**iptables** - это утилита для настройки программного Firewall’а (межсетевого экрана) linux, которая предустанавливается по умолчанию во все сборки Linux, начиная с версии 2.4. Запускается iptables из командной строки (CLI) под пользователем с правами root и настраивается там же.

## Топология Сети

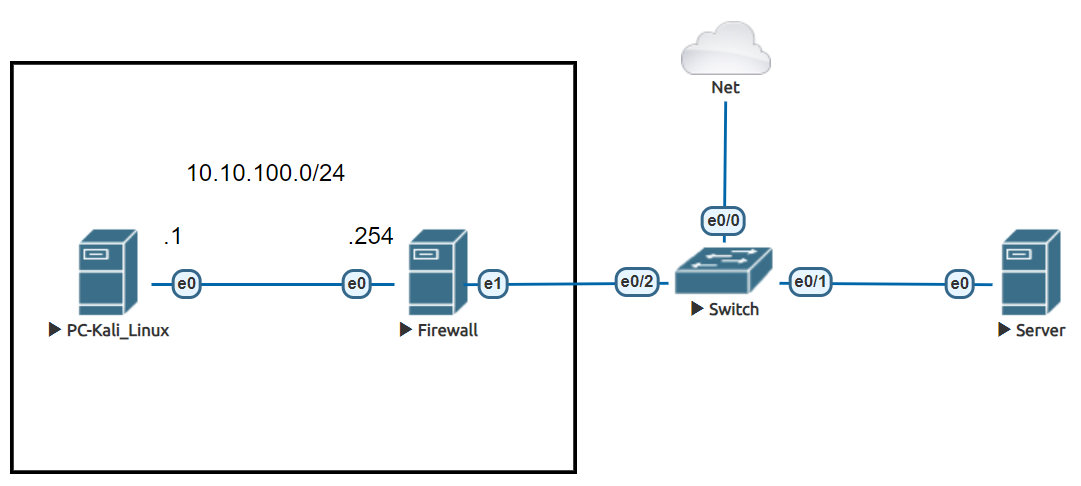


Рис. 1.

Настраиваем интерфейс на сервере.

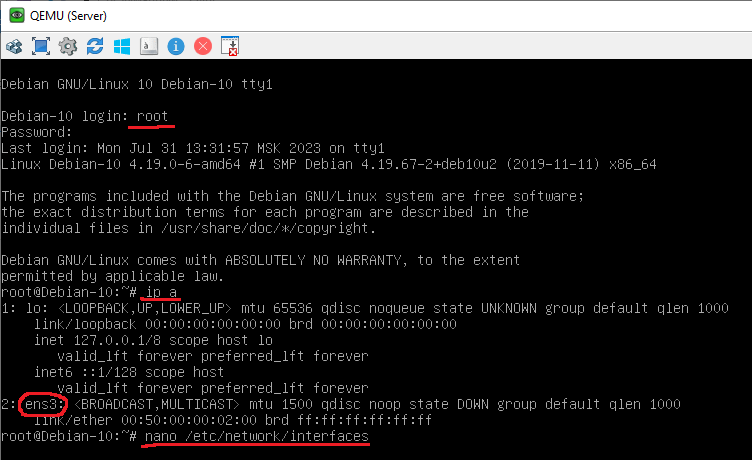


Рис. 2.

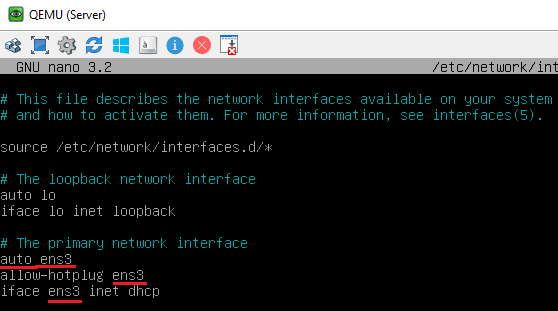


Рис. 3.

CTRL+O – сохранить файл

CTRL+X – выход из NANO

systemctl restart networking.service – перезапустить службу

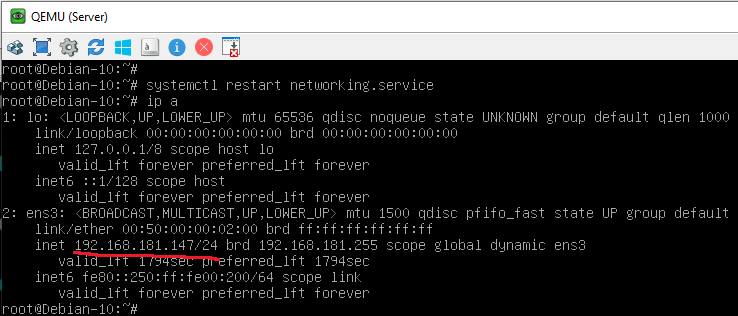


Рис. 4.

Получили адрес по DHCP.

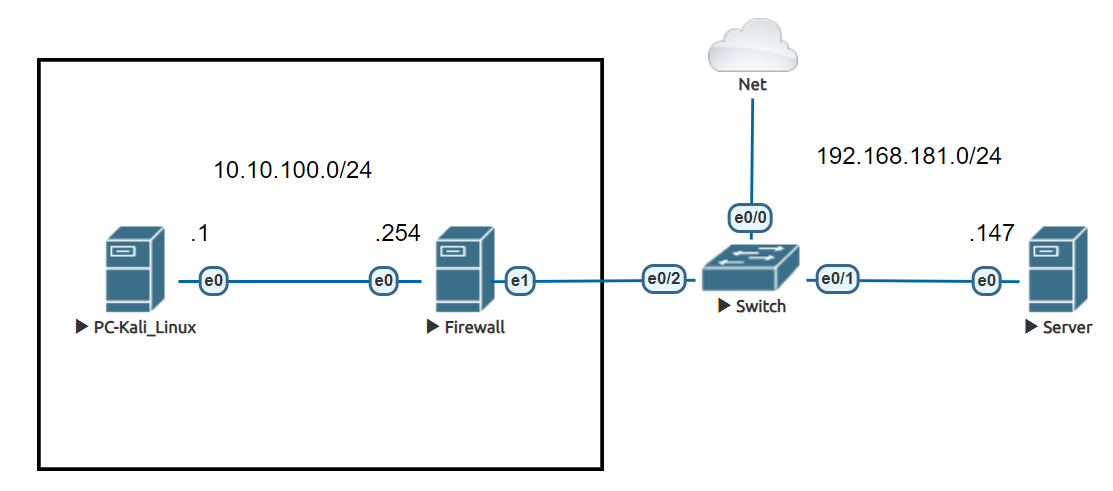


Рис. 5.

Настраиваем интерфейс на файерволе.

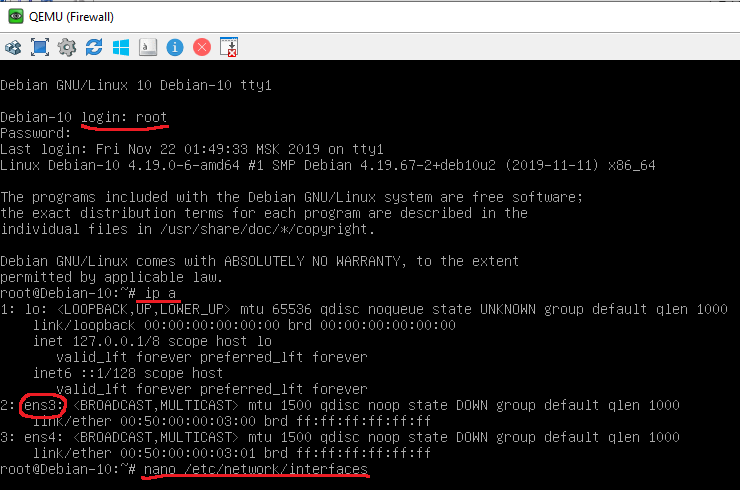


Рис. 6.

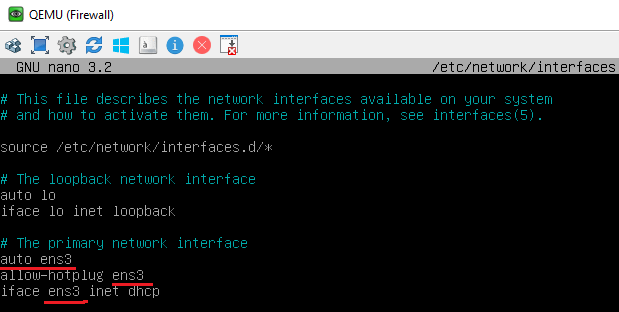


Рис. 7.

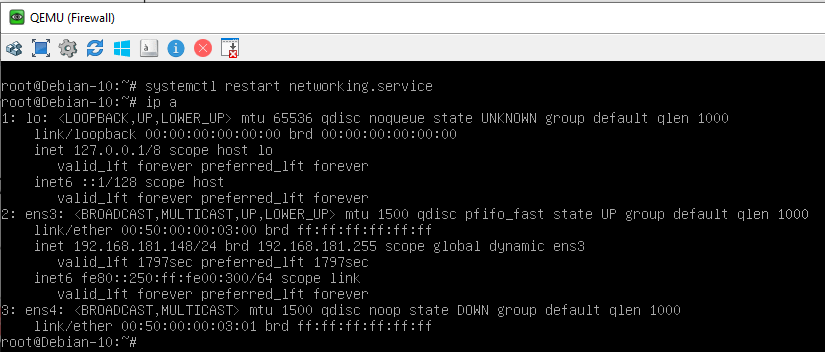


Рис. 8.

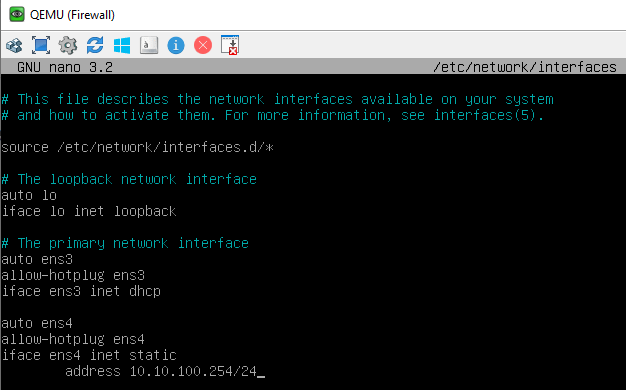


Рис. 9.

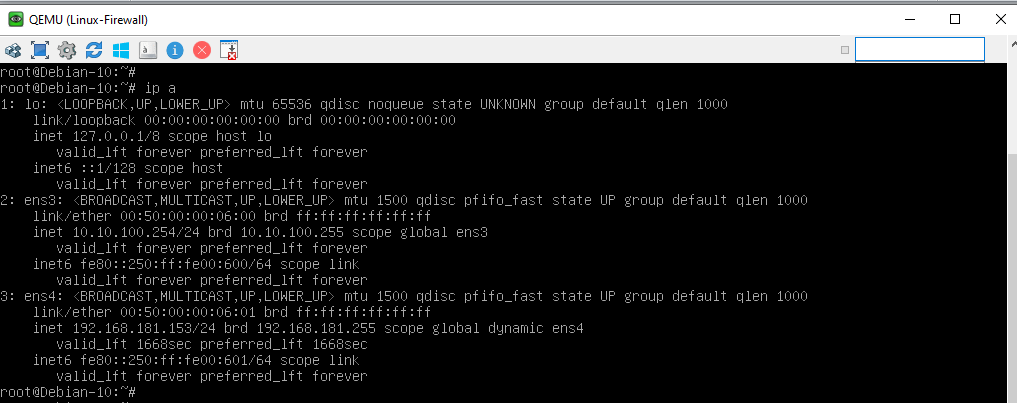


Рис. 10.

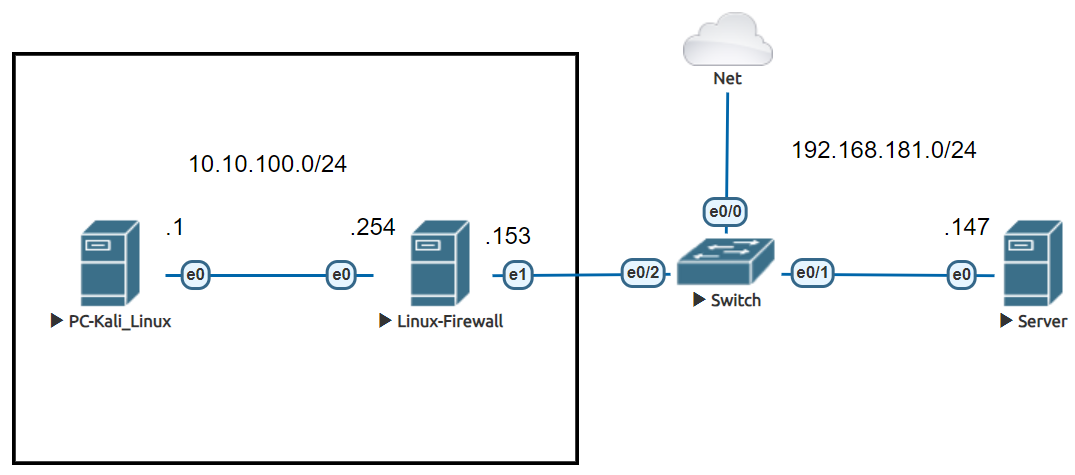


Рис. 11.

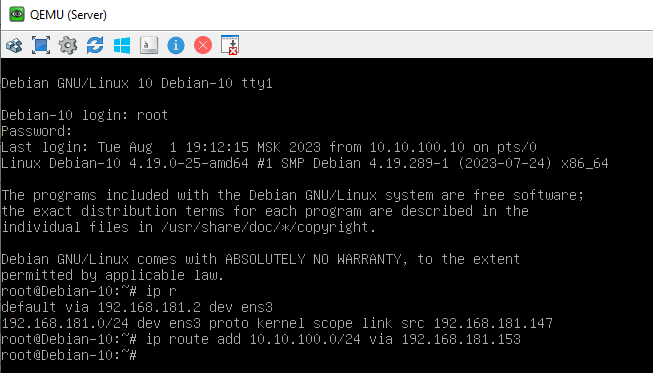


Рис. 12.

Теперь сделаем из этого linux-сервера настоящий linux-роутер

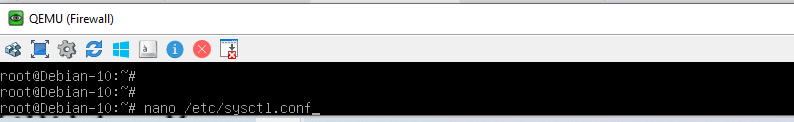


Рис. 13.

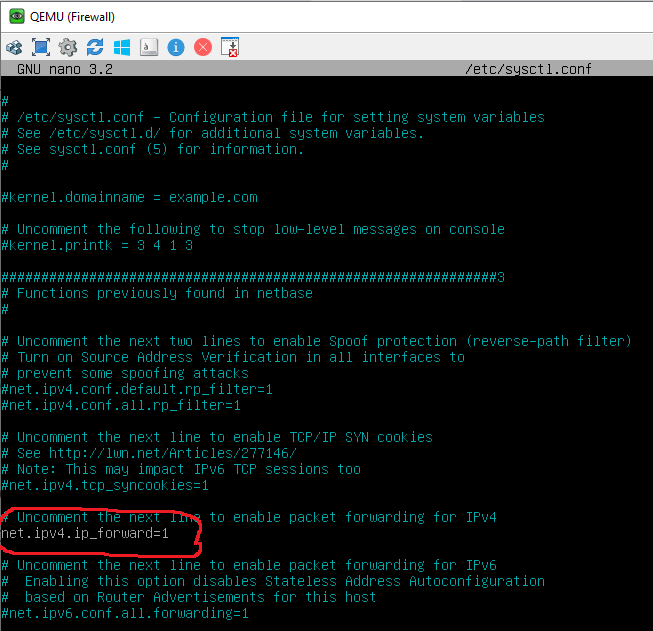


Рис. 14.

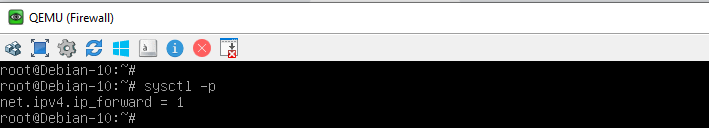


Рис. 15.

Настраиваем интерфейс на кали-линуксе

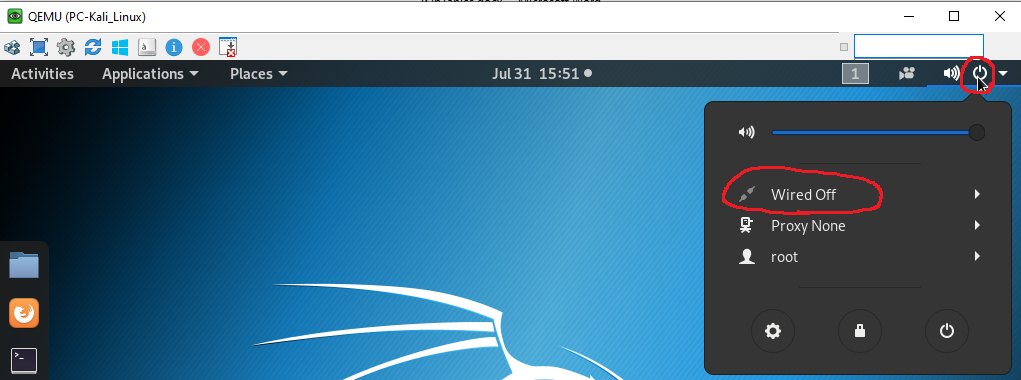


Рис. 16.

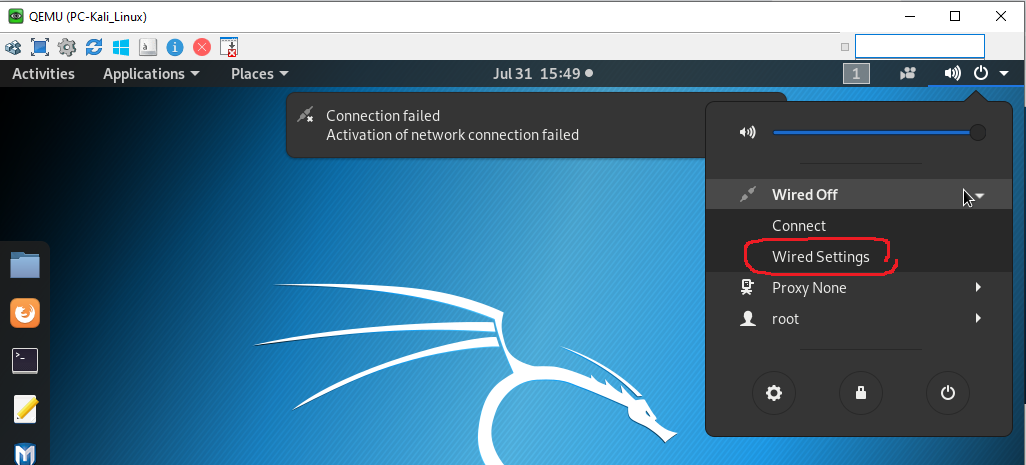


Рис. 17.

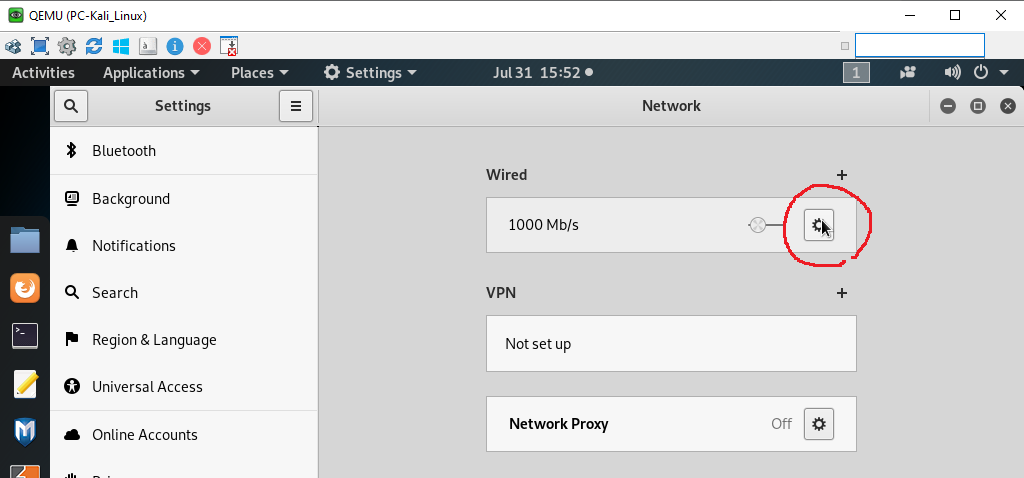


Рис. 18.

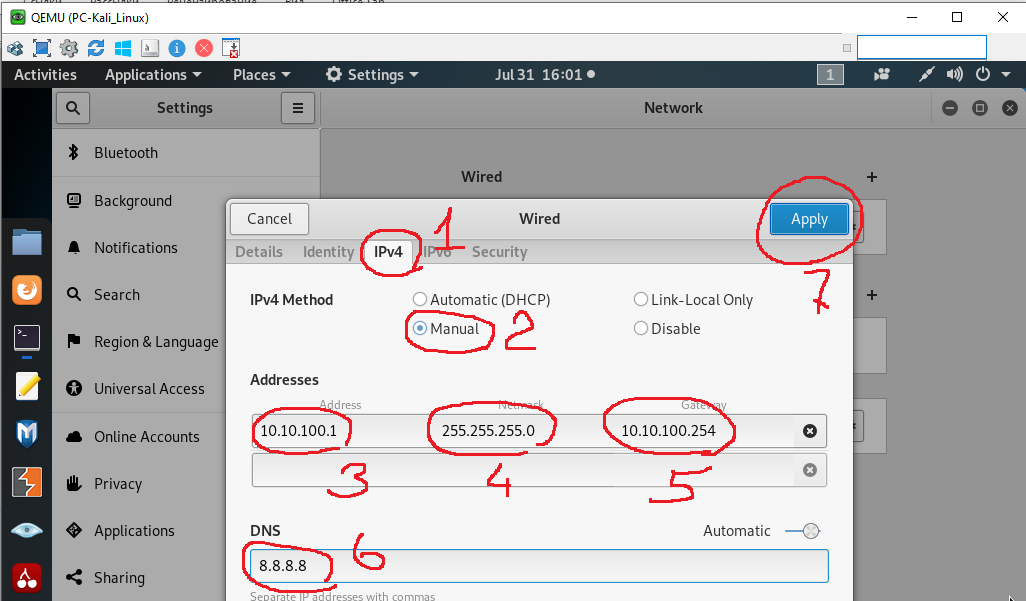


Рис. 19.

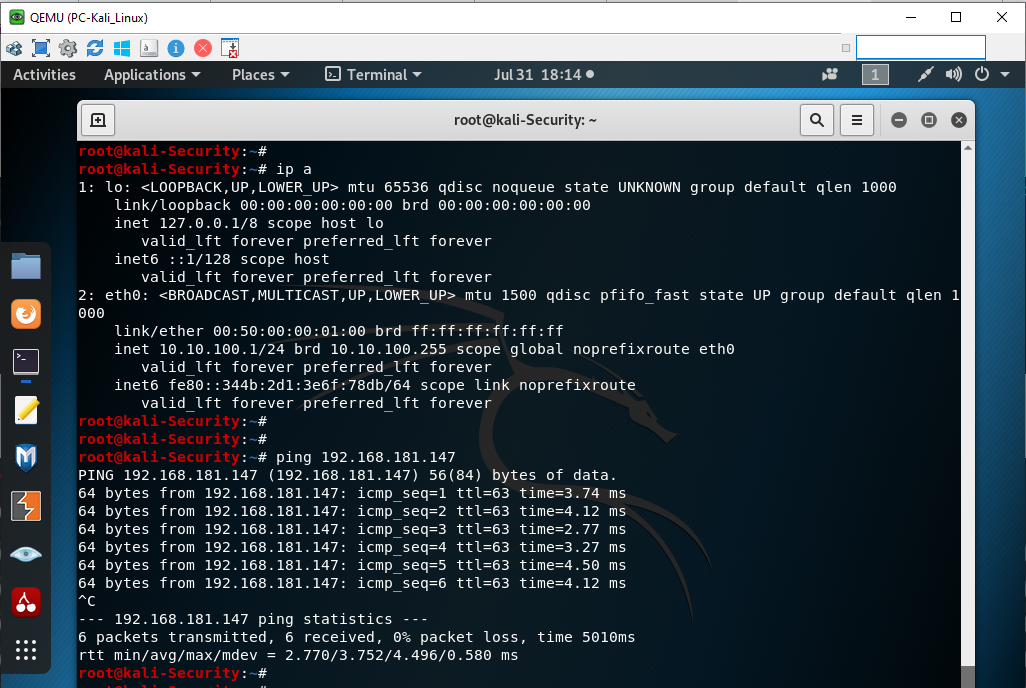


Рис.20.

Установка Nginx на Web-server (пк Server).

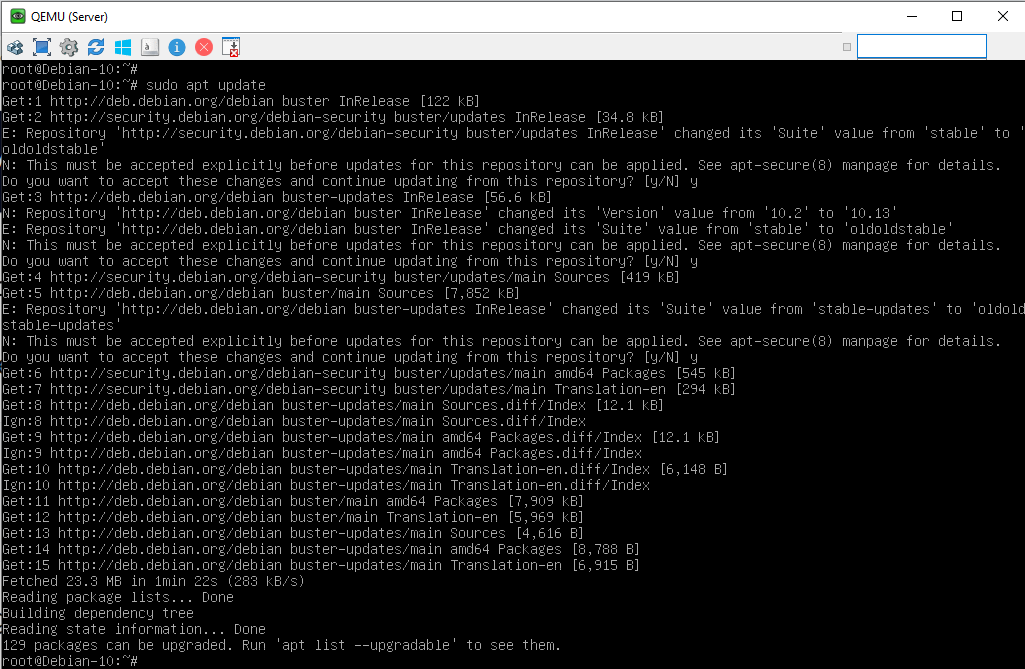


Рис. 21.

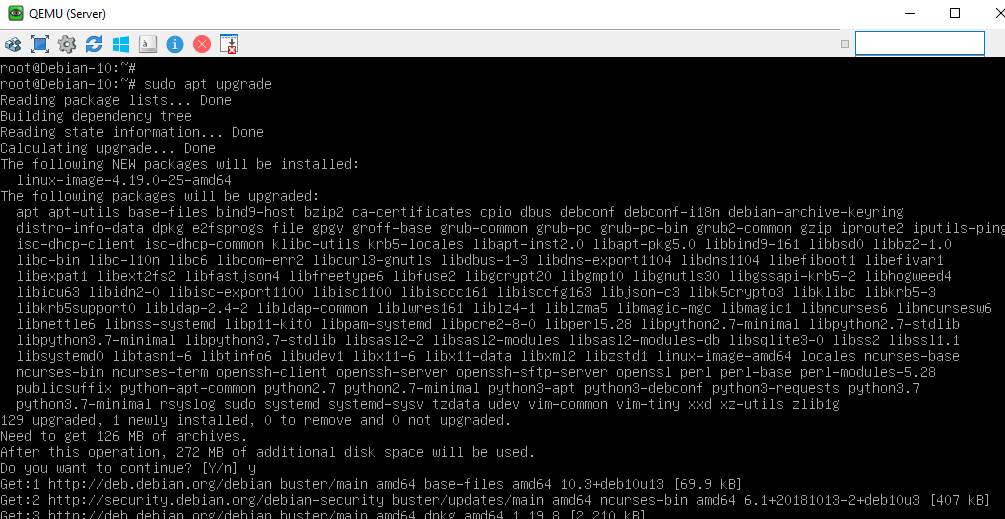


Рис. 22.

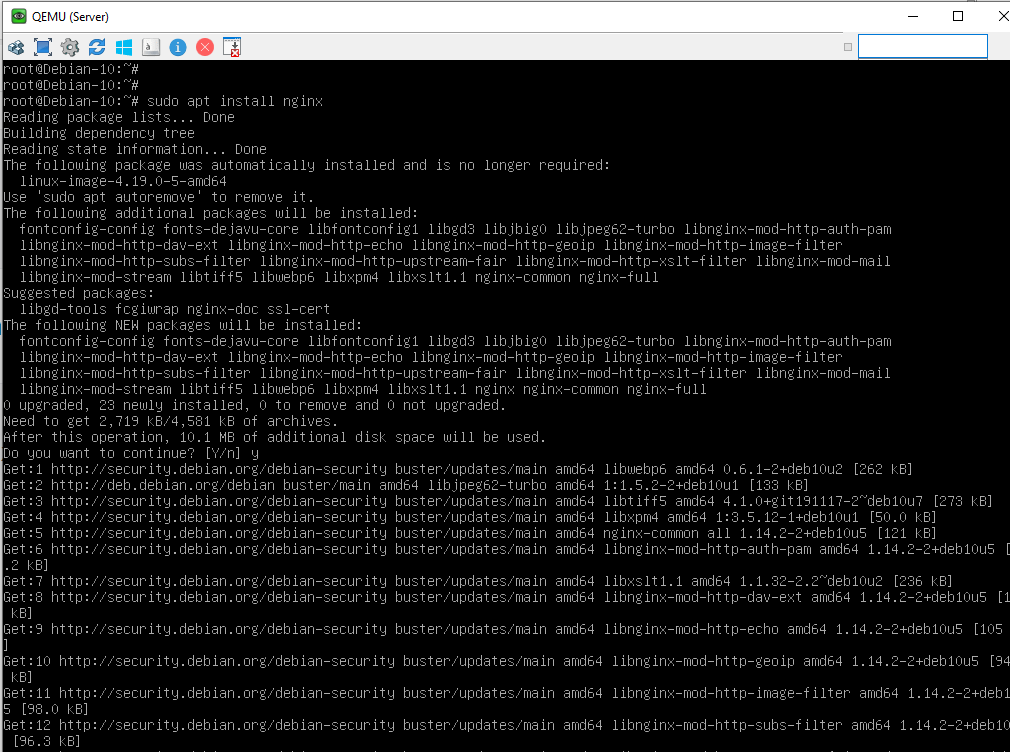


Рис. 23.

Проверяем установку

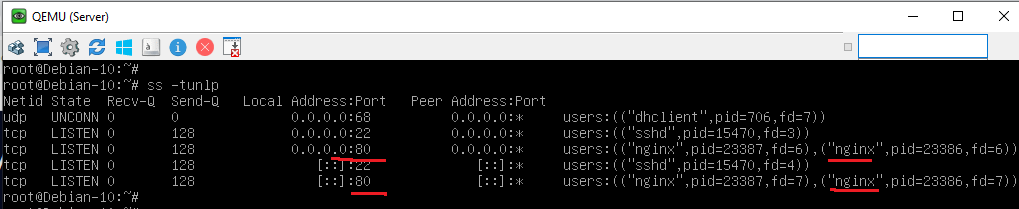


Рис. 24.

Здесь мы видим, что наряду с 80 портом открыт еще и порт 22, т.е. ssh.

Наша задача состоит в том, что бы на Firewall доступ до Web-server осуществлялся только по 80 порту. То есть что бы по SSH с PC не было возможно подключится до Web-server.

Для начала проверим подключение по SSH до Web-server.

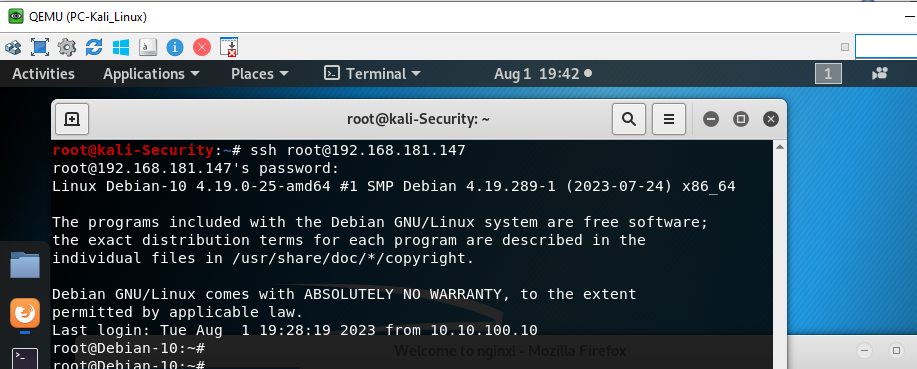


Рис. 25.

Видим что **Nginx** работает.

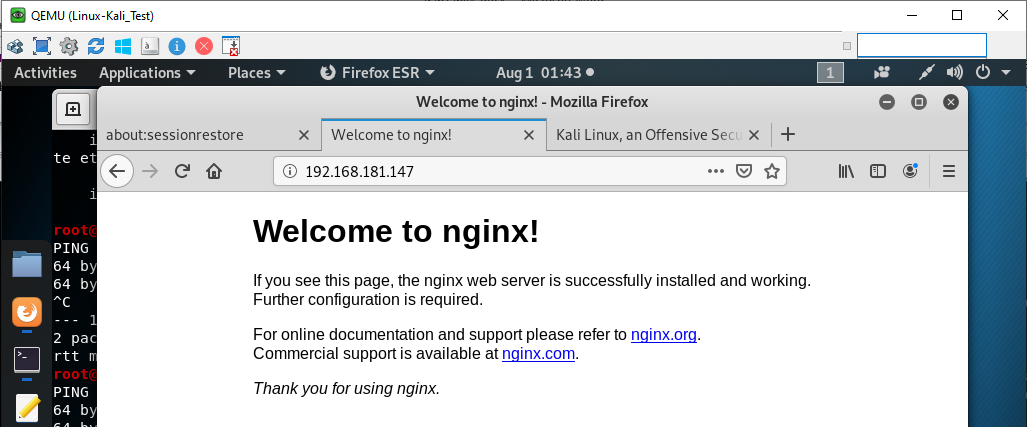


Рис. 26.

Для настройки Firewall будем использовать утилиту iptables.

Выполним 3 действия.

1. Разрешающее правило, что бы подключатся к Web-server. И разрешаюшее правило, что бы мы не потеряли SSH соединение. (для 80 порта и 22 порта) + establish connection, что бы нас обратно пропускали.  
2. Политика. Input Drop.  
3. Разрешающее правило Forward для 80 порта.

Проверим текущие правила и политики iptables:

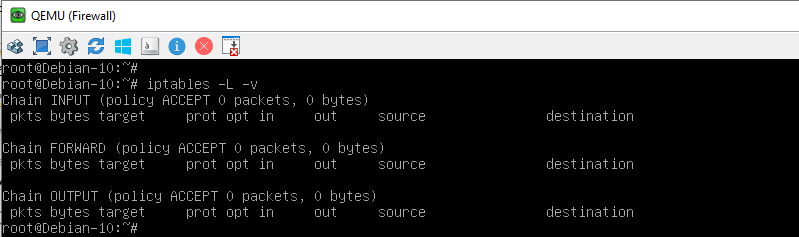


Рис. 27.

Синтаксис iptables можно посмотреть по адресу: https://1cloud.ru/help/linux/nastrojka\_linus-firewall\_iptables

Прописываем правило и проверяем применилось ли оно

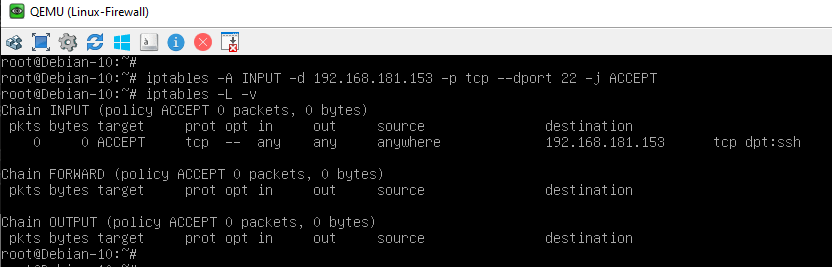


Рис. 28.

Очень важно понять и помнить, что правила в iptables применяются иерархически, т.е. правило стоящее выше выполнится раньше.

Пропишем правила для Forward

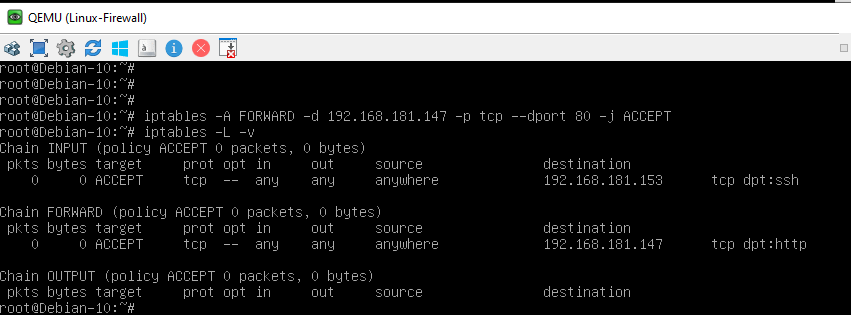


Рис. 29.

Все остальное дропнем.

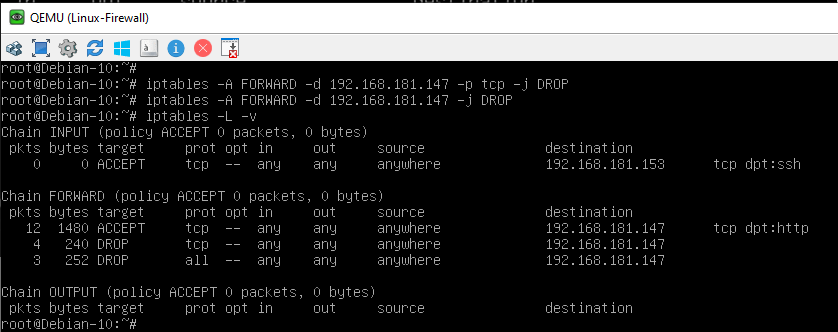


Рис.30.

Траффик на **http** разрешается, а весь остальной траффик запрещается. Посмотрим как это все работает на нашей Kali Linux. Попробуем пропинговать и подключится по SSH

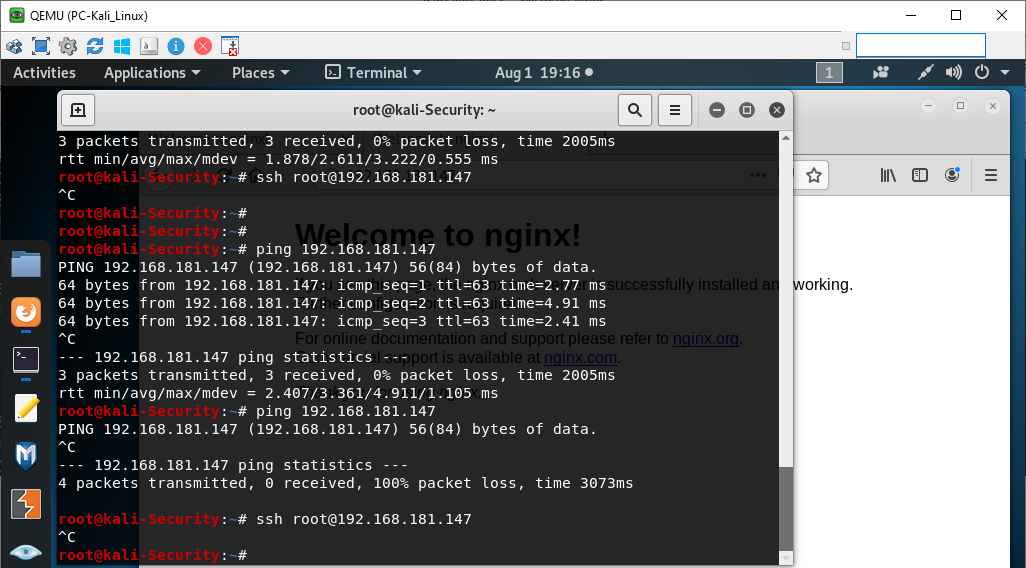


Рис. 31.

Видим, что не пигнуется и не подключается по SSH. Значит наши правила применились. Но если обновим веб-страницу, то все работает.

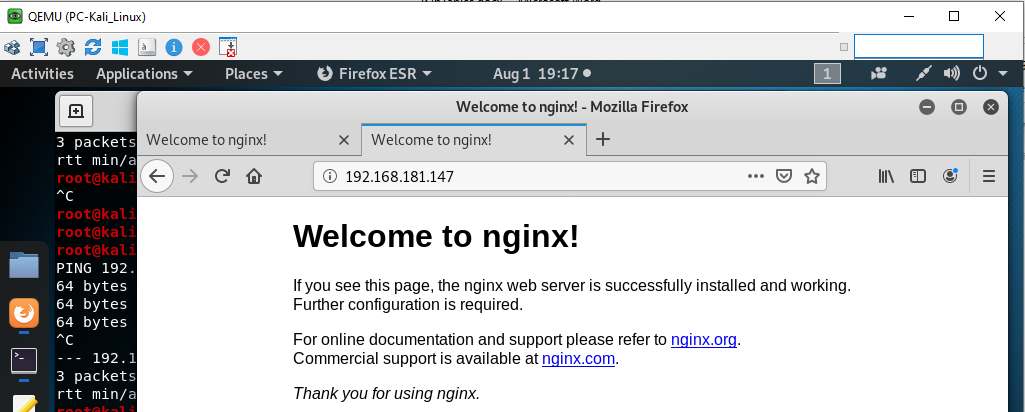


Рис. 32.