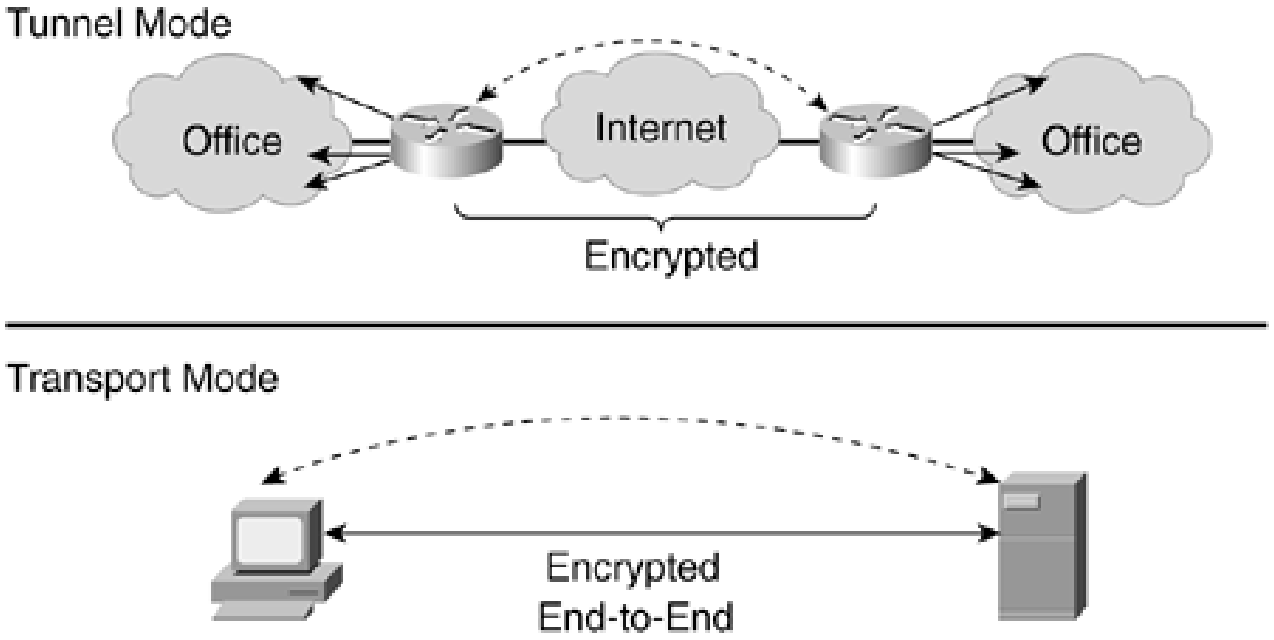
VPN – IPsec & Openvpn

VPN – Virtual Private Network

- Virtuelt privat netværk over åben forbindelse, som internettet
- Bruges af alle
- IP er en connectionless/stateless protokol
- IP understøtter ikke kryptering

IPsec

- Connection-oriented
- Confidentiality
- Data Integrity
- Authentication
- Replay attack prevention



