

Fritz!Box Hacks: VPN mit WireGuard unter Linux & Android

PC-Treff-BB Aidlingen

Ingolf Wittmann

Agenda

- Warum VPN
- VPN erklärt
- Installationen
 - Fritz!Box
 - Handy / Tablet [Android]
 - Laptop [Debian 12]
 - Windows 11
 - Other

Warum VPN

- **Sicherheit:** Daten werden verschlüsselt und vor unbefugtem Zugriff geschützt.
- **Anonymität:** Online-Aktivitäten bleiben verborgen und die IP-Adresse wird durch die des Servers ersetzt.
- **Freiheit:** Es kann Zensuren und Blockierungen umgehen und auf Inhalte zugreifen, die im eigenen Land gesperrt sind oder im Ausland nicht zugreifbar.
- **Nachteil:** Die Nutzung von VPNs ist in einigen Ländern verboten und dass die Übertragungsgeschwindigkeit durch eine VPN-Verbindung oft verringert wird.

VPN Provider versus Fritz!Box

Provider ...

- Ein VPN-Anbieter bietet ein Netzwerk für anonyme Internetverbindungen
- Kostenpflichtige VPNs bieten oft eine starke Verschlüsselung und eine No-Logs-Richtlinie.
- VPN-Anbieter bieten möglicherweise zusätzliche Funktionen wie Werbeblocker, Split-Tunneling und Multi-Hop-Verbindungen.
- Unsichtbares Surfen im Internet

Alternative → Tor Netzwerk

Fritzbox ...

- Mit einem FRITZ!Box VPN können sichere Verbindungen zum Heimnetzwerk hergestellt werden
- Mit einem FRITZ!Box VPN kann man sich mit dem VPN eines Unternehmens verbinden.
- Mit einem FRITZ!Box VPN kann man mehrere Heimnetzwerke miteinander verbinden.
- Dienste und Server hinter der eigenen Fritz!Box erreichen
- Internetdiensten vortäuschen, dass man aus dem Heimnetzwerk surft (Mediatheken, Streaminganbieter, ...)
- Ist man mit der IP-Adresse des Routers im Internet sichtbar

IPSec versus WireGuard

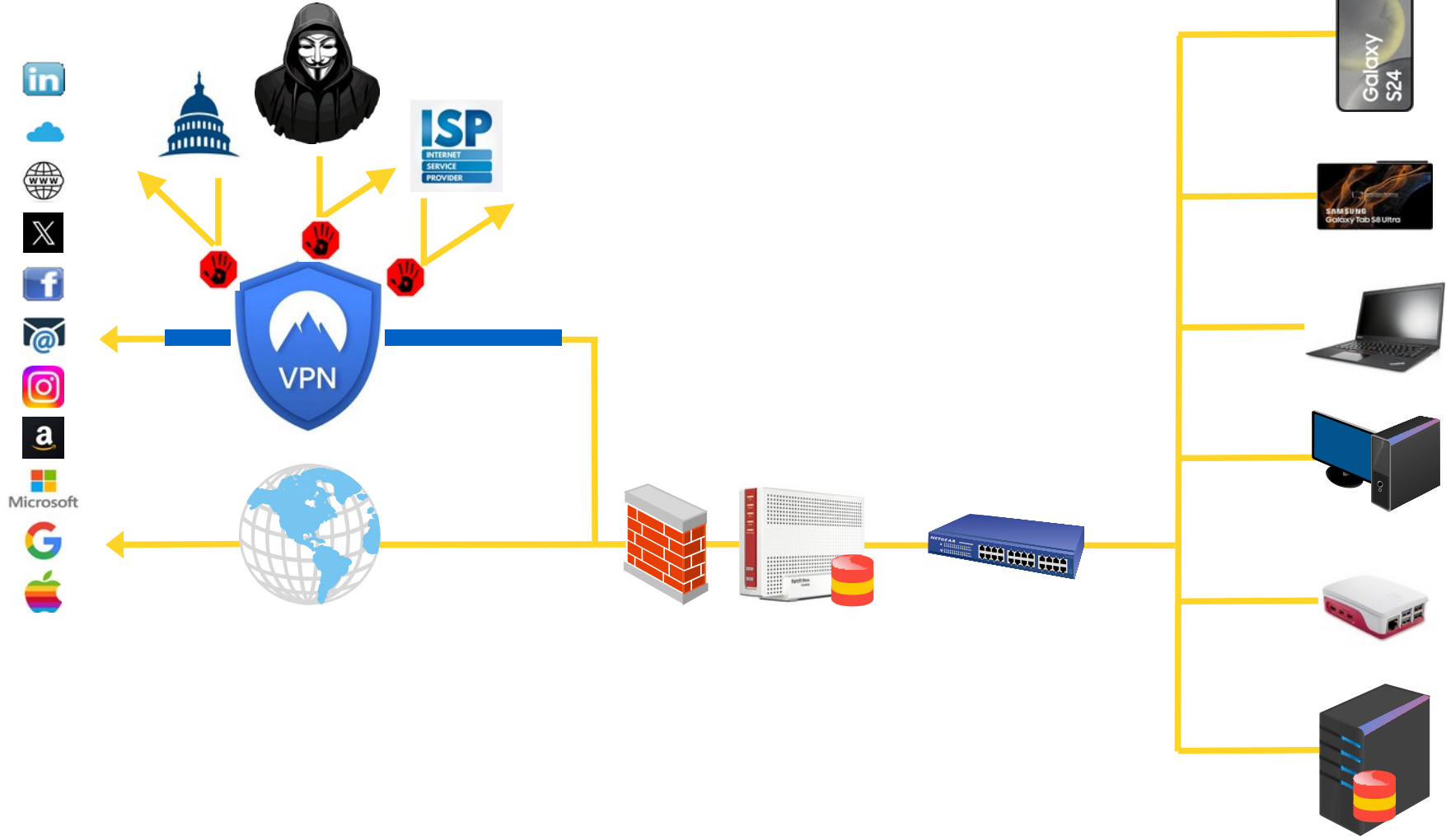
IPsec ...

- Frei und OpenSource
- kann erweitert werden um z.B. moderne Poly1305 und ChaCha20 Verschlüsselung zu verwenden
- technische Expertise notwendig
- Schlüsselaustausch: Internet Key Exchange (IKE)
- Protokoll: TCP & UDP

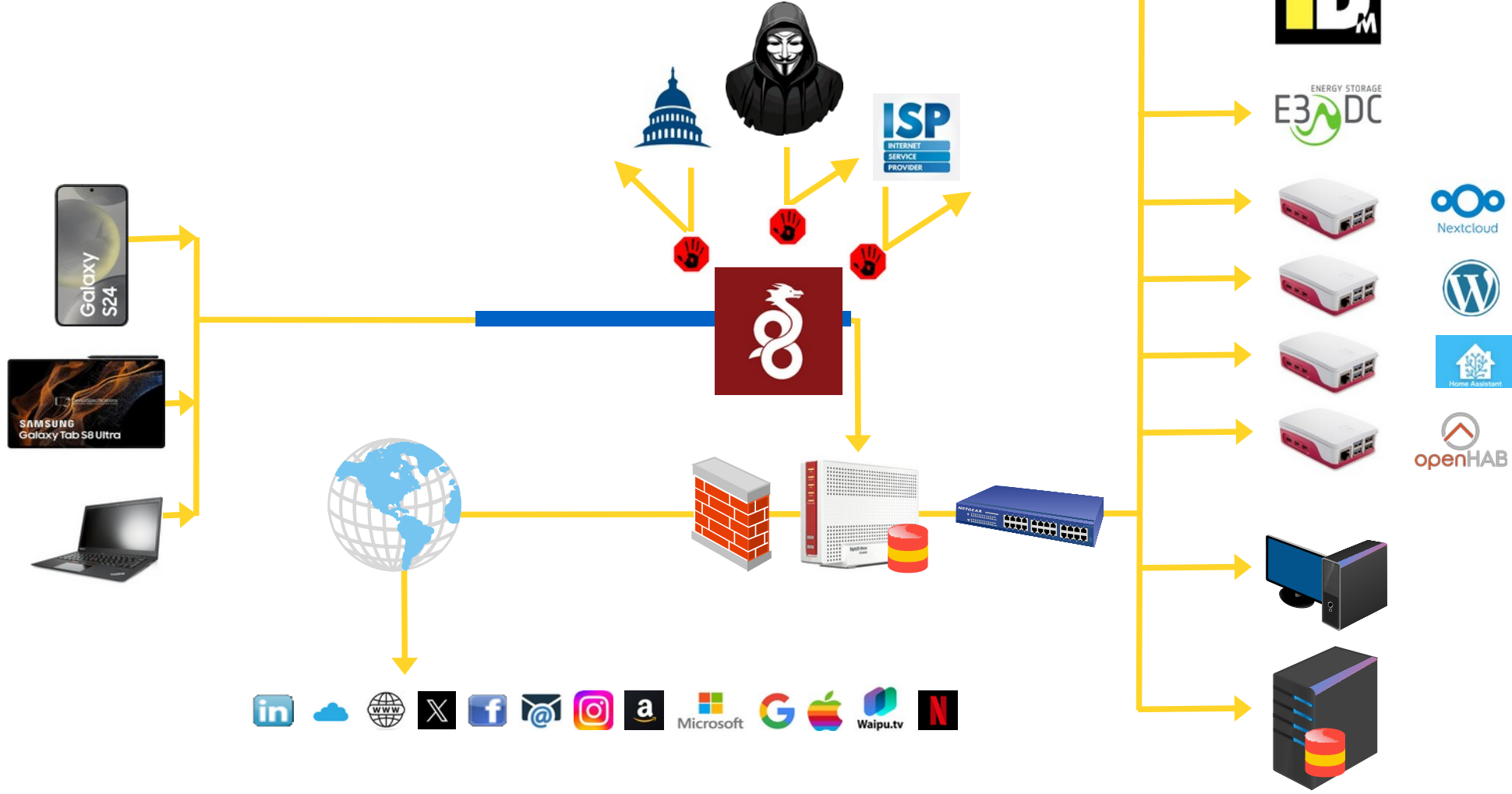
WireGuard ...

- Frei und OpenSource
- ist schneller und effizienter
- State-of-the-art Verschlüsselung
- einfacher aufzusetzen
- Schlüsseltausch: Noise Protokoll
- Protokoll: UDP

VPN Tunnel erklärt

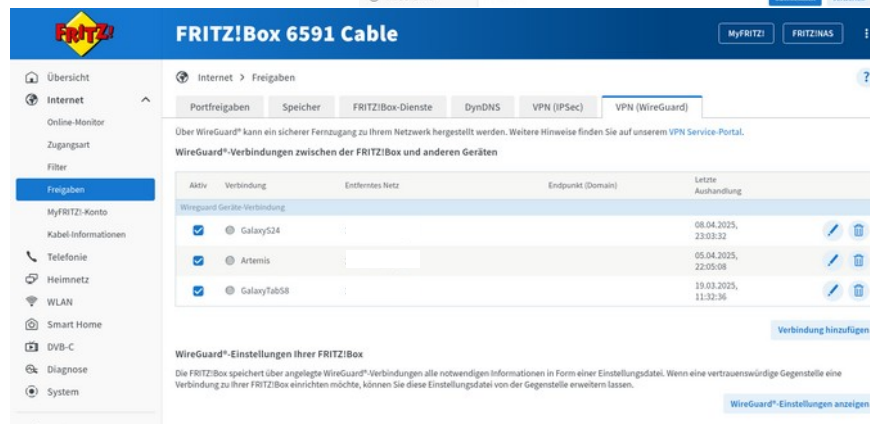
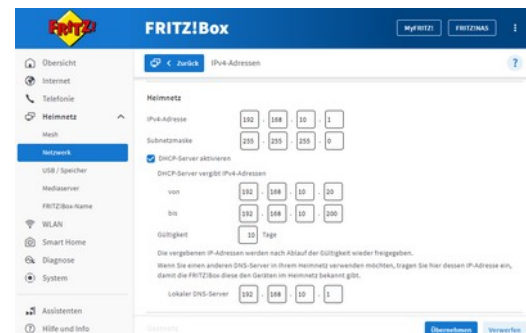
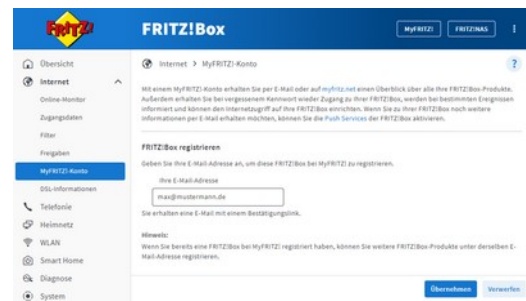


Fritz!Box VPN Tunnel erklärt



WireGuard Einrichten Fritz!Box

- MyFritz!-Konto einrichten
- IP-Netzwerk der Fritz!Box anpassen
- WireGuard auf Laptop, Handy, Tablett installieren
- VPN-Verbindung in der Fritz!Box einrichten



<https://fritz.com/service/vpn/wireguard-vpn-zur-fritzbox-am-computer-einrichten/>

WireGuard Einrichten Fritz!Box cont.


FRITZ!Box 6591 Cable
MyFRITZ!
FRITZ!NAS

Willkommen im WireGuard®-Assistenten

Welche WireGuard®-Verbindung möchten Sie erstellen?

☒ Einzelgerät verbinden

Richten Sie eine WireGuard®-Verbindung zu dieser FRITZ!Box für ein Smartphone, Tablet oder einem einzelnen Computer ein.



☐ Netzwerke koppeln oder spezielle Verbindungen herstellen

Richten Sie eine WireGuard®-Verbindung zwischen zwei FRITZ!Box-Netzwerken, dieser FRITZ!Box und einem VPN-Anbieter, dieser FRITZ!Box und einem WireGuard®-Server oder andere spezielle WireGuard®-Verbindungen ein.



☐ Für eine Verbindung zweier FRITZ!Box-Produkte (LAN-LAN) erstellen Sie hier die WireGuard®-Verbindung und importieren Sie diese auf der zweiten FRITZ!Box.

Weiter >
Abbrechen


FRITZ!Box 6591 Cable
MyFRITZ!
FRITZ!NAS

WireGuard®-Verbindung erstellen

Vergeben Sie einen individuellen Namen für die WireGuard®-Verbindung, um sie in der Übersicht unter diesem Namen zu finden.

Name der WireGuard®-Verbindung

< Zurück
Fertigstellen
Abbrechen


FRITZ!Box 6591 Cable
MyFRITZ!
FRITZ!NAS

VPN (WireGuard®)

✓ Die WireGuard®-Verbindung wurde erfolgreich erstellt.

Einstellungen auf Ihr Gerät übertragen

Sie haben nun die Möglichkeit, die Einstellungen über eine Datei auf Ihren Desktop oder Laptop zu übertragen oder über einen QR-Code an Ihr Smartphone / Tablet weiterzugeben. Nach dem Übertragen der Einstellungen auf Ihr Gerät können Sie den Fernzugriff nutzen.

Im Folgenden beschreiben wir Ihnen in kurzen Schritten, was zur Übertragung zu tun ist.

Smartphone oder Tablet



QR-Code scannen

Desktop oder Laptop



Einstellungen herunterladen

So funktioniert es:

Für die Verwendung mit einem Smartphone oder Tablet benötigen Sie die WireGuard®-App und den oben angezeigten QR-Code.

1. Installieren Sie die WireGuard®-App über den jeweiligen App-Store auf dem bevorzugten Gerät.

[Mehr Informationen in Hilfe anzeigen](#)

2. Starten Sie WireGuard®, tippen Sie auf das Plus „+“ und anschließend auf „aus QR-Code erstellen“.
3. Scannen Sie mit der Kamera Ihres Gerätes den oben angezeigten QR-Code ein.
4. Folgen Sie den weiteren Anweisungen in der WireGuard®-App.

Hinweis:

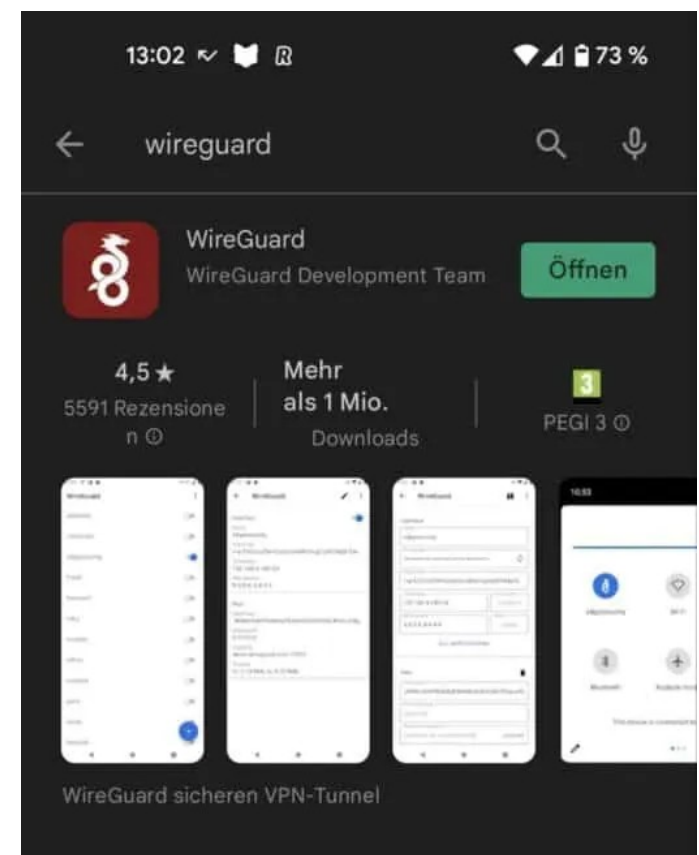
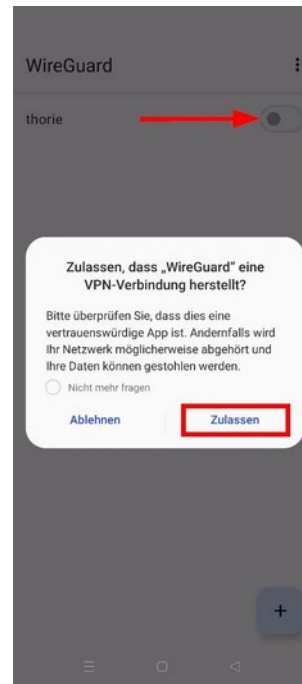
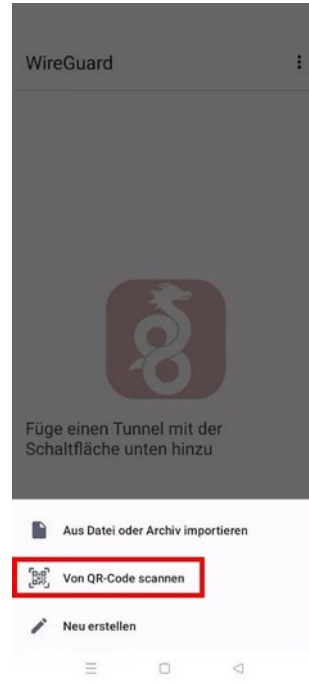
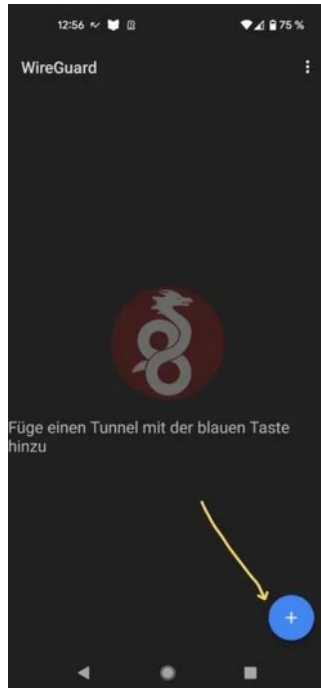
Beachten Sie, dass keine weiteren Geräte diese Verbindung zeitgleich nutzen können.

Wenn Sie die Einstellungen auf Ihrem Gerät übernommen haben, können Sie diese Ansicht schließen. Die neue Verbindung wird Ihnen dann auf der Übersicht der WireGuard®-Verbindungen angezeigt.

Schließen

WireGuard auf Android

- WireGuard app über Google Play installieren
- Tunnel hinzufügen
- Tunnel einschalten



WireGuard auf Debian12

- <https://fritz.com/service/vpn/wireguard-vpn-zur-fritzbox-am-computer-einrichten/>
<https://www.wireguard.com/install/>
- ```
sudo apt-get install wireguard
```

wireguard starten
- ```
# sudo modprobe wireguard
```
- ```
sudo systemctl start wg-quick@wg0.service
```
- ```
# sudo systemctl enable wg-quick@wg0.service
```
- ```
sudo systemctl status wg-quick@wg0.service
```

wiregard GUI installieren -> die original wiregard GUI funktioniert erst mit Gnome 44

- <https://github.com/UnnoTed/wireguird?tab=readme-ov-file>  

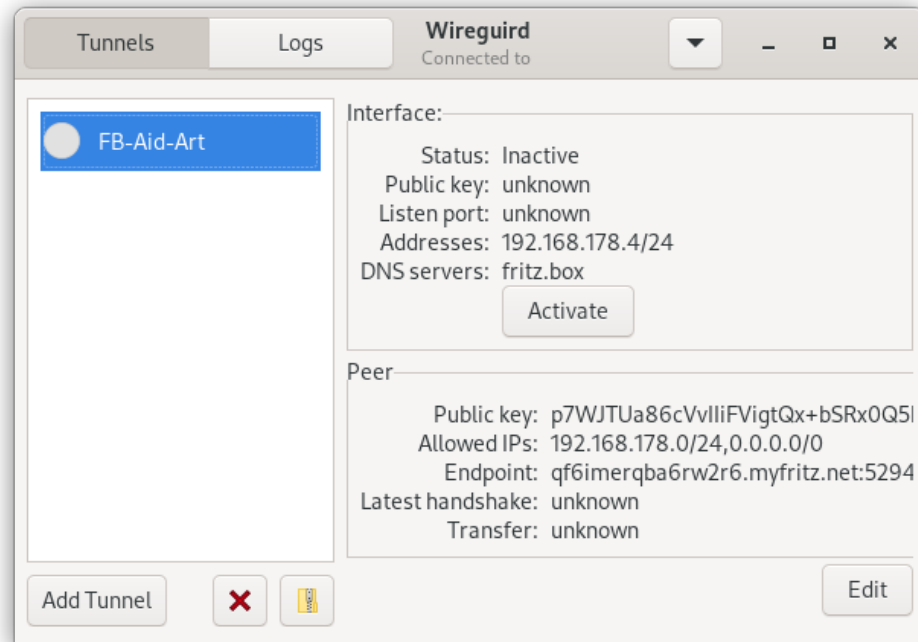
```
sudo apt-get install ./wireguird_amd64.deb
```

oder
- ```
# wget https://github.com/UnnoTed/wireguird/releases/download/v1.1.0/wireguird_amd64.deb
```
- ```
sudo dpkg -i ./wireguird_amd64.deb
```

wireguird starten

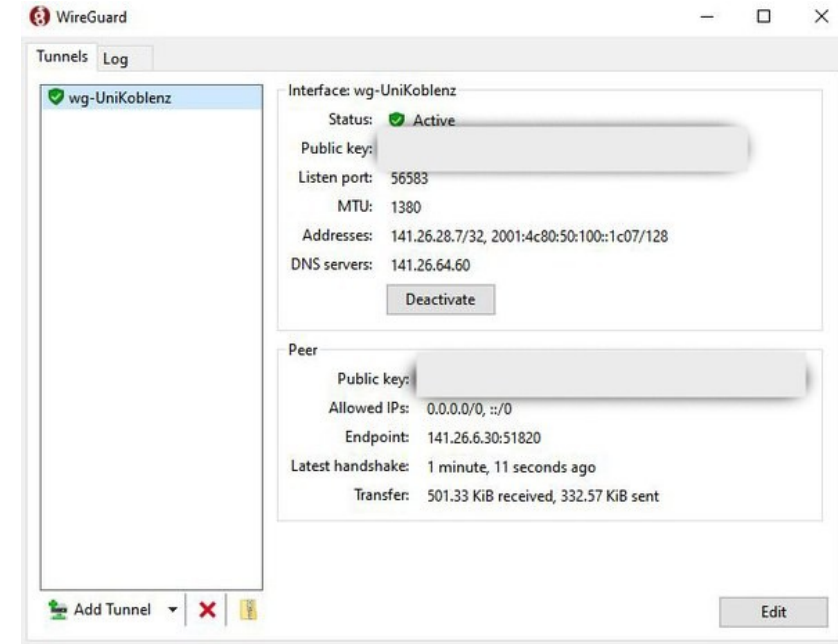
- ```
# wireguird
```

Tunnel hinzufügen
der Name der Config Datei darf nicht länger als 15 Zeichen sein
Tunnel aktivieren



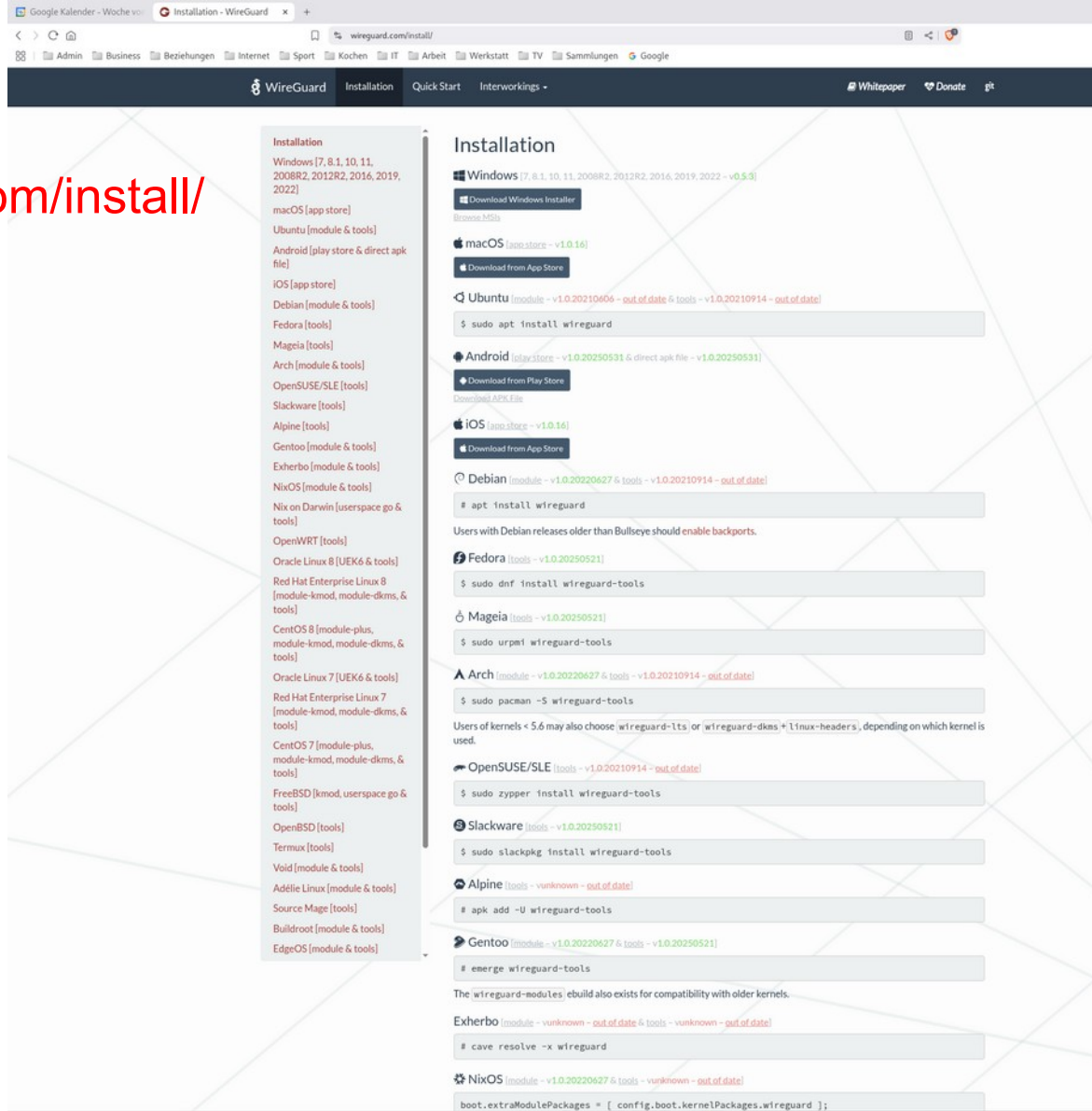
WireGuard auf Windows 11

- Installieren der [Windows-Wireguard-Software](#)
- Wireguard starten und importieren der Config Datei. .
- Wireguard ist unten rechts in der Taskbar (evtl. zusammengefasst hinter dem Pfeil). Dort startet man mit (Button "activate") und stoppt (Button "deactivate") die VPN-Verbindung



