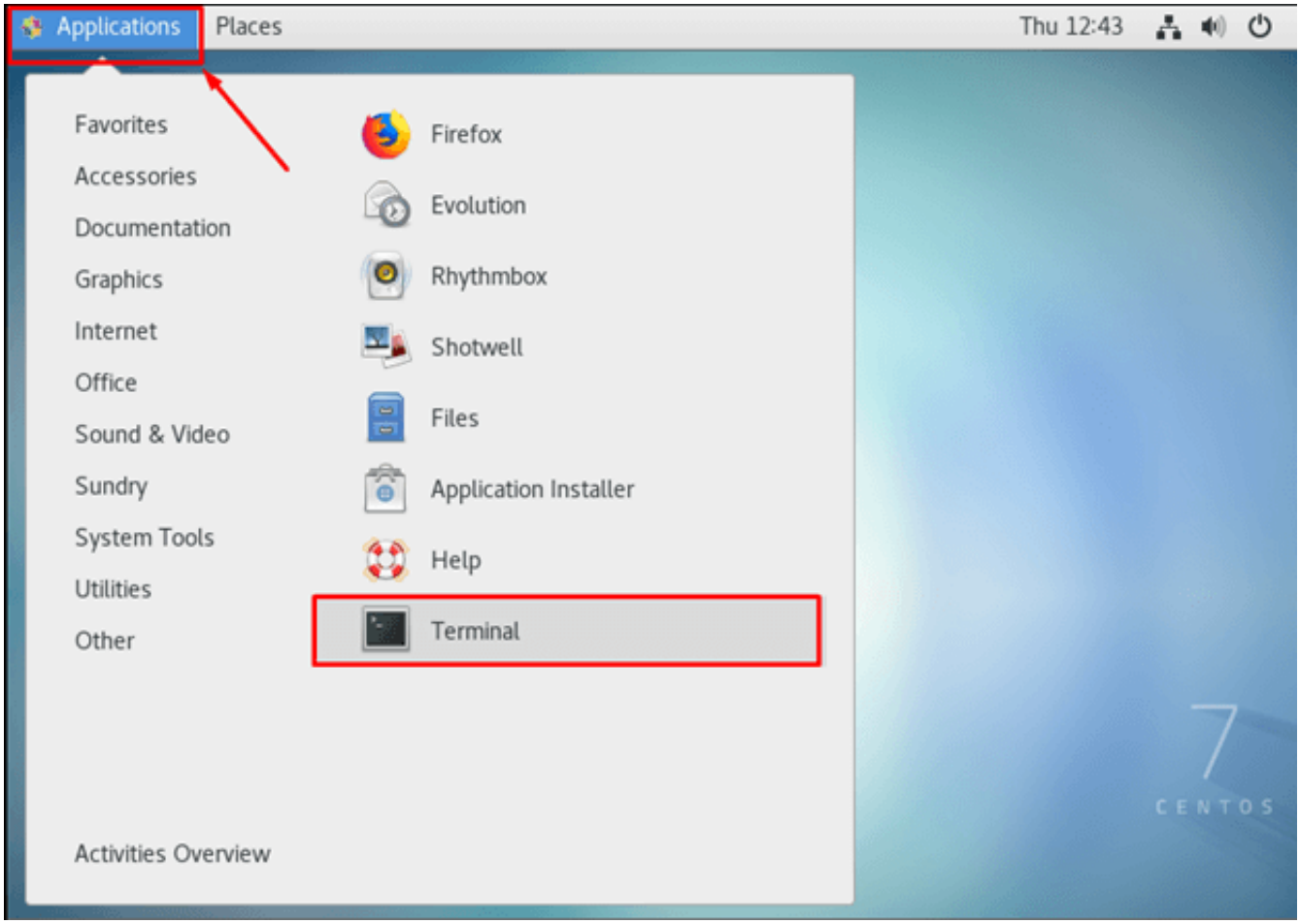
How to Setup PureVPN on Cent OS

Power your Cent OS with PureVPN by following the easy-to-understand tutorial presented in this support guide.

PPTPL2TPOpenVPN

1 Go to the ‘Applications’ option and search and open the ‘Terminal’.



2 Now you need to install **PPTP** Type the following three commands one by one:

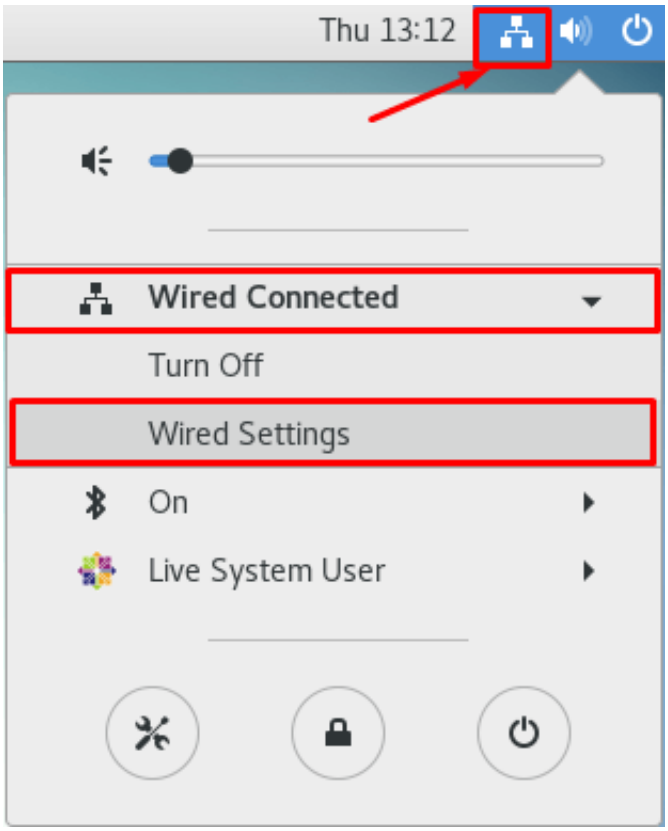
- **sudo yum update**
- **sudo yum install epel-release**
- **sudo yum install NetworkManager**

- **sudo yum install NetworkManager-pptp-gnome**

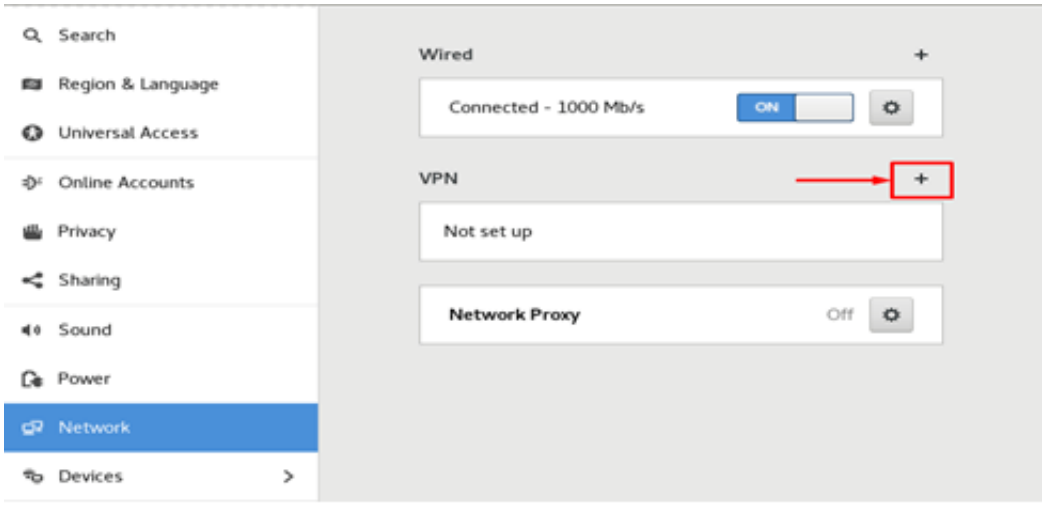
When you finished the commands, logout/login is required. (Or preferably, restart the system)

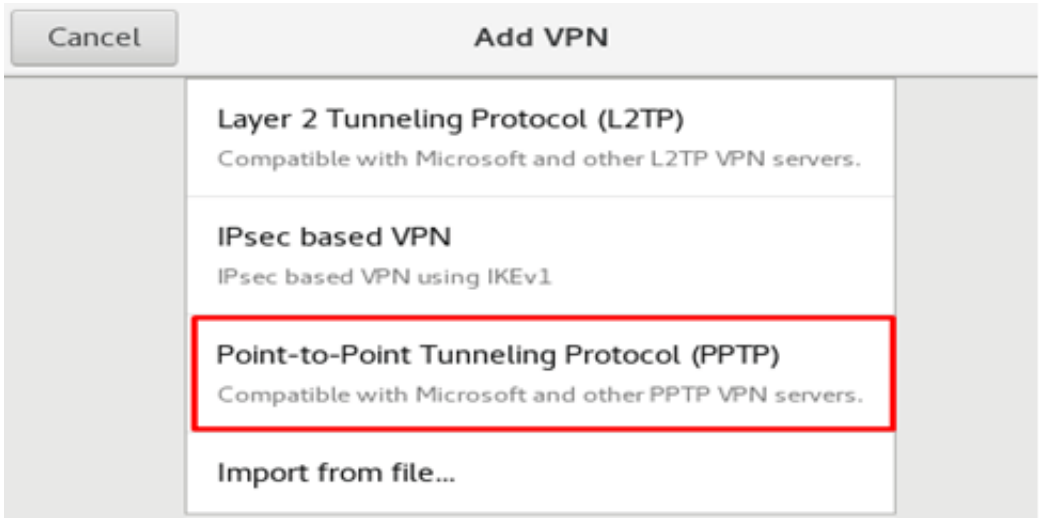
3 Now, select the following options:

- Click on "**Network Connection Icon**"
- Go to "**Wired Connected**" and select "**Wired Settings"**



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

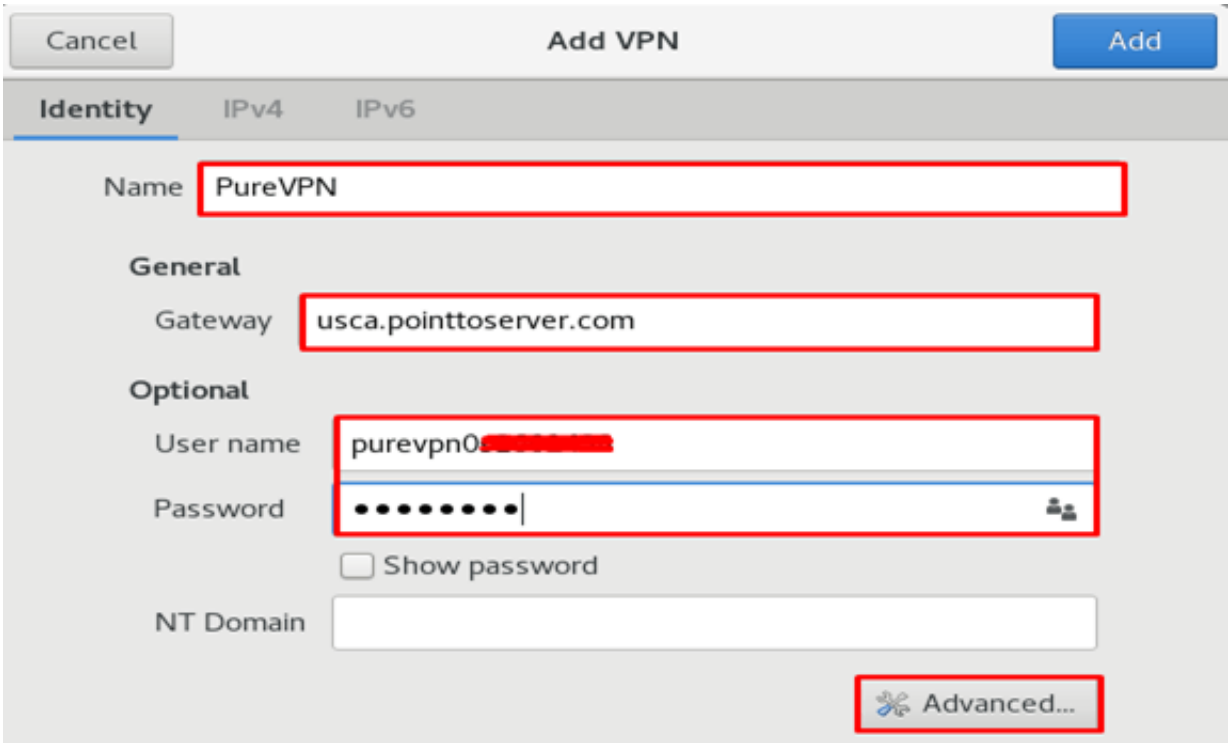




5 When the new window appear, complete the fields as below

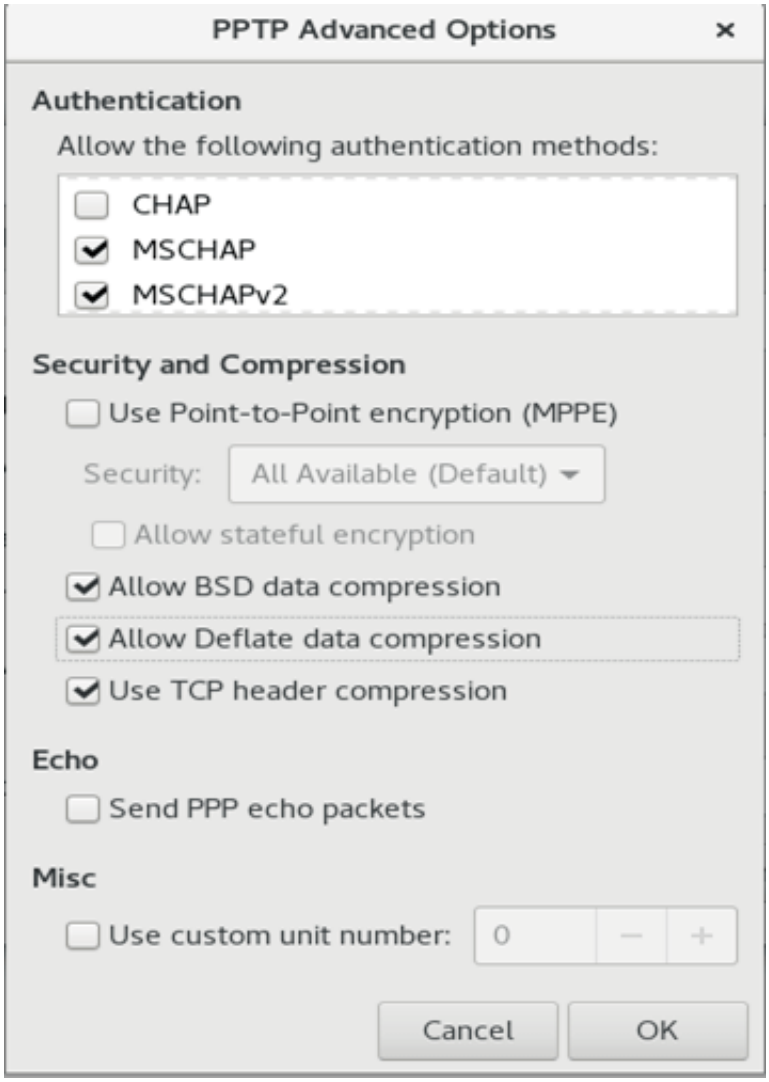
- Enter Connection name: **PureVPN**
- Enter Gateway: **usca.pointtoserver.com** (you can use your desired server address here, in order to see the complete list click here)
- Enter **Username** provided by **PureVPN**
- Enter **Password** provided by **PureVPN**

Click Advanced option.



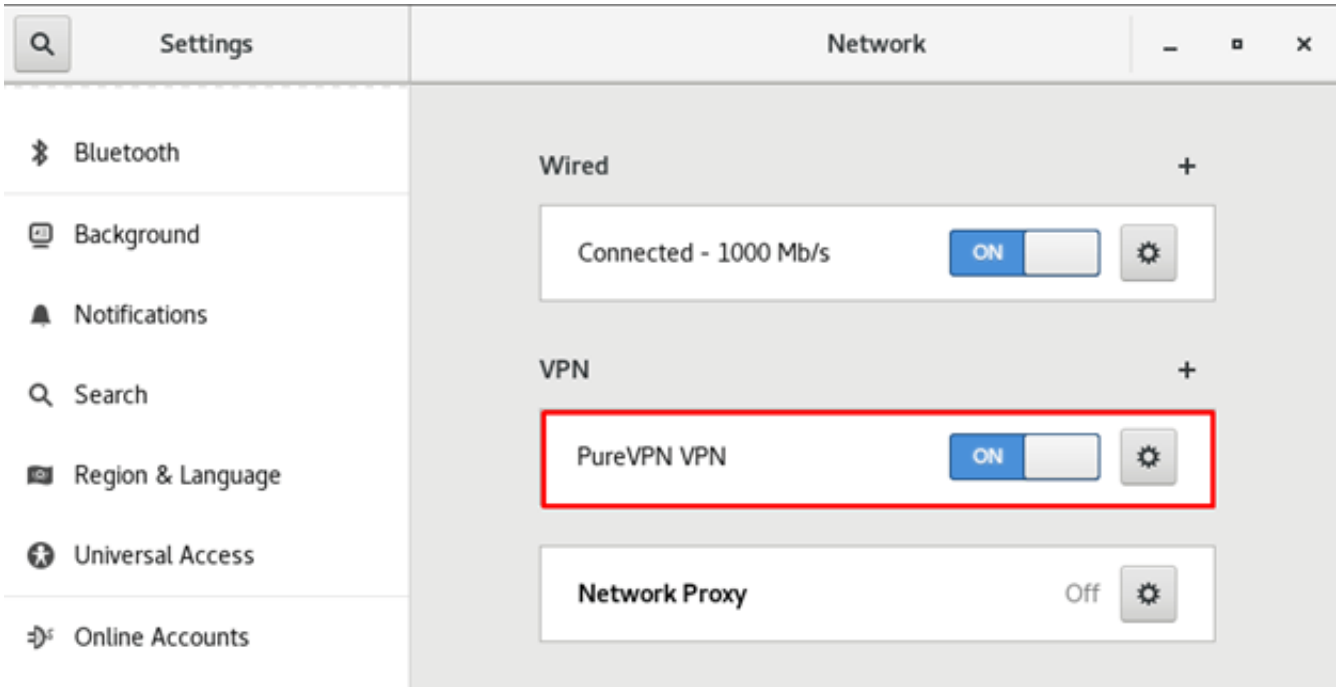
Now, select the following:

- MSCHAP
- MSCHAPv2
- Allow BSD data compression
- Allow Deflate data compression
- Use TCP header compression



?lick “OK” and then click “Add” from the top right corner.

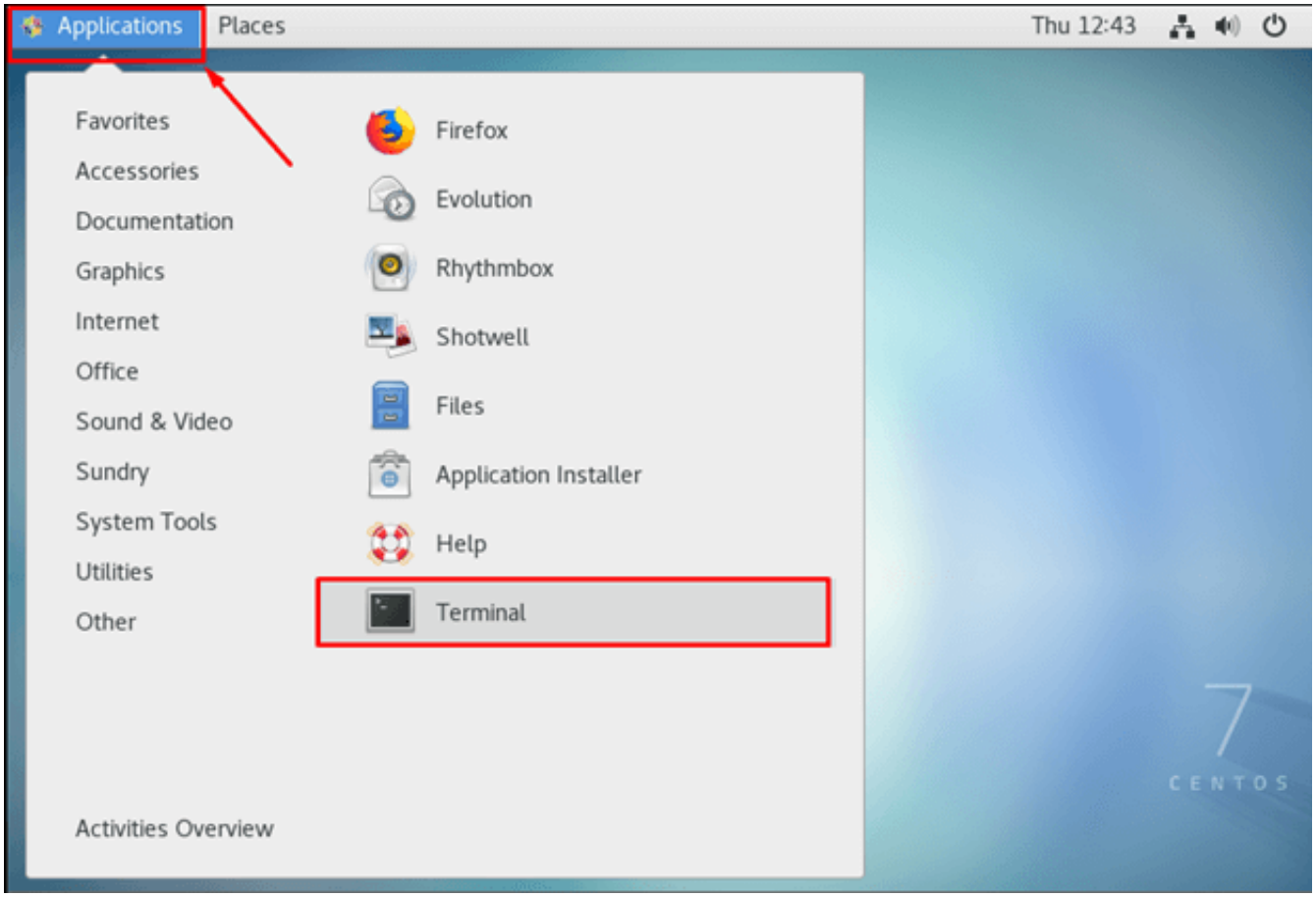
6 Now, enable your VPN by swiping the toggle button.



7 You are now connected!

8 You can turn off the VPN connection by swiping the toggle button “Off”.

1 Go to the ‘Applications’ option and search and open the ‘Terminal’.



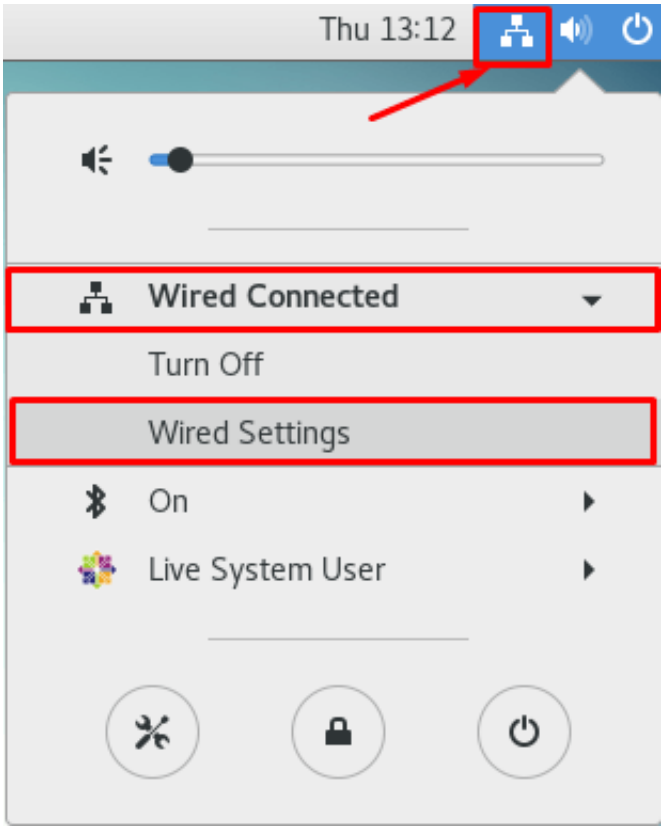
2 Now, you need to install **L2TP** dependencies. Type the following three commands one by one:

- **sudo yum update**
- **sudo yum install epel-release**
- **sudo yum install NetworkManager**
- **sudo yum –enablerepo=epel-testing install NetworkManager-l2tp-gnome**

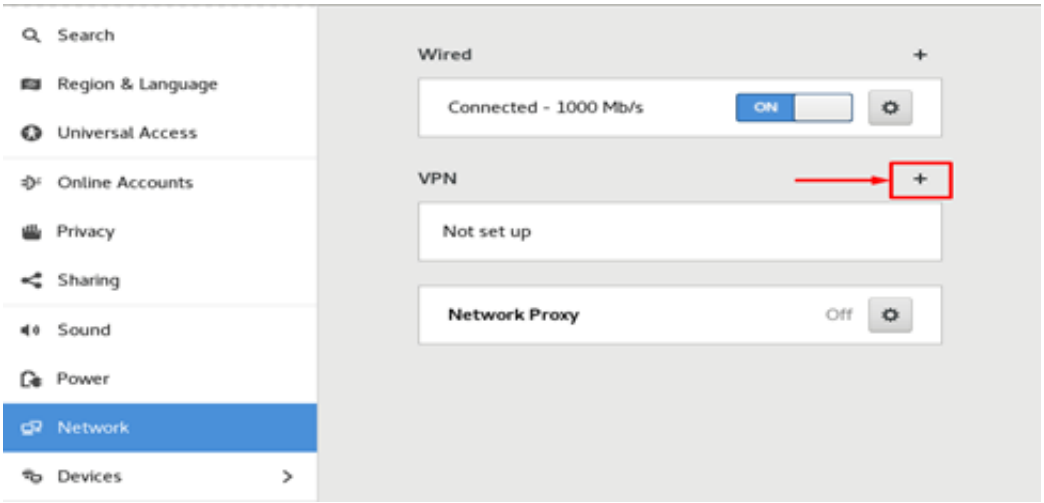
When you finished the commands, logout/login is required. (Or preferably, restart the system)

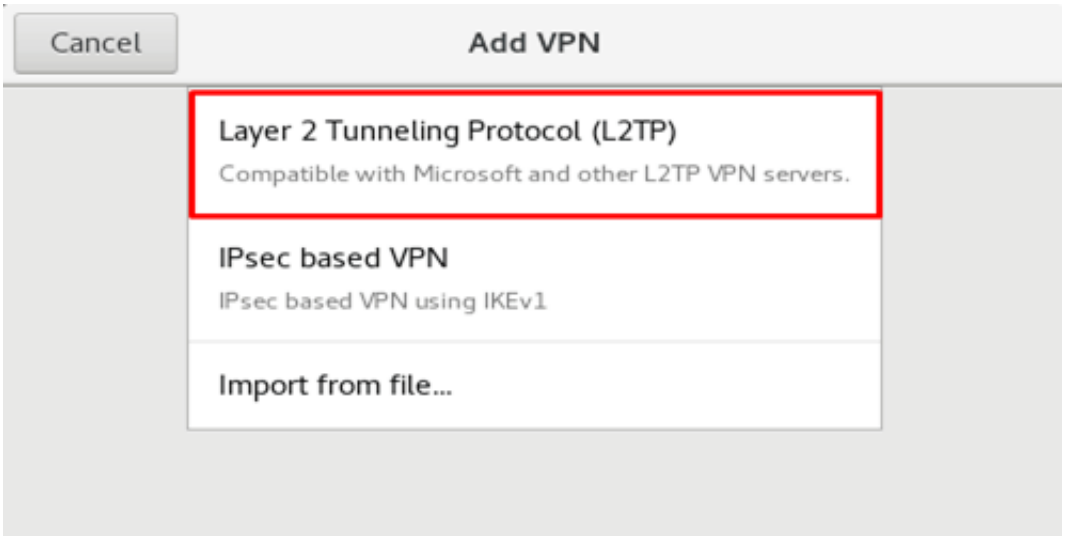
3 Now, select the following options:

- Click on “**Network Connection Icon**“
- Go to “**Wired Connected**” and select “**Wired Settings”**



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





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

- Enter Connection name: **PureVPN**
- Enter Gateway: **usca.pointtoserver.com** (you can use your desired server address here, in order to see the complete list click here)
- Enter **Username** provided by **PureVPN**
- Enter **Password** provided by **PureVPN**

Go to the **'IPsec Settings…**'

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

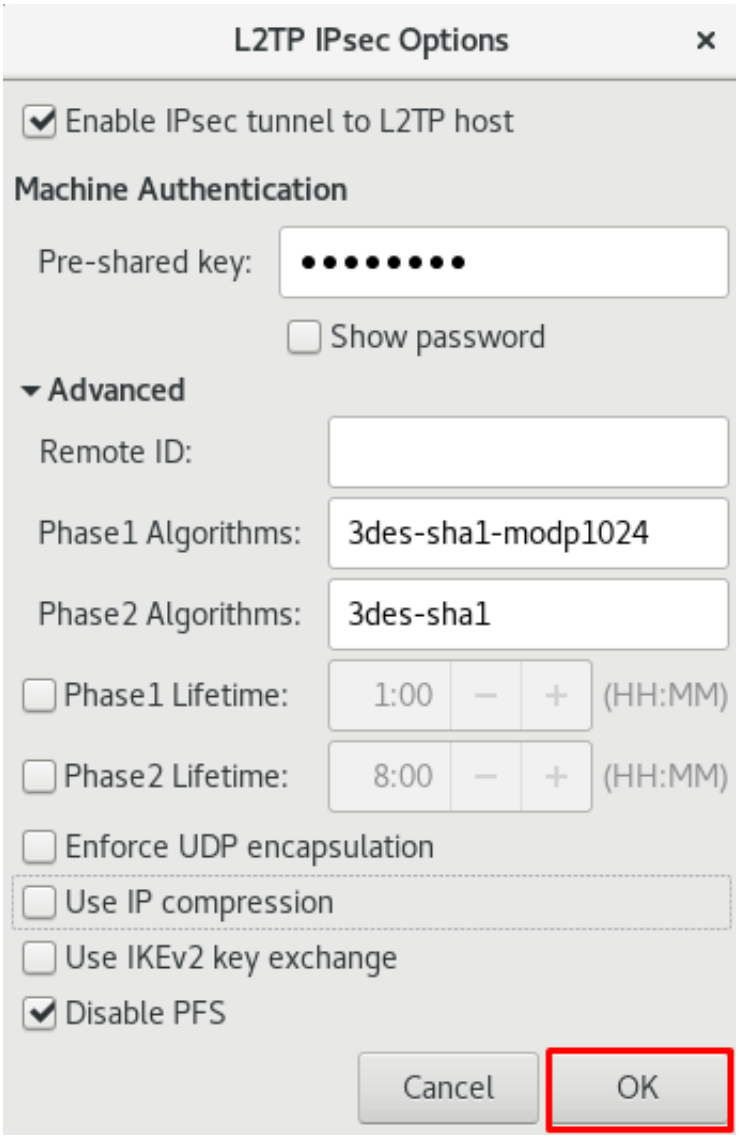
Go to the **'Advanced…**' option, then enter the following details:

For phase 1= 3des-sha1-modp1024 and

For phase 2 = 3des-sha1

Check the "**Disable PFS**" option.

