

## Parancssorban

A tűzfal állapotának lekérdezése:

**netsh advfirewall show allprofiles state**

A tűzfal letiltása - minden profilban:

**netsh advfirewall set allprofiles state off**

A tűzfal engedélyezése - minden profilban:

**netsh advfirewall set allprofiles state on**

## Grafikus felületen

Windows tűzfal (Vezérlőpult\Rendszer és biztonság\Windows Defender tűzfal):

**firewall.cpl**

Fokozott biztonságú Windows tűzfal:

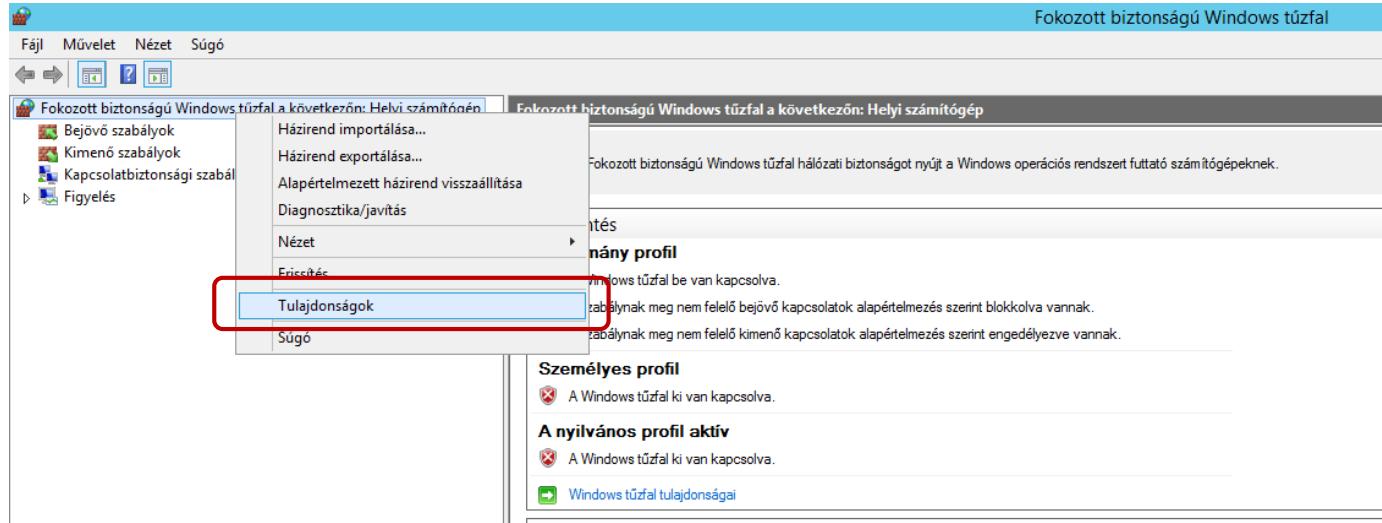
**wf.msc**

## Tűzfal beállítása (Windows szerveren)

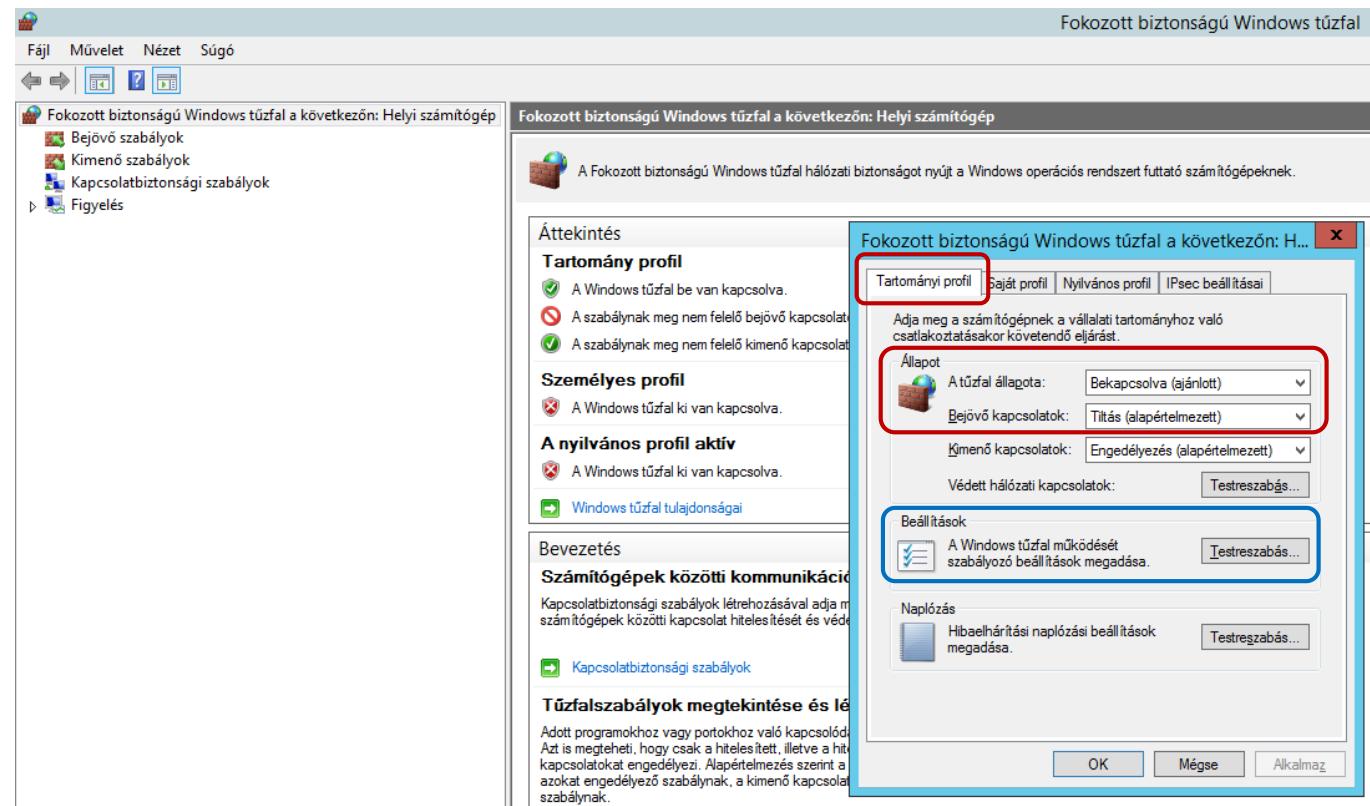
Indítsuk el a szerveren a **Fokozott biztonságú Windows tűzfal** kezelőjét:

(Kiszolgálókezelő / Eszközök menü / Fokozott biztonságú Windows tűzfal)

Nyissuk meg a Fokozott biztonságú Windows tűzfal *tulajdonság lapját*:



A tűzfalon **Profilokhoz** rendelve állíthatjuk **Be/Ki** állapotba a tűzfalat; illetve, hogy a **Bejövő- és Kimenő kapcsolatokat** engedélyezzük, avagy tiltjuk. Alapértelmezetten minden enged kifelé és minden tilt befelé.



A **Beállítások / Teszteszabás...** gombra kattintva kérhetünk értesítést a tűzfaltól, ha egy program szeretne a tűzfalon átjutni, de nem jogosult.

A Bejövő szabályokra kattintva kapunk egy listát azokról a szabályokról, amelyek engedélyeznek vagy tiltanak a **BEFELÉ** irányban, azaz **a szerver felé érkező kérésekre** vonatkozó szabályok.

Fokozott biztonságú Windows tűzfal						
Fájl	Művelet	Nézet	Súgó			
<b>Felügyelt biztonságú Windows tűzfal a következőn: Helyi számítógép</b>						
Bejövő szabályok	Csoport	Profil	Engedélyezve	Művelet	Felülbírálás	
Bejövő szabályok	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Kimenő szabályok	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Kapcsolatbiztonsági szabályok	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Pélyelés	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
<b>Bejövő szabályok</b>						
Név						
Active Directory-tartomány-vezérlő - echo request (ICMPv4, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - echo request (ICMPv6, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - Biztonságos LDAP (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - Biztonságos LDAP a globális katalógushoz (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - LDAP (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - LDAP (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - LDAP a globális katalógushoz (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - NetBIOS-névfordítás (UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - SAM/LSA (NP-TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - SAM/LSA (NP-UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő - W32Time (NTP-UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő (RPC)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory-tartomány-vezérlő (RPC-EPMAP)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem	
Active Directory webszolgáltatások (TCP, bejövő)	Active Directory webszolgáltatások	Mind	Igen	Megeng...	Nem	
Webszolgáltatások (bejövő HTTPS-forgalom)	Biztonságos webszolgáltatások (HTTPS)	Mind	Igen	Megeng...	Nem	
BranchCache Content Retrieval (HTTPI-n)	BranchCache - Content Retrieval (Uses HTTP)	Mind	Nem	Megeng...	Nem	
BranchCache Hosted Cache Server (HTTPI-n)	BranchCache - Hosted Cache Server (Uses HTTPS)	Mind	Nem	Megeng...	Nem	
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discovery (Uses WSD)	Mind	Nem	Megeng...	Nem	
Certification Authority Enrollment and Management Protocol (CERTSVC-DCOM-IN)	Certification Authority	Mind	Igen	Megeng...	Nem	
Certification Authority Enrollment and Management Protocol (CERTSVC-RPC-EPMAP-IN)	Certification Authority	Mind	Igen	Megeng...	Nem	
Certification Authority Enrollment and Management Protocol (CERTSVC-RPC-NP-IN)	Certification Authority	Mind	Igen	Megeng...	Nem	

Ez egy hosszú lista a **Bejövő**- és **Kimenő szabályok** esetén is.

Lehet rendezni (pl. *csoport*, *portszám*, *protokoll* szerint):

Fokozott biztonságú Windows tűzfal					
Fajl	Művelet	Nézet	Súgó		
<b>Fokozott biztonságú Windows tűzfal a következőn: Helyi számítógép</b>					
Bejövő szabályok Kimenő szabályok Kapsolatlebontási szabályok Figyelés					
<b>Bejövő szabályok</b>					
Név	Csoport	Profil	Engedélyezve	Művelet	Felülbírálás
Active Directory-tartományvezérlő - echo request (ICMPv4, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartományvezérlő - echo request (ICMPv6, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - Bázisági LDAP (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - Bázisági LDAP a globális katalógushoz (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - LDAP (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - LDAP (UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - LDAP a globális katalógushoz (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - NetBIOS-rekordok (UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - SAM11SA (NP-UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - SAM11SA (NP-UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - W2k3ime (NTP-UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - W2k3ime (NTP-UDP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - W2k3ime (RPC)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Active Directory-tartomány-vezérlő - W2k3ime (TCP, bejövő)	Active Directory-tartomány szolgáltatások	Mind	Igen	Megeng...	Nem
Webböngészők (Bejövő HTTPS-forgalom)	Active Directory-webböngészők	Mind	Igen	Megeng...	Nem
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retrieval (Uses HTTP)	Mind	Nem	Megeng...	Nem
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache Server (Uses HTTPS)	Mind	Nem	Megeng...	Nem
BranchCache Peer Discovery (Uses WSD)	BranchCache - Peer Discovery (Uses WSD)	Mind	Nem	Megeng...	Nem
Certification Authority Enrollment and Management Protocol (CERTSVC-DCOM-IN)	Certification Authority	Mind	Igen	Megeng...	Nem
Certification Authority Enrollment and Management Protocol (CERTSVC-RPC-EPMAP-IN)	Certification Authority	Mind	Igen	Megeng...	Nem
Certification Authority Enrollment and Management Protocol (CERTSVC-RPC-NP-IN)	Certification Authority	Mind	Igen	Megeng...	Nem
Certification Authority Enrollment and Management Protocol (CERTSVC-RPC-TCP-IN)	Certification Authority	Mind	Igen	Megeng...	Nem
COM-háttérzáró hozzáférés (DCOM-In)	COM-háttérzáró hozzáférés	Mind	Nem	Megeng...	Nem
COM-kétfelügyelet (DCOM-In)	COM-kétfelügyelet	Mind	Nem	Megeng...	Nem
DHCPv4-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	Igen	Megeng...	Nem
DHCPv4-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	Igen	Megeng...	Nem
DHCPv4-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	Igen	Megeng...	Nem
DHCPv4-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	Igen	Megeng...	Nem
DHCPv4-kiszolgáló - Távoli szolgáltatás-felügyelet SCIM használatával (RPC, bejövő)	DHCP-kiszolgáló felügyelete	Mind	Igen	Megeng...	Nem
DHCP-kiszolgáló (RPC-In)	DHCP-kiszolgáló felügyelete	Mind	Igen	Megeng...	Nem
DHCP-kiszolgáló (RPCSS-In)	DHCP-kiszolgáló felügyelete	Mind	Igen	Megeng...	Nem
DHCP-kiszolgáló (SMB, bejövő)	DHCP-kiszolgáló felügyelete	Mind	Igen	Megeng...	Nem
DHCP-kiszolgáló feladatainak kezelése (TCP, bejövő)	DHCP-kiszolgáló felügyelete	Mind	Igen	Megeng...	Nem
DHCPv4-továbbítók (Layer4) (UDP-Be)	DHCP-továbbítók (Layer4)	Mind	Igen	Megeng...	Nem
DHCPv4-továbbítók (Layer4) [Kiszolgáló] (UDP-In)	DHCPv4-továbbítók (Layer4)	Mind	Igen	Megeng...	Nem
DNS (TCP, Incoming)	DNS Service	Mind	Igen	Megeng...	Nem
DNS (UDP, Incoming)	DNS Service	Mind	Igen	Megeng...	Nem
RPC (TCP, Incoming)	DNS Service	Mind	Igen	Megeng...	Nem
RPC Endpoint Mapper (TCP, Incoming)	DNS Service	Mind	Igen	Megeng...	Nem
Elosztott fájrlrendszerek kezelése (DCOM-In)	Elosztott fájrlrendszerek kezelése	Mind	Igen	Megeng...	Nem

Lehet szűrni (pl. *profil*, *csoport*, *portszám*, *protokoll* szerint):

Van lehetőség a **csoport nélküli** (pl. általunk létrehozott) szabályok szűrésére is:

The screenshot shows the 'Fokozott biztonságú Windows tűzfal' (Advanced Firewall) application window. The left sidebar lists categories: 'Bejövő szabályok', 'Kimenő szabályok', 'Kapcsolatbiztonsági szabályok', and 'Figyelés'. The main area has a title bar 'Fokozott biztonságú Windows tűzfal' and a toolbar with icons for 'Fájl', 'Művelet', 'Nézet', and 'Súgó'. A red box highlights the 'Bejövő szabályok' section, which contains a table with columns: Név, Csoport, Profil, Engedélyezve, Művelet, Felülírás, and Program. One row is selected: 'Passzív FTP-Egyedi szabály'. The right sidebar shows a 'Műveletek' (Actions) menu with options like 'Új szabály...', 'Szűrés profil alapján', 'Szűrés állapot alapján', 'Szűrés csoport alapján', 'Az összes szűrő törlése', 'Netzett', 'Frissítés', and 'Lista exportálása...'. The status bar at the bottom shows 'Fokozott biztonságú Windows tűzfal a következőben: Helyi számítógép'.

## Szűrés egy adott szolgáltatásra (pl. *DHCP*, *DNS* vagy *Active Directory* tartományi szolgáltatások alapján)

Fokozott biztonságú Windows tűzfal

**Bejövő szabályok** Szűrés Active Directory tartományi szolgáltatások alapján

Név	Csoport	Profil	Engedélyezve	Művelet	Felülvizualizáció	Program
Active Directory-tartományvezérlő - echo request (ICMPv4, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	Bármely
Active Directory-tartományvezérlő - echo request (ICMPv6, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	Bármely
Active Directory-tartományvezérlő - Bitárosos LDAP (TCP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő - Bitárosos LDAP a globális katalógushoz (TCP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő - LDAP (TCP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő - LDAP (UDP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő - LDAP a globális katalógushoz (TCP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő - NetBIOS-névteljesítés (UDP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	System
Active Directory-tartományvezérlő - SAM/LSA (NP-TCP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	System
Active Directory-tartományvezérlő - SAM/LSA (NP-UDP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő - W32Time (NTP-UDP, bejövő)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő (RPC)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Active Directory-tartományvezérlő (RPC-EPMAP)	Active Directory tartományi szolgáltatások	Mind	Igen	Megengedés	Nem	%SystemRoot%\System

**Műveletek**

- Bejövő szabályok
- Új szabály...
- Szűrés profil alapján
- Szűrés állapot alapján
- Szűrés csoport alapján
- Az összes szűrő törlése
- Nézet
- Frisítés
- Lista exportálása...
- Súgó

## A szabályok Engedélyezhetőek / Tilthatóak

Fokozott biztonságú Windows tűzfal

**Bejövő szabályok**

Név	Csoport	Profil	Engedélyezve	Művelet	Felülvizualizáció	Program
IPC Endpoint Mapper (TCP, Incoming)	DNS Service	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Elosztott fájlrendszer kezelése (DCOM-In)	Elosztott fájlrendszer kezelése	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Elosztott fájlrendszer kezelése (SMB-In)	Elosztott fájlrendszer kezelése	Mind	Igen	Megengedés	Nem	System
Elosztott fájlrendszer kezelése (TCP-In)	Elosztott fájlrendszer kezelése	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Elosztott fájlrendszer kezelése	Elosztott fájlrendszer kezelése	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Elosztott fájlrendszer replikációs szolgáltatása (RPC-EPMAP)	Elosztott fájlrendszer replikációs szolgáltatás	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Elosztott fájlrendszer replikációs szolgáltatása (RPC-In)	Elosztott fájlrendszer replikációs szolgáltatás	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Elosztott transzakciós koordinátora (RPC)	Elosztott transzakciós koordinátora	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Elosztott transzakciós koordinátora (RPC-EPMAP)	Elosztott transzakciós koordinátora	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Elosztott transzakciós koordinátora (TCP, bejövő)	Elosztott transzakciós koordinátora	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Fájl- és nyomatékoncigazság (Echo kérés - ICMPv4-be)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	Bármely
Fájl- és nyomatékoncigazság (Echo kérés - ICMPv6-be)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	Bármely
Fájl- és nyomatékoncigazság (LLMNR-UDP, bejövő)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Fájl- és nyomatékoncigazság (NetBIOS-datagram, bejövő)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	System
Fájl- és nyomatékoncigazság (NetBIOS-munkamenet, bejövő)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	System
Fájl- és nyomatékoncigazság (NetBIOS-név, bejövő)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	System
Fájl- és nyomatékoncigazság (Sorképzeli szolgáltatás - RPC)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Fájl- és nyomatékoncigazság (Sorképzeli szolgáltatás - RPC-EPMAP)	Fájl- és nyomatékoncigazság	Mind	Igen	Megengedés	Nem	Bármely
Fájl- és nyomatékoncigazság (SMBDirect használatával) (IWARP, bejövő)	Fájl- és nyomatékoncigazsás SMBDirect	Mind	Nem	Megengedés	Nem	System
Fájlkiszolgáló távoli felügyelete (DCOM-In)	Fájlkiszolgáló távoli felügyelete	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Fájlkiszolgáló távoli felügyelete (SMB-In)	Fájlkiszolgáló távoli felügyelete	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Fájlkiszolgáló távoli felügyelete (WMI-In)	Fájlkiszolgáló távoli felügyelete	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Fájleréplikáció (RPC)	Fájleréplikáció	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Fájleréplikáció (RPC-EPMAP)	Fájleréplikáció	Mind	Igen	Megengedés	Nem	%SystemRoot%\System
Bitárosos FTP-kiszolgáló (bejövő SSL-FTP-forgalom)	FTP-kiszolgáló	Mind	Igen	Megengedés	Nem	%windir%\System
FTP-kiszolgáló (bejövő FTP-forgalom)	FTP-kiszolgáló	Mind	Igen	Megengedés	Nem	%windir%\System
Passzív FTP-kiszolgáló (bejövő)	FTP-kiszolgáló	Mind	Igen	Megengedés	Nem	C:\Windows\system
Hálózati felderítése (LLMNR-UE)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Hálózati felderítése (NetBIOS-datagram)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	System
Hálózati felderítése (NetBIOS-név)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	System
Hálózati felderítése (nivályán VSI)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Hálózati felderítése (SSDP, bejövő)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Hálózati felderítése (Universal PnP)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	System
Hálózati felderítése (WSD EventSe)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Hálózati felderítése (WSD, bejövő)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	%SystemRoot%\System
Hálózati felderítése (WSD-eseményekbe)	Hálózati felderítése	Mind	Nem	Megengedés	Nem	%SystemRoot%\System

**Műveletek**

- Bejövő szabályok
- Új szabály...
- Szűrés profil alapján
- Szűrés állapot alapján
- Szűrés csoport alapján
- Az összes szűrő törlése
- Nézet
- Frisítés
- Lista exportálása...
- Súgó

Vegyük sorra a szerveren elérhető szerepköröket / szolgáltatásokat és a hozzájuk tartozó beállításokat

## DHCP

A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat!

Fokozott biztonságú Windows tűzfal

**Bejövő szabályok**

Név	Csoport	Profil	Program	Protokoll	Helyi port	Távoli pc
Certification Authority Enrollment and Management Protocol (CERTSVC-RPC-TC...	Certification Authority	Mind	%SystemRoot%\system32\certsvr.exe	TCP	Dinamikus RPC-port	Bármely
COM+ hálózati hozzáférés (DCOM-In)	COM+ hálózati hozzáférés	Mind	%SystemRoot%\system32\svchost.exe	TCP	135	Bármely
COM+ távfelügyelet (DCOM-In)	COM+ távfelügyelet	Mind	%SystemRoot%\system32\dhcpcsvc.exe	TCP	Dinamikus RPC-port	Bármely
DHCP-kiszolgáló - Távoli szolgáltatás-felügyelet SCM használatával (RPC, bejövő)	DHCP-kiszolgáló felügyelete	Mind	%SystemRoot%\system32\services.exe	TCP	Dinamikus RPC-port	Bármely
DHCP-kiszolgáló (RPC-In)	DHCP-kiszolgáló felügyelete	Mind	%SystemRoot%\system32\svchost.exe	TCP	Dinamikus RPC-port	Bármely
DHCP-kiszolgáló (RPCSS-In)	DHCP-kiszolgáló felügyelete	Mind	%SystemRoot%\system32\svchost.exe	TCP	RPC végpontról kepező	Bármely
DHCP-kiszolgáló (SMB, bejövő)	DHCP-kiszolgáló felügyelete	Mind	System	TCP	445	Bármely
DHCP-kiszolgáló feladatátvételle (TCP, bejövő)	DHCP-kiszolgáló felügyelete	Mind	%SystemRoot%\system32\svchost.exe	TCP	647	Bármely
DHCpv4-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	%SystemRoot%\system32\svchost.exe	UDP	67	Bármely
DHCpv4-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	%SystemRoot%\system32\svchost.exe	UDP	68	Bármely
DHCpv4-továbbítóügynök (Ügyfél) (UDP-Be)	DHCP-továbbítóügynök	Mind	%SystemRoot%\system32\svchost.exe	UDP	67	Bármely
DHCpv6-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	%SystemRoot%\system32\svchost.exe	UDP	546	Bármely
DHCpv6-kiszolgáló (UDP-In)	DHCP-kiszolgáló	Mind	%SystemRoot%\system32\svchost.exe	UDP	547	Bármely
DHCpv6-továbbítóügynök [Kiszolgáló] (UDP-In)	DHCPv6-továbbítóügynök	Mind	%SystemRoot%\system32\svchost.exe	UDP	547	Bármely
DNS (TCP, Incoming)	DNS Service	Mind	%SystemRoot%\system32\dns.exe	TCP	53	Bármely
DNS (UDP, Incoming)	DNS Service	Mind	%SystemRoot%\System32\dns.exe	UDP	53	Bármely
Elosztott fájlrendszer kezelése (DCOM-In)	Elosztott fájlrendszer kezel...	Mind	%SystemRoot%\system32\svchost.exe	TCP	135	Bármely
Elosztott fájlrendszer kezelése (SMB-In)	Elosztott fájlrendszer kezel...	Mind	System	TCP	445	Bármely
Elosztott fájlrendszer kezelése (TCP-In)	Elosztott fájlrendszer kezel...	Mind	%SystemRoot%\system32\dfsrshost...	TCP	Dinamikus RPC-port	Bármely

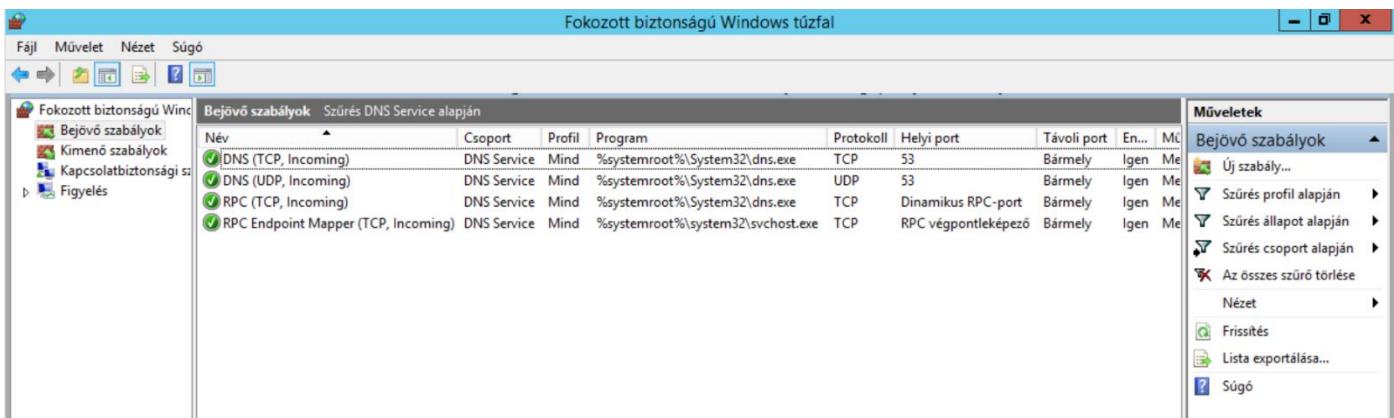
**Műveletek**

- Bejövő szabály...
- Új szabály...
- Szűrés...
- Szűrés...
- Nézet
- Frisítés
- Lista e...
- Súgó

- Kijelölt ...
- Szabál...
  - Kivágás
  - Másol...
  - Törles
  - Súgó

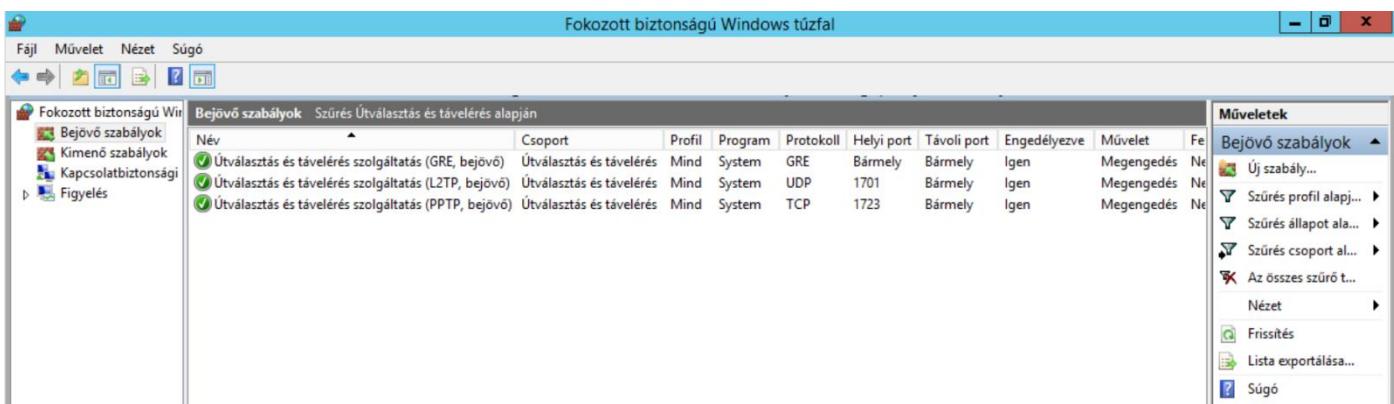
## DNS

A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat!



## Távelérés (VPN)

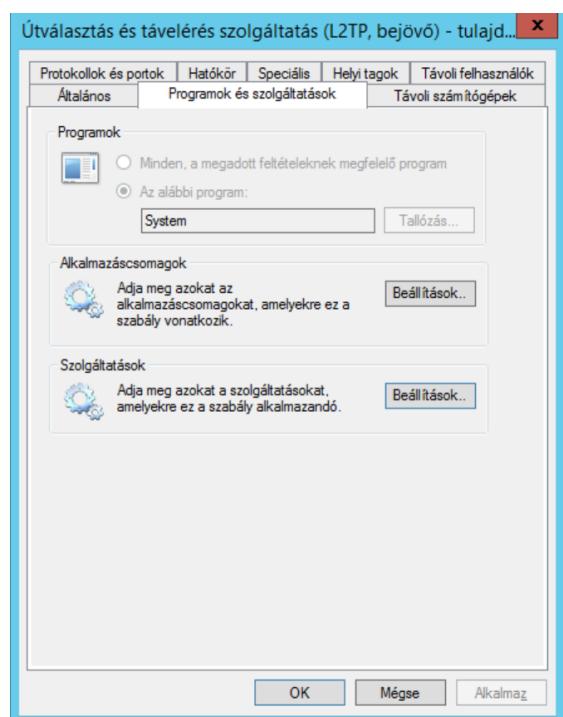
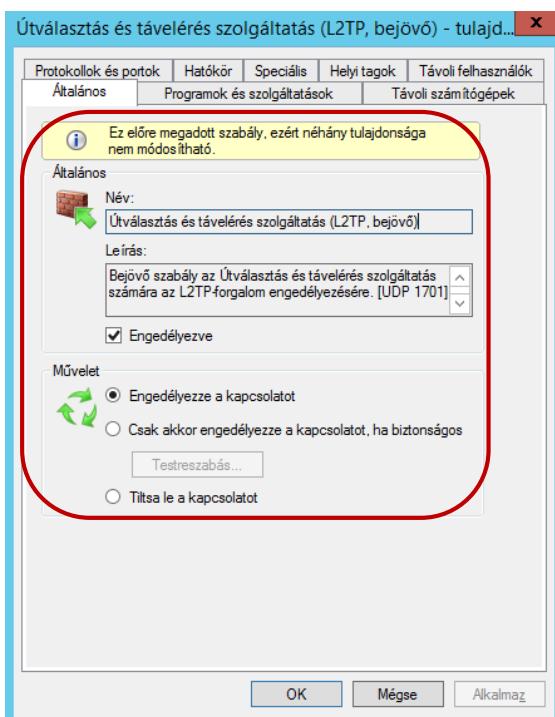
A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat!



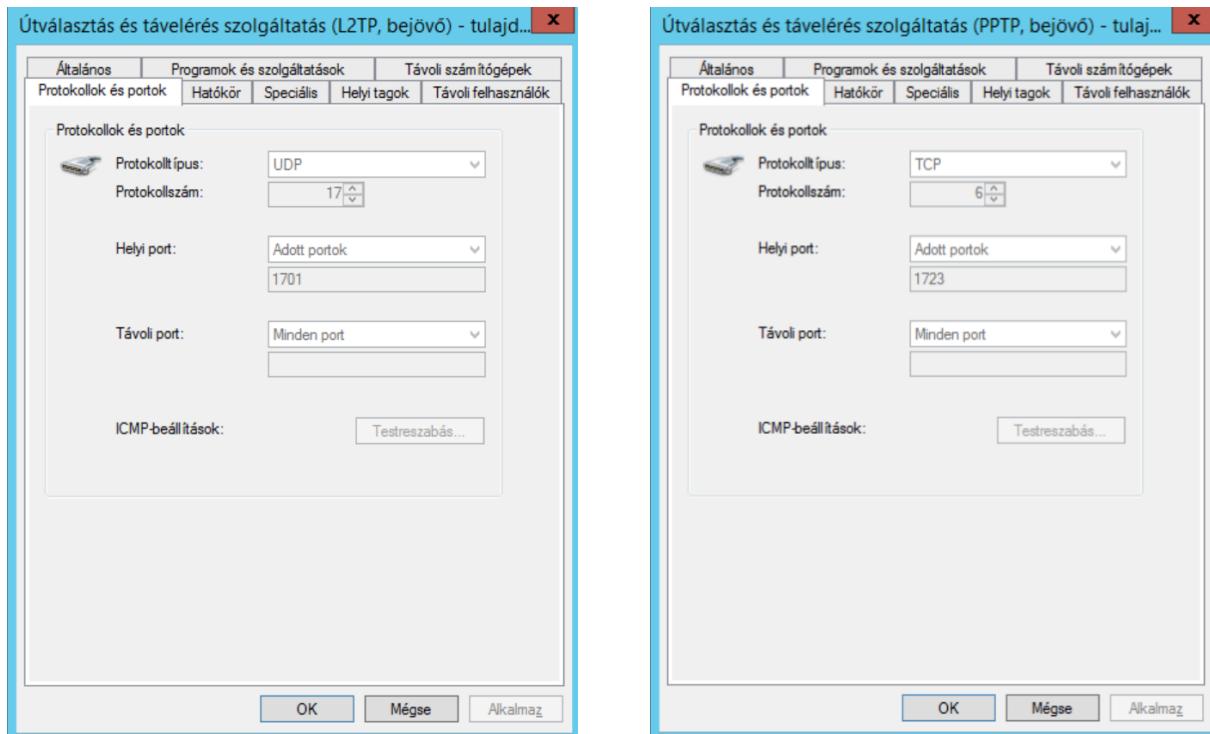
Ha az egyik ide tartozó szabályon duplán kattintva megnézhetjük a tulajdonságait. A képen az *L2TP protokollhoz* tartozó szabály részleteit látjuk. A rendszer által létrehozott szabályok nem módosíthatóak.

De tudjuk engedélyezni / tiltani a szabályt.

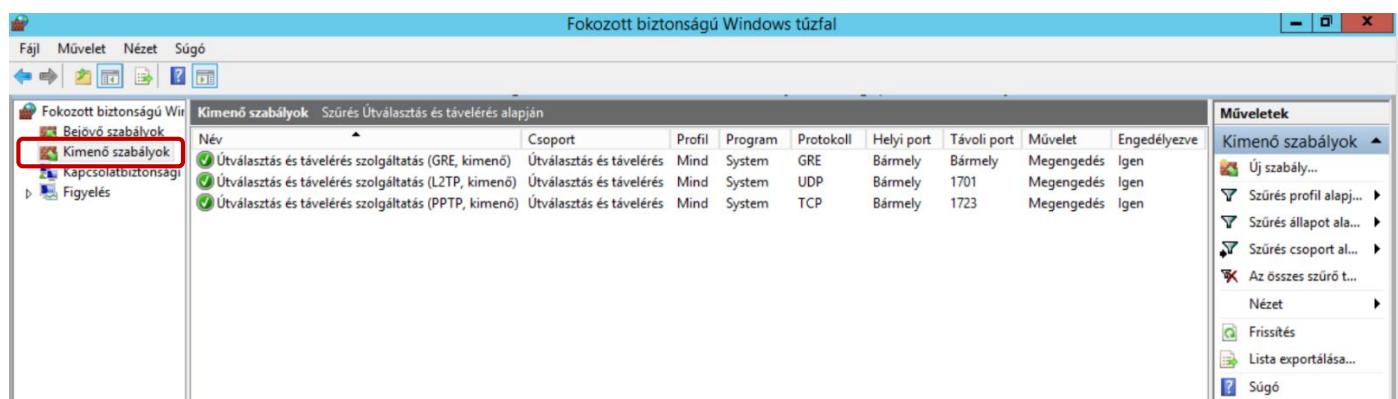
A **Program**, ami használja csak egyszerűen a **System**.



A Távelérés (VPN) a **TCP** protokollt és a **1701**, illetve a **1723**-es portot használja.

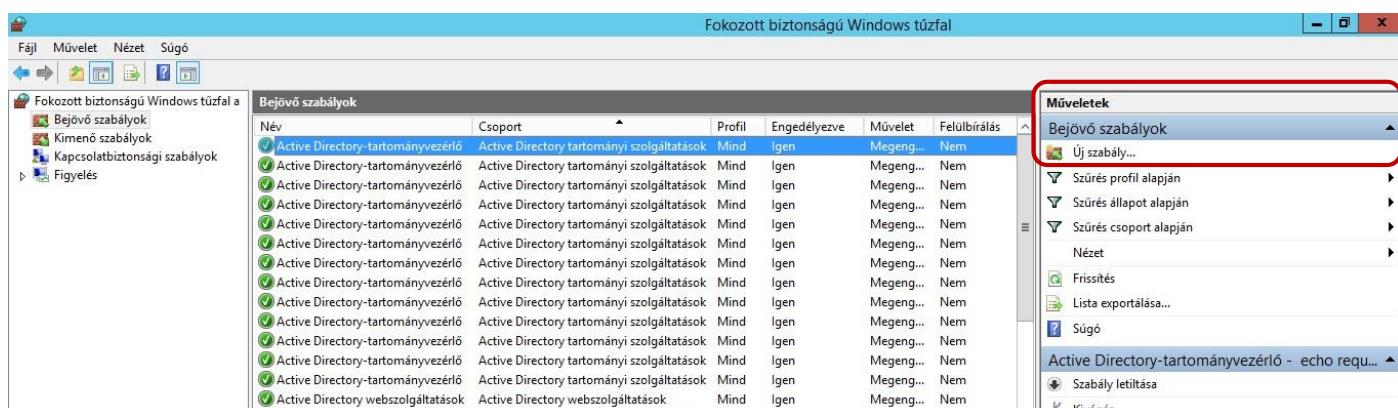


Nézzük meg a **Kimenő szabályok** között is a **Távelérés szabályait**. A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat! (Kifelé irányban nem tiltjuk a forgalmat; de a szabály létezik, ami átengedné!)

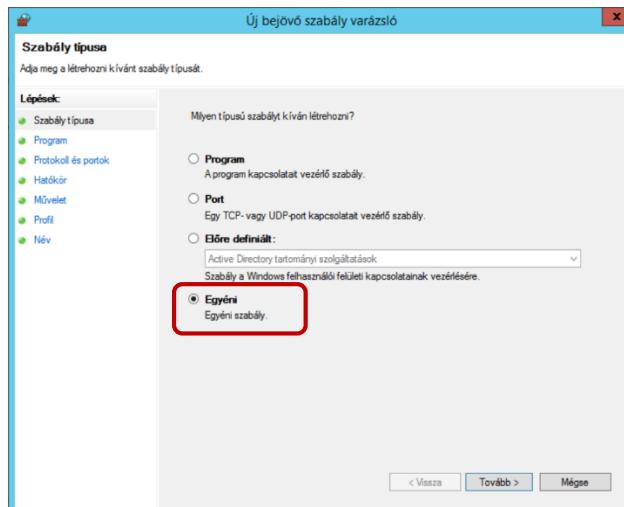


Nézzük meg, hogy tudunk saját szabályokat létrehozni. A legegyszerűbb ilyen szabály talán a **PING** parancs forgalmának engedélyezése.

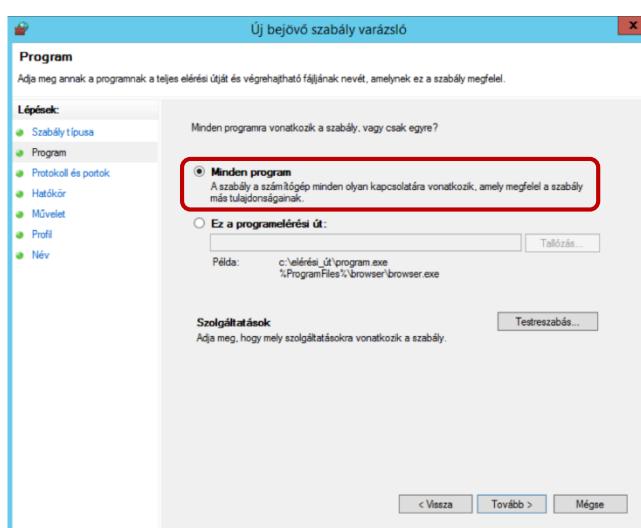
Bejövő szabályt hozunk hozzá létre:



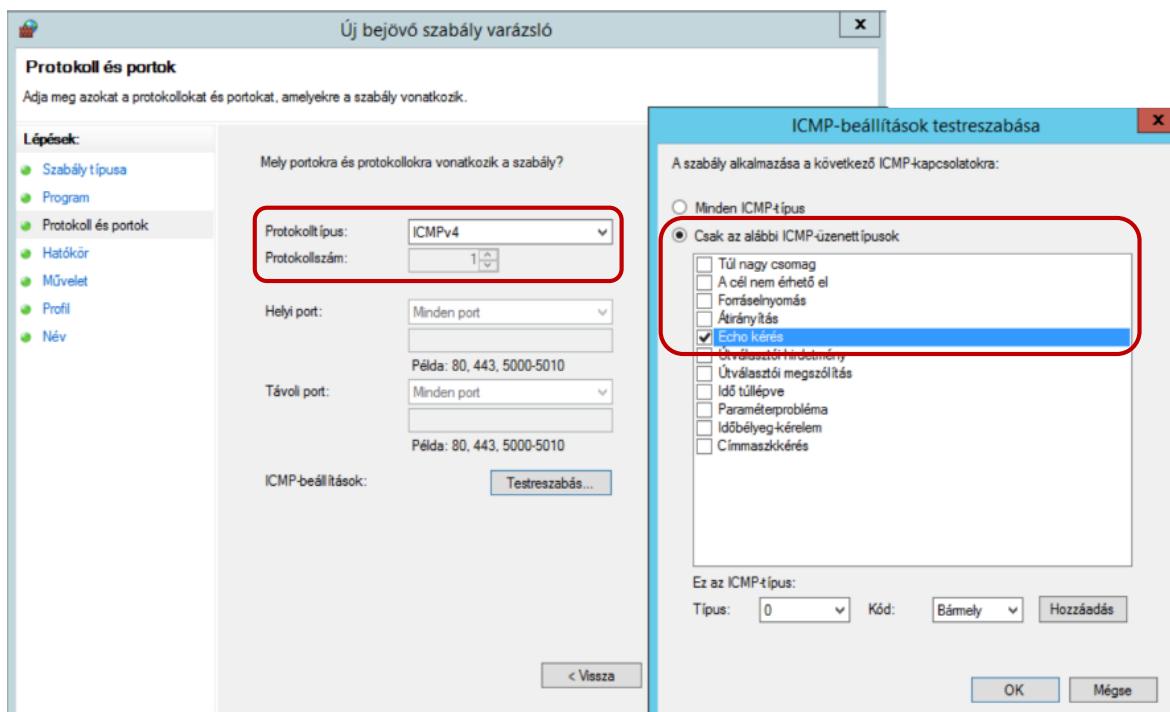
Egyéni szabályt hozunk létre:



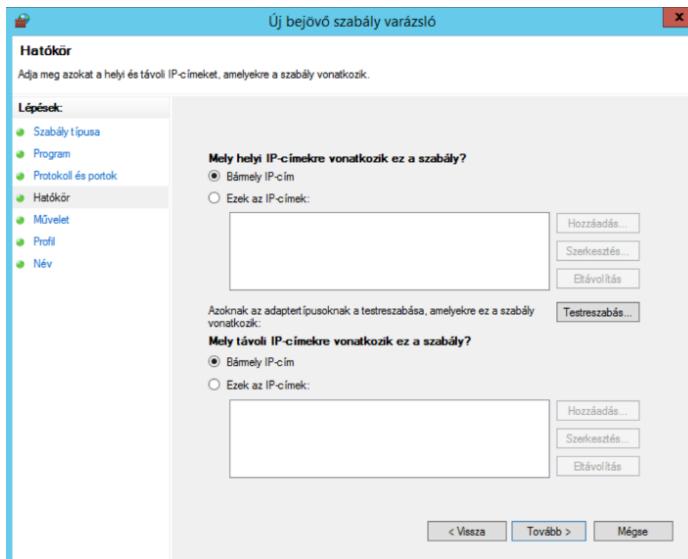
Minden programnak engedélyezzük:



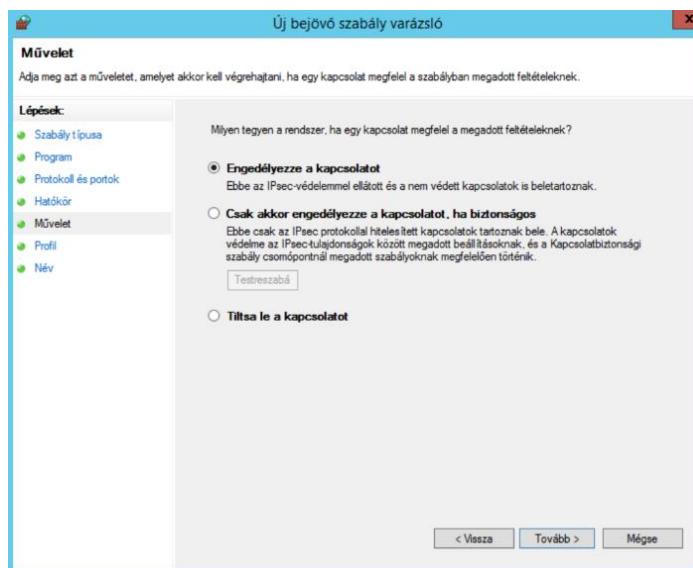
Beállítjuk a protokolltípust, **PING** esetén ez **ICMPv4** és a **Testreszabás** gombra kattintva kijelöljük az **Echo kérést**:



Nem korlátozzuk, hogy milyen IP-címről érhetik el a szervert PING kérések:



Engedélyező szabályt hozunk létre:

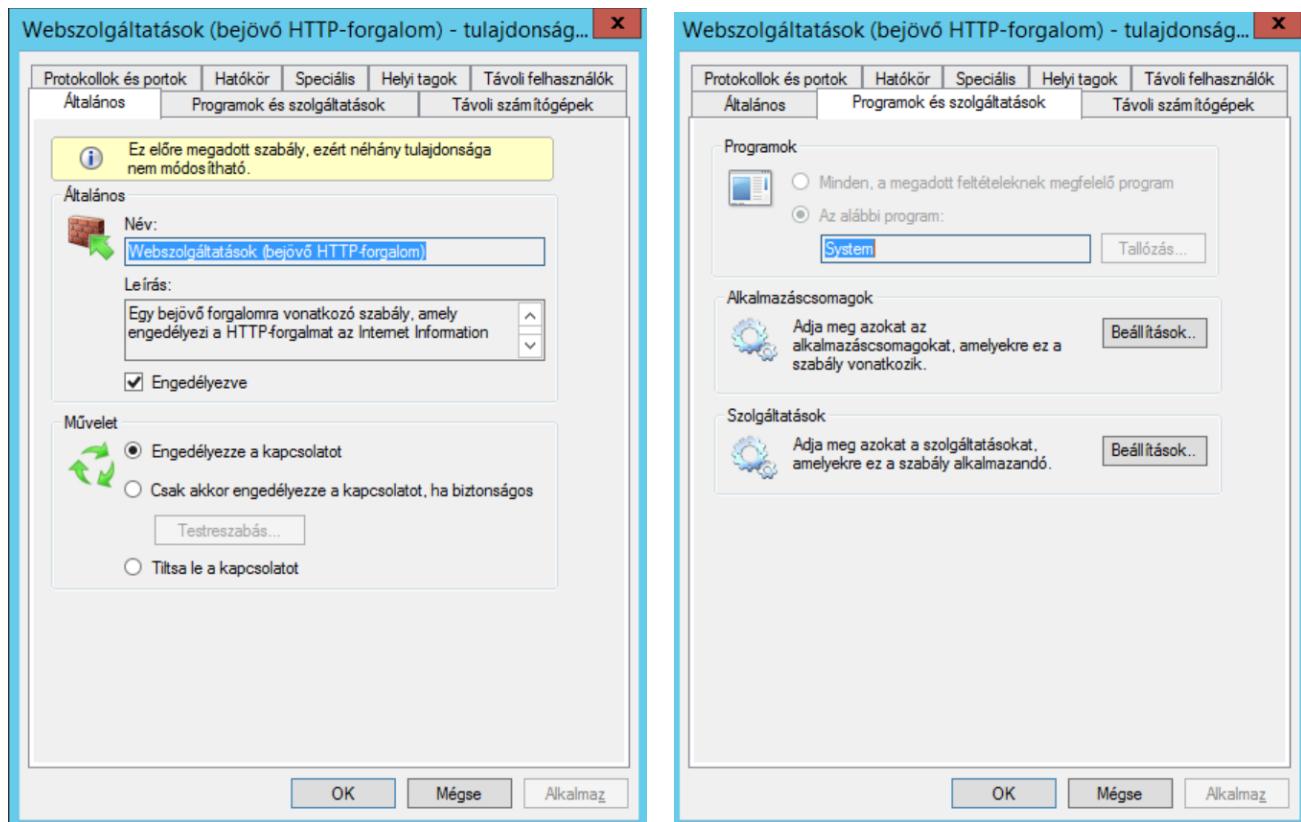


Minden profilra érvényesítjük a szabály beállításait és végül nevezzük el a szabályt:

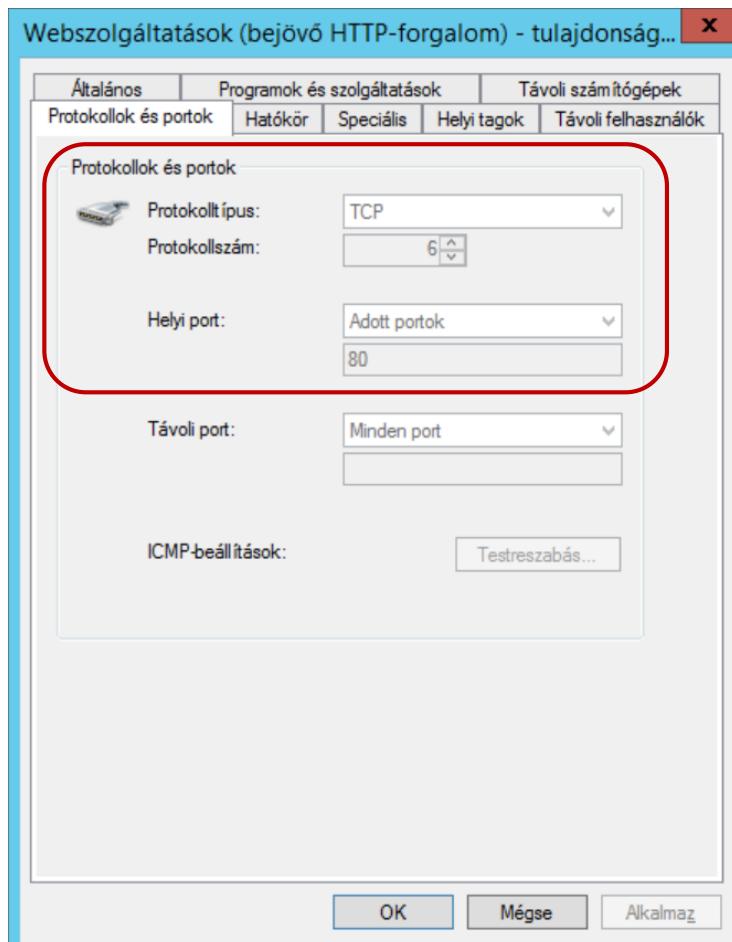
The screenshots show the 'Új bejövő szabály varázsló' (New incoming rule wizard) with the title 'Új bejövő szabály varázsló'.  
Left screenshot: 'Profil' step. It asks for profiles and lists conditions: 'Mikor lép érvénybe ez a szabály?'. Options include 'Tartomány' (A számítógép vállalati tartományhoz való csatlakozásakor alkalmazandó), 'Személyes' (A számítógép magánhálózati (például otthoni vagy munkahelyi) helyhez való csatlakozásakor alkalmazandó), and 'Nyilvános' (A számítógép nyilvános hálózati helyhez való csatlakozásakor alkalmazandó). Navigation buttons: '< Vissza' (Back), 'Tovább >', 'Mégse' (Cancel).  
Right screenshot: 'Név' step. It asks for a name and description. The name is 'PING' and the description is 'Leírás (nem kötelező): PING engedélyezése szerver felé.' Navigation buttons: '< Vissza' (Back), 'Befejezés' (Finish), 'Mégse' (Cancel).

## **WEB kiszolgáló:**

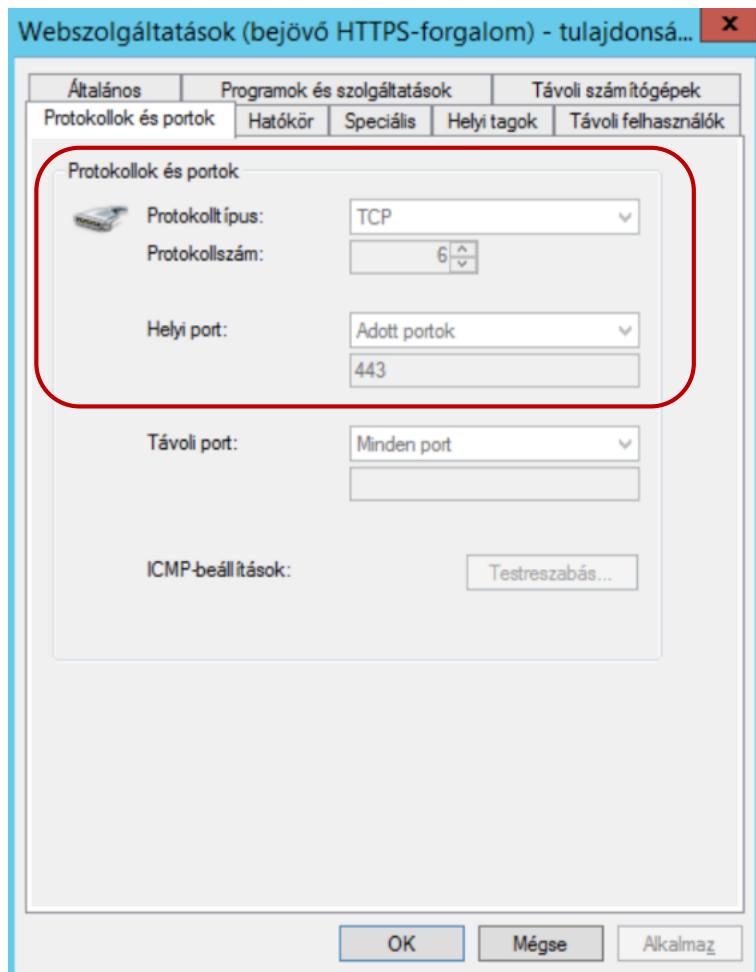
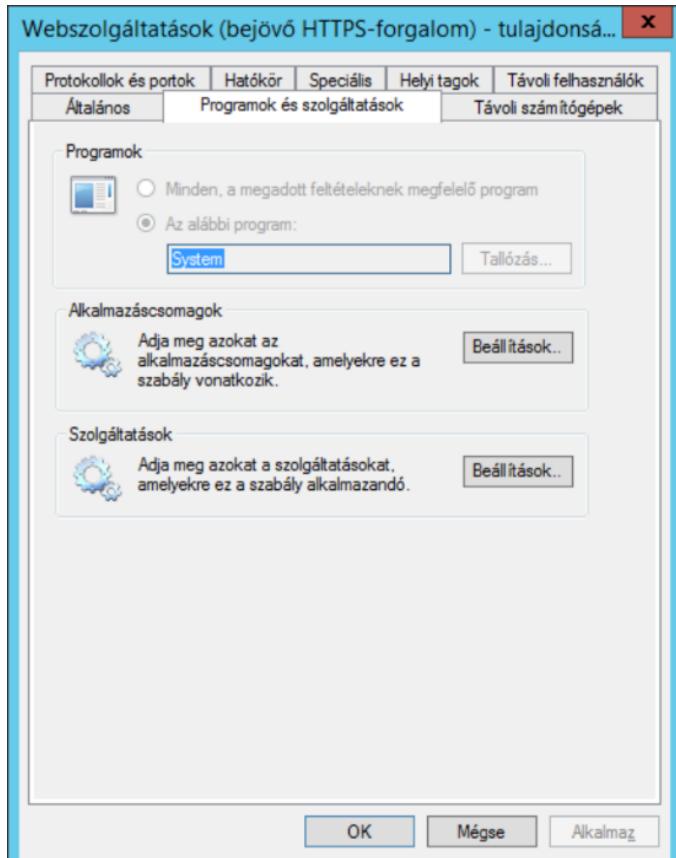
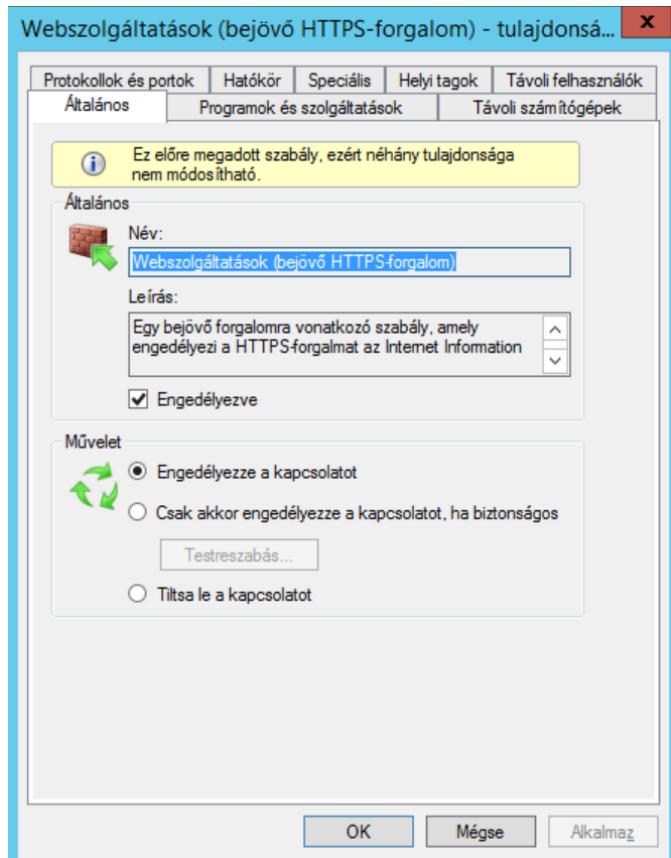
Ha csak az alapértelmezett portokat (**80, 443**) használjuk a szerveren, akkor nem igényel beállítást, a rendszer felvette a szükséges szabályokat!



Alapértelmezett **80**-as porton keresztül, **TCP** protokoll:



Ugynéz ha **https protokollt** használunk, **443-as porton** keresztül és **TCP protokollen** keresztül:



Amennyiben egyedi portokat használnánk, akkor készítsünk (az előző szabályok alapján) egyedi szabályokat:

### Nem biztonságos webes kapcsolathoz (**http** protokoll, egyedi **8080**-as porton keresztül)

<p>Webszolgáltatások - HTTP 8080 - tulajdonságok</p> <p>Protokollok és portok Hatókör Speciális Helyi tagok Távoli felhasználók</p> <p>Általános Programok és szolgáltatások Távoli számítógépek</p> <p><b>Általános</b></p> <p>Név: Webszolgáltatások - HTTP 8080</p> <p>Leírás: 8080</p> <p><input checked="" type="checkbox"/> Engedélyezve</p> <p>Művelet</p> <p><input checked="" type="radio"/> Engedélyezze a kapcsolatot</p> <p><input type="radio"/> Csak akkor engedélyezze a kapcsolatot, ha biztonságos</p> <p><input type="radio"/> Tiltsa le a kapcsolatot</p> <p>Testreszabás...</p> <p>OK Mégse Alkalmaz</p>	<p>Webszolgáltatások - HTTP 8080 - tulajdonságok</p> <p>Protokollok és portok Hatókör Speciális Helyi tagok Távoli felhasználók</p> <p>Általános Programok és szolgáltatások Távoli számítógépek</p> <p><b>Programok</b></p> <p><input type="radio"/> minden, a megadott feltételeknek megfelelő program</p> <p><input checked="" type="radio"/> Az alábbi program: System <input type="button" value="Tallózás..."/></p> <p><b>Alkalmazáscsomagok</b></p> <p><input type="checkbox"/> Adja meg azokat az alkalmazáscsomagokat, amelyekre ez a szabály vonatkozik. <input type="button" value="Beállítások..."/></p> <p><b>Szolgáltatások</b></p> <p><input type="checkbox"/> Adja meg azokat a szolgáltatásokat, amelyekre ez a szabály alkalmazandó. <input type="button" value="Beállítások..."/></p> <p>OK Mégse Alkalmaz</p>
--	---

Webszolgáltatások - HTTP 8080 - tulajdonságok

Általános Programok és szolgáltatások Távoli számítógépek

Protokollok és portok Hatókör Speciális Helyi tagok Távoli felhasználók

**Protokollok és portok**

Protokolltípus: TCP

Protokollsáml: 6

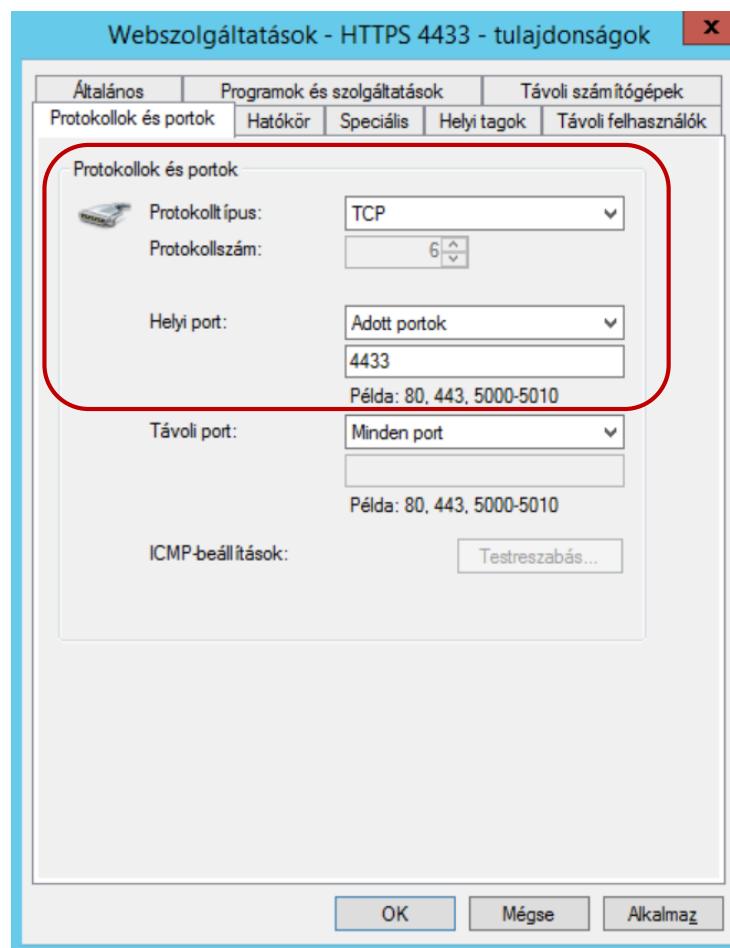
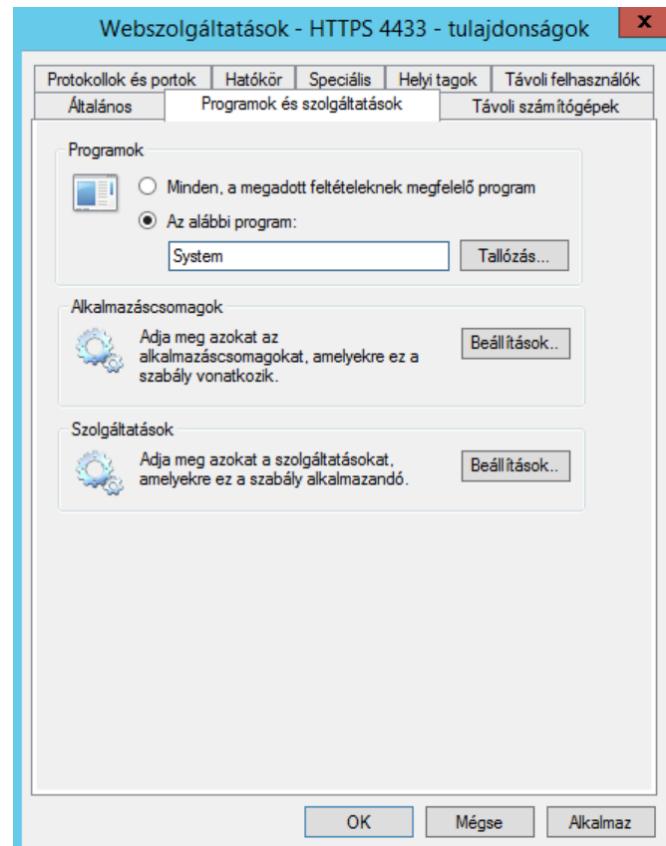
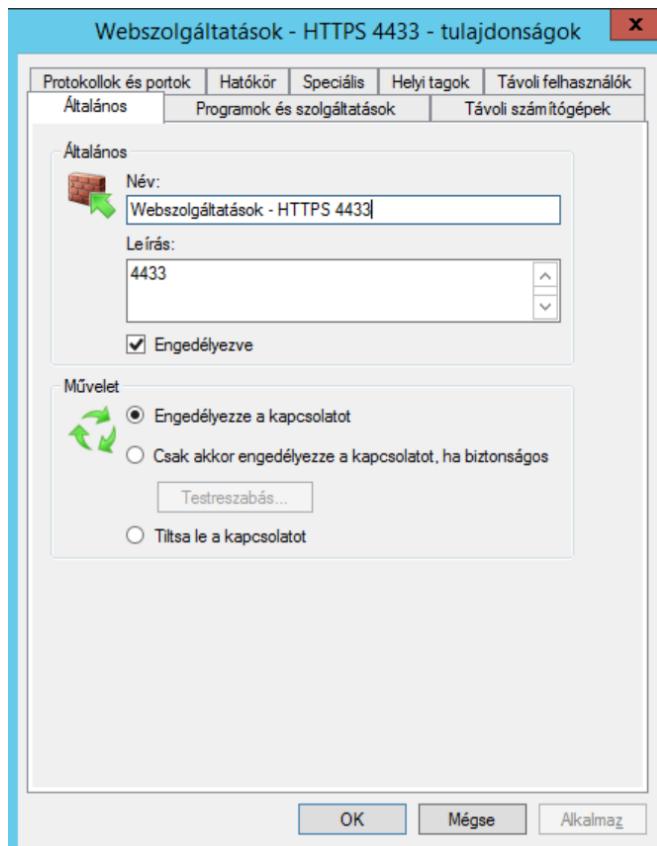
Helyi port: Adott portok  
8080  
Példa: 80, 443, 5000-5010

Távoli port: minden port  
Példa: 80, 443, 5000-5010

ICMP-beállítások:

OK Mégse Alkalmaz

## Biztonságos webes kapcsolathoz ([https](https://) protokollal, 4433-as porton keresztül)



## FTP kiszolgáló

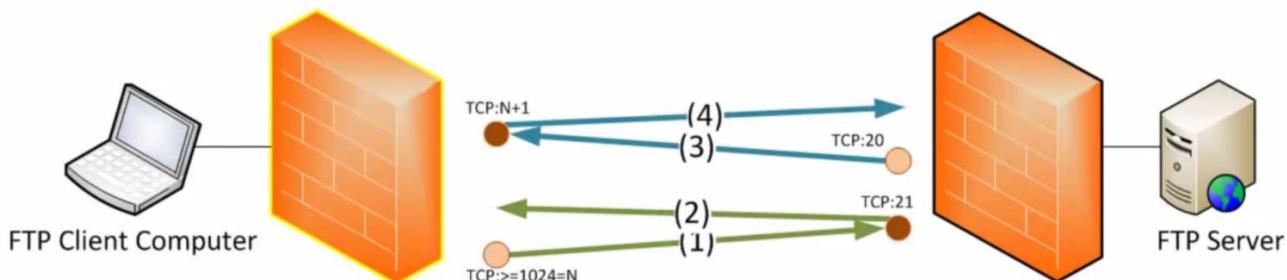
Kétféle módon működhet az FTP kiszolgáló és ennek megfelelően a tűzfal szabályokat is kétféleképpen hozhatjuk létre. Annak megfelelően, hogyan szeretnénk működtetni az FTP kiszolgálónkat.

### Aktív FTP

Ebben az esetben a *kiszolgáló vezérli a folyamatot* és a szerveren csak két porthoz (**BE: 21** és **KI: 20**) kell hozzáférést biztosítanunk, TCP protokoll mellett. A kliensen viszont engedélyeznünk kell **MINDEN 1024-nél magasabb portot!**

Ezt nem minden felhasználó szeretné, ezért is ritka ez a megoldás. A kiszolgálóra is többlet terhet jelent, hiszen ő vezérli a folyamatot is.

## Active FTP



Mindezek megvalósítása részletezve:

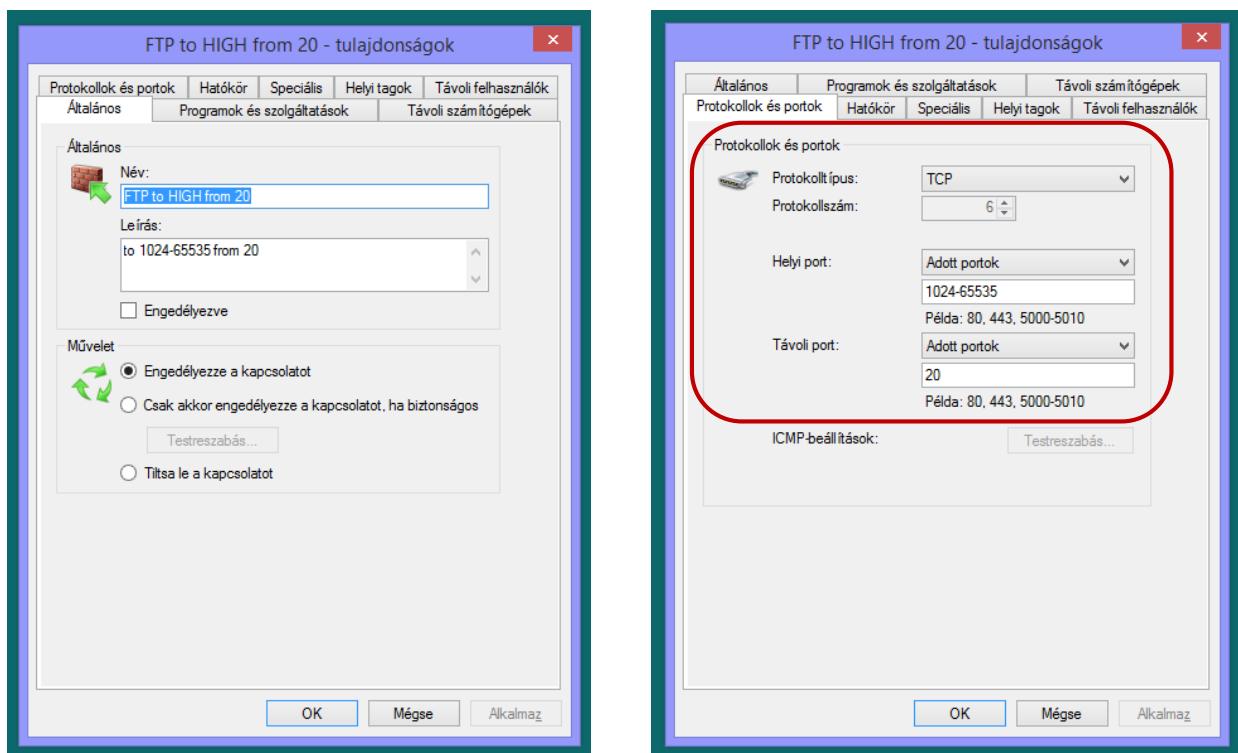
### Szerveren:

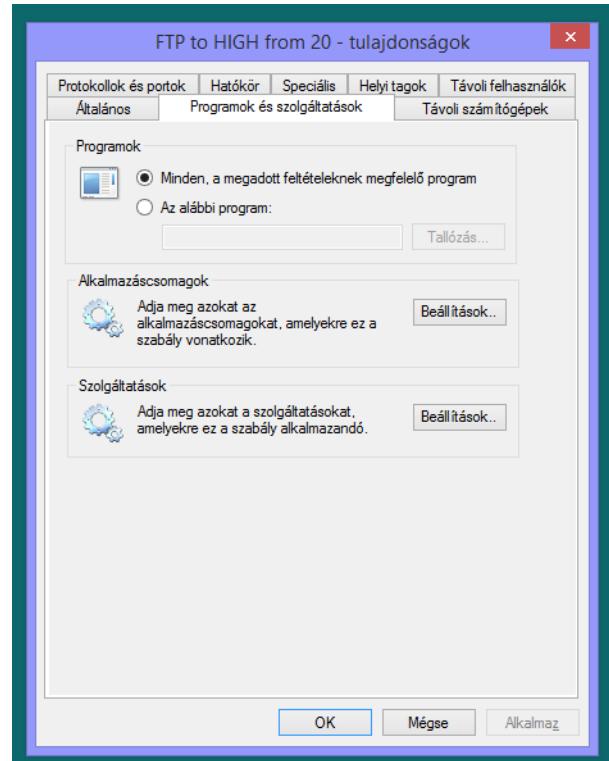
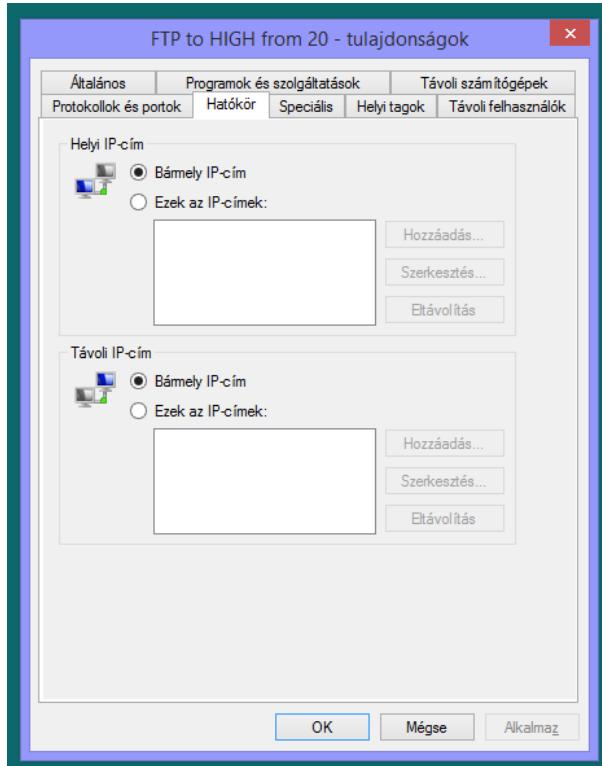
Bejövő szabály: nem igényel beállítást, a rendszer felvette a szükséges szabályt!

Kimenő szabály: nem igényel beállítást, a rendszer felvette a szükséges szabályt!

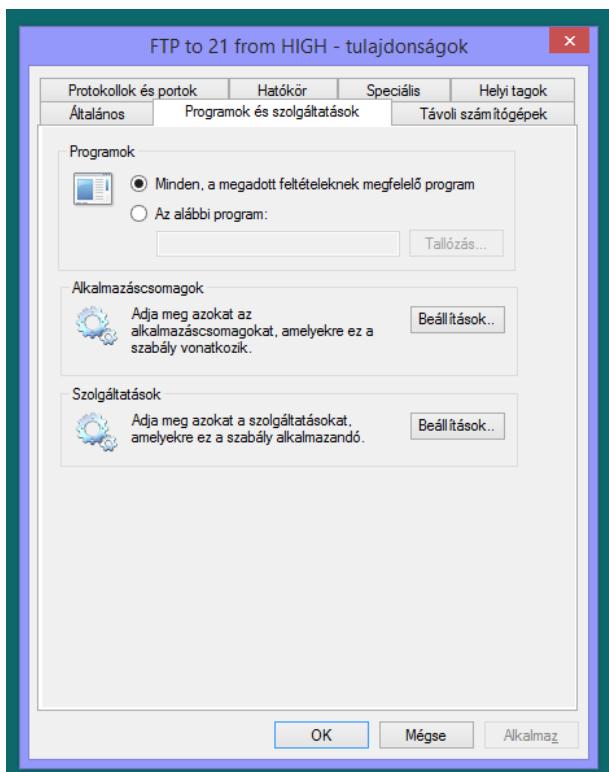
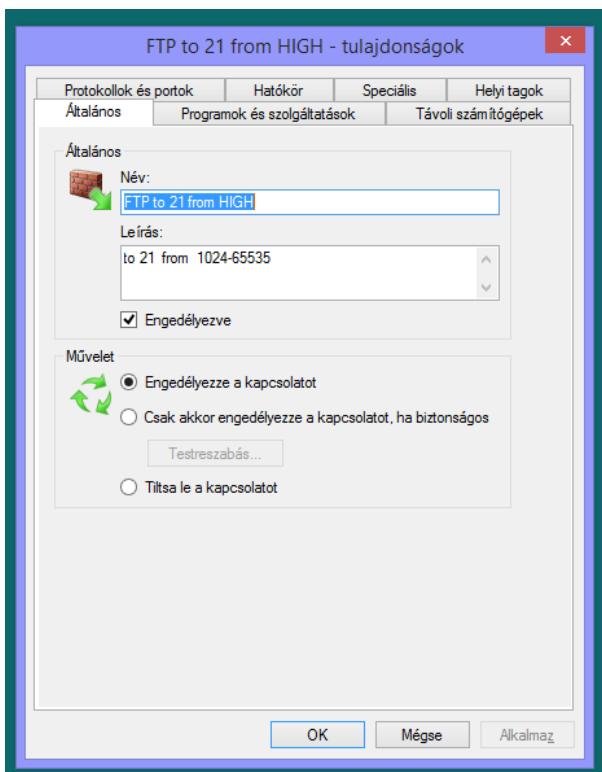
### Kliensen:

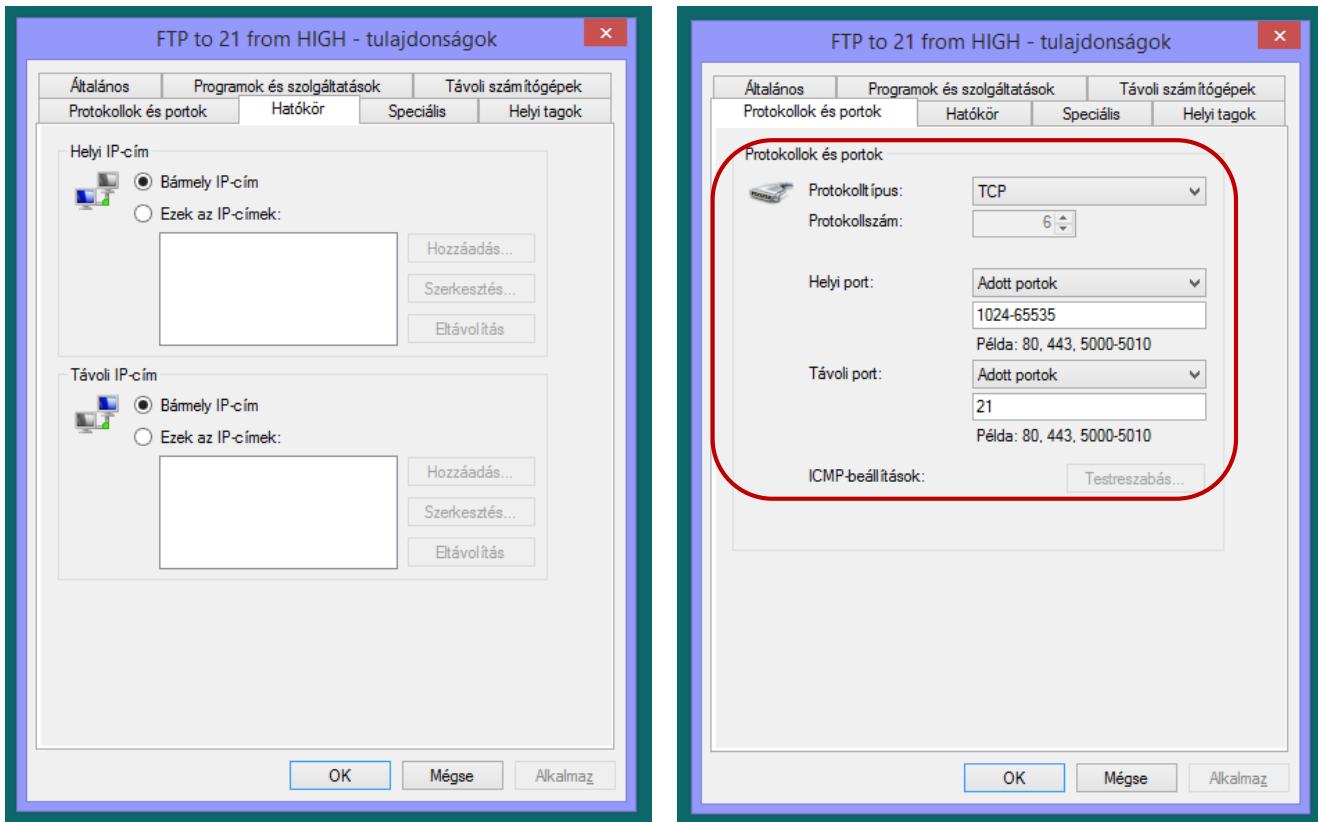
Bejövő szabály: (a képen **még** nincs engedélyezve!)





Kimenő szabály:



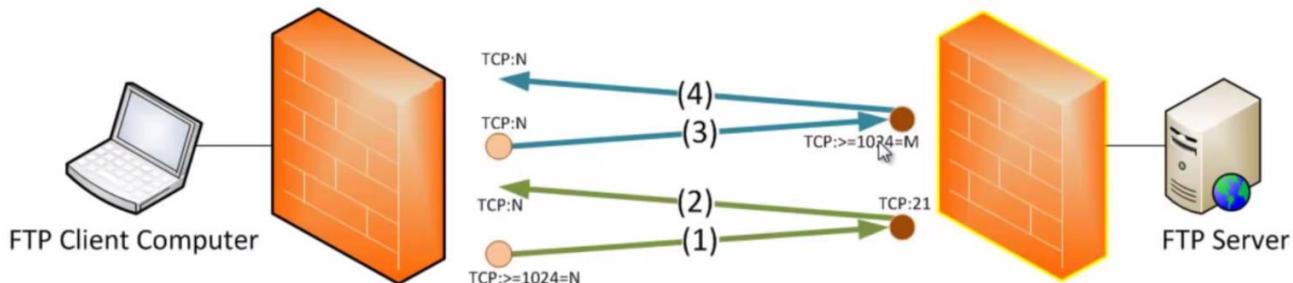


## Passzív FTP

Ebben az esetben a kliens vezérli a folyamatot és a szerveren hozzáférést kell biztosítanunk a **21-es** porthoz (**BE** irányban), illetve az **1024-nél magasabb** portokhoz (**KI** irányban); **TCP protokoll** mellett!

A kliensen az **1024-nél magasabb portokhoz** kell szabályt rendelnünk, viszont **csak Kimenő forgalomra!** (A kliens által kiküldött csomagokra vissza érkező válaszokat átengedi a kliens tűzfala!)

## Passive FTP



Mindezek megvalósítása részletezve:

### Szerveren:

Bejövő szabály: nem igényel beállítást, a rendszer felvette a szükséges szabályt!

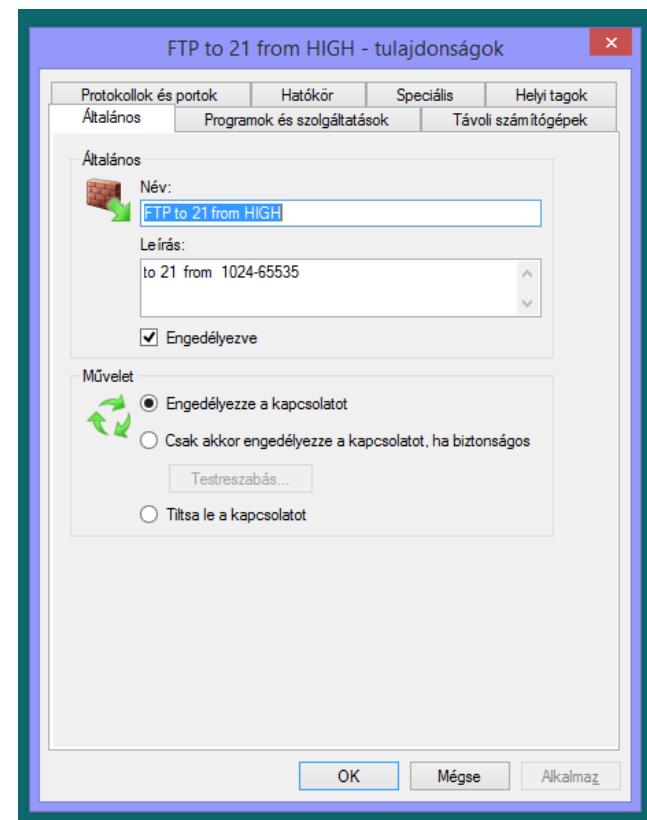
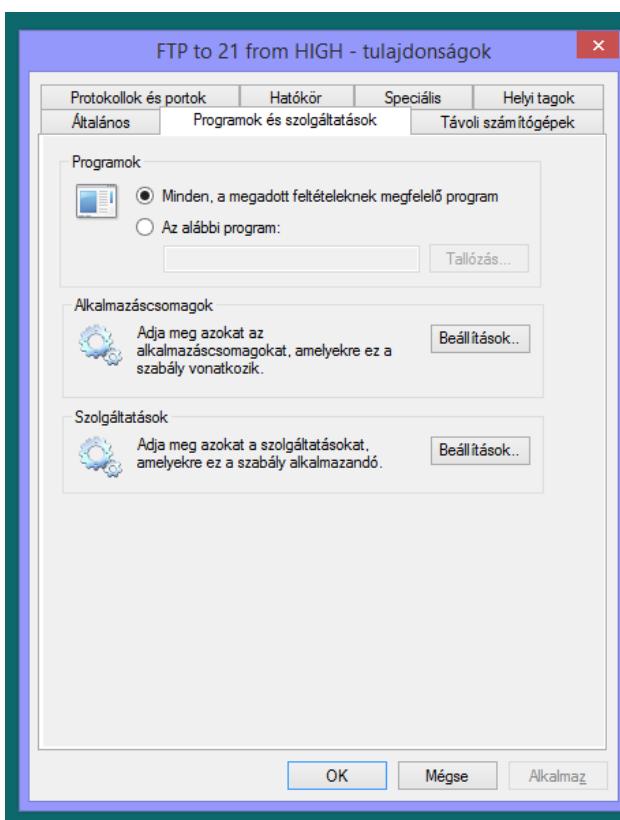
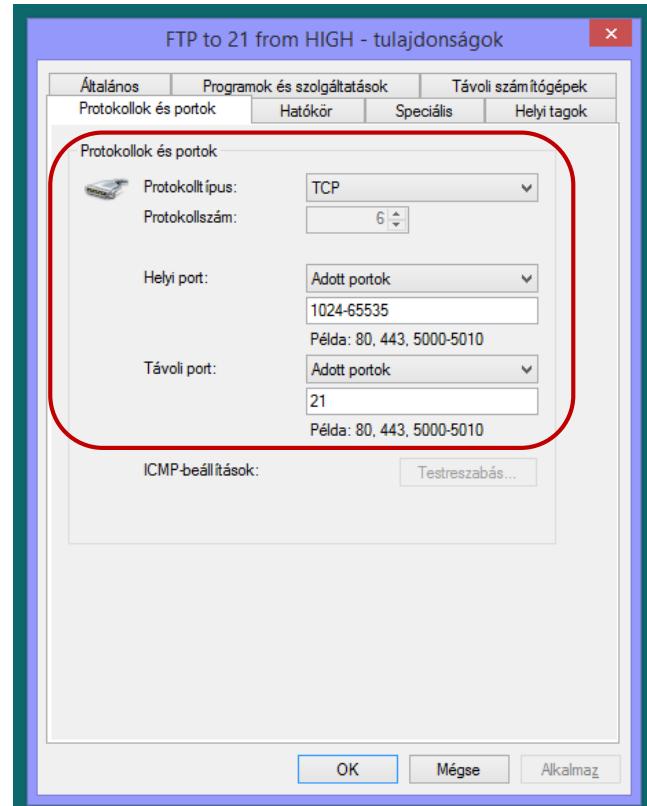
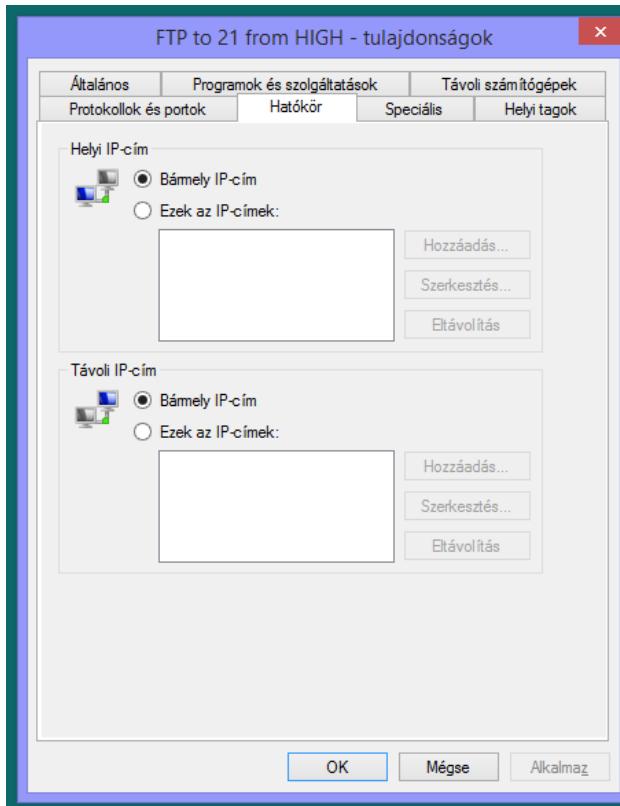
Kimenő szabály: nem igényel szabályt!

