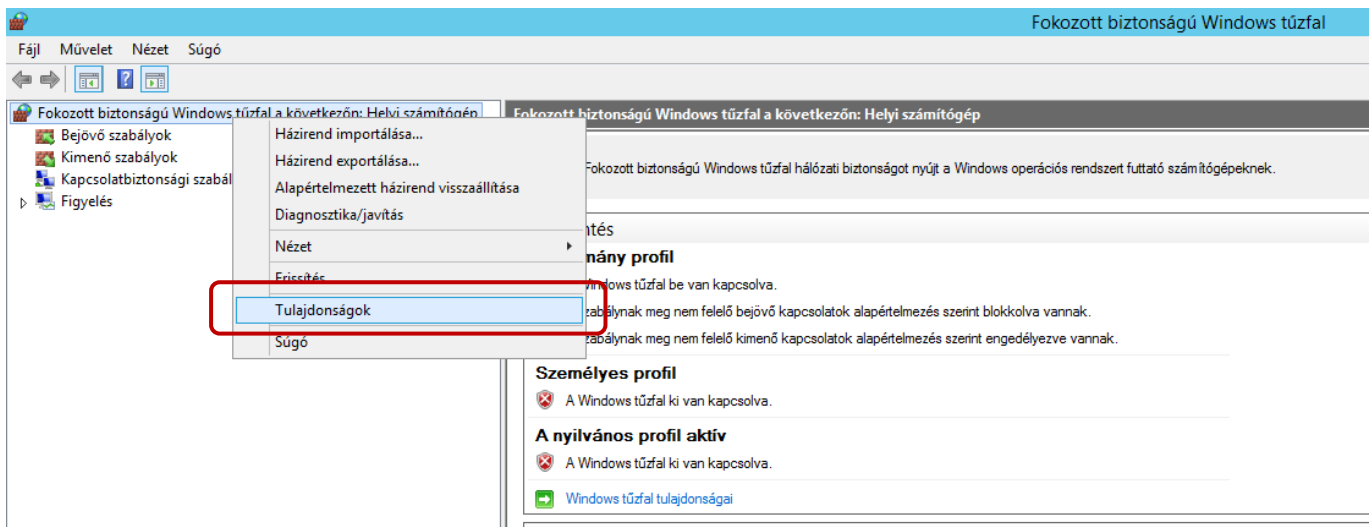


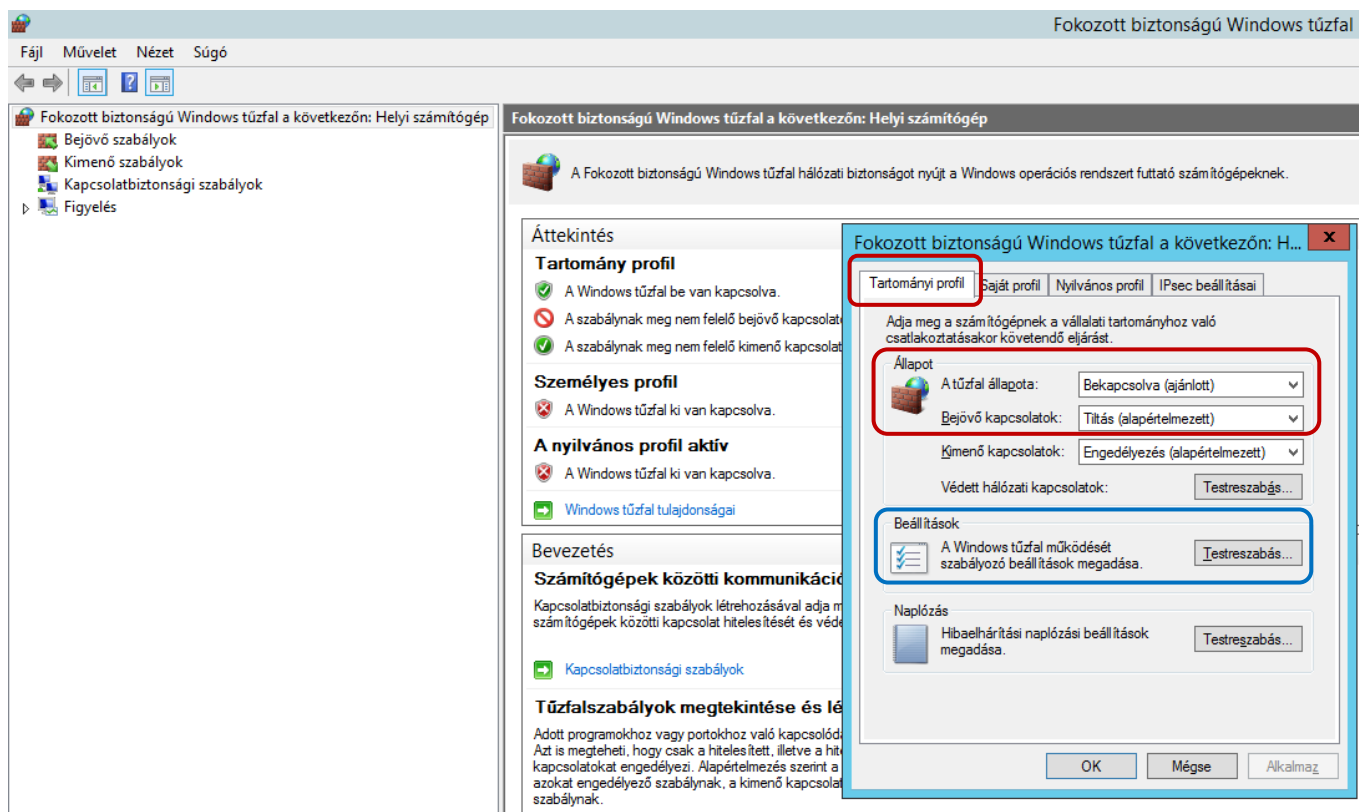
Tűzfal beállítása

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*:

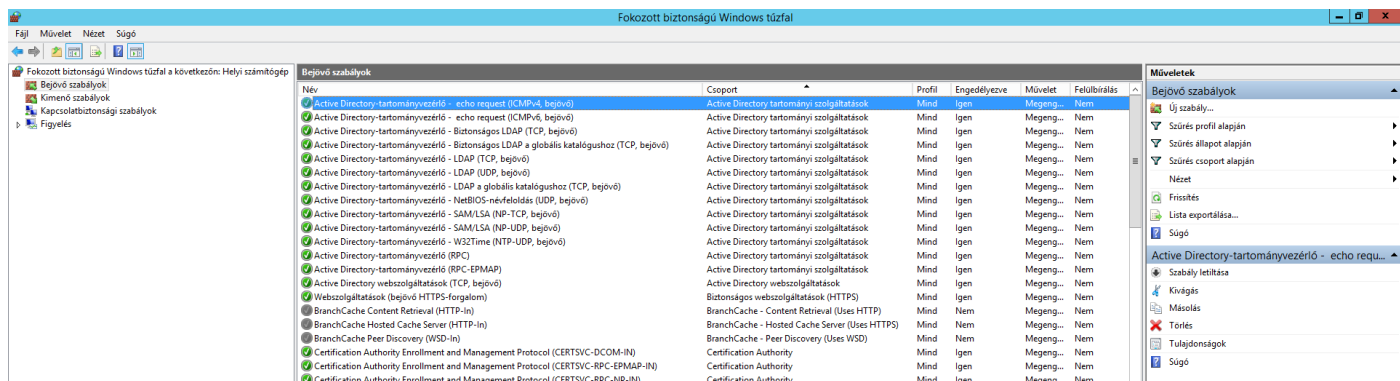


A tűzfalon **Profilokhoz** rendelve állíthatjuk **Be/Ki** állapotba a tűzfalat; illetve, hogy a **Bejövő**- és **Kimenő kapcsolatokat** engedélyezzük, avagy tiltjuk. Alapértelmezetten mindent enged kifelé és mindent tilt befelé.



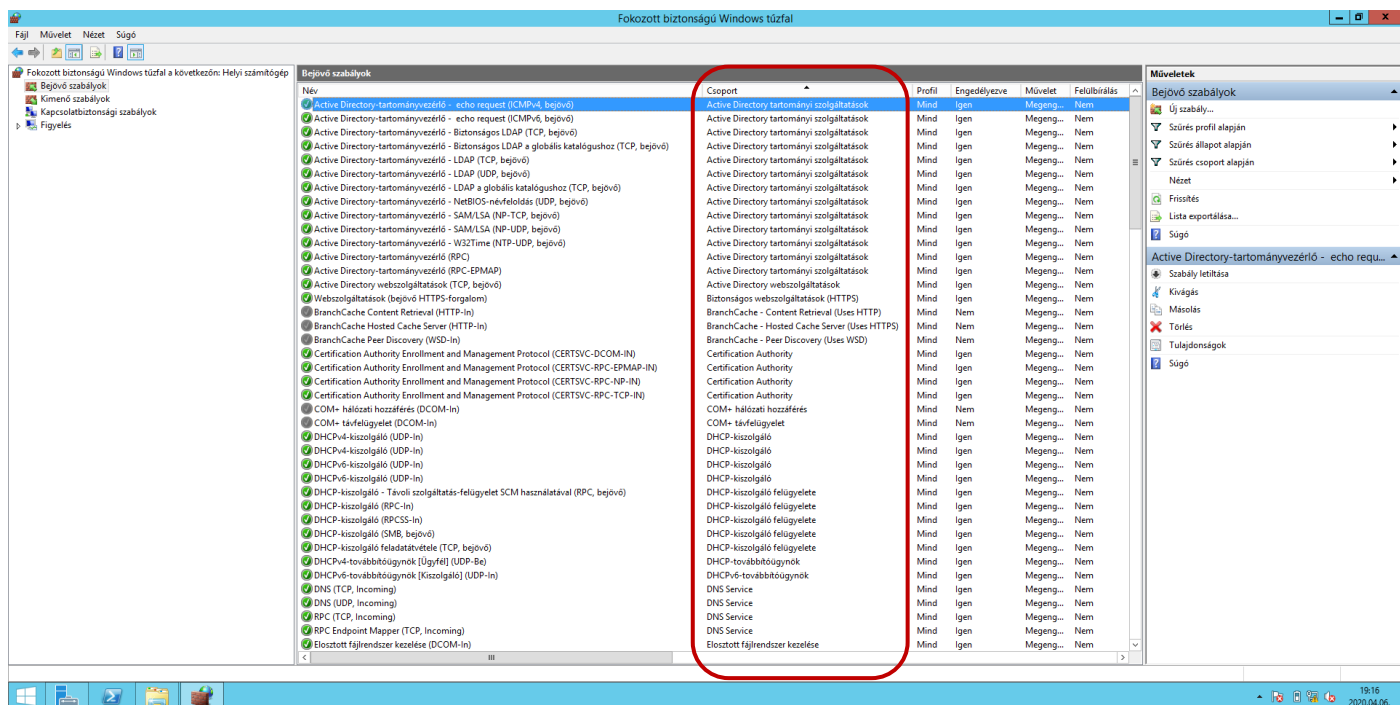
A **Beállítások / Testreszabás...** gombra kattintva kérhetünk értesítést a tűzfaltól, ha egy program szeretne a tűzfalon átjutni, de nem jogsult.

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.

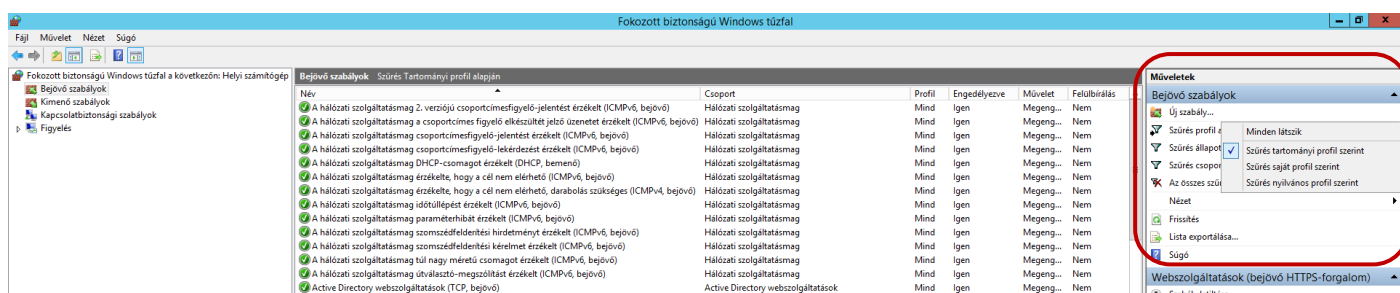


Ez egy hosszú lista a **Bejövő**- és **Kimenő szabályok** esetén is.

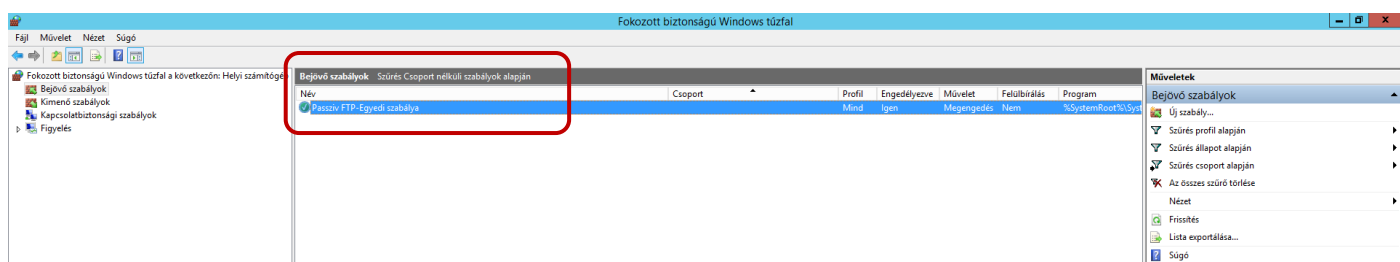
Lehet rendezni (pl. **csoport**, **portszám**, **protokoll** szerint):



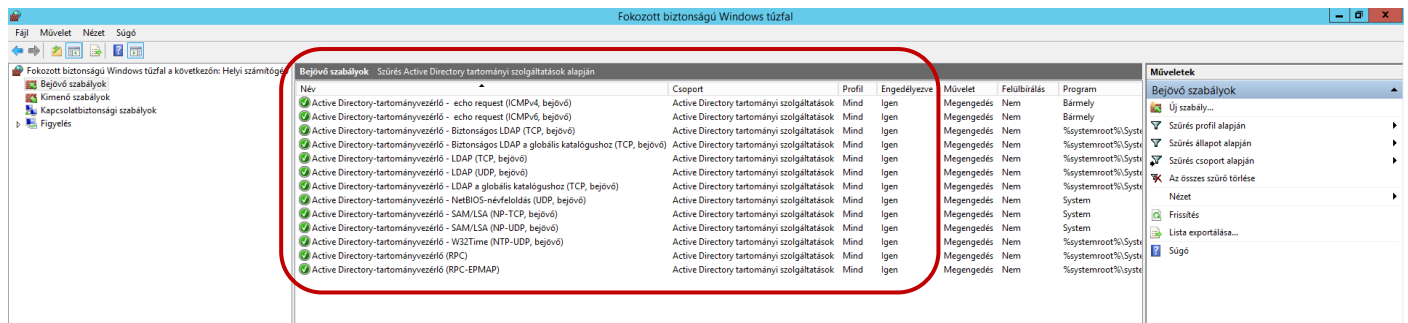
Lehet szűrni (pl. **profil**, **csoport**, **portszám**, **protokoll** szerint):



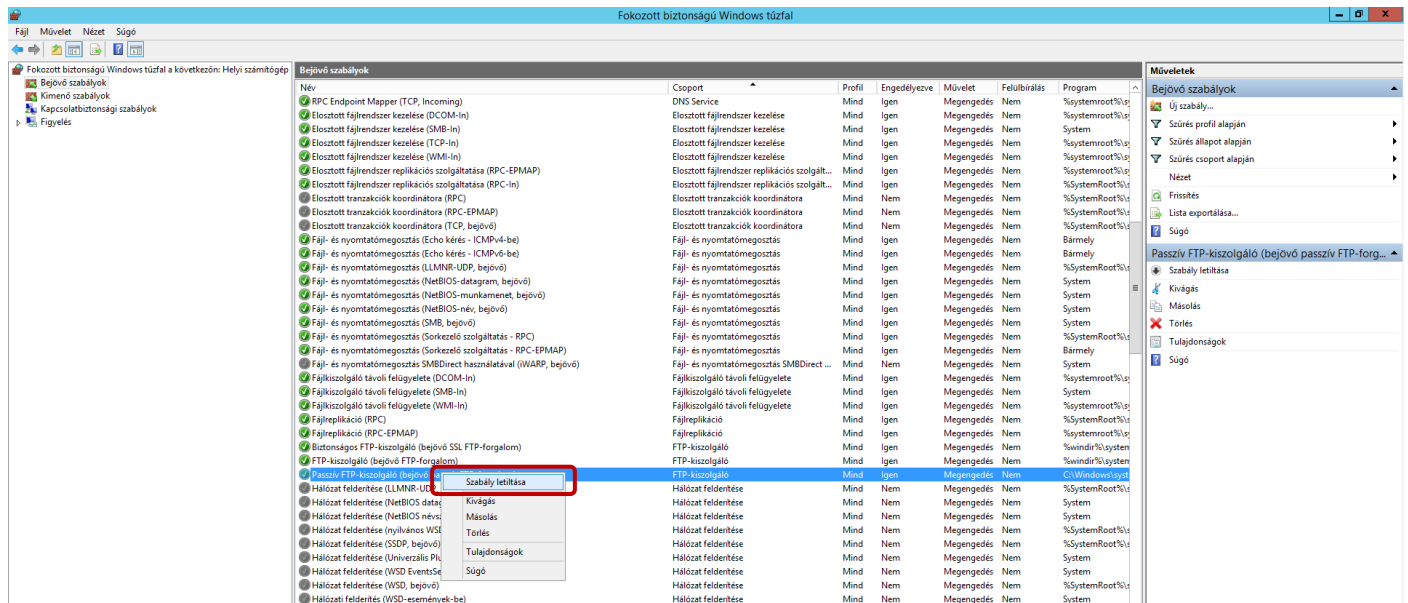
Van lehetőség a **csoport nélküli** (pl. általunk létrehozott) szabályok szűrésére is:



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



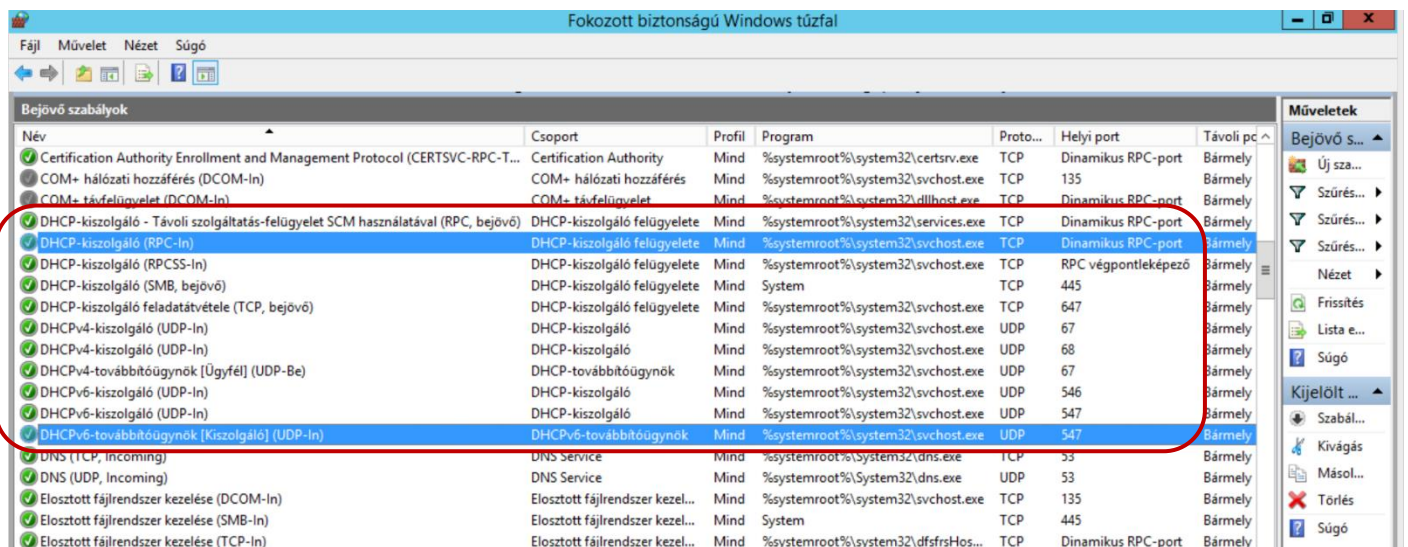
A szabályok Engedélyezhetőek / Tilthatóak



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

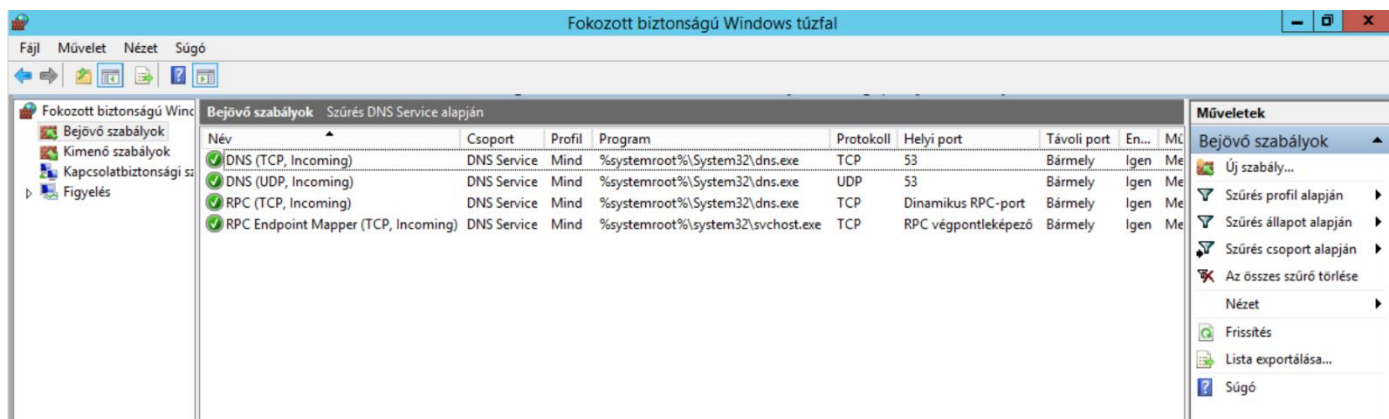
DHCP

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



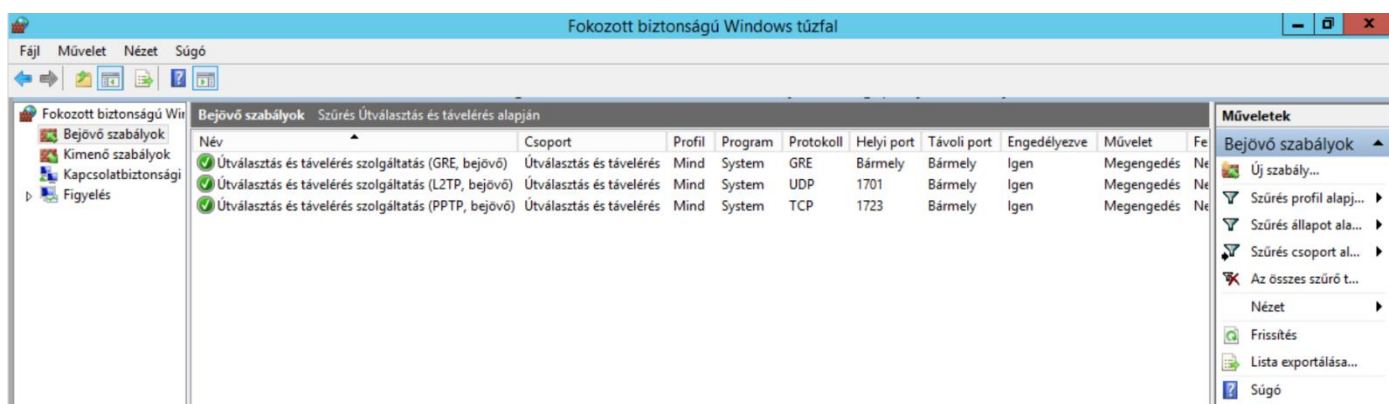
DNS

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



Távélerés (VPN)

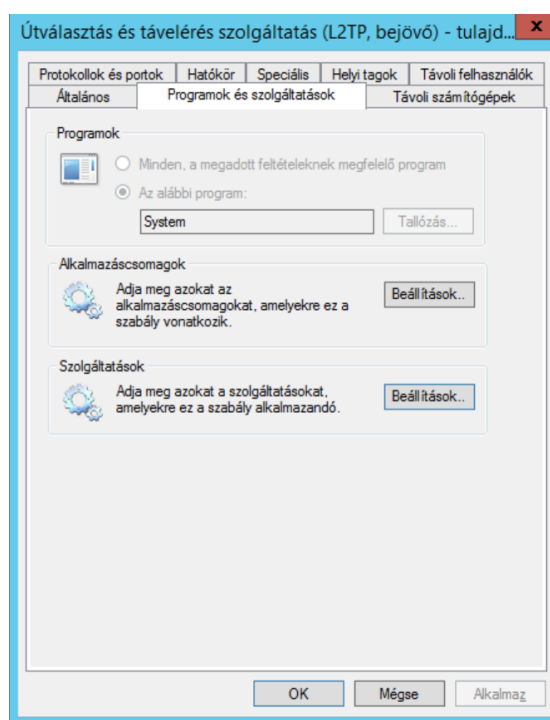
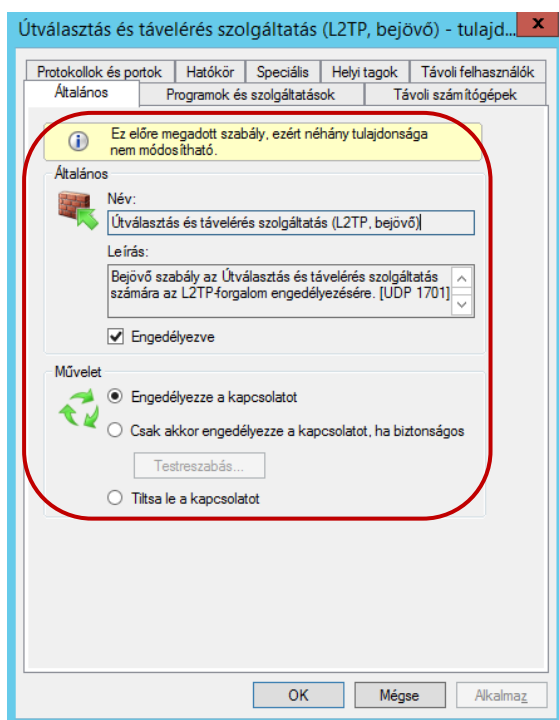
A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat!



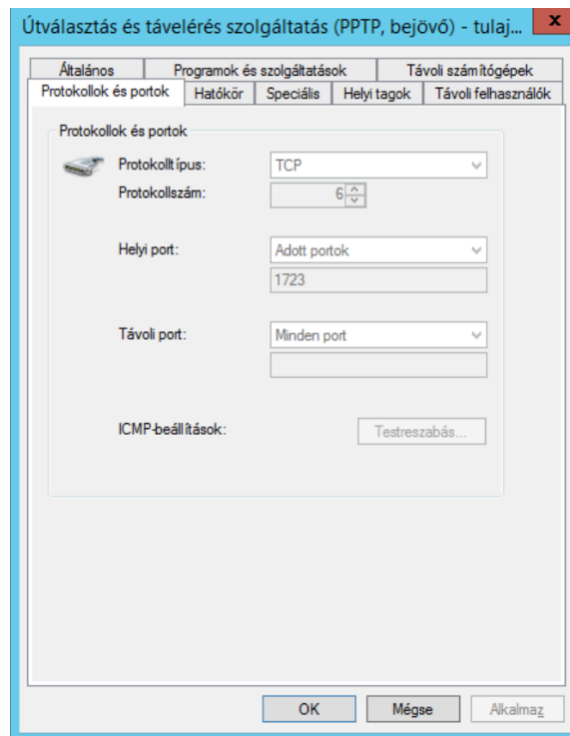
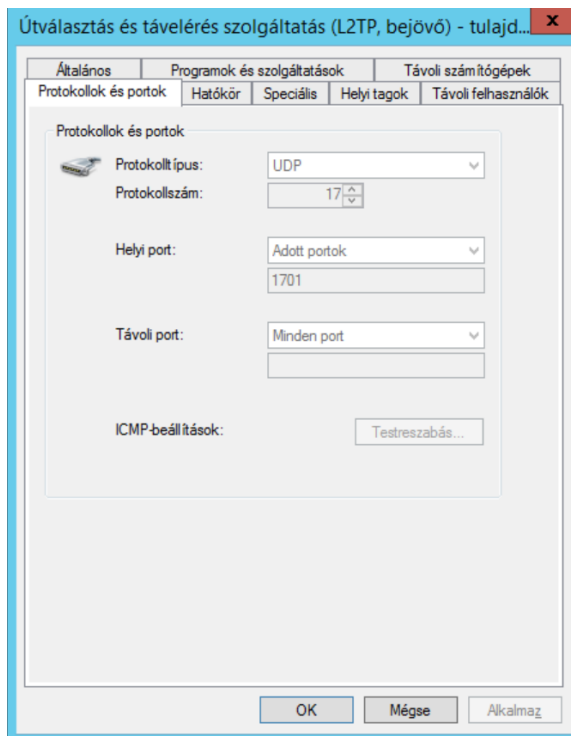
Ha az egyik ide tartozó szabályon duplán kattintva megnézhetjük a tulajdonságait. A képen az **L2TP protokollhoz** tartozó szabály részleteit látjuk. A rendszer által létrehozott szabályok nem módosíthatóak.

De tudjuk engedélyezni / tiltani a szabályt.

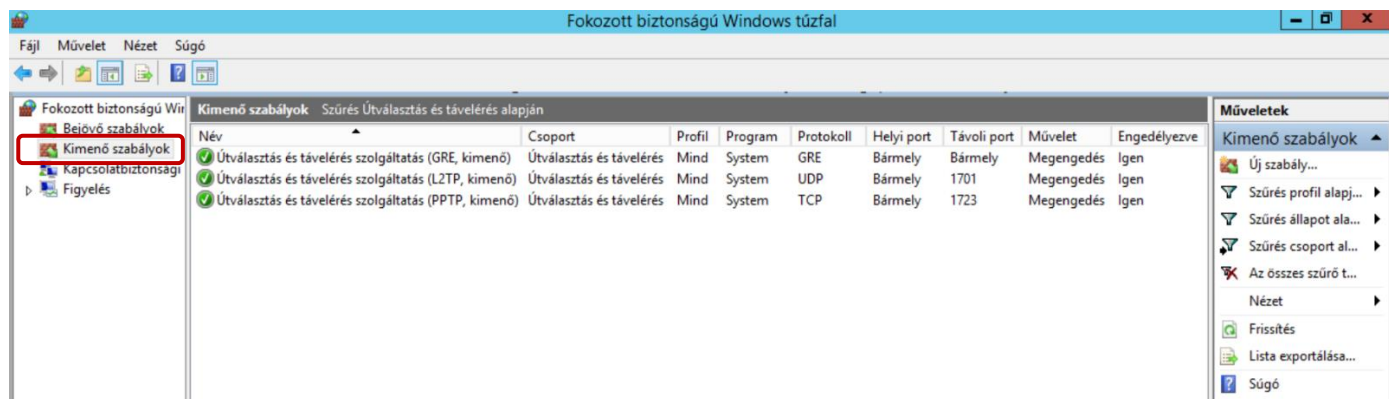
A **Program**, ami használja csak egyszerűen a **System**.



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

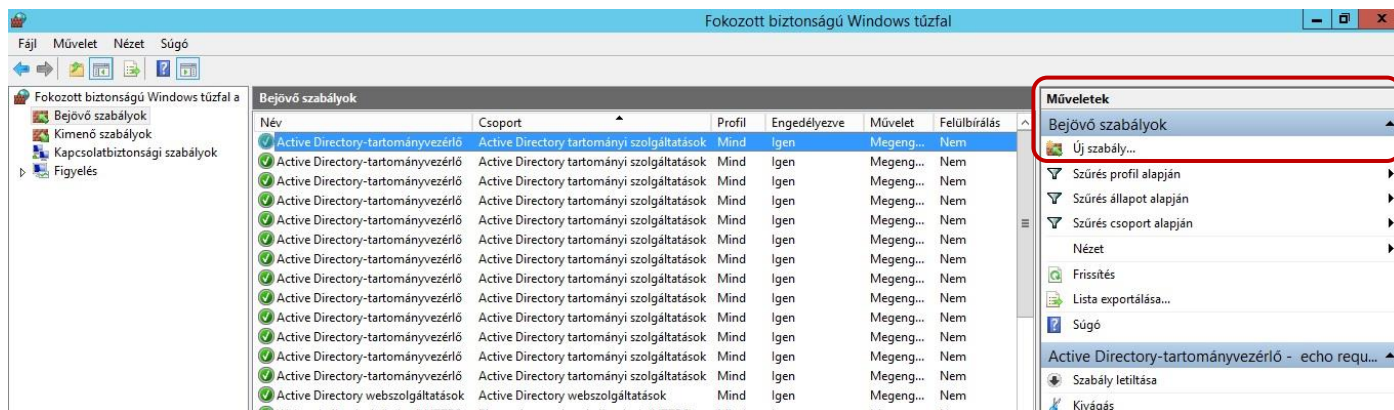


Nézzük meg a **Kimenő szabályok** között is a **Távélerés szabályait**. A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat! (Kifelé irányban nem tiltjuk a forgalmat; de a szabály létezik, ami átengedné!)

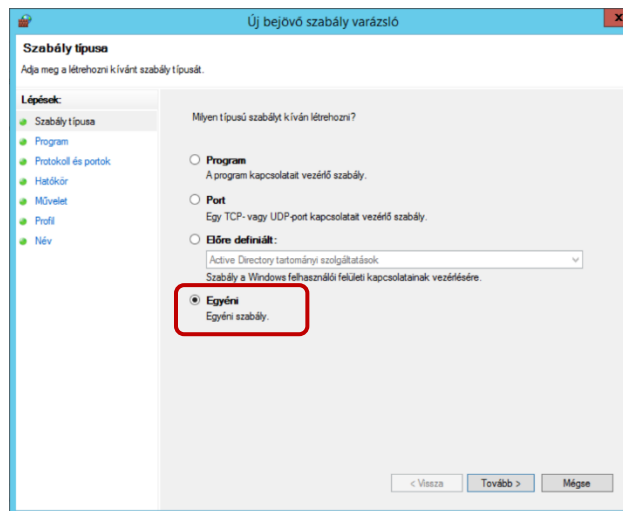


Nézzük meg, hogy tudunk **saját szabályokat** létrehozni. A legegyszerűbb ilyen szabály talán a **PING** parancs forgalmának engedélyezése.

