# VPN über Tor

Um einen VPN-Server mit WireGuard einzurichten, der den ausgehenden Traffic über das Tor-Netzwerk leitet, sind mehrere Schritte erforderlich. Hier ist eine allgemeine Anleitung, wie Sie dies umsetzen können:

### Voraussetzungen
- Ein Server (z. B. ein VPS) mit einem Linux-Betriebssystem (z. B. Ubuntu).
- Grundkenntnisse in der Verwendung der Kommandozeile.
- Root-Zugriff auf den Server.

### Schritt 1: WireGuard installieren

1. **Server aktualisieren**:
   ```bash
   sudo apt update
   sudo apt upgrade
   ```

2. **WireGuard installieren**:
   ```bash
   sudo apt install wireguard
   ```

### Schritt 2: WireGuard konfigurieren

1. **Schlüssel generieren**:
   ```bash
   umask 077
   wg genkey | tee privatekey | wg pubkey > publickey
   ```

2. **WireGuard-Konfigurationsdatei erstellen**:
   Erstellen Sie eine Datei `/etc/wireguard/wg0.conf` und fügen Sie Folgendes hinzu:
   ```ini
   [Interface]
   PrivateKey = <Ihr privater Schlüssel>
   Address = 10.0.0.1/24  # VPN-Subnetz
   ListenPort = 51820

   [Peer]
   PublicKey = <Öffentlicher Schlüssel des Clients>
   AllowedIPs = 10.0.0.2/32  # IP des Clients
   ```

   ```

3. **WireGuard aktivieren**:
   ```bash
   sudo wg-quick up wg0
   ```

### Schritt 3: Tor installieren

1. **Tor installieren**:
   ```bash
   sudo apt install tor
   ```

2. **Tor konfigurieren**:
   Bearbeiten Sie die Tor-Konfigurationsdatei `/etc/tor/torrc` und fügen Sie Folgendes hinzu:
   ```ini
   SocksPort 9050
   ```

3. **Tor-Dienst starten**:
   ```bash
   sudo systemctl start tor
   sudo systemctl enable tor
   ```

### Schritt 4: Traffic über Tor leiten

1. **IP-Forwarding aktivieren**:
   Bearbeiten Sie die Datei `/etc/sysctl.conf` und stellen Sie sicher, dass die folgende Zeile nicht auskommentiert ist:
   ```ini
   net.ipv4.ip_forward=1
   ```
   Wenden Sie die Änderungen an:
   ```bash
   sudo sysctl -p
   ```

2. **iptables-Regeln hinzufügen**:
   Fügen Sie die folgenden iptables-Regeln hinzu, um den Traffic über Tor zu leiten:
   ```bash
   sudo iptables -t nat -A POSTROUTING -o tor0 -j MASQUERADE
   sudo iptables -A FORWARD -i wg0 -o tor0 -j ACCEPT
   sudo iptables -A FORWARD -i tor0 -o wg0 -m state --state ESTABLISHED,RELATED -j ACCEPT
   ```
   ```

3. **Routing für WireGuard konfigurieren**:
   Bearbeiten Sie die WireGuard-Konfigurationsdatei `/etc/wireguard/wg0.conf` und fügen Sie die folgende Zeile hinzu:
   ```ini
   PostUp = iptables -t nat -A POSTROUTING -o tor0 -j MASQUERADE
   PostDown = iptables -t nat -D POSTROUTING -o tor0 -j MASQUERADE
   ```

### Schritt 5: Client konfigurieren

1. **Client-Schlüssel generieren** (auf dem Client):
   ```bash
   umask 077
   wg genkey | tee privatekey | wg pubkey > publickey
   ```

2. **Client-Konfigurationsdatei erstellen**:
   Erstellen Sie eine Datei (z. B. `wg0-client.conf`) und fügen Sie Folgendes hinzu:
   ```ini
   [Interface]
   PrivateKey = <Ihr privater Schlüssel des Clients>
   Address = 10.0.0.2/24  # IP des Clients

   [Peer]
   PublicKey = <Öffentlicher Schlüssel des Servers>
   Endpoint = <Server-IP>:51820
   AllowedIPs = 0.0.0.0/0  # Leitet gesamten Traffic über den VPN
   ```

3. **Client aktivieren**:
   ```bash
   sudo wg-quick up wg0-client
   ```

### Schritt 6: Testen

- Überprüfen Sie, ob der Client erfolgreich mit dem Server verbunden ist.
- Testen Sie, ob der Traffic über das Tor-Netzwerk geleitet wird, indem Sie eine Website wie `check.torproject.org` besuchen.

###

---

Revision #1
Created 15 May 2025 20:02:53 by Admin
Updated 15 May 2025 20:03:27 by Admin