Linux방화벽 환경에서 Secure Shell(SSH)의 Port Forwarding을 이용한 안전한 서버 구성

임준형° 이종철
서경대학교 전산정보관리학과
{saster, jclee}@bukak.skuniv.ac.kr

Secure Server Configuration Using Secure Shell(SSH) Port Forwarding Behind Linux-based Firewall

Joon-Hyung Lim° Jong-Chul Lee
Dept. of Computer Information Management, Seokyeong University

요 약

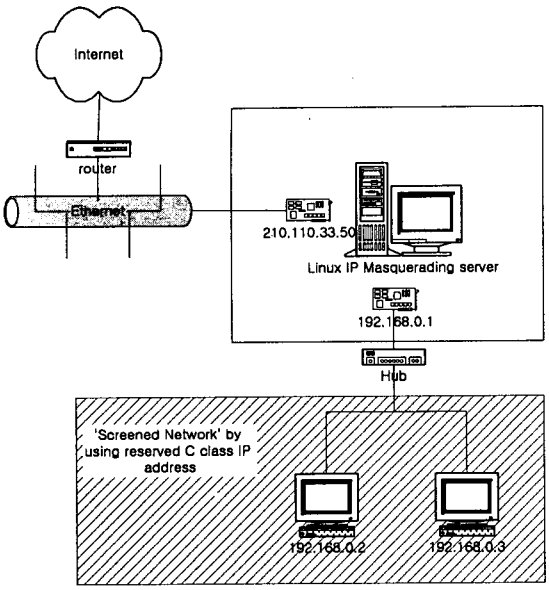
인터넷환경에서 네트워크구축이 보편화된 요즈음, 보안문제가 이슈로 대두되고 있다. 대형 네트워크상에서는 벌써 수년 전부터 방화벽이 보안장비의 중추를 담당하며 사용되고 있으나, 중소규모의 네트워크 환경을 유지관리하기 위한 보호대책은 미비한 편이다. 특히 라우터 전후에서 기능을 하는 방화벽 외에 대형 네트워크 안에서 중소규모의 네트워크를 운영 하고자 할 때, 새로운 방화벽서버를 사용할 수 있다면, 작은 규모의 네트워크에 적합한 패킷필터링이 가능하여, 외부의 침입으로부터 좀 더 안전한 네트워크의 구성이 가능해진다. 본 논문에서는 상대적으로 비용이 저렴하고 setup이 간단한 Linux방화벽을 통해 외부망에서 접근할 수 없는 사설(private)IP주소를 사용하는 사설망(Private Network)안에 서버를 구성했을 때, Secure Shell에서 지원하는 Port forwarding기능을 사용하여, 사설망안에 위치한 웹서버, 메일서버등에 접근할 수 있는 방법을 제시하고자 한다.

1. 서론

1년여 전부터 시작된 Linux 보급 열풍에 힘입어 상대적으로 저렴한 가격의 pc급 서버들이 급격히 증가하고 있어 대규모 네트워크 안에서도 곳곳에 웹서버 등을 중심으로 소규모 네트워크 구축이 활성화되고 있다. 하지만, 일반적인 대형 네트워크 곳곳에 위치한 이런 공인된 IP 주소[1]가 부여된 Linux 서버들은 자칫 관리를 소홀히 하면, 전체 네트워크에 심각한 '보안 헛점'(security hole)이 될 수 있다. 대형 네트워크를 관리하는 관리자가 모든 Linux서버의 위치를 파악하고, 전체 네트워크의 방화벽을 강도 높게 설정할 수도 있겠으나, 이로 인해 전체 네트워크의 성능 저하가 예상되기 때문에, 어쩔수 없이 기본적인 방화벽 정책만을 유지하는 것이 일반적이다. 본 논문에서는, 네트워크상의 Linux서버가 보안헛점이 되는 것을 방지하기위해 Linux방화벽에 의해 외부망과 완전히 차단된 사설 IP 주소를 사용하는 사설망(private network)을 구성하고 내부에 각종 서버들을 두었을 때, 외부망에서 사설망 안에 있는 서버의 특정서비스에만 접근할수 있도록, Secure Shell의 port forwarding 기능을 이용하여 안전한 서버를 구성하는 방안에 대해 기술 한다.

2. IP Masquerading

Linux를 이용하면 NAT(Network Address Translation)[2]의 한 종류인 IP Masquerading[4,5] 기능을 사용하여, 외부 인터넷망에 대해 완전히 가려지는 네트워크를 구성할 수 있다. 인터넷망에서는 사용할 수 없는, '예약된 IP 주소'[1]를 사용하여 사설 네트워크를 구성하고, 그 앞단에 IP Masquerading기능을 하는 Linux 서버를 구성하는 방법이다. 사설 네트워크안의 호스트들은 인터넷에 참여하기 위해 모두 IP Masquerading 서버에 할당된 공인된 IP 주소를 그 시작점으로 사용한다. 사설망에 있는 어떤 호스트가 외부 인터넷망으로 나가는 것은 NAT에 의해 가능하지만, 외부의 어떤 호스트가 사설망내의 어떤 호스트로 접근하는 것은 불가능하다. [그림 1]은 일반적인 IP Masquerading 구성도를 보여주고 있다. 인터넷상에서는 사용하지 않는, 예약된 C class의 IP 주소를 부여하여 외부에서 완전히 보이지않는 네트워크를 형성할 수 있다. 외부 네트워크에서는 사설망 내부를 볼수 없으나, 내부에서 외부로의 통신은 IP Masquerading 서버가 NAT기능을 수행하기 때문에 가능하다. 사설망 내부의 호스트들은 IP Masquerading에 의해 한번 가려지고, IP Masquerading 서버에서 방화벽 규칙 설정을 함으로써 다시 한번 보호된다.



[그림 1] IP Masquerading 구성도

2.1 Ipchains를 이용한 방화벽 구성.

Ipchains[3]는 Linux용 응용프로그램으로 입출력되는 모든 packet들을 미리 설정해둔 각종 규칙에 따라 filtering한다. Masquerading서버에서 ipchains를 사용함으로써 효과적인 Linux방화벽을 구성할 수 있다. Ipchains는 커널 2.1.102(개발버젼) 부터 사용가능하다.

2.2 사설망내에서 서버시스템의 운영.

웹서버나 메일서버등을 사설망내에 구성한다면, 방화벽의 영향아래 둘 수 있고, 또한 외부에서는 그 실체가 보이지 않으므로, 보안상으로도 좋은 효과를 기대할 수 있다.

2.3 IP Masquerading 환경의 문제점.

한 개의 공인 IP 주소를 가지고 NAT를 통해 사설망내의 여러 호스트들이 동시에 인터넷을 이용할 수 있고, 외부 네트워크에서는 직접적으로 가려진 호스트들이 보이지 않기 때문에, 직접적인 연결에 의한 보안상의 문제를 해결할 수 있는 장점이 있다. 하지만, 사설망 내부에 웹 서버나 메일 서버등을 구성 한다면, 이러한 서버들은 외부에서 접근할 방법이 없으므로 인터넷 서버로서의 기능을 상실하게 된다.

3. Secure Shell을 이용한 해결방안.

3.1 Secure shell(SSH)이란?

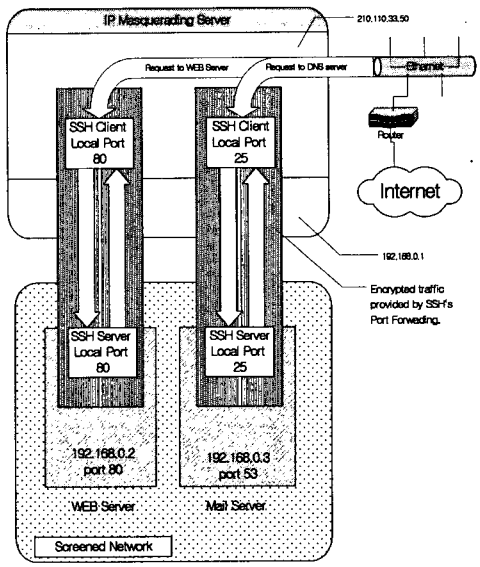
일반적으로 원격접속에 사용하는 telnet의 경우, 클라이언트와 서버사이에 오가는 모든 정보는 '평문(plain text)'으로 전달된다. 이는 Ethernet상에서 packet sniffing[7]공격이 행해지고 있다면, telnet 로그인시 입력하는 password까지 그대로 악의적인 해커에게 노출되게 되는 문제점이 발생한다. SSH[7]는 원격 시스템에 로그인해서 암호화된 연결을 해주는 프로그램 으로서, 22번 port를 사용하는 안전한 연결을 보장하는 telnet이라고 할 수 있다. 전송되는 모든 패킷에 3DES,RC4,Twofish[8] 등의 암호화 알고리즘을 사용하는 등, 일반적인 telnet연결보다는 훨씬 보안성이 높다. 일반적인 사용자 인증뿐만 아니라 두 호스트 사이에서의 인증을 위해 Public Key encryption 기법을 사용하기 때문에, session hijacking[7]이나 DNS spoofing[6,7] 공격을 막으면서 안전하게 원격 호스트에 로그인할 수 있다. 로그인을 위해서는 원격 호스트에 SSH 서버가 작동 중이어야 한다. 현재 SSH1 버전과 SSH2 버전이 나와있다.

3.2 Secure shell의 port forwarding기능을 이용한 사설망 내부의 서버 구성 방안.

본 논문에서는 방화벽 외부로부터 사설망 내부의 서버에게 들어오는 요청을 처리하기 위해서, SSH2의 port forwarding[7,8] 기능을 사용하는 방안을 제시하고, 이를 일반적인 외부로부터의 접속, 원격지에서의 관리자 접속, 안전한 POP3 접속의 세가지로 나누어 기술한다. [그림 2] 에서와 같이 Secure shell 은 클라이언트측(local)의 특정 port와 원격측의 특정 port를 지정하면, local측에 지정된 특정 port로 들어오는 모든 요청을 원격측의 지정된 port로 전달해주는, port forwarding 기능을 제공한다. 이를 사용해 사설망 내부에 각종 서버를 구성하면, 외부망에서는 서버의 실체가 보이지 않고, 서버들이 방화벽 후위에 위치한 효과를 얻을수 있다.

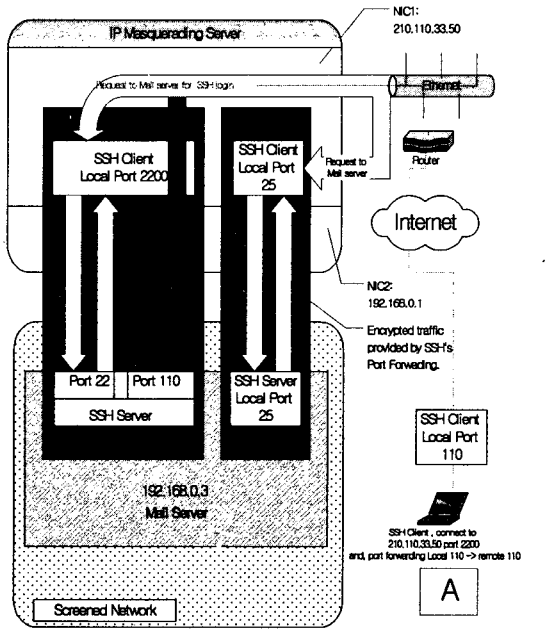
3.3 Port forwarding

[그림2] 는 다음과 같은 방법으로 구성할 수 있다.
Masquerading서버의 SSH 클라이언트에서,
ssh -l root -L 80 : 192.168.0.2 : 80 192.168.0.2
---- -- -------- -- --------
login (local port)(R address)(R port) R address
- (R: remote)



[그림 2] SSH를 이용한 port forwarding

위와 같이 실행함으로서, 가상망내의 web서버와 SSH접속을 하게되며, local측의 80번 port를 원격측의 80 port로 forwarding하게 된다.



[그림 3] 원격지에서의 관리 및 안전한 POP3연결

3.4 안전한 원격지 관리.

[그림 3]과 같이, 원격지에서 관리자가 사설망내의 서버를 관리할 필요가 있을 때, 방화벽 서버의 특정 port를 사설망내의 해당 서버의 22번 port로 forwarding시켜둔다면, 원격지의 관리자는 SSH2 클라이언트 프로그램으로 방화벽서버의 지정한 특정port에 접속하는 것만으로 사설망내의 서버에 접근할 수 있다. 메일 서버를 위한 관리용 port는 다음과 같이 열어둘 수 있다.

ssh -l root -L 2200:192.168.0.2:22 192.168.0.2

관리자는 이제 메일서버에 로그인 하기위해, 원격지에서 SSH 클라이언트를 사용해 Masquerading서버의 2200번 port로 접속하면 된다. 인터넷상의 원격지에서부터 사설망내의 서버까지 완전히 secure한 터널이 형성되는 것이다.

3.5 원격지에서의 POP3를 이용한 안전한 메일확인.

원격지에서 메일서버에 접속해 메일을 클라이언트 측으로 가져오는 POP3 역시 기본적으로 안전한 연결을 제공하지 않는다. [그림 3]에서와 같이, 원격지의 관리자가 메일서버에 도착한 메일을 POP3를 통해 가져 오고자 할 때 역시 SSH를 이용하여, A의 위치에서, 다음과 같이 하면 A의 110번 port가 메일서버의 110번 port와 연결된다.

ssh -l root -L 110:210.110.33.50:110 210.110.33.50 -p 2200

SSH연결 후, A의 관리자는 POP3 클라이언트 프로그램에서 접속할 메일서버 주소를 'localhost'로 지정함으로써 secure한 POP3연결을 할 수 있다.

4. 결론

본 논문에서는 소규모 네트워크의 보호를 위해, Linux에서의 NAT인 IP Masquerading을 이용한 방화벽을 구성하고, , SSH의 Port Forwarding기능을 적용하여, 방화벽 내부에 사설 IP를 사용하는 서버를 두었을 때, 외부로부터 오는 다양한 요청들을 처리하는 방안을 기술 하였다. 물론 IP Masquerading환경 하에서 사용할 수 있는 IPPORTFW[4] 와 같은 port forwarding프로그램들이 존재하긴 하지만, 이들은 Linux 커널의 특정부분 패치 및 재 컴파일이 필요하거나, 경우에 따라선, 각 서비스별 Masquerading module에 의존적이라서, 특정 서비스 port의 forwarding에 대해서는 제한을 받을 수 있다. 뿐만 아니라, 안전한 port forwarding또한 제공하지않는다. 하지만 SSH의 port forwarding기능은 masquerading module과 상관없이 독립적으로 작동되므로, 필요에 따라 어떠한 port라도 forwarding시킬수 있다. SSH 클라이언트측에서, 필요에 따라, 단 한줄의 명령만으로 forwarding시킬 port들을 지정해줄 수 있고, 관리의 측면에서도, 사설망 내부의 서버에 원격지에서 SSH 클라이언트를 이용하여 접속하면, packet sniffing등의 악의적인 해킹공격으로부터 안전해질 수 있다. 이상 본 논문에서는 이미 구성되어 있는 Network상에 서버들을 추가로 참여 시킬 때, 기존의 네트워크환경에 변화를 주지않고, 독립적으로 서버시스템의 보안효과를 향상시켜줄 수 있는 방안을 Linux와 SSH을 중심으로 기술하였다.

5. 참고 문헌

[1] Y. Rekhter, B. Moskowitz, "Address Allocation for Private Internets - RFC1918", Feb. 1996

[2] K. Egevang, P. Francis, "The IP Network Address Translator (NAT) -RFC1631", May. 1994

[3] Rusty Russel, "Linux ipchains HOWTO", http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html, Jul. 2000

[4] David Ranch , Ambrose Au, "Linux IP Masquerade HOWTO",http://mirrors.indyramp.com/ipmasq/ipmasq-HOWTO-1.82.html

[5] Mohammed J. Kabir, "RedHat Linux 6 Server", IDG Books Worldwide, 1999

[6] Paul Albitz, Cricket Liu, "DNS&BIND,3rd Ed.",O'REILLY & Assciates,1999

[7] Postech Laboratory Unix Security, "Security PLUS for UNIX", youngjin.com, 2000

[8] Carasik, Anne, "UNIX: Using Secure Shell", Osborne McGraw-Hill, 1999