Ubuntu 20.04 LTS Set Up OpenVPN Server In 5 Minutes

Author: Vivek Gite • Last updated: July 19, 2023 • 103 comments

I am a new Ubuntu Linux 20.04 LTS server system administrator. How can I set up an OpenVPN Server on an Ubuntu Linux version 20.04 LTS server to shield my browsing activity from bad guys on public Wi-Fi, encrypt all traffic while connecting to 4G LTE network, and more?

Introduction OpenVPN is extremely popular and a full-featured SSL VPN (Virtual Private Network) software. It implements OSI layer 2 or 3 secure network extension using the SSL/TLS protocol. Like much other popular software, it is open-source, free software and distributed under the GNU GPL. A VPN allows you to connect securely to an insecure public network such as wifi network at the airport or hotel. In many enterprises and government offices, VPN is needed to access your corporate server resources. Another widespread usage to bypass the geo-blocked sites/apps and increase your privacy or safety online. This tutorial provides step-by-step instructions for configuring an OpenVPN server on Ubuntu Linux 20.04 LTS server.

Tutorial requirements	
Requirements	Ubuntu Linux 20.04 LTS
Root privileges	Yes
Difficulty level	Intermediate
Category	OpenVPN
Est. reading time	13 minutes

Tutorial requirements

Table of contents ↓

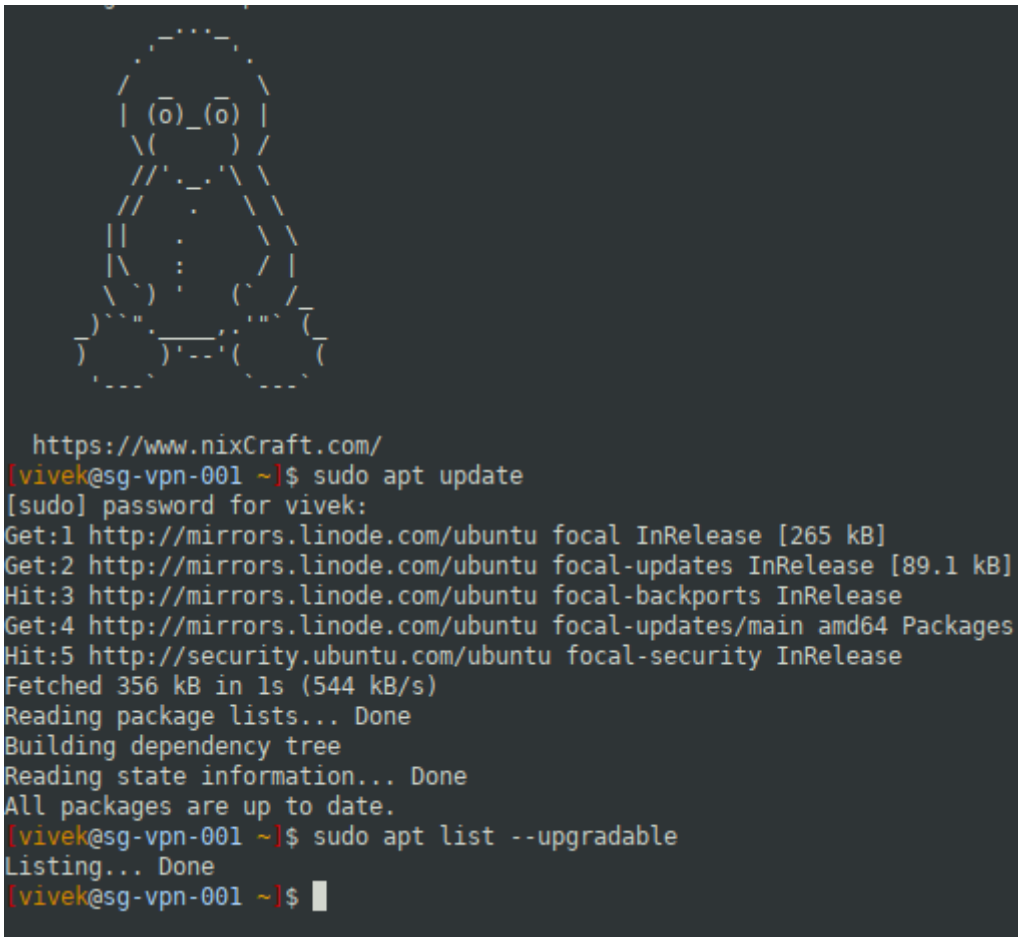
Procedure: Ubuntu 20.04 LTS Set Up OpenVPN Server In 5 Minutes

The steps are as follows:

Step 1 – Update your system

First, run the apt command to apply security updates:

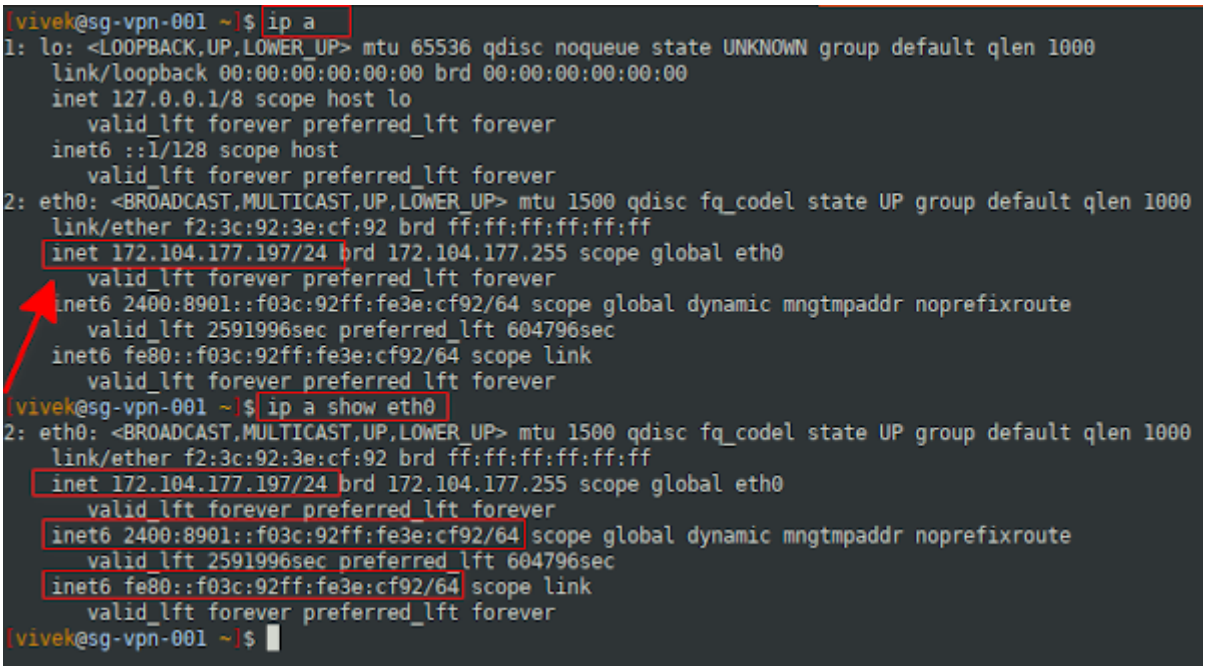
```
sudo apt update
sudo apt upgrade
```



Step 2 – Find and note down your IP address

Use the ip command as follows:

```
ip a
ip a show eth0
```



Alternatively we can run the following dig command/host command to find out our public IP address from Linux command line itself:

```
dig +short myip.opendns.com @resolver1.opendns.com
## Get IPv4 ##
dig -4 +short myip.opendns.com @resolver1.opendns.com
## Find IPv6 ##
dig -6 +short myip.opendns.com @resolver1.opendns.com
## OR ##
dig TXT +short o-o.myaddr.l.google.com @ns1.google.com | awk
-F'"' '{ print $2}'
```

A note about IP address assigned to your server

Most cloud and bare-metal servers have two types of IP address provided by the ISP:

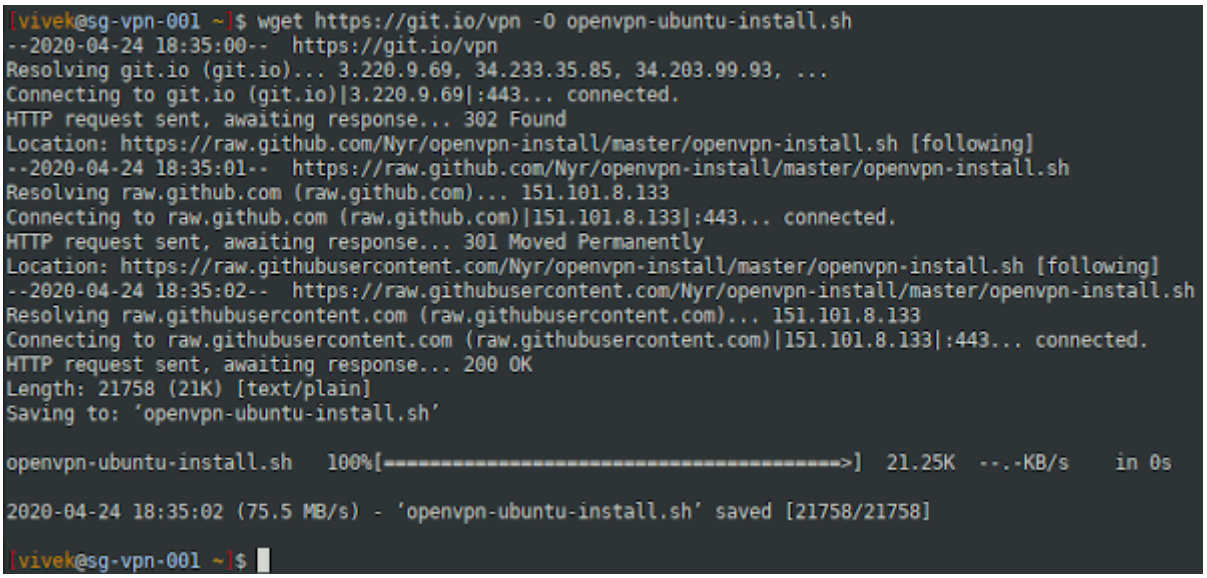
1. **Public static IP address directly** assigned to your box and routed from the Internet. For example, Linode, Digital Ocean, and others give you direct public IP address.
2. Private static IP address directly attached to your server and **your server is behind NAT with public IP** address. For example, AWS EC2/Lightsail give you this kind of NAT public IP address.

The script will automatically detect your networking setup. All you have to do is provide a correct IP address when asked for it.

Step 3 – Download and run openvpn-install.sh script

I am going to use the wget command as follows:

```
wget https://git.io/vpn -O openvpn-ubuntu-install.sh
```



ATTENTION: Do you want **password authentication** along with certificates? Try the following:

```
wget https://raw.githubusercontent.com/angristan/openvpn-inst
```

Now we downloaded the script and it is time to make it executable. Hence, set up permissions using the chmod command:

```
chmod -v +x openvpn-ubuntu-install.sh
mode of 'openvpn-ubuntu-install.sh' changed from 0644 (rw-r--r--) to
0755 (rwxr-xr-x)
```

One can view the script using a text editor such as nano/vim:

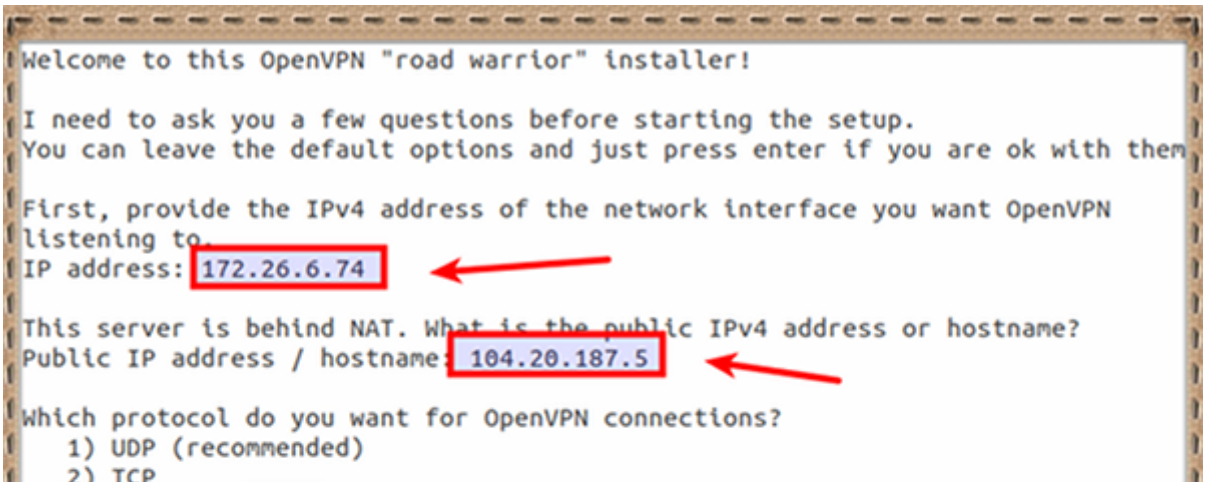
```
nano openvpn-ubuntu-install.sh
```

Run openvpn-ubuntu-install.sh script to install OpenVPN server

Now all you have to do is:

```
sudo ./openvpn-ubuntu-install.sh
```

Sample session **from AWS/Lightsail where my cloud server is behind NAT**:



```
Protocol [1-2]: 1

What port do you want OpenVPN listening to?
Port: 1194

Which DNS do you want to use with the VPN?
   1) Current system resolvers
   2) 1.1.1.1
   3) Google
   4) OpenDNS
   5) Verisign
DNS [1-5] 2

Finally, tell me your name for the client certificate.
Please, use one word only, no special characters.
Client name: desktop

Okay, that was all I needed. We are ready to set up your OpenVPN server now.
Press any key to continue...
```

Sample session from **Linode/DO server where cloud server has direct public IPv4 address**:

```
Welcome to this OpenVPN road warrior installer!

I need to ask you a few questions before starting setup.
You can use the default options and just press enter if you are ok with them.

Which protocol do you want for OpenVPN connections?
   1) UDP (recommended)
   2) TCP
Protocol [1]:

What port do you want OpenVPN listening to?
Port [1194]:

Which DNS do you want to use with the VPN?
   1) Current system resolvers
   2) 1.1.1.1
   3) Google
   4) OpenDNS
   5) NTT
   6) AdGuard
DNS [1]: 2

Finally, tell me a name for the client certificate.
Client name [client]: linuxdesktop

Okay, that was all I needed. We are ready to set up your OpenVPN server now.
Press any key to continue...
```

Hit the [Enter] key

© www.cyberciti.biz

If you downloaded the second script as per step #3, you could set up a password for the client too. Here is how it will look on your screen:

Tell me a name for the client.

The name must consist of alphanumeric character. It may also include an underscore or a dash.

Client name: **linuxdesktop**

Do you want to protect the configuration file with a password?

(e.g. encrypt the private key with a password)

1) Add a passwordless client

2) Use a password for the client

Select an option [1-2]: **2**

⚠️ You will be asked for the client password below ⚠️

I strongly suggest that you always choose the DNS server option as 1.1.1.1 or Google DNS or any other DNS service provided that you trust as per your needs. Make sure you choose fast Geo-distributed DNS servers and reached from anywhere on the Internet. At the end we should see information as follows:

> Your client configuration is available at: /root/linuxdesktop.ovpn
> If you want to add more clients, just run this script again!

How do I start/stop/restart OpenVPN server on Ubuntu 20.04 LTS?

We need to use the systemctl command as follows:

Stop the OpenVPN server

```
sudo systemctl stop openvpn-server@server.service
## OR when using password to protect vpn ##
sudo systemctl stop openvpn@server.service
```

Start the OpenVPN server

```
sudo systemctl start openvpn-server@server.service
## OR when using password to protect vpn ##
sudo systemctl start openvpn@server.service
```

Restart the OpenVPN server after changing configuration options

```
sudo systemctl restart openvpn-server@server.service
## OR when using password to protect vpn ##
sudo systemctl restart openvpn@server.service
```

Show status of the OpenVPN server

```
sudo systemctl status openvpn-server@server.service
## OR when using password to protect vpn ##
sudo systemctl status openvpn@server.service
```

```
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service;
     Active: active (running) since Tue 2020-06-16 09:01:19 UTC;
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 1982 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 2282)
     Memory: 1.1M
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn
             └─1982 /usr/sbin/openvpn --status /run/openvpn-serve

Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Socket Buffers: R=[2129
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: UDPv4 link local (bound
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: UDPv4 link remote: [AF_
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: GID set to nogroup
```

```
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: UID set to nobody
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: MULTI: multi_init calle
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: IFCONFIG POOL IPv6: (IP
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: IFCONFIG POOL: base=10.
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: IFCONFIG POOL LIST
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Initialization Sequence
```

Warning: AWS EC2/Lightsail users need to open the default OpenVPN port UDP/1194 using Amazon EC2 security groups for the Linux instances feature. Run the following ss command to see your OpenVPN port on EC2 cloud instance:

```
sudo ss -tulpn | grep -i openvpn
```

OpenVPN UDP port 1194 opened using AWS EC2/Lightsail Linux instance

Step 4 – Connect an OpenVPN server using iOS/Android/Linux/Windows desktop client

Note for Windows user: Please download scp clients such as PSCP or WinSCP to copy the .ovpn file to your Windows machine. Some versions of windows may come with both ssh/sftp/ssh clients.

On server your will find a client configuration file called /root/linuxdesktop.ovpn. All you have to do is copy this file to your local desktop using the scp command (replace 172.104.177.197 with your actual IP address):

```
scp root@172.104.177.197:/root/linuxdesktop.ovpn .
```

If root is not allowed to log in into the server, try the following scp command:

```
ssh vivek@172.104.177.197 "sudo -S cat
/root/linuxdesktop.ovpn" > linuxdesktop.ovpn
```

Next, provide this file to your OpenVPN client to connect:

1. Apple iOS client
2. Android client
3. Apple MacOS (OS X) client
4. Windows 8/10 client

Tip: Forgotten your .opvn file location on the Ubuntu 20.04 LTS server? Try locating by typing the following command:

```
sudo find / -iname "*.ovpn"
```

Unable to bind service to VPN port?

It would help if you force Linux to bind an IP address that doesn't exist with net.ipv4.ip_nonlocal_bind Linux kernel option. For example, during Ubuntu 20.04

LTS startup (boot) time, OpenVPN IP addresses such as 10.8.0.1/32 may not be available to services such as HTTPD or SSHD. Edit the following file:

```
$ sudo nano /etc/sysctl.d/1000-force-openvpn-bind.conf
## OR when using password to protect vpn ##
$ sudo vim /etc/sysctl.d/1000-force-openvpn-bind.conf
```

Append the following:

```
net.ipv4.ip_nonlocal_bind=1
```

Reload changes using the sysctl command:

```
$ sudo sysctl -p /etc/sysctl.d/1000-force-openvpn-bind.conf
```

Linux Desktop: OpenVPN client configuration

First, install the openvpn client for your desktop using the yum command/dnf command/apt command:

```
sudo dnf install openvpn
```

OR

```
sudo apt install openvpn
```

Next, copy desktop.ovpn as follows:

```
sudo cp linuxdesktop.ovpn /etc/openvpn/client.conf
```

Test connectivity from the CLI:

```
sudo openvpn --client --config /etc/openvpn/client.conf
```

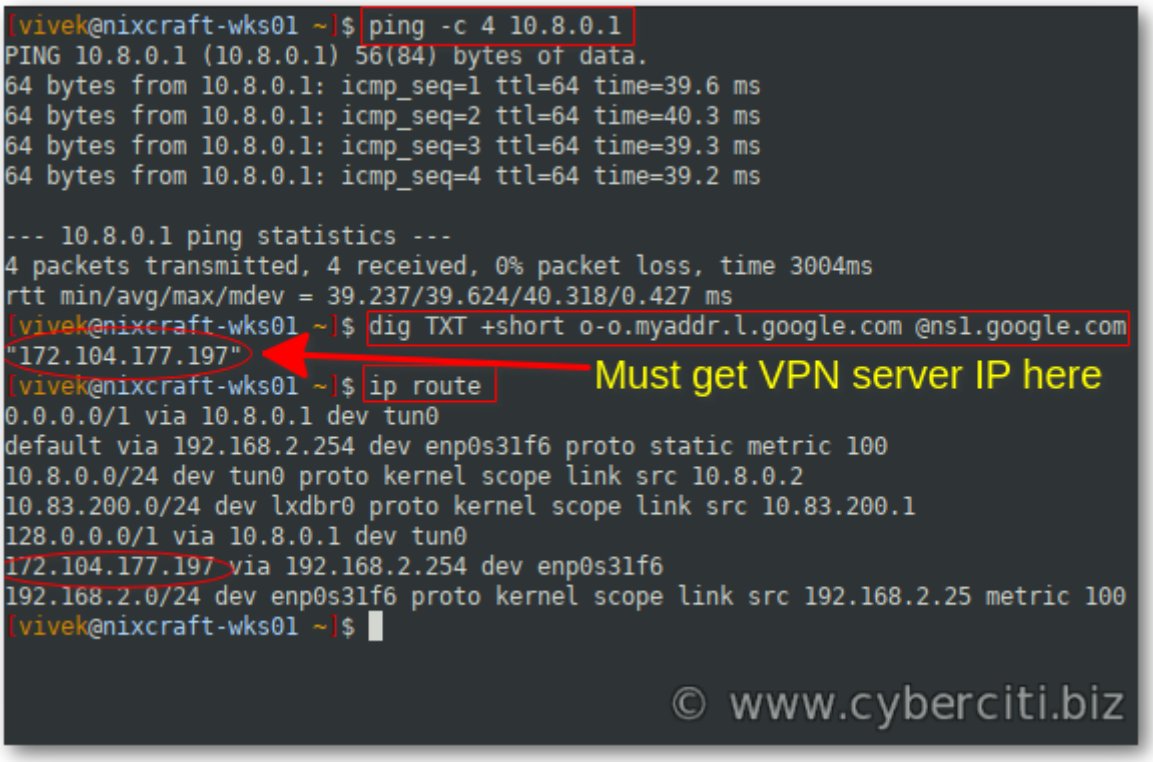
Your Linux system will automatically connect when computer restart using openvpn script/service:

```
sudo systemctl start openvpn@client # <--- start client
service
```

