

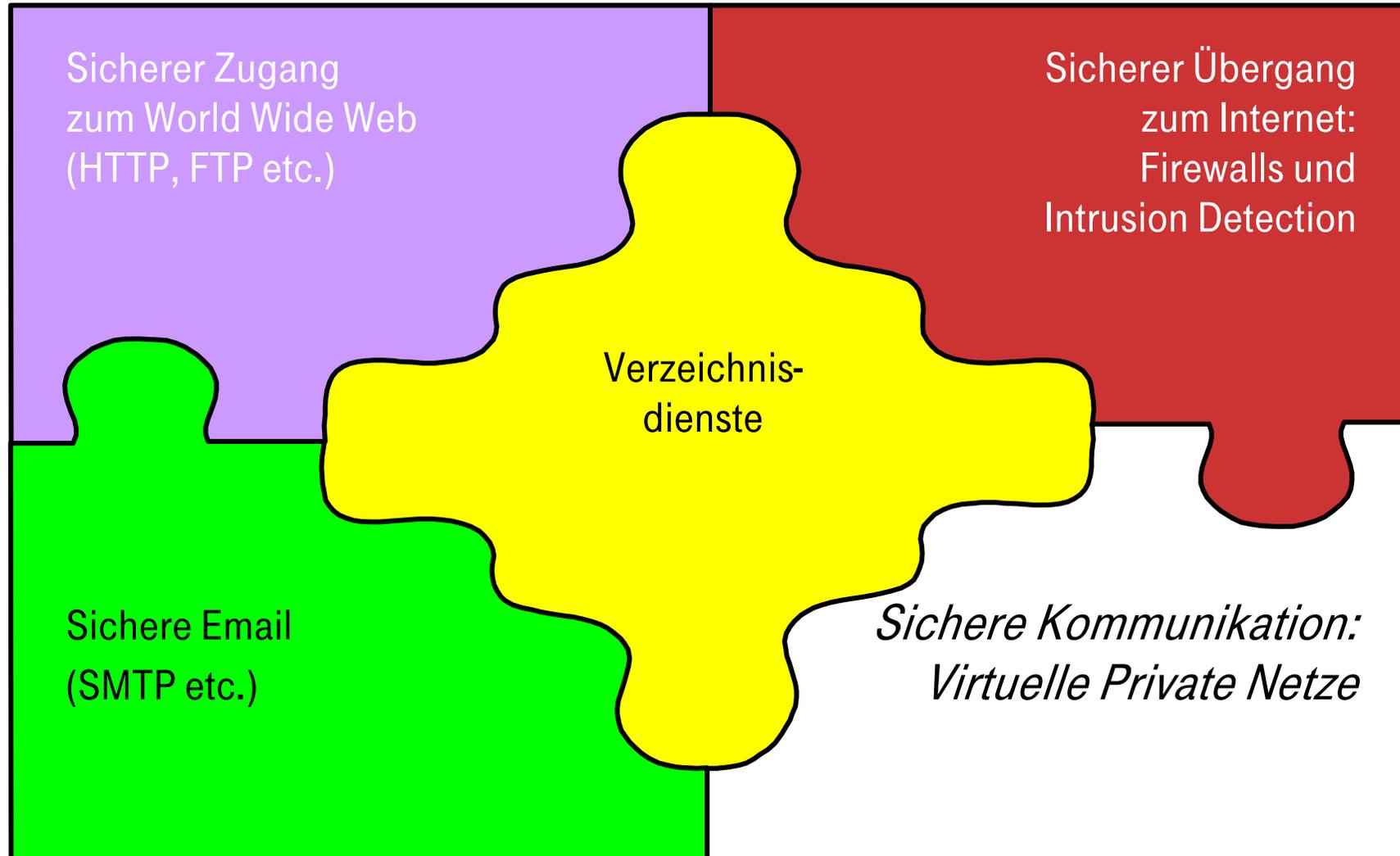
# Integrierte IT-Service-Management- Lösungen anhand von Fallstudien

## „Virtuelle Private Netze“ Teil 1

Dr. Michael Nerb et al.,  
Prof. Dr. Heinz-Gerd Hegering  
SoSe 2008

# Virtuelle Private Netze

## Einordnung in den Teil „Grundlagen“



# Virtuelle Private Netze

## Inhalte dieses Teils (verteilt auf zwei Termine)

### n Virtuelle Private Netze

- Begriffsdefinition und Charakteristika von VPN's
- Beispiel eines VPN's
- Anforderungen und Klassifikation von VPN's

### n Technologien für Internet-basierte VPN's

- Layer-2 Technologien
- Layer-3 Technologien
- Layer-4-7 Technologien

### n VPN's in Weitverkehrsnetzen

- Cell, Frame und Label Switching
- MPLS basierende VPN's
- QoS in MPLS-Netzen

# Virtuelle Private Netze

## Charakteristika

### n Virtual:

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

### n Private:

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

### n 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

### n Wirtschaftlichkeit:

- Kostengünstige Lösungen
- Hohe Flächenabdeckung, Einbettung von mobilen Benutzern

### n Sicherheit und Qualität:

- vergleichbar einem privaten Netz (z.B. auf Basis „leased lines“)
- Flexible, individuelle Quality of Service (QoS), Bandbreiten-Management

### n 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

- n 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)
- n 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
- n Anbindung **der Fahrzeuge**:
  - Ortung der Lieferwagen, Optimierung der Routen/Leerfahrten
  - Auftragslisten für Gabelstapler, Verteilbändersteuerung...

