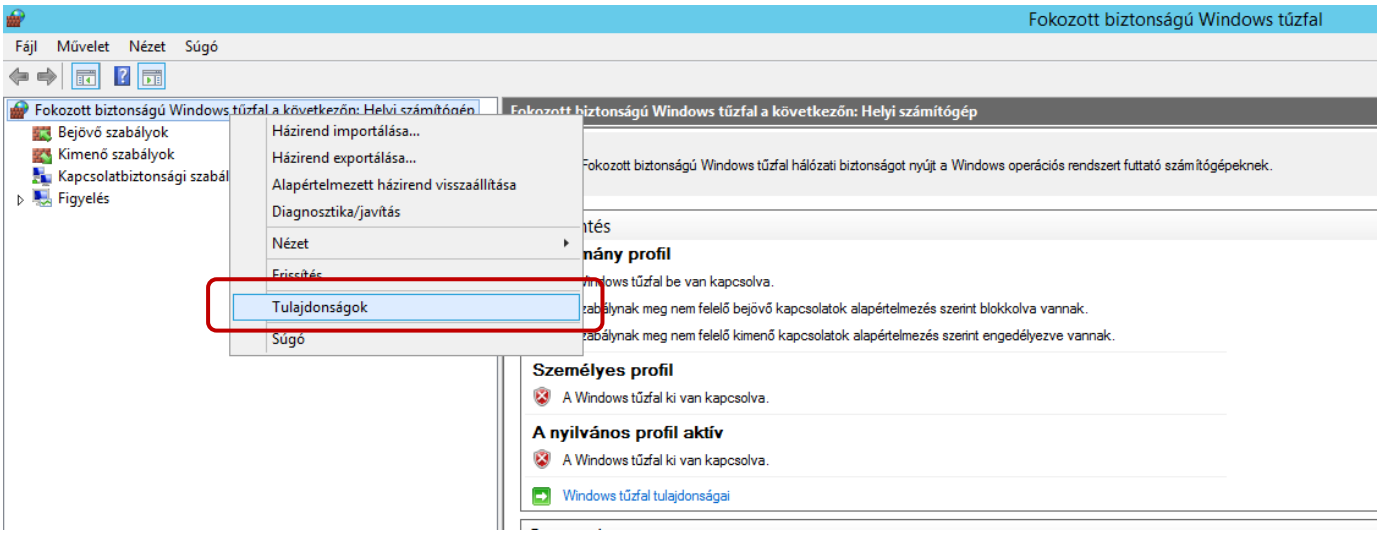
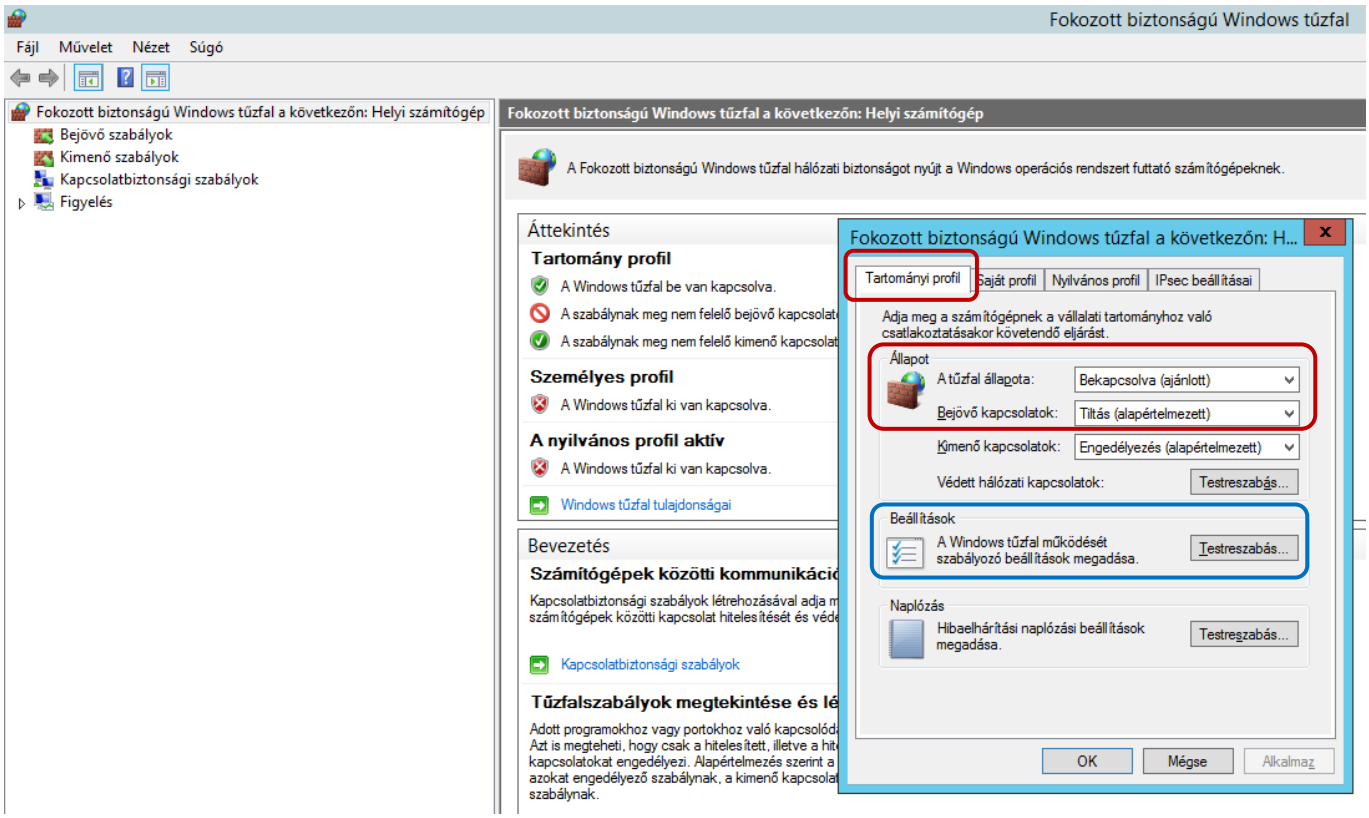
**Tűzfal beállítása**

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*:

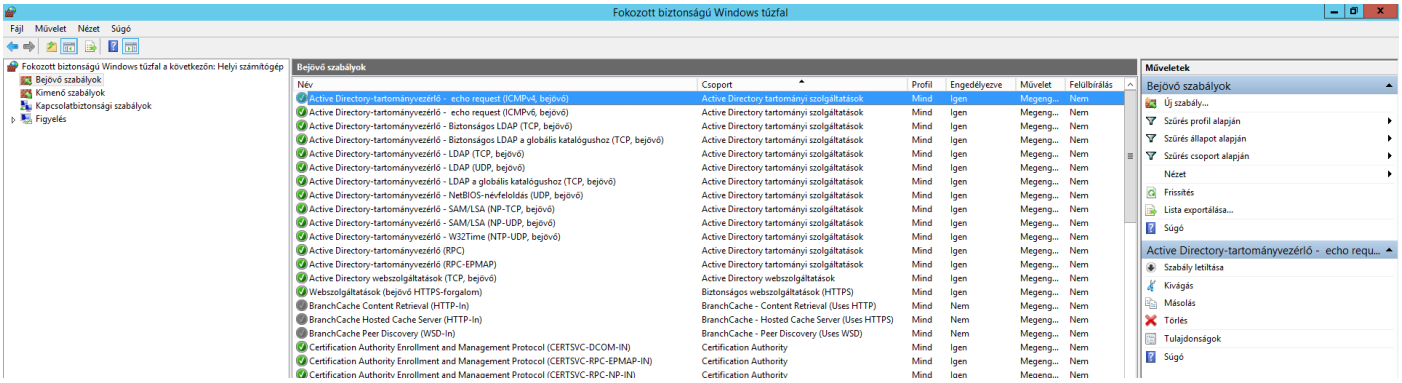



A tűzfalon ***Profilokhoz*** rendelve állíthatjuk ***Be/Ki*** állapotba a tűzfalat; illetve, hogy a ***Bejövő***- és ***Kimenő kapcsolatokat*** engedélyezzük, avagy tiltjuk. *Alapértelmezetten mindent enged kifelé és mindent tilt befelé*.



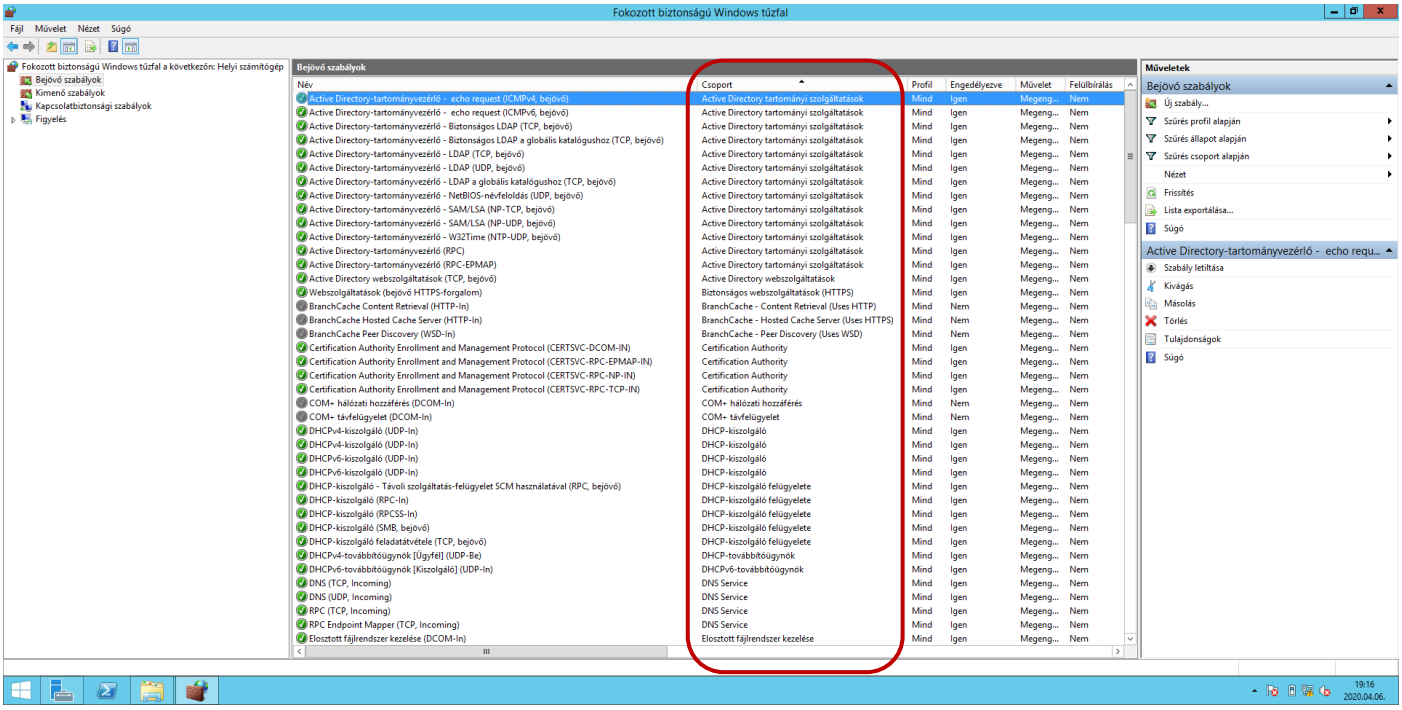

A **Beállítások / Testreszabás…** gombra kattintva kérhetünk értesítést a tűzfaltól, ha egy program szeretne a tűzfalon átjutni, de nem jogosult.

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.

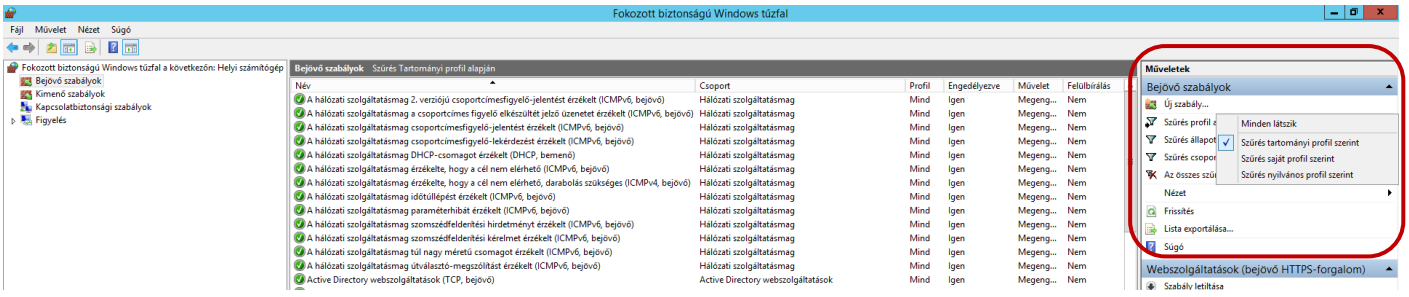



Ez egy hosszú lista a ***Bejövő***- és ***Kimenő szabályok*** esetén is.

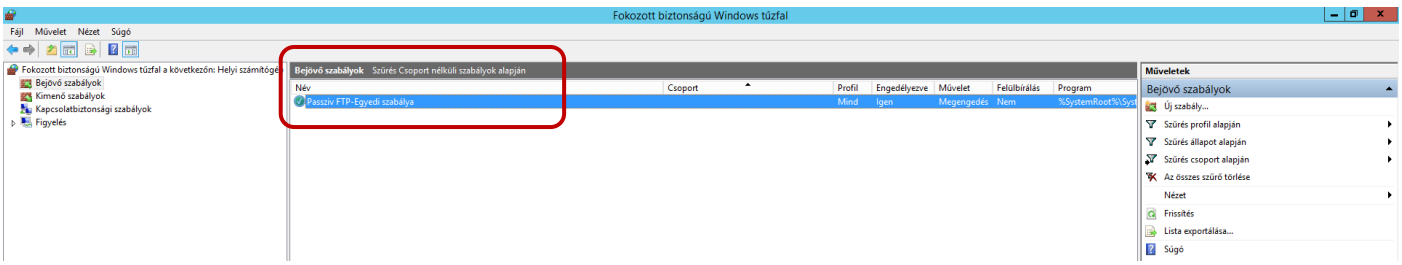
Lehet rendezni (pl. *csoport, portszám, protokoll* szerint):



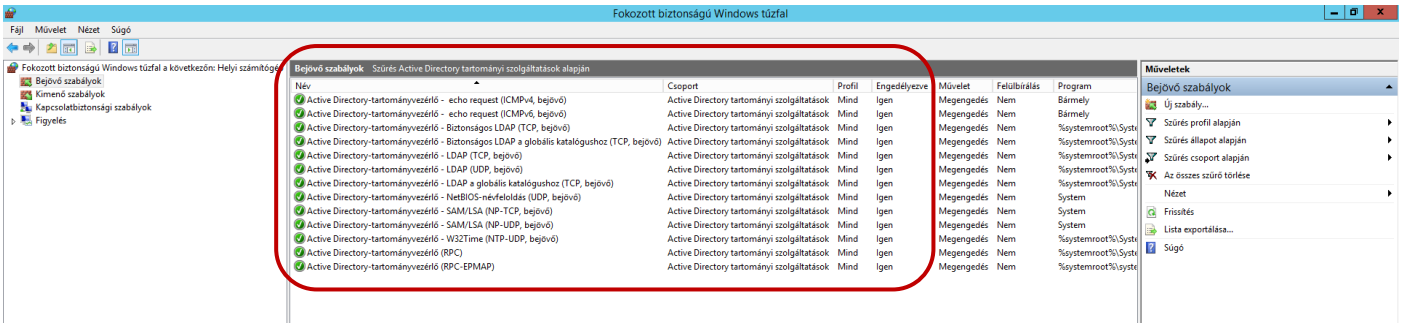

Lehet szűrni (pl. *profil, csoport, portszám, protokoll* szerint):



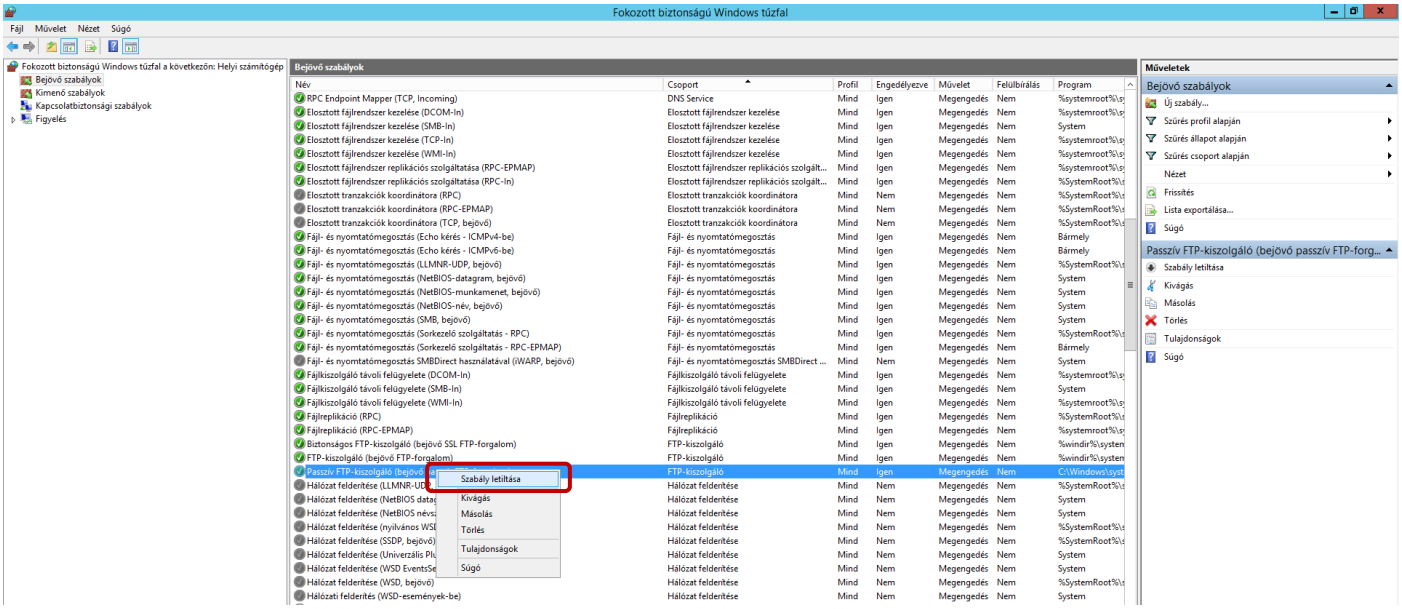

Van lehetőség a ***csoport nélküli*** (pl. általunk létrehozott) szabályok szűrésére is:



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



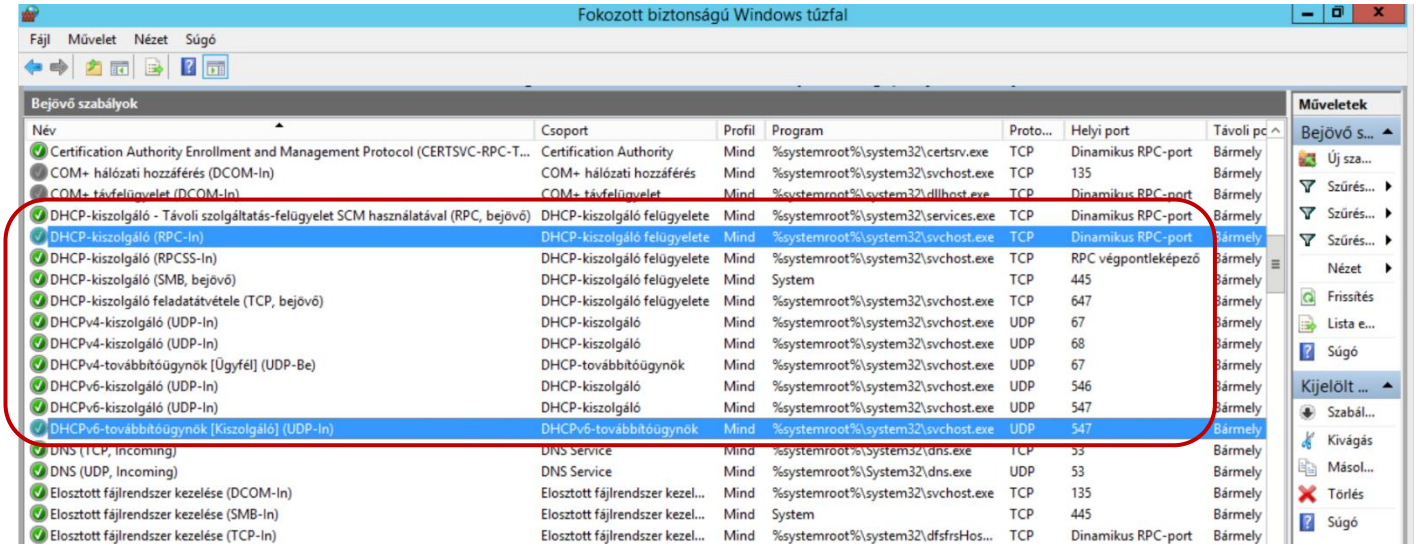

A szabályok Engedélyezhetőek / Tilthatóak




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

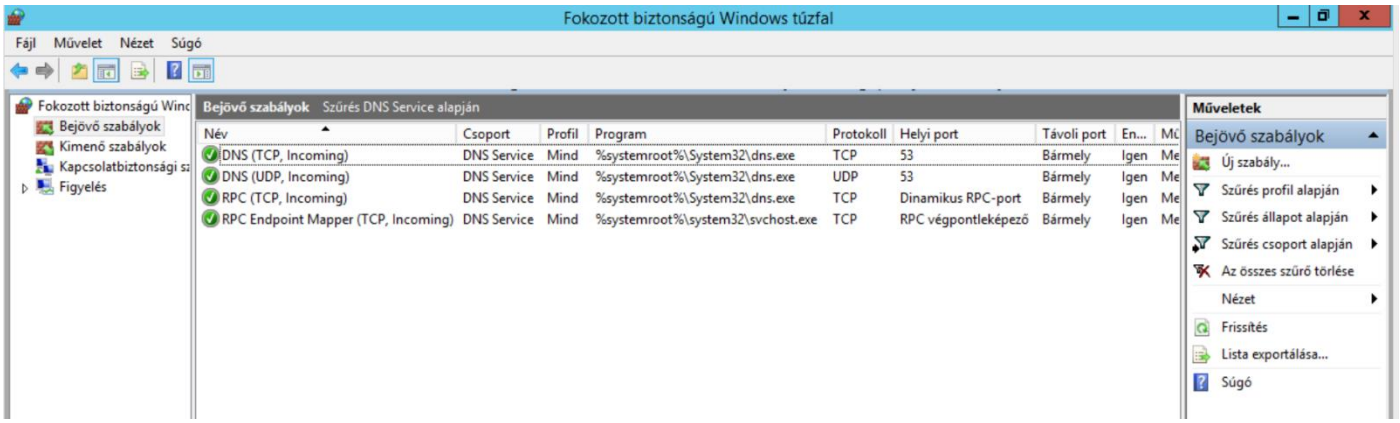
**DHCP**

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



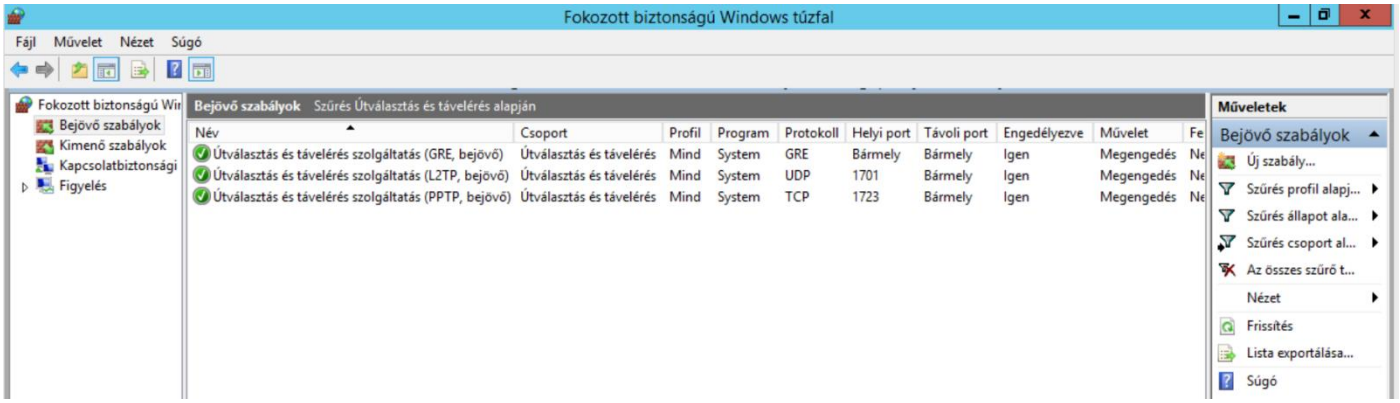
## DNS

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




## Távelérés (VPN)

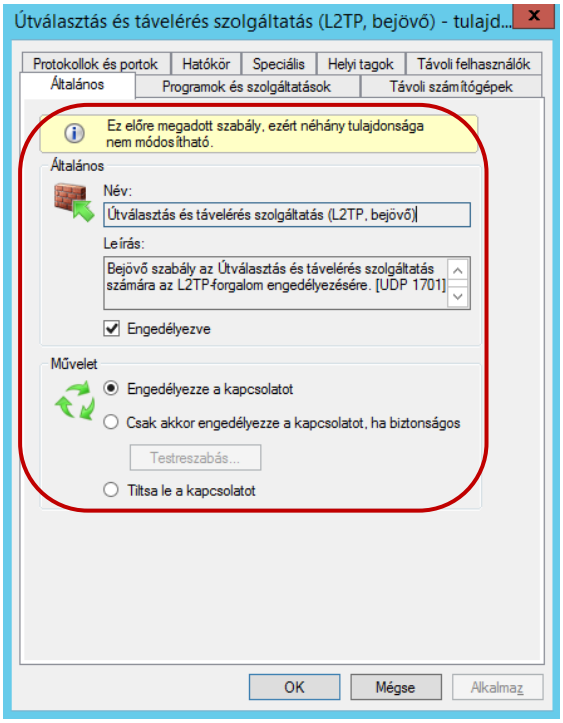
A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat!

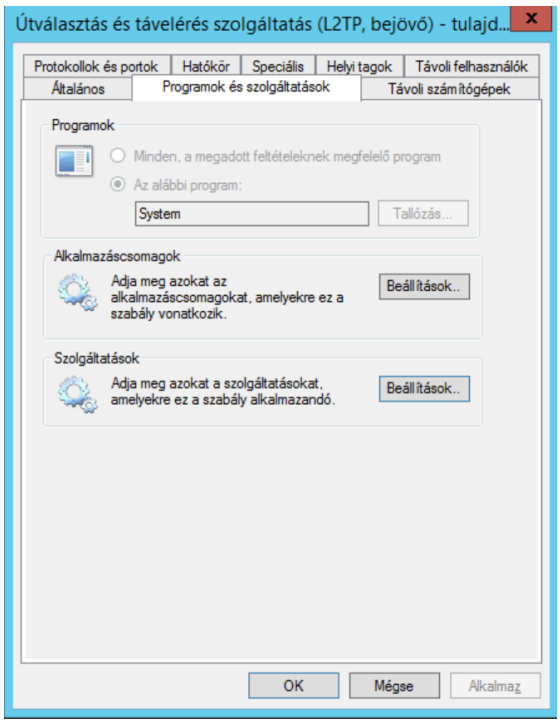



Ha az egyik ide tartozó szabályon duplán kattintva megnézhetjük a tulajdonságait. A képen az ***L2TP*** *protokollhoz* tartozó szabály részleteit látjuk. A rendszer által létrehozott szabályok nem módosíthatóak.

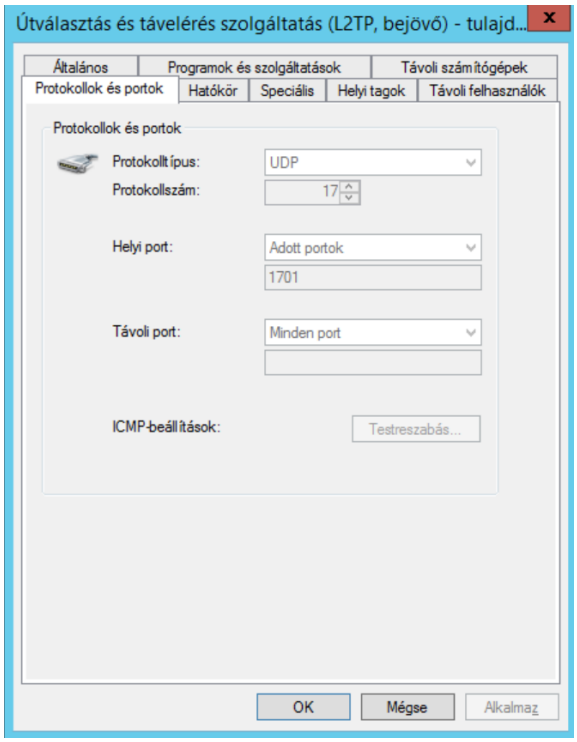
De tudjuk engedélyezni / tiltani a szabályt.

