Instytut Tele- i Radiotechniczny

Centrum Badawcze Technologii Teleinformatycznych

Modem komunikacyjny

Instrukcja konfiguracji serwera i klienta OpenVPN

Wersja dokumentu: 3

Obowiązuje od: 16.04.2019

Spis treści

1. Wprowadzenie

1.1. Symbole

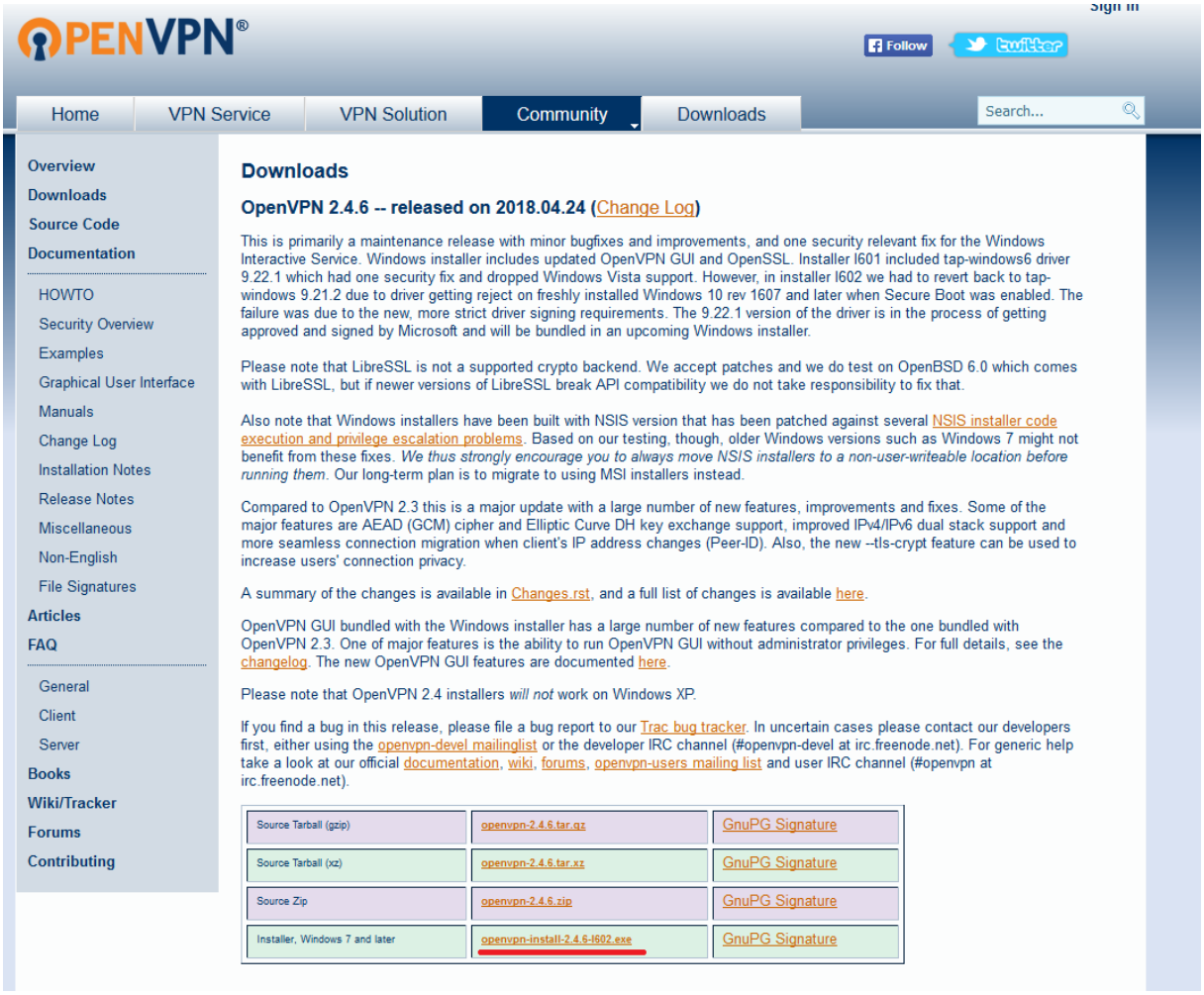
Znak ostrzeżenia elektrycznego wskazujący na ważną informację związaną z obecnością zagrożenia, które może spowodować porażenie prądem elektrycznym.

Znak ostrzeżenia, wskazujący na ważną informację związaną z zagrożeniem, które mogłoby spowodować uszkodzenie lub niewłaściwe działanie urządzenia.

Znak informacyjny, wskazujący na wyjaśnienie istotnych cech i parametrów urządzenia.

2. Wymagane oprogramowanie dla klienta

Na komputerze z systemem Windows należy zainstalować oprogramowanie *openvpnGUI*, które można znaleźć na stronie **https://openvpn.net/index.php/open-source/downloads.html**



Po pobraniu instalatora instalujemy program z domyślnymi ustawieniami. Podczas pierwszego uruchomienia programu *openvpnGUI* utworzony zostanie folder „config" znajdujący się w katalogu: *(home)/OpenVpn/config*. W tym folderze będą trzymane pliki konfiguracyjne klienta.

Na urządzeniu z systemem Linux należy pobrać aplikację „openvpn" poleceniem

```
sudo apt-get install openvpn
```

3. Konfiguracja serwera

Rozpakowujemy przykładowy plik konfiguracyjny, który następnie będziemy zmieniali:

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

Edytujemy plik /etc/openvpn/server.conf :

1. Podanie lokalizacji certyfikatów

```
# 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/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key # This file should be kept secret
```

2. Zmieniamy długość klucza RSA na 2048

```
# 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 dh2048.pem
```

3. Przekierowanie ruchu internetowego (usuwamy średnik przy *push „redirect-gateway def1 bypass-dhcp”*)

```
# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
push „redirect-gateway def1 bypass-dhcp”
```

4. Servery DNS (usuwamy średniki przy push”dhcp-option DNS… ”)

```
# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses. CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
push „dhcp-option DNS XXX.XXX.XXX.XXX”
push „dhcp-option DNS XXX.XXX.XXX.XXX”
```

5. Ustawiamy prawa dostępu (usuwamy średniki przy wpisach *user* i *group*)

```
# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
user nobody
group nogroup
```

6. Komunikacja klient-klient (usunąć średnik)

```
# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
client-to-client
```

4. Przekierowanie pakietów

Zezwalamy na przekazywanie pakietów:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
nano /etc/sysctl.conf
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

5. Generowanie kluczy i certyfikatów serwera

4.1. Easy-rsa

W celu pobrania oprogramowania *easy-rsa* klonujemy repozytorium git.

```
git clone https://github.com/OpenVPN/easy-rsa-old.git
```

Tworzymy folder */etc/openvpn/easy-rsa/* i kopiujemy zawartość sklonowanego z repozytorium folderu *./easy-rsa-old/easy-rsa/2.0/** do folderu */etc/openvpn/easy-rsa/**.

Tworzymy katalog

```
mkdir /etc/openvpn/easy-rsa/keys
```

Ustawiamy parametry certyfikatu:

```
nano /etc/openvpn/easy-rsa/vars


# This variable should point to
# the openssl.cnf file included
```

```
# with easy-rsa.
export KEY_CONFIG=$EASY_RSA/openssl-1.0.0.cnf

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="PL"
export KEY_PROVINCE="Mazowieckie"
export KEY_CITY="Warszawa"
export KEY_ORG="ITR"
export KEY_EMAIL="itr@itr.org.pl"
export KEY_OU="ITR"
export KEY_NAME="server"
```

5.2. Klucz Diffie-Hellman

Tworzymy klucz Diffie-Hellman

```
openssl dhparam --out /etc/openvpn/dh2048.pem 2048
```

5.3. Certyfikat CA

Tworzymy certyfikat CA

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

Potwierdzamy enterem wszystkie decyzje.

Generujemy autoryzacyjny klucz tls

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

5.4. Certyfikat i klucz dla servera

Tworzymy certyfikat i klucz dla serwera (pozostając w katalogu /etc/openvpn/easy-rsa)

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

Powinniśmy otrzymać komunikat

```
……
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

6. Uruchomienie serwera vpn

Kopiujemy utworzone klucze i certyfikaty do katalogu głównego OpenVPN, a następnie uruchamiamy server

```
cp /etc/openvpn/easy-rsa/keys/{server.crt,server.key,ca.crt} /etc/openvpn
service openvpn start
```

Innym sposobem uruchomienia serwera jest przejście do katalogu:

```
cd /etc/openvp
```

I wykonanie polecenia

```
openvpn ./server.conf
```

7. Tworzenie profilu klienta

7.1. Generowanie klucza i certyfikatu

Będąc w katalogu /etc/openvpn/easy-rsa tworzymy klucz i certyfikat dla klienta „pc”

```
./build-key pc
```

7.2. Tworzenie profilu klienta

Kopiujemy przykładową konfigurację przed edytowaniem

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

nano /etc/openvpn/easy-rsa/keys/pc.ovpn
```

Ustawiamy adres ip serwera

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote ADRES_IP_SERWERA 1194
;remote my-server-2 1194
```

Zmniejszamy przywileje dla użytkownika i grupy przez usunięcie średników przed „user” i „group”

```
# Downgrade privileges after initialization (non-Windows only)
user nobody
group nogroup
```

Blokujemy ścieżki do certyfikatów

```
# SSL/TLS parms.
# See the server config file for more
# description. It’s best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
;ca ca.crt
;cert client.crt
;key client.key
```

Zapisujemy zmiany w pliku.

Importujemy CA, certyfikat i klucz do profilu użytkownika:

```
echo '<ca>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn
cat /etc/openvpn/ca.crt >> /etc/openvpn/easy-rsa/keys/pc.ovpn
echo '</ca>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn

echo '<cert>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn
cat /etc/openvpn/easy-rsa/keys/pc.crt | grep -A 100 "BEGIN CERTIFICATE" | grep -B 100
"END CERTIFICATE" >> /etc/openvpn/easy-rsa/keys/pc.ovpn
echo '</cert>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn

echo '<key>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn
cat /etc/openvpn/easy-rsa/keys/pc.key >> /etc/openvpn/easy-rsa/keys/pc.ovpn
echo '</key>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn

echo '< tls-auth>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn
cat /etc/openvpn/ta.key >> /etc/openvpn/easy-rsa/keys/pc.ovpn
echo '</ tls-auth>' >> /etc/openvpn/easy-rsa/keys/pc.ovpn
```

Można też wywołać skrypt:

```
/etc/openvpn/easy-rsa/keys/makeUser.sh <nazwa_profilu>  <adres_ip_servera>
```

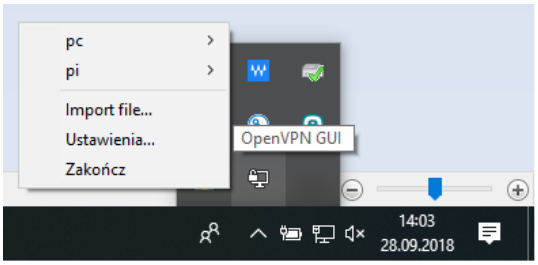
8. Uruchomienie klienta

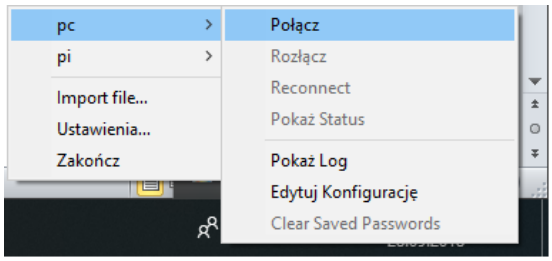
Kopiujemy plik konfiguracyjny „pc.ovp” do odpowiedniego folderu w zależności od zainstalowanego systemu operacyjnego:

8.1. Windows

Plik kopiujemy do folderu (home)/OpenVpn/config/

Uruchamiamy openvpnGUI, naciskamy na ikonę programu prawym przyciskiem myszy, wybieramy odpowiedni profil, a następnie klikamy połącz.





Jeśli wszystko zostało poprawnie skonfigurowane powinien pokazać się komunikat z przydzielonym adresem IP:

8.2. Linux

Plik kopiujemy do folderu /etc/openvpn/client/

A następnie uruchamiamy aplikację kliencką poleceniem

```
cd /etc/openvpn/client
sudo openvpn --config pc.ovpn --daemon
```

9. Firewall

Plik konfigurujący iptables o nazwie „iptables” znajduje się na repozytorium i należy go umieścić w katalogu /etc/network/

W celu automatycznego wczytywania reguł przy starcie systemu tworzymy plik (lub pobieramy go z repozytorium) „firewall-rules.service” w katalogu /etc/systemd/system/ o treści:

```
[Unit]
Description = Apply base firewall rules for router functionality

[Service]
Type=oneshot
ExecStartPre=/etc/network/iptables
ExecStart=/sbin/iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eno1 -j SNAT --to 192.168.1.208

[Install]
```

```
WantedBy=network-pre.target
```

Adres 192.168.1.208 należy zmienić na adres serwera.

Po wykonaniu tych czynności wywołujemy komendy

```
Chmod +x /etc/network/iptables
sudo systemctl enable firewall-rules.service
```

Plik konfiguracyjny można załadować manualnie poleceniem

```
/etc/network/iptables
```

Restartujemy server.

10. Linki

https://www.piotrdyduch.pl/instalacja-i-konfiguracja-serwera-openvpn/

https://nucco.org/2018/05/ubuntu-18-04-chronicles-applying-firewall-rules-on-startup-pre-network.html

https://sekurak.pl/praktyczna-implementacja-sieci-vpn-na-przykladzie-openvpn/