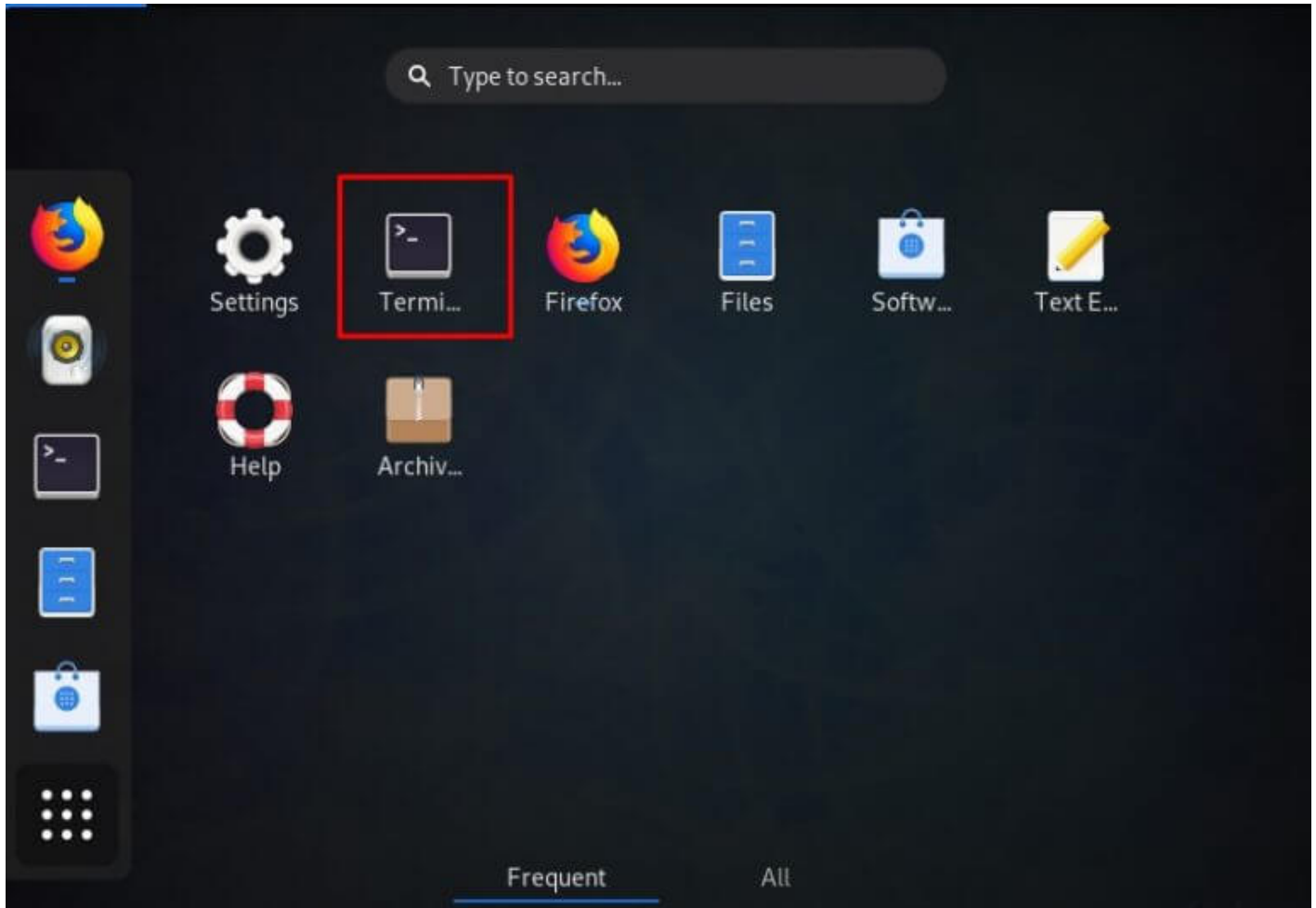


## How to Setup PureVPN L2TP on Linux Fedora 31

You can now enjoy secure browsing on your Linux Fedora. Follow the steps in this tutorial and learn how you can configure PureVPN on your Linux Fedora 31 system using the L2TP protocol:

1 First, go to **Activities** and open the **Terminal**.



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

```
sudo dnf install xl2tpd
```

```
sudo dnf install NetworkManager-l2tp
```

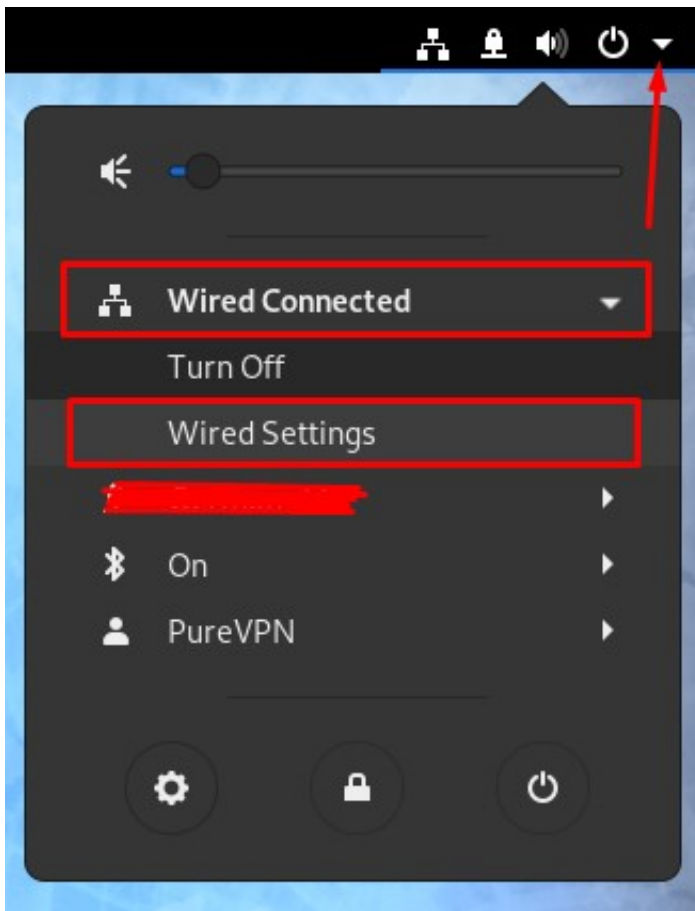
```
sudo dnf install NetworkManager-l2tp-gnome
```

Restart the Network Manager by using the command:

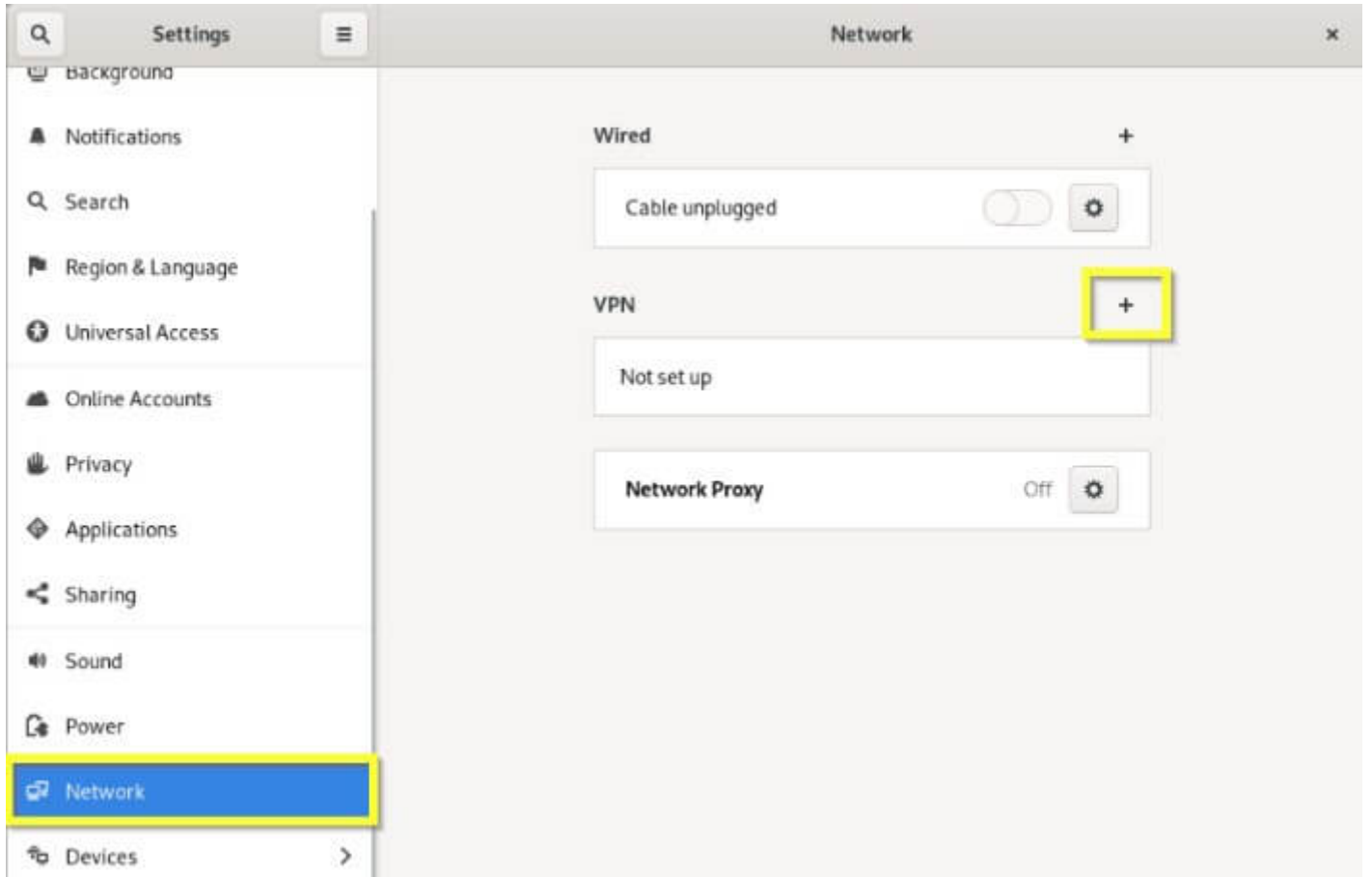
**service NetworkManager restart**

3 Finally, follow these steps:

- Click the **Network Connection**
- Go to **Wired Connected** and select **Wireless Settings**.



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



Cancel Add VPN

---

**Layer 2 Tunneling Protocol (L2TP)**  
Compatible with Microsoft and other L2TP VPN servers.

---

**Multi-protocol VPN client (openconnect)**  
Compatible with Cisco AnyConnect, Juniper Network Connect and Junos Pulse, and PAN GlobalProtect SSL VPNs.

---

**OpenVPN**  
Compatible with the OpenVPN server.

---

**Point-to-Point Tunneling Protocol (PPTP)**  
Compatible with Microsoft and other PPTP VPN servers.

---

**SSH**  
Compatible with the SSH server.

---

**Cisco Compatible VPN (vpnc)**  
Compatible with various Cisco, Juniper, Netscreen, and Sonicwall IPsec-based VPN gateways.

---

**Import from file...**

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

- Connection name: **L2TPConnection**
- Gateway: **pointtoserver.com** (you can use your desired server address here, please [check here](#) for more server addresses)
- Username: **Your VPN username**
- Password: **Your VPN password**

The screenshot shows the 'L2TP Connection VPN' configuration window with the 'Identity' tab selected. The window has a title bar with 'Cancel' and 'Apply' buttons. Below the title bar are tabs for 'Details', 'Identity', 'IPv4', and 'IPv6'. The 'Identity' tab is active. The 'Name' field contains 'L2TP Connection'. Under the 'General' section, the 'Gateway' field contains 'usca.pointtoserver.com'. Under the 'User Authentication' section, the 'User name' field contains 'purevpn' followed by a redacted password. The 'Password' field contains a series of dots and a 'Show password' checkbox. The 'NT Domain' field is empty. At the bottom, there are two buttons: 'IPsec Settings...' (highlighted with a red box) and 'PPP Settings...'.

Click the **IPSec Settings** button after you're done, and use the following settings:

- Check the Enable IPSec tunnel to IPsec host box
- Pre-share key: **12345678**
- Select the **Advanced** option
- Enter Phase 1 Algorithms: **3des-sha1-modp1024**
- Enter Phase 2 Algorithms: **3des-sha1**
- Check the **Disable PFS** box
- Once done, click **OK**.

**L2TP IPsec Options**

Enable IPsec tunnel to L2TP host

**Machine Authentication**

Pre-shared key: ●●●●●●●●

Show password

▼ **Advanced**

Remote ID:

Phase1 Algorithms: 3des-sha1-modp1024

Phase2 Algorithms: 3des-sha1

Phase1 Lifetime: 1:00 - + (HH:MM)

Phase2 Lifetime: 8:00 - + (HH:MM)

Enforce UDP encapsulation

Use IP compression

Use IKEv2 key exchange

Disable PFS

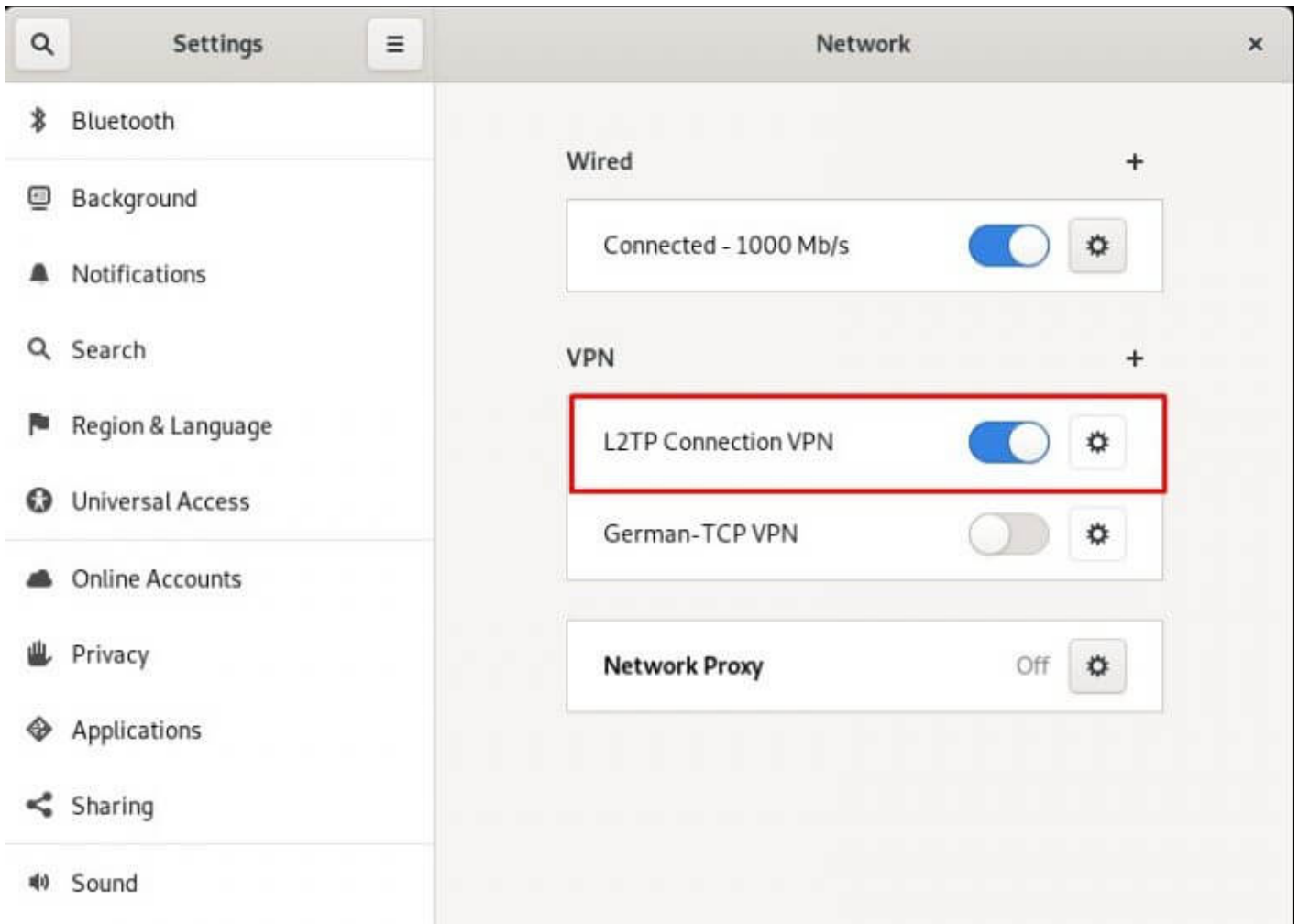
Cancel OK

Next, click the **L2TP PPP Settings** button and use the following settings:

- Check the **Use Point to Point Encryption (MPPE)**
- Check the **Allow BSD data compression**
- Check the **Allow Deflate data compression**
- Check the **Use TCP header compression**
- Check the **Use Protocol field compression negotiation**
- Check the **Use address/control compression**
- Click **Ok** and then **Apply**.



6 Enable your VPN by swiping the toggle.



7 Voila! You are now connected.