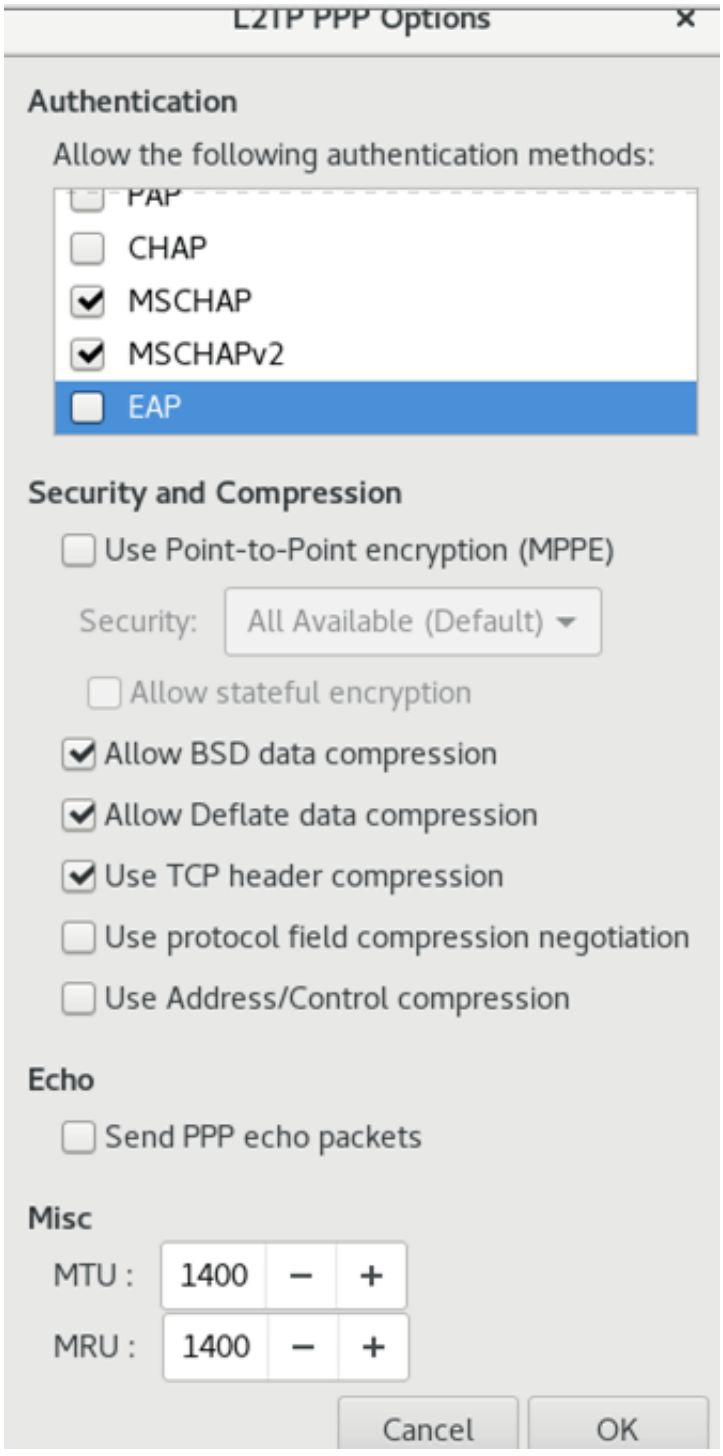
Click **'OK'**



Go to the '**PPP Settings…**' button.

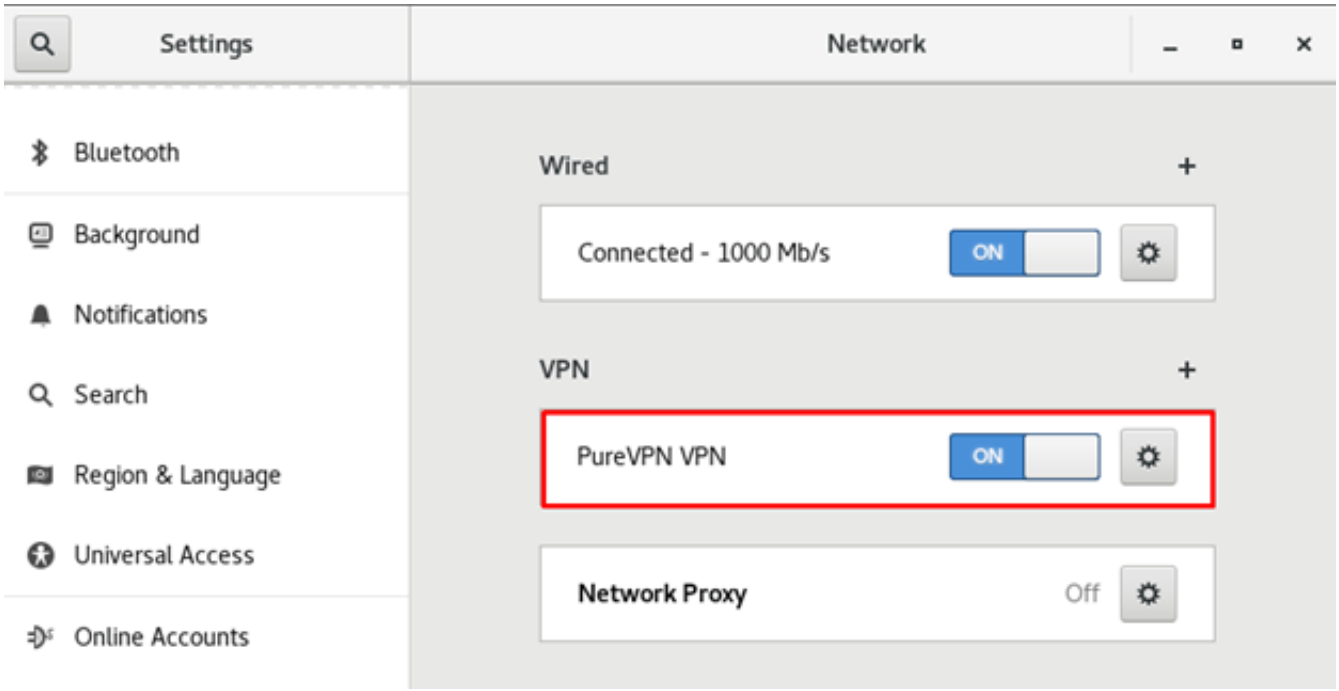
Only allow the following options:

- MSCHAP
- MSCHAP2
- Allow BSD data compression
- Allow Deflate data compression
- Use TCP header compression



?lick “OK” and then click “Add” button from the top right corner.

6 Enable your VPN by swiping the toggle button.



7 You are connected now!

8 You can turn off the VPN connection by swiping the toggle button “Off”

1 Firstly, go to your desired web browser and download PureVPN OpenVPN configuration files.

2 You will get a prompt asking what to do with the ZIP archive, select “**Save File**” and click “**OK**“. It should be downloaded to your “**Downloads**” directory.

3 Go to your “**Downloads**” directory, right click the ZIP archive and select “**Open With Archive Manager**” and then “**Extract**” the files.

4 Rename the Extracted file as “openvpn”

5 Next step is installing the config files. Installing config files requires sudo privilege. Copy and paste the contents of the Zip file to directories that override Selinux, such as /etc/ and /opt

Follow the steps below when Selinux doesn’t allow Network-Manager to access certificate files that are needed by OpenVPN. Click “Applications” at the top left of the screen, type “Terminal” in the search field to open the Terminal application.

In order to copy the extracted files to /opt/ partition, first change your directory to Downloads.

Run the following commands step by step:

sudo su

cd Downloads/

sudo yum install epel-release

sudo yum install openvpn

sudo yum install NetworkManager-openvpn-gnome

mkdir -p /etc/openvpn

sudo cp -rp openvpn /opt/

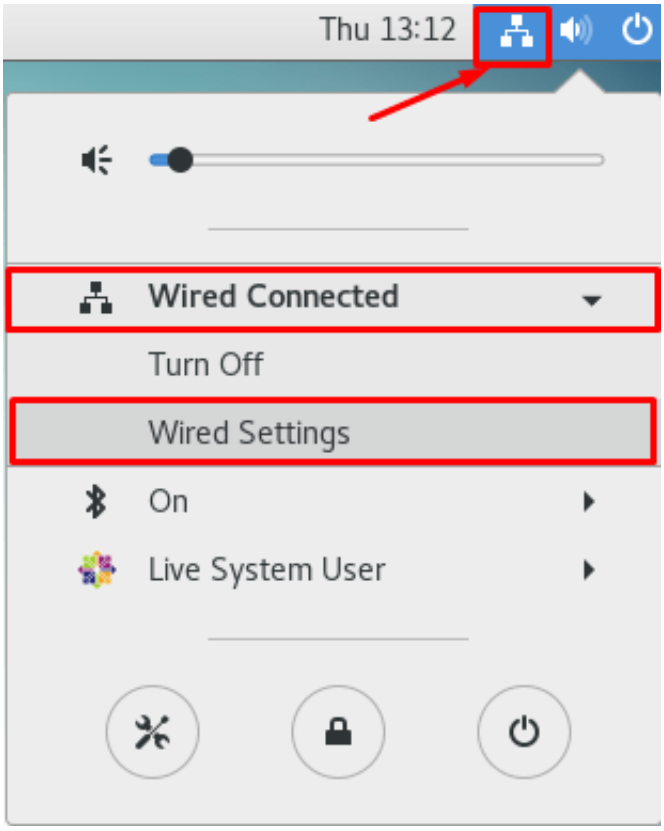
sudo chmod 644 openvpn/*

sudo chmod -R 755 /etc/openvpn/client

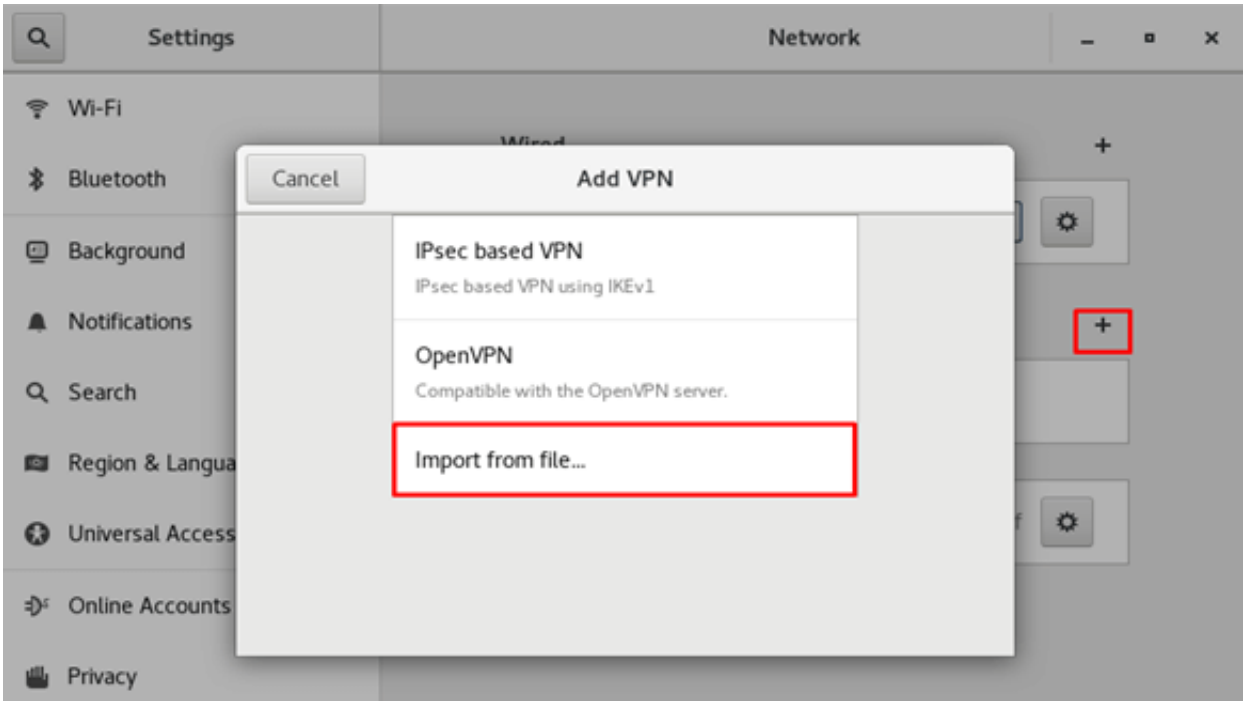
6 Go to the “Downloads” directory, copy the ‘openvpn’ folder and paste it under the ‘etc’ >’openvpn’>’client’ folder.

7 Select the following options:

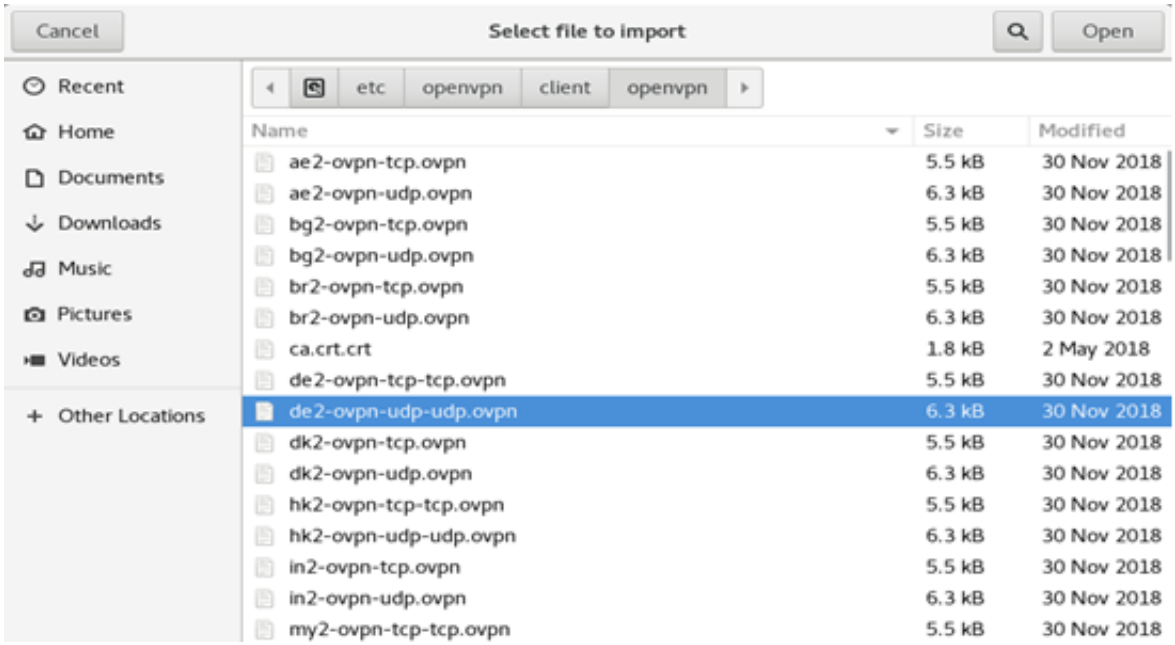
- Click on “**Network Connection Icon**“
- Go to “**Wired Connected**” and select “**Wired Settings**“



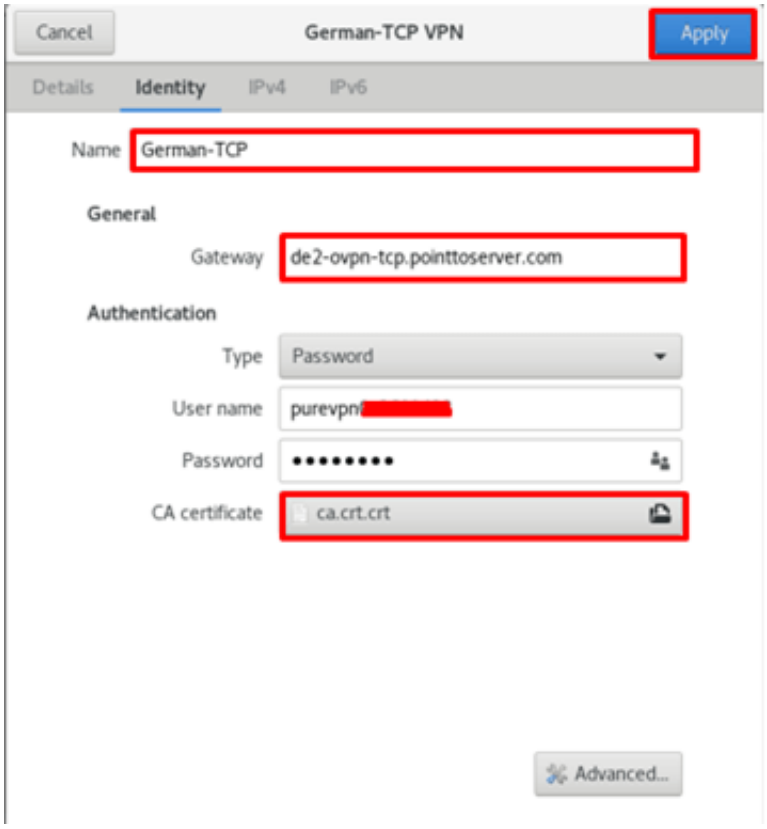
8 Click on the '**+**' icon to add a VPN connection and select '**Import from File Option**' option.



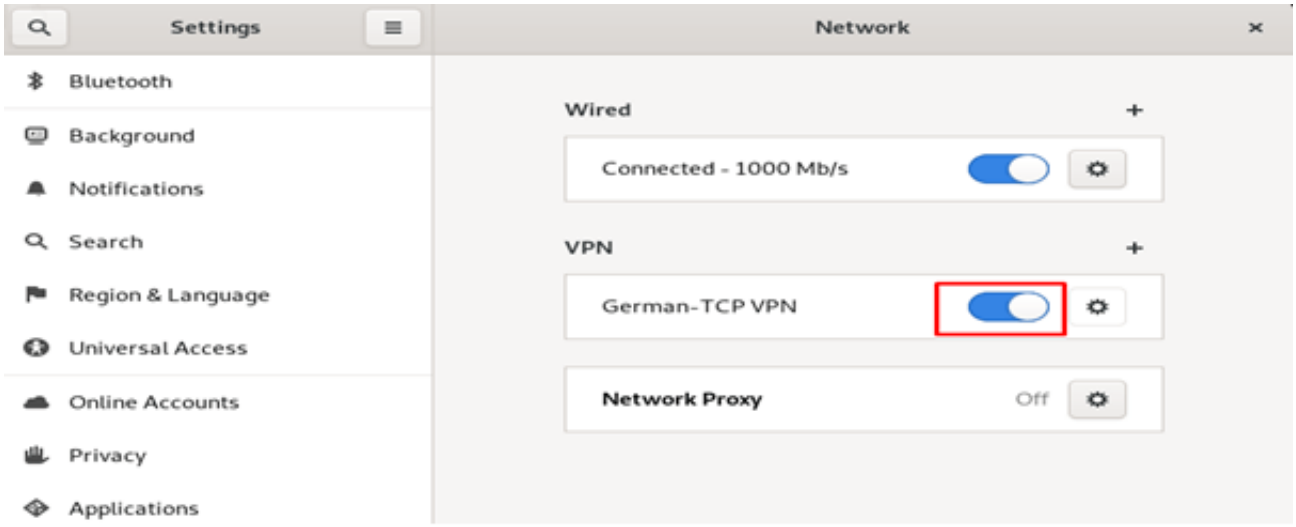
9 Go to the newly created directory with config files in the “openvpn” folder under ‘/etc/openvpn/client’. Select the desired file with “.ovpn” extension. Click “Open” button.



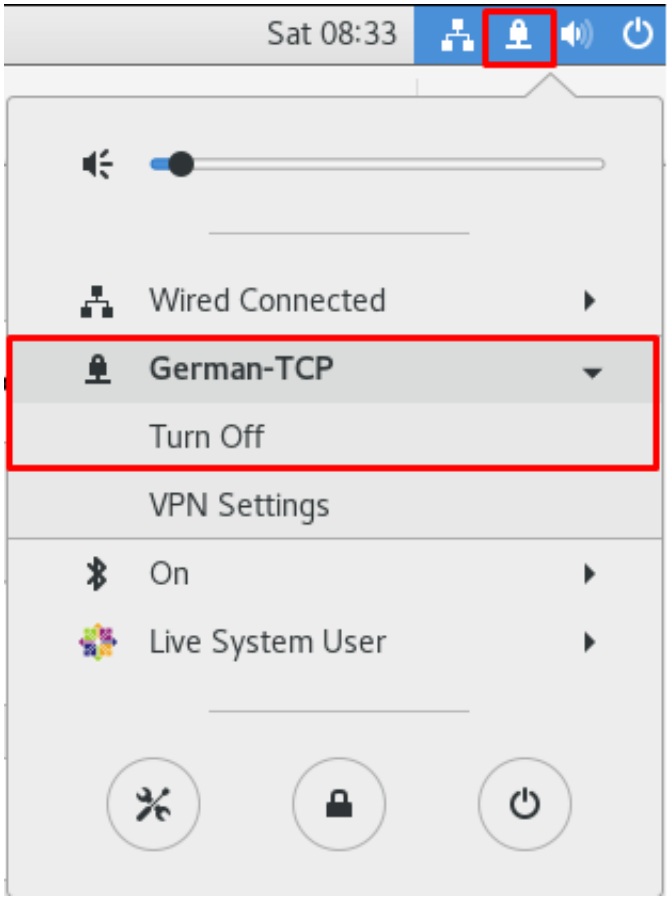
- Enter Connection name: **German-TCP** (Here we use German-TCP, you can change it any other name)
- Select Type: **Password** from drop down menu
- Enter **Username** provided by **PureVPN**
- Enter **Password** provided by **PureVPN**
- Click on folder icon from Certificate folder and add the **‘ca.crt.crt’** file.
- Click ‘**Apply**’



10 Now, connect to PureVPN now. Select the VPN connection you have created. Toggle on the button to connect the VPN.



11 You are connected to VPN now!


Sat 08:33
Wired Connected
German-TCP
Turn Off
VPN Settings
On
Live System User