• Настроить статическую конфигурацию (без DHCP) в Ubuntu через ip и netplan.  
Настроить IP, маршрут по умолчанию и DNS-сервера (1.1.1.1 и 8.8.8.8).  
Проверить работоспособность сети.

sudo nano /etc/netplan/01-network-manager-all.yaml

network:

version: 2

renderer: NetworkManager

ethernets:

enp0s3:

dhcp4: no

addresses: [192.168.0.134/24]

routes:

- to: default

via: 192.168.0.1

nameservers:

addresses:

- 8.8.8.8

- 1.1.1.1

ping [gb.ru](http://gb.ru/) -c 5 // проверяем соединение

• Настроить правила iptables для доступности сервисов на TCP-портах 22, 80 и 443.  
Также сервер должен иметь возможность устанавливать подключения к серверу обновлений.  
Остальные подключения запретить.

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT // добавляем в конец правило, что запрещаем все входящие соединения кроме соединения от 22 порта

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT // добавляем в конец правило, что запрещаем все входящие соединения кроме соединения от 80 порта

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT // добавляем в конец правило, что запрещаем все входящие соединения кроме соединения от 443 порта

sudo iptables -A INPUT -i lo -j ACCEPT // принимаем все соединения от себя

sudo iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT // подключение к серверу обновлений

sudo iptables -A INPUT -m state --state RELATED -j ACCEPT // подключение к серверу обновлений

sudo iptables -P INPUT DROP

• Запретить любой входящий трафик с IP 3.4.5.6.

sudo iptables -I INPUT -s 3.4.5.6 -j DROP

•\* Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере).

sudo iptables -t nat -A PREROUTING -p tcp --dport 8090 -j REDIRECT --to-port 80

•\* Разрешить подключение по SSH только из сети 192.168.0.0/24.

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

sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.0.0/16 -j DROP