

# 차세대 보안 시장의 핵심 'UTM'

현재 IPS, IDS, 방화벽, VPN 등의 보안 어플라이언스들이 보안 시장의 핵심 제품이라고 할 수 있다. 그러나 이 제품들이 향후 보안시장에서 획기적인 시스템으로 정착될 수 있을까. 최근 IDC에 발표된 '세계적인 위협 관리 보안 어플라이언스 분야 2004~2008년 예측 및 2003년 시장 점유율 분석' 자료는 향후 보안 어플라이언스 시장의 중심이 점차 UTM(Unified Threat Management) 시장 쪽으로 전환할 것이라고 전망했다. 여기서는 무한한 성장 잠재력을 보유한 UTM의 시장성에 대해 알아본다.

김종덕  
포티넷코리아 이사장

UTM이란, 한 가지 이상의 보안 기능 수행을 목적으로 개발된 하드웨어, 소프트웨어, 네트워킹 기술들의 결합체라 정의할 수 있다. 이러한 UTM 보안 어플라이언스는 엄격한 운용 시스템을 갖춘 하드웨어와 세련적인 애플리케이션 세트에 구성되며, 사용자의 별도 소프트웨어 설치를 필요로 하지 않는다. 주요 기능으로는 보안 관리, 정책 관리, 서비스 품질 관리, 로드 밸런싱, 고가용성, 대역관리 등이 있다.

새롭게 부상하는 UTM 시장은 2003년 매출 규모가 1억500만 달러에 불과했다. 하지만 차후 5년 이내에 UTM 보안 어플라이언스 판매로 인해 발생하는 매출이 기존의 보안 제품 매출을 초과할 것이라고 IDC에서는 전망하고 있다. 이러한 UTM 시장은 2008년까지 연 평균 17% 수준으로 성장해 전체 시장 점유율의 85%를 차지할 것으로 보인다. 이는 총 시장 규모 34억5천만 달러에 육박하는 규모이다.(그림 참조).

## UTM의 성장 가능성

그렇다면 보안 시장에 기존의 보안 어플라이언스가 많음에도 불구하고, 사용자들이 UTM 보안 어플라이언스를 선택할 수밖에 없는 이유를 짚어보자. 이것이 바로 보안 시장에서의 UTM의 무한한 성장 가능성을 짐작할 수 있게 하기 때문이다.

무엇보다 UTM 보안 어플라이언스는 단일 제품의 접근법으로 제품 선택, 통합, 지원 서비스가 단순해져 복잡성을 완화했다는 점이다. 게다가 플러그 앤 플레이 방식으로 설치가 용이할 뿐 아니라 블레박스식 접근법을 통해 사용자로 인한 피해를 줄일 수 있으며, 장애를 줄이고 보안성을 높여준다. 특히 보안 어플라이언스에 어떠한 보안 위협이 발생했을 때, 이를 신속히 차단한 후 대응할 수 있다.

## UTM 보안 시장의 주요 기술

UTM 보안 어플라이언스 시장에서 성공하기 위해서는 성능 개선과 기능 개편을 통한 제품 차별화는 물론 이거니와 앞서 언급한 바와 같이 신규 공격에 대한 빠른 보안대응 서비스가 관건이라고 할 수 있다. 그렇다면 UTM 보안 어플라이언스 시장에서 차별성을 갖기 위한 핵심 보안 기술은 무엇인가.

현재 점차 지능화되어 가는 보안 위협을 해결하기 위해 네트워크 보안 기술도 끊임없이 발전했다. 초기에



는 물리적 공격에 대한 단순 방어로 시작했으나 지능화된 보안 위협에 대처하기 위해 스테이트풀 인스펙션(Stateful Inspection) 기술을 사용했다. 기존의 방화벽이 대표적인 어플라이언스들이다.

그러나 더욱 정교하게 지능화된 보안 위협이 증가하자 스테이트풀 인스펙션 기술의 한계점이 드러났고, 결국 딥 패킷 인스펙션(DPI: Deep Packet Inspection)이 개발되었다. 이는 IDS와 IPS가 탄생한 배경이 되었다. 물론 딥 패킷 인스펙션은 보안 위협이 소량 패킷에 숨어 있을 경우 이를 효과적으로 탐지하고 차단할 수 있으나 딥 패킷 인스펙션으로 제어가 가능한 패킷은 1천500바이트에 불과하다.

보통 인터넷으로 전송되는 대부분의 바이러스와 웜은 크기가 수백 혹은 수천 바이트로 구성되거나 수백만 바이트 길이의 파일에 숨어져 있기도 한다. 따라서 한번의 소량의 패킷만 검사하는 콘텐츠 분석방법으로 모든 바이러스와 웜을 검색할 가능성이 매우 낮을 수밖에 없다. 이같은 딥 패킷 인스펙션 기술의 한계를 극복함은 물론 UTM 보안 시장에서 차별화된 기술력으로 시장 장악력을 높일 수 있는 것이 바로 킴플릿 콘텐츠 인스펙션(CCI: Complete Contents Inspection) 기술이다.

킴플릿 콘텐츠 인스펙션의 핵심은 패킷 페이로드를 파일, 문서, 프로그램과 같은 어플리케이션 수준의 개체로 재조합한 후 해당 개체를 분석해 콘텐츠 기반 공격을 검사하는 것이다. 이러한 콘텐츠 재조합 기술을 이용하면 용량이 큰 파일에 숨어있는 바이러스 및 웜 같은 주요 위협을 확실히 제거할 수 있다. 즉, 딥 패킷 인스펙션 방식의 완벽하지 못한 바이러스, 웜 검색 및 유해한 웹 콘텐츠나 스팸 메일의 처리 한계 등의 결함을 킴플릿 콘텐츠 인스펙션을 통해 보완할 수 있는 것이다.

그러나 킴플릿 콘텐츠 인스펙션은 기존의 딥 패킷 인스펙션보다 더 많은 시간과 자원을 필요로 하기 때문에 하드웨어 기반의 ASIC 솔루션이 아니고서는 성능문제로 인해 상용화되기 매우 힘든 기술이다.

앞서 UTM 보안 시장의 치열한 경쟁 속에서 우위를 확보하기 위해서는 차별화된 기술력과 위협 대응 서비스가 우선시되어야 한다고 밝혔다. 국내를 넘어서 전세계 사용자에게 UTM 보안 어플라이언스를 공급하기 위해서는 무엇보다도 완벽한 보안 위협에 대한 대응 방법이 필요하다. 이에 따라 킴플릿 콘텐츠 프로텍션 기술과 새로운 위협에 대해 대응 인프라를 갖추는 것이 UTM 보안 시장에서 경쟁력을 확보할 수 있는 차별화된 능력이 될 것이다.

(그림) 2003~2004년 세계 보안 시장 전망(CAGR: 연평균영업이익성장률)

