□ 기술해설 □

TIS-FWTK을 이용한 방화벽 구현

한국전산원 송 익·김남욱·이병만*·송관호**

1. 서 론

오늘날 컴퓨팅 환경의 가장 큰 변화는 인터넷의 일반화라고 보아도 큰 무리가 없을 것이다. 즉, 인터넷에 대한 관심의 증대와 더불어 실제로 인터넷에 연결된 호스트의 숫자가 폭발적으로 증가함에 따라 사용자들은 이를 통해 세계 도처에 산재된 유용한 정보들을 장소와 시간의 제약없이 손쉽게 얻을 수 있게 된 것이다,

그러나 인터넷이 우리에게 반드시 좋은 점들만을 가져다 주는 것은 아니다. 인터넷을 통한 불법 침입으로 인해 내부 정보자산이 파괴되거나 유출되는 사례가 종종 발생하고 있으며, 이러한 침입으로 인한 피해나 손실의 정도 또한 날로 늘어나고 있는 것이다. 방화벽은 이러한 인터넷을 통한 침입으로부터 비교적 적은 비용과 노력으로 내부 네트웍을 보호하기 위한 한 솔루션으로 대두되고 있다.

현재 국내에도 여러 종류의 외국산 방화벽 제품들이 수입, 판매되고 있고 몇몇 뜻있는 국내 업체에 의해서도 방화벽 소프트웨어가 개발되어 판매되고 있으나, 국산 방화벽의 경우에는 개발의 시작 단계이고 기술 또한 부족하며, 외국산 방화벽의 경우에는 아직 충분한 시험과 검증이 이루어지지 않은 상태이므로 실제 사용자들이 방화벽 제품을 선택하고 설치하여 운용하는데 어려움이 많은 것으로 생각된다.

본 고에서는 우선, 독자의 이해를 돕기위해서 방화벽에 대한 개념을 설명하고 TIS사의 방화벽 툴킷을 이용하여 한국전산원에서 구현한 내용을 소개하고, 끝으로 구현된 방화벽의 발전전망을 예측해 본다.

*정 회 원
**종신회원

2. 방화벽 개요

2.1 방화벽이란?

외부로부터 내부망을 보호하기 위한 네트웍 구성요소 중의 하나로써 외부의 불법 침입으로부터 내부의 정보자산을 보호하고 외부로부터 유해정보 유입을 차단하기 위한 정책과 이를 지원하는 H/W 및 S/W를 총칭한다.

2.2 주요기능

방화벽은 외부망과 연동하는 유일한 창구로서 외부로부터 내부망을 보호하기위해 각 서비스(예 : ftp, telnet)별로 서비스를 요구한 시스템의 IP 주소 및 port 번호를 이용하여 외부의 접속을 차단하거나 또는 사용자 인증에 기반을 두고 외부접속을 차단한다. 또한 상호 접속된 내 외부 네트웍에 대한 트래픽을 감시하고 기록한다.

2.3 용어정의

본고에서 사용할 용어에 대해서 먼저 정의한다.

○ Bastion Hosts

베스천호스트는 어떠한 공격에도 철저한 방어기능을 갖는 호스트이다.

○ 프락시(proxy)

프락시는 클라이언트와 실제 서버사이에 존재하여 둘 사이의 프로토콜 및 데이터 relay

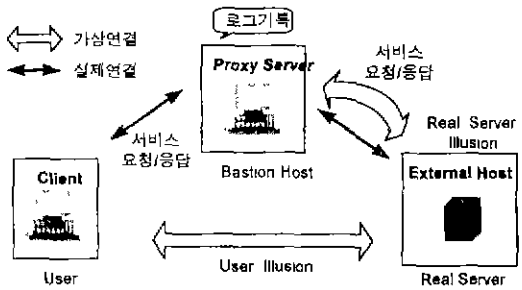


그림 1 프락시 개념도

역할을 한다. 그래서 프락시를 전송자 또는 전달자(forwarder)라고 말하는 사람도 있다.

프락시의 동작과정을 살펴보면 클라이언트가 방화벽으로 접속을 요구할때 방화벽 상의 프락시 서버는 접속허용 규칙을 이용하여 클라이언트의 접속여부를 결정한다. 만약 접속이 거부되면 연결을 끊고 접속이 허용되면 프락시 서버가 실제 서버로 접속을 요구하여 프락시 서버와 실제 서버간의 연결을 맺는다. 또한 프락시는 클라이언트로 접속 요청에 대해 응답을 보내어 클라이언트와 프락시 서버와 연결을 맺는다.

이렇게 연결이 구성되었을 때 프락시는 클라이언트와 서버사이에서 전달자 역할을 하게 된다. 일단 접속이 이루어지면 사용자는 방화벽의 존재를 전혀 의식하지 못하게 되고 실제 서버와 직접 통신하는 것처럼 느끼게 된다.

2.4 구성 요소

○패킷필터링 라우터
○베스천 호스트
  -패킷필터링 게이트웨이
  -어플리케이션 게이트웨이
  -서킷 게이트웨이
  -하이브리드 게이트웨이

본 고에서는 방화벽의 구성요소를 구분하는데 있어서 H/W적인 측면에서 패킷필터링 라우터, 베스천 호스트로 구분하고 이렇게 구분된 방화벽 구성요소에 방화벽 기능측면을 고려하여 세분하였다. 그림 2는 OSI모델에 기준을 두고 각각에 대해 구분한 것이다.

2.4.1 패킷필터링 라우터

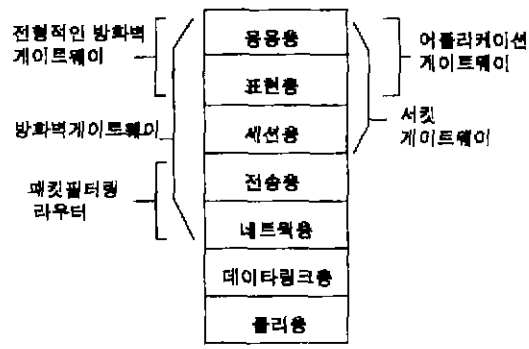


그림 2 OSI 모델에서 방화벽 기능 구분

패킷필터링 라우터 및 패킷 필터링 게이트웨이는 OSI 모델에서 네트웍층(IP 프로토콜)과 전송층(TCP 프로토콜)층에서 패킷 필터링 규칙을 이용하여 패킷 통과여부를 결정하며 통과된 패킷에 대한 경로배정을 한다. 패킷필터링 라우터는 패킷의 출발지 및 목적지 IP 주소 정보, 각 서비스에 port 번호, TCP Sync 비트를 이용한 접속제어를 한다.

1) 장점

이 방화벽의 장점은 방화벽 기능이 OSI 7 모델에서 제 3, 4계층에서 처리되기 때문에 다른 방식에 비해 처리속도가 빠르며, 사용자에게 투명성을 제공한다. 또한 기존에 사용하고 있는 응용 서비스 및 새로운 서비스에 대해서 쉽게 연동할 수 있는 유연성이 있다.

2) 단점

TCP/IP 프로토콜의 구조적인 문제 때문에 TCP/IP 패킷의 헤더는 쉽게 조작 가능하다. 따라서 외부침입자가 이러한 패킷의 정보를 조작한다면 내부시스템과 외부시스템이 직접 연결된다. 또한 ftp, mail에 바이러스가 감염된 파일 전송시 잠재적으로 위험한 데이터에 대한 분석이 불가능하며 접속제어 규칙의 갯수 및 접속제어 규칙 순서에 따라 방화벽에 부하를 많이 줄 수 있다. 또한 다른 방식에 비해서 강력한 로깅 및 사용자 인증 기능을 제공하지 않는다.

2.4.2 베스천 호스트(Bastion Host)

가. 어플리케이션 게이트웨이

어플리케이션 게이트웨이는 OSI 7계층 네트

웍 모델의 어플리케이션 계층에 방화벽 기능이 들어있다. 이 게이트웨이는 각 서비스별로 프락시 데몬이 있어 프락시 게이트웨이 또는 응용게이트웨이라고도 언급한다.

어플리케이션 게이트웨이는 각 서비스별 프락시를 이용하여 패킷필터링 방식처럼 IP 주소 및 TCP port를 이용하여 네트웍 접근제어를 할 수 있으며 추가적으로 사용자 인증 및 파일 전송시 바이러스 검색기능과 같은 기타 부가적인 서비스를 지원한다.

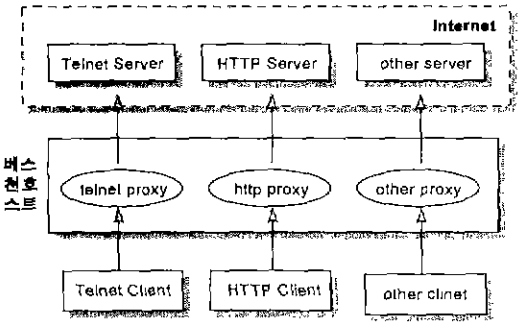


그림 3 어플리케이션 게이트웨이

앞서 언급된 프락시는 클라이언트와 서버사이에 존재하여 그 접속을 관리하며 이미 접속된 연결에 대해서는 데이터 전달을 위한 전달자로서 기능을 한다. 따라서 클라이언트는 프락시를 통해서만 실제 서버로의 데이터를 주고받을 수 있다. 즉, 클라이언트와 실제 서버간에 직접적인 연결을 허용하지 않는다.

1) 장점

○내부 시스템과 외부 시스템간에 방화벽의 프락시를 통해서만 연결이 허용되고 직접 연결(IP Connection)은 허용되지 않기 때문에 외부에 대한 내부망의 완벽한 경계선 방어 및 내부의 IP 주소를 숨길 수 있다. 따라서, 패킷 필터링 기능의 방화벽보다 보안성이 뛰어나다.

○다른 방화벽에 비해서 강력한 로깅 및 감사 기능을 제공한다.

○S/Key, Secure ID 등 일회용 패스워드를 이용한 강력한 인증기능을 제공할 수 있다.

○프락시의 특성인 프로토콜 및 데이터 전달 기능을 이용하여 새로운 기능 추가가 용이하다.

2) 단점

○트래픽이 OSI 7계층에서 처리되기 때문에 다른 방식과 비교해서 방화벽의 성능이 떨어지며, 또한 일부 서비스에 대해서는 사용자에게 투명한 서비스를 제공하기 어렵다.

○방화벽에서 새로운 서비스를 제공하기 위해서 새로운 프락시 데몬이 있어야 한다. 즉 새로운 서비스에 대한 유연성이 없다.

나. Circuit Gateway

서킷 게이트웨이는 OSI 네트웍 모델에서 5계층에서 7계층 사이에 존재하며 어플리케이션 게이트웨이와는 달리 각 서비스별로 프락시가 존재하는 것이 아니고, 어느 어플리케이션도 이용할 수 있는 일반적인 프락시가 존재한다.

방화벽을 통해서 내부 시스템으로 접속하기 위해서는 먼저 클라이언트측에 서킷 프락시를 인식할 수 있는 수정된 클라이언트 프로그램이 필요하다. 따라서 수정된 클라이언트 프로그램이 설치되어있는 클라이언트만 방화벽과 circuit 형성이 가능하다.

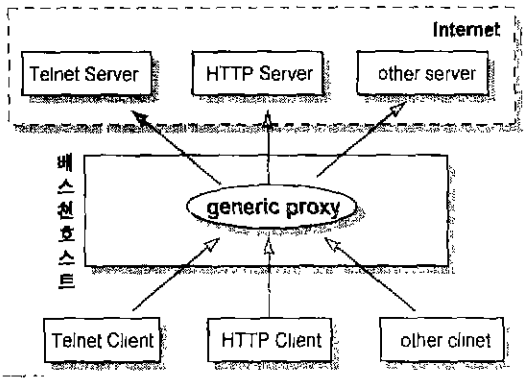


그림 4 서킷 게이트웨이

1) 장점

내부의 IP 주소를 숨길 수 있으며 수정된 클라이언트 프로그램이 설치된 사용자에게 투명한 서비스를 제공할 수 있다.

2) 단점

방화벽에 접속을 위해서 서킷게이트웨이를 인식할 수 있는 수정된 클라이언트 프로그램이 필요하다.

