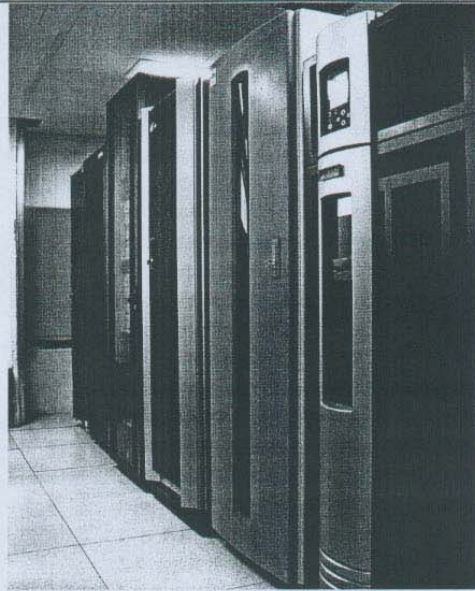


# 통합보안장비 안티바이러스 IPS 월도입

세계 · 전국지사 VPN으로 연결, 인터넷 속도도 향상

자동차 부품 제조업체 화신은 지난해 12월 안티바이러스 IPS 월을 도입했다. 화신은 안티바이러스 IPS 월 구축 이후 각종 바이러스에 영향받지 않고 네트워크를 운영할 수 있는 보안환경을 갖추게 됐다. 네트워크의 문제가 제조공정의 문제로 이어지는 상황에서 각종 네트워크에 관한 문제를 해결함으로써 제조공정의 안전을 꾀할 수 있게 된 것이다. 이번에 화신이 도입한 안티바이러스 IPS 월은 VPN, 방화벽, 웹필터링 등의 기능도 갖고 있다. 고원규 기자 wkko@ky.net



지난해 11월 자동차 부품 전문 생산업체 화신은 VPN으로 각 지사와 자회사를 연결한다는 목표를 세우고 제품 선정에 들어갔다. 몇 개 업체를 대상으로 세부사항을 확인하던 중 VPN외에 여러 가지 통합보안기능을 지원하는 제품이 있다는 사실을 확인했다.

화신의 정보기술팀은 통합보안제품을 도입하는 방향으로 VPN 프로젝트를 수정하고 해당 솔루션을 보유하고 있는 업체를 대상으로 제품 검토에 들어갔다.

## 포티넷의 포티게이트-3000 도입

화신은 각사의 제품에 대한 자체 기능분석 결과 포티넷의 포티게이트-3000을 도입하기로 잠정 결정

### ● (주)화신

1999년에 설립된 화신산업사를 모태로 자동차 Chassis 및 Body 부품을 생산하는 전문 업체이다. 지난해 1900억원의 매출을 기록했으며 현재 국내외에 8000여명의 직원이 근무하고 있다.

화신은 현대자동차, 기아자동차, 대우자동차 등 국내 자동차 회사의 내구성, 주행성 및 고효율 연비를 구현하는 기능부품 양산에 주력하고 있다. 1987년에 설립된 연구소를 중심으로 소재의 경량화와 다량화 및 부품의 최적 설계를 통해 환경 친화적인 완성차의 양산에 기여하고 있다. 회사 특성에 맞는 전산실 구축을 위해 다양한 업체의 개발제품을 통해 IT인프라를 구성할 정도로 경영진의 IT환경에 대한 관심이 높다.

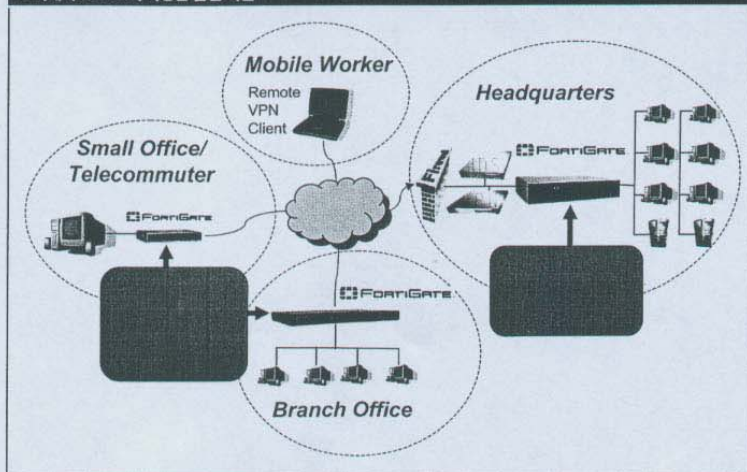
했다. 처음 도입하는 장비라 일정기간의 시험을 거쳐 장비의 안정성을 확인한 다음 제품을 도입했다. 화신의 제품 도입은 검토후 1개월만에 신속히 이루어졌다. 포티넷의 제품이 그만큼 설치하고 사용하기 쉬웠다는 반증이다.

화신의 관계자에 따르면 제품 설치는 이틀만에 끝

났다. 기존 장비를 제거하는 데 하루, 설치하고 기존 제품들과 연동성 및 정책 조율을 하는데 하루가 걸렸다는 것. 지난 2000년 화신이 ERP 시스템 도입을 검토하는 데만 6개월이 걸린 것과 비교하면 눈감작할 사이에 시스템 구축이 끝난 것이다.

장비를 구축에는 알가텔의 네트워크 장비인 백본

포티게이트 3000의 다양한 옵션 지원



출처: 포티넷

옵니 스위치 7800이 함께 사용됐다.

화신이 포티게이트를 도입해 얻어낸 효과는 크게 세 가지이다.

첫 번째, 인터넷 속도의 향상이다. 기존에 설치되었던 소프트웨어 기반의 방화벽은 전격적으로 교체될 만큼 커다란 문제점을 일으키진 않았지만 시스템의 과부하로 다운되거나 때로 인터넷의 속도를 저하시키는 원인이 됐던 것은 사실이었다. 이번 시스템 구축은 이전에 사용하던 소프트웨어 방화벽을 제거해 내부 데이터의 처리속도를 향상시켰다. 방화벽과 나머지 기능의 구동에 있어서도 속도저하는 아직까지 발견되지 않고 있다고 한다.

두 번째, 안정적인 네트워크 기반을 갖추게 되었다. 하드웨어 일체형 바이러스 윌을 도입해 바이러스, 웜 등의 혼합보안위협으로부터 벗어나게 된 것이다. 실제로 포티게이트를 구축한 후 화신은 최근 기습을 부린 신종 바이러스 썬더와 번종들의 공격에 별다른 영향을 받지 않은 것으로 전해진다.

세 번째, VPN의 활용이다. 화신은 이번 포티게이트 보안장비의 구축으로 중국 공장에 설치되어 있는 포티게이트-300과 본사의 포티게이트-3000을 VPN으로 연결해 사용하고 있다. 정보보안을 위한 안전성 확보 차원에서 미국 지사 역시 VPN으로 연결하는 작업을 진행 중에 있다. 화신은 이를 시작으로 포티게이트-3000을 이용해 현재 구축되어 있지 않은 지점의 네트워크까지 보안 적용 범위 확대한다는 계획을 갖고 있다.



▲화신이 지난 12월에 도입한 안티바이러스 IPS 윌 포티게이트-3000 통합보안장비. 구축 후 타사의 네트워크 제품들과의 연동에도 아무런 문제가 없으며 만족감을 나타내고 있다.

인터뷰 전석균 정보기술팀 대리

## “통합보안제품 구축으로 관리효율성 제고”

“기존 소프트웨어 방화벽의 단점과 다양한 기능 요구 때문에 하드웨어로 교체했다.”

전석균 화신 정보기술팀 대리는 포티넷의 통합보안장비를 도입하게 된 데는 여러 이유가 있었다고 설명했다.

전석균대리에 따르면 중국과 미국에 지사를 두고 있는 화신은 본사와의 원활한 소통을 위해 VPN을, 또 소프트웨어 방화벽의 한계를 극복하기 위해 두가지 장비의 도입과 교체를 검토하고 있었다. 아울러 다양해지는 윈도우 공격에 대응하기 위해 하드웨어 일체형 장비에 대해서도 관심을 기울이고 있었다는 것이 전대리의 설명.

전석균 대리는 이어 “통합보안장비의 도입을 결정한 이후 다른 공급업체의 추천을 통해 4개사의 제품을 저울질하던중 포티넷 3000의 가격, 기능, 성능 등이 우수하다고 판단되어 도입을 결정했다”고 포티넷 도입 배경을 설명했다.

이번 구축으로 화신은 경북 영천 본사에서 중국과 현재 구축 중인 미국까지 VPN으로 구축하게 되었다. 국내 자회사들과도 VPN 연결을 검토중에 있어 내부 의사소통의 편의성이 크게 향상될 것으로 기대된다.

전석균 대리는 “화신의 공장 시스템은 네트워크 ERP 시스템을 통해 전산화가 이루어졌기 때문에 네트워크가 죽으면 전 공정이 멈추게 된다”고 네트워크의 중요성을 강조했다. 네트워크 이 생산 공정에 그대로 영향을 미친다는 얘기이다.



화신이 도입한 포티게이트 3000의 장점을 묻는 질문에 전 대리는 특별히 관리할 것이 없으며 매뉴얼도 쉬워 신경 쓸 것이 거의 없다고 말했다. “처음 세팅한 이후 저금까지 손을 댄 적이 거의 없다”며 제품에 만족감을 나타냈다.

전석균 대리는 무엇보다 만족하고 있는 기능은 VPN이라고 말했다. 화신은 중국과 미국, 인도에 공장이 있고 국내에 지회사, 연구소, 공장을 포함 6개의 관계사가 있어 보안을 강화시킨 네트워크의 활용이 무엇보다 중요한데 VPN이 이 문제를 해결해준다는 것이다.

확을 갖고 있다. 지난해 화신에 포티게이트가 도입될 당시만 해도

통합보안장비라는 인식 자체가 부족해 ‘방화벽’, ‘바이러스 윌’ 등이 각각의 이름으로 사용자들에게 인지되었다. 고객들은 거기에 부가적인 기능이 패키지 형식으로 지원되는 것으로만 알고 있었다. 화신의 한 관계자도 처음 방화벽에 나머지 기능이 부가적으로 지원되는 것으로 알았다고 말했다.

화신이 이번에 구축한 포티게이트-3000은 안티바이러스, 방화벽, VPN, 웹필터링, IPS 등의 5가지 보안 기능 패키지로 구성되었다. 포티게이트는 본사와 2곳의 공장 네트워크를 연결하는 게이트웨이 단에 설치되었다.

### 가지 보안 기능 패키지로 구성

이번에 도입된 포티게이트-3000 시스템은 ASIC 하드웨어를 기반으로 하는 방화벽과 콘텐츠 필터링, VPN, IPS, IDS, 트래픽 관리 기능, 스팸메일 차단기능 등이 하드웨어 기반으로 구현되는 일체형 솔루션으로 대기업 및 서비스 프로바이더 등의 엔터프라이즈 애플리케이션 보호에 적합한 장비다.

## 화신에 도입된 포티게이트 3000의 특징 및 기능

### 안티바이러스

- 이메일, 웹 콘텐츠, 다운로드에 첨부되어 있는 서명, 매크로 바이러스 등을 스캔하는 바이러스 차단 기능
- 모든 이메일의 첨부 파일, 웹바이러스, 새로 등장하는 바이러스를 실시간 차단
- 포티 ASIC 콘텐츠서 집합을 이용해 HTTP 트래픽을 방어하는 동안 네트워크 속도 저하 방지
- 동시에 많은 사용자 인터넷 사용 시 바이러스 방역으로 인한 병목현상 억제

### IPS

- 34가지의 필터링 유형으로 사용자 입계처 설정 가능
- 백도어 탐지 및 DoS/DDoS 공격, 다양한 형태의 트래픽 공격 차단으로 바이러스와 웹바이러스에 의한 네트워크 고란 및 성능저하 원천적 차단
- 침입 자동 차단 기능
- 3000개 침입 탐지 패턴 분류로 오탐지율 최소화
- 사용자 침입 유형을 만들어 고객 네트워크 환경에 최적화된 침입탐지 시스템 구축
- IP Spoofing, SYN Flood, ICMP flood, UDP flood, Address sweep, Tear Drop, Winuke, Port Scan, Ping of Death, Land attack, DoS/DDoS 등의 공격 능동적 차단
- 공격이 걸리지 시 최대 3곳의 이메일 주소에 공격내용 발송

### 스팸 필터링

- 외부 SMTP 서버에서 전송되는 스팸 메일을 내부 메일 서버에 도달하기 전에 차단
- 일반 사용자들이 불편 생성으로 발도 필터링
- 키워드 별, 도메인 별, 메일계정 별 차단, 화이트 리스트 제공으로 스팸메일 차단 방식 지원

### 웹 콘텐츠 필터링

- 부적절한 내용과 악성 스크립트의 차단을 위한 웹 사이트, 웹 페이지 접속을 차단에 필요한 URL과 키워드 및 문장 검색 등을 통한 모든 웹 콘텐츠 필터링
- 야브릭, 자바 애플릿, 쿠키 등 같은 웹 플러그인을 차단하는 스크립

자체 개발한 포티ASIC(FortiASIC™) 콘텐츠 프로세서 집이 내장되어 있어 포티게이트 플랫폼을 통해 기존 네트워크를 이용할 때 성능에 저하를 초래하지 않는다. 바이러스와 웹 그리고 감염된 인터넷 브라우저, DoS/DDoS 등 기업의 내· 외부의 유해 트래픽 위험으로부터 네트워크를 보호하는 기능도 탑재되어 있다. 이와 함께 네트워크의 장애포인트와 관리포인트가 증가될 때 한 사람의 IT담당자가 관리할 수 있도록 조작 편의와 관리 효율성이 강화되

### 트 필터링

#### 바이러스 방역

- 바이러스 검색 엔진이 ASIC화
- 모든 패킷 메인 메모리 저장 후 빠른 검색
- 타사 제품 대비 최대 33배 이상의 트래픽 처리

#### 콘텐츠 기반의 검색

- 레이어7 기술을 이용해 전송 패킷 콘텐츠 수준으로 조합· 검색해 방어 체계 구축
- 패킷 헤더를 포함한 전체 내용 검색 가능
- 복수 패킷에 나누어 전송되는 바이러스 검색 가능

#### 로그 처리 옵션

- 로그를 시스템 메모리, 내장 하드디스크 또는 별도 시스템 등으로 저장
- 인터넷 트래픽 양, 시스템 일반 이벤트 공격, 공격 로그를 저장, 저장 로그 검사

#### 실시간 세션 감시

- 실시간 장비 통과 세션들의 정보들 GUI를 통해 확인
- 비정상적 클라이언트, 바이러스에 감염된 네트워크 공격 사용자 파악 용의

#### 보고서 출력

- 로그 분석기 제공, 자동 통계 및 보고서
- 알람/주말/월별로 트래픽, 백 도어 및 웹 활동현황, 바이러스 차단현황, 침입현황, 침입차단 현황, 바이러스 공격자 등 리포트 및 보고서 작성

#### 관리

- 인터넷 익스플로러 이용 원격 관리
- HTTPS로 자체 통신 보안성 강화
- 한국어, 영어, 중국어, 일본어 메뉴 등 지원
- 수백개 장비 운영 사이트에서 중앙에서 장비 모니터링, 관리

어 있다.

포티게이트-3000 내부에는 자체 개발한 포티OS(FortiOSTM) 운영 시스템이 내장되어 있다. 이 시스템은 안티바이러스, 방화벽, IPsec VPN, IDS 등 4가지 항목에서 ICSA(국제컴퓨터보안협회: International Computer Security Association) 인증을 받을만큼 객관적인 기술 우수성이 입증되어 있다. 이를 통해 네트워크를 독립적으로 구분할 수 있어 각 지역의 독립적인 보안 및 보안 정책 수립을 구현하게 해준

다. 또한 이중화된 핫 스왑(Hot Swap) 방식의 충분한 전력 공급을 바탕으로 멈추지 않는 서비스를 제공한다. 때문에 보다 효과적이고 안정된 네트워크 보안을 구축할 수 있다.

네트워크 최전방에 위치하는 네트워크 보호 게이 트웨이는 포티넷의 콘텐츠 분석시스템인 ABACAS(Accelerated Behavior and Content Analysis System) 기술을 기반으로 설계되어 있다.

ABACAS 기술은 포티게이트의 네트워크 안티바이러스(NAV) 시스템을 응용한 것으로 포티ASIC 콘텐츠 프로세서와 포티OS 운영 시스템 두 가지의 핵심 기술로 구성되어 있으며 바이러스 등에 감염되지 않아 일정한 네트워크 보안 및 콘텐츠 분석 능력을 유지할 수 있다.

포티게이트-3000은 위협요소가 발견되면 트래픽의 공격을 차단하고 공격 샘플을 포티넷 위협 응답팀(Fortinet Threat Response Team)에 전송한다.

이 곳에서는 샘플을 받는 즉시 새로운 데이터 베이스의 구축과 함께 북미와 유럽, 아시아 및 일본에 흩어져 있는 포티리스폰스 분산 서버(FortiResponse Distribution Servers)를 통해 상황에 맞는 패턴 패치를 펌웨어 형태로 전세계에 있는 모든 포티넷 장비에 푸쉬 업데이트(Push Update) 시켜 고객의 네트워크를 최적의 상태로 유지 시켜준다.

화신의 전산실장 박준근 차장은 "여러 곳에 흩어져있는 공장을 VPN으로 연결하기 위해 다양한 제품을 알아보던 중 VPN 이외에 다양한 보안 기능을 제공하는 포티게이트가 향후 전 지점을 연결하는 보안 네트워크 확장 프로젝트에 적합하다고 판단했다"며 "장비 현대의 가격으로 다양한 기능을 고객의 환경에 따라 사용 할 수 있는 TCO 절감 역시 제품 선택에 큰 영향을 끼쳤다"고 만족감을 나타냈다.

김종덕 포티넷 지사장은 "포티게이트는 국내시장 진입초기에 고객과 시장의 요구에 의해 주로 안티바이러스 기능만 사용되었다. 하지만 지난해 하반기부터 새로운 네트워크를 구축하거나 기존 장비를 제거하고 3-4개 이상의 보안 기능사용을 원하는 고객들이 늘고 있어 통합보안장비로 인정받고 있다"라고 말했다. ■