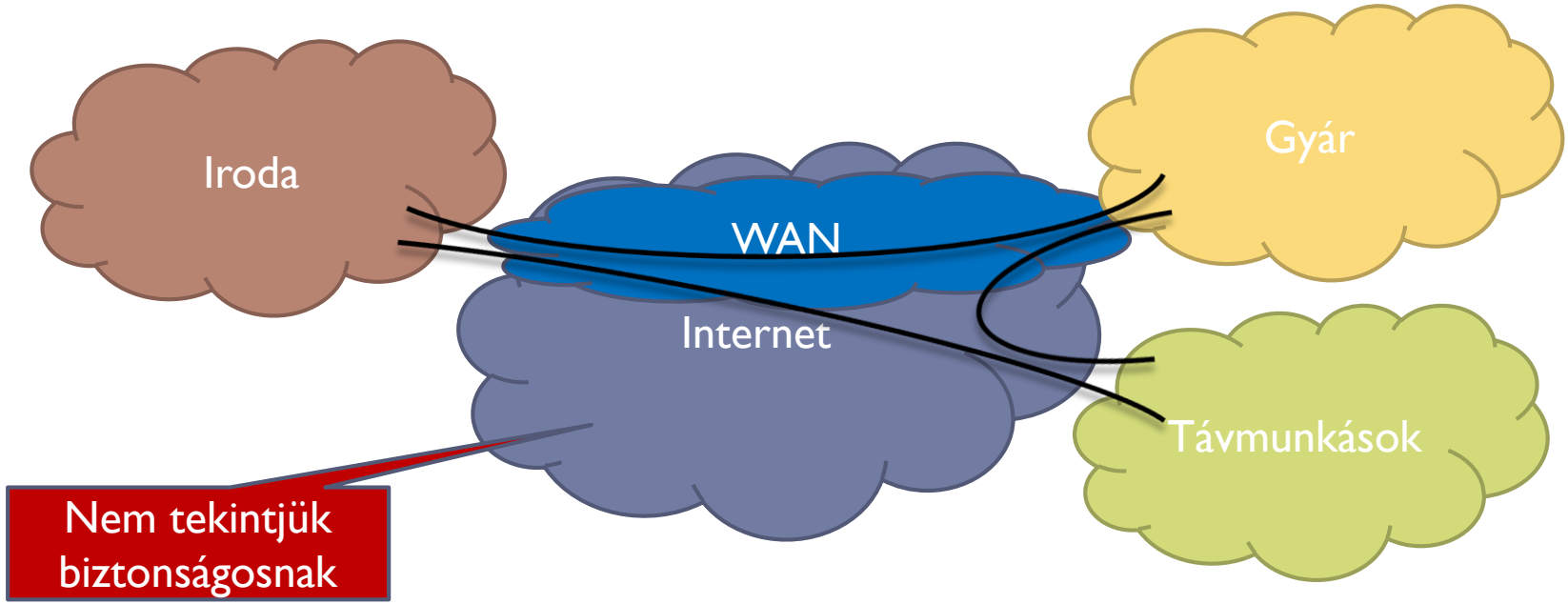
Virtuális magánhálózatok / VPN

Hálózatok összekapcsolása - tunneling

- Virtuális magánhálózatok / Virtual Private Network (VPN)



Virtuális magánhálózatok

- Telephelyek összekapcsolása
  - WAN (Wide Area Network)
  - Lehet elkülönítve az Internet forgalomtól
    - Kapcsolatminőségi védelem
    - De ettől még védeni kell a forgalmat
  - Nagyvállalati környezetben: WAN Edge
- Távmunkások bekapcsolása
  - Interneten keresztül lehetséges
  - Nagyvállalati környezetben: Internet Edge

Magánhálózat kialakítás

- Hálózat fizikai elkülönítése
  - Elkülönítésre alkalmas hálózati technológia alkalmazása
    - Bérelt vonal
    - Optikai kábel esetén különböző hullámhossz
- Adatcsomagok elkülönített irányítása
  - IP hálózatokban, adott szolgáltatón belül
    - Multiprotocol Label Switching – MPLS
      - A forgalom meg van címkézve, amint beér a hálózatba
      - A címkék rögzített útvonalon közlekednek
      - Opcionálisan erőforrás-foglalás is (Minőségi garancia)
- Elkülönítés titkosítással
  - IP szintű titkosítás
  - Adatkapcsolat szintű alagutak

Virtuális!

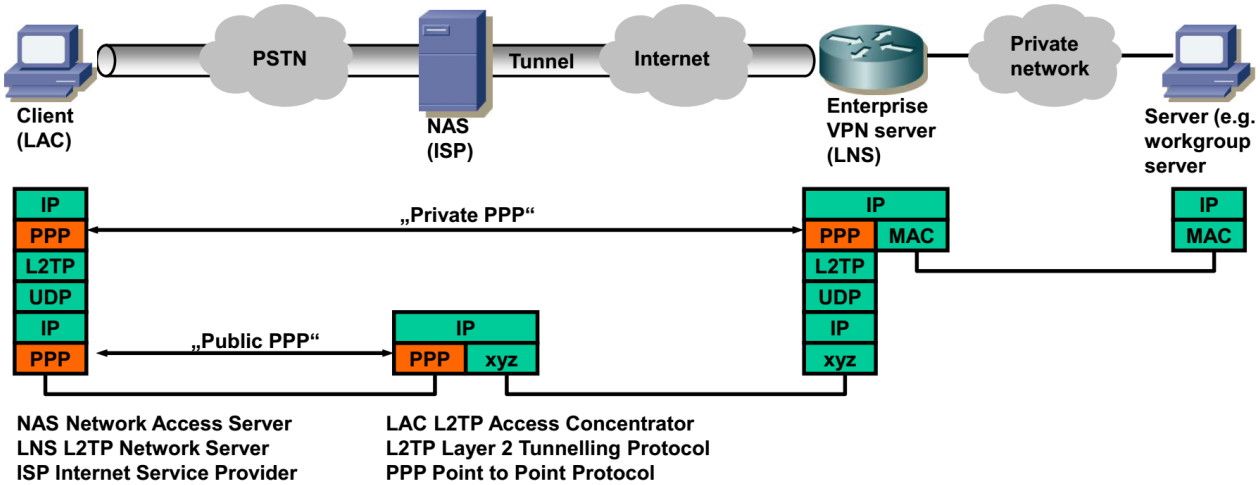
Gyakorlatban a legnagyobb biztonság

Elkülönítés titkosítással

- A magánhálózat adata a többi forgalommal együtt halad
- A titkosítás biztosítja, hogy illetéktelen személy nem férhet hozzá
  - Nem tudhatja meg tartalmát
  - Nem módosíthatja
  - Nem hozhat létre új (valós) csomagokat
  - De törölheti (rombolás)
- Nincsen prioritásos kezelés, nincs minőségi garancia
  - Best effort Internet
  - Más protokollokkal kiegészíthető
- Független a hordozó hálózat biztonságától

