韓國컴퓨터情報學會 論文誌
第15卷 第9號, 2010. 9.

2010-15-9-3-2

통합 보안 시스템에서의 효율적인 보안 정책 관리 모델

주 헌 식*, 김 종 완**

An Efficient Management Model of Security Policy in the Unified Threat Management System

Heon Sik Joo*, Jong wan Kim**

요 약

본 논문에서는 기존의 단일 보안 시스템의 Firewall과 IPS 시스템의 문제점 분석을 통하여 통합보안 시스템 강화가 비용 대비 효율적임을 나타내었다. 문제점 분석 결과 Firewall과 IPS 의 처리 시간 지연과 효율성 부재를 나타냈다. 따라서 개별 Firewall과 IPS 시스템과 통합 시스템으로 성능 평가를 하였다. 평가 결과 기존 시스템 보다 제안한 통합보안시스템이 응답 처리 시간에서는 평균 5배 이상 성능을 나타났고, 초당 세션 처리에서도 5배 이상 그리고 CPU 처리 성능에서는 6배의 처리 속도가 우수함을 나타냈다. 또한 여러 보안 정책들을 수용하였고, 유해 트랙픽 처리에서도 높은 성능을 나타났다. 결론적으로 본 논문에서는 통합 보안 시스템이 개별 시스템 강화 보다 경제적 측면, 관리적 측면, 물리적 측면, 시간적 측면, 공간적 측면 등 여러 측면에서 효율적임을 강조하였다.

Abstract

This paper showed that the integrated system to fortify security was much more efficient than the respective system through the analysis of problems from Firewall and IPS system in the existing security systems. The results of problem analysis revealed that there were the delay of processing time and lack of efficiency in the existing security systems. Accordingly, their performance was evaluated by using the separated Firewall, IPS system, and the integrated system. The result of evaluation shows that the integrated security system this paper suggested is five times faster than the existing one in terms of processing speed of response. This paper demonstrated the excellence of the proposed security system is also more than fivefold in session handling per second and six times process speeding in the CPU processing performance. In addition, several security policies are applied, and it provided a fact that it gave an excellent performance when it comes to protecting from harmful traffic attacks. In conclusion, this paper emphasized that fortifying the integrated security system was more efficient than fortifying the existing one considering in various respects such as cost, management, time, space and so on.

▸ Keyword : 분산서비스거부(DDos: Distributed Denial of Service), 통합보안시스템(UTM: Unified Threat Management)

• 제1저자, 교신저자 : 주헌식
• 투고일 : 2010. 07. 19, 심사일 : 2010. 08. 07, 게재확정일 : 2010. 08. 19.
* 삼육대학교 컴퓨터학부 부교수 ** 삼육대학교 경영정보학과 연구교수
※ 본 연구는 삼육대학교 2009년 학술연구비 지원에 의해 수행되었음

Ⅰ. 서 론

최근 발생한 7.7 DDos 공격 등 IT환경이 변하고 시대가 변할수록 금적적인 이익을 위한 사이버 위협과 공격은 점점 더 지능화· 다양해지고 있으며 이러한 복잡한 공격들은 보안 담당자들에게 방어를 더욱 어렵게 만든다[1,2,3]. 이에 대응하기 위해서 기업의 보안담당자들은 다양한 보안 솔루션을 도입해 방어해 왔다. 하지만 이렇게 도입된 다양한 보안 솔루션들은 보안 투자비용의 상승과 관리상의 문제점 등으로 효율적인 보안을 담보하지 못했다. 그런데 통합은 이러한 문제들을 해결하고 관리, 비용 등의 총제적인 측면에서 많은 이점을 가지고 있기 때문에 시장에서는 이미 기술적 진화를 거친 고성능 통합(UTM: Unified Threat Management)에 대한 요구가 증가하고 있었고 최근 에 다시 주목을 받고 있다[4,5,6,7].

정보 보호의 필요성과 시스템 보안으로 침입 차단시스템(Firewall), 침입 탐지 시스템(IDS: Intrusion Detection System), 침입 방지 시스템(IPS: Intrusion Prevention System) 등을 운용하고 실시간 탐지를 하고 있지만 침입 유형이 매우 다양화와 고도화 되면서 침해 대응이 어렵고, 개별 보안시스템 중심의 네트워크 보안 관리의 어려움이 중요한 문제로 대두 되고 있다[8,9,10,11]. DDos 공격 등 이러한 공격에 대한 대응 방안으로 여러 해결책들이 있을 수 있지만 기존 보안 장비의 노후화와 성능 저하로 해킹이나 DDos 공격에 취약함으로 장비 업그레이드 측면을 고려하였다. 따라서 기존 보안 장비의 취약성을 인식하고 새로운 보안 장비로 성능을 강화 시키는 것이다. 보안 장비 강화에 앞서 몇 가지 고려 사항들을 먼저 숙고 해 보아야 한다. 장비 구입에 따른 효율성으로서 가격 대비 성능이 얼마만큼 효율성을 갖는지 숙고해 보아야 한다. 본 논문에서는 단일 기능을 수행하는 보안 장비 구입보다는 복합적인 기능을 지원 할 수 있는 통합 보안 장비가 더 경제성이 있다고 판단한다. 따라서 본 논문에서는 통합 보안 장비 구축에 따른 비용 절감과 효율성 측면에서 제안한다. 제안한 통합 보안 시스템을 적용하기 위해 단일 장비 Firewall과 IPS를 대상으로 실험하고, 제안한 통합 장비 시스템으로도 실험하여 효율성을 나타낸다. 2장에서는 관련 연구로 통합 보안 장비에 관련한 장점들을 기술하였고, 3장에서는 단일 장비 Firewall과 IPS에 대해서 문제점을 분석한다. 4장에서는 기존 시스템의 문제점에 대한 보안 강화로 통합 시스템의 성능 테스트 결과를 기술하고 5장에서는 결론을 나타낸다.