## Kliensen:

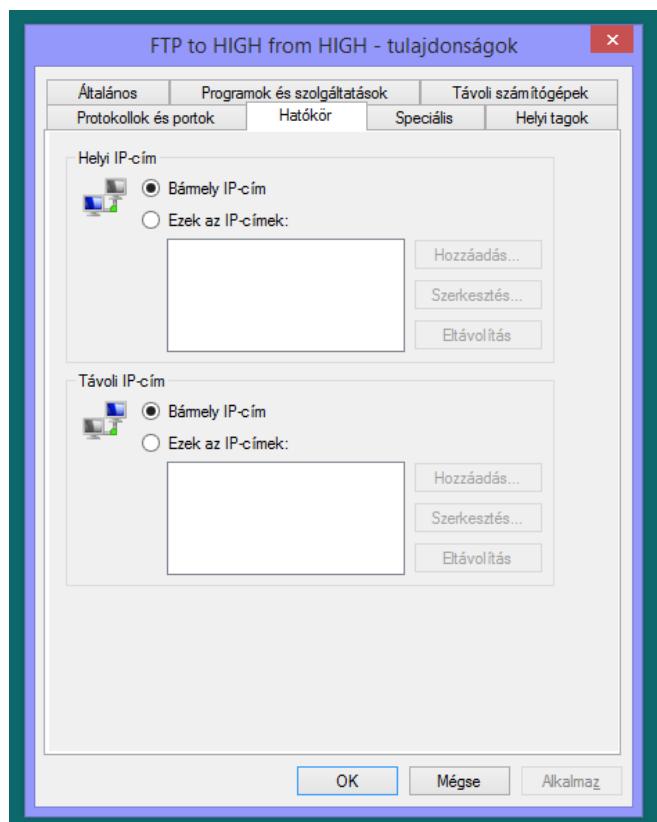
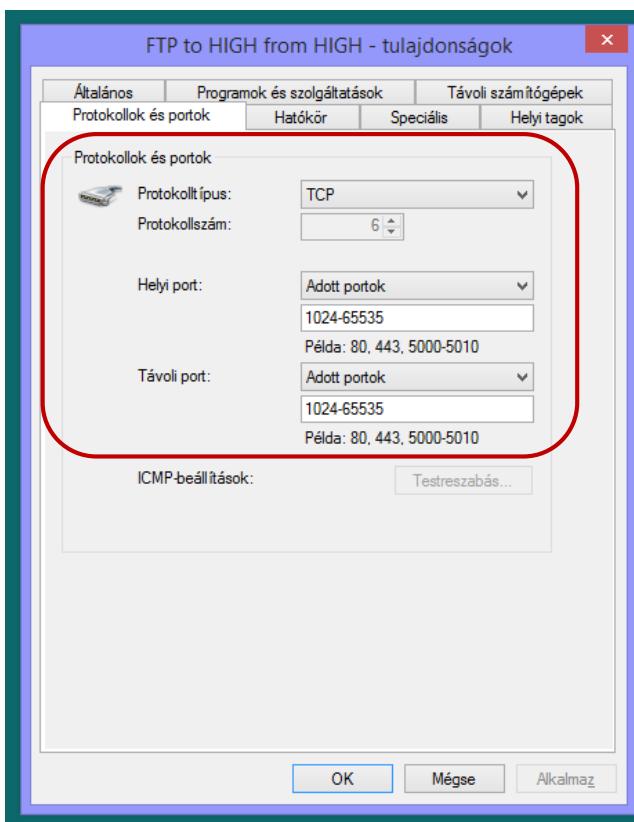
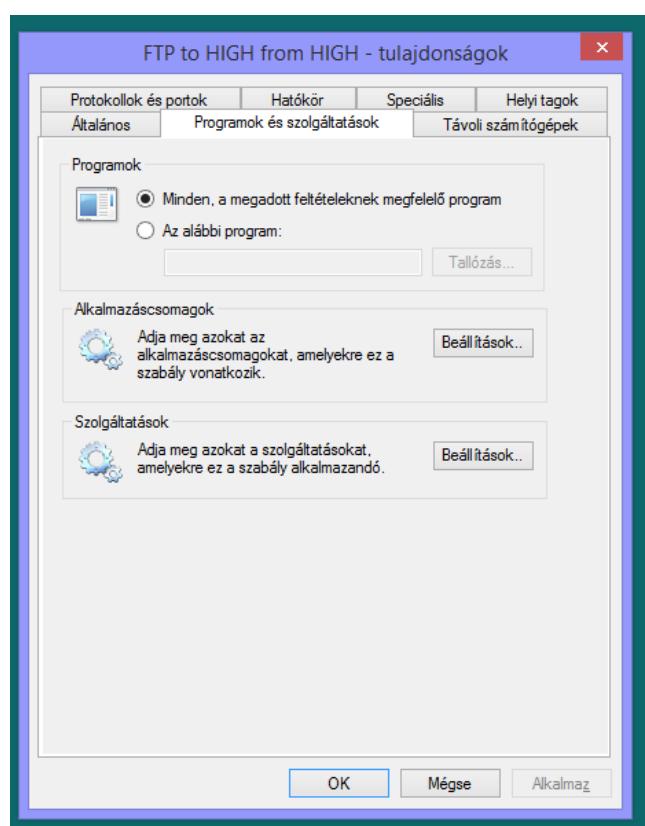
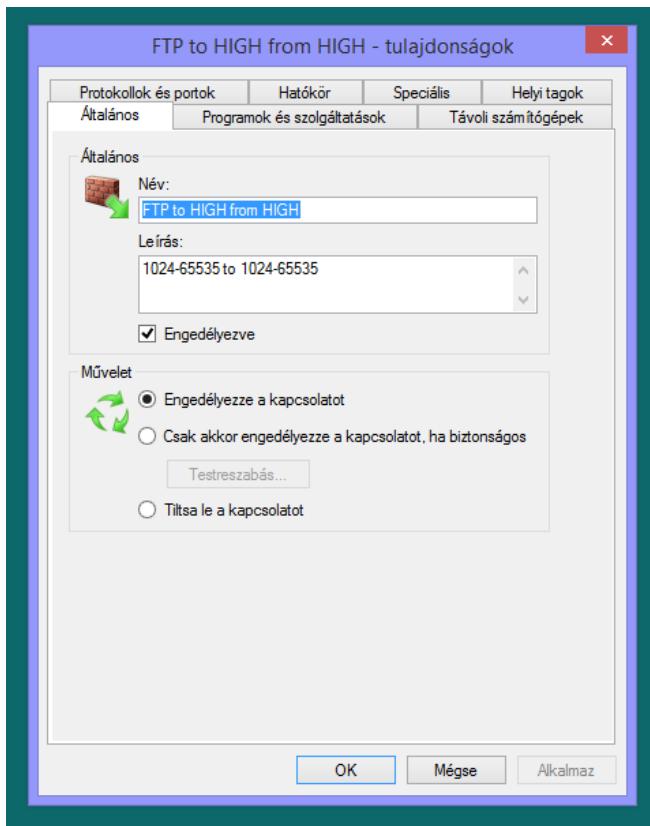
Bejövő szabály: nem igényel szabályt!

Kimenő szabály: két szabályt kell létrehoznunk!

1. Az első szabály a kliens magas (**port > 1024**) portjairól engedélyezi a kapcsolatot a **szerver 21-es portjához**:

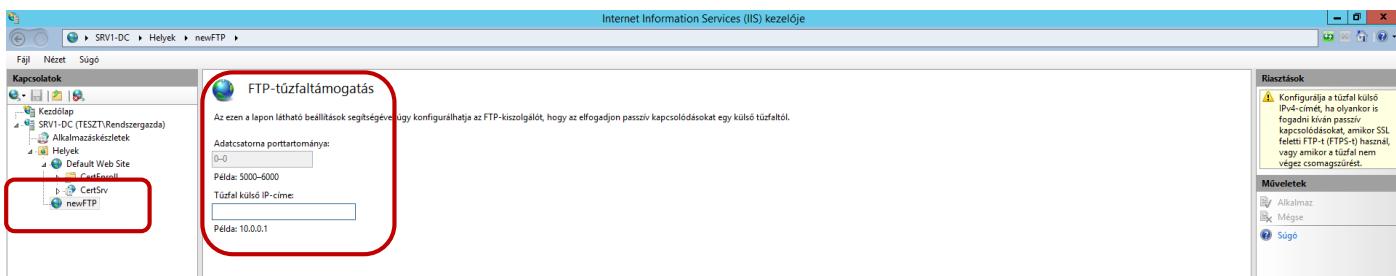


2. A második szabály **a kliens magas** (port > 1024) portjairól engedélyezi a kapcsolatot **a szerver magas portjaihoz:**

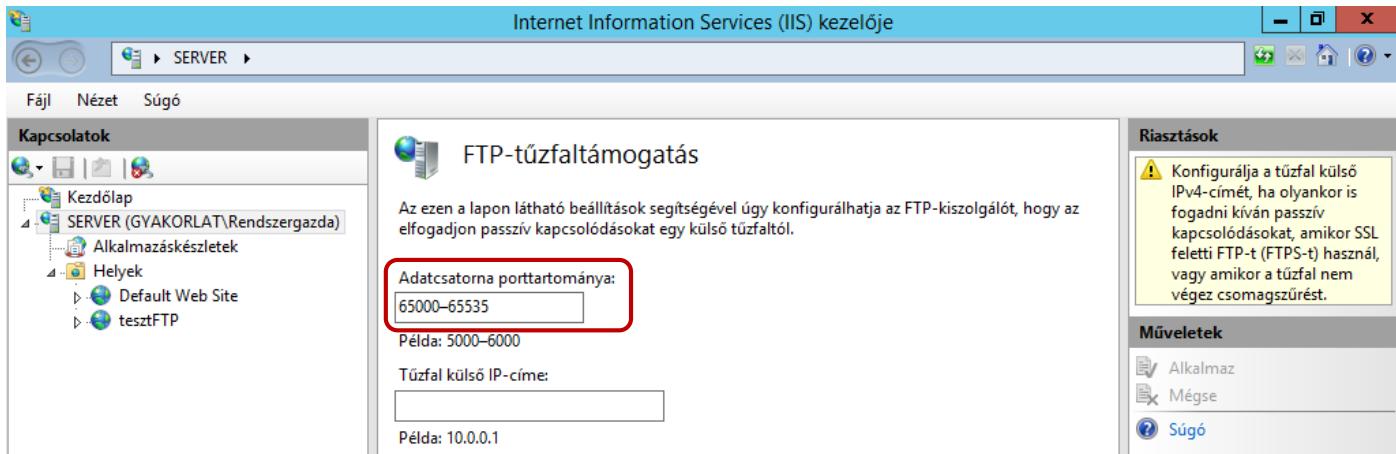


Ez az általánosabban elterjedt megoldás. Viszont a kiszolgálón sok nyitott portot jelent, erre megoldás lehet az **FTP kiszolgáló egyedi porttartománnal**:

Az FTP kiszolgálón létrehozott FTP-helyen nem tudjuk beállítani az egyedi porttartományt:



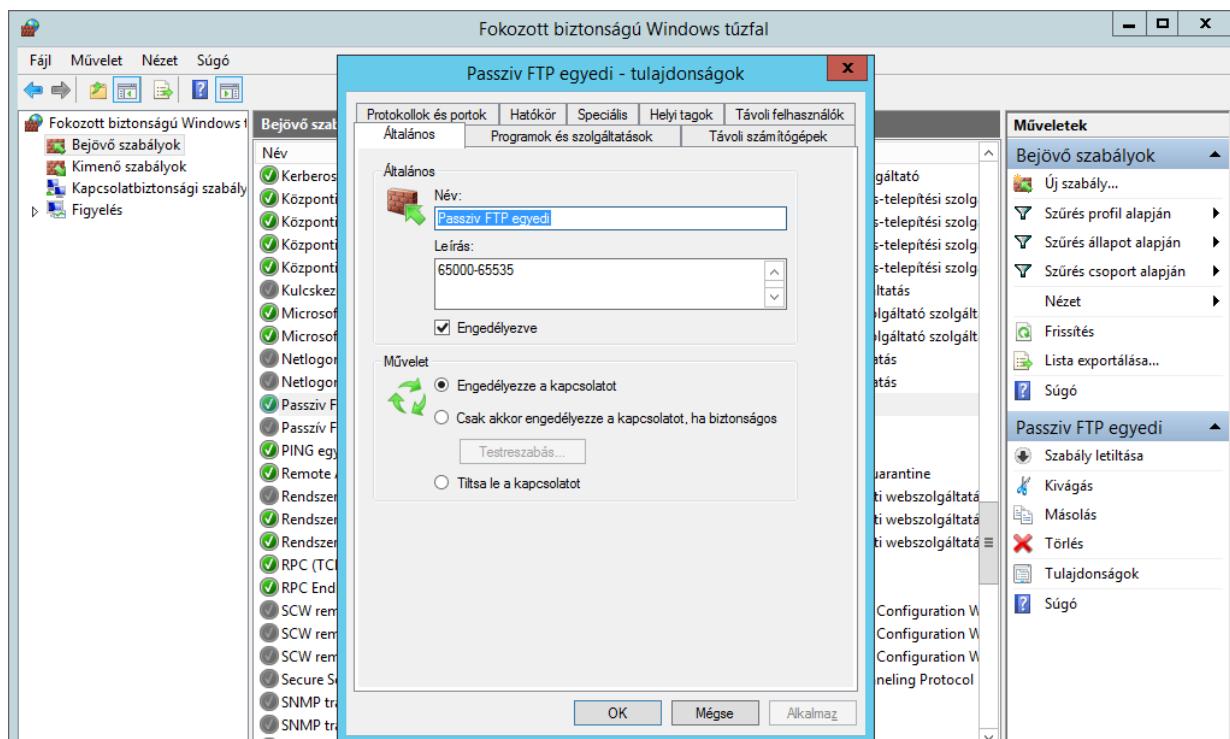
Ez szerver szintű beállítás: (a képen a kiosztott portok: 65000-65535):



A beállítás elvégzése után újra **KELL** indítani az **FTP kiszolgálót!**

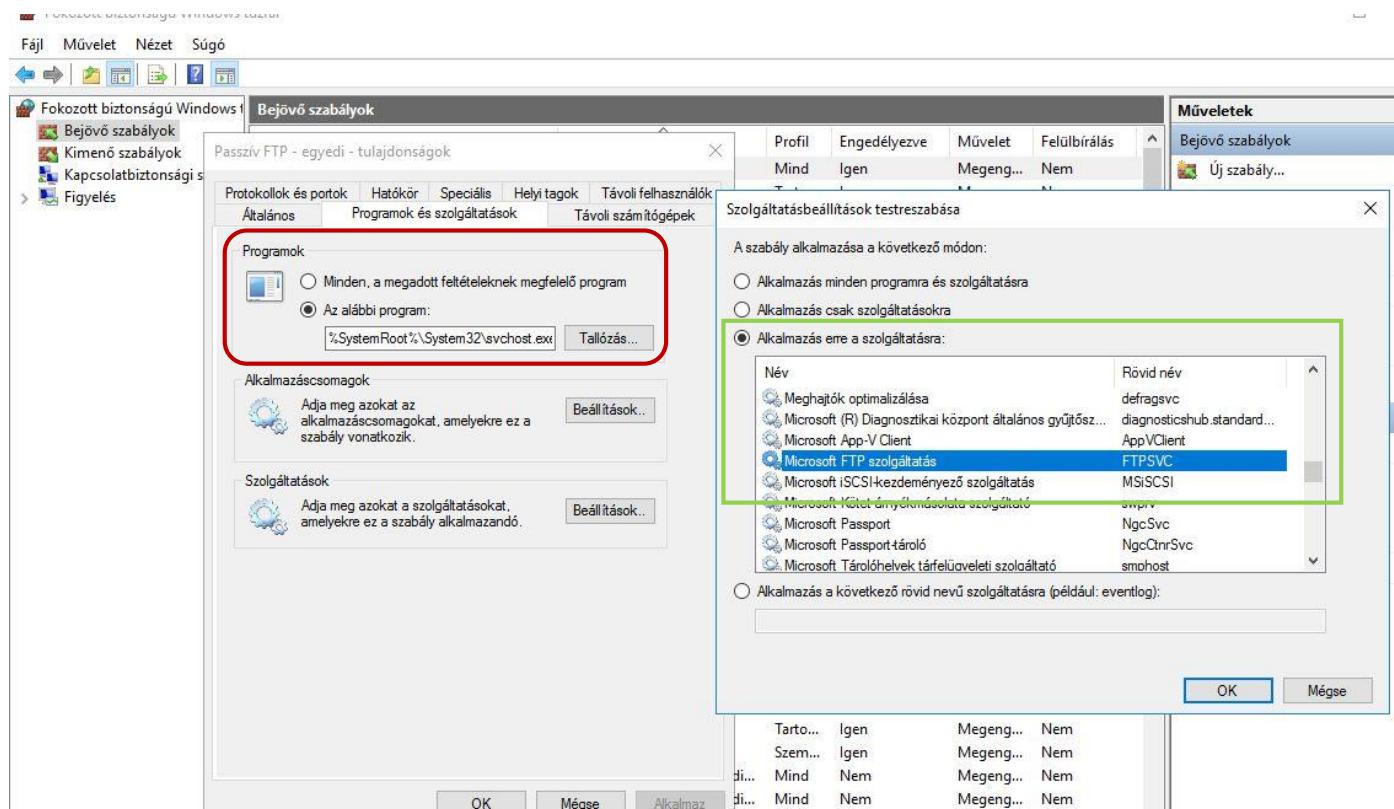
A tűfalon a rendszer által (az *alapértelmezett Passzív FTP kapcsolathoz*) létrehozott szabályt keressük meg és **TILTSUK LE!**

Hozunk létre egy új szabályt az alábbi beállításokkal:

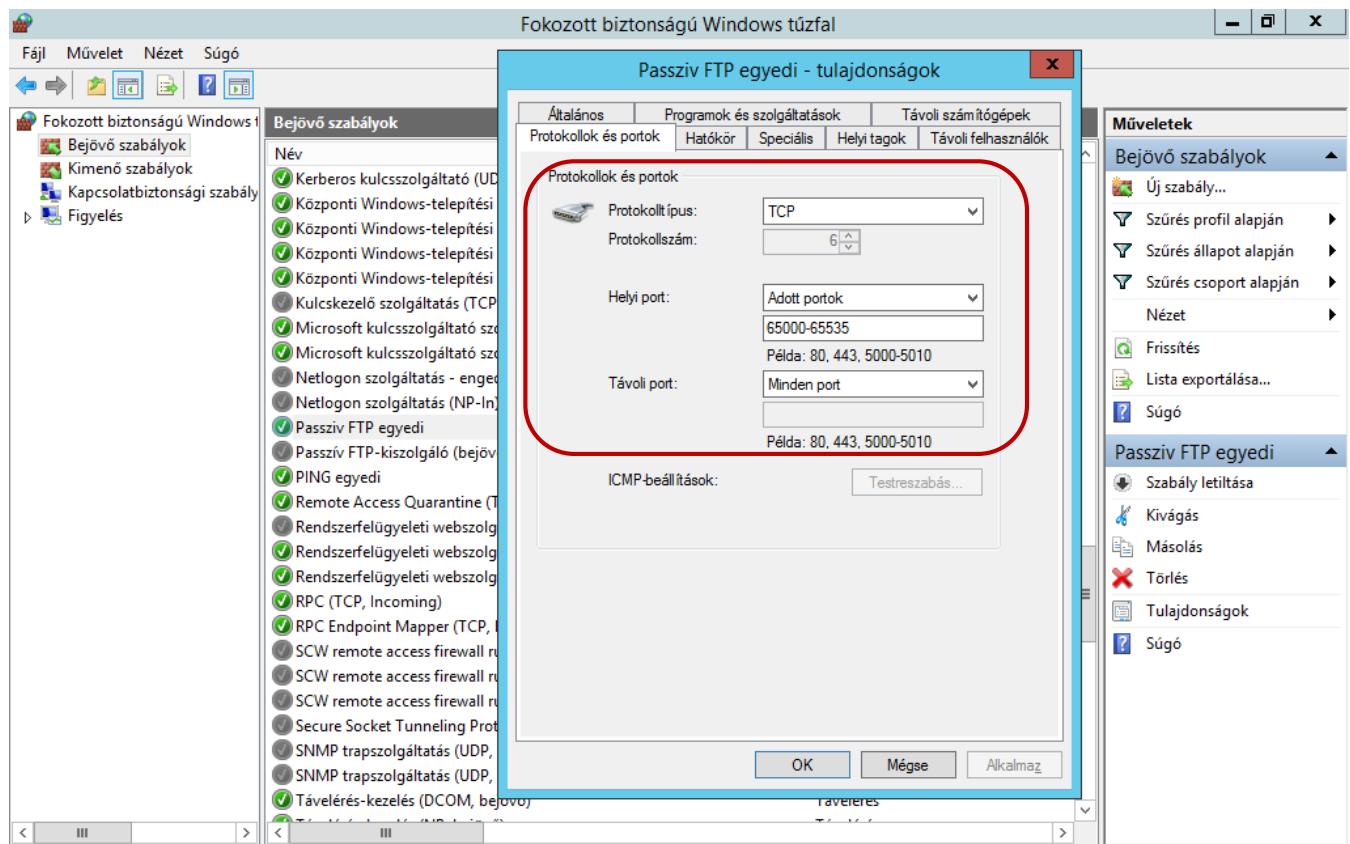


Nem minden programnak nyitjuk meg a porttartományt, csak (a képen látható módon) az FTP szolgáltatásnak!

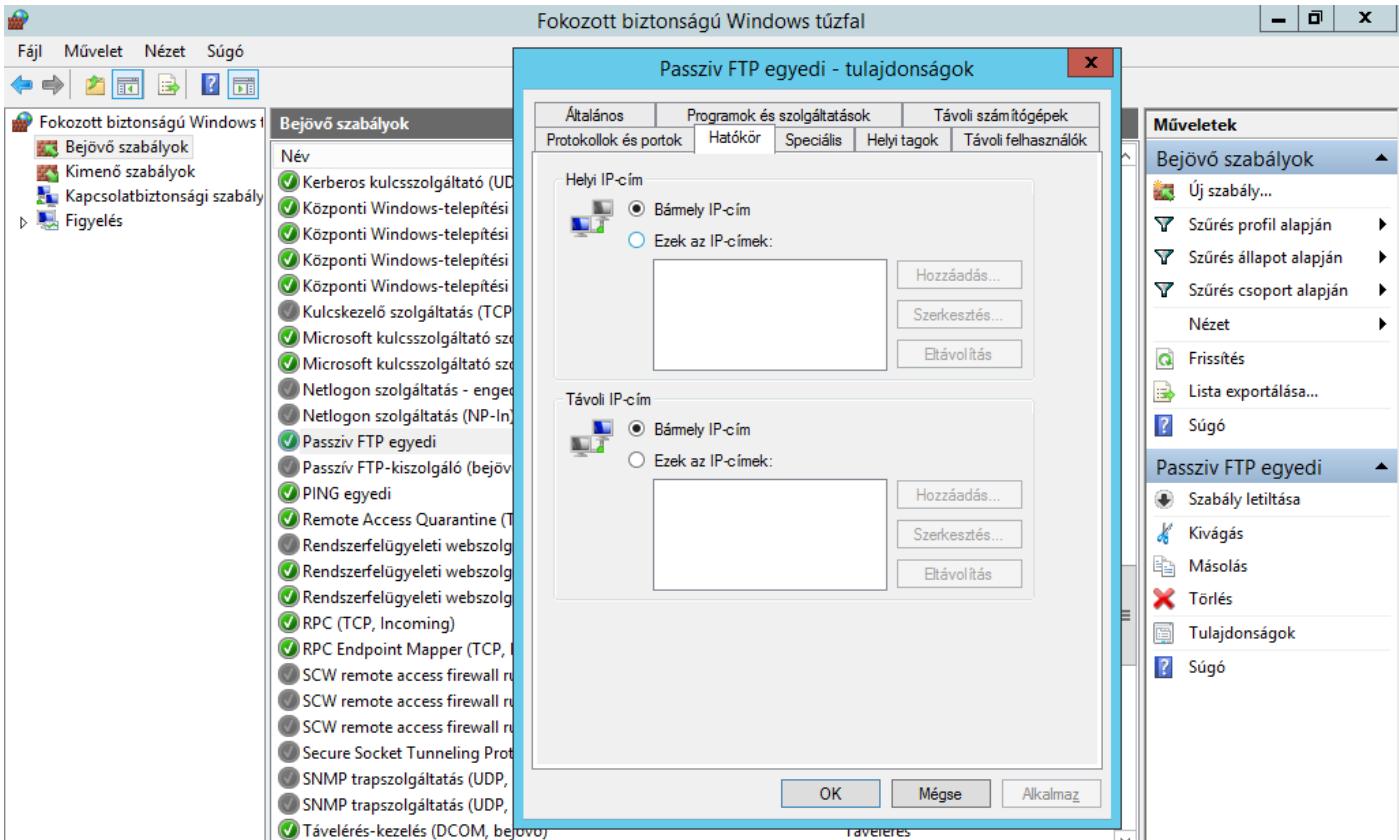
(Az **svchost.exe**, mint szolgáltatáskezelő részére és azon belül a **Microsoft FTP szolgáltatás** **FTPSVC**)



Beállítjuk a protokolلت (TCP) és a porttartományt (65000 - 65535):



Szükség esetén itt is korlátozhatsuk IP-cím szerint is az FTP szerverhez való hozzáférést:



Kiegészítés a szerveren nyitott „magas portok” meghatározásához/módosításához:

Dinamikus port tartomány lekérdezése:

```
netsh int ipv4 show dynamicportrange tcp
```

módosítása:

```
netsh int ipv4 set dynamicportrange tcp start=10000 num=55535
```

## Levelező kiszolgáló

Beállíthatjuk a konkrét levelező kiszolgáló programot (a képen: **hMailServer.exe**) illetve a levelezéskor használt adott protokollok szerint (**pop3, smtp, imap**) is hozhatunk létre szabályokat:

