

높이지는 법적 규제, 웹 방화벽 ‘필수’

전세계 웹 방화벽 시장 성장 지속 ... 고용량 신기술 탑재 경쟁 ‘점화’

연재순서

1. 웹 공격, 단순함파 정교함의 조화
2. 웹 방화벽, 웹 공격 방어 기술의 총집합
3. 웹 방화벽, 그리고 웹 보안의 미래(이번호)

최 근 웹을 둘러싼 급격한 환경 변화는 웹 보안에 있어 서도 많은 이슈를 야기하고 있다. 클라우드 컴퓨팅, 소셜 네트워킹 서비스(SNS)나 스마트 단말의 보급 확대는 웹 기반 서비스의 확대를 의미할 뿐만 아니라, 보다 심각한 웹 보안 위협의 등장을 내포하고 있기도 하다.

나아가 웹 기반 서비스의 확대는 웹 트래픽의 증가를 수반하고 있으며, 이에 대응할 수 있는 대용량 웹 트래픽의 실시간 처리 기능을 필요로 하고 있다. 이러한 웹 환경의 변화는 보안 이슈를 증가시키며 웹 방화벽의 시장확대 요인으로 작용하고 있다. 이번호에서는 웹 방화벽의 기술 발전 동향과 국내외 시장 동향을 살펴본다.

클라우드 컴퓨팅 환경에서의 웹 방화벽

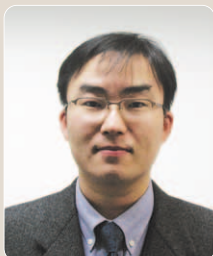
클라우드 컴퓨팅은 구름(클라우드) 내에 있는 임의의 서

버, 서비스를 PC나 스마트 폰과 같은 단말 종류에 상관 없이 접속, 사용하게 된다. 복잡한 이기종 환경의 지원을 위해 대부분의 클라우드 기반 서비스는 HTTP를 표준 프로토콜로 하는 웹 브라우저 기반의 접속 프로그램을 사용한다.

이러한 HTTP 기반의 접속 방식은 기존의 웹 보안 대상이었던 조직 내의 웹 서버 뿐만 아니라 클라우드 환경 내의 가상 웹 서버 및 스마트 단말까지 보호 대상을 확장하도록 만들고 있다. 한편 가상화 환경 내에서 운영되는 웹 서버들의 보호는 기존 어플라이언스 방식의 보안 시스템과는 다른 접근 방식을 요구하고 있다. 클라우드 환경 내에서 웹 보안을 해결할 솔루션으로 웹 방화벽은 단연 각광 받는 존재로, 클라우드 컴퓨팅의 다양한 서비스 방식에 맞춰 발전하고 있다.

SaaS(Software as a Service) 방식의 웹 방화벽 서비스는 국내외에서 실용화돼 제공되고 있으며, IaaS(Infrastructure as a Service) 방식의 웹 방화벽 서비스도 해외에서는 제공 중이다. 국내에서는 2011년 하반기에 최초로 펜타시큐리티 시스템에서 IaaS 방식의 가상 어플라이언스(virtual appliance) 기반의 웹 방화벽 서비스를 제공할 예정이다.

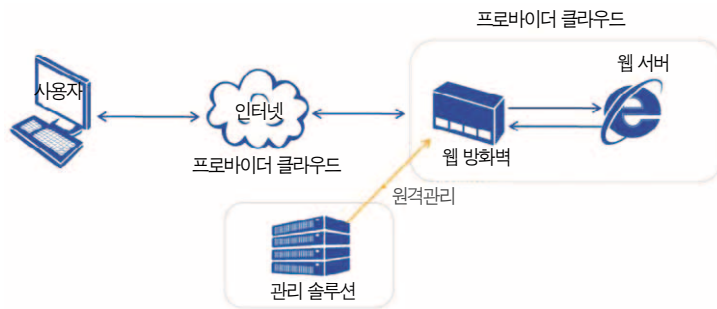
SaaS 모델의 웹 방화벽은 모든 웹 서버마다 소프트웨어 기반의 웹 방화벽을 설치해 중앙 관리하거나, 웹 서버 앞에 어플라이언스 형태의 웹 방화벽을 설치해 운영하게 된다. 이



웹은 편리성이 높지만, 편리성만큼 위험도 높다는 보안의 명제를 증명하고 있다. 최근 발생한 다양한 공격의 출발점 또한 웹으로, 웹을 통해 악성코드를 유포하거나 웹 서버 등을 해킹, DDoS 공격이나 정보유출의 진원지로 활용한 것이다. 이러한 웹 공격 이슈와 더불어 대응책으로서 웹 방화벽에 대해 알아본다. <편집자>

이충우 펜타시큐리티시스템 이사 / bazle@pentasecurity.com

〈그림 1〉 SaaS 방식의 웹 방화벽 서비스

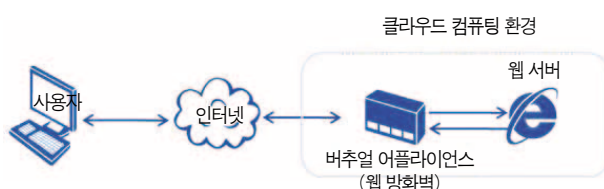


러한 SaaS 기반의 웹 방화벽 서비스는 호스팅 서비스나 전문 보안 관제 기업에 의해서 제공되고 있으며, 소규모 웹 사이트 뿐만 아니라 온라인 서비스를 주 사업으로 하는 거대 기업으로 이용이 확대되고 있다. 해외에서는 아마존 웹 서비스(AWS)를 기반으로 하는 SaaS 웹 방화벽 서비스가 등장, 제공되고 있다.

IaaS 방식의 웹 방화벽 서비스는 일반적으로 가상 어플라이언스 기반의 웹 방화벽을 통해 제공된다. 가상화 환경 내에서 운영되는 가상 호스트(virtual host)인 웹 서버를 가상 웹 방화벽으로 보호하게 되므로, 가상 서버를 구매하듯 사용자가 웹 방화벽의 수량을 직접 선택, 일정액을 지불하고 사용하게 되며, 보안 관리를 사용자가 직접 담당하게 된다. 가상 환경에서 모든 시스템이 동작하게 되므로, 동적 자원 할당에 따른 과부하 상황에 대한 대처, 장애 발생 시 가상 서버의 재할당 및 재시작 등으로 가용성이 매우 높아지는 한편, 보다 적은 비용으로 구축, 운영할 수 있다는 장점이 있다.

향후에는 웹 방화벽 또한 하이퍼바이저(hypervisor) 커널 모듈 수준으로 구성돼 클라우드 API를 이용한 데이터 수집과 동적 보안정책 수행과 같은 새로운 기능을 수행하는 방향으로 발전할 것이다.

〈그림 2〉 가상 어플라이언스 형태의 웹 방화벽



대용량 웹 트래픽 처리

웹 기반 서비스의 확대는 필연적으로 웹 트래픽의 증가를 수반한다. 웹 트래픽은 연평균 30%씩 늘어나 2009년부터 2014년까지 3.7배 증가할 것으로 예측되고 있고, 이에 맞춰 트래픽을 처리할 웹 서버도 증가하고 있다. 이미 국내의 경우, 대용량 웹 트래픽을 수반하는 각종 웹 서비스가 10Gbps 기반의 네트워크로 전환되고 있다.

일상 수요가 많은 방송, 신문사뿐만 아니라 특정 기간에 대규모 트래픽이 발생하는 공공 및 민간 서비스는 이미 백본망이 10Gbps 네트워크로 구성돼 있으며, 그 하부 네트워크에는 대규모 웹 서버를 포함하고 있다. 이 같은 경우, 최대 1000대를 넘는 웹 서버를 보호하기 위해 개별적으로 웹 방화벽을 구축, 운영하기에는 많은 비용이 소요될 뿐만 아니라 운영 및 관리상의 부담 또한 매우 크게 발생한다.

이를 해결하는 방안은 백본 영역에 웹 방화벽을 구축해 비용 대비 효과를 최대화하는 것이며, 이에 따라 10Gbps 급의 대용량 웹 트래픽을 처리할 수 있는 웹 방화벽이 요구되고 있다. 이러한 웹 방화벽은 어플라이언스 방식으로 독자적인 웹 트래픽 처리 방식을 구현하고 있으며, 소프트웨어 방식이나 네트워크 스위치 기반, 경우에 따라서는 NPU(Network Processing Unit)와 같은 하드웨어의 보조처리를 이용하기도 한다.

스위치 기반이나 NPU와 같은 하드웨어 이용은 애플리케이션 트래픽 처리가 쉽지 않다는 점과 생산 비용 등의 문제가 있다. 따라서 실제 10Gbps 급의 웹 트래픽 처리를 위해서는 소프트웨어 처리가 주류를 이루고 있다. 올해부터 도입이 본격화되고 있는 10Gbps급 웹 방화벽은 네트워크 방화벽이나 IPS의 사례와 마찬가지로 국내 제품 가운데서도 극소수만이 공급 가능할 것으로 예측된다.

기술적으로 보면, 평판 기반의 탐지 등 신기술 접목이 예상된다. 평판(reputation) 기반의 탐지 및 차단 기술은 다수의 웹 방화벽으로부터 수집된 데이터를 바탕으로 공격의 위험도, 출발지 정보 등을 분석해 웹 공격을 차단하는 방식이다. 최근의 웹 공격은 다형성을 갖고 있어 하나의 탐지 방식으로는 탐지가 힘든 경우가 있다. 맬스 SQL 인젝션공격 같은 경우, 기본적으로 SQL 인젝션 공격이지만 최종적으로 사

용자에게 피해를 주는 것은 XSS(Cross Site Scripting) 공격이며, 이 공격은 자동화된 웹으로 수행된다. 게다가 보안시스템으로부터의 차단을 우회하고자 공격을 쿠키에 담아 전송하는 등 다양한 변형이 이뤄지고 있어 복합적인 분석 및 대응이 요구된다.

이러한 공격을 차단하기 위해서는 SQL 인젝션이나 XSS를 막기도 해야 하지만, 웹에 감염된 출발지 IP를 식별해 접근을 근본적으로 막아 추가적인 공격을 원천 봉쇄해야 할 필요가 있다. 왜냐하면 웹에 감염된 PC는 상대적으로 보안이 취약하다는 의미이며, 하나의 웹만 아니라 다른 악성코드에 감염돼 스팸 메일을 발송하거나 좀비 PC가 되어 분산서비스 거부(DDoS) 공격을 수행할 수도 있기 때문이다.

7·7 대란과 같은 DDoS 공격의 경우, 국내뿐만 아니라 해외에 있는 수 만대의 좀비 PC로부터 주요 기관의 웹 서버에 대한 웹 접속이 집중돼 발생했다. 이러한 DDoS 공격에 사용되는 웹 접속 요청은 정상적인 웹 접속과 구분하기 힘들기 때문에, 평판 기반의 탐지를 통해 효과적으로 탐지, 차단이 가능하다. 국가 규모 또는 이를 넘어서는 공격의 발생 시 초기에 그 징후를 파악하고 대처할 때 평판 기반의 탐지 및 차단 기술이 그 진가를 발휘할 수 있을 것이다.

연평균 20% 이상 고성장 '예감'

각종 침해사고와 대규모 개인정보 유출사고가 이어지면서 웹 보안, 그 가운데 웹 방화벽의 중요성은 더욱 높아져가고 있다. 이제 웹 방화벽은 실질적으로 웹 공격 방어 시스템의 핵심으로 간주되고 있으며, 컴플라이언스 준수를 위해서도 필수적인 시스템으로 여겨지고 있다.

해외의 경우, PCI-DSS를 준수하기 위해서는 반드시 필요한 보안시스템이며, 국내에서도 발효된 개인정보보호법의 기술적·관리적 보호조치를 위해서는 반드시 갖춰야 하는 보안 시스템으로 언급되고 있다. 이렇듯 보안 기술, 법률적인 필요에 의해 웹 방화벽 시장은 급속하게 성장하고 있으며, 이러한 성장세는 당분간 지속될 전망이다.

테크나비오의 보고서에 따르면, 웹 방화벽 시장은 2008년 1억8180만달러에서 2013년 4억3760만달러에 도달, 동기간 연평균 성장률(CAGR) 24.6%로 급격히 늘어날 것으로 예측되고 있다. 또 프로그래밍&설리반의 보고서에서는 아시아 태평양 시장의 웹 방화벽 시장 성장률이 2010년 기준 28.4%

웹 방화벽 매출 전망

(단위 : 백만원)

구분	2009년	2010년	2011년	2012년	2013년	2014년	2015년	CAGR
2009년 보고서	27,184	29,462	31,739	34,017	36,294	38,572	-	6.0%
2010년 보고서	43,411	49,957	50,956	51,955	52,954	53,953	54,952	1.9%

(자료 : KISA)

에 달하며, 연평균 성장률 38.6%로 2015년에는 3억1501만 달러에 도달할 것으로 예상되고 있다.

이러한 시장 성장 전망은 해를 거듭할수록 웹 방화벽 시장 규모를 크게 산정하고 있어, 실제 웹 방화벽 시장 규모가 예측 기관의 전망보다도 빠르게 성장하고 있음을 반증하고 있다. 시장별로는 금융, 전자상거래, 정부기관이 18%대로 비슷한 규모의 시장을 형성하고 서비스, 교육, 제조 분야가 8~12%를 차지하는 것으로 분석된다.

국내 웹 방화벽 시장 조사도 이러한 경향을 보여주고 있다. KISA에서 매년 조사, 발표하는 보고서에 따르면, 2009년에 예측한 2011년 시장 규모가 2010년 보고서에는 약 200억원 가량 늘어나 있어 시장 전망보다 빠르게 성장하고 있는 것으로 추정할 수 있다.

이러한 시장 규모는 네트워크 방화벽의 시장 규모를 뛰어넘는 것으로, 조사 방식에 따라 편차가 있을 수는 있으나 시장의 기대감이 그만큼 크다는 것을 반영하고 있음을 알 수 있다. 반면에 국내 시장의 경우 공공 분야의 비중이 57.7%를 차지, 해외에 비해 기업 시장의 확대 여지가 매우 클 것으로 예상된다.

한편 국내 웹 방화벽 시장은 급격한 성장기를 거치면서 주요 제조사를 중심으로 재편되고 있다. 누적 판매 1500대를 돌파한 펜타시큐리티시스템이 올해 점유율 60%를 넘길 것으로 보이는 가운데, 펜타를 포함한 3개 제조사가 전체 시장의 90% 이상을 장악할 것으로 예상되고 있다.

웹 방화벽은 웹 공격 차단과 개인정보 유출방지라는 실질적인 보안 시스템으로서의 가치와 더불어 개인정보보호법과 같은 컴플라이언스를 준수하기 위한 필수 보안시스템이라는 요소를 함께 갖추고 있다.

한편 단순히 웹 서버를 보호하는 시스템에 그치지 않고 독자적인 평판 기반 시스템 구현이나 클라우드 컴퓨팅 지원과 같이 외연을 계속 넓혀 나가고 있다. 이렇듯 웹을 기반으로 하는 모든 시스템에서 보안을 위해 웹 방화벽이 우선적으로 고려되고 있으며 향후에도 그 가치는 더욱 높아질 것이다. 