

Wireguard de diepte in

**hcc**<sup>!</sup>  
opensource



André Fondse – 15-02-2025

# Programma

- Biografie
- Scope sessie
- Hoe kom je aan Wireguard?
- Configuratie Wireguard via PiVPN
- QR codes configuratie weergeven
- Basis configuratie Wireguard
- Configuratie geen toegang tot intern netwerk
- Configuratie blokkade intern netwerk m.u.v. 1 webserver
- Alleen toegang tot 1 webserver
- Alleen toegang tot intern netwerk
- Verbinding tussen 2 computers
- WG tunnel op Android
- Meer over Wireguard configuraties lezen?
- Vragen?



- 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.
- Ongeveer 5 jaar geleden voor thuisserver overgestapt naar Debian
- Ongeveer 10 jaar Linux Mint op desktop als hoofdbesturingssysteem
- Auteur van artikelen in Linux Magazine
- Actief lid binnen NLLGG sinds september 2018
- In 2021 gestart met plaatsen Nederlandstalige informatie over Linux en Open Source op <https://www.hetnetwerk.org>

# Scope sessie

1. Na installatie Wireguard via PiVPN
2. Verschillende configuratiemogelijkheden
3. Uitleg van de belangrijkste begrippen
4. Nadruk op toepassingsmogelijkheden
5. Voorbeelden in deze sessie zijn resultaat van door mij proberen. Er kunnen betere configuraties zijn.



# Hoe kom je aan Wireguard?

1. Installeren via [PiVPN](#)  
`curl -L https://install.pivpn.io | bash`
2. Installeren via je [distro](#)
3. Opgenomen in hardware, bijvoorbeeld [routerfirmware](#)



# Configuratie Wireguard via PiVPN

- 1 -

- Standaard alle configuratiebestanden van de Wireguard netwerk interfaces in `/etc/wireguard` ==> root of sudo rechten nodig
- PiVPN setup variabelen Wireguard in `/etc/pivpn/wireguard/setupVars.conf`
- Configuratiebestanden Wireguard clients in configs directory van homedir, meestal `~/configs`



- Na installatie Wireguard via PiVPN start Wireguard met interface wg0 automatisch op via SystemD
- Bij testen Wireguard is dit handiger dit automatische opstarten uit te zetten via:  
**sudo systemctl disable --now wg-quick@wg0.service**
- Aanzetten automatisch starten interface wg0 doe je door middel van:  
**sudo systemctl enable --now wg-quick@wg0.service**



# QR codes WireGuard configuratie weergeven

1. `pivpn -qr`

2. `qrencode -t ansiutf8 < wireguard-client.conf`



# Basis configuratie Wireguard – 1 -

- Toepassing eigen gebruik: altijd veilige verbinding + toegang intern netwerk

- Inhoud /etc/wireguard/wg0.conf

```
[Interface]
```

```
PrivateKey = [Privé sleutel van server]
```

```
Address = 10.89.19.1/24
```

```
MTU = 1420
```

```
ListenPort = 51830
```

- wg0: naam van de interface
- PrivateKey: privé sleutel van de VPN verbinding
- Address: IP adres en subnet van de VPN verbinding
- ListenPort = poort die deze VPN verbinding gebruikt



# Basis configuratie Wireguard – 2 -

Na toevoegen client via PiVPN zijn volgende regels toegevoegd aan `/etc/wireguard/wg0.conf`

```
### begin andre_laptop ###
```

```
[Peer]
```

```
PublicKey = [Publieke sleutel client]
```

```
PresharedKey = [Gedeelde sleutel tussen server en client]
```

```
AllowedIPs = 10.89.19.2/32
```

```
### end andre_laptop ###
```

- [Peer]: Geeft aan dat dit configuratie client is
- AllowedIPs = 10.89.19.2/32: IP adres 10.89.19.2 met als subnet alleen het eigen IP adres (10.89.19.2).



# Werking basis configuratie Wireguard

- VPN zoals je mag verwachten
- Toegang tot interne netwerk!
- Demonstratie met de volgende uitgangspunten:
  - Telefoon is hotspot voor laptop via Wifi
  - Telefoon maakt via 4G verbinding met internet
  - Enige internetverbinding laptop is met Wifi Hotspot telefoon
- Uitgangspunten gelden ook voor alle volgende demonstraties



# Configuratie: geen toegang tot intern netwerk – 1 -

**Toepassing:** internetverbinding voor iemand buiten EU

**Vraag:**

Hoe zou je toegang tot interne netwerk kunnen voorkomen?



# Configuratie: geen toegang tot intern netwerk – 1 -

**Toepassing:** internetverbinding voor iemand buiten EU

**Vraag:**

Hoe zou je toegang tot interne netwerk kunnen voorkomen?

1. Aanpassen AllowedIPS bij client ==> kan gebruiker client zelf ook doen



# Configuratie: geen toegang tot intern netwerk – 1 -

**Toepassing:** internetverbinding voor iemand buiten EU

**Vraag:**

Hoe zou je toegang tot interne netwerk kunnen voorkomen?

1. Aanpassen AllowedIPS bij client ==> kan gebruiker client zelf ook doen
2. Via Firewall regels



# Configuratie: geen toegang tot intern netwerk – 2 -

- Veiligste manier om dit te doen is via Firewall regels
- Op server toevoegen onder [interface] door middel van *PostUp* en *PostDown*.
- Meerdere regels toegestaan



# Configuratie: geen toegang tot intern netwerk – 3 -

```
PostUp = iptables -A FORWARD -d 192.168.0.0/16  
-i wg0 -j REJECT --reject-with icmp-port-unreachable
```

- *PostUp*: want wg0 bestaat nog niet
- *-A*: firewall regel toevoegen
- *-d 192.168.0.0/16*: d = destination -> alle ip adressen met 192.168.x.x weigeren



# Configuratie: geen toegang tot intern netwerk – 4 -

```
PostDown = iptables -D FORWARD -d  
192.168.0.0/16 -i wg0 -j REJECT --reject-with  
icmp-port-unreachable
```

- *PostDown*: na het deactiveren van wg0
- *-D*: firewall regel verwijderen
  
- Demonstratie



# Configuratie: blokkade intern netwerk m.u.v. 1 webserver – 1 -

## **Toepassing:** demonstratie

```
PostUp = iptables -A FORWARD -d 192.168.3.13 -i  
wg0 -p tcp -m tcp --dport 443 -j ACCEPT  
PostUp = iptables -A FORWARD -d 192.168.0.0/16 -  
i wg0 -j REJECT --reject-with icmp-port-  
unreachable
```

- ACCEPT regel voor REJECT regel
- IP adres webserver intern netwerk 192.168.3.13
- Poort 443 is voor HTTPS protocol



# Configuratie: blokkade intern netwerk m.u.v. 1 webserver – 2 -

```
PostDown = iptables -D FORWARD -d 192.168.3.13  
-i wg0 -p tcp -m tcp --dport 443 -j ACCEPT
```

```
PostDown = iptables -D FORWARD -d  
192.168.0.0/16 -i wg0 -j REJECT --reject-with  
icmp-port-unreachable
```

Demonstratie zie volgende dia



# Alleen toegang tot 1 webserver -1- peerconfiguratie

**Toepassing:** toegang leverancier zonnepanelen tot omvomer

[Interface]

PrivateKey = [Privé sleutel peer]

Address = 10.167.144.2/24

#DNS = 208.67.222.222, 208.67.220.220

[Peer]

PublicKey = [Publieke sleutel server]

PresharedKey = [Gedeelde sleutel server en peer]

Endpoint = andre.fondse.eu:51830

AllowedIPs = 10.167.144.0/24, 192.168.3.13/32

- **DNS:** Gebruik geen DNS. Anders mogelijk geen DNS op internet verbinding buiten VPN
- **AllowedIPs:** IP reeks van VPN (10.167.144.0/24) en IP adres waar toegang tot verkregen moet worden (192.168.3.13/32)



Alleen toegang tot 1 webserver -2-

**Waar zit het veiligheidslek in de configuratie op de vorige dia?**



## Alleen toegang tot 1 webserver -2-

**Waar zit het veiligheidslek in de configuratie op de vorige dia?**

*Eigenaar peer computer kan AllowedIPS aanpassen waardoor toegang gekregen kan worden tot meer van het interne netwerk.*



# Alleen toegang tot 1 webserver -2-

**Waar zit het veiligheidslek in de configuratie op de vorige dia?**

*Eigenaar peer computer kan AllowedIPS aanpassen waardoor toegang gekregen kan worden tot meer van het interne netwerk.*

**Hoe los je dit lek op?**



## Alleen toegang tot 1 webserver -2-

**Waar zit het veiligheidslek in de configuratie op de vorige dia?**

*Eigenaar peer computer kan AllowedIPS aanpassen waardoor toegang gekregen kan worden tot meer van het interne netwerk.*

**Hoe los je dit lek op?**

*Via firewall regels op de Wireguard server.*



# Alleen toegang tot 1 webserver – 3 - Serverconfiguratie – 1 -

[Interface]

PrivateKey = [Privé sleutel van server]

Address = 10.167.144.1/24

MTU = 1420

ListenPort = 51830

**PostUp = iptables -A FORWARD -i wg0 -d 192.168.3.13/32 -  
p tcp --dport 443 -j ACCEPT; iptables -A FORWARD -i wg0  
-j REJECT --reject-with icmp-port-unreachable**

**PostDown = iptables -D FORWARD -i wg0 -d 192.168.3.13/32  
-p tcp --dport 443 -j ACCEPT; iptables -D FORWARD -i  
wg0 -j REJECT --reject-with icmp-port-unreachable**



# Alleen toegang tot 1 webserver – 3 - Serverconfiguratie – 2 -

```
### begin andre-laptop ###  
[Peer]  
PublicKey = [publieke sleutel peer]  
PresharedKey = [gedeelde sleutel server en peer]  
AllowedIPs = 10.167.144.2/32  
### end andre-laptop ###
```

- Dit deel van de configuratie hoeft geen wijziging.
- Demonstratie volgende dia





**hcc**   
opensource

**Wat zien we  
hier?**



# Alleen toegang intern netwerk – 1 -

Vergeleken met configuratie alleen toegang tot 1 webserver hoeven op de Wireguard server alleen de PostUp en de PostDown regels aangepast te worden naar:

```
PostUp = iptables -A FORWARD -i wg0 -d  
192.168.3.0/24 -j ACCEPT; iptables -A FORWARD -i  
wg0 -j REJECT --reject-with icmp-port-  
unreachable
```

```
PostDown = iptables -D FORWARD -i wg0 -d  
192.168.3.0/24 -j ACCEPT; iptables -D FORWARD -i  
wg0 -j REJECT --reject-with icmp-port-  
unreachable
```



# Alleen toegang intern netwerk – 2 -

- 192.168.3.0/24: 192.168.3.0 t/m 192.168.3.255
- Wil je 192.168.0.0 t/m 192.168.255.255, dan gebruik je 192.168.0.0/16
- Op de client pas je in de configuratiefile de regel AllowedIPs aan naar:  
`AllowedIPs = 10.167.144.0/24, 192.168.3.0/24`
- Demonstratie zie volgende dia



# Verbinding tussen 2 computers – 1 - Serverconfiguratie

```
[Interface]
PrivateKey = [Privé sleutel server]
Address = 10.167.144.1
MTU = 1420
ListenPort = 51830

### begin andre-laptop ###
[Peer]
PublicKey = [Publieke sleutel client]
PresharedKey = [Gedeelde sleutel tussen server en client]
AllowedIPs = 10.167.144.2/32
### end andre-laptop ###
```



# Verbinding tussen 2 computers – 2 - Clientconfiguratie

[Interface]

PrivateKey = [Privé sleutel client]

Address = 10.167.144.2

[Peer]

PublicKey = [Publieke sleutel client]

PresharedKey = [Gedeelde sleutel tussen server en client]

Endpoint = andre.fondse.eu:51830

AllowedIPs = 10.167.144.0/24



# Verbinding tussen 2 computers – 3 - demonstratie

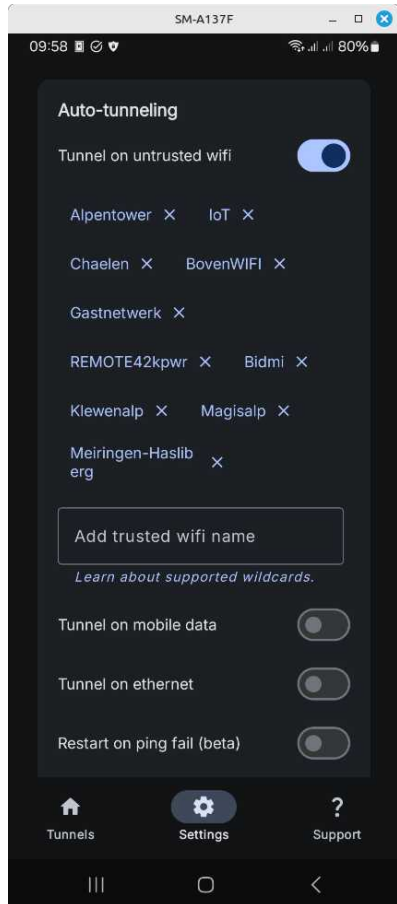
Links: server  
Rechts: client

```
linux@rpi4: ~  
Bestand Bewerken Beeld Zoeken Terminal Hulp  
linux@rpi4:~ $ hostname -I  
192.168.1.11 10.167.144.1  
linux@rpi4:~ $ ip route  
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.11 metric 100  
10.167.144.2 dev wg0 scope link  
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.11 metric 100  
linux@rpi4:~ $ ping -c1 10.167.144.2  
PING 10.167.144.2 (10.167.144.2) 56(84) bytes of data:  
64 bytes from 10.167.144.2: icmp_seq=1 ttl=64 time=1.35 ms  
  
--- 10.167.144.2 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 1.351/1.351/1.351/0.000 ms  
linux@rpi4:~ $ traceroute 10.167.144.2  
traceroute to 10.167.144.2 (10.167.144.2), 30 hops max, 60 byte packets  
1 10.167.144.2 (10.167.144.2) 2.703 ms 2.558 ms 2.611 ms  
linux@rpi4:~ $ traceroute -m3 www.startpage.com  
traceroute to www.startpage.com (67.63.58.133), 3 hops max, 60 byte packets  
1 router.local (192.168.1.1) 0.603 ms 0.547 ms 0.496 ms  
2 254-68-92-185.internet.netrebel.net (185.92.68.254) 0.891 ms 0.864 ms 0.7  
95 ms  
3 192.168.8.3 (192.168.8.3) 1.857 ms 1.906 ms 1.974 ms  
linux@rpi4:~ $
```

```
root@andre-Latitude-7390:/home/andre# hostname -I  
192.168.190.105  
root@andre-Latitude-7390:/home/andre# wg-quick up rpi4  
[#] ip link add rpi4 type wireguard  
[#] wg setconf rpi4 /dev/fd/63  
[#] ip -4 address add 10.167.144.2 dev rpi4  
[#] ip link set mtu 1420 up dev rpi4  
[#] ip -4 route add 10.167.144.0/24 dev rpi4  
root@andre-Latitude-7390:/home/andre# hostname -I  
192.168.190.105 10.167.144.2  
root@andre-Latitude-7390:/home/andre# ip route  
default via 192.168.190.49 dev wlp2s0 proto dhcp src 192.168.190.105 metric 600  
10.167.144.0/24 dev rpi4 scope link  
192.168.190.0/24 dev wlp2s0 proto kernel scope link src 192.168.190.105 metric 6  
00  
root@andre-Latitude-7390:/home/andre# ping -c1 10.167.144.1  
PING 10.167.144.1 (10.167.144.1) 56(84) bytes of data:  
64 bytes from 10.167.144.1: icmp_seq=1 ttl=64 time=99.4 ms  
  
--- 10.167.144.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 99.448/99.448/99.448/0.000 ms  
root@andre-Latitude-7390:/home/andre#  
exit  
andre@andre-Latitude-7390:~$ ssh linux@10.167.144.1  
Linux rpi4 6.6.51+rpt-rpi-v8 #1 SMP PREEMPT Debian 1:6.6.51-1+rpt3 (2024-10-08)  
aarch64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Sat Nov 2 16:11:56 2024  
linux@rpi4:~ $
```

# WG Tunnel voor Android

**hcc**<sup>!</sup>  
opensource



- Kan veel meer dan standaard Wireguard app voor Android
- Verkrijgbaar via [Playstore](#) en [F-Droid](#)
- Mogelijkheid instellen automatisch VPN gebruiken bij niet vertrouwde WIFI netwerken



# Meer over Wireguard configuraties lezen?

In het eerste nummer van 2025 van

ALLES OVER OPEN SOURCE  
**LINUX**  
MAGAZINE

komt een artikel over dit onderwerp.

# Vragen / opmerkingen?



Wireguard configuraties downloaden?

<https://lmi.hetnetwerk.org>

Klik daarna op de volgende mappen:

- 2025
- LM 2025-1
- Wireguard configuraties