

# Sicher und anonym mit VPN?

Was VPNs wirklich leisten kann und was nicht.

Referent: Mateusz Roik

Augsburger Linux-Infotag 2025

26. April 2025

Technische Hochschule Augsburg



# Anonymität & Privatsphäre

# Anonymität

- **Anonymität ist der Zustand, in dem eine Person innerhalb einer Gruppe ununterscheidbar bleibt und somit nicht eindeutig identifiziert werden kann.**
- **wichtige Aspekte**
  - Keine Rückverfolgbarkeit
  - Gruppengröße
  - Abhängigkeit vom Kontext

# Anonymität im Internet

**Anonymität bezeichnet die Eigenschaft eines Systems, bei dem ein Akteur (z. B. ein Nutzer) zwar teilnimmt, aber nicht identifizierbar ist und seine Aktionen nicht eindeutig ihm zugeordnet werden können.**

# Privatsphäre

## Privatsphäre

- das Recht auf Selbstbestimmung über persönliche Daten
- das Recht auf räumliche und kommunikative Abgeschiedenheit (z. B. Wohnung, Briefgeheimnis)
- der Schutz vor ungewollter Beobachtung oder Überwachung

## Im digitalen Kontext

- personenbezogene Daten nicht ohne Zustimmung erhoben, verarbeitet oder weitergegeben werden dürfen → Datenschutz / DSGVO

# Was ist VPN

- **VPN: Virtual Private Network / Virtuelles Privates Netzwerk.**
- **Schutz der übertragenen Daten vor Dritten**
  - Vertraulichkeit
  - Integrität
  - Authentizität
- **Die drei VPN-Protokolle**
  - IPSec
  - OpenVPN
  - Wiregurd

# Aktuelle Marktaufteilung der VPN-Protokolle

Wireguard 20%

OpenVPN 50%

IPSec 30 %



# VPN-Protokolle: Chronologie

## IPSec

1990: Anfänge 1990

1995: erste RFC 1995

2005: aktuelle RFC

## Ziel

Datenverkehr auf IP-Ebene zu sichern – also sichere Kommunikation über unsichere Netzwerke wie das Internet zu ermöglichen.



# VPN-Protokolle: Chronologie

## openVPN

- 2001: James Yonan entwickelt openVPN
- 2002-2010: zahlreiche Verbesserungen
- 2009: Gründung von OpenVPN Technologies Inc. (heute OpenVPN Inc.)

## Ziel

ein einfaches, sicheres und portables VPN-System, das unter der Open-Source-Lizenz steht.

# VPN-Protokolle: Chronologie

## Wireguard

2015: Jason A. Donenfeld beginnt die Entwicklung

2017: erste Module für Linux

2018: Zahlreiche positive Sicherheitsreviews

2020:

- Bestandteil des Linux Kernels
- Start der Implementierung für Windows, macOS, Android, iOS