Ⅱ. 관련 연구

2.1 통합보안 장비의 장점

최근 보안 시장의 가장 큰 이슈는 UTM이라는 다기능, 고성능의 통합 보안이다. UTM이 사용자의 요구사항을 충분히 만족시키는 고성능의 장비로 발전 한다면 더 이상의 보안 장비는 없을 것이라는 견해도 있다. 즉 그만큼 UTM은 미래 차세대 통합 보안 장비로 서 우수하다고 판단한 것이라 볼 수 있다 [12,13]. 방화벽, VPN, IPS, Anti-Virus, Anti-spam, Anti-spy ware, NAC, WAF, SSL 등의 솔루션들을 도입하려면 어마어마한 초기 구축비용이 소요될 뿐만 아니라, 각 솔루션 별 유지보수 계약을 별도로 체결하고 이에 더하여 별도의 유지보수 비용과 관리 인력을 책정, 운영해야 하는 매우 비효율적인 상황이 발생할 수도 있다. 기업의 보안 정책에 의해 고 비용 구조임에도 반드시 전용 장비를 도입해야 하는 기업이 아니라면 통합 보안장비는 기업에 강력한 비용절감 효과를 제공한다[14]. 보안 효율성을 향상시킬 수 있다는 점이 통합 보안 장비의 장점이다. 통합 보안 솔루션은 일반적으로 게이트웨이 보안 장비이다. 게이트웨이에서 여러 종류의 보안 위협을 차단하면 내부 네트워크는 더욱 안전하게 보호된다. 악성 프로그램들이 데스크탑 이나 서버까지 침투할 수 없기 때문에 기업 내부의 중요한 파일이나 애플리케이션을 보호할 수 있다[15,16,17]. 관리의 편리성과 인건비 절감도 통합 보안 장비가 각광받는 이유 중 하나이다. 여러 개의 단독형 전용 보안 장비를 사용하고 있는 기업에서는 그에 따른 보안 인력을 많이 보유하기가 쉽지 않은 관계로 보안 관리자나 운영자가 모든 장비를 관리할 수 밖에 없다. 이는 각기 다른 업체에서 만들어낸 다른 기능을 가진 장비를 다루다 보니 특성이 다른 각 장비들을 컨트롤 및 모니터링을 위해 많은 시간을 투자 하여야 한다. 심지어 보안 담당자가 장비의 컨트롤을 엔지니어에게 종속 될 수 있다[18]. 또 다른 측면으로 로그 포맷이나 저장위치도 시스템 별로 각각 달라 기업의 네트워크 상황을 전체적으로 파악하기 위해서는 각각의 로그를 별도로 수집하고 이를 분석해야 하는데 통합 보안 솔루션을 이용하면 이를 간단히 해결할 수 있다[19,20]. 또한 통합 보안 장비는 기업 전반에 걸쳐 일관성 있는 보안 정책을 적용 할 수 있다는 것이 가능하다는 점에서 유용하다. 모든 보안 서비스를 통합 하여 한 대의 장비에 탑재하였기 때문에 보안 정책의 적용과 변경이 용이하다[21,22]. 따라서 UTM은 방화벽, 가상

사설망(VPN), 침입 탐지 시스템 및 침입방지 시스템(IPS), 안티 바이러스, 안티 스팸과 같은 다양한 보안 기능을 단일 Appliance 형태로 구성해 관리의 복잡성을 최소화하고 복합적인 위협 요소를 효율적으로 방어하기 위해서 통합 보안 솔루션이 빠르게 성장해 왔다. 향후에는 대형 사이트에서 복잡해지는 보안기기에 대한 관리에 대한 어려움과 성능에 대한 이슈로 복합적으로 처리해 주는 통합 시스템이 주요 보안 솔루션으로 자리 매김할 것이며 통합 보안 장비가 각광을 받게 될 것이라고 사료한다.

