

WEBFRONT-K

Web Application Firewall



WEBFRONT-K Web Application Firewall

국내 최고 성능 웹방화벽으로 금융, 포털, 공공, 기업 등 다양한 서비스 규모와 산업에서 웹 보안을 인정받고 있습니다.

웹방화벽은 웹 서버와 웹 서비스 사용자 사이에서 요청 검사와 응답 검사를 통해 웹 서버 및 데이터를 보호하는 웹 전용 보안 솔루션입니다.

파이오링크 웹방화벽인 WEBFRONT-K는 웹 보안에 최적화된 전문 플랫폼을 기반으로 웹 트래픽만을 선별하여 보안 검사를 수행하는 웹 보안 전용 엔진과 CPU 성능을 최대한으로 활용할 수 있는 코어 부하 분산 기능을 탑재한 고성능 웹방화벽입니다.

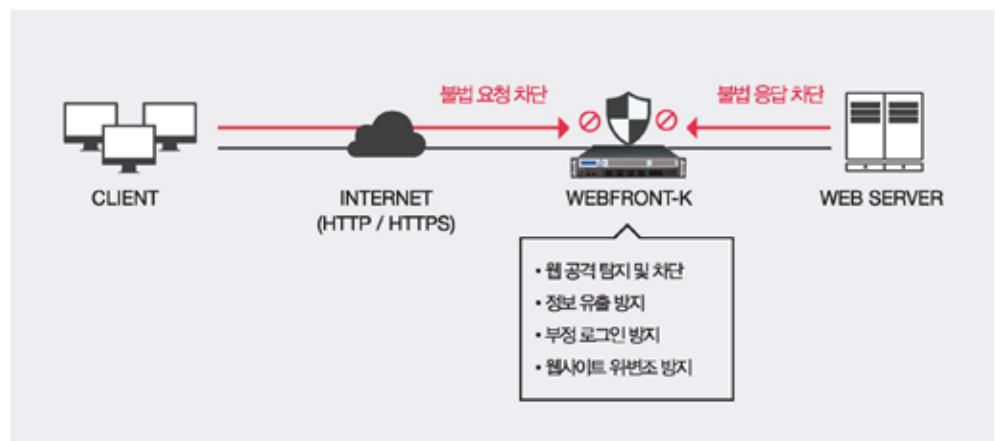
 <p>국내 최고 20Gbps 동시세션, CPS, TPS 등에서도 국내 최고</p>	 <p>국내 최고 SSL 처리성능 RSA 2048bit key 환경</p>	 <p>OWASP Top10, 국정원 8대 취약점 대응</p>
 <p>가상화 지원 (WEBFRONT-KS)</p>	 <p>다양한 설치 방식 지원</p>	
		

웹보안

OWASP Top10,
국정원 8대 취약점 완벽 대응

WEBFRONT-K는 웹 애플리케이션 서비스 보안에 최적화된 제품으로 고객에게 신뢰할 수 있는 웹 보안을 제공합니다. 웹 서버 앞에 위치해 사용자의 서비스 요청과 서버의 응답을 검사하여 정상 트래픽은 통과시키고 인젝션, 인증 및 세션관리 취약점, 크로스사이트 스크립팅 등과 같은 악의적인 요청은 차단합니다. 그리고 신용카드, 계좌번호 등 민감한 정보 유출에 대한 응답도 차단합니다.

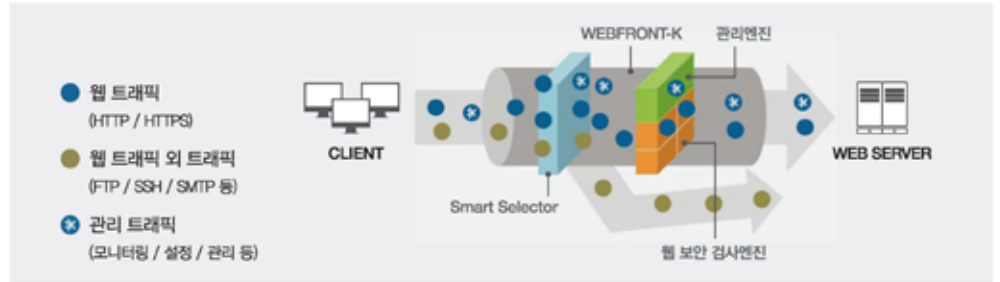
애플리케이션 정보 학습 기능을 제공해 관리자가 다양한 보안 정책을 간단하고 손쉽게 적용할 수 있도록 돕습니다. 또한, 위장 기능을 통해 클라이언트에게 실제 서버 존의 위치와 정보를 숨겨 악의적인 웹 사이트 공격을 막습니다.



고성능 강점

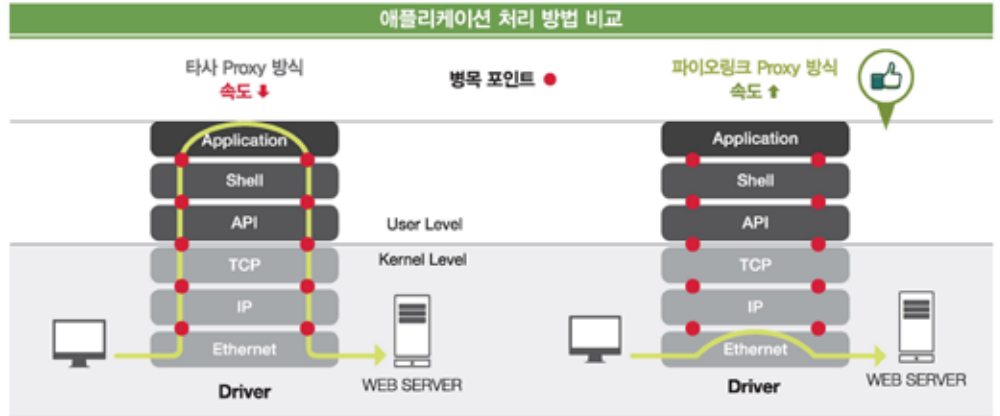
자체 개발 하드웨어로 웹 트래픽 처리 및 리소스 사용 극대화

WEBFRONT-K의 고성능은 포트에 유입된 트래픽 선별부터 시작됩니다. 독자적인 Smart Selector 기술로 오직 웹 트래픽만 선별하고 나머지 패킷은 빠르게 서버로 전달합니다. 이렇게 선별된 웹 트래픽은 웹보안 전용 엔진을 통해 보안검사가 이루어집니다. 이때 설정, 모니터링, 업데이트 등과 같은 관리 부분은 관리전용 엔진에서 별도로 처리하기에 보안검사에만 집중할 수 있습니다. 게다가 웹보안 전용 엔진은 코어 부하분산처리 기술이 적용되어 웹 트래픽이 특정 코어에 집중되지 않아 CPU를 효율적으로 사용함으로써 고성능을 실현합니다. 이에 반해 타 웹방화벽은 범용 어플라이언스에 보안 소프트웨어를 올린 방식이라 구조적으로 시스템 성능의 한계가 있을 수 밖에 없습니다.



병목 포인트 제거로 애플리케이션 처리를 빠르게

특히 받은 파이오링크의 고성능 애플리케이션 프락시 기술(DAP: Dynamic Application Proxy)은 복잡한 네트워크 스택 구성을 단순화하여 사용자 레벨과 커널 레벨 간의 병목 포인트를 제거합니다. 대용량, 다양화 되는 웹 애플리케이션 서비스를 빠르게 처리하는 독자 기술로 타사에 비해 월등히 빠른 성능을 자랑합니다.

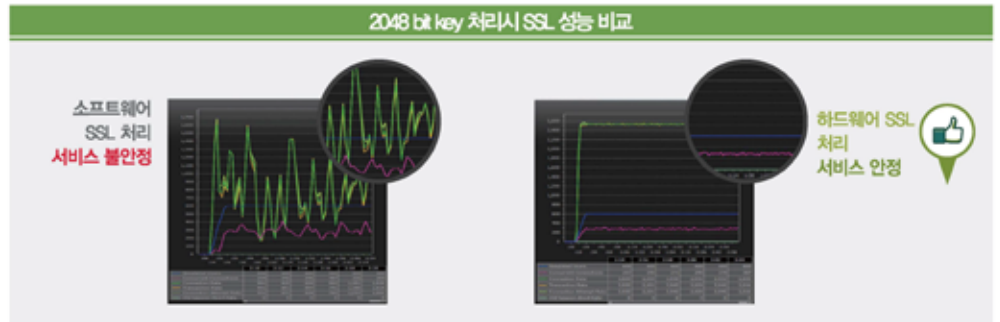


하드웨어 SSL 카드로 국내 최고의 성능

SSL 백서



정보 보호를 위해 금융, 포털, 온라인 상거래 등 많은 웹사이트가 SSL 암호화 통신을 하고 있습니다. 웹방화벽은 웹서버 앞에서 SSL 암호화 및 복호화를 수행하고, 여러 서버가 직접 관리해야 하는 인증서 및 키를 대신 관리하면서 서버의 성능이 저하되지 않도록 합니다. 파이오링크 WEBFRONT-K는 하드웨어 SSL 전용 가속카드를 통해 SSL을 빠르게 처리합니다. 타웹방화벽의 소프트웨어 SSL에서는 감당할 수 없는 높은 키 사이즈(key size)까지 안정적으로 처리합니다. 최근 웹 사이트는 보다 안전한 SSL 통신을 위해 RSA 2048bit key 사용을 권장하고 있으며, 추후 더 높은 키 사이즈가 요구되더라도 파이오링크는 자체적인 하드웨어 설계로 서버의 안정성을 보장해 드릴 것입니다.



다양한 설치 방식

사용자는 설치 및 관리가 편리한 'In-Line', 웹 서버 보호가 용이한 'Reverse Proxy', 웹방화벽 부하를 최소화 하는 특정 서버 지정 Reverse Proxy 방식인 'One Armed Reverse Proxy', ADC를 이용해 웹방화벽 확장이 용이한 'Transparent Reverse Proxy' 등 자사의 네트워크 환경에 맞춘 설치 방식을 선택할 수 있습니다. 위의 기본 방식 외에도 WEBFRONT-K는 아래와 같이 독자적인 설치 방식을 지원합니다. 특히, 금융, 포털, 게임 등 가용성에 중점을 둔 서비스에 적합한 지원 모드를 선택해 설치할 수 있어 안정성이 보장됩니다.

Mirroring

실시간 보안보다 모니터링에 중점을 둔 설치 방식

- 스위치를 통과하는 모든 패킷을 웹방화벽에 복사
- 망으로부터 독립적으로 운영되기 때문에 웹방화벽을 통한 서비스 장애와 네트워크 속도 지연 없음.

Hybrid

Mirroring모드와 In-Line 모드의 혼합형 설치 방식

PIOLINK ONLY

- 한 대의 웹 방화벽으로 미러링, 인라인 두 모드 구현 가능
- 가용성과 보안성을 동시에 만족

Rapid In-line

프락시 처리를 하지 않는 고속 검사 수행 방식

PIOLINK ONLY

- 사용자와 서버간 세션 투명성을 제공함
- 사용자의 요청과 이에 대한 응답에만 관여해 빠른 속도 구현

Virtual Appliance

범용 서버(x86) 설치 방식

- 빠른 비즈니스 요구에 대응
- 서비스 단위로 웹방화벽 장애 포인트 분산
- 전용 어플라이언스에 비해 구매, 설치, 유지 등 경제적 부담 절감

보안 분석 및 통계 관리 (Analyzer V2)

Analyzer V2는 여러 대의 WEBFRONT-K를 한 곳에서 모니터링하는 분석 솔루션입니다. Analyzer V2는 장비의 보안 상태를 실시간으로 모니터링하여 경보를 발생시키거나, 로그 정보를 분석해 사용자가 향후 보안 대책 수립에 반영할 수 있도록 다양한 보고서를 제공합니다. 사용자는 Analyzer V2를 통해 여러 대의 장비를 효과적으로 관리할 수 있습니다.



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 모니터링하고 이를 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 패턴 발생지, 웹 공격 유형, 공격 근거 등 확인 가능

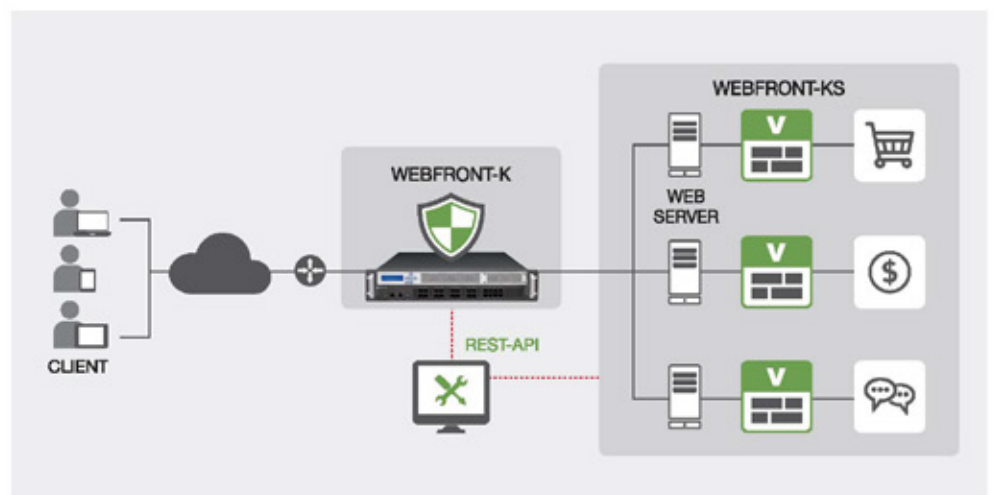
실시간 보안 경보

- 사용자가 정의한 보안 정책에 위반되는 상황 발생시 이메일로 알림

유연한 관리




PREST API™

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






스펙 및 주요 기능

WEBFRONT-K 기본 모델

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		
Memory(RAM)	4 GB	8 GB	16 GB	24 GB	48 GB	48 GB
SSD / HDD	160 GB / 1TB	160 GB / 1 TB (up to 2TB, optional)				
CPU	1 x 2-core	1 x 4-core	1 x 4-core	1 x 6-core	2 x 6-core	
Power Consumption	100 W	156 W	156 W	232 W	257 W	257 W
Power Input	100-240VAC, 50-60 Hz (free voltage) / Dual Power (hot-swappable)					
Dimension(WxDxH,mm)	428 x 566 x 44 (1RU)			428 x 606 x 88 (2RU)		
Weight	8.9 kg	14 kg	14 kg	14.6 kg	15.1 kg	15.1 kg
Throughput	600 Mbps	2 Gbps	4 Gbps	10 Gbps	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

WEBFRONT-K(B) 바이패스 모델

WEBFRONT	K1600(B)	K2200(B)	K2400(B)	K4200(B)	K4400(B)	K8200(B)
						
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	-	-	-
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	
Module Extension (Optional)	-	-	-	Select one from - 8 x 1GbE Fiber (SFP) or - 8 x 1GbE Copper or - 1 pair x 10GbE Fiber Bypass or - 1 pair x 1GbE Copper Bypass		
Memory(RAM)	4 GB	8 GB	16 GB	24 GB	48 GB	48 GB
SSD / HDD	160 GB / 1TB	160 GB / 1 TB (up to 2TB, optional)				
CPU	1 x 2-core	1 x 4-core	1 x 4-core	1 x 6-core	2 x 6-core	
Power Consumption	100 W	156 W	156 W	232 W	257 W	257 W
Power Input	100-240VAC, 50-60 Hz (free voltage) / Dual Power (hot-swappable)					
Dimension(WxDxH,mm)	428 x 566 x 44 (1RU)			428 x 606 x 88 (2RU)		
Weight	8.9 kg	14 kg	14 kg	14.6 kg	15.1 kg	15.1 kg
Throughput	600 Mbps	2 Gbps	4 Gbps	10 Gbps	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

WEBFRONT-KS 가상화 모델

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

최소 사양 서버 환경(WEBFRONT-KS 한 개 설치시)

CPU	Memory	HDD	HyperVisor
x86, 64 bit CPU with Intel VTx or AMD-V	4 GB	40 GB	-GEMU/KVM 1.0.0 or higher -VMware ESXi 5.0 or higher -OpenStack Juno or higher -Xen 4.1 or higher

주요 기능

*스팩은 제품의 성능 및 기능 향상인쇄상의 오류 등으로 인해 사전 예고 없이 변경될 수 있습니다. 오른쪽의 QR코드를 스캔하여 최신 스펙을 확인 할 수 있습니다.



요청 검사 (Request Inspection)	<ul style="list-style-type: none"> • 애플리케이션 접근 제어 • 폼 필드 무결성 검사 • 폼 필드 형식 검사 • 쿠키 무결성 검사 • 쿠키 형식 검사 • 과다 요청 검사 • 업로드 검사 	<ul style="list-style-type: none"> • 다운로드 검사 • Slowloris 차단 • 금칙어 차단 • 신용카드 정보 유입 차단 • 버퍼 오버플로우 차단 • SQL 삽입 차단 • 스크립트 삽입 차단 	<ul style="list-style-type: none"> • 검사 회피 차단 • 요청 형식 검사 • 디렉토리 리스팅 차단 • 인클루드 인젝션 차단 • 주민번호 유입 차단 • HTTP Post 공격 차단 • WISE Filter™
응답 검사 (Response Inspection)	<ul style="list-style-type: none"> • 웹 변조 방지 • 신용 카드 정보 유출 차단 • 주민 등록 번호 유출 차단 • 계좌 번호 유출 차단 	<ul style="list-style-type: none"> • 응답 형식 검사 • 코드 노출 차단 • WISE Filter™ 	
학습(Learning)	<ul style="list-style-type: none"> • 접근 제어 학습 • 폼 필드 학습 • URL 구조 학습 		
위장(Cloacking)	<ul style="list-style-type: none"> • URL 변환 • 부적절한 에러 처리 	<ul style="list-style-type: none"> • 서버 정보 위장 	

PIOLINK

(주)파이오링크 | 대표전화 02.2025.6900 | www.PIOLINK.com

- 이 문서의 내용은 제품의 성능 및 기능 향상, 인쇄상의 오류 수정 등으로 인해 사전 예고 없이 변경될 수 있습니다.
- 이미지는 실제와 다를 수 있습니다.
- 기재되어 있는 회사, 제품 및 서비스 이름은 각 사의 상표 또는 서비스 표시입니다.
- 제품은 공인 파트너를 통해 구매할 수 있으며 당사 영업부서 또는 홈페이지에서 확인할 수 있습니다.

제품 구매 및
온라인 문의

