

Praxisnahe, schrittweise Anleitung, wie du auf einem VPN-Router VPN einrichtest. Es gibt verschiedene Wege, je nach Router-Firmware und VPN-Protokoll. Die wichtigsten Varianten: OpenVPN, WireGuard, IPsec (L2TP/IPsec).

### 1) Vorbereitung – was du brauchst

- Einen Router, der VPN-Unterstützung hat (z. B. Router mit OpenWrt/Duos, Asuswrt-M Merlin, DD-WRT, PfSense oder ein kommerzieller VPN-Router).
- VPN-Abonnement oder eigenen VPN-Server (z. B. OpenVPN- oder WireGuard-Server). Viele VPN-Anbieter liefern Konfig-Dateien, Zertifikate und Anmeldedaten.
- Falls du Router-Firmware wechseln willst: sichere Backups, notiere aktuelle Einstellungen, und beachte Garantie-/Supportfolgen.
- Netzwerkkonzept klären: Soll der komplette Traffic über VPN gehen (Cone), oder nur bestimmte Geräte (Split-Tunneling)?

### 2) Protokoll und Methode auswählen

- OpenVPN: sehr kompatibel, gut sicher, oft als .ovpn-Dateien; funktioniert zuverlässig.
- WireGuard: sehr schnell, einfacher Konfig, aber Unterstützung je nach Router/Zugang möglicherweise weniger integriert.
- IPsec/L2TP: weit verbreitet, oft in Unternehmensumgebungen genutzt, evtl. langsamer oder komplizierter zu konfigurieren.
- Tipp: Wenn dein VPN-Anbieter eine fertige Router-App oder vorgefertigte Firmware-Templates anbietet, nutze diese.

### 3) Firmware/Router vorbereiten

- Falls nötig, Firmware aktualisieren oder auf eine VPN-freundliche Variante flashen (Beispiele: Asuswrt-Merlin, DD-WRT, OpenWrt).
- Backup erstellen: Konfiguration, WLAN-Passwörter, ggf. Router-Login.

### 4) VPN-Serverdaten zusammentragen

- Serveradresse ( hostname oder IP )
- Protokoll (OpenVPN, WireGuard, IPsec)
- Authentifizierung: Benutzernamen/Passwort oder Zertifikate/Schlüssel
- Falls OpenVPN: CA-Zertifikat, Client-Zertifikat/Schlüssel oder eine .ovpn-Datei
- Falls WireGuard: Public/Private Keys, AllowedIPs, Endpoint

- DNS-Einstellungen (manuell oder via VPN-tunneled DNS, z. B. DNS über VPN)

## 5) Router konfigurieren (Beispiele)

### A) OpenVPN (übliches Szenario)

- Öffne das Admin-Interface deines Routers (z. B. 192.168.1.1).
- VPN-/WAN-Einstellungen finden: „VPN Client“, „OpenVPN Client“ oder Ähnliches.
- Importiere die OpenVPN-Konfiguration:
  - .ovpn-Datei hochladen oder CA/Zertifikate separat einfügen.
  - Falls Zertifikate separat: CA, Client-Zertifikat, Client-Schlüssel, ggf. passwortgeschützten Schlüssel.
  - Benutzername/Passwort (falls per Login statt Zertifikat).
- VPN-Verbindung testen: Speichern, verbinden, Status prüfen.
- Optional: Neustart des Routers; prüfen, ob VPN-Verkehr durchgeht (Was läuft über VPN? Browser/IP prüfen).
- DNS: sicherstellen, dass DNS-Anfragen auch VPN-bedingt über VPN gehen (DNS-Leaks vermeiden).
- Split-Tunneling (optional): nur bestimmte Geräte oder Subnetze über VPN leiten.

### B) WireGuard

- Öffne VPN-Client-Einstellungen.
- WireGuard-Konfig importieren (Public/Private Keys, Endpoint, AllowedIPs).
- Verbindung aktivieren und testen.
- Beachte: Manche Router bieten eine einfache GUI für WireGuard-Clients oder verwenden ein eigenes WireGuard-Paket.