2.2 통합 보안 비용절감 및 효율성

현재 국내·외 보안 시장의 가장 큰 이슈는 다기능의 성능을 갖춘 통합 보안이라고 할 수 있다. 다양한 보안 기능을 하나로 통합한 통합 보안 장비를 도입하면 기존에 개별 전용장비를 구입하여 보안 시스템을 구축하는 것과 달리 여러 장점을 갖게 되는데 그 중 하나로 비용 절감 효과를 들 수 있다. 보안 기능이 필요할 때마다 그 기능에 맞는 전용장비를 구입한다면 구입비용은 물론 유지보수 비용, 인건비 등 훨씬 더 많은 보안 예산이 필요하다. 따라서 UTM의 도입은 고가의 Point Solution을 구입할 필요가 없기 때문에 구축 및 운용에 있어 상당한 비용절감 효과가 나타난다. 비용절감 효과로서 ROI(Return on Investment)는 비용 절감 효과를 나타낸다. 일례로 단순한 인건비와 업무 시간 절감에 대해서 ROI로 정량적인 효과를 나타내 본다. 예를 들어서 하루 8시간을 근무하는 L 기업에 방화벽, IDS, IPS, VPN 등 여러 보안솔루션을 사용하고 있다고 하자. 네트워크 및 보안을 담당하는 3명의 담당자(인건비와 간접비 포함, 6천만원/ 1년)가 있으며, 이들의 보안 업무와 기술지원을 해주는 1명의 직원(인건비와 간접비 포함, 5천만원/ 1년)이 있다고 할 때, 계산을 하면 다음과 같다.

1년 동안 보안관리 비용 = 보안 담당자(명) X 인건비+지원 담당자 및 부대비용 3명 X 60,000,000원 +50,000,000원 =230,000,000원이다.

L 기업이 1년 동안 보안 관리에 지출하는 인건비는 총 2억 3천 만원 이었다. 이것을 분산된 보안 장비를 효과적으로 관리하기 위해 ESM(Enterprise Security Management)로 나타내면 〔표 1〕과 같다.

표 1. ROI 결과
Table 1. ROI Result

(단위: 천원, 시간)

구분		ESM 도입 전		ESM 도입 후		증감치
		소요 금액 (연)	소요 시간(일)	소요 금액 (연)	소요 시간(일)	증감금액
보안업무	개별보안 시스템모니터링/ 로그분석	74,750	2.6	23,000	0.8	-51,750
	보안시스템 통합모니터링/로 그분석	17,250	0.6	5,750	0.2	-11,500
	개별보안시스템보 고서산출	17,250	0.6	5,750	0.2	-11,500
	보안시스템통합보 고서산출	63,250	2.2	20,125	0.7	-43,125
	신규취약성 분석 및 조치	28,750	1.0	8,625	0.3	-20,125
	보안 기획	11,500	0.4	23,314		
	기타 업무	8,625	0.3	17,486		
	정책 관리 및 수립	8,625	0.3	30,857		
						-138,000

ROI 결과 L 기업은 ESM를 적용하여 계산해 보았을 때 연간 138,000,000원 절감할 수 있고, 일일 업무시간 중 4.8 시간을 절약 할 수 있는 것으로 나타난다.

III. 기존 보안 시스템 분석

본 장에서는 기존 보안 시스템의 보안 장비 강화로서 단일 보안 장비 시스템인 Firewall과 IPS보안 장비 시스템 강화를 중점으로 보안 장비 시스템을 분석하고 이에 대한 보강책을 강구하는 방향을 모색 하고자 한다. 특히 DDOS 등 대량 접속을 통한 공격은 서버 다운을 유발할 수 있는데 그 원인으로 지연(delay)과 효율성(efficiency)의 부재라 볼 수 있다. 따라서 본 장에서는 기존 보안 시스템의 지연과 효율성의 원인 분석을 하고 그 문제점을 해결하고자 한다.

3.1 기존 보안 시스템 분석

기존 보안 시스템은 〔그림 1〕와 같이 L사의 단일 보안 시스템으로 도입 시기는 2003년 3월경으로 보안 업체 J사의

NS-500과 IDP-500를 도입하여 운영하고 있는데 그 시스템의 지연과 효율성을 중점적으로 분석하여 나타내고자 한다.

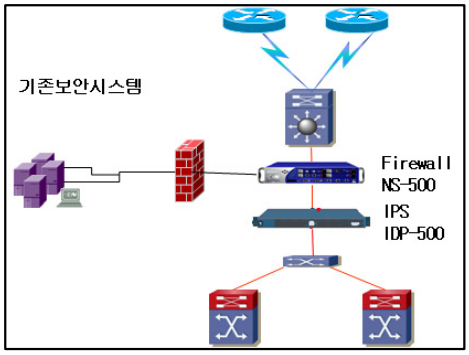

그림 1. L사 NS-500과 IDP-500
Fig. 1. L Company NS-500 and IDP-500

3.2 응답 처리 시간 분석

기존 시스템은 〔그림 1〕에서와 같이 단일 보안 장비로서 도입 시점이 2003년도로 초기 도입 사용 후 7년이 지난 현재의 시점에서 보안 장비 시스템의 성능 평가하기 위해 응답 속도와 초당 처리 세션을 평가해 보기로 한다. 응답 속도 평가 결과 〔그림 2〕와 같이 나타내었다.

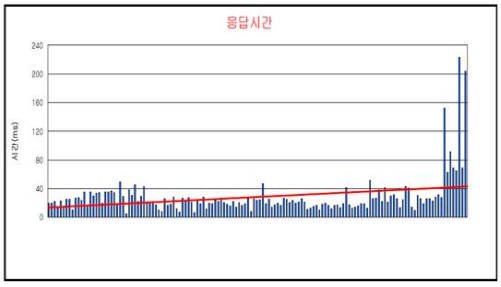

그림 2. 기존 보안시스템의 응답 시간
Fig. 2. Response time of previous Security System

〔그림 2〕에서 보는 것처럼 응답 처리 시간 분석 결과 응답 속도는 평균 54nm이며 최대 220nm까지 나타내고 있는데 이 결과는 보안 장비의 권장 응답 수치 10~20nm에 비해서 상당히 지연 전송 되고 있는 것으로 나타나고 있다. 따라서 이러한 장비의 지연은 DDOS 등 대량 접속 공격에 대응하기에는 취약하다고 사료 된다. 따라서 보안 시스템을 보안 강화가 필요하다고 사료한다.

3.3 초당 세션 처리 분석

두 번째 분석 실험으로 NS-500의 초당 세션 분석 평가 결과 〔그림 3〕과 같다.

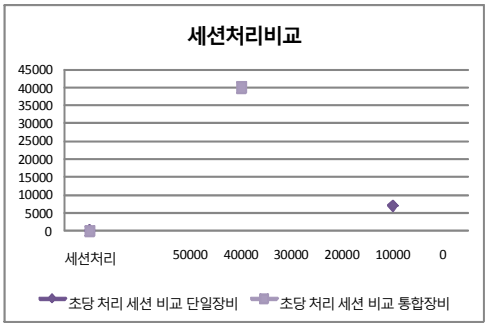

그림 3. 기존 NS-500 응답 시간
Fig. 3. Previous NS-500 Response Time

〔그림 3〕의 NS-500 실험 결과에서 보는 것과 같이 단일 장비의 초당 처리 세션은 7,000세션으로 이는 한 사람이 4개의 세션을 발생시킬 경우 이를 환산하여 보면 7,000 세션(초당) / 4 세션 = 동시 1,750명의 수치가 나온다. 이것은 초당 7,000 세션을 초과 할 경우 응답 속도에 상당한 지연이 발생할 수 있음을 알게 된다.

3.4 기존 시스템의 성능 분석

다음은 기존 보안 시스템의 성능을 나타낸 것으로 〔표 2〕과 같다. 〔그림 3〕에서 보는 것 같이 기존 NS-500의 응답 시간이 초당 세션 처리에서 우수하지 못함을 나타내고 있는데 〔표 2〕에서 보는 것처럼 초당 세션, 방화벽, 인터페이스, 트랙픽 처리, DDOS 등 여러 기능에서 성능이 우수하지 못함을 알 수 있다.

표 2. 기존 보안 시스템 성능
Table 2. Previous Security System Capacity

기존보안시스템 시스템			
NS500		IDP-500	
동시세션	250,000	동시세션	220,000
초당세션	7,000	초당세션	5,000
방화벽 성능	700M	IPS성능	500M
인터 페이스	8x10/100 4xGBIC	인터 페이스	2x10/100/1000 2xGBIC
트랙픽 처리	CPU	트래픽 처리	CPU
NAT	지원	AV 기능	미지원
DDOS 차단	미지원		

3.5 CPU 사용량 분석

기존 보안 시스템의 CPU의 사용량 분석 결과 CPU의 부하가 60~70% 발생하고 있음을 나타낸다. 이는 CPU 권장 30% 이내의 성능에 반해서 60~70%의 CPU 부하는 2배 이상 성능이 낮은 것으로 분석 된다. 따라서 이러한 문제들을 해결하기 위해 여러 해결책들을 강구해 보지만 현재 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 어려움이 나타난다. 따라서 이 문제 요소들을 해결하기 위해서는 새로운 시스템을 도입하는 것인데 단일 품목의 보안 기능보다는 가격 대비 성능으로 보았을 때 통합 기능이 있는 통합 보안 시스템을 강화하는 것이 적합하다고 판단하고 제안한다.

IV. 효율적인 통합 보안 정책 관리 모델 제안

본 장에서는 UPT(IPS)기능과 방화벽 기능을 [그림 4]와 같이 효율적인 통합 보안 시스템으로 나타내었다.

