

## Konfiguracja VPN

### Serwer

#### 1. Instalacja pakietów

```
apt-get install bridge-utils openvpn libssl-dev openssl
```

#### 2. Konfiguracja mostka sieciowego z interfejsem eth0

Plik: /etc/network/interfaces

Założenia adres lokalny serwera: 192.168.0.160

```
auto br0
iface br0 inet static
    address 192.168.0.160
    netmask 255.255.255.0
    gateway 192.168.0.1
    network 192.168.0.0
    broadcast 192.168.0.255
    bridge_ports eth0
    dns-nameservers 8.8.8.8 4.4.4.4
```

#### 3. Włączenie forwardowania pakietów pomiędzy interfejsami

Plik: /etc/sysctl.conf

Upewnić się, że jest następująca linia:

```
net.ipv4.ip_forward=1
```

#### 4. Przygotowania katalogu do generowania kluczy i certyfikatów

```
apt-get install easy-rsa
make-cadir /etc/openvpn/easy-rsa
```

#### 5. Ustawienie zmiennych niezbędnych do wygenerowania certyfikatu

Plik: /etc/openvpn/easy-rsa/vars

```
export KEY_COUNTRY="PL"
export KEY_PROVINCE="Podlaskie"
export KEY_CITY="Białystok"
export KEY_ORG="Politechnika Białostocka"
export KEY_EMAIL="a@pb.edu.pl"
export KEY_OU="PB"
```

#### 6. Wygenerowanie kluczy serwera:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pktool --initca
./pktool --server server
cd keys
openvpn --genkey --secret ta.key
```

#### 7. Skopiowanie kluczy do katalogu /etc/openvpn

```
cp server.crt server.key ca.crt dh2048.pem ta.key /etc/openvpn/
```

## 8. Wygenerowanie certyfikatów klienta

```
cd /etc/openvpn/easy-rsa
source vars
```

```
./pkitool client-name, czyli np. ./pkitool jan-kowalski
```

## 9. Utworzenie skryptów startujących/stopujących usługę.

Plik: /etc/openvpn/up.sh

```
#!/bin/sh
```

```
BR=$1
```

```
DEV=$2
```

```
MTU=$3
```

```
/sbin/ifconfig $DEV mtu $MTU promisc up
```

```
/sbin/brctl addif $BR $DEV
```

Plik: /etc/openvpn/up.sh

```
#!/bin/sh
```

```
BR=$1
```

```
DEV=$2
```

```
/sbin/brctl delif $BR $DEV
```

```
/sbin/ifconfig $DEV down
```

oraz ustawienie praw do nich:

```
sudo chmod 755 /etc/openvpn/down.sh
```

```
sudo chmod 755 /etc/openvpn/up.sh
```

## 10. Konfiguracja serwera VPN

Skopiować przykładowy (dostarczany z pakietem) plik do katalogu /etc/openvpn

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

i rozpakowanie

```
gzip -d /etc/openvpn/server.conf.gz
```

Zmienić w pliku: /etc/openvpn/server.conf

```
;dev tap
```

```
dev tun
```

```
na
```

```
dev tap0
```

```
;dev tun
```

```
dh dh1024.pem
```

```
na
```

```
dh dh2048.pem
```

```
server 10.8.0.0 255.255.255.0
```

```
na
```

```

;server 10.8.0.0 255.255.255.0

;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100
na
server-bridge 192.168.0.160 255.255.255.0 192.168.0.161 192.168.0.170
;OpenVPN server will assign DHCP addresses between 192.168.0.161-192.168.0.170 to connecting
clients

;push "route 192.168.10.0 255.255.255.0"
na
push "route 192.168.0.1 255.255.255.0"

;push "redirect-gateway def1 bypass-dhcp"
na
push "redirect-gateway def1 bypass-dhcp"

;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"
na
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 8.8.8.8"

;tls-auth ta.key 0 # This file is secret
na
tls-auth ta.key 0 # This file is secret

;user nobody
;group nogroup
na
user nobody
group nogroup

```

i na końcu pliku dodać

```

up "/etc/openvpn/up.sh br0"
down "/etc/openvpn/down.sh br0"
script-security 3

```

11. Zrestartować usługę openvpn

```

service openvpn restart

```

## Konfiguracja klienta

1. Skopiować z serwera pliki:

```

/etc/openvpn/ca.crt
/etc/openvpn/ta.key

```

*/etc/openvpn/easy-rsa/keys/client-name.crt*  
*/etc/openvpn/easy-rsa/keys/client-name.key*

2. W menadżerze połączeń sieciowych ustawić połączenie.