ANLEITUNG UND HILFESTELLUNG WIREGUARD UND OPENVPN MIT EINEM RASPBERRY PI

Beitrag von „anonymous_writer“ vom 29. November 2021, 21:57

OpenVPN und WireGuard kann man dazu verwenden sich dauerhaft mit seinem Heimnetz zu verbinden. Dabei spielt es keine Rolle ob man das Netzt wechselt von WLAN zu Mobil. Beide Lösungen verbinden sich stets automatisch neu mit dem Heimnetzwerk.

Voraussetzung für diese Anleitung ist natürlich ein vorhandener Raspberry Pi. Welche Variante spielt eigentlich keine Rolle.

Ich selber habe einen PI 3 und einen PI Zero W. Auf beiden Varianten ist die Installations gleich und auch die Funktion nach dem Einrichten Identsich.

Als Betriebssystem nutze ich "Raspberry Pi OS" vom Link. Dieses Betriebssystem baut auf Debian aufbaut. Der Installer auf der Seite macht die Installation absolut easy und zum Einrichten gibt es auch einige Anleitungen.

https://www.raspberrypi.com/software/

Vorbereitung:

Wichtig ist das ihr dem PI eine statische Adresse vergebt und wenn ihr mit VPN auch IPV6 nutzen möchtet zusätzlich eine statische IPV6 Adresse.

Hier mein Beispiel:

Code

```
1. sudo nano /etc/dhcpcd.conf
```

Code

```
1. interface eth0
2. static ip_address=192.168.12.3/24
3. static ip6_address=fdf3::/64
4. static routers=192.168.12.1
5. static domain_name_servers=192.168.12.1
```

static ip_address > IPV4 Adresse des PI. Muss natürlich im Heimnetz sein.

static ip6_address > IPV6 Adresse des PI. Frei wählbar muss aber dem IPV6 Syntax entsprechen > Optional wenn IPV6 gewünscht.

static routers > IPV4 Adresse des Routers im Netz

static domain_name_servers > Lokaler DNS Server im Netz. Normalerweise die gleiche IPV6 Adresse wie der Router.

Aktivierung Weiterleitung

Damit IPV4 und wenn erwünscht auch IPV6 erfolgreich weitergeleitet wird vom Pi ins Heimnetz muss die sysctl.conf bearbeitet werden.

Code

```
1. sudo nano /etc/sysctl.conf
```

Die Datei ergänzen oder wenn die Einträge bereits vorhanden sind verändern um die folgenden Einträge:

Code

1. net.ipv4.ip_forward=1
2. net.ipv6.conf.all.forwarding=1

Öffentliche Adresse:

Damit das Heimnetz auch immer von ausserhalb erreichbar ist müsst ihr natürlich erst mal eine öffentliche Adresse einrichten. Die meisten Router bitten dazu bereits eine Möglichkeit.

Telekom Speedport unter "Einstellungen für dynamisches DNS".

FritzBox > MyFritz Konto.

Da wir einen PI habe gehe ich an dieser Stelle auf dynv6.com ein. Dynv6 ist kostenlos und ohne jegliche Zwangsanmeldungen jeden Monat um das Konto erneut zu aktivieren.

https://dynv6.com

Debian biettet den Daemon "ddclient" an zur Übermittlung der öffentlichen IP's an einen Dynamic DNS Server. Funktioniert für alle Anbieter.

Code

1. sudo apt-get install ddclient
2. sudo nano /etc/ddclient.conf

Code

1. protocol=dyndns2
2. use=web
3. ssl=yes
4. server=dynv6.com
5. login=none
6. password='Passwort zu finden unter Instructions'
7. 'dynv6 generierte Adresse zu finden unter Instructions'

Jetzt noch den Daemon nach jedem Neustart aktivieren.

Code

```
1. sudo systemctl enable ddclient
```

Mit diesem Befehl kann man sich den Status ansehen und die Ausführung sofort erzwingen.

Code

```
1. sudo ddclient -debug -verbose -noquiet -force
```

IPV6 Ergänzung:

Es gibt auch ein Script mit welchem man dynv6 sehr einfache updaten kann. Zusätzlich wird mit dem Script auch die öffentliche IPV6 Adresse weitergegeben.

https://gist.github.com/corny/7a07f5ac901844bd20c9

Ich habe das Script in einen neuen Ordner kopiert "/home/pi/ddclient_dynv6" und darin ein zweites Script erstellt welches die Anmeldeinformationen an das Script weitergibt.

Inhalt des Scripts wie folgt:

Code

```
1. cd /home/pi/ddclient_dynv6
2. token='Passwort zu finden unter Instructions' sh ./dynv6.sh 'dynv6 generierte Adresse zu finden unter Instructions'
```

Beide Scripts ausführbar machen:

Code

```
1. chmod u+x /home/pi/ddclient_dynv6/*
```

Die Datei "/etc/ddclient.conf" muss jetzt am Ende um folgenden Eintrag ergänzt werden:

Code

1. postscript=/home/pi/ddclient_dynv6/start.sh

Ab jetzt sollte auch die IPV6 Adresse bei dynv6 deiner öffentlichen Router Adresse folgen.

Installation OpenVpn und WireGuard:

Es gibt ein Skript das die Installation beider Vpn Lösungen auf dem Pi sehr vereinfacht.

https://www.pivpn.io/

Im Terminal folgenden Befehl ausführen und der Anleitung folgen:

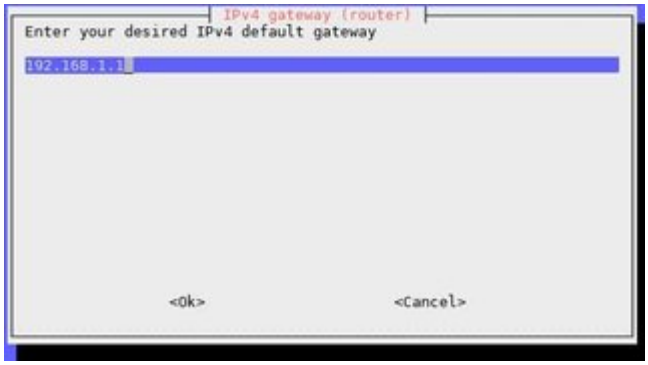
Code

1. curl -L https://install.pivpn.io | bash

Ich möchte das ganze etwas Abkürzen da die Hilfestellung beim ausführen des Scripts eigentlich selbsterklärend ist. Daher hier nur eine Beschreibung der wichtigsten Eingaben.

Falls man wie bereits oben beschrieben eine statische Adresse dem PI vergeben hat kann man hier auf NO gehen. Ansonsten kann man das hier noch nachholen.

Hier kommt die IPV4 Adresse vom Router rein.



Das ist der Port welcher am Router freigegeben werden muss damit der VPN-Dienst auf dem Pi von außerhalb der Router Firewall erreichbar ist. Am besten ist wenn man hier das Protokoll UDP wählt. Standard wird entgegen dem Bild für WireGuard Port 51820 vorgeschlagen. Es ist natürlich auch ganz wichtig das die Portfreigabe zum Pi auch auf dem Router eingerichtet wird. Wie das geht steht in der Router Anleitung.

Hier so wie im Bild markiert auswählen und deine öffentliche Adresse eintragen. Adresse ganz oben in der Anleitung "'dynv6 generierte Adresse zu finden unter Instructions". Als Beispiel "name.dynv6.net".

Hier ganz nach unten Scrollen und denn eigenen DNS-Server eintragen. Ist normalerweise die Adresse vom Router. Ansonsten funktioniert die interne Namensauflösung nicht.

Um OpenVPN und WireGuard auf dem PI zu installieren das Script nochmal ausführen mit dem anderen Dienst als Auswahl.

OpenVPN bittet eine höhere Sicherheit als WireGuard. Dafür ist WireGuard schlanker und soll schneller sein. Für den Normalnutzer ist aber sicher die Sicherheit von beiden Diensten ausreichend.

Damit ist die Grundkonfiguration beider Dienste abgeschlossen und mit dem folgenden Befehl können die Clients hinzu gefügt werden bei Installation von nur einem der beiden Dienste.

Code

1. pivpn add

Wen beide Dienste installiert sind muss man dazuschreiben für welchen Dienst.

Code

1. pivpn wg add
2. pivpn ovpn add

Wo findet man die Client APP und wie konfigurieren?

Mit WireGuard kann man sich zum Einscannen in die Client App einen QR-Code erzeugen lassen.

Code

1. pivpn wg -qr

Beide Dienste erzeugen eine Konfigurationsdatei für den Client die man am Ende in der Client App laden kann.

WireGuard Client ist im App Store zu finden für OSX als auch für IOS.

https://apps.apple.com/de/app/wireguard/id1441195209

OpenVPN Client für IOS ebenfalls im App Store.

https://apps.apple.com/de/app/openvpn-connect/id590379981

Für OSX gibt es eine Installer.

https://openvpn.net/download-open-vpn/

Monterey

Seit Monterey muss ich für beide Dienste die MTU (Maximum Transmission Unit) ergänzen. Das ist anscheinend nicht immer nötig, aber bei mir wird die Verbindung ohne die MTU geblockt. Ich habe diese Konfiguration direkt in die Pi Konfiguration eingetragen.

WireGuard:

Code

1. sudo nano /etc/wireguard/wg0.conf

und in der Konfigurationsdatei folgende Zeile unter [Interface] ergänzen:

Code

```
1. MTU = 1280
```

Für OpenVPN das gleiche:

Code

```
1. sudo nano /etc/openvpn/server.conf
```

und das ergänzen:

Code

```
1. tun-mtu 1280
```

Additional IPV6

WireGuard kann man auch sehr leicht um IPV6 erweitern. Voraussetzung ist natürlich das in deinem Heimnetz auch IPV6 eingerichtet wurde.

Die WireGuard Konfiguration muss dazu um die nötigen IPV6 Einstellungen ergänzt werden.

Hier als Beispiel.

[Interface] erhält zusätzlich für wg0 eine feste IPV6 Adresse und denn dazu gehörigen Adressbereich

Code

```
1. Address = 10.6.0.1/24, fd06::1/64
```

Weiter muss in [Interface] eine Routing Weiterleitung auf eth0 ergänzt werden. Ich bin mir nicht sicher ob das bei jeder Pi Konfiguration nötig ist oder nur bei meiner da ich auf dem Pi auch dnsmasq am laufen habe als eignen DNS, IPV4 und IPV6 Server.

Weiter oben in der Anleitung haben wir ja bereits ein Routing für IPV4 und IPV6 gesetzt.

Code

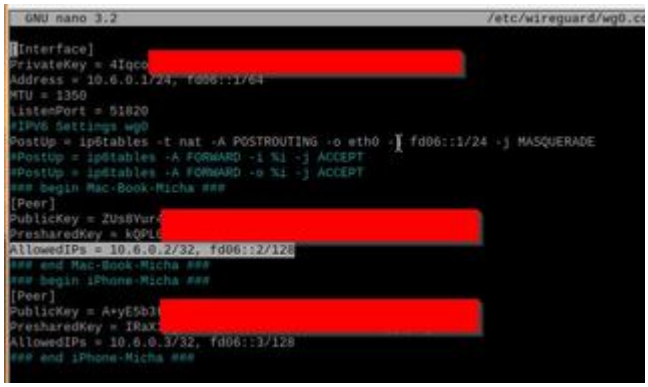
1. PostUp = ip6tables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
2. PostDown = ip6tables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

Jetzt noch für die Clients die IPV6 Adresse ergänzen. Nach dem Ergänzen müssen die Client Konfigurationen neu erstellt werden oder ihr ergänzt das zusätzlich in der Client Konfiguration.

Code

1. AllowedIPs = 10.6.0.2/32, fd06::2/128

Am Ende sieht meine Konfiguration wie folgt aus mit funktionierendem IPV6.



Abschluss

Nicht vergessen einen Neustart vom Pi machen damit auch alles neue eingestellte aktiviert wird.

Folgende Befehle sind Hilfreich zur Fehlersuche und zum Prüfen ob die Verbindung klappt.

Code

1. ifconfig
2. pivpn wg -c
3. pivpn wg -d
4. pivpn ovpn -c

5. pivpn ovpn -d

Viel Spass mit OpenVpn und WireGuard.

Freue mich über jegliche Anmerkungen und Verbesserungsvorschläge. Ist nicht einfach eine Anleitung aus dem Kopf zu schreiben und hat sicher Verbesserungspotential.

Beitrag von „Wolfe“ vom 30. November 2021, 14:45

Bei mir läuft auch ein Vpn über Pi und Wireguard. Funktioniert prima. Ich habe noch watchdog aktiviert, damit das vpn immer verfügbar ist.