

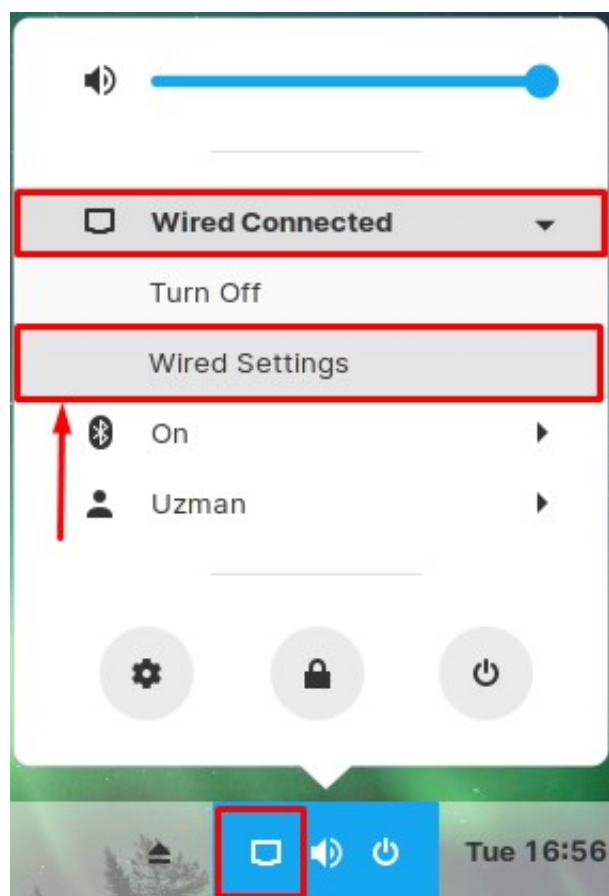
How to Setup PureVPN on Zorin OS

Configuring PureVPN on Zorin OS requires only a few simple steps. Check out the following guide to learn how to set up PureVPN on Zorin OS using different protocols.

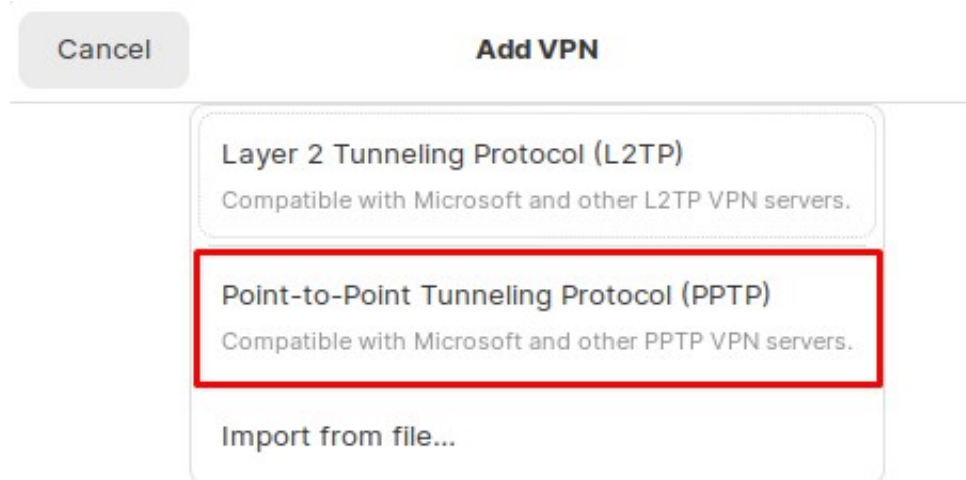
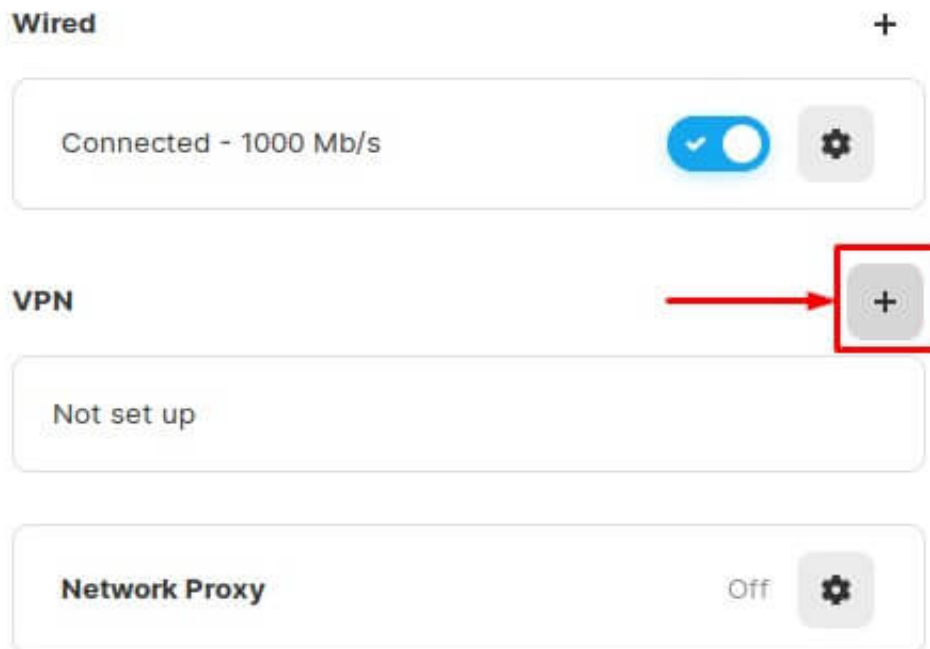
PPTPL2TPSSTPOpenVPN

1 Select the following options:

- Click **Wired Connected**
- Go to **Wired Settings**



2 Click the '+' icon to add a VPN connection and select '**Point-to-Point Tunneling Protocol (PPTP)**' option.



3 When a new window appears, complete the fields as below:

PureVPN Support

Solution of Your Problems

<https://support.purevpn.com>

- Connection name: **PureVPN**
- Gateway: **pointtoserver.com** (you can use your desired server address here, in order to see the complete list [click here](#))
- Username: **Your VPN username**
- Password: **Your VPN password**

The screenshot shows a configuration window for adding a VPN. At the top, there are buttons for 'Cancel', 'Add VPN', and 'Add'. Below these are tabs for 'Identity', 'IPv4', and 'IPv6'. The 'Identity' tab is selected. The 'Name' field contains 'PureVPN'. Under the 'General' section, the 'Gateway' field contains 'usca.pointtoserver.com'. Under the 'Optional' section, the 'User name' field contains 'purevpn0sxxxx', the 'Password' field is masked with dots, and there is a 'Show password' checkbox. At the bottom right, there is an 'Advanced...' button with a gear icon.

4 **Now**, go to the '**Advanced...**'

Only allow the following options:

- MSCHAP
- MSCHAP2

Also, select the following:

PureVPN Support

Solution of Your Problems

<https://support.purevpn.com>

- Allow BSD data compression
- Allow Deflate data compression
- Use TCP header compression

PPTP Advanced Options

Authentication

Allow the following authentication methods:

- MSCHAP
- MSCHAPv2
- EAP

Security and Compression

Use Point-to-Point encryption (MPPE)

Security: All Available (Default) ▾

Allow stateful encryption

- Allow BSD data compression
- Allow Deflate data compression
- Use TCP header compression

Echo

Send PPP echo packets

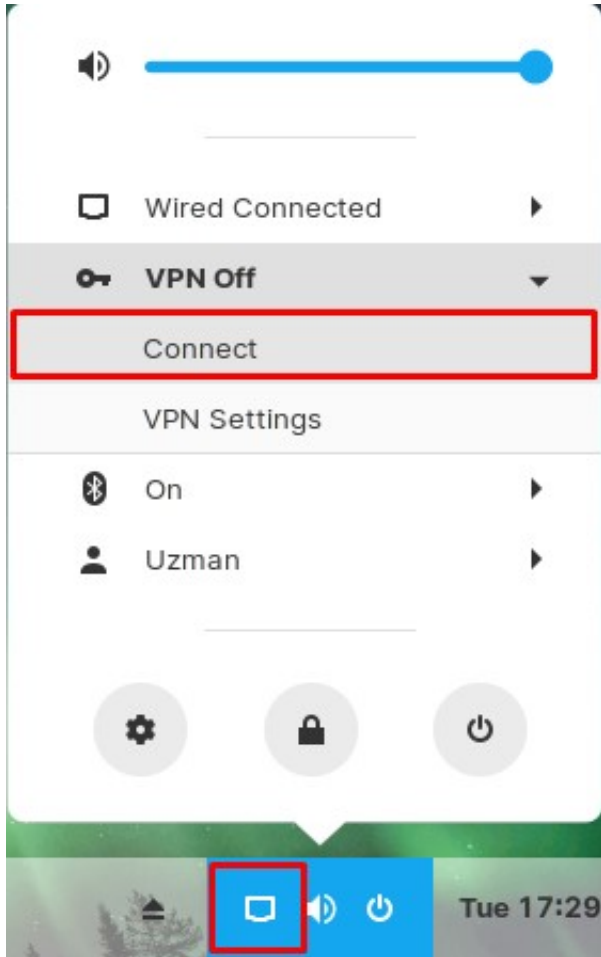
Misc

Use custom unit number: 0 - +

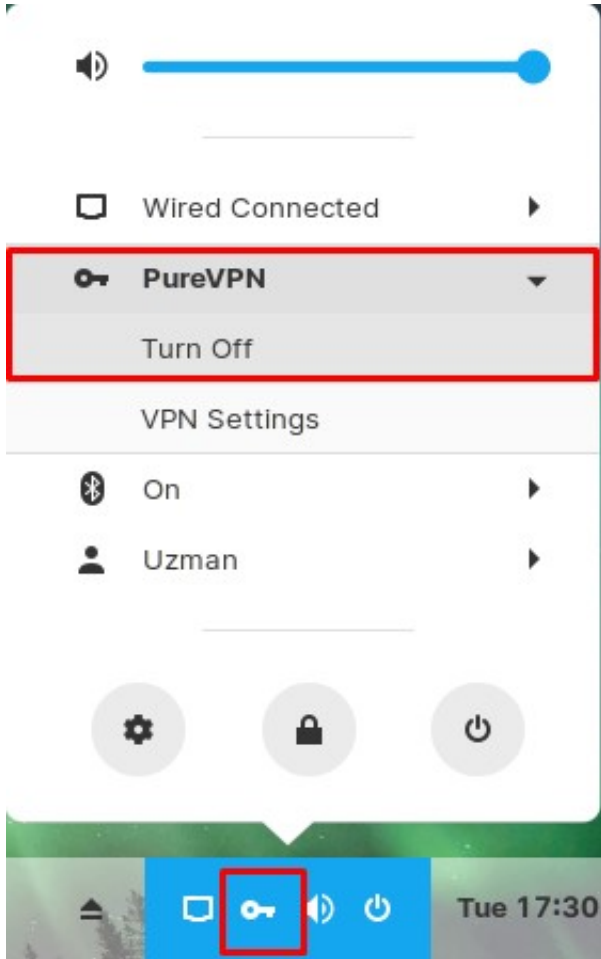
Cancel OK

Click **OK** and then click **Add**.

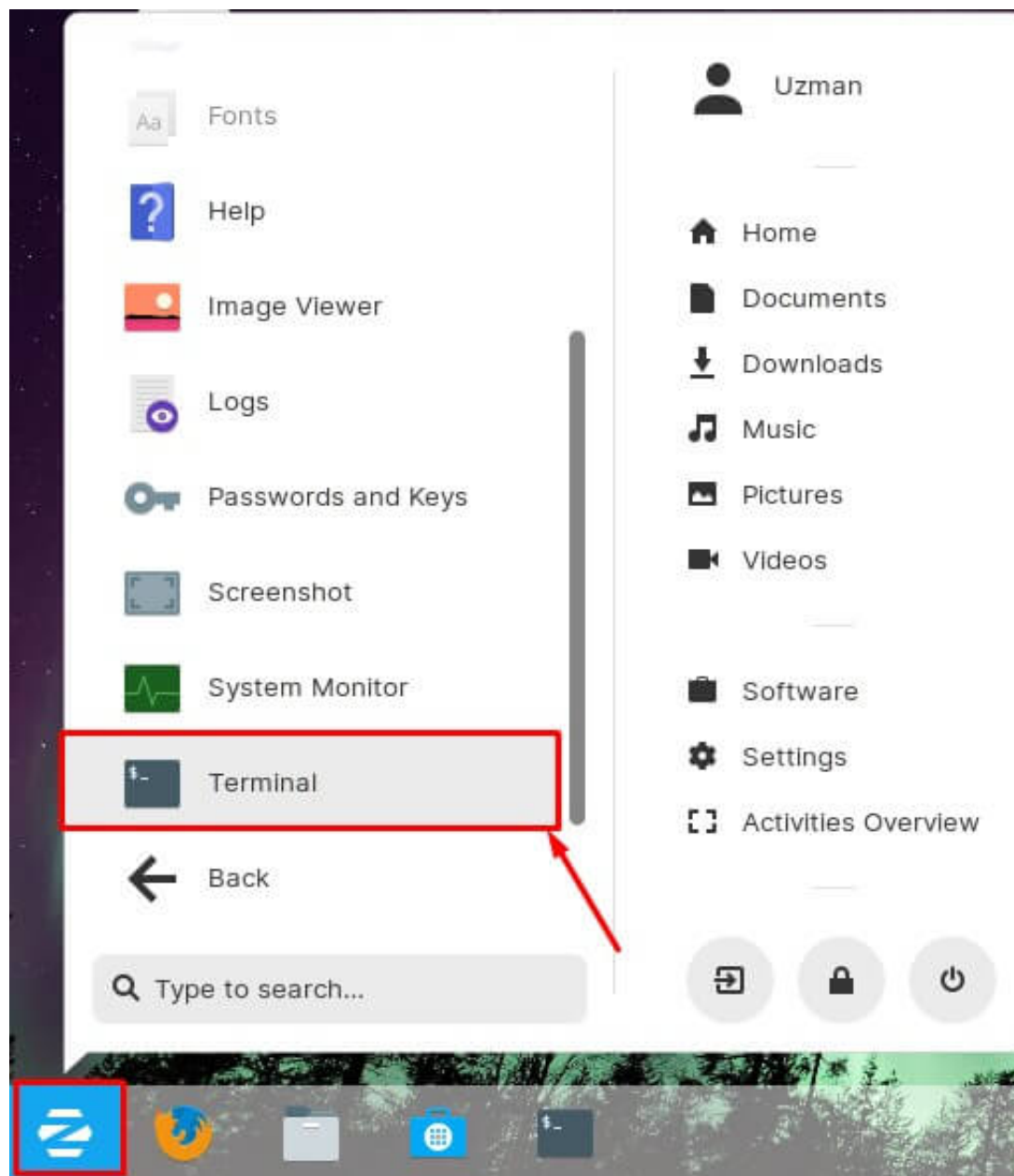
5 Now go to the **Wired Connected** option and under **VPN** click the newly added **Connect** to activate VPN.



6 You are connected to VPN now!



1 Go to the **'Menu'** and search and open the **'Terminal'**.

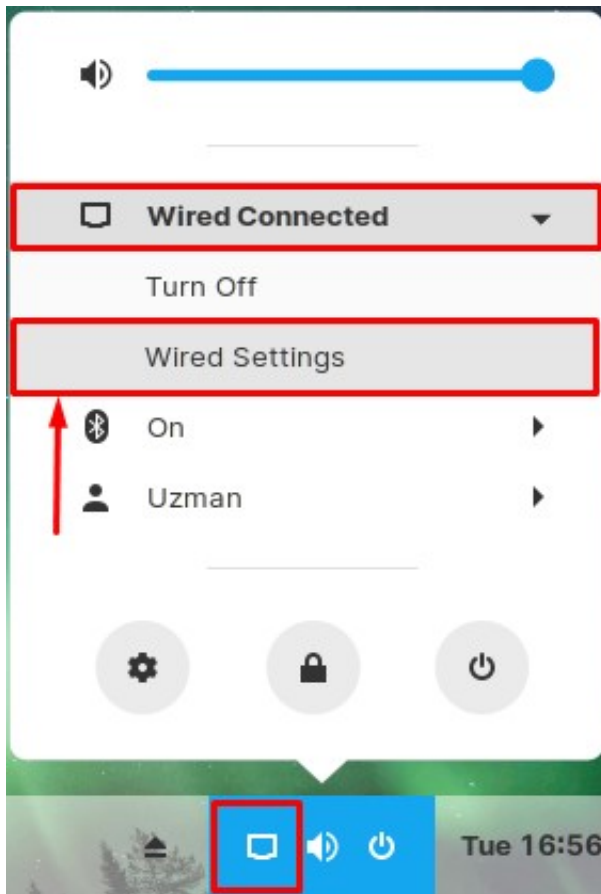


2 Now you need to install L2TP module. Type the following commands one by one:

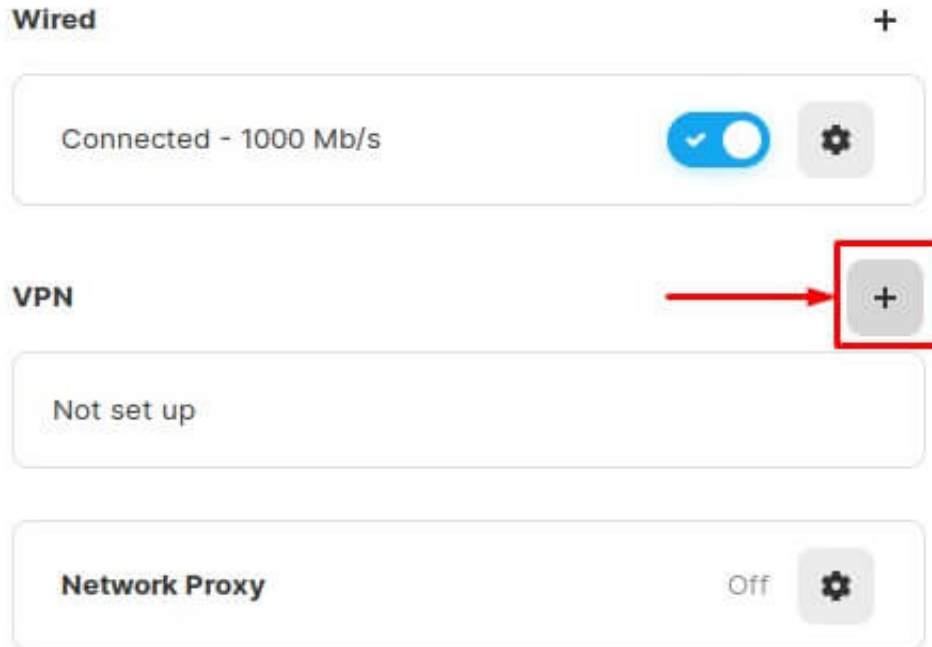
- **sudo apt-get update**
- **sudo apt-get install xl2tpd**
- **sudo apt-get install network-manager-l2tp**
- **sudo apt-get install network-manager-l2tp-gnome**

3 Now select the following options:

- Click **Wired Connected**
- Go to **Wired Settings**



4 Click the '+' icon to add a VPN connection and select '**Layer 2 Tunneling Protocol (L2TP)**' option.



Cancel

Add VPN

- Layer 2 Tunneling Protocol (L2TP)**
Compatible with Microsoft and other L2TP VPN servers.
- Point-to-Point Tunneling Protocol (PPTP)**
Compatible with Microsoft and other PPTP VPN servers.
- Import from file...

5 When the new window appears, complete the fields as below:

- Connection name: **PureVPN**
- Gateway: **pointtoserver.com** (you can use your desired server address here, in order to see the complete list [click here](#))
- User name: **Your VPN username**
- Password: **Your VPN password**

Cancel Add VPN Add

Identity IPv4 IPv6

Name PureVPN

General

Gateway usca.pointtoserver.com

User Authentication

User name purevpn0sxxxx

Password ●●●●●●●●●●

Show password

NT Domain

IPsec Settings... PPP Settings...

6 Go to the 'IPsec Settings...'

- Check the 'Enable Ipsec tunnel to IPsec host'
- Pre-share key: **12345678**

Under 'Advanced' option

- Phase1 Algorithm: 3des-sha1-modp1024
- Phase2 Algorithm: 3des-sha1

Click **OK**

L2TP IPsec Options ✕

Enable IPsec tunnel to L2TP host

Machine Authentication

Pre-shared key:

Show password

▼ **Advanced**

Remote ID:

Phase1 Algorithms:

Phase2 Algorithms:

Phase1 Lifetime: (HH:MM)

Phase2 Lifetime: (HH:MM)

Enforce UDP encapsulation

Use IP compression

Use IKEv2 key exchange

Disable PFS

7 Go to the '**PPP Settings...**'

Only allow the following options:

- MSCHAP
- MSCHAP2

Also, select the following:

- Allow BSD data compression
- Allow Deflate data compression
- Use TCP header compression

L2TP PPP Options ✕

Authentication

Allow the following authentication methods:

- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- EAP

Security and Compression

Use Point-to-Point encryption (MPPE)

Security: All Available (Default) ▾

Allow stateful encryption

Allow BSD data compression

Allow Deflate data compression

Use TCP header compression

Use protocol field compression negotiation

Use Address/Control compression

Echo

Send PPP echo packets

Misc

MTU : 1400 - +

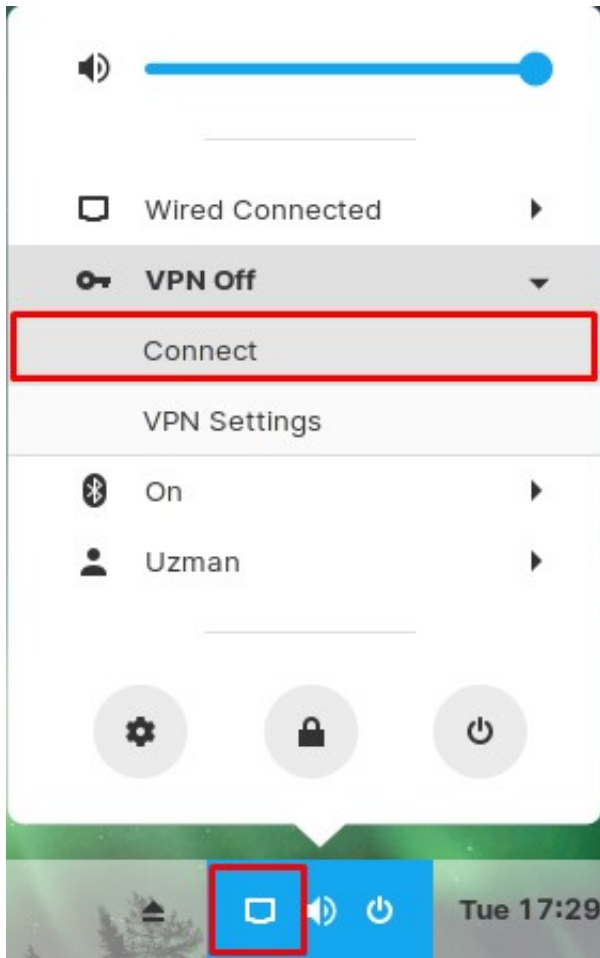
MRU : 1400 - +

Cancel

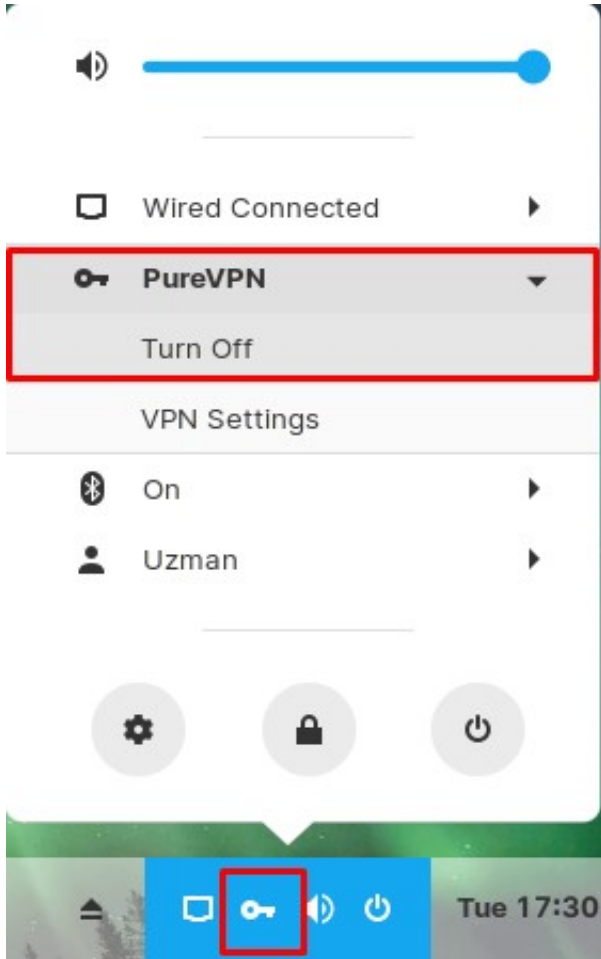
OK

?lick **OK** then click **Add**.

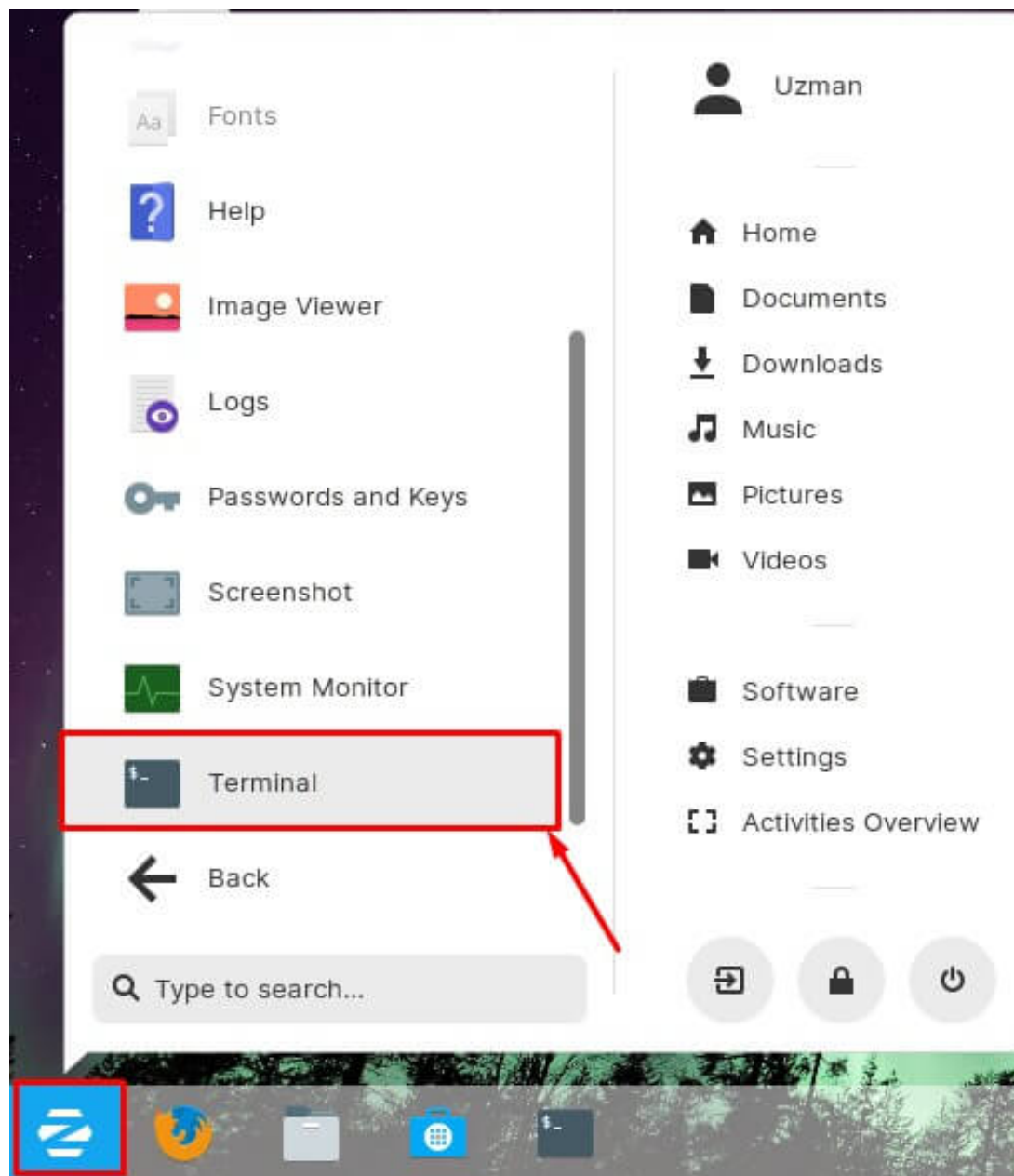
Go to **Wired Connected** option and under **VPN** click the newly added **Connect** to activate VPN.



9 You are connected to VPN now!



1 Go to **'Menu'** and search and open **'Terminal'**.



2 Now you need to install SFTP packages. The sftp-client and network-manager packages is available via PPA on launchpad. You can import the gpg key using the following command:

- **sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 61FF9694161CE595**
- **sudo nano /etc/apt/sources.list.d/sftp-client.list**

Now insert the following two lines into the file:

```
deb http://ppa.launchpad.net/eivnaes/network-manager-sftp/ubuntu vivid main
```


deb-src <http://ppa.launchpad.net/eivnaes/network-manager-sstp/ubuntu> vivid main

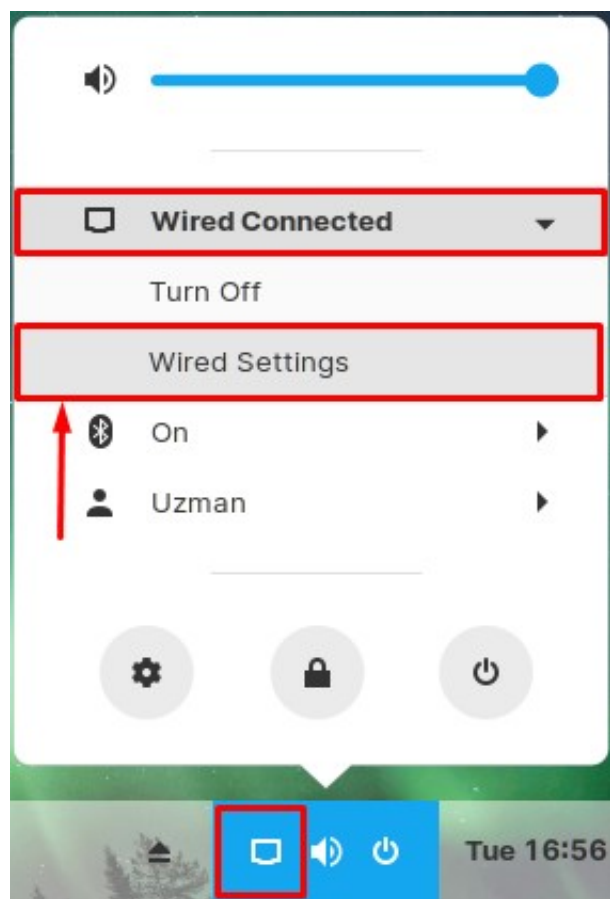
Note: Save and Exit the file.

Lastly, run the following commands one by one:

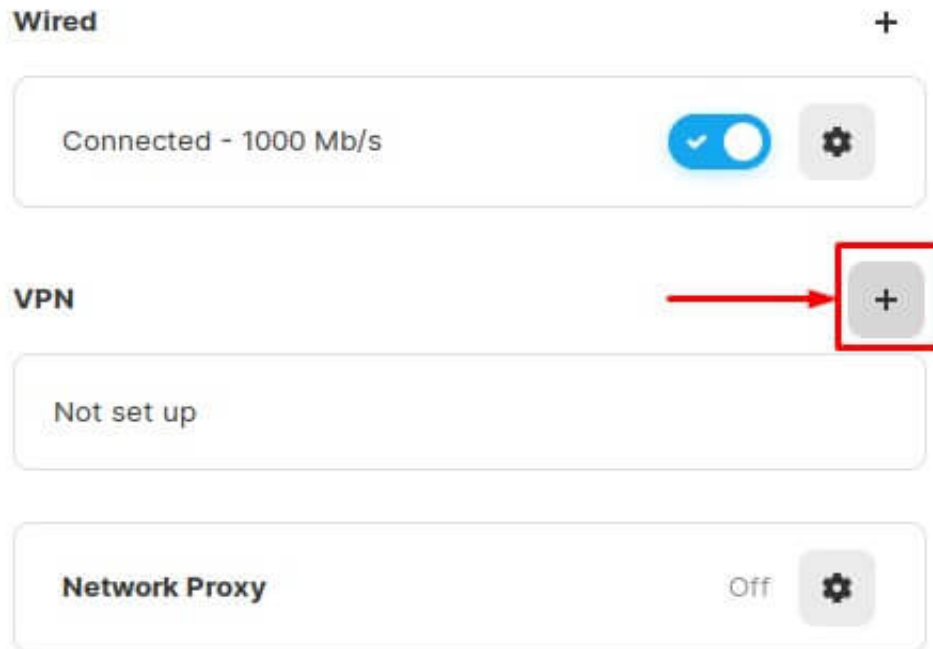
- **sudo apt-get update**
- **sudo apt-get install -y network-manager-sstp sstp-client**

3 Now select the following options:

- Click **Wired Connected**.
- Go to **Wired Settings**.



4 Click the '+' icon to add a VPN connection and select '**Point-to-Point Tunneling Protocol (SSTP)**'.





5 When a new window appears, complete the fields as below:

- Name: **PureVPN**
- Gateway: **pointtoserver.com** (you can use your desired server address here, in order to see the complete list [click here](#))
- User name: **Your VPN username**
- Password: **Your VPN password**
- Check the '**Ignore Certificate Warnings**' option.

Cancel **Add VPN** Add

Identity IPv4 IPv6

Name

General

Gateway

Optional

User name

Password

Show password

NT Domain

CA Certificate

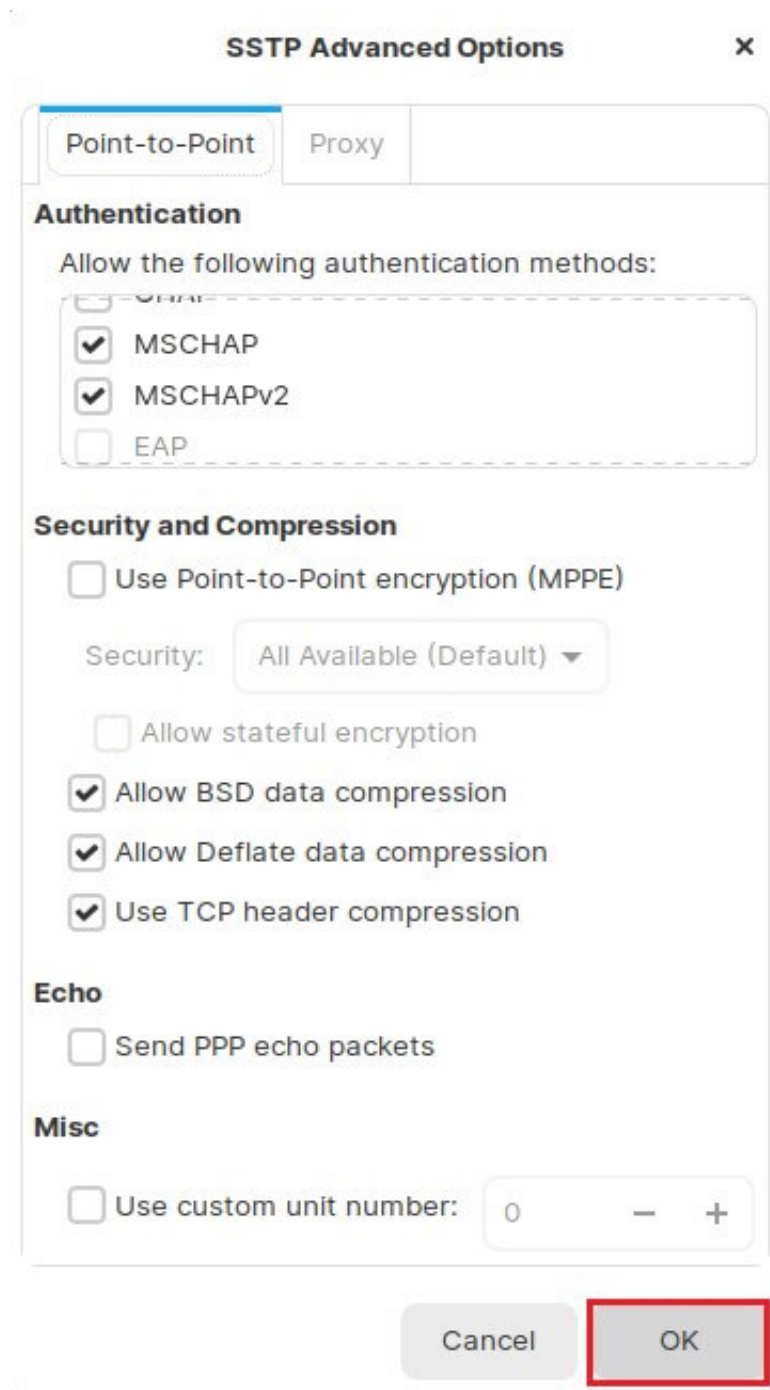
Ignore certificate warnings

Use TLS hostname extensions

Advanced...

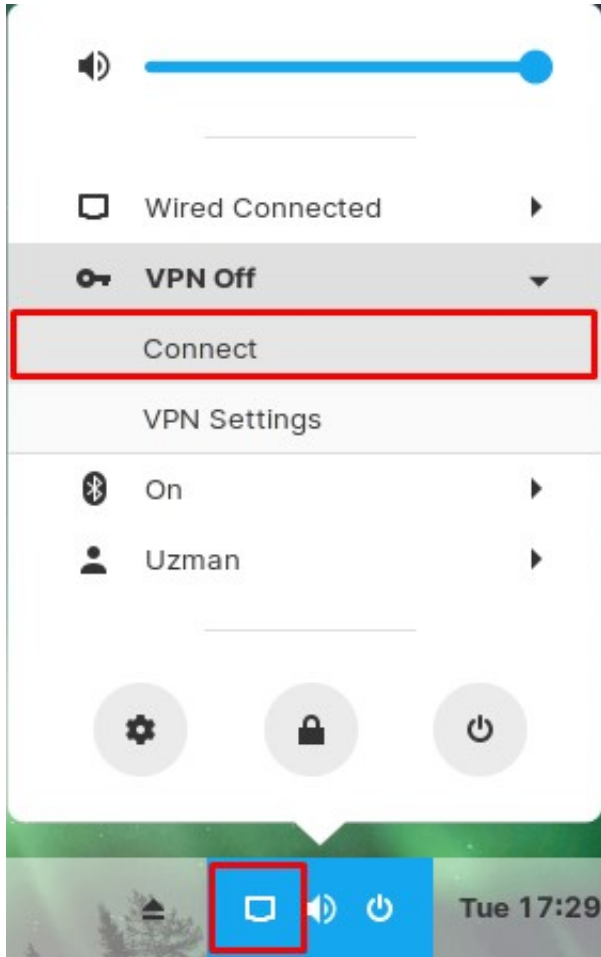
6 Click on **“Advanced...”** option and check the following options under it:

- MSCHAP
- MSCHAP2
- Allow BSD compression
- Allow Deflate compression
- Allow TCP Header compression

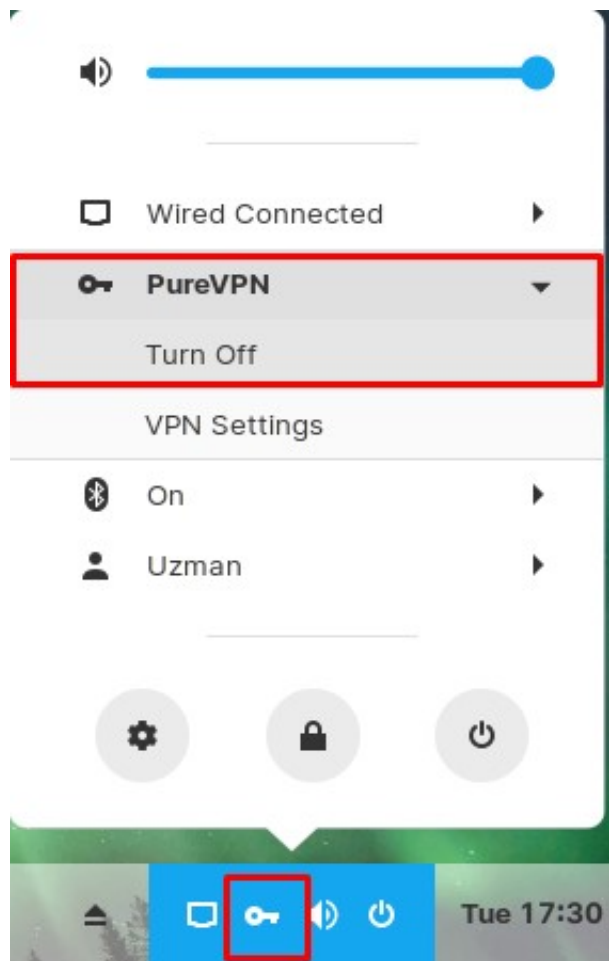


?lick **OK** then click **Add**.

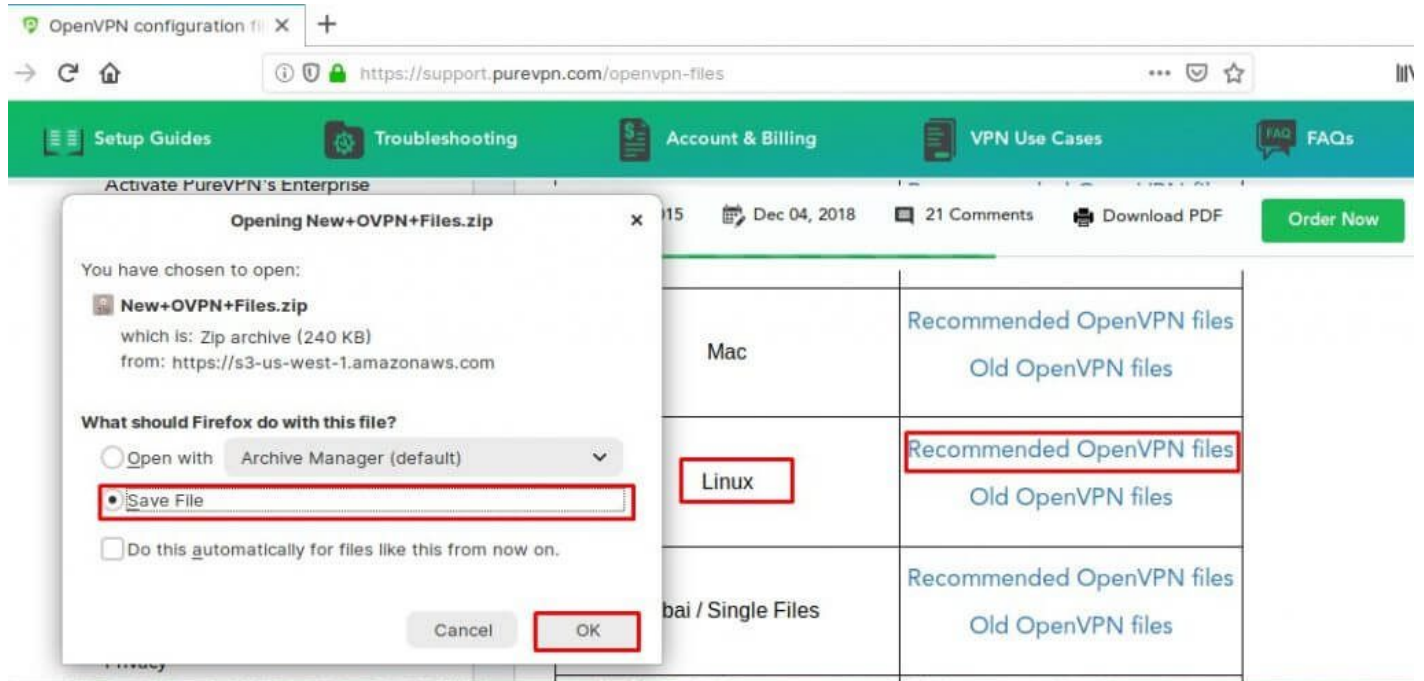
7 Now go to **Wired Connected** option and under **VPN** click the newly added **Connect** to activate VPN.

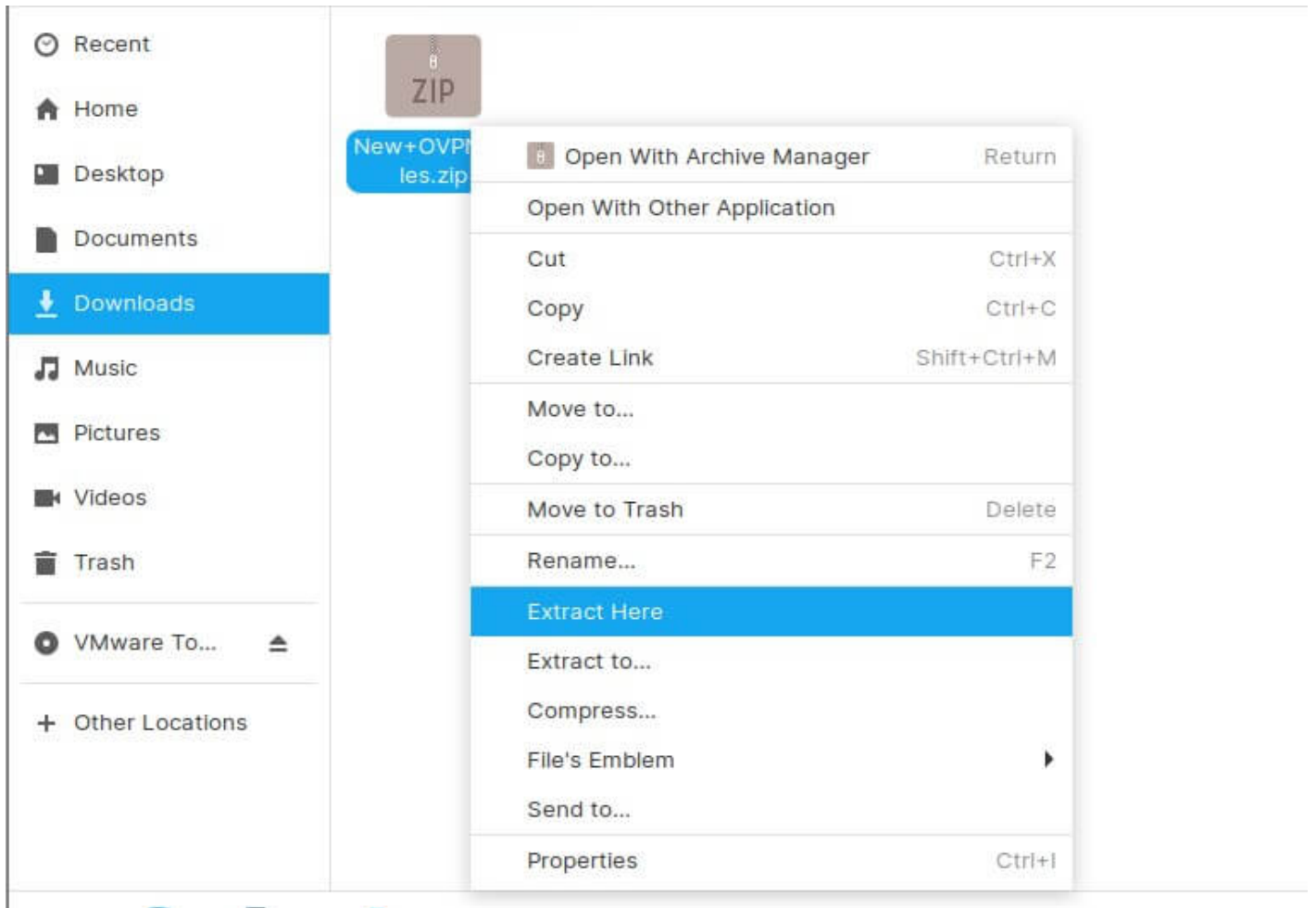


8 You are connected to VPN now!

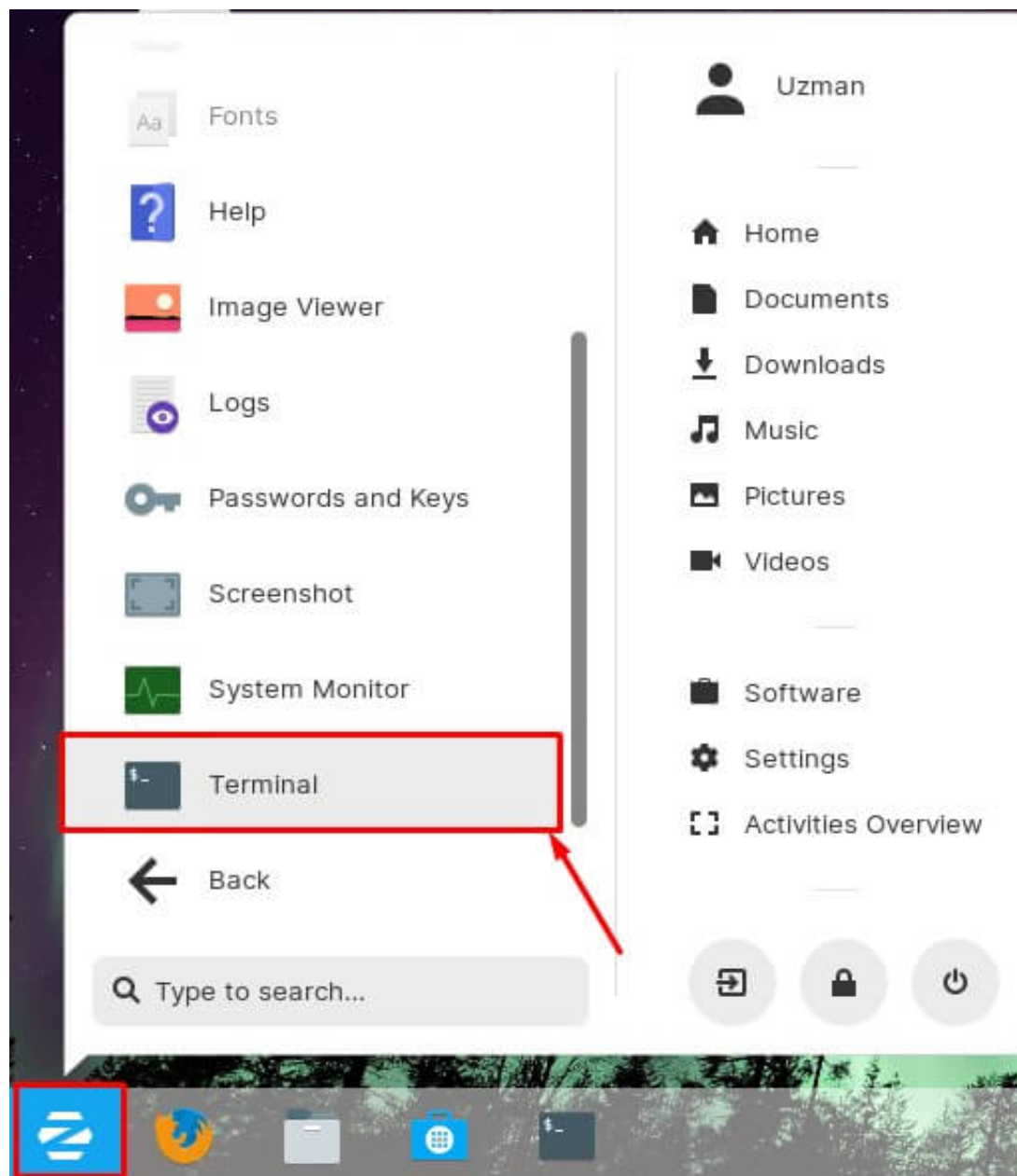


1 Firstly, go to your desired web browser and download the [PureVPN OpenVPN configuration](#) files and extract them.





2 Go to the **Menu** and search then open **Terminal**

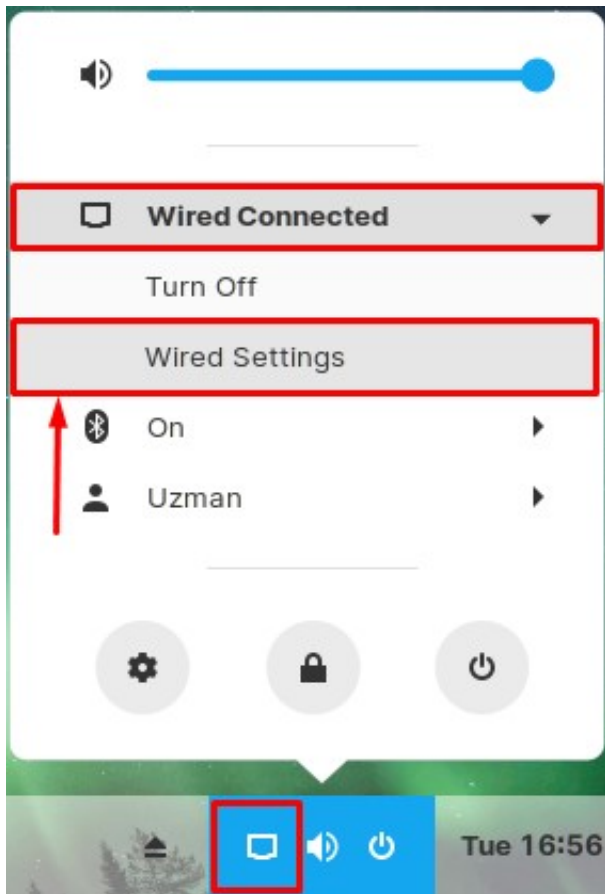


3 Now you need to install OpenVPN packages. Type the following commands one by one:

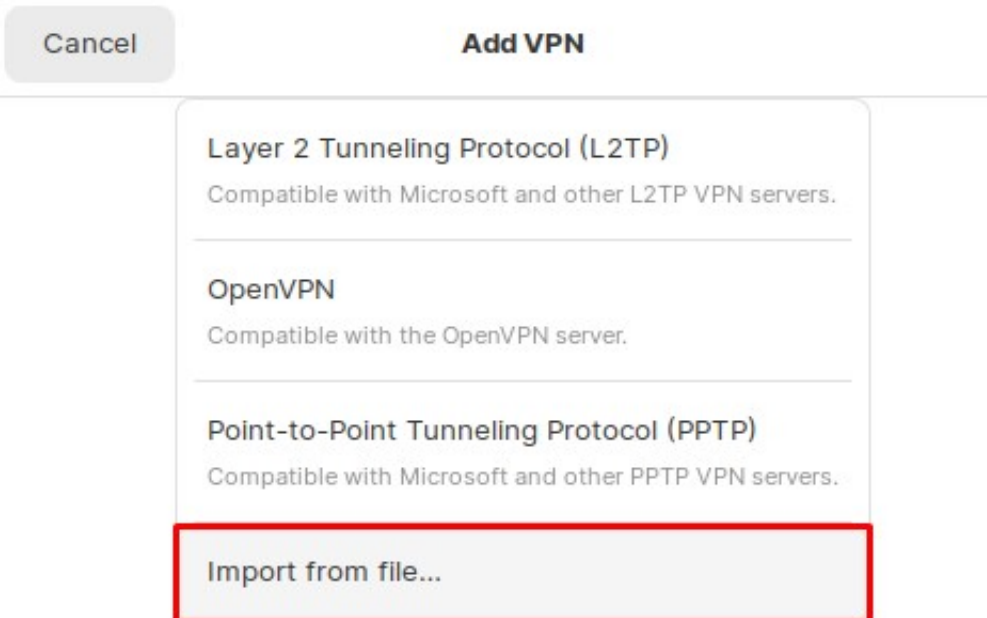
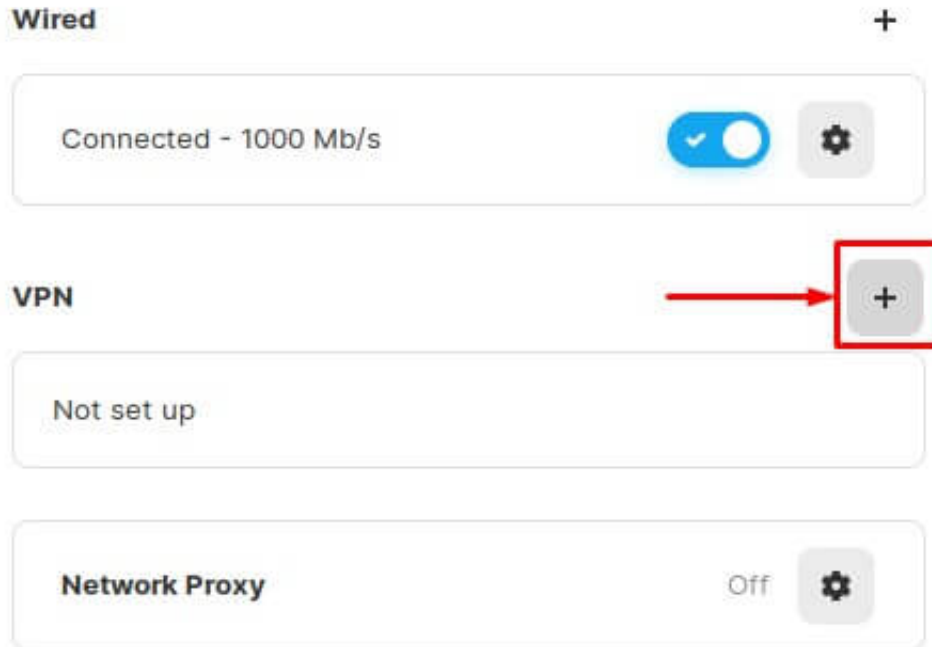
- **sudo apt-get update**
- **sudo apt-get install openvpn**
- **sudo apt-get install network-manager-openvpn**
- **sudo apt-get install network-manager-openvpn-gnome**

4 Now select the following options:

- Click **Wired Connected**
- Go to **Wired Settings**



5 Click the '+' icon to add a VPN connection and select '**Import from file...**' option.



6 Go to **Downloads** directory, select the folder containing OpenVPN files i.e. '**New OpenVPN Files**'. Select the desired file with ".ovpn" extension, then click **Open**.



The screenshot shows a file selection interface titled "Select file to import". At the top right, there is a search icon and an "Open" button. Below the title bar, there are navigation tabs: "purevpn", "Downloads", "New+OVPN+Files", and "New OVPN Files" (which is selected). The main area displays a table of files with columns for "Name", "Size", and "Modified". The file "de2-ovpn-udp-udp.ovpn" is highlighted in blue.

Name	Size	Modified
ae2-ovpn-tcp.ovpn	5.5 kB	30 Nov 2018
ae2-ovpn-udp.ovpn	6.3 kB	30 Nov 2018
bg2-ovpn-tcp.ovpn	5.5 kB	30 Nov 2018
bg2-ovpn-udp.ovpn	6.3 kB	30 Nov 2018
br2-ovpn-tcp.ovpn	5.5 kB	30 Nov 2018
br2-ovpn-udp.ovpn	6.3 kB	30 Nov 2018
ca.crt.crt	1.8 kB	2 May 2018
de2-ovpn-tcp-tcp.ovpn	5.5 kB	30 Nov 2018
de2-ovpn-udp-udp.ovpn	6.3 kB	30 Nov 2018
dk2-ovpn-tcp.ovpn	5.5 kB	30 Nov 2018
dk2-ovpn-udp.ovpn	6.3 kB	30 Nov 2018
hk2-ovpn-tcp-tcp.ovpn	5.5 kB	30 Nov 2018
hk2-ovpn-udp-udp.ovpn	6.3 kB	30 Nov 2018
in2-ovpn-tcp.ovpn	5.5 kB	30 Nov 2018
in2-ovpn-udp.ovpn	6.3 kB	30 Nov 2018
my2-ovpn-tcp-tcp.ovpn	5.5 kB	30 Nov 2018
my2-ovpn-udp-udp.ovpn	6.3 kB	30 Nov 2018
my-kl2-ovpn-tcp.ovpn	5.5 kB	30 Nov 2018
my-kl2-ovpn-udp.ovpn	6.3 kB	30 Nov 2018

7 Now enter the details as mentioned below:

- Name: **PureVPN** (Here we use PureVPN, you can change it any other name)
- **Gateway**: already inserted
- Authentication Type: Select **Password** from drop down menu
- Insert **Username** provided by **PureVPN**
- Insert **Password** provided by **PureVPN**
- Click on folder icon from Certificate folder and add the '**ca.crt.crt**' file.
- ?lick **Add**.

CancelAdd VPNAdd

IdentityIPv4IPv6

Name

General

Gateway

Authentication

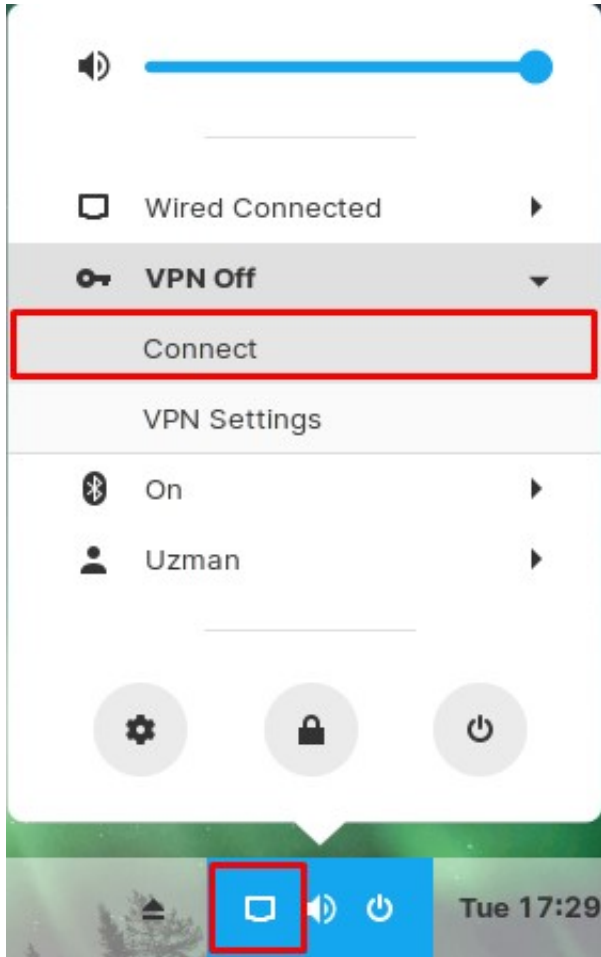
Type ▼

User name

Password

CA certificate

8 Now go to **Wired Connected** option and under **VPN** click the newly added **Connect** to activate VPN.



9 You are connected to VPN now!

PureVPN Support

Solution of Your Problems

<https://support.purevpn.com>

