2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

학교전산망 보호를 위한 스크린드 호스트 게이트웨이 방화벽 구축에 관한 연구

기우서*, 김병철**, 오재철**
*순천대학교 정보과학대학원
**순천대학교 컴퓨터과학과
e-mail:k00165@chollian.net

A Study on the Screened Host Gateway Firewall Construction to Protect the School Network

Woo-Seo Ki*, Byung-Chul Kim**, Jae-Chul Oh**
*Graduate School of Information Science, Sun-Chon University
**Dept of Computer Science, Sun-Chon University

요약

최근 인터넷의 발달로 인하여 보안에 대한 위험이 점차 증가하고 있어 보안에 관한 보다 더 철저한 대응 필요성이 대두되고 있다. 이 연구에서는 패킷 필터링 라우터와 프락시 서버를 결합한 스크린드 호스트 게이트웨이 방화벽을 제안하여 단위 학교전산망에 알맞은 방화벽을 구축하는데 경제적 효과를 기대할 수 있다.

1. 서론

20세기가 기계 문명의 산업 사회라면 21세기는 지식과 정보가 부와 가치 창출의 중심이 되고 삶의 질을 결정하는 정보화 사회가 될 것이다. 이러한 정보화 사회에 절대적 영향력을 확대해갈 것으로 예상되는 것이 인터넷이고, 인터넷의 사용이 급속히 확산되면서 웹을 이용한 기업의 상업적 목적-전자 결재, 광고, 사이버 쇼핑, 게시판-과 연구소 및 학교 등의 교육적 목적으로 활용되고 있다.

인터넷의 활용이 다양한 방면으로 확대되면서 인터넷의 개방된 네트워크 구조와 접근의 용이성으로 인하여 보안에 대한 위험이 점차 증가되고 있으나 이러한 위험에 대한 심각성에 대한 관심도가 낮으며 기술적 대응도 소홀히 되고 있다.

본 연구는 학교전산망이 해커들의 경유지가 되어 가는 것을 방지하고, 해커들의 불법적인 노출, 변조, 파괴로부터 학교의 정보를 보호하며, 학교의 업무처리에 효율화를 기할 수 있는 실질적이면서 경제적인 보안 대책으로 어떠한 보안 정책을 수립하고 이에 따른 효과적인 보안 방법을 확보하는 스크린드 호스트 게이트웨이 방화벽 시스템을 제안하였다.

2. 인터넷 보안

인터넷이 단일 표준 기술을 사용하고 있는 폭넓은 범용성 및 편의성과 자체에 내재되어 있는 보안의 문제로 인하여 전산망 침입자들의 목표가 되고 있다. 정보를 제공하는 기관의 네트워크와 서버는 인터넷과 항상 접속되고 접근이 가능하여야 함으로 이러한 개방성은 보안상의 문제를 야기시킬 잠재적 위협이 되고 있다. [1]

이러한 문제점들을 야기하는 주요 원인을 살펴보면 다음과 같다. [3]

첫째, 인터넷에 연결된 모든 시스템은 모든 사용자에게 공개되어 있으며 접근 가능한 상태이다.

둘째, 프로그램의 버그나 Unix, TCP/IP와 같은 개방된 네트워크 구조를 갖는다.

셋째, 인터넷상에서의 불법 침입에 대한 정보 교환이 쉽게 이루어지고 보안사고의 경위와 피해, 방어 기술 등이 공개되지 않는다.

2.1 보안의 목표

정보를 보호하는데 궁극적인 목표는 기관의 정보 시스템을 효율적으로 관리하여 정보 자산의 신뢰성

을 확보하는 것이라고 할 수 있으며 이를 위해서 다음과 같이 네 가지를 추구한다고 볼 수 있다.

첫째, 정보의 비밀성(Information Confidentiality)으로 정보는 허가된 대상에게만 제공되어야 하고 외부의 다른 세계로부터는 비밀이 유지되어야 한다.

둘째, 정보의 무결성(Information Integrity)으로 정보는 외부의 영향에 의하여 변경되지 않고 진실성 혹은 정확성이 모두 보존되어야 한다.

셋째, 정보의 가용성(information Availability)으로 정보는 허가 받은 사용자에게 필요한 시점에서 사용 가능해야 한다.

넷째, 서비스의 책임추적성(service Accountability)으로 보안 침해의 문제가 발생하였을 때 그러한 침해 사실이 누구에 의해서 어떤 방법으로 발생하였는지 추적 가능해야 한다.

2.2 보안 정책

어떤 기관이든 보안 시스템을 설치하기에 앞서 보안 정책이 수립되어야 한다. 이러한 보안 정책은 학교의 정보 시스템 자원을 어떻게 관리, 보호할 것인가에 대한 지침과 규약을 말하며 다음과 같은 항목을 말할 수 있다.

첫째, 최소의 권한(Least Privilege)으로 기본적으로 어떠한 객체도 자신의 임무를 수행하는데 있어 필요한 최소한의 권한만을 부여한다.

둘째, 겹겹의 방어(Defence in Depth)로 단일한 보안 메커니즘이 실패하면 전체 네트워크의 보안이 훼손을 받으므로 방어 체계를 구축할 때 여러 단계로 두텁게 쌓는다.

셋째, 병목점(Choke Point)으로 전산망 공격자가 좁은 채널을 사용하도록 강제해서 그 채널을 모니터하고 통제할 수 있게 한다.

넷째, 취약부분(Weakest Point)으로 보안에 있어 기본적인 개념으로 가장 약한 부분이 전체의 보안 정도를 나타내며 외부 침입자는 취약점을 발견하고 거기에 공격을 집중한다.

다섯째, 고장허용(Fail-Safe)으로 비상시에도 시스템이 가능한 범위까지는 안전해야 한다는 것이다.

3. 인터넷 보안 도구 방화벽

인터넷에 접속한다는 것은 인터넷에 연결되어 있는 수많은 정보 서버에 접근할 수 있는 가능성을 높여주지만 또 한편으로는 접속 서버 및 네트워크가 외부에 공개되는 보안상의 문제도 있다할 수 있다.

이런 인터넷의 역기능으로부터 학교전산망을 보호하기 위한 도구로 방화벽 시스템이 널리 사용되고 있다. 방화벽을 설치함으로써 시스템 하나 하나를 보안하던 것을 네트워크상의 한 곳에서 네트워크 전체에 대한 보안 정책을 수립하여 관리할 수 있어 모든 트래픽을 감시하고 제어할 수 있다.

3.1 방화벽의 주요 기능

방화벽은 인터넷의 각 서비스별로 요구하는 시스템의 IP 주소, port 번호, 사용자 인증에 기준을 두고 외부 네트워크의 침입을 차단한다. 방화벽은 네트워크 사용자에게 서비스를 제공하면서 서비스 허용 및 실패에 대한 log를 기록한다.

방화벽의 주요 기능을 살펴보면 다음과 같다.

첫째, 외부망과 연동하는 유일한 창구로써 외부망으로부터 사설망 보호

둘째, 서비스 접속 및 거부

셋째, 사용자 인증

넷째, 내부 및 외부의 상호 접속된 네트워크에 대한 트래픽 감시 및 기록

3.2 방화벽의 종류

방화벽은 앞에서 설명한 여러 구성 요소들을 다양한 방식으로 배열함으로써 다양한 상황에 맞는 보안 서비스를 제공할 수 있다. 이러한 배열 방법은 여러 가지 가정할 수 있지만 대체로 OSI 네트워크 계층 모델을 이용하여 방화벽의 적용 유형을 구분하고 있다.

방화벽은 적용 방식에 따라 다음과 같이 3가지로 구분된다.

첫째, 네트워크 수준의 방화벽

둘째, 어플리케이션 수준의 방화벽

셋째, 혼합형 방화벽

3.3 방화벽 구축시 고려 사항

앞에서 설명한 구성 요소를 가지고 실질적으로 방화벽 시스템에서 요구하는 대부분의 기능을 구현할 수 있다. 방화벽 시스템의 가장 중요한 목적인 내부 사설망의 보호라는 관점에서 다음의 고려 사항을 염두에 두고 방화벽의 설계 및 사양을 정하고 설치를 어떻게 할 지를 판단하여야 한다. [3]

첫째, 해당 업체의 조직이 어떻게 시스템을 운영할 것인지에 대한 정책을 반영한다.

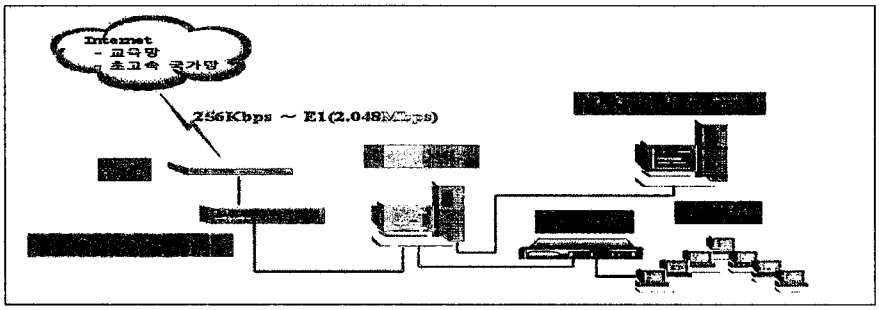
둘째, 어느 정도 수준의 모니터링과 백업 및 제어를 원하는가에 대한 문제이다.

셋째, 방화벽 시스템의 설치 및 구현에 드는 비용과 지속적인 유지 보수에 드는 비용 등이 계산되어야 한다.

4. 학교전산망 보호를 위한 스크린드 호스트 게이트웨이 방화벽 모델 구축

4.1 학교전산망의 구성도

학교전산망은 근거리 통신망이 지원하는 일반적인 기능들을 포함하고 있으며 사용자들이 컴퓨터의 전문가가 아닌 일반인이라는 점을 고려하여 학교전산망의 조작 방법을 배우고 익히는 데에 요구되는 시간 등을 최소화할 수 있도록 설계되어야 한다.



<그림 4-1> 학교전산망 구성도

<그림 4-1>에서 보듯이 학교전산망은 스크리닝 라우터는 모든 트래픽을 필터링할 수 있도록 최전방에 위치하고 방화벽은 학교전산망 관리 서버와 내부 학교전산망 앞에 위치하여 스크리닝 라우터를 통과한 트래픽을 다시 점검할 수 있게 하였다.

4.2 학교전산망의 방화벽 구현

보안 정책에 따라 스크린드 호스트 방화벽에서 패킷 필터링과 Web-Station2 환경 설정의 일부분을 살펴보면 다음과 같다.

1) 패킷 필터링 환경 설정

패킷 필터링 규칙에 의해 스크리닝 라우터의 환경을 설정하자면 아래의 경우와 같이 설정할 수 있는데 해당 패킷을 액세스 리스트 내에 정의해놓은 패킷 필터링 규칙들과 순차적으로 비교/적용한다.

```
ip access-group 11 in
ip access-group 10 out
access-list 10 deny 211.34.*.*
access-list 10 permit any
access-list 11 deny 211.34.*.*
access-list 11 permit any
```

위의 패킷 필터링 환경 설정에서 보면 access-list에서 211.34.*.*에서 나가는 트래픽은 허용하지 않고 나머지 트래픽은 모두 허용한다는 것을 나타내고 있으며 211.34.*.*로 들어오는 트래픽은 거부하고 나머지 호스트로 들어오는 트래픽은 허용한다는 것을 나타내고 있다.

2)Web-station 환경 설정

Web-Station2의 환경을 설정하자면 다음과 같은데 좌측은 프로토콜을 우측은 허가된 IP를 나타내고 있으며 아래는 그 일부로 첨가/삭제가 가능하다.

```
telneta-in.telnetd: permit-hosts 210.183.82.* -exec /usr/sbin/in.telnetd
telneta-in.telnetd: permit-hosts 192.168.* -exec /usr/sbin/in.telnetd
telneta-in.telnetd: permit-hosts 210.112.114.* -exec /usr/sbin/in.telnetd
```

접근을 허가하는 permit-hosts외에 접근을 거부하는 deny-hosts도 추가할 수 있다. -exec...은 접속이 되면 실행할 프로그램이고 /usr/local/etc/...은

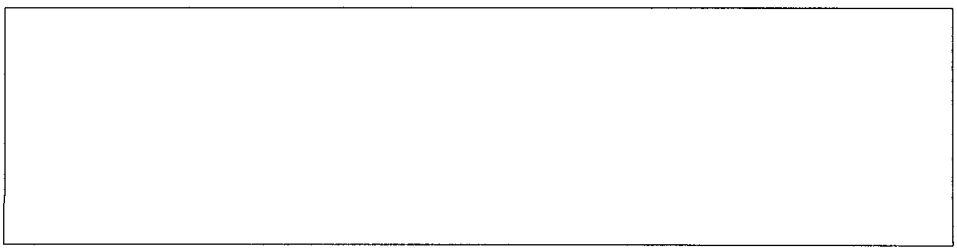


그림 4-2 로그파일

firewall이며 다른 것은 일반 데몬이다.

4.4 결과 고찰

구현 모델은 HP netserver E60 시스템에 Rustle 4501 라우터를 사용하였고 Web-Station 2를 방화벽 소프트웨어로 설치하여 실시하였으며 접속기록의 자료는 log 파일로 저장하였다.

접속 상황을 기록한 로그 파일에는 접속을 시도한 사람의 ID, 프로토콜명, 접속 시도 호스트의 IP 주소, 접속 요일, 월, 날짜와 접속 시간이 기록되어 투명하지 않은 트래픽의 내부 호스트로 접근을 파악할 수 있다.

<그림 4-2>에서 볼 수 있듯이 Web-Station2는 최근에 root 계정으로 telnet과 ftp로 접속한 사용자의 들어온 시간과 정보를 제공하며, 메일 서버로 사용할 경우 클라이언트가 메일을 읽는 시간이나 외부에서 메일이 도착한 정보를 알려준다.

<그림 4-3>에서 볼 수 있듯이 웹스테이션2를 Proxy로 사용하고 있는 모든 클라이언트에 대하여 웹을 사용한 통계를 볼 수 있다.

스크린드 호스트 게이트웨이 방화벽 시스템은 인터넷과 배스천 호스트 사이에 스크리닝 라우터를 접속하고 스크리닝 라우터와 내부망 사이에서 배스천 호스트를 접속한다. 인터넷과 같은 외부 네트워크로부터 내부망으로 들어오는 패킷 트래픽을 스크리닝 라우터에서 패킷 필터링 규칙에 의해 1차로 방어하고 스크리닝 라우터를 통과한 트래픽은 모두 Proxy 서버를 구동하는 배스천 호스트에서 점검하기 때문에 2단계의 방어로 안전하고 융통성이 좋으며 각종 기록 정보를 생성 및 관리하기 쉽고 설치 및 유지보수가 편하며 다른 구축 형태의 방화벽에 비해 경제적인 측면에서 장점이 있다.

V. 결 론

인터넷 기술을 기반으로 한 네트워크를 사용하는 기관들이 안고 있는 문제점은 학교전산망의 구축 형태에 관계없이 신뢰할 수 있는 외부 네트워크로부터 투명한 접근을 허용하고 신뢰할 수 없는 외부 네트워크로부터는 모든 트래픽을 접근 제어하는 보안상의 문제점이라고 할 수 있다.

본 연구에서는 제한된 재정 환경 속에서 보안 문제점들을 상호 보완하여 학교전산망을 보호하기 위한 방화벽으로 스크린드 호스트 게이트웨이 방화벽을 제안하였는데, 네트워크 계층 방화벽 역할을 하는 스크리닝 라우터와 내부 사설망 사이에 어플리케이션 계층의 방화벽 역할을 하는 프락시 서버를 두어 모든 트래픽이 프락시 서버를 거쳐 갈 수 있도록 구현하였다.

앞으로 네트워크를 통한 상거래, 업무 흐름 등을 보다 안전하게 보호할 수 있도록 해야 하나 방화벽이 해킹 수법의 발달과 보안 대상의 변화로 보안에 기여하지 못하므로 방화벽의 개념을 포괄하면서 강력한 인증과 암호 방법을 제공하는 새로운 방화벽의 형태, 접근 기록을 분석할 수 있는 여러 가지 방법 및 신뢰할 수 없는 접근에 대한 감사 추적 방법에 대한 연구가 필요할 것이다.

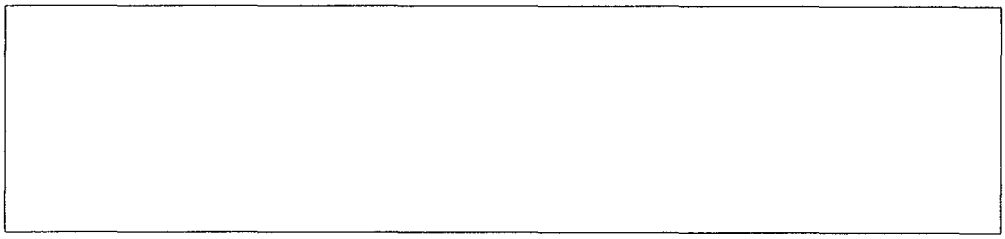


그림 4-3 로그파일분석

참고문헌

[1]. 채규혁 역. "인터넷 방화벽 구축하기". 한빛미디어. 1998.

[2]. 비비컴 역. "그림으로 풀어보는 인트라넷". 비비컴. 1997.

[3]. 홍승필, 고제욱. "정보보안 기술과 구현". 파워북. 1998.

[4]. http://secinf.net/info/howto/firewall-howto.html

[5]. http://secinf.net/info/fw/cisco/add.html

[6]. http://secinf.net/info/nt/fw/firewall.htm

[7]. 박천룡. (1997). 전산망 보호를 위한 혼합형 방화벽 시스템 구현. 충북; 충북대학교 전기전산 공학과 석사학위 논문.

[8]. 신원. (1998). 인트라넷 환경 내에서의 보안 모델에 관한 연구. 부경대학교 전자계산학과 석사학위 논문.