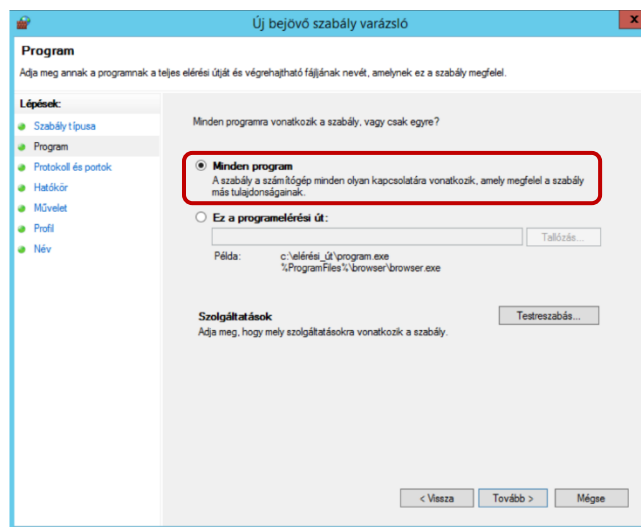
Bejövő szabályt hozunk hozzá létre:



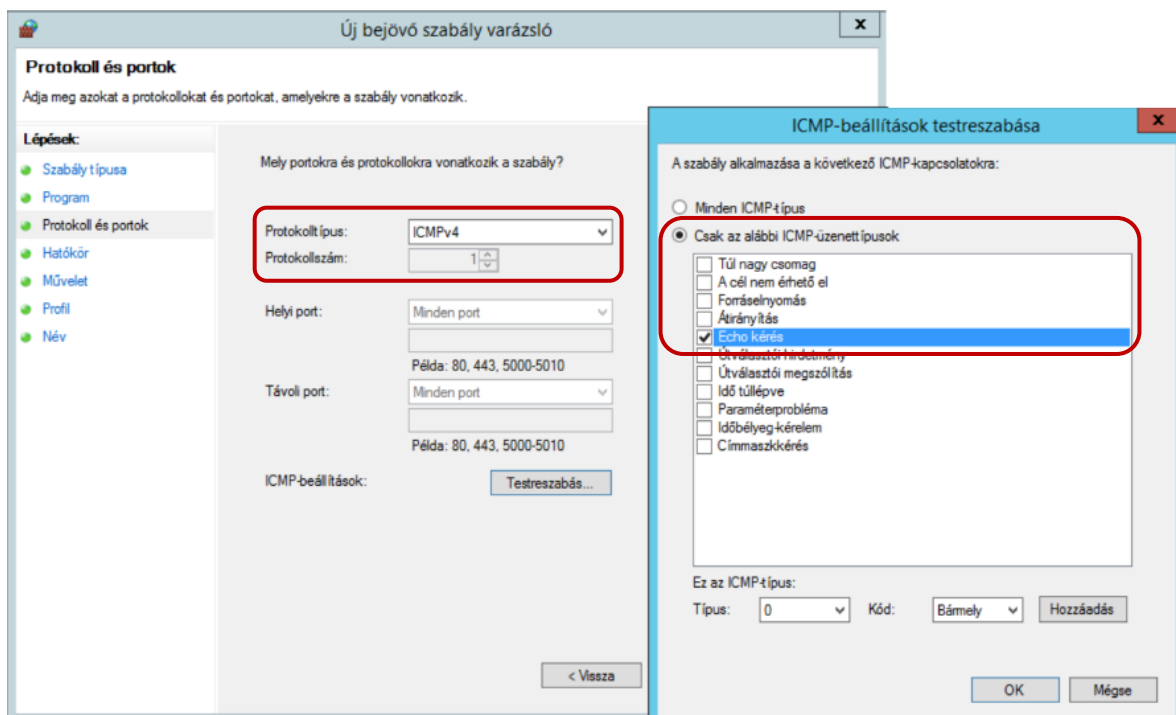
Egyéni szabályt hozunk létre:



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 szerveret PING kérések:

Új bejövő szabály varázsló

Hatókör
Adja meg azokat a helyi és távoli IP-címeket, amelyekre a szabály vonatkozik.

Lépések:

- Szabály típusa
- Program
- Protokoll és portok
- **Hatókör**
- Művelet
- Profil
- Név

Mely helyi IP-címekre vonatkozik ez a szabály?

☒ Bármely IP-cím

☐ Ezek az IP-címek:

Hozzáadás... Szerkesztés... Elávolítás

Azoknak az adapter típusoknak a testreszabása, amelyekre ez a szabály vonatkozik:

Mely távoli IP-címekre vonatkozik ez a szabály?

☒ Bármely IP-cím

☐ Ezek az IP-címek:

Hozzáadás... Szerkesztés... Elávolítás

Testreszabás...

< Vissza Tovább > Mégse

Engedélyező szabályt hozunk létre:

Új bejövő szabály varázsló

Művelet
Adja meg azt a műveletet, amelyet akkor kell végrehajtani, ha egy kapcsolat megfelel a szabályban megadott feltételeknek.

Lépések:

- Szabály típusa
- Program
- Protokoll és portok
- Hatókör
- **Művelet**
- Profil
- Név

Milyen tegyem a rendszer, ha egy kapcsolat megfelel a megadott feltételeknek?

☒ **Engedélyezze a kapcsolatot**
Ebbe az IPsec-védelemmel ellátott és a nem védett kapcsolatok is beletartoznak.

☐ **Csak akkor engedélyezze a kapcsolatot, ha biztonságos**
Ebbe csak az IPsec protokollal hitelesített kapcsolatok tartoznak bele. A kapcsolatok védelme az IPsec-tulajdonságok között megadott beállításoknak, és a Kapcsolatbiztonsági szabály csomópontnál megadott szabályoknak megfelelően történik.

Testreszabás

☐ **Tiltsa le a kapcsolatot**

< Vissza Tovább > Mégse

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

Új bejövő szabály varázsló

Profil
Adja meg azokat a profilekat, amelyekre ez a szabály vonatkozik.

Lépések:

- Szabály típusa
- Program
- Protokoll és portok
- Hatókör
- Művelet
- **Profil**
- Név

Mikor lép érvénybe ez a szabály?

☒ **Tartomány**
A számítógép vállalati tartományához való csatlakozásakor alkalmazandó.

☒ **Személyes**
A számítógép magánhálózati (például otthoni vagy munkahelyi) helyhez való csatlakozásakor alkalmazandó.

☒ **Nyilvános**
A számítógép nyilvános hálózati helyhez való csatlakozásakor alkalmazandó.

< Vissza Tovább > Mégse

Új bejövő szabály varázsló

Név
Adja meg a szabály nevét és leírását.

Lépések:

- Szabály típusa
- Program
- Protokoll és portok
- Hatókör
- Művelet
- Profil
- **Név**

Név:

PING

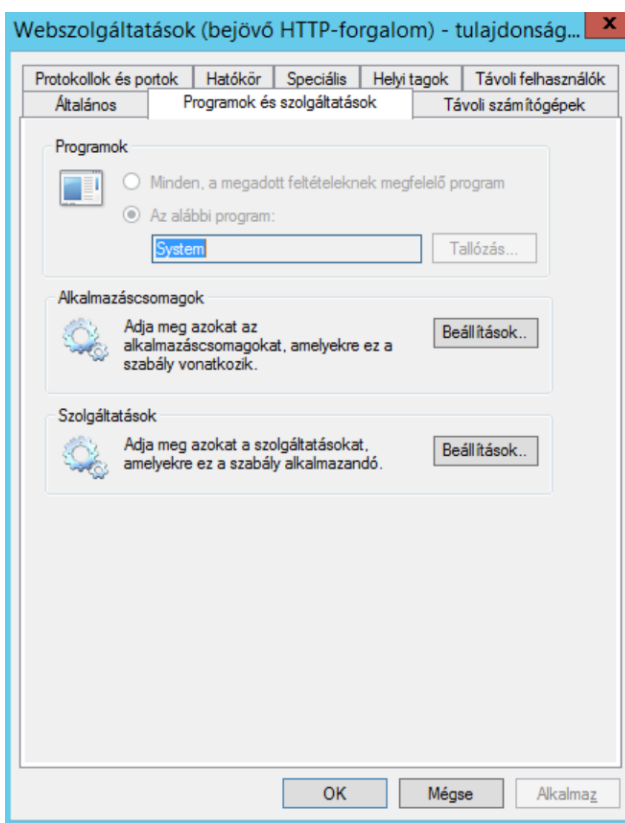
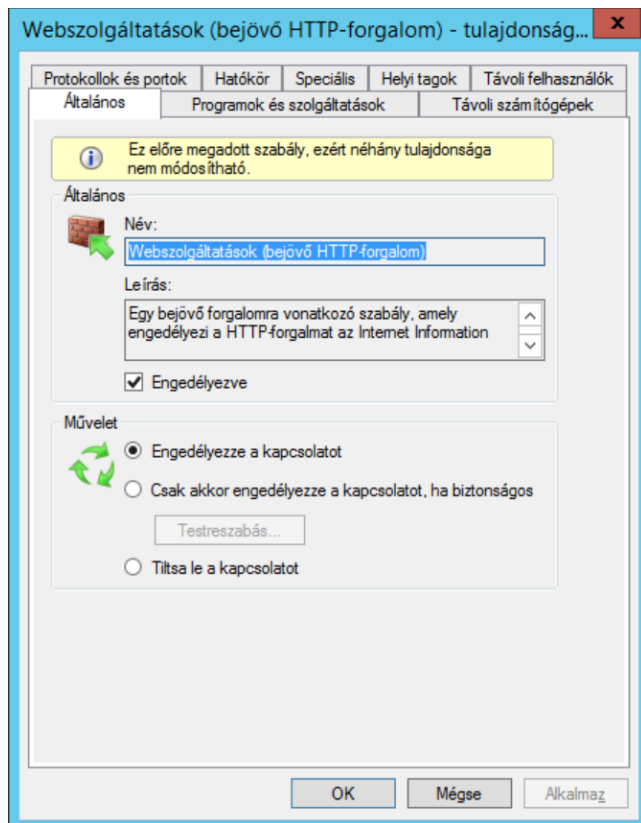
Leírás (nem kötelező):

PING engedélyezése szerver felé.

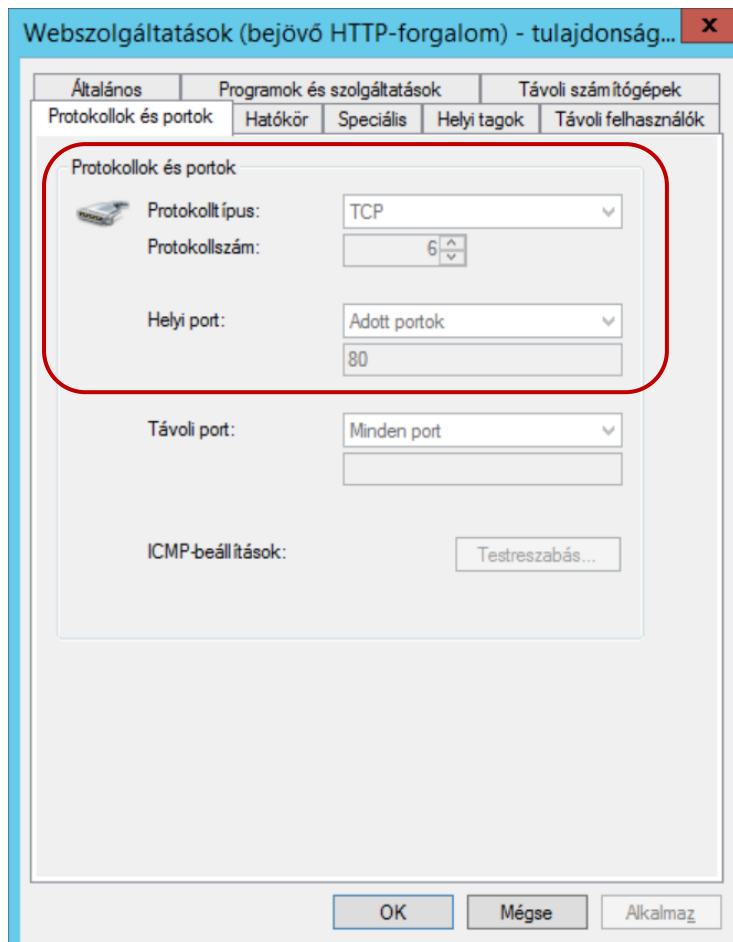
< Vissza Befejezés Mégse

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:



Ugyanez ha **https protokollt** használunk, **443-as** porton keresztül és **TCP** protokollon keresztül:

Webszolgáltatások (bejövő HTTPS-forgalom) - tulajdonságok

Protokollok és portok | Hatókör | Speciális | Helyi tagok | Távoli felhasználók

Általános | Programok és szolgáltatások | Távoli számítógépek

Ez előre megadott szabály, ezért néhány tulajdonsága nem módosítható.