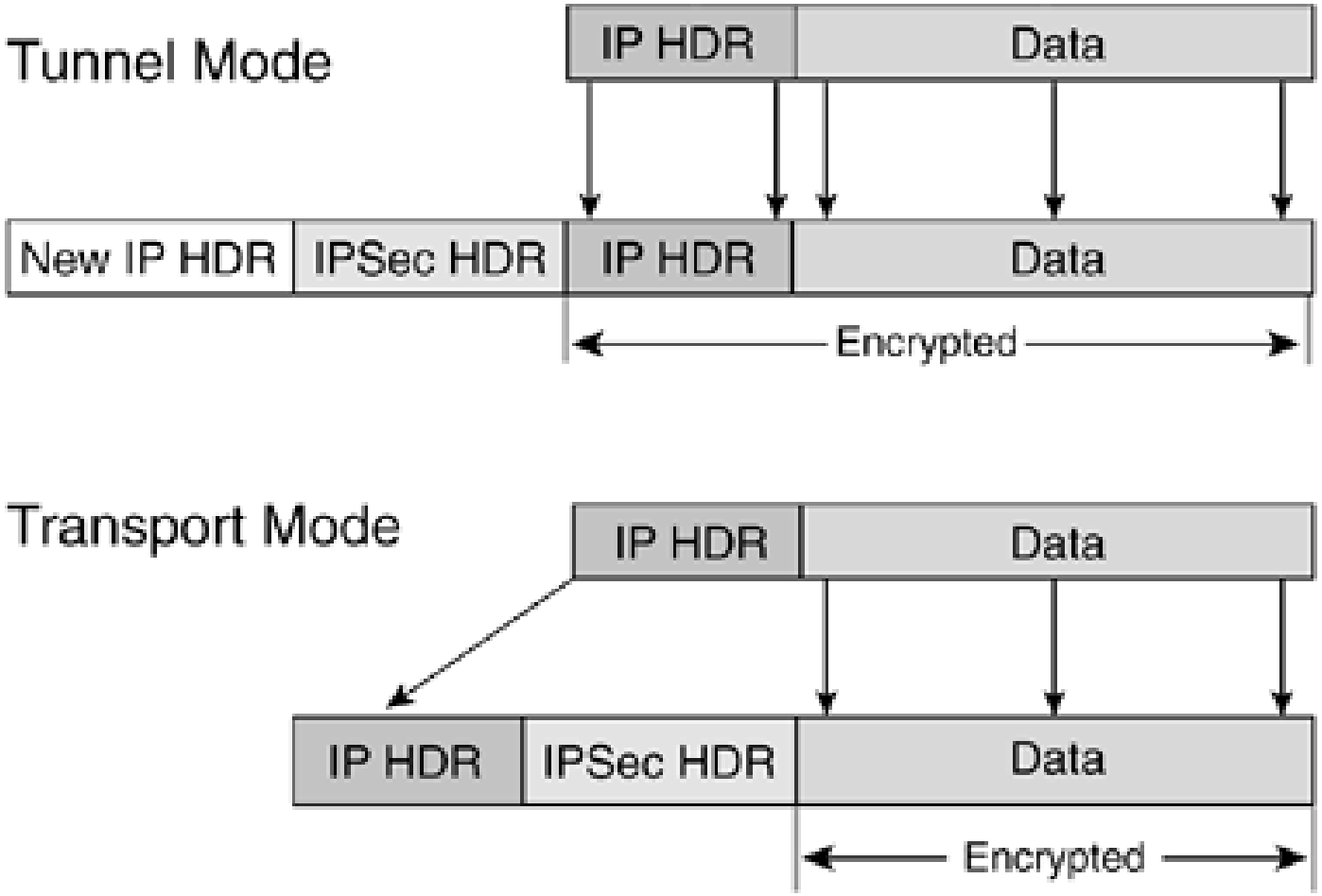
IPsec – Transport mode

- End to end
- Payload Protection

Transport mode med AH	Transport mode med ESP
Tunnel mode med AH	Tunnel mode med ESP

IPsec – Tunnel mode

- Site to site
- PPTP, L2TP & IPsec
- Beskytter hele pakken
- Tilføjer ny IP header



IPsec – IKE: Internet Key Exchange

- Framework for policy og key management forhandlinger
- Internet Security Association and Key Management Protocol (ISAKMP)
- Security Association
- UDP port 500
- 2 faser

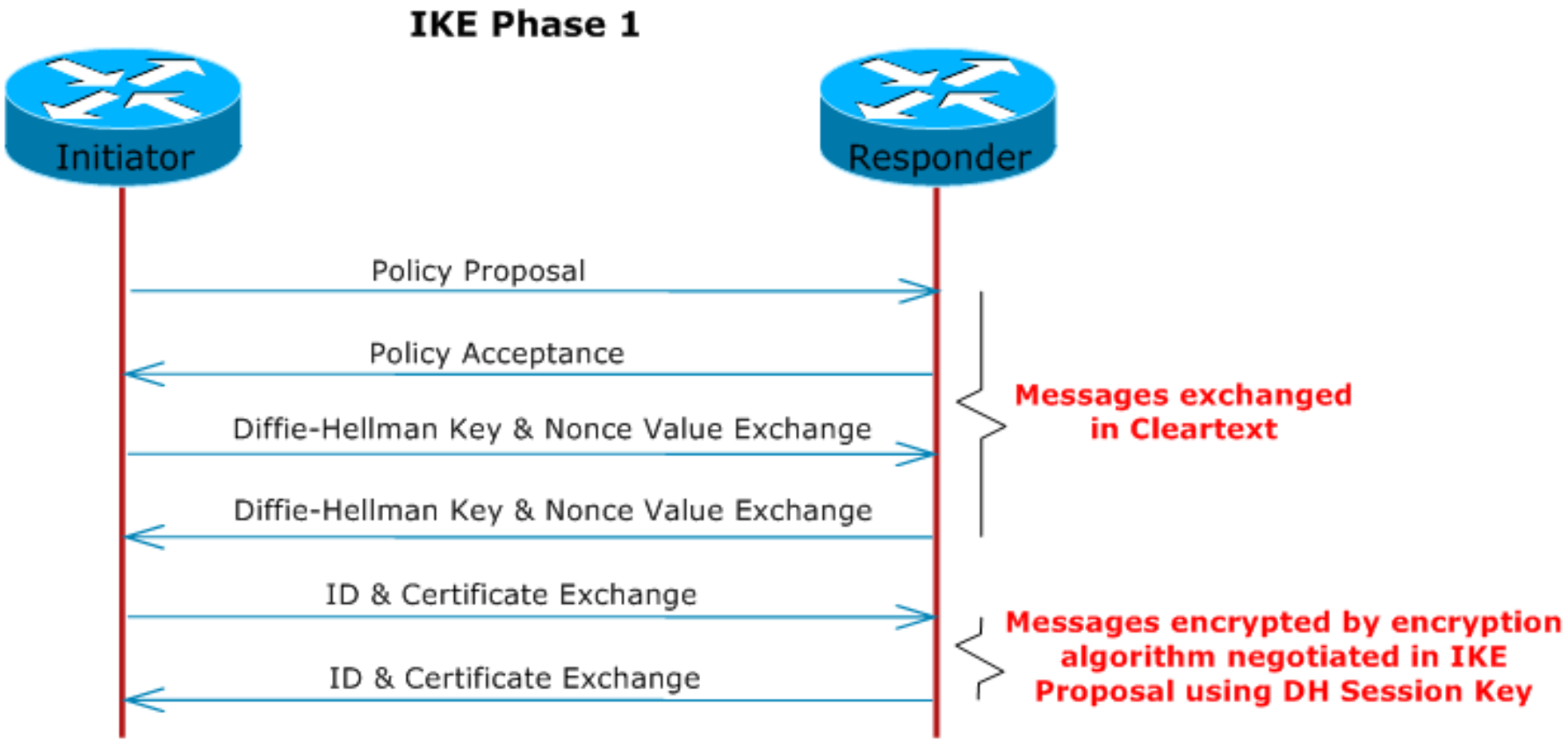
IPsec – IKE: Security Association

- 32-bit SA identifier: Security Parameter Index (SPI)
- Origin SA interface
- Destination SA interface
- Type of encryption used (e.g., 3DES with CBC)
- Encryption key
- Type of integrity check used (e.g., HMAC with MD5)
- Authentication key
- Gemmes i SAD

