ОНЛАЙН-ОБРАЗОВАНИЕ

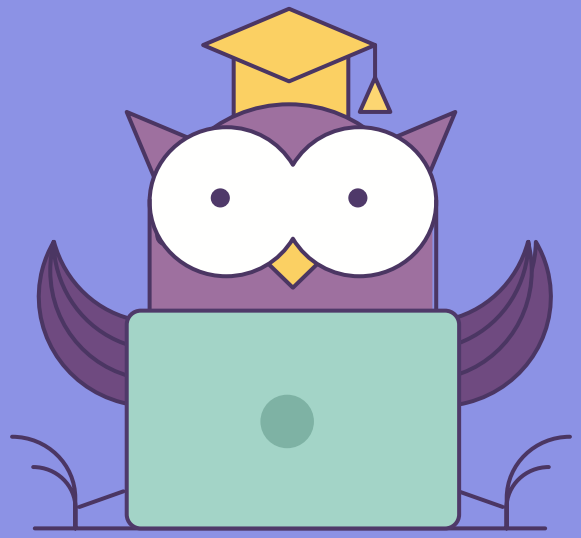
OTUS

Исследование возможностей стандартных файрволлов

Windows, Linux

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

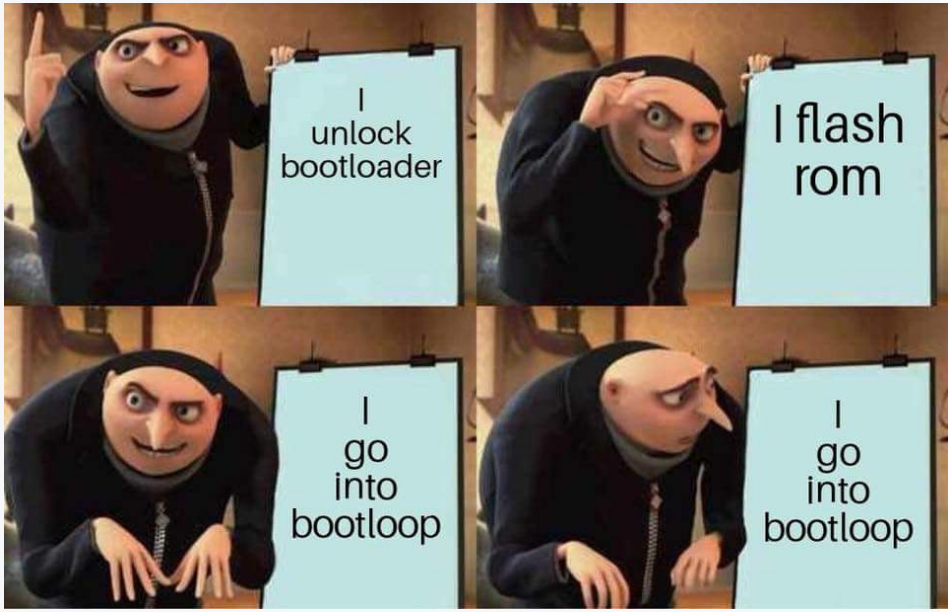
- Что такое файрволл
- Операционная система Windows
  - Как работает файрволл
  - Как настраивать
  - Особенности

- Операционная система Linux
  - Как работает файрволл
  - Как настроить
  - Особенности

Цель занятия

1. Изучить функционал стандартных файрволлов популярных операционных систем

2. Закрепить знания на практике



01

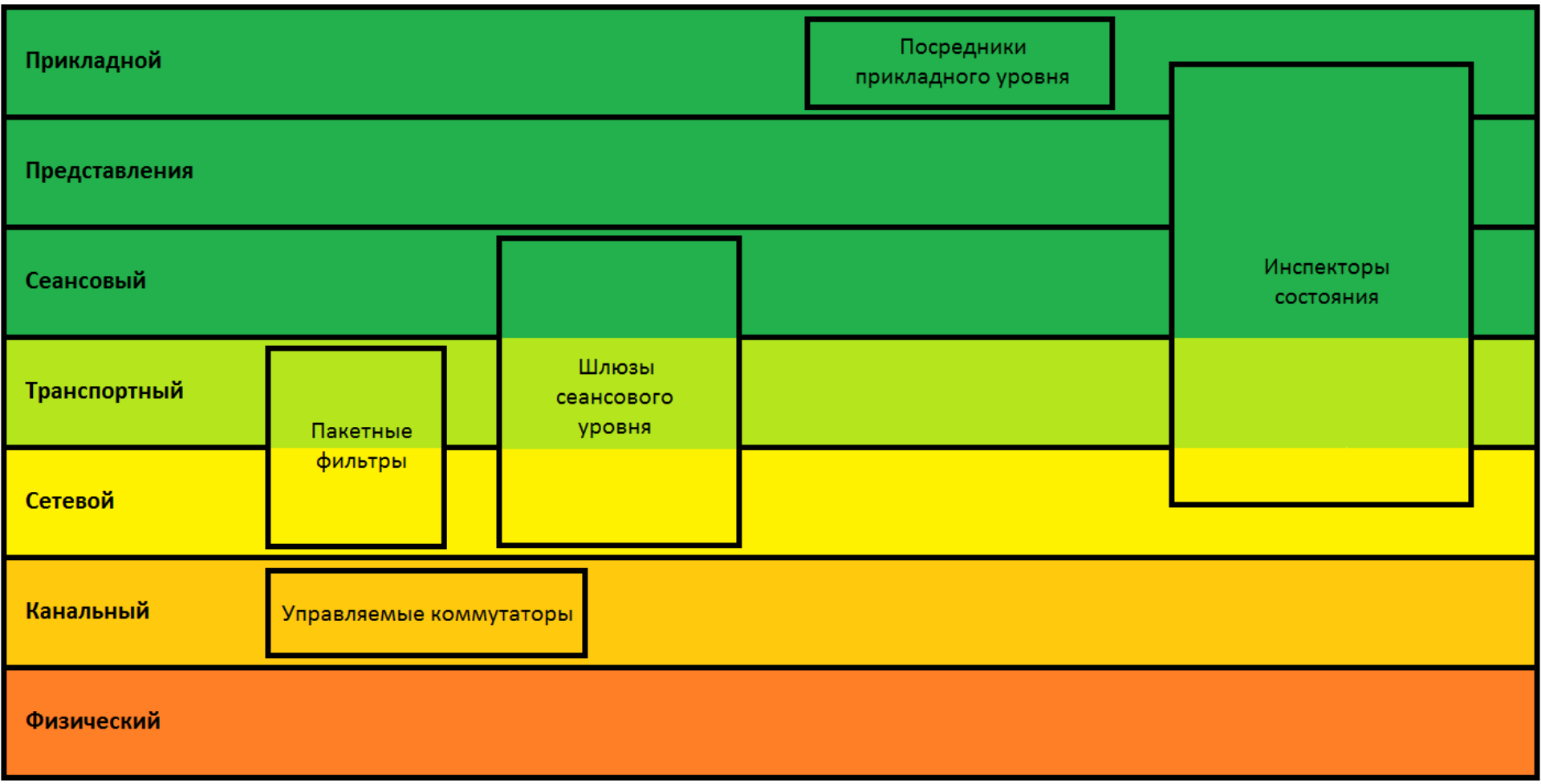
Что такое файрволл

Основные понятия

FireWall - в русской литературе межсетевой экран. Предотвращает несанкционированный или нежелательный обмен сообщениями между хостами в сети.

Так же его могут называть брандмауэр

Типы файрволлов в проекции на OSI



Что означают

Управляемые коммутаторы - коммутаторы L2 уровня, которые могут предоставлять зеркалирование, VLAN. Настраиваются посредством веб-интерфейса или консоли.

Пакетные фильтры - используются для анализа и управления исходящего и входящего трафика. Анализируют проходящие пакеты, извлекая из них данные заголовков (Ethernet, IP, ICMP, UDP, TCP). Так же работают по правилам.

Шлюз сеансового уровня - следит за подтверждением связи между клиентом и внешним хостом. Просматривает информацию IP, TCP заголовков протоколов.(SOCKS)

Инспектор состояния - включает в себя большее количество возможностей контроля сети. Может производить фильтрацию на уровне: пакетов, сессий, приложений.

Посредник прикладного уровня - тоже самое, что и шлюз сеансового уровня, за исключением - осуществление посреднической функции между двумя узлами. Обычно, указывается как proxy

02

Операцинная система Windows

WFP

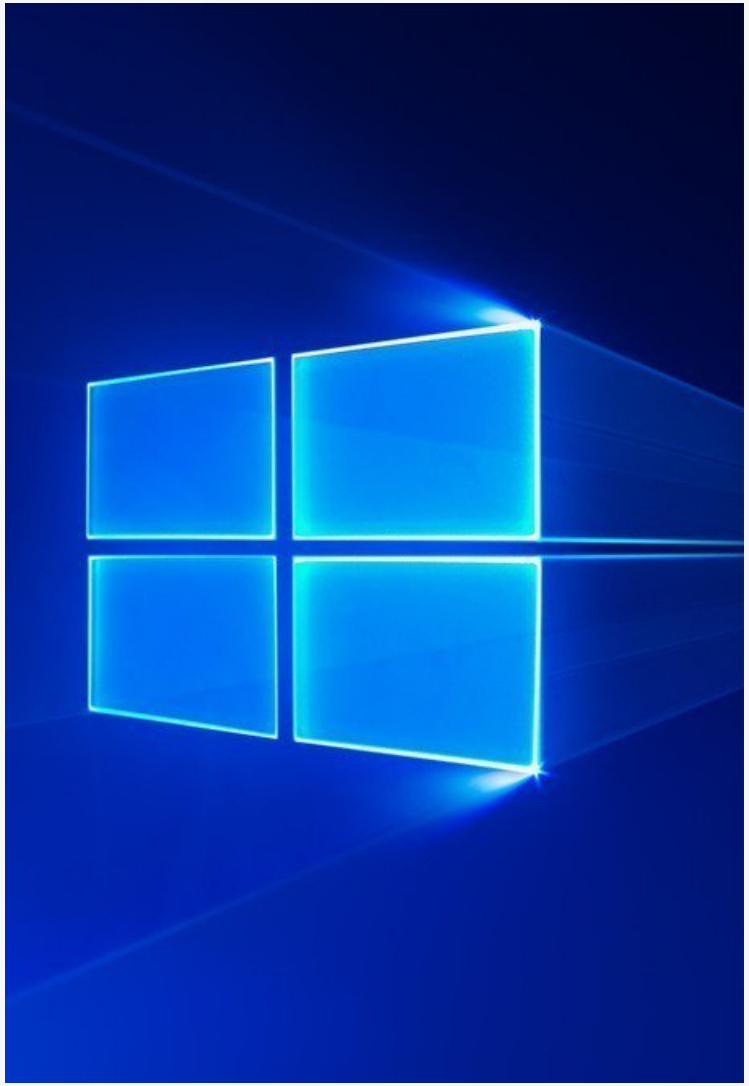
Windows Filtering Platform - платформа для фильтрации трафика в получаемого и передаваемого операционной системой Windows

Особенность - была принята взамен старой версии фильтрующих интерфейсов.

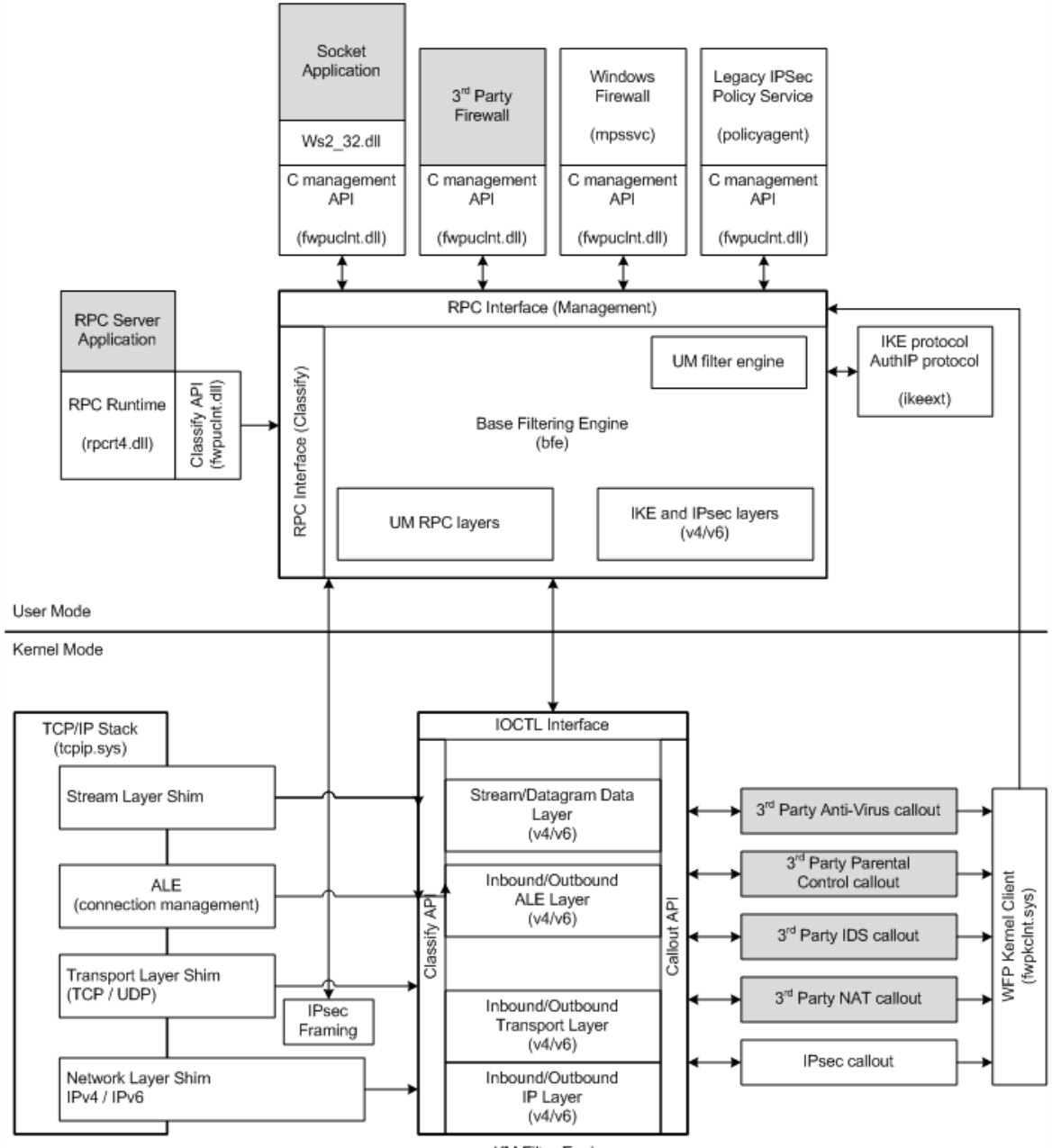
Построена на базе хуков в сетевом стеке и фильтрующего движка, который координирует сетевое взаимодействие хоста.

Основные элементы платформы:

- WFP компонент
- Описание
- Фильтр движок



Windows Filtering Platform Architecture Overview



Основные понятия подсистемы

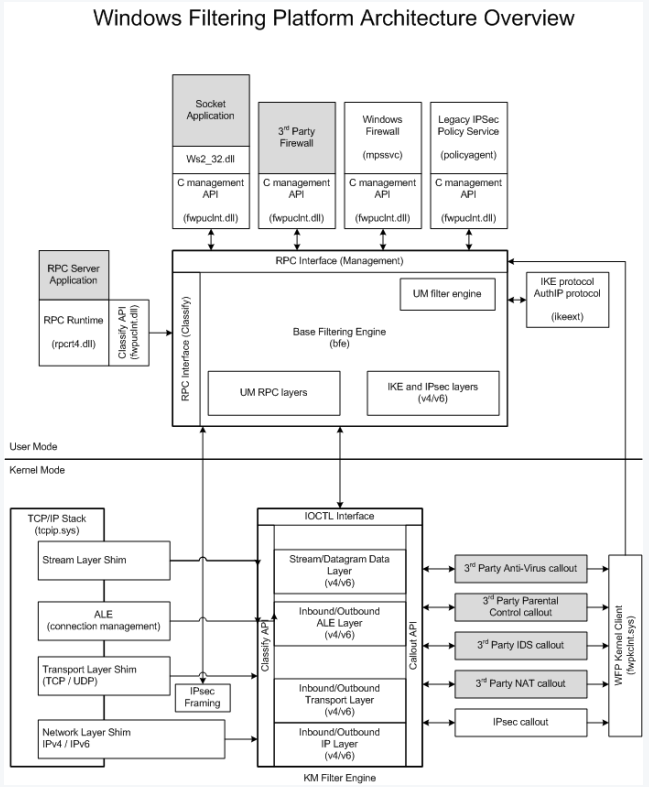
Filter Engine - ядро фильтрующей инфраструктуры.

Base Filtering Engine - сервис, который контролирует работу WFP:

- Принимает конфигурацию для платформы
- Разграничивает доступ к правилам обработки трафика
- Предоставляет информацию по соединениям, включая статистику

Shims - компоненты уровня ядра, предоставляют функции для фильтрации трафика на различных уровнях.

Callouts - набор функций, который может предоставлять нестандартное поведение при процессинга трафика (отличное от Allow и Blocked)



01

Как настроить файрволл Windows

Способы настройки Windows firewall

Графический:

Позволяет собирать информацию перед глазами. Автоматизировать проблематично, но так же возможно. (Займет больше времени)

Настройку можно произвести из оснастки:

- Win+R -> firewall.cpl

Консольный:

Наиболее быстрый, можно автоматизировать, предоставляет больше информации и гибкости для настройки.

Настройка производится посредством утилиты:

- Win+R->netsh

Конфигурирование правил Windows FireWall

Практическое задание:

- Настроить блокировку кода ICMP для входящих соединений, который используется утилитой ping
- Настроить блокировку протокола UDP для всех портов входящих соединений

Полезные команды:

- netsh advfirewall firewall add rule name=«ICMP Block» protocol=icmpv4:8,any dir=in action=block
- netsh advfirewall firewall show allprofiles
- netsh advfirewall firewall set {profilename} state on/off

02

Операцинная система Linux

Linux Firewall

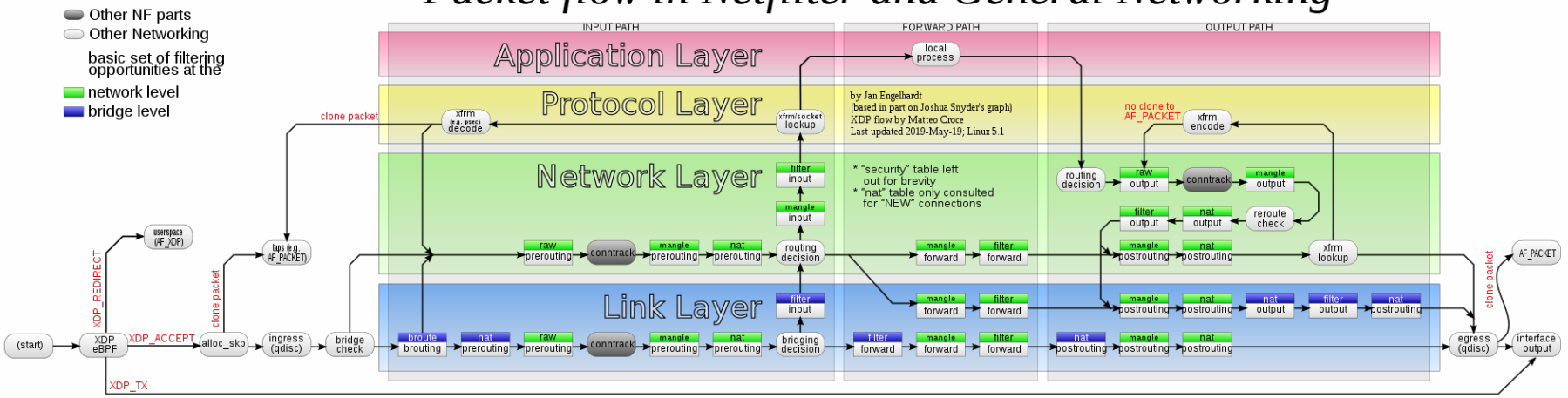
Файрволл в операционной системе Linux состоит из 2 частей:

- netfilter
- iptables

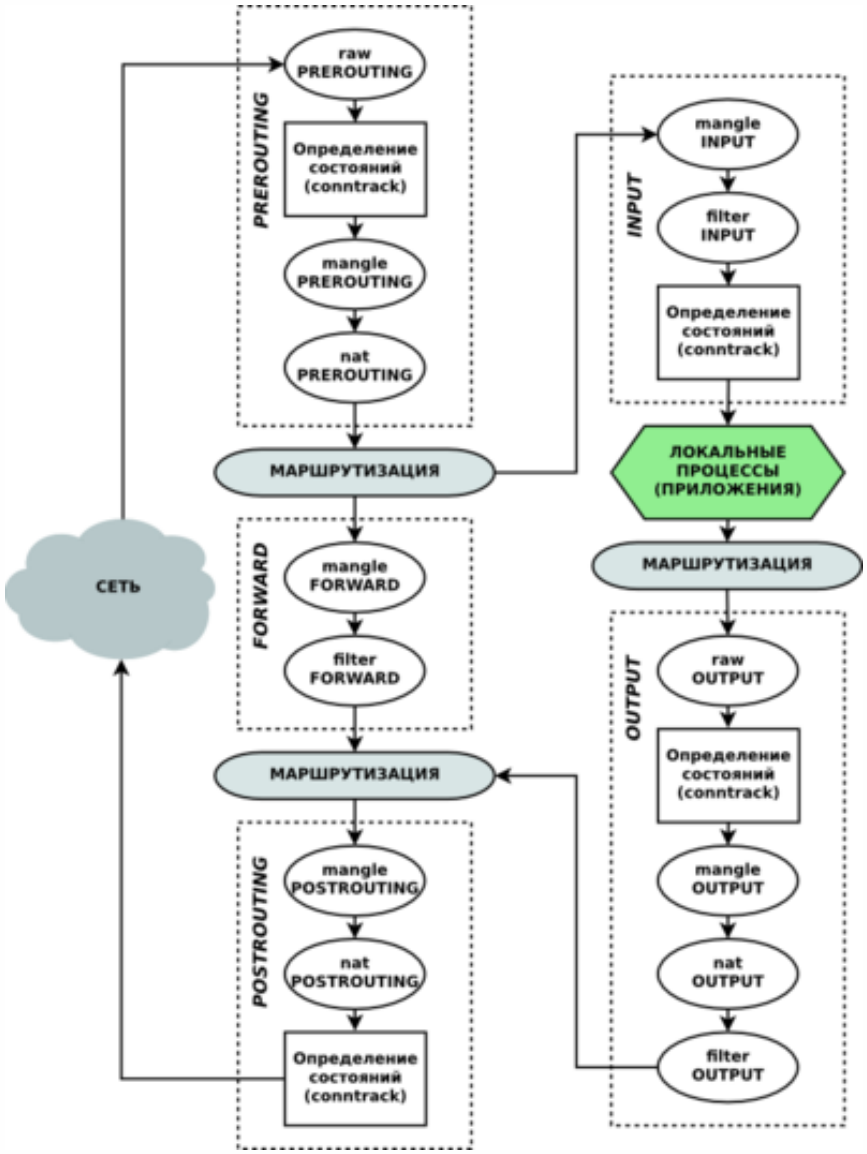
Netfilter - код, который работает в операционной системе и сравнивает весь трафик с правилами, которые заведены.

iptables - утилита для управления настройками netfilter.

Packet flow in Netfilter and General Networking



Проверка пакета в netfilter



02

Как настроить файрволл Linux

Практическое занятие

Задание:

- Заблокировать передачу данных по UDP от любого хоста на порт 10000
- Запретить подключения по UDP протоколу от любого хоста на порт 10000
- Заблокировать передачу данных по TCP от любого хоста на порт 5000
- Запретить передачу данных по TCP от любого хоста на порт 5000

Полезные команды:

- iptables -I INPUT -p {protocol} —dport {portnumber} -j DROP
- iptables -I INPUT -p {protocol} —dport {portnumber} -j REJECT
- iptables -L INPUT
- iptables -L INPUT —line-numbers

Александр Колесников

Спасибо
за внимание!