# Rechnernetze II

## SoSe 2020

Roland Wismüller
Betriebssysteme / verteilte Systeme
roland.wismueller@uni-siegen.de
Tel.: 0271/740-4050, Büro: H-B 8404

Stand: 29. Mai 2020

# Rechnernetze II

## SoSe 2020

## 5 VPN, IP-Tunnel und IPsec

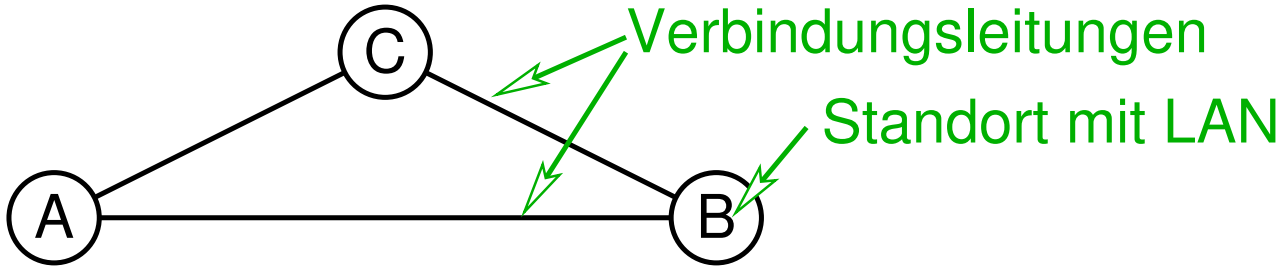
## Inhalt

- Virtuelle Private Netze und IP-Tunnel
- IPsec

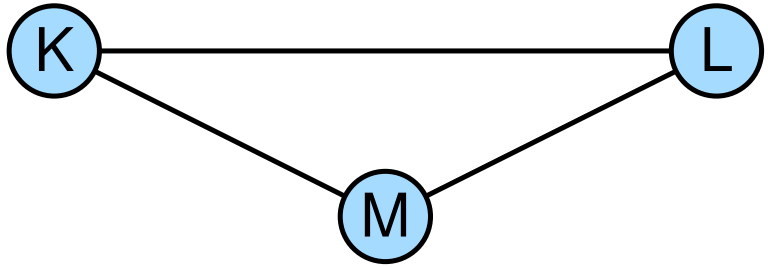
- Tanenbaum, Kap. 5.6.8, 8.6.1
- Peterson, Kap. 4.3.5, 8.3.4
- Kurose/Ross, Kap. 4.7, 7.8
- William Stallings: *Cryptography and Network Security, 3rd Edition*, Prentice Hall, 2003, Kap. 16
- CCNA, Kap. 7

# 5.1 Virtuelle private Netze (VPN) und IP-Tunnel

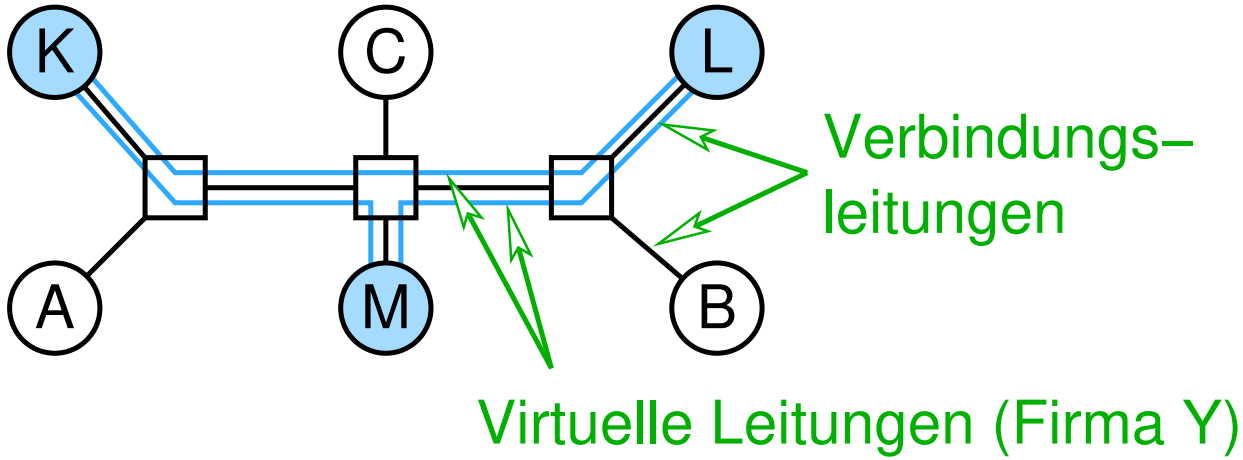
- Zwei private Netzwerke:
  - Firma X:




  - Firma Y:

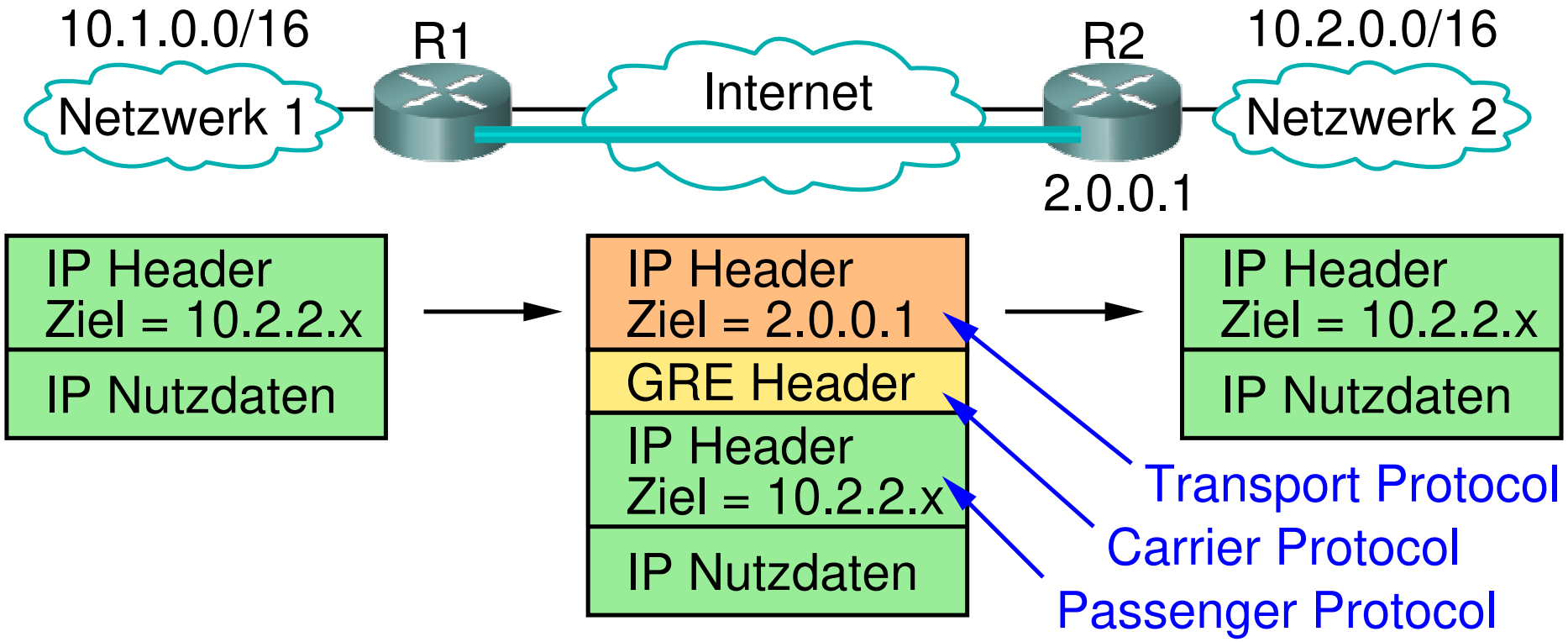



- Zwei VPNs:



# 5.1 Virtuelle private Netze (VPN) und IP-Tunnel ...

- Virtuelle Leitung simuliert eine Layer-2-Verbindung über ein Layer-3-Netz (z.B. Internet)
- Realisierung von virtuellen Leitungen: Tunnel




- Carrier-Protokoll kann ggf. auch fehlen
  - Aufgaben u.a. Multiplexing, Authentifizierung, Reihenfolge, ...

# 5.1 Virtuelle private Netze (VPN) und IP-Tunnel ...

- Einsatz von Tunneln:
  - spezielle Fähigkeiten von R1, R2 (z.B. Multicast)
  - Kopplung von nicht-IP-Netzen über das Internet
  - VPNs: Verschlüsselung und Authentifizierung im Tunnel
- Arten von VPNs
  - *Site-to-site* VPN: verbindet z.B. zwei Standorte
    - statisch
    - VPN für interne Hosts nicht sichtbar
    - Realisierung durch Router (VPN *Gateways*), typ. mit IPsec
  - *Remote-access* VPN
    - externer Client verbindet sich dynamisch mit VPN *Gateway*
    - Lösungen über TLS (eingeschränkt) bzw. IPsec

## Vorbemerkung:
## Welche Schicht sollte Sicherheit implementieren?

- Vermittlungsschicht

- Anwendungsschicht

## Vorbemerkung: Welche Schicht sollte Sicherheit implementieren?

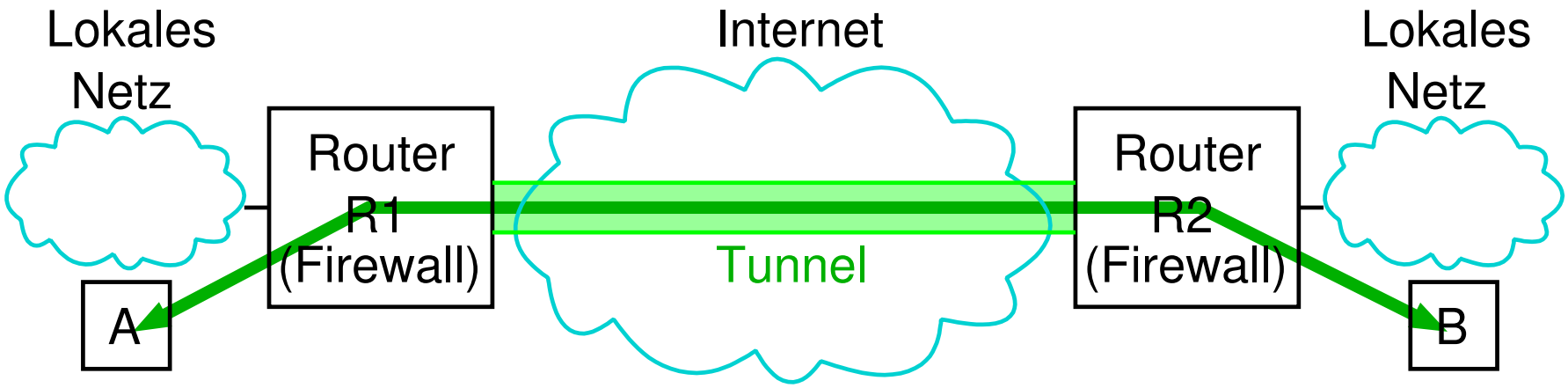
- Vermittlungsschicht
  - \+ Transparent für Anwendungen
  - \+ Sicherheitsvorgaben durch Administrator
  - \+ Erschwert Verkehrsflußanalysen
  - – Muß i.a. vom gesamten Netz unterstützt werden
  - – Abhören zw. Anwendung und Vermittlungsschicht möglich
- Anwendungsschicht
  - \+ Keine Anforderungen an Netzinfrastruktur
  - – Schlüsselverwaltung in Anwendungen problematisch
  - – Keine Sicherung gegen Verkehrsflußanalysen

## Überblick

- Ziel: Sichere Übertragung von IP-Paketen
- Unterstützung optional bei IPv4, vorgeschrieben bei IPv6
- Zwei Sicherheitsprotokolle
  - *Authentication Header* (AH) Protokoll
  - *Encapsulating Security Payload* (ESP) Protokoll
  - Kombination AH + ESP möglich
- Zwei Betriebsarten
  - Transport-Modus: Sicherheit für Protokolle über IP
    - keine Vertraulichkeit des IP-Headers
  - Tunnel-Modus: Sichere Verbindung zwischen zwei Routern

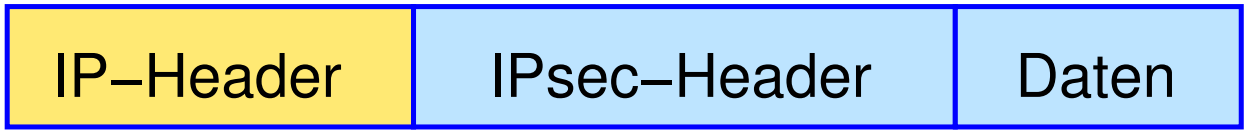
## Tunnel-Modus (mit ESP)

- Ermöglicht die Realisierung sicherer VPNs



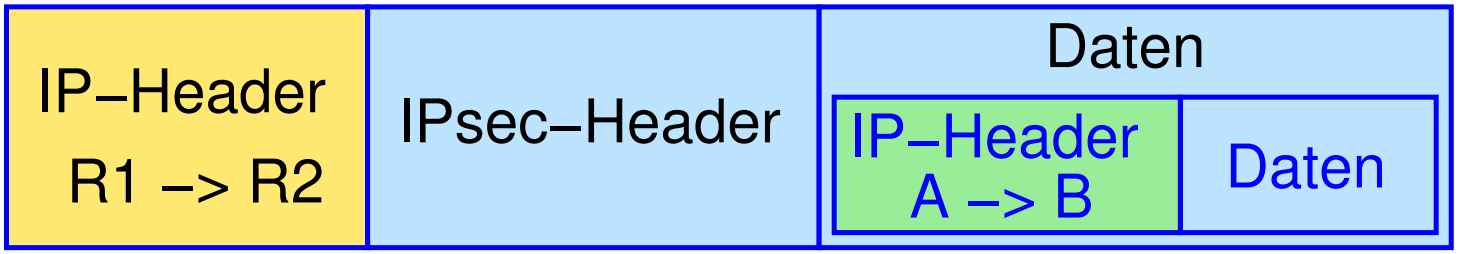

- Im Tunnel: gesamtes IP-Paket verschlüsselt und authentifiziert
  - Daten können nicht gelesen oder verändert werden
  - Quelle und Ziel können nicht ermittelt werden
    - Schutz vor Verkehrsflußanalyse

## Aufbau eines IP-Pakets mit IPsec




- Weiterleiten der Pakete über „normales“ Internet möglich

## Aufbau eines IP-Pakets im Tunnel-Modus von IPsec




- Sicherer Tunnel zwischen Router $R1$ und $R2$
  - Teilnehmer $A$ und $B$ müssen IPsec nicht implementieren

## *Security Association* (SA, RFC 4301)

- Unidirektionale „Verbindung“
- Fasst Parameter für ein Sicherheitsprotokoll (AH oder ESP) zusammen, z.B.:
  - Betriebsart (Transport / Tunnel)
  - kryptographische Parameter
    - Chiffren, Schlüssel, Schlüssel-Lebensdauer, ...
  - aktuelle Paket-Sequenznummer (für Replay-Schutz)
  - Lebensdauer der SA
- SA eindeutig identifiziert durch IP-Adresse des Partners, Sicherheitsprotokoll und *Security Parameter Index* (SPI)
  - mehrere SAs pro Partner möglich

## AH-Protokoll (RFC 4302, 4305, 7321)

- Authentifiziert das gesamte IP-Paket
  - IP-Header und Erweiterungs-Header
    (außer Felder, die sich bei Übertragung ändern)
  - AH-Header (außer Authentifizierungsdatenfeld)
  - Nutzdaten des IP-Pakets
- Aufbau des AH-Headers:

| NextHeader | HeaderLen | Reserviert |
|---|---|---|
| Security Parameter Index (SPI) | | |
| Sequenznummer | | |
| Authentifizierungsdaten variabler Länge ( = HMAC–Wert) | | |

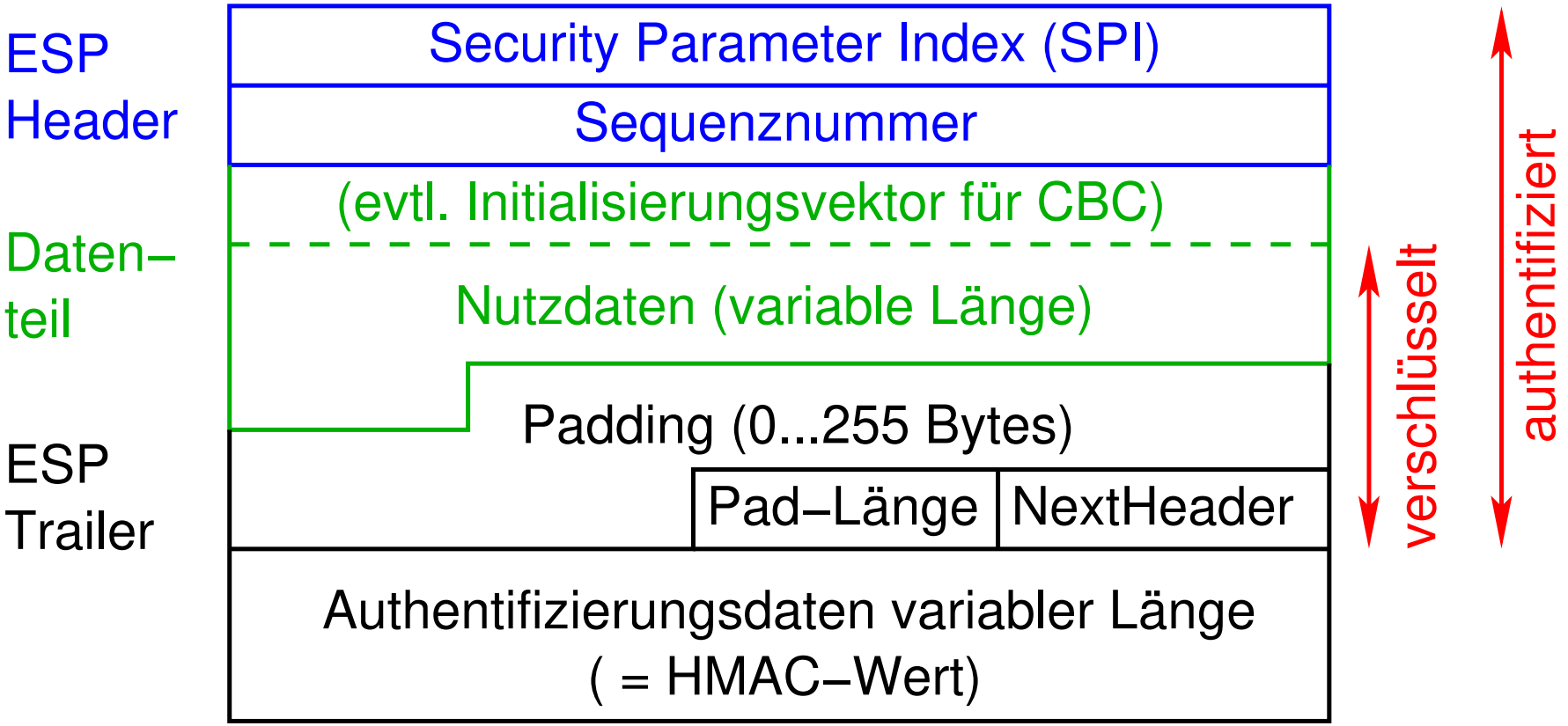
## AH-Protokoll ...

- SPI: zur Idenitifizierung der *Security Association* (SA)
- Sequenznummer dient zur Abwehr von Replay
- HMAC = auf Hashfunktion basierender MAC (*Message Authentication Code*)
  - sichert Authentizität und Integrität
  - $HMAC(M, K) = H(K \oplus \texttt{opad} \parallel H(K \oplus \texttt{ipad} \parallel M))$
    $\texttt{ipad} = \mathbf{0011\ 0110\ ...\ 0011\ 0110_2}$
    $\texttt{opad} = \mathbf{0101\ 1010\ ...\ 0101\ 1010_2}$
- Verschiedene Hashfunktionen möglich
  - jede IPsec-Implementierung muß SHA2-256-128 unterstützen (SHA2 mit 256 Bit Schlüssellänge, Hashwert mit 128 Bit)
  - (derzeit muss auch noch SHA1-96 implementiert werden)

## **ESP-Protokoll** (RFC 4303, 4305, 7321)

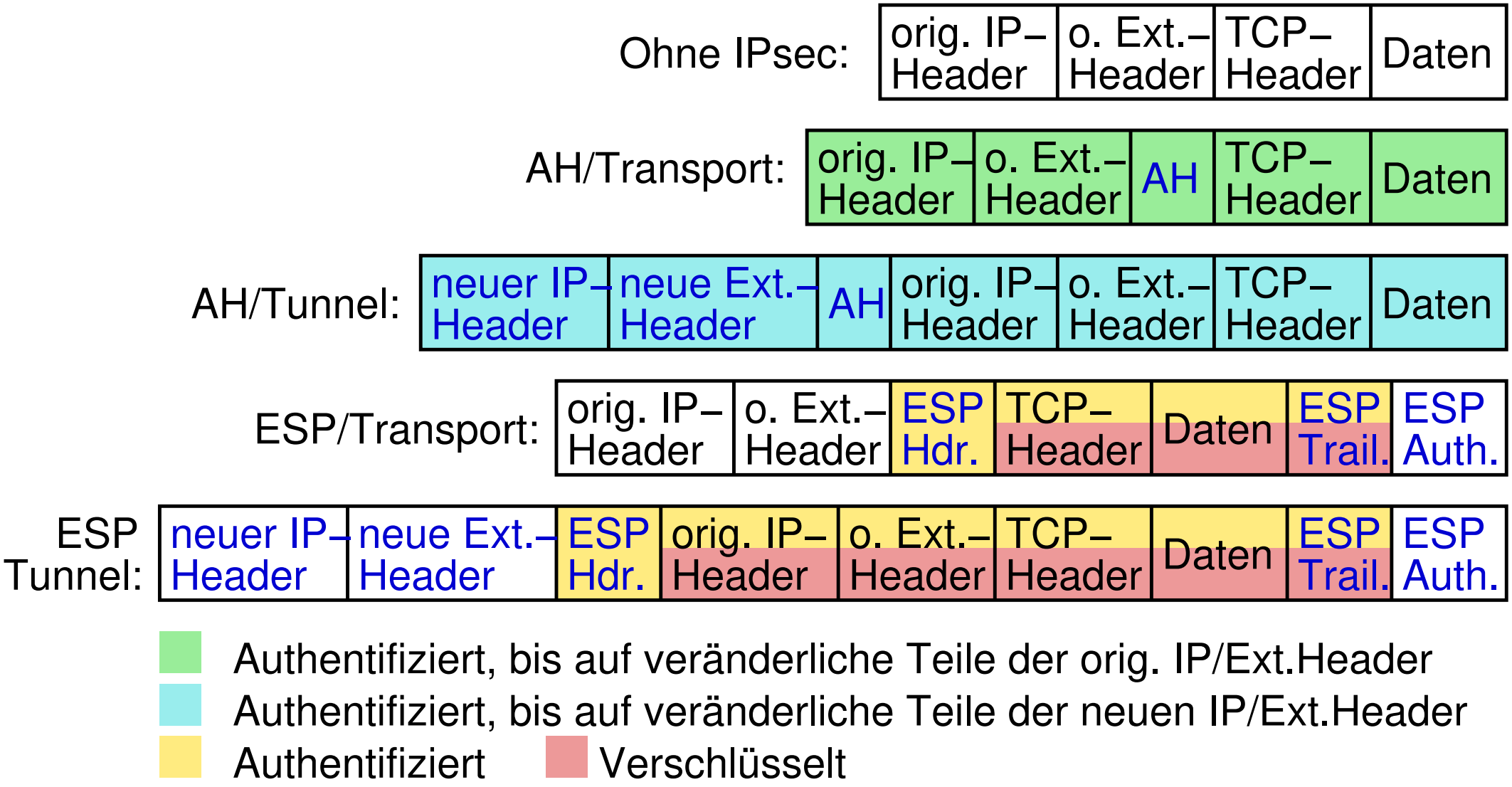
- Verschlüsselung und Authentifizierung des **Datenteils** eines IP-Pakets
  - Authentifizierung ist optional
- Verschiedene Verschlüsselungsverfahren möglich
- Jede IPsec-Implementierung muß unterstützen:
  - AES-CBC und AES-GCM-16 zum Verschlüsseln
    - AES: Blockchiffre, Schlüssellänge 128, 192 oder 256 Bit
    - CBC (*Cipher Block Chaining*): Chiffretexte der einzelnen Datenblöcke hängen voneinander ab
    - GCM (*Galois/Counter Mode*): Verschlüsselung und Integritätssicherung, sehr effizient realisierbar
  - HMAC-SHA2-256-128 u. HMAC-SHA1-96 zur Authentifizierung

## Paketformat beim ESP-Protokoll




➥ Padding wegen Verwendung von Blockchiffren

## Zusammenfassung: Paketformate (mit IPv6)



## Zusammenfassung: Betriebsarten und Protokolle

| Protokoll: | AH | | ESP | |
|---|---|---|---|---|
| Betriebsart: | Transp. | Tunn. | Transp. | Tunn. |
| Verschlüssel. orig. IP-Header | − | − | − | + |
| Authentifiz. orig. IP-Header | + | + | − | (+) |
| Verschlüsselung Nutzdaten | − | − | + | + |
| Authentifizierung Nutzdaten | + | + | (+) | (+) |
| End-to-End Sicherheit | + | − | + | − |

- Kombinationen (Verschachtelung) möglich!
  - z.B. AH im Transport-Modus über ESP Tunnel

## Konfiguration von IPsec: Strategie-Datenbank

- Jeder IPsec-Knoten enthält eine Strategie-Datenbank (*Security Policy Database*, SPD)
- SPD legt für jede ein- und ausgehende Verbindung fest, wie Pakete zu behandeln sind:
  - unverschlüsselte Weiterleitung
  - Verwerfen
  - Anwendung von IPsec
    - Verschlüsselung und/oder Authentifizierung
    - Sicherheits-Parameter (Chiffren, Schlüssellänge / -lebensdauer, Tunnel- / Transportmodus, ...)

    $\Rightarrow$ Nutzung / Erzeugung einer *Security Association* (SA)
- Analog zu Filtertabellen in Firewalls

## Beispieleintrag in Strategie-Datenbank

*src*: 192.168.2.1 - 192.168.2.10
*dest*: 192.168.3.1
*ipsec-action*: *esp* req *cipher* aescbc
*integrity* hmacsha1 *keylen* 128
*expiry* (seconds) 60
transport
*ah* req *integrity* hmacsha2 *keylen* 256
*expiry* (seconds) 60
tunnel

- Verschlüsselung/Authentifizierung der Daten durch ESP im Transport-Modus
- Zusätzlich Authentifizierung des Gesamtpakets durch AH im Tunnel-Modus

## Verbindungsaufbau (Beispiel)

1. Paket soll gesendet werden
2. Nachsehen in Strategie-Datenbank: noch keine SA vorhanden
3. Erzeugen einer oder mehrerer SAs durch *Internet Security Association and Key Management Protocol* (ISAKMP)
   - wechselseitige Authentifizierung mit Schlüsselaustausch
     - *Internet Key Exchange* Protokoll (IKE, RFC 4306)
   - alternativ: *Pre-shared Keys*
   - Aushandeln der Sicherheitsattribute
4. Speichern der SA
   - Löschung nach Ablauf der Lebensdauer
5. Senden des Pakets

## Bewertung

- Keine Verbindlichkeit (digitale Unterschrift)
- Schwierige Konfiguration (Strategie-Datenbank)
- IP ist verbindungsloses Protokoll
  - Integrität zunächst nur für einzelne Pakete garantiert
  - $\Rightarrow$ Zusatzmechanismen (Sequenznr., Anti-Replay-Fenster)
- IPsec erlaubt hostbasierte Schlüsselvergabe
  - selber Schlüssel für alle Verbindungen zw. zwei Rechnern
  - eröffnet Angriffsmöglichkeiten
    - nutze einen Rechner als Entschlüsselungsdienst
- IPsec derzeit v.a. für sichere Tunnels (VPNs) eingesetzt

## VPN

- „Verschlüsselter Tunnel“

## IPsec

- Sicherheit auf der Vermittlungsschicht
- Zwei Protokolle:
  - AH: Authentizität für gesamtes IP-Paket
  - ESP: Authentizität und/oder Vertraulichkeit für Nutzdaten
    - Tunnel-Modus: auch Original-IP-Header verschlüsselt
- Basis für Kommunikation: *Security Association* (SA)
  - unidirektionale Verbindung, legt Sicherheitsparameter fest
  - Erzeugung der SA über ISAKMP / IKE
    - incl. Schlüsselaustausch und Partner-Authentifizierung