PIOLINK

웹방화벽

WEBFRONT-K / WEBFRONT-KS

㈜파이오링크

Optimizing Your Cloud Data Center

CONTENTS

WEBFRONT-K 웹방화벽

WAF **고성능 웹 방화벽**	HTTPS:// **고성능 SSL**	**OWASP Top10,** **국정원 8대 취약점** 대응
V **가상화 지원** (WEBFRONT-KS)	다양한 설치 방식 지원	**관리** 솔루션 (AV2)
GOOD Software **GS**인증	PCI DSS PCI-DSS 준수	ITSCC CC인증

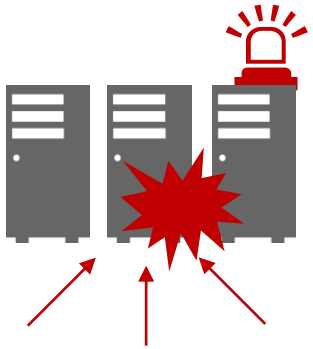
"

WEBFRONT-K 웹방화벽은 웹 서버 앞에 위치해 불법 요청 및 응답을 차단하는 **웹 트래픽에 특화된 보안 솔루션**입니다.

PIOLINK

고성능 웹방화벽 시장 확대

지능적이고 고도화된
해킹 공격 증가



모바일 사용 확대로
게임/포털/금융 등 **동시 접속자 수 급증**

전반적인 산업의 IT 인프라 고도화
10Gbps 지원 장비 요구 증가

PIOLINK

WEBFRONT-K 주요 기능

요청 검사

웹 서버 앞에 위치해 클라이언트의 서비스 요청을 검사하여 정상 트래픽은 통과시키고 인젝션, 인증 및 세션 관리 취약점, 크로스사이트 스크립팅 등과 같은 악의적인 요청 차단

응답 검사 (콘텐츠 보호)

클라이언트 요청에 대한 웹 서비스의 응답을 확인해 신용카드, 계좌번호 등 민감한 정보 유출에 대한 응답을 차단하여 콘텐츠 보호

학습

정상적인 웹 서비스에 대한 요청과 응답을 기준으로 애플리케이션 정보 학습 기능을 제공해 관리자가 다양한 보안 정책을 간단하고 손쉽게 적용할 수 있도록 지원

위장

실제 웹 서비스 URL과 가상 URL을 상호 변환시켜 서버존을 가상화함으로써 클라이언트에게 실제 서버존의 위치와 정보를 숨겨 악의적인 웹사이트 공격 방어

규제 및 인증 준수

국정원 8대 취약점 완벽 대응

국내 각 기관에서 홈페이지 해킹에 많이 악용되었던 취약점 8종

- Directory Listing 취약점
- File Download 취약점
- Cross Site Script(XXS) 취약점
- File Upload 취약점
- Web DAV 취약점
- TechNote 취약점
- ZeroBoard 취약점
- SQL Injection 취약점

OWASP Top 10 취약점 대응

국제 웹 보안 표준 기구가 3년마다 웹 애플리케이션 취약점 중 빈도가 높은 해킹 기법을 정기적으로 발표

- 인젝션
- 인증 및 세션 관리 취약점
- 크로스 사이트 스크립팅
- 취약한 직접 객체 참조
- 보안 설정 오류
- 민감 데이터 노출
- 기능 수준의 접근 통제 누락
- 크로스 사이트 요청 변조
- 알려진 취약점이 있는 컴포넌트 사용
- 검증되지 않은 리다이렉트 및 포워드

PCI-DSS 표준 3.0 준수

Payment Card Industry Data Security Standard(결제 카드 산업 데이터 보안 표준)에 완벽하게 대응

- 보안 네트워크 구축 및 유지
- 카드 소유자 데이터 보호
- 취약점 관리 프로그램 유지
- 강력한 접근 통제 방안 수립
- 정기적인 네트워크 모니터링 및 테스트
- 정보보호 정책 유지

CC인증 EAL4 대응

IT보안인증사무국에서 발행하는 정보보호제품에 대한 인증

PIOLINK

웹 보안 컨설팅으로 체계적 웹방화벽 구축

파이오링크는 WEBFRONT-K 구축 과정에 웹 보안 컨설팅을 진행합니다. (선택 사항)
취약점 분석, 모의해킹, 신규 정책 발굴 등으로 이루어진 웹 보안 컨설팅을 통해
웹방화벽을 구축하고 운영하는 전 과정을 전문적이고 체계적으로 제공하고 있습니다.

웹 취약점 분석

- 웹 취약점 진단 항목 및 방법 선정
- 네트워크 정보 등 데이터 수집
- 시스템 정보 취약점 분석

모의 해킹

- 수집된 취약점 공격
- 단계별 공격 및 우회
- 관리자 권한 획득
- 타 시스템 공격

취약점 공격

공격전이 (2차 공격)

신규 웹 보안 정책 발굴

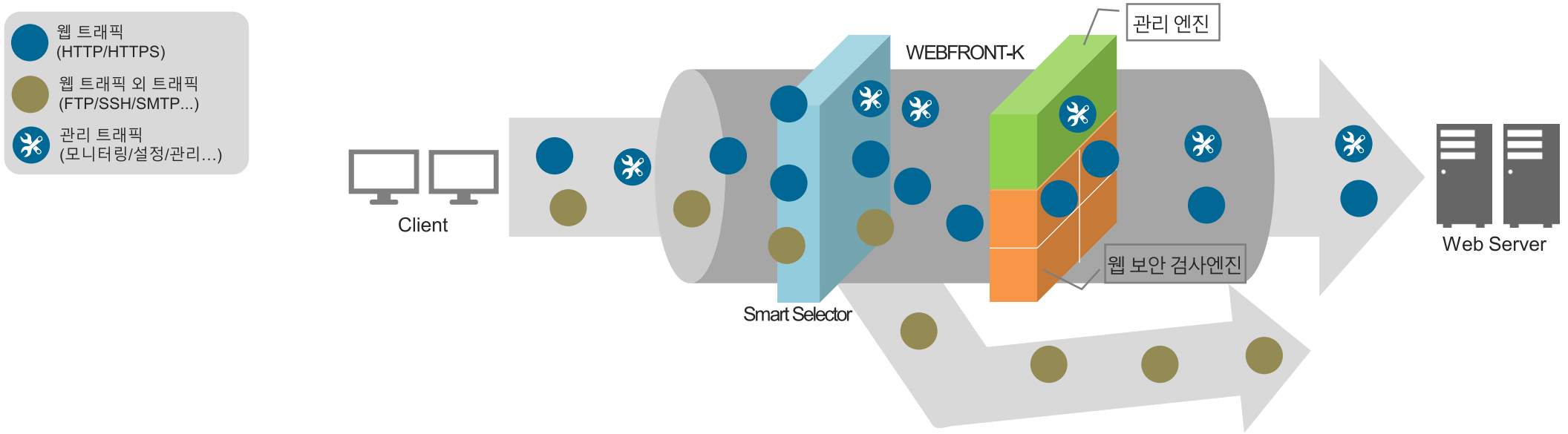
- 모의해킹 결과 세부내역 확인, 대응방안
- 신규 웹 보안 정책 수립 및 적용

WEBFRONT-K 특장점

- 고성능 설계
- 다양한 설치 환경 지원
- 효율적인 관리
- 가상화 솔루션(WEBFRONT-KS)

PIOLINK

고성능 하드웨어 – 웹 보안 전용 플랫폼



외부 유입 트래픽 중 **웹 트래픽만 선별**

- 포트에 유입된 트래픽 중 독자적인 Smart Selector™ 기술로 웹 트래픽만 선별하여 웹 보안 검사 전용엔진으로 전달
- 그 외 트래픽은 서버로 빠르게 전달
- 웹 보안 전용 엔진과 관리 전용 엔진 분리하여 설정/모니터링/업데이트 등과 같은 관리 항목은 관리 전용 엔진으로 전달

웹 보안 검사 엔진에서 **웹 트래픽 보안 검사**

- Smart Selector™ 기술로 선별한 웹 트래픽에 대해서만 보안 검사
- 시스템 자원(CPU/Memory)을 웹 트래픽 보안 검사에 집중할 수 있어 효율성 증가

사용자 정보 기반 **코어 분산 처리**(기술 특허: 10-1019251)

