

# Lernzusammenfassung

## VPN

**Virtual Private Network** beschreibt ursprünglich eine Technik, die es erlaubt, von jedem Ort auf der Welt sicher auf Ressourcen in privaten Netzwerk zuzugreifen. VPN verschlüsselt Ihre Internetverbindung beginnend von Ihrer Netzwerkkarte bis hin zu einem VPN-Server.

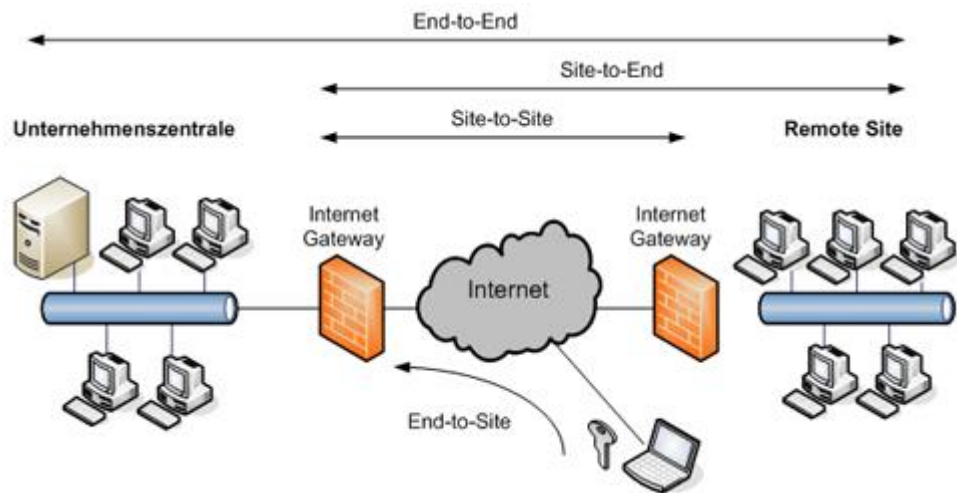
Verbindung kann erfolgen zwischen: VPN-Router, VPN Gateway, VPN-Server, Security Appliance, Firewall, Verbindung zwischen den einzelnen Komponenten, oder Endgeräten

### VPN Arten:

Site-to-Site:

End-to-Site:

End-to-End:

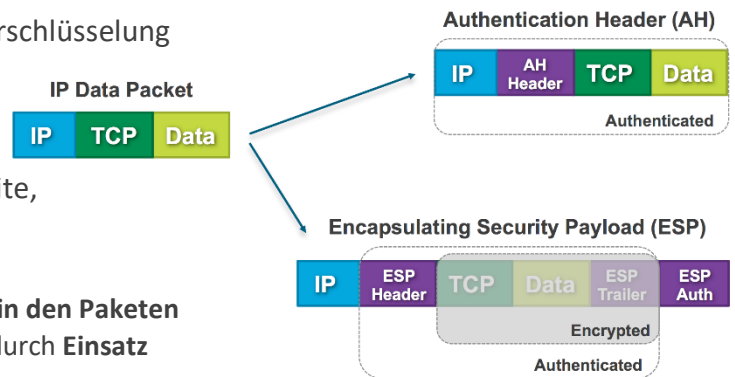


Sicherheitsaspekte:

- Authentizität** – Echtheit der Daten + Versender
- Integrität** – Daten sind unverändert
- Vertraulichkeit** – Daten nicht mitlesen -> Verschlüsselung

Umgesetzt durch:

**Internet Protocol Security (IPsec):** Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll. **Vertraulichkeit, Authentizität und Integrität** wird in den Paketen realisiert (AH), ebenso die **Verschlüsselung** der Daten durch **Einsatz versch. Header (ESP)**.



### Betriebs-Modi:

Im **Transportmodus** verbindet IPsec zwei Endpunkte direkt miteinander (Punkt-zu-Punkt), zum Beispiel über eine auf den Endpunkten installierte Software. Im **Tunnelmodus** hingegen werden zwei IP-Netze miteinander verbunden. Die Endpunkte werden hier von zwei Routern bzw. VPN-Gateways gebildet, zwischen denen der Tunnel aufgebaut wird.

