Netzwerksicherheit

“Transilvania” Universität aus Brasov

Inhaltsverzeichnis

- Netzwerksicherheit
- Virtual Private Network

Kapitel

1. Netzwerksicherheit
2. OSI-Schichten und Netzsicherheit
3. RADIUS
4. Sicherheitstechniken

Kap. 1 Netzwerksicherheit

- Einfühung
- Virtual Private Network(VPN)
- VPN Tunneling
- Vorteile des VPN-Tunnelings
- Unterscheidungen von IP-VPNs

Einführung

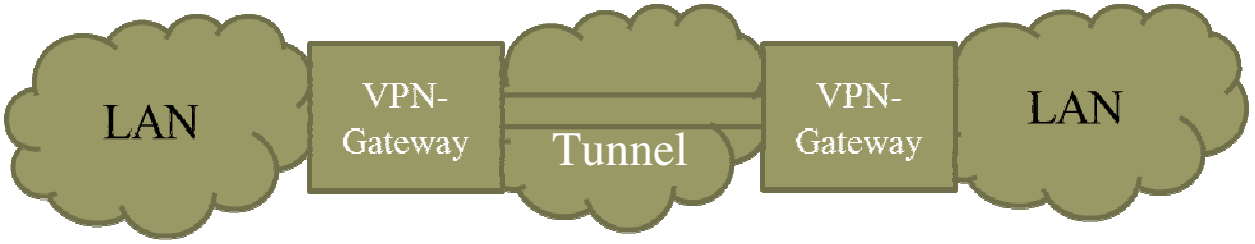
- Situation: Kommunikation zwischen unterschiedlich geschützten Rechnernetzen:
  1) Lokale geschützte Rechnernetze
  2) Ungeschützte Weitverkehrsnetze
  3) Weltweite Kommunikation über kostengünstige offene IT-Systeme
  4) Fernzugriff auf Rechner in geschützten und ungeschützten Bereichen
- Ziel: Sichere Kommunikation in einem logischen Netz

Virtual Private Network(VPN)

- Provides secure data transfer between two or more private or trusted network (bridge net)
- Emulates a point-to-point private link over an untrusted bridge net as a virtual private network (Homogenous Principe)

Virtual Private Network(VPN)(2)

- The data being sent is encapsulated with a header to traverse the bridge net between the two tunnel endpoints (Tunnel Principe)



- Maintains the security conditions of the corporate LAN to other LANs (Branch offices, Partner corporations) or Remote Workers using a dial-up connection to the local ISP across the Internet

VPN Tunneling

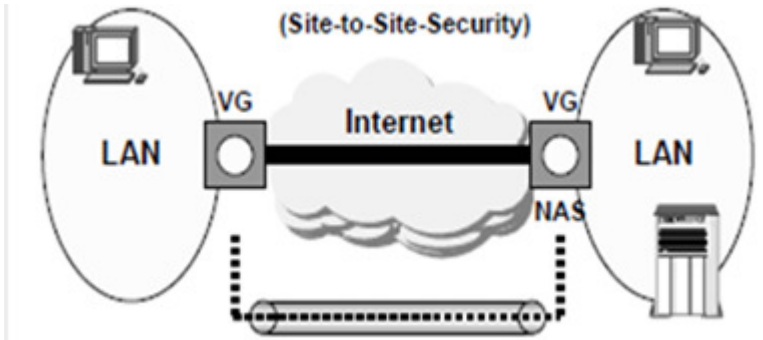
- Encapsulation: Frames or packets of a protocol to be securely transferred over a bridge net are encapsulated in an additional header (tunnel header) at the tunnel start point (VPN client, VPN-Gateway)
- Routing: The tunnel header contains routing and security information (encryption, authentication parameters) such as the IP addresses of the tunnel start and end point
- Decapsulation: Reaching the tunnel endpoint (VPN server) the frames are decapsulated and forwarded to its final destination

VPN Tunneling(2)

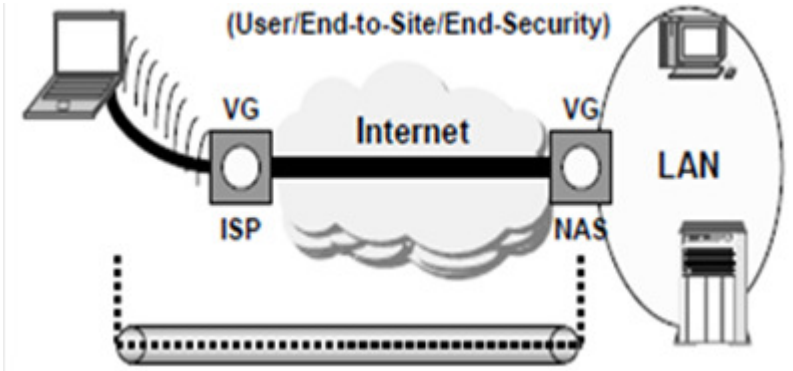
- Tunneling technology can be used on Layer 2 (data-link layer with frames) or/and Layer 3 (network layer with packets) of the OSI reference model
- Network Security Protocols offer different features and are categorized in:
  1) Layer 2 tunneling protocol: PPTP, L2TP (based on PPP which is used between a dial-up client and a NAS)
  2) Layer 3 tunneling protocol: IPSec with IKE

VPN Tunneling(3)

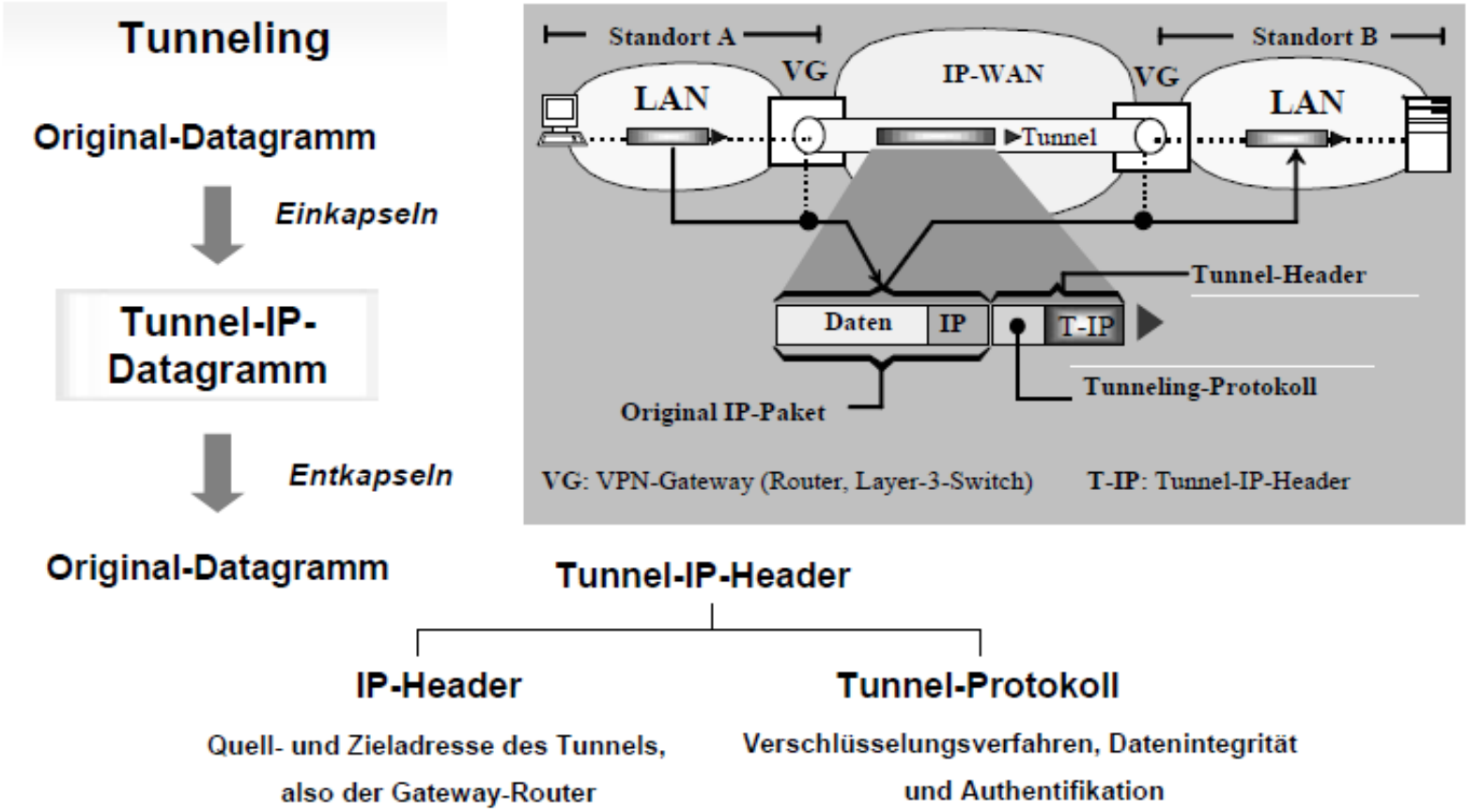
- Arten von VPN-Tunneling:
  1) Gateway-to-Gateway-VPN



  1) Client-to-Gateway-VPN



VPN Tunneling(4)



Vorteile des Tunnelings

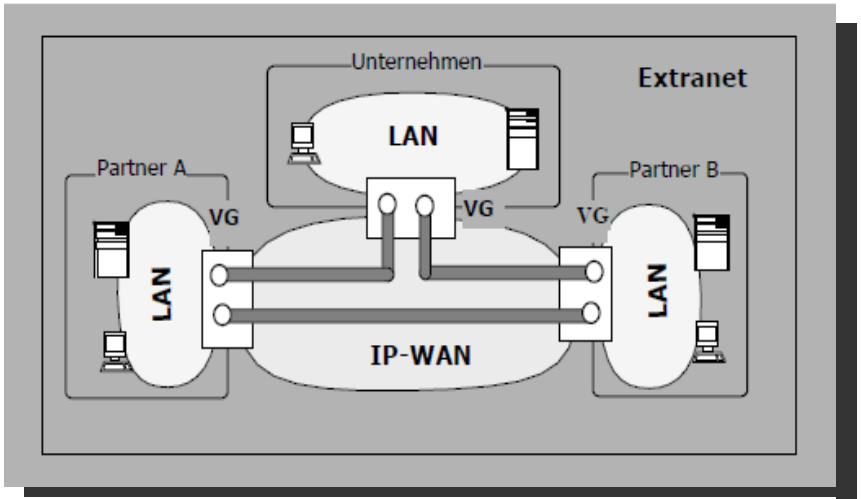
- Extranet Access: sichere Kommunikation mit Kunden usw.
- Intranet Access: Vernetzung einer Unternehmen zu einem virtuellen Netz, Remote Access
- Sichere Punkt-zu-Punkt-Verbindung durch Tunneling: keine Verkehrsflussanalysen, Kapselung bzw. Entkapselung erfolgen in den Endpunkten

Unterscheidungen von IP-VPNs

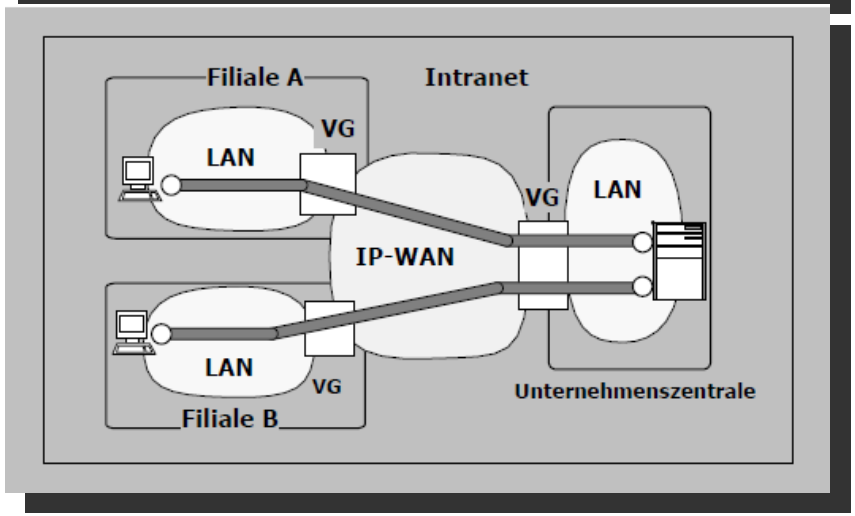
- Öffentliches IP-VPN: VPN auf Basis des öffentlichen Internets; IPSec als Sicherheitsprotokoll für Tunneling; kein Quality of Service (QoS) möglich
- Privates IP-VPN: VPN auf Basis eines privaten Provider-IP-Weitverkehrnetzes; Multi Protocol Label Switching (MPLS) als Routingverfahren, wobei nur der absendende Router den vollständigen Weg zur Zieladresse kennt; QoS möglich (IP-Adresse Priorisierung)

Unterscheidungen von IP-VPNs(2)

- Site-to-Site VPN

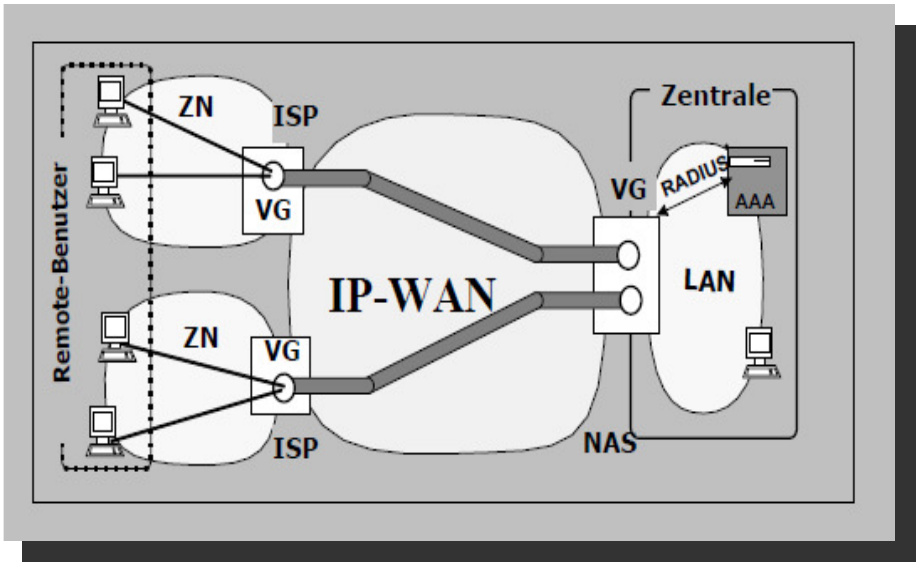


- End-to-End VPN



Unterscheidungen von IP-VPNs(3)

- Remote-Access-VPN



Kap. 2 OSI-Schichten und Netzsicherheit

- OSI-Schichten
- Verschlüsselungsarten
- VPN L2TP Tunneling
- IP-Datagram
- VPN IPSec Tunneling
- VPN L2TP/IPSec Tunneling
- VPN-Sicherheitsfunktionen der Netzwerkprotokolle

OSI-Schichten

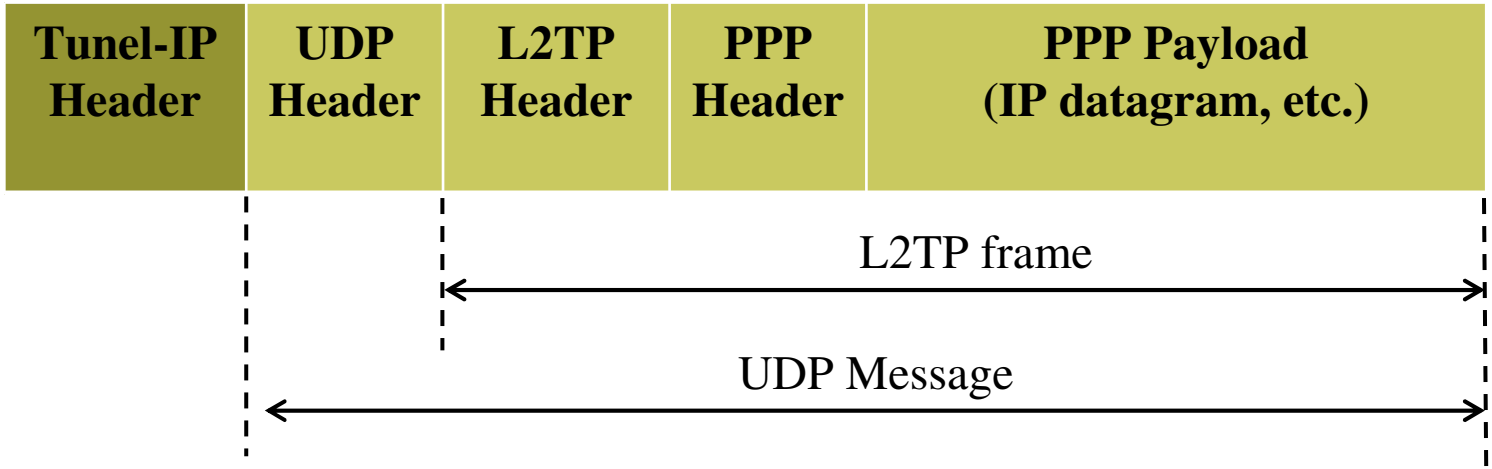
Schicht	Sicherheitsprotokolle
7 Application Layer	PGP; SET; S-MIME; S-HTTP
6 Presentation Layer (Präsentationsschicht)	
5 Session Layer (Sitzungsschicht)	SSL/TLS; SSH; IKE ;WTLS
4 Transport Layer (Transportschicht)	IPSec (AH, ESP)
3 Network Layer (Netzwerkschicht)	PAP; CHAP; EAP; PPTP; L2TP
2 Data Link Layer (Sicherrungsschicht)	MAC addr. filtering
1 Physical Layer (Bitübertragungsschicht)	

Verschlüsselungsarten

Verbindungsverschlüsselung	End-to-End-Verschlüsselung
• auf den Schichten 1 und 2 • Nutzdaten in Netzknoten als Klartext • transparent für Benutzer und Anwendungen • Verschlüsselung der Pakete unabhängig von Anwendung, Dienst bzw. Benutzer; nur gemeinsamer Schlüssel • Authentifikation nur von Systemen, aber nicht Prozesse bzw. Benutzer • u.a. PPTP, L2TP, EAP	• auf den Schichten 3 und 4 • Nutzdaten in Netzknoten verschlüsselt • Anpassungen der Anwendungen mehr oder weniger notwendig • Verschlüsselung der Pakete differenziert nach Anwendung, Dienst bzw. Benutzer möglich; auch unterschiedliche Schlüssel verwendbar • Authentifikation von Systemen, Prozessen und Benutzern • u.a. IPSec, SSL/TSL, S-HTTP, SET, PGP

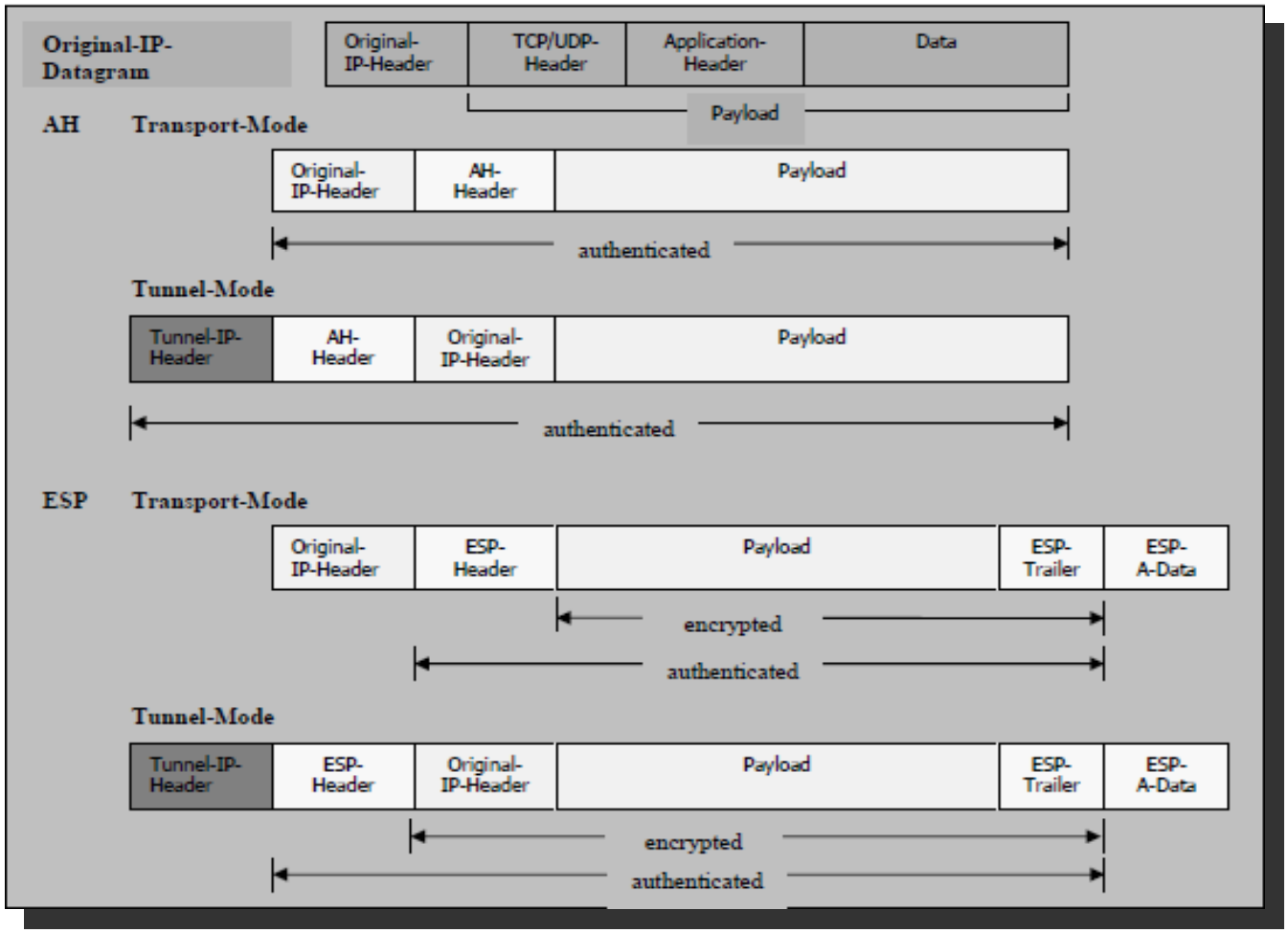
VPN L2TP Tunneling

- Ist ein Protokoll, das PPP-Frames kapselt und diese über IP, Frame Relay und ATM Networks sendet
- Erbt die PPP Verschlüsselungsvervahren (DES, Triple DES) und die PPP-Benutzerauthentifizierung-Mechanismen



