SSL 처리에 강한 웹방화벽 'WEBFRONT-K'

웹방화벽 선택 기준 - SSL 성능지표 가이드

연재 순서

웹에서 데이터를 암호화하고 안전한 통신을 제공하기 위해 SSL(Secure Sockets Layer[1], 이하 SSL)을 이용한다. 초기 SSL이 고객의 로그인 정보를 보호하기 위한 용도로 사용되었다면 최근에는 웹 서비스 전체에 대해서 암호화를 수행하는 추세이며, 구글이나 야후 등 대표적인 포털 사이트는 전체 서비스에 대해 SSL을 적용하고 있다. 그만큼 웹에서 SSL은 선택이 아닌 필수로 자리매김하고 있다.

웹방화벽은 웹 서버 앞단에서 SSL 암·복호화를 수행하고, SSL 인증서와 키를 서버 대신 관리하면서 SSL로 암호화된 공격 트래픽을 감시 및 차단하고 있다.

휴대폰, 태블릿PC, 스마트워치 등 다양한 디바이스에서 웹을 이용하면서 대량의 웹 트래픽이 발생하고 있다. 글로벌 조사 기관에 따르면, 약 25% 이상의 트래픽이 암호화된 트래픽인 것으로 발표한 바 있다. SSL 트래픽을 소프트웨어적으로 처리하기 위해서는 CPU 리소스를 많이 사용하게 되고 웹방화벽의 보안 성능을 유지하기 위한 CPU 리소스 활용에 부하가 발생하여 웹방화벽 성능이 저하된다.

따라서 몇몇 웹방화벽 제조사는 소프트웨어 기반 SSL 처리 성능의 한계를 인식하고 SSL을 위한 하드웨어 기반의 장비를 이용하여 처리 성능을 높이는 방식을 제안한다.

파이오링크 웹방화벽 "WEBFRONT-K"는 하드웨어 SSL 카드를 장착하여 웹방화벽 리소스 사용의 부담을 줄이고 국내 최고의 SSL 성능을 제공하고 있다.

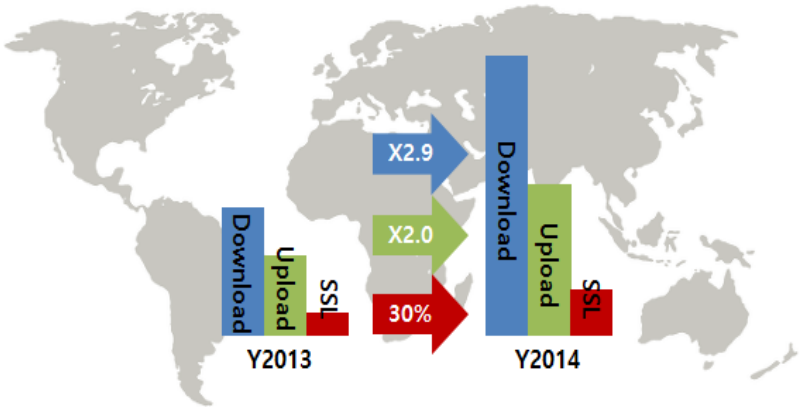
본 백서에서는 SSL에 대한 중요도가 점차 증가함에 따라 SSL 성능으로 표기하는 CPS와 TPS에 대한 측정 방법을 알아보고 SSL 성능 기준을 안내하고자 한다.

[1]. 본 백서에서의 SSL(Secure Sockets Layer)은 HTTPS에 대해 국한하여 소개하며 이해를 돕기 위해 HTTPS 성능을 SSL 성능으로 통칭하도록 한다.

시장 현황

글로벌 조사 기관에 따르면, 전세계 유무선 트래픽 중 암호화 트래픽 비중은 2013년 대비 2014년에 다운로드 2.9배, 업로드가 2배 증가하였다고 한다. 또한 연간 암호화 트래픽 증가율은 20%로 예상하며 기업의 트래픽 중 약 25~30%가 암호화 트래픽인 것으로 조사된 바 있다.

[그림 1. 글로벌 트래픽 현황]



웹 공격 또한 이에 맞춰 SSL 암호화를 이용하는 진화된 위협이 증가하고 있으며 2017년 네트워크 대상 공격의 50% 이상은 암호화된 트래픽이 차지할 것이라는 조사도 있다.

구글은 보안 프로토콜 의무화를 통해 암호화 트래픽 확산을 추진하고 있고 검색 서비스와 Gmail에 이어 자체 데이터센터 간 트래픽 전송 구간을 암호화하고 있다. 또한 암호화 키에 대해서도 보안 인증이 상대적으로 취약한 RSA 1024 bit Key를 대신해 RSA 2048 bit Key로 업그레이드하였다.

페이스북은 2012년부터 기본적으로 SSL 통신을 적용하여 이용자들에게 암호화된 연결과 서비스를 제공하며, 안전한 데이터 송수신을 위해서 구글과 마찬가지로 데이터센터 간 트래픽 전송구간을 암호화하고 있다.

국내의 경우 공인인증서 의무화 폐지와 Active-X 중단 등 보안 환경의 변화가 진행되고 있으며 2016년 들어 Active-X 걷어내기에 집중하고 있다.

본 백서에서는 보안에 대한 강화 및 웹 트렌드 변화에 따라 그 중요성이 강조되고 있는 SSL에 대해 보다 정확히 파악하고자 한다. 다음 장에는 SSL에 대한 성능 기준을 설명하고, 파이오링크 고성능 웹방화벽인 “WEBFRONT-K”의 고객 사례를 통해서 SSL에 대한 고객사의 대응 방안에 대해 소개한다.

SSL 처리 성능의 이해

SSL 적용을 고민하는 많은 고객의 가장 큰 걱정거리는 바로 성능이다.

SSL은 사용자와 서버 간 전달되는 데이터를 암·복호화 하는 데에 수학적인 알고리즘이 적용되어있어 서버의 자원을 크게 소모시킨다. 따라서 안정적인 서비스를 유지해야 하는 운영자들의 입장에서는 서버 자원 소모로 인한 서비스의 안정성이 흔들리는 것이 가장 큰 고민거리이다.

시장에는 고객의 니즈에 맞춰 SSL을 빠르고 안정적으로 처리해 주는 관련 제품들이 많이 소개되어 있다. 이러한 제품들은 SSL의 효과적인 처리를 위해 전용 하드웨어 가속기를 탑재하고 있으며, 제조사마다 처리성능 지표를 제공하여 고객들에게 제품 선택 시 참고할 수 있도록 하고 있다.

SSL 성능 지표

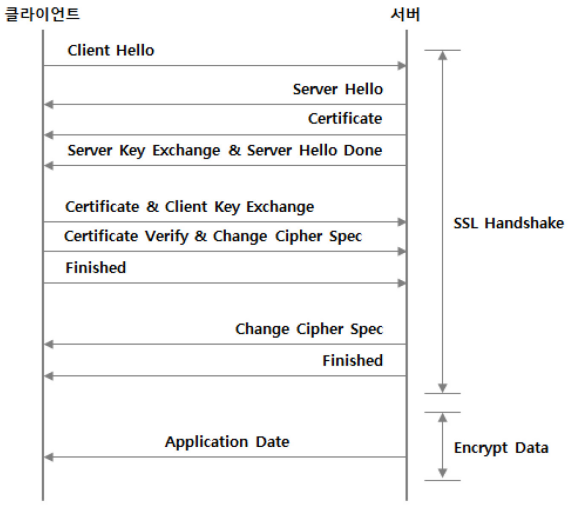
SSL을 지원하는 장비를 선택하기 위해서 가장 크게 관심을 가져야 하는 부분이 바로 성능이다. SSL 성능 지표에는 어떤 것들이 사용될까?

각 제조사별로 제공하는 제품 데이터시트를 참고하면 해당 제품의 최대 처리 성능을 확인할 수 있다. 데이터시트에 명시된 성능치의 정확한 의미를 이해하기 위해서는 [그림 2]와 같이 SSL의 처리과정을 살펴볼 필요가 있다.

[그림 2]에서 볼 수 있듯이 SSL 처리과정은 크게 두 단계로 나누어 볼 수 있다.

먼저 SSL 통신을 하기 위해서는 클라이언트와 서버간 인증서 및 키를 교환하는 SSL 핸드쉐이크 과정이 필요하다. SSL 핸드쉐이크가 완료되면, 해당 세션을 통해 암호화된 데이터를 전달하게 된다.

[그림 2. SSL 처리 과정]



이 두 가지 과정에서 성능 이슈가 발생하며 **초당 SSL 핸드쉐이크 처리 수, 초당 SSL 암호화 트래픽 처리량으로 SSL의 성능**을 확인할 수 있다.

따라서 웹방화벽 도입을 고려할 때 아래 두 항목에 대한 성능 수치를 올바르게 파악해야 한다.

- 초당 SSL 핸드쉐이크 처리 능력
- 초당 암호화된 트래픽 처리 능력

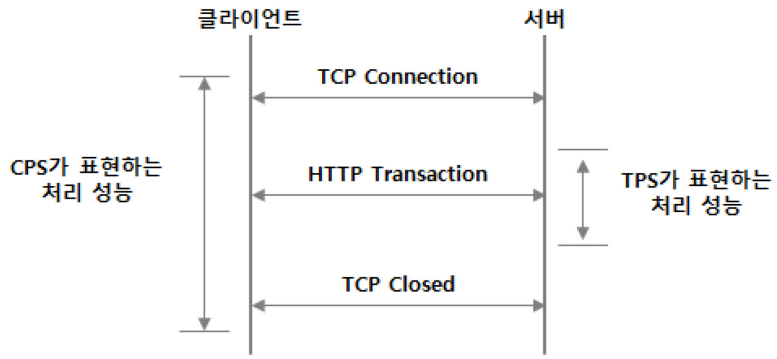
각 웹방화벽 제조사는 제품의 처리 성능 사양을 브로슈어 및 제품 소개 자료에 제공하고 있다. 그러나 [표 1]과 같이 파이오링크를 제외한 국내 웹방화벽 제조사는 모두 TPS 성능만을 제공하고, 외산 제조사의 경우 CPS(Connection Per Second) 또는 TPS(Transaction Per Second)만 제공하여 성능을 표현하는 단위가 제조사마다 다른 것을 확인할 수 있다.

[표 1. 제조사 별 성능 측정 단위 및 암호화 키 사이즈]

구분	PIOLINK	국내 A사	국내 B사	해외 C사	해외 D사
성능 기준	TPS / CPS	TPS	TPS	CPS	TPS
암호화 Key 사이즈	RSA 2048bit	RSA 1024bit	RSA 1024bit	RSA 2048bit	RSA 2048bit

제조사마다 제시하는 성능 단위가 다르기 때문에 제품별 비교를 해야 하는 고객의 입장에서 성능 기준을 마련하기 어려움이 따른다.

[그림 3. CPS와 TPS 처리 성능 개요]



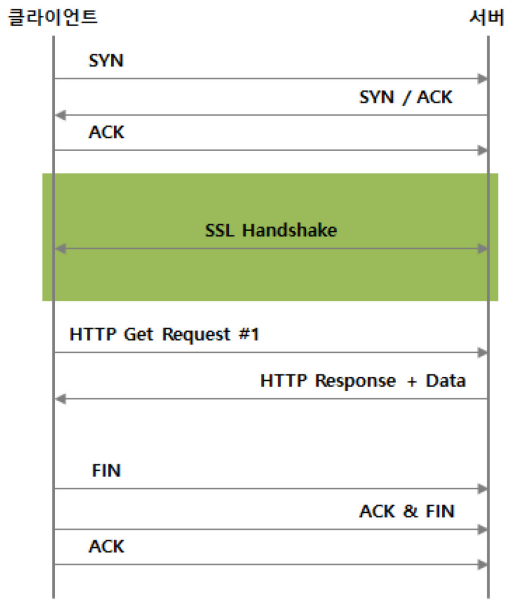
웹은 클라이언트와 서버간 수행되는 HTTP 통신 과정이다. [그림 3]에서와 같이 CPS는 초당 TCP 커넥션 처리 능력을 나타내고, TPS는 초당 HTTP 트랜잭션 처리 능력을 나타내는 지표이다.

- 1 CPS: 초당 1개의 TCP 커넥션을 정상적으로 수립한 후 에러 없이 종료함
- 1 TPS: 초당 1개의 HTTP 요청과 응답을 정상적으로 처리함

SSL에서 혼란스런 TPS의 의미

SSL의 성능을 올바르게 이해하려면, 다음[그림 4]의 SSL Handshake 부분의 “초당 SSL 핸드쉐이크 처리 능력”을 알아야 한다.

[그림 4. SSL 핸드쉐이크 처리 성능 테스트]



하지만 각 제조사마다 SSL 최대 처리 성능 수치를 CPS 또는 TPS로 제공하고 있는 실정이다. 그렇다면 CPS와 TPS 중 어느 것을 SSL 성능 지표로 사용해야 ‘초당 SSL 핸드쉐이크 처리 능력’으로 볼 수 있을까?

파이오링크는 CPS를 SSL 성능 지표로 제안하며, TPS 성능을 제시할 경우 측정 방식 등을 함께 제공하고 있다.

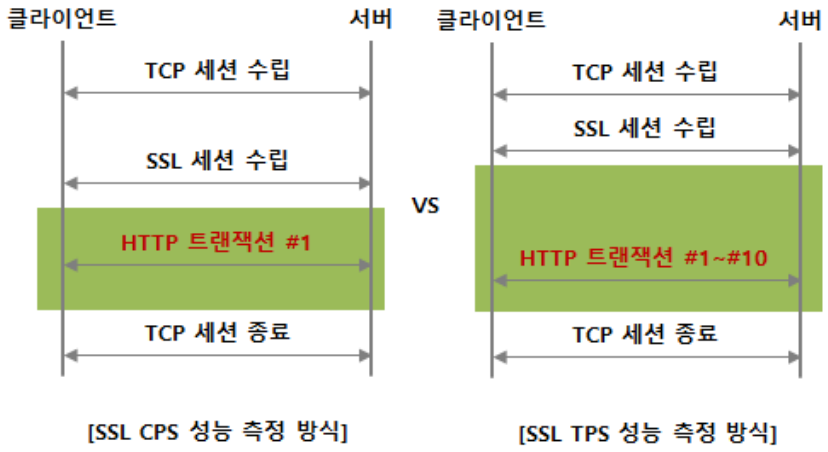
계측기로 SSL 성능을 측정하기 위해서는 TCP 세션과 HTTP 트랜잭션을 모두 설정해야 한다. SSL만 단독으로 테스트할 수 있는 방법이 없기 때문이다. 다시 말해, SSL은 HTTP 트랜잭션을 암호화하기 위한 프로토콜이고 HTTP 트랜잭션은 TCP 기반에서 동작하므로 두 요소를 모두 테스트하여 SSL 성능을 확인할 수 있는 것이다.

일반적으로 CPS와 TPS를 계측하는 방식에서 가장 큰 차이점은 클라이언트와 서버 간 동작 방식이다. CPS는 하나의 커넥션에 오직 하나의 HTTP 트랜잭션을 시도하며, TPS는 하나의 커넥션에 다수의 트랜잭션을 시도하는데 BMT시에는 통상 10번의 트랜잭션으로 측정한다.

- CPS: 1 Transaction / 1 Connection
- TPS: 10 Transaction / 1 Connection

앞에서 설명한 SSL성능을 나타내는 CPS와 TPS를 정리하면 아래와 같다.

[그림 5. SSL CPS, TPS 성능 계측 방식 비교]



SSL TPS 성능 측정 방식의 경우 한 사용자가 SSL 세션을 수립한 이후 트랜잭션을 얼마나 많이 수행하는지를 볼 수 있다. 하지만 실제 웹 서비스에서는 한 사람이 접속해서 많은 트랜잭션이 발생하기 보다, 많은 사람이 접속해서 일정량의 트랜잭션을 발생시키기 때문에 SSL 성능을 파악하기 위해서는 CPS 성능 측정 방식을 주요 지표로 하고, TPS 성능 측정 방식을 보조 지표로 함께 본다면 SSL 성능을 파악하는데 도움이 될 것이다.

국내 제조사의 경우 TPS를 SSL 성능 수치로 사용하고 있지만 계측 방법이나 조건을 명확히 공개하지 않고 있기 때문에 고객은 이에 대한 추가 확인이 필요하다. 이와 대조적으로 파이오링크는 SSL 처리 성능 수치를 제공할 때 TPS는 물론 CPS 성능까지 제공하여 고객의 이해를 돕고 있다.

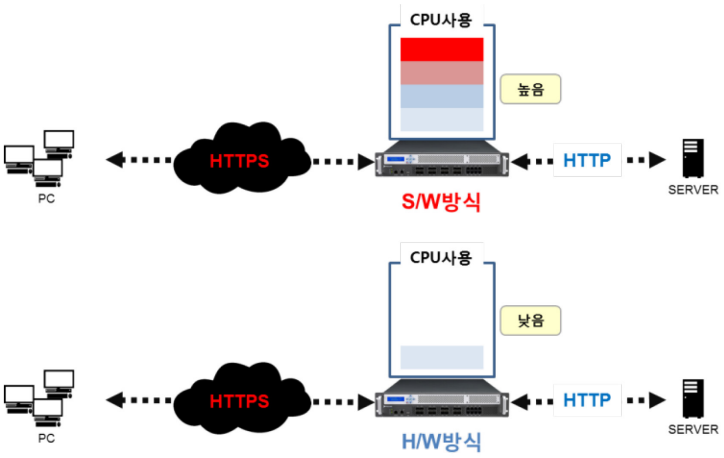
따라서 SSL CPS가 성능 표준으로 자리 잡아야 하며, 웹방화벽 도입 시 TPS 정보만 표기된 경우, 사용자는 계측방법이나 테스트 조건을 추가로 요청할 필요가 있다.

WEBFRONT-K SSL의 특장점

SSL은 복잡한 암·복호화 연산 처리를 주로 수행하기 때문에 장비의 리소스를 많이 사용하게 된다. SSL 처리량이 많아질수록 장비의 성능에 미치는 영향이 크며, 이 경우 웹방화벽 단일 장비에서 동시에 처리하게 되면 HTTP 서비스에도 문제가 발생할 수 있다. 따라서 안정적인 서비스를 위해서는 암·복호화 를 전용으로 처리하는 별도의 어플라이언스 장비 또는 SSL 가속카드의 사용을 권장한다. WEBFRONT-K 는 소프트웨어 방식과 하드웨어 방식을 모두 제공하여 기업의 환경과 요구에 맞게 유연하게 적용할 수 있다.

아래 [그림 6]에서는 소프트웨어 방식과 하드웨어 방식의 처리 방식을 설명한다.

[그림 6. 소프트웨어 vs 하드웨어 SSL 처리 방식 비교]



WEBFRONT-K는 소프트웨어 방식의 SSL 처리 기능을 제공할 뿐만 아니라 국내 최초로 하드웨어 기반의 SSL 가속카드를 장착한 웹방화벽으로, 암호화 키 사이즈가 RSA 2048bit 의 높은 보안 환경에서도 빠르고 안정적인 SSL 처리 성능을 보이고 있어 성능과 안정성에 있어 국내 최고를 자랑한다.

[표 2. 파이오링크 웹방화벽 WEBFRONT-K4400 모델에 대한 SSL 처리 성능 비교] [2]

구분	소프트웨어 방식	하드웨어 방식
CPS	1,000	7,000
TPS	10,000	50,000
Throughput	4Gbps	6Gbps
비고	● 소프트웨어 방식은 SSL 트래픽을 처리하는 데 CPU 자원을 98% 이상 사용하기 때문에 웹방화벽 보안 성능이 낮아짐 ● 하드웨어 방식은 별도의 SSL 가속 카드에서 SSL 트래픽을 처리하기 때문에 성능을 그대로 유지하면서 웹방화벽의 보안 기능에 집중 가능	

[2] 참고: [표2] 측정 환경
- 암호화 키: RSA 2048 bit
- CPS
  1 Transaction / 1 Connection,
  응답사이즈 1KB
- TPS
  10 Transactions / 1 Connection,
  응답사이즈 1KB

고객사 도입 사례

사례 1

증권 중개 및 자산관리, 기업 금융과 자금 운용에 이르는 금융 서비스를 제공하는
종합 금융 투자회사

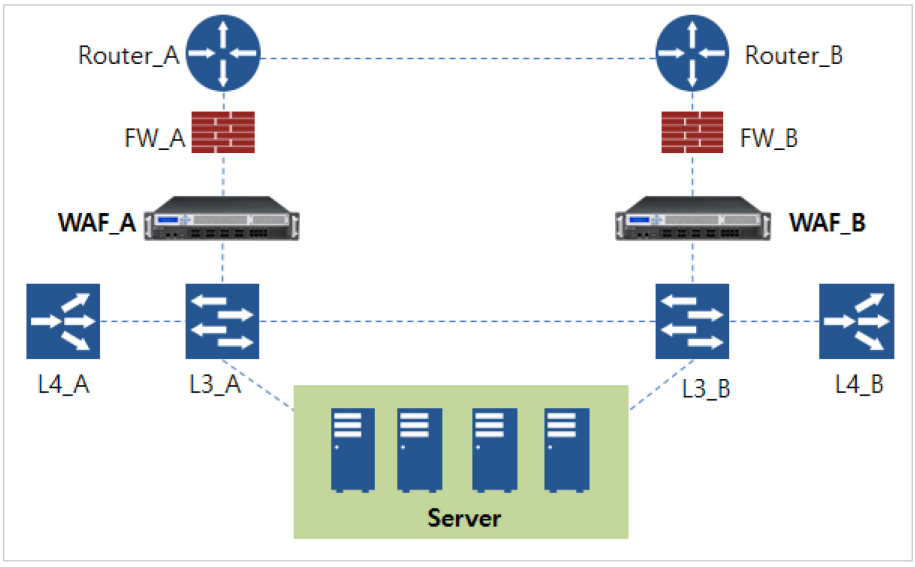
가) 도입 배경

실시간 실시간 증권 거래 및 대외 홈페이지 서비스에 대한 웹 보안 필요성의 증가로 안정적으로 SSL 데이터를 처리할 수 있는 하드웨어 기반의 웹방화벽이 필요하게 되었다. 이에 국내 웹방화벽 제조사를 통해 BMT 를 진행하였고 하드웨어 SSL 카드를 사용하고 있는 고성능 웹방화벽 WEBFRONT-K 를 도입하게 되었다.

나) 구성 특징

① 일반적인 인라인 브리지 구성
② 이중화 네트워크 구성 (Active-Standby)
③ WEBFRONT-K는 이중화 없이 독립적(Stand-alone)으로 운영

다) 구성도



라) 도입 효과

① 하드웨어 기반의 SSL 가속카드를 통해 안정적인 SSL 웹 보안 서비스 구축
② 증권거래를 포함한 대표 웹 애플리케이션 서비스에 대한 웹 보안 강화

사례 2

대형 항공사를 포함해 각종 글로벌 비즈니스를 운영하는 국내 대기업

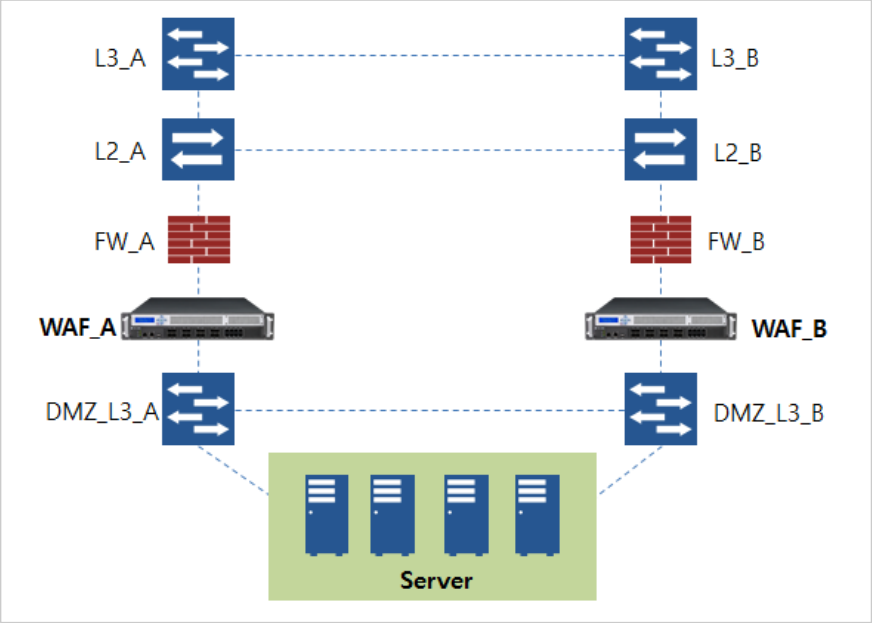
가) 도입 배경

그룹사 전체의 대용량 SSL 트래픽을 안정적으로 처리하고 실시간 항공 예약에 있어서 서비스의 가용성이 중요한 환경이다. 이에 따라 기존에 사용 중이던 타사 웹방화벽을 대신할 고성능 웹방화벽이 필요하게 되었다. 특히 PCI-DSS[3] 요구사항을 만족해야 했다. 국내에서는 WEBFRONT-K 가 PCI-DSS 요구사항을 만족하는 동시에 안정성과 성능 측면에서도 타사에 비해 월등하여 WEBFORNT-K 를 도입하게 되었다.

나) 구성 특징

① 일반적인 인라인 브리지 구성
② 이중화 네트워크 구성 (Active-Standby)
① WEBFRONT-K는 이중화 구성없이 독립적(Stand-alone)으로 운영

다) 구성도



라) 도입 효과

① 하드웨어 기반의 SSL 가속카드를 통한 안정적인 SSL 서비스 구축
② 실시간 항공티켓 발매를 포함한 웹 서비스 보안 강화

[3] PCI-DSS (Payment Card Industry Data Security Standard): 신용카드 업계의 산업 보안표준으로 핀테크 분야에서도 필수 인증으로 간주되고 있음

사례 3

보험 운용에서 기업 자산 관리에 이르기까지 종합 금융
서비스를 제공하는 국내 보험사의 중국 지사

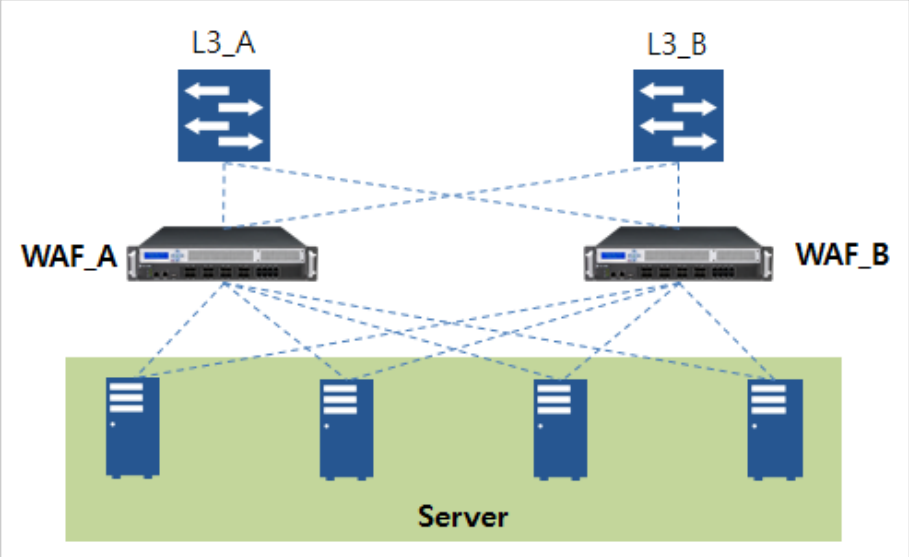
가) 도입 배경

고객의 민감한 정보를 암호화하여 보안을 강화해야 하는 상황으로 중국 현지 고객의 수가 많고 일반 개인 고객부터 기업 고객까지 다양한 종류의 데이터를 안전하게 처리해야 했다. 또한 별도의 부하분산 장비 도입 비용을 절감하기 위해서 웹방화벽에서 부하분산 기능이 필요했다.

나) 구성 특징

① 웹방화벽의 자체 L7 SLB기능을 적용
② 웹방화벽 간 Active-Standby 이중화 구성

다) 구성도



라) 도입 효과

① 별도의 부하분산 장비 도입 비용 절감
② HTTP 및 SSL 웹 애플리케이션에 대한 보안 강화

웹방화벽 선택 시 Check Point

2000년대 중반부터 시장에 웹방화벽이 소개된 지 10년 이상 지났다. 웹 애플리케이션의 취약점을 이용한 보안사고가 심심치 않게 매스컴을 통해 알려지기 시작하였고 중요한 고객 정보의 유출로 피해가 극심해지면서 웹방화벽의 수요 또한 비례적으로 늘어나게 되었는데, 이런 시기를 거쳐 현재 웹방화벽은 보안시장의 주요 장비로 자리매김을 하게 되었다.

웹방화벽의 출시 초기인 2000년대 중반만 하더라도 대부분의 웹사이트들은 HTTP 기반이었다. 대형포털과 쇼핑몰 등을 제외하고는 접속량도 많지 않았기 때문에 주요 고객들은 Throughput 1Gbps 미만의 장비로도 충분하였다.

2000년대 후반 아이폰을 시작으로 스마트폰, 태블릿PC, 스마트밴드 등의 포터블 디바이스들의 보급이 급격하게 늘어나면서 모바일 기반의 웹 애플리케이션 서비스 수와 접속량이 가파르게 증가하였다.

이 때문에 정부와 지역자치단체, 기업 등에서도 망 고도화 사업을 기반으로 Throughput 10Gbps 기반의 네트워크가 구축되었고, 이를 지원할 수 있는 네트워크 및 보안장비에 대한 요구가 커지게 되었다.

웹방화벽도 예외는 아니다. 더구나 웹방화벽은 웹 애플리케이션 서비스에 직접적으로 관여하는 장비이다 보니 보안성만큼이나 처리성능에 대한 요구도 크다.

최근에는 SSL 적용 범위가 확대되고 있으며, RSA 2048 bit 이상의 인증서를 기본적으로 적용하여 보안성을 높일 것을 권고하고 있으므로 안정적인 운영 성능을 위해 하드웨어 기반의 SSL 카드가 탑재된 웹방화벽이 필수적이다.

웹방화벽을 선택할 경우 반드시 고려해야 할 사항은 다음과 같다.

1. 웹서비스의 가용성을 보장할 수 있는 처리성능을 갖추고 있는가?
- 웹방화벽의 성능 성능 비교 (CPS / TPS / Throughput / Concurrent Connection)

2. RSA 2048 bit 기반의 인증서를 적용한 상태에서 처리성능은 충분한가?
- SSL 처리 성능 비교 (CPS / Throughput)
- 하드웨어 기반의 SSL 가속카드 탑재 여부

3. 웹 애플리케이션 취약점을 이용한 대비는 충실한가?
- OWASP TOP 10 대응
- 국정원 8대 취약점 대응
- Layer 7 기반의 DDoS 대응

4. 운영을 위한 관리의 편의성은 잘 갖추고 있는가?
- GUI 기반의 웹방화벽 관리 화면 제공
- 다양한 브라우저 호환

크게 위의 4가지 체크 항목을 기준으로 제품을 비교한다면, 고객의 보안 요구 사항에 최적화된 웹방화벽을 선택하는데 도움이 될 것이다.

더 많은 정보는 www.PIOLINK.com 에서 확인하실 수 있습니다.

(주)파이오링크

파이오링크는(코스닥170790) 클라우드 데이터센터 최적화 전문 기업입니다. 업계 최고의 애플리케이션 가용성, 성능, 보안을 보장하고 데이터센터의 민첩성과 유연성을 확보하는 데 주력하고 있습니다. 데이터센터 운영과 보안관제 서비스를 포함한 다양한 IT 인프라 제품과 솔루션을 제공하며, 통신, 금융, 공공, 기업 등 다양한 산업 고객의 비즈니스를 극대화하고 있습니다.