OPENVPN SERVER HOW TO IN UBUNTU (tunnel Mode)

Installation

To install **openvpn** in a terminal enter:

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

Server Certificates

Now that the **openvpn** package is installed, the certificates for the VPN server need to be created.

First, copy the `easy-rsa` directory to `/etc/openvpn`. This will ensure that any changes to the scripts will not be lost when the package is updated. You will also need to adjust permissions in the `easy-rsa` directory to allow the current user permission to create files. From a terminal enter:

```
sudo mkdir /etc/openvpn/easy-rsa/
sudo cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
sudo chown -R $USER /etc/openvpn/easy-rsa/
```

Next, edit `/etc/openvpn/easy-rsa/vars` adjusting the following to your environment:

```
export KEY_COUNTRY="MW"
export KEY_PROVINCE="LL"
export KEY_CITY="Lilongwe"
export KEY_ORG="Baobab Health Trust"
export KEY_EMAIL="baobab@baobabhealth.org"
```

Enter the following to create the server certificates:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
cd keys
openvpn --genkey --secret ta.key
sudo cp server.crt server.key ca.crt dh1024.pem ta.key /etc/openvpn/
```

Client Certificates

The VPN client will also need a certificate to authenticate itself to the server. To create the certificate, enter the following in a terminal:

```
cd /etc/openvpn/easy-rsa/
source vars
./pkitool hostname
```

Replace *hostname* with the actual hostname of the machine connecting to the VPN

Copy the following files to the client:

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/hostname.crt
- /etc/openvpn/easy-rsa/keys/hostname.key

- /etc/openvpn/ta.key

Remember to adjust the above file names for your client machine's *hostname***.**

It is best to use a secure method to copy the certificate and key files. The **scp** utility is a good choice, but copying the files to removable media then to the client, also works well.

Configuration

Server Configuration

Now configure the **openvpn** server by creating `/etc/openvpn/server.conf` from the example file. In a terminal enter:

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

Edit `/etc/openvpn/server.conf` changing the following options to:

```
#Change the VPN subnet address to one that makes sense to you (and don't collide with any other net)
server 10.9.0.0 255.255.255.0
#If you wish the computers on the VPN to be able to connect to each other then uncomment
client-to-client
# You can uncomment this out on
# non-Windows systems.
user nobody
group nogroup
#If this is uncommented then a separate log will be written for OpenVPN (If both log lines are uncommented, then syslog is used)
log-append  openvpn.log
#To enable per client configurations uncomment:
client-config-dir client-configs
```

Replace all IP addresses and domain names above with those of your network.

Client Configuration

First, install **openvpn** on the client:

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

Then with the server configured and the client certificates copied to the `/etc/openvpn/` directory, create a client configuration file by copying the example. In a terminal on the client machine enter:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn
```

Now edit `/etc/openvpn/client.conf` changing the following options:

```
dev tun
remote 192.168.5.98 1194
cert hostname.crt
key hostname.key
```

```
tls-auth ta.key 1
```

/etc/init.d/openvpn restart