Intelligent Web Application Firewall

APPLICATION INSIGHT WAF

2020.11. VER 5.0

MONITORAPP

DONGHOON 동훈아이텍

Contents

1. WEB 보안의 필요성

IT 및 주요 환경의 변화

IT 환경의 변화

- 스마트 기기의 발달로 언제 어디서든 인터넷 접속이 가능 하여 개인 또는 회사 업무의 연속성 증가
- 접근성과 사용 편의성으로 주요 데이터 및 정보가 웹으로 집중
- 서비스,금융, 쇼핑, 의료 등 다양한 웹 서비스의 증가

중요 자산으로서 정보의 가치 상승

- 대다수의 웹 서비스 사용을 위해 기본적인 개인정보 요청이 빈번히 발생
- 데이터 및 개인정보 탈취를 목적으로 한 공격 증가
- 사고발생 시 심각한 기업 이미지 저하 및 경제적 손실 초래

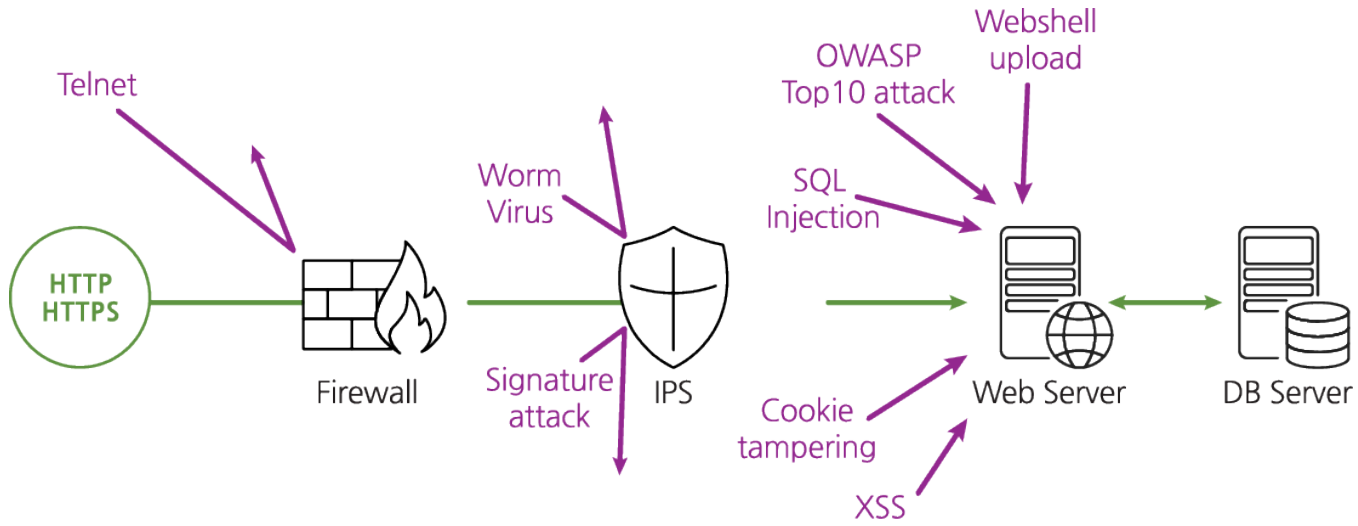
IT Compliance & 법률 강화

- IT Compliance 요구 증대
- ISMS 인증 대상 확대
- 개인정보 보호법 발효로 처벌 기준 및 책임소재 강화

기존 보안 솔루션의 한계점

- 웹 서비스를 위한 포트는 반드시 오픈 되어 있음
- IPS는 SSL 통신에 대한 방어능력이 미흡(시스템 부하 급증)하며 세부적인 정책 설정을 제공하지 않음
- 웹에 대한 강력하고 전문적인 솔루션이 필요

기존 보안 시스템의 한계



■ 방화벽 및 IPS와 웹 방화벽의 기능 비교

구분	방화벽	IPS	웹 방화벽
내용	• 네트워크 인프라를 보호하는 데 임무의 초점 • 80, 443 포트는 정상적인 통신으로 간주 • 웹 프로토콜(HTTP, HTTPS)에 대한 제어 불가능	• L3 – L7 Layer 전반에 걸친 보안 기능 제공 • SSL 통신에 대한 방어 능력 미흡 • 시그니처 방식에 의존 하므로, 우회 취약구간 다수 발생 • 세부 정책 구현 미 제공	• HTTP, HTTPS에 대한 강력하고 전문적인 보안 가능 • Positive Security Model 구현으로 알려지지 않은 공격에 대해 원천적으로 차단 가능

WAF Vs IPS / NG FW

	Web Application Firewall	Intrusion Prevention System	Next-Generation Firewall
Multiprotocol Security	○	●	●
IP Reputation	◑	◑	◑
Web Attack Signatures	●	◑	○
Web Vulnerabilities Signatures	●	◑	◑
Automatic Policy Learning	●	○	○
URL, Parameter, Cookie, And From Protection	●	○	○
Leverage Vulnerabilities Scan Results	●	◑	○

● = good to very good ◑ = average on fair ○ = below average

출처: Gartner

웹 애플리케이션의 변화

OWASP Top 10 2013		OWASP Top 10 2017		OWASP Top 10 2021
A1-인젝션		A1:2017-인젝션		**A1:2021-접근 권한 취약점**
A2-취약한 인증과 세션 관리		A2:2017-취약한 인증		**A2:2021-암호화 오류 [변경]**
A3-크로스 사이트 스크립팅(XSS)		A3:2017-민감한 데이터 노출		**A3:2021-인젝션**
A4-안전하지 않은 직접 객체 참조		A4:2017-XML 외부 개체(XXE)		**A4:2021-안전하지 않은 설계**
A5-잘못된 보안 구성		A5:2017-취약한 접근 통제		**A5:2021-보안 설정 오류 [변경]**
A6-민감한 데이터 노출		A6:2017-잘못된 보안 구성		**A6:2021-취약하고 오래된 요소**
A7-기능 수준의 접근 통제 누락		A7:2017-크로스 사이트 스크립팅(XSS)		**A7:2021-식별 및 인증 오류**
A8-크로스 사이트 요청 변조(CSRF)		A8:2017-안전하지 않은 역직렬화		**A8:2021-소프트웨어 및 데이터 무결성 오류 [신규]**
A9-알려진 취약점이 있는 구성요소 사용		A9:2017-알려진 취약점이 있는 구성요소 사용		**A9:2021-보안 로깅 및 모니터링 실패 [변경]**
A10-검증되지 않은 리다이렉트 및 포워드		A10:2017-불충분한 로깅 및 모니터링		**A10:2021-서버 측 요청 위조(SSRF) [신규]**

출처: https://www.owasp.org

핵심 포인트

- 웹 서버는 특성상 서비스를 위해 항상 외부에 노출되어 운영
- 위와 같은 이유로, 전체 해킹 사고의 약 80%는 웹 서버를 타켓으로 하여 발생하며 점진적 확대
- 웹사이트 코드 내에 포함되어 있는 취약점들이 문제이며, 이런 취약점들 중 절반을 해결 하는데 평균 100일 소요
- 해커들은 매년 향상된 실력으로 웹 사이트의 취약점을 찾아내어 공격하고 있어 해결되지 않은 웹 취약점은 소니, AT&T 등의 대량 정보유출 사고와 같은 결과를 초래

2. APPLICATION INSIGHT WAF
소개 및 특장점

APPLICATION INSIGHT WAF Line-UP

Specification	AIWAF-100_Y20	AIWAF-200_Y20	AIWAF-500_Y20	AIWAF-1000_Y20	AIWAF-2000_Y20	AIWAF-4000_Y20	AIWAF-8000_Y20
Appearance							
RAM	4GB	8GB (최대 128GB)	16GB (최대 128GB)	32GB (최대 2TB)	32GB (최대 2TB)	64GB (최대 2TB)	64GB (최대 2TB)
HDD	500G	500G	500G	2TB	2TB	2TB	2TB
MGMT / HA	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port
Network (Default)	1G UTP * 2	1G UTP * 4	1G UTP * 4	-	-	-	-
Network (Option)	-	Slot 1 - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	Slot 1 - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port
CPS HTTP / HTTPS	5,000/1,500	30,000/10,000	55,000/15,000	130,000/35,000	200,000/50,000	250,000/70,000	350,000/100,000
TPS HTTP / HTTPS	9,000/5,000	55,000/35,000	80,000/55,000	250,000/100,000	300,000/150,000	400,000/200,000	550,000/300,000
Throughput HTTP / HTTPS	400M/200M	2G/1G	4G/2G	10G/5G	14G/8G	15G/9G	16G/10G

- Slot에 NIC 모듈을 선택/조합하여 장착할 수 있으며, SSL 가속카드를 옵션으로 장착 가능 합니다.
- 본 제품의 사양은 성능향상을 위하여 예고 없이 변경될 수 있습니다.
- 성능 수치는 계측기 프로파일 및 환경에 따라 차등적 일 수 있습니다. 계측 환경은 APPLIANCE SHEET 정보를 참고하시기 바랍니다.

Full Transparent Proxy

■ 네트워크 구성 변경 없는 간단한 구축

- APPLICATION INSIGHT WAF는 별도의 IP 부여 없이 Stealth-mode로 운영 됨
- 기존 네트워크 환경 변화 없음

❖ Transparent Proxy

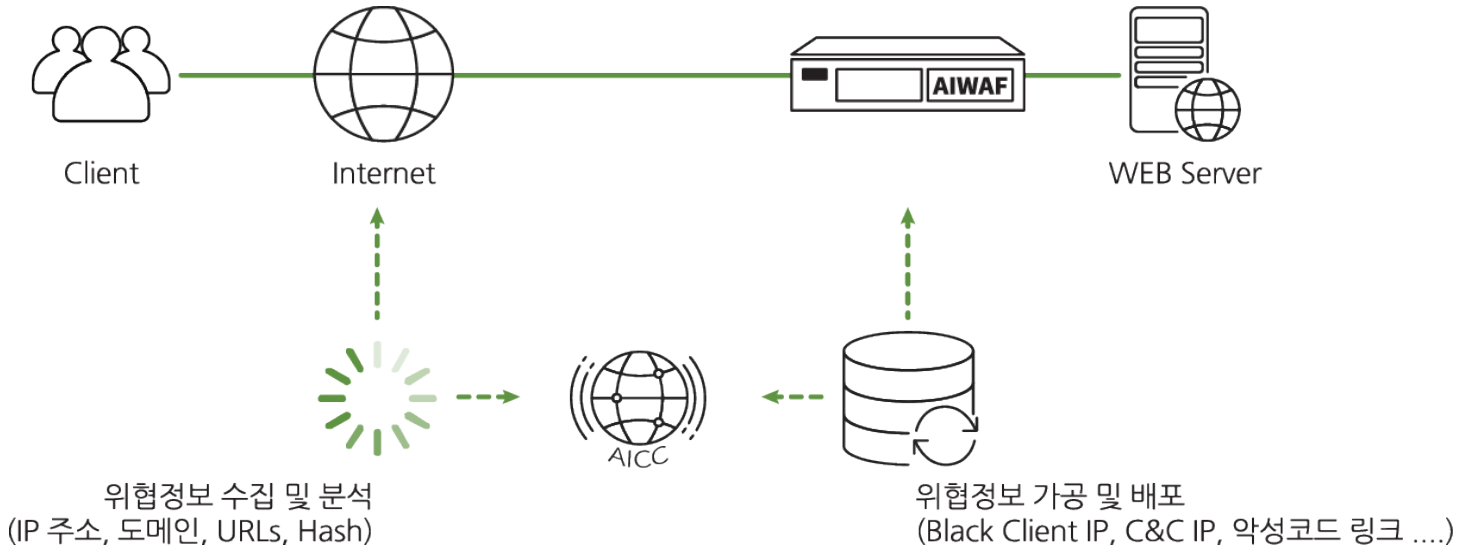
Proxy base Full Transparent Mode - 특허기술 (제 10-0695489호)

Cyber Threat Intelligence Platform 연동

■ 보안 규칙 만으로 해결 할 수 없는 다양한 위협에 대한 선제적 대응

- Cyber Threat Intelligence Platform 연동을 통한 다양한 웹 공격 위협에 대한 실시간 대응
- Proxy IP, Black Client IP, C&C IP, 악성코드 링크 삽입 등에 대한 포괄적/신체적 대응 체계 구축
- Attack IP에 대한 평판정보 제공

❖ AICC(Application Insight Cloud Center)

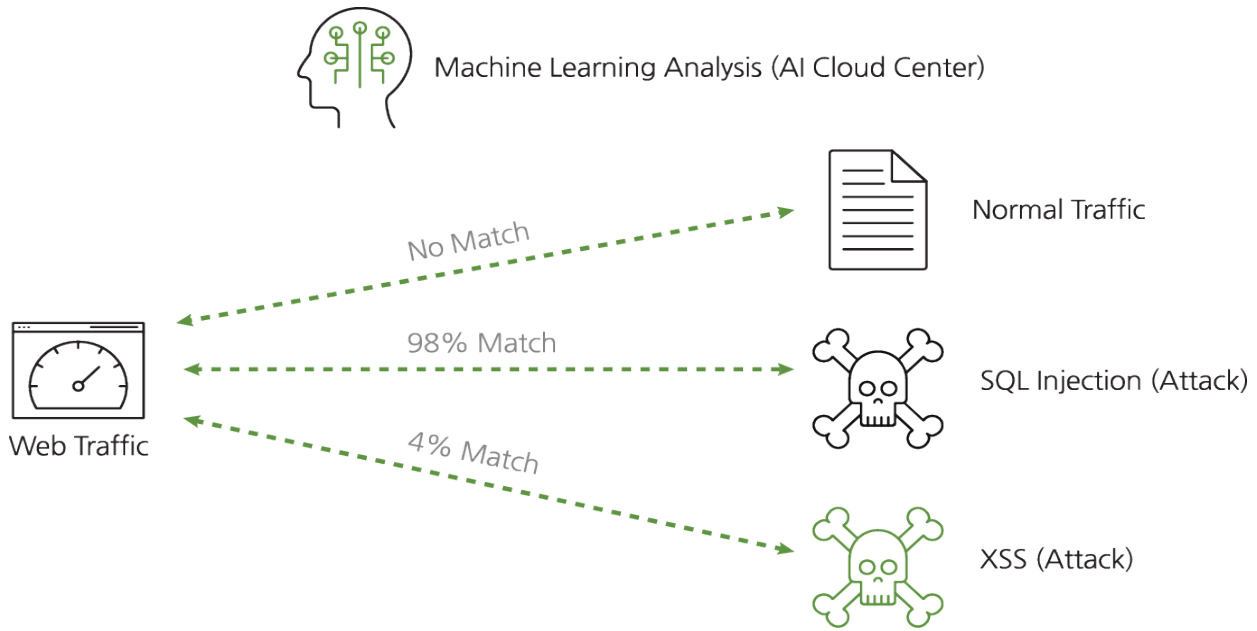


Machine Learning 기반 Unknown Attack 탐지

■ 대응 패턴이 없는 신규 웹 취약점에 대한 효율적 대응

- 이상 행위 및 위협 탐지를 위한 머신 러닝(클라우드 센터) 연동
- 알려진 위협을 비롯하여 알려지지 않은 공격으로부터 웹 기반 애플리케이션 보호

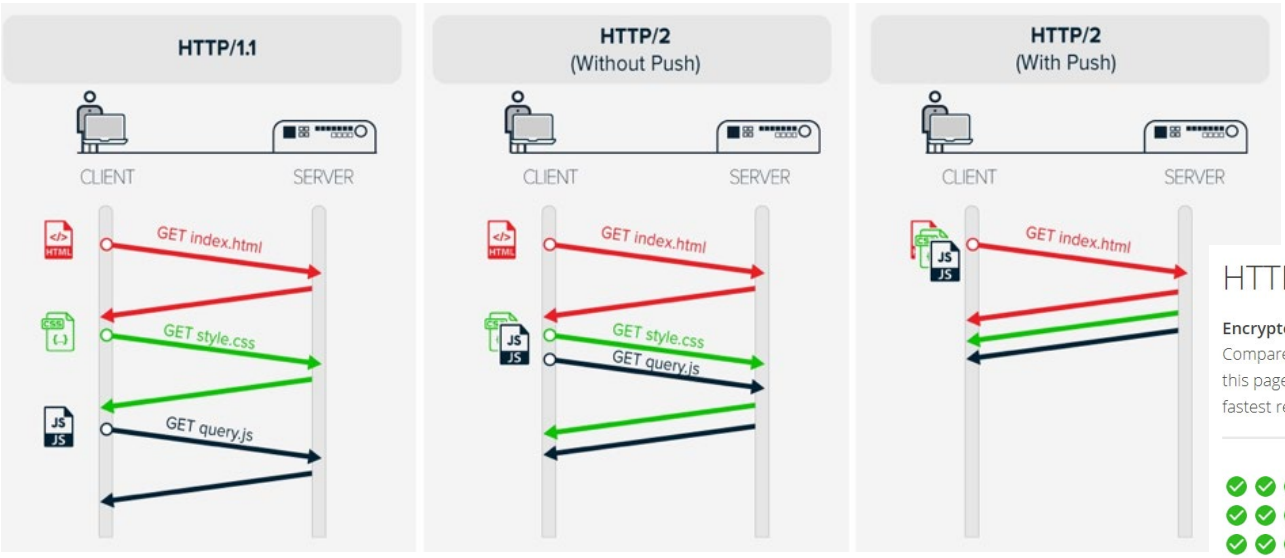
❖ Machine Learning

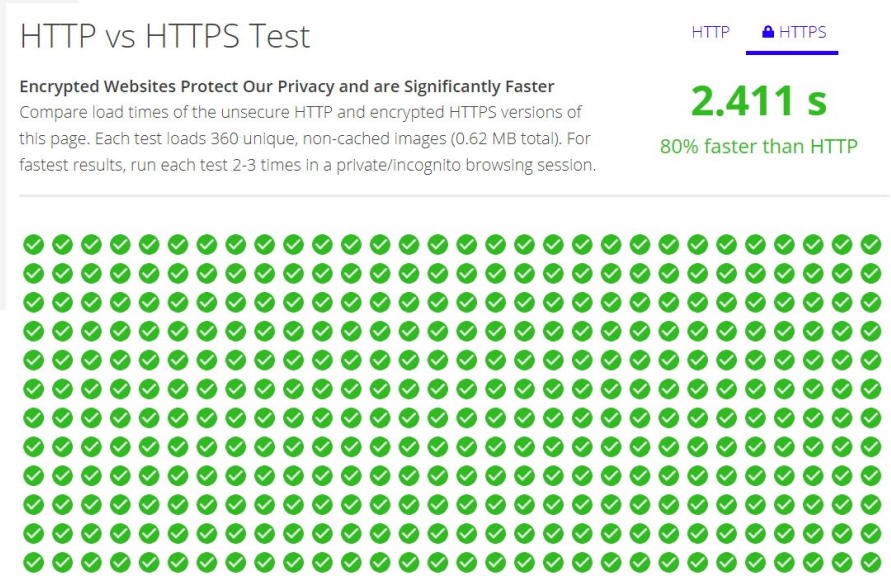


HTTP/2 프로토콜 제어

■ 기존 웹 서비스의 HTTP/2 로 손쉬운 전환

- HTTP/2는 HTTP/1.1과 전혀 다른 구조의 프로토콜이며 암호화(HTTPS) 통신만 지원
- HTTP/2 트래픽에 대한 완전한 Parsing 및 모든 보안 기능 동일 적용