### C) IPsec/L2TP

- VPN-Client konfigurieren mit Serveradresse, IPsec-Pre-Shared Key (PSK) oder Zertifikaten.
- Benutzername/Passwort je nach Setup.
- Firewall/regeln prüfen, damit VPN-Verkehr durchkommt.

## 6) Sicherheits- und Funktionalitäts-Optionen

- Kill-Switch (Verbindungsabbruch-Schutz): verhindert Leaks, wenn VPN abbrechen sollte.
- DNS-Sicherheit: nutze VPN-gesteuerten DNS oder DNS über VPN, um Leaks zu vermeiden.
- Split-Tunneling: sinnvoll, wenn nicht alles über VPN gehen soll.
- Automatische Neustarts/Verbindungswiederherstellung: VPN-Verbindung automatisch neu starten, falls Verbindungsabbruch.
- Remote-Management abschalten, Admin-Zugriff per VPN oder stark absichern.

## 7) Test und Validierung

- Prüfe deine IP-Adresse im Browser (z. B. [whatismyipaddress.com](https://whatismyipaddress.com)): sollte die VPN-Server-IP zeigen.
- Prüfe, ob dein echter Standort verborgen ist (optional).
- Teste, ob lokale Geräte weiter erreichbar bleiben (z. B. Drucker, NAS, Smart-Home-Geräte).
- Falls Split-Tunneling genutzt wird, verifiziere, dass nur die gewünschten Geräte/Traffic durchs VPN geht.

## 8) Typische Troubleshooting-Hinweise

- Fehlende Zertifikate oder falsche Pfade: Double-Check Dateiupload und Pfadangaben.
- VPN verbindet sich nicht: Firewall am Router oder ISP blockiert bestimmte Ports; probiere alternatives Protokoll/Ports.
- Langsame Verbindung: WireGuard ist oft schneller; OpenVPN-Parameter (Cipher, MTU) optimieren.
- DNS-Leaks: Stelle sicher, dass DNS-Anfragen über VPN gehen; ggf. nutze DNS über VPN oder setze DNS-Server im Router.

## 9) Praktische Tipps

- Wenn du neu bist, nutze einen Router mit fertigem VPN-Speicher (z. B. Asuswrt-Merlin kompatibel) oder einen VPN-Router des Anbieters.
- Nutze die Unterstützung deines VPN-Anbieters: viele bieten Router-Anleitungen, fertige Konfig-Dateien oder sogar vorkonfigurierte Firmware-Images.
- Dokumentiere deine Konfiguration (Screenshot oder Notizen): nützlich, falls du später wieder ändern musst.

Optionale Beispiel-Kurzleitfaden (OpenVPN auf einem typischen DD-WRT/Asuswrt-Merlin Router)

- Lade die OpenVPN-Dateien deines VPN-Anbieters herunter (CA, Client-Zertifikat, Key) oder eine .ovpn-Datei.
- Öffne Router-Admin-Oberfläche > VPN > OpenVPN Client.
- Wähle „Import“ oder kopiere die Konfigurationsdaten ein.
- Falls Zertifikate separat: Trage CA, Client-Zertifikat, Client-Schlüssel ein.
- Speichere, starte die VPN-Verbindung.
- Prüfe die Verbindung über ein Verbouncer (IP reveal) und teste DNS.
- Stelle DNS-Leaks sicher (Nutze VPN-DNS oder setze DNS-Server auf VPN-Provider).

Wenn du mir sagst, welchen Router du hast (Modell) und welches VPN-Protokoll du bevorzugst (OpenVPN, WireGuard, IPsec) bzw. welchen VPN-Anbieter du nutzt, kann ich dir eine konkrete, schrittweise Anleitung zugeschnitten auf dein Setup geben.