Securitatea retelelor

Universitatea “Transilvania” din Brasov

Cuprins

- Securitatea retelelor
- Retele virtuale private

Capitole

1. Securitatea retelelor
2. Nivelurile OSI si securitatea retelelor
3. RADIUS
4. Tehnici de securitate

Cap. 1 Securitatea retelelor

- Introducere
- Retele virtuale private (VPN)
- VPN Tunneling
- Avantajele VPN Tunneling
- Tipuri de IP-VPN

Introducere

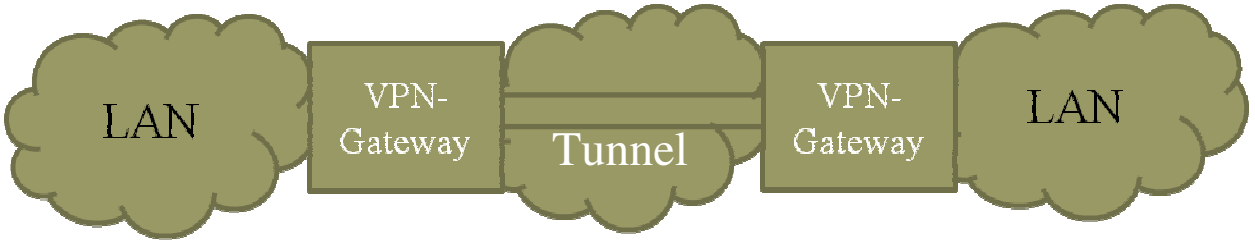
- Situatie: Comunicarea intre diferite retele de calculatoare:
  1) retele de calculatoare locale protejate
  2) retelele de arie larga neprotejate
  3) comunicare la nivel mondial prin sisteme IT deschise si low-cost
  4) acces de la distanta la calculatoare din domenii protejate si neprotejate
- Scop: Comunicare sigura intr-o retea logica

Retele virtuale private (VPN)

- Furnizeaza transferul de date sigur intre doua sau mai multe retele private sau de incredere (bridge net)
- Simuleaza o legatura privata peste un bridge net care nu este de incredere, ca o retea privata virtuala (Principiul omogenitatii)

Retele virtuale private (VPN)(2)

- Data care se trimite este incapsulata cu un antet pentru a traversa bridge net-ul intre doua tunele endpoint (Principiul tunelului)



- Mentine conditiile de securitate din reteaua LAN a companiei altor retele LAN (filiale, corporatii partenere) sau lucratorilor de la distanta, folosind o conexiune dial-up la ISP-ul local, prin intermediul intrnetului

VPN Tunneling

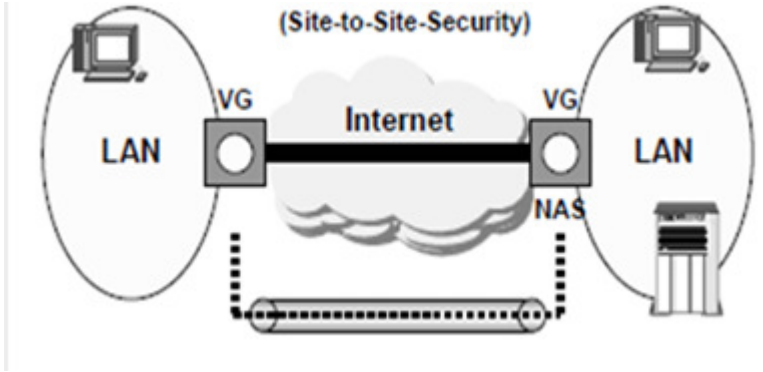
- Incapsulare: Cadre sau pachete dintr-ul protocol care urmeaza sa fie transferat printr-un bridge net sunt incapsulate intr-un antet aditional (antet tunel) la punctul de start al tunelului (Client VPN, Poarta VPN)
- Routare: Antetul tunel contine informatii de routare si securitate (criptare, parametrii de autentificare), cum ar fi adresele IP de la inceputul si capatul tunelului
- Decapsulare: Atunci cand ajung la capatul tunelului (serverul VPN), cadrele sunt decapsulate si transmise la destinatia finala

VPN Tunneling(2)

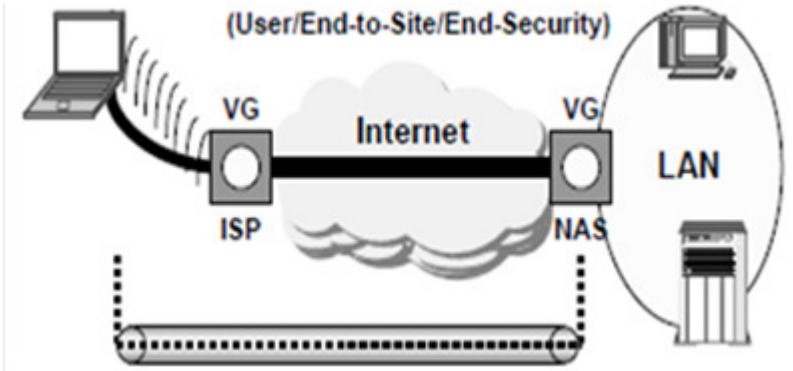
- Tehnologia pentru tunneling poate fi folosita pe stratul 2 (data link layer cu cadre) si/sau stratul 3 (network layer cu pachete) al modelului de referinta OSI
- Protocoalele de securitate a retelelor ofera caracteristici diferite si sunt clasificate in:
  1) Layer 2 tunneling protocol: PPTP, L2TP (bazat pe PPP, care este folosit intre un client dial-up si NAS
  2) Layer 3 tunneling protocol: IPSec cu IKE

VPN Tunneling(3)

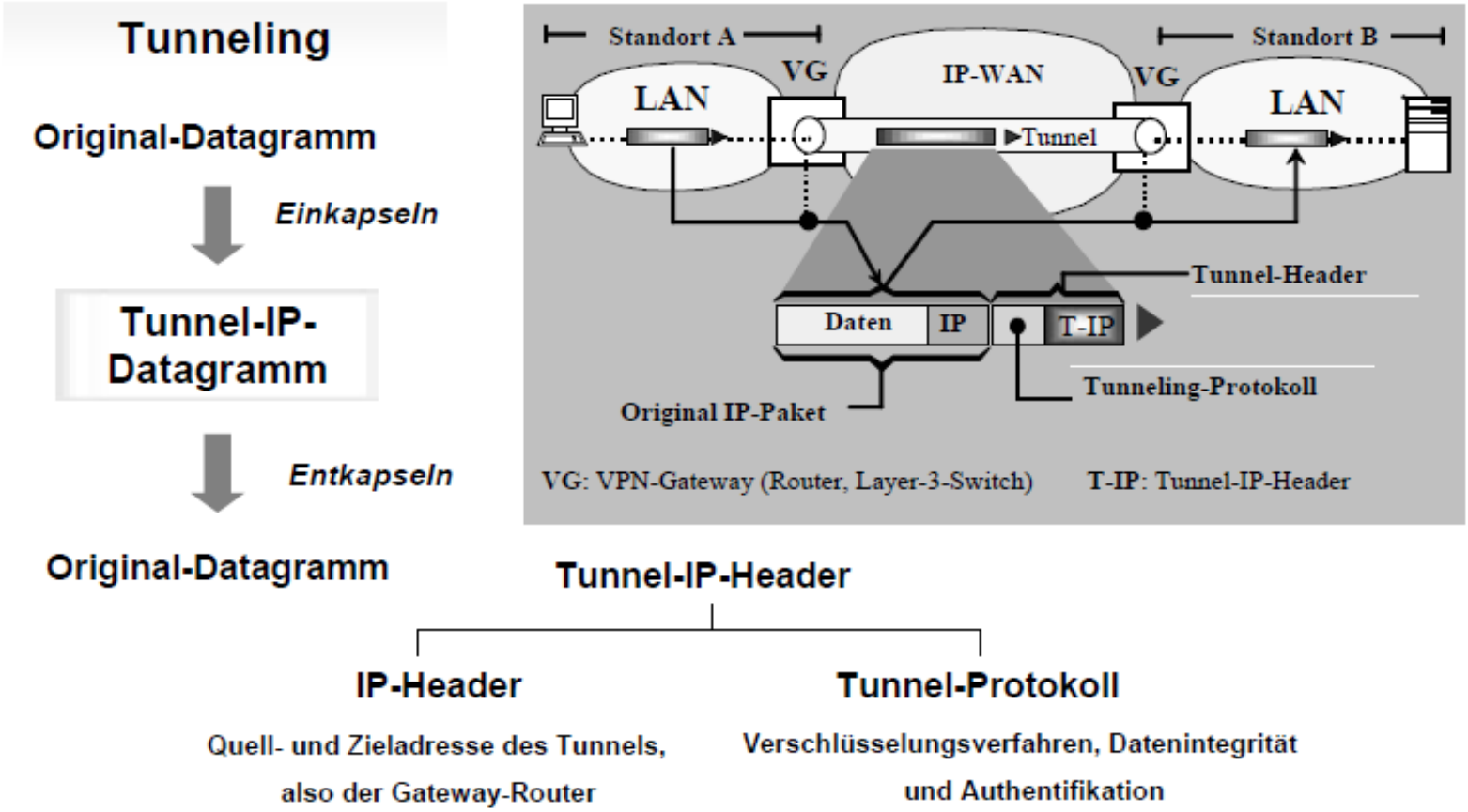
- Tipuri de tunneling VPN:
  1) Gateway-to-Gateway-VPN



  1) Client-to-Gateway-VPN



VPN Tunneling(4)



Avantajele VPN Tunneling

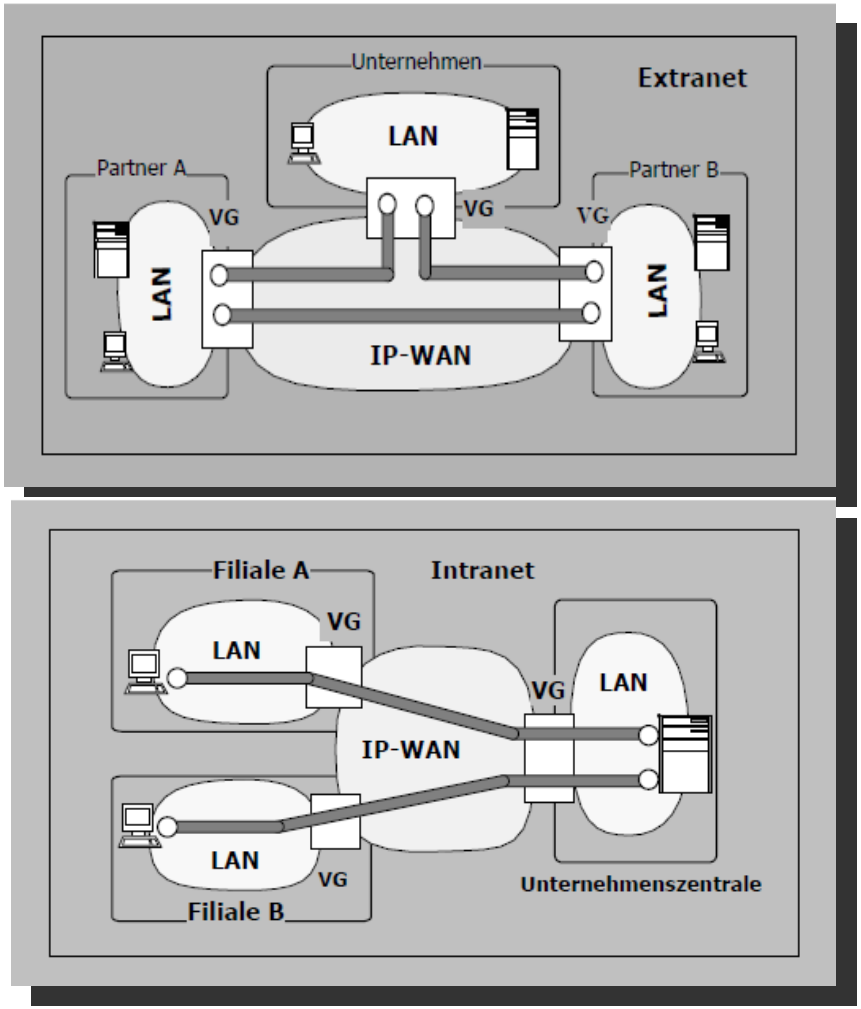
- Acces extranet: comunicare sigura cu clientii, partenerii, furnizorii
- Acces intranet: Conectarea unei companii la o retea virtuala, acces la distanta
- Conexiune point-to-point sigura prin tunneling: fara analiza fluxului de trafic, incapsularea si decapsularea au loc in end-points

Tipuri de IP-VPN

- IP-VPN deschise: retele virtuale private pe baza internetului deschis; IPSec ca si protocol de securitate pentru tunneling; nu este posibila Quality of Service (QoS)
- IP-VPN private: retele virtuale private pe baza unui furnizor de IP pentru retele wide-area; Multi Protocol Label Switching (MPLS) ca proces de routare, unde doar routerul initial cunoase drumul complet al adresei tinta; este posibila Quality of Service (QoS) prin prioritizarea adreselor IP

Tipuri de IP-VPN(2)

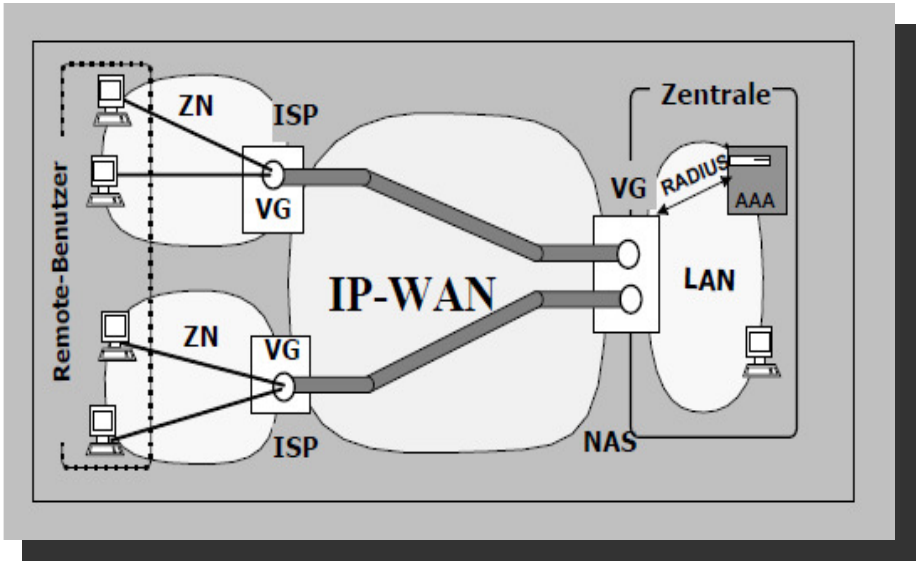
- Site-to-Site VPN



- End-to-End VPN

Tipuri de IP-VPN(3)

- Remote-Access-VPN



Cap. 2 Straturile OSI si securitatea retelelor

- Straturile OSI
- Tipuri de criptare
- VPN L2TP Tunneling
- IP-Datagram
- VPN IPSec Tunneling
- VPN L2TP/IPSec Tunneling
- Functiile de securitate VPN ale protocoalelor de retea

Straturile OSI

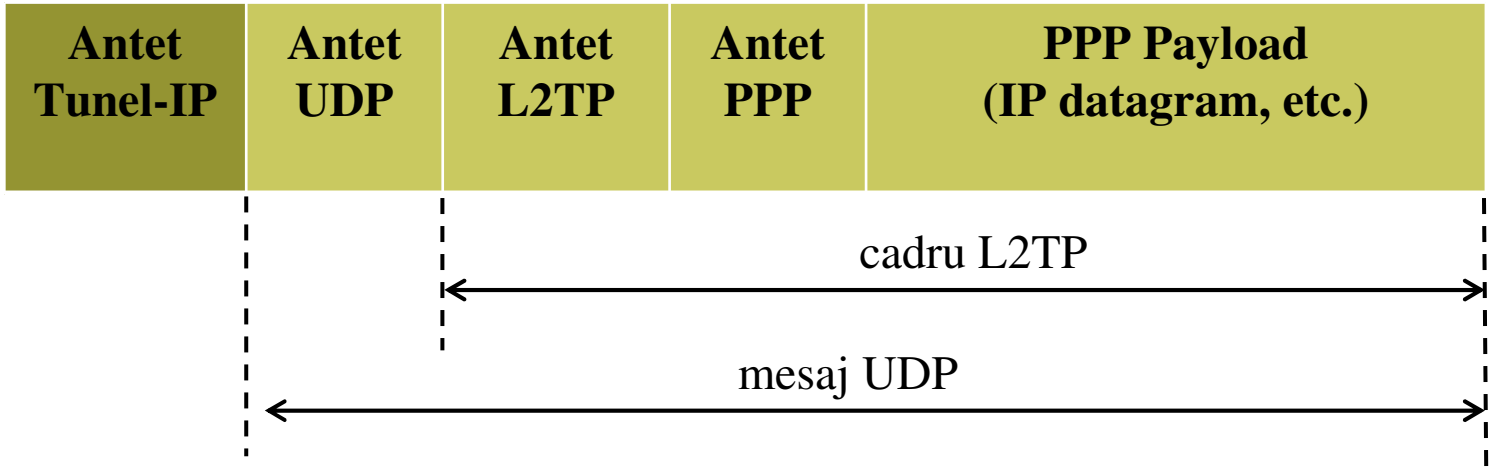
Strat	Protocol de securitate
7 Application Layer (Stratul de aplicatie)	PGP; SET; S-MIME; S-HTTP
6 Presentation Layer (Stratul de prezentare)	
5 Session Layer (Stratul de sesiune)	SSL/TLS; SSH; IKE ;WTLS
4 Transport Layer (Stratul de transport)	IPSec (AH, ESP)
3 Network Layer (Stratul de retea)	PAP; CHAP; EAP; PPTP; L2TP
2 Data Link Layer (Stratul de siguranta)	MAC addr. filtering
1 Physical Layer (Stratul de transmitere a bitilor)	

Tipuri de criptare

Criptare de legatura	Criptare End-to-End
• Pe straturile 1 si 2 • Datele in noduri de retea ca text clar • Transparenta pentru utilizator si aplicatie • Criptarea pachetelor este independenta de aplicatie, serviciu sau utilizator; doar cheie comuna • Autentificarea doar a sistemelor, nu si a proceselor sau a utilizatorilor • Altele: PPTP, L2TP, EAP	• Pe straturile 3 si 4 • Datele incapsulate in noduri de retea • Mai mult sau mai putin necesara acomodarea cu aplicatia • Este posibila criptarea diferentiata a pachetelor, dupa aplicatie, serviciu sau utilizator; pot fi folosite chei diferite • Autentificarea sistemelor, proceselor si a utilizatorilor • Altele: IPSec, SSL/TSL, S-HTTP, SET, PGP

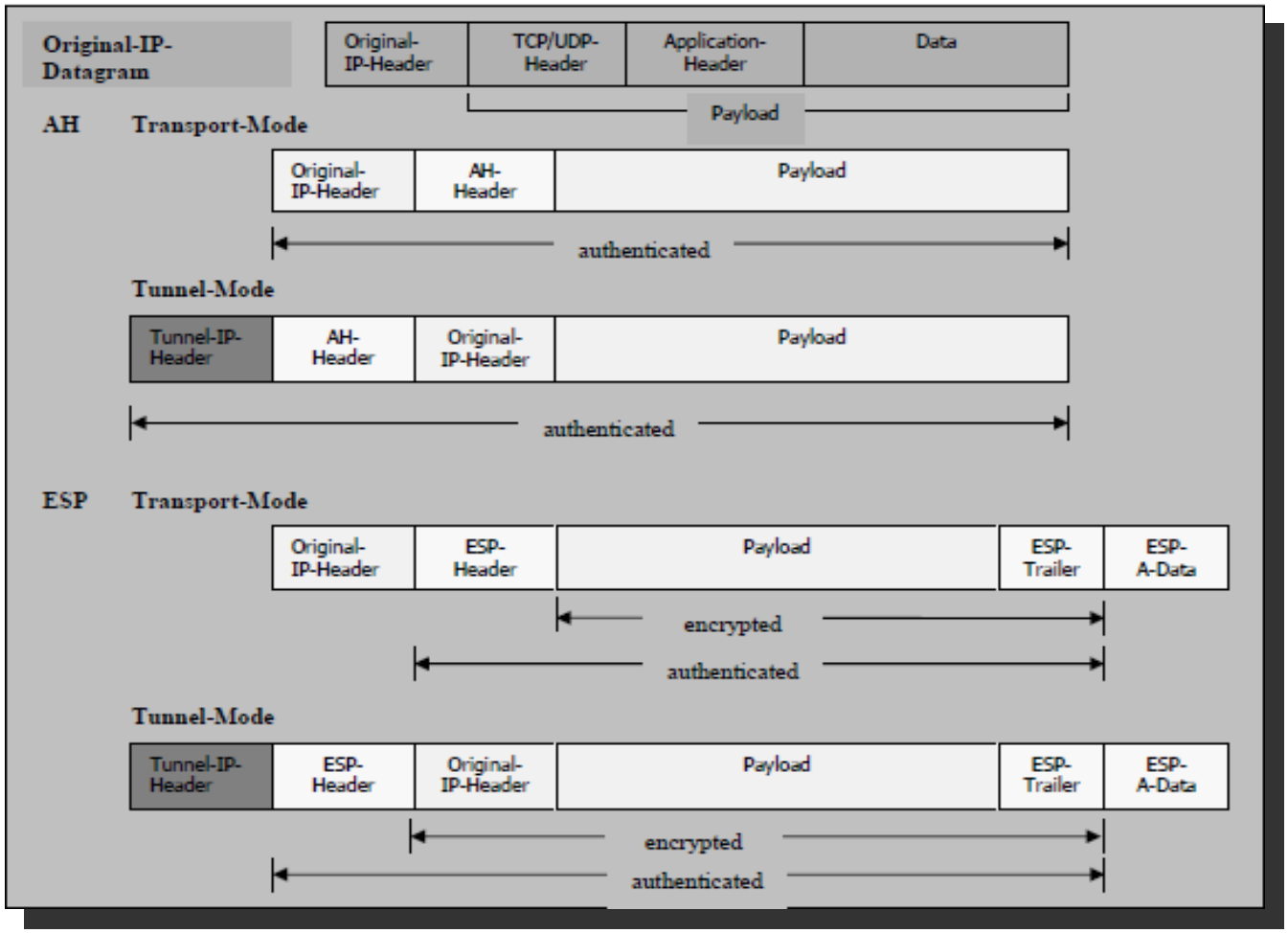
VPN L2TP Tunneling

- Este un protocol care incapsuleaza cadrele PPP si le trimite prin IP, Frame Relay si retele ATM
- Mosteneste metodele de criptare PPP (DES, triplu DES) si mecanismele PPP de autentificare a clientilor



Pachet de date L2TP

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)

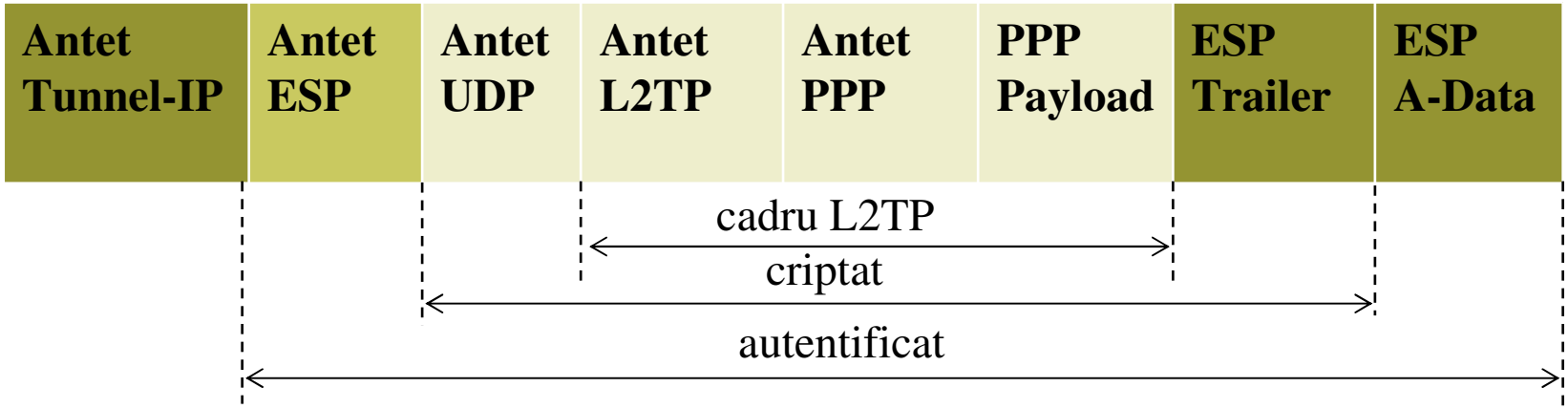
- Tunneling de la ISP
  1) Emitatorul incapsuleaza pachetele IP cu adresa hostului tinta in cadre PPP si le trimite printr-o conexiune PPP (sau ISDN) catre ISP
  2) ISP incapsuleaza cadrele PPP in pachete L2TP si le trimite prin UDP/IP (Port 1701) catre NAS al LAN-ului tinta, unde vor fi decapsulate si trimise la host-ul tinta
- Tunneling de la client
  1) Emitatorul incapsuleaza pachetele IP in cadre PPP, iar cadrele in pachete L2TP
  2) Trimiterea pachetelor L2TP direct catre NAS, in special host-ul tinta

VPN IPSec Tunneling

- IPSec lucreaza la stratul de retea (3)
- Este un standard deschis al Internet Engineering Task Force (RFC 2401)
- Ofera servicii de securitate (extensii ale IPv4-, continute de IPv6): criptare cu sesiuni de cheie rapide, autentificarea in sistem, integritatea datelor
- Protocoale de securitate: Authentication Header Protocol (AH) si Encapsulating Security Payload Protocol (ESP)
- Necesita Security Associations (SA) stabile, pentru a schimba date prin tunel

VPN L2TP/IPSec Tunneling

- Deoarece L2TP are dezavantaje, poate fi folosita o combinatie intre cele doua
- VPN L2TP/IPSec este o implementare a protocolului L2TP, care foloseste IPSec pentru a proteja traficul L2TP
- Functiile de securitate sunt controlate de o politica de securitate



Pachetul de date L2TP/IPSec ESP (modul transport)

Functiile de securitate VPN ale protocoalelor de retea

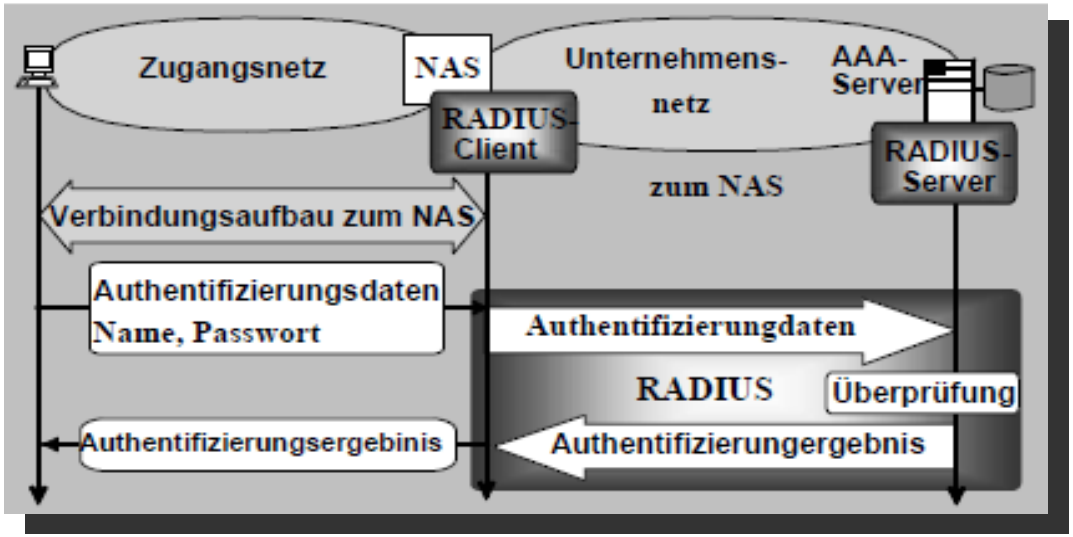
Trasatura	Protocol de securitate a retelei				
	PPTP/ PPP	L2TP/ PPP	IPSec Transport	IPSec Tunnel	L2TP/ IPSec
Autentificarea utilizatorului	X	X			X
Autentificarea aparatului			X	X	X
Confidentialitate	X	X	X	X	X
Autentificarea pachetului de date			X	X	X
PKI	X	X	X	X	X
Compatibilitate NAT	X	X			
Multi-protocol	X	X			X
Suport multicast	X	X		X	X

Cap. 3 Radius

- Scurte precizari

Scurte precizari

- Protocolul Radius functioneaza dupa conceptul Client/Server si stabileste cooperarea dintre un NAS si un server AAA. Serverul Radius poate fi vazut ca un server AAA, in care sunt disponibile informatiile complete despre utilizatorii la distanta. Clientul Radius reprezinta un modul functie, care va fi instalat pe NAS.



Cap. 4 Tehnici de securitate

- Tehnici de securitate in Internet
- Tehnici de securitate in retelele mobile

Tehnici de securitate in internet

- Secure Socket Layer (SSL)
- Transmitere sigura a informatiilor web:
  1) Conectare si autentificare(RSA)
  2) Negocierea metodelor criptografice
  3) Schimb de chei(RSA, DH)
  4) Schimb de date (DES, IDEA)
  5) Integritate (MD5, SHA)
  6) Produse USA doar cu cheie DES pe 40 de biti

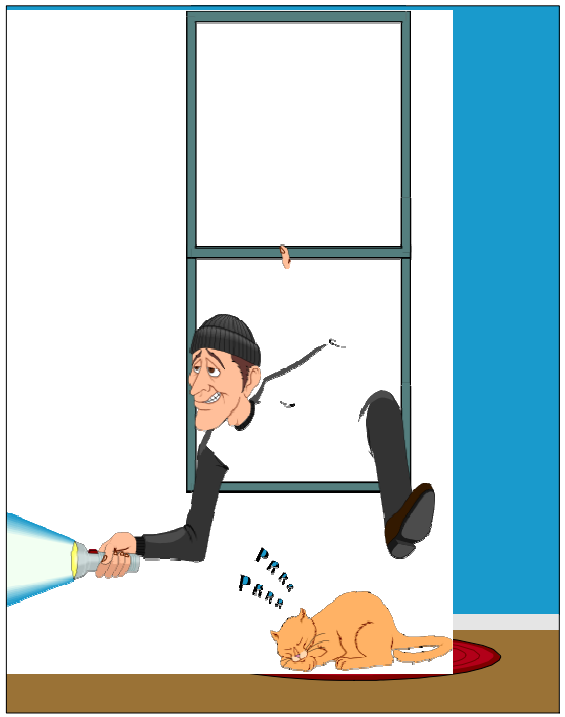
Tehnici de securitate in retelele mobile

- Wireless Transport Layer Security (WTLS)
- Transmitere sigura a tranzactiilor WAP
  1) Conectare si autentificare(RSA, PIN)
  2) Negocierea metodelor criptografice
  3) Schimb de chei(RSA,EC-DH)
  4) Schimb de date(3DES, IDEA)
  5) Integritate (MAC-SHA)

Recapitulare

IT Security

S E C U R I T A T E



Ce părere aveți?