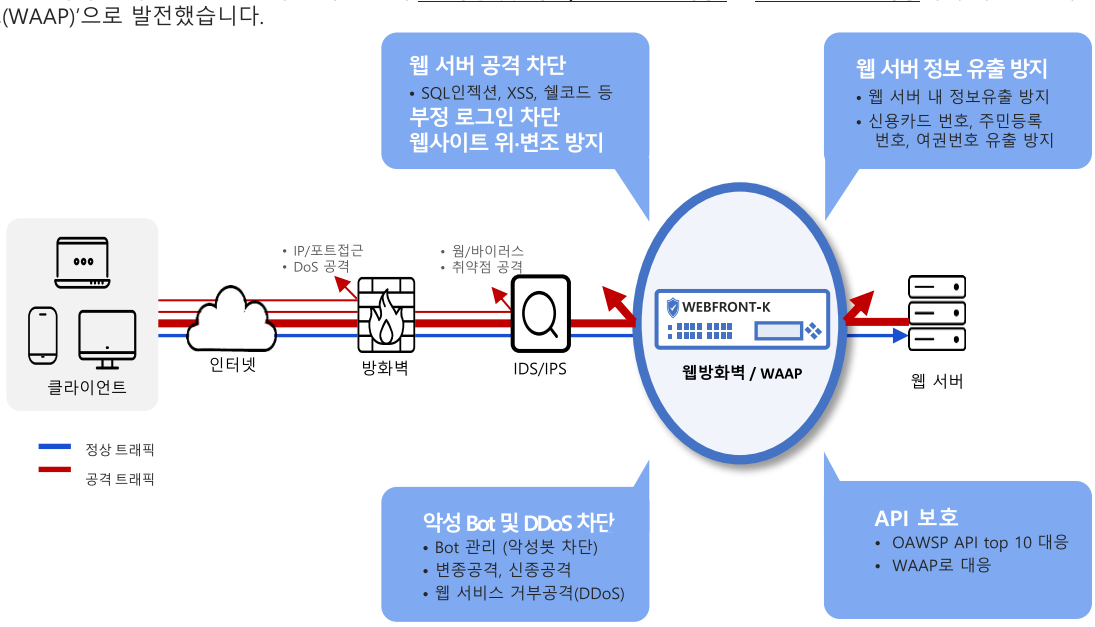
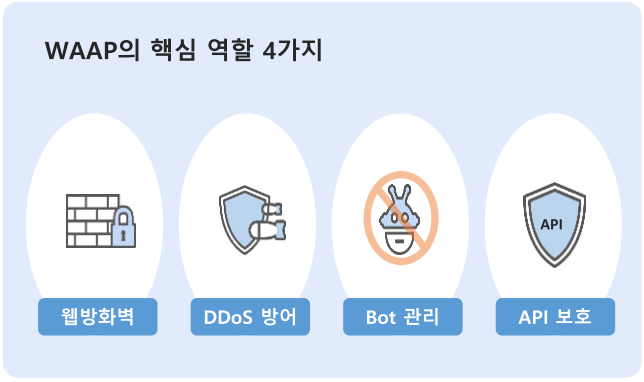
웹방화벽: 웹 보안부터 API 보안까지

- 웹방화벽은 방화벽, IPS 등과 달리 OSI 7 layer(애플리케이션 영역)에 해당하는 HTTP/HTTPS 트래픽 공격을 차단합니다.
- 웹방화벽은 **▲웹 서버 공격 차단**, **▲ 웹 서버 내 정보 유출 방지**, **▲ 부정 로그인 방지**, **▲ 웹사이트 위·변조 방지** 등 기본적인 웹 보안을 제공합니다.
- 최신 웹방화벽은 새로운 웹 환경에 맞게 발전해 **▲ 악성 봇 차단, ▲ DDoS 대응** 및 **▲ API 보호 기능**이 추가된 '웹 애플리케이션 및 API 보호(WAAP)'으로 발전했습니다.



WAAP으로 발전한 WEBFRONT-K

WEBFRONT-K는 **API 보호 기능이 추가된 웹방화벽**으로, **웹 애플리케이션 및 API 보호(WAAP**, Web Application and API Protection) 솔루션으로 발전했습니다.



