



## VPN szerver építése OpenWRT-vel

# VPN szerver építése OpenWRT-vel

Ha szeretnénk gyorsan és biztonságosan elérni az otthoni hálózatunkat, célszerű beüzemelnünk a saját [VPN](#)  szerverünket. A legegyszerűbben ezt az [OpenVPN](#)  illetve egy [OpenWRT](#)-t futtató router segítségével tehetjük meg.



Fontos megjegyzés: Amennyiben korábban telepítettük a **luci-ssl** csomagot a routerünkre, a

**opkg remove luci-ssl && /etc/init.d/uhttpd restart** parancs segítségével távolítsuk el ezt, mert ütközni fog a VPN tanúsítványaival!

Először is az **opkg update** paranccsal frissítsük a tárolókat majd az

```
opkg install openvpn-easy-rsa luci-app-openvpn openvpn-openssl  
nano
```

parancs kiadásával telepítjük a szükséges csomagokat. Ha megvagyunk le kell generálnunk még pár tanúsítványt a VPN szerverünk számára. Az **mkdir /etc/config/openvpn-config** elkészítjük a VPN kiszolgálónk konfigurációs mappáját. Ebbe a mappába az


```
mv /etc/easy-rsa/* /etc/config/openvpn-config/
```

 parancs segítségével átmozgatjuk /etc/easy-rsa mappából a fájlokat, és az **rm -rf /etc/easy-rsa/** paranccsal töröljük azt. Ezután pedig az **ln -s /etc/config/openvpn-config/ /etc/easy-rsa** paranccsal létrehozunk egy, az új mappáról a régre mutató symlinket.

Ezek után nanoval szerkesztenünk kell a **/etc/easy-rsa/vars** fájlt. Ebben a fájlban keressük ki az alábbi sorokat, vegyük ki előlük a **#**-et, valamint értelemszerűen módosítsuk őket:

```
1 set_var EASYRSA_REQ_COUNTRY "Ország kód"  
2 set_var EASYRSA_REQ_PROVINCE "Megye"  
3 set_var EASYRSA_REQ_CITY "Város"  
4 set_var EASYRSA_REQ_ORG "Cégnév vagy személy"
```

```
5 set_var EASYRSA_REQ_EMAIL "E-mail cím"
6 set_var EASYRSA_REQ_OU "Cégnév vagy személy"
```

A `set_var EASYRSA_KEY_SIZE=2048` sor elől is távolítsuk el a `#`-et, de ennek az értékén ne változtassunk. A következő lépésben lépünk be a `/etc/easy-rsa/` könyvtárba, és az `init-pki` paranccsal léptessük érvénybe az előzőleg véghez vitt módosításainkat. Majd az `easyrsa build-ca` paranccsal elkészítjük a tanúsítvány-kibocsájtó tanúsítványunkat. Mivel ezt a tanúsítványt érdemes jól megvédeni, fontos, hogy erős jelszót adjunk meg. Miután elkészült a tanúsítványunk, szükséges még létrehoznunk egy [Diffie-Hellman](#)  kulcsot is. A kulcs létrehozásához egyszerűen csak adjuk ki az `easyrsa gen-dh` parancsot. A Diffie-Hellman kulcs elkészítése, a routerünk teljesítményétől függően körül-belül 10-15 percet is igénybe vehet, úgyhogy legyünk türelmesek. Miután elkészült a Diffie-Hellman kulcsunk az

```
easyrsa gen-req server nopass && easyrsa sign-req server server
```

hozzuk létre a szerverünk tanúsítványát és kulcsát.

A következőkben az alábbi parancsokkal létrehozzuk azt az interfészt amin keresztül a VPN kommunikálni fog:

```
1 uci set network.vpn0="interface"
2 uci set network.vpn0.ifname="tun0"
3 uci set network.vpn0.proto="none"
4 uci set network.vpn0.auto="1"
5 uci commit network
```

A következő parancsokkal pedig beállítjuk a tűzfalt, hogy engedélyezze a VPN kommunikációt:

```
1 uci add firewall rule
2 uci set firewall.@rule[-1].name="Allow-OpenVPN-Inbound"
3 uci set firewall.@rule[-1].target="ACCEPT"
4 uci set firewall.@rule[-1].src="wan"
5 uci set firewall.@rule[-1].proto="udp"
6 uci set firewall.@rule[-1].dest_port="1194"
7 uci add firewall zone
8 uci set firewall.@zone[-1].name="vpn"
9 uci set firewall.@zone[-1].input="ACCEPT"
10 uci set firewall.@zone[-1].forward="ACCEPT"
11 uci set firewall.@zone[-1].output="ACCEPT"
12 uci set firewall.@zone[-1].masq="1"
```

```
13 uci set firewall.@zone[-1].network="vpn0"
14 uci add firewall forwarding
15 uci set firewall.@forwarding[-1].src="vpn"
16 uci set firewall.@forwarding[-1].dest="wan"
17 uci add firewall forwarding
18 uci set firewall.@forwarding[-1].src="vpn"
19 uci set firewall.@forwarding[-1].dest="lan"
20 uci commit firewall
```

Majd az `/etc/init.d/network reload` és az `/etc/init.d/firewall reload` parancsokkal érvénybe léptetjük a változtatásainkat.

Ezek után az alább található parancsokkal engedélyezzük a VPN-ünket (A VPN-ünk neve *myvpn* lesz), beállítjuk a VPN protokollt és a kommunikációs portot:

```
1 uci set openvpn.myvpn="openvpn"
2 uci set openvpn.myvpn.enabled="1"
3 uci set openvpn.myvpn.dev="tun"
4 uci set openvpn.myvpn.port="1194"
```

A következő parancsokkal, pedig megadjuk azt hogy mennyi ideig tartsa életben a kapcsolatot a szerver amennyiben nem kap jelet a kientől, valamint beállítjuk a logfájlok elérési útját:

```
1 uci set openvpn.myvpn.comp_lzo="yes"
2 uci set openvpn.myvpn.status="/var/log/openvpn_status.log"
3 uci set openvpn.myvpn.log="/tmp/openvpn.log"
4 uci set openvpn.myvpn.verb="3"
5 uci set openvpn.myvpn.mute="5"
6 uci set openvpn.myvpn.keepalive="10 120"
7 uci set openvpn.myvpn.persist_key="1"
8 uci set openvpn.myvpn.persist_tun="1"
```

Azért, hogy minimalizáljuk a biztonsági kockázatokat nem szabad rootként futtatni a VPN-ünket, ezért az alábbi két paranccsal megváltoztatjuk a szerver futtató felhasználót:

```
1 uci set openvpn.myvpn.user="nobody"
2 uci set openvpn.myvpn.group="nogroup"
```

A következőkben megadjuk, az előzőleg elkészített tanúsítványok elérési útját az OpenVPN-nek:

```
1 uci set openvpn.myvpn.ca="/etc/config/openvpn-config/pki/ca.crt"
2 uci set openvpn.myvpn.cert="/etc/config/openvpn-config/pki/issued/server."
3 uci set openvpn.myvpn.key="/etc/config/openvpn-config/pki/private/server."
4 uci set openvpn.myvpn.dh="/etc/config/openvpn-config/pki/dh.pem"
```

Most ténylegesen megmondjuk a routerünkön futó OpenVPN-nek hogy szerverként működjön, és beállítjuk, hogy a csatlakozott kliensek lássák egymást a hálózaton:

```
1 uci set openvpn.myvpn.mode="server"
2 uci set openvpn.myvpn.tls_server="1"
3 uci set openvpn.myvpn.server="10.8.0.0 255.255.255.0"
4 uci set openvpn.myvpn.topology="subnet"
5 uci set openvpn.myvpn.route_gateway="dhcp"
6 uci set openvpn.myvpn.client_to_client="1"
```

Most már majdnem megvagyunk a VPN konfigurációjával. Már csak az van hátra, hogy megadjuk a szerverünknek, hogy milyen beállításokat továbbítson a klienseknek csatlakozáskor:

```
1 uci add_list openvpn.myvpn.push="comp-lzo yes"
2 uci add_list openvpn.myvpn.push="persist-key"
3 uci add_list openvpn.myvpn.push="persist-tun"
4 uci add_list openvpn.myvpn.push="user nobody"
5 uci add_list openvpn.myvpn.push="user nogroup"
6 uci add_list openvpn.myvpn.push="topology subnet"
7 uci add_list openvpn.myvpn.push="route-gateway dhcp"
8 uci add_list openvpn.myvpn.push="redirect-gateway def1"
9 uci add_list openvpn.myvpn.push="route 10.10.1.0 255.255.255.0"
10 uci commit openvpn
```

Ezek után nincsen már más dolgunk mint a `/etc/init.d/openvpn start` paranccsal

elindítani majd a `/etc/init.d/openvpn enable` engedélyezni a VPN szolgáltatást.

Ahhoz, hogy a későbbiekben csatlakozni tudjunk a VPN-ünkhöz, meg kell nyitnunk a 1194-es portot az internet felé. Ezt legkönnyebben grafikusán, a <http://openwrt.lan> címen tudjuk megtenni, a Hálózat → Tűzfal → Port Forwards menüpontba navigálva. Itt hozzunk létre egy új továbbítási szabályt: A Protocol-t állítsuk `udp`-re az Source zone legyen `wan`, az External port -ot állítsuk egyaránt `1194`-re, Source zone -nak pedig adjuk meg a `vpn0` zónát.

#### Firewall - Port Forwards - VPN

Általános beállítások | Speciális beállítások

Név: VPN

Protokoll: UDP

Source zone: wan wan: wan6:

External port: 1194  
Match incoming traffic directed at the given destination port or port range on this host

Célzóna: vpn vpn0:

Internal IP address: bármely  
Redirect matched incoming traffic to the specified internal host

Internal port: 1194  
Redirect matched incoming traffic to the given port on the internal host

Most már a szerverünk készen áll a kliensek fogadására, itt az idő, hogy létrehozzuk a kliens kulcsainkat és a kliensek `.ovpn` fájlját. Kliens-kulcsokat az `easyrsa build-client-full felhasználónév nopass` paranccsal tudjuk létrehozni.

A lentebb található `openvpn` fájl megfelelő helyeire másoljuk be a kulcsainkat, majd mentjük el `.ovpn` kiterjesztéssel, és ha mindent jól csináltunk a `sudo openvpn felhasználónév.ovpn` parancs kiadásával, csatlakozni is tudunk a saját VPN-ünkhöz.

```
1 dev tun
2 proto udp
3
4 <ca>
5 -----BEGIN CERTIFICATE-----
6 ca.crt (/etc/easy-rsa/pki/ca.crt)
```

```
7  -----END CERTIFICATE-----
8
9  </ca>
10
11 <cert>
12 -----BEGIN CERTIFICATE-----
13 felhasználónév.crt (/etc/easy-rsa/pki/issued/felhasználónév.crt)
14 -----END CERTIFICATE-----
15
16 </cert>
17
18 <key>
19 -----BEGIN PRIVATE KEY-----
20 felhasználónév.key (/etc/easy-rsa/pki/private/felhasználónév.key)
21 -----END PRIVATE KEY-----
22
23 </key>
24
25 client
26 float
27 remote-cert-tls server
28 remote example.hu 1194
```

A tartalom PenguinPit Creative Commons Nevezd meg! - Ne add el! licenc alatt érhető el. | Futtatja: [Wiki.js](#)