OpenVPN и stunnel

В некоторых случаях необходимо обернуть OpenVPN во что-то для прохода через фаерволы. Отличным вариантом является stunnel.

Устанавливаем stunnel

Устанавливаем на сервер и на клиенте:

```
apt install stunnel4
```

Настраиваем сервер

Создаем ключи:

```
cd /etc/stunnel
openssl genrsa -out key.pem 2048
openssl req -new -x509 -key key.pem -out cert.pem -days 3650
cat key.pem cert.pem >> stunnel.pem
```

Создаем файл конфигурации /etc/stunnel/stunnel.conf

```
chroot = /var/lib/stunnel4
pid = /stunnel.pid
output = /stunnel.log
setuid = stunnel4
setgid = stunnel4
socket = l:TCP_NODELAY=1

[openvpn]
accept = XX.XX.XX.XX:YYYY
connect = 127.0.0.1:1194
cert=/etc/stunnel/cert.pem
key=/etc/stunnel/key.pem
```

где XX.XX.XX.XX - адрес на котором stunnel будет слушать, а YYYY - порт

Для того, чтобы сервис stunnel стартовал автоматически необходимо отредактировать файл /etc/default/stunnel4

```
ENABLED=1
```

Открываем порт на фаерволе (в моем случае это ufw):

```
sudo ufw allow YYYY
```

Теперь перезапустим службу stunnel, сервис должен полноценно заработать и начать принимать входящие соединения:

```
# sudo /etc/init.d/stunnel4 restart
```

Настраиваем клиента

Копируем stunnel.pem - сертификат с сервера в /etc/stunnel

Создаем файл конфигурации /etc/stunnel/stunnel.conf

```
output = /stunnel.log
client = yes

[openvpn]
cert = /etc/stunnel/stunnel.pem
accept = ZZ.ZZ.ZZ.ZZ:1194
connect = XX.XX.XX.XX:YYYY
```

где

- XX.XX.XX.XX - адрес сервера к которому stunnel будет подключаться, а YYYY - порт
- ZZ.ZZ.ZZ.ZZ - адрес сервера OpenVPN

Теперь перезапустим службу stunnel, клиент должен подключиться:

```
# sudo /etc/init.d/stunnel4 restart
```

Далее в OpenVPN со стороны клиента настраиваем подключение к ZZ.ZZ.ZZ.ZZ:1194 и проверяем работу

openvpn, stunnel, vpn