

## PiVPN

The simplest way to setup and manage a VPN,  
designed for Raspberry Pi™.



### The PiVPN Project

*Secure connectivity for the masses.*

*Low cost, high security.*

# Programma



- Biografie
- Waarom VPN?
- Wat is PiVPN?
- Demonstratie PiVPN met WireGuard
- Netwerk configuratie
- Installatie PiVPN
- Portforwarding op router aanzetten
- Gebruik PiVPN
- Configuratie clients
- Meer info en links
- Vragen
- Aan de slag

## PiVPN

The simplest way to setup and manage a VPN, designed for Raspberry Pi™.

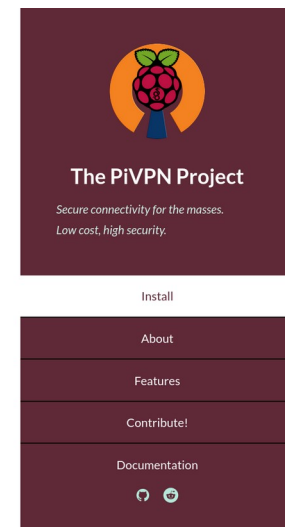
```
</> ::: INSTALLATION :::  
curl -L https://install.pivpn.io | bash  
  
::: Test (unstable) Branch :::  
curl -L https://test.pivpn.io | TESTING= bash
```

**SIMPLE** ::: Yes, that's it! It is "almost" that simple.

To elaborate a little more, you will want to install Raspberry Pi OS Lite on a Raspberry pi, we strongly recommend using the latest Raspberry Pi OS Lite image but the normal Raspberry Pi OS image will work as well, preferably enable ssh access and then begin.

After install, you may need to open a port on your router.

There is a (now slightly outdated) guided walkthrough of the install available here.



# Biografie



- Ongeveer 20 jaar open source gebruiker: begonnen met PHP en MySQL
- Ongeveer 15 jaar geleden Linux gaan gebruiken door op Pogoplug Arch Linux te zetten
- Door goede WIKI Arch op thuisserver gaan gebruiken en kennis Arch/Linux verder uitgebreid.
- Auteur van artikelen in Linux Magazine
- In 2017 gaan bijdragen aan Nextcloud
- Lid programma commissie NLLGG sinds september 2018
- In 2021 gestart met plaatsen Nederlandstalige informatie over Linux en Open Source op <https://www.hetnetwerk.org>

# Waarom VPN met je internetaansluiting thuis?



- Beveiligde verbinding maken als je op openbare WIFI zit.
- Buiten EU Nederlandse TV programma's kunnen kijken.

# Wat is PiVPN?



PiVPN is software voor de Raspberry Pi (maar eigenlijk voor alle op Debian en afgeleide distributies) waarmee je op een eenvoudige manier WireGuard of OpenVPN installeert en configureert.

## PiVPN

The simplest way to setup and manage a VPN,  
designed for Raspberry Pi™.

# Demonstratie PiVPN met WireGuard



**NLGG**  
Nederlandse Linux Gebruikers Groep

# Netwerk configuratie - 1



In principe kan PiVPN de netwerkconfiguratie aanpassen, maar dit gaat niet altijd goed. Advies is om een vast IP adres in te stellen. In Raspberry Pi OS (ook de AMD64 versie) vind je de netwerkconfiguratie in het bestand `/etc/dhcpd.conf`

# Netwerk configuratie - 2



Voorbeeld configuratie vast IP adres in /etc/dhcpd.conf:

```
# static profile on eth0
interface eth0
static ip_address=192.168.1.11/24
static routers=192.168.1.1
static domain_name_servers=192.168.1.1
```

Geel gemarkeerde IP adressen aanpassen aan eigen situatie.

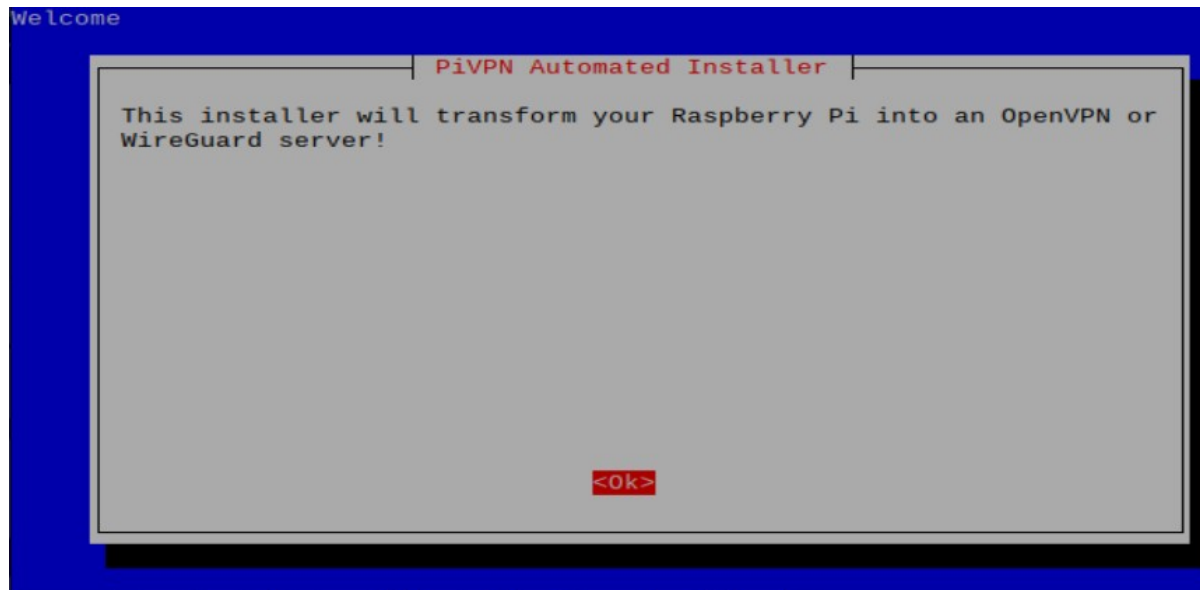


# Installatie PiVPN – 1 -



Installatie start met één commando:

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



# Installatie PiVPN – 2 -



Je komt in een wizard terecht. Bij twijfel altijd advies uit wizard overnemen.

- Melding vast IP adres nodig
- Forceren IPv6 verbindingen via IPv4
- Setup static (IPv4) address
- Current IP(v4) settings as static address
- Melding IP conflict
- Choose local user for vpn configuration
- Keuze Wireguard of OpenVPN

# Installatie PiVPN – 3 Wireguard -



- Default Wireguard port: 51820
- Keuze DNS provider
- Keuze “public IP or DNS”

Als je een eigen subdomein hebt dat aan je thuis internet verbinding gekoppeld is, is DNS handigst.

- Enable unattended upgrades
- Advice reboot your Pi
- Type ‘pivpn -d’ om forward probleem op te lossen

# Installatie PiVPN – 4 OpenVPN -



- Installation mode ==> no
- Default OpenVPN port: 1194
- Keuze DNS provider
- Keuze “public IP or DNS”

Als je een eigen subdomein hebt dat aan je thuis internet verbinding gekoppeld is, is DNS handigst.

- Enable unattended upgrades
- Advice reboot your Pi

# Installatie PiVPN – 5 einde wizard -



**NLLGG**  
Nederlandse Linux Gebruikers Groep

Make it so.

**Installation Complete!**

Now run 'pivpn add' to create the client profiles.  
Run 'pivpn help' to see what else you can do!

If you run into any issue, please read all our documentation  
carefully.  
All incomplete posts or bug reports will be ignored or deleted.

Thank you for using PiVPN.

**<Ok>**

# Portforwarding op router aanzetten



Uitgaande van door de installer voorgestelde poorten:

- Open VPN poort: 1194
- WireGuard poort: 51820

## Port Forwarding

On	Protocol	Src Address	Ext Ports	Int Port	Int Address	Description	
On	UDP		1194		192.168.1.68	OpenVPN op Raspberry PI OS	▲
On	UDP		51820		192.168.1.68	WireGuard op Raspberry PI OS	✖

# Gebruik PiVPN



Type 'pivpn' en je ziet alle mogelijkheden:

```
andre@raspberrypi:~ $ pivpn
::: Control all PiVPN specific functions!
:::
::: Usage: pivpn <command> [option]
:::
::: Commands:
::: -a, add [nopass]      Create a client ovpn profile, optional nopass
::: -c, clients           List any connected clients to the server
::: -d, debug             Start a debugging session if having trouble
::: -l, list              List all valid and revoked certificates
::: -r, revoke           Revoke a client ovpn profile
::: -h, help             Show this help dialog
::: -u, uninstall        Uninstall PiVPN from your system!
::: -up, update          Updates PiVPN Scripts
::: -bk, backup          Backup Openvpn and ovpn dir
andre@raspberrypi:~ $ █
```

- Voor **iedere** client maak je met 'pivpn -a' een client profiel aan.
- Het 'pivpn -c' commando is handig om te zien wie er ingelogd zijn.

# Configuratie Wireguard clients – 1 -



## Raspberry Pi:

- Aanmaken Client certificaten op Raspberry Pi:  
pivpn -a
- IP adres Raspberry Pi uitlezen:  
hostname -I
- Zorgen dat SSH aanstaat met:  
sudo raspi-config  
of Raspberry Pi configuration (grafisch)

```
andre@raspberrypi: ~  
Bestand  Bewerken  Beeld  Zoeken  Terminal  Hulp  
andre@raspberrypi:~ $ pivpn -a  
Enter a Name for the Client: nllggdemo  
::: Client Keys generated  
::: Client config generated  
::: Updated server config  
::: WireGuard reloaded  
  
=====  
::: Done! nllggdemo.conf successfully created!  
::: nllggdemo.conf was copied to /home/andre/configs for easytransfer.  
::: Please use this profile only on one device and create additional  
::: profiles for other devices. You can also use pivpn -qr  
::: to generate a QR Code you can scan with the mobile app.  
=====  
andre@raspberrypi:~ $ hostname -I  
192.168.1.68 10.76.170.1  
andre@raspberrypi:~ $
```



# Configuratie Wireguard clients – 2 -



**Linux – werkende grafische interface heb ik niet gevonden**

- `sudo apt install wireguard resolvconf`
- `sudo scp naam@ip_rpi:configs/naamconf.conf /etc/wireguard`

VPN verbinding maken:

- `sudo wg-quick up naamconf`

VPN verbinding verbreken:

- `sudo wg-quick down naamconf`

**Bron:** <https://engineerworkshop.com/blog/how-to-set-up-a-wireguard-client-on-linux-with-conf-file/>



# Configuratie WireGuard clients – 3 –



## Android

- Type op Raspberry Pi 'pivpn -qr' en kies het profiel.
- QR code verschijnt op het scherm.
- Installeer op Android device WireGuard app via Playstore
- Open app en klik op '+'. Kies daarna 'Scan from QR code'.
- Geef de verbinding een naam.
- Zet de schakelaar naar rechts om de verbinding te activeren.

## IOS

- Ongeveer vergelijkbaar.



# Configuratie OpenVPN clients



## Raspberry Pi


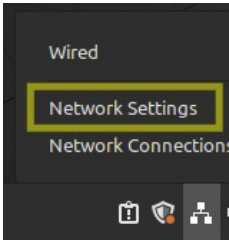
- Aanmaken Client certificaten op Raspberry Pi:  
    pivpn -a  
of pivpn -a nopass
- IP adres Raspberry Pi uitlezen:  
hostname -I
- Zorgen dat SSH aanstaat met:  
    sudo raspi-config  
of Raspberry Pi configuration (grafisch)

```
andre@raspberrypi: ~  
File Edit Tabs Help  
Write out database with 1 new entries  
Data Base Updated  
* Notice:  
Certificate created at: /etc/openvpn/easy-rsa/pki/issued/nllgg.crt  
Client's cert found: nllgg.crt  
Client's Private Key found: nllgg.key  
CA public Key found: ca.crt  
tls Private Key found: ta.key  
=====  
Done! nllgg.ovpn successfully created!  
nllgg.ovpn was copied to:  
  /home/andre/ovpns  
for easy transfer. Please use this profile only on one  
device and create additional profiles for other devices.  
=====  
andre@raspberrypi:~ $ hostname -I  
192.168.1.68 10.19.38.1  
andre@raspberrypi:~ $
```