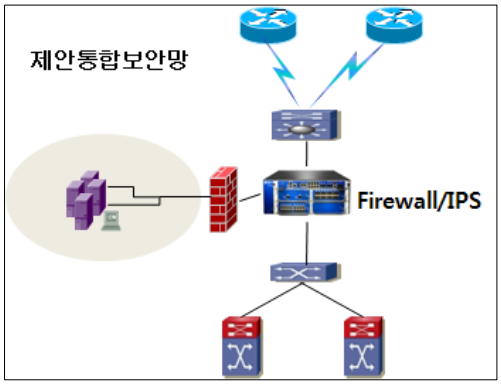

그림 4. 통합 보안 시스템 구성도
Fig. 4. Propose System Architecture

방화벽과 IPS 시스템을 통합 보안 모델을 구성함으로써 단일 보안 시스템에 비해서 여러 측면에서 효율성이 있음을 나타낸다. 첫 번째로 IPS에 대한 정책으로 [그림 5]와 같이 IPS 내의 CPU 3개를 각각 기능 수행에 따라 분류함으로써 지연(Delay)의 문제를 해결 한다.

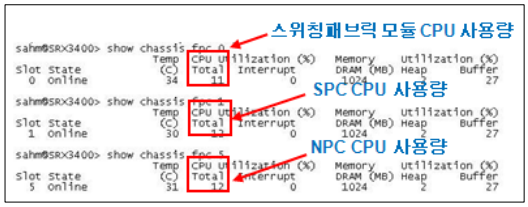

그림 5. 각각 특성에 따른 CPU 정책
Fig. 5. CPU policy depending on individually characteristics

기존 시스템에서는 1개의 CPU를 수행하여 처리함으로 인해 CPU의 작업량이 높아 시스템의 안정화를 주지 못했다. 그런데 제안한 시스템에서는 CPU의 정책을 3개로 적용함으로써 통합 보안의 성능을 향상시키고, 안정적으로 운영한다. 따라서 [그림 2]에서는 1개의 CPU로 처리함으로 상당한 지연(Delay)이 발생하였던 것을 [그림 5]에서 보는 것처럼 방화벽과 IPS을 통합하고 CPU를 각 특성에 맞게 정책으로 적용함으로써 지연(Delay) 문제를 해결 하였다. 제안한 방법은 기존 방식에서는 IPS - 방화벽 - IPS 인 경우 3 hop을 경유한다. 이에 비해서 제안한 방안은 1홉으로 네트워크를 구성함으로써 구간의 delay 감소하는 것이다. 또한 이때 통합 보안의 경우 [그림 4]와 같이 한 단말에서 각 인터페이스 별로 방화벽 혹은 IPS 단일 정책을 적용하거나 각 인터페이스 별로 적절한 정책을 적용하므로 장비의 효율을 높일 수 있다. 특히 CPU 사용이 장비 성능에 대부분을 차지하는 IPS의 경우 내부 보안 상태가 높을 경우 내부 인터페이스에 IPS등 보안장비의 정책을 단순 하게 하고 타 인터페이스의 정책으로 높임으로 성능을 향상시켜 준다. 또 다른 효율성으로 단일 보안시스템을 설치 시 내부 시스템의 CPU 자원이 남아도 외부 보안 시스템에 사용할 수 없고 반대로 내부 보안 시스템이 자원이 부족해도 타 장비의 자원을 사용 할 수가 없었다. 그러나 통합으로 CPU를 적용할 경우에는 최대한의 효율성을 기대할 수 있다. 단 이 경우 통합 보안 시스템이 단일 시스템보다 성능이 월등하게 좋아야 한다. 또 다른 방안으로 최신의 경우 보안 주체에서 예전에는 인터넷 부분 즉 라우터 외부 사용자가 보안의 주체였지만 1.25대란, 7.7 사태 등을 거치면서 웜 바이러스와 DDoS 공격으로 망 외부 단말뿐만 아니라 내부 단말 사용자에 보안이 취약하게 됐고 그로 인해 운영 중인 서버를 위해 DMZ 구간을 만들어 내부 사용자도 보안의 주체가 되었다. [그림 1]에서는 단일 보안시스템이 도입했을 경우 L사의 경우처럼 방화벽의 DMZ 구간을 만들고 2곳의 Interface에 IPS를 설치하여야 함으로 내부사용자와 외부사용자의 공격에서 서버의 운영이나 전산자원을 보호하게 되는 반면 [그림 4]와 같이 통합 보안의 경우 한 단말에서 각 인터

페이스 별로 방화벽 혹은 IPS 단일 정책을 적용하거나 각 인터페이스 별로 적절한 정책을 적용하므로 장비의 효율을 높일 수 있다. 또 다른 방안으로 웜 바이러스나 DDoS 공격 중 단순한 Flooding 공격 같은 경우 CPU자원을 사용하는 것 보다는 ASIC 기반의 단순처리로 해당 세션만 종료하므로 네트워크 전체가 사용하지 못하는 것을 미연에 방지하도록 제안한다. 그리고 효율성의 또 다른 측면으로 단일 제품을 운영함으로써 제품 기술에 따른 습득 시간, 관리 시간, 장애 점검 시간 등 유지 보수 및 운영 관리에 대한 비효율성이 나타난다. 따라서 그림[4]와 같이 시스템을 구성함으로써 [표 1]의 ROI에서 보여는 것처럼 시간적, 공간적, 물리적, 관리나 정책 적용에서 상당한 효율성을 나타난다. 본 장에서는 단일 장비 Firewall(NS-500)과 IPS(IDP)에 대해 통합 장비 SRX3400의 실험 결과를 분석하여 나타낸다.

4.1 제안 적용 및 분석 결과

3장에서 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 성능을 [표 3]와 같이 나타내었다.

표 3. 제안 시스템의 성능 비교
Table 3. Propose System Capacity Comparison

시스템 / SPC.	기존	제안	기존	제안
	NS-500	SRX3400	IDP-500	SRX3400
동시 세션	250,000	500,000	220,000	500,000
초당 세션	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
DDOS 차단	미지원	지원		

4.2 응답 처리 시간 평가 결과

[그림 2]에서의 기존 보안 스템의 응답 속도와 제안한 시스템에서의 응답속도는 [표 4]와 같이 기존 시스템의 응답처리 속도는 평균 54인테 비해 제안 통합 시스템은 평균 10ms 내외로 [그림 6]과 같다. 따라서 제안 시스템에서는 처리 속도에 대한 평균 5배 이상의 처리 속도를 나타내어 지연 문제가 해결됨을 나타내었다.

표 4. 제안 통합보안 시스템 응답 처리속도 비교
Table 4. Propose UTM Security System Response Time

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

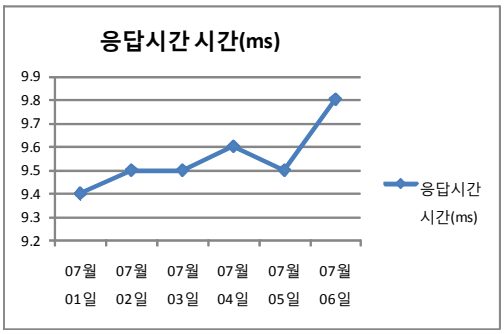

그림 6. 제안 시스템 응답 처리속도 비교
Fig. 6. Propose System Response Time

4.3 초당 세션 처리 평가 결과

앞에서 초 당 동시 세션 7,000를 초과할 경우 응답 속도 지연이 발생 하였으나 [그림 3]의 초당 세션 비교 통합 장비 참조와 [표 3]의 제안 시스템에서 40,000 정도의 세션 성능으로 초과 시에 지연이 발생한다 하더라도 성능이 5.7배 이상을 나타낸다. 따라서 향후 트래픽을 고려한다 하더라도 향후 7~8년은 문제가 발생하지 않을 것으로 사료한다.

4.4 CPU 사용 평가 결과

기존 시스템에서의 응답 처리 속도 문제로서 초당 세션 초과에 따른 CPU의 처리속도로 기존 시스템에서는 [표 5]와 CPU 1개로 처리하였는데 제안 시스템에서는 CPU 3개로 처리함으로써 기존 시스템의 평균 60~70%에 비해서 제안 시스템은 평균 10% 사용을 나타냄으로서 6배의 CPU 처리 성능을 나타내며 [표 5]와 같이 CPU에 따른 사용량 비교를 나타내었다.

표 5. 제안 시스템 CPU 및 응답 처리 속도
Table 5. Propose System CPU and Response Time

CPU 사용량	기존보안시스템	제안통합 보안시스템
CPU 개수비교	1개	3개 모듈별 CPU/ Memory 사용
CPU사용량 비교	평균 60~70% 사용	평균 10% 사용

4.5 정책기능 적용 평가 결과

또 다른 평가 결과로서 정책 기능 적용을 [표 6]와 같이 기존 보안 시스템 시스템과 제안 통합 보안 시스템에 대해 방벽 보안정책, DDos공격 차단정책, IPS 보안정책 기능 적용을 내부와 외부, DMZ에 정책적으로 적용한 것을 나타내었다. 결과에서 보는 것과 같이 기존 시스템에서는 미적용 되었던 DDos 공격 차단으로 외부에서 내부도 차단되었고, DMZ로 외부에서 내부로 적용 되었다. IPS 보안 정책에서도 기존 보안시스템에서는 외부에서 내부로 미적용 되었던 것을 제안한 시스템에서는 외부에서 내부로 정책이 적용 되었다. 따라서 정책 기능에서 보다 강화된 시스템을 보장한다.

표 6. 제안 시스템 정책 비교
Table 6. Policy Comparison of Propose System

정책 기능 \ 시스템 비교		기존 보안 시스템	제안통합 보안 시스템
방화벽 보안 정책	내부⇨외부	적용	적용
	외부⇨내부	적용	적용
Dos 공격 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

4.6. 유해 트랙픽 차단 정보 평가 결과

외부에서 대량의 TCP/UDP 트래픽으로 내부 진입을 시도하여 DDos 공격과 같은 해킹 공격을 유발하다. 기존 시스템에서는 정책적으로 적용되지 않았던 유해 대량 트래픽을 제안한 시스템에서는 정책적으로 적용하여 분류함으로써 DDos 공격 같은 대량 트래픽을 차단 한다. [그림 7]에서 보는 것과 같이 갑자기 숫자가 높아지는 것은 유해 트래픽으로 의심하여 집중 적으로 분류하고 트래픽을 차단하여 이러한 공격으로부터 데이터와 시스템을 보호하여 안정된 통합 보안 시스템을 유지한다.

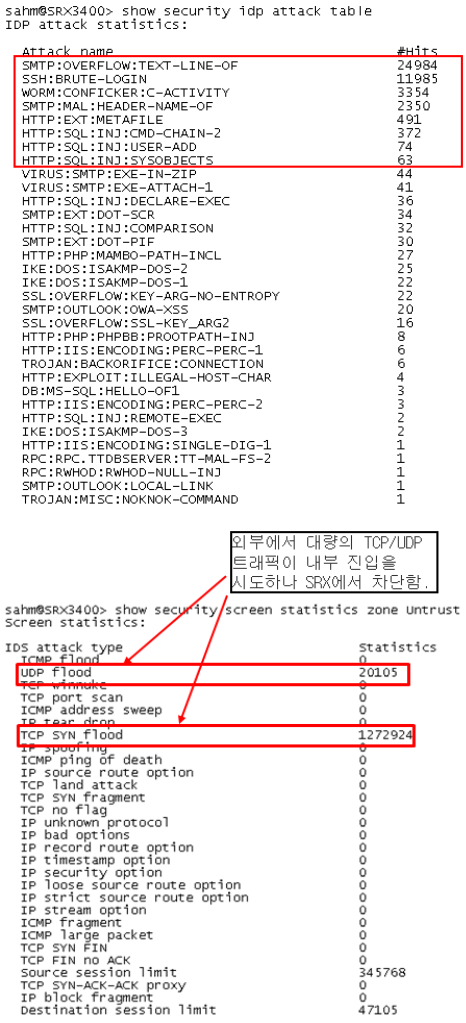

그림 7. 유해 트랙픽 차단
Fig. 7. Injuriousness Traffic Intercept

V. 결론

본 논문에서는 통합 보안 시스템의 효율적인 보안 정책 관리 모델을 적용하여 비용 절감 및 효율성 측면을 나타내었다. 또한 시스템이 통합 관리가 되면 기능적인 측면에서도 상호 보완이 이루어져 보다 강화된 보안을 유지 할 수 있고, 유지 보수면에서도 상당히 효율적임을 나타내었다. 물리적 측면에서 볼 때도 시설 설비 비용 및 공간 확보 등 여러 면에서 경제

적인 효율성을 나타내었다. 또한 시간적 측면에서도 각 시스템 유지 관리에 대한 학습과 제어에 따른 시간적 측면 등 많은 경제적 효율성을 나타내었다. 따라서 통합보안 시스템으로 운영할 경우 여러 측면에서 효율성을 나타내었다. 또한 통합보안 시스템이 네트워크에서 발생하는 delaly 문제가 해결됨을 볼 수 있었다. 4장의 실험 결과에서 나타낸 것 같이 제안한 시스템으로 평가한 결과 기존 시스템에 비해서 응답 처리 속도에서 평균 5배 이상 성능 향상을 나타내었고, CPU 사용량도 평균 10%로 6배 이상 효율성을 나타내었다. 또한 초당 처리 세션에서도 5. 7배의 성능을 나타내었다. 뿐만 아니라 보안 정책에서도 기존 방화벽의 보안 정책들을 적용하였고 추가적으로 DDos 공격을 차단 기능도 강화하여 보다 안정적인 보안 시스템으로 비용 대비 효율성의 우수함을 나타내었다.

참고문헌

〔1〕 최희식, 전문석, " DDos TCP Syn Flooding Backscatter 분석 알고리즘", 한국컴퓨터정보학회 논문지 제 14권, 제 9호, 55-66쪽, 2009년 9월.

〔2〕 구민정, 오창석, "IPv6환경에서 DDoS 침입탐지", 한국컴퓨터정보학회, 제 11권, 제 6호, 186쪽, 2006년 12월.

〔3〕 Christos Siaterlis, Vasilis Maglaris, "One step ahead to multisensor data fusion for DDos detection," journal of Computer Security, v.13 n.5, pp.779-806, Oct. 2005.

〔4〕 윤재영, "네트워크 통합 보안 기술 및 시장 동향 : UTM 급속 확산, 경영과컴퓨터, 통권 364호, 120-123쪽, 2007년 2월.

〔5〕 임채호, "보안 위협에 따른 UTM 필요성 : 다양해진 보안 위협 대비 위한 UTM 장비 점차 각광", 경영과컴퓨터, 통권 365호, 140-143쪽, 2007년 3월.

〔6〕 서현석, "네트워크 보안 통합의 필요성 보안성 향상 비용 절감; 공격 고도화 UTM이 해답" ,Network times, 통권 제 179호, 224-226쪽, 2008년 7월.

〔7〕 정국용, " 네트워크 시스템의 통합보안 방안에 대한 연구", 서울산업대석사학위논문, 1-56쪽, 1996년.

〔8〕 Deawoo Park."A study about dynmic intelligent network security system to decrease by malicious traffic," International Journal of Computer Science and Network Security, V.6, N.9B, pp. 193-199, Sep. 2006.

〔9〕 Alan Murphy and Ken Salchow, "Applied Application Security -Positive and Negative Efficiency," F5 Networks, Oct. 2007.

〔10〕 천우성, 박대우, "DoS공격에 대한 N-IDS 탐지 및패킷 분석 연구", 한국컴퓨터정보학회 논문지,제 13권, 제 6호, 217-224쪽, 2008년 11월.

〔11〕 Karen Scarfone, Peter Mell, "Guide to Intrusion Detection and Prevention System," Recommendations of the National Institute of Standards and Technology, Feb.2007.

〔12〕 이창우, 김석훈, 송정길, "분산 환경에서의 침입방지를 위한 통합보안 관리 시스템 설계", 한국컴퓨터정보학회 논문지, 제 11권, 제 2호, 통권 제 40호, 75-82쪽, 2006년 5월.

〔13〕 유응구, "통합 보안 관리자를 이용한 이동 에이전트 이주 성능 향상 연구", 한국컴퓨터정보학회논문지, 제2권, 제 5호, 통권 제 49호, 57-64쪽, 2007년 11월.

〔14〕 강민균, 김석수 "통합보안관리 시스템에서 내부 보안을 향상시킨 보안 솔루션 구조의 설계 및 구현", 한국콘텐츠학회논문지, 제 5권, 제 6호, 360-367쪽, 2005년 12월.

〔15〕 박대우, 서정만, "TCP/IP 공격에 대한 보안 방법연구", 한국컴퓨터정보학회, 제 10권, 제 5호, 219쪽, 2005년 11월.

〔16〕 박대우, "외부 이동단말의 접근제어를 위한 IP 프로토콜 설계 및 성능 개선에 관한 연구", 한국컴퓨터정보학회 논문지 제 9권, 제 2호, 41-48쪽, 2004년 6월.

〔17〕 김성락, "통합보안관리 에이전트를 확장한 웹 어플리케이션 공격 탐지 연구", 한국컴퓨터정보학회 논문지, 제 12권, 제 1호, 통권 제 45호, 161-168쪽, 2007년 3월.

〔18〕 김용탁, 권오준, 이종민, 김태석, "통합 관리를 위한 정책 기반의 보안시스템 설계 및 구현", 멀티미디어 학회 논문지, 제 10권 제 8호, 1052-1059쪽, 2007년 8월.

〔19〕 손우용, 송정길, "통합보안 관리시스템의 침입탐지 및 대응을 위한 보안 정책 모델 대응을 위한 보안 정책 모델", 한국 컴퓨터정보학회 논문지, 제 9권, 제 2호, 81-87쪽, 2004년 6월.

〔20〕 김석훈, 김은수, 송정길 "통합보안관리 시스템에서의 침입탐지 및 대응을 위한 보안 정책 모델에 관한 연구". 정보보증논문지. 제 5권 제 2호, 9-17쪽, 2005년 6월.

〔21〕 이호, "통합 접근 제어를 위한 시뮬레이션 모델 설계", 한국 컴퓨터정보학회 논문지, 제 9권, 제 4호, 49-54쪽, 2004년 12월.

〔22〕 장성민, 원유헌, "다중 계층 웹 필터를 사용하는 웹 애플리케이션 방화벽의 설계 및 구현" 한국 컴퓨터정보학회 논문지, 제 14권, 제 12호, 157-167쪽, 2009년 12월.

저 자 소 개

주 헌 식

2005년 : 아주대학교 컴퓨터공학과 (공학박사)

1997 ~ 현재 : 삼육대학교 컴퓨터학부 부교수

관심분야 : 모바일컴퓨팅, 네트워크 보안, 센서네트워크

김 종 완

2007 : 고려대학교 컴퓨터학과 (이학박사)

2009 : 건국대학교 정보통신대학 연구교수

2010 : 삼육대학교 경영정보학과 연구 교수

관심분야 : 분산 모바일 시스템, 센서네트워크, 차량간통신 (V2V)