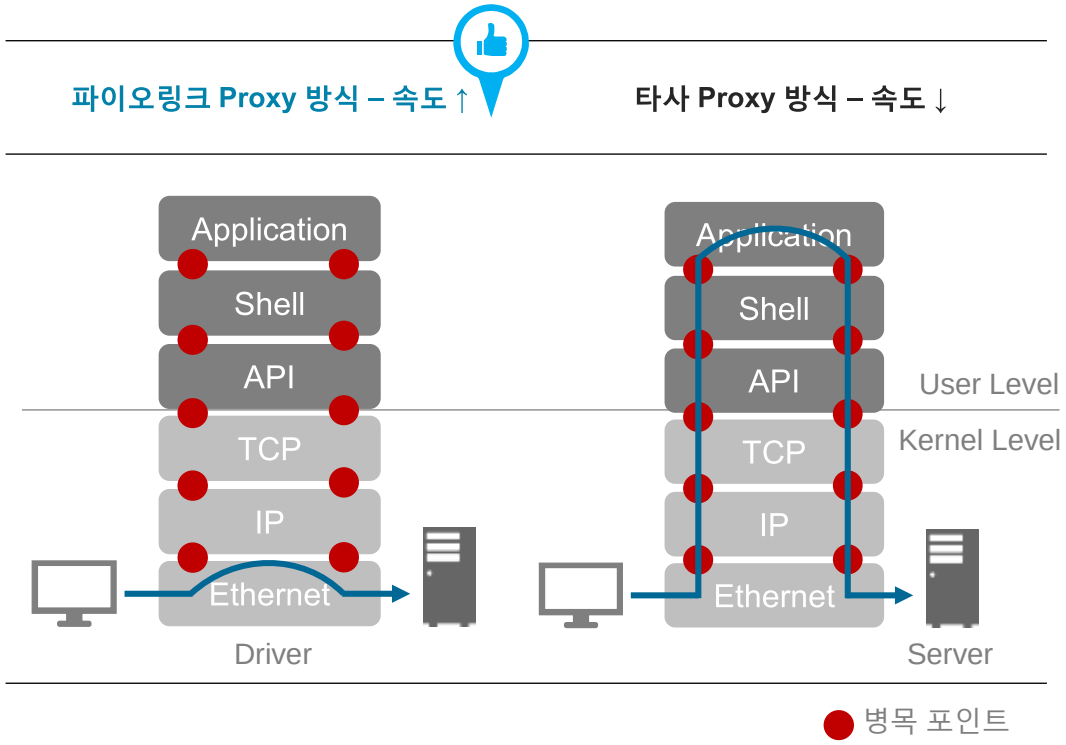
- 웹 보안 전용 엔진에 코어 부하 분산 처리 기술 적용
- 유입 트래픽을 모든 코어에 고르게 분산시켜 웹 트래픽이 특정 코어에 집중되지 않도록 하여 빠른 패킷 처리 보장
- 가장 효율적인 CPU 사용을 구현함으로써 고성능 실현

PIOLINK

고성능 소프트웨어

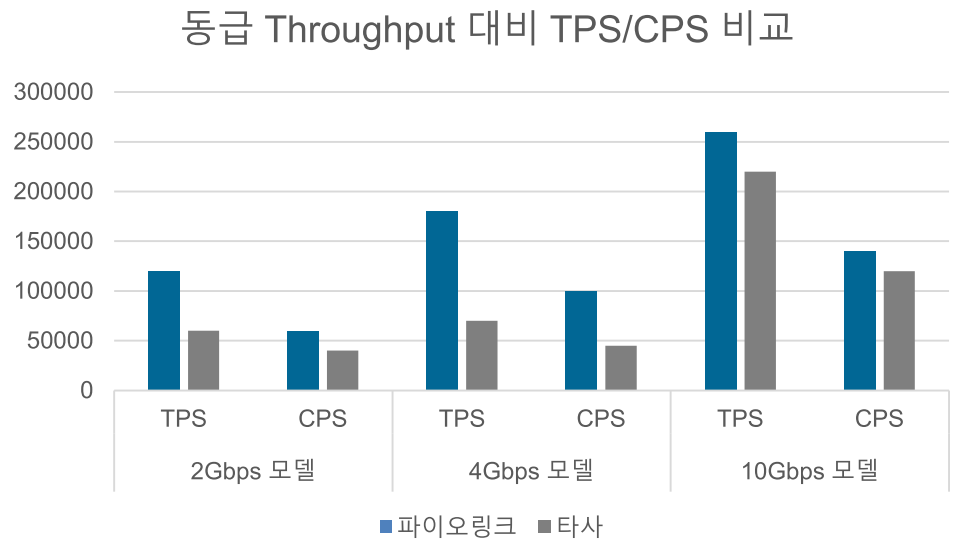
커널 기반 고성능 프락시(기술 특허: 10-0669975)

- 자체 개발 Dynamic Application Proxy(DAP™) 방식
- 복잡한 네트워크 구성을 단순화하여 사용자 레벨과 커널 레벨 간의 병목 포인트 제거
- 대용량, 다양화되는 웹 애플리케이션 서비스를 빠르게 처리



동급 Throughput 대비 CPS/TPS 비교

- 경쟁사 모델 대비 동급 모델 성능 우위
- 특히 2Gbps/4Gbps 모델은 동급 Throughput 모델 대비 TPS 약 130%, CPS 약 86% 우위



고성능 SSL

하드웨어 SSL 처리 방식 - 파이오링크

- 하드웨어 SSL 가속 카드를 장착한 SSL 전용 엔진
- RSA 1024 bit key부터 RSA 4096 bit key 까지 안정적 처리 성능 보장
- EV-SSL 인증 지원
- 중소 고객부터 대형 고객까지 성능과 안정성 인정

RSA Key Size	최대 TPS	최대 CPS	최대 Throughput
1024 bit	50,000 TPS	15,000 CPS	7,000 Mbps
2048 bit	35,000 TPS	7,000 CPS	6,000 Mbps

RSA 2048 bit key 처리시 SSL 성능 비교

- 타사 웹방화벽 SSL 처리 방식은 소프트웨어 기반으로 CPU 사용량이 급증해 RSA 2048 bit key 처리시 심각한 속도 저하 발생

하드웨어 SSL 처리 – 서비스 안정

소프트웨어 SSL 처리 – 서비스 불안정

PIOLINK

다양한 설치 방식 지원 – 기본 모드

In-Line

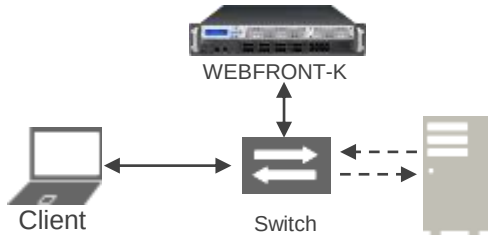
- 일반적인 설치 방식
- 비정상적인 트래픽을 능동적으로 차단하는데 가장 효과적

Reverse Proxy

- 웹방화벽이 웹 서버의 Reverse Proxy 역할로 사용자 요청에 대신 응답
- 외부로부터 웹 서버 보호 목적

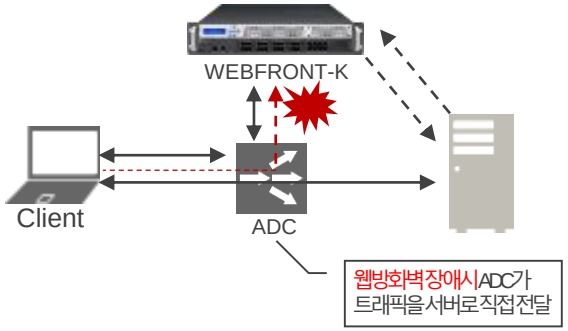
One Armed Reverse Proxy

- 특정 서버에 대한 요청만 웹방화벽이 서버 대신 응답
- 그 외 모든 트래픽은 웹방화벽을 거치지 않고 실제 서버로 직접 전달
- 스위치를 통해 지정된 서버에 해당하는 트래픽만 웹방화벽에 전달함으로써 부하 최소화



Transparent Reverse Proxy

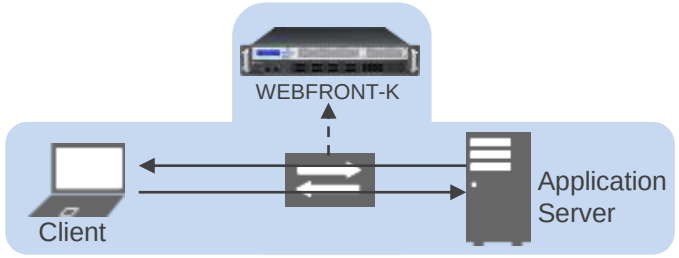
- 웹방화벽이 웹 서버의 Reverse Proxy 역할로 사용자 요청에 대신 응답
- 웹방화벽 장애시 ADC가 트래픽을 서버로 직접 전달해 서비스 가용성 유지 가능
- ADC를 이용해 웹방화벽 확장 용이



다양한 설치 방식 지원 – 확장 모드

Mirroring
실시간 모니터링에 중점

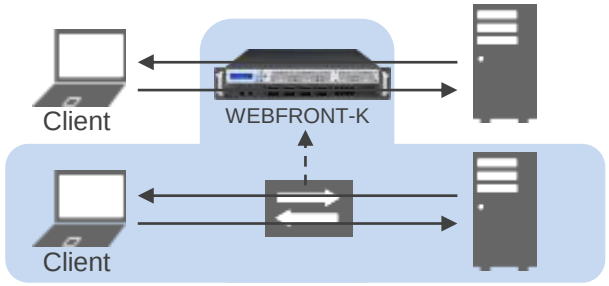
- 스위치를 통과하는 모든 패킷을 웹방화벽에 복사
- 불법 요청에 대한 차단 가능
- 망으로부터 독립적으로 운영
- 웹방화벽을 통한 서비스 장애 및 네트워크 속도 지연 無



Hybrid
Mirroring 과 In-Line 혼합

PIOLINK Only

- 한 대의 웹방화벽으로 미러링, 인라인 두 모드 구현
- 가용성과 보안성을 동시에 만족

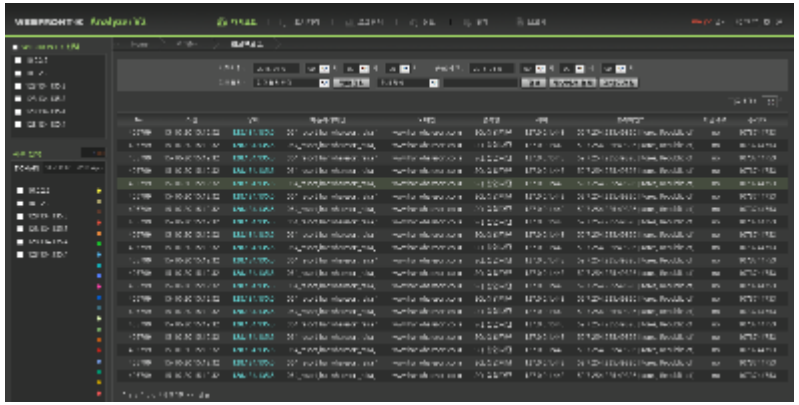


Rapid In-Line
고속 검사 수행 방식

PIOLINK Only

- 프락시 처리를 하지 않는 고속 검사 수행 방식
- 사용자와 서버간 세션 투명성 제공
- 사용자의 요청과 이에 대한 응답에만 관여
- 빠른 속도 구현

통합 관리 솔루션 – Analyzer V2



모니터링 및 이벤트 관리

- 웹 서비스, 바이러스 공격, 보안 결함 등을 실시간으로 모니터링
- 공격자, 공격 유형, 공격 대상, 포트, 프로토콜, 보안 규칙 등을 실시간으로 확인

다양한 통계 보고서 지원

- 공격과 공격 패턴을 모니터링하여 그래프나 테이블 등으로 시각화하여 제공
- 한글 보고서, 기간별 보고서 등을 지원

효율적 로그 분석

- 웹 보안, 네트워크 보안, 접근, 감사, 시스템 등 다양한 로그 수신 및 분석
- 웹 공격 패킷 발생지, 웹 공격 유형, 공격 근거 확인 가능

실시간 보안 경보

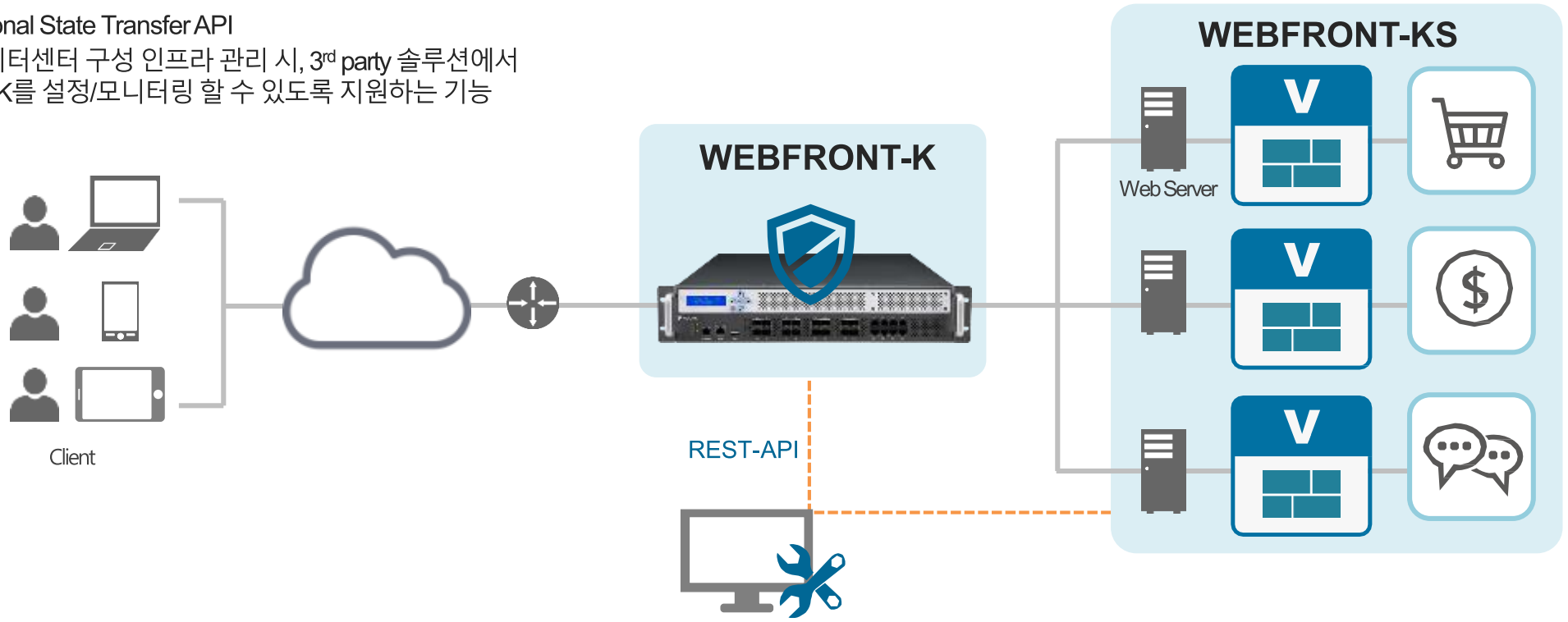
- 사용자가 정의한 보안 정책에 위반되는 상황 발생시 이메일로 알림

PIOLINK

유연한 서비스 확장 및 관리

PREST API™

- Representational State Transfer API
- 클라우드 데이터센터 구성 인프라 관리 시, 3rd party 솔루션에서 WEBFRONT-K를 설정/모니터링 할 수 있도록 지원하는 기능

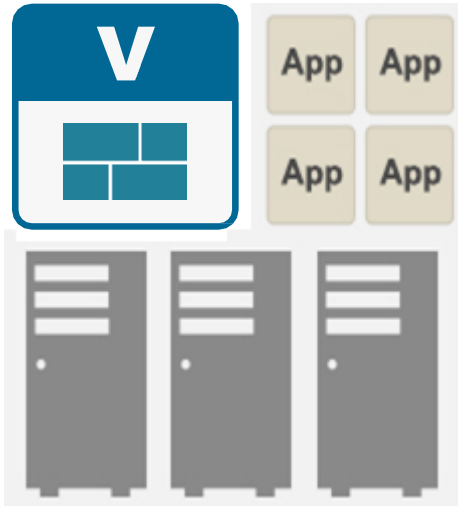


PIOLINK

WEBFRONT-K 가상화

WEBFRONT-KS

- 웹방화벽 기능을 범용 서버(x86)에 설치할 수 있는 소프트웨어 애플리케이션
- 빈번한 가상 서버의 생성/삭제 등 빠른 비즈니스 서비스 요구에 대응
- 서비스 단위로 웹방화벽 장애 포인트 분산
- 전용 어플라이언스에 비해 구매, 설치, 유지 등에 대한 경제적 부담 절감
- 서버, 스토리지 및 웹방화벽 자원까지 완벽히 가상화된 자원 풀(Resource pool)로 구성하는 소프트웨어 정의 데이터센터, 클라우드 서비스 센터 구축의 기반



구축 사례 및 스펙

- 온라인 증권 서비스 보안
- 그룹사 전체 웹보안 서비스 보안
- 웹 보안과 로드밸런싱 활용
- 제품 스펙

PIOLINK

온라인 증권 서비스 보안

“

증권 서비스를 위한 빠른 SSL 처리 성능
SSL에 숨은 공격까지 차단

- 기존 웹방화벽의 SSL 성능이 충분하지 못해 WEBFRONT-K로 교체
- 고성능 WEBFRONT-K는 서비스 지연 없이 안정성과 보안성을 보장
- RSA 2048 bit 환경에서도 SSL 처리시 매우 안정적
- 수시로 변경하는 보안 정책 적용이 쉽고 유연함

