효율적인 다중 서버 운영을 위한 리눅스기반 통합 보안시스템 설계 및 구현

정성재, 유두훈, 장희진, 소우영
한남대학교 컴퓨터공학과

Design and Implementation of Integrated Security System based on Linux for Efficient Multi-Server Operation

Sung-Jae Jung, Du-Hun You, Hui-Jin Jang, Woo-Young Soh
Dept. of Computer Engineering, HanNam University

요 약

리눅스는 오픈 소스로서 관련 소프트웨어 비용이 거의 들지 않아 여러 대의 서버를 구축하는 데도 많은 비용 부담 없이 적기 때문에 리눅스를 이용한 다중 서버 사용이 점차 증가하고 있다. 그러나, 다중 서버 사용 시 최적화된 서버관리와 인터넷상의 서버 노출에 따른 보안 등의 문제가 고려되어야 한다. 본 논문에서는 리눅스 커널(Kernel) 2.4 기반의 다중 리눅스 서버 구성에서 발생할 수 있는 부하분산(Load Balancing)과 보안상의 문제를 iptables의 패킷 필터링 및 방화벽 기능을 이용하여 효율적으로 운영할 수 있는 방법을 제시하고, 또한 공개용 침입탐지시스템인 snort를 이용한 통합 보안 시스템을 구현하고 그 활용방안을 제안하고자 한다.

1. 서론

초기의 리눅스는 주로 개인이나 중소기업에 의해 비용 부담을 덜기 위해 서버 운영체제로 사용되었으나 최근에는 한 대의 서버에 웹, 메일, DNS(Domain Name System) 등의 기능을 통합한 서버로 구성하거나 또는 PC급 하드웨어와 공인 IP(Internet Protocol) 주소 하나만으로도 손쉽게 서버를 구축할 수 있게 되었다. 그러나 최근에는 초고속 인터넷망의 확충과 더불어 인터넷사용자의 급증으로 1대의 서버에서 모든 서비스를 처리할 수 없게 되었다. 이러한 변화로 리눅스를 이용한 서버구축도 1대의 서버를 이용한 서비스에서 여러 대의 서버를 통한 서비스가 보편화되어 가는 추세이다[1]. 다중 서버를 통한 서비스는 서비스 이용자들에게는 좀 더 빠르고 다양한 서비스를 받을 수 있지만 서버 운영자들에게는 최적화된 서버관리를 위한 방법과 더불어 안전한 서비스를 위해 보안관리 문제를 해결해야 한다.

리눅스는 오픈 소스에 기반을 두고 많은 사람들이 응용 소프트웨어를 개발 함으로써 다양하고 강력한 도구들이 많이 제공된다. 본 논문에서는 리눅스 도구 중 다중서버를 효율적으로 관리할 수 있고 방화벽 및 패킷필터링 기능이 있는 iptables를 이용하여 최적화된 관리 및 보안 기법을 제시하고, 아울러 snort라는 공개용 침입탐지도구를 추가하여 침입차단 및 침입탐지를 동시에 사용가능한 통합보안시스템을 구현하고자 한다. 또한 이 보안시스템을 다중 서버 구축 상황에 맞게 이용할 수 있는 방법을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장은 iptables와 리눅스 서버 구성에 대하여 소개하고, 3장에서는 방화벽 프로그램인 iptables을 이용하여 부하분산을 통한 효율적인 서버관리 방법을 제시한다. 4장에서는 snort를 이용하여 침입차단 및 침입탐지가 가능한 통합보안시스템을 제안하고, 5장에서는 구성된 통합보안시스템의 활용방안에 대하여 논하고, 6장에서 결론을 맺는다.

2. iptables 와 리눅스 서버 구성

2.1 iptables에 대하여

리눅스는 오픈 소스에 기반을 두고 있는 운영체제로서 관련 도구들도 공개용 프로그램이 많다. 이 중에서 다중 서버 운영 및 보안을 위한 기능을 가진 도구로 iptables가 있다. 리눅스 커널 2.4에서 패킷필터링 및 방화벽 기능을 하는 iptables는 대상 보안영역으로 설정된 서브넷(Subnet)상의 패킷을 헤더(Header) 내용에 따라 필터링하는 기능을 포함하고 있으며, 이 패킷 필터링 기능을 이용하여 방화벽을 구현할 수 있다. 또한 하나의 IP로 여러 대의 시스템을 공유하여 동시에 인터넷을 사용하거나, 반대로 하나의 IP로 여러 대의 서버를 운영하도록 구성할 수 있다. 하나의 IP를 가지고 인터넷을 공유하거나 다중 서버로 사용가능하게 하는 기술을 NAT(Network Address Translation)이라고 한다. iptables에서의 NAT는 SNAT(Source NAT)와 DNAT(Destination NAT)로 나뉜다. SNAT는 하나의 IP로 여러 대의 시스템이 인터넷을 공유하는 것을 의미 한다. 예를 들면 사설 IP가 부여된 시스템이 인터넷을 사용하여 특정 목적지에 도착하기 전에 공인 IP로 변환시켜 주며, DNAT는 하나의 공인 IP에 여러 대의 서버를 구현하는 것은 말한다. DNAT는 외부의 특정 클라이언트의 요청이 오면 방화벽에 부여된 공인 IP로 패킷이 들어오며 이 패킷을 보고 만약 웹서비스 요청이면 사설 IP가 부여된 서버 중 웹서버로 목적지 주소를 바꿔주는 기술을 말한다. 본 논문에서는 다중서버의 효율적인 운영과 보안을 위해 iptables의 DNAT기술을 이용하여 하나의 공인 IP로 여러 대의 서버를 운영할 경우 발생할 수 있는 부하분산 방법과 다중 서버의 보안 방법[2][7-9]에 초점을 두고 있다.

2.2 리눅스를 이용한 일반적인 서버구축

초기의 리눅스 서버 구축에서는 일반적으로 하나의 서버에 DNS서버, 웹서버, 메일서버 등을 모두 같이 사용하도록 구현하였다. 그러나, 인터넷 인구의 폭발적인 증가와 다양한 멀티미디어 컨텐츠 사용으로 인하여 하나의 서버에서 모든 기능을 수행하기에는 점차 어려워지는 추세에 있다. 현재는 여러 대의 서버에 공인 IP를 부여하고 각각 웹서버, 메일서버, DNS 서버 등의 형태로 나눈다. 이 경우 각 서버가 독립적으로 기능을 수행하므로 단일 서버에 비해 클라이언트에게 좀 더 빠른 서비스를 제공할 수 있는 장점이 있다. 그러나, 서버 관리자의 입장에서 보면 DNS서버의 zone 파일을 많이 수정해야 하며, 외부에 노출되어 있는 여러 대의 서버를 동시에 관리해야 되므로 서버의 보안 관리 문제 등의 단점이 있다[3].

2.3 iptables을 이용한 다중 서버 구축

본 논문에서 제안하고자 하는 다중 서버의 부하 분산 방법은 iptables의 패킷 필터링 기능을 이용하여 여러 대의 서버를 그 운영 목적과 기능에 따라 역할을 분담케 하는 것이다. 이 경우 iptables의 방화벽 기능을 이용하여 부하 분산과 동시에 서버의 보안을 강화할 수 있다.

[그림 1]은 이와 같이 방화벽을 기준으로 공인 IP와 사설 IP로 나누어 서버를 구축하는 예를 보이고 있다. NIC(Network Information Center)에 등록된 공인 IP에 리눅스 방화벽을 설치하고 하나의 이더넷 카드를 추가로 장착하여 사설 IP를 부여한다. 허브(Hub)를 사용하여 방화벽에 부여된 사설 IP와 각 서버들을 연결시킨다. 방화벽에서는 들어오는 패킷들을 분석하여 요구되는 응용 서비스를 미리 정해진 서버들의 역할에 따라 해당 서버에 연결함으로써 부하를 분산시킨다[4].

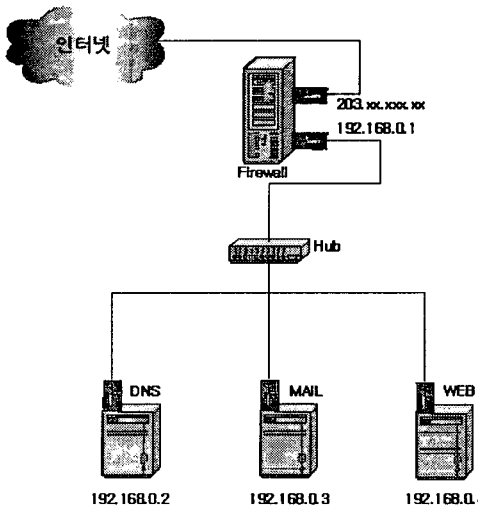

그림 1. iptables를 이용한 부하분산

이 경우 부하 분산은 다음과 같이 이루어진다. DNS 서버로 등록된 공인 IP를 가진 시스템에 리눅스와 iptables를 설치하고 방화벽으로 사용한다. 외부에서 웹서비스 요청은 80번 포트로 들어오므로 80번 포트로 들어오는 요청을 192.168.0.4로 보내고, 메일관련 요청은 25번 포트와 110번 포트로 들어오므로 192.168.0.3으로 보내고, DNS 조회는 53번 포트로 들어오므로 192.168.0.2 서버로 보낸다. 따라서 각각의

서버들은 해당 요청 이외의 다른 서비스에 대해서는 응답할 필요가 없게 된다. 즉, 웹 서버는 웹 서버 관련 프로그램만 작동시키고 포트도 80번 포트만 열어두고, DNS서버는 DNS서버 관련 프로그램과 53번 포트만 열어두면 되므로, 다른 서비스에 대한 포트를 열거나 데몬 프로세스를 작동시킬 필요가 없어지므로 부하 분산과 더불어 다중 서버의 보안상에도 매우 안전하므로 시스템을 안전하고 효율적으로 관리할 수 있다[5].

3. iptables를 이용한 다중 서버 장단점

전술한 바와 같이 방화벽을 이용한 부하 분산 방법은 다음과 같은 장점이 있다. 첫째, 서버들에 대한 보안상의 안전성이다. 방화벽 안쪽에 서버들이 사설 IP로 관리되기 때문에 외부에서 해당 서버들로의 직접 접근이 불가능하고 방화벽에서 필요한 서비스 포트, 프로토콜 및 내·외부의 사용자 접속에 대한 허가/차단 기능을 수행 할 수 있어 다양한 형태로 최적화된 서버를 구현할 수 있다. 둘째, 공인 IP 하나로 구현할 수 있기 때문에 IP 부족 현상으로 인한 서버 증설의 어려움도 해결할 수 있으며, 사설 IP이므로 추후 서버 증설의 어려움을 줄일 수도 있다. 셋째, 보안 관리상의 업데이트가 요구될 경우에 방화벽 서버만 업데이트하면 되므로 용이하게 불법 침입의 피해를 줄일 수 있다. 또한 각각의 서버 업데이트도 용이하다. 웹서버에 문제가 발생하더라도 다른 메일서버나 DNS 서버의 서비스 중단없이 해당 웹서버만 해결하면 되므로 문제 해결과 업데이트가 매우 용이하다. 넷째, 계정관리 측면에서도 매우 편리하다. 만약 메일 계정 이외에 다른 접속이 없다면 메일서버에만 계정등록을 하면 되므로 다른 서버에 불필요한 계정 생성과 접근도 막을 수 있다. 다섯째, 방화벽에서는 접속되는 포트를 보고 포워딩을 시켜주므로 서버의 구축 운영시 메일서버는 솔라리스, DNS서버는 윈도우2000 등으로 변경이 용이하고, 서로 다른 운영체제의 웹서버를 구현할 수도 있다[6].