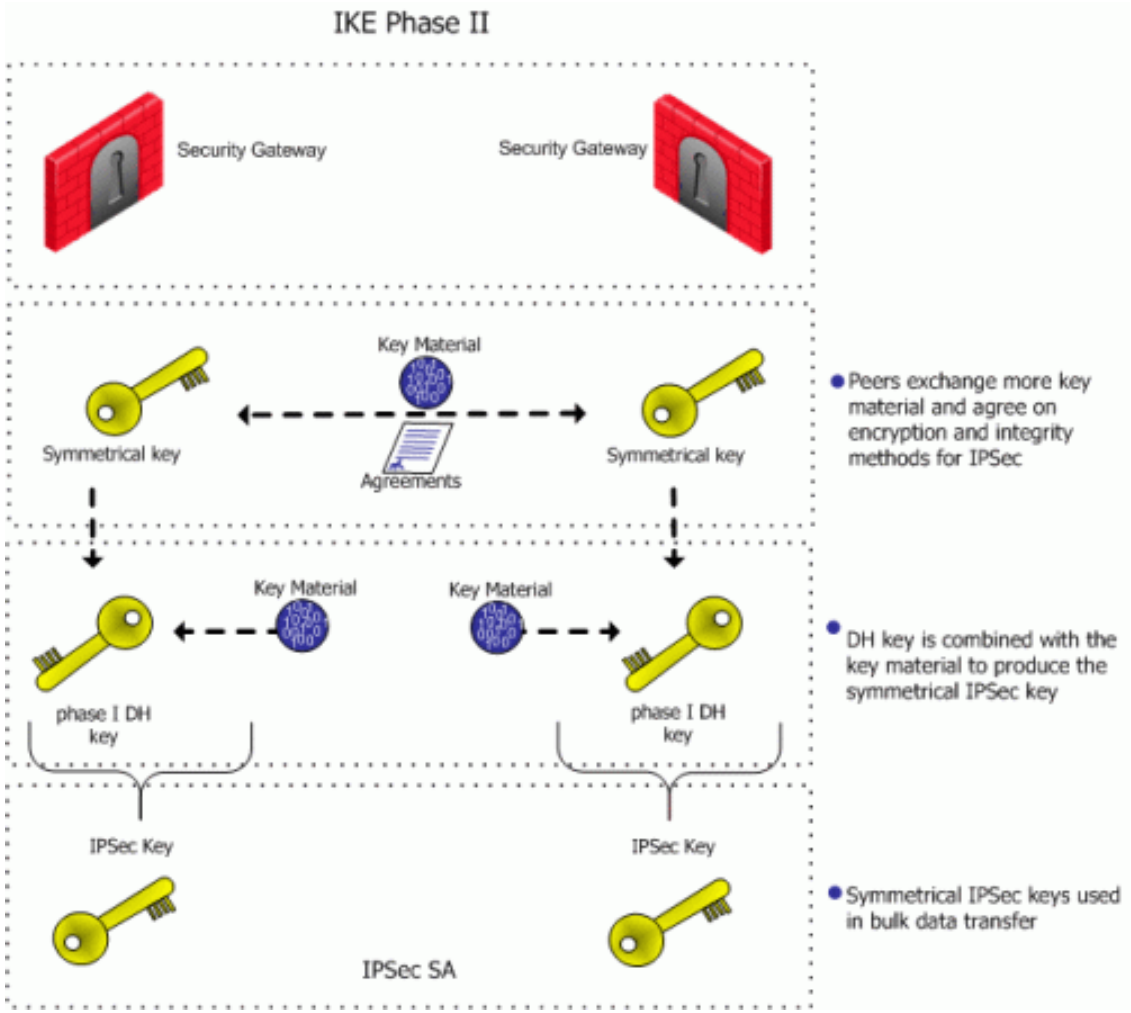
IPsec – IKE: Phase 1

- Encryption Algorithm; DES, AES
- Hash Algorithm; MD5, SHA
- Authentication Method; Pre-shared Private Key
- Key Exchange; Diffie-Hellman
- IKE SA Lifetime
- Bi-directional

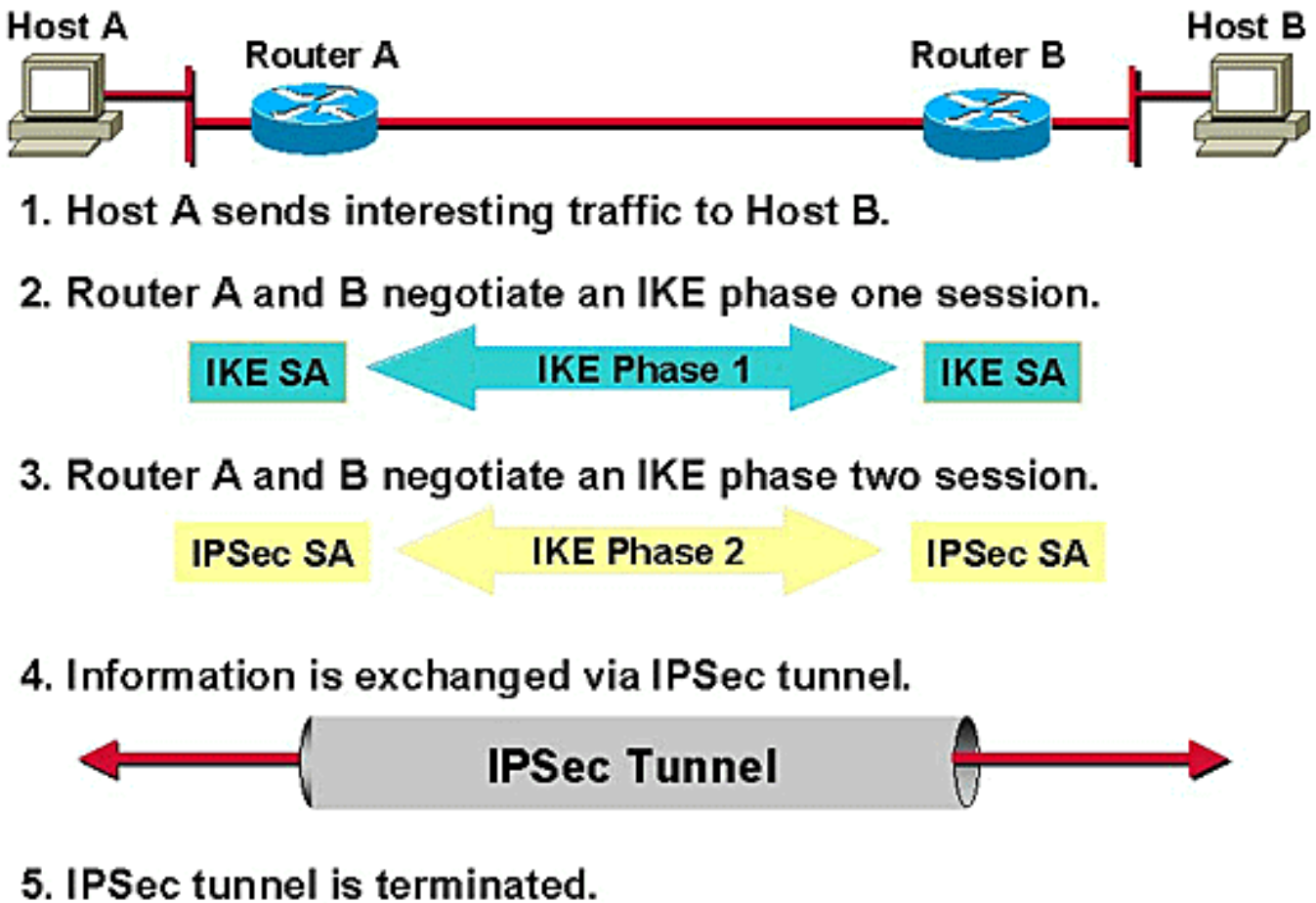
IPsec – IKE: Phase 1



IPsec – IKE: Phase 2

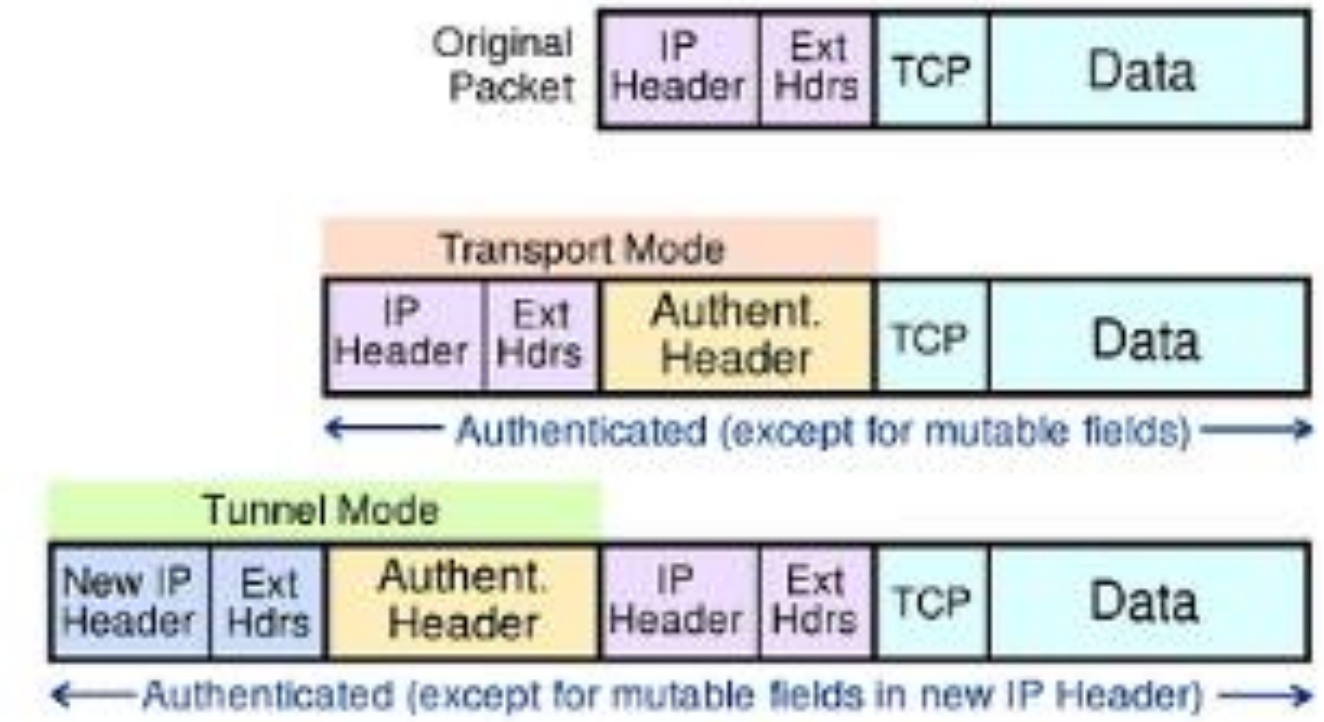


IPsec – IKE: Phase 1 & 2



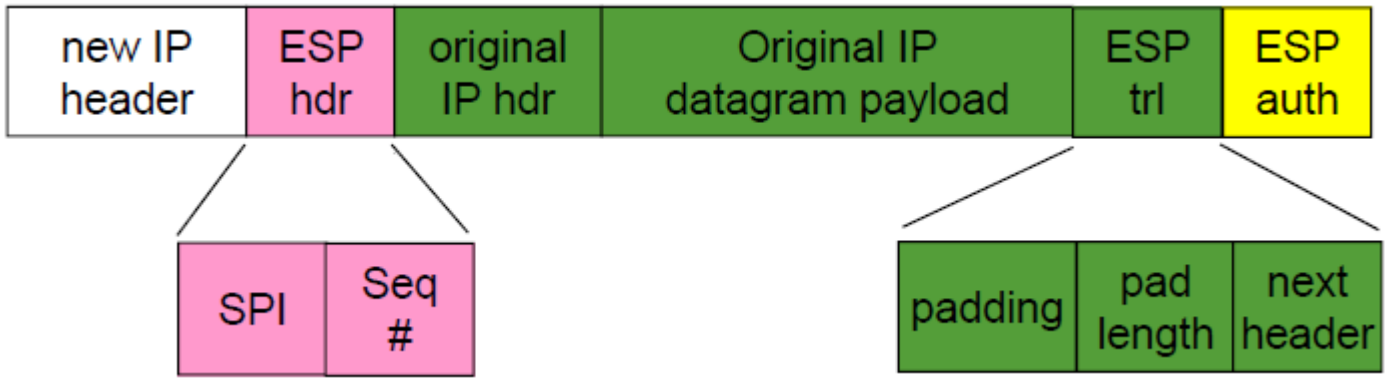
IPsec – AH: Authentication Header

- Integrity check af header
- Understøtter ikke NAT
- Understøtter ikke kryptering
- Ikke så anvendt

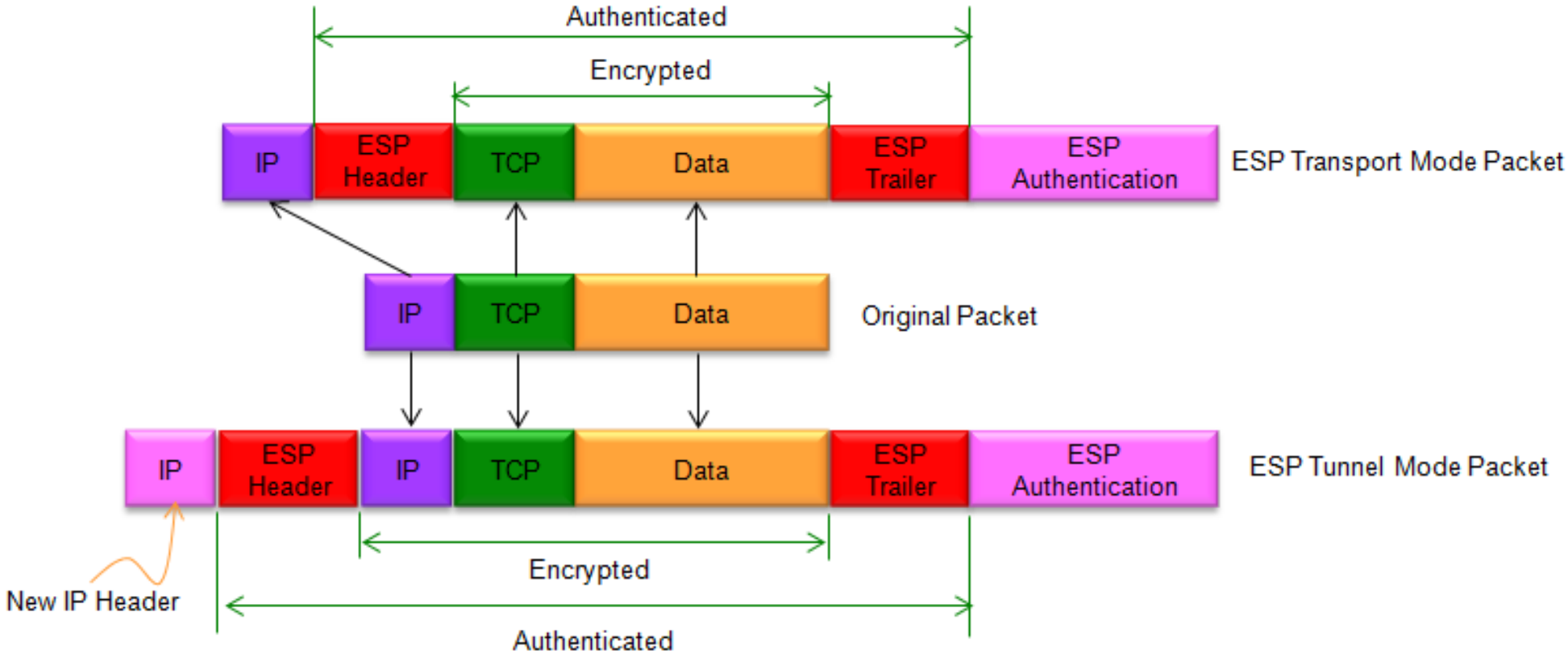


IPsec – ESP: Encapsulation Security Payload

- Understøtter kryptering
- Understøtter NAT
- Intet integrity check af header
- SPI (Replay attack)
- Layer 4 Header
- Kan kombineres med AH
- Mest anvendte



IPsec – ESP: Encapsulation Security Payload



Open vpn

- Open-source VPN software udviklet af James Yonan
- Bruger SSL/TLS til key exchange
- Kompatibel med NAT og firewalls
- Authentication med PSK, certifikater og user/pw login
- Op til 256 bit kryptering
- Bruger OpenSSL krypterings-biblioteket og SSLv3/TLSv1
- Understøtter ikke IKE, IPsec, L2TP og PPTP

Overvejelser

- Kommercielle VPNs er baseret på tillid – stoler bruger på udbyder?
- VPN vs leased line
- Installation og management