VPN – Virtual Private Network

Definition

Ein geschlossenes, logisches Netzwerk zur sicheren Übertragung von Daten über ein öffentlich zugängliches Netz.

Tunneling

- Verpacken der Anwenderdaten (= payload), z.B. ppp in Daten des Transportprotokolls, z.B. IP.
- Anwenden von Sicherheitsmechanismen
  - Verschlüsselung, z.B. RC4, DE5, 3DES, AES
  - Authentifizierung, z.B. Benutzername und Passwort, Zertifikate
  - Hashwerte
  - Digitalsignatur

Vorteile:

- sicherer Zugriff auf lokale Ressourcen über das Internet
- hohe Flexibilität
- niedrige Kosten für die Übertragung

Einsatzgebiete:

- Side to End – VPN (Standort – Rechner), z.B. Heimarbeitsplatz
- Side to Side – PN (Standort – Standort)
- End to End – VPN (Rechner – Rechner)

Unterschiede zwischen PPTP und L2TP

- PPTP:
  - Authentifizierung auf Benutzerebene (Benutzername + Passwort)
  - Verschlüsselung mit RC4 (40, 56 oder 128 Bit-Schlüssel) → Unsicher
  - Verschlüsselung erst nach dem Verbindungsaufbau
- L2TP:
  - Authentifizierung
    - Benutzer mit CHAP, MS-CHAP
    - Computer mit Zertifikaten
  - kein eigener Verschlüsselungsalgorithmus
    - Kombination mit IPSec (z.B. DES, 3DES

Ziele von VPN

- Vertraulichkeit: Informationen / Daten nur für Berechtigte zugänglich
  - technische Umsetzung: Verschlüsselung
- Integrität: Daten vor Manipulation und Verlust schützen
  - Umsetzung: Integritätsprüfwerte, digitale Signatur
- Authentifizierung: Sichere Zuordnung eines Datenpakets zum Absender
  - Umsetzung: Benutzerverwaltung, Zertifikate, Authentifizierungscode