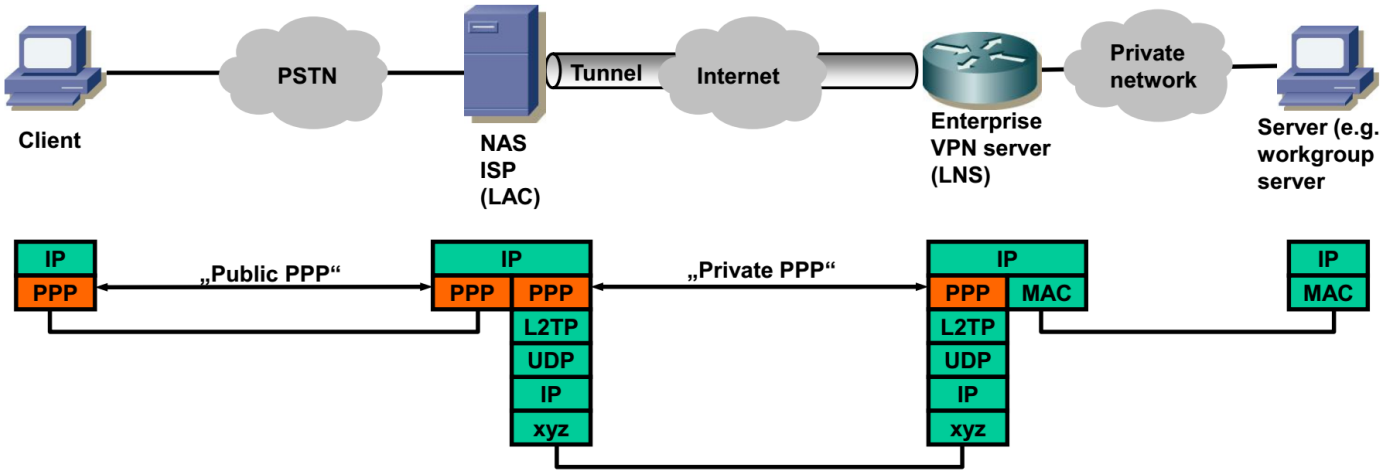
VPN típusok

- Kliens által indított VPN
  - A VPN kliens a felhasználó gépén
  - L2 tunneling, a felhasználó vállalati IP címet kap
  - A VPN felállításáról a felhasználó dönt



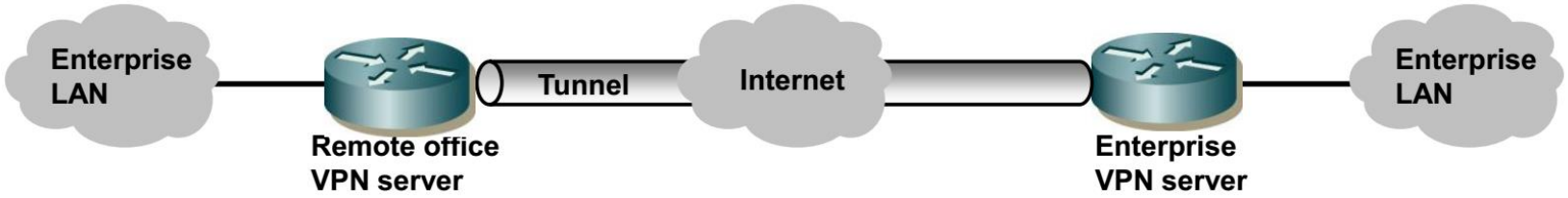
VPN típusok

- NAS által kezdeményezett VPN
  - A NAS a felhasználó számára indít VPN kapcsolatot
  - A hozzáférési rész nem védett!
  - A VPN felállításáról a NAS dönt



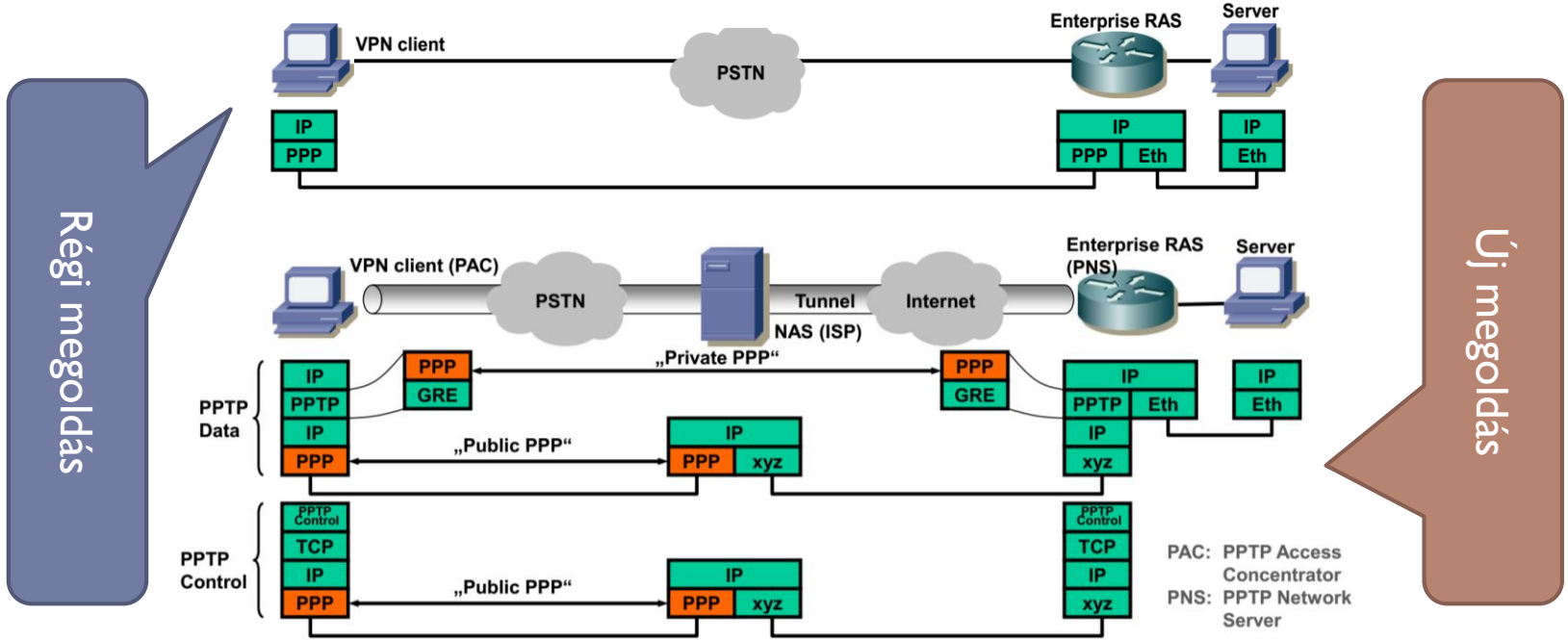
VPN típusok

- Intranet / Extranet VPN
  - A VPN egy tunnlet állít fel a két helyszín között
  - A két helyszín egy hálózatba kerül (L2 vagy L3 kapcsolat)



Tunneling protokollok - PPTP

- PPTP – Point to Point Tunneling Protocol (RFC2637)



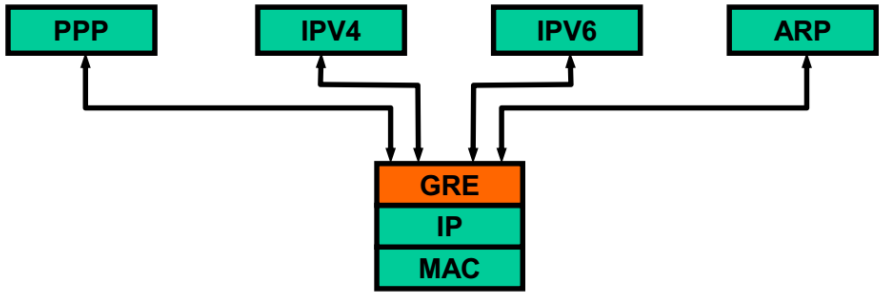
PPTP - Point to Point Tunneling Protocol

- PPTP
  - PPP: Point to Point Protocol
    - Hitelesítés (PAP, CHAP, MSCHAP, EAP), titkosítás és tömörítés
  - GRE: Generic Routing Encapsulation
    - Multiprotokoll beágyazás. Bármi (L2 és L3) átvihető, az alkalmazás számára teljesen transzparens
  - PPTP Control
    - A PPTP tunnel felállítására szolgál
    - TCP felett. Nincs védelem a protokoll számára.
  - A korai időszakban a legelterjedtebb VPN protokoll a kliens csatlakozására

GRE – Generic Routing Protocol

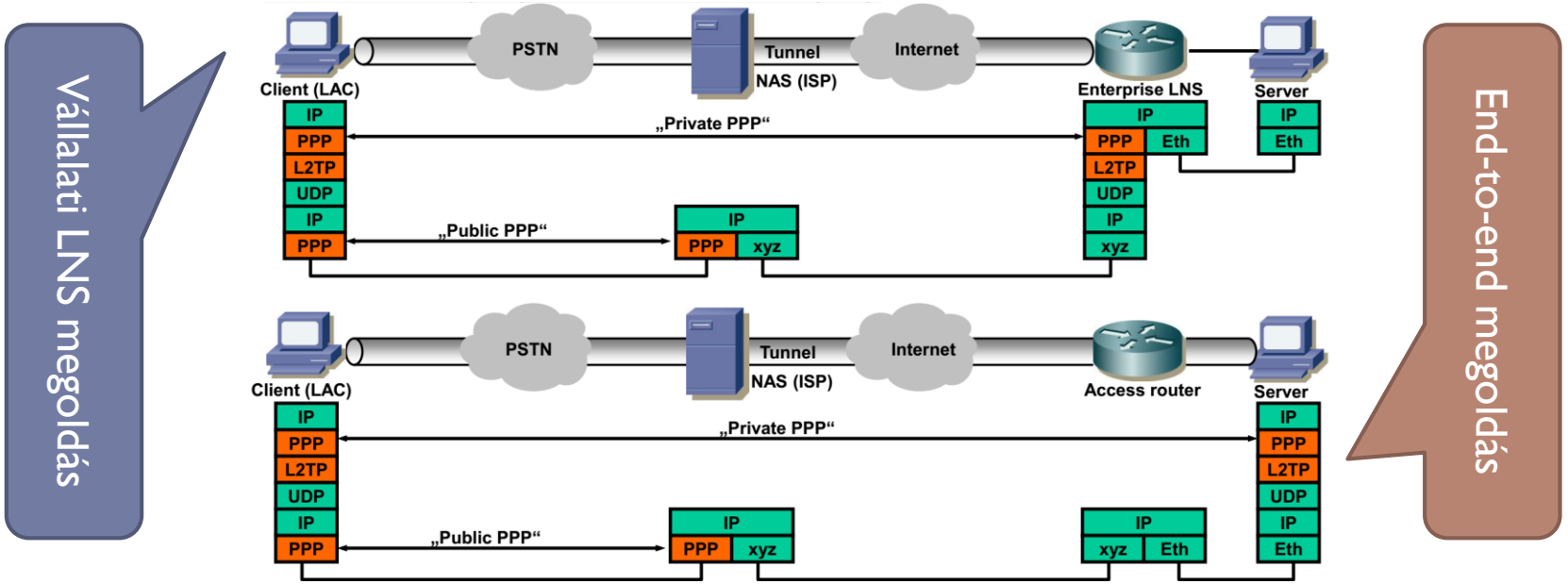
- GRE
  - Tetszőleges protokoll beágyazása
  - Megszűnteti a ”valami in valami” protokollok burjánzását

- Sorszámok
- Kis overhead
- Multicast támogatás
- Nincs titkosítás
- NAT-on átjutáshoz segítség kell



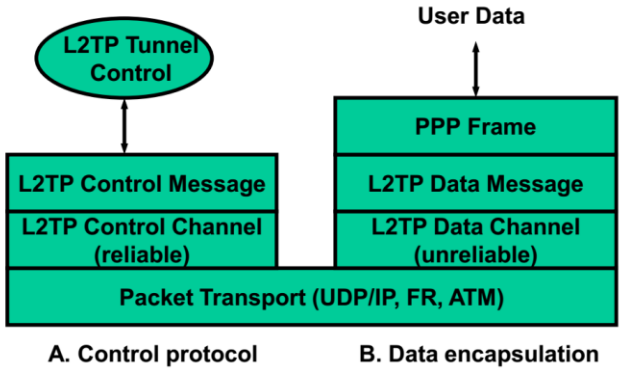
L2TP - Layer 2 Tunnelling Protocol

- L2TP - Layer 2 Tunnelling Protocol (RFC2661)



L2TP - Layer 2 Tunnelling Protocol

- L2TP
  - A. Controll protokoll tunnelek felállítására és bontására
    - Megbízható transzport protokoll szükséges hozzá
  - B. Adat beágyazás a tunnelekben
    - Nem szükséges megbízható transzport protokoll



L2TP - Layer 2 Tunnelling Protocol

- L2TP tulajdonságok
  - L2TP bármi felett (nem csak IP)
  - LNS és végpont – végpont összeköttetés is
    - Tetszőleges számú összeköttetés két végpont között
  - Egyetlen csomag formátum mind a kontroll, mind az adat számra
  - Felhasználó és tunnel azonosítás is
    - A tunnel az L2TP-vel, a felhasználó a PPP-vel hitelesít
  - Tűzfalon átjutáshoz IP/UDP használat

- De NINCS teljes titkosítás!!!
  - A PPP titkosít, de csak a payload részt, mást nem
  - Ezért szükséges, hogy más protokoll biztosítsa a védelmet (IPSec)

IPSec

IPSec – IP Security

- IPSec (RFC2401)
  - Szabványos protokoll az Internetes adatforgalom biztonságára

- IPSec tulajdonságai
  - Hozzáférés védelem
    - Mások nem láthatják az adatforgalmat
  - Integritásvédelem
    - Az adatforgalmat nem lehet megváltoztatni
  - Hitelesítés
    - Bizonyosság, hogy valóban a küldő fél küldte az adatokat
    - A kapcsolatban lévő felek ismerik egymást
  - Védelem a visszajátszások ellen
    - Az adatforgalmat nem lehet ugyanazokkal az IP csomagokkal megismételni később

Security Association

- SA – Security Association
  - Logikai kapcsolat két kommunikáló pont között
  - Leírja a kapcsolat biztonsági szolgáltatásait
    - Üzemmód
    - Algoritmusok
    - Kulcsok
  - Egy SA: egyetlen kapcsolat
    - Duplex esetben két SA szükséges
    - Kombinált üzemmódok esetén szintén több SA

SAD – SA adatbázis

- Az aktív SA-k tárolása
  - Külső IP cím, protokoll, Paraméter index (SPI)
  - Paraméterek
    - Hitelesítési algoritmus és kulcs, Titkosító algoritmus és kulcs, élettartam, protokoll üzemmód, visszajátszás elleni sorszámok, biztonsági házirend hivatkozás

SPD – Biztonsági házirend adatbázis

- Minden egyes csomagra megvizsgálj a házirendet (szabályok)
- Csomag és házirend azonosítása
  - Cél IP cím, forrás IP cím, név (falhasználó vagy rendszernév), transzport protokoll, forrás és cél portok.