다. Hybrid 방화벽

여러 유형의 방화벽들을 경우에 따라 복합적

으로 구성할 수 있는 방화벽이다. 이 방화벽은 서비스의 종류에 따라서 사용자의 편의성, 보안성 등을 고려하여 방화벽 기능을 선택적으로 부여할 수 있지만 서비스의 종류에 따라서 다양한 보안정책을 부여함으로써 구축 및 관리하는데 어려움이 따를 수 있다.

3. TIS-FWTK을 이용한 방화벽 구현

3.1 TIS-FWTK 소개

앞서 방화벽에 대한 일반적인 내용을 설명하였고 여기서는 방화벽을 구현하는데 있어서 공개소프트웨어로 제공되고있는 미국 TIS사의 FWTK(FireWall ToolKit)의 간단한 소개 및 FWTK을 이용하여 추가로 구현했던 내용들을 설명하고자 한다.

FWTK의 핵심 구성요소는 각 서비스별로 IP주소를 이용한 접근제어를 하기위한 netacl (network access control) 모듈과 각 서비스별 프락시로 구성되어 있으며, 각 프락시는 인증기능이 부여될 수 있어서 인증서버가 존재한다. 이러한 각 서비스 모듈은 서비스를 제공하기 위한 보안 정책을 정의한 netperm-table파일을 참조하여 서비스 제공여부를 결정하고 서비스 접속거부 및 허용에 대한 관련 기록들을 남긴다.

가. netacl(network access control)

netacl은 각 서비스별로 IP주소를 이용하여 외부 시스템의 접근제어를 한다. 이 요소는 주로 방화벽 관리자가 원격에서 방화벽 관리를 하기 위한 요소로 사용되고 있다.

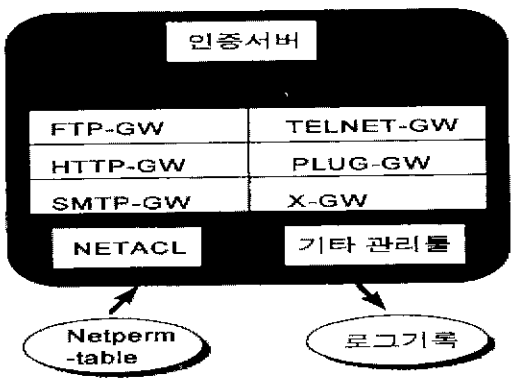


그림 5 TIS-FWTK 구성요소

나. Proxy(전달자)

프락시는 ftp, telnet 및 rlogin, X, WWW 및 gopher 서비스를 위한 프락시와 TCP 기반의 서비스 중에서 사용자에게 투명성 있는 서비스를 제공하기 위한 plug 프락시, sendmail의 보안기능을 강화시킨 smap/smapd가 존재한다.

다. 인증서버

인증기능은 선택기능으로써 각 프락시에서 이 기능을 사용할 수 있다. 지원 가능한 인증방식은 다음과 같다.

- Bellcore's S/KEY
- plaintext 패스워드
- Enigma logics' Silver Card
- Digital Pathways's Secure Net Key
- Security Dynamic's SecurID

라. 기타 tools : 로그관리, 시스템 관리 툴 등

3.2 TIS-FWTK 설치 및 구축

○베스천 호스트를 구축한다.
○소스 패키지를 가져온다.
○자신의 O.S. 환경에 맞게 컴파일한다.
○보안정책에따라 netperm-table을 수정한다.
○서비스제공 관련 파일을 수정한다.
- /etc/inetd.conf
- /etc/services

○접근제어 규칙을 정의한다.
- netperm-table

가. 베스천 호스트를 구축한다.
○필요 없는 모든 서비스를 중지시킨다.
○불필요한 사용자 계정을 모두 삭제한다.
○중요치 않은 파일과 명령은 지운다.
○대용량의 로그를 저장할 수 있도록 한다.
○IP Forwarding기능, Source Routing 기능을 없앤다.
○보안점검 도구를 이용하여 보안취약성을 제거한다.

나. 소스코드를 가져온다.
소스 : ftp : //ftp.tis.com/pub/firewalls/toolkit/~
관련정보 : ftp : //ftp.tis.com/pub/firewalls/~
압축을 풀게되면 기본적으로 "/usr/local/

etc" 디렉토리에 소스코드들이 풀리게 된다.

다. 컴파일

운영체제에 맞는 Makefile.config 파일을 만들고 컴파일 관련 환경변수를 설정하여 컴파일 한다.

```
#cd /usr/local/etc
#cp Makefile.config.solaris Makefile.config
#vi Makefiel.config
#make install
```

라. 서비스 관련 파일을 수정한다.

네트웍 서비스를 총 관장하는 데몬은 Inetd 이고 이 데몬은 inetd.conf 파일에 정의된 서비스를 제공해주기 때문에 inetd.conf 파일을 수정하여 외부에서 어떤 서비스 요청이 있으면 해당 방화벽 서비스를 제공할 수 있도록 만들어 주어야한다. 또한 이러한 서비스들은 /etc/services 파일에 정의되어 있어야 한다.

○다음은 inetd.conf 파일의 ftp 서비스에 대해서 기존 서비스를 중지시키고(comment out) ftp 프록시가 동작될 수 있도록 설정한 예이다.

```
#ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd
ftp stream tcp nowait root /usr/local/etc/ftp-gw ftp-gw
```

○다음은 services 파일의 예이다.

```
ftp-data 20/tcp
ftp 21/tcp
telnet 23/tcp
```

○inetd를 다시 띄운다.

```
%kill-HUP inetd-proccess-number
```

마. 접근제어 규칙을 정의한다.

netperm-table에는 어떠한 네트웍/호스트에 대해서 서비스를 제공할 것인지 아닌지를 결정하기 위한 접근제어 규칙을 정의하게 된다. 이 파일의 위치는 기본적으로 "/usr/local/etc/" 이고 " : "(콜론)의 왼쪽은 서비스 이름을 나타내고 오른쪽은 허용 네트웍 및 관련 정보들을 기술하게 된다. 다음은 1.1.1.1 호스트만 방화벽을 통과하여 ftp 서비스를 받을 수 있도록 접근제어 규칙을 정의한 예를 보여주고 있다.

```
ftp-gw : denial-msg /usr/local/etc/ftp-deny.txt
ftp-gw : timeout 3600
ftp-gw : permit-hosts 1.1.1.1 -log{retr stor}
```

3.3 방화벽 기능 시험

방화벽의 기능을 간단히 시험하는 방법은 같은 이더넷 상에 있는 호스트를 이용하여 그 기능을 점검할 수 있다. 앞서 정의했던 접근제어 규칙을 이용하여 시험할 수 있다. 다른 네트웍 서비스에 대해서도 같이 테스트할 수 있다.

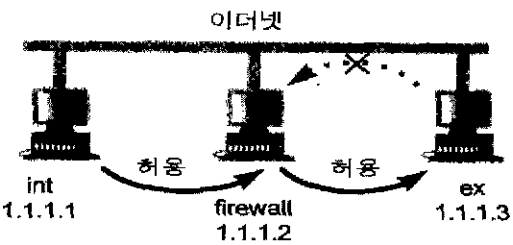


그림 6 기능 시험 구성도

○접속실패

방화벽과 같은 이더넷 상에 있는 호스트 중에서 ex(1.1.1.3) 호스트는 접근제어 규칙에 정의되어 있지 않기 때문에 방화벽으로 접속은 거부될 것이다.

○접속성공

방화벽에서 int 호스트로부터 ftp 접속요구가 있을 때 ftp 서비스를 허용하도록 접근제어 규칙에 정의 하였기 때문에 int 호스트에서 방화벽 시스템으로 접속을 허용하게 될 것이고 방화벽은 ftp 서비스를 제공하기 위한 관련 메시지를 보여준다. 사용자는 방화벽으로 접속을 성공한 후에 실제 서버(ex)로의 접속을 함으로써 원하는 파일을 access할 수 있다. 다음은 ftp 서비스 요청시 접속허용되었을 경우 방화벽에서 클라이언트에게 보여주는 메시지다.

```
[int]% ftp firewall
Connected to firewall
Name (firewall : test) : test@ex
```