# Klassifikation VPN's nach Organisation und Nutzungsformen

## n Intranet VPN:

- Internes Netz einer Organisation/Firma
- Verbindet z.B. Zentrale, Niederlassungen, Außenstellen, etc.
- Intranet ist über Firewalls usw. vom Internet abgeschottet

## n 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.

## n 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

- n „Site-to-Site“:
  - Quasi-Standverbindung zwischen den Standorten
  - Transparent für die Benutzer/Applikationen
  - Typischerweise bei Intranet/Extranet
- n „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
- n „End-to-End“:
  - Höchste Sicherheit, da Daten durchgehend verschlüsselt
  - Kein „typisches“ Einsatzszenario, aber gut geeignet für Web-basierte Anwendungen

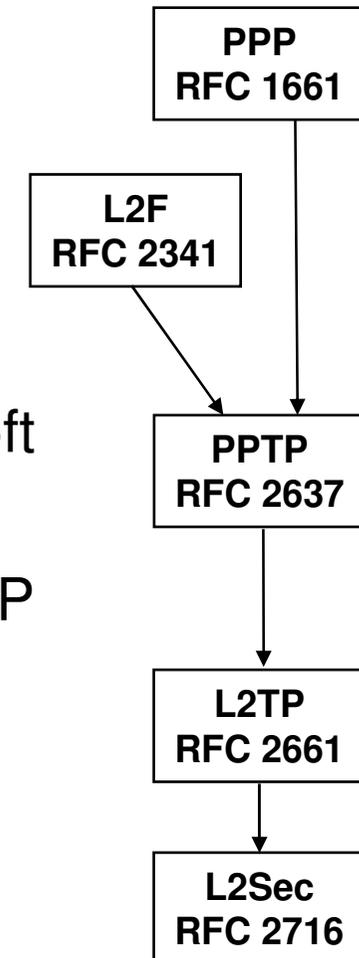
# Klassifikation VPN's nach OSI-Schichtenmodell

- n Layer-2 Technologien:
    - L2F, PPTP, L2TP, L2Sec
  - n Layer-3 Technologien:
    - IPSec
  - n Layer-4-7 Technologien:
    - SSH, SSL/TLS, SSL-VPN's
  - n 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

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



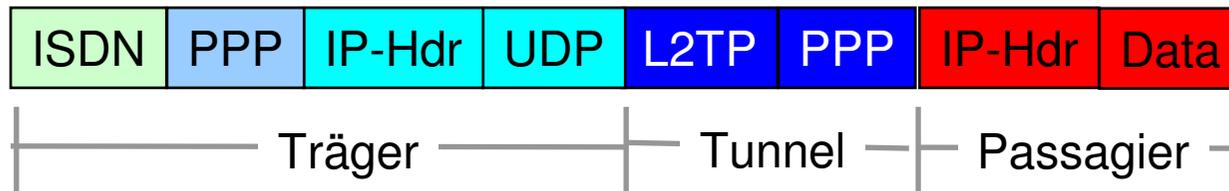
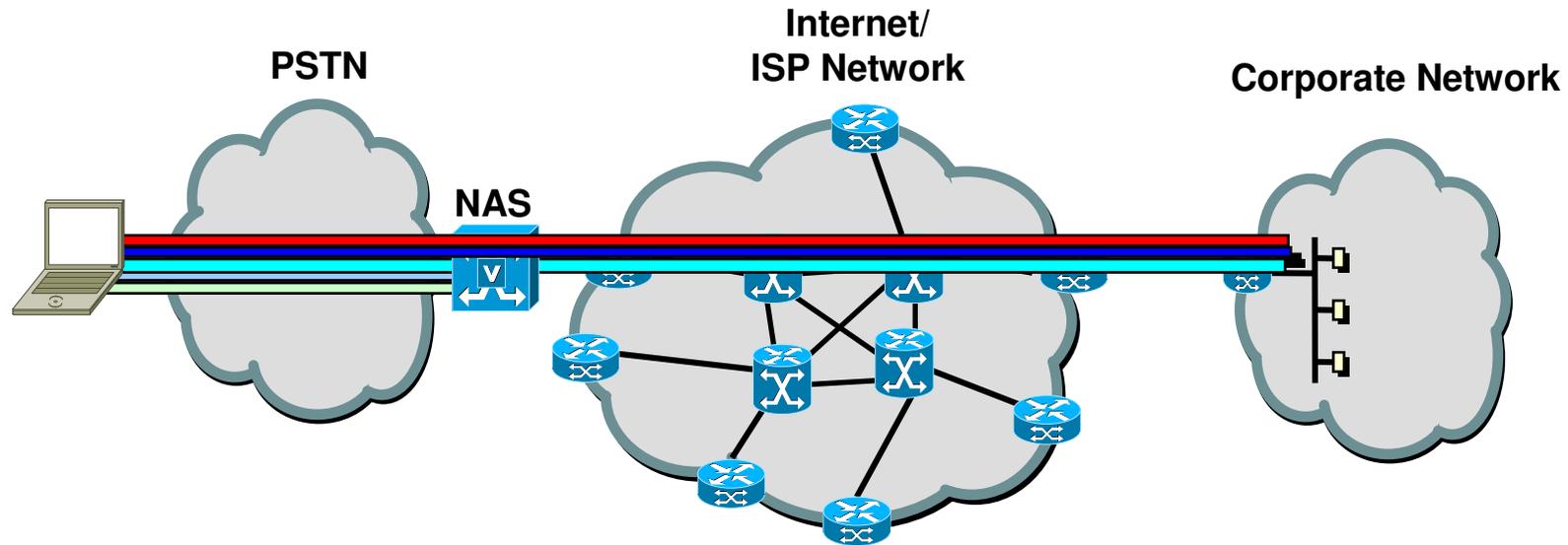
# Tunneling

## Beschreibung des Mechanismus

- n Realisierung einer Schicht (N+1) Kommunikationsbeziehung über ein Schicht (N) Trägernetz
- n Tunnel damit oft vergleichbar (mit Nutzung) einer (virtuellen) Verbindung
- n Bestandteile des Tunnelmechanismus:
  - Passagier-Protokoll (passenger protocol)
  - Tunnel-Protokoll (encapsulating protocol)
  - Träger-Protokoll (carrier protocol)
- n 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

### n Wirtschaftlichkeit:

- Trägerprotokoll ist IP
- Kostengünstige Realisierungsmöglichkeiten für kleine Umgebungen

### n Sicherheit:

- Schwache/keine Mechanismen zur Authentifizierung, Integrität und Vertraulichkeit
- Keine (starke) Kryptografie zur Verschlüsselung (Ausnahme: L2Sec)

### n Interoperabilität und Integration in Geschäftsprozesse:

- Unabhängigkeit vom Trägernetz durch Tunneling
- Durch Trägerprotokoll IP hohe Interoperabilität und Integration
- Hohe Verbreitung durch Microsoft PPTP

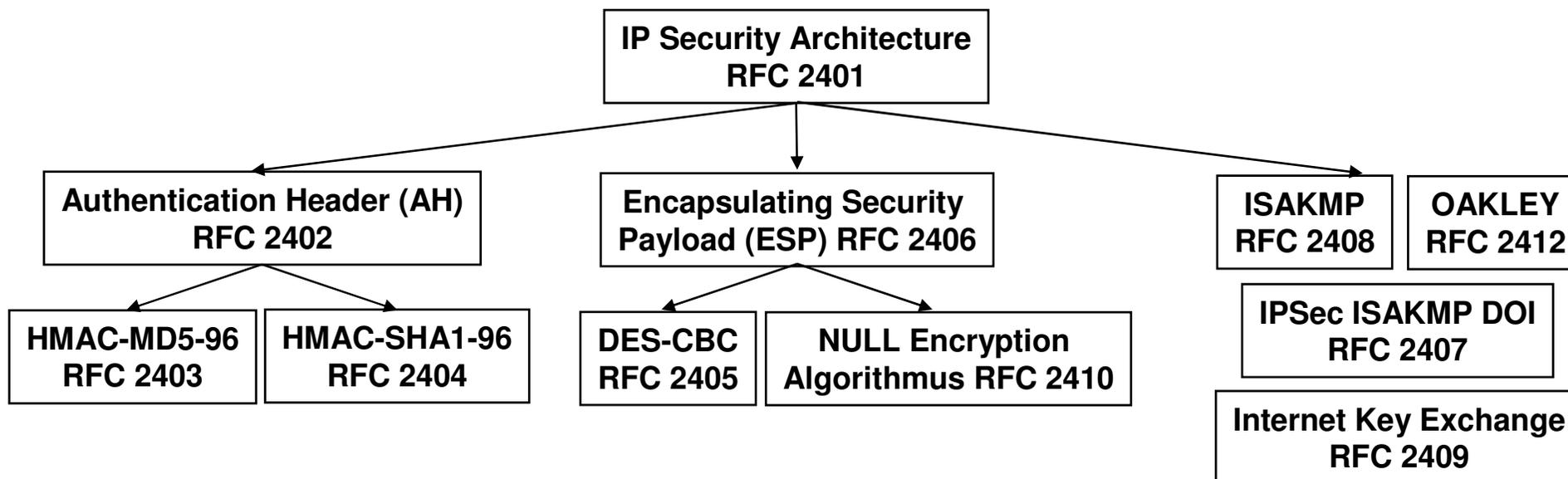
### n Aber auch:

- Quality of Service?
- Mangelnde Sicherheit erfordert Einsatz anderer Mechanismen!

# Layer-3 Technologien

## IPSec – Einordnung und Überblick

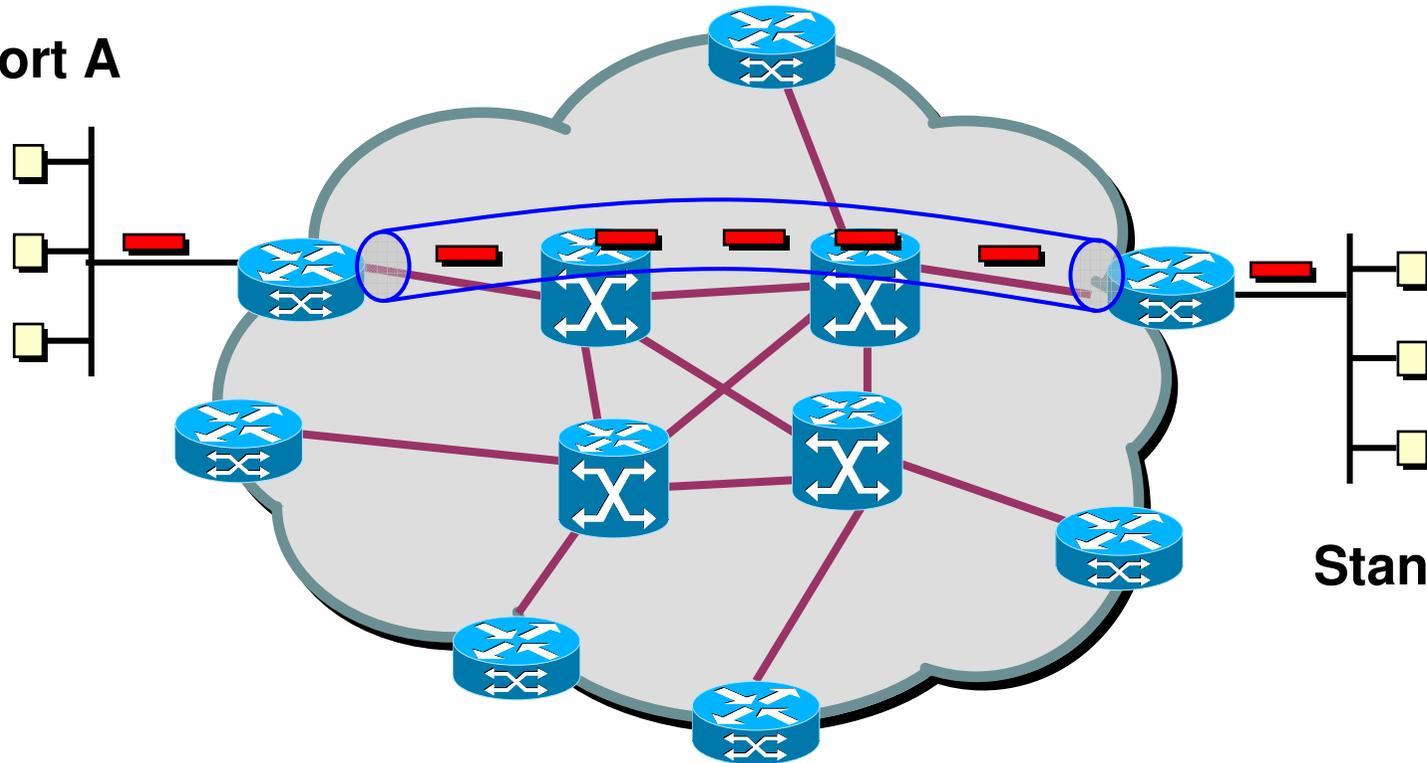
- n IETF Working Group (WG) „IPSec“
- n Framework für Sicherheitsfunktionen auf OSI-Layer 3
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Management von Sicherheitsassoziationen und Schlüsseln



