site:

<https://www.wireguard.com/>

инструкция по установке:

https://losst.pro/ustanovka-wireguard-v-ubuntu

так-же GPT генерирует хорошую инструкцию

Установка WireGuard на сервере и клеенте под Ubuntu:

sudo apt install wireguard -y

так-же WireGuard есть в Ubuntu App Center, Client-GUI не работал

Генерация privatekeys и publickeys:

wg genkey | tee name\_privatekey | wg pubkey > name\_publickey

как минимум сгенерировать нужно для снрвера и клиента:

wg genkey | tee server\_privatekey | wg pubkey > server\_publickey

wg genkey | tee client\_privatekey | wg pubkey > client\_publickey

при генерации ключей они не устанавливаются в программу автоматически, это нужно делать вручную, поэтому удобнее генерировать все ключи на клиенте и записать их в один файлик.

Посмотреть ключи терминале:

cat server\_privatekey

cat server\_publickey

cat client\_privatekey

cat client\_publickey

cat name\_privatekey

cat name\_publickey

Посмотреть сетевые устройства:

ip address

Создать файл конфигурации на **сервер**е и открыть его в nano:

sudo nano /etc/wireguard/wg0.conf

Файл wg0.conf должен содержать:

[Interface]

Address = 10.0.0.1/24

SaveConfig = true

PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

ListenPort = 51820

PrivateKey = <Содержимое файла server\_privatekey>

[Peer]

PublicKey = <Содержимое client\_publickey>

AllowedIPs = 10.0.0.2/32

[Interface] - настройки сервера

Address - настройки vpn подсети, можно изменять

eth0 - название сетевого устройства сервера

ListenPort - порт сервера к которому будут подключатся клиенты

[Peer] - настройки клиента

AllowedIPs - назначаемый данному клиенту IP в vpn сети, в данном случае «/32» жестко

!Внимание! Редактирование конфигурационного файла при запущенном WireGuard невозможно.

Включаем переадресацию пакетов (чтобы клиенты могли выходить в интернет через VPN):

sudo nano /etc/sysctl.conf

раскоментируем строку (убрать #):

#net.ipv4.ip\_forward=1

Применяем изменения:

sudo sysctl -p

Запустить программу WireGuard сейчас, внести в автозагрузку системы, применить wg0 конфиг файл, использовать во всех стандартных случаях:

sudo systemctl enable --now [wg-quick@wg0](mailto:wg-quick@wg0)

Запустить/остановить WireGuard через systemd (если закрыть терминал продолжит работать, но после перезагрузки сам не запустится) и применить wg0 конфиг файл:

sudo systemctl start wg-quick@wg0

sudo systemctl stop wg-quick@wg0

перезагрузить WireGuard через systemd:

sudo systemctl restart wg-quick@wg0

Включить/отключить автозагрузку WireGuard при старте системы:

sudo systemctl enable [wg-quick@wg0](mailto:wg-quick@wg0)

sudo systemctl disable [wg-quick@wg0](mailto:wg-quick@wg0)

Запустить/остановить WireGuard в терминале (если закрыть остановится и после перезагрузки сам не запустится) и применить wg0 конфиг файл:

sudo wg-quick up wg0

sudo wg-quick down wg0

!Примечание: имя файла wg0.conf является стандартным, но может быть любым; при запуске WireGuard в команде нужно передавать имя конфигурационного файла; файлов может быть несколько, но тогда запускать нужно программу с каждым файлом отдельно.

Посмотреть статус WireGuard с конфигом wg0 при помощи systemd:

sudo systemctl status [wg-quick@wg0](mailto:wg-quick@wg0)

Примечание: статус «active (exited)» является нормальным.

Посмотреть статус WireGuard в самой программе:

sudo wg show

Разрешение/запрет доступа к порту по протоколу UDP в брандмауэера:

sudo ufw allow 51820/udp

sudo ufw deny 51820/udp

Примечание: в статье на losst открывали порт для WireGuard, но работало и без этого, имхо лучше не открывать.

Посмотреть используемые порты в системе:

netstat -tulnp

ss -tulnp

Создать файл конфигурации на **клиенте** и открыть его в nano:

sudo nano /etc/wireguard/wg0.conf

Файл wg0.conf должен содержать:

[Interface]

PrivateKey = <Содержимое client\_privatekey>

Address = 10.0.0.2/24

DNS = 8.8.8.8

[Peer]

PublicKey = <Содержимое server\_publickey>

Endpoint = serverIP:51820

AllowedIPs = 0.0.0.0/0

PersistentKeepalive = 25

[Interface] - настройки клиента

Address - настройки vpn подсети, можно изменять, зависят от настрояк сервера

[Peer] - настройки сервера

Endpoint - ip адрес и порт сервера

AllowedIPs - допустимый ip диапазон сервера - все

Запустить/останавливать программу WireGuard на клиенте можно так-же как и на сервере (смотри выше), но имхо удобнее:

sudo wg-quick up wg0

sudo wg-quick down wg0