Netzwerk
VPN Verfahren

Ein VPN-Tunnel kann eine Netzwerkverbindung auf Layer 2 (Bridge) oder Layer 3 (Route) aufbauen.
• Bridge: VPN- Clients und LAN sind im selben Netzsegment. Jeder Paketmüll wird auf VPN übertragen.
• Route/Tunneling: virtueller LAN-Adapter legt ein Transfer-Netz an, VPN über Routing-Regeln, Traffic kann auf lokal / VPN aufgetailt werden.

Portforwarding/Routing
Steht der VPN-Router hinter einem anderen Router, so müssen die entsprechenden VPN-Ports auf den VPN-Router geforwarded werden.
Außerdem ist ein Routing im DSL-Router auf das interne Transfernetz des VPN-Routers erforderlich!

Übertragungs-/Verschlüsselungsverfahren

- **IPSec - seit 1993**
  - proprietäre Software, Lizenz pro Client erforderlich
  - Mainmode (berücksichtigt WAN-IP der Gegenseite, sicherer) und AggresiveMode (kann dynam. IP)
  - Verschlüsselung mit PreShare oder Zertifikaten
  - NAT-Probleme können umgangen werden mit IPsec-Passthrough oder IPsec mit NAT-Traversal
  - Breite Geräteunterstützung: Lancom, Lucom, Vigor, Fritzbox (nur IKE v1)
  - Windows OS: NCP-Client (Bintec, Lancom..), native Unterstützung mit Zertifikaten
  - Android OS: native Unterstützung je nach Version und Gerät, teils nur IKE v.1, mit Zertifikat
  - kein einheitlicher, geräteübergreifender Standard zum Austausch der Konfiguration

- Wireguard **- seit 2015**
  - Open Source / GPLv2-Lizenz
  - Client kostenlos und für alle Betriebssysteme verfügbar, seit 2020 direkt im Linuxkernel integriert (also auch embedded Devices)
  - modern, stabil, einfach konfigurierbar, roamingfähig, schlank und schnell (höhere Übertragungsgeschwindigkeit, geringere Latenz)
  - jede Verbindung hat eigene Public- und Private Key und funktioniert ähnlich wie SSH-Keys
  - jeder Public Key wird mit Liste erlaubter Netze verknüpft (Wildcard 0.0.0.0/0 bedeutet: alle Netze gehen durch Tunnel)
    In Versandrichtung verhält sich diese Liste wie eine Routing Tabelle.
    In Empfangsrichtung dient sie als Access Control List.
  - keine Zertifikate erforderlich, Key-Paar kann vom Router oder offline erzeugt werden
  - Server erstellt (je nach Gerät) fertige Conf-Datei oder QR-Code, der einfach

am Client eingebunden wird
- Clients bekommen statische IPs und der Access läßt sich individuell pro Gerät steuern
- Default Port: 51820 (UDP), frei änderbar, problemlos über NAT
- energieeffizient, kaum Daten im Leerlauf, geeignet für Mobilgeräte
- viele Softwarelösungen: pfSense, OpenSense, OpenWRT
- bisher wenig Geräte: Fritzbox ab FW 7.50, Vigor, GL.iNet, MikroTik (ab RouterOS 7)

- **OpenVPN - seit 2002**
  - Open Source Software, Client kostenlos und für alle Betriebssysteme verfügbar
  - Verschlüsselung mit OpenSSL oder embedTLS, (Zertifikat und Preshare)
  - Transport flexibel, wahlweise per UDP oder TCP
  - Default Port: 1194 (UDP)
  - NAT ist kein Problem, weil OpenVPN weder IP-Adresse noch Portnummer authentifiziert
  - einfach konfigurierbar, langsam gegenüber IPSec oder Wireguard
  - erlaubt, dass sich mehrere Clients gleichzeitig mit demselben Zertifikat anmelden. Dann können aber Clients nicht einzeln deaktiviert werden.
  - .ovpn ist ein fast einheitlicher Standard zum Übertragen der Konfiguration auf Clients (enthält die notwendigen "ca.crt", "client01.crt" und "client01.key").
  - verfügbar für alle Betriebssysteme (Debian, Ubuntu, MS Windows, macOS, Android und iOS)
  - Konfiguration lässt sich inclusive Zertifikate exportieren und auf der Gegenstelle importieren (Datei oder QR-Code, geräteabhängig)
  - breite Geräteunterstützung (Lucom, Lancom R&S Firewall, Fritzbox, Vigor, MikroTik, GL.iNet, OpenWRT, DD-WRT)
  Anleitung: https://blog.hartinger.net/openvpn-einrichten-bei-einer-lancom-unified-firewall/

- **SSL**
  - Verschlüsselung mit TLS und SSL, gute Verschlüsselungsstärke
  - nutzt nur Port 443 und funktioniert praktisch überall, kompatibel zu NAT
  - geringer Konfigurations- und Wartungsaufwand
  - kein Tunneling, ausschließlich für RemoteAccessVPN geeignet
  - normaler Browser dient üblicherweise als VPN-Client (Anwendung muß browserbasierend sein), über PlugIns auch Weiterleitung/Gateway auf andere Dienste möglich
  Geräte: Vigor, Lancom R&S Firewall

- L2TP over IPSec
  - funktioniert auf allen OS mit Boardmitteln
  - funktioniert ohne Zertifikate und ist einfach konfigurierbar
  - die Kombination von L2TP und IPsec hebt die Schwächen beider Protokolle

gegenseitig auf
Geräte: MikroTik, Vigor

- PPTP (veraltet)
  - unsichere oder keine Verschlüsselung
  - stabil, einfach, früher weit verbreitet

Eindeutige ID: #1414
Verfasser: Uwe Kernchen
Letzte Änderung: 2023-03-25 12:06