

Praxisnahe Anleitung, wie man auf einem VPN-Router VLANs einrichtet. Der genaue Ablauf hängt davon ab, welches Router-Betriebssystem du nutzt (z. B. OpenWrt, pfSense, DD-WRT). Ich gebe dir daher zwei gängige Beispiele und danach allgemeine Hinweise.

Allgemeine Grundprinzipien vorweg

- VLAN (802.1Q) trennt Logiknetzwerke auf derselben physischen Hardware.
- Du brauchst: eine Router-/Firewall-Plattform, eine oder mehrere LAN-Ports bzw. der Switch im Router muss VLAN fähig sein, und idealerweise einen Managed-Switch für weitere Ports.
- Plane deine VLAN-IDs (z. B. VLAN 10 für Gäste, VLAN 20 fürs IoT, VLAN 30 fürs Büro). Lege auch IP-Adressbereiche pro VLAN fest (z. B. 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24).
- DHCP und Firewall regeln, welcher Zugriff erlaubt ist. Falls du über VPN-Gateways nur bestimmten VLANs Zugriff geben willst, plane das entsprechend.

A) Öffentliche Schritte (unabhängig vom System)

1) Plane VLAN-IDs und IP-Bereiche

- Beispiel: VLAN 10 (Gäste) 192.168.10.0/24, VLAN 20 (IoT) 192.168.20.0/24, VLAN 30 (Büro) 192.168.30.0/24.

2) Prüfe, welche Ports dein Router/Switch unterstützt

- Unterstützt der Router 802.1Q VLANs auf seinen LAN-Ports? Gibt es einen integrierten Managed Switch?

3) Sichere die aktuelle Konfiguration, notiere vorhandene Einstellungen.

4) Plane Firewall-Regeln pro VLAN und ggf. welche VLANs über VPN erreichbar sein sollen.

5) Nach der Umsetzung: teste von einem Client in jedem VLAN die Erreichbarkeit des Gateways, DHCP, Internetzugang und die Firewall-Regeln.

B) Beispiel 1: OpenWrt

Voraussetzung: OpenWrt läuft, du hast Zugriff über LuCI oder SSH. Du brauchst einen physikalischen Port, der als Trunk genutzt wird (in OpenWrt oft der physische Port, z. B. eth0, mit VLAN-Interfaces wie eth0.10, eth0.20).

1) VLANs definieren

- Öffne LuCI → Network → Interfaces. Prüfe Existing LAN.

- Gehe zu Network → Switch (oder VLAN-Paket je nach Modell).
- Erstelle VLANs auf dem richtigen PHY-Port (z. B. eth0.10, eth0.20, eth0.30). Setze VLAN IDs 10, 20, 30 und markiere die Ports, die getaggt oder untagged sein sollen (für die Ports, die direkt an Geräte gehen, meist Tagged, für den Router-Port untagged).

2) Interfaces anlegen

- Lege neue Interfaces an, z. B. vlan10, vlan20, vlan30, jeweils mit der entsprechenden IP-Subnetzmaske (z. B. 192.168.10.1/24).
- Zugehöriges Protokoll: DHCP server aktivieren, Bereich z. B. 192.168.10.100–200.

3) Firewall/Zonen konfigurieren

- Erstelle drei Firewall-Zonen: VLAN10, VLAN20, VLAN30. Zugeordneten Interfaces zuweisen.
- Richte Basissicherheitsregeln ein (z. B. Internetzugang erlaubt, inter-VLAN-Verkehr nur falls gewünscht, VLAN 10 darf evtl. nicht auf VLAN 20 zuzugreifen).
- Falls der Router selbst als VPN-Gateway dient, definiere, welche VLANs über VPN routen sollen.

4) DHCP, DNS, ggf. VPN

- DHCP-Prozesse pro VLAN aktivieren; Reserve- oder feste IPs für wichtige Geräte.
- Wenn du VPN-Tunnel (z. B. WireGuard/OpenVPN) benutzt, bestimme, ob bestimmte VLANs über VPN gehen sollen oder nicht.

5) Ports zuordnen

- Ordne je VLAN die Ports des Routers zu (z. B. LAN-Port als Tag/Untag für die jeweiligen VLANs, Uplink zu Modem oder Switch entsprechend konfigurieren).

6) Apply/Tests

- Apply die Änderungen, starte bei Bedarf Dienste neu.
- Teste von Clients in VLAN 10, 20, 30: IP erhalten, Gateway erreichbar, Internetzugang, Firewall-Regeln greifen.

C) Beispiel 2: pfSense

Voraussetzung: pfSense auf Hardware/Router oder VM.

1) VLANs auf dem physischen Interface erstellen

- Interfaces → Other Types → VLANs
- Neues VLAN-Interface: Parent ist dein WAN- oder LAN-Interface (meist LAN). VLAN-Tag 10, 20, 30.

2) VLAN-Interfaces zuweisen

- Interfaces → Assignments: Die neu erstellten VLANs als Interfaces hinzufügen (z. B. OPT1, OPT2, OPT3 oder klare Namen VLAN10, VLAN20, VLAN30).

3) IP- und DHCP-Konfiguration

- Jeder VLAN-Interface eine IP-Adresse geben (z. B. 192.168.10.1/24, 192.168.20.1/24, 192.168.30.1/24).
- DHCP Server auf jedem VLAN aktivieren, passenden Adressbereich definieren.

4) Firewall-Regeln

- Neue Firewall-Zonen erstellen (VLAN10, VLAN20, VLAN30) und Interfaces zuweisen.
- Standardregeln festlegen (z. B. Internet frei zugänglich, inter-VLAN-Verkehr je nach Bedarf erlaubt/gesperrt).

5) VPN-bezogene Einstellungen

- Falls VPN-Tunnel (OpenVPN/WireGuard) vorhanden, Richte Routen bzw. Regeln so ein, dass nur gewünschte VLANs über VPN gehen.

6) Ports konfigurieren

- Falls du einen Trunk auf dem physischen Interface nutzt, stelle sicher, dass der Switch Port VLANs taggt. Auf pfSense ist das meist am Interface-Plan nicht direkt sichtbar; der physische Port muss entsprechend als Trunk konfiguriert sein.

7) Apply/Tests

- Apply alle Änderungen, Router neu starten, Tests pro VLAN (DHCP, Gateway, Internet, Inter-VLAN-Zugriffe, VPN-Verbindung).

D) Allgemeine Tipps und Fallunterscheidungen

- Wenn dein Router kein integriertes VLAN-Switching unterstützt, brauchst du einen Managed Switch zwischen Router und Geräten, um VLAN-Ports sinnvoll aufzuteilen.
- Wenn du mehrere WLAN-Schnittstellen nutzt, kannst du auch VLANs über WLAN implementieren (z. B. Guest-VLAN auf separater SSID). Das ist je nach Router-Modell unterschiedlich konfigurierbar.
- Sicherheit zuerst: Trage klare Regeln ein, wer mit wem kommunizieren darf. Standard ist, VLANs voneinander zu isolieren und nur notwendige Verbindungen zu erlauben.
- Prüfe VLAN-Tagging auf allen betroffenen Ports (sowohl am Router als auch am Switch). Ein falsches Tagging kann komplette Verbindungsprobleme verursachen.
- Erstelle sinnvolle Namenskonventionen, z. B. VLAN10_Gäste, VLAN20_IoT, VLAN30_Büro, damit es wartbar bleibt.