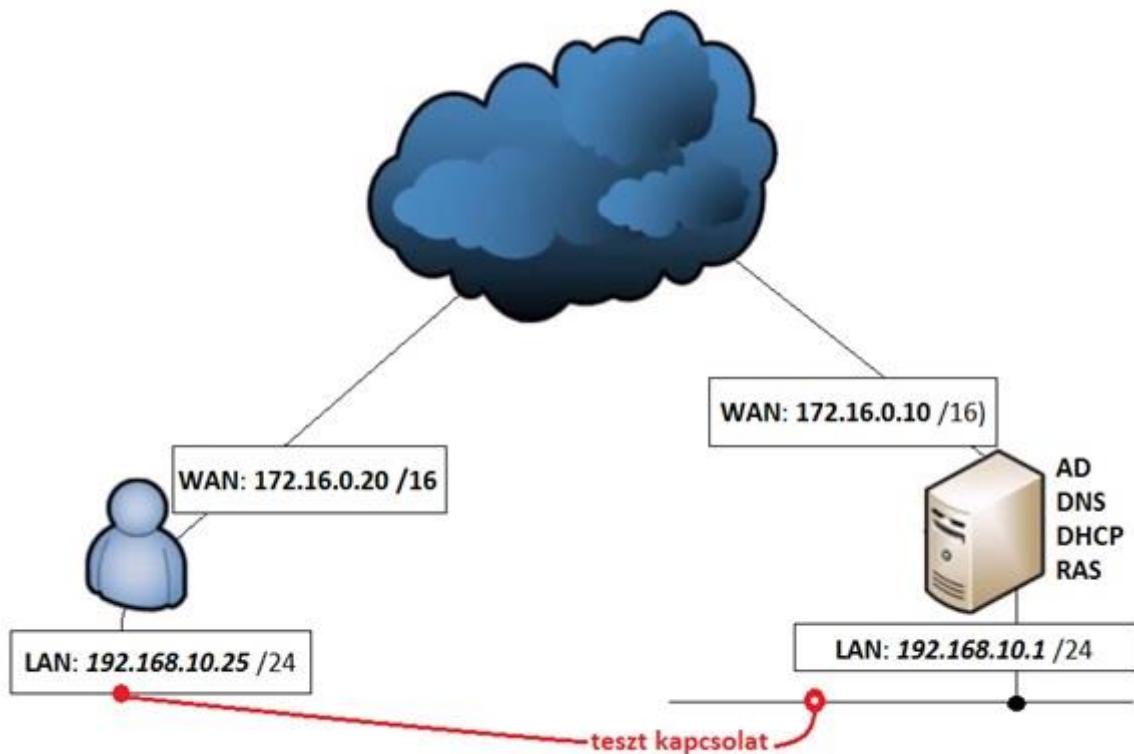
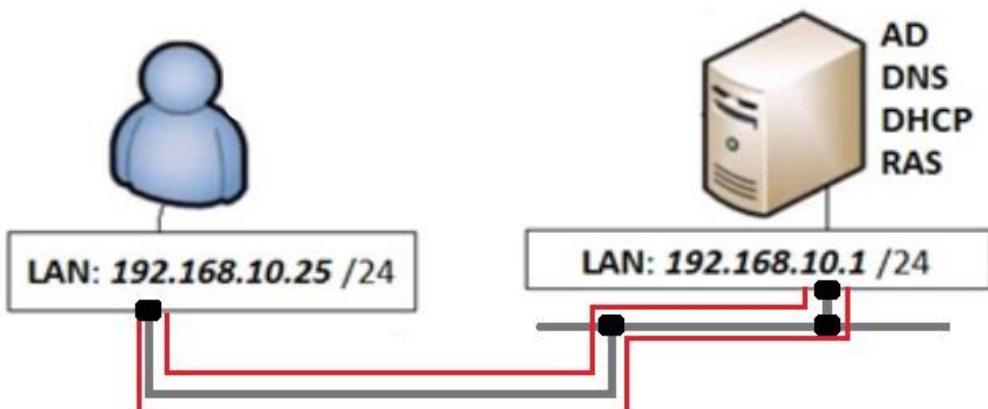


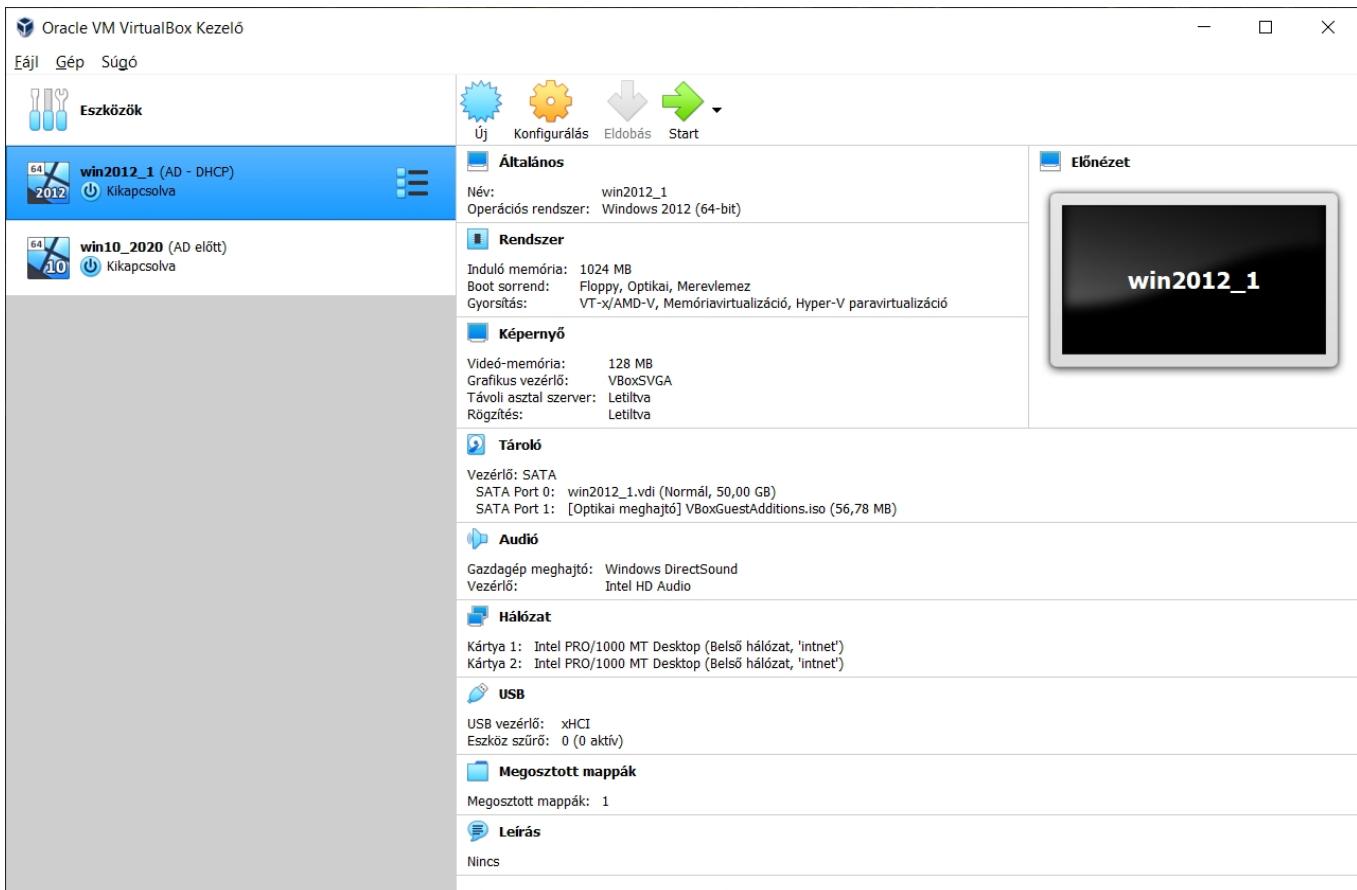
VPN kapcsolat (2-2 Ethernet hálózati csatolóval)



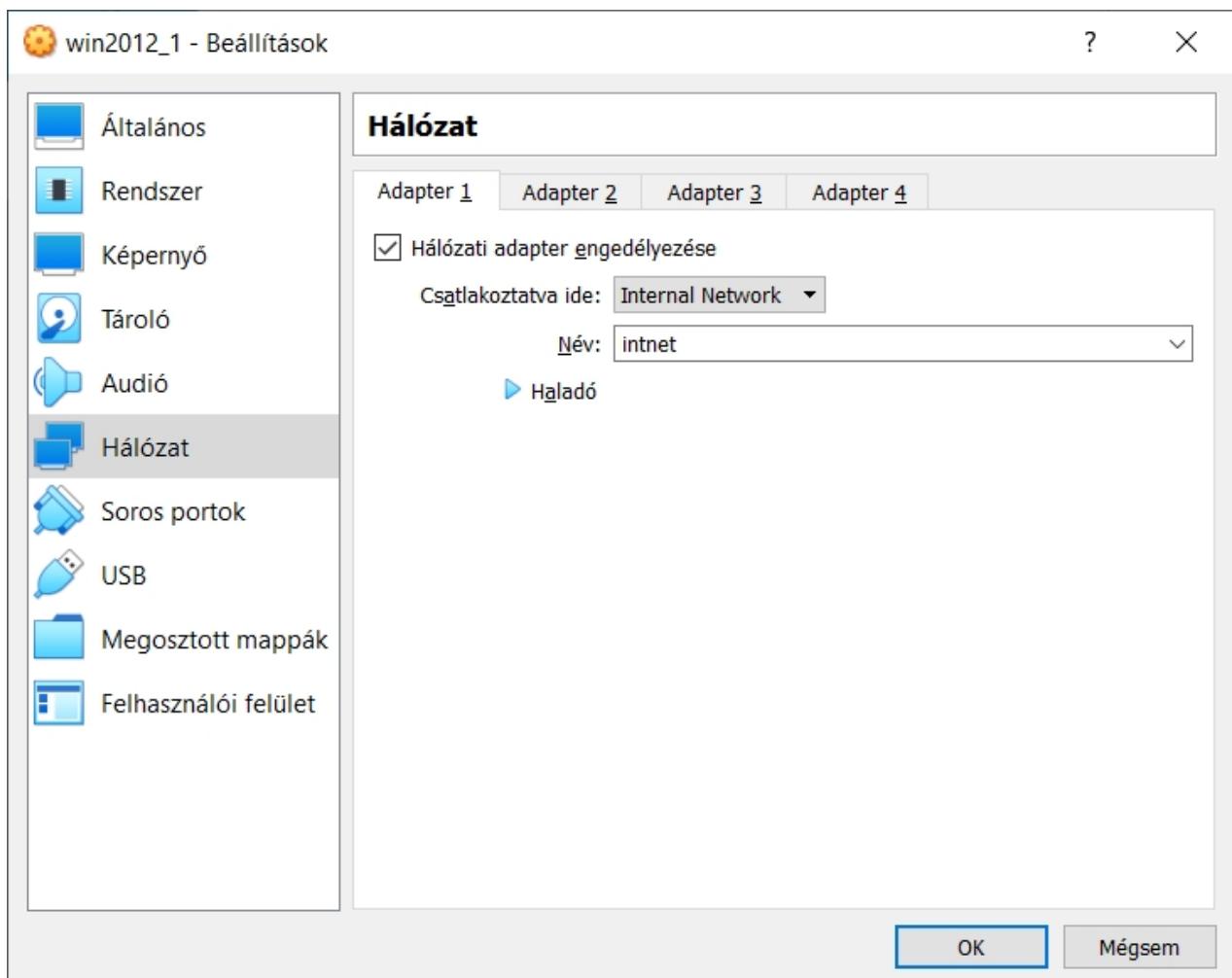
VPN kapcsolat (1-1 Ethernet hálózati csatolóval)



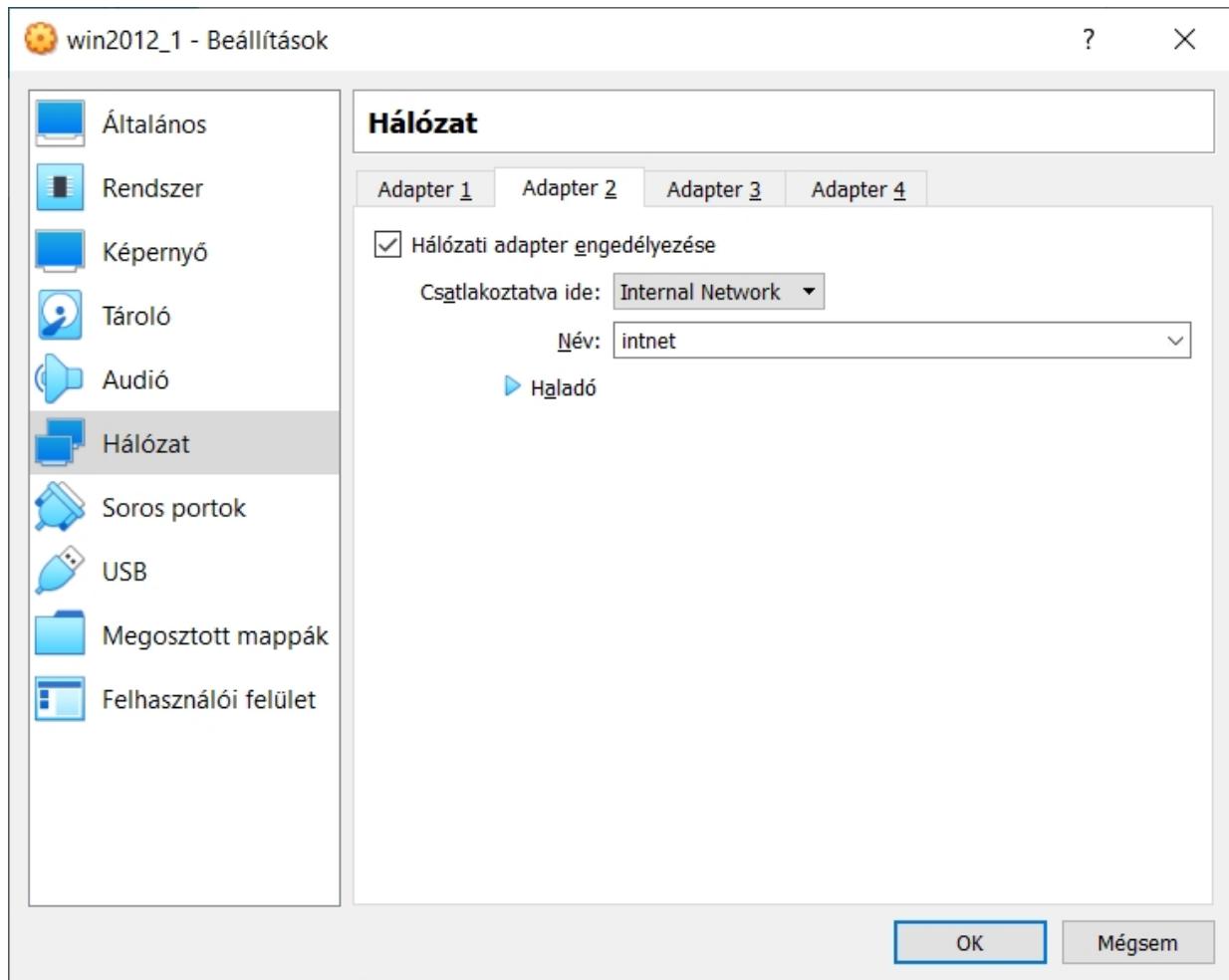
## Szerver konfigurálása 2 hálózati kártyával – VPN:



Ez az eredetileg is a gépen található hálózati csatoló:



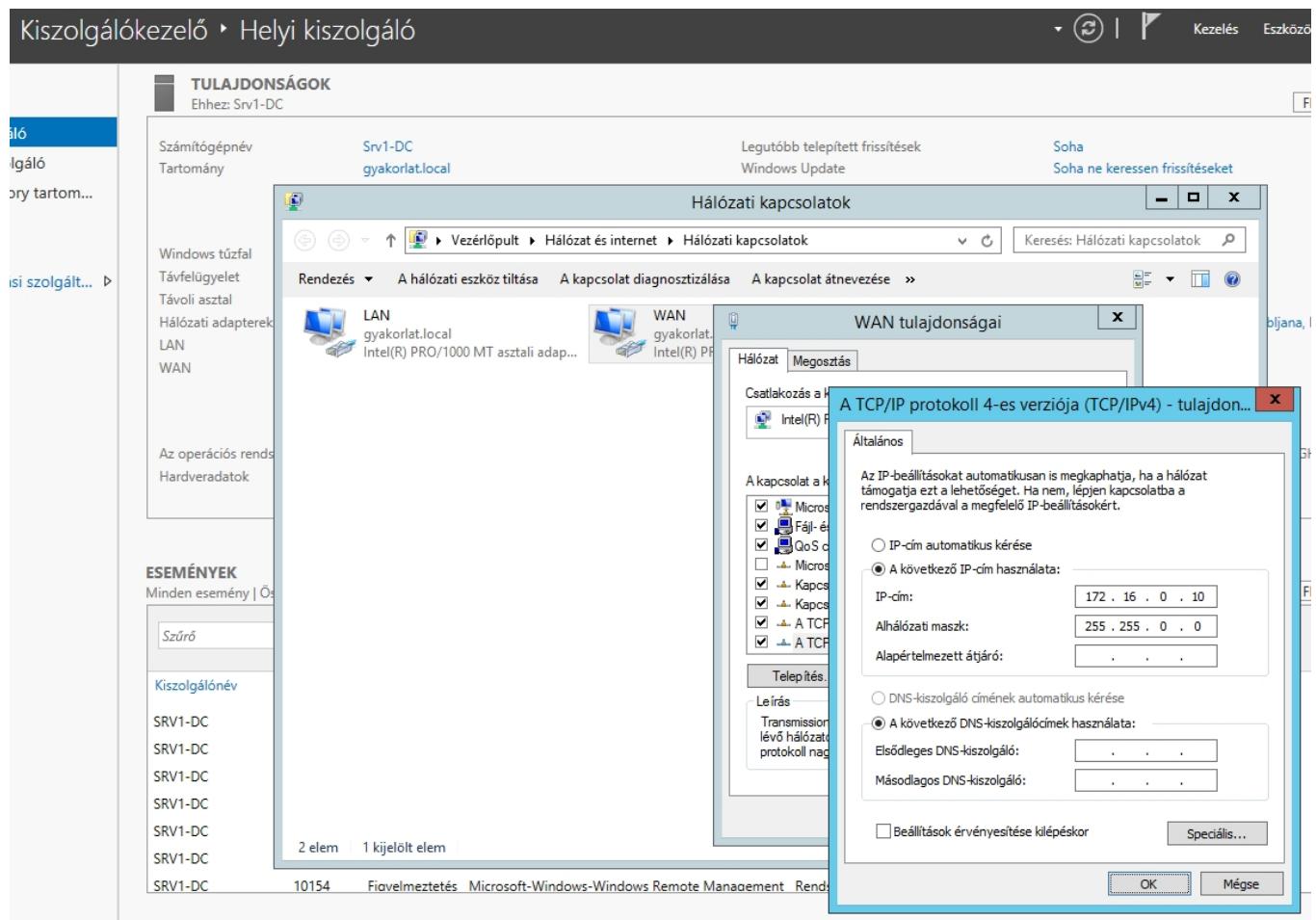
Ez a hozzáadott második hálózati csatoló:



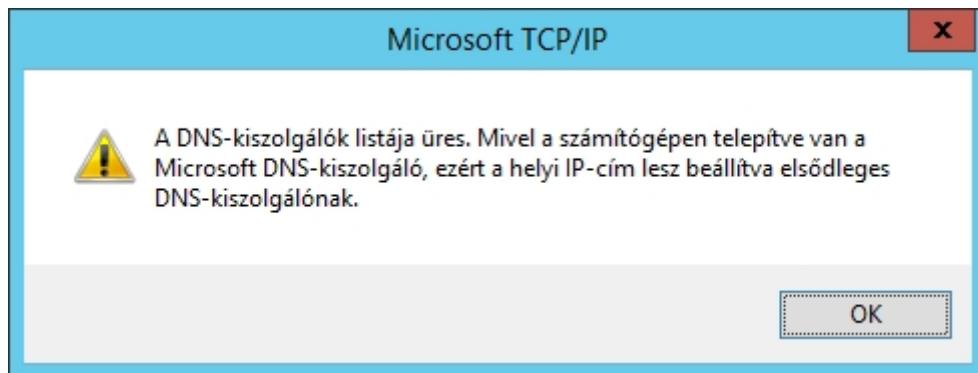
Szerver indítása után jól látszik a második hálózati kártya még DHCP-n keresztül próbál IP-címet kapni:

The screenshot shows the 'Local Server Properties' dialog under 'Kiszolgálókezelő > Helyi kiszolgáló'. The left sidebar lists 'Szolgáltató', 'Tároló', 'Tároló tartomány...', 'Helyi szolgáltató...', and 'Tároló tartomány...'. The main pane is titled 'TULAJDONSÁGOK' and shows properties for the server 'Srv1-DC'. The properties listed are: Számítógépnév (Srv1-DC), Tartomány (gyakorlat.local), Windows tűzfal (Tartomány: Bekapcsolva), Távfelügyelet (Engedélyezve), Távoli asztal (Engedélyezve), Hálózati adapterek összevonása (Letiltva), Ethernet (192.168.10.1; IPv6 engedélyezve), and Ethernet 2 (DHCP által kiosztott IPv4-cím; IPv6 engedélyezve).

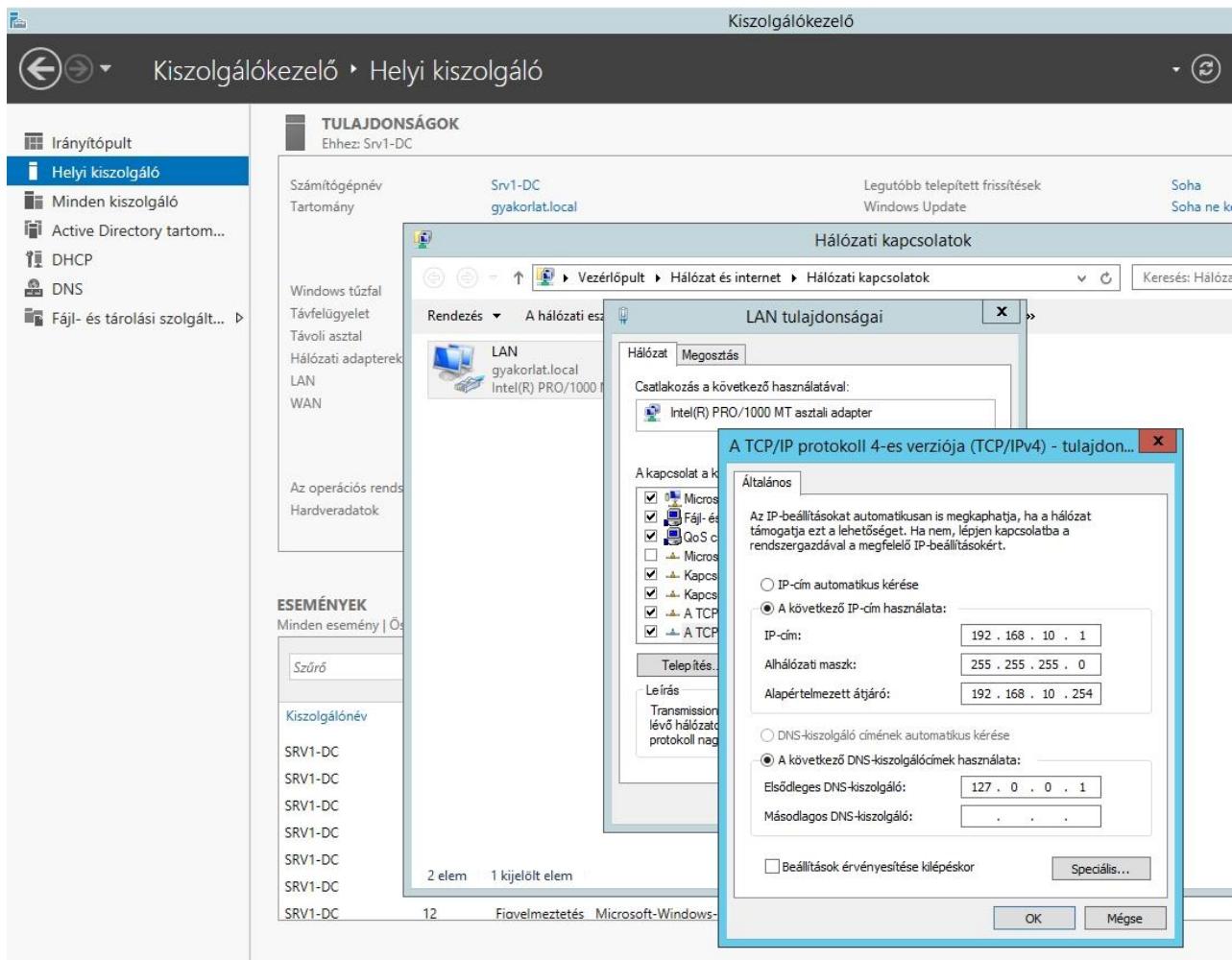
Nevezzük át a hálózati kapcsolatokat és konfiguráljuk a hálózatunknak megfelelően:



A **WAN** kapcsolatunk szimulálja az Internetet, de nincs működő DNS kiszolgáló azon a hálózaton, **OK**:



Ellenőrizzük a **LAN** nevű hálózati csatoló beállításait is:



Itt célszerű ellenőrizni, hogy a kártyák és az IP protokoll is megfelelően működik-e:

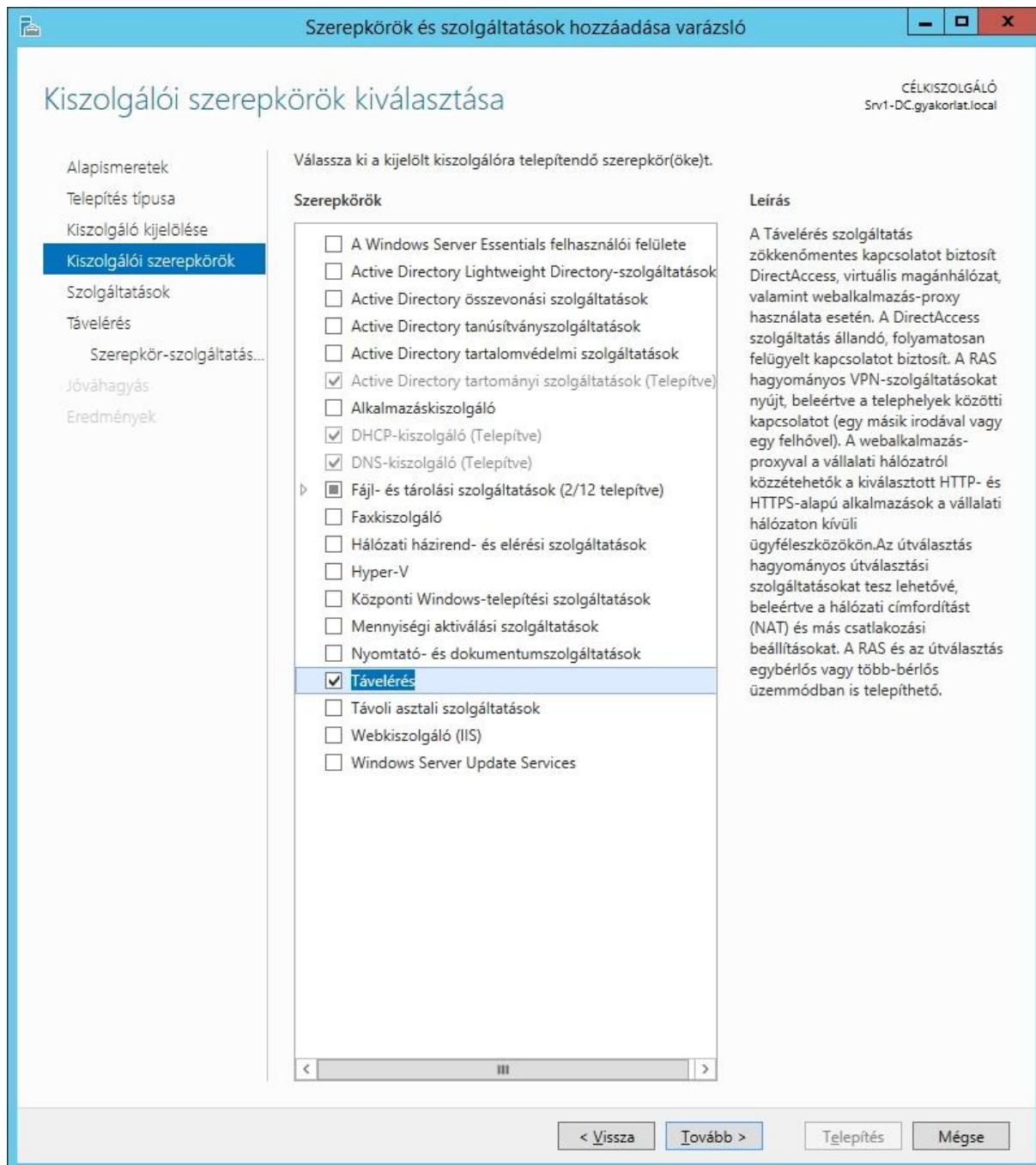
Parancssor:

**ping 192.168.10.1**

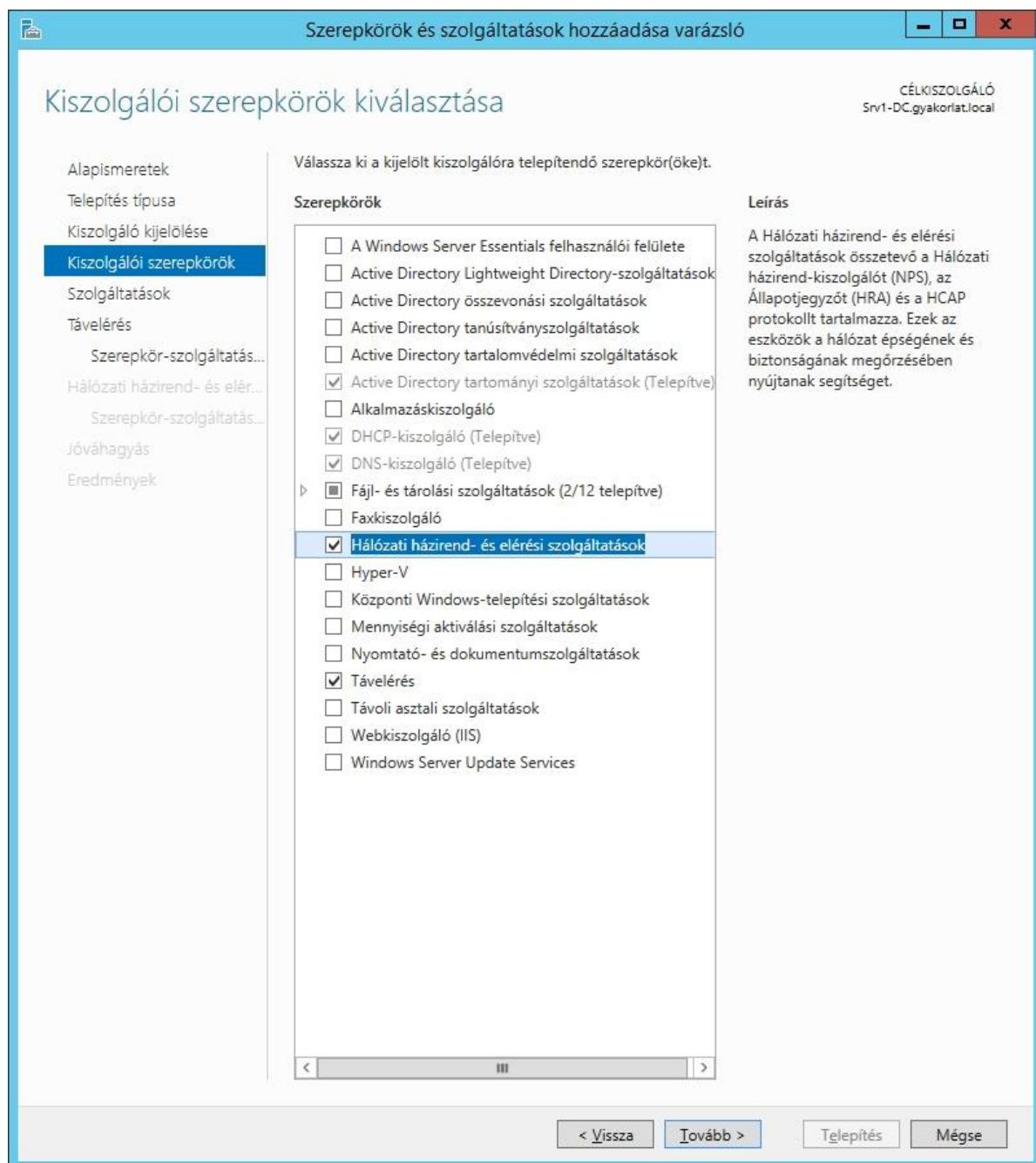
**ping 172.16.0.10**

Szerverünkhez adjuk hozzá a szükséges szerepköröket:

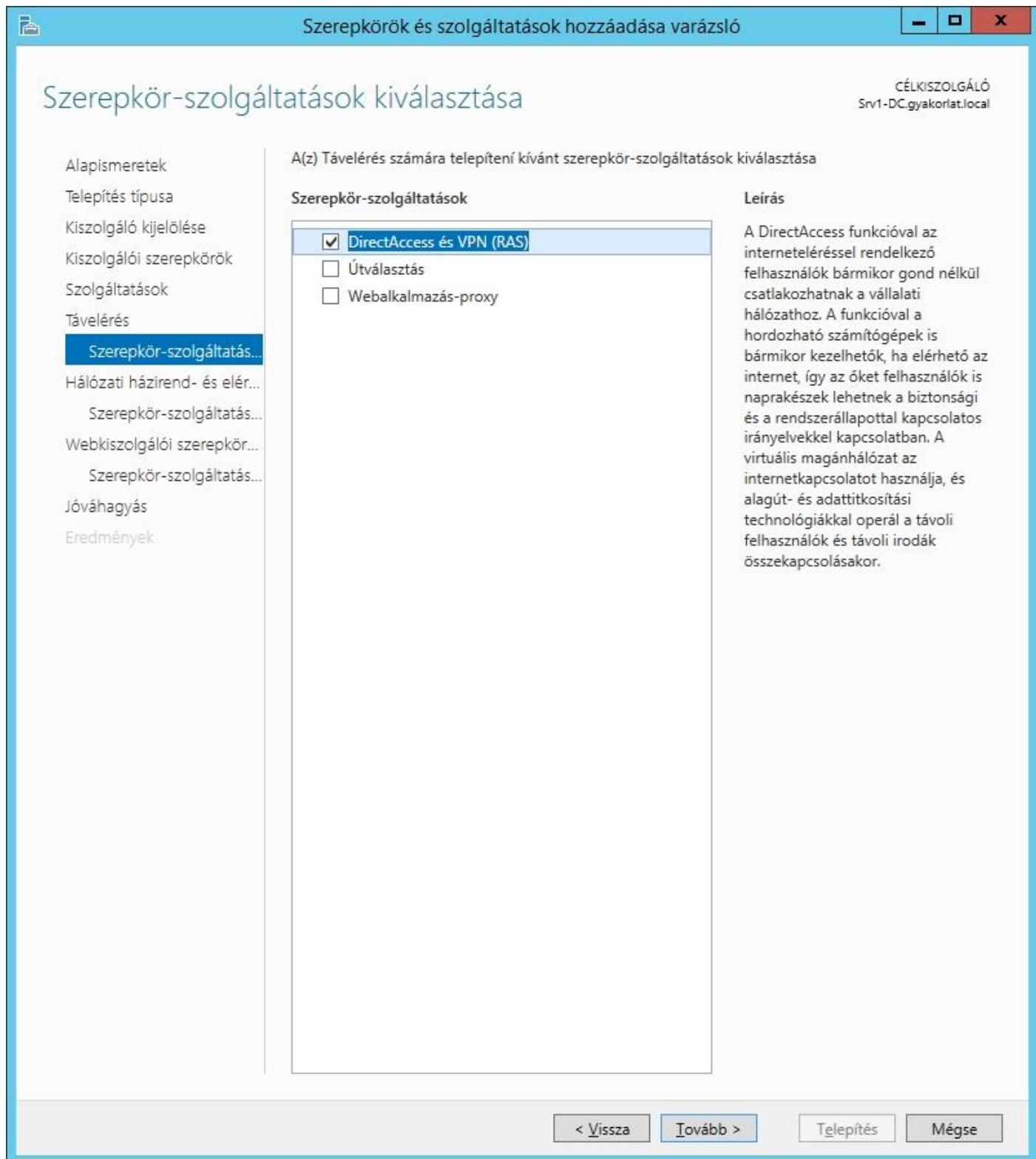
**Távelérés:**



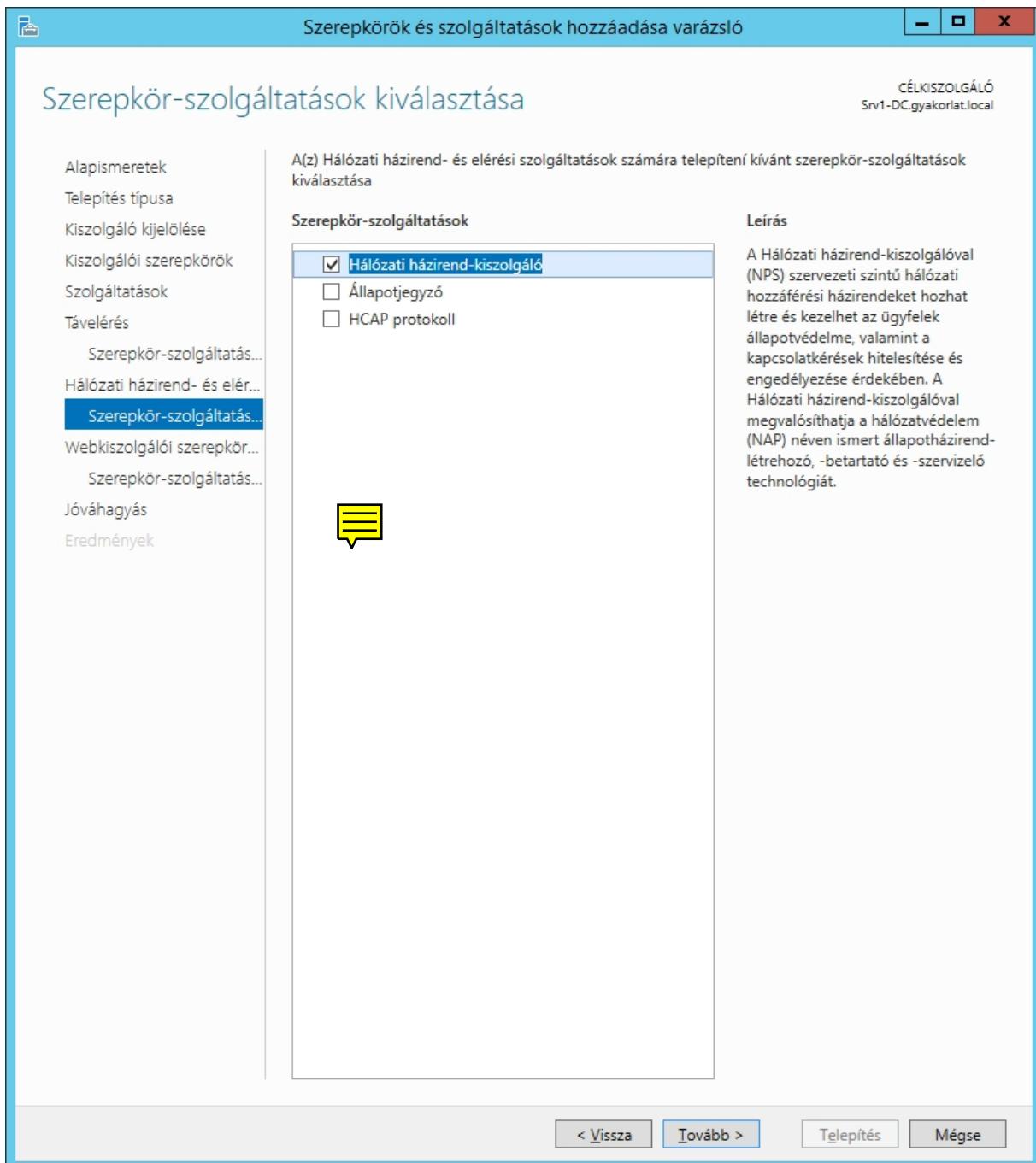
## Hálózati házirend- és elérési szolgáltatások:



A Távelérés szerepkörből a **VPN (RAS) szerepkör-szolgáltatásra** lesz szükségünk:



A Hálózati házirend-kiszolgáló már meg van jelölve telepítésre:



A Távelérés szerepkör működéséhez telepíti a Webkiszolgálói szerepkört automatikusan megjelölve amire szüksége van, pl. az **IP-cím és tartomány korlátozása** szerepkör-szolgáltatást:

Szerepkörök és szolgáltatások hozzáadása varázsló

CÉLKISZOLGÁLÓ  
Srv1-DC.gyakorlat.local

## Szerepkör-szolgáltatások kiválasztása

Alapismeretek

Telepítés típusa

Kiszolgáló kijelölése

Kiszolgálói szerepkörök

Szolgáltatások

Távelérés

Szerepkör-szolgáltatás...

Hálózati házirend- és elér...

Szerepkör-szolgáltatás...

Webkiszolgálói szerepkör...

Szerepkör-szolgáltatás...

Jóváhagyás

Eredmények

A(z) Webkiszolgáló (IIS) számára telepíteni kívánt szerepkör-szolgáltatások kiválasztása

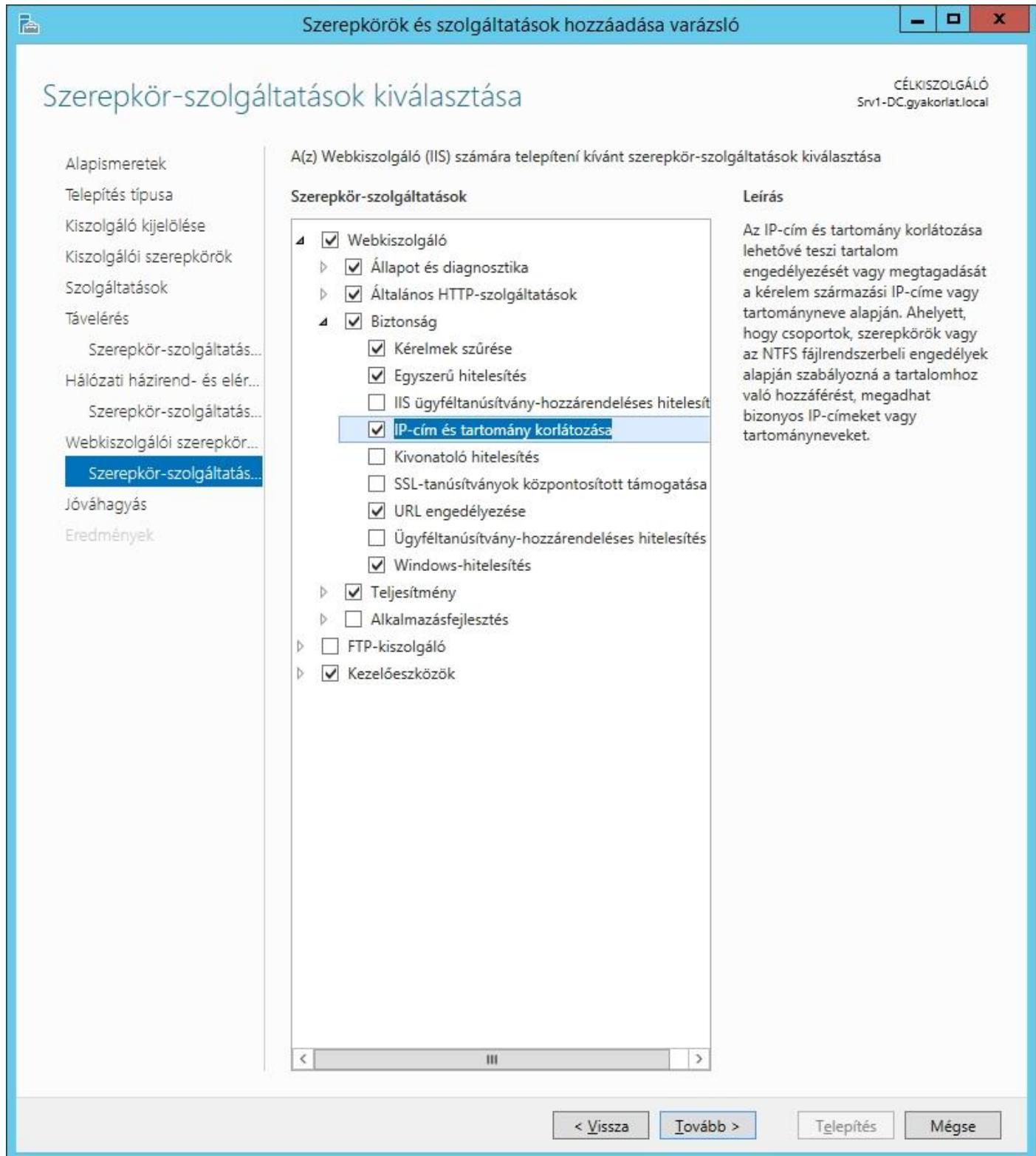
**Szerepkör-szolgáltatások**

<input checked="" type="checkbox"/> Webkiszolgáló	A kezelőeszközök biztosítják az IIS 8 szolgáltatást futtató webkiszolgálók kezeléséhez szükséges infrastruktúrát. A webkiszolgáló kezeléséhez használhatja az IIS felhasználói felületét, parancssori eszközöket, illetve parancsprogramokat. A konfigurációs fájlok közvetlenül is szerkesztheti.
<input checked="" type="checkbox"/> Állapot és diagnosztika	
<input checked="" type="checkbox"/> Általános HTTP-szolgáltatások	
<input checked="" type="checkbox"/> Biztonság	
<input checked="" type="checkbox"/> Kérelmek szűrése	
<input type="checkbox"/> Egyszerű hitelesítés	
<input type="checkbox"/> IIS ügyféltanúsítvány-hozzárendeléses hitelesítés	
<input checked="" type="checkbox"/> IP-cím és tartomány korlátozása	
<input type="checkbox"/> Kivonatoló hitelesítés	
<input type="checkbox"/> SSL-tanúsítványok központosított támogatása	
<input type="checkbox"/> URL engedélyezése	
<input type="checkbox"/> Ügyféltanúsítvány-hozzárendeléses hitelesítés	
<input type="checkbox"/> Windows-hitelesítés	
<input checked="" type="checkbox"/> Teljesítmény	
<input type="checkbox"/> Alkalmazásfejlesztés	
<input type="checkbox"/> FTP-kiszolgáló	
<input checked="" type="checkbox"/> Kezelőeszközök	

< III >

< Vissza Tovább > Telepítés Mégse

Amennyiben a webkiszolgálóhoz további szerepkör-szolgáltatásokat szeretnénk adni, azt most is megtehetjük:



Indulhat a telepítés:

Szerepkörök és szolgáltatások hozzáadása varázsló

## Telepítendő összetevők megerősítése

CÉLKISZOLGÁLÓ  
Srv1-DC.gyakorlat.local

Alapismeretek

Telepítés típusa

Kiszolgáló kijelölése

Kiszolgálói szerepkörök

Szolgáltatások

Távelérés

- Szerepkör-szolgáltatás...
- Hálózati házirend- és elér...
- Szerepkör-szolgáltatás...
- Webkiszolgálói szerepkör...
- Szerepkör-szolgáltatás...

Jóváhagyás

Eredmények

Ha telepíteni kívánja a következő szerepköröket, szerepkör-szolgáltatásokat vagy szolgáltatásokat a megadott kiszolgálón, kattintson a Telepítés gombra.

Célkiszolgáló automatikus újraindítása, ha szükséges

Előfordulhat, hogy ezen a lapon választható szolgáltatások (például felügyeleti eszközök) is megjelennek, mivel automatikusan lettek kiválasztva. Ha ezeket nem szeretné telepíteni, kattintson a Vissza gombra, és törölje a jelet a megfelelő jelölőnégyszekből.

Belső Windows-adatbázis

Hálózati házirend- és elérési szolgáltatások

Hálózati házirend-kiszolgáló

RAS - csatlakozáskezelő felügyeleti csomag (CMAK)

Távelérés

DirectAccess és VPN (RAS)

Távoli kiszolgálófelügyelet eszközei

Szerepkör-felügyeleti eszközök

A Hálózati házirend- és elérési szolgáltatások eszközei

Távelérés-kezelési eszközök

Távelérési grafikus felhasználói felület és parancssori eszközök

Távelérési modul a Windows PowerShell szolgáltatáshoz

Webkiszolgáló (IIS)

Kezelőeszközök

IIS-kezelő konzol

IIS-kezelési parancsprogramok és eszközök

Webkiszolgáló

Általános HTTP-szolgáltatások

Alapértelmezett dokumentum

Könyvtár tallózása

HTTP-hibák

Statikus tartalom

Állapot és diagnosztika

HTTP-naplózás

Teljesítmény

Konfigurációs beállítások exportálása

Alternatív forrás elérési útjának megadása

< Vissza    Tovább >    Telepítés    Mégse

A telepítés befejezésekor megjelenik az [Első lépések varázsló megnyitása](#) link. Kattintsunk rá és várjuk meg amíg elindul a varázsló:

Szerepkörök és szolgáltatások hozzáadása varázsló

CÉLKISZOLGÁLÓ  
Srv1-DC.gyakorlat.local

## Telepítési folyamat

Alapismeretek

- Telepítés típusa
- Kiszolgáló kijelölése
- Kiszolgálói szerepkörök
- Szolgáltatások
- Távelérés
  - Szerepkör-szolgáltatás...
  - Hálózati házirend- és elér...
  - Szerepkör-szolgáltatás...
  - Webkiszolgálói szerepkör...
  - Szerepkör-szolgáltatás...
- Jóváhagyás

Eredmények

### Telepítési folyamat megtekintése

#### Szolgáltatás telepítése

Konfigurálás szükséges. A telepítés sikeres volt a(z) Srv1-DC.gyakorlat.local kiszolgálón.

#### Távelérés

- DirectAccess és VPN (RAS)
- Szerepkör konfigurálása
  - [Az Első lépések varázsló megnyitása](#)

#### Belső Windows-adatbázis

- Hálózati házirend- és elérési szolgáltatások
- Hálózati házirend-kiszolgáló
- RAS - csatlakozáskezelő felügyeleti csomag (CMAK)
- Távoli kiszolgálófelügyelet eszközei
- Szerepkör-felügyeleti eszközök
  - A Hálózati házirend- és elérési szolgáltatások eszközei
- Távelérés-kezelési eszközök
  - Távelérési grafikus felhasználói felület és parancssori eszközök
  - Távelérési modul a Windows PowerShell szolgáltatáshoz

#### Webkiszolgáló (IIS)

- Kezelőeszközök
  - IIS-kezelő konzol
  - IIS-kezelési parancsprogramok és eszközök

#### Webkiszolgáló

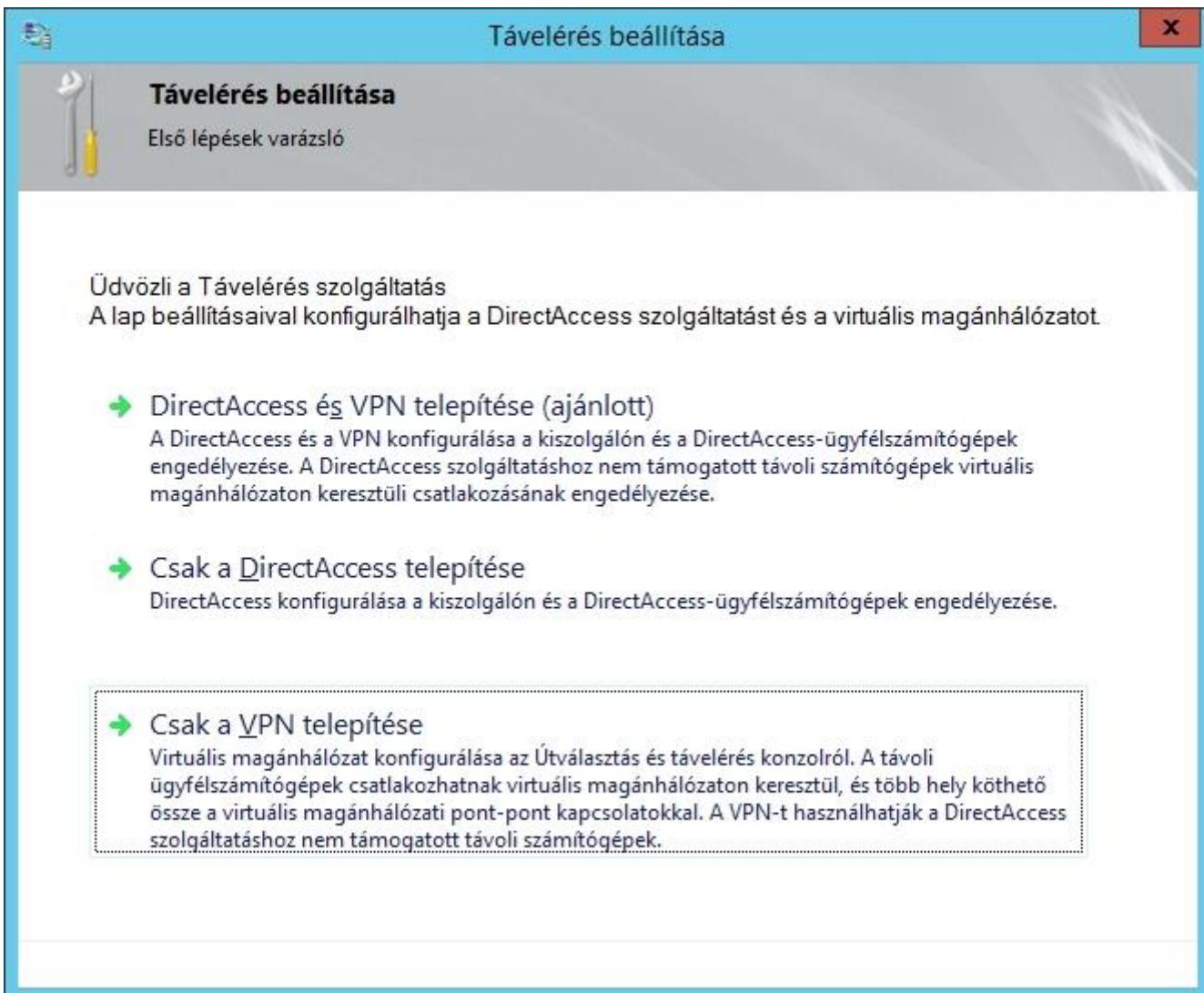
- Általános HTTP-szolgáltatások
  - Alapértelmezett dokumentum
  - Könyvtár tallózása
  - HTTP-hibák
  - Statikus tartalom
- Állapot és diagnosztika
  - HTTP-naplázás

Ezt a varázslót a futó műveletek megszakítása nélkül bezárhatja. A művelet folyamatát megtekintheti vagy ezt a lapot újra megnyithatja a parancssáv Értesítések elemére, majd a Feladat részletei parancsra kattintva.