Általános

Név: Webszolgáltatások (bejövő HTTPS-forgalom)

Leírás: Egy bejövő forgalomra vonatkozó szabály, amely engedélyezi a HTTPS-forgalmat az Internet Information

☒ Engedélyezve

Művelet

☒ Engedélyezze a kapcsolatot

☐ Csak akkor engedélyezze a kapcsolatot, ha biztonságos

Testreszabás...

☐ Tiltsa le a kapcsolatot

OK Mégse Alkalmaz

Webszolgáltatások (bejövő HTTPS-forgalom) - tulajdonságok

Protokollok és portok | Hatókör | Speciális | Helyi tagok | Távoli felhasználók

Általános | Programok és szolgáltatások | Távoli számítógépek

Programok

☐ Minden, a megadott feltételeknek megfelelő program

☒ Az alábbi program:

System Tallózás...

Alkalmazáscsomagok

Adja meg azokat az alkalmazáscsomagokat, amelyekre ez a szabály vonatkozik. Beállítások...

Szolgáltatások

Adja meg azokat a szolgáltatásokat, amelyekre ez a szabály alkalmazandó. Beállítások...

OK Mégse Alkalmaz

Webszolgáltatások (bejövő HTTPS-forgalom) - tulajdonságok

Általános | Programok és szolgáltatások | Távoli számítógépek

Protokollok és portok | Hatókör | Speciális | Helyi tagok | Távoli felhasználók

Protokollok és portok

Protokolltípus: TCP

Protokollsorszám: 6

Helyi port: Adott portok

443

Távoli port: Minden port

ICMP-beállítások: Testreszabás...

OK Mégse Alkalmaz

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

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

The 'Webszolgáltatások - HTTP 8080 - tulajdonságok' dialog box is shown with the 'Általános' tab selected. The 'Név' field contains 'Webszolgáltatások - HTTP 8080' and the 'Leírás' field contains '8080'. The 'Engedélyezve' checkbox is checked. Under the 'Művelet' section, the 'Engedélyezze a kapcsolatot' radio button is selected. The 'OK', 'Mégse', and 'Alkalmaz' buttons are at the bottom.

The 'Webszolgáltatások - HTTP 8080 - tulajdonságok' dialog box is shown with the 'Programok és szolgáltatások' tab selected. The 'Programok' section has the 'Az alábbi program:' radio button selected, with 'System' entered in the text box. The 'Alkalmazáscsomagok' and 'Szolgáltatások' sections have 'Beállítások...' buttons. The 'OK', 'Mégse', and 'Alkalmaz' buttons are at the bottom.

The 'Webszolgáltatások - HTTP 8080 - tulajdonságok' dialog box is shown with the 'Protokollok és portok' tab selected. The 'Protokolltípus' is set to 'TCP' and the 'Protokollsorszám' is set to '6'. The 'Helyi port' is set to 'Adott portok' with '8080' entered in the text box. The 'Távoli port' is set to 'Minden port'. The 'ICMP-beállítások' section has a 'Testreszabás...' button. The 'OK', 'Mégse', and 'Alkalmaz' buttons are at the bottom.

Biztonságos webes kapcsolathoz (**https** protokollal, **4433**-as porton keresztül)

Webszolgáltatások - HTTPS 4433 - tulajdonságok

Protokollok és portok | Hatókör | Speciális | Helyi tagok | Távoli felhasználók

Általános | Programok és szolgáltatások | Távoli számítógépek

Általános

Név: Webszolgáltatások - HTTPS 4433

Leírás: 4433

☒ Engedélyezve

Művelet

☒ Engedélyezze a kapcsolatot

☐ Csak akkor engedélyezze a kapcsolatot, ha biztonságos

Testreszabás...

☐ Tiltsa le a kapcsolatot

OK Mégse Alkalmaz

Webszolgáltatások - HTTPS 4433 - tulajdonságok

Protokollok és portok | Hatókör | Speciális | Helyi tagok | Távoli felhasználók

Általános | Programok és szolgáltatások | Távoli számítógépek

Programok

☐ Minden, a megadott feltételeknek megfelelő program

☒ Az alábbi program:

System Tallózás...

Alkalmazáscsomagok

Adja meg azokat az alkalmazáscsomagokat, amelyekre ez a szabály vonatkozik. Beállítások...

Szolgáltatások

Adja meg azokat a szolgáltatásokat, amelyekre ez a szabály alkalmazandó. Beállítások...

OK Mégse Alkalmaz

Webszolgáltatások - HTTPS 4433 - tulajdonságok

Általános | Programok és szolgáltatások | Távoli számítógépek

Protokollok és portok | Hatókör | Speciális | Helyi tagok | Távoli felhasználók

Protokollok és portok

Protokolltípus: TCP

Protokollszám: 6

Helyi port: Adott portok

4433

Példa: 80, 443, 5000-5010

Távoli port: Minden port

Példa: 80, 443, 5000-5010

ICMP-beállítások: Testreszabás...

OK Mégse Alkalmaz

FTP kiszolgáló

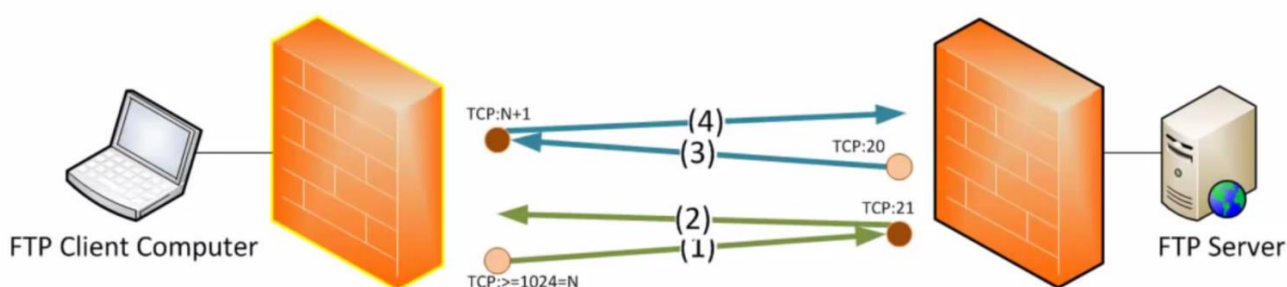
Kétféle módon működhet az FTP kiszolgáló és ennek megfelelően a tűzfal szabályokat is kétféleképpen hozhatjuk létre. Annak megfelelően, hogyan szeretnénk működtetni az FTP kiszolgálónkat.

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:

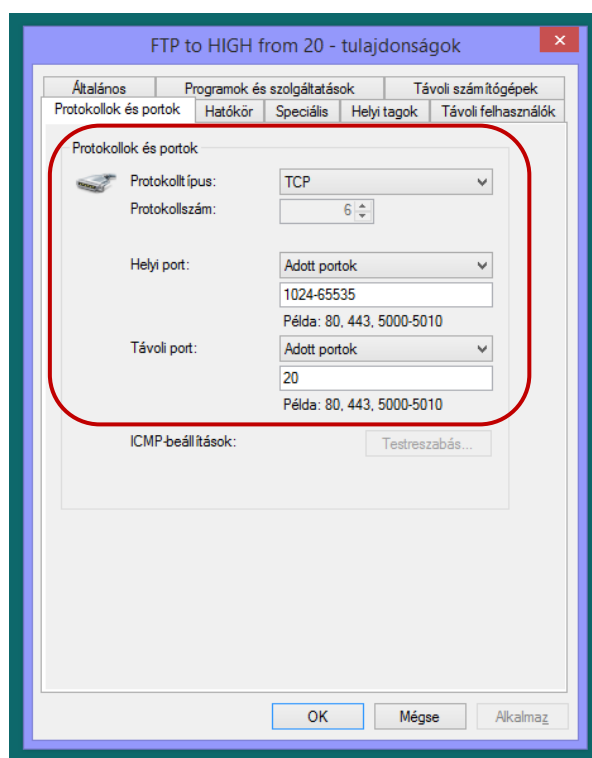
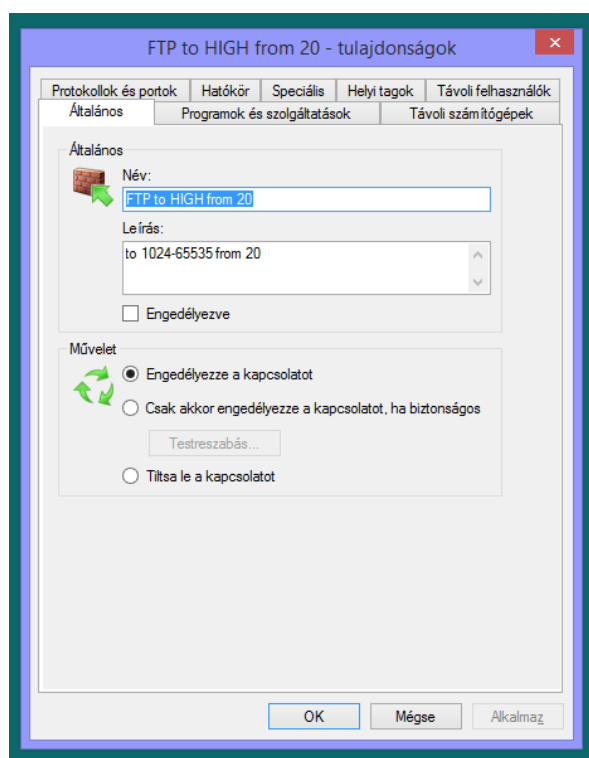
Szerveren:

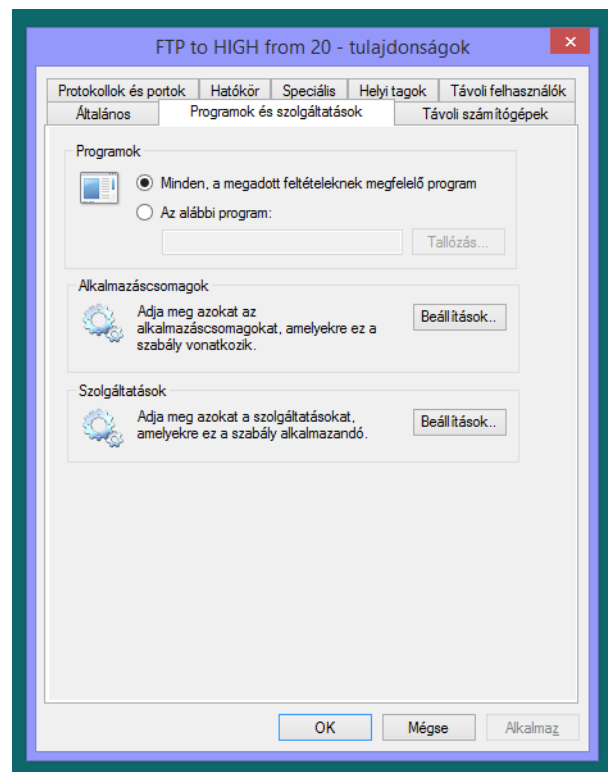
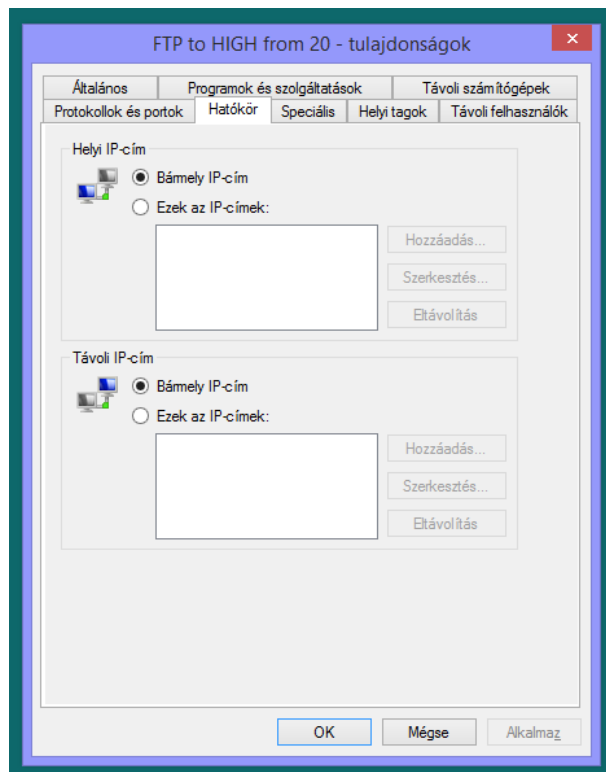
Bejövő szabály: nem igényel beállítást, a rendszer felvette a szükséges szabályt!

