



Rechnernetze II

SoSe 2025

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

Stand: 8. April 2025



Rechnernetze II

SoSe 2025

5 VPN, IP-Tunnel und IPsec



Inhalt

- ➔ Überblick
- ➔ Details
- ➔ Konfiguration und Verbindungsaufbau
- ➔ Zusammenfassung
- ➔ 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 Überblick



(Animierte Folie)

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

5.1 Überblick ...



IPsec (Secure IP)

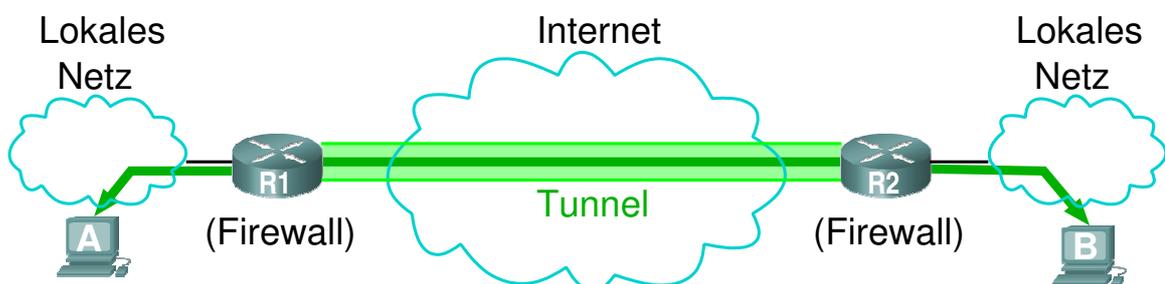
- ➔ Ziel: Sichere Übertragung von IP-Paketen
- ➔ Unterstützung optional bei IPv4, vorgeschrieben bei IPv6
- ➔ Zwei Sicherheitsprotokolle
 - *Authentication Header* (AH) Protokoll
 - *Encapsulating Security Payload* (ESP) Protokoll
 - Kombination AH + ESP möglich
- ➔ Zwei Betriebsarten
 - Transport-Modus: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

5.1 Überblick ...



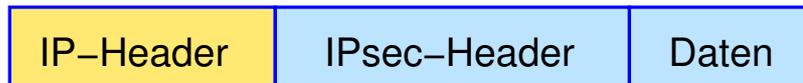
Tunnel-Modus (mit ESP)

- ➔ Ermöglicht die Realisierung sicherer VPNs



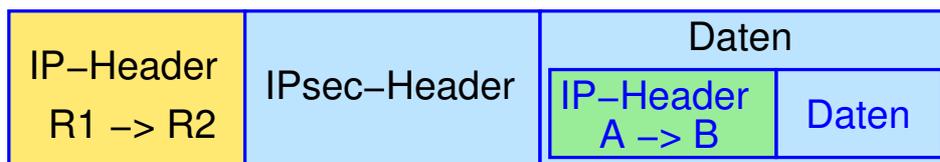
- ➔ Im Tunnel: gesamtes IP-Paket verschlüsselt und authentifiziert
 - Daten können nicht gelesen oder verändert werden
 - Quelle und Ziel können nicht ermittelt werden
 - Schutz vor Verkehrsflußanalyse

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

5.2 Details

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, 8221)

- ➔ 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 Identifizierung der *Security Association* (SA)
- ➔ Sequenznummer dient zur Abwehr von Replay
- ➔ HMAC = auf Hashfunktion basierender MAC (*Message Authentication Code*)
 - sichert Authentizität und Integrität
 - $HMAC(M, K) = H(K \oplus_{\text{opad}} || H(K \oplus_{\text{ipad}} || M))$
ipad = 0011 0110 ... 0011 0110₂
opad = 0101 1010 ... 0101 1010₂
- ➔ 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, 8221)

- ➔ 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

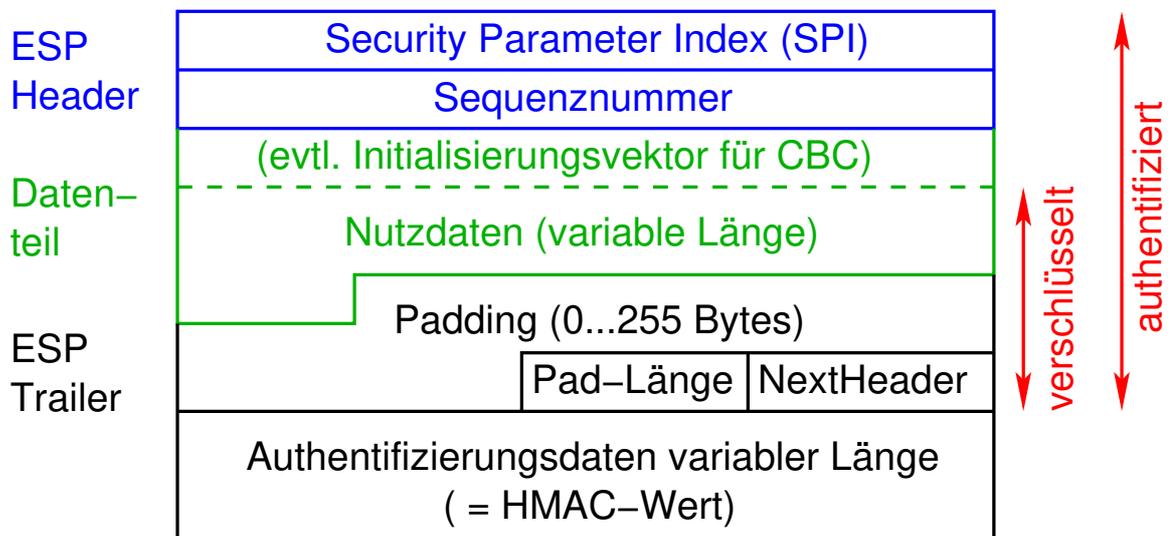
Anmerkungen zu Folie 171:

Beim *Cipher Block Chaining* wird jeder Klartextblock mit dem vorangegangenen Chiffretextblock EXOR verknüpft.

Der *Galois/Counter Mode* arbeitet nach einem ähnlichen Prinzip wie der *Counter Mode*, der bei WPA2 eingesetzt wird.



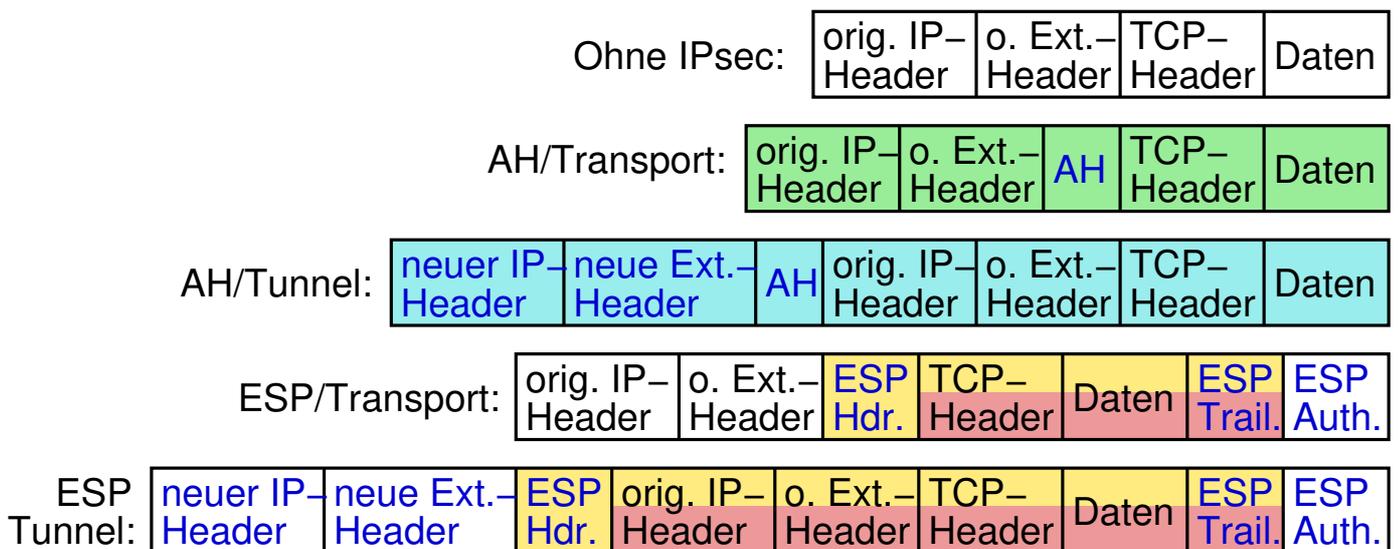
Paketformat beim ESP-Protokoll



➔ Padding wegen Verwendung von Blockchiffren



Zusammenfassung: Paketformate (mit IPv6)



- Authentifiziert, bis auf veränderliche Teile der orig. IP/Ext.Header
- Authentifiziert, bis auf veränderliche Teile der neuen IP/Ext.Header
- Authentifiziert ■ Verschlüsselt

Zusammenfassung: Betriebsarten und Protokolle

Protokoll: Betriebsart:	AH		ESP	
	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 und Verbindungsaufbau



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, ...)
- ⇒ 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

Anmerkungen zu Folie 176:

Das Beispiel auf der Folie soll lediglich andeuten, welche Information in den IPsec-Knoten gespeichert werden muss, soll aber keine konkrete Syntax vorstellen. Eine konkrete Konfiguration für IPsec im Tunnel-Modus auf einem Cisco-Router kann wie folgt aussehen (die zusätzlich notwendige Konfiguration des eigentlichen Tunnels ist ausgelassen):

- ➔ Erstellen einer ACL für die mit IPsec zu übertragenden Pakete:

```
R1(config)# access-list 102 permit ip 10.0.0.0 0.255.255.255
                                         172.16.0.0 0.0.3.255
```

Im Beispiel sind dies alle IP-Pakete von 10.0.0.0/8 nach 172.16.0.0/22.

- ➔ Festlegung einer Policy für Authentifikation und Schlüsselaustausch:

```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key !Secret! address 64.100.13.2
```

Im Beispiel wird ein *Pre-shared Key* verwendet. Zum Schlüsselaustausch wird Diffie-Hellman Gruppe 5 (1536-bit Schlüssel) und AES verwendet.

➔ Konfiguration der IPsec Protokolle:

```
R1(config)# crypto ipsec transform-set MySet esp-aes esp-sha-hmac
```

In diesem Fall wird ESP mit AES-Verschlüsselung und HMAC-SHA1-Authentifizierung verwendet.

➔ Verbindung der ACL mit der IPsec-Konfiguration:

```
R1(config)# crypto map MyMap 2 ipsec-isakmp
R1(config-crypto-map)# set peer 64.100.13.2
R1(config-crypto-map)# set transform-set MySet
R1(config-crypto-map)# match address 102
R1(config-crypto-map)# exit
```

Hier wird die Verbindung zwischen der ACL mit der Nummer 102, der IPsec-Konfiguration „MySet“ und dem Partner-Host 64.100.13.2 hergestellt.

➔ Anwendung der Einstellungen auf eine ausgehende Schnittstelle:

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map MyMap
```

176-2

Konfiguration und Verbindungsaufbau ...



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 7296)
 - ➔ Authentifizierung z.B. über *Pre-shared Key*
 - ➔ Aushandeln der Sicherheitsattribute
4. Speichern der SA
 - ➔ Löschung nach Ablauf der Lebensdauer
5. Senden des Pakets



- ➔ 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



Bewertung

- ➔ Keine Verbindlichkeit (digitale Unterschrift)
- ➔ Schwierige Konfiguration (Strategie-Datenbank)
- ➔ IP ist verbindungsloses Protokoll
 - Integrität zunächst nur für einzelne Pakete garantiert
 - ⇒ 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