Step 5 – Verify/test the connectivity

Simply visit [this page to check your IP address](#) and it much change to your VPN server IP address. Next, execute the following commands after connecting to OpenVPN server from your Linux desktop:

```
ping 10.8.0.1 #Ping to the OpenVPN server gateway
ip route #Make sure routing setup working
## the following must return public IP address of OpenVPN
server ##
dig TXT +short o-o.myaddr.l.google.com @ns1.google.com
```



Step 6 – How to add or remove a new VPN user

with a certificate

You need to run the same script again for adding or removing a new VPN user to TLS certificate. For instance:

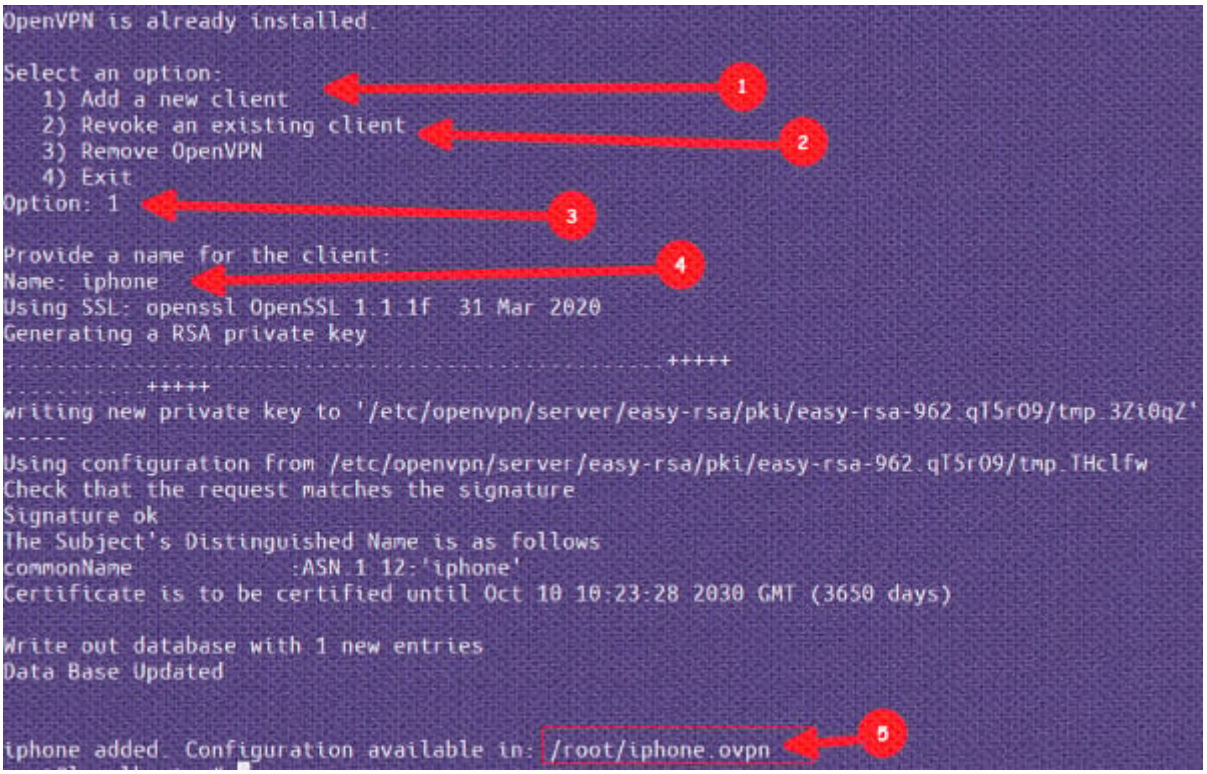
```
$ sudo ./openvpn-ubuntu-install.sh
```

You will see menu as follows:

```
OpenVPN is already installed.

Select an option:
   1) Add a new client
   2) Revoke an existing client
   3) Remove OpenVPN
   4) Exit
Option:
```

Choose option # 1 to add a new VPN client/user and option # 2 to remove the existing VPN client and user. Let us add a new client/user called iphone:



A note about trouble shooting OpenVPN server and client issues

Type the following commands on your Ubuntu 20.04 Linux LTS server. First, check OpenVPN server for errors:

```
sudo journalctl --identifier openvpn
```

```
-- Logs begin at Tue 2020-06-16 08:53:36 UTC, end at Tue 2020-06-16 09:09:57 UTC. --
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenS
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: library versions: OpenSSL 1.1.1f  31 Mar 2020
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Diffie-Hellman initialized with 2048 bit key
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Outgoing Control Channel Encryption: Cipher '
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Outgoing Control Channel Encryption: Using 25
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Incoming Control Channel Encryption: Cipher '
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Incoming Control Channel Encryption: Using 25
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: TUN/TAP device tun0 opened
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: TUN/TAP TX queue length set to 100
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: /sbin/ip link set dev tun0 up mtu 1500
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: /sbin/ip addr add dev tun0 10.8.0.1/24 broadc
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: /sbin/ip -6 addr add fddd:1194:1194:1194::1/6
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Could not determine IPv4/IPv6 protocol. Using
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Socket Buffers: R=[212992->212992] S=[212992-
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: UDPv4 link local (bound): [AF_INET]45.79.125.
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: UDPv4 link remote: [AF_UNSPEC]
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: GID set to nogroup
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: UID set to nobody
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: MULTI: multi_init called, r=256 v=256
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: IFCONFIG POOL IPv6: (IPv4) size=252, size_ipv
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: IFCONFIG POOL: base=10.8.0.2 size=252, ipv6=1
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: IFCONFIG POOL LIST
Jun 16 09:01:19 sg-vpn-001 openvpn[1982]: Initialization Sequence Completed
```

Is firewall rule setup correctly on your server? Use the cat command to see rules:

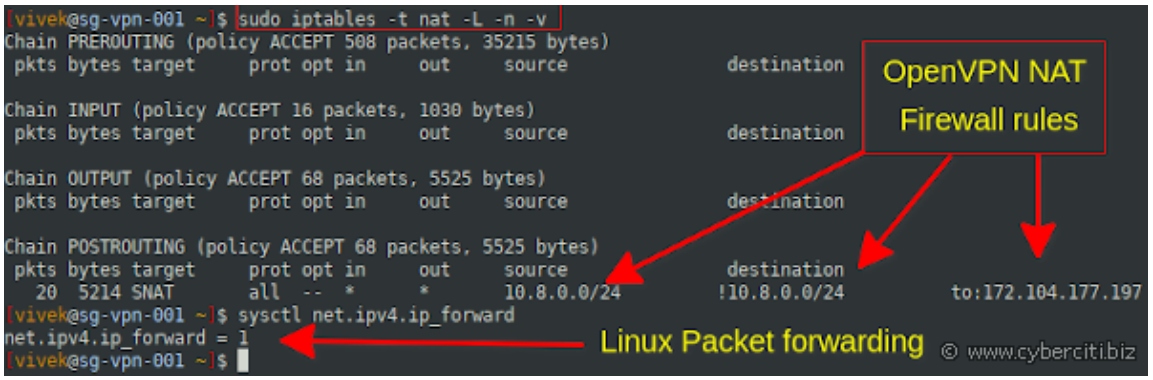
```
sudo cat /etc/systemd/system/openvpn-iptables.service
## OR when using password to protect vpn ##
sudo cat /etc/systemd/system/iptables-openvpn.service
```

Config:

```
[Unit]
Before=network.target
[Service]
Type=oneshot
ExecStart=/sbin/iptables -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT
ExecStart=/sbin/iptables -I INPUT -p udp --dport 1194 -j ACCEPT
ExecStart=/sbin/iptables -I FORWARD -s 10.8.0.0/24 -j ACCEPT
ExecStart=/sbin/iptables -I FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
ExecStop=/sbin/iptables -t nat -D POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT -
ExecStop=/sbin/iptables -D INPUT -p udp --dport 1194 -j ACCEPT
ExecStop=/sbin/iptables -D FORWARD -s 10.8.0.0/24 -j ACCEPT
ExecStop=/sbin/iptables -D FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
ExecStart=/sbin/ip6tables -t nat -A POSTROUTING -s fddd:1194:1194:1194::/64 ! -d fddd:1
ExecStart=/sbin/ip6tables -I FORWARD -s fddd:1194:1194:1194::/64 -j ACCEPT
ExecStart=/sbin/ip6tables -I FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
ExecStop=/sbin/ip6tables -t nat -D POSTROUTING -s fddd:1194:1194:1194::/64 ! -d fddd:11
ExecStop=/sbin/ip6tables -D FORWARD -s fddd:1194:1194:1194::/64 -j ACCEPT
ExecStop=/sbin/ip6tables -D FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
RemainAfterExit=yes
[Install]
WantedBy=multi-user.target
```

Another option is to run iptables command and sysctl command commands to verify NAT rule setup on your server:

```
sudo iptables -t nat -L -n -v
sysctl net.ipv4.ip_forward
sudo cat /etc/sysctl.d/30-openvpn-forward.conf
## OR when using password to protect vpn ##
sudo cat /etc/sysctl.d/99-openvpn.conf
```



NAT Firewall OpenVPN Rules Verification

Insert the rules if not inserted using the following command:

```
sudo systemctl start openvpn-iptables.service
## OR when using password to protect vpn ##
sudo systemctl start iptables-openvpn.service
sudo sysctl -w net.ipv4.ip_forward=1
sudo sysctl -p -f /etc/sysctl.d/30-openvpn-forward.conf
## OR when using password to protect vpn ##
sudo sysctl -p -f /etc/sysctl.d/99-openvpn.conf
```

Is OpenVPN server running and port is open? Use the ss command or netstat command and pidof command/ps command:

```
## 1194 is the openvpn server port ##
netstat -tulpn | grep :1194
## 1194 is the openvpn server port ##
ss -tulpn | grep :1194
## is the openvpn server running? ##
ps aux | grep openvpn
## is the openvpn server running? ##
ps -C openvpn
## find the openvpn server PID ##
pidof openvpn
```

If not running, restart the OpenVPN server:

```
sudo systemctl restart openvpn-server@server.service
```

Look out for errors:

```
sudo systemctl status openvpn-server@server.service
```

Can the Linux desktop client connect to the OpenVPN server machine? First you need to run a simple test to see if the OpenVPN server port (UDP 1194) accepts connections:

```
nc -vu 172.104.177.197 1194
Connection to 172.104.177.197 port [udp/openvpn] succeeded!
```

If not connected it means either a Linux desktop firewall or your router is blocking access to server. Make sure both client and server using same protocol and port, e.g. UDP port 1194.

Conclusion

Congratulations. You successfully set up an OpenVPN server on Ubuntu Linux 20.04 LTS server running in the cloud. See the OpenVPN website here, Ubuntu page here and Github script page here for additional information or use the man command/help command to read docs locally:

```
man openvpn
openvpn --help
# Use the more command/less command as a filter #
openvpn --help | more
```

This entry is **11** of **13** in the **OpenVPN Tutorial** series. Keep reading the rest of the series:

1. How To Setup OpenVPN Server In 5 Minutes on Ubuntu Server
2. Install Pi-hole with an OpenVPN to block ads
3. Update/upgrade Pi-hole with an OpenVPN
4. OpenVPN server on Debian 9/8
5. Import a OpenVPN .ovpn file with Network Manager
6. Ubuntu 18.04 LTS Set Up OpenVPN Server In 5 Minutes
7. CentOS 7 Set Up OpenVPN Server In 5 Minutes
8. Pi-Hole and Cloudflare DoH config
9. Debian 10 Set Up OpenVPN Server In 5 Minutes
10. CentOS 8 OpenVPN server in 5 mintues
11. Ubuntu 20.04 LTS OpenVPN server in 5 mintues
12. Debian 11 set up OpenVPN server in 5 mintues
13. Ubuntu 22.04 LTS Set Up OpenVPN Server In 5 Minutes

About the author: Vivek Gite is the founder of nixCraft, the oldest running blog about Linux and open source. He wrote more than 7k+ posts and helped numerous readers to master IT topics. Join the nixCraft community via RSS Feed or Email Newsletter.

🙄 Was this helpful? Please add a comment to show your appreciation or feedback.