VPN-Systeme

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Einleitung: Definitionen und Ziele
- Konzepte von VPNs und Anwendungsformen
- Ansätze für VPN Lösungen
- IPSec - Standard
- IPSec Schlüssel-Management (IKE)
- Praktischer Einsatz von VPNs
- IPSec Client
- Zusammenfassung

Inhalt

- **Einleitung: Definitionen und Ziele**
- Konzepte von VPNs und Anwendungsformen
- Ansätze für VPN Lösungen
- IPSec - Standard
- IPSec Schlüssel-Management (IKE)
- Praktischer Einsatz von VPNs
- IPSec Client
- Zusammenfassung

Der Begriff VPN

- In der Fachliteratur wird der Begriff VPN in zwei verschiedenen Bedeutungen verwendet:

  1. als eine **Methode von Bandbreiten-Management** und Quality of Service (QoS) oder

  2. als Möglichkeit zur **Realisierung einer vertrauenswürdigen Kommunikation** mit Hilfe von kryptographischen und anderen Sicherheitsfunktionen

Definition von VPN

Definition »V... P... N...«

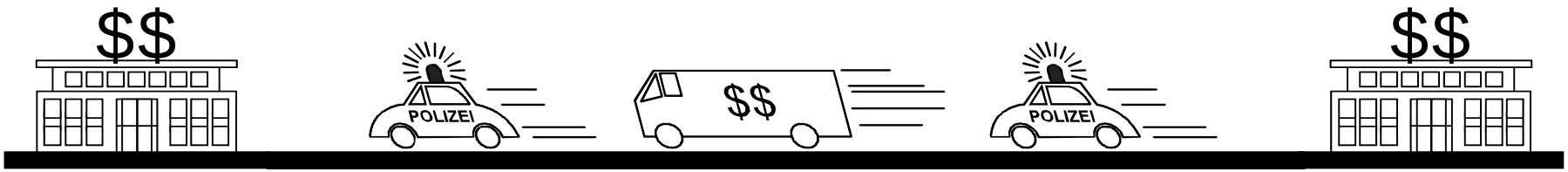
- **»Virtual«** bedeutet, dass es sich – aus Anwendersicht – scheinbar um nur »ein« Netzwerk handelt, auch wenn sich viele reale Teilnetzwerke hinter »einem« VPN verbergen.

- **»Private«** bedeutet, dass die Kommunikation vertrauenswürdig – also nicht öffentlich – durchgeführt und das Risiko eines Schadens bei der Übertragung minimiert wird.

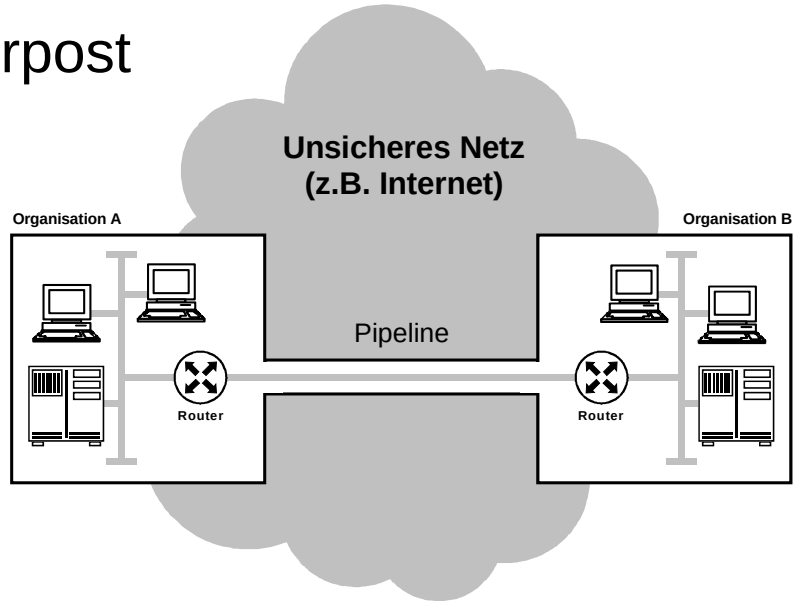
- **»Network«** bedeutet, dass eine definierte Gruppe von Rechnersystemen miteinander verbunden wird und mit Hilfe eines Protokolls (typischerweise ist das die TCP/IP-Protokollfamilie) kommuniziert.

Analogien

- Sicherheitstransporter



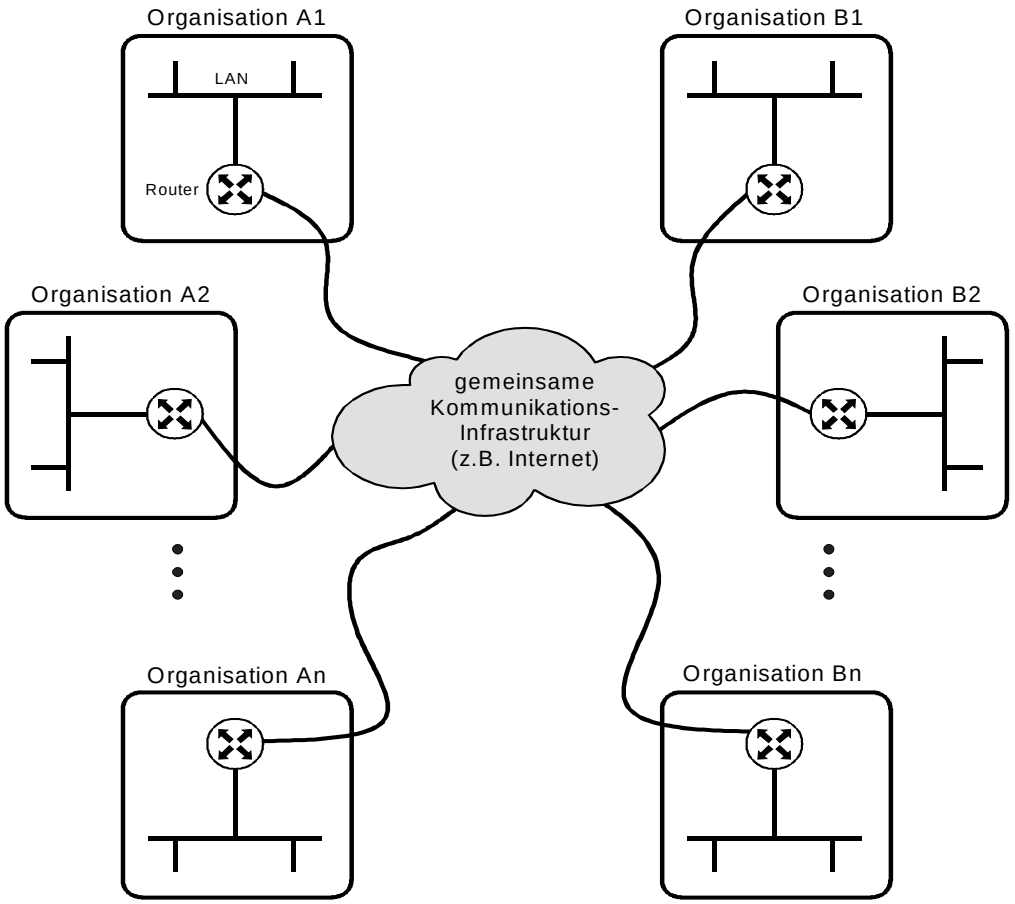
- Pipeline und Rohrpost



Realisierungsansätze
→ Übersicht

Kopplung von Organisationseinheiten

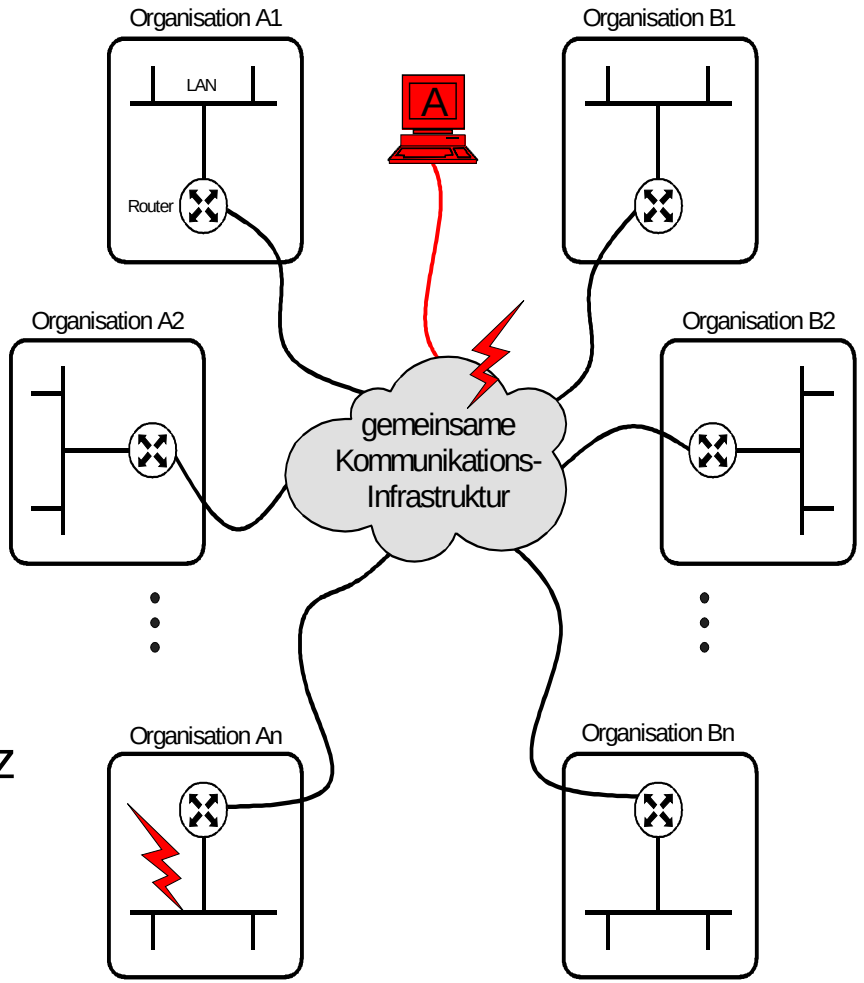
1. Corporate Network
2. Öffentliche Kommunikationsinfrastruktur



Realisierungsansätze
→ Risiken

- **Angriff auf die übertragenen Daten**
  - Mitlesen
  - Manipulation
  - Löschen
  - Verkehrsflußanalyse

- **Angriff auf die Rechnersysteme**
  - High-Tech-Spione stehlen Know-How- oder Strategiepläne
  - Hacker brechen in das lokale Netz ein und können Rechnersysteme einer gesamten Organisation lahmlegen



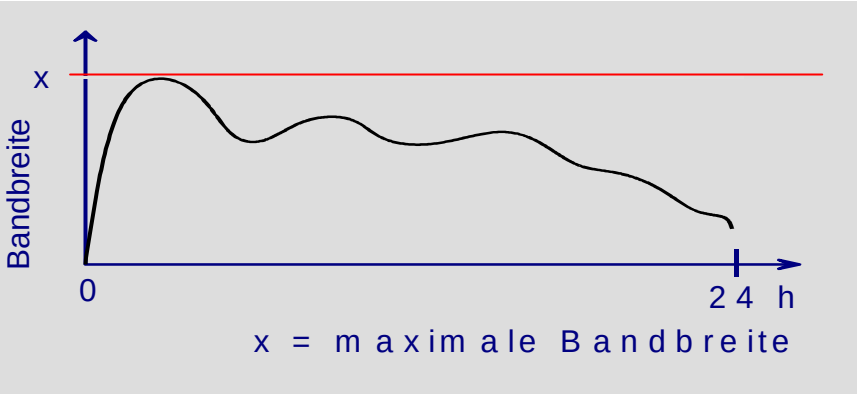
Realisierungsansätze
→ Corporate Network: ein eigenständiges Netz

Vorteile

- Freiheit bei der Gestaltung der Kommunikationsinfrastruktur
- Höhere Sicherheit und zugleich höhere Verfügbarkeit
- Nutzung als Intranet
- Eigene Security Policy können auf allen Ebenen eigenverantwortlich durchgesetzt werden

Nachteile

- Investitionen, Betrieb und Wartung müssen selbst getragen werden
- Neue Innovationen im IT-Bereich zwingen jeweils zu neuen Investitionen
- Maximaler Durchsatz bestimmt die maximale Bandbreite



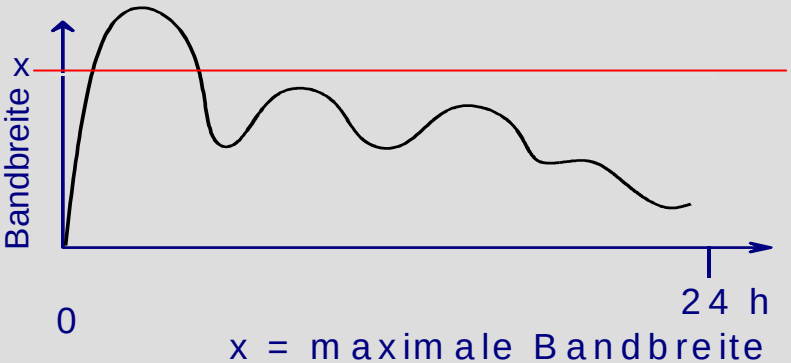
Realisierungsansätze
→ Öffentliche Kommunikationsinfrastruktur

Vorteile

- Innovationen durch die Anbieter stehen unmittelbar zur Verfügung, ohne eigene Investitionen.
- Niedrigere Kosten für öffentliche Kommunikationsinfrastruktur.
- Flexible Kommunikation mit Kunden, Lieferanten, Geschäftspartnern, da offen.
- Verantwortlichkeit des Anbieters für die Servicequalität im puncto Verfügbarkeit, Performance und Management.
- Relativ hoher Schutz, der schnell zur Verfügung steht.

Nachteile

- Abhängigkeit des Anwenders vom Anbieter und dessen Sicherheitsstrategie.
- Nicht einheitlicher Schutzbedarf.
- Definition der Security-Policy des Anbieters nicht immer eindeutig.
- Die Eintrittswahrscheinlichkeit eines Angriffes ist sehr hoch.



Aufbau von Virtual Private Networks

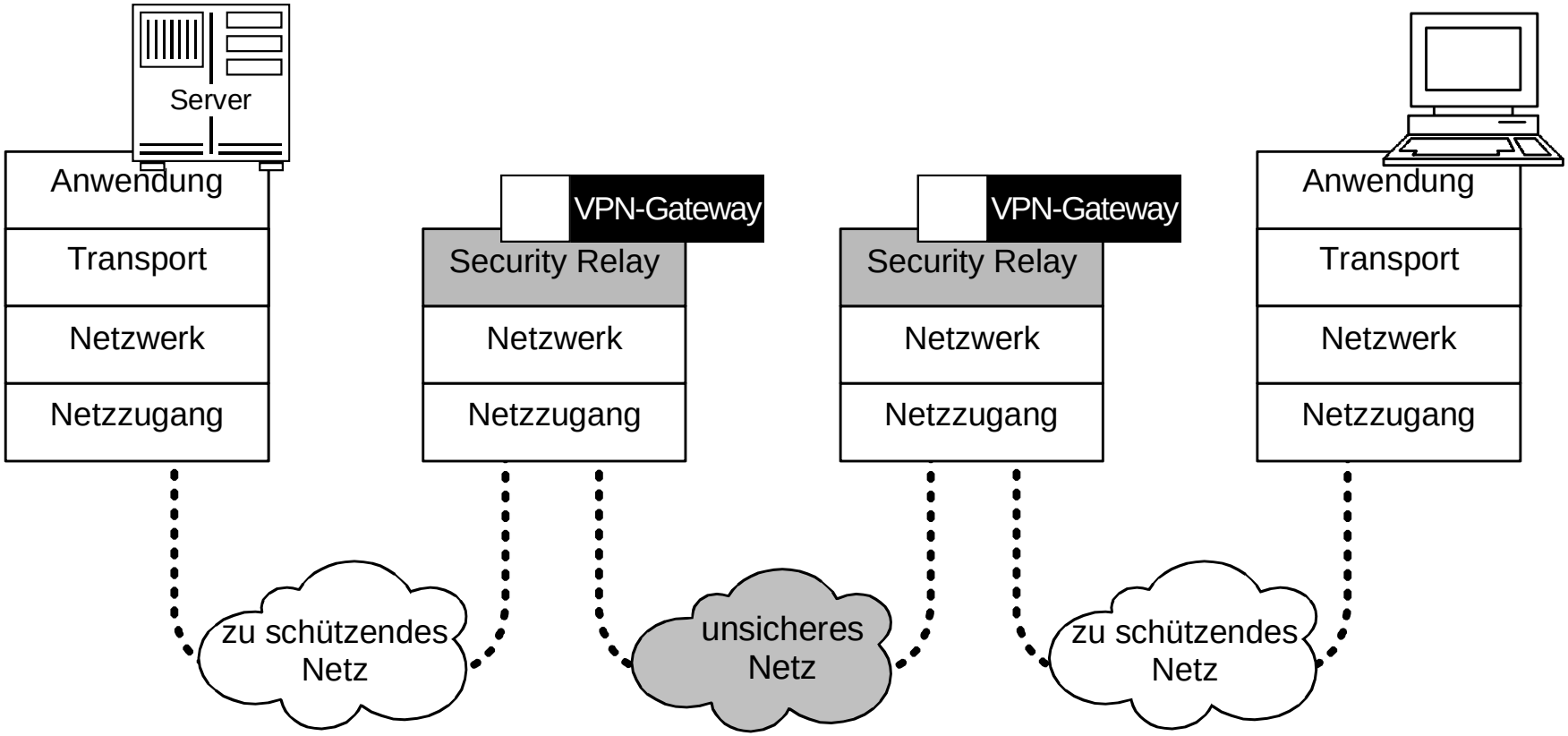
- **Grundsätzliche Idee bei Virtual Private Networks (VPNs):**
  - offene Kommunikationsinfrastruktur z.B. Internet nutzen
    - kostengünstig,
    - weltweit verfügbar **UND**
  - **allen Bedrohungen und Risiken sinnvoll entgegenwirken**

- **Sicherheitsmechanismen von VPNs**
  - Verschlüsselung (schützt Vertraulichkeit)
  - Authentikation (gewährleistet Eindeutigkeit des Benutzers)
  - MAC-Funktionen (sorgen für die Unversehrtheit der Daten)
  - Tunneling (verschleiert Datentransfer)
  - Firewalling (schützt Netzwerkressourcen)

Inhalt

- Einleitung: Definitionen und Ziele
- **Konzepte von VPNs und Anwendungsformen**
- Ansätze für VPN Lösungen
- IPSec - Standard
- IPSec Schlüssel-Management (IKE)
- Praktischer Einsatz von VPNs
- IPSec Client
- Zusammenfassung

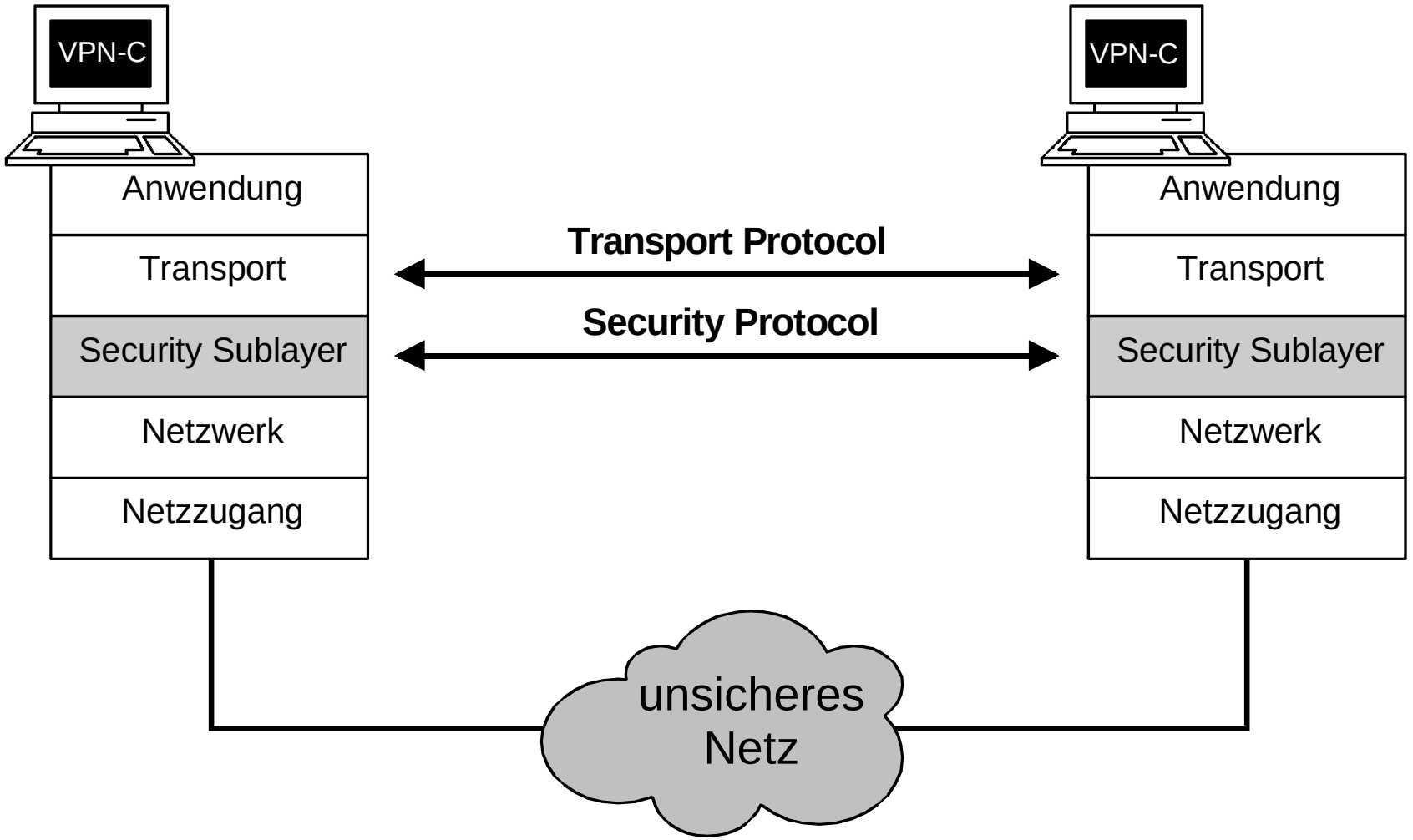
Konzepte
→ VPN-Gateway



Konzepte
→ Vorteile einer VPN-Gateway-Lösung

- Die Gateway-Lösung ist **unabhängig von Workstations** (PCs, UNIX-Systeme, Host-Rechner, ...) **und deren Betriebssystemen** (Microsoft DOS, Microsoft Windows 95/98/NT/2000/..., OS/2, LINUX, VMS usw.).
- Die Gateway-Lösung erlaubt die **Einrichtung von Sicherheitsfunktionen** zwischen Endsystemen, in die ansonsten keine Sicherheitsfunktionen integriert werden könnten (z.B. Terminals).
- Bei heterogenen Systemen (unterschiedliche Hardware, Software, Betriebssysteme, ...) kann **immer das gleiche Gateway** verwendet werden, wodurch sich der notwendige Aufwand verringert.
- Gateways sind **leichter »sicher« zu realisieren** als spezielle Software-Lösungen in Rechnersystemen und sie sind **immer ansprechbar**.
- Die Sicherheitseinrichtungen sind hinsichtlich der Sicherheitsqualität **unabhängig von anderen Systemkomponenten**.
- Die Sicherheit ist **anwendungsunabhängig**.

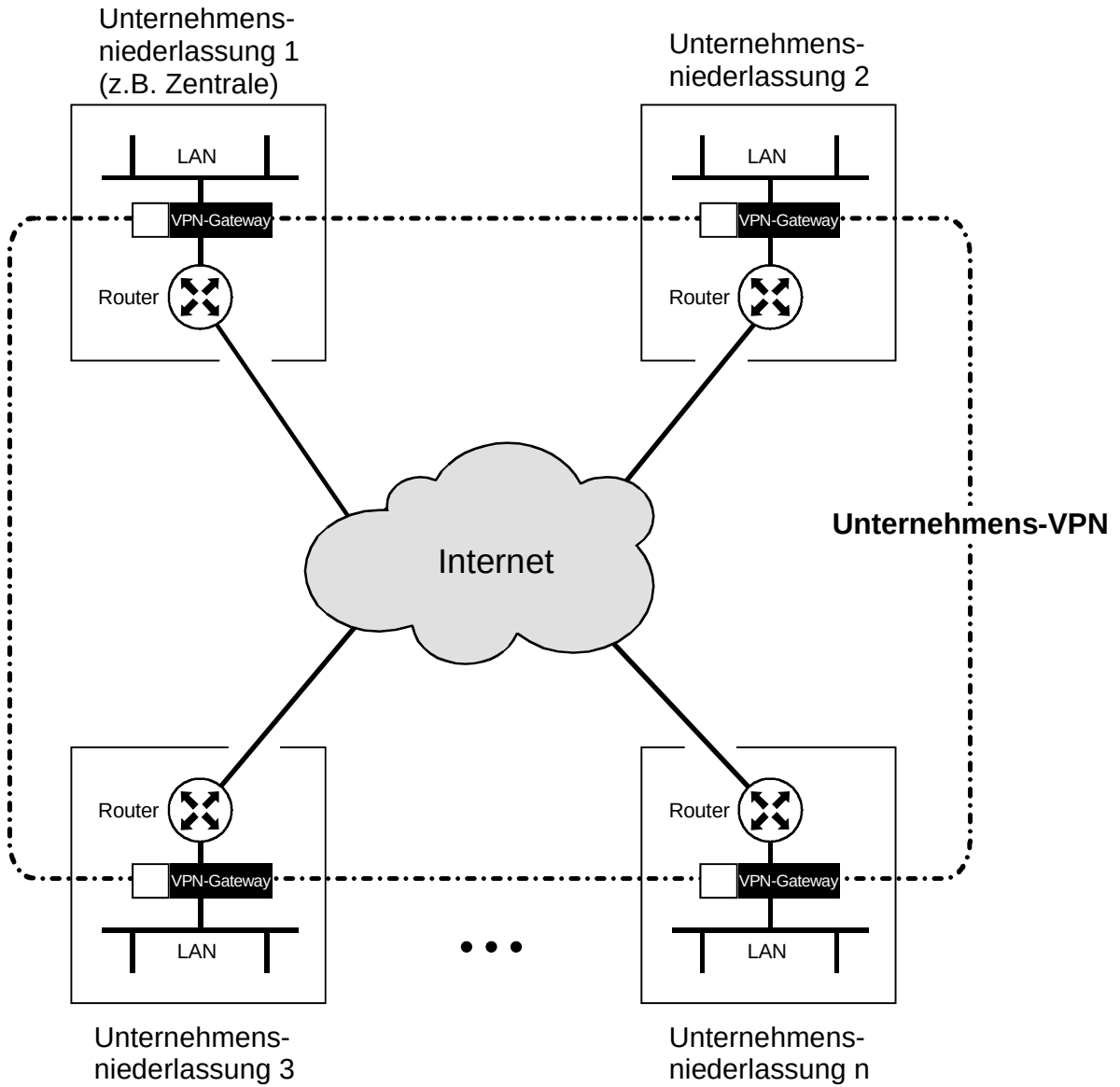
Konzepte
→ VPN-Client



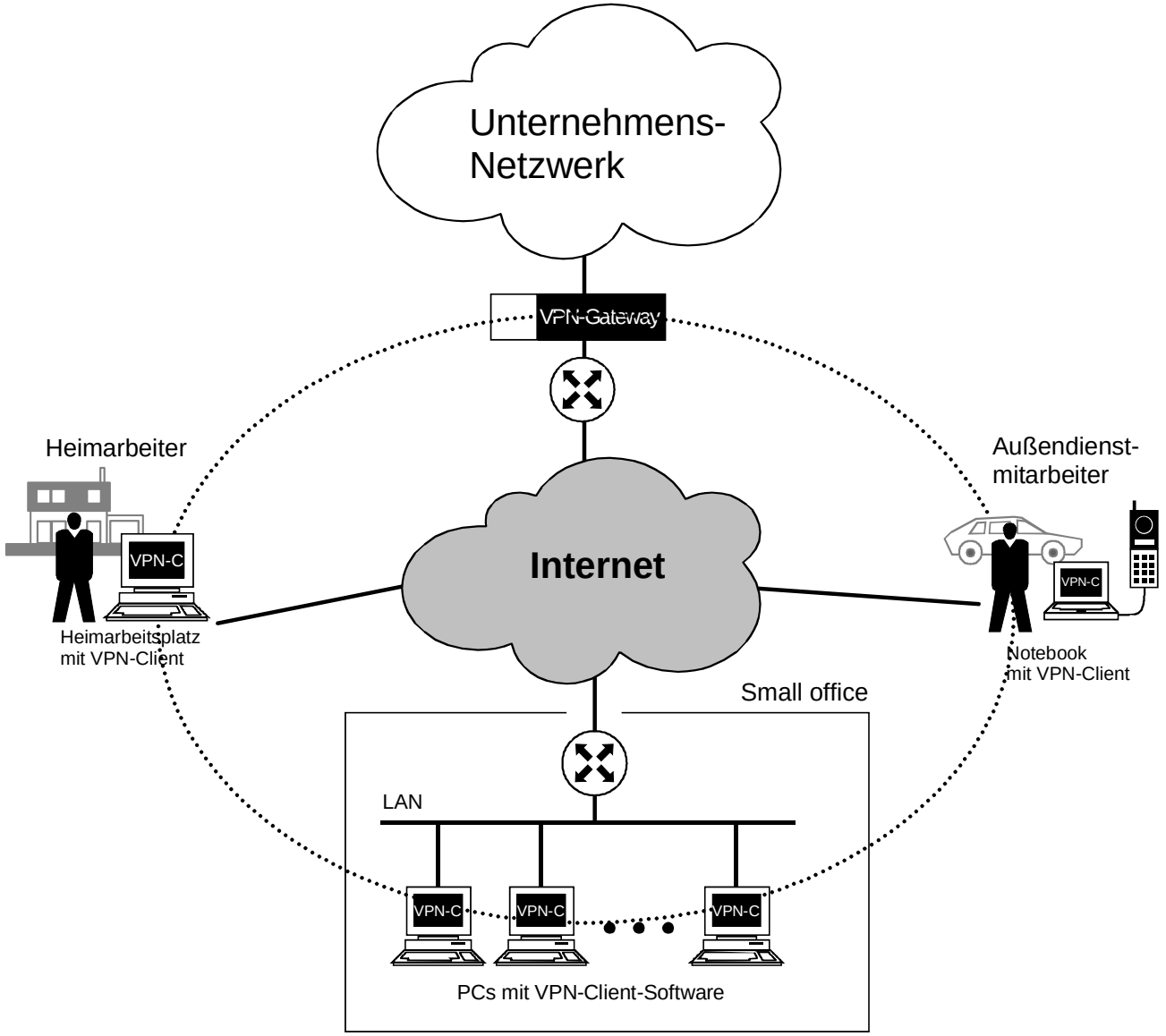
Konzepte
→ Vorteile einer VPN-Client-Lösung

- Der VPN-Client ist **kostengünstiger** als die VPN-Gateway-Lösung.
- Der VPN-Client bietet **End-to-End-Sicherheit**.
  Das bedeutet, dass nicht nur die Verbindung zwischen verschiedenen LAN-Segmenten nach außen hin abgeschottet wird, sondern auch jede einzelne Workstation (PC) gegenüber anderen.
- Eine **»Person« kann authentisiert werden**.

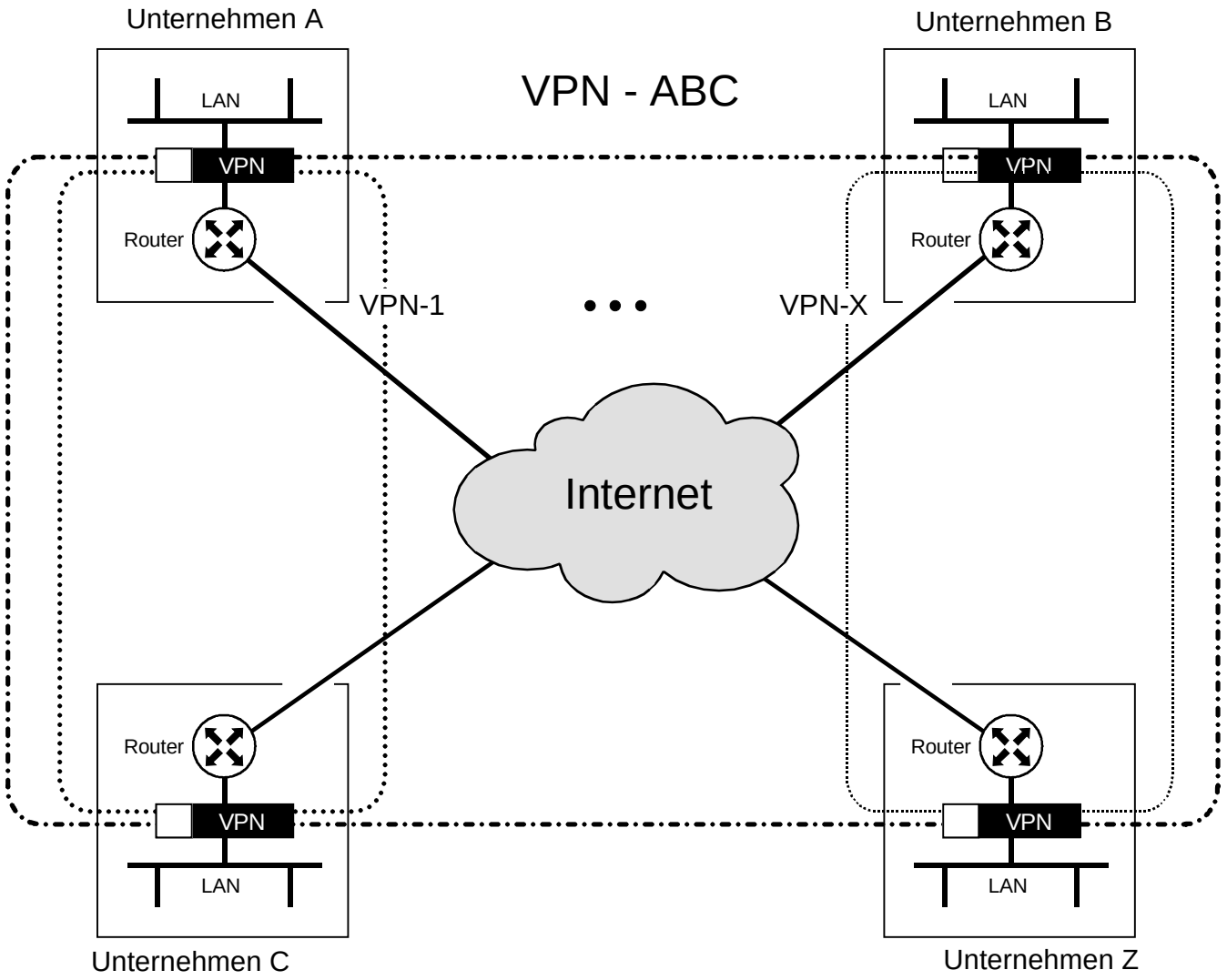
Anwendungsformen von VPNs (1/4)
→ Unternehmensweites VPN



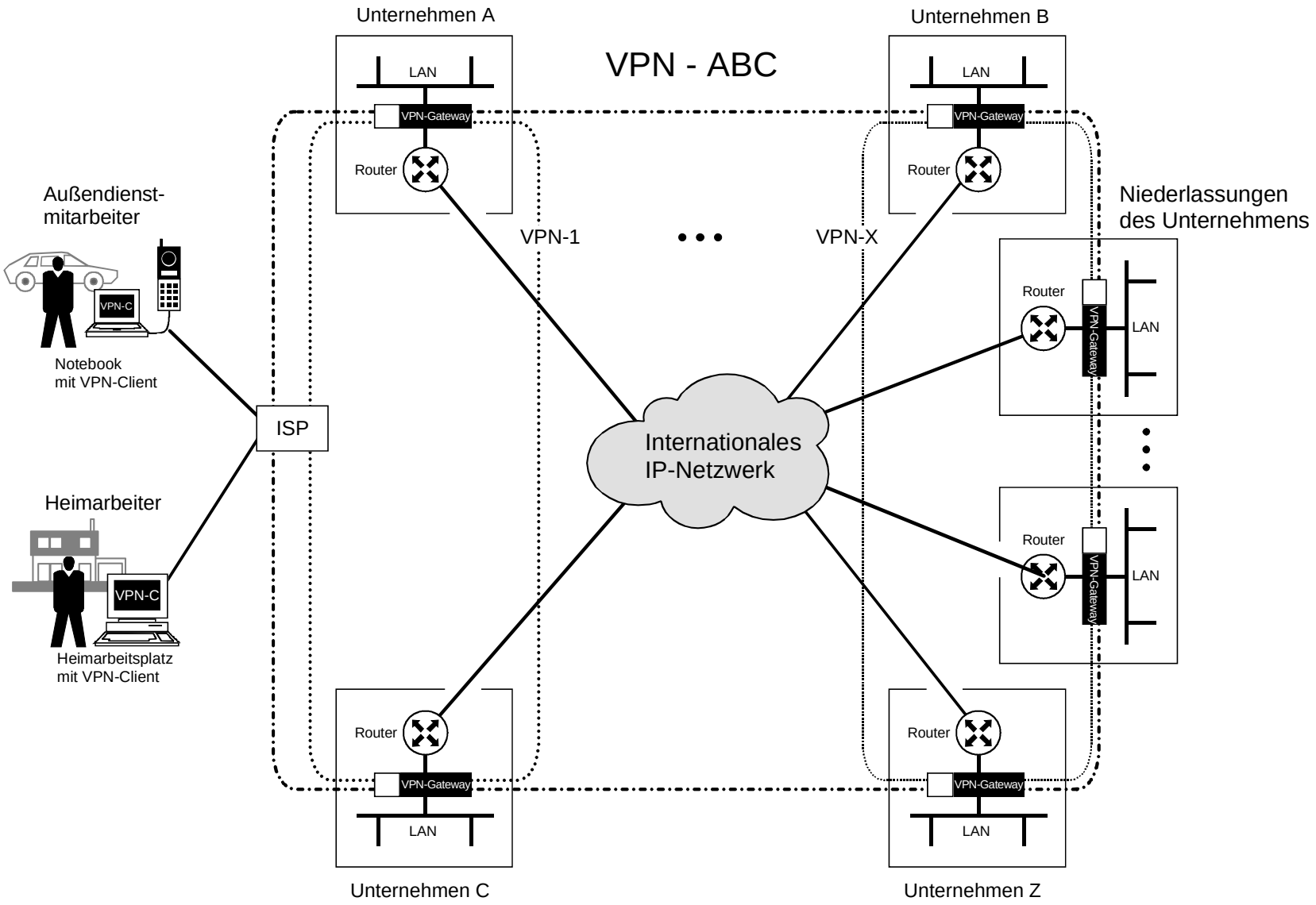
Anwendungsformen von VPNs (2/4)
→ Sichere Remote-Ankopplung



Anwendungsformen von VPNs (3/4)
→ VPN zwischen verschiedenen Unternehmen



Anwendungsformen von VPNs (4/4)
→ Kombination der Anwendungsformen



Inhalt

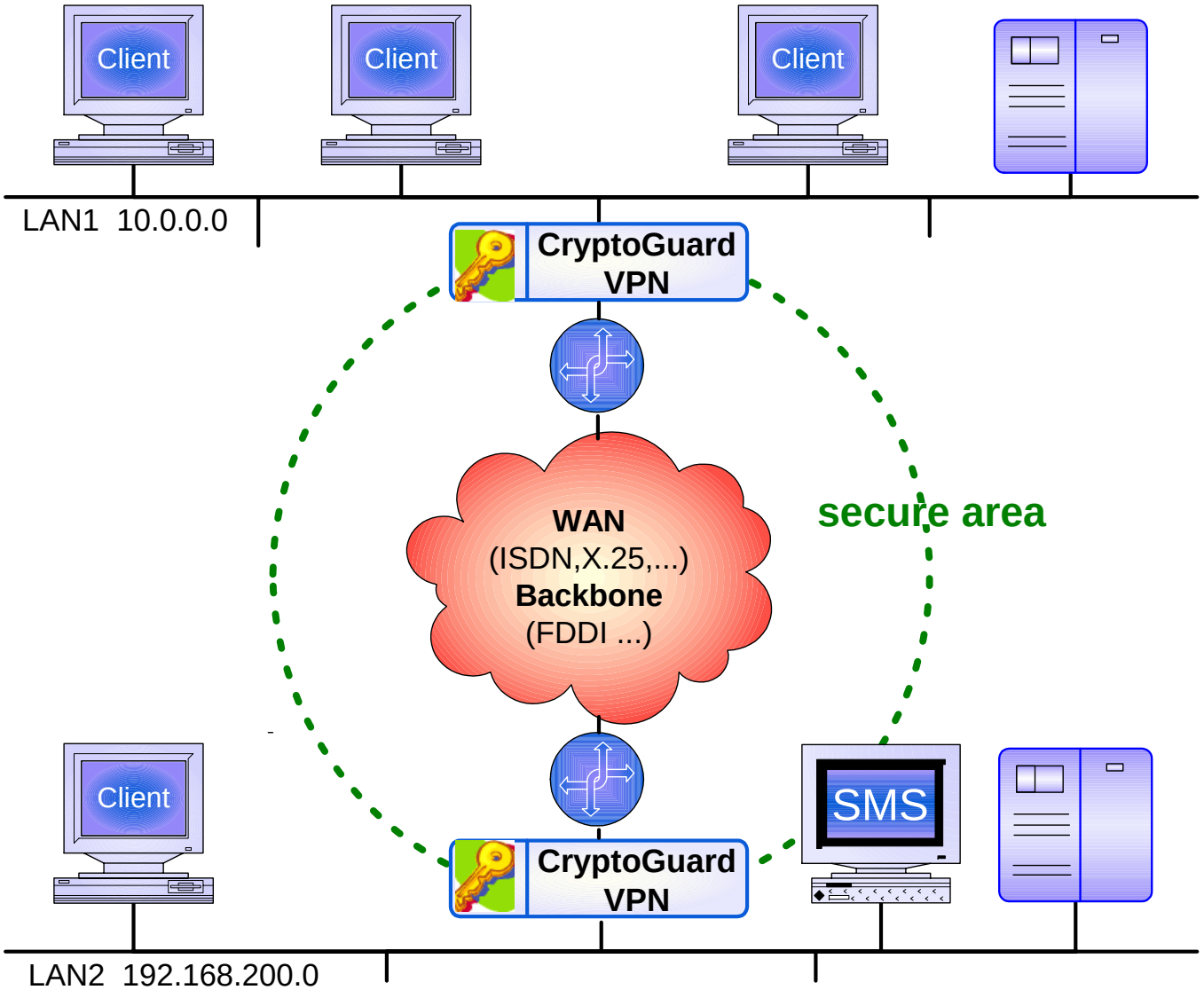
- Einleitung: Definitionen und Ziele
- Konzepte von VPNs und Anwendungsformen
- **Ansätze für VPN Lösungen**
- IPSec - Standard
- IPSec Schlüssel-Management (IKE)
- Praktischer Einsatz von VPNs
- IPSec Client
- Zusammenfassung

Ansätze für VPN Lösungen
→ Allgemein

- **Spezielle Security-Protokolle für einen geschwindigkeitsoptimierten Ansatz**
  - Absolute Transparenz,
  - Sehr geringe Verzögerungszeiten,
  - Quality of Service (keine Verschlüsselung des TCP/UDP-Headers)
  - Kein Overhead während der Kommunikation (Header, Fragmentierung,...),
  - Abhängig von Herstellern.
  - **Beispiel: CryptoGuard VPN**

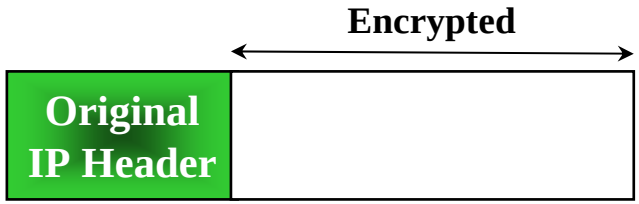
- **IPSec: Internet-Sicherheitsstandard**
  - Zwei Mechanismen (Authentication Header und Encapsulated Security Payload),
  - Beide Mechanismen mit Tunneling kombinierbar,
  - Herstellerübergreifend (wünschenswert ??? !!!)

Ein Ansatz: CryptoGuard VPN
→ Übersicht



Ein Ansatz: CryptoGuard VPN
→ Verschlüsselungsmode

- **Beispiel: IP**



- **Protokolle (Schicht 2 bis 4)**
  - Neben IP
    DIX2, IEEE802.3, IEEE802.3, OSI-CLNO, ICMP, TCP, UDP
- **Verschlüsselung**
  - 128 Bit ADES
    (in jeder zweiten Runde wird ein unterschiedlicher Schlüssel verwendet)
  - CFB-Mode (auf Byte Ebene)

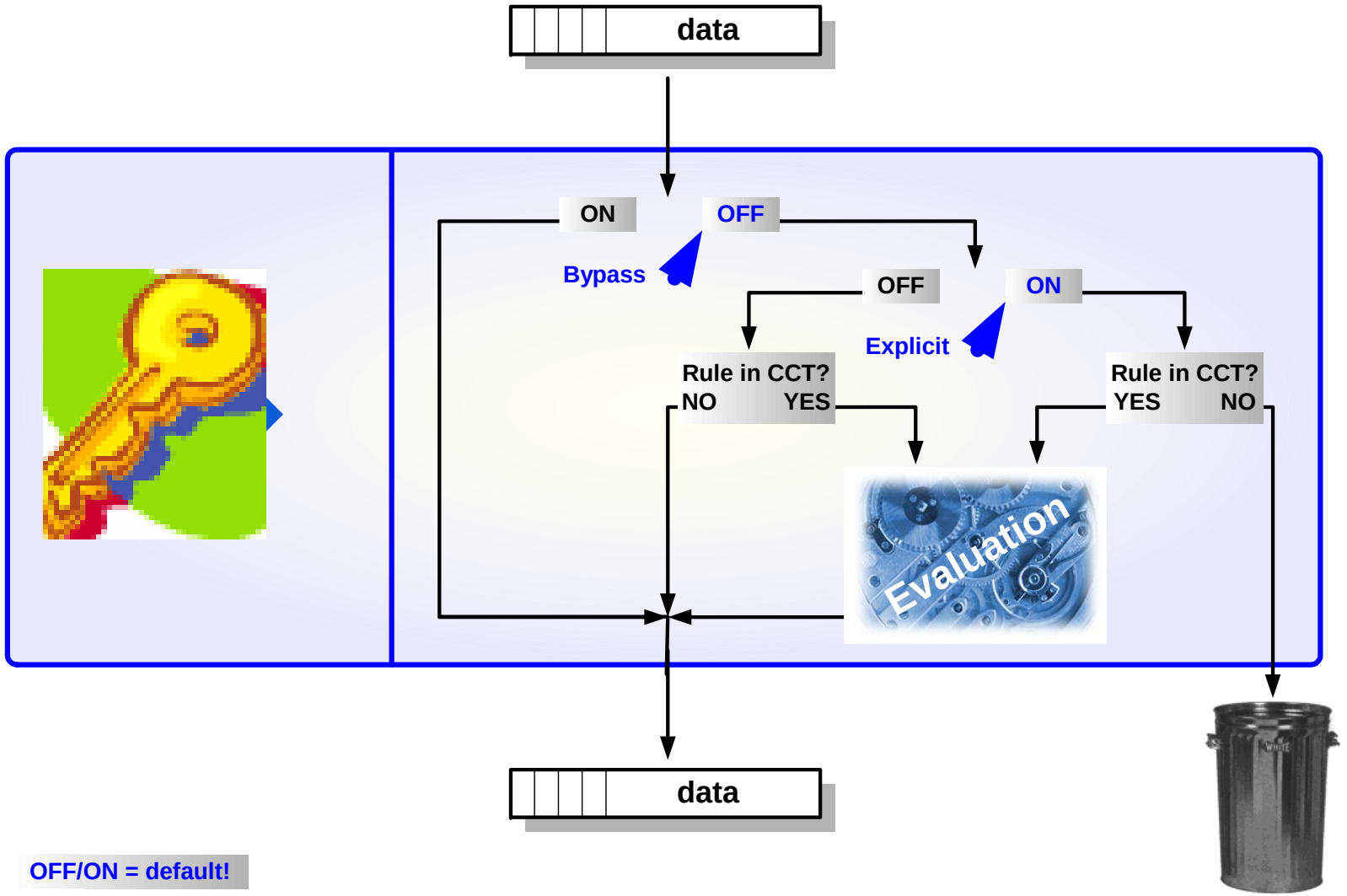
Ein Ansatz: CryptoGuard VPN
→ Schlüsselsätze

- **System Master Key Satz (SMK)**
  - 3 Schlüssel
  - 1. Satz wird über serielles Kabel geladen (Personalisierung)
  - dient der Authentikation
  - Generierung des dynamischen Verbindungsschlüssels
- **Verbindungsschlüsselsatz (CKT)**
  - 64 Schlüssel
  - über Index ausgewählt
  - Verschlüsselung der Nutzdaten
  - Wechsel eines Satzes erfolgt in allen VPN-Gateways des Systems gesteuert von der SMS.

Ein Ansatz: CryptoGuard VPN
→ Zustände

- **Manufacturing State**:
  - nach Auslieferung: Bypass
- **Personalization State**:
  - Schlüssel und IP-Adresse in der CG VPN
  - **Bypass**
- **Connection Control State**:
  - Verschlüsselung ist aktiv

Ein Ansatz: CryptoGuard VPN
→ Funktionsweise



OFF/ON = default!

Ein Ansatz: CryptoGuard VPN
→ Kommunikation mit der SMS

- **über serielles Kabel**
- **via IP**
  - Management über Port 57 UDP
    - Authentikation
    - dynamisch verschlüsselt basierend auf SMK der Box
  - Spontane Meldungen Port 87 UDP

Inhalt

- Einleitung: Definitionen und Ziele
- Konzepte von VPNs und Anwendungsformen
- Ansätze für VPN Lösungen
- **IPSec - Standard**
- IPSec Schlüssel-Management (IKE)
- Praktischer Einsatz von VPNs
- IPSec Client
- Zusammenfassung

IPSec
→ Standards (09-99)

RFC 1828 : IP Authentication using Keyed MD5	
RFC 1829 : The ESP DES-CBC Transform	
RFC 1851 : The ESP Triple DES Transform (status experimental)	
RFC 2085 : HMAC-MD5 IP Authentication with Replay Prevention	Feb 97
RFC 2104 : HMAC: Keyed-Hashing for Message Authentication	Feb 97
RFC 2401 : Security Architecture for the Internet Protocol	Nov 98
RFC 2402 : IP Authentication Header	Nov 98
RFC 2403 : The Use of HMAC-MD5-96 within ESP and AH	Nov 98
RFC 2404 : The Use of HMAC-SHA-1-96 within ESP and AH	Nov 98
RFC 2405 : The ESP DES-CBC Cipher Algorithm With Explicit IV	Nov 98
RFC 2406 : IP Encapsulating Security Payload (ESP)	Nov 98
RFC 2407 : The Internet IP Security Domain of Interpretation for ISAKMP	Nov 98
RFC 2408 : Internet Security Association and Key Management Protocol (ISAKMP)	Nov 98
RFC 2409 : The Internet Key Exchange (IKE)	Nov 98
RFC 2410 : The NULL Encryption Algorithm and Its Use With IPSec	Nov 98
RFC 2411 : IP Security Document Roadmap	
RFC 2412 : The OAKLEY Key Determination Protocol	Nov 98
RFC 2451 : The ESP CBC-Mode Cipher Algorithms	Nov 98

IPSec
→ Drafts (09-99)

The ESP Triple DES Transform

The ISAKMP Configuration Method

The Use of HMAC-RIPEMD-160-96 within ESP and AH

Dynamic configuration of IPSEC VPN host using DHCP

Extended Authentication Within ISAKMP/Oakley

A Hybrid Authentication Mode for IKE

A Framework for Group Key Management for Multicast Security

PKI Requirements for IP Security

Security Policy Specification Language

Intra-Domain Group Key Management Protocol

Security Policy System

IPSec Monitoring MIB

IPSec DOI Textual Conventions MIB

Policy Framework for IP Security

IPsec Interactions with ECN

IKE Extensions Methods

IPsec Policy Schema

The Internet Key Exchange (IKE)

The ESP SKIPJACK-CBC Cipher Algorithm With Implicit IV

Additional ECC Groups For IKE

ISAKMP DOI-Independent Monitoring MIB

Content Requirements for ISAKMP Notify Messages

Security Policy Protocol

IKE Base Mode

IPSec
→ Das sichere Internet Protokoll

- **IPSec (Internet Protocol Security)** ist ein Sicherheitsstandard für den geschützten IP-Datentransfer, der von der Internet Engineering Task Force (IETF) entwickelt wurde.
- Die Nutzung dieses Standards soll eine ”gemeinsame Sprache” verwirklichen, mit der Sicherheitsprodukte verschiedener Hersteller miteinander sicher kommunizieren können.
- IPSec ergänzt das bestehende IPv4 um folgende Sicherheitsfunktionen:
  - Jedes Paket kann **gegen Manipulation geschützt werden**
  - Jedes Paket kann **verschlüsselt werden**
  - Jedes Paket kann **vor Wiedereinspielung geschützt werden**
  - Die IP-Kommunikation kann **gegen Verkehrsflußanalyse geschützt werden.**
  - Die Kommunikationspartner (Personen oder VPN-Gateways) **können authentisiert werden.**

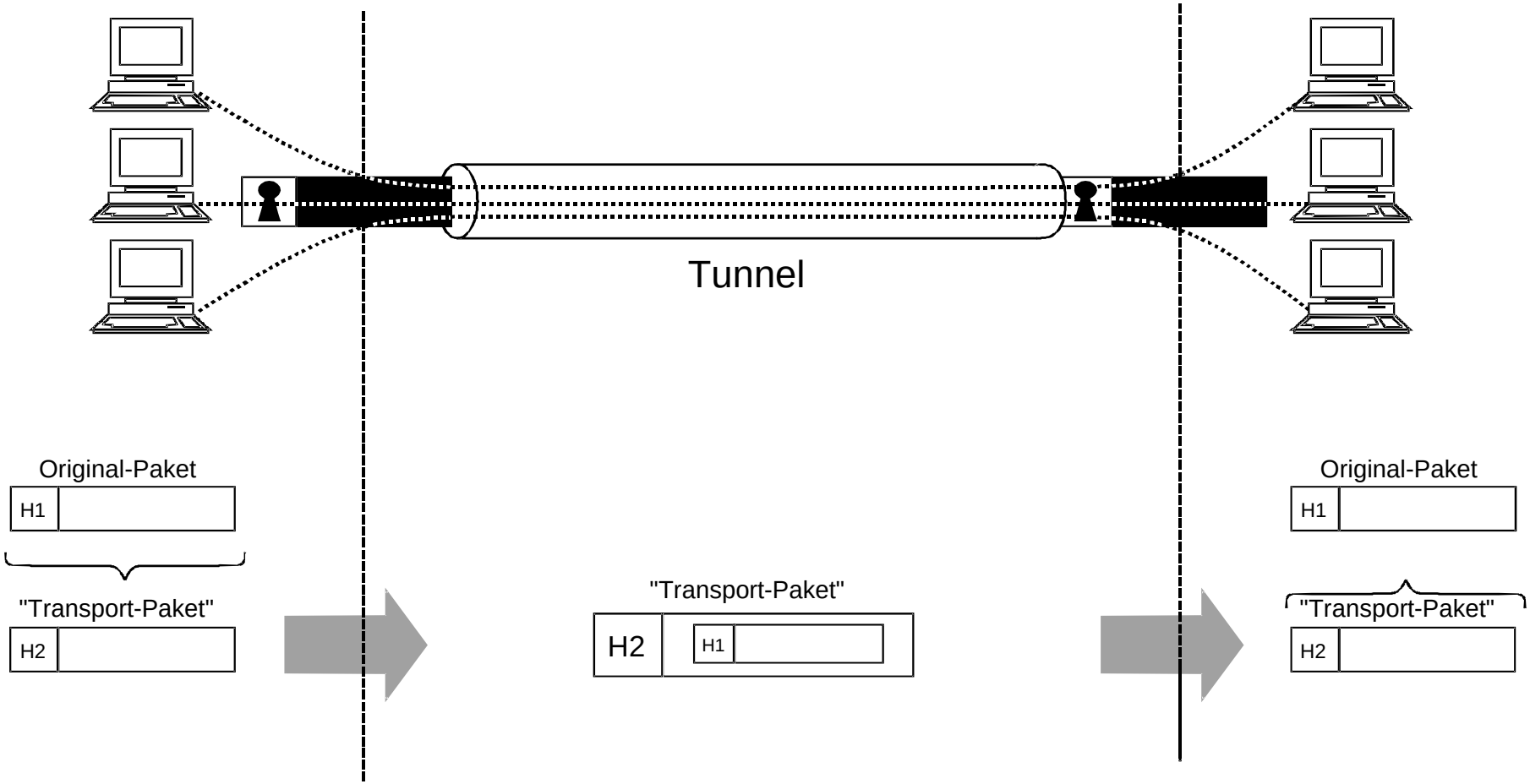
IPSec
→ Übersicht der Mechanismen

- IPSec realisiert die **zusätzlich Sicherheit** durch das Einfügen **zusätzlicher Informationen (Header)** in die IP Pakete.
- Diese Zusätze bezeichnet man als:
  - **Authentication Header** (AH, RFC 2402)
    - Datenunversehrtheit
    - Authentikation
    - Anti-replay Service (Optional)
  - **Encapsulated Security Payload** (ESP, RFC 2406)
    - Datenunversehrtheit und Authentikation (Optional)
    - Anti-replay Service (Optional)
    - Verschlüsselung (Optional)

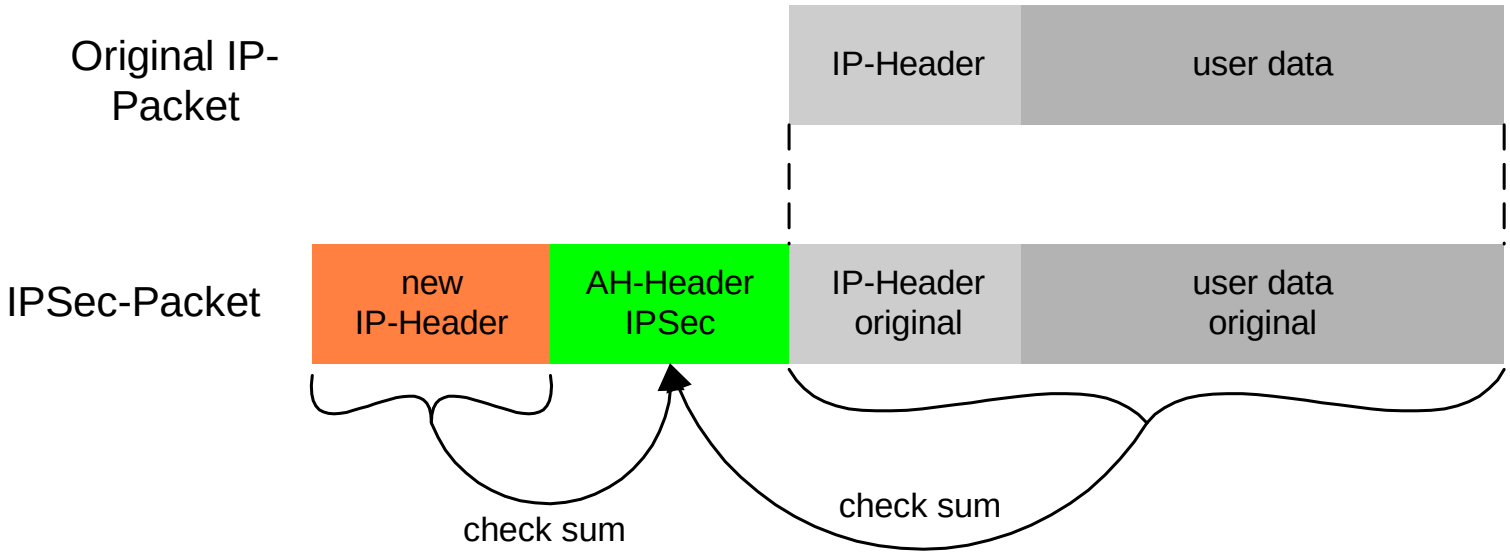
'Transport-Mode' = Verschlüsselung der Nutzdaten

'Tunnel-Mode' = Verschlüsselung des IP-Headers und der Nutzdaten

IPSec Tunneling
→ Idee

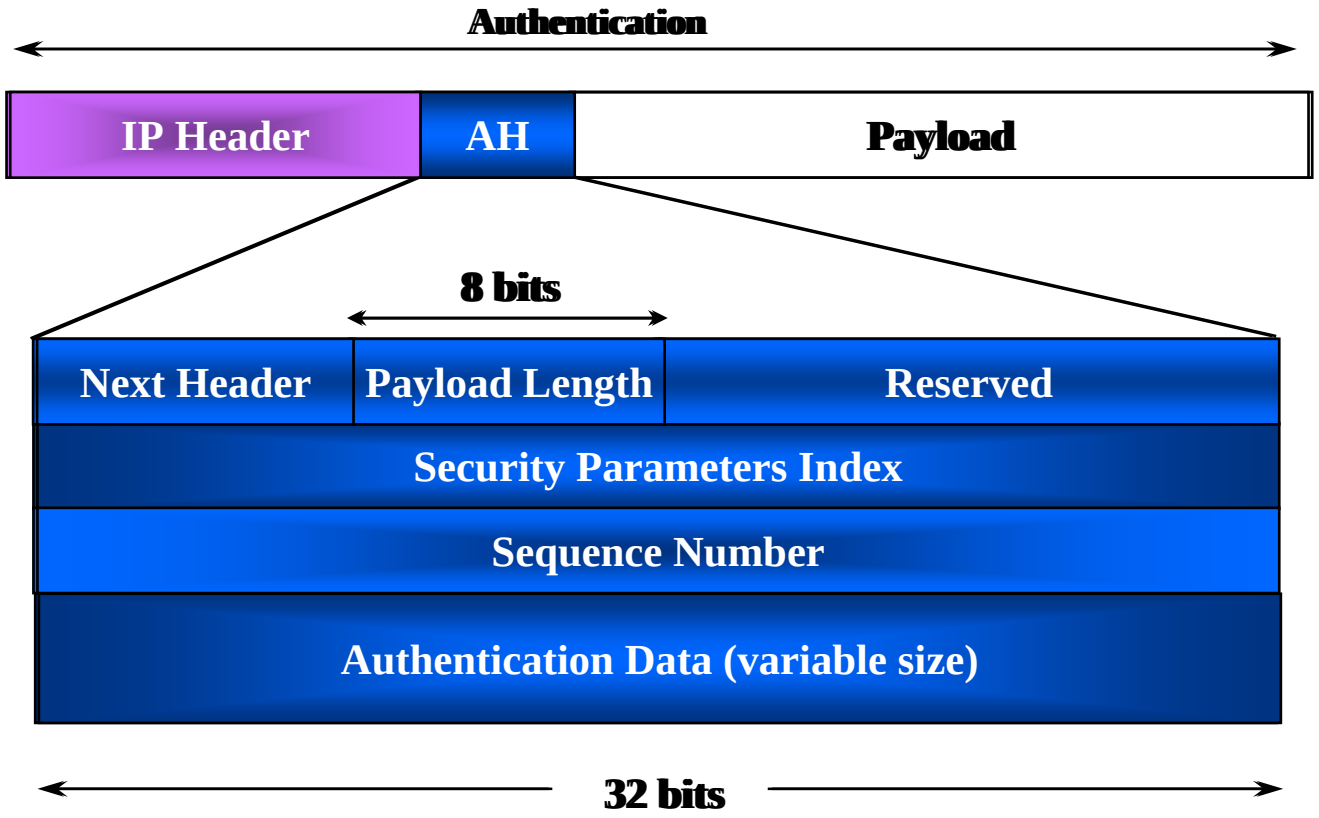


Authentication Header (Tunnel-Mode)
→ Übersicht



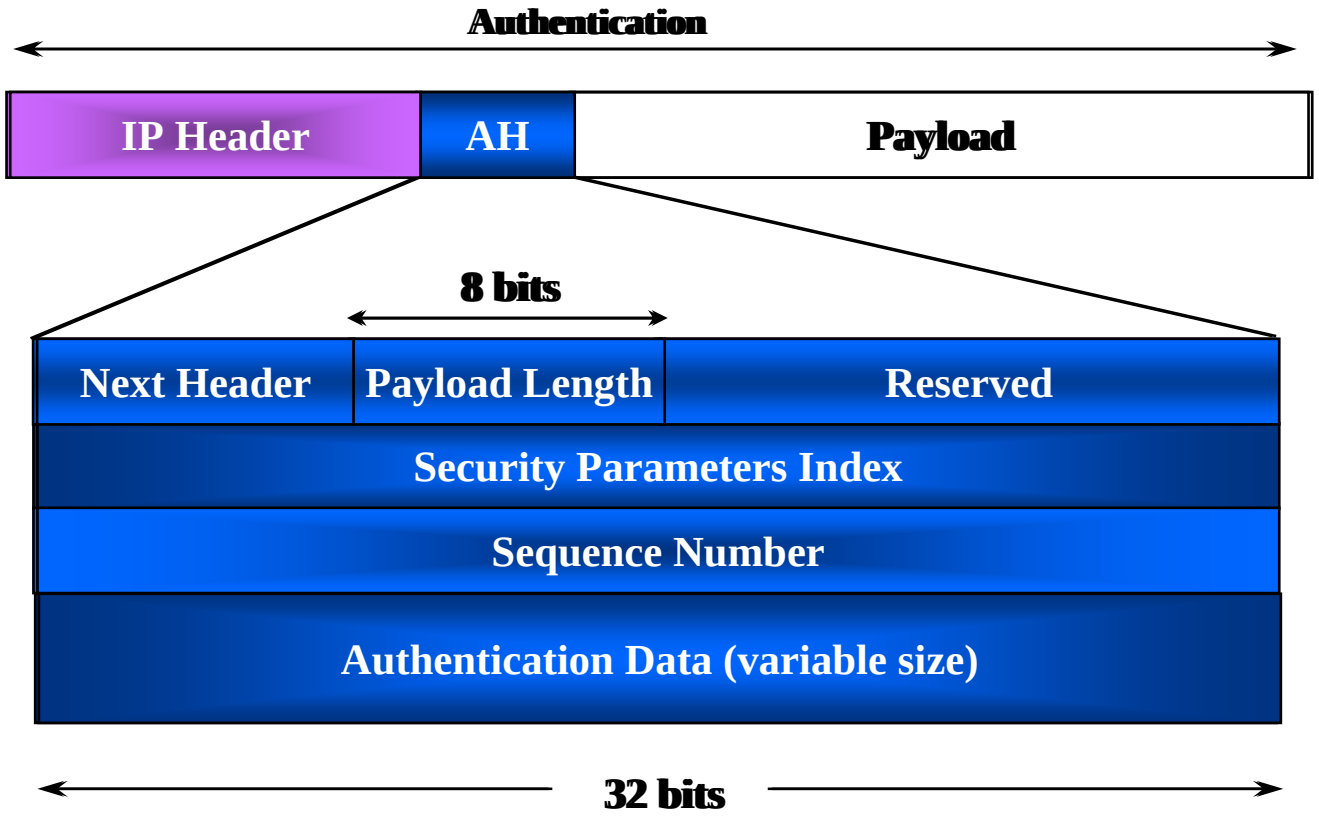
- Starke Integrität und Authentizität der IP Pakete
- HMAC (z.B. mit SHA-1) über das gesamte IP Paket, außer
  - Feldern, die während des Transportes modifiziert werden (Time to Live (TTL), TOS, Flags, Header Checksum, ...)
  - dem Authentication-Feld selbst

Authentication Header (AH)
→ Beschreibung des Headers (1/2)



- **Next Header** ist ein 8-Bit Feld, das den Typ der nächsten Daten hinter dem Authentication Header identifiziert.
- **Payload Length** (8 Bit-Feld) beschreibt die Länge des AH in 32-bit Worten.
- **Reserved** ist reserviert für zukünftige Funktionen.

Authentication Header (AH)
→ Beschreibung des Headers (2/2)

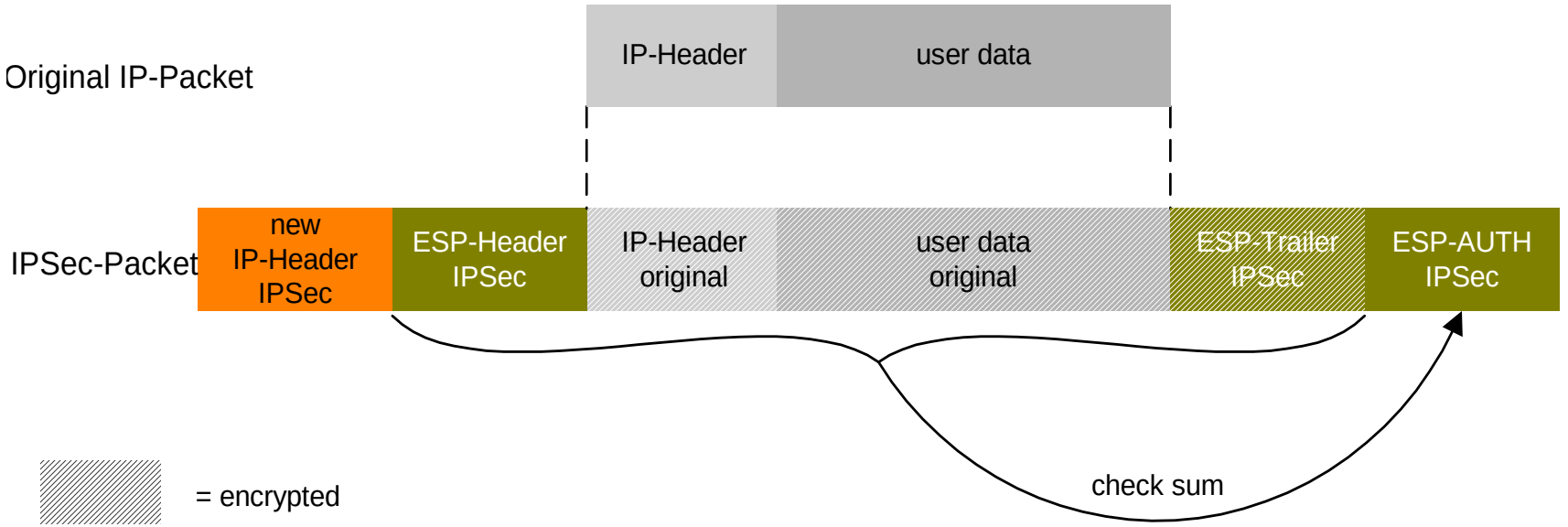


- **SPI** ist ein beliebiger 32-Bit Wert, der in Kombination mit der Ziel IP-Adresse und dem Security Protocol (AH) eindeutig die Security Association für dieses Paket definiert.
- **Sequence Number** (32 Bit-Feld) beinhaltet einen Zähler (Replay-Angriff).
- **Authentication Data** ist ein Feld mit variabler Länge, das die Integrity Check Value (ICV) dieses Paketes enthält (Ergebnis von HMAC).

Authentication Header (AH)
→ Zusammenfassung

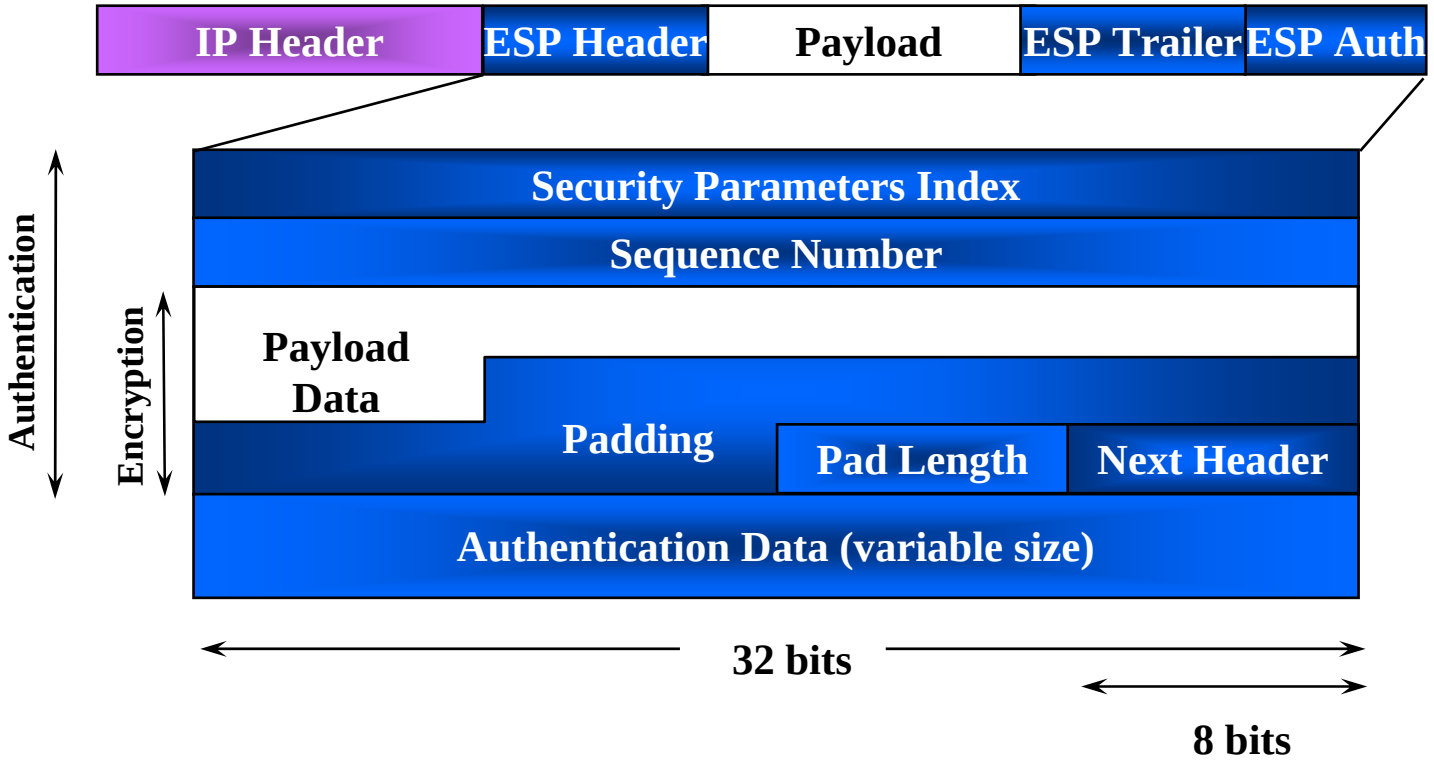
- Mit der AH-Datenstruktur kann gewährleistet werden, dass eine eventuelle **Manipulation von Daten** auf dem Weg durch das Netzwerk entdeckt wird.
- Außerdem findet die **Authentikation des Absenders** der Pakete statt.
- Beim ausschließlichen Einsatz des AH-Headers findet keine Verschlüsselung über IPSec statt.

Encapsulated Security Payload (Tunnel-Mode)
→ Übersicht



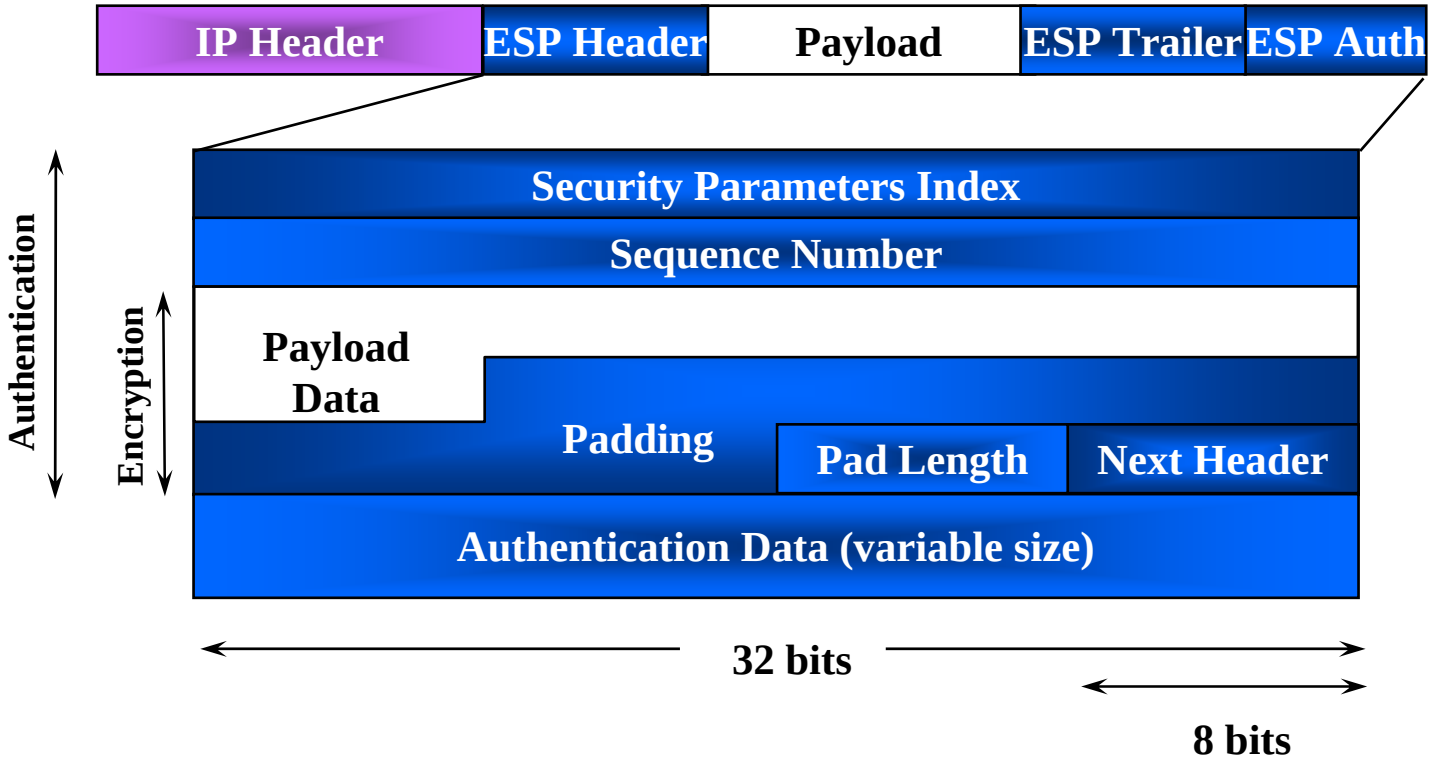
- ESP verschlüsselt den IP-Header und die Nutzdaten mit einem symmetrischen Verschlüsselungsverfahren (3DES, AES, IDEA, Blowfish, ...).
- Integrität und Authentizität der IP Pakete (nicht der „Outer IP-Header“)

Encapsulated Security Payload (ESP)
→ Beschreibung des Headers (1/2)



- **SPI** ist ein beliebiger 32-Bit Wert, der in Kombination mit der Ziel IP-Adresse und dem Security Protocol (ESP) eindeutig die Security Association für dieses Paket definiert.
- **Sequence Number** (32-Bit Feld) beinhaltet einen Zähler (Replay-Angriff).
- **Payload Data** ist ein Feld variabler Länge, das das originale IP-Paket beinhaltet (evtl. IV zu Beginn, falls notwendig).

Encapsulated Security Payload (ESP)
→ Beschreibung des Headers (2/2)



- **Padding** wird zum Auffüllen genutzt (0-255Bit), falls der Verschl.-Mode dies erfordert.
- **Pad Length** beschreibt die Länge des Feldes Padding.
- **Next Header** (8 Bit Feld) identifiziert den Datentyp in Payload Data.
- **Authentication Data** beinhaltet den Integrity Check Value (ICV), berechnet über das ESP ohne den Authentication Data Anteil.

Encapsulated Security Payload (ESP)
→ Zusammenfassung

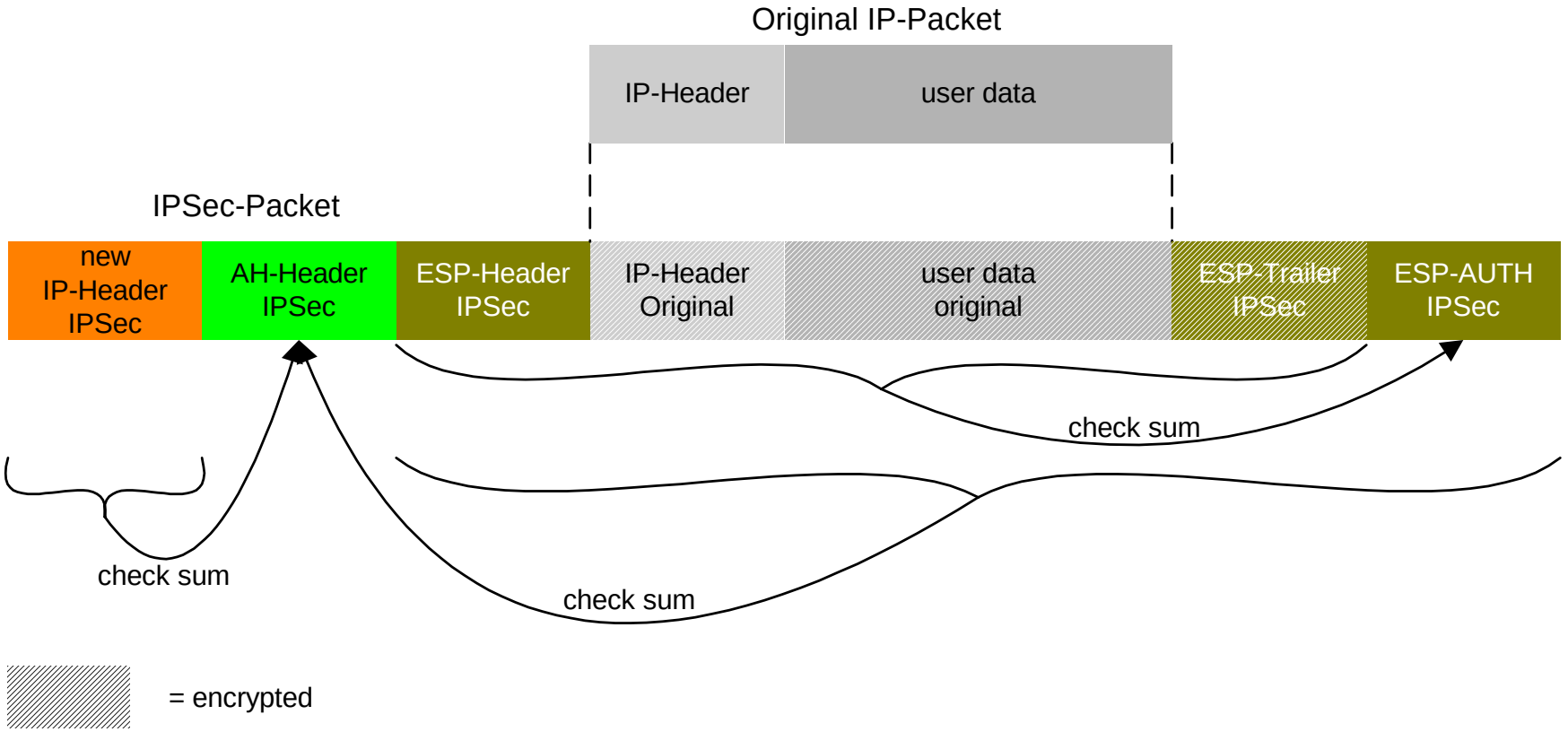
- Mit Hilfe von ESP können
  - Vertraulichkeit der Übertragung,
  - Authentikation des Absenders und
  - Integrität der Daten garantiert werden,

  da neben der Verschlüsselung auch ähnliche Mechanismen wie in AH definiert werden können.

- Im Unterschied zu ESP bezieht sich **die Authentikation von AH auch auf den IP-Header**, so dass die Kombination von AH und ESP Vorteile im Sicherheitsbereich bietet, allerdings mehr Ressourcen auf den beteiligten Rechnern benötigt!

Kombination mit AH und ESP

→ Tunnel-Mode



- AH und ESP können einzeln oder auch gemeinsam eingesetzt werden, wobei dann innerhalb des Netzwerkpakets der AH-Header vor dem ESP-Header stehen muss.

IPSec
→ Verbindung zur Security Association (SA)

- Die beiden Header selbst enthalten keine Informationen über
  - die zur Absicherung eingesetzten Algorithmen und
  - Schlüssellängen,

- sondern nur einen Verweis **(Security Parameter Index, SPI)** auf eine Datenstruktur mit diesen Informationen (Security Association, SA).

IPSec Anti-Replay Service
→ Schutz vor Wiedereinspielung von IP-Paketen

- **Sequence Number (SN)**
- **Initiator:**
  - Bei der Tunnel-Initialisierung wird SN = 0 gesetzt
  - Das erste Paket wird mit SN = 1 gesendet
  - Das Feld wird vor dem Versand jedes weiteren Paketes um 1 erhöht
- **Receiver:**
  - Überprüft, ob die Sequenz Nummer in der richtigen Reihenfolge ist.
  - Wenn dies nicht ist, wird das Paket verworfen.
  - Damit wird das Wiedereinspielen von alten Paketen unterbunden.

Siehe Protokollmitschnitt

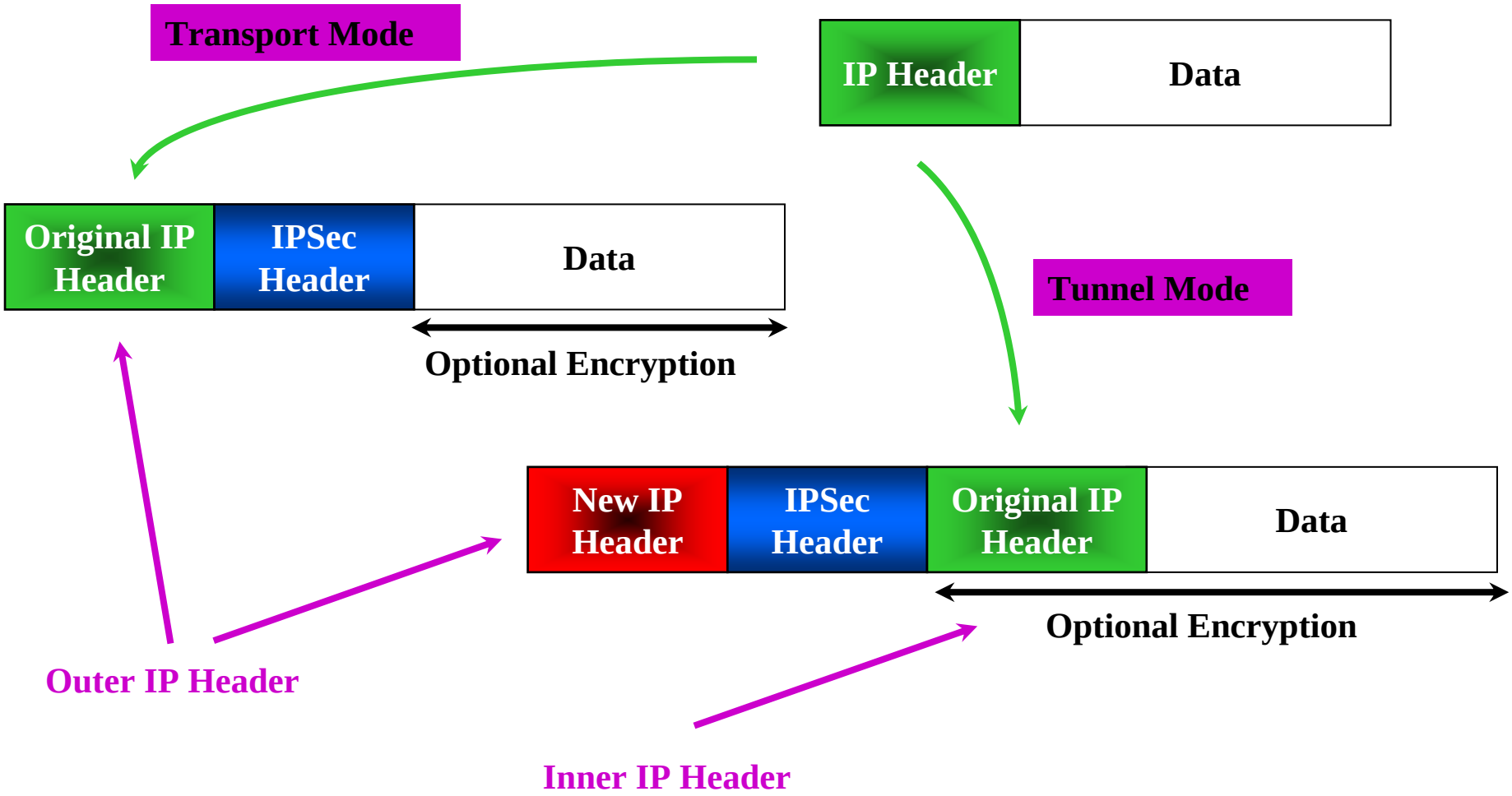
IPSec
→ Transport- und Tunnelmodus: Beschreibung

- IPSec kann im Transport- oder im Tunnelmodus betrieben werden.

- Im Transportmodus wird der IP-Header des ungesicherten IP-Pakets beibehalten und nur sein **Datenteil wird gesichert**.
- Bis auf das Feld „Länge des IP-Paketes“ und die „Prüfsumme“ bleibt der alte IP-Header unverändert.

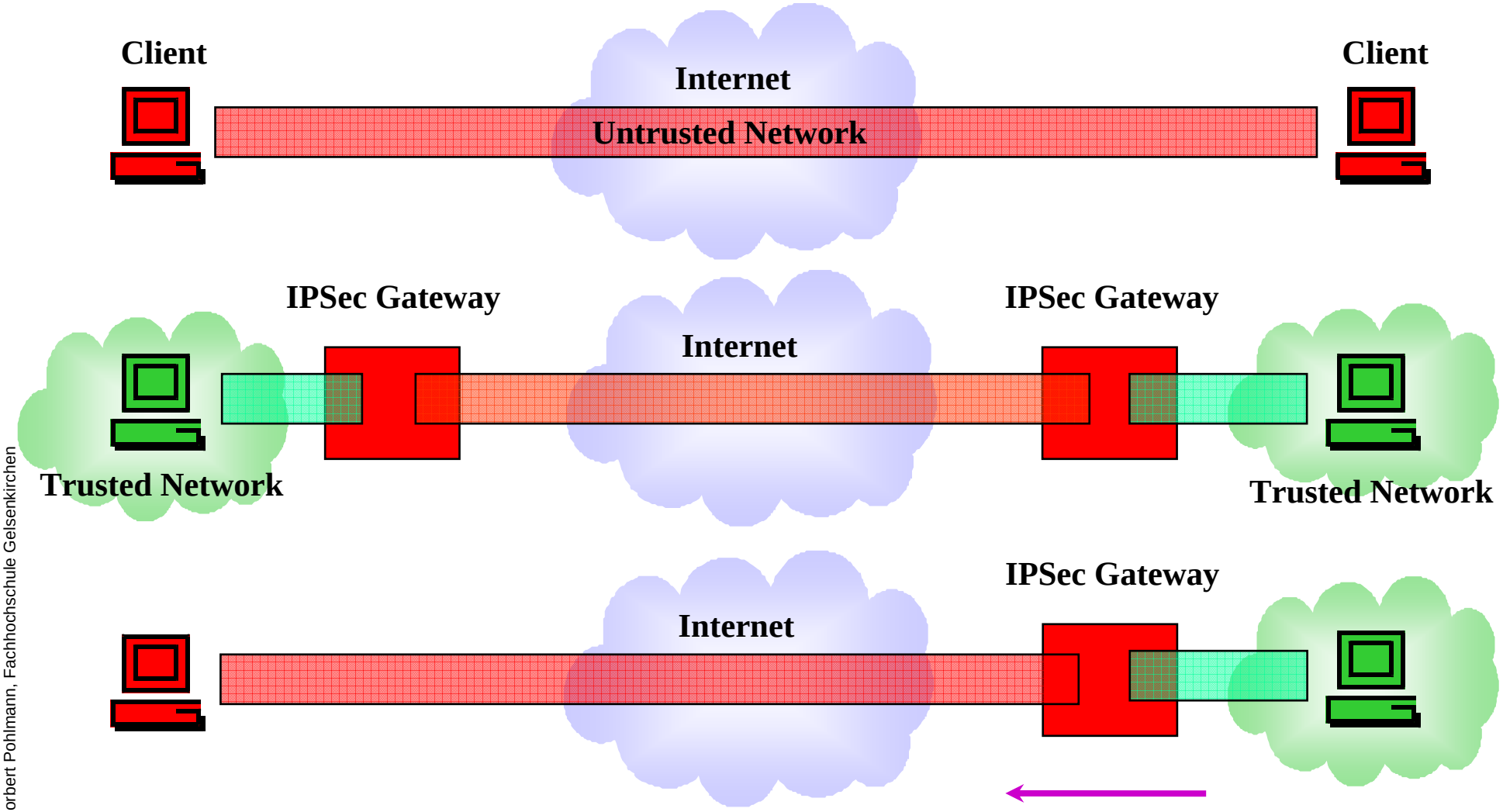
- Im Tunnelmodus hingegen wird das gesamte IP-Paket in die Nutzdaten des IPSec-Pakets übernommen, so dass die alte IP-Adresse bei der Verschlüsselung nicht mehr sichtbar ist.

IPSec
→ Transport- und Tunnelmodus: Übersicht



IPSec

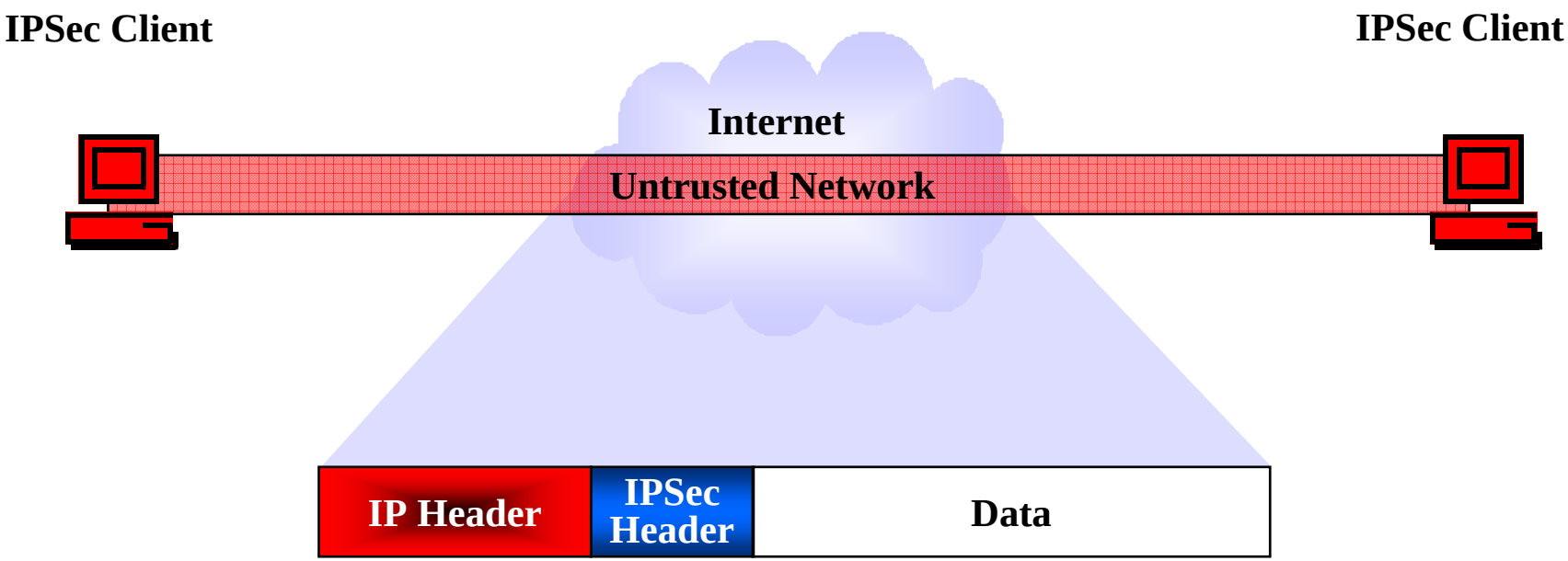
→ Client und Gateway: mögliche Kombinationen



Es werden zwei Verschlüsselungskanäle aufgebaut!

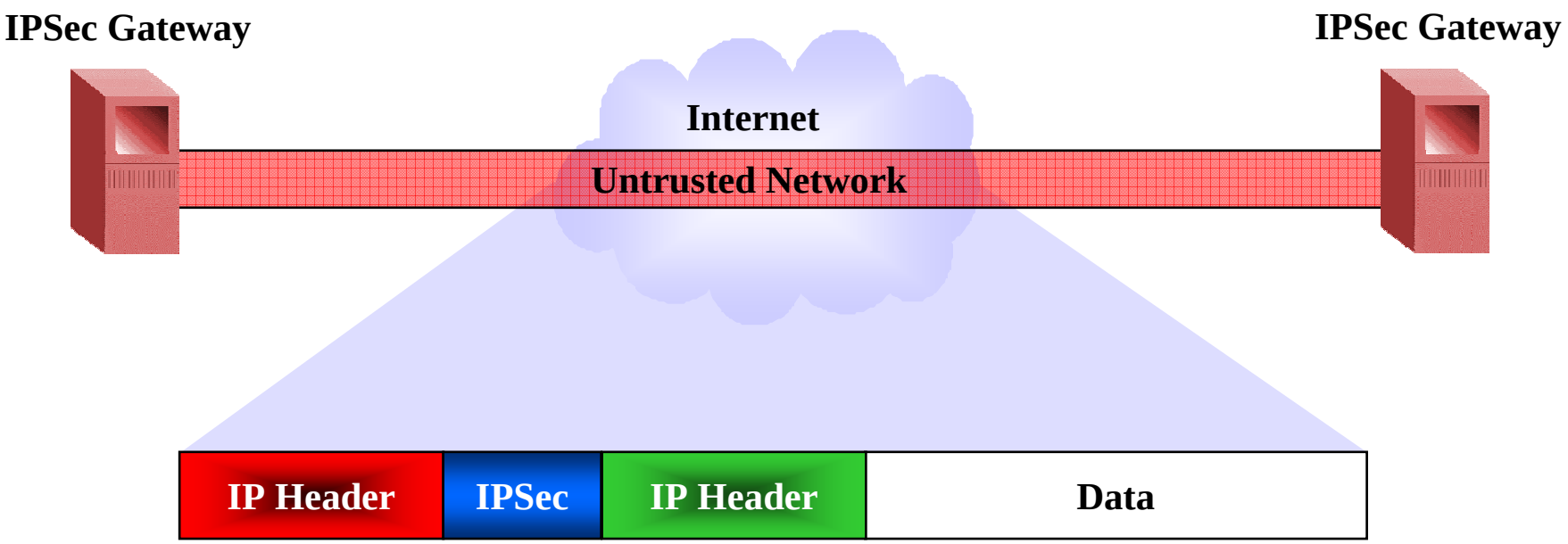
IPSec

→ Beispiel: Transportmodus



- Bei 1:n- oder m:n-VPNs mit Clients kommt nur der Transportmodus zum Einsatz.

IPSec
→ Beispiel: Tunnelmodus



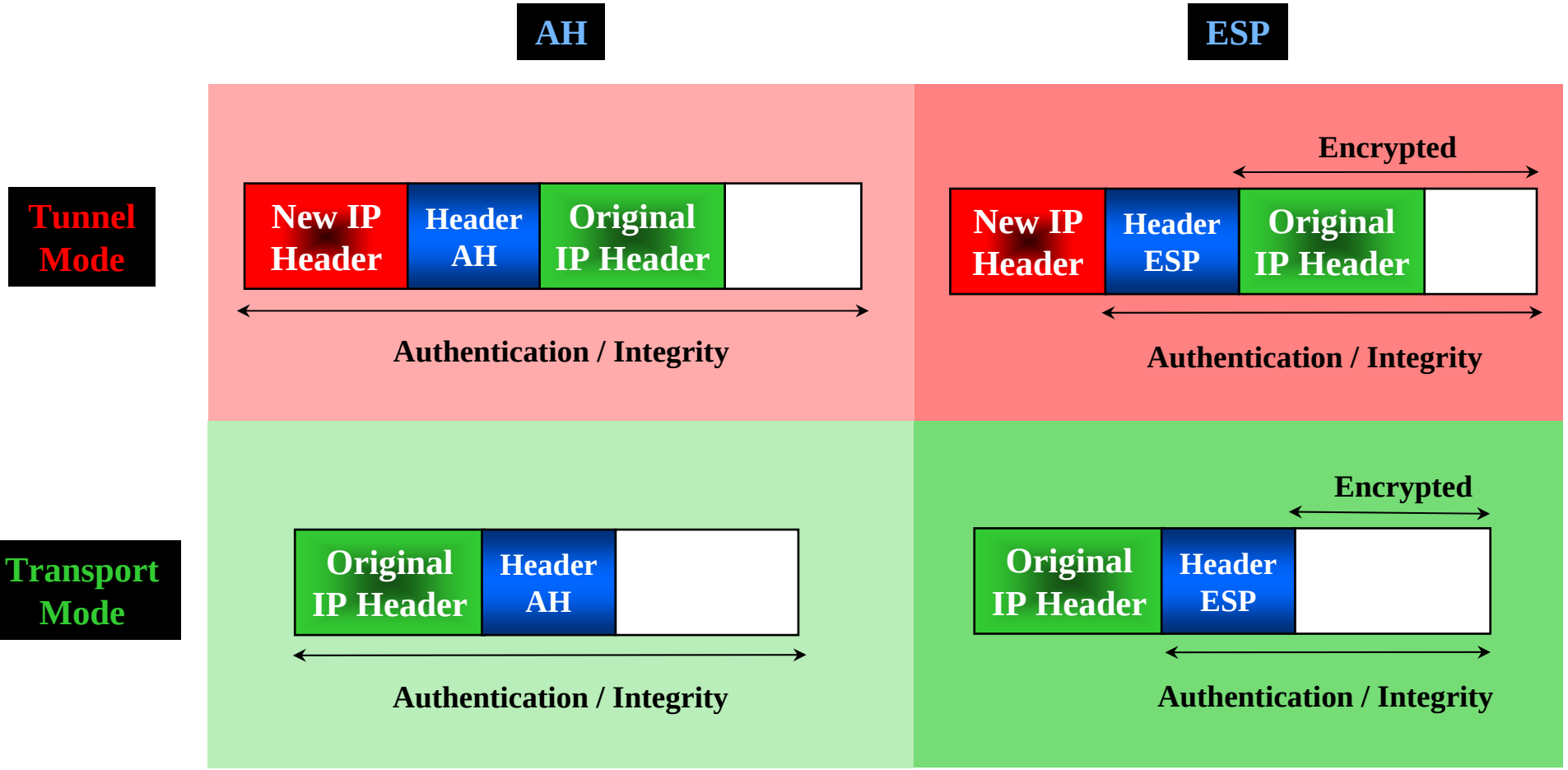
- Bei 1:1-VPNs, die beispielsweise zwischen zwei Firewall-Systemen oder sonstigen Security-Gateways eingerichtet werden, wird immer der Tunnelmodus genutzt.
- Damit bleiben die echten IP-Adressen der Kommunikations-Partner einem Angreifer verborgen.

IPSec
→ IPSec Gateway

- Die Konfiguration eines IPSec Gateways ähnelt in bestimmten Aspekten der einer Firewall (Paket Filter).
- Je Quelladresse, Zieladresse, Schnittstelle, Protokoll, Port und so weiter wird definiert, ob das Paket verworfen oder (verschlüsselt oder entschlüsselt) weitergeleitet wird.
- Bei einem IPSec Gateway kommt als dritte Möglichkeit der Versand durch einen Tunnel in Frage.
- Für diesen Fall müssen die Parameter des Tunnels definiert werden.
- Der wichtigste Parameter ist natürlich die Adresse des Ziel-Gateways.

IPSec

→ Schutz in Abhänigkeit vom Mode und Protokoll



IPSec
→ Verwendete Algorithmen

	IPSec
Ciphering algorithm	DES* Triple DES RC5 IDEA CAST Blowfish
Hash algorithm	MD5* SHA-1* Tiger
Authentication	RSA digital signatures DSS digital signatures Pre-shared secret key *

* Necessarily supported by all IPSec implementations

Inhalt

- Einleitung: Definitionen und Ziele
- Konzepte von VPNs und Anwendungsformen
- Ansätze für VPN Lösungen
- IPSec - Standard
- **IPSec Schlüssel-Management (IKE)**
- Praktischer Einsatz von VPNs
- IPSec Client
- Zusammenfassung

IKE
→ Security Association (SA)

- Eine Security Association (SA) legt alle Informationen fest, die zwischen der Verbindung von zwei Security-Gateways benötigt werden.
  - Security Parameter Index (SPI)
  - genutzter IPSec-Service (AH oder ESP oder beide)
  - Modus (Transport oder Tunnel)
  - Quell- & Ziel-IP-Adresse, evtl. Adresse des Gateways
  - evtl. genutzte Protokolle, Quell- & Zielportnummer
  - genutzte Algorithmen & Schlüssel für die SA
  - Sequenznummer
  - Dauer der Gültigkeit der SA (kann über einen längeren Zeitraum sein!)
  - Statusinformation der Anti-Replay-Windows
- Es können mehrere SA´s mit unterschiedlichen Inhalten gleichzeitig zum selben Ziel existieren.

IKE
→ Security Parameter Index (SPI)

- Der Security Parameter Index (SPI) ist ein beliebiger Wert, der in Kombination mit der Ziel IP-Adresse und dem Security Protocol eindeutig die Security Association (SA) für dieses Paket definiert.
- Wenn IKE zum Aufbau der Security Associations genutzt wird, ist der SPI einer jeden Security Association eine **Pseudozufallszahl** (siehe PM).
- Der SPI wird manuell für jede Security Association festgelegt, wenn IKE nicht zum Einsatz kommt.

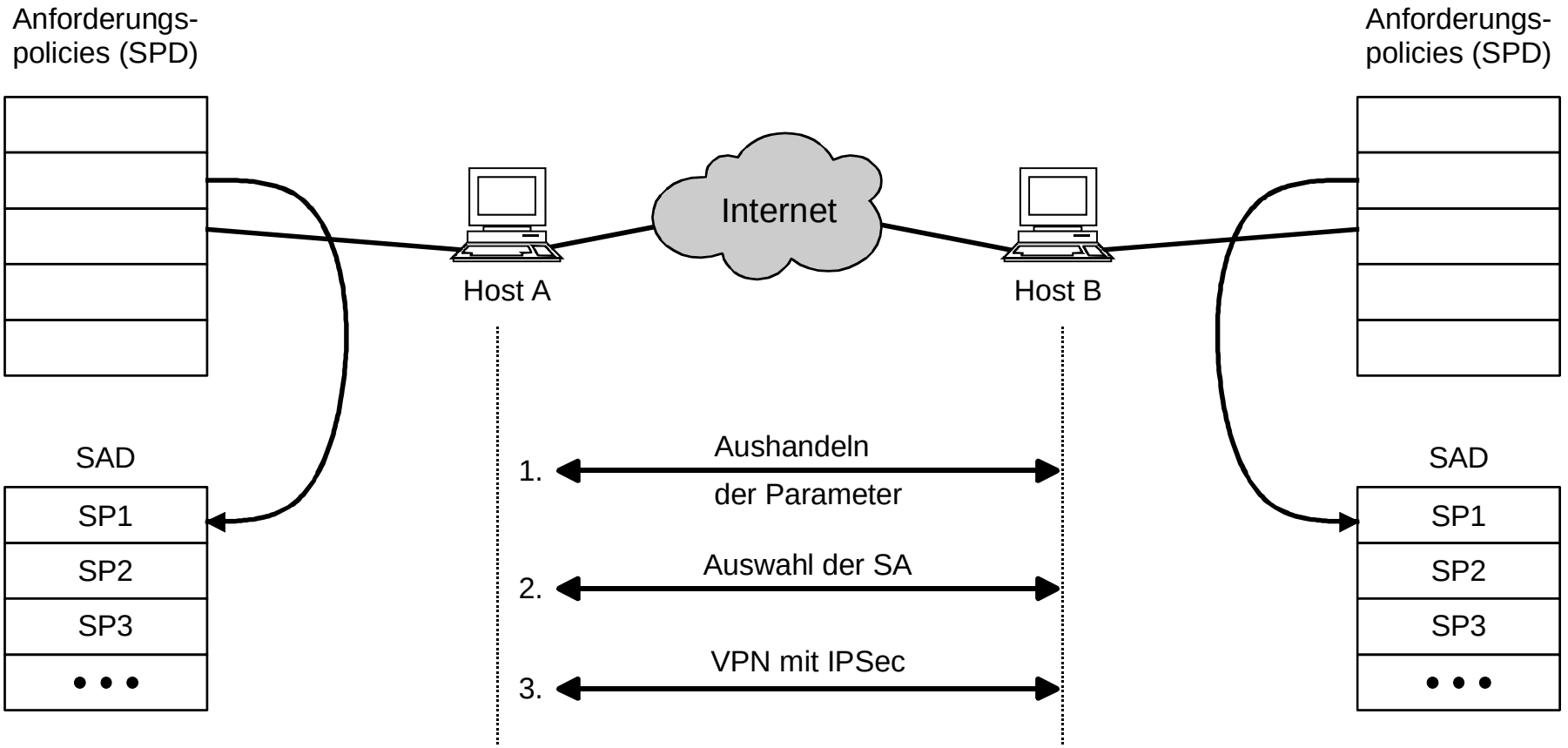
IKE
→ Security Policy Database (SPD)

- Die Security Policy Database definiert den **Sicherheitsstandard für ein System**.
- Sie wird während des automatisierten Schlüsselaustausches konsultiert:
  - Quell- & Ziel-IP-Adressen oder Ranges
  - Quell- & Zielportnummer
  - Protokoll (TCP, UDP, ...)
  - eine Liste mit den zugelassenen Algorithmen für das System
  - falls notwendig: Beschreibung des Tunnelendpunktes
  - Informationen über die Nutzung der Anti-Replay-Windows und der maximalen Lebensdauer der SA´s

IKE
→ Security Association Database (SAD)

- In der Security Association Database sind alle Security Association eingetragen.
- Für jede SA werden folgende Parameter festgelegt:
  - Identifier:
    - Ziel-IP-Adressen oder Ranges
    - Security Protokoll
    - SPI
  - Parameter:
    - Algorithmen für die Authentikation und Verschlüsselung
    - Lebensdauer der SA
    - Security Protocol Mode (tunnel or transport)
    - Anti-Replay-Service
    - Link mit der Policy in der SPDSA´s

IKE
→ Security Association (SA): Übersicht



IKE
→ Etablierung einer SA

- Eine Security Association (SA) beinhaltet eine Policy und Schlüssel, um Informationen zu schützen.

- **Security Associations (SA) werden ausgehandelt :**
  - manuell
    - kleine Netzwerke
  - automatisch
    - Netzwerke aller Größen

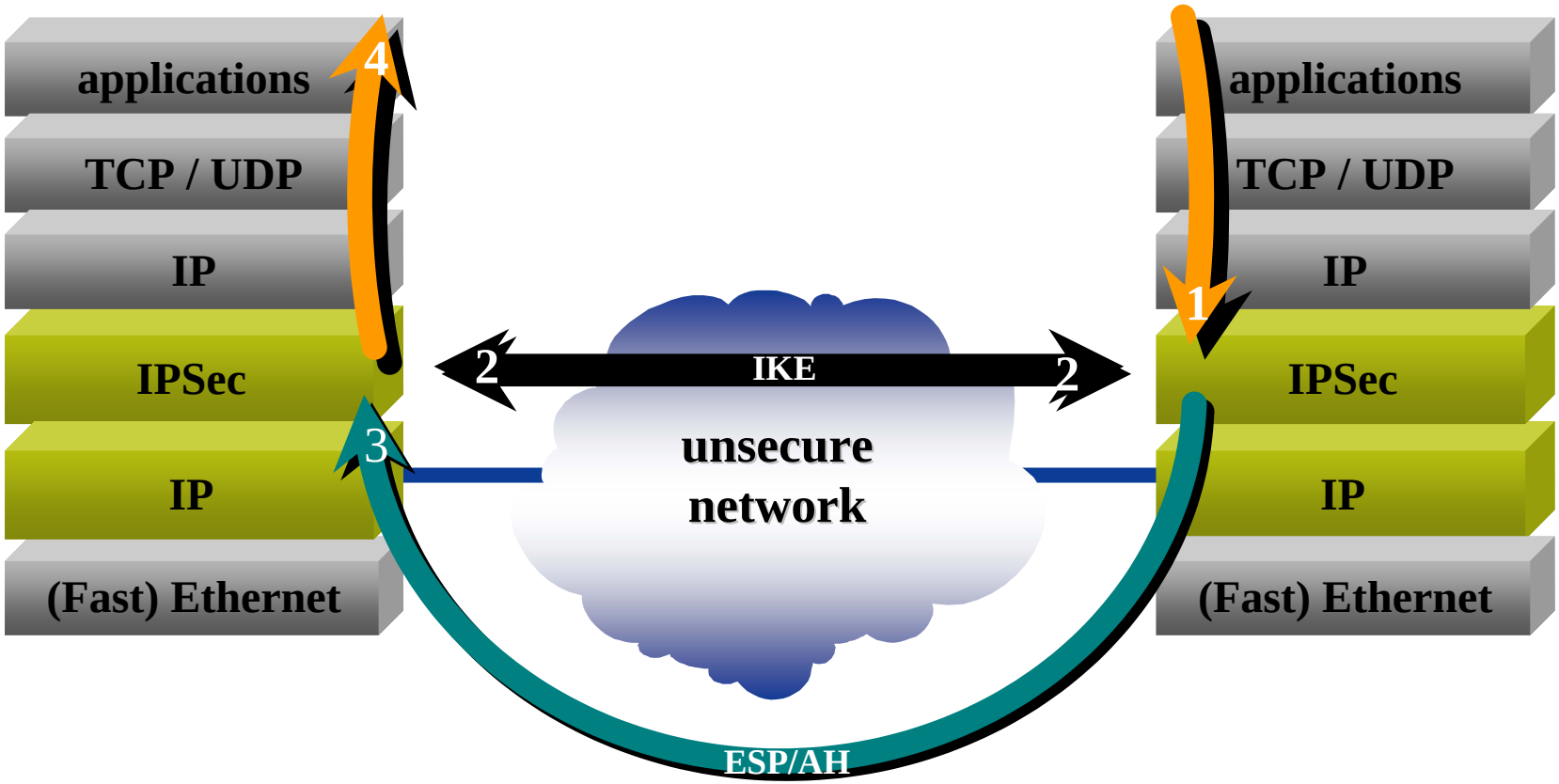
- **Das automatische SA-Management:**
  - ISAKMP RFC 2408
  - IKE RFC 2409

IKE
→ Schlüssel-Management

- **Manual Keying**
  - Die notwendigen Schlüssel werden auf einem der Kommunikationspartner oder einem zentralen Management generiert.
  - Dann werden diese Schlüssel auf einem **sicheren Weg** zu allen beteiligten Partnern (Client und Gateways) transferiert.

- **IKE - Internet Key Exchange**
  - IKE ist das offizielle Schlüsseltransferprotokoll von IPSec.
  - Beide Seiten brauchen nur eine **identische Passphrase** (Pre-Shared Key).
  - Darauf basierend wird unter dem Einsatz des Diffie-Hellman-Protokolls ausgehandelt, z.B. welche Algorithmen zur Verschlüsselung eingesetzt werden.

IKE
→ IPSec mit IKE in Aktion



IKE
→ Verschiedenen Modi und Phasen: Übersicht

- IKE = Protokoll, um eine sichere ISAKMP- u. IPSec-SA zu etablieren
- Basiert auf UDP, Port 500 (Quelle und Ziel)
- Zwei Phasen:
  - 1 - Main Mode/Aggressive Mode
  - 2 - Quick Mode

Exchange Mode	IKE Phase	No. of Mesg's	Agree On Key	Authent. IDs	Conceal IDs	No. of Proposals
Main	1	6	Yes	Yes	Yes	Multiple
Aggressive	1	3	Yes	Yes	No	Only One; No DH Group
Quick	2	3	Yes	Yes	No	Multiple

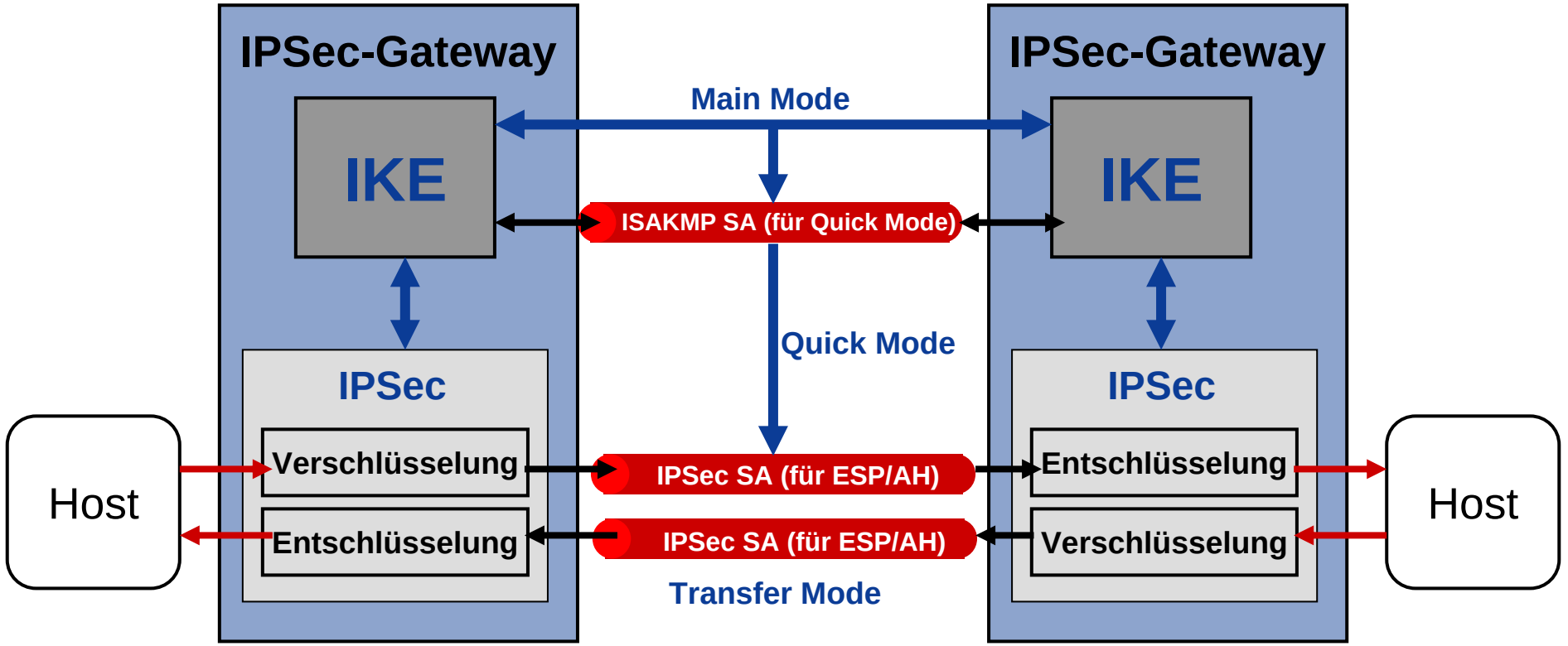
IKE
→ Phase 1: Aufbau der ISAKMP SA

- In der **Phase 1** wird ein sicherer Kanal (ISAKMP SA) zwischen beiden Endpunkten etabliert.
- Die Phase 1 wird ISAKMP Security Association oder äußere SA genannt.
  (ISAKMP = Internet Security Association and Key Management Protocol)
- In der Phase 1 werden mit Hilfe des Main Modes/Aggressive Modes:
  - IKE-Parameter (ISAKMP) aushandelt:
    - Authentikationmethode (PKI oder PSK)
    - Algorithmen für Authentikation und Verschlüsselung
    - Schlüsselaustausch (für die SAs)
  - und eine **Nutzerauthentisierung** durchgeführt.

IKE
→ Phase 2: Aufbau der IPSec SA

- **Phase 2** dient dem Aushandeln der IPSec SA mit Hilfe des so genannten Quick Modes innerhalb der sicheren ISAKMP SA (aus der Phase 1):
  - Aushandeln der IPSec-Parameter:
    - Security Protokoll (AH, ESP)
    - Algorithmen und Schlüssel
      die für die Authentisierung und Verschlüsselung der Daten (IP-Pakete) genutzt werden.
      Hinweis:
      Diese können anders sein, als in der Phase 1.
  - Alle Pakete der Phase 2 werden durch in der Phase 1 ausgehandelte Algorithmen und Schlüssel geschützt.

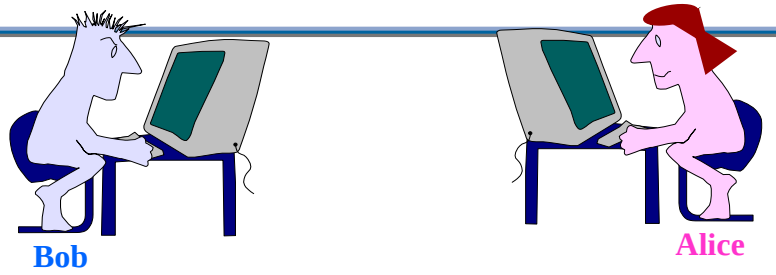
IPSec und IKE
→ Übersicht und Zusammenhang



- **Main Mode:** Aufbau der ISAKMP SA sowie **Policy Absprachen** und **Authentikation**
- **Quick Mode:** Aufbau der IPSec SA sowie **Mode/Protokoll (AH, ESP) Absprache** und **Key-Management**
- **Transfer Mode: Sicherung der IP-Pakete** mit AH/ESP und Anti-replay Service

IKE
→ SA Aushandlung

- Phase 1 : ISAKMP SA Establishment
  - **Main Mode**
    - **Three two-way exchange**
    - **Identity protection**
  - **Aggressive Mode**
    - **No identity protection**
    - **Increase the speed**
- Phase 2 : IPSec SA Establishment
  - **Quick Mode**



ISAKMP parameters negotiation

Key Exchange

Authentication

ISAKMP parameters Negotiation, key exchange and Alice's authentication

Bob's authentication

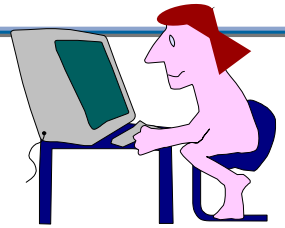
IPSec parameters negotiation, key exchange

Acquittal

ISAKMP SA Aufbau

→ Phase 1 - IKE Main Mode - Step 1

Bob



Alice

Message 1 →

ISAKMP SA Offer	
Authentication method	ISAKMP Header
Authentication algorithm	
Encryption algorithm	

← Message 2

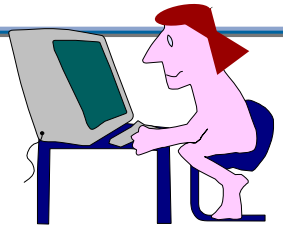
ISAKMP Header	ISAKMP SA Approval

Hier werden die Basis-Algorithmen (Policy) für die Verschlüsselung und Authentikation der ISAKMP SA ausgehandelt.

ISAKMP SA Aufbau

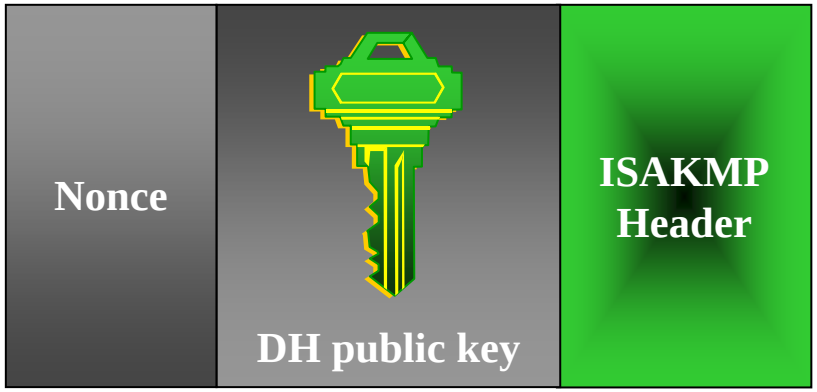
→ Phase 1 - IKE Main Mode - Step 2

Bob

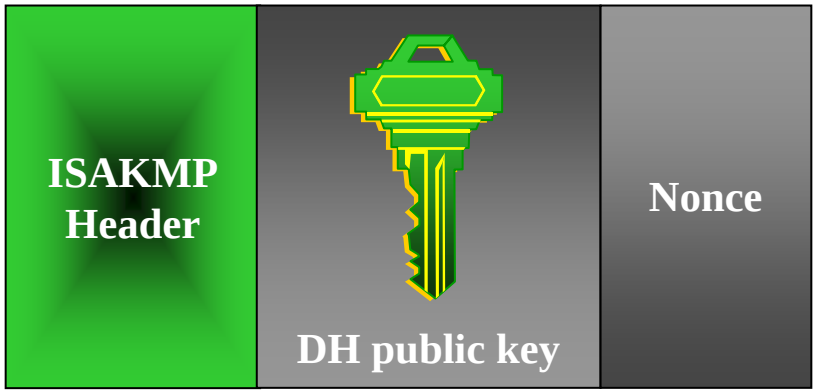


Alice

Message 3 →



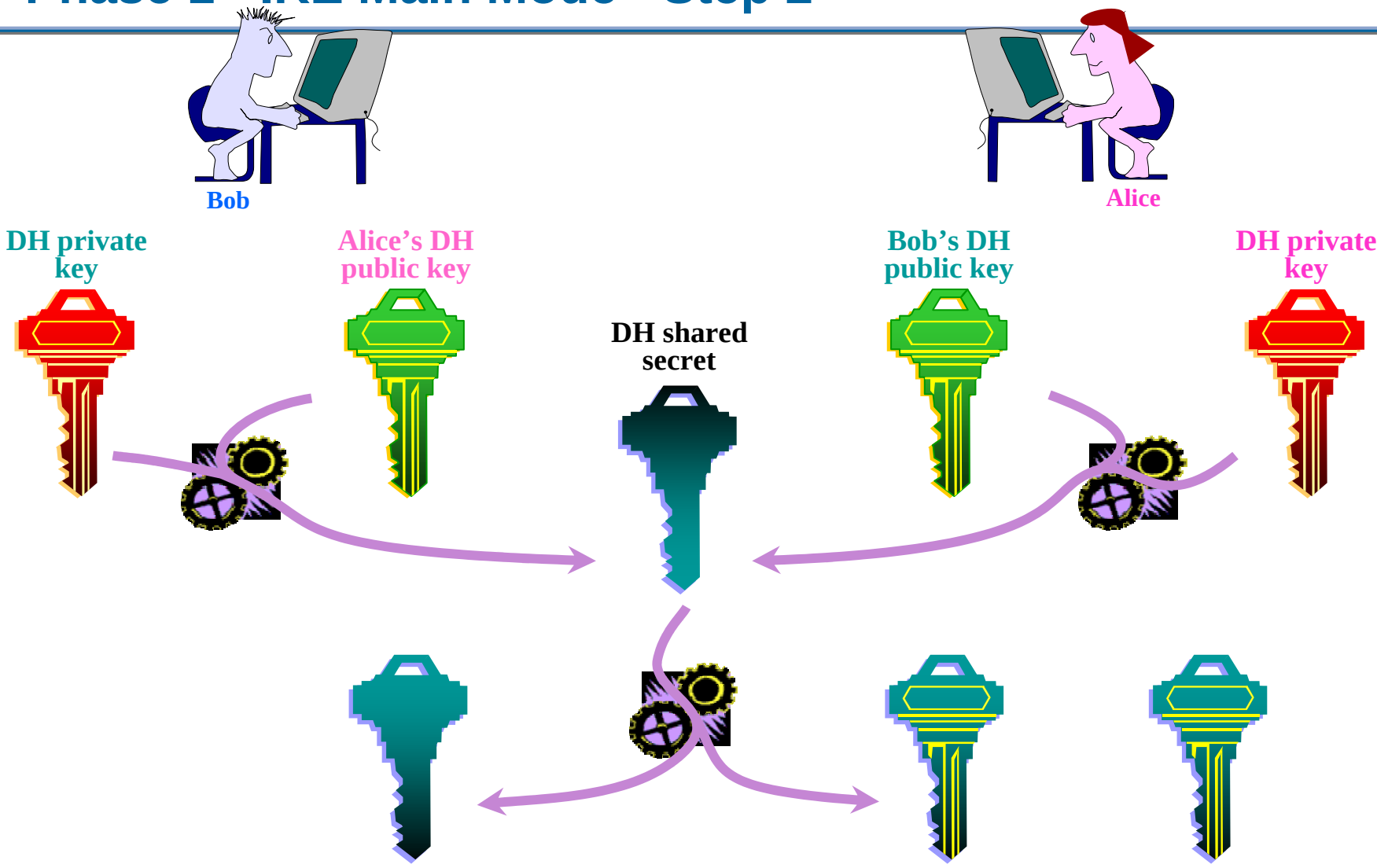
Message 4 ←



In „Nonce“ wird eine Zufallszahl ausgetauscht, die für die Authentikation im Step 3 verwendet wird.

ISAKMP SA Aufbau

→ Phase 1 - IKE Main Mode - Step 2



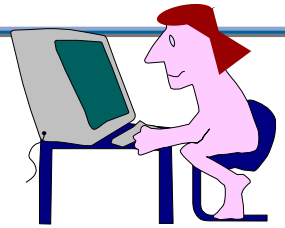
wird für den Quick-Mode verwendet

für Auth. u. Verschlüssel. im Step 3

ISAKMP SA Aufbau

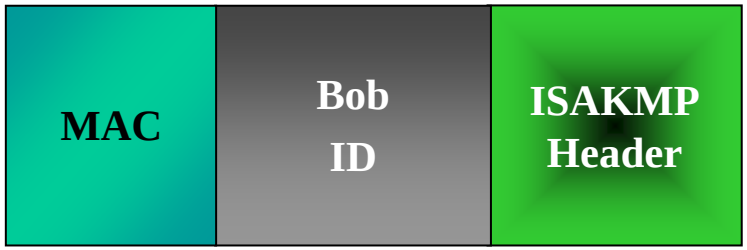
→ Phase 1 - IKE Main Mode - Step 3

Bob



Alice

Message 5 →

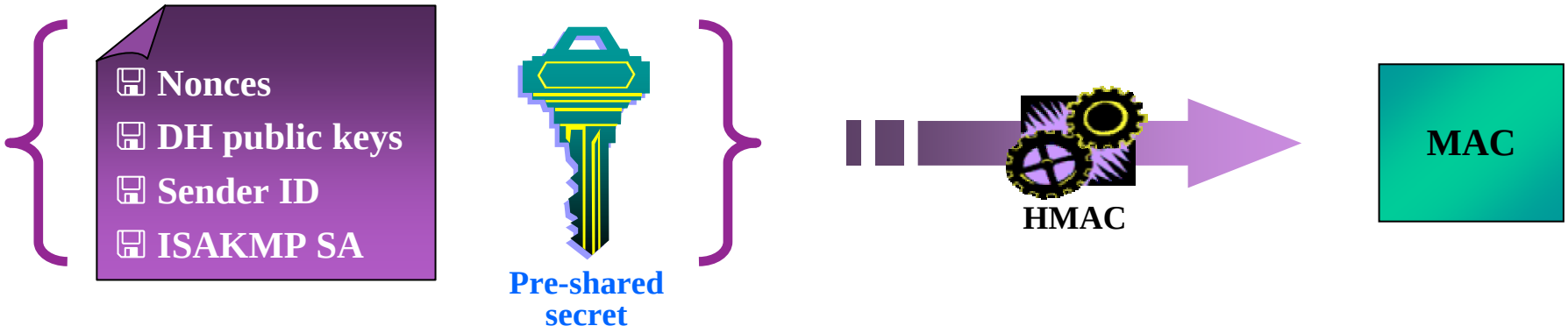


Message 6 ←

In diesem Schritt werden die Kommunikationspartner verifiziert.
Da die beiden Pakete verschlüsselt sind, können die IDs nicht mitgelesen werden!

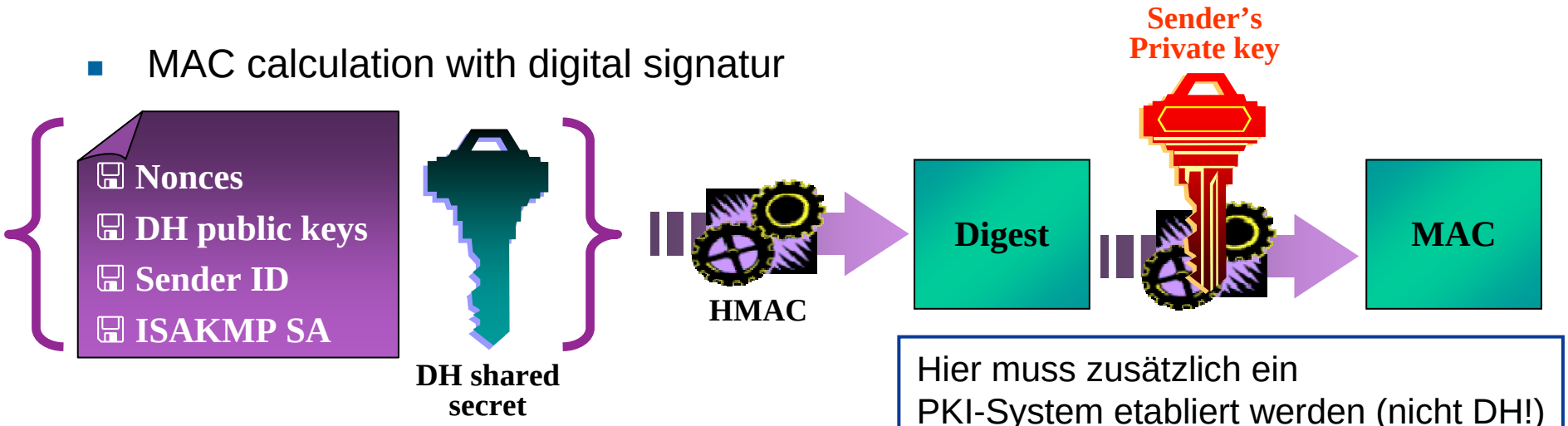
ISAKMP SA Aufbau
→ Phase 1, Step 3 - Authentication methods

- MAC calculation with pre-shared secret authentication



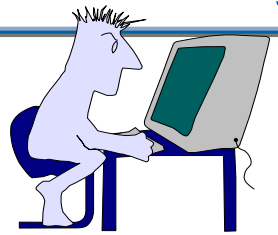
Der „Pre-shared secret“ wird vorher eingegeben! Wenn alle den gleichen „Pre-shared secret“ in einer Organisation nutzen, wird nur die Zugehörigkeit verifiziert (z.B. bei Gateways).

- MAC calculation with digital signatur

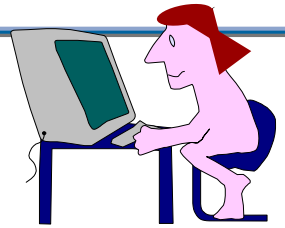


Hier muss zusätzlich ein PKI-System etabliert werden (nicht DH!)

ISAKMP SA Aufbau
→ Phase 1 - IKE Aggressive Mode



Bob



Alice

Message 1 →

Bob ID	Nonce	DH public key	ISAKMP SA Offer	ISAKMP Header

← Message 2

ISAKMP Header	ISAKMP SA Approval	DH public key	Nonce	Alice ID	MAC

Message 3 →

MAC	ISAKMP Header

Der „Aggressive Mode“ ist schneller, da er mit nur 3 Paketen auskommt.
Es werden aber nicht die IDs verschlüsselt!

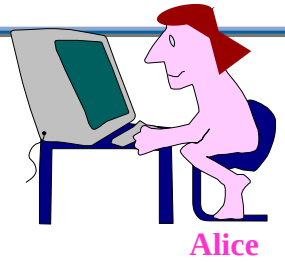
IPSec SA Aufbau
→ Phase 2 - Quick Mode: Übersicht

- Die Authentikation und Verschlüsselung aller Phase-2 Pakete wird mit dem Schlüssel (Derivation Key) aus der Phase 1 realisiert

- **IPSec SA Aushandlung findet in der ISAKMP SA statt**
  - **Auswahl** von:
    - Security Protocol (ESP or AH)
    - Authentication Algorithm (SHA-1, MD5)
    - Encryption Algorithm (if ESP)
  - **Schlüssel Austausch**

- **Es gibt zwei Methoden den Basis-Schlüssel (KEYMAT) zu berechnen:**
  - **Basic Quick Mode** (der Phase-1 „Derivation Key“ wird benutzt)
  - **Perfect Forward Secrecy** (wie Quick Mode aber zusätzlich Diffie-Hellman Shared Secret)

IPSec SA Aufbau
→ Phase 2 - Quick Mode



Message 1 →

Nonce	IPSec SA Offer Security Protocol Authentication algorithm Encryption algorithm	ISAKMP Header

← Message 2

ISAKMP Header	IPSec SA Approval	Nonce

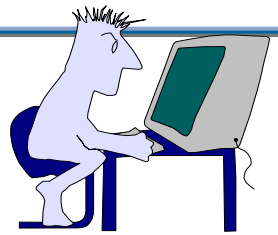
Message 3 →

Acquittal	ISAKMP Header

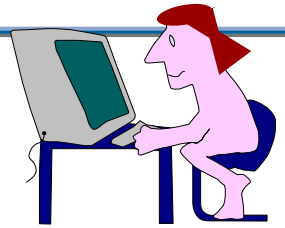
Zur Verschlüsselung dieser Pakete wird als Basis der „Derivation Key“ aus der 1. Phase verwendet.

IPSec SA Aufbau

→ Phase 2 - Perfect Forward Secrecy



Bob



Alice

Message 1 →

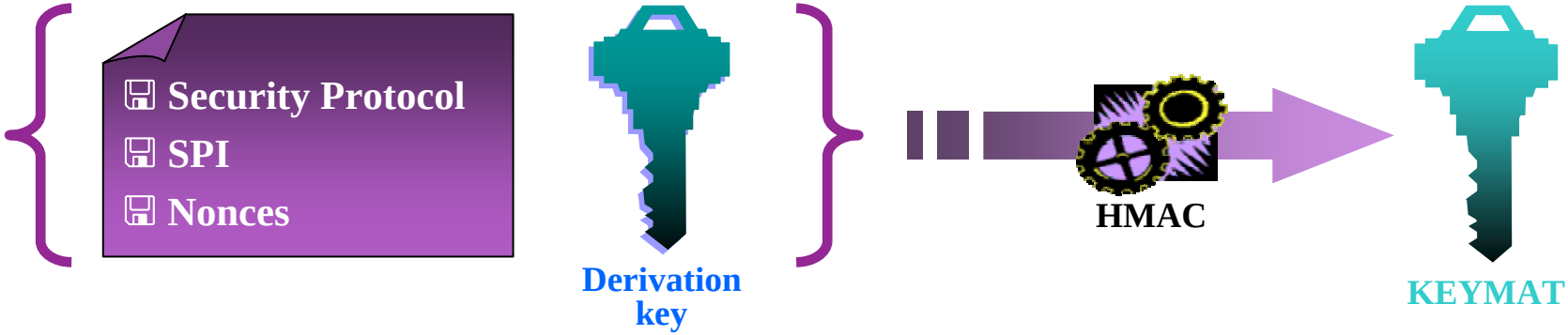
← Message 2

Message 3 →

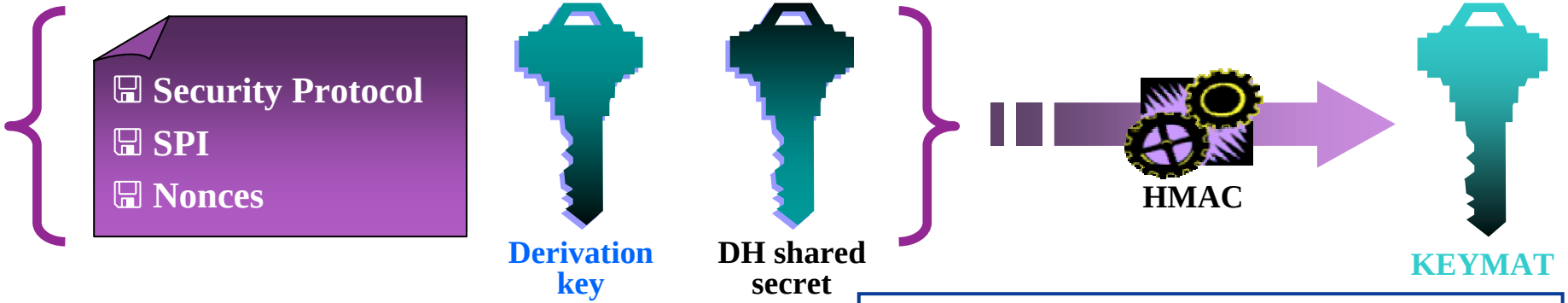
Wie Basic Quick Mode, aber zusätzlich mit Diffie-Hellmann Verfahren.

IPSec SA
→ Phase 2 - Berechnung von KEYMAT

- Keying Material with **Basic Quick Mode**



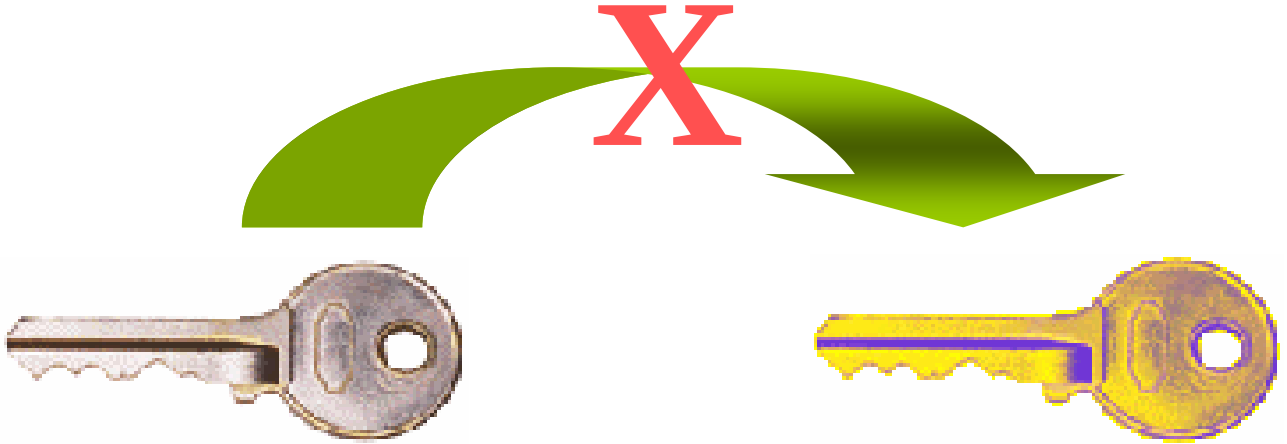
- Keying Material with **Perfect Forward Secrecy (PFS)**



Hinweis: Der „Derivation Key“ kann über einen längeren Zeitpunkt gültig sein!

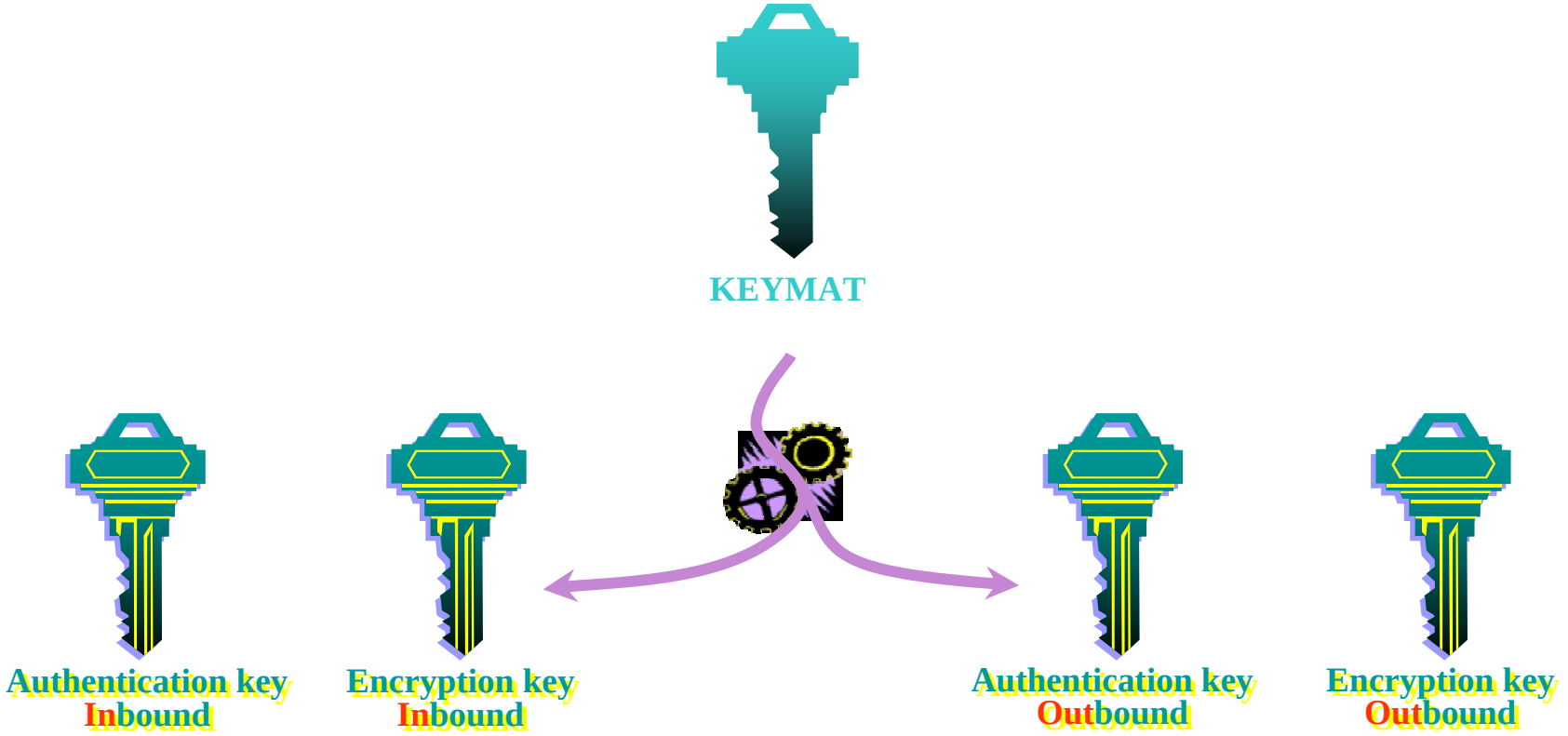
IPSec SA
→ Perfect Forward Secrecy (PFS): Idee

- Das Perfect Forward Secrecy (PFS) ist eine kryptographische Charakteristik, die eine Aussage über die Abhängigkeit von Schlüsseln untereinander trifft.



- Mit aktiviertem PFS sind bei einem kompromittierten Schlüssel (z.B. Derivation Key) alle weiteren nicht gleichzeitig auch kompromittiert, da die **Schlüssel nicht voneinander abhängen**.
- Dieses kann durch die **zusätzliche Verwendung des DH-Verfahren** (Aushandlung eines speziellen Shared Secret) erreicht werden!

IPSec SA
→ Phase 2 - Session key generation



Es werden zwei separate „Kryptographie-Kanäle“ aufgebaut!

Die Diffie-Hellman Methode
→ Überblick

- Diffie-Hellman ist kein Verschlüsselungsmechanismus!

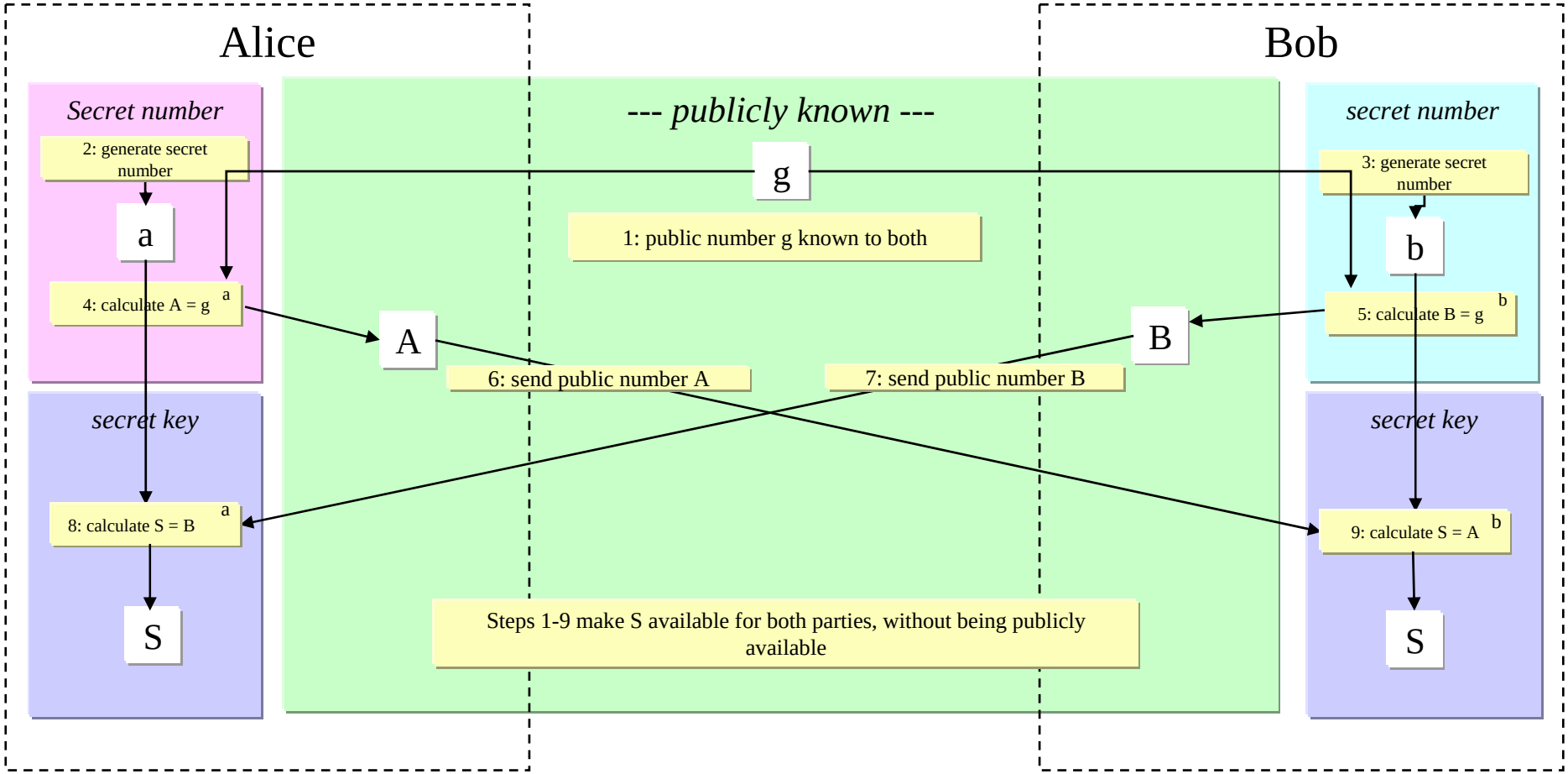
- Diffie-Hellman ist eine Methode, sicher **Schlüssel „auszutauschen“**.

- Das wichtige Feature des Diffie-Hellman Protokolls ist seine Fähigkeit, "shared secrets" zu generieren.
  Das sind identische kryptographische Schlüssel, die auf zwei Seiten generiert werden können und somit nicht selbst übertragen werden müssen.

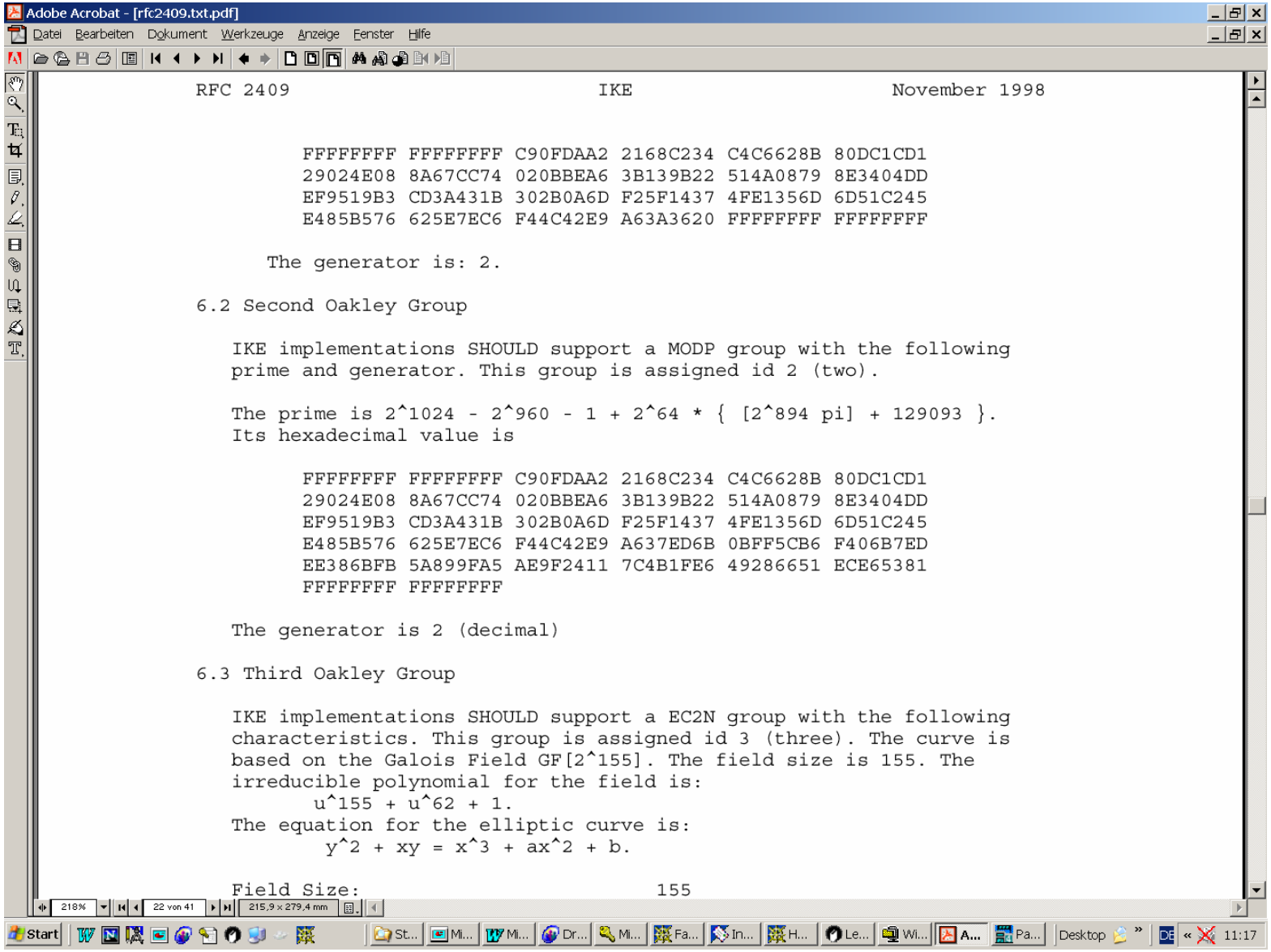
- Das „shared secret“ ist als Resultat ein **Schlüssel**, der zur Berechnung der Schlüssel im Main Mode (Derivation Key, Authentication Key und Encryption Key) oder im Perfect Forward Secrecy (KEYMAT) verwendet wird.

Die Diffie-Hellman Methode
→ Ablauf

The procedure is based on the exchange of uncritical information!



Die Diffie-Hellman
→ p und g (aus RFC 2409)

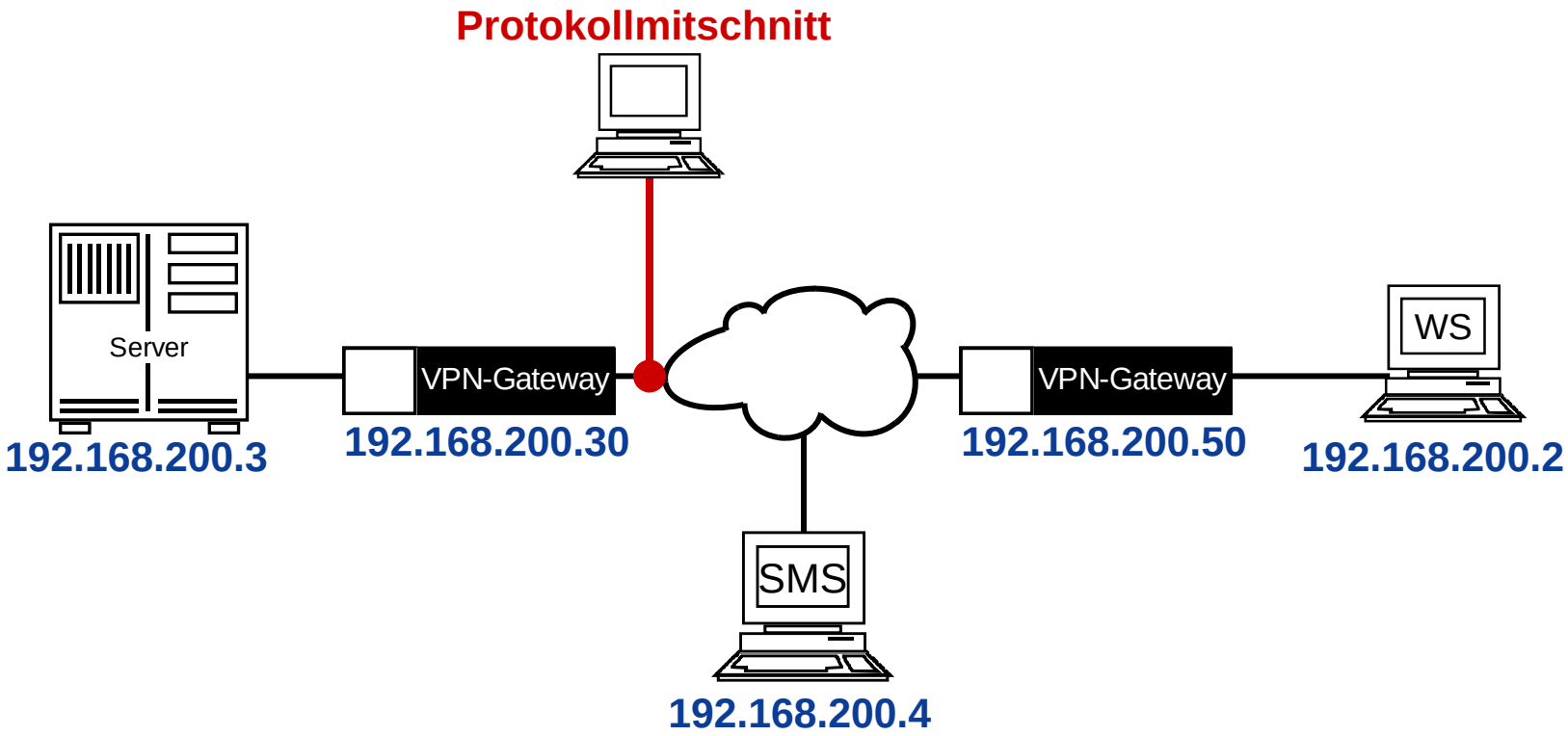


IPSec und IKE
→ Komplexität

- Die Aufteilung auf zwei verschiedene SAs (Phase 1 und Phase 2) ist einer der Gründe für die Komplexität von IPSec.
- Die Trennung bietet aber auch Vorteile:
  - Der Quick Mode ist sehr schnell, weil **keine** Authentikation mehr notwendig ist.
  - Der Schlüssel, der im Main Mode für die äußere ISAKMP SA ausgehandelt wurde, kann lange Zeit benutzt werden, weil nur sehr wenige Pakete damit verschlüsselt werden.
  - Die Lifetime der ISAKMP SA kann also wesentlich höher sein als die Lifetime der IPSec SAs.
  - Außerdem kann die ISAKMP SA auch „auf Verdacht“ aufgebaut werden, um die Etablierung von IPSec SAs bei Bedarf zu beschleunigen.

IPSec - Protokollmitschnitte

IPSec und IKE
→ Protokollmitschnitt - Übersicht (1/2)



Aufbau einer Telnet-Session mit Login-Prozedur!

IPSec und IKE

→ Protokollmitschnitt - Übersicht (2/2)

No.	Time	Source	Destination	Protocol	Info
141	686.400720	192.168.200.50	192.168.200.30	ISAKMP	Identity Protection (Main Mode)
142	686.401656	192.168.200.30	192.168.200.50	ISAKMP	Identity Protection (Main Mode)
143	686.415341	192.168.200.50	192.168.200.30	ISAKMP	Identity Protection (Main Mode)
144	686.429389	192.168.200.30	192.168.200.50	ISAKMP	Identity Protection (Main Mode)
145	686.443334	192.168.200.50	192.168.200.30	ISAKMP	Identity Protection (Main Mode)
146	686.457499	192.168.200.30	192.168.200.50	ISAKMP	Identity Protection (Main Mode)
147	686.459620	192.168.200.50	192.168.200.30	ISAKMP	Quick Mode
148	686.461093	192.168.200.30	192.168.200.50	ISAKMP	Quick Mode
149	686.462319	192.168.200.50	192.168.200.30	ISAKMP	Quick Mode
150	686.616779	192.168.200.50	192.168.200.30	ESP	ESP (SPI=0x9b0e9336)
151	686.617720	192.168.200.30	192.168.200.50	ESP	ESP (SPI=0x76aa8a80)
152	686.618398	192.168.200.50	192.168.200.30	ESP	ESP (SPI=0x9b0e9336)
153	686.619782	192.168.200.30	192.168.200.50	ESP	ESP (SPI=0x76aa8a80)
154	686.620293	192.168.200.50	192.168.200.30	ESP	ESP (SPI=0x9b0e9336)
155	686.620420	192.168.200.50	192.168.200.30	ESP	ESP (SPI=0x9b0e9336)
156	686.758705	192.168.200.30	192.168.200.50	ESP	ESP (SPI=0x76aa8a80)

Main Mode

Quick Mode

Transfer Mode

Wir sehen nur die IP-Adressen der VPN-Gateways,
die Rechner (Client und Server) dahinter bleiben verborgen !

IKE
→ Protokollmitschnitt - Main Mode: Step 1, M1 (1/2)

```
Frame 141 (318 bytes on wire, 318 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x0000000000000000
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...0 = No encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 276
    Security Association payload
        Next payload: Vendor ID (13)
        Length: 228
        Domain of interpretation: IPSEC (1)
        Situation: IDENTITY (1)
        Proposal payload # 0
            Next payload: NONE (0)
            Length: 216
            Proposal number: 0
            Protocol ID: ISAKMP (1)
            SPI size: 8
            Number of transforms: 8
            SPI: A2FAB77526000000
            Transform payload # 0
                Next payload: Transform (3)
                Length: 24
                Transform number: 0
                Transform ID: KEY_IKE (1)
                Encryption-Algorithm (1): 3DES-CBC (5)
                Hash-Algorithm (2): SHA (2)
                Authentication-Method (3): PSK (1)
                Group-Description (4): 1536 bit MODP group (5)
```

Angebot an Policy Teil 1

IKE
→ Protokollmitschnitt - Main Mode: Step 1, M1 (2/2)

```
Transform payload # 1
    Next payload: Transform (3)
    Length: 24
    Transform number: 1
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): 3DES-CBC (5)
    Hash-Algorithm (2): MD5 (1)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
Transform payload # 2
    Next payload: Transform (3)
    Length: 24
    Transform number: 2
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): IDEA-CBC (2)
    Hash-Algorithm (2): SHA (2)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
Transform payload # 3
    Next payload: Transform (3)
    Length: 24
    Transform number: 3
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): IDEA-CBC (2)
    Hash-Algorithm (2): MD5 (1)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
Transform payload # 4
    Next payload: Transform (3)
    Length: 28
    Transform number: 4
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): BLOWFISH-CBC (3)
    Key-Length (14): Key-Length (128)
    Hash-Algorithm (2): SHA (2)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
```

Angebot an Policy Teil 2

```
Transform payload # 5
    Next payload: Transform (3)
    Length: 28
    Transform number: 5
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): BLOWFISH-CBC (3)
    Key-Length (14): Key-Length (128)
    Hash-Algorithm (2): MD5 (1)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
Transform payload # 6
    Next payload: Transform (3)
    Length: 24
    Transform number: 6
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): CAST-CBC (6)
    Hash-Algorithm (2): SHA (2)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
Transform payload # 7
    Next payload: NONE (0)
    Length: 24
    Transform number: 7
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): CAST-CBC (6)
    Hash-Algorithm (2): MD5 (1)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
Vendor ID payload
    Next payload: NONE (0)
    Length: 20
    Vendor ID: unknown vendor ID: 0x76A24BC83FBD44BCAB267FBAC708F47A
```

Angebot an Policy Teil 2

IKE
→ Protokollmitschnitt - Main Mode: Step 1, M2

```
Frame 142 (134 bytes on wire, 134 bytes captured)
Internet Protocol, Src Addr: 192.168.200.30 (192.168.200.30), Dst Addr: 192.168.200.50
(192.168.200.50)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...0 = No encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 92
    Security Association payload
        Next payload: Vendor ID (13)
        Length: 44
        Domain of interpretation: IPSEC (1)
        Situation: IDENTITY (1)
        Proposal payload # 0
            Next payload: NONE (0)
            Length: 32
            Proposal number: 0
            Protocol ID: ISAKMP (1)
            SPI size: 0
            Number of transforms: 1
            Transform payload # 0
                Next payload: NONE (0)
                Length: 24
                Transform number: 0
                Transform ID: KEY_IKE (1)
                Encryption-Algorithm (1): 3DES-CBC (5)
                Hash-Algorithm (2): SHA (2)
                Authentication-Method (3): PSK (1)
                Group-Description (4): 1536 bit MODP group (5)
    Vendor ID payload
        Next payload: NONE (0)
        Length: 20
        Vendor ID: unknown vendor ID: 0x76A24BC83FBD44BCAB267FBAC708F47A
```

Payload # 0 wurde ausgewählt!

Pre-**s**hared secret **k**ey

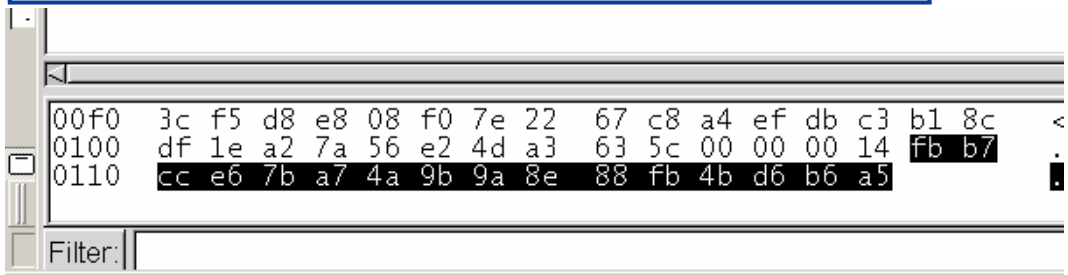
Angabe, welcher DH Public-Key aus der RFC 2409 verwendet werden soll

IKE
→ Protokollmitschnitt - Main Mode: Step 2, M3

```
Frame 143 (286 bytes on wire, 286 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Key Exchange (4)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...0 = No encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 244
    Key Exchange payload
        Next payload: Nonce (10)
        Length: 196
        Key Exchange Data
    Nonce payload
        Next payload: NONE (0)
        Length: 20
        Nonce Data
```

„Public Number“ von **192.168.200.50 (**Diffie Hellman)

Zufallszahl für die Authentikation von **192.168.200.50**

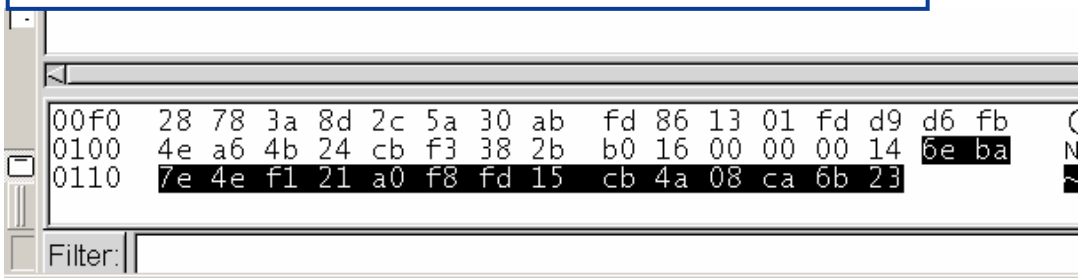


IKE
→ Protokollmitschnitt - Main Mode: Step 2, M4

```
Frame 144 (286 bytes on wire, 286 bytes captured)
Internet Protocol, Src Addr: 192.168.200.30 (192.168.200.30), Dst Addr: 192.168.200.50
(192.168.200.50)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Key Exchange (4)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...0 = No encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 244
    Key Exchange payload
        Next payload: Nonce (10)
        Length: 196
        Key Exchange Data
    Nonce payload
        Next payload: NONE (0)
        Length: 20
        Nonce Data
```

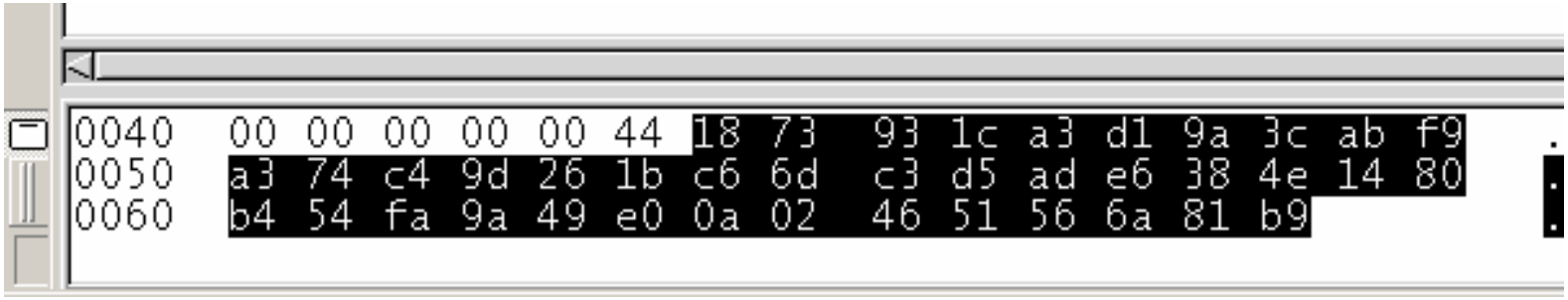
„Public Number“ von 192.168.200.30 (Diffie Hellman)

Zufallszahl für die Authentikation von 192.168.200.30



IKE
→ Protokollmitschnitt - Main Mode: Step 3, M5

```
Frame 145 (110 bytes on wire, 110 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Identification (5)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...1 = Encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 68
    Encrypted payload (40 bytes)
```



```
0040   00 00 00 00 00 44 18 73  93 1c a3 d1 9a 3c ab f9   .
0050   a3 74 c4 9d 26 1b c6 6d  c3 d5 ad e6 38 4e 14 80   .
0060   b4 54 fa 9a 49 e0 0a 02  46 51 56 6a 81 b9
```

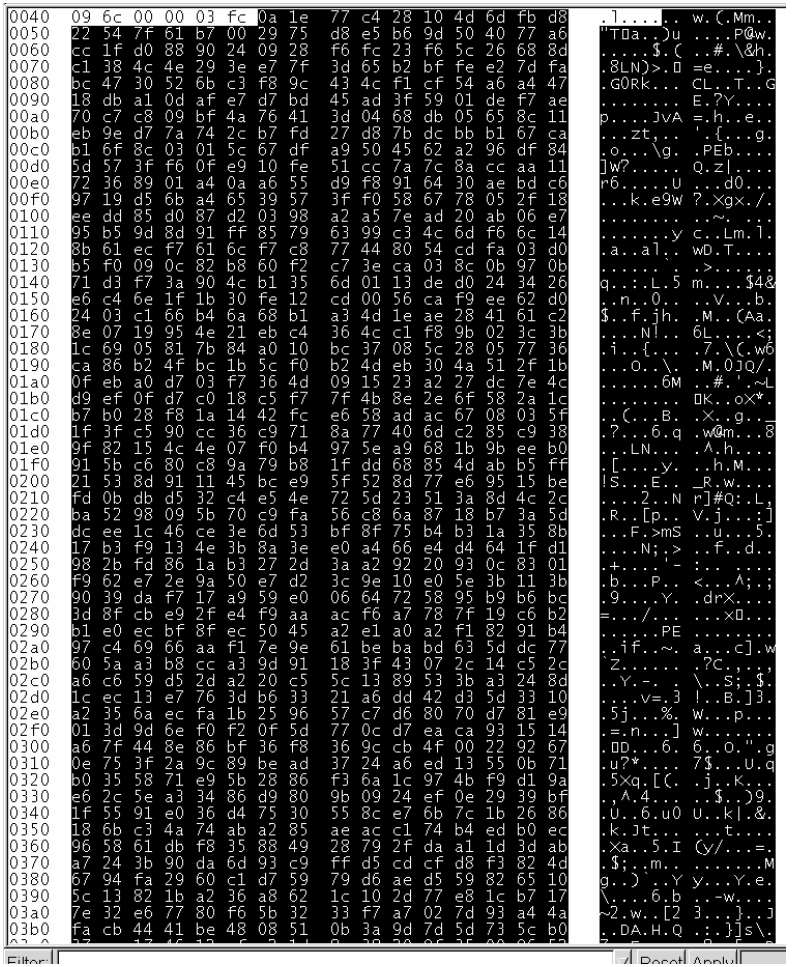
Da in diesem Step verschlüsselt wird, sehen wir nicht, was ausgehandelt wird!

IKE
→ Protokollmitschnitt - Main Mode: Step 3, M6

```
Frame 146 (110 bytes on wire, 110 bytes captured)
Internet Protocol, Src Addr: 192.168.200.30 (192.168.200.30), Dst Addr: 192.168.200.50
(192.168.200.50)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Identification (5)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...1 = Encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x00000000
    Length: 68
    Encrypted payload (40 bytes)
```

IKE
→ Protokollmitschnitt - Quick Mode: M1

```
Frame 147 (1062 bytes on wire, 1062 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags
        .... ...1 = Encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x9C92096C
    Length: 1020
    Encrypted payload (992 bytes)
```



IKE
→ Protokollmitschnitt - Quick Mode: M2

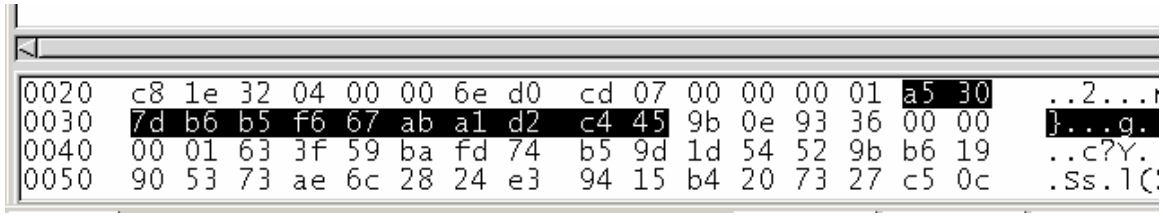
```
Frame 148 (206 bytes on wire, 206 bytes captured)
Internet Protocol, Src Addr: 192.168.200.30 (192.168.200.30), Dst Addr: 192.168.200.50
(192.168.200.50)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags
        .... ...1 = Encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x9C92096C
    Length: 164
    Encrypted payload (136 bytes)
```

IKE
→ Protokollmitschnitt - Quick Mode: M3

```
Frame 149 (94 bytes on wire, 94 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 0xA2FAB77526000000
    Responder cookie: 0x8858C80E93000000
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags
        .... ...1 = Encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID: 0x9C92096C
    Length: 52
    Encrypted payload (24 bytes)
```

IPSec
→ Protokollmitschnitt - IPSec mit AH und ESP (1/7)

```
Frame 150 (150 bytes on wire, 150 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x6ed0cd07
    Sequence: 0x00000001
    ICV
Encapsulating Security Payload
    SPI: 0x9b0e9336
    Sequence: 0x00000001
    Data (84 bytes)
```

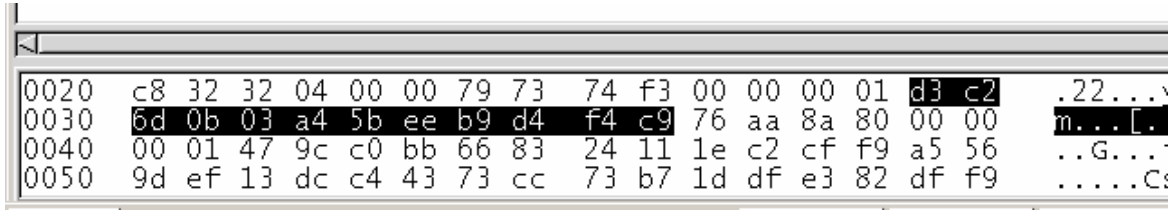



```
0000  63 3f 59 ba fd 74 b5 9d 1d 54 52 9b b6 19 90 53   c?Y..t...TR....S
0010  73 ae 6c 28 24 e3 94 15 b4 20 73 27 c5 0c 0e 31   s.l($.... s'...1
0020  5a e4 16 9d aa 22 05 ed a3 52 4b e8 75 ba 12 7d   Z...."...RK.u..}
0030  8c db b9 6e 1c 2e 42 3f eb f6 79 08 ae d5 a1 8a   ...n..B?..y.....
0040  59 17 f0 4e c2 0a 3e e7 08 1e ca 07 95 a8 43 80   Y..N..>.......C.
0050  c4 28 ec 5a                                       .(.Z
```

IPSec

→ Protokollmitschnitt - IPSec mit AH und ESP (2/7)

```
Frame 151 (134 bytes on wire, 134 bytes captured)
Internet Protocol, Src Addr: 192.168.200.30 (192.168.200.30), Dst Addr: 192.168.200.50
(192.168.200.50)
Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x797374f3
    Sequence: 0x00000001
    ICV
Encapsulating Security Payload
    SPI: 0x76aa8a80
    Sequence: 0x00000001
    Data (68 bytes)
```



```
0020   c8 32 32 04 00 00 79 73  74 f3 00 00 00 01 d3 c2   .22...
0030   6d 0b 03 a4 5b ee b9 d4  f4 c9 76 aa 8a 80 00 00   m...[.
0040   00 01 47 9c c0 bb 66 83  24 11 1e c2 cf f9 a5 56   ..G...
0050   9d ef 13 dc c4 43 73 cc  73 b7 1d df e3 82 df f9   .....Cs
```

```
0000  47 9c c0 bb 66 83 24 11 1e c2 cf f9 a5 56 9d ef   G...f.$......V..
0010  13 dc c4 43 73 cc 73 b7 1d df e3 82 df f9 c0 6a   ...Cs.s........j
0020  4c 5a 90 35 f2 6c ae d7 ee 60 c1 6e 47 bf 1c 9d   LZ.5.l...`.nG...
0030  d6 e1 6a 68 ff 24 cf ff 38 0b e9 ec 81 75 ec c1   ..jh.$..8....u..
0040  70 44 ea d8                                       pD..
```

IPSec
→ Protokollmitschnitt - IPSec mit AH und ESP (3/7)

```
Frame 152 (134 bytes on wire, 134 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x6ed0cd07
    Sequence: 0x00000002
    ICV
Encapsulating Security Payload
    SPI: 0x9b0e9336
    Sequence: 0x00000002
    Data (68 bytes)

0000  89 8b 81 a1 3e a4 9d 19 f8 ae 19 bd d8 f5 a8 51   ....>..........Q
0010  9a 47 34 01 c2 ec e8 98 b6 34 88 43 65 f6 71 91   .G4......4.Ce.q.
0020  ad b1 95 62 ee 7e 32 9e d8 c9 c0 8b 5c a5 2d fc   ...b.~2.....\.-.
0030  6d c3 14 c6 f6 e6 9f d5 41 20 1a fe cc 4e 30 32   m.......A ...N02
0040  90 e5 a7 36                                       ...6
```

IPSec

→ Protokollmitschnitt - IPSec mit AH und ESP (4/7)

```
Frame 153 (150 bytes on wire, 150 bytes captured)
Internet Protocol, Src Addr: 192.168.200.30 (192.168.200.30), Dst Addr: 192.168.200.50
(192.168.200.50)
Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x797374f3
    Sequence: 0x00000002
    ICV
Encapsulating Security Payload
    SPI: 0x76aa8a80
    Sequence: 0x00000002
    Data (84 bytes)

0000  42 c2 41 ce 1f d1 0d a9 1a 4b 44 d8 db 07 87 ee   B.A......KD.....
0010  00 72 23 2a 8e ce 19 47 54 de 6f c0 1e 60 1c 7c   .r#*...GT.o..`.|
0020  5c 80 5f 7b 6a 0b da 1a 54 89 60 ba 51 43 f4 3d   \._{j...T.`.QC.=
0030  3f 1a 6a 5a 97 d8 c9 02 b2 39 95 1d 2e ed 15 a9   ?.jZ.....9......
0040  61 cc 03 51 98 9b d6 c6 fe 24 9f 3c 60 32 a0 de   a..Q.....$.<`2..
0050  3a 3e ff 39                                       :>.9
```

IPSec
→ Protokollmitschnitt - IPSec mit AH und ESP (5/7)

```
Frame 154 (158 bytes on wire, 158 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x6ed0cd07
    Sequence: 0x00000003
    ICV
Encapsulating Security Payload
    SPI: 0x9b0e9336
    Sequence: 0x00000003
    Data (92 bytes)

0000  28 08 80 24 c2 4a 31 6d 89 89 5a 07 bb 57 83 d1   (..$.J1m..Z..W..
0010  cc 15 12 ab 3e a7 d3 f5 e0 63 40 91 d2 66 e1 9d   ....>....c@..f..
0020  c2 76 77 e5 6f 32 2e fe 10 1f e3 ed 9e 77 6e bf   .vw.o2.......wn.
0030  12 d6 37 52 90 e5 98 23 22 13 dc 71 83 18 d2 4e   ..7R...#"..q...N
0040  29 60 a4 72 92 5b 8c d1 cf 3c 05 17 91 d9 b6 f7   )`.r.[...<......
0050  2e bc 99 31 d0 cd f8 e7 df 17 0f 25               ...1.......%
```

IPSec
→ Protokollmitschnitt - IPSec mit AH und ESP (6/7)

```
Frame 155 (134 bytes on wire, 134 bytes captured)
Internet Protocol, Src Addr: 192.168.200.50 (192.168.200.50), Dst Addr: 192.168.200.30
(192.168.200.30)
Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x6ed0cd07
    Sequence: 0x00000004
    ICV
Encapsulating Security Payload
    SPI: 0x9b0e9336
    Sequence: 0x00000004
    Data (68 bytes)

0000  82 11 d2 57 d2 d5 4e 97 13 ef 89 23 6e c0 c9 aa   ...W..N....#n...
0010  fb 60 cf 0b 59 6e 54 61 12 43 d3 cd bb 24 5c 07   .`..YnTa.C...$\.
0020  0b 33 ac e5 f7 69 09 5b d9 85 98 a4 ac 96 18 b7   .3...i.[........
0030  c4 55 ed a1 31 8e ec 73 d7 2b b4 f1 4d 10 3e 46   .U..1..s.+..M.>F
0040  dd ba 2d ed                                       ..-.
```

IPSec

→ Protokollmitschnitt - IPSec mit AH und ESP (7/7)

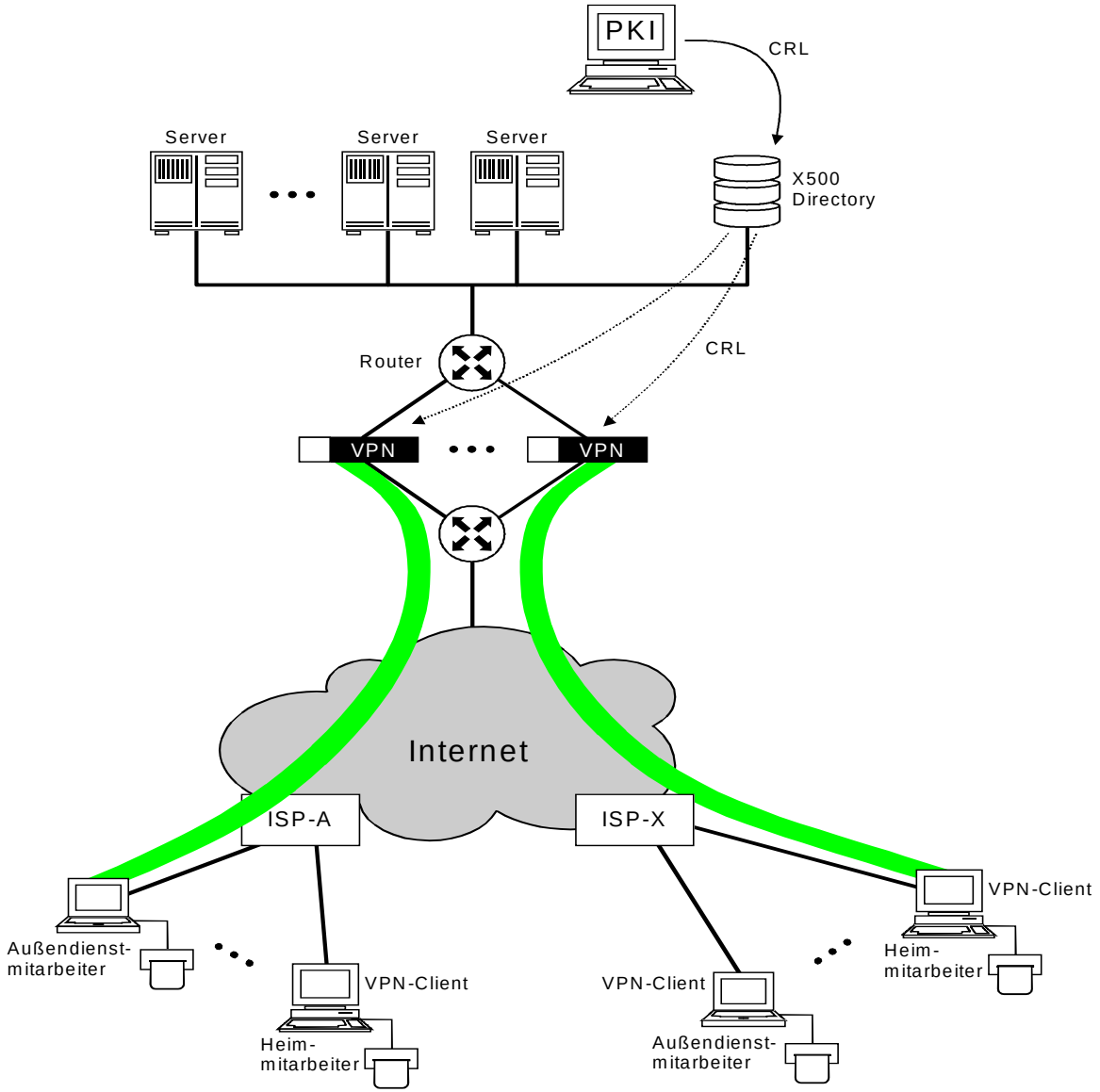
```
Frame 156 (134 bytes on wire, 134 bytes captured)
Internet Protocol, Src Addr: 192.168.200.30 (192.168.200.30), Dst Addr: 192.168.200.50
(192.168.200.50)
Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x797374f3
    Sequence: 0x00000003
    ICV
Encapsulating Security Payload
    SPI: 0x76aa8a80
    Sequence: 0x00000003
    Data (68 bytes)

0000  a1 6f 1f f2 82 7a 6f 6c e3 52 d0 64 c7 af 0f 75   .o...zol.R.d...u
0010  fa 1c 51 b7 43 8b 45 d9 3e 97 55 0b 3b 04 3c ec   ..Q.C.E.>.U.;.<.
0020  46 e7 59 3a d0 8b 45 0e 66 57 e7 e5 78 21 4d 1b   F.Y:..E.fW..x!M.
0030  0f 6f 57 71 bb fc 6c 42 08 fb dc ba 0e 1d d5 96   .oWq..lB........
0040  53 86 2f 42                                       S./B
```

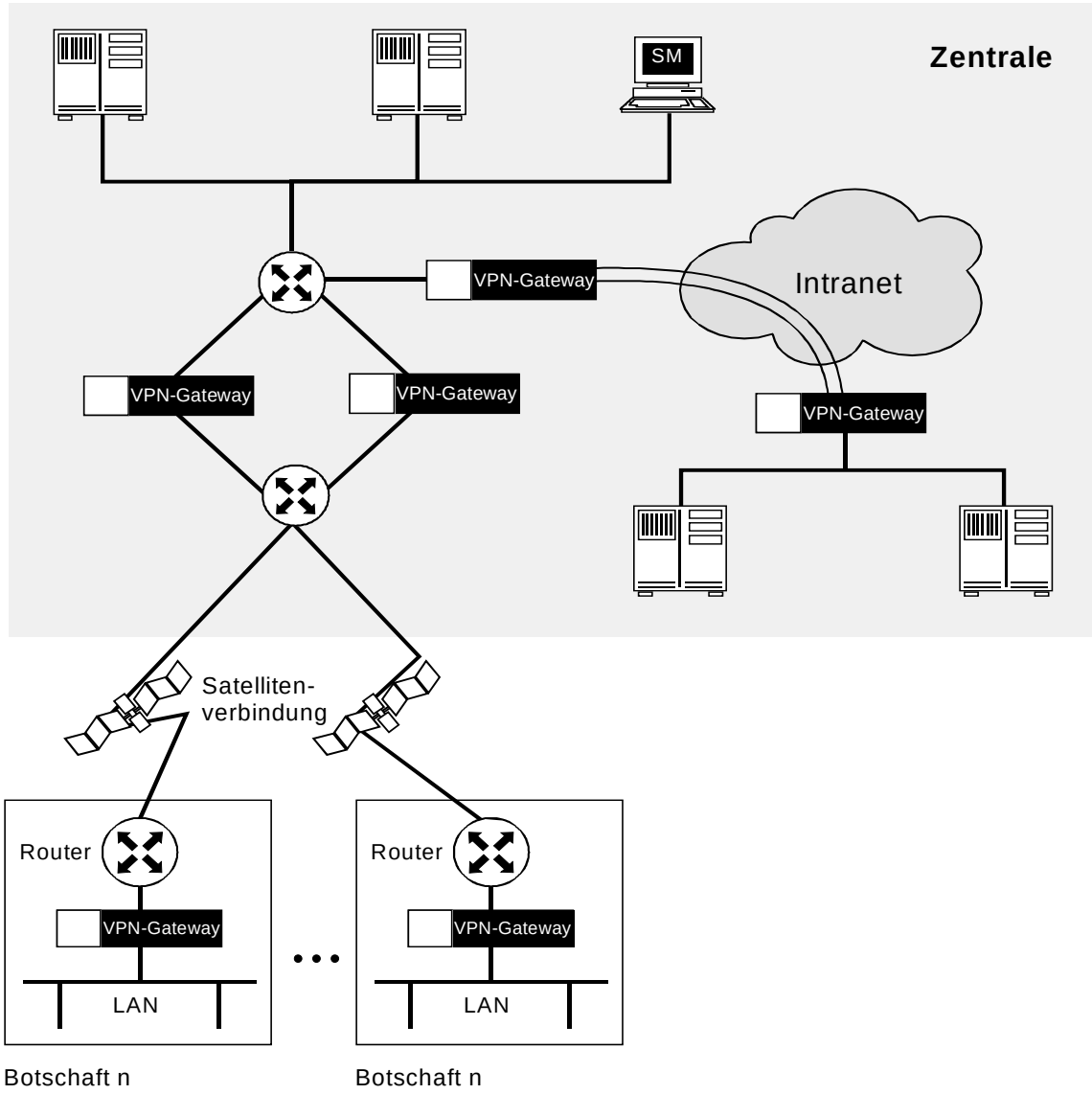
Inhalt

- Einleitung: Definitionen und Ziele
- Konzepte von VPNs und Anwendungsformen
- Ansätze für VPN Lösungen
- IPSec - Standard
- IPSec Schlüssel-Management (IKE)
- **Praktischer Einsatz von VPNs**
- IPSec Client
- Zusammenfassung

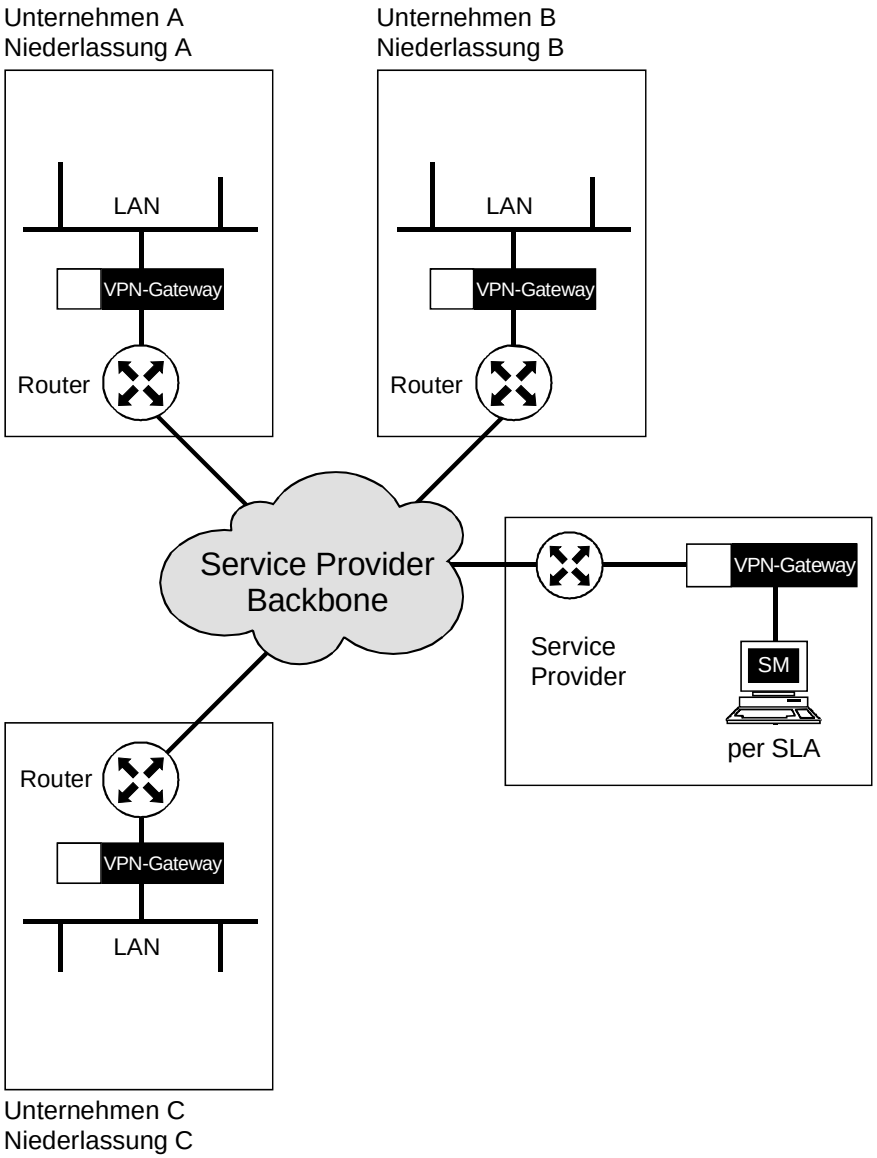
Praktischer Einsatz von VPNs (1/4)
→ Sichere Ankopplung (Authentikation mit PKI)



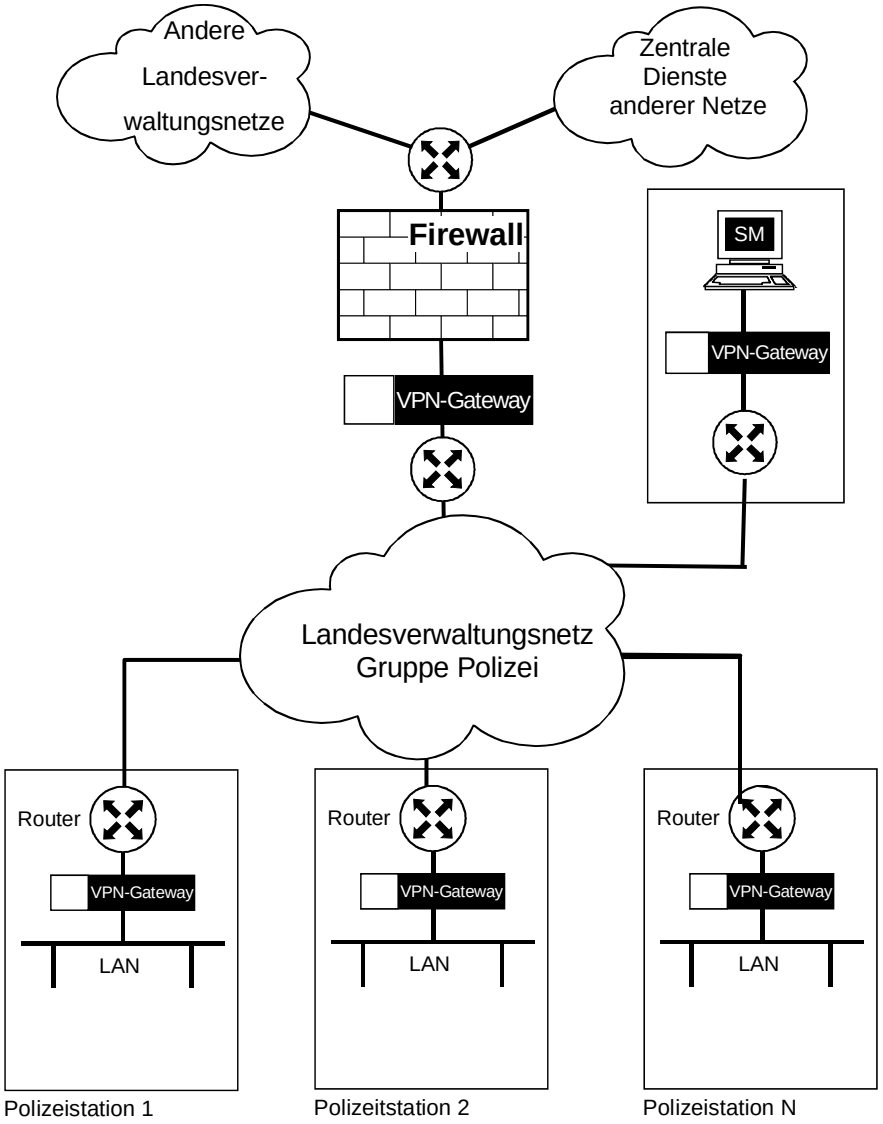
Praktischer Einsatz von VPNs (2/4)
→ Internationales IP-Netzwerk



Praktischer Einsatz von VPNs (3/4)
→ Angebot eines Service Provider



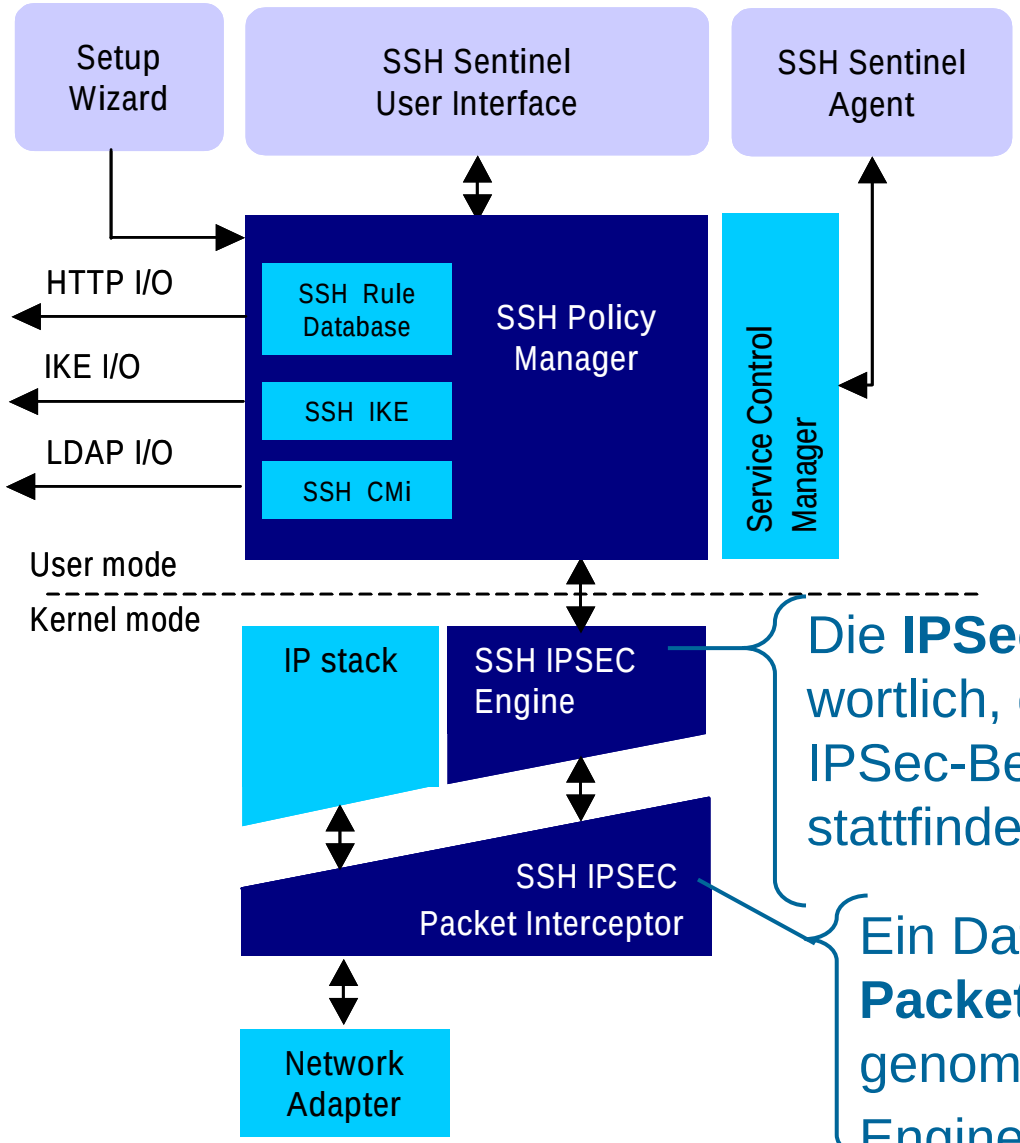
Praktischer Einsatz von VPNs (4/4)
→ Vertrauenswürdige Vernetzung



Inhalt

- Einleitung: Definitionen und Ziele
- Konzepte von VPNs und Anwendungsformen
- Ansätze für VPN Lösungen
- IPSec - Standard
- IPSec Schlüssel-Management (IKE)
- Praktischer Einsatz von VPNs
- **IPSec Client**
- Zusammenfassung

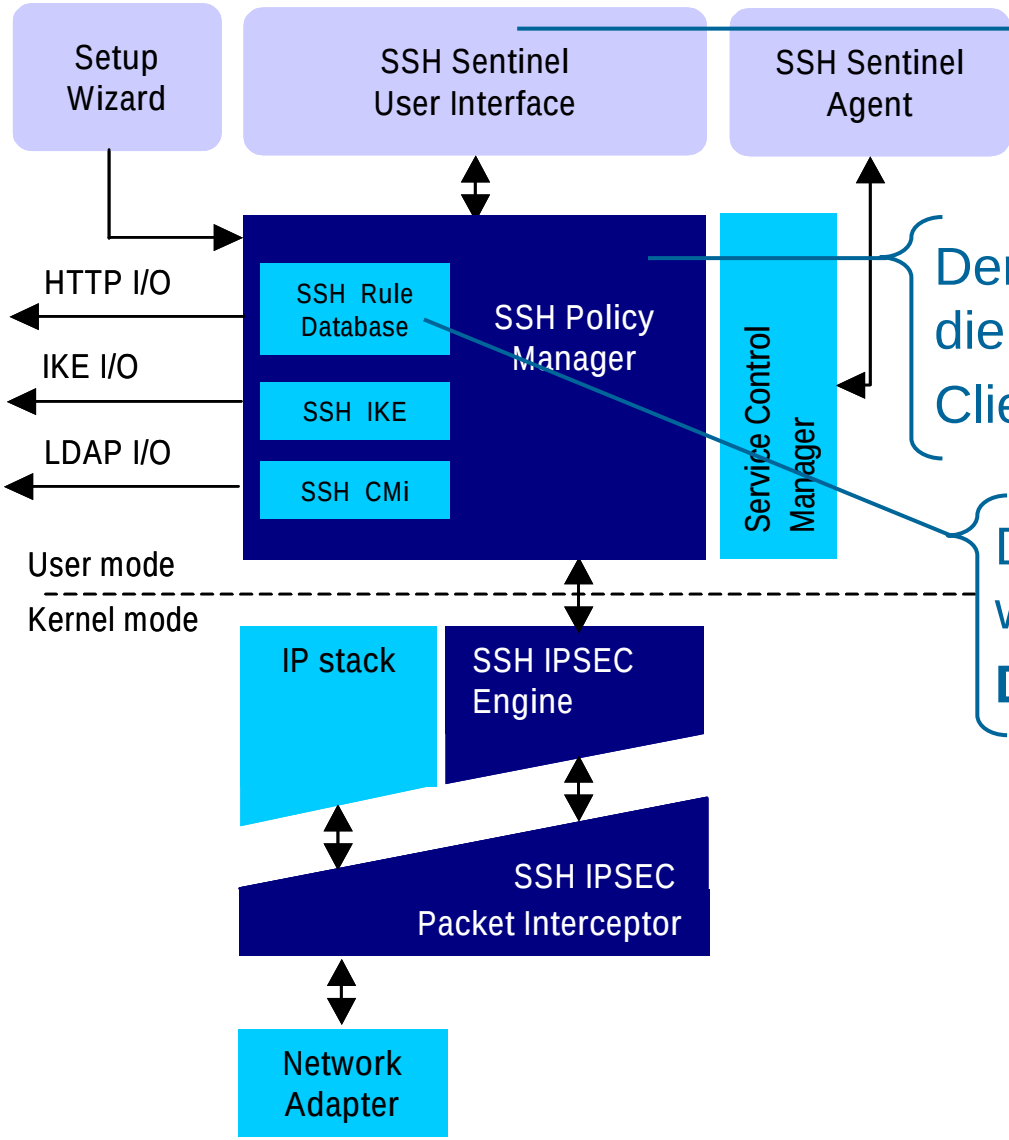
SSH Architektur



Die **IPSec Engine** ist dafür verantwortlich, dass die festgelegte IPSec-Behandlung der Pakete stattfindet.

Ein Datenpaket wird vom **IPSec Packet Interceptor** entgegengenommen und an die IPSec Engine weitergegeben.

SSH Architektur



Der Nutzer administriert die Regeln mit dem **User Interface**.

Der **Policy Manager** setzt die Security Policy des Client-Systems um.

Die Regeln der Policy werden in der **Rule Database** gespeichert.

Inhalt

- Einleitung: Definitionen und Ziele
- Konzepte von VPNs und Anwendungsformen
- Ansätze für VPN Lösungen
- IPSec - Standard
- IPSec Schlüssel-Management (IKE)
- Praktischer Einsatz von VPNs
- IPSec Client
- **Zusammenfassung**

Zusammenfassung
→ IPSec

- Jedes Paket wird vor Manipulation geschützt und kann zusätzlich verschlüsselt werden.
- IPSec-Realisierung durch zusätzliche Header (AH & ESP).
- Security Associations sind für die Policy, Algorithmen, Mechanismen und das Key-Management verantwortlich
- Die gesamte Kommunikation zwischen zwei Punkten ist aufgrund der Nutzung der Diffie-Hellman Mechanismen bei IPSec abgesichert.
- ... und IPSec ist ein weltweiter Sicherheitsstandard!

Zusammenfassung
→ Probleme der IPSec Standardisierung

- Der IPSec Standards ist **sehr umfangreich** und auf viele RFCs verteilt.
- Die Standards sind nicht immer eindeutig, das heißt es gibt an einigen Stellen **Interpretationspielräume**.
- Als Folge dieser Komplexität und wegen der Flexibilität der Standards, **ist die Interoperabilität nicht selbstvertändlich**.
- Gerade bei großen, heterogenen Netzen kann sie teilweise ohne den **Verzicht auf bestimmte Funktionalitäten** überhaupt nicht erreicht werden.
- Nutzung einer gemeinsamen Public-Key-Infrastruktur ?
- Flow-Control-Funktionen.
- Auswirkung auf die Routing Performance.
- IP-Pakete transportieren weniger Nutzdaten.
- Router müssen evtl. Daten fragmentieren.

Zusammenfassung
→ Kriterien für die Auswahl von VPN-Lösungen

- Vertrauenswürdigkeit
- Offenheit und Transparenz der Sicherheit
- Nachweis geprüfter Sicherheit
  - Evaluierung, Zertifizierung

- Sicherheit ohne staatliche Restriktionen wie
  - Reduzierte Schlüssellängen
  - Key Recovery
  - Key Escrow-Mechanismen
  - Trapdoors („Hintertüren“)

VPN-Systeme

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen