3계층 클라이언트/서버 시스템의 고속 전송 침입 차단 시스템 구현

홍현술* · 정민수** · 한성국**

An Implementation of Firewall System Supporting High Speed Data Transmission in 3-tier Client/Server Systems

Hyeun-Sool Hong* · Min-Soo Jung** · Sung-Kook Han**

이 논문은 2001년도 원광대학교 교내연구비를 지원받았음

요 약

3계층 클라이언트/서버 시스템에 일반적인 방화벽을 설치하면 어플리케이션의 서버와 방화벽의 프락시 기능이 중복되어 전송속도 저하 현상이 야기된다. 따라서, 본 논문에서는 어플리케이션 서버의 프락시 기능을 정의하고 네트워크 인터페이스 카드를 어플리케이션에 추가로 장착하여 듀얼-홈드 게이트웨이를 구성하고, 어플리케이션을 보호하기 위하여 외부망과 내부망으로 분리하는 스크린드 라우터를 설치하여 스크린드 서브넷 게이트웨이를 구성하는 침입차단 시스템을 제안하였다.

본 논문에서 제안된 시스템은 3계층 클라이언트/서버 시스템에 방화벽을 설치하는 것보다 네트워크의 통신량 분산에 효과적이며, 중복된 기능을 하지 않기 때문에 고속전송이 가능하다. 또한, 방화벽 구입에 대한 비용 효과도 있다.

ABSTRACT

In the firewall systems of 3-tier client/server systems, in general, data transmission speed is declined rapidly according to the duplicated proxy services in application server and fire wall server. In this paper, an application server configuration containing the proxy functions of firewall system is proposed so that the high speed data transmission can be achieved. The proposed application server can form the dual-homed gateway by means of the additional network interface card. The screened router of application server forms the screened subnet gateway that can separate the internal network.

The proposed server configuration is more effective in traffic control than the traditional firewall systems and provides high speed data transmission with the functions of firewall. It can be also cost-effective alternative to the firewall system.

* 원광보건대학 컴퓨터응용개발과

** 원광대학교 전기전자 및 정보공학부

접수일자: 2001. 12. 12

키워드
3계층 클라이언트/서버 시스템, 방화벽, 듀얼-홈드 게이트웨이, 스크린드 라우터, 스크린드 서브넷 게이트 웨이

Ⅰ. 서 론

정보통신 기술은 데이터 통신의 고속화에 대한 요구와 웹기술의 발달과 더불어 급속도로 발전되어 왔다. 이러한 데이터 통신의 발전은 네트워크의 보안에 관련된 문제들을 야기 시켰고, 이를 해결하기 위한 많은 방법들이 연구되고 있다. 현재 네트워크의 대부분이 기가비트 이더넷(Gigabit Ethernet)이 선호되고 있는데, 이에 대한 보안을 유지하려면 여러 개의 방화벽이 병렬로 설치된 침입 차단 시스템이 되어야 한다. 또한 네트워크 시스템에 여러 개의 방화벽을 설치할 경우, 로드 밸런싱(load balancing)을 위해 레이어 4 스위치가 추가로 설치되어야 하기 때문에 많은 비용이 소요된다[1,2,3,4,5].

최근 컴퓨팅 환경에서 개발되어지는 어플리케이션 시스템들은 클라이언트/서버 구조로 이루어진 3계층 구조를 가지는 시스템이 일반적이다. 3계층은 상층부, 중층부, 하층부로 구성되며, 중층부의 서버는 강력한 LAN 서버 기능을 가지고 있다. 즉, 하층부의 요청을 받아 적절한 처리를 거쳐 상층부에 있는 데이터베이스에 데이터를 요청하여 다시 클라이언트에 결과를 돌려보내는 역할을 담당하고 있다. 이러한 기능적인 측면에서 볼 때, 중층부의 서버들은 두 개의 역할을 동시에 수행하며, 이를 접속형태로 다시 나누면, 하층부와 중층부의 통신 연결과 중층부와 상층부의 통신이 연결되는 형태로 볼 수 있다. 하나의 네트워크에서 이루어지는 두 종류의 통신을 2개의 통신대역으로 나누어보면, 침입차단시스템은 Dual-homed 게이트웨이 구조를 가져야 한다. 그러나, Dual-homed 게이트웨이에서 중층부의 관리를 위해 로그인 기능을 넣게 되면, 서버가 외부의 공격에 노출되게 되고, 로그인 기능을 열어 놓지 않았더라도 서비스 거부 공격(DoS : Denial of Service)을 통해서 서버의 통신자체가 불가능하게 되는 등, 보안을 위해 취해진 조치로 인하여 통신이 불가능해지는 문제가 발생한다. 이러한 문제를 해결하는 방법 중의 하나는 외부에서 들어오는 패킷을 적절히 차단하는 것이며, 이를 위해서는 패킷 차단에 대한 보안 정책이 필요하다. 보안 정책의 보안과 편리성은 상대적 관계로서, 보안을 높이게 되면 사용의 편리성이 약하게 되고, 사용의 편리성을 높이게 되면 상대적으로 낮은 단계의 보안이 적용된다[6,7,8,9,10].

본 논문은 기존의 3계층 클라이언트/서버 시스템에서 발생하였던 하층부와 중층부의 패킷과 중층부와 상층부에서 발생한 패킷이 동시에 하나의 네트워크를 통과해야 하기 때문에 발생했던 병목현상을 두 개의 독립된 네트워크를 이용하여 해결하는 방법을 제시한다. 본 논문에서 제시된 침입차단시스템은 스크린드 라우터를 사용함으로써 고속 데이터전송이 가능하고 서비스를 제공하는 포트를 미리 알고 있으므로 접근제어목록을 명확하게 작성할 수 있으며, 불필요한 패킷을 차단함으로써 중층부와 상층부의 네트워크에 부하를 줄일 수 있는 특징이 있다.

Ⅱ. 3계층 클라이언트/서버 시스템의 구조

네트워크 컴퓨팅 환경에서 개발되어지는 어플리케이션 시스템들은 클라이언트/서버 구조로 이루어지며, 일반적으로 3계층으로 구성되어진다[11,12,13]. 3계층 구조는 상층부, 중층부, 하층부로 구성되어 있으며, 상층부에는 공용 데이터를 관리하는 데이터베이스가 설치되어 있는 중형급 이상의 서버가 존재하고, 중층부에는 강력한 LAN 시스템을 제공하는 서버가 있으며, 하층부에는 일반 사용자가 사용하는 컴퓨터들로 구성된다. 이러한 3 계층 구조를 기반으로한 보안 시스템을 만들기 위해, 중층부의 서버를 이용하는 방안에 대하여 서술한다.

1. 어플리케이션 방화벽

어플리케이션 방화벽의 기본 구조는 프락시 서버를 기반으로 하고 있다. 어플리케이션 방화벽은 2개의 네트워크간에 직접적인 트래픽을 막고, 트래픽에 대한 로그, 감사 기능 등이 지원되는 프락시를 실행하는 시스템을 말한다. 어플리케이션 방화벽의 기본 구조가 되

는 프락시 서버에서의 프로세서 전달은 그림 1과 같다.

