

Távközlési informatika

IPSEC, VPN

Dr. Beinschróth József

IPSec

- A security eredetileg nem volt jelentős szempont (bizalmasság, sértetlenség)
 - Problémák
 - Titkosítatlan (lehallgatható) átvitel, letagadható, megváltoztatható üzenetek stb.
 - Pótlási lehetőségek
 - Alkalmazásokba integrálva
 - A forrás alkalmazás titkosít, védelemmel lát el stb., a cél alkalmazás dekódol...
 - Még kell változtatni az alkalmazásokat
 - A hálózati rétegbe integrálva – ez terjedt el
 - IP Security – **IPSec**, keretrendszer, többféle szolgáltatást, algoritmust stb. tartalmaz
 - RFC 2401, 2402, 2406
 - Nem opcionális, de létezik null titkosítási algoritmus: RFC 2410

IPSec - jellemzői

- Összeköttetés alapú (a kapcsolatnak állapota van):
szimplex összeköttetés a két végpont között, melyhez biztonsági azonosító is tartozik (Két irány – két kapcsolat) (Az IP kapcsolat tipikusan nem összeköttetés alapú!)
- Többnyire szimmetrikus **kriptográfiát** alkalmaz
- A headerben újabb információ jelenik meg: biztonsági azonosító, sértetlenséget biztosító adatok stb.
- Két mód
 - Transport (Szállítási) mód
 - Az eredeti IP header kiegészül
 - Tipikusan végpont-végpont közötti kapcsolatok esetén
 - A csomagméret nem nő jelenősen
 - Tunnel (Alagút) mód
 - Az IP csomag belekerül egy új IP csomagba és ennek a headerje hordozza a járulékos információt
 - Ha az alagút vége nem a célállomás
 - Lényeges csomagméret növekedés

IPSec - jellemzői

- IPv4 és IPv6 esetén egyaránt értelmezett
 - IPv4: opcionális
 - IPv6: kötelezően megvalósítandó szolgáltatás
- Az IPSec három fő biztonsági szolgáltatást képes nyújtani
 - Csak hitelesítési (AH - Authentication Header)
 - Kombinált hitelesítés és titkosítás (ESP - Encapsulating Security Payload)
 - A mindkettőt kiszolgáló kulcskezelés (IKE - Internet Key Exchange).
- Mind az AH mind az ESP egyaránt használatos transport és tunnel módban!
- Alapfogalma a Security Association (SA - Biztonságos Kapcsolat)
 - SA: **egyirányú** kapcsolat a kommunikáló partnerek között - összeköttetés
 - Kétirányú biztonságos kapcsolatokhoz két SA szükséges
 - Egy SA vagy egy AH, vagy egy ESP által megvalósított egyirányú biztonságos kapcsolatot ír le
 - Egy SA-t három paraméter azonosít egyértelműen
 - Security Parameter Index (SPI) - Biztonsági Paraméter Index: kulcs, algoritmusok, protokoll mód, sorszám, ablak, stb.
 - Az IP célcím
 - A használt biztonsági protokoll (AH vagy az ESP)

IPSec –Transport mód

- Az eredeti IP header kiegészül
- Az IPSec alkalmazását a a Protocol mezőben elhelyezett kód jelzi (51), az eredeti az IP header kiegészítő részébe kerül
- A transzport mód tipikusan **két host** (IP kommunikációs szereplő) közti végpont-végpont kapcsolatokban használatos – gépek közötti forgalom védelmét biztosítja
- Elsősorban a felsőbb szintű protokollok (jellemzően a TCP vagy UDP szegmensek), azaz az IP csomag adatmezejének a védelmére szolgál
 - Az ESP az IP fejléc nélküli **adat mezőt titkosítja**, opcionálisan hitelesíti
 - Az AH az IP csomag adatait és az IP fejléc bizonyos részeit **hitelesíti**

IPSec – Tunnel mód

- A tunnel mód leginkább **két csomópont** (pl. tűzfal vagy router) között használatos: a két csomópont között egy VPN-t (Virtual Private Network, virtuális magánhálózat) jön létre
- Az egész eredeti csomagot egy másik IP csomag belsejébe helyezik (IP-IP tunnelezés), így biztosított, hogy az egész eredeti csomag a (publikus) hálózaton való áthaladás közben változatlan marad
- Tunnel móddal biztonságos kommunikáció valósítható meg anélkül, hogy az összes kommunikáló gépen IPSec-et kellene implementálni (csak a tunnel két végpontján szükséges IPSec) – hálózatok közötti forgalom védelmére képes
- A titkosítás és autentikáció csak a tunnel két végén levő gépen (routerek) történik, a titkosítás nem terheli a hálózat gépeit
- A kisszámú résztvevő miatt egyszerűbb a kulcskezelés
- Az eredeti IP fejléc a célcímen kívül tartalmazhat **egyéb routing információkat** is (source routing utasítások, hop-by-hop opciók), emiatt az **új IP fejlécbe is be kell írni** az eredeti routing információkat, (Egyébként a közbülső routerek nem lesznek képesek megfelelő módon kezelni a titkosított tunnelezett csomagot - belső IP header a csomag tartalmával együtt titkosítva van, emiatt a közbülső routerek nem tudnak vele mit kezdeni)
- A VPN-ként használt tunneles ESP lehetetlenné teszi a forgalmi analízisen alapuló támadásokat

IPSec – Az IP header (ismétlés)

...

Szolgálat típusa: pl. VoIP

Teljes hossz.:max. 65535Byte

Azonosítás: melyik csomag

DF: Don't Fragment

MF: More Fragments

Darabeltolás: A darab (fragment)
sorszáma

Protokoll: tcp (6), udp (17)

...