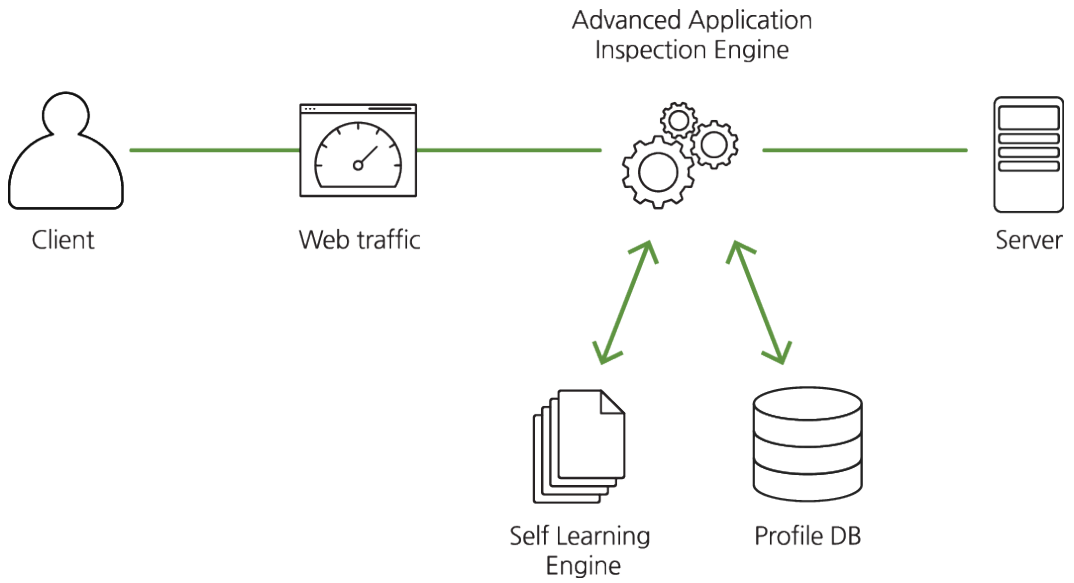




Adaptive Profiling Technology

■ 실시간 공격 차단 목적 보다는 사후분석 용도로 효과적

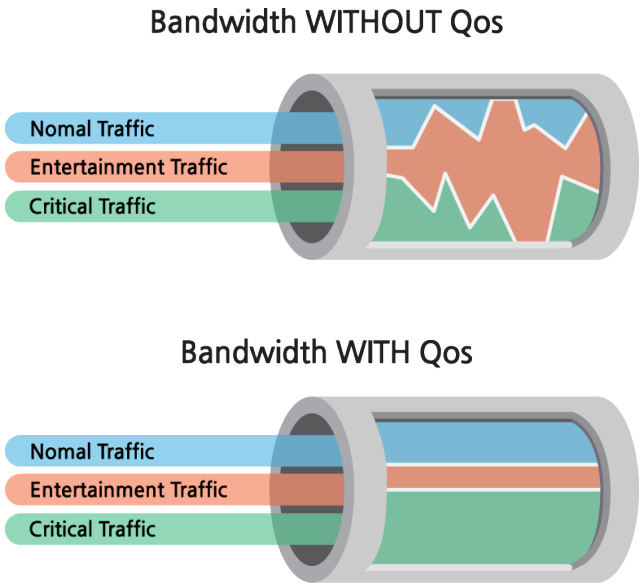
- Self-Learning 엔진에 의해 클라이언트의 정상적인 request와 웹 서버의 response를 토대로 프로파일 데이터베이스 구축
- 클라이언트들의 request를 프로파일 데이터 베이스와 비교하여 비정상적인 형태의 request 원천 차단
- 알려지지 않은 공격에 대한 최상의 방어 모델



