

# 보안성 향상·비용 절감·그린IT 보안통합 '일석삼조'

"2010년 위협의 10% 만이 포인트 솔루션 필요" ... 공격 고도화 UTM이 '해답'

네트워크 보안에 대해 고민하고 있는 각기업의 보안 담당자라면 끊임없이 진화하고 있는 보안 위협 요소들과 관련 법규의 준수 문제로 고심하고 있을 것이다. 뿐만 아니라 최근에는 환경적인 이슈로 인해 전력 과소비, 이산화탄소 과다 배출 등의 문제까지도 IT 관리자가 고려해야 요소가 되고 있다. 통합위협관리(UTM) 플랫폼을 통한 네트워크 보안의 통합이 이와 같은 당면 과제를 어떻게 처리하는지, 보다 효율적인 보안의 구축과 비용 절감, 나아가 환경에 미치는 영향까지 해결할 수 있는 방법은 어떤 것인지에 대해 알아본다. (관정자)

## 연재순서

- 1회: 네트워크 보안 통합의 필요성(이번호)
- 2회: 통합을 통한 비용절감 사례
- 3회: 고성능 UTM 구현 기술



서현식 // 데이터넷2010 부장  
hsseo@datanet.com

**오** 늘날 공간 부족, 전력 과다 사용, 예산 문제 등의 여러 요인으로 인해 통합의 문제는 CIO에서부터 IT 담당자에 이르기까지, 매우 중요한 전략적이고 전술적인 화두가 됐다. 통합은, 그것이 실질적 통합이든 가상 통합이든 간에 낮은 비용과 전력 사용량의 절감, 관리성 개선, 환경 부담 절감 등의 혜택을 제공한다.

일반적으로 지금까지 통합에 대한 관심은 데이터센터, 정확히는 특정 애플리케이션 서버의 통합에 집중돼 왔다. 하지만 이러한 편중된 관심은 통합이 실현됐을 때 극적인 이점들을 가져다 줄 수 있는 분야, 즉 네트워크 보안 영역에서는 오히려 간과된 측면이 많다. UTM 플랫폼을 이용한 네트워크 보안 통합은 기업의 전체 네트워크 상에 존재하고 있는 다양한 종류의 보안 위협을 효과적으로 관리한다는 기본적인 이점을 제공해 준다.

아울러 네트워크 보안 통합은 비용적 측면에서도 이득이 크다. 가트너는 기업의 보안 관련 부서를 대상으로 한 최근 조사에서, '여러 종류의 보안 기능을 하나의 장비에 통합함으로써 정보보안에 관련한 예산 절감을 달성할 수 있다'고 언급한 조사결과를 내놓았다. 또한 가트너는 2005년에는 새로 등장하는 보안 위협 중 약 80%가 방어를 위해 특정 포인트 솔루션을 필요로 했던 것과 달리 2010년에는 오직 10%의 위협만이 포인트 솔루션을 필요로 할 것으로 예측하고 있기도 하다.

이처럼 네트워크 보안 분야에서의 통합은 다른 엔터프라이즈 컴퓨팅 분야에서 통합이 제공하는 일반적 이점인 비용절감, 관리성 개선, 친환경적인 혜택 이외에도 보안 기능의 향상이라는 추가적인 혜택을 제공해 준다.

### 통합을 통한 보안 향상

보안 문제를 염려하고 있는 IT 관리자에게 네트워크 보안 통합은 매우 반가운 소식이 아닐 수 없다. 전반적 IT 예산의 감축, 컴플라이언스 이슈 증가 등 최근 벌어지고 있는 일련의 흐름으로 인해 보안과 관련된 담당자의 부담이 더욱 높아지고 있기 때문이다.

전반적인 IT 예산의 감축은 전사회적으로 나타나는 현상 중 하나다. 한 조사 결과에 따르면, 각 기업 IT 관련 의사 결정권자들의 2.5%만이 자사의 IT 예산을 늘릴 예정이다. IT 예산

은 기업의 수익에 의존하는 경향이 크기에 최근의 경기 불황은 이러한 추세를 더욱 부추기는 악순환을 낳을 수 있다. 이러한 상황 속에서 비용 이점을 줄 수 있는 통합은 필수적이라고 할 수 있다.

날로 정교해지는 보안 위협과 나날이 늘어나는 컴플라이언스 준수 필요성, 새로운 애플리케이션이나 기술의 발전에 따른 새로운 취약성 등 네트워크 보안이 점점 더 복잡성을 띄게 된다는 점도 통합 솔루션의 도입을 필연적으로 만드는 요소라고 할 수 있다.

오늘날 네트워크를 해킹하는 행위는 급진적인 목적으로 이뤄지고 있으며, 네트워크 보안의 약점을 이용하기 위해 조직적인 범죄의 형태로 급속도로 증가하고만 있다. 더불어 민감한 데이터의 보호에 대한 모든 절차가 이루어졌는지를 입증하기 위해 많은 양의 데이터를 기록 및 감시해야 하는 컴플라이언스 준수의 부담은 어느 때 보다 커지고 있다.

UTM 플랫폼을 통한 네트워크 보안 통합은 보다 저렴한 비용으로 효과적인 보안을 제공하면서 이러한 문제를 해결할 수 있는 길을 제시할 수 있다. 나아가 UTM을 통한 통합은 그린IT를 실현할 수 있는 효과도 제공할 수 있다.

### 네트워크와 콘텐츠 위협이 대부분

오늘날 기업이 직면하고 있는 위협은 네트워크와 콘텐츠 기반의 위협이 대부분이다. 네트워크 위협에는 서비스 거부(DoS), 침입, 일반적인 웜 등이 있으며, 이러한 위협들은 방화벽이나 침입방지시스템(IPS), VPN으로 해결이 가능하다. 콘텐츠 기반의 위협에는 보다 복잡한 웜, 바이러스, 피싱, 과잉, 스파이웨어, 스톱 페일 등이 있으며, 이를 처리하기 위해서는 안티바이러스, 안티스팸, 웹 필터링 등과 같은 콘텐츠 검사 기술이 필요하다.

그러나, 최근 조직적인 범죄가 늘어남에 따라 해커의 공격 유형은 더욱 복잡해지고, 네트워크나 콘텐츠 레벨 위협의 혼합 공격도 늘어나 모인트 솔루션을 통한 대응을 어렵게 만들고 있다. 이는 통합 보안을 요구하는 요소가 된다. UTM 플랫폼 도입은 여러 대응 방안에 대한 지능적인 공유가 가능하기 때문에 일반적인 공격은 물론, 보다 정교한 공격 요인을까지도 탐지하고 예방이 가능하다는 장점이 있다.

예를 들어, 시그니처 기반의 안티바이러스 엔진에 침입 방지 엔진을 결합한 통합 시스템은 단일 기능의 솔루션보다 훨씬 더 효과적이다. 비슷한 원리로 웹 필터링, 안티바이러스, 그리고 IPS 기능을 통합해 여러 엔진의 기능을 연동할 수 있다면, 아무리 복잡한 유형의 공격이라도 효과적으로 막아 낼

수 있게 된다. 이는 공격이 일어난 후 초기에 방어 체계를 갖추 수 있게 한다는 것을 의미한다. 즉, 공격 침투 성공률을 저하시켜 연관된 피해를 줄일 수 있는 것이다.

### 관리 효율성 극적 개선

UTM을 통한 네트워크 보안의 통합은 모든 솔루션의 기능을 중앙 집중화된 방식으로 관리할 수 있어 보안 관리자의 생산성을 크게 향상시킬 수 있는 장점도 제공한다. 이는 비통합 방식으로는 쉽게 이를 수 없는 부분으로, 실제 다양한 벤더의 보안 솔루션을 단일화된 중앙 집중적인 솔루션으로 관리할 수 있는 방안은 존재하지 않는다고 해도 과언이 아니다.

통합은 다양한 보안 관리 임무를 통합 솔루션을 통해 쉽게 처리하게끔 하는 장점도 있다. 중앙 관리를 통해 여러 장비를 한 번에 원격으로 관리할 수 있으며, 계층적인 규정이나 유연한 그룹화 기능 등과 같은 여러 가지 확장 기능을 추가로 지원할 수 있는 것, 그리고 하나의 콘솔에서 특정 도메인이나 모든 도메인에 관련된 설정을 수립하고, 조정하는 것도 가능하다. 기업이 성장하면 할수록 솔루션을 확장하는 능력이 중요해지는데, 중앙 관리 애플리케이션을 사용하게 되면 모든 종류의 장비를 효율적으로 운영할 수 있게 돼 운영 효율을 극적으로 개선하는 이점도 있다.

통합은 성공적인 위협 관리를 위한 보안위협 연구조사의 단일화를 가능하게 해 보안위협 인텔리전스를 강화시킬 수 있다. 과거에는 안티바이러스 연구자들과 취약성 연구자들 사이에 경쟁의식이 많았지만 해커의 공격이 더욱 복잡하고 다양해짐에 따라 두 분야를 혼합하는 하이브리드 연구 방식은 이제 반드시 필요한 것이 됐다. UTM 솔루션이 보안 위협에 대한 대응 방안을 공유함으로써 효과적으로 처리하는 것과 같이 다양한 종류의 위협에 대한 연구 프로그램의 통합을 통해서 보다 정확한 대응책을 세울 수 있기 때문이다.

이러한 협업은 통합되지 않은 방식으로는 접근이 쉽지 않은 분야이다. 자사의 제품 보안을 위해 OEM 기술에 의존하는 벤더는 공급자가 제시하는 위협 정보에 의존하게 만들며, 조사의 수준이나 시의성 등에 대한 책임 회피 문제도 발생될 수 있다. 그리고 여러 종류의 위협에 대한 이해가 벤더 별로 상이할 수 있어 아무리 전문화된 지식을 갖추고 있다 하더라도 여러 분야에 거친 지식에 대한 신속한 공유에는 제한이 아주 많을 수밖에 없다.

최근 UTM에 대한 폭발적인 관심에 편승해 일시적이며 자외적인 방식으로 타 회사의 솔루션을 끼워 맞추기 식으로 제작된 '급조 UTM' 등이 등장하는 경향이 존재한다. 앞서 연

급한 이유로 이러한 제품에는 일단 주의를 기울일 필요가 있다고 조언하고 있다.

이와는 대조적으로 진정한 통합 UTM 솔루션은 수년간 다양한 위협 요인과 대응책에 경험을 쌓은 전문가들로 이뤄져 있다. 지식 공유 체계와 프로세스가 잘 구성돼 새롭게 생겨나는 혼합 보안 위협들을 파악할 수 있는 것. 이를 통해 대응책 수립을 담당하는 연구원들은 내부 지식 공유 프로그램이 제공하는 정보를 통해 깊이 있는 정보를 얻을 수 있으며, 이러한 체계는 새로운 위협에 대한 감지와 이에 대한 대응책이 더욱 빠르고 정확하게 이뤄질 수 있게 하는 요인이다.

### 통합을 통한 비용 절감

네트워크 보안에서도 비용 문제를 결코 소홀히 할 수 없는 부분이다. 네트워크 보안 임원들도 다른 IT 분야와 마찬가지로 운영 비용(OpEx) 및 구매비용(CapEx)을 절감하기 위한 노력의 일환으로 TCO를 절감하면서도 오히려 서비스를 향상시켜야 하는 문제로 고심하고 있다.

운영 비용의 관점에서 볼 때 네트워크 보안 통합의 혜택은 분명하다. 여러 시스템을 구입할 필요성이 없어 초기 투자비용을 줄일 수 있게 될 뿐 아니라 케이블링이 줄어드는 아주 사소한 부분에서도 비용을 절감할 수 있기 때문이다.

나아가 극히 제한적인 기업의 데이터센터 공간에서 추가적인 랙 공간에 대한 부담을 줄임으로써 얻는 장점도 있다. 그리고 가상화 기술을 통해 많은 장비를 각각의 목적에 따라 추가할 필요 없이 여러 보안 도메인을 한 장비에서 관리할 수 있어 운영비용 절감에 기여할 수 있다.

통합 네트워크 보안 플랫폼의 가장 중요한 TCO 혜택으로는 확장성을 들 수 있다. 일반적으로 한 기업이 UTM의 모든 요소를 즉시 구현하는 일은 매우 드물다. 먼저 방화벽, VPN, IPS 등과 같은 보안 기능을 통합하고, 나머지 기능은 언티바이러스나 웹 필터링 등 포인트 솔루션 제품 수명이 다한 후 이를 UTM으로 대체하는 경우가 많은 것이다. 이는 통합 솔루션이 이 기능들을 이미 구비하고 있어 새로운 박스를 구매하고 설치할 필요가 없을 뿐만 아니라, 해당 기능을 추가 구매하고 장비에서 설정만 하면 쉽게 추가가 가능하다는 장점이 있기 때문이다. 이처럼 네트워크 보안 통합은 최소한의 금액으로 새로운 기능의 추가가 용이해 기업의 보안 대한 투자를 보호하는데 기여할 수 있다.

### 통합 = 그린IT

전세계적으로 지구 온난화를 비롯한 환경 문제가 중요 화

두로 떠오르면서 모든 산업 전반에 걸쳐 친환경 기술이 각광을 받고 있다. 가트너는 향후 IT 장비의 제조, 운반, 사용에 따르는 탄소 배출량이 전세계 탄소 배출량의 약 2%를 차지할 것이라고 전망한 바 있는데 이는 항공 업계에서 배출하고 있는 탄소의 양과 비슷한 수준이다. IT가 환경에 미치는 영향도 적지 않은 것이다.

이에 따라 에너지 소비와 위험 물질의 사용을 줄이는 '그린 IT'는 오늘날 IT의 업계의 주요한 이슈로 급부상하고 있다. IT에 있어서도 에너지 절감 문제가 솔루션 선택의 주요 조건이 되고 있는 것이다. 이는 IDC의 조사 결과에서도 증명된다. IDC에 따르면, 50%가 넘는 고객은 공급자를 선택하는데 있어, 그 기업이 친환경적인 의식에 대한 관심도를 중요시 하는 것으로 나타났으며, 33%는 친환경적 기술의 제품 요소를 중요하게 생각하고 있다. 나아가 조사에 참여한 기업 임원진 중 80%는 그린IT를 매우 중요한 요소로 꼽고 있다.

네트워크 보안 통합은 하드웨어의 효율적인 에너지 사용을 가능하게 한다. 특히, 세시 또는 블레이드 기반의 UTM 솔루션의 경우 전력 사용 비용을 크게 절감할 수 있다. 예를 들어 네트워크 보안을 위해 방화벽, VPN, IPS, 언티바이러스 게이트웨이, 웹 필터링 등을 운용하고 있다고 가정하면, 이들 장비가 각각 300W의 전력만을 소비한다고 해도 총 총 1500W의 전력을 소비가 요구된다. 하지만, 이를 독립 시스템을 통합 네트워크 보안 시스템으로 대체한다면, 단지 기존의 20%에 해당하는 300W 시스템 하나로 모든 동일한 기능을 제공할 수 있게 된다.

이러한 전력 감소는 단순히 전력비용 절감 뿐 아니라 냉각 비용 절감 효과도 불러일으킨다. 또 사용되는 케이블의 양도 절감할 수 있다. 전사회적으로 범위를 확대하면, 이러한 저전력 소비는 이산화탄소 발생을 줄여 환경에 기여할 수 있게 한다. 또한 케이블링 감소는 환경적으로 좋지 않은 PVC 케이블의 사용을 줄이는 효과도 있다.

이처럼 네트워크 보안 통합은 친환경적이다. 또한 보다 효율적인 예산 지출이 가능하도록 한다. 특히 교육, 지원, 위협 업데이트 비용 및 관리 비용 부담을 줄여, 전반적인 운영 비용을 크게 절감할 수 있게 하며, 추가적인 하드웨어 없이 새로운 보안 기능을 탑재가 가능해 기업의 투자를 보호하는 효과도 제공한다. 또한 앞서 설명한 것처럼 네트워크 보안의 통합이야말로 고도화된 위협에 대응해 기업의 보안을 강화할 수 있는 유일한 방안이라고 할 수 있다. 