Konfigurációs beállítások exportálása

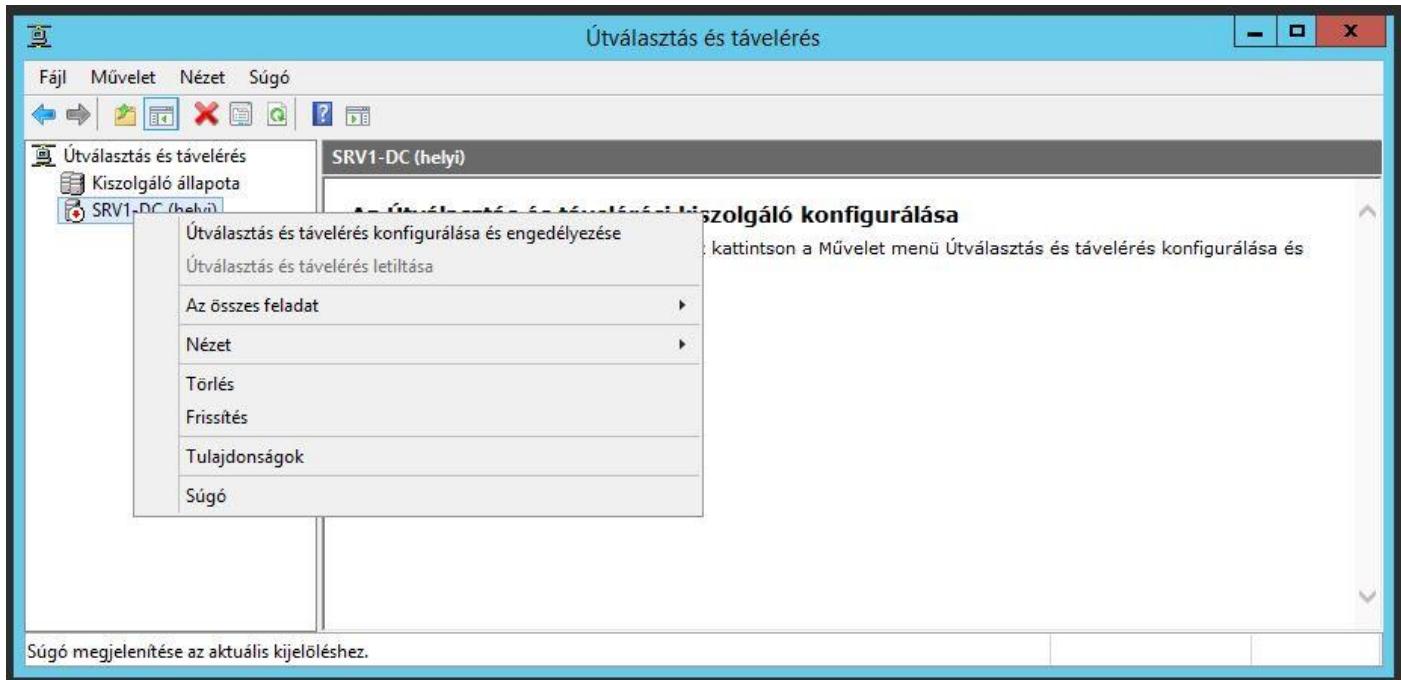
< Vissza Tovább > Bezárás Mégse

Az **Első lépések varázsló**: Kattintsunk a **Csak VPN telepítése** lehetőségre:

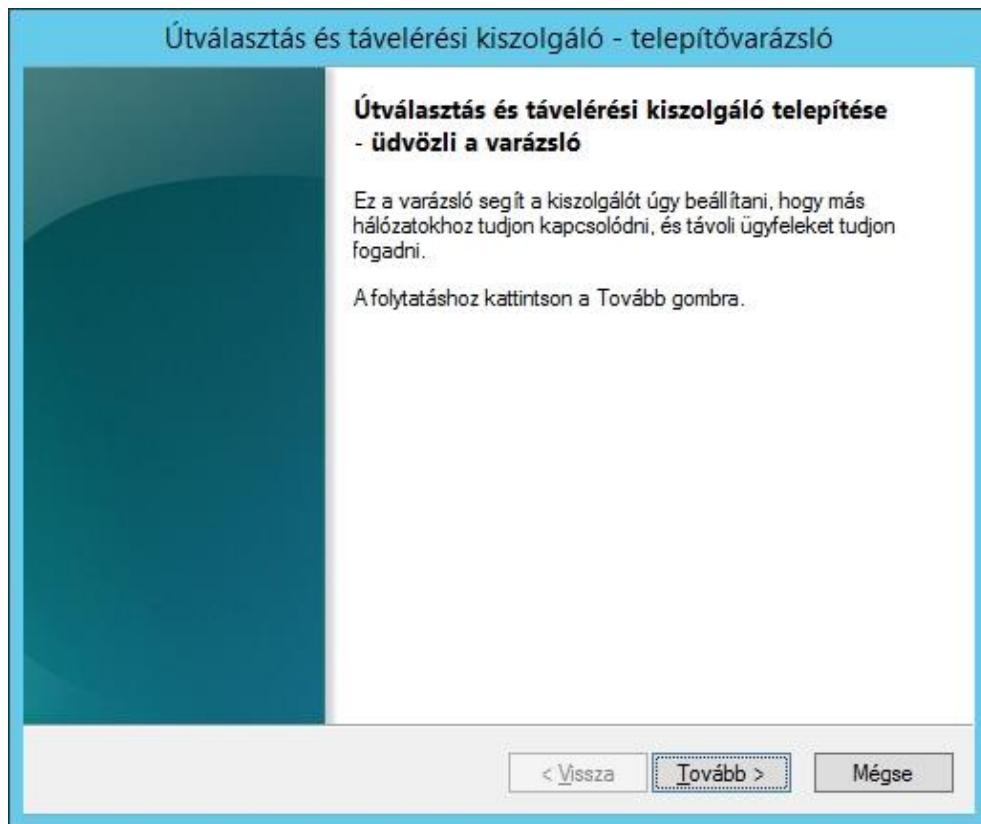


Az **Első lépések varázsló** elindítja az Útválasztás és távelérés kezelőt (A Kiszolgáló kezelő / Eszközökben is elérhető)

A szerverünkre jobb egérrel kattintva előtűnik a helyi menü, válasszuk a **távelérés konfigurálását és engedélyezését**:



Tovább:



Válasszuk az **Egyéni konfiguráció**-t:

**Útválasztás és távelérési kiszolgáló - telepítővarázsló**

**Konfiguráció**  
Engedélyezheti a következő szolgáltatáskombinációk bármelyikét, vagy testreszabhatja ezt a kiszolgálót.

**Távelérés (telefonos vagy VPN)**  
Távoli ügyfelek kapcsolódhatnak ehhez a kiszolgálóhoz telefonos vagy biztonságos virtuális magánhálózaton (VPN) keresztül.

**Hálózati címfordítás (NAT)**  
Belső ügyfelek kapcsolódhatnak az internethez egyetlen nyilvános IP-cím használatával.

**Virtuális magánhálózati (VPN) hozzáférés és NAT**  
Távoli ügyfelek kapcsolódhatnak ehhez a számítógéphez az interneten keresztül, valamint helyi ügyfelek kapcsolódhatnak az internetre egyetlen nyilvános IP-cím használatával.

**Biztonságos kapcsolat két magánhálózat között**  
A hálózat összekötése egy távoli hálózattal, pl. egy másik iroda hálózatával.

**Egyéni konfiguráció**  
Az útválasztási és távelérési funkciók tetszőleges kombinációjának kiválasztása.

[\*\*< Vissza\*\*](#) [\*\*Tovább >\*\*](#) [\*\*Mégse\*\*](#)

Virtuális magánhálózat, azaz VPN:

**Útválasztás és távelérési kiszolgáló - telepítővarázsló**

**Egyéni konfiguráció**  
Miután a varázsló bezárt, a kiválasztott szolgáltatásokat az Útválasztás és távelérés konzolban lehet beállítani.

Válassza ki azokat a szolgáltatásokat, amelyeket engedélyezni szeretne ezen a kiszolgálón.

**Virtuális magánhálózat**

**Telefonos hálózat**

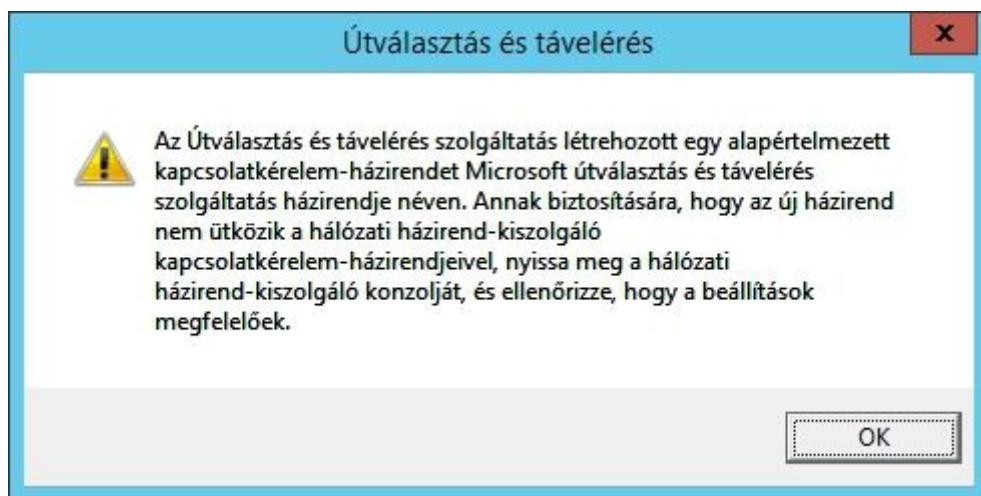
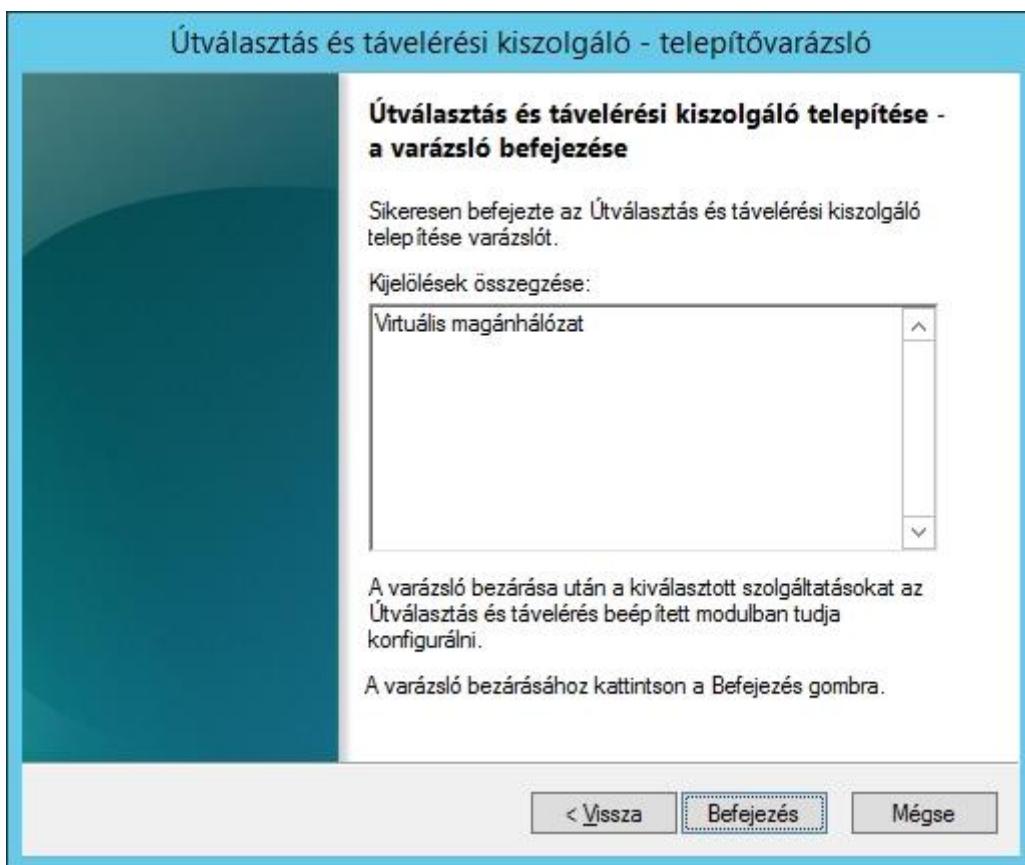
**Igény szerinti kapcsolat (irodai útválasztáshoz)**

**Hálózati címfordítás (NAT)**

**LAN-útválasztás**

[\*\*< Vissza\*\*](#) [\*\*Tovább >\*\*](#) [\*\*Mégse\*\*](#)

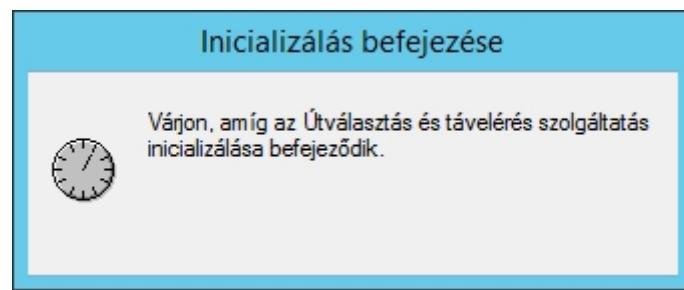
Miután a **Befejezésre** kattintunk, a rendszer létrehoz egy **alapértelmezett kapcsolatkérelem-házirendet**:



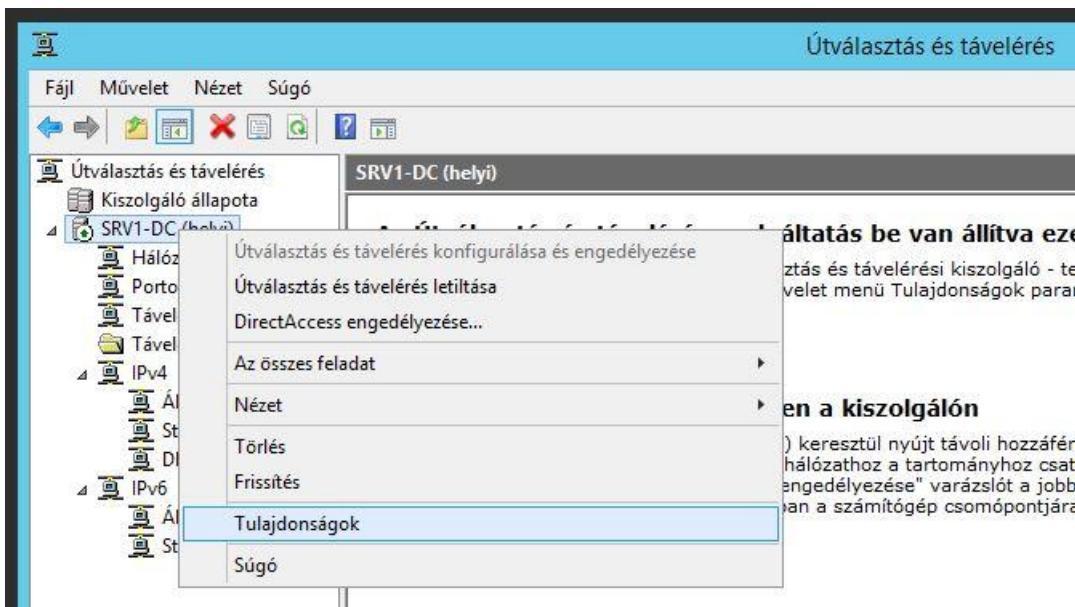
Indítsuk el a szolgáltatást:



Türelem 😊:



A távelérés kiszolgáló tulajdonságait a szerveren jobb egér kattintással elérhető helyi menüben találhatjuk:



Az **Általános lapon** nincs teendő. Az **IPv4 lapon** csak akkor, ha nem az alapértelmezett DHCP kiszolgálót szeretnénk használni. Ez esetben a Távelérés kiszolgáló (RAS) képes DHCP-ként címeket osztani a VPN kapcsolatoknak:

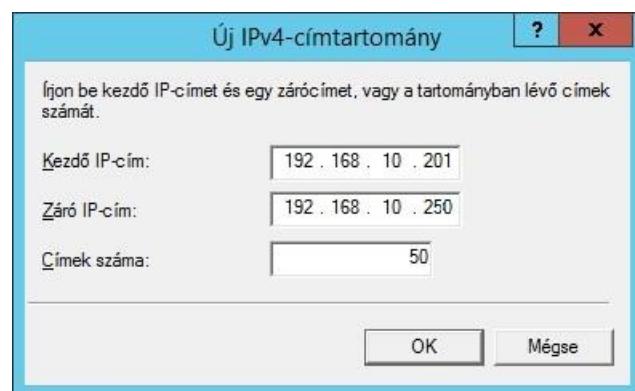
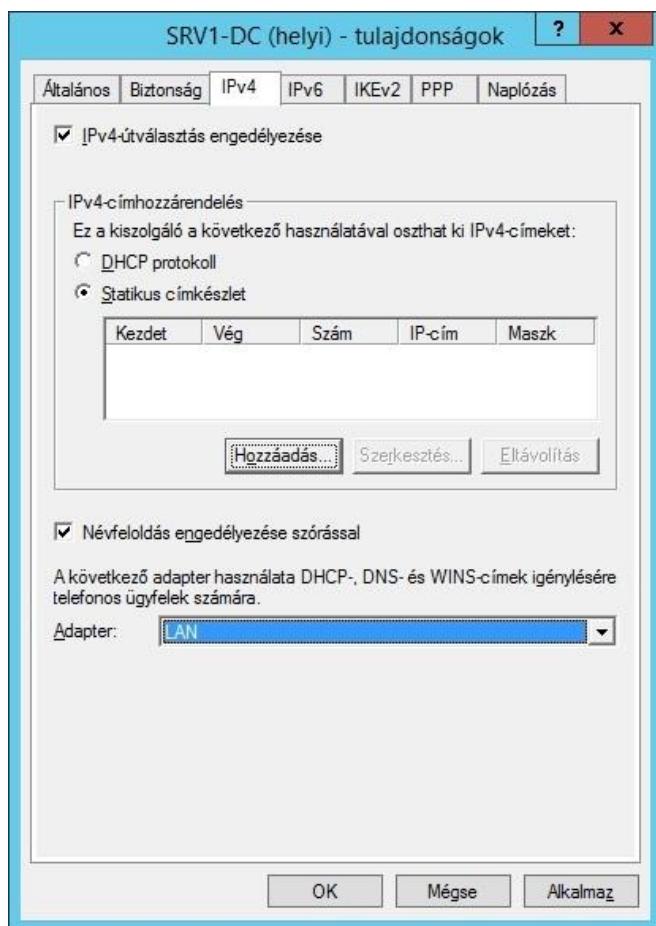
The left window shows the 'General' tab with the following settings:

- IPv4-Router
- Only local network (LAN) routing
- LAN- and remote address-based routing
- IPv6-Router
- IPv6 Routerless routing

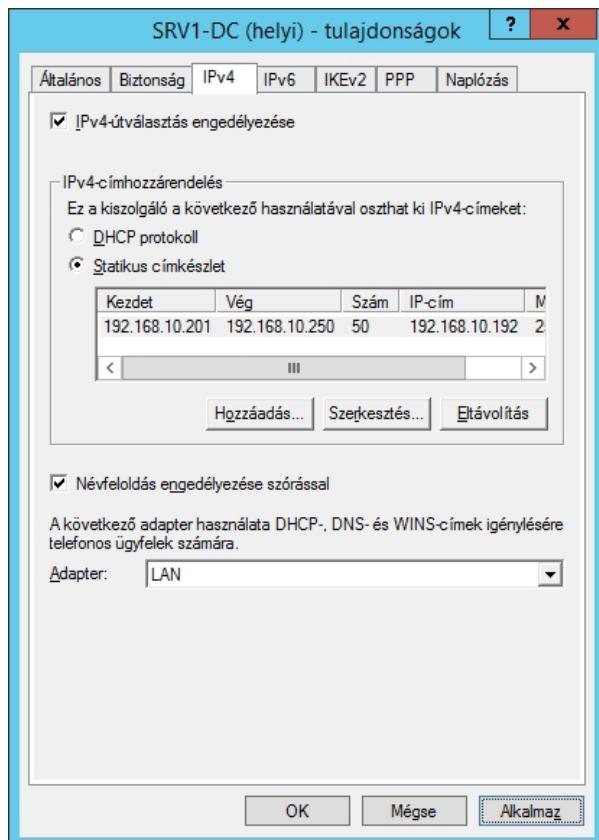
The right window shows the 'IPv4' tab with the following settings:

- IPv4-routing enabled
- DHCP protocol
- Static address assignment
- Enable DNS resolution
- Adapter: LAN

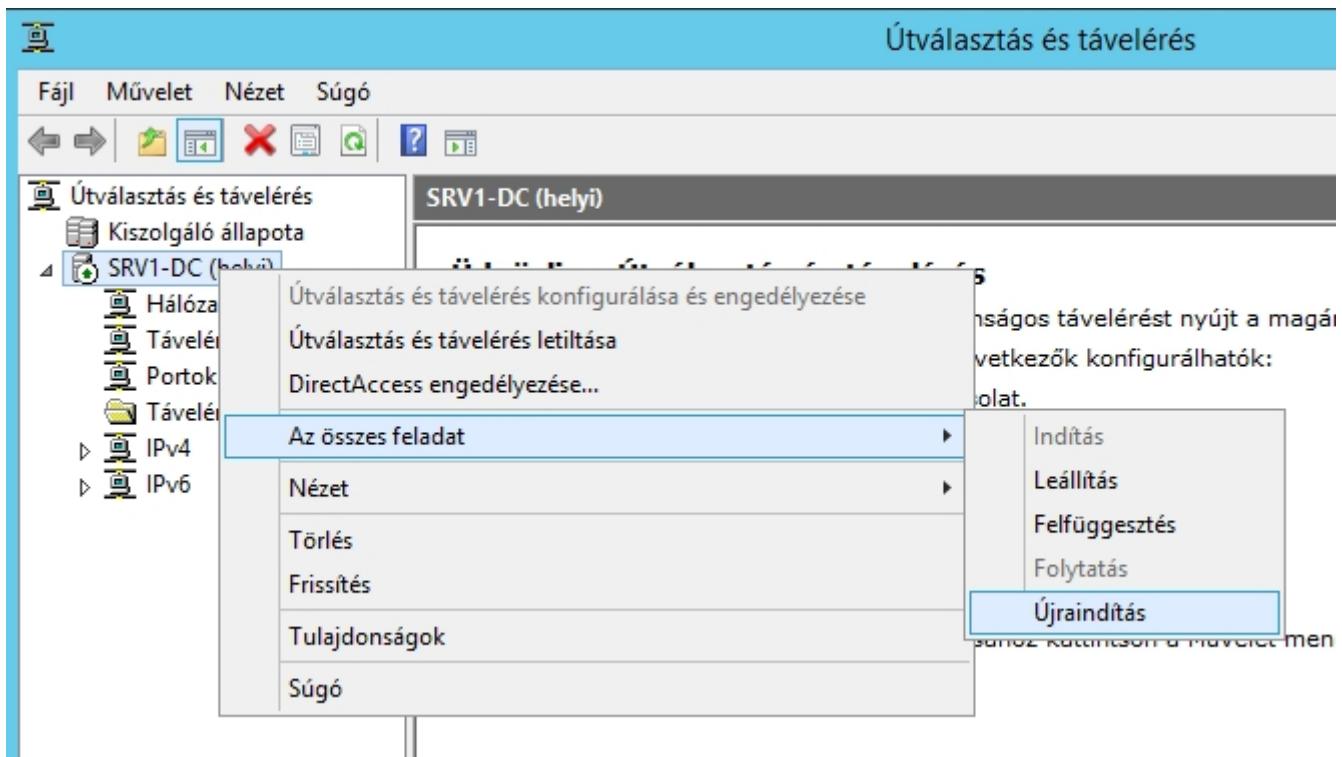
Ha **statikus címkészletet** használunk, a tartományunk címtartományának megfelelően adjuk meg a címkészletet:



A címtartományunk elkészült, a Távelérés kiszolgáló működésre kész:



Bizonyos esetekben szükségünk lehet a **Távelérés kiszolgáló újraindítására, felfüggesztésére** vagy **leállítására**:



A Hálózati házirend-kiszolgáló konfigurálása előtt hozunk létre néhány teszt felhasználót:

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, there's a navigation pane with icons for File, Tools, View, and various Active Directory objects like users, groups, and domains. The main pane displays a table with columns: Név (Name), Típus (Type), and Leírás (Description). There are three entries: 'Teszt1' (User), 'Teszt2' (User), and 'tesztelők' (Global security group). The 'tesztelők' entry has a small user icon next to it.

A Hálózati házirend-kiszolgáló kezelőjét elindíthatjuk közvetlenül a Távelérés kiszolgálóból is.

A **Távelérés naplázása és házirendjei** konzolfa résznél: ez esetben csak a Táveléréshez szükséges nézetben indul el:

This screenshot shows the Routing and Remote Access (RRAS) Management console. The left pane lists various components: 'Útválasztás és távelérés' (Routing and Remote Access), 'Kiszolgáló állapota' (Server status), 'SRV1-DC (helyi)' (Local SRV1-DC), 'Hálózati illesztők' (Network adapters), 'Portok' (Ports), 'Távelérésű ügyfelek (0)' (0 Remote access clients), 'Távelérésnaplózás és házirende' (Traffic shaping and policies), 'IP' (IP), and 'Aittalanos' (Default). A context menu is open over the 'IP' item, with options: 'Nézet' (View), 'Frissítés' (Update), and 'Súgó' (Help). The right pane is titled 'Távelérés naplázása és házirendjei' and contains descriptive text about traffic shaping and policies.

Azonban, ha minden funkciót szeretnénk elérni a Hálózati házirend-kiszolgáló kezelőjében akkor indítsuk a **Kiszolgáló kezelő / Eszközök / Hálózati házirend-kiszolgáló kezelőt**:

This screenshot shows the Server Manager console. The top navigation bar includes File, Tools, View, and Help. The 'Eszközök' (Tools) tab is currently selected. The left pane has sections for 'Legutóbb telepített frissítések' (Recently installed updates), 'Windows Update', 'Frissítések legutóbbi ellenőrzése' (Check latest updates), 'Windows hibajelentés' (Windows error reporting), 'Felhasználói élmény fokozása program' (User experience optimization program), 'Internet Explorer - Fokozott biztonsági ellenőrzés' (Internet Explorer - Enhanced security check), 'Időzóna' (Time zone), and 'Termékazonosító' (Product key). The bottom pane shows system details: 'Standard' (Standard), 'Processzorok' (Processors), 'Memória (RAM) mérete' (Memory (RAM) size), and 'Teljes lemezterület' (Total disk space). The right pane lists various management tools under the 'Eszközök' tab, with 'Hálózati házirend-kiszolgáló' (Network Policy and Services) highlighted.

Hálózati házirend-kiszolgáló kezelőben kezdetben **csak két tiltó házirend** van:

Házirend neve	Állapot	Feldolgozási sorrend	Hozzáférési típus	Forrás
Kapcsolatok a Microsoft Útválasztás és távelérés szolgáltatását futtató kiszolgálóval	Engedélyezve	999998	Hozzáférés tiltása	Meghatározatlan
Kapcsolatok más elérési kiszolgálókkal	Engedélyezve	999999	Hozzáférés tiltása	Meghatározatlan

Hozzunk létre új házirendet amivel mindenki betud lépni VPN-en keresztül, hétköznapokon: 8-18 között:

A hálózati házirendek segítségével megadhatja, ki jogosult a hálózathoz való kapcsolódásra, valamint megszabhatja a csatlakozás feltételeit.

Adjunk nevet a házirendünknek és válasszunk hálózat-hozzáférési típust:

**Új hálózati házirend**

### Adja meg a hálózati házirend nevét és a kapcsolattípust

Megadhatja a hálózati házirend nevét, illetve azon kapcsolattípusokat, amelyekre a házirend érvényes.

**Házirend neve:**  
VPN - mindenkinék|

Hálózati kapcsolódás módja  
Az NPS számára kapcsolódási kérelmet küldő hálózatelérési kiszolgáló típusának kiválasztása. Kiválaszthatja a hálózatelérési kiszolgáló típusát vagy a Szállítóspecifikus értéket, de egyik sem kötelező. Ha a hálózatelérési kiszolgáló 802.1X szabvány szerint hitelesítő kapcsoló vagy vezeték nélküli hozzáférési pont, válassza a Meghatározatlan lehetőséget.

Hálózathozzáférési kiszolgáló típusa:  
Távolerési kiszolgáló (telefonos VPN)

Szállítóspecifikus:  
10

[Vissza](#) [Tovább](#) [Befejezés](#) [Mégse](#)

### **Feltételek:**

Kötelezően meg kell adjunk **egy feltételelt minimum**, mi most adjuk meg az időre vonatkozó feltételünket:

**Új hálózati házirend**

### Feltételek megadása

Adjja meg azokat a feltételeket, amelyek meghatározzák, hogy a hálózati házirend ki lesz-e értékelve a kapcsolatkérelmekhez. Legalább egyet kell megadni.