멀티 도메인 정책 및 트래픽 관리

■ 효율적인 도메인(서비스)별 품질 관리

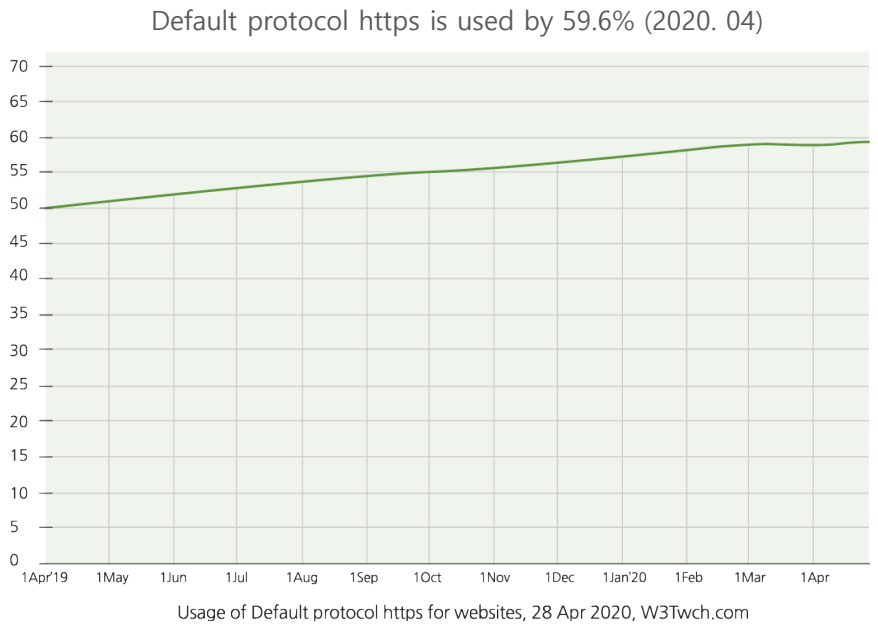
- 웹 서버에 제공하는 여러 도메인(서비스)에 대해 각 각의 도메인 별 차등적 정책 적용
- 각 도메인 별 관리자 지정(복수 지원)을 통한 독립적 모니터링/로그분석/정책 운영의 편의성 제공
- 웹 사이트(도메인)별 QoS 대역폭 제한 설정



유연하고 손 쉬운 HTTPS 트래픽 관리

■ HTTPS 서비스 관리로 인한 장애포인트 최소화

- SSL / TLS 사용의 일반화와 대중화에 따른 HTPS 암호화 트래픽 급증
- 유연한 암호화 트래픽 제어와 고성능 처리 능력이 웹 방화벽 솔루션의 중요 포인트로 대두
  - TLS 1.3 지원
  - 멀티도메인 인증서 지원
  - 다양한 확장자 지원(인증서 변환 과정 불 필요)에 따른 간편한 인증서 등록
  - 실제 웹 서버 활성화 Cipher-Suite 목록과 동기화(자동 설정)
  - 인증서 만효 사전 알림 및 인증서 만료시 자동 바이패스 기능



요청 및 응답 트래픽에 대한 URL Rewrite

■ 복잡한 URL을 간단하고 일관된 웹 주소로 변환

- 와일드카드(*) 및 정규표현식을 통해 요청/응답 트래픽의 URL, 헤더, 본문 Rewrite 규칙 정의
- 검색 엔진 최적화(SEO) 및 사용자 환경 개선

- Request의 "URL, 헤더, 본문" 조건이 규칙에 부합 하는 경우

  설정한 규칙 내용으로 Rewrite(치환 또는 삽입) 후 서버로 전송
  지정된 URL로 클라이언트에 301, 302 Redirect 응답
  사전 정의한 응답코드와 HTML 내용으로 클라이언트에 응답

- Response의 "헤더, 본문" 조건이 규칙에 부합 하는 경우

  설정한 규칙 내용으로 Rewrite(치환 또는 삽입) 후 클라이언트로 전송

악성코드 경유지 · 유포지 악용 탐지

■ 웹 사이트 방문자 및 브랜드 가치 보호

- 웹 서버 공격의 주된 목적은 정보 유출을 비롯하여 악성코드 경유지/유포지로 사용 하기 위함
- 웹 서버의 모든 응답 데이터를 대상으로 응답 페이지에 삽입된 악성코드를 검출 함으로서
- 웹 방화벽을 우회하여 유입된 공격이나, 웹 방화벽 도입이전 부터 악성코드 경유지/유포지로의 악용 탐지 및 차단

멀티 · 더블 인코딩 공격 탐지

■ 정탐↑ 오탐↓

- 일부 웹 서비스(페이지)는 필요에 따라 다양한 형태의 인코딩 데이터로 통신
- 인코딩 된 쿼리 값 또는 페이로드 값에 공격 구문이 삽입될 경우 보안 정책 우회 가능한 Hole 발생
- Normalization을 통해 다양한 형태의 인코딩 된 데이터를 디코딩 후 Inspection 수행
- URL, HEX, UNICODE, BASE64 인코딩 지원

보안 규칙 최적화

■ 보안 Hole ↓

보안 규칙 별 상세 설정

- 오탐 발생시 Rule 별 예외 처리를 통해 서비스 가용성 보장 및 보안 Hole 최소화
- 적용 IP/URL 및 예외 IP/URL 설정
- 차단 페이지 차등 설정
- Disable 패턴 차등 설정
- 스케쥴 설정 등

Non HTTP 트래픽 제어

■ 수 많은 웹 서버 관리에 따른 불편 요소 제거

- 보호대상으로 등록된 웹 서버 중 HTTP(S) 이외의 서비스가 존재하는 경우
  프로토콜 유형 분석을 통해 WEB 이외의 트래픽은 자동 바이패스 시키는 기능
- 관리자의 잘못된 설정으로 인해 발생 가능한 서비스 장애 요소에 대한 효율적 운영 옵션

웹 서비스 품질 모니터링

■ 웹 서비스 이상 발생시 웹 방화벽 문제 인지 부터 간단하게 확인

- 보호대상 웹 서버들에 대한 실시간 웹 서비스 상태 모니터링
  TCP PORT 체크 방식이 아닌 실제 HTTP(S) 헬스체크 트래픽 발생

- 현재 상태, 응답 속도(최소, 최대, 평균), 가용률에 대한 웹 서버 품질 정보 제공
  웹 방화벽에 의한 서비스 속도 저하 여부 판별이나 장애 분석 시 용이한 데이터로 활용

Self 정책 점검

■ 신규 취약점 탐지 여부에 대한 빠른 판단

- 신규 최약점 발생 시 샘플코드를 입력하거나, 모의 해킹(웹 취약점 진단) 등 정책 설정 점검 목적으로
  웹 방화벽 보안 정책에서 어느 규칙이나 패턴으로 탐지 되는지 Self 테스트 수행

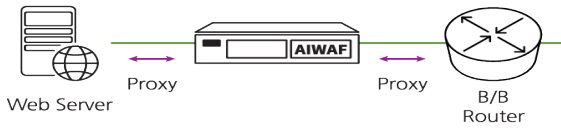
- 사용자가 직접 수립한 보안 규칙의 오류나 중복, 탐지 여부 사전 점검으로 운영 편의성 제고

3. 다양한 구축 방안

다양한 구성 방식

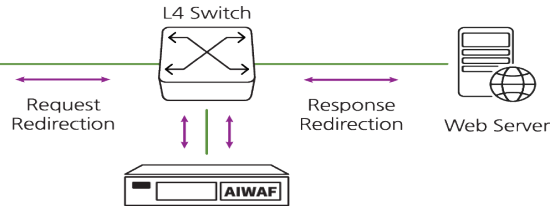
Transparent Proxy(IN-Line)

- 운영 모드: Transparent Proxy
- 물리적 구성: IN-Line
- 네트워크 경로상에 Bridge 형태로 In-line 구성
- IP가 없는 Transparent Proxy Mode로 작동
- 모든 보안 기능 제공
- 구축 레퍼런스 중 80% 구성 방식



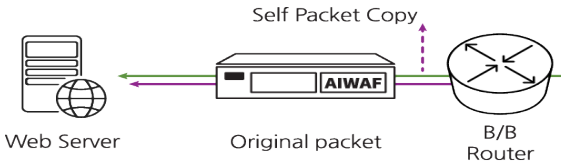
Port Redirection(Out-of-path)

- 운영 모드: Port Redirection
- 물리적 구성: One-Armed
- L3, L4 Switch 에서 Port Redirection 필요
- 구축 또는 장애 시 서비스 단절 없음
- 모든 보안 기능 제공
- 구축 레퍼런스 중 5% 구성 방식



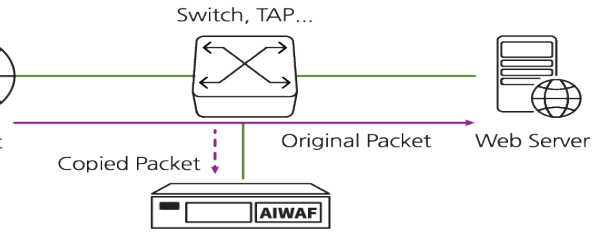
Sniffing(In-Line)

- 운영 모드: Sniffing
- 물리적 구성: IN-Line
- 패킷 복사 방식의 스니핑 타입으로 고성능 제공
- RSA 타입의 HTTPS 트래픽만 지원
- 전체 보안 기능 중 85% 제공
- 구축 레퍼런스 중 5% 구성 방식



Mirroring(Out-of-path)

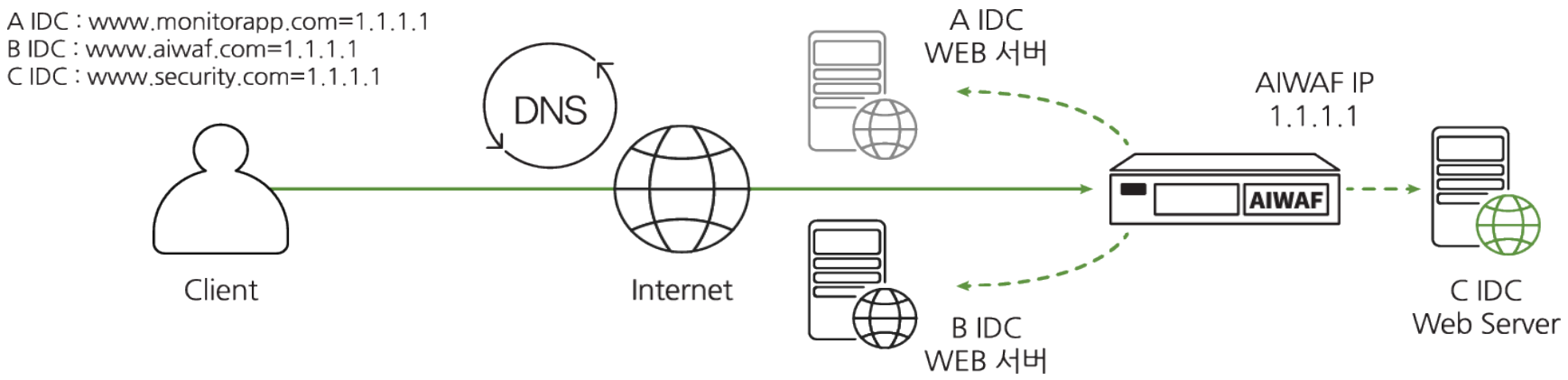
- 운영 모드: Mirroring
- 물리적 구성: One-Armed
- Switch 또는 TAP으로부터 복사 트래픽 수신
- 별도 차단 인터페이스를 통해 공격 트래픽 차단
- 전체 보안 기능 중 85% 제공
- 구축 레퍼런스 중 5% 구성 방식



다양한 구성 방식

Reverse Proxy(Out-of-Path)

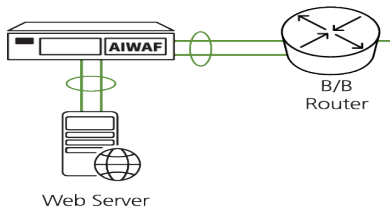
- 운영 모드: Reverse Proxy
- 물리적 구성: Out-Of-Path
- DNS 정보 중 웹 서버 IP를 웹 방화벽 IP로 변경 적용
- 단일개의 웹 방화벽 시스템에서 분산 배치 되어 있는 웹 서버 군에 대한 광범위 보호 제공
- Multi-Segment 지원
- 구축 레퍼런스 중 5% 구성 방식



다양한 네트워크 환경 지원

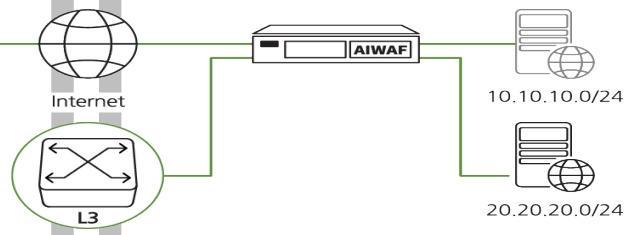
Port Trunk

- Port Trunk, Tag VLAN, LACP 구성 지원
- 네트워크 및 웹 서버의 IP 구성 환경 변화 없음



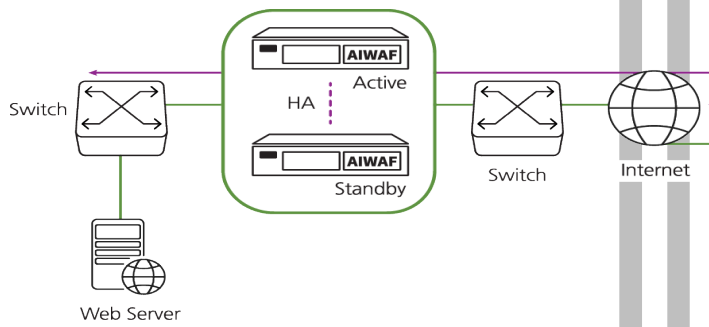
Multi-Segment

- N개의 Segment 지원 (인터페이스 수량에 따름)
- 네트워크 및 웹 서버의 IP 구성 환경 변화 없음
- Segment별 Fail-Open 기능 제공



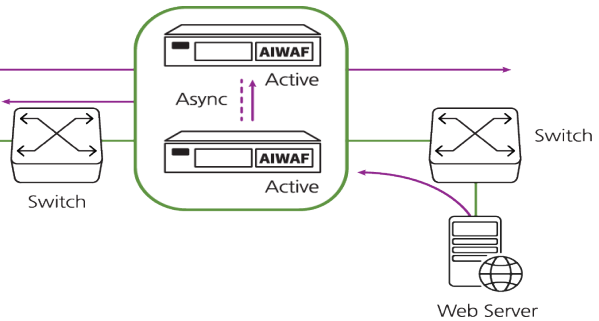
Active-Standby

- 웹 방화벽 시스템 간 상태 체크 수행
- 시스템 장애 발생 시 HA(Fail-Over) 제공
- Master, Slave 설정을 통한 자동 Fail-back 선택



Asynchronous

- 웹 방화벽 시스템 간 비동기 트래픽 포워딩 수행
- Multi-Segment 환경 지원



THANK YOU

제조사 ㈜모니터랩 | 주소 : 서울시 구로구 디지털로 27가길 27 아남빌딩 8,9층 08375 | Tel : 02-749-0799 | Fax : 02-749-0798 | Web : www.monitorapp.com
E-mail : sales@monitorapp.com | 사업자등록번호 : 214-87-66413

총판사 ㈜동훈아이텍 | 주소 : 서울시 강남구 역삼로 225, 동훈빌딩 3층, 6층 06224 | Tel : 02-580-6300 | Fax : 02-538-3241 | Web : www.dhitech.co.kr
E-mail : marketing@dhitech.co.kr | 사업자등록번호 : 220-81-88123 |