

[zurück](#)

VPN-Sicherheit - IPSec, WireGuard, OpenVPN, Risiken & Best Practices

Ein VPN (Virtual Private Network) baut einen geschützten, verschlüsselten Tunnel zwischen zwei Punkten auf - z. B. Home → Firma oder Endgerät → Server.

Diese Seite erklärt:

- Unterschiede der VPN-Protokolle
- Sicherheitsrisiken
- Firewallregeln
- Split-Tunneling
- Best Practices für sicheres VPN-Design

1. Warum VPN?

VPNs schützen Daten vor:

- Mitlesen (Public WLAN)
- Manipulation
- Geobasiertem Traffic-Abgriff
- Angriffen durch Provider oder öffentliche Netzwerke

Sie ermöglichen:

- sicheren Zugriff auf interne Systeme
- entfernte Administration
- Standortvernetzung (Site-to-Site)
- Zero-Trust-Konzepte

2. Protokolle im Vergleich

WireGuard (modern, schnell, sicher)

Eigenschaften:

- basiert auf modernen Kryptoverfahren (Curve25519, ChaCha20)
- minimaler Code → weniger Angriffsfläche
- extrem schnell, sehr stabil

- einfache Konfiguration (Public/Private Key)
- UDP-basiert (Standard: 51820/udp)

Sicherheit:

- state-of-the-art
 - kaum Angriffsfläche
 - empfohlen für neue Setups
-

OpenVPN (weit verbreitet, flexibel)

Eigenschaften:

- TLS-basiert
- läuft über TCP oder UDP
- viele Optionen → flexibel, aber komplexer
- gut für Firmen und komplexe Umgebungen

Sicherheit:

- stark, wenn richtig konfiguriert
 - komplex = Fehleranfällig
 - gute Protokollreife
-

IPSec (klassisch, oft in Firmen & Routern)

Eigenschaften:

- sehr robust
- Standard in Firewalls, Routern, Gateways
- ideal für Standortvernetzung

Sicherheit:

- hoch, aber schwerer zu konfigurieren
- benötigt oft besondere Firewallregeln
- alte Implementierungen können Schwachstellen haben

ASCII-Vergleich:

```
WireGuard → modern, leicht
OpenVPN   → bewährt, flexibel
IPSec     → sehr robust, komplex
```

3. Risiken bei VPNs

VPN ist *kein* Freifahrtschein für Sicherheit.

Typische Gefahren:

a) Kompromittierte Endgeräte

Wenn das Gerät infiziert ist, hilft keine Verschlüsselung.

b) Split-Tunneling

Nur interner Traffic geht durch den Tunnel, der Rest direkt ins Internet.

Risiko:

- Angreifer kann durch lokales Netzwerk ins VPN springen
- besonders gefährlich bei Home-Office

c) Falsche Firewallregeln

Beispiele:

- VPN-Clients können sich gegenseitig sehen
- ungewollter Zugriff auf Server
- IPv6-Traffic nicht gefiltert
- kein DNS-Filter aktiv

d) Schwache Authentifizierung

- nur Passwort ohne MFA
- geteilte VPN-Keys
- altes TLS (OpenVPN)

e) Unsichere Protokolle

- PPTP (veraltet, unsicher → nicht nutzen!)
-

4. Firewallregeln - sicherer Betrieb

Für WireGuard

- nur UDP 51820 öffnen
- kein Verkehr zwischen Clients (Client-Isolation)
- Regeln pro Peer definieren („AllowedIPs“)
- Logging aktivieren

Für OpenVPN

- Port 1194/udp (oder TCP für Fallback)
 - * restriktives Client-to-Client-Routing
 - * TLS \geq 1.2
 - * keine schwachen Cipher-Suites

Für IPsec

- ESP-Protokoll erlauben
 - * UDP 500 & 4500 öffnen
 - * NAT-Traversal beachten
-

5. Split-Tunneling - Ja oder Nein?

Split-Tunnel: AN

Nur Firmenverkehr durch VPN.

Vorteile:

- weniger Last auf VPN-Server
 - * schnelleres Internet

Nachteile:

- UNSICHERER: parallele Nutzung von zwei Netzen
 - * gefährlich bei infizierten Heimnetzen

Split-Tunnel: AUS (Full Tunnel)

Alles läuft durch VPN.

Vorteile:

- höchste Sicherheit
 - * volle Kontrolle über DNS/Traffic
 - * perfekt für Zero Trust

Nachteile:

- mehr Last auf VPN-Gateway

Empfehlung: → privat egal,

→ beruflich (Unternehmen) **kein Split-Tunnel.**

6. Starke Authentifizierung

Empfohlen:

- MFA (z. B. FIDO2)
- individuelle Benutzerzertifikate
- starke Schlüssel (RSA 4096, ECC bevorzugt)
- kurze Schlüssel-Lebensdauer
- Passphrase für Private Keys
- kein Sharing von Keys

7. Logging & Monitoring

Überwachen:

- Verbindungsversuche
 - fehlgeschlagene Logins
 - * ungewöhnliche Geo-IP
 - * Geräte mit altem Client
 - * hohe Datenübertragung (Data Exfiltration)

Tools:

- Grafana → VPN-Statistiken
 - Suricata → VPN-Traffic analysieren
 - * CrowdSec → Angreifer blocken

8. Best Practices für sicheres VPN

- WireGuard bevorzugen
 - kein PPTP
 - * starke Schlüssel, keine schwachen Ciphers
 - * Full-Tunnel für Firmen
 - * kein Client-to-Client Verkehr
 - * Logging aktiv
 - * MFA für Benutzer
 - * kurze Zertifikatsgültigkeit
 - * IPv6 im VPN richtig filtern
 - * DNS im Tunnel erzwingen (kein Leaking)
 - * Updates für Server & Client

Zusammenfassung

- WireGuard = modern & sicher
 - OpenVPN = flexibel & bewährt
 - * IPsec = ideal für Standortvernetzung
 - * Split-Tunneling kann extrem gefährlich sein
 - * Firewalls müssen restriktiv sein
 - * MFA & starke Schlüssel sind Pflicht
 - * Logging & Monitoring unverzichtbar
 - * VPNs schützen nur, wenn Endgeräte sauber sind

From:
<http://wiki.nctl.de/dokuwiki/> - `Veni. Vidi. sudo rm -rf / vici.`

Permanent link:
http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerkdienste:vpn_sicherheit&rev=1764855987

Last update: **04.12.2025 14:46**

