

## Выполнил студент группы 2345 Романенко Кирилл

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

Создал dummy3

```
ip link add dummy3 type dummy
```

Присвоил ip

```
ip addr add 33.33.33.33/32 dev dummy3
```

Включил dummy

```
ip link set up dev dummy3
```

```
5: dummy3: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether be:01:b8:a3:7e:36 brd ff:ff:ff:ff:ff:ff
    inet 33.33.33.33/32 scope global dummy3
        valid_lft forever preferred_lft forever
```

Хотел настроить автоматическое поднятие модуля при запуске машины, но в ДЗ №2 уже сделал это:

```
vim /etc/modules
```

```
dummy
```

Настроил dummy3

```
vim /etc/sysconfig/network-scripts/ifcfg-dummy3
```

```
DEVICE=dummy3
ONBOOT=yes
IPADDR=33.33.33.33
PREFIX=32
NETMASK=255.255.255.255
MACADDR=02:22:22:ff:ff:ff
TYPE=dummy
NM_CONTROLLED=no
```

Перезагрузил dummy

```
ifdown dummy3
```

```
ifup dummy3
```

```
5: dummy3: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 02:22:22:ff:ff:ff brd ff:ff:ff:ff:ff:ff
    inet 33.33.33.33/32 brd 33.33.33.33 scope global dummy3
        valid_lft forever preferred_lft forever
    inet6 fe80::22:22ff:feff:ffff/64 scope link
        valid_lft forever preferred_lft forever
```

2. НЕ анонсировать этот интерфейс в OSPF.

Проверил сети, которые анонсирую

```
sh running-config
```

```

server3# sh routing-config
% Unknown command: sh routing-config
server3# sh routing-config
% Unknown command: sh routing-config
server3# sh running-config
Building configuration...

Current configuration:
!
frr version 8.3
frr defaults traditional
hostname server3
log syslog informational
no ip forwarding
no ipv6 forwarding
!
router ospf
 network 3.3.3.3/32 area 0
 network 192.168.23.0/24 area 0
exit
!
end

```

Сети 33.33.33.33/32 среди таких нет

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

## SERVER3

### 1. Создал удостоверяющий центр (CA)

Добавил epel-репозиторий  
yum install epel-release -y

Установил OpenVPN 2.4 и easy-rsa3  
yum install openvpn easy-rsa -y

Скопировал стандартную директорию для easy-rsa в директорию с OpenVPN:

```

cd /etc/openvpn/
cp -r /usr/share/easy-rsa /etc/openvpn/
cd /etc/openvpn/easy-rsa/3

```

||

```

[root@server3 ~]# cd /etc/openvpn/
[root@server3 openvpn]# cp -r /usr/share/easy-rsa /etc/openvpn/
[root@server3 openvpn]# cd /etc/openvpn/easy-rsa/3
[root@server3 3]# ll
итого 84
-rwxr-xr-x. 1 root root 76946 апр 29 17:44 easyrsa
-rw-r--r--. 1 root root  4616 апр 29 17:44 openssl-easyrsa.cnf
drwxr-xr-x. 2 root root   122 апр 29 17:44 x509-types

```

Создал файл vars с настройками для выдачи сертификатов:  
vim vars

```
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"
```

Сделал vars исполняемым файлом:  
chmod +x vars

Далее, используя файл с переменными, мы можем построить свою собственную инфраструктуру PKI. Ключ noppass генерирует приватные ключи, которые не требуют пароля при обращении с ними. Это хорошая идея для тестирования настроек, но лучше так не делать в реальных имплементациях.

## 2. Создал удостоверяющий центр

Создал удостоверяющий центр  
./easyrsa init-pki

Создал сертификат удостоверяющего центра  
./easyrsa build-ca noppass

```
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
```

Создал ключи для сервера  
./easyrsa gen-req server noppass

Подписал сертификат сервера у удостоверяющего центра:  
./easyrsa sign-req server server

Проверил валидность выписанного сертификата:  
openssl verify -CAfile pki/ca.crt pki/issued/server.crt

```
pki/issued/server.crt: OK
```

## 3. Создал ключ для клиента

Выписал сертификат для клиента

```
./easysrsa gen-req client01 nopass
```

Подписал выписанный сертификат у CA:

```
./easysrsa sign-req client client01
```

Проверил валидность сертификата

```
openssl verify -CAfile pki/ca.crt pki/issued/client01.crt
```

```
pki/issued/client01.crt: OK
```

#### 4. Создал Diffie-Hellman-ключ:

```
./easysrsa gen-dh
```

По желанию можно создать Certificate Revoking List (CRL) для отзыва сертификатов, но для теста этого не требуется.

Скопировал выписанные сертификаты в папку /etc/openvpn/server и /etc/openvpn/client

Посмотрел, где я нахожусь

```
pwd
```

Создал необходимые файлы серверной и клиентской части

```
cp pki/ca.crt /etc/openvpn/server/
```

```
cp pki/issued/server.crt /etc/openvpn/server/
```

```
cp pki/private/server.key /etc/openvpn/server/
```

```
cp pki/ca.crt /etc/openvpn/client/
```

```
cp pki/issued/client01.crt /etc/openvpn/client/
```

```
cp pki/private/client01.key /etc/openvpn/client/
```

```
cp pki/dh.pem /etc/openvpn/server/
```

Создал конфиг для сервера при помощи файла /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      #Из какой подсети выдавать ip
push "redirect-gateway def1"    #Маршрут такой, что весь трафик идет через
тоннель
# Using the DNS from https://dns.watch
push "dhcp-option DNS 8.8.8.8"  #DNS гугла
#Enable multiple client to connect with same Certificate key
duplicate-cn
# TLS Security
cipher AES-256-CBC
tls-version-min 1.2
```

```

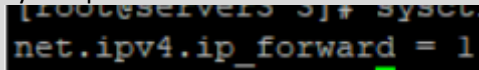
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-
SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
auth SHA512
auth-nocache
# Other Configuration
keepalive 200 600      #Поставил значения 200 600, чтобы соединение не отваливалось,
пока я туплю)))
persist-key
persist-tun
comp-lzo yes
daemon
user nobody
group nobody
# OpenVPN Log
log-append /var/log/openvpn.log      #Лог-файл
verb 3                               #Глубина логирования

```

Включил форвардинг

```
echo 'net.ipv4.ip_forward = 1' >> /etc/sysctl.conf
```

```
sysctl -p
```



Разрешил OpenVPN в iptables

Разрешил пересылку

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Разрешил подключаться к openvpn-серверу с любой стороны

```
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
```

Разрешил всем openvpn-клиентам соединение с интернетом для Статического ip

<https://www.linux.org.ru/forum/admin/7810894>

Также есть такой вариант: <https://russianpenguin.ru/2016/01/27/openvpn-настройка-на-собственном-сервере-ча-4/>

Если на интернет интерфейсе динамический ip

```
iptables -A FORWARD -i tun -o enp0s3 -j ACCEPT
```

```
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Статический ip

```
iptables -A FORWARD -i tun -o enp0s3 -j ACCEPT
```

```
iptables -t nat -A POSTROUTING -o enp0s3 -j SNAT --to-source 192.168.1.82
```

Настраиваю политику безопасности

```
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Запустил сервис, проверяем состояние OpenVPN-юнита и наличие сокета на UDP 1194:

```
systemctl start openvpn@server
```

```
systemctl enable openvpn@server
```

```
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 Пн 2022-08-29 18:55:11 MSK; 30s ago
 Main PID: 3232 (openvpn)
   Status: "Initialization Sequence Completed"
    CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
            └─3232 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf

авг 29 18:55:11 server3 systemd[1]: Starting OpenVPN Robust And Highly Flexible Tunneling Applicati...r...
авг 29 18:55:11 server3 systemd[1]: Started OpenVPN Robust And Highly Flexible Tunneling Applicatio...ver.
Hint: Some lines were ellipsized, use -l to show in full.

```

## 5. Создал конфиг клиента и указываем там IP-адрес VPN-сервера:

```

cd /etc/openvpn/client
vim client01.ovpn

```

```

client
dev tun
proto udp
remote 192.168.1.82 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-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
resolv-retry infinite
compress lz4
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3

```

Упаковал сертификаты клиента, сертификат CA и конфиг клиента в архив

```

cd /etc/openvpn/
tar -czvf client01.tar.gz client/*

```

```

client/ca.crt
client/client01.crt
client/client01.key
client/client01.ovpn

```

### SERVER 1

Добавил epel-репозиторий

```

yum install epel-release -y

```

Скачал архив на машину клиента и распаковываем. Кроме этого, скачиваем пакеты для использования OpenVPN-клиента:

```

yum install openvpn network-manager-openvpn -y

```

Скачал файл конфигурации в текущую директорию

```

scp root@192.168.1.82:/etc/openvpn/client01.tar.gz .

```

Разархивировал файл и подключился к серверу

```
tar -xzf client01.tar.gz
```

Перешел в папку, где хранятся ключи и запустил OpenVPN-клиента

```
cd client
```

```
openvpn --config client01.ovpn
```

```
Mon Aug 29 20:02:33 2022 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=enp0s3 HWADDR=
Mon Aug 29 20:02:33 2022 TUN/TAP device tun0 opened
Mon Aug 29 20:02:33 2022 TUN/TAP TX queue length set to 100
Mon Aug 29 20:02:33 2022 /sbin/ip link set dev tun0 up mtu 1500
Mon Aug 29 20:02:33 2022 /sbin/ip addr add dev tun0 local 10.8.1.6 peer 10.8.1.5
Mon Aug 29 20:02:33 2022 /sbin/ip route add 192.168.1.82/32 dev enp0s3
Mon Aug 29 20:02:33 2022 /sbin/ip route add 0.0.0.0/1 via 10.8.1.5
Mon Aug 29 20:02:33 2022 /sbin/ip route add 128.0.0.0/1 via 10.8.1.5
Mon Aug 29 20:02:33 2022 /sbin/ip route add 10.8.1.1/32 via 10.8.1.5
Mon Aug 29 20:02:33 2022 Initialization Sequence Completed
```