단점으로는 첫째, 방화벽에서는 들어오는 포트만 보고 포워딩 시켜주므로 해당 서버가 정상적으로 작동되지는 여부는 점검하지 않는다. 즉 웹서버를 192.168.0.10부터 192.168.0.12번까지 3대를 가동한다고 했을 때 방화벽에서는 80번 포트로 들어오는 웹서비스 요청에 대해 192.168.0.10 부터 192.168.0.12 번까지 순차적으로 분산한다. 이 경우 만약 192.168.0.11번 웹서버가 작동을 하지 않는다면 방화벽에서는 이 서버의 작동 유무를 체크하지 않으므로 외부의 웹서비스 요청자가 작동하지 않는 서버로 연결되어 서비스 연결이 되지 않을 수도 있다. 물론 reload를 하면 다른 웹서버로 연결되겠지만 계속적으로 작동하지 않는 서버로 연결될 수도 있다. 둘째, 방화벽에서는 열어놓은 해당 포트로 불법적인 침입시도를 감지하지 못한다. 방화벽에서는 해당 포트, 예를 들면 웹서비스 포트인 80포트를 열거나 닫을 뿐이지 해당 포트로 접속하는 패킷이 정상적인 패킷인지 불법적인 침입시도를 위한 패킷인지를 감지하지 못한다.

4. snort를 이용한 침입탐지시스템

iptables의 방화벽 기능만을 이용하면 방화벽에서 허가한 포트로 들어오는 침입시도는 감지하지 못하는 단점이 있다. 리눅스에서 이러한 침입시도를 탐지해내는 공개용 프로그램으로 snort가 있다. snort는 일종의 침입 탐지 시스템이다. 침입탐지시스템이란 특정한 로그 패턴을 분석하여 침입 시도나 침입에 대한 신속한 탐지와 대응이 이루어지도록 해주는 시스템이다.

snort는 실시간 트래픽 분석, 프로토콜 분석, 내용 검색/매칭을 수행할 수 있으며, 침입탐지 규칙에 의거하여 오버플로우, 포트스캔, CGI공격, OS확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있다. 또한 침입탐지 규칙은 지속적으로 사용자모임에 의해 업데이트되거나 사용자가 직접 규칙을 작성하여 추가할 수 있도록 설계되어 있으므로 최신 공격에 대한 적응에 빨리 대체할 수 있다. snort를 iptables가 설치된 방화벽에 같이 설치/운영하게 되면 부하분산을 통한 효율적인 다중서버 운영뿐만 아니라 침입차단 및 침입탐지 기능을 수행하는 통합 보안 시스템을 구성할 수 있다[10]. 즉 iptables의 방화벽기능만 가지고 침입차단만 하게 되면 해당포트에 대한 허가/거부만을 할 뿐이지 해당 포트로 들어오는 패킷에 대한 선별을 하지 않는다. 악의적인 목적을 가지고 접근하는 패킷이라고 하더라도 방화벽에서 허가한 포트이면 접근이 가능하다. 이러한 방화벽의 단점을 snort를 이용하면 로그패턴을 분석하여 방화벽에서 허가된 포트로 접속을 시도하는 패킷이라도 악의적인 목적을 가진 패킷들의 특정한 패턴을 가지고 비교하고, 패턴이 침입탐지를 위한 패턴과 일치하게 되면 거부하도록 한다.

5. 통합보안시스템의 활용방안

침입차단 기능과 침입탐지 기능을 한 시스템에 구현

해도 운영해도 되지만 두 가지 기능을 한 시스템에 운영하면 프로세스 처리속도도 느려지고 효율성도 약간 떨어지므로, 두 기능을 각각의 시스템으로 구현할 수 있다[그림2].

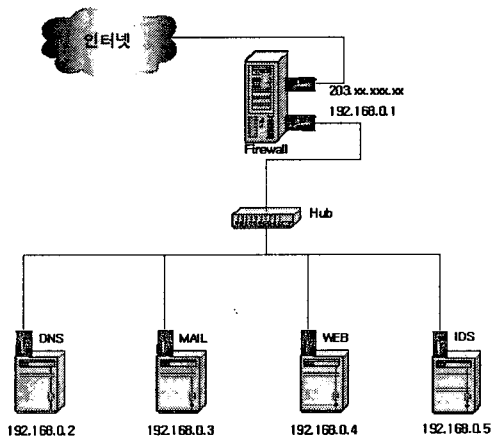

그림 2. 통합보안시스템의 구현

침입탐지 기능을 하는 시스템을 여러 서버들과 같이 사설 IP를 부여하여 내부에서 다중 서버들의 로그분석을 통하여 관리할 수 있다. 이러한 침입탐지시스템을 독립적으로 구현하면, 침입차단 및 침입탐지기능을 한 시스템으로 구현함으로서 발생할 수 있는 부하를 줄일 수 있게 된다. 이렇게 시스템 부하를 줄이게 되면 해당 시스템에 새로운 기능을 추가하여 운영할 수도 있게 된다. 즉 침입탐지기능이 구현된 시스템을 방화벽 및 내부의 여러 서버들을 실시간으로 상황에 따라 정책을 내릴 수도 있고, 효율적인 운영을 위한 관리시스템으로써의 구현도 가능하다.

6. 결론

iptables를 이용하여 다중 서버를 구축할 경우 서버의 부하 분산을 가능하게 하여 효율적인 서버 운영의 방법을 제공하며, 방화벽 기능도 하여 서버를 안전하고 편리하게 관리할 수 있는 효율적인 방법이 될 수 있다. 그러나 iptables는 패킷에 대하여 설정된 정책에 따라 거부하거나 허가할 뿐 침입을 시도하는 탐지기능은 가지고 있지 못하다. 이러한 방법을 해결하려면 snort라는 프로그램을 방화벽에 추가로 설치하여 침입차단 및 침입탐지가 가능한 통합보안시스템으로의 구현이 가능하다.

침입탐지의 효율성을 높이고 방화벽과 내부에 있는 다중 서버들의 효율적인 관리를 위해 침입탐지시스템을 단독으로 구축할 수도 있다. 이 시스템을 이용할 경우 침입이 발생하면 방화벽에 자동적으로 거부정책을 내리도록 할 수 있으며, 또한 내부적으로 존재하는 웹서버, 메일서버, DNS서버에 접근하여 제어할 수 있는 유일한 관리시스템으로의 구현도 가능하다.

리눅스 기반에서 iptables를 이용한 부하 분산 방법 및 방화벽 기능, snort를 이용한 침입탐지기능을 통합하면 다중 서버를 효율적으로 관리할 수 있는 통합보안 시스템을 구현할 수 있다. 이러한 통합 보안시스템은 리눅스를 이용한 다중 서버의 기능을 향상시키고 보안기능도 높여 효율적이고 안전한 다중 서버를 구현하는데 유용한 방법으로 활용될 수 있을 것이다.

[참고문헌]

[1] Matt Welsh, Matthias Kalle Dalheimer & Lar Kaufman, "Running Linux, 3rd Edition", O'Reilly, 2000

[2] Robert L. Ziegler, "Linux Firewalls", New Riders, 2000

[3] Brian Hatch, James Lee, Geooge Kurtz, "Hacking Linux Exposed", McGraw-Hill, 2001

[4] Elizabeth D. Zwicky, Simon Cooper, & D. Brent Chapman, "Building Internet Firewalls", O'Reilly, 2000

[5] Ed Skoudis, "Counter Hack", PHPTR, 2002

[6] Joel Scambray, Stuart McClure, George Kurtz, "Hacking Exposed Second Edition", McGraw-Hill, 2001

[7]http://www.linuxguruz.org/iptables/howto/iptables-HOWTO.html

[8]http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html

[9]http://kldp.org/Translations/html/Virtual_Server-KLDP/VS-NAT.html

[10]http://kldp.org/HOWTO/html/Snort-Statistics-HOWTO/