

특별기획 2_네트워크 업체 보안사업 현황과 전략

업체들은 SNMP(Simple Network Management Protocol), VLAN(가상랜), ACL(접근통제리스트), 802.1x에 기반한 인증 및 암호화 방식 등 한정된 수준이 아니라 보안 문제를 해결할 수 있는 고급 기술을 추가하고 있다.

보안 전문기술과 솔루션 확보

네트워크 업체들은 최근 몇 년간 보안업체와 제휴하거나 인수합병해 전문기술을 확보하고 있으며, 스위치나 라우터에 전문적

인 보안 기능을 추가하거나 기능별로 추가할 수 있는 임베디드 보안 모듈을 개발하는 흐름이 두드러지고 있다. 심지어는 보안 전용 솔루션을 출시해 보안시장에 출사표를 던지고 있다.

네트워크 분야의 대표주자인 시스코 시스템즈의 모습은 이같은 현실을 단적으로 보여주고 있다. 이 회사는 보안 사업을 시작한 지는 이미 오래되었지만 최근 2-3년간 특히 보안 정책과 전략을 지속적으로 업데이트하며 강화하고 있다.

또한 최근 이루어진 주니퍼 네트워크의 넷스크린 인수합병은 네트워크 업계의 보안 분야 수용이 본격화되었음을 알리는 신호탄으로 여겨지고 있다.

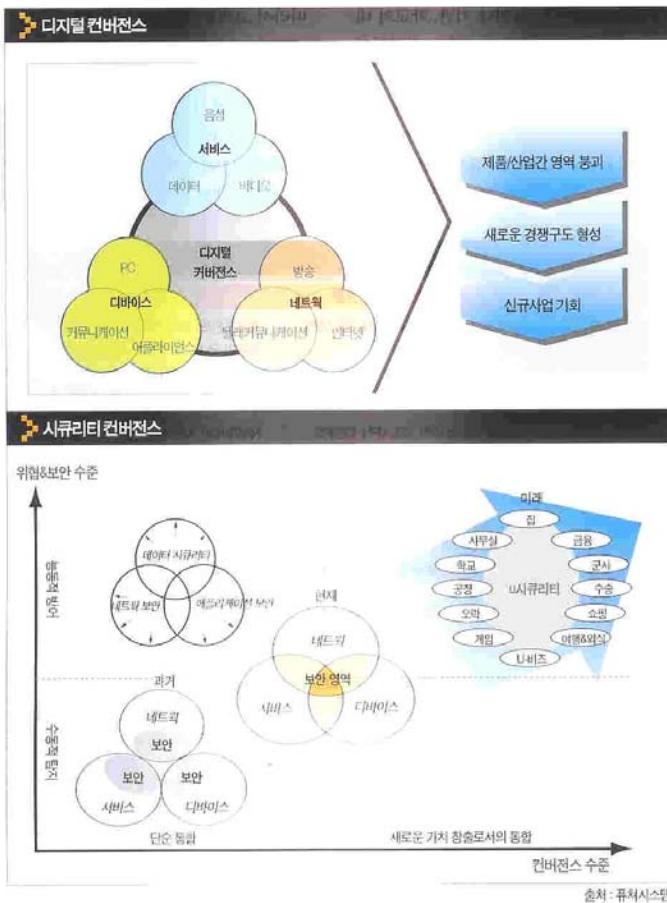
엔터라시스 네트워크는 '시큐어 네트워크'를 구성한다는 통합형 네트워크 솔루션 전략을 전면으로 내세우고 있으며, 쓰리콤 또한 '퍼베이시브(Pervasive) 네트워크 보안' 전략을 수립했다. 노텔 네트워크, 루슨트테크놀로지스, 알카텔, 엑스트라넷네트워크, 파운드리네트워크 등 대부분의 업체들도 새롭게 보안 관련 장비를 출시하는 등 적극적인 움직임을 보이고 있다.

이미 시장에서는 기존에 로드 밸런싱 장비로 활용되어온 L4/L7 스위치가 보안과 성능 문제를 동시에 해결하는 유해트래픽 차단솔루션으로 각광을 받고 있으며, QoS도 보안을 위한 주요기능으로 부각되고 있다. 뿐만 아니라 이제는 백본/에지 스위치나 라우터에 전문적인 보안 기능을 내장한 솔루션이 네트워크 보안의 해결사로 등장하고 있다.

내·외부 네트워크 전체의 통합보안기능 제공

네트워크 업체들이 강조하고 있는 보안은 인터넷 관문을 통해 외부에서 유입되는 유해트래픽에 대한 필터링만이 아니라 내부 사용자에 의해 발생한 공격, 그리고 어떠한 방식으로든 경계 보안 제품인 방화벽을 뚫고 들어온 침입을 모두 포괄한다.

인터넷 관문이라는 외부와 내부 네트워크 경계에 기본적으로 방화벽이 설치되어 있다고 볼 때, 이는 1차적인 방어체제일 뿐 유해트래픽을 100% 막지 못하기 때문이다. 또한 엑스트라넷으로 협력사 서버와 직접 연결되어 내·외부 경계가 불투명해진 환경에서 광범위한 내·외부 접점마다 보안 솔루션을 설치하기는 쉽지 않은 탓이다. 따라서 네트워크 업체들은 전체 네트워크를 보호할 수 있는 장치와 수단이 필요하며, 그 역할을 네트워크 장비인 스위치단에서 수행해



출처: 퓨처시스템



야한다고 주장하고 있다.

즉, 집의 대문에 자물쇠를 채워놓았어도 현관이나 방문을 단단히 잠그지 않으면 도둑이 들어올 수 있는 것과 같이 때문에, 이미 현관이나 방문과 같이 통로마다 설치되어 있는 장비인 스위치가 비정상 네트워크 흐름을 감지하고 차단해 보안 문제를 해결해야 한다는 것이다.

물론 단계마다 방화벽이나 IDS를 구축하고 종단의 호스트에 이르러까지 전문 보안 솔루션을 구축해 1, 2, 3차 방어체제를 겹겹이 구축함으로써 보안 문제를 해결할 수 있다. 그러나 네트워크 보호와 함께 성능과 가용성을 모두 확보해야 하는 입장에서서는 네트워크 대기시간 지연 및 대역폭 감소를 유발하는 보안 장비를 완벽하게 구비하기는 쉽지 않다. 더구나 보다 빠른 처리속도를 낼 수 있는 장비를 다수로 구입해야 하는 비용 및 관리 문제로 어려움을 증가시키는 요인이 된다. 이밖에 일부 네트워크 업체들은, 보안솔루션이 해킹이나 바이러스 등 공격을 감별해 걸러주는 기능을 하지만 정상적인 패킷의 신호를 보내오는 경우에는 이를 막는데 한계가 있기 때문에 네트워크 전반에서 이상 패킷을 골라낼 수밖에 없다는 입장을 나타내고 있다.

따라서 네트워크 업체들은 보다 효율적이고 안정적으로 네트워크를 운영, 관리할 수 있다는 이점을 내세워 시장에 걸속이 되고 들고 있다.

모듈화 및 통합화,

전용 솔루션 등 사업방식 다변

보안을 하나의 요소 기능으로 네트워크 전체에 안정성과 효율성을 제공하는 업체들의 목적은 비슷하겠지만, 세부적으로 보안을 구현하기 위한 접근방식에 있어서는 업체들마다 조금씩 차이를 보인다.

외부와 내부 전체를 강조하기 위한 솔루션을 포괄적으로 제시하는 업체가 있는 반면, 전문 보안솔루션 영역을 일정한 세 내부 이상 트래픽 모니터링을 통해 이상 유형

새로운 네트워크 환경을 위한 필요요소

네트워크의 새로운 패러다임 '5C'



- Continuity**
장비의 안정성이 아닌 비즈니스의 연속성이 보장되어야 한다.
- Context**
네트워크 인프라는 단순한 패킷 전송만을 위한 것이 아니라, 그 이상의 정보를 제공할 수 있어야 한다.(IPV6 환경의 보안)
- Control**
네트워크상의 장비를 관리하고 제어하는 것이 아니라, 비즈니스 정책에 따라 네트워크 인프라가 유기적으로 반응할 수 있어야 한다.
- Compliance**
네트워크는 비즈니스 운영 정책이 그대로 반영될 수 있어야 한다. 네트워크 접근 및 사용 내역은 곧 비즈니스의 근거이기 때문에 반드시 기록으로 관리되어야 한다.
- Consolidation**
네트워크는 더 많은 애플리케이션을 유연하게 통합할 수 있어야 한다.

출처: 엔터리시스

감지 시 조치를 취하는 네트워크 업체 고유의 관리 방식으로도 접근하고 있다.

나 세부적으로 들어가면 코어 장비(백본 스위치)에서 보안을 수행하는 경우와 에지 스위치(액세스)단의 보안 기능 제공에 집중하는 경우, 이 둘을 모두 포괄하는 경우로 나뉜다. 그리고 장비에 임베디드(모듈화)하는 방식과 소프트웨어를 탑재해 통합하는 경우, 자체 스위치나 라우터 장비에서 수행할 수 있는 정교한 네트워크 모니터링 기법을 적용해 트래픽을 정확히 분석함으로써 조치를 취하도록 하는 경우, 기본 보안 기능을 제공하면서 보안 전용 장비와 연동해 보다 높은 수준의 보안을 제공하는 방식 등이다. 물론 전문 보안장비를 내놓고 별도의 사업을 펼치는 경우도 있다.

네트워크 통합 및 임베디드 방식의 보안기능 제공 흐름은 단연 시스코 시스템즈가 주도하고 있다. 시스코는 전세계 하드웨어 보안 시장 1위라는 명성에 걸맞게 장비에 내장되는 가장 많은 보안모듈과 전용 솔루션을 구비하고 있다.

모듈 방식의 접근이 처음 시도될 시기에는 보안 기능 추가가 결국 장비 성능 저하 문제를 발생시킬 수 있다는 점에서 많은 의구심을 받아왔지만, 타 벤더들이 모듈 방식이나 보안 통합 장비를 내놓는 현 시점에서

는 고객들에게 보안 문제 해결과 네트워크 안정성 확보 면에서 가장 효율적이고 유용한 방법으로 인식되고 있는 과정이다.

시스코는 현재 방화벽, IPSec/SSL VPN, IDS/IPS(네트워크 및 호스트), 인증(ACS), 통합관리 5개 분야의 솔루션을 보유하고 있으며, 스위치에 탑재하는 방화벽과 VPN, IDS 모듈과 라우터 IOS 솔루션, 그리고 전용 장비도 갖고 있다. 최근에는 IBM과 제휴해 게정관리 분야도 추가했으며, 관리문제를 해결하기 위해 위협대응 장비인 CTR(Cisco Threat Response)도 확보했다.

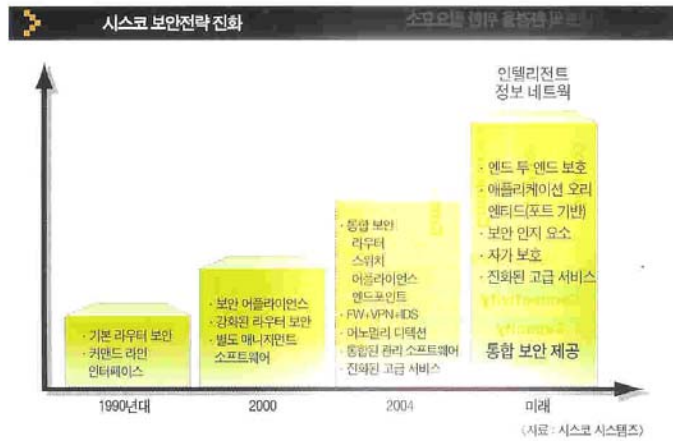
2002년에 호스트 기반 임베디드 방화벽 모듈을 내놓았던 쓰리콤은 최근 엔터프라이즈급 통합 보안 스위치인 '쓰리콤 보안 스위치 6200'를 출시했다. 이 제품은 크로스플림과 협력해 개발한 장비로, 체크포인트의 방화벽/VPN과 ISS의 IDS, 안티바이러스, 컨텐츠 필터링 기능을 지원한다.

올해 보안 스위치를 출시한 쓰리콤은 앞으로 보안 분야에 전략적으로 접근하겠다는 계획을 세웠다. 보안 분야의 업체와 협력관계를 강화해 토달 네트워크 보안 솔루션을 제공할 것이라는 것이다.

IPSec VPN과 SSL VPN 및 통합 VPN, 기가비트 방화벽, 17 스위치, 무선랜 스위치 등 다양한 네트워크 보안 장비를 보유하고 있는



특별기획 2_ 네트워크 업체 보안사업 현황과 전략



노텔 네트워크도 올 7월 백본 스위치 '세스 포트 8600'에 통합된 SDM(Service Delivery Module)을 내놓을 계획이다. 알태온 스위치에 방화벽/VPN 소프트웨어를 탑재하는 방식으로 일체감치 보안 시장에 진출했던 노텔은 이번 모듈 출시로 백본 스위치에서도 방화벽, SSL VPN, IP 아카운팅 기능을 제공하게 됐다.

주니퍼 네트워크는 지난해부터 '3프로젝트' 솔루션을 통해 방화벽, NAT (Network Address Translation) 등 보안 기능을 향상시키기 위한 노력에 나섰다. 최근 네트워크 보안 및 액세스 솔루션 전문업체인 넷스킨을 인수함에 따라 향후 보다 전문화된 보안 기술이 장비에 통합될 것으로 보인다.

정교한 네트워크 트래픽 모니터링 기술 보급

파운드리네트워크와 엑스트림네트워크는 정교한 네트워크 트래픽 모니터링 기술을 활용해 네트워크 전체를 구성요소 산더미로써 방화벽을 통과해 들어오거나 내부에서 발생한 이상 트래픽을 감지하고 신속히 대처할 수 있는 솔루션을 제공하고 있다. 이러한 방식은 하드웨어적으로 모니터링하고 처리해 장비의 부담을 최소화하며, 별도의 고가의 장비를 필요로 하지 않는다는

장점에서 비용 효율적이다.

기존에 시스템에서 사용했던 NetFlow와 비슷한 기능을 하는 RMON, 스니핑은 상시 및 동시다발적인 모니터링 할 때 성능 저하 현상이 일어나거나 별도 관리 장비를 구축해야 하기 때문에 비용면에서 부담이 되기도 했지만 이들 두 업체는 장비에 ASIC화해 이러한 문제를 해결했다.

파운드리네트워크는 sFlow(RFC3176)이라는 표준 모니터링 기술을 백본 및 모든 에지 스위치에 ASIC화했으며, 802.1x에 기반한 엔드유저의 인증과 ACL, QoS, MAC 어드레스 필터링 등과 함께 제공해 네트워크 보안 솔루션을 제공한다. 통계적인 패킷 샘플링 모니터링 기법을 통해 직관적으로 볼 수 있는 네트워크를 구성하며, 이상 트래픽을 감지, 차단한다. 특히 장비의 특정 포트와 연결되어 동일 MAC 어드레스를 가지거나 IP 스핑을 통해 수신 수만개의 13/14 세션을 발생시키는 IX가 해커의 정확한 위치를 파악해 조치할 수 있도록 한다.

엑스트림네트워크는 표준 모니터링 기법인 sFlow의 기본 기능을 기반으로 자체 패킷 모니터링 기술인 Clear Flow를 선보였다. 이 기술은 지난해 하반기 출시한 10기 가비트 백본 스위치 신제품인 '블랙다이아

몬드 10K'에 적용되어, 스위치로 인입되는 모든 패킷에 대해 하드웨어적(ASIC)으로 모니터링 한다. 일부 IDS 기능을 포함하고 있긴 하지만 IDS, 방화벽 등 보안 솔루션과 공조해 성능에 관계없이 더욱 강력한 보안 체계를 구현할 수 있도록 했으며, 이상 패킷 발생시 외부에 설치된 IDS에 통보해 자동 차단하는 기능을 수행할 수 있도록 한다. 이 외에도 익스트림은 ICMP 형태의 공격 제한, ACL, 네트워크 기반 라우팅 기능을 제공한다.

한편, 알카텔은 철저한 인증 절차를 통한 내부 보안과 사후 대응책 마련이 아니라 바이러스 감염 및 확산 방지를 위한 예방 차원의 솔루션을 제공하고 있다.

'알카텔 크리스탈섹(CrystalSec)'이라 불리는 알카텔의 보안 솔루션은 12 인증 방법을 사용하고 있다. 인증은 디바이스와 사용자 인증 두가지 방식으로 제공하고 있는데, 디바이스 인증은 디바이스 자체 인증과 디바이스로 인입되는 트래픽에 대한 보안, VLAN 및 인증 VLAN, MAC을 이용한 접근 제한을 수행한다. 사용자 인증을 위해서는 생체인식과 ID/패스워드, 스마트카드나 IC 카드를 사용할 수 있다. 지난해 하반기에는 사용자 인증 전에 PC의 바이러스를 자동 체크하는 솔루션도 추가했다.

전문 보안솔루션 신제품 출시

루센트테크놀로지도 기존 협력업체인 트렌드마이크로(안티바이러스), RSA(시큐어토큰) 외에 최근 엔터사스(IDS)와 보안 제휴를 체결하고 보안 강화에 나서고 있다.

VPN/방화벽 제품군을 보유하고 있었지만 국내에서는 공급하지 않았던 한국루센트는 지난달 업그레이드 버전인 LVF (Lucent VPN Firewall) 7.2 신제품이 출시된 것을 계기로 대화과 엔터프라이즈 시장을 대상으로 본격적인 국내 공급을 시작했다.

LVF는 방화벽/VPN 게이트웨이 어플라이언스인 '브릭'과 보안관리서버인 'LSMS (Lucent Security Management Server)'로 구



성되며, 리모트 액세스 VPN을 위한 IPSec 클라이언트도 포함하고 있다. 방화벽과 VPN 기능뿐 아니라 QoS 기능도 제공한다. '브릭'은 현재 소형 장비에서 28기가비트 방화벽 성능을 지원하는 대형 장비까지 6개 모델이 있다.

토종 스위치 장비 및 NI 업체인 콤팩시스템도 최근 보안솔루션 공급 비중을 확대하고 있다. NI업체이기 때문에 방화벽, VPN, IPS, 문서보안 등 다양한 보안 솔루션을 공급해왔지만 올해 특히 IPS 제품 공급에 힘을 쏟고 있다. 현재 방화벽으로는 시큐어아이닷컴의 제품을, VPN은 이클립정보기술과 퓨처시스템, 포트넷(안티바이러스 포함) 제품을, M3테크(유니트리스트사)의 문서보안 제품을, IPS와 보안스위치는 각각 지모컴과 인크라 네트워크의 장비를 제공하고 있다.

콤팩시스템은 네트워크를 구성하는데 있어 보안이 포함된 통합 네트워크 건설 및 구축 전략을 구사할 방침이며, 현재 자사 스위치인 '아이렉스'에도 802.1x 기반 VLAN 및 네트워크 접속 제어, 사용자 인증 기능을 제공하고 있다.

노텔 네트워크는 방화벽, VPN, 무선랜 및 L7스위치를 중심으로 한 보안 제품을 공급하고 있으며, 올해에는 특히 L7스위치인 'AAS(Aleon Application Switch)'와 지난해 초 출시한 무선랜 스위치 'WSS(WLAN Security Switch)', 지난 3월 출시한 IPSec 및 SSL VPN 통합 제품 'VPN 게이트웨이 3050'과 '컨티비티' 제품군에 집중할 방침이다. 이들 제품군은 모두 현재 초기 시장이지만 보안시장의 뜨거운 감자인 IPS와 IPSec 및 SSL VPN 통합, 무선랜 보안 분야에 해당된다.

노텔은 현재 제코포인트(방화벽)와 펄크오디세이(상호인증), 마이크로소프트(IPSec VPN)와 협력하고 있으며, 지난 3월 국내에서 바이러스 대응 능력을 높이기 위해 하우리와 바이러스 필터링 관련 제휴를 맺었다. 노텔은 패킷 형태로 네트워크 공격을 시도하는 신종 웜이나 바이러스가 발생할

때마다 바이러스 필터링 패턴을 하우리로부터 받아 'AAS'에 탑재한다.

L4/L7 스위치 공급업체인 라드웨어는 최근 L7스위치가 보안 솔루션으로 각광을 받고 있는 추세와 더불어 대학과 금융권에서 좋은 평가를 거두고 있다. 현재 L7스위치인 '에플리케이션 스위치 III(AS III)'와 지난해 말 출시한 스위치 기반 IPS '디펜스 프로' 영업에 박차를 가하고 있다.

라드웨어의 제품은 스위치 기반 제품이라는 이점으로 최대 3Gbps의 높은 처리속도를 제공하고 있다. 최근 국내업체와 공격패턴 분석 및 리포팅 기능을 제공하는 'RMS(Radware Management System)'을 개발했으며, 공격필터 자동업데이트 서비스를 제공해 스위치 기반 제품으로서의 약점도 보완했다.

이동통신 자동보호 인프라 구현

네트워크 업체들의 보안 전략은 보안 기능 추가 및 통합 솔루션 제공뿐 아니라 지능형 네트워크 관리를 통한 자동 보호체계 수립으로 빠르게 나아가고 있다.

시스코는 새로운 SDN(Self-Defending Network) 이니셔티브를 내걸고 인텔리전트 자동보호 전략 수행에 나서고 있으며, 엔터라이스도 '시큐어 네트워크' 솔루션 전략으로 최근 네트워크 환경과 침해 유형 변

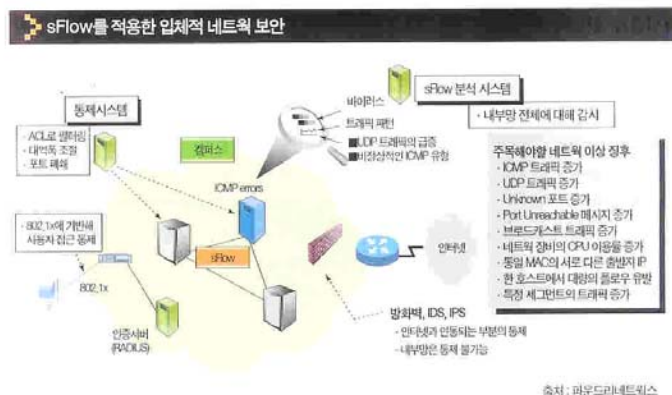
화에 대응하는 보안 지능형 인프라를 구축한다는 목표다.

시스코의 SDN은 꾸준히 추진해온 네트워크 통합 보안과 이동 산업간 협력을 통해 엔드 투 엔드 시스템 수준의 능동형 네트워크 보안을 목표로 하고 있으며, 그 1단계로 지난해 11월부터 NAC(Network Admission Control) 프로그램을 운영하고 있다.

NAC은 바이러스나 웜 등 보안 위협으로부터 네트워크 손실을 최소화하는데 초점을 둔 산업 협력 프로그램으로, 현재 네트워크 어쏘시에이즈, 시만텍, 트랜즈마이크로가 참여하고 있다.

참여 업체들과 시스코와의 상호 호환 기술을 통해 사용자의 PC나 PDA 등 디바이스가 회사의 보안 정책을 준수하고 있는지 여부를 확인, 정상일 때 네트워크에 접근해 사용할 수 있도록 하고, 비정상일 경우 백신 업데이트 등 조치를 취하게 한다. 적절한 조치가 수행되지 않는 컴퓨터 등 디바이스 사용자는 네트워크 접속이 원천적으로 차단, 고립되거나 제한된 접근만이 허용된다. 따라서 네트워크 상의 모든 호스트와 네트워크 액세스 장비, 보안정책 서버가 연동해 보안 위협으로부터 안정된 네트워크를 보장하게 된다.

시스코는 현재 호스트단의 시스코 트리스트 에이전트(CTA) API에 시스코 보안 에





특별기획 2_네트워크 업체 보안사업 현황과 전략

이전트와 백신 소프트웨어를 탑재했으며, 향후 개인 방화벽이나 호스트 IPS, 오피스 등 각종 애플리케이션까지 확장할 방침이다. 운영체제(OS) 또한 윈도우즈 외 리눅스, 솔라리스 등 타 플랫폼까지 지원하도록 확대할 계획이다. 네트워크 액세스 디바이스에 NAC 적용은 올 상반기 라우터에 먼저 이루어지며, 내년부터 스위치와 무선랜, AP 등 모든 장비에 진행할 예정이다.

엔터시스는 지난해부터 네트워크 환경과 침해 유형 변화에 따른 보안 지능형 인프라 제공을 목표로 '시큐어 네트워크' 솔루션을 제공하고 있다.

'시큐어 네트워크' 솔루션은 네트워크 내에 있는 개별 사용자가 무엇을 하려는지 미리 파악하고 변화하는 네트워크 환경에 적응해 온갖 위협을 막는 등 전체적이고 지능적으로 반응할 수 있는 네트워크(Networks That Know) 구성을 제공한다. 특히 애저단의 내부 보안에 특화된 '인텔리전트 에지' 네트워크를 구축하는 데 집중하고 있다.

지난해 내놓은 '시큐어 네트워크' 솔루션은 '메트릭스 N 시리즈' 스위치와 '드래곤 IPS', '넷사이트 아틀라스' 보안정책관리 시스템으로 구성되며, 최근 'DIR (Dynamic Intrusion Response)' 솔루션을 발표, 기존 솔루션에 통합했다. DIR은 네트워크상의 민첩적이고 비정상 행위를 탐지, 제어하며 네트워크 취약성을 찾아내 잠재 위협을 자동 완화시킬 수 있도록 하며, 기존 드래곤과 넷사이트, 네트워크 관리, 정책 기반 스위칭 인프라스트럭처와 통합되어 종합적인 기능을 수행한다. '시큐어 네트워크'는 인터넷 관문에서 있는 드래곤 IPS가 1차 침해를 감지해 차단할 수 행하며, 통합 관리인 넷사이트 콘솔에서 네트워크 서비스 정책을 넷사이트 스위치에 배포해 2차, 3차 방어/차단 조치를 수행한다.

엔터시스는 또한 인텔리전트 시큐어 네트워크 인프라 구성을 위해 최근 SNCPP (Secure Networks Certified Partner Program) 라는 파트너 프로그램을 운영하고 있다.

SNCPP 파트너들과 기술 및 서비스를 결합해 엔터시스의 자격부여, 테스트, 인증 및 컨설팅을 펼쳐 멀티벤더 네트워크 환경에서 쉽게 보안 수준을 향상시키는 데 목표를 두고 있다. 파트너 제품들은 엔터시스의 시큐어 네트워크 프레임워크 내에서 인증을 받게 된다.

파트너로 루슨트가 참여하고 있으며, 앞으로 루슨트의 VPN Firewall '브릭'을 비롯해 자동 IP 어드레스 관리 등이 시큐어 네트워크 프레임워크에 추가된다.

엔터시스는 라우터 장비인 'XSR-1800 시리즈'에서도 방화벽 및 보안관리 애플리케이션 기능을 제공한다.

내구성 및 보안업체, 장기 전략 수립 필요

네트워크 업체들의 보안 사업 진출 및 강화 흐름은 분명히 최근 이슈화 되고 있는 컨버전스 경향을 반영하고 있지만, 아직은 네트워크 업체들이 갈 길은 멀어 보인다.

'컨버전스'는 이종 산업 및 기술이 결합해 전혀 새로운 제품이나 서비스가 탄생된다는 면에서 보안에 접근하는 네트워크 업체들은 장기적인 비전 수립이 필요하다.

현 수준에서 네트워크 업체들의 보안 사업 현황을 면밀히 들여다보면 몇몇 업체를 제외하고는 그 준비 정도가 여전히 미약한 상황이고, 수익 창출에 중점을 두고 사업에 진출했다기 보다는 네트워크 분야의 경쟁력 확보의 한 요소로서나 시장 요구 반영을 위해 구축을 갖추는 수준에서 출발하고 있는 실정이다.

네트워크 업체들의 입장에서는 보안솔루션의 가격이 네트워크 장비의 10%에도 못미치는 상황에서 보안 사업에 힘을 어려움 네트워크 장비에 집중하는 것이 투자 대비 성과 면에서 더욱 효과적이다. 그리고 시장이 너무 작다는 사실은 여전히 네트워크 업체들이 보안기술 개발 등에 직접 투자하고 본격적으로 나서는 것을 망설이게 하는 요인으로 작용하고 있다. 특히 국내 시장은 K4와 CC 인증평가로 공공 및 금융시장에 진입할 수

없이 규모가 더욱 한정되어 있다.

이러한 여러 가지 요인 때문에 노텔, 루슨트, 시스코, 쓰리콤, 알카텔 등 네트워크 업체들은 보안 업체들과의 공조를 지속적으로 확대하면서 조심스럽게 보안 분야에 접근하고 있다. 그럼에도 불구하고 고객들이 점점 '보안'을 필수 네트워크 구축 및 운영 요소로 꼽고, 네트워크 업체들에게 그러한 기능을 요구하고 있다. 일단 네트워크 업체들이 보안에 두 발을 담근 이상 결국 보안 전문 업체들과의 경쟁은 불가피할 것으로 보인다. 현재에도 전면적이지는 않지만 이미 특정 영역에서 경쟁이 붙고 있으며, 앞으로 네트워크 보안 전문업체들과의 경쟁관계는 보다 첨예해질 것으로 보인다.

그렇다면 이러한 최근의 흐름에 대한 보안 전문업체들의 시각은 어떠한가. 보안업계에서도 최근 네트워크 업체와의 공조해 새로운 방향을 모색하거나 뚜렷한 장기적인 전략의 수립으로 컨버전스라는 새로운 환경에 경쟁력있게 대응할 수 있는 체제를 마련해야 할 것이라는 지적이 제기되고 있다.

현재 안티바이러스나 PC 및 서버 시스템 보안, PKI 등 비 네트워크 보안 영역의 업체들은 네트워크 업체들과 협력해 새로운 사업을 창출할 수 있는 기회로 삼을 수 있다는 점에서 네트워크 업체의 보안사업 진출에 상대적으로 느긋한 입장이다. 하지만 네트워크 보안업체들은 네트워크와 보안의 컨버전스가 일시적인 바람이 아니라 대세로 자리잡고 있어 점차 영역에 관계없이 위기로 다가올 것이며, 이를 기회로 만들기 위한 민가의 대책을 마련해야 한다고 주장하고 있다. "전문적인 기술을 제공해 경쟁력을 갖추다"는 그동안 필치는 전략의 수정이 불가피하다는 얘기이다.

시스코나 엔터시스에서 주장하는 것처럼 만약 네트워크 업체들의 지능형 보호 네트워크 구축이 현실로 다가올 때 보안 전문업체들의 입지는 여전한지 의문이라는 소리도 나오고 있다. 앞으로 보안 시장의 판도가 어떻게 재편될지 궁금하다.



업체별 보안 전략

보안 기능 강화한 신제품 출시, 전문업체와 제휴 및 인수 박차

노텔 네트워크 코리아

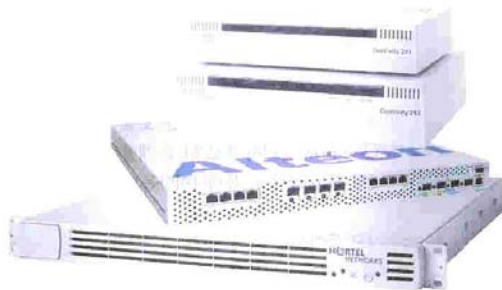
백본 스위치 부문

IPSec VPN인 '컨티미티'와 스위치 기반 방화벽 'ASF(Alteon Switched Firewall)'로 국내 시장에서 선전해온 노텔은 지난해 L7 스위치인 'AAS(Alteon Application Switch)'와 무선랜 보안스위치 'WSS(WLAN Security Switch)', 그리고 SSL VPN인 '알테온 SSL VPN'으로 IPS와 SSL VPN, 무선랜 보안 분야로 시장을 확대하고 있다.

지난 3월 IPSec VPN에 SSL VPN을 추가 제공할 수 있는 하드웨어 액셀러레이터인 'VPN 게이트웨이 3050'을 출시했으며, 하반기에 SSL 소프트웨어를 '컨티미티'에 통합 제공할 예정이다. 현재 방화벽과 상호인증, IPSec VPN 분야의 레퍼포인트와 핑크오디세이, 마이크로소프트와 협력하고 있으며, 국내 시장에 적극 대응하기 위해 최근 하우리와 제휴를 체결했다. 이에 따라 노텔은 하우리로부터 받은 바이러스 패턴을 'AAS'에 탑재한다.

올 7월에는 '메소프트 8000'에 통합된 SDM(Service Delivery Module)을 내놓고, 백본 스위치에서 방화벽, SSL VPN, IP 어카운팅 기능을 제공한다.

노텔은 다양한 신제품 출시로 올해 보안 분야에서 지난해 대비 2~3배 이상 성과를 거둘 것으로 기대하고 있다.



라드웨어 코리아

L7 스위치에 보안 기능 강화해 IPS 시장 공략

트래픽 관리와 애플리케이션 보안을 동시에 수행할 수 있는 L4/L7 스위치 업체인 라드웨어는 지난해부터 보안 시장에서 크게 두각을 나타내고 있다.

현재 대표제품격인 L4/L7 장비인 '애플리케이션 스위치 III'과 스



위치 기반 IPS인 '디펜스 프로', SMB 및 대기업 지사를 타깃으로 하는 소형 제품 '링크프루프 브랜치'를 보유하고 있으며, 대학과 기업 외에 금융권, 공공기관을 집중 타깃으로 영입을 받고 있다.

현재 보안 관리 기능을 강화하기 위해 자체 기술을 활용해 공격 필터 자동업데이트 서비스를 제공하고 있으며, 넷스큐어테크놀러지와 에이원정보기술 등 국내업체와 라드웨어 매니지먼트 시스템(RMS)을 개발해 리포팅 기능도 향상시켰다.

IPS 전용장비로 지난해 말 출시된 '디펜스 프로'는 3Gbps를 지원하며 ASIC 기반 가속기인 스트림메치 엔진을 장착해 유해트래픽 필터링을 가속화해 웹, 바이러스 등을 빠른 속도로 차단하며, 트래픽 패턴을 분석해 서비스 거부(DoS) 및 SYN(동기화) 공격도 차단한다. 올해 '애플리케이션 스위치 III'와 함께 하반기 스트림메치 엔진이 정식 탑재되면서 '디펜스 프로'에 대한 영입에 박차를 가할 계획이며, 웨이브텍 코리아와의 OEM 계약을 바탕으로 소형 스위치 IPS로 제품을 다각화할 방침이다.

올해 라드웨어의 IPS 관련 매출 목표액은 220억원이다.



특별기획 2_네트워크 업계 보안사업 현황과 전략

시스코 시스템즈 코리아

SDN 구축 권

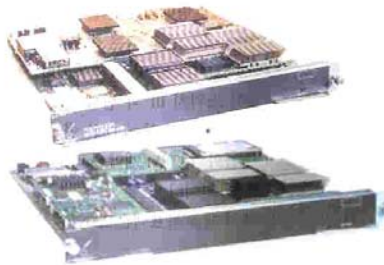
안티바이러스를 제외한 방화벽, IPSec/SSL, VPN, IDS/IPS(네트워크 및 호스트), 인증, 통행관리 등 전 분야의 보안솔루션을 보유하고 있으며, 최근 계정관리(CIM)와 위협대응 솔루션 등도 추가 확보했다. 이 중 방화벽과 VPN, IDS는 전용 장비와 스위치 임베디드 서비스 모듈, 라우터용 IDS 솔루션이 있으며, 대형 엔터프라이즈 시장에서는 특히 임베디드(모듈) 방식의 보안 솔루션에 집중하고 있다. 시스코는 최근 새로운 SDN(Software Defined Network) 이니셔티브를 내걸고 인텔리전트 자동보호 네트워크 구축에 나서고 있으며, 이 일환으로 지난해 11월부터 추진하고 있는 NAC(Network Admission Control) 기술이 스위치(기타리스트)에 적용되는 올 상반기부터 SDN 마케팅을 강화할 방침이다.

NAC은 바이러스나 웜 등 보안 위협으로부터 네트워크 손실을 최소화하는데 초점을 둔 신임 협력 프로그램으로, 현재 네트워크어쏘시어즈, 시맨텍, 트래드마크가 참여하고 있다. NAC 참여업체들은 시스코와 기술을 호환한다. NAC 기술을 적용한 네트워크에서는 사용자의 IP나 MAC 등 디바이스가 회사의 보안 정책을 준수하고 있는지 여부를 확인해 적절하지 못한 디바이스에 자동 조치를 수행토록 하며, 해당 조치가 불가능할 경우 사용자는 네트워크 접속이 원천적으로 차단되거나 제한된 접근만이 허용된다.

현재 모든 호스트단의 시스코 트러스트 에이전트(CTA) API에 시스코 보안 에이전트와 핵심 소프트웨어가 탑재되었으며, 향후 개인 방화벽이나 호스트 IPS, 오피스 등 각종 애플리케이션을 추가할 예정이다. 운영체제(OS) 또한 윈도우즈 외 리눅스, 솔라리스 등 다 플랫폼까지 지원하도록 확대할 계획이다.

네트워크 액세스 디바이스에 기술적응은 올 상반기 라우터에 먼저 이루어지며, 내년부터 스위치와 무선랜, AP 등 모든 장비에 진행할 예정이다.

지난해 보안 분야의 매출액은 700만 달러 정도로 전년 대비 30% 정도 증가했으며, 올해에도 성장세를 꾸준히 이어갈 것으로 예상하고 있다.



엔터라시스 네트워크 코리아

'시큐어 네트워크' 솔루션으로 내·외부 보안체계 수립

2000년 보안업체를 인수해 2001년 드래곤 IDS를 내놓은 엔터라시스는 지난해 10월 네트워크 환경과 침해 유형 변화에 따른 보안 지능형 인프라 제공을 목표로 한 '시큐어 네트워크' 솔루션을 내놓았다.



'시큐어 네트워크' 솔루션은 '네트릭스 N 시리즈' 스위치와 '드래곤 IPS', '넷사이트 아틀라스' 보안정책관리 시스템으로 구성되며, 최근 침입탐지 및 제어기능을 수행하는 'DIR(Dynamic Intrusion Response)' 솔루션을 기존 솔루션군에 추가 통합했다. DIR은 인터넷 관문에서 드래곤 IPS가 1차 침해를 감지해 유해 트래픽을 차단하며, 통합 관리툴인 넷사이트 콘솔에서 침입탐지 및 방어를 위한 네트워크 서비스 정책을 다시 IPS와 에지 스위치에 배포해 필요시 적절한 보안 조치를 수행, 내·외부 보안 위협으로부터 네트워크를 보호한다. 라우터의 시큐어 네트워크 솔루션으로는 'XSR-1800 시리즈'도 있으며, 방화벽 및 보안관리 애플리케이션 기능을 제공한다.

엔터라시스는 또한 인텔리전트 시큐어 네트워크 인프라 구성을 위해 최근 SNCPP(Secure Networks Certified Partner Program)을 파트너 프로그램도 운영하고 있으며, 첫 파트너로는 무순테크놀로지스가 참여했다.

올해 드래곤 IPS(엔클루와 기술 협력)의 성능을 획기적으로 개선한 버전을 출시할 예정이며, 장기적으로 10기가비트 네트워크에 적용할 수 있는 고속화된 제품을 개발할 방침이다.

보안 분야는 전체 매출액의 30% 정도를 차지하고 있으며, 올해 전년 대비 30% 정도의 성장률을 목표로 하고 있다.

익스트림네트워크 코리아

10기가비트 백본 장비에 'Clear Flow' 적용

익스트림은 표준 기법인 sFlow의 기본 기능을 수용, 보강한 자체 패킷 모니터링 기술인 'Clear Flow(클리어 플로우)'를 개발해 지난해 11월 출시한 10기가비트 백본 스위치 '블랙다이아몬드 10K'에 적용했다.

'Clear Flow'는 스위치로 들어오는 모든 트래픽을 모니터링하며, 이상 트래픽이 발생했을 때에는 외부에 있는 IDS와 운영자에



게 통보해 차단 및 조치를 수행하도록 한다. 자체적으로도 IDS 기능이 있지만 전문적인 기술을 통해 강력한 보안체제 구축을 위해 보안솔루션과 역할을 분배했다. 하드웨어적(ASIC)으로 처리해 성능 저하 현상을 극복했으며 서비스 거부 공격에 대한 CPU 자동보호 기능, 특정 IP 이더넷 공격 패턴 자동 인지 기능도 제공한다.

이외에도 엑스트림은 자체 장비에서 ICMP 패킷 처리, ACL, 네트워크 기반 라우팅 기능, 802.1x 지원 등을 제공한다. 글로벌 파트너로서 보안업체로는 넷스크린이 있다.



과 퓨처시스템, 그리고 포티넷 제품을 공급하고 있으며, MS테크(옵티트리스트)의 문서보안제품과 지모컴의 IPS, 포티넷의 안티바이러스, 인크라 네트워크의 보안 스위치를 각각 공급하고 있다.

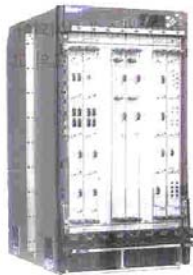
또한 자사 스위치인 '아이텍스'에도 802.1x 기반 VLAN 및 네트워크 접속 제어, 사용자 인증 기능 등을 제공하고 있다. 지난해 보안 분야 매출 실적은 100억원이며, 올해에는 160억원을 목표로 하고 있다.

주니퍼 네트워크스 중대비

기술 향상

지난해 '프로젝트'를 통해 'E-시리즈', 'T-시리즈', 'M-시리즈' 플랫폼 전반에 보안 기능을 향상시켜왔다. 특히 코어 보다는 에지 장비에서의 보안 기능 제공에 중점을 두었으며, 현재 방화벽과 NAT(Network Address Translation), 플로우 및 트래픽 모니터링 기능을 제공하고 있다.

주니퍼는 지난달 네트워크 보안 및 액세스 솔루션 전문업체 넷스클린 인수를 완료함에 따라 라우터 장비에 보다 강화된 보안 기능을 추가할 것으로 예상된다.



주니퍼는 이달 중 기술 통합 등에 대한 구체적인 전략을 발표할 방침이지만 넷스크린이 보유한 기존 방화벽/VPN과 IDP 등 제품군은 기존과 동일한 방식으로 지속적으로 공급할 것으로 보인다.

클래시스랩

VPN·보안 전용장비 공급 확대

2001년 VPN을 시작으로 보안제품을 공급하기 시작한 클래시스랩은 최근들어 보안솔루션 공급 비중을 확대하고 있으며, 특히 현재 지모컴의 IPS인 '워브레이커'에 대한 능동적인 시장 접근을 시도하고 있다.

현재 방화벽은 시큐아이닷컴의 제품을, VPN은 어울림정보기술

한국루슨트테크놀로지스

VPN/방화벽 새 비전 출시해 보안시장 본격 진출

지난달 방화벽/VPN 신제품인 'LVF(Lucent VPN Firewall) 7.2'가 출시된 것을 계기로 국내 시장에 보안 제품 공급을 시작한다. 'LVF'는 방화벽/VPN 게이트웨이 어플라이언스인 '브릭'과 보안 관리서버인 'LSMS(Lucent Security Management Server)'로 구성되며, 리모트 액세스 VPN을 위한 IPsec 클라이언트도 포함하고 있다. 또한, 방화벽과 VPN 기능뿐 아니라 VLAN, 가상 방화벽(Virtual Firewall), QoS 기능도 지원한다. 현재 '브릭'은 소호 장비에서 2.8기가비트 성능을 지원하는 대형 장비까지 6개 모델이 있다. 주 공략 대상은 대학과 엔터프라이즈 시장이며, 하반기 VoIP 솔루션과 함께 로드쇼와 솔루션 세미나 등 프로모션을 벌일 계획이다.

한편, 루슨트는 안티바이러스와 시큐이토른 분야의 트랜드마이



특별기획 2_네트워크 업체 보안사업 현황과 전략

크로와 RSA와 협력관계를 맺고 있으며, 지난해 2월 엔터사িস와 보안 관련 제휴를 체결했다.

한국쓰리콤

미래이커가 네트워크 관련 기술 수월 보안 스위치 출시

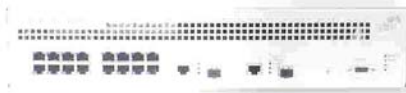
엔터프라이즈급 통합 보안 스위치인 '쓰리콤 보안 스위치 6200'을 출시한 쓰리콤은 최근 '퍼베이시브(Pervasive) 네트워크 보안' 전략을 발표하고 본격적인 보안시장 진출을 선언했다. '퍼베이시브 네트워크 보안' 전략은 주요 보안 기술을 하드웨어, 소프트웨어, 기타 네트워크 운영 요소에 집속함으로써 고객들에게 토털 보안 네트워크 솔루션을 제공하는 것을 목표로 하고 있다.

이를 위해 네트워크 장비의 보안 기능 강화뿐 아니라 네트워크 인프라에 집중시킬 수 있는 다양한 보안 전용 장비를 함께 제공하며, 자체 기술 개발뿐 아니라 협력업체와의 전략적인 협력을 동시에 진행할 방침이다.

지난달 출시된 '쓰리콤 보안 스위치 6200'은 지난해 11월 크로스비와 협력해 개발한 장비로, 체크포인트의 방화벽/VPN과 ISS의 IDS, 안티바이러스, 킨텍스 센터링 기능을 지원한다.

이밖에도 쓰리콤은 내부보안을 위한 호스트 기반 방화벽 모듈인 '쓰리콤 임메디트 프라이빗 솔루션'과 방화벽/VPN '쓰리콤 슈퍼스택 3 방화벽', 소호용 제품인 '쓰리콤 오피스가넷 VPN 방화벽' 및 '오피스가넷 시큐어 라우터'를 보유하고 있다.

올 보안 매출 비중은 전체 매출의 5% 정도를 차지할 것으로 예상하고 있다.



한국알카텔

·적 사진 예방 및 내부보안 강화

철저한 인증 절차를 통해 내부 보안과 사진 예방 차원의 솔루션 제공에 중점을 두고 있으며, 12 인증 방식을 적용한 '알카텔 크리스탈섹(CrystalSec)' 솔루션을 갖고 있다. 디바이스와 사용자 인증 두 가지로 제공하는 인증 방식은 디바이스 자체 인증과 디바이스로 입입되는 트래픽에 대해 VLAN 및 인증 VLAN, MAC을 이용한 접근통제 기능을 수행하며, 사용자 인증을 위해서는 생체인식과 II/패스워드, 스마트카드나 IC카드를 사용한다. 지난해 하반기에는 사용자 인증 전에 PC의 바이러스를 자동 체크하는 솔루션도 추

가했다.

알카텔은 현재 RADIUS 서버, LDAP 디렉토리 서버, 방화벽, VPN, 통합관리, 침입방어, 취약점 관리, 안티바이러스 등 전 보안 영역에 걸쳐 펑크소프트웨어, 마이크로소프트, 노벨, RSA, 시큐어컴퓨팅, 스톤소프트, 트립아이어, 에스피온, 넷스 크린, 네트워크어쏘시에이즈 등 총 22개 업체와 협력하고 있다.



한국파운드리네트웍스

'SFlow' 활용해 '볼 수 있고, 통제할 수 있는' 네트워크 구축

표준 모니터링 기술인 'SFlow'를 모든 스위치(백아이언, 패스트아이언) 장비에 ASIC화했다. 이 기술을 활용함으로써 네트워크 곳곳의 동시다발적인 트래픽을 모니터링하고 분석해 적절한 조치를 수행, 안정적인 네트워크 운영 환경을 보장한다는 것이다.

'SFlow'는 통계적인 패킷 샘플링 모니터링 기법을 사용하며, 802.1x에 기반한 엔드유저의 인증과 ACL, QoS, MAC 어드레스 필터링 기능 등과 함께 비정상 트래픽을 감지하고 차단 조치를 수행하도록 한다.

네트워크 전체를 구성구석 직관적으로 볼 수 있기 때문에 자칫 방화벽이나 IDS가 걸러내지 못한 이상 패킷도 잡아낼 수 있으며, 갑작스런 트래픽 폭증 시에도 즉각적인 조치를 취할 수 있다. 하드웨어적인 처리로 성능 저하 문제를 극복했으며, 기존에 설치되어 있는 네트워크 관리 서버(NMS)를 활용하면 되기 때문에 별도의 고가 장비를 구축할 필요가 없다. **kw**

