Application Delivery Leader
MONITORAPP

MONITORAPP

Application Security Leader

2021

Contents

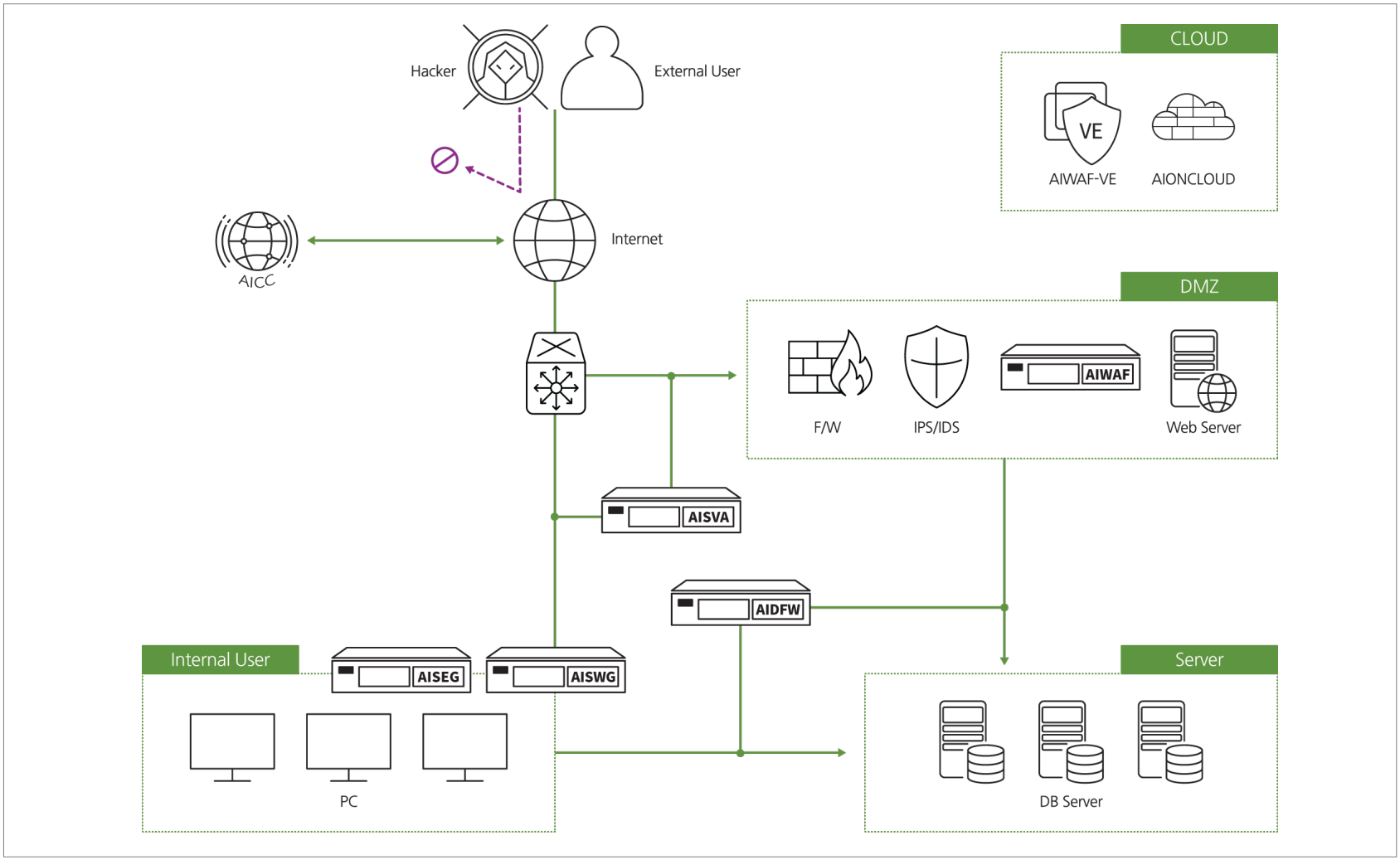
1. 모니터랩 소개

회 사 명	(주)모니터랩 (MONITORAPP)	설 립 일	2005년 2월 22일
인원/매출액	91명 / 107억 (2020년)	사업 종목	소프트웨어자문, 개발및공급, 정보보안솔루션
본점 소재지	서울시 구로구 디지털로 27가길 27	서비스URL	www.monitorapp.com

