Hálózatbiztonság

II. rész

NAT összefoglalás

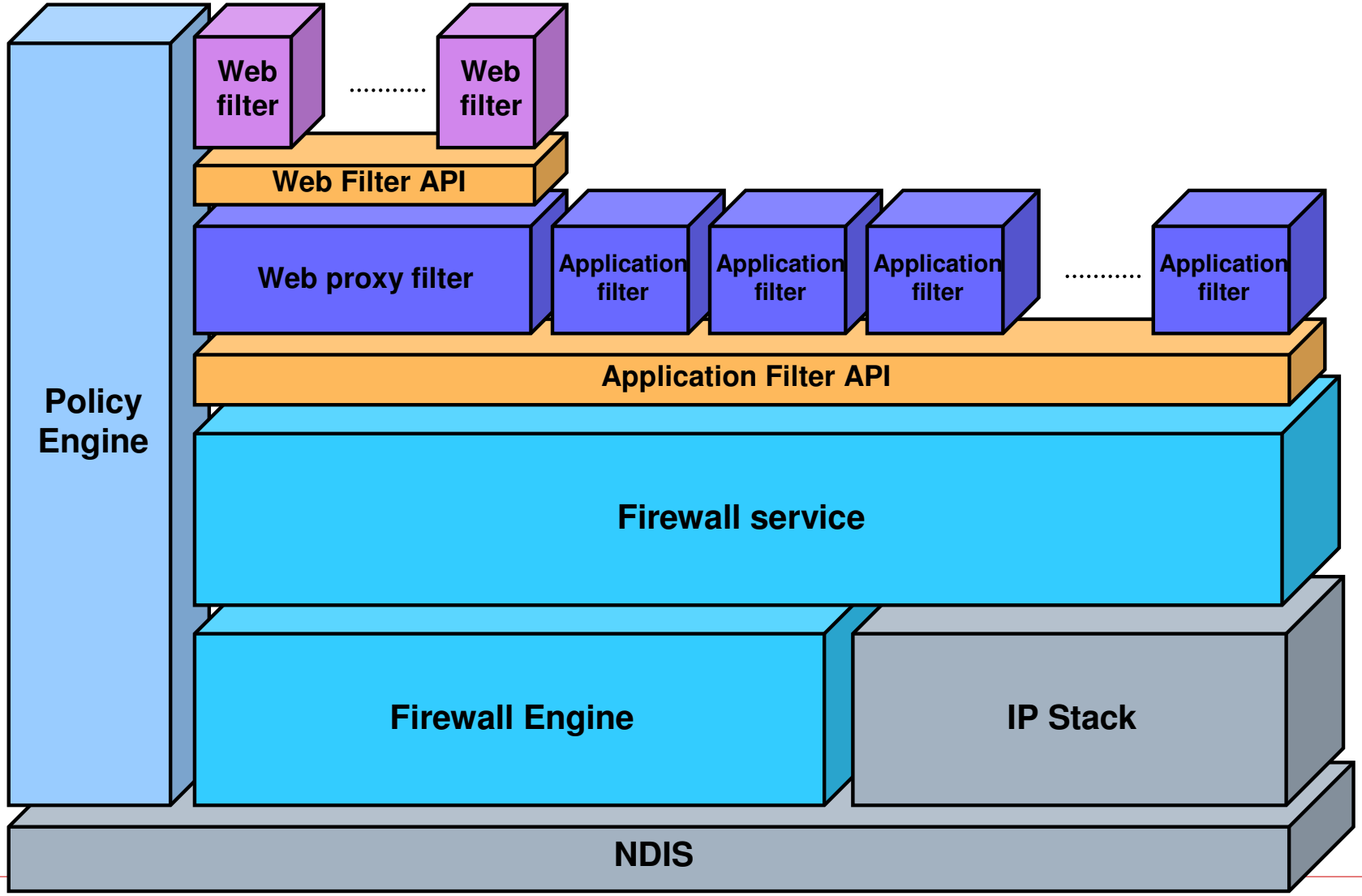
- Aggregálás egy multiplexelési szint elvesztésével (IP<->port)
- Beavatkozás a vég-vég kapcsolatba
- Körültekintéssel használható
  - Nem NATolható protokollok
  - Másodlagos kapcsolatok
  - Korlátozott tűzfalfunkció
- Kínában 3-4-szeres NATolás van

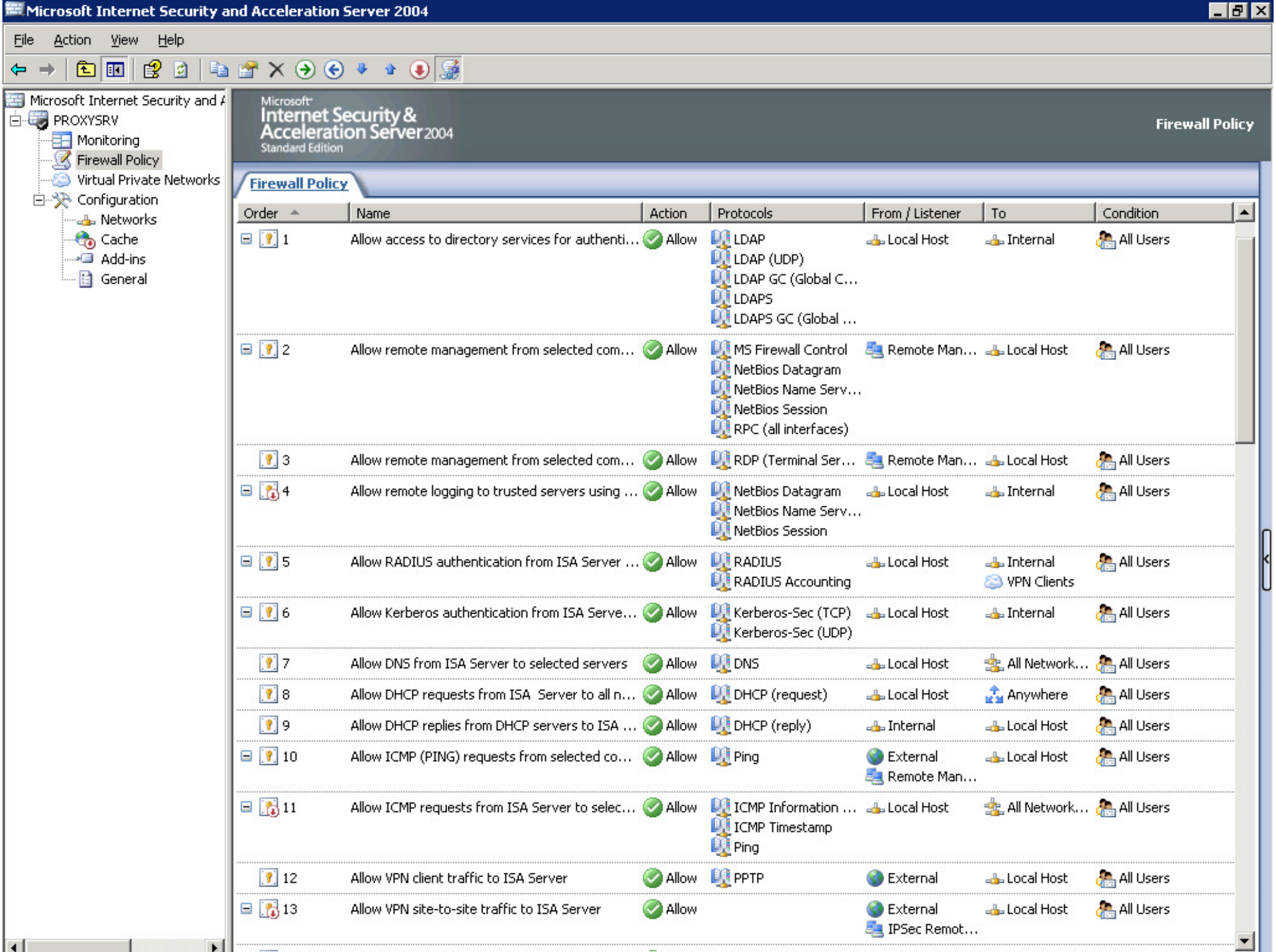
Tűzfalak

Tűzfal szolgáltatásai

- Szabály alapú forgalomszűrés és továbbítás
- Tűzfal működési típusok
  - állapotalapú (stateful) vagy állapotmentes (stateless)
  - NAT vagy routing
  - Közzététel (publishing) támogatása
  - Protokoll és alkalmazás szintű szűrés támogatása (alkalmazás tűzfal)
- Egyéb funkciók
  - Proxy
    - Gyorsítótárral
    - HTTP és FTP forgalomra
  - VPN kiszolgáló
  - Monitorozás, naplózás, riasztás, jelentések

Egy korszerű tűzfal-architektúra

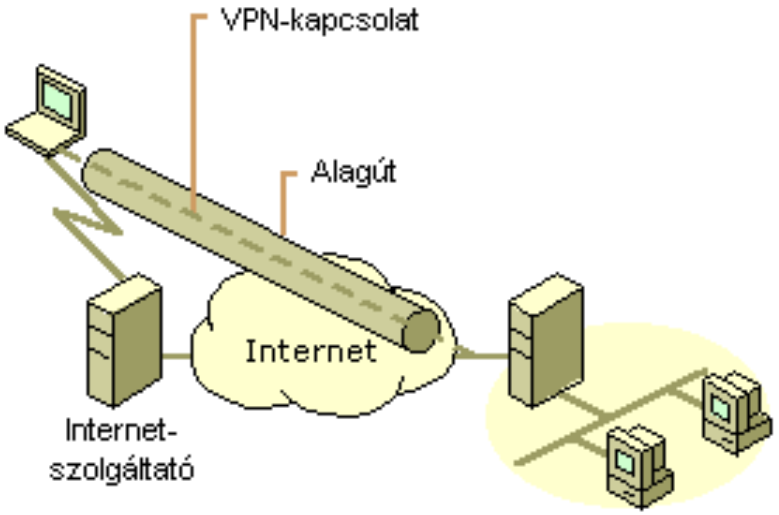



Microsoft Internet Security and Acceleration Server 2004
File Action View Help
Microsoft Internet Security and A
PROXYSRV
Monitoring
Firewall Policy
Virtual Private Networks
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004 Standard Edition
Firewall Policy
Firewall Policy
Order
Name
Action
Protocols
From / Listener
To
Condition
1 Allow access to directory services for authenti... Allow LDAP; LDAP (UDP); LDAP GC (Global C...; LDAPS; LDAPS GC (Global ... Local Host Internal All Users
2 Allow remote management from selected com... Allow MS Firewall Control; NetBios Datagram; NetBios Name Serv...; NetBios Session; RPC (all interfaces) Remote Man... Local Host All Users
