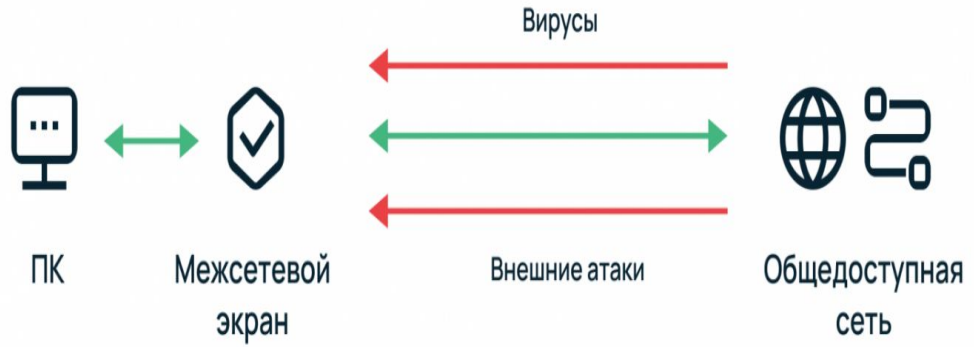
Особенности работы межсетевых экранов на ОС Linux.

Выполнил студент группы БКС1901
Гусев Павел

Что такое межсетевой экран?

- Представляет собой программно-аппаратный или программный комплекс, который отслеживает сетевые пакеты, блокирует или разрешает их прохождение.



Для чего нужен МЭ и как он работает

- Это одно из устройств, при помощи которого обеспечивается сетевая безопасность компании.
- Останавливает подмену трафика.
- Защищает корпоративную сеть(и не только) от DDoS-атак.
- Блокирует передачу данных на неизвестный адрес.

Типы межсетевых экранов

- Программно-аппаратный межсетевой экран
- Программный межсетевой экран

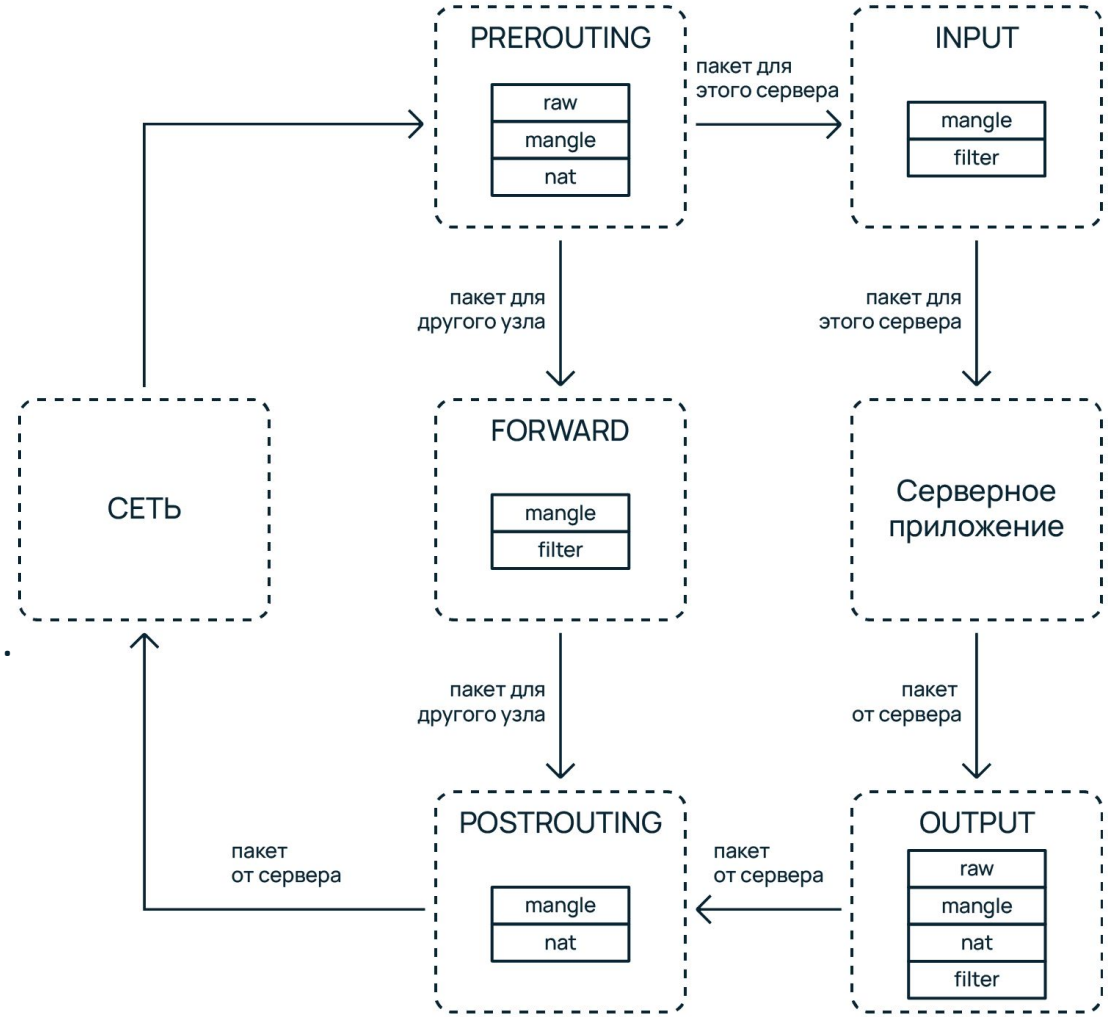
Netfilter / iptables

- Представляет собой самый популярный брандмауэр с фильтрацией пакетов под платформой Linux

- Существует три типа правил iptables:
  Input – для контроля поведения входящих соединений
  Forward – для обработки входящих сообщений и их перенаправления в конечный пункт
  Output – для исходящих соединений

Логика работы брандмауэра

- Любой, поступивший пакет на сервер с iptables, проходит через ядро, а именно межсетевой экран netfilter. Каждый из них классифицируется в зависимости от его назначения, попадает в соответствующую ему таблицу и проходит по цепочкам, содержащим правила, установленные администратором.
- На основе этих правил, выполняется действие — принять пакет, отбросить, удалить или передать следующему узлу сети.



Еще одна служба - firewalld

- Управляет соединениями и интерфейсами
- Поддерживает IPv4 и IPv6
- Поддерживает сетевые мосты
- Действует в реальном времени без перезапуска службы

Разница между iptables и firewalld

- Iptables

- Все правила должны быть обновлены, чтобы они вступили в силу
- Использует правила цепочки
- Разрешен по умолчанию

- Firewalld

- Возможность динамически изменять одно правило, динамически управлять наборами правил и разрешать обновление правил без разрушения существующих сеансов и соединений
- Использует регионы и сервисы
- Отклоняется по умолчанию и может быть отменен после настройки
- Не имеет функции межсетевого экрана, но должен быть реализован через сетевой фильтр ядра(через iptables)

Nftables. Почему лучше предшественника?

- Разработан в netfilter
- Решает проблемы настройки iptables
- Его инфраструктура проще, чем у iptables
- Работает аналогично iptables

Спасибо за внимание!