OpenVPN — easy-rsa

Fix Me!

Стандартный вариант настройки OpenVPN это использование `easy-rsa`

Администратору системы должны быть доступны все файлы, в том числе и Клиентские - это нужно для отзыва клиентского сертификата

Начальная настройка сервера

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

/etc/openvpn/easy-rsa/vars

```
export KEY_COUNTRY="RU"
export KEY_PROVINCE="Province"
export KEY_CITY="City"
export KEY_ORG="Firma"
export KEY_EMAIL="info@domain.ru"
```

```
chmod +x vars
```

/etc/openvpn/easy-rsa/openvpn.cnf

```
[ ca ]
default_ca              = CA_default
[ CA_default ]
dir                     = /etc/openvpn/easy-rsa/keys
crl_dir                 = $dir/crl
database                = $dir/index.txt
new_certs_dir           = $dir/certs
certificate             = $dir/ca.crt
serial                  = $dir/serial
crl                     = $dir/crl.pem
private_key             = $dir/ca.key
RANDFILE                = $dir/.rand
default_days            = 3650
default_crl_days        = 30
default_md              = md5
unique_subject          = yes
policy                  = policy_any
x509_extensions         = user_extensions
[ policy_any ]
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
[ req ]
default_bits            = 2048
default_keyfile         = privkey.pem
distinguished_name      = req_distinguished_name
x509_extensions         = CA_extensions
[ req_distinguished_name ]
organizationName        = Organization Name (must match CA)
organizationName_default = Company
organizationalUnitName  = Location Name
commonName              = Common User or Org Name
```

```
commonName_max          = 64
[ user_extensions ]
basicConstraints        = CA:FALSE
[ CA_extensions ]
basicConstraints        = CA:TRUE
default_days            = 3650
[ server ]
basicConstraints        = CA:FALSE
nsCertType              = server
```

Создание сертификата сервера

```
cd /etc/openvpn/easy-rsa
source ./vars
./clean-all
./build-ca
```

Создание ключа сервера

```
cd /etc/openvpn/easy-rsa
source ./vars
./build-key-server server
```

Создание ключа Диффи — Хеллмана

```
cd /etc/openvpn/easy-rsa
source ./vars
./build-dh
```

Создание ключа для tls-аутификации

```
openvpn --genkey --secret keys/ta.key
```

Создание пустого списка отозванных сертификатов

/etc/openvpn/easy-rsa/Create_Empty_crl-pem.sh

```
#!/bin/sh
cd /etc/openvpn/easy-rsa
source ./vars
openssl ca -config openvpn.cnf -gencrl -out keys/crl.pem
```

Копирование серверных ключей в папку сервера

```
mkdir /etc/openvpn/keys
cd /etc/openvpn/easy-rsa/keys
cp server.crt server.key ca.crt dh1024.pem dh2048.pem crl.pem ta.key /etc/openvpn/keys
```

Создании ключа клиента

create_user.sh

```
#!/bin/bash

cd /etc/openvpn/easy-rsa
source ./vars
./build-key ИМЯ_КЛИЕНТА
```

Просмотр списка отозванных клиентских сертификатов

/etc/openvpn/easy-rsa/List_crl-pem.sh

```
#!/bin/sh
cd /etc/openvpn/easy-rsa
source ./vars
./list-crl
```

Отзыв клиентского сертификата

Отзыв (аннулирование) клиентского сертификата, создание CRL файла

Для отзыва выполняем:

```
cd /usr/share/doc/openvpn/examples/easy-rsa/2.0
. ./vars
./revoke-full ИМЯ_КЛИЕНТА
```

Копируем `crl.pem` на сервер и добавляем в файл `openvpn.conf` сроку `crl-verify crl.pem`

Если файл `crl.pem` отсутствует, а директива `crl-verify crl.pem` в `openvpn.conf` присутствует, то сервер не пустит ни одного клиента !

Ссылки

https://sysadminmosaic.ru/openvpn/easy-rsa

2019-05-08 22:37