# 전산망 보호를 위한 혼합형 방화벽 시스템 구현

이 용 준† · 김 봉 한†† · 박 천 용††† · 오 창 석†††† · 이 재 광†††††


## 요 약

본 논문에서는 스크리닝 라우터, 듀얼-홈드 게이트웨이, 스크린드 호스트 게이트웨이, 그리고 응용 레벨 게이트웨이를 사용한 혼합형 방화벽 시스템을 제안하였다. 스크린드 호스트 게이트웨이는 스크리닝 라우터와, DMZ, 그리고 배스천 호스트로 구성되었으며, 외부의 모든 트래픽은 프로토콜 필터링 기능을 가진 스크리닝 라우터에서 필터링되고, 그리고 응용 레벨 필터링을 수행하기 위하여 배스천 호스트로 전송된다. 듀얼-홈드 게이트웨이는 외부의 사용자가 내부 네트워크를 직접 접근을 못하도록 중개 역할을 한다. 응용 레벨 게이트웨이는 프럭시 서버를 통해서만 트래픽 전송이 가능하도록 한다. 외부 사용자는 DMZ에 있는 공개 서버를 통해서만 내부 네트워크로의 접근이 가능하지만 내부 사용자는 외부 네트워크를 용이하게 사용할 수 있다. 그리고 DMZ에 있는 시스템의 효율적인 관리를 위하여 시스템 관리자만 Telnet 접속이 가능하도록 규칙기반을 적용하였다. 실험 결과, 접근 거부는 Web, Mail, FTP, Telnet 순으로 나타났으며, DMZ에 있는 공개 서버를 제외한 나머지 시스템에 대한 접근은 거부되었다. 프로토콜별 접근 거부는 모든 네트워크에 broadcast하는 BOOTP와 NETBIOS를 사용하는 호스트가 많았기 때문에 TCP보다 UDP가 많이 나타났다. 또한 내부 네트워크에 불법적인 Telnet이나 FTP는 거의 없었다.


# Implementation of Hybrid Firewall System for Network Security

Yong Joon Lee† · Bong Han Kim†† · Cheon Yong Park††† · Chang Suk Oh†††† · Jae Gwang Lee†††††


## ABSTRACT

In this paper, a hybrid firewall system using the screening router, dual-homed gateway, screened host gateway and the application level gateway is proposed. The screened host gateway is composed of screening router, DMZ and bastion host. All external input traffics are filtered by screening router with network protocol filtering, and transmitted to the bastion host performing application level filtering. The dual-homed gateway is an intermediate equipment prohibiting direct access from external users. The application level gateway is an equipment enabling transmission using only the proxy server. External users can access only through the public servers in the DMZ, but internal users can access through any servers. The rule base which allows Telnet only to the administrator is applied to manage hosts in the DMZ. According to the experimental results, denial of access was in order of Web, Mail, FTP, and Telnet. Access to another servers except for server in DMZ were denied. Protocol denials of UDP was more than that of TCP, because the many hosts broadcasted to networks using BOOTP and NETBIOS. Also, the illegal Telnet and FTP that transfer to inside network were very few.


†정 회 원 : 한국전자통신연구원 책임연구원
††준 회 원 : 한남대학교 컴퓨터공학과 박사과정
†††정 회 원 : 한국항공우주연구소 선임기술원
††††정 회 원 : 충북대학교 컴퓨터공학과 교수
†††††정 회 원 : 한남대학교 컴퓨터공학과 부교수
논문접수 : 1997년 10월 6일, 심사완료 : 1998년 4월 27일

## 1. 서 론

인터넷은 컴퓨터 통신을 근간으로 하는 네트워크들의 집합체로서 전 세계적으로 많은 네트워크와 호스트들로 연결되어 있다. 또한, 인터넷의 활용 범위도 놀라운 속도로 변화하고 있어서 정보화 사회의 필수적인 도구로서 자리 잡아가고 있다. 또한, 인터넷은 TCP/IP를 기반으로 이 기종간의 통신이 가능하므로 급속히 발전하였으며, 정보화 사회에 있어서 정보와 통신이 결합되어 움직이는 명실 상부한 "정보화 사회의 기반" 구조가 될 것이 확실하다[1-3].

그러나 인터넷에서 사용하는 TCP/IP 개방형 구조는 UNIX 시스템과 통신 유틸리티 등의 소스 개방으로 인하여 많은 보안상의 취약점을 가지고 있기 때문에 불법 침입자 또는 해커에 의한 피해 사례가 계속 늘어가고 있는 추세이다[4]. 최근에는 상용 서비스의 확산으로 매우 중요한 데이터들이 인터넷을 통하여 상호 교환되고 있으며, 이를 위한 인트라넷 구축도 활발히 진행되고 있다. 이러한 인터넷 상에서 전송되는 중요한 데이터들이 악의적으로 검색, 수정 및 파괴될 경우 그 파급효과는 매우 클 것이 확실하다.

이와 같이 인터넷에 연결하여 사용하는 내부 네트워크의 자원 및 중요한 정보들을 해커로부터 보호하기 위해서는 방화벽 시스템의 설치가 절실히 요구되고 있다. 방화벽 시스템의 설치는 외부의 모든 불법 침입자들을 완벽하게 막아줄 수는 없으나 위험지역을 최소화하는데 그 목적이 있다.

본 논문에서는 스크리닝 라우터와 스크린드 호스트 게이트웨이의 문제점을 해결하는 효과적인 혼합형 방화벽 모델을 제안하고자 한다. 특히, 스크리닝 라우터에서 패킷 필터 규칙을 통과한 모든 트래픽이 베스천 호스트로 전달되도록 스크린드 호스트 게이트웨이를 사용하였으며, 스크린트 호스트 게이트웨이의 단점인 스크리닝 라우터의 경로정보가 내부 네트워크로 직접 전달되지 않도록 듀얼-홈드 게이트웨이를 사용하였다. 듀얼-홈드 게이트웨이에서는 두 개의 네트워크 인터페이스 간에 트래픽이 직접 전달되지 않기 때문에 응용 게이트웨이 서버를 통해서 트래픽이 전달되고 모든 접속기록이 베스천 호스트에 기록되도록 하였다. 또한 외부 네트워크와 내부 네트워크 사이에 완충지역인 DMZ를 두어 공개 서버들을 사용하기 쉽게 구현하였다.

본 논문에서는 2 장에서 인터넷 보안과 방화벽에 대해 살펴보았고, 3 장에서는 혼합형 방화벽 구현 모델링을 기술하였다. 그리고 4 장에서는 구현 모델에 대한 결과분석 및 고찰을 기술하였고, 5 장에서 결론을 맺었다.

## 2. 인터넷 보안과 방화벽

### 2.1 전산망 침입 수법의 분류

일반적으로 불법 침입자가 이용하는 수법으로는 〈표 1〉과 같이 신뢰성 있는 호스트로 위장하기 위한 IP 속임과 네트워크 모니터링 도구를 이용하여 네트워크 상에서 전송되는 패킷을 검사하는 스니핑이 있으며, 네트워크 상에서 디스크를 효율적으로 이용하기 위한 NFS 설계시 보안 취약점 공격 방법들이 있다. 또한, 전자우편을 보내고 받을 때 root의 권한을 사용하는 Sendmail의 취약점을 이용하거나 자신의 계정 유무에 관계없이 대상 시스템의 보안 취약점을 분석하는 도구들을 이용한다[3, 6, 7, 8].

〈표 1〉 시스템 침입 수법
〈Table 1〉 Techniques of system intrusion

| 침 입 수 법 | 내 용 |
|---|---|
| IP 스푸핑 | • TCP/IP의 구조적 결함을 이용하여 침입자가 사용하는 시스템을 신뢰성 있는 호스트로 위장하는 방법 |
| 패킷 스니핑 | • Tcpdump, Spoof, Sniff 등과 같은 네트워크 모니터링 도구를 이용하는 방법 |
| NFS 공격 | • NFS 설계시 보안 취약점을 이용하는 방법 |
| Sendmail 공격 | • 구성화일의 설정시 취약점을 이용하는 방법<br>• 내부 버그를 이용하는 방법<br>• 운영체제 자체의 취약점을 이용하는 방법 |
| Network 스캐닝 | • ISS, SATAN, Tiger 등의 보안 취약점 분석 도구를 이용하는 방법 |

### 2.2 방화벽

인터넷은 TCP/IP를 기반으로 이 기종간의 통신이 가능할 뿐만 아니라 통신과 컴퓨터 기술의 발달 그리고 최근 인터넷에 대한 관심이 높아지면서 규모와 이용자 수가 급속도로 증가하고 있는 추세이다.

그러나 인터넷은 UNIX 및 TCP/IP 소스가 공개되어 있기 때문에 근본적으로 보안상의 문제점을 가지고

있어서 불법적인 사례들이 계속 증가하고 있다. 이는 소스를 분석하여 새로운 불법적인 프로그램을 개발하기도 하고 인터넷을 통한 해킹 방법에 대한 정보 획득을 통하여 시스템의 운영체제나 응용 프로그램에 존재하는 버그를 통한 불법 침입 등과 같은 구조적인 취약점을 이용한 불법침입 사례가 증가하고 있다. 이러한 불법적인 사례들은 초기에는 패스워드를 알아내거나 알려진 취약점을 찾는 수법이었으나, 최근에는 TCP/IP의 구조적인 문제점을 파악하거나 패킷 스니핑, IP 속임과 같은 고도의 지능적인 수법들이 이용되고 있으므로 이에 대한 대비책으로 방화벽을 많이 이용하고 있다.

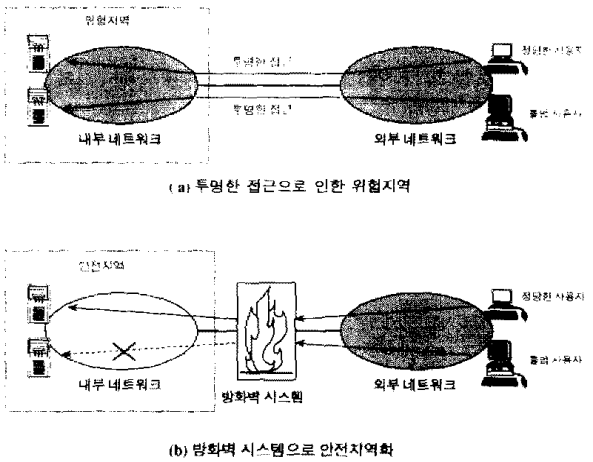
방화벽은 내부 네트워크를 보호하기 위해 외부의 불법적인 트래픽 유입을 막고, 허가되고 인증된 트래픽만을 허용하려는 적극적인 방어 대책으로 주요 목적은 중요한 데이터 및 자원에 대하여 정당하지 않은 사용자의 접근을 막고, 정당한 사용자는 투명한 접근이 가능하도록 하는 것이다[5]. 이에 대한 기본 개념은 (그림 1)과 같다. (그림 1)에서 (a)는 인터넷에 대한 일반적인 접속방법으로 외부 네트워크와 투명한 접근이 가능하므로 내부 네트워크 전체가 위험지역임을 보여주고 있다. (그림 1 (b))는 외부 네트워크와 내부 네트워크 사이의 유일한 경로에 방화벽 시스템을 둠으로써 불법적인 트래픽을 막을 수 있게 되므로 내부 네트워크를 안전지역으로 만들 수 있음을 보여준다[2, 3].

국내 대부분의 기관에서 이미 구축된 내부 네트워크는 외부 네트워크로부터 투명한 접근을 허용함에 따라 내부 네트워크 전체가 위험지역이 된다. 또한 내부적으로 보안 전문가 및 보안기술의 부족, 보안 정책 등도 미비한 실정이어서 많은 보안상의 문제점을 내포하고 있으며, 다양한 하드웨어와 운영체제 및 응용 프로그램 등에 포함되어 있는 많은 취약점을 찾아서 수정하기란 매우 어렵다.

인터넷에 연결된 내부 네트워크의 시스템을 보호하기 위하여 시스템 접속기록 및 제어 도구, 패스워드 파일 보안 도구, 시스템 보안 취약점 분석 및 점검 도구, 방화벽 설치 등을 이용한다[4, 6, 9, 10].

### 2.3 방화벽 구현 방법

방화벽 시스템은 OSI 참조 모델과 관련하여 방화벽 시스템이 동작하는 프로토콜 계층에 따라 패킷 필터링과 응용 게이트웨이로 분류되며, 그 특성을 〈표 2〉에 비교하였다.




(그림 1) 위험지역과 안전지역
(Fig. 1) Dangerous area and safe area

〈표 2〉 패킷 필터링과 응용 게이트웨이 비교
〈Table 2〉 Comparison of packet filtering and application gateway

| 구분 | 패킷 필터링 | 응용 게이트웨이 |
|---|---|---|
| 구성요소 | • 스크리닝 라우터<br>• 패킷 필터링 기능을 가진 호스트 | • 베스천 호스트<br>• 각 서비스별 Proxy 데몬 필요 |
| 기능 | • 출발지 및 목적지 IP 주소의 접속을 제어함<br>• 응용 서비스별 접근을 제어함<br>• 프로토콜별 접근을 제어함 (TCP, UDP, ICMP,...)<br>• 최초 접속제어(TCP sync bit) 장·단점을 가짐 | • 서비스 요청에 대한 축적-전달 기능을 제공함<br>• 일회용 패스워드 같은 강력한 인증 기법이 요구됨<br>• Log 기능 제공함 |
| 장점 | • 처리속도가 빠름<br>• 투명성을 제공함 | • 내부 네트워크에 직접 연결 못함<br>• 강력한 인증 및 Logging 기능제공함<br>• 프로토콜, IP 주소, 사용자등의 제한이 가능함 |
| 단점 | • 유연성이 낮음<br>• screen rule이 복잡함<br>• IP 패킷 헤더의 조작이 가능함<br>• Logging 및 인증기능 제공 안함 | • 패킷 필터링보다 성능이 떨어짐<br>• 새로운 서비스 추가에 대해 Proxy 기능 추가해야함<br>• 일부 Proxy의 경우 클라이언트와 서버 소프트웨어를 수정해야함 |

#### 2.3.1 패킷 필터링

패킷 필터링 방법에서는 스크리닝 라우터를 사용하며, 스크리닝 라우터는 OSI 참조 모델의 네트워크 계층과 전송 계층에서 동작되기 때문에 이들 계층에서 동작하는 프로토콜인 IP, TCP 혹은 UDP의 헤더에 포함

된 내용을 분석하여 동작한다. 최근 상용 라우터들은 프로토콜의 유형, 프로토콜의 출발지와 목적지 주소 필드, 프로토콜의 제어 필드등과 같은 표준을 기초로 하여 패킷을 보호하는 기능을 가지고 있으므로 스크리닝 라우터로 활용할 수 있다.

스크리닝 라우터의 장점으로는 라우터 하나로 내부 네트워크 전체를 동일하게 보호할 수 있으며, 필터링 속도가 빠르고 비용이 저렴하다. 단점으로는 네트워크 계층과 전송 계층에 대한 트래픽만 방어가 가능하며 보안 정책이 유연하지 못하고 패킷 필터링 규칙에 대한 검증의 어려움이 있다. 또한 접속기록을 할 수 없으며 패킷내 데이터에 대한 공격은 차단이 불가능하다.

2.3.2 응용 게이트웨이

1) 듀얼-홈드 게이트웨이

듀얼-홈드 게이트웨이는 두개의 네트워크 인터페이스를 가진 베스천 호스트를 말하며, 이들 인터페이스 사이에 라우팅 기능이 불가능하므로 외부의 신뢰성 없는 네트워크로부터 내부의 네트워크를 분리시키는데 사용될 수 있다. 듀얼-홈드 게이트웨이는 TCP/IP 트래픽을 직접 통과시키지 않기 때문에 내부와 외부 네트워크간의 트래픽을 완전하게 막는다.

라우팅이 없는 듀얼-홈드 게이트웨이를 이용하여 인터넷 또는 내부 네트워크의 정당한 사용자들이 응용 서비스를 제공받는 방법으로는 첫번째, 듀얼-홈드 게이트웨이에서 제공하는 Proxy 서버를 사용하는 방법과 두번째, 응용 서비스를 제공해주는 듀얼-홈드 게이트웨이에 직접 로그인한 다음 다시 내부 네트워크로 접근하는 방법인데, 이 경우에는 일회용 패스워드와 같은 강력한 인증 방법이 구현되어야 한다. 듀얼-홈드 게이트웨이의 가장 큰 위험은 외부로부터 직접 로그인을 허용하는 것이다. 이를 예방하기 위해서는 외부로부터의 신뢰성 없는 로그인에 대하여 강력한 인증이 요구된다[8, 9, 11, 14].

2) 스크린드 호스트 게이트웨이

스크린드 호스트 게이트웨이는 스크리닝 라우터와 베스천 호스트를 혼합한 형태로서, 스크리닝 라우터의 포트는 외부 네트워크와 내부 네트워크로 각각 연결되어 있으며, 베스천 호스트의 네트워크 인터페이스는 내부 네트워크에 연결되도록 구성된 종류이다.

스크리닝 라우터를 구성할 때 외부 네트워크로부터 내부 네트워크로 가는 모든 트래픽을 받은후, 트래픽에 대한 필터 규칙을 적용한 다음 베스천 호스트로 먼저 보내도록 해야 한다. 또한 베스천 호스트는 응용 게이트웨이 서버 기능을 사용하여 나가거나 들어오는 요청을 허용할 것인지 거절할 것인지를 결정해야 한다[8, 9, 11, 14].

3) 응용 게이트웨이 서버

응용 게이트웨이 서버는 방화벽 시스템에서 구동되는 응용 소프트웨어를 말한다. 축적-전달 트래픽뿐만 아니라 대화형의 트래픽을 처리할 수 있으며, 사용자 응용 계층에서 트래픽을 분석할 수 있도록 프로그램 된다.

응용 게이트웨이 서버는 사용자 단계에서 들어오고 나가는 모든 트래픽에 대한 기록을 관리하고 제어할 수 있으며, 해커 및 불법 침입자를 방어하기 위한 일회용 패스워드와 같은 강력한 인증기법이 필요하다[14]. 응용 게이트웨이 서버는 사용되는 응용 서비스에 따라 각각 다른 소프트웨어를 구현하여 사용하기 때문에 높은 수준의 보안을 제공할 수 있다.

응용 게이트웨이 서버는 실제 서버의 관점에서 볼 때 클라이언트처럼 동작하며, 클라이언트 관점에서 볼 때는 실제 서버처럼 동작한다. 응용 게이트웨이의 구현 예는 Telnet 게이트웨이, FTP 게이트웨이, Sendmail, NNTP News Forwarder 등이 있다[2].

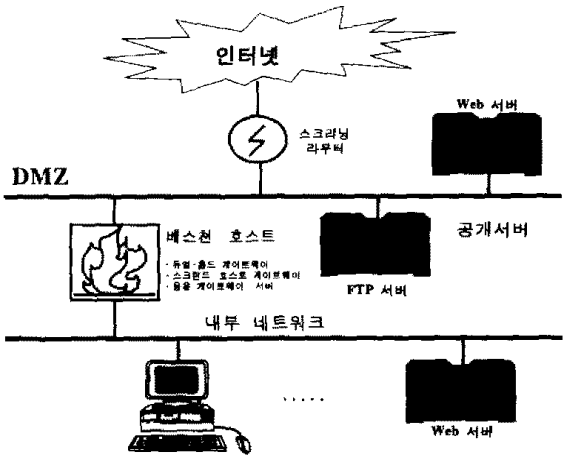
## 3. 방화벽 구축 모델링

3.1 고려사항

네트워크의 보안 정책을 수립할 때 정책을 먼저 수립하는 이유가 보안에 투자하는 노력이 비용에 비해 효과적이기 때문이다. 따라서 내부 네트워크를 보호하기 위해서는 보호하고자 하는 하드웨어, 소프트웨어, 각종 중요한 정보, 시스템 사용자, 시스템 관리에 대한 문서 등과 같은 자원의 보호와 보호하고자 하는 자원 및 정보에 대한 위협에는 어떤 유형의 위협이 있는지, 보호하고자 하는 자원이 얼마나 중요한지, 비인가된 외부인, 인가된 외부인, 내부인에 대한 접근 허용범위를 어떻게 할 것인지, Web, FTP, Telnet, Mail, News 등과 같은 사용 가능한 응용 및 서비스들에 대한 인가범위를 얼마로 할 것인지, 시스템 및 전산망을 효과적으로 보호하기 위하여 비용 대 효과측면을 고려한 실현 가능한 기법에 대한 사항들을 위험분석으로 고려해야 한다.

### 3.2 혼합형 방화벽 설계

스크리닝 라우터의 기능은 네트워크층과 전송층의 트래픽만 방어가 가능하기 때문에 적절한 보안정책을 수행할 수 없으며 접속기록에 대한 관리기능이 없다. 스크린드 호스트 게이트웨이에서 베스천 호스트가 하나의 네트워크 인터페이스로 구성되었을 때, 스크리닝 라우터의 경로정보에 이상이 발생하면 베스천 호스트의 기능이 우회되는 것을 방지하기 위하여 듀얼-홈드 게이트웨이를 사용하였다. 듀얼-홈드 게이트웨이에서 두 개의 네트워크 인터페이스 사이에 트래픽이 직접 전송되지 않기 때문에 응용 게이트웨이 서버 기능을 사용하여 허가된 트래픽만이 전달되도록 하였으며, 또한 모든 접속기록이 베스천 호스트에 누적되도록 하였다.

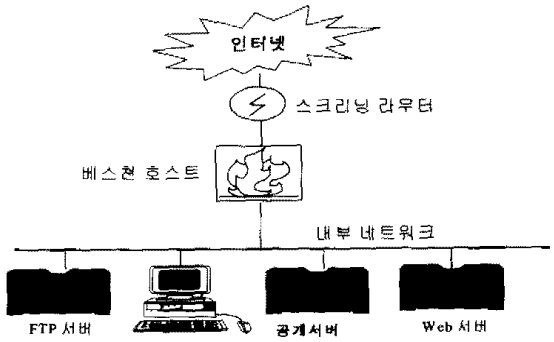



(그림 2) 혼합형 방화벽
(Fig. 2) Hybrid firewall system

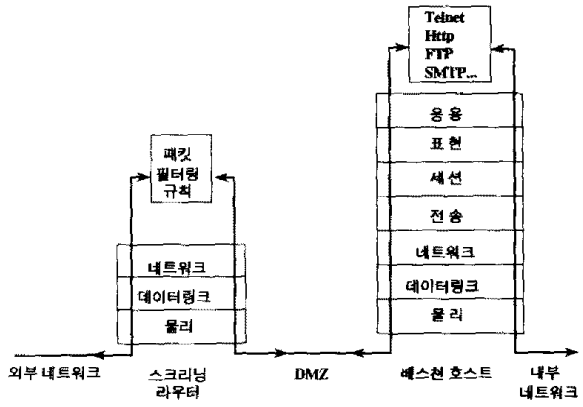
본 논문에서는 (그림 2)와 같이, 스크리닝 라우터, 듀얼-홈드 게이트웨이, 스크린드 호스트 게이웨이, 응용 게이트웨이 서버의 기능을 가진 혼합형 방화벽 시스템으로 설계하였으며, 완충지역인 DMZ에는 내부 또는 외부 사용자가 쉽게 접근할 수 있는 공개 서버들을 설치하였다. 본 논문에서 제안한 혼합형 방화벽 시스템과의 비교 평가를 위하여, (그림 3)처럼 스크리닝 라우터와 베스천 호스트만을 갖춘 방화벽 시스템을 구성하였다.

