

Installate Debian 7.5, con solo il server SSH.
Configurate un IP statico come segue

```
da root: nano /etc/network/interfaces
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 192.168.1.13
netmask 255.255.255.128
gateway 192.168.1.1
dns-nameservers 192.168.1.7 192.168.1.1
```

Aggiornate il vostro sistema

```
apt-get update
apt-get upgrade
apt-get dist-upgrade
```

Verificate il supporto all'interfaccia TUN

```
test ! -c /dev/net/tun && echo openvpn requires tun support || echo tun is available
```

Installate OpenVPN

```
apt-get install openvpn
```

Impostare Easy RSA

```
cp -prv /usr/share/doc/openvpn/examples/easy-rsa/2.0 /root/easy-rsa
cd /root/easy-rsa
cp vars{,.orig}
```

Impostate i valori di default di Easy-RSA

```
nano ./vars
KEY_SIZE=2048
```

```
KEY_COUNTRY="IT"  
KEY_PROVINCE="ER"  
KEY_CITY="Citta"  
KEY_ORG="la via"  
KEY_EMAIL="email@dominio.tld"
```

Esportate i valori

```
source ./vars
```

Eliminate tutti i certificati precedentemente creati (non dovrebbe essere il nostro caso)

```
./clean-all
```

Generare il certificato CA

```
./build-ca
```

Generare il certificato del server

```
./build-key-server nomedelserver  
Sign the certificate? [y/n]:y  
1 out of 1 certificate requests certified, commit? [y/n]y
```

Generare il certificato PEM Diffie-Hellman

```
./build-dh
```

Generare il certificato per il client

```
./build-key tuodevicename  
Sign the certificate? [y/n]:y  
1 out of 1 certificate requests certified, commit? [y/n]y
```

Generare l'HMAC (Hash-based Message Authentication Code)

```
openvpn --genkey --secret /root/easy-rsa/keys/ta.key
```

Distribuire i certificati

Note sui certificati:

Il certificato pubblico **ca.crt** è necessario sia sui server che sui client

La chiave segreta **ca.key** key è necessaria solo sulla macchina che ha generato la chiave

Il server necessita di: **server.crt**, **dh2048.pem** (pubblica), **server.key** and **ta.key** (privata)

Il client necessita di: **client.crt** (public), **client.key** and **ta.key** (privata)

Spostare i certificati

```
mkdir -p /etc/openvpn/certs
cp -pv /root/easy-rsa/keys/{ca.{crt,key},neutron.{crt,key},ta.key,dh2048.pem}
/etc/openvpn/certs/
```

From:

<https://dwiki.webninja.ovh/> - -- Wiki ICT --

Permanent link:

https://dwiki.webninja.ovh/openvpn_debian?rev=1403942851

Last update: **2021/04/17 19:12**