접근하고자 하는 시스템의 사용자 ID와 시스템 명을 넣어준다.

```
331-(-GATEWAY CONNECTED TO ex-)
331-(220 ex FTP server (UNIX(r) System V Release 4.0) ready.)
331 Password required for test
```

Password :
230 User test logged in.
ftp>

3.4 추가 개발내용

○FTP를 이용하여 파일전송시
바이러스 검색 및 경보
○vt100 터미널을 이용한 사용자
인터페이스
○불법 침입자에 대한 경보기능
○S/Key를 이용한 일회용 패스워드 기능

3.4.1 FTP 서비스 제공시 바이러스 검색

앞서 설명했듯이 프록시의 특징은 실제 서버와 클라이언트 중간에서 프로토콜 및 데이터 전달기능을 제공하고 있기 때문에 이점에 착안하여 기존 ftp 프록시에 데이터 전달과정에서 파일에 대한 바이러스 검색을 할 수 있도록 기능을 추가하였다. 현재는 압축되지 않은 DOS용 실행파일에 대한 바이러스 검색을 하고 있다.

3.4.2 사용자 인터페이스

TIS-FWTK의 사용자 인터페이스는 모두 텍스트 기반이므로 사용상의 편의성을 제공해 주지 않는다고 볼 수 있다. 이에 반해 대분분의 상용 방화벽 제품들은 각기 나름대로 GUI (Graphic User Interface) 기반의 사용자 인터페이스를 제공하고 있어, 방화벽 시스템 관리자에서 편의성을 제공해 주고 있다. 따라서 TIS Firewall Toolkit을 설치하여 방화벽 시스템을 운용하는 관리자가 사용하기 쉽도록 하기 위해서 GUI를 추가하는 것은 필수적이라고 본다. GUI 기반의 사용자 인터페이스 추가에는 몇 가지 방법이 제시되고 있는데, 먼저 vt100 터미널을 지원하는 문자기반의 인터페이스를 구현하였으며, 현재는 일반 사용자들에게 익숙한 WEB 기반의 인터페이스를 구현하고 있다.

3.4.3 로깅/리포팅/경보

TIS Firewall Toolkit과 같이 프록시를 사용하는 Application/Proxy Gateway 방식의 방화벽 호스트가 갖는 중요한 장점 중의 하나는 방화벽 호스트를 통하는 모든 네트워 트래픽이나 사용자 인증과 관련한 정보를 로깅할 수 있고, 이 로깅 정보를 방화벽 시스템 관리자에게 리포팅 할 수 있다는 것이다.

기존의 리포팅 기능에 추가적으로 파일전송시 바이러스 감염에 대한 리포팅기능과 지정된 횟수 이상 로긴 실패시 관리자에게 알려주는 경보기능을 추가하였다.

3.4.4 일회용 패스워드 S/Key

S/Key는 Bellcore사에서 개발한 일회용 패스워드 시스템의 소프트웨어 패키지이다. 즉, 시스템의 각 패스워드는 인증을 위해 한번만 사용될 뿐 재사용이 불가능하다. 또한 현재의 패스워드가 다음에 사용될 패스워드와 관련된 어떠한 정보도 제공해 주지 못하기 때문에, 네트웍 스니핑(sniffing)으로부터 네트웍을 보호할 수 있다. 참고로 다음 사이트에서 파일을 다운로드 받을수 있다.

ftp : //thumper.bellcore.com/pub/nmh/skey

4. 결론 및 발전방향

본 고에서는 방화벽에 대한 일반적인 개념에 대한 설명과 TIS-FWTK 소개 및 이를 이용하여 한국전산원에서 구현한 내용에 대해서 설명하였다. TIS-FWTK은 공개소프트웨어로써 실제적인 방화벽의 동작원리를 이해하고 싶거나 새로운 방화벽 개발을 하는데 좋은 참조모델이 될 것으로 생각된다. 지금까지 개발된 내용에 추가적으로 개선시켰으면 하는 내용들은 다음과 같다.

○바이러스 검색 기능 강화

방화벽에서도 바이러스 검색을 할 수 있어 네트웍을 통한 바이러스 차단의 가능성을 보여주고 있어서 압출화일에 대한 바이러스 검사, 전자메일을 통한 화일 바이러스 검사 기능 등을 추가한다면 방화벽은 네트웍을 통한 바이러스 차단에 큰 역할을 할 것을 기대된다.

○리포팅 기능 강화

현재 TIS Firewall Toolkit이 갖는 리포팅 기능은 매우 충실하다고 볼 수 있으나, 문자기반의 리포팅 형태를 취하고 있으므로 리포팅된 보고서의 분석이 다소 어려울 수도 있다.

이러한 리포팅 기능을 사용자 인터페이스와 마찬가지로 GUI화하여 방화벽 시스템 관리자에게 보다 쉽고 효율적인 리포팅을 제공하고, 각 서비스에 대한 부하 및 장애를 실시간적으로 모니터링할 수 있는 기능을 추가하는 것이 필요할 것으로 본다.

○저가 장비로의 방화벽 이식

현재는 UNIX 기반의 Workstation 시스템에서 방화벽 설치 및 시험 운영을 하였다. 이러한 시스템은 고가의 장비이기 때문에 다소 저가의 플랫폼(예 : 인텔머신에 Linux 설치)에 방화벽 소프트웨어를 이식할 수 있도록 할 필요성이 있다.

○방화벽에서의 불건전 정보차단

인터넷을 통하여 유용한 정보들을 얻을 수 있는 반면 불건전 정보(예 : 성, 마약, 폭력 등)에 관련된 정보와 불온 정보(예 : 북한 정보)를 부문별하게 접한다는 것은 문제가 될 것으로 본다. 따라서 이에 대한 문제점을 방화벽에 추가 개발하는 것이 필요하다고 본다.

참고문헌

[1] Karanjit Siyan and Chris Hare, "Internet Firewalls and Network Security", NRP, 1995.

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

[3] William R. Cheswick and Steven M.Bellovin, "Firewall and Internet Security". Addision-Wesley, 1994.

[4] 한국통신정보보호학회 논문집, p.185-189, "방화벽에서 바이러스 및 불건전정보 차단에 관한 연구", 1996. 11.

[5] "방화벽 프로토타입 개발 보고서", 한국전산원, 1996. 12.

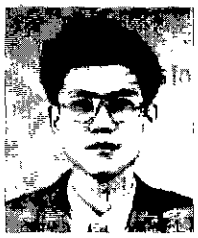
[6] "방화벽 시스템의 구축과 운용", 한국전산원, 1996. 12.

[7] "컴퓨터 바이러스 감염 예방 시스템 개발에 관한 연구", 한국전산원, 1995.

[8] WISC '96 논문집, p.238-249, "SOCKS를 이용한 방화벽시스템 설 계와 GUI 개발".

송 의

1984 전북대학교 정보통신공학과 학사
1995.1~현재 한국전산원 표준본부 보안기술표준팀
관심분야 : 시스템 및 네트워크 보안



김 남 욱

1984 아주대학교 전자공학과 학사
1989 아주대학교 전자공학과 석사
1989.1~1996.5 대우통신(주) 종합연구소 컴퓨터연구부(주전산기 운영체제 개발)
1996.6~현재 한국전산원 표준본부 보안기술표준팀
관심분야 : 시스템 및 네트워크 보안

이 병 만

1982 고려대학교 물리학과(학사)
1982~1985 금성반도체 컴퓨터기술부 사원
1985~1992 대이콤 컴퓨터공학연구실 선임연구원
1992~현재 한국전산원 표준본부 보안기술표준팀장
관심분야 : 컴퓨터 및 네트워크 보안, 정보시스템 위험분석, 시스템 성능평가 등

송 관 호

1979~1985 금성전선연구소 정보시스템 과장
1980 서울대학교 전자공학과 학사
1982 한양대학교 전자공학과 석사
1985~1987 대이콤(주) 미래연구실장
1987~현재 한국전산원 표준본부 본부장
1995.2 광운대학교 전자통신공학과 박사
1996~현재 소프트웨어 산업육성 전문위원, 코리아네트 운영위원장
1997~현재 한국인터넷협회 운영위원장
관심분야 : 초고속통신망, 멀티미디어, 통신프로토콜, 분산시스템 등