# Занятие 20.

***Тема:*** **Сетевое администрирование Linux. Iptables.**

***Вид занятия:*** лекция, практическое занятие.

***Учебные вопросы:***

1. Таблицы. Цепочки. Прохождение трафика. Механизм определения состояний.
2. Базовый синтаксис и команды.

***Время:*** 90 минут

***Литература:***

1. Oscar Anderson. Iptables Tutorial. В переводе Андрея Киселева. http://www.opennet.ru/docs/RUS/iptables/
2. Таблицы Iptables. http://www.protocols.ru/modules.php?name=News&file=article&sid=100

## Ход занятия.

1. Iptables — это программный интерфейс к файрволу ядра Netrfilter. Iptables представляет собой утилиту командной строки, а Netfilter загружается в ядро в качестве модулей (основным из которых является ip_tables).

Ядро обрабатывает трафик в определенном порядке. Модули для обработки трафика называются таблицами, в которых существуют по умолчанию несколько цепочек для обработки пакетов. Вот список существующих таблиц и их назначение:

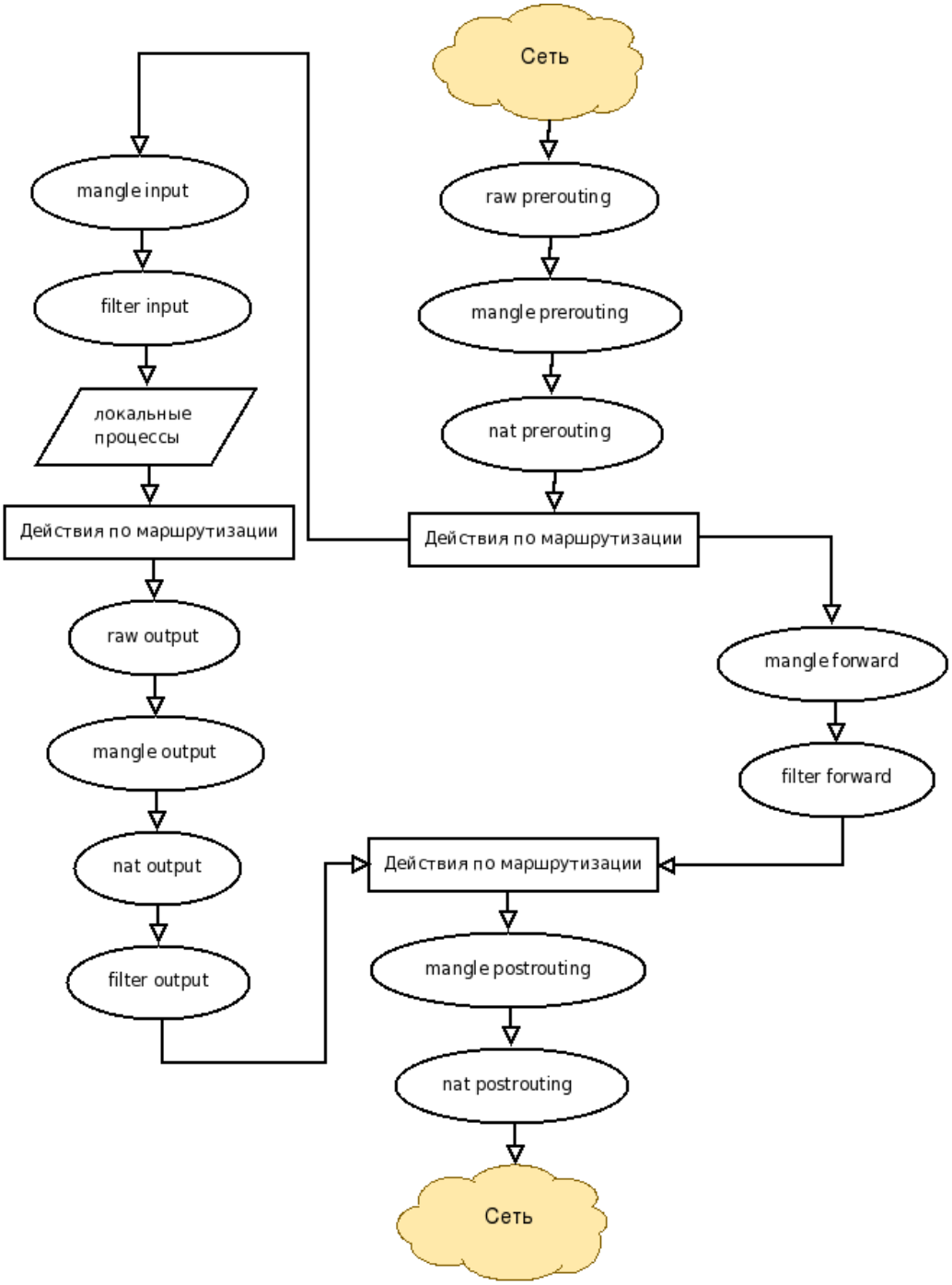
| **Название таблицы** | **Цепочки по умолчанию** | **Назначение** |
|---|---|---|
| RAW | PREROUTING, OUTPUT | Выбор пакетов, не обрабатываемых системами контроля соединений и nat. Возможные действия: NOTRACK |
| MANGLE | PREROUTING, INPUT, OUTPUT, FORWARD, POSTROUTING | Внесение изменений в заголовки пакетов. Основные действия: TOS, TTL, MARK |
| NAT | PREROUTING, OUTPUT, POSTROUTING | Преобразование сетевых адресов. Основные действия: DNAT, SNAT, MASQURADE, |
| FILTER | INPUT, OUTPUT, FORWARD | Фильтрация пакетов. Основные действия: ACCEPT, DROP |

Синтаксис Iptables позволяет создавать свои цепочки, куда перенаправлять трафик по определенным критериям. Общая схема прохождения трафика такова, что в одной таблице пакету может быть назначено только одно действие, однако пакет может быть обработан в других таблицах. Наиболее используемые действия:

| **Действие** | **Значение** |
|---|---|
| Переход | При соответствии пакета указанным критериям, он передается на обработку в свою созданную цепочку, после прохождения которой, пакет будет возвращен в цепочку, откуда вызван переход, если в своей цепочке он не был обработан |
| ACCEPT | Пакет принят в этой таблице. Передается на обработку в следующую. |
| DROP | Пакет отброшен. Движение пакета прекращается. |
| DNAT | Destination NAT. Имеет дополнительный параметр --to-destination IP |
| SNAT | Source NAT. Имеет дополнительный параметр --to-source IP |
| REJECT | Пакет не принят. Хост-источник получит пакет Destination unreachable |

| | |
|---|---|
| LOG, ULOG | Позволяют журналировать информацию о пакете. Имеют много дополнительных параметров |
| MASQUERADE | По сути это SNAT, но динамически определяющий IP на исходящем интерфейсе, что позволяет его использовать, например, с DHCP. Имеет пареметр --to-ports. |
| REDIRECT | Позволяет перенаправлять пакеты с одного порта на другой. Имеет параметр --to-ports |

Вот схема прохождения трафика по цепочкам:



Кроме основного функционала, Iptables способен подгружать дополнительные модули, для дополнительной обработки. Одним из таких модулей является модель обработки состояний пакета state. Он позволяет указывать состояние пакета:

| **Состояние** | **Описание** |
|---|---|
| NEW | Пакет открывает новое соединение (TCP) или принадлежит однонаправленному потоку |
| RELATED | Показывает, что пакет принадлежит уже имеющемуся соединению, но открывает новое. Например, открывается сессия передачи данных в FTP |
| ESTABLISHED | Соединение установлено, пакеты идут в обоих направлениях |
| INVALID | Пакет связан с неизвестным потоком или соединением или имеет ошибки в заголовке |

2. Консольная команда iptables принимает в качестве параметров описание одного правила. В базовом варианте для загрузки правил подразумевается создание скрипта вида:

```
#!/bin/bash
#rc.firewall — load iptables rules
PROG='/sbin/iptables'
#clear all chains tables
$PROG -F

#filter table
$PROG -A INPUT -t filter -p TCP -s 80.32.5.7/32 -d 0.0.0.0 —dport 80 -j ACCEPT
…
```

Команда принимает следующие основные параметры для работы с цепочками:

| | |
|---|---|
| -A CHAIN | добавить правило в конец цепочки CHAIN |
| -F CHAIN | обнулить цепочку CHAIN |
| -I CHAIN N | вставить правило в цепочку CHAINc номером N |
| -D CHAIN | удалить правило из цепочки CHAIN |
| -R CHAIN N | заменить правило N в цепочке CHAIN |
| -L CHAIN | показать список правил в цепочке CHAIN |
| -N CHAIN | создать цепочку CHAIN |
| -X CHAIN | удалить цепочку CHAIN |
| -E CHAIN1 CHAIN2 | переименовать цепочку CHAIN1 в CHAIN2 |
| -P CHAIN policy | задать политику по умолчанию (ACCEPT или DROP) |
| -Z CHAIN | обнулить все счетчики внутри цепочки |

Для параметров используются критерии:

| | |
|---|---|
| -t TABLE | указывает таблицу для цепочки |
| -p | протокол (IP, TCP, UDP, ALL и т.д.) |
| -s | адрес источника с маской |
| -d | адрес приемника с маской |
| -i | входящий интерфейс |
| -o | исходящий интерфейс |
| --sport | порт на источнике (только для TCP и UDP) |
| --dport | порт на приемнике (только для TCP и UDP) |
| --tcp-flags | флаги (только для TCP). Принимает значения SYN, ACK, RST, FIN, URG, PSH |
| --syn | соответствует пакетам с установленным флагом SYN и сброшенными флагами ACK и FIN (только для TCP) |
| --icmp-type | указывает тип ICMP-пакета (только для ICMP) |
| -m модуль | загружает дополнительный модуль |
| -m mac --mac-source | позволяет указать MAC-адрес источника |
| -m state --state | позволяет определить состояние пакета |
| -j | указывает действие |

Примеры:

```
iptables -P INPUT ACCEPT -t filter
iptables -A INPUT -t filter -p TCP -s 192.168.1.1/32 -d 192.168.2.0/24 --dport 25 -j DROP
iptables -A POSTROUTING -t nat -p ALL -s 192.168.1.0/24 -j SNAT --to-source 192.168.1.5
iptables -N mychain -t filter
iptables -A OUTPUT -t filter -d 193.19.64.11 --dport 21 -j mychain
iptables -A mychain -t filter -s 192.168.1.0/24 -j ACCEPT
iptables -A mychain -t filter -s 192.168.2.0/24 -j REJECT
iptables -A FORWARD -t filter -m mac --mac-source 11:22:33:44:55:66 -j ACCEPT
iptables -A INPUT -t filter -p TCP -d 192.168.1.0/32 --dport 21 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```