

VPN Configuration on VYOS

1. SITE TO SITE VPN :

```
configure
```

```
set vpn ipsec ipsec-interfaces interface eth0
```

```
set vpn ipsec ike-group IKE-1W proposal 1
```

```
set vpn ipsec ike-group IKE-1W proposal 1 encryption aes128
```

```
set vpn ipsec ike-group IKE-1W proposal 1 hash sha1
```

```
set vpn ipsec ike-group IKE-1W proposal 1 dh-group 5
```

```
set vpn ipsec ike-group IKE-1W proposal 2
```

```
set vpn ipsec ike-group IKE-1W proposal 2 encryption aes128
```

```
set vpn ipsec ike-group IKE-1W proposal 2 hash sha1
```

```
set vpn ipsec ike-group IKE-1W proposal 2 dh-group 2
```

```
set vpn ipsec ike-group IKE-1W lifetime 3600
```

```
show vpn ipsec ike-group IKE-1W
```

```
set vpn ipsec esp-group ESP-1W proposal 1
```

```
set vpn ipsec esp-group ESP-1W proposal 1 encryption aes128
```

```
set vpn ipsec esp-group ESP-1W proposal 1 hash sha1
```

```
set vpn ipsec esp-group ESP-1W proposal 2
```

```
set vpn ipsec esp-group ESP-1W proposal 2 encryption 3des
```

```
set vpn ipsec esp-group ESP-1W proposal 2 hash md5
```

```
set vpn ipsec esp-group ESP-1W lifetime 1800
```

```
set vpn ipsec esp-group ESP-1W pfs dh-group5
```

```
show vpn ipsec esp-group ESP-1W
```

```
set vpn ipsec site-to-site peer 1.103.2.42 authentication mode pre-shared-secret
```

```
edit vpn ipsec site-to-site peer 1.103.2.42
```

```
set authentication pre-shared-secret secret
```

```
set default-esp-group ESP-1W set ike-group IKE-1W
set local-address 192.168.0.5
set tunnel 1 local prefix 192.168.0.0/24
set tunnel 1 remote prefix 192.168.1.0/24
set authentication remote-id 192.169.0.3
commit
save
exit
```

2. Remote-access configuration VYOS (OpenVPN) :

a. Server side :

```
configure
set interfaces openvpn vtun0
set interfaces openvpn vtun0 mode server
set interfaces openvpn vtun0 server subnet 192.168.200.0/24

set interfaces openvpn vtun0 tls cert-file /config/auth/server.crt
set interfaces openvpn vtun0 tls dh-file /config/auth/dh.pem
set interfaces openvpn vtun0 tls key-file /config/auth/server.key
set interfaces openvpn vtun0 tls ca-cert-file /config/auth/ca.crt

set interfaces openvpn vtun0 server push-route 35.0.0.0/24
set interfaces openvpn vtun0 openvpn-option "--client-cert-not-required
--script-security 3 --auth-user-pass-verify /usr/share/vyos-oc/auth_pam.pl via-file"

commit
save
exit
```

b. Client side :

Note :

1. First install openvpn
2. Copy ca.art from server and copy to /etc/openvpn/
3. Create client.conf , and add below lines, save it to /etc/openvpn/

```
auth-user-pass
remote-cert-tls server
ca /etc/openvpn/ca.crt
remote 192.168.20.134
client
dev tun
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
verb 3
```

Now run on client side following command

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

3. Remote-access configuration VYOS (L2TP/IPsec) :

a. Server side :

```
configure
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec nat-traversal enable
```

```
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
set vpn l2tp remote-access outside-address 192.168.104.27
set vpn l2tp remote-access client-ip-pool start 192.168.200.1
set vpn l2tp remote-access client-ip-pool stop 192.168.200.100
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret
secret
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username test password
test
commit
save
show vpn l2tp remote-access
exit
```

b. Client side :

1. Packages required:

```
sudo apt-get install openswan
sudo apt-get install xl2tpd
sudo apt-get install l2tp-ipsec-vpn
```

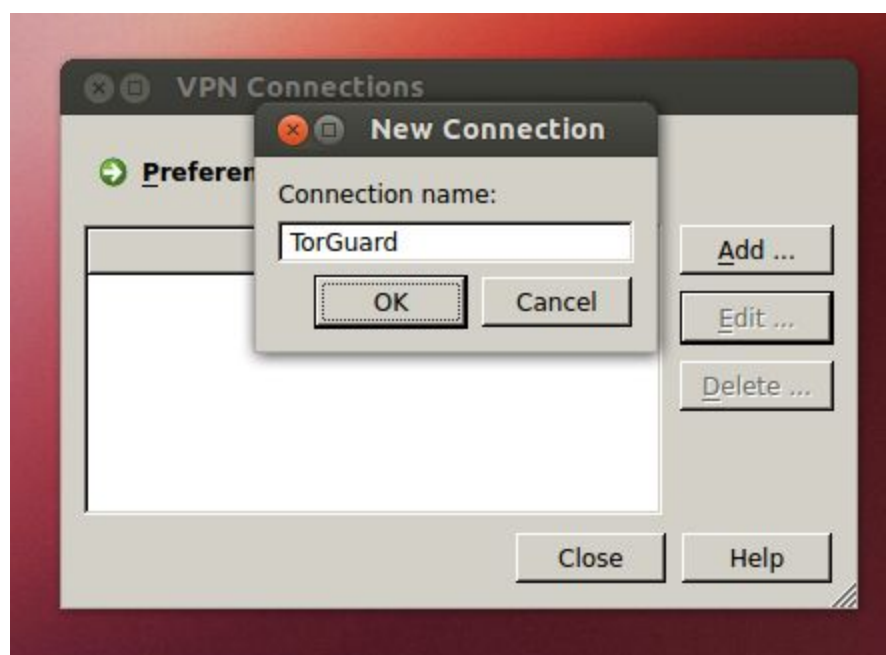
Click on "Dash home", run the "L2TP Ipsec VPN Applet".



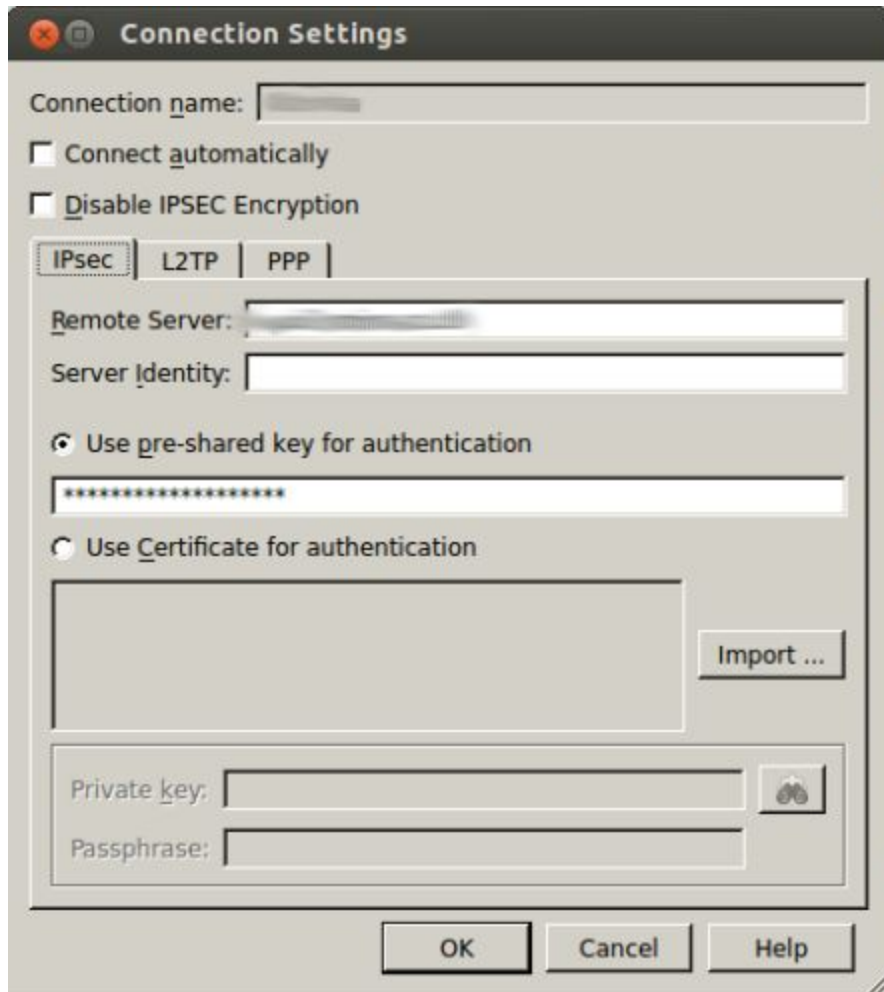
This will create an icon on your top panel with two computers. Click on that icon and choose "Edit Connections...". Provide your Ubuntu user password and click "OK".



The "VPN Connections" window will appear. Click the "Add..." button. Enter the desired "Connection name" (TorGuard for example) and click "OK".



Enter the VPN server address and the pre-shared key



The image shows a 'Connection Settings' dialog box with a title bar containing a close button, a maximize button, and the text 'Connection Settings'. The dialog has several sections:

- Connection name:** A text input field.
- Connect automatically:** A checkbox.
- Disable IPSEC Encryption:** A checkbox.
- Protocol tabs:** Three tabs labeled 'IPsec', 'L2TP', and 'PPP'. The 'IPsec' tab is selected.
- Remote Server:** A text input field.
- Server Identity:** A text input field.
- Authentication options:**
 - Use pre-shared key for authentication:** A radio button that is selected. Below it is a text input field containing a series of asterisks.
 - Use Certificate for authentication:** A radio button that is unselected. Below it is a large empty rectangular box.
- Import button:** A button labeled 'Import ...' located to the right of the certificate box.
- Private key:** A text input field with a key icon button to its right.
- Passphrase:** A text input field.
- Buttons:** At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

Go to the PPP tab and enter the username and password (you can let all the protocols checked as we will unban them later):



The image shows a 'Connection Settings' dialog box with the 'PPP' tab selected. The 'Connection name' field is empty. The 'Connect automatically' checkbox is unchecked. The 'Disable IPSEC Encryption' checkbox is unchecked. The 'PPP' tab is active, showing the 'Use Extensible Authentication Protocol (EAP)' option selected. Below it is a 'Properties ...' button. The 'Allow these protocols' section has four unchecked checkboxes: 'Unencrypted password (PAP)', 'Challenge Authentication Protocol (CHAP)', 'Microsoft CHAP (MS-Chap)', and 'Microsoft CHAP Version 2 (MS-CHAPv2)'. The 'User name' field is empty, and the 'Password' field is filled with asterisks. At the bottom are buttons for 'Peer authentication ...', 'IP settings ...', 'Advanced ...', 'OK', 'Cancel', and 'Help'.

Connection name:

☐ Connect automatically

☐ Disable IPSEC Encryption

IPsec | L2TP | **PPP**

☒ Use Extensible Authentication Protocol (EAP)

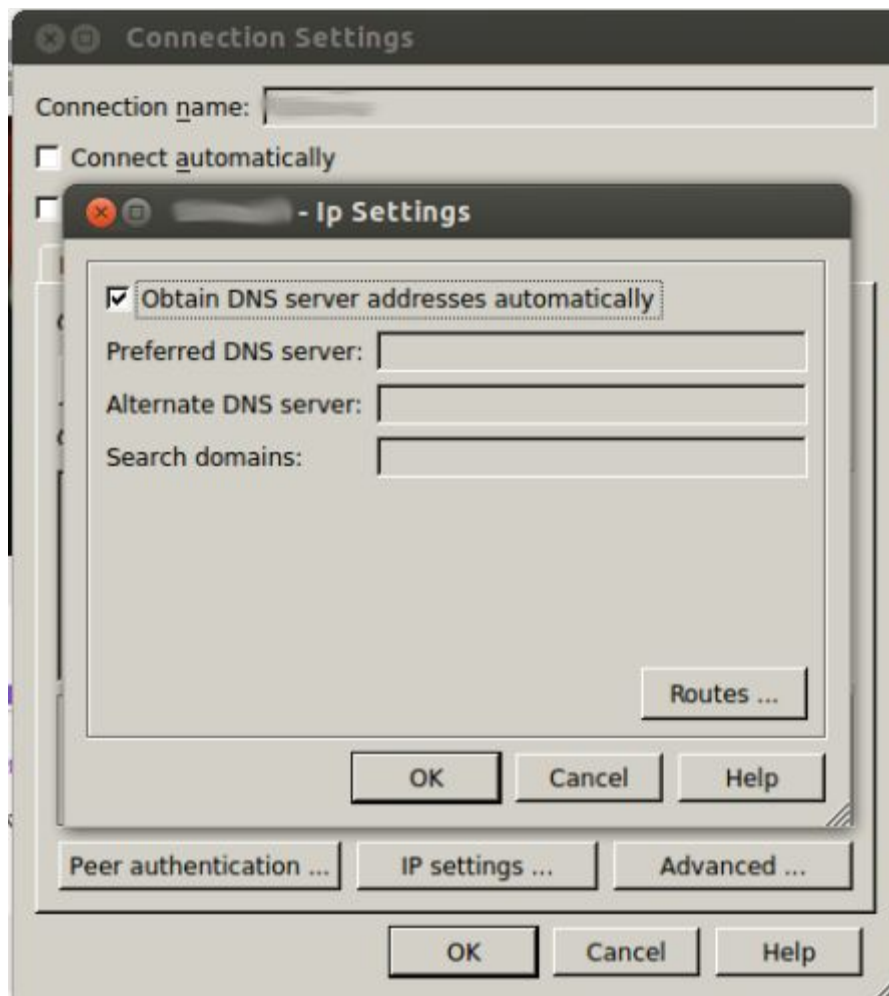
☒ Allow these protocols

- ☐ Unencrypted password (PAP)
- ☐ Challenge Authentication Protocol (CHAP)
- ☐ Microsoft CHAP (MS-Chap)
- ☐ Microsoft CHAP Version 2 (MS-CHAPv2)

User name:

Password:

Click on “IP Settings” and check the box:



Close the “L2TP IPSEC VPN Manager” to apply the changes.

2. Before connecting to the VPN you need to make some more changes in the configuration files

In the file **/etc/ppp/<your_vpn_connection_name>.options.xl2tpd**

- Add the password line
- Be sure the lines refuse-xxxx are commented:

```
$ sudo vi /etc/ppp/<your_vpn_connection_name>.options.xl2tpd
```

```
#debug
```

```
#dump
```

```
#record /var/log/pppd
```

```
plugin passprompt.so
```

```
ipcp-accept-local
```

```
ipcp-accept-remote
```

```
idle 72000
```

```
ktune
```

```
noproxyarp
```

```
asynctest 0
```

```
#noccp
```

```
noauth
```

```
crtstcts
```

```
lock
```

```
hide-password
```

```
modem
```

```
noipx
```

```
ipparam L2tpIPsecVpn-<your_connection>
```

```
promptprog "/usr/bin/L2tpIPsecVpn"
```

```
#refuse-eap
```

```
#refuse-pap
```

```
#refuse-chap
```

```
#refuse-mschap
```

```
#refuse-mschap-v2
```

```
#require-mschap-v2
```

```
remotename ""
```

```
name "<your_username>"
```

```
password "<your_password>"
```

```
defaultroute
```

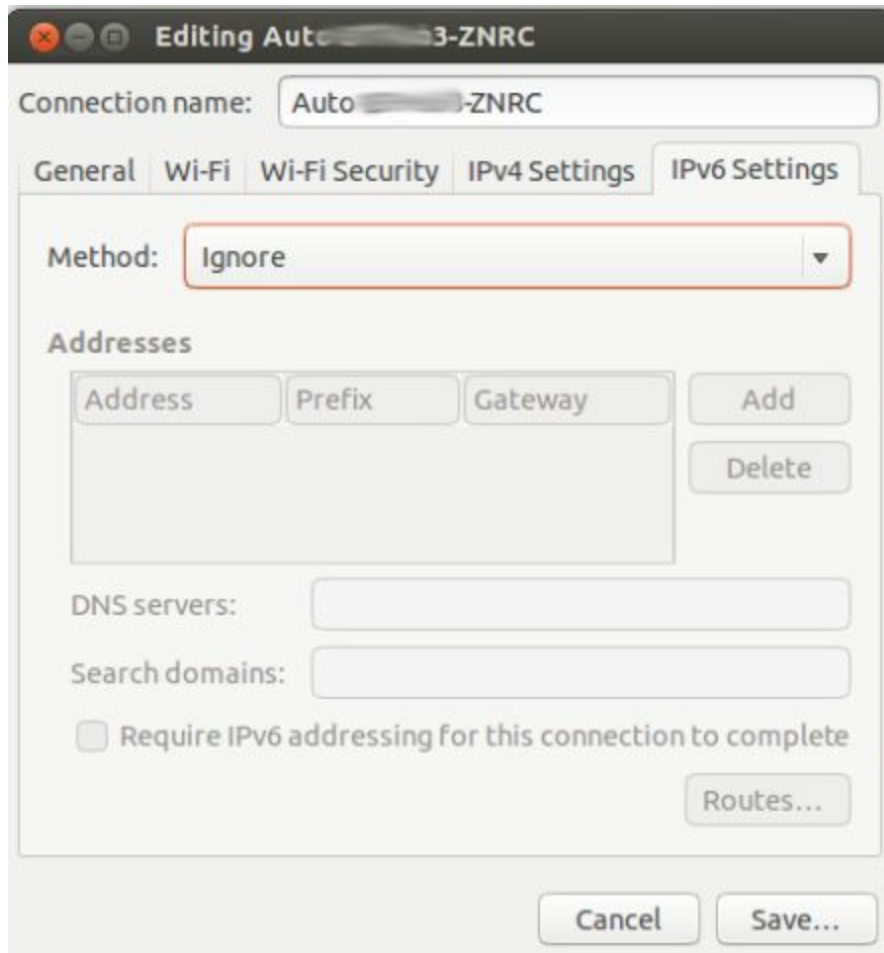
```
usepeerdns
```

3. Restart xl2tp and ipsec to apply the changes

```
sudo /etc/init.d/ipsec restart
```

```
sudo /etc/init.d/xl2tp restart
```

4. Finally, go to your (home) connection settings and deactivate the IPv6:



5. You can now connect to connect to the VPN connection you just created