

# 안전한 엑스트라넷 구성을 위한 리눅스기반 VPN 설계 및 구현

정성재, 장희진, 소우영

한남대학교 컴퓨터공학과

## Design and Implementation of VPN System based on Linux for safe Extranet

Sung-Jae Jung, Hui-Jin Jang, Woo-Young Soh

Dept. of Computer Engineering, HanNam University

### 요약

최근의 기업의 업무관련 네트워크가 인터넷의 발달, 글로벌(Global)경영, 전자상거래의 발달 등으로 인하여 전용선을 구축하여 인트라넷(Intranet) 환경에서 처리하던 업무들을 엑스트라넷(Extranet) 환경으로 확장하게 되었다. 엑스트라넷은 해당 기업의 여러 지사뿐만 아니라, 제조업체, 공급업체, 협력업체, 고객, 다른 비즈니스업체들과 안전한 공유를 위해서는 꼭 필요하다. 그러나, 이러한 엑스트라넷 구성은 비용적인 측면과 보안적인 측면 모두 고려해야된다. 현재의 추세는 기존의 공중망을 이용하여 사설망처럼 사용하는 VPN(Virtual Private Network)를 구성하고 있다. 본 논문에서는 리눅스기반에 IPsec 프로토콜을 사용하여 VPN을 구성할 수 있는 freeS/WAN과 방화벽기능을 하는 패킷 필터링(Packet Filtering) 프로그램인 iptables를 이용하여 비용적 부담이 적고 안전한 엑스트라넷을 구성하고자 한다.

### 1. 서론 1)

초고속 인터넷망의 확충과 인터넷 사용자의 폭발적인 증가는 기업활동에 있어서도 커다란 변화를 가져오게 되었다. 기업에서 주요 업무를 전화나 팩스로 처리하던 것들이 인트라넷(Intranet)을 구성하여 인터넷을 통한 처리가 보편화되고 있다. 또한, 기업의 영업 형태가 국내나 특정 국가에 한정되던 형태에서 글로벌(Global)경영, 다국적 기업의 등장, 전자상거래의 발달 등으로 해당 기업의 해외 지사뿐만 아니라, 제조업체, 공급업체, 협력업체, 고객, 다른 비즈니스업체들과 안전한 공유를 하기 위해 엑스트라넷(Extranet)구성이 활발히 진행되고 있다. 현재 엑스트라넷은 비용적인 측면과 보안적인 측면을 고려하여 기존의 공중망(Public Network)인 인터넷을 이용하여 사설망(Private Network)을 구축하는데 이러한 방법을 가상사설망(VPN:Virtual Private Network)이라고 한다.

본 연구는 한국과학재단 지역협력연구사업(R12-2003-004-1002-0)지원으로 수행되었음.

본 논문에서는 현재 기업에서 보편적으로 구성하는 사설IP/Private Internet Protocol)기반 사설망과 외부망의 사설망간의 안전한 엑스트라넷 구성을 위한 리눅스 기반 방화벽 프로그램인 iptables를 이용한 NAT기법과 VPN 프로그램인 freeS/WAN을 이용하여 비용적 부담이 적고 안전한 엑스트라넷 VPN을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 리눅스의 iptables를 이용한 NAT구성을 소개하고 3장에서는 freeS/WAN을 이용한 VPN을 구현하고, 마지막으로 4장에서 결론과 향후 연구방향에 대해서 기술한다.

### 2. iptables를 이용한 NAT구성

#### 2.1 iptables에 대하여

iptables는 리눅스 커널 2.4기반에서 패킷필터링 및 방화벽 기능을 하는 프로그램이다. 대상 보안영역으로 설정된 서브넷(Subnet)상의 패킷을 헤더(Header) 내

용에 따라 필터링하는 기능을 포함하고 있으며, 이 패킷필터링 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 사용 가능하게 하는 기술을 NAT(Network Address Translation)이라고 한다. iptables에서의 NAT는 SNAT(Source NAT)과 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 클라이언트로 사용되는 PC(Personal Computer)를 외부로부터 보호하고 부족한 공인IP 문제를 해결할 수 있는 SNAT 기술을 이용한다.[1][2]

## 2.2 리눅스 iptables의 SNAT 기술을 이용한 사설망 구성

SNAT는 하나의 공인IP주소를 공유하여 인터넷을 사용하도록 하는 것이다. 이러한 구성이 가능하려면 먼저 iptables가 설치된 리눅스 시스템에 공인IP주소가 부여되는 이더넷(Ethernet)카드와 사설IP주소가 부여되는 이더넷카드 등 총 2개의 카드를 장착하고 허브(Hub)를 이용하여 내부의 클라이언트 PC들과 연결시킨다.

[그림1]의 네트워크 구성에서 iptables가 설치된 리눅스 시스템은 외부망에서 내부의 시스템에 직접적인 접근이 불가능하므로 방화벽 역할을 할 뿐만 아니라, 내부 시스템이 외부망으로 접근시에 게이트웨이(Gateway)역할과 더불어 내부시스템의 통제도 가능하게 된다. 또한 내부 시스템 확장시 큰 어려움없이 확장이 가능하고, 또한 특정한 운영체제에 상관없이 사용자의 뜻대로 사용이 가능하게 된다. [3]

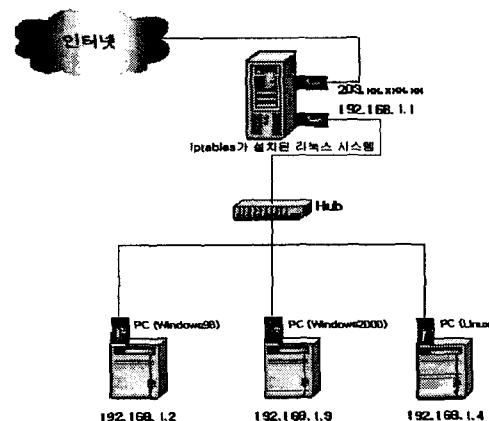


그림 2. 리눅스 iptables의 SNAT 구성

## 3. freeS/WAN을 이용한 VPN 구현

### 3.1 VPN(Virtual Private Network)에 대하여

기업의 보안을 위해서는 전용선을 설치하는 것이 좋다. 그러나, 보안상으로는 매우 안전하지만 비용적인 부담이 크고, 확장이 어렵다는 단점이 있다. VPN은 이러한 단점을 극복하고자, 공중망을 기반으로 마치 전용선을 구축하여 사용하게 하는 기술이다. VPN은 터널링 프로토콜(Tunneling Protocol)을 사용하여 일대일 연결시 '터널'을 형성하고, 데이터 패킷들은 이 터널을 통해 안전하게 전달된다.

터널링에 사용되는 VPN 프로토콜은 프로토콜이 어디에서 동작하는지에 따라 구분되며 OSI(Open Systems Interconnection) 참조 모델에서의 2계층, 3계층, 또는 5계층을 기반으로 한다. 2계층에서는 PPTP, L2TP 가 이용되고 3계층에서는 IPSec, 5계층에서는 SOCKS V5 등이 이용된다.[4]

리눅스에서 VPN을 구현시 사용되는 freeS/WAN은 3계층 프로토콜이자 인터넷 표준인 IPSec을 사용한다. IPSec은 AH(Authentication Header)모드와 ESP(Encapsulation Security Payload)모드로 나눈다. AH모드는 데이터에 대한 무결성을 중요시하고 ESP모드는 데이터에 대한 보안을 중요시한다.

### 3.2 FreeS/WAN

FreeS/WAN(Secure Wide Area Network)은 인터넷 표준 프로토콜인 IPSec을 기반으로 하는 오픈 소스 패키지(Open Source Package)이다. 리눅스에서 FreeS/WAN을 이용하여 VPN을 구성하려면 리눅스

커널(Kernel)에서 관련프로토콜인 IPSec을 지원해야 하는데 기본적으로 커널에서 지원하지 않는다. 따라서, 커널을 컴파일(Compile)하여 IPSec을 지원하도록 한 뒤에 FreeS/WAN을 설치해야 한다.

일반적으로 네트워크 접속을 위해 텔넷(Telnet)을 사용한다. 그러나 텔넷은 평문전송을 하므로 패킷 캡처링(Capturing)을 당했을 경우 전송된 내용이 외부에 노출될 수 있다. 이러한 대안으로 사용하는 것이 SSH(Secure Shell)이다. 그러나, SSH는 원격 쉘(Remote Shell)의 일종의 접속시에 양쪽 시스템에 암호화된 키를 부여하여 데이터전송을 암호화를 하여 패킷이 캡처링을 당해 외부에 노출되더라고 내용을 볼 수 없도록 한다. 그러나 SSH는 원격 쉘에서만 한정된다. FreeS/WAN은 이러한 여러가지 단점을 보완할 수 있다. 접속하고자 하는 망의 양단에 게이트웨이(Gateway)를 설치하고 게이트웨이와 게이트웨이간 보안을 설정한다. 이러한 구성은 SSH처럼 접속시 양쪽 시스템간의 보안 설정이 필요없어 게이트웨이안에 속해 있는 모든 시스템들이 별도의 설정없이 이용이 가능하다. 또한 어떠한 응용프로그램이던지 암호화된 터널안에서 실행되므로 일반프로그램까지 안전한 상태에서의 보안이 가능해진다. [5][6]

### 3.3 FreeS/WAN과 iptables를 이용한 VPN구현

리눅스 iptables의 SNAT를 이용하여 사설IP로 구성한 사설망은 또 다른 사설망과는 접속이 불가능하다. 즉 하나의 사설망은 공인IP인 203.247.xxx.xxx를 가지고 192.168.1.0 대역의 C클래스 사설 네트워크대역을 가지고 구성하였고, 다른 사설망은 210.96.xxx.xx의 공인IP에 192.168.3.0 대역의 C클래스 사설 네트워크 대역으로 구성하였다면 192.168.1.0 네트워크에 속한 192.168.1.2 호스트와 192.168.3.0에 속한 192.168.3.2 호스트는 전혀 다른 사설망이므로 직접 접근이 불가능하게 된다. 그러나, 이 경우 VPN으로 구성하면 전혀 다른 사설망에서 있는 사설IP로 구성한 호스트라도 접근이 가능하게 된다.[7][8]

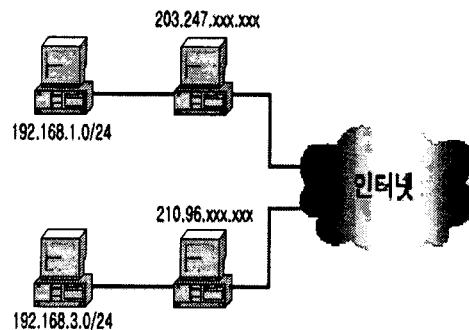


그림 3. VPN 구성 예

### 4. 결론 및 향후 연구 과제

리눅스기반 iptables의 SNAT 기능과 freeS/WAN을 이용한 VPN구성은 여러 곳에 있는 사설망을 연결하는 엑스트라넷 구성시 저렴한 비용으로 공중망을 이용한 전용선 구축이 가능하다. 또한 각 사설망내에서의 있는 호스트들이 사설IP를 사용한 경우에도 접속이 가능하고, 확장이 용이하다. 또한, 어떠한 응용프로그램을 이용하더라도 특별한 암호화없이 모든 프로그램이 암호화된다는 장점이 있다.

향후 연구과제로는 제안된 구현법을 이용하여 사설IP 대역을 사용한 다중 서버의 원격관리기법 등 좀 더 다양한 형태의 연구가 필요하다.

### [참고문헌]

- [1] <http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html>
- [2] 정성재, 유두훈, 장희진, 소우영 “효율적인 다중서버 운영을 위한 리눅스기반 통합보안시스템 설계 및 구현”, 한국멀티미디어학회 춘계학술발표논문집 6권 1호, pp. 322-325, 2003
- [3] Elizabeth D. Zwicky, Simon Cooper, & D. Brent Chapman, “Building Internet Firewalls”, O’Reilly, 2000
- [4] <http://www.ietf.org/html.charters/ipsec-charter.html>
- [5] <http://www.freeswan.org>
- [6] <http://www.ipsec.com>
- [7] <http://www.linuxguruz.org/iptables/howto/iptables-HOWTO.html>
- [8] [http://kldp.org/Translations/html/Virtual\\_Server-KLD/P/VS-NAT.html](http://kldp.org/Translations/html/Virtual_Server-KLD/P/VS-NAT.html)