OpenVPN - Instalacja i konfiguracja

Instalacja serwera

Treść

Musimy zainstalować dwa pakiety serwer OpenVpn i easy-rsa do generowania certyfikatów.

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

Tworzymy katalog i kopiujemy skrypyty do tworzenia certyfikatów.

```
mkdir -p /etc/mojeCA;
cp -v /usr/share/easy-rsa/* /etc/mojeCA;
cd /etc/mojeCA;
```

Edytujemy plik vars który będzie nam potrzeby do generowania certyfikatów.

```
vim vars;

export KEY_COUNTRY="PL"                                 # Kod kraju
export KEY_PROVINCE="Slaskie"                 # Województwo
export KEY_CITY="Katowice"                        # Miasto
export KEY_ORG="eDokumenty"                        # Organizacja
export KEY_EMAIL="biuro@edokumenty" # Email
```

Ustawiamy zmienne i tworzymy certyfikat dla CA

Dla pola *Organizational Unit Name* wpisujemy Centrum Certyfikacji

```
source vars;
./clean-all;
./build-ca;
```

Następnie wytwarzamy klucz dla algorytmu Diffie-Hellman. Jest to odpowiednio duża liczba pierwsza wykorzystywana w protokole wymiany kluczy prywatnych wykorzystywanych podczas szyfrowania.

```
./build-dh;
```

Na koniec tworzymy jeszcze plik ta.key, który będzie wykorzystywany do polecenia tls-auth, które dodaje dodatkową warstwę zabezpieczenia. Pozwala na weryfikacje spójności pakietów podczas nawiązywania połączenia.A także nie pozwala na wykrycie portu na którym działa OpenVPN, gdyż skaner rozpozna go jako zamknięty.

```
openvpn --genkey --secret ta.key;
```

Krokiem kolejnym jest utworzenie certyfikatu i klucza serwera. Jako *Organizational Unit* podajemy Serwer OpenVPN (to tylko opis w celu rozróżnienia kluczy). Najważniejsze jest kolejne pole tj. *Common Name*, gdzie wpisujemy nazwę, z którą będą się łączyć klienci. Jeśli mamy swoją firmową domenę możemy przygotować adres w postaci vpn.firma.pl my podamy nazwe *server*. Na pytanie czy podpisać certyfikat wybieramy *y*.

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

Certyfiakty dla klientów

```
./build-key-pass client;
```

Wpisujemy hasło potrzebe do połaczenia.

Jako Common Name podajemy nazwę, na podstawie której OpenVPN rozpozna klienta i przekaże mu odpowiednią konfigurację, w praktyce stosuję inicjał i nazwisko np. jgula, ale tutaj wybraliśmy client. Podpisujemy certyfikat i dodajemy do bazy (y).

Konfiguracja serwera

```
cd /etc/openvpn;
```

Tworzymy plik openvpn.conf i wklejamy konfiguracje zmieniamy adres ip i port

```
vim openvpn.conf;

local 10.0.0.145 # Adres IP naszego serwera
port 1194 # Port na którym nasluchujemy
proto udp
dev tun # Rodzaj tunelu
mssfix 1000
fragment 1000
keepalive 10 120 # Czestotliwosc pakietow keepalive
ca /etc/mojeCA/keys/ca.crt
cert /etc/mojeCA/keys/server.crt
key /etc/mojeCA/keys/server.key
dh /etc/mojeCA/keys/dh2048.pem
tls-auth /etc/mojeCA/ta.key 0
cipher AES-256-CBC
server 10.8.0.0 255.255.255.0 # Adresy IP przydzielane dla klientow
ifconfig-pool-persist ipp.txt
# push "route 10.100.0.0 255.255.255.0" # Trasa do sieci firmowej
# client-config-dir firma # Katalog ustawien klientow
# ccd-exclusive # Dopuszczamy tylko ZNANYCH klientow
```

Przekierowanie pakietów.

```
vim /etc/sysctl.conf;
net.ipv4.ip_forward = 1
sysctl -p;

openvpn --config /etc/openvpn/openvpn.conf;
```

Po poprawnym uruchomieniu serwera powinnniśmy otrzymac komunikat *Initialization Sequence Completed*

Konfiguracja Firewall

Konfiguracja dla klienta Windows

Tworzymy paczke z certyfiakatami.

```
tar -cvf certyfiaty.tar keys/client.key keys/client.crt keys/ca.crt ta.key;
```

Łaczymy się do servera za pomoc np FilleZilla.

- Serwer: sftp://ADRES_SERWERA
- Nazwa użytkownika: user_name
- Hasło: pass
- Port: 22

Przechodzimy do katalogu */etc/mojeCA* i kopiujemy paczkę z certyfikatami.

Kopiujemy pobrane certyfikaty *(client.crt, client.key, ca.crt ta.key)* na dysk C:

Instalujemy OpenVPN GUI i Tap-windows OpenVPN

Uruchamiamy OpenVPN GUI

W trayu klikamy prawy przyciskiem na ikonę i wybieramy *Edytuj konfiguracje*

Wklejamy konfiguracje. Ustawiamy IP i port następnie Połącz.

```
cert "C:\\client.crt"
key "C:\\client.key"
```

```
remote 10.0.0.145 1194
client
fragment 1000
dev tun
proto udp
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
ca C:\\ca.crt
ns-cert-type server # Upewniamy sie ze laczymy sie z serwerem
tls-auth C:\\ta.key 1
cipher AES-256-CBC
verb 3
```