인바운드 네트워크의 성능 및 보안성 향상에 관한 연구

정회원 전 정 훈*

Study of the Enhancement Performance and Security of Inbound Network

Jeong-hoon Jeon* ***Regular Member***

요 약

오늘날 네트워크 규모가 확대되고, 다양한 서비스가 개발됨과 동시에 공격기법들 또한 함께 진화하고 있다. 이러한 공격기술들에 대해 다양한 보안시스템들을 적용하고 있으며, 이들 보안시스템 중, 아웃바운드(Outbound) 네트워크 공격에 효과적으로 대응하기 위한 방화벽의 사용은 네트워크 보호에 필수적이다. 하지만 이러한 전형적인 방화벽(Conventional Firewall)은 오히려 인바운드(Inbound) 네트워크의 성능 및 보안성 저하에 직접적인 영향을 미치고 있으며, 내부 공격에 효과적이지 못하다. 따라서 본 논문에서는 인바운드 네트워크의 성능 및 보안성을 향상시키기 위해 보안대상에 따른 "기능성방화벽(Functional Firewall)"을 제안하고자 한다.

Key Words : Conventional Firewall, Functional Firewall, Inbound Network

ABSTRACT

Recently, Network technology evolve out of expansion a scale of Network and development various Service. also Hacking skill. We have applied to various Security Systems to make a counterattack on this hacking skill. and A Firewall among these security systems is very effective a defense against in the Outbound Network attack. so we need certainly a Firewall to protect a network. But this Conventional Firewall has an directly effect on reduction to the Performance and Security of Inbound Network. and have no effect on a Inner Network Attacking. In this paper, I propose to a "Functional Firewall" as a Secure Objects for the enhancement Performance and Security of Inbound Network

Ⅰ. 서 론

최근 네트워크는 고속화와 다양화로 규모는 점차 확대되고, 네트워크의 보호와 통합관리의 체계로 급변하고 있으며, 새로운 변화와 함께 다양한 공격기법들 또한 진화되고 있다. 따라서 공격가능성을 줄이고, 신속한 대응을 위한 보안시스템의 적용은 네트워크 보호의 필수 요소가 되었다. 그러나 성능과 보안성이 반비례하는 특성을 고려해 볼 때, 네트워크의 보안성만을 강화할 목적이라면, 추가적인 보안시스템 및 기능의 사용이 불가피해지며, 이에 따른 부작용으로 인바운드 네트워크의 성능저하를 가중시키게 된다[13]. 따라서 보안시스템의 선택과 배치는 네트워크의 성능과 보안성을 결정하는 중요한 요인이라 할 수 있다. 보안시스템을 차단, 탐지, 관리(데이터, 시스템)로 분류하고, 시스템 부하 및 활용도, 보안목적 등을 고려해볼 때, 인바운드 네트워크의 성능에 직접적인 영향을 미치는 보안시스템으로 방

※ 본 연구는 2007년도 동덕여자대학교 교내학술연구비 지원에 의해 수행된 것임.
* 동덕여자대학교 정보학부 컴퓨터전공 전임강사(nerdrandy@dongduk.ac.kr)
논문번호 : KICS2008-06-264, 접수일자 : 2008년 6월 9일, 최종 논문접수일자 : 2008년 7월 31일

화벽을 꼽을 수 있다.

이러한 방화벽은 그림1[12]과 같이 정보보호 제품 중 꾸준한 매출전망을 나타내고 있어, 향후에도 높은 수요를 예상케 하고, 정보보호시스템의 매출비중을 살펴볼 때, 그림2[12]와 같이 보안관리 시스템 다음으로 큰 비중을 차지하고 있어, 정보보호에 반드시 필요한 보안시스템으로 자리 잡고 있음을 알 수 있다.

방화벽은 네트워크의 내·외부를 보호하는 중요한 시스템으로 특히 아웃바운드 네트워크로부터의 DoS(Denial of Service), Sniffing 그리고 Flooding과 같이 잘 알려진 공격에 매우 뛰어난 방어능력을 보이기 때문에 네트워크 및 시스템 보호를 위해 가장 보편적으로 사용되는 보안시스템 중에 하나이며, 트래픽 량이 많은 곳에 위치해 출입하는 모든 데이

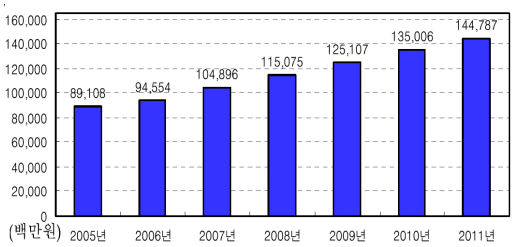


그림 1. 방화벽의 매출전망

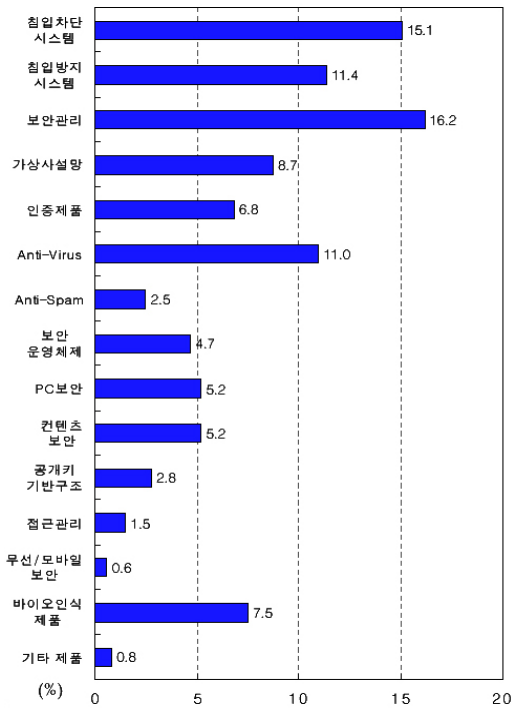


그림 2. 시스템 및 네트워크 정보보호제품 분야의 소분류별 매출액 비중

터를 검증할 수 있는 장점이 있다. 그러나 한정적인 배치영역과 모든 데이터의 검증수행으로 인바운드 네트워크의 성능저하에 많은 영향을 미치며, 한번 허용된 불법적인 접근에 대해서는 차단할 수 없고, 불필요한 정책들이 중복 적용되는 단점이 있다. 또한 방화벽의 사용은 아웃바운드 네트워크에 비해 인바운드 네트워크의 공격에 취약하고, 내부 보안을 보장할 수 없으며, 시스템의 증가는 성능과 반비례하여 여러 관리 및 보안문제들이 복합적으로 발생하게 된다[1][2][6][13].

최근 들어 IDS(Intrusion Detection System)와 바이러스 백신(Virus Vaccine), VPN(Virtual Private Network) 등과 같은 기타 보안시스템들과 통합 및 연동하는 형태로 성능 및 관리 측면에 많은 진화가 진행되고 있지만, 각종 보안기능의 추가가 정책 증가와 네트워크의 성능저하를 가속화하는 요인이 되고 있다. 따라서 본 논문에서는 이러한 인바운드 네트워크의 부하를 경감하여 성능과 보안성을 함께 향상시킬 수 있는 방안으로 보안대상에 따른 기능성방화벽(Functional Firewall)의 사용을 제안하고자 한다. 이러한 제안내용에 대한 논리적 근거를 위해 논문의 Ⅱ장에서는 관련분야에 대한 연구내용으로 네트워크의 방화벽과 전형적인 방화벽(Conventional Firewall)기능의 성능을 분석하고, Ⅲ장에서는 제안하는 기능성 방화벽의 모델링 및 구축방법에 대해서 기술한다. 그리고 Ⅳ장의 성능 및 보안성에 대한 비교분석과 Ⅴ장의 결론부분으로 이글을 마치도록 한다.

Ⅱ. 관련연구

이 장에서 방화벽 사용에 따른 인바운드 네트워크의 성능을 분석하기 위해 방화벽의 기능, 정책 수에 따른 성능실험을 수행한다.

2.1 방화벽 기능에 따른 분석

2.1.1 패킷필터링(Packet Filtering)기능분석

패킷필터링을 분석하기 위해 사용유무와 전송속도, 필터링 인자(IP와 MAC)에 대한 처리효율을 다음과 같이 실험한다. 실험은 리눅스8.0기반에 Iptable을 통해 IP와 MAC에 대해 100개의 규칙들을 각각 적용하고, 전송속도를 달리하여 처리효율을 측정한다. 실험결과 그림3은 패킷필터링을 사용할 경우, 그렇지 않을 경우보다 최대 3.8~4.3배의 처리지연을 나타내고, IP보다 MAC에 의한 처리지연도 약2.5~3배 증가했다. 그리고 전송속도가 증가함

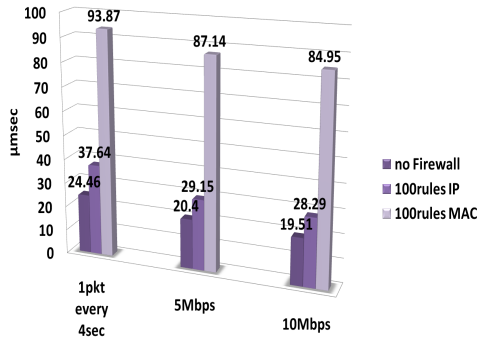


그림 3. 전송률증가에 따른 처리효율

에 따라 패킷필터링의 처리지연은 오히려 1.0~1.2배 감소함으로써, 전송속도에 반비례함을 알 수 있다 [1][2].

2.1.2 주소변환(Network Address Translation)기능분석

주소변환의 분석을 위해 주소변환 사용유무에 따른 단일 및 다중 사용자의 처리지연을 비교하고자 한다[7][8][11]. 실험은 리눅스8.0에 펜티엄3 노트북2대, WLAN이 지원되도록 linux-wlan-ng드라이버와 802.11이 지원되는 100Mbps Ethernet으로 구성하고, NAT의 오버헤드 측정을 위해 단일 또는 다중 사용자가 FTP서버로 동작하는 노트북으로부터 파일(1KB에서 4M까지의 데이터)을 다운로드 받을 경우, 처리효율을 Iperf로 각각 측정한다. 실험결과 그림4의 단일사용자는 주소변환을 사용할 경우(Client2)가, 사용하지 않을 경우(Client1)보다 처리효율이 약1.3~2.7배정도 저하되었고, 그림5에서 다중사용자가 주소변환을 사용할 경우(Client2), 사용하지 않을 경우보다(Client1) 처리효율이 약2~3.5배 정도 저하됨을 알 수 있다[10][11][14].

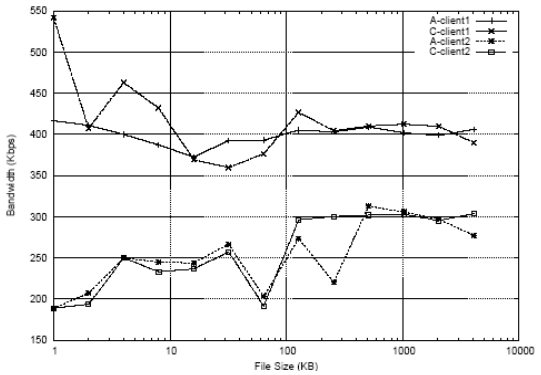


그림 4. NAT 단일 사용자

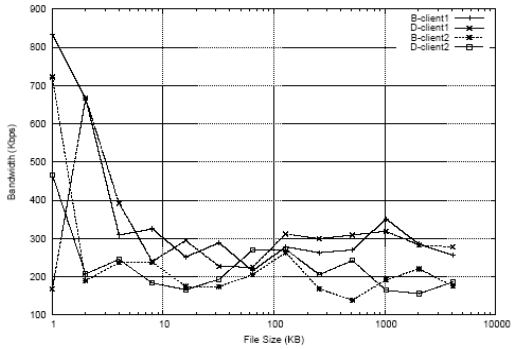


그림 5. NAT 다중 사용자

2.1.3 프락시(Proxy), 게이트웨이, 주소변환 기능분석

프락시[3]를 분석하기 위해 방화벽을 사용하지 않을 경우와 게이트웨이, 주소변환, 프락시를 각각 사용했을 경우의 처리효율을 비교한다. 실험은 2대의 리눅스8.0시스템에 NAT1.0과 프락시(http 설정)를 각각 구축하고, 스마트비트를 통해 가변 데이터를 전송한다. 실험결과 그림6과 같이 프락시만을 사용했을 경우(Proxy), 방화벽을 사용하지 않았을 경우(TCP)에 비해 약3배의 처리효율이 저하되었고, 게이트웨이(Gateway)와 NAT는 거의 동일하였다. 그리고 프락시는 방화벽의 다른 기능에 비해 낮은 대역폭 처리효율을 나타냈다[1][9].

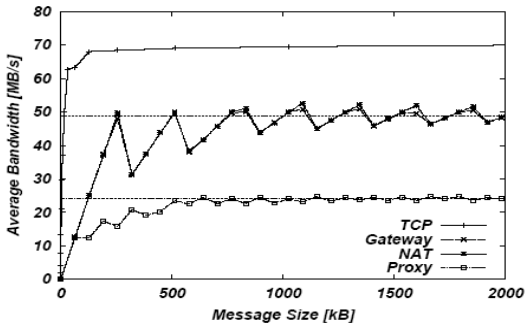


그림 6. 메시지에 따른 테스트결과

2.1.4 정책(Policy)에 따른 성능분석

정책 수[6]가 방화벽과 네트워크의 성능저하에 어떠한 영향을 미치는지를 알아보기 위해 리눅스8.0에 방화벽 프로그램인 Iptable의 정책 수를 증가하여 처리효율의 변화를 비교한다. 그리고 TCP와 UDP, IP, MAC에 대해서도 정책의 증감에 따른 처리효율을 함께 분석한다. 실험결과 그림7, 8과 같이 정책수가 증가함에 따라 처리효율이 함께 감소함을 알

수 있다. 특히 IP의 경우, 비교적 완만한 기울기의 처리효율을 보이지만, MAC과 TCP, UDP는 급격한 증가를 보이며, IP와 최대 5배 이상의 처리효율 차이를 나타냈다[2].

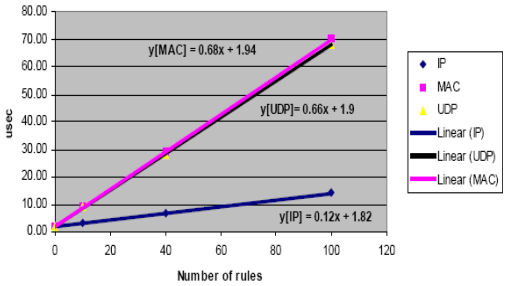


그림 7. UDP연결시 방화벽 규칙수에 따른 처리시간

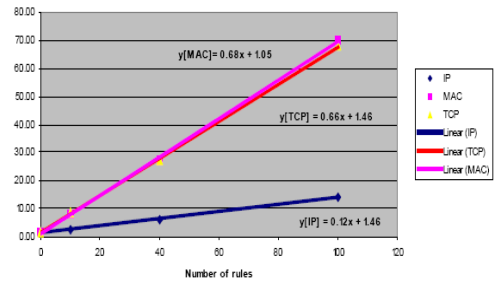


그림 8. TCP연결시 방화벽 규칙수에 따른 처리시간

2.2 인바운드 네트워크의 보안성 분석

인바운드, 아웃바운드 네트워크의 보안성분석을 위해 방화벽으로 보호되고 있는 네트워크에 잘 알려진 공격을 시도한다. 실험은 Iptable이 설치된 리눅스 시스템에 2개의 인터페이스로 인바운드, 아웃바운드 네트워크를 연결하고, 아웃바운드의 공격을 시도하고, 내부 사용자를 대신하는 노트북 2대를 설치하여 인바운드 공격을 시도한다. 실험결과 표1과 같이 인바운드, 아웃바운드 네트워크의 공격허용유무에 대한 결과를 나타낸 것으로, 대부분의 공격을 방어하는 아웃바운드 네트워크에 비해, 인바운드 네트워크에서는 알려진 공격이 모두 가능함을 알 수 있다.

표 1. 공격에 따른 방어유무 비교

공격유형	인바운드 네트워크의 공격허용유무	아웃바운드 네트워크의 공격허용유무
Sniffing Attack	허용	거부
Spoofing Attack	허용	허용
Shared Attack	허용	거부
Flooding Attack	허용	거부
Password Cracking	허용	거부
Worm & Virus	허용	허용
Scanning Attack	허용	거부

Ⅲ. 제안하는 기능성방화벽

3.1 기능성방화벽

일반적으로 인바운드 네트워크는 편의성과 확장성을 고려하여 부서나 배치구조, 사용자, 시스템 등의 주어진 환경에 따라 전형적인 방화벽을 배치한다. 이유로는 방화벽을 보안대상에 따라 구축할 경우, 다수의 방화벽을 사용해야 하며, 이로 인해 성능이 저하될 뿐만 아니라, 관리상의 문제가 발생하기 때문이다. 결과적으로 보안대상에 따른 방화벽의 배치가 아닌, 전체 네트워크 보호를 위한 배치가 불가피하게 된다. 따라서 이글에서 제안하는 '기능성방화벽'은 전형적인 방화벽의 주요 기능을 분리하여 개별 시스템으로 운영할 수 있도록 한 소규모의 기능 전용의 방화벽을 말하며, 전형적인 방화벽과는 달리, 기능성방화벽은 인바운드 네트워크의 보안대상에 따라 독자적으로 운용이 되기 때문에 보안대상을 클러스터링하여 불필요한 정책과 중복을 줄이고, 시스템의 부하를 경감하여 인바운드 네트워크의 성능과 보안성을 함께 향상시키고자한다. 인바운드 네트워크의 보안대상으로는 사용자 또는 시스템 그리고 네트워크, 서비스로 구분할 수 있으며, 보안대상을 클러스터링한 후, 표2와 같이 전형적인 방화벽의 주요 기능인 패킷필터링과 프락시, 주소변환으로 분리하고, 이를 보안대상에 따라 클러스터링 된 소규모의 네트워크 보호를 위해 배치한다. 여기서 기능성방화벽은 전형적인 방화벽의 주요기능인 패킷필터링 기능을 'IO 방화벽'으로, 프락시 기능을 'Gate 방화벽', 주소변환 기능을 'NAT 방화벽'이라 명명하고, 각각의 보안대상, 기능과 적용에 대해서 알아보도록 한다.

표 2. 기능성방화벽의 유형

방화벽 유형	기능	보안성	보안대상
IO 방화벽	패킷필터링	접근통제성	사용자 및 데이터
NAT 방화벽	주소변환	접근통제성	네트워크
Gate 방화벽	프락시	인증성, 접근통제성	서비스

- IO 방화벽(IO/F: Inner & Outer Firewall)의 보안대상은 사용자와 데이터(패킷)이며, 보안기능은 접

근통제이다. 주된 기능은 패킷필터링으로 2.1.1절에서의 성능분석 자료와 같이 네트워크의 최종단에서 약60%의 처리효율 저하문제를 해결하기 위해 단순정책과 전용시스템으로 구성한다. 그리고 특정 Local 부분에 대한 보안대상 기반의 클러스터링으로 독립성을 제공한다.

- NAT 방화벽(N/F: NAT Firewall)의 보안대상은 네트워크 보안기능은 재구성과 분할에 의한 접근통제이다. 주된 기능은 주소변환으로 2.1.2절에서의 성능분석 자료와 같이 사설주소를 이용한 네트워크 분할이다. 특정 Local 부분만 별도로 관리함으로써, 정책중복에 따른 성능저하 및 시스템 부하 문제[7][8][11][14]를 해결하기 위해 보안대상 기반의 클러스터링을 제공한다.
- Gate 방화벽(G/F: Gateway Firewall)의 보안대상은 서비스이며, 보안기능은 인증성과 접근통제이다. 주된 기능은 프락시로, 2.1.3절의 성능분석 자료와 같이 각 서비스에 따른 시스템의 성능향상과 트래픽의 효율적인 관리를 위해 해당 서비스 프로토콜에 따른 별도의 독립 장비로 구성된다. 그리고 특정 Local 부분에 대한 보안대상 기반의 클러스터링으로 독립성을 제공한다.

3.2 기능성방화벽에 따른 네트워크 클러스터링

기능성 방화벽을 배치하기 전에 인바운드 네트워크에 대한 보안영역(Secure Zone)의 구분이 필요하다. 보안영역은 네트워크에 적절한 기능성방화벽을 배치하고 보안등급별 관리를 위해 사용된다. 그리고 표2에서의 보안대상에 따라 네트워크를 3개의 보안영역으로 분할한다.

네트워크는 그림9와 같이 보안영역으로 분할하며, “1st Secure Zone”은 기능성방화벽인 G/F의 배치영역으로서 서비스에 따른 1차 분할영역이다. 그리고 2차 네트워크 방어 영역인 “2nd Secure Zone”은 기능성방화벽인 N/F가 위치하는 영역으로 1차 서비스에 따라 분리된 인바운드 네트워크를 내부의 접근통제를 보장하기 위해 네트워크를 분할하며, 마지막으로 “3rd Secure Zone”은 1차, 2차 방어영역으로도 강한 접근통제를 보장받기 위해 보안성이 높은 영역에 대한 보안영역으로 기능성방화벽 IO/F의 배치영역이다. 이러한 보안영역들은 표3과 같이 보안대상에 따라 재분할 되어야 하며, 재분할된 보안영역들은 해당 보안영역의 기능성방화벽으로 보호받게 된다.

보안영역으로 분할된 네트워크는 또다시 그림10과 같이 동일 보안대상에 따라 클러스터링 되고 클러스터링 된, 소 네트워크(Small Network)는 표4와 같이 보안등급에 따라 필요한 기능성방화벽이 배치된다. 보안등급은 Level1이 가장 상위 등급으로 높은 보안성이 필요할 경우에 적용되며, Level3은 가장 낮은 등급이다. 그림11과 같이 보안등급에 따라 클러스터링 된 소 네트워크에 기능성방화벽을 배치한다.

표 3. 보안영역

보안영역	기능성방화벽
1st Secure Zone	G/F(Proxy)
2nd Secure Zone	N/F(Private Network)
3rd Secure Zone	IO/F(Packet Filter)

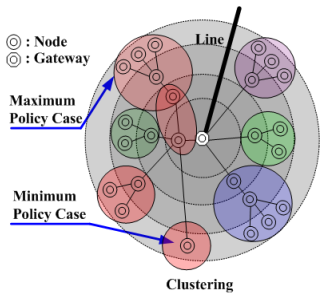


그림 10. 클러스터링

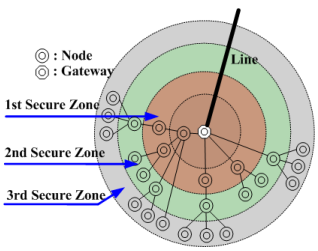


그림 9. 보안영역 구분

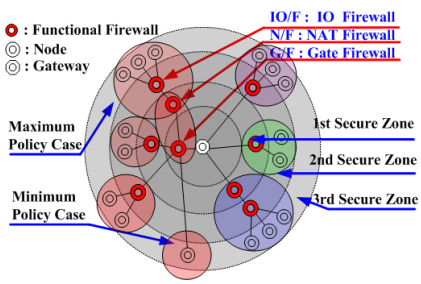


그림 11. 클러스터링 된 소 네트워크에 배치된 기능성방화벽

표 4. 보안등급별 기능성방화벽

보안등급	방화벽 수	기능성방화벽
Level 1	3	(G/F-N/F-IO/F)
Level 2	2	(G/F-N/F), (G/F-IO/F), (N/F-IO/F)
Level 3	1	(G/F), (N/F), (IO/F)

Ⅳ. 성능평가

방화벽의 사용유무에 따른 성능분석과 네트워크의 성능, 정책 수, 보안성에 대해 전형적인 방화벽과 제안하고 있는 기능성방화벽의 성능을 비교해 본다.

4.1 방화벽 사용 유무에 따른 분석

방화벽의 전형적인 배치구조에 대한 성능측정을 위해 리눅스 기반의 방화벽인 Iptable을 두 대의 시스템에 각각 설치하고, 인바운드 네트워크에 내부 사용자로 노트북 1대씩을 연결한다. 성능측정을 위해 1Mbyte크기의 데이터를 노트북 간에 5, 10Mbps로 전송하였을 경우, 방화벽의 사용과 미사용에 따른 처리지연을 리눅스 서버와 노트북 클라이언트 각각에 설치한 Iperf 도구를 통해 측정한다. 실험결과 그림12는 한대의 방화벽으로 모든 네트워크의 트래픽을 담당하는 전형적인 방화벽 배치구조로서 네트워크가 확대됨에 따라 점차 부하를 가중시켜, 인바운드 네트워크의 성능을 저하시킨다. 그림13은 그림12의 배치구조에 따른 처리지연을 측정한 것으로서 방화벽의 사용이 미사용일 경우보다 약4배 이상의 처리지연이 발생하고 있음을 알 수 있다.

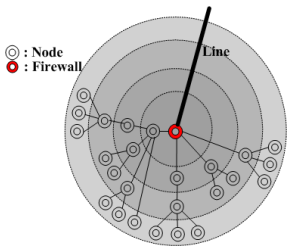


그림 12. 방화벽의 전형적인 배치구조

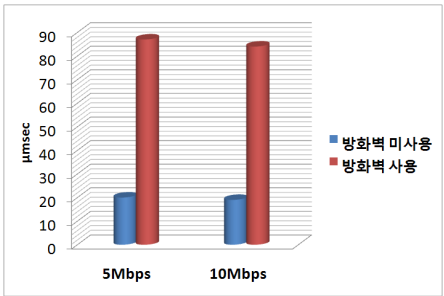
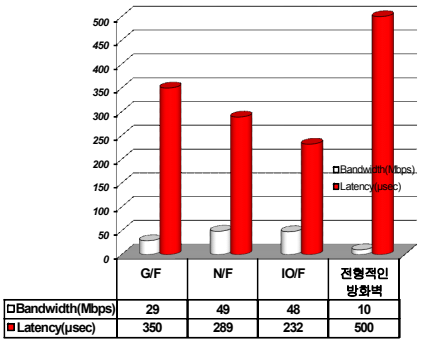


그림 13. 방화벽사용유무에 따른 성능분석

4.2 네트워크 성능 실험

기능성방화벽의 성능분석을 위해 전형적인 방화벽의 주 기능인 패킷필터링과 NAT, 프락시, 게이트웨이를 운영하였을 경우와 기능성방화벽을 각각 운영했을 경우의 동일 정책 조건하에 성능을 측정한다. 리눅스9.0환경에서 CPU433Mhz, 메모리256M과 하부 네트워크의 사용자를 가정하기 위해 노트북을 5대 연결한다. 그리고 기존 방화벽 기능을 대신할 Iptable과 NAT1.0, Proxy(Squid)를 설치하고, FTP를 통해 파일을 다운로드 한다. 측정을 위해 4.1의 실험과 동일하게 Iperf를 통해 대역폭과 처리효율을 각각 측정한다.

실험결과 그림14와 같이 기존 방화벽과 기능성방화벽의 대역폭 처리효율과 처리지연을 비교한 것으로 성능에 큰 차이를 보였다. 기존 방화벽 보다 게이트 방화벽은 대역폭 처리효율이 약3배 이상 향상되었으며, 처리지연은 30%절감되었다. 그리고 NAT 방화벽은 대역폭 처리효율이 약5배 이상 향상되었으며, 처리지연은 43%절감되었다. 마지막으로 IO방화벽은 대역폭 처리효율이 약5배 이상 향상되었으며 54%의 처리지연의 절감효과를 나타냈다.



	G/F	N/F	IO/F	전형적인 방화벽
Bandwidth(Mbps)	29	49	48	10
Latency(μsec)	350	289	232	500

그림 14. 기능성방화벽 성능비교

4.3 정책 수 비교

기능성방화벽의 사용에 따른 방화벽의 정책 수의 변화를 알아보기 위해 리눅스9.0환경에서 CPU433Mhz, 메모리256M과 하부 네트워크의 사용자를 가정하기 위해 노트북 4대를 연결하였다. 기존

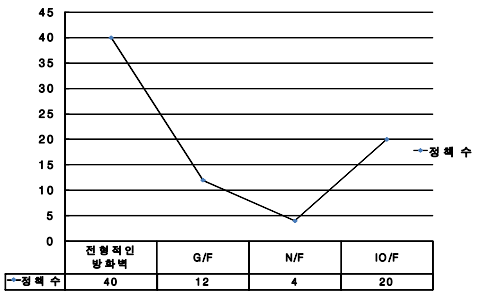


그림 15. 정책 수 비교

방화벽 기능을 대신할 Iptable과 NAT, Proxy (Squid)를 설치하고, 사설 네트워크의 클라이언트에서 FTP서비스를 통한 파일 1M의 파일을 다운로드 할 경우의 기존 방화벽의 정책 수와 기능성방화벽의 정책 수를 비교한다. 그러나 기존 방화벽은 배치 위치로 인해 내·외부 네트워크 모두 방어하기 위한 최소한의 정책이어야 하며, 기능성방화벽의 경우 정책의 수를 최소화할 수 있는 경우로 비교한다. 실험측정을 위한 도구로 Iperf를 사용해 처리지연을 측정한다. 실험결과 그림15와 같이 정책 수는 방화벽 시스템의 성능과 반비례하는 것을 알 수 있으며, 전형적인 방화벽과 기능성방화벽의 정책 수를 비교하였을 경우, 정책 수를 최소화함으로써 시스템의 성능을 향상시킬 수 있음을 알 수 있다.

4.4 인바운드 네트워크의 보안성 비교

전형적인 방화벽과 기능성방화벽을 사용하였을 경우, 인바운드 네트워크에 대한 공격을 시도함으로서 이에 대한 대응능력을 알아본다. 공격은 잘 알려진 공격유형들로 2.1절과 동일하게 실험한다. 표5의 실험결과와 같이 전형적인 방화벽은 인바운드 네트워크에 대한 보안성을 보장할 수 없음을 알 수 있다. 반면 기능성 방화벽의 경우에는 내부 공격자에 의한 방어가 이뤄짐을 알 수 있다.

표 5. 인바운드 네트워크의 보안성 비교

공격유형	전형적인 방화벽 사용	기능성방화벽 사용
Sniffing Attack	허용	거부
Spoofing Attack	허용	허용
Shared Attack	허용	거부
Flooding Attack	허용	거부
Password Crack	허용	거부
Worm & Virus	허용	허용
Scanning Attack	허용	거부

V. 결 론

본 논문에서는 전형적인 방화벽을 기능별로 분리하고 이를 기능성방화벽으로 구성하여 인바운드 네트워크의 성능과 보안성을 향상시키고자 제안하였다. 그리고 효율적인 관리와 배치를 위해 보안영역과 보안등급을 네트워크에 부여하여 소 네트워크로 재구성하였으며, 실험을 통해 인바운드 네트워크의 보안성을 유지하면서 전형적인 방화벽의 성능보다도 향상됨을 알 수 있었다.

따라서 이러한 특징들로부터 제안한 기능성방화벽은 전형적인 방화벽의 시스템 부하와 정책의 중복 및 수를 줄임으로써 인바운드 네트워크의 성능을 향상시키며, 네트워크의 독립성과 보안성을 보장하고, 보안대상별 구분으로 효율적인 관리를 수행하는데 적합하다. 그리고 점차 규모가 커지고 서비스가 다양해지며, 지능화되어 가는 공격기법들에 대해, 아웃바운드 네트워크로부터의 공격 대응에 치중하던 현 시점에서 인바운드 네트워크의 보안은 실질적인 보안사고의 예방과 대응 방법이 될 것이며, 인가자에 의한 내부 공격으로부터도 뛰어난 보안성을 제공할 것이다. 하지만 향후 체계적인 보안대상의 정의와 기준 모델이 필요하며, 기능 보완과 통합관리와의 연동 및 보안 네트워크의 설계에 대한 추가적인 연구가 필요하다.

참 고 문 헌

〔1〕 Chris Kostick, Matt Mancuso “Firewall Performance Analysis Report” 10 August 1995.

〔2〕 James Harris and Americo J. Melara, Hugh Smith and Phillip Nico, California Polytechnic State University “Performance analysis of the Linux firewall in a host” June 12, 2002.

〔3〕 Evaluating Application-aware Firewall Performance “Evaluating Application-aware Firewall Performance” 2004 www.agilent.com/comms.

〔4〕 Yuan-ni Guo 1, Ren-fa Li Computer and Communication Department Hunan University, Changsha, China,410082 “Design and Performance of firewall system Based on Embedded Computing”.

〔5〕 Seung-Hwa Chung Pohang, Korea Division of Electrical and Computer Engineering “Analysis of Bursty Packet Loss Characteristics on Underutilized Links” December 21, 2005.

〔6〕 Michael R. Lyu and Lorrien K. Y. Lau Department of Computer Science and Engineering The Chinese University of Hong Kong, Shatin, HK "Firewall Security: Policies, Testing and Performance Evaluation".

〔7〕 Kumrye Park, Sungyong Park, Ohyoung Kwon, and Hyoungwoo Park Dept. of Computer Science, Sogang University, Seoul, Korea "Private-IP-enabled MPI over Grid Environments".

〔8〕 HAYASHI yu-ichi University of Aizu, Graduation Thesis. "NAT Router Performance Evaluation" Mar, 2002.

〔9〕 Matthias M¨uller, Matthias Hess, Edgar Gabriel High Performance Computing Center Stuttgart (HLRS), Stuttgart, Germany, Innovative Computing Laboratory, Computer Science Department, University of Tennessee, Knoxville, TN, USA "Grid enabled MPI solutions for Clusters"

〔10〕 Jiejun Kong, Shirshanka Das, Edward Tsai, Mario Gerla Computer Science Department University of California, Los Angeles, CA 90095 "A Decentralized and Localized Access Control System for Mobile Wireless Access to Secured Domains"

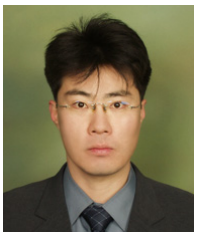
〔11〕 Siyoul Choi1, Kumrye Park, Saeyoung Han, Sungyong Park, Ohyoung Kwon, Yoonhee Kim, and Hyoungwoo Park Dept. of Computer Science, Sogang University, Seoul, Korea "An NAT-Based Communication Relay Scheme for Private-IP-Enabled MPI over Grid Environments"

〔12〕 한국정보보호 진흥원 "2006년 국내 정보보호산업 통계조사" p.25, 32.

〔13〕 이영석 "방화벽이 존재하는 캠퍼스 망에서의 P2P 트래픽 측정 및 분석", *한국통신학회논문지*, Vol.30 pp.750-757, 2005.

〔14〕 이현창, 이종언 "백도어형 사설망의 작업효율 개선에 관한 연구", *한국통신학회논문지*, Vol.31 pp.199-206 2005

전 정 훈 (Jeong-hoon Jeon) 정회원



1999년 2월 숭실대학교 컴퓨터공학과 졸업

2001년 2월 숭실대학교 컴퓨터공학과석사 졸업

2004년 3월 숭실대학교 컴퓨터공학박사 수료

2005년 3~현재 동덕여자대학교 전임강사

<관심분야> 네트워크보안, 시스템보안, 무선보안, 암호, 컴퓨터 포렌식