

1. Einleitung

Die Installation und Konfiguration des VPN-Clients findet auf einem Notebook mit der Desktop-Version von Ubuntu 22.04.1 LTS statt.

2. Repo und Pakete nachinstallieren

Es wird ein Terminal geöffnet:



In diesem Terminal werden folgende Befehle benutzt:

- Das Repo für den SSTP-Client wird hinzugefügt

\$ sudo apt update

- Der SSTP-Client und

\$ sudo apt install sstp-client

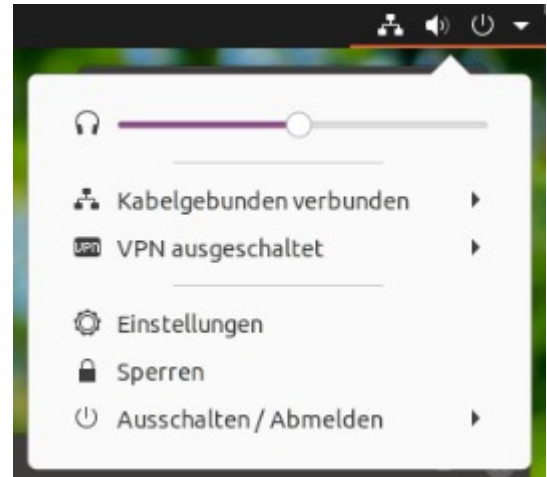
- die GUI für GNOME wird gleich mitinstalliert

- Zum Schluß wird der Netzwerk-Manager neugestartet

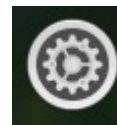
\$ sudo systemctl restart NetworkManager

3. Nach dem Neustart wird in „Einstellungen“ ausgewählt.

Die Einstellungen erhält man, wenn man oben rechts mit der linken Maustaste hineinklickt

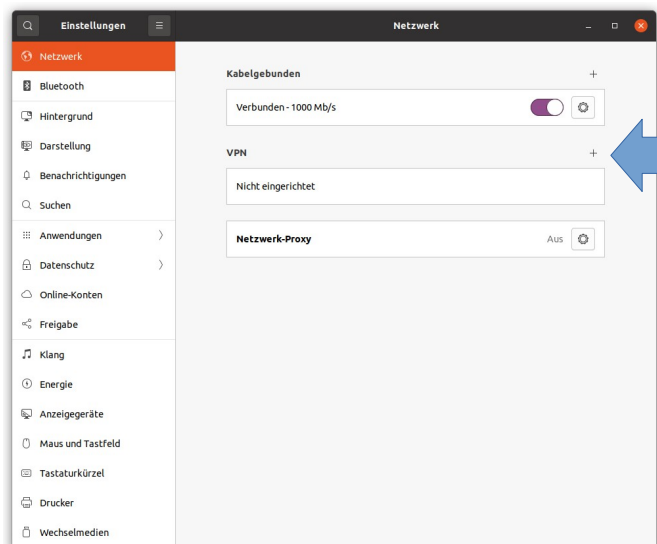


oder unter „Anwendungen anzeigen“ das folgende Symbole auswählt:



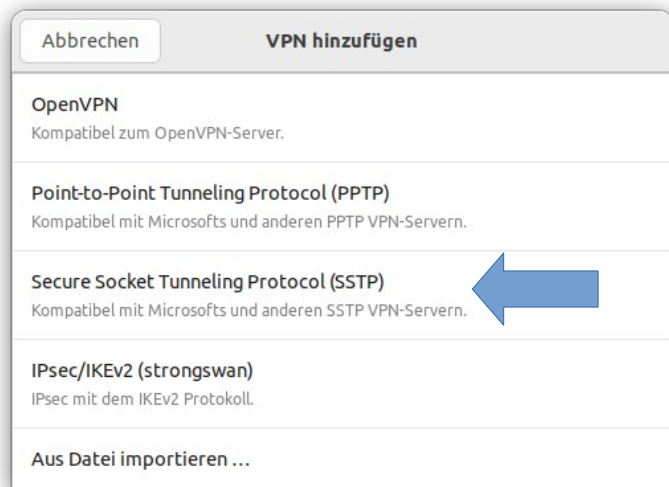
4. VPN unter „Einstellungen / Netzwerk“ einrichten

Unter Netzwerk klickt an das Plus-Symbole bei VPN an (siehe blauen Pfeil in der Abbildung rechts).



Nun öffnet sich das neue Fenster „VPN hinzufügen“.

Hier „Point-to-Point Tunneling Protocol (SSTP)“ auswählen.



5. Karte Identität

Auf der Karte „Identität“ werden folgende Daten eingetragen:

Namen (z.B.):

VPN HS Emden/Leer

Gateway:

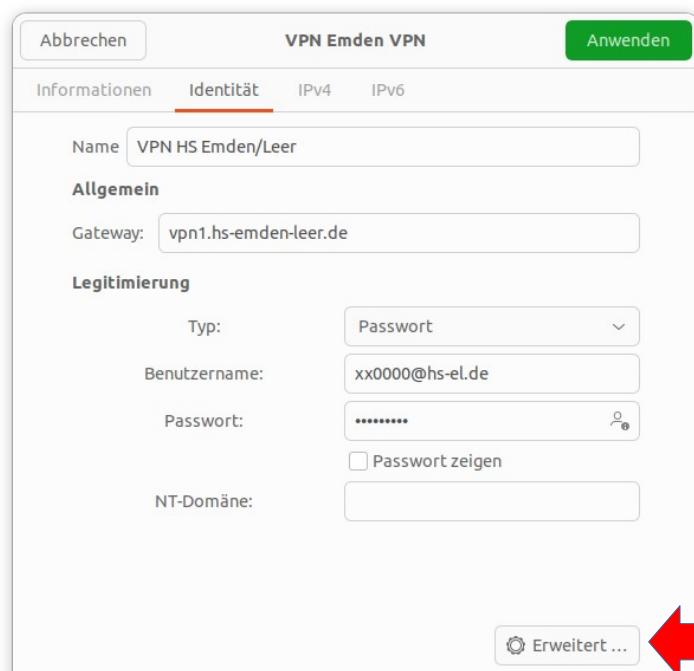
vpn1.hs-emden-leer.de

Benutzername: **xx0000@hs-el.de**

Tragen Sie hier bitte Ihren Hochschul-Login + hs-el.de ein.

Passwort: *********

Tragen Sie hier bitte das gültige Kennwort zu Ihrem Hochschul-Login ein.

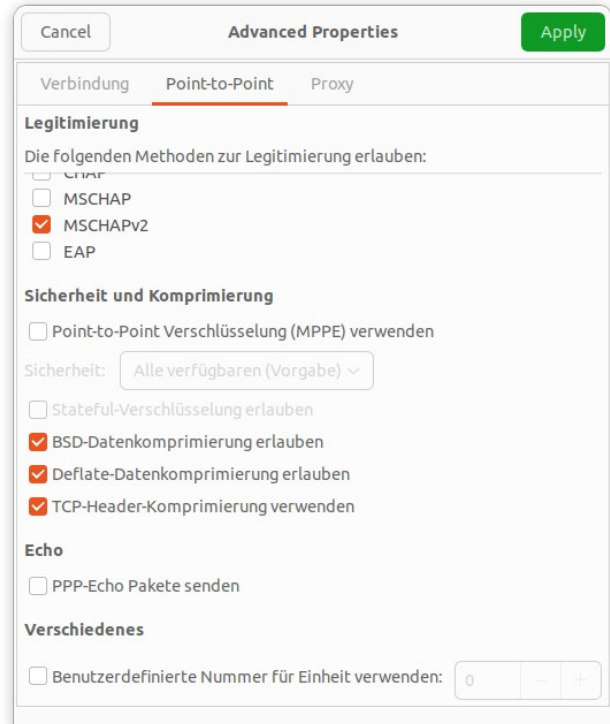


Nach der Eingabe der Daten werden noch die Einstellungen unter „Erweitert...“ (s. Roter Pfeil) bearbeitet.

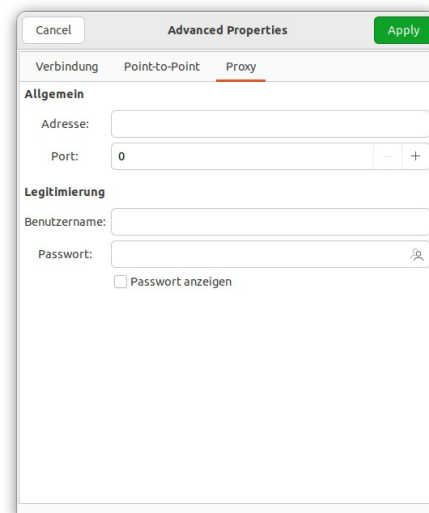
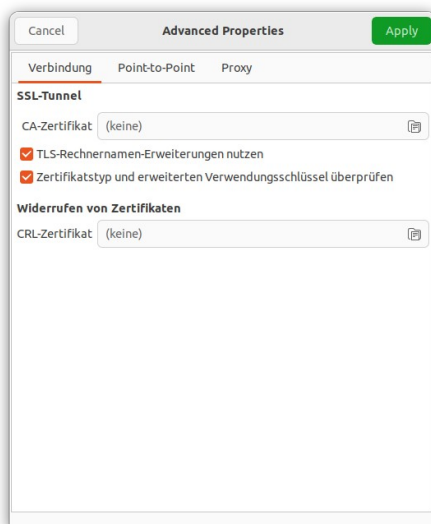
6. Erweiterte Einstellungen

Auf der Karte „Point-to-Point“ wird im Bereich „Legitimierung“ unter „Die folgenden Methoden zur Legitimierung erlauben“ nur noch ein Haken bei „MSCHAPv2“ gesetzt!

„MSCHAP“ und „EAP“ in der Default-Einstellungen werden abgewählt (Haken entfernt).



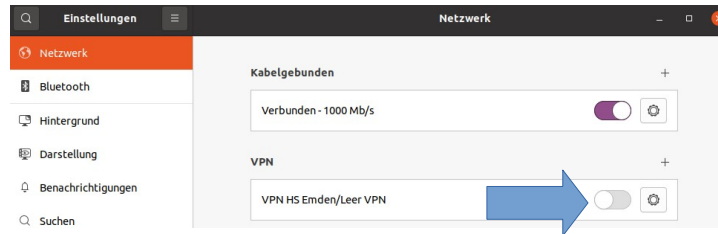
Auf den Karte „Verbindungen“ und „Proxy“ werden keine Änderungen vorgenommen.



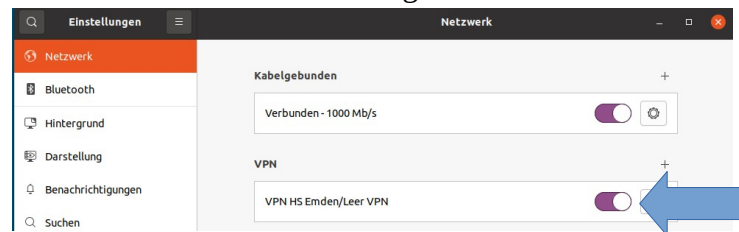
Zum Schluß auf „Apply“ und danach auf „Anwenden“ klicken.

7. VPN einschalten

Unter Einstellungen / Netzwerk wird der VPN-Client durch Ziehen des Schalters nach rechts eingeschaltet



und durch Schieben des Schalters nach Links ausgeschaltet.



Hinweis: Wenn der Schalter „ausgegraut“ ist, ist der VPN-Client nicht aktiv.

8. Verbindung testen

Wenn VPN aktiviert ist und das Paket net-tools installiert ist (`$ sudo apt install net-tools`) kann im „Terminal“ die Konfiguration mit dem Befehl `ifconfig` überprüfen.

Es wird ein Terminal geöffnet:



`$ ifconfig`

```
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.178.86 netmask 255.255.255.0 broadcast 192.168.178.255
        [..]

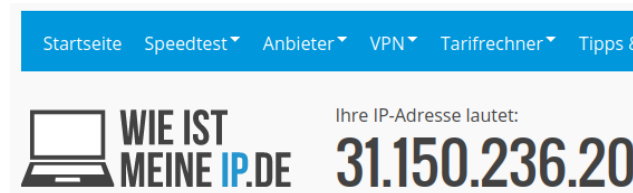
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        [..]

ppp0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1400
        inet 139.13.114.92 netmask 255.255.255.255 destination 139.13.114.50
        ppp txqueuelen 3 (Punkt-zu-Punkt-Verbindung)
        RX packets 11 bytes 371 (371.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 14 bytes 428 (428.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Die Schnittstelle „ppp0“ sollte nun erscheinen. Die IP-Nummer (grau unterlegt) gibt die VPN-IP der Hochschule Emden/Leer an (hier 139.13.114.92).

9. Überprüfen der IP-Nummer

Mit einem Browser wird nun die Webseite <https://www.wieistmeineip.de/> aufgerufen, dort sollte nun nicht mehr die IP: 139.13.114.92 stehen:



10. Split-Tunneling

Für einige Personen und Anwendungen im HomeOffice, kann es hilfreich sein, wenn nur der Datenverkehr zur Hochschule Emden/Leer durch einen VPN-Tunnel gesendet wird.

Bei einer aktiven VPN-Verbindung „**VPN HS Emden/Leer**“ wird ansonsten der komplette Datenverkehr durch den Tunnel gesendet.

Es wird ein Terminal geöffnet:



Konfigurationsdatei von der VPN-Verbindung bearbeiten:

```
$ sudo -i
# cd /etc/NetworkManager/system-connections/
# vi 'VPN HS Emden_Leer.nmconnection'

-> Zeilen in rot hinzufügen.
[connection]
id=VPN HS Emden/Leer
uuid=53b44368-a5c2-4f03-9d08-951db6602f
type=vpn
autoconnect=false
permissions=user:xx0000:;

[vpn]
connection-type=password
gateway=vpn1.hs-emden-leer.de
ignore-cert-warn=yes
password-flags=1
refuse-chap=yes
refuse-eap=yes
refuse-mschap=yes
refuse-mschapv2=no
refuse-pap=yes
tls-verify-key-usage=np
user=xx0000@hs-el.de
```

```
service-type=org.freedesktop.NetworkManager.sstp
```

```
[ipv4]  
method=auto  
never-default=true  
route1=139.13.64.0/18,139.13.114.50  
route2=139.13.0.0/20,139.13.114.50
```

```
[ipv6]  
addr-gen-mode=stable-privacy  
method=auto  
never-default=true
```

```
[proxy]
```

Den Service vom Network-Manager neustarten

```
# systemctl restart NetworkManager.service
```

Nach der Aktivierung der VPN-Verbindung wird im Terminal-Fenster die Routing-Tabelle angezeigt (z.B.):

```
# netstat -r  
Kernel-IP-Routentabelle  
Ziel Router Genmask Flags MSS Fenster irtt Iface  
default 192.168.178.1 0.0.0.0 UG 0 0 0 ens0  
139.13.0.0 139.13.114.50 255.255.240.0 UG 0 0 0 ppp0  
139.13.64.0 139.13.114.50 255.255.192.0 UG 0 0 0 ppp0  
vpn1.hs-emden-l 192.168.178.1 255.255.255.255 UGH 0 0 0 ens0  
139.13.114.50 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0  
link-local 0.0.0.0 255.255.0.0 U 0 0 0 ens0  
192.168.178.0 0.0.0.0 255.255.255.0 U 0 0 0 ens0  
192.168.178.1 0.0.0.0 255.255.255.255 UH 0 0 0 ens0
```

Wenn die beiden roten Zeilen vorhanden sind, wird nur noch der Datentransfer der „Hochschule Emden/Leer“ durch die VPN-Verbindung gesendet.