通信情報保護學會誌
第7卷 第4號, 1997. 12

TIS Toolkit을 이용한 방화벽 시스템 구축 방법

김 봉 한*, 김 점 구*, 이 명 선**, 이 용 준***, 이 재 광****

요 약

본 논문에서는 해커의 불법적인 공격으로부터 전산망을 안전하게 보호하기 위하여 Trusted Information System에서 발표한 공개 버전인 TIS Firewall Toolkit의 방화벽 시스템 구조와 구성요소를 분석하였고 그리고 구축방법에 대하여 기술하였다. 또한 툴킷에서 제공하는 관리 지원 도구인 port scanner, network subnet ping manager, reporting 도구 등을 분석하였다. 본 논문에서 기술한 TIS 툴킷을 이용한다면, 상용 방화벽 시스템을 구축하기 전에, 보다 쉽게 기관의 보안 정책 개발과 전산망 보호 기술을 확보할 수 있다.

1. 서 론

인터넷은 컴퓨터 통신을 근간으로하는 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 이기종간의 통신이 가능하므로 급속히 발전하였으며, 정보화 사회에 있어서 정보와 통신이 결합되어 움직이는 명실 상부한 "정보화 사회의 기반" 구조가 될것이 확실하다.

* 한남대학교 컴퓨터공학과 박사과정
** 한국과학기술원 부설 연구개발정보센터
*** 한국전자통신연구원
**** 한남대학교 컴퓨터공학과 교수

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. 최근에는 상용 서비스의 확산으로 매우 중요한 데이터들이 인터넷을 통하여 상호 교환되고 있으며, 이를 위한 인트라넷 구축도 활발히 진행되고 있다. 이러한 인터넷상에서 전송되는 중요한 데이터들이 악의적으로 검색, 수정 및 파괴될 경우 그 파급효과는 매우 클것이 확실하다.

이와같이 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 완벽하

게 막아줄 수는 없으나 위험지역을 최소화 하는데 그 목적이 있다. 이러한 방화벽 시스템의 기본 목표는 기관의 네트워크와 외부 인터넷 간의 트래픽에 대해 기관이 갖는 보안 정책에 따라 비인가된 트래픽은 철저하게 막고, 단지 인가된 트래픽만을 허용하는 것이다. 일반적으로 기관의 내, 외부 네트워크간의 트래픽은 IP 데이터그램에 의한 트래픽인 네트워크 레벨 트래픽이며, TCP나 UDP 패킷은 특정 응용 프로세스간의 접속(connection)과 상호 트래픽을 의미한다. 이때 정보의 교환을 위한 접속 정보는 상호 호스트간의 네트워크 주소(IP address)와 상호 응용에 관한 포트 번호(port number)로 이루어진다. 그래서 두 네트워크간의 인터페이스를 갖는 방화벽 시스템은 이 정보를 이용하여 트래픽을 분류하고, 기관에서 필요한 정보보호 서비스를 제공하는 것이다.

최근에 국내에서는 각 기관들이 인터넷/인트라넷 환경 구축을 활발하게 진행하고 있다. 이러한 인터넷/인트라넷 구축, 운용시 정보보호를 위한 보안 시스템으로 방화벽 시스템을 많이 이용하고 있다. 그러나 방화벽 시스템을 구축하는데는 비교적 적지 않은 비용이 들뿐만 아니라 국내에서는 방화벽 구축 기반 기술이나 관련 정보가 빈약한 실정이다.

따라서 본 논문에서는 해커의 불법적인 공격으로부터 전산망을 안전하게 보호하기 위하여 상용 방화벽 시스템을 구축하기 전에, 기관의 보안 정책 개발과 전산망 보호 기술 확보를 위하여 공개 버전인 TIS Firewall Toolkit을 이용한 방화벽 시스템 구축 및 관리에 대하여 기술하였다. 이를 효율적으로 이용한다면 강력한 사용자 인증(user authentication), 로깅(logging), 액세스 제어(access control), 응용 게이트웨이(application gateway), 기밀성(confidentiality) 기능을 갖는 방화벽 시스템을 구축할 수 있을 것이다.

2. TIS 방화벽 툴킷 구조

방화벽이란 건물에 화재가 발생했을 경우, 화재가 더 이상 주변으로 번지지 않도록 모든 가능한 통로를 차단하는 건출물을 말한다. 이러한 의미에서, 컴퓨터 통신망에서는 통신망에서 일어나는 해커들에 의한 불법적인 침입, 중요 정보에 대한 도용, 오용 등과 같은 보안 사고가 더 이상 확대되지 않도록 사용하는 시스템을 방화벽이라 한다. 따라서 기관의 정보 시스템 관리자는 불법적인 침해와 위협으로부터 컴퓨터 시스템과 네트워크를 효과적으로 보호할 수 있어야 한다. 이러한 방화벽은 두 네트워크사이에 위치한 구성 요소들의 집합체로서 다음과 같은 특성을 갖는다.

- 양 방향의 모든 트래픽(traffic)은 방화벽을 통과해야 한다.
- 기관의 보안 정책에 의해 허가된 트래픽만 통과할 수 있다.
- 방화벽 자체는 외부의 불법적인 침투로부터 안전해야한다.

방화벽 툴킷은 Trusted Information System사에 의하여 개발되어, 공개된 방화벽 시스템으로 단일 통합 패키지가 아니라 방화벽 구축에 사용되는 툴의 집합이라 할 수 있다. 이에 대한 전체적인 구조를 이해하기 위해서는 먼저 TIS 툴킷을 컴파일 하는 방법과 구조를 알아야 한다.

2.1 TIS 툴킷 파일 구조

TIS 툴킷을 구축하기 위해서는 먼저 구축하고자 하는 시스템에 화일을 다운로드받아야 한다. 이는 http://www.certcc.or.kr/Tools/tools/firewall/fwtk/에서 fwtk.tar.Z 화일을 다운로드

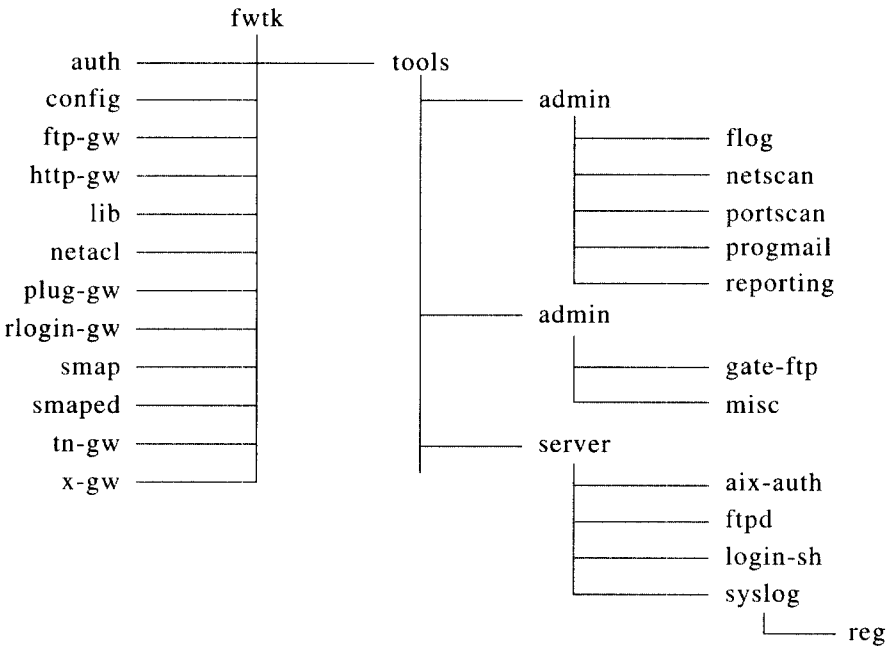


그림 1 TIS 툴킷 디렉토리 구조

받으면 된다. TIS 툴킷은 다운로드받은 후에 압축과 tar 화일을 풀어야 한다. tar 화일을 풀면 그림 1과 같은 디렉토리 구조가 만들어진다.

그리고 이를 컴파일해야 하는데, 그 전에 사이트에 따라 firewall.h와 Makefile.config 파일을 변경해야한다. 이때 고려할 사항은 툴킷의 설치 장소(기본값은 /usr/local/etc), 라이브러리, 컴파일러 구성 방법들이다. 컴파일한 다음에는 각 파일을 적당한 장소에 설치해야 한다. 이를 위한 가장 쉬운 방법은 다음 명령을 이용하면 된다.

```
make install
```

이 명령을 이용하면 각 객체들은 정확한 위치에 구성된다.

2.2 환경 설정 준비

TIS 툴킷을 구성하고자 할 때, 먼저 /etc/inetd.conf 파일을 편집하여 방화벽에 영향을 줄 수 있는 시스템에 구동중인 불필요한 서비스들을 제거하는 것이 좋다. 이는 시스템상의 로드를 줄일뿐만 아니라, 불필요한 포트에 대한 TCP 접속을 허가하지 않기 위해서이다.

불필요한 서비스를 중단시키는 이유는 방화벽을 설치한 시스템의 보안 위협 노출 가능성을 줄이기 위함이다. 또한 방화벽의 초기 설정과 구성을 위해 콘솔을 사용할 수 있다. /etc/inetd.conf 파일을 갱신한 후 기존에 구동중인 inetd 데몬을 제거하여야한다. 이는 다음 명령을 사용하면 된다.

```
kill -1 900 ← 기존에 구동중인 inetd 데몬의 프로세스 번호
```

이젠, inetd 데몬은 실행되지 않는다. 그리고 다음 서비스와 프로세스의 실행이 중단된다.

gated,cgd	pcnfsd	rwhod	mountd	portmap	sendmail	
named	printer	timed	nfsd	rstatd	xntpd	nfsiod

그 다음에 호스트를 네트워크로부터 분리한 후, 다음 단계인 TIS 툴킷 방화벽 구성요소를 구축한다.

2.3 환경설정과 관련된 파일들

TIS 방화벽 툴킷을 설치할 때, 환경 설정에 필요한 파일들을 살펴보면 다음과 같다.

1) netperm-table

/usr/local/etc/netperm-table에서 netperm-table는 Trusted Firewall Tookit(netacl, smap, smapd, ftp-gw, tn-gw, plug-gw) 구성요소들을 위한 마스터 파일이다. 툴킷에서 응용이 시작되면, netperm-table로부터 이에 대한 구성과 허가 정보를 읽어서 in-memory 데이터베이스에 저장한다. 이는 chroot 시스템 호출이 디렉토리 구조를 재구성하더라도 정보를 보존하기 위해 in-memory 데이터 베이스에 정보를 저장한다. 또한 각 proxy는 동작을 시작할 때 이 파일에서 허가/거부 사항을 읽어들인다.

2) /etc/inetd.conf

inetd.conf 파일은 inetd 명령에 대한 정보를 제공하는데 이용한다. 이것은 특정 TCP/IP 포트를 청취하여, 그 포트에 대한 연결을 요구할 때 적절한 명령어를 실행시킨다. 그래서 필요할 때만 데몬을 시작함으로써 시스템 자원을 절약할 수 있다.

3) /etc/services

/etc/services 파일은 호스트에서 사용하는 서비스 목록을 제공한다. 각 서비스에 대하여, 파일에 들어 있는 라인은 서비스 명, 포트 번호, 프로토콜 이름, 별칭과 같은 정보를 제공한다.

3. TIS 툴킷 방화벽 서버 구축

내부망이 외부망과 단절되어 있다면 외부망으로 부터의 위협은 전혀 고려하지 않아도 되나, 사용자는 외부망으로의 접속 서비스를 받을 수 없게 된다. 반대로 내부망과 외부망이 연결되어 있다면, 외부망으로부터의 위협을 감수하여야 한다. 이 두가지 문제를 적절히 해결할 수 있는 해결책은 보안 기능이 제공되는 특정 호스트를 통해서만 외부망에 접속하도록 하며, 외부망에서 내부망으로 접근시에도 특정 호스트를 통해서만 가능하도록 한다. 그러나 이러한 해결책은 사용자에게 투명한 서비스를 제공해주지 못하기 때문에 만족할 만한 해결책이 되지 못한다. 따라서 이러한 투명성을 해결하기 위해서 프럭시 시스템이 사용된다. 프럭시 시스템은 사용자에게 직접 듀얼 홈드 게이트웨이에 접속하도록 하는 대신에 모든 접속을 배후에서 처리해준다. 따라서 듀얼 홈드 게이트웨이와의 접속을 의식하지 않고 외부망 호스트에 접근할 수 있으며, 모든 접속은 프럭시 서버의 보안 기능에 의해 제어되므로 허가되지않은 사용자나 호스트의 접속을 막을 수 있다. 그림 2는 실제 접속과 프럭시에 의해 형성된 접속을 보여주고 있다.

본 논문에서 다루고 있는 TIS 방화벽 툴킷은 네트워크 접근 제어의 기능을 위한 netacl, telnet 서비스를 위한 tn-gw라는 telnet 프럭시, ftp 서비스를 위한 ftp 프럭시, 메일의 올바른 전송을 위하여 사용되는 smap와 smapd로 불

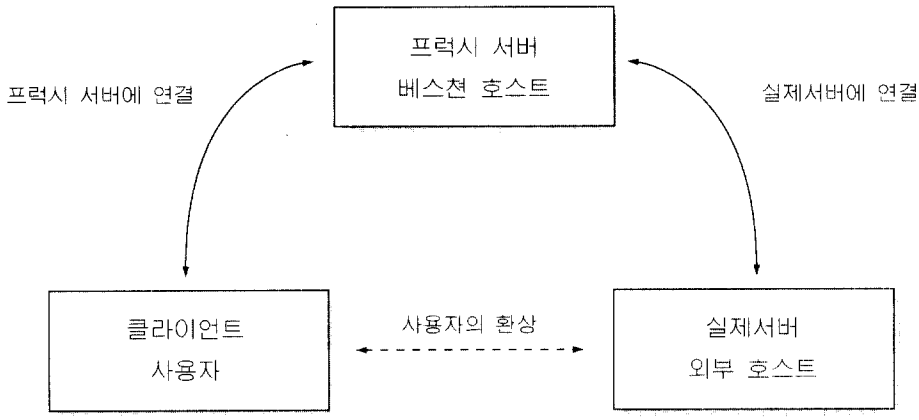


그림 2 프럭시를 통한 접속 방식

리는 2개의 프럭시, http 서비스를 위한 http 프럭시, 실제 서버 자체와 사용자 인증을 위한 인증서버, 그리고 NNTP와 POP 서비스를 위한 plug-gw 프럭시로 구성되어 있다. 위의 서비스를 구축한 후에야 실제로 안전한 전산망을 위한 방화벽 시스템을 구축할 수 있다.

본 장에서는 방화벽 시스템을 위하여 TIS 방화벽 툴킷을 이용하여 구축할 수 있는 서비스를 살펴보고 어떻게 각 서비스의 환경을 설정하고, 구동하는지를 알아본다.

3.1 netacl 구성

netacl은 네트워크 접속 제어 프로그램이다. 이것은 서버에서 사용 가능한 TCP-기반 서비스에 대한 접근 제어 등급을 제공한다. 따라서, 인가된 사용자만이 방화벽에 대한 telnet 접속을 가질 수 있다. netacl 프로그램과 정확한 규칙으로 이 서비스를 설정할 수 있다.

netacl 프로그램은 inetd를 통하여 시작된다. inetd을 점검한 후, netacl는 원격 사용자 시스템의 서비스 요청을 허가하거나 거부한다. netacl을 구성하려면 먼저 inetd.conf 파일을 다음과 같이 수정한다.

```
ftp stream tcp nowait root /usr/local/etc/netacl ftpd
```

이는 ftp 서비스에 대한 연결 요구를 받을 때, netacl 프로그램은 ftpd 인수에 의해 시작된다. inetd.conf 파일을 수정한 후 inetd 데몬을 재구동 한다. ftp 데몬이 수행되기전 netperm-table의 규칙을 이용하여 규칙을 만들어야 한다. netacl에 대한 규칙 이름은 서비스 이름에 따라 "netacl-" 다음에 오는 키워드로 구성된다. 만약 서비스 이름이 ftpd이면 규칙 이름은 다음과 같이 netacl-ftpd로 구성된다.

```
netacl-in.telnetd: permit-hosts 203.247.40.*-
exec /usr/etc/in.telnetd
netacl-in.ftpd: permit-hosts unknown -exec
/bin/cat /usr/local/etc/noftp.txt
netacl-in.ftpd: permit-hosts 203.247.39.* -
exec /usr/etc/in.ftpd
```

위의 예에서 netacl은 특정한 서브넷에 속한 호스트에 대하여 telnet을 허용하도록 구성된다. netacl은 유효한 DNS 이름인 "unknown"을 가지지 않는 시스템으로부터 모든 FTP 연결을 받아들이도록 구성된다. 그리고 접속이 이루어지면 파일을 표시하기 위해 cat

을 사용한다. 이것은 허가받지 못한 사람들에게 허가되지 않았음을 공지하도록 제공한다. 다음은 ftp 서비스가 허가된 호스트에 대한 사용 예이다.

c:\> *ftp adam*
connected to adam.hannam.ac.kr
220 adam.hannam.ac.kr FTP server (Version wu-2.4(1) Fri Jun 13 11:30:22 MST 1997) ready.
User (adam.hannam.ac.kr:(none)): chrish
331 password required for chrish.
Password:
230 User chrish logged in.
ftp>

3.2 Telnet Proxy 구성

telnet 프럭시인 tn-gw는 telnet 서비스를 통하여 제공한다. telnet 프럭시는 netacl 프로그램처럼 방화벽 호스트에 똑같은 형태의 접속을 제공하지는 않는다. telnet과 netacl을 같이 사용하는 목적은 방화벽 호스트에 접속을 안전하게 허용하고 telnet을 통한 로깅 제어를 제공하기 위해서이다. 안전한 telnet 서비스를 제공하기 위하여 먼저 inetd.conf 파일을 다음과 같이 수정한다.

telnet stream tcp nowait root /usr/local/etc/tn-gw tn-gw
telnet-a stream tcp nowait root /usr/local/etc/netacl telnetd

위와 같이 구성하면 전입(incoming) 연결이 telnet port에 수신될때, tn-gw 응용이 시작된다. tn-gw가 요구를 수신했을 때, 이것은 먼저 proxy에 접속을 요구하는 호스트를 허용해도 되는지를 확인한다.

다음으로 /etc/services 파일을 수정한다. 원격 관리 접속을 허용하는 telnet proxy를 설정해야하기 때문에 방화벽 관리자는 기본값보다는 TCP 포트상에서 실제 telnetd가 실행하도록 한다. 그리고 표준 TCP 포트에 proxy를 위치시킨다. 다음과 같이 /etc/services 파일을 편집한다.

telnet 23/tcp
telnet-a 2023/tcp

proxy에 대한 접속은 netperm-table에 명시된 규칙에 의해 결정된다. 이들 규칙은 netacl 응용을 위하여 사용되었던 것들과 유사하다. tn-gw 응용에 관한 초기 구성은 아래와 같다.

tn-gw: denial-msg /usr/local/etc/tn-deny.txt
tn-gw: welcome-msg /usr/local/etc/tn-welcome.txt
tn-gw: help-msg /usr/local/etc/tn-help.txt
tn-gw: timeout 3600
tn-gw: permit-hosts 203.247.39.* -dest *.hannam.ac.kr -dest !* -passok -xok

이 구성은 proxy server에 연결이 될 때나 되지않을 때, 또한 목적지로의 연결이 거절될 때 사용자에게 현 상황을 알려준다. timeout 라인은 방화벽이 이것을 종결하기 전에 얼마나 오랫동안 telnet 연결을 idle 하는지를 가리킨다. 마지막 라인은 tn-gw 응용에 대한 접속 규칙을 설정한다.

환경 설정이 완료되고 허가된 호스트가 proxy에 연결될 때 환영 파일의 내용(tn-gw 옵션내에 구성된)과 프롬프트가 화면에 나타난다.

$ *telnet adam*
welcome to the URG Firewall Telnet Proxy
supported commands are

```
c[onnect] hostname [port]
x-gw
help
exit
Enter Command>c ns.kordic.re.kr
Not permitted to connect to ns.kordic.re.kr
Enter Command>c netwk.hannam.ac.kr
trying 203.247.39.32 port 23...

SunOS Unix (netwk.hannam.ac.kr)
login:
```

위와 같이, tn-gw 응용이 시작되면 telnet 접속시 방화벽이 설치되어 있다는 것을 알 수 있다. 사용자가 첫 번째 ns.kordic.re.kr에 접촉을 시도하면 이것은 거부된다. 두 번째 netwk.hannam.ac.kr로의 연결 요구는 허가된다. 이것은 호스트의 목적지 규칙에 적용된 응답이다.

3.3 rlogin 게이트웨이 구성

rlogin proxy는 rlogin 서비스를 통해 제공되어진다는것을 제외하고는 telnet proxy와 유사하게 서비스를 제공한다. 일반적으로, rlogin을 사용하는 방화벽 접속은 허가하지 않는다. 왜냐하면 많은 문제점이 발생하기 때문이다. 따라서, 방화벽 호스트에 대한 접속은 telnet을 통해서만 허가한다.

3.4 FTP 게이트웨이 구성

FTP proxy는 방화벽을 통하여 사설 네트워크뿐만 아니라 공중 네트워크로의 FTP 트래픽을 허가한다. 방화벽상의 FTP 포트에 연결이 설정되면 FTP proxy가 실행된다. 이러한 연결이 방화벽에 만들어진다면 방화벽 시스템에 기본 포트의 FTP 트래픽을 허가하는 것은 좋지 않다. 이런 경우에는 다른 곳에 추가적인 FTP 서버 시스템을 갖는 것이 더 좋다.

/etc/inetd.conf 파일은 하나의 연결이 생성될 때 서비스 실행에 대한 실제 명세서를 만든다. 그래서 ftp 포트에 연결이 설정될 때 ftp-gw 응용이 시작된다. ftp-a 포트로 연결되면 실제 ftp 서버는 netacl 응용을 통하여 시작된다.

```
ftp stream tcp nowait root /usr/local/etc/ftp-gw
ftp-gw
ftp-a stream tcp  nowait root /usr/local
/etc/netacl ftpd
```

첫 번째 라인은 FTP proxy에 연결을 확립한다. 두 번째 라인은 방화벽 자체에 ftp 연결을 허락한다. ftp-gw proxy는 다른 툴킷 응용처럼, ftp-gw 응용 이름으로 시작하는 netperm-table 파일에서 규칙을 읽는다.

FTP 서비스는 /etc/services 파일에 나타난 것처럼 포트 21에서 시작한다. /etc/services파일에 앞에서 추가된 telnet-a와 유사한 ftp-a라 불리는 두 번째 ftp 엔트리를 추가하여 편집한다. 다른 2021 포트에서 실행하도록 이 ftp-a 서비스를 확립한다. 새로운 /etc/services 파일은 다음과 같다.

```
ftp 21/tcp
ftp-a 2021/tcp
```

ftp-gw 규칙은 다음과 같이 구성할 수 있으며, 호스트 접근 규칙을 통해 사설 네트워크에 접근하는 사용자 또는 내부 사용자들의 연결도 제어 할 수 있다.

```
ftp-gw: deny-hosts unknown
ftp-gw: permit-hosts 203.247.39.*
ftp-gw: denial-msg /usr/local/etc/ftp-deny.txt
```

ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt
ftp-gw: help-msg /usr/local/etc/ftp-help.txt
ftp-gw: timeout 3600
ftp-gw: denydest-msg /usr/local/etc/ftp-badest.txt

proxy를 통해 확립된 연결은 ftp 포트에 연결된 후, 명시된 호스트와 연결하게 된다. ftp-gw의 사용 예는 다음과 같다.

$ *ftp 203.247.37.33*
connected to 203.247.37.33.
220 adam.hannam.ac.kr FTP proxy (Version V1.3) ready.
User (203.247.37.33:(none)) : *anonymous@netwk.hannam.ac.kr*
331 - (- - - - GATEWAY CONNECTED To netwk.hannam.ac.kr - - - -)
331 - (220 net FTP server (Version wu -2.4(!) Fri Jun 13 22:42:18 EDT 1997) ready.)
331 Guest login ok, send your complete e-mail address as password.
password:
230- University Anonymous FTP Server.
230 Guest login ok, access restrictions apply.
ftp>

proxy를 통해 연결을 시도할때에는, 먼저 ftp 명령을 사용하여 방화벽에 연결한다. 연결이 된후 사용자 이름과 연결할 사이트를 명시한다. 허가된 사이트를 확인한 후에, proxy는 원격 시스템의 FTP 서버에 연결하고 적용된 사용자 이름을 이용하여 로그인을 시작한다. 이때에 원격 서버는 이때에 사용자 패스워드를 요구한다. 이것이 정확하면 연결이 허락된다.

3.5 Sendmail Proxy 구성

방화벽을 통한 메일 전송을 위해서 두 가지 응용이 사용되는데, 이는 smap와 smapd이다. smap 대리인(agent)은 SMTP를 구현하는 클라이언트이다. 이것은 smapd에 의해서 네트워크로부터 메시지를 받고 나중에 메시지를 전송하기 위해 메시지를 디스크에 저장한다. smapd 데몬은 samp에 의하여 저장되고 관리되는 메일 스풀 공간을 주기적으로 관리한다. 메일은 sendmail에 의해서 전송되고 전송이 완료되면 스풀 파일은 지워진다. 만약 메일이 정상적으로 전송되지 않으면 smapd을 위하여 스풀된 파일을 특정 공간에 저장한다.

이 두 가지 응용은 몇 가지 동작만 다를뿐 netperm-table 파일내에 같은 구성 정보를 공유한다. smap를 구동하기 위해서는 /etc/inetd.conf 파일에 다음 라인을 추가한다.

smtp stream tcp nowait root /usr/local/tc/smap smap

/etc/inetd.conf가 갱신된 후에, inetd 프로세스는 이전 서비스와 같이 smap 접속을 하기 위하여 다시 시작하여야 한다. smapd는 /etc/rc.local 스크립트로부터 시작되고 시스템이 구동될 때 같이 구동된다. 다음은 rc.local 파일에 추가되는 명령이다.

echo "Starting Firewall Mail processor ..."
/usr/local/etc/smapd

rc.local 파일을 수정한 후 netperm-table을 수정한다. 이 응용의 netperm-table 파일에서, maxbytes의 값은 가장 긴 메시지의 크기를 명시한다. 만약 메시지가 maxbytes 값보다 크면 메시지는 절단된다. 만약 maxbytes가 구성 정보에 포함되어 있지 않으면 메시지의 최대 크

기는 스풀 공간의 크기가 된다. 만약 maxbytes를 너무 작게 설정하면 메시지의 크기 때문에 사용자는 몇 가지 메시지는 받을 수 없게 된다.

```
smap: userid 6
smap: directory /var/spool/smap
smap: timeout 3600
smap: maxbytes 10000
smap: maxrecip 20
smapd: excutable /usr/local/etc/smapd
smapd: sendmail /usr/sbin/sendmail
smapd: baddir /var/spool/smap/bad
smapd: wakeup 900
```

몇 가지 옵션은 smap와 smapd에 공통으로 사용된다. userid와 디렉토리 규칙은 smapd 바이너리 실행의 사용자를 명시하며, 이 구성을 위해서 홈 디렉토리를 이용한다. sendmail 옵션은 sendmail 프로그램이 있는 곳을 명시한다. baddir 값은 저장된 메일 메시지를 전송하는 곳의 디렉토리 이름을 할당한다. 그러면 전송되지 않은 메시지를 저장하도록 하는 bad directory가 생성된다.

smapd에 관한 마지막 값은 큐의 처리에서 얼마나 오랫동안 지연이 되는지를 명시한다. 기본값은 60초이며, 위의 예에서는 15분 짜리 윈도우가 사용된다. 다음은 smap, smapd의 사용 예이다.

```
adam# telnet adam 25
Trying 203.247.37.33 ...
Connected to adam.hannam.ac.kr
Escape character is ' ^] '.
220 adam.hannam.ac.kr SMTP/smap Ready.
helo
250 Charmed, Im sure.
help
214 - Commands
214 - HELO MAIL RCPT DATA RSET
214  NOOP QUIT HELP VRFY EXPN
quit
221 Closing connection
Connection closed by foreign host.
adam#
```

3.6 HTTP proxy의 구성

inetd는 구성파일인 inetd.conf에 다음과 같은 라인을 추가하여야 한다. inetd.conf 파일을 수정한 후, inetd를 다시 시작하도록 지시한다. 이 과정이 완료될 때, http-gw proxy는 구성된다.

```
httpd stream tcp nowait root /usr/local/etc/
http-gw http-gw
gopher stream tcp nowait root  /usr/local/etc/
http-gw http-gw
```

HTTP 또는 고퍼 서버는 각각 TCP/IP의 70과 80포트상에서 실행된다. 따라서 이 포트에 inetd를 구성하고 proxy 대리인(agent)을 시작한다. 또한 /etc/services 파일에 다음 라인을 추가한다.

```
gopher 70/tcp
httpd 80/tcp
```

http proxy에 대한 netperm-table의 수정 사항은 다음과 같다.

```
http-gw: userid www
http-gw: timeout 1800
http-gw: default-httpd www.hannam.ac.kr
http-gw: default-gopher gopher.tc.umn.edu
http-gw: permit-hosts 203.249.39.* -deny ftp
http-gw: deny-hosts unknown
```

permit-host 라인은 proxy를 이용하여 방화벽을 통해 허락되는 호스트와 네트워크를 가리킨다. 특정한 호스트 또한 네트워크에 대한 접속을 거부하고자 할때는 deny-host 라인을 이용한다.

3.7 인증 서버의 구성

TIS firewall Toolkit은 확장된 인증 메커니즘을 가지고 있다. TIS 인증 서버는 두 개의 구성요소로 되어있는데, 이는 서버 자신과 사용자 인증 관리자이다. authsrv라는 인증 서버는 독립적으로 다중 인증 프로세스를 지원하도록 설계되어 있다. 이 서버는 각 사용자를 위한 레코드를 포함한 내부 사용자 데이터베이스를 관리한다. 각 사용자에 대한 정보는 다음과 같이 구성된다.

- 사용자 명
- 사용자 그룹
- 사용자의 full name
- 최근의 성공적인 인증

authsrv는 데몬이 아니다. 이것은 명시된 TCP 포트에 연결요구가 이루어질때만 수행한다. 따라서 다음과 같이 /etc/inetd.conf 파일에 라인을 추가해야한다.

```
authsrv stream tcp nowait root /usr/local
/etc/authsrv authsrv
```

authsrv는 안전한 호스트에서 수행하여야 한다. 이것은 일반적으로 방화벽 시스템이 된다. 인증서버를 구성하는데 사용되지 않는 TCP/IP 포트 번호를 찾아 이것을 /etc/services에 추가해야한다. 예를 들어, TCP 포트로 7777 포트를 사용한다면, 다음의 라인을 etc/services 파일에 추가한다.

```
authsrv 7777/tcp # TIS Toolkit Authentication
```

그리고 netperm-table 파일을 수정한다.

```
authsrv: hosts 127.0.0.1
authsrv: database /usr/local/etc/fw-authdb
authsrv: badsleep 1200
authsrv: nobogus true
authsrv permit-operation user chrish telnet-
gw netwk.hannam.ac.kr time 08:00 17:00
authsrv deny-operation user dasom telnet-gw
ai.hannam.ac.kr time 17:01 07:59
authsrv permit-operation group admin telnet-
gw * time 08:00 17:00
# Use the following lines to use the
authentication server
ftp-gw: authserver localhost 7777
ftp-gw: permit-hosts 203.247.39.* -log { retr
stor } -auth { stor }
```

이것은 서버에 접근이 허락된 로컬 호스트를 가리키고, /usr/local/etc/fw-authdb에 있는 인증 데이터 베이스를 명시한다. 그리고 1,200초가 될때까지 사용자는 5번의 login 실패후에는 인증을 시도할 수 없다. 만약 인증이 실패된다면 인증 실패에 대한 메시지를 출력한다.

사용자가 서버에 의해 인증되기 전에 사용자는 데이터 베이스에 들어있어야 한다. 이것은 authsrv 명령을 이용하면 된다. 시스템 관리자는 root 권한을 이용하여 authsrv를 실행하면 authsrv는 데이터 베이스에 대한 관리 권한을 부여한다. 인증 서버는 표.1과 같은 사용자 관리를 위한 명령을 가지고 있다.

이 관리자 명령의 사용은 데이터베이스에 새로운 사용자를 추가할때 지원한다. 이렇게 설정되면, 방화벽상의 루트처럼 로그인할 수

표.1 인증서버에서의 사용자 관리명령

명 령	설 명
adduser username[longname]	인증 데이터베이스에 사용자를 등록한다.
deluser username	인증 데이터베이스로부터 사용자를 삭제한다.
display username	상태, 인증 프로토콜, 명시된 사용자의 마지막 로그인를 표시한다.
enable username or	
disable username	로그인을 위해 명시된 사용자 계정을 사용하거나 사용하지 않는다.
group user groupname	명시된 사용자의 그룹을 설정한다.
list[group]	시스템에게 알려진 사용자와 명시된 그룹의 멤버들을 나열한다.
password[username]	
text	현 사용자를 위한 패스워드를 설정한다.
proto user protoname	명시된 사용자를 위해 지정된 프로토콜로 인증 프로토콜을 설정한다.
quit or exit	인증 서버로부터 연결을 해제한다.
superwiz user	광역 관리자처럼 명시된 사용자를 설정한다.
wiz user or unwiz user	명시된 사용자에게 그룹 관리자 플래그을 설정하거나 해제한다.
? or help	도움말을 보여준다.

있다. 그리고 authsrv 명령을 실행한다.

다음의 예는 인증 데이터 베이스에 사용자를 등록한 후, 인증 서버를 사용한 예이다.

adam# *ftp adam*
Connected to adam.hannam.ac.kr.
220-Welcome to the URG Firewall FTP Proxy
Name (adam.hannam.ac.kr:chrish): *chrish@netwk.hannam.ac.kr*
331-(----GATEWAY CONNECTED TO netwk .hannam.ac.kr ----)
331-(220 netwk.hannam.ac.kr FTP server (Version A) ready.)
331 Password required for chrish.
Password:
230 User chrish logged in.
Remote system type is Unix. Using binary mode to transfer files.
ftp>*put /tmp/trace*
local: /tmp/trace/ remote: /tmp/trace
200 PORT command successful.
500 command requires user authentication
ftp> *quote authorize chrish*
331 Enter authentication password for chrish
ftp> *quote response whisper*
230 User authenticated to proxy
ftp> *put /tmp/trace*
local: /tmp/trace remote: /tmp/trace
200 PORT command successful.
150 Opening BINARY mode data connection for /tmp/trace.
226 Transfer complete.
2181 bytes sent in 0.0061 seconds (3.5e+02 kbytes/s)
ftp> *quit*
221 Goodbye

3.8 plug-gw를 이용한 다른 서비스들

지금까지의 응용들은 네트워크 트래픽의 약 80%를 담당한다. 그리고 NNTP(Network News Transport Protocol) 또는 POP(Post

Office Protocol)을 지원하는 TIS 툴킷은 plug-gw 응용으로 지원할 수 있다. 이 응용들은 플러그 보드 형태의 연결을 제공한다.

NNTP와 POP 포트로 연결 요구가 있을 때마다 plug-gw 응용을 시작하도록 inetd를 구성한다. /etc/inetd.conf 파일에 다음 라인을 추가하고 inetd를 다시 시작한다.

```
nntp stream tcp nowait root /usr/local/etc/
plug-gw plug-gw 119
pop stream tcp nowait root /usr/local/etc/plug-
gw plug-gw 110
```

/etc/services 파일은 새로운 NNTP, POP 서비스를 추가하도록 편집한다.

```
nntp 119/tcp
pop 110/tcp
```

또한 netperm-table 파일에도 새로운 규칙을 추가한다.

```
plug-gw: port 119 203.247.39.* -plug-to
134.75.30.253
plug-gw: port 110 203.247.39.* -plug-to
203.247.40.31
```

이것은 로컬 LAN의 119 포트와 134.75.30.253에 있는 시스템의 같은 포트가 직접 연결되어 전송됨을 의미한다. 두 번째 라인은 203.247.39.* 네트워크로부터 203.247.40.31로의 연결이 110 포트에서 수신되었음을 나타낸다.

plug-gw를 이용하는 방화벽은 인증을 하지 못한다. 그것은 지정된 포트에서 들어온 연결을 단지 받고, 자신으로부터 같거나 다른 포트의 지정된 시스템으로 연결시키기 때문이다. 다음 동작은 POP포트에 telnet 연결을 보여 주고 있다.

```
$ telnet 203.247.39.32 110
+OK UCB Pop server (version 2. 1. 2-R3) at
203.247.40.31 starting.
USER chrish
+OK Pasword required for chrish.
PASS agdfer
+OK chrish has 0 message(s) (0 octets).
QUIT
Connection closed by foreign host.
$
```

4. TIS 방화벽 툴킷의 관리 지원 도구

TIS 방화벽 툴킷에는 방화벽 호스트를 구축하고 관리하기 위한 지원 도구를 포함하고 있다. 이는 port scanner, network subnet ping manager, log analysis, reporting 으로 구성되어 있다. 이들 도구를 구축하여 효율적으로 사용하면 보다 확실한 방화벽 시스템 수행 상황을 확인할 수 있다.

4.1 Portscan

portscan 프로그램은 시스템의 모든 TCP 포트에 접속을 시도한다. 기본동작은 지정된 호스트의 각 포트에 차례대로 연결을 시도한다. 다음의 예는 호스트 adam.hannam.ac.kr의 각 포트를 검사하는 예이다.

```
adam# ./portscan adam.hannam.ac.kr
ftp
telnet
gopher
httpd
pop
nntp
```

```
who
2021
2023
2120
7777
adam#
```

위의 portscan 출력을 보면 방화벽 시스템으로 사용되는 호스트에서 사용되는 포트가 많지 않음을 알 수 있다. 이와같이 방화벽 시스템으로 사용되는 호스트는 필요치 않은 서비스를 모두 삭제하여 시스템 자체의 보안 수준을 높여야 한다.

4.2 netscan

네트워크를 검사하기 위한 도구로 netscan이 있다. 이것은 네트워크 ping 프로그램이다. 이것은 네트워크 주소를 받아들여 네트워크상의 각 주소에 ping을 시작한다. 이것의 기본 출력은 호스트의 이름과 ping에 대하여 응답한 시스템의 주소 목록이다. netscan의 사용예는 아래와 같다.

```
adam# ./netscan 203.247.39
203.247.39.20
archone.hannam.ac.kr(203.247.39.31)
netwk.hannam.ac.kr(203.247.39.32)
203.247.39.51
203.247.39.52
203.247.39.53
203.247.39.54
203.247.39.55
203.247.39.60
203.247.39.61
^C
adam#
```

이 출력은 ping에 대해서 응답된 첫 번째 호스트가 203.247.39.20임을 보여주고 있다. 주의할 것은 각 주소에 ping을 할때 항상 응답이 있는 것은 아니다. 이것은 장치가 있지 않거나, ping에 대해서 응답하지 않는 장치에 netscan이 접촉을 시도했음을 나타낸다.

4.3 Reporting Tools

TIS 방화벽 툴킷에는 툴킷이 제공하는 응용에 의해 진행된 접속 요구와 처리들에 대한 정보를 기록하고 출력해주는 기능이 있다. TIS 방화벽 툴킷은 각종 프럭시의 로그 메시지 목록과 이에 대한 내용을 알려주는 몇 가지의 리포팅 도구들을 shell script의 형태로 제공하고 있다.

표.2는 각 리포팅 도구들에 대한 설명이다. 리포팅 도구를 사용할 때 주의할점은 이 리포팅 도구들이 툴킷 컴파일시에 자동으로 설치되지 않는다는 점이다. 따라서 tools/admin/reporting 디렉토리로 이동한 후 수동으로 make 명령을 수행하여 /usr/local/etc 디렉토리로 도구들이 복사되도록 하여야 한다.

5. 결 론

최근 국내에서는 각 기관들이 인터넷/인트라넷 환경을 구축하고 운용할때, 정보보호를 위한 보안 시스템으로 방화벽 시스템을 많이 이용하고 있다. 방화벽 시스템의 기본 목표는 기관의 네트워크와 외부 인터넷간의 트래픽에 대해 기관이 갖는 보안 정책에 따른 비인가된 트래픽은 철저하게 막고, 단지 인가된 트래픽만을 허용하는 것이다. 그러나 방화벽 시스템을 구축하는데는 비교적 적지 않은 비용이 들뿐만 아니라 국내에서는 방화벽 구축 기반 기술이나 관련 정보가 빈약한 실정이다.

표.2 리포팅 도구

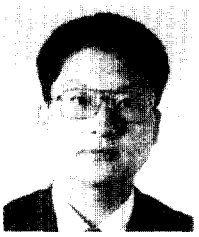
스크립트	설 명
authsrv-summ.sh	인증 서버 리포트를 요약해서 보여준다.
daily-report.sh	하루단위의 리포트 스크립트를 수행한다.
deny-summ.sh	서비스 거부 정보를 보여준다.
ftp-summ.sh	ftp-gw 트래픽을 요약해서 보여준다.
http-summ.sh	http-gw 트래픽을 요약해서 보여준다.
netacl-summ.sh	netacl 접근을 요약해서 보여준다.
smap-summ.sh	smap 전자우편 정보를 요약해서 보여준다.
tn-gw-summ.sh	tn-gw와 rlogin-gw 트래픽을 요약해서 보여준다.
weekly-summ.sh	각종 리포팅 출력을 종합하여 보여준다.

따라서 본 논문에서는 해커의 불법적인 공격으로부터 전산망을 안전하게 보호할 수 있는 방화벽 시스템의 개발, 구축 및 관리와 전산망 서버 보호 기술 설계 및 효율적인 구축 운영을 분석하기 위하여 TIS에서 발표한 공개 버전인 TIS Firewall Toolkit을 이용한 방화벽 시스템의 구축 및 관리 방안과 구축 운영에 대하여 연구하였다. 또한 툴킷에서 제공하는 관리 지원 도구인 port scanner, network subnet ping manager, log analysis, reporting 도구들을 분석하였다. 이 방화벽 툴킷을 효율적으로 이용한다면 전산망을 안전하게 보호할 수 있는 방화벽 시스템 구축과 보안 정책 수립에 많은 도움이 될것으로 사료된다.

참 고 문 헌

1. 임채호, UNIX 시스템 보안가이드, 통신정보보호학회지 1권2호, 1991. 8
2. 한국통신 연구개발단, 한국통신 전산망 보안체계 구축에 관한 연구, 1993.8
3. SERI/ 연구전산망, 관리자를 위한 인터네트 보안 지침서, 1997
4. 한국전산원, "전산망 보안을 위한 위험관리 지침서", 1994
5. 한국정보보호센터, "'96 정보보호 심포지움", 1996
7. 한국정보보호센터, "Firewall 시스템 총서", 1996
8. 한국전산원, "방화벽 시스템의 구축과 운용", 1996
9. D. Brent chapman & Elizabeth D. Zuicky, "Building Internet Firewalls", O' Reilly & Associates, Inc, 1997
10. Robert B. Reinhardt, "An Architectural Overview of UNIX Network Security", Oct.8, 1992
11. William Cheswick & Steven Bellovin, Firewalls and Internet Security, 1994
12. Bill Cheswick, "The Design of a Secure Internet Gateway", AT&T Bell Lab. 1991
13. William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addison-Wesley, 1994
14. John P. Wack, Lisa J. Carahan, "Keeping Your Site Comfortably Secure : Internet Firewall" ,NIST Special Publication 800-10.
15. http://www.certcc.or.kr/Tools/tools.html

□ 著者紹介



김 봉 한

1994년 청주대학교 전자계산학과(학사)
1996년 한남대학교 대학원 컴퓨터공학과(석사)
현재 한남대학교 대학원 컴퓨터공학과 박사과정

※ 주관심 분야 : 컴퓨터네트워크, 정보통신 정보보호

김 점 구

1990년 광운대학교 전자계산학과(학사)
1994년 광운대학교 대학원 전자계산학과(석사)
현재 한남대학교 대학원 컴퓨터공학과 박사과정
1995년 ~ 현재 시사컴퓨토피아 인터넷 사업본부장
1995년 ~ 현재 안양 전문대 전자통신과 외래강사

이 명 선

1982년 아주대학교 공과대학 전자공학과(학사)
1996년 한남대학교 대학원 컴퓨터공학과(석사)
1983년 ~ 현재 한국과학기술원 부설 연구개발정보센터 네트워크 실장

이 용 준

1984년 광운대학교 전자계산학과(학사)
1987년 연세대학교 대학원 전자계산학과(석사)
1993년 정보처리기술사(전자계산응용)
1984년 3월 ~ 현재 한국전자통신연구원 책임연구원

※ 주관심 분야 : 데이터베이스 설계, 정보통신 정보보호

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

※ 주관심 분야 : 컴퓨터 네트워크, 정보통신 정보보호