How To Set up OpenVPN Server In 5 Minutes on Ubuntu Linux

Author: Vivek Gite • Last updated: September 10, 2024 • 116 comments

I am a new Ubuntu Linux server user. How do I setup an OpenVPN Server on Ubuntu Linux version 18.04/20.04 LTS or 20.10 server to shield my browsing activity from bad guys on public Wi-Fi, and more?

OpenVPN is a full-featured SSL VPN (virtual private network). It implements OSI layer 2 or 3 secure network extension using the SSL/TLS protocol. It is an open source 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. VPN is also required to access your corporate or enterprise or home server resources. You can bypass geo-blocked site and increase your privacy or safety online. This tutorial provides step-by-step instructions for **configuring an OpenVPN “road warrior” server on Ubuntu Linux 18.04/20.04 LTS (20.10) version including ufw/iptables firewall configuration**. The steps are as follows:

1. Find and note down your public IP address

2. Download openvpn-install.sh script
3. Run openvpn-install.sh to install OpenVPN server
4. Connect an OpenVPN server using iOS/Android/Linux/Windows client
5. Verify your connectivity

> **NOTE:** You need at least Ubuntu Linux 18.04 LTS or higher is needed to complete this tutorial. Older Ubuntu versions such as 14.04/16.04 LTS are no longer supported.

Find your public IP address

Tutorial details	
Difficulty level	Easy
Root privileges	Yes
Requirements	Linux terminal
Category	OpenVPN
Prerequisites	Ubuntu Linux
OS compatibility	Debian • Linux • Ubuntu
Est. reading time	5 minutes

Use any one of the following command to find out your IPv4 public address. If your internface name is eth0 or eth1, enter:

```
$ ip addr show eth0
```

OR

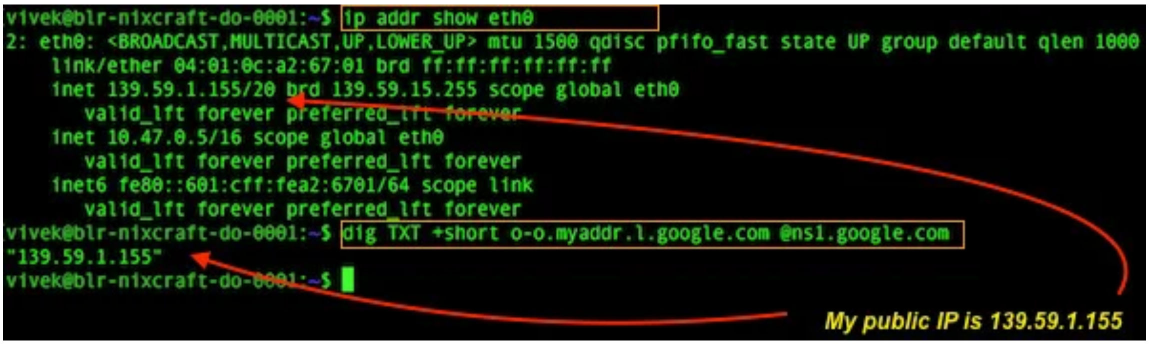
```
$ ip addr show eth1
```

Or use the host command or dig command as follows:

```
$ host myip.opendns.com resolver1.opendns.com
## get IPv4 ##
$ host -4 myip.opendns.com resolver1.opendns.com
```

OR

```
$ dig TXT +short o-o.myaddr.l.google.com @ns1.google.com
## see IPv4 instead of default IPv6 ##
$ dig -4 TXT +short o-o.myaddr.l.google.com @ns1.google.com
```



```
vivek@blr-nixcraft-do-0001:~$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 04:01:0c:a2:67:01 brd ff:ff:ff:ff:ff:ff
    inet 139.59.1.155/20 brd 139.59.15.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.47.0.5/16 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::601:cff:fea2:6701/64 scope link
       valid_lft forever preferred_lft forever
vivek@blr-nixcraft-do-0001:~$ dig TXT +short o-o.myaddr.l.google.com @ns1.google.com
"139.59.1.155"
vivek@blr-nixcraft-do-0001:~$
```

My public IP is 139.59.1.155

Fig.01: Find out your public IPv4 address using the CLI

Note down the public IPv4 address `172.105.102.90` (or IPv6 `2600:3c04::f03c:92ff:fe42:3d72`) i.e. public ip address of your OpenVPN server powered by Ubuntu Linux.

Download openvpn-install.sh script to set up OpenVPN server in 5 minutes on

Ubuntu

Type the following wget command or curl command:

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

wget grabbing the script:

```
--2020-12-09 09:15:57--  https://git.io/vpn
Resolving git.io (git.io)... 34.195.187.253, 52.87.143.234, 34.20
Connecting to git.io (git.io)|34.195.187.253|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.github.com/Nyr/openvpn-install/master/openv
--2020-12-09 09:15:57--  https://raw.github.com/Nyr/openvpn-insta
Resolving raw.github.com (raw.github.com)... 151.101.124.133
Connecting to raw.github.com (raw.github.com)|151.101.124.133|:44
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/m
--2020-12-09 09:15:57--  https://raw.githubusercontent.com/Nyr/op
Resolving raw.githubusercontent.com (raw.githubusercontent.com)..
Connecting to raw.githubusercontent.com (raw.githubusercontent.co
HTTP request sent, awaiting response... 200 OK
Length: 23079 (23K)
Saving to: 'openvpn-install.sh'

openvpn-install.sh  100%[===================>]  22.54K  --.-KB/s

2020-12-09 09:15:57 (36.9 MB/s) - 'openvpn-install.sh saved [2307
```

We can verify script using a text editor such as nano command or vim command:

```
$ nano openvpn-install.sh
```

Running openvpn-install.sh to install OpenVPN server

Type the following command:

```
$ sudo chmod +x openvpn-install.sh
$ sudo bash openvpn-install.sh
```

Make sure you provide needed information:

```
Welcome to this OpenVPN road warrior installer!

Which protocol should OpenVPN use?
   1) UDP (recommended)
   2) TCP
Protocol [1]: 1

What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
   1) Current system resolvers
   2) Google
   3) 1.1.1.1
   4) OpenDNS
   5) Quad9
   6) AdGuard
DNS server [1]: 2

Enter a name for the first client:
Name [client]: iphone

OpenVPN installation is ready to begin.
Press any key to continue...
```

Once you press any key such as [Enter] key, you will see:

```
writing new private key to '/etc/openvpn/server/easy-rsa/pki/easy
-----
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rs
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Dec  7 09:22:17 2030 GMT (36

Write out database with 1 new entries
Data Base Updated

Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020
Generating a RSA private key
....................................+++++
...................+++++
writing new private key to '/etc/openvpn/server/easy-rsa/pki/easy
-----
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rs
```

```
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'iphone'
Certificate is to be certified until Dec  7 09:22:17 2030 GMT (36

Write out database with 1 new entries
Data Base Updated

Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rs

An updated CRL has been created.
CRL file: /etc/openvpn/server/easy-rsa/pki/crl.pem



Created symlink /etc/systemd/system/multi-user.target.wants/openv
Created symlink /etc/systemd/system/multi-user.target.wants/openv

Finished!

The client configuration is available in: /root/iphone.ovpn
New clients can be added by running this script again.
```

Viewing and Seting up OpenVPN Server In 5 Minutes on Ubuntu Firewall Rules

That is all. Your OpenVPN server has been configured and ready to use. You can see added firewall rules `/etc/systemd/system/openvpn-iptables.service` file:

```
$ sudo systemctl cat openvpn-iptables.service
```

Sample rules. Please do not edit them:

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

You can view your openvpn server config file generated by the script as follows (agin do not edit this file by hand as it will break things for you):

```
$ sudo more /etc/openvpn/server/server.conf
```

Sample openvpn config:

```
local 172.105.102.90
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
```

```
auth SHA512
tls-crypt tc.key
topology subnet
server 10.8.0.0 255.255.255.0
server-ipv6 fddd:1194:1194:1194::/64
push "redirect-gateway def1 ipv6 bypass-dhcp"
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120
cipher AES-256-CBC
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 3
crl-verify crl.pem
explicit-exit-notify
```

How do I start/stop/restart OpenVPN server on Ubuntu Linux 18.04/20.04 LTS and 20.10?

Run the following systemctl command to stop the OpenVPN service:

```
$ sudo systemctl stop openvpn-server@server.service
```

Want to start it again? Try:

```
$ sudo systemctl start openvpn-server@server.service
```

The command to restart the OpenVPN service:

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

View status of your OpenVPN systemd based service:

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

```
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service;
     Active: active (running) since Wed 2020-12-09 09:22:18 UTC;
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 2017 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 4610)
     Memory: 1.2M
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn
             └─2017 /usr/sbin/openvpn --status /run/openvpn-serve

Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: Socket Buffers:
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: UDPv4 link loca
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: UDPv4 link remo
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: GID set to nogr
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: UID set to nobo
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: MULTI: multi_in
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: IFCONFIG POOL I
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: IFCONFIG POOL:
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: IFCONFIG POOL L
Dec 09 09:22:18 nixcraft-ubuntu-vm openvpn[2017]: Initialization
```

OpenVPN client configuration

On server your will find a client configuration file called ~/iphone.ovpn (or whatever name given during installation). Use the find command to locate OpenVPN config file:

```
$ sudo find / -type f -name "iphone.ovpn"
$ sudo find / -type f -name "*.ovpn" -ls
```

Now, all you have to do is copy this file to your local desktop using the scp and provide this file to your OpenVPN client to connect (replace iphone.ovpn and root username as per your set up):

```
{client-desktop:~}$ scp root@172.105.102.90:~/iphone.ovpn .
```

If you cannnot run the scp command as root then log in as a normal user on your server. For example:

```
{client-desktop:~}$ ssh {user}@172.105.102.90
{client-desktop:~}$ ssh vivek@172.105.102.90
```

Find the location of opvn file on the server:

```
$ sudo find / -type f -name "*.ovpn" -ls
```

```
34605854      4 -rw-r--r--   1 root     root         2774 May  6
```

Then copy that file using the cp command in your home directory (say /home/vivek/ on the server itself):

```
$ sudo cp /root/desktopclient.ovpn /home/vivek/
```

Now type the scp from your desktop:

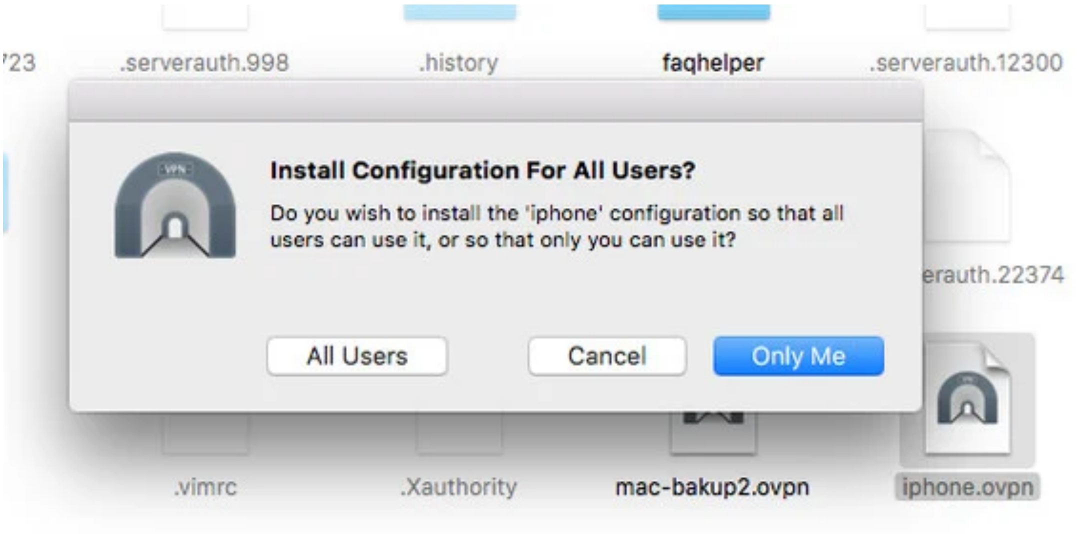
```
{client-desktop:~}$ scp vivek@172.105.102.90:/home/vivek/
desktopclient.ovpn .
```

Next, you need to download OpenVPN client as per your operating system or mobile device:

- Client for Apple iOS version 6.x or above
- Android client
- Apple MacOS (OS X)
- Windows 8/10 OpenVPN client

macOS/OS X OpenVPN client configuration

Just double click on iphone.ovpn file and it will open in your tunnelblick client > Click on the “Only me” to install it:



Install Configuration For All Users?

Do you wish to install the 'iphone' configuration so that all users can use it, or so that only you can use it?

Fig.03: MacOS / OS X openvpn client configuration

Once installed click on Connect button and you will be online. Use the following command on MacOS client to verify that your public IP changed to the VPN server IP:

```
$ dig TXT +short o-o.myaddr.l.google.com @ns1.google.com
```

You can ping to OpenVPN server private IP using the ping command:

```
$ ping 10.8.0.1
```

Linux OpenVPN client configuration

First, install the openvpn client, enter:

```
$ sudo yum install openvpn
```

OR

```
$ sudo apt install openvpn
```

Next, copy iphone.ovpn as follows:

```
$ sudo cp iphone.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 /etc/init.d/openvpn script:

```
$ sudo /etc/init.d/openvpn start
```

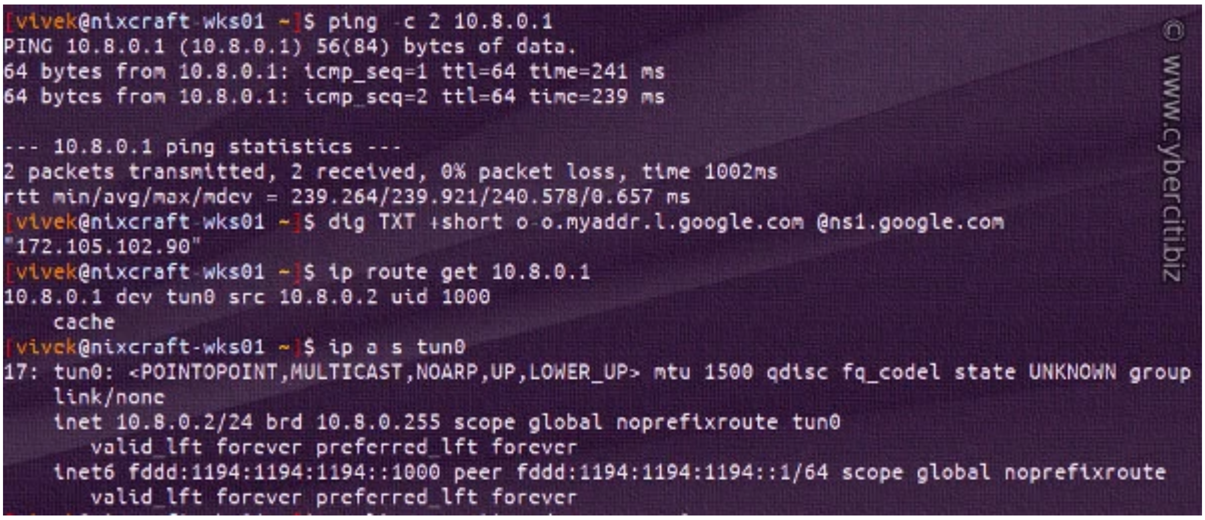
For systemd based system, use the following command:

```
$ sudo systemctl start openvpn@client
```

Test the OpenVPN connectivity on Linux desktop:

```
$ ping 10.8.0.1 #Ping to OpenVPN server gateway using the ping
```

```
command
$ ip route #Make sure routing setup using the ip command $ ip
route get 10.8.0.1
#Make sure your public IP set to OpenVPN server
$ dig TXT +short o-o.myaddr.l.google.com @ns1.google.com
```



```
[vivek@nixcraft-wks01 ~]$ ping -c 2 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=241 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=239 ms

--- 10.8.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 239.264/239.921/240.578/0.657 ms
[vivek@nixcraft-wks01 ~]$ dig TXT +short o-o.myaddr.l.google.com @ns1.google.com
"172.105.102.90"
[vivek@nixcraft-wks01 ~]$ ip route get 10.8.0.1
10.8.0.1 dev tun0 src 10.8.0.2 uid 1000
    cache
[vivek@nixcraft-wks01 ~]$ ip a s tun0
17: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group
    link/none
    inet 10.8.0.2/24 brd 10.8.0.255 scope global noprefixroute tun0
       valid_lft forever preferred_lft forever
    inet6 fddd:1194:1194:1194::1000 peer fddd:1194:1194:1194::1/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
```

FreeBSD OpenVPN client configuration

First, install the openvpn client using the pkg command:

```
$ sudo pkg install openvpn
```

Next, copy iphone.ovpn as follows:

```
$ mkdir -p /usr/local/etc/openvpn/
$ sudo cp iphone.ovpn /usr/local/etc/openvpn/client.conf
```

Edit /etc/rc.conf and add the following:

```
openvpn_enable="YES"
openvpn_configfile="/usr/local/etc/openvpn/client.conf"
```

Start the OpenVPN service:

```
$ sudo /usr/local/etc/rc.d/openvpn start
```

Verify it:

```
#Ping to OpenVPN server gateway from BSD
$ ping 10.8.0.1
#Make sure routing setup
$ netstat -nr
#Make sure your public IP set to OpenVPN server
$ dig +short myip.opendns.com @resolver1.opendns.com
```

How do I add a new client?

For demo purpose I added a new device called googlephone. Let us add one more device called googlephone by running the script again:

```
$ sudo bash openvpn-install.sh
```

```
Looks like OpenVPN is already installed

What do you want to do?
   1) Add a cert for a new user
   2) Revoke existing user cert
   3) Remove OpenVPN
   4) Exit
Select an option [1-4]:
```

Select option 1 and type googlephone as a client name:

```
Tell me a name for the client cert
```

```
Please, use one word only, no special characters
Client name: googlephone
Generating a 2048 bit RSA private key
.........+++
...........................................................................
writing new private key to '/etc/openvpn/easy-rsa/pki/private/googlephone.k
-----
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'googlephone'
Certificate is to be certified until Sep 25 07:31:46 2027 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Client googlephone added, certs available at ~/googlephone.ovpn
```

Now you can use googlephone.ovpn with Google Android phone. You can add as many users you want using this method.

How do I delete/revoke existing user certificate?

Run the script:

```
$ sudo bash openvpn-install.sh
```

Here is how it looks:

```
Looks like OpenVPN is already installed

What do you want to do?
   1) Add a cert for a new user
   2) Revoke existing user cert
   3) Remove OpenVPN
   4) Exit
Select an option [1-4]:
```

Type 2 option and you will see a list of all the existing client certificate you want to revoke:

```
Select the existing client certificate you want to revoke
     1) iphone6
     2) googlephone
     3) delllaptop
     4) macbook
Select one client [1-4]: 2
```

Sample outputs when I revoked googlephone certificate:

```
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.cnf
Revoking Certificate 09.
Data Base Updated
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.cnf

An updated CRL has been created.
CRL file: /etc/openvpn/easy-rsa/pki/crl.pem



Certificate for client googlephone revoked
```

Viewing log file

Try the journalctl command:

```
$ journalctl -u openvpn
```

Conclusion

And there you have it, OpenVPN server installed in five minutes to increase your privacy. Please see OpenVPN project and road warrior installer Linux script. Let us know if you have any problems or comments in the comments section below.

This entry is **1** 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