

---

# Virtual Private Networks

---

## IP VPNs - Fundamentals

---



Harald Greifensteiner  
Technology Consulting

All Rights Reserved



## Inhalt:

- 1. Hintergrund**
- 2. Verwendung von IPsec für VPNs**
  - 2.1. Was ist IPsec?
    - 2.1.1. IPv4 versus IPv6
  - 2.2. Der Aufbau von IPsec
    - 2.2.1. Security Associations
    - 2.2.2. Der Authentication Header
    - 2.2.3. ESP - Encapsulating Security Payload
    - 2.2.4. Eine Frage des Modes
  - 2.3. Key Management
    - 2.3.1. ISAKMP Prozedur und Oakley Mode
    - 2.3.2. Negotiating the SA
  - 2.4. Verwendung von IPsec
    - 2.4.1. Security Gateways
    - 2.4.2. Wild Card SAs
    - 2.4.3. Remote Hosts
    - 2.4.4. Applikationen
  - 2.5. Verbleibende Probleme mit IPsec
- 3. Verwendung von PPTP für VPNs**
  - 3.1. Was ist PPTP?
  - 3.2. Der Aufbau von PPTP
    - 3.2.1. PPP und PPTP
    - 3.2.2. Tunnels
    - 3.2.3. RADIUS
    - 3.2.4. Authentication und Encryption
    - 3.2.5. LAN-to-LAN Tunneling
  - 3.3. Verwendung von PPTP
    - 3.3.1. PPTP Servers
    - 3.3.2. PPTP Client SW
    - 3.3.3. Network Access Servers
    - 3.3.4. Beispielkonfiguration
  - 3.4. Anwendbarkeit von PPTP
- 4. Verwendung von L2TP für VPNs**
  - 4.1. Was ist L2TP?
  - 4.2. Der Aufbau von L2TP
    - 4.2.1. PPP und L2TP
    - 4.2.2. Tunnels
    - 4.2.3. Authentication und Encryption
    - 4.2.4. LAN-to-LAN Tunneling
    - 4.2.5. Key Management
  - 4.3. Verwendung von L2TP
    - 4.3.1. L2TP Network Servers
    - 4.3.2. L2TP Client SW
    - 4.3.3. Network Access Concentrators
    - 4.3.4. Beispielkonfiguration
  - 4.4. Anwendbarkeit von L2TP
- 5. Security Management**
- 6. IP Address Management**
- 7. Performance Management**