iptables – это утилита для настройки firewall - межсетевой экран для операционных систем Linux. Firewall (фаервол) нужен для:

* Фильтрации трафика: разрешает или блокирует пакеты на основе настроенных правил.
* Ограничения доступа к определённым портам или адресам.
* Контроля трафика внутри сети (локальный или внешний).
* Обеспечения безопасности при подключении к интернету или другим сетям.

Она работает с таблицами, цепочками и правилами. Базовые цепочки:

* INPUT: правила, применяемые к входящим пакетам (на локальную машину).
* FORWARD: правила, применяемые к проходящим транзитным пакетам (если машина выступает в роли маршрутизатора).
* OUTPUT: правила, применяемые к исходящим пакетам (от локальной машины наружу).

Можно задавать действия по умолчанию для каждой цепочки.

Основные действия над соединениями:

* ACCEPT – разрешить соединение
* DROP – "тихо" отбросить пакет (отправитель не получает уведомления об отказе)
* REJECT – отклонить пакет с уведомлением отправителю (отправитель узнает, что его пакет был отклонён).

Удалим все пользовательские цепочки:

sudo iptables -X

И выставим политики по умолчанию для всех цепочек в ACCEPT:

sudo iptables -P INPUT ACCEPT

sudo iptables -P FORWARD ACCEPT

sudo iptables -P OUTPUT ACCEPT

И посмотрим текущие правила:

iptables -L -v

Далее с помощью утилиты netcat будем слушать порт 5555 в tcp-режиме:

nc -l -p 5555

И аналогично будем слушать порт 6666 в udp-режиме

nc -u -l -p 6666

-l – слушать порт (listening mode).

-p – номер порта (port).

netcat (или nc) – это универсальная утилита для работы с сетевыми подключениями. Её можно использовать для:

* Прослушивания портов (в режиме "сервер"),
* Отправки данных (в режиме "клиент"),

На стороне отправителя будем слушать ICMP пакеты:

sudo tcpdump icmp and dst 192.168.0.111

Отправим сообщение по tcp и udp на соответсвующие порты:

echo "Hello from TCP" | nc -q 0 192.168.56.101 5555

echo "Hello from UDP" | nc -q 0 -u 192.168.56.101 6666

-q 0 – говорит nc, чтобы завершить соединение сразу после отправки данных

На стороне принимающего успешно получим два сообщения.

Далее добавим правило в цепочку INPUT для пакетов по протоколу tcp с действием отклонить с отправкой уведомления:

sudo iptables -A INPUT -p tcp -j REJECT

И проверим что правило добавилось:

iptables -L -v

Снова отправим два сообщения:

echo "Hello from TCP" | nc -q 0 192.168.56.101 5555

echo "Hello from UDP" | nc -q 0 -u 192.168.56.101 6666

И увидим что сообщение по tcp не было получено, причем отправитель получил ICMP оповещение об этом.

Далее добавим еще одно правило для отправки по UDP протоколу с действием отклонить без уведомления:

sudo iptables -A INPUT -p udp -j DROP

И снова отправим два сообщения:

echo "Hello from TCP" | nc -q 0 192.168.56.101 5555

echo "Hello from UDP" | nc -q 0 -u 192.168.56.101 6666

И увидим что никакое сообщение не дошло, при этом отправитель был оповещен что порт 5555 не достижим, и никаких сообщений про порт 6666 не было

И далее удалим два правила:

sudo iptables -D INPUT -p tcp -j REJECT

sudo iptables -D INPUT -p udp -j DROP