AIWAF Application Insight Web Application Firewall

웹 서버로 유입되는 트래픽을 검사하여 다양한 웹 공격으로부터 서버를 안전하게 보호하는
웹 어플리케이션 방화벽 어플라이언스 입니다.

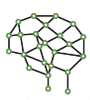
Why Do You Need a WAF?

공개 웹 서버에 대한 위협

- 웹은 서비스를 위해 항상 개방되므로 해커의 공격 위협에 노출
- 정보통신 기기 및 기술 등의 발달로 언제 어디서나 웹을 통한 주요 정보 접속 가능성 확대
- IDS, IPS 등 기존 네트워크 보안 솔루션의 한계에 따라 웹에 특화된 전문 솔루션 필요
- 웹 애플리케이션 해킹을 통한 DB 중요 정보 유출 가능성
- 보안 사고 발생 시 회사 평판에 대한 부정적 영향 초래

강화되는 IT 컴플라이언스

- 오늘날 기업의 IT 컴플라이언스는 생존과 경쟁을 위한 선택이 아닌 의무화
- 미 준수 시 경제적 손실, 인지도 하락 및 비즈니스 기회 상실 위험 발생
- 개인정보보호법
- HIPPA (Health Insurance Portability and Accountability Act)
- PCI-DSS (Payment Card Industry Data Security Standard) 등


Machine Learning


Threat Intelligence


Web socket and API


WEB DLP


Bot


HTTP/2

Key Benefits of AIWAF

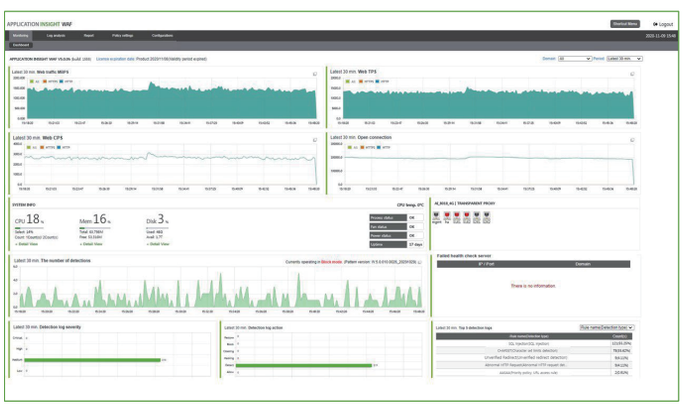
완전한 웹 서버 보안

- 요청 및 응답 데이터 구문 분석을 통한 포괄적인 웹 공격 탐지
  - SQL/LDAP Injection, XSS, CSRF, Web Shell, Overflow 등 요청기반 공격
  - Directory Listing, Error page 및 comment clocking 등 응답기반 공격
- Machine Learning & Threat Intelligence를 통한 Unknown 공격 대응
- 더블 & 멀티 인코딩 트래픽에 대한 디코딩 수행
- 주요 서버 정보 및 개인정보 유출 방지
- Script, Bot 등을 이용한 접속 트래픽 분석 및 탐지
- 웹 서버 응답페이지 분석을 통한 악성코드 검출 및 APT 대응
- 완전한 HTTP/2 연결 지원 및 HTTP/1.1과 동일한 보안 기능 제공

간편한 관리 및 운영

- 기존 네트워크에 영향 없는 Full Transparent Proxy 모드 제공
- HA(high availability) : active-standby, active-active
- 전체 또는 개별 웹 사이트 현황에 대한 통합 대시보드
- 도메인 별 차등적인 정책 설정 및 관리자 지정
- 탐지로그 내 요청/응답 데이터 로깅 및 탐지 근거 하이라이트 표기
- ESM, SNMP 등 모니터링 컨텐츠 커스터마이징
- HTTPS 인증서 관리 및 설정 자동화
- One-click 예외 처리, 오인탐지 정책 수립 자동 검증 등 다양한 운영 편의 기능
- 웹 서비스 품질 향상을 위한 웹 캐시 및 QoS
- 서버 Health check 및 Load Balancing
- 복호화 된 HTTPS 트래픽을 3rd party 솔루션으로 전송

AIWAF Administration GUI



01. 시스템 모니터링

〉실시간 시스템 상태 및 탐지, 트래픽 현황 모니터링
〉전체 또는 개별 웹 사이트 별 통합 대시보드 제공

02. 로그분석

〉다양한 검색조건을 통한 상세 로그 조회
〉탐지로그 내 요청/응답 본문 로깅 및 탐지 근거 하이라이트 표기

03. 정책설정

〉도메인별 독립된 차등 정책 설정
〉각 개별 정책 및 패턴 별 IP, URL 기준 적용 또는 예외 대상 설정

Key Features of AIWAF

1) 다양한 네트워크 구성모드
〉 In-line: Full Transparent Proxy

〉 Out-of-path: Reverse proxy, Mirroring

2) Passive Mirror
〉 3rd Party 보안 솔루션으로 복호화 된 HTTPS 트래픽 전송

3) Threat Intelligence 플랫폼
〉 AICC에 의한 실시간 위협 정보 업데이트

〉 proxy 경유, Black Client, C&C 트래픽 탐지

4) Machine Learning
〉 Machine Learning 기반 Unknown 공격 탐지

〉 공격 트래픽 판별 및 각 정책 별 탐지확률 제시

5) Adaptive Profiling
〉 Self-Learning 엔진에 의해 정상 요청 및 응답 데이터에 대한 프로파일 데이터베이스 구축

6) Full HTTP/2 지원
〉 완전한 HTTP/2 연결 및 구문 분석

〉 HTTP/1.1과 동일한 보안 기능 제공

7) ATP 대응
〉 악성코드에 의한 경유지・유포지 악용 탐지

〉 응답 데이터 본문 분석을 통한 악성코드 검출

8) 보안 최적화
〉 오인 탐지 발생 시 Rule별 예외 처리

〉 정책 별 차단 페이지 차등 설정

〉 각 개별 규칙 및 패턴에 대한 상세 제어

〉 수립 정책에 대한 정탐/오탐 여부 셀프 테스트

9) 트래픽 최적화
〉 웹 서비스 상태 및 품질 모니터링

〉 서비스 상태에 따른 Server Load Balancing

〉 각 도메인별 QoS(Bandwidth Limit) 설정

〉 URL Rewrite (요청/응답)

10) 웹 가속
〉 웹 캐싱 기능을 통한 트래픽 절감 및 서비스 응답 속도 향상

11) Bot 탐지
〉 Brute Force, Scraping, Denial of Inventory, Credential Stuffing 등에 사용되는 악성 Bot

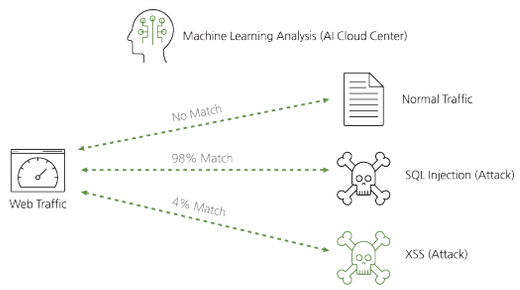
〉 Java Script Injection, Human Interaction 등 다양한 메커니즘을 통한 Bot 트래픽 식별 및 탐지

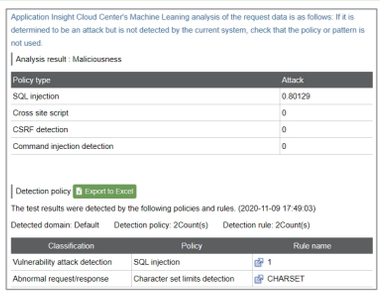
12) Multi-Layer 웹 공격 대응
〉 Signature, Threshold Limit, Profiling 등 다양한 탐지 알고리즘을 통해 Injection, XSS 등 OWASP TOP 10 공격군 부터 HTTP Application DoS 등 이미 알려진 웹 공격에 대한 포괄적 방어

13) 패턴 업데이트
〉 매월 정기 패턴 업데이트 제공

〉 긴급 취약점 발생 시 실시간 업데이트 및 공지

AICC for Machine Learning



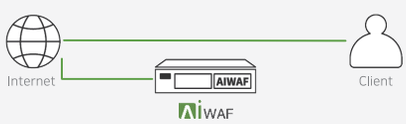


AIWAF Network Deployment

In-Line Mode (Full Transparent Proxy)
〉 인라인으로 배치되며 네트워크 구성 변경 불필요

〉 장애 발생 시 S/W 바이패스 및 H/W 바이패스 수행

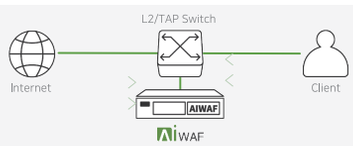
〉 멀티 세그먼트 제공 및 비동기 트래픽 처리



Out-of-path Mode (Reverse Proxy)
〉 분산 배치된 웹 서버군들에 대한 광범위 보호

〉 네트워크 경로나 DNS 주소 변경을 통해 AIWAF로 트래픽 유입

〉 HA 구성 또는 DNS Failover를 통한 서비스 연속성 확보



Out-of-path Mode (Mirroring)
〉 TAP, Switch 등 네트워크 시스템으로 부터 복사된 트래픽 수신

〉 장애 발생 시 네트워크 영향도 없음

〉 복사된 트래픽에 대한 보안 규칙 적용(차단 지원)

AIWAF Models & Specifications

AIWAF APPLIANCE의 표준 워크로드를 기반으로 작성되었으며, 실제 성능은 워크로드 요구 사항에 따라 크게 달라질 수 있습니다.

Specification	Appearance	RAM	HDD	MGMT/HA	NETWORK (Default)	NETWORK (Option)	CPS HTTP / HTTPS	TPS HTTP / HTTPS	Throughput HTTP / HTTPS	물품식별번호	조달등록가(VAT포함)
AIWAF-200 _Y20		8GB (Max 128GB)	500G	- Mgmt1 UTP Port - HA 1 UTP Port	1G UTP*4	Slot 1 - 1G UTP 4Port - 10G - 1G Fiber 4Port	30,000 10,000	55,000 35,000	2G 1G	24097068	24,800,000
AIWAF-500 _Y20		16GB (Max 128GB)	500G	- Mgmt 1 UTP Port - HA 1 UTP Port	1G UTP*4	Slot 1 - 1G UTP 4Port - 10G Fiber 2Port - 1G Fiber 4Port	55,000 15,000	80,000 55,000	4G 2G	24100922	34,000,000
AIWAF-1000 _Y20		32GB (Max 2TB)	2TB	- Mgmt 1 UTP Port - HA 1 UTP Port	-	Slot 8 - 1G UTP 4Port - 10G Fiber 2Port - 1G Fiber 4Port - 40G Fiber 2Port	130,000 35,000	250,000 1,000,000	10G 5G	24097069	40,850,000
AIWAF-2000 _Y20		32GB (Max 2TB)	2TB	- Mgmt 1 UTP Port - HA 1 UTP Port	-	Slot 8 - 1G UTP 4Port - 10G Fiber 2Port - 1G Fiber 4Port - 40G Fiber 2Port	200,000 50,000	300,000 150,000	14G 8G	24100921	47,210,000
AIWAF-4000 _Y20		64GB (Max 2TB)	2TB	- Mgmt 1 UTP Port - HA 1 UTP Port	-	Slot 8 - 1G UTP 4Port - 10G Fiber 2Port - 1G Fiber 4Port - 40G Fiber 2Port	250,000 70,000	400,000 200,000	15G 9G	24100920	57,715,000

제조사

MONITORAPP

(주)모니터랩
서울시 구로구 디지털로 31길 20, 407
TEL : 070-4633-7280
EMAIL : sales@monitorapp.com

조달 등록 업체

VISIONTEK

(주)비전테크
부산시 해운대구 센텀중앙로97 센텀스카이비즈 A동 2509호
TEL : 051-892-3723 FAX : 051-955-3723

조달 총판 업체

IFWIN

(주)아이티윈
부산 : 부산시 서구 보수대로 111, 동아빌딩 2F TEL : 051-245-5321
서울 : 서울시 서초구 반포대로 24길 15, 중앙빌딩 1층 TEL : 0 2-574-5321
대전 : 대전시 서구 대덕대로 319 , 우림빌유 213호 TEL : 042-483-5321