L2TP Data Packet

IP-Datagram


Original-IP-Datagram
Original-IP-Header
TCP/UDP-Header
Application-Header
Data
Payload
AH
Transport-Mode
Original-IP-Header
AH-Header
Payload
authenticated
Tunnel-Mode
Tunnel-IP-Header
AH-Header
Original-IP-Header
Payload
authenticated
ESP
Transport-Mode
Original-IP-Header
ESP-Header
Payload
ESP-Trailer
ESP-A-Data
encrypted
authenticated
Tunnel-Mode
Tunnel-IP-Header
ESP-Header
Original-IP-Header
Payload
ESP-Trailer
ESP-A-Data
encrypted
authenticated

VPN L2TP Tunneling (2)

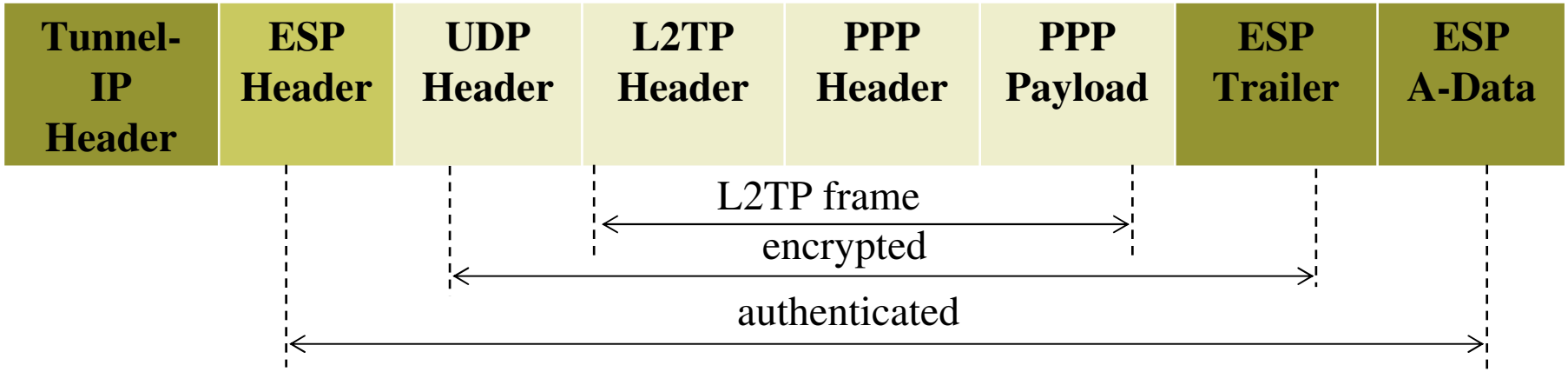
- Tunneling ab ISP
  1) Sender kapselt IP-Pakete mit der Adresse des Ziel-Hosts in PPP-Frames und sendet diese über eine PPP-Verbindung (u.a. ISDN) zum ISP
  2) Der ISP kapselt die PPP-Frames in L2TP Pakete und sendet diese über UDP/IP (Port 1701) zu dem NAS des Ziel-LANs, wo sie entpackt und dem Ziel-Host zugesandt werden
- Tunneling ab Client
  1) Sender kapselt IP-Pakete in PPP-Frames und diese in L2TP-Pakete
  2) Verschicken der L2TP-Packete direkt zum NAS bzw. Ziel-Host

VPN IPSec Tunneling

- IPSec arbeitet bei der Netzwerkschicht
- Ist eine offene Standard der Internet Engineering Task Force (RFC 2401)
- Bietet Sicherheitsdienste (Erweiterungen des IPv4-, IPv6 enthalten): Verschlüsselung mit schnelle Schlüsselsitzung, Systemautentifizierung, Datenintegrität
- Sicherheitsprotokolle: Authentication Header Protocol (AH) und Encapsulating Security Payload Protocol (ESP)
- Benötigt stabile Security Associations (SA), um die Daten durch Tunnel auszutauschen

VPN L2TP/IPSec Tunneling

- Weil L2TP Nachteile hat, dann kann man eine Kombination aus beidem verwenden
- VPN L2TP/IPSec ist eine Implementierung des L2TP Protokolls, die IPSec verwendet, um L2TP Verkehr zu schützen
- Sicherheitsfunktionen durch eine Sicherheitspolitik gesteuert



L2TP/IPSec ESP Data Packet (Transport Mode)

VPN-Sicherheitsfunktionen der Netzwerkprotokolle

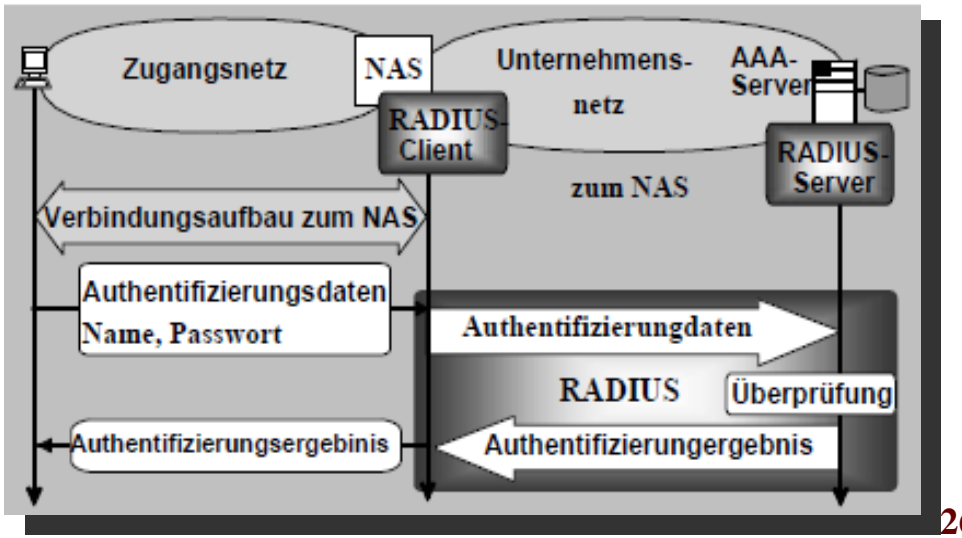
Feature	Network Security Protocol				
	PPTP/ PPP	L2TP/ PPP	IPSec Transport	IPSec Tunnel	L2TP/ IPSec
User Authentication	X	X			X
Machine Authentication			X	X	X
Confidentiality	X	X	X	X	X
Data Packet Authentication			X	X	X
PKI	X	X	X	X	X
NAT Compatibility	X	X			
Multi-protocol	X	X			X
Multicast Support	X	X		X	X

Kap. 3 RADIUS

- Kurze Bemerkungen

Kurze Bemerkungen

- Das Protokoll RADIUS funktioniert nach dem Client/Server-Konzept und legt die Kooperation zwischen einem NAS und einem AAA-Server fest. Der RADIUS-Server kann als ein AAA-Server gesehen werden, in dem sämtliche Informationen über Remote-Benutzer zur Verfügung stehen. Der RADIUS-Client stellt ein Funktionsmodul dar, das auf dem NAS installiert wird.



Kap. 4 Sicherheitstechniken

- Sicherheitstechnik im Internet
- Sicherheitstechnik in Mobilfunknetze

Sicherheitstechnik im Internet

- Secure Socket Layer (SSL)
- Sichere Übertragung von Web-Informationen
  1) Verbindungsaufbau und Authentisierung (RSA)
  2) Aushandlung der kryptographischen Methoden
  3) Schlüsselaustausch (RSA, DH)
  4) Datenaustausch (DES, IDEA)
  5) Integrität (MD5, SHA)
  6) USA-Produkte nur mit 40-Bit DES-Schlüssel

Sicherheitstechnik in Mobilfunknetze

- Wireless Transport Layer Security (WTLS)
- Sichere Übertragung von WAP-Transaktionen
  1) Verbindungsaufbau und Authentisierung (RSA, PIN)
  2) Aushandlung der kryptographischen Methoden
  3) Schlüsselaustausch (RSA,EC-DH)
  4) Datenaustausch (3DES, IDEA)
  5) Integrität (MAC-SHA)