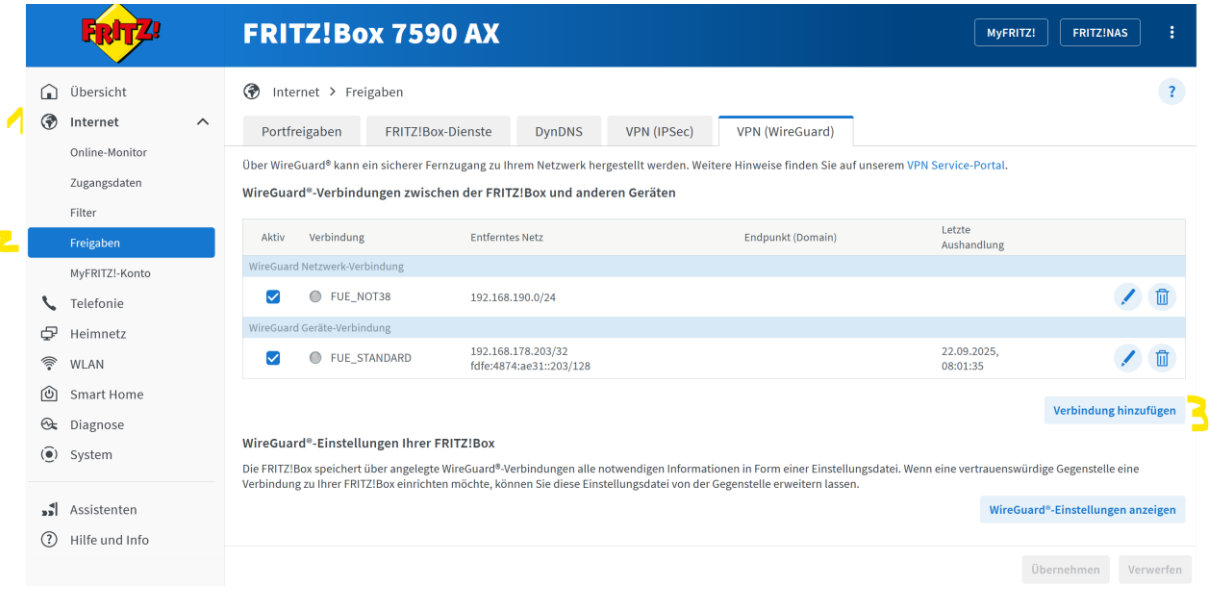
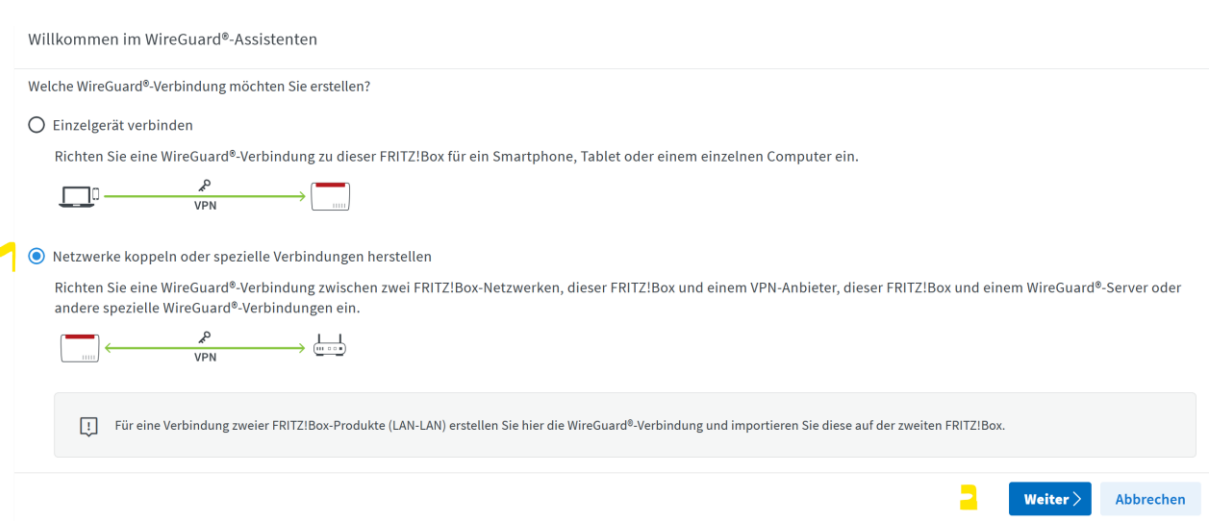
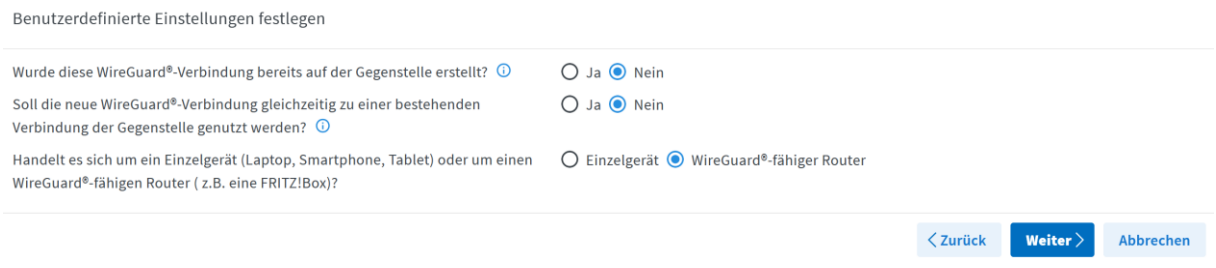
Wireguard Site-2-Site Verbindung von UDM (Client) zu Fritzbox (Server)

