1. Einleitung

Die Installation und Konfiguration des VPN-Clients findet auf einen PC mit der Desktop-Version von Ubuntu 20.04.2 LTS statt.

Neu: Mit Split-Tunneling-VPN

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 add-apt-repository ppa:eivnaes/network-manager-sstp
  $ sudo apt update

- Der SSTP-Client und

  $ sudo apt install sstp-client

- die GUI für GNOME werden installiert

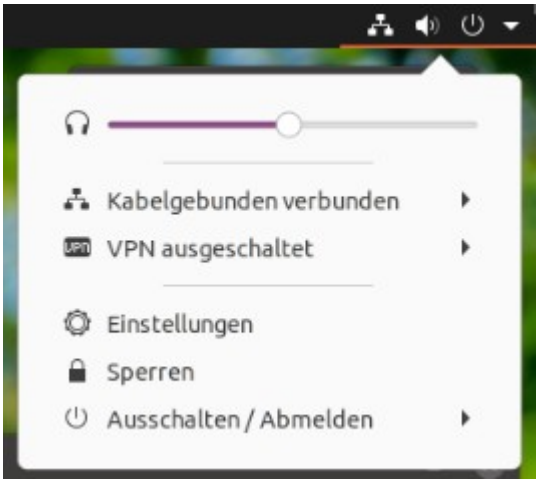
  $ sudo apt install network-manager-sstp-gnome

- Zum Schluß wird der PC neugestartet

  $ sudo reboot

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

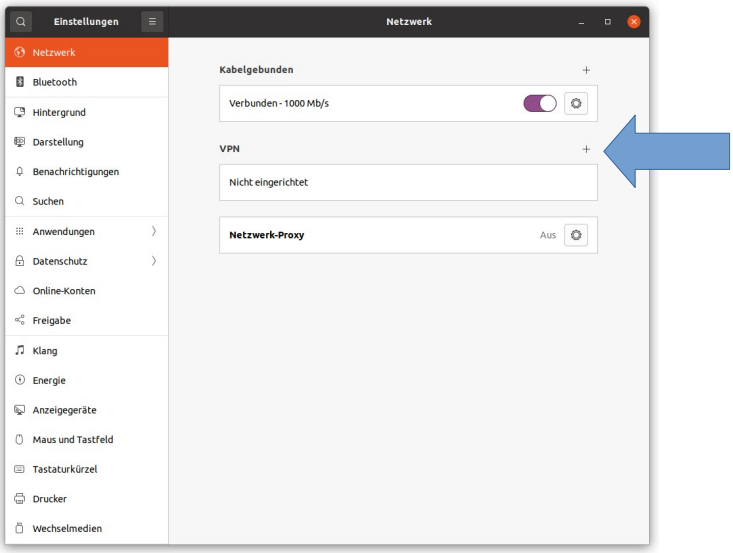
Die Einstellungen erhält man, wenn man oben rechts mit der linken Maustaste hineinklickt



oder unter „Anwendungen anzeigen“ das folgende Symbole auswählt:

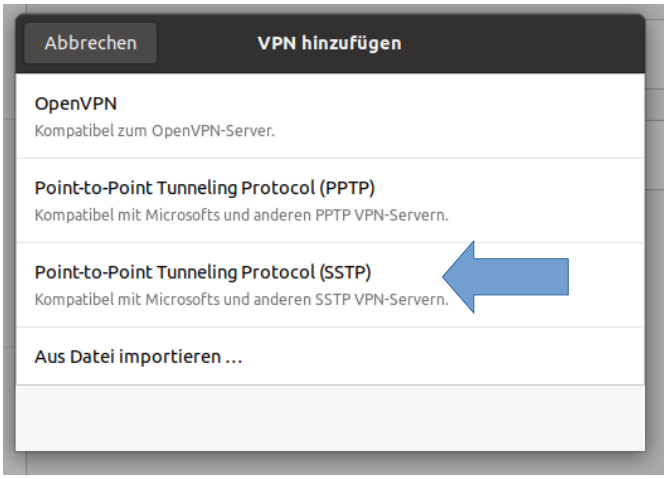
4. VPN unter „Einstellungen / Netzwerk“ einrichten

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



Nun öffnet sich das neues Fenster „VPN hinzufügen“.

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



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.

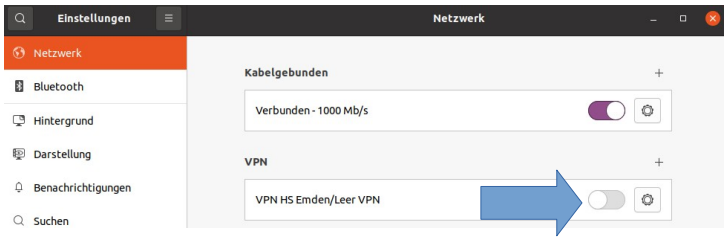
Passwort: **********
Tragen Sie hier bitte das gültige Login ein.

Zum Schluß auf „Anwenden“ klicken.

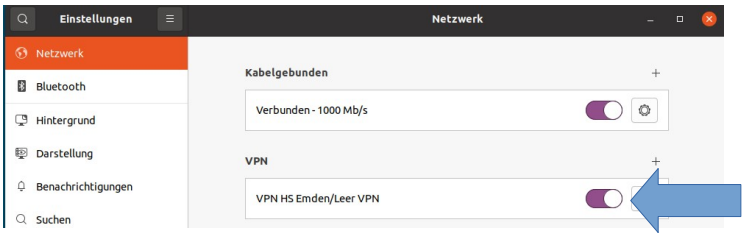
Achtung: **Alle anderen Karten werden nicht bearbeitet!**

5. 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.*

6. 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: 

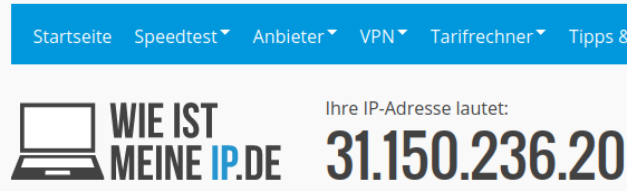
$ ifconfig

```
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).

7. IP – Überprüfung

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



8. 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]
gateway=vpn1.hs-emden-leer.de
password-flags=1
refuse-chap=yes
refuse-eap=yes
refuse-pap=yes
user=xx0000@hs-el.de
service-type=org.freedesktop.NetworkManager.sstp

[ipv4]
dns-search=
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
dns-search=
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.