How to Install OpenVPN Server on Ubuntu

Linux system administration (https://www.webhi.com/how-to/tutorial/linux-sysadmin/), Security (https://www.webhi.com/how-to/tutorial/cyber-security/)

OpenVPN is a free, open-source VPN (Virtual Private Network) software that allows you to securely connect to a remote network over the internet. In this article, we will guide you through the process of installing OpenVPN on an Ubuntu server 18.04/20.04/22.04.

Method 1:

Installing OpenVPN using a Script.

First, get the script and make it executable:

```
$ curl -O https://raw.githubusercontent.com/angristan/openvpn-install/master/openvpn-install.sh
$ chmod +x openvpn-install.sh
```

Then run it:

```
$ ./openvpn-install.sh
```

You need to run the script as root and have the TUN module enabled.

The first time you run it, you'll have to follow the assistant and answer a few questions to setup your VPN server.

When OpenVPN is installed, you can run the script again, and you will get the choice to:

```
root@ubuntu:~# ./openvpn-install.sh
Welcome to OpenVPN-install!
The git repository is available at: https://github.com/angristan/openvpn-install
It looks like OpenVPN is already installed.
What do you want to do?
   1) Add a new user
   2) Revoke existing user
   3) Remove OpenVPN
   4) Exit
Select an option [1-4]:
```

you can add a new user or revoke an existant user .

Method 2 :

Step 1: Update and Upgrade Ubuntu

Before installing any new software, it is always recommended to update and upgrade your Ubuntu system. You can do this by running the following commands:

```
$ sudo apt update
$ sudo apt upgrade
```

Step 2: Install OpenVPN

You can install OpenVPN on Ubuntu by running the following command:

```
$ sudo apt install openvpn easy-rsa
```

Step 3: Generate Certificates and Keys

OpenVPN uses certificates and keys to authenticate clients and servers. You can generate these files by running the easy-rsa script included with OpenVPN. To do this, follow these steps:

```
$ make-cadir ~/openvpn-ca && cd ~/openvpn-ca
```

Edit the `vars` file to set up the Certificate Authority (CA) variables:

```
$ nano ./vars
```

Edit the variables as needed, for example:

```
set_var EASYRSA_REQ_COUNTRY    "US"
set_var EASYRSA_REQ_PROVINCE   "California"
set_var EASYRSA_REQ_CITY       "San Francisco"
set_var EASYRSA_REQ_ORG        "Copyleft Certificate Co"
set_var EASYRSA_REQ_EMAIL      "me@example.net"
set_var EASYRSA_REQ_OU         "My Organizational Unit"
```

```
$ ./easyrsa init-pki
$ ./easyrsa build-ca
$ ./easyrsa gen-req server nopass
$ ./easyrsa sign-req server server
$ ./easyrsa gen-dh
$ openvpn --genkey --secret pki/ta.key
```

The certificates and keys will be created in the `/root/openvpn-ca/pki` directory.

Step 4: Configure OpenVPN

After generating the certificates and keys, you need to configure OpenVPN. To do this, create a new configuration file with the following command:

```
$ zcat \
  /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz \
  | sudo tee /etc/openvpn/server.conf > /dev/null
```

```
$ cp /root/openvpn-ca/pki/{ca.crt,dh.pem,ta.key} /etc/openvpn
$ cp /root/openvpn-ca/pki/issued/server.crt /etc/openvpn
$ cp /root/openvpn-ca/pki/private/server.key /etc/openvpn
```

Edit the following content in the configuration file `/etc/openvpn/server.conf` :

```
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
dh dh.pem
;tls-auth ta.key 0
tls-crypt ta.key
```

Save and close the file.

Enable IP Forwarding

```
$ sudo nano /etc/sysctl.conf
# Uncomment the following line:
net.ipv4.ip_forward=1
```

Then apply the changes:

```
$ sudo sysctl -p
```

Step 5: Start and Enable OpenVPN

You can start and enable the OpenVPN service with the following commands:

```
$ sudo systemctl start openvpn@server
$ sudo systemctl enable openvpn@server
```

The `@server` part specifies the name of the configuration file you created earlier.

Step 6: Configure Firewall

You need to allow OpenVPN traffic through the firewall. You can do this by creating a new rule with the following command:

```
$ sudo ufw allow OpenVPN
```

Step 7: Connect to OpenVPN Server

Now that the OpenVPN server is up and running, you can connect to it from a client computer. To do this, you need to install the OpenVPN client software on your computer and download the client configuration file from the server. You can do this by running the following command on the server:

```
$ ./easyrsa gen-req client1 nopass
$ ./easyrsa sign-req client client1
$ cp pki/private/client1.key /etc/openvpn/client/
$ cp pki/issued/client1.crt /etc/openvpn/client/
$ cp pki/{ca.crt,ta.key} /etc/openvpn/client/
```

Create a client configuration file into the `/root/openvpn-ca` directory to use as your base configuration:

```
$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /root/openvpn-ca/
```

Open this file using `nano` and edit this variables:

```
remote my-server-1 1194 # my-server-1 is the server public IP
user nobody
group nogroup
;ca ca.crt
;cert client.crt
;key client.key
;tls-auth ta.key 1
key-direction 1
```

Now create a script to compile the base configuration with the necessary certificate, key, and encryption files.

```
$ nano config_gen.sh
```

Add the following content:

```
#!/bin/bash
# First argument: Client identifier
KEY_DIR=/etc/openvpn/client
OUTPUT_DIR=/root
BASE_CONFIG=/root/openvpn-ca/client.conf
cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-crypt>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-crypt>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

After writing the script, save and close the config_gen.sh file.

Don't forget to make the file executable by running:

```
$ chmod 700 /root/openvpn-ca/config_gen.sh
$ ./config_gen.sh client1
```

This command will create a new file called `client1.ovpn` in the `/root/` directory.

Copy this file to your client computer and use it to connect to the OpenVPN server.

Conclusion

In this tutorial, we have shown you how to install and configure OpenVPN on an Ubuntu server. With OpenVPN, you can securely connect to a remote network and access its resources from anywhere in the world.