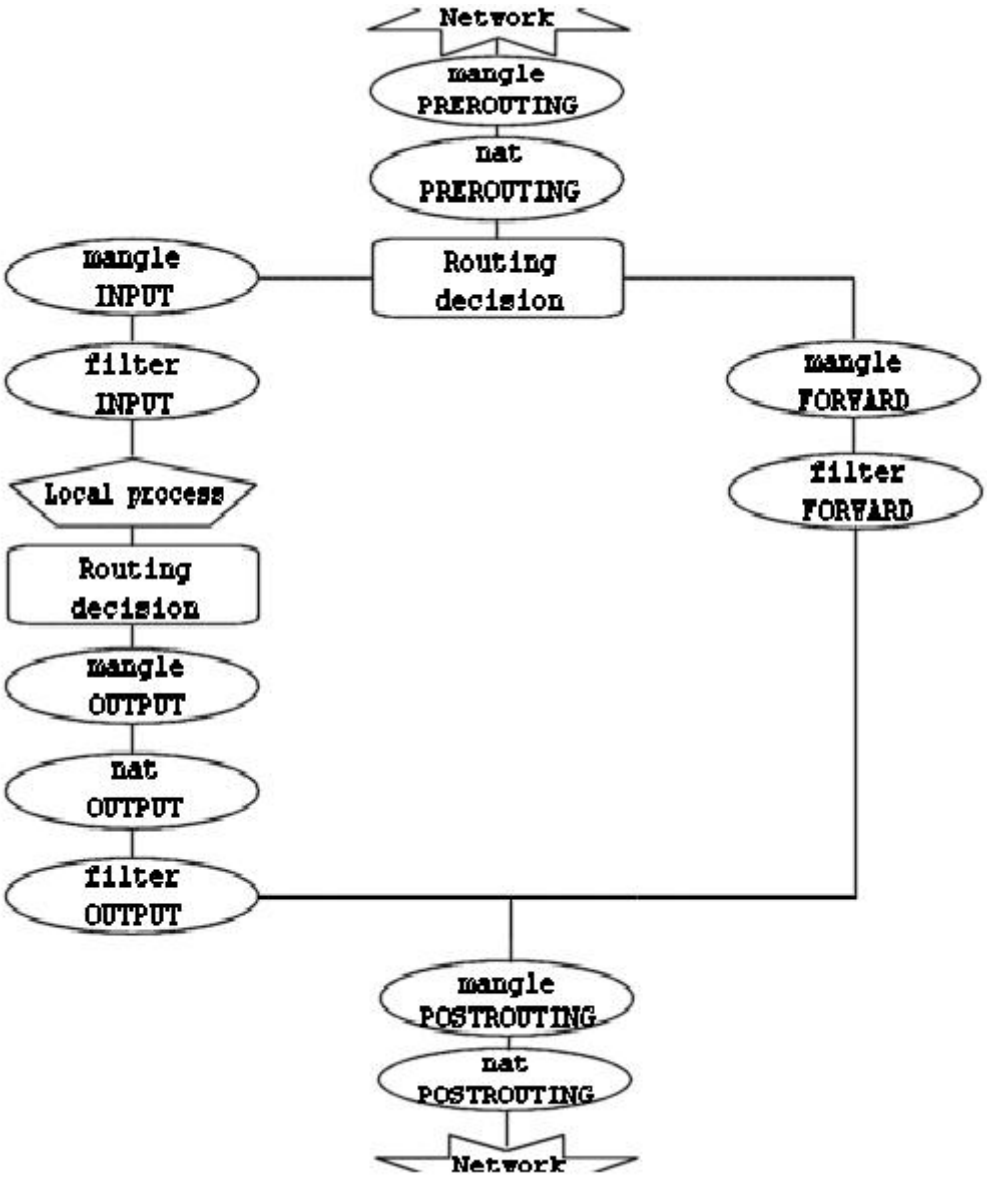
Что это?

iptables — утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для ядер Linux версий 2.4, 2.6, 3.x, 4.x. Для использования утилиты iptables требуются привилегии суперпользователя (root).

Цепочки, схема

Input — обрабатывает входящие пакеты и подключения. Например, если какой-либо внешний пользователь пытается подключиться к вашему компьютеру по ssh или любой веб-сайт отправит вам свой контент по запросу браузера. Все эти пакеты попадут в эту цепочку;
forward — эта цепочка применяется для проходящих соединений. Сюда попадают пакеты, которые отправлены на ваш компьютер, но не предназначены ему, они просто пересылаются по сети к своей цели.
output — эта цепочка используется для исходящих пакетов и соединений. Сюда, например, попадают пакеты, когда вы запускаете браузер и пытаетесь открыть любой сайт.
prerouting — в эту цепочку пакет попадает перед обработкой iptables, система еще не знает куда он будет отправлен, в input, output или forward;
postrouting — сюда попадают все проходящие пакеты, которые уже прошли цепочку forward



Добавление/удаление правил

Действия над пакетами:
ACCEPT — разрешить прохождение пакета дальше по цепочке правил;
DROP — удалить пакет;
REJECT — отклонить пакет, отправителю будет отправлено сообщение, что пакет был отклонен;
LOG — сделать запись о пакете в лог файл;
QUEUE — отправить пакет пользовательскому приложению.

Синтаксис:

```
# iptables -t таблица действие цепочка дополнительные_параметры
```

Опции:
-A — добавить правило в цепочку;
-C — проверить все правила;
-D — удалить правило;
-I — вставить правило с нужным номером;

-L — вывести все правила в текущей цепочке;
-S — вывести все правила;
-F — очистить все правила;
-N — создать цепочку;
-X — удалить цепочку;
-P — установить действие по умолчанию

Дополнительные опции:
-p — указать протокол, один из tcp, udp, icmp и др.;
-s — указать ip адрес устройства-отправителя пакета;
-d — указать ip адрес получателя;
-i — входной сетевой интерфейс;
-o — исходящий сетевой интерфейс;
-j — выбрать действие, если правило подошло.

Примеры:
Вывод всех правил на экран:

```
# iptables -L
```

Вывод всех правил на экран с нумерацией строк:

```
# iptables -L INPUT -n --line-numbers
```

Вывод правил для цепочки INPUT

```
# iptables -L INPUT
```

Блокировка всех входящих пакетов от 10.0.0.1:

```
# iptables -A INPUT -s 10.0.0.1 -j DROP
```

Блокировка всех исходящих пакетов от 10.0.0.1:

```
# iptables -A OUTPUT -s 10.0.0.1 -j DROP
```

Блокировка всех входящих соединений от 10.0.0.1 по ssh:

```
# iptables -A INPUT -p tcp --dport ssh -s 10.0.0.1 -j DROP
```

Очистить все правила

```
# iptables -F
```

Очистить все правила в цепочке INPUT:

```
# iptables -F INPUT
```

Удаления правила для всех входящих пакетов от 10.0.0.1:

```
# iptables -D INPUT -s 10.0.0.1 -j DROP
```

Добавить правило на 3 место в цепочке INPUT (остальные сдвинутся ниже):

```
# iptables -I INPUT 3 -p tcp --dport ssh -s 10.0.0.1 -j DROP
```

Удалить 3 правило в цепочке INPUT:

```
# iptables -D INPUT 3
```

Сохранение после перезагрузки

Debian:

```
# /sbin/iptables-save
```

Red Hat/CentOS:

```
# /sbin/service iptables save
```

или для Debian

```
# sh -c "iptables-save > /etc/iptables.up.rules"
```

и в настройках интефейса прописать

```
pre-up iptables-restore < /etc/iptables.up.rules
```

SNAT, DNAT, MASQUERADE

DNAT — от англ. Destination Network Address Translation — Изменение Сетевого Адреса Получателя. DNAT — это изменение адреса назначения в заголовке пакета. Зачастую используется в паре с SNAT. Основное применение — использование единственного реального IP-адреса несколькими компьютерами для выхода в Интернет и предоставления дополнительных сетевых услуг внешним клиентам.
SNAT — от англ. Source Network Address Translation — Изменение Сетевого Адреса Отправителя. SNAT — это изменение исходного адреса в заголовке пакета. Основное применение — использование единственного реального IP-адреса несколькими компьютерами для выхода в Интернет. В натоящее время диапазон реальных IP-адресов, по стандарту IPv4, недостаточно широк, и его не хватает на всех (переход на IPv6 разрешит эту проблему).
Маскировка (MASQUERADE) применяется в тех же целях, что и SNAT, но в отличие от последней, MASQUERADE дает более сильную нагрузку на систему. Происходит это потому, что каждый раз, когда требуется выполнение этого действия — производится запрос IP адреса для указанного в действии сетевого интерфейса, в то время как для SNAT IP адрес указывается непосредственно. Однако, благодаря такому отличию, MASQUERADE может работать в случаях с динамическим IP адресом, т.е. когда вы подключаетесь к Интернет, скажем через PPP, SLIP или DHCP.

Предположим у нас есть сервер с двумя интерфейсами. Один смотрит в Интернет, другой в локальную сеть и не забывает про правила для input и output. Раздадим интернет:
Для начала разрешаем шлюзу передавать транзитный трафик:

```
# sysctl net.ipv4.ip_forward=1
```

Разрешаем проходить трафику из и в локальную сеть,например, 10.1.30.0/24:

```
# iptables -A FORWARD -s 10.1.30.0/24 -j ACCEPT
# iptables -A FORWARD -d 10.1.30.0/24 -j ACCEPT
```

Для статического внешнего адреса интерфейса:

```
# iptables -A POSTROUTING -s 10.0.3.0/24 -o eth1 -j SNAT --to-
source внешний_адрес_интерфейса
```

Для динамического внешнего адреса интерфейса:

```
# iptables -A POSTROUTING -s 10.0.3.0/24 -o eth1 -j MASQUERADE
```

DNAT подменяет адрес назначения для входящих пакетов, позволяя «пробрасывать» адреса или отдельные порты внутрь локальной сети. Например:
Для начала разрешаем шлюзу передавать транзитный трафик:

```
# sysctl net.ipv4.ip_forward=1
```

Разрешаем проходить траффику из и в локальную сеть,например, 10.1.30.0/24:

```
# iptables -A FORWARD -s 10.1.30.0/24 -j ACCEPT
# iptables -A FORWARD -d 10.1.30.0/24 -j ACCEPT
```

Из внешнего источника по порту 29001 можно получить доступ по ssh к компьютеру во внутренней сети 10.1.30.40:

```
# iptables -A PREROUTING -s адрес/сеть_внешнего_источника -i eth1
-p tcp -m tcp --dport 29001 -j DNAT --to-destination
10.1.30.40:22
```

Рекомендуемые источники информации

Руководство по iptables (opennet.ru)
ru. wikibooks. nym .su/wiki/Iptables — Iptables
Базовая настройка брандмауэра iptables

—
Источники:
ru. wikibooks. nym .su/wiki/Iptables — Iptables
Настройка iptables для чайников (Материал распространяется под лицензией CC-BY-SA)
Руководство по iptables (opennet.ru)