韓國 컴퓨터情報學會 論文誌
第12卷 第2號, 2007. 5.

2007-12-2-1-12

효율적인 네트워크 보안운영을 위한 Exclusive Firewall 관한 연구

전 정 훈*, 전 상 훈**

A study on about a Exclusive Firewall for operation the efficient network security

Jeon Jeong Hoon*, Jeon Sang Hoon**

요 약

방화벽은 네트워크를 보호하기 위한 보안시스템으로 Trusted 네트워크 구축에 있어 필수적인 시스템이라 할 수 있다. 그러나 이러한 방화벽은 비효율적인 정책과 불필요한 트래픽으로 전체 네트워크의 성능을 약 60%이상까지 저하시킨다. 따라서 방화벽의 효율적인 운영과 재배치, 네트워크 성능 개선이 절실히 필요하다. 본 논문에서는 방화벽의 기능에 따른 시뮬레이션 결과를 통해 방화벽의 각 기능이 네트워크 성능에 미치는 영향을 분석하고, 효과적인 네트워크 운용을 위한 Exclusive 방화벽 구축을 제안한다.

Abstract

Firewall system is a security system for protect the network and is needed for constructing the trusted network. However, these firewall systems deteriorate the performance of whole network in about 60% because of Inefficiency policy establishment and unnecessary traffic occurrence. Therefore, there is a strong needs to establish the network performance elevation, efficient operation and reassignment of the firewall system. In this dissertation, we will analyze how each functionalities of the firewall system affect to the network performance via using a simulation result according to functionality of the firewall system and propose a exclusive firewall system for the efficient network operation.

▸ Keyword : 전용방화벽(Exclusive Firewall), 프락시(Proxy), 패킷필터링(Packet Filtering), NAT(Network Address Translation), 정책(Policy), 규칙(Rule)

• 제1저자 : 전정훈
• 접수일 : 2007.4.16, 심사일 : 2007.4.18, 심사완료일 : 2007. 5.20.
* 동덕여자대학교 정보학부 컴퓨터전공 교수, ** 숭실대학교 일반대학원 컴퓨터학과 박사과정

Ⅰ. 서 론

네트워크 관리자들은 각종 서비스의 다양화와 사용자 급증에 따른 보안의 필요성이 점차 증가하고, 침입자로부터 자산을 보호하기 위해 각종 보안시스템들을 이용한 Trusted 네트워크의 구축을 목표로 하고 있다.

네트워크 보호를 위한 대표적인 방안으로 방화벽시스템(Firewall System)의 적용을 들 수 있다. 방화벽시스템은 네트워크 내·외부로의 수많은 데이터의 허용과 차단 여부를 확인하고, 여러 보안기능들을 함께 수행해야 하기 때문에 약 60% 이상의 네트워크 속도저하를 감안해야만 한다. 따라서 전체 네트워크 성능저하와 중복정책에 따른 비효율적 운용 및 관리는 해결되어야할 큰 과제라 하겠다. 따라서 본 논문에서는 방화벽의 사용으로 인한 네트워크 성능감소 원인을 분석하고, 효율적인 대응방안을 제안하고자 한다. Ⅱ장에서는 관련분야에 대한 연구내용을 기술하고, Ⅲ장은 방화벽 기능별의 성능분석, Ⅳ장은 제안하는 Exclusive 방화벽에 대해 기술하고 Ⅴ장에서 결론부분으로서 이글을 마친다.

Ⅱ. 관련연구

2.1 방화벽(Firewall)

방화벽은 내·외부 네트워크를 보호하기 위한 보안시스템의 하나로 외부의 불법적인 침입으로부터 내부의 정보자산을 보호하고, 유해정보 유입을 차단하기 위한 정책과 하드웨어 및 소프트웨어를 총칭한다. 또 다른 기능으로는 외부 네트워크와 연동되는 유일한 출입경로로서 인바운드, 아웃바운드의 데이터의 헤더정보를 분석하여, 내·외부의 접속을 통제하거나, 인증절차를 통해 인가된 사용자를 선별한다. 그리고 접속된 내·외부 네트워크에 대한 트래픽을 모두 기록한다. 이 절에서는 방화벽에 대한 성능분석을 위해 유형별 방화벽의 기능 및 특징에 대해 기술한다.

2.2 기존 방화벽의 유형별 특징

(1) 패킷필터링(Packet Filtering)

OSI 7계층 모델의 네트워크와 트랜스포트 계층에 적용 가능한 전형적인 방화벽의 형태로서, IP 패킷과 TCP 세그먼트의 헤더 정보를 통해 허용 및 차단 기능을 수행한다. 다른 방화벽유형보다 처리속도가 우수하며, 정책 수립에 빠른 연동성과 유연성을 제공한다. 프로토콜별 통제가 가능하고, IP Spoofing, TCP SYN Flooding 공격으로부터 네트워크를 방어하며, 구축비용이 저렴하다[1].

◎ 문제점

TCP/IP 프로토콜 헤더 조작과 같은 공격에 취약하고, 트래픽의 상세한 분석이 어렵다. 그리고 모든 패킷에 대한 로그를 기록하지 못하며, 다양한 공격 형태에 따른 정책수립이 매우 복잡하다. 한번 승인된 사용자에 대해서는 내부 네트워크에 대한 접근이 자유롭지만, 재 인증 절차를 거치지 않는다는 점으로 인해 인증 상의 취약성도 내포하고 있다. 그 밖에 네트워크가 확장됨에 따라 정책은 점차 복잡해지며, 정책에 따른 규칙의 증가로 네트워크 성능은 크게 저하된다[2][3][5].

(2) 듀얼 홈드 게이트웨이(Dual Homed Gateway)

두 개의 네트워크 인터페이스를 갖춘 호스트가 내·외부 네트워크의 출입문역할을 수행한다. 두 개의 인터페이스 중 하나는 외부 네트워크를 연결하고, 또 다른 하나는 내부 네트워크를 연결하는 방식이다. 물리적으로 내·외부를 연결하며, 논리적으로 두 인터페이스 사이에 소프트웨어적으로 패킷에 대한 필터링을 수행한다. 이 방식은 일반적으로 라우터의 역할을 수행하기도 하며, 게이트웨이라 부르기도 한다. 정책에 의해 내·외부 네트워크의 통제가 가능하기 때문에 대부분의 방화벽이 이와 같은 유형을 적용하고 있다. 또한 한 대의 장비만으로도 구축이 가능하고, 출입하는 모든 데이터를 분석하여 기록을 남기기 때문에 역추적이 가능하다. 그밖에 구축비용이 저렴한 장점이 있고, 설치와 유지보수도 간편하다.

◎ 문제점

한 대의 장비로 네트워크의 중추적인 역할을 수행하기 때문에 해당 장비가 손상되거나 공격을 당했을 경우 대응하기가 어렵다. 그리고 정책수립이 복잡하기 때문에 정책설정시, 운영자의 실수로 인한 취약성 문제도 내포하고 있다. 또한 한 대의 장비가 네트워크의 모든 트래픽을 담당하고 있기 때문에 네트워크 성능의 저하요인이 된다.

(3) 프락시(Proxy)형

데몬(Daemon) 형태로 동작하며, 응용계층에서 사용되기 때문에 "프락시 게이트웨이(Gateway)" 또는 "프락시"라 한다. 패킷 필터링과 같은 접근통제 기능을 제공할 뿐 아니라 서비스별 통제가 가능하고, 직접적인 TCP세션

(Session)이 없음으로 내부 네트워크의 주소를 은폐할 수 있어, Connectionless 상태에서 각 서비스와 세션별 감사(Audit)가 가능하다[3][6].

◎ 문제점

응용프로그램 및 서비스에 따라 수행되기 때문에 내부 네트워크의 성능을 크게 저하시키는 단점이 있다. 그리고 새로운 서비스에 대한 빠른 대응이 불가능하여, 사용자에게 보안성 있는 서비스를 보장할 수 없다. 또한 다양한 서비스에 따른 정책적용은 성능저하의 주요원인이 된다[6].

(4) 하이브리드(Hybrid)형 방화벽

여러 유형의 방화벽 기능을 혼합 구성한 형태로 서비스와 IP, MAC 등을 통제관리 함으로써 편의성, 보안성을 가장 효과적으로 제공할 수 있도록 정책을 수립할 수 있다. 그러나 효과적인 네트워크의 구축과 관리를 위해 정책의 혼잡성과 속도저하라는 단점이 있다.

◎ 문제점

혼합기능으로 인해 정책의 중복문제가 발생할 수 있으며, 시스템의 성능에 따른 의존성이 크게 나타나게 된다. 다음 표1은 앞서 기술된 방화벽 유형들을 종류별로 각각의 장단점을 비교하였다.

표 1 방화벽 유형에 따른 장단점 비교
Table 1. Firewall's comparison

유형	기 능	장 점	단 점
패킷필터링 형	IP주소와 Port를 이용하여 제어	처리속도가 빠르고, 단순	TCP/IP헤더 조작에 대응 할 수 없음.
게이트웨이 형	네트워크의 출입문의 역할로 중추적인 기능수행가능	구축비용이 저렴, 유지보수가 용이, 관리가 편함.	공격에 대한 대응이 어려움.
프락시 형	소스를 감출 수 있고, 단순하며, 사용자에게 투명성을 보장	강력한 인증과 부가적 서비스제공	투명성 보장 못함.
하이브리드 형	여러 유형을 조합	효율적이고, 유연성 있는 보안정책을 부여가능	구축의 어려움

2.3 방화벽의 주요 성능저하 요인

(1) 패킷필터링(Packet Filtering)

네트워크에 인바운드, 아웃바운드 되는 모든 패킷에 대해 IP헤더와 상위 프로토콜 헤더를 검사하여 해당정보를 획득한 뒤, 이미 수립된 정책에 따라 서비스의 허용 및 거부를 결정한다. 따라서 네트워크 의 규모와 데이터 전송량에 따라 정책설정이 복잡해지며, 필터링 후, 감사로그에 따른 수행과 중복 정책으로 인한 오동작으로 시스템의 부하를 가중시켜, 전체 네트워크의 성능을 저하시킨다.

(2) 주소변환(NAT : Network Address Translation)

내부 네트워크의 관리 및 보호를 위해 사설 네트워크 및 내부 네트워크에서의 서버보안을 수행하는데 사용된다. 대표적인 기능으로 경로설정(Redirection) 기능은 서버를 보호하는데 사용되며, 원격지에서 사설네트워크로의 접속을 가능케 하기 위한 Reverse기능도 포함하고 있다. 그러나 Reverse기능이 악용 될 경우, 침입경로를 제공해 줄 수 있어 취약하며, 사설 네트워크의 규모와 데이터의 전송량에 따라 주소변환은 다른 방화벽 기능과 함께 시스템의 부하를 가중시켜, 네트워크의 성능을 저하시킨다[7][8][11].

(3) 프락시(Proxy)

네트워크 내·외부의 서비스에 대해 투명성을 제공한다. 서비스를 사용하고자 하는 어떠한 연결요청에도 TCP세션을 허용하지 않으며, 각 연결에 대해 인증기능을 제공함으로서 인가되지 않은 사용자의 접근을 차단한다. 그러나 방화벽 기능 중, 내부 사용자의 다양한 서비스를 통제해야하기 때문에 복잡한 정책설정과 인증절차로 인하여 네트워크의 성능저하의 주요원인이 되며, 시스템의 부하를 급증시킨다[3].

(4) 정책(Policy)

방화벽의 설계, 설치, 사용에 직접적인 영향을 줄 수 있으며, 네트워크보호를 수행하기 위한 기능들에 적용될 규칙들을 "정책"이라 한다. 사용자를 레벨(Level)별로 구분하고, 네트워크의 세션(Session) 및 연결(Connection)의 허용유무를 결정한다. 그리고 패킷 필터링, 프락시, 주소변환등과 같은 기능들은 각각의 정책들에 의해 종속적으로 동작한다. 따라서 정책은 네트워크 환경과 관리자의 보안의식, 보안시스템 제품과도 연관성을 갖게 된다.

표 2 주요 기능의 정책 연관성
Table 2. Major function's policy comparison

기 능	연관성 정책
패킷필터링 (내→외부)	- 접근통제(IP, Port 정책참조) - 인증(User DB참조) - NAT(정책참조) - 프락시(정책참조)
프락시 (내→외부)	- 패킷필터링(정책참조) - 접근통제(IP, Port 정책참조) - 사용자 인증(User DB참조)

	- NAT(정책참조) - 프락시(정책참조)
NAT (내→외부)	- 패킷필터링(정책참조) - NAT(정책참조) - 인증(User DB참조) - 접근통제(IP, Port 정책참조) - 프락시(정책참조)
인증 (내→외부)	- 관리자인증(정책참조) - 사용자인증(User DB참조) - 패킷필터링(정책참조) - NAT(정책참조) - 접근통제(IP, Port 정책참조) - 프락시(정책참조)

표2는 정책의 참조에 대해 나타낸 것과 같이 각 주요 기능의 정책들은 상호 연동성을 갖고 운영되고 있다. 따라서 각 기능에 다른 정책설정과 관리는 다른 기능들과의 연계성을 고려한 설정이 필요하다. 네트워크의 규모가 커지고, 사용자 및 장비가 증가함에 따라 정책의 적용과 관리상의 문제는 더욱더 복잡해지게 되며, 정책의 중복으로 인해 오동작이나 성능저하 등의 문제를 야기 시킨다[6].

III. 기능별 성능분석

방화벽의 기능별 성능실험을 통해 네트워크의 성능저하 원인을 분석한다. 그리고 방화벽에 따른 성능분석을 위해 대표적인 기능인 패킷필터링, 주소변환, 게이트웨이, 프락시, 정책에 대해 실험한다.

3.1 패킷필터링 분석

내·외부네트워크를 통과하는 모든 패킷들에 대해 헤더정보를 필터링함으로써 허용여부를 결정한다. 따라서 전송속도와 헤더정보인자인 IP와 MAC에 대해 성능을 분석한다. 실험환경으로 리눅스 8.0에 방화벽 프로그램인 IPchain과 설정된 규칙들을 적용하고, 스마트비트로 전송속도를 달리하여 패킷처리시간을 측정한다. 이 실험을 통해 패킷필터링 기능의 사용유무에 따른 처리율과 전송속도에 따른 처리율, 필터링 인자인 IP와 MAC에 대한 처리율을 분석한다. 다음 그림 1은 실험 결과를 나타낸 것이다.

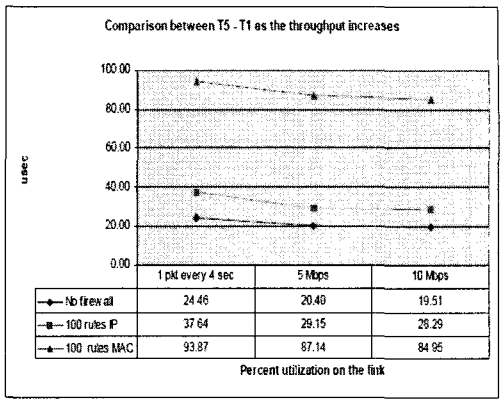

그림 1 전송률증가에 따른 지연시간
Fig 1. Latency time of comparison the throughput increases

그림1의 실험결과와 같이 패킷필터링 기능을 사용할 경우, 그렇지 않을 경우보다 최대 60~80% 처리지연이 발생되고, IP보다 MAC에 의한 지연도 약 10~15% 더 증가되었다. 또한 전송속도가 증가함에 따라 패킷필터링의 지연시간은 오히려 3~6% 감소함으로써, 전송속도와 지연시간이 반비례함을 알 수 있다. 결과적으로 방화벽의 사용유무와 필터링 인자에 따른 속도저하는 내부 네트워크의 성능저하에 직접적인 영향을 미치고 있다[1][2].

3.2 주소변환(NAT:Network Address Translation)분석

IP주소의 부족문제를 해결과 보안을 위한 기술로 공인주소를 다수의 사설주소로, 다수의 사설주소를 공인주소로 변환한다. 따라서 사설주소의 사용자 증가에 따른 처리효율의 변화를 통해 주소변환 성능을 분석한다. 성능분석을 위한 실험환경으로 리눅스 8.0에 펜티엄3 노트북 2대, WLAN이 지원되도록 linux-wlan-ng드라이버와 802.11이 지원되는 100Mbps Ethernet으로 구성하고, NAT의 오버헤드 측정을 위해 2가지 시나리오로 실험한다. 첫째 시나리오는 단일 사용자가 FTP서버로 동작하는 노트북으로부터 파일(1KB에서 4M까지의 데이터)을 다운로드 받을 때, 주소변환이 지원하는 경우와 지원하지 않을 경우를 비교하고, 두 번째 시나리오는 다중 사용자가 파일을 다운로드 하였을 때, 주소변환이 지원하는 경우와 그렇지 않은 경우, 대역폭 처리효율을 IPerf로 각각 측정한다. 이 실험을 통해 단일 또는 다중 사용자가 사용하였을 경우, 네트워크의 오버헤드(Overhead)를 분석한다. 다음 그림2와 3은 실험결과를 나타낸 것이다.

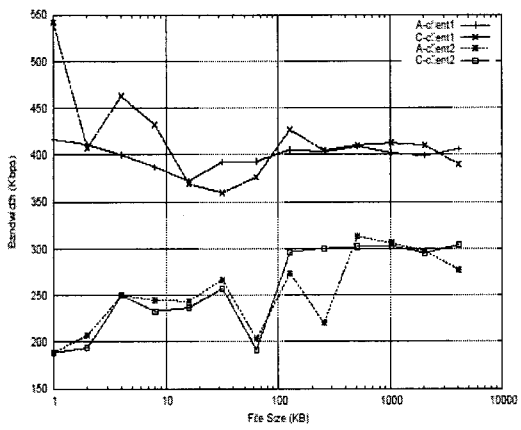

그림 2 NAT 단일 사용자
Fig 2. NAT Overhead : Single Guests

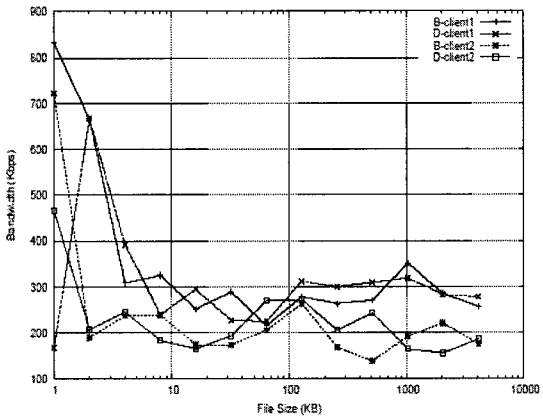

그림 3 NAT 다중 사용자
Fig 3. NAT Overhead : Multiple Guests

그림3의 실험결과와 같이 단일사용자가 주소변환을 사용할 경우, 그렇지 않을 때보다 처리효율이 약 30~50%정도 저하되고, 그림3의 실험결과와 같이 주소변환을 사용하는 경우, 대역폭의 처리효율의 차이는 약 20~30%정도의 차이를 보인다. 그리고 단일 사용자의 주소변환 사용유무 때와는 달리 큰 차이를 보이지 않았다. 결과적으로 전송하는 파일크기와 사용자 수에 따라 대역폭의 처리효율에 영향을 미치며, 다중 사용자의 경우, 사용자수와 무관하게 처리효율이 크게 저하되어, 내부 네트워크의 성능을 저하시킨다[10][11].

3.3 하이브리드형의 게이트웨이와 프락시 분석

게이트웨이와 프락시의 기능을 혼합하여 하이브리드 형 방화벽을 구성한다. 프락시 방화벽은 다양한 서비스를 통제하기 때문에 수많은 데이터들을 통제해야 한다. 따라서 메시지의 크기 변화를 통해 프락시 방화벽의 처리효율로 성능을 분석한다. 성능분석을 위한 실험환경으로 2대의 리눅스 8.0시스템에 NAT 1.0과 프락시 방화벽을 각각 구축하고, 스마트비트를 통해 임의의 크기로 데이터를 전송한다. 그리고 방화벽을 사용하지 않았을 경우와 게이트웨이, 주소변환, 프락시 각각의 기능만을 사용하였을 경우의 처리효율을 측정한다. 이 실험을 통해 방화벽을 사용하지 않았을 경우와 게이트웨이, 주소변환, 프락시 각각의 평균대역폭의 처리효율을 분석한다. 다음 그림5는 실험결과를 나타낸 것이다.

실험결과와 같이 방화벽을 사용하지 않았을 경우와 프락시를 사용했을 경우 약 3배의 처리효율의 차이를 나타내고, 게이트웨이와 NAT의 경우 동일하게 측정되었다.

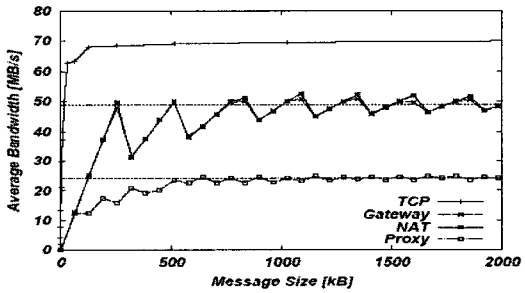

그림 4 메시지에 따른 테스트결과
Fig 4. Long message tests

따라서 다음과 같은 게이트웨이와 프락시 기능실험의 결론을 얻을 수 있다. 프락시는 방화벽의 다른 기능들에 비해 낮은 대역폭 처리효율을 나타내며, 방화벽시스템의 많은 부하를 발생시키는 원인이 된다. 그리고 게이트웨이나 주소변환보다도 더 많은 부하를 초래하기 때문에 다중 사용자의 서비스 경우, 처리효율의 감소 뿐 만 아니라, 내부 네트워크의 성능을 크게 저하시킨다[1][9].

3.4 하이브리드형의 주소변환과 프락시(Proxy) 분석

내부 네트워크의 다중 사용자관리 및 서비스를 위해 응용계층 방화벽에서는 주소변환과 프락시기능이 사용된다. 따라서 사용자 수에 따라 주소변환과 프락시의 처리효율로 비교분석한다. 성능분석을 위한 실험환경으로 리눅스 8.0기반에 NAT 1.0과 프락시 방화벽 2대를 각각 구축하고, 클라이언트 시스템을 각각 4대씩 연결하여 임의의 크기로 데이터를 전송한다. NAT와 프락시를 비교하기 위해 다음과 같은 시나리오로 실험한다. 실험은 사용자 수를 1:1, 2:1, 4:1, 4:4 통신의 경우, 프락시와 주소변환, 2중 프락시로 하여

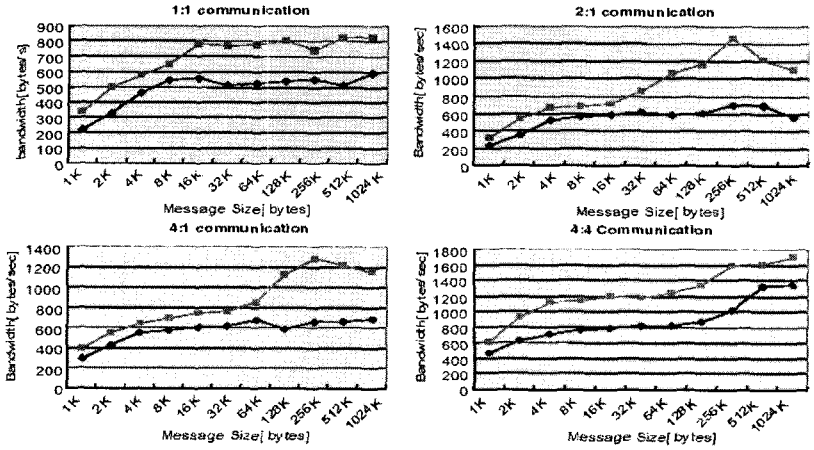

그림 5 메시지 크기에 따른 주소변환+프락시와 2중 프락시 대역폭 사용률비교
Fig 5. Bandwidth between NAT+Proxy and Double Proxy

각각의 대역폭 사용률을 측정한다. 이 실험을 통해 사용자의 증감에 따른 프락시와 주소변환의 처리효율을 분석한다.

그림6의 실험결과와 같이 주소변환+프락시와 2중 프락시의 경우, 사용자의 수와 메시지 크기에 따라 대역폭 사용률이 증가함을 알 수 있다. 1:1의 경우에는 약 1.3~1.5배, 2:1은 약 1.3~2.1배, 4:1은 1.3~1.8배, 4:4는 1.2~1.5배로 모두 메시지 크기가 변화함에 따라 대역폭 사용이 커지고, 사용자 수에 따른 처리효율이 증가하였다. 다음 그림6은 NAT+프락시와 2중 프락시의 처리지연시간을 비교한 것이다[1][9].

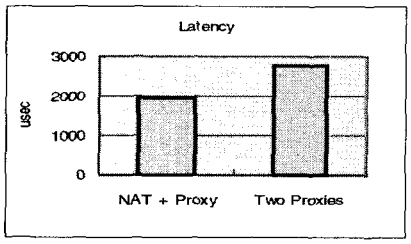

그림 6 NAT와 프락시의 지연
Fig 6. Latency between NAT and Proxy

그림7의 실험결과 프락시는 주소변환보다도 1.4배 더 많은 데이터 처리시간이 소요되며, 낮은 처리효율을 나타내고 있다. 따라서 다음과 같은 주소변환+프락시와 2중 프락시 실험의 결론을 얻을 수 있다. 주소변환과 프락시는 전송되는 데이터와 사용자가 증가함으로써 효율이 저하되고, 방화벽 시스템의 데이터 처리속도와 시스템 성능저하 뿐만 아니라 내부 네트워크의 효율성을 저하시킨다[7].

3.5 정책(Policy)에 따른 성능분석

방화벽의 설계, 설치, 사용에 직접적으로 영향을 줄 수 있는 네트워크보호의 수행 규칙들을 정책이라 한다. 패킷필터링과 프락시(Proxy), 인증(Authentication), 주소변환(NAT)등 각 기능에 따른 정책들이 있다. 따라서 정책의 수에 따라 시스템 및 네트워크의 성능에 어떠한 영향을 미치는지 분석한다. 성능분석을 위한 실험환경은 리눅스 8.0에 방화벽 프로그램인 IPchain을 미리 설정된 규칙들로 적용하고, 스마트비트로 전송속도를 달리하여 패킷처리시간의 차이를 측정한다. 정책에 따른 규칙의 수가 각 전송 프로토콜에 미치는 영향을 비교하기 위해 다음과 같은 시나리오로 실험한다. 실험은 각 기능에 따라 정책들을 설정하고, UDP와 TCP 전송방식을 기반으로 데이터를 전송하였을 경우, 이에 따르는 지연시간을 측정, 비교함으로써 규칙의 증감에 따른 처리시간을 분석한다.

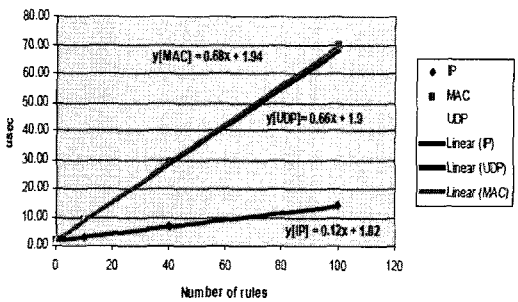

그림 7 UDP연결 시 방화벽의 규칙 수에 따른 처리시간
Fig 7. UDP connection linear relationship between the number of rules and the time to process the firewall

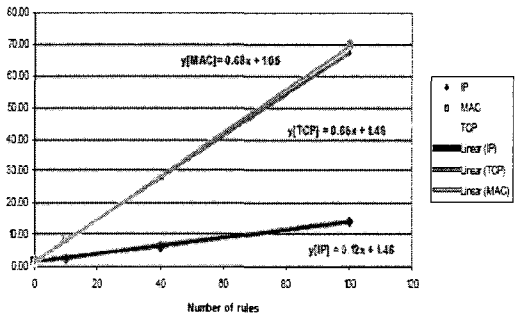

그림 8 TCP연결 시 방화벽의 규칙 수에 따른 처리시간
Fig 8. TCP connection linear relationship between the number of rules and the time to process the firewall

그림8과 9는 방화벽의 규칙수와 데이터형태(TCP, UDP, IP, MAC)에 따른 처리시간을 비교한 것으로 처리시간도 함께 비례함을 알 수 있다. IP의 경우 규칙이 증가함에 따라 비교적 완만한 기울기의 처리지연을 보이지만, MAC과 TCP, UDP의 경우 급격한 증가를 보이고 있다. 따라서 각기 다른 처리지연시간은 시스템과 네트워크의 성능저하와 전송 프로토콜에 따른 처리지연시간을 함께 비교해 볼 수 있다. 결과적으로 다음과 같은 정책과 전송 프로토콜에 따른 처리시간실험의 결론을 얻을 수 있다. 최대 5배 이상의 처리지연시간이 발생하며, 방화벽의 기능들과 사용한 정책인자들은 다음과 같은 연관성을 가지고 있음을 알 수 있다. 서비스에 대한 정책을 담당하는 프락시 기능은 TCP와 UDP 헤더로부터 정책에 필요한 정보를 수집하고, 패킷필터링과 주소변환은 IP와 MAC 헤더로부터 정보를 수집한다. 이러한 결과는 앞서 언급한 방화벽의 다른 기능들의 성능분석 결과와도 동일한 결과를 나타내고 있다[2].

IV. 제안하는 Exclusive 방화벽

방화벽에서의 주요기능에 따른 시스템 부하 및 성능저하 요인에 따른 문제해결을 위해 기능별 시스템을 구성하고, 각각의 독립적인 시스템 운영이 필요하다. 기능별 분류를 한다면, 방화벽의 기본기능인 패킷필터링 기능만을 수행하는 방화벽과 프락시 기능의 방화벽, 주소변환기능의 방화벽을 각각 구분한다[4]. 또한 감사기록의 관리는 기능별 방화벽에 SMS(System Management System)로 각 시스템을 관리하고 로그한다. 이렇게 함으로써 시스템에 남는 로그에 의한 방화벽 성능저하 및 정지, Shutdown현상을 방지할 수 있다. 그리고 프락시의 서비스별 방화벽 구성으로 서비스에 따른 성능을 향상시킬 수 있으며, 한 대의 방화벽만을 사용한 네트워크 부하를 분산 관리함으로써, 프로토콜에 따른 효율적인 네트워크 서비스를 제공할 수 있다. 다음 절에서는 제안하는 Exclusive 방화벽의 유형과 정책, 배치, 기대효과에 대해 기술한다.

4.1 Exclusive 방화벽의 분류

방화벽의 기능을 다음과 같이 분산하고 각 기능별 Exclusive 방화벽을 구축한다. 필요에 따라 Exclusive 방화벽 간의 연동도 고려할 수 있다.

가. IO 방화벽(Inner & Outer Firewall)

Inner & Outer 방화벽은 전체 네트워크의 외부공격으로부터의 방어와 내부 사용자의 접근통제가 주목적이며, 주요기능으로 패킷필터링 기능만을 수행한다. 3.1절에서의 성능분석을 근거로 네트워크의 최 종단에서 약60%의 속도저하문제를 야기 시켰던 패킷필터링 기능을 전용 시스템으로 구성하고, 필터링 기능이 필요한 위치에 배치함으로써, 속도 및 성능 저하를 개선하고, 필터링기능이 필요한 네트워크에 환경을 부분적으로 보호할 수 있는 장점이 있다. 방화벽의 배치는 외부로부터의 인가되지 않은 연결요청에 대해 차단을 목적으로 하는 Local 부분을 담당하게 되며, 외부 네트워크로의 최종 단에 배치된다.

나. NAT 방화벽(Network Address Translation Firewall)

주소변환방화벽은 사설네트워크를 구성하고, 네트워크의 분할과 접근통제를 수행하는 것이 주된 목적이며, 주요기능으로 패킷필터링과 주소변환(NAT)기능만으로 구성된다. 3.2절에서의 성능분석을 근거로 사설주소 네트워크의 사용으로 대역폭 효율의 약 30~50% 저하되는 현상을 해결하기 위해 사설네트워크의 구성이 필요한 Local 부분만을 별도로 관리하도록 한다. 그럼으로써, 정책의 중복과 방화벽의 다른 기능수행으로 인한 전체 네트워크의 성능저하를 방지할 수 있고, 효율적인 관리가 가능하다[7][8][11].

다. Gate 방화벽(각 서비스별 방화벽(HTTP, FTP, SMTP, POP3 등))

Gate 방화벽은 서비스별 통제가 목적이며, 프락시 기능만을 포함한다. 내부 사용자의 서비스를 통제함으로써 외부의 침해로부터 네트워크를 보호한다. Gate방화벽은 기존의 프락시에서 모든 서비스를 통합 관리했던 것과는 달리 하나의 서비스만을 담당한다. 3.3과 3.4절에서의 성능분석을 근거로 각 서비스에 따른 시스템의 성능저하 개선과 트래픽의 효율적인 관리를 위해 서비스 프로토콜에 따른 별도의 장비

로 구성된다. 이렇게 함으로써 내·외부 네트워크에서 대부분의 성능저하의 원인이 되었던 프락시 기능과 로그관리상의 문제를 해결할 수 있으며, 서비스에 따른 규칙의 수의 절감으로 시스템의 성능을 향상시킬 수 있다.

4.2 Exclusive 방화벽의 정책

방화벽의 정책들을 여러 시스템으로 분산하여 배치 및 관리함으로써, 표2에서의 참조정책을 근거로 정책의 중복문제를 해결하고, 성능을 향상시킬 수 있도록 한다. 또한 분산정책관리로 인한 장점들은 다음과 같다.

- 각 기능별 방화벽은 네트워크의 보안레벨에 따라 구성이 가능하고, 네트워크의 관리를 효율적으로 수행할 수 있다. 그리고 독립적인 정책설정을 통하여 관리되어지기 때문에 방화벽 시스템의 규칙증가에 따른 성능저하 문제를 해결할 수 있다.
- 보안레벨에 따라 구축된 네트워크는 성능저하를 최소화하며, 보안의 2중, 3중 정책을 수립할 수 있다. 불필요한 정책의 및 중복을 배제시키고, 보안레벨이 낮은 네트워크에 대해서 차등 정책을 수행할 수 있다.
- 분산정책에 따른 규칙 수를 감소시킴으로써, 시스템 자원의 활용을 극대화 할 수 있다.

4.3 Exclusive 방화벽 적용 Trusted 네트워크 구축

Exclusive 방화벽을 적용한 네트워크 구축은 3개의 보안지역으로 나뉘어 관리되고 감사되어진다. 기존의 방화벽을 배치한 네트워크의 획일적인 단일 구성과 1대의 장비에서 모든 네트워크를 담당하는 구조와는 달리, Exclusive 방화벽을 적용한 네트워크에서는 보안등급을 두어 낮은 등급에 해당하는 보안지역은 보안을 하지 않을 수 있다는 것이 큰 특징이다.

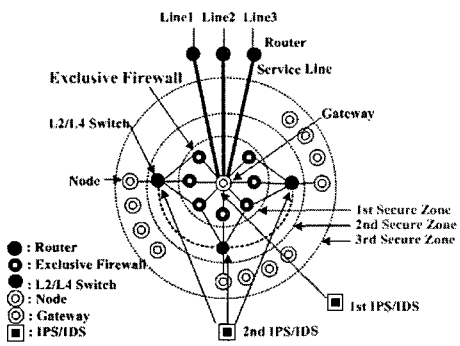

그림 9 Exclusive 방화벽 적용 네트워크 구축
Fig 9. Network design of the Exclusive firewall

그림10은 Exclusive 방화벽을 적용한 Trusted 네트워크를 나타내고 있다. "1st Secure Zone"은 Exclusive 방화벽의 배치지역으로 보안시스템들로 이뤄진 네트워크의 1차 방어지역이다. 여기서 각 보호 목적에 따라 해당하는 Exclusive 방화벽들을 통해 "3rd Secure Zone"의 Node들을 연결한다. "3rd Secure Zone"에서는 Node 각각을 보호하기보다 Node에서 사용 중인 서비스 및 연결을 통제하는 역할을 수행한다. 따라서 Node들에 대해 별도의 보안 시스템을 두지 않는다. 이유로는 2차 네트워크 방어 영역인 "2nd Secure Zone"에서 내부 네트워크의 침입탐지 및 차단을 수행하기 때문에 내부 침입 및 내부 침입을 "3rd Secure Zone"의 IPS/IDS를 통해 감시, 감사관리 하기 때문이다.

4.4 기존 방화벽과의 성능비교

다음은 기존 방화벽과의 Exclusive 방화벽의 성능비교를 위한 실험환경이다. 리눅스 9.0환경에서 CPU 433Mhz, 메모리 256M와 하부 네트워크의 사용자를 가정하기 위해 노트북을 5대 연결하였다. 기존 방화벽의 기능을 대신할 Iptable을 설치하고, 테스트를 위한 전송 메시지 크기를 300k 사이즈로 하였다. 실험측정을 위한도구로 IPerf를 이용해 대역폭과 지연시간을 측정하였다. 시나리오로는 기존 방화벽의 환경과 같이 패킷필터링과 NAT, 프락시, 게이트웨이 기능을 포함한 방화벽을 운영하였을 경우와 본 논문에서 제안하는 Exclusive 방화벽을 각각 운영했을 경우의 성능을 측정하여 비교하기로 한다.

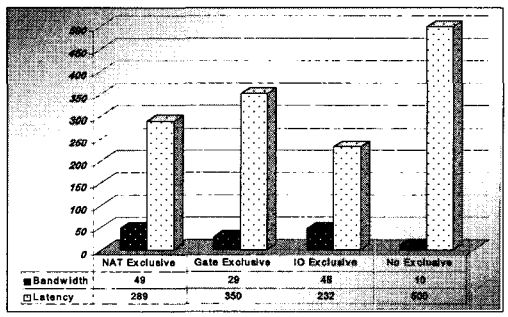

그림 10 Exclusive 방화벽 성능비교
Fig 10. Response time as rule numbers

그림11의 결과는 지연현상과 대역폭의 활용률을 비교한 것으로 기존의 방화벽보다 Exclusive방화벽의 성능이 큰 차이를 보이고 있다. NAT Exclusive는 기존방화벽보다 처리율을 약 5배 향상되었고, 지연시간은 43%절감되었으며,

Gate는 처리율 3배 향상과 지연 30%절감, IO는 처리율 약 5배 향상과 지연54%절감 효과를 나타내었다. 그러나 실제 네트워크의 보안 레벨에 따른 적용을 하여 Exclusive 방화벽을 배치한다면, 기존의 방화벽보다 더 큰 성능차이를 보일 것이다.

4.5 기대효과

기존의 방화벽은 기능 및 서비스를 통합 관리함으로써, 많은 성능저하와 기능상의 오류 및 네트워크 속도저하 등의 문제가 발생하였다. 그러나 시스템의 효율적인 재배치 및 기능분할, 서비스의 분할관리 운영으로 성능저하 및 네트워크 속도저하현상을 개선할 수 있다.

가. 네트워크 성능 기대효과

표 3 대역폭과 지연의 비교
Table 3. Bandwidth and Latency's comparison

	Bandwidth (MB/sec)	Latency (μsec)
Network	135.5	12.5
TCP	70	14
Gateway	49	232
NAT	49	289
Proxy	29	350

기존의 방화벽을 이용한 Trusted 네트워크 구성은 비효율적인 관리와 운영, 중복정책들로 인한 네트워크의 속도지연 등의 문제가 있다. 그러나 Exclusive 방화벽시스템을 이용한 Trusted 네트워크 구성은 내부 네트워크 속도를 향상시키고, 불필요한 정책을 배제하며, 보안레벨에 따르는 차별화된 보안레벨을 전체 네트워크에서 부분 적용이 가능하기 때문에 내부 네트워크의 트래픽을 효율적으로 관리할 수 있다. 따라서 표3과 같은 지연을 한대의 장비에서 부담하는 것이 아니라, Exclusive 방화벽들 각각에서 분담하기 때문에 그림 11의 결과처럼 내부 네트워크에서 사용하는 대역폭 활용률을 높이고 지연시간 을 낮출 수 있어 전체 네트워크의 성능을 향상시킬 수 있다.

나. 정책관리의 기대효과

다음 그림12와 13[11]은 방화벽의 모든 기능에 따른 정책을 적용하였을 경우, 규칙에 따른 응답시간과 처리율의 변화를 나타낸 것이다. 정책에 따른 규칙의 수가 증가할 경우, 응답시간은 지연되고, 처리율은 저하되는 현상을 보여 규칙의 수와 네트워크의 성능이 반비례함을 알 수 있다.

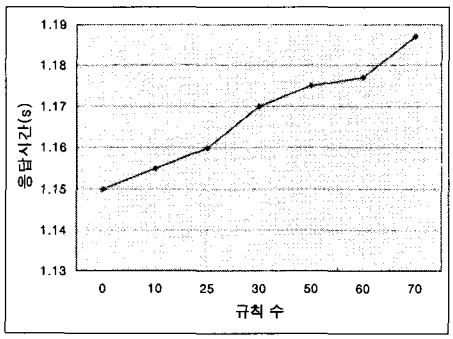

그림 11 규칙 수에 따른 응답시간
Fig 11. Response time as rule numbers

한 대의 방화벽에서 모든 기능을 담당하여 정책이 복잡해지고, 규칙의 수가 증가함에 따라 응답시간을 지연시켰지만, 기능에 따른 Exclusive 방화벽으로 분산관리 할 경우, 각 시스템에 해당하는 정책들로만 운용되기 때문에 처리율이 증가하게 된다.

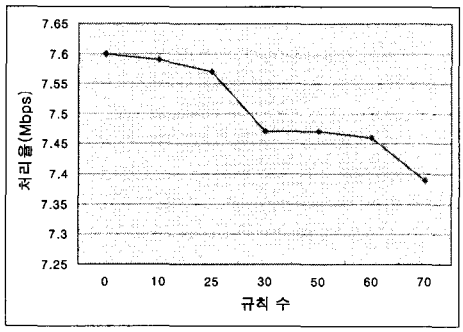

그림 12 규칙 수에 따른 처리율
Fig 12. Throughput as rule numbers

결과적으로 중복정책 적용 및 다기능 정책으로 인한 지연시간 문제를 해결하고, 정책오류를 피할 수 있으며, 시스템 성능과 네트워크 성능개선에 따르는 비용절감을 할 수 있다. 또한 서비스의 속도를 향상시키며, Exclusive 방화벽 사용으로 인해 내부 네트워크의 보다 정밀한 정책설정이 가능하여 보안성을 더욱 극대화 할 수 있다.

V. 결론

불법 침입자들로부터의 공격유형이 다양화되어지고 있고, 공격으로부터 방어를 하기 위해 이에 따른 보완대책들이 필요한 이 시점에서 효율적인 네트워크 관리와 보안시스템의

기능별 분산배치는 개선되어야 할 것이다. 본 글에서 제안한 Exclusive 방화벽을 활용한 Trusted 네트워크의 구축은 향후 IPV6과 유비쿼터스 장비 및 다양화되는 서비스에 효과적으로 대응할 수 있으리라 기대한다. 그러나 기능에 따른 다양한 Exclusive 방화벽의 구입비용과 관리장비의 증가는 단점으로 작용할 수 있다. 따라서 앞으로 이에 대한 보완대책과 통합관리의 추가적인 연구가 필요하며, 효율적인 통합관리시스템체계로의 연구도 함께 병행되어야 할 것이다.

참고문헌

[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"

저 자 소 개

전 정 훈

숭실대학교 컴퓨터공학석사
숭실대학교 컴퓨터공학박사수료
동덕여자대학교 전임강사
관심분야 : 네트워크 보안, 디지털 포렌식, 인증, 무선보안

전 상 훈

숭실대학교 컴퓨터공학석사
숭실대학교 컴퓨터공학박사수료
관심분야 : 네트워크 보안, 인증