시스템 보안을 위한 프락시 애플리케이션 방화벽 시스템 구축

김선정*, 나현식**
*호남대학교 정보기술원
**호남대학교 정보통신공학부
e-mail: sun103@itc.honam.ac.kr, nahs@mail.honam.ac.kr

Building a Proxy Application Firewall System for System Security

Sun-Jeung Kim*, Hyun-Shik Na**
*Information Technology Center, Honam University
**Dept. of Information and Communication Eng., Honam University

요 약

인터넷이 일반화되면서 컴퓨터 관련 전공자가 아니더라도 시스템을 관리하고 운영하는 경우가 자주 발생하면서 크래커들의 침입에 대응이 늦거나 침입 사실조차 모르는 경우가 있어 시스템 운영에 차질이 발생하고 있다. 또한 방화벽을 설치하더라도 전문 지식이 많지 않아 투자비용에 비교해서 큰 효과를 거두지 못하는 경우도 있다.

본 논문에서는 비용 절감과 방화벽 시스템 운영시 필요한 보안정책과 보안 기술 확보를 위하여 공개 버전인 방화벽 Toolkit을 이용한 프락시 애플리케이션 방화벽 시스템 구축 방법 및 관리 방안을 제시하였다.

1. 서 론

인터넷이 추구하는 정보공유와 개방성은 많은 연구에 비용 절감 효과를 가져오고, 또한 기관의 홍보 매체로서 많은 효율성을 제공하게 되었다. 그러나, 외부로부터의 시스템 침입이 잦아지면서 시스템 운영에 필요한 파일을 변경한다거나 중요한 자료들이 삭제 당하는 일들이 자주 발생하면서 시스템 운영에 차질을 갖게 되었다. 즉, 인터넷이 일반화되면서 시스템의 노출 위험도도 증가하게 되면서 방화벽 같은 보안 솔루션들이 필요하게 되었다.

방화벽(firewall)은 외부로부터 내부 망을 보호하고 외부의 불법 침입으로부터 내부의 정보자산을 보호하기 위한 목적으로 사용되는 네트워크 구성 요소를 의미한다. 따라서 외부로부터 유해정보 유입을 차단하기 위한 정책과 이를 지원하는 하드웨어 및 소프트웨어가 필요하다.

이를 위해 여러 가지 방화벽 중 일반적으로 안전한 방식은 프락시(proxy) 애플리케이션 방식이다. 이는 OSI 7 계층의 애플리케이션 계층에 각 서비스별로 프락시 데몬(Proxy Daemon)이 있게 된다. 각 서비스별 프락시를 이용한 패킷필터링 방식처럼 IP 주소 및 TCP 포트를 이용하여 네트워크 접근제어를 할 수 있으며 클라이언트는 프락시를 통해서만 실제 서버로의 데이터를 주고받을 수 있다.

이에 본 논문에서는 크래커(cracker)들의 불법적인 침입 및 공격으로부터 시스템을 안전하게 보호하기 위하여 공개용 버전인 방화벽 Toolkit을 사용하도록 한다. 상용 방화벽 시스템을 구축하기 전에, 보안 정책 및 보안 기술을 습득할 수 있게 이를 이용한 베스천(bastion) 호스트 기반에 접근 제어 기능과 프락시 애플리케이션 방화벽 시스템 구축 및 관리에 대하여 기술하였다.

2. 방화벽 Toolkit 구성

방화벽 Toolkit은 TIS사에서 무료로 제공하는 방화벽 소프트웨어로 이를 사용자가 필요한 서비스를

선택하고 실행할 수 있도록 해주는 툴들의 묶음이다.

소스는 한국정보보호진흥원(CERTCC-KR) 사이트(http://www.certcc.or.kr)에 접속하여 "기술자료/보안도구" 항목을 통해서 다운로드 받을 수 있다.

TIS Firewall Toolkit
- 구할 수 있는 곳 : TIS Firewall Toolkit
- 요약 : 인터넷 방화벽 구축용 공개 소프트웨어

위에서 다운로드한 TIS Firewall Toolkit 파일(fwtk.tar.Z)을 압축해제하면 다음과 같은 구성파일이 생성된다.

① Makefile : 컴파일 시 make가 참조하는 환경파일
② Makefile.config : Makefile에서 include하는 파일
③ firewall.h : 컴파일 시 읽어들이는 헤더파일
④ auth/ : 인증 서버 관련 디렉토리
⑤ config/ : 시스템 관련 환경설정 디렉토리
⑥ ftp-gw/ : FTP 프락시 서버 관련 디렉토리
⑦ http-gw/ : 웹 프락시 서버 관련 디렉토리
⑧ netacl/ : 접근 제어 프로그램 관련 디렉토리(TCP Wrapper와 흡사)
⑨ tn-gw/ : 원격접속 프락시 서버 관련 디렉토리
⑩ smap/ : SMTP의 최소한의 요구 사항을 구현하는 관련 디렉토리
⑪ smapd/ : 메일 스풀 디렉토리 검사 및 메일 전달 관련 디렉토리
⑫ tools/ : 로깅 및 보고서 생성 관련 디렉토리

이 중 네트워크 서비스에서 가장 많이 사용하는 원격접속 서비스와 FTP 서비스에 대한 프락시 애플리케이션을 구현하여 효율적이고 안정적인 방화벽 시스템을 구축한다. 또한 기능 강화를 위해 외부로부터의 시스템 접근을 제어 차단하기 위해 netacl를 추가한다.

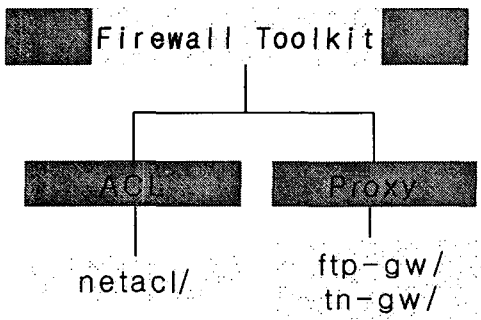

그림 1. 프락시 애플리케이션 방화벽 구조

3. 프락시 애플리케이션 방화벽 시스템 구축

3.1 시스템 환경 설정

Toolkit을 설치할 때는 make 컴파일하기 전에 자신의 시스템에 맞게 Makefile.config를 수정하고 make를 실행한다. 에러 발생 없이 컴파일이 끝나면 원하는 경로에 make install을 한다.

환경 설정에 필요한 파일은 크게 세 가지로 아래와 같다.

(1) /etc/inetd.conf

inetd daemon이 참조하는 환경 파일로 인터넷 관련 서비스 요청이 있을 때는 해당 서비스를 invoke하기 때문에 시스템 자원을 효율적으로 운용할 수 있다.

(2) /etc/services

시스템에서 사용하는 서비스에 대한 프로토콜 및 포트에 대한 정보를 제공한다.

(3) /usr/local/etc/netperm-table

방화벽 Toolkit 구성 요소들을 위한 주 환경 파일이며, 프락시 애플리케이션을 시작할 때에 이 파일로부터 승인 및 거부에 대한 사항을 읽어 들여 제어한다.

방화벽 Toolkit의 내부 동작 원리는 다음과 같다.

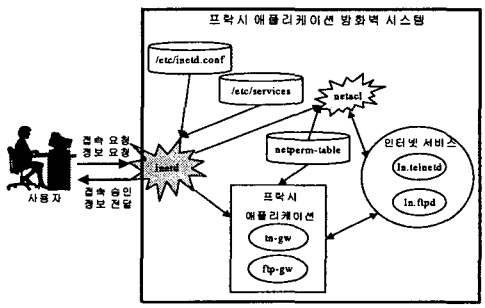

그림 2. 방화벽 Toolkit 내부 동작 원리

3.2 시스템 구축 방법

(1) netacl

netacl은 네트워크 접속 제어 프로그램으로 서버에서 사용 가능한 TCP 기반의 인터넷 서비스에 대한 접근 제어 목록을 제공한다. 따라서, 서버에 접속 시 승인 된 IP 클래스 대역의 사용자만이 원격 접속 및 FTP로의 접속을 할 수 있다.

netacl은 inetd daemon에 의해 관리되므로 inetd를 확인한 후 사용자들의 서비스 요청을 승인하거나 거

부하게 된다.

inetd.conf에서 netacl 서비스 관련 부분은 아래와 같다.

```
telnet stream tcp nowait root /usr/local/etc/netacl
      /usr/sbin/in.telnetd
ftp stream tcp nowait root /usr/local/etc/netacl
      /usr/sbin/in.ftpd
```

원격접속, FTP 서비스에 대한 요청이 있을 때는 netacl이 동작하고 in.telnetd, in.ftpd는 netacl 인수로 전달된다.

netacl은 서비스 요청이 있을 때는 /usr/local/etc/netperm-table의 보안 정책 규칙에 따라 승인 및 거부 사항을 제어한다.

```
netacl-in.telnetd: permit-hosts 211.227.240.* 211.44.64.217
  -exec /usr/sbin/in.telnetd
netacl-in.ftpd: permit-hosts 211.227.240.* 211.44.64.217
  -exec /usr/sbin/in.ftpd
```

여기서 netacl은 특정 클래스 대역과 다른 호스트에 대하여 원격 접속을 승인하도록 하고 있다.

(2) 원격접속 프락시

원격접속 프락시는 방화벽을 통하여 원하는 서버로의 원격접속 서비스에 대한 유일한 경로를 제공하고, 외부에서 내부로의 접속과 내부에서 외부로의 접속을 제어할 수 있다. 또한 원격접속 프락시는 방화벽의 직접 접근을 제공하지 않고, 단지 로그인 경로만을 제공받게 된다.

netacl과 원격접속 프락시를 같이 사용하려면 서비스 포트 번호를 다르게 하여 /etc/services 파일에 지정해 주고 /etc/inetd.conf에 서비스를 추가해 주면 된다.

즉, 일반적인 telnet 23번 포트는 tn-gw가 서비스를 제공하게 하여 외부로부터의 원격접속 서비스 요청이 있을 때는 프락시 방화벽으로 접근을 제어하고, 직접 프락시 방화벽 시스템에 접근을 원할 때는 새로 추가한 2023포트를 이용하여 시스템에 접근한다.

```
# cat /etc/inetd.conf ↵
telnet stream tcp nowait root /usr/local/etc/tn-gw
   tn-gw
telnet-a stream tcp nowait root /usr/local/etc/netacl
   /usr/sbin/in.telnetd
```

```
# cat /etc/services ↵
telnet     23/tcp
telnet-a   2023/tcp
```

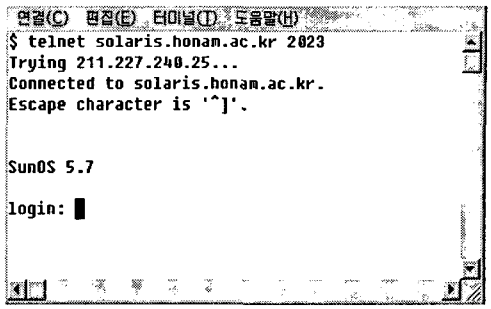

그림 3. 원격접속 프락시 서버로 직접 접근

원격접속 프락시 접근에 대한 보안 정책 규칙은 /usr/local/etc/netperm-table에 정의된 규칙에 의해 결정되어진다.

```
# cat /usr/local/etc/netperm-table ↵
tn-gw: denial-msg /usr/local/etc/tn-deny.txt
tn-gw: welcome-msg /usr/local/etc/tn-welcome.txt
tn-gw: prompt "Input CMD>"
tn-gw: timeout 3600
tn-gw: permit-hosts 211.227.240.* -dest * -passok
   -xok
tn-gw: permit-hosts 211.44.64.* -dest *.honam.ac.kr
   -dest !* -passok -xok
```

위 규칙이 적용되게 되면 211.227.240.* 네트워크로부터의 접근만을 허용하게 되며, 211.44.64.* 네트워크로부터의 접근 요청이 있을 때는 *.honam.ac.kr로의 접속만을 허용하고 이외의 모든 접속 요청은 거부한다.

timeout은 얼마나 오랫동안 telnet 연결을 유휴하는지를 나타낸다.

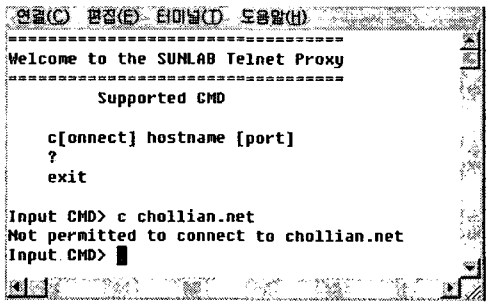

그림 4. 211.44.64.* 에서 요청 시

(3) FTP 프락시

FTP 프락시도 원격접속 프락시와 마찬가지로 /usr/local/etc/netperm-table의 보안 정책 규칙에 따라 접속 승인 및 거부에 대한 제어를 하게 된다.

즉, 일반적인 ftp 21번 포트는 ftp-gw가 서비스를 제공하게 하여 외부로부터의 ftp 서비스 요청이 있을 때는 프락시 방화벽으로 접근을 제어하고, 직접 프락시 방화벽 시스템에 ftp 접근을 원할 때는 새로 추가한 2021포트를 이용하여 시스템에 ftp 접근을 한다.

```
# cat /etc/inetd.conf ↵
ftp stream tcp nowait root /usr/local/etc/ftp-gw ftp-gw
ftp-a stream tcp nowait root /usr/local/etc/netacl
   /usr/sbin/in.ftpd

# cat /etc/services ↵
ftp        21/tcp
ftp-a      2021/tcp

# cat /usr/local/etc/netperm-table ↵
ftp-gw: denial-msg /usr/local/etc/ftp-deny.txt
ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt
ftp-gw: timeout 3600
ftp-gw: deny-hosts unknown
ftp-gw: permit-hosts 211.227.240.* 211.44.64.217 -log
   {retr stor}
```

위와 같이 규칙이 적용되면 도메인을 DNS에서 찾을 수 없을 경우의 시스템 접근은 거부되고, 211.227.240.* 및 211.44.64.217 네트워크로부터의 접근은 허용하게 된다.

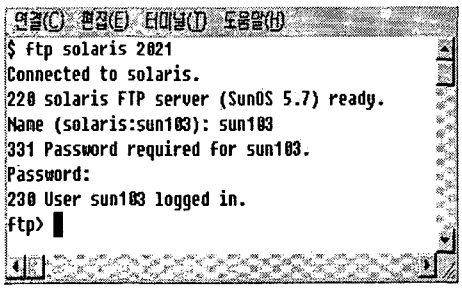

그림 5. FTP 프락시 서버로 직접 접근

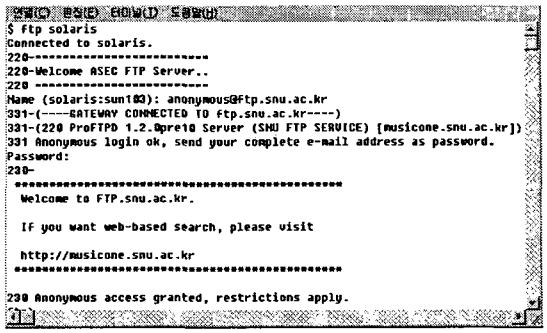

그림 6. 방화벽을 통해서 외부 접근

4. 결 론

본 논문에서 구현한 프락시 애플리케이션 방화벽 시스템은 외부 네트워크와 내부 네트워크의 침입을 OSI 7계층 중 애플리케이션 층을 이용하도록 하였다. 그리고 보다 안전하게 방어할 수 있도록 보안 정책 수립 방법과 시스템 관리 기법을 습득 할 수 있게 시스템을 구축하였다.

특히 비용 절감과 방화벽 시스템을 운영할 때 필요한 보안정책과 보안 기술 확보를 위하여 공개 버전인 방화벽 Toolkit을 이용한 프락시 애플리케이션 방화벽 시스템 구축 방법 및 관리 방안을 제시하였다. 앞으로 이러한 내용을 활용한다면 상용 방화벽 시스템 도입시 비용 절감 대비 많은 효과와 이 분야의 전공이 아닌 관리자들에게 많은 도움이 될 것이다.

참고문헌

[1] PLUS, "Security PLUS for UNIX", 영진닷컴 2000.

[2] D. Brent Chapman & Elizabeth D. Zwicky, "Building Internet Firewalls", O'Reilly & Associates, 1995

[3] 최재철 외, "유닉스 보안 취약성 분석 도구 개발", 정보처리논문지, 제3권 제1호, 1997.

[4] 윤여울 외, "해킹을 대비한 보안 도구 및 추적 방법", 정보처리논문지, 제4권 제1호, 1997.

[5] http://www.certcc.or.kr