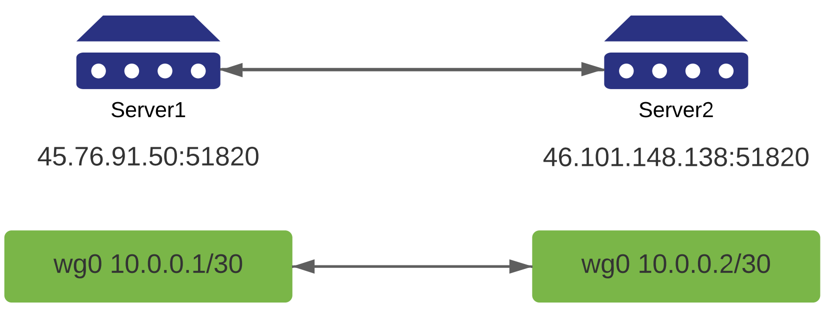
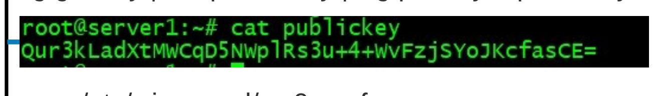
Point - to - Point



Point-2-Point настройка Server1

apt update
apt upgrade
apt install wireguard
umask 077

wg genkey | tee privatekey | wg pubkey > publickey



```
root@server1:~# cat publickey
Qur3kLadXtMWCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
```

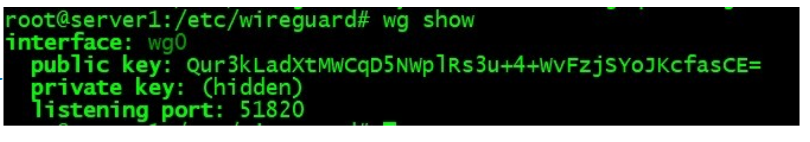
```
root@server1:~# cat privatekey
KBxgNAljKTqNj1p8AZ/FGngE/KZYW3yvlfDWX++IAHY=
```

nano /etc/wireguard/wg0.conf

```
[Interface]
PrivateKey = <Server 1 private key>
Address = 10.0.0.1/30
ListenPort = 51820
```

PrivateKey - Приватный ключ сгенерированный на Server1. Не забывайте подставить вместо <Server 1 private key> свой приватный ключ
Address - IP адрес в wireguard vpn тоннеле на стороне Server1
ListenPort - порт на котором висит wireguard. На этот порт подключаются клиенты которые хотят посроить vpn тоннель.

systemctl enable wg-quick@wg0
systemctl start wg-quick@wg0



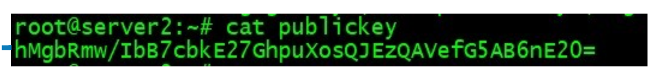
```
root@server1:/etc/wireguard# wg show
interface: wg0
  public key: Qur3kLadXtMWCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
  private key: (hidden)
  listening port: 51820
```

```
root@server1:~# cat /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.1/24
ListenPort = 51820
PrivateKey = KBxgNAljKTqNj1p8AZ/FGngE/KZYW3yvlfDWX++IAHY=
```

Point-2-Point настройка Server2

apt update
apt upgrade
apt install wireguard
umask 077

wg genkey | tee privatekey | wg pubkey > publickey



```
root@server2:~# cat publickey
hMgbRmw/IbB7cbkE27GhpuXosQJEzQAVefG5AB6nE20=
```

```
root@server2:~# cat privatekey
OO0uPOK/+8C/SNlUSV71VB7eXYWKS+zxZFefo0PJkn8=
```

nano /etc/wireguard/wg0.conf

```
[Interface]
PrivateKey = <Server 2 private key>
Address = 10.0.0.2/30
ListenPort = 51820
```

PrivateKey - Приватный ключ сгенерированный на Server2. Не забывайте подставить вместо <Server 2 private key> свой приватный ключ
Address - IP адрес в wireguard vpn тоннеле на стороне Server2
ListenPort - порт на котором висит wireguard. На этот порт подключаются клиенты которые хотят посроить vpn тоннель.

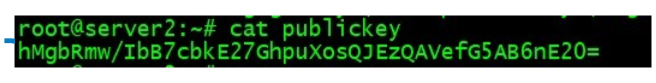
systemctl enable wg-quick@wg0
systemctl start wg-quick@wg0

```
root@server2:~# wg show
interface: wg0
  public key: hMgbRmw/IbB7cbkE27GhpuXosQJEzQAVefG5AB6nE20=
  private key: (hidden)
  listening port: 51820
```

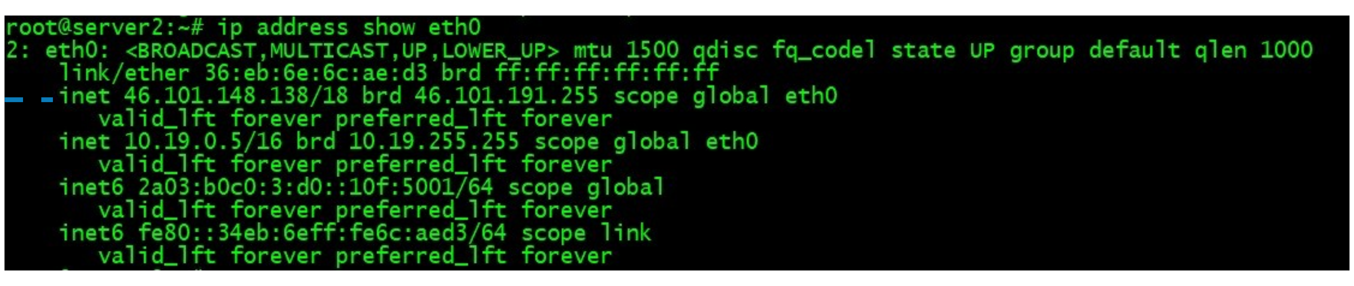
```
root@server2:~# cat /etc/wireguard/wg0.conf
[Interface]
PrivateKey = OO0uPOK/+8C/SNlUSV71VB7eXYWKS+zxZFefo0PJkn8=
Address = 10.0.0.2/30
ListenPort = 51820
```

Настройка client на **Server1**

nano /etc/wireguard/wg0.conf



```
root@server2:~# cat publickey
hMgbRmw/IbB7cbkE27GhpuXosQJEzQAVefG5AB6nE20=
```



```
root@server2:~# ip address show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 36:eb:6e:6c:ae:d3 brd ff:ff:ff:ff:ff:ff
    inet 46.101.148.138/18 brd 46.101.191.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.19.0.5/16 brd 10.19.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2a03:b0c0:3:d0::10f:5001/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::34eb:6eff:fe6c:aed3/64 scope link
       valid_lft forever preferred_lft forever
```

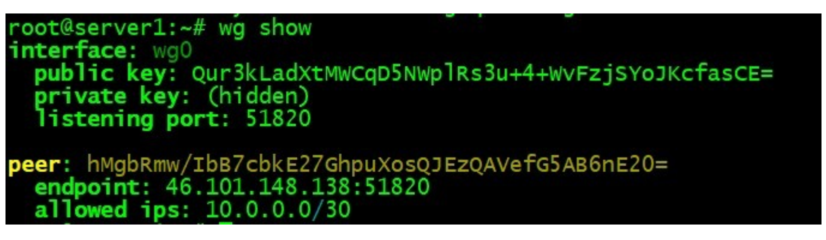
```
[Peer]
PublicKey = <Server2 Public key>
Endpoint = <Server2 Public IP>:51820
AllowedIPs = 10.0.0.0/30
```

PublicKey = Публичный ключ клиента который подключается к этому серверу
Endpoint = Публичный ip адрес клиента который подключается к серверу
AllowedIPs = Список сетей смаршрутизированных в тоннель

systemctl restart wg-quick@wg0

Если в конфиге сервера нет опции SaveConfig = true то перед редактированием конфига не обязательно останавливать сервер WG. В противном случае если SaveConfig = true присудствует то обязательно остановите сервер через systemctl stop wg-quick@wg0.service, только после этого можно редактировать конфигурационный файл и созранить его, после чего необходимо включить сервер через systemctl start wg-quick@wg0.service

Если всё сделано правильно то после настройки вывод следующих команд на server1 должен выглядеть так

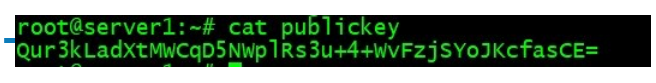


```
root@server1:~# wg show
interface: wg0
  public key: Qur3kLadXtMWCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
  private key: (hidden)
  listening port: 51820

peer: hMgbRmw/IbB7cbkE27GhpuXosQJEzQAVefG5AB6nE20=
  endpoint: 46.101.148.138:51820
  allowed ips: 10.0.0.0/30
```

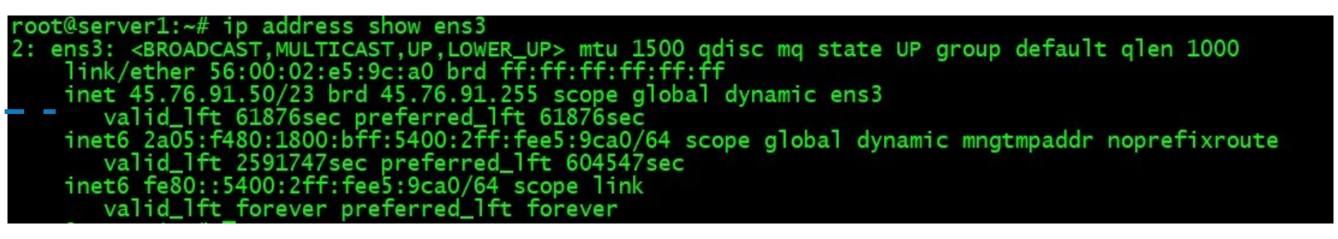
```
root@server1:~# ip address show wg0
12: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.0.0.1/24 scope global wg0
       valid_lft forever preferred_lft forever
```

Настройка client на **Server2**

nano /etc/wireguard/wg0.conf



```
root@server1:~# cat publickey
Qur3kLadXtMWCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
```



```
root@server1:~# ip address show ens3
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 56:00:02:e5:9c:a0 brd ff:ff:ff:ff:ff:ff
    inet 45.76.91.50/23 brd 45.76.91.255 scope global dynamic ens3
       valid_lft 61876sec preferred_lft 61876sec
    inet6 2a05:f480:1800:bff:5400:2ff:fee5:9ca0/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591747sec preferred_lft 604547sec
    inet6 fe80::5400:2ff:fee5:9ca0/64 scope link
       valid_lft forever preferred_lft forever
```

```
[Peer]
PublicKey = <Server1 Public key>
Endpoint = <Server1 Public IP>:51820
AllowedIPs = 10.0.0.0/30
```

PublicKey = Публичный ключ клиента который подключается к этому серверу
Endpoint = Публичный ip адрес клиента который подключается к серверу
AllowedIPs = Список сетей смаршрутизированных в тоннель

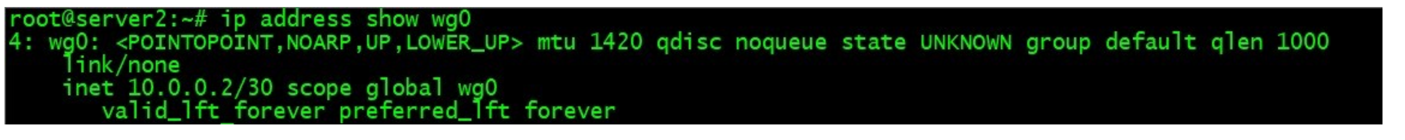
systemctl restart wg-quick@wg0

Если в конфиге сервера нет опции SaveConfig = true то перед редактированием конфига не обязательно останавливать сервер WG. В противном случае если SaveConfig = true присудствует то обязательно остановите сервер через systemctl stop wg-quick@wg0.service, только после этого можно редактировать конфигурационный файл и созранить его, после чего необходимо включить сервер через systemctl start wg-quick@wg0.service

Если всё сделано правильно то после настройки вывод следующих команд на server1 должен выглядеть так

```
root@server2:~# wg show
interface: wg0
  public key: hMgbRmw/IbB7cbkE27GhpuXosQJEzQAVefG5AB6nE20=
  private key: (hidden)
  listening port: 51820

peer: Qur3kLadXtMWCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
  endpoint: 45.76.91.50:51820
  allowed ips: 10.0.0.0/30
  latest handshake: 29 seconds ago
  transfer: 348 B received, 436 B sent
```

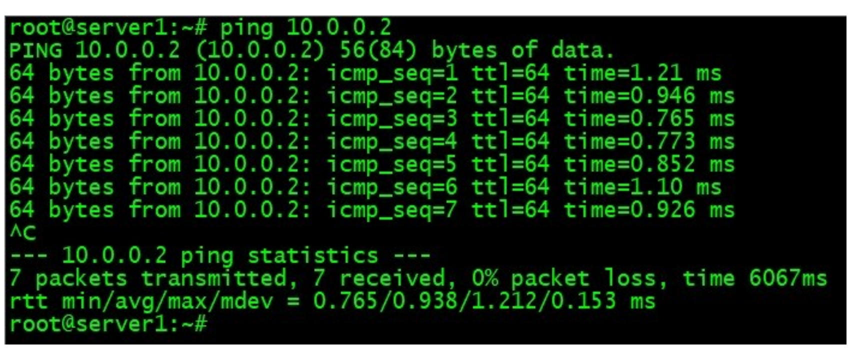
Данные о последнем "рукопожатии" между клиентом и сервером становятся доступны только плсле того как соединение будет успешно установленно.
Ниже распологаются данные о колличестве трафика переданные между сервером и клиентом за время сессии.



```
root@server2:~# ip address show wg0
4: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.0.0.2/30 scope global wg0
       valid_lft forever preferred_lft forever
```

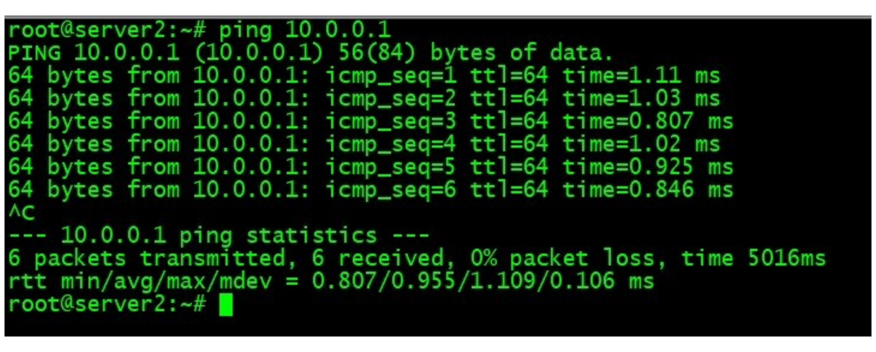
Тестирование наличия соединения

Server1



```
root@server1:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.946 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.765 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.773 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.852 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=1.10 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=0.926 ms
^C
--- 10.0.0.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6067ms
rtt min/avg/max/mdev = 0.765/0.938/1.212/0.153 ms
root@server1:~#
```

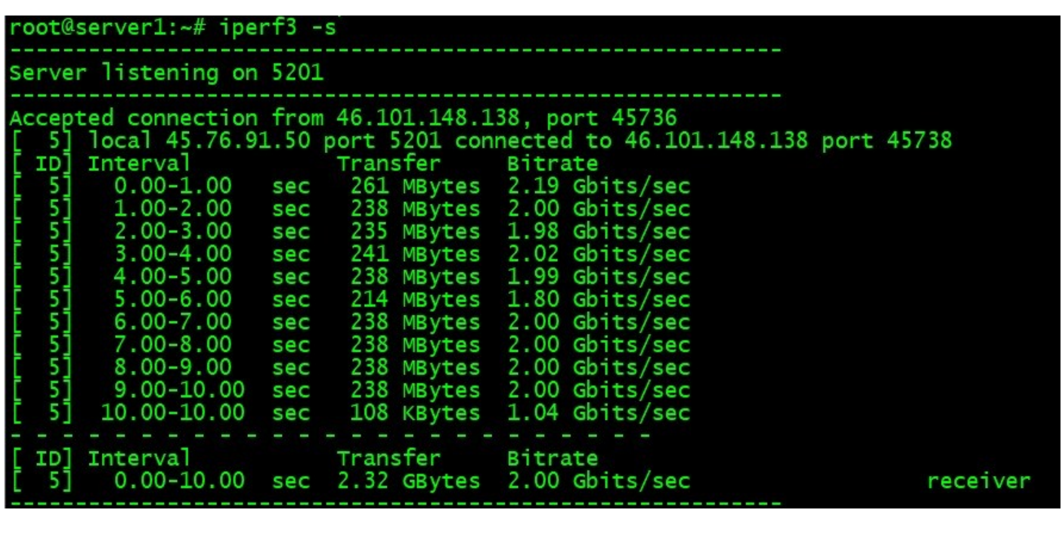
Server1



```
root@server2:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=1.03 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.807 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=1.02 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=0.925 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=0.846 ms
^C
--- 10.0.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5016ms
rtt min/avg/max/mdev = 0.807/0.955/1.109/0.106 ms
root@server2:~#
```

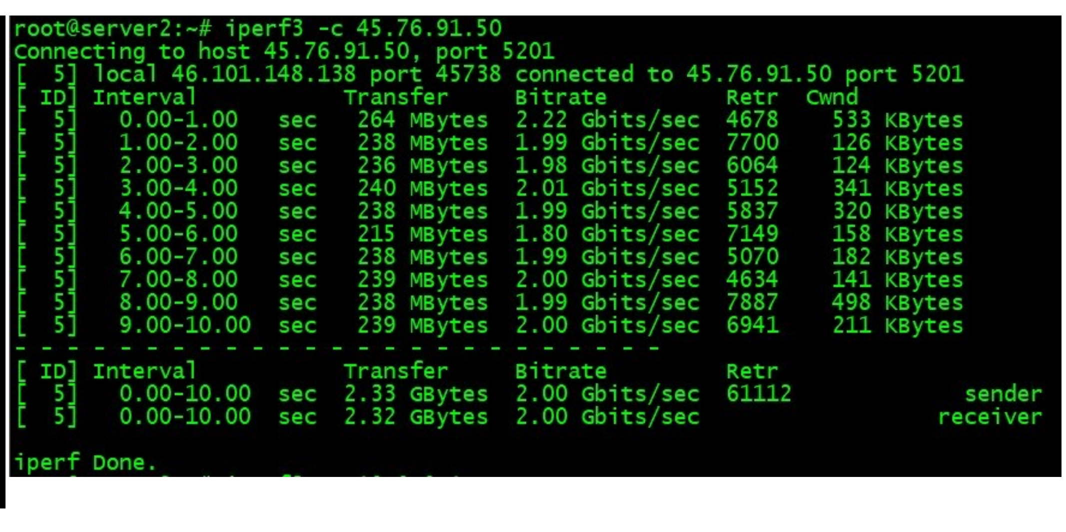
Тестирование скорости

Server1

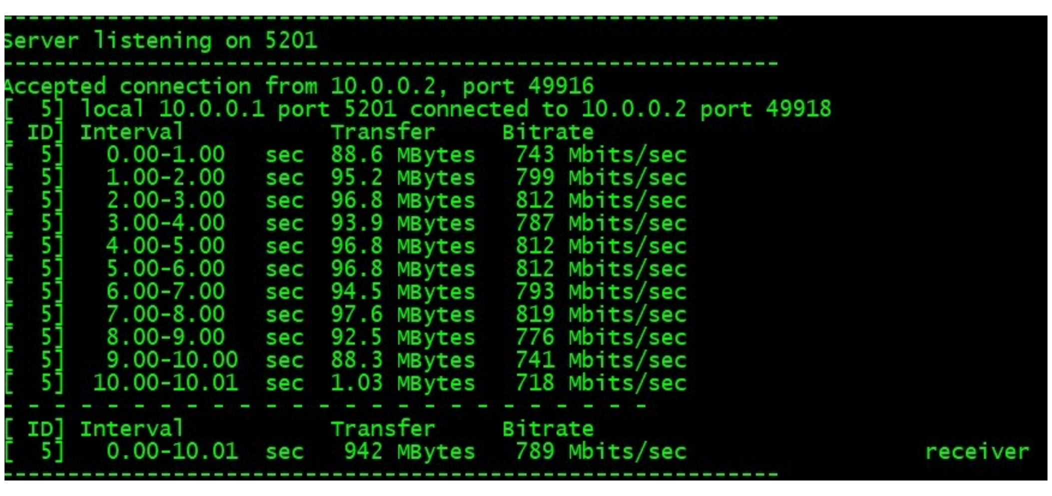


```
root@server1:~# iperf3 -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 46.101.148.138, port 45736
[  5] local 45.76.91.50 port 5201 connected to 46.101.148.138 port 45738
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec   261 MBytes  2.19 Gbits/sec
[  5]   1.00-2.00   sec   238 MBytes  2.00 Gbits/sec
[  5]   2.00-3.00   sec   235 MBytes  1.98 Gbits/sec
[  5]   3.00-4.00   sec   241 MBytes  2.02 Gbits/sec
[  5]   4.00-5.00   sec   238 MBytes  1.99 Gbits/sec
[  5]   5.00-6.00   sec   214 MBytes  1.80 Gbits/sec
[  5]   6.00-7.00   sec   238 MBytes  2.00 Gbits/sec
[  5]   7.00-8.00   sec   238 MBytes  2.00 Gbits/sec
[  5]   8.00-9.00   sec   238 MBytes  2.00 Gbits/sec
[  5]   9.00-10.00  sec   238 MBytes  2.00 Gbits/sec
[  5]  10.00-10.00  sec   108 KBytes  1.04 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec  2.32 GBytes  2.00 Gbits/sec                  receiver
-----------------------------------------------------------
```

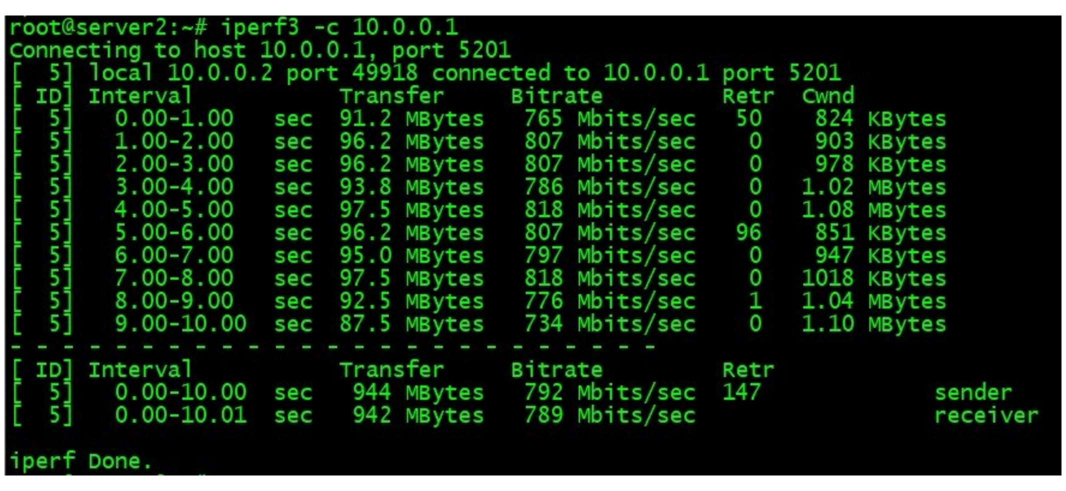
Server1



```
root@server2:~# iperf3 -c 45.76.91.50
Connecting to host 45.76.91.50, port 5201
[  5] local 46.101.148.138 port 45738 connected to 45.76.91.50 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   264 MBytes  2.22 Gbits/sec  4678    533 KBytes
[  5]   1.00-2.00   sec   238 MBytes  1.99 Gbits/sec  7700    126 KBytes
[  5]   2.00-3.00   sec   236 MBytes  1.98 Gbits/sec  6064    124 KBytes
[  5]   3.00-4.00   sec   240 MBytes  2.01 Gbits/sec  5152    341 KBytes
[  5]   4.00-5.00   sec   238 MBytes  1.99 Gbits/sec  5837    320 KBytes
[  5]   5.00-6.00   sec   215 MBytes  1.80 Gbits/sec  7149    158 KBytes
[  5]   6.00-7.00   sec   238 MBytes  1.99 Gbits/sec  5070    182 KBytes
[  5]   7.00-8.00   sec   239 MBytes  2.00 Gbits/sec  4634    141 KBytes
[  5]   8.00-9.00   sec   238 MBytes  1.99 Gbits/sec  7887    498 KBytes
[  5]   9.00-10.00  sec   239 MBytes  2.00 Gbits/sec  6941    211 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  2.33 GBytes  2.00 Gbits/sec  61112             sender
[  5]   0.00-10.00  sec  2.32 GBytes  2.00 Gbits/sec                  receiver

iperf Done.
```

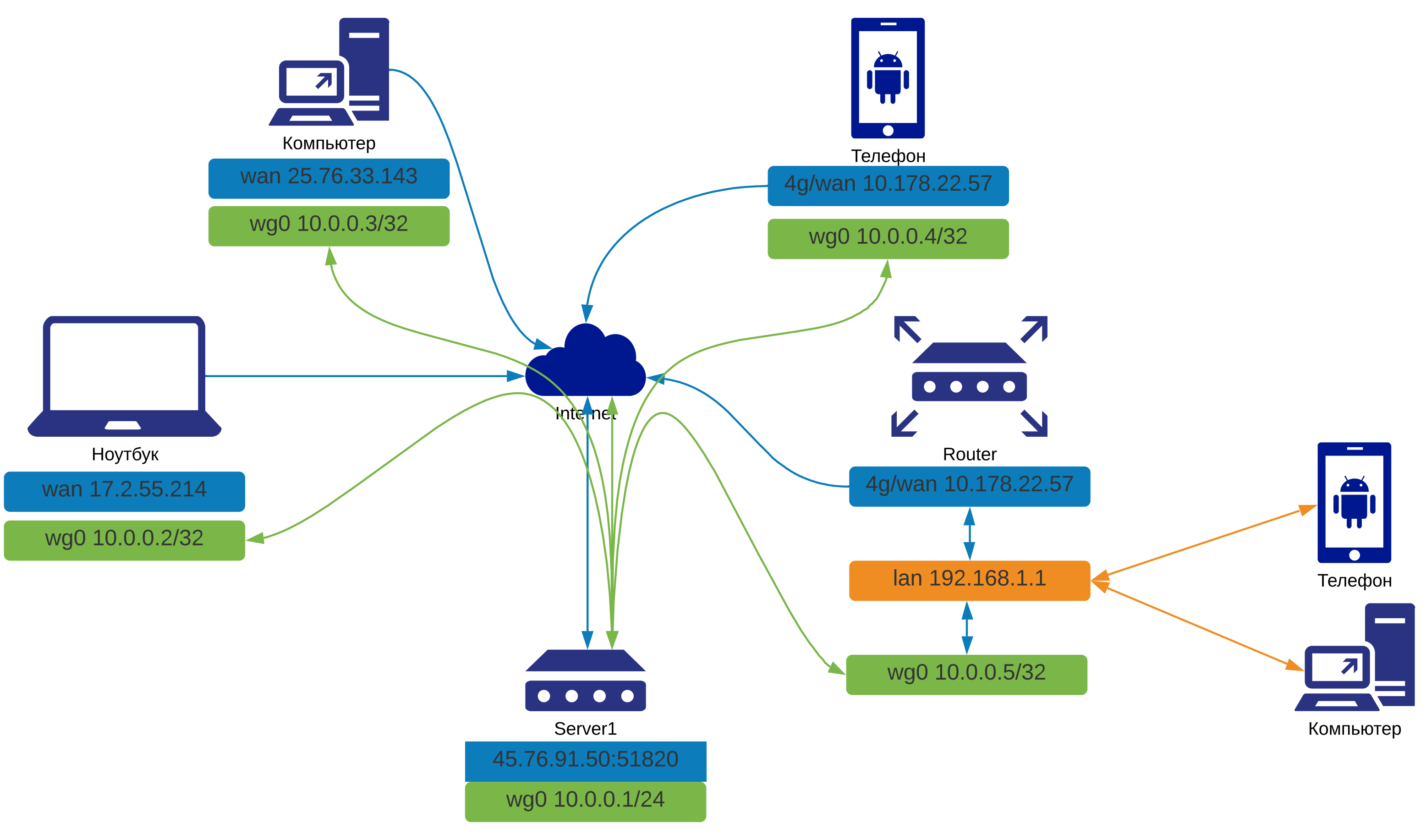


```
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 10.0.0.2, port 49916
[  5] local 10.0.0.1 port 5201 connected to 10.0.0.2 port 49918
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  88.6 MBytes   743 Mbits/sec
[  5]   1.00-2.00   sec  95.2 MBytes   799 Mbits/sec
[  5]   2.00-3.00   sec  96.8 MBytes   812 Mbits/sec
[  5]   3.00-4.00   sec  93.9 MBytes   787 Mbits/sec
[  5]   4.00-5.00   sec  96.8 MBytes   812 Mbits/sec
[  5]   5.00-6.00   sec  96.8 MBytes   812 Mbits/sec
[  5]   6.00-7.00   sec  94.5 MBytes   793 Mbits/sec
[  5]   7.00-8.00   sec  97.6 MBytes   819 Mbits/sec
[  5]   8.00-9.00   sec  92.5 MBytes   776 Mbits/sec
[  5]   9.00-10.00  sec  88.3 MBytes   741 Mbits/sec
[  5]  10.00-10.01  sec  1.03 MBytes   718 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.01  sec   942 MBytes   789 Mbits/sec                  receiver
-----------------------------------------------------------
```



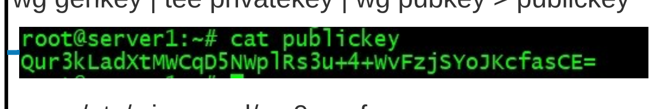
```
root@server2:~# iperf3 -c 10.0.0.1
Connecting to host 10.0.0.1, port 5201
[  5] local 10.0.0.2 port 49918 connected to 10.0.0.1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  91.2 MBytes   765 Mbits/sec   50    824 KBytes
[  5]   1.00-2.00   sec  96.2 MBytes   807 Mbits/sec    0    903 KBytes
[  5]   2.00-3.00   sec  96.2 MBytes   807 Mbits/sec    0    978 KBytes
[  5]   3.00-4.00   sec  93.8 MBytes   786 Mbits/sec    0   1.02 MBytes
[  5]   4.00-5.00   sec  97.5 MBytes   818 Mbits/sec    0   1.08 MBytes
[  5]   5.00-6.00   sec  96.2 MBytes   807 Mbits/sec   96    851 KBytes
[  5]   6.00-7.00   sec  95.0 MBytes   797 Mbits/sec    0    947 KBytes
[  5]   7.00-8.00   sec  97.5 MBytes   818 Mbits/sec    0   1018 KBytes
[  5]   8.00-9.00   sec  92.5 MBytes   776 Mbits/sec    1   1.04 MBytes
[  5]   9.00-10.00  sec  87.5 MBytes   734 Mbits/sec    0   1.10 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec   944 MBytes   792 Mbits/sec  147             sender
[  5]   0.00-10.01  sec   942 MBytes   789 Mbits/sec                  receiver

iperf Done.
```

Star (звезда)



Star настройка Server1

apt update
apt upgrade
apt install wireguard
umask 077
wg genkey | tee privatekey | wg pubkey > publickey



```
root@server1:~# cat publickey
Qur3kLadXtMwCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
```

```
root@server1:~# cat privatekey
KBxgNA1jKTqNj1p8AZ/FGngE/KZYW3yvlfDWX++IAHY=
```

nano /etc/wireguard/wg0.conf

```
[Interface]
PrivateKey = <Server 1 private key>
Address = 10.0.0.1/24
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o ens3 -j MASQUERADE
ListenPort = 51820
SaveConfig = true
```

PrivateKey - Приватный ключ сгенерированный на Server1. Не забывайте подставить вместо <Server 1 private key> свой приватный ключ
Address - IP адрес в wireguard vpn тоннеле на стороне Server1. В топологии "Звезда" желательно использовать маску большого размера
ListenPort - порт на котором висит wireguard. На этот порт подключаются клиенты которые хотят посроить vpn тоннель.
SaveConfig - Автоматически сохраняет в конфигурационный файл параметры EndPoint клиентов подключившихся к серверу
PostUP - Набор команд или скрипт который будет запущен после старта сервера.
PostDown - Набор команд или скрипт который будет запущен после остановки сервера.
В PostUP и PostDown нужно поменять имя сетевого интерфейса на котором настроен публичный ip на своё!!

systemctl enable wg-quick@wg0
systemctl start wg-quick@wg0

```
root@server1:/etc/wireguard# wg show
interface: wg0
  public key: Qur3kLadXtMwCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
  private key: (hidden)
  listening port: 51820
```

```
root@server1:~# cat /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.1/24
ListenPort = 51820
PrivateKey = KBxgNA1jKTqNj1p8AZ/FGngE/KZYW3yvlfDWX++IAHY=
SaveConfig = true
```

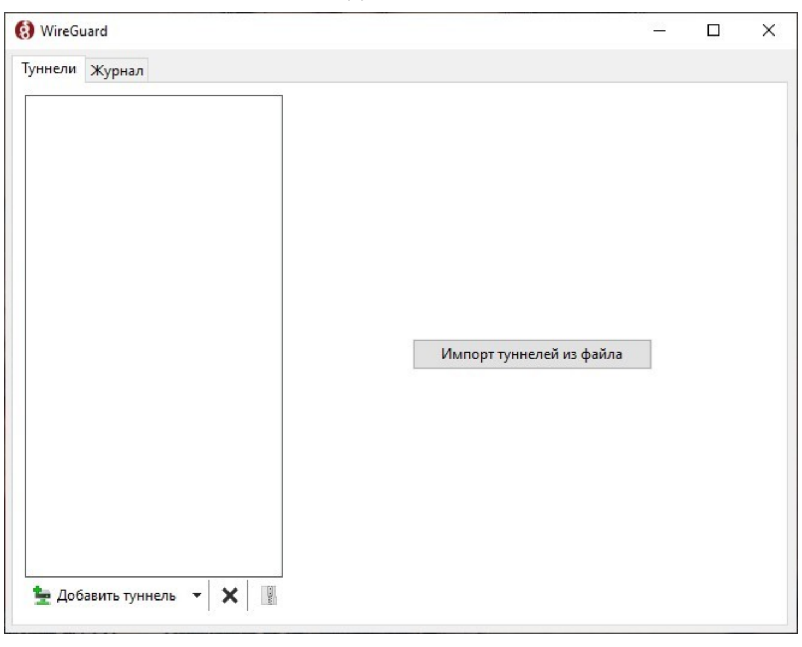
Включение Форвординга

Раскоментируем в файле /etc/sysctl.conf параметр
net.ipv4.ip_forward=1

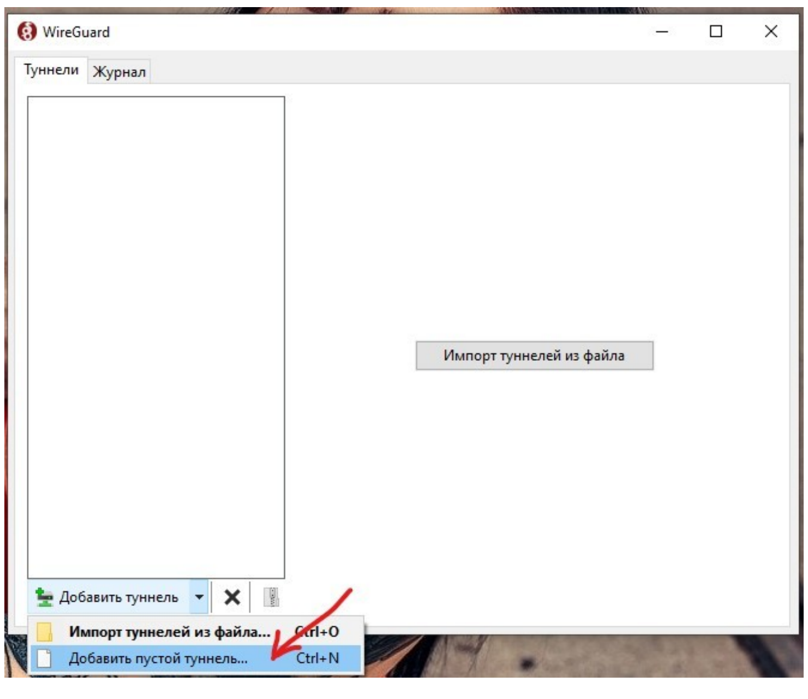
После этого выполняем команду
echo 1 > /proc/sys/net/ipv4/ip_forward

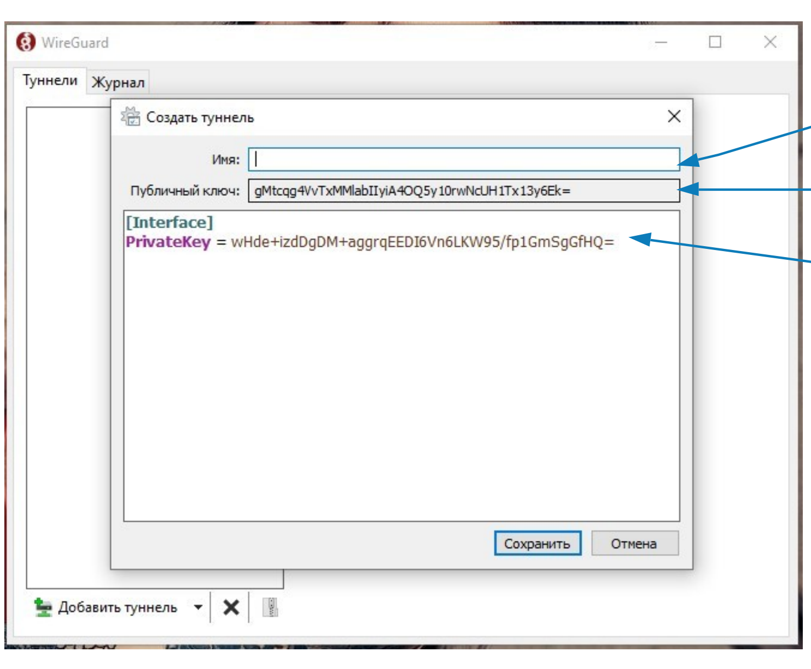
Star настройка Windows Client

Скачиваем с официального сайта https://www.wireguard.com/ клиент для windows и устанавливаем.
Главное окно клиента выглядит вот так.



Добавляем пустоятоннель





Имя:
Публичный ключ: gMtcqg4VvTxMMlabIIyiA4OQ5y10rwNcUH1Tx13y6Ek=

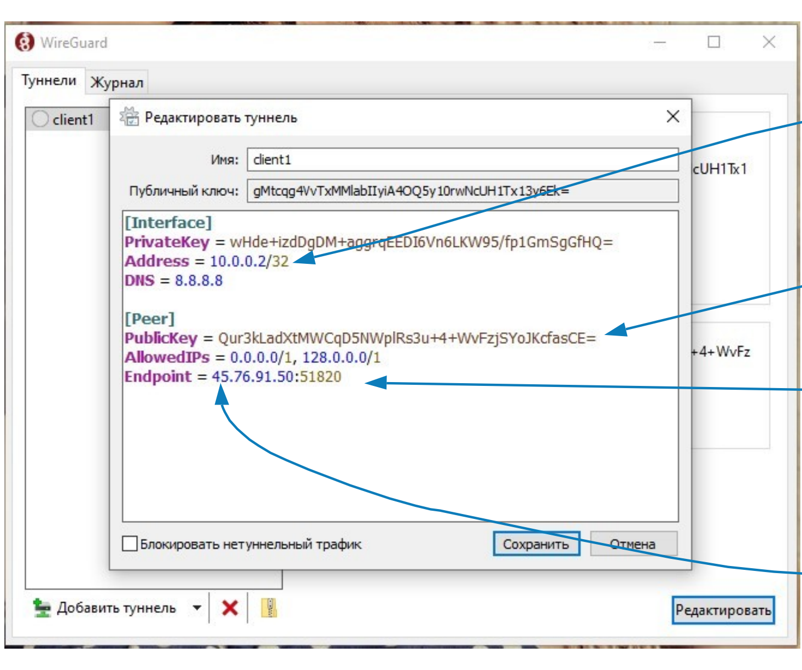
```
[Interface]
PrivateKey = wHde+izdDgDM+aggrqEEDI6Vn6LKW95/fp1GmSgGfHQ=
```

Имя нового подключения.
Оно будет отображатся в программе и не влияет ни на что.

Публичный ключь. Копируется на сервер

Приватный ключь. Остаются у клиента

Конфигурационный файл клиента составляется в соответствии с этими правилами:

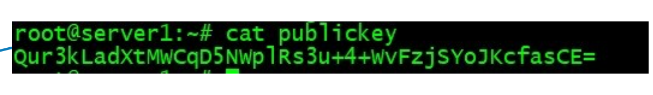


Имя: client1
Публичный ключ: gMtcqg4VvTxMMlabIIyiA4OQ5y10rwNcUH1Tx13y6Ek=

```
[Interface]
PrivateKey = wHde+izdDgDM+aggrqEEDI6Vn6LKW95/fp1GmSgGfHQ=
Address = 10.0.0.2/32
DNS = 8.8.8.8

[Peer]
PublicKey = Qur3kLadXtMWCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
AllowedIPs = 0.0.0.0/1, 128.0.0.0/1
Endpoint = 45.76.91.50:51820
```

Адрес клиента внутри VPN тонеля с маской /24 как на сервере

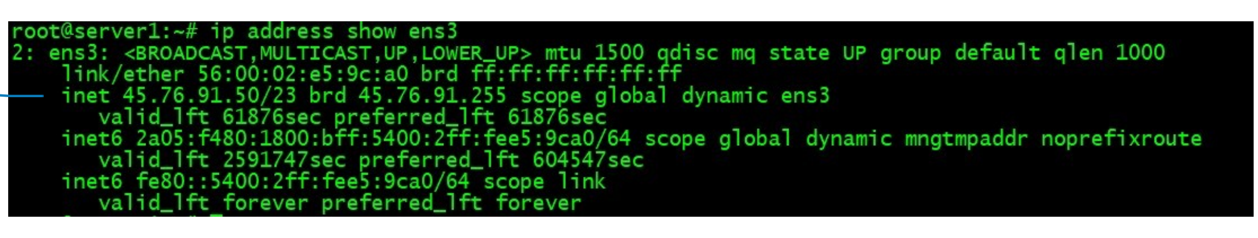
Публичный ключ взятый с сервера



```
root@server1:~# cat publickey
Qur3kLadXtMwCqD5NWplRs3u+4+WvFzjSYoJKcfasCE=
```

Публичный IP адрес сервера и порт на котором поднят wireguard

```
root@server1:~# cat /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.1/24
ListenPort = 51820
PrivateKey = KBxgNA1jKTqNj1p8AZ/FGngE/KZYW3yvlfDWX++IAHY=
```



```
root@server1:~# ip address show ens3
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 56:00:02:e5:9c:a0 brd ff:ff:ff:ff:ff:ff
    inet 45.76.91.50/23 brd 45.76.91.255 scope global dynamic ens3
       valid_lft 61876sec preferred_lft 61876sec
    inet6 2a05:f480:1800:bff:5400:2ff:fee5:9ca0/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591747sec preferred_lft 604547sec
    inet6 fe80::5400:2ff:fee5:9ca0/64 scope link
       valid_lft forever preferred_lft forever
```

После всех настроек нажимаем кнопку сохранить.
Параметр DNS устанавливает ip адрес DNS сервера который будет использоватся при отправке запросов через VPN тоннель.
Если вы хотите маршрутизировать весь трафик через wireguard то вам необходимо поставить параметр AllowedIPs = 0.0.0.0/1, 128.0.0.0/1
Этит параметр установит ваш Wireguard как шлюз по умолчанию.

Добавление клиента на Server1

nano /etc/wireguard/wg0.conf

```
[Peer]
PublicKey = <Client1 Public key>
AllowedIPs = 10.0.0.2/32
```

Перед всеми манипуляциями с конфигурацией сервера надо остановить wireguard!! Делается это коммандой systemctl stop wg-quick@wg0.service
PublickKey - Публичный ключ клиента который передаётся серверу
Address - IP адрес клиента

systemctl enable wg-quick@wg0
systemctl start wg-quick@wg0

Клиент wireguard android

Качаем приложение с плеймаркета по ссылке https://play.google.com/store/apps/details?id=com.wireguard.android или ищем через поиск и устанавливаем на устройство.

Открываем программу и нажимаем на плюс в нижнем левом углу. Выбираем "Создать вручную".
Задаём имя подключения.
Генерируем приватный и публичный ключ нажатием на две стрелки в поле "Приватный ключ".
В поле "IP-адреса" пишем ip адрес внутри vpn тоннеля который будет использоватся на стороне нашего клиента, в данном случае это телефон. Поле "порт" оставляем пустым.
В поле DNS указываем 8.8.8.8 или любой публичный DNS сервер.
Поле MTU можно оставить пустым. Оптимальное значение MTU чаще всего устанавливается автоматически.

Публичный ключ клиента, необходимо скопировать и вставить в конфигурацию сервера.

Интерфейс
Имя: vpn
Приватный ключ: ••
Публичный ключ: LpnfuUCypYGYM3hQPn+YLHzpkcXHLkFBh...
IP-адреса: 10.0.0.3/32
Порт: (авто)
DNS-серверы: 8.8.8.8
MTU: (авто)

Добавление клиента на Server1

nano /etc/wireguard/wg0.conf

```
[Peer]
PublicKey = <Client2 Public key>
AllowedIPs = 10.0.0.3/32
```

Перед всеми манипуляциями с конфигурацией сервера надо остановить wireguard!! Делается это коммандой systemctl stop wg-quick@wg0.service
PublickKey - Публичный ключ клиента который передаётся серверу
Address - IP адрес клиента

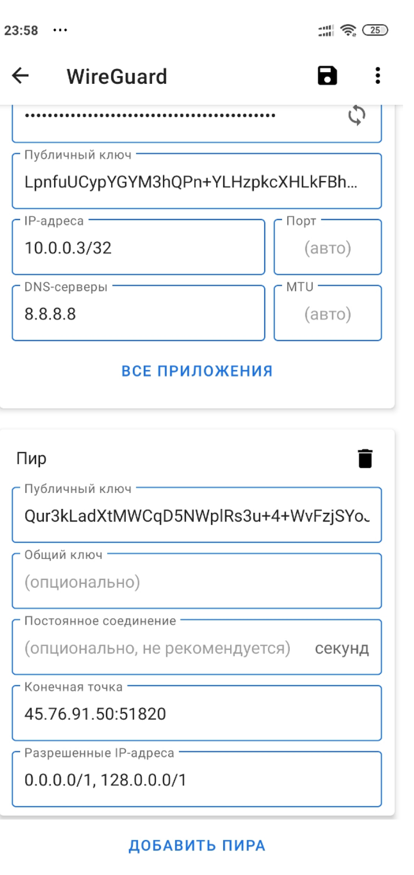
systemctl enable wg-quick@wg0
systemctl start wg-quick@wg0

После всех манипуляций с сервером и добавления второго клиента, конфиг сервера выглядит так.

```
root@server1:~# cat /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.1/24
SaveConfig = true
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o ens3 -j MASQUERADE
ListenPort = 51820
PrivateKey = KBxgNA1jKTqNj1p8AZ/FGngE/KZYW3yvlfDWX++IAHY=

[Peer]
PublicKey = gMtcqg4VvTxMMlabIIyiA4OQ5y10rwNcUH1Tx13y6Ek=
AllowedIPs = 10.0.0.2/32

[Peer]
PublicKey = LpnfuUCypYGYM3hQPn+YLHzpkcXHLkFBhm4qZMT5oDw=
AllowedIPs = 10.0.0.3/32
root@server1:~#
```

В устройстве с Android в созданном нами подключении нажимаем на кнопку "Добавить пира"
В поле "публичный ключь" вставляем публичный ключ сервера.
Поля "Общий ключ" и "Почтоянное соединение" оставляем пустыми.
Поле "Конечная точка" должно содержать IP адрес и порт сервера на котором висит wireguard
В поле "Разрешённые IP-адреса" вводим 0.0.0.0/1, 128.0.0.0/1

После добавления всех настроек, нажимаем на изображение дискеты и сохраняем настройки.
Затем можно активировать VPN тоннель.



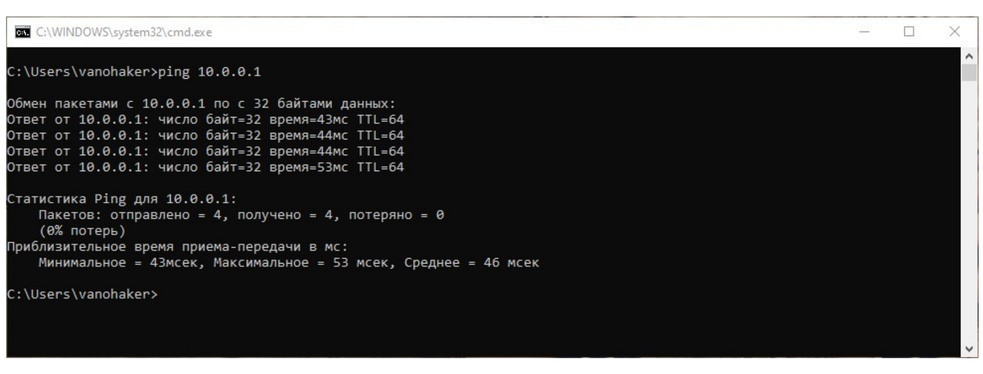
Публичный ключ: LpnfuUCypYGYM3hQPn+YLHzpkcXHLkFBh...
IP-адреса: 10.0.0.3/32
Порт: (авто)
DNS-серверы: 8.8.8.8
MTU: (авто)

Пир
Публичный ключ: Qur3kLadXtMWCqD5NWplRs3u+4+WvFzjSYo...
Общий ключ: (опционально)
Постоянное соединение: (опционально, не рекомендуется) секунд
Конечная точка: 45.76.91.50:51820
Разрешенные IP-адреса: 0.0.0.0/1, 128.0.0.0/1

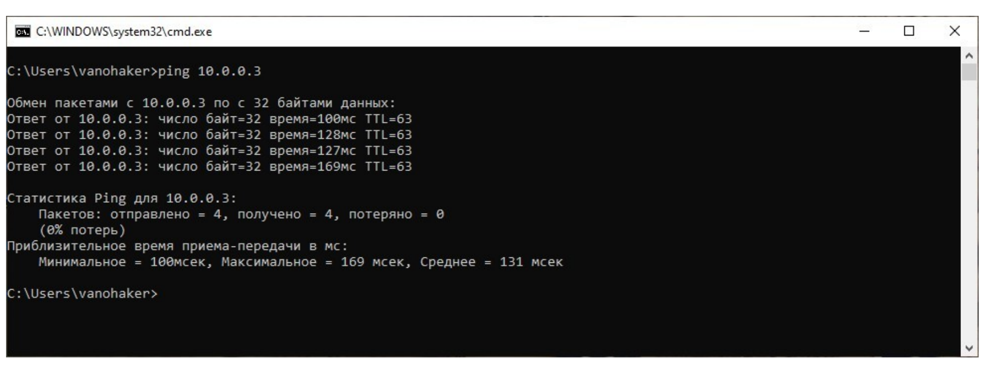
Проверка работоспособности VPN между пирами и наличия доступа в интернет

Windows 10. 2ip.ru, tracert, ping

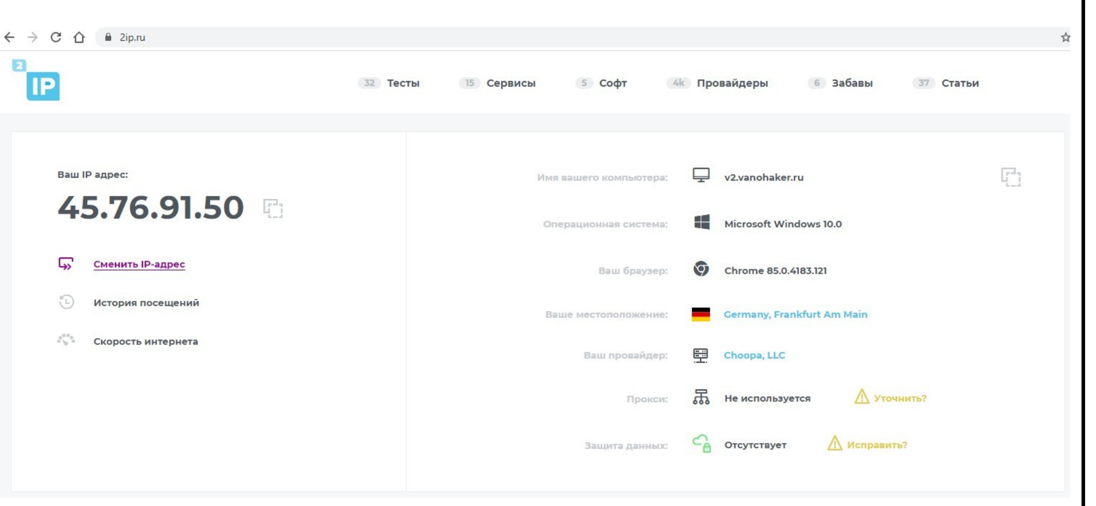
```
C:\Users\vanohaker>tracert google.ru

Трассировка маршрута к google.ru [216.58.208.35]
с максимальным числом прыжков 30:

  1    44 ms    43 ms    43 ms  10.0.0.1
  2     *        *        *     Превышен интервал ожидания для запроса.
  3    47 ms    47 ms    47 ms  vl199-ds1-b5-R3B06.fkt3.choopa.net [45.63.118.33]
  4     *        *        *     Превышен интервал ожидания для запроса.
  5     *        *        *     Превышен интервал ожидания для запроса.
  6    44 ms    44 ms    44 ms  ipv4.de-cix.fra.de.as15169.google.com [80.81.192.108]
  7    48 ms    48 ms    54 ms  108.170.252.1
  8    48 ms    45 ms    45 ms  66.249.94.147
  9    45 ms    46 ms    46 ms  fra15s12-in-f35.1e100.net [216.58.208.35]

Трассировка завершена.

C:\Users\vanohaker>
```



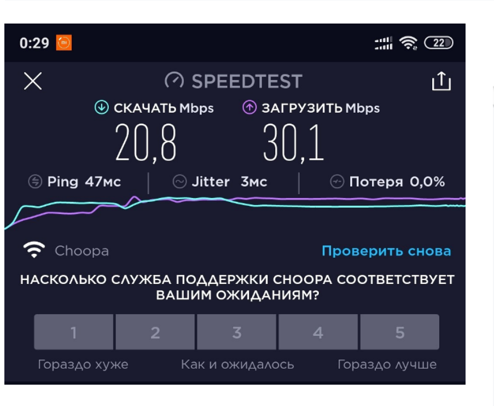
```
C:\Users\vanohaker>ping 10.0.0.1

Обмен пакетами с 10.0.0.1 по с 32 байтами данных:
Ответ от 10.0.0.1: число байт=32 время=43мс TTL=64
Ответ от 10.0.0.1: число байт=32 время=44мс TTL=64
Ответ от 10.0.0.1: число байт=32 время=44мс TTL=64
Ответ от 10.0.0.1: число байт=32 время=53мс TTL=64

Статистика Ping для 10.0.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 43мсек, Максимальное = 53 мсек, Среднее = 46 мсек

C:\Users\vanohaker>
```



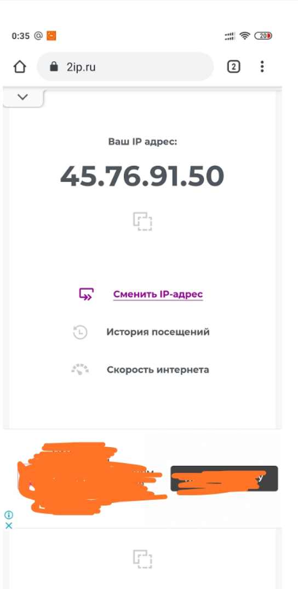
```
C:\Users\vanohaker>ping 10.0.0.3

Обмен пакетами с 10.0.0.3 по с 32 байтами данных:
Ответ от 10.0.0.3: число байт=32 время=100мс TTL=63
Ответ от 10.0.0.3: число байт=32 время=128мс TTL=63
Ответ от 10.0.0.3: число байт=32 время=127мс TTL=63
Ответ от 10.0.0.3: число байт=32 время=169мс TTL=63

Статистика Ping для 10.0.0.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 100мсек, Максимальное = 169 мсек, Среднее = 131 мсек

C:\Users\vanohaker>
```



Ваш IP адрес: 45.76.91.50
Имя вашего компьютера: v2.vanohaker.ru
Операционная система: Microsoft Windows 10.0
Ваш браузер: Chrome 85.0.4183.121
Ваше местоположение: Germany, Frankfurt Am Main
Ваш провайдер: Choopa, LLC
Прокси: Не используется
Защита данных: Отсутствует



СКАЧАТЬ Mbps 20,8
ЗАГРУЗИТЬ Mbps 30,1
Ping 47мс
Jitter 3мс
Потеря 0,0%
Choopa

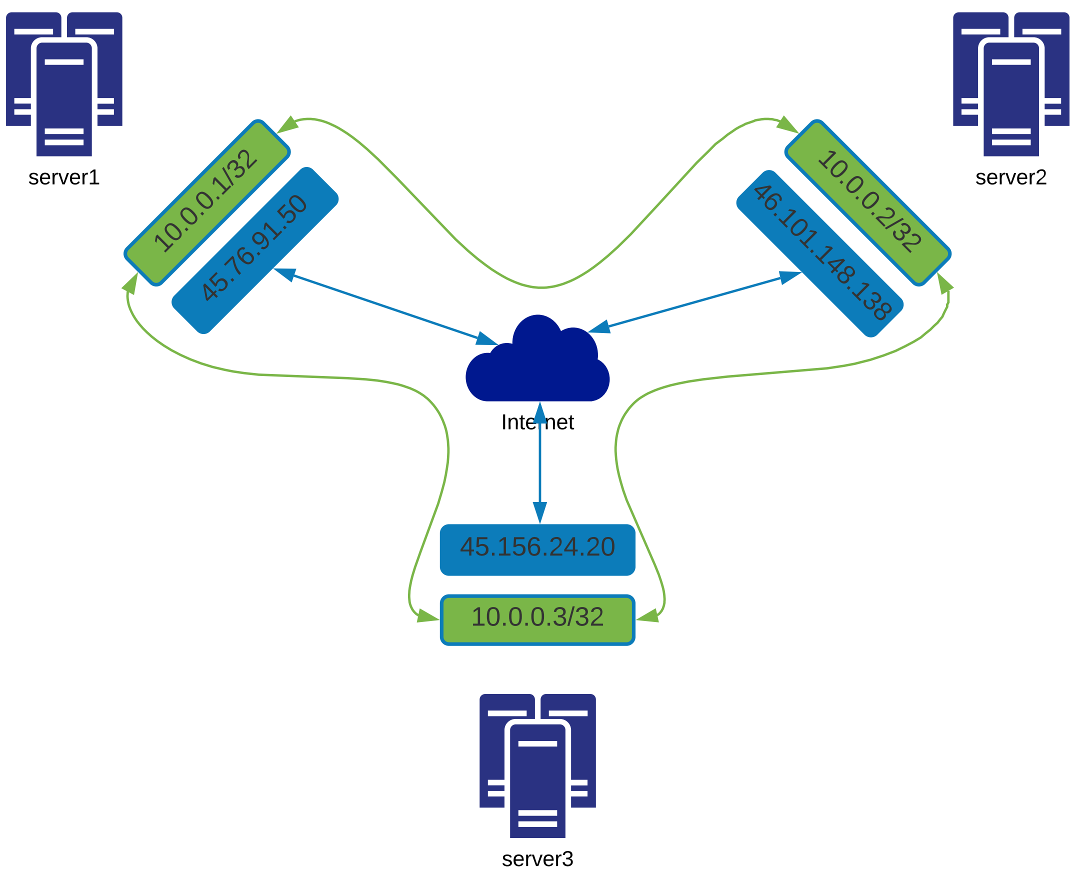


Ваш IP адрес: 45.76.91.50

[redacted]

Имя вашего компьютера:

Mesh



Установка

```
apt update
apt upgrade
apt install wireguard
```

Создаём ключи на всех серверах

```
umask 077
wg genkey | tee privatekey | wg pubkey > publickey
```

```
root@server1:~# wg genkey | tee privatekey | wg pubkey > publickey
root@server1:~# cat privatekey
WEGZ5E+kzU8YQlm4Y3OuRQJPx3eFIqdcZHPNp26eeFw=
root@server1:~# cat publickey
oOuqVyllg5GK1Bz+5ntexj46p7hOBFbTgE6cjVvwvQw=
root@server1:~#
```

```
root@server2:~# wg genkey | tee privatekey | wg pubkey > publickey
root@server2:~# cat privatekey
QFhk1d3XiJNg+YLtAoUxvfLkBoSc53ZmO+r4Zk/lYUI=
root@server2:~# cat publickey
DQIcYT2xn4HibAesToDTQXIjAisdMuzjTrYCStWRgz0=
root@server2:~#
```

```
root@server3:~# wg genkey | tee privatekey | wg pubkey > publickey
root@server3:~# cat privatekey
GJXeiAo+AwetoxiYQktEwieIC/LmavTWnn0EC/+ymH4=
root@server3:~# cat publickey
gC22IaN/JjNwmgTNcC9MBszSWcleit272jTpYx56Tyg=
root@server3:~#
```

Создаём полный конфигурационный файл на Server1

```
nano /etc/wireguard/wg0.conf
[Interface]
PrivateKey = < Server1 private key >
Address = 10.0.0.1/32
ListenPort = 51820
[Peer]
PublicKey = < Server2 public key >
AllowedIPs = 10.0.0.2/32
Endpoint = < Server2 ip address >:51820
[Peer]
PublicKey = < Server3 public key >
AllowedIPs = 10.0.0.3/32
Endpoint = < Server3 ip address >:51820
```

```
root@server1:~# cat /etc/wireguard/wg0.conf
[Interface]
PrivateKey = WEGZ5E+kzU8YQlm4Y3OuRQJPx3eFIqdcZHPNp26eeFw=
Address = 10.0.0.1/32
ListenPort = 51820

[Peer]
PublicKey = DQIcYT2xn4HibAesToDTQXIjAisdMuzjTrYCStWRgz0=
AllowedIPs = 10.0.0.2/32
Endpoint = 46.101.148.138:51820

[Peer]
PublicKey = gC22IaN/JjNwmgTNcC9MBszSWcleit272jTpYx56Tyg=
AllowedIPs = 10.0.0.3/32
Endpoint = 45.156.24.20:51820
root@server1:~#
```

Создаём полный конфигурационный файл на Server2

```
nano /etc/wireguard/wg0.conf
[Interface]
PrivateKey = < Server2 private key >
Address = 10.0.0.2/32
ListenPort = 51820
[Peer]
PublicKey = < Server1 public key >
AllowedIPs = 10.0.0.1/32
Endpoint = < Server1 ip address >:51820
[Peer]
PublicKey = < Server3 public key >
AllowedIPs = 10.0.0.3/32
Endpoint = < Server3 ip address >:51820
```

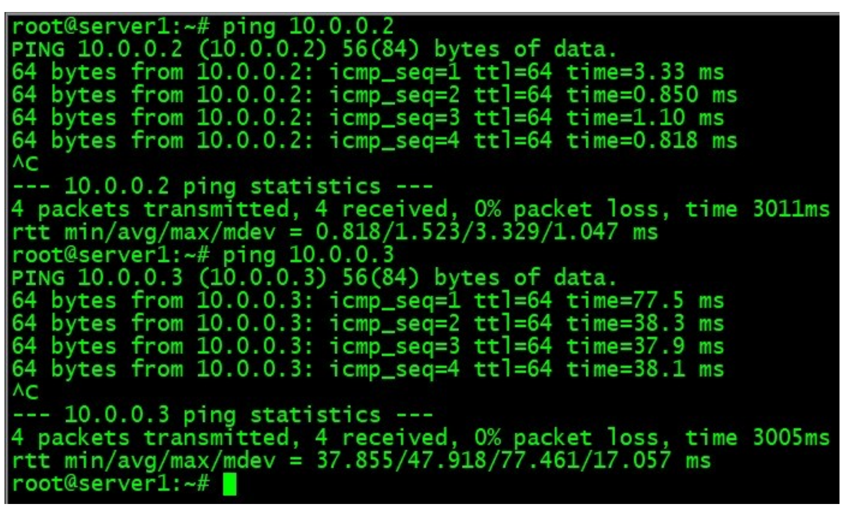
```
root@server2:~# cat /etc/wireguard/wg0.conf
[Interface]
PrivateKey = QFhk1d3XiJNg+YLtAoUxvfLkBoSc53ZmO+r4Zk/lYUI=
Address = 10.0.0.2/32
ListenPort = 51820

[Peer]
PublicKey = oOuqVyllg5GK1Bz+5ntexj46p7hOBFbTgE6cjVvwvQw=
AllowedIPs = 10.0.0.1/32
Endpoint = 45.76.91.50:51820

[Peer]
PublicKey = gC22IaN/JjNwmgTNcC9MBszSWcleit272jTpYx56Tyg=
AllowedIPs = 10.0.0.3/32
Endpoint = 45.156.24.20:51820
root@server2:~#
```

Создаём полный конфигурационный файл на Server3

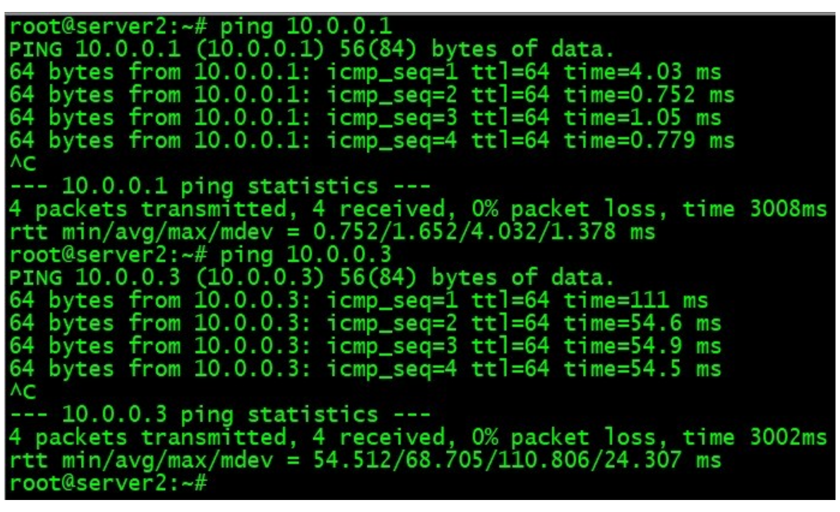
```
nano /etc/wireguard/wg0.conf
[Interface]
PrivateKey = < Server3 private key >
Address = 10.0.0.3/32
ListenPort = 51820
[Peer]
PublicKey = < Server1 public key >
AllowedIPs = 10.0.0.1/32
Endpoint = < Server1 ip address >:51820
[Peer]
PublicKey = < Server2 public key >
AllowedIPs = 10.0.0.2/32
Endpoint = < Server2 ip address >:51820
```

```
root@server3:~# cat /etc/wireguard/wg0.conf
[Interface]
PrivateKey = GJXeiAo+AwetoxiYQktEwieIC/LmavTWnn0EC/+ymH4=
Address = 10.0.0.3/32
ListenPort = 51820

[Peer]
PublicKey = oOuqVyllg5GK1Bz+5ntexj46p7hOBFbTgE6cjVvwvQw=
AllowedIPs = 10.0.0.1/32
Endpoint = 45.76.91.50:51820

[Peer]
PublicKey = DQIcYT2xn4HibAesToDTQXIjAisdMuzjTrYCStWRgz0=
AllowedIPs = 10.0.0.2/32
Endpoint = 46.101.148.138:51820
root@server3:~#
```

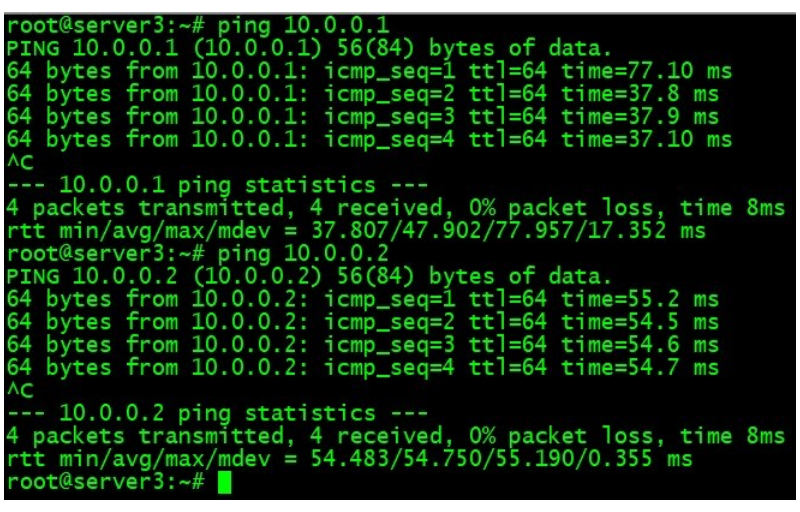
Тестирование



```
root@server1:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=3.33 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.850 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.818 ms
^C
--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 0.818/1.523/3.329/1.047 ms
root@server1:~# ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=77.5 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=38.3 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=37.9 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=38.1 ms
^C
--- 10.0.0.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 37.855/47.918/77.461/17.057 ms
root@server1:~#
```



```
root@server2:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=4.03 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.752 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.779 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.752/1.652/4.032/1.378 ms
root@server2:~# ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=111 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=54.6 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=54.9 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=54.5 ms
^C
--- 10.0.0.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 54.512/68.705/110.806/24.307 ms
root@server2:~#
```



```
root@server3:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=77.10 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=37.8 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=37.9 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=37.10 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 37.807/47.902/77.957/17.352 ms
root@server3:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=55.2 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=54.5 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=54.6 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=54.7 ms
^C
--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 54.483/54.750/55.190/0.355 ms
root@server3:~#
```

Примечание

В данном примере в качестве третьего сервера использовался Debian 10. В маём примере wireguard сразу не запустился на этом дистрибутиве. В случае возникновения проблем попробуйте выполнить комманду

```
sudo apt-get install linux-headers-$(uname -r|sed 's/[^-]*-[^-]*-//')
```