Multiwan

Multi-WAN am VPN-Router bedeutet, dass der VPN-Router zwei (oder mehr) Internet-Verbindungen nutzen kann und du gezielt bestimmst, welcher Traffic über welche Leitung geht. Ob der ISP-Router das unterstützen muss, ist nicht zwingend nötig – aber du musst die Topologie so gestalten, dass dein VPN-Router direkt vom Internet erreichbar ist (oder zumindest die WAN-Schnittstellen sinnvoll nutzen kann).

Wichtige Vorab-Infos

- Multi-WAN ist eine Funktion des VPN-Routers selbst (oder der Firmware), z. B. Router mit OpenWrt/DD-WRT/PfSense, oder spezialisierte Router/Firewalls.

- Typische Topologien:

  - Two-WAN hinter einem Modem/ISP-Gateway: ISP-Gateway → VPN-Router (WAN1, WAN2). Der ISP-Router sollte ideally im Modem-/Bridge-Modus arbeiten, damit der VPN-Router direkt eine öffentliche IP erhält (oder im wenigstens durch Weiterleitung/DMZ arbeiten).

  - Zwei verschiedene Internetquellen (z. B. zwei ISPs oder eine LTE/5G-Beziehung als WAN2).

  - Heimnetz mit Double-NAT: möglich, aber komplizierter (Karten für VPN-Tunnel können Probleme machen).

- Wichtiger Punkt: Wenn dein WAN hinter CG-NAT (Carrier-Grade NAT) hängt, erreichst du meist keinen eigenen öffentlichen IP-Endpunkt. Viele VPN-Tunnel (insbesondere Remote-Zugriffe oder eingehende Verbindungen) funktionieren dann nicht zuverlässig. Bridge/Pass-Through-Modus vom ISP oder ein konkreter IPv4-Public-IP-Zugang ist oft nötig.

Schritt-für-Schritt-Anleitung (allgemein, auf PfSense/OpenWrt/DD-WRT-ähnliche Systeme übertragbar)

1) Ziel definieren

- Entscheid, ob du Failover (Ausfall-Schutz) oder Load-Balancing (Schnellere Nutzung beider Verbindungen) möchtest.

- Leg fest, welcher Traffic über welche WAN-Schnittstelle laufen soll (Policy-Based Routing). Typisch: allgemeiner Internetverkehr über WAN1, VPN-Verkehr über WAN2, oder umgekehrt.

2) Voraussetzungen prüfen

- Mindestens zwei unabhängige Internetverbindungen (WAN1, WAN2) oder eine mehr oder weniger stabile zweite Verbindung (LTE/5G).

- Firmware/Hardware, die Multi-WAN unterstützt (PfSense, OPNsense, OpenWrt/DD-WRT mit Multi-WAN-Paket, oder kommerzielle Router mit Multi-WAN).

- WAN-Schnittstellen funktionsfähig und konfiguriert (IP-Adressvergabe per DHCP, statische IP, oder PPPoE je nach Anbieter).

- Öffentliche IP auf mindestens einer WAN-Schnittstelle (kein reiner CG-NAT). Falls CG-NAT, klär Bridge-Modus oder Modem in Bridge/Pass-Through.

3) Netzwerk-Topologie festlegen

- ISP-Gateway im Forward-Modus oder Bridge-Modus betreiben, damit der VPN-Router die WANs direkt erreichen kann.

- Falls Bridge-Modus nicht möglich, stelle sicher, dass der VPN-Router im DMZ-/Port-Weiterleitungsmodus des ISP-Gateways erreichbar ist (je nach Gerät). Beachte: Double NAT kann Probleme verursachen, besonders für VPN-Tunnels.

4) VPN-Router vorbereiten

- Wähle eine Firmware, die Multi-WAN unterstützt (z. B. PfSense/OPNsense auf passender Hardware, oder OpenWrt/DD-WRT mit Multi-WAN-Packages).

- Lege zwei WAN-Schnittstellen an (WAN1, WAN2) und weise ihnen entsprechende Gateways zu.

- Richte DNS so, dass keine Leaks entstehen (z. B. DNS über VPN oder eigenes DoTDoH).

5) VPN-Tunnel konfigurieren

- Erzeuge je nach Bedarf einen oder zwei VPN-Tunnel (z. B. OpenVPN/IPsec/WireGuard) vom VPN-Router ins VPN-Netzwerk des Providers oder zu einem externen VPN-Anbieter.

- Falls du nur aus dem LAN in das VPN gehen willst, genügt ein Tunnel; für Multi-WAN-Tunneling bleibe flexibel: Traffic kann über WAN1 oder WAN2 gehen, der VPN-Tunnel kann vorn oder nur über WAN1 initiiert werden.

- Falls du eingehende VPN-Verbindungen brauchst, stelle sicher, dass der öffentliche IP-Endpunkt erreichbar ist (Port-Weiterleitung/Firewall-Regeln).

6) Traffic-Regeln und Policy-Based Routing einrichten

- Erstelle Regeln, die bestimmten Traffic über WAN1 oder WAN2 senden.

  - Beispiel: Alle Alltags-Internetverkehr über WAN1; VPN-Verkehr (Tunnel) über WAN2.

- Lastausgleich: gleiche Verteilung mehrerer Verbindungen, oder gewichtetes Balancing.

- Richte Failover ein: WAN2 wird nur genutzt, wenn WAN1 ausfällt (Health Checks, Dead-Gateway-Detection).

7) Sicherheit und Stabilität

- VPN-Verbindung sollte einen Kill-Switch haben, damit Traffic nicht ungewollt außerhalb des VPNs geht, falls der Tunnel bricht.

- MTU/NAT-Überlegungen prüfen; Roadwarrior-Verbindungen brauchen manchmal MTU-Anpassungen.

- Regelmäßige Tests: Verbindungszustand, Tunnelstatus, DNS-Löschung.

8) Testen

- Single-Tunnel testen (VPN-Verbindung funktioniert).

- WAN1 vs WAN2 testen: Traffic-Verteilung, Failover-Funktion, Latenz und Durchsatz prüfen.

- DNS-Leaks testen (z. B. über browserbasierte Tools).

- Sicherheitstests (Firewallregeln, Portfreigaben).

9) Troubleshooting-Hinweise

- Wenn der VPN-Tunnel nicht aufgebaut wird, prüfe öffentliche IPs der WAN-Schnittstellen, NAT/Firewall am Router, ggf. Bridge-Modus des ISP-Gateways.

- CG-NAT-Problem: Falls keiner der WANs eine echte öffentliche IP hat, VPN-Tunnel akzeptiert möglicherweise keine eingehenden Verbindungen. Lösung: Bridge-Modus beim ISP, oder Nutzung eines Anbieters mit echter IP, oder VPN-Anbieter mit NAT-Traversal (aber das kann problematisch sein).

- Logs prüfen: VPN-Logs, System-Logs, Firewall-Logs.

Was braucht dein konkreter Fall?

- Welche Hardware/Software nutzt du für den VPN-Router (PfSense, OPNsense, OpenWrt, DD-WRT, oder ein fertiger Router)?

- Welche beiden Internetquellen stehen dir zur Verfügung (z. B. zwei ISPs, oder eine Verbindung plus LTE)?

- Funktioniert der ISP-Gateway im Bridge-Modus oder bleibt dein Router hinter dem Modem?

- Möchtest du nur Failover oder auch Lastverteilung?

Kurzfassung der Empfehlung

- Nutze eine Routerlösung mit Multi-WAN (PfSense/OPNsense oder OpenWrt/DD-WRT mit Multi-WAN-Package) und zwei unabhängigen WANs.

- Stelle sicher, dass du zumindest eine öffentliche IP am WAN hast oder nutze Bridge-/Pass-Through-Modus des ISP-Gateways, um Problemen durch CG-NAT vorzubeugen.

- Richte Policy-Based Routing ein: Traffic du VPN will über WAN2, sonst über WAN1 (oder entsprechend deiner Priorität).

- Teste Failover, Latenz, DNS-Leaks und bring Sicherheitsvorkehrungen wie Kill-Switch, DNS-Abschaltung, etc. in Ordnung.

Wenn du mir konkrete Hardware-Modelle (Router-Modell, Firmware) und deine WAN-Quellen nennst, kann ich dir eine detaillierte Schritt-für-Schritt-Anleitung maßgeschneidert geben.