Выполнил Мешечкин Д. Инфобез-2345

Задание 1: На сервере R3 добавить еще один интерфейс — dummy с IP-адресом 33.33.33.33/32.

На сервере R3 создается новый dummy интерфейс 33.33.33.33/32, воспользовавшись ДЗ к вебинару №2:

#ip link add dummy1 type dummy
#ip addr add 33.33.33.33/32 dev dummy1
#ip link set up dev dummy1

И необходимо изменить правило **dummy.conf** добавив второй интерфейс dummy и опцию количество dummy интерфейсов:

cat > /etc/modprobe.d/dummy.conf
install dummy /sbin/modprobe --ignore-install dummy numdummies=2; /sbin/ip link set dev dummy0 name dummy0; /sbin/ip link set dev dummy1 name dummy1

И добавляю конфиг dummy1
cat > /etc/sysconfig/network-scripts/ifcfg-dummy0
NAME=dummy1
DEVICE=dummy1
MACADDR=00:22:33:ff:ff:ff
IPADDR=33.33.33.33
PREFIX=32
ONBOOT=yes
TYPE=dummy
NM_CONTROLLED=no

Так же есть вариант с добавлением **#cat > /etc/modprobe.d/dummyopts.conf**
options dummy numdummies=2
Что примерно приведёт к подобному исходу с возможностью запуска двух и более dummy интерфейсов.

Данный интерфейс ни где не отображается и в итоге пинг с серверов R2 и R1 улетает наружу.

```
[root@server1 ~]# traceroute 33.33.33.33
traceroute to 33.33.33.33 (33.33.33.33), 30 hops max, 60 byte packets
 1  RT-AC66U-C1B0 (192.168.1.1)  0.430 ms  0.533 ms  0.678 ms
 2  ASR5-10.kmv.ru (217.13.214.45)  2.899 ms  2.877 ms  2.861 ms
 3  P20g1Pyat-68.kmv.ru (217.13.213.193)  2.844 ms  2.827 ms  2.812 ms
```

```
[root@server2 ~]# traceroute 33.33.33.33
traceroute to 33.33.33.33 (33.33.33.33), 30 hops max, 60 byte packets
 1  RT-AC66U-C1B0 (192.168.1.1)  0.459 ms  0.535 ms  0.638 ms
 2  ASR5-10.kmv.ru (217.13.214.45)  2.578 ms  2.693 ms  2.668 ms
```

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

Для поднятия VPN сервера понадобится epel-release, openvp и easy-rsa.
Первый этап - подготовка сертификатов.

Копирование стандартной директории easy-rsa в openvpn:
cp -r /usr/share/easy-rsa /etc/openvpn/
cd /etc/openvpn/easy-rsa/3
ll

```
[root@server3 3]# ll
total 84
-rwxr-xr-x. 1 root root 76946 Aug 27 09:07 easyrsa
-rw-r--r--. 1 root root  4616 Aug 27 09:07 openssl-easyrsa.cnf
drwxr-xr-x. 2 root root   122 Aug 27 09:07 x509-types
```

Создаю **vars** с настройками для выдачи сертификатов:
touch 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"

Делаю vars исполняемым файлом
chmod +x vars

Запуск инфраструктуры PKI с nopass ключом для генерации приватных ключей не требующих пароля при обращении с ними.

./easyrsa init-pki
./easyrsa build-ca nopass

```
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
```

Сертификат CA создан, далее создание ключей для сервера и клиента:

./easyrsa gen-req server nopass

```
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
```

Далее сертификат подписывается у CA:
./easyrsa sign-req server server

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

Далее можно проверить валидность сертификата:
openssl verify -CAfile pki/ca.crt pki/issued/server.crt

```
[root@server3 3]# openssl verify -CAfile pki/ca.crt pki/issued/server.crt
pki/issued/server.crt: OK
```

Далее подготовка сертификата для клиента:
./easyrsa gen-req clientR1 nopass

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/3/pki/reqs/clientR1.req
key: /etc/openvpn/easy-rsa/3/pki/private/clientR1.key

Подпись сертификата:
./easyrsa sign-req client clientR1
Certificate created at: /etc/openvpn/easy-rsa/3/pki/issued/clientR1.crt

И проверка его:
openssl verify -CAfile pki/ca.crt pki/issued/clientR1.crt

```
[root@server3 3]# openssl verify -CAfile pki/ca.crt pki/issued/clientR1.crt
pki/issued/clientR1.crt: OK
```

Далее создаю Diffie-Hellman ключ:
./easyrsa gen-dh
После раскидываю сертификаты по директориям **/etc/openvpn/server** и **/etc/openvpn/client/**
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/

После копирования создаю конфиг файл для сервера:

touch /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

 # Redire10.8.1.0 255.255.255.0
push "redirect-gateway def1"

 # Using the DNS from https://dns.watch
push "dhcp-option DNS 8.8.8.8"

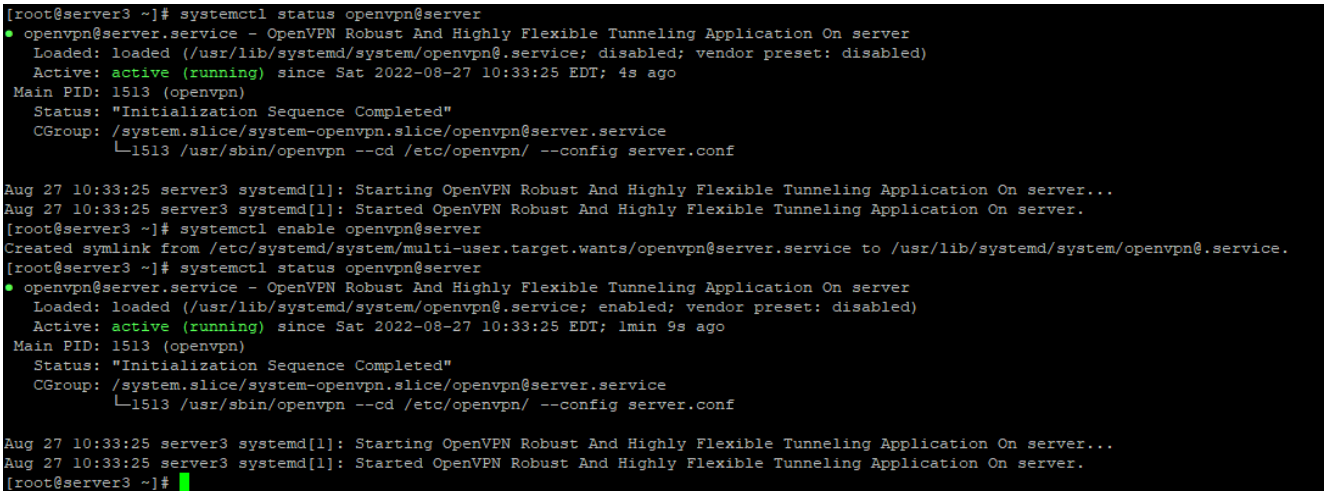
#Enable multiple client to connect with same Certificate key
duplicate-cn

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

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

Далее проба запуска сервера:
systemctl start openvpn@server
systemctl enable openvpn@server
systemctl status openvpn@server
и проверка занятого порта
ss -tulpan | grep 1194



Создаю конфиг клиента с указанием IP vpn сервера:

cd /etc/openvpn/client
touch clientR1.ovpn
client
dev tun
proto udp
remote 192.168.1.193 1194 # IP адрес сервера
ca ca.crt
cert clientR1.crt
key clientR1.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

Далее перенос сертификатов на клиентскую машину:
воспользуюсь папкой nfs_1 из ДЗ к вебинару №2
cd /etc/openvpn/
tar -czvf clientR1.tar.gz client/*
cp -r clientR1.tar.gz /nfs_1/

На сервере R1:
yum install openvpn network-manager-openvpn -y
cd /tmp/export/nfs_1/

cp /mnt/export/nfs_1/clientR1.tar.gz /etc/openvpn/ /после из директории стёр архив
cd /etc/openvpn/
tar -xzvf clientR1.tar.gz
cd client
и перед запуском vpn клиента необходимо открыть порт 1194
openvpn --config client01.ovpn
далее ctrl+c и запуск клиента в фоне
openvpn --config client01.ovpn &
bash /для выхода к терминалу

```
Sat Aug 27 13:09:42 2022 /sbin/ip route add 0.0.0.0/1 via 10.8.1.5
Sat Aug 27 13:09:42 2022 /sbin/ip route add 128.0.0.0/1 via 10.8.1.5
Sat Aug 27 13:09:42 2022 /sbin/ip route add 10.8.1.1/32 via 10.8.1.5
Sat Aug 27 13:09:42 2022 Initialization Sequence Completed
```

Помимо этого стал пинговаться интерфейс dummy1 на R3 33.33.33.33

```
10: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 10.8.1.10 peer 10.8.1.9/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::f3b7:128:b5a6:559f/64 scope link flags 800
       valid_lft forever preferred_lft forever
[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=0.428 ms
64 bytes from 33.33.33.33: icmp_seq=2 ttl=64 time=0.416 ms
64 bytes from 33.33.33.33: icmp_seq=3 ttl=64 time=0.415 ms
64 bytes from 33.33.33.33: icmp_seq=4 ttl=64 time=0.403 ms
64 bytes from 33.33.33.33: icmp_seq=5 ttl=64 time=0.431 ms
^C
--- 33.33.33.33 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.403/0.418/0.431/0.024 ms
```

Выключаем openvpn client, проверяю 33.33.33.33, пинг не идёт. Задание выполнено.

```
Sat Aug 27 13:25:16 2022 /sbin/ip route del 192.168.1.193/32
Sat Aug 27 13:25:16 2022 /sbin/ip route del 0.0.0.0/1
Sat Aug 27 13:25:16 2022 /sbin/ip route del 128.0.0.0/1
Sat Aug 27 13:25:16 2022 Closing TUN/TAP interface
Sat Aug 27 13:25:16 2022 /sbin/ip addr del dev tun1 local 10.8.1.6 peer 10.8.1.5
Sat Aug 27 13:25:16 2022 SIGINT[hard,] received, process exiting
[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 ---
7 packets transmitted, 0 received, 100% packet loss, time 6000ms
```

Единственное в чём не очень разобрался с ходу - вывод приложение из фонового режима. По сути просто посмотрел через **ps** PID openvpn процесс и просто грохнул его ¯_(ツ)_/¯