```
$ sudo nano /etc/netplan/01-netcfg.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      addresses:
        - 192.168.1.100/24
      gateway4: 192.168.1.1
      nameservers:
          addresses: [1.1.1.1, 8.8.8.8]
$ sudo netplan apply
$ sudo apt-get install iptables
#!/bin/bash

# Очистка правил и цепочек
iptables -F
iptables -X

# Запрещаем все входящие и исходящие соединения по умолчанию
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Разрешаем уже установленные соединения
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Разрешаем локальный трафик
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Разрешаем SSH-соединения только из сети 192.168.0.0/24
iptables -A INPUT -p tcp --dport 22 -s 192.168.0.0/24 -j ACCEPT

# Разрешаем доступ к TCP-портам 22, 80 и 443
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# Разрешаем подключение к серверу обновлений
iptables -A OUTPUT -p tcp --dport 80 -d security.ubuntu.com -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -d security.ubuntu.com -j ACCEPT

# Запрещаем входящий трафик с IP 3.4
$ sudo nano iptables_rules.sh
```