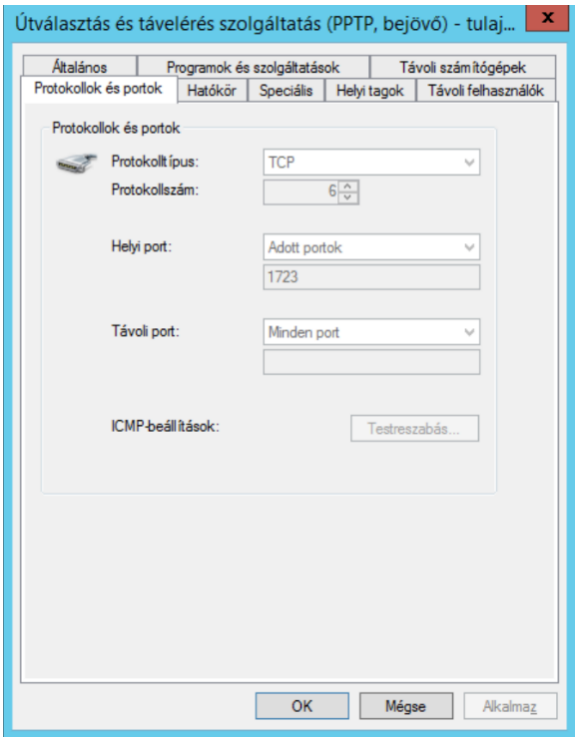
A ***Program***, ami használja csak egyszerűen a ***System.***



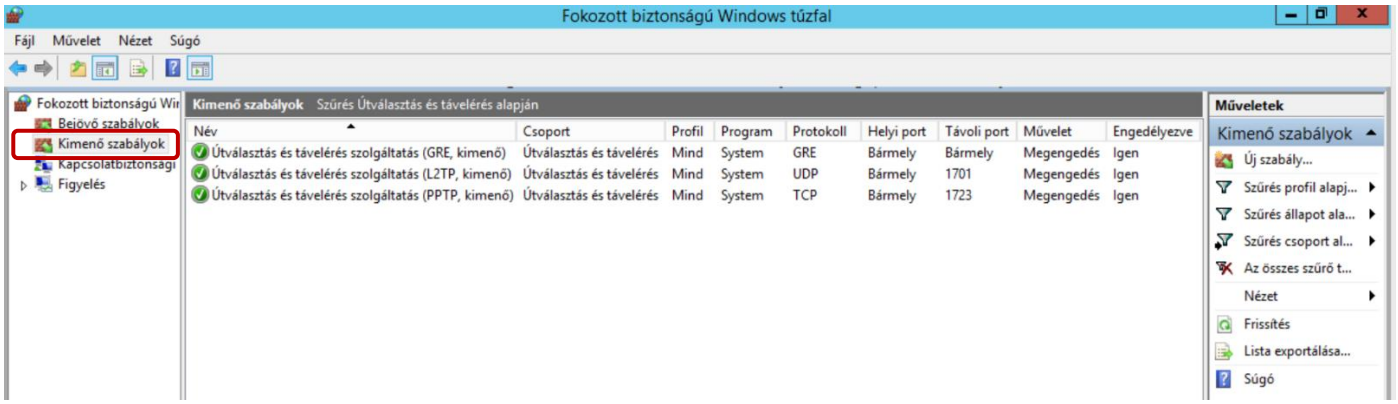



A Távelérés (VPN) a **TCP** protokollt és a **1701,** illetve a **1723-es** portot használja



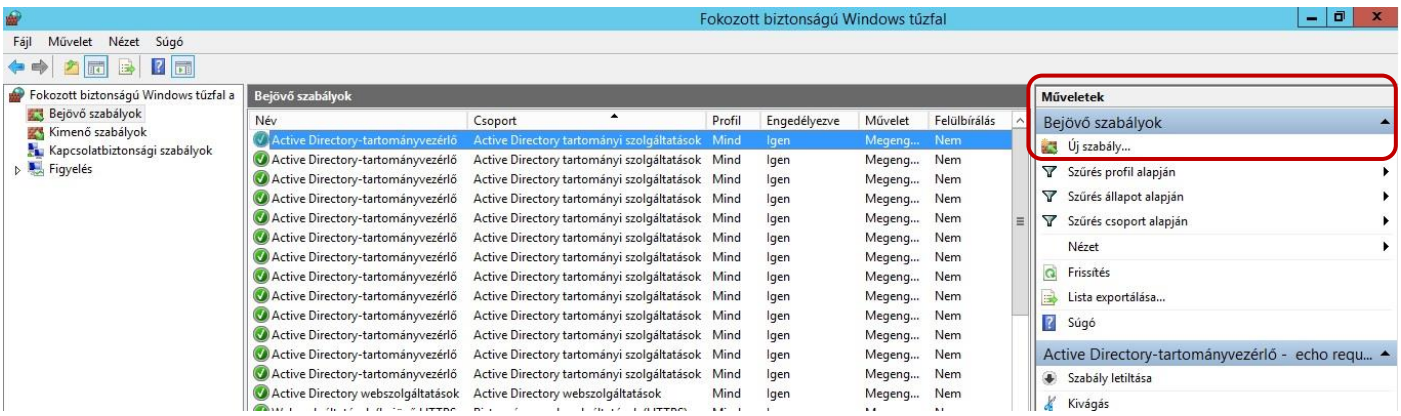




Nézzük meg a **Kimenő szabályok** között is a **Távelérés szabályait.** A szerveren nem igényel beállítást, a rendszer felvette a szükséges szabályokat! (Kifelé irányban nem tiltjuk a forgalmat; de a szabály létezik, ami átengedné!)

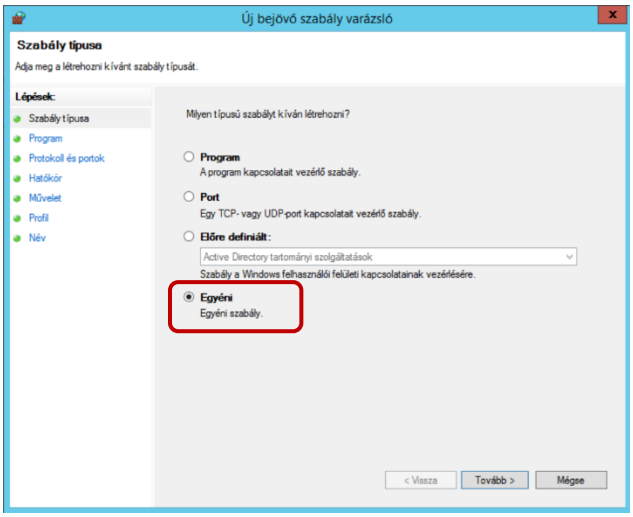



Nézzük meg, hogy tudunk **<u>saját szabályokat</u>** létrehozni. A legegyszerűbb ilyen szabály talán a **PING** parancs forgalmának engedélyezése.

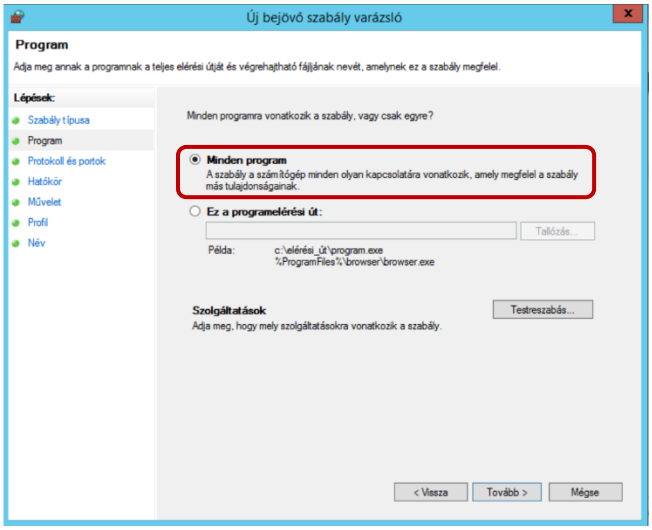
Bejövő szabályt hozunk hozzá létre:



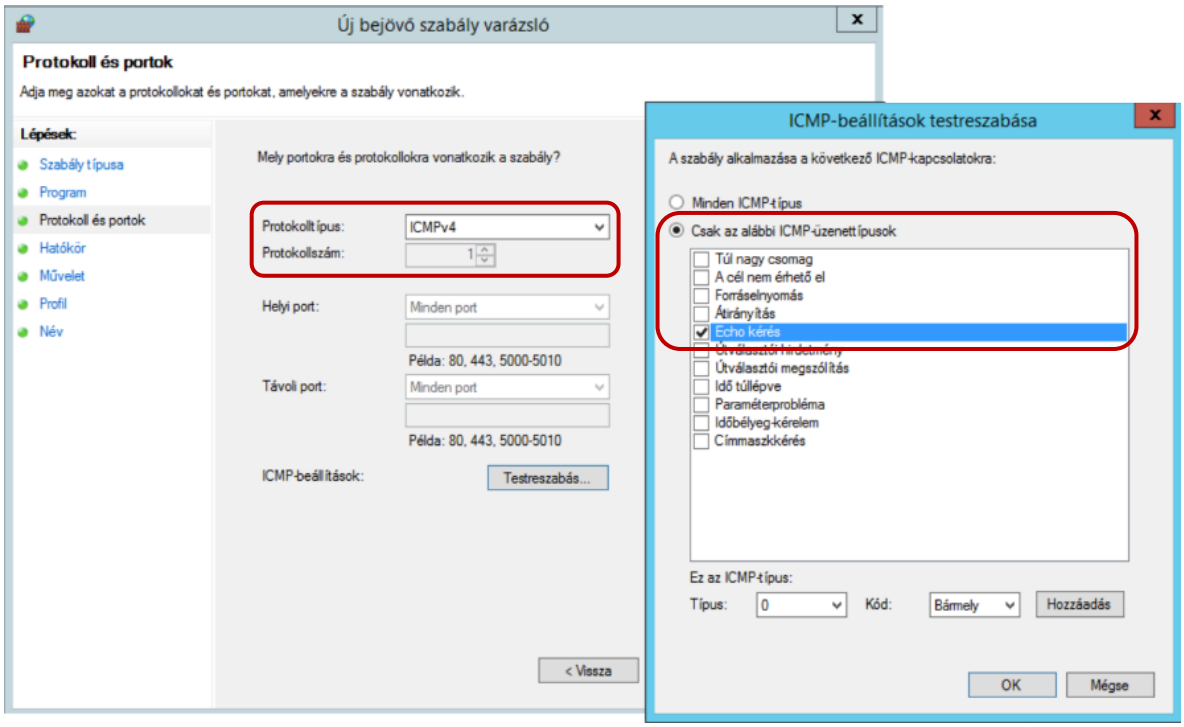
Egyéni szabályt hozunk létre:



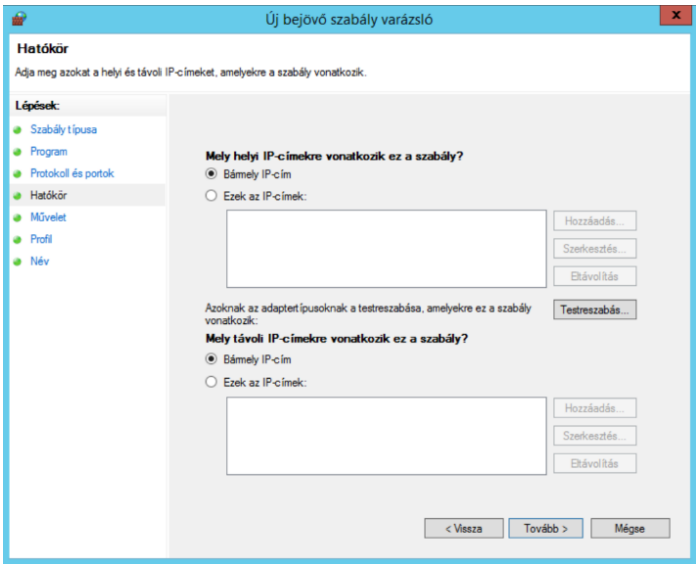

Minden programnak engedélyezzük:



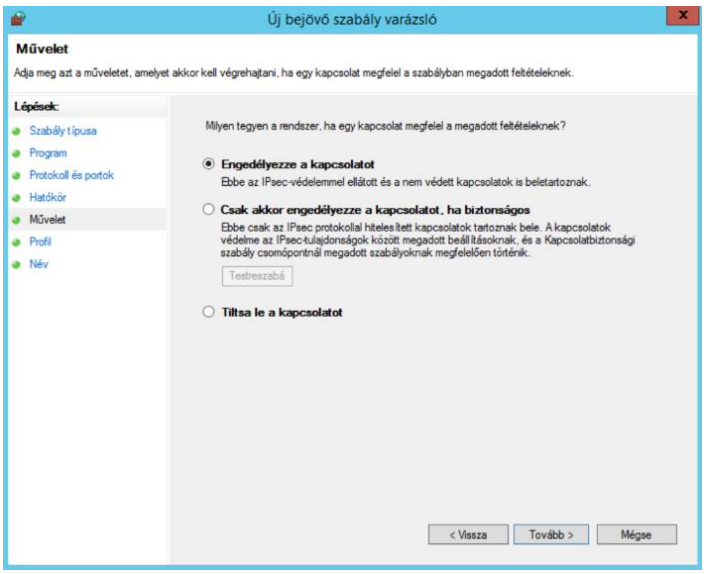

Beállítjuk a protokolltípust, ***PING*** esetén ez ***ICMPv4*** és a ***Testreszabás*** gombra kattintva kijelöljük az ***Echo kérést***:



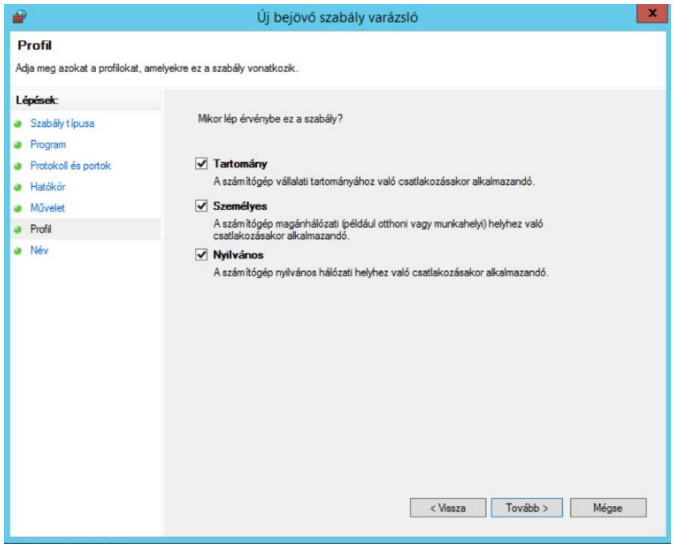
Nem korlátozzuk, hogy milyen IP-címről érhetik el a szervert PING kérések:

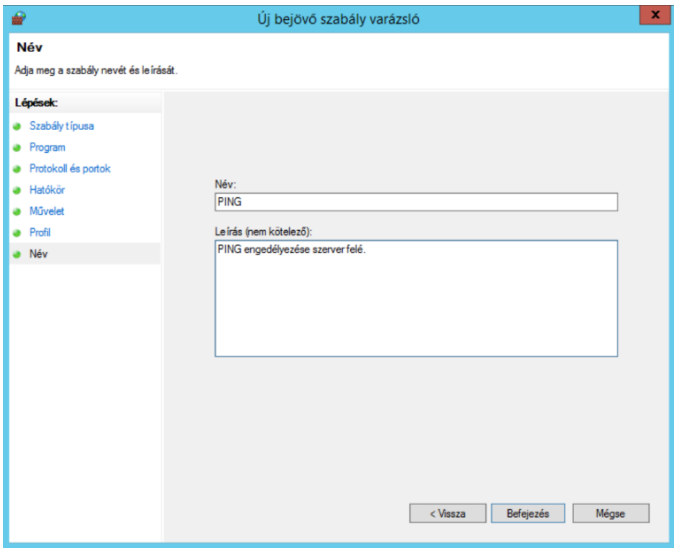



Engedélyező szabályt hozunk létre:



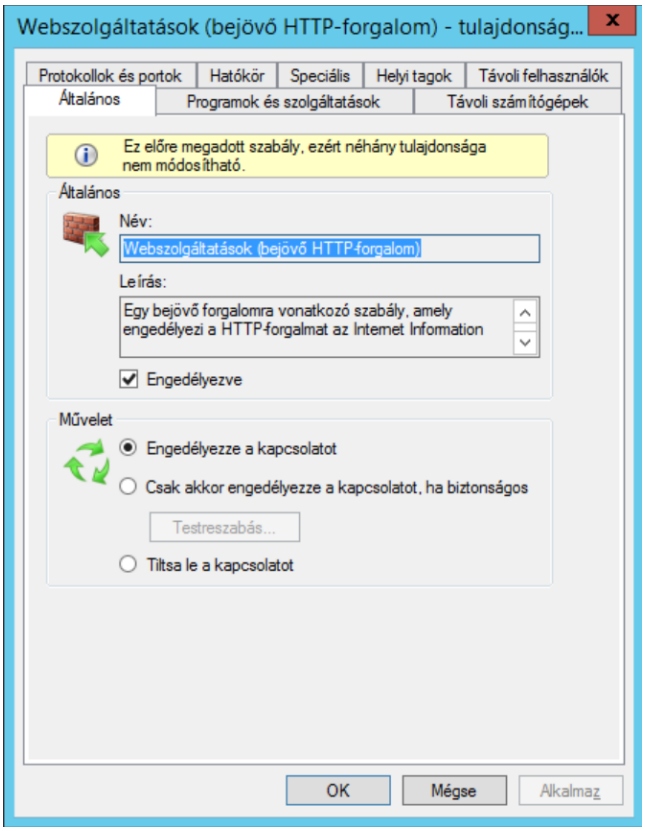

Minden profilra érvényesítjük a szabály beállításait és végül nevezzük el a szabályt:

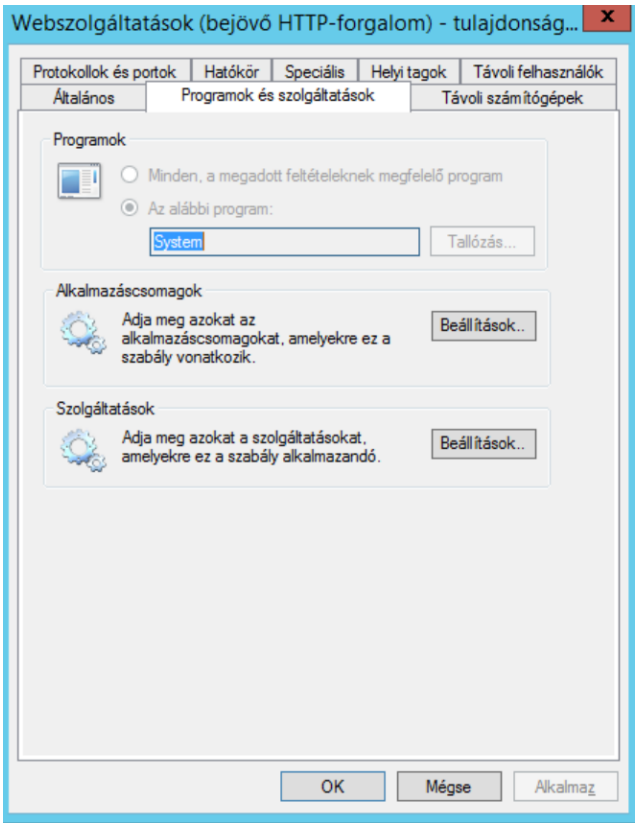


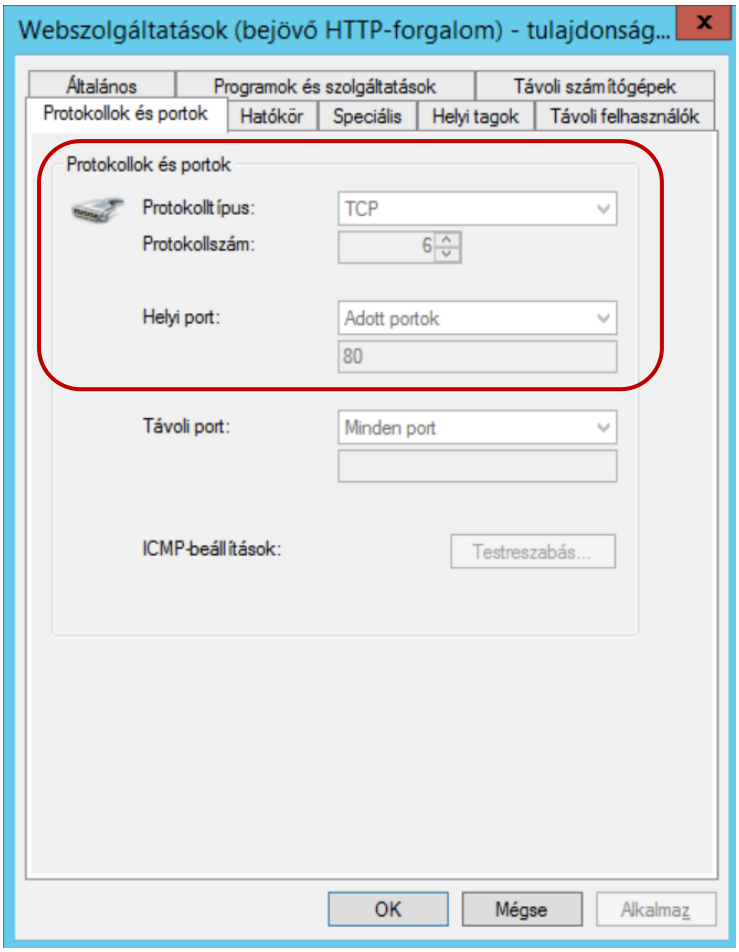
**WEB kiszolgáló:**

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

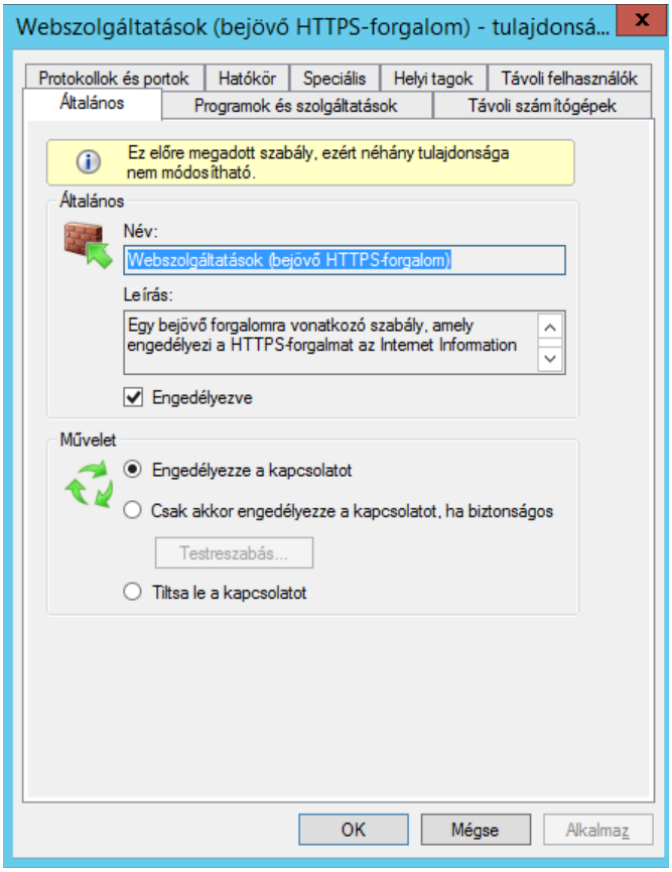


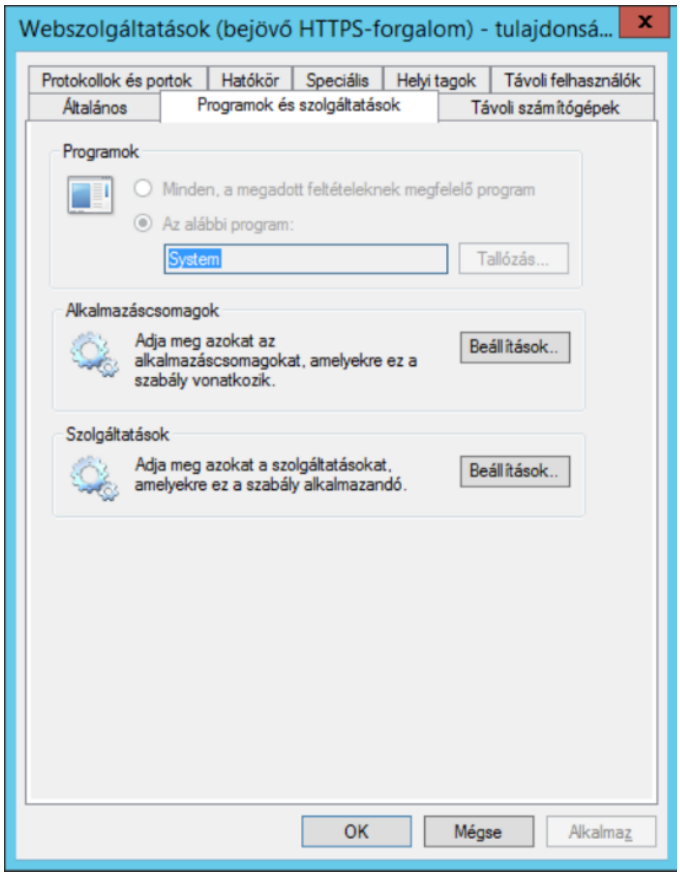



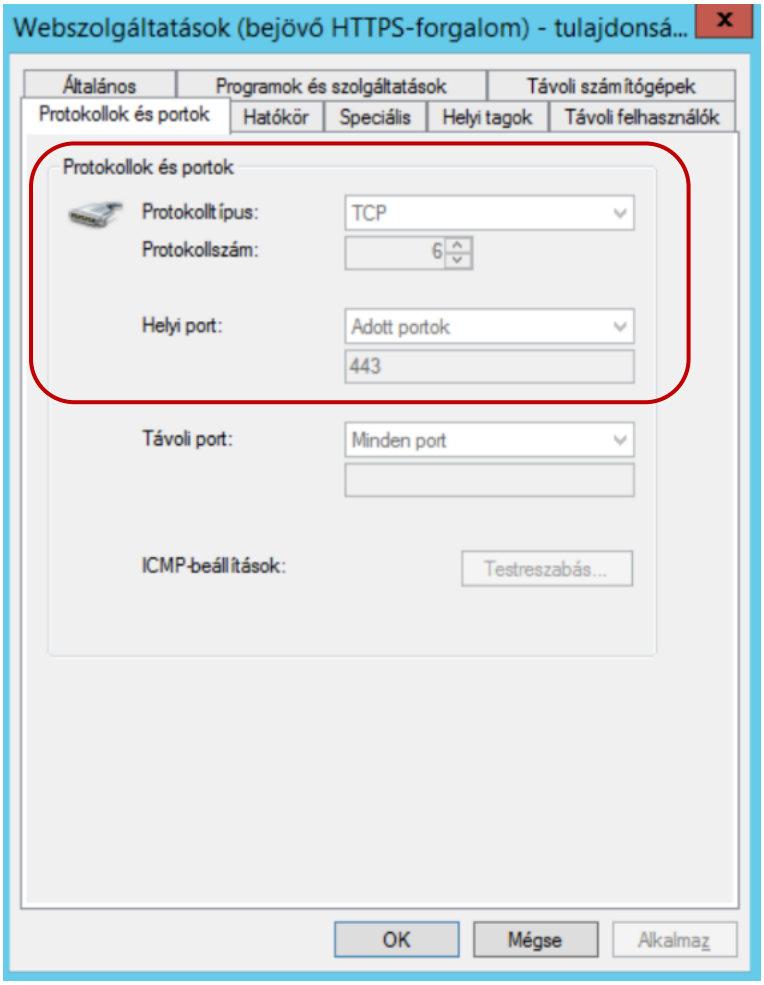

Alapértelmezett ***80***-as porton keresztül, ***TCP*** protokoll:



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

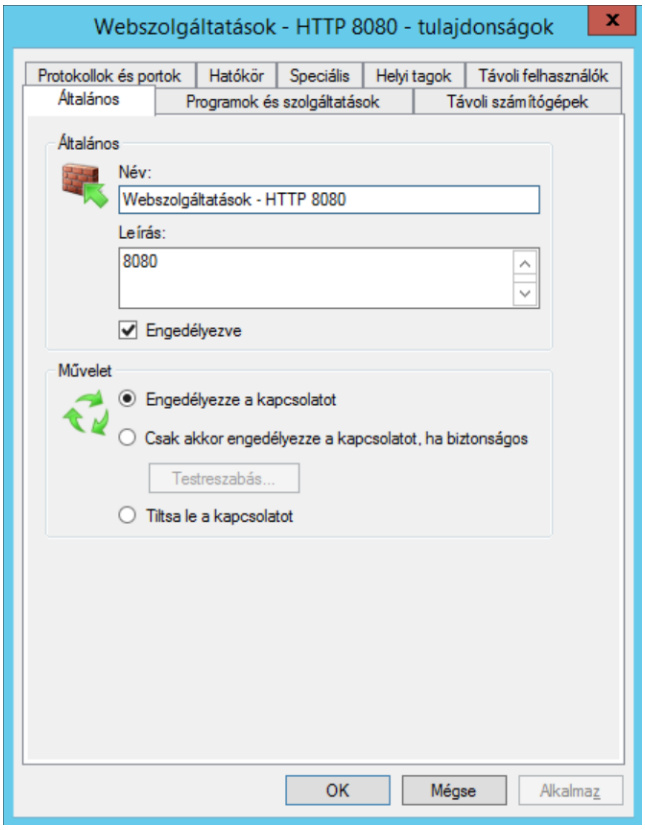


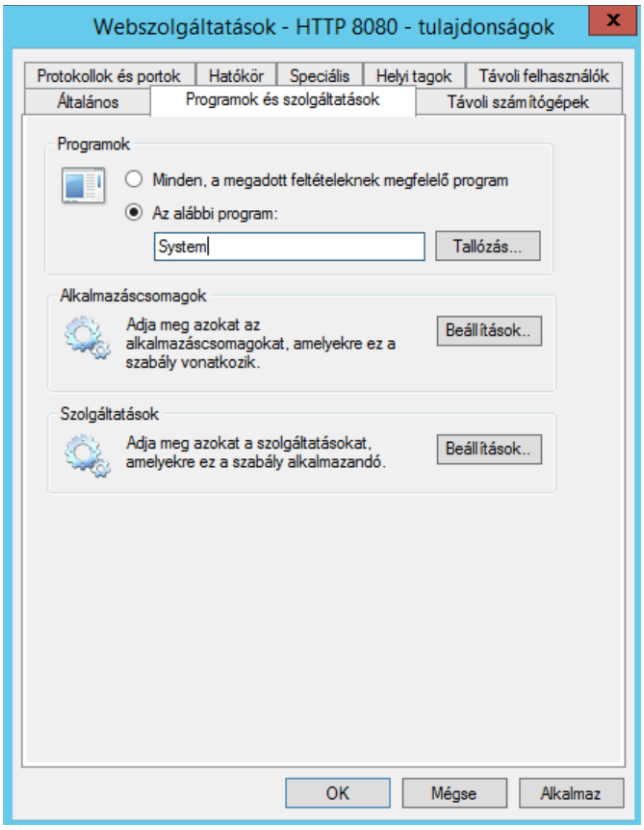



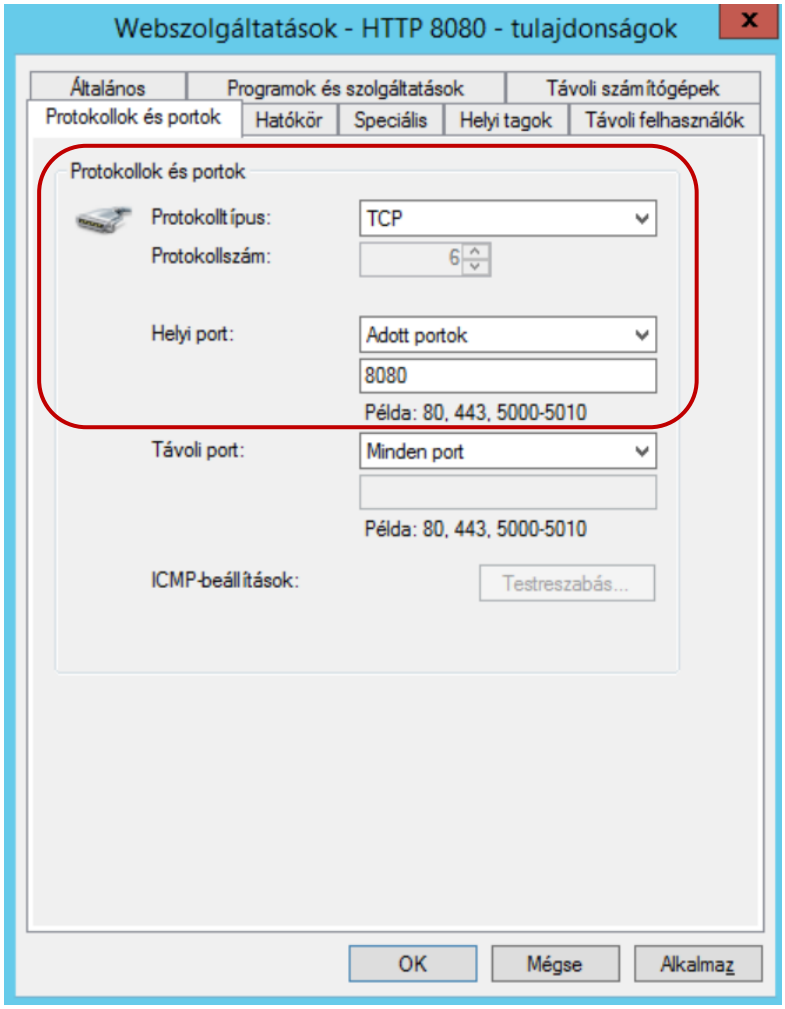



Amennyiben egyedi portokat használnánk, akkor készítsünk (az előző szabályok alapján) egyedi szabályokat:

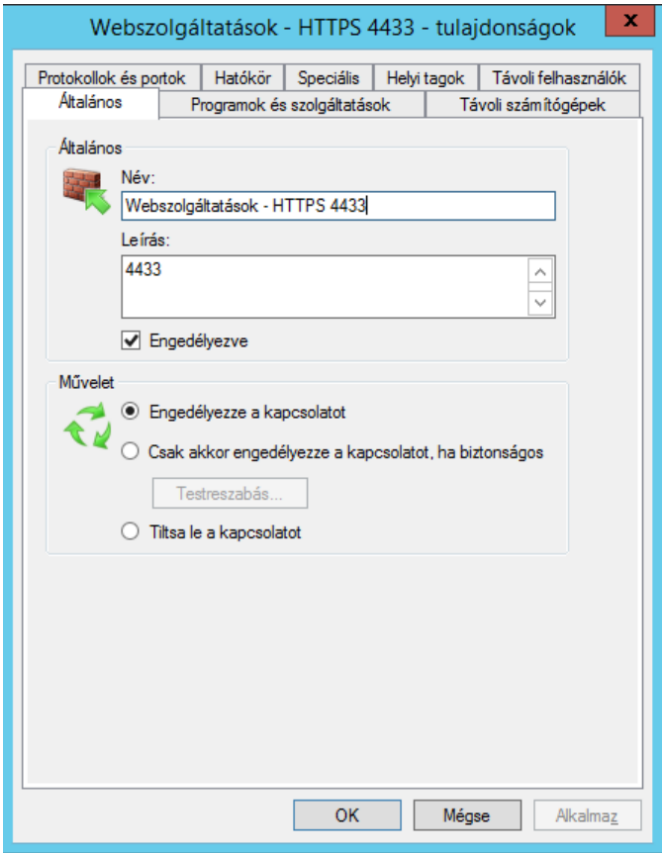
**Nem biztonságos webes kapcsolathoz** (***http*** protokoll, egyedi ***8080***-as porton keresztül)

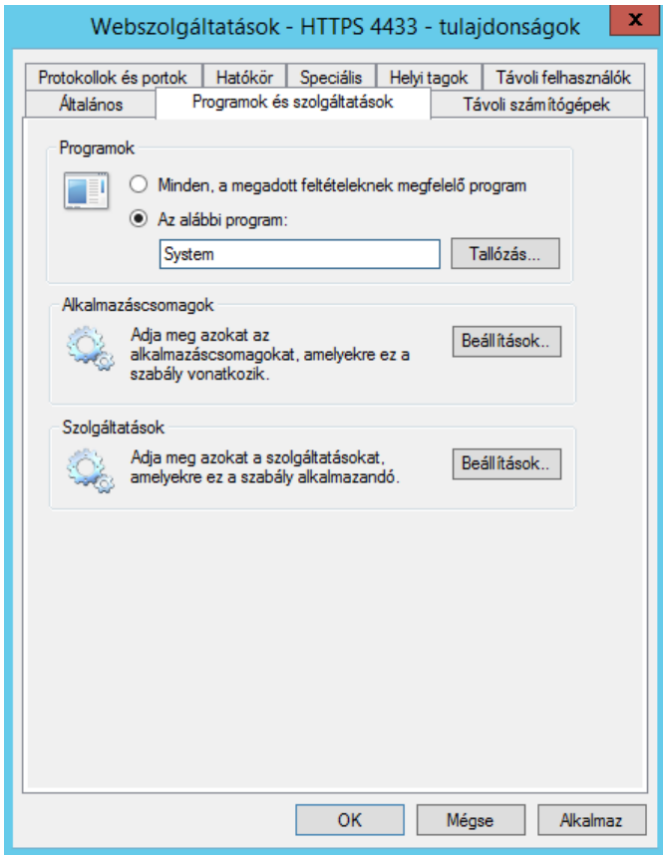


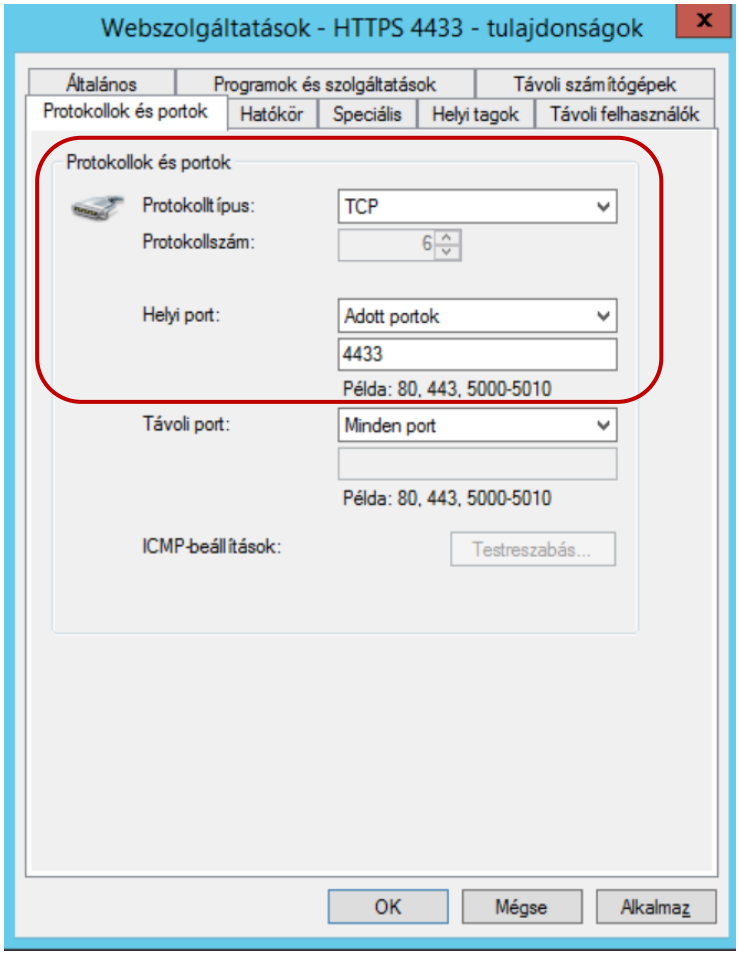



**Biztonságos webes kapcsolathoz** (***https*** protokollal, ***4433***-as porton keresztül)



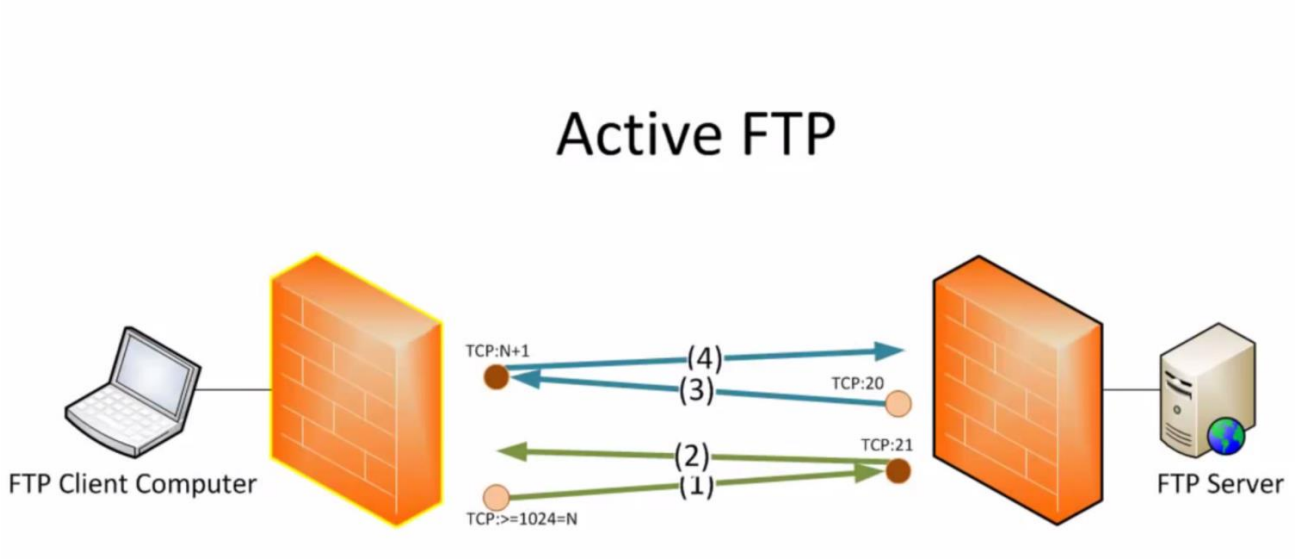
**FTP kiszolgáló**

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.




Mindezek megvalósítása részletezve:

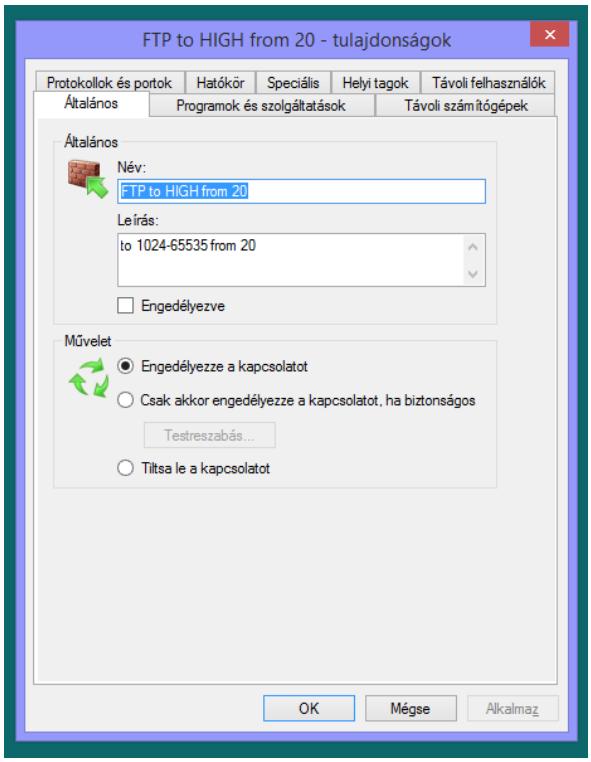
**Szerveren:**

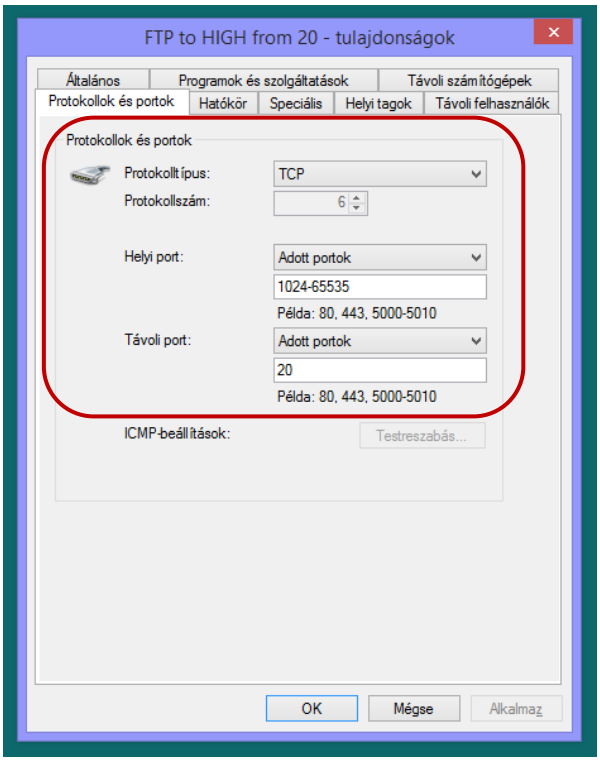
Bejövő szabály: nem igényel beállítást, a rendszer felvette a szükséges szabályt!

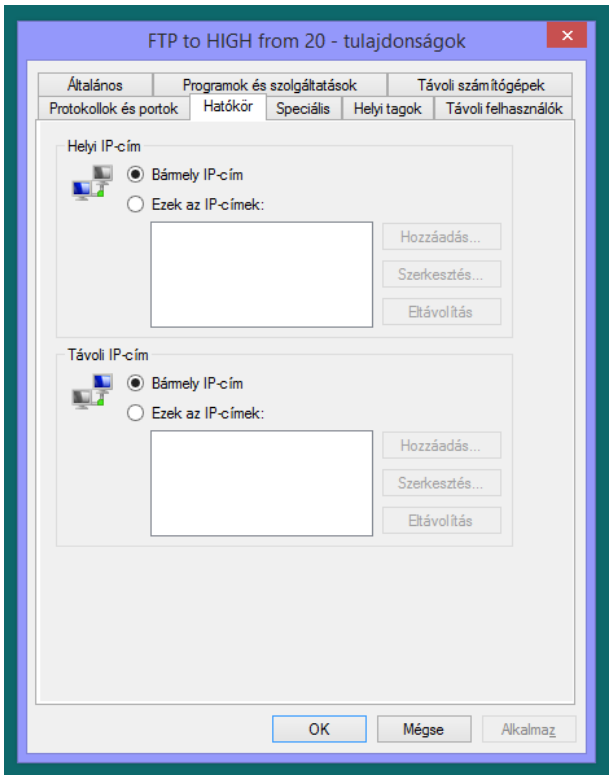
Kimenő szabály: nem igényel beállítást, a rendszer felvette a szükséges szabályt!

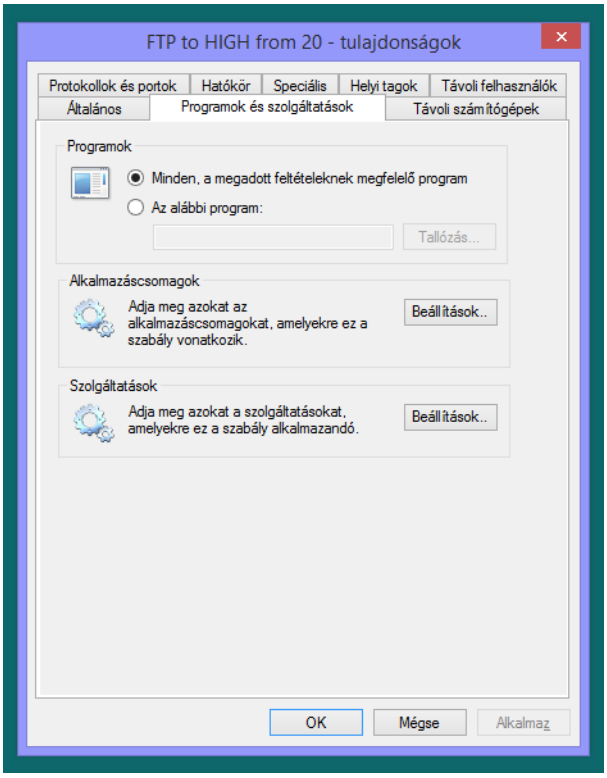
**Kliensen:**

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

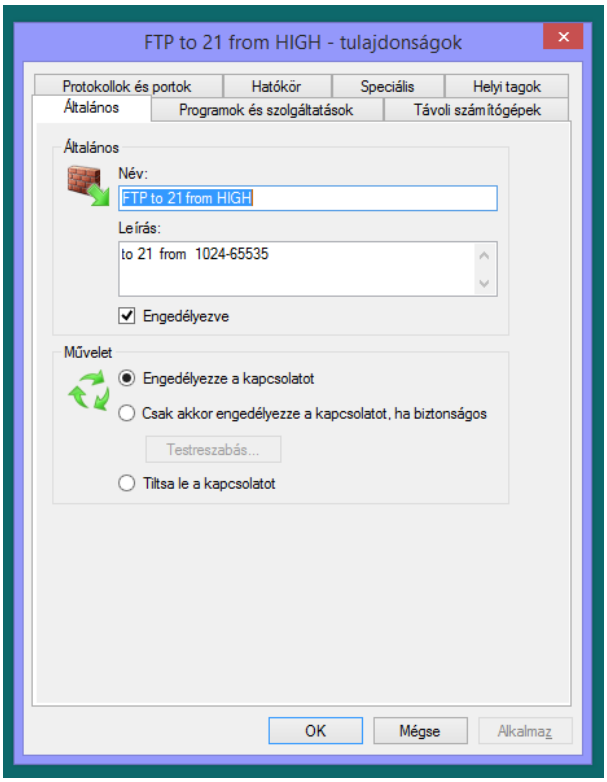


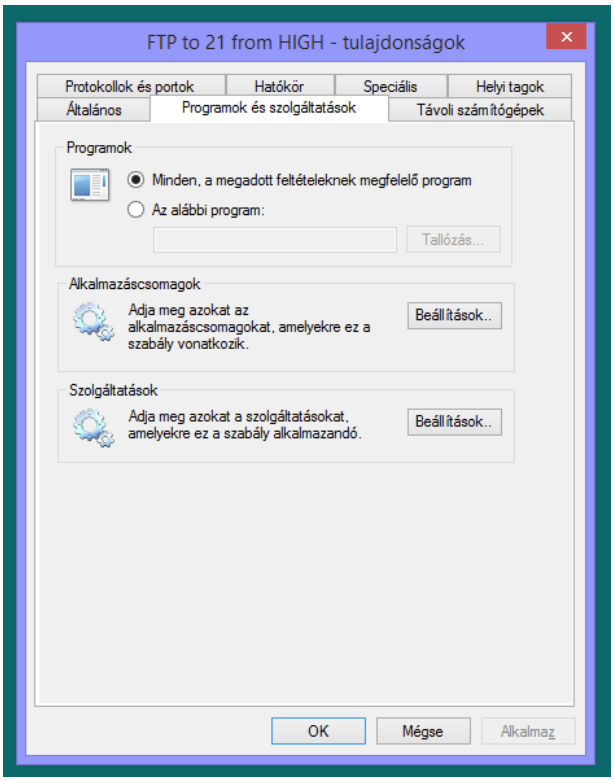



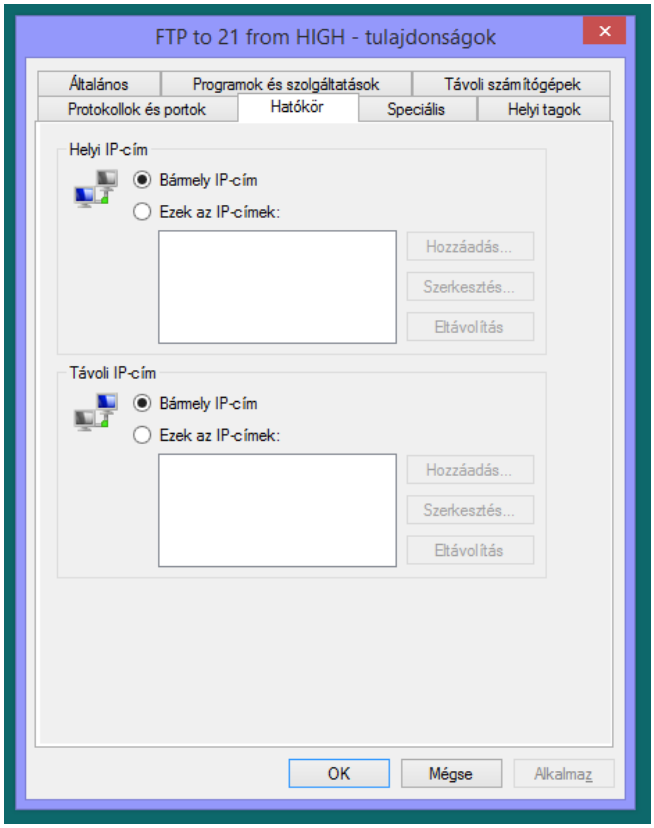


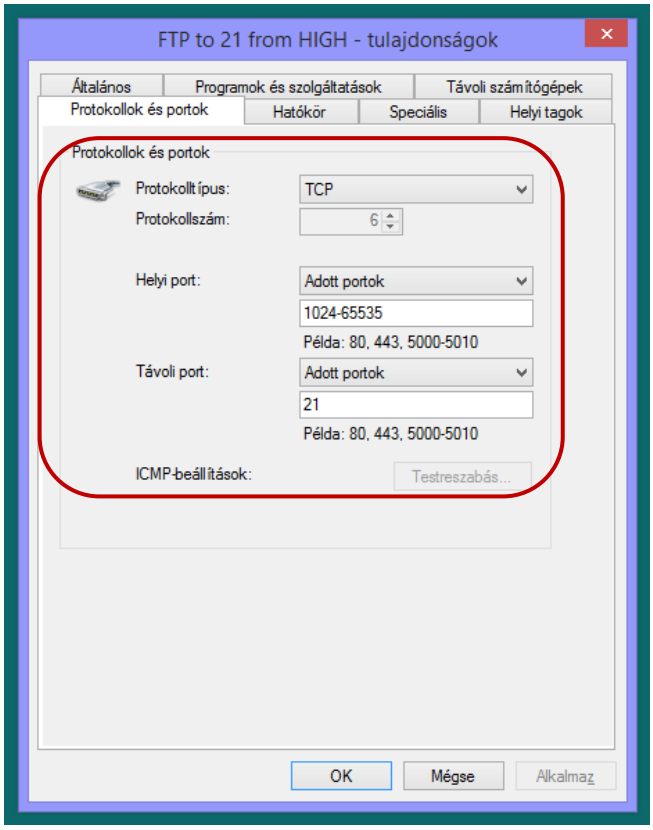




Kimenő szabály:



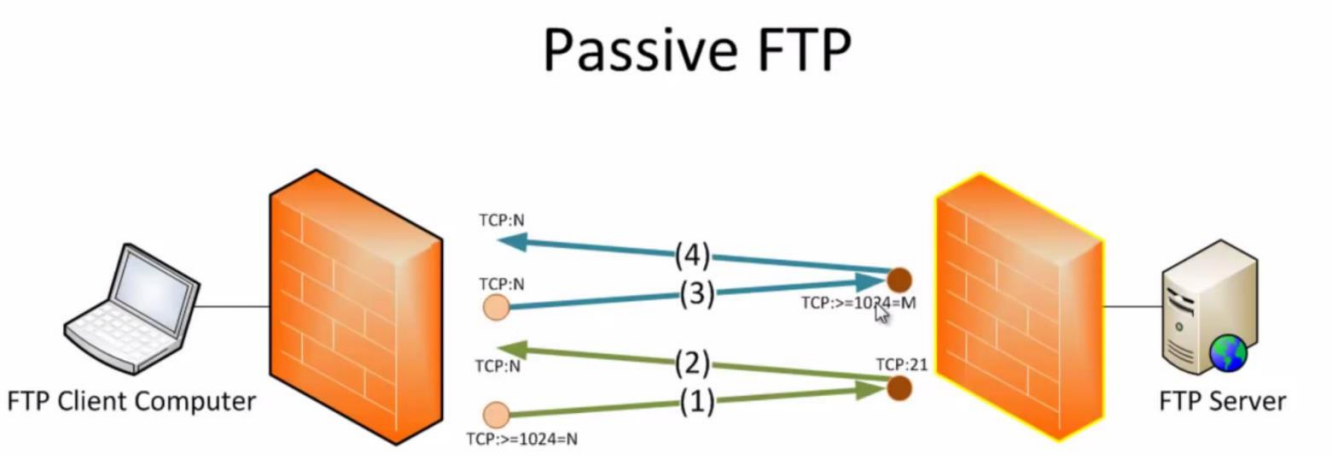



**Passzív FTP**

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!)*




Mindezek megvalósítása részletezve:

**Szerveren:**

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

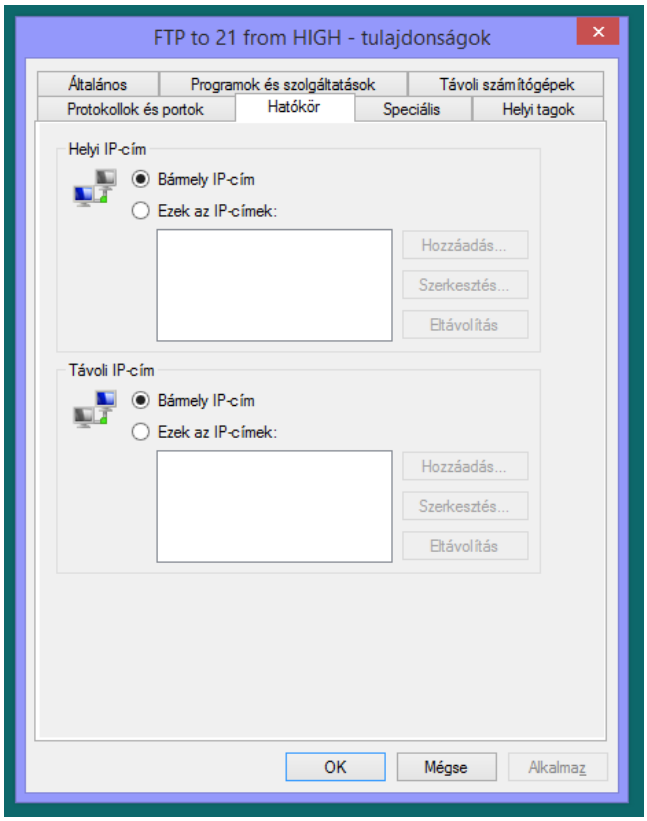
Kimenő szabály: nem igényel szabályt!

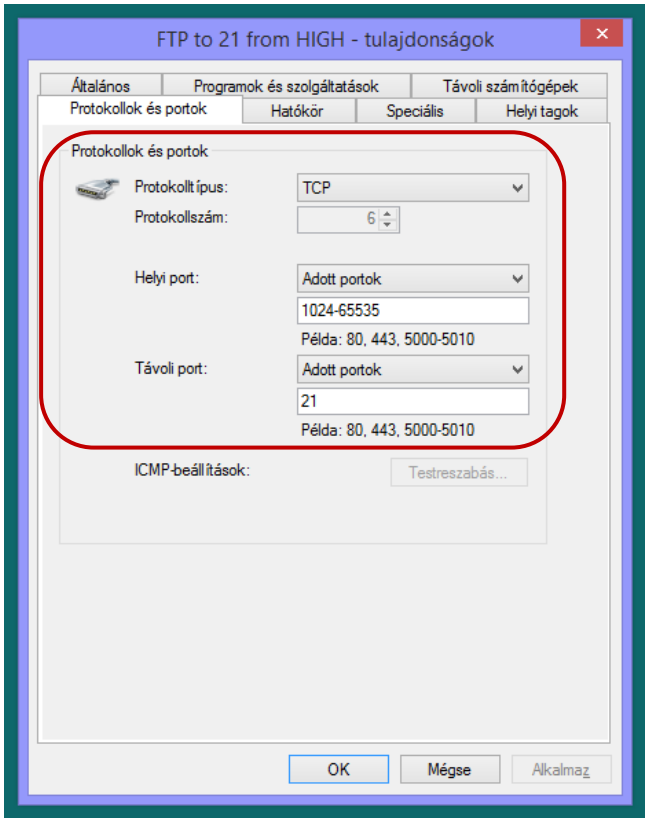
**Kliensen:**

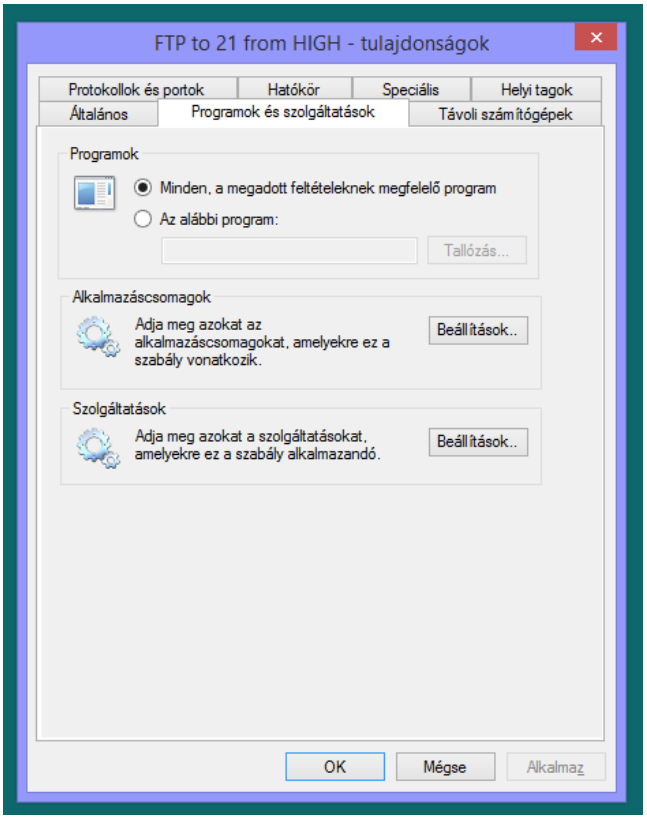
Bejövő szabály: nem igényel szabályt!

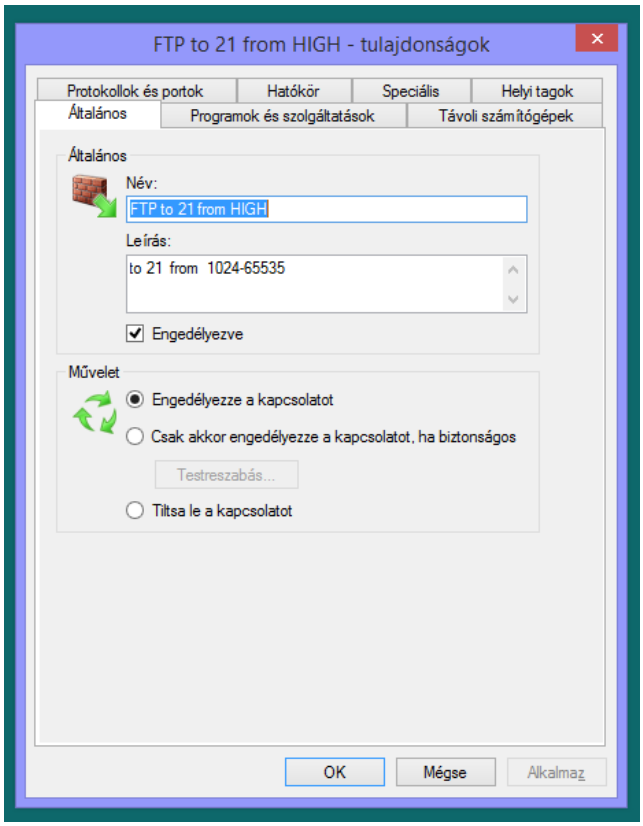
Kimenő szabály: *két szabályt kell létrehoznunk!*

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

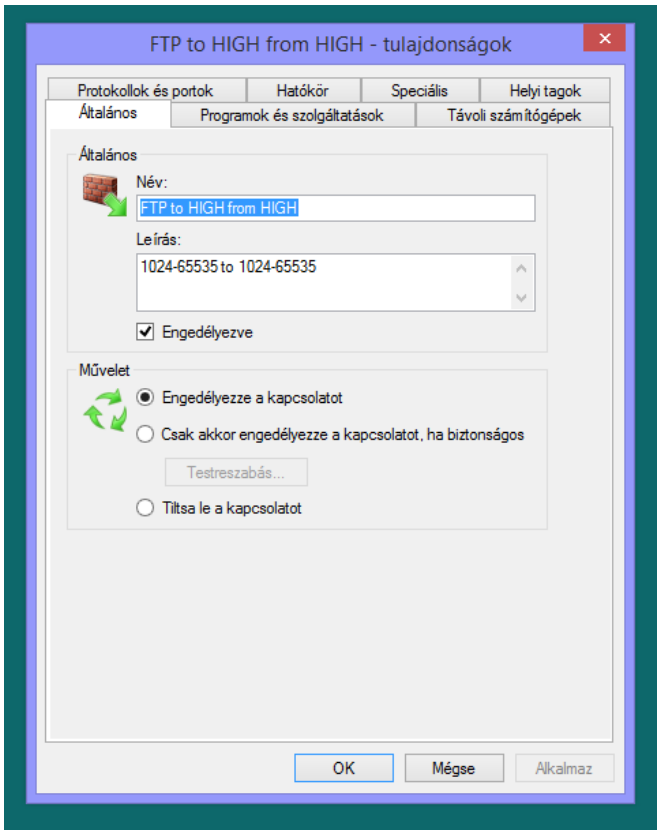


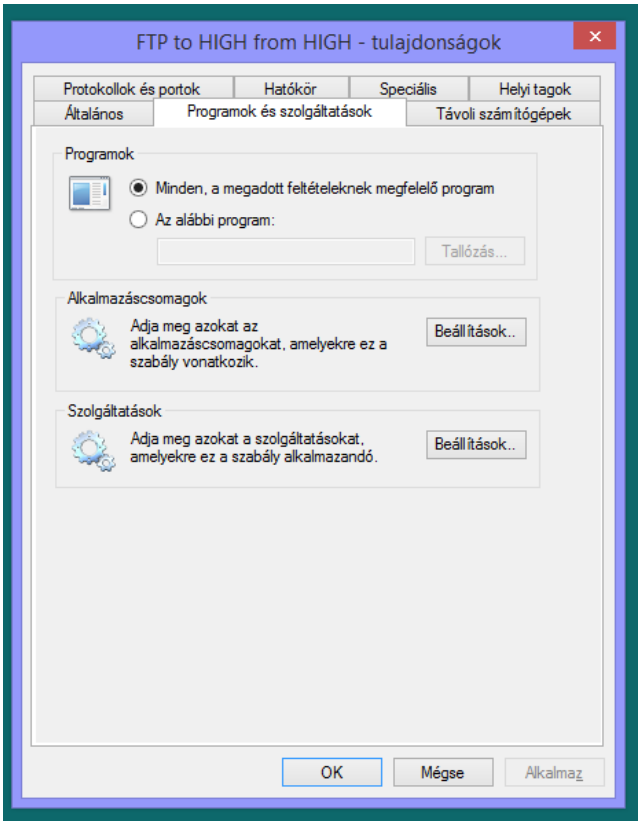



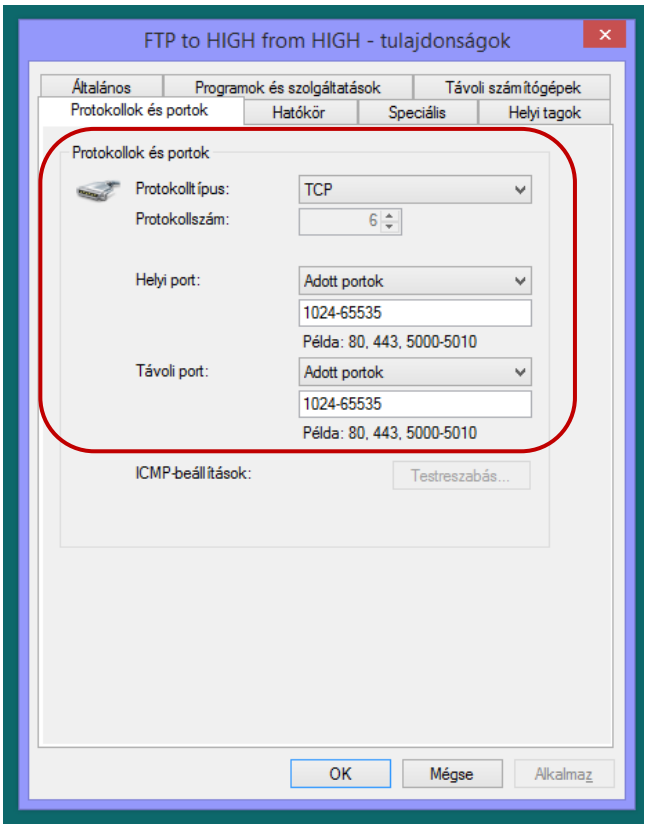



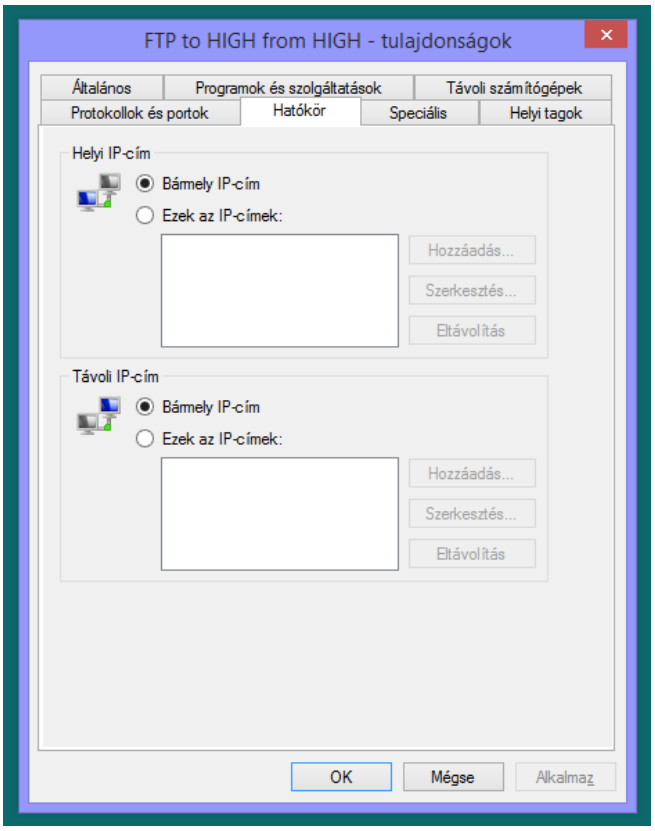



2. A második szabály ***a kliens magas*** (*port > 1024*) portjairól engedélyezi a kapcsolatot ***a szerver magas portjaihoz***:



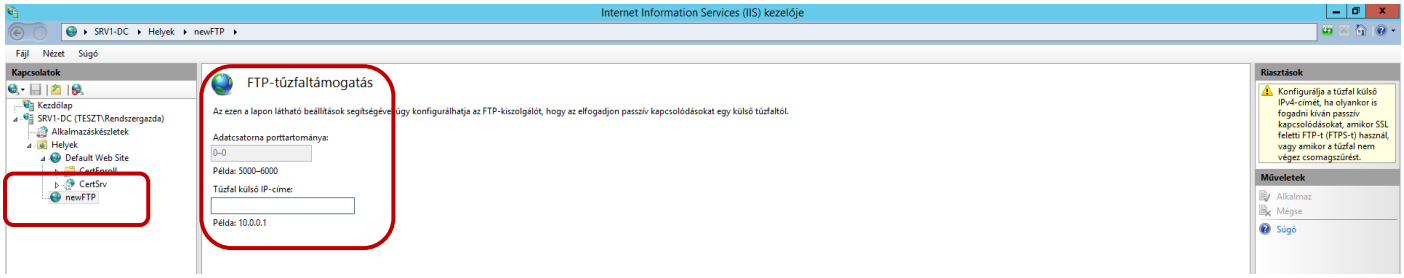



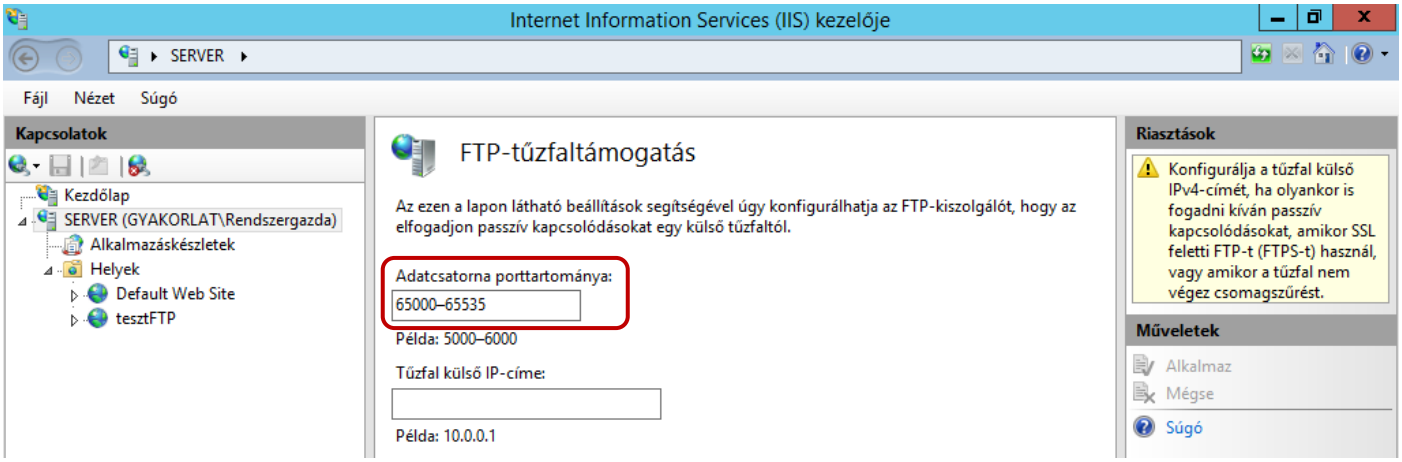



Ez az általánosabban elterjedt megoldás. Viszont a kiszolgálón sok nyitott portot jelent, erre megoldás lehet az ***FTP kiszolgáló egyedi porttartománnyal***:

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



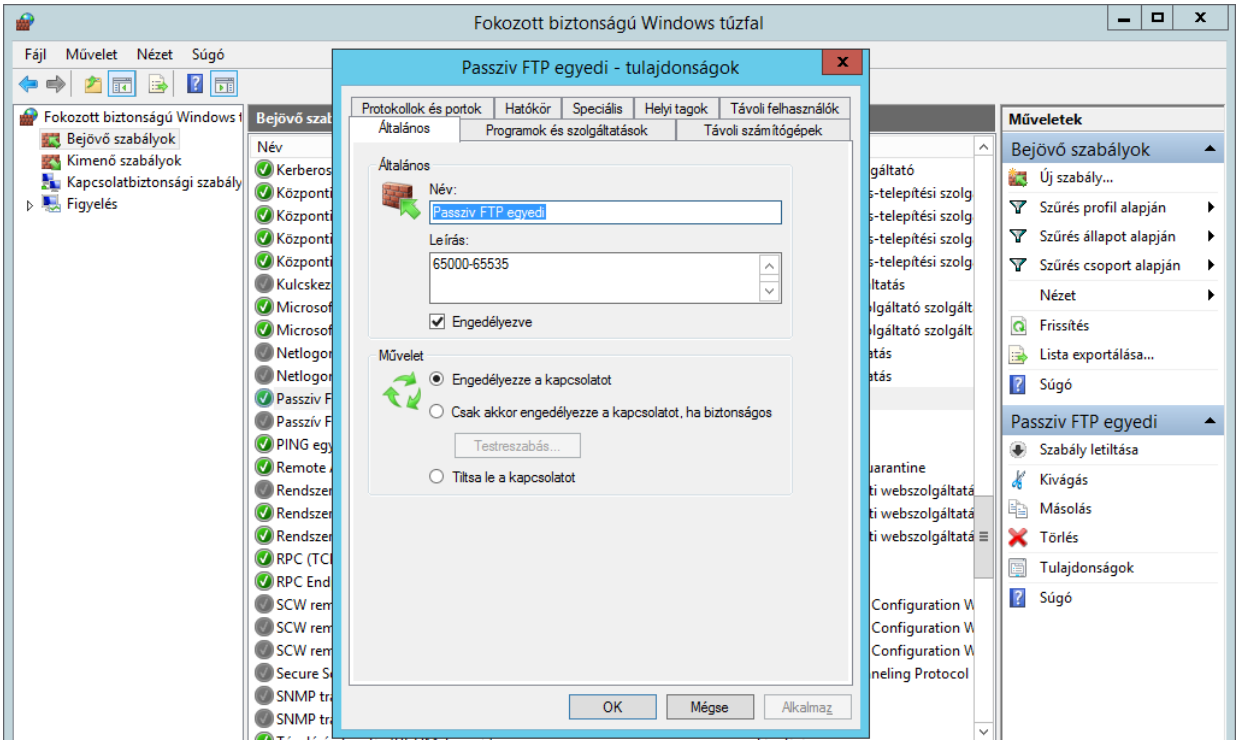

<u>Ez szerver szintű beállítás:</u> (a képen a kiosztott portok: 65000-65535):




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

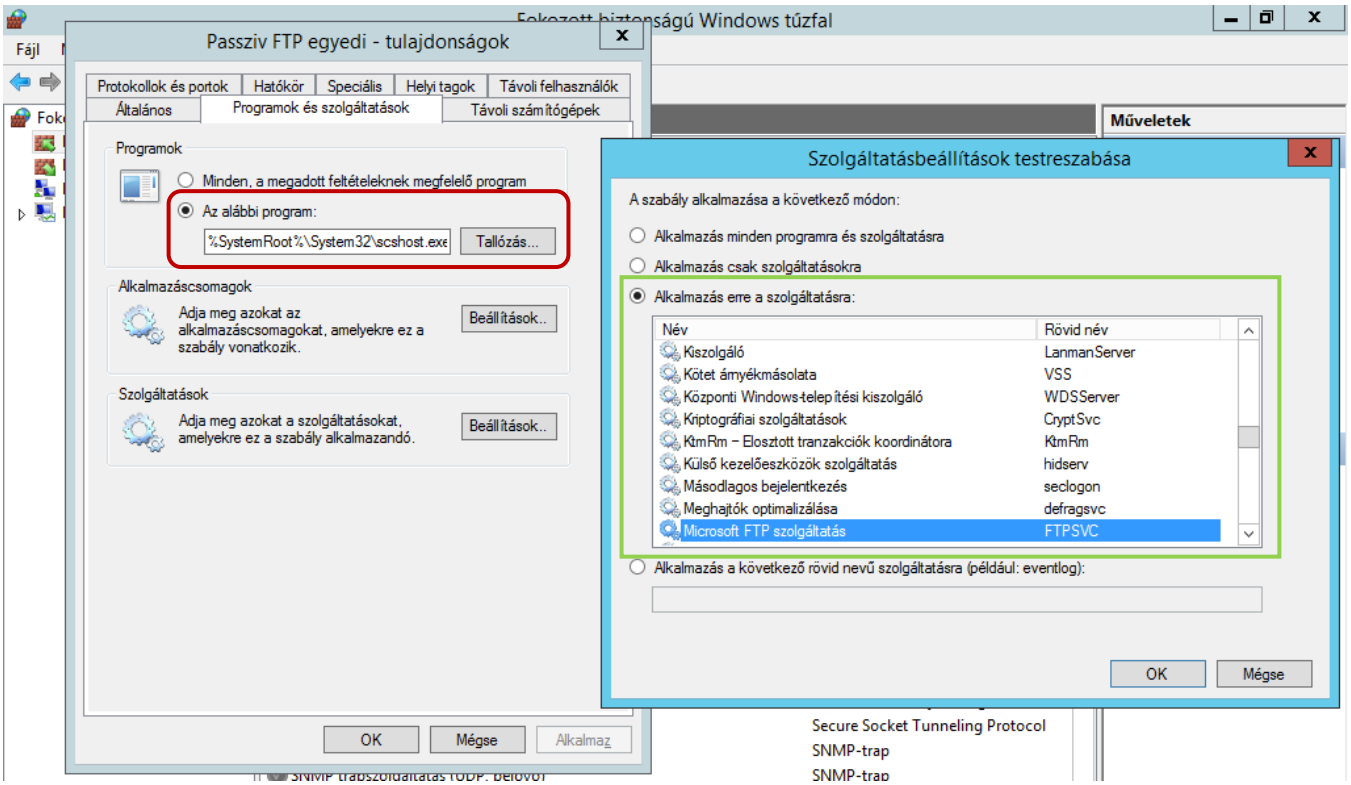
A tűzfalon a rendszer által (az *alapértelmezett Passzív FTP kapcsolathoz*) létrehozott szabályt keressük meg és ***<u>TILTSUK LE!</u>***

Hozzunk létre egy új szabályt az alábbi beállításokkal:

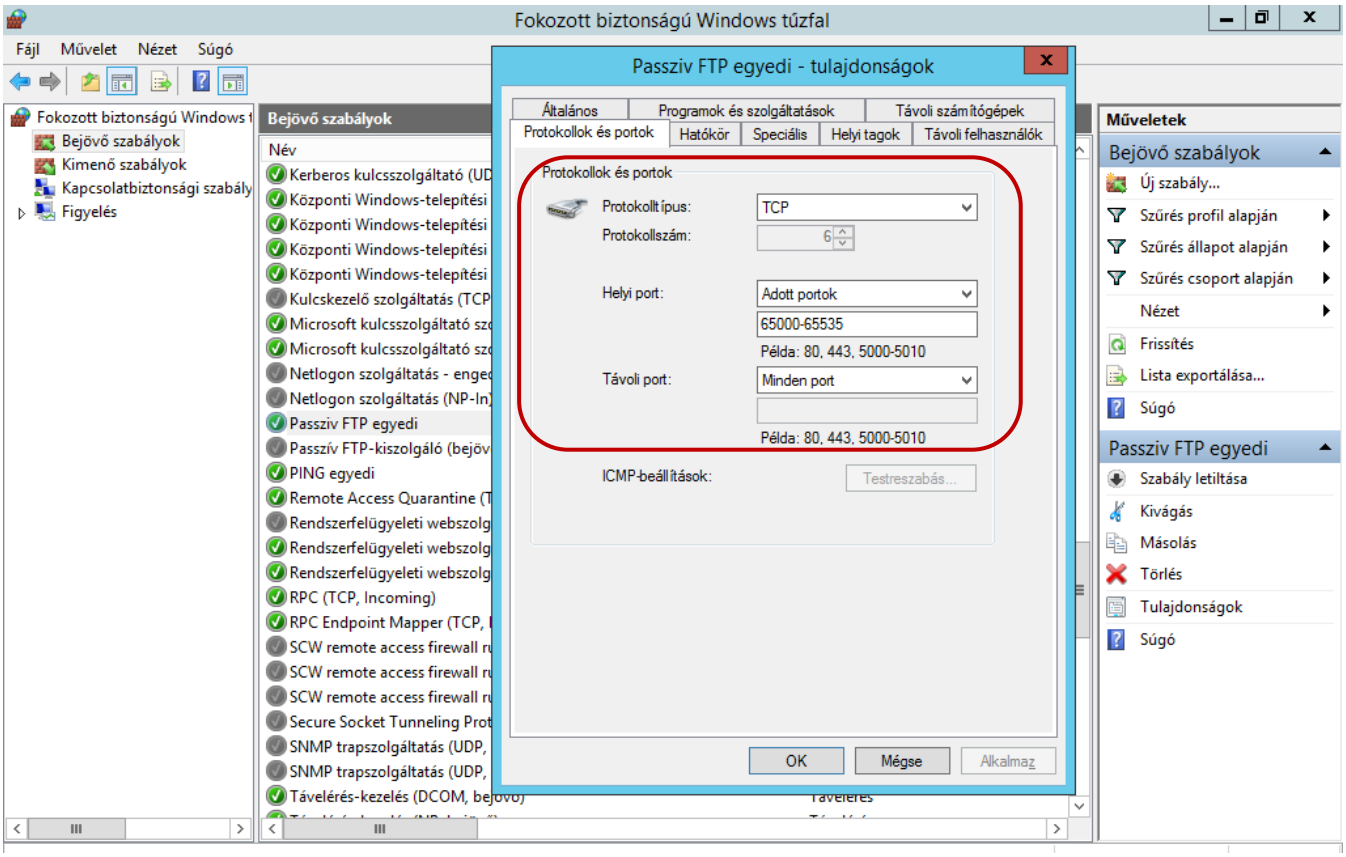


Nem minden programnak nyitjuk meg a porttartományt, csak *(a képen látható módon)* az FTP szolgáltatásnak!

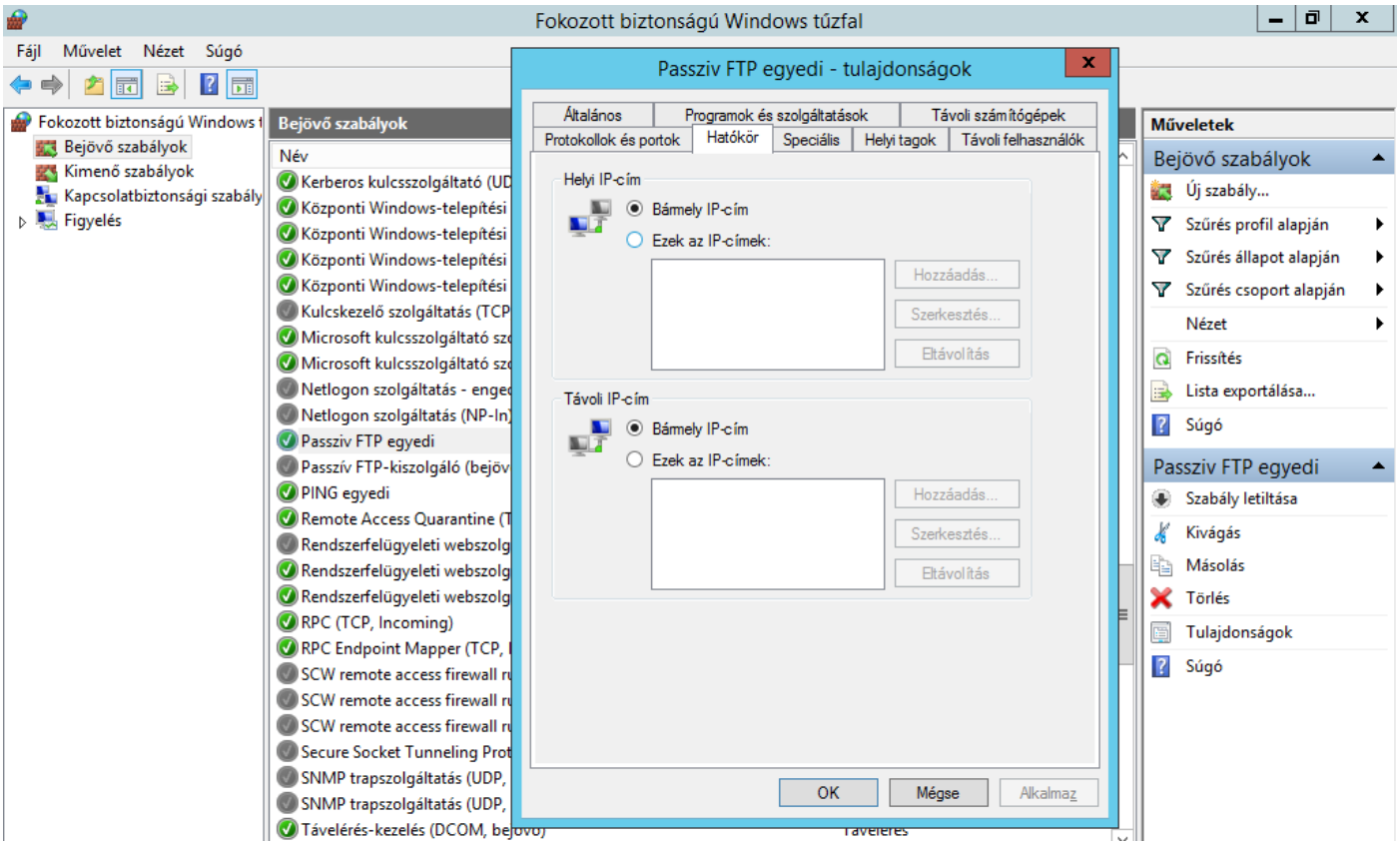
*(Az **scshost.exe**, mint szolgáltatáskezelő részére és azon belül a **Microsoft FTP szolgáltatás** FTPSVC)*




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: