IP маскиране с ipchains

Миналия месец, аз и брат ми решихме да направим малка домашна мрежа, така че да можем да свържем към Интернет повече от един компютър с използване само на един модем и телефонна линия. Моята машина е тази с модема и на нея е инсталиран Linux(Server). Машината на брат ми е с Windows95(Client). Направих известни проучвания и намерих документация относно изграждането на "частни" мрежи. Реших да използвам техниката на IP маскирането при свързване на нашата малка "частна" мрежа към Интернет.

IP маскирането е техника, при която на компютрите се назначават "вътрешни" IP адреси (в случая 10.0.0.1 за server и 10.0.0.2 и 10.0.0.3 за client) и споделяш връзката на един компютър с останалите клиенти, без да е нужно да им се назначават "външни" (реални IP) адреси. Прочетох доста от документацията и наистина си изясних процеса като цяло, но така и не успях да го настроя да върви правилно на моята машина. Тогава влязох в #LinuxIRC канала на Undernet.org и там намерих един тип с прякор Mongoose, който ми помогна. Даде ми линка към бързия справочник за настройване на IP маскиране с ipchains, който той беще написал. Програмата ipchains се разпространява с RedHat 6.0 и се използва за настройване на IP маскиране и firewall.
След като го прочетох, пуснах мрежата за по-малко от 10 минути. Поради това отново се свързах с него и той се съгласи да публикувам справочника му в Linux Gazette.

Следва справочника:

БЕЛЕЖКИ

В долния пример са използвани:

0.0.0.0 IP адрес на шлюза по подразбиране (default gateway)
10.0.0.1 IP адрес на мрежовия адаптер eth0 на server
10.0.0.2 IP адрес на мрежовия адаптер eth0 на client1
10.0.0.3 IP адрес на мрежовия адаптер eth0 на client2

НАСТРОЙКА НА SERVER

1. Зареждане модула на ethernet адаптера (ако е нужно):
   /sbin/modprobe ne2k-pci (всеки адаптер е с отделно име)
2. Стартиране на адаптера:
   (добавете го към /etc/rc.d/rc.local, ако нямате стандартни скриптове за интерфейсите)
   /sbin/ifconfig eth0 10.0.0.1 netmask 255.255.255.0 up
   /sbin/route add -net 10.0.0.0 netmask 255.255.255.0 eth0
   /sbin/route add default gw 0.0.0.0 eth0
3. Разрешете на IP MASQ клиентите на ползват inet
   A. Добавете следното в края на /etc/hosts.allow
   ALL:10.0.0.2
   ALL:10.0.0.3
   B. Добавете IP адресите в други конфигурационни файлове ако трябва.
4. НАСТРОЙКА НА LINUX IP MASQ КЛИЕНТ (с адрес 10.0.0.2)

1. Зареждане модула на ethernet адаптера (ако е нужно):
   /sbin/modprobe ne2k-pci
2. Стартиране на адаптера:
   (добавете го към /etc/rc.d/rc.local, ако нямате стандартни скриптове за интерфейсите)
   /sbin/ifconfig eth0 10.0.0.2 netmask 255.255.255.0 up
   /sbin/route add -net 10.0.0.0 netmask 255.255.255.0 eth0
   /sbin/route add default gw 10.0.0.1 eth0

ПРОВЕРКА НА МРЕЖАТА

1. Ping 10.0.0.1 (сървъра) от клиентите и обратно
2. Използвайте /sbin/ifconfig да видите трафика на пакети от всеки хост
3. Би трябвало да може да направите telnet/ftp връзка от клиентите към сървъра и обратно, ако не можете, то проверете /etc/hosts.allow

НАСТРОЙКА НА IP МАСКИРАНЕТО

1. Настройка на рутирането (IP forwarding) на пакети:
   A. Разрешете рутирането на пакети в сървъра:
   echo "1" > /proc/sys/net/ipv4/ip_forward

B. Разрешете рутирането на пакети в сървъра при бутване на машината:
а)За RedHat редактирайте /etc/sysconfig/network както следва:
FORWARD_IPV4=true
б)За други дистрибуции добавете в края на /etc/rc.d/rc.local следното:
echo "1" > proc/sys/net/ipv4/ip_forward
C. За да сте сигурни, че никой не smurf-ира мрежата добавете към rc.local следното:
echo "1" > /proc/sys/net/ipv4/tcp_syncookies

2. Настройка на маскирането. Може да добавите следното към rc.local, за да се изпълнява всеки път:
A. Забранете маскирането по подразбиране:
/sbin/ipchains -P forward DENY
B. Маскиране на пакетите на машини 10.0.0.2 и 10.0.0.3
/sbin/ipchains -A forward -s 10.0.0.2/24 -j MASQ
/sbin/ipchains -A forward -s 10.0.0.3/24 -j MASQ
C. Добавете IP MASQ модулите, които желаете
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_quake
/sbin/modprobe ip_masq_irc
/sbin/modprobe ip_masq_user
/sbin/modprobe ip_masq_raudio

С тези указания, вашата мрежа би трябвало да тръгне веднага. След настройване на маскирането се натъкнах на друг проблем - клиентите можеха да се свързват с сървъра само по IP адрес. Така че, се наложи да пусна и DNS на машината с Linux, за да могат клиентите да се свързват и по име. Единственото, което трябва да се направи е да се въведат в /etc/resolv.conf адресите на DNS сървърите, и да се уверите че named демона е активиран. Това би трябвало да реши проблема.
Ако искате да научите повече за IP MASQ и Firewalling може да проверите HOWTO документацията на: