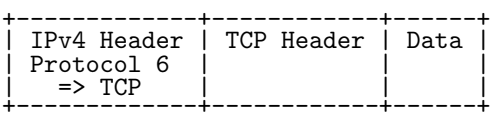
IPsec

Security Functions

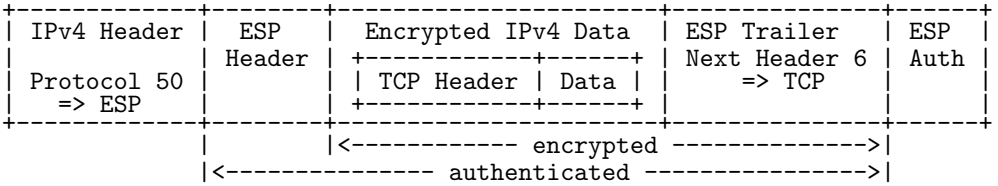
- IPsec Protocol Encapsulation
  - AH (Authentication Header): nur authentication + integrity
  - ESP (Encapsulation Security Protocol): authentication + integrity + confidentiality
  - ESP+AH: funktioniert nicht bei NAT
- Confidentiality: symmetrische Verschlüsselung
  - DES: block-cipher, 56-bit key
  - 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 ein unsicheres Netz