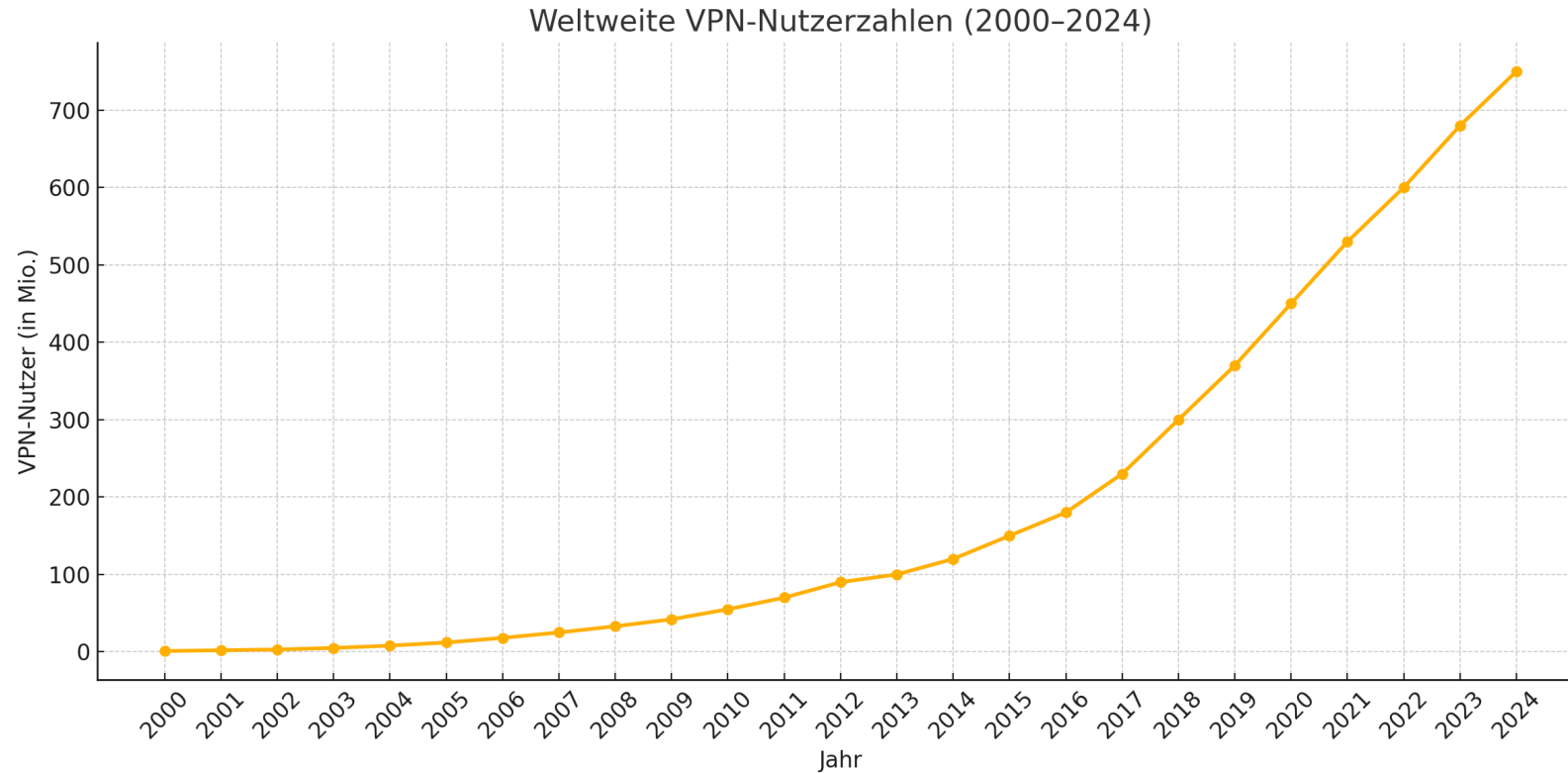
## Ziel

Ein modernes VPN-Protokoll, das sicher, schlank, effizient und leicht zu konfigurieren ist – im Gegensatz zu komplexen Systemen wie IPsec und OpenVPN.

# VPN-Protokolle: Vergleich

Merkmal	IPsec	OpenVPN	WireGuard
<b>Authentifizierung</b>	X.509 , Benutzer/Passwort, PSK, 2FA (über radius)	X.509, Benutzer/Passwort, PSK, 2FA	Public/Private Keys
<b>Performance</b>	++	+	+++
<b>Einrichtung</b>	--	0	++
<b>Sicherheitsniveau</b>	Hoch, bei korrekter Konfiguration	Hoch, bei korrekter Konfiguration	Sehr hoch, modernes Design
<b>Stabilität bei Roaming</b>	Mittel	Gut, je nach Konfiguration	Sehr gut, extrem schnell im Roaming
<b>Standardports</b>	500, 4500	UDP 1194	keins
<b>Hauptanwendungsfälle</b>	Site-to-Site VPNs, Unternehmenslösungen	Remote Access (RAS), flexible Lösungen	Mobile VPNs, moderne VPN-Setups

# VPN-Anbieter: Nutzerzahlen



Quelle: Schätzungen basierend auf Daten von Statista, GlobalWebIndex, VPN-Anbietern

# VPN-Anbieter: Deutschland (2023)

- 61,7 % der Befragten gaben an, VPN zu kennen
- 25,5 % der Deutschen nutzt VPN
  - davon 46,7 % kostenpflichtige Angebote
  - 36,9 % entscheiden sich für kostenlose Dienste
- 38 % „der User verwenden ein VPN hauptsächlich, um ihre Online-Privatsphäre zu schützen.“
- 33 % „um Geräte und Online-Konten zu schützen“

# VPN-Mythen und Behauptungen

# Mythos: VPN verschleiert Ihren Standort.

- Es existieren öffentliche Datenbanken, die einer IP eine recht genaue Ortsangabe zuordnen. → richtig
- Smartphones/ Tablets greifen direkt auf das GPS zu! → falsch

# Mythos: Sicheres Surfen

**„Genieße jedes Mal, wenn du online gehst, ein sorgenfreies Surf-Erlebnis:**

- **Vermeide das Herunterladen von Schadsoftware**
- **surfe sicher vor Schnüfflern, Trackern und Werbung.“**



# Sicheres Surfen: Herunterladen von Schadsoftware

- Direkter Zugriff auf den gesamten / ausgewählten Traffic → schlecht für Privatsphäre

# Sicheres Surfen: sicher vor Schnüfflern, Trackern und Werbung

## Blockiert ein VPN Facebook-Tracking?

„Ein VPN kann deinen virtuellen Standort verbergen,

**aber**

es wird Facebook nicht daran hindern, dich zu tracken, während du seine Dienste nutzt. Facebook kann immer noch sehen, welche Profile du ansiehst und was du postest, auch wenn die Datenschutzrichtlinien des Unternehmens die Möglichkeiten zur Nutzung dieser Daten einschränken.

Ein VPN verhindert jedoch, dass jemand, der dein Netzwerk überwacht, sieht, dass du Facebook benutzt.“

# Sicheres Surfen: sicher vor Schnüfflern, Trackern und Werbung

## Bedrohungsschutz Pro™

- DNS-Filterung → direkter Zugriff auf den Namen der Seite
- Schadsoftware-Scanners → direkter Zugriff auf die Daten
- URL-Trimmer → direkter Zugriff auf die URL

# Protokolliert NordVPN wirklich keine Daten?

**„Ja, unsere VPN-Praktiken wurden von der PricewaterhouseCoopers AG Schweiz gründlich geprüft – wir führen keine Nutzungsprotokolle über deine Online-Aktivitäten. Um unsere Dienste anbieten zu können, speichern wir jedoch einige Kundendaten (z. B. deinen Benutzernamen).“**

# Protokolliert NordVPN wirklich keine Daten?

„Stichprobenartig habe ich mir mal die NordVPN-App (Version 3.9.8) für Android angeschaut. Diese beinhaltet nicht nur einige Tracker, sondern übersendet eure E-Mail-Adresse, zusammen mit eindeutigen Identifikationsmerkmalen wie die Google Advertising-ID, bei der Registrierung sogar noch an einen Drittanbieter“

MIKE KUKETZ, 21. JANUAR 2019

# Protokolliert NordVPN wirklich keine Daten?

**„Hello there! We use these tools to monitor aggregated data to improve UI/UX and determine the efficiency of our marketing campaigns. They are not related to the user's activity when using our VPN service. In case you have further questions, do not hesitate to drop us a DM!“**

Support von NordVPN

# Mythos: „Ein VPN macht mich im Internet unsichtbar.“

„Wenn du ein Premium-VPN verwendest, das keine Protokolle anlegt, können dein Surfverhalten und deine IP-Adresse von niemandem nachverfolgt werden.

Wenn du dich jedoch bei Websites und Diensten anmeldest oder Apps auf deinem Gerät verwendest, können durchaus einige Informationen nachverfolgt werden.

Wenn du dich beispielsweise in deinem Google-Konto anmeldest, verfolgt und speichert Google Informationen über die von dir besuchten Websites, deine Google-Suchen, die Inhalte, die du dir angesehen hast und wie lange, sowie weitere ähnliche Informationen.“

# Mythos: "Ein VPN schützt mich vor allen Gefahren im Netz."

- Ein VPN schützt Ihre Verbindung im VPN-Tunnel, aber nicht vor Malware, Phishing oder unsicheren Webseiten.
- Ein VPN ist eine Schutzschicht – kein vollständiger Ersatz für Sicherheitsbewusstsein und Virenschutz.
- Phishing: Abholung von Email erfolgt verschlüsselt.



# Mythos: "Ein VPN schützt automatisch vor Viren und Schadsoftware."

- Ein VPN bietet keine Erkennung oder Abwehr von Schadsoftware. Dafür sind andere Schutzmaßnahmen nötig.
- Ergänzen Sie Ihr VPN mit einem aktuellen Virenschutz und gesunder Vorsicht beim Surfen.

# Mythos: "VPNs sind illegal oder nur für Hacker."

- In den meisten Ländern ist die Nutzung von VPNs legal
- Kann aber gegen die AGBs von z.B. Streaming-Diensten verstossen

## **(Zwischen)-Fazit**

- **Die Versprechen der VPN-Anbieter werden zwar gehalten, haben aber in der Regel geringen nutzwert.**
- **Schutz der Privatsphäre vor dem ISP, WLAN-Betreiber**
- **Blocken von Geolokation**
- **Die meisten Verbindungen sind bereits mit https verschlüsselt.**

# Anonym im Internet

- Für hohe Anonymität → TOR
- Wichtig:
  - Fehlerhafte Nutzung ( Anmeldung, Informationen preisgeben )
  - Unsichere Zusatzsoftware
  - Einstiegsknoten-Überwachung
  - Exit-Node Risiken
  - Timing- und Verkehrsanalysen
  - Browser-Fingerprinting

# Datenverfügbarkeit

- Unabhängig von VPN
- Entscheidend beim Thema Privatsphäre

„Automatisierte Scans: Microsoft sperrt Kunden unangekündigt für immer aus“

<https://heise.de/-7324608>


# Die Alternative: nextcloud

- **Kalender**
- **Dateimanager**
- **Notizen**
- **Officesuite**
- **Physische Gewalt über Ihre Daten**
- **Sie entscheiden, wer den Zugriff auf Ihre Daten hat.**

# Verbunden über Fritzbox

- IPSec ( ab 2016 ?)
- Ab Version 7.50 ( Dezember 2022 ) auch Wireguard

# Fritzbox: Einrichtung von Wireguard 1/6

**FRITZ!Box 7530 AX**

MyFRITZ!FRITZ!NAS

Übersicht

Internet

Online-Monitor

Zugangsdaten

Filter

Freigaben

MyFRITZ!-Konto

DLL-Informationen

Telefonie

Heimnetz

WLAN

Smart Home

Diagnose

System

Assistenten

Hilfe und Info

Internet > Freigaben

PortfreigabenFRITZ!Box DiensteDynDNSVPN (IPSec)VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden. Weitere Hinweise finden Sie auf unserem [VPN Service-Portal](#).

**Zur Einrichtung benötigen Sie Folgendes:**

- Die WireGuard®-App für Smartphones und Tablets oder die WireGuard®-Software für Computer  
Zur Übertragung der Einstellungen können Sie je nach verwendetem Gerät zwischen einem QR-Code oder einer Datei wählen. Die erforderlichen Download-Optionen finden Sie am Ende der Einrichtung.
- Eine MyFRITZ!-Adresse oder DynDNS-Adresse für Ihre FRITZ!Box  
Ihre WireGuard®-Verbindungen werden über Ihre MyFRITZ!-Adresse erstellt.

**WireGuard®-Verbindungen zwischen der FRITZ!Box und anderen Geräten**

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung
Es sind keine WireGuard®-Verbindungen eingerichtet.				

[Verbindung hinzufügen](#)

**WireGuard®-Einstellungen Ihrer FRITZ!Box**


Die FRITZ!Box speichert über angelegte WireGuard®-Verbindungen alle notwendigen Informationen in Form einer Einstellungsdatei. Wenn eine vertrauenswürdige Gegenstelle eine Verbindung zu Ihrer FRITZ!Box einrichten möchte, können Sie diese Einstellungsdatei von der Gegenstelle erweitern lassen.

[WireGuard®-Einstellungen anzeigen](#)

ÜbernehmenVerwerfen



# Fritzbox: Einrichtung von Wireguard 2/6


**FRITZ!Box 7530 AX**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

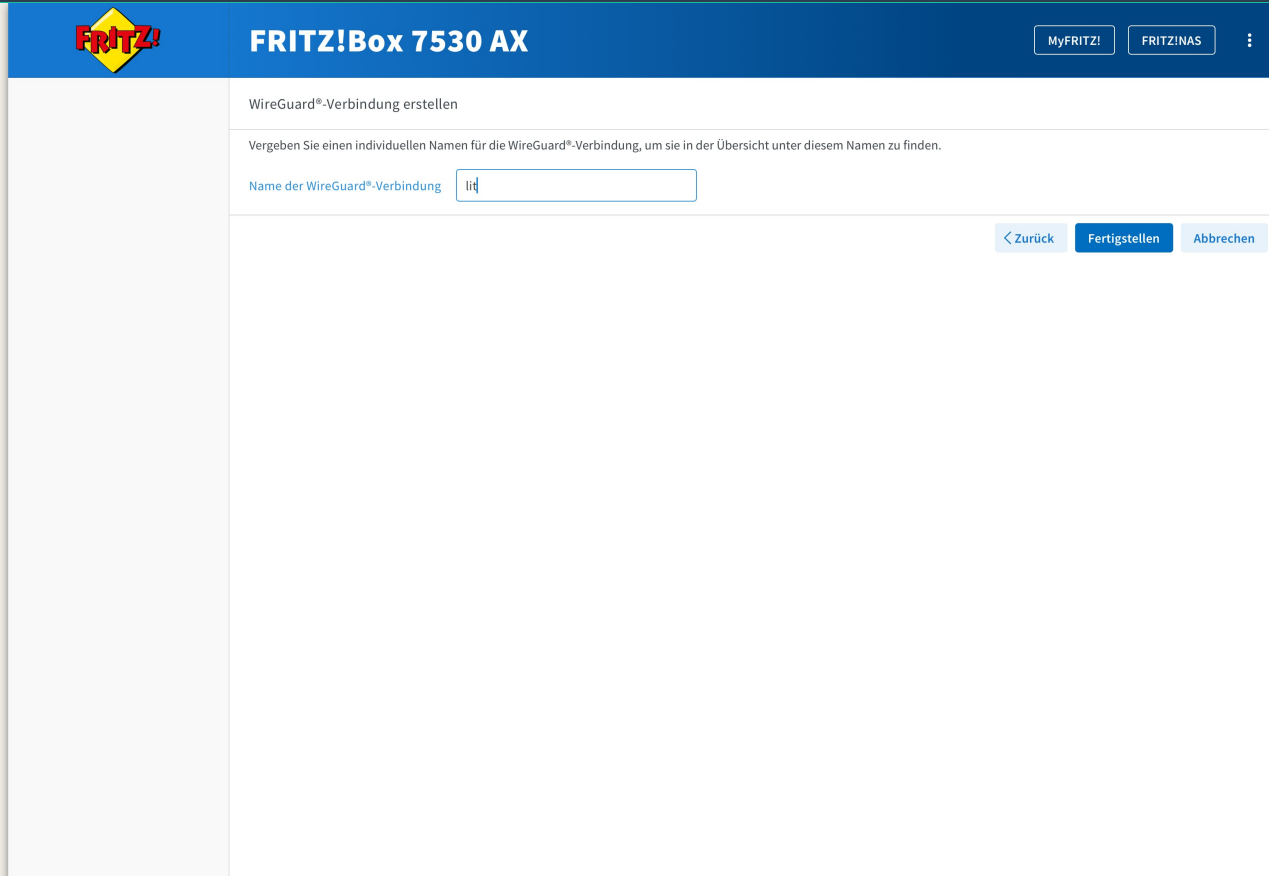
Richten Sie eine WireGuard®-Verbindung zwischen zwei FRITZ!Box-Netzwerken, dieser FRITZ!Box und einem VPN-Anbieter, dieser FRITZ!Box und einem WireGuard®-Server oder andere spezielle WireGuard®-Verbindungen ein.



 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

# Fritzbox: Einrichtung von Wireguard 3/6



The screenshot shows the FritzBox 7530 AX web interface. The top navigation bar is blue with the Fritz! logo on the left, the title "FRITZ!Box 7530 AX" in the center, and two buttons "MyFRITZ!" and "FRITZ!NAS" on the right. The main content area is white and titled "WireGuard®-Verbindung erstellen". Below the title, there is a instruction: "Vergeben Sie einen individuellen Namen für die WireGuard®-Verbindung, um sie in der Übersicht unter diesem Namen zu finden." followed by a text input field labeled "Name der WireGuard®-Verbindung" containing the text "lir". At the bottom right of the form, there are three buttons: "< Zurück", "Fertigstellen", and "Abbrechen".

FRITZ!

FRITZ!Box 7530 AX

MyFRITZ! FRITZ!NAS

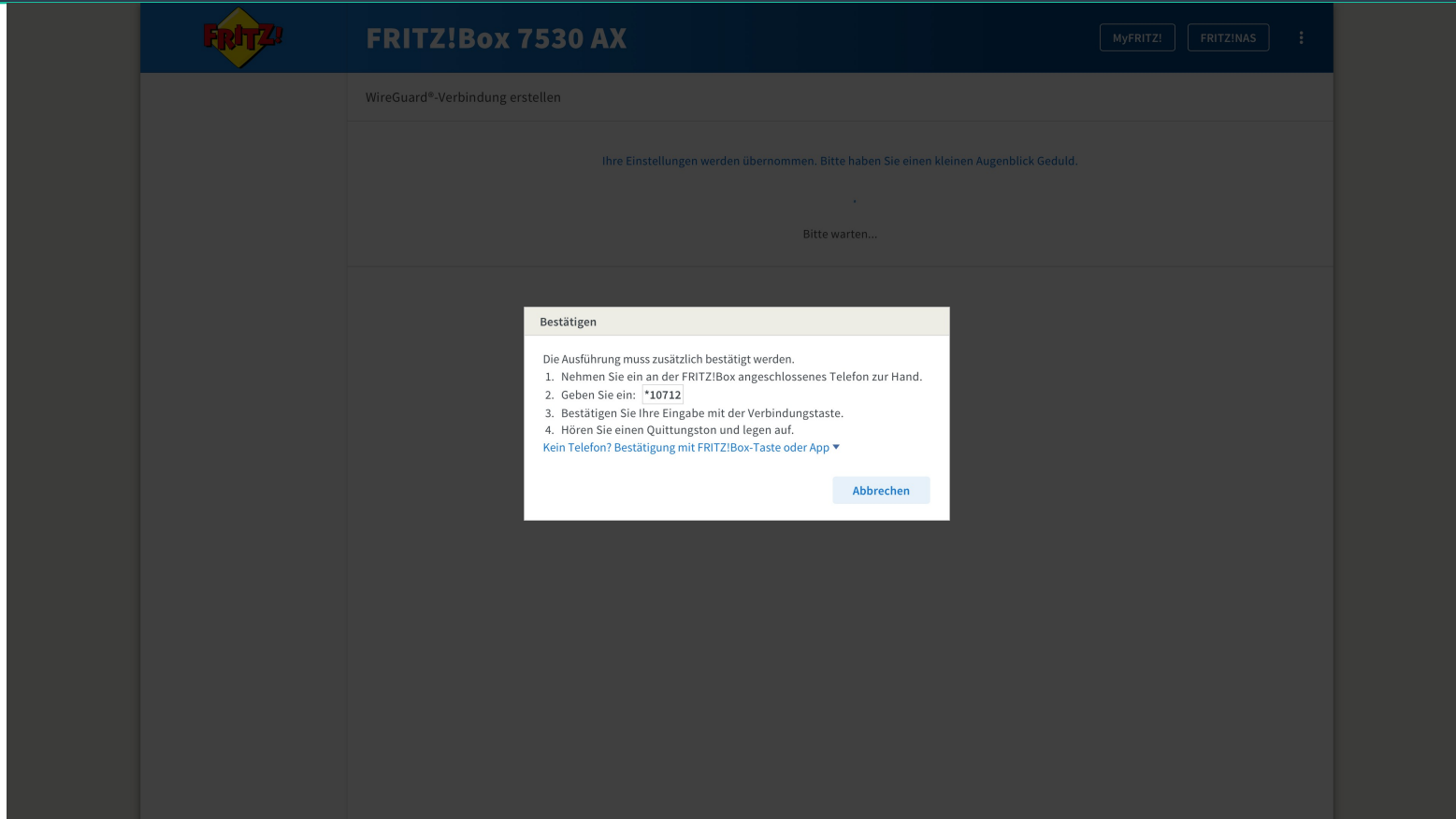
WireGuard®-Verbindung erstellen

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

# Fritzbox: Einrichtung von Wireguard 4/6



# Fritzbox: Einrichtung von Wireguard 5/6



## FRITZ!Box 7530 AX

[MyFRITZ!](#)[FRITZ!NAS](#)

### VPN (WireGuard®)

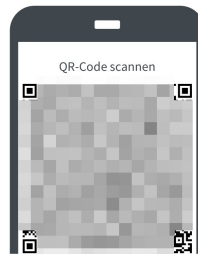
✓ Die WireGuard®-Verbindung wurde erfolgreich erstellt.

