

'포티넷' - 사양 · 인터페이스 돋보여 ... 큰 조직에 효과적 - '서브게이트'

중소기업용 올인원 박스, '성능 · 사용 편의성' 대체로 만족

작은 회사나 원격 사무소에서 IT를 책임지고 있는 사람이

라도 컴퓨팅 자원을 소중하게 생각하기는 포춘지 500대

기업의 사람들과 마찬가지로

이다. 문제는 네트워크 보

안이 복잡한 기술이며, 아

마도 모든 세부적인 것들에 대한 여분의 IT 자

원을 갖고 있지 못할 경우가 많다는 것이다. 이 점을 염두

에 두고 *넷워크컴퓨팅*에서는 중소기업이나 지사에

적합한 하나의 박스에 진보된 보안 기능들을 담은 올인원

장비들을 테스트해 보았다.

(Hugh Smith · husmith@netprf.calpoly.edu)



우리가 요청한 것은 상황적 변화벽 기능, 장비에서의 안티바이러스 스캐닝, 침입 탐지/방지, VPN, 그리고 콘텐츠 필터링 중 최소한 네 개의 기능을 수행하는 장비들이었다. 보다 큰 조직이라면 이런 기능들을 갖춘 별도의 보안 장비를 보유하는 게 효과가 있겠지만, 규모가 작은 조직에서는 단순함이 열쇠다. 사실 조직의 규모에 관계없이 단순할수록 더 안전한 경우가 많다. 게다가 우리는 작은 세팅에 초점을 두었기 때문에 최대 인터페이스 속도를(웹, 랜, 혹은 DMZ에서) 100Mbps로 한정시켰다.

아스타로(Astaro), 포티넷(Fortinet), 서브게이트 테크놀로지스(ServGate Technologies), 소닉월(Sonic Wall) 및 시만텍(Symantec) 등이 우리 발주를 만족시켰

으며 참가에 동의했다. 크로스빔 시스템즈(Crossbeam Systems)와 ISS(Internet Security Systems)는 요구되는 기능을 갖춘 장비를 갖고 있고 두 업체 다 테스트 참여에 관심을 보였지만, 테스트 당시 두 곳 모두 보다 하이엔드의 기기비트 인터넷 장비만을 내놓은 상태였다. 시스코시스템즈는 참가를 기절했다.

우리는 캘리포니아주 샌루이스오비스에 위치한 캘리포니아 폴리테크닉 주립대학에 있는 본지 실시간 파트너 랩에 장비들을 모아 칼 폴리 넷 PRL(Cal Poly Network Performance Research Laboratory)에 구축한 테스트베드에 이들을 던져 놓았다.

규모가 작을 때 중요한 것들

중소기업을 염두에 두고 우리가 가장 먼저 질문한 것은, 'IT 지원의 부담을 최소한으로 줄이면서 우리의 작은 사무소를 보호하는 데 있어 중요한 기능은 무엇인가'였다. 참가 장비에 막대한 부하 테스트를 실시하긴 했지만, 소규모 사무소 용으로는 네트워크 부하가 구성의 편이나 포괄적인 사양 세트 만큼 중요한 게 아니라는 사실을 알고 있었기 때문에 테

Executive Summary

보안 어플라이언스

한정된 IT와 예산 자원에도 불구하고 보안을 심각하게 생각하는 중소기업과 자사용으로 나온 제품들을 살펴보기 위해 샌 루이스 오비스포에 있는 캘리포니아 폴리테크닉 주립대학에 있는 파트너 랩에 다섯 가지의 다용도 보안 장비를 모아 보았다. 요구한 기능은 상황적 방화벽 기능, 장비상에서의 안티바이러스 스캐닝, 침입 탐지/방지, 가상사설망 및 콘텐츠 필터링 가운데 최소 네 가지였다.

아스테로, 포트넷, 서브게이트, 소닉월 및 시만텍에서 테스트용 장비를 보내왔으며, 우리는 이 장비들의 모든 기능성을 철저히 점검해 보았다. 예를 들어 콘텐츠 필터링에 대해서는 80개의 포르노 및 도박 URL의 목록을 만들어 업체의 가입자 블랙리스트를 테스트했다. 안티바이러스 테스트에는 80가지 바이러스 스트림을 이메일로 장비에 통과시켜서 차단되는 숫자를 기록했다. 그런 다음에는 대용량 압축 파일을 각 장비로 통과시켜 이것이 안티바이러스 기능을 막지 않는지를 확인했다.

결과적으로는 모든 장비가 만족스러웠다. 하지만 직관적 인터페이스가 핵심 셀링포인트라는 생각에서 포트넷 포트게이트-60을 에디터즈 초이스로 선정했다. 보다 규모가 큰 조직이라면 서브게이트 에지포스를 눈여겨 보기 바란다. 약간 비싸긴 하지만 강력한 작업처리량과 인상적인 사양들을 갖추고 있기 때문이다.

스트 계획을 짤 때 이 점을 염두에 두었다. 우선 하나의 웹 인터페이스와 하나의 공용 IP 어드레스를 이용해 소규모 사무소 네트워크를 구성했다.

내부적으로 이 작은 사무소에는 전용 IP 어드레스와 웹, 이메일 및 FTP 서버용 DMZ가 있는 하나의 로컬 네트워크가 있었다. 랜 사용자는 DHCP를 이용해 구성됐으며, 보안 장비들은 DMZ와 랜 트래픽 모두용으로 NAT(Network Address Translation)를 제공했다. 장비들은 또한 웹과 DMZ 서버간의 트래픽 포트 전송도 책임졌다.

제품간 성능 큰 차이 없어

아무리 좋은 올인원 장비라 하더라도 보안에 대한 모든 근심을 덜어주진 못하겠지만(여전히 패치 작업을 해야 하고 데스크톱 방화벽이 필요할 것이다), 전체적으로 장비들은 만족스러운 수준이었다.

장비는 우리와 바깥 세계 사이에 놓였기 때문에, 트래픽 필터링, NAT 및 포트 전송 등과 같은 방화벽 기능들을 갖추고 있어야 했다. syn이나 smurf와 같은 DoS(Denial of Service) 공격을 막기 위한 상황적 방화벽 기능이 있다면 금상첨화다. 게다가 일부 작은 조직에서는 이런 장비가 DHCP 및 DNS 서버로 작동하기를 원하기도 할 것이다. 모든 제품이 우리가 찾는 기본적인 방화벽 기능들을 제공했지만, 포트넷과 소닉월 장비는 DNS 서버로 작동할 수 없었으며, 시만텍 장비는 DHCP 기능을 제공하지 않는다.

방화벽을 정확히 구성했고, 서버와 데스크톱 운영시스템이 최신 것이라고 가정한다면, 조직에의 최대 위협은 사용자에 의해 외부에서 보내지는 트래픽이다. 따라서 우리는 장비들의 인스트림 안티바이러스 기능을 살펴보았는데, 이는 곧 장비가 수신되는 이메일과 FTP 및 웹 트래픽에 바이러스 스캐닝을 실시하는 것을 의미한다. 이러한 스캐닝은 데스크톱 안티바이러스 소프트웨어가 하는 것과 유사하다. 바이러스가 발견되면 장비는 이메일을 유실, 유실 및 송신자에게 경고, 경고와 함께 전송, 혹은 격리시도록 구성될 수 있다. 소닉월의 장비만이 바이러스 스캐닝을 지원하지 않았는데, 대신 이것은 데스크톱 중심의 방안을 채택하고 있었다.

포트넷에는 강력한 안티바이러스 솔루션이 있으며, 그 장비는 목록에 있는 모든 프로토콜에서 바이러스 스캐닝을 지원한다는 점에서 독특했다. 아스테로나 서브게이트 장비는 어떤 것도 HTTP 트래픽을 스캐닝할 수 없었으며, 모든 업체들이 바이러스 서명을 최신으로 유지하기 위해 연간 유료 가입을 요구했다.

또 한 가지 위협은 방화벽을 통해 허용된 트래픽에서 서버에 가해지는 공격이다. 여기가 바로 침입 탐지/방지 방안이 적용되는 곳이다. 우리는 하나의 아이템 아래 DoS 공격 탐

지, 침입 방지 및 침입 탐지 그룹을 나누었다. 보안 업계 전문가들은 여기에 동의하지 않을지도 모르지만, 이러한 작업들은 모두가 누군가 당신의 시스템에 모종의 작업을 시도하고 있다는 사실을 파악하기 위한 모니터링과 관련되는 것이다.

침입 탐지를 수행하는 보안 장비의 경우는 딥 패킷 검사기를 이용하여 하며 애플리케이션을 웹, 이메일, 혹은 FTP 서버인 채로 이해해야 한다. 업체들은 이러한 기능을 갖추는 데는 발이 느린 편으로, 테스트한 장비들 중 시만텍과 포티넷 두 곳에서만 전통적인 IDS로 알려진 기능을 자랑했다. 시만텍은 IDS 이행에 있어 포티넷보다 한단계 더 나아가 네트워킹 트래픽의 빈치적인 행동을 역동적으로 모니터링하는 알고리즘도 또한 제공하고 있다. 다른 업체들의 장비에는 제한된 공격 방지 기능은 있었지만(예를 들어 DOS 공격에 대한 것 등), 딥 패킷 검사는 수행하지 않았다.

콘텐츠 필터링은 장비가 원치 않는 사이트를 얼마나 잘 차단할 수 있도록 해주는가를 다루고 있다. 우리는 각각의 보안 장비에 URL 블랙리스트를 제공했는데, 이는 곧 가상의 우리 사용자들이 액세스가 허용되지 않는 사이트들을 말한다. 테스트에 참가한 모든 업체가 포르노나 게임 등의 그룹별로 URL 블랙리스트를 관리하는 유료 가입자 서비스로서의 액세스를 제공했으며, 원하는 경우는 이 블랙리스트를 수동으로 업데이트할 수 있었다.

시만텍은 블랙리스트를 장비로 직접 다운로드했으며, 외부 서버에서 지원되는 목록과 최근의 목록만이 장비에서 캐싱된다. 블랙리스트 외에, 포티넷과 시만텍 장비는 우리가 파일 유형(.exe나 .bat 등)을 기반으로 콘텐츠 필터링을 수행할 수 있게 해주는 한편, 시만텍을 제외한 모든 장비는 수동으

로 입력된 키워드나 문구를 기반으로 트래픽을 필터링하기도 했다.

그리고 마지막으로 장비들의 VPN 이행을 평가했다. 소규모 사무소 시나리오임을 감안해 우리는 CO나 다른 원격 사무소로 한정된 수의 VPN 터널을 셋업하는 데 주로 관심을 두었다. 따라서 얼마나 많은 터널이 설정될 수 있는지를 따져보았다기보다는 적은 수의 터널에서 오는 트래픽의 효과를 살폈다. 테스트에서는 VPN 트래픽용 작업처리량과 대기시간을 살펴보았을 뿐만 아니라 정상적인 암호화되지 않은 트래픽에 미치는 그 영향도 조사했다. 모든 장비는 기본적인 VPN 테스트에서 잘 수행했으며, 그 가운데서도 시만텍의 제품이 가장 강력한 하이엔드 VPN 수치를, 서브게이트가 그에 근접하는 두 번째 수치를 내놓았다.

관리와 이용 편이

IT 자원이 한정된 조직에서는 장비의 관리 인터페이스가 협상을 가로막는 요소(deal breaker)가 될 수 있다. 기능을 적절히 구성할 수 없거나 메뉴얼을 공부하느라 며칠씩 보낼 필요 없이 이것이 적절히 작동하고 있는지를 파악할 수 없다면 아마도 보안에 대해 잘못 이해하고 있기 때문일 것이다. 따라서 우리는 각 장비의 관리 인터페이스를 면밀하게 살펴 보았으며, 그 결과 보안이 복잡한 문제긴 하지만 구성이 반드시 어려울 필요는 없다는 사실을 알 수 있었다. 물론, 예를 들어 '프록시나 중계 에이전트를 켜시오'라고 알리는 메시지 박스가 'SMTP 트래픽용 안티바이러스를 켜시오'라고 말해주는 체크박스만큼 유용한 것으로 평가되지 않는다는 점을 비롯해 개선의 여지는 있었다.

올인원 보안 장비, “만병통치약은 아니다”

이러한 올인원 보안 장비들은 유용하긴 하지만 만병통치약은 아니다. 방화벽, 안티바이러스, 콘텐츠 필터링 및 IDS 의무를 수행하는 제대로 구성된 예지 장비가 있다 하더라도 내부 보안에 대해서 경계를 늦추서는 안되는데, 내부 보안으로는 다음과 같은 것들이 포함된다.

- ▶ **워크스테이션 방화벽:** 각 방화벽은 소프트웨어 방화벽을 돌려야 하며 그것도 정기적으로 해야 한다. 많은 패키지들이 나와 있지만 그 중에서도 특히 존랩스 존 알람 프로(ZoneLabs Zone Alarm Pro)나 시만텍의 안티바이러스/방화벽 통합 패키지를 추천한다.
- ▶ **OS 업데이트:** 마이크로소프트는 매일 첫

째 토요일에 중요한 윈도우 업데이트를 발표하고 있다. 모든 윈도우 기계는 윈도우 업데이트 기능을 이용해 매일 업데이트해야 한다.

▶ **안티바이러스 소프트웨어:** 모든 워크스테이션에는 안티바이러스 소프트웨어가 필요하다. 예지 보안 장비가 스캐닝할 수 없는 펌웨어 보호, zip 파일을 통해 바이러스는 너무도 쉽게 네트워크를 통과할 수 있다. 전체 조직에 고통을 주는 데는 한 장의 감염된 디스크만 있으면 충분하다.

▶ **서버 백업:** 보안 전략의 일부로 백업이 포함되어야 한다. 이것은 마지막 방어선이라고 할 수 있으며, 지원되는 모든 조직에서는 백업을

매일 스스로 확인해보는 게 중요하다. 그렇지 않을 경우 웹이 서버를 점령하고 나서야 백업을 담당하는 사람이 두달 전 상태로 내버려 뒀다는 사실을 알게 될 것이다.

소규모 조직에서는 각각의 워크스테이션과 서버 상태를 현재로 유지하는 데 많은 작업이 필요치 않다. 월급을 받는 날마다 매일 관리자가 각 장비에 정확한 업데이트가 돼 있는지를 점검해볼 수 있다. 점검해야 할 것들에 대해 목록을 쉽게 만들 수 있으며, 새로운 바이러스나 웜이 발표될 때 많은 돈을 절약할 수 있을 것이다.

먼저 전체적인 장비 파라미터와 방화벽 규정 및 정책을 구성하는 데 있어서의 편이를 살펴 보았다. 그런 다음 안티바이러스, 콘텐츠 필터링, 침입 탐지 및 방지 등과 같은 고급 사양을 구성하는 데로 이동했다. 그 결과 사용자 인터페이스를 이행하는 방법에 있어 역할 모델은 소닉월이었다. 그 인터페이스에는 마법사가 있어 기본적인 장비 구성과 방화벽 규정 세트를 도와주었으며, 고급 사양을 구성하는 일은 매우 직관적이었다. 시만텍과 아스테로 장비에서 고급 사양을 구성하기는 더 힘들었으며, 기능이 적절히 작동하는지 여부를 알리기는 훨씬 더 힘들었다.

또한, 장비의 관리 인터페이스에서 이용할 수 있는 진단 툴도 살펴 보았다. 경로추적(trace route), 핑(ping) 및 DNS 폭언이 포함된 이러한 툴들은 이행 문제를 디버깅하는 데 유용하다. 그 외에 고려한 관리 기능들로는 상태 페이지, 장비 상태 결정, 로깅 및 통보 능력 등이 포함됐다. 아스테로의 시스템 앤 네트워크(System and Network) 상태 페이지는 현재 장비 작동을 그래프로 보여주는 등 특히 두드러졌다.

테스트한 다섯 개 장비를 가운데 두 개의 장비는 전용 하드웨어와 운영시스템을 사용하며, 나머지 세 개는 리눅스 기

반이다. 포티넷과 소닉월의 전용 장비들은 전체적인 파워와 사양 면에서 뒤떨어지긴 하지만, 사용과 구성은 훨씬 간편했다. 세 개의 리눅스 기반 장비들은 보다 나은 기능성과 보다 뛰어난 작업처리량을 갖고 있지만 셋업에 보다 많은 시간과 기술, 그리고 인내심이 필요했다.

전용과 리눅스 기반

그렇다면 자신에게 가장 잘 맞는 장비는 어떤 장비일까? 한정된 IT 지원을 갖춘 소기업에서는 에디터즈 초이스를 수상한 포티넷의 포티게이트-60(FortiGate-60)이 마음에 들었다. 이 장비에는 인상적인 사양과 직관적인 사용자 인터페이스가 있어서 최소한의 IT 지원만 있다 하더라도 조직에서 필요로 하는 보호를 제공하도록 장비를 설치하고 구성할 수 있음을 확인할 수 있었기 때문이다.

강력한 IT 지원 인력을 갖춘 보다 규모가 큰 기업에서는 서브게이트 에지포스(EdgeForce)가 인상적인 사양과 강력한 고성능 작업처리량을 보유함으로써 두 번째 자리를 차지했다.

비용을 비교하기 위해 우리는 업체들에게 50 라이선스 조

Executive Summary

보안 어플라이언스 테스트 방법

우선 장비들은 칼 폴리 넷PRL 네트워크의 예제에 배치됐다. 여기서 각각은 SMTP, HTTP, FTP 및 SSH 트래픽을 DMZ에 있는 서버로 포트 전송하는 한편 LAN에서 WAN으로 트래픽을 허용하도록 구성됐다. 게다가 로깅을 켜고 콘텐츠 필터링, 안티바이러스 및 침입 탐지 등과 같은 장비의 고급 기능 이행을 조사해보았다.

그런 다음 우리는 장비를 웹으로 옮겨 성능 테스트를 실시했다. 작업처리량과 대기시간을 모니터링했으며, 이런 측정치에 고급 기능이 미치는 영향도 조사해 보았다. 뿐만 아니라 테스트를 하는 동안 미야뚨 바이러스가 오도록 하는 '행운'도 누릴 수 있었다(나온 지 24시간 후에 이것을 각 장비로 통과시켜 어떤 업체가 바이러스 점의를 업데이트하는지를 살펴보았다).

장비 상에서의 안티바이러스를 지원하는 네 업체가 모두 미야뚨 등 우리가 던져넣은 모든 바이러스를 잡아냈으며, 대용량 압축 파일도 문제없이 처리했다. 테스트 관점에서 볼 때 이 네 장비

들은 잘 수행했다.

장비가 HTTP, FTP, SMTP 트래픽의 막대한 부하를 처리할 수 있는지 여부를 판단하기 위해서는 HTTP 및 FTP 트래픽용 익스웹(ixWeb)을 돌리고 SMTP 트래픽용으로는 웹로드(WebLoad)를 돌리는 익시어 1600T 트래픽 생성기를 이용했다. 시스템의 활성 사용자 수는 50명으로 시뮬레이션했으며, 그 중 30명은 HTTP, 20명은 FTP를 사용하게 했다. 트래픽 부하는 20Mbps로 설정했다.

그 외에도 우리는 75KB의 이메일 메시지를

매 2~3초마다 장비로 통과시켰으며, 어플라이언스들은 네트워크 자원에 필요한 방화벽 규정을 갖도록 구성됐다.

대기시간을 모니터링하기 위해서는 4Kbps의 HTTP 요청과 응답을 4~5초 이내 간격으로 이용했다. 그리고 레퍼런스용으로 장비에 어떤 다른 트래픽도 없이 이 접속의 대기시간을 측정했다. 모든 장비에서 레퍼런스 대기시간은 3ms 이하였다. 이러한 접속에서 생기는 변화를 관찰함으로써 다양한 부하가 장비에 미치는 영향을 파악할 수 있었다. <표: 성능 테스트>에서 '통과'란

<표 : 성능 테스트>

	20Mbps 부하	20Mbps 부하와 2Mbps VPN 트래픽	제로 로스 작업처리량 임호화 속도(Mbps)
아스테로	통과	통과	30
포티넷	통과	통과	16
서브게이트	통과	통과	27
소닉월	통과	통과	16.5
시만텍	통과	통과	55

적에 대한 견적을 의뢰했다. 물론, 가격은 설치기반의 규모에 따라 달라질 것이다.

B+ 포티넷 포티게이트-60

포티넷 포티게이트 60은 아웃 오브 더 박스로 우승을 차지했다. 이것은 몇 파운드가 더 나갈 뿐이며 랩마운팅용으로는 의미가 없지만, 두 개의 랜과 하나의 DMZ, 그리고 네 개의 스위치드 랜 인터페이스를 제공하며, 모두 10/100Mbps다. 두 번째 랜 인터페이스는 자동 페일오버용으로 구성될 수 있다.

포티게이트-60의 사용자 인터페이스는 직관적이다. 셋업 마법사는 우리가 기본적인 사양을 쉽게 구성할 수 있게 도와 주었다. 소닉월의 장비와 달리 포티게이트-60은 방화벽 규정과 정책용 마법사는 없었다. 그렇다 하더라도 장비는 따라하기 쉬운 메뉴 덕분에 셋업하기가 간단했다. 옵션 구성을 끝낼 때마다 기능이 예상대로 작동하고 있음을 확인할 수 있었다. 아스테로나 시만텍 장비에서는 이렇듯 좋은 느낌을 받지 못했다. 포티게이트-60은 웹 인터페이스에서부터 디버깅 들

은 제공하지 않지만 CLI(Command Line Interface)에서 사용 가능하다.

포티게이트-60의 안티바이러스 이행은 강력하다. 사실 이것은 우리의 위시 리스트에 있는 모든 프로토콜에 대한 안티바이러스를 지원하는 유일한 업체다. 안티바이러스 구성은 간단했다. 이 장비는 바이러스가 탐지된 후 보내지는 통보를 맞춤화할 수 있게 해주었으며, 단 바이러스가 발견될 때 '거부/송신자 통보'나 '거부/수신자 통보'만 지원한다. 바이러스 격리 기능은 포티게이트-200으로 시작되는 포티넷의 하이엔드 모델에서 이용할 수 있다.

타 장비에서 스캐닝하는 바이러스가 6만~8만개에 이르는 데 비해 포티넷의 안티바이러스를 이행하면 3천100가지 바이러스만 스캐닝된다. 이렇듯 크게 차이가 나는 것은 포티넷이 인더와일드(in-the-wild) 바이러스들에 초점을 두고 있기 때문이다. 이런 바이러스들은 주로 최근에 실제 네트워크에서 볼 수 있는 것들로, 윈도우 3.1과 같은 예전 기술에 대한 바이러스는 포함돼 있지 않다. 이러한 문제는 이번 분석의 범주에서 벗어나는 것이다. 하지만 포티넷 장비는 우리가 통과해 보낸 80개의 모든 실제 바이러스들을 탐지했으며, 네

장비가 레퍼런스 값에서 2ms가 미만으로 대기 시간을 늘렸을 때 제공된 트래픽 부하를 처리할 수 있었다는 것을 뜻한다.

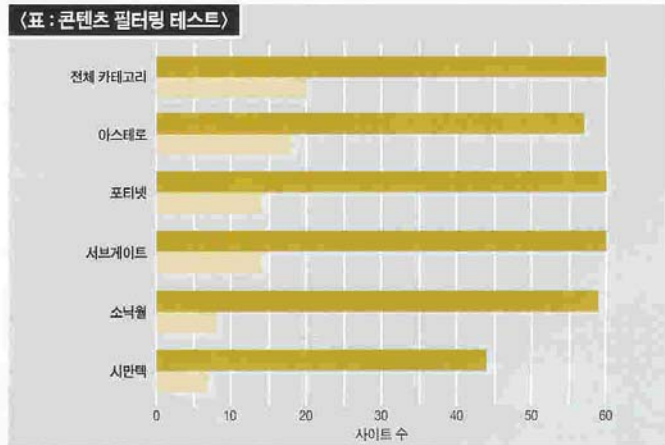
VPN 테스트에서는 두 가지 결과를 제공하고 있는데, 첫째는 20Mbps의 HTTP 및 FTP 트래픽으로 2Mbps의 수신 VPN 트래픽을 추가한 결과다. 이 트래픽은 익시어의 익스VPN과 익스채리엇(IxChariot) 소프트웨어를 이용해서 만들어냈다. 그런 다음에는 VPN 트래픽만을 위해 제로 로스 작업처리량 테스트를 실시했다. 이 테스트에서는 정비로 짧은 트래픽 버스트를 보내 이들이 데이터를 암호화할 수 있는 능력을 측정했다. 이 제로 로스 작업처리량 수치를 통해 우리는 장비들의 하이엔드 VPN 능력을 엿볼 수 있었다.

마지막으로 각 장비의 콘텐츠 필터링 능력을 테스트하기 위해 구글 검색엔진에서 'porn'과 'gambling'을 입력했다. 그런 다음 각 검색으로 나온 임의의 URL을 가지고 이들이 실제로 범주 안에 속해 있는지를 확인해 보았다. 이 URL들을

차단하도록 장비의 블랙리스트를 구성한 후 우리는 LAN에서 WAN으로 장비를 통과시키면서 60개의 포르노 사이트와 20개의 도박 사이트로

액세스를 시도했다. (표: 콘텐츠 필터링 테스트)에서는 전송된 80개 URL들 중 차단된(거부된) URL 수를 보여준다(수치가 높을수록 좋다).

(표 : 콘텐츠 필터링 테스트)



Lab Test 보안 어플라이언스

보낸지 24시간 내에 마이돔(MyDoom)을 잡아냈다.

콘텐츠 필터링을 위해서 포티넷은 시베리언(Cerberian)이 제공하는 가입자 서비스를 이용하고 있다. 구성은 간단해서 웹을 통해 시베리언 서비스에 로그인 하고 관심있는 몇 개 분야를 선택한 다음 몇몇 필드를 업데이트하기만 하면 됐다. FTP용 콘텐츠 필터링이 지원되지 않는 것은 다소 놀라웠으며, SMTP용 콘텐츠 필터링도 마찬가지로 지원되지 않았다. 포티넷은 SMTP 지원은 다음 릴리즈에서 가능할 것이라고 밝혔다.

테스트한 장비들 중에서 포티넷과 시만텍의 제품만이 IDS 기능을 제공했다. 포티넷은 시만텍의 변칙 탐지 기능은 따라가지 못하지만, 포티게이트-60은 1천400개 이상의 IDS 서명을 스캐닝했으며, 34개의 DoS와 침입 공격을 능동적으로 막아냈는데, 소기업들에게는 이 점이 더 중요하다.

소기업을 대상으로 하는 장비로서 포티게이트-60은 해야 할 일을 해낼만한 충분한 힘을 갖추고 있다. 이것은 작업처리량이 가장 높진 않지만 20Mbps FTP/HTTP 테스트를 최고 12Mbps의 VPN 트래픽으로 쉽게 처리했다. 50 사용자 시나리오용이 약 2천400달러로 1년치 안티바이러스 및 콘텐츠 필터링 가입이 포함된 포티게이트-60은 소기업 보안을 위

해 선택하기 매우 좋은 제품임이 관명됐다.

포티게이트-60

가격: 995달러

안티바이러스 가입: 249달러, 콘텐츠 필터링 가입(50 사용자): 1천100달러

www.fortinet.com

B+ **서브게이트**
에지포스 인티그레이티드 시큐리티 플랫폼

세 개의 리눅스 기반 장비들 가운데서는 서브게이트 에지포스(ServGate EdgeForce)가 최고였다. 에지포스는 1U 랙마운터블 제품으로 웹, DMZ 및 LAN 트래픽용의 세 개의 인터페이스가 있다. 포티넷 장비와 달리 여기에는 자동 패일 오버를 위한 추가 웹 포트를 포함해 있지 않다.

서브게이트는 기본 구성용의 마법사를 제공하지 않으며, 그 인터페이스는 포티넷이나 소닉월 장비의 인터페이스처럼 멋지지도 직관적이지도 않다. 하지만 이 장비는 구성이 매우 간편하며 어떠한 리눅스 지식도 요구되지 않는다.

서브게이트 안티바이러스 이행은 8만개 이상의 바이러스

보고서 카드 / 보안 어플라이언스 제품별 최종평가

Security Appliances

	포티넷 포티게이트-60	서브게이트 에지포스 인티그레이티드 시큐리티 플랫폼 EFI	아스테로 시큐리티 리눅스	소닉월 TZ 170	시만텍 게이트웨이 시큐리티 5420
관리 및 유용성					
고급 기능 구성(10%)	4	4	3.5	4.5	2.5
방화벽 및 기본 구성(10%)	4.5	4.5	4.5	5	3.5
상태 모니터링, 로깅, 보고(5%)	4	4	4	4.5	3
안티바이러스					
업선 및 구성(10%)	4	4	3.5	2.5	3.5
바이러스 테스트(5%)	4.5	4.5	4.5	0	4.5
성능(15%)	4.5	4.5	4.5	4.5	4
가격(15%)	4.5	3.5	3	4.5	3.5
콘텐츠 필터링					
콘텐츠 필터링 테스트(5%)	4.5	4.5	4.5	3.5	2.5
업선 및 구성(5%)	4	3.5	4	3.5	4
IDS/IPS					
DoS 탐지/방지(7%)	4.5	4.5	4	4.5	4.5
침입 탐지/방지(3%)	4	0	0	0	4.5
VPN					
하이엔드 능력(5%)	3	4	4	3	4.5
VPN 평균 부하 테스트(5%)	4.5	4.5	4.5	4.5	4.5
총 평균(100%)	4.26	4.02	3.993	3.82	3.68



주) A 4.9, B 3.5, C 2.5, D 1.5, F(1.5, A-C 점수에는 그 범위에 + 혹은 -가 포함됨. 총 평균 및 비중 수치는 0-5 범위를 기준으로 한 것.

를 스캐닝한다. 하나를 발견하면 이메일을 유실시키거나 수신자에게 경고를 하거나, 혹은 바이러스를 격리시킬 수 있다. 이 장비에는 바이러스 격리를 위한 4GB 이상의 공간이 있다. SMTP, POP3 및 FTP 트래픽에 대해 바이러스를 스캐닝하지만 HTTP 트래픽은 스캐닝할 수 없다. 스팸 필터링은 애드온, 즉 맥아피 스팸어쌐신(McAfee SpamAssassin)을 통해 사용 가능한데, 이것은 테스트 해보지 않았다.

에지포스는 콘텐츠 필터링 테스트에서 잘 수행됐다. 콘텐츠 필터링이 FTP 뿐만 아니라 HTTP에서도 지원된다는 점은 마음에 들었지만, 서브게이트에서는 웹센스 엔터프라이즈 콘텐츠 필터(WebSense Enterprise Content Filter) 패키지를 돌리는 데 윈도 서버 셋업을 필요로 했다. 이 외장 박스 구성은 어렵진 않았지만 별도의 단계를 거쳐야 하는 일이다. 일단 이 외장 서버가 배치되자 장비에서의 콘텐츠 필터링은 간단히 구성할 수 있었다.

에지포스는 하이엔드 테스트에서 포트게이트-60을 앞서서 20Mbps의 HTTP 및 FTP 트래픽을 쉽게 처리하는 동시에 20Mbps VPN 트래픽을 처리하는 막강한 성능을 보여주었다. 특급 프로세싱 파워가 필요하다면 4천300달러 정도의 가격(콘텐츠 필터링용 윈도 서버 비용 별도)에 강력한 보안 장비를 확보할 수 있을 것이다.

에지포스 인티그레이티드 시큐리티 플랫폼

장비(에지포스 프로페셔널 모듈 포함): 1천395달러, 안티바이러스 가입: 1천295달러, 콘텐츠 필터링 가입(50 사용자): 1천570달러
www.servgate.com

B 아스타로 시큐리티 리눅스 4 엔터프라이즈 에디션

아스타로 소프트웨어는 도시바 서버에 설치된 상태로 왔지만 스탠드얼론 소프트웨어로 구입할 수 있다.

아스타로의 구성은 최고 성적을 낸 두 제품에 비해서는 직관성이 떨어졌다. 이 장비는 어떠한 마법사도 제공하지 않기 때문이다. 하지만 네트워크 인터페이스를 셋업하고 방화벽을 구성하기 위해 소프트웨어를 중심으로 우리의 길을 내비게이션할 수는 있었다. 이미 우리가 리눅스에 익숙한 점이 도움이 됐다.

SG30에는 두 개의 별도 인터페이스가 함께 왔는데, 우리는 웹 액세스용으로 하나를 사용했으며, 실질적으로 6개의 스위치드 포트인 나머지 하나는 DMZ 및 랜 트래픽에 사용했다.

고급 사양은 셋업이 훨씬 더 힘들었으며 안티바이러스와 콘텐츠 필터링 구성이 특히 힘들었는데, 여기서는 옵션을 이해하기 위한 얼마간의 노력이 요구됐다. 예를 들어 '안티바

이러스'나 '콘텐츠 필터링'이란 체크박스가 있는 대신 소프트웨어에서는 HTTP 프로세스를 켜고 구성해서 안티바이러스용의 SMTP 릴레이와 콘텐츠 필터링을 가져올 것을 요구했다. 게다가 서비스를 적절히 구성했는지 여부도 쉽게 판단할 수 없었다. 처음에는 안티바이러스를 적절히 구성했다고 생각했으며 나중에는 장비가 어떤 바이러스도 차단하지 못했을 때에서야 실수를 발견할 수 있었다.

이 장비는 적절히 구성된 후에 안티바이러스 테스트를 잘 통과해서 바이러스가 탐지됐을 때 거부/송신자 통보, 거부/수신자 통보, 이메일 유실 및 격리 등을 할 수 있게 해주었다. 불행히도 아스타로 안티바이러스 이행은 HTTP나 FTP 트래픽은 스캐닝하지 않는다.

아스타로 소프트웨어는 테스트한 것들 중 가장 값이 비쌌는데, 여기에는 하이엔드급 하드웨어도 얼마간 원인이 있다. 하지만 훌륭한 제품들 중 독특하게도 소프트웨어 전용 이행을 제공하고 있기 때문에 약 1천달러 가격에 안티바이러스 및 콘텐츠 필터링 가입비를 추가하면 자신의 서버에 이 소프트웨어를 설치할 수 있다. 아스타로가 권장하는 최소 사양은 펜티엄 II 450MHz에 8GB 하드드라이브와 128MB 램이다.

아스타로 리큐리티 리눅스(도시바 매그니아 SG30에서)

테스트된 장비: 3천795달러(소프트웨어만: 995달러), 안티바이러스 가입(50 사용자): 695달러, 콘텐츠 필터링 가입(50 사용자): 950달러
www.astaro.com

B 소닉월 TZ 170 인터넷 시큐리티 어플라이언스

소닉월의 사용자 인터페이스는 우수한 수준이었다. 기본적인 구성과 방화벽 규정 및 정책은 사용자 친화적인 마법사를 이용해 설정됐다. 그리고 콘텐츠 필터링 구성용으로 어떠한 마법사도 제공되지 않았지만, VPN 셋업을 돕기 위한 마법사는 있었다. 첫 로그인 페이지에서 경고와 네트워크 인터페이스 데이터를 포함한 상태 정보가 제공되는 점도 마음에 들었다. 나아가 소닉월의 로깅 기능은 훌륭한 장비들 중 최고로 쉽게 켜고 읽고 이해할 수 있었다.

하지만 테스트 도중에 TZ 170에서 문제에 부딪혔는데, 우선 이 장비는 VPN 기능의 펌웨어 이행에서 버그가 있었다. 소닉월에서는 이것을 조사해서 펌웨어를 수정했으며, 그 픽스는 다음 릴리즈에서 제공될 것이다. 또한 콘텐츠 필터링을 사용할 때 로깅에도 문제가 있었다. 이 장비의 로깅 기능은 차단된 수많은 URL을 제빨리 이어서 액세스를 시도하자 제대로 지칭해내지 못했다.

Lab Test 보안 어플라이언스

이번 분석에서 소닉월에게 불리하게 작용한 한 가지는 이것이 장비에서 안티바이러스 스캐닝을 지원하지 않는다는 점이다. 해결책으로 제시한 방법은 클라이언트 워크스테이션에서 최신 서명 파일을 들어가는 안티바이러스 소프트웨어가 있음을 TZ 170이 확인하게 하는 것이었다. 서명 파일이 업데이트가 필요하다면 소닉월은 클라이언트 측 안티바이러스 소프트웨어가 새로운 서명 파일을 다운로드하도록 투명하게 강요한다. 이러한 푸시 기능이 마음에 들고 모든 클라이언트 워크스테이션에 안티바이러스 소프트웨어가 설치돼 있으리라 믿긴 하지만, 이보다는 에지와 워크스테이션을 모두 보호

해주는 다단계 솔루션이 보다 강력할 것이다.

소닉월 TZ 170

장비: 995달러, 안티바이러스 가입(50 노드): 1천625달러, 콘텐츠 필터링 가입: 345달러

www.sonicwall.com



시만텍

게이트웨이 시큐리티 어플라이언스 5400 시리즈

침입 탐지 및 방지 영역에서 시만텍의 장비는 가장 강력했

보안 어플라이언스 제품별 사양표

	아스테로 시큐리티 리눅스	포티넷 포티게이트-60	서브게이트 에지포스 인티그레이티드 시큐리티 플랫폼 E91	소닉월 TZ170	시만텍 게이트웨이 시큐리티 5420
일반적인 장비 사양					
별도의 DMZ 네트워크 인터페이스	N	Y	Y	Y	Y
로컬 웹 액세스용 추가 스위치 포트	Y	Y	N	Y	Y
관리 인터페이스의 동시 사용자 지원	N	Y	Y	N	Y
다중정비 관리 소프트웨어 제공	Y	Y	Y	Y	Y
네트워크 인터페이스의 GUI 상태 페이지	Y	N	Y	Y	Y
랜과 DMZ 인터페이스 모두에서 NAT/PAT 지원	Y	Y	Y	Y	Y
DHCP 서버로 작동 가능	Y	Y	Y	Y	N
SNMP 지원(MIB-II 준수)	Y	Y	Y	Y	Y
사용자 인증	LDAP, 로컬 데이터베이스, 레디우스	LDAP, 로컬 데이터베이스, 레디우스	LDAP, 로컬 데이터베이스, 레디우스	로컬 데이터베이스, 레디우스	LDAP, 로컬 데이터베이스, 레디우스
액세스 제한 사용자 그룹	Y	Y	N	N	N
사용자의 서비스 액세스 스케줄링	N	Y	Y	Y	Y
일반 구성 마법사	N	Y	N	Y	Y
방화벽 규정 마법사	N	N	N	Y	Y
정적 경로 구성	Y	Y	Y	Y	Y
RIP 지원	N	Y	N	Y	Y
서비스/프로토콜별 대역폭 제한	Y	Y	Y	Y	Y
DNS 서버로 작동 가능	Y	N	Y	N	Y
네트워크 진단 툴	Y	N	Y	Y	N
구성용 CLI 옵션	Y	Y	Y	Y	Y
안티바이러스 사양					
프로토콜 장비의 안티바이러스 지원	POP3, SMTP	FTP, HTTP, IMAP, POP3, SMTP	FTP, POP3, SMTP	적용불가능	FTP, HTTP, SMTP
바이러스가 탐지됐을 때 취해지는 옵션	유실/통보 없음, 격리, 송신 자 혹은 수신자 통보	송신자나 수신자 통보	유실/통보 없음, 격리, 송신자 통보	적용불가능	유실/통보 없음, 격리, 송신자나 수신자 통보
클라이언트 워크스테이션에서 최신 바이러스정의이행	N	N	N	Y	N
스캐닝용도로 파일 크기 제한 구성 가능	N	Y	N	적용 불가능	Y
집 파일의 바이러스 스캔	Y	Y	Y	적용 불가능	Y
바이러스 통보 메시지 맞춤 가능	N	Y	Y	적용 불가능	Y
자동 바이러스 정의 업데이트 스케줄링	Y	Y	Y	적용 불가능	Y
가입자 서비스로 바이러스 업데이트 푸싱	N	Y	N	적용 불가능	Y
VPN 트래픽 바이러스 스캐닝	Y	Y	Y	적용 불가능	Y

주: Y, 지원함, N, 지원하지 않음

지만 또한 가장 복잡하기도 했다. 700개 이상의 공격용으로 침입 탐지 기능을 제공하는 것 외에도 5400은 전체 애플리케이션 점검 및 프로토콜 이상 탐지를 수행해서 원치 않는 트래픽을 능동적으로 찾아낸다. 이 IDS 기능은 시만텍의 맨헌트(ManHunt) 엔진을 기반으로 하며, 이것은 프로토콜 이상 탐지라는 기술을 이용해 네트워크 흐름을 분석함으로써 새롭고 알려지지 않은 공격을 식별한다. 마이둠이나 코드 레드 같은 공격은 디플트로 방어된다.

시만텍 장비에는 수많은 문제들이 있다. 그 자바 기반 사용자 인터페이스는 사용하기에 느리고 실망스러우며, 사용자 인터페이스는 가장 덜 직관적이며 언제나 여러 가지 메뉴 옵션을 찾아야 고급 기능을 켤 수 있게 돼 있었다. 이런 인터페이스는 별도의 안내서와 시간이 요구되는 것 외에도 기능의 오구성을 유도하고 그렇지 않은 데 보호되고 있는 것처럼 느끼게 만든다.

5400의 테스트에서는 운이 뒤섞였다. 두 가지 부하 테스트들이 한창인 가운데 이 장비는 멈춰버려 다시 재시동시켜야 했다. 시만텍은 우리 소프트웨어를 업그레이드했으며, 문제는 해결된 것처럼 보였다. 하지만 5400에는 또한 콘텐츠 필터링 테스트에서 가장 나쁜 점수를 받기도 했다. 반면에 이 장비는 안티바이러스 테스트는 잘 수행했으며, 그 VPN 성능은 인상적이었다. 이 제품은 가장 높은 VPN 작업처리량 수치를 보여주었다.

시만텍은 장비와 안티바이러스 및 콘텐츠 필터링의 가격을 따로 나누지 않고 있다.

시만텍 게이트웨이 시큐리티 5420

장비와 안티바이러스 및 콘텐츠 필터링 가입(50 노드): 5천278달러
www.symantec.com **N/C USA**

보안 어플라이언스 제품별 사양표 (계속)

	아스텔로 시큐리티 리눅스	포터넷 포터게이트-60	시브게이트 에지포스 인티그레이티드 시큐리티 플랫폼 EF1	소닉월 TZ170	시만텍 게이트웨이 시큐리티 5420
콘텐츠 필터링					
CF 프로토콜	HTTP, SMTP	HTTP, IMAP, POP3	FTP, HTTP, POP3, SMTP	HTTP	HTTP, NNTP, SMTP
입체에서 CF 블랙리스트 저장	Y	Y	N	Y	Y
장비에 전체 블랙리스트 저장	N	N	N	N	Y
로컬 서버에서 가입자 블랙리스트 보유 의무	N	N	Y	N	N
범주별로 URL 블랙리스트 이용 가능	Y	Y	Y	Y	Y
수동 입력된 구문을 기반으로 콘텐츠 차단	Y	Y	Y	Y	N
수동 블랙리스트 URL 엔트리	Y	Y	Y	Y	Y
수동 화이트리스트 엔트리	Y	Y	Y	Y	Y
화이트/블랙리스트용 와일드카드 지원	Y	Y	N	N	Y
범주별로 수동 화이트/블랙리스트 조직화	Y	N	N	N	Y
차단되는 파일	액티브X, 쿠키, 자바애플릿, 자바스크립트, MIME 유형들	액티브X, 쿠키, 자바 애플릿, 자바 스크립트, 기타	액티브X, 자바 애플릿, 자바 스크립트, MIME 유형들	액티브X, 쿠키, 자바 애플릿	액티브X, 자바 애플릿, 자바 스크립트, MIME 유형들, 기타
IDS/IPS					
탐지/방어되는 총 공격 수	0	1,434	13	22	700
탐지/방어되는 DoS 공격 수	11	24	13	4	적용불가능
IDS 풀 패킷 점검	0	1,400	0	0	적용불가능
IPS 풀 패킷 점검	0	10	0	0	적용불가능
IDS/IPS 데이터베이스에 수동으로 서명 추가 가능	N	Y	N	N	N
VPN					
IPSec 지원	Y	Y	Y	Y	Y
PPTP 지원	Y	Y	Y	N	N
L2PT 지원	Y	Y	N	Y	N
암호화	AES, 3DES	AES, 3DES	AES, 3DES	AES, 3DES	AES, 3DES
인증	MD-1, SHA-1	MD-1, SHA-1	MD-1, SHA-1	MD-1, SHA-1	MD-1, SHA-1
일격 VPN 클라이언트 소프트웨어	Y	Y	Y	Y	Y

주) Y: 지원함, N: 지원하지 않음