32 bit

Verzió	Fejrész hossz	Szolgálat típusa (6bit)	Teljes hossz	
Azonosítás			DF, MF bitek	Darabeltolás
Élettartam		Protokoll	Fejrész ellenőrző összeg	
Forrás cím				
Cél cím				
Opciók (0 vagy több szó)				

20 byte rögzített, utána változó hosszúságú opcionális rész

A továbbítás a verzióval kezdődik

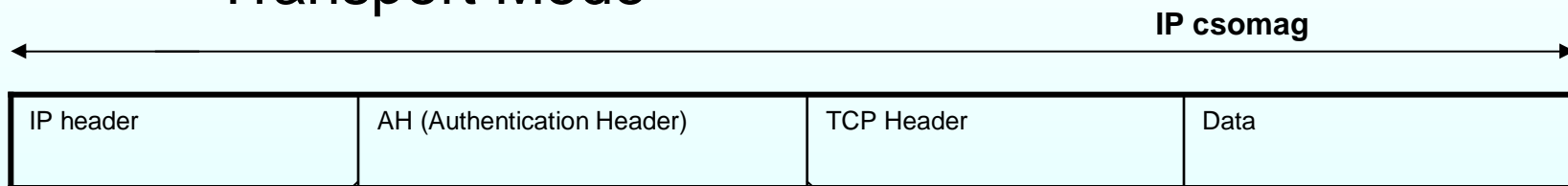
IPSec - AH

- **Hitelesítés**
 - A fejlés hitelesítése
 - Az adatmező **sértetlenségének** ellenőrzésére és a **replay** (újrajátszás) támadások elleni védelemre nyújt módot
 - Az IP headerhez kapcsolódóan megjelenik egy új mező (AH header) (Az IPv4-ben új fejlécként, az IPv6-ban mint kiegészítő fejléc jelenik meg)
 - Az AH headerben az adatmező digitális aláírása is szerepel, ez biztosítja a sértetlenség kontrollját
 - Replay elleni védelem: sorozatszám
 - Az AH titkosítást nem végez

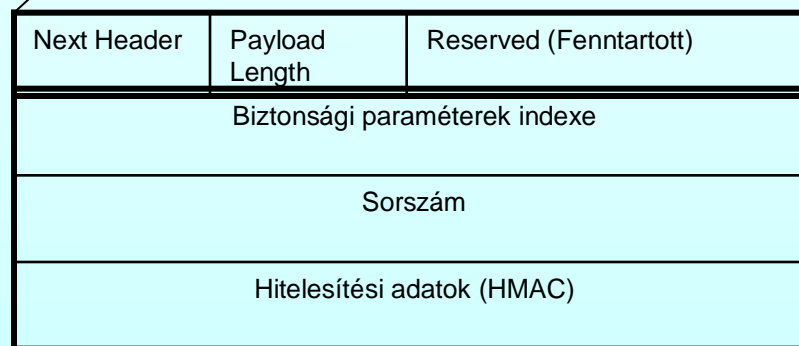
IPSec - AH

- Authentication Header
 - Transport Mode

Az AH Tunnel módban az új és a régi IP header közé kerül!



Az AH header hasonlít az IPv6 kiegészítő fejrész formátumához



32 bit

Hitelesítési adatok (HMAC - Hashed Message Authentication Code): Az adatmező (és az IP header bizonyos mezőinek) digitális aláírása

Next Header: az IP header Protocol mezőjének értékét tartalmazza, miután az le lett cserélve (51-re)

Payload Length: az AH Headerben levő 32 bites szavak száma mínusz kettő

Biztonsági paraméterek indexe: Összeköttetés azonosító, az összeköttetést leíró információk (ez tartalmazza a kulcsot is)

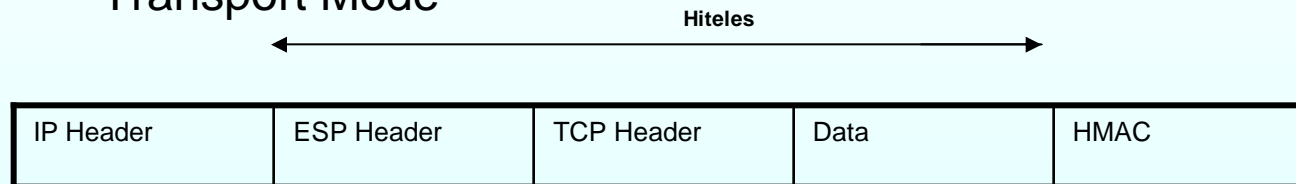
Sorszám: az SA csomagjainak sorszáma, minden csomag új sorszámot kap még újraküldés esetén is (az újrarátszás ellen)

IPSec – ESP (Encapsulating Security Payload) protokoll

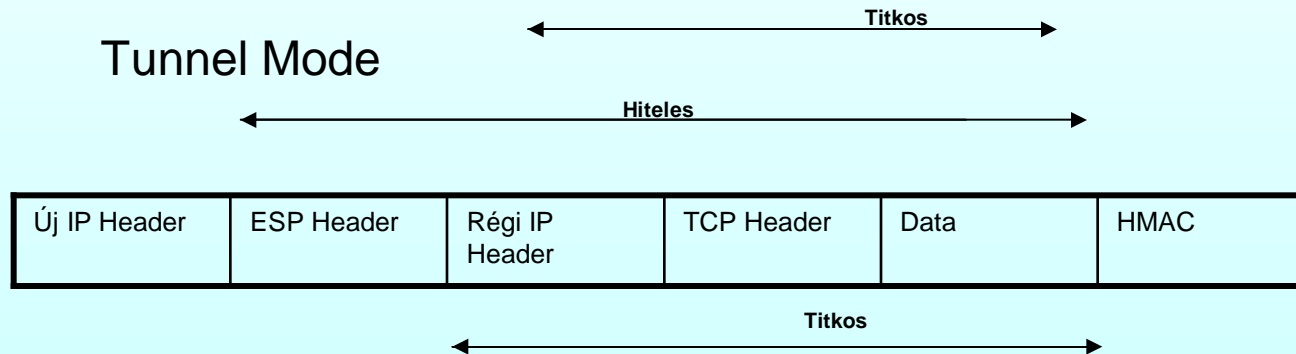
- Az AH alternatívája
- Alapvetően titkosítási szolgáltatást nyújt, védve az üzenet tartalmát a lehallgatások ellen, valamint korlátozott védelmet tud nyújtani a forgalmi adat-analízisen alapuló támadások ellen
- Az ESP opcionálisan az AH-hoz hasonló hitelesítési szolgáltatásokra is képes
- Az ESP perspektívikusabb az AH-nál (az opciókat is használva több szolgáltatást is nyújt – titkosítás)