- Házirend
  - Csomag eldobás, átengedés, IPSec alkalmazás
  - IPSec esetén
    - Biztonsági protokoll és üzemmód
    - Engedélyezett műveletek (visszajátszás ellen, hitelesítés, titkosítás)
    - Algoritmusok
  - Hivatkozás az SAD-re

IPSec protokollok

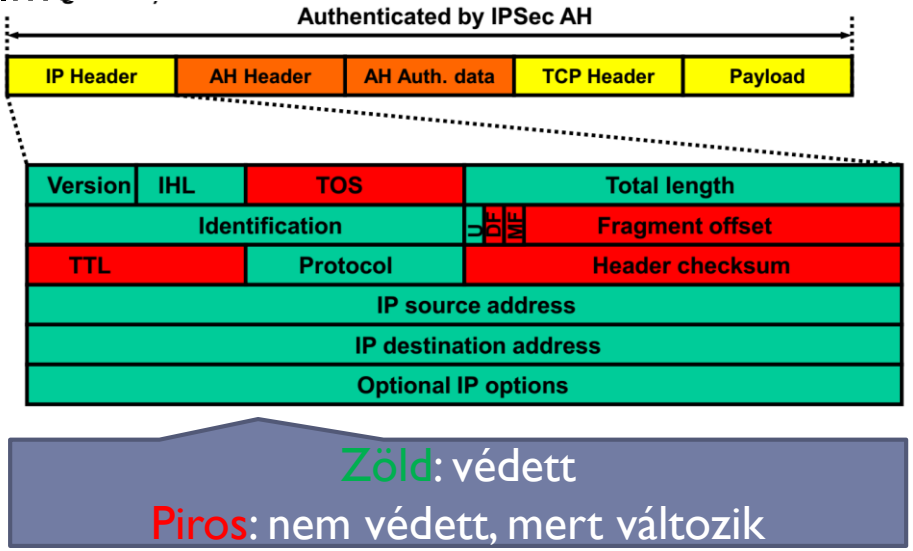
- Hitelesítés – Authentication Header (AH)
  - Az adat (IP fejléc és magasabb rétegek) eredetének hitelesítése
    - Hash függvény segítségével a továbbítás közben nem változó mezők tartalma
  - Integritás védelem
  - Védelem a visszajátszás ellen
  - Nincs titkosítás

- Titkosítás – Encapsulating Security Payload (ESP)
  - Az adatok titkossága
  - Plusz hitelesítés és integritásvédelem
    - De csak ESP adatok + tartalom, IP fejléc nem hitelesített
  - Visszajátszás elleni védelem

- Titkosítás és hitelesítés AH + ESP
  - Titkosított tartalom és a hitelesítés kiterjed az IP fejlécekre is

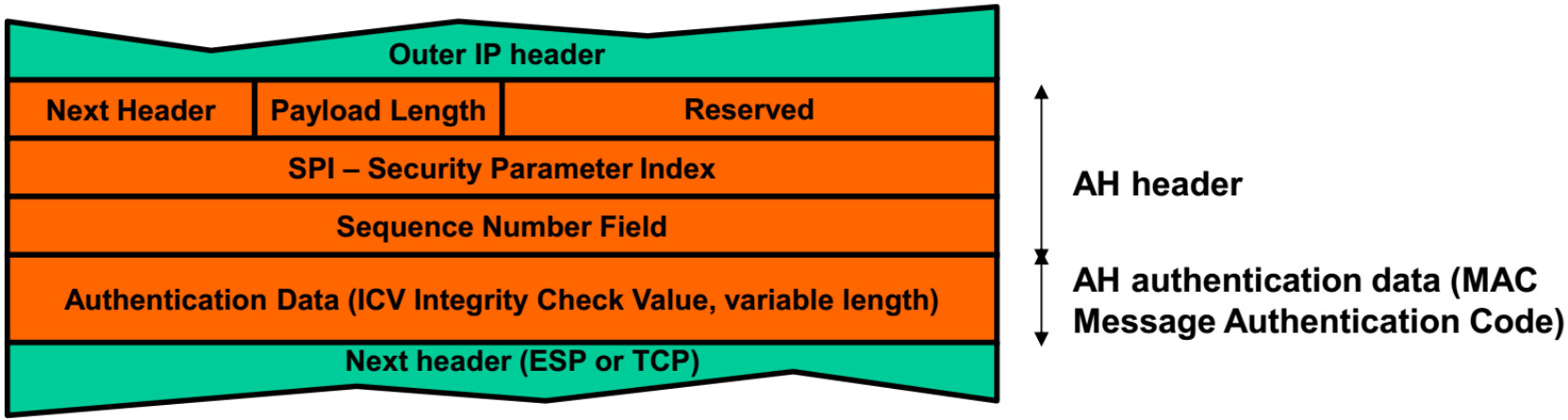
IPSec – AH – Authentication Header

- IPSec AH
  - Hitelesítésre használják
    - Adat (payload) integritás védelme
      - Sorrend védelme
      - Visszajátszás elleni védelem
      - Nem visszavonható
    - Végpont hitelesítése
    - Külső IP fejlécmezők védelme
      - Csak azok, amelyek nem változnak az átvitel során



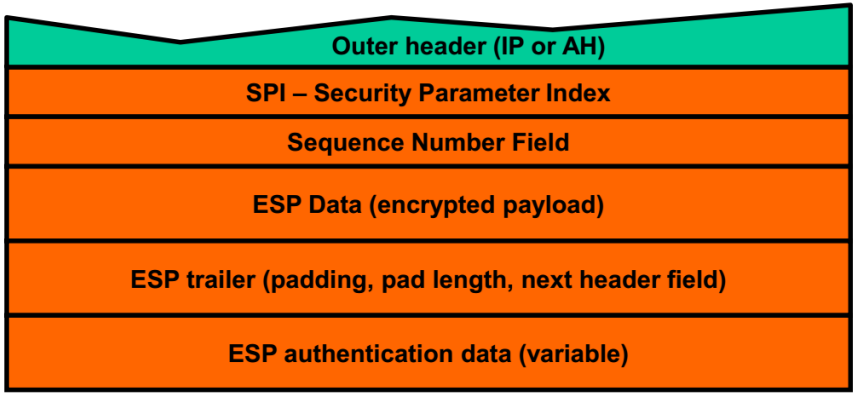
IPSec – AH – Authentication Header

- AH fejléc
  - Security Parameter Index
    - Kapcsolat paramétereinek azonosítása
  - Sequence Number Filed
    - Sorszám a védelemhez (sorrend, visszajátszás ellen)



IPSec – ESP – Encapsulating Security Payload

- IPSec ESP
  - Titkosításra használják
    - Adat integritásának ellenőrzése
      - Visszajátszás elleni védelem
      - NINCS külső IP fejléc hitelesítés
    - Végpont hitelesítése (opcionális)
      - Amennyiben AH-val együtt van, felesleges

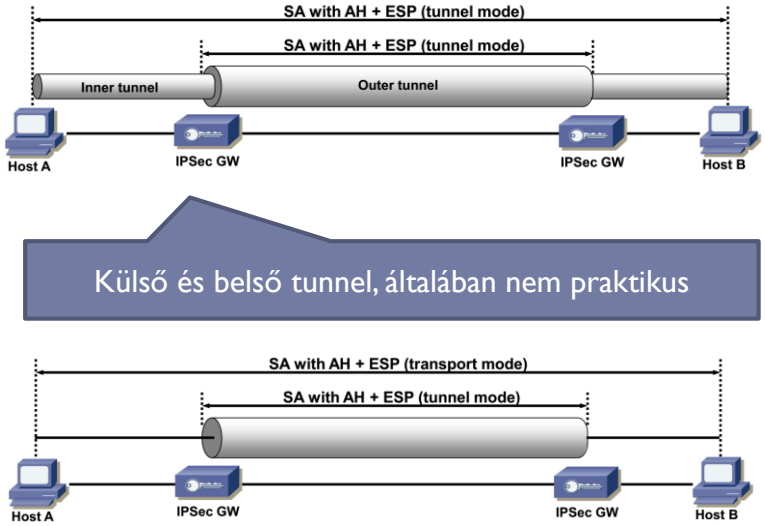


AH + ESP módok

- Szerepek elkülönítése
  - AH: hitelesítés
  - ESP: titkosítás
- Vannak esetek, amikor a hitelesítés elégséges és a titkosítás vagy túl költséges vagy szabályokba ütközik
- Az ESP is csinál hitelesítés, de vannak különbségek
  - AH: külső mezők hitelesítése is
  - ESP: csak a payload hitelesítése
- Az AH és ESP tetszőlegesen kombinálható

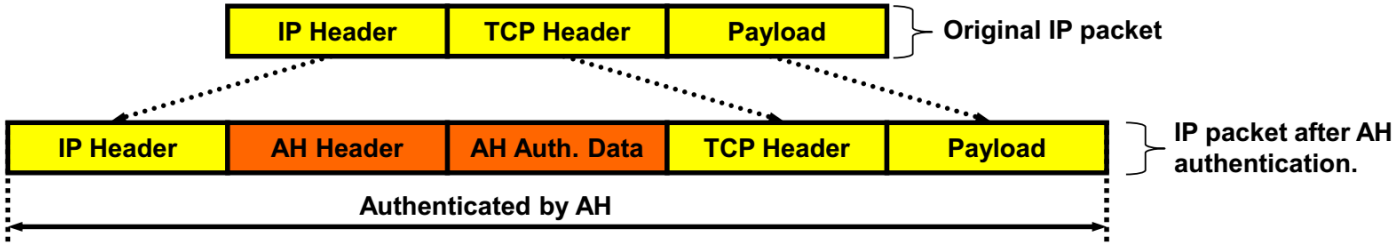
IPSec üzemmódok

- Szállítási (Transport) üzemmód
  - Védelem az IP réteg feletti protokolloknak
  - IPSec host
- Alagút (Tunnel) üzemmód
  - Az egész IP csomag védelme
  - IPSec gateway

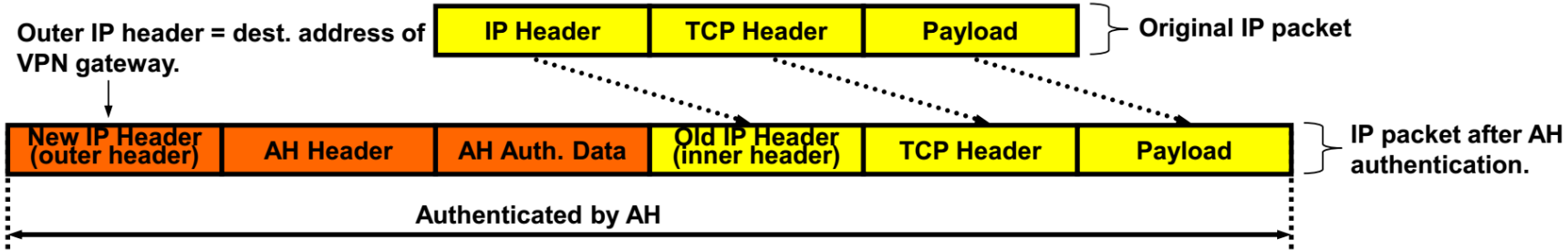


IPSec Transport és Tunnel

- AH Transport mód

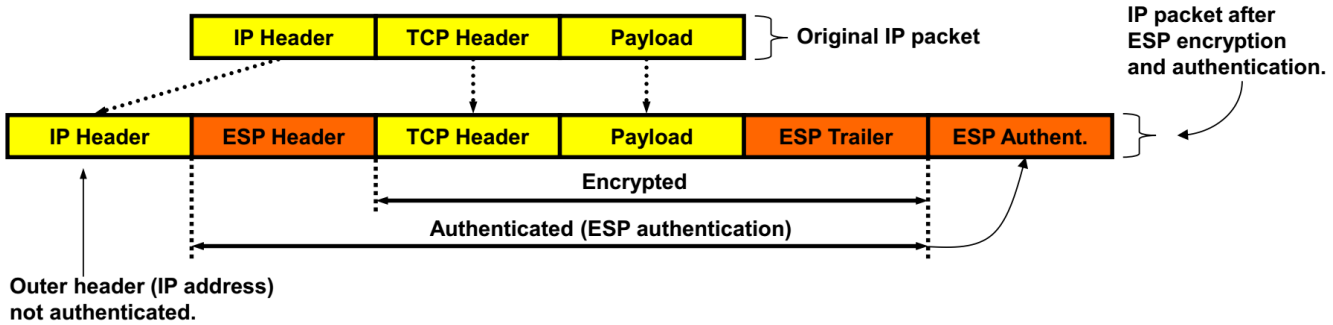


- AH Tunnel mód

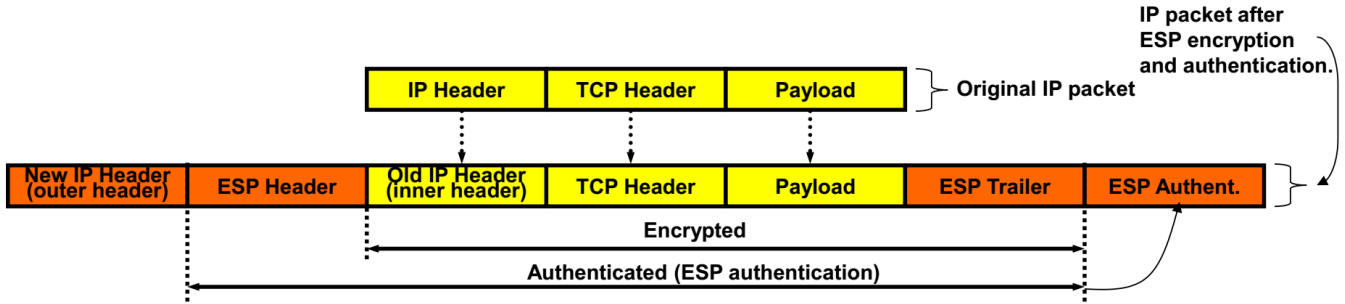


IPSec Transport és Tunnel

- ESP Transport mód

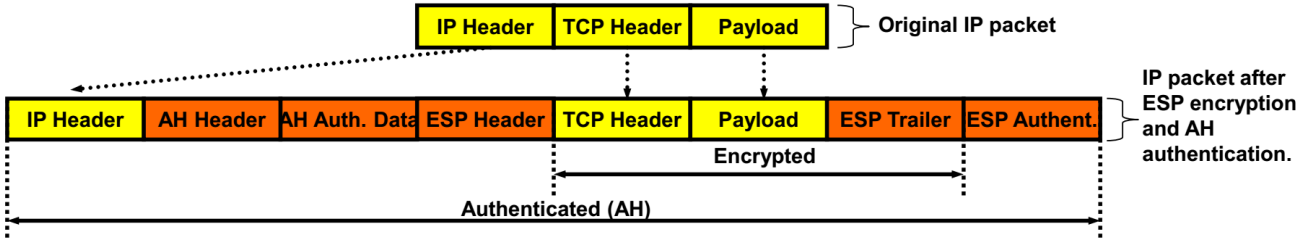


- ESP Tunnel mód

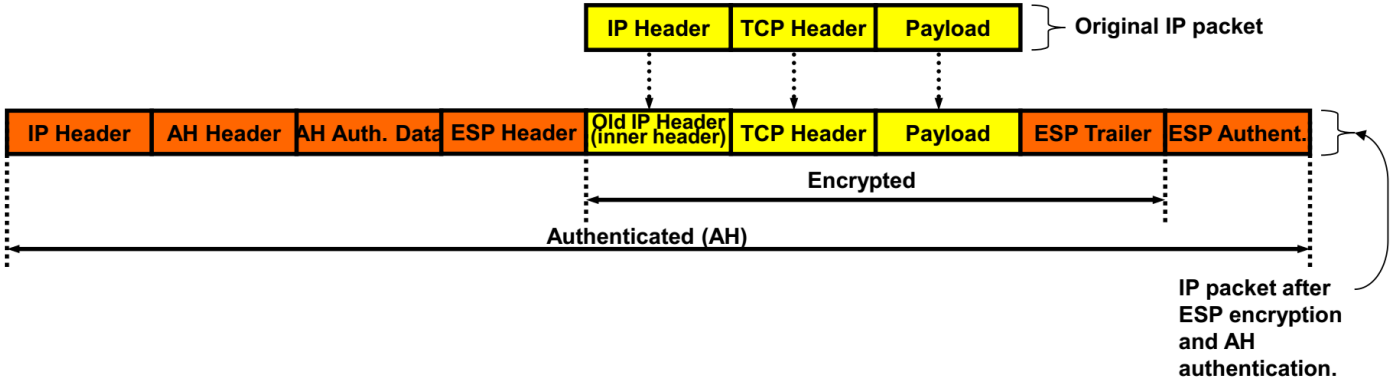


IPSec Transport és Tunnel

- AH+ESP Transport



- AH+ESP Tunnel



AH és ESP összehasonlítása

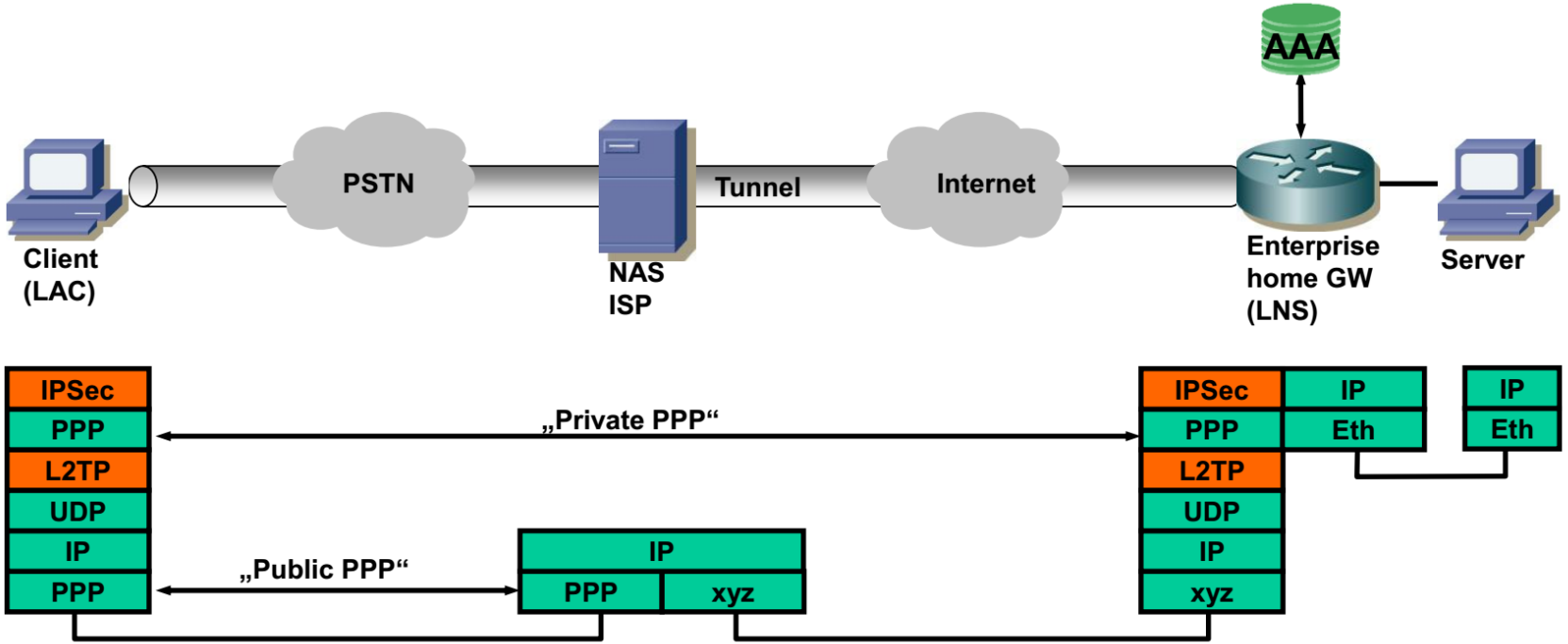
	AH	ESP	AH+ESP
Encryption	No	Yes	Yes
Sender and receiver authentication	Yes	Yes (IPSec tunnel mode only)	Yes
Data integrity	Yes	Yes	Yes
Replay protection	Yes	Yes	Yes
Sender and receiver confidentiality	No	Yes (IPSec tunnel mode only)	Yes (IPSec tunnel mode only)

IPSec építési szabályok

- Ha az egyik végpont GW, akkor a tunnel mód előnyösebb
- Ha mindkét pont végpont, a transzport mód előnyösebb
- Ha szükséges a teljes védelem, akkor tunnel mód. Ez még az eredeti fejlécet is rejti, védi
- Ha AH és ESP kombináció van, akkor a külső az AH a belső az ESP protokoll (integritás hiba esetén nem kell ESP-t dekódolni)
- AH és ESP kombináció esetén mindkét protokoll ugyanabban az üzemmódban (vagy transport vagy tunnel)

VPN kombinációk 1.

- IPSec over L2TP

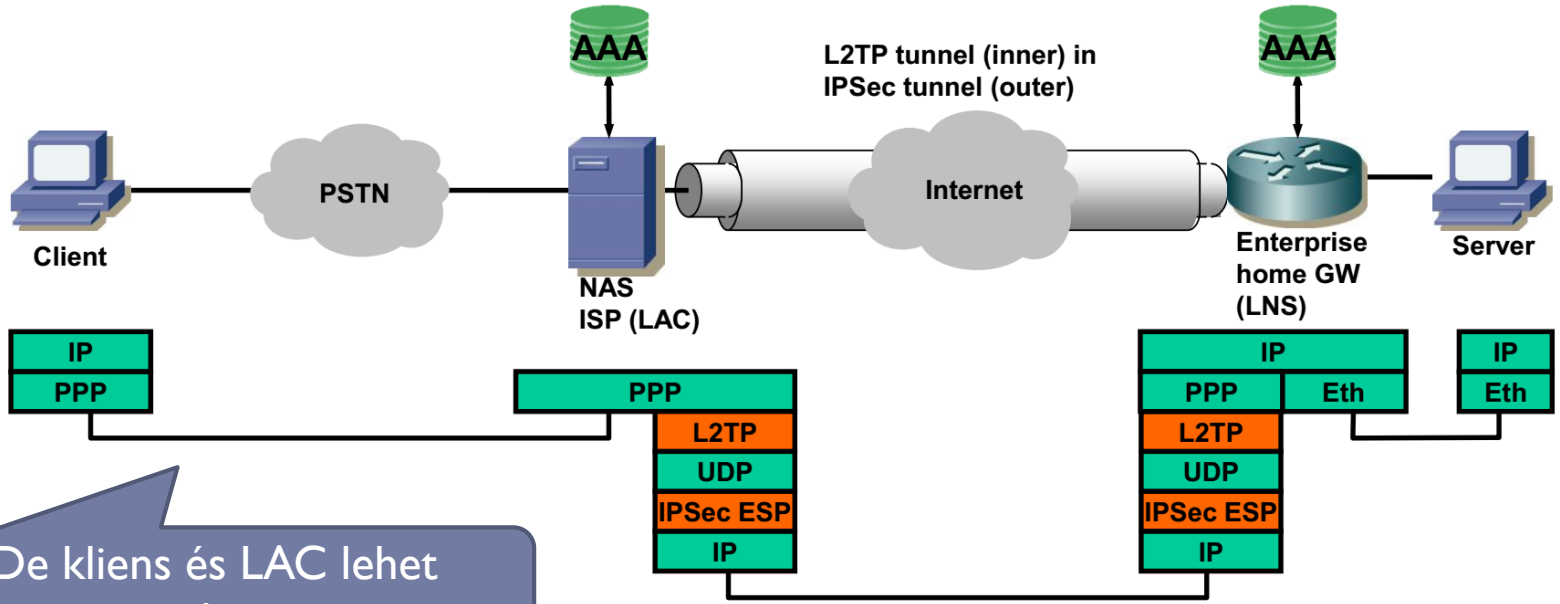


IPSec over L2TP

- Az IPSec biztosítja a titkosított átvitelt
- Az L2TP átviszi az IPSec-et a NAT-on
- Nincs felhasználó azonosítás, de van végpont hitelesítés

VPN kombinációk 2.

- L2TP over IPSec

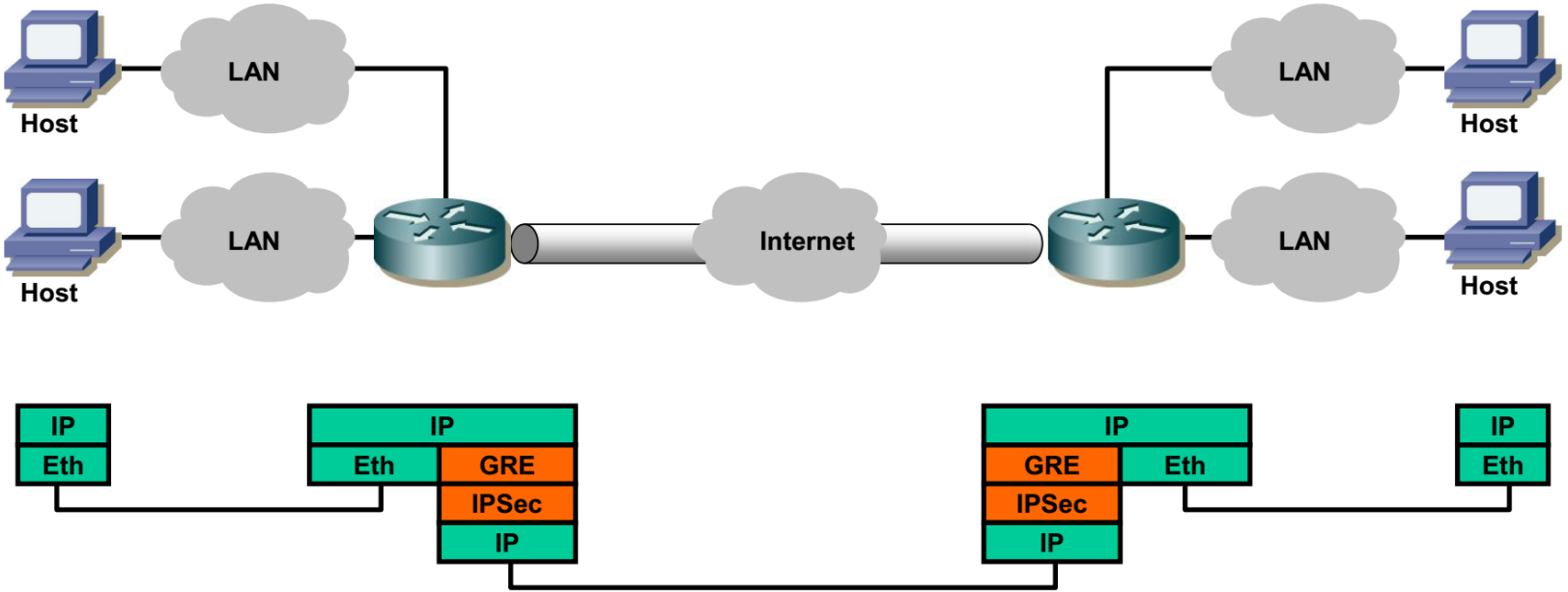


L2TP over IPSec

- IPSec (L3) felett van az L2TP (L2) protokoll
- Először az IPSec épül ki, amely biztonságos átvitelt nyújt. Ez után kerül sor az L2TP kiépítésére
- NAT átjutáshoz egyéb protokollok szükségesek
- Végpont és felhasználó hitelesítés

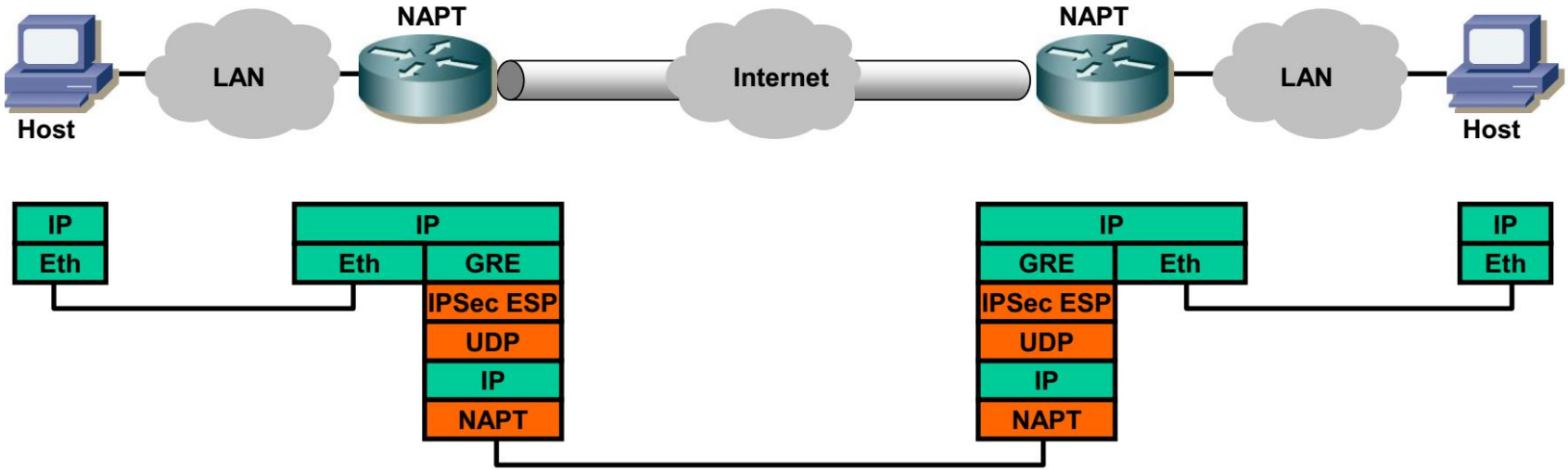
VPN kombinációk 3.

- Multiprotocol over IPSec using GRE



VPN kombinációk 4.

- IPSec over UDP (NAT-T)



IPSec over UDP

- NAT átjáráshoz szükséges
  - Az IPSec AH nem jut át a NAT-on, mert ott a portszámok (és esetleg cím is) megváltoznak
  - Az IPSec ESP átjutna a NAT-on, de ez viszont nem TCP/UDP, így nem tud a NAT mit kezdeni vele
- Megoldás, hogy UDP-be csomagolják az IPSec-et
  - Ugyanazt a portot használja, mint a kulcs egyeztetés (IKE), így csak egyetlen port szükséges

IPSec és kulcsok

- Az IPSec protokollok működéséhez szükséges a megfelelő kulcsok ismerete a végpontokon
  - Manuális kulcselosztás
    - Félrekonfigurálási hibák, tipikusan gyenge kulcsok, nem jól skálázható
  - Automatikus kulcsmenedzsment
    - Erős kulcsok, dinamikusan új kulcsok, nincs emberi hiba, skálázható

- Internet Key Exchange (IKE)
  - Működés
    - Titkos csatorna kialakítása
    - Végpontok hitelesítése
      - Jelszó, aláírás (RSA, DSA), tanúsítvány
    - Paraméteregyeztetés
  - Kulcscsere
    - Diffie-Hellman kulcscsere
    - Kerberos (Windows)

ISAKMP – Oakley – SKEME - IKE

- ISAKMP - Internet Security Association and Key Management Protocol
  - Általános keret kulcscseréhez
  - Nem definiálja, hogy mely protokollt kell használni
- Oakley
  - Kulcs generálás
  - Felhasználó védelme
  - Hitelesítés
- SKEME – Secure Key Exchange Mechanism
  - Anonimitás
  - Visszavonhatatlan
  - Gyors kulcsfrissítés
- IKE Internet Key Exchange (IPSec)
  - ISAKMP + Oakley + SKEME
  - Periódikus kulcscsere
  - IPSec protokoll egyeztetésre is (AH vagy ESP)

SSL VPN

SSL VPN alapok

- A böngésző, mint univerzális kliens
  - HTML alapú alkalmazások (Application delivery platform)
  - Böngésző bővítmények használata (Java, ActiveX, …)

- A HTTPS a biztonság alapja
  - IPSec –cel azonos biztonsági szint (hasonló mechanizmusok, algoritmusok)
    - De ezt biztonságosabbnak tartják
  - Mindig működik!
    - NAT, proxy problémák kikerülése

SSL VPN architektúra

- Böngészőn keresztül azonosítás, végpont védelem
- HTTPS (TLS) használata a biztonságos kommunikációhoz

L7 VPN

Kliens nélküli (böngésző)

Web appok
- Fájl műveletek
- Web Mail
- Csapatmunka

L4 VPN

Vékony kliens (port forward)

Előkészített alkalmazások
- RDP,VNC
- X Windows
- Citrix, …

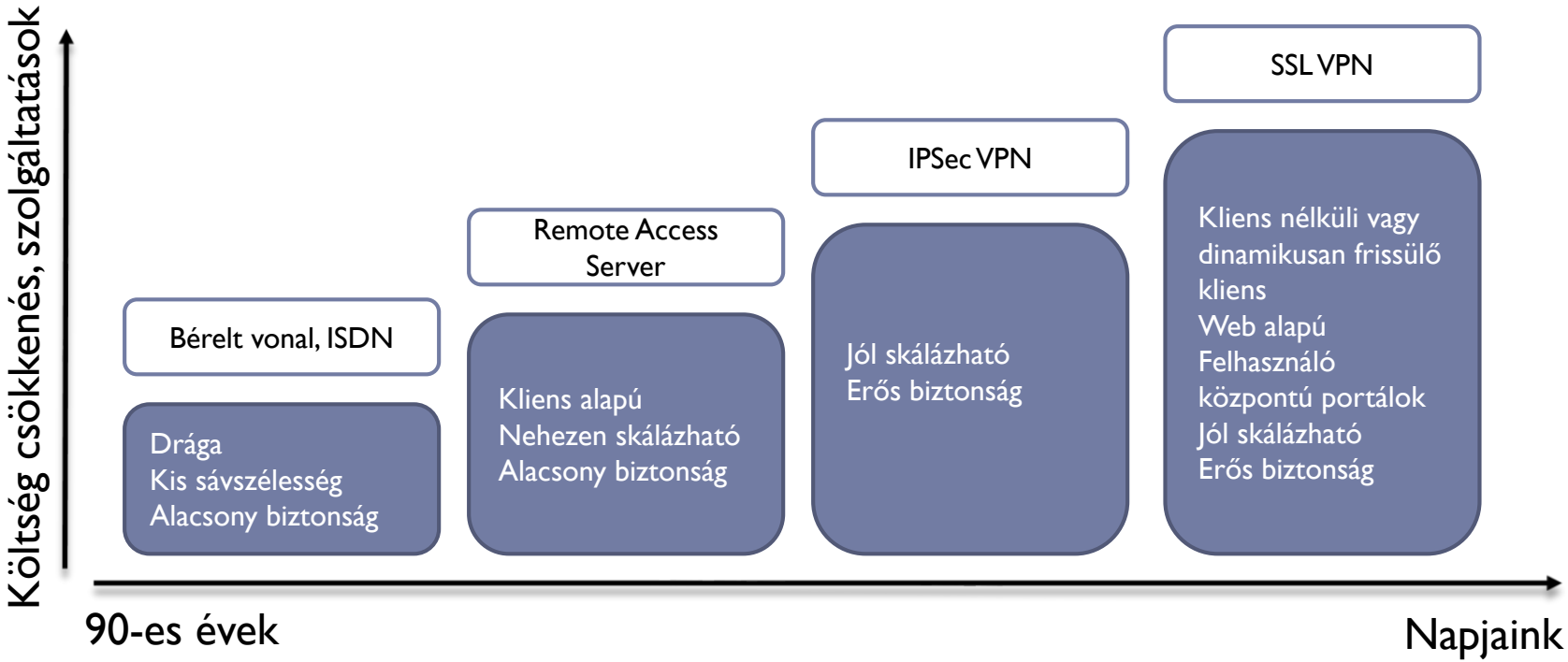
L3 VPN

Bővítmények segítségével

Teljes hálózati hozzáférés
- TLS kapcsolat

Könnyű telepítés

VPN fejlődés



SSL VPN DEMO

- https://sslvpn.demo.sonicwall.com

Más VPN megoldások

Más VPN megoldások

- Secure Shell (SSH)
  - X Windows biztonság
  - Port forwarding megoldások (lokális és távoli)
  - Teljes értékű VPN
- OpenVPN
  - Nyílt alapokon
- Felhő VPN
- Microsoft SSTP (Secure Socket Tunneling Protocol)

Felhasznált anyagok

- Peter R. Egli – Virtual Private Networks