1. **На сервере server3 добавить еще один интерфейс — dummy с IP-адресом 33.33.33.33/32.**

```
5: dummy1: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 9e:18:c9:a7:59:0b brd ff:ff:ff:ff:ff:ff
    inet 33.33.33.33/32 brd 33.33.33.33 scope global dummy1
       valid_lft forever preferred_lft forever
    inet6 fe80::9c18:c9ff:fea7:590b/64 scope link
       valid_lft forever preferred_lft forever
```

2. НЕ анонсировать этот интерфейс в OSPF.

Ок

3. Поднять openvpn-сервер на server3 и обеспечить возможность подключения клиента server1, используя сертификаты.

Поднимаем openvpn server на r3

```
[root@server3 client]# systemctl status openvpn@server
● openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Application On server
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2021-07-04 11:18:59 EDT; 1h 56min ago
 Main PID: 1844 (openvpn)
   Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─1844 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf

Jul 04 11:18:59 server3 systemd[1]: Starting OpenVPN Robust And Highly Flexible Tunneling Application On server...
Jul 04 11:18:59 server3 systemd[1]: Started OpenVPN Robust And Highly Flexible Tunneling Application On server.
[root@server3 client]#
```

Создаём сертификаты для сервера и для клиента подписываем их у CA

```
[root@server3 client]# ls
ca.crt  client01.crt  client01.key  client01.ovpn  client01.tar.gz
[root@server3 client]# ls /etc/openvpn/server
ca.crt  dh.pem  server.crt  server.key
[root@server3 client]# ls
ca.crt  client01.crt  client01.key  client01.ovpn  client01.tar.gz
[root@server3 client]#
```

Копируем клиентскую часть на машину с которой буем подключаться

Настраиваем конфиги клиента

```
client01.ovpn      [----]  0 L:[  1+ 0   1/ 24] *(0   / 444b) 0099 0x063↔
client
dev tun
proto udp

remote 192.168.23.13 1194 # IP адрес сервера

ca ca.crt
cert client01.crt
key client01.key

cipher AES-256-CBC
auth SHA512
auth-nocache
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA25

resolv-retry infinite
compress lzo
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
```

Подключаемся с клиента к туннелю

`openvpn --config client01.ovpn`

```
[1] 2276
[root@server1 client]# Tue Jul  6 07:30:47 2021 OpenVPN 2.4.11 x86_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [
EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 21 2021
Tue Jul  6 07:30:47 2021 library versions: OpenSSL 1.0.2k-fips  26 Jan 2017, LZO 2.06
Tue Jul  6 07:30:47 2021 WARNING: No server certificate verification method has been enabled.  See http://openvpn.net/howto.html#mitm for
more info.
Tue Jul  6 07:30:47 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.23.13:1194
Tue Jul  6 07:30:47 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Tue Jul  6 07:30:47 2021 UDP link local: (not bound)
Tue Jul  6 07:30:47 2021 UDP link remote: [AF_INET]192.168.23.13:1194
Tue Jul  6 07:30:47 2021 TLS: Initial packet from [AF_INET]192.168.23.13:1194, sid=0fbbcfef 3ae526d7
Tue Jul  6 07:30:47 2021 VERIFY OK: depth=1, CN=Easy-RSA CA
Tue Jul  6 07:30:47 2021 VERIFY OK: depth=0, CN=server
Tue Jul  6 07:30:47 2021 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Tue Jul  6 07:30:47 2021 [server] Peer Connection Initiated with [AF_INET]192.168.23.13:1194
Tue Jul  6 07:30:48 2021 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Tue Jul  6 07:30:48 2021 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway local,dhcp-option DNS 8.8.8.8,route 10.8.1.1,topolog
y net30,ping 20,ping-restart 60,ifconfig 10.8.1.6 10.8.1.5,peer-id 0,cipher AES-256-GCM'
Tue Jul  6 07:30:48 2021 OPTIONS IMPORT: timers and/or timeouts modified
Tue Jul  6 07:30:48 2021 OPTIONS IMPORT: --ifconfig/up options modified
Tue Jul  6 07:30:48 2021 OPTIONS IMPORT: route options modified
Tue Jul  6 07:30:48 2021 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Tue Jul  6 07:30:48 2021 OPTIONS IMPORT: peer-id set
Tue Jul  6 07:30:48 2021 OPTIONS IMPORT: adjusting link_mtu to 1625
Tue Jul  6 07:30:48 2021 OPTIONS IMPORT: data channel crypto options modified
Tue Jul  6 07:30:48 2021 Data Channel: using negotiated cipher 'AES-256-GCM'
Tue Jul  6 07:30:48 2021 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Tue Jul  6 07:30:48 2021 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Tue Jul  6 07:30:48 2021 ROUTE_GATEWAY 192.168.2.2/255.255.255.0 IFACE=ens33 HWADDR=00:0c:29:68:56:9c
Tue Jul  6 07:30:48 2021 TUN/TAP device tun0 opened
Tue Jul  6 07:30:48 2021 TUN/TAP TX queue length set to 100
Tue Jul  6 07:30:48 2021 /sbin/ip link set dev tun0 up mtu 1500
Tue Jul  6 07:30:48 2021 /sbin/ip addr add dev tun0 local 10.8.1.6 peer 10.8.1.5
Tue Jul  6 07:30:48 2021 /sbin/ip route del 0.0.0.0/0
Tue Jul  6 07:30:48 2021 /sbin/ip route add 0.0.0.0/0 via 10.8.1.5
Tue Jul  6 07:30:48 2021 /sbin/ip route add 10.8.1.1/32 via 10.8.1.5
Tue Jul  6 07:30:48 2021 Initialization Sequence Completed
```

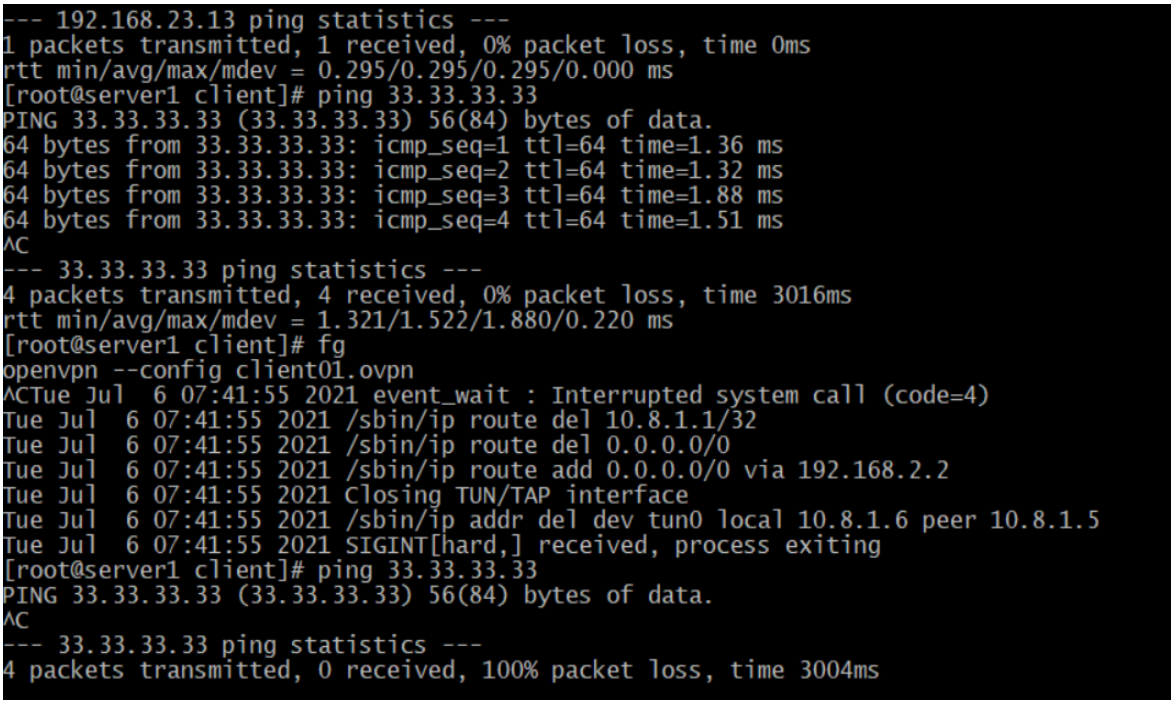
Проверяем пингуем адрес сервера vpn

```
--- 10.8.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 1.182/1.285/1.389/0.109 ms
[root@server1 client]# ping 10.8.1.1
PING 10.8.1.1 (10.8.1.1) 56(84) bytes of data.
64 bytes from 10.8.1.1: icmp_seq=1 ttl=64 time=1.29 ms
64 bytes from 10.8.1.1: icmp_seq=2 ttl=64 time=1.51 ms
64 bytes from 10.8.1.1: icmp_seq=3 ttl=64 time=1.35 ms
64 bytes from 10.8.1.1: icmp_seq=4 ttl=64 time=1.80 ms
^C
```

Работает

4. Убедиться, что server1 может пропинговать 33.33.33.33, когда VPN подключен, и не может этого сделать, когда VPN не подключен.

Проверяем пингуем 33.33.33.33 отключаем VPN и пробуем ещё раз



Работает.