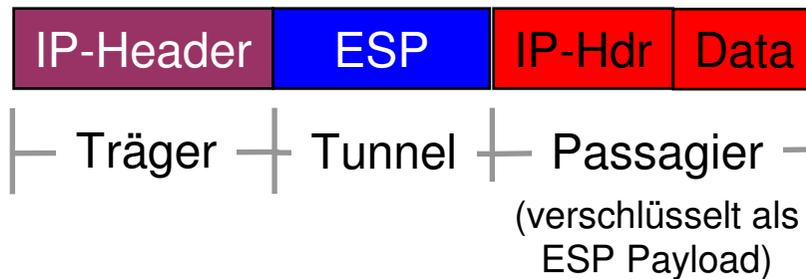
# Tunneling für Layer-3 Technologien

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

Standort A



Standort B



# IPSec – Funktionen und Protokolle

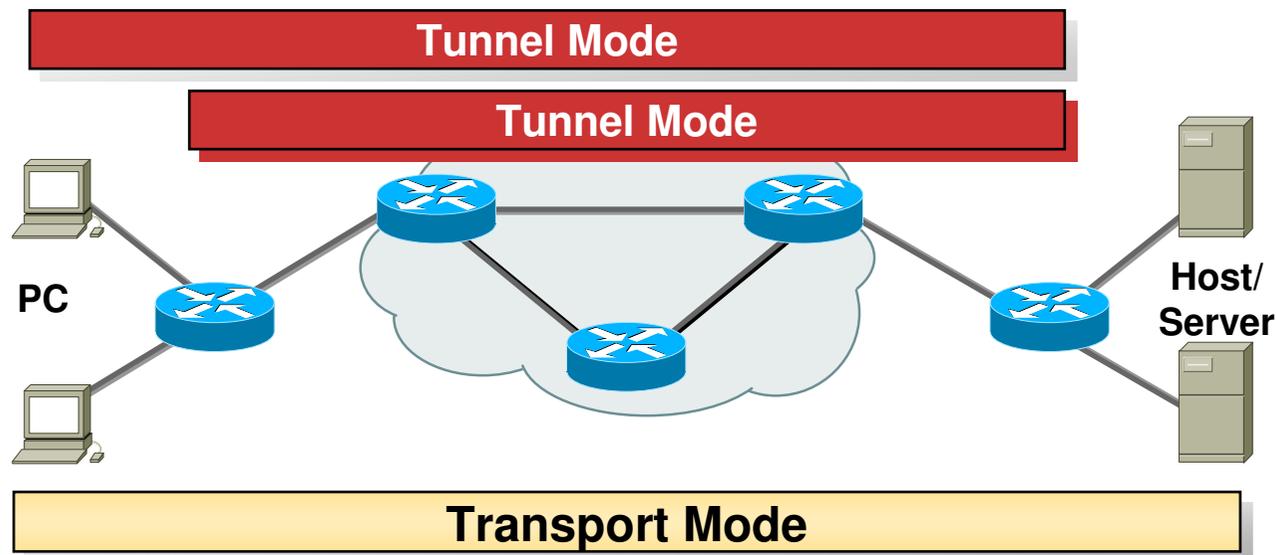
## Transport- und Tunnel-Modus

### n Tunnel-Modus:

- Komplettes IP-Paket wird gekapselt (inkl. IP Header)
- Anwendung: „Site-to-Site“ oder „End-to-Site“

### n Transport-Modus:

- Nur IP-Daten („Payload“) werden gekapselt
- IP-Header mit IP-Adressen bleibt erhalten
- Anwendung für „End-to-End“



# IPSec – Funktionen und Protokolle

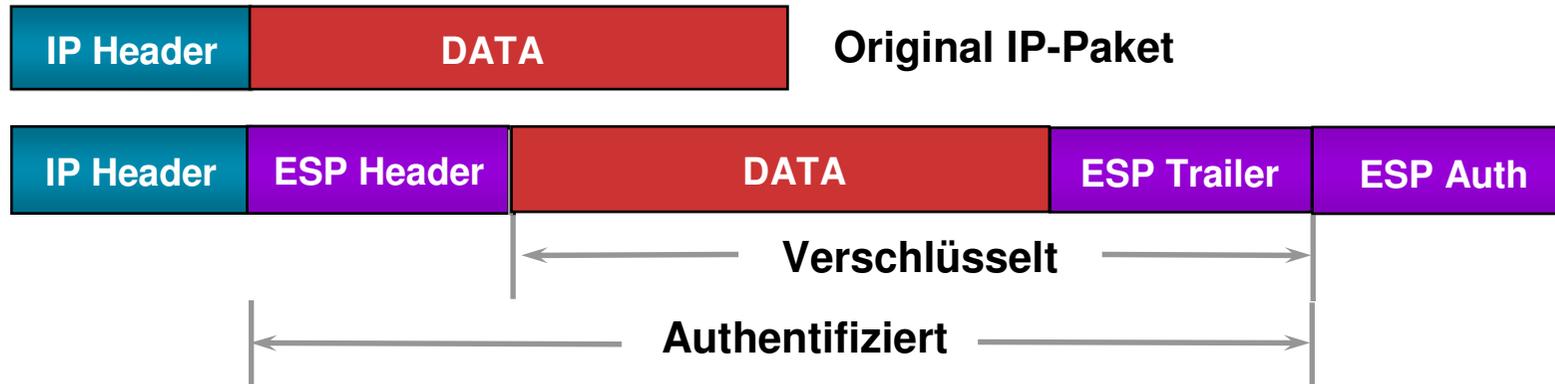
## AH und ESP

- n Authentication Header (AH):
  - Protokoll zur Sicherstellung von Integrität und Authentizität
  - Kryptographische Prüfsumme (Hash, HMAC) über IP Paket (MD5, SHA1)
  
- n Encapsulating Security Payload (ESP):
  - Protokoll zur Sicherstellung von Vertraulichkeit und Authentizität
  - Verschlüsselung des IP-Pakets oder Payload (DES, 3DES, Blowfish, RC4, AES...)
  
- n 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“

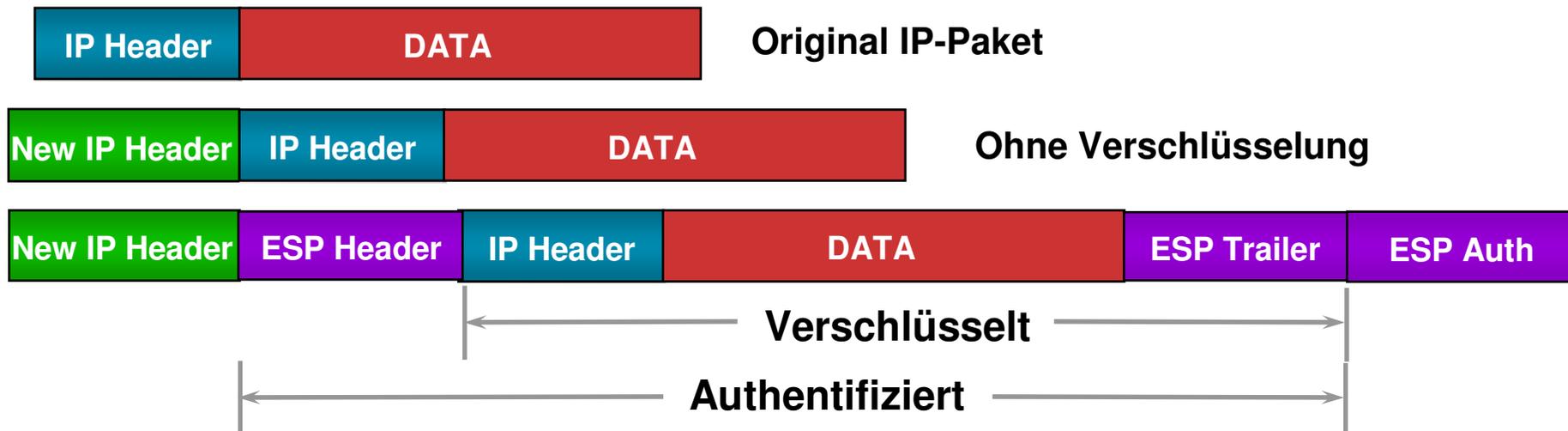
# Details: ESP im Transport und Tunnel Modus

## PDU Formate

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



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



# IPSec – Funktionen und Protokolle

## Management von Sicherheitsassoziationen (SA)

- n 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
- n IPSec DOI for ISAKMP (RFC 2407): „Domain Of Interpretation“
  - konkrete Spezifikation für ISAKMP
- n Oakley Key Determination Protocol (RFC 2412)
  - Schlüsselaustausch auf Basis von Diffie-Hellman Key Exchange
  - Etablieren eines gemeinsamen, geheimen Schlüssels über einen unsicheren Kanal
- n Internet Key Exchange (RFC 2409):
  - Konkrete Implementierung von ISAKMP und Oakley

# IPSec – Funktionen und Protokolle

## IKE Phasen und Modi

### n 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

### n IKE Phase 2 (Aufbau der IPSec Security Associations):

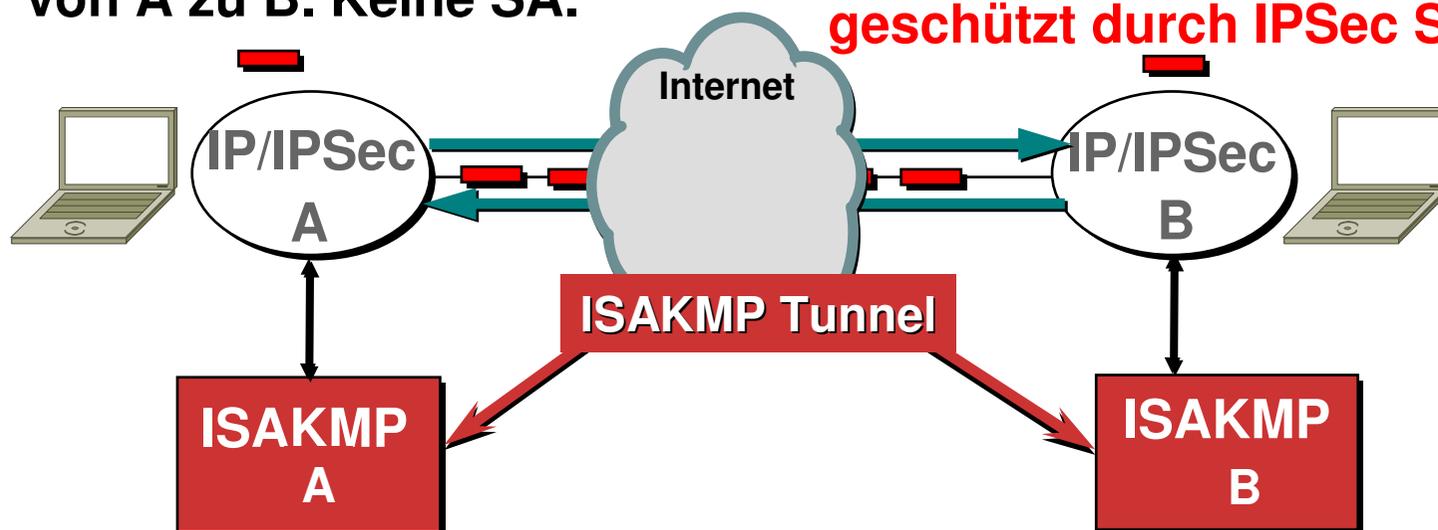
- „Quick Mode“
  - § Aufbau zweier unidirektionaler IPSec SA's (über ISAKMP-Tunnel)
  - § Daten (Payload) werden über diese IPSec SA's übertragen
  - § „Perfect Forward Secrecy“ (PFS): Neue Schlüssel für Phase 2

# 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

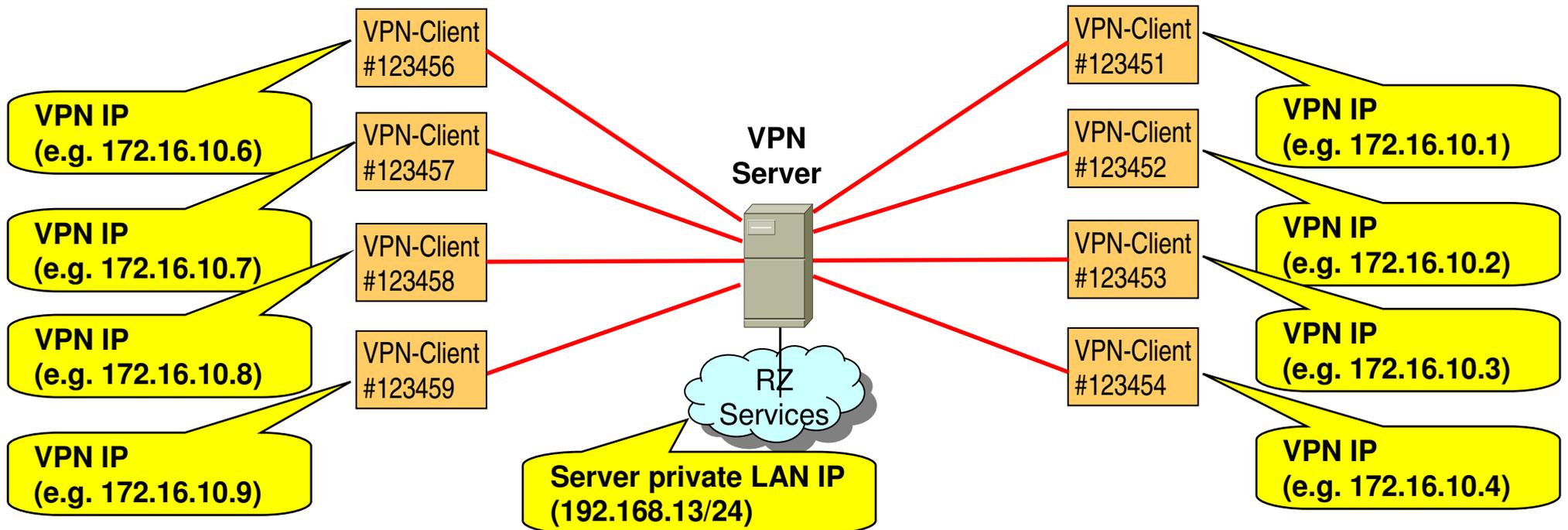
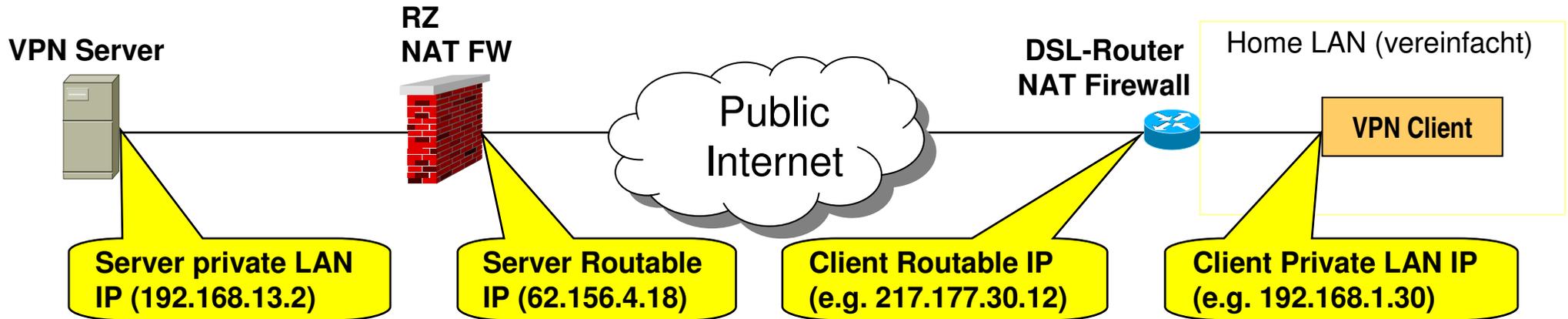


2. A's ISAKMP beginnt Verhandlung mit B.

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“

- n Problem: VPN-Client und/oder VPN Server werden geNATted
- n 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#
- n Aber: IPSec Paket hat kein sichtbares TCP/UDP Header (verschlüsselt!)



- n 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)



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

# IPSec

## Zusammenfassung

### n Wirtschaftlichkeit:

- Trägerprotokoll ist IP
- Kostengünstige Realisierungsmöglichkeiten

### n Sicherheit:

- Mechanismen zur Authentifizierung, Integrität und Vertraulichkeit
- Einsatz starker Kryptografie zur Verschlüsselung

### n Interoperabilität und Integration in Geschäftsprozesse:

- Unabhängigkeit vom Trägernetz durch Tunneling
- Durch Trägerprotokoll IP hohe Interoperabilität und Integration

### n Aber auch:

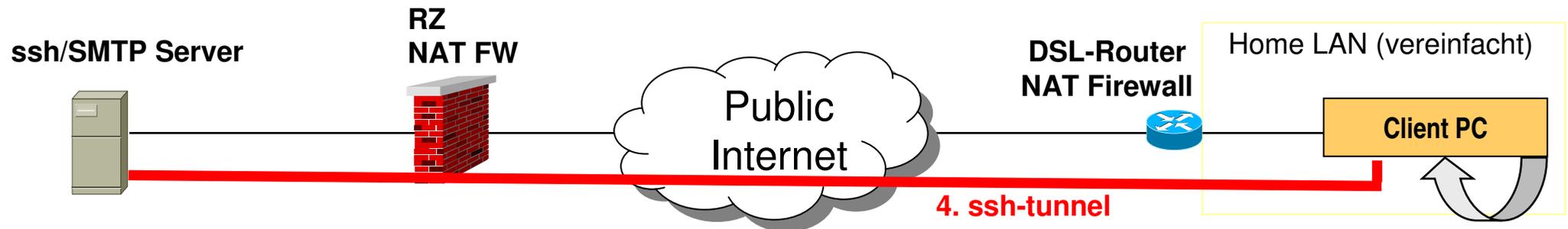
- Quality of Service?
- Komplexität der IPSec Standards und Implementierungen?
- Interoperabilität von verschiedenen IPSec Implementierungen?
- Aufwände durch Aufbau von Certification Authorities (CA) usw.

# Layer-4-7 Technologien

## Einordnung und Überblick

- n 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)
- n 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
- n TLS (Transport Layer Security)
  - IETF WG „Transport Layer Security“, TLS Version 1 (RFC 2246)
  - Konzeptionell und inhaltlich nahezu identisch zu SSLv3
- n „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

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

# Layer-4-7 Technologien

## Zusammenfassung

### n 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

### n 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, Virenschanning usw.)
  - § An der Grenze zum Internet (Firewalls, IDS, Virenschanning, usw.)

# Literatur

## Links zum Thema

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

# Das wärs für heute...

- n Fragen / Diskussion
- n Verbesserungsvorschläge
- n Die Folien von heute sind bereits auf die Web-Seite der Vorlesung
- n Nächste Woche (15. Mai 2008): VPN, Teil 2
- n Einen schönen Abend !!!