Создадим второй dummy интерфейс.
Т.к модуль dummy у нас уже включен

```
[root@R3 ~]# cat /etc/modules-load.d/dummy.conf
dummy
[root@R3 ~]#
```

Добавим ещё один интерфейс отредактировав файл
vim /etc/modprobe.d/dummy.conf

R1 | R2 | R3

```
options dummy numdummies=2
~
~
~
~
~
~
~
```

Делаем ребут, видим что появился новый интерфейс

```
Using username "root".
Last login: Sat Aug 27 10:23:14 2022 from 192.168.0.214
[root@R3 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:e9:4a:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.203/24 brd 192.168.0.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee9:4a4e/64 scope link
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:e9:4a:58 brd ff:ff:ff:ff:ff:ff
    inet 192.168.23.2/24 brd 192.168.23.255 scope global noprefixroute ens34
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee9:4a58/64 scope link
       valid_lft forever preferred_lft forever
4: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether f6:7d:fd:fe:a7:8f brd ff:ff:ff:ff:ff:ff
    inet 3.3.3.3/32 brd 3.3.3.3 scope global dummy0
       valid_lft forever preferred_lft forever
    inet6 fe80::f47d:fdff:fefe:a78f/64 scope link
       valid_lft forever preferred_lft forever
5: dummy1: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 0a:cb:08:30:35:6e brd ff:ff:ff:ff:ff:ff
```

Настроим его по аналогии с dummy0

vim /etc/sysconfig/network-scripts/ifcfg-dummy1

R1 | R2 | **R3**

```
DEVICE=dummy1
TYPE=dummy
IPADDR=33.33.33.33
PREFIX=32
ONBOOT=yes
~
```

Установим необходимые утилиты для установки CA и VPN

R3

sudo yum install epel-release -y

yum install openvpn easy-rsa -y

Скопируем файлы из easy-rsa в директорию openvpn.
Создадим файл vars с переменными

```
[root@R3 share]# cp -r /usr/share/easy-rsa/ /etc/openvpn/
[root@R3 share]# cd /etc/openvpn/easy-rsa/
[root@R3 easy-rsa]# ll
total 0
lrwxrwxrwx. 1 root root  5 Aug 27 11:32 3 -> 3.0.8
lrwxrwxrwx. 1 root root  5 Aug 27 11:32 3.0 -> 3.0.8
drwxr-xr-x. 3 root root 66 Aug 27 11:32 3.0.8
[root@R3 easy-rsa]# cd 3
[root@R3 3]# vim vars
[root@R3 3]# chmod +x vars
[root@R3 3]# vim vars
[root@R3 3]#
```

R1 | R2 | R3

```
set_var EASYRSA "$PWD"
set_var EASYRSA_PKI "$EASYRSA/pki"
set_var EASYRSA_DN "cn_only"
set_var EASYRSA_REQ_COUNTRY "RU"
set_var EASYRSA_REQ_PROVINCE "Moscow"
set_var EASYRSA_REQ_CITY "Moscow"
set_var EASYRSA_REQ_ORG "EXAMPLE CERTIFICATE AUTHORITY"
set_var EASYRSA_REQ_EMAIL "openvpn@example.com"
set_var EASYRSA_REQ_OU "Example.com EASY CA"
set_var EASYRSA_KEY_SIZE 2048
set_var EASYRSA_ALGO rsa
set_var EASYRSA_CA_EXPIRE 7500
set_var EASYRSA_CERT_EXPIRE 365
set_var EASYRSA_NS_SUPPORT "no"
set_var EASYRSA_NS_COMMENT "EXAMPLE CERTIFICATE AUTHORITY"
set_var EASYRSA_EXT_DIR "$EASYRSA/x509-types"
set_var EASYRSA_SSL_CONF "$EASYRSA/openssl-1.0.cnf"
set_var EASYRSA_DIGEST "sha256"
~
```

Инициализируем CA и создаем сертификат для CA

```
[root@R3 3]# ./easyrsa init-pki

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/3/pki


[root@R3 3]# ./easyrsa build-ca nopass

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
Generating RSA private key, 2048 bit long modulus
.....................................................................................+++
.........................+++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/3/pki/ca.crt


[root@R3 3]#
```

Создаем ключ для сервера

```
[root@R3 3]# ./easyrsa gen-req server nopass

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
Generating a 2048 bit RSA private key
.....................................................................................................+++
.........................+++
writing new private key to '/etc/openvpn/easy-rsa/3/pki/easy-rsa-2396.6WfaWL/tmp.7tLZJk'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [server]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/3/pki/reqs/server.req
key: /etc/openvpn/easy-rsa/3/pki/private/server.key
```

Подписываем серверный ключ нашим удостоверяющим центром, тем самым получаем сертификат для сервера.

```
[root@R3 3]# ./easyrsa sign-req server server

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 365 days:

subject=
    commonName                = server


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/3/pki/easy-rsa-2423.I4aqlE/tmp.HVhgCf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Aug 27 09:07:55 2023 GMT (365 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/3/pki/issued/server.crt
```

Создаем ключ для vpn клиента

```
[root@R3 3]# ./easyrsa gen-req client01 nopass

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
Generating a 2048 bit RSA private key
.................................................+++
..............+++
writing new private key to '/etc/openvpn/easy-rsa/3/pki/easy-rsa-2497.OBNoGj/tmp.WtBCvO'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [client01]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/3/pki/reqs/client01.req
key: /etc/openvpn/easy-rsa/3/pki/private/client01.key
```

Подписываем ключ нашим удостоверяющим центром, тем самым получаем сертификат клиента

```
[root@R3 3]# ./easyrsa sign-req client client01

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 365 days:

subject=
    commonName                = client01


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/3/pki/easy-rsa-2524.N784wv/tmp.VygNCL
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'client01'
Certificate is to be certified until Aug 27 09:11:37 2023 GMT (365 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/3/pki/issued/client01.crt
```

Создаем Диффи Хеллмана ключ

```
[root@R3 3]# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 1.0.2k-fips  26 Jan 2017
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....................................................................
.+.....................................+.....................................
..+.................+.+.....................................................+..
.........................+.....................................................
.....................................................................+.............
```

Сертификат удостоверяющего центра, ключ Диффи Хеллмана, сертификат и ключ сервера - копируем в папку vpn сервера

Сертификат удостоверяющего центра, сертификат и ключ клиента - копируем в папку vpn клиента

```
[root@R3 3]# cp pki/ca.crt /etc/openvpn/server/
[root@R3 3]# cp pki/issued/server.crt /etc/openvpn/server/
[root@R3 3]# cp pki/private/server.key /etc/openvpn/server/
[root@R3 3]# cp pki/ca.crt /etc/openvpn/client/
[root@R3 3]# cp pki/issued/client01.crt /etc/openvpn/client/
[root@R3 3]# cp pki/private/client01.key /etc/openvpn/client/
[root@R3 3]# cp pki/dh.pem /etc/openvpn/server/
```

Отредактируем файл конфигурации нашего vpn сервера

vim /etc/openvpn/server.conf

```
# OpenVPN Port, Protocol and the Tun
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 10.8.1.0 255.255.255.0
push "redirect-gateway def1"
# Using the DNS from https://dns.watch
push "dhcp-option DNS 8.8.8.8"
#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-WITH-AES-256-CBC-SHA256:TLS-DHERSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
auth SHA512
auth-nocache
# Other Configuration
keepalive 200 600
persist-key
persist-tun
comp-lzo yes
daemon
user nobody
group nobody
# OpenVPN Log
log-append /var/log/openvpn.log
verb 3
~
```

Разрешим forwarding

vim /etc/sysctl.conf

```
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward = 1
```

Применим изменения

```
sysctl -p
```

Разрешаем сервис openvpn в файрволле.
Добавляем туннельный интерфейс в доверенную зону
Применяем правила.

```
[root@R3 3]# firewall-cmd --permanent --add-service=openvpn
success
[root@R3 3]# firewall-cmd --permanent --zone=trusted --add-interface=tun0
success
[root@R3 3]# firewall-cmd --reload
success
[root@R3 3]#
```

Запускаем сервер, добавляем в автозагрузку

```
[root@R3 3]# systemctl start openvpn@server
[root@R3 3]# systemctl enable openvpn@server
Created symlink from /etc/systemd/system/multi-user.target.wants/openvpn@server.service to /usr/lib/systemd/system/openvpn@.service.
[root@R3 3]# 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 Sat 2022-08-27 12:46:04 MSK; 14s ago
 Main PID: 2655 (openvpn)
   Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─2655 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf
```

Проверим появился ли у нас порт 1194

```
[root@R3 3]# ss -tuna
Netid  State      Recv-Q Send-Q                                                Local Address:Port
udp    UNCONN     0      0                                                        3.3.3.3:53
udp    UNCONN     0      0                                                    127.0.0.1:53
udp    UNCONN     0      0                                                          *:111
udp    UNCONN     0      0                                                          *:1194
udp    UNCONN     0      0                                                          *:20048
udp    UNCONN     0      0                                                          *:53890
udp    UNCONN     0      0                                                    127.0.0.1:659
udp    UNCONN     0      0                                                          *:54095
```

Создадим конфиг файл для клиента

cd /etc/openvpn/client

vim 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-WITH-AES-256-CBC-SHA256:TLS-DHERSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
resolv-retry infinite
compress lzo
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
~
```

Упаковываем в архив всю папку клиента, в которой хранится ключ клиента, сертификат, сертификат CA, и конфиг клиента

```
[root@R3 openvpn]# tar -czvf client01.tar.gz client/*
client/ca.crt
client/client01.crt
client/client01.key
client/client01.ovpn
[root@R3 openvpn]# ll
total 12
drwxr-x---. 2 root openvpn   81 Aug 27 12:57 client
-rw-r--r--. 1 root root    4998 Aug 27 13:02 client01.tar.gz
drwxr-xr-x. 3 root root      39 Aug 27 11:32 easy-rsa
drwxr-x---. 2 root openvpn   70 Aug 27 12:22 server
-rw-r--r--. 1 root root     956 Aug 27 12:32 server.conf
[root@R3 openvpn]#
```

Установим на R1 клиентскую часть openvpn

```
[root@R1 ~]# yum install openvpn network-manager-openvpn
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.docker.ru
 * extras: mirror.awanti.com
 * updates: mirror.awanti.com
No package openvpn available.
No package network-manager-openvpn available.
Error: Nothing to do
[root@R1 ~]#
```

Получаем сообщение no package available

Оказывается openvpn отсутствует в стандартном репозитории и нам требуется epel репозиторий
Установим epel-release

yum install epel-release

```
Downloading packages:
epel-release-7-11.noarch.rpm
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : epel-release-7-11.noarch
  Verifying  : epel-release-7-11.noarch

Installed:
  epel-release.noarch 0:7-11

Complete!
```

Пробуем ещё раз

yum install openvpn network-manager-openvpn

```
[root@R1 ~]# yum install openvpn network-manager-openvpn
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink
 * base: mirror.docker.ru
 * epel: ftp.lysator.liu.se
 * extras: mirror.awanti.com
 * updates: mirror.awanti.com
epel
(1/3): epel/x86_64/group_gz
(2/3): epel/x86_64/updateinfo
(3/3): epel/x86_64/primary_db
No package network-manager-openvpn available.
Resolving Dependencies
--> Running transaction check
---> Package openvpn.x86_64 0:2.4.12-1.el7 will be installed
--> Processing Dependency: libpkcs11-helper.so.1()(64bit) for package: openvpn-2.4.12-1.el7.x86_64
--> Running transaction check
---> Package pkcs11-helper.x86_64 0:1.11-3.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                    Arch                    Version
================================================================================
Installing:
 openvpn                    x86_64                  2.4.12-1.el7
Installing for dependencies:
 pkcs11-helper              x86_64                  1.11-3.el7
```

Успешно.

Копируем архив на машину R1

```
[root@R1 ~]# scp 192.168.23.2:/etc/openvpn/client01.tar.gz .
The authenticity of host '192.168.23.2 (192.168.23.2)' can't be established.
ECDSA key fingerprint is SHA256:4DIzIiEHmNIZHAUZOZ/2dcI5yi03w458v2wUGj0KG7A.
ECDSA key fingerprint is MD5:af:8f:d0:f6:7e:26:b4:c9:7b:f5:d3:a9:92:e4:7b:34.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.23.2' (ECDSA) to the list of known hosts.
root@192.168.23.2's password:
client01.tar.gz
[root@R1 ~]# ll
total 28
-rw-------. 1 root root  1391 Aug 16 21:42 anaconda-ks.cfg
-rw-r--r--. 1 root root  4998 Aug 27 13:20 client01.tar.gz
-rw-r--r--. 1 root root 15484 Aug 20 14:40 frr-stable-repo-1-0.el7.noarch.rpm
[root@R1 ~]#
```

Разархивируем нашу папку с файлами клиента

tar -xzvf client01.tar.gz

На R1 также разрешим в файрволле openvpn

```
[root@R1 client]# firewall-cmd --permanent --add-service=openvpn
success
[root@R1 client]# firewall-cmd --permanent --zone=trusted --add-interface=tun0
success
[root@R1 client]# firewall-cmd --reload
success
[root@R1 client]#
[root@R1 client]#
```

Запускаем openvpn

openvpn --config client01.ovpn &

```
[root@R1 client]# openvpn --config client01.ovpn &
[1] 3374
[root@R1 client]# Sat Aug 27 13:26:40 2022 OpenVPN 2.4.12 x86_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar 17 2022
Sat Aug 27 13:26:40 2022 library versions: OpenSSL 1.0.2k-fips  26 Jan 2017, LZO 2.06
Sat Aug 27 13:26:40 2022 WARNING: No server certificate verification method has been enabled.  See http://openvpn.net/howto.html#mitm for more info.
Sat Aug 27 13:26:40 2022 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.23.2:1194
Sat Aug 27 13:26:40 2022 Socket Buffers: R=[212992->212992] S=[212992->212992]
Sat Aug 27 13:26:40 2022 UDP link local: (not bound)
Sat Aug 27 13:26:40 2022 UDP link remote: [AF_INET]192.168.23.2:1194
Sat Aug 27 13:26:40 2022 TLS: Initial packet from [AF_INET]192.168.23.2:1194, sid=11b0446d 28992927
Sat Aug 27 13:26:40 2022 VERIFY OK: depth=1, CN=Easy-RSA CA
Sat Aug 27 13:26:40 2022 VERIFY OK: depth=0, CN=server
Sat Aug 27 13:26:40 2022 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Sat Aug 27 13:26:40 2022 [server] Peer Connection Initiated with [AF_INET]192.168.23.2:1194
Sat Aug 27 13:26:41 2022 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Sat Aug 27 13:26:41 2022 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1,dhcp-option DNS 8.8.8.8,route 10.8.1.1,topology net30,ping 200,ping-restart 600,ifconfig 10.8.1.10 10.8.1.9,peer-id 1
,cipher AES-256-GCM'
Sat Aug 27 13:26:41 2022 OPTIONS IMPORT: timers and/or timeouts modified
Sat Aug 27 13:26:41 2022 OPTIONS IMPORT: --ifconfig/up options modified
Sat Aug 27 13:26:41 2022 OPTIONS IMPORT: route options modified
Sat Aug 27 13:26:41 2022 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Sat Aug 27 13:26:41 2022 OPTIONS IMPORT: peer-id set
Sat Aug 27 13:26:41 2022 OPTIONS IMPORT: adjusting link_mtu to 1625
Sat Aug 27 13:26:41 2022 OPTIONS IMPORT: data channel crypto options modified
Sat Aug 27 13:26:41 2022 Data Channel: using negotiated cipher 'AES-256-GCM'
Sat Aug 27 13:26:41 2022 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Sat Aug 27 13:26:41 2022 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Sat Aug 27 13:26:41 2022 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=ens33 HWADDR=00:0c:29:fb:63:98
Sat Aug 27 13:26:41 2022 TUN/TAP device tun0 opened
Sat Aug 27 13:26:41 2022 TUN/TAP TX queue length set to 100
Sat Aug 27 13:26:41 2022 /sbin/ip link set dev tun0 up mtu 1500
Sat Aug 27 13:26:41 2022 /sbin/ip addr add dev tun0 local 10.8.1.10 peer 10.8.1.9
Sat Aug 27 13:26:41 2022 /sbin/ip route add 192.168.23.2/32 via 192.168.0.1
Sat Aug 27 13:26:41 2022 /sbin/ip route add 0.0.0.0/1 via 10.8.1.9
Sat Aug 27 13:26:41 2022 /sbin/ip route add 128.0.0.0/1 via 10.8.1.9
Sat Aug 27 13:26:41 2022 /sbin/ip route add 10.8.1.1/32 via 10.8.1.9
Sat Aug 27 13:26:41 2022 Initialization Sequence Completed
```

Пробуем пинговать 33.33.33.33

```
[root@R1 ~]# ping 33.33.33.33
PING 33.33.33.33 (33.33.33.33) 56(84) bytes of data.
```

Пинг не идёт.

Смотрим tcpdump туннельного интерфейса

```
[root@R1 ~]# tcpdump -nni tun0
\tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
13:08:15.264610 IP 10.8.1.6 > 33.33.33.33: ICMP echo request, id 5286, seq 27, length 64
13:08:16.269699 IP 10.8.1.6 > 33.33.33.33: ICMP echo request, id 5286, seq 28, length 64
13:08:17.276653 IP 10.8.1.6 > 33.33.33.33: ICMP echo request, id 5286, seq 29, length 64
13:08:18.280418 IP 10.8.1.6 > 33.33.33.33: ICMP echo request, id 5286, seq 30, length 64
13:08:19.284307 IP 10.8.1.6 > 33.33.33.33: ICMP echo request, id 5286, seq 31, length 64
13:08:20.285551 IP 10.8.1.6 > 33.33.33.33: ICMP echo request, id 5286, seq 32, length 64
^C
```

На тунельном интерфейсе пакетики отправляются.
Посмотрим интерфейс team0, из которого в сторону 192.168.23.2 по задумке должны идти udp пакеты.

```
[root@R1 ~]# tcpdump -nni team0 udp or icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on team0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
[root@R1 ~]#
```

Никаких пакетов нету. Хотя откуда то они отправляться точно должны. Смотрим интерфейс ens33, который смотрит во внешнюю сеть.

```
13:01:44.429299 IP6 fe80::e6c3:2aff:felb:4e20.51295 > ff02::c.1900: UDP, length 432
13:01:44.878082 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:45.882610 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:46.889038 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:47.890380 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:48.868403 IP 192.168.0.1.57166 > 192.168.0.202.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
13:01:48.879428 IP 192.168.0.1.36895 > 192.168.0.202.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
13:01:48.894049 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:48.936273 IP 192.168.0.1.43257 > 192.168.0.203.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
13:01:48.947310 IP 192.168.0.1.53834 > 192.168.0.203.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
13:01:48.970230 IP 192.168.0.1.51494 > 192.168.0.201.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
13:01:48.981209 IP 192.168.0.1.45072 > 192.168.0.201.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
13:01:49.897282 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:50.902304 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:51.907366 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:52.913299 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:53.917366 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
13:01:54.920000 IP 192.168.0.201.37282 > 192.168.23.2.1194: UDP, length 109
```

Видим что с нашего внешнего интерфейса отправляются udp пакеты на адрес 192.168.23.2. Мы этот адрес прописывали в конфиге клиента, как адрес openvpn сервера. Но пакеты эти приходят в мой домашний роутер, который, естественно ничего не знает о сети где находится 192.168.23.2. Роутер просто отбрасывает эти пакеты.

Попробуем поправить конфиг клиента и укажем адрес сервера 192.168.0.203. Это интерфейс R3 который смотрит в интернет.

R1

vim client01.ovpn

```
client
dev tun
proto udp
remote 192.168.0.203 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-DHERSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
resolv-retry infinite
compress lzo
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
```

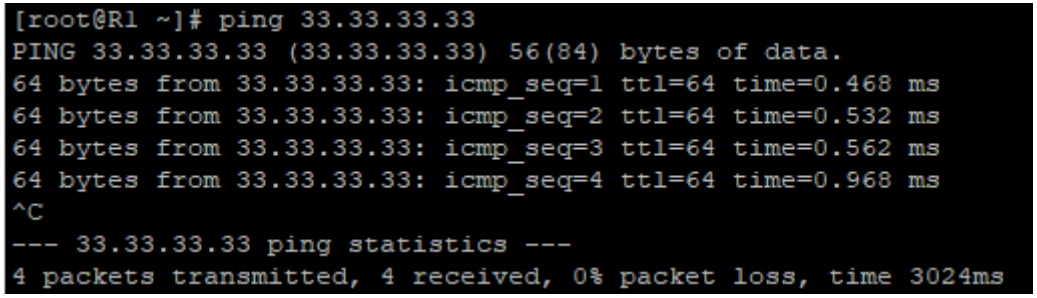
openvpn --config client01.ovpn

Попробуем пропинговать туннельный интерфейс сервера

```
[root@R1 ~]# 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=0.502 ms
64 bytes from 10.8.1.1: icmp_seq=2 ttl=64 time=0.709 ms
64 bytes from 10.8.1.1: icmp_seq=3 ttl=64 time=0.454 ms
^C
```

Успешно

Пробуем пинг 33.33.33.33


[root@R1 ~]# 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=0.468 ms
64 bytes from 33.33.33.33: icmp_seq=2 ttl=64 time=0.532 ms
64 bytes from 33.33.33.33: icmp_seq=3 ttl=64 time=0.562 ms
64 bytes from 33.33.33.33: icmp_seq=4 ttl=64 time=0.968 ms
^C
--- 33.33.33.33 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3024ms

Успешно