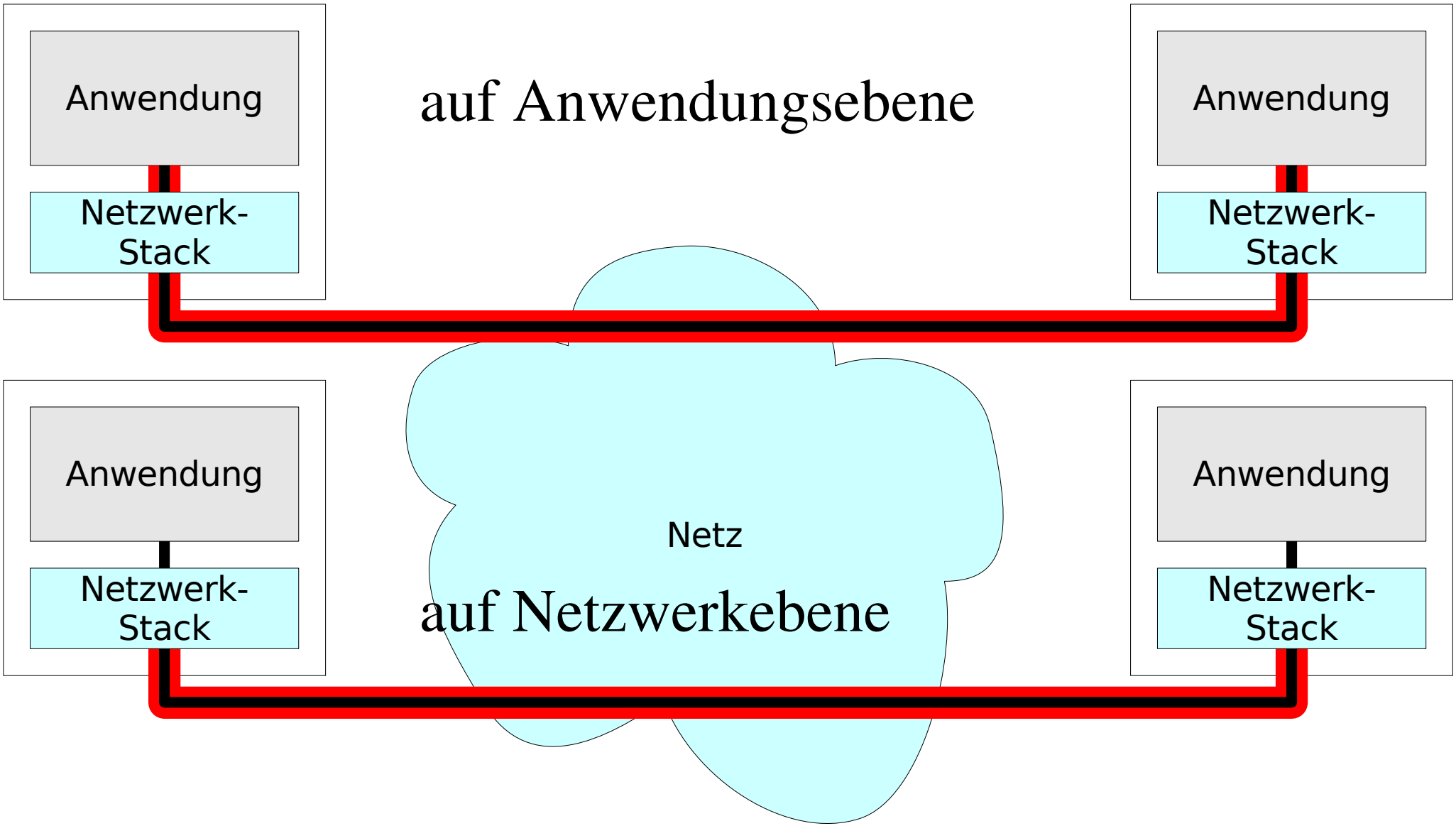
IPSec

- Motivation
- Architektur
- Paketsicherheit
- Sicherheitsrichtlinien
- Schlüsselaustausch

Motivation


Anwendung
Netzwerk-
Stack
auf Anwendungsebene
Anwendung
Netzwerk-
Stack
Anwendung
Netzwerk-
Stack
Netz
auf Netzwerkebene
Anwendung
Netzwerk-
Stack

Motivation

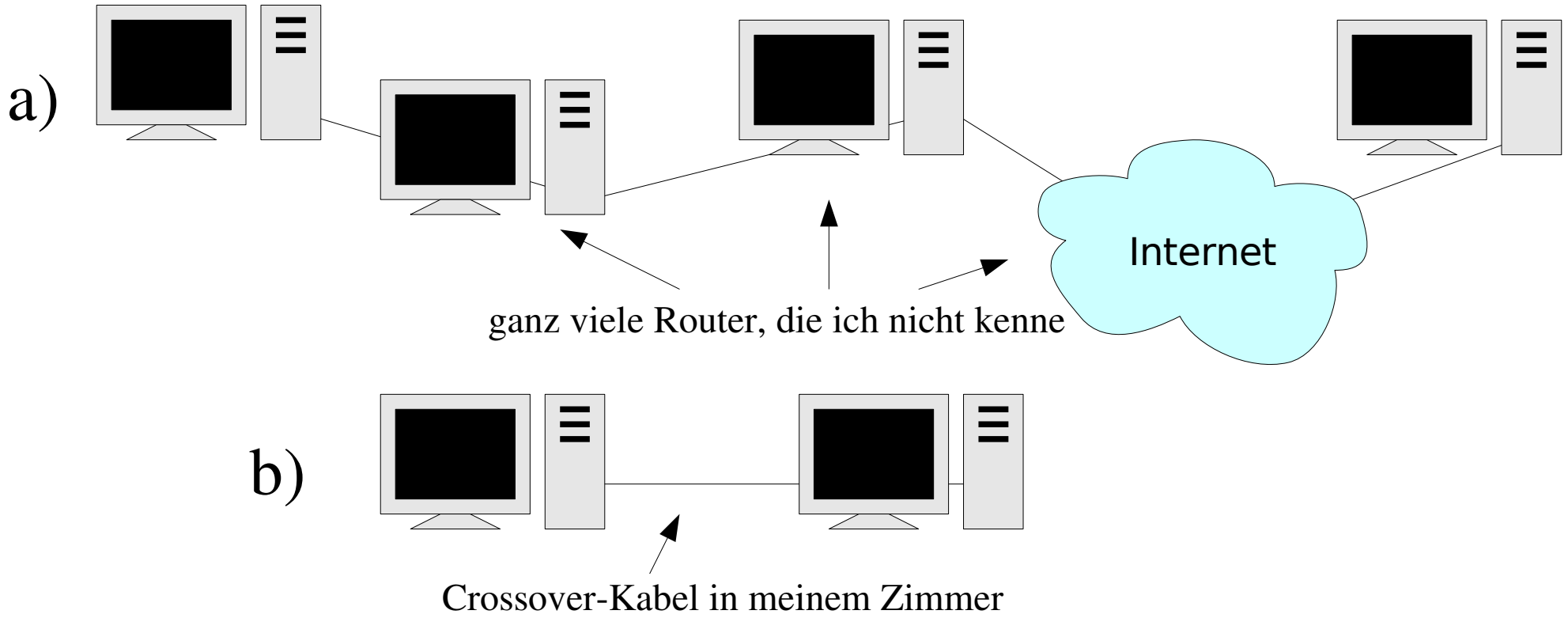
- Sicherheitsmerkmale in Anwendung
  - Netzwerksubsystem einfacher
  - applikationsspezifische Authentisierung, Schlüssel etc.
  - muss Netz als „black box“ betrachten
  - Hardware-Assist schwierig
- Sicherheitsmerkmale in Netzwerksubsystem
  - komplexes Netzwerksubsystem
  - anwendungsunabhängige Sicherheit; ggf. Verhandlung mit Anwendung
  - Hardware-Assist leicht

Motivation

z.B. Anwendung möchte Daten vertraulich übertragen

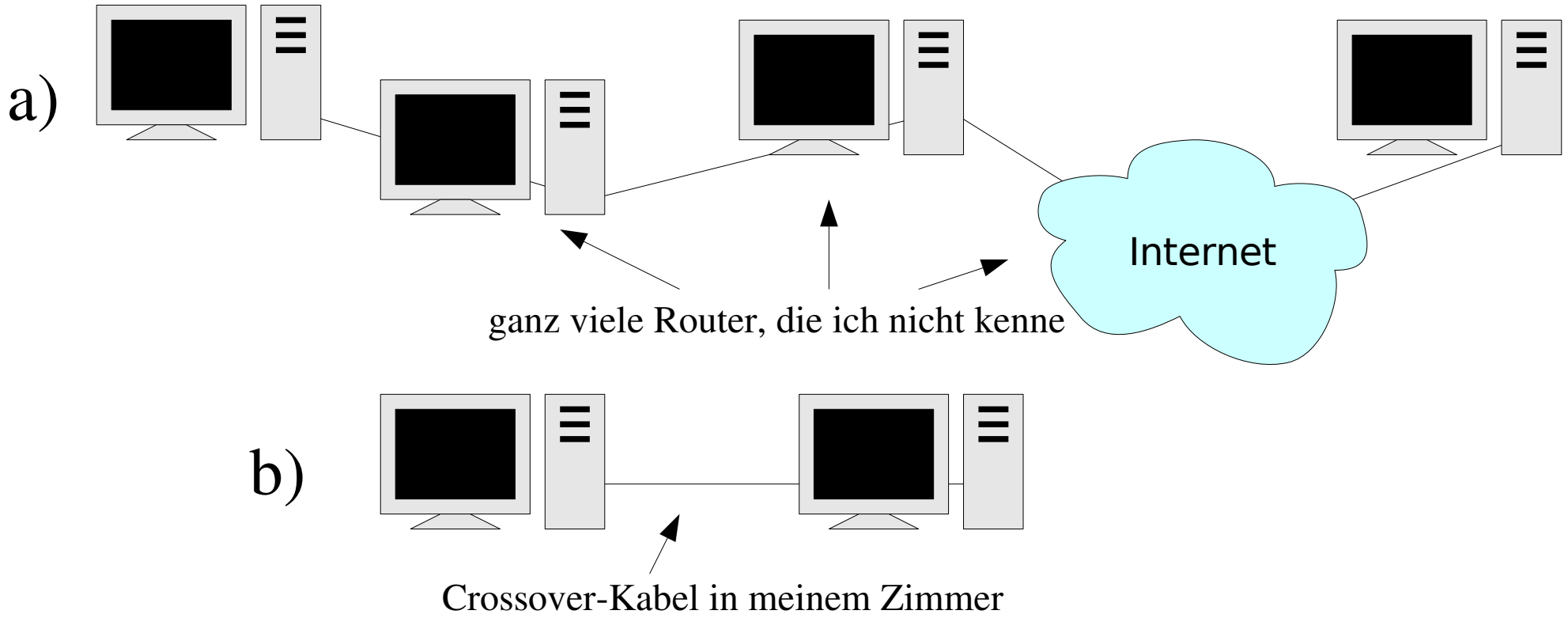
Verschlüsselung erforderlich?

bei a) wohl besser schon; bei b) ziemlich überflüssig



Motivation

Unterscheidung zwischen a) und b) erfordert *Topologie* des Netzes zu kennen. Anwendung kennt diese nicht, die Netzwerkschicht schon.



Motivation

Grund-Ideen:

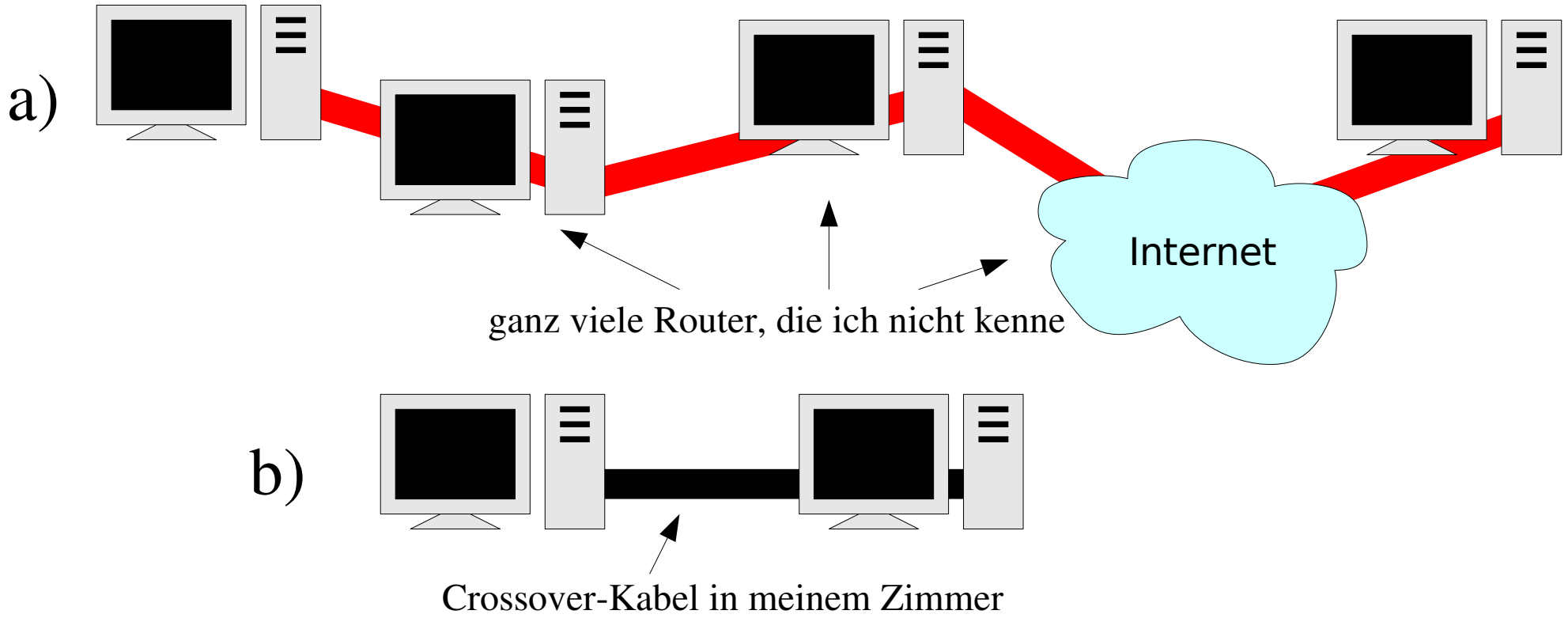
- Administrator/Anwendungen können Sicherheits*anforderungen* spezifizieren
- Netzwerkschicht stellt Sicherheits*mechanismen* bereit
- Administrator stellt Sicherheits*richtlinien* auf
  - definiert, wie Anforderungen durch Mechanismen erfüllt werden

Motivation

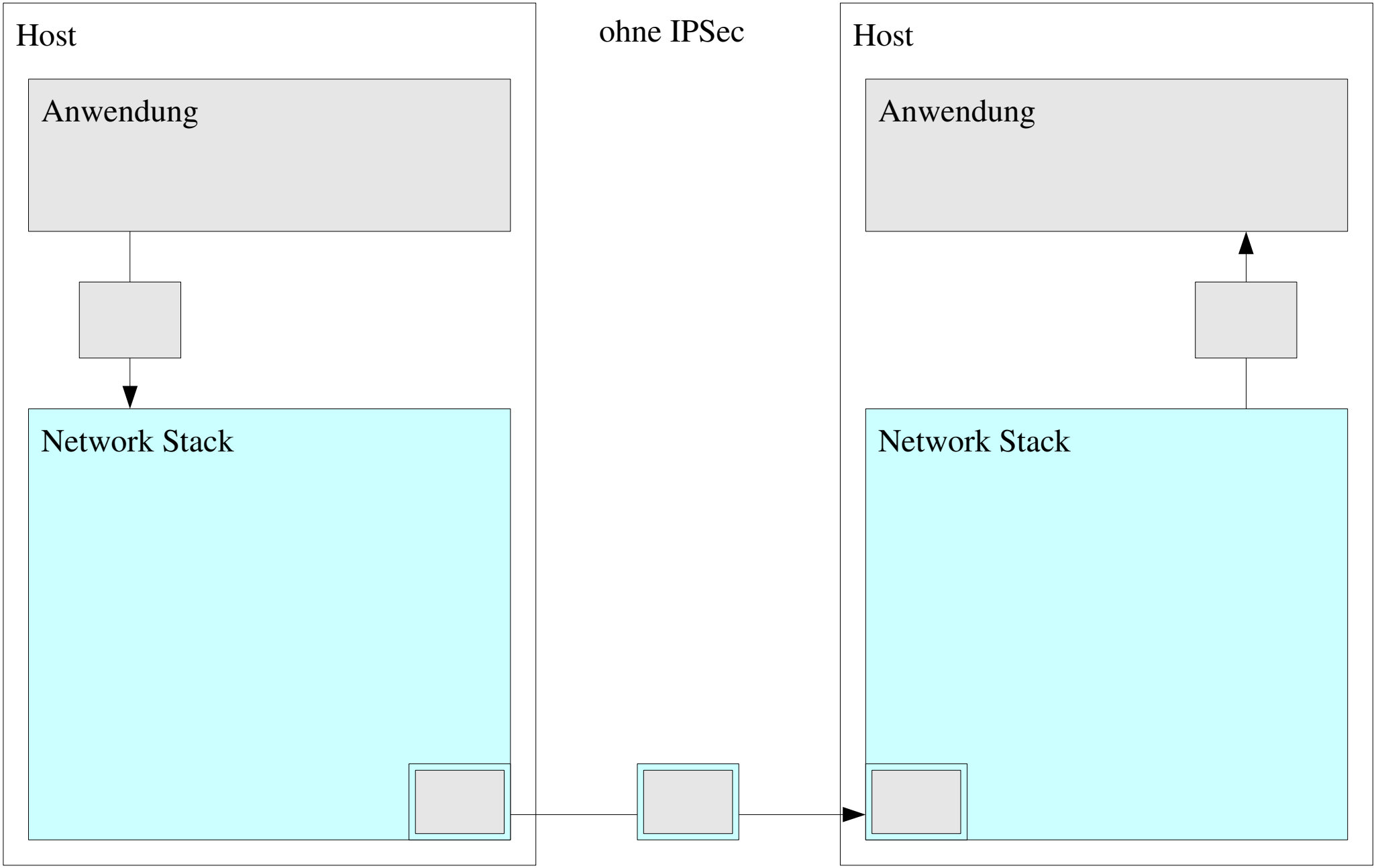
Richtlinie, z.B.:

- „vertrauliche“ Daten nur **verschlüsselt** über Internet
- „vertrauliche“ Daten im lokalen Netz **unverschlüsselt**

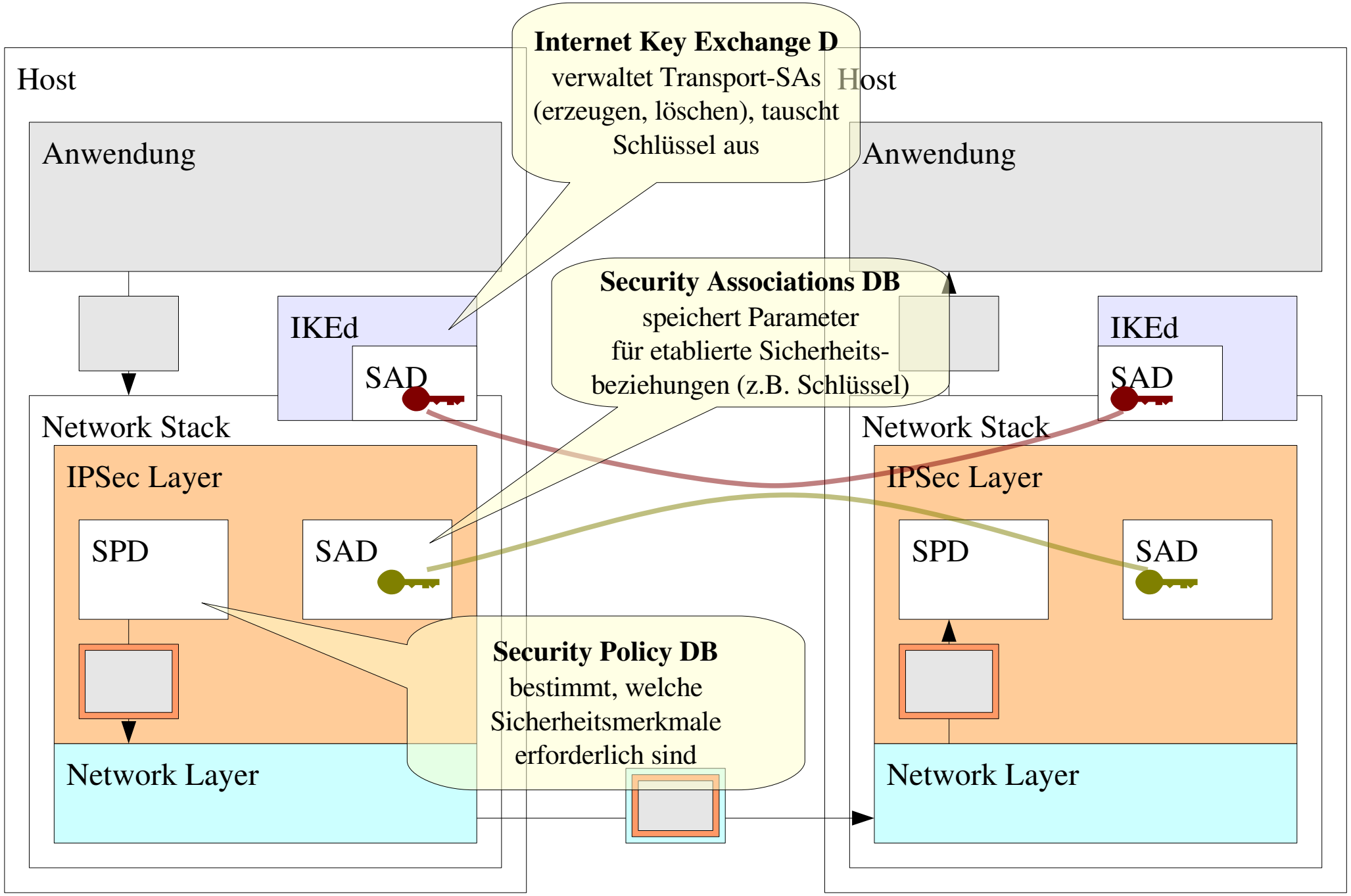
Daten als „vertraulich“ klassifiziert



1 IPSec Architektur



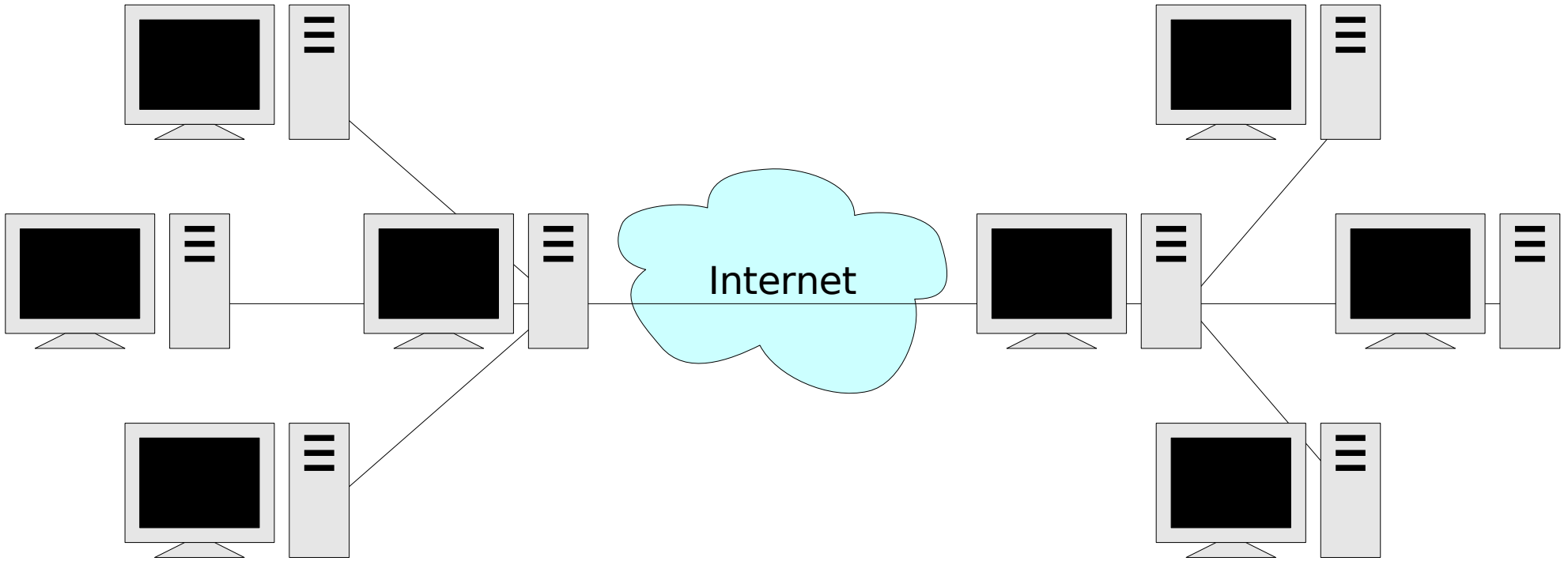
1 IPSec Architektur



1 IPSec Architektur

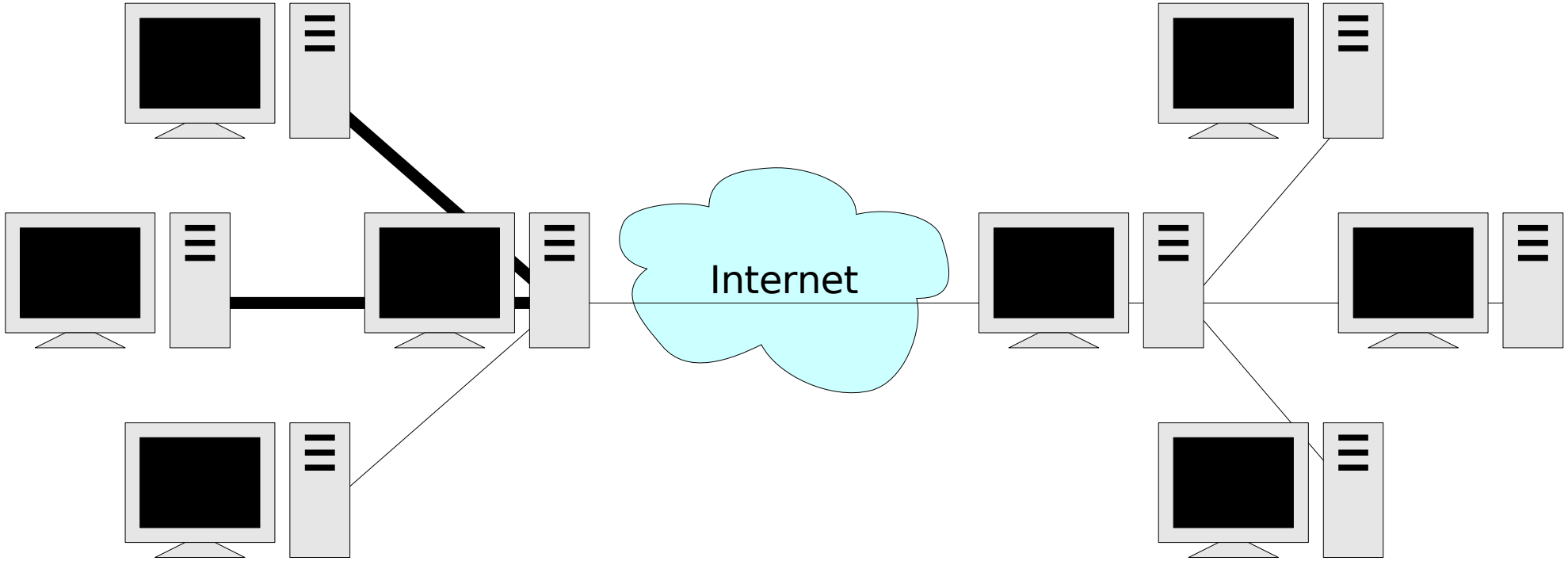
- Sicherheit des Kommunikationskanals
  - Vertraulichkeit, Authenzität, Integrität
- Richtliniendatenbank
- Umsetzung der Richtlinien
  - Sicherheitsattribute ermitteln
  - Kommunikationspartner authentisieren, Schlüsselaustausch
  - Sicherheitsassoziationen managen

1 IPSec Architektur
Szenarien



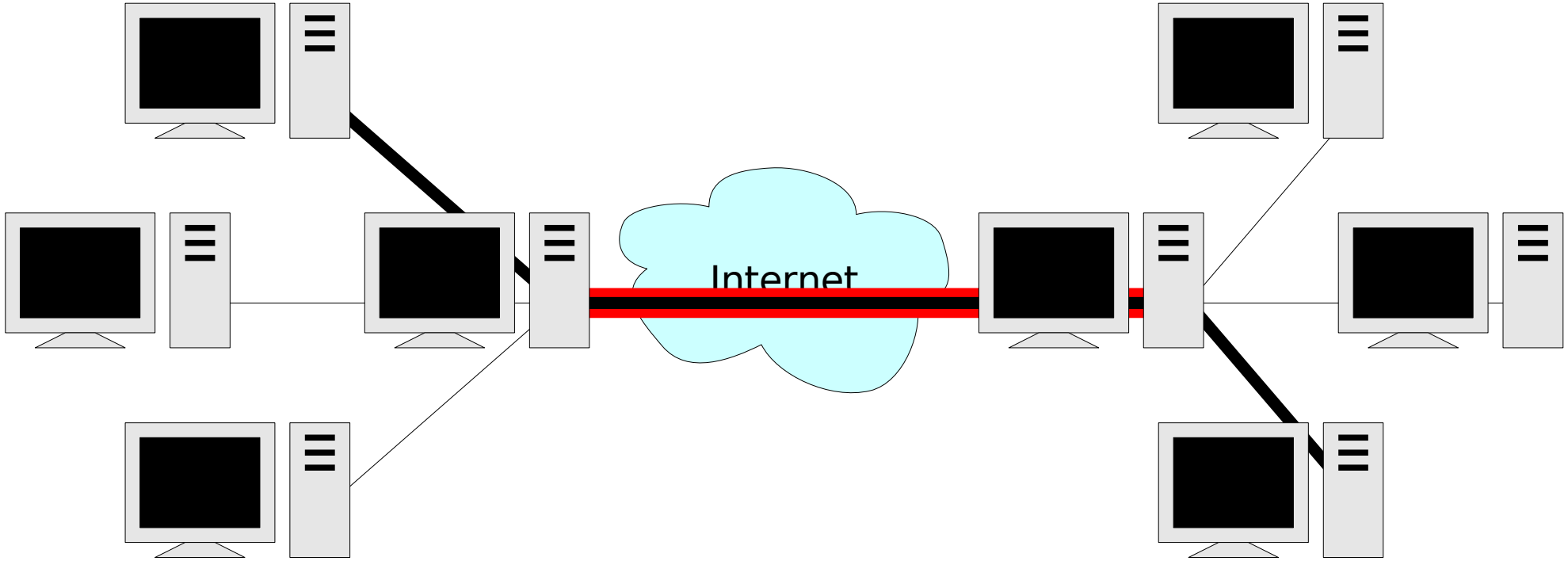
1 IPSec Architektur
Szenarien

- im lokalen Netz ohne Verschlüsselung vertraulich



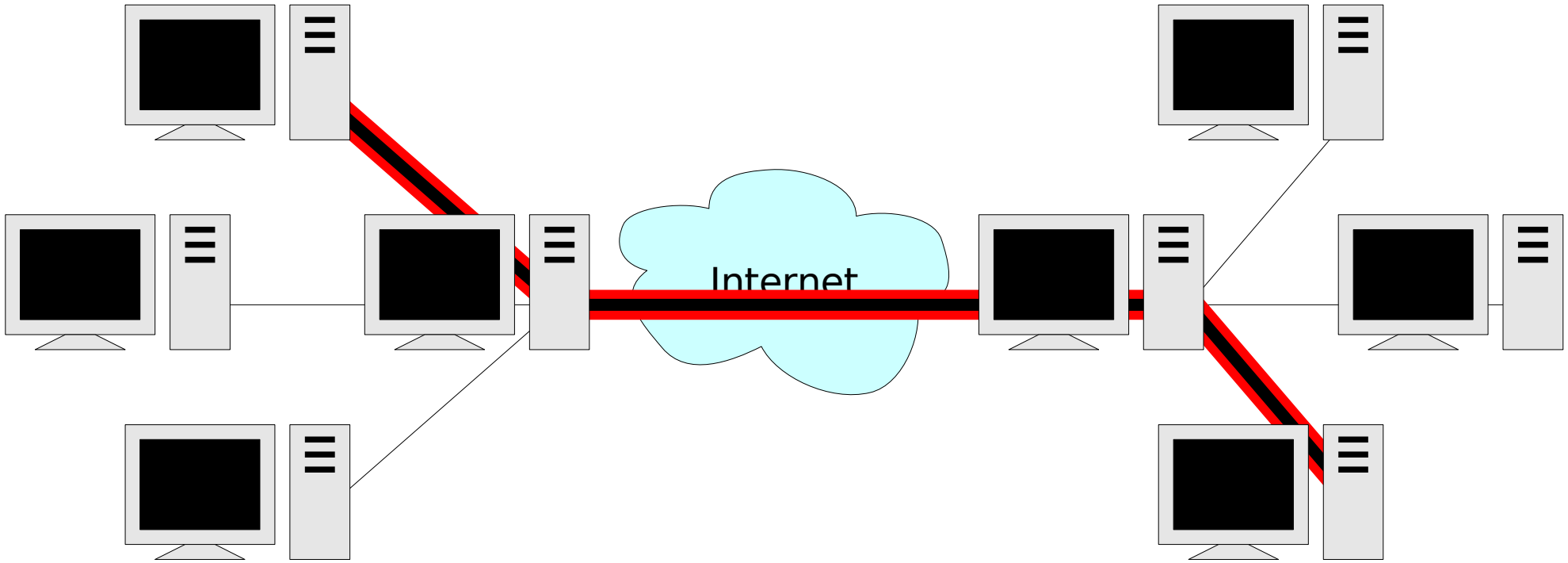
1 IPSec Architektur
Szenarien

- Verschlüsselung durch Security Gateway

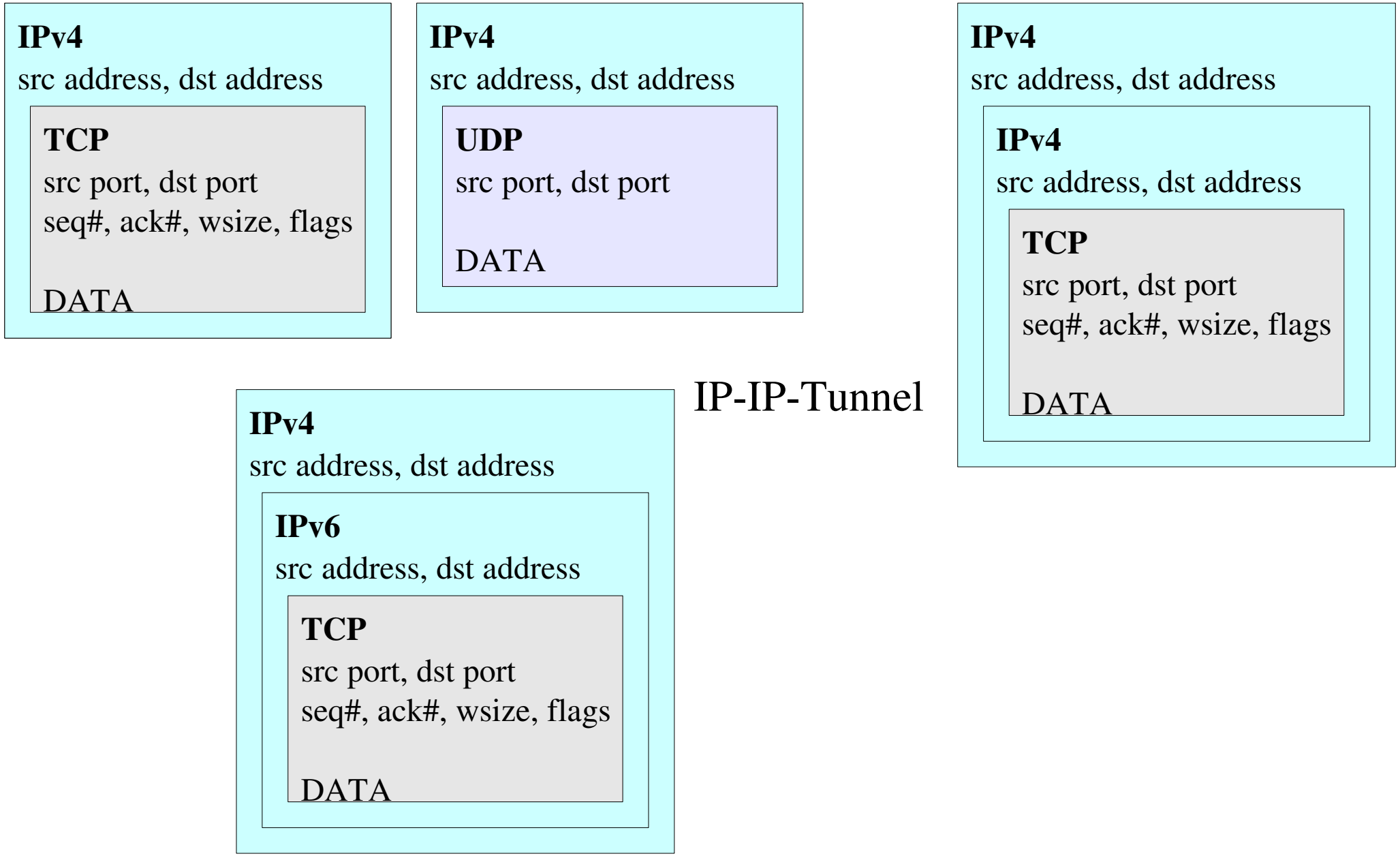


1 IPSec Architektur
Szenarien

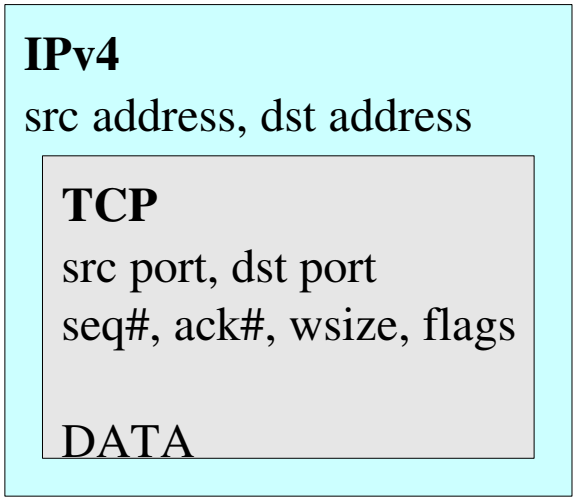
- unter Sicherheitsaspekten besser: Ende zu Ende

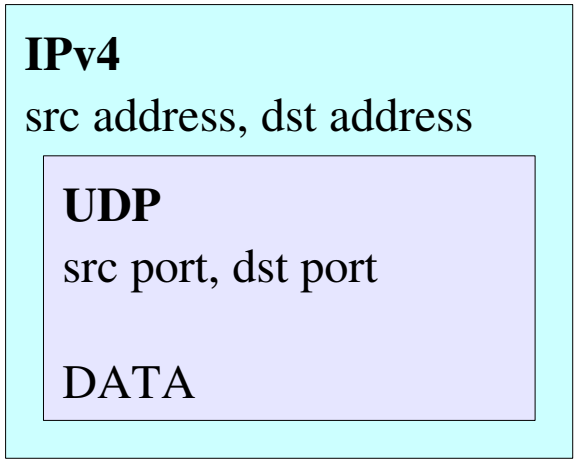


2 IPSec Paketsicherheit

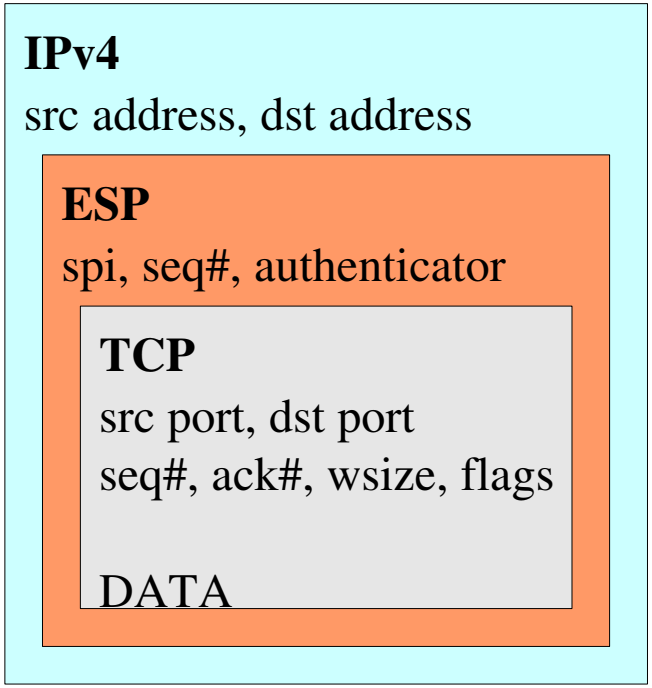


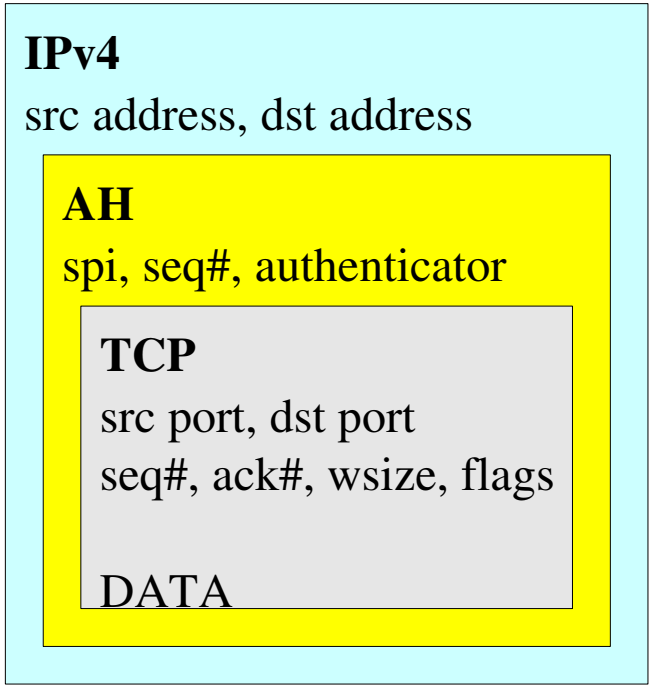
2 IPSec Paketsicherheit

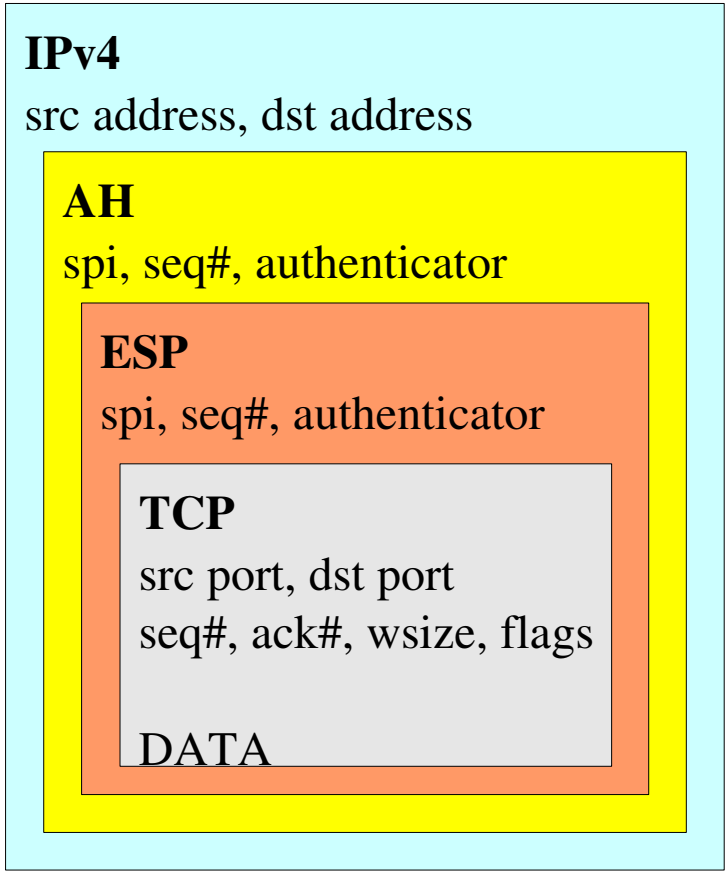




Neue Payload-Typen:
Encapsulated Security Payload
Authentication Header

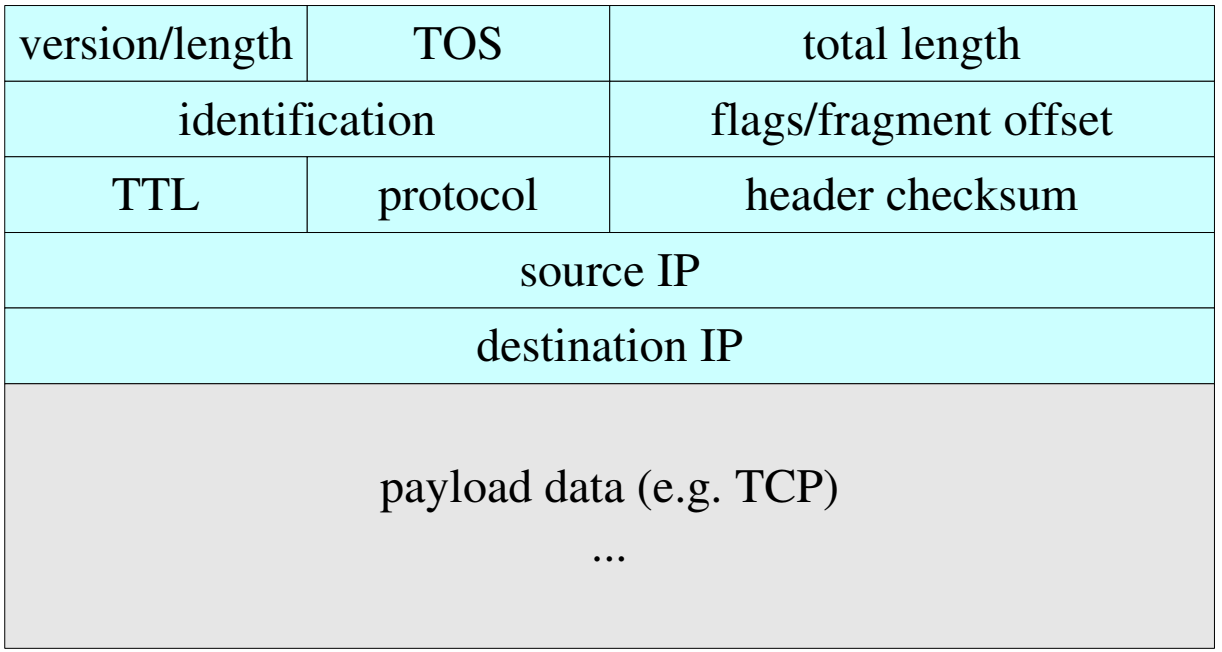




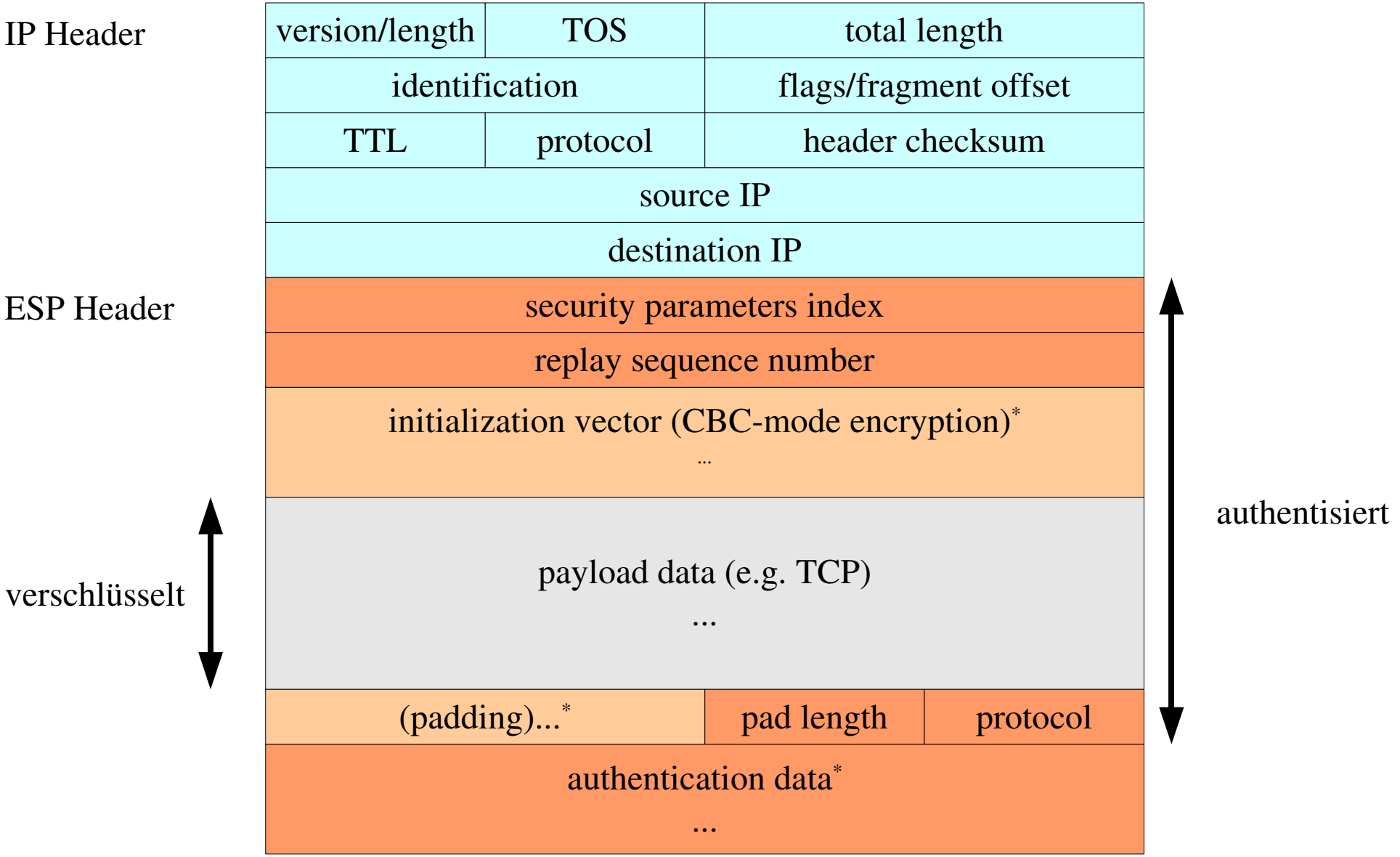


2 IPSec Paketsicherheit
"normales" IP-Paket

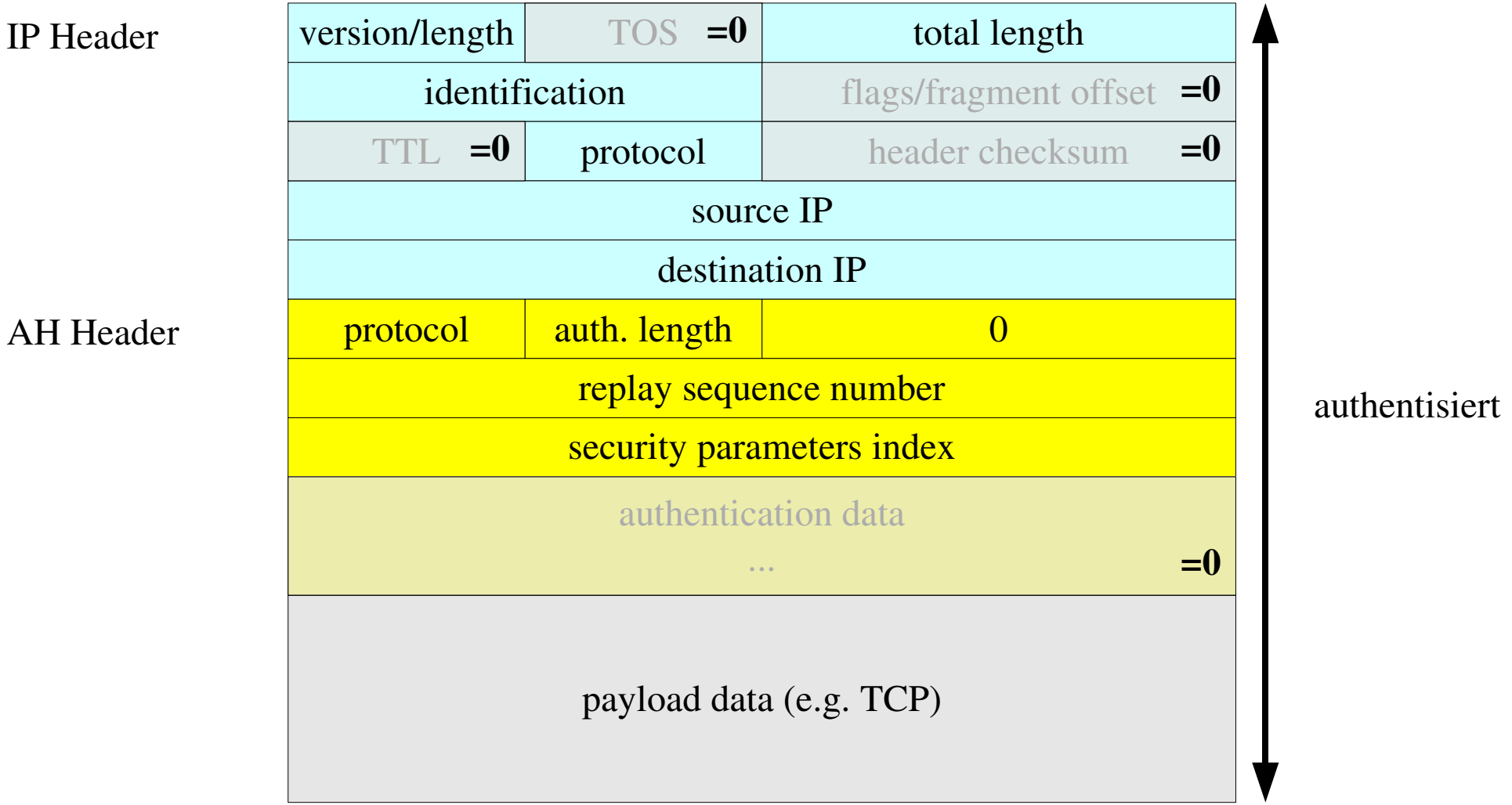
IP Header



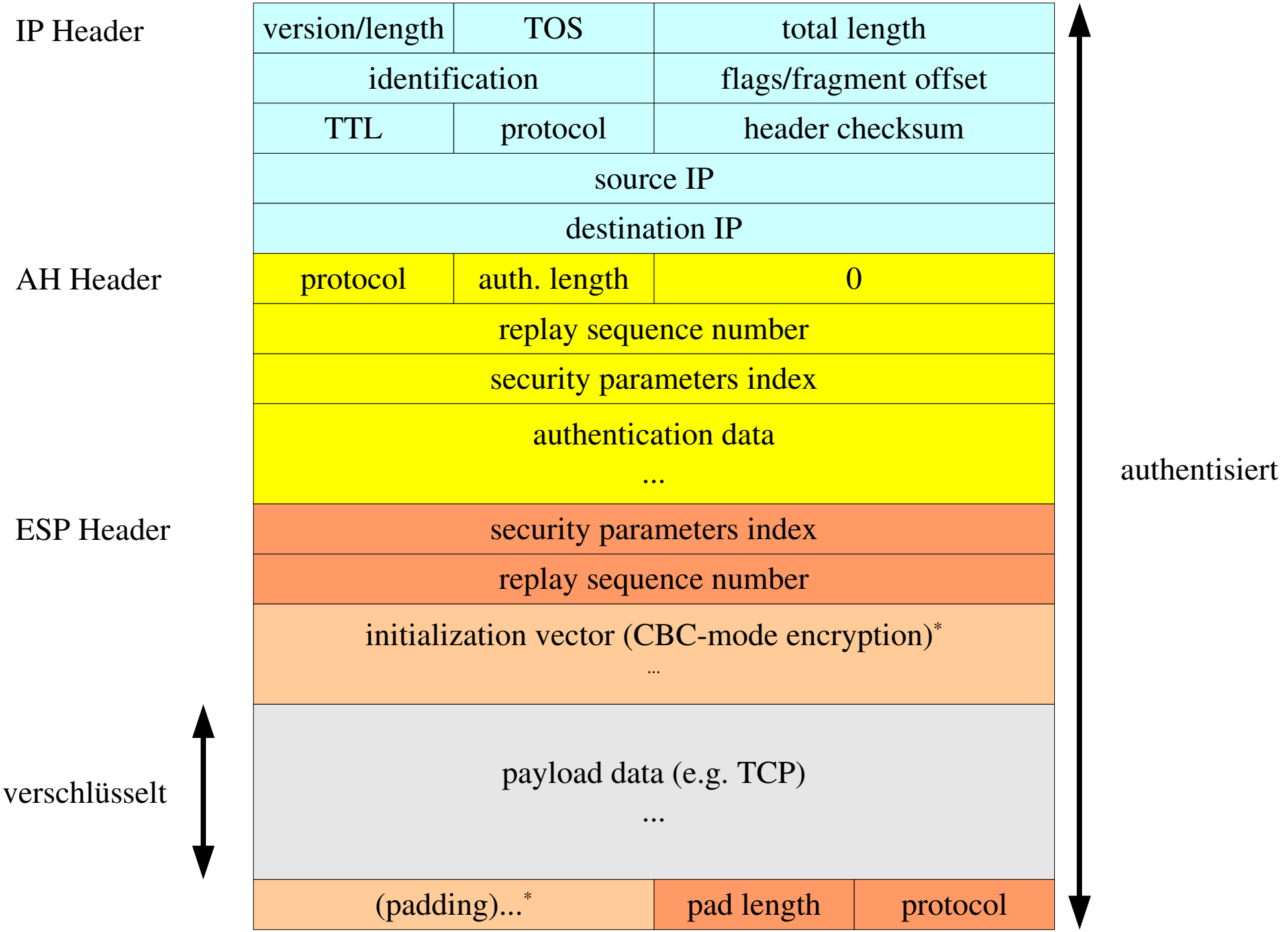
2 IPSec Paketsicherheit
ESP-Paketformat

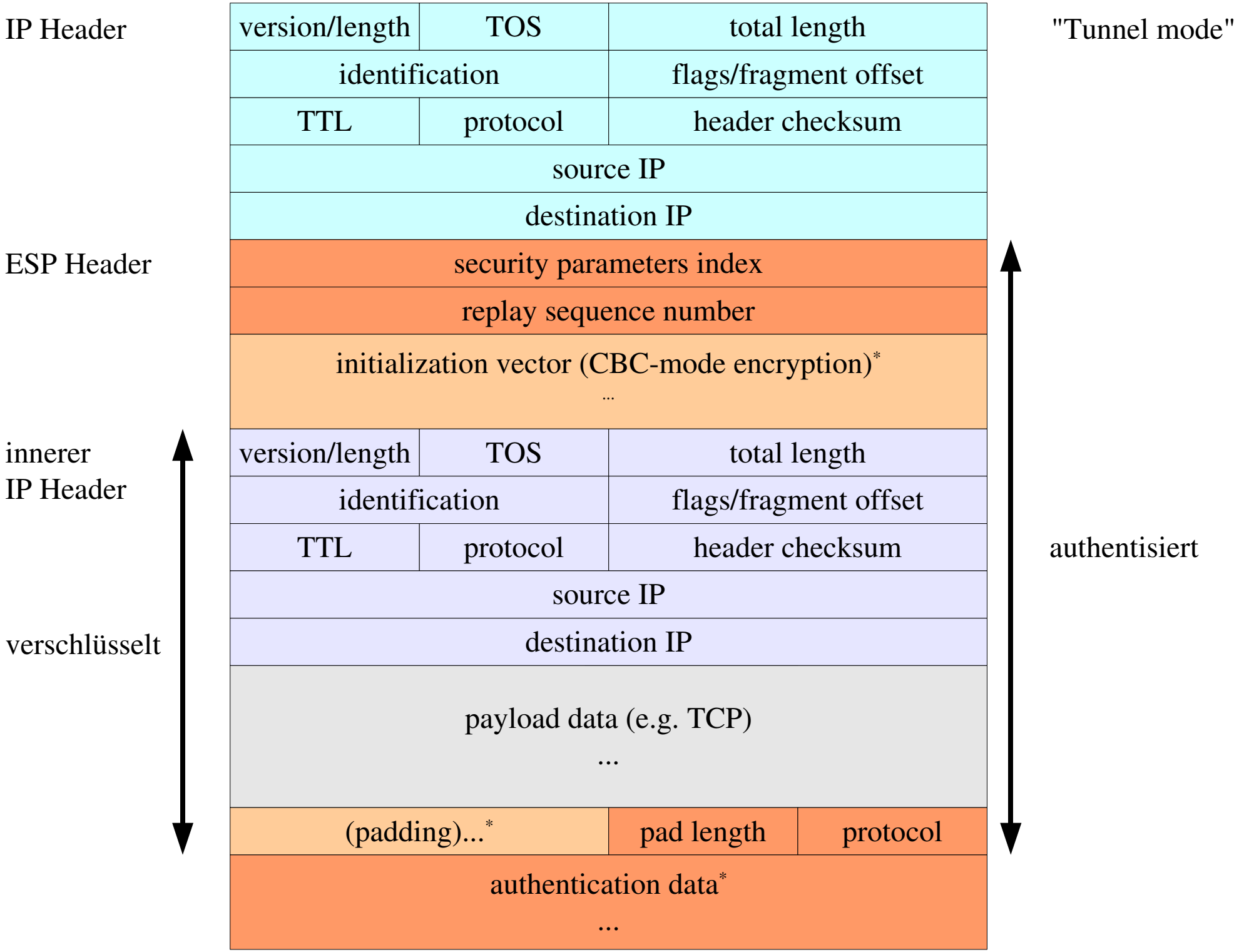


2 IPSec Paketsicherheit
AH-Paketformat



zur Berechnung des Authentikators werden veränderbare Felder auf 0 gesetzt


IP Header
version/length
TOS
total length
identification
flags/fragment offset
TTL
protocol
header checksum
source IP
destination IP
AH Header
protocol
auth. length
0
replay sequence number
security parameters index
authentication data
...
ESP Header
security parameters index
replay sequence number
initialization vector (CBC-mode encryption)*
...
payload data (e.g. TCP)
...
(padding)...*
pad length
protocol
verschlüsselt
authentisiert


IP Header
version/length
TOS
total length
"Tunnel mode"
identification
flags/fragment offset
TTL
protocol
header checksum
source IP
destination IP
ESP Header
security parameters index
replay sequence number
initialization vector (CBC-mode encryption)*
...
innerer
IP Header
version/length
TOS
total length
identification
flags/fragment offset
TTL
protocol
header checksum
authentisiert
source IP
destination IP
verschlüsselt
payload data (e.g. TCP)
...
(padding)...*
pad length
protocol
authentication data*
...

2 IPSec Paketsicherheit

übliche Praxis

- "Tunnel mode": nur ESP-Header (mit Auth.)
- Transport mode: ESP (ohne Auth.) + AH
  - zwei separate SAs erforderlich!
- Security gateways: meistens "Tunnel mode"
  - es ist *problemlos* möglich, transport mode zu verwenden
  - manchmal Verschleierung der "inneren IP" erwünscht

2 IPSec Paketsicherheit
Security Associations Database

- Tupel (src, dst, Protokoll, SPI) definiert Assoziation
- Tabelle enthält zu jeder Assoziation auszuführende Aktionen (Chiffre, Authentisierung etc.)

139.20.16.62, 139.20.16.55, ESP, 260	DES-CBC key=0xabc129ef9cde3f76, HMAC-SHA1 key=...
139.20.16.62, 157.11.9.201, AH, 537	HMAC-SHA1 key=...
139.20.16.62, 139.20.16.55, ESP, 932	AES-CBC key=..., HMAC-MD5 key=...
139.20.16.62, 139.20.16.55, AH, 260	DES-CBC-MAC key=...
139.20.16.62, 139.20.16.55, ESP, 261	AES-CBC key=...

- weitere Informationen könnten an SA gekoppelt sein (z.B. Nutzeridentität, Security Label)

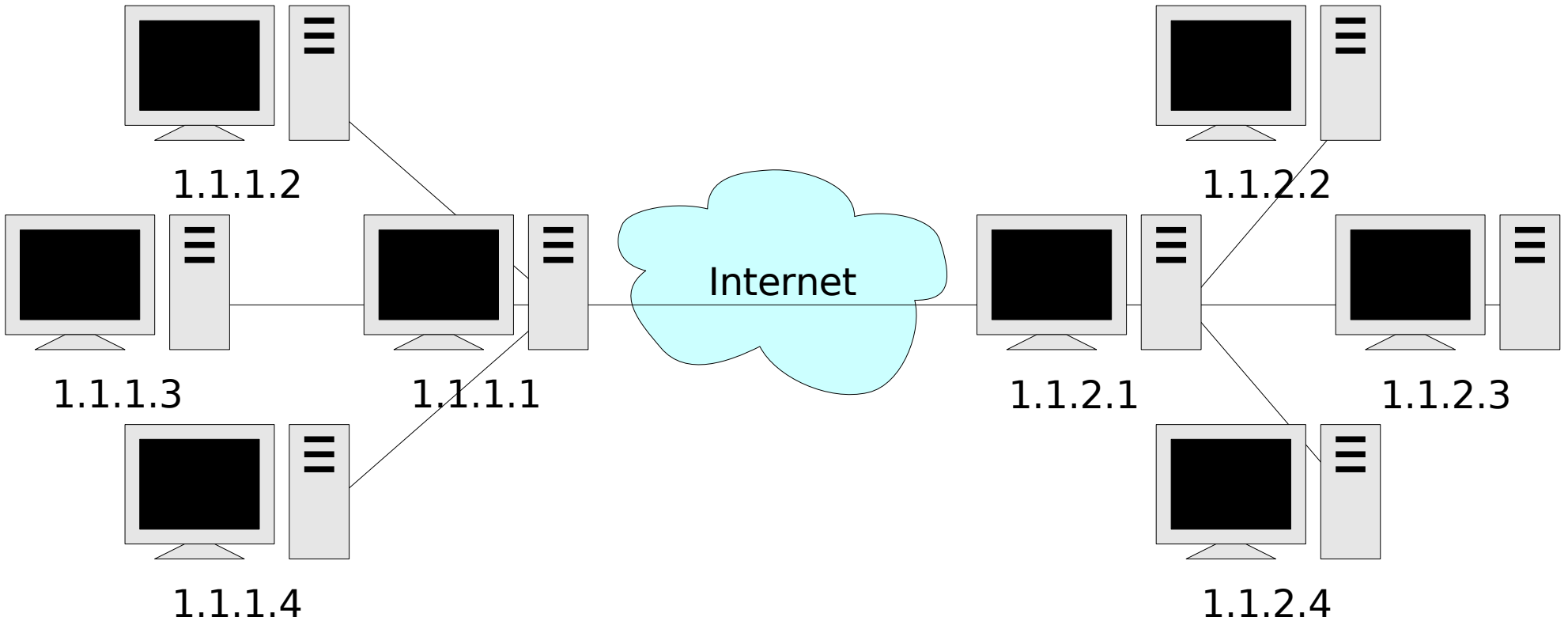
2 IPSec Paketsicherheit
Security Associations Database

- theoretisch machbar:
  - weitere Informationen an SA sein (z.B. Identität von Kommunikationspartnern, Security Labels)
  - Authentisierung "out-of-band"
  - Multi-User-Systeme: SA pro Nutzer
- praktische Hürden
  - IKE ungeeignet
  - SA-Attribute an Applikation übergeben

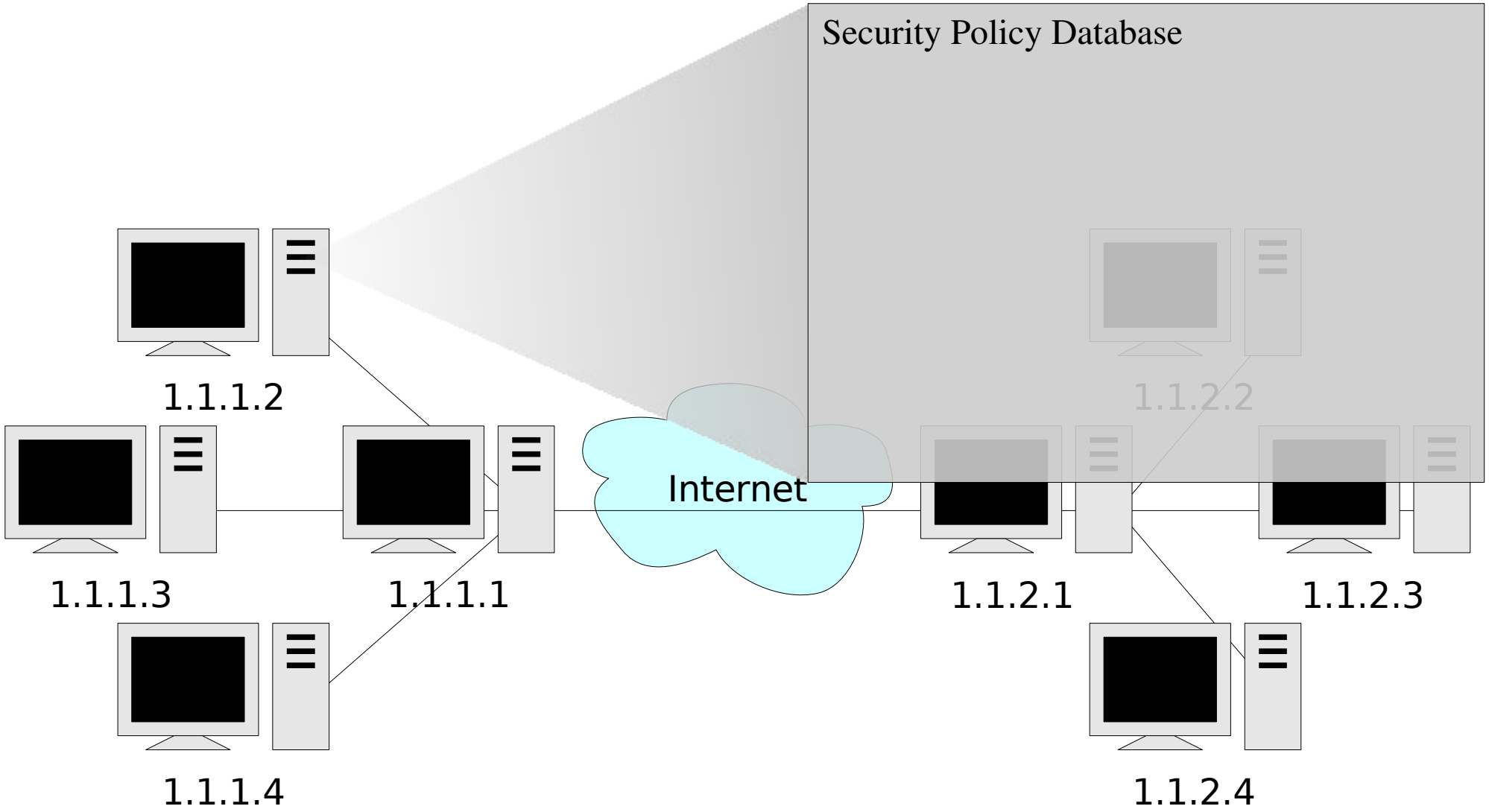
3 Sicherheitsrichtlinien
Security Policy Database (SPD)

- Spezifikation, welcher Typ von Kommunikationsverbindung welche Sicherheitsmerkmale aufweisen muss
- Vergleichbar mit Routing-Tabelle
  - Implementierungsabhängig, nicht in Standard spezifiziert
  - in "primitiven" Implementierungen (z.b. VPN Client): "auf *alle* Daten anwenden"
  - meist aber feinere Granularität, z.B.
    - Ports
    - Applikationswünsche
    - MAC labels

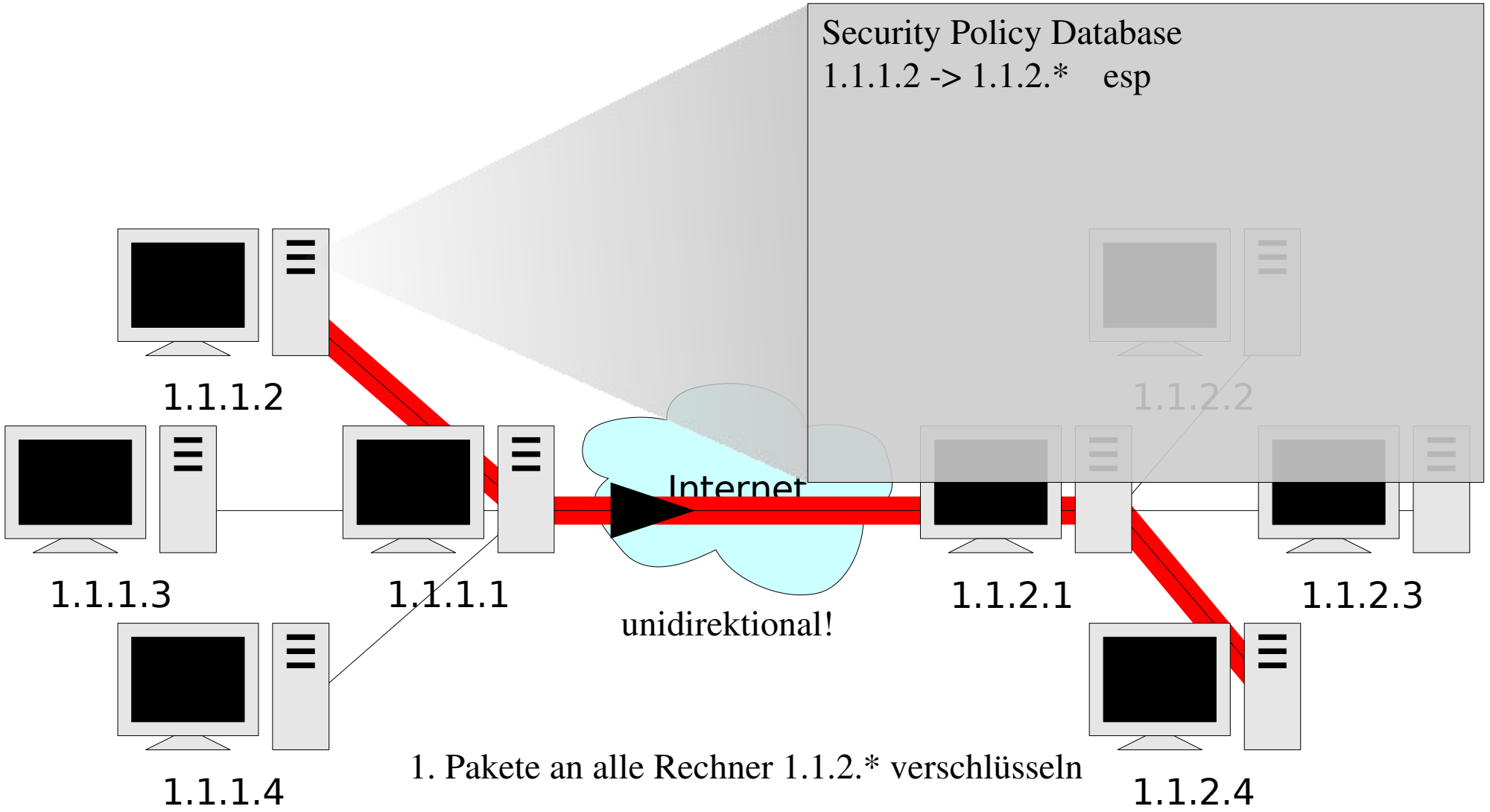
3 Sicherheitsrichtlinien



3 Sicherheitsrichtlinien



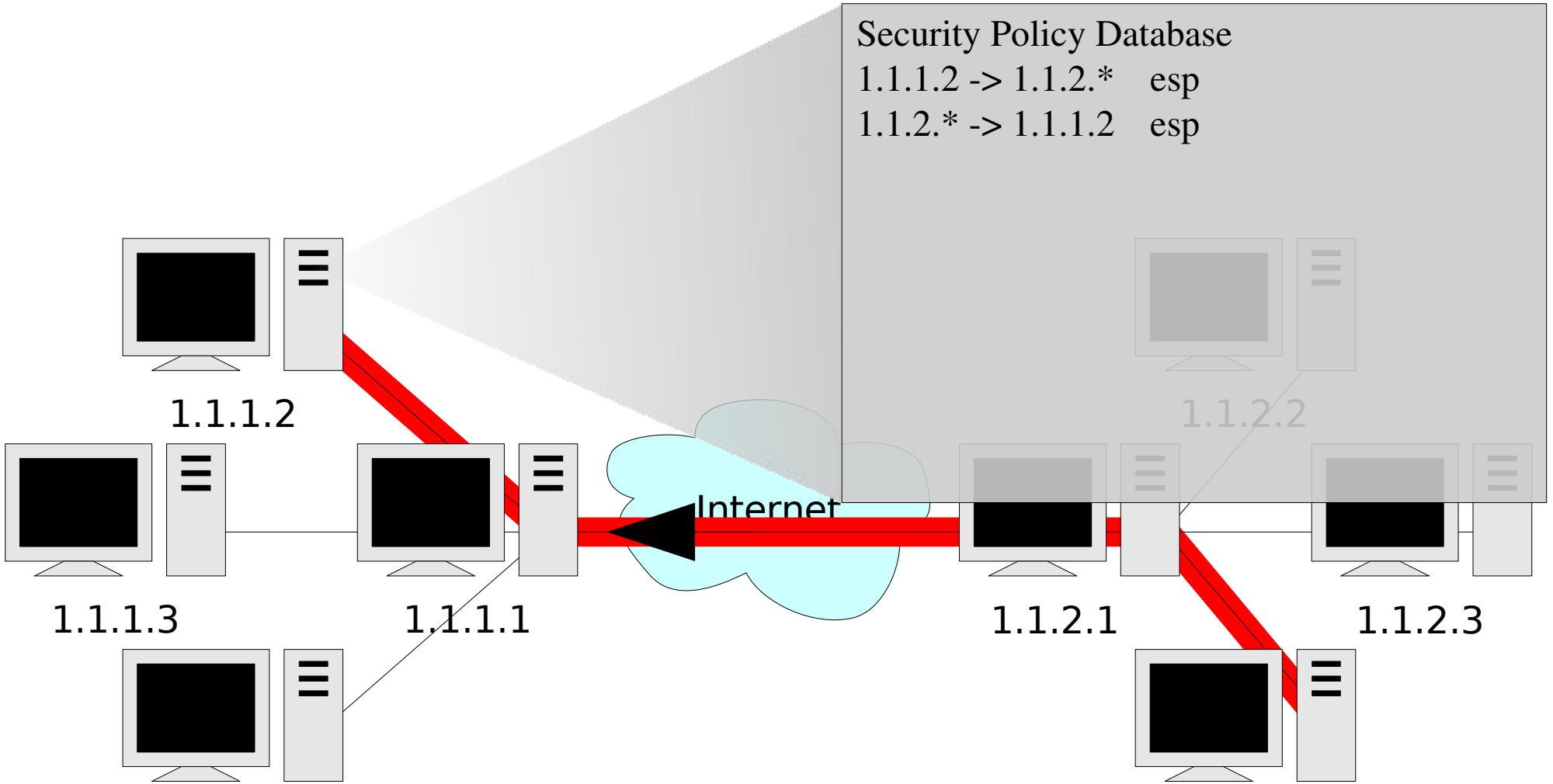
3 Sicherheitsrichtlinien



1. Pakete an alle Rechner 1.1.2.* verschlüsseln

```
spdadd 1.1.1.2 1.1.2.0/24 any -P out ipsec esp/transport//require
```

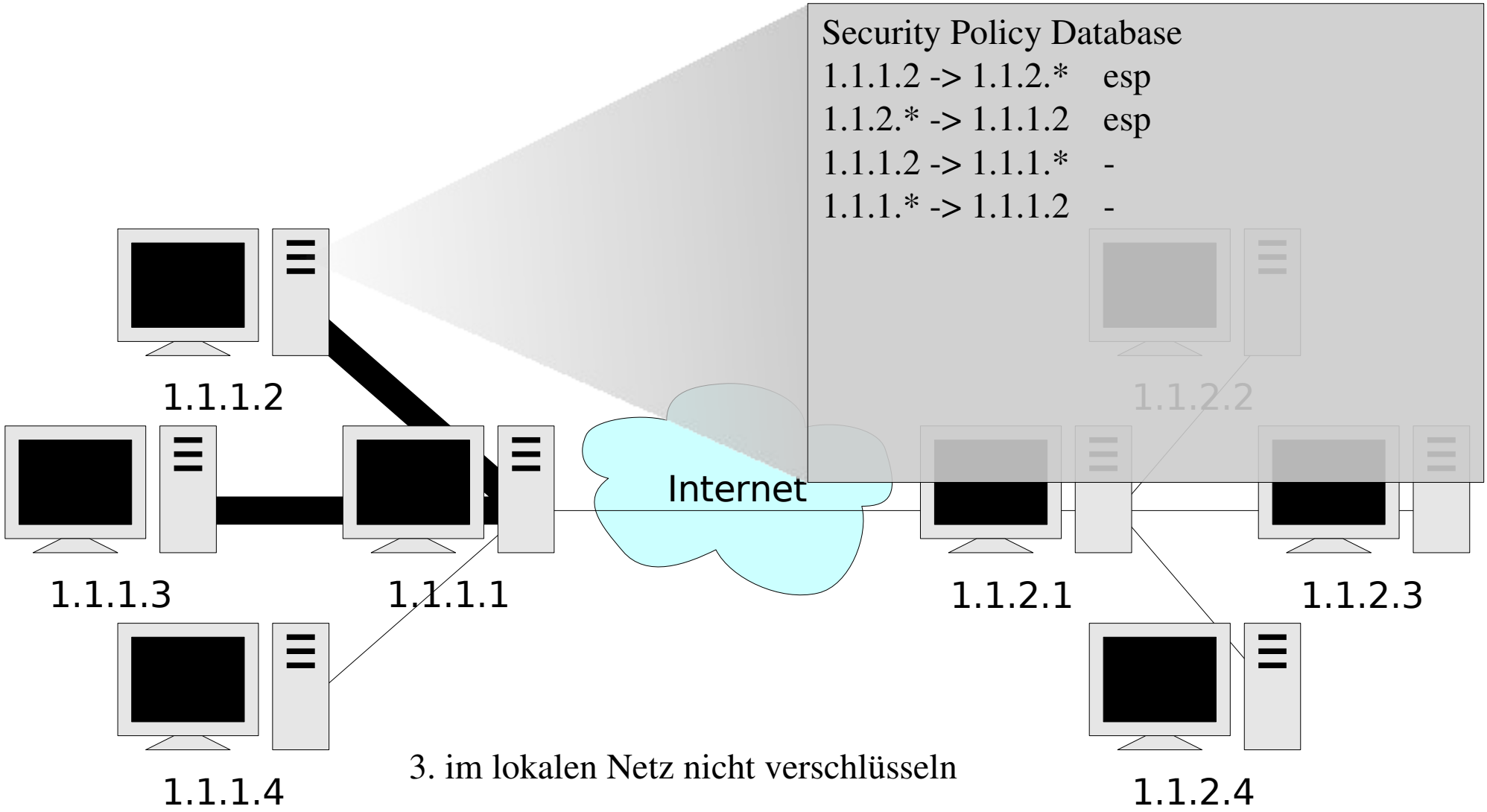
3 Sicherheitsrichtlinien



2. von Rechnern 1.1.2.* nur verschlüsselte Pakete empfangen

```
spdadd 1.1.2.0/24 1.1.1.2 any -P in ipsec esp/transport//require
```

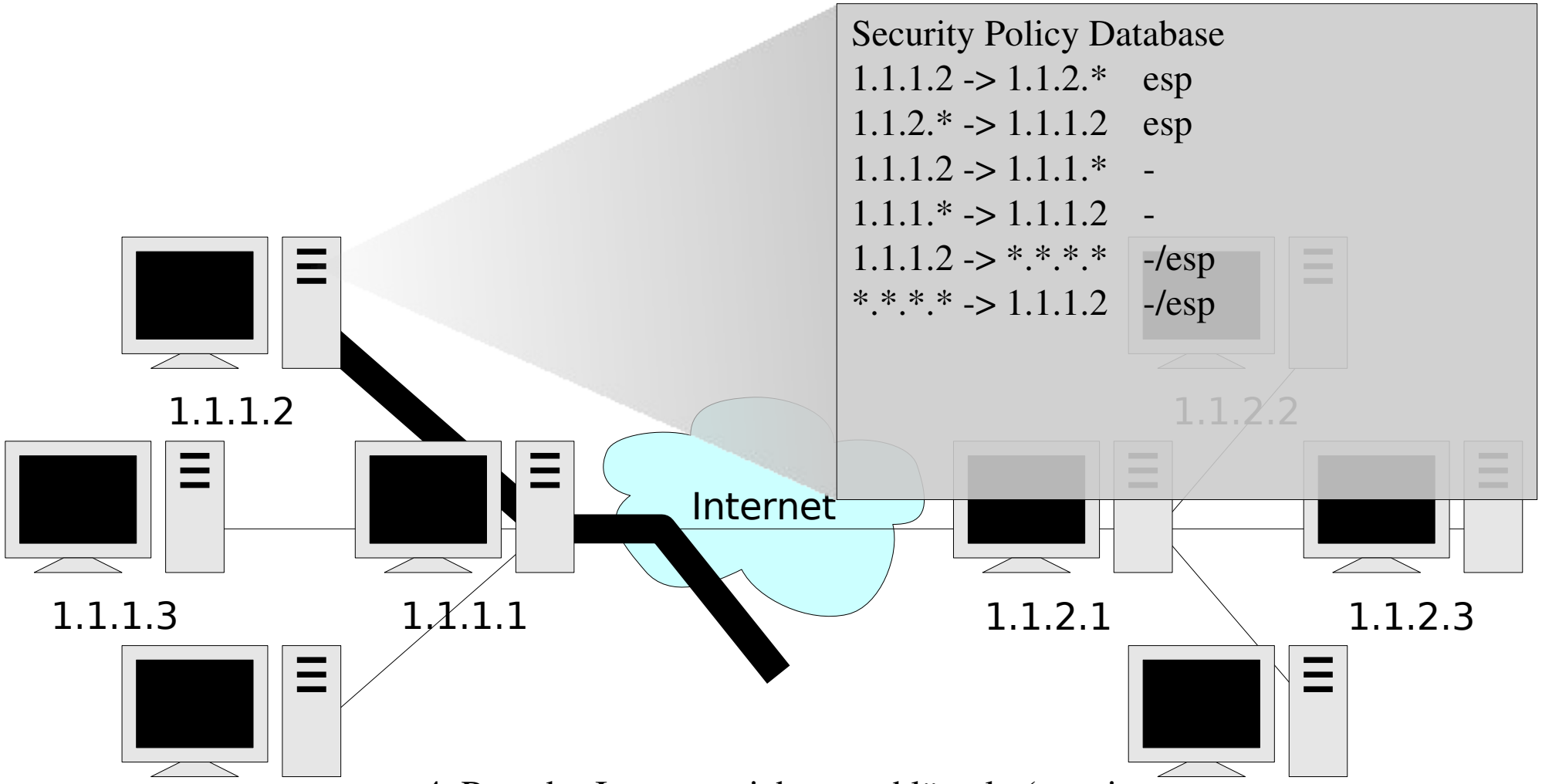
3 Sicherheitsrichtlinien



3. im lokalen Netz nicht verschlüsseln

```
spdadd 1.1.1.2 1.1.1.0/24 any -P out none
```

3 Sicherheitsrichtlinien



4. Rest des Internet: nicht verschlüsseln (es sei denn SA verfügbar, z.B. von Partner initiiert)

```
spdadd 1.1.1.2 0.0.0.0/0 any -P out ipsec esp/transport//use
```

3 Sicherheitsrichtlinien

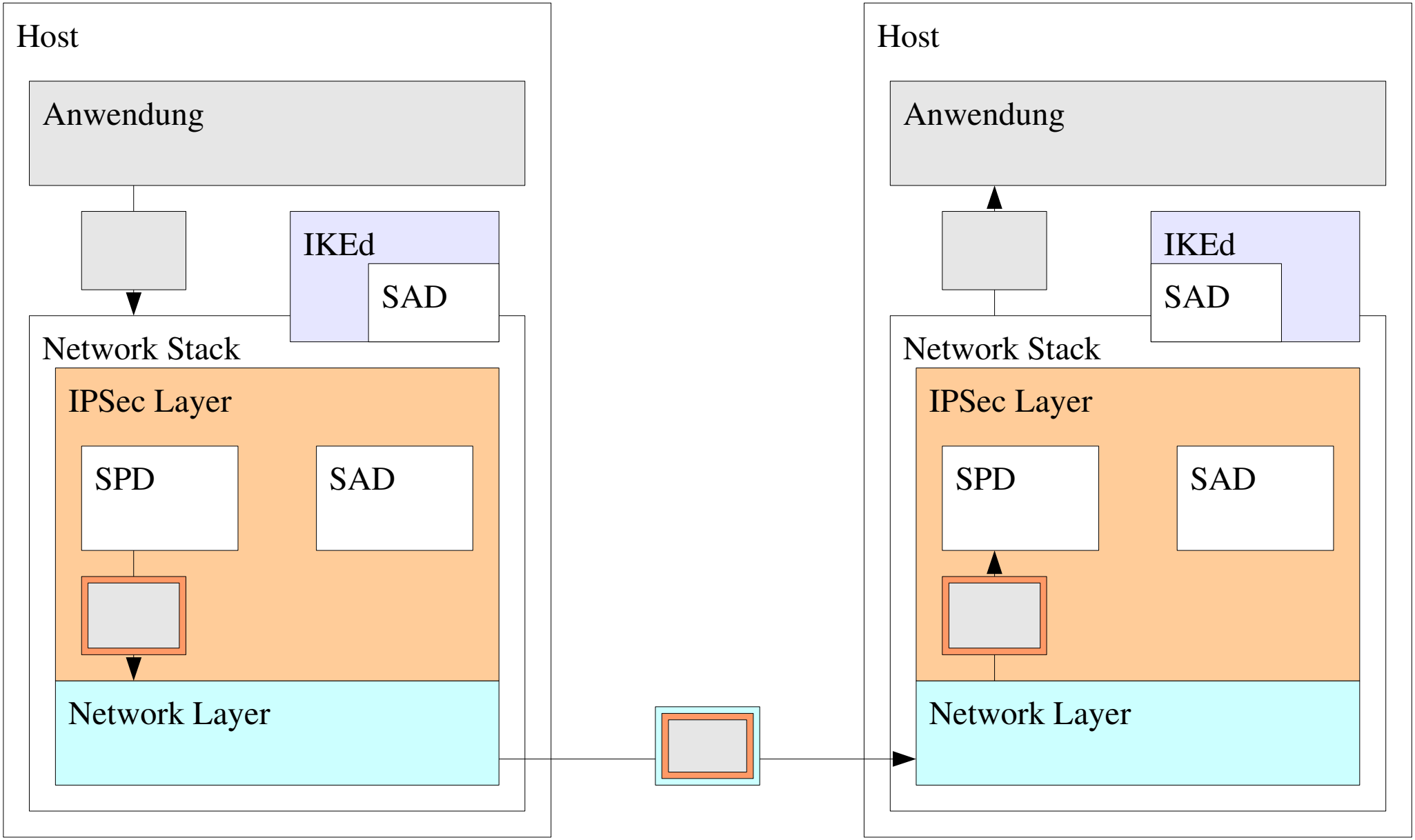
- Management von Sicherheitsrichtlinien in komplexem Netz nicht-trivial
  - Konsistenz
  - dynamisches Routing
    - SPD korrespondiert zu Topologieinformation
    - was, wenn Routing sich ändert?
  - Automatische Verteilung im Netz?
  - deswegen leider meistens doch Security Gateways :(

4 Schlüsselaustausch

- IPSec Paketsicherheit setzt etablierte IPSec-SAs voraus
- Management der SAs in separatem Protokoll
  - meist als separater Systemdienst implementiert
- Mehrere Kandidaten
  - Internet Key Exchange v1 (am weitesten verbreitet)
  - Internet Key Exchange v2 (noch rar)
  - KINK (experimentell)

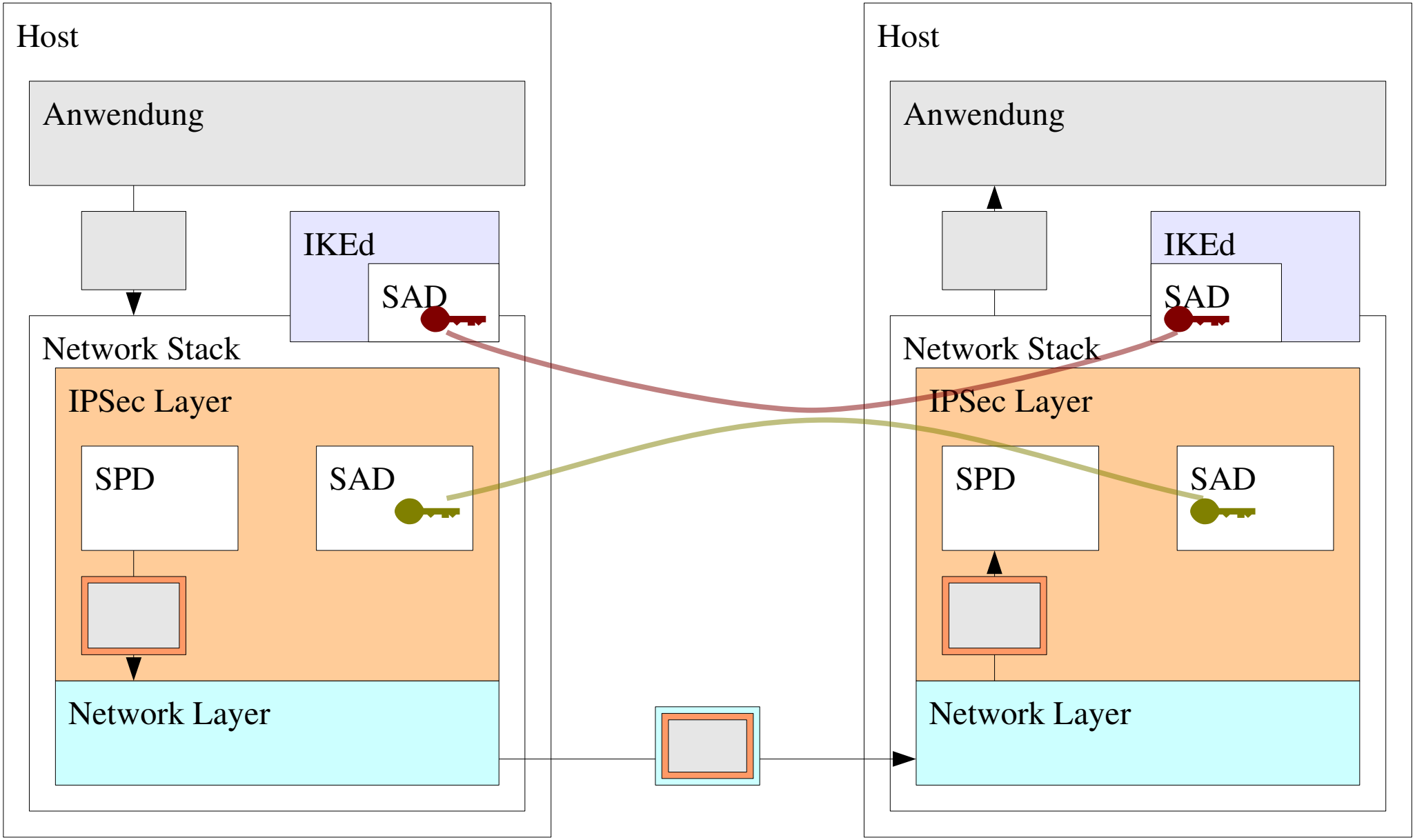
4 Schlüsselaustausch

4.1 IKEv1



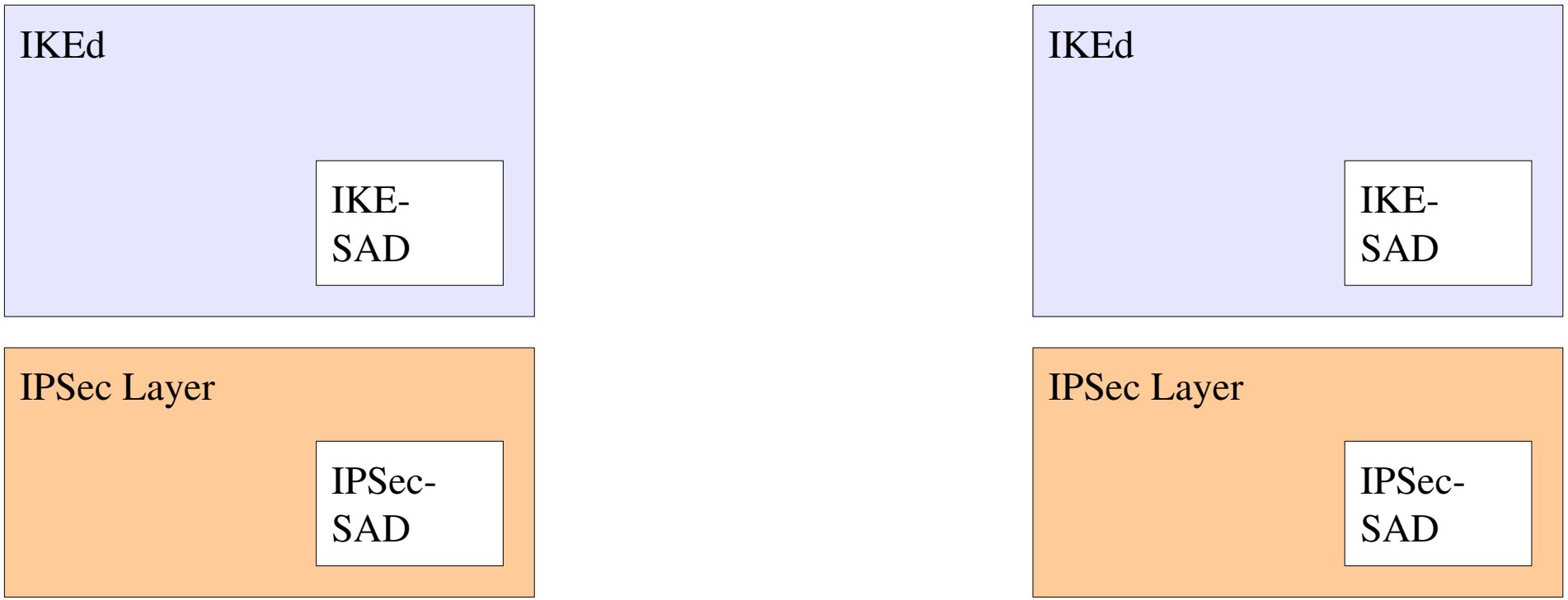
4 Schlüsselaustausch

4.1 IKEv1



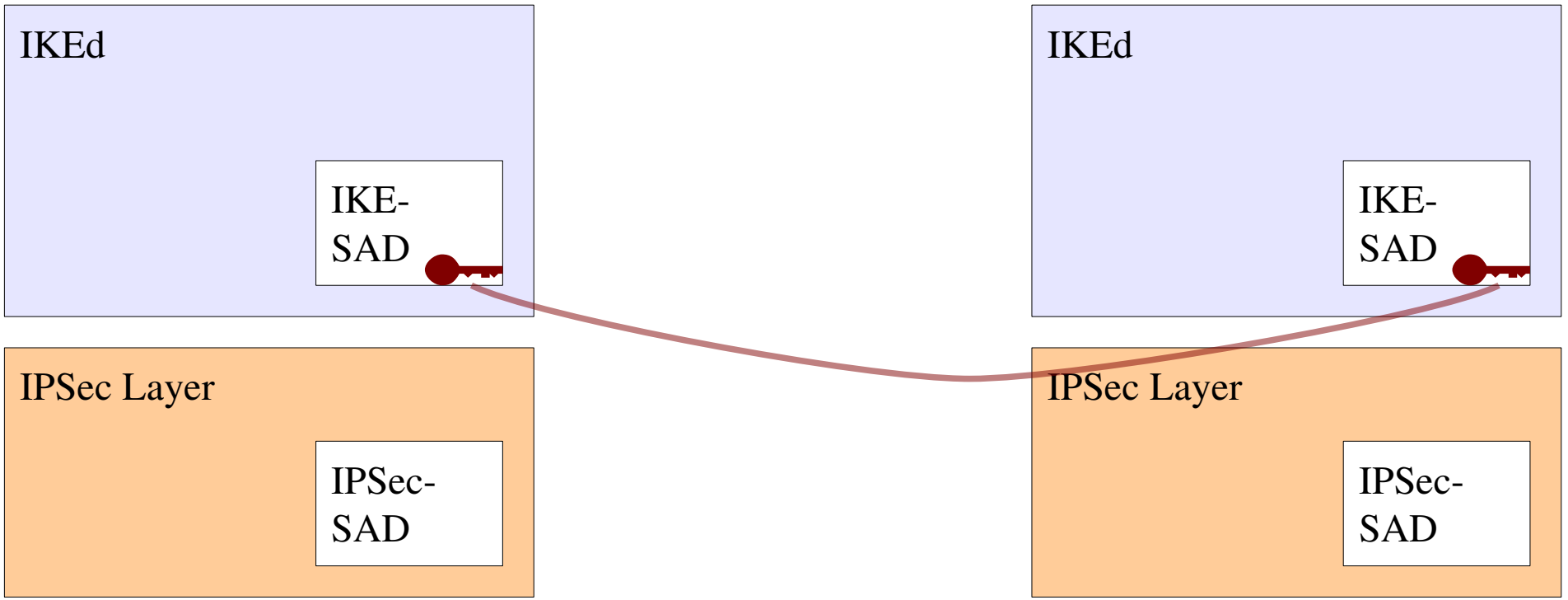
4 Schlüsselaustausch
4.1 IKEv1

- Austausch in zwei Phasen



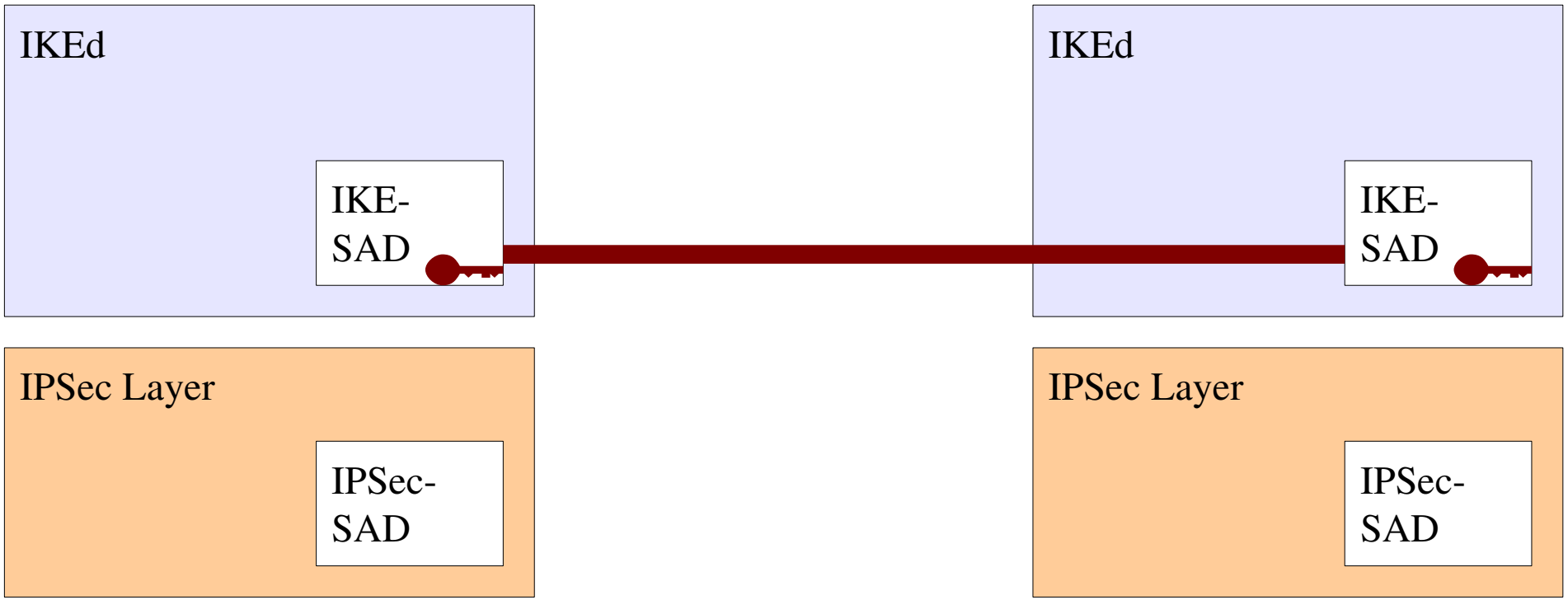
4 Schlüsselaustausch
4.1 IKEv1

- Phase 1: IKE-SA etablieren
  - beide IKE-Daemons authentisieren sich gegenseitig
  - etablieren sicheren Kommunikationskanal



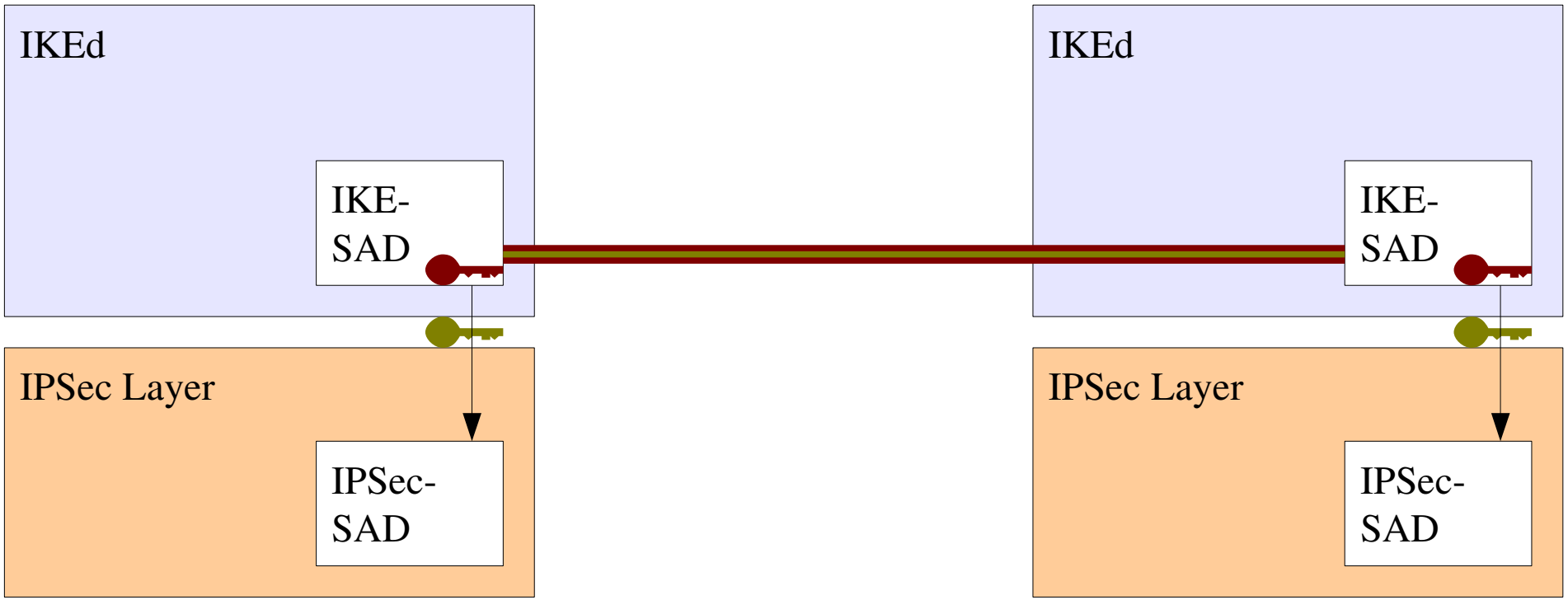
4 Schlüsselaustausch
4.1 IKEv1

- gesamte weitere Kommunikation über diesen etablierten Kanal



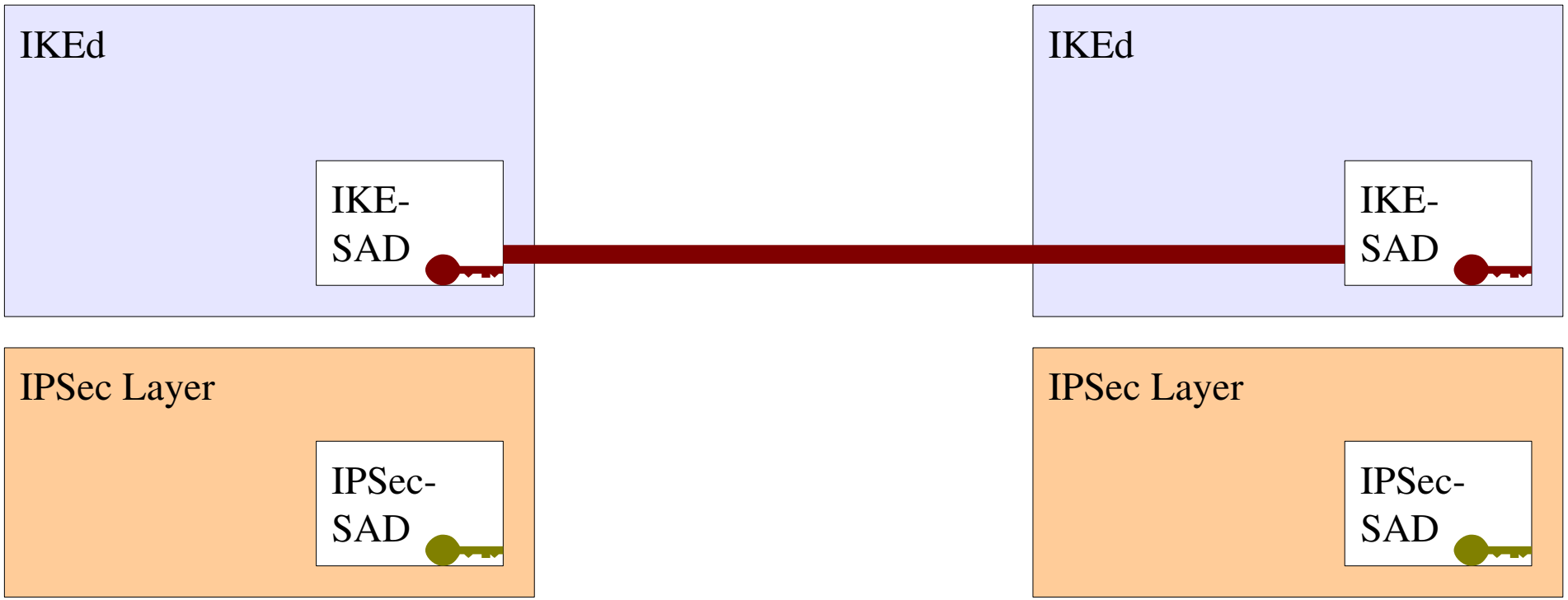
4 Schlüsselaustausch
4.1 IKEv1

- Phase 2: Daten für IPSec-SA austauschen
  - Identität des Gegenübers ist gesichert
  - Schlüssel generieren und an IPSec-Layer übertragen



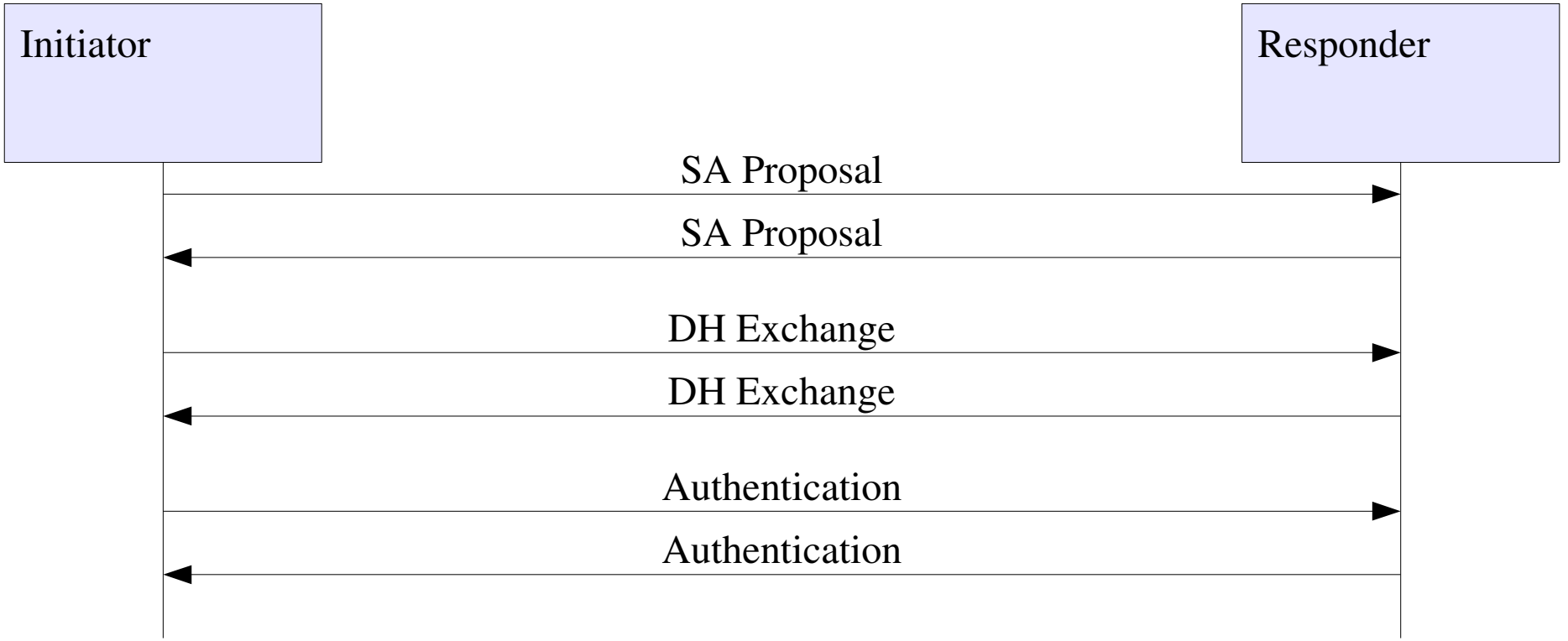
4 Schlüsselaustausch
4.1 IKEv1

- IPSec-SA wird in Phase 2 etabliert



4 Schlüsselaustausch
4.1 IKEv1

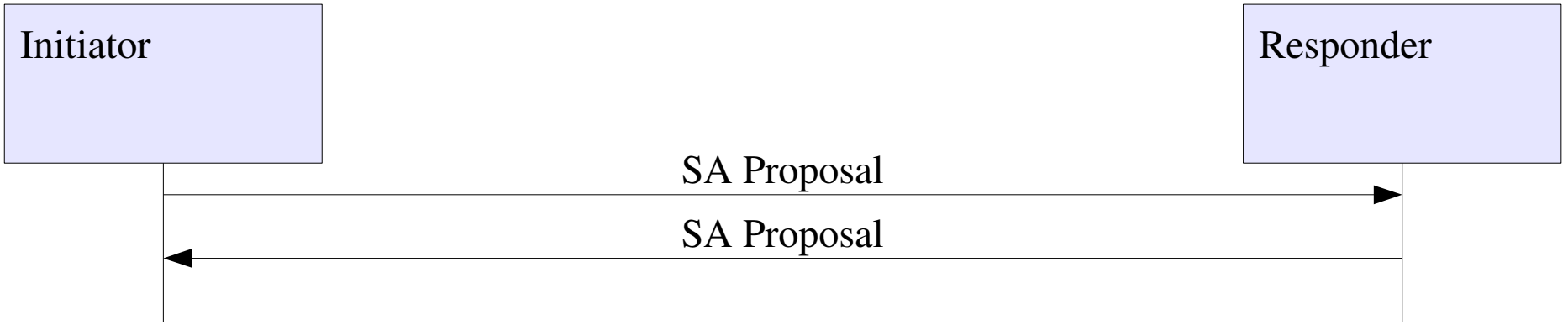
- Nachrichtenaustausch (Main mode)



Hinweis: Nachrichteninhalte leicht vereinfacht dargestellt; bitte RFC lesen!

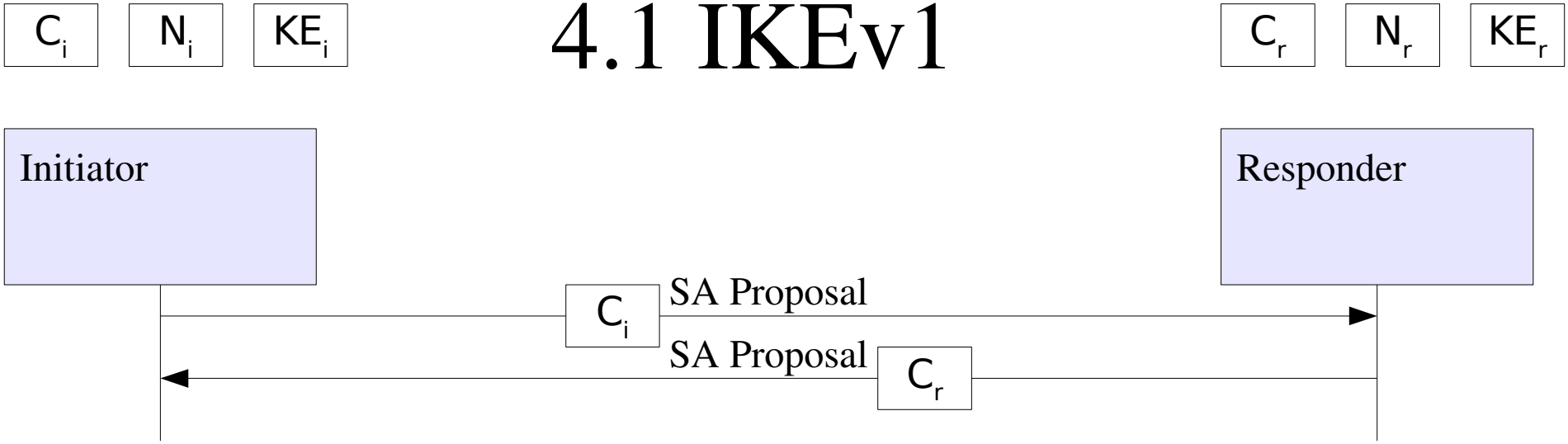
4 Schlüsselaustausch
4.1 IKEv1

- Vorschlag, eine SA zu etablieren
- Parameter werden ausgehandelt
  - verfügbare Algorithmen
  - gewünschte Authentisierung
- genauer Inhalt nachfolgender Pakete von Authentisierungsmethode abhängig



4 Schlüsselaustausch

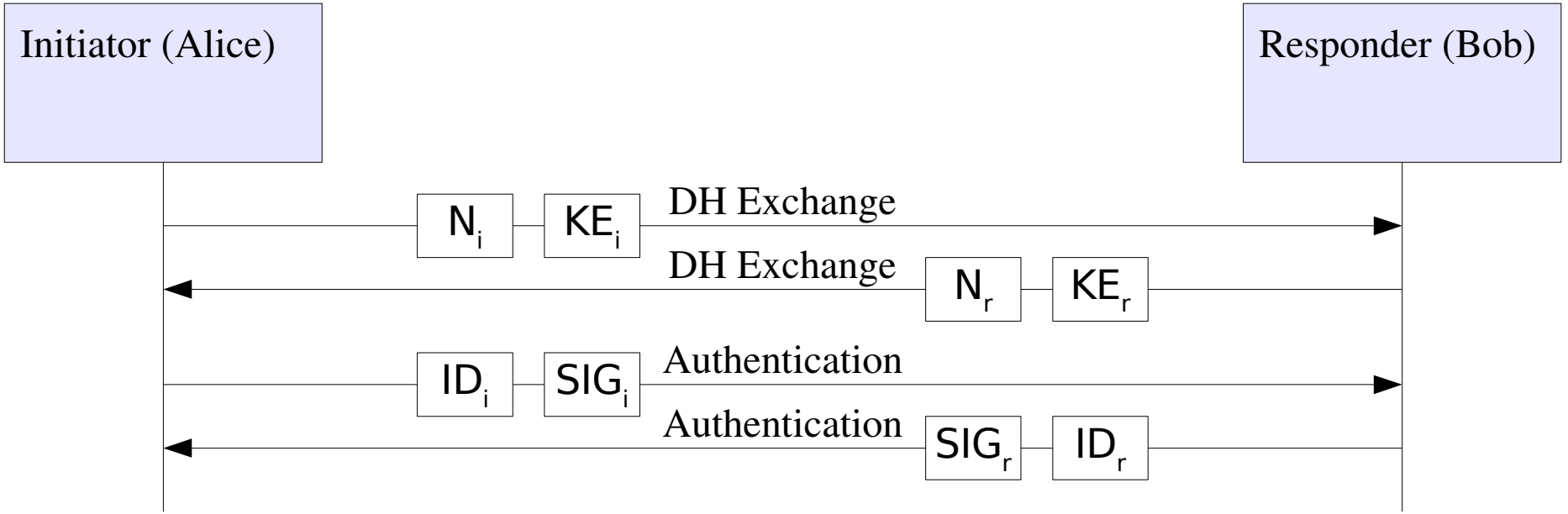
4.1 IKEv1



- immer: beide Parteien generieren folgende Daten, aus denen Schlüssel berechnet wird:
  - Cookie: identifiziert gleichzeitig SA Proposal
  - Nonce: Zufallszahl; gleichzeitig Schutz gegen Replay
  - zwei Werte für Diffie-Hellman-Austausch

4 Schlüsselaustausch
4.1 IKEv1

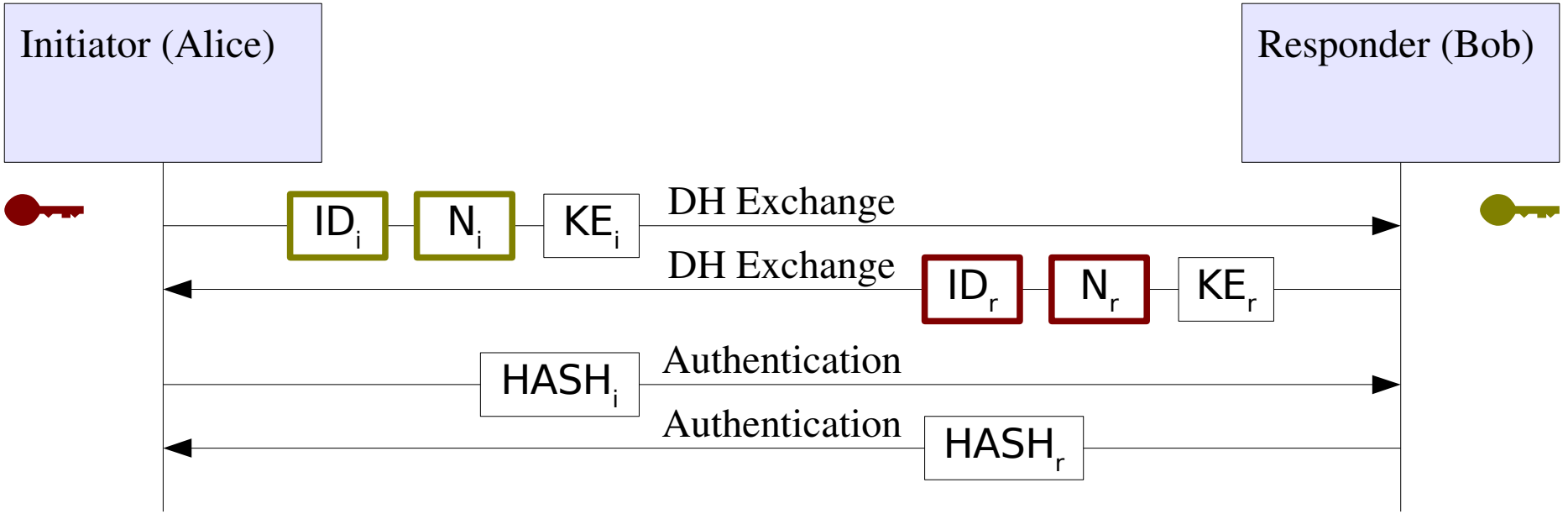
- z.B. digitale Signaturen



wenn Alice N_i N_r KE_i KE_r ID_i mit privatem Signaturschlüssel signiert,
dann kann Bob verifizieren, dass Alice am Austausch beteiligt war,
und umgekehrt

4 Schlüsselaustausch
4.1 IKEv1

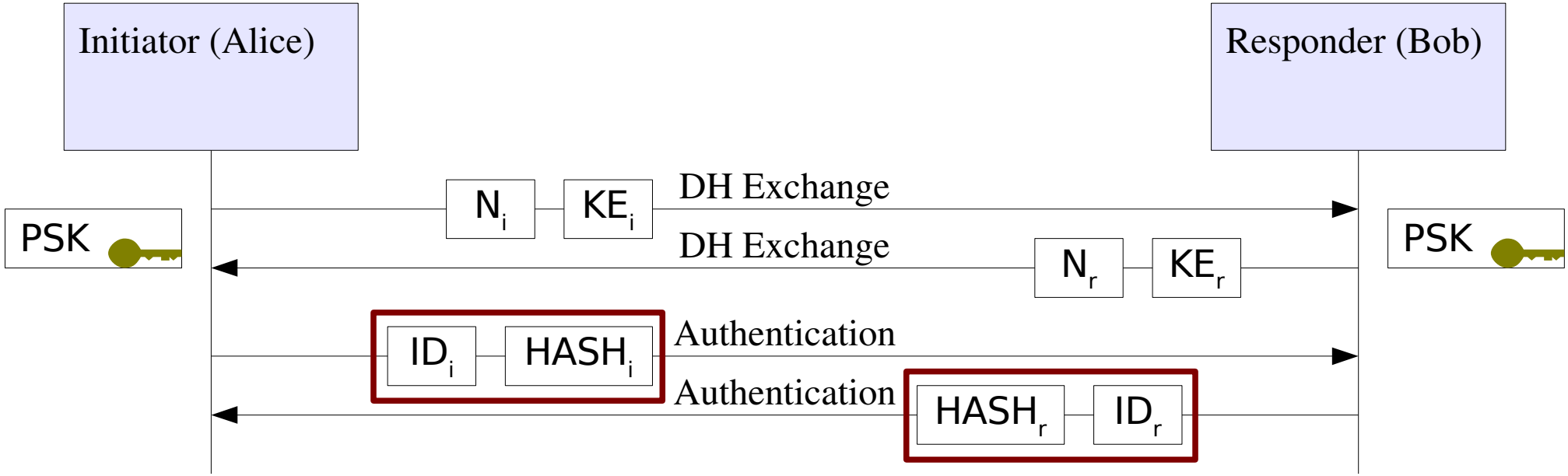
- z.B. public-Key-Kryptographie



wenn Alice N_i mit Bobs öffentlichem Schlüssel verschlüsselt,
dann kann nur Bob N_i lesen (entsprechend für Bob)
nur Alice und Bob können korrekten Hash über KE_i KE_r C_i C_r N_i N_r
berechnen

4 Schlüsselaustausch
4.1 IKEv1

- z.B. vorher bekannter geheimen Schlüssel (PSK)



nur Alice und Bob können korrekten Hash über C_i C_r N_i N_r PSK berechnen
Hashes und Identitäten durch Sitzungsschlüssel geschützt übertragen

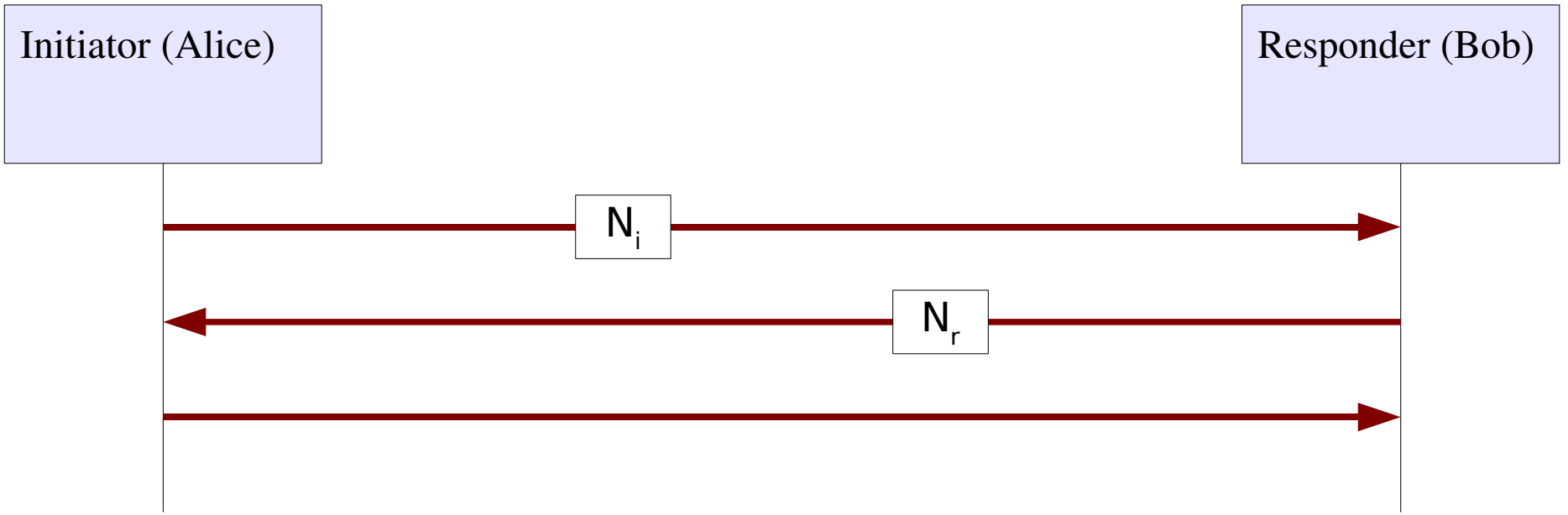
wichtig für späteres Verständnis: Alice muss $HASH_i$ berechnen, bevor Sie Identifizierung ID_r von Bob erhalten hat!

4 Schlüsselaustausch
4.1 IKEv1

- Schlüsselmaterial: C_i C_r N_i N_r KE
- gemeinsame Sitzungsschlüssel wird erzeugt; für weitere Kommunikation verwendet
  - Verwendung des Schlüsselmaterials von Authentisierungsmethode abhängig
- Aggressive mode Variante des Austauschs
  - weniger Nachrichten
  - anfälliger für DoS-Angriffe
  - Identität

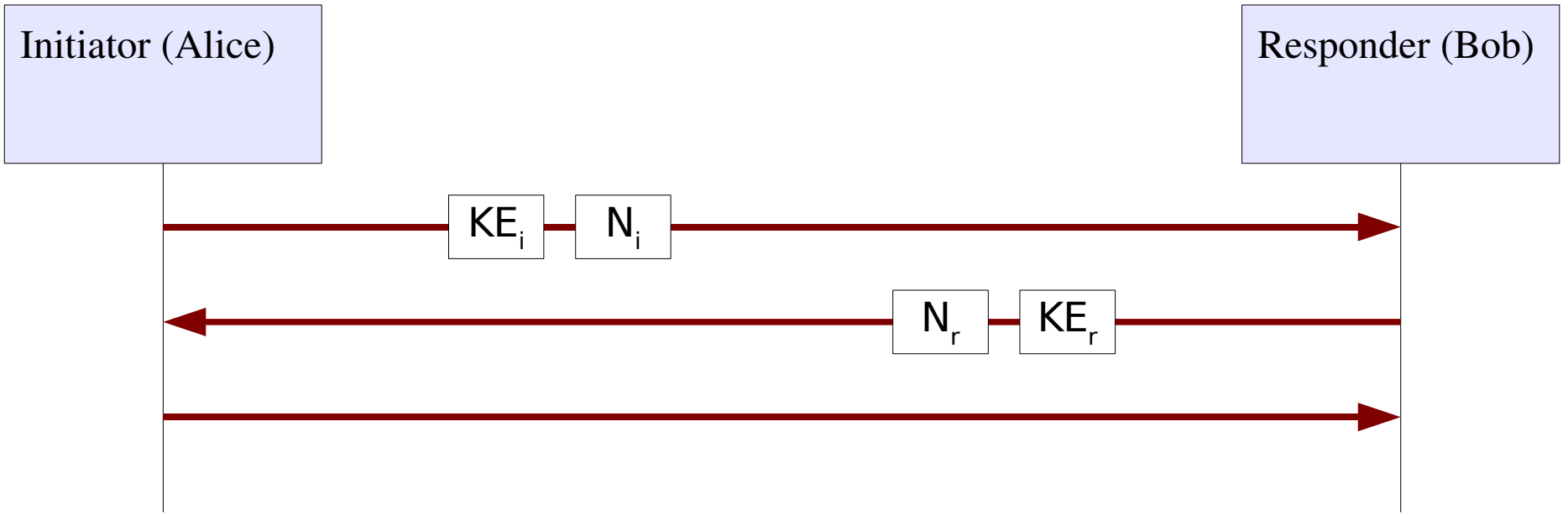
4 Schlüsselaustausch
4.1 IKEv1

- Phase 2: In etabliertem sicheren Kanal Material für IPSec-SAs Austauschen



4 Schlüsselaustausch
4.1 IKEv1

- optional: weiterer DH-Austausch (PFS)



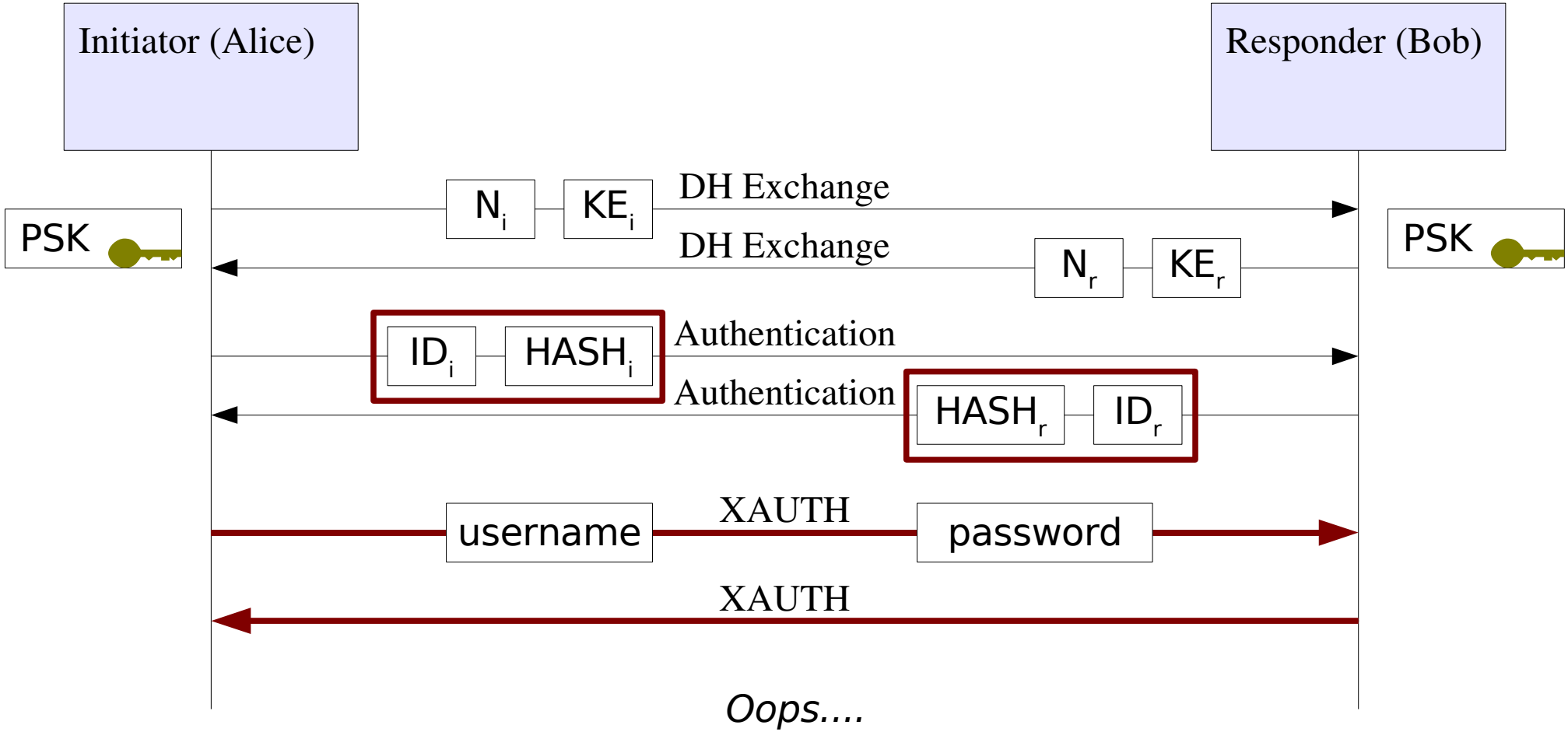
4 Schlüsselaustausch
4.1 IKEv1

- Public-Key-Kryptographie in IKE erfordert PKI
- IKE erlaubt Übertragung von Zertifikaten in Phase 1
  - Schlüssel müssen nicht mehr an alle IKE-Instanzen verteilt werden
  - Schlüssel vertrauen, wenn Zertifikat durch vertrauenswürdige Zertifizierungsinstanz signiert ist
  - "nur noch" Vertrauensbeziehungen zu Zertifizierungsinstanz herstellen

4 Schlüsselaustausch
4.2 XAUTH

- insbesondere von Cisco forciert, um "legacy authentication systems" zu integrieren
  - Zertifikate manchen zu umständlich
  - "preshared key": vor Schlüsselermittlung nur IP-Adresse von Partner bekannt
    - "Auswahl" von Key nur anhand IP – was ist mit DHCP?
  - "nachträgliche" Nutzerauthentisierung in zusätzlicher Phase zwischen Phase 1 und Phase 2

4 Schlüsselaustausch
4.2 XAUTH



Ende