Fachhochschule Gelsenkirchen

# Die Rolle von VPNs für eine sichere externe Unternehmenskommunikation

**Prof. Dr. Norbert Pohlmann**

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
**https://www.internet-sicherheit.de**

if(is) internet-sicherheit.

# Inhalt

- Historischer Hintergrund
- Definitionen und Ziele von VPN-Systemen
- Konzepte von VPNs und Anwendungsformen
- Standards und Sicherheitsdienste
- Zusammenfassung

# Inhalt

- **Historischer Hintergrund**
- Definitionen und Ziele von VPN-Systemen
- Konzepte von VPNs und Anwendungsformen
- Standards und Sicherheitsdienste
- Zusammenfassung

# Historischer Hintergrund → VPN

- **seit 6000 Jahren gibt es Schrift,**
  **seit rund 3000 Jahren Verschlüsselung** und
  **seitdem auch den Versuch, die Verschlüsselung zu knacken!**
- Romeo und Julia
- **Maria Stuart und das Babington-Komplott 1586**


- Eintritt der USA in den 1. Weltkrieg: Zimmermann-Telegramm 1917
- **Enigma-Entschlüsselung**

- **Link- oder Netzverschlüsselungsgeräte**
  - 2 M Bit/s, 34 M Bit/s, usw.
  - X.25, Frame Relay, ATM, usw.

- **Mit IP (Internet) kamen VPNs**
  - Die ersten Geräte waren **firmenspezifisch**
  - Heute hat sich **IPSec** als Standard für die Sicherung der externen Unternehmenskommunikation durchgesetzt

# Unternehmenskommunikation
## → Situation heute, morgen, ...

- Es werden immer **wertvollere Daten** über Kommunikationsnetze ausgetauscht.
- **Die Angriffmöglichkeiten werden immer größer.**
- Aufgrund der zunehmenden Mobilität findet die Kommunikation im zunehmend **unsicheren Umgebungen statt.**
- Die Eintrittswahrscheinlichkeit eines Angriffes steigt zunehmend!
- **Jedes Verschlüsselungssystem wird irgendwann gebrochen!** (siehe Grundlagen der Verschlüsselung)

# Grundlagen der Verschlüsselung
## → Rechnerische, praktische Sicherheit

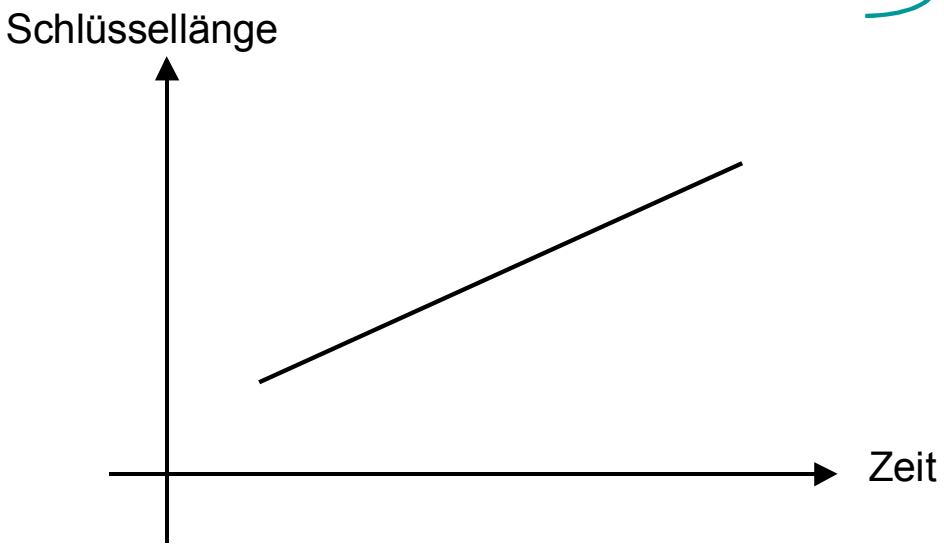
- Bei der **rechnerischen** oder **praktischen Sicherheit** ist es zwar **theoretisch möglich, das Kryptosystem zu brechen**, praktisch wird dazu jedoch so enorm viel Rechnerzeit bzw. Speicherplatz benötigt, dass dieser Weg einem jeden Kryptoanalytiker aussichtslos erscheinen muss.
- **Die meisten Informationen werden sowieso nach einer längeren Zeit wertlos.**
- Die rechnerische, praktische Sicherheit kann durch eine mathematische **Analyse der Komplexität** festgestellt werden.
  - In der Regel werden die kryptographischen Verfahren, die entwickelt werden, der **Kryptologen Gemeinde** (mehrere 100 Mathematiker in der Welt) zur Verfügung gestellt, damit die Kryptoanalyse beginnen kann.
  - **Vorstellung der Verfahren mit allen Design-Aspekten auf öffentlichen Konferenzen, wie z.B. Eurocrypt, Crypto, Asiacrypt, ...**
  - Erst, wenn **nach ca. 5 Jahren** keiner es geschafft hat, dass Verfahren zu brechen, gilt ein Verfahren als **praktisch sicher**.

# Grundlagen der Verschlüsselung
## → Geschwindigkeit von Computern

- Der Zeitfaktor und die Innovationen (z.B. Quantenrechner) müssen berücksichtigt werden

- **Praktische Sicherheit**
  - vor 20 Jahren eine Schlüssellänge von 64 Bit (*DES*
  - heute 128 Bit (*Triple DES, AES*)
  - für die nächsten 20 Jahre 256 Bit (*AES*)

**Alle 10 bis 15 Jahre ist ein Wechsel der Algorithmen notwendig!**



# Inhalt

- Historischer Hintergrund
- **Definitionen und Ziele von VPN-Systemen**
- Konzepte von VPNs und Anwendungsformen
- Standards und Sicherheitsdienste
- 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...«

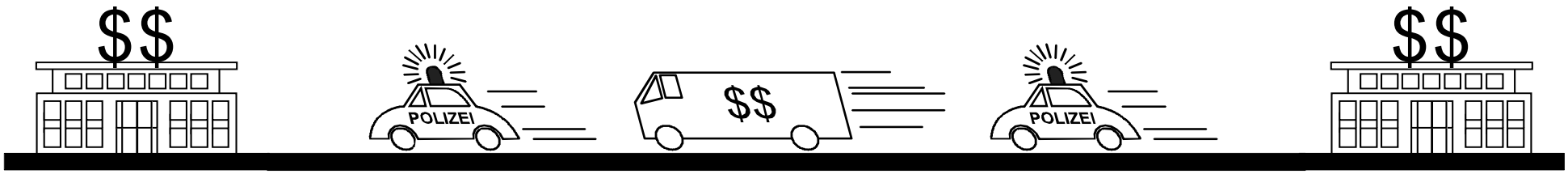
- **»Virtual«** bedeutet, dass es sich – aus Anwendersicht – scheinbar um nur »ein« Netzwerk handelt, auch wenn sich viele reale Teilnetzwerke hinter »einem« VPN verbergen.

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

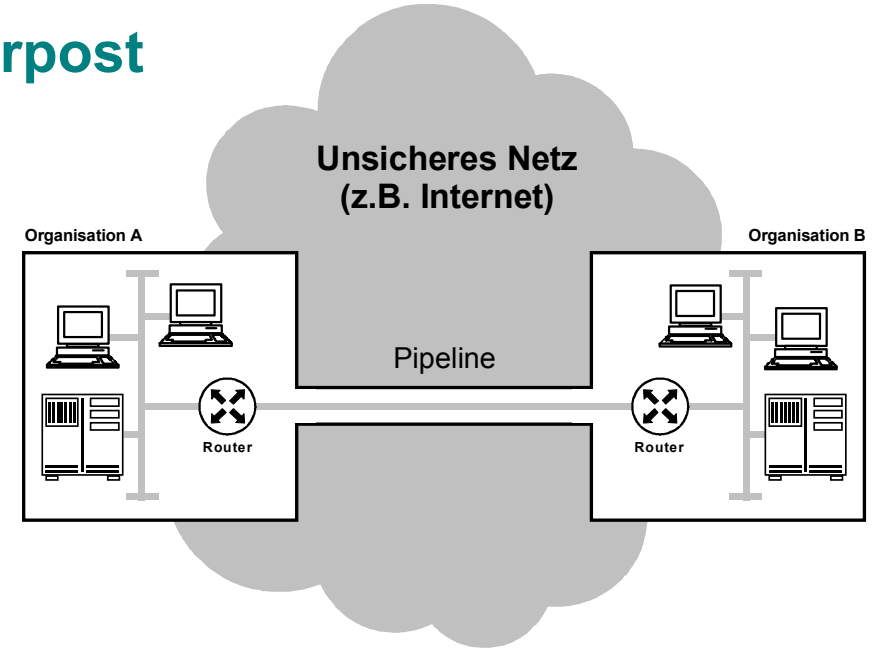
- **»Network«** bedeutet, dass eine definierte Gruppe von Rechnersystemen miteinander verbunden wird und mit Hilfe eines Protokolls (typischerweise ist das die TCP/IP-Protokollfamilie) kommuniziert.

# Analogien von VPN

- **Sicherheitstransporter**



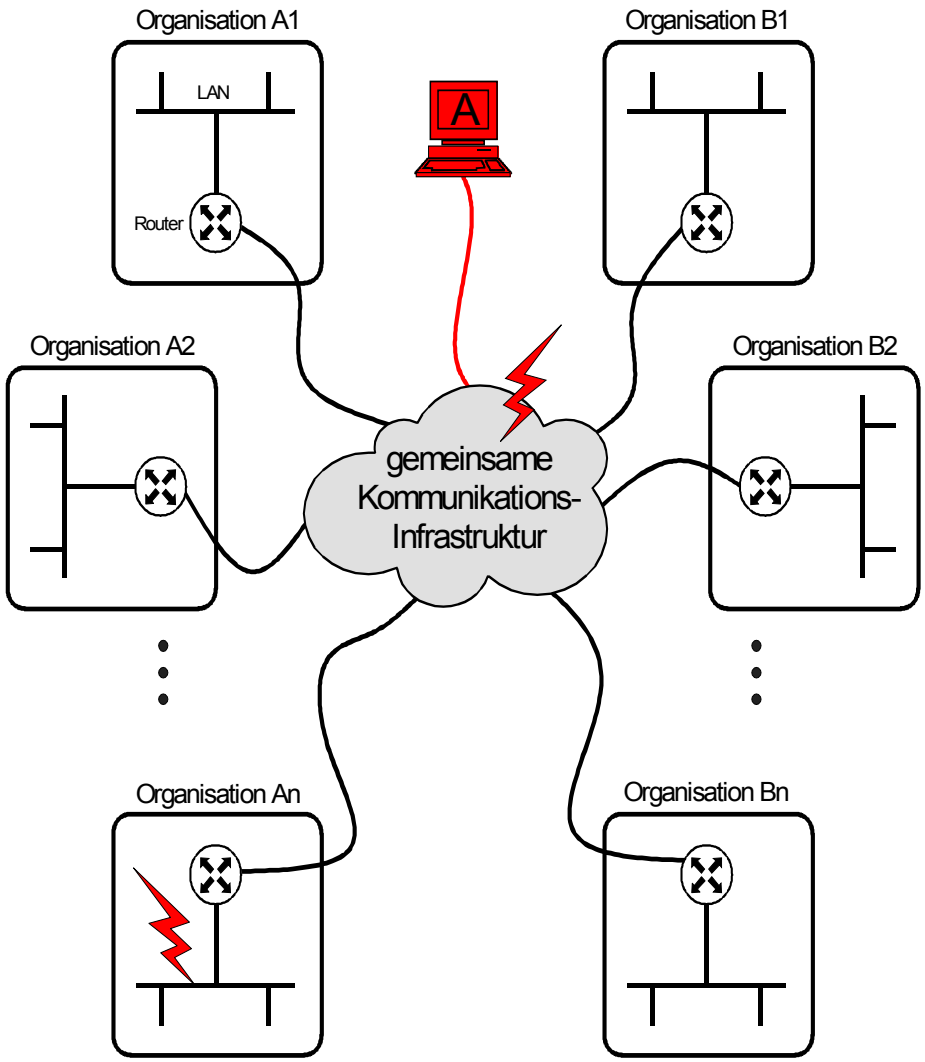

- **Pipeline und Rohrpost**



# Unternehmenskommunikation
## → 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



# Virtual Private Networks
## → Idee

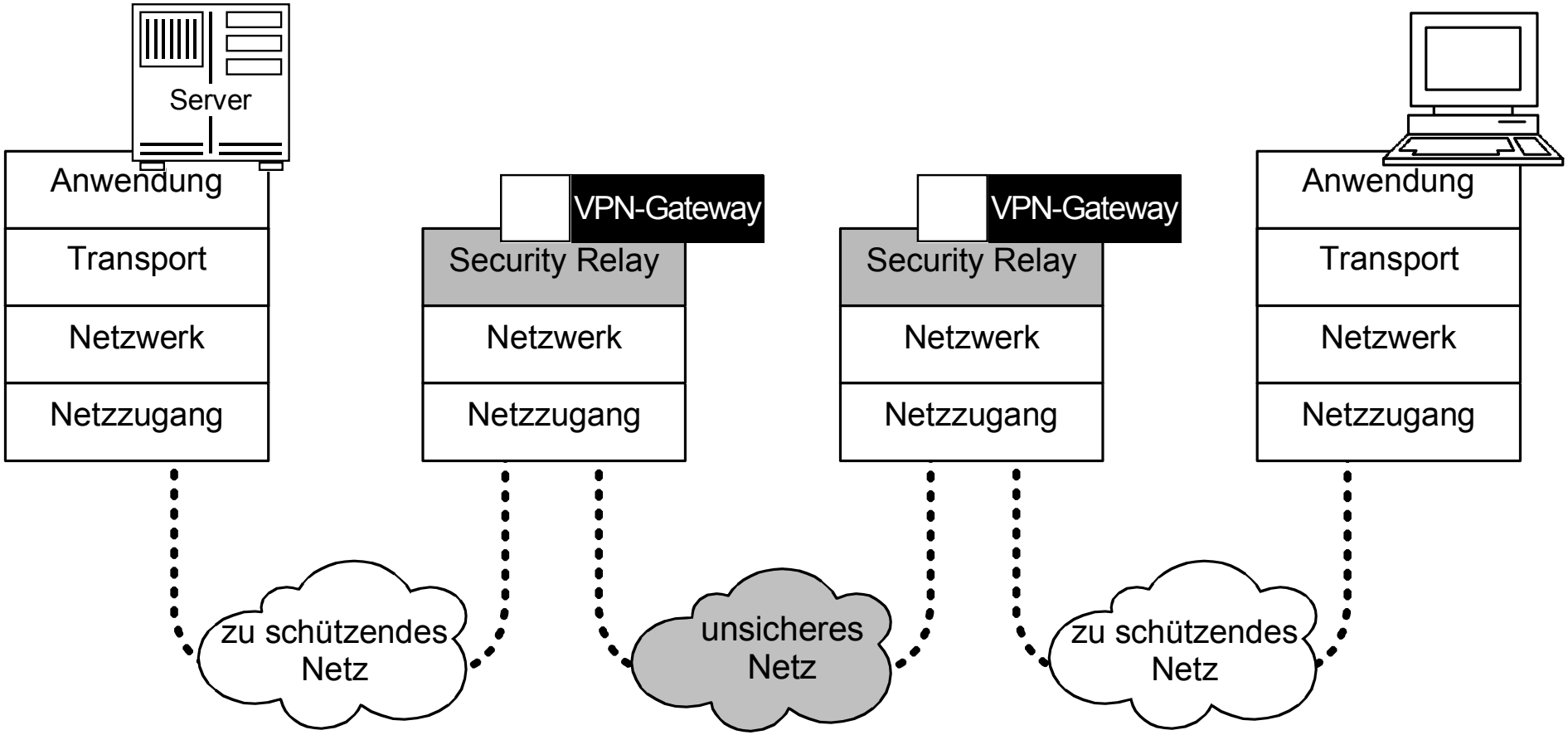
- **Grundsätzliche Idee bei Virtual Private Networks (VPNs):**
  - offene Kommunikationsinfrastruktur z.B. Internet nutzen
    - kostengünstig,
    - weltweit verfügbar **UND**
  - **allen Bedrohungen und Risiken sinnvoll entgegenwirken**

- **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

- Historischer Hintergrund
- Definitionen und Ziele von VPN-Systemen
- **Konzepte von VPNs und Anwendungsformen**
- Standards und Sicherheitsdienste
- Zusammenfassung

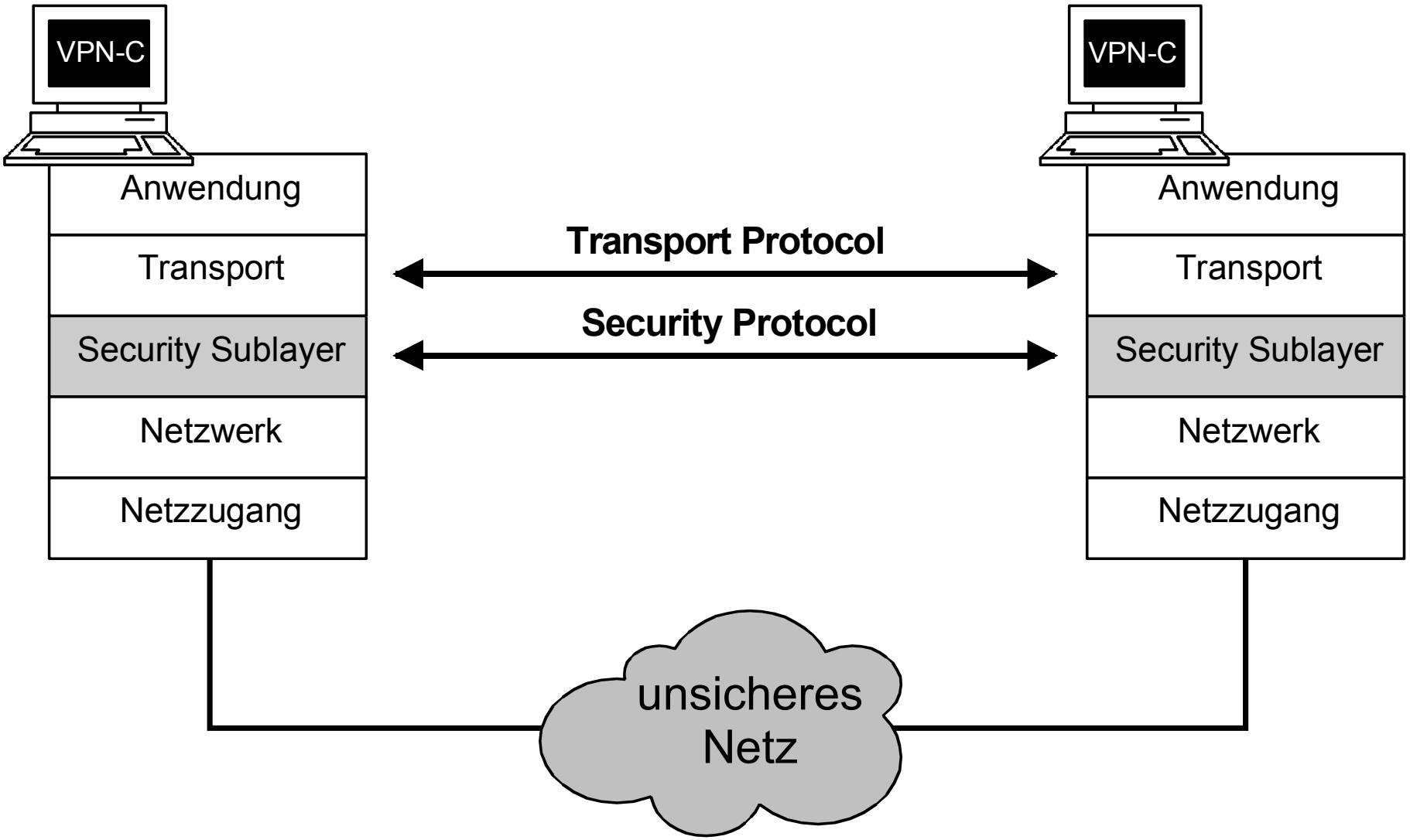
# Konzepte
## → VPN-Gateway



# 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 98/NT/2000/XP, ..., 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.**

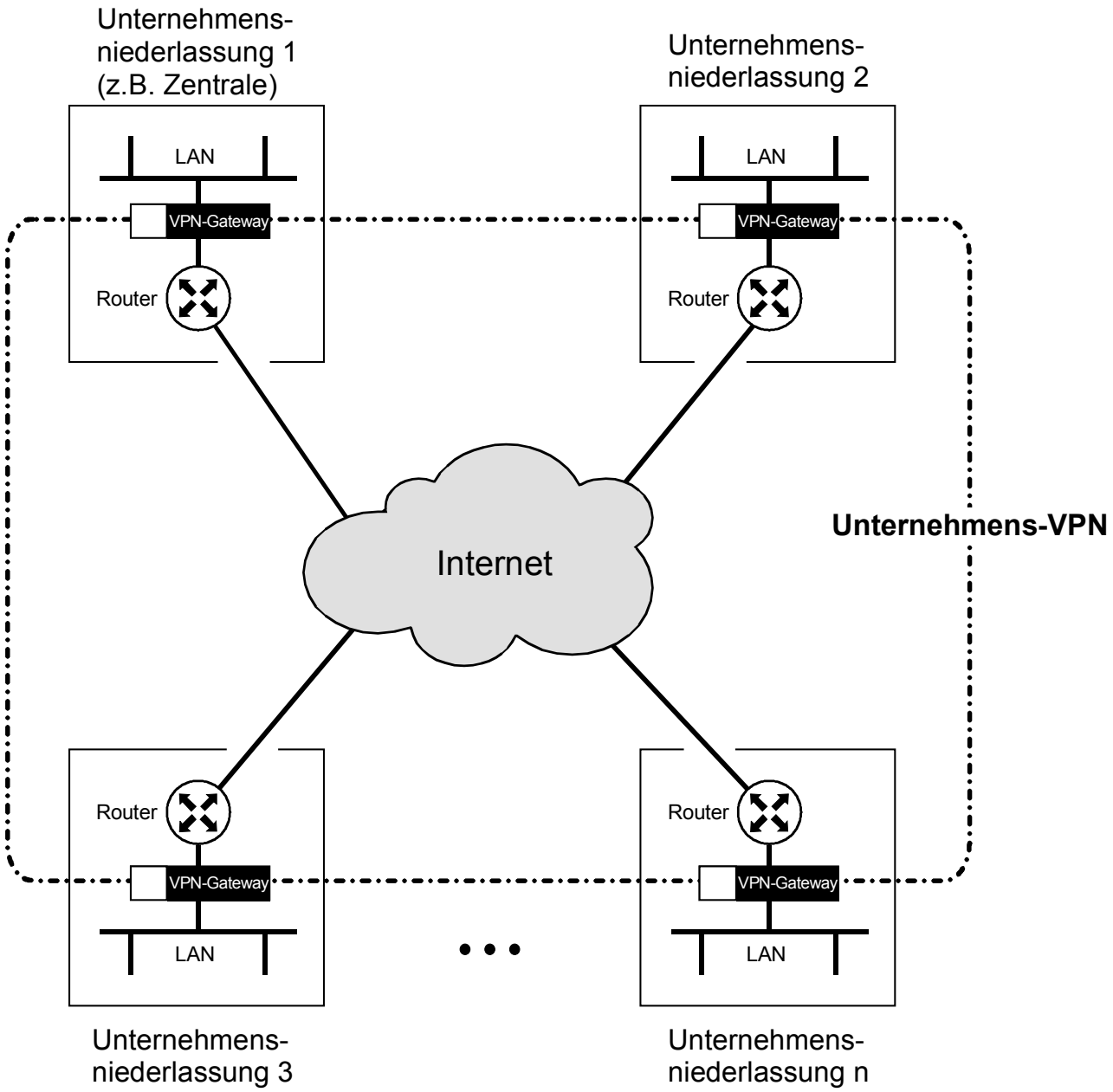
# Konzepte
## → VPN-Client



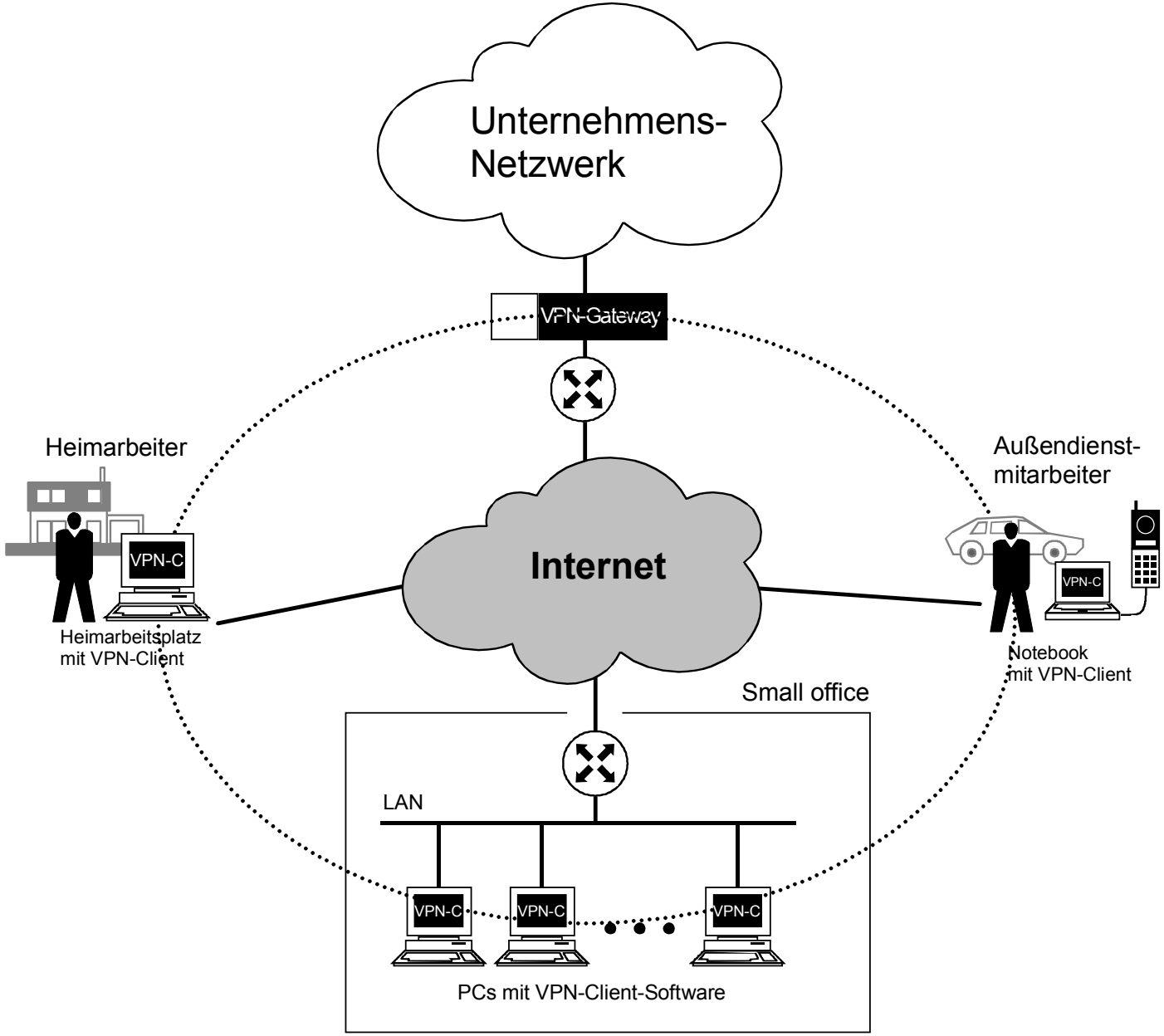
# Konzepte
## → Vorteile einer VPN-Client-Lösung

- 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.**

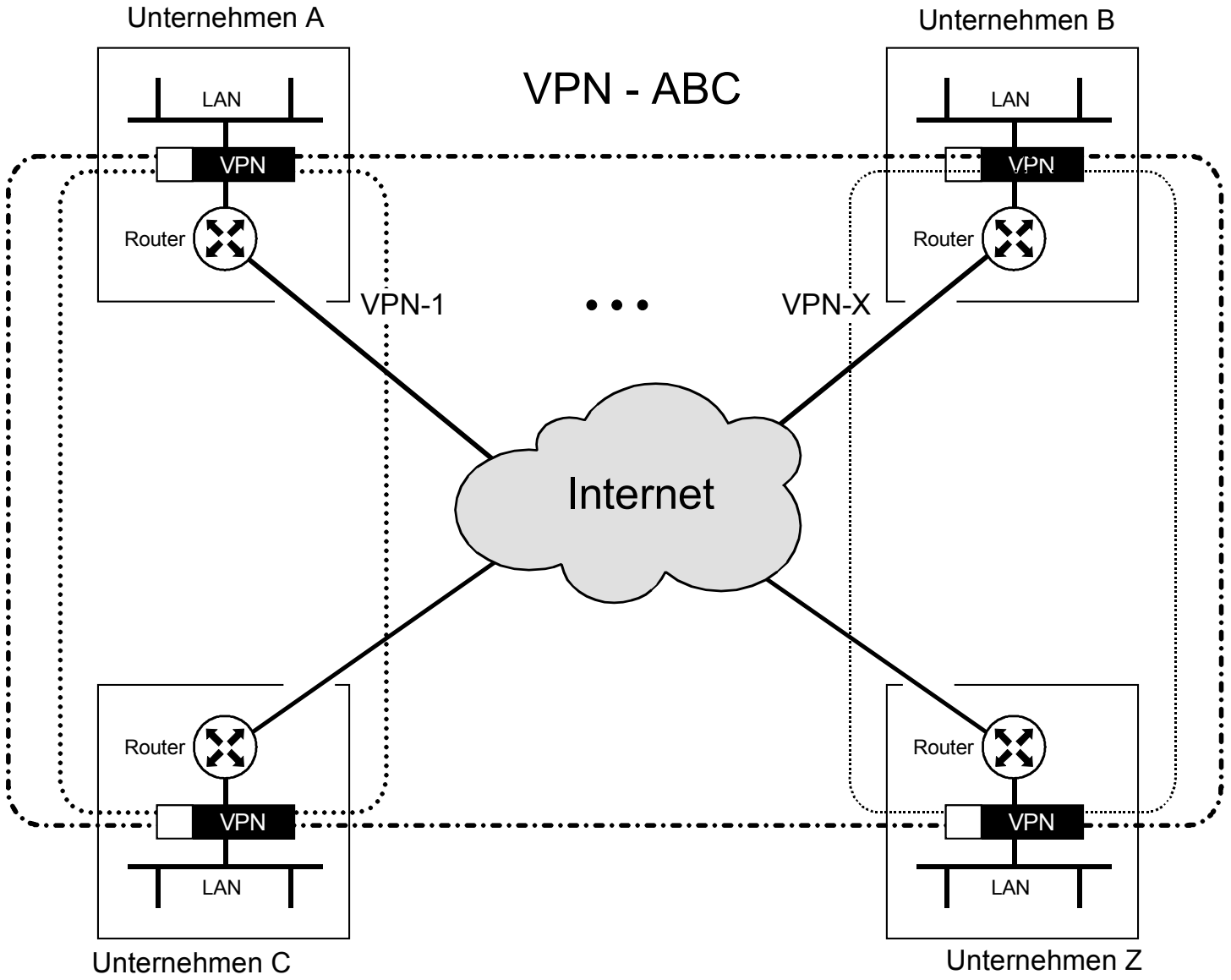
# Anwendungsformen von VPNs (1/4)
## → Unternehmensweites VPN



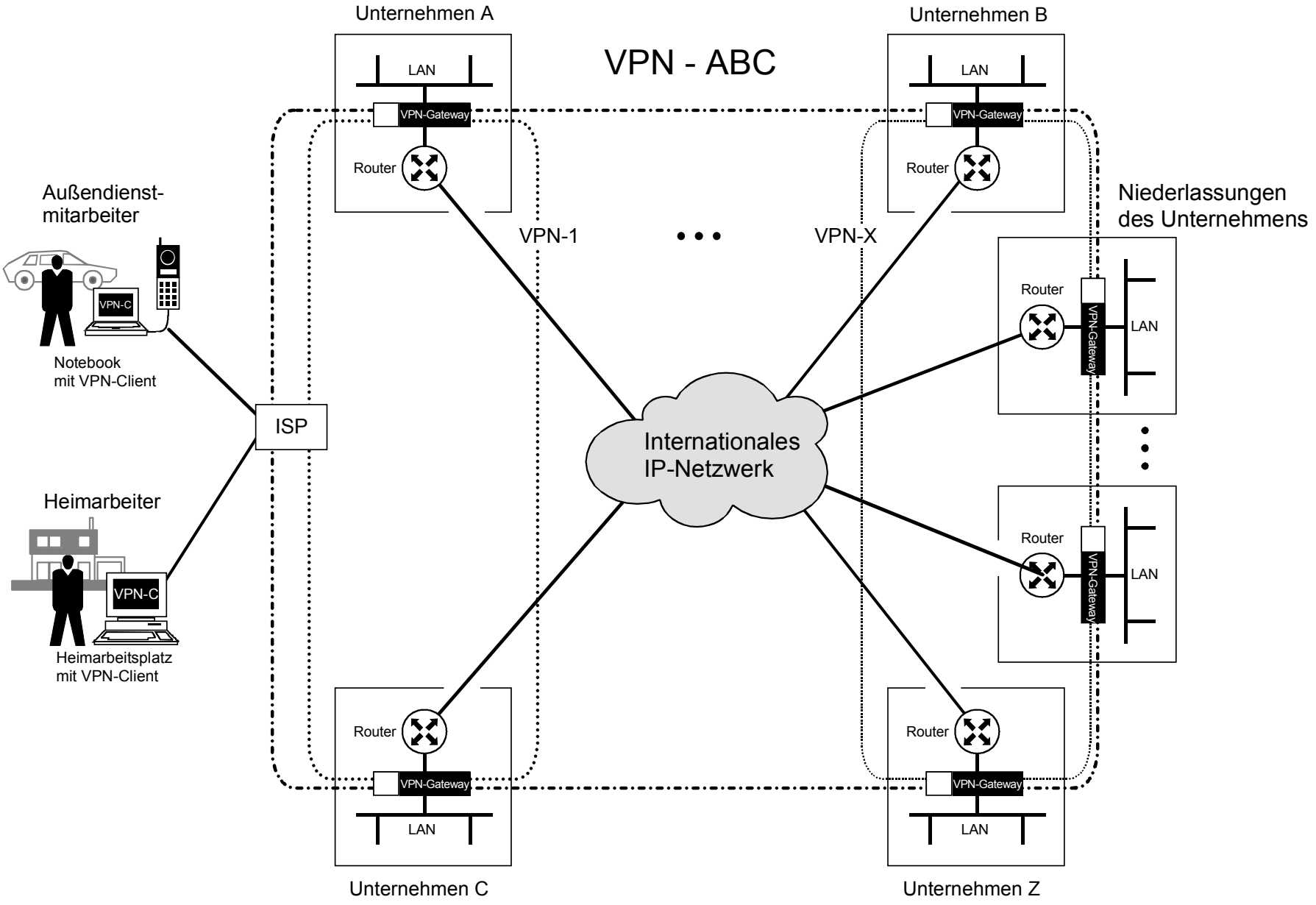
# Anwendungsformen von VPNs (2/4)
## → Sichere Remote-Ankopplung



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



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



# Inhalt

- Historischer Hintergrund
- Definitionen und Ziele von VPN-Systemen
- Konzepte von VPNs und Anwendungsformen
- **Standards und Sicherheitsdienste**
- Zusammenfassung

# 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.**

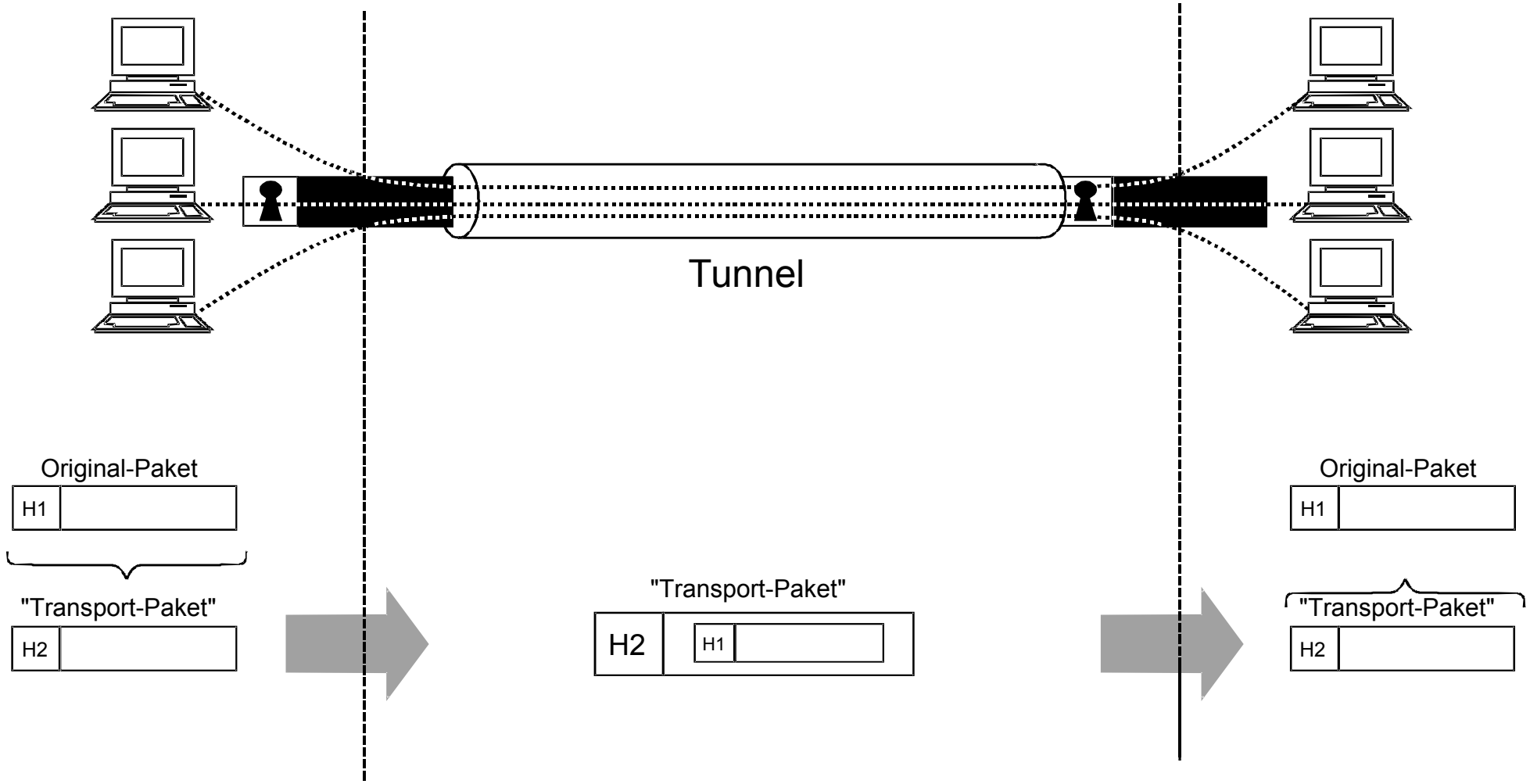
# IPSec
## → Übersicht der Mechanismen

- 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)

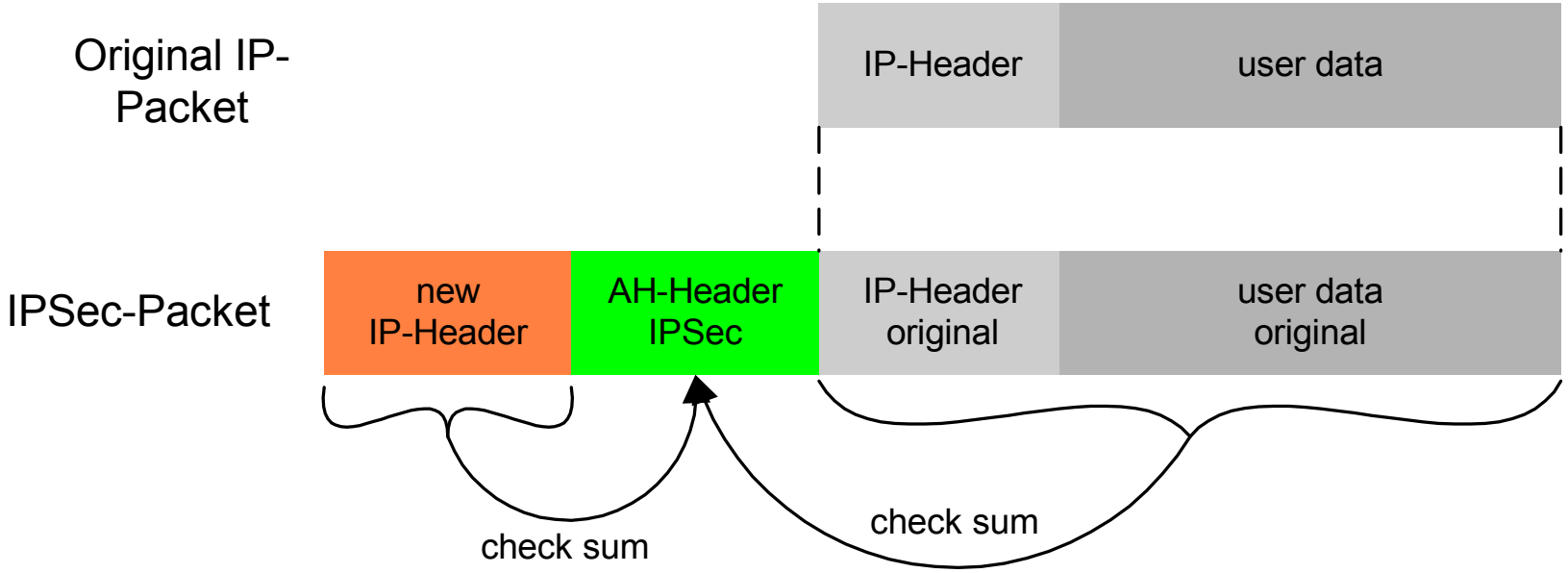
**'Transport-Mode'** = Verschlüsselung der Nutzdaten

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

# IPSec Tunneling
## → Idee



# Authentication Header (Tunnel-Mode) → Übersicht

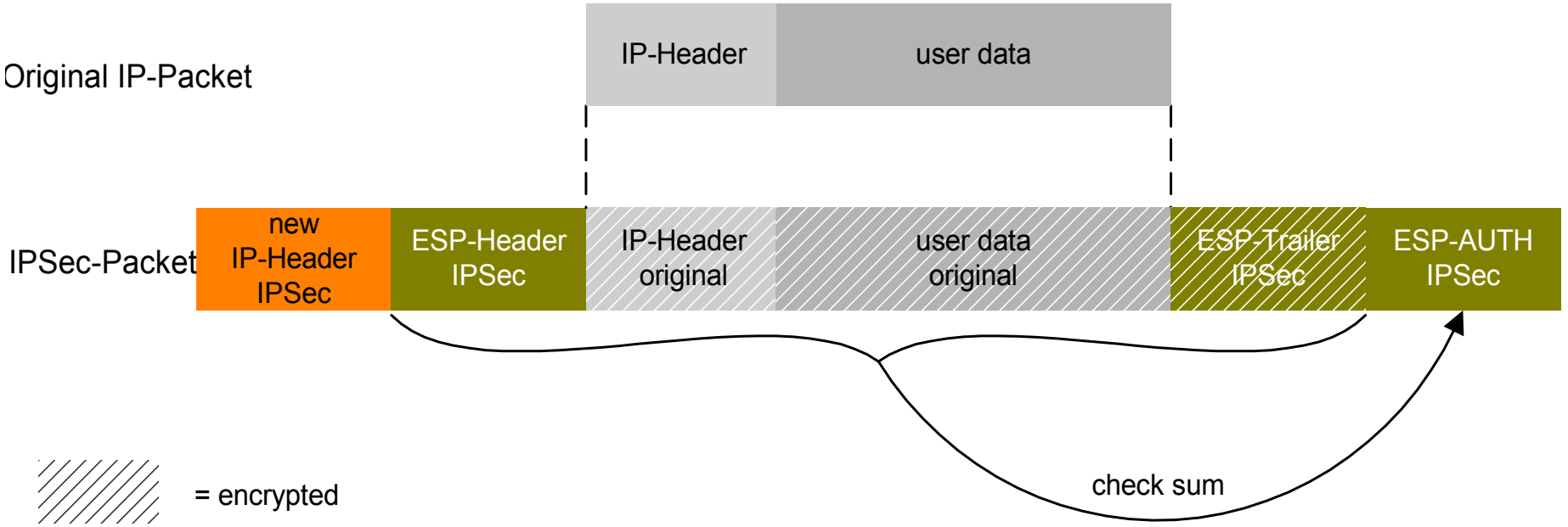



- Starke Integrität und Authentizität der IP Pakete
- HMAC (z.B. mit SHA-1) über das gesamte IP Paket, außer
  - Feldern, die während des Transportes modifiziert werden (Time to Live (TTL), TOS, Flags, Header Checksum, ...)
  - dem Authentication-Feld selbst

# Authentication Header (AH)
## → 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
## → Übersicht (Tunnel-Mode)




- 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“)

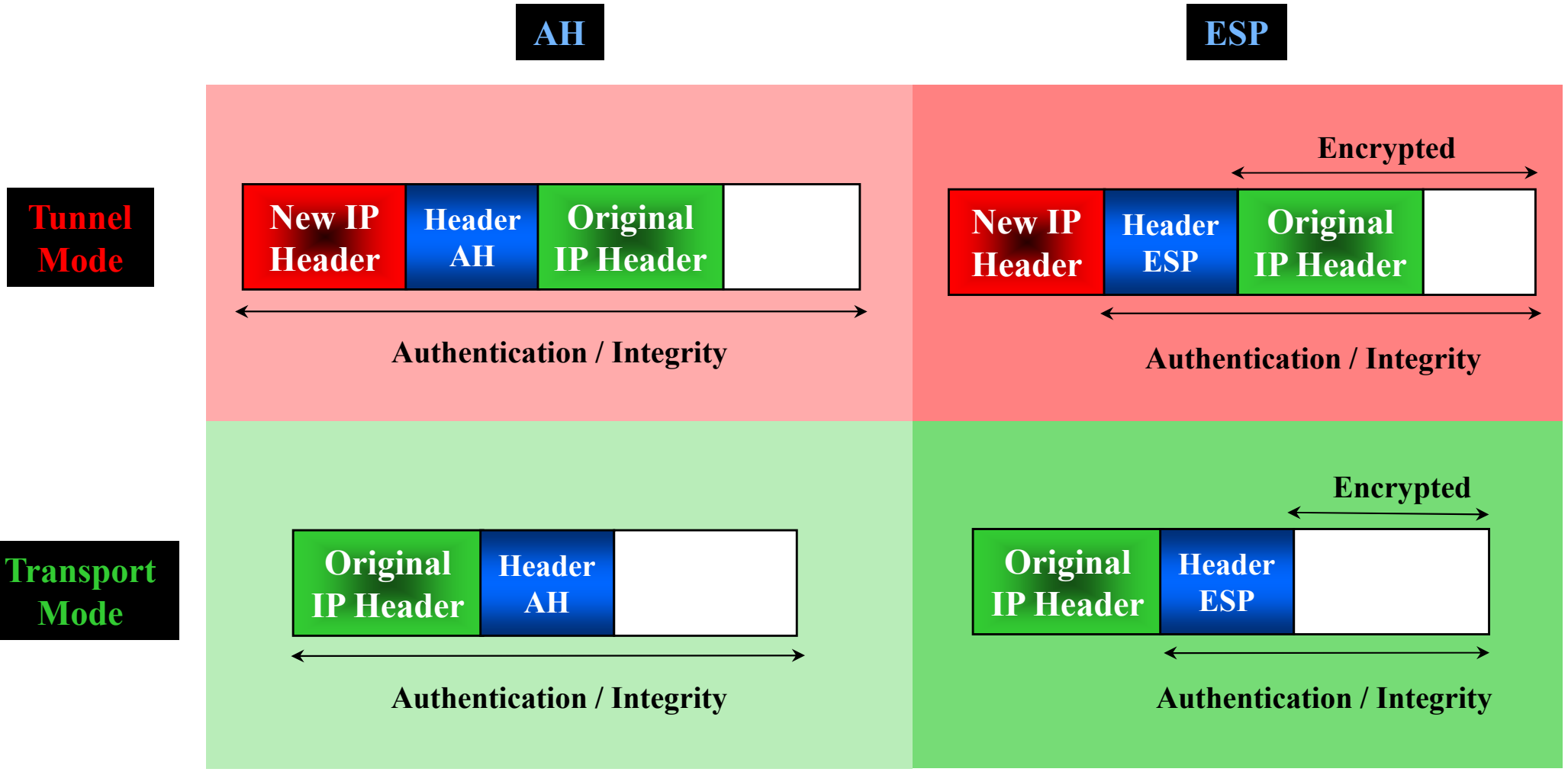
# Encapsulated Security Payload (ESP) → Zusammenfassung

- 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!

# IPSec
## → Schutz in Abhänigkeit: Mode/Protokoll

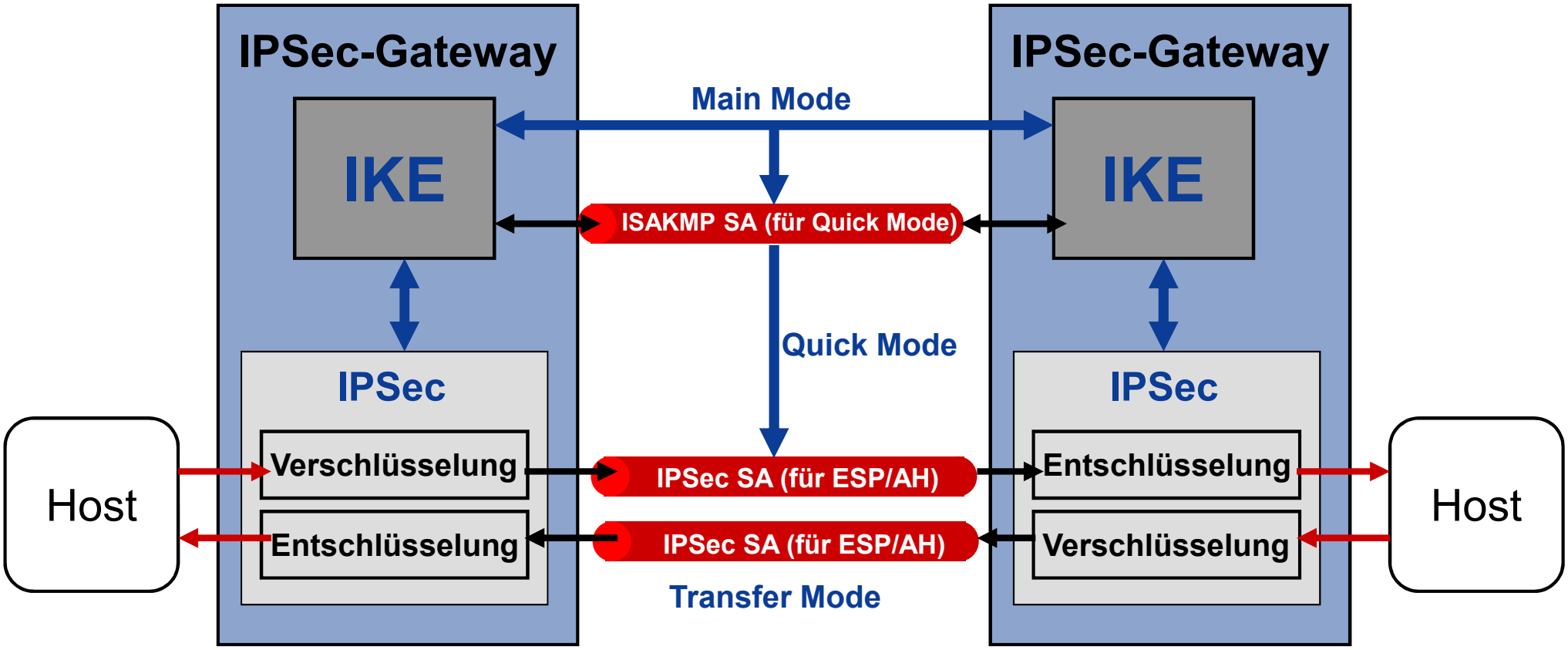


# IKE
# → Schlüssel-Management

- **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.

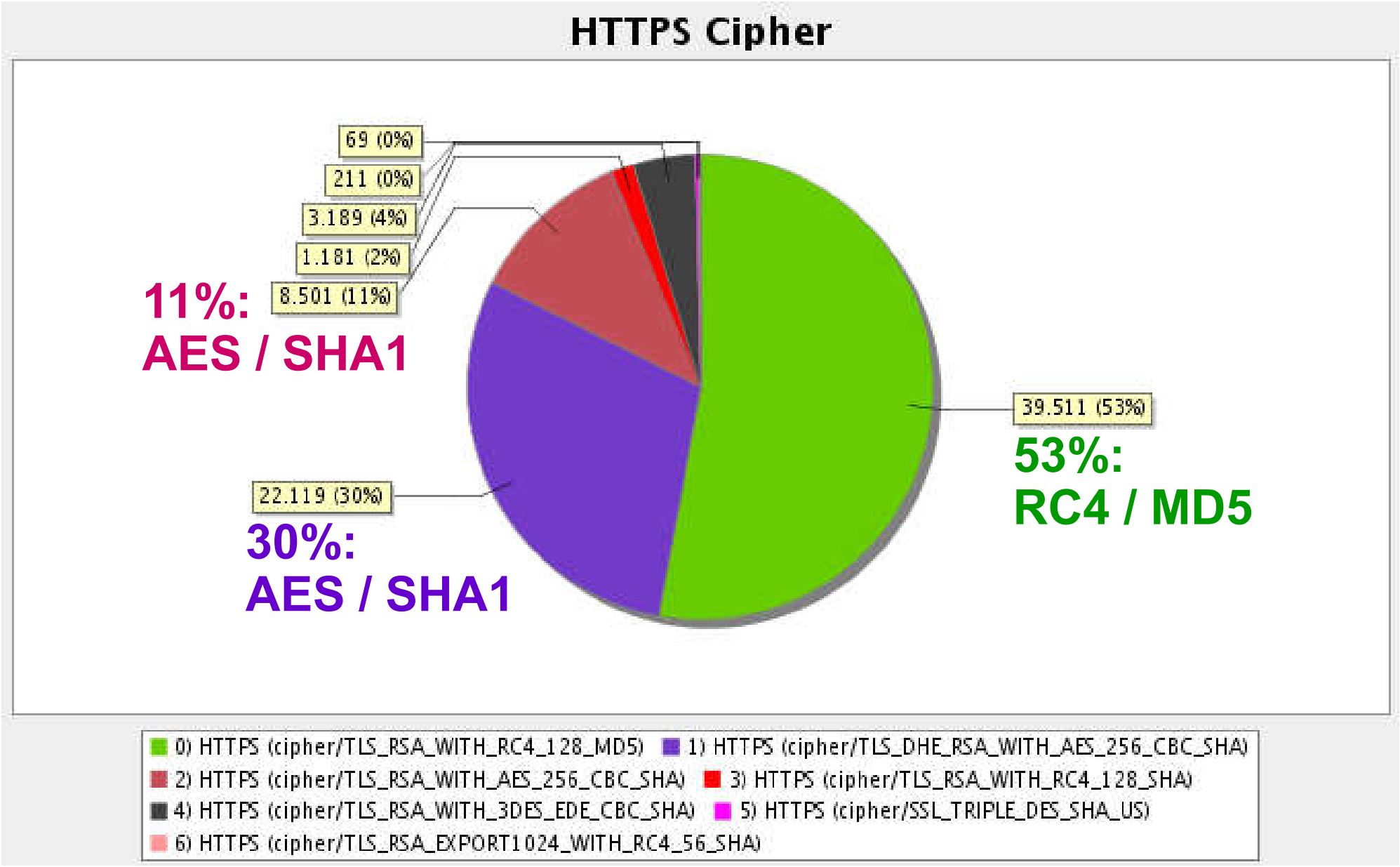
- **IKE - Internet Key Exchange**
  - IKE ist das offizielle Schlüsseltransferprotokoll von IPSec.
  - Beide Seiten brauchen nur eine **identische Passphrase (Pre-Shared Key).**
  - Darauf basierend wird unter dem Einsatz des Diffie-Hellman-Protokolls ausgehandelt, z.B. welche Algorithmen zur Verschlüsselung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

# 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

# Transparenz
## → Problem: Auswahl der Profile



# Inhalt

- Historischer Hintergrund
- Definitionen und Ziele von VPN-Systemen
- Konzepte von VPNs und Anwendungsformen
- Standards und Sicherheitsdienste
- **Zusammenfassung**

# Zusammenfassung
## → Die Rolle von VPNs

- **VPNs sind ein sehr geeignetes Mittel, die externe Unternehmenskommunikation angemessen zu sichern!**

- **Kriterien für die Auswahl von VPN-Lösungen**
  - Vertrauenswürdigkeit
  - Offenheit und Transparenz der Sicherheit
  - Sicherheit ohne staatliche Restriktionen wie
    - Reduzierte Schlüssellängen
    - Key Recovery und Key Escrow-Mechanismen
    - Trapdoors („Hintertüren“)
  - **Nachweis geprüfter Sicherheit**
    - Evaluierung, Zertifizierung

Fachhochschule Gelsenkirchen

# Die Rolle von VPNs für eine sichere externe Unternehmenskommunikation

## Vielen Dank für Ihre Aufmerksamkeit
## Fragen ?

**Prof. Dr. Norbert Pohlmann**

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
**https://www.internet-sicherheit.de**