Other

<https://www.wireguard.com/install/>



Google Kalender - Woche von... Installation - WireGuard x +

Admin Business Beziehungen Internet Sport Kochen IT Arbeit Werkstatt TV Sammlungen Google

WireGuard Installation Quick Start Interworkings - Whitepaper Donate

Installation

Windows [7, 8.1, 10, 11, 2008R2, 2012R2, 2016, 2019, 2022 - v0.5.3]
[Download Windows Installer](#)
[Windows 32bit](#)

macOS [app store - v1.0.16]
[Download from App Store](#)

Ubuntu [module - v1.0.20210606 - out of date & tools - v1.0.20210914 - out of date]

```
$ sudo apt install wireguard
```

Android [play store - v1.0.20250531 & direct apk file - v1.0.20250531]
[Download from Play Store](#)
[Download APK File](#)

iOS [app store - v1.0.16]
[Download from App Store](#)

Debian [module - v1.0.20220627 & tools - v1.0.20210914 - out of date]

```
# apt install wireguard
```


 Users with Debian releases older than Bullseye should enable backports.

Fedora [tools - v1.0.20250521]

```
$ sudo dnf install wireguard-tools
```

Mageia [tools - v1.0.20250521]

```
$ sudo urpmi wireguard-tools
```

Arch [module - v1.0.20220627 & tools - v1.0.20210914 - out of date]

```
$ sudo pacman -S wireguard-tools
```


 Users of kernels < 5.6 may also choose 'wireguard-lts' or 'wireguard-dkms + linux-headers', depending on which kernel is used.

OpenSUSE/SLE [tools - v1.0.20210914 - out of date]

```
$ sudo zypper install wireguard-tools
```

Slackware [tools - v1.0.20250521]

```
$ sudo slackpkg install wireguard-tools
```

Alpine [tools - vunknown - out of date]

```
# apk add -U wireguard-tools
```

Gentoo [module - v1.0.20220627 & tools - v1.0.20250521]

```
# emerge wireguard-tools
```


 The 'wireguard-modules' ebuild also exists for compatibility with older kernels.

Exherbo [module - vunknown - out of date & tools - vunknown - out of date]

```
# cave resolve -x wireguard
```

NixOS [module - v1.0.20220627 & tools - vunknown - out of date]

```
boot.extraModulePackages = [ config.boot.kernelPackages.wireguard ];
```

Installation
 Windows [7, 8.1, 10, 11, 2008R2, 2012R2, 2016, 2019, 2022]
 macOS [app store]
 Ubuntu [module & tools]
 Android [play store & direct apk file]
 iOS [app store]
 Debian [module & tools]
 Fedora [tools]
 Mageia [tools]
 Arch [module & tools]
 OpenSUSE/SLE [tools]
 Slackware [tools]
 Alpine [tools]
 Gentoo [module & tools]
 Exherbo [module & tools]
 NixOS [module & tools]
 Nix on Darwin [userspace go & tools]
 OpenWRT [tools]
 Oracle Linux 8 [UEK6 & tools]
 Red Hat Enterprise Linux 8 [module-kmod, module-dkms, & tools]
 CentOS 8 [module-plus, module-kmod, module-dkms, & tools]
 Oracle Linux 7 [UEK6 & tools]
 Red Hat Enterprise Linux 7 [module-kmod, module-dkms, & tools]
 CentOS 7 [module-plus, module-kmod, module-dkms, & tools]
 FreeBSD [kmod, userspace go & tools]
 OpenBSD [tools]
 Termux [tools]
 Void [module & tools]
 Adelle Linux [module & tools]
 Source Mage [tools]
 Buildroot [module & tools]
 EdgeOS [module & tools]

Quellen und Materialien

- https://de.wikipedia.org/wiki/Virtual_Private_Network
- <https://vpntester.org/>
- <https://www.wireguard.com/install/>

Ingolf Wittmann



ingolf@ijwittmann.de



facebook.com/ingolf.wittmann.7



[@ijwatHAL](https://twitter.com/ijwatHAL)



de.linkedin.com/pub/ingolf-wittmann/27/189/132/



instagram.com/ingolf9591/