

# Wireguard Server Installation ganz einfach!

## Wireguard Server Installation ganz einfach!

Wer einen eigenen Wireguard Server betreiben möchte steht meistens vor der Herausforderung einige Fachkenntnisse mitzubringen. Daher haben wir eine Lösung entwickelt mit der es ganz einfach auch für Anfänger wird. In unserer Anleitung zeigen wir Dir den Weg und beschreiben jedes Detail des Vorganges. Mit dieser Anleitung sollten daher auch Neueinsteiger zu Recht kommen und in wenigen Minuten Ihren eigenen Wireguard Server in Betrieb haben.

### Inhaltsverzeichnis

---

## Der eigene Wireguard VPN Server.

In dieser Anleitung zeigen wir wie man einen VPN Server mit Wireguard selbst aufsetzt, dabei einen virtuellen Cloud Server verwendet mit einer statischen IP Adresse und diesen für verschiedene Anwendungen verwenden kann. Das ganze basiert auf dem Betriebssystem Ubuntu 20.04.xx und der Software und die Codebasis, welche Jason A. Donenfeld (Entwickler von Wireguard) veröffentlicht hat. Es ist aber auch möglich, allerdings nicht von uns getestet, andere Linux Betriebssysteme damit zu verwenden. Änderungen können in diesem Fall dazu notwendig sein. Ebenso können bei der Verwendung anderer Cloud Server Hostern eventuell andere Vorgehensweisen notwendig werden.

## Wireguard Server mit grafischer Benutzeroberfläche (GUI)

Du hast bei der Bedienung der Wireguard Servers anschließend eine grafische Benutzeroberfläche zur Verfügung und musst keine Programmierkenntnisse mitbringen.

Verbinden kannst Du dich mit den Geräten über die Verwendung der Wireguard Clients. Diese kannst Du in den Appstores, oder auch auf der Wireguard Projektseite finden und laden: [Wireguard Download](#). Es gibt die Clients für viele Gerätearten und Betriebssysteme auch für Windows, MacOS, Android, Apple iOS, Linux usw.

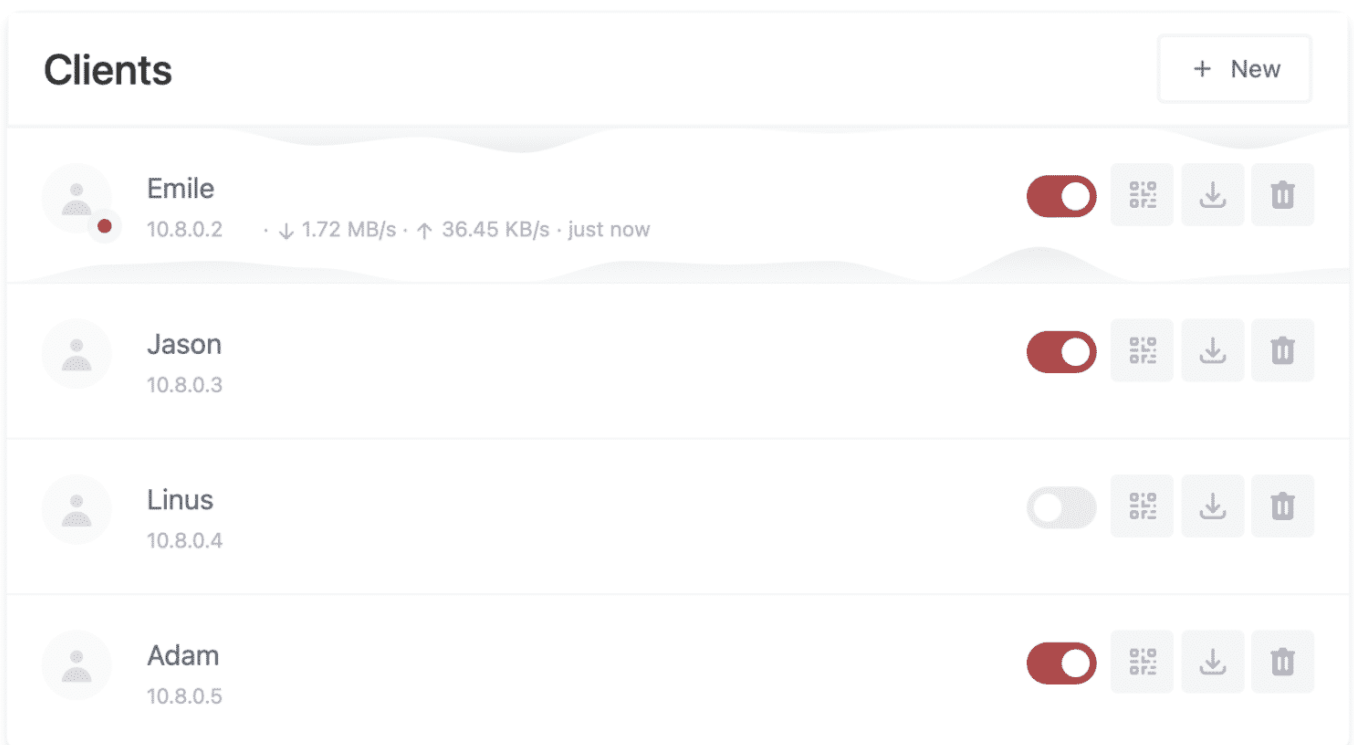
Der Wireguard Client auf Deinem Gerät baut dann einen verschlüsselten VPN Tunnel zum VPN Server auf und fortan werden alle Daten des Gerätes über diese VPN Verbindung gesendet und empfangen. Bei der Nutzung des internets erscheint nun die Server IP Adresse und nicht mehr die des verwendeten und verbunden Gerätes.

Dieser Wireguard Server unterscheidet sich in der Sicherheit und auch Ausführung nicht von den Servern die auch bei den meisten VPN Provider verwendet werden.

Wenn Du Dir nicht ganz sicher bist, dann Folge exakt unserer Anleitung, diese wird dich sicher zum Erfolg führen!

*Der ganze Vorgang um einen Wireguard Server selbst betreiben zu können ist sehr einfach und auch für Anfänger der Materie leicht durchführbar.*

## WireGuard



The screenshot shows the 'Clients' section of a WireGuard web interface. At the top right, there is a '+ New' button. Below it, a list of four clients is displayed, each with a profile icon, name, IP address, status toggle, and action buttons (QR code, download, delete).

Client Name	IP Address	Status	Transfer Rate	Time
Emile	10.8.0.2	On	↓ 1.72 MB/s · ↑ 36.45 KB/s	just now
Jason	10.8.0.3	On		
Linus	10.8.0.4	Off		
Adam	10.8.0.5	On		

Der eigene Wireguard Server ganz ohne Programmierkenntnisse

## Vor- und Nachteile eines eigenen Wireguard Servers

**Vorteile eines eigenen Wireguard Servers:**

- Eine statische IP Adresse verwenden
- Geringe Kosten und keine Bindung
- Wireguard Clients sind für alle geräte verfügbar:  
Windows, Mac, Android, iOS, Linux, VPN Router
- Du kannst damit lokale Internetsperren umgehen
- 100% Sicherheit vor Überwachung durch den  
Internetanbieter

## Nicht geeignet ist ein eigener Wireguard Server für:

- Umgehung von geografischen Sperren bei Streaming Diensten ist nur sehr begrenzt möglich.
- Anonymität und Schutz vor einer Ausforschung sind technisch bedingt nicht gegeben. Daher keine Torrent Nutzung damit.
- KillSwitch und andere sicherheitsrelevante Funktionen sind nicht direkt vorhanden und müssen wenn dann über manuelle Einstellungen am Client umgesetzt werden.

## Tipps

- Möchtest Du Wireguard aber mit einem professionellen VPN Dienst verwenden, dann empfehlen wir Dir die „nativen“ [Wireguard VPN Anbieter](#) zu verwenden.
- Möchtest Du Dich noch informieren, was Wireguard ist, dann haben wir einen entsprechenden Artikel der Dir dabei helfen wird: [Was ist Wireguard?](#)

Wir helfen darüber hinaus mit vielen weiteren Berichten zu diesem Thema, verwende dazu einfach unsere Suche auf der Webseite.

---

## Vorbereitungen für den eigenen VPN Server

Es sind nur wenige Dinge notwendig und Du kannst den eigenen Server verwenden. Diese Anleitung ist so einfach wie möglich gehalten und Du brauchst dazu nur wenige Anwendungen, wie zum Beispiel eine gültige EMail Adresse, eine Rufnummer für den Erhalt von SMS Nachrichten und auf Deinem PC/Mac eine Terminalanwendung.(Windows Konsole, Terminal)

## Terminalanwendung

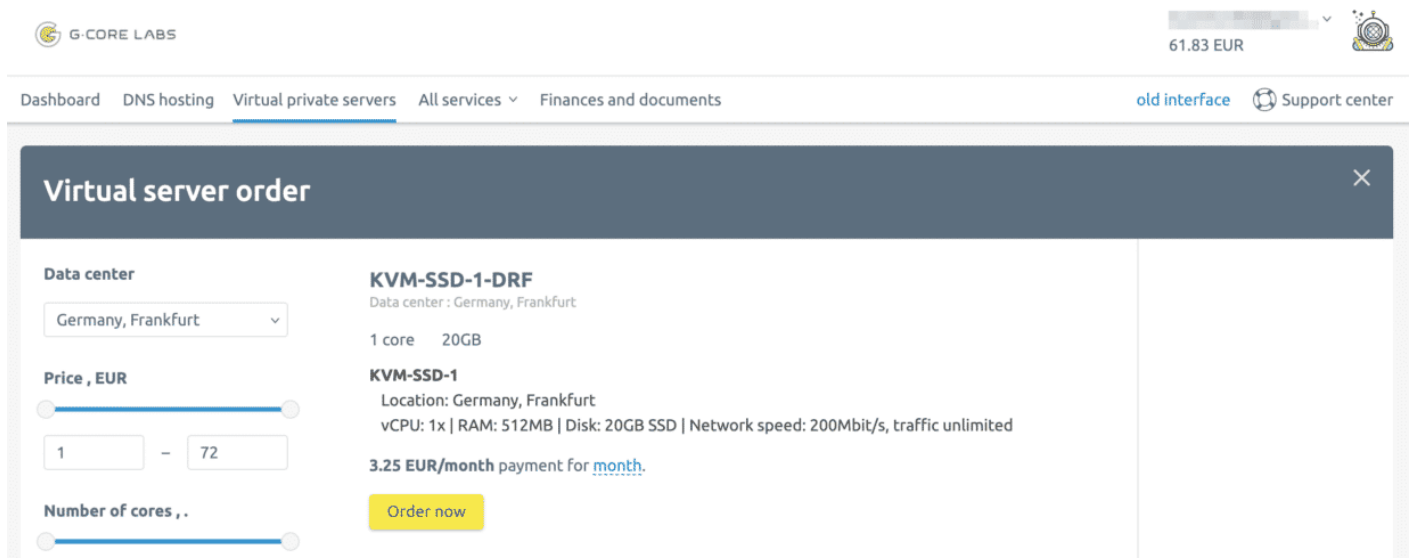
- Die Windows Konsole startest Du einfach mit der Tastenkombination Windowstaste+R öffnet sich „Ausführen“.
- Auf MacOS findest Du „Terminal“ im Zubehör unter den „Programmen“.

"Terminal" im Zubehör unter den "Programmen"

„Terminal“ im Zubehör unter den „Programmen“

## vServer bestellen

Du benötigst auf jeden Fall ein G-Core Labs Konto um die Prozedur umzusetzen. vServer sind dort auf täglicher oder monatlicher Basis PREPAID zu mieten. Die Kosten betragen weniger als €3,25 Euro pro Monat. Inkludiert ist eine statische IPv4 und eine IPv6 Adresse. Die Server haben mehr als 99,99% Betriebslaufzeit und sind nicht nur zuverlässig sondern dank SSD Speichern auch sehr schnell.



The screenshot shows the G-Core Labs website interface for ordering a virtual server. The top navigation bar includes 'Dashboard', 'DNS hosting', 'Virtual private servers', 'All services', and 'Finances and documents'. The user's account balance is shown as 61.83 EUR. The main content area is titled 'Virtual server order' and features a dropdown menu for 'Data center' set to 'Germany, Frankfurt'. Below this, there are sliders for 'Price, EUR' (set to 1) and 'Number of cores' (set to 72). The selected server plan is 'KVM-SSD-1-DRF' with specifications: 1 core, 20GB RAM, 1 vCPU, 512MB RAM, 20GB SSD, and 200Mbit/s network speed. The price is 3.25 EUR/month. A yellow 'Order now' button is visible.

GCore Labs Virtuelle Server bestellen

G-Core Labs Konto erstellen

[Videoanleitung: Wireguard Server Installation](#)

---

## Detaillierte Schritt für Schritt Anleitung

Es ist ganz einfach unserer Anleitung zu folgen. Verwende die in der Anleitung vorhandenen Links um zu den richtigen Ressourcen zu springen.

### Anleitung: Wireguard Server Installation

In dieser Anleitung zeigen wir Dir Schritt für schritt, wie Du einen eigenen Wireguard Server erstellen kannst und Geräte die Du damit verbinden möchtest verwaltest. Die Anleitung enthält Beispieldaten die Du durch Deine eigenen daten des vServers den Du erstellen wirst austauschen solltest. (IP Adresse des Server und Deine Passwörter). Jeder andere Schritt sollte einfach umzusetzen sein.

#### **1** *G-Core Labs Konto erstellen*

Erstelle ein G-Core Labs Konto indem Du diesem Link folgst: [G-Core Labs](#)

#### **2** *Erstelle einen virtuellen Server*

Im Kundenbereich kannst Du einen „virtuellen Server erstellen“. Das führt Dich zu dieser Seite: [vServer erstellen](#)

3

### *Standort und Größe wählen*

Wähle den für die passenden Standort und die Größe des vServers aus. Du benötigst die folgenden minimum Anforderungen:

- 512 MB Ram
- 1 Core
- mindestens 5GB SSD Speicher

**Info:** Du brauchst im weiteren Schritt keine zusätzliche IP Adresse auswählen. Eine ist IPv4 und eine IPv6 ist immer inkludiert.

Du kannst in dem folgenden Schritt auch die Zahlungsweise auswählen.

4

### *Bestellvorgang*

Die Konfiguration des Servers sollte auf „Ubuntu 20.xx“ geändert werden. Bei IOv4 und IPv6 braucht es keine Änderungen. Es muss auch keine Domain die statt der IP Adresse verwendet werden kann eingegeben werden.

  
**5** *Warte bis der Server aktiv ist*

Nun wird der Server erstellt. Dieser Vorgang kann bis zu 10 Minuten dauern. Setze den Vorgang fort, wenn der Server mit „Active“ gekennzeichnet ist.

  
**6** *Server Konfigurationsdaten*

Du kannst nun auch die Server Konfigurationsdaten einsehen. Du wirst im Anschluß der nächsten Schritte, die IP Adresse des Server als auch das Passwort benötigen.



**7**

## *Öffne ein Terminalfenster*

Du solltest nun ein Terminalfenster öffnen. In diesem gibst Du ein:

```
ssh root@89.43.107.97
```

Bestätige mit ENTER

Die IP Adresse stammt aus den Serverkonfigurationen die Du bei G-Core im Kundenbereich findest aus dem Schritt 6. Der Benutzername ist immer „root“

**8**

## *Anmeldung bestätigen*

In diesem Schritt musst Du bestätigen, dass Du die SSH Verbindung aufbauen möchtest. Gib dazu

```
yes
```

ein und bestätige mit ENTER

**9**

## *Passwort eingeben*

Nun musst Du das Passwort, das Du in der Serververwaltung angezeigt bekommst an dieser Stelle eingeben. Ich empfehle es langsam einzutippen und nicht rein zu kopieren. Danach bestätigst Du mit ENTER

**10**

## *Server Daten aktualisieren*

In diesem Schritt leitest du den Server an, die neuesten Verweise zu aktualisieren. dazu gibst Du

```
apt-get update
```

ein und bestätigst mit ENTER

**11**

## *Server aktualisieren*

In diesem Schritt wirst Du nach Updates für den Server suchen. Gib dazu

```
apt-get upgrade
```

ein und bestätige mit ENTER

## 12 *Docker installieren*

In diesem schritt wirst Du „Docker“ installieren. Gib dazu

```
sudo apt-get install docker.io
```

ein und bestätige mit ENTER

## 13 *Größe bestätigen*

Du musst nun bestätigen, dass Du die Daten von Docker auf Deinen Server laden willst. Gib dazu

```
Y
```

ein und bestätige mit ENTER

## 14

### Wireguard Server installieren

In diesem Schritt installierst Du den Wireguard Server mit einer grafischen Benutzeroberfläche auf den Server.

Gib dazu die folgenden Befehle ein (als ganzes kopieren und einfügen):

```
docker run -d \  
  --name=wg-easy \  
  -e WG_HOST=89.43.107.97 \  
  -e PASSWORD=DeinPasswort \  
  -v ~/.wg-easy:/etc/wireguard \  
  -p 51820:51820/udp \  
  -p 51821:51821/tcp \  
  --cap-add=NET_ADMIN \  
  --cap-add=SYS_MODULE \  
  --sysctl="net.ipv4.conf.all.src_valid_mark=1" \  
  --sysctl="net.ipv4.ip_forward=1" \  
  --restart unless-stopped \  
  weejewel/wg-easy
```

Die IP Adresse (**89.43.107.97**) und das **DenPasswort** sollte passend zu Deinen Daten aus dem Schritt „6“ ausgetauscht werden.

## 15

### Wireguard Verwaltung im Browser

Nun kannst Du in einem Browser die Wireguard Server Verwaltung öffnen. Gib dazu die IP Adresse Deines Server und den Port 51821 getrennt durch ein „:“ Zeichen ein.

Beispiel: „89.43.107.97:51821?“  
und bestätige mit ENTER

Die Verwaltung wird angezeigt.

Du kannst nun Das selbst gewählte Passwort, im Schritt12 ersichtlich“ eingeben und bestätigen.



## 16 *Client Verwaltung*

Du kannst nun neue Client Zugangsdaten erstellen für Deinen Wireguard Server



## 17 *Namen des Client angeben*

Du solltest einen eindeutigen und selbstgewählten Namen für die einzelnen Clients die. Du mit dem Wireguard Server verwenden möchtest angeben,

## 18

## Verwaltung der Clients

Di kannst die Konfigurationen für die einzelnen Clients als QR Code anzeigen lassen oder auf Dein Gerät laden. Ebenso kannst Du den Client Sperren oder erneut löschen.

## Anpassungen für erfahrene Nutzer

**Erfahrene Nutzer können auch weitere Einstellungen am VPN Server vornehmen.** Wir setzen hier Ubuntu ein, es kann auch zu notwendigen Anpassungen bei anderen Betriebssystemen wie Debian usw kommen. Diese Installation mit Docker lässt sich auch auf raspberry Pi mit ausreichender Leistung verwenden, wir haben dies allerdings nicht getestet.

### Konfigurationen anpassen

Die Konfigurationsdaten des Server werden unter „~/wg-easy“ gespeichert. (config.js ) Dort können diese auch später jederzeit angepasst werden.

### Optionen bei der Installation

Diese Optionen können durch Setzen von Umgebungsvariablen mit -e KEY="VALUE" im Befehl docker run konfiguriert werden.

Env	Standard	Beispiel	Beschreibung
PASSWORD	–	DeinPasswort	Wenn diese Option aktiviert ist, ist bei der Anmeldung bei der Web-Benutzeroberfläche ein Passwort erforderlich.
WG_HOST	–	vpn.myserver.com	Der öffentliche Hostname Ihres VPN-Servers.
WG_PORT	51820	1234	Der öffentliche UDP-Port Ihres VPN-Servers. WireGuard wird innerhalb des Docker-Containers immer auf 51820 lauschen.
WG_MTU	null	1420	Die MTU, die die Clients verwenden werden. Der Server verwendet die Standard-WG-MTU.
WG_PERSISTENT_KEEP_ALIVE	0	25	Wert in Sekunden, um die „Verbindung“ offen zu halten.
WG_DEFAULT_ADDRESS	10.8.0.x	10.6.0.x	IP-Adressbereich des Clients.
WG_DEFAULT_DNS	1.1.1.1	8.8.8.8	DNS-Server, den die Clients verwenden.
WG_ALLOWED_IPS	0.0.0.0/0, ::/0	192.168.15.0/24, 10.0.1.0/24	Erlaubte IPs, die die Clients verwenden.
WG_POST_UP	...	iptables ...	siehe config.js für den Standardwert.
WG_POST_DOWN	...	iptables ...	siehe config.js für den Standardwert.

## Updating

Um auf die neueste Version zu aktualisieren, führen Sie einfach aus:

- docker stop wg-easy
- docker rm wg-easy
- docker pull weejewel/wg-easy

Und führen Sie dann den obigen Befehl „docker run -d \ ...“ erneut aus.

Links:

<https://www.edvpfau.de/wireguard-netzwerk-mit-routing-einrichten/>

<https://unix.stackexchange.com/questions/689975/mount-smb-share-after-wireguard-with-fstab-or-systemd>

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

---

Revision #7

Created 2023-04-11 19:07:03 UTC by willi

Updated 2024-11-17 16:51:21 UTC by willi