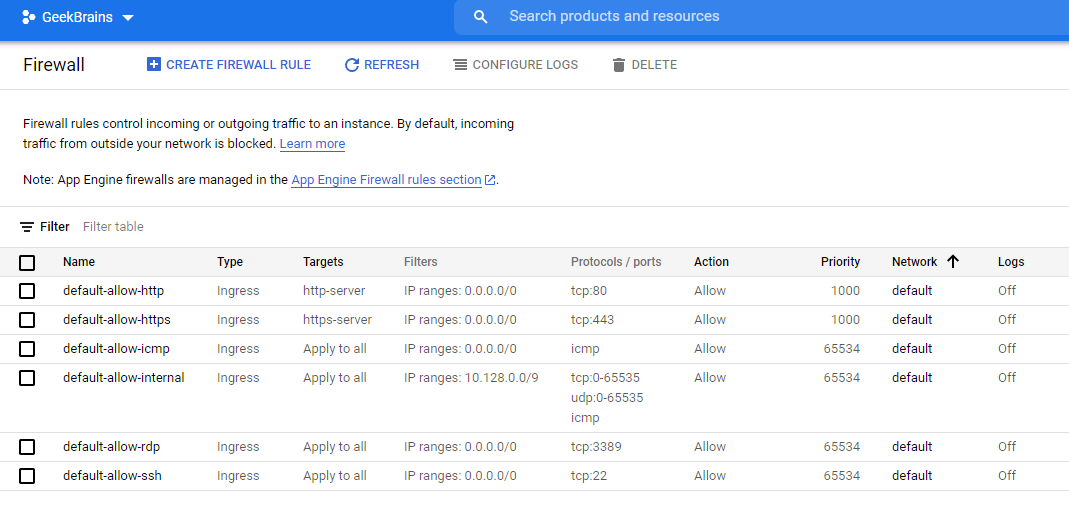
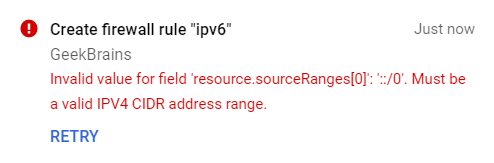
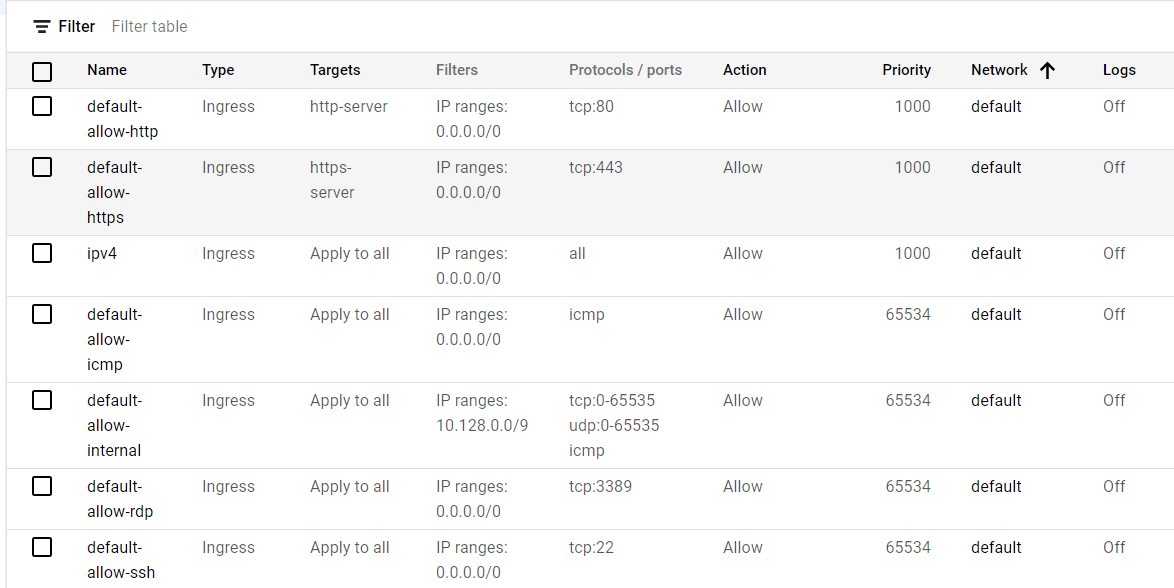
**1. Настроить сетевой фильтр, чтобы из внешней сети можно было обратиться только к сервисам http (80 и 443) и ssh. Отключить фаервол облачного провайдера.**

В Google cloud перешла на вкладку Firewall

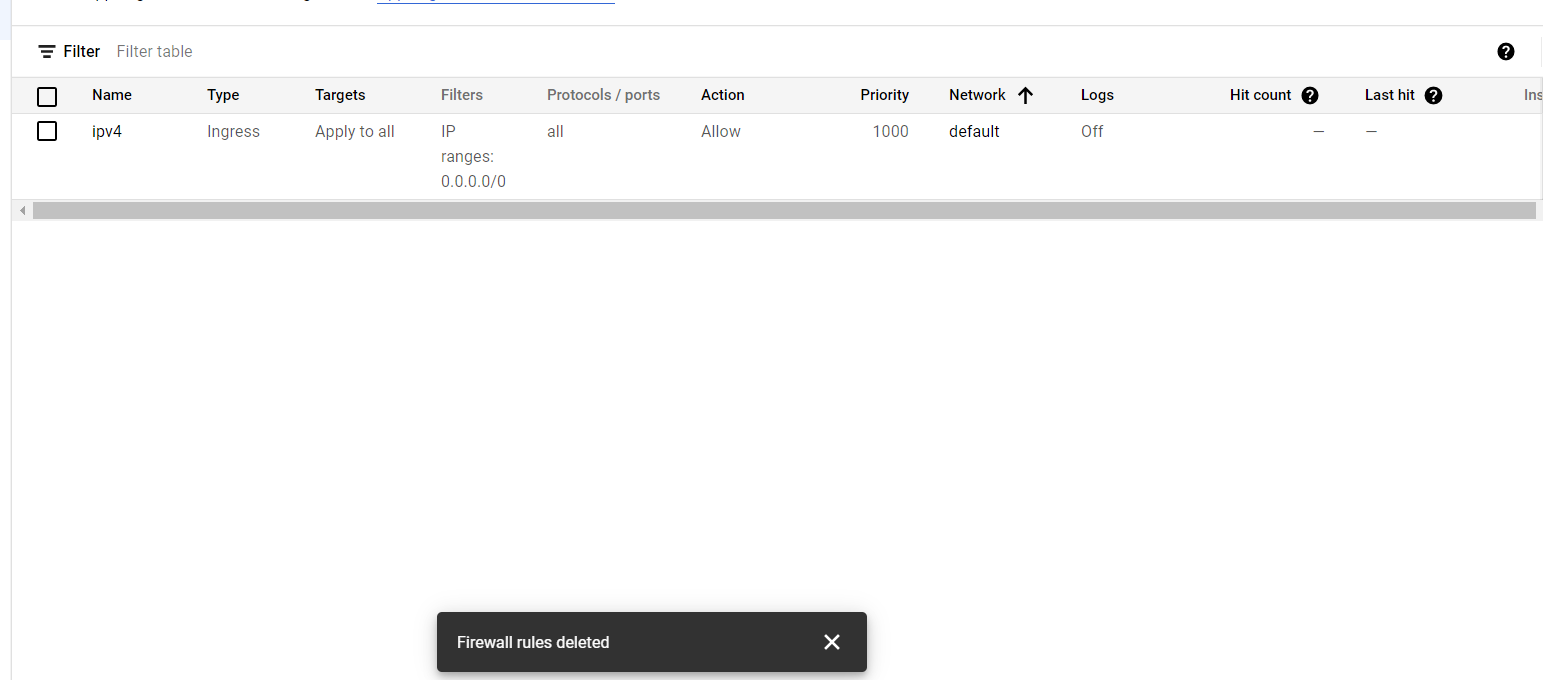


Добавила новый протокол ipv4 (ipv6 не удалось добавить)

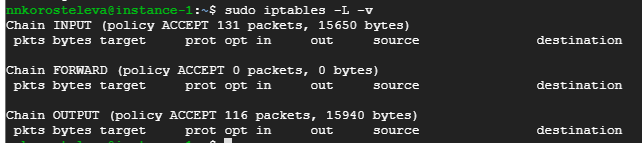




Удалила все правила, кроме ipv4



Проверка текущего состояния Iptables: sudo iptables -L –v

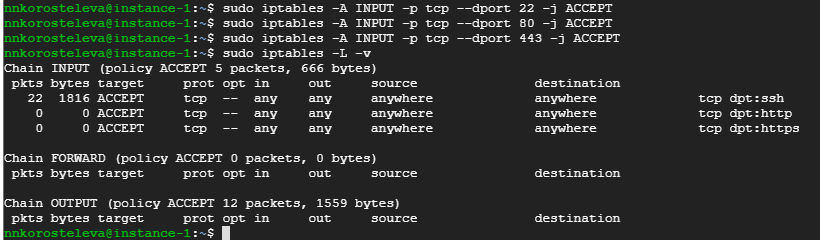


Разрешение подключений к портам HTTP, SSH и SSL

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

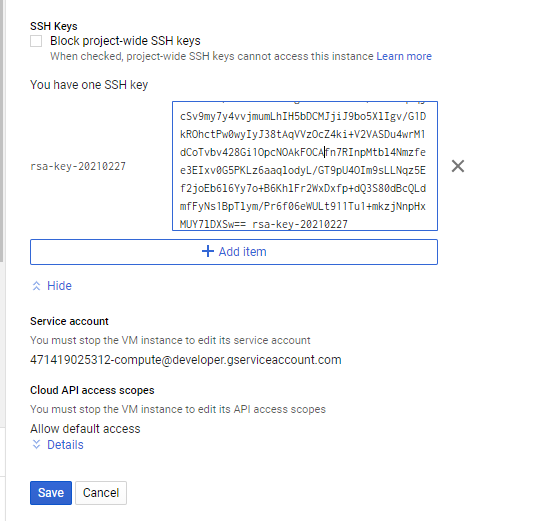


Сохранение изменений в iptables: sudo iptables-save > /etc/iptables.rules

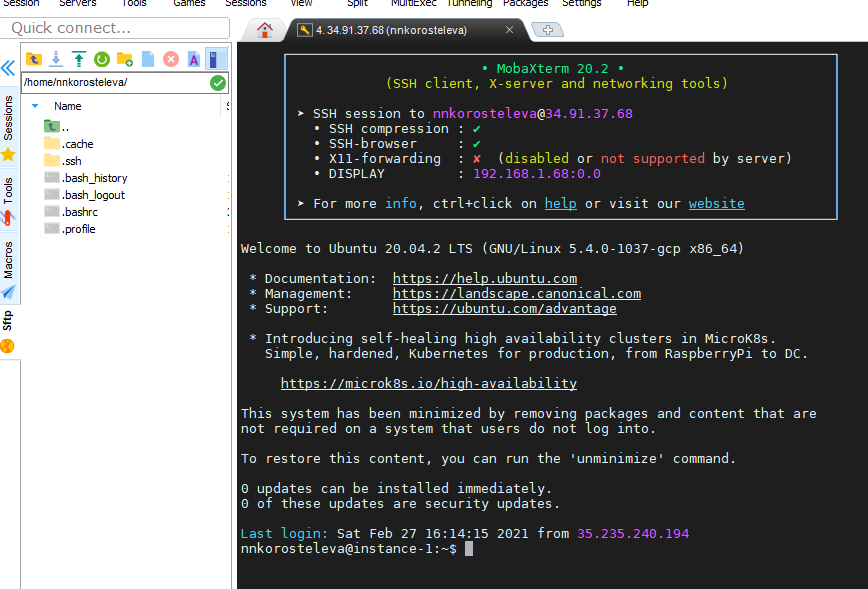
**2. Настроить SSH аутентификацию только по ключу, отключить парольную аутентификацию, запретить логин под root**

В puttygen сгенерировала публичный и приватный ключ. Приватный сохранила в файл с расширением ppk, а публичный скопировала.

Публичный ключ вставила в виртуальный сервер



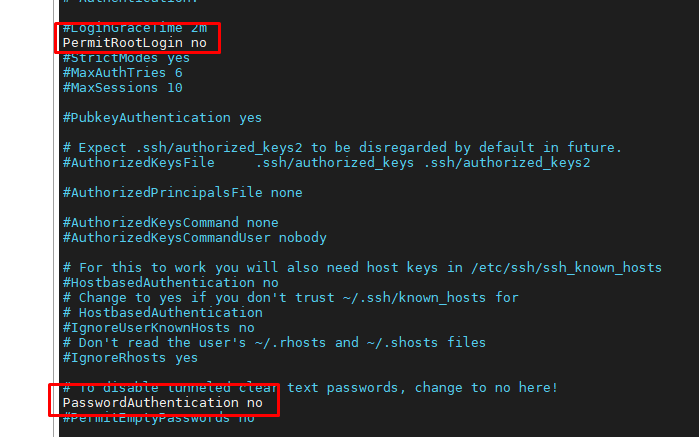
Приватный ключ использовала при подключении к серверу



Правим конфигплан для отключения возможность логиниться руту и доступ по паролям: sudo nano /etc/ssh/sshd\_config

PermitRootLogin no

PasswordAuthentication no

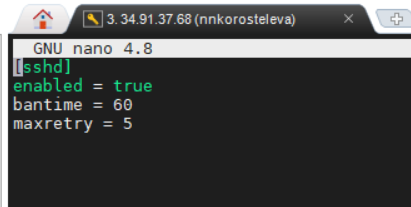


**3. Поставить и настроить fail2ban на блокировку SSH запросов с неверным паролем/ключом. Проверить работу fail2ban**

Поставила пакет fail2ban: sudo apt install fail2ban

Изменила файл конфигурации: sudo nano /etc/fail2ban/jail.d/defaults-debian.conf

И перезагрузила fail2ban: sudo systemctl restart fail2ban.service



Создала еще один виртуальный сервер и пробую подключиться к первоначальному

После 5 попыток блокирует пользователя

