Fábián Zoltán – Hálózatok elmélet

VPN – Virtual Private Network

(R)RAS – Routing and Remote Access – Útválasztás és távelérés

VPN – Virtual Private Network

- **Virtuális magánhálózat**
  - Egy lokális hálózathoz külső távoli kliensek csatlakoznak biztonságosan
  - Két telephelyen lévő lokális hálózatot nyílt hálózaton kötünk össze biztonságosan
  - A hálózatot a kliensek több szintű jogosultsággal érik el

Windows szerveres környezetben ezt valósítja meg az RRAS

Miért jó az RRAS?

- A távmunka szerepe növekszik a világon
  - Távoli munkaerők
  - Mobil felhasználók
  - „Drót nélküli” felhasználók
  - Üzleti partnerek (dolgozók, beszállítók, vevők)
- A több telephellyel rendelkező cégek hálózatainak összekapcsolása

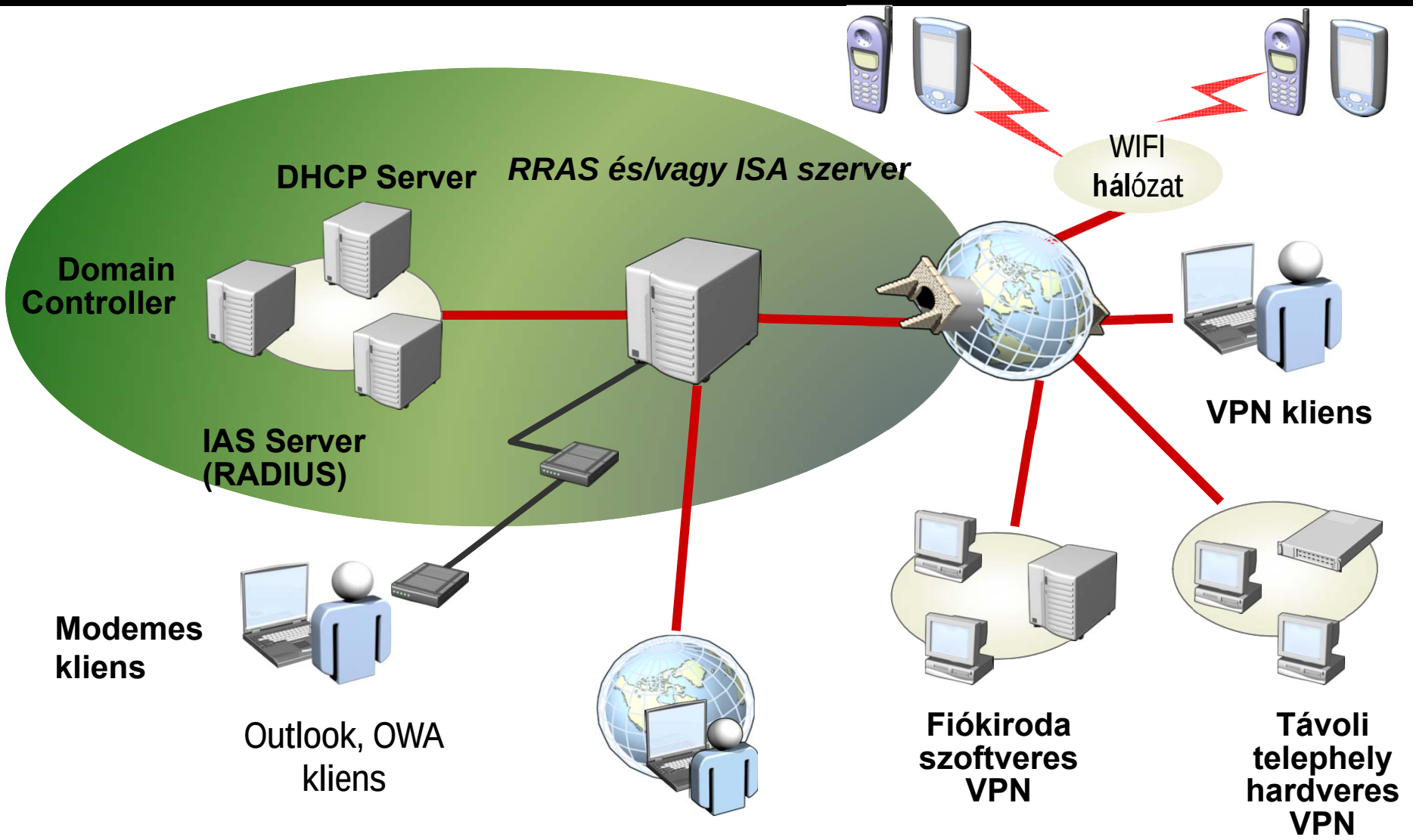
Ellenjavallat…

- A távoli elérés sohasem teljesen biztonságos
- Nehezebb a központi felügyelet
- Nem biztos, hogy van Csoport Házirend, szoftverfrissítés, stb…

Milyen szolgáltatások kellhetnek?

- Távoli asztal (Remote Desktop), VPN-en
- Érjük el az intranetes alkalmazás web szerverét belülről (számlázás, ügyfél adatai)
- Exchange adatok elérése
- Cégen belüli számlázó szoftver használata
- Nyomtatás a céges nyomtatóra ☺
- A két telephely közötti adatforgalom biztosítása!

Az igények


DHCP Server
RRAS és/vagy ISA szerver
Domain Controller
IAS Server (RADIUS)
WIFI hálózat
VPN kliens
Modemes kliens
Outlook, OWA kliens
Fiókiroda szoftveres VPN
Távoli telephely hardveres VPN

A megvalósításhoz szükséges hardverek és szolgáltatások

- Fizikai eszközök
  - Legalább két hálózati csatoló az RRAS szerveren (LAN vagy Modem)
- Szolgáltatások
  - Távoli eléréshez – betárcsázás vagy VPN kapcsolat
  - Telephelyek közti kapcsolathoz: (betárcsázás vagy VPN)
  - NAT - Name Address Translating (= Címfordítás)
  - Routolás – Forgalomirányítás – a több hálózati csatoló között (LAN / Wifi / Modem)
  - DHCP szolgáltatás a távoli kapcsolódók részére
  - Dinamikus Domain szolgáltatás?