2005	02	㈜모니터랩 설립
2006	02	웹방화벽 WISG (AIWAF의 구버전) 출시
	04	수출유망 중소기업 선정 (중소기업청)
	06	WISG 제품 CC 및 GS 인증 취득
2007	03	'프로파일링 기반 웹 서비스 보안 시스템' 기술 특허 등록
	05	'원격 웹 서비스 보안 시스템' 기술 특허 등록
	11	AIDFW, DB 방화벽 출시
2008	05	'프로파일링 기반 DB 보안 시스템' 기술 특허 등록
	06	AIDFW, DB 방화벽 GS 인증 취득
2009	02	AIVFW, VoIP 방화벽 출시
	04	AIWAF 및 AIDFW 제품 CC 인증 취득
	05	'투명 프록시 시스템 및 패킷 처리 방법' 기술 특허 등록
2010	01	'웹-DB 간 로그 데이타 상관관계 추적에 의한 통합 보안' 기술 특허 등록
	05	AIVFW, VoIP 방화벽 CC 인증 취득
2011	08	태국 SI 업체 BlueZebra 와 총판 계약
2012	01	클라우드 용 웹방화벽 AIWAF-VE 출시
	04	태국 국회에 AIDFW 공급
2013	02	말레이시아의 보안 전문 업체 TechLab Security 와 총판 계약
	09	유해 사이트 차단 솔루션 AISWG 출시
2014	02	국제웹보안표준기구 OWASP 기업회원 가입
2015	03	AIWAF-VE 제품을 AWS(아마존웹서비스) 마켓플레이스에 게시
	11	SSL 가시성 장비, AISVA 출시
	12	AISWG 제품 GS 인증 취득
2016	08	일본 법인 설립
	09	베트남의 ISP 업체 Netnam 과 총판 계약
	10	SECaaS 플랫폼 AIONCLOUD 출시
	11	인도네시아의 NI 업체 RML 과 총판 계약
2017	02	일본 NI 업체 Artiza Networks 와 AISVA ODM 계약 체결
	03	나라장터 조달 시스템 SSL 가시성 분야에 AISVA 등록
	07	'데이터 마이닝을 통한 웹-DB 사용자 추적 방법' 기술 특허 등록
	12	AhnLab 및 아토리서치와 AIONCLOUD에 대한 White Label 파트너십 체결
2018	03	'보호 대상 서비스 자동 인식 방법' 기술 특허 등록
	04	AIONCLOUD에서 WMS 서비스 출시
	05	AIONCLOUD가 NIPA의 클라우드 품질 및 성능 인증 획득
	08	웹방화벽 제품 AIWAF 에 대한 CC 인증 획득
	11	메가존 클라우드와 AIONCLOUD에 대한 파트너십 체결
	12	UAE 벤더 ABS Mena와 AIWAF 에 대한 파트너십 체결
	12	일본 벤더 Secure Innovation과 AIONCLOUD에 대한 White Label 파트너십 체결
2019	04	미국 법인 설립
	06	일본 보안업체 앳시그널(@SIGNAL)과 SECaaS 공동사업 협약 체결
	07	'보안장치 경유 SSL 접속 불가 사이트 접속 지원 방법 및 시스템' 특허 등록
2020	02	'U R L 처리 장치 및 방법' 기술 특허 등록
	03	'세션 관리 방법 및 이를 이용한 보안중계장치' 기술 특허 등록
	06	'다중 문자열 패턴 탐색 방법 및 장치' 기술 특허 등록
	06	'머신러닝을 이용한 웹 기반 부정 로그인 차단 장치 및 방법' 기술 특허 등록

Product Map

- 모니터랩은 신속하고 안전한 애플리케이션 전송을 보장하기 위해 고성능 애플리케이션 프락시 기술을 기반으로 다양한 애플리케이션 가속기술과 애플리케이션 보안기술을 연구 개발하는 통합 애플리케이션 보안 기업입니다.



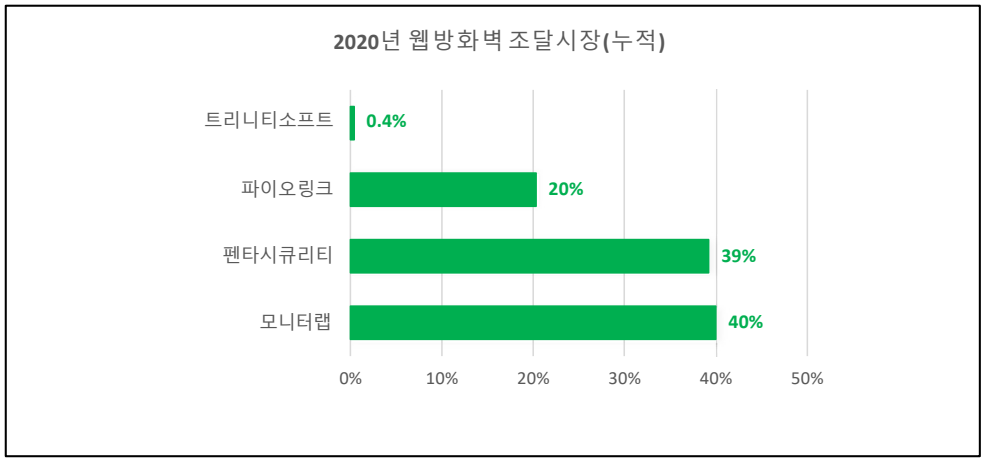
Reference

- 제안사는 다음과 같은 주요 고객사(450여곳)에 유지보수 기술지원을 하고 있습니다. (총 납품 3,500고객사 이상)

20년 조달시장 매출현황

[단위 : 백만원]

제조사명	모니터랩	펜타시큐리티	파이오링크	트리니티소프트	합계
제품명	WIWAF	Wapples	WEBFRONT	WEBS-RAY	
2020년 1월	258.0	94.6	71.8	0.0	424.4
2020년 2월	160.0	213.6	105.9	0.0	479.6
2020년 3월	397.7	346.4	154.2	0.0	898.3
2020년 4월	49.0	259.4	49.5	0.0	357.9
2020년 5월	119.0	378.4	201.5	0.0	698.9
2020년 6월	238.2	178.5	231.9	0.0	648.6
2020년 7월	132.0	248.7	0.0	0.0	380.7
2020년 8월	147.4	43.9	267.7	0.0	459.0
2020년 9월	424.5	292.7	132.1	0.0	849.3
2020년 10월	407.7	328.6	143.6	33.0	912.7
2020년 11월	544.7	332.0	63.4	0.0	940.1
2020년 12월	245.0	346.3	165.2	0.0	756.5
2020년 누적	3,123.1	3,063.1	1,586.7	33.0	7,805.9
점유율(%)	40%	39%	20%	0.4%	100%



2. 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

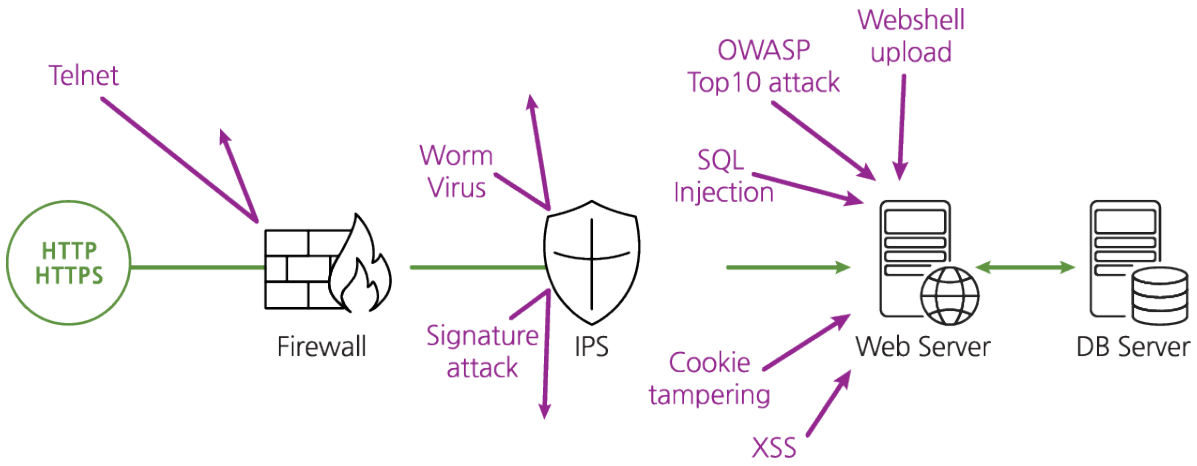
IT Compliance & 법률 강화

- 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

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

3. 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

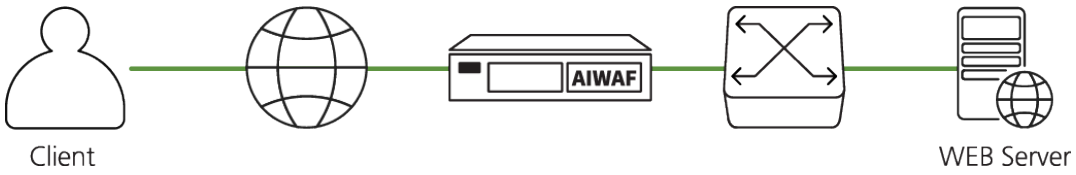
- Slot에 NIC 모듈을 선택/조합하여 장착할 수 있으며, SSL 가속카드를 옵션으로 장착 가능 합니다.
- 본 제품의 사양은 성능향상을 위하여 예고 없이 변경될 수 있습니다.
- 성능 수치는 계측기 프로파일 및 환경에 따라 차등적 일 수 있습니다. 계측 환경은 APPLIANCE SHEET 정보를 참고하시기 바랍니다.

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



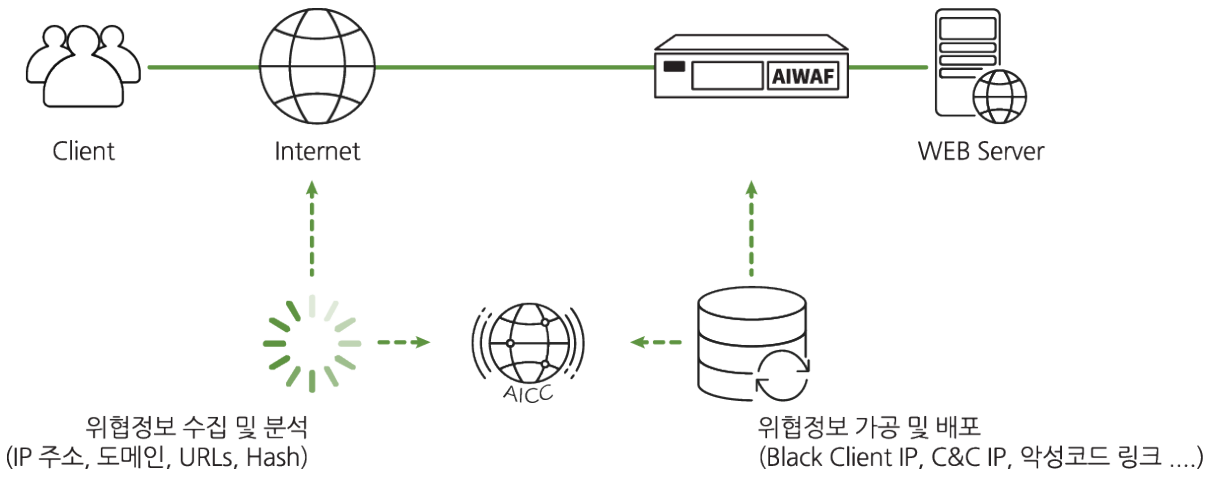
Proxy base Full Transparent Mode - 특허기술 (제 10-0695489호)

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)

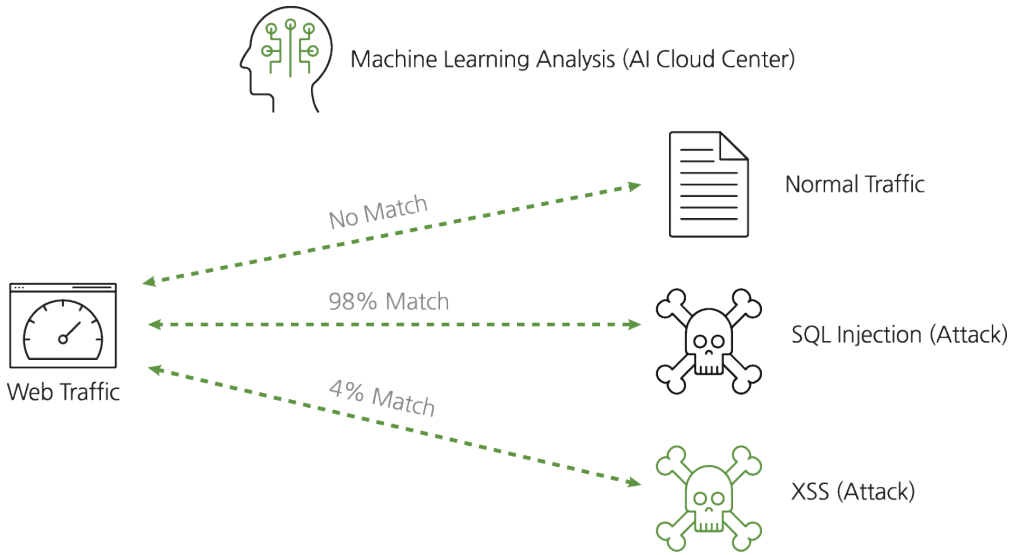


Machine Learning 기반 Unknown Attack 탐지

■ 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

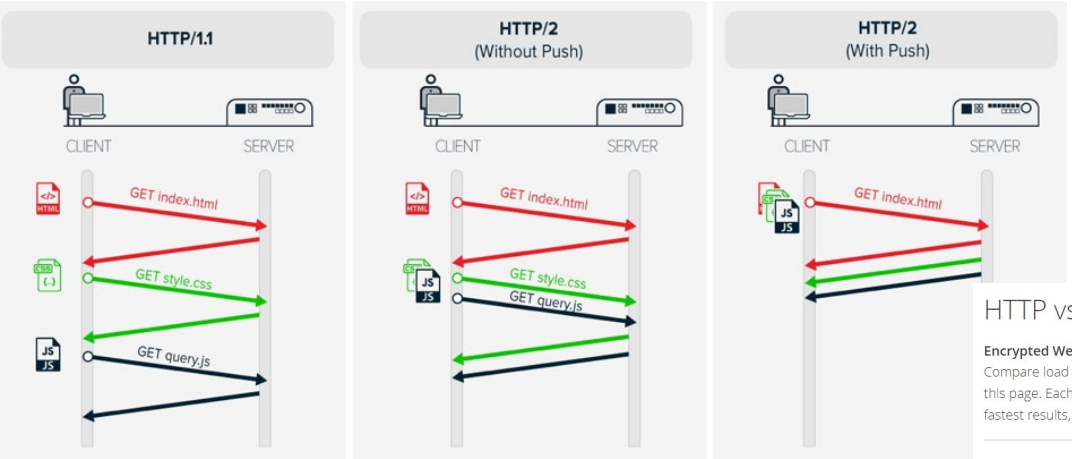
❖ Machine Learning

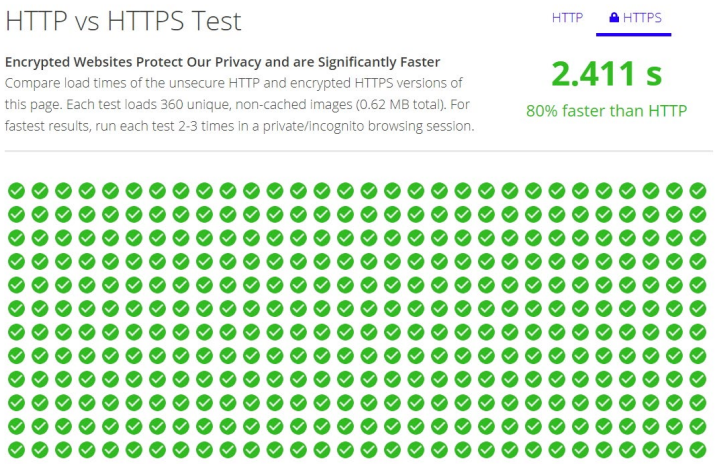


HTTP/2 프로토콜 제어

■ 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

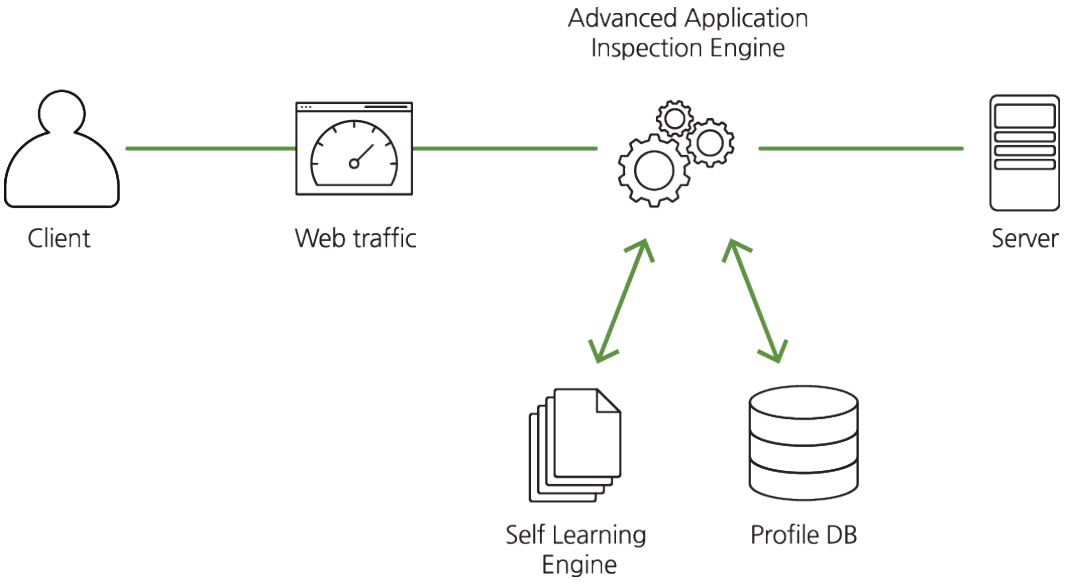




Adaptive Profiling Technology

■ 실시간 공격 차단 목적 보다는 사후분석 용도로 효과적

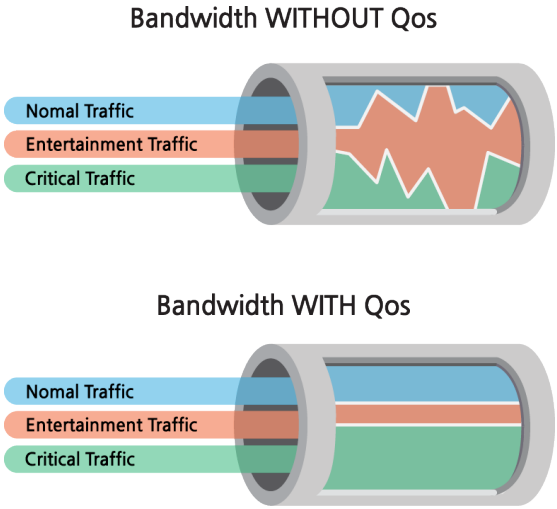
- Self-Learning 엔진에 의해 클라이언트의 정상적인 request와 웹 서버의 response를 토대로 프로파일 데이터베이스 구축
- 클라이언트들의 request를 프로파일 데이터 베이스와 비교하여 비정상적인 형태의 request 원천 차단
- 알려지지 않은 공격에 대한 최상의 방어 모델



멀티 도메인 정책 및 트래픽 관리

■ 효율적인 도메인(서비스)별 품질 관리

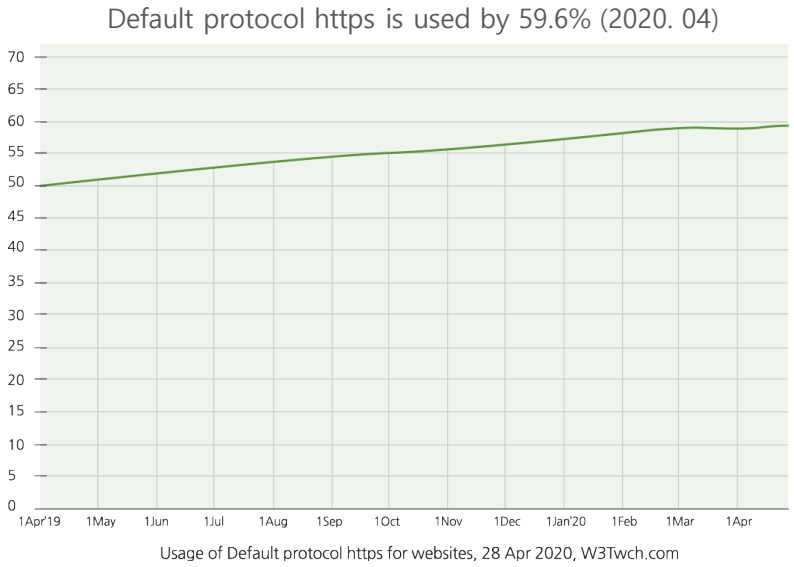
- 웹 서버에 제공하는 여러 도메인(서비스)에 대해 각 각의 도메인 별 차등적 정책 적용
- 각 도메인 별 관리자 지정(복수 지원)을 통한 독립적 모니터링/로그분석/정책 운영의 편의성 제공
- 웹 사이트(도메인)별 QoS 대역폭 제한 설정



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



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

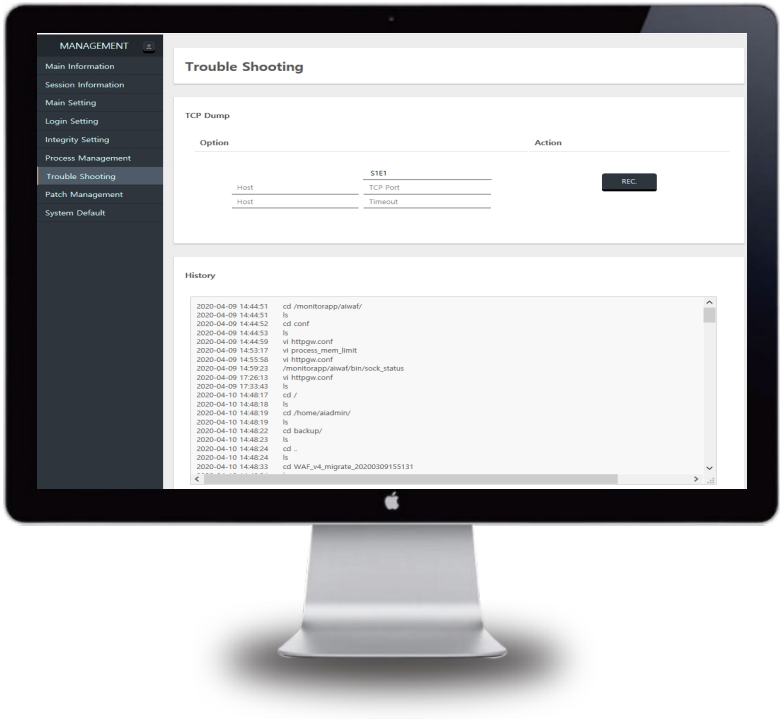
- 사용자가 직접 수립한 보안 규칙의 오류나 중복, 탐지 여부 사전 점검으로 운영 편의성 제고

Trouble Shooting

Trouble Shooting

- 기술지원 엔지니어나 고급 관리자를 위한
  제품 관리 및 트러블 슈팅 목적의 별도 UI 제공

- 제품 패치
- 제품 초기화
- 긴급 복구 모드
- 패스워드 초기화
- Debug Log 수집
- TCPDUMP 수집
- 이슈 분석에 필요한 주요정보 자동 수집
- 중요 설정 값 변경 및 조회



4. 구축 방안 및 사례

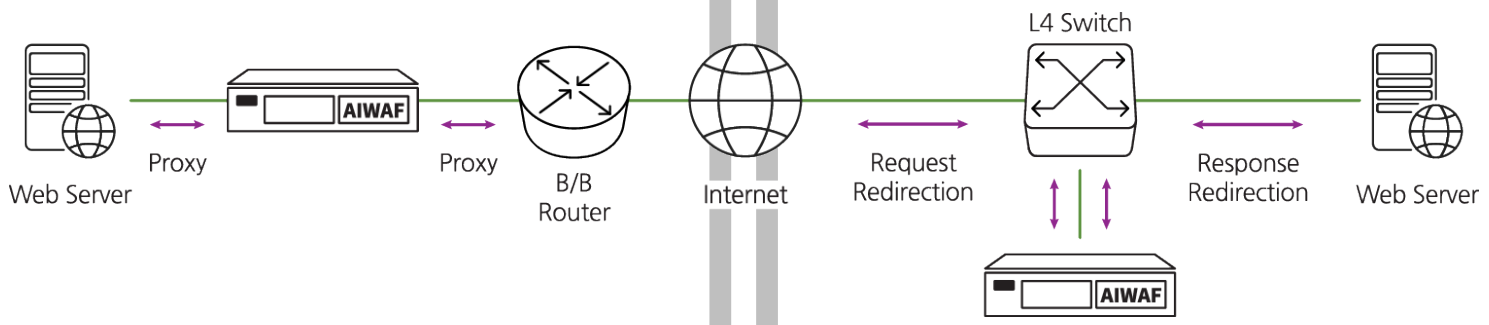
다양한 구성 방식

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)

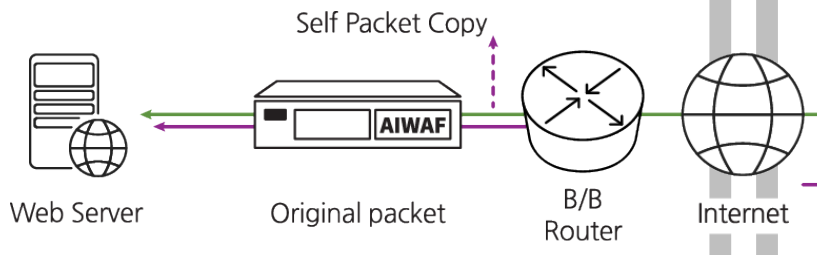
- 운영 모드: Port Redirection
- 물리적 구성: One-Armed
- L3, L4 Switch 에서 Port Redirection 필요
- 구축 또는 장애 시 서비스 단절 없음
- 모든 보안 기능 제공
- 구축 레퍼런스 중 5% 구성 방식



다양한 구성 방식

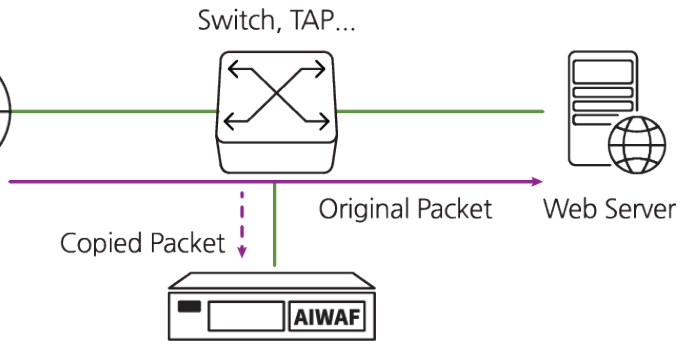
Sniffing(In-Line)

- 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)

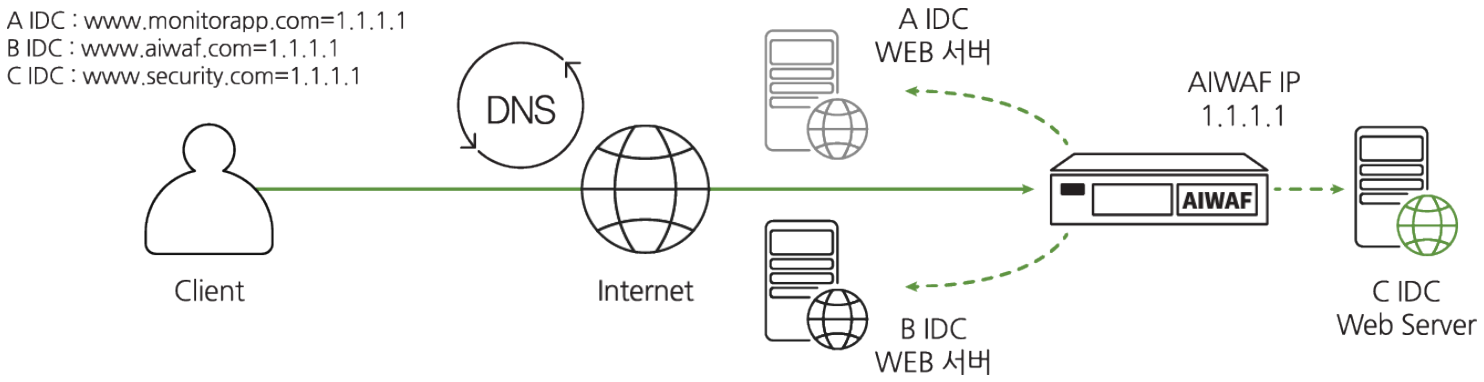
- 운영 모드: Mirroring
- 물리적 구성: One-Armed
- Switch 또는 TAP으로부터 복사 트래픽 수신
- 별도 차단 인터페이스를 통해 공격 트래픽 차단
- 전체 보안 기능 중 85% 제공
- 구축 레퍼런스 중 5% 구성 방식



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



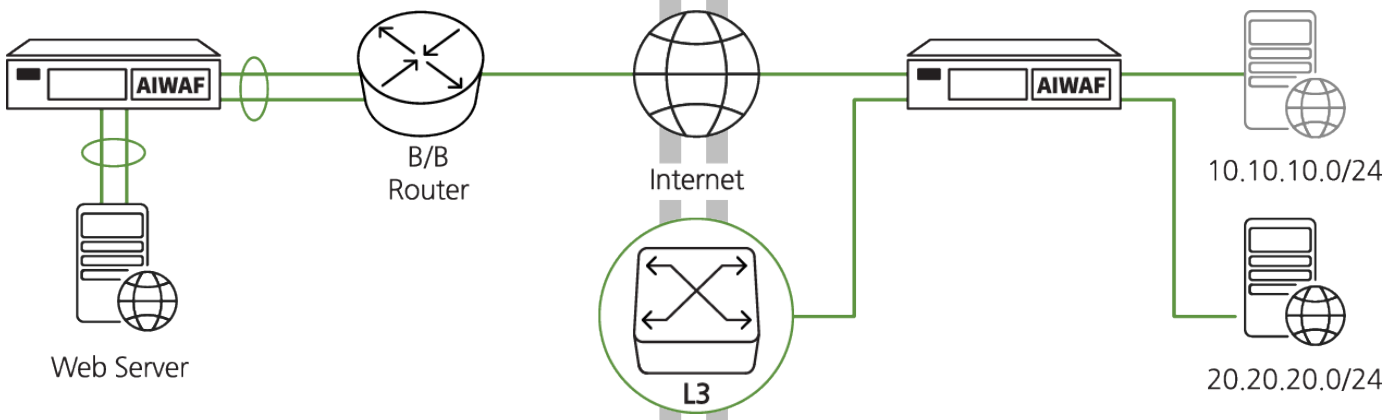
다양한 네트워크 환경 지원

Port Trunk

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

Multi-Segment

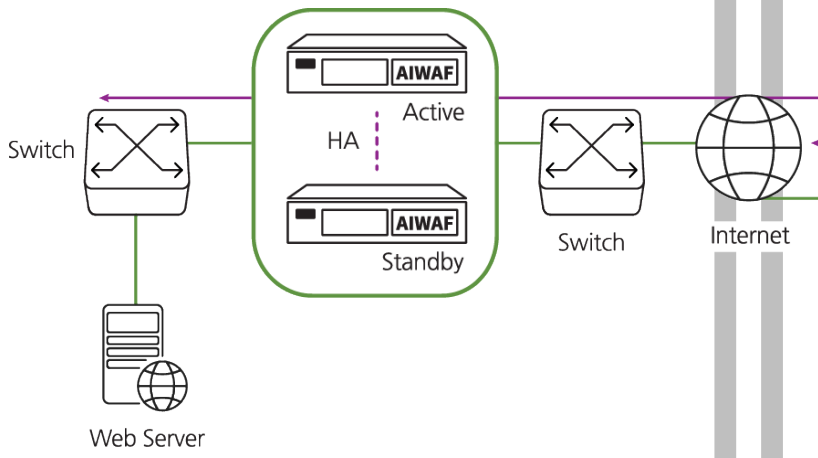
- N개의 Segment 지원 (인터페이스 수량에 따름)
- 네트워크 및 웹 서버의 IP 구성 환경 변화 없음
- Segment별 Fail-Open 기능 제공



다양한 네트워크 환경 지원

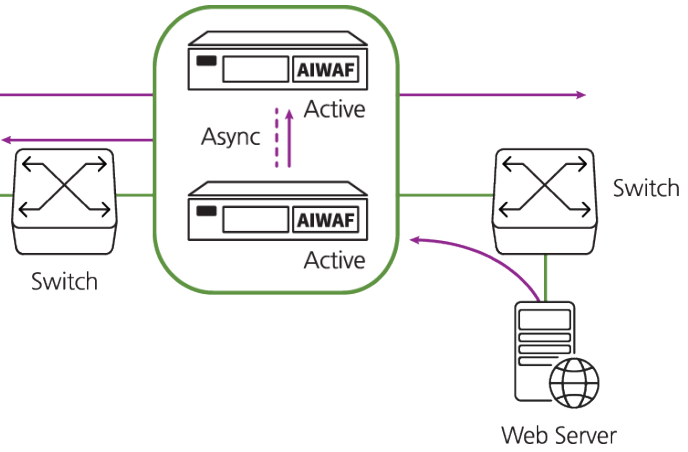
Active-Standby

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



Asynchronous

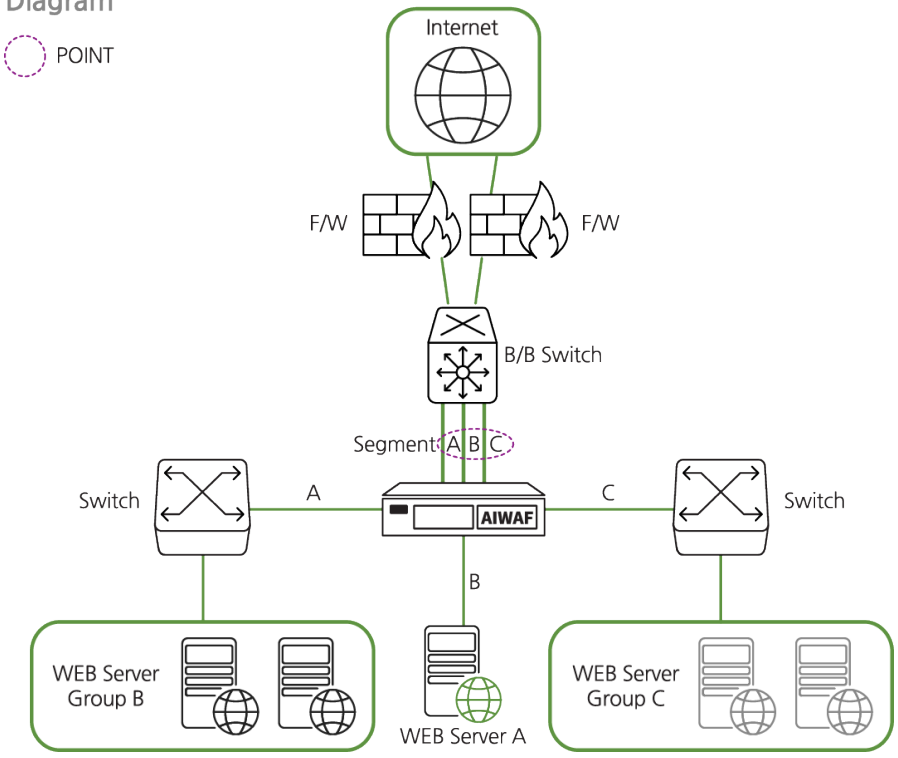
- 웹 방화벽 시스템 간 비동기 트래픽 포워딩 수행
- Multi-Segment 환경 지원



구축사례 (공공/해외 – I기관)

Diagram

POINT



Overview

- 각 웹 서비스 별 차등 정책 적용 (멀티 도메인)
- Tagged VLAN 환경 수용
- 웹 방화벽에 내장된 물리적 Bypass 기능을 통해 시스템 장애상황에서도 서비스 가용성 보장

Deployment

- 1개 웹 방화벽에서 분산 배치된 다양한 웹 서버군 수용
- 3 Multi Segment 구성

Effectiveness

- 기존 네트워크 모든 환경 구성 유지(환경 설정 변경 불필요)
- 대외 서비스 / 대내 서비스에 대한 효율적인 방어 체계 구축
- 각 웹 서버 담당자 별 보안 정책 설정 환경 제공

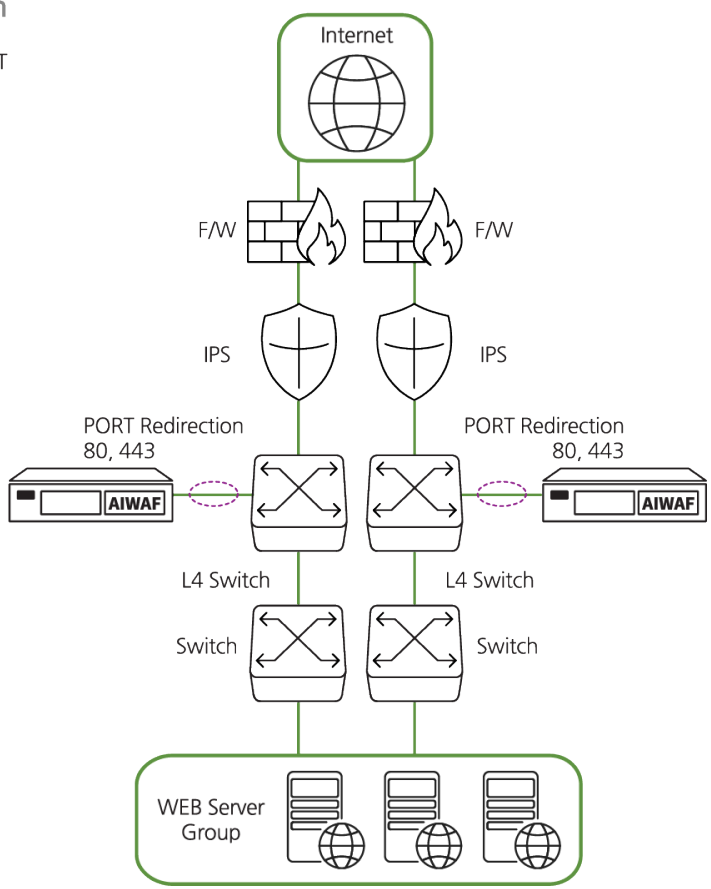
Main Policy

- SQL INJECTION, XSS, 어플리케이션 취약성 탐지

구축사례 (공공/국내 – H기관)

Diagram

POINT



Overview

- IPS에서 제어 불가한 상세 파라메터 제어
- 사용자 구분에 따른 접속 허용 URL 분리
- 취약한 라이브러리(openssl, bash 등) 버전 사용 웹 서버들에 대한 사전 방어

Deployment

- L4 스위치 Port Redirection 설정
  - HTTP / HTTPS 트래픽(Service Port) 양방향 필터
- 네트워크 전체 용량 대비 저용량 웹 트래픽 처리에 적합

Effectiveness

- IPS 탐지율 대비 19.4% 탐지율 향상 (IPS 미 탐지 건수 비교)
- 다수 웹 서버 패치 적용까지 발생 되는 Zeroday Attack 방어
- 사용자 IP별로 접속 가능한 웹 서비스 구분 적용

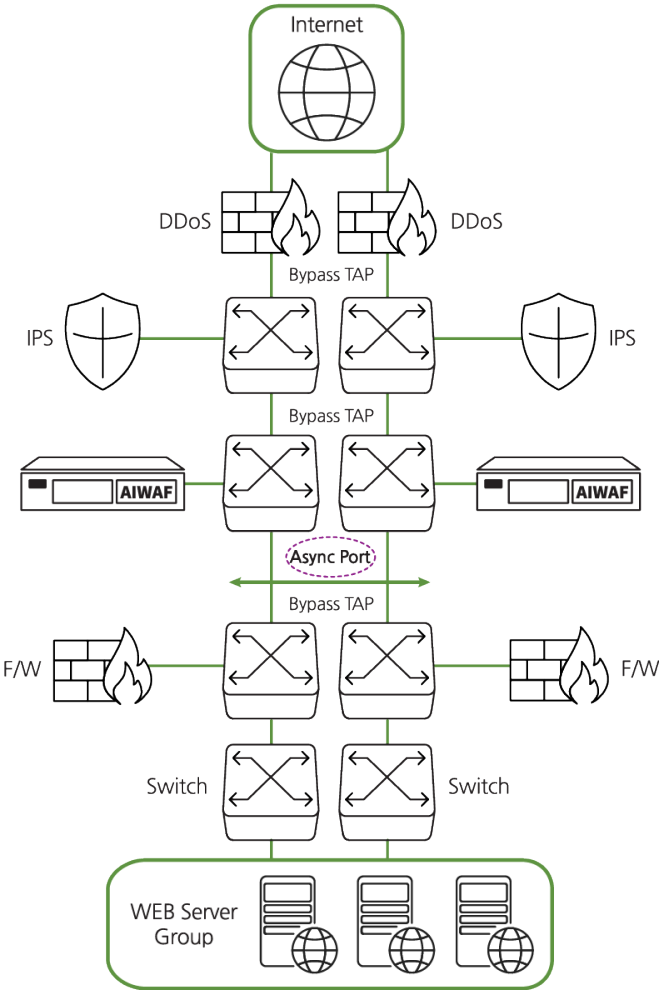
Main Policy

- URL 접근 룰, 헤더 취약성 탐지, 웹 서버 취약성 탐지

구축사례 (기업/국내 – P사)

Diagram

POINT



Overview

- 비동기 트래픽 네트워크 환경 지원
- 유명 해커 그룹 경고에 대응하기 위한 포괄적 웹 사이트 방어
- 이미 업로드 되어 있는 Webshell 파일 접근 확인 및 신규 Webshell 파일 업로드 차단

Deployment

- Bypass TAP 기반 인라인 구성
- 비동기 트래픽 처리를 위한 WAF 시스템간 Async Port 연결

Effectiveness

- 세션 포워딩 기능을 활용한 비동기 트래픽 처리
- 고객사 자체 모의해킹 진단 시 방어율 98% (2%의 경우 진단 툴 오탐)
- 악성 파일 업로드 시도 율 22.8% 감소

Main Policy

- SQL INJECTION, 악성 파일 업로드 탐지, 악성 파일 접근 탐지

THANK YOU

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