차세대 네트워크 기술로서 통합보안 솔루션에 관한 연구

주 헌 식*

◈ 목 차 ◈

1. 서 론

정보 통신 기술의 급속한 발전은 각종 인터넷 서비스 사용에 대한 비중을 증대시켰다. 또한 인터넷은 각종 서비스의 순기능을 제공하여 삶에 많은 편리를 제공하고 있지만 그와 더불어 역기능인 정보시스템의 침해 사고 및 네트워크 침해 사고가 급증하고 있다. 정보 보호의 필요성과 시스템 보안으로 침입 차단시스템(Firewall), 침입탐지시스템(IDS: Intrusion Detection System), 침입방지시스템(IPS: Intrusion Prevention System) 등을 운용하고 실시간 탐지를 하고 있지만 침입 유형이 매우 다양화되고 고도화 되면서 침해 대응이 어렵고, 개별 보안시스템 중심의 네트워크 보안 관리의 어려움이 중요한 문제로 대두 되고 있다. 최근 발생한 7.7 DDoS 공격은 악성코드를 사용해 특정 PC들을 좀비 PC로 만들어 정해진 시간에 트래픽을 증가시켜 사이트가 정상적으로 동작하지 못하도록 하는 방법으로 DDoS 공격을 하였다[1,2]. 이와 같은 해킹, 웜, 바이러스 및 서비스거부공격 등의 디지털 공격은 계속 증가하고 있으며 공격기법과 공격 대상은 점점 다양해지고 있다. 과거에는 단일 보안 기능을 제공하는 보안솔루션을 통해 보안위협에 대응해 왔으나 다수개의 단일 보안 솔루션으로 구축한 보안의 경우, 어떤 종류의 보안 위협은 시스템과 시스템 사이의 틈새를 통해 통제를 벗어날 수 있으며 서로 다른 OS, 사용자 인터페이스, 로그 포맷 및 리포트 포맷을 가진 포인트 보안 솔루션을 구축하고 운영하는 것은 비용에 있어서도 효율적이지 못하다. 보안 위협이 보다 다양해지고 복합적인 형태로 나타나면서 다수개의 보안 기능을 통합해서 제공하는 통합위협관리시스템 UTM(Unified Threat Management)이 대두 되고 있다[3,4]. 지금까지 보안 솔루션은 그 목적에 따라 방화벽, IDS, IPS, VPN, DB 보안, 웹 보안, 콘텐츠 보안 등 다양한 솔루션 형태로 분화 및 발전해 왔다. 그로인해 다양한 보안 솔루션의 도입에 따른 비용 과다 문제와 각각의 보안 솔루션 운용 방법을 익히기 위한 시간 비용, 그리고 운용을 위한 물리적 공간과 인력 확보가 요구되면서 이에 대한 효과적인 관리 대안이 필요 되었고, 그 강구책으로 등장한 것이 바로 통합 보안시스템(UTM) 이다. 본 논문에서는 차세대 네트워크 기술로 부상하고 있는 통합 보안 솔로션에 대해 기술하고자 한다[5]. 논문 구성은 2장에서는 통합보안시스템의 진화로서 UTM에서 대해서 기술하고 3장에서는 XTM의 진화에 대해서 기술하고, 4장에서는 통합 보안시스템 적용 사례에 대해서 기술하고 5장에서는 결론으로 맺는다.

* 삼육대학교 컴퓨터학부

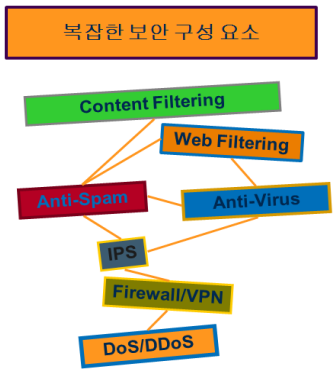
2. UTM의 진화

최근 보안에서 가장 커다란 이슈로 등장한 것이 UTM (Unified Threat Management)이다. UTM은 다기능,

고성능의 통합보안으로 방화벽, 가상사설망(VPN), 침입탐지시스템 및 침입방지시스템(IPS), 안티 바이러스, 안티 스팸과 같은 다양한 보안 기능을 단일 Appliance 형태로 구성해 관리의 복잡성을 최소화하고 복합적인 위협 요소를 효율적으로 방어하기 위한 통합보안솔루션이다. IT환경이 변하고 시대가 변할수록 금적적인 이익을 위한 사이버 위협과 공격은 점점 더 지능화되고 다양화되고 있으며 이러한 복잡한 공격들은 보안을 방어하는데 더욱 어렵게 만든다. 이에 다양한 보안 솔루션들이 도입되어 구축되고 있으며 단일 솔로션이 강구되어 구축되고 있는데 이들은 보안투자비용의 상승과 관리상의 문제점 등으로 효율적인 보안을 담당하기에 비효율적이라고 사료된다. 따라서 이러한 보안을 위협하는 문제들을 해결하고 관리, 비용 등의 총제적인 측면에서 많은 이점을 가지고 있는 통합보안이 대두되었다[5].

2.1 통합 보안 트랜드 변화

2009년 네트워크 보안의 핵심 키워드는 '통합'이었으며 차세대 네트워크 기술로서 통합 보안 시스템(UTM)이 이슈화 될 것으로 전망한다. 7.7 DDoS 대란은 보안솔루션 인식에 큰 변화를 가져오는 계기가 되었다. DDoS 단일 장비만으로 방어의 한계가 있고 그에 따른 대응체계를 통합적으로 구축함으로써 피해를 최소화 할 수 있다는 보안의 트렌드가 형성됨으로써 전용 장비로서 특정 목적을 위해서만 개발 되고 설치·운영 되는 보안의 트렌드에 변화를 가져왔다[6]. (그림 1)은 UTM의 통합보안구성요소의 기능들이다.



(그림 1) UTM의 통합 보안 구성 요소

통합보안장비와 전용보안장비에 대한 이견이 있는데 다음 예로서 통합 장비에 대한 트랜드 변화를 인지하도록 한다. 요즘 출시되는 핸드폰은 멀티 기능을 가지고 있다. 전화기, 사진기, 전자사전, 게임기, 전자수첩, mp3 플레이어, 동영상 플레이어, 거기에 거울기능까지 다양한 기능들을 제공하고 있다. 이들 다양한 기능들은 고유의 독립적인 장치들을 핸드폰으로 통합하여 운용하고 있는 것이다. 전용보안장비와 비교해 볼 때 전화기는 통화 품질에 관해서 최적의 품질을 보증하지만 이동성이나 다른 멀티 기능의 수행에서는 제약을 받게 된다. 마찬가지로 한부분에 대한 보증은 가능하지만 다른 고유의 기능에 제한을 받는 것을 멀티 기능을 추가함으로써 다양한 기능 제공과 더불어 다른 고유한 기능들을 수행할 수 있게 된다. 마찬가지로 통합보안장비에서도 전용 장비로서 한 가지 기능만 제공하였던 것을 다양한 기능들을 통합적으로 지원할 수 있도록 한 것이 통합 보안시스템이다. 이처럼 전용보안장비만큼의 품질과 성능을 제공하면서 다양한 기능들을 추가적으로 제공함으로써 더 좋은 효율성과 품질을 제공하는 통합보안시스템으로의 트래드 변화를 가져왔다.

2.2 통합보안시스템 동향

통합보안솔루션의 등장은 2000년대 초·중반 외산제품인 FortiGate가 국내에 처음 소개되면서 시작되었고 국내 업체로는 최초로 2007년 중반 안철수 연구소가 TrusGuard 제품을 출시하면서 등장하게 되었다[7].

UTM 시장 규모는 작년 2008년 327억으로 2007년 313억에 비해 4.4% 성장했으며 올해에도 4% 성장할 수 있을 것으로 예상되고 있다. 전 세계적으로 본다면 UTM 시장규모는 작년에만 20% 성장한 것으로 알려졌으며 올해도 이와 비슷할 것으로 업계는 전망하고 있다.

IDC의 자료에 의하면 2009년 Global UTM 시장의 규모는 전통적인 방화벽/VPN 시장을 넘어 설 것으로 예측하고 있다. 기존 네트워크 보안 시장의 강자였던 체크포인트, 주니퍼, 시스코 등이 UTM 솔루션을 출시했고 많은 업체들이 통합보안 시스템 제품을 생산하였다.

글로벌 시장에서도 UTM이 전용 솔루션으로 장악하고 있는 High-end 대형고객 시장 진입하였고 모든 역량을 쏟아 수십 기가 처리량의 UTM 제품으로 진출하고 있다.

한편 국내에서도 UTM이 중소·중견기업(SMB)를 대상으로 하는 솔루션으로 인식되고 있다. 우리나라의 UTM 솔루션은 대부분 방화벽이나 VPN, IPS 기반으로 통합솔루션 형태로 변화했기 때문에 다른 보안기능에 대해서는 신뢰도가 부족했지만 여러 보안업체들이 캐리어급 네트워킹 지원과 UTM솔루션의 기능을 보강한 엔터프라이즈급 솔루션으로 체질변환을 나타내면서 많은 부분에 인식이 전환되었다.

올해 또한 UTM시장은 공공기관과 중소기업에 이어 교육망 사업에 집중하고 있는 경향을 보이고 있다. 특히 시군구 단위 교육청 산하 교육망의 경우 CC인증 없이 구축이 가능한 사례가 많아 이를 중점적으로 공략하는 업체가 늘어가고 있다.

현재 국내외 시장에 나와 있는 제품들만 보더라도 대부분의 업체들이 방화벽, IPS, 바이러스월 외에 VPN, 스팸차단, URL 필터링과 같은 기능들을 제공하고 있으며 이러한 추가 기능들은 경쟁적 차원에서 보다 가속화될 전망이다.

따라서 방화벽은 기본이고 IPS, QoS, 스파이웨어 등 고객들이 선호하는 각종 기능을 통합보안장비에 추가했다. 통합보안의 시장적인 측면에서 보다 다양한 형태로 발전할 전망인데 먼저 SMB에 치중돼 있던 통합보안 시장이 내년에는 중대형 시장으로 더욱 확대될 것이라고 예상하며 10G급 통합보안 제품들로 통합보안 시스템이 활발히 전개될 것으로 예상한다.

2.3 통합보안, 비용절감·효율성이 장점

UTM의 도입은 고가의 Point Solution을 구입할 필요가 없기 때문에 구축 및 운용에 있어 상당한 비용절감 효과를 가져 온다는 것이 가장 큰 장점이다[8]. 즉 방화벽 외에 별도의 IPS, VPN, Web Filtering, Anti-Spam, Anti-Virus, Dos / DDoS, Content Filtering, Gateway 등의 솔루션을 도입하려면 어마어마한 초기 구축비용이 소요될 뿐만 아니라, 각 솔루션 별 유지보수 계약을 별도로 체결하고 이에 더하여 별도의 유지보수 비용과 관리 인력을 책정하여 운영해야 하는 매우 비효율적인 상황이 발생 한다. UTM은 우선 Firewall-based Security를 포함한 다양한 보안위협에 효과적으로 대응할 수 있다. 보안의 기본 인프라는 Gateway단에서 내·외부로 흐르는 트래픽의 기본적인 통제를 해주는 방화벽이라고 할 수 있는데 방화벽은 정해진 내부 보안정책에 따라 합법적인 접근과 불법적인 접근을 구분하고 불법적인 접근에 대한 효과적인 접근 제어를 목적으로 하고 있다. 더 나아가서 합법적인 접근 내에 숨어 있는 비정상적인 공격에 대해서도 다양한 보안 기능들의 유기적인 정책으로 적용하여 보다 안정된 보안을 유지할 수 있다.

한 예로서 웹 취약점을 활용하여 내부정보 또는 사용자 계정을 탈취하는 SQL Injection 해킹은 방화벽만으로는 막을 수 없다. 그러나 UTM은 IPS Signatures에 SQL Injection 공격기법의 패턴을 보유하고 있어 효율적인 방어를 제공할 수 있다. 또한 일부 진화된 UTM 솔루션은 IPS Signature 기반의 (D)DoS 방어 기능에 더하여 별도의 DDoS 방어 엔진을 보유해 다양한 종류의 DDoS 공격에 효과적으로 대응할 수 있다

UTM의 가장 큰 장점은 하나의 장비에 여러 보안기능이 함께 동작하므로 여러 장비를 사용하지 않아도 되므로 관리적인 측면과 경제적인 측면에서 크나큰 장점으로 볼 수 있다. UTM은 진화된 형태의 IPS로 인식하고 있으므로 UTM의 가장 핵심적인 기술은 무엇보다도 IPS(Intrusion Prevention System) 기능이라고 할 수 있다. IPS 기능은 단순 알려진 위협만을 처리하는 것이 아니라 알려지지 않은 위협에 대해서도 대응해야 하므로 자가 학습을 통한 이상징후(Anomaly) 판단이 필수적인 요소라고 할 수 있다. 또한 패킷 레벨에서부터 응용 레벨에 이르기까지 탐지 영역을 확대하여 보안 정책을 적용하여 보다 강하된 보안을 담당한다.

한편 현재 기관 망 및 대형 사이트의 대역폭은 1G에서 10G로 확대된 상황이므로 기존의 1G급의 장비로 현재의 네트워크를 대처하는 것은 많은 비용과 관리적인 어려움이 있다. 하지만 각 제품사 별로 Trade-In 하여 업그레이드 하면 비용면에서 상당히 경제적인 방법이 된다.

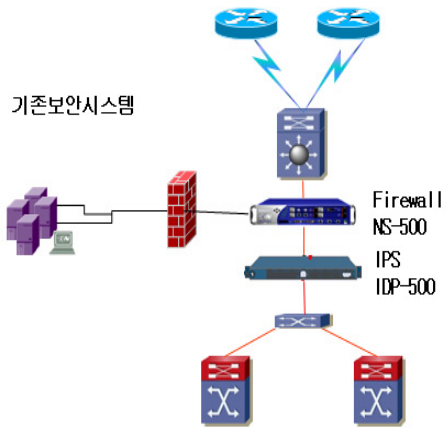
3. XTM의 진화

IDC는 XTM이라는 용어를 새롭게 정의하면서 '네트워크 보안의 미래'라고 소개했다. XTM 플랫폼은 보안 기능과 네트워킹 역량, 관리 유연성을 대폭 확장하여 전통적인 보안 경계를 허물고 네트워크 보안을 새롭게 정의하였다. eXtensible Threat Management의 약자인 XTM은 '확장'을 뜻하는 X, 알려지지 않은 미지수 'x'를 의미하면서 향후 미래형 위협에 대해서도 적극적인 대응이 가능하다는 점을 강조하고 있다. 이 XTM의 조건으로는 기존 보안 기능에 덧붙여서 새로운 위협에 대한 대응을 위해 실시간 업데이트가 가능하고 중앙 집중화 된 단일 콘솔을 통해 강력한 관리 기능(통합로깅, 통합 리포팅, 이벤트 상관관계 분석 등), 네트워크 트래픽 컨트롤 가능, 취약성 관리기능 제공, 도입 비용 보호를 위한 유연성 제공 등을 제공한다[9]. 초창기의 UTM은 방화벽, VPN, IPS/IDS 정도로 사용되어 왔지만(하드웨어의 한계 등에 의해), 보다 강력한 보안을 위해 여러 단계의 진화를 거치고 UTM의 한계점을 극복하여 XTM(eXtensible Threat Management)이 나오게 되었다. UTM의 한계점 이라고 할 수 있는 A/V, A/S, DDoS, NAC, WAF, SSL.. 등 UTM에서 구현하지 못했던 기능들을 확장하여 제공함으로써 다양한 공격에 대응할 수 있도록 설계하였고, 차세대 네트워크의 가장 큰 이슈가 되는 IPv6 기술인 IPv4-IPv6 Translation, IPv4-IPv6 Tunneling, IPv6 Masquerading 등을 완벽하게 지원함으로써 네트워크망에 최적화로 개발 하였다. XTM은 Multicore Based Processing 환경으로 개발되었으며 Multicore process는 특정 기능들을 각 별도의 Process에 할당하여 분산 처리함으로써 성능의 한계점을 극복하고 최고의 성능을 낼 수 있게 설계 하였다. 또한 점점 늘어나는 트래픽을 처리할 수 있도록 10G 인터페이스를 지원하며 Hybrid-Model S/W설계로 데이터와 기능 분할을 접목하여 효과적으로 트래픽을 처리할 수 있도록 설계 하였다. XTM의 한 제품은 기존의 방화벽에 안티스팸·게이트웨이 안티 바이러스·IPS(침입방지 시스템)·URL 필터링 등을 통합한 UTM(통합위협관리) 제품군에 더욱 다양한 보안기능과 네트워킹 기능을 추가하고 관리 기능을 대폭 향상시켰으며 엔터프라이즈급 성능, 강력한 연결 옵션, HTTPS와 VoIP 보안, 인스턴트 메시징 및 P2P 애플리케이션 블로킹 등 혁신적인 기능을 추가하여 네트워크를 강력하게 보호 하는 기능을 제공한다. 또한 클러스터링, 로드 밸런싱 등 첨단 네트워킹 기능은 물론 역할기반 액세스 컨트롤 (RBAC), 중앙집중형 멀티박스 관리 기능, 리포팅 기능도 대폭 향상시켰다[10,11].

또한 웹 취약점이나 DDoS 공격 방어, VPN 네트워크를 구축함에 있어 통합보안솔루션의 가장 큰 장점은 VPN 터널을 통해 전파되는 악성코드의 전체 네트워크 확산을 방지할 수 있고 End-point 백신 솔루션과 연동하여 NAC 형태의 이중 보안을 구축할 수 있도록 하였다. 따라서 UTM의 한계를 심층 해결한 진화를 나타낸다[12,13,14].

4. 통합보안적용사례

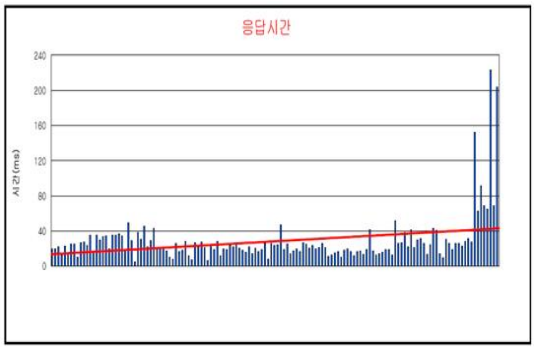
일반 업체인 L 사는 보안 시스템을 도입하여 보안 정책을 구축하고 있는데 보안 시스템 도입 시기가 2003년으로 다소 오래된 보안 시스템으로 보안 시스템 교체를 앞두고 있었다. 따라서 L 사는 인지도가 있는 J 사의 통합 보안 시스템으로 교체하기를 계획하였다. 기존 장비는 J사의 보안장비로서 NS-500과 IDP-500를 도입하여 운영하였으며 (그림 2)와 같다[15,16].



(그림 2) L사 NS-500과 IDP-500

4.1 평가 분석

초기 도입 후 많은 시간의 경과로 시스템의 성능이 많이 떨어진 상태인데 시스템의 성능을 테스트 하기 위해 응답 속도와 초당 처리 세션을 평가해 보니 (그림 3)과 같은 결과를 나타내었다[17,18].

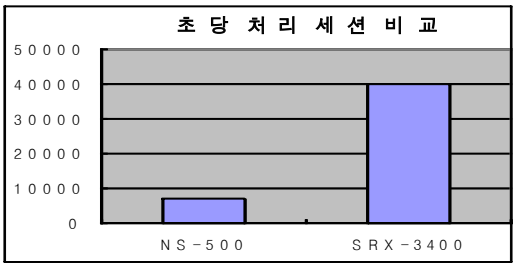


(그림 3) 기존 보안시스템의 응답 시간

(그림 3)에서 보는 것처럼 응답처리시간 분석 평가에서 응답 속도는 평균 54nm이며 최대 220nm까지 나타내고 있는데 이것은 보안 장비의 권장 응답 수치 10~20nm에 비해서 방화벽에서 상당히 전송이 지연되고 있는 것으로 볼 수 있다.

4.1.1 초당 세션 처리 분석 평가

두 번째 실험에서는 NS-500의 초당 세션을 평가해 보기로 하였다. 실험 결과는 (그림 4)과 같다.



(그림 4) 기존 방화벽 응답 시간

(그림 4)의 실험 결과 초당 처리 세션에서는 7,000 세션을 나타냈는데 이것은 한사람이 4개의 세션을 발생시킬 경우 7,000 세션(초당) / 4 세션 = 동시 1,750 명의 수치가 나온다.(참고로 www.naver.com 접속시 10개의 세션이 생성됨). 실험결과 초당 7,000 세션을 초과 할 경우 응답 속도 지연이 발생됨을 알 수 있다. 기존보안시스템의 장비 성능은 (표 1)과 같다.

(표 1) 기존 보안 시스템 성능

기존보안시스템 시스템			
NS500		IDP-500	
동시세션	250,000	동시세션	220,000
초당세션	7,000	초당세션	5,000
방화벽성능	700M	IPS성능	500M
인터페이스	8x10/100 4xGBIC	인터페이스	2x10/100/1000 2xGBIC
트랙픽처리	CPU	트래픽처리	CPU
NAT	지원	AV 기능	미지원
DDoS차단	미지원		

4.1.2 CPU 사용량 분석 평가

실험 결과 CPU의 60~70% 부하가 발생하고 있음이 나타났다. 권장 CPU는 30% 이내인데 반해 60~70%는 CPU 부하에 2배 이상 높은 것으로 나타났다. 그래서 이러한 문제들을 해결하기 위한 여러 해결책을 강구해 보았지만 사용 중인 IPS-500 제품의 OS 업그레이드는 이미 중단 되었고 NS-500 제품은 2006년에 생산, 판매가 중단되어 H/W 장애 시 빠른 복구에 어려움과 기술 지원에 어려움을 인지하게 되었다. 그래서 이들 보안 장비의 대안으로 대두 된 것이 UTM 보안장비로 보안기술 및 성능 향상을 통합적으로 지원하는 시스템을 선택하게 되었다.

4.2 제안 통합 보안 시스템 설계 및 구현

기존 보안 장비 성능 분석 결과 응답 시간 지연은 초당 처리 세션 초과로 인한 응답 시간 지연이 발생하고 있음을 되었다. 따라서 이러한 문제들을 해결하기 위한 장비 보강으로 (표 2)와 같이 나타내었다.

(표 2) 기존 보안시스템과 제안 통합 보안 시스템 성능 비교

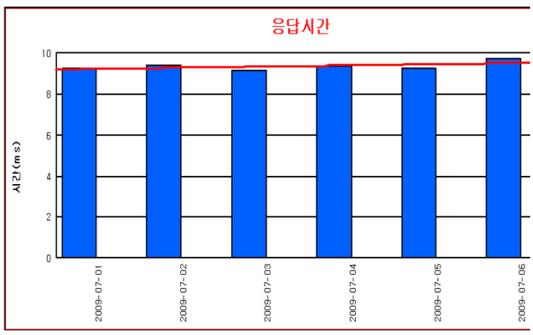
시스템 / SPC.	기존	제안	기존	제안
	NS-500	SRX3400	IDP-500	SRX3400
동시세션	250,000	500,000	220,000	500,000
초당세션	7,000	40,000	5,000	40,000
방화벽 성능	700M	10G		
IPS성능			500M	1G
인터 페이스	8x10/100 4xGBIC	8X10/100 /1000 4xGBIC	2x10/100 /1000 2xGBIC	2x10/100/ 1000 4xGBIC
트래픽 처리	CPU	NPU (ASIC)	CPU	NPU (ASIC)
NAT	지원	지원		
AV기능			미지원	지원예정
DDoS차단	미지원	지원		

4.2.1 응답처리시간 평가 결과

(그림 3)에서의 기존보안시스템의 응답 속도와 제안 통합 보안 시스템에서의 응답속도는 (표 3)와 (그림 5)과 같이 제안 보안시스템에서는 상당히 응답 처리 속도가 빠름을 나타내었다.

(표 3) 제안 통합보안 시스템 응답 처리속도 비교

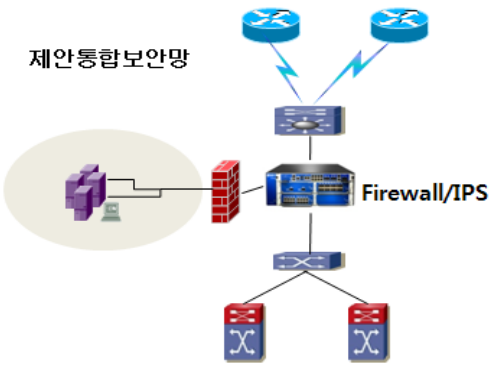
시스템 비교	기존보안시스템	제안통합 보안시스템
응답속도	평균 54ms 최대 220ms	평균 10ms 최대 10ms



(그림 5) 제안 통합보안시스템 응답 처리속도 비교

4.2.2. 초당 세션 처리 평가 결과

앞에서 초 당 동시 세션 7,000를 초과할 경우 응답 속도 지연이 발생 하였으나 [표 4]의 제안 시스템에서 40,000만 초과 시에 지연이 발생함으로 3배이상의 성능을 나타내고 있다. 또한 트래픽을 고려하여 앞으로 7~8년 이상 사용할 수 있는 보안 장비 스팩이라고 제안 되며, 스위칭 패브릭 ASIC 기반의 차세대 방화벽 및 IPS로 모듈 추가를 통한 성능 향상을 지원하며 대량의 초당 세션 및 트랙픽 처리에 적합하고 NUP 기반의 Dos 및 DDoS 차단 기능을 제공하여 syn-frag, tcp-no-flag, fin-no-ack, winnuke, icmp-flood, udp-flood, block-frag, icmp-fragment, icmp-id, icmp-large, ip-bad-option 기능들을 수행한다. 따라서 향후 장비 교체 없이 UTM(통합 보안) 기능까지 수용할 수 있는 통합 보안 시스템으로 보안 장비에 대한 경제성에 있어서 상당한 기여가 될 수 있음을 나타내었고 통합 보안 시스템은 (그림 6)과 같다.



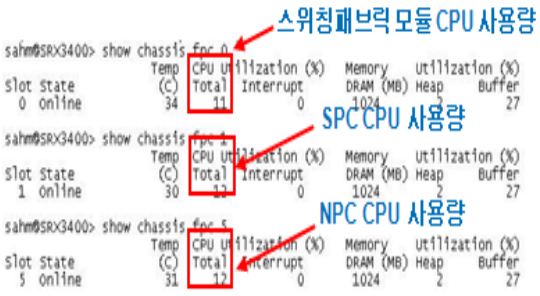
(그림 6) 제안 통합 보안 시스템 구성도

4.2.3 CPU 사용 평가 결과

또한 (그림 3)의 응답처리속도가 느린 것은 초당 세션 초과에 따른 CPU의 처리속도로 기존 보안시스템에서는 CPU 1개로 처리하는 기존보안시스템과 CPU 3개로 처리하는 제안통합보안시스템은 기존 보안시스템에서의 평균 60~70%에 비해서 제안통합보안 시스템은 평균 10% 사용을 나타내며 처리에서 5배의 성능으로 빠른 응답처리 속도를 나타내며 (표 4)와 (그림 7)로 비교를 나타내었다.

(표 4) 제안 통합 보안시스템 CPU 및 응답 처리 속도

CPU 사용량	기존보안시스템	제안통합 보안시스템
cpu 개수비교	1개	3개 3개 모듈이 개별 cpu/Memory 사용
cpu사용량 비교	평균 60~70% 사용	평균 10% 사용



(그림 7) 제안통합보안시스템 CPU

4.2.4 정책기능 적용 평가 결과

또 다른 평가 결과로서 정책 기능 적용을 (표 5)와 같이 기존 보안 시스템 시스템과 제안 통합 보안 시스템에 대해 방벽 보안정책, DDoS공격 차단정책, IPS 보안정책 기능 적용을 내부와 외부, DMZ에 정책적으로 적용된 것을 나타내었다. 결과에서 보는 것과 같이 기존보안시스템에서는 미적용 되었던 DDoS 공격차단의 외부에서 내부 그리고 DMZ로 적용되었던 것을 제안통합보안시스템에서는 적용되었고, IPS보안정책에서도 기존보안시스템에서는 외부에서 내부로 미적용 되었던 것을 제안통합보안시스템에서는 신규 적용 하였다. 따라서 정책기능에서 보다 강화되어 시스템을 보장한다.

(표 5) 기존보안시스템과 제안통합보안시스템의 정책 비교

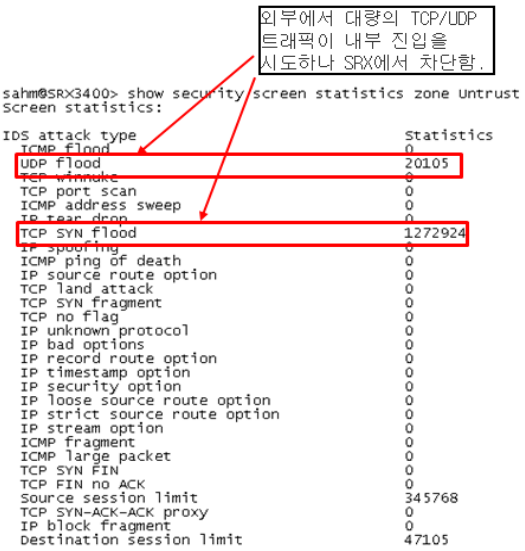
정책 기능 \ 시스템 비교		기존보안 시 스 템	제안통합 보안시스템
방화벽 보안 정책	내부⇨외부	적용	적용
	외부⇨내부	적용	적용
Dos공격 차단	내부⇨외부/DMZ	적용	적용
	외부⇨내부/DMZ	미적용	신규적용
	외부⇨DMZ	미적용	신규적용
IPS 보안 정책	내부⇨외부	적용	적용
	외부⇨내부	미적용	신규적용

4.2.5 유해 트랙픽 차단 정보 평가 결과

외부에서 대량의 TCP/UDP 트래픽으로 내부 진입을 시도하여 DDoS 공격과 같은 해킹 공격을 유발하려고 함으로 정책적으로 적용되지 않은 유해 대량 트래픽으로 분류하여 DDoS 공격 같은 대량 트랙픽을 차단한다. (그림 8)에서 보는 것과 같이 갑자기 숫자가 높아지는 것은 유해 트랙픽으로 의심하여 집중 적으로 분류하고 트래픽을 차단하여 이러한 공격으로부터 데이터와 시스템을 보호하는 안정된 통합보안 시스템으로 보안 담당하게 한다.

```
sahm@SRX3400> show security idp attack table
IDP attack statistics:

  Attack name                                  #Hits
  SMTP:OVERFLOW:TEXT-LINE-OF                   24984
  SSH:BRUTE-LOGIN                              11985
  WORM:CONFICKER:C-ACTIVITY                    3354
  SMTP:MAL:HEADER-NAME-OF                      2350
  HTTP:EXT:METAFILE                            491
  HTTP:SQL:INJ:CMD-CHAIN-2                     372
  HTTP:SQL:INJ:USER-ADD                        74
  HTTP:SQL:INJ:SYSOBJECTS                      63
  VIRUS:SMTP:EXE-IN-ZIP                        44
  VIRUS:SMTP:EXE-ATTACH-1                      41
  HTTP:SQL:INJ:DECLARE-EXEC                    36
  SMTP:EXT:DOT-SCR                             34
  HTTP:SQL:INJ:COMPARISON                      32
  SMTP:EXT:DOT-PIF                             30
  HTTP:PHP:MAMBO-PATH-INCL                     27
  IKE:DOS:ISAKMP-DOS-2                         25
  IKE:DOS:ISAKMP-DOS-1                         22
  SSL:OVERFLOW:KEY-ARG-NO-ENTROPY              22
  SMTP:OUTLOOK:OWA-XSS                         20
  SSL:OVERFLOW:SSL-KEY_ARG2                    16
  HTTP:PHP:PHPBB:PROOTPATH-INJ                 8
  HTTP:IIS:ENCODING:PERC-PERC-1                6
  TROJAN:BACKORIFICE:CONNECTION                6
  HTTP:EXPLOIT:ILLEGAL-HOST-CHAR               4
  DB:MS-SQL:HELLO-OF1                          3
  HTTP:IIS:ENCODING:PERC-PERC-2                3
  HTTP:SQL:INJ:REMOTE-EXEC                     2
  IKE:DOS:ISAKMP-DOS-3                         2
  HTTP:IIS:ENCODING:SINGLE-DIG-1               1
  RPC:RPC.TTDBSERVER:TT-MAL-FS-2               1
  RPC:RWHOD:RWHOD-NULL-INJ                     1
  SMTP:OUTLOOK:LOCAL-LINK                      1
  TROJAN:MISC:NOKNOK-COMMAND                   1
```



(그림 8) 유해 트랙픽 차단

V. 결 론

본 논문에서는 차세대 네트워크 기술로서 통합 보안 솔루션을 제안하였다. 오늘날 보안 이슈 및 해킹 공격 기법이 다량화, 대형화, 지능화가 되면서 특정 장비 및 단일 솔로션 도입만으로 보안 위협에 안전하지 않다. 따라서 다수의 단일 보안 솔로션은 비용에 있어 비효율적이며 시스템이 관리 측면에서도 상호 보완이 이루어야 보다 강화된 보안을 유지 할 수 있다. 개별 운용은 시간적, 물리적, 공간적, 관리적 측면에서 비 효율적이다. 따라서 통합시스템인 UTM으로 진화하였고, UTM은 통합시스템으로서 단일 시스템에서의 비 효율성을 해결하는 대안으로 대두 되었다. 하지만 UTM의 장점이 많이 있음에도 불구하고 UTM의 한계를 보완하는 확장으로서 XTM으로 진화하였다. XTM 솔로션은 향후 차세대 네트워크 솔로션으로 상당한 각광을 받을 것으로 예상한다. 본 논문에서는 통합보안시스템의 적용 사례를 통해 비용과 성능의 효율성으로 실험을 결과를 나타내었다. 실험 결과 기존 보안시스템에 비해서 제안한 통합보안시스템은 응답처리속도에서 80%의 성능 향상을 나타내었고, CPU 사용량도 평균 10%로 모듈별 CPU를 사용함으로써 트래픽 증가 시에도 기존 보안 시스템 대비 사용량분 석 평가에서 85%의 감소를 나타내었다. 또한 초당처리세션에서는 3배의 성능을 보였다. 방화벽에서도 기존 보안정책들을 수용할 뿐아니라 추가적인 기능들을 적용함으로써 보안의 안정성을 강화하였다. 향후 보안 시스템 강화시 각 솔루션의 특성과 경제성을 고려한 보안 강화를 제안한다.

참 고 문 헌

[1] 이근수, 박지현, 장진용, 송주석, 유동영, “DDoS 공격에 대한 탐지 및 추적 시스템제안”, 한국정보보호학회, 제 11권, 제1호, 39-40쪽, 2001년.

[2] 최희식, 전문석, “ DDoS TCP Syn Flooding Backscatter 분석 알고리즘”, 한국컴퓨터정보학회 논문지 제14권 제 9호, 55-66쪽, 2009년 9월. [3] 윤재영, “네트워크 통합 보안 기술 및 시장 동향: UTM 급속 확산, 경영과컴퓨터, 통권 364호, 120-123쪽, 2007년 2월.

[4] 임채호, “보안 위협에 따른 UTM 필요성 : 다양해진 보안 위협 대비 위한 UTM 장비 점차 각광”, 경영과컴퓨터, 통권 365호, 140-143쪽, 2007년 3월.

[5] 김정은, “국내 통합보안 솔루션 적용 실태 와 전망”, 컴퓨터월드, 통권 제 307호, 25-47쪽, 2009년 5월.

[6] 정국용, “ 네트워크 시스템의 통합보안 방안에 대한 연구”, 서울산업대석사학위논문, 1-56쪽, 1996년.

[7] 이창우, 김석훈, 송정길, “분산 환경에서의 침입방지를 위한 통합보안 관리 시스템 설계”, 한국컴퓨터정보학회논문지, 제 11권, 제 2호, 통권 제 40호, 75-82쪽, 2006년 5월.

[8] 서현석, “네트워크 보안 통합의 필요성 보안성 향상 비용 절감,, 공격 고도화 UTM이 해답” ,Network times, 통권 제 179호, 224-226쪽, 2008년 7월.

[9] 이창우, 손우용, 송정길 “통합보안 관리를 위한 침입대응 시스템 설계”, 정보보증논문지. 제5권, 제2호, 51-56쪽, 2005년 6월.

[10] 유응구, “통합 보안 관리자를 이용한 이동 에이전트 이주 성능 향상 연구”, 한국컴퓨터정보학회 논문지, 제 12권, 제 5호, 통권 제 49호, 57-64쪽,

2007년 11월.
[11] 박대우, 서정만, “TCP/IP 공격에 대한 보안 방법 연구”, 한국컴퓨터정보학회, 제 10권, 제 5호, 219쪽, 2005년 11월.
[12] 이춘재, 조기량, “네트워크 이중 인증을 통한 역할 기방 개방형 네트워크 접근 통제 시스템의 구현”, 한국통신학회논문지 32권 8호, 502-508쪽, 2007년 8월.
[13] 박대우, “외부 이동단말의 접근제어를 위한 IP 프로토콜 설계 및 성능 개선에 관한 연구”, 한국컴퓨터정보학회 논문지 9권 2호, 41-48쪽, 2004년 6월.
[14] 구민정, 오창석, “IPv6환경에서 DDoS 침입탐지”, 한국컴퓨터정보학회, 제 11권, 제 6호, 186쪽, 2006년 12월.
[15] 김용탁, 권오준, 이종민, 김태석, “통합 관리를 위한 정책 기반의 보안시스템 설계 및 구현”, 멀티미디어학회 논문지, 10권 8호, 1052-1059쪽, 2007년 8월.
[16] 손우용, 송정길, “통합보안 관리시스템의 침입탐지 및 대응을 위한 보안 정책 모델”, 한국 컴퓨터정보학회 논문지 9권 2호, 81-87쪽, 2004년 6월.
[17] 김석훈, 김은수, 송정길 “통합보안관리 시스템에서의 침입탐지 및 대응을 위한 보안 정책 모델에 관한 연구”. 정보보증논문지. 제5권 제2호, 9-17쪽, 2005년 6월.
[18] 강민균, 김석수 “통합보안관리 시스템에서 내부보안을 향상시킨 보안 솔루션 구조의 설계 및 구현”, 한국콘텐츠학회논문지, 제5권, 제6호, 360-367쪽, 2005년 12월.

◐ 저 자 소 개 ◑

주 헌 식
1994년 : 호서대학교 이학석사
2005년 : 아주대학교 공학박사
1997년- 현재:
삼육대학교 컴퓨터학부 부교수
관심분야 : 정보보안, 네트워크보안, 모바일 네트워크