애플리케이션 개발에 API 사용이 보편화되면서 API 취약점을 노린 공격이 증가하고 있습니다. **API를 통해 민감한 정보가 오가는 새로운 웹 환경에서 레거시 웹방화벽만으로는 효과적으로 보호할 수 없기 때문에 API 보호 기능이 추가된 웹방화벽 및 WAAP 도입은 필수**입니다.

WEBFRONT-K는 자체 개발 플랫폼 기반으로 국내 최고 성능을 자랑하며, 사용자 행위 기반 탐지를 포함한 지능형 탐지 기술을 적용해 신종 웹 공격에 대응하는 웹방화벽이자 WAAP입니다.

API 보호 기술 적용 웹방화벽 국내 최초!

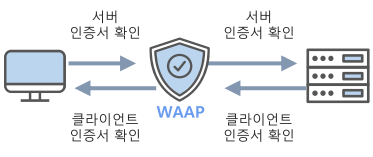
WEBFRONT-K

API 보호를 위한 핵심 기술 6가지 적용

- 파이오링크 WEBFRONT-K는 **국내 최초로 API 보안 기술을 적용한 웹방화벽/WAAP**입니다.

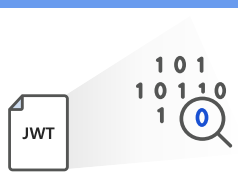
API 보안을 위한 핵심 기술 6가지

양방향 TLS(mTLS)

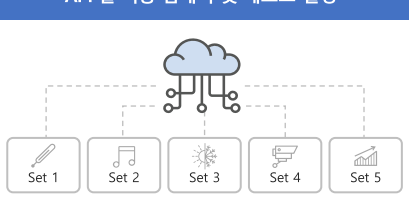


식별정보 클로킹

API 토큰 인증 및 무결성 검사

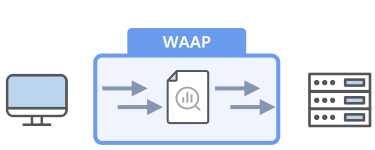


API 별 허용 임계치 및 메소드 설정



JSON 응답 클로킹

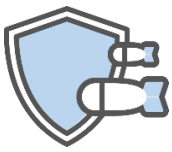
JSON 요청 필드 검사



WAAP의 핵심 역할 4가지 지원

- WEBFRONT-K는 웹 해킹/DDoS/봇 공격 등 **웹 애플리케이션 보호** 기능에 새롭게 **API 보호 기능이 추가**되었습니다.
- **API 보호 기능까지 포함하는 웹방화벽이 WAAP**입니다.

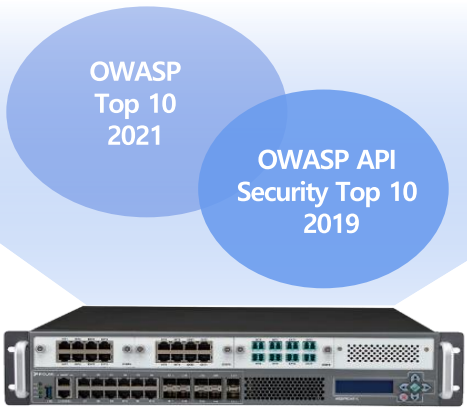
웹방화벽(WAF)



DDoS 방어

Bot 관리

API 보호



Web Application Firewall

API 보안을 지원하는 웹방화벽

파이오링크 WEBFRONT-K는 설계부터 차별화된 웹 보안 플랫폼에 다양한 탐지기술이 적용된 **국내 최고 성능 웹방화벽·WAAP**입니다.

국내 최고 성능 웹방화벽
자체 설계한 웹 보안 최적화 플랫폼 적용

국내 최초 API 보호 기능 추가 웹방화벽
웹 애플리케이션 및 API 보호(WAAP)

애플리케이션 운영 자동화 지원
Full REST-API, ANSIBLE

관리 편의성 향상
GUI 기반 관리콘솔, 웹 보안 로그분석/리포트 제공

SSL/TLS 복호화 및 미러링 지원
복호화 트래픽을 타 위협분석 장비로 전달해 차단 지원

C-TAS 연동을 통한 최신 위협 대응
KISA 제공 최신 위협 IP를 매일 업데이트해 탐지·차단

설계부터 다른 고성능

- 웹 보안 최적화를 위해 하드웨어부터 소프트웨어까지 **파이오링크가 직접 설계 / 개발**합니다.