1. Verbindung in Fritzbox anlegen







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: NAME

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 IPv4-Netzwerk: 192 . 168 . 200 . 0

Subnetzmaske: 255 . 255 . 255 . 0

IPv6-Adresse (/64):

Geben Sie die DNS-Domains der WireGuard®-Gegenstelle ein, um die Heimnetz-Geräte der Gegenstelle mit ihrem Namen zu adressieren.

DNS-Domains

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.
- [x] 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

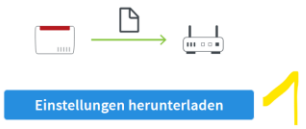
VPN (WireGuard®)

✓ Die WireGuard®-Verbindung wurde erfolgreich erstellt.

Einstellungen auf Ihrem Gerät manuell hinzufügen

Die nachfolgenden Einstellungen ermöglichen es Ihnen, die WireGuard®-Verbindung ebenfalls auf der WireGuard®-Gegenstelle zu hinterlegen.
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.



So funktioniert es:

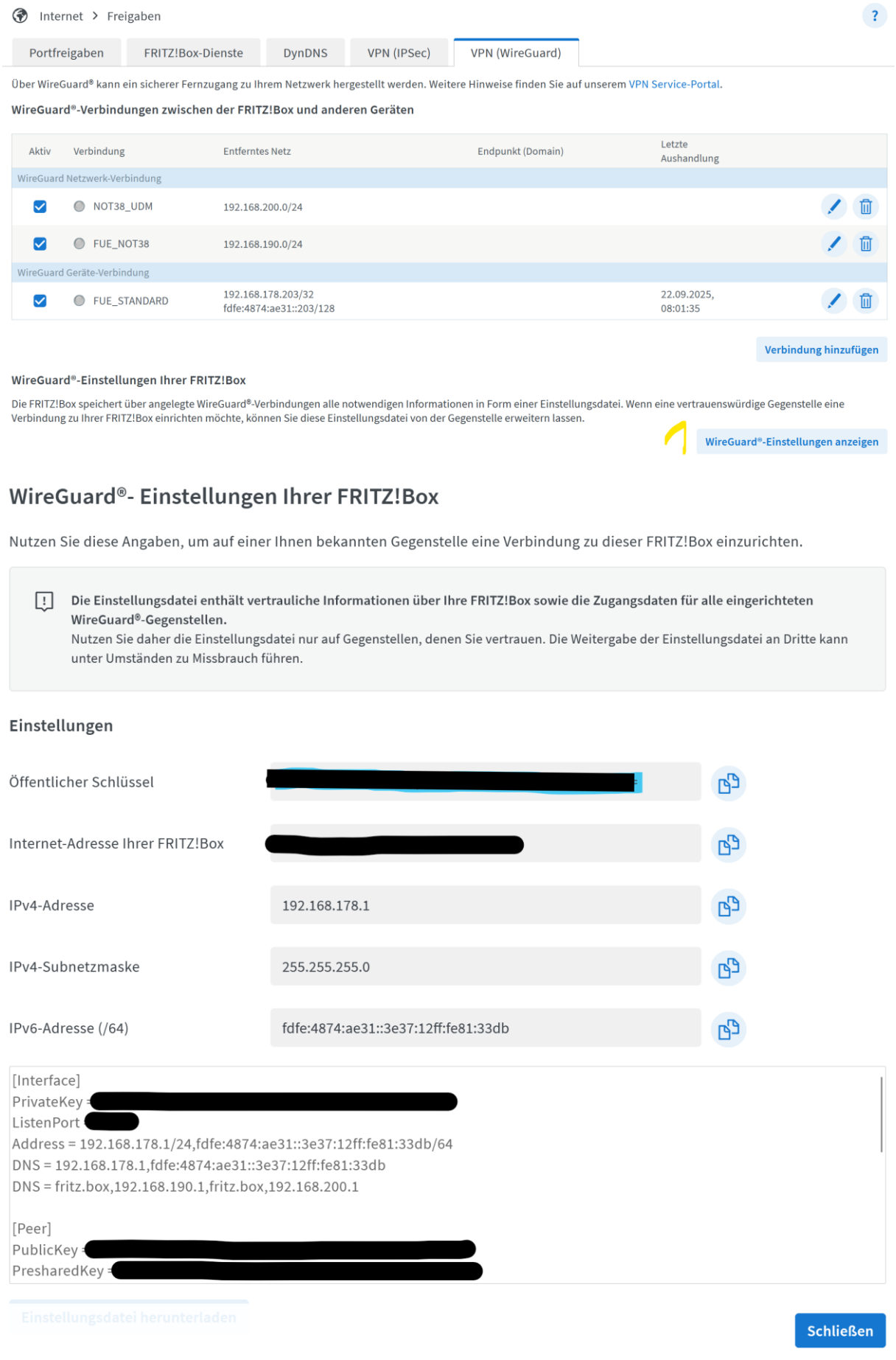
Für die Übertragung der Einstellungen auf die Gegenstelle benötigen Sie einen Desktop oder Laptop, den Zugang zur Benutzeroberfläche der Gegenstelle und die Datei mit den Einstellungen, die hier zum Download bereitsteht.

1. Klicken Sie auf „Einstellungen herunterladen“, um die Einstellungen für Ihre WireGuard®-Verbindung nutzen zu können.
2. Öffnen Sie WireGuard® auf der Benutzeroberfläche der Gegenstelle.
3. Importieren Sie die oben angezeigte Datei und folgen Sie den weiteren Anweisungen der Software.

Wenn Sie die Einrichtung der WireGuard®-Verbindung auf der Gegenstelle vorgenommen haben, können Sie diese Ansicht schließen. Die neue Verbindung wird Ihnen dann auf der Übersicht aller WireGuard®-Verbindungen angezeigt.

2 Schließen

2. Wireguard-Konfiguration der Fritzbox anpassen



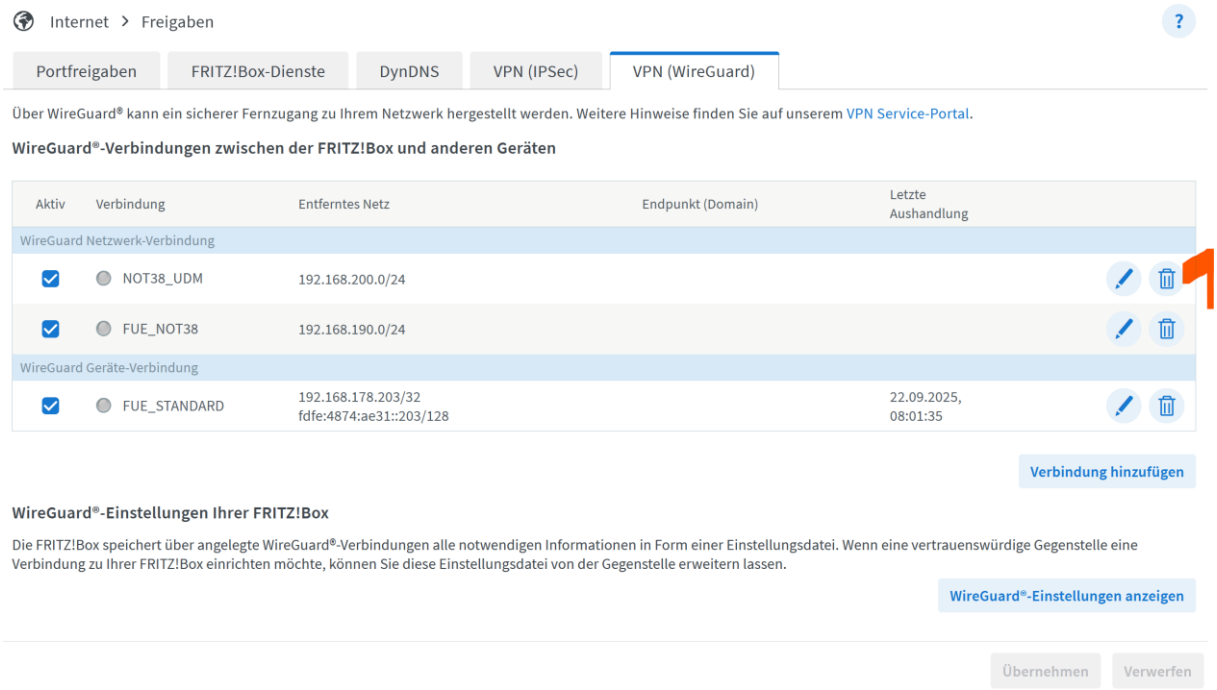
Text aus Konfigurationsanzeige kopieren und als Datei (z.B. „wg_config_FB.conf“) speichern:

```
[Interface]
PrivateKey = xxx
ListenPort = xxx
Address = 192.168.178.1/24,fdfe:4874:ae31::3e37:12ff:fe81:33db/64
DNS = 192.168.178.1,fdfe:4874:ae31::3e37:12ff:fe81:33db
DNS = fritz.box,192.168.190.1,fritz.box,192.168.200.1

[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.178.203/32,fdfe:4874:ae31::203/128
PersistentKeepalive = 25
[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.190.0/24
PersistentKeepalive = 25
[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.200.0/24
PersistentKeepalive = 25
```

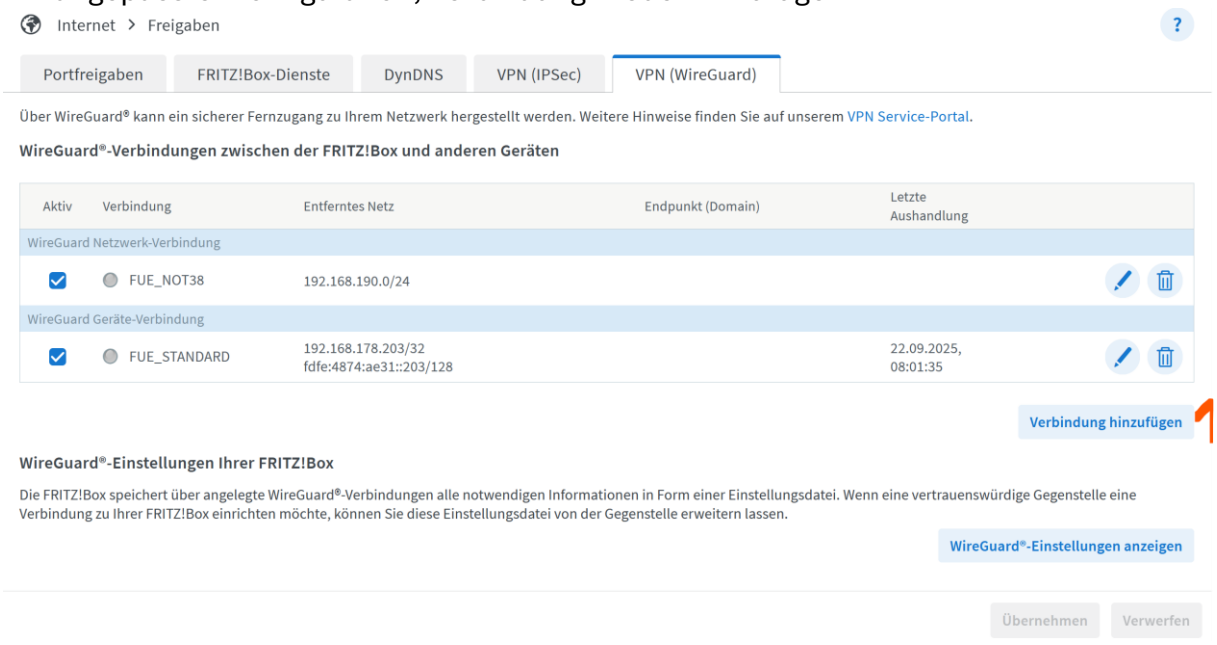
Modifikation der Konfiguration durchführen
→ Nicht anzupassende Peers (andere VPN-Verbindungen der FritzBox) löschen
→ DNS-Eintrag vereinfachen
→ AllowedIPs für Peer erweitern (hier muss jedes Netzwerk der UDM, das erreicht werden soll eingetragen werden)

```
[Interface]
PrivateKey = xxx
ListenPort = xxx
Address = 192.168.178.1/24
DNS = 192.168.178.1

[Peer]
PublicKey = xxx
PresharedKey = xxx
AllowedIPs = 192.168.200.0/24, 192.168.60.0/24
PersistentKeepalive = 25
```

Zuvor erstellte Verbindung löschen



Mit angepasster Konfiguration, Verbindung wieder hinzufügen



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

Benutzerdefinierte Einstellungen festlegen

Wurde diese WireGuard®-Verbindung bereits auf der Gegenstelle erstellt? ⓘ ◉ Ja ○ Nein

< Zurück Weiter > Abbrechen

Einstellungen einer bestehenden WireGuard®-Verbindung importieren

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

Name der WireGuard®-Verbindung NAME 1

Wählen Sie die Datei, aus der die WireGuard®-Einstellungen importiert werden sollen.

2 Durchsuchen... wg_config_FB.conf

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.

3 ☑ 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.

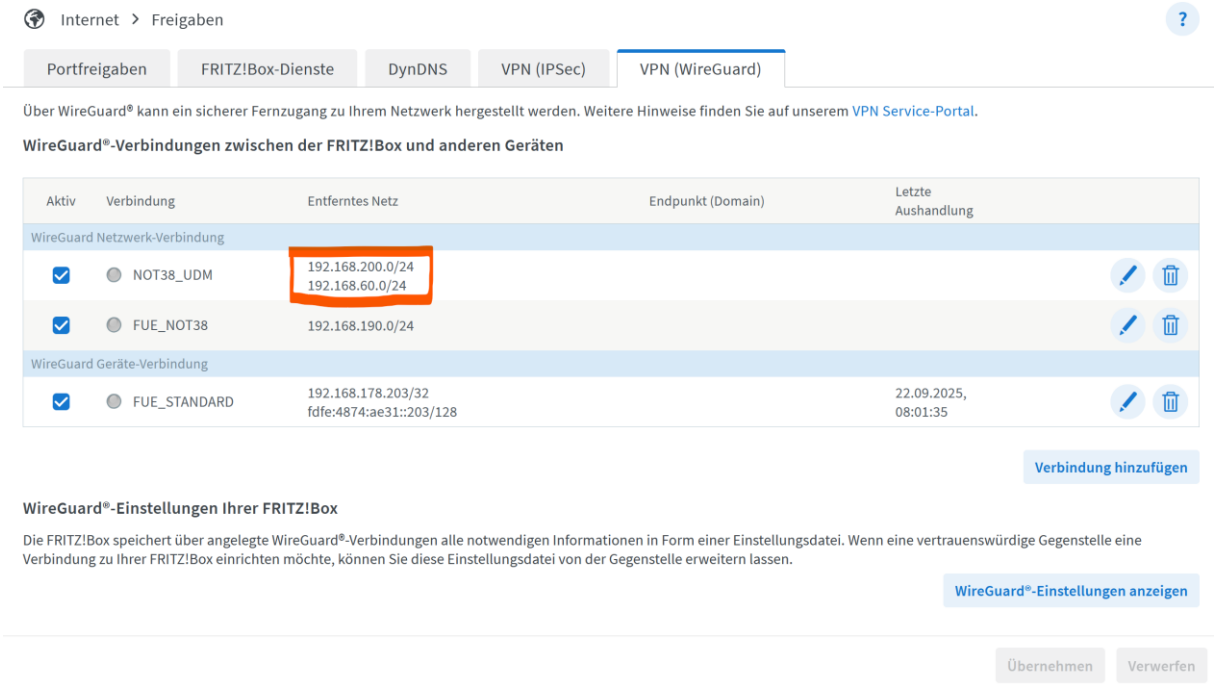
☐ Nur bestimmte Geräte im Heimnetz sollen über diese WireGuard®-Verbindung erreichbar sein:

Um die ausgewählten Einstellungen anzuwenden, klicken Sie auf „Fertigstellen“.

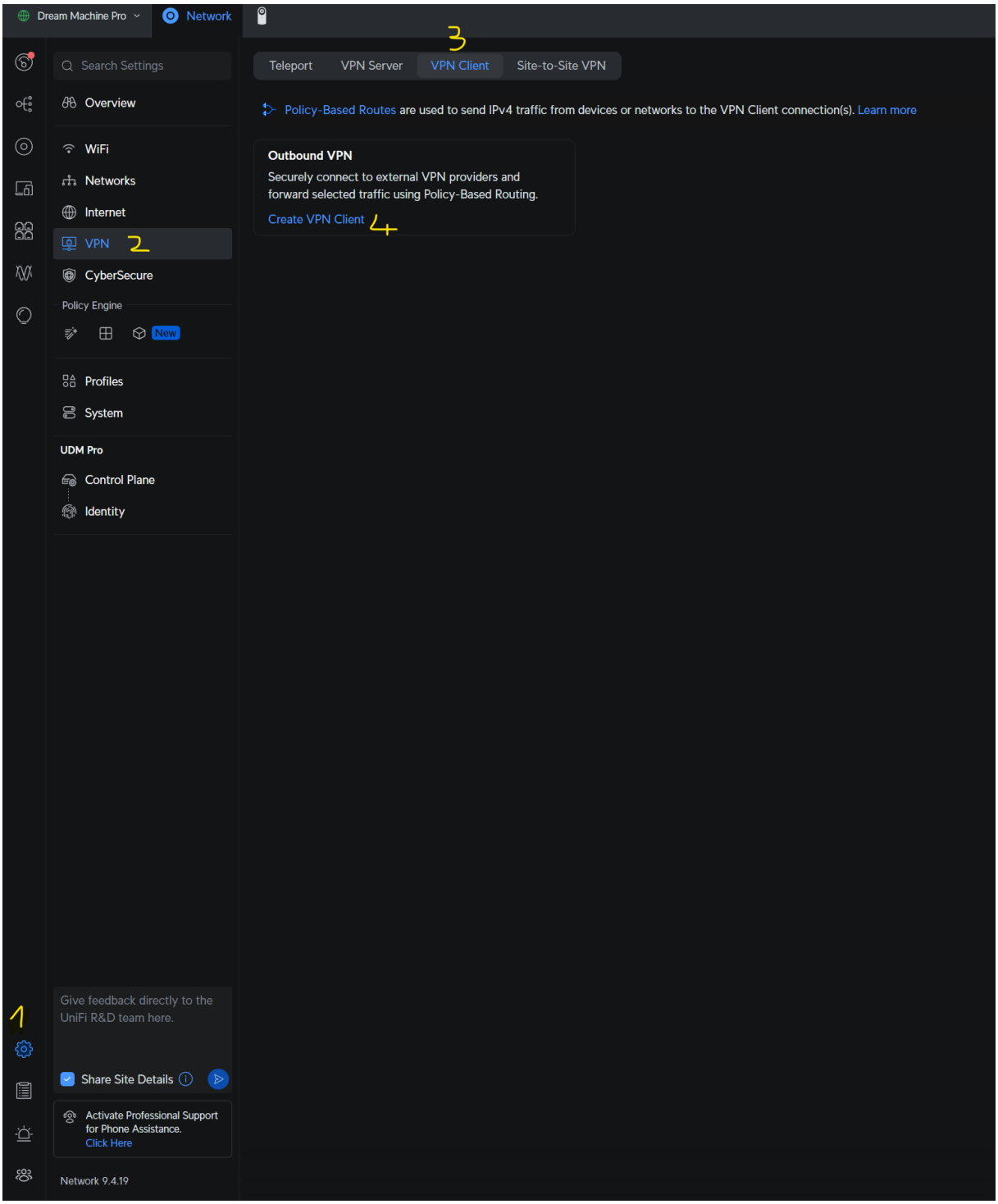
< Zurück Fertigstellen Abbrechen

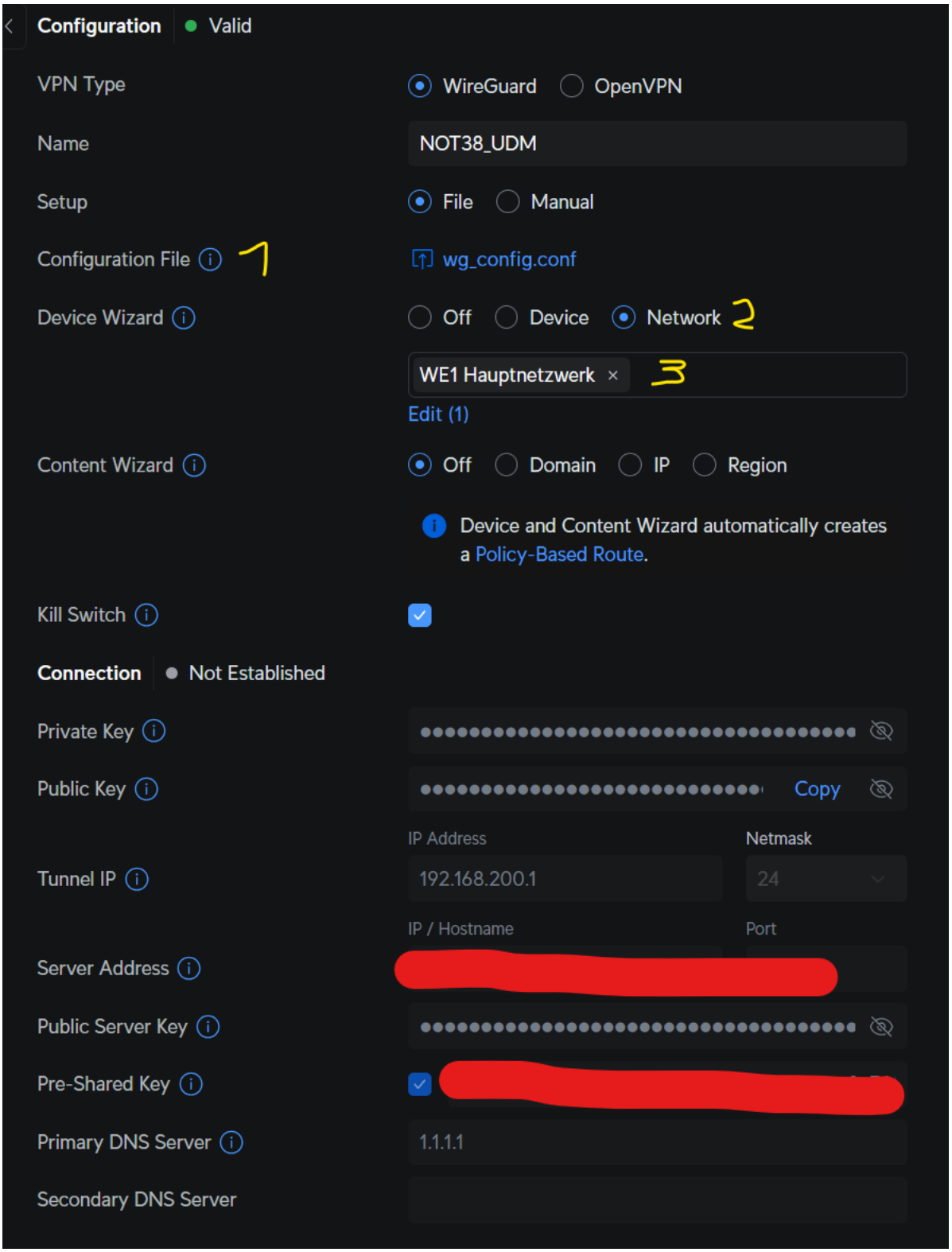
4

Als entferntes Netz wird nun auch das gewünschte Netzwerk zu UDM angezeigt (wichtig für Routing) in der Fritzbox



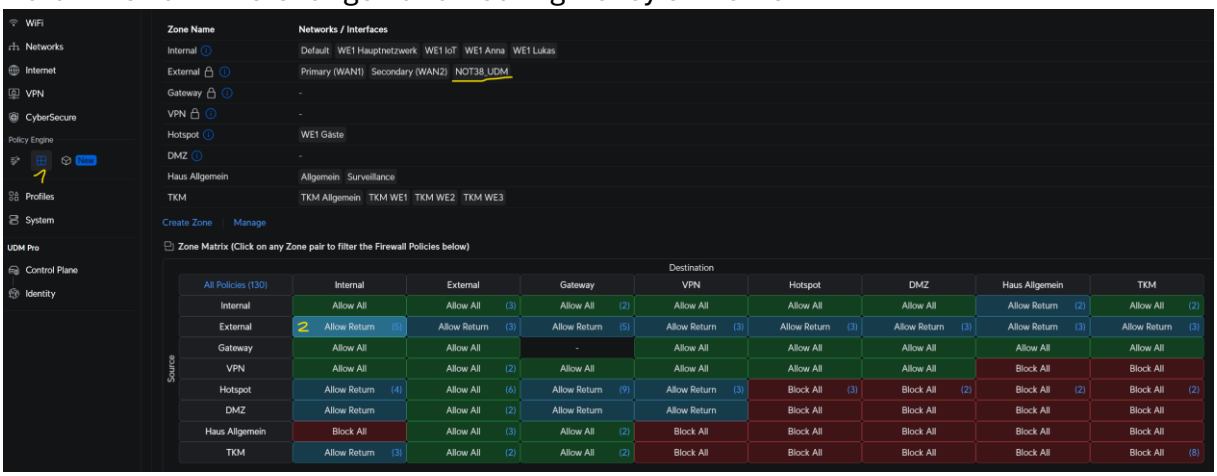
3. VPN-Client in der UDM einrichten

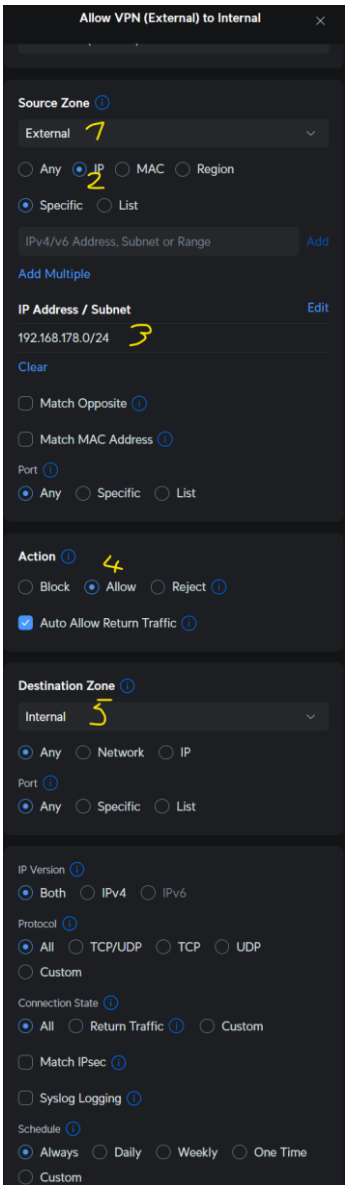


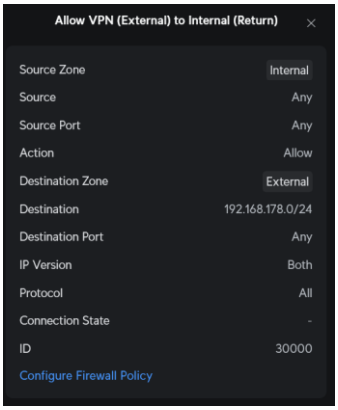

Configuration
Valid
VPN Type
WireGuard
OpenVPN
Name
NOT38_UDM
Setup
File
Manual
Configuration File
wg_config.conf
Device Wizard
Off
Device
Network
WE1 Hauptnetzwerk
Edit (1)
Content Wizard
Off
Domain
IP
Region
Device and Content Wizard automatically creates a Policy-Based Route.
Kill Switch
Connection
Not Established
Private Key
Public Key
Copy
IP Address
Netmask
Tunnel IP
192.168.200.1
24
IP / Hostname
Port
Server Address
Public Server Key
Pre-Shared Key
Primary DNS Server
1.1.1.1
Secondary DNS Server

Apply

VPN-Client wird als in der Zone-Based-Firewall (ZBF) im Bereich „External“ geführt.
Dafür Firewall-Einstellungen und Routing-Policy einrichten.







Diese Routing-Policy hat die UDM beim Erstellen der VPN-Verbindung bereits angelegt.