3 Allow remote management from selected com... Allow RDP (Terminal Ser... Remote Man... Local Host All Users
4 Allow remote logging to trusted servers using ... Allow NetBios Datagram; NetBios Name Serv...; NetBios Session Local Host Internal All Users
5 Allow RADIUS authentication from ISA Server ... Allow RADIUS; RADIUS Accounting Local Host Internal; VPN Clients All Users
6 Allow Kerberos authentication from ISA Serve... Allow Kerberos-Sec (TCP); Kerberos-Sec (UDP) Local Host Internal All Users
7 Allow DNS from ISA Server to selected servers Allow DNS Local Host All Network... All Users
8 Allow DHCP requests from ISA Server to all n... Allow DHCP (request) Local Host Anywhere All Users
9 Allow DHCP replies from DHCP servers to ISA ... Allow DHCP (reply) Internal Local Host All Users
10 Allow ICMP (PING) requests from selected co... Allow Ping External; Remote Man... Local Host All Users
11 Allow ICMP requests from ISA Server to selec... Allow ICMP Information ...; ICMP Timestamp; Ping Local Host All Network... All Users
12 Allow VPN client traffic to ISA Server Allow PPTP External Local Host All Users
13 Allow VPN site-to-site traffic to ISA Server Allow External; IPSec Remot... Local Host All Users