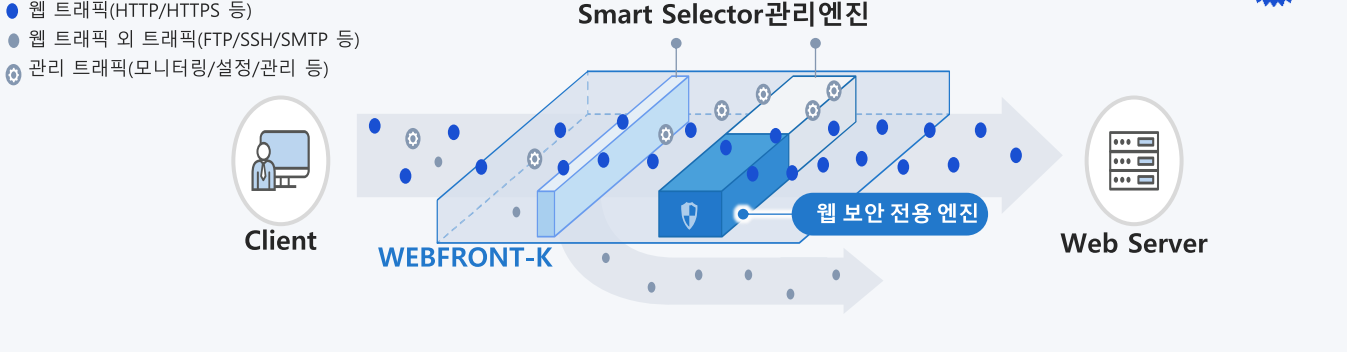
웹 트래픽만 선별 처리

- 독자적인 Smart Selector™기술이 장비 포트에 적용
- 유입된 트래픽 중 웹 트래픽(HTTP, HTTPS)만 선별하여 [웹 보안 엔진]으로 전달
- 웹 트래픽 중에서 설정/모니터링/업데이트 등과 같은 관리 항목은 [관리 엔진]으로 전달
- 웹 트래픽이 아닌 FTP, SSH, SMTP 등은 [서버]로 바로 전달하여 리소스 사용 극대화

코어 부하분산 패킷 처리

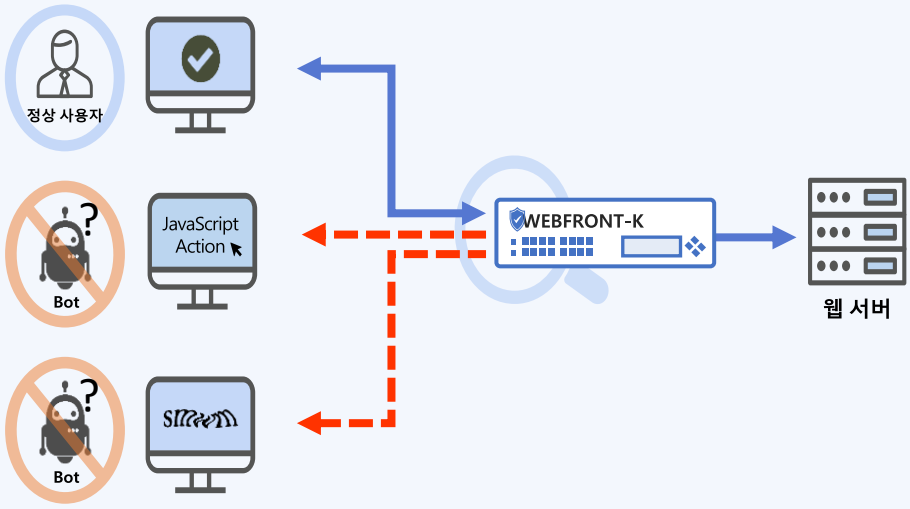
- 웹 트래픽 탐지 시, 특정 CPU 코어에 집중되지 않도록 부하 분산하여 빠르게 패킷 탐지
- 가장 효율적인 CPU 사용을 구현함으로써 고성능 웹 보안 제공
- 사용자 정보 기반 코어 분산 처리 기술 특허 보유 (등록번호:10-1019251)

PIOLINK ONLY

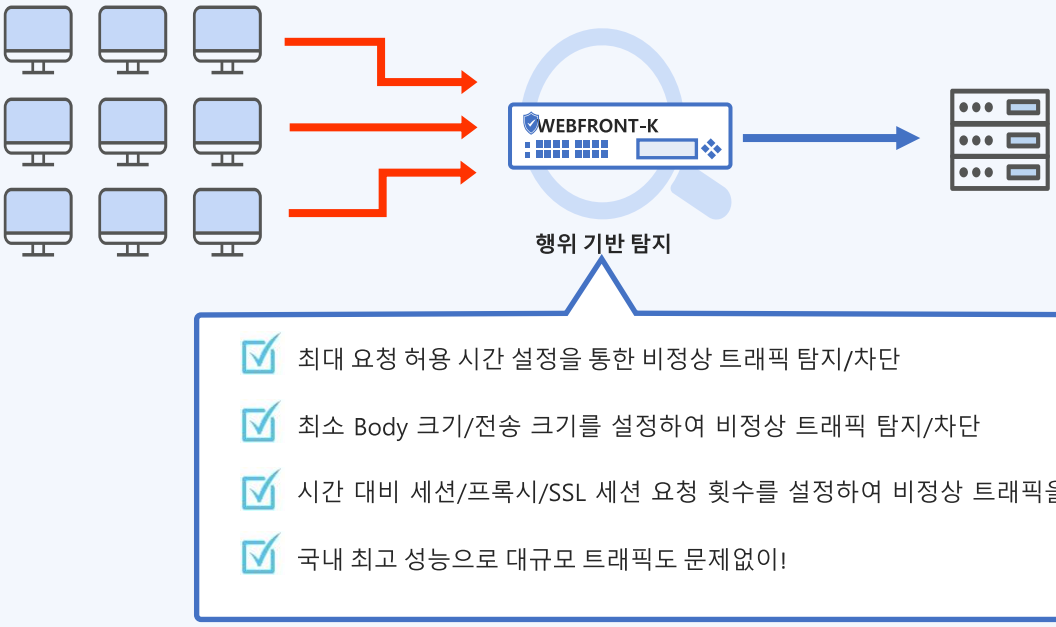


Bot 차단을 위한 CAPTCHA, 자바스크립트 인증 적용

- 부적절한 Bot에 대한 제어를 위하여 **CAPTCHA 및 JavaScript** 액션 기반 인증 기술을 적용했습니다.



DDoS 대응을 위한 다양한 행위 기반 탐지 적용



- 최대 요청 허용 시간 설정을 통한 비정상 트래픽 탐지/차단
- 최소 Body 크기/전송 크기를 설정하여 비정상 트래픽 탐지/차단
- 시간 대비 세션/프록시/SSL 세션 요청 횟수를 설정하여 비정상 트래픽을 탐지/차단
- 국내 최고 성능으로 대규모 트래픽도 문제없이!

다양한 설치 방식 지원

Inline, Out-of-Path 외 다양한 설치방식을 지원합니다.

Mirroring:
실시간 모니터링에 중점

- 스위치를 통과하는 모든 패킷을 웹방화벽·WAAP에 복사
- 불법 요청에 대한 차단 가능
- 망으로부터 독립적으로 운영
- 웹방화벽을 통한 서비스 장애 및 네트워크 속도 지연 없음

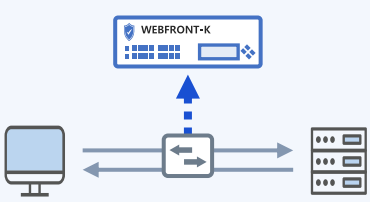
Hybrid:
Mirroring 과 In-Line 혼합

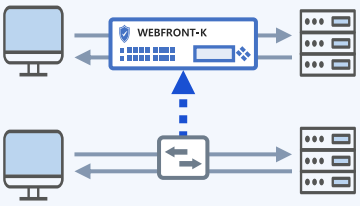
PIOLINK ONLY

- 한 대의 웹방화벽·WAAP으로 미러링, 인라인 두 모드 구현
- 가용성과 보안성을 동시에 만족

Rapid In-Line:
고속 검사 수행 방식

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

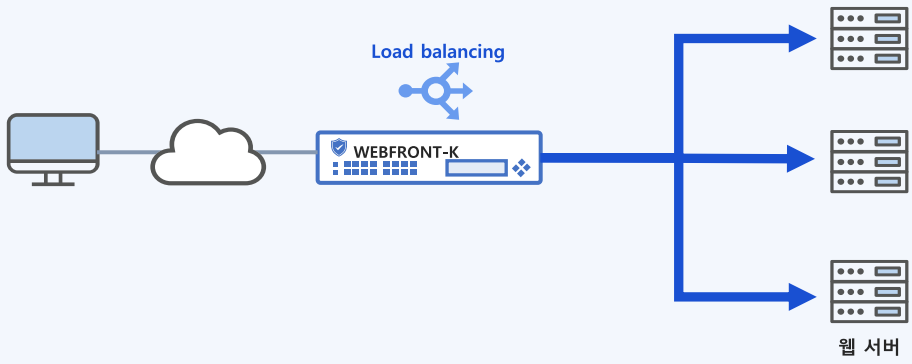




부가 기능 – 트래픽 부하분산

LB

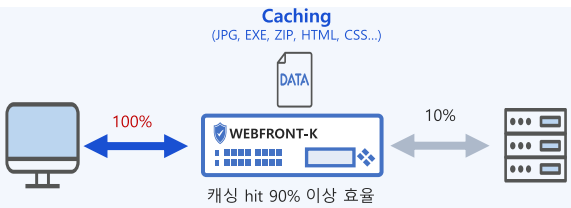
- 동일한 웹 애플리케이션을 운용하는 다수의 웹 서버에 트래픽을 균형 있게 전달하는 로드밸런싱을 지원
- 서버의 로드율 증가, 부하량, 속도저하 등을 고려해 트래픽 폭주에도 서비스 안정성 제공
- 별도의 로드밸런서(ADC, L4/L7 스위치)를 설치하지 않아도 돼 투자 비용 절감



부가 기능 – 캐싱 / 압축 / QoS

캐싱

- 사용자가 자주 요청하는 콘텐츠를 지정하여 서버 대신 저장
- 사용자 요청시 서버 대신 응답하기 때문에 서버로 직접 전달하는 트래픽을 감소시키고 사용자에게 더 빠른 서비스 제공

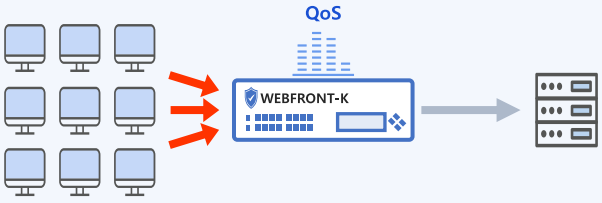


압축

- 이미지 등 주요 콘텐츠 파일을 압축하여 사용자에게 전송

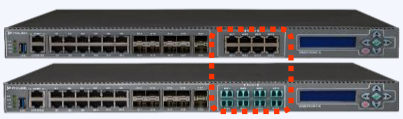
QoS

- 서버로 향하는 과다한 트래픽 폭주를 막기 위해 사용자 요청 웹 트래픽 대역폭에 대해 임계치 지정
- CPS 제한, 동시세션 제한, BPS 제한 등
- DDoS 차단, 서버 보호 및 효율적인 네트워크 유지



제품 사진

K1800

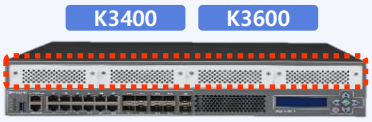


K1800 (후면)

- 바이패스 타입 선택

K3200 K4600

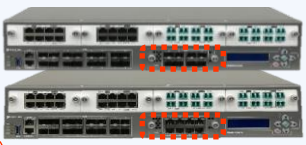
K3400 K3600



K3400 / K3600 (후면)

- 바이패스 모듈 최대 4개 선택 (Fiber / Copper)

K5600 K5620 K5800



K5600 / K5800 (후면)

- 바이패스 모듈 최대 4개 선택 (Fiber / Copper)
- 이더넷 포트 모듈 선택 (1GbE / 10GbE / 40GbE)

K8600

K8600 (후면)

- 바이패스 기본 및 추가 선택 (Fiber)