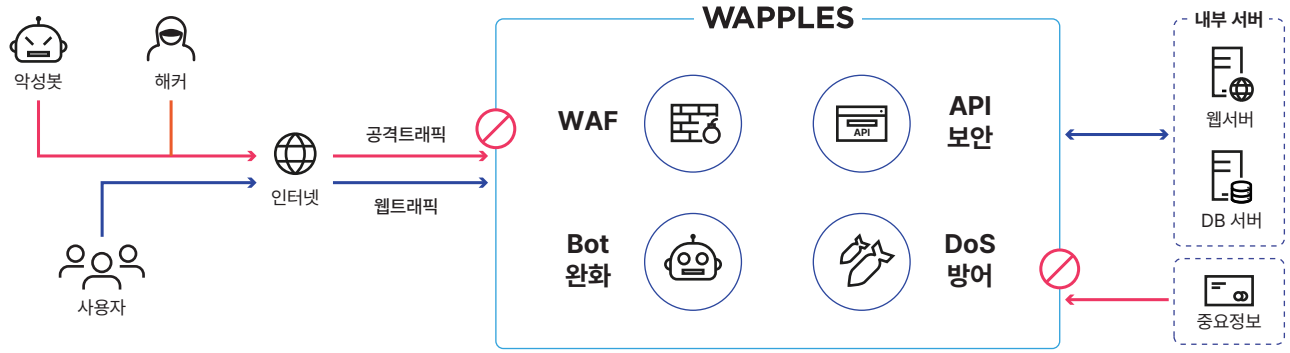
**Bot 완화**

- **고도화된 악성 Bot 탐지 및 악성 트래픽 차단**
  - Bot 트래픽 검사, CAPTCHA 및 Browser Fingerprinting 등의 기술을 통해 탐지 및 차단
  - 계정 탈취 공격 방지 및 IP 주소 위변조 감지 및 차단

1) **IMS** : 고객 대응관리 시스템 Incident Management System
2) **IDS** : 정보 전달 시스템 Information Delivery System

## WAPPLES

**WAPPLES**은 웹 애플리케이션 보호 뿐만 아니라 API 보안, Bot 완화, DoS 방어에 특화된 지능형 **WAAP 솔루션**입니다.
특허 받은 지능형 탐지 엔진 ※COCEP™을 바탕으로 웹 공격에 대응하며, API 형식 위변조, Bot 부정행위, L7 기반의 DoS를 방어하는 다기능 웹방화벽입니다.



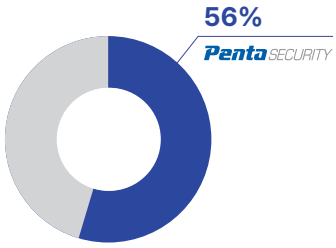

### WAAP란?

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

※ **COCEP™** : 논리연산탐지엔진 Contents Classification and Evaluation Processing

## 국내 최고의 탐지 성능, COCEP 엔진

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




**18년 연속 국내 시장점유율 1위**
2008-2024년 나라장터 기준 웹방화벽 누적 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 제로데이 웹 공격 방어
- 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
- CAPTCHA 지원
- Browser Fingerprinting
- 계정탈취(Account Take-over)공격 방지
- Malicious IP/ Bot 자동 업데이트 기능

### API 보안

- OWASP API Security TOP 10 취약점 유형 대응
- API 형식 검사를 통한 고도화된 API 공격 방어
- API 페이로드 실시간 보호
- JSON/XML/YAML/GraphQL 지원
- mTLS 모드 제공으로 보안성 강화

### DoS 방어

- L7 DoS 탐지 및 트래픽 차단

### 관리

- 제품에 이슈 발생 전 자동으로 서비스를 복구하거나 알림을 주는 자가점검 기능
- 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 부문 등재

2024 CYBERSECURITY
Globee Awards for Cybersecurity
Gold Winner

CC 인증

GS 인증

ISO 9001 인증

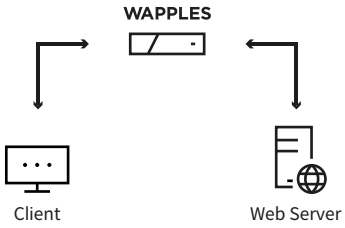
IPv6 Ready Logo

녹색인증
녹색인증

국정원 검증필
암호모듈

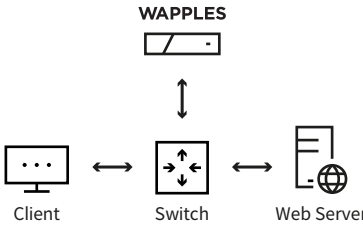
## WAPPLES 구성도

### 인라인모드 Inline



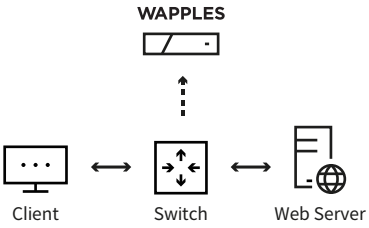

WAPPLES의 존재가 노출되지 않고, 웹 서버로 가는 모든 패킷을 WAPPLES에서 탐지 및 차단 할 수 있도록 하고 싶은 경우

### 리버스프록시모드 Reverse Proxy




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

### 미러링모드 Mirroring




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

## WAPPLES 사양

| Class | | Economy | | Value |
|---|---|---|---|---|
| Model | | W1700 T1 | W1700 T2 | W2700 |
| Max HTTP Throughput | | 6 Gbps | 6 Gbps | 10 Gbps |
| Form Factor | | 1 U | 1 U | 2 U |
| Memory | | 16 GB | 16 GB | 32 GB |
| Size (mm) | | 438 x 480 x 44 | 438 x 480 x 44 | 438 x 558 x 88 |
| SSD (OS+Log) | | 1 TB | 1 TB | 1 TB + 1 TB |
| Management Port | | 4 x 1G Copper | 4 x 1G Copper | 2 x 1G Copper |
| NIC Options | 1G Copper | ○ | ○ | ○ |
| | 1G Fiber | ○ | ○ | ○ |
| | 10G Fiber | – | – | ○ |
| | 40G Fiber | – | – | – |
| | 100G Fiber | – | – | – |
| Power | | Single | Redundant | Redundant |

| Class | | Performance | | High End |
|---|---|---|---|---|
| Model | | W4700 | W5700 | W14000 |
| Max HTTP Throughput | | 15 Gbps | 25 Gbps | 37 Gbps |
| Form Factor | | 2 U | 2 U | 2 U |
| Memory | | 64 GB | 64 GB | 128 GB |
| Size (mm) | | 438 x 600 x 88 | 438 x 600 x 88 | 438 x 600 x 88 |
| SSD (OS+Log) | | 1 TB + 1 TB | 1 TB + 1 TB | 1 TB + 1 TB |
| Management Port | | 2 x 1G Copper | 2 x 1G Copper | 2 x 1G Copper |
| NIC Options | 1G Copper | ○ | ○ | ○ |
| | 1G Fiber | ○ | ○ | ○ |
| | 10G Fiber | ○ | ○ | ○ |
| | 40G Fiber | ○ | ○ | ○ |
| | 100G Fiber | – | ○ | ○ |
| Power | | Redundant | Redundant | Redundant |


Penta SECURITY

**펜타시큐리티(주)**
서울특별시 영등포구 여의공원로 115 세우빌딩 8,9층, 07241

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

**JAPAN** TOKYO
**VIETNAM** HANOI
**UAE** ABU DHABI