NAT и DHCP за пять минут

Настраиваем NAT

Для начала, нужно включить *ip forwarding*. Проверим, не включен ли он:

```
$ cat /proc/sys/net/ipv4/ip_forward
```

Если выдаст 0 – выключен, 1 – соответственно включен.

Чтобы включить:
```
$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

А чтобы включит навсегда в файл */etc/sysctl.conf* добавляем следующие строчки:

```
net.ipv4.conf.default.forwarding=1
net.ipv4.conf.all.forwarding=1
```

Затем включаем (раскомментируем) в файле */etc/sysctl.conf* параметр

```
net.ipv4.ip_forward=1
```

Теперь, чтобы изменения вступили в силу выполним команду

```
sysctl -p
```

Осталось включить NAT. Делается это всего одной командой (*см. ниже*):

```
iptables -A POSTROUTING -t nat -j MASQUERADE
```

Однако сделать так, чтобы данное правило применялось после перезапуска системы несколько сложнее, но не сильно.

Создаем в директории */etc/network/if-pre-up.d/* файл с любым именем, к примеру, *nat* и вносим в него следующие строки:

```
#!/bin/sh
/sbin/iptables -A POSTROUTING -t nat -j MASQUERADE
```

Сохраняем файл, после чего выставляем ему права на запуск командой:

```
chmod +x /etc/network/if-pre-up.d/nat
```

Все, на этом простейшая настройка NAT в Debian закончена. Тем не менее, хорошим дополнением к NAT будет функция автоматической раздачи IP-адресов, которую обеспечивает DHCP-сервер.

Устанавливаем DHCP-сервер под Debian

```
aptitude install isc-dhcp-server
```

Настраиваем DHCP-сервер

Прежде всего открываем файл /etc/default/isc-dhcp-server и в строке INTERFACES=”” вписываем имя интерфейса, который будет обслуживать DHCP сервер, к примеру:

```
INTERFACES="eth1"
```

Теперь нужно настроить основной конфигурационный файл nano /etc/dhcp/dhcpd.conf. Параметры, которые нам интересны:

default-lease-time 36000; – устанавливает через сколько происходит повторный запрос адреса,
max-lease-time 72000; – сколько будет действовать адрес после того, как не удалось повторно получить адрес от сервера,
authoritative; – раскомментируем строку, если это основной DHCP-сервер в сети

Далее идет описание подсети:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
range 192.168.0.10 192.168.0.100;
option domain-name-servers 8.8.8.8;
option routers 192.168.0.2;
}
```

Где в первой строке указаны подсеть и маска подсети, во второй – с какого и по какой выдавать адреса, в третьей – список DNS-

серверов, в четвертой — роутер по умолчанию.

После внесения данных настроек можно запускать DHCP-сервер:

```
/etc/init.d/isc-dhcp-server start
```

Настроим минимальную фильтрацию входящих и пересылаемых пакетов. Исхожу из того, что *eth1 — интерфейс к внутренней сети*, а *eth0 — к внешней*. При желании, можно добавить адрес используемой подсети, но интерфейса, в целом, достаточно.

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p icmp -j ACCEPT #ICMP, например, echo responce, echo request, fragmentation needed,
#port unreachable, no route to host и прочие. К слову, нагрузка в icmp может служить незаткнутым каналом
#передачи, внимательнее изучите его при настройке корпоративных сетей.
iptables -A INPUT -i eth1 -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT #Если, к примеру, хотим пустить ssh извне.
iptables -A INPUT -i eth0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

Кроме того, NAT должен осуществляться *только в одном направлении*, поэтому:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

После всего этого добра сохраним результат:

```
iptables-save > /etc/network/if-pre-up.d/nat
```

Логирование

По умолчанию, логируется всё в */var/log/syslog*, что не очень удобно если вам нужно работать с логами.

Создадим файл */etc/rsyslog.d/dhcpd.conf* с содержимым:

```
local7.* /var/log/dhcpd.log
```

Для ротации логов в файл */etc/logrotate.d/rsyslog* вставить строку:

```
/var/log/dhcpd.log
```

Перезапускаемся:

```
# /etc/init.d/isc-dhcp-server restart
# /etc/init.d/rsyslog restart
```

Теперь, смотрим лог в */var/log/dhcpd.log*
На этом пока закончим настройку NAT и DHCP-сервера под Debian.