

Mérési Utasítás

OpenVPN telepítése

OpenVPN kapcsolat létrehozása

szerver telepítése

1. Telepítse fel az openvpn csomagot!

apt-get install openvpn

2. Tömörítse ki az alapértelmezett server konfigurációs állományt!

```
gunzip -c /usr/share/doc/openvpn/examples/sample-config-
files/server.conf.gz > /etc/openvpn/server.conf
```

3. Futtassa le a make-cadir scriptet, mely a szerverez szükséges összes állományt átmásolja a /etc/openvpn/easy-rsa könyvtárba, majd lépjen be az adott könyvtárba.

make-cadir /etc/openvpn/easy-rsa && cd /etc/openvpn/easy-rsa/

4. Hozzon létre szimbolikus linket a openssl-1.0.0.cnf-re

ln -s openssl-1.0.0.cnf openssl.cnf

5. Szerkessze a /etc/openvpn/server.conf-t, és adja meg benne a tanusítványok és kulcsok helyét abszolút elérési úttal.

Any X509 key management system can be used. # OpenVPN can also use a PKCS #12 formatted key file # (see "pkcs12" directive in man page). ca /etc/openvpn/easy-rsa/keys/ca.crt cert /etc/openvpn/easy-rsa/keys/server.crt key /etc/openvpn/easy-rsa/keys/server.key # Diffie hellman parameters.

Generate your own with: # openssl dhparam -out dh1024.pem 1024 # Substitute 2048 for 1024 if you are using # 2048 bit keys. dh /etc/openvpn/dh1024.pem

6. Szerkessze a /etc/openv/easy-rsa/vars fájlt a következőképpen:

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



Széchenyi István Egyetem Győr Távközlési Tanszék

7. Válassza ki forráskét (source) a most szerkesztett vars fájlt. Majd törölje az esetleges fennmaradt/nemhasznált kulcsfájlokat

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

8. Hozza létre a Diffie-Hellman kulcsot.

openssl dhparam 1024 > /etc/openvpn/dh1024.pem

9. Az OpenVPN két csatornát használ. Az egyik a data flow csatorna melyen értelem szerűen az adatok titkosítva utazhatnak a két végpont között. A control csatorna pedig a kapcsolat felépítésére szolgál. Ahhoz, hogy ez is títkosítva kulcs alapon történjen a következő sort kell beszúrni a server.conf-ba:

tls-auth ta.key

Majd létre kell hozni ezt a HMAC szignatúrát.

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

10. A szerver és kliens kulcspárok létrehozása:

```
./build-ca
./build-key-server server
```

11. Kliens kulcspárok létrehozása

cd /etc/openvpn/easy-rsa && source ./vars && ./build-key client

Így létrejött a szerver és 1 kliens kulcspár.

A változtatások érvénybe lépéséhez be kell tölteni a tun modult és újra kell indítani az openvpn-t:

```
modprobe tun
/etc/init.d/openvpn restart
```

Kliens telepítése

- 0. Indítsa el a fehér gépet!
- 1. Másolja át a kliens konfigurációs állományát a fekete gépen:

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
/etc/openvpn/easy-rsa/keys/client.conf
```

[HÁLÓZATOK-BIZTONSÁGA]



Széchenyi István Egyetem Győr Távközlési Tanszék

Majd szerkessze azt a következő képpen:

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote <fekete gép IP címe> 1194
tls-auth ta.key 1
```

2. tömörítse be a szükséges kulcsokat

- /etc/openvpn/easy-rsa/keys/ca.crt
- /etc/openvpn/easy-rsa/keys/client1.crt
- /etc/openvpn/easy-rsa/keys/client1.key
- /etc/openvpn/easy-rsa/keys/client.conf
- /etc/openvpn/easy-rsa/keys/ta.key

a következő paranccsal:

```
tar -C /etc/openvpn/easy-rsa/keys -cvzf /etc/openvpn/client1.tar.gz
{ca.crt,client1.crt,client1.key,client.conf,ta.key}
```

Majd másolja át a már felbootolt fehér gépre a létrejött állományt:

```
scp /etc/openvpn/client1.tar.gz root@feher1:/root
```

3. Telepítse fel az openvpn csomagot a fehér gépre:

apt-get install openvpn

4. Tömörítse ki a /root könyvtárban található client1.tar.gz-t a /etc/openvpn/ könyvtárba.

```
cp /root/client1.tar.gz /etc/openvpn/ && cd /etc/openvpn && tar -xzvf
client1.tar.gz
```

5. Indítsuk el az openvpnt az általunk létrehozott client.conf-al.

```
openvpn --config /etc/openvpn/client.conf &
```

Ha minden jól ment csatlakozott a szerverhez.

Teszt:

Pingelje meg a 10.8.0.1-et a fehér gépről.