Linux IP Masquerade mini HOWTO

Ambrose Au, ambrose@writeme.com
v1.20, 10 November 1997

강차훈 chahkang@pusan.ac.kr , 김도석 doseok@ix.netcom.com , 김병찬 redhands@linux.sarang.net , 황성민 smhwang@turing.korea.ac.kr

이 문서는 당신의 리눅스 컴퓨터를 통하여 등록된 인터넷 IP 주소가 없는 컴퓨터를 인터넷에 연결시키는 리눅스 호스트상에서 IP Masquerade 기능을 사용하는 방법을 서술한다

목 차

제 1 절 Introduction 서론

1.1 Introduction 서론

이 문서는 당신의 리눅스 컴퓨터를 통하여 등록된 인터넷 IP 주소가 없는 컴퓨터를 인터넷에 연결시키는 리눅스 호스트상에서 IP Masquerade 기능을 사용하는 방법을 서술한다. 전화선을 이용한 ppp를 연결하는 것들과 마찬가지로 당신의 컴퓨터를 이떠넷을 통하여 리눅스 컴퓨터에 연결하는 것도 가능하다. 이 문서는 이떠넷 연결에 중점을 둘 것이다. 왜냐면 그것이 가장 일반적인 경우이기 때문이다.

> **This document is intended for users using kernels 2.0.x. Development kernels 2.1.x are NOT covered. 이 문서는 2.0.x 커널의 사용자를 위한 것이다. 개발커널인 2.1.x에 관한 것은 여기서 취급되지 않는다.**

1.2 머리말, 의견 & 공로

나는 많은 초보자들이 2.x 커널과같은 새로운 커널에서 IP Masquerade를 설치하는데 매우 혼동되고 있다는 것을 발견했다. 비록 FAQ와 메일링 리스트가 있지만 이것을 전적으로 다룬 문서가 없고 HOWTO같은 것을 만들라는 요구가 메일링리스트 상에 있었다. 그래서 나는 초보자를 위한 출발점으로 문서를 만들고자 하는 이들을 위한 토대로 이 글을 쓰기를 결정했다. 만일 내가 이것을 잘 하지 못한다면 기탄없이 말하라 그래서 내가 더 잘 할 수 있게 해달라.

이문서는 Ken Eves가 지은 FAQ와 IP Masquerade 메일링 리스트의 많은 도움되는 내용에 많은 것을 바탕으로 하고 있다. 그리고 메일링 리스트에서 나에게 IP Masquerade를 설치하고 이글을 쓰게끔 영감을 준 Matthew Driver씨에게 특별히 감사를 드린다.

만일 잘못된 내용이나 빠진 내용이 있다면 나에게 `ambrose@writeme.com`으로 제언이나 의견을 보내주기 바란다. 당신의 중요한 제언들이 나중에 이 하우투에 반영될 것이다.

이 하우투는 가장 짧은 시간에 IP Masquerade를 작동시키는 빠른 안내를 의미한다. 나는 전문적인 필자가 아니므로 일반적이지 않고 목적에 벗어난 내용 발견할수 있을 것이다. 최근의 뉴스와 정보는 내가 관리하고 있는 *IP Masquerade Resource* <http://ipmasq.home.ml.org/> 웹페이지에서 발견할수 있을 것이다. 만일 만일 IP Masquerade에 관해 기술적인 질문이 있으면 시간이 모자라는 내게 email을 보내기 보다는 IP Masquerade의 개발자들이 당신의 질문에 답할 수 있는 메일링 리스트에 참여하기 바란다.

이문서의 최근판은 *IP Masquerade Resource* <http://ipmasq.home.ml.org/>에서 HTML판과 Postscript판을 구할 수 있다.

- http://ipmasq.home.ml.org/
- 다른 가능한 미러사이트를 사용하기 위해 *IP Masquerade Resource Mirror Sites Listing* <http://ipmasq.home.ml.org/index.html##mirror>을 참조하기 바란다.

1.3 판권과 포기

이 문서는 Ambrose Au에게 판권이 있고 자유문서이며 GNU 일반공공면허 아래서 마음대로 재배부할수 있다.

이문서의 정보와 다른 내용들은 내 지식으로 최선을 다한 것이다. 그러나 IP Masqurade는 실험적이고 내가 잘못을 범할 수 도 있으므로 이 문서의 내용에 따를 것인가를 당신이 결정해야한다.

이문서의 내용의 사용으로 인한 손해나 컴퓨터의 손상에 대해 책임질 사람은 아무도 없다.

이 문서의 정보에 의해 행해진 행위 때문에 발생된 어떤 손상도 저자는 책임지지 않는다.

제 2 절 기초지식

2.1 IP Masquerade란 무엇인가?

IP Masquerade는 리눅스 안의 개발되는 네트웍 기능중의 하나이다. 만일 한 리눅스 호스트가 가능한 IP Masquerade를 가지고 인터넷에 연결되었다면 그 호스트에 이떠넷이나 모뎀으로 연결된 다른 컴퓨터들도 *공식적으로 할당된 IP주소를 가지지 않더라*도 인터넷에 연결될 수 있다.

이것은 컴퓨터들이 인터넷에 사용되는 오직 하나의 컴퓨터로 나타나게 되는 출입로(Gateway) 컴퓨터 뒤에 숨어서 인터넷으로 *보이지 않게* 접속하는 것을 가능하게 한다. 잘 설치된 Masquerading 컴퓨터의 보안을 깨는 것은 패킷 필터 방식의 방호벽을 깨는 것보다 더 어렵다. (둘다 버그가 없다고 가정할 때)

2.2 현황

IP Masqurade는 아직 실험적인 단계이다. 그러나 1.3.x 이후 커널은 이미 커널 자체에서 지원하고 있다. 많은 사람들과 심지어는 회사들도 그것을 사용하고 결과에 만족하고 있다

웹페이지 보기와 텔넷은 IP Masquerade 상에서 잘 작동한다고 보고 되었다. FTP, IRC 와 리얼오디오 듣기는 적절한 모듈이 있으면 작동한다. 트루 스피치와 인터넷 웨이브와 같은 다른 네트웍 흐름 오디오들도 역시 잘 작동한다. 심지어 메일링 리스트의 몇몇 동료 사용자들은 화상회의 소프트웨어도 시도하고 있다. Ping도 새롭게 사용 가능가능하게 된 ICMP 짜집기(패치)를 사용하면 작동한다.

4.3절에 있는 지원되는 소프트웨어의 전체목록을 참조하기 바란다.

IP Masquerade는 여러 다른 운영체계와 컴퓨터 기종에서 사용자 컴퓨터(Client Machines)으로 잘 작동하고 있다. 유닉스, 윈도우즈 95, 윈도우즈 NT, TCP/IP를 사용한 윈도우즈 웍그룹, OS/2, Mac TCP, Mac Open Transport를 사용한 맥킨토시, NCSA 텔넷을 이용한 도스, VAX, 리눅스를 사용한 알파, 심지어는 AmiTCP 혹은 AS225-stack을 사용한 아미가 등을 사용한 많은 성공한 예가 있다.

2.3 누가 IP Masquerade로부터 이득을 보는가?

- 당신의 리눅스 호스트가 인터넷에 연결되어 있으면서
- 당신이 국부적인 네트웍상에서 리눅스에 연결시키기 위해 TCP/IP를 사용하는 몇몇의 컴퓨터를 가지고 있으면서 혹은
- 당신의 리눅스 호스트가 다른 것들과 연결하는 PPP 혹은 SLIP 서버로서 작동하고 하나 이상의 모뎀을 가지고 있으면서
- **다른** 컴퓨터들이 정식 등록된 IP 주소를 가지지 않으면서(이들 컴퓨터들은 여기서 **다른** 컴퓨터라고 표현된다.)
- 그리고 물론 당신이 이들 **다른** 컴퓨터들을 인터넷에 연결시키기 위하여 추가 비용을 들이기를 원치 않는다면 :)

2.4 누가 IP Masquerade를 필요로 하지 않는가?

- 당신의 리눅스 호스트가 단독으로 인터넷에 연결된다면 IP Masquerade를 돌린다는 것은 의미없다.
- 당신의 **다른** 컴퓨터들이 정식 등록된 IP 주소를 가지고 있다면 IP Masquerade가 필요없을 것이다.
- 그리고 물론 당신이 '무임승차'라는 발상을 좋아하지 않으면.

2.5 어떻게 IP Masquerade가 작동하는가?

켄 이브스의 IP Masquerade FAQ로 부터

```
여기에 가장 단순한 설치의 그림이 있다.
      SLIP/PPP          +------------+                    +-------------+
      인터넷으로          |   리눅스     |      SLIP/PPP       | 다른 컴퓨터    |
    <---------- 모뎀1|               | 모뎀2 ----------- 모뎀 |               |
      111.222.333.444    |              |          192.168.1.100    |               |
                        +------------+                     +-------------+
위의 그림에서 IP Masquerading을 가지는 설치 가동중에 있는 리눅스 상자가 모뎀1을 사용하여 SLIP
이나 PPP를 통하여 인터넷에 연결되어 있다. 그것은 할당된 111.222.333.444라는 IP 주소를 가진다. 모뎀2는 사용자가 SLIP 혹은 PPP 연결을 하여 로긴하도록 한다.
리눅스를 돌리지 않는 두 번째 시스템이 리눅스 박스 안으로 SLIP 혹은 PPP 연결을 한다. 그것은 인터넷상의 할당된 IP 주소를 가지지 않으므로 192.168.1.100을 사용한다.(아래 참고)
IP Masquerade와 적절히 구성된 경로(Route)를 가지는 다른 컴퓨터는 몇가지 예를 제외하고는 인터넷에 정말로 연결된 것 같이 사용될수 있다.
폴린 미들링크의 인용:
다른 박스는 리눅스 박스를 그것의 출입로(Gateway)로서 설정되야 한다는 것을 잊지 말기 바란다. (기본 경로(default route)혹은 단지 서브넷(subnet)인가는 문제되지 않는다.)
만일 다른 컴퓨터가 이렇게 설정할수 없다면 리눅스 컴퓨터는 모든 지정된 경로의 주소를 위하여 프록시 알프(proxy arp)를 해야만한다. 그러나 그것은 이 문서의 범위를 벗어나는 일이다.
아래는 comp.os.linux.networking에 올라온 글 중에서 발췌한 것이고 위에서 사용된 이름에 맞도록 편집되었다.
  o 나는 SLIP으로 연결된 리눅스 컴퓨터가 출입로(gateway)라고 다른 컴퓨터가
    알도록 하였다.
  o 다른 컴퓨터로부터 리눅스 컴퓨터로 하나의 패킷(packet)이 올 때 리눅스 컴퓨터는
    새로운 입력폴트번호(source port number)를 할당하고
    패킷 헤더(packet header)안의 원래의 IP 주소를 거부하고 원래의 것을 저장한다.
    리눅스 컴퓨터는 SLIP이나 PPP로부터 넘겨받은 변경된 패킷을 인터넷으로 보낸다.
  o 하나의 패킷이 인터넷으로부터 리눅스 컴퓨터로 올 때 만일 포트 번호가 위에서 할당된
    것들 중 하나이면 원래의 포트와 IP 주소를 가져다가 패킷 헤더에 다시 복구하여
    다른 컴퓨터로 패킷을 보낸다.
  o 패킷을 보내는 호스트는 절대로 구별할 수 없다.
```

IP Masquerading의 한 예

아래의 그림이 전형적인 예이다.

```
+----------+
|          |  Ethernet
|   abox   |::::::
|          |2   :192.168.1.x
+----------+    :
                  :   +----------+   PPP
+----------+     :  1|  Linux     |   link
|          |      ::::  | masq-gate |:::::::::// Internet
|   bbox   |::::::      |          |
|          |3    :   +----------+
+----------+     :
                  :
+----------+     :
|          |      :
|   cbox   |::::::
|          |4
+----------+

<-내부  네트웍->
```

위의 예에서 우리가 생각해야할 4대의 컴퓨터가 있다. 오른쪽 끝에는 인터넷으로 IP 연결되어 있고 더 오른쪽에는 인터넷상에 서로 정보를 교환해야할 어떤 것이 있다고 가정되어져 있다. 리눅스 컴퓨터의 masq-gate는 인터넷에 연결되야 될 abox, bbox 그리고 cbox라는 컴퓨터들의 내부 네트웍을 위한 Masqurade를 하는 출입로(masquerading gateway)이다. 내부 네트웍은 할당된 개인 네트웍 주소중의 하나를 사용한다. 이 경우 클라스 C의 network 주소인 192.168.1.1과 다른 컴퓨터들은 네트웍상의 하나씩의 주소를 가진다. **Windows 95, 매킨토시 MacTCP** 혹은 다른 리눅스 컴퓨터와 같은 IP를 사용할 수 있는 다른 운영체계를 가질 수 있는 세 컴퓨터인 abox, bbox 그리고 cbox는 인터넷 상의 다른 컴퓨터들과 연결될 수 있다. 그러나 마스큐레이딩 시스템인 masq-gate는 그들의 접속을 모두 변환해서 그들이 masq-gate로부터 시작되는 것처럼 보이게 하고 마스큐레이드된 연결로 되돌아오는 데이터를 원래의 컴퓨터로 되돌려주게 된다. 그래서 내부 네트웍상의 컴퓨터들은 인터넷으로 직접 통할수 있고 그들의 데이터들이 마스큐레이드되었다는 것을 모르게 된다.

2.6 리눅스 2.x상에서 IP Masquerade를 사용하기위한 요구사항

**** 이 HOWTO를 자주 갱신하기 어렵기 때문에 최근의 정보를 위하여 *IP Masquerade Resource* <http://ipmasq.home.ml.org/>를 참조하기 바란다. ****

- 커널 2.0.x 소스는 ftp://ftp.funet.fi/pub/Linux/kernel/src/v2.0/에서 구할 수 있다.
  (예 당신은 필요한 지원을 위하여 커널을 다시 컴파일 해야되고 최신의 안정된 커널이 추천된다.)
- 적재될수 있는 커널모듈 2.0.0 혹은 최신이 좋고http://www.pi.se/blox/modules/modules-2.0.0.tar.gz에서 구할수 있다.
  (modules-1.3.57이 최소한의 요구사항이다.)
- 제대로 설치된 TCP/IP 네트웍
  Linux NET-2 HOWTO <http://www.caldera.com/LDP/HOWTO/NET-2-HOWTO.html> and the *Network Administrator's Guide* <http://linuxwww.db.erau.edu/NAG/>에서 다뤄진다.
- 리눅스 호스트를 위한 인터넷 연결
  Linux ISP Hookup HOWTO <http://www.caldera.com/LDP/HOWTO/ISP-Hookup-HOWTO.html>,

Linux PPP HOWTO <http://www.caldera.com/LDP/HOWTO/PPP-HOWTO.html> and *Linux PPP-over-ISDN mini-HOWTO* <http://www.caldera.com/LDP/HOWTO/mini/PPP-over-ISDN>에서 다뤄진다.

- Ipfwadm 2.3 혹은 최신의 것으로 ftp://ftp.xos.nl/pub/linux/ipfwadm/ipfwadm-2.3.tar.gz에서 구할 수 있다.
  버전 요구사항에 대한 더 자세한 정보는 *Linux Ipfwadm page* <http://www.xos.nl/linux/ipfwadm/>에 있다.
- 다른 기능을 위한 IP Masquerade 패치를 선택적으로 사용할 수 있다. 더 자세한 정보는 *IP Masquerade Resources* <http://ipmasq.home.ml.org/>에서 구할 수 있다. (이 패치들은 모든 2.0.x 커널에 적용된다.)

제 3 절 IP Masquerade의 설치

만일 당신의 개인 네트웍에 중요한 정보가 있다면 IP Masquerade를 사용하기 전에 주의 깊게 생각하라. 이것은 인터넷에 들어가는 당신을 위한 출입구가 될 수 있고 역으로 지구상의 다른 곳의 어떤 사람이 역으로 당신의 네트웍으로 들어올 수도 있다.

3.1 IP Masquerade 지원을 위한 커널의 컴파일

**** 이 HOWTO를 자주 갱신하기 어렵기 때문에 최근의 정보를 위하여 *IP Masquerade Resource* <http://ipmasq.home.ml.org/>를 참조하기 바란다. ****

- 무엇보다도 먼저 버전 2.0.0혹은 그 이상의 안정 커널 소스가 필요하다.
- 만일 첫 번째 컴파일이면 겁부터 먹지 마라. 사실 쉽고 *Linux Kernel HOWTO* <http://www.caldera.com/LDP/HOWTO/Kernel-HOWTO.html>를 참조하기 바란다..
- 커널 소스를 /usr/src/에다 `tar xvzf linux-2.0.x.tar.gz -C /usr/src`명령을 사용해서 압축을 풀라. 여기서 x는 2.0이상의 패치수준 이다.
  (linux라는 디렉토리가 있나 혹은 심볼릭 링크가 되어 있나 확인하라)
- 적절한 패치를 적용하라. 새로운 패치들이 나오고 있는 관계로 여기에 자세한 내용은 포함시키지 않았다. 최신의 정보는 *IP Masquerade Resources* <http://ipmasq.home.ml.org/>를 참고하기 바란다.
- 커널 컴파일의 지시사항은 커널 소스 디렉토리안의 README 파일이나 커널 HOWTO를 참고하기 바란다.
- 여기에 컴파일할 때 필요한 몇가지 선택이 있다. 아래의 항목에 *YES*라고 대답하라.

```
* Prompt for development and/or incomplete code/drivers
  CONFIG_EXPERIMENTAL
  - 이것은 실험적인 IP Masquerade 코드를 커널 안으로 컴파일되게 해준다.
* Enable loadable module support
  CONFIG_MODULES
  - 모듈을 적재할 수 있게 해준다.
* Networking support
  CONFIG_NET
* Network firewalls
  CONFIG_FIREWALL
* TCP/IP networking
  CONFIG_INET
* IP: forwarding/gatewaying
  CONFIG_IP_FORWARD
```

```
* IP: firewalling
  CONFIG_IP_FIREWALL
* IP: masquerading (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE
  - 비록 실험적이지만 *반드시* 해야 한다.
* IP: ipautofw masquerade support (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE_IPAUTOFW
  -추천함
* IP: ICMP masquerading
  CONFIG_IP_MASQUERADE_ICMP
  - 마스큐레이딩 ICMP 패킷의 지원, 선택사항
* IP: always defragment
  CONFIG_IP_ALWAYS_DEFRAG
  - 강력히 추천함
* Dummy net driver support
  CONFIG_DUMMY
  - 추천함
```

주목: 이것들은 단순히 IP Masquerade를 위해 필요한 요소들이다. 당신이 원하는 설치를 위해 다른 것들을 선택하라.

- 커널을 컴파일한후 꼭 모듈을 컴파일하고 인스톨해야 한다.

```
make modules; make modules_install
```

- 그후 매번 다시 부팅할 때 자동적으로 /lib/modules/2.0.x/ipv4/안에 위치한 필요한 모듈들을 불러들이기 위해 /etc/rc.d/rc.local 혹은 당신 생각에 적절하다고 생각되는 파일안에 몇줄을 더 추가해야 한다.

```
        .
        .
        .
/sbin/depmod -a
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_raudio
/sbin/modprobe ip_masq_irc
(그리고 당신이 패치를 적용했다면 p_masq_cuseeme, ip_masq_vdolive 같은 다른 모듈들도 포함되야 한다.)
        .
        .
        .
```

주목: ip_masq를 사용하기 전에 수동으로 설치할 수 있으나 이를 위해 kerneld를 사용하지 말라. 그건 작동하지 않는다!

3.2 내부 IP 주소의 할당

모든 **다른** 컴퓨터들이 공식적으로 할당된 주소를 가지지 않기 때문에 반드시 컴퓨터들에게 적절한 방법으로 주소를 지정해야 한다.

IP Masquerade FAQ로 부터

외부와 연결되지 않은 네트웍에 사용되는 IP 주소는 RFC (#1597)에 나와 있다. 특별히 이런 목적으로 3종류의 주소들이 있다. 내가 사용하고 있는 것은 192.168.1.n에서 192.168.255.n까지의 255개의 Class-C 하부 넷트웍이다.

```
RCF 1597로부터:
```

```
Section 3: 내부 주소 공간
인터넷 할당 주소 당국(IANA)은 사설 네트웍을 위한 주소 공간을 아래와 같이 3가지 덩어리로 예약해 놓았다.
              10.0.0.0        -   10.255.255.255
              172.16.0.0      -   172.31.255.255
              192.168.0.0     -   192.168.255.255
우리는 24숏블록으로 첫 번째 덩어리를, 20숏블록으로 두 번째를, 16숏블록으로 세 번째를 언급한다.  첫 번째 블록은 단 하나의 A 클라스의 주소이고, 두 번째 블록은 16개의 연속된 B 클라스의 주소이고 세 번째는 255개의 연속된 C 클라스 주소들이다.
```

만일 C 클라스 네트웍을 사용한다면 반드시 192.168.1.1, 1.92.168.1.2, 1.92.168.1.3, ..., 192.168.1.x 와 같이 번호를 지정해야 한다.

192.168.1.1은 일번적으로 인터넷에 연결되는 리눅스 호스트인 출입로 컴퓨터로 사용된다. 예약된 192.168.1.0와 192.168.1.255은 각각이 네트웍 주소와 방송주소로 사용된다. 이들 주소를 당신의 컴퓨터의 주소로 사용하는 것은 피하라.

도메인 네임 서비스를 위해 가능한 어떤 DNS에도 추가할수 있다. 가장 명백한 것은 당신의 리눅스가 사용하는 것이 되어야 한다. 당신은 마찬가지로 어떠한 도메인 찾기 접미사(domain search suffix)를 추가할 수 있다.

이들 IP 주소를 재설정한 뒤에는 적절한 서비스를 재실행 하거나 컴퓨터를 다시 실행시키는 것을 기억하라.

아래의 설정 지시는 리눅스 호스트의 주소로서 192.168.1.1의 C 클라스를 사용하는 것을 가정하고 있다. 192.168.1.0과 192.168.1.255는 예약되어 있다는 것을 주목하기 바란다.

]OTHER 컴퓨터의 구성

적재될수 있는 커널 모듈, `http://www.pi.se/blox/modules/modules-2.0.0.tar.gz`로부터 구할수 있는 2.0.0 혹은 최근의 것이 좋다.
(모듈-1.3.57이 최소한의 필요사항이다.)

잘 설치된 TCP/IP 네트웍
`<http://www.caldera.com/LDP/HOWTO/NET-2-HOWTO.html>`뺌滑또炙催竄 각각의 컴퓨터를 위한 적절한 IP 주소를 정하는 것 외에도 역시 적절한 출입구를 정해주어야 한다. 일반적으로 그것은 직접적이다. 단순히 출입로 주소로서 당신의 리눅스 호스트(192.168.1.1)의 주소를 넣어주면 된다.

도메인 네임 서비스를 위해 가능한 어떤 DNS에도 추가할수 있다. 가장 명백한 것은 당신의 리눅스가 사용하는 것이 되어야 한다. 당신은 마찬가지로 어떠한 도메인 찾기 접미사(domain search suffix)를 추가할 수 있다.

이들 IP 주소를 재설정한 뒤에는 적절한 서비스를 재실행 하거나 컴퓨터를 다시 실행시키는 것을 기억하라.

아래의 설정 지시는 리눅스 호스트의 주소로서 192.168.1.1의 C 클라스를 사용하는 것을 가정하고 있다. 192.168.1.0과 192.168.1.255는 예약되어 있다는 것을 주목하기 바란다.

3.2.1 Windows 95 설정

1. 당신이 네트웍카드와 카드 드라이버를 설치하지 않았다면 지금 설치하라.
2. *'Control Panel'/'Network'*로 가라.
3. *'TCP/IP protocol'*이 없다면 추가하라.
4. *'TCP/IP properties'*안에서 *'IP Address'*가서 IP 주소를 192.168.1.x, (1 < x < 255)로 설정하고 서브넷 마스크를 255.255.255.0로 설정하라
5. *'Gateway'*아래로 당신의 출입로인 192.168.1.1을 입력하라.
6. *'DNS Configuration'/'DNS Server search order'*아래에 당신의 리눅스가 사용하고 있는 DNS(보통 `/etc/resolv.conf`안에서 발견된다)를 입력하라. 선택적으로 적절한 도메인 찾기 접미사를 추가할수도 있다.

7. 당신이 모르는 나머지는 원래값 그대로 두라.
8. 모든 대화상자에서 *'OK'*를 선택하고 컴퓨터를 재시동 시켜라.
9. `Ping` 네트웍 연결을 시험하기 위한 리눅스 컴퓨터: *'Start/Run'*한 후, `ping 192.168.1.1`을 입력하라. (이것은 단지 LAN 연결 시험이다. 당신은 아직 바깥 세상에 `ping`을 할 수 없다.)
10. 당신은 선택적으로 윈도우즈 디렉토리안에 `HOSTS`을 만들어서 당신의 LAN상의 컴퓨터의 호스트 이름을 사용할 수 있다. There is an example called 윈도우즈 디렉토리 안에 `HOSTS.SAM`이라는 예제 파일이 있다.

3.2.2 윈도우즈 워그룹 3.11 설정

1. 당신의 네트웍카드와 카드 드라이버가 설치되지 않았다면 지금 설치하라.
2. TCP/IP 32b 꾸러미가 설치되지 않았다면 설치하라.
3. *'Main'/'Windows Setup'/'Network Setup'*안의 *'Drivers'*를 선택하라.
4. *'Network Drivers'*란에 *'Microsoft TCP/IP-32 3.11b'*를 선택한 후 *'Setup'*을 클릭하라.
5. IP 주소를 192.168.1.x (1 < x < 255)로 설정하고 서브넷 마스크도 255.255.255.0로 설정하고 기본 출입로도 192.168.1.1로 설정하라.
6. *'Automatic DHCP Configuration'*을 작동하지 않게 하고 *'WINS Server'*안에는 윈도우즈 NT 도메인 안에 있지 않거나 당신이 모르면 아무것도 입력하지 말라.
7. *'DNS'*을 클릭하고 3.3.1절의 6번째 단계에서 언급된 적절한 정보를 입력하고 다되면 *'OK'*를 클릭하라.
8. *'Advanced'*을 클릭하고 3.3.1절의 10번째 단계에서 언급된것과 유사한 룩업 호스트(Look up host) 파일을 사용한다면 *'Enable DNS for Windows Name Resolution'*과 *'Enable LMHOSTS lookup'*을 선택하라.
9. 모든 대화상자의 *'OK'*를 클릭하고 컴퓨터를 재시동시켜라.
10. `Ping` 네트웍 연결을 시험하기 위한 리눅스 컴퓨터: *'Start/Run'*한 후, `ping 192.168.1.1`을 입력하라. (이것은 단지 LAN 연결 시험이다. 당신은 아직 바깥 세상에 `ping`을 할 수 없다.)

