게이트웨이 모드와 브리지 모드를 동시에 지원하는 침입차단시스템 구현에 관한 연구

박창서*
*동양대학교

A Study of Implementation of a Firewall that Using the both Gateway Mode and Bridge Mode

Chang-Seo Park*
*DongYang University
E-mail : totalpark@empal.com

요 약

인터넷의 급속한 발전으로 네트워크 보안을 위하여 침입차단시스템의 사용이 보편화 되고 있다. 최근에 많이 사용되고 있는 Linux나 FreeBSD 커널(Kernal) 기반의 침입차단시스템은 게이트웨이 모드(Gateway Mode)와 브리지 모드(Bridge Mode)를 선택적으로 지원한다. 본 연구에서는 FreeBSD 커널에서 게이트웨이 모드와 브리지 모드를 동시에 지원하는 침입차단시스템을 구현하였다. 응용서비스(Application Service)에 대하여 별도의 프록시(Proxy) 없이 침입차단시스템을 구축할 수 있는 확장성이 뛰어난 네트워크 구축 방안을 제안한다.

ABSTRACT

Because of the rapid growth of Internet, the firewall is generally used to protect the network security. The firewall on Linux or FreeBSD Kernal, which is widely used, supports either Gateway or Bridge Mode. In this study, we present the firewall which supports simultaneously Gateway and Bridge Mode. For the application service, it is suggested that the firewall which has excellent expandability can construct a network without another proxy.

키워드
Firewall, Gateway Mode, Bridge Mode, FreeBSD Kernel

Ⅰ. 서 론

인터넷이 활성화 되면서 네트워크 보안을 위하여 침입차단시스템의 도입이 보편화 되었다. 침입차단시스템을 사용하는 목적은 정당한 권한을 갖지 않는 사용자가 내부 네트워크의 자원에 접근하려는 시도를 차단하고 기밀성을 가지는 정보가 외부로 유출되는 것을 방지하는데 있다[1]. 침입차단시스템의 적용기술에 따라서 패킷 필터링 게이트웨이(Packet Filtering Gateway) 방식과 프록시(Proxy)를 사용한 어플리케이션 프록시 방식(Application Proxy) 방식으로 구분할 수 있으나 대부분의 시스템은 이 두가지 방식을 모두 포함하는 혼합형(Hybrid)을 사용하고 있다[2]-[4]. 패킷 필터링 방식은 단순히 패킷헤더(Packet Header)의 정보만 검사하는 방식 보다 내용까지 해석하는 스테이트풀 인스펙션(Sateful Inspection) 방식을 사용한다. 스테이풀 인스펙션 방식은 네트워크 계층(Network Layer)에서 접속을 가로채어 인스펙션 엔진에 전달하고 어플리케이션 계층(Application Layer)로부터 정책 결정에 필요한 상태관련 정보를 다이나믹 스테이트 테이블(Dynamic State Table)에 보관하고, 이후에 들어오는 접속에 대해서 이것과 비교해서 통과여부를 결정하게 된다. 기

본적으로 다이나믹 패킷 필터링을 사용하지만 어플리케이션 데이터에 대해서는 적은 부하를 들여서 해석하는 속도가 빠른 장점이 있다. 하지만 프로토콜별로 세부적인 제어를 하는데 있어서는 어플리케이션 프록시에 미치지 못한다. Linux와 FreeBSD 커널에서는 패킷 필터링이 동작하는 계층에 따라서 네트워크 계층에서 동작하는 게이트웨이 모드와 데이터 링크 계층(Data Link Layer)에서 동작하는 브리지 모드가 있다[5][6]. 게이트웨이 모드는 네트워크 구성시 DMZ(Demilitarized Zone) 구성이 가능하고 NAT(Network Address Translation) 기능을 구현할 수 있다. 하지만 VoIP 등의 특정 어플리케이션 서비스를 위해서는 반드시 프록시가 제공되어야 한다. 반면에 브리지 모드는 DMZ와 NAT를 구성을 할 수 없으나 침입차단시스템을 설치하기 위하여 게이트웨이 모드처럼 네트워크 구성을 변경하지 않고 마치 허브(Hub)를 설치하듯이 기존의 네트워크의 적당한 위치에 설치하면 된다. 따라서, 공인 IP(Internet Protocal)를 사용하고 있으며 DMZ를 반드시 구축할 필요가 없는 환경에서는 처리속도가 빠른 브리지 모드를 선호한다.

본 연구에서는 FreeBSD 커널[7] 기반에서 기존의 침입차단시스템이 패킷 필터링을 위하여 게이트웨이 모드나 브리지 모드 중에서 선택적으로 지원하는 불편함을 제거하고 네트워크 구성시 확장성을 뛰어난 게이트웨이-브리지 모드의 침입차단시스템 구축 방안을 제안한다.

II. 설계 및 구현

그림 1은 FreeBSD 커널의 네트워크 스택(Network Stack)에서 IP 처리 모듈을 추가해서 입력되는 패킷이 커널에서 패킷 필터링 정책과 비교하여 통과여부를 결정한다. 통과된 패킷에 대하여 별도의 처리가 필요 없는 경우에는 커널에 있는 경로 설정 테이블(Routing Table)에 의해서 전송되어야 할 인터페이스를 지정받아 전송된다.

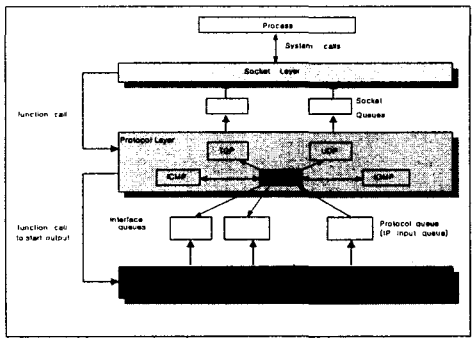

그림 1. FreeBSD 커널에서 네트워크 스택
Fig. 1 The Network Stack on the FreeBSD Kernel

만약 특별한 처리가 필요하다면 패킷은 해당하는 프로세스로 전송되어 해당 프로세스의 처리를 받아 다시 커널로 보내져 전송 절차를 따른다.

그림 2는 게이트웨이-브리지 모드의 커널 구조를 나타낸 것이다. 서로 다른 이더넷 인터페이스(Ethernet Interface)를 통하여 패킷을 입력받아 패킷 필터링 정책을 거쳐서 각각 별도의 이더넷 인터페이스로 전송된다.

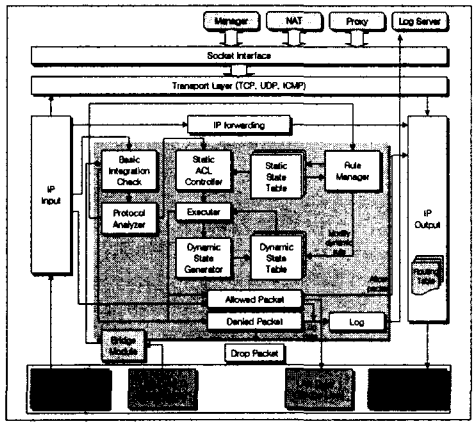

그림 2. 게이트웨이-브리지모드 커널 구조
Fig. 2 Kernel Configuration of Gateway -Bridge Mode

그림 3은 OSI(Open Systems Interconnection) 계층에서 스테이트풀 인스펙션의 동작상태를 표시한 것으로 데이터링크 계층에서 동작하는 브리지 모드와 네트워크 계층에서 동작하는 게이트웨이 모드가 각각 패킷을 인스팩트 엔진(Inspect Engine)으로 전달하는 것을 보여준다.

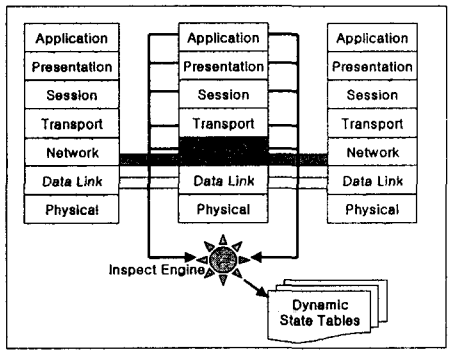

그림 3. 게이트웨이-브리지모드의 스테이트풀 인스팩션 동작
Fig. 3 Stateful Inspection Operation of Gateway-Bridge Mode

그림 4는 게이트웨이-브리지 모드로 구성된 침입차단시스템을 나타낸다. 게이트웨이 모드에는 3

개의 이더넷 인터페이스를 지원하고 브리지 모드에서는 2개의 이더넷 인터페이스를 제공한다. 따라서 하나의 커널상에서 마치 2개의 침입차단시스템이 동작하는 것과 같다.

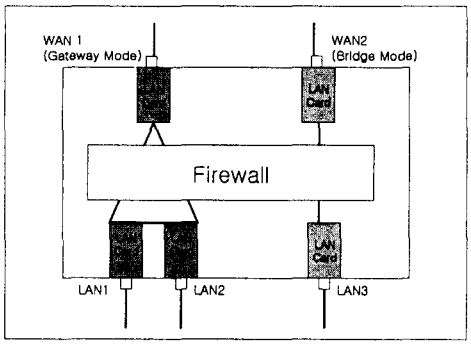

그림 4. 게이트웨이-브리지 모드 침입차단 시스템 구성도
Fig. 4 Firewall Configuration of Gateway -Bridge Mode

그림 5는 실제로 게이트웨이-브리지 모드의 침입차단시스템을 네트워크 상에서 구축한 경우를 나타낸다. 각종 응용서버들을 공인 IP 사용해서 브리지 모드로 연결하면 별도의 프록시 없이 보안성을 확보할 있으며 일반 사용자가 사용하는 클라이언트들은 기존의 게이트웨이 모드와 동일하게 NAT 사용하여 보안성을 높일 수 있다.

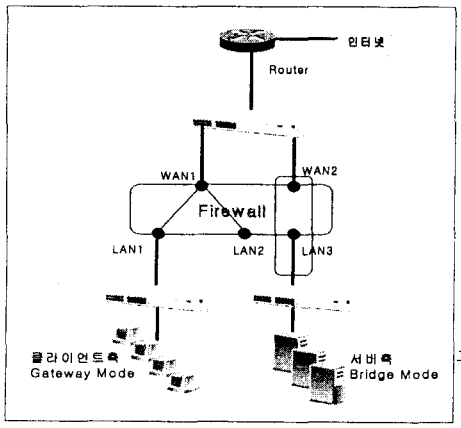

그림 5. 게이트웨이-브리지 모드의 침입차단 시스템을 사용한 네트워크 구성도
Fig. 5 Network Configuration used the Firewall of Gateway-Bridge Mode

III. 결 론

기존의 침입차단시스템이 게이트웨이 모드나 브리지 모두 중 한가지를 선택적으로 사용하여야하는 불편함을 제거하기 하기위하여 하나의 FreeBSD 커널에서 독립적인 이더넷 인터페이스를 활용하여 2가지 모두를 동시에 지원하였다. 침입차단시스템이 설치된 네트워크에서 VoIP 서버와 같이 별도의 프록시가 요구되는 경우에도 제안한 시스템을 사용하여 네트워크를 구축할 경우 전혀 문제가 없다. 따라서 새로운 어플리케이션에 따른 침입차단시스템에서 프록시를 추가로 개발해야 되는 문제점을 제거 할 수 있다. 나아가 메트로 이더넷(Metro Ethernet) 스위치처럼 복수개의 이더넷 인터페이스를 제공하는 단말에 효율적으로 적용할 수 있으며 침입차단시스템의 처리속도를 2배로 높일 수 있다.

참고 문헌

[1] M. J. Ranum, "Thinking about Firewalls", Proceedings of the International Conference On Systems and Network Security and Management, 1993.

[2] W. R. Chewick and S. M. Bellovin, "Firewalls and Internet Security", Addsion-Wesley, 1994.

[3] Karanjit Siyan, "인터넷 방화벽과 네트워크 보안", 이한출판사, 1996.

[4] D. Brent Chapman, "인터넷 방화벽 구축하기", 한빛미디어, 1999.

[5] 이주택, 배민호, 박미영, "네트워크 보안과 방화벽 구축", 가남사, 2002.

[6] 최준호, 김승영, 오준선, 편용현, "About FreeBSD", 영진닷컴, 2001.

[7] Marshall Kirk McKusick, Keith Bostic, Michael J. Karels, John S. Quarterman, "The Design and Implementation of the 4.4 BSD Operation System", Addison Wesley, 1996.