

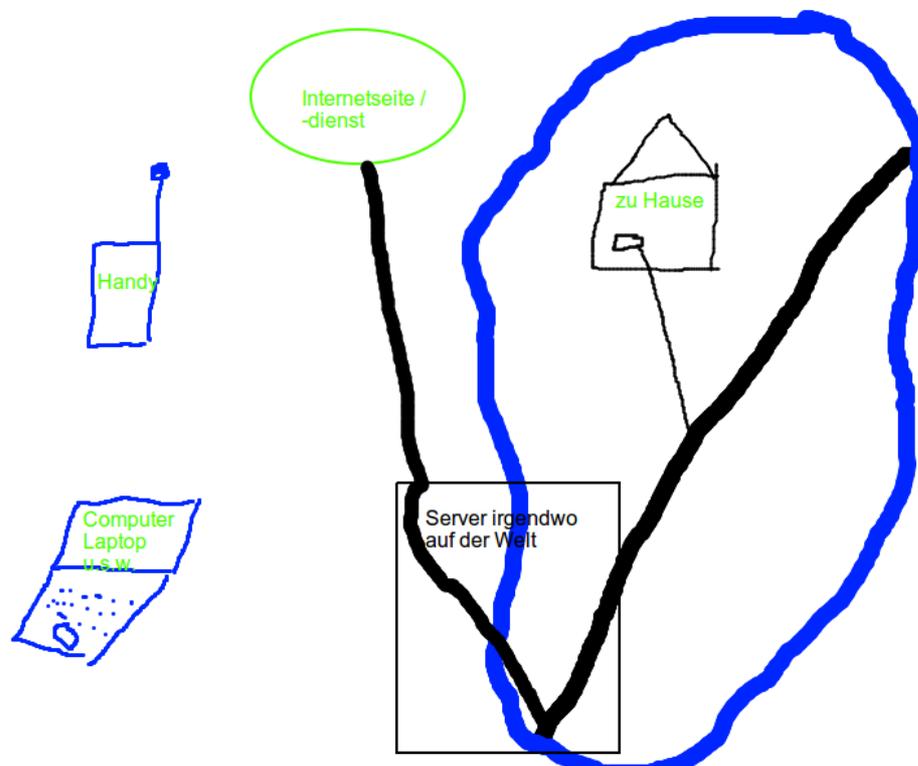
Linux-Mint-Rechner (18.3 Sylvia) via VPN mit Fritzbox (7520) verbinden:

Vorwort:

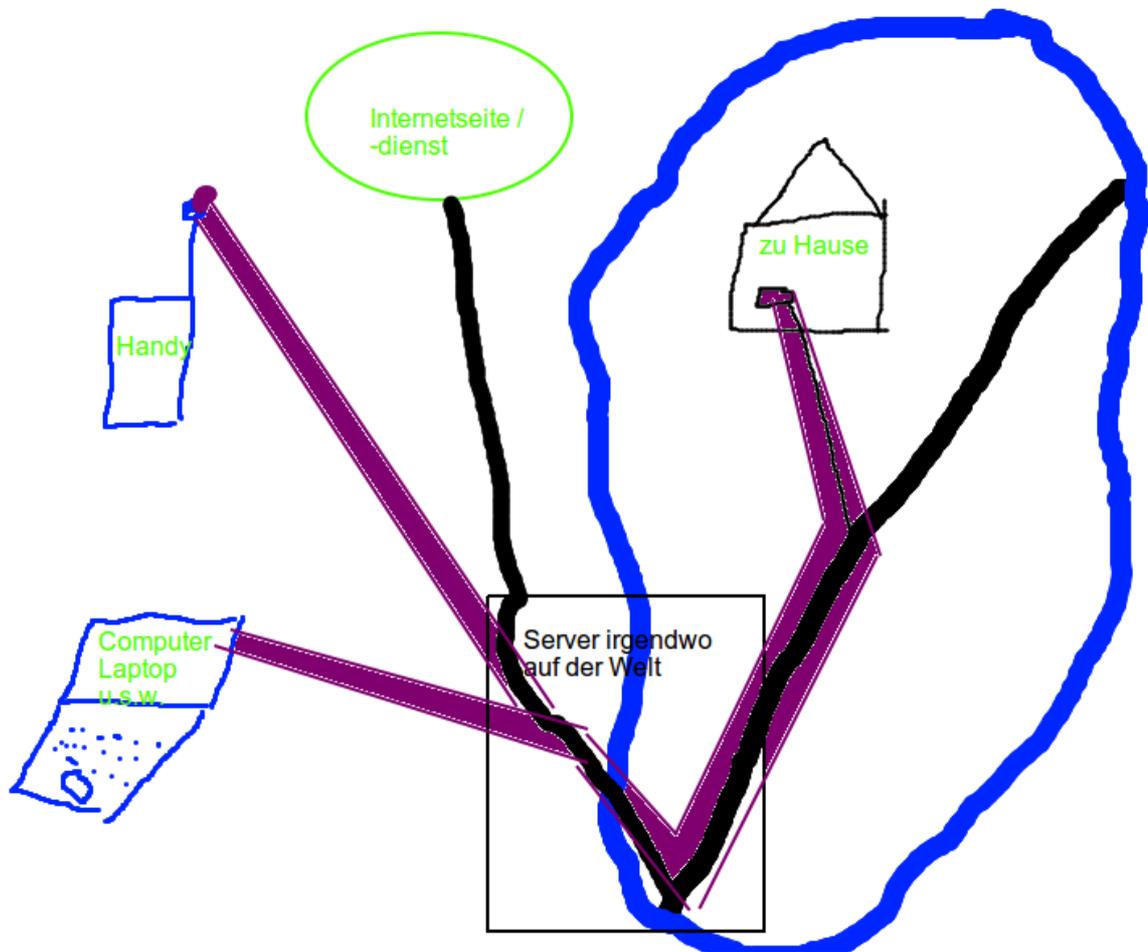
Grundsätzlich können wir auf einen Internetdienst von zu Hause über den PC und den Router zugreifen. Von dort aus wird die „heimische“ IP gesendet. Die Internetseite empfängt also die IP, sagen wir mal aus unserem zu Hause in Hannover. Die Internetseite weiß das / kann das wissen / herausfinden. Seiten z.B. mit Geoblocking können verhindern oder gerade erfordern, dass / ob ein Rechner aus einem bestimmten Bereich / Netzbetreiber kommt. Die Seite wird – je nach Einstellung – also nur dann – oder gerade nicht – angezeigt, wenn die bestimmte Anforderung erfüllt ist.

Wenn wir z.B. mit Handy oder Laptop außerhalb des WLAN zu Hause sind – z.B. im Urlaub – kann es daher sein, dass diese Seite nicht angezeigt wird. Das kann ja sogar die eigene Webseite sein, die zur Vermeidung von Hackerangriffen nicht aus bestimmten Staaten erreichbar sein soll. Sagen wir: grundsätzlich soll niemand auf die eigene Webseite aus dem Land Q zugreifen dürfen. Nun sind wir aber selbst auf Reise in dem Land Q und möchten auf unsere eigene Webseite zugreifen. Das wäre ein Beispiel, wofür wir den VPN nutzen können. Denn der VPN baut einen „Tunnel“ zum eigenen Router zu Hause auf, wodurch dann der Laptop zunächst auf den eigenen Router „zu Hause“ zurückgreift und dieser dann die Webseite abrufen und durch den Tunnel schicken. Die (eigene) Webseite, die in das Land Q nicht senden wollen würde, sendet tatsächlich nur an die FritzBox zu Hause, hier also Hannover und von dort wird der Seiteninhalt weitergeleitet durch den Tunnel auf unser eigenes Endgerät in Land Q.

Gedanklicher Aufbau OHNE VPN:



Gedanklicher Aufbau MIT VPN:



In diesem Beispiel wird der VPN-Tunnel in violett dargestellt. Die mobilen Geräte bauen um die bzw. innerhalb der „Internetleitung“ einen Tunnel auf, in den der „öffentliche“ Netzverkehr nicht hineinschauen kann. Deshalb bietet sich VPN auch an, wenn man z.B. auf einen Server zu Hause zugreifen möchte und weder der eigene Telefonnetzbetreiber noch ein Betreiber eines öffentlich genutzten WLAN in den Datentransfer hineingucken können soll. Vom Router zu Hause läuft die Verbindung dann so, als würde man aus dem eigenen WLAN zu Hause sitzen..... „Von Router zur abgerufenen Internetseite“ bietet der VPN-Tunnel also keine gesonderte Sicherheit. Das ist also so sicher, als wenn man vom Arbeitsplatz zu Hause (in Hannover) aus die Internetseite abrufen.

Nun zur Umsetzung von A-Z auf den nächsten Seiten:

TEIL 1: Vorbereitung

Die Fritz-Box muss **für einen Zugriff via Internet** eine öffentliche IP4-Adresse haben. Das bedeutet, dass externe Rechner über die IP darauf zugreifen dürfen.

Als Kunde von 1&1 musste ich das dort (durch 1&1) einschalten / freischalten lassen damals.

Am besten machen wir uns schon jetzt Gedanken, welche Passworte und Variablen wir später benutzen möchten – hierfür gerne in „meine eigene“ schon vorab etwas ausdenken / später eintragen:

Variable	hier in der Anleitung als Beispiel	„meine eigene“
ddns-subdomain	leitungnachhause.ddns.net	
Anmeldename bei ddns-Anbieter	Benutzer1212@mail.xy	
Passwort bei ddns-anbieter	xyz4	
VPN-Benutzer in FritzBox	FB-Benutzername	
Passwort für FritzBox-VPN-Benutzer	abc4	
Gruppenpasswort (wird von der Fritzbox jeweils individuell festgelegt)	DfGGeRQs4	

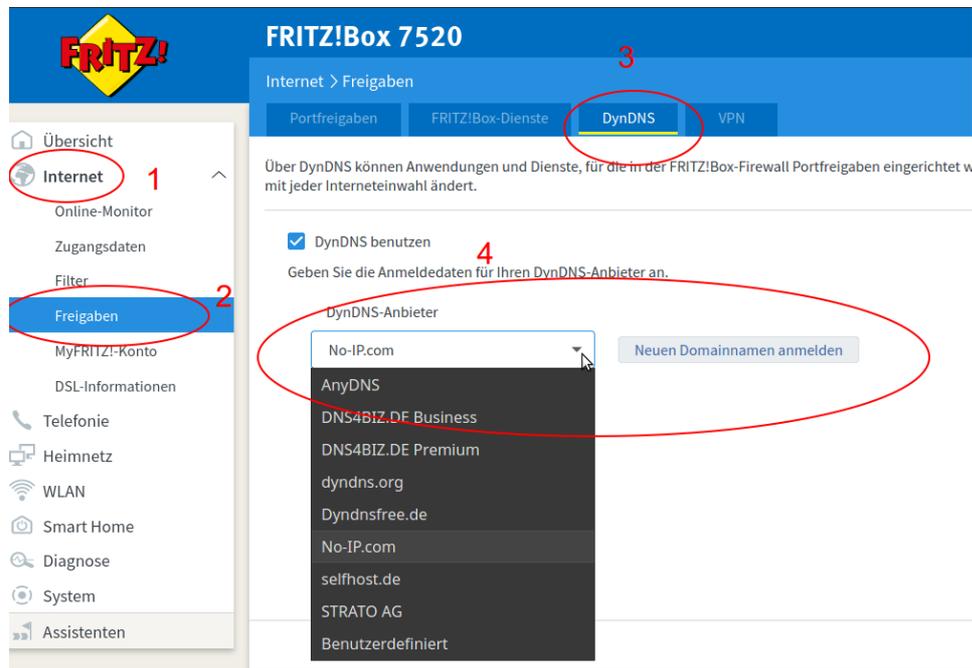
TEIL 2: Fritzbox von extern erreichbar machen:

Die Fritzbox erhält vom eigenen Internetanbieter (z.B. Vodafone, 1&1, Telekom etc.) eine IP zugeteilt. Allerdings ist die Regel, dass diese IP sich ändern, wenn sich die Fritzbox neu mit dem Internet verbindet. In aller Regel geschieht dies mindestens ein Mal täglich.

Die eigene IP kann man sich über verschiedene Internetdienste anzeigen lassen. Ich nutze in der Regel: <https://www.wieistmeineip.de/>

Mit dieser herausgefundenen IP – z.B. 92.115.55.111 – kann man die eigene Fritzbox ansprechen. Problem: Wenn sich die IP ändert, kann man von extern ja nicht die IP herausfinden, die der eigene heimische Internetanschluss gerade vom Telefonanbieter zugewiesen bekommen hat.

Dafür gibt es verschiedene Dienste, die auch die Fritzbox unterstützt. Man kann ihn in der Fritzbox einstellen:



Ich selbst nutze No-IP.com und bin damit sehr zufrieden. Man muss dort ein Kundenkonto erstellen und sich eine dort angebotene „Subdomain“ [z.B. leitungnachhause.ddns.net] eintragen. Das geht sehr schnell. Die dortigen Zugangsdaten muss man dann in der vorstehenden Seite eintragen und schon registriert sich die Fritzbox bei jedem Start / IP-Wechsel dort und die selbst gewählte Subdomain – hier: als Beispiel - leitungnachhause.ddns.net weist immer auf die aktuelle IP, so dass wir also die fritzbox über leitungnachhause.ddns.net immer erreichen können und uns der Wechsel der IP-Adresse nach spätestens 24 Stunden nicht stört.

Für das Beispiel NO-IP wäre diese Seite dann in dem Beispiel wie folgt auszufüllen:

Portfreigaben FRITZ!Box-Dienste **DynDNS** VPN

Über DynDNS können Anwendungen und Dienste, für die in der FRITZ!Box-Fire mit jeder Internetwahl ändert.

DynDNS benutzen

Geben Sie die Anmeldedaten für Ihren DynDNS-Anbieter an.

DynDNS-Anbieter
No-IP.com [Neuen Domainname](#)

Domainname
leitungnachhause.ddns.net

Benutzername
Benutzer1212@mail.xy

Kennwort
xyz4

Dann mit OK bestätigen.

Dann müsste die Fritzbox von extern erreicht werden können über [hier im Beispiel]

leitungnachhause.ddns.net

Das brauchen wir dann auch für unser VPN gleich.

Um sicher zu gehen, sollte noch sichergestellt sein, dass das aus eingestellt ist. Das kann hier eingesehen werden. Falls nicht aktiviert, muss die Checkbox angeklickt werden und ferner müssten jedenfalls die Erreichbarkeit leitungnachhause.ddns.net eingestellt werden.

Es müsste etwa so aussehen:

FRITZ!Box 7520

Internet > Freigaben

Portfreigaben **FRITZ!Box-Dienste** DynDNS VPN

Sie können hier den sicheren Zugriff auf Ihre FRITZ!Box einrichten. Der Zugriff auf die FRITZ!Box-Bedienoberfläche erfolgt über Ihren Benutzernamen und Ihr Kennwort geschützt.

Hinweis:
Einstellungen, die Sie hier vornehmen, gelten auch für den Zugang zur FRITZ!Box aus dem Internet über den Dienst MyF

Internetzugriff

Internetzugriff auf die FRITZ!Box über HTTPS aktiviert
Diese Option ermöglicht den Zugang auf die FRITZ!Box aus dem Internet. Zugang haben alle FRITZ!Box-Benutzer. Bitte beachten Sie bei dieser Einstellung unsere Hinweise für sichere Kennwörter.

TCP-Port für HTTPS: 49686
(im Bereich von 1 bis 65535)

Internet-Adresse Ihrer FRITZ!Box: leitungnachhause.ddns.net:49686 oder
https://92.115.55.111:49686

Unter diesen Adressen ist Ihre FRITZ!Box aus dem Internet erreichbar.

TEIL 3: VPN auf Fritzbox aktivieren / einstellen:

1. auf **INTERNET** klicken
2. auf **FREIGABEN** klicken:

Beispiel:

FRITZ!

Übersicht

Internet 1

Online-Monitor

Zugangsdaten

Filter

Freigaben 2

MyFRITZ!-Konto

DSL-Informationen

Telefonie

Heimnetz

WLAN

3. auf VPN klicken:

Beispiel:

The screenshot shows the FritzBox web interface. In the left-hand navigation menu, the 'Internet' tab is circled in red and labeled with a red '1'. Below it, the 'Freigaben' (Port Forwarding) tab is also circled in red and labeled with a red '2'. In the top navigation bar, the 'VPN' tab is circled in red and labeled with a red '3'. The main content area shows the 'VPN' settings page, with a table for 'VPN-Verbindungen zur FRITZ!Box' and a section for 'VPN-Verbindungen zwischen der FRITZ!Box und anderen Netzwerken'.

4. auf VPN-VERBINDUNG hinzufügen klicken:

The screenshot shows the 'VPN' settings page. The 'VPN' tab in the top navigation bar is circled in red and labeled with a red '3'. Below the navigation bar, there is a text block: 'Über VPN kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden. Weitere Hinweise, Werkzeuge und Tipps zu VPN finden Sie auf www.avm.de/service/vpn.' Below this, there are two tables. The first table has columns for 'Internet', 'Virtuelle IP-Adresse', and 'Status'. The second table has columns for 'lokales Netz', 'entferntes Netz', 'Datenübertragung über VPN', and 'Status'. Below the second table, it says 'Es sind keine VPN-Verbindungen eingerichtet.' At the bottom right, a button labeled 'VPN-Verbindung hinzufügen' is circled in red and labeled with a red '4'.

DANN:

Bitte wählen Sie die Art der VPN-Verbindung, die erstellt werden soll:

Fernzugang für einen Benutzer einrichten

Wählen Sie auf der folgenden Seite den gewünschten FRITZ!Box-Benutzer, öffnen Sie den E

Ihr Heimnetz mit einem anderen FRITZ!Box-Netzwerk verbinden (LAN-LAN-Kopplung)

Diese FRITZ!Box mit einem Firmen-VPN verbinden

Eine VPN-Konfiguration aus einer vorhandenen VPN-Einstellungsdatei importieren

DANN: mir Weiter bestätigen

DANN: Benutzer hinzufügen anklicken

DANN: Benutzernamen für die Fritzbox eingeben, hier im Beispiel: **FB-Benutzername**

DANN: Kennwort für den Benutzer eingeben, hier im Beispiel: **abc4**

unten: Checkbox für VPN anklicken

Dann auf Übernehmen klicken und damit den Benutzer speichern.

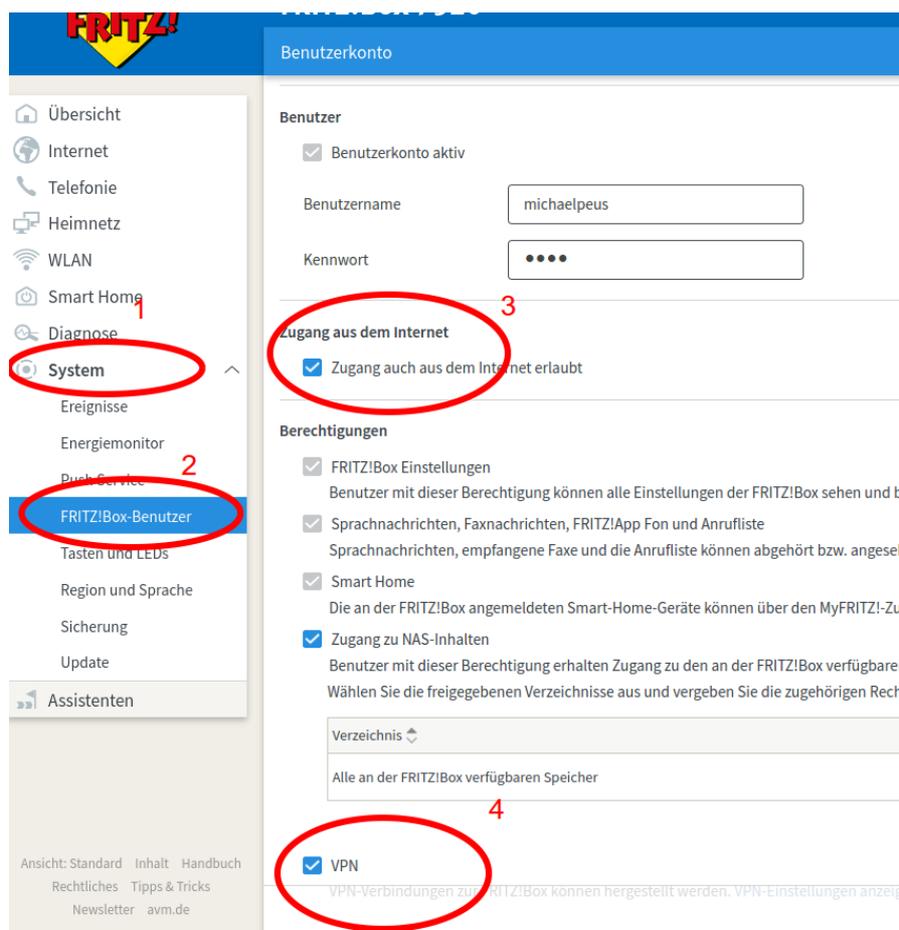
Jetzt fordert die Fritzbox eine Bestätigung an und die LEDs blinken. Entweder man hat Zugriff auf die Fritzbox und drückt dort (irgend) einen (beliebigen) Knopf ODER man hat ein an der Fritz-Box angeschlossenes Telefon verfügbar und gibt den angeforderten Code „*.....“ ein und drückt die Wahl-Taste.

Im Pop-Up-Fenster dann „Ok“ drücken, um den Vorgang abzuschließen.

Jetzt kommt ein Popup, welches fragt, ob man sich die Einstellungen für iOS und Androidgeräte. Hier drücken wir auf OK. Besonders relevant ist die Zeile „IPSec-Schlüssel / Shared Secret“ mit dem dahinterstehenden Code. Dieser Code ist das, was ich im Beispiel **DfGGeRQs4** genannt habe. Den Code, der in dieser Zeile steht, sollte dann oben in die „eigene“ Tabelle eingetragen werden. Dann kann das Fenster geschlossen werden.

WIR ÜBERPRÜFEN alles und stellen den Benutzer auf der Fritzbox ggfls. noch so ein:

Wenn das alles so eingestellt ist (insbesondere Checkbox in Nr. 4; Nr. 3 MUSS NICHT), ist nun alles fertig in den Einstellungen der Fritzbox!

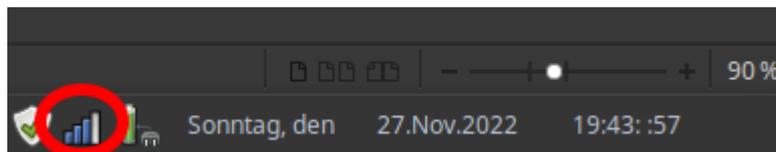


TEIL 4: jetzt kommt die Einstellung beim Endgerät

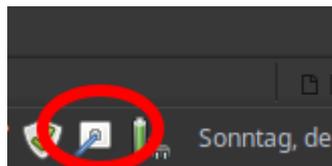
A. Linux-Mint 18.3 Sylvia

1. Rechtsklick auf das Symbol zur Internetverbindung

entweder WLAN:



oder LAN:



Einstellungen in LINUX - VPN [CISCO-kompatibler.....] auswählen im Network-Manager - Edit Connections - Add wie folgt vornehmen:

Name der Verbindung (egtl egal, wir nennen sie evtl. VV14)

Gateway: leitungnachhause.ddns.net

Benutzername des FRITZ!Box-Benutzers: [FB-Benutzername](#)

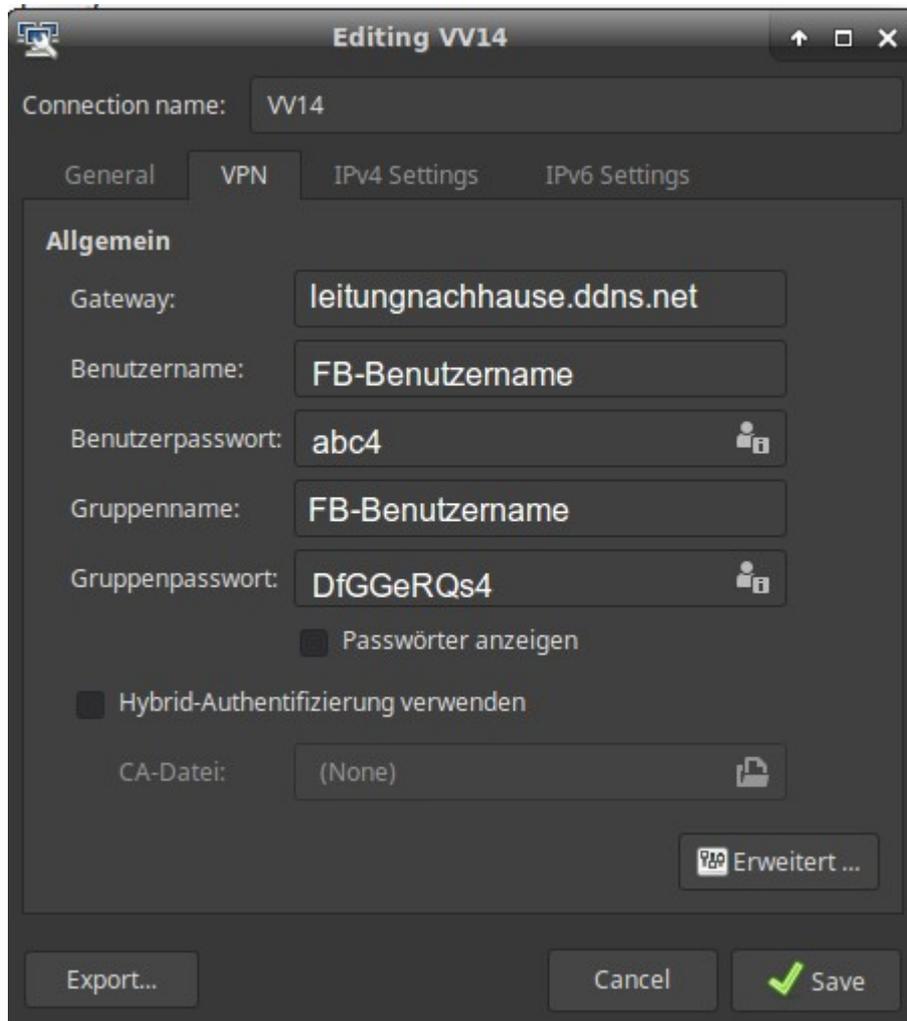
Benutzerpasswort: [abc4](#)

Gruppenname: [FB-Benutzername](#)

Gruppenpasswort: [DfGGeRQs4](#)

TIPP: in den Passwortfeldern kann man „hinten“ anklicken und dann erscheint die Auswahl, ob das jeweilige Passwort immer abgefragt werden soll, oder für jeden Benutzer eingetragen wird etc. Ich habe ausgewählt, dass es für jeden Benutzer (des Gerätes) gespeichert wird. DANN kann man es auch eintragen – *in der Standardeinstellung nicht.*

Das müsste dann wie folgt aussenen:

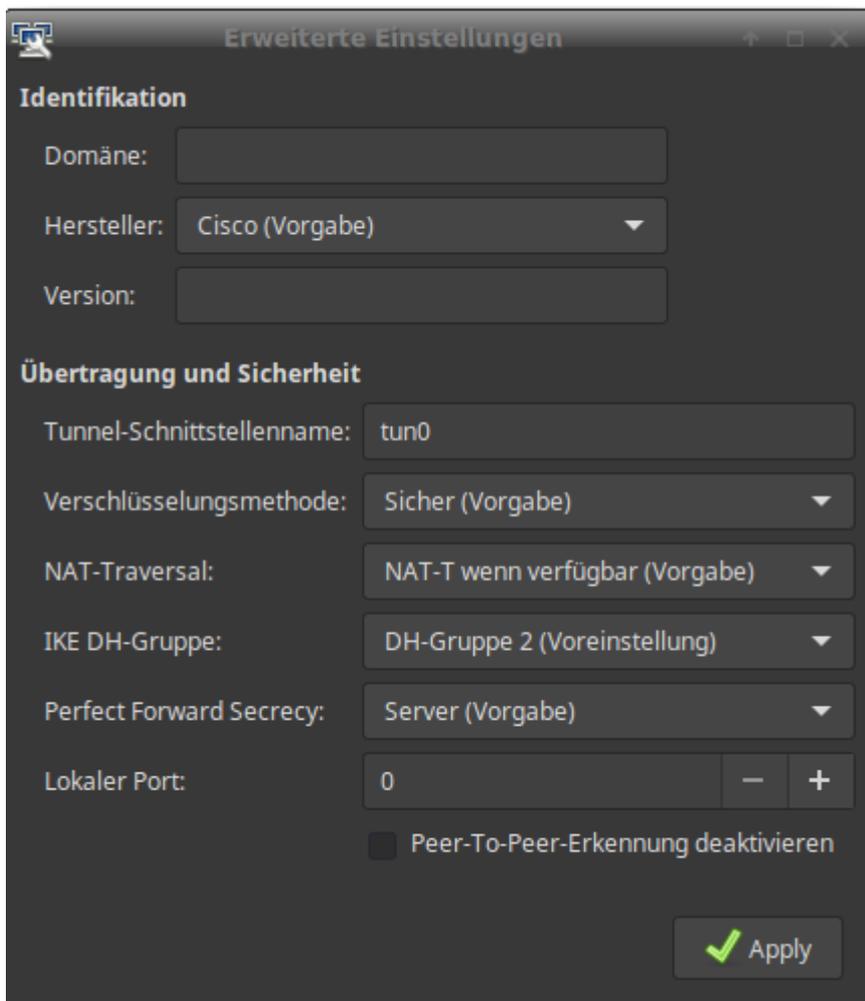


2. WIR MÜSSEN IN DEM FENSTER NOCH WEITER MACHEN !!!!!!!!!!!!!!!

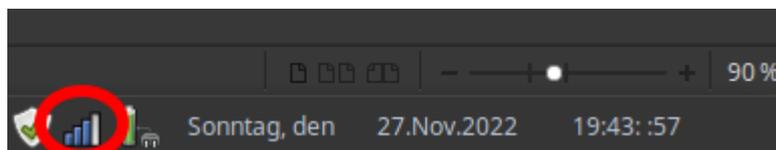
zunächst auf „Erweitert“ klicken und in erweiterten Einstellungen:

bei Tunnel-Schnittstellenname **tun0** eintragen.

Das sieht dann aus wie folgt:



**3. Damit klappt nun unsere VPN-Verbindung:
Noch einmal auf das Netzwerksymbol klicken:
entweder WLAN:**

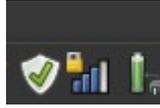


oder LAN:



Dann auf „VPN-Connections“ klicken und in dem aufploppenden Seitenfenster die Verbindung anwählen (hier: „VV14“)

Dann kommt zu der Verbindung ein „Schloss“ hinzu:



4. Das Gerät (Laptop, Computer) hat allerdings noch eine IP6-Adresse. Es kann daher sein, dass Seiten, die man aufruft, noch immer die IP6-Adresse sehen, die der Rechner vom Internetanbieter „vor Ort“ bekommen hat. Das kann dazu führen, dass etwaige Internetseiten, die man besuchen möchte, einem erklären, dass man sich noch in dem „falschen“ Ortsbereich befindet und man daher die Seite nicht aufrufen dürfe.

LÖSUNG: IP6-Adresse abschalten – entweder „einmalig“ und nach jedem Neustart des PC neu – oder dauerhaft, hier die beiden Lösungswege:

einmalig und jedesmal neu:

a) wir öffnen den Terminal (idR schwarzes Fenster mit Eingabezeilen) durch Drücken von Strg+Alt+T.

b) wir geben `sudo su` ein und bestätigen das mit der ENTER-Taste

c) dann wird das Passwort abgefragt. Hier muss man dann das eigene LINUX-Passwort eingeben, wenn man als dieser Benutzer admin-Rechte hat. Ansonsten muss man sich als der admin / root anmelden.

d) jetzt geben wir `ip address show | grep inet6` ein und bestätigen mit ENTER-Taste. Es werden dann irgendwelche IP6-Adressen angezeigt.

e) jetzt geben wir `echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6`

ein und bestätigen wieder mit der ENTER-Taste. Dadurch wird die IP6 abgeschaltet.

f) zur Kontrolle geben wir wieder `ip address show | grep inet6` ein und bestätigen mit ENTER-Taste. Es werden dann KEINE IP6-Adressen mehr angezeigt. ERGEBNIS: die Internetseiten können nicht mehr die IP6-Adresse sehen von dem Netz, in dem sich der Rechner befindet. Lokalsperren wären jetzt abgeschaltet (genauer: richten sich danach, wo unsere FRITZ-Box steht)

wie erklärt, muss man diesen Lösungsweg nach jedem Neustart des PC wiederholen. Es geht auch dauerhaft:

dauerhaftes Abschalten:

a) Dateiname: beispiel.sh erstellen mit folgendem Inhalt:

```
#!/bin/sh
case "$2" in
vpn-up)
# IPv6 abschalten
echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6
;;
vpn-down)
# IPv6 aktivieren
echo 0 > /proc/sys/net/ipv6/conf/all/disable_ipv6
;;
esac
```

b) nun folgende Befehle in die Befehlszeile des Terminals schreiben & ENTER drücken: (ggfls. muss der Pfad von beispiel.sh angepasst werden):

```
sudo cp beispiel.sh /etc/NetworkManager/dispatcher.d/15-vpn-ipv6 <ENTER>
```

```
sudo chown root:root /etc/NetworkManager/dispatcher.d/15-vpn-ipv6 <ENTER>
```

```
sudo chmod 755 /etc/NetworkManager/dispatcher.d/15-vpn-ipv6 <ENTER>
```

c) FERTIG. Nun wird die IP6 auch bei einem Neustart abgeschaltet, sobald die VPN-Verbindung hergestellt wird (zu Testen im Terminal mit `ip address show | grep inet6`)