그룹사 전체 웹 서비스 보안

“

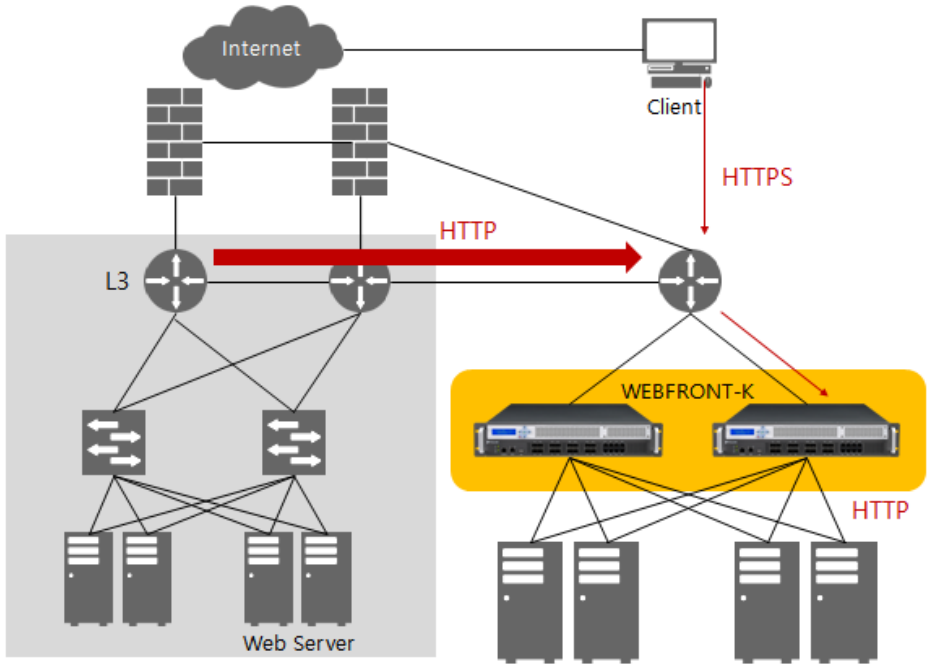
홈쇼핑, 티켓 예매, 택배 등 대규모 트래픽 발생 환경에서 **고성능 보안과 다양한 구성 방식 지원**

- 방송, 유통, 엔터테인먼트, 운송, 식음료 등 각 사업에 대한 웹 서비스 보안 담당
- 대용량 트래픽 처리를 위한 10G 이상 고성능 웹방화벽 도입
- 미러링, 인라인 등 다양한 구성 방식으로 가용성을 높임
- 정책과 공격 탐지 패턴을 쉽게 변경할 수 있어 탄력적으로 운영
- 파이오링크 웹방화벽 만족도가 높아, 교체 시기에 재 도입

웹 보안과 로드밸런싱, 1석 2조 활용

웹 서버의 보안과 가용성을 한번에 해결
데이터센터 효율성 증대

- 고객은 장비 구매 부담을 줄이고, 운영면에서 가용성과 보안을 한번에 해결하기 원함
- WEBFRONT-K는 파이오링크의 고성능 스위칭 기반 애플리케이션 전송 기술이 적용되어 있음
- 로드밸런서 추가 구매 없이 웹방화벽으로 L7 부하분산, 웹보안, 오프로딩 등 수행
- SSL 가속 모듈을 장착해 이중화로 구성, 끊김 없이 안정적인 웹 보안 서비스 실현



PIOLINK

구축사례 모음

금융

SSL 암호화 트래픽에서도 안정적인 웹 보안을 보장받고 있습니다.

국가교통정보센타
국가정보원
도로교통공사
서울시청
경기평생교육진흥원
경북도청
군포시청
나주시청
논산시청
대한상공회의소
문화재청
부산광역시 상수도사업본부
부산광역시 소방안전본부
엔비레즈
웅진홀딩스
인천도시가스

부산북구청
부산수영구청
부산진구청
사이버민족방위사령부
서울시복지재단
성북구 도시관리공단
세종연구소
소방시설협회
순천시청
안전보건공단
여수시청
영상물등급위원회
영암군청
운전면허관리단
유네스코아태무형유산센터
의정부경전철
인천 아시안게임조직위
인천부평구청
전남영광군청
정보사회진흥원
농민신문사
뉴데일리

대학

수강신청처럼 트래픽이 한꺼번에 몰려도 성능과 보안 문제가 없습니다.

제주해양수산관리단
제천시청
창원시청
충남도청
충북음성군청
충주시청
한국수력원자력
한국수력원자력 중앙연구원
한국원자력통제기술원
한국전력거래소
부산교통공사
LG유플러스
더존
아시아나IDT
로젠택배

경기도 교육청
전라남도교육청
한국교육개발원
건양사이버대학교
경기도 가평교육지원청
경기도 교육연수원
경기도 김포교육지원청
경기도 부천교육지원청
경기도 시흥교육지원청
경기도 안산교육지원청
경기도 안성교육지원청
경기도 여주교육지원청
경기도 연천교육지원청
골든브릿지증권
공평저축은행
교보생명
국민연금
나라사랑카드
대한생명
동부CNI
동원테크
금호타이어

병원/기업

웹 보안 적용이 쉽고, 고객 기술 지원도 만족스럽습니다.

경기도 화성오산교육지원청
계명대학교
동국대학교 경주캠퍼스
동남권원자력병원
부산학생문화회관
부천대학교
서강대학교
에이앤디신용정보
한화손해보험
현대카드 캐피탈
매일신문
미니스톱
서울우유

통신/쇼핑

웹 보안 뿐만 아니라 네트워크 성능까지 우수합니다.

인하공업전문대학
제주영어교육도시
조선대학교
중원대학교
진천도서관
창원경상대학교병원
한국교육학술정보원
포스코터미널
하림
한경닷컴
한국건강기능식품협회
금성출판사
바로크레디트
서울디지털대학교
세종대학교
수원과학대학
순천대학교
안산대학교
안양대학교
버거킹
부광약품
삼립식품

일진그룹
자동차연구원
제이티아이
커스데이타넷
크라운제과
고속버스운송사업조합
NH투자선물
SC스탠다드캐피탈
고려신용정보
GE엔터테인먼트
KBS
KFC
SBS
SK가스

PIOLINK

WEBFRONT-K 스펙

WEBFRONT	K1600	K2200	K2400	K4200	K4400	K8200
Ethernet Ports(Total)	16	24		16 or 24		
- 10GbE Fiber (SFP+)	-	-	-	16	16	16
- 1GbE Fiber (SFP)	8	16	16	-	-	-
- 1GbE Copper	8	8	8	-	-	-
Module Extension (Optional)	-	-		Select one from · 8 x 1GbE Fiber (SFP) or · 8 x 1GbE Copper or · 1 pair x 1/10GbE Fiber Bypass or · 1 pair x 1GbE Copper Bypass		
Throughput	600 Mbps	2 Gbps	4 Gbps	10Gbps	12 Gbps	20 Gbps
Concurrent Session	1.2 M	4 M	8 M	12 M	20 M	20 M
CPS / TPS	30,000 / 50,000	60,000 / 120,000	100,000 / 180,000	140,000 / 250,000	200,000 / 320,000	230,000 / 360,000

- **바이패스 모델**

WEBFRONT	K1600(B)	K2200(B)	K2400(B)	K4200(B)	K4400(B)	K8200(B)
			상세 스펙은 위와 동일			
Bypass Ports	· 2 pairs x 1GbE Fiber or · 2 pairs x 1GbE Copper	· 2 pairs x 1GbE Fiber or · 2 pairs x 1GbE Copper or · 1 pair x 1GbE Fiber, 1 pair x 1GbE Copper		2 pairs x 10GbE Fiber		

- **가상화 모델**

WEBFRONT	KS100	KS500	KS1000	KS6000
Throughput	100 Mbps	500 Mbps	1 Gbps	6 Gbps

주요 기능

요청 검사

- 애플리케이션 접근 제어
- 폼 필드 무결성 검사
- 폼 필드 형식 검사
- 쿠키 무결성 검사
- 쿠키 형식 검사
- 과다 요청 검사
- 업로드 검사
- 다운로드 검사
- Slowloris 차단
- 금칙어 차단
- 신용카드 정보 유입 차단
- 버퍼 오버플로우 차단
- SQL 삽입 차단
- 스크립트 삽입 차단
- 검사 회피 차단
- 요청 형식 검사
- 디렉토리 리스팅 차단
- 인클루드인젝션 차단
- 주민번호 유입 차단
- HTTP Post 공격 차단
- WISE Filter™

응답 검사

- 웹 변조 방지
- 신용 카드 정보 유출 차단
- 주민 등록 번호 유출 차단
- 계좌 번호 유출 차단
- 응답 형식 검사
- 코드 노출 차단
- WISE Filter™

학습

- 접근 제어 학습
- 폼 필드 학습
- URL 구조 학습

위장

- URL 변환
- 부적절한 에러 처리
- 서버 정보 위장

WEBFRONT-K 사진

K1600

K2200 / K2400

K4200 / K4400 / K8200

K1600(B)

K2200(B) / K2400(B)

K4200(B) / K4400(B) / K8200(B)

*(B) 는 바이패스(Bypass) 모델입니다.

K1600, K1600(B)

K2200, K2200(B) / K2400, K2400(B) /
K4200, K4200(B) / K4400, K4400(B) / K8200, K8200(B)