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

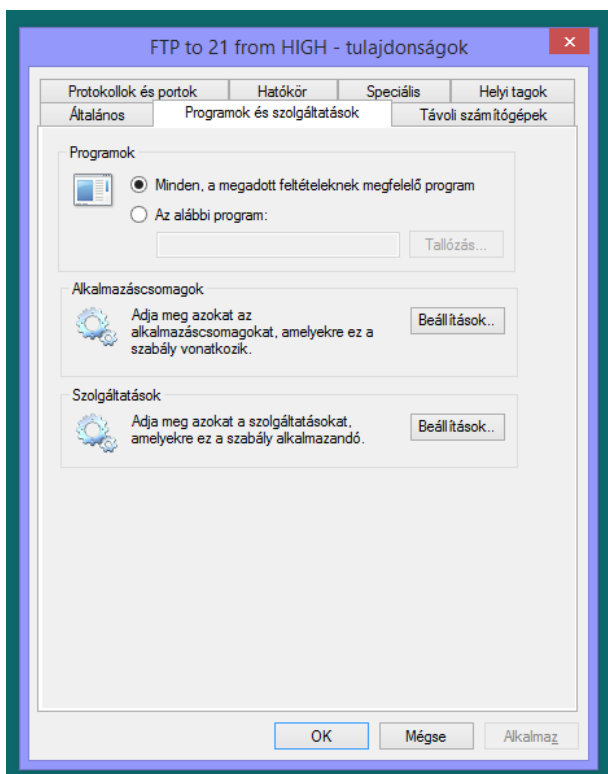
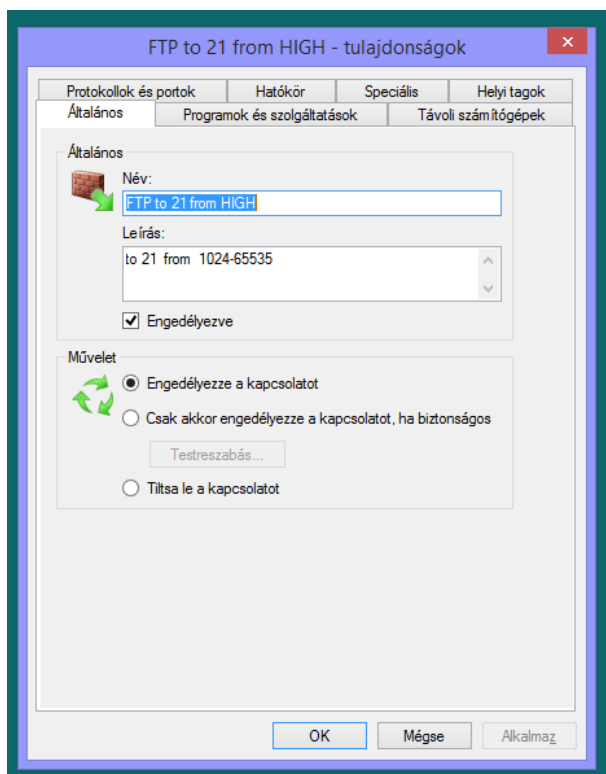
Kliensen:

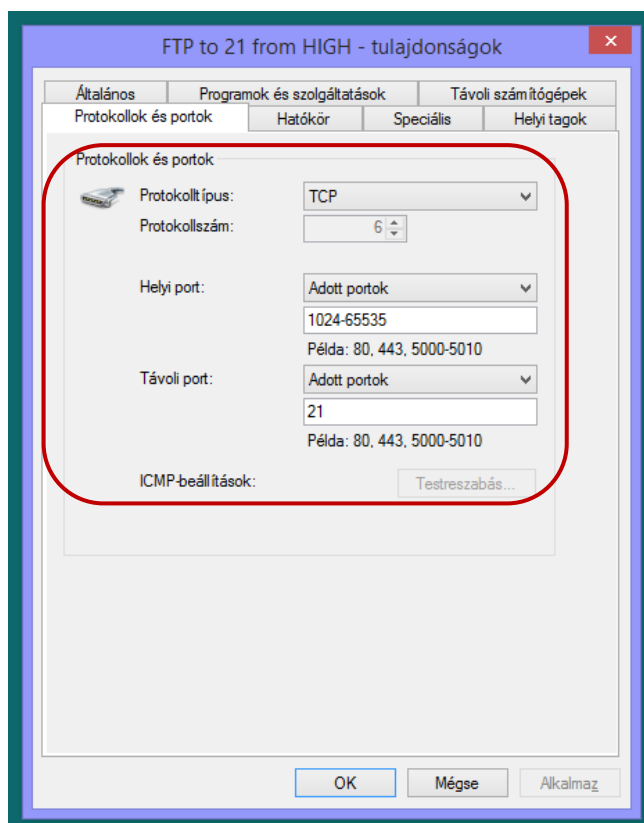
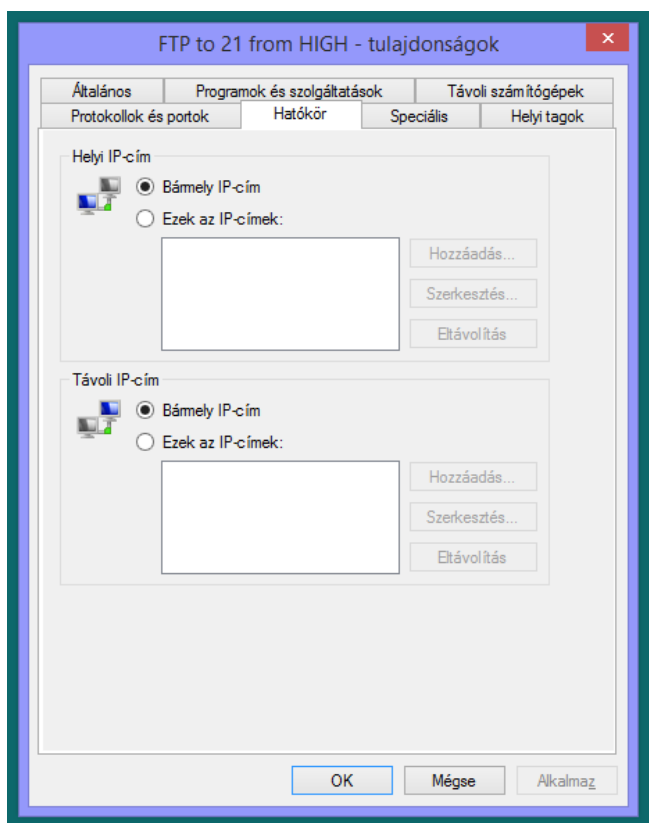
Bejövő szabály: (a képen **még** nincs engedélyezve!)





Kimenő szabály:



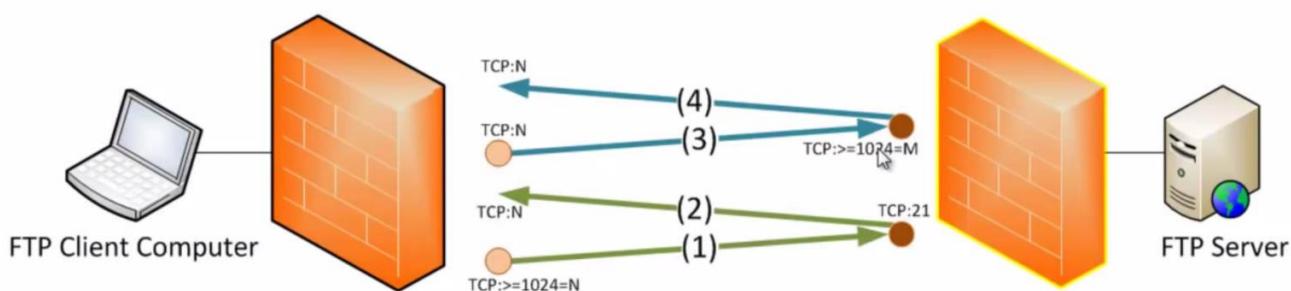


Passzív FTP

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!

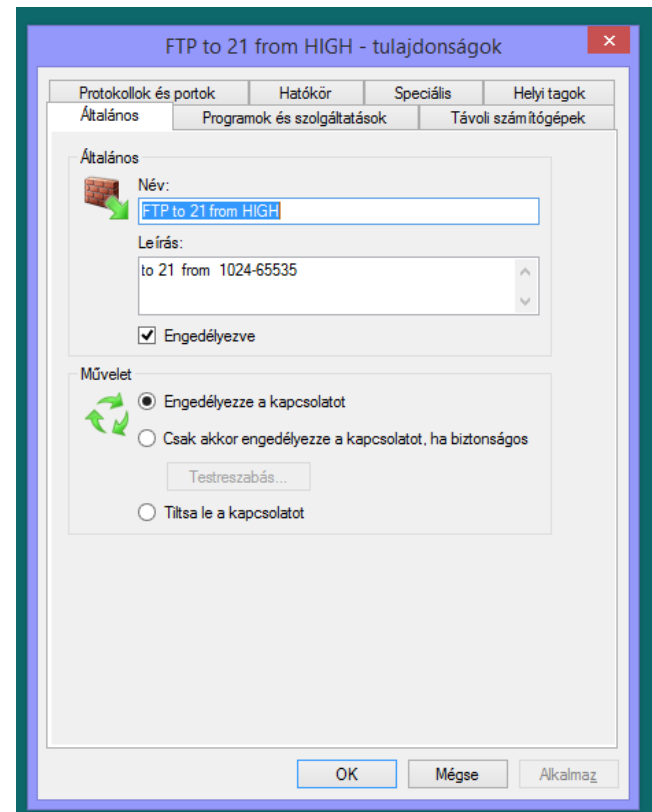
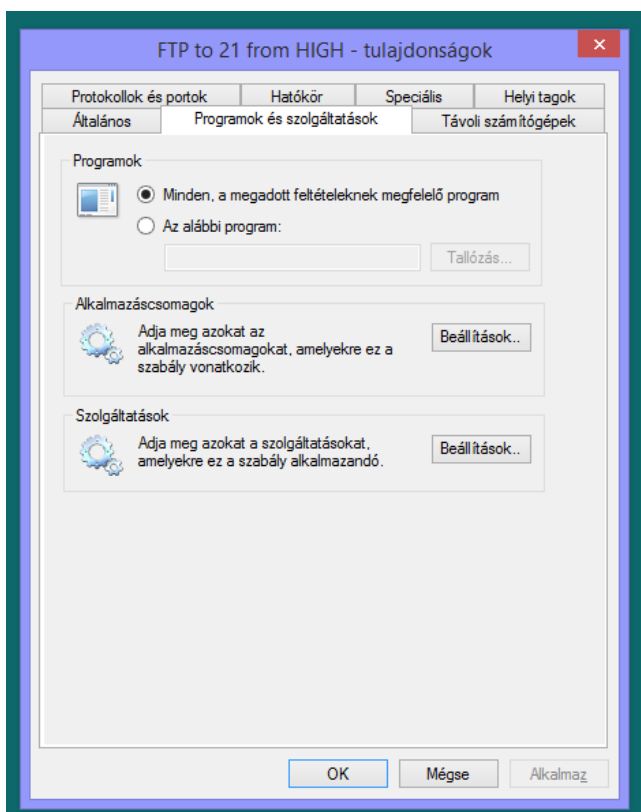
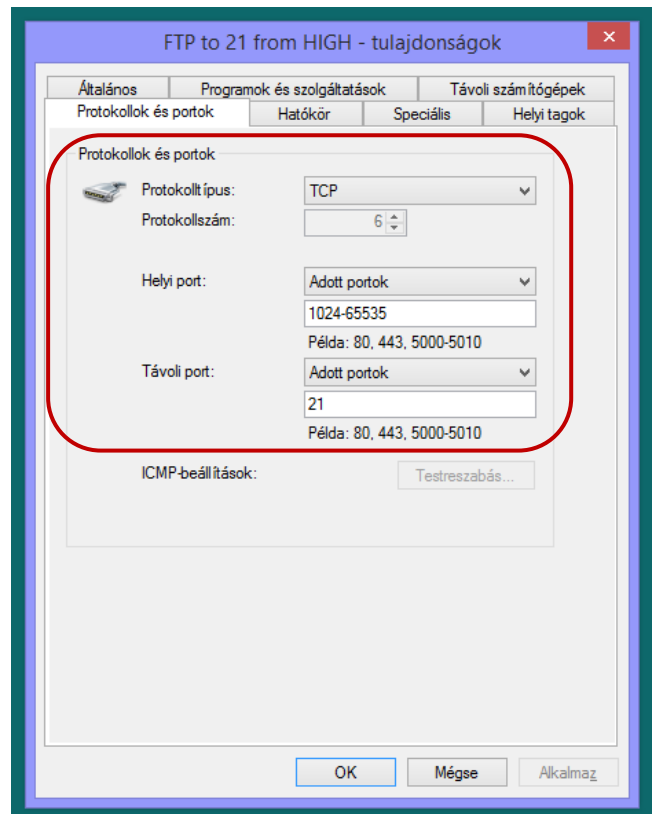
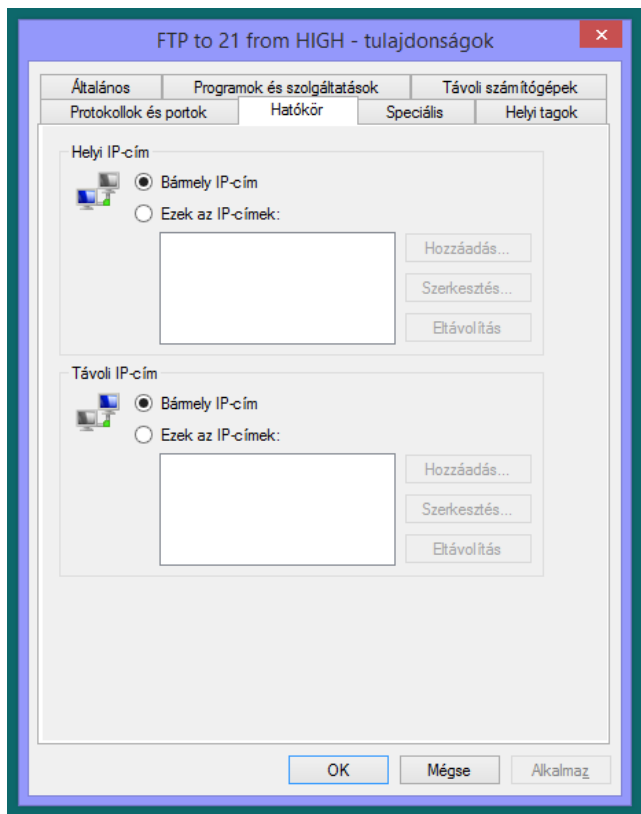
Kimenő szabály: nem igényel szabályt!

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 szervert magas portjaihoz**:

FTP to HIGH from HIGH - tulajdonságok

Protokollok és portok Hatókör Speciális Helyi tagok

Általános Programok és szolgáltatások Távoli számítógépek

Általános

Név: FTP to HIGH from HIGH

Leírás: 1024-65535 to 1024-65535

☒ Engedélyezve

Művelet

☒ Engedélyezze a kapcsolatot

☐ Csak akkor engedélyezze a kapcsolatot, ha biztonságos

Testreszabás...

☐ Tiltsa le a kapcsolatot

OK Mégse Alkalmaz

FTP to HIGH from HIGH - tulajdonságok

Protokollok és portok Hatókör Speciális Helyi tagok

Általános Programok és szolgáltatások Távoli számítógépek

Programok

☒ Minden, a megadott feltételeknek megfelelő program

☐ Az alábbi program:

Tallózás...

Alkalmazáscsomagok

Adja meg azokat az alkalmazáscsomagokat, amelyekre ez a szabály vonatkozik.

Beállítások...

Szolgáltatások

Adja meg azokat a szolgáltatásokat, amelyekre ez a szabály alkalmazandó.

Beállítások...

OK Mégse Alkalmaz

FTP to HIGH from HIGH - tulajdonságok

Általános Programok és szolgáltatások Távoli számítógépek

Protokollok és portok Hatókör Speciális Helyi tagok

Protokollok és portok

Protokolltípus: TCP

Protokollszám: 6

Helyi port: Adott portok

1024-65535

Példa: 80, 443, 5000-5010

Távoli port: Adott portok

1024-65535

Példa: 80, 443, 5000-5010

ICMP-beállítások: Testreszabás...

OK Mégse Alkalmaz

FTP to HIGH from HIGH - tulajdonságok

Általános Programok és szolgáltatások Távoli számítógépek

Protokollok és portok Hatókör Speciális Helyi tagok

Helyi IP-cím

☒ Bármely IP-cím

☐ Ezek az IP-címek:

Hozzáadás... Szerkesztés... Eltávolítás

Távoli IP-cím

☒ Bármely IP-cím

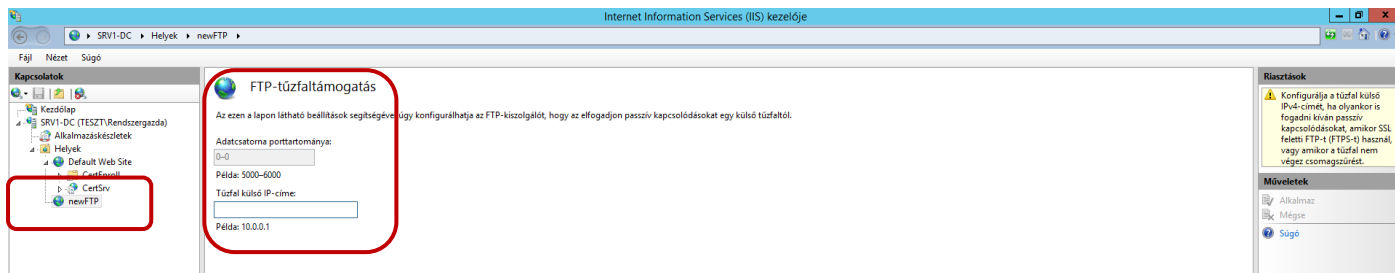
☐ Ezek az IP-címek:

Hozzáadás... Szerkesztés... Eltávolítás

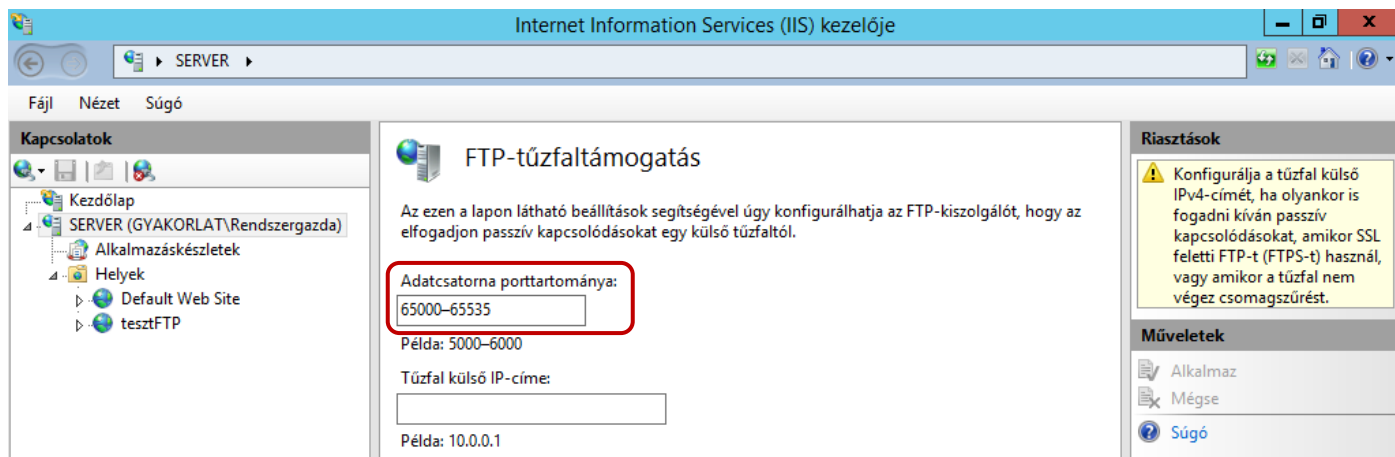
OK Mégse Alkalmaz

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

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



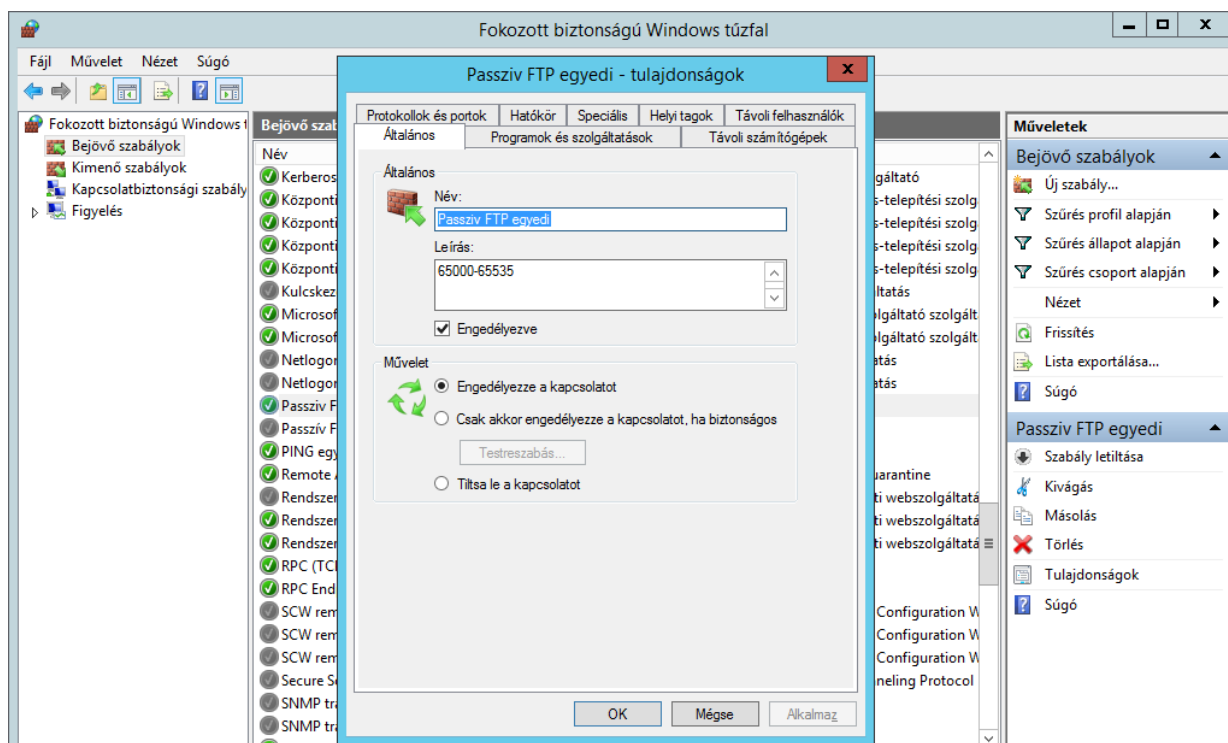
Ez a szerver szintű beállítás: (a képen a kiosztott portok: 65000-65535):



