

차세대 통합네트워크 보안, '선택이 아니라 필수다'

다양한 기술 · 시장 전망 포괄적 소개 ... 뜨거운 관심속 약 400여명 참석

지난달 22일 본지가 주최한 'Next Generation Network Security Vision 2004' 세미나가 약 400여명의 기업 전산관리자 및 유수 IT 기업 관계자들이 참석한 가운데 성황리에 막을 내렸다. 각종 웜과 바이러스, 해킹 등으로부터 위협받는 기업의 사업연속성을 보장해 줄 차세대 통합네트워크 보안 솔루션에 대한 다양한 정보와 향후 전망, 기술적인 특성과 효율적인 구성방안, 적용사례 등 알찬 정보로 가득찬 이번 세미나는 참석자들의 뜨거운 열기속에 진행됐다. 그 열띤 세미나의 현장으로 들어가본다.

글 · 장운정 기자 · linda@datanet.co.kr | 사진 · 김구름 기자 · photoi@datanet.co.kr |



손영우 | 한국쓰리콤 차장
"쓰리콤은 음성 네트워크 장비에 보안기능까지 강화, 궁극적으로 데이터 유출 없이 음성, 데이터, 영상 등 모든 데이터를 단일망에서 구현할 수 있는 진정한 의미의 시큐어 컨버지드 네트워크를 지향한다"



김현수 | 한국네트워킹 협회 회장
"FS는 복잡한 네트워크 패킷과 플로우를 검사하는 시스템으로 방화벽보다 몇 배 이상의 처리능력을 갖춘 성능 및 안정성, 광범위한 데이터 캡처 모드 사용으로 강력한 포렌식 관리 및 시추조사 기능을 지원해야 한다"



이상석 | 라드웨어코리아 차장
"네트워크와 보안의 통합이 이뤄지고 있는 시점에서 스위치 기반 IPS는 O/S, 멀티 서그먼트 지원, 번 쿼리(Syncookies)를 이용한 인 플러딩 등의 효과적인 네트워크 보안을 지원할 수 있다"

국 내 기업들은 날로 지능화되고 복잡화되는 공격 및 워파 바이러스 등의 위협에 그대로 노출된 상태다. 전산시스템의 선진화에는 많은 투자를 하면서도 보안에는 턱없이 적은 예산만을 책정하는 기업 문화 때문이다. 그러나 이제 보안에 대한 투자는 선택이 아닌 필수다.

지난해 1.25대란을 통해 경험한 초유의 인터넷 미비사태는 기업 전산인프라가 아무리 훌륭하다 해도 외부로부터의 침입에 노출돼 있다면 기업연속성을 보장할 수 없다는 것을 경험했기 때문이다. 하지만 수많은 보안장비와 솔루션의 홍수속에서 어떤 보안장비로 어떤 정책을 적용해야 효율적인 보안을 구현할 수 있을지 막연했던 것이 사실이다.

이번 세미나는 무엇보다도 전산 관리자들에 높은 관심에 비해 체계적인 대안 제시에 어려움이 있었던 통합보안 시장에 대해 새로운 이정표를 제시했다는 점에서 큰 의미가 있다. 불과 몇 분이전 전 세계를 감동시킬 수 있다는 각종 욕망이 극성을 부리는 최근의 현황에서 네트워크 가용성을 보장, 기업 연속성을 지킬 수 있는 솔루션과 구성 방법 등 효과적인 보안정책에 목말라했던 관리자들에게 새로운 해답을 제시했다는 평이다.

특히 이번 세미나에서는 최근 IT 시장의 최대 관심사로 떠오른 IPS(Intrusion Prevention

System)에 대한 주제 발표가 심층적으로 논의됐으며, 통합 네트워크 보안, 콘텐츠 필터링 등에 대한 기술 및 시장 동향, 전망, 활용 방안 등이 집중적으로 소개됐다.

차세대 통합보안의 키워드 'IPS' 집중 조명

한국맥아피, 라드웨어코리아, 싸이비텍홀딩스, 셀타비전, 한국쓰리콤, 시스코시스템즈코리아, 엔터라시스네트웍스코리아, 인토스(Re6티크놀로지), 제크포인트코리아, 포트넷코리아 등 10개사 후원으로 개최한 이번 세미나는 총 10개 세션의 주제 및 발표 내용 중 차세대 보안의 화두인 IPS에 대한 주제발표가 절반이 넘는 7개를 차지해 IPS에 대한 시장의 관심을 반영했다. 특히 발표를 맡은 10개사는 세미나 장소에 데모 부스를 설치하고, 참석자들에게 자사의 솔루션을 직접 체험할 수 있는 기회를 제공해 눈길을 끌었다.

먼저 첫 번째 세션을 시작한 포트넷코리아는 '확장형 IPS를 이용한 차세대 보안'이라는 대주제 아래 IPS의 현재 및 미래, 알려진 다양한 네트워크 공격에 대한 대응방법 -eIPS라는 소주제로 세미나의 막을 열었다.

포트넷코리아의 이종열 부장은 "기존 보안 대책과 장비로는 완벽한 네트워크 방어를 위해 부족하다. 새로운 대책과 장비가 필요하다는 인식



김지윤 | 사이버트러스트 CTO
네트워크 중단없이 보안을 제공한다는 것이 얼마나 중요한지 고객들이 깨닫기 시작했으며, 가용성은 보안에서 제공해야 할 첫 번째 고려대상으로 부상했다.



조지시 | SSG네트웍로지 사장
피레이는 기가비트, 10기가비트 기반의 필터링과 데이터믹 월드 레벨 어드미니스 트레이션(Administration) 기반의 프로그래밍 관리, 그리고 스마트 데이터베이스 기반의 리포팅 지원 등의 인터넷 콘텐츠 필터링이 지원될 것이다.



안종석 | 인터넷보안 이사
'앞으로는 안전한 네트워크와 지능적인 접속이 주 관심사 될 것이며 상존하는 위협에 효과적으로 맞설 수 있는 장비에 일베드된 아키텍처로서의 보안사태가 열릴 것이다.'

아래 IPS가 탄생했다"며 "IPS는 현존하는 모든 위협을 차단해낼 수 있는 차세대 보안솔루션"이라고 언급했다. 또 이 부장은 "알려지지 않은 공격에 대응할 수 있는 딥 패킷 인스펙션을 구현, 현재 가장 각광받는 보안장비가 바로 IPS"라며 "차세대 보안시장의 관심은 콘텐츠 인스펙션으로 이행될 것"이라는 전망을 제시했다.

두 번째로 '퍼베이시브 시큐리티 네트워크(Pervasive Security Network) 구현'이라는 주제로 한국쓰리콤 손영웅 차장이 네트워크에서의 전사적인 보안방법에 대해 설명했다. 그는 "퍼베이시브 네트워크란 모든 IT 장비마다 IP네트워크가 필요하다는 개념으로 쓰리콤은 4년전부터 퍼베이시브 네트워크를 주장했다"며 "그러나 이제 보안에 대한 관심이 높아지고 있는 최근 쓰리콤은 퍼베이시브 시큐리티 네트워크로 IT에 보안이 반드시 필요하다는 점을 인식시킬 것"이라고 언급했다.

또 손 차장은 "쓰리콤의 통합보안 전략은 다양한 규모의 기업 고객이 기초부터 안전한 네트워크를 손쉽게 구축할 수 있게 하며 TCO도 절감해주는 협력적인 제안"이라며 "쓰리콤은 음성 네트워크 장비에 보안기능까지 강화해서 궁극적으로 데이터 유출 없이 음성, 데이터, 영상 등 모든 데이터를 단일망에서 구현할 수 있는 진정한 의미의 시큐어 킴바시드 네트워크를 지향한

다"고 강조했다.

다음으로 제로데이 공격을 차단하기 위한 IPS의 조건에 대해 설명한 한국백아의 김현수 팀장은 "IPS는 IDS와 달리 모든 네트워크 트래픽에 대한 완벽하고 철저한 프로토콜 분석, 새로운 공격, 변종 공격을 차단하기 위한 어노말리(Anomaly) 탐지 등 고도의 정확성을 갖춰야 한다"며 "IPS는 복잡한 네트워크 패킷과 플로우를 검사하는 시스템으로 방화벽보다 몇 배 이상의 처리능력을 갖춘 성능 및 안정성, 광범위한 데이터 캡처 모드 사용으로 강력한 포렌직 관리가 가능한 관리 및 사후조사 기능 등의 기능을 지원해야 한다"고 차세대 IPS가 갖춰야 할 조건들에 대해 상세히 설명했다.

오전의 마지막 세션을 맡은 라드웨어코리아의 이상석 차장은 스위치기반의 IPS와 L7스위치의 차이점을 주제로 IPS에 대한 참석자들의 궁금증을 해결하기 위해 IPS의 정의와 장단점, 각종 사례 등을 내놓았다.

이 차장은 "멀티 레이어 스위치와 IPS는 다양한 형태의 공격에 대한 정확한 차단과 인라인 모드에 설치되는 점 등은 같지만 QoS 기능을 지원하고 프로토콜 디스커버리 지원, 멀티 세그먼트 지원, 쿠키키(Synccookies)를 이용한 SYN 플로딩(Syn flooding) 차단, 아웃포스트 미러링 등은 스위치 기반 IPS가 갖춰야 할 장점"이라고 소개했다.



박근억 | 센터비전 보안연구소 소장
IPS는 방화벽과 네트워크 IDS를 통합한 개념이며 차세대 정보보호 시스템은 네트워크 IPS가 아닐 것이다.



김성철 | 체크포인트코리아 차장
"일일 보안 솔루션은 리포팅, 로드 밸런싱, 엔드 포인트 시큐리티, SSL VPN, IPSec VPN 등이 모두 통합돼야 할 것이다."



최우형 | 시스코코리아 과장
현대의 보안 트렌드는 자동화된 방어, 통합된 멀티미디어 보안, 시스템 레벨의 보안 서비스 등을 원하고 있다



이중열 | 포티넷코리아 부장
"기존 보안 대책과 장비로는 완벽한 네트워크 방어를 위해 부족하다. 이를 위한 가장 좋은 대안이 바로 PSC다"

보안 시장의 현안과 해결책 다각도 '모색'

오전의 세션을 마친 참석자들은 점심식사 후 오후 세미나가 시작되기 전에 후원업체들이 전시한 데모부스를 돌아보며 차세대 통합네트워크 보안에 대한 이해를 증폭시켰다. 특히 참석자들은 후원업체 스텝원 하나하나에 큰 관심을 보이며 장시간 업체들의 시연과 설명을 경청하는 등 진지한 모습을 보였다.

오후 세션의 시작은 인도스에서 국내 디스트리뷰터를 맡고 있는 8e6테크놀로지 본사 사장인 조지 시(George Shih)가 방한. 영어와 한국어를 동시통역하며 인터넷 콘텐츠 필터링의 과거와 현재 그리고 미래에 대한 자세한 설명했다.

조지 시 8e6테크놀로지 사장은 "인터넷 콘텐츠 필터링의 과거에는 캐시, 방화벽, 프록시 기반의 필터링과 IP 플랫(Flat) 프로파일 관리, 기본 로깅 또는 매뉴얼 리포트 중심이었지만 현재는 스마트 로드밸런싱에 의한 필터링, 에이전트 기반의 액티브 디렉토리 서포드 프로파일 관리, 데이터웨어하우스 기반의 리포팅 등으로 관심이 이동하고 있다"며 "미래에는 기가비트, 10기가비트 기반의 필터링과 다이내믹 필터 레벨 어드미니스트레이션(Administration) 기반의 프로파일 관리, 스마트 데이터베이스 기반의 리포팅 지원 등의 인터넷 콘텐츠 필터링이 지원될 것"이라고 설명했다.

다음으로 일찍부터 시큐어네트웍스를 주창했던 엔터라시스는 '차세대 엔터프라이즈 네트워크의 미래와 차세대 보안플랫폼과 서비스 시장'에 대해 세계 유수의 조사기관의 보안시장에 대한 전망치를 예로 들어 객관적인 현황과 전망을 제시했다.

엔터라시스의 안중석 사장은 "지난 90년대는 통신을 위한 단순 포트를 제공하는 수준에 그쳤던 보안이 Y2K를 지나 현재 위협의 이전 시대로 반응적인 보안 부지를 위한 보안을 구현하기 위해 노력중"이라며 "앞으로는 안전한 네트워크와 지능적인 접속이 주 관심이 될 것이며 상존하는 위협에 효과적으로 맞설 수 있는 장비에 임베디드된 아키텍처로서의 보안시대가 열릴 것"이라고 전망했다. 또 그는 엔터프라이즈를 위한 시큐어네트웍스에 사용될 다양한 정책, 업무 프로세스의 자동화 등과 보안이 기본 내장



된 IPv6로 현재의 네트워크 이행시에도 밀트인 보안 등이 구현되어야한다는 점을 설명했다.

통합 네트워크 보안에 대한 뜨거운 관심 반영

역시 IPS의 현황과 활용방안, 향후 전망에 대해 주제를 이은 센터비전과 체크포인트코리아, 싸이버백홀딩스는 현재 국내 고객들이 치한 보안시장의 문제점과 해결방안, 향후 전망에 대해 IPS로 이를 해결할 수 있는 다양한 해법들을 풀 어놓았다.

먼저 센터비전의 박근덕 보안연구소 소장은 "일일이 관리자의 설정이 필요로 하는 방화벽의 한계, 침입시도를 탐지하기만 하는 IDS의 한계 등으로 인해 IPS가 등장했다"며 "이런 관점에서 네트워크 IPS는 침입차단시스템인 방화벽과 침입탐지시스템인 IDS를 통합한 제품이어야 할을 기본으로 한다"고 주장했다. 또 박 소장은 최근 보안시장에서 관심이 되고 있는 공통평가기준(CC:Common Criteria)에 대해서도 설명. 참석자들의 많은 관심을 받았다.

이어 체크포인트코리아의 김성철 차장은 엔터프라이즈 환경에서의 효과적인 통합네트워크 보안 적용방안에 대해 강의했는데 점심시간 후 자칫 풀리기 쉬운 시간, 강의 중간중간 참석자들에게 퀴즈를 내고 경품을 줌으로써 참석자들의 관심을 유도했다.



김 차장은 "오늘 세미나에서 IPS에 대한 강연이 대부분을 차지해 IPS로 주제를 국한시키지 않은 점이 조금 후회되기도 하지만 현재 국내 보안시장에서 최대 화두가 되고 있는 것은 통합보안일 것"이라며 "지금까지 통합되어온 보안 솔루션은 방화벽, URL 필터, 안티바이러스, IDS, IPS 등이었으며 앞으로 통합돼야 할 보안 솔루션은 앞서의 것들을 포함해 리포팅, 로드밸런싱, 엔드 포인트 시큐리티, SSL VPN, IPSec VPN 등이 모두 통합해야 할 것"이라고 주장했다. 또 그는 "이런 통합네트워크를 구현하기 위해 고려해야 할 5가지 사항으로 보안성, 성능, 관리성, 호환성, 확장성 등을 고려, 자칫 통합에서 이런 요소들을 간과했다가는 안전하고 효율적인 기업네트워크의 지원을 보장하지 못할 것"이라고 덧붙였다.

잠시 커피 타임으로 참석자들에게 한숨들리게 한 후 시작한 세미나는 '차세대 능동보안 아키텍처'라는 주제를 내세운 싸이버텍홀딩스의 세션으로 이어졌다. 김지훈 싸이버텍홀딩스 CTO는 "고전적 정보보호 우선순위는 기밀성, 안정성, 가용성으로 가용성에 대한 고려는 보안의 주된 관심사가 아니었다"며 "그러나 이제는 네트워크 중단없이 보안을 제공한다 것이 얼마나 중요한지 깨닫기 시작했으며, 가용성은 보안에서 제공해야 할 첫 번째 고려대상으로 부상했다"고 언급했다.

마지막으로 안전한 네트워크 보안설계 방법에 대해 설명한 시스코코리아의 최우형 과장은 전자정부 기관 네트워크 구성예제, 캠퍼스네트워크 구성예제, 기업네트워크 구성예제 등의 실제 사례를 들어가며 각 네트워크들이 실제로 해결 당하는 상황을 시연하며 안전한 네트워크를 구현할 수 있는 해답을 제시했다. 최 과장은 "과거의 보안 트렌드는 리액티브(Reac-

tive), 스텟드 얼론, 제품별 지원 등이었으나 현재는 자동화된 방어, 통합된 멀티레이어 보안, 시스템 레벨의 보안 서비스 등을 원하고 있다"며 이를 위한 시스코의 셀프디펜딩 네트워크(SDN)에 대해 설명했다.

무려 400여명의 기업 전산관리자 및 유수 IT업체 관계자가 참석한 가운데 성황리에 막을 내린 이번 세미나는 오전 9시 30분부터 오후 6시까지 9시간 가까이 진행됐음에도 불구하고, 자리를 끝까지 지키는 참석자가 많아 차세대 통합보안에 대한 뜨거운 관심을 새삼 확인할 수 있었다.

정보 제공에 충실했던 강의 내용과 눈으로 직접 확인할 수 있었던 데모 시스템, 그리고 무엇보다 그 동안 효과적인 보안 정책에 대한 정보가 부족했던 사용자들에게 IPS와 네트워크 보안, 콘텐츠 필터링 등의 구성 및 발전 방향에 대한 관심 등 3박자가 고루 어우러진 가운데 열린 Next Generation Network Security Vision 2004 세미나는 효율적인 보안정책 및 활용을 위한 돌파구를 마련한 뜻 깊은 자리였다. **NT**

세미나 개요

- 주제 : Next Generation Network Security Vision 2004
- 일시 : 2004년 6월 22일 오전 9시 ~ 오후 6시 40분
- 장소 : 코엑스인터컨터넬호텔 지하 1층 하모니볼룸
- 주관 :月刊 NETWORK TIMES
- 후원 : 라드웨어코리아, 선더버전, 시스코시스템즈코리아, 싸이버텍홀딩스, 엔터시스스코리아, 인투스, 체크포인트코리아, 포터넷코리아, 한국백아피, 한국스리콤
- 경품후원 : 안철수연구소, 오리스링크코리아, 하우리, 한국메이트로소프트, 한국스리콤, 한국HP

라드웨어 / 디펜스프로

지능형 보안 제공하는 3Gbps 속도의 스위치 기반 IPS

라드웨어(대표 정윤연)의 디펜스 프로는 웹, 바이러스, 악의적인 침입 그리고 서비스거부(DoS) 등의 공격을 3기가비트의 속도로 비정상 트



▲ 라드웨어 디펜스프로

래픽을 탐지와 동시에 차단할 수 있는 스위치 기반 침입 탐지시스템(IPS)으로 다계층 레이어 애플리케이션 방어를 위해 현충 빨라지고 한 발 앞선 지능형 보안 기능을 제공해 유해 트래픽의 공격을 실시간으로 격리, 차단, 방어한다.

ASIC 기반의 고속기인 스트림패시 엔진을 장착한 디펜스 프로는 유해 트래픽 필터링을 최고 10배까지 가속화해 웹 바이러스, 트로이 바이러스를 빠른 속도로 차단하며 서비스거부, 분산 서비스거부(DDoS) 및 동기화(SYN) 공격 등에 대해서도 트래픽 패턴을 분석, 네트워크 침입과 공격을 사전에 차단한다.

효과적인 보안을 위해 인라인(inline)으로 배치된 디펜스 프로는 패킷의 크기와 무관하게 실시간으로 1천300개 이상의 라드

웨어 시큐리티 데이터베이스의 악성 공격 시그니처와 대조하는 작업을 통해 각각의 패킷마다 정밀한 검사를 실시한다. 알려지지 않은 공격은 프로토콜 변칙 검사를 이용해 탐지하는데

프로토콜 및 트래픽 이상현상을 실시간으로 인식해 DoS/DDoS와 SYN 같은 악의적인 트래픽을 실시간으로 차단한다.

디펜스 프로는 고객들이 바이러스나 웹 같은 악의적인 공격에 신속하고 효율적으로 대처할 있도록 공격 필터 자동 업데이트 서비스(Security Update Service)를 제공하는데 △ 위기 관리를 위한 일일 24시간 보안 운영 센터(SOC) 스케닝 △ 공격 필터의 일주일 단위 정기적 자동 업데이트 △ 주중 긴급 상황 발생시, 자사 홈페이지를 통한 신속한 대응 △ 특정 기업용 겨냥한 개별 공격에 대한 맞춤 필터값 제공 등으로 구성된다.

문의 : 02-3452-1240 / www.radware.com

센타비전 / 랩터 ICS

방화벽 · IDS · IPS · QoS 기능 통합한 통합보안제품

보안전문업체인 센타비전(대표 이승훈)의 '랩터(RAPTUS) ICS'는 방화벽과 IDS, IPS, QoS(Traffic Shaping) 기능을 모두 탑재한 침입방지시스템(IPS)이다. 랩터 ICS는 하나의 통합 솔루션 도입으로 관리의 편리성 증대와 더불어 전체적인 구축비용 및 유지보수 비용 절감 효과가 높으며 주요 엔진의 온 오프 모드를 제공함으로써 기존 구축된 보안 솔루션 등과의 자유로운 네트워크 보안 구성이 가능한 커널기반 기가비트 통합 보안 제품이다.



▲ 센타비전 랩터 ICS

고속의 네트워크 환경에서 랩터 ICS는 통계 엔진으로 패킷을 필터링하고 탐지엔진으로 패킷의 데이터까지 검사해 불합리한 접근과 웹, 바이러스 등을 실시간으로 탐지/차단하며 기존의 수동적인 보안 제품에 비해 차별화된 성능을 제공한다.

또한 알려지지 않은 DoS, DDoS 공격 등에 대응하기 위해 트래픽 셰이핑(Traffic Shaping)기능을 갖추고 있어서 불필요한

서비스 대역폭을 줄여 다른 서비스의 대역폭을 확보할 수 있어 보안뿐만 아니라 효율적인 네트워크 관리까지도 가능하다. 기존 IDS의 탐지 기능이 애플리케이션 레벨에서 구현됐던 것에 반하여 랩터 ICS는 커널 레벨에서 구현돼 패킷 처리의 병목 현상을 해결했으며, 방화벽 기능과 함께 IDS보다 한층 더 업그레이드된 탐지 및 차단기술을 보유하고 있는 차세대 IPS기능을 제공한다.

이러한 랩터 ICS는 게이트웨이 방식과 브릿지(Transparent) 방식 모두를 지원해 방화벽이 있는 사이트에서는 IPS와 같은 형태고, 방화벽이 없는 사이트에서는 방화벽의 역할과 IPS의 역할을 동시에 수행할 수 있으며 어떠한 구성에서도 유연하게 동작하므로 소규모 네트워크에서 대규모 네트워크까지 어디서나 적용이 가능하다.

문의 : 02-401-3547 / www.raptus.co.kr

시스코시스템즈 / 방화벽 & IDS 모듈

강력하고 신뢰성있는 엔터프라이즈급 보안 모듈

시스코시스템즈코리아(대표 김운)의 PIXR 506E 파이어월은 기존 시스코 PIX 506 파이어월의 향상된 버전으로 원격 사무실/지사 사무실 환경에 적합한 엔터프라이즈급의 보안 기능을 강력하고, 신뢰성 있는 장비에 제공해준다.

시스코 PIX 506E 파이어월은 상태 보호(Stateful) 감시 방화벽, VPN(가상사설망), 침입 차단 기능을 하나의 장치 안에 모두 포함하는 전용 보안 장비다. 또 PIX 506E는 시스코의 혁신 ASA(Adaptive Security Algorithm) 및 PIX 운영 체제를 사용해 모든 사용자들 인터넷에 접속해 있는 위협으로부터 안전하게 보호해 준다.

1,000Mbps 속도를 자랑하는 시스코 IDS 4250-XL은 부분적으로만 활용되는 여러 개의 기가비트 서버네트를 제공할 뿐 아니라 기가비트 링크가 100% 전용되는 것을 막아 주는 맞춤형 하드웨어 가속 기능을 제공함으로써 이제까지 볼 수 없었던 탁월한 성능을 발휘하는 것이 특징이다. 이 제품은 또한 기가비트 서버네트와



▲ 시스코 PIXR 506E 파이어월, IDSM-2 모듈.

트래픽 통과(traffic traversing) 스위치를 보호하는데 사용될 수 있을 뿐 아니라 간단히 하드웨어를 업그레이드해 완벽한 기가비트 성능을 구현할 수 있게 해준다. 또 모든 IDS 센서와 서비스 모듈은 네트워크 위협에 대한 폭 넓은 분석과 보호 기능을 제공해 주는 최신 IDS 소프트웨어 v. 4.0을 지원한다.

한편 카탈리스트 6500 시리즈를 위한 제2세대 IDS 서비스 모듈인 시스코 IDSM-2는 600Mbps의 성능을 제공한다. IDSM-2는 고객의 네트워크를 통과하는 패킷을 검사하고 이를 사전에 배경된 서명(signature)과 비교한 후, 이들 패킷이 파악된 각종 네트워크 공격에 부합하는 유형인지 아닌지를 검색한다. 공격을 감지하면 IDSM-2는 관리자에게 경고하고 방화벽, 라우터 및 스위치의 ACL을 가변적으로 조절하는 기능을 포함한 광범한 대응을 통하여 예방적 조치를 제공할 수 있다.

문의: 080-808-8082 / www.cisco.com/kr

사이버텍홀딩스 / 노키아 · 티펑포인트 · 임퍼바

고성능 보안기능 제공하는 종합 보안 솔루션

노키아, 티펑포인트, 임퍼바, 체크포인트 등의 보안솔루션을 국내에 공급하고 있는 사이버텍홀딩스(대표 김상배)는 최근 티펑포인트의 네트워크 IPS와 임퍼바의 호스트 IPS 등을 내놓으며 IPS 시장에 주력할 방침이다.

티펑포인트의 유니티원(UnityOne)은 ASIC 기반의 고성능 침입방지시스템(IPS)으로 기존 방화벽을 우회 통과한 사이버 침입 공격을 즉각적으로 탐지하고 사전 차단함으로써 네트워크를 보호해주는 솔루션이다.

이를 위해 실시간 네트워크 트래픽 분석을 초고속(Micro Second 단위)으로 처리해 응용 프로그램 계층(Layer 7)까지 전체 패킷 검사를 수행하며, 최근 피해가 급증하고 있는 클러스터, 소닉, 나뉘 등과 같은 최신 웜으로부터 기업 네트워크를 완벽하게 보호할 수 있다. 특히 유니티원은 영국의 보안 및 네트워크 솔루션 독립평가기관인 NSS로부터 IPS 부문에서 '골드 어워드(Gold Award)'를 획득한 바 있다.



▲ 티펑포인트 유니티원.

또한 사이버텍홀딩스에서 제공하는 임퍼바의 시큐어스피어(SecureSphere)는 기업 데이터베이스를 포함한 웹 애플리케이션에 대한 심도 있는 보호와 보안을 제공하는 웹 애플리케이션 침입방지시스템이다.

DB 센서, 웹 센서와 분석서버로 구성되어 있으며 진보된 비정상 행위 탐지 알고리즘 및 웹과 데이터베이스의 상관분석을 통해 의심되는 시스템에 대한 이상 징후(Anomalies)를 신속히 탐지하며, 동시에 시스템 및 네트워크 자원의 중단 없이 정상적인 사용자에게는 영향을 미치지 않고 해당 공격 및 공격자를 대상으로 한 즉각적인 차단을 수행한다.

또한 기존의 애플리케이션 인프라에 변경 없이 적용이 가능하며, HTTP, HTTPS, XML 및 SQL에 대한 지원으로 보다 나은 확장성 및 안정성을 보장한다.

문의: 02-785-0103 / www.cybertek.co.kr

엔터라시스 / 시큐어네트웍스

비즈니스 연속성 보장하는 차세대 네트워크 보안 솔루션

엔터라시스의 시큐어 네트워크 솔루션은 별도의 네트워크 보안 제품을 용도에 따라 하나씩 더해가는 기존방식의 접근 방식이 아니다. 엔터라시스의 네트워크 장비를 이용해 네트워크를 구성했을 때, 장비 자체의 임베디드 아키텍처를 이용해 종합적이고, 전체적인 보안기능을 갖추게 됨은 물론, 더 나아가 네트워크에서 일고자하는 모든 서비스를 원타임으로 제공하는 솔루션이다.

시큐어 네트워크의 가장 큰 이점은 네트워크 관리자가 중앙의 정책 매니저(Policy Manager) 및 NMS에서 모든 네트워크를 일괄적으로 원격 적용/관리할 수 있다는 점인데, 관리담당자는 중앙의 정책 매니저에서 다양한 정책을 세팅하고 한번의 클릭으로 네트워크상의 모든 시큐어 네트워크 장비들에게 정책을 배포, 실행케 한다. 따라서 네트워크가 크면 클수록 관리에 따



▲ 엔터라시스 매트릭스 N시리즈, 매트릭스 F시리즈

르는 비용 및 인력을 현격하게 절감함은 물론, 새로운 위협요소(웜바이러스 등)가 갑자기 출현하는 경우에도 매우 신속한 대응을 가능케 함으로써, 네트워크의 생산성 향상은 물론 네트워크 소유자의 본인의 미션크리티컬한 업무를 보호할 수 있다.

시큐어 네트워크 솔루션은 여러 가지 요소기술의 단순 조합을 통해 기능구현이 아니라, 장비 자체의 설계시부터 반영된 임베디드 아키텍처를 통하여 중앙의 정책관리자에서 일괄적으로 정책을 부여

하고, 모니터링하며, 역동적으로 수정, 리액션(re-action)이 가능한 네트워크 인프라스트럭처 자체가 보안 및 다양한 정책을 적용토록 하는 선진화되고, 통합적인 솔루션으로서 궁극적으로 고객의 시간 및 투자를 보호하고 본인의 비즈니스를 영속케 하는 차세대 네트워크 솔루션이다.

문의 : 02-2649-0700 / www.enterasys.com/kr

인토스 / 8e6 보안 제품군

대규모 네트워크에 강한 콘텐츠 필터링 & 레포팅 어플라이언스 장비

인토스(대표 정철주)는 보안전문회사인 8e6 제품군을 기반으로 인터넷상의 부적절한 콘텐츠를 효과적으로 필터링 및 관리하고, 다양한 고객의 요구에 맞는 적절한 솔루션을 제공한다.

인토스의 8e6 보안제품군 중 R3000은 대용량 네트워크 환경에서의 웹 액세스를 필터링하기 위해 제작된 최신의 하드웨어 일체형 장비다.

스탠드얼론(Stand-Alone) 솔루션으로써 기존 운영 시스템과는 독립적으로 동작하며, 어떠한 네트워크 환경에도 적용시킬 수 있다. 또한, 방화벽이나 프록시 애플리케이션에 별도의 소프트웨어를 설치하지 않으며, 기존 리소스의 사용을 필요



▲ 8e6테크놀로지 R3000, 엔터프라이즈 리포트 3.0

로 하지 않는다.

엔터프라이즈 리포트 3.0은 R3000 본래의 필터링 속도/성능이나 다른 서버/네트워크의 기능 저하 없이 인터넷 사용 현황을 리포트하는 전용 스탠드 얼론 서버 어플라이언스다. ER3.0은 독창적인 8e6 아키텍처를 기반으로 만들어진 전용 데이터 베이스이며, R3000과 연동하여 사용되고, 짧은 시간 안에 상세리포트 또는 요약 리포트를 처리하고 생성할 수 있다.

인토스는 장기적으로 인터넷 필터링, 모니터링, 리포팅 및 안티스피엄 등의 서비스를 제공하는 종합 인터넷 접속관리센터(Internet Access Management Center)로 성장하는 것을 목표로 하고 있다.

한편 8e6테크놀로지(www.8e6.com)는 미국 캘리포니아 오렌지 카운티에 위치한 회사로서, 전 세계 기업, ISP, 교육기관 등에 인터넷 접속 관리 솔루션을 제공하고 있으며, 앞선 기술은 인터넷 콘텐츠 필터링 및 카테고리 DB 분야에서 두각을 나타내고 있으며 ISP전문 업체다.

문의 : 080-0826-826 /

체크포인트코리아 / 인터스펙트

능직한 월차단기로 네트워크 내부에서 공격 차단 '확실'

체크포인트코리아(대표 손선목)의 '인터스펙트(InterSpect)'는 네트워크 내부에서 웹과 공격의 확산을 차단하고, 네트워크 영역 세분화 기능을 제공하는 내부 보안 게이트웨이이다. 인터스펙트는 기존의 네트워크 환경에 별다른 영향을 주지 않고 쉽게 설치 가능하도록 설계됐으며, 특별히 내부 보안용에 적합하도록 설계된 관리 인터페이스를 제공한다.

통합 웜방지기(Intelligent Worm Defender)는 체크포인트의 스테이트풀 인스펙션(Stateful Inspection) 및 능직적 애플리케이션(Application Intelligence) 테크놀로지를 적용한 내부 네트워크 웹 보호 장치다. 인터스펙트는 보호해야 할 네트워크 영역 간에 설치하여, 연결된 장비들로부터의 트래픽을 검사하고 위험한 트래픽을 차단함으로써 웹이 네트워크 내부에서 확산되는 것을 방지한다.

인터스펙트는 네트워크를 복수의 관리자가 정의된 보안 영역으로 세분화해 영역간의 비인가된 접속을 차단한다. 이로써 네트워크상의 사용자나 감염으로 손상된 컴퓨터가 검색이 허가되



▲ 체크포인트 인터스펙트.

지 않은 정보와 시스템에 접근하는 것을 차단할 수 있다.

특히 인터스펙트는 보안패치를 새로이 적용하는 동안에도 컴퓨터들의 검색이 가능하다. 이로써 네트워크 관리자가 패치를 검증, 설치 및 시험하는 동안에도, 감염의 위험을 완화시키는 데에 도움을 준다. 이처럼 인터스펙트는 확인된 공격 및 미확인 공격에 대해 사전에 능동적인 보호 기능을 제공하여, 기업으로 하여금 취약한 부분이 부당하게 사용되기 전에 이에 대한 방어를 할 수 있도록 도와준다. 인터스펙트는 내부 보안에서 요구되는 성능을 갖춘 장비로 이 장비는 체크포인트의 보안 운영 체제인 시큐어플랫폼(SecurePlatform)에 기반을 두고 있다.

문의 : 02-786-3303 / www.checkpoint.com

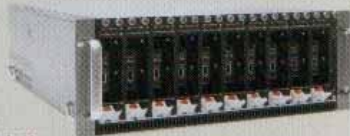
포티넷코리아 / 포티게이트 시리즈

7가지 보안기능 결합한 차세대 통합보안 솔루션

포티넷코리아(대표 김종덕)가 공급하고 있는 포티게이트(FortiGate) 시리즈는 안티바이러스, IPS, VPN, 방화벽, 콘텐츠 필터링, 트래픽 관리 기능, 스텔스 차단 등의 기능들을 하나의 박스로 통합시킨 차세대 네트워크 통합보안 솔루션이다.

포티게이트의 '안티바이러스-IPS' 특징은 네트워크 최전방인 게이트웨이에서 ASIC 기반의 기가비트 속도로 안티바이러스 기능을 수행한다는 것이다. 또한 포티게이트 안티바이러스-IPS는 현재 IPS 패킷 필터링의 주요 기술로 알려진 딥패킷인스펙션(Deep Packet Inspection) 기술이 2개 이상의 패킷에 분산되어 침입하는 웹과 바이러스를 차단할 수 없는 치명적 결함을 보완해 주는 컴플릿 콘텐츠 프로텍션(Complete Content Protection) 기능을 제공하고 있다.

이와 함께 포티넷의 컴플릿 콘텐츠 프로텍션은 기존 안티바이러스 솔루션으로 차단이 불가능했던 분산된 패킷을 리어샘블링해 분



▲ 포티넷 '포티게이트-4000'.

석함으로써 모든 종류의 웹과 바이러스 차단 기능을 제공한다.

이밖에도 안티바이러스-IPS는 복수지점에 설치된 장비들의 중앙 집중적인 관리 포인트 단순화, 빠르고 간편한 실시간 패턴 업데이트, L2(Bridge Mode) 모드 지원을 통한 네트워크 변경 없는 구축기능, IP 및 서미스별 IPS 정책 별도 지정 등의 기능을 제공한다. 한편 포티넷이 개발한 자체 포티OS(FortiOS) 운영 시스템은 IPS, 안티바이러스, 방화벽, IPSec VPN 등의 4가지 항목에서 ICSA 인증을 받았으며 네트워크를 독립적으로 구분해 각 지역의 독립적인 보안 및 보안 정책 수립이 가능해 고객의 다양한 요구를 충분히 만족시키고 있다.

포티게이트 시리즈는 설치 환경에 맞는 11가지 종류로 구분되어 있으며 크게 소호시장용 70Mbps ~ 120Mbps의 성능을 지원하는 60~200 시리즈, 200 Mbps ~ 4Gbps를 지원하는 엔터프라이즈용 300~3600 시리즈가 있다. 또 ISP나 통신회사를 대상으로 한 포티게이트-4000은 10Gbps, 포티게이트-5000은 8Gbps 성능을 지원한다.

문의 : 02-6007-2007 / www.fortinet.co.kr

한국맥아피 / 인트루시드 4000

멀티기가비트 속도 지원하는 엔터프라이즈용 IPS 솔루션

한국맥아피(대표 문경일 구 한국네트워크 이쓰시에이츠)의 네트워크기반 IPS인 '맥아피 인트루시드(McAfee Intrushield)4000'은 시그니처(signature), 이상현상(anomaly), 서비스 거부(DoS) 등 세 가지 공격에 대한 탐지능력을 결합, 통합적으로 공격을 차단할 수 있다. 실시간 네트워크 침입 탐지 및 방지 아키텍처에 기반하고 있는 맥아피 인트루시드는 다양한 네트워크 공격에 대한 통합적인 보안능력을 멀티기가비트 속도로 제공한다라는 것이 강점이다.

또한 맥아피 인트루시드는 지능적 탐지(Intrusion Intelligence) 기능을 도입, 침입 식별, 침입 경로 및 방향, 영향력, 포렌직 등에 대한 세밀하고 정확한 분석을 통해 보다 자세하고 신뢰도 높은 정보를 제공함으로써 수동적인 탐지 수준에서 한발 나아가 보다 빠르고 효과적인 능동적인 침입 방지 능력을 제공해준다.



▲ 맥아피 인트루시드

임계치 기반(threshold-based) 탐지와 특허받은 셀프러닝 프로파일 기반 탐지 기업을 결합, 현충 지능적인 DoS 탐지능력을 제공한다라는 것도 강점이다.

특히 네트워크 이용상황과 트래픽 패턴을 스스로 연구하고 터득할 수 있는 셀프러닝 능

력을 갖춰 정확성 높은 탐지능력을 제공한다. 또 하드웨어 기반의 맥아피 인트루시드는 유선속도(wire speed)를 유지하면서도 단 하나의 패킷 손실 없이 수천개의 시그니처를 지원, 엔터프라이즈 환경에 이상적인 네트워크 IPS 솔루션이다.

IPS 독립 테스트 인증기관인 NSS 그룹으로부터 2기가 속도 지원 능력을 인정받은 바 있는 맥아피 인트루시드는 프로토콜 분석, 통계 분석, 가상 네트워크 등 반복적인 작업을 빠르게 처리할 수 있도록 설계됐으며, 이를 통해 방화벽보다 8~10배 높은 처리 능력을 제공한다.

문의 : 02-3458-9800 / www.nai.com/kr

한국쓰리콤 / 퍼베이시브 네트워크 보안 솔루션

보안 스위치 · 인텔리잭 등으로 구성된 기업용 네트워크 보안 솔루션

한국쓰리콤(대표 최호원)이 공급하고 있는 기업용 네트워크 보안 솔루션은 쓰리콤의 퍼베이시브 네트워크 보안(Pervasive Network Security) 전략에 따른 것으로 대표적인 제품에는 '보안 스위치6200(Security Switch6200)', '슈퍼스택3스위치 4400 (SuperStack3 Switch 4400)', '인텔리잭 스위치 NJ220(IntelliJack Switch NJ220)' 등이 있다.

쓰리콤 보안 스위치6200은 가격 대비 성능이 뛰어난 엔터프라이즈급 네트워크 보안 스위치로서, 대기업 본사와 데이터 센터 같은 대규모 엔터프라이즈 환경에 이상적이며, 보안 애플리케이션을 폭 넓게 지원하는 통합형 보안 장비다. 다양한 애플리케이션을 지원하는 고성능 보안 플랫폼으로서 체크포인트의 NG 방화벽-1/VPN-1(NG FireWall-1/VPN-1), ISS 리얼시큐어(RealSecure)의 침입 탐지, 안티바이러스, 콘텐츠 및 메일 필터링 등의 기능 등을 지원한다. 또한 슈퍼스택3스위치4400 제품군은 스택 가능한 이더넷 스위치로서 관리가 용이하고 규모와 상관없이 모든 네트워크에 적합한 제품이다. 고급 QoS 기능이 전사적자원관리(ERP)시스템, 랜 텔레포니 및 비디오 스트



▲ 쓰리콤 '보안 스위치6200', '슈퍼스택3스위치4400', '인텔리잭 스위치 NJ220'

리밍과 같은 애플리케이션을 식별하고 우선순위를 지정해 데이터 흐름을 최적화하며 802.1x 네트워크 로그인 및 레디우스를 지원, 완벽한 유·무선 네트워크 보안을 제공한다.

쓰리콤 인텔리잭 스위치 NJ220은 네트워크 에지에 새로운 케이블을 설치할 필요 없이 벽면의 1개 포트를 4개의 이더넷 스위치 포트로 변환할 수 있는 벽면 부착형 스위치로서 네트워크 결근 제어를 위한 표준 기반의 보안 및 지능형 관리 기능이 탑재돼있다.

문의 : 02-3455-6414 / www.3com.co.kr