# Configuratie OpenVPN clients



## Linux Mint

- Met bijvoorbeeld FileZilla configuratie downloaden (IP zie vorige dia)
- Na inloggen staat configuratie in subdir ovpn van homedir
- Download Open VPN configuratie
- Klik op Netwerk symbool onderaan taakbalk 
- Klik op 'Network settings' 
- Klik op het plus teken links onderin en kies daarna voor 'Import from file'
- Kies hier de gedownloadede Open VPN configuratie en klik op 'Open' en daarna op 'Add'
- Klik in 'Network settings' op VPN verbinding en zet schakelaar op aan.

# Configuratie OpenVPN clients

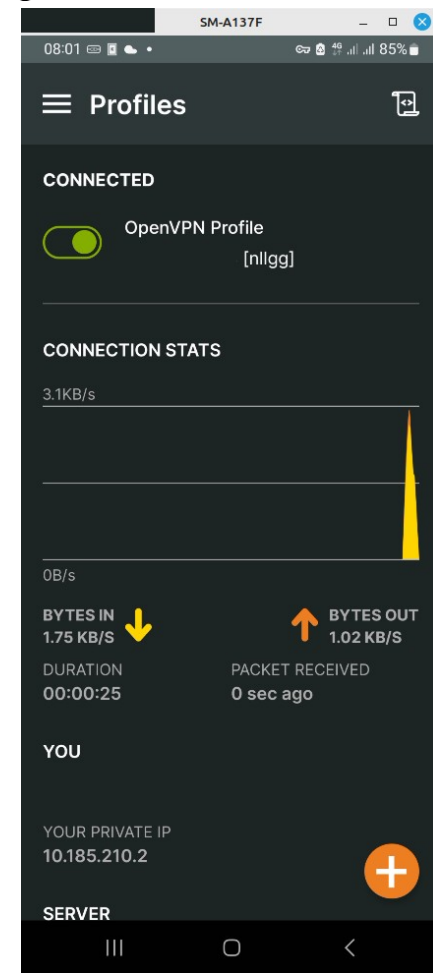


## Android

- Via USB kabel OpenVPN configuratiefile (zie vorige dia) van desktop naar Android kopiëren
- Installeren OpenVPN connect app via Playstore
- In OpenVPN connect tik op 'Upload file' en selecteer configuratiefile
- Tik daarna op 'CONNECT' en je maakt verbinding met de VPN server

## IOS

- Ongeveer vergelijkbaar.



# Meer informatie en links



- Website PiVPN: <https://pivpn.io/>
- Website WireGuard: <https://www.wireguard.com/>
- Website OpenVPN: <https://openvpn.net/>
- Workshop PiVPN: Nummer 6 uit 2022 van Nederlandstalige Linux Magazine



The PiVPN Project

*Secure connectivity for the masses.*

*Low cost, high security.*



ALLES OVER OPEN SOURCE  
**LINUX**  
MAGAZINE

# Vragen / opmerkingen?



# Aan de slag – 1 -



## Tijdens workshop:

1. Pas eventueel netwerkconfiguratie aan
2. Installeer PiVPN: `curl -L https://install.pivpn.io | bash`
3. Kies voor WireGuard of OpenVPN
4. Bij WireGuard forward probleem oplossen:  
`pivpn -d`
5. Installeer clients op telefoon of laptop



# Aan de slag – 2 -



## Thuis:

1. Verwijder alle aangemaakte clients met 'pivpn -r clientnaam'.  
Overzicht van clients krijg je met 'pivpn -l'.  
Verwijder aangemaakte configuraties ook van telefoon, laptop etc.
2. Pas configuratie PiVPN aan naar internetaansluiting thuis (public IP adres of subdomeinnaam):  

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

  
Kies voor 'Reconfigure' en pas alleen de gegevens bij 'Public IP or DNS' aan
3. Schakel portforwarding in op de router
4. Maak opnieuw clients aan ('pivpn -a')
5. Configureer clients (telefoon, laptop etc.) opnieuw.