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

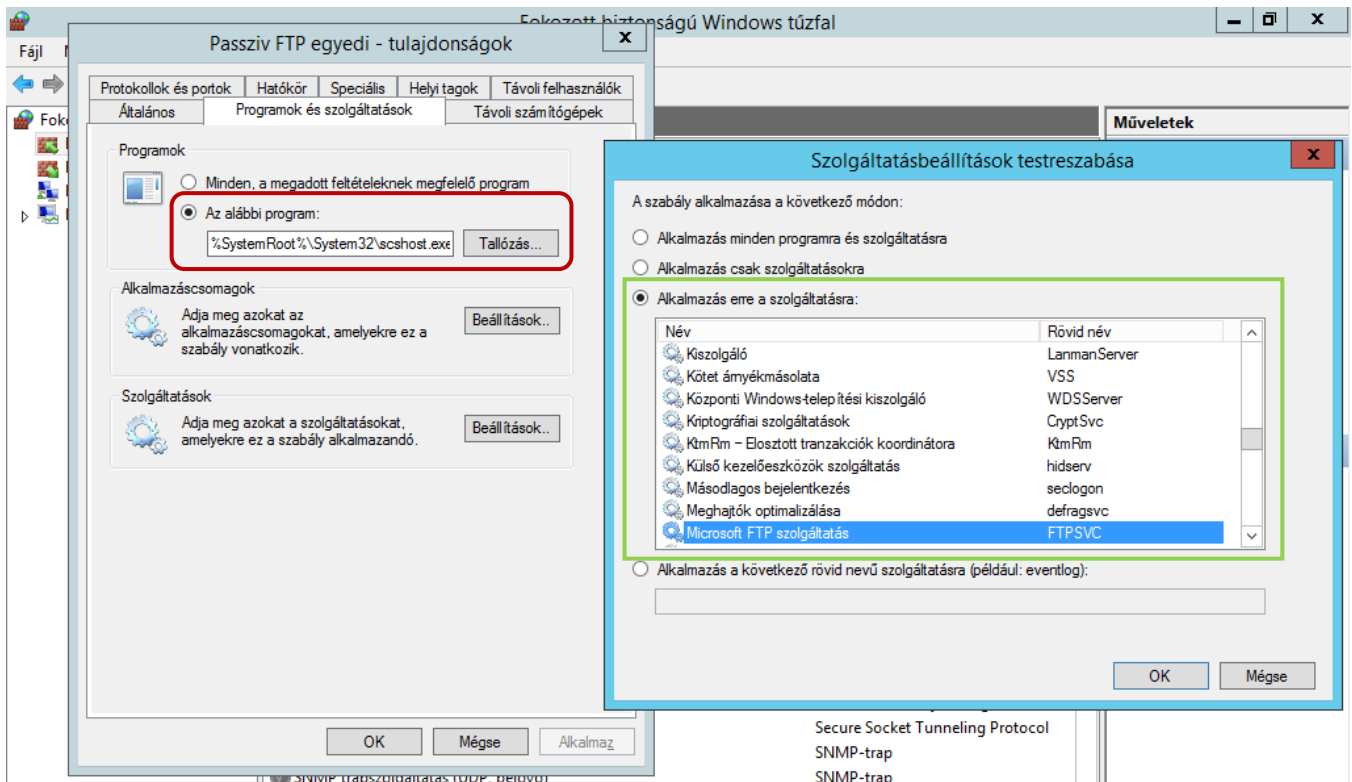
A tűzfalon a rendszer által (az *alapértelmezett Passzív FTP kapcsolathoz*) létrehozott szabályt keressük meg és **TILTSUK LE!**

Hozunk létre egy új szabályt az alábbi beállításokkal:

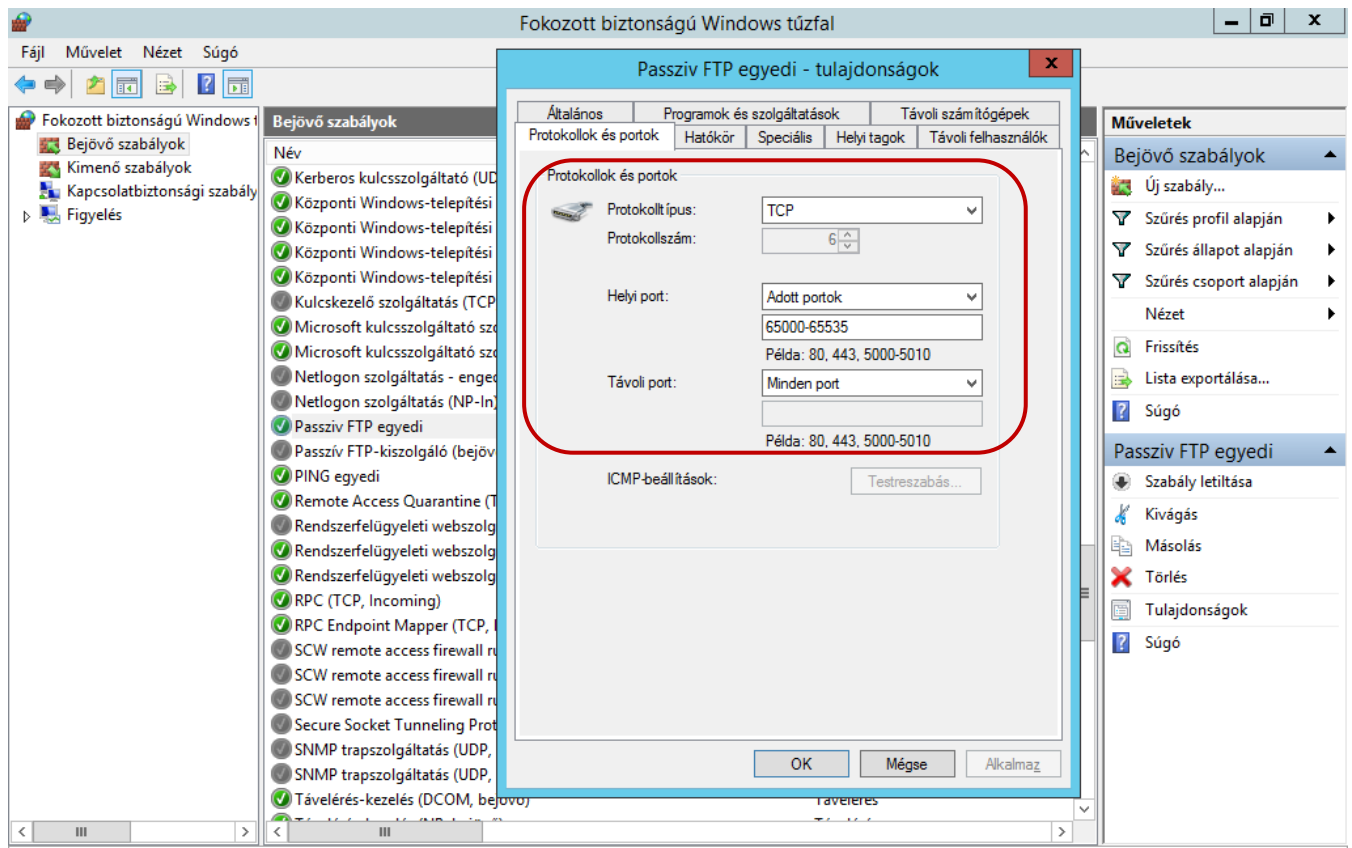


Nem minden programnak nyitjuk meg a porttartományt, csak (a képen látható módon) az FTP szolgáltatásnak!

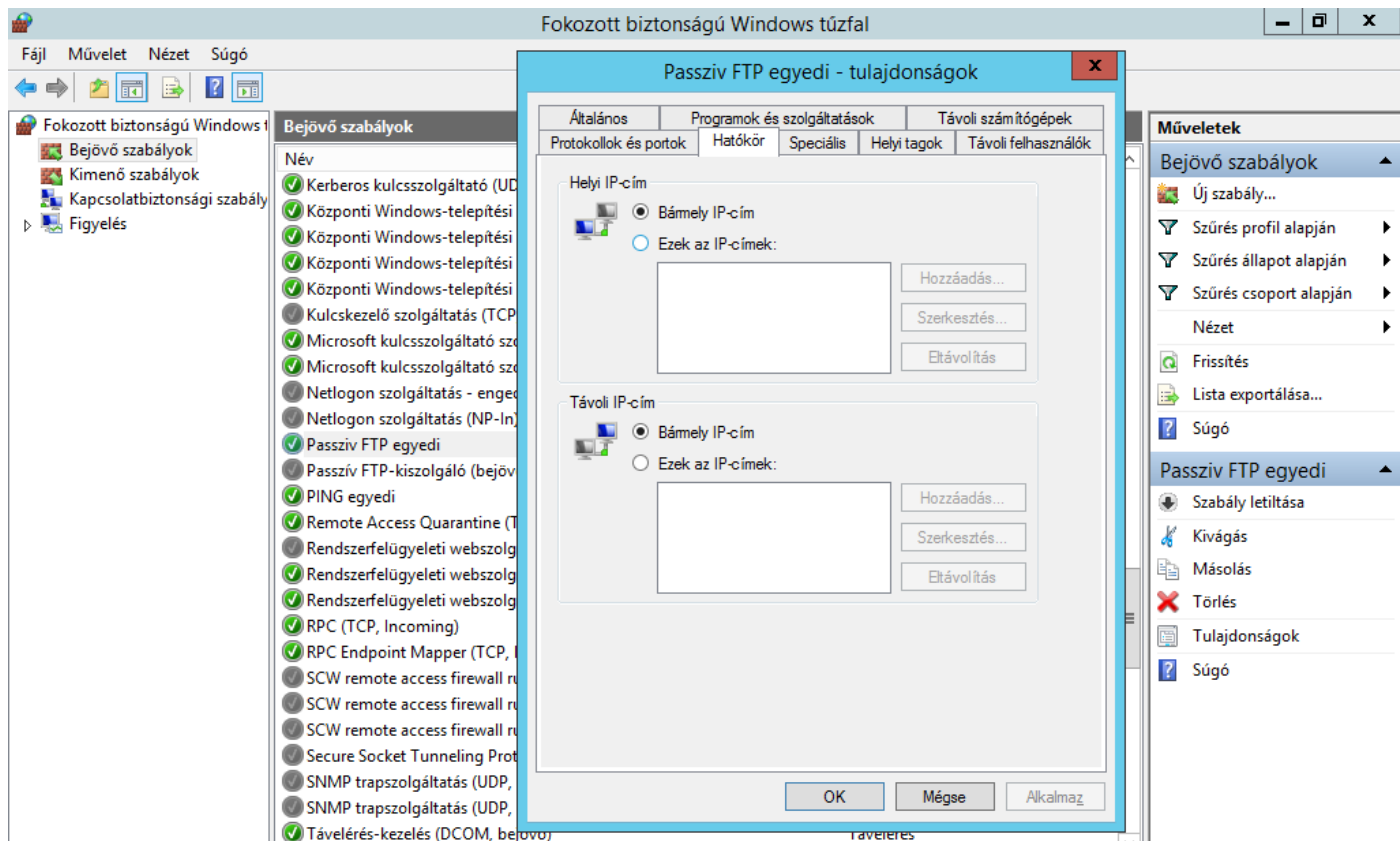
(Az *scshost.exe*, mint szolgáltatáskezelő részére és azon belül a **Microsoft FTP szolgáltatás** FTPSVC)



Beállítjuk a protokollt (**TCP**) és a porttartományt (**65000 - 65535**):



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



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:

