



OPENVPN rendszer telepítése és mérése.

Szerver telepítése

1. SSH segítségével lépjen be a távoli gépre! (185.143.48.2XX)
2. Telepítse fel az openvpn csomagot!

```
apt-get install openvpn easy-rsa
```

3. A `/usr/share/easy-rsa/vars` állomány végén értelemszerűen javítsa ki a következő sorokat!

```
export KEY_COUNTRY="HU"  
export KEY_PROVINCE="GYMS"  
export KEY_CITY="GYOR"  
export KEY_ORG="TILB"  
export KEY_EMAIL="openvpnadmin@sze.hu"
```

4. Hozzon létre egy keys könyvtárat a `/etc/openvpn`-en belül!

```
mkdir /etc/openvpn/keys
```

5. Másolja át a `/etc/openvpn` könyvtárba a `/usr/share/easy-rsa/openssl-1.0.0.cnf` -et, `openssl.cnf` néven, majd a `whichopenssl.cnf` illetve a `pktool` fájlokat.

```
cp /usr/share/easy-rsa/openssl-1.0.0.cnf /etc/openvpn/openssl.cnf  
cp /usr/share/easy-rsa/whichopenssl.cnf /etc/openvpn/  
cp /usr/share/easy-rsa/pktool /etc/openvpn/
```

6. Adja ki a következő parancsokat úgy, hogy a `/etc/openvpn` könyvtárban áll!

```
./usr/share/easy-rsa/vars  
./usr/share/easy-rsa/clean-all  
./usr/share/easy-rsa/build-ca  
./usr/share/easy-rsa/build-dh
```

Ezekkel a parancsokkal legenerálta az openvpn azonosításhoz szükséges digitális aláírásokat és kulcsokat (certificateket).

7. Lépjen be a `/usr/share/easy-rsa` könyvtárba és ott adja ki a következő parancsokat:

```
./build-key-server server  
./build-key client
```

Ezekkel létrehozta a szerver és a kliens kulcsait mellyel autentikálhat az openvpn-be. A létrehozás során ne adjon meg jelszót!

8. Csomagolja ki a `/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz`-t az `/etc/openvpn` könyvtárba:

```
cd /etc/openvpn  
cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz .
```



```
gzip -d server.conf.gz
```

9. Hozza létre a statikus kulcsot:

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

10. A konfigurációs állományban adja meg a szükséges állományok pontos elérési útját:

```
ca /etc/openvpn/keys/ca.crt  
cert /etc/openvpn/keys/server.crt  
key /etc/openvpn/keys/server.key # This file should be kept secret  
dh /etc/openvpn/keys/dh2048.pem  
tls-auth /etc/openvpn/keys/ta.key 0 # This file is secret
```

11. A modprobe segítségével töltsse be a tun modult majd indítsa el az openvpn szervert és ellenőrizze futását:

```
modprobe tun  
  
systemctl start openvpn@server  
  
systemctl status openvpn*.service
```

Kliens telepítése

1. Lépjön be a fekete gépbe majd telepítse fel az openvpn-t!
2. Az scp segítségével másolja át a szerver gépről a kliens azonosítás során szükséges certificate állományokat a /etc/openvpn könyvtárba!

```
/etc/openvpn/keys/ca.crt
```

```
/etc/openvpn/keys/client.crt
```

```
/etc/openvpn/keys/client.key
```

```
/etc/openvpn/keys/ta.key
```

3. Másolja át a /usr/share/doc/openvpn/examples/sample-config-files/client.conf állományt az /etc/openvpn könyvtárba, majd módosítsa a következőképpen:

```
remote x.x.x.x (a szerver gép IP címe)
```

4. Töltsse be a modprobe segítségével a tun modult, majd indítsa el az openvpn

```
modprobe tun  
  
systemctl start openvpn@client
```

Ellenőrzés

Az ifconfig parancs segítségével kérdezze le a szerveren és a kliensen is a hálózati interfészeket!

pingelje meg a 10.8.0.1-et a fekete gépről!