#### 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



#### 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.

#### Desktop oder Laptop

[Einstellungen herunterladen](#)

#### So funktioniert es:

Für die Verwendung mit einem Desktop oder Laptop benötigen Sie die WireGuard®-Software und die oben bereitgestellten Einstellungen.

1. Klicken Sie auf „Einstellungen herunterladen“, um die Einstellungen für Ihre WireGuard®-Verbindung nutzen zu können.
2. Installieren Sie die WireGuard®-Software für das Betriebssystem Ihres Desktops oder Laptops.

[Software auf www.wireguard.com finden](#)


3. Starten Sie WireGuard® und klicken Sie auf „Tunnel aus Datei importieren“.
4. Importieren Sie die oben angezeigte Datei und folgen Sie den weiteren Anweisungen der Software.

Hinweis:

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

[Schließen](#)

# Fritzbox: Einrichtung von Wireguard 6/6

**FRITZ!Box 7530 AX**

MyFRITZ!FRITZ!NAS

Übersicht

Internet

Online-Monitor

Zugangsdaten

Filter

Freigaben

MyFRITZ!-Konto

DSL-Informationen

Telefonie

Heimnetz

WLAN

Smart Home

Diagnose

System

Assistenten

Hilfe und Info

Internet > Freigaben

PortfreigabenFRITZ!Box-DiensteDynDNSVPN (IPSec)VPN (WireGuard)

Über WireGuard® kann ein sicherer Fernzugang zu Ihrem Netzwerk hergestellt werden. Weitere Hinweise finden Sie auf unserem [VPN Service-Portal](#).

WireGuard®-Verbindungen zwischen der FRITZ!Box und anderen Geräten

Aktiv	Verbindung	Entferntes Netz	Endpunkt (Domain)	Letzte Aushandlung
WireGuard Geräte-Verbindung				
<input checked="" type="checkbox"/>	lit			

Verbindung hinzufügen

WireGuard®-Einstellungen Ihrer FRITZ!Box

Die FRITZ!Box speichert über angelegte WireGuard®-Verbindungen alle notwendigen Informationen in Form einer Einstellungsdatei. Wenn eine vertrauenswürdige Gegenstelle eine Verbindung zu Ihrer FRITZ!Box einrichten möchte, können Sie diese Einstellungsdatei von der Gegenstelle erweitern lassen.

WireGuard®-Einstellungen anzeigen

ÜbernehmenVerwerfen

# Fritzbox: Hinweise

- **Wie bei VPN-Anbietern: Mit Wireguard wird der gesamte Traffic über die Fritzbox geleitet.**

## Wichtig

- kein Port forwarding!
- keine selbstständige Portfreigaben für dieses Gerät erlauben
- kein Exposed Host

# Anmeldung mit iPhone 1/2



# Anmeldung mit iPhone 2/2





# Wireguard Hinweise

- **Verbindungsaufbau bei Bedarf**
- **Danach wird die Verbindung automatisch aufrecht erhalten**

# Fritzbox: mögliche Probleme

- Viele ISP bieten nur IPv6 an
- Nicht alle Wlan-Betreiber unterstützen IPv6
- Manche WLAN-Betreiber blockieren ungewöhnliche Ports

# Fazit

## Was kann ein VPN-Anbieter leisten

- Schutz vor Geolokation
- Privatsphäre vor dem Wlan-Anbieter / ISP

## Was kann ein VPN-Anbieter nicht leisten

- Anonymität
- Privatsphäre über WLAN-Anbieter / ISP sicherstellen
- umfassenden Schutz vor Phishing / Malware / Viren

**Nutzen Sie nextcloud an der Fritzbox mit Wireguard !**

- <https://fritz.com/service/vpn/wireguard-vpn-zur-fritzbox-am-computer-einrichten/>
- <https://nextcloud.com/de/>
- **Lugatreff: jeden 1. Mittwoch im Monat ab 19:00 bei tuxedo.**
- <https://www.luga.de>
- <https://www.tuxedocomputers.com>
- **Geolokation: <https://ifconfig.co/>**

Vielen Dank für Ihr Interesse.

Viel Erfolg beim Einrichten von Wireguard und Nextcloud!

Kontakt:

Mateusz Roik, [lit@romavisio.net](mailto:lit@romavisio.net)