Teljesítmény kérdések

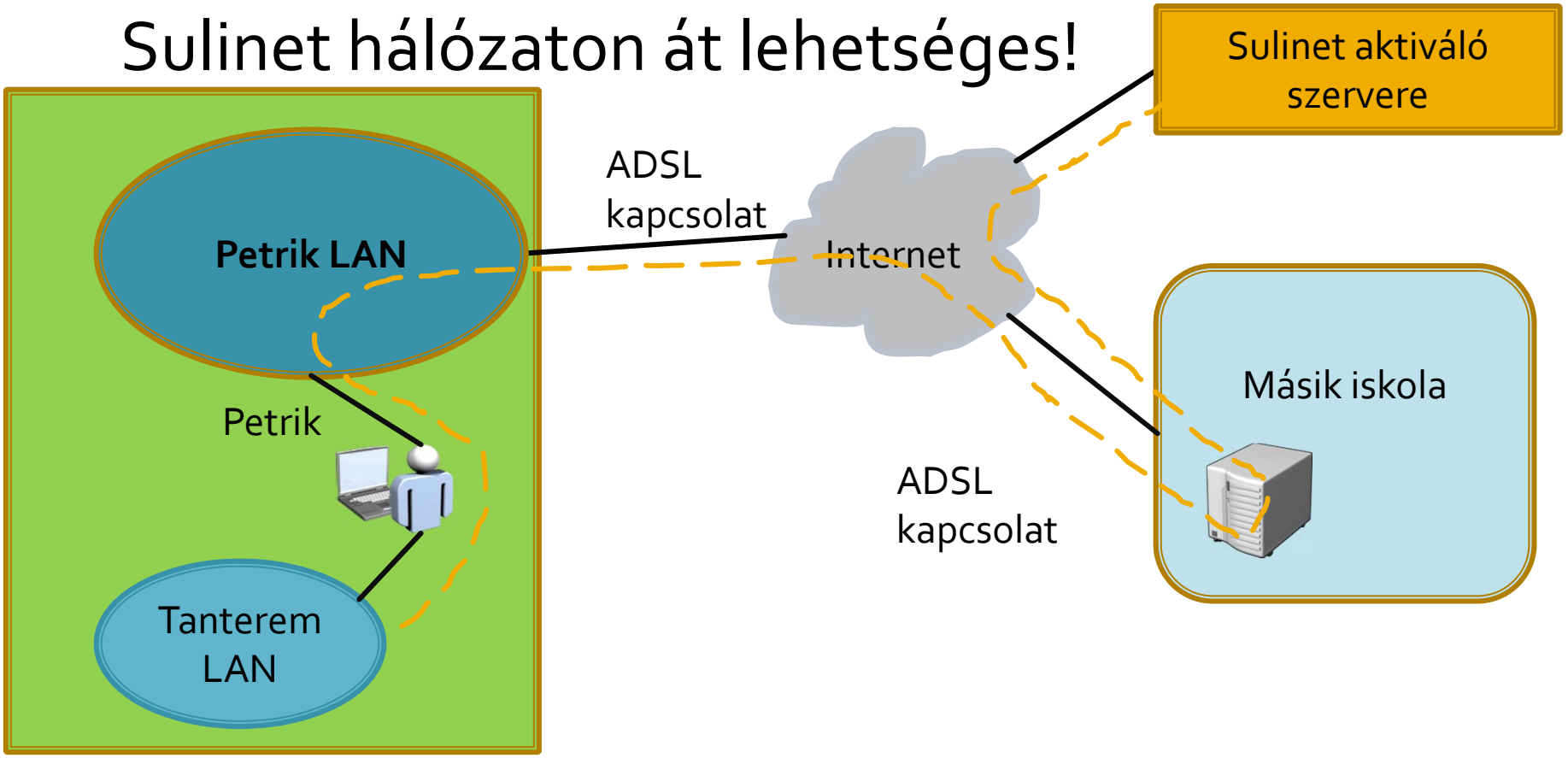
- Mekkora lesz a sávszélesség igény?
  - Hány párhuzamos kapcsolatot kell kiszolgálni?
  - Szükséges-e QoS, Load Balancing?
  - Milyen a tipikus adatforgalom – párbeszéd, stream, fájltranszfer?
- Milyen szoftverre és hardverre van pénz?
- Milyen a konfigurálási igény

Teszteredmények: Átlagos szg., Win2000 forgalom 70-100 Mbit/s átviteli sebesség 1 Gbit/s LAN esetén.

A titkosítás és visszafejtés processzorigényes!

Extrém szükséglet (mese)

- Az iskola Windows 7-einek aktiválása csak a Sulinet hálózaton át lehetséges!



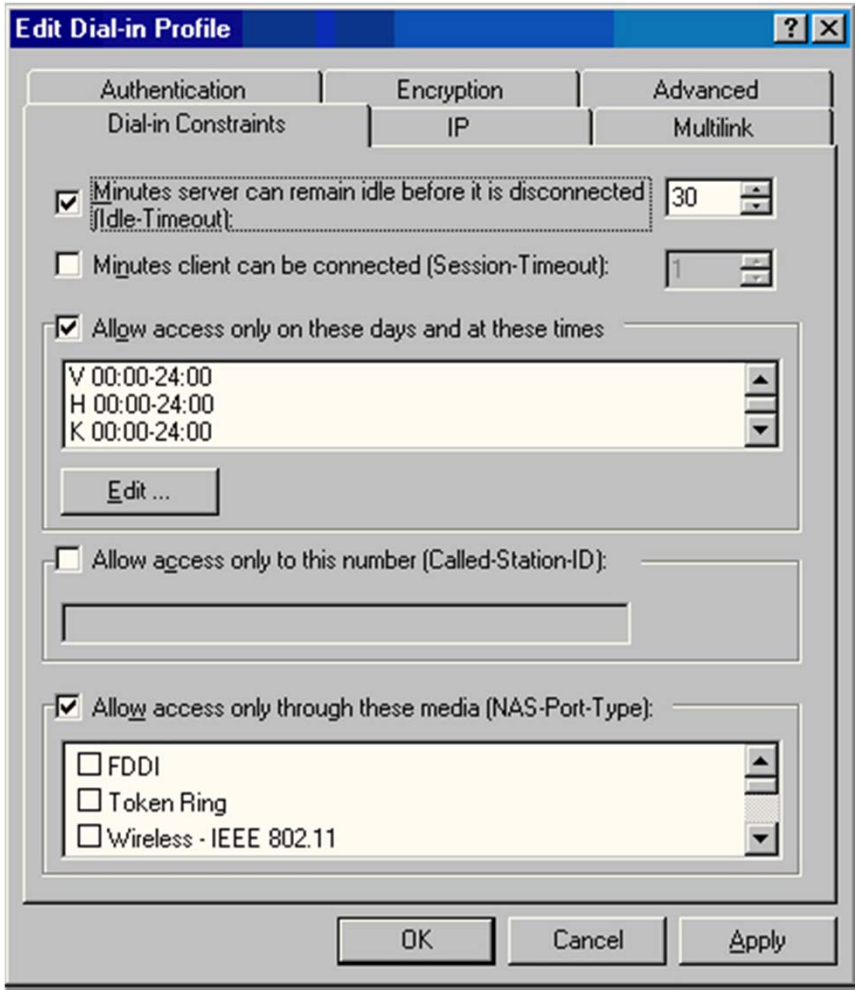
A használt eszközök

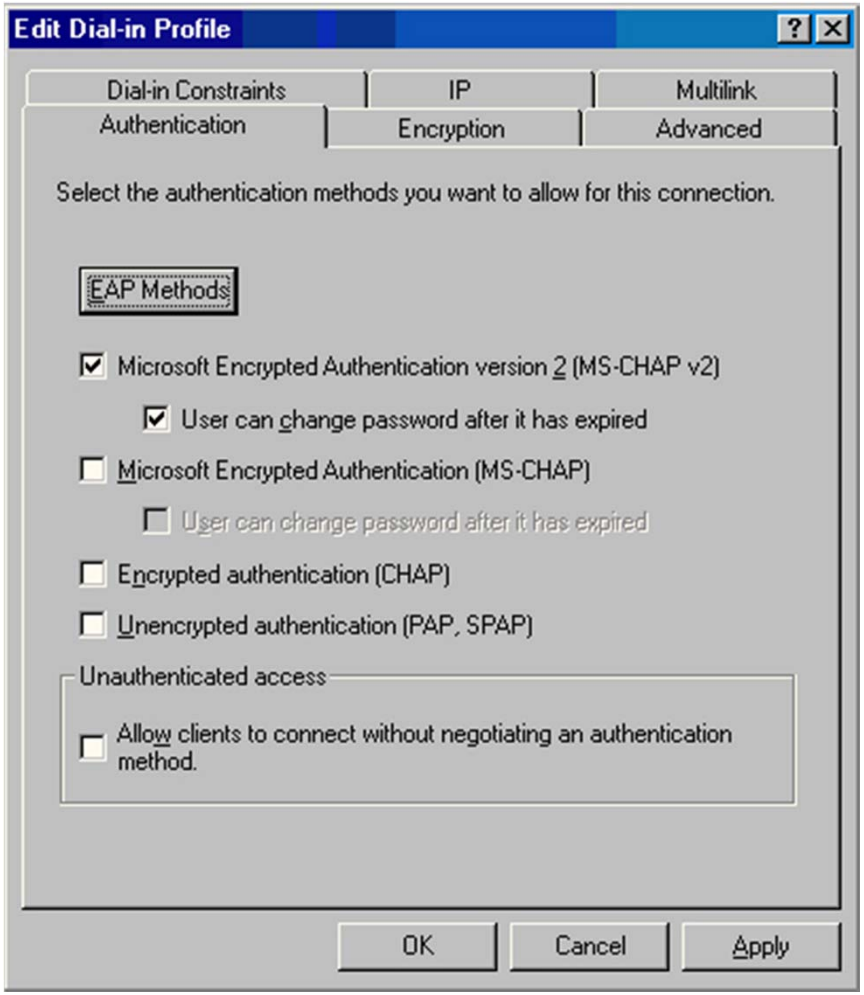
- Notebook
  - Ethernet csatoló – ehhez kapcsoltuk a tanterem LAN-ját
  - Wifi – ezzel kapcsolódott az iskolai hálózatra
  - VPN kliensként működik!
- VPN szerver
  - Notebook interneten keresztül belép a másik iskola szerverén lévő VPN kliensre (Virtuális Hálózati kártya a szerveren)
  - A szerveren routolják a forgalmat a fizikai hálózat felé – Sulinetes hálózat

Az RRAS-hoz szükséges Windows 2003 komponensek

- Az RRAS eleve fent van a szerveren
- Távelérési házirendek
  - Üresjárat, max. munkamenet hossza, időbeli szigorítás, stb.
- Connection Manager használata
- RADIUS (IAS) támogatás
  - Hitelesítés és házirendek központilag
- VPN karantén (csak W2K3)
  - A VPN kliensek rendszabályozásához

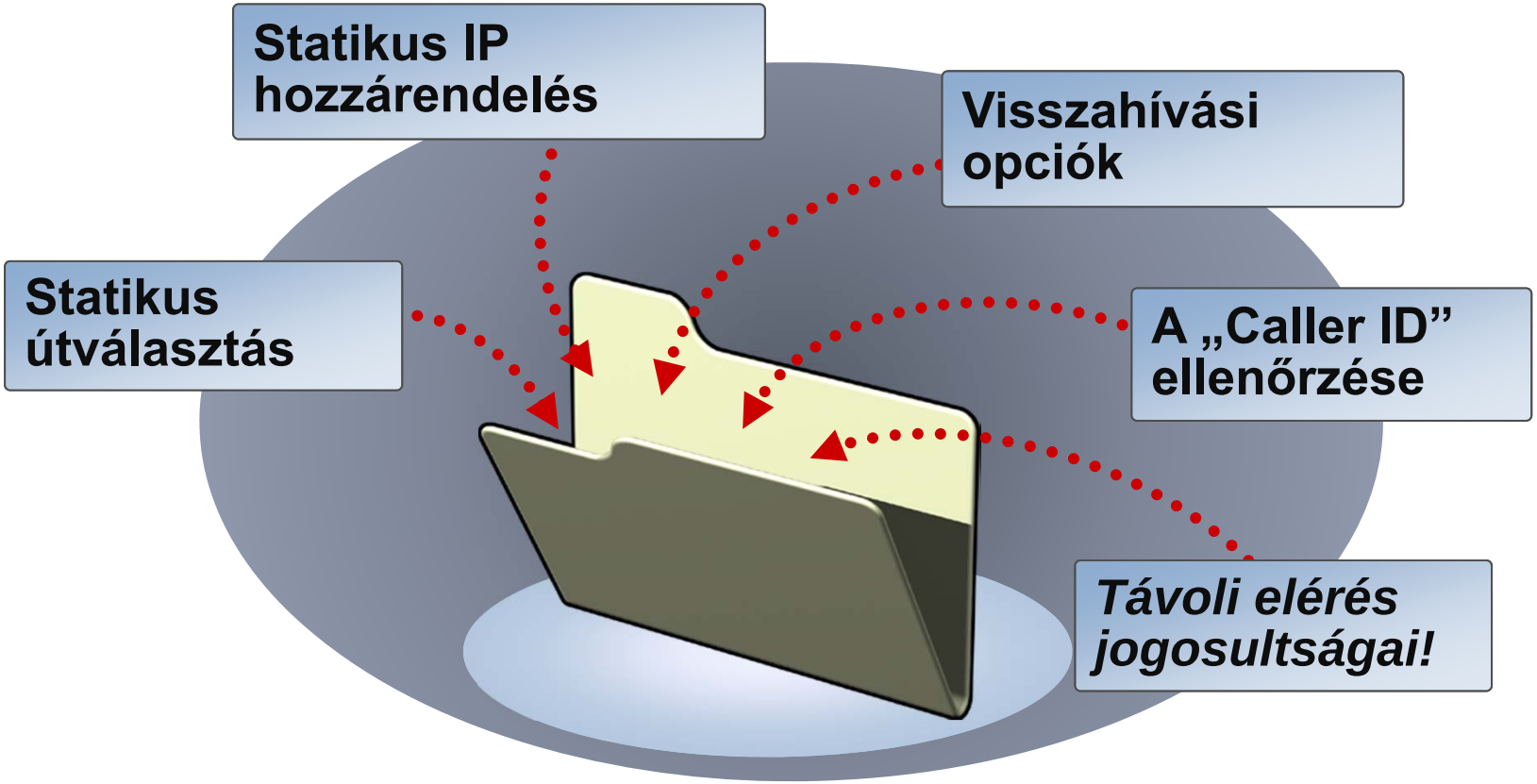
Windows Server 2003 komponensek





Windows Server 2003 komponensek

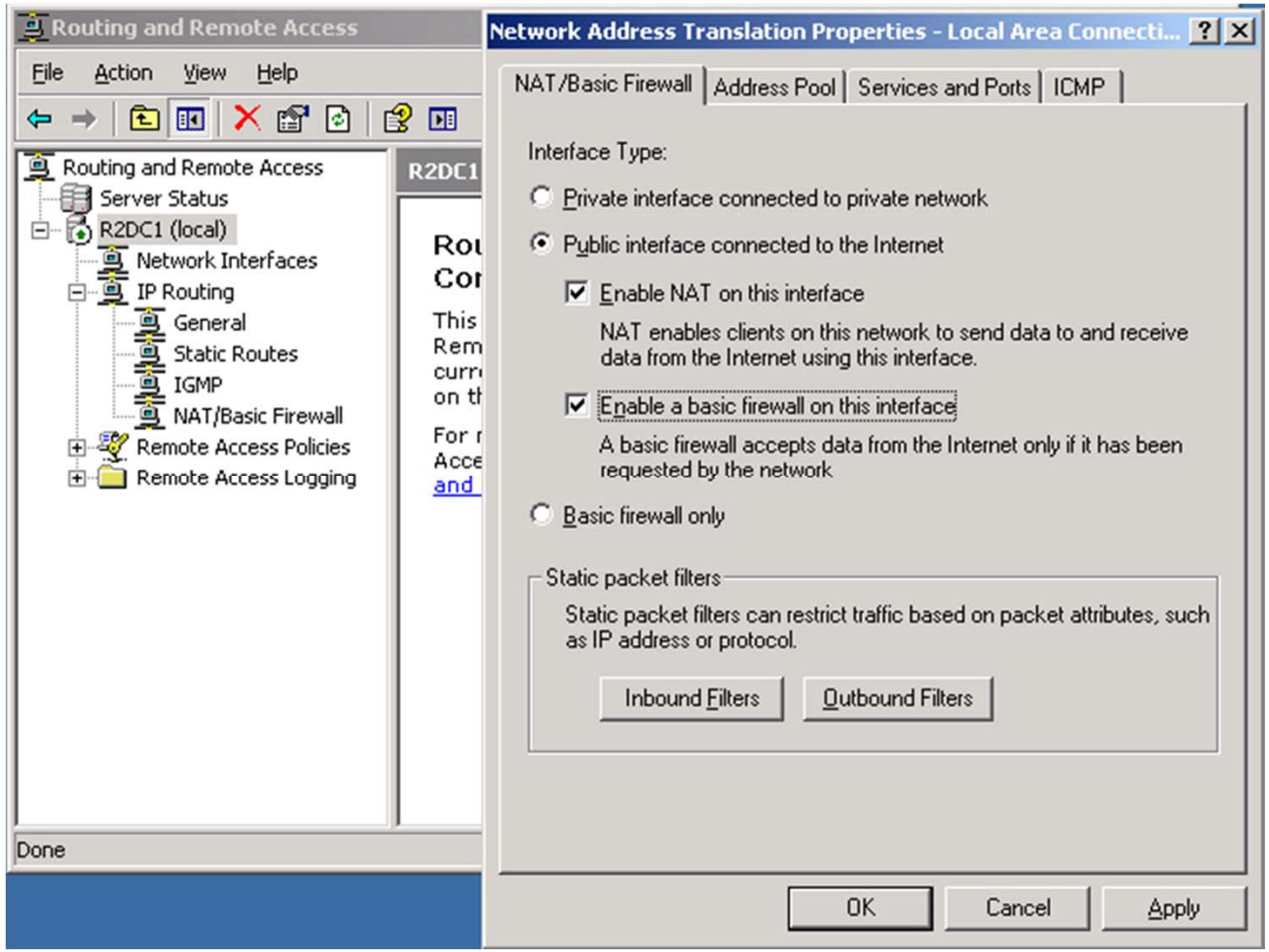
RRAS beállítások a címtárban



RRAS Tűzfal

- Statikus szűrés + basic tűzfal beépítve
  - DMZ-be, vagy ki a nyílt Netre
  - Semmi extra
  - Statikus szűrési lehetőségek
    - Forrás, cél, port száma, iránya
  - Alap tűzfal
    - VPN képes és NAT képes
- A Windows 2003 Server saját tűzfalát ki kell kapcsolni

RRAS Firewall beállítási lehetőségei



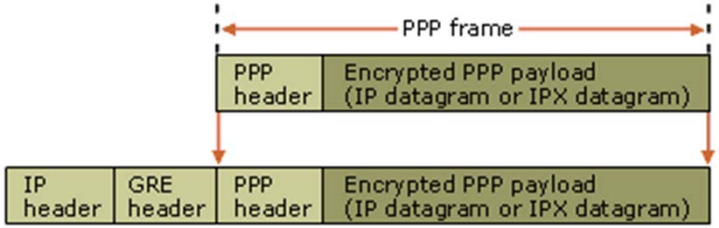
RRAS parancssorból is konfigurálható
Elengedett kézzel ülni a bikán? Ez extrém sport ☺

- Netsh parancs használata
  - Netsh ras add authtype add authtype [type =] PAP|SPAP|MD5CHAP|MSCHAP|MSCHAPv2|EAP
  - Netsh ras add registeredserver
  - Netsh ras add multilink [type =] MULTI|BACP
  - Netsh ras aaaa set authentication [provider =] WINDOWS|RADIUS
  - Netsh ras dump > “<filename>”
  - Netsh exec “<filename>”

VPN protokollok (PPP, PPTP)

- Point-2-Point (Win98, NT 4)
  - TCP-IP alapú bujtató szolgáltatás
- PPTP (Point-to-Point Tunneling Protocol) (Windows XP, Windows 2003)
  - A PPP (Point-To-Point) protokoll továbbfejlesztése
  - Feladatai: Hitelesítés, Titkosítás, Adattömörítés
  - Hitelesítés, titkosítás: MS-CHAP, az MS-CHAP v2, PKI támogatás is > SmartCard (EAP-TLS)
  - Egyszerűen NAT-olható
  - Egyszerű, gyorsan beüzemelhető, biztonságos

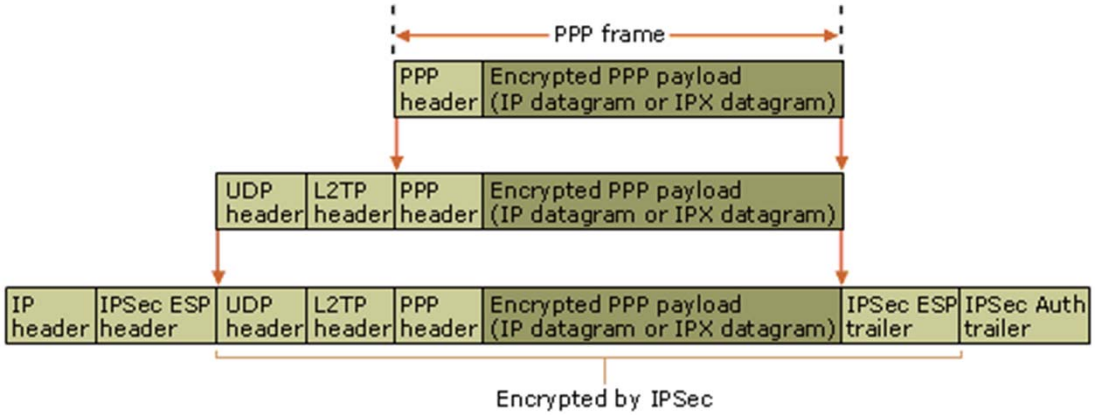
- Az eredeti adat a PPP frame-ben helyezkedik el. A PPP frame áll egy PPP headerből és a titkosított IP vagy IPX csomagból
- A protokoll egy új IP headert (forrás- és cél címzeit) és egy általános routing fejlécet tesz hozzá



VPN protokoll (L2TP)

- L2TP (Layer Two Tunneling Protocol)
  - Tanúsítvány alapú hitelesítés
  - Az IPSec protokollon alapul
  - A TCP/IP protokollal együtt kell telepíteni
  - PKI infrastruktúra szükséges
    - Azaz lényegesen bonyolultabb a beüzemelése, viszont fokozottan biztonságos

- A titkosított IP csomag + a PPP keret kap egy UDP fejlécet, egy L2TP fejlécet.
- Az így kapott csomag elé egy IP fejléc és egy IPSEC fejéc kerül,
  a csomag végére egy IPSEC lezáró és egy IPSEC hitelesítési lezárót kap.



Site-to-site VPN

- **Kettő vagy több hálózat összekötése**
- **Távoli VPN kiszolgáló**
  - Szoftver / Hardver
- **PPTP v. L2TP / IPSec v. IPSec**
  - Megosztott kulcskezeléssel
- **Címkiosztás és útválasztás**
  - IP címtartomány a távoli hálózatnak
  - A forgalom tipikusan a két hálózat között szükséges
  - A „hídfők” egyben VPN routerek is

VPN karantén

- A VPN kliensnek alapesetben mindent szabad
- VPN karantén
  - Előre elkészített kliens oldali VPN kapcsolat telepítő exe program formájában
  - A kliens nem férhet hozzá bárhogyan, bármihez
- VPN karantén létrehozása
  - Engedélyezni kell a szerveren
  - Connection Manager Administration Kit segítségével, varázslóval lehet előállítani a fenti exe-t.
  - Kliensen testreszabott VPN kapcsolat lesz
  - A kliens a kész programot kapja, amit otthon feltelepít a gépére

RRAS beállítás és egy kliens konfigurálása - Screencast

- A screencast a Microsoft Magyarország által kiadott Rendszerfelügyelet Rendszergazdáknak című könyvhöz tartozik

  http://szpfiles.petriktiszk.hu/II-1-2c-RRAS-Infrastruktura.avi

- Ha a video lejátszása nem működne, akkor ezt a codecet kell hozzá letölteni:

  http://szpfiles.petriktiszk.hu/Video Codec.exe