학교망을 위한 혼합방화벽 구축 및 접근제어 규칙을 위한 그래픽 인터페이스 구현

박찬정†

요 약

인터넷의 출현으로 많은 교육자들은 인터넷을 교육용 도구로 사용하고 있고, 학교내의 많은 업무가 전산화되면서 인터넷을 활용한 사례가 증가하고 있다. 하지만, 인터넷의 개방성으로 인해 학교망은 외부망에 그대로 노출되어 있기 때문에 교육자료의 파손이나 온라인 성적처리 시 데이터 변경 등의 문제점을 가지고 있다. 외부망으로부터 보호에 대한 요구가 증가하고 있으나, 아직 방화벽을 구축하고 있는 중·고등학교가 전무하며 설치 및 운영 시에도 어려움이 따른다. 본 논문에서는 이와 같은 문제점을 해결하기 위해 학교망을 위한 혼합방화벽을 용이하게 구축·관리할 수 있는 방안을 제시하고, 외부로부터 접근제어를 위해 접근제어 규칙을 용이하게 기술할 수 있고 로그 분석, 실시간 네트워크 트래픽 감시, 날짜별 트래픽 통계 정보 등을 제공하는 그래픽적인 사용자 인터페이스를 구현한다.

Construction of an Hybrid Firewall for School Networks and Implementation of a Graphical Interface for Access Control Rules

Chan-Jung Park†

ABSTRACT

Due to the advantages of Internet, many teachers use Internet as an educational tool and due to the computerized works in schools, the usages of the Internet increase. However, because of the openness of the Internet, the sensitive data of an organization are exposed to outsiders and the Internet-based working has some problems such as the corruptions of instructional data or on-line assessment results. The need for protecting a school network from outsiders increases but the school networks with firewalls rarely exist. In this paper, in order to solve the security problem of a school network, we construct a hybrid firewall for school networks. In addition, we implement a graphical user interface for teachers to set up the access control rules of a hybrid firewall easily. The interface also provides the facilities such as log analysis, a real-time monitor for network traffics, and the statistic on traffics.

1. 서 론

정보화시대에 다양한 정보에 접근하여 필요한 것들을 획득하고 가공함으로써 창의적인 정보를 창출하고 유통할 수 있는 능력이 요구되면서, 교육분야에서도 다양한 정보 활용 기술이나 자기주도적 학습과 같은 수요자 중심의 교육 및 열린교육, 평생 교육 등을 구현할 수 있는 인터넷 활용 교육에 대한 노력이 이루어지고 있다[1][2].

† 정 회 원: 제주대학교 컴퓨터교육과 전임강사
논문접수: 2000년 8월 12일, 심사완료: 2000년 10월 25일

인터넷이 지닌 장점으로 인해 현재 전 세계적으로 많은 교육자들은 인터넷을 교육용 도구로 사용하고 있고, 우리나라에서도 교육정보화 사업의 일환으로 1997년 전국 인터넷 연결 시범 사업을 전개하면서부터 인프라 구축이 본격적으로 이루어지기 시작했다[1]. 우선적으로 학교망을 추진하였으나, 학교망의 도입이 학교 현장에 대한 체계적인 분석없이 이루어짐으로써 다양한 서비스를 원활하게 지원할 수 없어서 현재 학교망 도입과 운영에 대한 방안이 논의되고 있다[3][4].

점차 학교망의 중요성이 부각되고 이용이 증가하면서 학교망을 이용하여 자원의 공유나, 게시판, 웹 등을 이용한 교수-학습용 서비스, 학사관리 활동에 필요한 각종 문서의 작성, 인터넷의 자료 및 검색, 온라인 성적처리 및 데이터베이스화, 수행평가 등을 위한 학사업무용 서비스, 학교 홈페이지의 운용이나 교수-학습 자료의 효율적인 관리, 학생, 학부모, 학교간의 정보교환을 위한 서비스 등이 이루어지고 있다[5].

하지만, 학교망도 인터넷 기술을 이용함에 따라 인터넷이 갖는 장점과 함께 문제점들도 공유한다. 즉, 인터넷은 정보의 보고이기도 하면서 정보를 훼손하고 파손할 수 있는 능력을 제공해 주기도 한다[6]. 인터넷을 통한 불법 침입으로 인해 내부 정보 자산이 파괴되거나 유출되는 사례가 발생하고 있고, 인터넷의 개방성으로 인해 학교망 내부에서도 외부망으로의 접근이 용이하기 때문에 학생들의 불건전사이트로의 접근 가능성이 높아지고 있으며, 온라인 성적 처리 등으로 데이터가 송신되는 중의 기밀 유지 필요성도 높아지고 있다.

따라서, 최근 학교망에서도 방화벽에 대한 요구가 증가하고 있고 학교망에 적합한 방화벽 모델 등에 대한 연구가 진행되고 있다. [6]의 연구에서는 초등학교 인트라넷 구축을 위한 방화벽시스템의 구조를 비용측면과 내부사용자에 대한 가정을 다르게 하여 새로운 모델을 제시하고 있다. 하지만, 통계적으로 내부 사용자에 의한 침해가 더 많이 이루어지고 있으며, 학생들이 외부망으로 접속을 시도할 때 이를 그대로 방치할 수 없다. 또한, [6]이 제시한 모델은 서브넷 형태의 모델을 다소 변형한 것인데 서브넷은 방화벽 구축 모형상 가장 안전하지만 대규모의 조직에 접합하며 비용측면에서 많은 하드웨어를 요구해 다른 모형보다 고가에 속한다고 할 수 있다[7].

본 논문에서는 학교망이 외부망(인터넷)에 노출되어 있기 때문에 발생될 수 있는 문제를 해결하기 위하여 학교망을 위한 혼합방화벽(hybrid firewall)을 저가로 쉽게 구축할 수 있는 방안을 제시하고, 방화벽에서 접근제어를 위한 규칙들을 쉽게 갱신할 수 있는 그래픽 규칙 에디터를 구현한다. 구축할 혼합방화벽은 응용 계층에서 Socks[8]와 네트워크 계층에서 패킷 필터링 기능을 수행하는 Ip_filter[9]를 혼합한 것이며, 이를 위한 인터페이스의 주요 기능으로는 접근제어 및 로그 관리, 실시간 트래픽 감시, 일별 및 주별, 트래픽 통계 처리가 있다.

혼합방화벽은 다른 것에 비해 성능면이나 기능면에서 유리하지만 접근제어 규칙을 기술한 파일 관리의 경우, 혼합방화벽의 특성상 관리자의 부담을 가중시킬 수 있다. 즉, 혼합방화벽은 보안정책을 기술한 규칙기술 언어를 이용하여 트래픽의 흐름을 제어하는데 여러 네트워크 계층을 위한 접근규칙 기술방식들이 서로 상이하기 때문에 관리자에게 어려움을 준다. 구현한 그래픽 인터페이스는 이와 같은 어려움을 해결해 준다.

본 논문의 구성은 다음과 같다. 2장에서는 학교망의 특성과 혼합방화벽의 정의 및 장·단점을 기술한다. 3장에서는 학교망을 위한 혼합방화벽 구축에 대한 내용을 기술하고 4장에서는 접근제어 규칙을 위한 인터페이스에 대한 설계와 구현을 논의한 후 5장에서 결론을 맺는다.

2. 연구 배경

이 장에서는 우선, 학교망의 특성을 기술하고 혼합방화벽의 기능을 제시한다.

2.1 학교망의 특성

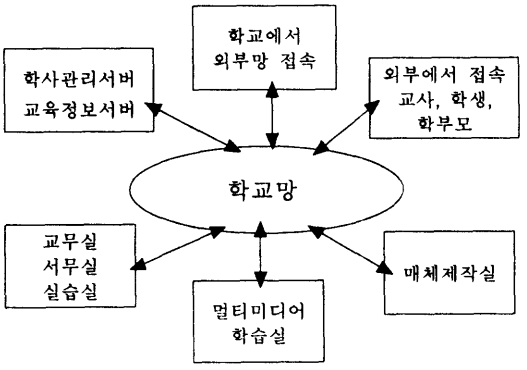
학교망 시스템은 수십 킬로미터 이내의 범위에서 고속의 전송속도를 갖는 매체를 이용한 근거리 통신망의 일종이다. 특히, 사용자들이 컴퓨터 전문가가 아닌 일반 교사나 학생임을 고려하여

학교망 시스템의 조작방법이 용이하도록 설계된 통신망이다[10].

근거리망의 특성에 따라 학교망에서는 분산처리기능, 고속의 전송속도, 자원이용의 효율을 높일 수 있다. 학교망의 효과적인 활용을 위해서는 네트워크 서버의 성능 저하를 최소화할 수 있는 방향으로 교육용 소프트웨어가 개발되어야 하며, 이를 통하여 고속의 전송속도를 이용한 파일의 공유와 화면의 검색 등에 활발히 이용될 수 있을 것이다.

활용측면에서 보면, 학교망은 학습과정에서 교사와 학생간에 이루어지는 의사소통 수단이며, 한정된 컴퓨터와 교육예산의 범위에서 장비활용도를 크게 신장시킬 수 있다. 교육용 소프트웨어를 호출하거나 분배하는 수단으로 활용하고 다수의 학생이 프린터를 공유하는 수단으로도 활용될 수 있다. 컴퓨터 조작 지도나 학생의 학습진행 상황을 원격지에서 확인하는 수단으로도 활용하고 자료를 효과적으로 입력하거나 검색하는 수단으로도 사용한다.

학교망의 특성은 다음 (그림 1)과 같이 나타낼 수 있고, 다음과 같은 기능을 수행한다고 할 수 있다[5].



(그림 1) 학교망 모형

첫째는 교수-학습용 서비스로, 교사들간, 학생들간, 교수-학생간 의견을 채팅이나 전자메일을 통해 상호작용할 수 있게 해준다. 둘째는 학사업무용 서비스로, 학사관리 활동에 필요한 각종 문서의 작성을 비롯하여 학생들의 정보를 입·출력하고 각종 교수자료로 이용할 수 있는 서비스를 제공해야 한다. 셋째는 교육정보서버로, 자료의 효율적인 관리, 교사, 학생, 학부모간의 정보교환, 홈페이지 운영, 응용 소프트웨어 관리를 위한 서비스를 제공해야 한다.

2.2 혼합방화벽

방화벽 시스템은 기관의 보안정책에 따라서 인가된 인터넷 서비스에 대한 접근은 허용하고 인가되지 않은 서비스에 따르는 트래픽을 철저하게 막음으로써 효율적인 보안서비스를 제공하도록 한다[11]. 물론, 방화벽을 구현하는 것이 기관의 보안을 완전하게 보장하지는 않지만 가장 효과적이고 비용이 비교적 적게 드는 방법이라고 할 수 있다.

일반적으로, 방화벽을 구축하는 방식은 크게 두 가지로 나눌 수 있다. 첫째, 전체 네트워크를 보호하여야 할 내부 네트워크와 외부 네트워크로 물리적 구분을 한 후, 라우터(router), 브리지(bridge), 또는 두 개의 네트워크 카드를 가진 개인용 컴퓨터에 패킷 필터링(filtering) 기능을 추가하여 방화벽을 설치하는 방식이다. 둘째, 네트워크를 외부 네트워크와 내부 네트워크로 물리적으로 구분하는 것이 아니라, 소프트웨어만으로 응용 프로그램 게이트웨이를 만든다. 보호받아야 할 내부 네트워크 안에 놓인 모든 호스트들의 응용 프로그램들은 응용 프로그램 게이트웨이 안의 프록시(proxy)만을 통해서 외부 네트워크와 접속하고, 외부 네트워크에서 내부 네트워크로 접속할 경우에도 직접 내부 네트워크에 접속할 수 없고 게이트웨이의 프록시를 통해 접속하는 방식이다[12].

최근, 방화벽을 판매하는 회사들은 위와 같은 두 가지 형태의 방화벽을 통합하여 만든 혼합방화벽을 개발하고 있다. 혼합방화벽은 네트워크 인터페이스 카드간에 패킷을 전달하고 패킷에서 필요한 정보를 얻어내는 역할을 하는 필터(filter) 모듈과 필터 모듈에서 전달해 준 정보와 네트워크 관리자가 만든 규칙을 이용해서 회선의 접속을 허락하거나 감시하는 것을 결정하는 침입차단(firewall) 모듈로 구성되어 있다. 필터 모듈은 라우터와 같은 기능을 수행하기 때문에 혼합방화벽

은 게이트웨이 방식의 방화벽과는 달리 사용자에게 투명성을 보장해 줄 수 있다. 또한, 침입차단 모듈이 네트워크 서비스별로 자세한 접근제어를 할 수 있기 때문에 게이트웨이 방식 방화벽처럼 접근제어와 로그(log) 기록을 수행할 수 있다[13].

혼합방화벽에서는 게이트웨이 방식 방화벽과 마찬가지로 접속을 허가 여부에 대한 결정이 응용계층에서 이루어지고, 실제로 접속이 이루어진 후에는 대부분의 데이터는 응용 프로그램 계층에서 처리되지 않고, 네트워크 계층에서 직접 전송된다. 혼합방화벽의 장점은 대부분의 데이터가 네트워크 계층에서 처리되기 때문에 모든 데이터가 응용 프로그램 계층에서 처리되는 게이트웨이 방식 방화벽에 비해 성능이 뛰어나고 게이트웨이 방식 방화벽처럼 다양한 접근제어가 가능하면서도 사용자에게 투명성을 제공해 줄 수 있다는 것이다[13].

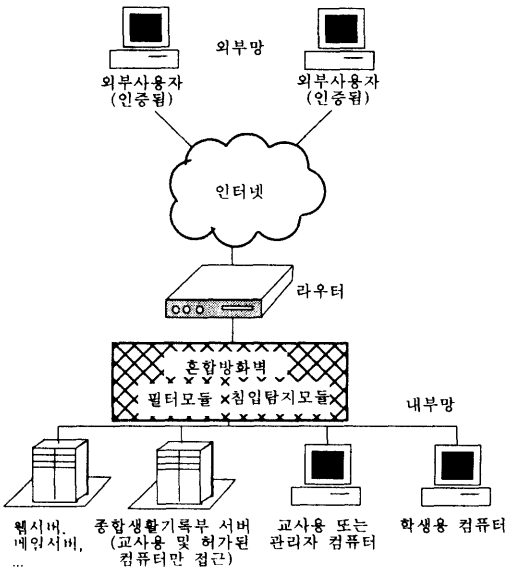
Checkpoint사의 Firewall-1 방화벽[14], Eagle 방화벽[15], Borderware 방화벽[16]은 알려진 혼합방화벽으로, 이들이 제공하는 사용자 인터페이스의 기능들을 살펴보면, 크게 접근제어, 로그 분석 및 관리, 네트워크 상태 감시, 시스템 자원 관리, 사용자 관리 등으로 구분할 수 있다. 이와 더불어 제품들은 각각 고유한 사용자 인터페이스를 제공하고 있다. 하지만, 비용의 측면을 고려해 볼 때, 고가의 제품이라는 문제를 가진다. 반면, 본 논문에서 구현하는 혼합방화벽의 사용자 인터페이스는 다른 방화벽에서 제공하는 기능들을 제공하면서 공개용 방화벽 프로그램들에서 사용하고 있는 서로 다른 접근제어 규칙 기술 방식을 하나의 방식으로 통합한 그래픽 사용자 인터페이스를 제공한다. 즉, 통합된 인터페이스를 제공하므로써 관리자는 하나의 인터페이스로부터 자신들이 원하는 방화벽 프로그램의 접근제어 규칙을 생성하게 되어, 관리를 용이하게 할 수 있고 확장성을 향상시킬 수 있다.

3. 학교망을 위한 혼합방화벽의 구축

이 장에서는 학교망을 위한 혼합방화벽을 구축하는 방안을 제안한다. 다음 (그림 2)처럼 필터모듈과 침입탐지모듈을 장착하고 있는 혼합방화벽을 듀얼-홈드(dual- homed) 방식을 채택하여 구축할 수 있다. 장점은 추가적인 하드웨어를 거의 필요로 하지 않아 경제적인 측면에서 유리하고, 빠른 성능을 보이며 패킷에 대해서 자세히 접근할 수 있기 때문에 응용 게이트웨이처럼 각 서비스에 대한 접근제어가 가능하다.

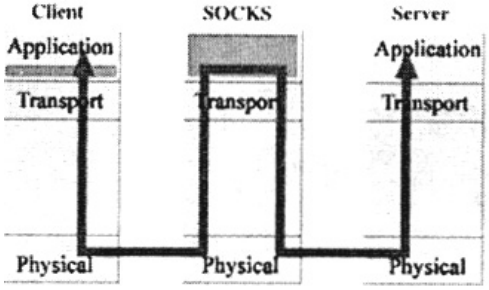
패킷 필터링을 위해서는 Ip_filter[9]를 사용하며 응용 게이트웨이 방식을 위해 Socks v5[8]를 사용한다. Ip_filter는 TCP/IP 패킷 여과기로써 보통 운영체제의 커널 모듈로 적재하므로 사용자가 방화벽을 사용하는지 여부를 느끼지 못하게 하는 투명성을 제공한다. 외부에서 내부로나 내부에서 외부로 응용계층에서 접속이 이루어진 후에는 네트워크 계층에서 직접 데이터를 전송하게 되어 응용 게이트웨이보다 성능을 높일 수 있다.

Socks[8]는 한 개의 포트(port)(1080)로 모든 tcp 프로토콜을 사용하는 응용 프로그램들에게 회선-단계(circuit-level)의 프록시 기능을 제공하는 범용성을 가진 방화벽이다. 즉, Socks는 클라이언트와 서버사이에 통신 채널이 설정되면 TIS사의 FWTK(Firewall Toolkit)[17]과는 다르게 모든 응용에 대한 채널을 보호하고 관리하므로 새로운 응용이 나왔을 때 적응성이 매우 높다.



(그림 2) 학교망에서의 혼합방화벽

Socks 서버와 Socks 클라이언트 라이브러리로 구성되어 있다[8]. 다음 (그림 3)과 같이 Socks 서버는 응용 계층에 위치하는 반면, Socks 클라이언트 라이브러리는 클라이언트의 응용 계층과 전송(transport) 계층 사이에 놓인다.



(그림 3) Socks 방화벽

Socks는 네트워크 내부에서 인터넷 상에 존재하는 특정 서버와 연결을 원할 때 응용 게이트웨이 상에 존재하는 프록시 서버격인 "sockd" 프로그램과 연결을 맺는다. 이 후에 sockd는 내부망의 컴퓨터와 인터넷 상의 특정 서버사이의 데이터를 중계(relay)해주는 역할을 한다. 역의 경우에도 성립하는데 이를 통해 다양한 로그 데이터를 추출할 수 있게 된다. 따라서, 외부망으로부터 내부망으로의 접속 시는 트래픽을 제어하기 위해 Socks를 이용하므로써 보안성을 높일 수 있게 된다.

Socks 4.3의 경우에는 인증기능이 전무하여 추가적인 구현이 요구되었으나 Socks v5는 학교나 연구기관에서 연구의 목적으로 사용가능하고 이 경우에는 자체에서 인증기능을 제공하고 있기 때문에 접근제어 이외에 사용자 인증을 하게 됨으로써 더욱 보안단계를 강화시킬 수 있게 되었다. 두 개의 메시지를 이용한 인증방법 협상 및 두 가지 인증 기능을 제공하는데, 첫 번째 메시지는 클라이언트에 의해 Socks 서버로 보내지며 그 내용은 클라이언트가 지워할 수 있는 인증방법으로 되어 있다. 두 번째 메시지는 Socks 서버가 클라이언트로 보내게 되는데 그 내용은 클라이언트가 사용해야 될 인증방법이 들어 있다. Socks v5는 사용자ID/패스워드 인증[18]과 커버로스(Ker- beros) 5에 입각한 GSS-API[19] 인증 방법을 이용하여 클라이언트를 인증한다.

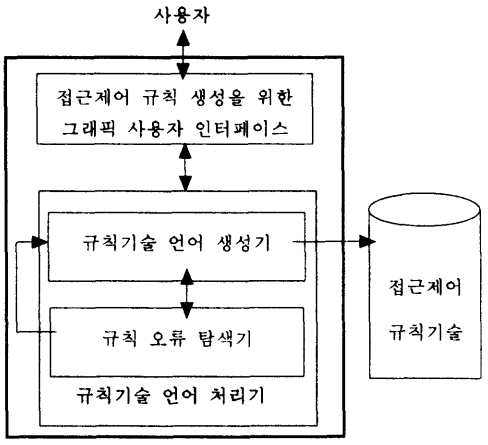
한편, 학교망에서는 중요한 성적 정보등이 망을 통해 전송되는 경우, 무결성을 보장하기 위하여 가상사설망(virtual private network : VPN)기능을 요구한다. 즉, 서로 물리적으로 떨어져 있는 두 개 이상의 사설 TCP/IP 네트워크를 코넷과 같은 개방형 네트워크로 연결한 후, 이들 사설 네트워크들 간에 오가는 데이터를 암호화 및 복호화하여 서로 전달함으로써 마치 전용선으로 구축된 사설 학교망에서 통신하는 것과 같은 안전성을 제공한다. Socks v5는 외부망과 학교망간의 익스트라넷(extranet)을 위한 보안 솔루션을 제공하는 암호화 기법(DES, 3DES, RC4)을 지원한다. 즉, 메시지 무결성과 기밀성을 GSS-API를 이용하여 제공할 수 있다.

4. 접근제어 규칙을 위한 그래픽 사용자 인터페이스 설계 및 구현

이 장에서는 3장에서 기술한 혼합방화벽을 위한 그래픽 사용자 인터페이스와 인터페이스에서 제공하는 기능들을 차례대로 기술한 후, 그래픽 인터페이스를 설계하고 기능별로 구현 내용을 기술한다.

제공하는 기능에는 접근제어 규칙 관리 및 가상 사설망(VPN) 기능, 네트워크 주소 변환(network address translation : NAT) 기능, 실시간 트래픽 감시 기능, 로그 관리 및 통계 처리 기능이 있다. NAT 기능은 실제 할당된 주소보다 더 많은 호스트를 연결할 수 있게 해주고 내부주소를 감춤으로써 보안성을 높인다. NAT는 정적모드와 동적모드로 나눌 수 있는데, 정적방식은 정해진 규칙에 의해 내부주소와 외부주소를 매핑하고 동적방식은 그때 그때마다 다른 매핑이 사용되어진다. 보통 내부 네트워크 주소는 비공인 IP 주소를 사용한다.

그래픽 사용자 인터페이스는 다음 (그림 4)와 같은 구조도를 가지며 전체 메뉴 구성은 <표 1>과 같다. 본 프로그램은 Tcl/Tk[20]를 이용하여 구현하였으며, 현재 Tcl/Tk를 이용한 CGI 프로그램으로 갱신 중에 있다.



(그림 4) 그래픽 사용자 인터페이스 구조도

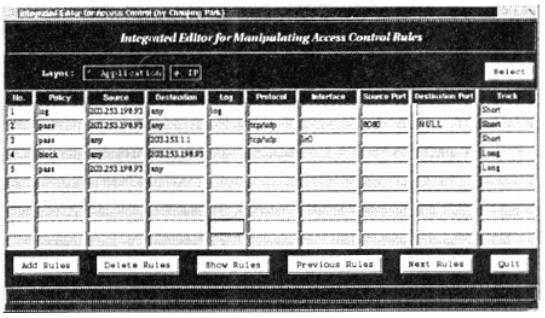
<표 1> 그래픽 인터페이스 메뉴 구조

주메뉴	서브메뉴
파일메뉴	◎ 파일관리메뉴 : 접근제어규칙 파일 관리, 가상사설망 규칙 파일, 로그파일, 네트워크 주소 변환 파일, 라우팅 파일 ◎ 방화벽 디몬 프로세스 구동 메뉴 ◎ 방화벽 디몬 프로세스 종류 메뉴 ◎ 프로그램 종료 메뉴
모니터메뉴	◎ 실시간-모니터 메뉴 ◎ 패킷 정보 메뉴 ◎ 네트워크 상태 메뉴
통계메뉴	◎날짜별 통계정보 메뉴 ◎주간별 통계정보 메뉴 ◎월별 통계정보 메뉴
도움말	◎프로그램 사용 설명 메뉴

4.1 접근제어

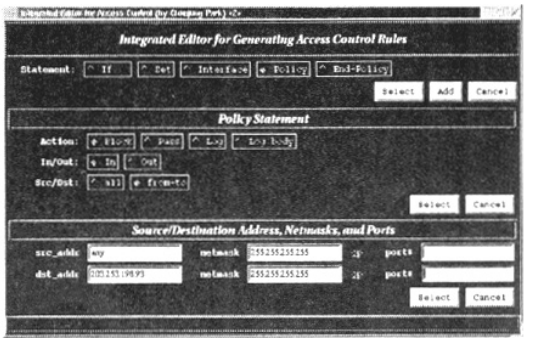
이 절에서는 접근제어 규칙의 생성 및 삭제, 출력과 같은 관리 기능을 수행하는 그래픽 사용자 인터페이스를 구현한 내용을 기술한다. 하나의 규칙은 다음 (그림 5)와 같이 허용 혹은 거절과 같은 보안정책과 출발지 및 도착지 호스트명, 트래픽 로그 여부, 프로토콜 명 등과 같은 정보로 이루어져 있다.

화면의 구성은 다음과 같다. 사용자는 어떤 네트워크 계층을 위한 방화벽, 즉 Socks 혹은 Ip_filter 중에 하나를 결정하여 접근제어 규칙을 설정한다. 네트워크 계층이 결정되면, 그에 대응되는 규칙들이 동시에 10 개씩 화면에 출력된다. 규칙이 10 개 이상인 경우는 "Next Rules" 버튼과 "Prev Rules" 버튼을 이용하여 다음 10 개의 규칙 혹은 이전 10 개의 규칙을 출력하는 화면으로 이동한다.



(그림 5) 접근제어 규칙을 출력한 화면

(그림 5)에서 "Add Rules"라는 메뉴버튼을 선택하면, (그림 6)과 같이 사용자가 규칙을 기술하기 위해서 선택할 수 있는 문장들이 출력되고, 추가하고 싶은 문장을 선택하면 된다. "Delete Rules"는 삭제하기를 원하는 규칙의 번호를 입력하여 규칙을 삭제할 수 있다. "Show Rules"은 그래픽 사용자 인터페이스를 통해 생성한 규칙이 실제로 어떻게 표현되었는지 제안한 규칙기술 언어의 형태로 출력한다. 이 때, 텍스트로 표현된 규칙들을 직접 수정할 수 있고, 수정된 내용은 다시 (그림 5)에 반영이 되어진다.

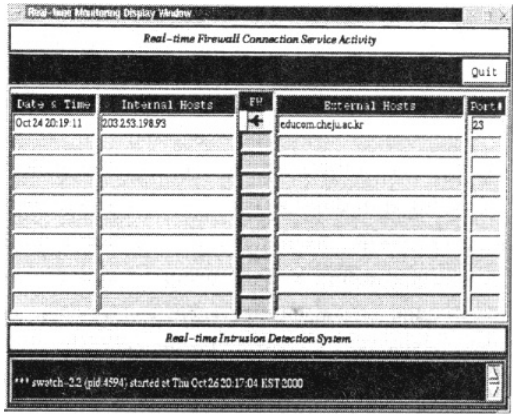


(그림 6) 새로운 규칙을 삽입하는 일 예

[13]의 연구와 비슷한 면이 있으나 두드러진 차이는 Socks v5를 사용하였다는 점과 학교망에 맞도록 Ip_filter와 Socks v5의 규칙 기술 언어를 중점적으로 처리하였다는 점이며 이를 통해 성능을 향상시킬 수 있다.

4.2 네트워크 감시

감시(monitoring) 기능은 네트워크를 감시하기 위한 기능으로써 실시간 트래픽 감시와 패킷 정보 출력 기능, 네트워크 게이트웨이 정보를 제공한다.

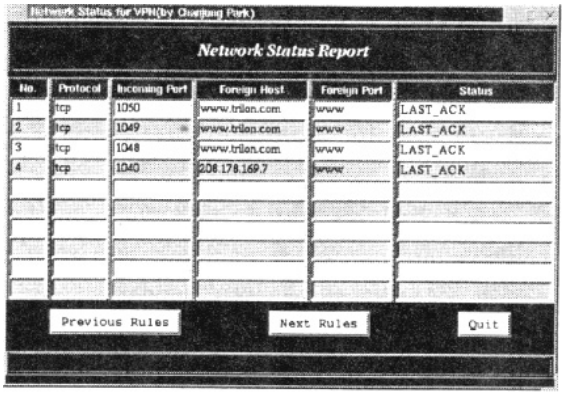


(그림 7) 실시간 트래픽 감시 화면

(그림 7)과 같이 실시간 트래픽 감시 기능은 실시간적으로 방화벽으로 들어오는 트래픽과 나가는 트래픽 정보를 Swatch[21]라는 프로세스를 이용하여 검출해서 포트번호와 입력 및 출력 방향 등과 함께 출력한다. Swatch는 지정된 로그 파일에서 검출을 원하는 문자열이 발견되면, 사용자에게 경고 메시지를 실시간적으로 전송한다. 그 밖에 호출기 호출과 같은 기능도 수행할 수 있다. 한편, 네트워크 상태 감시 기능은 현재 시스템에 연결되어 있는 네트워크 개체들의 목록을 (그림 8)과 같이 출력하고, 라우터 감시 기능은 라우터 테이블 정보를 출력한다.

4.3 통계 처리

통계처리 기능에는 <표 2>와 같이 일별 및 주간별, 월별로 외부로부터 얼마만큼의 접속이 있



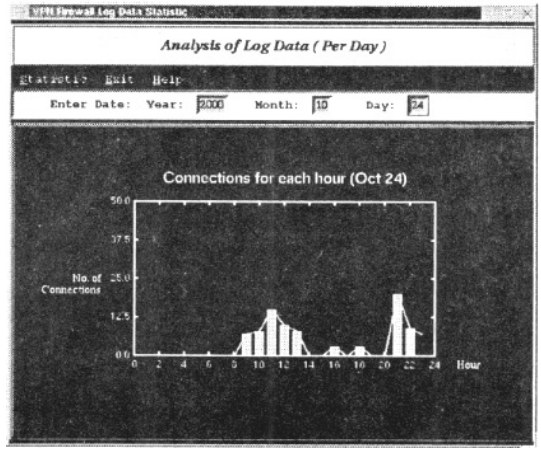
(그림 8) 네트워크 상태 출력

었는지 접속회수와 얼마만큼의 데이터들이 전송되었는지를 나타내는 데이터 전송량을 시간별 및 날짜별로 구분하여 출력한다. 즉, 사용자가 출력해 보고자 하는 날짜를 지정하면, 다음 (그림 9)와 같이 그래프 형식으로 출력이 된다.

<표 2> 통계자료 기준

통계치 \ 날짜	일별	주간별	월별
접속회수	① 시간대별	① 시간대별 ② 날 짜 별	① 시간대별 ② 날 짜 별
데이터량	① 시간대별	① 시간대별 ② 날 짜 별	① 시간대별 ② 날 짜 별

(그림 9)는 하루동안 접속된 통계치를 시간별로 나타내고 있다. 즉, 그래프에서 의미하는 내용은 주로 오전 9시 ~ 오후 1시, 20시~ 22시에 연결이 많았음을 알 수 있다.



(그림 9) 통계자료 화면

5. 결 론

학교망에서도 보안에 대한 요구가 증가하면서 방화벽의 필요성이 대두되고 있다. 방화벽 구축 시에 접근제어 규칙을 정확히 기술하는 것은 매우 중요한 문제이다. 하지만, 어떤 방화벽을 사용하느냐에 따라서, 상이한 규칙기술 언어들을 제공하고 있기 때문에 관리자에게 어려움을 주고 있다. 만일, 하나의 언어로 다양한 방화벽의 접근제어 규칙들을 생성한다면, 특히 학교 내에서 전문가가 아닌 관리자들의 관리 용이성을 제공할 수 있다.

본 논문에서는 학교망을 위한 혼합방화벽을 구축하는 방안에 대해서 제시하였다. 또한, 혼합방화벽에서 제공하는 접근제어 규칙들을 생성하기 위해서 단일한 형태의 접근제어 규칙기술을 기술할 수 있는 그래픽 사용자 인터페이스를 구현하였다. 이 인터페이스에는 네트워크 관리를 위해서, 로그 관리 및 실시간 트래픽 감시, 날짜별 통계처리 기능을 제공하였다.

향후, 인터페이스의 미흡한 부분을 웹기반에 맞도록 추가 수정할 계획이며 방화벽과 함께 사용자 인증을 위한 기능도 강화시키려고 한다. 또한, 학교에서 혼합방화벽을 구축하는 사용자 집단의 특성을 파악하여 더욱 관리가 용이하도록 기능의 변경 및 추가를 진행 중에 있으며 한글을 지원하도록 수정 중에 있다. 하지만 안전한 학교망을 위해서는 무엇보다도 학교망을 사용하는 사용자들의 보안에 대한 의식 변화가 우선되어야 하겠다.

참고문헌

[1] 한병래, 김홍래, 송기상(1999). 교수-학습을 위한 학내전산망 구축의 문제점 및 개선 방안. 한국컴퓨터교육학회 논문지, 2(2).

[2] 서정칠, 김미량(2000). 인터넷 활용수업의 실태조사 및 분석, 한국컴퓨터교육학회 논문지, 3(1).

[3] 김병욱(1998). '98 에듀넷 운영. 멀티미디어 교육지원센터.

[4] 인티(1999). 네트워크 문제. http://www.mo- nalisa.co.kr/white.asp.

[5] 신성균(1998). 교육정보화 기반 구축 통합모델에 관한 연구. 멀티미디어 교육지원센터.

[6] 이미향, 전우천(1999). 초등학교 인트라넷 구축을 위한 보안 시스템 설계. 한국정보교육학회 동계 학술대회 발표지.

[7] 한국통신(1997). KT-ISEC'97 방화벽 구축 기술집.

[8] NEC USA(1999). Socks Version 5. http:// www.socks.nec.com/socksv5.html

[9] D. Reed(1999). IP Filter, http://cheops.anu.edu.au/~avalon/ip-filter.html.

[10] 김종식(1991). 학교교육용 컴퓨터 활용의 효율화를 위한 교실망 연구. 한국교육개발원.

[11] M. J. Ranum(1993). Thinking about Firewalls. Proceedings of the International Conference on Systems and Network Security Management.

[12] W. R. Cheswick(1994). Firewalls and Internet Security, Addison-Wesley.

[13] 박찬정(1999). 혼합형 침입차단시스템을 위한 통합 접근제어 규칙기술 언어 및 그래픽 사용자 인터페이스 구현. 한국통신정보보호학회 논문지 9(1).

[14] CheckPoint Software Technologies Ltd., FireWall-1 User Guide, Version2.1, June 1996.

[15] Raptor Systems, The Eagle Firewall Technical White Paper, http://www.raptor.com/whitepaper/ title.html, 1997.

[16] Secure Computing Corporation, Borderware Firewall Server 4.0 White Paper, http://www.sctc.com/borderware/white.html, November 1996.

[17] TIS Advanced Research and Engineering (1999). Internet Firewall Toolkit Overview.

http://www.tis.com/research/software/fwtk_over.html.

[18] M. Leech(1996). Username/Password Authentication Method for SOCKS Version 5. IETF Network Working Group RFC 1929.

[19] P. McMahon(1996). GSS-API Authentication Method for SOCKS V5. IETF Network Working Group RFC 1961.

[20] B. B. Welch(1997). Practical Programming in Tcl and Tk, 2nd Ed. Prentice Hall.

[21] S. E. Hansen and E. T. Atkins(1993), Automated System Monitoring and Notifi- cation with Swatch. Proceedings of LISA.

박 찬 정

1988 서강대학교전자계산학과 (학사)

1990 한국과학기술원 전산학과 (석사)

1998 서강대학교 전자계산학과 (박사)

1990.3~1999.9 한국통신 멀티미디어연구소 전임연구원

1999.9~현재 제주대학교 컴퓨터교육과 전임강사

관심분야: 웹기반교육, 데이터보안, 인터넷보안, 실시간시스템

E-Mail: cjpark@cheju.cheju.ac.kr