

Vereinfachter PC-Zugriff auf das entfernte Netzwerk über den Fritz!Box WireGuard VPN Assistenten

Seit neuestem unterstützen bestimmte Fritz!Boxen [WireGuard](#) VPN, so zum Beispiel die Fritz!Box 7590 mit der neuen Firmware 7.50. Für andere Fritz!Boxen wird derzeit nur eine Beta-Firmwareversion von AVM, dem Hersteller der Fritz!Box, zur Verfügung gestellt. Die Einrichtung für PC Clients ist komfortabel, lässt jedoch keine individuelle Konfiguration zu. AVM stellt [hier](#) eine gute Anleitung zur standardmäßigen Einrichtung des WireGuard VPN-Servers und Nutzung des Assistenten für den Export von PC-Clientkonfigurationen zur Verfügung. Auch im [Video](#) von Fritz!Tec erläutert die Firma AVM, was VPN ist, welche Möglichkeiten die Fritz!Box für VPN-Verbindungen bereitstellt und welche Voraussetzungen zum Betrieb erfüllt sein müssen. Schließlich erläutert AVM [hier](#) die Funktionen von WireGuard und unterstreicht die einfache Umsetzung auf der Fritz!Box.

The screenshot shows the Fritz!Box 7590 web interface. The top navigation bar includes the Fritz! logo, the model name 'FRITZ!Box 7590', and buttons for 'MyFRITZ!' and 'FRITZINAS'. The left sidebar contains a menu with options like 'Übersicht', 'Internet', 'Freigaben', 'Telefonie', 'Heimnetz', 'WLAN', 'Smart Home', 'Diagnose', 'System', 'Assistenten', and 'Hilfe und Info'. The main content area is titled 'Internet > Freigaben' and features tabs for 'Portfreigaben', 'FRITZ!Box-Dienste', 'DynDNS', 'VPN (IPSec)', and 'VPN (WireGuard)'. The 'VPN (WireGuard)' tab is selected and circled in red. Below the tabs, there is a section titled 'Zur Einrichtung benötigen Sie Folgendes:' with two bullet points: 'Die WireGuard®-App für Smartphones und Tablets oder die WireGuard®-Software für Computer' and 'Eine MyFRITZ!-Adresse oder DynDNS-Adresse für Ihre FRITZ!Box'. A table below shows 'WireGuard®-Verbindungen zwischen der FRITZ!Box und anderen Geräten' with columns for 'Aktiv', 'Verbindung', 'Entferntes Netz', 'Endpunkt (Domain)', 'Letzte Aushandlung', and 'Gesamter Datenverkehr (IPv4)'. The table is currently empty, with a note 'Es sind keine WireGuard®-Verbindungen eingerichtet.' and a 'Verbindung hinzufügen' button.

Wenn nun auf einem PC der WireGuard Client aktiviert wird, in dem die durch den Fritz!Box Assistenten erzeugte Konfigurationsdatei (.conf) importiert wird, kann dieser PC nicht mehr auf lokale Netzwerkgeräte und Freigaben im Clientsegment zugreifen, sondern nur noch auf die im entfernten. Unter Umständen ist dieses Verhalten jedoch nicht erwünscht.

The screenshot shows the 'Willkommen im WireGuard®-Assistenten' screen. It asks 'Wie möchten Sie die WireGuard®-Verbindung erstellen?' and offers two options: 'Vereinfachte Einrichtung' (selected) and 'Benutzerdefinierte Einrichtung'. The 'Vereinfachte Einrichtung' option includes a diagram showing a smartphone connected to a PC via a 'VPN' connection. A red text box next to the diagram states 'Hier ist der Assistent für den Clientzugriff für einen PC.' The 'Benutzerdefinierte Einrichtung' option includes a diagram showing two computers connected via a 'VPN' connection. At the bottom, there is a note: 'Für eine Verbindung zweier FRITZ!Box-Produkte (LAN-LAN) erstellen Sie hier die WireGuard®-Verbindung und importieren Sie diese auf der zweiten FRITZ!Box.' The screen ends with 'Weiter >' and 'Abbrechen' buttons.

WireGuard VPN Client und Fritz!Box

Der WireGuard VPN-Assistent der Fritz!Box erzeugt standardmäßig zum Beispiel folgende Konfigurationsdatei. Keys und IP-Adressen sind im Beispiel aus Demonstrationszwecken eingeblendet, aber nicht real im Einsatz. Die entfernte Fritz!Box hat im Beispiel die interne IPv4 Adresse 192.168.1.1 und kann über die öffentliche myfritz.net Adresse über den Port 57062 im Internet angesprochen werden. Das lokale Netzwerk des Client-PCs darf - wie immer - nicht im gleichen Netzwerksegment des VPN-Servers bzw. der Fritz!Box, also im Bereich 192.168.1.0/24 liegen! Der Client-PC greift auf das entfernte Netzwerk mit der IP-Adresse 192.168.1.204 zu.

```
[Interface]
PrivateKey = Y1A283x4a5F687I8E9j0D1H2Z3w4j506k7x8a9+0A1I=
Address = 192.168.1.204/24
DNS = 192.168.1.1
DNS = fritz.box

[Peer]
PublicKey = O1u2W3F4h5I6C7I8v9x0I1W2g3/4D5L6Y738k9N2b03I=
PresharedKey = O/ueWUFjhbINCUIVvaxleWTgI/1D4LnY43/kINXbi3o=
AllowedIPs = 192.168.1.0/24,0.0.0.0/0
Endpoint = 11t2y3k4c5i6w728.myfritz.net:57062
PersistentKeepalive = 25
```

WireGuard Konfigurationsdatei Beispiel.conf

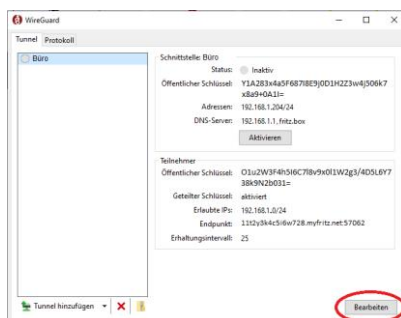
Die AVM WireGuard Definition unterdrückt lokale Netzwerkzugriffe und Freigaben auf dem Client-PC.

Wird diese Datei unverändert über den WireGuard Client eingelesen, so kann dieser PC nicht mehr auf lokale Netzwerkgeräte, also in seinem Netzwerksegment (z.B. 192.168.90.0/24) zugreifen, sondern nur noch auf Geräte und Freigaben im entfernten Netzwerk (192.168.1.0/24).

Für dieses Verhalten ist die Zeile *AllowedIPs = 192.168.1.0/24,0.0.0.0/0* verantwortlich. Der Ausdruck *0.0.0.0/0* sorgt dafür, dass alle DNS-Anfragen über die entfernte Fritz!Box bzw. über den dortigen DNS-Server via Internet aufgelöst werden. Dieses Verhalten kann zwar erwünscht sein, wenn alle Netzwerkaufgaben ausschließlich über das entfernte Büronetzwerk durchgeführt werden sollen. Sinnvoll ist eine solche Konfiguration, wenn ein Mitarbeiter aus einem öffentlichen Netzwerk auf das Firmennetzwerk zugreift (Café, Restaurant, Hotel etc.).

Andererseits, wenn ein Client auch auf die Geräte und Freigaben seines lokales Netzwerkes wie auch auf die des entfernten zugreifen soll, so muss diese Zeile auf *AllowedIPs = 192.168.1.0/24* reduziert werden. Der Ausdruck *,0.0.0.0/0* entfällt gänzlich.

Diese Änderung können Sie über den WireGuard Client auf Ihrem PC unter *Bearbeiten* leicht ändern.



WireGuard VPN Client und Fritz!Box

Insbesondere ist eine solche Konfiguration nützlich, um entfernte PCs per VPN-Verbindung zu warten und gleichzeitig uneingeschränkt auf lokale Ressourcen im eigenen Wartungsnetz zugreifen zu können. Natürlich können Sie so auch relativ einfach Dateien von beliebigen lokalen Netzwerkfreigaben zum entfernten System übertragen. Hingegen unterbindet die Standardkonfiguration von AVM ja solche Aktionen.

Grafische Benutzeroberfläche von WireGuard startet nur mit administrativen Rechten

Ein weiteres Problem liegt in der Tatsache, dass der WireGuard Client (GUI) nicht startet, wenn der aufrufende Benutzer ein Standardbenutzer, also kein Administrator ist. Außerdem darf nur ein Administrator die WireGuard Konfigurationsdatei einlesen.

Auf [Andys Blog](#) wird folgende Lösung des Problems - zumindest für die Professional und höheren Windowsversionen - aufgeführt. Ein Administrator des PCs startet unter seinem Benutzerkonto den Kommandoprompt mit erhöhten Rechten. Dort setzt er folgende Zeile ab:

```
reg add HKLM\Software\WireGuard /v LimitedOperatorUI /t REG_DWORD /d 1 /f
```

Anschließend führt er die Standardbenutzer, die die WireGuard Oberfläche nutzen sollen, der Gruppe der *Netzwerkkonfigurations-Operatoren* hinzu. Danach startet er den PC am besten neu. Nun muss er unter jedem Standardbenutzer den WireGuard Client mit administrativen Rechten (Rechtsklick: Als Administrator) einmalig aufrufen.

Ab sofort kann auch der „so behandelte“ Standardbenutzer den WireGuard Client aufrufen und die VPN-Verbindung starten und beenden. Leider können Nutzer der Windows Home-Editionen nicht unter *System-Computerverwaltung-Lokale Benutzer und Gruppen* die Benutzer- bzw. Gruppenrechte setzen, da diese Einstellung dort schlichtweg fehlt.

Im nächsten Kapitel werden wir demnächst die Besonderheiten beim WireGuard VPN Client am DS-Lite Anschluss besprechen. Lesen Sie dazu auch den Artikel [DDNS mit IPv6 in der Fritz!Box](#) einstellen.