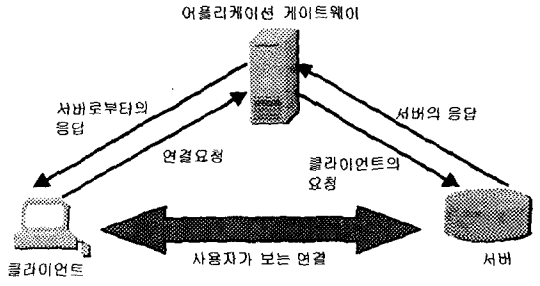

그림 1. 프락시 서버의 처리 흐름
Fig. 1 Process flow of proxy server

프락시는 클라이언트와 서버사이에 존재하여 둘 사이의 프로토콜 및 데이터 릴레이 역할을 수행한다. 프락시의 수행 과정을 살펴보면, 클라이언트가 방화벽으로 접속을 요구할 때 방화벽 상의 프락시 서버는 접속 허용 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 클라이언트의 접속 요청에 대한 응답을 보내어 클라이언트와의 연결도 맺는다[5,11,13,14]. 일단 클라이언트와 서버간에 접속이 이루어지면 사용자는 방화벽의 존재를 전혀 의식하지 못하게 되고 실제 서버와 직접 통신하는 것처럼 느끼게 된다. 이처럼, 어플리케이션 레벨 방화벽은 외부로부터 내부 시스템을 보호하기 위한 1차적인 방어수단을 제공한다.

2. 3계층 클라이언트/서버 시스템의 방화벽

3계층 클라이언트/서버 시스템의 구조적 특성에 대하여 서술하고, 2계층 구조에서 3계층 구조로의 변화에 따른 3계층 구조의 정의와, 3계층 구조에서 프로세서의 처리에 따른 전달 과정에 대하여 고찰한다.

(1) 3계층 클라이언트/서버의 정의와 처리 흐름

계층적 클라이언트/서버 시스템에서 2 계층 구조는 업무 규칙에 근거하는 처리 논리 즉, 업무 논리가 클라이언트 층과 서버 층에 산재되어 있다. 전형적인 클라이언트에서 업무처리는 사용자 인터페이스에 부수되어 일어나는 이벤트처리와 긴밀하게 결합된 형태로 지원되기 때문에, 업무 논리 또한 클라이언트 측에 집중되는 경향이 있다. 반면에, 3계층 클라이언트/서버 구조는 업무 논리를 명확히 식별하여 분리하고 클라이언트 층과 서버 층 사이에 또 하나의 독립된 층을 마련하여 한 쪽으로의 집중을 예방하고 있다. 그림 2는 클라이언트/서버 시스템 구조의 2계층에서 3계층으로의 변화를 보여준다.

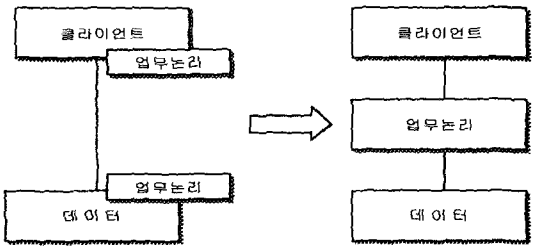

그림 2. 2계층 시스템에서 3계층 시스템으로 변화
Fig. 2 Transformation from 2-tier to 3-tier system

3계층 클라이언트/서버 구조는, 1계층은 사용자의 인터페이스를 주로 처리하는 프리젠테이션 층, 2계층은 기능층, 3계층은 데이터베이스 엑세스 층이다. 3계층 클라이언트/서버 시스템의 기본 개념은 시스템에 확장성과 유연성을 갖게 하기 위해서 시스템 구성을 계층화하여 서로 밀접하게 결합됨으로서 발생하는 종속성을 방지하는 것이다[3,4,6,11].

3계층 클라이언트/서버 시스템에서 클라이언트의 요구사항이 처리되는 과정은 그림 3과 같다.

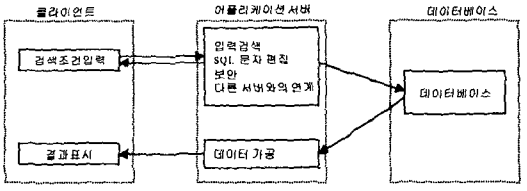

그림 3. 3계층 클라이언트/서버의 처리 흐름
Fig. 3 Processing in 3-tier client/server system

클라이언트 시스템의 사용자가 검색조건을 입력하고 어플리케이션 서버에게 서비스를 호출하게 되고, 어플리케이션 서버는 클라이언트가 요청한 서비스가 정당하게 요청되었는지를 검사하게 된다. 클라이언트가 정당한 사용자이면 데이터베이스에게 요청할 SQL

문장을 편집하여, 데이터베이스에게 SQL 문장을 전송하거나 다른 어플리케이션과 연계하여 서비스를 호출하게 된다. 데이터베이스는 어플리케이션이 전송한 SQL 문장을 실행하여 그 결과를 어플리케이션 서버에게 전달하게 되고, 어플리케이션 서버는 전달된 데이터를 가공하여 클라이언트에게 전달하게 된다[15,16,17].

(2) 3계층 구조에서 방화벽을 설치한 예

프락시는 OSI 7계층의 어플리케이션 계층에서 동작하는 것으로, 각 서비스별로 프락시 데몬(proxy demon)이 존재하여, 서비스별로 프락시를 이용한 세션정보에 의해 네트워크 접근제어가 가능하다. 따라서, 3계층 구조에서 클라이언트가 필요한 데이터를 어플리케이션 서버에게 요구할 수 있도록 제공되는 서비스와, 프락시 서버의 프락시 데몬이 제공하는 서비스는 동일한 형태의 처리 흐름을 보인다. 프락시는 Stored- Forward 방식을 사용하여 트래픽을 검사하기 때문에 속도 저하가 발생한다. 또한 3계층 클라이언트/서버 시스템에서도 어플리케이션 서버가 Stored-Forward 방식을 사용하여 데이터를 클라이언트에게 전달하고 있으므로 속도 저하가 발생한다. 따라서 3계층 클라이언트/서버 시스템에 프락시를 이용한 방화벽을 설치하게 되면, 프락시 서버에서 수행하는 중계에 의한 지연과 어플리케이션 서버에서 데이터 전달에 따른 지연으로 인해 2배 이상의 지연이 발생하게 된다[12,13,17,18]. 그림 4는 3계층 클라이언트/서버 시스템에 방화벽을 설치한 예를 보인 것이다.

본 논문에서는 프락시 구조를 가지고 있는 어플리케이션 서버를 사용하여 방화벽을 구축함으로써 방화벽에 의한 중계지연을 방지하였으며, 어플리케이션 서버에서 제공하는 서비스만 허용되도록 하였다.

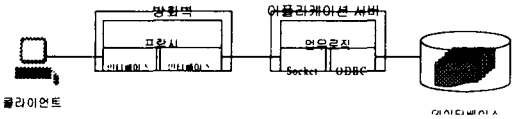

그림 4. 3계층 구조에 방화벽을 설치한 예
Fig. 4 Firewall in 3-tier system

3. 3계층 클라이언트/서버 시스템의 통신망 구성

본 논문에서는 3계층 구조의 일반적인 구조에 보안 시스템을 구축하기 위해, 중층부의 서버를 응용한다. 그림 5는 3계층 기본 구조에서 계층별 연결 형태를 표시한 것이다.

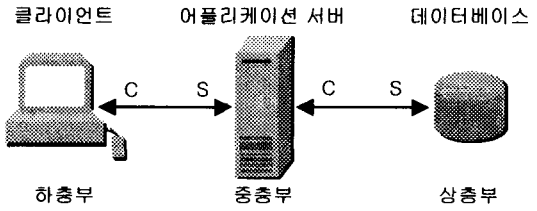

그림 5. 3계층에서 계층별 연결 형태
Fig. 5 Layer connection of 3-tier system

3계층 구조에서 중층부는 클라이언트가 요구하는 데이터를 데이터베이스에 요구하여 전달하는 중계자 역할을 담당한다. 이러한 역할을 순수한 클라이언트와 서버 관계로 고찰해 보면 하층부 클라이언트와 서버 역할을 하는 중층부, 클라이언트 역할을 하는 중층부와 서버 역할을 하는 데이터베이스로 분할 할 수 있다.

이러한 3계층의 연결 형태를 통신 형태로 해석해보면 다음과 같다. 일반적으로 중층부 서버는 하나의 네트워크 인터페이스 카드(Network Interface Card : NIC)를 가지고 상층부(데이터베이스)와의 통신과 하층부(클라이언트)와의 통신을 모두 수행한다. 따라서 NIC에 많은 양의 데이터가 흐르므로, 통신시에 병목현상이 발생한다[11,14,16,17]. 그림 6은 일반적인 중층부 서버의 구성 형태를 보여준다.

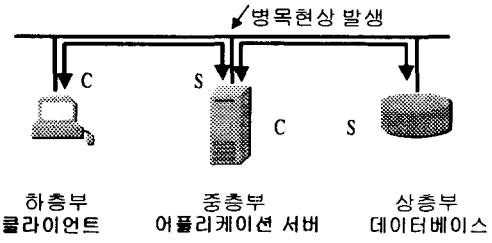

그림 6. 일반적 중층부 서버의 구성 형태
Fig. 6 General configuration of middle-tier

특정 네트워크의 통신부하를 분석해보면, 1개의 어플리케이션 서버의 통신량 TA는 다음과 같다.

$$TA = \sum(CA) + \sum(AD) + \sum(DA) + \sum(AC)$$

CA = 클라이언트와 어플리케이션 서버간의 통신량
AD = 어플리케이션 서버와 데이터베이스 서버의 통신량
DA = 데이터베이스 서버와 어플리케이션 서버의 통신량
AC = 어플리케이션 서버와 클라이어트의 통신량

n개의 어플리케이션 서버의 통신량 nTA는 다음과 같다.

$$nTA = \sum_{i=1}^{n}(\sum(CA)) + \sum_{i=1}^{n}(\sum(AD)) + \sum_{i=1}^{n}(\sum(DA)) + \sum_{i=1}^{n}(\sum(AC))$$

위 식에서 보면, 네트워크의 특성에 따라 서버의 수가 일정 범위를 넘게 되면, 충돌에 의해 어플리케이션 서버의 증가에 따른 통신 부하는 기하급수적인 증가 형태를 보인다.

이를 해결하기 위해서 어플리케이션 서버에 두 개의 NIC를 장착한다. 이렇게 함으로써, 하나의 NIC를 갖는 어플리케이션 서버에서 발생했던 병목현상이 두 개의 NIC로 인해 데이터가 분산되어 이동하기 때문에 병목현상이 해소된다. 또한, 데이터베이스와 어플리케이션 서버사이에 일어나는 통신의 내용을 클라이언트가 볼 수 없기 때문에 안전한 통신이 보장된다[11,14,19]. 그림 7은 어플리케이션 서버의 분리된 통신 형태를 나타낸다.

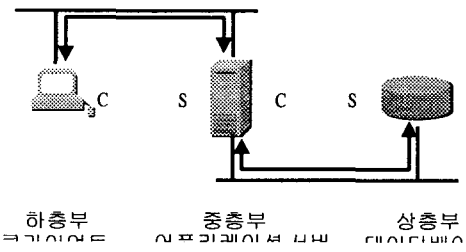

그림 7. 듀얼-홈드 게이트웨이 구성 형태
Fig. 7 Configuration of dual-homed gateway

네트워크의 통신량을 보면 1개의 어플리케이션 서버의 통신량 $TA1$과 $TA2$는 다음과 같다. $TA1$은 클라이언트와 어플리케이션 서버간의 통신량이고, $TA2$는 어플리케이션 서버와 데이터베이스 서버간의 통신량이다.

$$TA1 = (CA + AC)$$
$$TA2 = (AD + DA)$$

위 식에서 보는바와 같이, 네트워크의 통신량이 하층부와 중층부 사이의 네트워크에 대한 통신량과 중층부와 상층부 사이의 통신량으로 분산되어 전체 네트워크에 대한 통신량이 줄어드는 효과를 볼 수 있다.

Ⅲ. 침입차단시스템의 설계

방화벽 시스템의 설계, 설치, 사용에 직접적으로 영향을 줄 수 있는 네트워크 정책에는 두 가지 레벨이 존재한다. 상위 레벨의 정책은 명확한 이슈 즉, 제한된 네트워크로부터 서비스를 허락할 것인가 또는 명확히 거부할 것인가를 정의하는 네트워크 액세스 정책이다. 하위 레벨의 정책은 어떻게 방화벽이 실질적으로 액세스를 제한하고 상위 레벨의 정책에서 정의한 서비스를 필터링 할 것인가에 대한 사항 등이다[5,14,19,20].

일반적인 3계층 보안에서 상층부는 다른 계층보다 가장 높은 수준의 보안 정책이 요구된다. 반면에, 중층부는 외부에 공개되어 있는 하층부와 통신을 담당하므로 상층부보다는 낮은 중간 수준의 보안 정책이 요구된다. 따라서, 본 논문의 시스템 보안 수준은 데이터베이스를 높은 단계의 보안 정책을 어플리케이션은 중간 단계의 보안정책이 필요하다고 가정하여 설정한다.

1. 듀얼 홈드 게이트웨이

어플리케이션 서버에 두 개의 NIC를 장착하는 침입차단 시스템의 구조는 프락시 서버에 두 개의 NIC를 장착하여 듀얼-홈드 게이트웨이(Dual- homed gateway)와 같은 구조를 구성한다. 중층부의 서버가 어플리케이션 방화벽과 같은 기능을 수행하도록, 서버에 NIC를 두 개 장착하고, 두 개의 NIC에는 서로 다른 IP 어드레스를 할당한다. 서로 다른 두 개의 IP 어드레

스는 사설 IP와 공용 IP로 설정된다. 하층부와 중층부의 통신은 어디서나 가능해야 하므로 기존의 IP주소를 그대로 유지하고, 상층부와 중층부간의 통신에는 사설 IP를 설정하여 외부와 완전히 독립되는 형태를 갖도록 한다.

그러나, 듀얼-홈드 게이트웨이 구조의 단점으로 나타나는 문제의 보완이 필요하다. 즉, 중층부의 보안 관리를 위해 로그인 기능을 수행시키게 되면, 패스워드 확인이라는 한번의 취약한 보안 검사만으로 서버가 외부의 공격에 노출될 수 있기 때문이다. 또 다른 문제는 로그인 기능을 수행시키지 않더라도 DoS를 통해서 서버를 무력화시키면 통신자체가 불가능해지게 되므로, 보안을 위한 조치가 통신을 불가능하게 만드는 문제를 야기시킬 수 있다. 이것을 피할 수 있는 방법 중에 하나는 외부에서 들어오는 패킷을 적절히 차단하는 방법을 사용하는 것으로 스크린드 호스트 게이트웨이(Screened host gateway)가 이에 해당된다.

2. 스크린드 호스트 게이트웨이

두 개의 NIC를 장착한 어플리케이션 서버는 듀얼-홈드 게이트웨이의 단점을 가지고 있다. 어플리케이션 서버는 클라이언트와의 통신을 위해 외부에 공개되므로, 어플리케이션 서버를 공격하고자 하는 사용자의 공격에 노출되게 된다. 그런데, 어플리케이션 서버는 특정 서비스만 전달하는 역할을 하고 있다. 따라서, 어플리케이션 서버가 제공하는 서비스의 프로토콜과 제공하지 않는 프로토콜을 필터링하여 어플리케이션 서버에게 필요한 프로토콜만 전달하도록 한다. 이를 위해, 어플리케이션 서버의 앞쪽에 스크린드 라우터를 설치한다. 스크린드 라우터는 OSI 참조 모델의 3계층과 4계층에서 동작하는 필터링을 사용하므로 빠른 속도를 유지할 수 있다.

스크린드 라우터는 송신자의 인터넷 주소, 수신자의 인터넷 주소, TCP나 UDP의 송신포트와 수신포트를 바탕으로 외부에서 오는 패킷을 필터링한다. OSI 7 계층중 IP와 TCP, UDP 계층에서 필터링을 하기 때문에 속도가 빠르고 비용이 적게 드는 장점을 가지고 있으며, 네트워크 계층에서 동작하므로 클라이언트와 서버를 변화시키지 않는 장점을 가진다. 듀얼-홈드 게이트웨이 앞쪽에 스크린드 라우터를 설치하며 스크린드 호스트 게이트웨이(*Screened host gateway*)를 구성하면 그림 8의 형태가 된다.

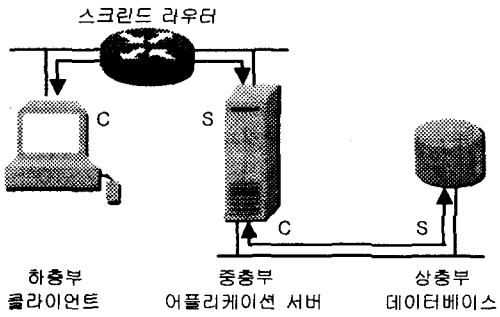

그림 8. 스크린드 호스트 게이트웨이 구성 형태
Fig. 8 Configuration of screened host gateway

그림 8에서 스크린드 라우터는 내부 네트워크 상에 놓여있는 중층부 서버를 제외하고 외부에서 들어오는 모든 패킷을 차단한다. 클라이언트가 중층부 서버에 서비스를 요청하게 되고 중층부 서버는 데이터베이스에 질의를 하면, 데이터베이스는 자료를 중층부 서버에 전달하게 되고 중층부 서버는 스크린드 라우터를 통해서 클라이언트에 전달하게 된다. 이러한 형태의 통신상에서 외부에 공개된 유일한 연결점은 중층부 서버이므로, 중층부 서버는 항상 보호되고 감시되어야 한다.

스크린드 라우터는 내부 네트워크에 대해서 두 가지 옵션을 가지며, 그 옵션은 내부 호스트를 인터넷상의 특정 서비스와 연결할 수 있게 허용하거나, 또는 외부로의 모든 연결을 차단할 수 있게 하는 것이고, 내부 호스트들이 중층부 서버를 통해서 서비스가 될 수 있도록 강요한다.

스크린드 호스트 게이트웨이의 단점은 모든 패킷이 하나의 중층부 서버를 통하도록 되어 있어, 라우팅 테이블이 변경되면 내부 네트워크의 다른 서버에 접근할 수 있으며, 여러 대의 중층부 서버가 있는 경우 적용 될 수 없는 구성형태라는 점이다.

3. 스크린드 서브넷 게이트웨이

스크린드 호스트 게이트웨이로 구성된 침입차단 시스템에서 스크린드 라우터가 공격받게 되면, 호스트를 공격할 수 있는 네트워크의 접근도 가능해지므로 스크린드 라우터의 중요성이 강조된다. 그러나, 스크린드

라우터는 필터링의 기능만 수행하기 때문에 로그나 감사(audit)에 필요한 데이타를 유지할 수 없다. 따라서, 어플리케이션 서버의 뒤쪽에도 스크린드 라우터를 하나 더 설치하고 데이터베이스가 속해 있는 네트워크를 새로 구성하여, 구성된 네트워크에는 어플리케이션 서버만이 접근하도록 함으로써, 클라이언트와 어플리케이션 서버 사이에 있는 스크린드 라우터가 공격당하더라도 데이터베이스 서버까지 도달하지 못하도록 한다. 이처럼, 데이타베이스와 어플리케이션 서버 사이에 스크린드 라우터를 하나 더 설치한 방화벽 구성 형태는 스크린드 서브넷 게이트웨이(Screened subnet gateway)가 된다.

보안 정책면에서 데이터베이스 서버가 있는 네트워크는 높은 수준의 보안을 유지시켜야 하며, 이를 위해 데이터베이스 서버가 위치하는 네트워크는 사설 네트워크로 구성하여 인터넷과 분리한다. 그리고, 스크린드 라우터는 데이터베이스 서버의 서비스 프로토콜만을 필터링하여 통과시킴으로써 공격자로부터 공격을 차단하도록 한다.

스크린드 서브넷 게이트웨이에서 클라이언트와 데이터베이스 서버 사이에 있는 네트워크를 DMZ 네트워크로 구성한다. 그림 9는 스크린드 서브넷 게이트웨이의 구성형태를 보여준다.

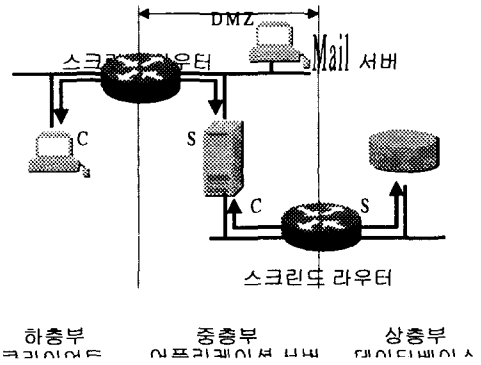

그림 9. 스크린드 서브넷 게이트웨이의 구성형태
Fig. 9 Configuration of screened gateway

DMZ 네트워크는 스크린드 라우터와 어플리케이션 게이트웨이와 같은 다른 방화벽 사이에 존재하는 네트워크로 정의한다. DMZ 네트워크는 스크리닝 라우터의 필터링으로 제어가 이루어지지만 안전한 부분은 아니다. 일반적으로 DMZ 안에는 외부로 서비스하는 호스트들, 예를 들면 FTP, WWW, 3계층 구조의 어플리케이션 서버 등의 중층부 서버가 존재하게 된다. 이 중층부 서버는 외부의 많은 사람들에게 공개되어 있어야 하는 호스트이므로 방화벽의 밖에 두어서 접근을 쉽게 한다.

4. 패킷 필터링

스크린드 라우터의 중요한 역할은 패킷을 필터링하는 것으로, 패킷 필터링은 보안 정책에 따라 적용된다. 어플리케이션 서버가 위치하는 보안 수준은 보안 정책에서 중간 단계로 설정되어 있다. 클라이언트에게 서비스를 제공하는 어플리케이션 서버에 대해서는 정확한 파악이 가능하기 때문에 보안 정책을 명확하게 수립할 수 있다.

반면에, 데이터베이스 서버가 위치하는 네트워크의 보안 수준은 높은 수준의 단계를 요구한다. 이 네트워크에 접속할 수 있는 대상은 어플리케이션 서버만 해당이 된다. 따라서, 패킷 필터링에서는 어플리케이션 서버를 나열하고 서비스 포트를 제한하여 높은 수준의 보안을 유지할 수 있다.

Ⅳ. 구현 및 성능평가

본 논문에서 설계한 침입차단시스템을 대학 학사행정 시스템에 적용하여 성능을 평가하였다. 대학 학사행정 시스템을 3계층 구조로 보면, 상층부에는 데이터베이스 서버가 위치해 있으며, 중층부에는 학사 행정용 어플리케이션 서버가 여러 대 설치되어 있고, 하층부에 해당되는 학사행정에 대한 서비스는 학내외 어디에서나 사용 가능하다. 하층부에 해당되는 학사 행정 서비스를 어디에서나 사용이 가능하므로, 방화벽을 인터넷과 내부 네트워크를 연결하는 라우터 뒤에 설치하는 것은 무의미하다.

1. 학사 행정 시스템의 네트워크 구성

일반적인 대학에서는 방화벽을 외부와 접속되는 위치에 배치시킴으로써 내부와 외부를 분리하려하고 있으나, 대학의 특성상 데이터베이스에 대해 내부의 침

입자가 더 많다는 약점이 존재한다. 또한, 내부의 서버를 보호하기 위해 LAN쪽에 방화벽을 설치하더라도 WAN과는 달리 LAN의 속도로 인해 방화벽의 성능이 미약하여 효과를 기대하기 어렵다. 일반적인 방화벽의 처리능력은 10Mbps이하의 트래픽을 감시하는데 상당히 고비용 하드웨어 사양의 서버를 요구하고 있으며, 처리 능력의 향상을 위해 병렬처리가 요구된다.

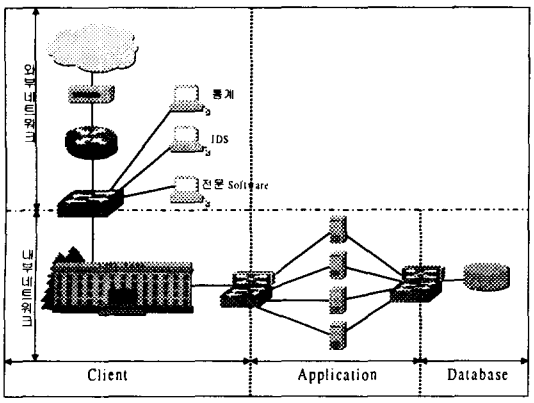

그림 10. 학사행정 네트워크 구성
Fig. 10 Network for academic administration

그림 10은 학사 행정 시스템에 대한 전체 네트워크 구성을 나타낸 것이다. 본 논문에서는 3 계층으로 구성된 학사 행정시스템을 대상으로 어플리케이션 서버를 듀얼-홈드 게이트웨이로 구성함으로써 방화벽의 효과를 발휘하도록 하였고, 추가적으로 스위치를 스크린드 라우터로 사용함으로써 스크린드 서브넷 게이트웨이를 구성하였다.

먼저, 어플리케이션 서버의 듀얼-홈드 게이트웨이를 만들기 위해 NIC를 추가로 1개를 더 장착한다. 추가된 NIC에 사설 네트워크를 구성하기 위해 사설 IP를 배정하였고 디폴트 게이트웨이는 외부쪽 스위치로 지정한다. 사설 네트워크로 디폴트 게이트웨이를 설정하게 되면, 통신이 되지 않는다. 외부쪽과 내부쪽의 스위치는 라우팅이 가능한 Cisco 제품군의 2948G를 선택하였다.

그림 11은 본 논문에서 구성한 침입차단 시스템의 전체 구성도 이다.

NIC를 두 개 장착한 어플리케이션 서버의 라우팅 테이블은 표 1과 같다.

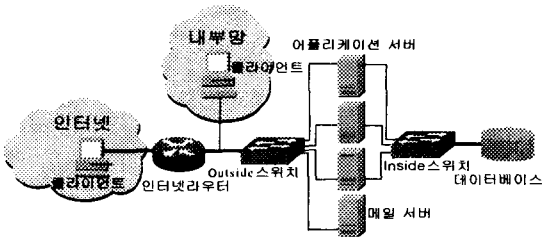

그림 11. 침입차단 시스템의 전체 구성도
Fig. 11 Overall architecture of intrusion detection system

표 1. NIC가 두 개인 어플리케이션 서버의 라우팅 테이블
Table. 1 Routing table for application server with 2 NICs

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	210.X.X.1	210.X.X.52	1
10.X.X.0	255.255.255.0	10.X.X.1	10.X.X.1	1
10.X.X.1	255.255.255.255	127.0.0.1	127.0.0.1	1
10.X.X.255	255.255.255.255	10.X.X.1	10.X.X.1	1
10.X.Y.0	0.0.0.255	10.X.Y.2	10.X.Y.1	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
210.X.X.0	255.255.255.0	210.X.X.52	210.X.X.52	1
210.X.X.52	255.255.255.255	127.0.0.1	127.0.0.1	1
210.X.X.255	255.255.255.255	210.X.X.52	210.X.X.52	1

210.X.X.0/21 네트워크는 어플리케이션 서버 스스로가 처리하게 되어 있고, 추가적으로 10.X.X.0/21 네트워크도 어플리케이션 서버가 처리하게 되어 있다. 여기서 디폴트 게이트웨이는 외부쪽으로 설정하여 네트워크의 라우팅이 되도록 구성한다. 또, 데이터베이스와 통신을 위해 10.X.Y.0/21은 내부쪽의 라우터로 전달되도록 구성하였다.

2. 보안 정책

최근에는 TCP/IP 프로토콜의 취약성을 이용한 다양한 공격방법들이 보고되고 있다. 이러한 공격법의 예로는 IP spoofing, SYN flooding, Ping bombing, NFS/NIS/DNS spoofing 등이 포함된다. 이러한 프로토콜 공격에 대비하고 기타 여러 침입 방법에 대해 미연에 방지하기 위해서 외부 네트워크에서 내부 네트워크로 들어오는 패킷들에 대해 패킷 필터링을 적용할 수 있다. 패킷 필터링은 보안 정책에 따라 라우터와 방

화벽을 통해 구현된다.

(1) 서비스 포트에 의한 보안

일반적으로 인터넷을 포함한 외부 네트워크들로부터 내부 네트워크에 있는 서비스들을 사용할 이유가 없는 것들이 있다. 예를 들어 NFS, NIS, TFTP 등의 서비스는 특정 서브네트워크에 존재하는 호스트끼리 서비스를 이용하는 경우가 대부분이며 특별한 경우를 제외하면 외부로부터 서비스를 받게 할 이유가 없다. 이러한 서비스 포트들은 보안상의 많은 취약점들이 발견되고 있으며 외부로부터 내부 시스템에 침입하기 위한 공격 대상이 될 뿐이다. 이러한 포트들은 패킷 필터링을 통해 공격을 미연에 방지하여야 한다.

잘 알려져 있는 서비스 포트들은 라우터나 방화벽에서 패킷 필터링을 적용할 때 외부로부터 접근을 허락할 것인지, 허락하는 경우에는 모든 외부 네트워크에서의 접근을 허락할 것인지, 일부 네트워크나 호스트들에서만 접근을 허락할 것인지 고려해야 한다. 기본적인 정책은 외부 네트워크에서 접근하여 사용하지 않는 포트들은 필터링 하도록 하는 것이다.

rlogin(TCP/513), rsh(TCP/514)등의 서비스들은 CERT에서 필터링을 권장하고 있다. 일반적인 경우 이 포트들은 외부 네트워크에서 서비스를 이용할 이유가 없으므로 포트를 막도록 권하고 있다.

(2) 필터링 규칙

라우터와 방화벽을 이용하여 패킷 필터링을 적용하고자 할 때 일반적으로 내부에서 외부로 나가는 연결에 대해서는 열어두고, 외부에서 내부로 들어오는 연결에 대해서만 접근제한을 두게 된다. 이때, 접근 제한을 두는 방식에는 두 가지가 있다. 첫 번째 방식은 보안상의 위험성이 보고된 포트들을 필터링 하여 막고 나머지는 모두 허락하는 방식이다. 두 번째 방식은 그와 반대로 접근 허가할 포트들만 특정 호스트와 네트워크에 대해서 열어두고 나머지는 막는 방식이 있다.

첫 번째 방식은 서비스의 제약이 많지 않으므로 새로운 서비스들이 추가되는 경우에 필터링 규칙을 새로 적용하여야 하는 번거로움이 없다. 따라서, 보안이 아주 엄격할 필요보다는 사용의 편이성이 우선이 되는 경우 라우터를 이용하여 패킷 필터링 하는 경우에 적당하다.

두 번째 방식은 방화벽을 이용하여 보안 정책을 구현해 나가는 경우에 적합한 방식이다. 따라서, 보안이 엄격한 곳에서 외부에 대해 허가된 내부 서비스에 대해서는 열어두고 나머지 경우들에 대해서는 외부 접근을 막는 방식이 가능하다.

표 2는 스크린드 라우터에 설정되어 있는 ACL을 보여준다. 대학 학사 행정시스템에 대한 보안을 위해 개략적인 내용만을 보였다.

표 2. 인터넷 접속 라우터의 ACL
Table. 2 ACL for Internet-connected router

Cisco 7507의 ACL <인터넷 접속 라우터>
①access-list 102 deny ip any 0.0.0.255 255.255.255.0 ②access-list 102 deny ip any 0.0.255.255 255.255.0.0 ③access-list 102 deny ip any 0.255.255.255 255.0.0.0 ④access-list 102 deny ip any 0.0.0.0 255.255.255.0 ⑤access-list 102 deny ip 10.0.0.0 0.255.255.255 any ⑥access-list 102 deny ip 172.0.0.0 0.31.255.255 any ⑦access-list 102 deny ip 192.168.0.0 0.0.255.255 any ⑧access-list 102 permit tcp any host mailhost eq smtp ⑨access-list 102 deny tcp any 203.X.X.0 0.0.X.255 eq smtp ⑩access-list 102 deny tcp any 210.X.X.0 0.0.X.255 eq smtp ⑪access-list 102 permit ip any any
interface Serial 0/0 ip access-group 102 in

①~⑦ 인터넷에서 유통되지 않아야 하는 라우팅 정보(사설IP주소, 로컬호스트 IP주소등)와 목적지가 x.x.x.255 나 x.x.x.0인 IP의 차단

⑧ mail host만 smtp 허용

⑨~⑩ 내부 네트워크의 모든 호스트에 대해 smtp 차단

⑪ 위에서 차단한 것 외에는 모두 허용

표 2의 ACL에는 외부에서 내부 네트워크 주소나 사설 주소로 접근 할 때는 모두 차단하고, 메일에 대해서는 메일 호스트만 메일을 받도록 하여 스팸 메일(SPAM mail)을 방지하도록 하였다.

패킷 필터링 수행결과는 그림 12와 같다.

표 3은 외부쪽 스위치에 대한 ACL을 보여주며, 그림 13은 외부쪽 스위치의 패킷 필터링 결과를 나타낸다.

```
# sh ip access-list
Extended IP access list 102
 deny ip 10.0.0.0 0.255.255.255 any (6614 matches)
 deny ip 172.0.0.0 0.31.255.255 any (4447 matches)
 deny ip 192.168.0.0 0.0.255.255 any (111178 matches)
 permit tcp any host mailhost eq smtp (207995 matches)
 deny tcp any 203.X.X.0 0.0.X.255 eq smtp (94713 matches)
 deny tcp any 210.X.X.0 0.0.X.255 eq smtp
 permit ip any any (415721241 matches)
```

그림 12. 인터넷 라우터의 패킷 필터링 결과
Fig. 12 Packet filtering result of Internet router

표 3. 외부쪽 스위치의 ACL
Table. 3 ACL for outside switch

Cisco 2948G ACL<outside 스위치>
①access-list 101 permit tcp any 210.X.X.0 0.0.0.255 eq app-por ②access-list 101 permit tcp any 203.X.X.0 0.0.0.255 eq dns ③access-list 101 deny ip any any
interface VLAN1 ip access-group 101 in

① 어플리케이션 서버에 접근 할 수 있는 주소는 어디에서나 가능하고, 접근이 가능한 서비스 포트는 app-port만 허용
② DNS에 접근할 수 있는 주소는 어디에서나 가능하고, 접근이 가능한 서비스 포트는 dns 만 허용
③ 위에서 지정한 주소 및 포트를 제외하고 모두차단

```
# sh ip access-list
Extended IP access list 101
    permit ip any 210.X.X.0 0.0.0.255 (71661 matches)
    permit ip any 203.X.X.0 0.0.0.255 (1321 matches)
    deny ip any any (2147 matches)
```

그림 13. 외부쪽 스위치 패킷 필터링 결과
Fig. 13 Packet filtering result of outside switch

표 4와 그림 14는 각각 내부쪽 스위치의 ACL과 내부쪽 스위치의 패킷 필터링 결과를 보여준다.

표 4. 내부쪽 스위치의 ACL
Table. 4 ACL for inside switch

Cisco 2948G ACL<inside 스위치>
①access-list 101 permit tcp 10.X.X.0 0.0.0.255 host 10.X.Y.1 eq db-port ②access-list 101 deny ip any any
interface VLAN1 ip access-group 101 in

① 데이터베이스 서버에 접근 할 수 있는 주소는 어플리케이션 서버만 가능하고, 접근이 가능한 서비스 포트는 db-port만 허용
② 위에서 지정한 주소 및 포트를 제외하고 모두 차단

```
# sh ip access-list
Extended IP access list 101
   permit ip 10.X.X.0 0.0.0.255 host 10.X.Y.1 eq db-port
     (54145 matches) deny ip any any (0 matches)
```

그림 14. 내부쪽 스위치 패킷 필터링 결과
Fig. 14 Packet filter result of inside switch

3. 성능 평가

표 5는 어플리케이션 서버를 듀얼-홈드 게이트웨이로 구성하지 않았을 때의 결과이다.

표 5. 듀얼-홈드 게이트웨이로 구성하지 않은 경우
Table. 5 Case without dual homed gateway

출발지	목적지	패킷수	통신량
210.X.X.50	210.X.X.52	43	4344
210.X.X.52	210.X.X.50	51	12275
210.X.X.52	203.X.X.21	1	81
203.X.X.21	210.X.X.52	1	220
210.X.X.52	203.X.X.41	157	12992
203.X.X.41	210.X.X.52	193	29284

210.X.X.50 : 클라이언트
210.X.X.52 : 어플리케이션 서버
203.X.X.21 : DNS
203.X.X.41 : 데이터베이스 서버

어플리케이션 서버가 하나의 NIC를 가지고 있기 때문에 클라이언트(210.X.X.50)가 어플리케이션 서버

(210.X.X.52)에 서비스를 요청하게 된다. 어플리케이션 서버(210.X.X.52)는 클라이언트가 요청한 서비스에 대한 응답을 하기 위해 데이터베이스(203.X.X.41)에 SQL문장을 전달하여 결과 값을 받게 된다. 어플리케이션 서버는 결과 값을 처리한 뒤 클라이언트(210.X.X.50)에게 서비스에 대한 요청을 전달하게 된다.

이 과정에서 클라이언트가 서비스를 요청한 주소와 데이터베이스에 접근된 주소는 210.X.X.52로 되었다.

210.X.X.52의 네트워크 인터페이스를 통과한 트래픽은 4344 + 12275 + 81 + 220 + 12992 + 29284 = 59196 이 된다.

표 6은 어플리케이션 서버를 듀얼-홈드 게이트웨이로 구성되었을 때 외부에 공개된 네트워크에 대한 결과이다.

표 6. 듀얼-홈드 게이트웨이로 구성한 경우
TAble. 6 Case for dual homed gateway

출발지	목적지	패킷수	통신량
210.X.X.50	210.X.X.52	39	4002
210.X.X.52	210.X.X.50	45	11811
210.X.X.52	203.X.X.21	1	81
203.X.X.21	210.X.X.52	1	220

203.X.X.21 : DNS
210.X.X.50 : 클라이언트
210.X.X.52 : 어플리케이션 서버

외부에 공개된 어플리케이션 서버의 네트워크 인터페이스는 210.X.X.52 이다. 따라서 클라이언트 210.X.X.52를 통해서 서비스를 요청하게 된다. 어플리케이션은 일련의 과정을 거친 후 다시 클라이언트에게 서비스에 대한 응답을 하게 된다. 외부에 공개된 네트워크를 통과하는 패킷의 종류는 서비스의 요청과 응답에 대한 것만이 존재한다. 따라서, 데이터베이스와 어플리케이션 서버가 동작하는 패킷은 외부 네트워크에는 보이지 않게 된다.

210.X.X.52의 네트워크 인터페이스를 통과한 트래픽은 4002 + 11811 + 81 + 220 = 16114 가 된다.

표 7은 어플리케이션 서버를 듀얼-홈드 게이트웨이로 구성되었을 때 외부에 공개되지 않은 네트워크에 대한 결과이다.

표 7. 공개되지 않은 네트워크의 결과
Table. 7 Result of unopened network

출발지	목적지	패킷수	통신량
10.X.X.1	10.X.Y.1	156	12928
10.X.Y.1	10.X.X.1	154	26788

10.X.X.1 : 어플리케이션 서버
10.X.Y.1 : 데이터베이스 서버

어플리케이션 서버가 내부망에서 사용하는 네트워크 인터페이스의 주소는 10.X.X.1이다. 즉, 클라이언트가 서비스를 요청한 210.X.X.52와 다른 주소를 가지고 데이터베이스에 접근하게 된다. 내부망에 나타나는 트래픽의 종류는 DNS, 어플리케이션 서버가 SQL문장을 데이터베이스에 보내는 패킷, 데이터베이스가 어플리케이션 서버에게 결과 값을 전달하는 패킷만이 존재하게 된다. 내부망의 트래픽은 외부에 노출되지 않기 때문에 데이터베이스에 대한 보안은 높아지게 된다.

10.X.X.1 의 네트워크 인터페이스를 통과한 트래픽은 12928 + 26788 = 39716이 된다.

결과에서 보듯이 외부망의 트래픽은 내부망 보다 트래픽이 2.5배 적다. 하지만 클라이언트의 수는 어플리케이션 서버보다 많기 때문에 클라이언트가 연결될 외부망의 트래픽은 내부망보다 크게 된다. 따라서, 내부망이 외부망 보다 적은 트래픽이 발생됨으로써 트래픽이 효율적으로 분산된다.

실험 결과에서 도출된 문제로는 여러 종류의 스위치들에 주소 테이블이 가득 차게 되면, 모든 네트워크 세그먼트로 트래픽을 브로드캐스팅(broadcasting)하게 된다. 따라서 공격자는 위조된 MAC 주소를 지속적으로 네트워크에 흘림으로서 스위칭 허브의 주소 테이블을 오버플로우(overflow)시켜 다른 네트워크 세그먼트의 데이터를 스니핑(sniping)할 수 있다. 이는 보안 원리의 하나인 Fail close 를 따르지 않기 때문에 발생한다. 스위치들은 사실상 보안보다는 기능과 성능 위주로 설계되어져 있기 때문이다.

스위치를 설정할 때, 스위치의 주소 테이블을 정적(static)으로 설정하여 스위칭 환경에서의 스니핑을 막을 수 있는 방법이 있다. 표 8과 같이 스위치의 각 포트에 대하여 MAC 주소를 정적으로 대응시키면 ARP spoofing, ARP redirect 등의 공격을 막을 수 있다. 이러한 방법은 보안관리에 많은 시간을 소모하게 되지만

매우 효과적인 대응방법이다.

표 8. 스위치의 MAC 주소 테이블
Table. 8 MAC address table of switch

포트	MAC주소	permanence
1	00:60:97:c4:0f:3f	Yes
2	00:60:97:c4:0f:3b	Yes
3	08:00:20:79:c9:ea	Yes
4	00:60:97:c4:0f:3c	Yes
5	00:a0:24:28:c4:47	Yes
...	...	...

V. 결 론

일반적인 방화벽의 경우 많은 접근 제어목록과 다양한 통제기능을 가지고 있어, 적용해야 할 규칙이 많아지면 처리 속도가 저하되고, 네트워크 속도가 수십 Mbps가 되면 처리하지 못하는 단점을 지니고 있다. 또, 데이터가 방화벽을 우회하게 되면 감시가 되지 않기 때문에 일정한 통로로 모든 트래픽을 유도하도록 고안되어 있어 병목현상이 불가피하게 발생하게 된다.

하드웨어 장비의 발전과 함께 고용량의 스위치가 저렴하게 제공되고 있어 이러한 장비를 이용하여 보다 효과적인 네트워크 보안을 실현할 수 있다. 본 논문에서는 3 계층으로 구성되어 있는 클라이언트/서버 시스템에서 서버의 특성상 어플리케이션 서버를 듀얼-홈드 게이트웨이로 구성하면 통신 부하의 감소와 방화벽의 특성을 가지도록 구성할 수 있음을 보였다.

또한 내부망이 외부망보다 적은 트래픽이 발생됨을 보였다. 많은 클라이언트가 존재하는 외부망의 트래픽이 내부망 보다 2.5배 적기 때문에 기존의 방화벽을 사용하는 침입 탐지 시스템보다 트래픽 분산에 대해 더 효율적임을 보였다. 따라서, 트래픽 감소에 따른 대역폭의 증가와 중복된 프락시 기능을 없애줌으로 처리 지연시간이 감소하고 고속 전송이 가능한 침입차단 시스템을 구성할 수 있으며, 방화벽 설치비용을 절감할 수 있다.

내부의 스크린드 라우터와 외부의 스크린드 라우터에 접근제어목록은 라우터에서 제공되는 소프트웨어에 따라 차이는 있으나 다양한 종류의 방법이 개발되고 있기 때문에 보안정책에 따라 더 세분화 할 수 있고 다양하게 구현 할 수 있음이 기대 된다.

앞으로는 효과적인 로깅(logging)과 함께 침입차단과 탐지에 대한 방법도 같이 고려된 시스템 구성에 대한 연구가 있어야 할 것이다.

참 고 문 헌

[1] 송관호, 이병만, "전산망 안전보안에 관한 연구", 한국전산원, 1996.

[2] 정국환, "우리나라 인터넷 동향, 전망 및 발전방향 연구", 한국전산원, 1996.

[3] 조유근, 박근수, "인터넷을 위한 방화벽 및 네트워크 통신보호시스템 연구", 서울대학교, 1998.

[4] MBS정보화연구소, "3층 클라이언트/서버 시스템 구축 기법", MBS정보화연구소보고

[5] Douglas E. Comer, Internetworking With TCP/IP Volume 1: Principles Protocols, and Architecture, Prentice Hall, 2000.

[6] 박웅기, 손기욱, 정현철, "전산망 보호를 위한 방화벽 시스템", 주간기술동향(ETRI) 748호, 1996.

[7] 임채호, "중요 정보통신망 해킹시 침입자기법 분석과 대응", 한국정보보호센터, 1999.

[8] 한국전산원, "전산망 보안관리를 위한 지침서", 1995.

[9] 한국정보보호센터, "정보통신망 침입차단 시스템 평가기준", 1998.

[10] PLUS(포항공대 유닉스 보안연구회), Security PLUS for UNIX, 영진닷컴, 2000.

[11] Douglas E. Comer, Internetworking With TCP/IP Volume III: Client-Server Programming and Applications, Linux/POSIX Socket Version (with D. Stevens), Prentice Hall, 2000.

[12] David Dittrich, "The DoS Project's 'trinoo' distributed denial of service attack tool", October 21,1999,(http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt)

[13] David Dittrich, "The "Tribe Flood Network" distributed denial of service attack tool", October

21, 1999, (http://staff.washington.edu/ dittrich/misc/tfn.analysis.txt)
[14] Douglas E. Comer, Internetworking With TCP/IP Volume II: Design, Implementation, and Internals (with D. Stevens), Prentice Hall, 1999.
[15] John Bloomer, Power Programming with RPC, O'Reilly&Associates, Inc., 1992.
[16] Packet Storm Security Archives, "Distributed Attack Tools",(http://packetstorm.securify.com/distributed/)
[17] Simple Nomad, "Strategies for Defeating Distributed Attacks", 2000, (http://www. hideaway.net/Server_Security/Library/Denial_of_Service/dos/strategies.htm)
[18] David Dittrich, "The "stacheldraht" distributed denial of service attack tool", December 31, 1999,(http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt)
[19] NightAxis and Rain Forrest Puppy, "Packet Storm Contest Entry - Purgatory 101: Learning to cope with the SYNs of the Internet", (http://packetstorm.securify.com/papers/contest/RFP.doc)
[20] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", (Internet RFC/STD/FYI/BCP Archives : rfc2267), January 1998, (http://www.landfield.com/rfcs/rfc2267.html)

저 자 소 개

홍현술(Hyeun-Sool Hong)
1985년 원광대학교 경영학과 학사
1987년 원광대학교 대학원 경영학과 경영학석사
1990년 원광대학교 대학원 전자계산기공학과 공학석사
2001년 원광대학교 대학원 컴퓨터공학과 공학박사
1989~현재 원광보건대학 컴퓨터응용개발과 교수
※관심분야 : 객체지향시스템, 디자인패턴, 컴퓨터교육, WBI, 인터넷정보기술

정민수(Min-Soo Jung)
1992년 원광대학교 전자계산공학과 학사
2001년 원광대학교 정보과학대학원 석사
1995~현재 원광대학교 정보전산원 근무
※관심분야 : 라우팅 및 스위치를 이용한 통신, XML, C/S 환경, LDAP

한성국(Sung-Kook Han)
1979년 인하대학교 전자공학과학사
1981년 인하대학교 대학원 전자공학과 공학석사
1988년 인하대학교 대학원 전자공학과 공학박사
1984~현재 원광대학교 전기전자 및 정보공학부 교수
※관심분야 : 인공지능(자연언어처리), 정보공학, 인지과학, 객체지향시스템, 컴파일러, WBI, 인터넷정보기술