3.2.3 Windows NT 설정

1. 당신의 네트웍카드와 카드 드라이버가 설치되지 않았다면 지금 설치하라.
2. *'Main'/'Control Panel'/'Network'*로 가라
3. TCP/IP 서비스를 설치하지 않았다면 TCP/IP 프로토콜을 추가하고 *'Add Software'*메뉴로부터 연관된 요소를 추가하라.
4. Under *'Network Software and Adapter Cards'*란 아래서 *'Installed Network Software'*선택 상자에서 *'TCP/IP Protocol'*을 선택하라.
5. *'TCP/IP Configuration'*안에서 `[1]Novell NE2000 Adapter`등과 같이 적절한 네트웍카드를 선택하라. 그리고나서 IP 주소를 192.168.1.x (1 < x < 255)로 설정하고 서브넷 마스크를 255.255.255.0로 기본 출입로를 192.168.1.1로 설정하라.
6. *'Automatic DHCP Configuration'*을 작동하지 않게 하고 *'WINS Server'*안에는 윈도우즈 NT 도메인 안에 있지 않거나 당신이 모르면 아무것도 입력하지 말라.
7. *'DNS'*을 클릭하고 3.3.1절의 6번째 단계에서 언급된 적절한 정보를 입력하고 다되면 *'OK'*를 클릭하라.

8. *'Advanced'*을 클릭하고 3.3.1절의 10번째 단계에서 언급된것과 유사한 룩업 호스트(Look up host) 파일을 사용한다면 *'Enable DNS for Windows Name Resolution'*과 *'Enable LMHOSTS lookup'*을 선택하라.
9. 모든 대화상자의 *'OK'*를 클릭하고 컴퓨터를 재시동시켜라.
10. Ping 네트웍 연결을 시험하기 위한 리눅스 컴퓨터: *'Start/Run'*한 후, `ping 192.168.1.1`을 입력하라. (이것은 단지 LAN 연결 시험이다. 당신은 아직 바깥 세상에 ping을 할 수 없다.)

3.2.4 UNIX Based Systems의 설정

1. 당신이 네트웍카드를 설치하지 않았거나 적절한 카드 드라이버를 포함해서 커널을 다시 컴파일 하지 않았다면 지금 그렇게 하라.
2. nettools 꾸러미와같은 TCP/IP 네트워킹을 설치하지 않았다면 설치하라.
3. *IPADDR*을 192.168.1.x (1 < x < 255)로 *NETMASK*를 255.255.255.0로, *GATEWAY*를 192.168.1.1로, 그리고 *BROADCAST*를 192.168.1.255로 정한다.
   예를들면, 레드햇 니눅스의 `/etc/sysconfig/network-scripts/ifcfg-eth0`을 수정하거나 단순히 제어판을 통하여 이를 할수 있다.
   (it's different in 이것은 SunOS, BSDi, Slackware Linux등에 따라 다르다.)
4. 영역 이름 서비스(DNS)와 영역 찾기 접미사를 `/etc/resolv.conf`에 추가한다.
5. 어떻게 설정되었나에 따라 `/etc/networks`를 갱신할 필요가 있다.
6. 적절한 서비스를 다시 실행시키거나 아니면 단순히 컴퓨터를 다시 실행 시킨다.
7. `ping` 명령을 해본다: 당신의 출입로 컴퓨터와의 연결을 점검하기 위해서 `ping 192.168.1.1`을 사용한다.
   (이것은 단지 LAN연결을 점검하기 위한 것이다. 아직 바깥세상에는 `ping`을 할수 없다.

3.2.5 using NCSA 텔넷 꾸러미를 사용한 DOS 설정하기

1. 당신의 네트웍카드가 설치되지 않았다면 지금 설치하라.
2. 적절한 패킷드라이버를 설치하라. NE2000카드의 경우 IRQ 10이고 하드웨어 주소가 0x300으로 지정되어 있으면 라면 `nwpd 0x60 10 0x300`으로 실행시킨다.
3. 새로운 디렉토리를 만들고 NCSA 텔넷 꾸러미를 푼다. `pkunzip tel2308b.zip`
4. 문서 편집기를 사용하여 `config.tel`을 연다.
5. `myip=192.168.1.x` (1 < x < 255), 와 netmask=255.255.255.0을 지정한다.
6. 앞의 예에서 `hardware=packet, interrupt=10, ioaddr=60`을 꼭 지정해준다.
7. 리눅스 호스트 같이 적어도 하나의 컴퓨터를 게이트웨이로서 지정해야 한다.

```
name=default
host=yourlinuxhostname
hostip=192.168.1.1
gateway=1
```

8. 도메인 이름 서비스를 위해 추가설정이 필요한다.

```
name=dns.domain.com ; hostip=123.123.123.123; nameserver=1
```

   주의: 당신의 리눅스 호스트가 사용하는 DNS에 관련된 적절한 값으로 바꿔라. Note: substitute the appropriate information about the DNS that your Linux host uses

9. `config.tel` 파일을 저장하라.

10. 네트워 연결을 시험하기 위해 리눅스 컴퓨터로 텔넷을 하라. `telnet 192.168.1.1`

3.2.6 MacTCP를 사용하는 MacOS기반의 컴퓨터 설정하기.

1. 이떠넷 카드에 적절한 드라이버가 설치되지 않았다면 지금 바로 설치하라.

2. *MacTCP control panel* 을 열고 적절한 네트웍 드라이버를 선택하라(EtherTalk가 아니고 Ethernet이다) 그리고 *'More...'*버튼을 클릭한다.

3. *'Obtain Address:'*에서 *'Manually'*을 클릭한다.

4. Under *'IP Address:'*에서 팝업메뉴로부터 *class C*를 선택한다. 나머지는 무시한다.

5. *'Domain Name Server Information:'*에 적절한 값을 입력한다.

6. *'Gateway Address:'*에 192.168.1.1을 입력한다.

7. 이 설정을 저장하기 위해 *'OK'*을 클릭한다. *MacTCP control panel*의 메인 창문 안의 *'IP Address:'*상자에 당신의 Mac의 IP 주소(192.168.1.x, 1 < x < 255)를 입력한다.

8. *MacTCP control panel*을 닫는다. 만일 컴퓨터를 재시작하라는 메시지가 나오면 재시동하라.

9. 네트웍 연결을 검사하기 위해 리눅스 컴퓨터로 선택적으로 ping을 할수 있다. 만일 공개프로그램인 *MacTCP Watcher*을 가지고 있다면 *'Ping'*단추를 클릭하고 팝업된 대화상자에 리눅스 컴퓨터의 주소(192.168.1.1)를 입력한다. (이것은 단지 LAN 연결을 검사하기 위한것이고 바깥 세상에는 아직 ping할 수 없다.)

10. 시스템 폴더 안의 `Hosts`화일을 선택적으로 만들 수 있으므로 당신의 LAN안에서 컴퓨터들이 호스트 이름을 사용할 수 있다. 그 파일은 당신의 시스템 폴더에 이미 있어야 하고 당신의 필요에 따라서 변경될 수 있는 몇가지 (주석표시가 제거된) 예제들을 가져야 한다.

3.2.7 Open Tranasport를 사용하는 MacOS기반의 컴퓨터 설정하기.

1. 아직 이떠넷 어댑터를 위해서 적절한 드라이버를 설치하지 않았다면 지금이 하기 바란다.

2. *TCP/IP Control Panel*를 열고 *Edit*로부터 *'User Mode ...'*을 선택한다. 적어도 사용자 모드를 *'Advanced'*를 설정하고 *'OK'*을 눌러주는 것을 명심하라.

3. *File*메뉴로부터 *'Configurations...'*을 선택하라. *'Default'* 구성을 선택하고 *'Duplicate...'* 단추를 클릭한다. 'IP Masq'(혹은 이것이 특별한 설정이라는 것을 알 수 있도록 하는 다른 이름)을 *'Duplicate Configuration'*다이알로그에 입력한다. *'Deafault copy'*같은 것이라 말할 것이다. 그때 *'OK'*버튼과 *'Make Active'*버튼을 클릭한다.

4. *'Ethernet'*을 *'Connect via:'* 팝업에서 선택한다.

5. *'Configure:'*팝업으로부터 적절한 항목을 선택하라. 어떤 선택을 해야 할지 모른다면 아마도 다시 *'Default'*설정을 선택하고 끝낸다. 나는 *'Manually'*을 사용한다.

6. 당신의 맥의 IP 주소(192.168.1.x, 1 < x < 255)를 *'IP Address:'*상자 안에서 입력하라.

7. 255.255.255.0를 *'Subnet mask:'*상자에 입력하라.

8. 192.168.1.1을 *'Router address:'*상자에 입력하라.

9. 당신의 도메인 이름 서버들의 IP 주소를 *'Name server addr.:'*안에 입력하라.

10. 당신의 인터넷 도메인(예: 'microsoft.com')을 *'Implicit Search Path:'*아래의 *'Starting domain name'*상자에 입력하라.

11. 따르는 절차는 선택적이다. 부적절한 값의 입력은 비정상적인 행동을 일으키게 될 수도 있다. 확실하지 않으면 빈칸이나 선택하지 않은채로 남기는게 더 좋을지도 모른다. 필요하다면 그들 항목의 내용을 지워라. 내가 아는한 TCP/IP 다이얼로그를 통하여 이전에 선택한 양자택일적인 "Hosts" 화일을 사용하지 않도록 하는 방법은 없다. 만일 당신이 안다면 흥미있을 것이다.
당신의 네트웍이 802.3 후레임 타입을 요구한다면 *'802.3'*을 클릭하라.

12. *'Options...'*을 클릭하여 TCP/IP가 활성화 되어있는지 확인하라. 나는 *'Load only when needed'*을 사용한다. 당신이 TCP/IP 프로그램을 재부팅하지 않고 빈번하게 사용한다면 *'Load only when needed'*을 선택하지 않는 것이 메모리 관리 측면에서 효과적인 것을 발견하게 될 것이다. 그항목을 선택하지 않으면 TCP/IP protocol stacks은 항상 적재되어 사용가능하게 된다. 체크된다면 TCP/IP stacks는 자동적으로 필요할 때 적재되면 필요없을 때 해제된다. 그것은 컴퓨터의 메모리를 조각조각으로 만드는 원인이 되는 로딩 언로딩 프로세스이다.

13. 네트웍 연결을 검사하기 위해서 리눅스 박스를 ping해도 된다. 만일 프리웨어 프로그램인 *MacTCP Watcher*을 사용한다면 *'Ping'*버튼을 누르고 팝업된 다이알로그 박스안에다 리눅스 컴퓨터의 주소(192.168.1.1)를 입력한다. (이것은 단지 LAN 연결을 검사한다. 아직 바깥 세상에는 ping을 할수 없다.)

14. `Hosts`화일을 당신의 시스템 폴더에 만들 수 있고 당신은 당신의 LAN상에서 컴퓨터의 호스트네임을 사용할수 있다. 이 파일은 시스템 폴더안에 있을수도 없을수도 있다. 만일 있다면 당신의 필요에 따라 주석표시를 제거하므로 변경할수 있는 예들을 담고 있다. 만일 없다면 MacTCP를 사용하고 있는 컴퓨터로부터 복사하거나 직접 만들 수도 있다.(RFC 1035의 33페이지에 서술된 것과 같이 `/etc/hosts` 유닉스 화일 형식을 따른다.) 일단 이화일이 만들어지면 *TCP/IP control panel*을 열고 *'Select Hosts File...'*버튼을 클릭한 다음 `Hosts`화일을 연다.

15. 닫기 박스를 클릭하거나 *File*메뉴로부터 *'Close'*혹은 *'Quit'*을 선택하고 변경된 내용을 저장하기 위해 *'Save'*버튼을 클릭한다.

16. 변경상항은 즉각적으로 효력을 발생한다. 그러나 다시 재부팅하는 것도 해가되지는 않는다.

3.2.8 DNS를 사용하는 노벨 네트웍의 설정

1. 당신의 이떠넷 카드를 위한 적절한 드라이버가 설치되지 않았다면 지금 설치하라.

2. `<ftp.novell.com/pub/updates/unixconn/lwp5>`로부터 tcpip16.exe을 다운로드 받는다.

3. `c:\nwclient\startnet.bat`을 편집하라

   : (아래는 내 것의 사본이다.)

```
SET NWLANGUAGE=ENGLISH
LH LSL.COM
LH KTC2000.COM
LH IPXODI.COM
LH tcpip
LH VLM.EXE
F:
```

4. `c:\nwclient\net.cfg`을 편집하라

   : (링크 드라이버를 당신것에 맞게 바꾼다. 예: NE2000)

```
Link Driver KTC2000
        Protocol IPX 0 ETHERNET_802.3
        Frame ETHERNET_802.3
        Frame Ethernet_II
        FRAME Ethernet_802.2
NetWare DOS Requester
           FIRST NETWORK DRIVE = F
           USE DEFAULTS = OFF
           VLM = CONN.VLM
           VLM = IPXNCP.VLM
           VLM = TRAN.VLM
           VLM = SECURITY.VLM
           VLM = NDS.VLM
           VLM = BIND.VLM
           VLM = NWP.VLM
           VLM = FIO.VLM
           VLM = GENERAL.VLM
           VLM = REDIR.VLM
           VLM = PRINT.VLM
           VLM = NETX.VLM
Link Support
        Buffers 8 1500
        MemPool 4096
Protocol TCPIP
        PATH SCRIPT     C:\NET\SCRIPT
        PATH PROFILE    C:\NET\PROFILE
        PATH LWP_CFG    C:\NET\HSTACC
        PATH TCP_CFG    C:\NET\TCP
        ip_address      xxx.xxx.xxx.xxx
        ip_router       xxx.xxx.xxx.xxx
```

5. 그리고 마지막으로

   ```
   c:\bin\resolv.cfg
   ```

   을 만들라:

   ```
   SEARCH DNS HOSTS SEQUENTIAL
   NAMESERVER 207.103.0.2
   NAMESERVER 207.103.11.9
   ```

6. 나는 이것이 노벨넷 온라인을 가진 이들에게 도움이 되기를 바란다. 이것은 넷웨어 3.1x 혹은 4.x에 사용되어질수 있다.

3.2.9 OS/2 Warp의 설정

1. 당신의 네트웍카드와 카드 드라이버가 설치되지 않았다면 지금 설치하라.
2. TCP/IP 프로토콜이 아직 없다면 설치하라
3. *Programms/TCP/IP (LAN) / TCP/IP* 세팅으로 가라.
4. *'Network'*안에 TCP/IP주소와 넷마스크(255.255.255.0)를 추가하라.

5. *'Routing'*하에서 *'Add'*를 눌러라. *Type*을 *'default'*로 정하고 *'Router Address'*항목에 리눅스 컴퓨터의 IP 주소를 입력한다. (192.168.1.1)
6. 리눅스 컴퓨터의 *'Hosts'*에서 사용하는것과 같은 DNS(Nameserver) 주소를 지정한다.
7. TCP/IP 제어판을 닫고 따르는 질문에 yes라고 답한다.
8. 재부팅한다.
9. 네트웍설정을 검사하기 위해 리눅스 컴퓨터를 ping할수도 있다. 'OS/2 Command prompt Window'안에서 `'ping 192.168.1.1'`을 입력한다. 핑 패킷이 도착한다면 모든 것이 제대로 된것이다.

3.2.10 다른 컴퓨터의 설정

설치를 위해서 같은 이론이 따라야 한다. 위의 섹션들을 점검하라. 당신이 이들 시스템에 관하여 흥미를 가지고 있다면 자세한 설치방법을 `ambrose@writeme.com`으로 보내주세요.

3.3 IP Forwarding 방법의 IP 설정

지금 시점에서 당신은 당신의 모듈이 적재되야 함은 물론 당신의 커널과 다른 요구되는 꾸러미들을 설치되었어야 한다. 또한 IP 주소, 출입로 그리고 DNS가 **다른**컴퓨터에 설치되어 있어야 한다.

지금 오직 해야 할 일은 적절한 컴퓨터로의 적절한 패킷을 전달하기 위해 ipfwa으을 사용하는 것이다.

> **** 이것은 많은 다른 방법들로 이루어 질수 있다. 따르는 제안이나 예들은 내경우에 작동했지만 당신은 다른 생각을 가질 것이므로 더 자세한 것은 섹션 4.4와 ipfwadm 맨페이지를 참조하라. ****

```
ipfwadm -F -p deny
ipfwadm -F -a m -S yyy.yyy.yyy.yyy/x -D 0.0.0.0/0
```

x는 당신의 서브넷의 클라스에 따르는 숫자들 중에 하나이고 yyy.yyy.yyy.yyy는 네트웍 주소이다.

```
netmask         | x  | Subnet
~~~~~~~~~~~~~~~~|~~~~|~~~~~~~~~~~~~~~
255.0.0.0       | 8  | Class A
255.255.0.0     | 16 | Class B
255.255.255.0   | 24 | Class C
255.255.255.255 | 32 | Point-to-point
```

예를들면 만일 클라스 C 서브넷이면 아래와 같이 입력할 것이다.

```
ipfwadm -F -p deny
ipfwadm -F -a m -S 192.168.1.0/24 -D 0.0.0.0/0
```

bootp는 클라이언트가 모르는 정당한 IP없이 오는 패킷을 요구하기 때문에 마스큐레이드/화이어월 컴퓨터안의 bootp서버를 가진 사람들을 위해서 deny 명령을 사용하기 전에 아래의 내용이 필요하다:

```
ipfwadm -I -a accept -S 0/0 68 -D 0/0 67 -W bootp_clients_net_if_name -P udp
```

당신은 또한 컴퓨터당 기분으로 할수도 있다. 예를들면 내가 192.168.1.2와 192.168.1.8을 인터넷에 접속하기를 원하고 다른 것은 못하게 하고자 한다면 나는 아래와 같이 입력해야 한다.

```
ipfwadm -F -p deny
ipfwadm -F -a m -S 192.168.1.2/32 -D 0.0.0.0/0
ipfwadm -F -a m -S 192.168.1.8/32 -D 0.0.0.0/0
```

선택적으로 당신은 그 값대신에 넷마스크를 사용할수 있다. 예: 192.168.1.0/255.255.255.0

일반적인 실수를 범하게 되는 것이 첫 번째 명령을 다음과 같이 만드는 것이다.

```
ipfwadm -F -p masquerade
```

기본 정책으로 마스큐레이드를 만들지 **말라**. 그렇지 않으면 그들의 루팅을 조절할 수 있는 이들이 당신의 출입로를 통하여 곧장 터널을 만들어 그들이 누구인가를 가리는데 사용될수도 있다.

다시 당신은 `/etc/rc.local`혹운 당신이 선호하는 어떠한 rc화일에 이 명령들을 추가하거나 IP 마스큐레이딩이 필요할 때마다 일일이 수작업으로 할수 있다.

ipfwadm에 대한 자세한 안내는 4.4 섹션을 읽기 바란다.

3.4 IP Masquerade의 시험

지금이 모든 힘든 일들을 마치고 시도해볼 때다. 리눅스 호스트가 인터넷에 제대로 연결되어 있는가 확인하라.

당신은 **다른** 컴퓨터상에서 몇몇 *'인터넷!!!'* 웹사이트를 보려고 시도할수 있고 만일 제대로 榮摸墉섟瘟甄墨廡 당신의 DNS 설정이 잘못될 수도 있기 때문에 나는 첫 번째 시도에서 호스트네임보다는 IP 주소를 사용하기를 권한다

예를들면 `http://152.2.254.81/mdw/linux.html`에 입력으로 리눅스 문서 프로젝트 사이트 http://sunsite.unc.edu/mdw/linux.html에 접속할수 있다.

만일 돗단배를 본다면 축하! 작동합니다. 당신은 무엇이든 IP 마스큐레이딩에 의해 지원되는 호스트이름, 텔넷, ftp, 리얼오디오, 트루 스피치 등으로도 시도해볼수 있다.

지금까지, 위의 설정으로 아무런 문제가 없었다. 이런 훌륭한 기능을 작동하게 만들기 위해 자기의 시간을 소비하는 사람들의 큰 명예이다.

제 4 절 다른 IP Masquerade 문제와 무른모 지원

4.1 IP Masquerade가 가진 문제점들

몇몇 프로토콜은 폴트 번호에 관한 것들을 가정하거나 주소와 폴트에관한 데이터 흐름을 암호화하기 때문에 마스큐레이딩이 현재 작동하지 않는다. 이들 요즘의 프로토콜은 그들이 작동하도록 만드는 마스큐레이딩 코드로 지어진 특별한 프록시를 필요로 한다.

4.2 들어오는 서비스

마스큐레이딩은 들어오는 서비스를 전혀 다루지 못한다. 그들을 가능하게 하는 몇가지 방법이 있으나 그들은 마스큐레이딩과는 완벽하게 분리되어 있고 정발로 표준 방화벽 실습의 부분이다.

만일 당신이 고수준의 보안이 필요하지 않으면 단순히 폴트를 새방향으로 돌릴수 있다. 이것을 하는 여러 가지 방법이 있다. 나는 수정된 redir 프로그램(선사잇이나 그 미러에 곧 가능하게 되기를 바란다)을 사용한다. 만일 당신이 들어오는 연결상에서 몇가지 수준의 위임을 가지 기를 원한다면 단지 지정된 IP 주소를 통하는 것만을 허락하는 redir(0.7 혹은 그이상)의 꼭대기에서 TCP wrappers, Xinetd 혹은 다른 도구를 사용한다. TIS 방화벽 툴킷은 도구와 정보를 찾기 위해서 좋은 장소이다.

보다 자세한 내용은 *IP Masquerade Resource* `<http://ipmasq.home.ml.org>`에서 찾을수 있다.

4.3 지원되는 클라이언트 소프트웨어와 다른 설치 노트

**** 아래 목록은 도이상 유지되지 않는다. 리눅스 IP 마스큐레이딩이 작동하는 프로그램상의 *this page* <http://masqapps.home.ml.org>와 보다 자세한 내용을 위해 *IP Masquerade Resource* <http://ipmasq.home.ml.org/>을 참조하기 바란다. ****

일반적으로 TCP와 UDP를 사용하는 프로그램은 작동해야 한다. 만일 IP 마스큐레이드를 하는 프로그램에 관한 어떤 제안이나 힌트 혹은 질문이 있으면 Lee Nevo의 *applications that work thru Linux IP masquerading* <http://masqapps.home.ml.org>를 방문하기 바란다.

4.3.1 작동하는 클라이언트들

일반 클라이언트

HTTP

모든 지원되는 플랫폼, 웹 파도타기

POP & SMTP

모든 지원되는 플랫폼, 전자우편 클라이언크

Telnet

모든 지원되는 플랫폼, 원격 컴퓨터사용

FTP

모든 지원되는 플랫폼, ip_masq_ftp.o 모듈 필요 (특정한 클라이언트로 모든 사이트가 가능하지 않다; 몇몇 사이트는 ws_ftp32로 갈 수 없지만 netscape는 갈 수 있다)

Archie

모든 지원되는 플랫폼, 파일 찾기 클라이언트(모든 알치 클라이언트는 지원되지 않는다)

NNTP (USENET)

모든 지원되는 플랫폼, 유즈넷 뉴스 클라이언트

VRML

윈도우즈(아마도 모든 지원되는 플랫폼), 가상현실 파도타기

traceroute

대부분이 유닉스 기반의 플랫폼, 몇몇 변형된 것들은 작동하지 않는다.

ping

모든 플랫폼, ICMP 패치가 필요

IRC를 기반으로 하는 모든 것

모든 지원되는 플랫폼, ip_masq_irc.o 모듈 필요

Gopher client

모든 지원되는 플랫폼

WAIS client

모든 지원되는 플랫폼

멀티미디아 클라이언츠

리얼오디어 재생기

윈도우즈, 네트웍 흐름 오디오, ip_masq_raudio 모듈의 적재 필요

트루 스피치 재생기 1.1b

윈도우즈, 네트웍 흐름 오디오

엔터넷 웨이브 재생기

윈도우즈, 네트웍 흐름 오디오

월드 챗 0.9a

윈도우즈, 클라이언트-서버 3D 대화 프로그램

알파 월드

윈도우즈, 클라이언트-서버 3D 대화 프로그램

인터넷 폰 3.2

윈도우즈, 피어-투-피어 오디오 통신, 당신이 전화를 걸면 사람들과 연결 될 수 있으나 다른 사람들은 당신에게 전화할수 없다.

Powwow

윈도우즈, 피어-투-피어 문자/오디오 칠판 통신, 당신이 연결할 때만 다른 사람들과 연결할 수 있으나 다른 사람들은 당신에게 연결할수 없다.

CU-SeeMe

모든 지원되는 플랫폼, cuseeme 모듈 필요, 자세한 것은 *IP Masquerade Resource* `<http://ipmasq.home.ml.org/>`을 보기 바람

VDOLive

윈도우즈, vdolive 패치가 필요

노트: 인터넷 폰이나 파우와우 같은 몇몇 클라이언트들은 *ipautofw 꾸러미*(섹션 4.6 참조)를 사용하여 연결을 시작하지 하지 않아도 작동할 수도 있다.

다른 클라이언츠

NCSA Telnet 2.3.08

도스, telnet, ftp, ping등을 담고있는 꾸러미

PC-anywhere for windows 2.0

윈도우즈, TCP/IP상에서 컴퓨터를 원격조종, 단지 클라이언트일때만 작동하고 호스트 일때는 작동하지 않는다.

Socket Watch

ntp를 사용 - 네트웍 시간 프로토콜

리눅스 net-acct 꾸러미

리눅스, 네트웍 관리계정 꾸러미

4.3.2 작동하지 않는 클라이언츠

인텔 인터넷 폰 베타 2

연결되지만 한쪽방향으로만 소리가 전달된다.

인텔 Streaming Media Viewer Beta 1

서버에 연결할수 없다.

Netscape CoolTalk

상대편으로 연결할수 없다.

talk,ntalk

작동하지 않는다. - 쓰여진 커널 프록시가 필요.

WebPhone

현재까지 작동안함 (주소에 대하여 잘못된 가정을 만듬).

X

시험 안됨, 내 생각엔 아마도 마스큐레이딩 코드로의 외부 프로그램인 X 프록시를 만들지 않는한 작동하지 않을 것이다. 이것의 한 방법이 연결로서의 **ssh**와 성공하게 만드는 그것의 내부 X 프록시를 사용하는 것이다.

4.3.3 다른 머신으로 테스트된 플랫폼/OS

- Linux
- Solaris
- Windows 95
- Windows NT (워크테이션과 서버 둘다)
- Windows For Workgroup 3.11 (TCP/IP 꾸러미 필요)
- Windows 3.1 (Chameleon 꾸러미 필요)
- Novel 4.01 Server
- OS/2 (Warp v3도 포함)
- Macintosh OS (MacTCP or 오픈 트랜스퍼 필요)
- DOS (NCSA Telnet 꾸러미 필요, DOS Trumpet은 부분적으로 작동한다.)
- Amiga (AmiTCP or AS225-stack 필요)
- UCX (VMS를 위한TCP/IP stack)을 가지는 VAX Stations 3520 과 3100
- Linux/Redhat을 사용한 Alpha/AXP
- SCO Openserver (v3.2.4.2 와 5)
- AIX가 돌아가는 IBM RS/6000
- (다른 플랫폼을 시도해본 사람은?)

4.4 IP Firewall 관리 (ipfwadm)

이 섹션에서는 ipfwadm을 사용하는 좀더 자세한 내용을 다룬다.

이것은 따르는 정적 PPP 주소를 가지는 PPP 링크 뒤의 방화벽/마스큐레이딩을 위한 설정이다. 믿을만한 인터페이스는 192.168.255.1이고 PPP 인터페이스는 죄의식을 덜기 위해 바꾸었다. :). 나는 채워진 루팅 그리고/혹은 마스큐레이딩과 마찬가지로 개인적으로 IP 속임수를 잡아내는 각각의 들어오고 나가는 인터페이스들의 목록을 작성하였다. 마찬가지로 명백하게 허락되지 않은 어떤 것도 금지된다.

```
#!/bin/sh
#
# /etc/rc.d/rc.firewall, 방화벽 설정의 정의, rc.local로부터 불려진다.
#
PATH=/sbin:/bin:/usr/sbin:/usr/bin
# 테스팅, 잠시 기다린 후 모든 방화벽 규칙을 제거한다.
# 만일 10분후에 방화벽이 자동적으로 해제 되기를 바란다면 아래 줄들의 주석을 제거하라.
#
# (sleep 600; \
# ipfwadm -I -f; \
# ipfwadm -I -p accept; \
# ipfwadm -O -f; \
# ipfwadm -O -p accept; \
# ipfwadm -F -f; \
# ipfwadm -F -p accept; \
# ) &
# 들어오기의 모든 방침을 없애고 기본방침을 거부로 정의한다.
# 실제로 기본 방침은 거부와 기록의 모든 규칙을 잡아내기 때문에 부적절하다.
ipfwadm -I -f
ipfwadm -I -p deny
# 지역 인터페이스, 지역 컴퓨터, 어디로 나가던지 유효
ipfwadm -I -a accept -V 192.168.255.1 -S 192.168.0.0/16 -D 0.0.0.0/0
# 원격 인터페이스, IP 속이기를 몰아내도록 지역 컴퓨터에 요구
ipfwadm -I -a deny -V 당신의.정적.PPP.주소 -S 192.168.0.0/16 -D 0.0.0.0/0 -o
# 원격 인터페이스, 영구 PPP주소로 가는 어떠한 출처도 유효
ipfwadm -I -a accept -V 당신의.정적.PPP.주소 -S 0.0.0.0/0 -D
당신의.정적.PPP.주소/32
# loopback 인터페이스가 유효
ipfwadm -I -a accept -V 127.0.0.1 -S 0.0.0.0/0 -D 0.0.0.0/0
# 모든 규칙을 잡아내고 모든 다른 들어오는 것들을 거부하고 기록함
# 방침에는 기록하도록 선택하는 것은 없지만 대신에 이것이 그역할을 한다.
ipfwadm -I -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o
# 나가기의 모든 방침을 없애고 거부의 기본 방침을 정한다.
# 실제로 기본 방침은 거부와 기록의 모든 규칙을 잡아내기 때문에 부적절하다.
ipfwadm -O -f
ipfwadm -O -p deny
# 지역 인터페이스를 거쳐 지역 렘막鮫 오는 어떠한 출처도 유효
ipfwadm -O -a accept -V 192.168.255.1 -S 0.0.0.0/0 -D 192.168.0.0/16
# 원격 인터페이스를 거쳐 지역 렘막括현나가기, 채워진 루팅, 거부
ipfwadm -O -a deny -V 당신의.정적.PPP.주소 -S 0.0.0.0/0 -D 192.168.0.0/16 -o
# 원격 인터페이스를 거쳐 지역 렘막觀壙驕 나가기, 내용을 가진 마스큐레이딩, 거부
ipfwadm -O -a deny -V 당신의.정적.PPP.주소 -S 192.168.0.0/16 -D 0.0.0.0/0 -o
```

```
# 원격 인터페이스를 거쳐 지역 렘막觀壙驕 나가기, 채워진 마스큐레이딩, 거부
ipfwadm -O -a deny -V 당신의.정적.PPP.주소 -S 0.0.0.0/0 -D 192.168.0.0/16 -o
# 원격 인터페이스를 거쳐 나가는 것은 유효
ipfwadm -O -a accept -V 당신의.정적.PPP.주소 -S 당신의.정적.PPP.주소/32 -D
0.0.0.0/0
# loopback 인터페이스 유효
ipfwadm -O -a accept -V 127.0.0.1 -S 0.0.0.0/0 -D 0.0.0.0/0
# 모든 규칙을 잡아내고 모든 다른 나가는 것들을 거부하고 기록함
# 방침에는 기록하도록 선택하는 것은 없지만 대신에 이것이 그역할을 한다.
ipfwadm -O -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o
# 되돌리기의 모든 방침을 없애고 거부의 기본 방침을 정한다.
# 실제로 기본 방침은 거부와 기록의 모든 규칙을 잡아내기 때문에 부적절하다.
ipfwadm -F -f
ipfwadm -F -p deny
# 지역 렘막觀壙驕 지역 인터페이스를 거쳐 다른 곳으로 나가는 마스큐레이딩
ipfwadm -F -a masquerade -W ppp0 -S 192.168.0.0/16 -D 0.0.0.0/0
# 모든 규칙을 잡아내고 모든 다른 되돌리기를 거부하고 기록함
# 방침에는 기록하도록 선택하는 것은 없지만 대신에 이것이 그역할을 한다.
ipfwadm -F -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o
```

당신은 특정한 사이트로의 트래픽을 -I, -O or -F.를 사용하여 막을수 있다. 규칙의 모임들은 위에서부터 아래로 읽혀지고 -a는 기존의 명령어들에다 추가하는 것을 뜻하므로 어떠한 제약들이 전역적인 규칙앞에 와야만 한다. 예를들면(시험되지 않음) :-

-I 규칙을 사용하기. 가장 빠른 것이지만 단지 지역 컴퓨터들만을 막을 뿐이고 방화벽 자신은 금지된 사이트로 접근할수 있다. 물론 당신은 이러한 조합들을 허락하기를 원할 것이다.

```
... -I 규칙의 시작 ...
# 204.50.10.13으로 가는 지역 컴퓨터들을 지역 인터페이스가 거부하고 기록함
reject and log local interface, local machines going to 204.50.10.13
ipfwadm -I -a reject -V 192.168.255.1 -S 192.168.0.0/16 -D 204.50.10.13/32 -o
# 지역 인터페이스를 거쳐 다른 곳으로가는 지역 컴퓨터가 유효
ipfwadm -I -a accept -V 192.168.255.1 -S 192.168.0.0/16 -D 0.0.0.0/0
... -I 규칙의 끝 ...
```

-O 규칙 사용하기. 패킷이 마스큐레이등을 먼저 거치기 때문에 가장 느리지만 이 규칙은 금지된 사이트에 방화벽이 접근하는 것도 막는다.

```
... -O 규칙의 시작 ...
# 204.50.10.13으로가는 것을 거부하고 기록함
ipfwadm -O -a reject -V 당신의.정적.PPP.주소 -S 당신의.정적.PPP.주소/32 -D
204.50.10.13/32 -o
# anything else outgoing on remote interface is valid
ipfwadm -O -a accept -V 당신의.정적.PPP.주소 -S 당신의.정적.PPP.주소/32 -D
0.0.0.0/0
... -O 규칙의 끝 ...
```

-F 규칙 사용하기. -I 보다는 느릴테지만 아직 마스큐레이드된 내부 컴퓨터들을 막을 수 있지만 방화벽은 아직도 금지된 사이트에 갈수 있다.

```
... -F 규칙의 시작 ...
```

```
# PPP 인터페이스를 거쳐 지역 렝막觀壙驕 204.50.10.13으로가는 것을 거부하고 기록함
ipfwadm -F -a reject -W ppp0 -S 192.168.0.0/16 -D 204.50.10.13/32 -o
# 지역 인터페이스를 거쳐 지역 렝막觀壙驕 다른 곳으로 가는 것을 마스큐레이드함.
ipfwadm -F -a masquerade -W ppp0 -S 192.168.0.0/16 -D 0.0.0.0/0
... -F 규칙의 끝 ...
```

192.168.0.0/16을 204.50.11.0로 가는 것을 허락하는 특별한 규칙은 필요없다. 그것은 전역 규칙에 의해 커버된다.

위의 규칙들에서 인터페이스를 짜는 여러 가지 방법이 있다. 예를 들면 -V 192.168.255.1대신에 -W eth0로 쓸 수 있다. -V 당신의.정적.PPP.주소 대신에 -W ppp0라고 쓸 수 있다. 개인적인 취향과 작성방법일 뿐이다.

4.5 IP Masquerade와 필요시 전화걸기

1. 당신이 인터넷에 자동적으로 연결되도록 네트웍을 설치하고자 하면 *diald* 필요시 전화걸기 꾸러미가 가장좋은 도구가 될것이다.
2. diald를 설치하기 위해서 *Setting Up Diald for Linux Page* `<http://home.pacific.net.sg/harish/diald.config.html>`을 확인해 보기 바란다.
3. 일단 diald와 IP Masquerade가 설치되면 당신은 어떠한 다른 컴퓨터에 가서 웹, 텔넷 혹은 ftp를 시작할 수 있다.
4. Diald는 들어오는 요구신호를 알아채고 당신의 인터넷 제공회사에 전화를 걸어 연결시킬 것이다.
5. 시간초과가 첫번째 연결 시에 발생할 것이다. 이것은 만일 아날로그 모뎀을 사용한다면 피할 수 없다. 모뎀으로 PPP 연결을 만들기 위해 사용되는 시간이 당신의 클라이언트 프로그램에서 시간초과를 발생시킨다. 만일 ISDN을 사용한다면 이것은 피할 수 있다. 당신이 해야할 것은 지금 사용하는 클라이언트 프로그램을 중지시키고 다시 실행하는 것 밖에는 없다.

4.6 IPautofw 패킷 전송자

IPautofw `<ftp://ftp.netis.com/pub/members/rlynch/ipautofw.tar.gz>`은 리눅스 마스큐레이딩을 위한 TCP와 UDP의 포괄적인 전달자이다. 일반적으로 UDP를 필요로 하는 꾸러미를 사용 가능하게 하려면 ip_masq_raudio, ip_masq_cuseeme 등과 같은 지정된 ip-masq 모듈이 적재되어야 한다. ipautofw는 보다 포괄적인 방법으로 행동한다. 특정한 그 어플리케이션에 특정한 모듈이 전송하지 않을 것들을 포함하는 어떠한 형태의 트래픽도 전송할 것이다. 이것은 적절하게 관리되지 않으면 보안에 구멍을 만들 수 있다.

제 5 절 기타

5.1 도움 구하기

**** 제발 IP Masquerade의 문제점이나 질문에 대하여 나에게 email을 보내지 않도록 하라. 개인적으로 처리해야 할 일들 때문에 website에 관련되지 않은 모든 질문에 대해 답장을 약속할수 없다. 대신에 제발 당신이 가진 질문을 도움을 받는 가장 좋은 방법이라고 개인적으로 생각되는 IP Masquerade mailing list에 올려라. 이점에 대해 미안하지만 나는 몇주 후에 당신이 답장을 받는 것을 원하지 않는다.**

- *IP Masquerade Resource page* `<http://ipmasq.home.ml.org/>`은 IP 마스큐레이드를 설치하는데 충분한 정보를 가지고 있다.

- IP 마스큐레이드 메일링 리스트에 참가하라(추천)
구독하기 위해서 masq-request@indyramp.com로 "subscribe"(따옴표 없이)를 제목을 쓰고 메일 보내라.
구독을 취소하기 위해 masq-request@indyramp.com로 "unsubscribe"(따옴표 없이)를 제목을 쓰고 메일 보내라.
메일링 리스트를 사용하는 도움을 얻기 바라면 masq-request@indyramp.com로 "archive help" 혹은 "archive dir"(따옴표 없이)를 제목을 쓰고 메일 보내라.

- *IP masquerade mailing list archive* <http://www.indyramp.com/masq/list/>는 메일링 리스트에 보내진 모든 지나간 내용을 담고 있다.

- 이 *Linux IP Masquerade mini HOWTO* <http://ipmasq.home.ml.org/ipmasq-HOWTO.html>는 커널 2.x을 위한것이다. (만일 1.3.x 혹은 2.x 커널을 사용한다면)

- 만일 오래된 커널을 사용한다면 *IP Masquerade HOWTO for kernel 1.2.x* <http://ipmasq.home.ml.org/ipmasq-HOWTO-1.2.x.txt>

- *IP masquerade FAQ* <http://www.indyramp.com/masq/ip_masquerade.txt>은 몇가지 일반적인 정보를 가지고 있다.

- *X/OS Ipfwadm page* <http://www.xos.nl/linux/ipfwadm/>은 ipfwadm 꾸러미에 관한 솔스, 실행화일, 문서 그리고 그밖의 정보를 가지고 있다.

- Lee Nevo의 *applications that work thru Linux IP masquerading* <http://masqapps.home.ml.org>에는 IP 마스큐레이드에서 프로그램들이 작동하도록 하게하는 팁과 속임수를 마련해 놓고 있다.

- *LDP Network Administrator's Guide* <http://linuxwww.db.erau.edu/NAG/>는 네트웍을 설치하고자 하는 초보자들게 필수적이다.

- *Linux NET-2 HOWTO* <http://www.caldera.com/LDP/HOWTO/NET-2-HOWTO.html> 또한 리눅스 네트워킹에 관한 많은 유용한 정보를 가지고 있다.

- *Linux ISP Hookup HOWTO* <http://www.caldera.com/LDP/HOWTO/ISP-Hookup-HOWTO.html> 과 *Linux PPP HOWTO* <http://www.caldera.com/LDP/HOWTO/PPP-HOWTO.html>는 인터넷에 리눅스 호스트를 어떻게 연결시키는가에 관한 정보를 준다.

- *Linux Ethernet-Howto* <http://www.caldera.com/LDP/HOWTO/Ethernet-HOWTO.html>는 좋은 이떠넷을 돌리는 LAN을 설치하는데 관련된 좋은 정보들을 가지고 있다.

- 당신은 아마도 *Linux Firewalling and Proxy Server HOWTO* <http://www.caldera.com/LDP/HOWTO/Firewall-HOWTO.html>에 관심을 가질지도 모른다.

- *Linux Kernel HOWTO* <http://www.caldera.com/LDP/HOWTO/Kernel-HOWTO.html>는 커널 컴파일 과정을 안내해 줄것이다.

- 다른 Kernel HOWTO와 같은 *Linux HOWTOs* <http://www.caldera.com/LDP/HOWTO/HOWTO-INDEX-3.html>

- 유즈넷 뉴스그룹 comp.os.linux.networking으로 게시

5.2 감사하기

- Gabriel Beitler, gbeitler@aciscorp.com
on providing 섹션 3.3.8을 제공 (Novel 설정하기)

- Ed Doolittle, dolittle@math.toronto.edu
개선된 보안을 위해 ipfwadm 명령에 -V옵션의 사용을 제안

- Matthew Driver, mdriver@cfmeu.asn.au
  섹션 3.3.1(윈도우즈 95 설정)을 마련하고 이 HOWTO에 널리 도움을 줌
- Ken Eves, ken@eves.com
  이 하우투를 위한 고귀한 정보를 마련한 FAQ작성
- Ed. Lott, edlott@neosoft.com
  검사된 시스템과 소프트웨어의 긴 목록을 위해
- Nigel Metheringham, Nigel.Metheringham@theplanet.net
  이 하우투를 보다 좋고 기술적인 문서로 만든 그의 IP 패킷 필터링과 IP 마스큐레이딩 하우투를 기부
  섹션 4.1, 4.2, 과 기타
- Keith Owens, kaos@ocs.com.au
  ipfwadm 섹션 4.2에서 훌륭한 안내를 마련함
  보안 구멍을 피하기 위한 `ipfwadm -deny` 옵션의 교정과 IP 마스큐레이드상에서 `ping`의 상태를 명확하게 함.
- Rob Pelkey, rpelkey@abacus.bates.edu
  섹션 3.3.6과 3.3.7을 마련 (MacTCP 와 Open Transport의 설정)
- Harish Pillay, h.pillay@ieee.org
  섹션 4.5를 마련(diald를 사용하는 다이알-온-디맨드)
- Mark Purcell, purcell@rmcs.cranfield.ac.uk
  섹션 4.6(IPautofw)를 마련
- Ueli Rutishauser, rutish@ibm.net
  섹션 3.3.9를 마련 (OS/2 Warp의 설정)
- John B. (Brent) Williams, forerunner@mercury.net
  섹션 3.3.7을 마련(Open Transport를 설정)
- Enrique Pessoa Xavier, enrique@labma.ufrj.br
  bootp 설정 제안
- 이러한 훌륭한 기능을 마련한 IP 마스큐레이드 개발자들
  - Delian Delchev, delian@wfpa.acad.bg
  - Nigel Metheringham, Nigel.Metheringham@theplanet.net
  - Keith Owens, kaos@ocs.com.au
  - Jeanette Pauline Middelink, middelin@polyware.iaf.nl
  - David A. Ranch, trinity@value.net
  - Miquel van Smoorenburg, miquels@q.cistron.nl
  - Jos Vos, jos@xos.nl
  - 그리고 여기에 언급안된 많은 이들 (알려주세요)
- 메일링리스트에 답변과 제안을 보내준 많은 사용자들, 특별히 문서의 잘못을 보고한 사람들과 지원되고 안되는 클라이언츠들을 보고해준 사람들
- 만일 동료 사용자가 내게 보내준 정보를 포함하지 않았다면 사과한다. 내게 많은 계안과 아이디어가 보내졌지만 단지 검증할 충분한 시간이 없었거나 그 기록을 잃어버렸다. 이 하우투에 내게 보내준 모든 정보를 포함시키려고 최선을 다하고자 했다. 당신의 노력에 감사하고 내 상황을 이해하기를 바란다.

5.3 참고

- Ken Eves의 IP masquerade FAQ
- Indyramp Consulting의 IP masquerade mailing list archive
- X/OS의 Ipfwadm page
- 리눅스 하우투에 연관된 다양한 네트워킹