KSIDC
Korea Server Hosting Inc

KS Korea Server Hosting 코리아서버호스팅

웹방화벽 : WAPPLE

- 클라우드 부문 미래창조경영우수기업 대상
- 3년 연속 한국소비자만족지수 1위
- 2010년부터 랭키닷컴 IDC 분야 1위 유지
- 한국정보방송대연합 인증 정보보호준비도 평가
- 한국클라우드산업협회 인증 클라우드 확인제
- 한국품질혁신우수기업 선정
- 한국인터넷진흥원 시행 고객만족우수기업
- IDC부분 기술혁신 대상
- 대한민국 신성장동력 미래선도기업

코리아서버 호스팅은 보다 차별화된 유지관리로 기업과 개인의 전략적 파트너가 되겠습니다.

서울시 서초구 서초동 1710-1 SK 브로드밴드 IDC 센터
TEL : 02-593-8320 FAX : 02-6264-8321

웹방화벽

KSIDC
Korea Server Hosting Inc

KSIDC의 웹방화벽 서비스는
웹소스의 보안취약점으로 인한
공격을 탐지하고 **차단하는 서비스**입니다.

웹방화벽이란?

웹방화벽 서비스란 네트워크보안장비(Firewall, IDS, IPS) 서비스와는 달리 웹소스의 보안취약점으로 인하여 웹해킹 등의 보안사고가 발생하기 때문에 근본적으로 해결하기 위해서는 웹소스를 보안이 강화되도록 수정하는 작업이 필요합니다.
하지만 중소기업에서 웹보안소스로 수정하는 작업이 상당히 힘든점을 감안하여 KSIDC에서는 웹방화벽서비스를 지원하여 드립니다.
웹방화벽 서비스는 애플리케이션 계층(Layer 7)분석 기술과 정규화 기술을 바탕으로 HTTP/HTTPS 프로토콜에 대한 트래픽을 감시하여 불법적인 공격을 탐지하고, 해당 공격이 고객 웹서버에 도달하기전에 차단하는 서비스입니다.

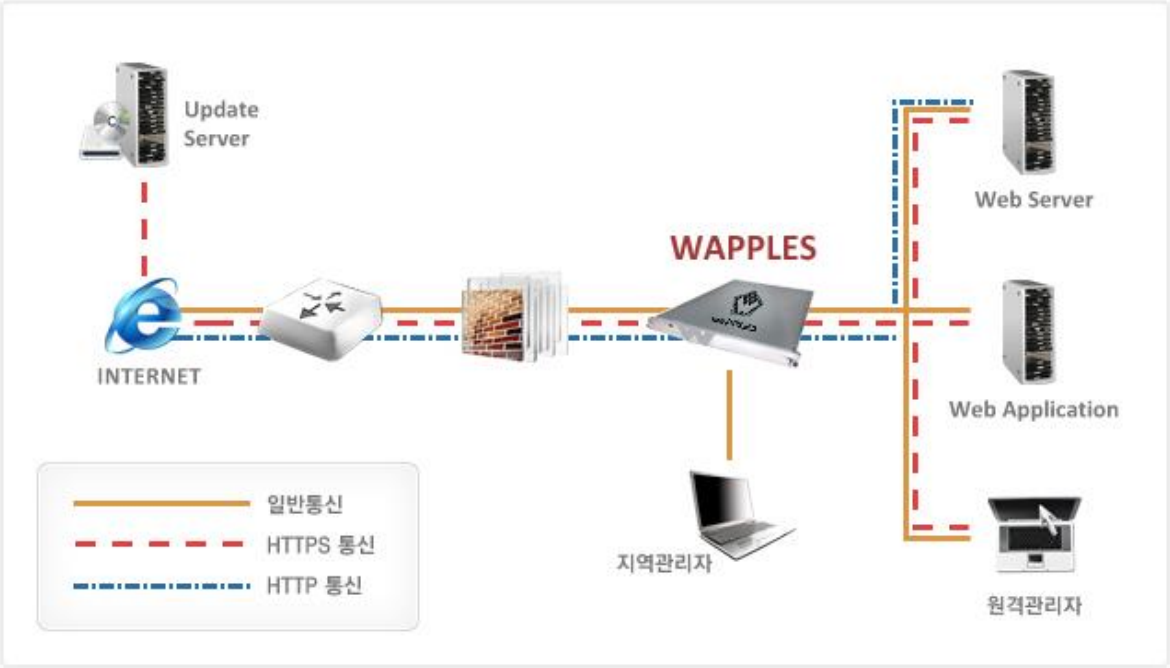
OWASP TOP10 웹 애플리케이션 보안 취약점

1. 다양한 리눅스 플랫폼 설치 지원 (Cent OS, Fedora 최선버전)
2. 인젝션 취약점 (Injection Flaws)
3. 악성 파일 실행 (Malicious File Execution)
4. 안전하지 않은 직접 개체 참조 (Insecure Direct Object Reference)
5. 크로스사이트 요청 변조 (CSRF: Cross Site Request Forgery)
6. 정보유출 및 부적절한 오류처리 (Information Leakage and Improper Error Handling)
7. 취약한 인증 및 세션관리 (Broken Authentication and Session Management)
8. 불안전한 암호화 저장 (Insecure Cryptographic Storage)
9. 불안전한 통신 (Insecure Communications)
10. URL 접속제한 실패 (Failure to Restrict URL Access)

웹방화벽

KSIDC
Korea Server Hosting Inc

- 하드웨어 웹방화벽서비스 (Wapple)
  - ✔ 투명프록시(Transparent Proxy) 방식



- 웹 서버와 방화벽 사이에 In-line 방식으로 설치, 운용
- 네트워크 설정의 변경 없이 구축 가능
  - 웹 서버 IP 및 DNS 변경 불필요
- 웹 클라이언트의 IP가 웹 서버에게 그대로 보존 전달
- Bypass 기능 지원

웹방화벽

KSIDC
Korea Server Hosting Inc

제품기능

✔ Inbound 트래픽에 대한 3단계 검사

- 전처리기
  - SSL 복호화 및 Normalization, HTTP 규약의 준수 여부 검사를 통해 이상 트래픽 제거
- Positive Security Model 모듈
  - URI별 접근제어를 수행, 허가된 URI 이외의 접속을 거부
- Negative Security Model 모듈
  - 접속이 허가된 요청 가운데 공격이 포함되어 있는지 여부를 검사

✔ Outbound 트래픽에 대한 검사

- Content Filter 모듈
  - 개인정보 포함 여부, 변조된 페이지 여부 확인, 에러 메시지 분석을 통한 정보 노출 방지
- Encryption 모듈
  - 변조 가능한 쿠키 및 히든 필드 등에 대한 무결성 검증값을 연산
- 공격 메커니즘 분석 탐지
  - 일반적인 웹 공격 탐지 기법의 한계

· 이미 알려진 다양한 공격 패턴을 감지하므로 패턴 업데이트 이전에 발생하는 zero-day attack에 취약
· 고정적인 형식을 갖지 않는 SQL/Command Injection 공격에 취약
· 학습 기간 내에 발생한 공격에 대한 학습 가능성 존재
· 반드시 예외 상황이 존재하므로 관리자의 조정이 필요
· 웹 사이트의 개편 혹은 수정 시 추가적인 학습 필요

웹방화벽

KSIDC
Korea Server Hosting Inc

- 단순 패턴 매칭이 아닌 애플리케이션 공격 로직 분석 기능 제공
  - · 알려지지 않은 새로운 취약점이라도 해당 공격기법 탐지 규칙을 통해 방지
  - · 입력값 내용이 공격 가능한 논리 구조를 가짐이 판명되면 이를 탐지 차단
  - · HTTP 처리 능력을 시험 -> 브라우저로 위장한 Worm 및 취약점 스캐너를 탐지
- 웹 공격 탐지에 최적화된 구조
  - · 단순 패턴 매칭으로 탐지할 수 없는 다양한 변형 공격 탐지 가능
  - · 관리자의 개입 최소화

- **알려지지 않은 공격 탐지**
- Input Content Filtering (사용자 정의 룰)
  - 사용자 입력 문자열을 탐지
  - 지정한 문자열로 변경 지원
- Invalid HTTP
  - HTTP의 규격에서 벗어난 요청이나 응답, 존재하지 않는 웹 사이트에 대한 요청 차단
  - 알려지지 않은 취약점을 이용한 웜을 비롯한 공격 도구들로부터 생성되는 비정상적인 트래픽을 차단
- Invalid URI
  - RFC에 정의된 형식을 벗어난 URI 요청을 차단
  - RFC 표준을 침해하는 신규 취약점에 대한 공격 방지
- Suspicious Access 탐지 규칙
  - 정상적인 웹 브라우저가 아닌 클라이언트의 접속을 대상으로 이상 징후를 판단하거나 접근을 제한
  - 신규 취약점에 대한 스캐닝, 자동화된 공격도구의 접근 방지