VPN guide for Linux – Ubuntu

What is VPN and what is VPN used for?

VPN stands for **V**irtual **P**rivate **N**etwork and offers the possibility to establish a secure and encrypted connection via the insecure and public internet. The prerequisite for setting up a connection is an existing Internet connection. It is necessary that the protocol is not blocked by the local provider.

In addition to encryption, when a VPN connection is established, the client is assigned an official Internet address (IP address) from the address range of the University of Bonn and thus has access to services that are otherwise only available to computers at the university.

Furthermore, the VPN connection can only be established after successful authentication with the University of Bonn's Uni-ID.

Establishing a VPN connection to the VPN servers of the University of Bonn is currently required in the following cases:

- Use of the WLAN at the University of Bonn
- Use of the vast majority of literature databases and electronic journals (eMedia) from home or on the road
- Working from the home office

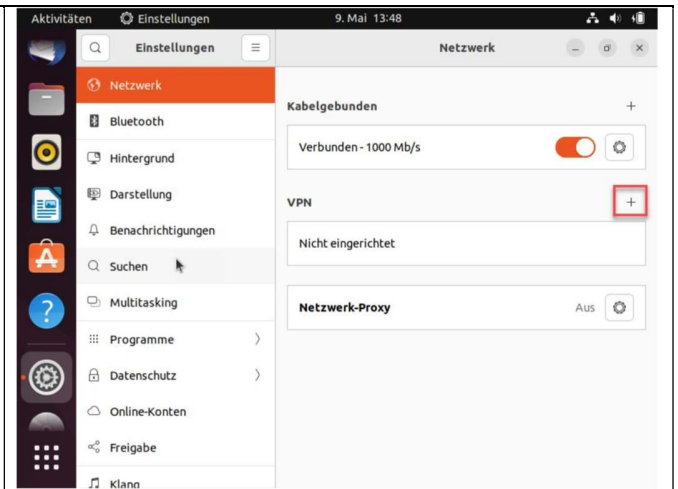Please note that a service may be subject to further restrictions and VPN is not sufficient for access in all cases.
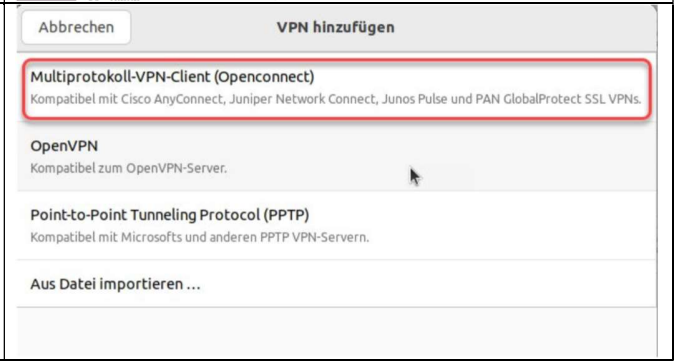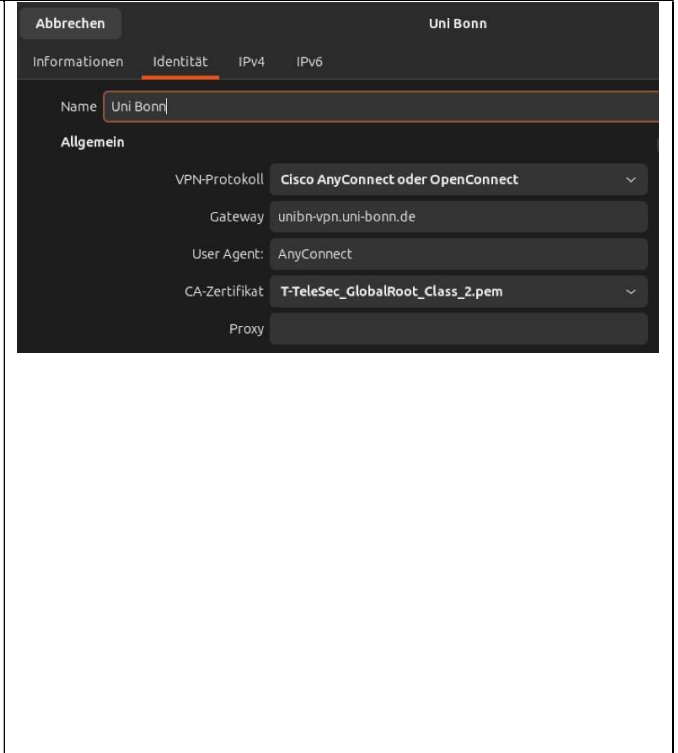
Setting up VPN
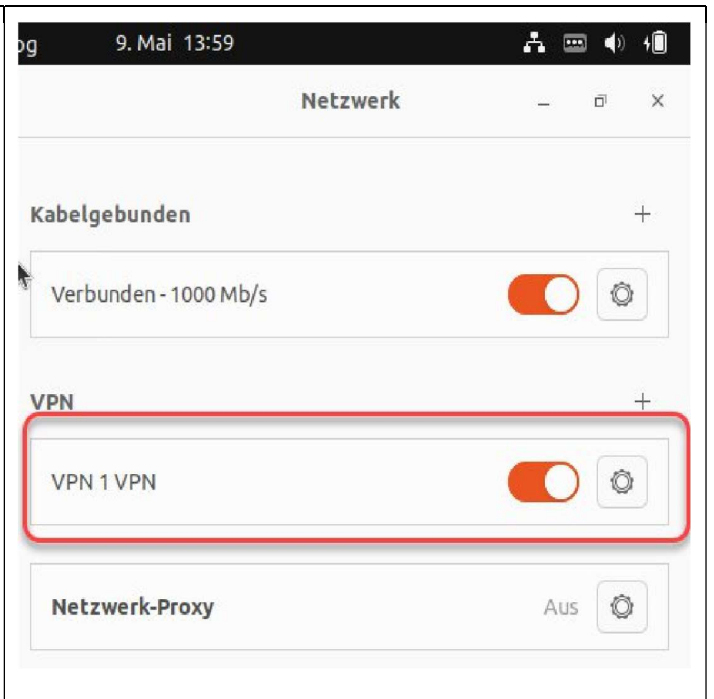
There are two different servers:

- Connections from **external** or home:

    unibn-vpn.uni-bonn.de

- Connections from the WLAN or the network of the University of Bonn **internally**:

    unibn-wlan.uni-bonn.de

Step by step guide

1. Open a terminal window with, for example, the key combination <STRG><Alt><T>.	

2. enter the following commands:
 	
`sudo apt install network-manager-openconnect`
`sudo apt install network-manager-openconnect-gnome`	

3. Enter admin password and install.	
4. Then restart the computer.	

5. Select the settings for the "**Network**" via "**Activities/System settings**" and click on the + sign next to VPN.	
6. Here, "VPN connection compatible with Cisco AnyConnect (openconnect)" must be selected.	
7. Set the following settings: Name: any VPN protocol: Cisco AnyConnect or OpenConnect Gateways for an external connection: **unibn-vpn.uni-bonn.de** CA certificate: via Browse under /etc/ssl/certs/T-TeleSec_GlobalRoot_Class_2.perm to select the certificate. The field user agent should also be displayed here and should be filled with 'AnyConnect'. If this field is not displayed, enter the following into the terminal and repeat the installation steps from the beginning. `sudo apt remove openconnect` If the field is still not displayed afterwards, your system does not support this feature and you will have to log in on the command bar.	
8. Leave all other details unchanged and save the connection via the button "Add".	

Using the VPN Client

1. Now the VPN connection can be switched on and off as desired via the slider.	
2. For authentication, enter the Uni-ID (without @uni-bonn.de) with the corresponding password and click the button "**Connect**".	
3. If you would like to use the VPN client within the university in order to be able to use certain services, you must create another VPN connection according to the instructions above. All details are identical, except that the gateway must now be entered as: unibnwlan.uni-bonn.de	