VPN – Virtual Private Network

Virtuális magánhálózat

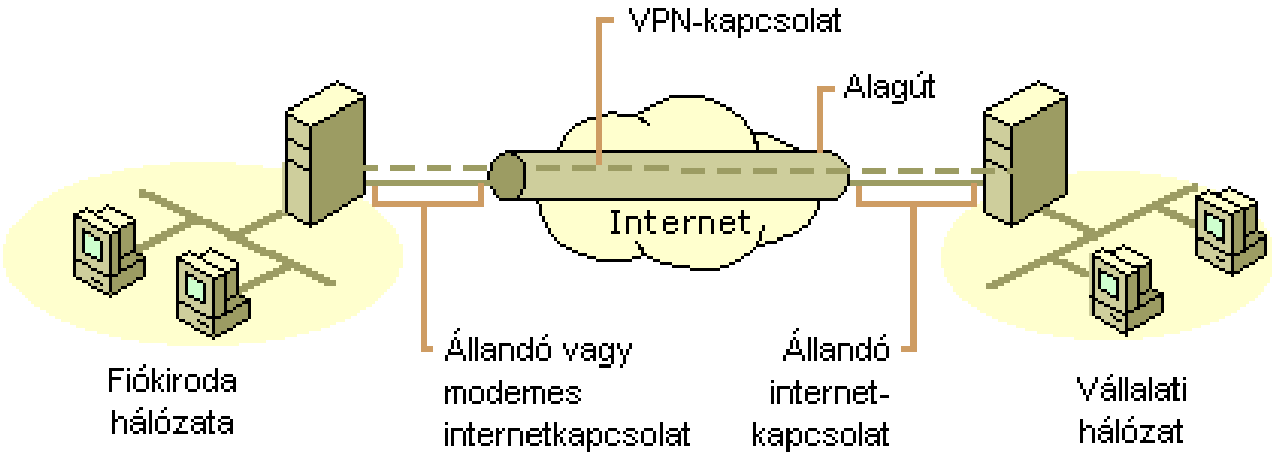
VPN az ügyfél típusa szerint



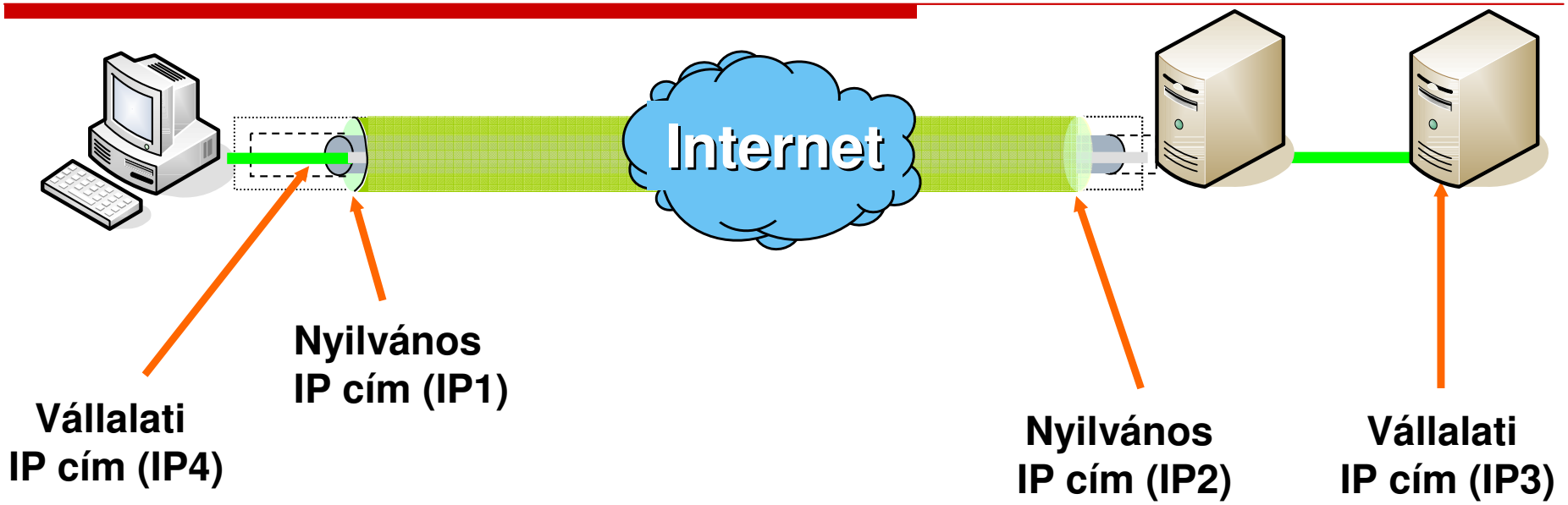
Ügyfél-kiszolgáló

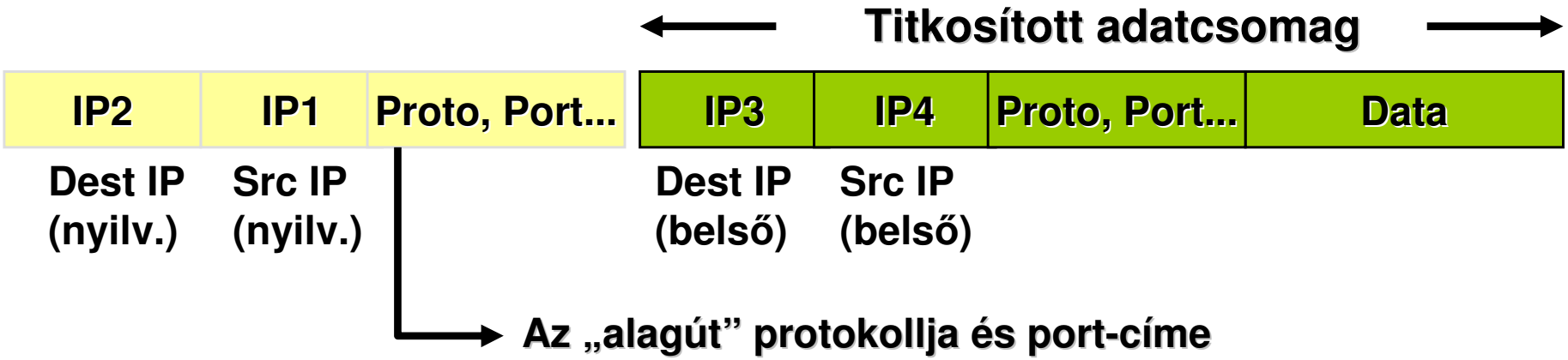
Kiszolgáló-kiszolgáló

Router-to-Router



„Alagúthálózat”





VPN protokollok

- PPTP - Point to Point Tunneling Protocol
  - Hitelesítés:
    - EAP (tanúsítvány), MS-CHAPv2, CHAP, PAP
  - Titkosítás:RC4
  - Kommunikáció:
    - PPTP Control Connection: TCP 1723 port
    - Adatforgalom (GRE): IP 47
- L2TP (+IPsec) - Layer 2 Tunneling Protocol
  - Cisco L2F alapokon nyugszik (RFC 2661)
  - UDP kommunikáció, 1701-es port
    - Az adat és a kontrollforgalomhoz egyaránt
    - Az IPSec titkosítás ezt a portot elrejti
  - Hitelesítés: EAP, MS-CHAPv2, CHAP, PAP
  - Titkosítás:IPSec
- Natív IPsec

Összefoglalás

- AAA
  - Hitelesítés
  - Jogosultságkezelés
  - Számlázás
- Titkosítás
- NAT – Hálózati címfordítás
- Tűzfalak
- VPN – Virtuális magánhálózat