Работа firewall

Используем iptables

iptables - это фильтр пакетов. Все сетевые пакеты проходят через него

Типы пакетов

INPUT - это те, которые были отправлены на этот компьютер
OUTPUT - отправленные из этого компьютера в сеть
FORWARD - это пакеты, которые просто должны быть пересланы дальше, например, если ваш компьютер выступает в качестве маршрутизатора.

Цепочки правил

Это группы правил которые объединены визуально

Стандартные цепочки это:

INPUT
OUTPUT
FORWARD

То есть по дефолту весь входящий трафик всегда проходит через цепочку INPUT. Для того чтобы он фильтровался нашей цепочкой например FILTERS надо прицепить цепочку FILTERS к INPUT с помощью команды
iptables -A INPUT -j FILTERS

Основные команды iptables

iptables -L -n - Показать весь список правил, с числовым отображением ip
iptables -L -n --line-numbers - Показывать номера строк в цепочке правил
iptables -A {Цепочка} {Правило} - Вставить правило в самый конец цепочки
iptables -I {Цепочка} {Номер строки} {Правило} - Вставить правило в определенное место цепочки
iptables -D {Цепочка} {Номер строки} - Удалить определенную строчку в цепочке правил
iptables -F - очистить все правила
iptables -F {Цепочка} - Удалить все правила в цепочке

Правила

-p - указать протокол, один из tcp, udp, udplite, icmp, icmpv6,esp, ah, sctp, mh;
-s - указать ip адрес устройства-отправителя пакета;
-d - указать ip адрес получателя;
-i - входной сетевой интерфейс;
-o - исходящий сетевой интерфейс;
-j - выбрать действие, если правило подошло.

Действия:
ACCEPT - разрешить прохождение пакета дальше по цепочке правил;
DROP - удалить пакет;
REJECT - отклонить пакет, отправителю будет отправлено сообщение, что пакет был отклонен;
LOG - сделать запись о пакете в лог файл;
QUEUE - отправить пакет пользовательскому приложению.

Как устроен наш firewall

На каждом нашем сервер есть файл /etc/rc.local - он запускается при старте сервера. На самом деле это просто баш файл который запускает 2 других файла. Вот как он выглядит:

```
#!/bin/bash

iptables-restore -n /etc/firewall.conf
ip6tables-restore -n /etc/firewall6.conf
/etc/init.d/fail2ban restart

exit 0
```

Наши правила

Если посмотреть на наши правила то можно заметить что мы блочим только весь входящий трафик -A INPUT -j REJECT
Только какие то определенные ip или порты оставляем открытыми
Основной цепочкой правил в наших конфигах является FILTERS. Так что если надо найти какой то порт/ip который залочен, то лучше искать там

fail2ban

Простой в использовании локальный сервис, который отслеживает log–файлы запущенных программ, и на основании различных условий блокирует по IP

Настройки f2b у нас в основом лочат только при неправильном вводе пароля ssh

В завершении

Я намеренно упустил много моментов про роутинг и маскарад так как это большая тема для разговоров. Так же я у не сильно в ней разбираюсь