**VPN - Virtual Private Network**

Privates Netzwerk über öffentliches Netz aufbauen

* Zugriff auf Netzexterne Ressourcen
* Sichere Kommunizieren bzw. Datenaustausch

**Sicherstellen:**

* Authentizität: Identifizierung von Nutzer und Überprüfung ob Daten von autorisierter Quelle
* Vertraulichkeit: Verschlüsselung der Daten
* Integrität: Daten dürfen nicht von Dritten verändert werden

Tunnel wird aufgebaut

**VPN-Typen:**

* End-to-Site-VPN
  + Szenario: Heimarbeitsplätze oder Außendienststellen mit Unternehmen verbinden
    - Verbindung zu Remote-Netzwerk herstellen
    - möglichst geringer, technischer und finanzieller Aufwand
  + 2 Komponenten notwendig:
    - NAS (Network Access Server) oder RAS (Remote Access Sever)
      * Übernimmt Authentifizierung
    - VPN-Client Software
* Site-to-Site-VPN
  + Szenario: Mehrere Netzwerke von Filialen zu einem virtuellen Netzwerk verbinden
  + Medium:
    - Über angemietete Standleitung (hohe Kosten)
    - Über Internet-Verbindung (deutlich billiger)
  + 2 Arten:
    - Intranet VPN (Geschwindigkeit wichtig, Grundsätzliches Vertrauen)
    - Extranet VPN (Sicherheit wichtig)
* End-to-End-VPN
  + Verbindung zwischen Clients (beidseitig VPN-Software nötig)
  + Anwendung: Remote-Desktop (fehlenden Verschlüsselung RDP und VNC)

**VPN-Server**

* Teil der Verschlüsselten Verbindung (Tunnel)
  + VPN Software
* Pakete werden über Server verschickt und verpackt
* Client isoliert von äußerem Netz (nur Server kennt ihn)

**VPN-Protokolle**

* Secure Socket Layer (Application Layer)
  + Verbindung über Browser aufgebaut (Keine Extrasoftware nötig)
    - Authentifizierung und SSL- Verschlüsselung
* [IPsec](http://www.elektronik-kompendium.de/sites/net/0906191.htm) (Vermittlungsschicht)
  + Bietet sichere, verschlüsselte Kommunikation
  + IP über Internet ist unsicher > IPsec
    - Daten kommen an den richtigen Empfänger durch:
      * Verschlüsselung (Session Secret Key)
      * Datensignierung (Sichere Quelle)
* [Point to Point Tunneling Protocol](http://www.elektronik-kompendium.de/sites/net/0906141.htm) (Sicherheitsschicht)
  + Einfachstes VPN-Protokoll (Schwache Verschlüsselung)
  + Sehr kompartibel (außer Mac OSX und IOS)
  + Verwendet TCP (zuverlässig)
* [Layer 2 Tunneling Protocoll over IPsec](http://www.elektronik-kompendium.de/sites/net/1410061.htm) (Sicherheitsschicht)
  + Langsamer als PPTP, aber sicherer
  + Verwendet UDP > schneller (unzuverlässiger als PPTP)
* Open VPN (Sicherheitsschicht)
  + (Client = Browser, HTTPS, Alternative zu IPsec, Erleichterte Handhabung)
  + TCP oder UDP
  + Verschlüsselung und Authentifizierung