
Virtual Private Networks

im Rahmen des Seminars 18.415:
Sicherheit in vernetzten Systemen.

Vortragende:
Marcus Heinzl, Alexander Scheibe, Nils Michaelsen

Virtual Private Networks - Gliederung

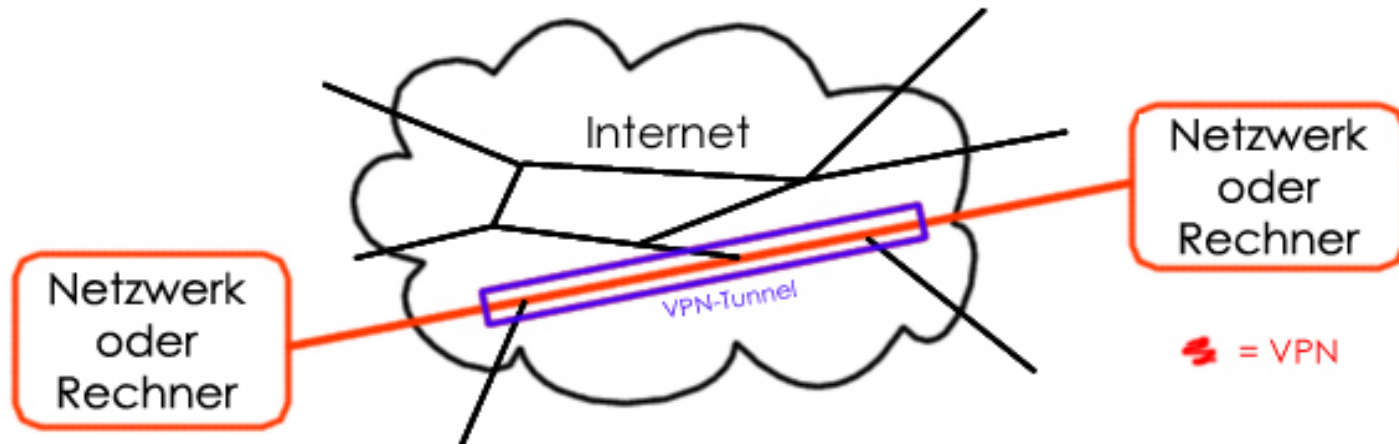
- 1) Einleitung
 - Betriebswirtschaftlicher Hintergrund
 - Begriffsabgrenzung
 - Anforderungen an VPN
- 2) Sicherheitskonzept für VPNs
- 3) Netzwerkkarchitektur
 - Aufbau eines VPN,
 - VPN und Firewalls,
 - VPN-Typen
 - VPN-Szenarien
- 4) Implementation eines gesicherten Übertragungskanal
 - Tunneling
 - L2F, L2TP, PPTP
 - IPSEC
 - SSL
- 5) Schlussbetrachtung

1) Betriebswirtschaftlicher Hintergrund

- Immer kürzer werdende Produktentwicklungs- und Lebenszyklen fordern flexiblere und effiziente Kommunikationsmöglichkeiten, um die Konkurrenzfähigkeit eines Unternehmens zu gewährleisten
 - zunehmende Globalisierung und weltweite Verteilung von Standorten eines Unternehmens fordern IuK-Technologien, die die Filialen eines Unternehmens effizient zusammenführen
- ➔ VPN sind eine Technologie, die genau dies ermöglichen

1) Begriffsabgrenzung „VPN“

- VPN = virtuelles **p**rivates **N**etzwerk
- Verbindung von Netzwerken oder Rechnern verschiedener Standorte von Unternehmen / Institutionen, mittels öffentlicher Kommunikationsnetze, zu einem in sich geschlossenen Gesamtnetz zur gemeinsamen Nutzung von Diensten



1) Begriffsabgrenzung „VPN“

- **virtuell**, weil durch Verbindung mittels öffentlicher Kommunikationsplattformen keine physikalische Verbindung entsteht.
→ Weg und Bandbreite von Daten werden dynamisch bestimmt
- **privat**, weil die Kommunikationspartner an die Verbindung den Anspruch haben, dass sie gesichert ist, so dass kein unbefugter dritter die Kommunikation beeinflussen kann
→ Einsatz kryptographischer Verfahren, um hinsichtlich Integrität, Vertraulichkeit und Authentizität gesicherte Verbindung aufzubauen
- ➔ *Es gibt eine Vielzahl von Ansätzen VPN auf verschiedenen Schichten des OSI-Referenzmodells, den individuellen Ansprüchen von Unternehmen entsprechend, zu implementieren*

1) Anforderungen an VPN

Anforderungen an die Netzwerksicherheit

- Verschlüsselung der Daten
- Identifizierung und Authentifizierung
- Zugriffsberechtigung
- Datenintegrität
- Angriffssicherheit

1) Anforderungen an VPN

Logistische Anforderungen

- Skalierbarkeit der Leistungsfähigkeit
- Weiterentwicklungsmöglichkeiten
- Administrierbarkeit
- Integration in vorhandene Benutzungsumgebungen
- ...

1) Anforderungen an VPN

Anforderungen bzgl. Abwicklung betriebswirtschaftlicher Prozesse

- Globalisierung
- Virtuelle Arbeitsgruppen
- Mobile Arbeiter
- Kundenintegration
- ...

Virtual Private Networks - Gliederung

- 1) Einleitung
 - Betriebswirtschaftlicher Hintergrund
 - Begriffsabgrenzung
 - Anforderungen an VPN
- 2) Sicherheitskonzept für VPNs
- 3) Netzwerkkarchitektur
 - Aufbau eines VPN,
 - VPN und Firewalls,
 - VPN-Typen
 - VPN-Szenarien
- 4) Implementation eines gesicherten Übertragungskanal
 - Tunneling
 - L2F, L2TP, PPTP
 - IPSEC
 - SSL
- 5) Schlussbetrachtung

2) VPN-Sicherheitskonzept

Zentraler Aspekt eines VPN:

mittels kryptographischer Verfahren eine hinsichtlich Integrität, Vertraulichkeit und Authentizität gesicherte Verbindung herzustellen.

Problem:

Aus dem Einsatz einer derart gesicherten Verbindung entsteht eine komplexe Infrastruktur von Kommunikationseinrichtungen

➔ Eine verschlüsselte Verbindung allein reicht nicht aus, um eine vor Angriffen gesicherte Verbindung aufzubauen

2) VPN-Sicherheitskonzept

Einflussfaktoren auf die Erstellung des Sicherheitskonzeptes

- Was ist der Rahmen des Sicherheitskonzeptes?
 - VPN-Sicherheitskonzept ist eine Ergänzung zu einem generellen Sicherheitskonzept für Netzwerke
 - Dementsprechend bleibt es im Rahmen eines vorhandenen Sicherheitskonzeptes für Netzwerke
- Welche Absicherungsmaßnahmen sind für VPN notwendig?
 - Schutzmaßnahmen für Quell- und Zielpart der Verbindung
 - Welche Sicherheitsprotokolle sollen eingesetzt werden
 - Auswahl der kryptographischen Verfahren und Verschlüsselungssysteme
- Wer ist für den Aufbau der gesicherten Verbindung zuständig?
 1. Die gesicherte Verbindung ist bei einem Service-Provider angemietet
 2. Das Unternehmen kümmert sich selbst um die Implementation einer gesicherten Verbindung

2) VPN-Sicherheitskonzept

Mögliche Absicherungsmaßnahmen auf den OSI-Ebenen

	Schichtbeschreibung	Schutzmaßnahmen
5-7 ↕	Anwendungsebenen	SSH, Kerberos, Virus scans, Content Screening, IPSEC (IKE), ...
OSI-Level 3-4 ↕	Transport- und Netzwerkebene	
	TCP / UDP IP	SSL, Socks V5, TLS IPSEC (AH, ESP), Packet Filtering, NAT
1-2 ↕	Link- / physikalische Ebene (Bitübertragungs- und Sicherungsschicht)	Tunneling Protokolle (L2TP, PPTP, L2F), CHAP, PAP, ...

Virtual Private Networks - Gliederung

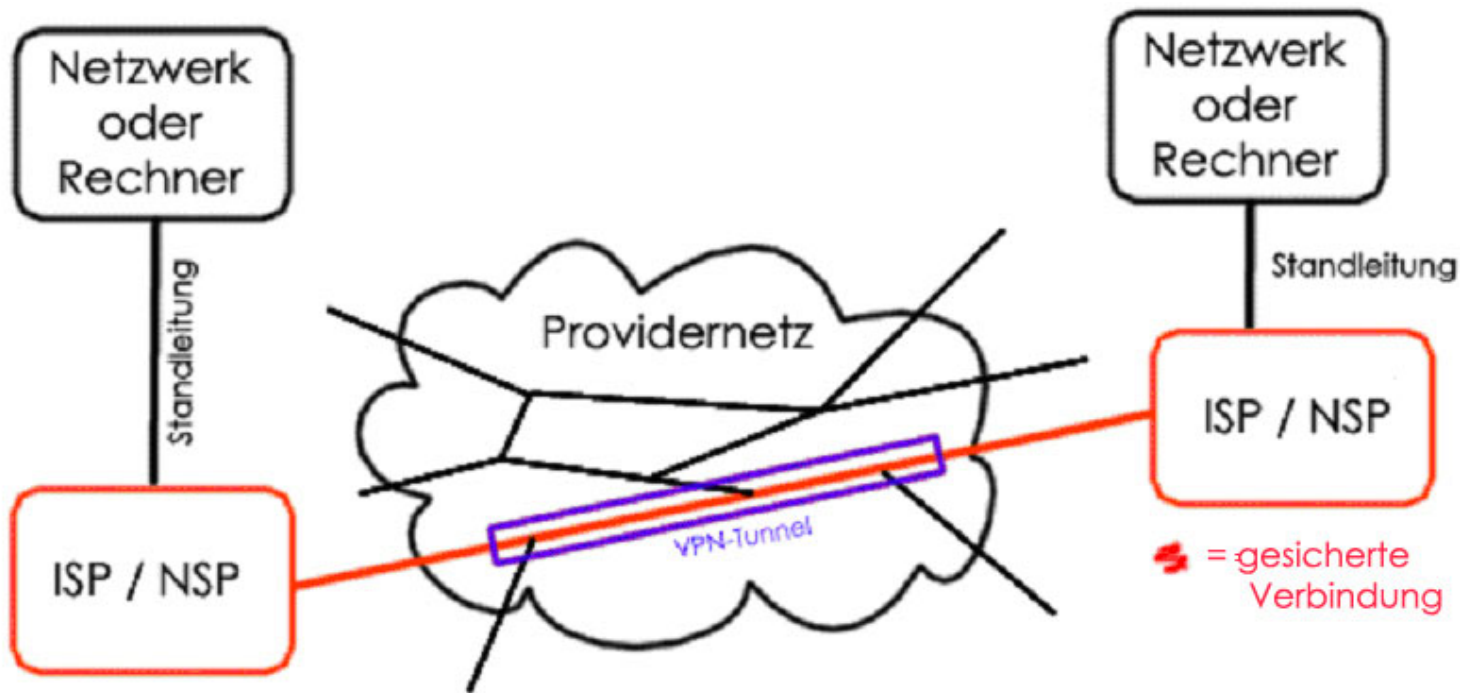
- 1) Einleitung
 - Betriebswirtschaftlicher Hintergrund
 - Begriffsabgrenzung
 - Anforderungen an VPN
- 2) Sicherheitskonzept für VPNs
- 3) **Netzwerkarchitektur**
 - **Aufbau eines VPN,**
 - **VPN und Firewalls,**
 - **VPN-Typen**
 - **VPN-Szenarien**
- 4) Implementation eines gesicherten Übertragungskanal
 - Tunneling
 - L2F, L2TP, PPTP
 - IPSEC
 - SSL
- 5) Schlussbetrachtung

3) Aufbau eines VPN

Es gibt zwei Möglichkeiten eine VPN-Infrastruktur aufzubauen:

1. Compulsory Mode:

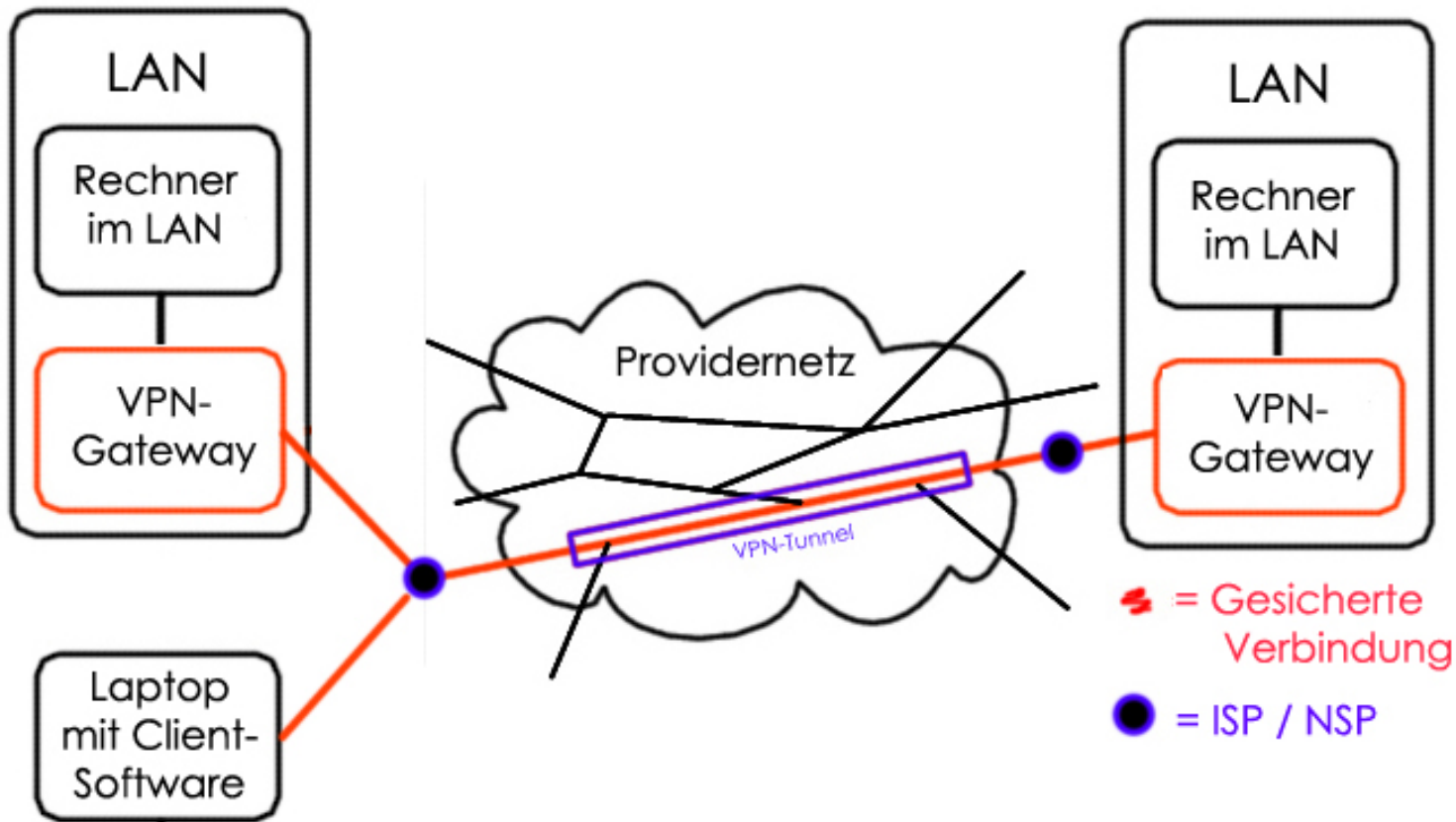
Bei einem ISP / NSP wird eine VPN-Lösung angemietet.



3) Aufbau eines VPN

2. Voluntary Mode:

Implementation einer VPN-Lösung in Eigenregie



3) VPN und Firewall

Philosophie von Firewalls:

Die Firewall ist die einzige Verbindung ins Internet, alles andere befindet sich dahinter, also auch das VPN-Gateway

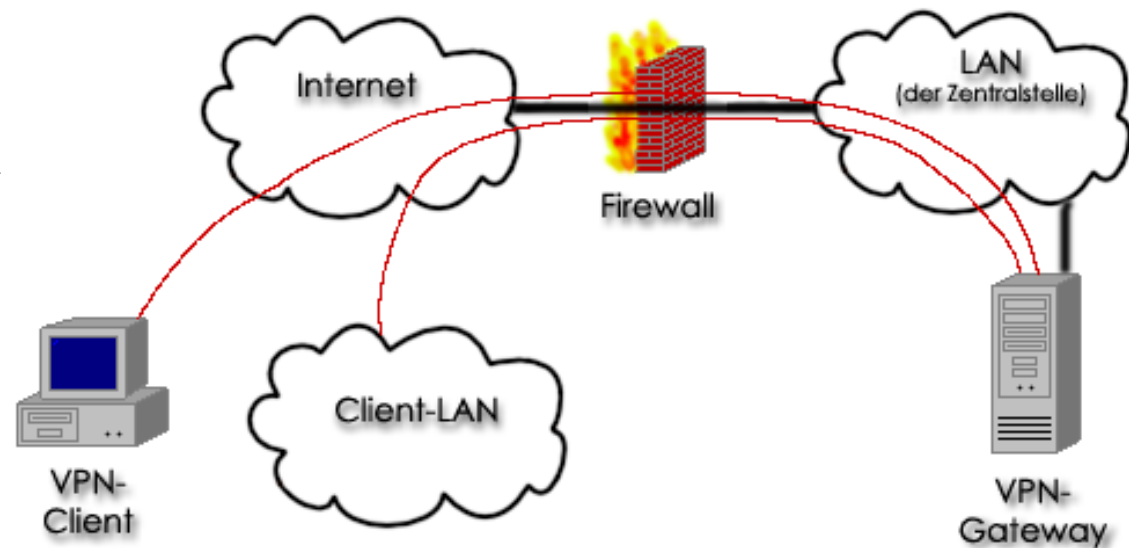
Problematik:

Verbindungen zwischen VPN-Gateways sind verschlüsselt und nicht von der Firewall analysierbar.

3) VPN und Firewall

Variante 1:

VPN-Gateway befindet sich hinter der Firewall



Vorteile:

- Die Firewall ist die einzige Verbindung ins Internet

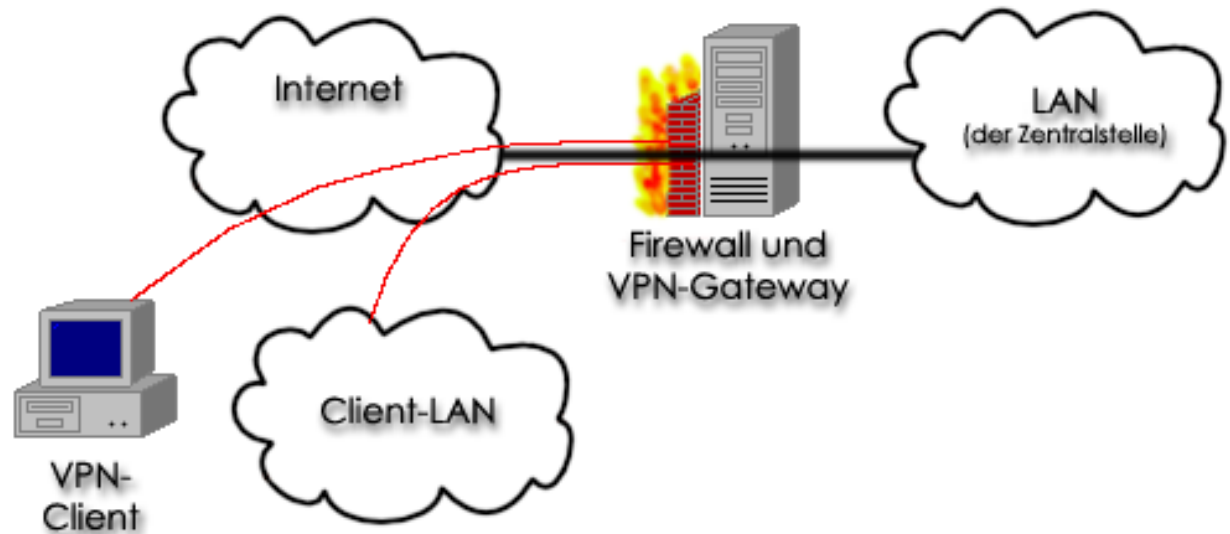
Nachteile:

- Daten zum VPN-Gateway sind verschlüsselt und nicht von der Firewall analysierbar

- Zielrechner und Ports können nur vom VPN-Gateway erkannt werden

3) VPN und Firewall

**Variante 2:
VPN-Gateway und
Firewall befinden sich
auf einem Rechner**



Vorteile:

- Nachteile von Variante 1 werden ausgeschaltet
- Administrationsaufwand beschränkt sich auf einen Rechner

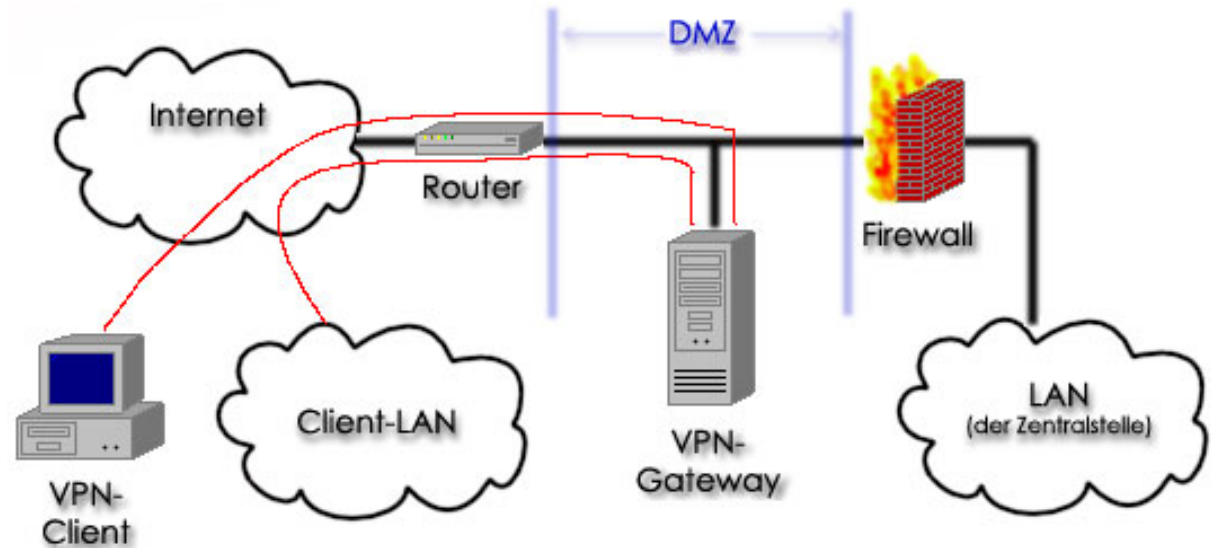
Nachteile:

- Nach draußen sind neue Ports geöffnet

3) VPN und Firewall

Variante 3:

VPN-Gateway befindet sich in einer demilitarisierten Zone



Vorteile:

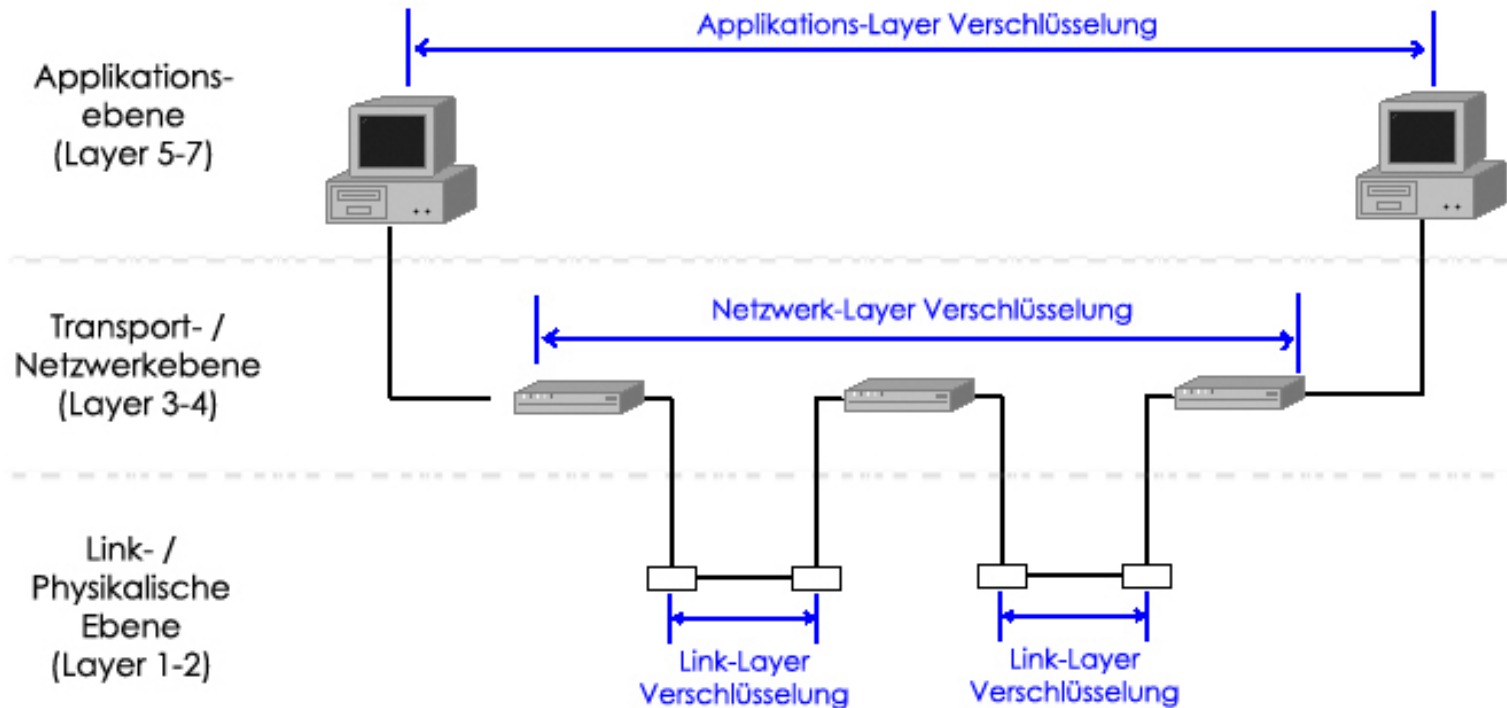
- Nachteile von Variante 2 werden ausgeschaltet
- Jedes Paket passiert entschlüsselt(!) die Firewall
- Zugriff ins Netz ist auf bestimmte Ressourcen u. Rechner beschränkt

Nachteile:

- Erhöhter Administrationsaufwand

3) VPN-Typen

Unterteilung der 7 OSI-Layer in drei Ebenen von VPN-Typen:



3) VPN-Typen

Einsatzgebiete

- VPN auf der Anwendungsebene:
 - Kommunikation mit Partner-Netzen
- VPN auf Layer 4 (Transportschicht)
 - oft in Anwendungen integriert (Tunnel wird automatisch geöffnet [z.B. InternetBrowser mit SSL])
 - Erlaubt hohe individuelle Sicherheit, da viele Verschlüsselungsverfahren unterstützt werden
- VPN auf Layer 3 (Vermittlungsschicht)
 - bietet die Möglichkeit neben TCP auch UDP oder RPCs einzusetzen
- VPN auf Layer 2 (Sicherungsschicht)
 - Unabhängig von spezifischen Netztypen (IP-Netze, ATM, ...) einsetzbar
 - Verbindungen die ohne feste IP-Nummern initialisierbar sein sollen

3) Typische VPN-Szenarien

Intranet-VPN (Site-To-Site):

Zielsetzung:

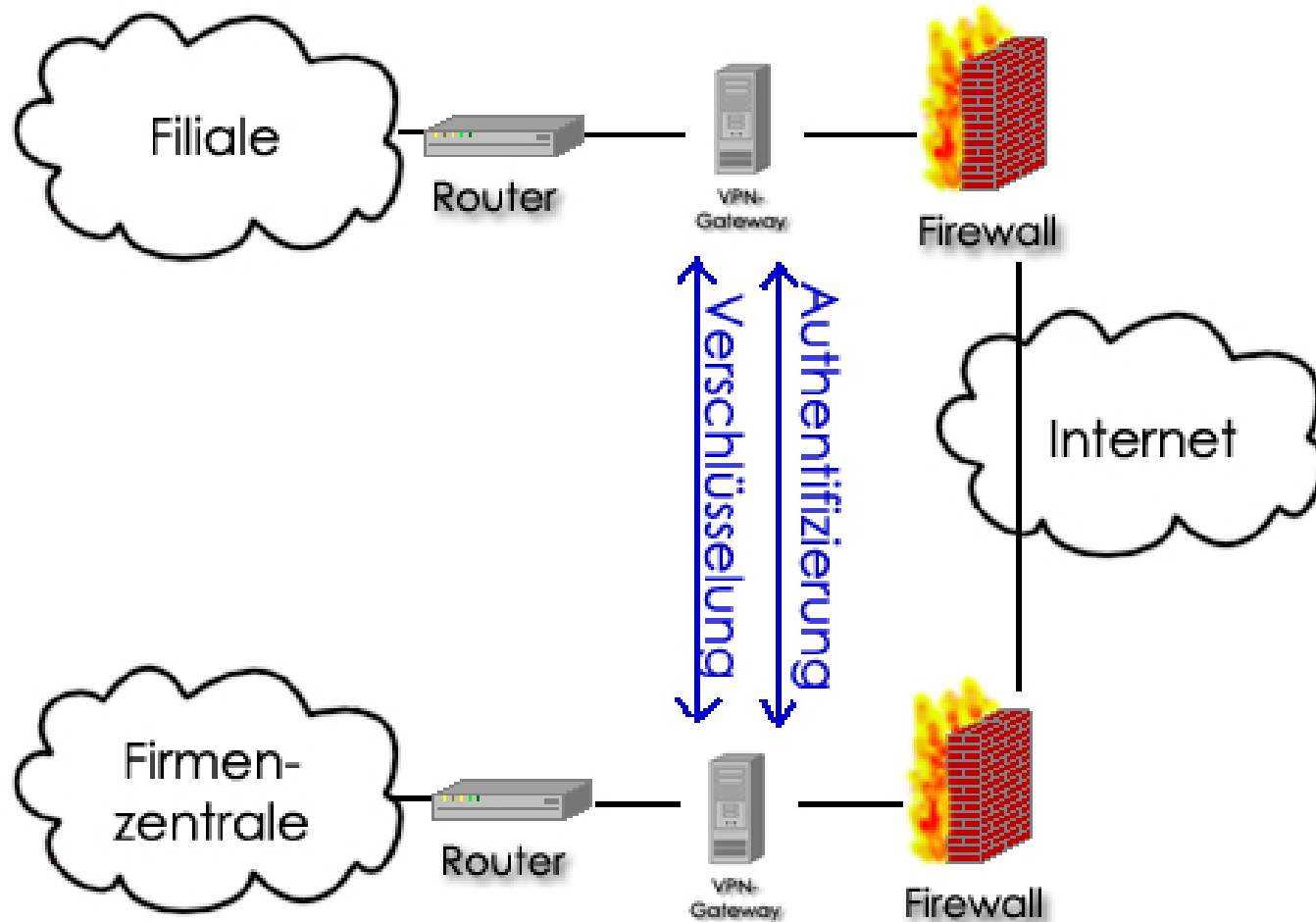
- Filialen und Geschäftsstellen verbinden,
- In den Filialen die gleichen Geschäftsprozesse wie in der Zentrale ermöglichen

Anforderungen:

- Sichere Verbindung über das Internet zwischen zwei VPN-Gateways, die sich in der demilitarisierten Zone der zu verbindenden Netze befinden.

3) Typische VPN-Szenarien

Intranet-VPN (Site-To-Site):



3) Typische VPN-Szenarien

Extranet-VPN (End-To-End):

Zielsetzung:

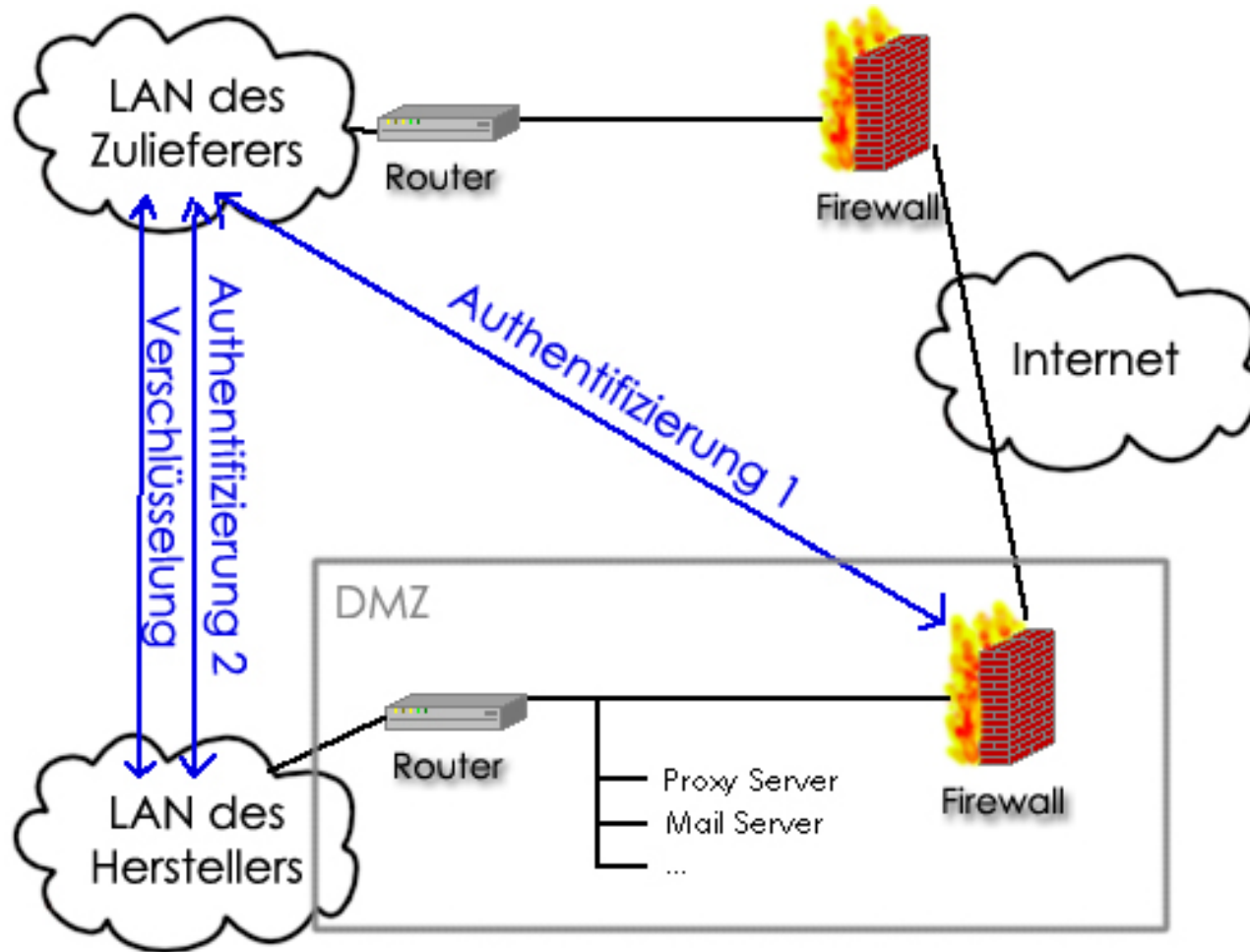
- Optimierung betriebsinterner Geschäftsprozesse durch Integration von Zulieferern, Partnerunternehmen und Kunden,
- Optimierung der Wertschöpfungskette,
- Verbesserter Kundenservice, usw.

Anforderungen:

- Die Teilnehmer am Extranet müssen sich identifizieren und authentifizieren, um bestimmte Berechtigungen wahrzunehmen
- Sehr oft ist der gesamte Übertragungsweg von einem End-Gerät zu dem End-Gerät eines anderen Netzes zu sichern, wenn Unterabteilungen von Unternehmen miteinander kommunizieren (z.B. Einkauf und Verkauf)

3) Typische VPN-Szenarien

Extranet-VPN (End-To-End):



3) Typische VPN-Szenarien

Remote-Access-VPN (End-To-Site):

Zielsetzung:

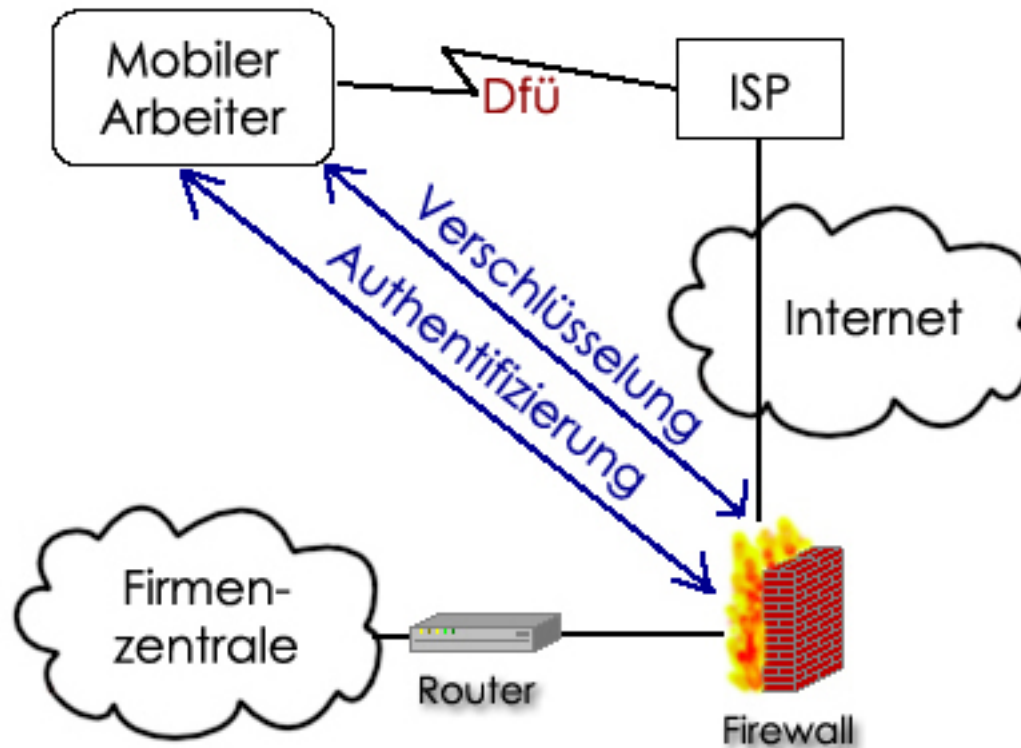
- Mobilen Außendienstmitarbeitern einen Zugang zum Firmennetz von jedem beliebigen Zugang zum Internet gewährleisten

Anforderungen:

- Gesicherte Verbindung vom Rechner des Außendienstmitarbeiters bis zu einem VPN-Gateway in der DMZ der Zentrale

3) Typische VPN-Szenarien

Remote-Access-VPN (End-To-Site):



Virtual Private Networks - Gliederung

- 1) Einleitung
 - Betriebswirtschaftlicher Hintergrund
 - Begriffsabgrenzung
 - Anforderungen an VPN
- 2) Sicherheitskonzept für VPNs
- 3) Netzwerkkarchitektur
 - Aufbau eines VPN,
 - VPN und Firewalls,
 - VPN-Typen
 - VPN-Szenarien
- 4) **Implementation eines gesicherten Übertragungskanal**
 - **Tunneling**
 - **L2F, L2TP, PPTP**
 - **IPSEC**
 - **SSL**
- 5) Schlussbetrachtung

4) Tunneling

Das Prinzip des Tunnelings

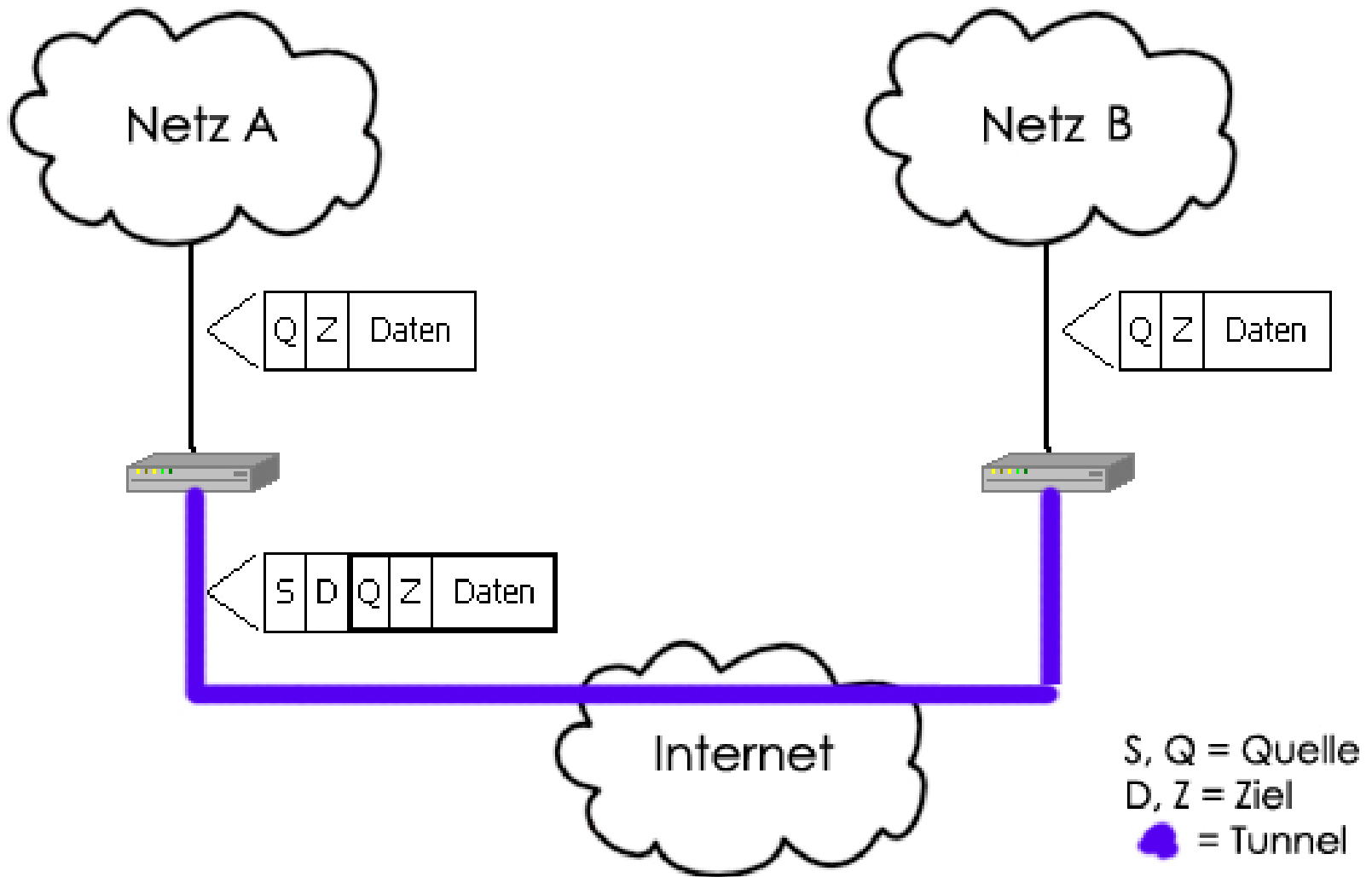
- beliebige Datenpakete, eines beliebigen Protokolls können über ein Transitnetz verschickt werden
- die Datenpakete sind die Nutzlast eines anderen Protokolls (ein für das Transitnetz zuständiges)
- Z.B. können so IPv6-Pakete über ein auf IPv4 ausgelegtes Teilnetz verschickt werden

4) Tunneling

Encapsulation

- Das Verpacken eines Protokoll-Paketes als Nutzlast eines anderen Protokolls wird als *Encapsulation* bezeichnet
- Dem gekapselten Protokoll wird ein sogenannter Tunnel-Header vorangestellt, in dem sich Quell- und Zielports befinden
- Der Anfangspunkt eines Tunnels befindet sich dort, wo der Tunnel-Header angefügt wird. Analog dazu befindet sich der Endpunkt des Tunnels dort, wo der Header wieder entfernt wird

4) Tunneling



4) Tunneling

Vorteile des Tunneling im Einsatz für VPN

- Ein Transfer über Netze verschiedener Protokolle ist möglich
- Die Payloaddaten können verschlüsselt werden
 - Zielport und Adresse des ursprünglichen Pakets sind verschlüsselt
 - Die Daten des ursprünglichen Pakets sind verschlüsselt

4) Tunneling

General Routing Encapsulation Tunnel (GRE-Tunnel)

- Versuch einer Standardisierung für Tunnelverfahren von 1994
- Drei Abschnitte des GRE-Pakets werden unterschieden:
 - GRE-Header (Protokollkopf): Enthält Informationen über die eingesetzten Tunnel- und Verschlüsselungsalgorithmen
 - Netzwerk-Protokollkopf: Speichert das Tunnelziel außerhalb des Tunnels
 - Nutzlast (Payload)

4.2) Layer-2-Techniken

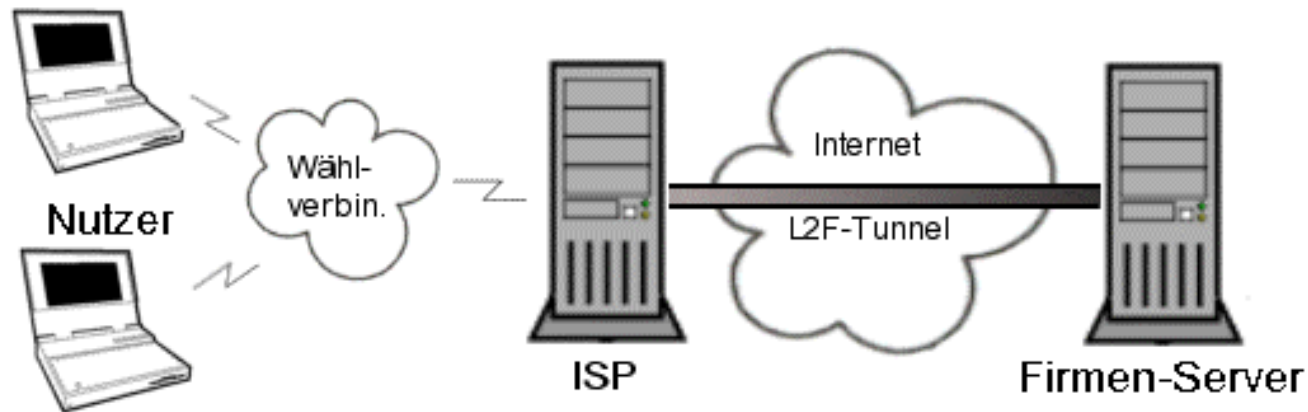
- L2F, PPTP, L2TP, L2Sec
- Vorteil gegenüber Layer-3-Verfahren:
 - Multiprotokollfähigkeit
 - einfachere Wartung und Betreuung
 - problemlose Network Address Translation

L2F

Layer-2 Forwarding (L2F)

- ermöglicht VPN-Aufbau über ein öffentliches Netz
- arbeitet zusammen mit:
IP, Frame-Relay, ATM, FDDI, HDLC u.a.
- multiple Verbindungen gleichzeitig

Layer-2 Forwarding (L2F)



- Tunnel besteht nur zwischen POP und Sicherheits-Gateway und dem NAS des Unternehmens
- Authentifikation via PPP, zusätzlich auch TACACS+ oder RADIUS

PPTP

Point-to-Point-Tunnelling-Protocol (PPTP)

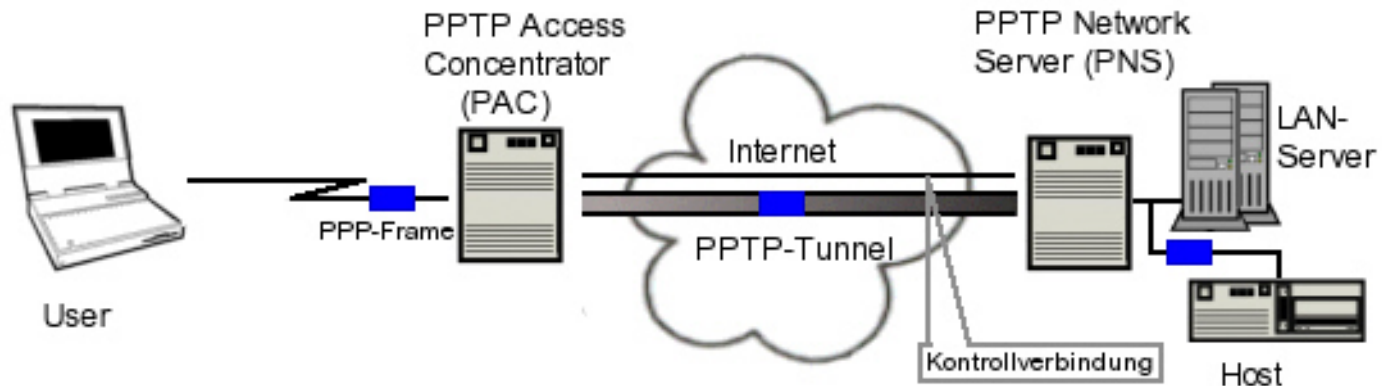
- ermöglicht VPN-Aufbau über ein öffentliches Netz
- Einfacherer Zugriff auf ein Unternehmens-LAN
- höhere Verbreitung als L2F

PPTP-Charakteristika

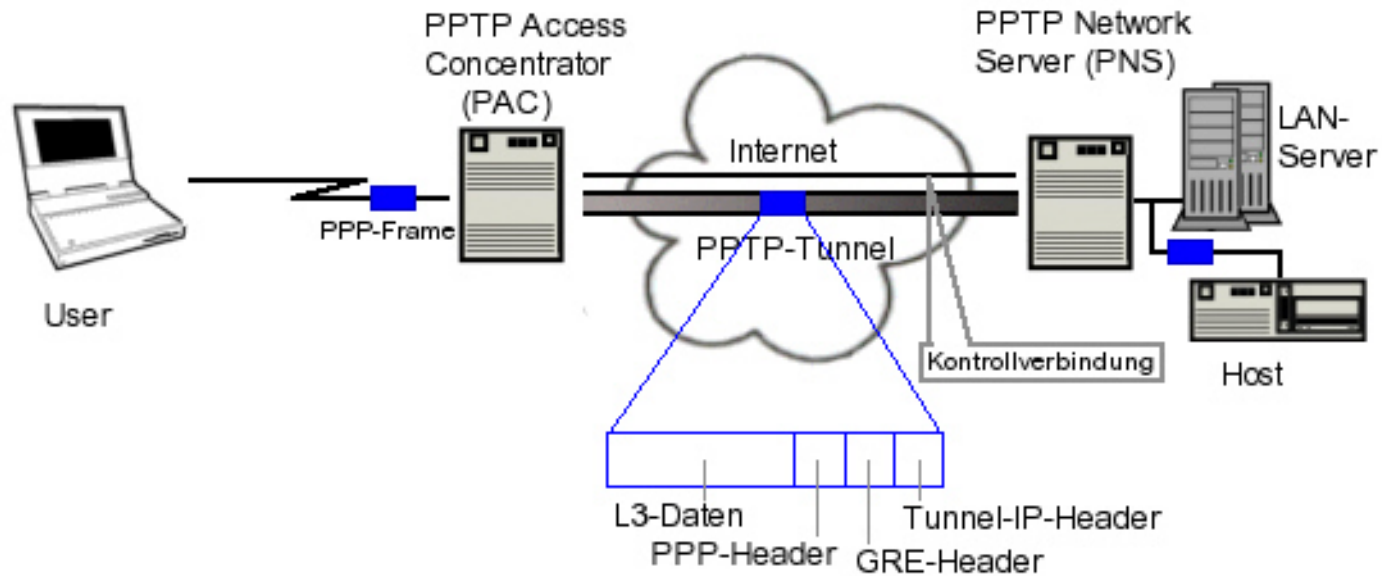
- Kontrollverbindung neben dem Tunnel.
- Initiierung nur auf Aufforderung von einem Endgerät
- Nur ein Tunnel pro Verbindung
- Verbindungen sind protokollunabhängig
- Authentifizierung via PPP nahe Mechanismen
- PPTP greift auf die eher schwachen Sicherheitsmechanismen von MPPE zurück.

PPTP-Tunnel-Prinzip (I)

- Trennung von Daten- und Kontrollfluss



PPTP-Tunnel-Prinzip (II)



- Der GRE-Header dient zur Regelung des Datenflusses und erlaubt dessen Kontrolle nach dem Sliding-Window-Prinzip

PPTP Verbindungsarten

- Auf Anfrage eines Fernnutzer vom NAS initiierte statische Verbindung (compulsory Mode)
- Nutzerinitiierte dynamische Dail-In-Verbindungen (voluntary Mode)

Compulsory vs. Voluntary Mode

vordefinierter Tunnelweg

„freier Weg“

PC-Endgerät kann den Weg nicht verlassen

beliebige Internetadressen ansteuerbar

multiple Verbindungen über den Tunnel möglich

nur eine Verbindungen über den Tunnel möglich

geringerer Overhead bei multiplen Verbindungen über einen Tunnel

hoher Overhead, bei gleicher Verbindungszahl.

Hoher Wartungs- und Betriebsaufwand

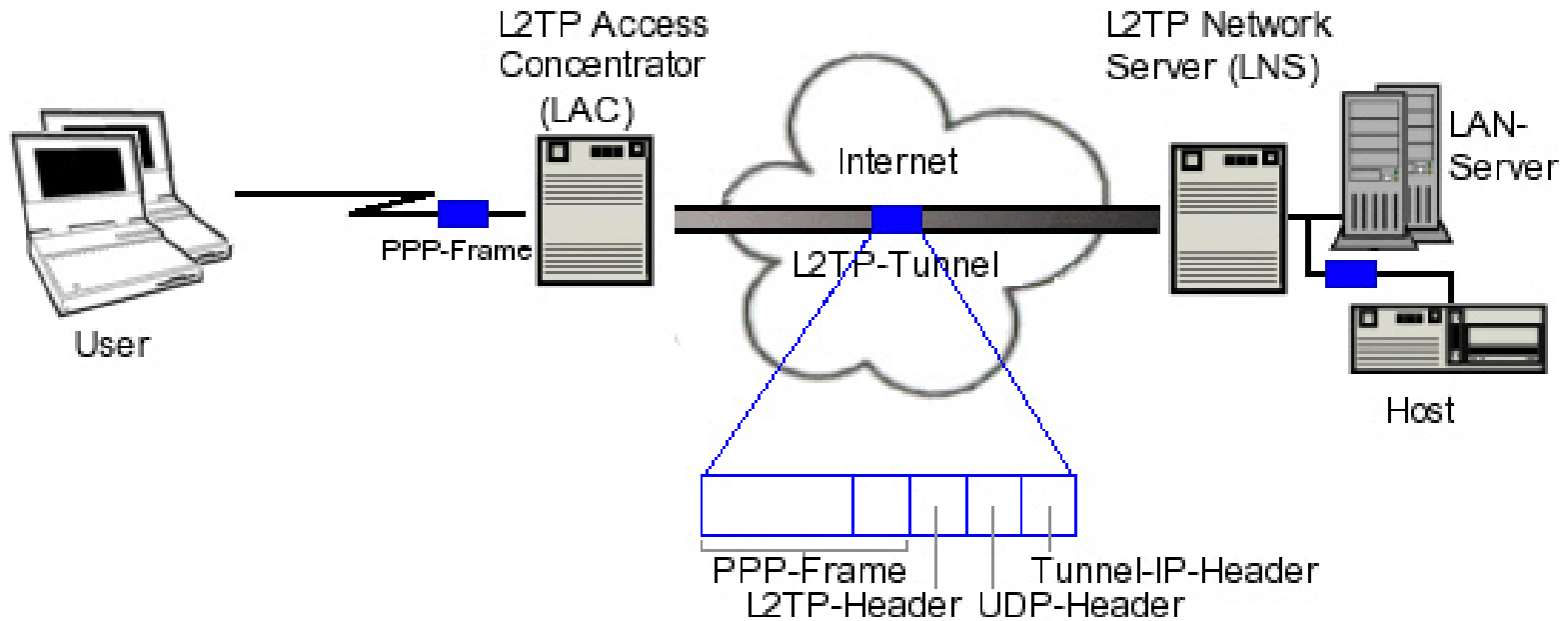
Einfacherer Wartungs- und Betriebsaufwand

L2TP

L2TP

- ermöglicht VPN-Aufbau über ein öffentliches Netz
- anerkannter Industriestandard
- Mischform aus L2F und PPTP
 - multiple Verbindungen über einen Tunnel
 - In-band-Kontrollfluss
 - Compulsory und Voluntary Modi
 - ATM, Frame-Relay und X.25 möglich

L2TP



Vertraulichkeit durch IPSec

L2Sec

L2Sec

- Standardisierungsvorschlag.
- Kann als Kombination aus L2TP und SSL/TLS-Auth. aufgefasst werden.
- beliebiger Protokolle wie SNA, NetBios, HDLC oder IPX nutzbar.
- Remote-Access auf hohem Sicherheitsniveau.

L2Sec - Nachteile

- keine einzelne Absicherung von Ports und Prozessen
- Starker Protokoll-Overhead gegenüber IPSec

Nachwort Layer-2 Techniken

- Alle beschriebenen Layer-2 Techniken gewährleisten lediglich die Datenintegrität und die Nutzer-Authentisierung, jedoch wird kein Schutz gegen Ausspähen, Maskieren oder anderer Manipulationen der Daten gewährleistet.

4.3) IPSec

- Menge von Sicherheitseigenschaften als Erweiterung für IPv4, in IPv6 enthalten
- Offenheit
- Die Sicherheitsarchitektur besteht aus
 - Security Association
 - Security Association Database
 - Security Policy Database

4.3) IPSec Ziele (1)

- Sicherung eines Kommunikationskanals
- Offenheit für
 - Herstellerunabhängige Implementation
 - Verschiedene Kryptografische Verfahren
 - Verschiedene Sicherungs-Protokolle (AH,ESP)
 - Neue Protokolle und Kryptographische Verfahren

4.3) IPSEC Ziele (2)

- Wahrung von
 - Data origin authentication
 - Connectionless integrity
 - Anti-Replay
 - Data confidentiality (optional)
 - Limited traffic flow confidentiality (optional)

4.3) Security Association (SA)

- Einigung der Endpunkte über Verbindungsparameter
- Tripel bestehend aus (SPI, Zieladresse ,Protokoll)
- SPI: eindeutiger Wert zur Identifikation der Verbindung
- Protokoll : zur Zeit AH und ESP
- Simplex / unidirektional
 - für jede Richtung (inbound / outbound) eine SA

4.3) Association Database (SAD)

- Verwaltung aktiver Security Associations
- Enthält zusätzliche Parameter einer IP-Sec Verbindung :
 - Sequence Number, ein 32-bit Zähler
 - Sequence Number overflow, bestimmt bei ausgehenden Verbindungen, ob ein Overflow ein Ereignis erzeugen soll
 - Anti-Replay Windows, bestimmt für eingehende Verbindungen, ob es sich um eine Wiederholung (Replay handelt)
 - Kryptographische Informationen für die AH Authentikation (Algorithmus, Schlüssel, etc.)
 - Kryptographische Informationen für die ESP Authentikation
 - Kryptographische Informationen über Algorithmus zur Verschlüsselung
 - *SA Lifetime*
 - *IPSec protocol mode*, Auswahl des Kommunikationsmodus für AH bzw. ESP; kann auch wildcard sein.
 - PMTU, Maximale MTU eines IP Datagrams

4.3) SAD eines Cisco Routers vielleicht später ?

Inbound esp sas:

Spi: 0x71BB425D(1908097629)

Transform: esp-des esp-md5-hmac

In use settings={Tunnel, }

Slot: 0, conn id: 2000, flow_id: 1, crypto map: mode

Sa timing: remaining key lifetime (K/sec): (4608000/3500)

IV size: 8 bytes

Replay detection support: Y

Nach „Inside Network Perimeter Security“ von Northcutt et. al.

4.3) Security Policy Database (SPD)

- Enthält Anforderungen an SA:
 - Destination IP
 - Source IP
 - Transport Layer Protocol
 - Systemname: FQDN oder X.500 DN
 - User ID: Fully Qualified DNS User Name oder X.500 DN
 - Verweis auf SA
- Wird vor Einrichtung einer inbound und outbound SA konsultiert
- Entscheidet über
 - Verwurf eines Packetes
 - Verarbeitung ohne IPsec
 - Verarbeitung mit IPsec

4.3) Kommunikationsmodus

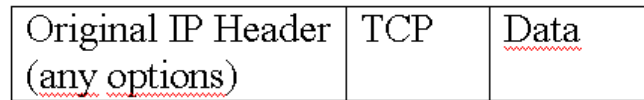
- Transportmodus
 - Sichert nur Nutzlast
 - Keine Verdeckung der internen Struktur
 - Geeignet für Host-zu-Host Kommunikation
- Tunnelmodus
 - Sichert Nutzlast und Adressinformationen
 - Kapselung in anderem Packet
 - Hier: IP over IP Tunnel
 - Geeignet für Kommunikation über Gateways
 - “Whenever either end of a security association is a security gateway, the SA MUST be tunnel mode.” (RFC2401)

4.3) Authentication Header (AH)

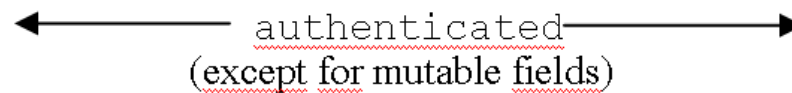
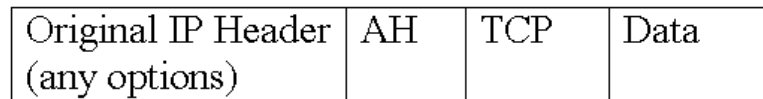
- Header Erweiterung - kein Protokoll nach OSI
- Wahrung von
 - Data origin
 - Connectionless Integrity
 - Anti Replay
- sichert Authentizität und Integrität durch ICV
- ICV ist in Authentication Data gespeichert und
 - Digitaler Signatur
 - Message Authentication Code (z.B. Hash mit Schlüsselinformation)
- NAT nur im Tunnelmodus möglich

Next header	Payload Len	RESERVED
Security Parameter Index(SPI)		
Sequence Number Field		
Authentication Data (variable)		

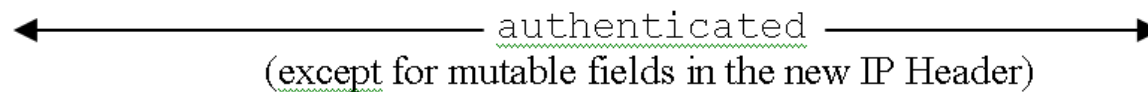
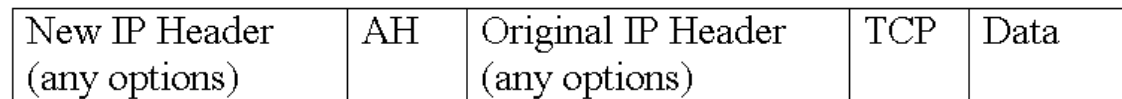
4.3) AH & Kommunikationsmodus



IPv4 Header vor der Anwendung des AH



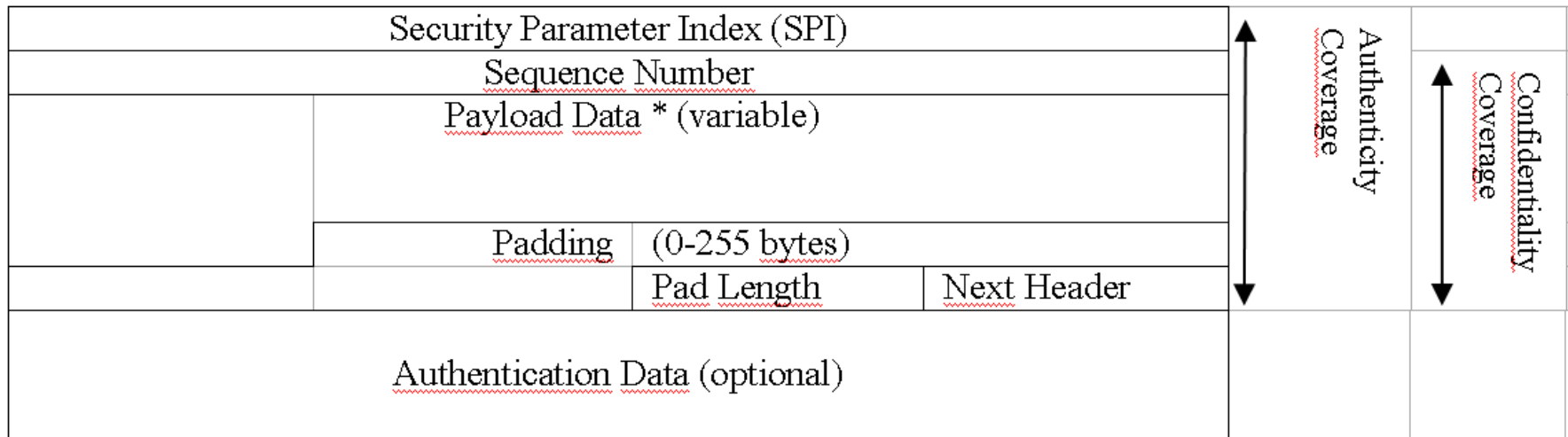
IPv4 Header nach der Anwendung des AH im Transport Modus



IPv4 Header nach der Anwendung des AH im Tunnel Modus

4.3) Encapsulating Security Payload (ESP)

- Sichert die Vertraulichkeit, genauer:
 - Data confidentiality
 - Limited Traffic Flow confidentiality
- Authentikation wie AH ist optional
- besteht aus Header, Trailer und optional aus Authentikationsteil
- NAT nicht möglich



4.3) ESP & Kommunikationsmodus

BEFORE APPLYING ESP

Original IP Header (any options)	TCP	Data
-------------------------------------	-----	------

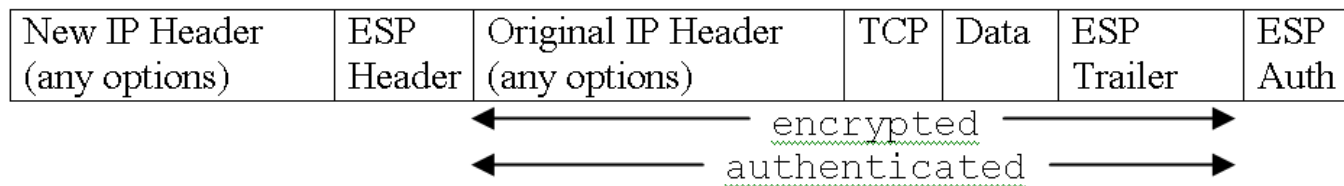
IPv4 Header vor der Anwendung des ESP

AFTER APPLYING ESP (Transport Modus)

Original IP Header (any options)	ESP Header	TCP	Data	ESP Trailer	ESP <u>Authentikation</u>
-------------------------------------	------------	-----	------	-------------	---------------------------



IPv4 Header vor der Anwendung des ESP im Transport Modus



IPv4 Header vor der Anwendung des ESP im Tunnel Modus

4.3) SA Negotiation

- Beiden Partnern einer IPSec-Verbindung müssen
- Authentikationsverfahren
- Verschlüsselungsmethode
- Schlüssel
- Bekannt sein
- Problem: bei manuellem Einstellen
 - entsteht zu hoher administrativer Aufwand
 - Schlüssel müssen regelmäßig aufgetauscht werden
- Lösung: automatischer Schlüsselaustausch
 - Urvater : Diffie-Hellman Keyexchange

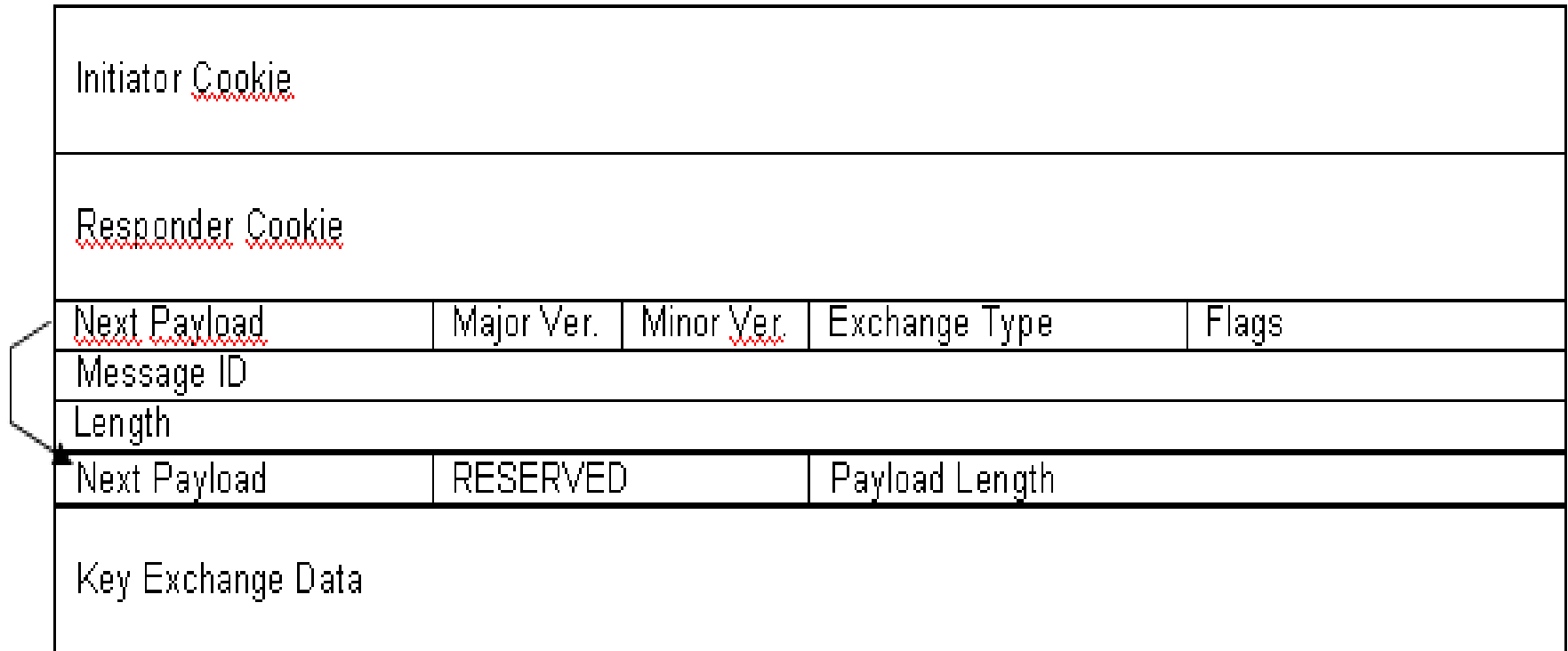
4.3) Internet Key Exchange (IKE)

- Ein (!) von IPSec vorgeschlagener Schlüsselaustausch
- Ziel: automatische und sichere Aushandlung einer IPSec Security Association
- Basiert auf ISAKMP (Rahmenwerk), OAKLEY, SKEME
- Besteht aus 2 Phasen:
 - Phase 1: Aufbau eines sicheren Kanals hinsichtlich Wahrung von Vertraulichkeit und Authentizität
 - Phase 2: Austausch der kryptographischen Informationen

4.3) ISAKMP

- Internet Security Association and Key Management Protocol
- Rahmenwerk für für Authentikation und Schlüsselaustausch
- Kein expliziter Schlüsselaustausch
- Anwendungsschichtprotokoll, Standardport: 500/UDP
- Definiert die 2 Phasen, die von IKE verwendet werden
- Definiert Protokoll zum Austausch von Informationene
 - Dabei: Header + 12 individuelle Payloads (ISAKMP SA, KE...)
- Einzige Implementation in IKE

4.3) ISAKMP Header



...

- Cookies gegen Denial of Service und Replay
- Key Exchange Data: “the data required to generate a session key”
→ Zufallszahlen, Diffie-Hellmannwerte

4.3) IKE Phase 1

- Art des Phase 1 Austausches
- Aushandlung einer ISAKMP SA für sichern Informationskanal
- Eine SA-Payload enthält mehrere Proposals mit Informationen, was eine Seite akzeptiert
- Starke Authentikation durch
 - Pre shared key
 - Public Key
 - Digitaler Signatur
- Übertragung von Zufallswerten (Nonce) oder Diffiehellman Werten zur Aushandlung eines symmetrischen Schlüssels zur Übertragung

4.3) IKE Phase 1 : Main-Mode & Agressive Mode

Main Mode

Initiator					Responder		
1	HDR	SA		→			
2				←	HDR	SA	
3	HDR	KEYEXCHANGE	<u>NONCE_i</u>	→			
4				←	HDR	KEYEXCHANGE	<u>NONCE_r</u>
5	HDR*	<u>IDINFORMATION_{ii}</u>	AUTH	→			
6				←	HDR*	<u>IDINFORMATION_r</u>	AUTH

Aggressive Mode

1	HDR	SA	KE	N _i	<u>ID_{ii}</u>	→						
2						←	HDR	SA	KE	<u>N_r</u>	<u>ID_{ir}</u>	AUTH
3	HDR*	AUTH				→						

4.3) IKE Phase 2: Quick Mode (1)

- Aushandlung von Authentikationsmethoden und Verschlüsselungsverfahren einer IPSec-SA
- Perfect Forwarded Security (PFS):
 - Kompromittierung eines Schlüssels gefährdet nicht die weiteren Schlüssel
- Base-Quick mode: verwendet die Schlüssel der Phase 1 auch für IPSec → keine PFS
- PFS-Quickmode: Aushandlung neuer Key Exchange Informationen

4.3) IKE Phase 2: Quick Mode (2)

1)	HDR*	HASH (1)	SA	<u>Nonce initiator</u>	[KE]	<u>[IDi, IDr]</u>	→						
2)							←	HDR*	HASH (2)	SA	<u>NONCE responder</u>	[KE]	<u>[IDi, IDr]</u>
3)	HDR*	HASH (3)						→					

- HASH in jeder Nachricht zur Authentikation
- Jede Nachricht ist verschlüsselt

4.3) Beispiel Cisco Router

Initiation IKE Phase 1 (IP ADDR=10.0.0.1)

SENDING>>>>ISAKMP OAK MM (SA)

RECEIVED<<<<ISAKMP OAK MM (SA)

SENDING>>>>ISAKMP OAK MM (KE, NON, VID, VID)

RECEIVED<<<<ISAKMP OAK MM (KE, NON, VID)

SENDING>>>>ISAKMP OAK MM* (ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)

RECEIVED<<<<ISAKMP OAK MM* (ID, HASH)

Established IKE SA

Initiation IKE Phase 2 (IP ADDR=10.0.0.1)

SENDING>>>>ISAKMP OAK QM* (KE, NON, ID, ID)

RECEIVED<<<<ISAKMP OAK QM* (HASH, SA, NON, ID, DINOTIFY:STATUS_RESP_LIFETIME)

SENDING>>>>ISAKMP OAK QM * (HASH)

Loading IPsec SA (message ID = 22E625C1 OUTBOUND SPI=AB2763F7 INBOUND
SPI=353BC22E)

4.3) Kritik: Schwächen von IPsec

- Komplexität: der Feind der Sicherheit
 - Zu viele Details, nur ESP-Tunnel sinnvoll
 - Vorkehrungen gegen DoS bringen nicht das gewünschte Ergebnis
- Schlechte, verwirrende Dokumentation
 - Wiederholungen
 - Keine Zielsetzungen / Begründungen
 - Schlechte HASH-Definition
- Schwächen aus Kryptographie (Vortrag 4)
- Implementationsfehler in ISAKMP-Dienst
 - Denial of Service Angriffe auf Port 500/UDP

4.4) Layer-4 Techniken

Secure Socket Layer (SSL) und Transport Layer Security (TLS)

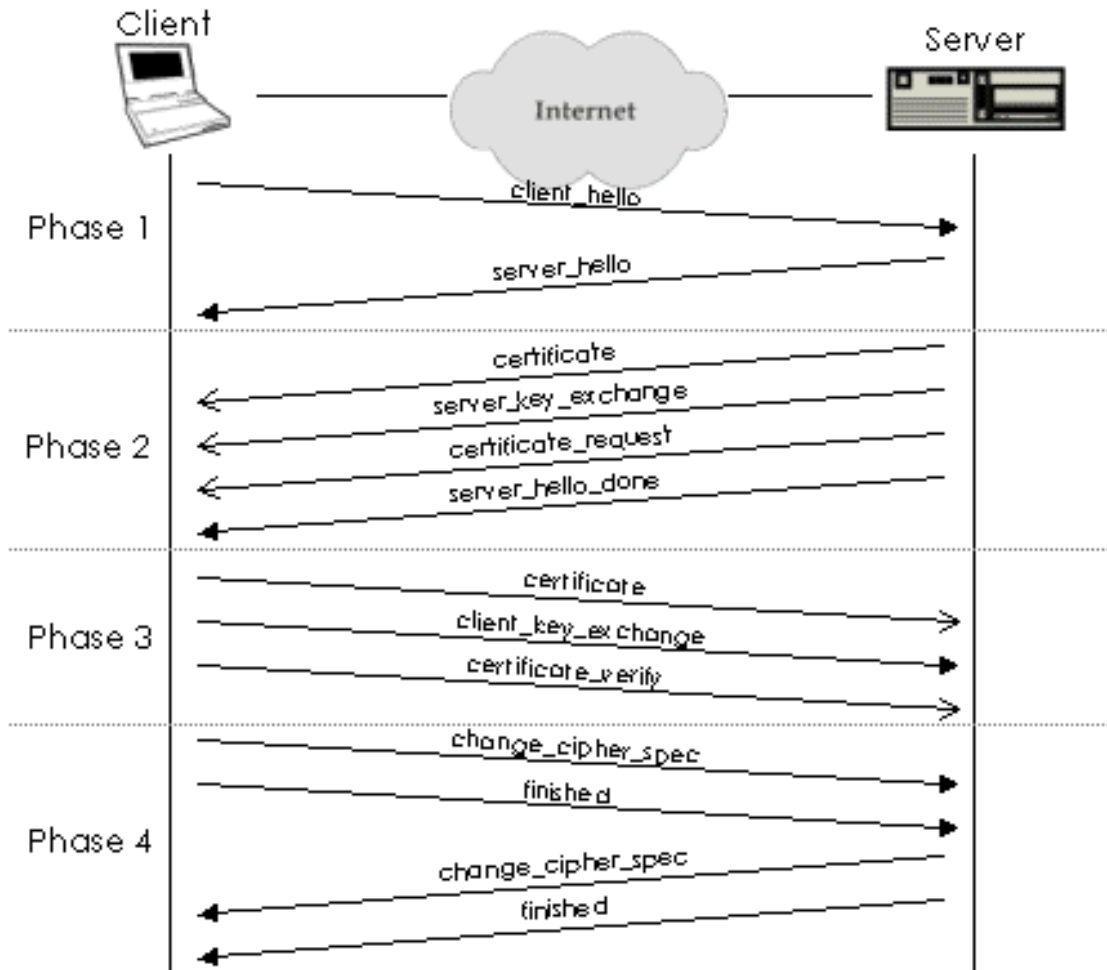
SSL / TLS

- Zur kryptographischen Verbindungsabsicherung zweier Anwendungen.
- Erlaubt nur die Kommunikation zwischen autorisierten Partnern.
- Unterbindet das Belauschen und Verfälschen von Informationen.

Einordnung von SSL in TCP/IP



SSL-Verbindungsaufbau



TLS und TLS/SSL-Sicherheit

- TLS ist als Erweiterung von SSLv3.0
- HMAC nach RFC-2104
- Einfaches Eindringen in SSL bei sehr hohem Rechenaufwand möglich
- Schützt gegen Bruce-Force-, Known-Plaintext-, Replay-, Man-in-the-Middle-, Sniffing-, IP-Spoofing und IP-Hijacking- (ab v3.0) Angriffe

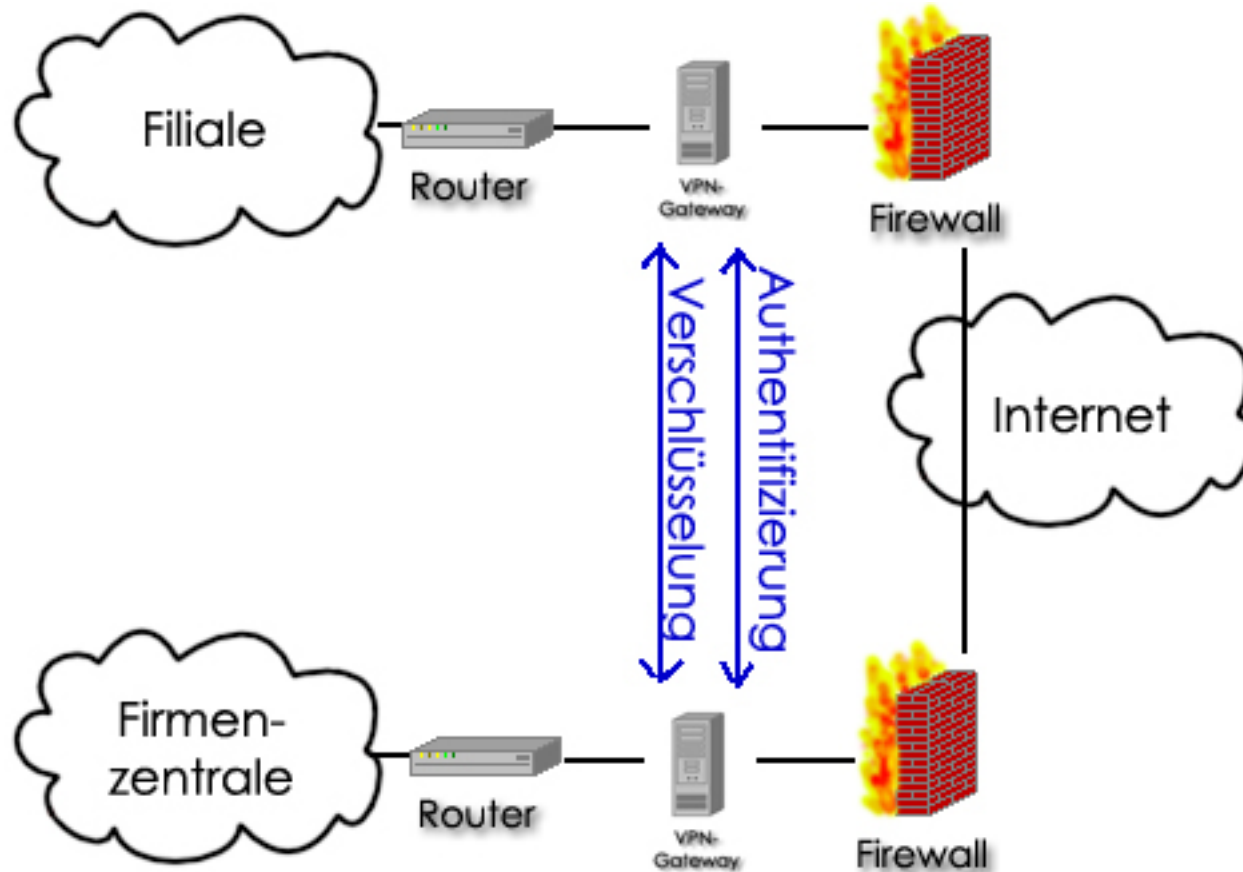
Virtual Private Networks - Gliederung

- 1) Einleitung
 - Betriebswirtschaftlicher Hintergrund
 - Begriffsabgrenzung
 - Anforderungen an VPN
- 2) Sicherheitskonzept für VPNs
- 3) Netzwerkkarchitektur
 - Aufbau eines VPN,
 - VPN und Firewalls,
 - VPN-Typen
 - VPN-Szenarien
- 4) Implementation eines gesicherten Übertragungskanal
 - Tunneling
 - L2F, L2TP, PPTP
 - IPSEC
 - SSL
- 5) **Schlussbetrachtung**

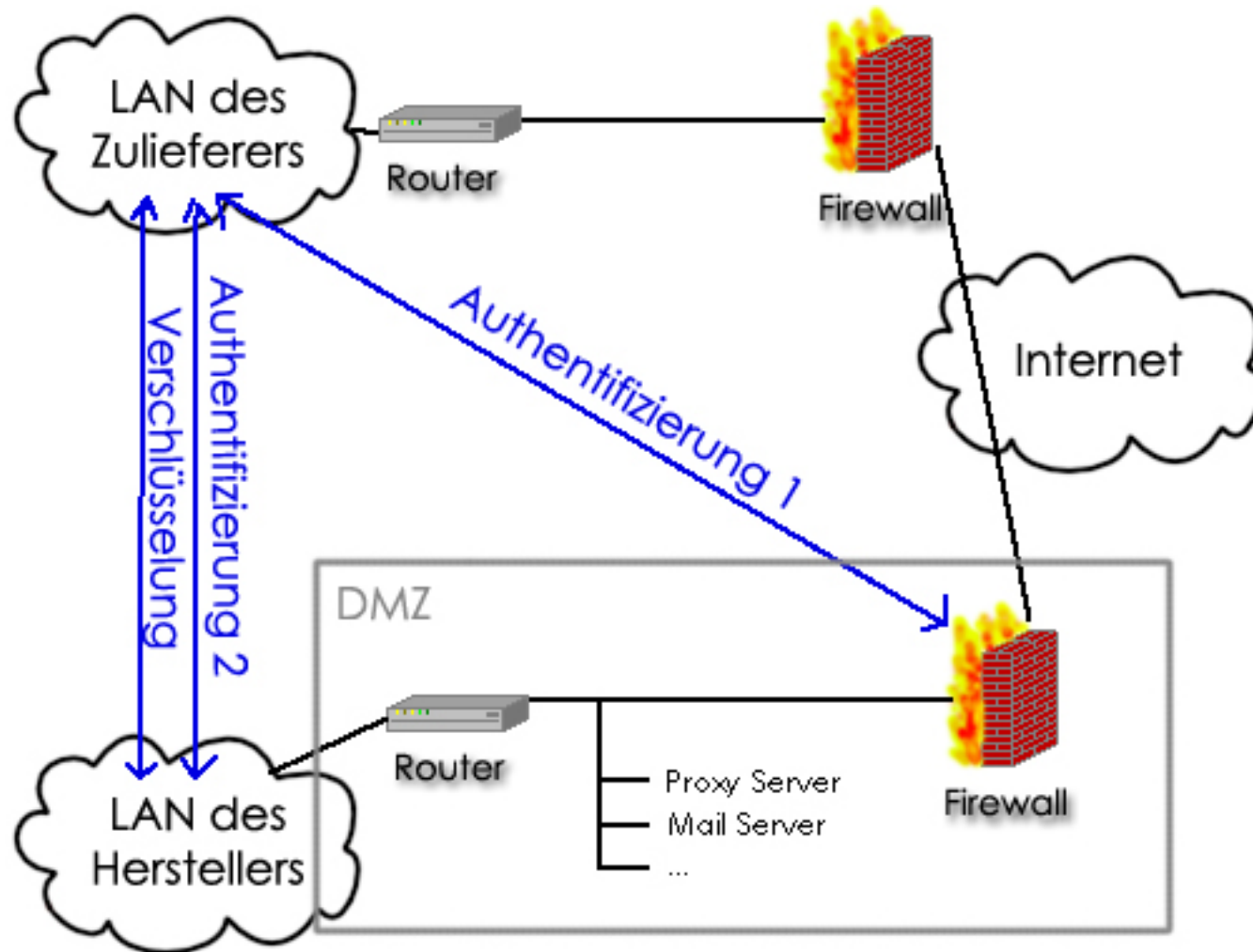
Schlussbetrachtung – Vergleich Layer 2 / 3

Eigenschaft	PPTP	L2TP	IPSec	L2Sec
Nutzer-Authentifizierung	Ja	Ja	Nein	Ja
NAT-Support	Ja	Ja	Nein	Ja
Multiprotokollfähigkeit	Ja	Ja	Nein	Ja
Dynamische Zuweisung von Tunnel-IP-Adressen	Ja	Ja	N/A	Ja
Verschlüsselung	begrenzt	Nein	Ja	Ja
PKI	Nein	Nein	Ja	Ja
Authentizitätsprüfung von Paketen	Nein	Nein	Ja	Ja
Überprüfung von Multicasts	Ja	Ja	Nein	Ja

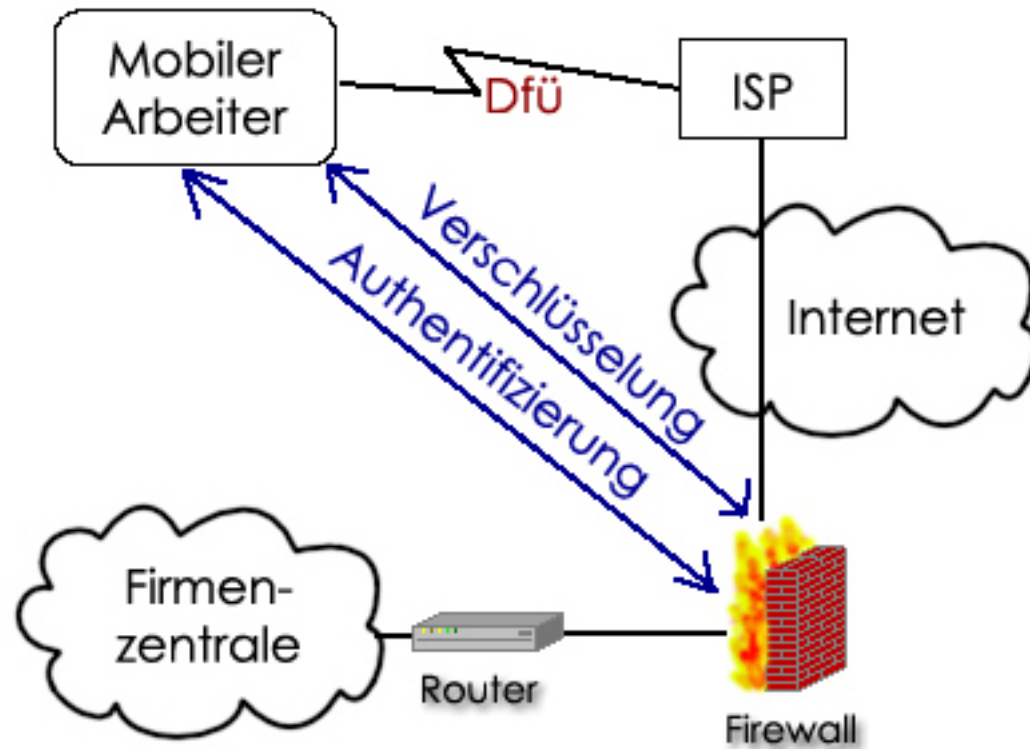
Schlussbetrachtung – Intranet-VPN



Schlussbetrachtung – Extranet-VPN



Schlussbetrachtung – Remote-Access-VPN



Literatur

- Böhmer, W.: „VPN – Virtual Private Networks; Die reale Welt der virtuellen Netze“, Carl Hanser Verlag, 1. Auflage, 2002
- Counterpane: N. Ferguson, B. Schneier: “A Cryptographic Evaluation of IPsec”, 1999, www.counterpane.com/ipsec.pdf
- C. R. Davis: „IPSec : Securing VPNs“, Osborne/McGraw-Hill, 1. Auflage, 2001
- Gerbich S., <http://www.informationweek.de/channels/channel05.htm>
- IETF, Request For Comments, Nummer xx, <http://www.ietf.org/rfc.html>
- Northcutt et al., S. Northcutt, L. Zeltser, S. Winters, K. K. Frederik, R. W. Ritchey: “Inside Network Perimeter Security”, New Riders, 1. Auflage, Juli 2002
- M. Mariach, E. Hofmann, I. Tsalman: „Kryptographische Verfahren“, Vortrag im Seminar „Sicherheit in vernetzten Systemen“, WS 2002/03, FB Informatik, Uni Hamburg
- Oppliger, Rolf: IT-Sicherheit. Vieweg Verlag, 1997.