

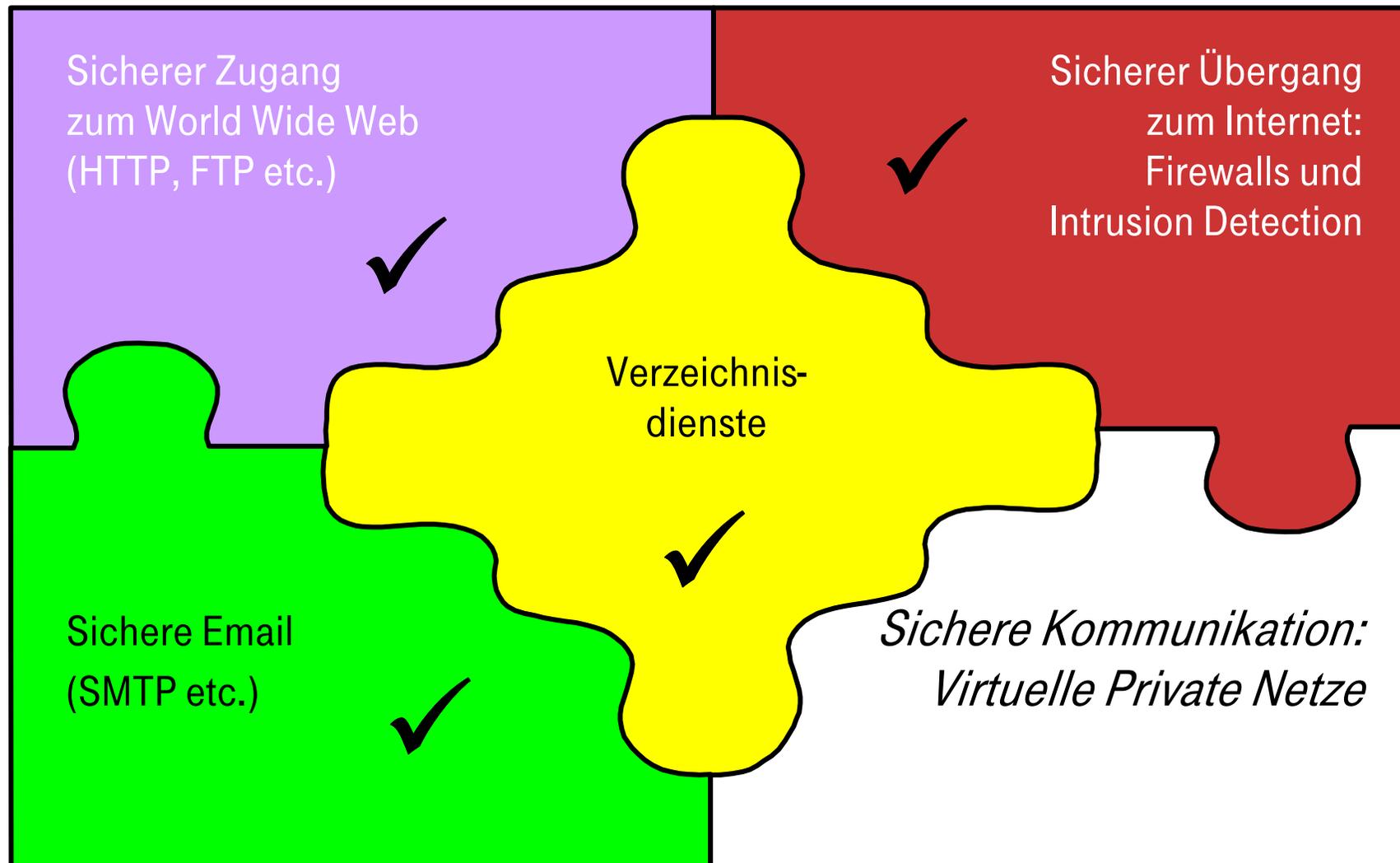
# Design und Realisierung von E-Business- und Internet-Anwendungen

## „Virtuelle Private Netze“ Teil 1

Dr. Michael Nerb et al.,  
Prof. Dr. Heinz-Gerd Hegering  
SoSe 2006

# Virtuelle Private Netze

## Einordnung in den Teil „Grundlagen“



# Virtuelle Private Netze

## Inhalte dieses Teils (verteilt auf zwei Termine)

- Virtuelle Private Netze
  - Begriffsdefinition und Charakteristika von VPN's
  - Beispiel eines VPN's
  - Anforderungen und Klassifikation von VPN's
- Technologien für Internet-basierte VPN's
  - Layer-2 Technologien
  - Layer-3 Technologien
  - Layer-4-7 Technologien
- VPN's in Weitverkehrsnetzen
  - Cell, Frame und Label Switching
  - MPLS basierende VPN's
  - QoS in MPLS-Netzen

# Virtuelle Private Netze

## Charakteristika

### ■ Virtual:

- Eine „logische“ Struktur
- Statisch oder dynamisch
- Unterschiedliche Technologien und Techniken zur Virtualisierung

### ■ Private:

- Beschränkter Zugang und Zugriff, „Closed User Groups“
- Mandantenfähigkeit
- Sicherstellung von Authentizität, Integrität, Vertraulichkeit

### ■ Network:

- Strukturen auf Basis einer „geschichten“ Infrastruktur, z.B.:
  - (In zunehmendem Maße) über das „Internet“
  - Aber auch Datennetze (z.B. Frame Relay, ATM, MPLS)
- Tunneling oder Tagging
- Transparent oder „Nicht-Transparent“ für Benutzer

# Virtuelle Private Netze

## Kundenanforderungen

- **Wirtschaftlichkeit:**
  - Kostengünstige Lösungen
  - Hohe Flächenabdeckung, Einbettung von mobilen Benutzern
- **Sicherheit und Qualität:**
  - vergleichbar einem privaten Netz (z.B. auf Basis „leased lines“)
  - Flexible, individuelle Quality of Service (QoS), Bandbreiten-Management
- **Interoperabilität und Integration in Geschäftsprozesse:**
  - Gesicherte Übergänge zu Internet / Intranet / Extranet
  - Zugriff auf Unternehmensdaten und –anwendungen
  - Verwendung vorhandener Adressen und Adressierungsschemata
  - Transparenz (bzw. einfache Anwendung) für Benutzer

## Beispiel

# Supply Chain Management bei Discountern

- Anbindung **aller Filialen** an eine Zentrale:
  - Sämtliche verkauften Waren werden an die Zentrale übermittelt
  - Zentrale kennt Lagerbestände der Filialen
  - Zentrale bestellt für alle Filialen Produkte bei Lieferanten gesteuert u.a. von Verbrauch, Jahreszeit, Wetter, Events (z.B. WM)
- Anbindung **aller Lieferanten** an die Zentrale:
  - Nehmen Bestellungen entgegen und verpacken/labeln diese
  - Transportieren die Ladungen zeitgenau zum Verteilzentrum
  - Umsortierung (anhand Barcode/RFID) und Weitertransport zu den Filialen
- Anbindung **der Fahrzeuge**:
  - Ortung der Lieferwagen, Optimierung der Routen/Leerfahrten
  - Auftragslisten für Gabelstapler, Verteilbändersteuerung...

# Klassifikation

## VPN's nach Organisation und Nutzungsformen

- Intranet VPN:
  - Internes Netz einer Organisation/Firma
  - Verbindet z.B. Zentrale, Niederlassungen, Außenstellen, etc.
  - Intranet ist über Firewalls usw. vom Internet abgeschottet
- Extranet VPN:
  - Kopplung von Firmen (z.B. B2B)
  - Bindet Zulieferer, Partner o.ä. an das Intranet einer Firma
  - Beispiele: Supply Chain Management, Online-Ordering o.ä.
- Remote Access VPN:
  - bindet mobile Nutzer („Road warriors“), Heimarbeitsplätze etc. an das Intranet an (z.B. über das Internet oder Dial-In)
  - Beispiele: Teleworker, Field Service o.ä.

# Klassifikation

## VPN's nach Kommunikations-Endpunkten

- „Site-to-Site“:
  - Quasi-Standverbindung zwischen den Standorten
  - Transparent für die Benutzer/Applikationen
  - Typischerweise bei Intranet/Extranet
- „End-to-Site“:
  - Erfordert VPN-Software auf dem Client, ist aber für die Benutzer/Applikationen sonst transparent
  - Nur mit Virens scanning und Personal Firewall zu empfehlen
  - Typischerweise bei Remote Access VPN
- „End-to-End“:
  - Höchste Sicherheit, da Daten durchgehend verschlüsselt
  - Kein „typisches“ Einsatzszenario, aber gut geeignet für Web-basierte Anwendungen

# Klassifikation VPN's nach OSI-Schichtenmodell

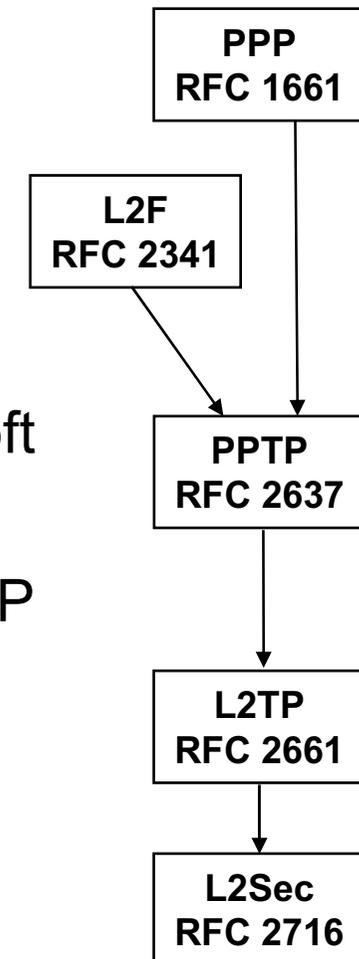
- Layer-2 Technologien:
  - L2F, PPTP, L2TP, L2Sec
- Layer-3 Technologien:
  - IPSec
- Layer-4-7 Technologien:
  - SSH, SSL/TLS, SSL-VPN's
- VPN-Technologien in WAN's
  - Virtuelle Verbindungen in Frame Relay Netzen
  - Virtuelle Pfade und Kanäle in zellbasierten Netzen (z.B. ATM)
  - Multiprotokoll Label Switching (MPLS)

→ Vertiefung der VPN's erfolgt anhand dieser Klassifikation

# Layer-2 Technologien

## Einordnung und Überblick

- PPP: Point to Point Protocol
  - Authentifizierung (PAP, CHAP), Kompression
- L2F: Layer 2 Forwarding, Cisco Systems
  - Keine Authentifizierung, keine Verschlüsselung
- PPTP: Point to Point Tunneling Protocol, v.a. Microsoft
  - Authentifizierung z.B. durch MS-CHAPv2
  - Verschlüsselung über MPPE (RFC2118) oder EAP
- L2TP: Layer 2 Tunneling Protocol
  - Keine Verschlüsselung -> z.B. IPSec erforderlich
- L2Sec: Layer 2 Security („SSL over L2TP“)
  - Authentifizierung und Verschlüsselung auf Basis von SSLv3 Mechanismen



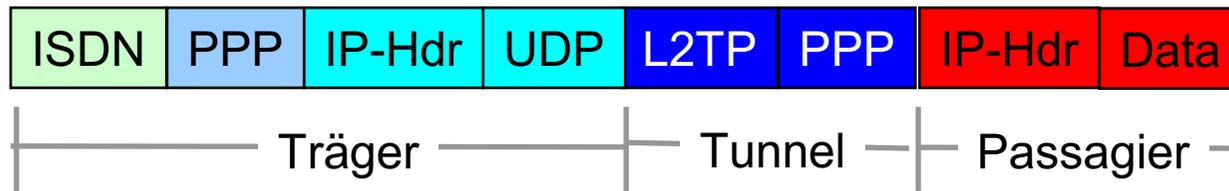
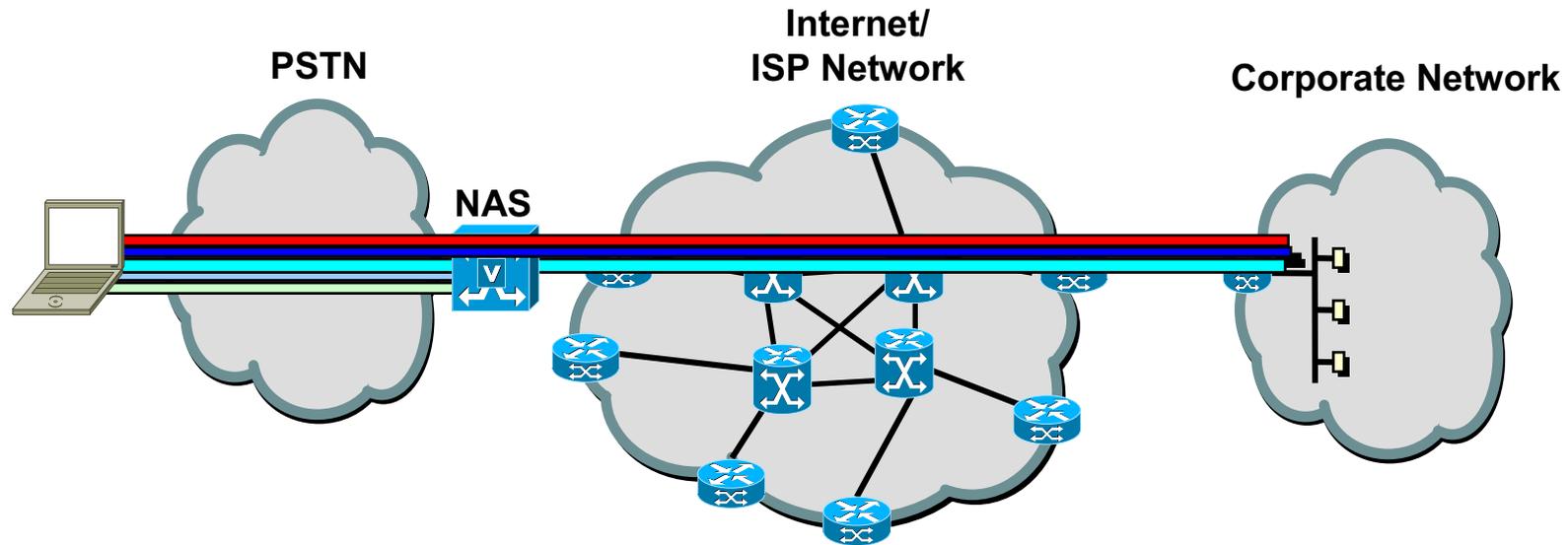
# Tunneling

## Beschreibung des Mechanismus

- Realisierung einer Schicht (N+1) Kommunikationsbeziehung über ein Schicht (N) Trägernetz
- Tunnel damit oft vergleichbar (mit Nutzung) einer (virtuellen) Verbindung
- Bestandteile des Tunnelmechanismus:
  - Passagier-Protokoll (passenger protocol)
  - Tunnel-Protokoll (encapsulating protocol)
  - Träger-Protokoll (carrier protocol)
- Kann dazu führen, dass der OSI-Stack etwas „durcheinander gewürfelt“ wird, z.B.:
  - Ein PPTP Protokoll (Schicht 2) wird über IP (Schicht 3) geführt
  - IP wird in IP eingebettet

# Tunneling für Layer-2 Technologien

## Beispiel: End-to-Site



# Layer-2 Mechanismen

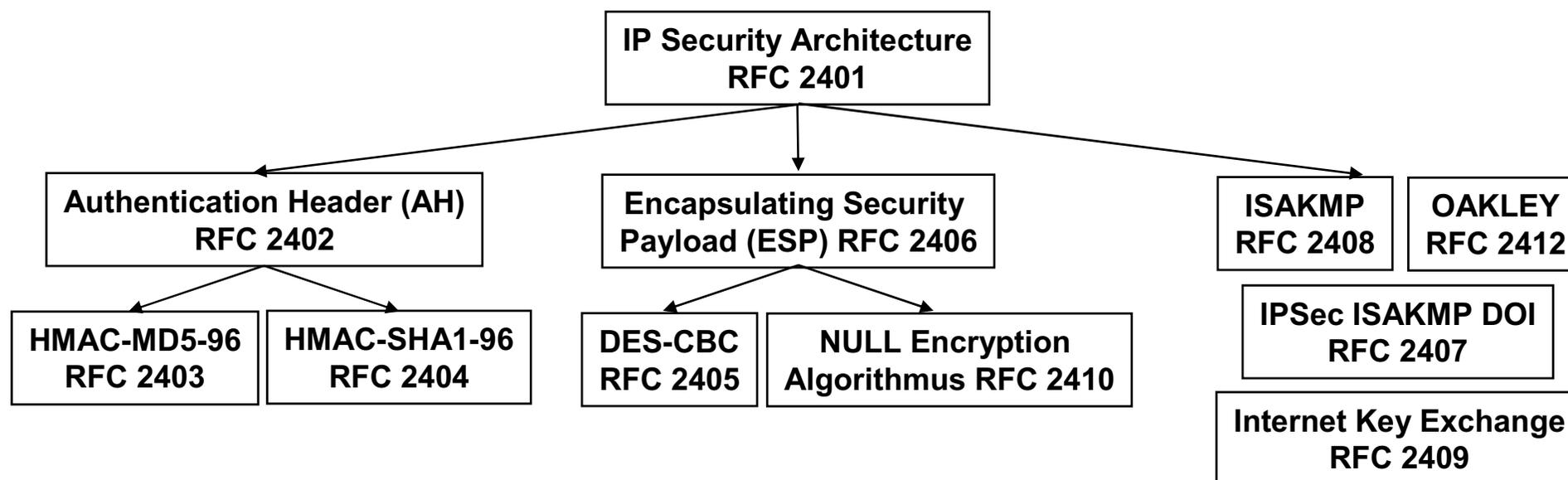
## Zusammenfassung

- **Wirtschaftlichkeit:**
  - Trägerprotokoll ist IP
  - Kostengünstige Realisierungsmöglichkeiten für kleine Umgebungen
- **Sicherheit:**
  - Schwache/keine Mechanismen zur Authentifizierung, Integrität und Vertraulichkeit
  - Keine (starke) Kryptografie zur Verschlüsselung (Ausnahme: L2Sec)
- **Interoperabilität und Integration in Geschäftsprozesse:**
  - Unabhängigkeit vom Trägernetz durch Tunneling
  - Durch Trägerprotokoll IP hohe Interoperabilität und Integration
  - Hohe Verbreitung durch Microsoft PPTP
- **Aber auch:**
  - Quality of Service?
  - Mangelnde Sicherheit erfordert Einsatz anderer Mechanismen!

# Layer-3 Technologien

## IPSec – Einordnung und Überblick

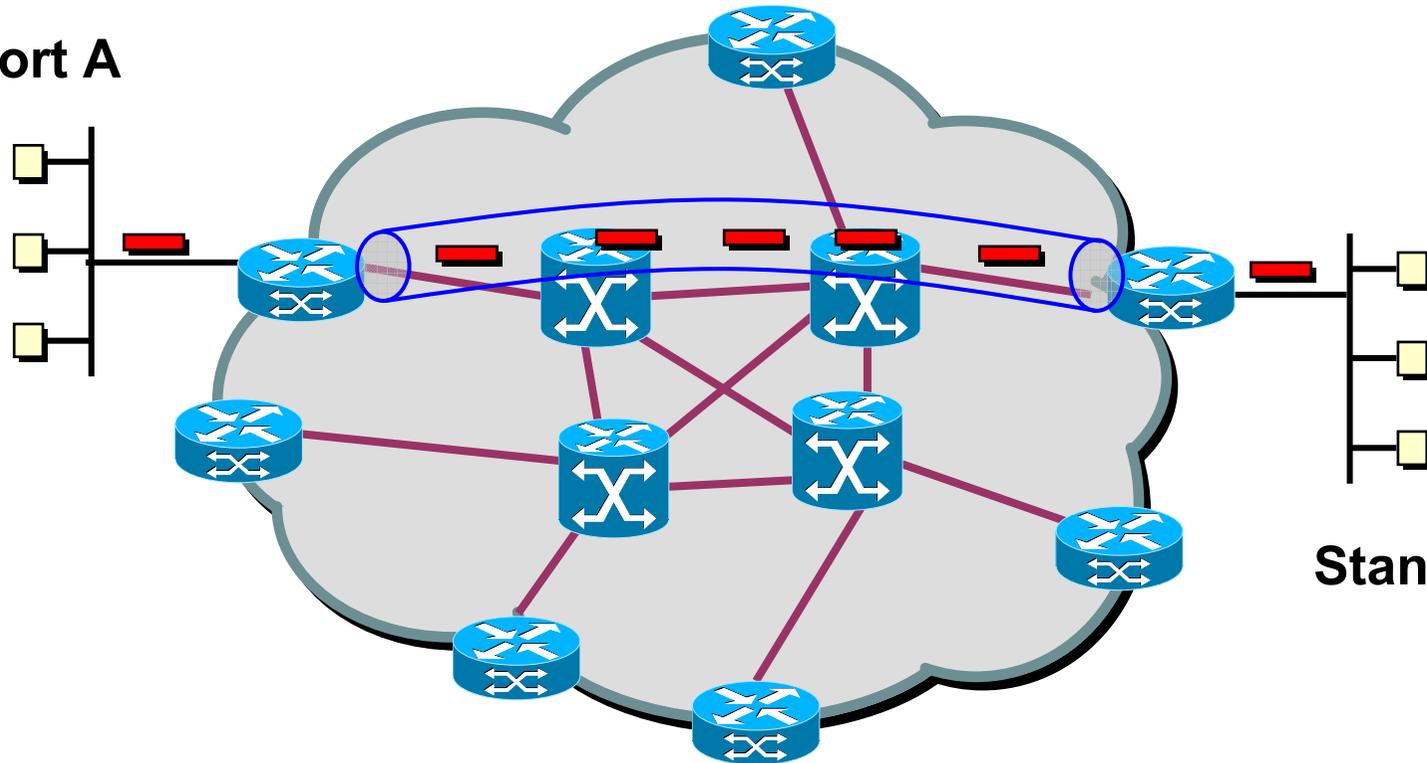
- IETF Working Group (WG) „IPSec“
- Framework für Sicherheitsfunktionen auf OSI-Layer 3
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Management von Sicherheitsassoziationen und Schlüsseln



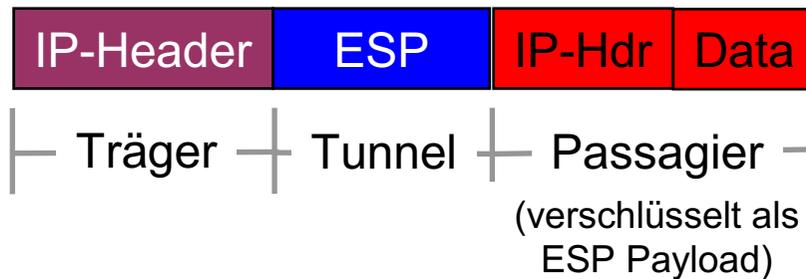
# Tunneling für Layer-3 Technologien

## Beispiel: Site-to-Site zwischen zwei Standorten

Standort A



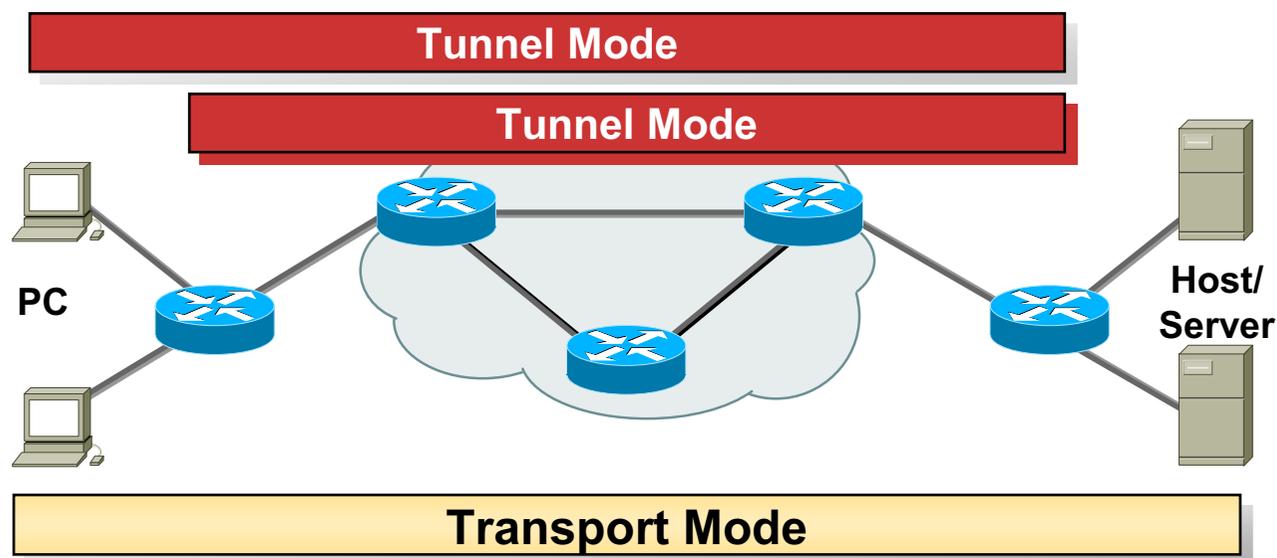
Standort B



# IPSec – Funktionen und Protokolle

## Transport- und Tunnel-Modus

- Tunnel-Modus:
  - Komplettes IP-Paket wird gekapselt (inkl. IP Header)
  - Anwendung: „Site-to-Site“ oder „End-to-Site“
- Transport-Modus:
  - Nur IP-Daten („Payload“) werden gekapselt
  - IP-Header mit IP-Adressen bleibt erhalten
  - Anwendung für „End-to-End“



# IPSec – Funktionen und Protokolle

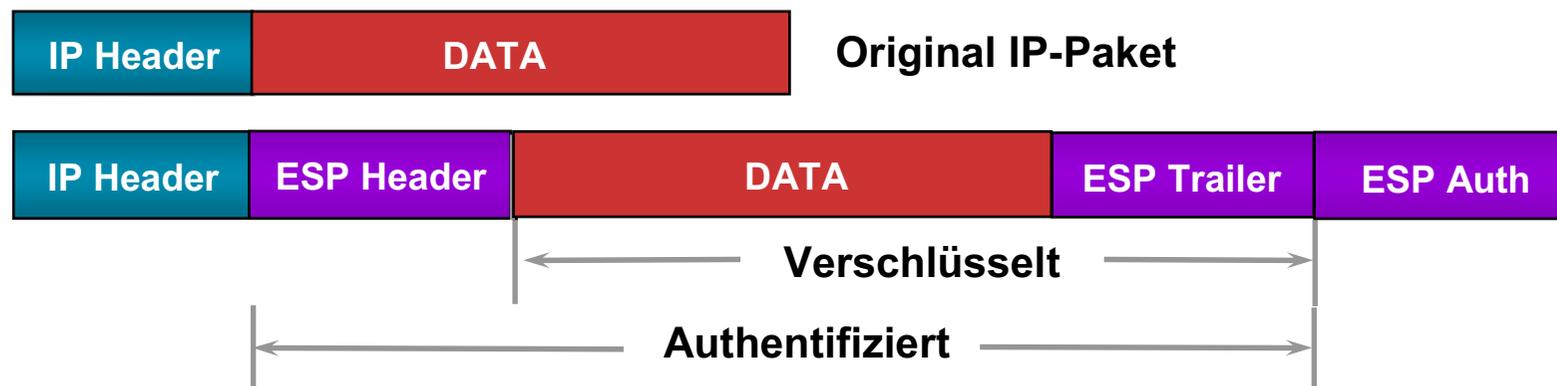
## AH und ESP

- Authentication Header (AH):
  - Protokoll zur Sicherstellung von Integrität und Authentizität
  - Kryptographische Prüfsumme (Hash, HMAC) über IP Paket (MD5, SHA1)
  
- Encapsulating Security Payload (ESP):
  - Protokoll zur Sicherstellung von Vertraulichkeit und Authentizität
  - Verschlüsselung des IP-Pakets oder Payload (DES, 3DES, Blowfish, RC4, AES...)
  
- AH und ESP können sowohl im Tunnel- als auch im Transport Modus verwendet werden
  - Vorsicht: Bei IPSec nutzen sowohl Tunnel- als Transport Mode den vorher vorgestellten Mechanismus des „Tunnelings“

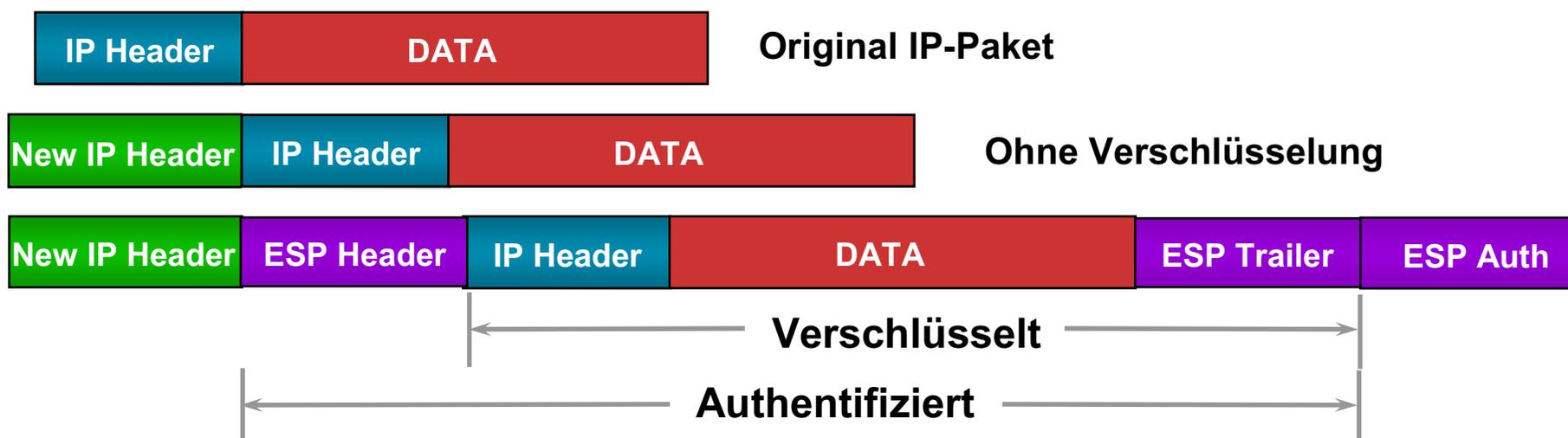
# Details: ESP im Transport und Tunnel Modus

## PDU Formate

### Transport Mode (z.B. im LAN):



### Tunnel Mode (z.B. Standortkopplung über das Internet):



# IPSec – Funktionen und Protokolle

## Management von Sicherheitsassoziationen (SA)

- ISAKMP (RFC 2408): Internet Security Association and Key Management Protocol
  - Prozeduren und Formate für Aufbau, Abbau, Verhandlung von SA's
  - Authentifizierung der Teilnehmer
  - abstrakte Protokollbasis
- IPSec DOI for ISAKMP (RFC 2407): „Domain Of Interpretation“
  - konkrete Spezifikation für ISAKMP
- Oakley Key Determination Protocol (RFC 2412)
  - Schlüsselaustausch auf Basis von Diffie-Hellman Key Exchange
  - Etablieren eines gemeinsamen, geheimen Schlüssels über einen unsicheren Kanal
- Internet Key Exchange (RFC 2409):
  - Konkrete Implementierung von ISAKMP und Oakley

# IPSec – Funktionen und Protokolle

## IKE Phasen und Modi

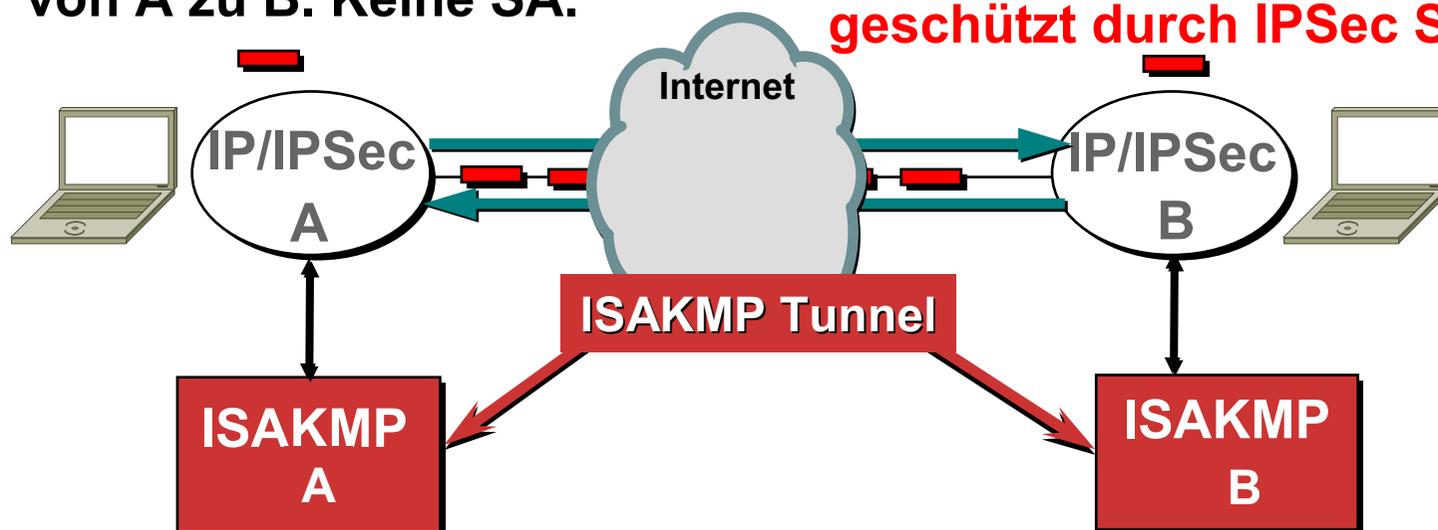
- IKE Phase 1 (Aufbau des ISAKMP Tunnels):
  - „Main Mode“:
    - ISAKMP Proposal, NAT-Traversal
    - Diffie-Hellman
    - VPN ID, Zertifikate, Authentifizierung (Zertifikate oder PSK)
    - IPSec Proposal, SPI und ESP
  - „Aggressive Mode“ für Pre-Shared-Keys (PSK):
    - Kommt mit weniger Nachrichten aus
    - Nicht empfehlenswert, da PSK im Klartext übertragen werden
- IKE Phase 2 (Aufbau der IPSec Security Associations):
  - „Quick Mode“
    - Aufbau zweier unidirektionaler IPSec SA's (über ISAKMP-Tunnel)
    - Daten (Payload) werden über diese IPSec SA's übertragen
    - „Perfect Forward Secrecy“ (PFS): Neue Schlüssel für Phase 2

# ISAKMP und Oakley

## Aufbau der SA und Schlüsselaustausch (vereinfacht)

1. Ausgehendes IP Paket von A zu B. Keine SA.

5. IP Paket von A zu B geschützt durch IPsec SA's



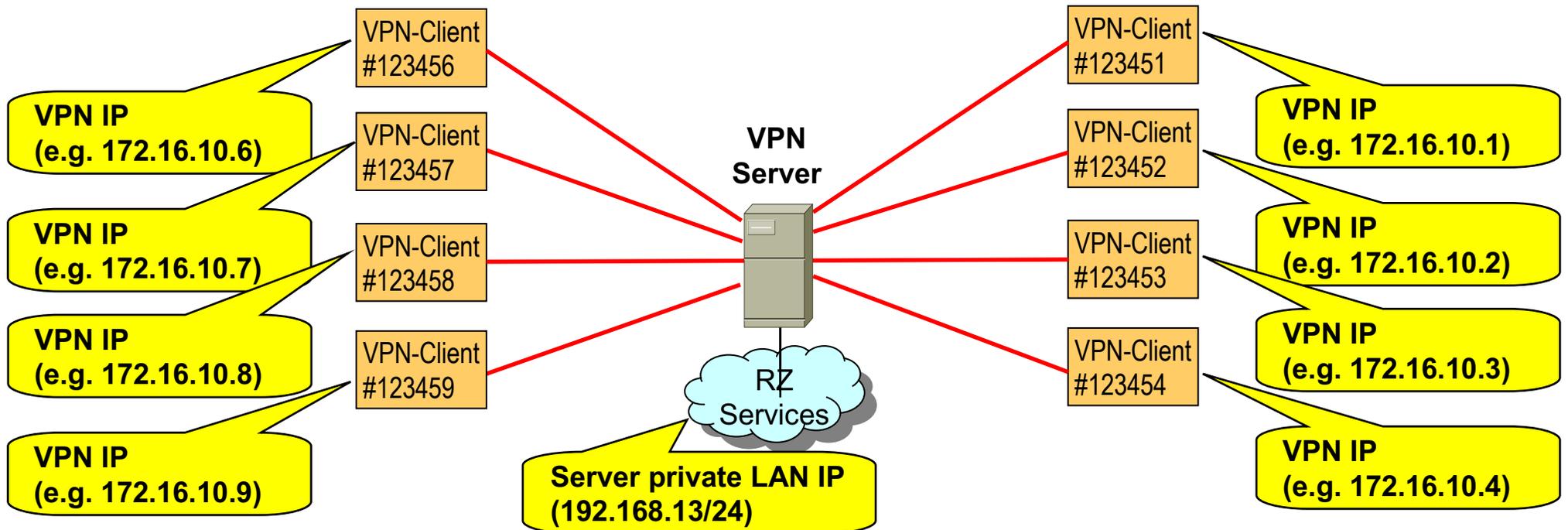
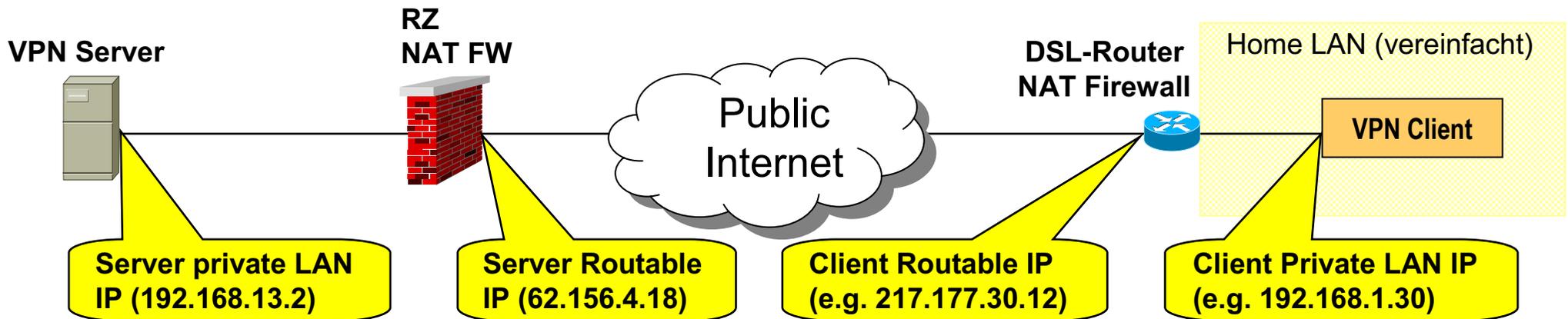
2. A's ISAKMP beginnt Verhandlung mit B.

4. Nun werden zwei (unidirektionale) IPsec SA's aufgebaut.

3. Verschlüsselung erfolgt anhand von „Pre-Shared“ Keys oder X.509 Zertifikaten (Oakley generiert dabei Schlüssel)

# Praktische Umsetzung - Beispiel

## End-to-Site IPSec VPN (vereinfacht)



# Praktische Umsetzung - Beispiel „NAT-Traversal“

- Problem: VPN-Client und/oder VPN Server werden geNATted
- Beispiel „NATting beim Client“:
  - NAT FW betreibt „Masquerading“ (Spezialfall von S-NAT)
  - Mehrere Clients sind hinter einer IP Adresse verborgen
  - NAT FW identifiziert Client anhand der IP Adresse und Port#
- Aber: IPSec Paket hat kein sichtbares TCP/UDP Header (verschlüsselt!)



- Lösung: NAT-Traversal (RFC 3947)
  - Während ISAKMP (IKE Phase 1) wird festgestellt, ob und wer geNATted ist
  - Bei Bedarf wird der IPSec Traffic in UDP enkapsuliert (Phase 2)



- Somit kann NAT FW diese Pakete wieder zum korrekten Client zuordnen

# IPSec

## Zusammenfassung

- **Wirtschaftlichkeit:**
  - Trägerprotokoll ist IP
  - Kostengünstige Realisierungsmöglichkeiten
- **Sicherheit:**
  - Mechanismen zur Authentifizierung, Integrität und Vertraulichkeit
  - Einsatz starker Kryptografie zur Verschlüsselung
- **Interoperabilität und Integration in Geschäftsprozesse:**
  - Unabhängigkeit vom Trägernetz durch Tunneling
  - Durch Trägerprotokoll IP hohe Interoperabilität und Integration
- **Aber auch:**
  - Quality of Service?
  - Komplexität der IPSec Standards und Implementierungen?
  - Interoperabilität von verschiedenen IPSec Implementierungen?
  - Aufwände durch Aufbau von Certification Authorities (CA) usw.

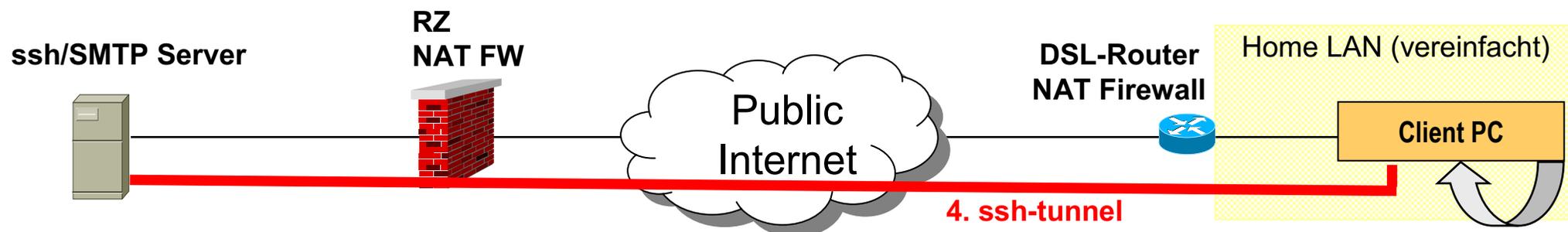
# Layer-4-7 Technologien

## Einordnung und Überblick

- SSH (Secure Shell):
  - Tatu Ylönen (Helsinki University of Technology)
  - Ursprüngliches Ziel: Ersetzen der „r-tools“ (rlogin, rsh, rcp usw.)
  - Heute: Tunneln von Anwendungen („weit verbreitet“: X11 Forwarding)
- SSL (Secure Socket Layer) Version 3:
  - Netscape Communications
  - „Sicherheitsschicht“ zw. Anwendungs- und Transportschicht,
  - geeignet für TCP-basierten Anwendungen (z.B. POP3, IMAP, HTTP)
  - OpenSSL als Open-Source Implementierung inkl. PKI und Zertifikatsmanagement
- TLS (Transport Layer Security)
  - IETF WG „Transport Layer Security“, TLS Version 1 (RFC 2246)
  - Konzeptionell und inhaltlich nahezu identisch zu SSLv3
- „SSL-VPN’s“: Produkte auf Basis von SSL/TLS

# Praktische Umsetzung - Beispiel

## „SMTP over ssh“ - Prinzipdarstellung



1. SSH daemon ist aus dem Internet erreichbar
2. Beim Booten des Client PC:  
„ssh -f -N -L 25:ssh-server-ip:25  
ssh-server-ip“
3. SSH daemon erlaubt login, wenn  
authorized\_key Eintrag vorhanden
4. **ssh-tunnel etabliert (rote Linie)**
5. Client-PC sendet E-Mail per SMTP:  
„telnet localhost 25“
6. Mail wird verschlüsselt durch den  
ssh-tunnel zum SMTP Server  
gesendet
7. SSH daemon empfängt und entschlüsselt die Daten;  
SMTP-Server verarbeitet die empfangene E-Mail

# Praktische Umsetzung – Beispiel

## OpenVPN

- Nutzt die SSL/TLS Bibliotheken und Funktionen
- Läuft auf den gängigen Plattformen (Linux, Windows, Mac)
- Volle Mächtigkeit bei:
  - Authentifizierung (PSK, Zertifikate)
  - Verschlüsselung (unterstützte Algorithmen)
- Lässt sich gut in Firewall/NAT-Umgebungen integrieren:
  - Benötigt nur eine TCP oder UDP „Verbindung“
  - Kann auch über HTTP getunnelt werden
- Bietet fast gleichen Funktionsumfang wie IPSec, u.a.
  - Routing von ganzen Netzen
  - DHCP, DNS und WINS Server
- Relativ einfach zu konfigurieren (GUI)
  - Interessante Alternative zu IPSec !

# Layer-4-7 Technologien

## Zusammenfassung

- Benutzerfreundlich und „Easy-to-use“:
  - Je nach Anwendung keine oder wenig zusätzliche Software erforderlich
  - Typischerweise überschaubarer Konfigurationsaufwand an den Clients
  - Viele Anwendungen sind inzwischen „Web-basiert“, d.h. Zugriff kann über HTTP erfolgen
  - Zertifikate usw. können auch anderweitig verwendet werden (z.B. für „2-Factor Authentication“ auf Client-PC, „Single-Sign-On“ o.ä.)
  - Ende-zu-Ende Authentifizierung und Verschlüsselung
  - Komplexität von IPSec und Layer-2 Technologien entfällt
- Aber auch:
  - Ausgabe/Verwaltung von Schlüsseln, Zertifikaten, Revocation Lists usw.
  - Initiator typischerweise der Client (nicht der Server), oft nur für TCP-basierte Anwendungen
  - Weiterhin Notwendigkeit für Schutzmaßnahmen
    - Auf jedem PC (Personal Firewalls, Virens scanning usw.)
    - An der Grenze zum Internet (Firewalls, IDS, Virens scanning, usw.)

# Literatur

## Links zum Thema

- RFC-Archiv im Internet, z.B. unter: <http://www.rfc-archive.org/>
- F. L. Bauer; „**Decrypted Secrets** - Methods and Maxims of Cryptology“, 3. Auflage 2002, Springer Verlag
- Helmar Gerloni, Barbara Oberhaitzinger, Helmut Reiser, Jürgen Plate: Praxisbuch „**Sicherheit für Linux-Server und Netze**“, Hanser Fachbuchverlag 2004
- Uyles Black: „**MPLS and Label Switching Networks**“, Prentice Hall, 2. Auflage, 2002
- Ralf Spenneberg: „VPN mit Linux“, Addison-Wesley, 2004
  
- C't Magazin 17/01 (Seite 164ff) und 18/01 (Seite 182ff)
- C't Magazin 07/06 (Seite 104ff)
- I'X Magazin 07/03 (Seite 84ff) und 10/02 (Seite 92ff)
- Bruce Schneier: <http://www.counterpane.com>, <http://www.schneier.com>
- SSH: <http://www.ssh.org>
- OpenSSL: <http://www.openssl.org>

# Das wärs für heute...

- Fragen / Diskussion
- Verbesserungsvorschläge
- Die Folien von heute sind bereits auf die Web-Seite der Vorlesung
- Übernächste Woche (01. Juni 2006): VPN's Teil 2
- Einen schönen Abend !!!