클라우드서 관리되는 보안 스위치 통해 안전한 캠퍼스 조성 … 보안·네트워크 관리 업무 향상

쉽고 편리한 클라우드 보안으로 사용자 환경 개선

대학은 수많은 학생과 교수, 연구원, 교직원이 네트워크를 사용하기 때문에 보안에 취약하다. 또한 보안 예산과 인력이 부족한 상황에서 많은 수많은 엔드포인트를 관리하는 것도 쉬운 일은 아니다. 조선대학교(총장 민영돈)는 파이오링크의 '티프론트 클라우드 보안 스위치'를 이용해 복잡한 엔드포인트 보안과 네트워크 가시성, IP 관리 등 많은 문제를 쉽게 해결했다.

〈김선애 기자·iyamm@datanet.co.kr〉

조선대학교(총장 민영돈)는 해방 직후인 1946년 7만2000여 설립동지회원이 설립한 우리나라 최초의 민립대학으로, 개성교육, 생산교육, 영재교육이라는 건학이념에 맞춰 기초학문과 응용학문이 융합 및 통섭하는 융복합의 교육철학을 갖추고, 학생 주도적으로 미래를 설계할 수 있는 교육체계를 제공하고 있다.

차세대 인재 양성을 위해 조선대는 IT 시스템에도 많은 투자를 단행하고 있으며, 학생과 교직원의 IT·네트워크 사용에 불편이 없도록 적극 지원하고 있다. 이로 인해 사이버 위협 수준도 높아졌다는 문제에 직면하게 됐는데, 사용자도 모르게 감염된 장비가 공격 통로로 이용될 가능성이 점점 높아지고 있었다.

신상철 조선대학교 정보관리팀 선생은 "대학의 네트워크 환경은 대단히 복잡해서 장애 발생과 보안 문제가 많이 발생한다. 외부에서 들어오는 공격 대응 만큼, 내부의 보안 리스크 관리도 매우 어려운 일"이라며 "특히 다수의 학생들이 사용하는 기기를 관리하는 것이 매우 어려운 일이다. 학생들이 소유한 수많은 기기에 모두 보안 정책을 적용하는 것은 불가능하기 때문에, 학생도 모르게 감염된 기기를 통해 네트워크가 감염되는 것을 막을 수 있는 방법이 시급했다"고 말했다.

클라우드 통한 중앙집중 제어 제공

조선대는 엔드포인트를 통한 위협을 방어하기 위해 보안 스위치 도입을 검토했다. 보안스위치는 사용자 단말과

가장 가까운 스위치에 보안 기능을 추가해 내부 네트워크에 접속 시 유입되는 유해 트래픽을 걸러내며, 관리자 입장에서도 네트워크를 통한 보안관리가 간편하다.

조선대는 클라우드로 관리할 수 있는 보안스위치를 도입하고자 했는데, 캠퍼스 규모상 스위치가 여러 곳에 분산 설치되고, 수량도 많아서 관리가 번거롭기 때문이다. 구축형 모델보다 클라우드를 통해 중앙에서 집중적으로 제어하고, 단일 관리 화면에서 다수 사이트를 관리할 수 있을 것으로 기대했다.

클라우드는 스위치와 컴퓨터를 일일이 연결하지 않고, 원격에서 일괄 관리할 수 있으며, 원격 장애대응이나 펌웨어 업데이트, IP관리, 정책 일괄관리 등의 이점이 있다. 사용하는 만큼 지불하며 초기 대규모 투자가 필요 없어 보안 예산을 절감할 수 있으며, 네트워크 확장에 따라 효율적으로 과금된다는 장점도 있다. 더불어 개방형 API를 통해 다양한 솔루션과 연동할 수 있기 때문에 추후 기능 확장에도 대응할 수 있을 것으로 기대했다.

자동화된 보안 관리로 보안성 강화

클라우드 보안 스위치를 도입할 때 조선대는 보안성과 관리 편의성을 가장 중요하게 생각했다. 적은 인력이 방대한 캠퍼스 네트워크를 관리해야 하기 때문에 관리자가 수동으로 개입하는 것을 최소화하고 설치와 운영, 구성변경이 일정 부분 자동화 되어 쉽게 운영할 수 있기를 원했다.

또 한눈에 확인하는 '네트워크 가시성'을 통해 서비스 중단 원인을 즉시 이해하고 예측하도록 하는 것도 관리 편의성을 위해 필요한 것이었다. 랜섬웨어나 봇 등 감염된 사용자 단말에서 내부망(랜구간)으로 확산하는 트래픽을 관리자 개입 없이 차단해야 하며, 유해 트래픽을 차단하더라도 정상 트래픽을 통한 업무와 서비스는 그대로 할 수 있도록 해야 했다. 더불어 클라우드 관리 시, 안전하게 보안통신(HTTPS)이 되어야 한다는 것도 중요한 검토 사항이었다.

조선대는 여러 경쟁 서비스를 검토한 후 파이오링크의 '티프론트(TiFRONT) 클라우드 보안 스위치'를 최종 선택했다. 특히 파이오링크의 스위치 관리 솔루션 '티컨트롤러'의 쉬운 관리 기능에 좋은 평가를 내렸다. 티컨트롤러는 여러 건물에 설치된 스위치와 연결된 단말을 중앙집중적으로 관리할 수 있으며, 하나의 관리 화면에서 NMS, QoS, ESM, NAC 기능을 사용할 수 있어 편리하고 비용 절감 효과도 있다고 판단했다.

대시보드에서 한눈에 이벤트를 확인할 수 있고, GUI 형태로 어려운 CLI 명령어 입력이 필요 없으며, 네트워크 장애시, 대시보드와 이메일, SMS로 알려주고, IP 관리와 비인가 공유기 차단, 케이블 루프나 연결 불량 등 확인으로 장애 원인을 파악 할 수 있다. 단순 하드웨어 에러일 때 원격으로 스위치를 재시동할 수 있고, 서울에 있는 제조사 엔지니어에게 원격으로 기술지원(기술지원도우미 기능 사용)을 받을 수 있었다.

신상철 선생은 "전산담당자에게 내부망 장애는 매우 골치아픈 일이다. 장애 지점과 원인을 파악하는 것도 어렵고, 보안 정책을 배포하고 관리하는 것도 쉽지 않다"며 "파이오링크 스위치 관리 솔루션 '티컨트롤러'는 직관적·중앙집중식 관리환경을 제공하고, 장애 원인 파악과 대응을 용이하게 한다. 또 기술지원 도우미 기능을 사용해 원격으로 기술지원을 받을 수 있어 적극적으로 도입을 추진했다"고 말했다.

엔드포인트·네트워크 가시성 확보

'티프론트(TiFRONT) 클라우드 보안 스위치'는 구축과정도 매우 간단했다. 스위치를 교체할 때 넓은 캠퍼스의 건물과 각 층을 돌아가면서 교체해야 하기 때문에 몇 개월의 시간이 걸린다. 티프론트 클라우드 보안 스위치는 본사 엔지니어가 설정 파일을 클라우드에 미리 업로드해 스위치를 랜케이블에 연결하면 자동으로 설정파일이 다운로드되고 수 분 내에 설치가 완료돼 신속하게 설치할 수 있었다.

신 선생은 "클라우드 보안 스위치는 스위치 별 설정정보가 자동으로 다운로드 되기 때문에 전문성이 충분하지 않은 사람들도 쉽게 구축하고 설치할 수 있어 빠르게 사업을 완료할 수 있었다. 나중에 장비를 교체할 때도 백업 없이 케이블만 연결하면 되기 때문에 교체·확장도 용이한 것으로 기대된다.

클라우드 보안 스위치 도입으로 인한 효과도 매우 만족스럽다. 엔드포인

트의 IP, 접속 시간, 트래픽 사용, 접속 애플리케이션 등의 정보는 네트워크 관리에 필요한 중요한 정보인데, 기존에는 관리 포인트가 많아 제대로 관리하지 못했고, 트러블 슈팅에 많은 리소스가 들어갔고, 네트워크가 지속적으로 확장되면서 연결 구성을 파악하는 것도 어려웠다.

보안 스위치를 감시센서로 활용해 수많은 엔드포인트에서 수집되는 다양한 정보와 네트워크 상태를 '티컨트롤러'에서 확인할 수 있어 가시성이 높아졌다. 지도와 토폴로지 맵으로 스위치 위치와 연결 구성을 관리할 수 있었다.

IP/MAC 정보, 물리포트 정보, 네트워크 속도, 링크 상태, 접속 시간, 트래픽 사용량, 연결단말의 제조사/운영체제/NetBIOS, NAT 탐지, 플로우 정보, 비정상 행위 등을 수집하며, 언제 어디서 어떤 경로로 공격이 들어왔는지 원인을 찾는데 도움이 된다.

보안 스위치는 트래픽 분석과 관리에 안성맞춤이다. 주로 확인해야 하는 스위치와 클라이언트별 트래픽 사용량 정

광범위한 캠퍼스·다양한 기기 사용하는 대학, 클라우드 보안 스위치가 최적

_ **신상철** 조선대학교 정보관리팀 선생

클라우드 보안 스위치를 도입하게 된 배경은.

넓은 캠퍼스에서 수많은 학생들이 자신의 기기를 이용해 네트워크에 접속하는 환경에서 보안과 관리 문제가 불거지게 됐다. 학생 자신도 모르게 멀웨어에 감염된 기기가 학교 네트워크에 접속해 공격자가 학교 재정, 개인정보, 학사정보 등 중요한 정보에 접근할 수 있는 가능성이 있었다. 학생들이 개인 공유기를 무단으로 연결해 루프가 발생하고 트래픽 과부하로 전교생이 인터넷을 사용하지 못하게 될 수도 있었다. 엔드포인트와 네트워크 가시성을 제대로 확보하지 못해 보안홀이 발생할 수도 있었다.

클라우드 보안 스위치는 클라우드를 이용해 중앙에서 집중관리할 수 있으며, 엔드포인트와 가장 가까운 스위치에서 유해트래픽을 차단하고 네트워크 가시성을 제공하는 솔루션이기 때문에 다양한 엔드포인트가 광범위한 캠퍼스에서 사용되는 학교 현장에 최적이라고 판단했다.

파이오링크의 '티프론트 클라우드 보안 스위치'를 선택한 이유는.

스위치 관리 솔루션 '티컨트롤러'의 쉬운 관리 기능이 조선대 환경에 최적이라고 평가했다. 티컨트롤러는 분산된 보안 스위치를 한 곳에서 관리할 수 있으며, NMS, QoS, ESM, NAC 등 여러 기능을 사용할 수 있다. 장애 지점과 원인을 신속하게 파악해 빠르게 대처할 수 있도록 하며, 옵션 추가 없이 IP 관리 기능도 이용할 수 있어 IP 충돌로 인한 문제도 미연에 방지할 수 있다.

쉬운 설치도 매우 중요한 선택 기준이었는데, 티프론트 보안 스위치가 랜케이블에 연결되면 클라우드에 업로드 된 설정 정보를 자동으로 다운받아 설치하기 때문에 전문성이 없는 사람들도 쉽게 설치할 수 있어 설치 기간을 대폭 단축할 수 있었다.

보안 스위치 도입으로 인한 효과는.

엔드포인트와 네트워크에 대한 보안성과 가시성을 획기적으로 개선할 수 있었다. 네트워크에 어떤 기기가 접속돼 있는지 확인하고 멀웨어는 엔드포인트와 가장 가까운 보안 스위치에서 차단해 내부 확산을 방지했으며, 장애를 신속하게 파악하고 대응할 수 있었다. 자동화된 IP 관리를 통해 이동성을 개선해 학생들과 교수, 교직원의 사용환경이 훨씬 자유로워졌다.

보, 보안 공격유형, 공격자, 공격대상별 정보는 아주 유용하게 사용하고 있다. 연결되는 기기가 많아지면서 IP 관리 솔루션도 필요했는데, 티컨트롤러에서 옵션 추가 없이 사용할 수 있었다. IP 관리뿐 아니라 교내 어떤 장치가 몇 개 접속했는지 알 수 있는데, 예를 들면 안드로이드 스마트폰 접속 대수, 그 중에서도 특정 브랜드의 스마트폰 접속 대 수까지 파악할 수 있었다.

유해 트래픽 차단 효과 높아

내부 보안이 향상됐다는 것은 가장 큰 효과라고 할 수 있다. 엔드포인트에서 발생하는 유해트래픽을 차단하기 때문에 위협이 내부로 확산되는 것을 미리 막을 수 있으며 스위치에서 바로 탐지/차단하기 때문에 보안 에이전트 설치 번거로움이 없다. 사용자 기기가 멀웨어에 감염됐다 해도 PC에서 가장 가까운 '티프론트'가 유해 트래픽을 차단한다. 정상 트래픽은 차단하지 않아 온라인 수업을 수강하는 중이라도영향을 받지 않는다.

조선대는 보안 스위치로 네트워크 장애를 줄이는 효과도 보았다. 학생들이 허가없이 IP를 변경하면 잘못된 IP로 중요 서비스와 충돌하고 장애가 발생하기도 한다. 와이파이 사용을 위해 개인 공유기를 무단으로 연결해 인터넷이 중단되거나 루프가 발생해 트래픽 과부하로 전교생이 인터넷을 사용하지 못하는 경우도 있다.

티컨트롤러는 IP 관리 메뉴를 통해 IP/MAC을 고정하고, 동일한 IP가 사용되면 클라우드 보안스위치에서 네트워크를 차단하고, 문제 발생시 이벤트 로그에서 확인할 수 있었다. 또 기숙사와 PC실습실 모두 인가된 DHCP를 통해 안정적으로 운영하게 됐다.

잘못된 케이블 연결이나 설정 실수로 네트워크 루프가 발생했을 때 장애 발생 지점을 찾는 것이 어려웠다. 티프론트는 루프를 발생하는 포트를 자동으로 차단할 뿐만 아니라, 티컨트롤러 대시보드에서 장애를 알려주기 때문에 대응이 편했다.

티프론트 클라우드 보안스위치는 접속 위치에 상관없이 각자의 네트워크를 통해 인터넷에 접속할 수 있다. 번거롭게 IP 변경하지 않아도 캠퍼스 내 어디서나 랜선만 꽂으면 된다. 그리고 티컨트롤러가 접속 정보를 자동으로 수집하기 때문에 보안을 유지할 수 있다.

신상철 선생은 "BYOD 환경, 무선까지 확장한 네트워크로 관리자가 파악하지 못한 수많은 단말이 내부망에 접속해 있다. 네트워크 액세스 포인트가 많다는 것은 그만큼 보안 홀도 많다는 뜻"이라며 "학생이나 직원이 스마트 기기를 사용하는 것을 막거나, 보안프로그램 설치를 강요하는 것도 현실적으로 어렵다"고 지적했다.

그는 "기존 스위치를 티프론트 클라우드 보안스위치로 교체하면, 엔드포인트를 네트워크에서 쉽게 관리할 수 있다. 특히 통합관리 솔루션 '티컨트롤러'는 스위치 관리, 단말 관리, 트래픽 관리, 보안까지 통합 관리 하기 때문에 전산담당자의 수고를 덜 수 있다"며 "적은 IT 관리 인원으로 대규모 네트워크를 안정적으로 운영하기 위해 최적의 솔루션"이라고 말했다.

파이오링크 '티프론트 클라우드 보안스위치'

파이오링크 '티프론트(TiFRONT) 클라우드 보안스위치'는 클라우드에서 쉽게 통합 관리할 수 있는, 보안기능이 추가된 스위치다. 내부 보안이 중요해짐에 따라 랜 구간 네트워크를 통해 확산하는 유해트래픽 차단 기능이 스위치에 추가됐다. 대표적으로 워너크라이 같은 랜섬웨어, DDoS 확산, 과다 트래픽 발생, 화면을 그대로 가로채는 ARP 스푸핑, 비인가 단말 접속 등을 탐지해 차단한다. 특히 클라우드 기반 통합관리시스템인 '티컨트롤러(TiController)'가 제품의 핵심으로 쉬운 운용, 보안, 가시성을 제공한다. 티컨트롤러를 통해 다수의 장비를 원격에서 중앙집중적으로 관리할 수 있으며, 티프론트 시리즈인 보안스위치, CCTV 스위치, 보안 AP, 백본스위치 등과도 결합돼 있다.