8 VPN and IPsec Concepts

8.1 VPN Technology, 8.2 Types of VPNs

VPN Benefits Cost Savings, Security, Scalability, Compatibility

A) Enterprise VPNs (managed by the Enterprise)

A1) Site-to-Site VPNs

VPN-Gateway - IPsec-Tunnel - VPN-Gateway (Cisco Adaptive Security Appliance (ASA))

- IPsec VPN: kompliziertert, sicherer
- GRE over IPsec
  - | IP-Header (Transport) | GRE (Carrier) | IP-Paket (Passenger) |
  - Passenger Protocol: IPv4, IPv6, Routingprotkoll, ...
  - Carrier Protocol: GRE (Generic Routing Encapsulation)
  - Transport Protocol: IPv4, IPv6
- DMVPN (Cisco Dynamic Multipoint Virtual Private Network)
  - DMVPN Hub-to-Spoke Tunnels (Central Site - Branch Sites), Multipoint Generic Routing Encapsulation (mGRE): ein Interface - mehrere Tunnels
  - DMVPN Hub-to-Spoke and Spoke-to-Spoke Tunnels
- VTI (IPsec Virtual Tunnel Interface
  - Virtuelles Interface anstatt static mapping

A2) Remote-Access-VPNs

VPN-Client - Tunnel - VPN-Gateway

- Client-based VPN connection, z.B. Cisco AnyConnect Secure Mobility Client
- Clientless VPN connection, SSL/TLS (z.B.HTTPS, IMAP, POP3), einfach, nur web-basiert (Browser) und Filesharing

B) Service Provider-Managed VPNs

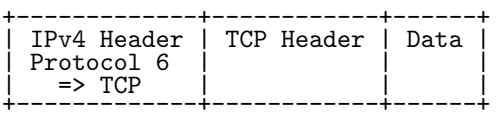
- Layer 2 MPLS: Virtual Private LAN Service (VPLS) ohne Routing
- Layer 3 MPLS: Customer Routes werden redistrubuted vom Provider
- Frame Relay (legacy)
- ATM (legacy)

8.3 IPsec

Security Functions

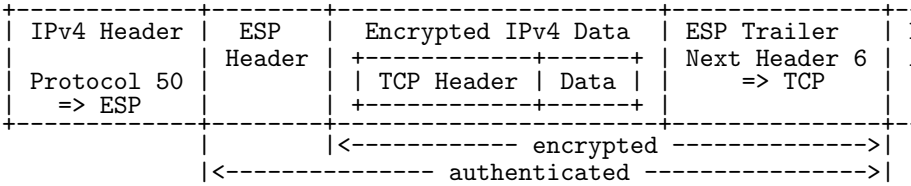
- IPsec Protocol Encapsulation
  - AH (Authentication Header): nur authentication + integrity
  - ESP (Encapsulation Security Protocol): authentication + integrity + confidentiality
  - ESP+AH: funktioniert nicht bei NAT
- Confidentiality: symmetrische Verschlüsselung
  - DES: block-cipher, 56-bit key
  - 3DES: block-cipher, 3x 56-bit-key
  - AES: block-cipher, 128, 192, 256-bit-key
  - SEAL: stream cipher, 160-bit-key
- Integrity: Hash-Algorithmen
  - MD5 (Message-Digest 5): 128-bit hash
  - SHA (Secure Hash Algorithm): 160-bit hash
- Authentication
  - PSK (pre shared key)
  - RSA (Rivest Shamir Adleman): uses certificates
- Diffie-Hellman (DH1, DH2, DH5), DH14, DH15, DH16, DH24 (key-exchange)
  - DH1, DH2, DH5: unsicher!
  - DH14, DH15, DH16: key-size 2048, 3072, 4096 bits, empfohlen bis 2030
  - DH19, DH20, DH21, DH24: key-size 256, 384, 521, 2048 bits, Elliptical Curve Cryptography (ECC)

Original IPv4 Packet



Transport mode

Für Verbindung zweier Computer im LAN



Tunnel mode

Für Verbindung zweier Netze über unsicheres Netz