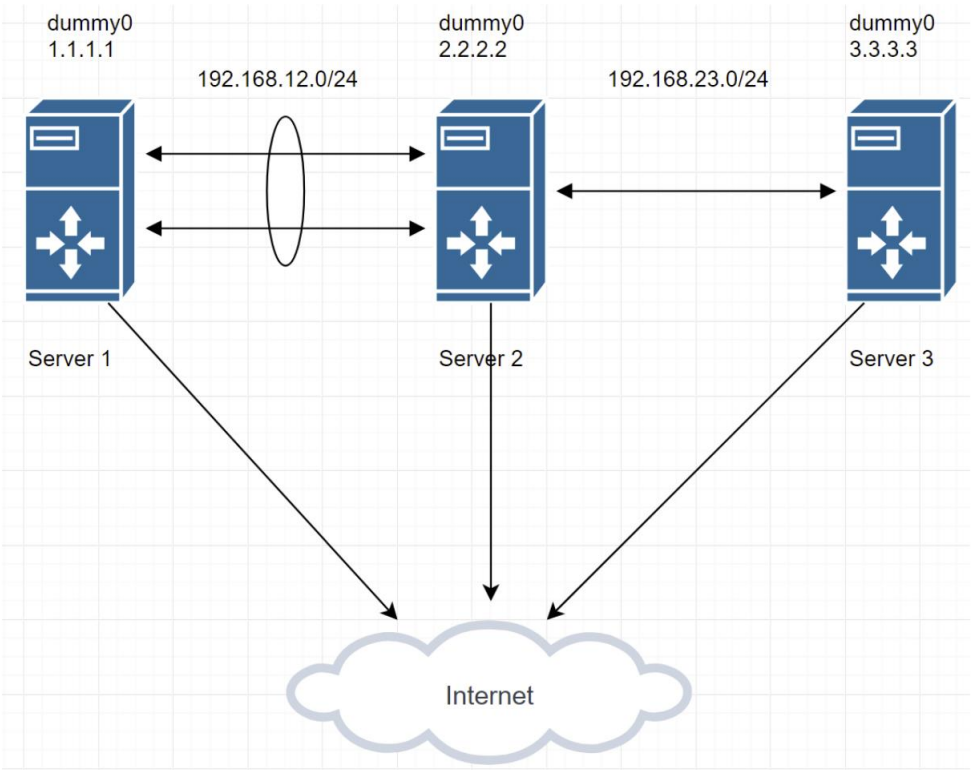
ЗАДАНИЕ №3

Топология:



1) На сервере server3 добавить еще один интерфейс — dummy с IP-адресом 33.33.33.33/32.
2) НЕ анонсировать этот интерфейс в OSPF.
3) Поднять openvpn-сервер на server3 и обеспечить возможность подключения клиента server1, используя сертификаты.
4) Убедиться, что server1 может пропинговать 33.33.33.33, когда VPN подключен, и не может этого сделать, когда VPN не подключен.

РЕШЕНИЕ:

1) echo "options dummy numdummies=2" > /etc/modprobe.d/dummy.conf
Dummy1 назначим IP 33.33.33.33

```
[root@server3 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noq
    link/loopback 00:00:00:00:00:00 brd 00:00:00:
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 15
    link/ether 00:15:5d:f5:e9:ed brd ff:ff:ff:ff:
    inet 172.21.201.34/28 brd 172.21.201.47 scope
       valid_lft forever preferred_lft forever
    inet6 fe80::b276:14d7:ece6:5801/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 15
    link/ether 00:15:5d:f5:e9:f3 brd ff:ff:ff:ff:
    inet 192.168.23.2/24 brd 192.168.23.255 scope
       valid_lft forever preferred_lft forever
    inet6 fe80::8b48:6a6e:7c94:19e3/64 scope link
       valid_lft forever preferred_lft forever
4: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500
    link/ether 7a:d2:50:6c:41:17 brd ff:ff:ff:ff:
    inet 3.3.3.3/32 brd 3.3.3.3 scope global dumm
       valid_lft forever preferred_lft forever
    inet6 fe80::78d2:50ff:fe6c:4117/64 scope link
       valid_lft forever preferred_lft forever
5: dummy1: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500
    link/ether f2:c4:c8:62:31:c6 brd ff:ff:ff:ff:
    inet 33.33.33.33/32 brd 33.33.33.33 scope glo
       valid_lft forever preferred_lft forever
    inet6 fe80::f0c4:c8ff:fe62:31c6/64 scope link
       valid_lft forever preferred_lft forever
```

2) Настройки ospf без изменений.

3)Подняты OpenVpn и в качестве CA easy-rsa3.

```
[root@server3 ~]# ls /etc/openvpn/easy-rsa/3/pki/
ca.crt           dh.pem     index.txt.attr      index.txt.old  private  reqs     safessl-easyrsa.cnf  serial.old
certs_by_serial  index.txt  index.txt.attr.old  issued         renewed  revoked  serial
[root@server3 ~]# systemctl status openvpn@server
● openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Application On server
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-07-08 01:33:56 MSK; 17min ago
 Main PID: 1746 (openvpn)
   Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─1746 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf

Jul 08 01:33:56 server3 systemd[1]: Starting OpenVPN Robust And Highly Flexible Tunneling Application On server...
Jul 08 01:33:56 server3 systemd[1]: Started OpenVPN Robust And Highly Flexible Tunneling Application On server.
[root@server3 ~]#
```

Конфиг сервера:

2. server3 | 8. server1

```
port 1194
proto udp
dev tun

# OpenVPN Server Certificate - CA, server key and certificate
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key

#DH key
dh /etc/openvpn/server/dh.pem

# Network Configuration - Internal network
# Redirect all Connection through OpenVPN Server
server 172.168.1.0 255.255.255.0
push "route 33.33.33.33 255.255.255.255"

#Enable multiple client to connect with same Certificate key
duplicate-cn

# TLS Security
cipher AES-256-CBC
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WIT
A256
auth SHA512
auth-nocache

# Other Configuration
keepalive 20 60
persist-key
persist-tun
comp-lzo yes
daemon
user nobody
group nobody

# OpenVPN Log
log-append /var/log/openvpn.log
verb 3
```

Конфиг клиента:

```
[root@server1 client]# ls /etc/openvpn/client/
ca.crt  client01.crt  client01.key  client01.ovpn
[root@server1 client]# cat /etc/openvpn/client/client01.ovpn
client
dev tun
proto udp

remote 192.168.23.2 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-WI
S-128-CBC-SHA256

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

Факт подключения к серверу:

```
[root@server1 client]# openvpn --config client01.ovpn
Thu Jul  8 01:53:13 2021 WARNING: file 'client01.key' is group or others a
Thu Jul  8 01:53:13 2021 OpenVPN 2.4.11 x86_64-redhat-linux-gnu [Fedora EP
INFO] [AEAD] built on Apr 21 2021
Thu Jul  8 01:53:13 2021 library versions: OpenSSL 1.0.2k-fips  26 Jan 201
Thu Jul  8 01:53:13 2021 WARNING: No server certificate verification metho
more info.
Thu Jul  8 01:53:13 2021 TCP/UDP: Preserving recently used remote address:
Thu Jul  8 01:53:13 2021 Socket Buffers: R=[212992->212992] S=[212992->212
Thu Jul  8 01:53:13 2021 UDP link local: (not bound)
Thu Jul  8 01:53:13 2021 UDP link remote: [AF_INET]192.168.23.2:1194
Thu Jul  8 01:53:13 2021 TLS: Initial packet from [AF_INET]192.168.23.2:11
Thu Jul  8 01:53:13 2021 VERIFY OK: depth=1, CN=Easy-RSA CA
Thu Jul  8 01:53:13 2021 VERIFY OK: depth=0, CN=server
Thu Jul  8 01:53:13 2021 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-
Thu Jul  8 01:53:13 2021 [server] Peer Connection Initiated with [AF_INET]
Thu Jul  8 01:53:14 2021 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Thu Jul  8 01:53:14 2021 PUSH: Received control message: 'PUSH_REPLY,route
ng 20,ping-restart 60,ifconfig 172.168.1.10 172.168.1.9,peer-id 1,cipher A
Thu Jul  8 01:53:14 2021 OPTIONS IMPORT: timers and/or timeouts modified
Thu Jul  8 01:53:14 2021 OPTIONS IMPORT: --ifconfig/up options modified
Thu Jul  8 01:53:14 2021 OPTIONS IMPORT: route options modified
Thu Jul  8 01:53:14 2021 OPTIONS IMPORT: peer-id set
Thu Jul  8 01:53:14 2021 OPTIONS IMPORT: adjusting link_mtu to 1625
Thu Jul  8 01:53:14 2021 OPTIONS IMPORT: data channel crypto options modif
Thu Jul  8 01:53:14 2021 Data Channel: using negotiated cipher 'AES-256-GC
Thu Jul  8 01:53:14 2021 Outgoing Data Channel: Cipher 'AES-256-GCM' initi
Thu Jul  8 01:53:14 2021 Incoming Data Channel: Cipher 'AES-256-GCM' initi
Thu Jul  8 01:53:14 2021 ROUTE_GATEWAY 172.21.201.33/255.255.255.240 IFACE
Thu Jul  8 01:53:14 2021 TUN/TAP device tun0 opened
Thu Jul  8 01:53:14 2021 TUN/TAP TX queue length set to 100
Thu Jul  8 01:53:14 2021 /sbin/ip link set dev tun0 up mtu 1500
Thu Jul  8 01:53:14 2021 /sbin/ip addr add dev tun0 local 172.168.1.10 pee
Thu Jul  8 01:53:14 2021 /sbin/ip route add 33.33.33.33/32 via 172.168.1.9
Thu Jul  8 01:53:14 2021 /sbin/ip route add 172.168.1.1/32 via 172.168.1.9
Thu Jul  8 01:53:14 2021 Initialization Sequence Completed
```

3)Пинг проходит только при активном VPN:

```
[root@server1 client]# ping 33.33.33.33
PING 33.33.33.33 (33.33.33.33) 56(84) bytes of data.
^C
--- 33.33.33.33 ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 11999ms

[root@server1 client]# openvpn --config client01.ovpn --daemon
[root@server1 client]# ping 33.33.33.33
PING 33.33.33.33 (33.33.33.33) 56(84) bytes of data.
64 bytes from 33.33.33.33: icmp_seq=1 ttl=64 time=0.628 ms
64 bytes from 33.33.33.33: icmp_seq=2 ttl=64 time=1.50 ms
64 bytes from 33.33.33.33: icmp_seq=3 ttl=64 time=1.83 ms
^C
--- 33.33.33.33 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.628/1.321/1.835/0.508 ms
[root@server1 client]# ip route get 33.33.33.33
33.33.33.33 via 172.168.1.5 dev tun0 src 172.168.1.6
    cache
[root@server1 client]#
```