



Administrator Linux.Basic

Сети. Iptables



Проверить, идет ли запись

Меня хорошо видно && слышно?



Преподаватель



Лавлинский Николай

Технический директор «Метод Лаб»

Более 15 лет в веб-разработке

Преподавал в ВУЗе более 10 лет

Более 4 лет в онлайн-образовании

Специализация: оптимизация производительности, ускорение сайтов и веб-приложений

https://t.me/methodlab_tg

<https://www.methodlab.ru/>

<https://www.youtube.com/c/NickLavlinsky>

https://www.youtube.com/@site_support

<https://vk.com/nick.lavlinsky>

Правила вебинара



Активно
участвуем



Off-topic обсуждаем
в Телеграм-чате



Задаем вопрос
в чат или голосом



Вопросы вижу в чате,
могу ответить не сразу

Условные обозначения



Индивидуально



Время, необходимое
на активность



Пишем в чат



Говорим голосом

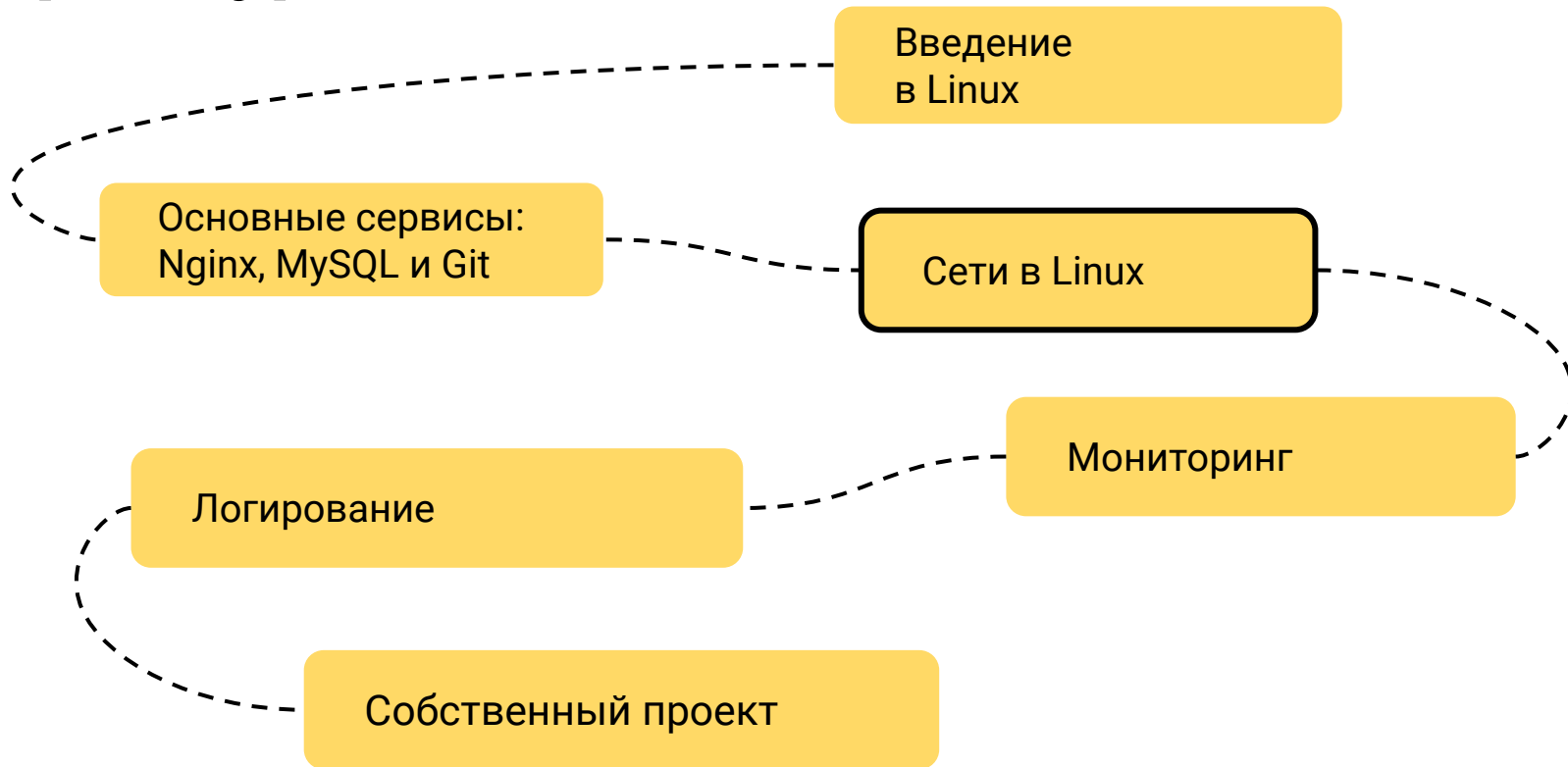


Документ

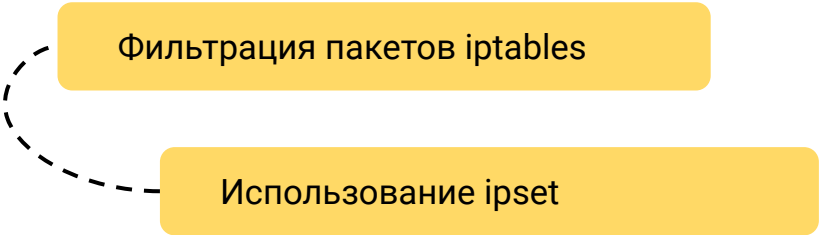


Ответьте себе или
задайте вопрос

Карта курса



Маршрут вебинара



Фильтрация пакетов iptables

Использование ipset

Цели вебинара

После занятия вы сможете

1. Понимать путь пакета в системе фильтрации
2. Настраивать базовые правила фильтрации
3. Сохранять конфигурацию

Смысл

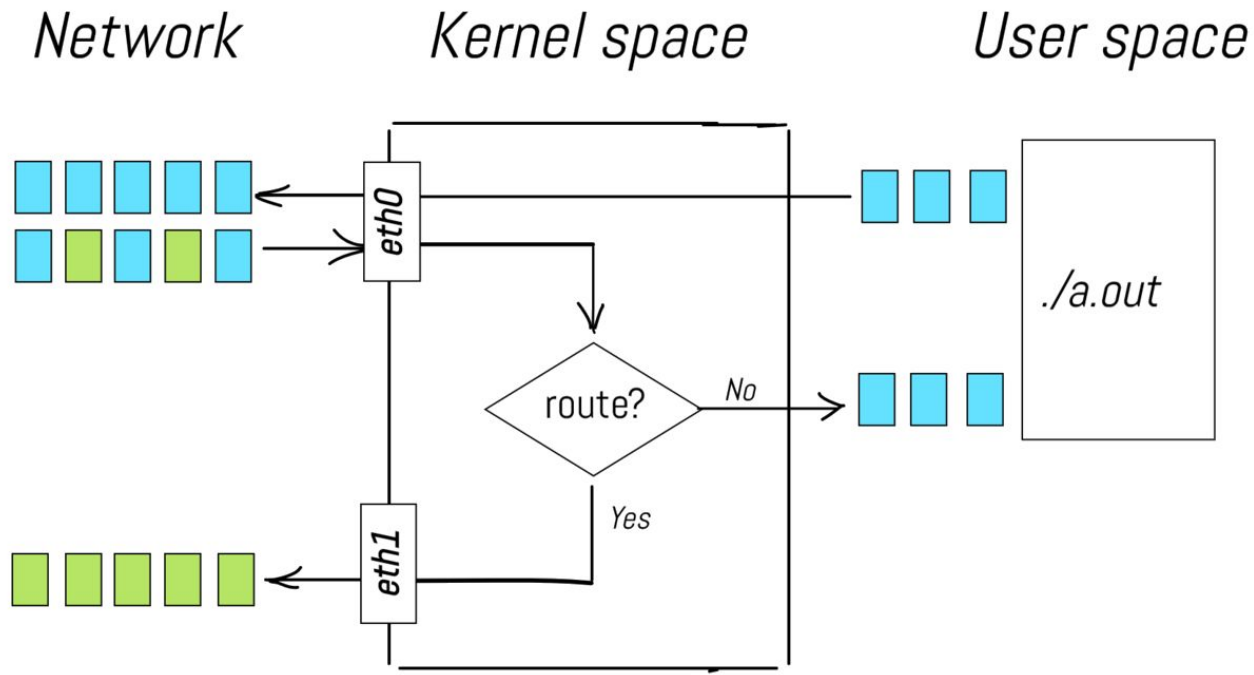
Зачем вам это уметь

1. Диагностировать работу сетевого фильтра
2. Повысить безопасность системы
3. Настраивать сетевой фильтр для сервера

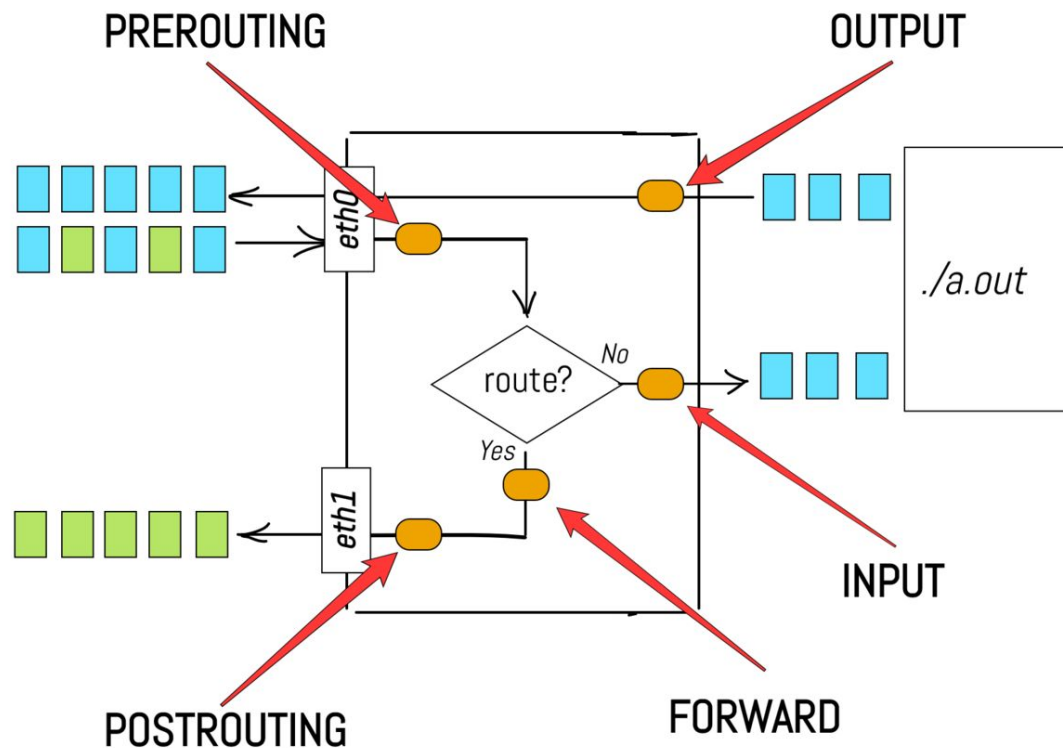


Сетевой фильтр в Linux

Путь пакетов



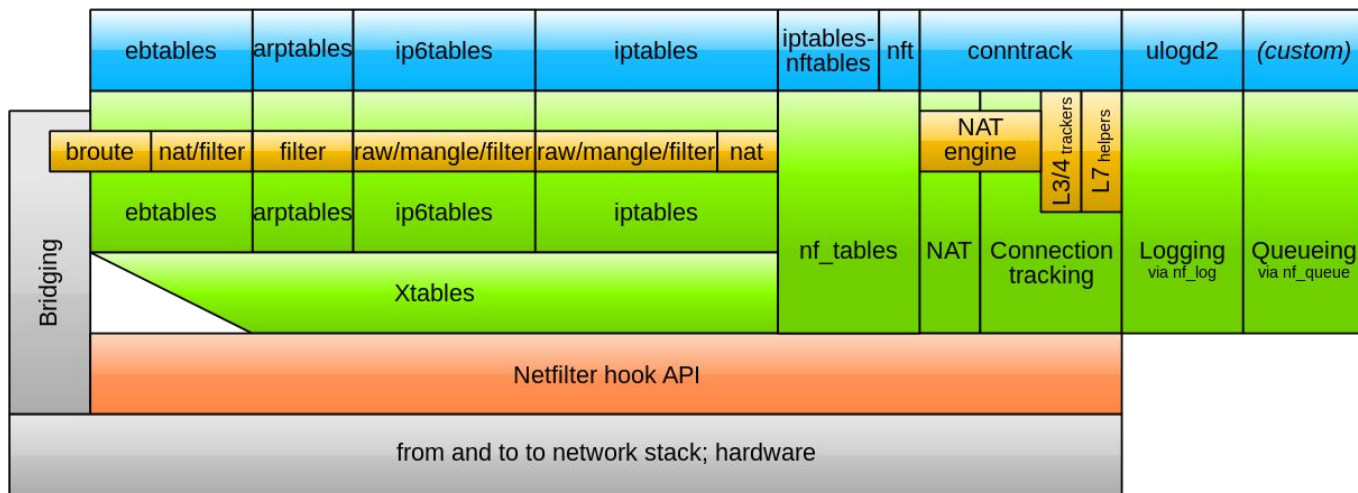
Цепочки



Компоненты системы Netfilter

Netfilter components

Jan Engelhardt, last updated 2014-02-28 (initial: 2008-06-17)



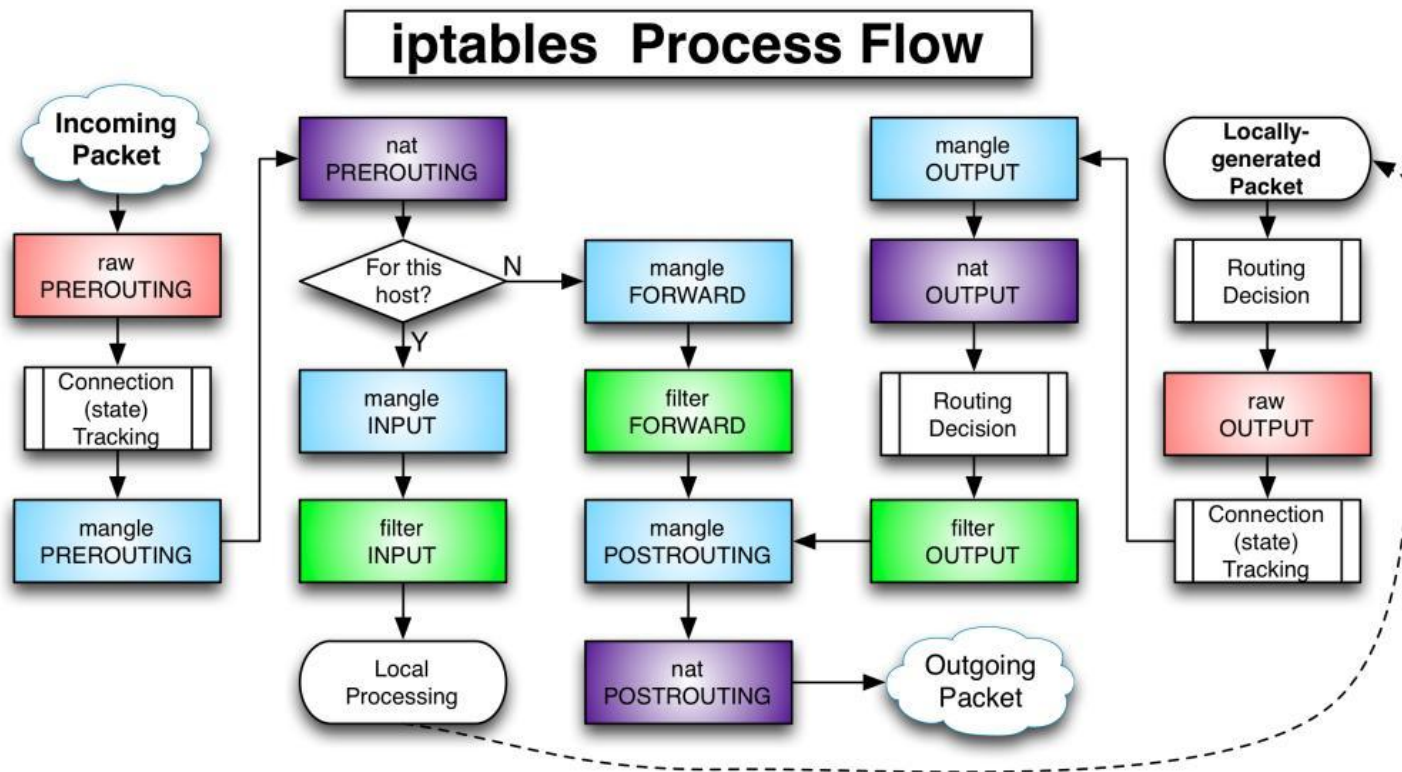
- Userspace tools
- Netfilter kernel components
- other networking components

<https://en.wikipedia.org/wiki/Netfilter>

Фильтрация пакетов iptables



Блок-схема пути пакета



Команды iptables

- `iptables -L` – просмотр списка правил
- `iptables -F` – сброс правил (политика остаётся)
- `iptables -P` – установка политики по умолчанию
- `iptables -I` – вставить правило в начало списка
- `iptables -A` – добавить правило в конец списка
- `iptables -D` – удалить правило

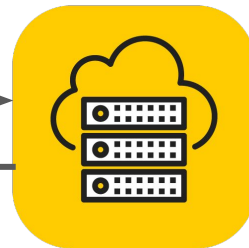
Направления: source и destination

Client 1.1.1.1

Server 2.2.2.2
SSH TCP 22

Source IP: 1.1.1.1 Source port: 32456
Dest IP: 2.2.2.2 Dest port: 22

Source IP: 2.2.2.2 Source port: 22
Dest IP: 1.1.1.1 Dest port: 32456



Критерии правил в iptables

- `-p` – протокол
- `-i` – интерфейс источника
- `-o` – интерфейс назначения
- `-s` – адрес источника
- `--dport` – порт назначения
- `--sport` – порт источника
- `-m multiport --dports` – несколько портов назначения
- `-m state --state` – статус соединения
- `--icmp-type` – тип ICMP-сообщения
- `-j` – действие

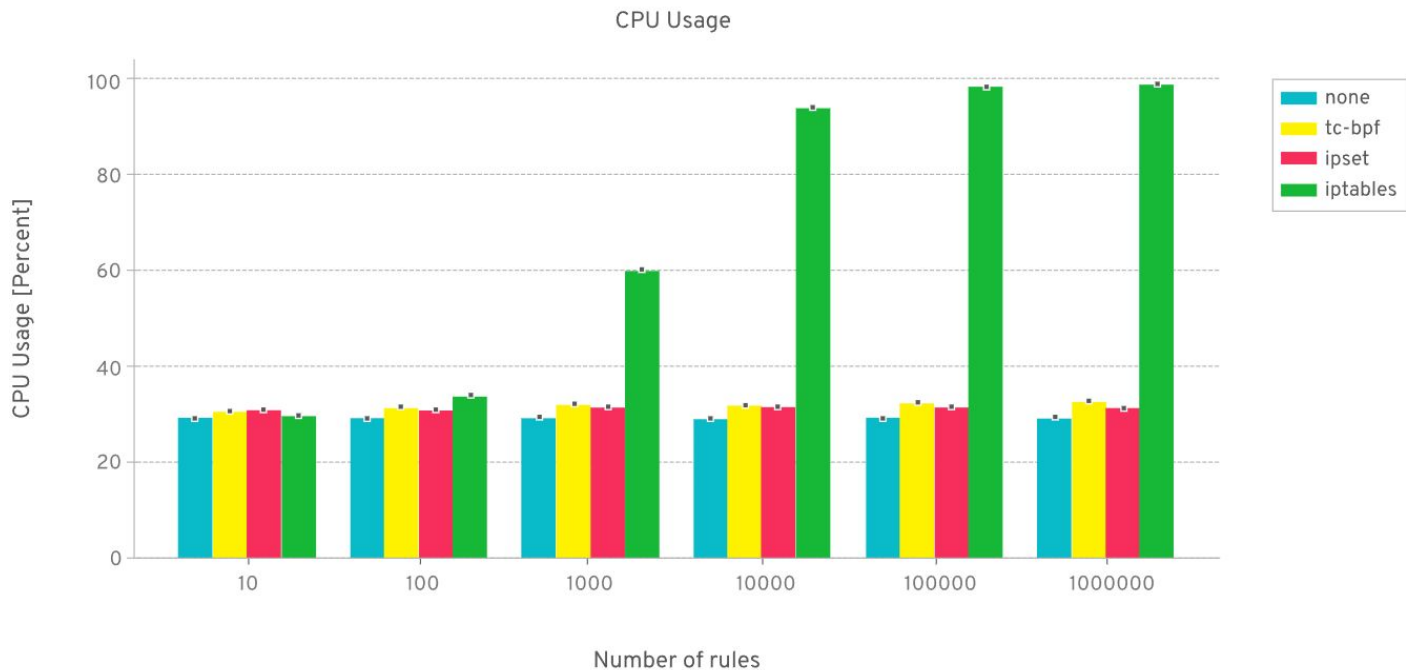
Сохранение правил в iptables

- Временно:
 - `iptables-save > ./iptables.rules`
 - `iptables-restore < ./iptables.rules`
- Постоянно:
 - `apt install iptables-persistent netfilter-persistent`
 - `netfilter-persistent save`
 - `netfilter-persistent start`

Настройка iptables для сервера LIVE

Фильтрация с ipset

Накладные расходы на фильтрацию



<https://kinvolk.io/blog/2020/09/performance-benchmark-analysis-of-egress-filtering-on-linux/>

Использование списков ipset

- Создать (отдельные IP): `ipset -N ddos iphash`
- Создать (подсети): `ipset create blacklist nethash`
- Добавить подсеть: `ipset -A ddos 109.95.48.0/21`
- Посмотреть список: `ipset -L ddos`
- Проверить: `ipset test ddos 185.174.102.1`
- Сохранение: `sudo ipset save blacklist -f ipset-blacklist.backup`
- Восстановление: `sudo ipset restore -! < ipset-blacklist.backup`
- Очистка: `sudo ipset flush blacklist`
- Правило:
`iptables -I PREROUTING -t raw -m set --match-set ddos src -j DROP`

Практика

Домашнее задание

1. Настроить разрешения в iptables, открыть TCP-порты 80, 22 и 443.
2. Запретить все входящие подключения, кроме указанных выше.
3. Сделать автовосстановление правил фильтрации после перезагрузки ОС.



Сроки выполнения: указаны в личном кабинете



Что мы изучили?

Подведем итоги

1. Путь пакета в netfilter
2. Принципы настройки фильтрации пакетов с помощью iptables
3. Сохранение правил фильтрации



Список материалов для изучения

1. <https://habr.com/ru/post/324276/>
2. <https://www.dmosk.ru/instruktions.php?object=iptables-settings>
3. <https://en.wikipedia.org/wiki/Netfilter>
4. https://wiki.nftables.org/wiki-nftables/index.php/Main_Page



Вопросы?



Ставим "+",
если вопросы есть



Ставим "-",
если вопросов нет



Рефлексия

Рефлексия



Что было самым полезным на занятии?



Как будете применять на практике то, что узнали на вебинаре?

**Заполните, пожалуйста,
опрос о занятии
по ссылке в чате**

Спасибо за внимание!

Приходите на следующие вебинары



Лавлинский Николай

Технический директор “Метод Лаб”

https://t.me/methodlab_tg

<https://www.methodlab.ru/>

<https://www.youtube.com/c/NickLavlinsky>

https://www.youtube.com/@site_support

<https://vk.com/nick.lavlinsky>

