

[zurück](#)

VPN - Grundlagen (IPsec, OpenVPN, WireGuard)

Ein VPN (**V**irtual **P**rivate **N**etwork) stellt eine sichere, verschlüsselte Verbindung über ein unsicheres Netzwerk (z. B. Internet) her.

Daten werden verschlüsselt, authentifiziert und vor Manipulation geschützt.

VPNs verbinden:

- Heim ↔ Firma
- Standort ↔ Standort
- Server ↔ Server
- Mobile Geräte ↔ Unternehmensnetz

Warum VPN?

- verschlüsselte Kommunikation
- Zugriff auf interne Ressourcen
- Schutz im öffentlichen WLAN
- sichere Standortvernetzung
- Grundlage vieler modernen Zero-Trust-Architekturen

Arten von VPN

1. Site-to-Site VPN

Standorte werden dauerhaft verbunden.

Büro A ⇌ Internet ⇌ Büro B

2. Remote Access VPN (Client-to-Site)

Einzelne Clients verbinden sich ins Firmennetz.

3 Hauptprotokolle

- **IPsec**
- **OpenVPN**
- **WireGuard**

IPsec - Der Klassiker

IPsec (**IP Security**) ist ein Netzwerkprotokoll auf **Layer 3**.

Verwendet in:

- OPNsense
- pfSense
- Cisco Firewalls
- Unternehmensroutern
- Site-to-Site VPNs

Merkmale

- sehr sicher
- läuft im Kernel
- komplex einzurichten
- ideal für Standortvernetzung
- unterstützt Hardware-Offloading

IPsec Betriebsmodi

Modus	Einsatz
Tunnel Mode	ganze Netze verbinden (Site-to-Site)
Transport Mode	Endpunkte direkt miteinander verbinden

IPsec Bausteine

- **IKEv1 / IKEv2** - Schlüsselaustausch
- **ESP** - Verschlüsselter Datentransport
- **AH** - Authentisierung (selten)
- **PFS** - Perfect Forward Secrecy

IPsec Ports

Protokoll	Port
IKEv2	UDP 500
IPsec ESP	IP-Protokoll 50
NAT-T (NAT Traversal)	UDP 4500

Client — UDP 500 — Key Exchange

Client — ESP (50) — Datenverkehr

Vorteile

- sehr sicher und erprobt
- Standard in Unternehmensnetzen
- extrem gut für Standort-VPNs

Nachteile

- komplex zu konfigurieren
- NAT kann Probleme verursachen
- Debugging schwierig

OpenVPN - Flexibel & weit verbreitet

OpenVPN ist ein **TLS-basiertes VPN**, arbeitet üblicherweise auf **Layer 3**, kann aber auch Layer 2 (TAP) transportieren.

Typisch in privaten & kommerziellen Umgebungen:

- Linux
- Windows
- pfSense/OPNsense
- OpenVPN Access Server

Merkmale

- basiert auf TLS/SSL
- Ports frei wählbar (UDP empfohlen)
- sehr flexibel
- stabil hinter NAT
- viele Auth-Methoden (Passwort, Zertifikat, MFA)

Standard-Ports

- **1194/UDP**

- oder jeder andere Port, z. B. 443/TCP (zum Tarnen als HTTPS)

Client — TLS — OpenVPN-Server — internes Netz

Vorteile

- sehr stabil
- flexibel
- funktioniert fast überall
- gute Logs

Nachteile

- langsamer als WireGuard
 - komplizierter als WG
 - Konfiguration oft umfangreich
-

WireGuard - modern & extrem schnell

WireGuard ist das jüngste VPN-Protokoll und basiert auf modernen Kryptoverfahren.

Merkmale:

- extrem schnell
- extrem einfach
- sehr sicher
- minimaler Code → weniger Angriffsfläche
- Kernelmodul für hohe Performance

Ports

- Standard: **51820/UDP**

WireGuard Prinzip

WireGuard arbeitet wie ein verschlüsselter Peer-to-Peer Tunnel.

Jeder Peer hat:

- privaten Schlüssel
- öffentlichen Schlüssel
- AllowedIPs (der Traffic, der durch den Tunnel geht)

Peer A — WireGuard (UDP) — Peer B

Beispielkonfiguration (Minimal)

Client:

```
[Interface]
PrivateKey = xxx
Address = 10.0.0.2/24

[Peer]
PublicKey = yyy
Endpoint = vpn.example.com:51820
AllowedIPs = 0.0.0.0/0
```

Server:

```
[Interface]
PrivateKey = yyy
Address = 10.0.0.1/24
ListenPort = 51820

[Peer]
PublicKey = xxx
AllowedIPs = 10.0.0.2/32
```

Vorteile

- extrem schnell
- extrem einfach
- leicht zu debuggen
- hohe Sicherheit

Nachteile

- kein integrierter Nutzer-/Zertifikatsmechanismus
- kein Layer-2-Modus
- AllowedIPs müssen sauber gepflegt werden

Vergleich - IPsec vs OpenVPN vs WireGuard

Feature	IPsec	OpenVPN	WireGuard
Geschwindigkeit	gut	mittel	sehr hoch
NAT-Kompatibilität	mittel	sehr gut	sehr gut
Komplexität	hoch	mittel	sehr niedrig
Sicherheit	sehr hoch	hoch	sehr hoch
Geeignet für	Standorte	Remote Access	alles, besonders Mobilgeräte
Ports	UDP 500/4500	1194/UDP	51820/UDP

Wichtige Einsatzszenarien

IPsec:

- Standortvernetzung
- Firewalls (OPNsense, Cisco, FortiGate)
- MPLS-/VPN-Ersatz

OpenVPN:

- Firmen-Remotenzugriff
- Linux-Server
- überall, wo Zertifikate wichtig sind

WireGuard:

- Mobilgeräte
 - kleine bis mittlere Firmen
 - Hochleistungs-VPNs
 - Docker-Hosts / Container-Netzwerke
 - Heimnetzwerke
-

Sicherheit bei VPNs

Pflichtregeln:

- starke Verschlüsselung
- sauberes Schlüsselmanagement
- NAT-Traversal klar konfigurieren
- Firewalls restriktiv halten
- Logging aktiv
- MFA-authentifizierte Zugänge

Zusammenfassung

- VPNs bauen verschlüsselte Tunnel über das Internet
 - IPsec → Klassiker, sehr sicher, aber komplex
 - * OpenVPN → flexibel, stabil, TLS-basiert
 - * WireGuard → modern, extrem schnell, einfach
 - * Remote Access vs Site-to-Site unterscheiden
 - * alle 3 Protokolle haben ihren Platz in modernen Netzen

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&rev=1764775375>

Last update: **03.12.2025 16:22**

