APPLICATION INSIGHT WAF

We Secure & Accelerate e-Business

MONITORAPP

What is APPLICATION INSIGHT WAF?

APPLICATION INSIGHT WAF는 완전한 HTTP Protocol 해석을 기반으로, Profile 기반의 자동화된 보안 정책과 주기적인 업데이트를 포함하는 정규화된 시그너쳐(Signature) 기반의 보안정책을 지원하며, 다양한 부가 기능을 통해 외부의 해킹으로부터 웹 서비스를 보호해주는 전용 웹 방화벽 제품입니다.

APPLICATION INSIGHT WAF는 기술력을 인정받은 신뢰성 있는 제품입니다.

- 다수의 공인 인증기관으로부터 인증서 획득
  - TTA : GS인증, IPv6 Verified 획득
  - 기술표준원 : NEP 인증
  - 국가정보원 : CC인증 (국내 최초 IPv6 포함) 획득
  - 기타 : IPv6 Ready Logo
- 다양한 기술 특허 보유
  - Transparent Gateway 특허 등록 (특허번호 제 10-0898371호)
  - Adaptive Profiling Technology 특허 등록 (특허번호 제 10-0695489호)
  - WEB-DB 공격 탐지 로그 데이터 상관관계 추적에 의한 통합 보안 시스템 특허 등록 (특허번호 10-0937020호)

APPLICATION INSIGHT WAF는 성능이 우수합니다.

- 고성능 패킷 처리 및 부하분산 알고리즘을 통한 대용량 트래픽 처리 성능 극대화
- 10G 웹 방화벽 기준 가장 많은 Reference 확보
- 요청 및 응답기반의 자동학습 정책 동시 제공 및 다중 방어모듈을 통한 완벽한 웹 공격 차단
- 중단 없는 웹 서비스 제공을 위한 Fail-open 및 Fail-over 기능 제공

Why APPLICATION INSIGHT WAF?

IT Compliance

- 개인정보보호법안 개정 - 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 보안 침입 차단 및 침입 탐지 기능을 갖춘 시스템을 설치 운영하여야 함
- HIPPA(미국 의료 데이터 보관 기준) 적용 관련 국내 건강정보보호법안 입법 준비 중
- PCI-DSS(신용카드 정보보안 표준) - 카드 가맹점, 서비스 제공자, 카드결제 대행업자(VAN) 등은 PCI SSC 가 마련한 기준 12개 항목을 모두 만족하고 인증을 받아야 함

APPLICATION INSIGHT WAF 도입 효과

- IT Compliance에 대응할 수 있는 정보보호시스템 구축
- 다양한 정책 적용을 통한 중요 정보 자산 보호

WEB Security Risks

- 80포트는 웹 서비스를 위해 항상 개방된 서비스이므로 해커의 공격 위협에 노출되어 있음
- 웹 애플리케이션 해킹을 통한 DB 중요 정보 유출 가능성
- IDS, IPS 등 기존 보안 제품의 한계에 따른 웹 공격 위험성 증대
- 스마트폰, SNS 등 정보통신 기기 및 기술 등의 발달로 언제 어디서나 웹을 통한 주요 정보 접속 가능성 확대

APPLICATION INSIGHT WAF Function

Diverse Web Security Functions

- OWASP TOP 10
- 국정원 8대 취약점
- 인코딩 우회 공격
- XSS/CSRF
- Injection
- Forceful Browsing
- Crawling/Scraping
- Directory Traversal
- Buffer-Overflow
- Application Exploits
- 쿠키 위변조
- 웜/바이러스
- 세션 공격/DoS 공격
- Web Shell

WEBINSIGHT WAF

강력한 웹 보안기능 제공

- 다양한 공격에 대한 요청/응답 기반 공격 탐지
- 파라미터 분석을 통한 공격 탐지 및 차단 기능
- 주요 서버 정보 및 개인정보 유출 방지 기능
- 화이트리스트/블랙리스트/공격자 IP 자동 탐지
- 암호화된 HTTPS 통신 웹 보안 기능
- SSL Offload/SSL Termination

편리한 사용자 인터페이스 제공

- 웹 사이트 별 현황에 대한 선택적 모니터링
- 유형별/시간별/일자별 로그 통계 및 보고 기능
- 침입로그에 대한 상세 검색 및 분석 기능
- 멀티 도메인 관리 기능
- 다수의 보안 시스템에 대한 통합 관리 기능
- 선택적 로깅 및 경고 기능
- ESM, SNMP 등 시스템 연동 기능
- Web server health check

APPLICATION INSIGHT WAF Physical Deployment

In-Line Mode

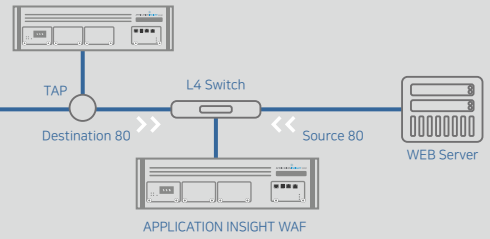
- 네트워크 경로상에 Bridge 형태로 In-Line 구성
- Transparent Proxy Mode 로 동작
- 보안 수준에 따른 탐지/차단 운영 가능
- Multi-Segment 지원
- 장비 이상 시 Bypass 지원

One-Armed Mode

- L4 Switch 에서 Port Redirection 을 이용한 구성
- Transparent Proxy Mode 로 동작
- 보안 수준에 따른 탐지 / 차단 운영 가능
- Multi-Segment 지원

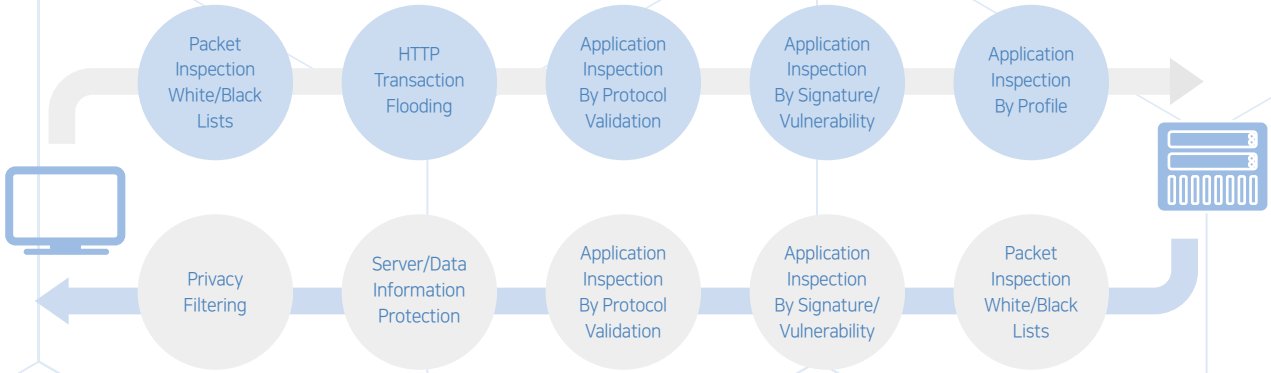
Mirroring Mode

- TAP 또는 L2 switch의 Mirror 기능을 이용한 구성
- HTTP/HTTPS 트래픽 처리 및 차단 기능 제공
- 기존 네트워크에 영향을 주지 않음



APPLICATION INSIGHT WAF Function Flow

웹 환경을 완벽히 보호하기 위한 다계층 보안 정책 적용



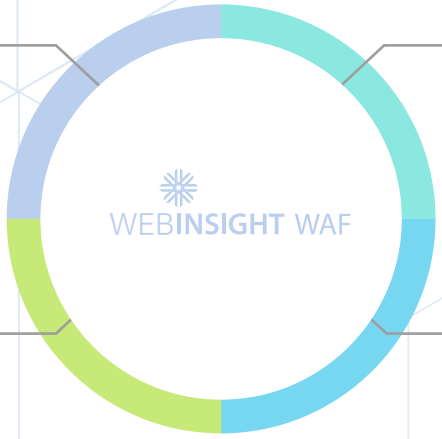
APPLICATION INSIGHT WAF Special Technology

Self Learning Profiling

- 자동화된 WEB 보안 정책 생성 및 적용
- Self Learning Engine에 의해 웹 서버의 정상적인 Request / Response를 토대로 Profile DB 구축 (특허번호 10-0695489)
- 비정상적인 Request 원천 차단

Various Web Attack Protections

- 웹 기반 DoS 공격 탐지 및 방어
- 웹쉘 업로드 탐지 및 접근 방어
- SSL Offload 및 SSL Termination
- IPv6 환경에서도 IPv4와 동일한 방어 기능



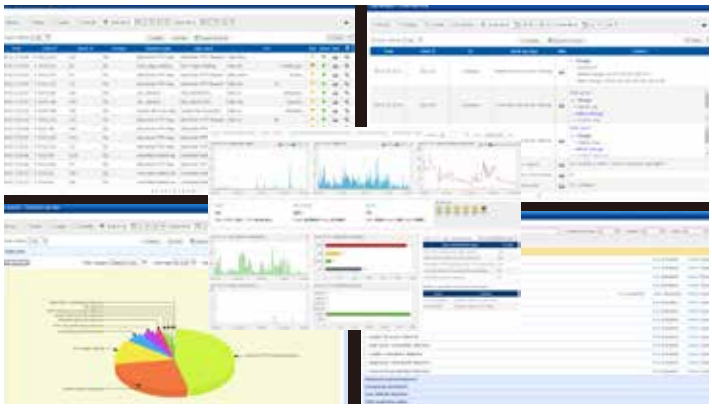
Proxy Gateway

- Transparent Proxy 방식 (특허번호 10- 0898371)
- 세계 최고 수준의 proxy 기술을 통한 웹서버 보호
- OWASP Top 10 취약점 방어
- 국정원 8대 웹 취약점 방어
- 개인정보 유입 및 유출 탐지

Various Network Deployment

- In-Line Mode
- One-Armed / Mirror Mode
- Reverse Mode
- Multi-Segment
- Bonding

APPLICATION INSIGHT WAF Graphic User Interface



통합 관리 기능
- Manager Center를 통한 다수의 WIWAF 통합 관리
- 개별 정책 마다 URL 및 Client IP에 대한 예외처리 기능 제공
- 도메인별 정책 적용 및 관리기능

로그 관리 기능
- 정책에 위반된 로그(요청/응답)에 대해 다양한 검색
- 조건을 통한 조회 및 관리

시스템 모니터링 기능
- WIWAF 의 시스템 상태 확인
- 트래픽 현황, 탐지 현황, 웹 서버 상태 등 포괄적인 웹 서비스
- 상태 정보 실시간 모니터링

통계 및 보고 기능
- 공격 유형/IP 등 공격 및 트래픽 현황에 대한 다양한 리포트
- 도메인 별 관리자에 의한 선택적 모니터링 및 리포팅 가능

APPLICATION INSIGHT WAF Feature

Gateway Configuration Mode
- Proxy Gateway : Transparent Proxy Mode

Physical Configuration Mode
- In-Line Mode : Bridge 구성
- One-Armed Mode : L4 Redirect 구성
- Reverse Mode : DNS 정보 변경 구성
- Multi-Segment, Port Trunk , Bonding

HA 기능
- Active-Standby
- Active-Active
- Link Synchronization
- 정책 동기화

취약성 공격 차단
- 취약성 공격 탐지 룰 : OWASP, 국정원 취약점, IIS, APACHE, CGI 등에 대한 차단 룰
- 사용자 정의 룰
- White List/Black List
- 공격자 IP 자동 탐지

비정상 요청/응답 차단
- Static Positive Security Policy : HTTP Request 파라메타 제어
- Dynamic Positive Security Policy : 자동학습 엔진에 의한 차단 룰

차단페이지 설정
- 정책 별 차등적인 차단메시지 설정

웹 서버 Cloaking
- 헤더 Cloaking : 응답 데이터에 포함된 주요 헤더를 제거하여 서버 정보 유출을 차단
- 에러페이지 Cloaking : 에러페이지를 지정된 페이지로 대체하여 에러를 통한 정보유출 차단

SSL Offload / SSL Termination
- SSL 미 지원 웹 서버를 대체한 SSL 통신 수행
- 웹 서버의 SSL 트래픽 부하 감소

HTTP 기반 비정상 공격 차단
- 요청 플러딩 차단
- 세션 공격 차단
- 스크래핑/크롤링 행위 차단 CAPTCHA 인증을 통한 Bot 차단

개인정보 유출 및 유입 방지
- 주민번호나 신용카드번호 등 주요 정보 유출 및 유입 차단

HTTP DoS 차단
- Slowloris, RUDY 등 HTTP DoS 공격 차단

웹 가속
- 웹 캐싱 기능을 이용한 가속 기능 제공

강제 브라우징 차단
- 강제 브라우징 공격 차단

웹쉘 탐지 솔루션 연동
- WEB API 기반 3rd Party 솔루션 연동

APPLICATION INSIGHT WAF Model & Specification

* Optional Interface

AIWAF-100- Y17

- Single Power Supply
- 10/100/1000 x 4

AIWAF-200- Y17

- Single Power Supply
- 10/100/1000 x 6
* 10/100/1000 *4 or 1G Fiber *4

AIWAF-500- Y17

- Redundant Power Supply
- 10/100/1000 x 6
* 10/100/1000 *4 * 2 or 1G Fiber *4 *2

AIWAF-1000- Y17

- Redundant Power Supply
- UTP 10/100/1000 x 2 and Fiber 10G x 2
* 10/100/1000 *4 *7 or 1G Fiber *4 *7 or 10G Fiber *2 *7

AIWAF-2000- Y17

- Redundant Power Supply
- UTP 10/100/1000 x 2 and Fiber 10G x 2
* 10/100/1000 *4 *7 or 1G Fiber *4 *7 or 10G Fiber *2 *7

AIWAF-4000- Y17

- Redundant Power Supply
- UTP 10/100/1000 x 2 and Fiber 10G x 2
* F10/100/1000 *4 *7 or 1G Fiber *4 *7 or 10G Fiber *2 *7

MONITORAPP

한국(본사):
서울특별시 구로구 디지털로 31길 38-9 306호
08376
Tel: 02-749-0799
Fax: 02-749-0798

일본(지사):
도쿄도 미나토구 신바시 6-14-3 오나리몽 Prex 8F
105-0004
Tel: +81-3-3432-2067
Fax: +81-3-5425-4468