

# Netzwerk

- [SSL-Verbindungstests mittels SSL Labs](#)
- [WireGuard-Verbindung zwischen FritzBox und Server herstellen](#)
- [Adminforge - Kostenlose Tools](#)
- [DNS-Zertifikat von Let's Encrypt über DynDNS bei deSEC \(DNS-Challenge\)](#)

# SSL-Verbindungstests mittels SSL Labs

Um zu testen wie gut eine Seite auf einer Domain hinsichtlich einer verschlüsselten Verbindung konfiguriert ist, kann man dazu folgende Seite nutzen:

<https://www.ssllabs.com/ssltest/index.html>

# WireGuard-Verbindung zwischen FritzBox und Server herstellen

Hier beschreibe ich das Vorgehen um zwischen einer FritzBox und einem Server (z.B. VPS) eine WireGuard-Verbindung aufzubauen.

Das kann sinnvoll sein, wenn man beispielsweise unverschlüsselte Daten verschlüsselt zum Server senden möchte. Dazu benötigt man einen VPN.

## Erster Schritt: WireGuard-Verbindung auf der Fritz-Box einrichten

Unter Internet->Freigaben->VPN(WireGuard) muss eine neue VPN-Verbindung eingerichtet werden. Dazu betätigt man den Button "Verbindung hinzufügen". Es startet sich ein Assistent.


Als erstes "Netzwerke koppeln oder spezielle Verbindung herstellen" auswählen:

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](#)

Nach "weiter" werden einige Fragen abgefragt diese wie folgt beantworten:

## Benutzerdefinierte Einstellungen festlegen

- Wurde diese WireGuard®-Verbindung bereits auf der Gegenstelle erstellt? [i](#)  Ja  Nein
- Soll die neue WireGuard®-Verbindung gleichzeitig zu einer bestehenden Verbindung der Gegenstelle genutzt werden? [i](#)  Ja  Nein
- Handelt es sich um ein Einzelgerät (Laptop, Smartphone, Tablet) oder um einen WireGuard®-fähigen Router (z.B. eine FRITZ!Box)?  Einzelgerät  WireGuard®-fähiger Router

 Das manuelle Hinzufügen der neuen Verbindungseinstellungen wird nur erfahrenen Benutzern empfohlen.

[< Zurück](#) [Weiter >](#) [Abbrechen](#)

Nach "weiter" muss eine Name für die Verbindung vergeben werden und die IP-Adresse des Servers mit einer Subnetzmaske. Am Schluss muss noch festgelegt werden, welche Geräte im eigenen (Heim-)Netzwerk über diese VPN-Verbindung kommunizieren sollen. Das kann zunächst auch offen bleiben und später festgelegt werden:

### Verbindung für einen WireGuard®-fähigen Router erstellen

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

Name der WireGuard®-Verbindung

Geben Sie das IP-Netzwerk der WireGuard®-Gegenstelle ein. Beachten Sie bitte, dass die Gegenstelle ein anderes Netzwerk als in Ihrem Heimnetz verwenden muss. Wenn die Gegenstelle eine manuelle IP-Adresse innerhalb des Netzwerks hat, geben Sie diese an.

Entferntes Netzwerk:  .  .  .

Subnetzmaske:  .  .  .

### Erweiterte Einstellungen zum Netzwerkverkehr

- Gesamten IPv4-Netzwerkverkehr über die VPN-Verbindung senden  
Aktivieren Sie diese Option, wenn diese FRITZ!Box sämtliche IPv4-Internetanfragen über die VPN-Verbindung zur WireGuard®-Gegenstelle senden soll.
- NetBIOS über diese Verbindung zulassen  
NetBIOS erlaubt es, einen Namen für Geräte netzwerkweit zu registrieren. Das ist besonders für Microsoft Windows Datei- und Druckerfreigaben wichtig.
- Nur bestimmte Geräte im Heimnetz sollen über diese WireGuard®-Verbindung erreichbar sein:  
Um eine Datei mit den ausgewählten Einstellungen zu erstellen, klicken Sie auf „Fertigstellen“.

[< Zurück](#) [Fertigstellen](#) [Abbrechen](#)

Mit "Fertigstellen" wird die Verbindung auf der FritzBox erstellt. Dieses muss mit der Verbindungstaste auf der FritzBox bestätigt werden.

Den weiteren Verlauf kann ich hier nicht mit Screenshots darstellen, weil bereits eine VPN-Verbindung zu dem Server besteht und es zu Netzwerkkonflikten kommt.

Man erhält am Schluss die Möglichkeit eine Konfigurationsdatei herunter zu laden. Diese kann dann nach leichter Modifikation auf dem Server genutzt werden:

```
[Interface]
PrivateKey = ....
Address = 77.237.247.4/24
```

```
#DNS = 192.168.0.2
#DNS = fritz.box

[Peer]
PublicKey = ....
PresharedKey = ....
AllowedIPs = 192.168.0.0/24
Endpoint = .....
PersistentKeepalive = 25
```

Die beiden DNS-Einträge entfernen oder mit einer "#" davor versehen!

## Zweiter Schritt: WireGuard-Verbindung auf dem Server einrichten

Auf dem Server müssen zunächst die WireGuard-Tools installiert werden. Unter ArchLinux wie folgt:

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

Die Konfigurationsdatei, die von der FritzBox heruntergeladen und leicht modifiziert wurde, muss nun auf dem Server abgelegt werden.

Am besten im folgenden Verzeichnis und mit dem Namen:

```
/etc/wireguard/wg0.conf
```

Nun kann diese Konfiguration mit folgendem Befehl im "NetworkManager" angelegt werden:

```
sudo nmcli connection import type wireguard file /etc/wireguard/wg0.conf
```

Anschließend müsste sich die neue Verbindung "wg0" automatisch mit der FritzBox verbinden.

# Adminforge - Kostenlose Tools

<https://adminforge.de>

# DNS-Zertifikat von Let's Encrypt über DynDNS bei deSEC (DNS-Challenge)

Im folgenden wird beschrieben, wie man mit Hilfe einer DynDNS bei deSEC ein DNS-Challenge hinbekommt, wenn der Domainanbieter dieses auf seinen DNS-Servern direkt nicht anbietet.

In meinem Fall ist der Anbieter "alldomains".

Der Inhalt wurde durch die KI von google generiert.

## Schritt 1: Kostenlose deSEC-Subdomain & Token erstellen

- Öffnen Sie die Website [desec.io](https://desec.io) und klicken Sie auf **Sign Up**.
- Registrieren Sie sich ganz einfach mit Ihrer **E-Mail-Adresse**. Sie erhalten einen Bestätigungs-Link.
- Nach dem Login erstellen Sie eine kostenlose Subdomain, die auf `.dedyn.io` endet (z. B. `thomass-itwiki-acme.dedyn.io`).
- Generieren Sie in den Einstellungen Ihres deSEC-Kontos einen **API-Token** (Geheimschlüssel) und kopieren Sie diesen.

## Schritt 2: Den CNAME-Eintrag bei alldomains setzen

Jetzt verknüpfen wir Ihre Hauptdomain mit deSEC, damit Let's Encrypt weiß, wo es suchen muss.

- Loggen Sie sich im Kundencenter von **alldomains.hosting** ein und öffnen Sie den DNS-/Zonen-Editor für Ihre Domain.
- Erstellen Sie einen neuen DNS-Eintrag mit diesen Werten:
  - **Typ:** `CNAME`
  - **Name / Host:** `_acme-challenge.iobroker`
  - **Wert / Ziel:** `thomass-itwiki-acme.dedyn.io.` (*Wichtig: Eventuell verlangt alldomains einen Punkt am Ende des Ziels*)

## Schritt 3: Zoraxy (Reverse Proxy) füttern

- Öffnen Sie **Zoraxy** -> **TLS / SSL** -> **ACME Tool**.
- Tragen Sie die Daten wie folgt ein:
  - **Domain(s):** Ihre echte Domain `iobroker.thomass-itwiki.de`

- **Validation Method:** `DNS-01`
- **DNS Provider:** Wählen Sie **deSEC** aus der Liste aus.
- **API Token / Credentials:** Fügen Sie hier den **API-Token** aus Schritt 1 ein.
- **Den Alias eintragen:**
  - Suchen Sie das Feld "**Challenge Alias**" (manchmal auch *DNS Domain Alias Mode* oder *ACME DNS*).
  - Tragen Sie dort Ihre deSEC-Adresse ein: `thomass-itwiki-acme.dedyn.io`
- Klicken Sie auf **Get Certificate**

## Weitere Subdomains in gleicher Weise hinzufügen:

Sie können all Ihre weiteren Subdomains über genau dieselbe eine Adresse bei deSEC absichern. Sie müssen dafür **kein** neues deSEC-Konto erstellen und auch **keine** neue Subdomain bei deSEC anlegen.

Die einzige Adresse `thomass-itwiki-acme.dedyn.io` dient ab jetzt als universeller „Briefkasten“ für all Ihre Zertifikatsprüfungen.

Alles, was Sie tun müssen, um eine neue Subdomain (zum Beispiel `nextcloud.thomass-itwiki.de`) hinzuzufügen, sind diese zwei Schritte:

Schritt 1: Den CNAME-Eintrag bei alldomains erweitern

Sie müssen bei alldomains für jede neue Subdomain einen eigenen CNAME-Eintrag anlegen. Das Prinzip ist immer dasselbe – der Name ändert sich, das Ziel bleibt exakt gleich.

- **Typ:** `CNAME`
- **Name / Host:** `_acme-challenge.nextcloud` (*bzw. passend zu Ihrer neuen Subdomain*)
- **Wert / Ziel:** `thomass-itwiki-acme.dedyn.io.` (*Wichtig: Eventuell wieder mit dem Punkt am Ende*).

Schritt 2: In Zoraxy das Zertifikat anfordern

Gehen Sie in Zoraxy wieder in das **ACME Tool** und tragen Sie die Daten für die neue Subdomain ein.