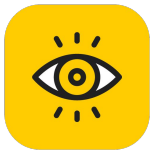
OTUS

Онлайн образование

otus.ru

Проверить, идет ли запись

Меня хорошо видно && слышно?



Фильтрация трафика. iptables, firewalld

Linux. Professional

Федоров Денис

Ведущий инженер по разработке в Сбер

fedorov.tech/denis

Преподаватель

Федоров Денис

Специалист по компьютерным сетям и linux-системам.
Более 5 лет в IT.

Начинал свой карьерный путь с младшего администратора в аутсорсинговой компании. В настоящий момент работает Ведущим инженером по разработке в Сбер.

Интересуется Linux и любит делится своим опытом с начинающими специалистами. Активно занимается преподавательской деятельностью на различных онлайн-образовательных площадках.

- преподаватель Linux в OTUS

Маршрут интенсива

- Знакомство ✅
- netfilter
- iptables
- firewalld

Правила вебинара

Активно участвуем

Задаем вопросы в чат

Вопросы вижу в чате,
могу ответить не сразу

2 дня
1.5 часа

Пишем в чат

Цели вебинара

Научиться настраивать брандмауэр в linux

1. Понятие firewall
2. iptables
3. FirewallD

Брандмауэр

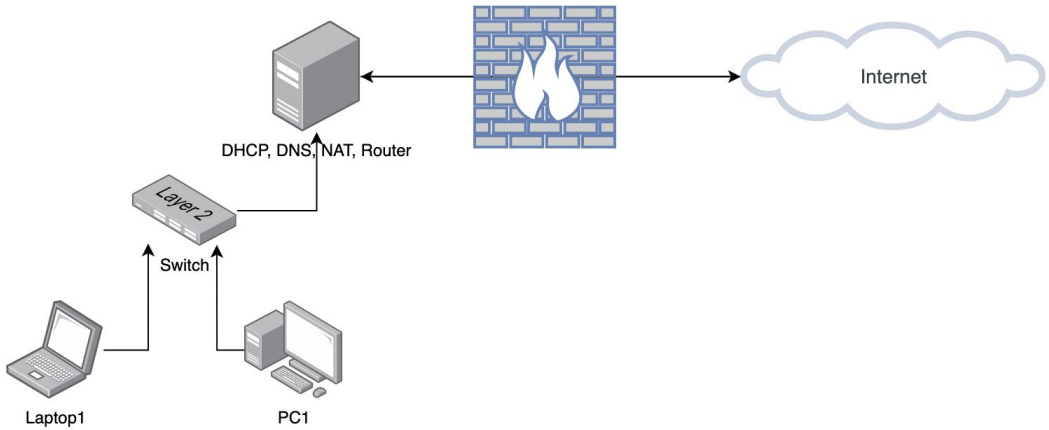
firewall

Реализация firewall

netfilter

1) iptables
2) nftables

A. firewalld
B. ufw



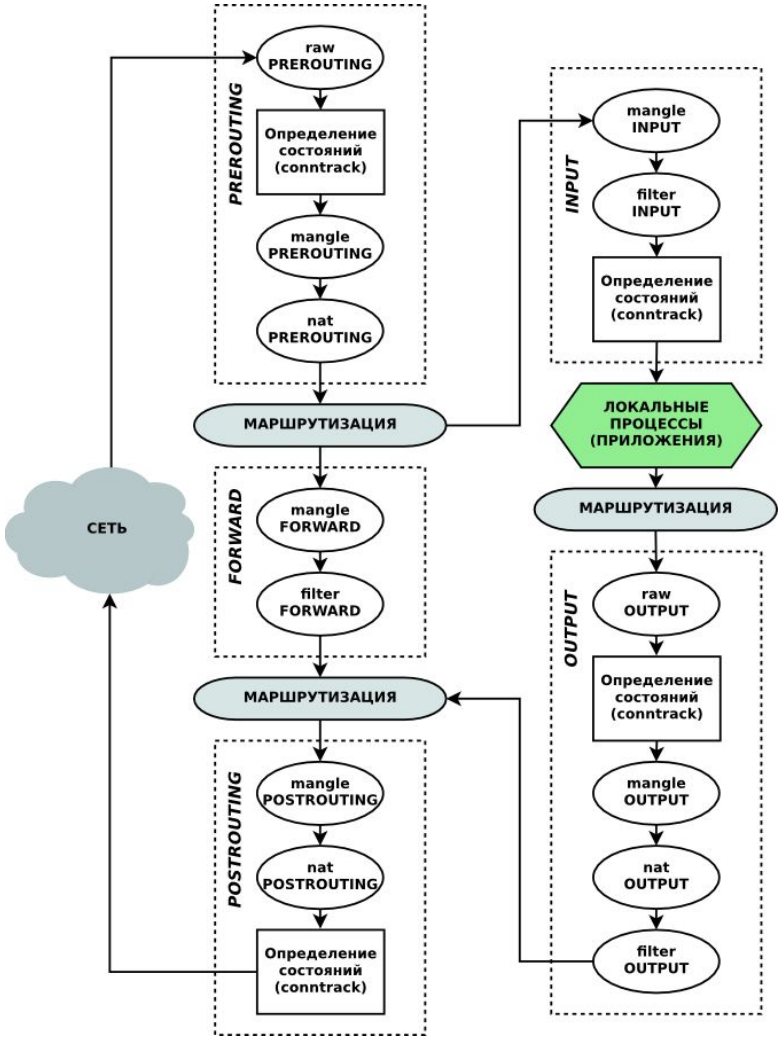
netfilter diagram

Цепочки

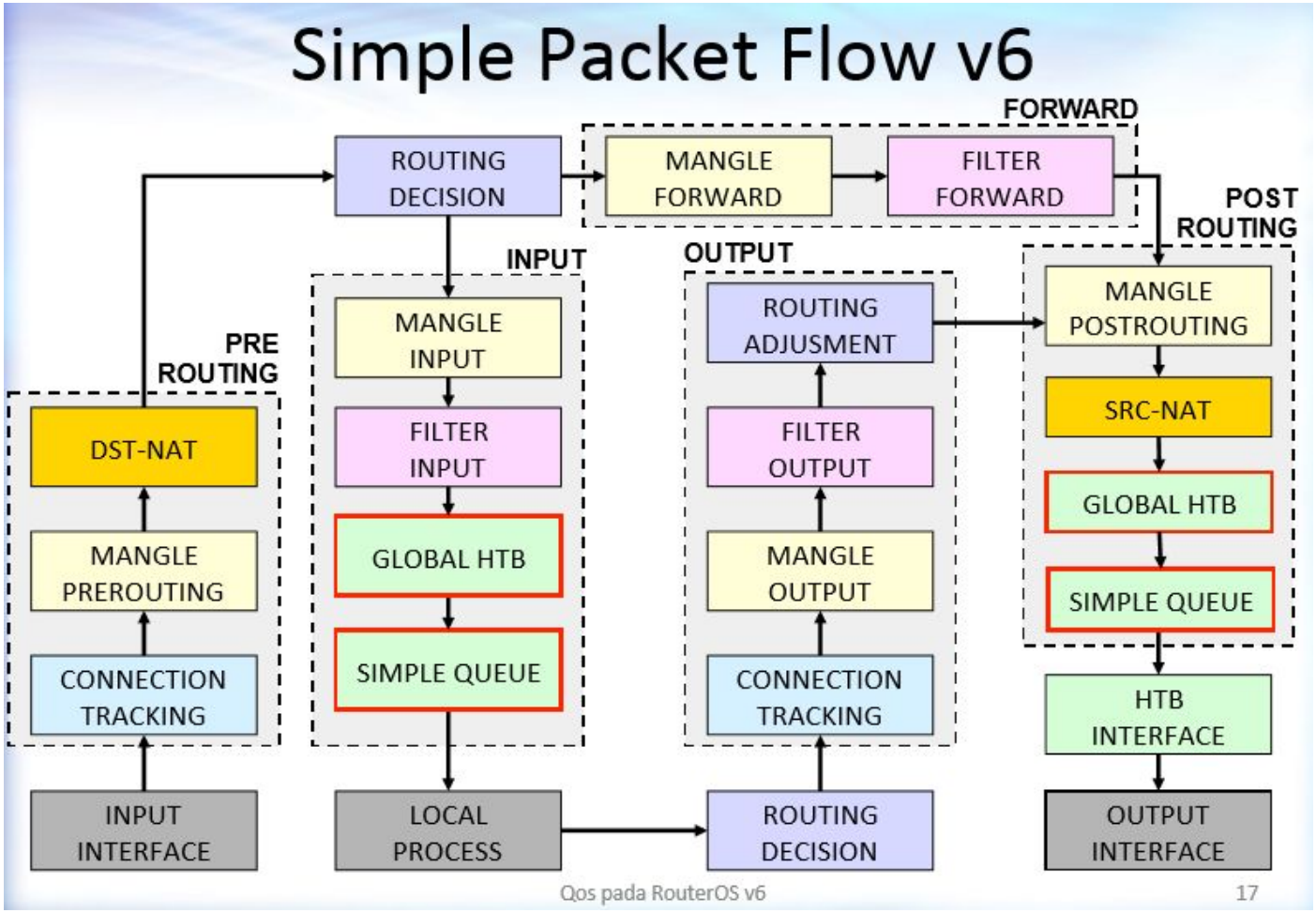
- PREROUTING
- INPUT
- FORWARD
- OUTPUT
- POSTROUTING

Таблицы

- raw
- mangle
- nat
- filter



Packetflow diagram



Практика
Правила firewall
iptables

Основные команды

```
iptables -nvL --line-numbers - Список всех правил таблицы
iptables -A chain rule - Добавить новое правило в конец
iptables -I [n] chain rule - Добавить новое правило в начало
iptables -D chain [n | rule] - Удалить правило
iptables -R chain [n | rule] - Изменить правило
iptables -S [chain] - вывести правила в формате iptables-save
iptables -F [chain] - Удалить все правила из таблицы или цепочки
iptables -N chain - создать новую цепочку
iptables -X - удалить цепочку
iptables -E - переименовать цепочку
iptables -P chain - политика по умолчанию для цепочки
iptables -t table [] - работа над правилами другой таблицы
```

Добавить правило в таблицу filter

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j
ACCEPT
```

-A - добавить правило в конец

INPUT - название цепочки

-m - matched - совпадение по модулю

 --ctstate - дополнительные параметры модуля

ESTABLISHED,RELATED - описание правила

-j - действие

ACCEPT - какое действие выполнить

Добавить правило в таблицу nat

Проброс порта:

```
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -i enp0s8 -m tcp -p tcp --dport 80
-j DNAT --to-destination 192.168.1.249
```

Правило маскарадинга

```
iptables -t nat -A POSTROUTING -o enp0s8 -j SNAT --to-source
11.0.0.2
```

или

```
iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
```

ipset

Добавление подсетей

ipset -N net_A nethash

ipset -N net_B nethash

ipset -N net_C nethash

```
ipset add net_A 10.0.0.0/8
ipset add net_B 172.16.0.0/12
ipset add net_C 192.168.0.0/16

iptables -A OUTPUT -o enp0s3 -m set --match-set net_{A..C} dst
-j DROP
```

ipset

Добавление списка адресов

```
ipset -N trusted iphash
ipset add trusted 192.168.1.221

iptables -A INPUT -i enp0s3 -m set --match-set trusted src -j
ACCEPT
```

Сохранить правила

iptables:

```
apt install iptables-persistent
systemctl enable --now iptables.service
netfilter-persistent save
```

ipset:

```
apt install ipset-persistent
systemctl enable --now ipset.service
netfilter-persistent save
```

Практика
Правила firewall

firewalld

Firewalld

зоны

- **drop**: самый низкий уровень доверия.
- **block**: отклоняются с сообщением icmp-host-prohibited или icmp6-adm-prohibited.
- **public**: публичные сети, к которым нет доверия.
- **external**: внешние сети. Эта зона настроена для маскировки NAT.
- **internal**: для внутренней части шлюза.
- **dmz**: используется для компьютеров в ДМЗ (изолированные компьютеры, у которых нет доступа к остальной части вашей сети). Разрешены только некоторые входящие соединения.
- **work**: используется для рабочих компьютеров.
- **home**: домашняя среда. Доверяете большей части других компьютеров и что будут приниматься запросы еще нескольких служб.
- **trusted**: все соединения разрешены.

Основные команды

`firewall-cmd --get-default-zone` - выводит зону по умолчанию

`firewall-cmd --get-active-zones` - список активных зон

`firewall-cmd --get-zones` - список всех доступных зон

`firewall-cmd --list-all` - список всех служб текущей зоны

`firewall-cmd --set-default - zone=work` - изменить зону по умолчанию

`firewall-cmd --get-services` - список всех доступных служб в системе

`firewall-cmd --zone=home --change-interface=eth0` - изменение зоны интерфейса

Работа с сервисами

Разрешаем, но временно

```
firewall-cmd --zone=public --add-service=http
firewall-cmd --zone=public --add-service=ftp
```

Разрешаем постоянно

```
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=ftp
firewall-cmd --reload
```

Список всех добавленных сервисов

```
firewall-cmd --permanent --zone=public --list-services
```

Вопросы?

Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

Подведение итогов

Фильтрация трафика. iptables, firewalld

Linux. Professional

Федоров Денис

Ведущий инженер по разработке в Сбер

fedorov.tech/denis

Заполните, пожалуйста, опрос о занятии

Спасибо за внимание!