스크리닝 라우터에서는 "명확하게 금지되지 않는 것은 허용한다"라는 방침에 따라 외부로부터 들어오는 프로토콜중에서 TFTP, Xdma, Ntp를 제외한 모든 패킷을 허용하도록 필터규칙을 적용하였으며, 모든 트래픽이 베스천 호스트로 전달되도록 경로를 설정하였다.

혼합형 방화벽 시스템의 모든 트래픽 경로는 (그림 4)와 같이 스크리닝 라우터와 DMZ, 베스천 호스트를 반드시 거쳐야만 내부 네트워크로 접속이 가능하도록 하였다.




(그림 3) 스크린 라우터와 베스천 호스트로 구성된 방화벽
(Fig. 3) A Firewall with screening router and bastion host

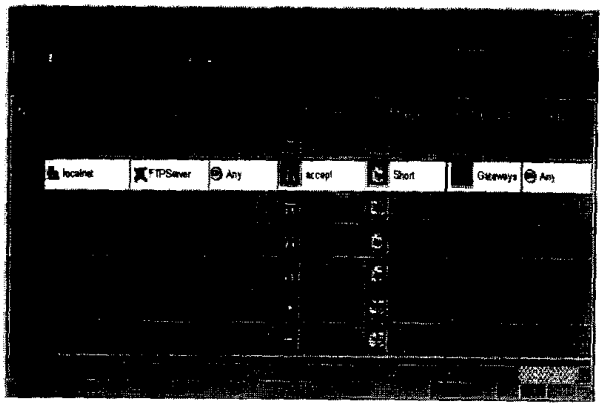



(그림 4) 네트워크 트래픽 경로
(Fig. 4) The path of network traffic

## 4. 실험 및 결과 고찰

### 4.1 실험

본 논문의 구현 모델은 Sun UltraSparc 1 시스템에 방화벽 소프트웨어를 설치하여 약 1개월동안 실시하였으며, 접속기록 자료는 하루 평균 20~30MB 정도가 압축, 누적되었다. 방화벽 시스템은 데이터 링크층과 네트워크층에서 내부적으로 패킷 필터링을 수행하며 라우터의 액세스 리스트를 그대로 수용한다. 로그 분석을 위하여 Log Viewer를 이용하였으며, 텍스트 형태로 변환하였다. 분석 대상은 (그림 3)과 같이 DMZ가 없




(그림 5) 적용된 규칙기반
(Fig. 5) Applied rule base

〈표 3〉 규칙기반
〈Table 3〉 Rule base

| 규칙 번호 | 적 용 내 용 |
|---|---|
| 1 | 게이트웨이에 접속하는 모든 사용자 및 서비스를 금지함 |
| 2 | 내부 네트워크의 모든 호스트가 FTP 서버를 제외한 모든 시스템에 접근을 허용함 |
| 3 | 내부 네트워크의 모든 호스트가 FTP서버의 접근을 허용함 |
| 4 | DMZ에 있는 메일 서버에 모든 호스트를 허용함 |
| 5 | DMZ에 있는 Web 서버에 모든 호스트를 허용함 |
| 6 | 관리자만이 DMZ에 있는 호스트에 Telnet을 허용함 |
| 7 | 그외 모든 트래픽을 금지하고 접근기록을 누적함 |

고 스크리닝 라우터와 베스천 호스트로만 구성된 모델과 (그림 2)와 같은 제안된 방화벽 시스템과의 내부 네트워크에 대한 허용 및 거부현황, 서비스 및 프로토콜별 거부현황과 접속현황 등이다.

실험 및 결과 분석을 수행하기 위하여 사용된 시스템 사양은 다음과 같다.

■ 방화벽 시스템 구축 사양
- SUN Ultra 1 Model 140
- CPU : 143MHz Ultra Sparc 1 processor
- O/S : Solaris 2.5
- Windows System : OpenWindows 3
- Hard Disk : 4GB
- Memory : 128 MB
- Network Interface : 10Mbps Ethernet
- Router : Cisco 7505 (IOS 11.1)

■ 규칙기반 설정

(그림 5)와 같이 외부 사용자에 대해서는 DMZ에 있는 공개 서버들만 사용이 가능하고 내부 사용자에 대해서는 모두 사용이 가능하도록 하였으며, DMZ에 있는 공개 서버들을 관리하기 위하여 관리자만이 Telnet을 할 수 있도록 규칙기반을 설정하였다. 또한 (그림 3)의 모델에서는 DMZ과 관련된 규칙기반을 삭제하였으며, 요청한 서비스를 제공하는 서버로만 접속이 가능하도록 하였다. (그림 5)에 대한 규칙기반에 대한 자세한 설명을 〈표 3〉과 같이 요약하였다.

### 4.2 결과 고찰

두 개의 모델에 대하여 1개월의 실험자료 중 가장 사용빈도가 많은 1주일간의 데이터를 분석 자료로 이용하였다. 구현 모델에서의 내부 네트워크에 대한 각각의 서비스와 프로토콜의 허용 및 거부현황을 분석하였으며, DMZ가 없는 모델과의 내부 네트워크에 대한 허용 및 거부현황을 비교하였다. 접속거부중에서 서비스와 프로토콜에 대하여 각각 현황을 분석하였으며 접속거부가 발생한 원인을 분석하였다. 또한, 외부 네트워크에서 DMZ 및 내부 네트워크로 접속한 서비스 및 프로토콜을 분석하여 보안정책이 타당한지를 알아보았다.

로그 파일은 매일 자동적으로 누적되며 자료를 분석하기 위해서 출력 형태를 (그림 6)과 같이 텍스트로 변환하였으며, 각 필드의 설명은 〈표 4〉와 같다.

```
Num   Date     Time     I/F   Orig          Type Action Service
Src                     Dst                 Proto Rule S_Po User    Info
5202  4Mar97   0:00:00  >le0  wall.kari.re.kr log  accept    96
203.234.255.134  150.197.201.13  4     5    1766  len       116
5203  4Mar97   0:00:00  >le0  wall.kari.re.kr log  accept 32977
203.234.255.134  150.197.201.13  2     5    4866  len       535
5204  4Mar97   0:00:01  >hme0 wall.kari.re.kr log  accept   138
150.197.126.186  255.255.255.255 udp   1    138   len       241
5205  4Mar97   0:00:01  >le0  wall.kari.re.kr log  accept  smtp
205.160.0.101    150.197.148.15  tcp   2    1451  len        44
5206  4Mar97   0:00:02  >le0  wall.kari.re.kr log  accept   140
203.234.255.134  150.197.201.13  4     5    1766  len       160
                 ------------------------
5230  4Mar97   0:00:43  >le0  wall.kari.re.kr log  reject  ident
202.30.143.17    150.197.122.2   tcp   8    5857  len        44
```

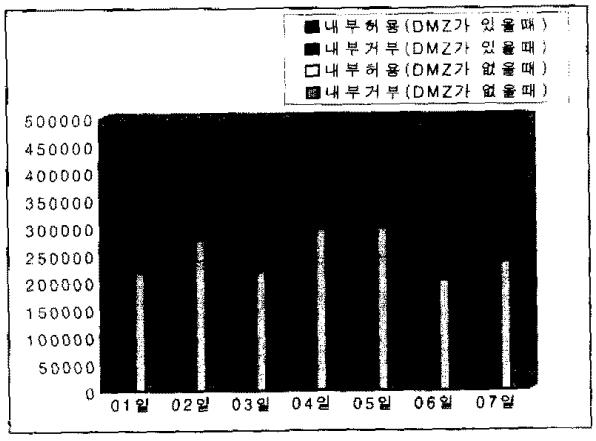
(그림 6) Log 파일
(Fig. 6) Log file

DMZ 있는 제안된 혼합형 방화벽 시스템과 DMZ 없는 비교 시스템에 대한 내부 네트워크의 허용 및 거부 현황은 (그림 7)과 같다. (그림 7)에서, 제안된 시

〈표 4〉 Log 파일 필드
〈Table 4〉 Log file field

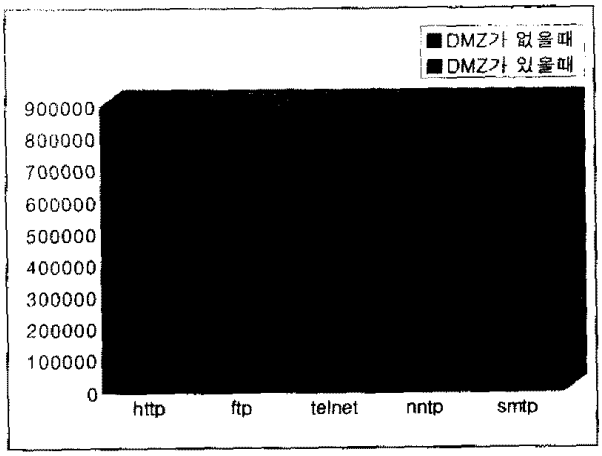
| 필 드 명 | 설 명 |
|---|---|
| Num | 시스템에서 자동적으로 부여되는 로그 엔트리 순서 |
| Date. Time | 이벤트가 발생한 날짜와 시간 |
| I/F | 로그 이벤트가 발생한 하드웨어 인터페이스 |
| Orig | 로그가 기록되는 호스트명 |
| Type | 로그의 형태(long, short) |
| Action | 처리 행위(accept, reject, drop, encrypt, decrypt) |
| Service | 서비스 이름 또는 포트번호 |
| Src | 출발지 호스트 IP 주소 |
| Dst | 목적지 호스트 IP 주소 |
| Proto | 프로토콜명 또는 프로토콜 번호 |
| Rule | 패킷이 적용된 규칙기반 번호 |
| S_Po | 출발지의 포트 번호 |
| User | 사용자명 |
| Info | 기타 추가 정보 |

스템의 내부 네트워크에 있는 서버들에 대한 접속은 상당히 거부되었으나 DMZ이 없는 비교 시스템에서는 내부 네트워크의 허용이 매우 증가하였으며, 많은 트래픽이 내부 네트워크로 유입됨을 알 수 있었다. (그림 7)에서의 혼합형 방화벽 시스템은 위의 〈표 3〉의 규칙기반을 만족하였으며, 내부 네트워크의 보안이 철저히 유지됨으로써 보안성능이 좋은 것으로 나타났다.




(그림 7) 내부 네트워크의 허용 및 거부현황
(Fig. 7) Conditions of permission and denial on inside network

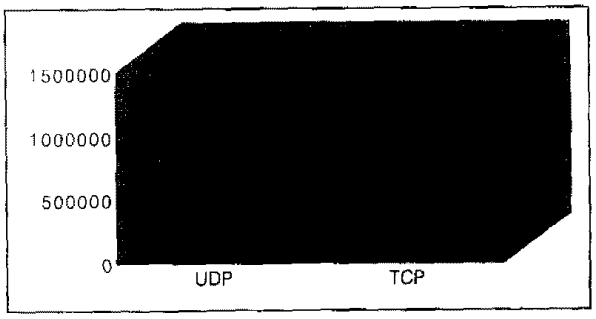
서비스별 거부현황은 (그림 8)과 같이 Web 서버, Ftp, Telnet, 뉴스서버, Mail 서버순으로 나타냈다. 서비스별 거부현황을 보면, DMZ이 있는 경우가 DMZ이 없는 경우보다 서비스별 거부현황이 매우 높게 나타났다. 즉 이것은 호스트에 대한 접속을 적게 허용함으로




(그림 8) 서비스별 거부현황
(Fig. 8) Denial conditions of each services

써 내부 네트워크를 보다 안전하게 유지할 수 있었다.

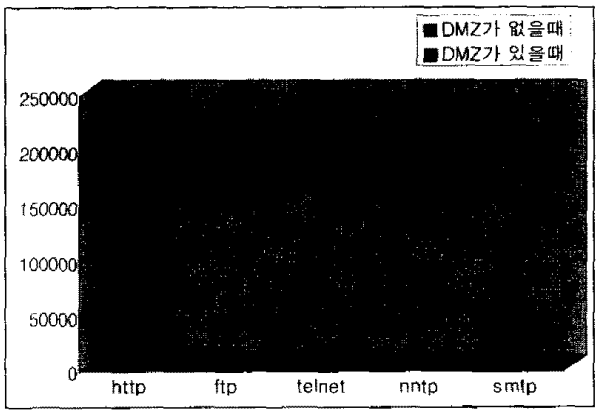
(그림 9)의 프로토콜별 거부현황은 UDP가 TCP보다 많이 나타났다. 이것은 BOOTP와 NETBIOS의 Name Service, Datagram Service를 이용하여 모든 네트워크(255.255.255.255)로 broadcast를 하는 호스트가 많았기 때문이었다. 혼합형 방화벽 시스템에서는 위의 모든 패킷을 거부함으로써 내부 네트워크를 안전하게 보호할 수 있음을 알 수 있었다.




(그림 9) 제안된 시스템에서의 프로토콜별 거부현황
(Fig. 9) Denial conditions of each protocols on proposed system

(그림 10)과 같이 서비스 접속현황을 보면 외부 네트워크에서 들어온 서비스는 Web 서버의 이용이 가장 많았고, 다음으로 SMTP가 많았으나, DMZ이 있을 경우, 내부 네트워크로의 접속이 많이 거부되었으며, DMZ가 없는 경우에는 많은 서비스가 통과되었다. 내부 네트워크의 많은 사용자가 인터넷의 메일링 그룹에 가입하여 메일을 자동으로 수신한 것으로 나타났으며, NNTP는 타 기관의 뉴스 서버로부터 많은 기사가 수신

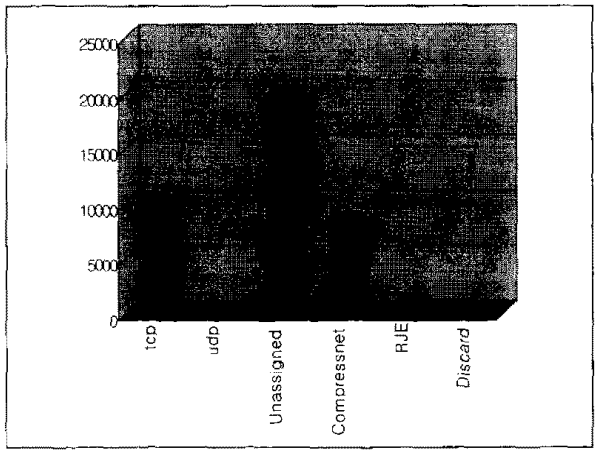
된 것으로 나타났다. 또한 불법 침입을 하기위한 Telnet과 FTP의 접속이 거부되었기 때문에 내부 네트워크에 대한 Telnet과 FTP의 접속이 매우 적어서, 혼합형 방화벽의 보안 성능이 좋은 것으로 나타났다.




(그림 10) 서비스별 접속현황(IN)
(Fig. 10) Connection conditions of each services(IN)

(그림 11)과 같이 프로토콜별 접속현황에서, 빈도 수에 의해 Unassigned가 상대적으로 많이 접속되었다. UDP가 전체적으로 적었으나, 이들 대부분이 BOOTP와 NETBIOS의 사용이었고 접속이 모두 거부되었기 때문에 혼합형 방화벽 시스템의 성능이 좋은 것으로 나타났다. 만약 UDP를 이용하는 DNS의 요청이 많았다면, DNS Spoofing 이용한 침입으로 간주하여 감사추적을 해야만 한다.

본 논문에서 구현된 혼합형 방화벽 시스템은 베스천




(그림 11) 프로토콜별 접속현황(IN)
(Fig. 11) Connection conditions of each protocols(IN)

호스트를 경유하는 모든 트래픽에 대하여 접속기록을 저장하였으며, 어느 사이트에서 연결 요청을 해 왔는가? 사용자가 요청한 서비스는 무엇인지? 언제, 몇 시, 몇 분에 서비스를 요청했는지? 등의 자료를 전산망 감사자료로 활용하였다.

특히, 베스천 호스트에 접속한 사용자의 ID는 무엇인지? 사용자가 시스템에 로그인하여 시스템의 자원을 얼마나 오랫동안 사용하였는지? 등에 대하여 wtmp 로그 화일을 이용하여 감사추적 자료로 사용하였으며, 일반적으로 UNIX에서 Super User가 되기 위해서는 su 명령을 사용하게 되는데, 이때 root의 비밀 번호를 입력하여야 한다. 본 논문의 구현 모델에서는 sudo 라는 프로그램을 이용하여 자신의 비밀번호만으로도 Super User가 될 수 있으므로 Super User의 비밀번호가 노출되지 않도록 하였으며, sudo의 로그 화일을 감사자료로 활용하였다.

## V. 결 론

인터넷을 사용하는 대부분의 기관들이 안고 있는 문제점은 내부 네트워크의 구축 형태에 관계없이 외부 네트워크로부터 투명한 접근을 허용하고 있기 때문에 보안상의 많은 문제점을 내포하고 있는 것이다.

본 논문에서는 네트워크 계층과 전송계층에서 패킷 필터링을 하는 스크리닝 라우터의 단점과 하나의 네트워크 인터페이스로 구축된 스크린드 호스트 게이트웨이의 문제점을 해결해주는 듀얼-홈드 게이트웨이 및 베스천 호스트를 통과하는 응용에 대해 접속기록을 할 수 있는 응용 게이트웨이 서버를 구축하고, 외부 네트워크와 내부 네트워크 사이에 DMZ을 두어 모든 외부로부터의 불법적인 침입을 내부 네트워크로 전송되지 않게 설계하였다. 본 논문에서 제안한 방화벽 시스템의 성능 평가를 위하여 스크리닝 라우터와 베스천 호스트로만 구성된 방법과 비교 분석하였다.

본 논문에서 제안된 DMZ이 있는 혼합형 방화벽 모델에 대하여 외부 사용자에 대해서는 DMZ에 있는 공개서버들만 사용이 가능하도록 하였으며, 내부 사용자에 대해서는 모든 접속이 가능하도록 하였다. 공개서버의 관리를 위하여 관리자만이 Telnet을 허용하도록 규칙기반을 적용하였다. 실험결과 제안된 시스템의 내부 네트워크에 있는 서버들에 대한 접속이 많이 거부되었음이 확인되었다. 그러나 DMZ이 없는 모델에서는 해

당 서비스를 제공하는 서버로 트래픽이 직접 전송되기 때문에, 내부 허용 및 트래픽이 매우 증가하였다. 그러므로, DMZ이 있는 혼합형 방화벽 모델이 내부 네트워크를 보다 안전하게 보호할 수 있는 것으로 입증되었다. 또한 비용 측면에서도 DMZ이 없는 모델보다 라우터와 허브만 추가되므로 혼합형 방화벽 시스템을 설치하는데 큰 영향을 끼치지 않는다.

본 논문의 연구결과는 방화벽 시스템이 구축되지 않았거나 미비한 기관에서 방화벽 시스템을 구축하기 위한 기반연구로 활용될 수 있을 것으로 기대된다. 향후 내부 네트워크를 보다 더 안전하게 보호할 수 있는 새로운 방화벽 모델 및 접속기록에 대한 다양한 분석방법과 감사추적에 관한 연구가 이루어져야 할 것이다.

## 참 고 문 헌


[1] 박응기, 손기욱, 정현철, "전산망 보호를 위한 방화벽 시스템", 주간기술동향, Vol.748, pp.23-40, 전자통신연구소, 1996. 5.

[2] 이재광, 이용준, 박성열, 인터넷 방화벽과 네트워크 보안, 이한출판사, 1996.

[3] John P. Wack, Lisa J. Carnahan, "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls", NIST.

[4] 서동일, 강훈, "인터넷 보안기술 동향분석", 주간기술동향, Vol.779, pp.14-37, 전자통신연구소, 1997. 1.

[5] 정보보호총서, 한국전산원 한국정보보호센터, 1996. 12.

[6] 인터네트 관리자를 위한 보안 지침서, 시스템공학연구소 슈퍼컴퓨터 센터, 1997. 1.

[7] 정보시스템 해킹 현황 및 대응, 한국전산원 한국정보보호센터, 1996. 11.

[8] Marcus J. Ranum, "Internet Firewalls Frequently Asked Questions", Available at http://www.clark.net/pub/mjr/pubs/fwfaq/index.htm

[9] Marcus J. Ranum, "Thinking About Firewalls", Trusted Information System, Inc., 1993

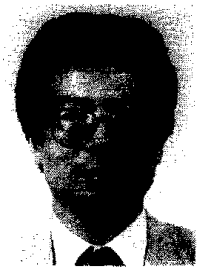
[10] B. Reinhardt, "An Archtectual Overview of UNIX Network Security", 1993. 2., Available at http://www.alw.nih.gov/Security/Docs/network-security.html

[11] Andrew T. Robinson, "Internet Firewalls An Introduction", netMAINE, 1994.

[12] D. Brent Chapman, "Network (In)Security Through IP Packet Filtering, Great Circle Associates.

[13] Marcus J. Ranum, Frederick M. Avolio, "A Toolkit and Methods for Internet Firewalls", Trusted Information System, Inc.

[14] N. Haller, "A One-Time Password System", RFC 1938, 1996. 5.


**이 용 준**

1984년 광운대학교 전자계산학과(학사)

1987년 연세대학교 대학원 전자계산학과(석사)

1993년 정보처리기술사(전자계산조직응용)

1984년 3월~현재 한국전자통신연구원 책임연구원

관심분야 : 데이터베이스 설계, 정보통신 정보보호



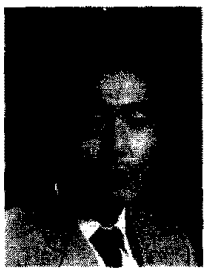
**김 봉 한**

1994년 청주대학교 전자계산학과(학사)

1996년 한남대학교 대학원 컴퓨터공학과(석사)

현재 한남대학교 대학원 컴퓨터공학과 박사과정

관심분야 : 컴퓨터네트워크, 정보통신 정보보호


**박 천 용**

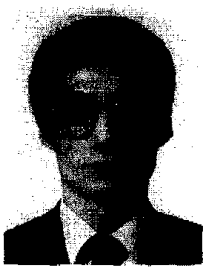
1985년 인하대학교 전자계산학과(학사)

1997년 충북대학교 산업대학원 전기전산공학과(석사)

1986년~1991년 4월 한국과학기술원 기술원

1991년 5월~현재 한국항공우주연구소 선임기술원

관심분야 : 컴퓨터통신, 컴퓨터보안



## 오 창 석

1978년 연세대학교 전자공학과 (학사)
1980년 연세대학교 대학원 전자공학과(석사)
1988년 연세대학교 대학원 전자공학과(박사)
1982년 12월~1984년 9월 전자통신연구소 연구원
1985년 3월~현재 충북대학교 컴퓨터공학과 교수
관심분야 : B-ISDN/ATM, 멀티미디어 통신, Internet 통신

## 이 재 광

1984년 광운대학교 전자계산학과 (학사)
1986년 광운대학교 대학원 전자계산학과(석사)
1993년 광운대학교 대학원 전자계산학과(박사)
1986년 3월~1993년 8월 군산전문대학 전자계산학과 부교수
1993년 8월~현재 한남대학교 컴퓨터공학과 부교수
관심분야 : 컴퓨터 네트워크, 정보통신 정보보호