IPSec - ESP

- Transport Mode



- Tunnel Mode



ESP Header: Biztonsági paraméterek indexe + Sorszám

IPSec – IKE (Internet Key Exchange)

- **Kulcskezelés**

- Az AH és ESP működése a kommunikálni akaró gépek titkos kulcsain alapul: titkos kulcsok szükségesek az autentikációhoz és a titkosításhoz egyaránt.
- Az IPSec két kulcskezelő mechanizmus támogatását teszi kötelezővé
 - Manuális: a rendszeradminisztrátor minden egyes résztvevő gépen manuálisan konfigurálja a gép saját és a kommunikáló partnerei kulcsait.
 - Automatizált: az automatizált kulcskezelés lehetővé teszi kulcsok új SA-k számára való igény szerinti generálását és a kulcsok automatikus propagálását

VPN – Virtual Private Network

- Több telephelyes vállalatok problémája
 - Az egyes telephelyek között kapcsolat szükséges
 - Feltétel az adatbiztonság megvalósulása
 - Hitelesség
 - Hozzáférés szabályozás
 - Titkosság
 - Adat integritás
 - Vállalati magánhálózat (Corporate Network) szükséges, amely a vállalat nem nyilvános információinak átvitelét biztosítja
 - Megoldások
 - Magánhálózat - bérelt vonal
 - Kapcsolat az Interneten keresztül – VPN (Virtuális magánhálózat: nyilvános hálózaton (például Interneten) keresztül megvalósított, titkosított hálózati kapcsolat)

VPN – Alapkövetelmény az adatbiztonság

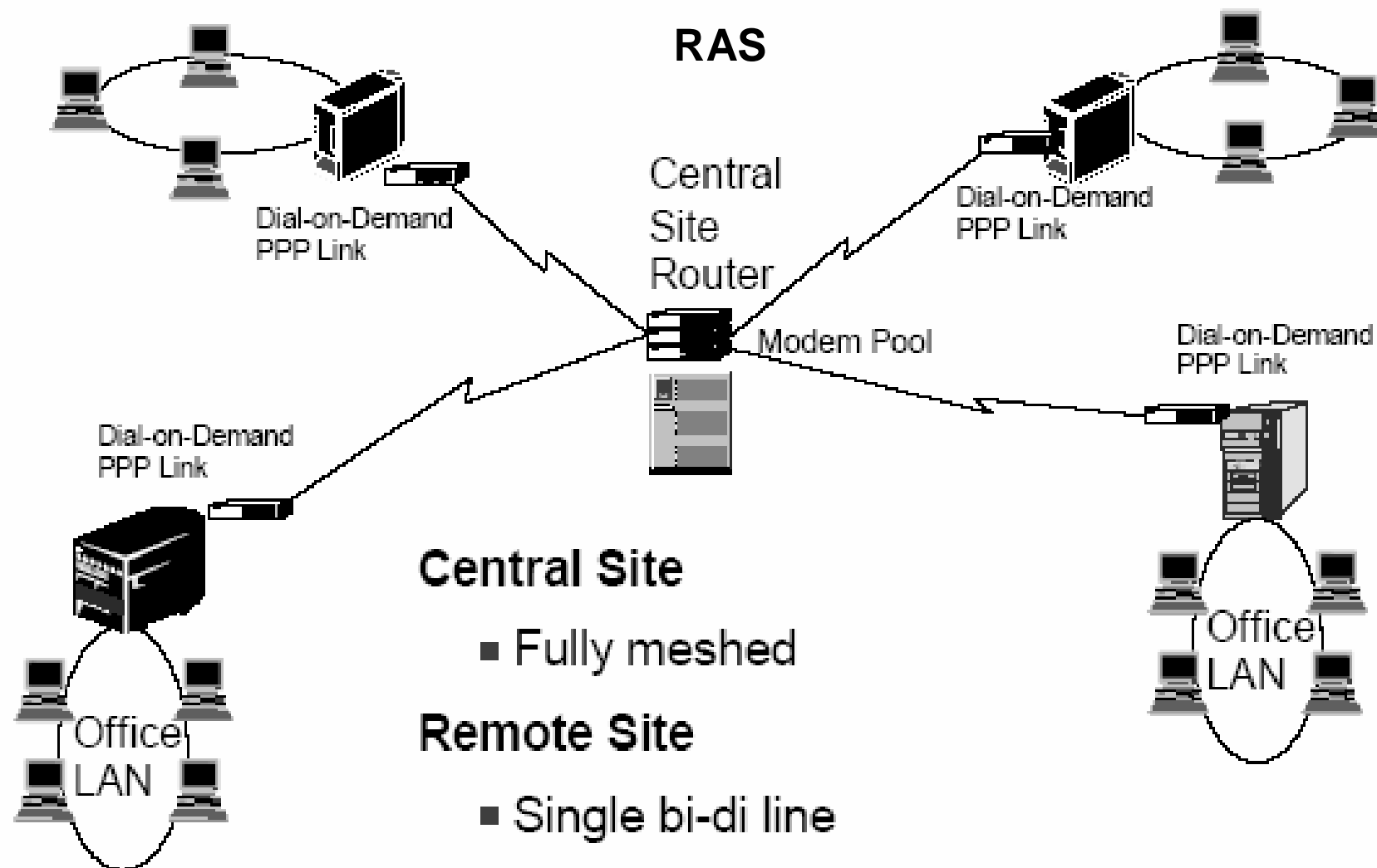
- Az adatbiztonság kritériumai:
 - Hitelesség (Authentication)
 - Annak biztosítása, hogy az adatok a megfelelő forrásból származzanak
 - Hozzáférés szabályozás (Access control)
 - Csak a megfelelő jogosultsággal rendelkező felhasználók kapcsolódhatnak a hálózathoz – érthessék el az adatokat
 - Titkosság (Confidentiality)
 - Annak megakadályozása, hogy a hálózaton illetéktelen elolvashassa vagy lemásolhassa az adatokat
 - Adat integritás (Data integrity)
 - Annak biztosítása, hogy a hálózaton senki nem változtathatja meg az adatokat

VPN – Megoldás1

- Az Internettől fizikailag is elkülönülő magánhálózat (Ez valójában nem is VPN, mert nem virtuál)
 - Az Internettől független bérelt vonalak – biztonságos, magas költség (régi megoldás)
 - A kezdeti vállalati magánhálózatok az adatbiztonságra vonatkozó feltételeket a nyitott infrastruktúrájú Internettől történő fizikai elkülönítéssel valósították meg
 - A megoldás hátrányai
 - Magas fenntartási költség
 - Távolsági összeköttetések (betárcsázás, bérelt vonal) magas költsége
 - A távoli kliensek számára a hozzáférés olyan mintha helyileg kapcsolódnának
 - A távoli kliensek IP címet is a magánhálózatnak kijelölt tartományból kapnak

VPN – Megoldás1 - példa

Az Internettől fizikailag is elkülönülő magánhálózat felépítése



VPN – Megoldás1 - problémák

- Problémák RAS esetén
 - A RAS kiszolgálóra telepített modemek, így az egyidejűleg kiszolgálható ügyfelek száma véges
 - A hívás díja elfogadhatatlanul magas lehet (távolsági hívás, hívás külföldről, hosszú ideig tartó hívások)
 - A modemek sebessége alacsony (max. 56kbit/s), ez a megszokott sebességeknél nagyságrendekkel alacsonyabb

VPN – Megoldás2

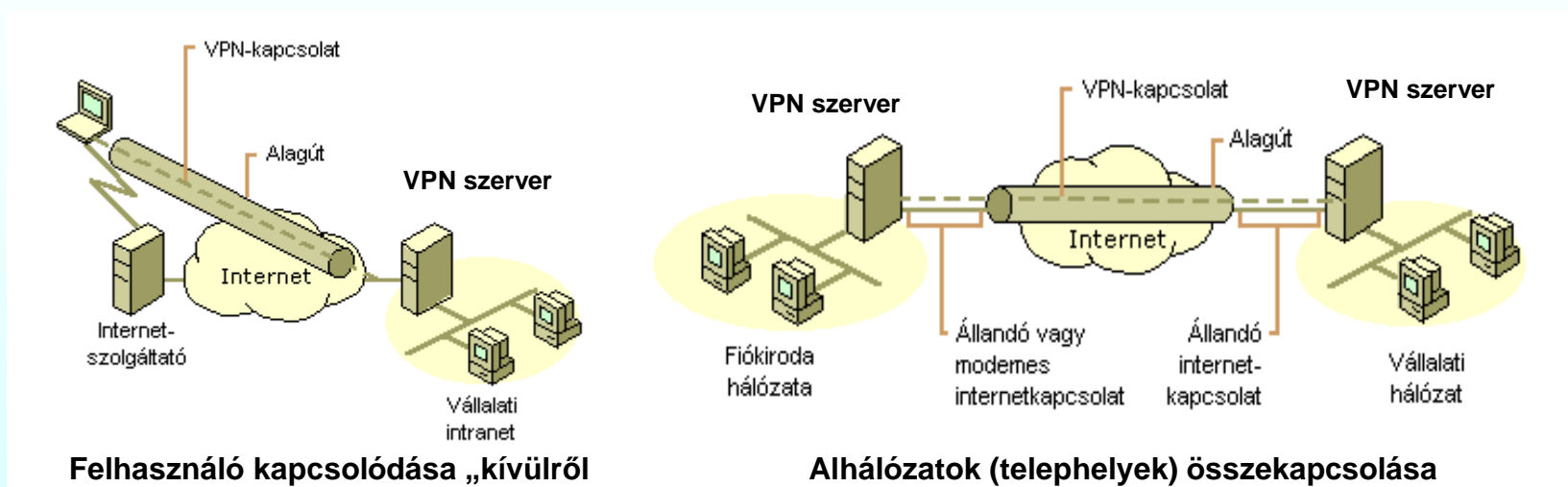
- VPN, az Interneten keresztül történő összeköttetések – olcsóbb, de a biztonság kritikus
 - Az egymástól földrajzilag távol elhelyezkedő vállalati telephelyek közötti információcsere lehetősége az interneten keresztül, biztonságosan
 - A vállalati Intranet használatának lehetősége az összes telephelyen – egységes, közös vállalati intranet
 - Az Internet nyitott infrastruktúrájának kihasználása
 - Relatív alacsony hálózati költségek
 - Az adatbiztonságra vonatkozó követelményeket is teljesülnek
 - Road Warrior (utcai harcos – utazó ügynök) is csatlakozhat
 - Virtuális: valósi fizikai összeköttetés nincs kiépítve
 - FR, ATM fölött, vagy közvetlenül az Interneten épül ki

VPN - Általános koncepció

- Az egyes (külső munkatársak vagy) telephelyek az Internet szolgáltatókhoz kapcsolódnak (ISP)
- Minden telephely el van látva tűzfallal
- Minden, a cég telephelyein levő két tűzfal között virtuális titkosított csatorna jön létre
- (A tűzfalak többnyire rendelkeznek VPN funkciókkal)
- Az interneten a csomagok ugyanúgy haladnak, mint bármely más csomag, a titkosítás a csomagtovábbítást nem befolyásolja
- A VPN a felhasználói alkalmazások számára **transzparens**, a távoli telephely elérése nem különbözik a lokálisétól

VPN - példa

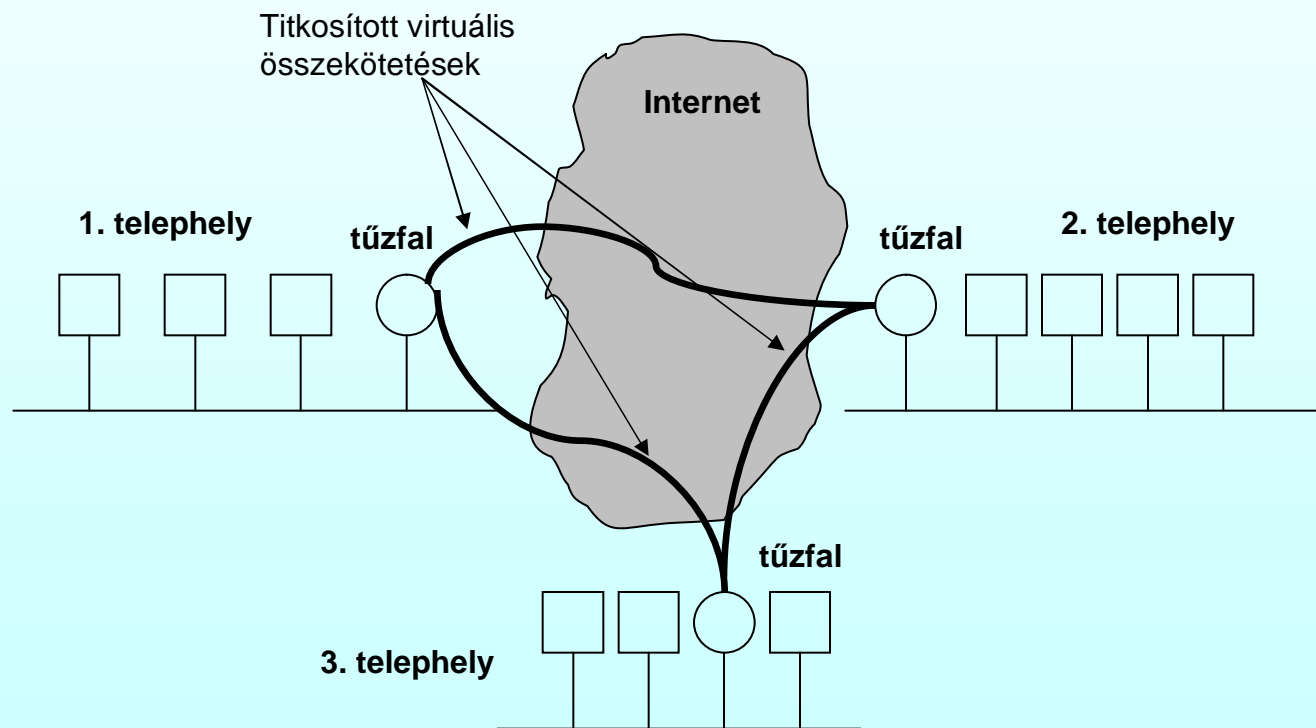
Sokféle változat képzelhető el



Kapcsolatok kiépülése

Az alagút úgy képzelhető el, mintha egy jól védett fizikai összeköttetés valósulna meg, de ezt valójában maga az internet biztosítja

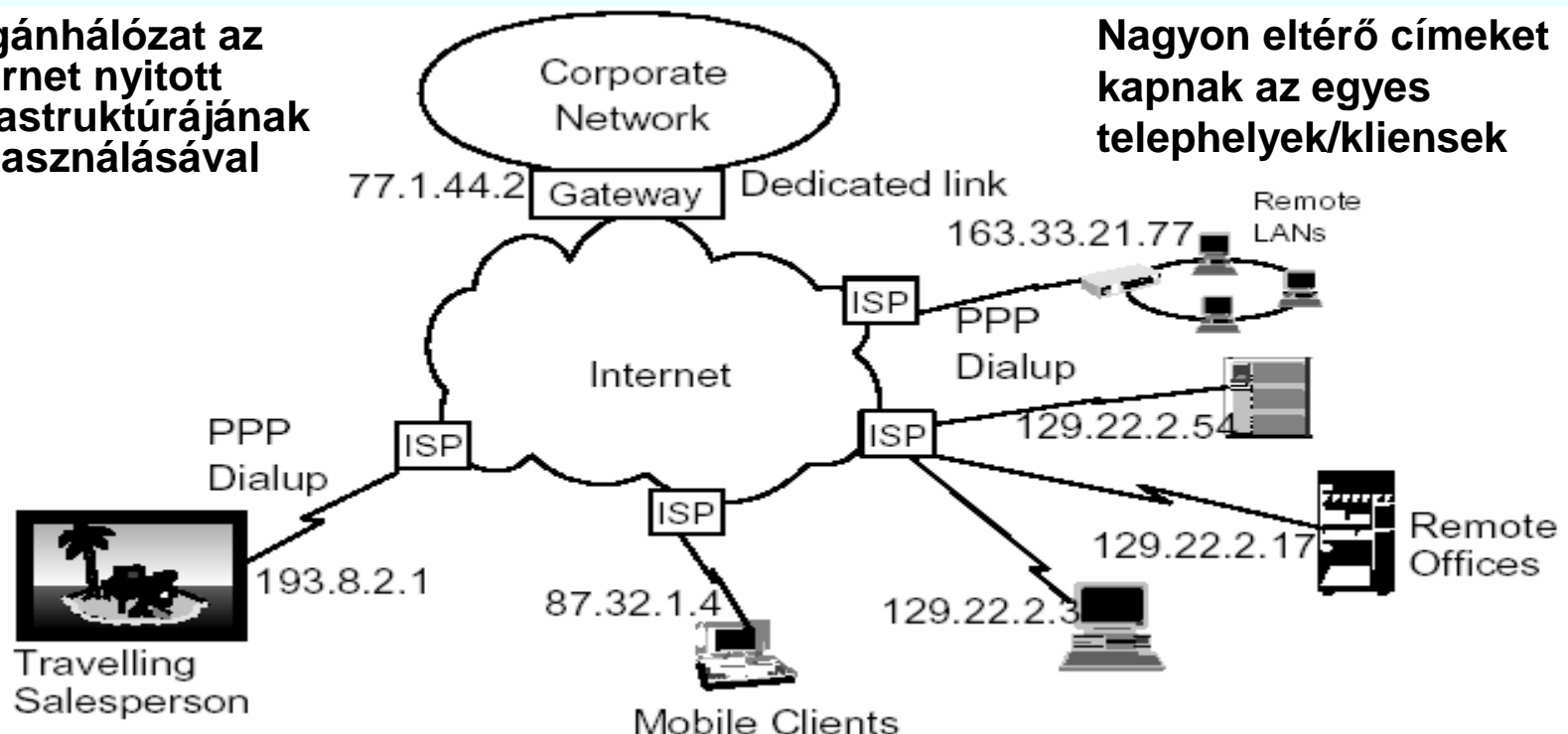
VPN - összetevők



VPN - ISP

- Probléma: az egyes telephelyek különböző ISP-khez kapcsolódnak. Mi lesz az IP címekkel?
- A kliensek attól az ISP-től kapnak IP címet akihez kapcsolódnak
- A kapcsolat kiépítés ugyancsak ehhez az ISP-hez történik

Magánhálózat az Internet nyitott infrastruktúrájának felhasználásával



VPN – követelmények és lehetőségek

- **Követelmények**
 - Megfelelő adatbiztonság elérése az Interneten
 - A kliens IP címek kezelése. (Az ISP osztja ki az IP címet dinamikusán)
 - A távoli felhasználót hogyan lehet az Internet használatában korlátozni vagy attól eltiltani
- **Megoldási lehetőségek**
 - Hardver közeli megoldások
 - Tűzfal alapú megoldások
 - Szoftveres megoldások – speciális protokollok (tunnelling protokollok) alkalmazása
 - L2F (Layer 2 Forwarding) – túlhaladott
 - PPTP (Point to Point Tunneling Protocol) (Win95, 98, NT, 2000)
 - L2TP (Layer 2 Tunneling Protocol)

VPN – hardver közeli és tűzfal alapú megoldások

- **Hardver közeli megoldások**
 - Az adatforgalom titkosítására alkalmas routerek alkalmazása
 - Minimális erőforrás igény – magas fokú hálózati áteresztőképesség
 - Nem kellőképpen rugalmasak, a hozzáférés vezérlés egy részét vagy egészét átengedik más eszköznek (pl. tűzfal)
- **Tűzfal alapú megoldások**
 - A tűzfalak + titkosítás
 - Kihasználják a tűzfal biztonsági mechanizmusok előnyeit
 - NAT
 - Bizonyos hálózatrészek elérésének korlátozása
 - Azonosítási mechanizmusok
 - Naplózás stb.
 - A performancia a titkosítás miatt kritikus lehet!

PPP (Point to Point Protocol) (ismétlés)

- RFC 1661
- Funkciók:
 - Duplex összeköttetést biztosít egy linken lévő két rendszer között. (Pont-pont összeköttetés)
 - 3. rétegi csomagokat továbbít
 - Lehetővé teszi ugyanazon a linken különböző 3. rétegi protokollok multiplexálását amellyel lehetőséget biztosít azok a linken történő egyidejű átvitelére. (Encapsulation)
 - Az összeköttetés vezérlésére definiálja a Link Control Protocol-t (LCP).
 - Lehetővé teszi a szállított 3. rétegi protokoll vezérlésére a Network Control Protocol (NCP) használatával. Az NCP-t az RFC 1661 nem tartalmazza.

VPN – szoftveres megoldások - PPTP

- RFC 2637 (Microsoft specifikus megoldás)
- MPPE (Microsoft Point-to-Point Encryption) titkosítás
- A PPP csomagokat (amelyek pl. már egy HDLC keretben helyezkednek el) újabb IP csomagba tesszük
- Korlátozott alkalmazhatóság
- Az azonosítás a windows domain biztonsági rendszerére korlátozódik
- A titkosítási módszerek gyengék, az alkalmazott kulcsok rövidek, a jelszavak a hash kódokból visszafejthetők
- A jelszókezelés vegyes környezetben nem elég körültekintően van megoldva, a statikus jelszavak könnyen kompromittálhatók
- A csomagazonosítás nincs megfelelően megoldva, emiatt a szerver támadható

VPN – szoftveres megoldások - L2TP

- RFC 2661
- Az L2TP a Point-Point Tunneling Protocol (PPTP) és Layer 2 Forwarding Protocol (L2F) tunneling protokollok utódjának tekinthető
- Célja a vállalati magánhálózat **kiterjesztése a távoli kliensekhez** egy közbenső hálózat felhasználásával
- Saját titkosítást nem tartalmaz, az IPSec-re épül, azzal együtt biztonságos adatátvitelt tesz lehetővé az Interneten (**L2TP over IPSec**)
- Privát hálózati hozzáférést biztosít a világ bármely részéről (vezetékes vagy mobil hálózatról) az Internet használatával
- A PPP-re épül, a PPP Authentication eljárásait (PAP, CHAP) alkalmazza
- A PPP lehetővé teszi más hálózati címek és protokollok (IPX, SNA, NetBios) alkalmazását is
- Az L2TP menedzseli a PPP adatkapcsolati rétegét is (pl. HDLC)

VPN – szoftveres megoldások - L2TP

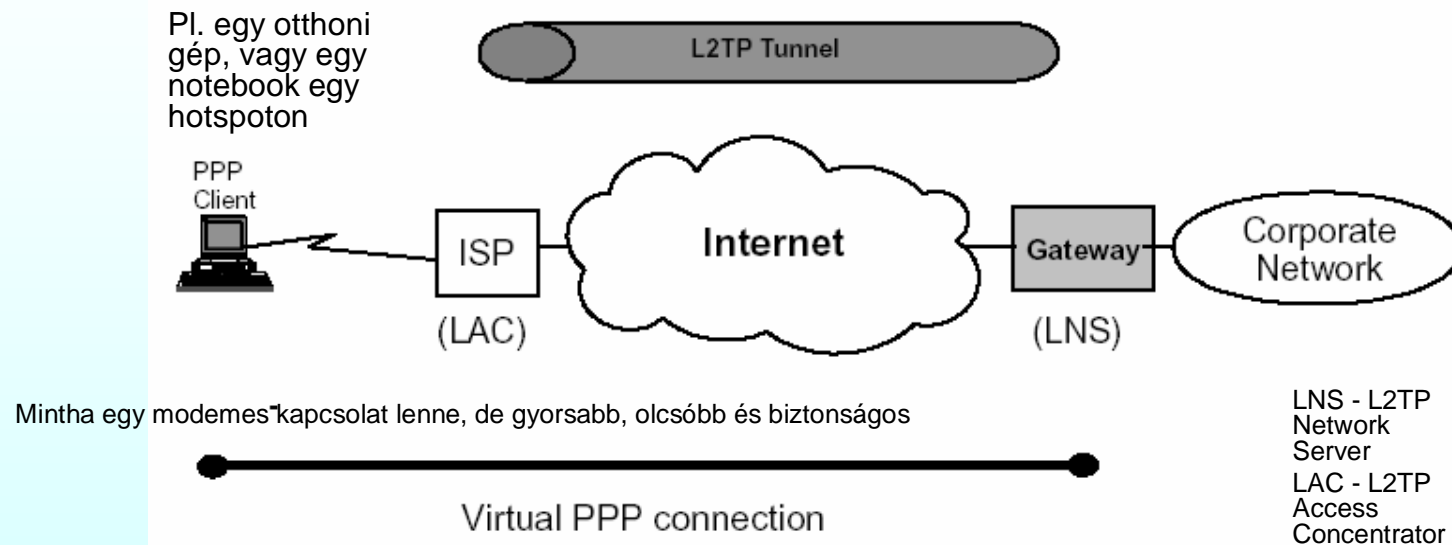
- A távoli kliensek ugyanúgy használhatják a vállalati hálózatot mint a helyiek
 - Az Interneten keresztül többnyire csak a vállalati hálózatot érik el, minden csomag a vállalati hálózathoz lesz továbbítva
 - Az Internethez többnyire csak a vállalati hálózaton keresztül kapcsolódhatnak
 - Ugyanazon biztonsági kapu szabályok vonatkoznak rájuk
 - Korlátozni vagy tiltani lehet az Internet hálózat használatát
 - Nincs szükség tűzfalra a távoli klienseknél
- Összetevők
 - LNS - L2TP Network Server
 - LAC - L2TP Access Concentrator
 - ISP – Internet Solution Provider
- Az LNS a privát hálózatban a tűzfalon belül helyezkedik el így belső IP cím alkalmazása lehetséges a tunnel másik végpontján is
- A LAC a távoli helyszínen működik, vagy a távoli ISP működteti, vagy magán a távoli gépen van

VPN – szoftveres megoldások - L2TP

- Két tunneling mód
 - Compulsory – kötelező (azért kötelező, mert a klientsztől minden az LNS-hez lesz továbbítva)
 - Voluntary - önkéntes
- A módok közötti különbség: melyek a virtuális PPP link végpontjai (az egyik végpont mindig az LNS (L2TP Network Server))
 - Compulsory tunnel: LNS és az ISP között
 - Voluntary tunnel: az LNS és a távoli kliens
- A Voluntary tunnel perspektivikusabb, mivel független az ISP-től
- A tunnel létrehozása után a magán hálózatban privát IP címek használatosak a tunnel „másik végén” is
- L2TP IP Address Management
 - Az LNS-nek a tunnel típusától függetlenül globális IP címmel kell rendelkeznie
 - A távoli kliens Compulsory tunnel esetén csak egy IP címmel rendelkezhet amely a vállalati hálózatnak megfelelő IP cím (tipikusan privát IP cím esetleg a corporate network által regisztrált globális cím), azaz nem kap globális IP címet a távoli ISP-től
 - A távoli kliens Voluntary tunnel esetén egy globális IP címmel és egy privát címmel rendelkezik, a közvetlen internet eléréshez a globális IP címet, a vállalati hálózatban a lokális címet használja, itt a globális IP címet a távoli ISP adja

VPN – szoftveres megoldások - L2TP

L2TP Compulsory tunnel felépítése



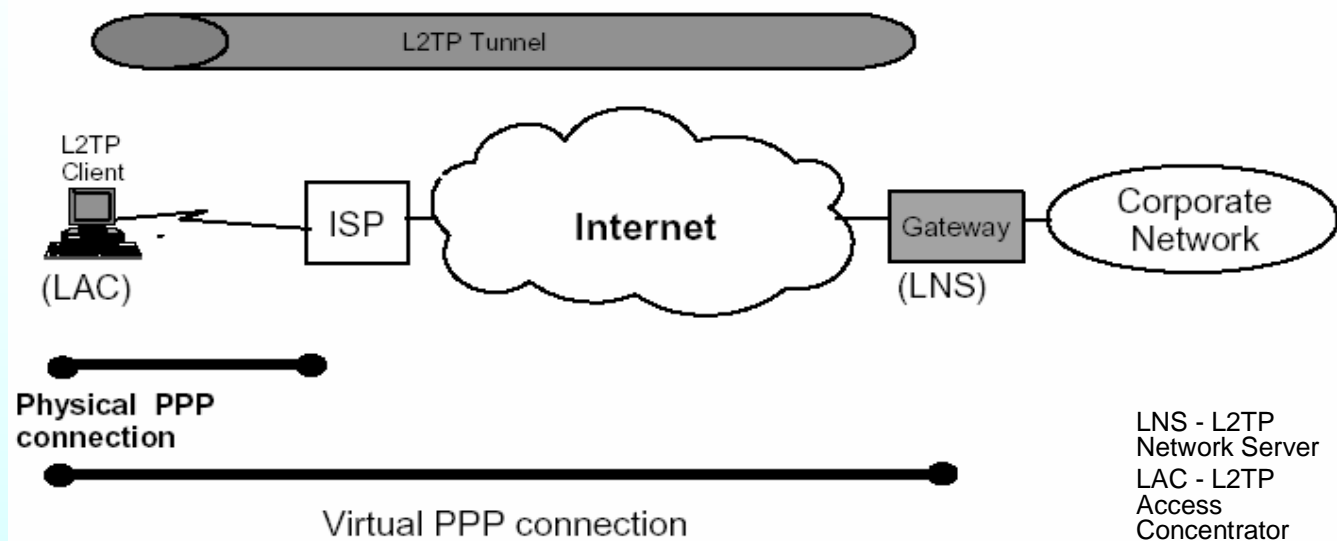
Kialakítás:

1. A távoli kliens kapcsolódik távoli ISP-hez (a saját LNS-ét ismeri)
2. Az ISP inicializálja az L2TP tunnelt
3. A távoli kliens PPP csomagokat küld a LAC-hoz, amely L2TP-be beágyazza azokat és a tunnel-en továbbítja az LNS-hez

- Az ISP valósítja meg LAC (L2TP Access Concentrator) funkciót
- A távoli klienseknél nincs szükség L2TP funkcióra
- A távoli kliens nem rendelkezik a távoli szolgáltató által adott globális IP címmel. (Csak egy session kiépítése lehetséges az LNS-hez, a kliensnek nincs közvetlen Internet hozzáférési lehetősége.)

VPN – szoftveres megoldások - L2TP

- **Az L2TP Voluntary tunnel felépítése**



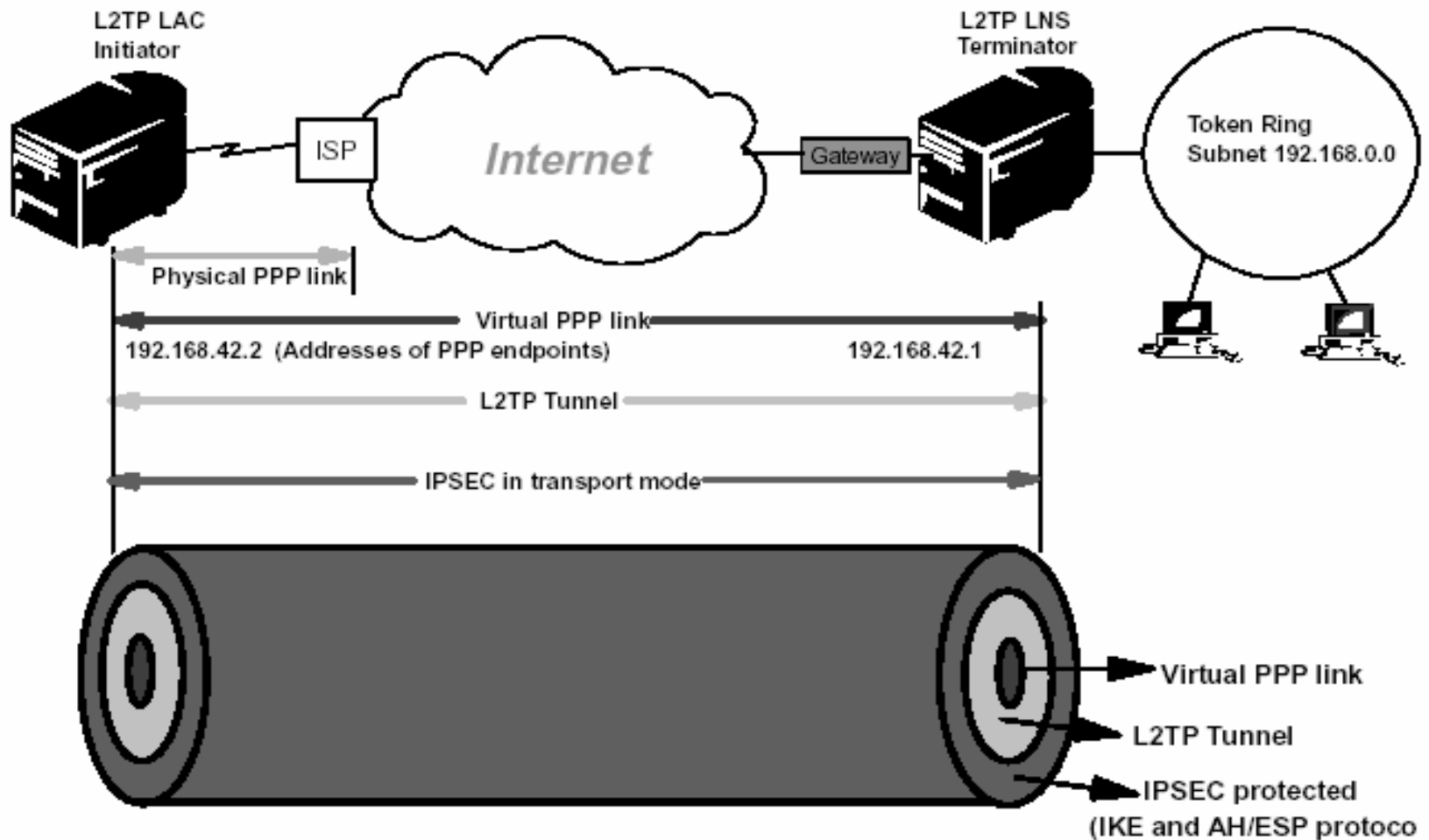
Kialakítás

1. A kliens először az ISP-vel hoz létre egy PPP kapcsolatot ahonnan egy globális IP címet kap.
2. A kliens a globális IP cím felhasználásával építi ki az L2TP tunnelt az LNS-hez
3. Létrejön a virtuális PPP link a kliens és az LNS között (protokoll egyeztetés, privát IP cím kiosztás)

- **A távoli kliensen megvalósul az L2TP ill. a LAC**
- **A tunnel transzparens az ISP-re és az Internet hozzáférési módszerre**
- **A kliens globális routolható IP címmel rendelkezik, ami közvetlen Internet hozzáférést biztosít, a kliens több IP címmel is rendelkezhet**

VPN – szoftveres megoldások - L2TP

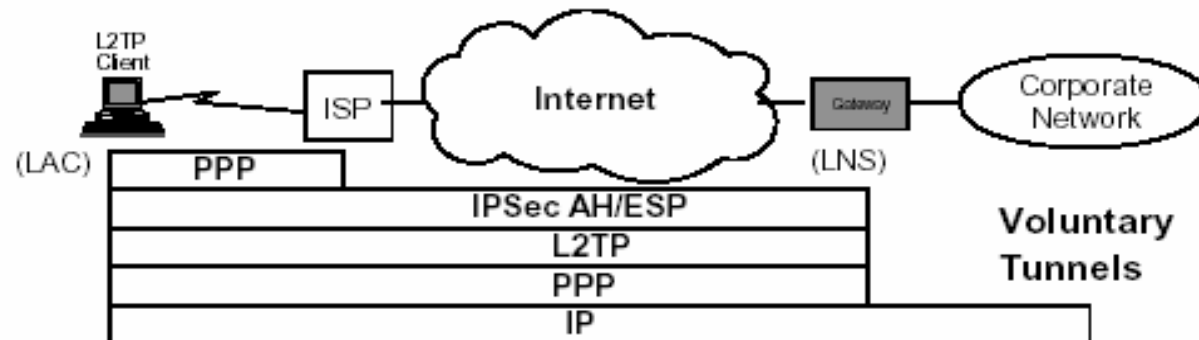
- Kapcsolódás (Voluntary tunnel)



VPN – szoftveres megoldások - L2TP

- Összeköttetések

Non-IPSec-enabled destinations:



IPSec-enabled destinations:

