Лабораторная работа № 15

Тема: Сетевые сервисы на Linux. PKI и OpenVPN.

Цель работы: Изучить основы настройки и использования виртуальной частной сети (VPN) с использованием инфраструктуры открытых ключей (PKI) на операционной системе Linux.

Необходимое оборудование и программное обеспечение: Виртуальные машины под управлением Linux (CentOS, Ubuntu или др.).

Пример настройки серверов.

Тестовый стенд состоит и трех виртуальных машин на Centos 7 и Ubuntu 22.04 desktop.

R1: (Centos 7)

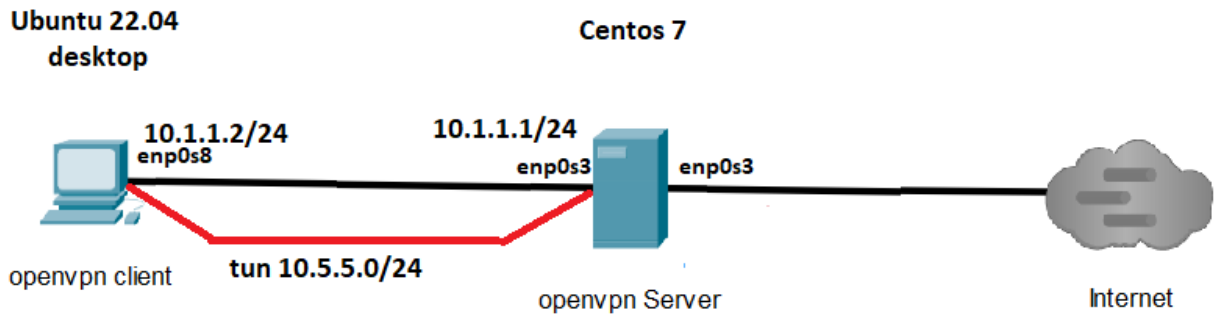
Nic1 – NAT (что бы был доступ в Интернет)

Nic2 – внутренняя сеть (lan1) 10.1.1.1/24

R2: (Ubuntu 22.04 desktop)

Nic1 – NAT (что бы был доступ в Интернет)

Nic2 – внутренняя сеть (lan1) 10.1.1.2/24



На втором хосте нужно установить пакеты:

sudo apt install openvpn network-manager-openvpn -y

sudo apt install nano

sudo apt install mtr

и пр.

Затем интерфейс Nic1 отключить, оставить только Lan1 (внутренняя сеть).

Сначала настроим сетевые интерфейсы:

Centos 7:

```
[root@r1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:0b:5e:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.158/24 brd 192.168.1.255 scope global noprefixroute dynamic e
np0s3
       valid_lft 85649sec preferred_lft 85649sec
    inet6 fe80::eda2:be1d:1730:52c7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:a8:9e:9d brd ff:ff:ff:ff:ff:ff
[root@r1 ~]#
```

Создание конф. файлов интерфейсов
nano /etc/sysconfig/network-scripts/ifcfg-enp0s8

DEVICE=enp0s8
BOOTPROTO=static
IPADDR=10.1.1.1
NETMASK=255.255.255.0
ONBOOT=yes
NM_CONTROLLED=yes

```
  GNU nano 2.3.1          Файл: /etc/sysconfig/network-scripts/ifcfg-enp0s8

DEVICE=enp0s8
BOOTPROTO=static
IPADDR=10.1.1.1
NETMASK=255.255.255.0
ONBOOT=yes
NM_CONTROLLED=yes
```

Перезапускаем сетевую службу и проверяем:

```
[root@r1 ~]# systemctl restart NetworkManager
[root@r1 ~]# ip a s enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
group default qlen 1000
    link/ether 08:00:27:a8:9e:9d brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.1/24 brd 10.1.1.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea8:9e9d/64 scope link
       valid_lft forever preferred_lft forever
[root@r1 ~]#
```

Ubuntu 22.04:

```
user@r2:~$ sudo nano /etc/netplan/01-network-manager-all.yaml
```

```
  GNU nano 6.2          /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s8:
      addresses:
        - 10.1.1.2/24
      gateway4: 10.1.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

```
user@r2:~$ sudo netplan apply

** (generate:2385): WARNING **: 18:49:25.360: `gateway4` has been deprecated, us
e default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:2383): WARNING **: 18:49:26.936: `gateway4` has been deprecated, use
 default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:2383): WARNING **: 18:49:27.819: `gateway4` has been deprecated, use
 default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:2383): WARNING **: 18:49:27.819: `gateway4` has been deprecated, use
 default routes instead.
See the 'Default routes' section of the documentation for more details.
```

```
user@r2:~$ ip a s enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:56:57:6e brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.2/24 brd 10.1.1.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe56:576e/64 scope link
       valid_lft forever preferred_lft forever
user@r2:~$
```

Проверяем связь между хостами:

```
user@r2:~/client$ ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=2.50 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=1.75 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=1.73 ms
^C
```

Выхода в интернет на 2-м хосте нет:

```
user@r2:~/client$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

Настройка OpenVPN

Сначала обновляем операционную систему и добавляем epel-репозиторий.

epel-release - это RPM-пакет, который добавляет репозиторий EPEL (Extra Packages for Enterprise Linux) в вашу систему CentOS или RHEL.:

```
[root@r1 ~]# yum install epel-release -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.hoster.kz
 * extras: mirror.hoster.kz
 * updates: mirror.hoster.kz
```

Устанавливаем OpenVPN и easy-rsa (или OpenSSL):

```
[root@r1 ~]# yum install openvpn easy-rsa -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.hoster.kz
 * epel: mirror2.totbb.net
```

Проверим директорию /etc/openvpn, в ней должны быть папки server и client:

```
[root@r1 easy-rsa]# ls -l  /etc/openvpn
total 0
drwxr-x---. 2 root openvpn 6 Mar 17  2022 client
drwxr-x---. 2 root openvpn 6 Mar 17  2022 server
[root@r1 easy-rsa]#
```

Для удобства копируем в нее стандартную директорию для easy-rsa:

```
[root@r1 easy-rsa]# cp -r /usr/share/easy-rsa /etc/openvpn/
[root@r1 easy-rsa]# ls -l  /etc/openvpn
total 0
drwxr-x---. 2 root openvpn  6 Mar 17  2022 client
drwxr-xr-x. 3 root root    39 Mar 21 04:33 easy-rsa
drwxr-x---. 2 root openvpn  6 Mar 17  2022 server
[root@r1 easy-rsa]#
```

Посмотрим содержимое easy-rsa:

```
[root@r1 ~]# ls -l  /etc/openvpn/easy-rsa/3.0.8
total 84
-rwxr-xr-x. 1 root root 76946 Mar 21 04:33 easyrsa
-rw-r--r--. 1 root root  4616 Mar 21 04:33 openssl-easyrsa.cnf
drwxr-xr-x. 2 root root   122 Mar 21 04:33 x509-types
[root@r1 ~]#
```

Создаём файл **vars** с настройками для выдачи сертификатов:

```
[root@r1 ~]# vim  /etc/openvpn/easy-rsa/3.0.8/vars
[root@r1 ~]#
```

```
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"
```

Делаем его исполняемым файлом:

```
[root@r1 ~]# chmod +x  /etc/openvpn/easy-rsa/3.0.8/vars
[root@r1 ~]# ls -l  /etc/openvpn/easy-rsa/3.0.8/
total 88
-rwxr-xr-x. 1 root root 76946 Mar 21 04:33 easyrsa
-rw-r--r--. 1 root root  4616 Mar 21 04:33 openssl-easyrsa.cnf
-rwxr-xr-x. 1 root root   680 Mar 21 04:42 vars
drwxr-xr-x. 2 root root   122 Mar 21 04:33 x509-types
[root@r1 ~]#
```

Создаем сертификат.

```
[root@r1 ~]# cd  /etc/openvpn/easy-rsa/3.0.8/
[root@r1 3.0.8]# ./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/3.0.8/pki


[root@r1 3.0.8]# ls -l
total 96
-rwxr-xr-x. 1 root root 76946 Mar 21 04:33 easyrsa
-rw-------. 1 root root  4616 Mar 21 04:48 openssl-1.0.cnf
-rw-r--r--. 1 root root  4616 Mar 21 04:33 openssl-easyrsa.cnf
drwx------. 4 root root    60 Mar 21 04:48 pki
-rwxr-xr-x. 1 root root   680 Mar 21 04:42 vars
drwxr-xr-x. 2 root root   122 Mar 21 04:33 x509-types
[root@r1 3.0.8]#
```

Ключ nopass генерирует приватные ключи, которые не требуют пароля при обращении с ними (для простоты). В реальности следует выполнять команду без ключа nopass, тогда у вас будет запрошен пароль (дважды) для нового сертификата.

```
[root@r1 3.0.8]# ./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]:catec

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/3.0.8/pki/ca.crt


[root@r1 3.0.8]#
req: /etc/openvpn/easy-rsa/3.0.8/pki/reqs/server.req
key: /etc/openvpn/easy-rsa/3.0.8/pki/private/server.key


[root@r1 3.0.8]#
```

Common Name (CN) в сертификате обычно представляет собой основное доменное имя (FQDN) или имя хоста, для которого вы создаете сертификат. Однако при создании корневого сертификата

CN может быть любым уникальным идентификатором, который вы выберете. Например, вы можете использовать что-то вроде "MyRootCA" или "InternalRootCA" в качестве значения CN.
В примере просто – **catec**. Можно ничего не вводить и просто нажать ENTER, в этом случае будет использоваться значение по умолчанию или пустое значение.
В результате в папке pki появился главный сертификат удостоверяющего центра **ca.crt**:

```
[root@r1 3.0.8]# ls -l ./pki
total 16
-rw-------. 1 root root 1147 Mar 21 04:53 ca.crt
drwx------. 2 root root    6 Mar 21 04:51 certs_by_serial
-rw-------. 1 root root    0 Mar 21 04:51 index.txt
-rw-------. 1 root root    0 Mar 21 04:51 index.txt.attr
drwx------. 2 root root    6 Mar 21 04:51 issued
drwx------. 2 root root   20 Mar 21 04:53 private
drwx------. 5 root root   76 Mar 21 04:51 renewed
drwx------. 2 root root    6 Mar 21 04:48 reqs
drwx------. 5 root root   76 Mar 21 04:51 revoked
-rw-------. 1 root root 4697 Mar 21 04:48 safessl-easyrsa.cnf
-rw-------. 1 root root    3 Mar 21 04:51 serial
[root@r1 3.0.8]#
```

Создаём ключи для сервера:

```
[root@r1 3.0.8]# ./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/3.0.8/pki/easy-rsa-11923.mdvhR
9/tmp.LLGWnO'
-----
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]:catec

Keypair and certificate request completed. Your files are:
```

Подписываем сертификат сервера у удостоверяющего центра:

```
[root@r1 3.0.8]# ./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                = catec


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
```

Проверяем валидность выписанного сертификата:

```
[root@r1 3.0.8]# openssl verify -CAfile pki/ca.crt pki/issued/server.crt
pki/issued/server.crt: OK
[root@r1 3.0.8]#
```

Теперь нужно создать сертификат для клиента:

```
[root@r1 3.0.8]# ./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/3.0.8/pki/easy-rsa-12024.rXMxS7/tmp.gVTVT5'
-----
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]:client01

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/3.0.8/pki/reqs/client01.req
key: /etc/openvpn/easy-rsa/3.0.8/pki/private/client01.key


[root@r1 3.0.8]#
```

Подписываем выписанный сертификат у CA:

```
[root@r1 3.0.8]# ./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/3.0.8/pki/easy-rsa-12052.TZGpQR/tmp.lnlZKV
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 Mar 21 09:18:14 2025 GMT (365 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/3.0.8/pki/issued/client01.crt


[root@r1 3.0.8]#
```

Проверяем валидность сертификата:

```
[root@r1 3.0.8]# openssl verify -CAfile pki/ca.crt pki/issued/client01.crt
pki/issued/client01.crt: OK
[root@r1 3.0.8]#
```

Создаём Diffie-Hellman-ключ:

```
[root@r1 3.0.8]# ./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
.....................................................................
.....................................+.................................
.....................+.....................................++++++*

DH parameters of size 2048 created at /etc/openvpn/easy-rsa/3.0.8/pki/dh.pem


[root@r1 3.0.8]#
```

В итоге:

Корневой сертификат:

```
[root@r1 3.0.8]# ls -l ./pki/
total 40
-rw-------. 1 root root 1147 Mar 21 04:53 ca.crt
drwx------. 2 root root   94 Mar 21 05:18 certs_by_serial
-rw-------. 1 root root  424 Mar 21 05:23 dh.pem
-rw-------. 1 root root  139 Mar 21 05:18 index.txt
-rw-------. 1 root root   20 Mar 21 05:18 index.txt.attr
-rw-------. 1 root root   20 Mar 21 05:11 index.txt.attr.old
-rw-------. 1 root root   68 Mar 21 05:11 index.txt.old
drwx------. 2 root root   44 Mar 21 05:18 issued
drwx------. 2 root root   58 Mar 21 05:17 private
drwx------. 5 root root   76 Mar 21 04:51 renewed
drwx------. 2 root root   44 Mar 21 05:17 reqs
drwx------. 5 root root   76 Mar 21 04:51 revoked
-rw-------. 1 root root 4697 Mar 21 04:48 safessl-easyrsa.cnf
-rw-------. 1 root root   33 Mar 21 05:18 serial
-rw-------. 1 root root   33 Mar 21 05:18 serial.old
[root@r1 3.0.8]#
```

Сертификаты сервера и клиента:

```
[root@r1 3.0.8]# ls -l ./pki/issued
total 16
-rw-------. 1 root root 4410 Mar 21 05:18 client01.crt
-rw-------. 1 root root 4517 Mar 21 05:11 server.crt
[root@r1 3.0.8]#
```

Приватные ключи сервера и клиента и УЦ:

```
[root@r1 3.0.8]# ls -l ./pki/private
total 12
-rw-------. 1 root root 1675 Mar 21 04:51 ca.key
-rw-------. 1 root root 1704 Mar 21 05:17 client01.key
-rw-------. 1 root root 1704 Mar 21 05:07 server.key
[root@r1 3.0.8]#
```

Копируем выписанные сертификаты в папку /etc/openvpn/server и /etc/openvpn/client:

```
[root@r1 3.0.8]# cp pki/ca.crt /etc/openvpn/server/
[root@r1 3.0.8]# cp pki/issued/server.crt /etc/openvpn/server/
[root@r1 3.0.8]# cp pki/private/server.key /etc/openvpn/server/
[root@r1 3.0.8]# cp pki/ca.crt /etc/openvpn/client/
[root@r1 3.0.8]# cp pki/issued/client01.crt /etc/openvpn/client/
[root@r1 3.0.8]# cp pki/private/client01.key /etc/openvpn/client/
[root@r1 3.0.8]# cp pki/dh.pem /etc/openvpn/server/
```

Проверяем:

mc [root@r1]:/etc/openvpn/client

Left File Command Options Right

<- /etc/openvpn/server

'n Name	Size	Modify time
/..	UP--DIR	Mar 21 04:33
ca.crt	1147	Mar 21 05:27
dh.pem	424	Mar 21 05:28
server.crt	4517	Mar 21 05:28
server.key	1704	Mar 21 05:28

<- /etc/openvpn/client

'n Name	Size	Modify time
/..	UP--DIR	Mar 21 04:33
ca.crt	1147	Mar 21 05:28
client01.crt	4410	Mar 21 05:28
client01.key	1704	Mar 21 05:28

Создаём конфиг для сервера при помощи файла /etc/openvpn/server.conf:

```
[root@r1 3.0.8]# 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
# VPN-подсеть, из которой будут получать адреса VPN-клиенты
server 10.5.5.0 255.255.255.0
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-
RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
auth SHA512
auth-nocache

# Other Configuration
```

Включаем форвардинг и разрешаем OpenVPN в файерволе:

```
[root@r1 3.0.8]# echo 'net.ipv4.ip_forward = 1' >> /etc/sysctl.conf
[root@r1 3.0.8]# sysctl -p
net.ipv4.ip_forward = 1
[root@r1 3.0.8]# firewall-cmd --permanent --add-service=openvpn
success
[root@r1 3.0.8]# firewall-cmd --permanent --zone=trusted --add-interface=tun0
success
```

--add-masquerade добавляет правило маскарадинга (NAT).

```
[root@r1 ~]# firewall-cmd --permanent --zone=public --add-masquerade
success
[root@r1 ~]# firewall-cmd --reload
success
```

Запускаем сервис, проверяем состояние:

```
[root@r1 3.0.8]# systemctl start openvpn@server
[root@r1 3.0.8]# systemctl status openvpn@server
● openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Applic
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; disabled; vendor
   Active: active (running) since Thu 2024-03-21 06:06:56 EDT; 34s ago
 Main PID: 12257 (openvpn)
   Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─12257 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf

Mar 21 06:06:56 r1 systemd[1]: Starting OpenVPN Robust And Highly Flexible Tun
Mar 21 06:06:56 r1 systemd[1]: Started OpenVPN Robust And Highly Flexible Tunn
[root@r1 3.0.8]#
```

Смотрим сетевые интерфейсы, должен появиться интерфейс **tun0** с IP-адресом из диапазона, указанного в server.conf:

```
[root@r1 3.0.8]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gr
oup 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
 state UP group default qlen 1000
    link/ether 08:00:27:0b:5e:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.158/24 brd 192.168.1.255 scope global noprefixroute
 dynamic enp0s3
       valid_lft 74951sec preferred_lft 74951sec
    inet6 fe80::eda2:be1d:1730:52c7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
 state UP group default qlen 1000
    link/ether 08:00:27:a8:9e:9d brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.1/24 brd 10.1.1.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea8:9e9d/64 scope link
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfif
o_fast state UNKNOWN group default qlen 100
    link/none
    inet 10.5.5.1 peer 10.5.5.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::1f05:b332:3432:22ac/64 scope link flags 800
       valid_lft forever preferred_lft forever
[root@r1 3.0.8]#
```

Настройка сервера завершена.

Настройка клиента:

```
[root@r1 3.0.8]# vim /etc/openvpn/client/client01.ovpn
[root@r1 3.0.8]#
```

```
client
dev tun
proto udp
remote 10.1.1.1 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-25
6-CBC-SHA256:TLS-DHERSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-1
28-CBC-SHA256
resolv-retry infinite
compress lzo
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
~
```

Теперь все, что нужно клиенту лежит в папке:

```
[root@r1 3.0.8]# ls -l /etc/openvpn/client/
total 20
-rw-------. 1 root root 1147 Mar 21 05:28 ca.crt
-rw-------. 1 root root 4410 Mar 21 05:28 client01.crt
-rw-------. 1 root root 1704 Mar 21 05:28 client01.key
-rw-r--r--. 1 root root  434 Mar 21 06:18 client01.ovpn
[root@r1 3.0.8]#
```

Упаковываем ее в архив:

```
[root@r1 3.0.8]# cd /etc/openvpn/
[root@r1 openvpn]# tar -czvf client01.tar.gz client/*
client/ca.crt
client/client01.crt
client/client01.key
client/client01.ovpn
[root@r1 openvpn]#
```

На клиентской машине скачиваем архив:

```
user@r2:~$ scp 10.1.1.1:/etc/openvpn/client01.tar.gz /home/user
The authenticity of host '10.1.1.1 (10.1.1.1)' can't be established.
ED25519 key fingerprint is SHA256:wGkcPSikfNigOKG626V4I8fDjFJhtupJjIhvjJ87Yzc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.1.1' (ED25519) to the list of known hosts.
user@10.1.1.1's password:
client01.tar.gz                               100% 4958   489.9KB/s   00:00
user@r2:~$ ls -l
итого 44
-rw-r--r-- 1 user user 4958 Hay 21 18:57  client01.tar.gz
drwx------ 3 user user 4096 Hay 21 18:24  snap
```

В домашней папке распакуем архив:

```
user@r2:~$ tar -xzvf client01.tar.gz
client/ca.crt
client/client01.crt
client/client01.key
client/client01.ovpn
```

Появился каталог client:

```
user@r2:~$ ls -l
итого 48
drwxrwxr-x 2 user user 4096 Hay 21 18:58  client
-rw-r--r-- 1 user user 4958 Hay 21 18:57  client01.tar.gz
drwx------ 3 user user 4096 Hay 21 18:24  snap
drwxr-xr-x 2 user user 4096 Hay 21 18:15  Видео
drwxr-xr-x 2 user user 4096 Hay 21 18:15  Документы
drwxr-xr-x 2 user user 4096 Hay 21 18:15  Загрузки
```

Перейдем в каталог client и запустим OpenVPN:

```
user@r2:~/client$ sudo openvpn --config client01.ovpn
2024-03-21 19:02:40 WARNING: Compression for receiving enabled. Compression has
been used in the past to break encryption. Sent packets are not compressed unles
s "allow-compression yes" is also set.
2024-03-21 19:02:40 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing
 in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore
 --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers or change
 --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this
 warning.
```

```
2024-03-21 19:02:41 net_route_v4_add: 10.5.5.1/32 via 10.5.5.5 dev [NULL] table
0 metric -1
2024-03-21 19:02:41 Initialization Sequence Completed
```

Запустим вторую консоль и проверим подключение к Интернет, работает:

```
user@r2:~/client$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=250 ttl=59 time=75.7 ms
64 bytes from 8.8.8.8: icmp_seq=251 ttl=59 time=76.2 ms
64 bytes from 8.8.8.8: icmp_seq=252 ttl=59 time=74.8 ms
64 bytes from 8.8.8.8: icmp_seq=253 ttl=59 time=75.9 ms
64 bytes from 8.8.8.8: icmp_seq=254 ttl=59 time=84.2 ms
64 bytes from 8.8.8.8: icmp_seq=255 ttl=59 time=77.3 ms
```

Убедимся, что трфик идет через туннель, с помощью команды **mtr 8.8.8.8:**

```
                          My traceroute  [v0.95]
r2 (10.5.5.6) -> 8.8.8.8 (8.8.8.8)                    2024-03-22T17:06:11+0600
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                 Packets                Pings
 Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.5.5.1                    0.0%    26    4.2   3.7   2.7   7.6   1.0
 2. 192.168.1.1                 0.0%    26    6.5   6.1   4.1  17.0   2.7
 3. 2.132.48.1.megaline.telecom.kz  0.0%  26    8.5   7.8   6.0  11.8   1.6
 4. 82.200.243.22               0.0%    26   62.0  61.3  58.5  77.3   4.2
 5. 95.59.172.46.static.telecom.kz  0.0%  26   61.0  62.7  59.5  82.7   4.5
 6. 95.56.166.2                 0.0%    26   58.3  61.3  57.9  79.1   5.4
 7. 89.218.6.74                 3.8%    26   61.4  65.3  60.0  88.9   6.8
 8. 216.239.50.155              0.0%    26   63.3  62.8  59.1  78.7   4.4
 9. 108.170.250.99              0.0%    26   65.1  61.4  59.0  65.3   1.8
10. 142.251.238.82              0.0%    26   78.0  79.0  76.5  92.5   3.3
11. 142.251.238.68              0.0%    26   77.2  78.5  76.6  88.4   2.5
12. 142.250.56.217              0.0%    26   75.7  76.8  75.1  82.8   1.8
13. (waiting for reply)
14. (waiting for reply)
15. (waiting for reply)
16. (waiting for reply)
17. (waiting for reply)
18. (waiting for reply)
19. (waiting for reply)20. (waiting   0.0%    25   77.9  79.1  76.4  84.3   2.3
```

На openvpn сервере запустим tcpdump (консольная утилита-анализатор трафика) и посмотрим трафик на интерфейсе enp0s3 (выход в Интернет)

```
[root@r1 ~]# tcpdump -nni enp0s3 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
07:11:43.704944 IP 192.168.1.158 > 8.8.8.8: ICMP echo request, id 0, seq 180, length 64
07:11:43.778038 IP 8.8.8.8 > 192.168.1.158: ICMP echo reply, id 0, seq 180, length 64
07:11:44.696545 IP 192.168.1.158 > 8.8.8.8: ICMP echo request, id 0, seq 181, length 64
07:11:44.769981 IP 8.8.8.8 > 192.168.1.158: ICMP echo reply, id 0, seq 181, length 64
07:11:45.697700 IP 192.168.1.158 > 8.8.8.8: ICMP echo request, id 0, seq 182, length 64
07:11:45.771580 IP 8.8.8.8 > 192.168.1.158: ICMP echo reply, id 0, seq 182, length 64
07:11:46.699587 IP 192.168.1.158 > 8.8.8.8: ICMP echo request, id 0, seq 183, length 64
07:11:46.772942 IP 8.8.8.8 > 192.168.1.158: ICMP echo reply, id 0, seq 183, length 64
```

Видно, что работает NAT, ip-адрес клиента заменяется на ip-адрес сервера.

Вот что приходит на интерфейс tun0:

```
[root@r1 ~]# tcpdump -nni tun0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
07:17:13.295980 IP 10.5.5.6 > 8.8.8.8: ICMP echo request, id 28, seq 485, length 64
07:17:13.375486 IP 8.8.8.8 > 10.5.5.6: ICMP echo reply, id 28, seq 485, length 64
07:17:14.380628 IP 10.5.5.6 > 8.8.8.8: ICMP echo request, id 28, seq 486, length 64
07:17:14.460790 IP 8.8.8.8 > 10.5.5.6: ICMP echo reply, id 28, seq 486, length 64
07:17:15.465703 IP 10.5.5.6 > 8.8.8.8: ICMP echo request, id 28, seq 487, length 64
07:17:15.545113 IP 8.8.8.8 > 10.5.5.6: ICMP echo reply, id 28, seq 487, length 64
07:17:16.552440 IP 10.5.5.6 > 8.8.8.8: ICMP echo request, id 28, seq 488, length 64
07:17:16.631762 IP 8.8.8.8 > 10.5.5.6: ICMP echo reply, id 28, seq 488, length 64
```

Теперь остановим openvpn на 1-м хосте:

```
[root@r1 ~]# systemctl stop openvpn@server
[root@r1 ~]# systemctl status openvpn@server
● openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Applicat
ion On server
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; disabled; vendor pr
eset: disabled)
   Active: inactive (dead)

Mar 21 06:00:23 r1 systemd[1]: Unit openvpn@server.service entered failed state.
Mar 21 06:00:23 r1 systemd[1]: openvpn@server.service failed.
Mar 21 06:06:56 r1 systemd[1]: Starting OpenVPN Robust And Highly Flexible .....
Mar 21 06:06:56 r1 systemd[1]: Started OpenVPN Robust And Highly Flexible T...r.
Mar 21 07:02:08 r1 systemd[1]: Stopping OpenVPN Robust And Highly Flexible .....
Mar 21 07:02:09 r1 systemd[1]: Stopped OpenVPN Robust And Highly Flexible T...r.
Mar 21 07:06:21 r1 systemd[1]: Starting OpenVPN Robust And Highly Flexible .....
Mar 21 07:06:21 r1 systemd[1]: Started OpenVPN Robust And Highly Flexible T...r.
Mar 21 07:07:45 r1 systemd[1]: Stopping OpenVPN Robust And Highly Flexible .....
Mar 21 07:07:45 r1 systemd[1]: Stopped OpenVPN Robust And Highly Flexible T...r.
Hint: Some lines were ellipsized, use -l to show in full.
[root@r1 ~]#
```

Снова проверим доступ в интернет на 2-м хосте:

```
user@r2:~/client$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

Не работает. Как и было задумано.

На локальный интерфейс сервера по-прежнему поступают пакеты, но файрволл их отбрасывает:

```
[root@r1 ~]# tcpdump -nni enp0s8 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
07:18:33.071420 IP 10.1.1.1 > 10.1.1.2: ICMP 10.1.1.1 udp port 1194 unreachable, length 145
07:18:34.180824 IP 10.1.1.1 > 10.1.1.2: ICMP 10.1.1.1 udp port 1194 unreachable, length 145
07:18:35.290199 IP 10.1.1.1 > 10.1.1.2: ICMP 10.1.1.1 udp port 1194 unreachable, length 145
07:18:36.399945 IP 10.1.1.1 > 10.1.1.2: ICMP 10.1.1.1 udp port 1194 unreachable, length 145
07:18:37.509201 IP 10.1.1.1 > 10.1.1.2: ICMP 10.1.1.1 udp port 1194 unreachable, length 145
07:18:38.618422 IP 10.1.1.1 > 10.1.1.2: ICMP 10.1.1.1 udp port 1194 unreachable, length 145
```

Задание:

1. Собрать стенд из 2-х виртуальных машин, согласно схеме и вашего варианта задания. Имена хостов должны содержать ваше имя на латинице, например: stepan-r1 или ravhat-r2.

2. Поднять openvpn-сервер на Centos 7 и обеспечить возможность подключения клиента Ubuntu 22.04, используя сертификаты.

3. Убедиться, что клиент может пропинговать 8.8.8.8, когда VPN подключен, и не может этого сделать, когда VPN не подключен

4. Проанализировать трафик на интерфейсах сервера.

5. Сделать выводы.

№ варианта	LAN 1	LAN 2 (сеть openvpn)
1	192.168.10.0/24	10.1.1.0
2	192.168.30.0/24	10.1.2.0
3	192.168.50.0/24	10.1.3.0
4	192.168.70.0/24	10.1.4.0
5	192.168.90.0/24	10.1.5.0
6	192.168.110.0/24	10.1.6.0
7	192.168.130.0/24	10.1.7.0
8	192.168.150.0/24	10.1.8.0
9	192.168.170.0/24	10.1.9.0
10	192.168.190.0/24	10.1.10.0
11	192.168.210.0/24	10.1.11.0
12	192.168.230.0/24	10.1.12.0
13	192.168.10.0/24	10.1.13.0
14	192.168.30.0/24	10.1.14.0
15	192.168.50.0/24	10.1.15.0
16	192.168.70.0/24	10.1.16.0
17	192.168.90.0/24	10.1.17.0
18	192.168.110.0/24	10.1.18.0
19	192.168.130.0/24	10.1.19.0
20	192.168.150.0/24	10.1.20.0