Создание сертификата, ключа и конфигурации в OpenVPN

Краткое описание

Сервис используется для удаленного доступа к оборудованию в дата-центрах.

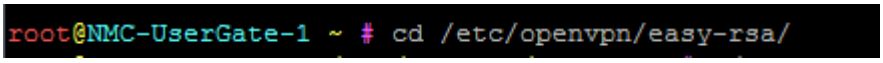
Исходная информация

Server name:	UserGate-1
IP внешний:	95.216.172.93
IP OpenVPN:	10.255.255.1
Используемый протокол:	TCP
Используемый порт:	1194
Сеть выдаваемая клиентам:	10.255.255.0/24
Запуск/остановка сервиса:	service openvpn start/stop
Статус сервиса:	service openvpn status

Выпуск сертификата клиента:

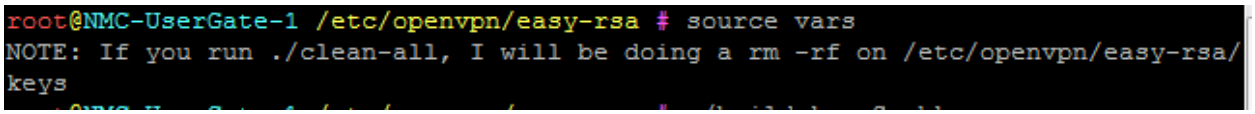
1. Заходим на сервер и переходим по пути:

```
cd /etc/openvpn/easy-rsa
```



2. Выполняем команду

```
source vars
```



3. Создаем ключ и сертификат клиента

> ./build-key client_name
>
> *Нужно быть внимательным, в конце будут запросы, отвечаем “y”.*
>
> Sign the certificate? [y/n]:y
>
> 1 out of 1 certificate requests certified, commit? [y/n]:y

```
root@NMC-UserGate-1 /etc/openvpn/easy-rsa # ./build-key Sashkaru
Generating a RSA private key
.+++++
.....................................................................................
..............+++++
writing new private key to 'Sashkaru.key'
-----
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.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) [MSK]:
Locality Name (eg, city) [Moscow]:
Organization Name (eg, company) [NMC]:
Organizational Unit Name (eg, section) [Community]:
Common Name (eg, your name or your server's hostname) [Sashkaru]:
Name [NMC]:
Email Address [Dv@bubnovd.net]:sashkaru74zelencov@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :PRINTABLE:'MSK'
localityName          :PRINTABLE:'Moscow'
organizationName      :PRINTABLE:'NMC'
organizationalUnitName:PRINTABLE:'Community'
commonName            :PRINTABLE:'Sashkaru'
name                  :PRINTABLE:'NMC'
emailAddress          :IA5STRING:'sashkaru74zelencov@gmail.com'
Certificate is to be certified until Nov 29 08:09:57 2029 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
```

Сертификат и ключ сгенерирован.

4. Далее нам необходимо вытащить сертификат и ключ с сервера, в моем случае используется Bitvise SSH Client.

   При соединении открывает не только ssh но и sftp.

   Переходим в папку “/etc/openvpn/easy-rsa/keys“, копируем файлы для клиента: CA.crt, client_name.crt, client_name.key.

5. Конфигурация для клиента:

```
dev tun
proto tcp-client
remote 95.216.172.93 1194
resolv-retry infinite
client
persist-key
persist-tun
ca "C:\\Program Files\\OpenVPN\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\client_name.crt"
key "C:\\Program Files\\OpenVPN\\client_name.key"
cipher AES-128-CBC
verb 3
```