



파이오링크 웹방화벽 ‘웹프론트-K’ 도입 … 성능 저하없는 암복호화 보장 … 끊임없는 서비스로 고객만족 ↑

SSL 가시성 확보한 웹방화벽으로 온라인 증권 서비스 고도화

키움증권(대표 권용원)은 국내 최초 온라인 종합증권사를 기치로 영업을 시작해 괄목할 만한 성장을 지속하고 있다. 2005년부터 11년 연속 주식시장 점유율 1위를 지키고 있으며, 수익성에서도 업계 최고의 ROE를 기록하고 있다. 업계 최저 수준의 판관비율, 최고 수준의 1인당 생산성을 보이며 저비용 고효율 구조의 증권사로 성장하고 있다. 키움증권은 다양한 온라인 금융 서비스를 고객에게 안정적으로 제공하기 위해 보안에 많은 투자를 단행하고 있으며, 특히 웹 기반 공격에 대응하기 위해 웹방화벽 고도화 사업을 진행했다. |글·김선애 기자·iyamm@datanet.co.kr| 사진·김구룡 기자·photoi@naver.com|

키움증권은 지속적으로 고객 맞춤형 서비스를 개발해왔으며, 현재 주식, 선물, 옵션거래 뿐만 아니라 해외주식, 국내외 선물, FX 마진 트레이딩, 온라인 투자자문, 동영상 투자 교육 서비스, 투자정보 커뮤니티, 금융센터 등 국내 1위 증권사의 위치에 걸맞는 자산관리 서비스를 제공하고 있다.

웹 기반 서비스 제공 위해 ‘보안’ 최우선 과제

키움증권의 다양한 서비스는 모두 다 온라인을 통해 이뤄지

기 때문에 인터넷 속도와 안정성, 보안성을 보장하는 것이 서비스 경쟁력을 지키는 길이라고 판단하고 있다. 특히 보안은 금융사 비즈니스를 지키는 핵심 요건으로, 다양한 사이버 공격을 막을 수 있는 보안 정책이 반드시 필요하다.

키움증권의 모든 서비스는 웹을 통해 이뤄지는 만큼 웹 기반 공격을 방어하는 것이 보안 분야의 최우선 과제다. 수시로 발생하는 DDoS 공격을 효과적으로 방어하고, 웹을 통해 유입되는 악성코드 및 지능형 공격을 차단하며, 정교하게 진행되는 타깃

공격을 탐지, 피해를 예방할 수 있는 방법이 필요했다.

이성구 키움증권 정보보안팀 과장은 “키움증권은 온라인 증권사 1위 기업으로, 경쟁사에 비해 온라인 이용 고객과 트래픽이 월등히 많다. 이에 따라 웹을 기반으로 한 사이버 공격도 수시로 발생하고 있으며, 정상 트래픽을 가장한 공격도 등장하고 있다. 따라서 지능화되는 공격을 방어할 수 있도록 여러 보안 시스템을 지속적으로 고도화하고 있다”고 말했다.

키움증권은 특히 웹 기반 공격을 방어할 수 있는 웹방화벽에 많은 투자를 진행해 왔으며, 최신 사이버 공격에 대응할 수 있는 방어 기술을 적용해 교묘하게 진행되는 타깃 공격도 정교하게 차단할 수 있도록 하고 있다.

성능저하 없는 ‘SSL 복호화’ 중점 검토

키움증권은 지난해 기존 운영하던 웹방화벽 교체 시점에 맞춰 웹방화벽 고도화 사업을 진행했다. 이 때 가장 중요하게 검토했던 사항이 SSL 트래픽 가시성이었다. 최근 사이버 공격은 SSL 암호화 트래픽에 공격요소를 숨겨 유입시킨다. 많은 보안 솔루션은 SSL 복호화 시 성능이 크게 떨어지기 때문에 SSL 트래픽을 복호화 하지 않고 그대로 허용한다.

기업/기관들은 경계구간에서 암호화 트래픽을 복호화하기 위해 웹 속도를 저하시킨다는 것은 사용자 경험을 낮추고 비즈니스에 피해를 줄 수 있다고 판단했다. 따라서 암호화 트래픽은 경계구간에서 분석하지 않고 내부 모니터링 시스템과 내부정보 유출방지 시스템 등 다른 시스템을 통해 분석하는 것이 일반적이었다.

그러나 SSL 사용 비중이 늘어나면서 암호화 트래픽에 악성 코드를 숨겨 유입시키는 공격도 급증해 암호화 트래픽의 가시성을 확보하는 것이 급선무가 됐다. 금융사의 경우 대부분의 트래픽이 암호화 돼 있기 때문에 암호화 트래픽에 공격이 숨어 유입되는 것을 철저히 차단해야 했다.

키움증권은 기존에 운영하던 웹방화벽은 SSL 복호화 지원에 제한적이었으며, 성능이 충분히 뒷받침되지 못해 다른 제품으로 교체해야 했다. 키움증권은 SSL 가시성을 지원하는 웹방화벽 제품을 다양하게 검토했으며, 실망에서 여러차례 테스트하면서 키움증권의 고객과 서비스를 보호할 수 있는 시스

템을 찾아냈다.

또한 키움증권의 웹 방화벽은 분산된 웹 환경을 지원할 수 있도록 여러 구간에 설치해야 했기 때문에 높은 비용의 고성능 제품보다 합리적인 가격으로 제공되는 안정성 높은 웹방화벽을 충분히 구축하는 것이 효과적이라고 판단했다.

HW-SW 자체 개발해 성능·보안 요건 만족

키움증권은 이 두가지 요건을 만족시킬 수 있는 국내의 웹방화벽을 다양하게 검토한 끝에 파이오링크의 고성능 웹방화벽 ‘웹프론트-K(WEBFRONT-K)’를 선택했다.

파이오링크 웹프론트-K는 국내 최고 성능인 20Gbps를 보장하는 고성능 웹방화벽으로 SSL 트래픽 처리에 탁월한 성능을 보여준다. 웹프론트-K는 더 높은 보안을 위해 사용되는 RSA 2048 비트 키 처리시에도 성능저하 없는 암호화를 보장한다.

CPS, TPS, 동시 세션 등에서도 타사 동급 대비 2, 3배 이상의 수치를 균형 있게 제공한다. 최대 2000만 동시 세션 지원으로 트래픽이 폭주할 때나 DDoS 등 네트워크 위협 상황에서도 웹 서버 보호 및 끊김 없는 서비스를 보장한다.

파이오링크는 하드웨어와 소프트웨어를 자체적으로 설계, 개발, 제작했기 때문에 어떠한 환경에서도 성능저하 없이 안전한 트래픽 처리를 보장할 수 있다. 특허 받은 고속 애플리케이션 처리 기술을 소프트웨어에 적용해 대용량 웹 트래픽을 빠르게 처리하며, 복잡한 네트워크 스택 구성을 단순화해 속도 한계에 영향을 주는 사용자 레벨과 커널 레벨 간의 병목 포인트를 제거했다.

이성구 과장은 “웹방화벽 고도화 사업을 진행할 때 SSL 복호화 시에도 높은 성능을 유지하고, 낮은 레이턴시와 데이터 유실이 없는 제품을 선정하는 것이 중요했다. 파이오링크 웹방화벽은 이러한 조건에서 타사 제품에 비해 월등한 성능을 보여줬다”고 말했다.

이어 그는 “파이오링크 웹방화벽을 구축, 운영하면서 공격 패턴을 분석해 본 결과, 기존에는 내부 보안 시스템에서 찾아낸 공격을 웹방화벽에서 효과적으로 차단하는 것을 확인했다. 웹을 통해 진행되는 지능형 공격을 웹의 가장 앞단에서부

터 차단해 보안 효과를 크게 높일 수 있었다”고 덧붙였다.

실망에서도 중단없이 웹방화벽 구축

키움증권이 웹방화벽을 선정하고 구축할 때 가장 우려했던 부분이 실망에 적용하는 시점에 장애가 발생할 가능성이 있다는 점이었다. 키움증권은 24시간 중단 없는 온라인 증권거래

서비스를 제공하고 있기 때문에 잠깐의 서비스 장애가 발생해도 막대한 피해로 이어질 수 있기 때문에 고도로 안정된 환경을 보장한 상태에서 테스트와 구축이 이뤄져야 했다.

키움증권의 서비스 망은 3중망으로 고도의 안전성을 보장하고 있다. 3중 망 중 하나에서 제품을 테스트하는 방식으로 실망에서의 웹방화벽 성능을 확인했다. 웹프론트-K로 제품

INTERVIEW

“SSL에 숨은 공격까지 차단해 안전한 온라인 증권 서비스 제공”

■ 웹방화벽 고도화 사업을 진행한 이유는.

기존에 운영하던 웹방화벽 교체연한이 다가와 성능과 기능이 개선된 차세대 웹방화벽으로 교체하기로 했다. 키움증권의 대부분의 트래픽이 금융 서비스인 만큼 암호화 트래픽 비중이 높은 편이기 때문에 성능저하 없이 트래픽을 복호화 할 수 있는 웹방화벽이 필요했다. 또한 온라인 기반 종합증권 서비스를 제공하고 있어 대규모 사용자들이 서비스에 접속했을 때 성능저하 없이 안전하게 이용할 수 있어야 한다는 점도 중요한 검토사항이었다.

■ 파이오링크 ‘웹프론트-K’를 선택한 이유는.

가장 중요한 점이 SSL 처리 성능이었다. 웹프론트-K는 경쟁제품과 비교했을 때 SSL 복호화 성능이 월등히 높았다. 다른 웹방화벽은 SSL 복호화시 성능이 대폭 하락하거나 장애가 발생하는 경우가 있었는데, 파이오링크 웹방화벽은 RSA 2048 환경에서도 안정적으로 트래픽을 복호화하고 공격을 찾아냈다.

고성능 장비를 합리적으로 제공한다는 것도 장점이었다. 웹방화벽은 분산된 환경에 여러 대의 장비를 구축해야 하기 때문에 기능과 성능이 동일하다면 제품의 가격 경쟁력도 검토하게 된다. 웹방화벽 제품 선정시 검토한 외산 솔루션의 경우 높은 성능의 제품을 도입했을 때 예산 부담이 크고, 웹방화벽 정책 설정과 운영이 키움증권 환경에 적합하지 않았다.

파이오링크 웹프론트-K는 외산제품에 비해 가격 경쟁력이 높으며, 고성능을 보장하면서도 안정적인 SSL 처리가 가능했으며, 정책 설정이 유연하고 편리해 운영이 용이하다는 장점이 있었다.

■ 웹방화벽 구축과 운영 과정에서 어려웠던 점은.

키움증권의 서비스가 100% 온라인을 기반으로 하는 만큼, 실망에서 실제로 성능과 안전성이 보장되는지 테스트 해야 했다. 키움증권 서비스는 3중망으로 고도의 안정성을 보장하고 있으며, 하나의 망에서 BMT를 진행하고 운영 중인 서비스에 실제 제품을 구축하도록 했다.

파이오링크 웹방화벽-K는 실망에서도 안전하게 테스트 할 수 있었으며, 실제 서비스에 적용됐을 때에도 서비스 중단 없이 구축해 운영할 수 있었다. 수시로 변경되는 웹방화벽 정책을 적용할 때에도 쉽고 유연하게 정책 적용이 가능했으며, 금융감독당국의 웹 보안 관련 권고사항이나 파이오링크가 자체적으로 탐지한 공격 패턴 등을 적용하는 것도 쉽게 진행될 수 있어 운영 상의 어려움은 없었다.

■ 웹방화벽을 구축하는 기업에게 조언을 해준다면.

웹방화벽은 웹 서비스에 직접적인 영향을 미칠 수 있기 때문에 운영과 관리가 어려운 솔루션으로 지목된다. 그래서 일부 보안 조직은 웹방화벽을 도입하고 정책을 전혀 변경하지 않은 채 웹방화벽을 운영하기도 하는데, 이 경우 수시로 변하는 웹 공격을 막지 못하는 무용지물로 전락하게 된다. 웹방화벽은 고객 최접점에 있는 웹을 보호하기 위한 솔루션인 만큼, 자사 비즈니스에 맞는 정책을 설정하고, 변화하는 공격 패턴에 따라 정책을 변경하면서 지능화된 공격을 막을 수 있도록 해야 한다. 또한 암호화 트래픽에 숨어 유입되는 공격을 차단하면서 고객 경험을 유지할 수 있도록 운영하는 것이 중요하다.



이성구 키움증권 정보보안팀 과장

을 선정 후 실망에 구축할 때에도 하나의 망에 적용해 운영하고 안정성을 테스트하고 다음 망에 적용하는 과정을 거쳐 서비스 중단 없이 웹방화벽 구축을 완료할 수 있었다.

이 과장은 “키움증권의 서비스가 100% 웹을 기반으로 제공되기 때문에, 실망에서 웹방화벽이 실제로 서비스에 영향을 주지 않으면서 공격을 차단할 수 있는지 확인하는 과정이 필요했다. 별도의 테스트 망에서는 잘 구동되던 제품이라도 실망에서 구동되지 않거나 장애가 발생하는 경우가 종종 발생하기 때문”이라며 “웹프론트-K는 실망에서 구동시켰을 때에도 서비스에 영향을 주지 않고 공격을 효과적으로 탐지해 내 키움증권의 요구에 딱 맞는 제품으로 평가됐다”고 설명했다.

유연한 관리 정책으로 지능형 공격 탐지 효과 높여

웹방화벽은 고객의 최접점인 웹을 제어하는 보안 제품이기 때문에 운영이 까다로운 보안 시스템으로 꼽힌다. 다양한 고객들이 여러 환경에서 접속하기 때문에 정상행위와 이상행위, 공격행위를 구분하기가 쉽지 않다.

웹방화벽 차단 정책을 강력하게 설정하면 정상 사용자의 이용을 불편하게 만들지만, 완화시키면 공격을 차단하지 못한다는 문제가 있다.

그러나 웹은 빠르게 바뀌는 환경으로, 수시로 새로운 서비스가 추가되는가 하면, 차단해야 하는 악성 URL도 수시로 변경된다. 기업/기관에서 찾아낸 공격 톨과 금융감독당국에서 탐지해 차단을 권고하는 공격도 웹방화벽에 반영해야 하며, 패턴과 임계치를 조정해 자사에 적합한 수준의 보안성을 유지해야 한다.

이처럼 복잡한 웹방화벽 정책을 수정하고 관리하는 작업은 매우 까다로우며, 자칫 잘못하면 웹 서비스에 장애를 일으킬 수 있기 때문에 웹방화벽 정책을 변경하지 않고 운영하는 경우가 많다.

키움증권 정보보안 조직에서 웹방화벽 정책 설정과 운영 등에 대한 전문적인 노하우를 갖고 있어 신변종 공격에 효과적으로 대응하고 있으며, 금융당국의 권고사항을 적극적으로 적용하는 한편, 사용자의 편의를 해치지 않도록 편의성도 보

장할 수 있다.

파이오링크 웹프론트-K는 정보보안팀의 전문성을 한층 더 높일 수 있도록 도와준다. 웹프론트-K는 웹 서비스 영향 없이 정책을 쉽게 변경하고 임계치를 조정할 수 있으며, 공격 방어 효과를 높일 수 있다. 파이오링크가 자체적으로 탐지한 공격을 웹프론트-K에 자동으로 적용해 신변종 공격에도 효과적으로 대응할 수 있다.

지능화되는 웹 공격 차단 기술 필수

웹을 통한 공격이 더욱 지능화되고 있어 키움증권은 웹 애플리케이션 개발 단계에서 시큐어코딩을 적용해 웹 취약점을 원천적으로 제거하고, 개발 완료된 서비스에 대해 철저하게 보안성 테스트를 하며, 주기적으로 모의해킹을 통해 서비스 취약점을 지속적으로 제거하고 있다. 이에 더해 차세대 웹방화벽을 도입해 지능적인 웹 기반 공격을 차단함으로써 서비스 안전성을 한차원 끌어올려 국내 1위 종합 증권사의 지위를 확고히 하고 있다.

이 과장은 “키움증권은 온라인 기반 증권 서비스가 핵심 비즈니스인 만큼, 보안에 가장 많은 투자를 진행하고 있다. 웹을 이용하는 공격을 방어할 수 있는 다양한 웹 보안 시스템을 운영하는 한편, SSL 가시성을 확보하기 위한 전문 솔루션 도입도 검토하고 있다. 더불어 수많은 보안 솔루션을 효과적으로 관리하는 분석 솔루션을 통해 은밀하게 진행되는 공격까지 차단하고 있다”고 밝혔다.

키움증권은 핀테크 시대에 맞는 새로운 서비스 개발에 많은 관심을 기울이고 있으며, 로보어드바이저를 도입해 고객의 성향·패턴을 분석해 투자자문 서비스를 제공한다. 핀테크 서비스를 위한 비대면 인증이나 클라우드 전환을 위한 신기술 투자 등에도 적극적으로 나서고 있다.

이 과장은 “핀테크 시대로 접어들면서 온라인을 기반으로 한 새로운 서비스가 제시되고 있으며, 키움증권도 이 트렌드에 맞춰 나아가 위해 지속적인 투자를 진행하고 있다. 온라인 서비스에는 반드시 보안이 뒷받침돼야 하기 때문에 온라인 서비스를 보호하는 보안 투자도 망설임없이 나서고 있다”고 말했다.