**Feltételek:**

Feltétel	Érték

**Feltétel kijelölése**

Jelöljen ki egy feltételt, majd kattintson a Hozzáadása gombra.

**HCAP-felhasználócsoporthoz:**  
A HCAP-felhasználócsoporthoz tartozó feltétel megadja a házirendnek való megfeleléshez szükséges felhasználócsoporthat. A HCAP protokoll a hálózati házirend-kiszolgáló és a kiszolgált felhasználó közötti kommunikációban használatos. A feltétel hálózati NAS-dokumentációt.

**Nap és időpont korlátozásai:**  
A nap- és időkorlátozások adják meg azokat a napokat és időpontokat, amikor a hálózat hozzáférését biztosító kiszolgálók közötti kommunikációban használatos. A feltétel hálózati NAS-dokumentációt.

**Hálózatvédelem:**

**Azonosítás típusa:**  
Az Azonosítás típusa feltétel azokra az ügyfelekre korlátozza a házirendet, akik a hálózatvédelmi rendszerről lapot-kimutatás (SoH) használatával azonosíthatók.

**MS-Service osztály:**

**Feltétel leírása:**

[Hozzáadás...](#) [Szerkesztés...](#) [Eltárolás...](#)

[Vissza](#) [Tovább](#) [Befejezés](#) [Mégse](#)

**Nap és időpont korlátozásai**

0 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 0

Minden
hétfő
kedd
szerda
csütörtök
péntek
sombat
vasárnap

Engedélyezve  Megtagadva

hétfő - péntek, 8:00 - 18:00

[OK](#) [Mégse](#)

Egy feltétel megadva ( minden VPN kapcsolat létrejöhét, ha ennek a feltételnek megfelel, azonban ha nem teljesül a feltétel, a rendszer már nem is vizsgálja tovább, a következő házirend szabályra ugrik):

X

### Új hálózati házirend

#### Feltételek megadása

Adja meg azokat a feltételeket, amelyek meghatározzák, hogy a hálózati házirend ki lesz-e értékelve a kapcsolatkérelmekhez. Legalább egy feltétel szükséges.

**Feltételek:**

Feltétel	Érték
<input checked="" type="checkbox"/> Nap és időpont korlátozásai	Hétfő 08:00-18:00 Kedd 08:00-18:00 Szerda 08:00-18:00 Csütörtök 08:00-18:00 Péntek 08:00-18:00

< III >

Feltétel leírása:  
A nap- és időkorlátozások adják meg azokat a napokat és időpontokat, amikor a kapcsolódási kérelmek engedélyezettek vagy nem engedélyezettek. Ezek a korlátozások azon az időzónán alapulnak, ahol az hálózati házirend-kiszolgáló található.

[Hozzáadás...](#) [Szerkeszt...](#) [Eltávolítás](#)

Vissza Tovább Befejezés Mégse

Engedélyező házirendet hozunk létre! A jelölő négyzet üresen hagyásával biztosítjuk, hogy a Hálózati házirend-kiszolgáló (NPS) beállításai határozzák meg, kapcsolódhat-e egy adott felhasználó vagy sem:

X

### Új hálózati házirend

#### Hozzáférési engedély megadása

Annak konfigurálása, hogy megadni vagy megtagadni kívánja-e a hálózati hozzáférést, ha a kapcsolatkérelem megfelel ennek a házirendnek.

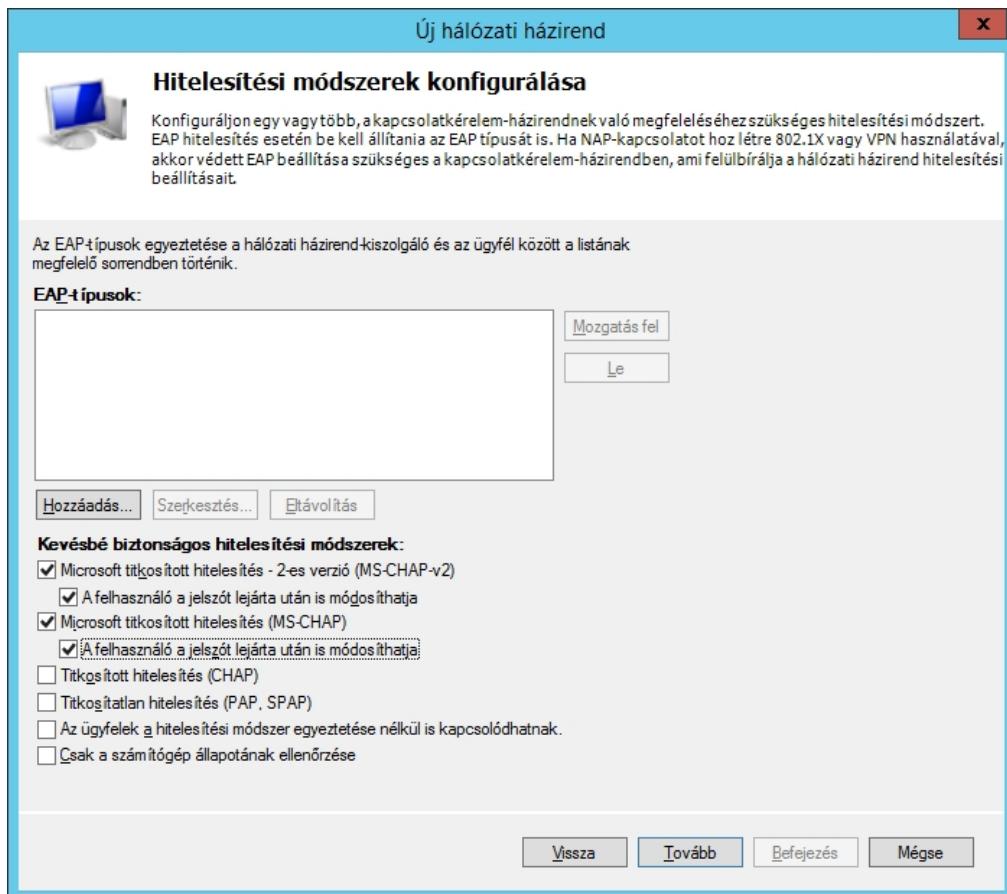
**Hozzáférés engedélyezve**  
A hozzáférés engedélyezése, ha az ügyfél kapcsolódási kísérletei megfelelnek a házirend feltételeinek.

**Hozzáférés megtagadva**  
A hozzáférés megtagadása, ha az ügyfél kapcsolódási kísérletei megfelelnek a házirend feltételeinek.

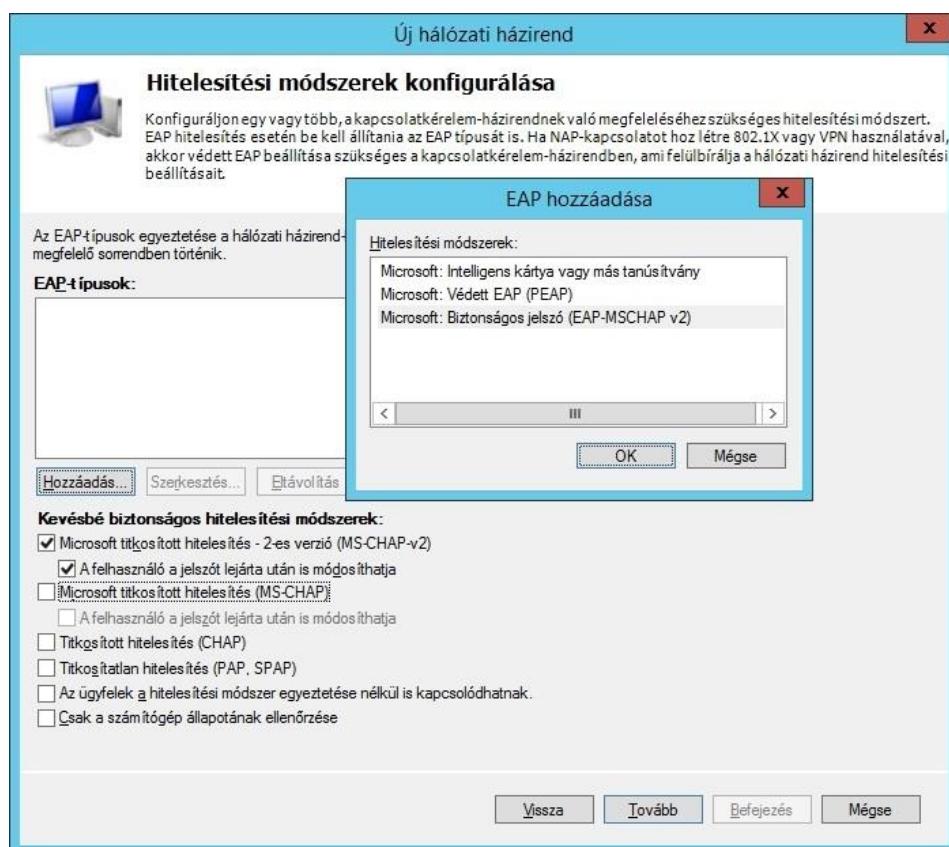
**A hozzáférést a felhasználói betárcsázás tulajdonságai határozzák meg (amelyek felülírják az NPS-házirendet)**  
A hozzáférés engedélyezése/megtadáása a betárcsázás tulajdonságai szerint, ha a kapcsolódási kísérlet megfelel a házirend feltételeinek.

Vissza Tovább Befejezés Mégse

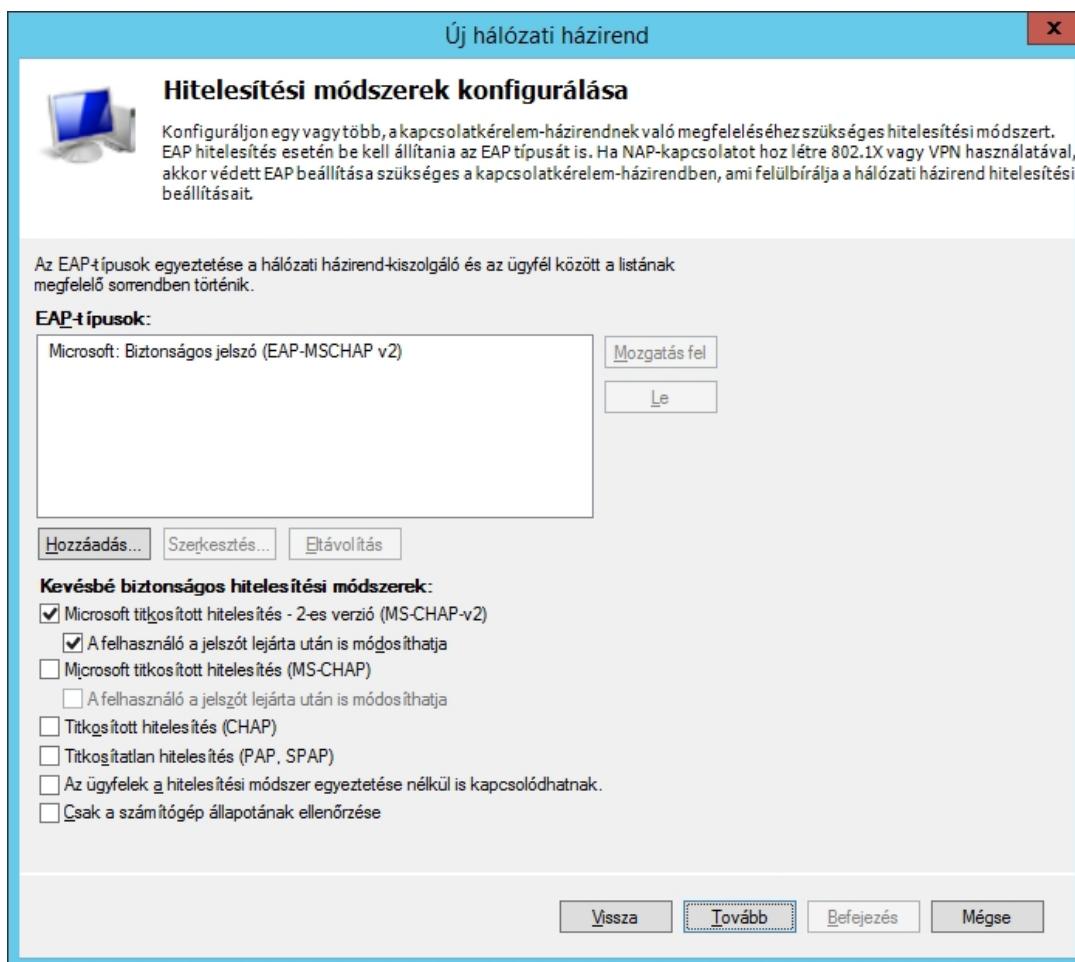
Hitelesítési módszerek közül távolítsuk el a régebbi (MS-CHAP) hitelesítést:



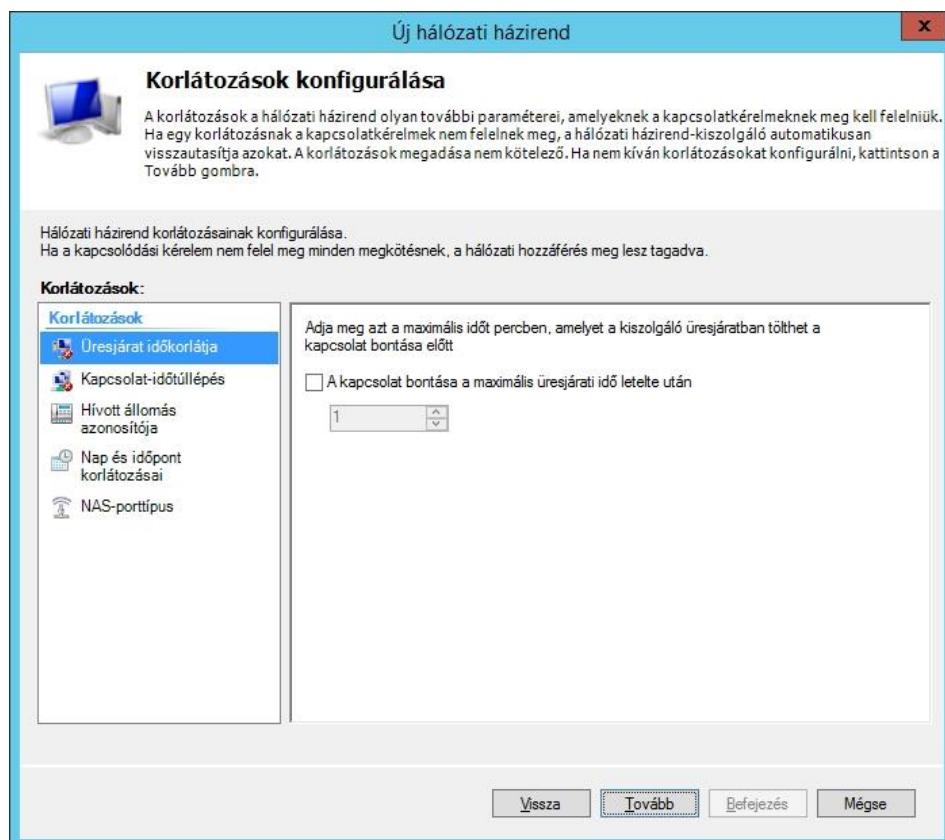
Adjuk hozzá a megbízhatóbb EAP-MSCHAPv2 hitelesítési módszert:



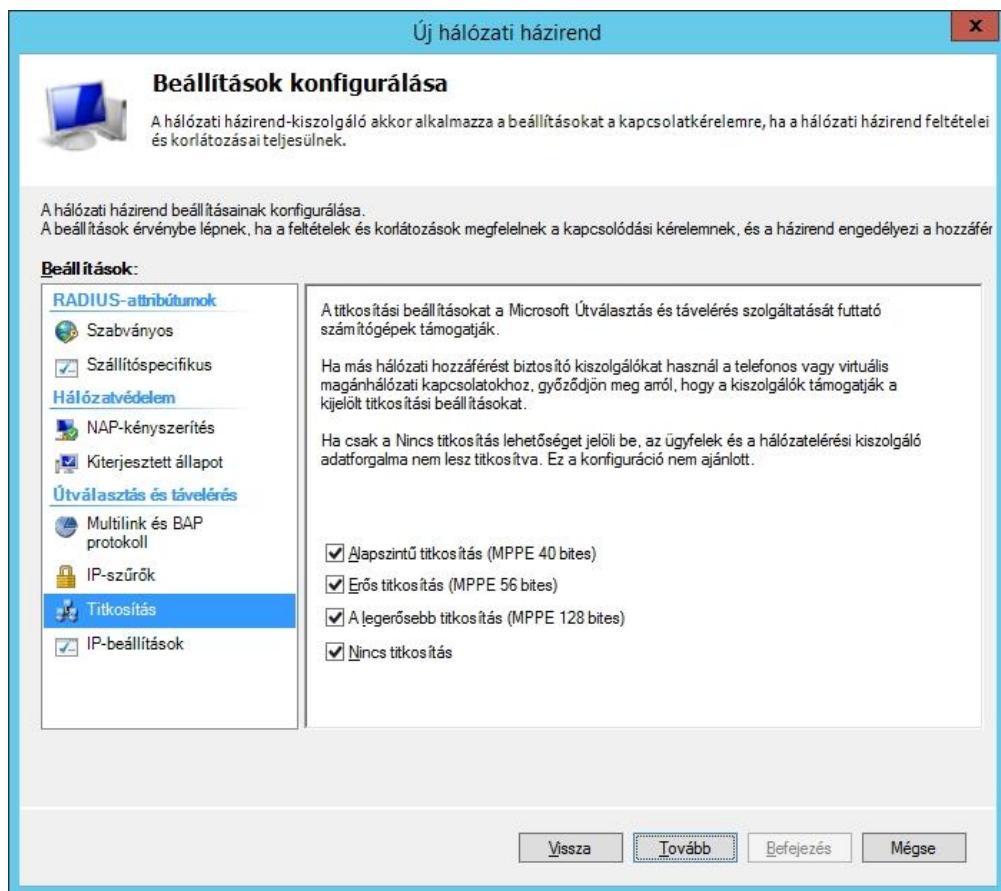
A felhasználó által használni kívánt hitelesítési módszernek az általunk itt megadott típusok egyikével kell egyeznie:



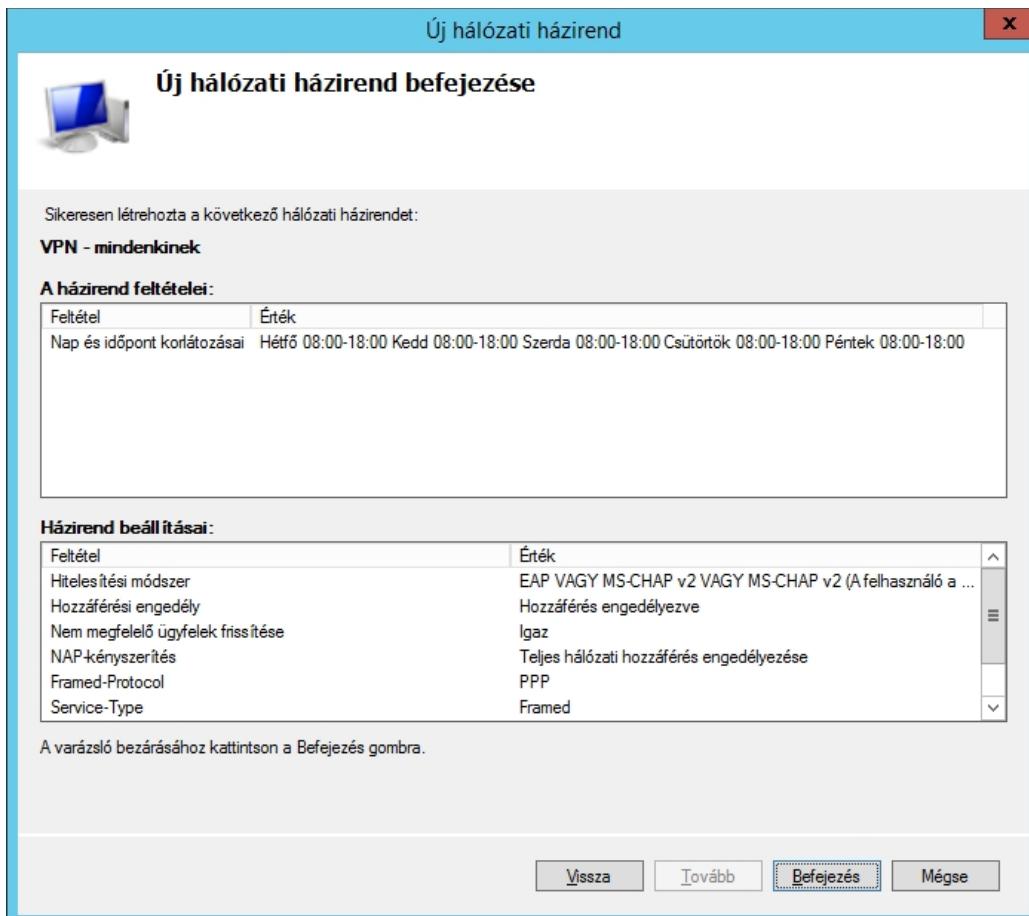
A Korlátozások között szerepel pl. a tétlensi idő: amennyiben nincs használatban az általunk megadott ideig a VPN kapcsolat, megszakítjuk. De meghatározhatjuk a VPN vonal maximális használati időtartamát is:



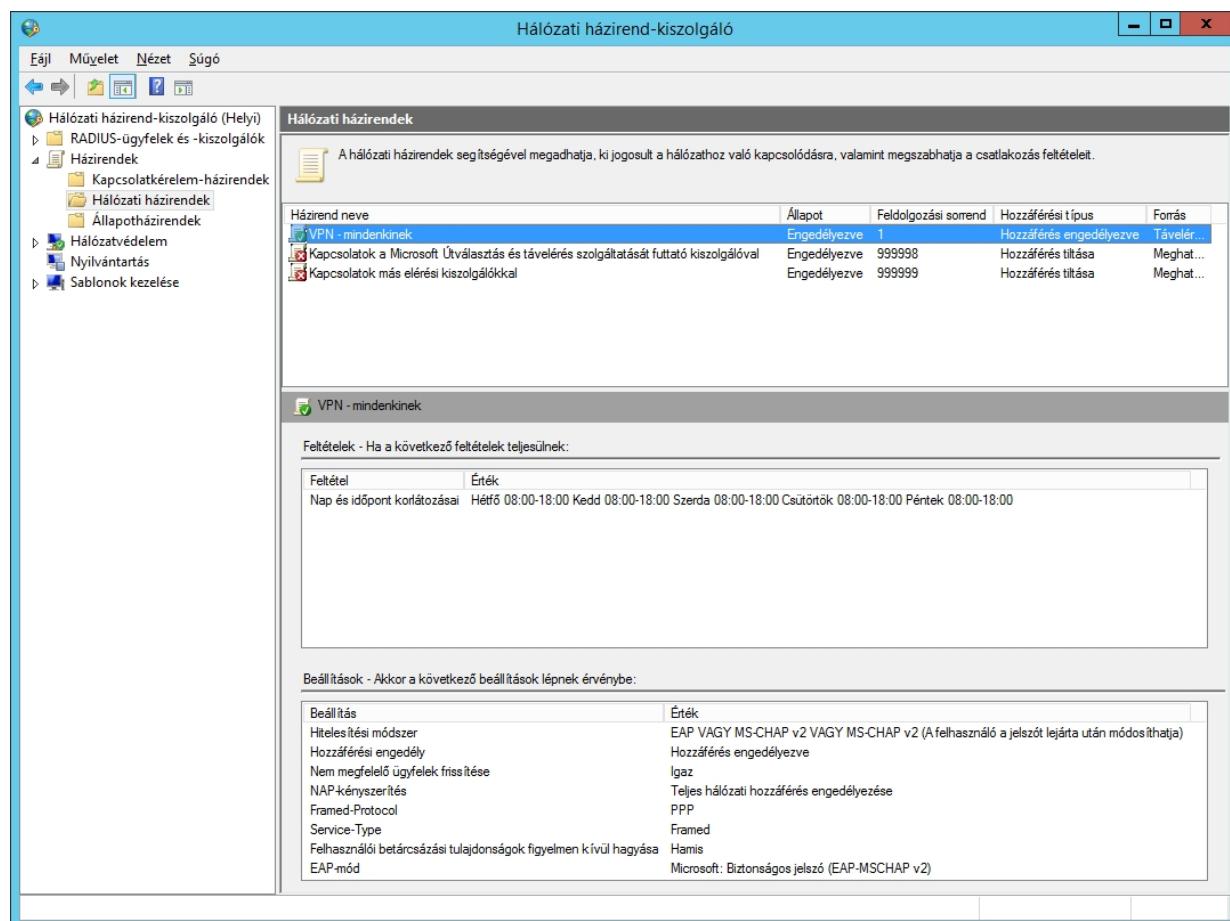
Megadhatunk a kapcsolatra érvényes beállításokat, pl. az elfogadott titkosítási módokat, a titkosítás nélküli kapcsolattól a legerősebb titkosításig. Kliens oldalon is csak az itt elfogadott beállításokat használhatjuk!



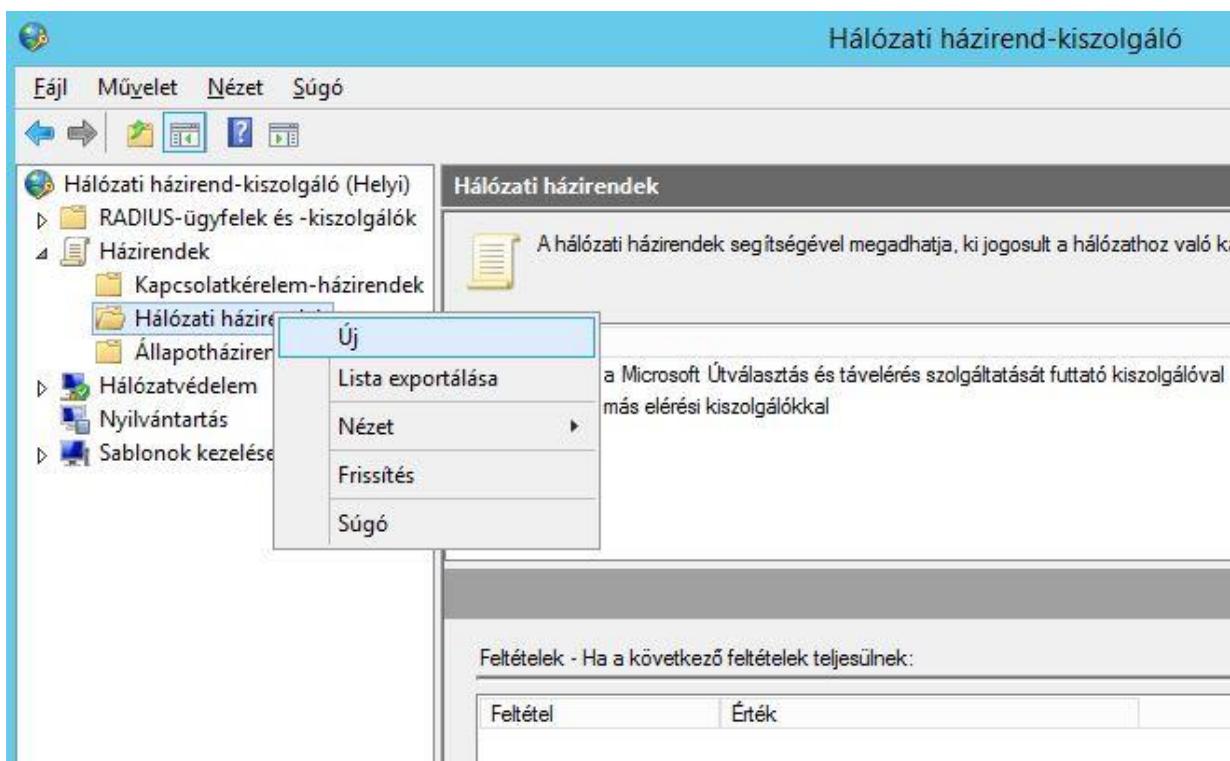
Elkészült a házirendünk 😊



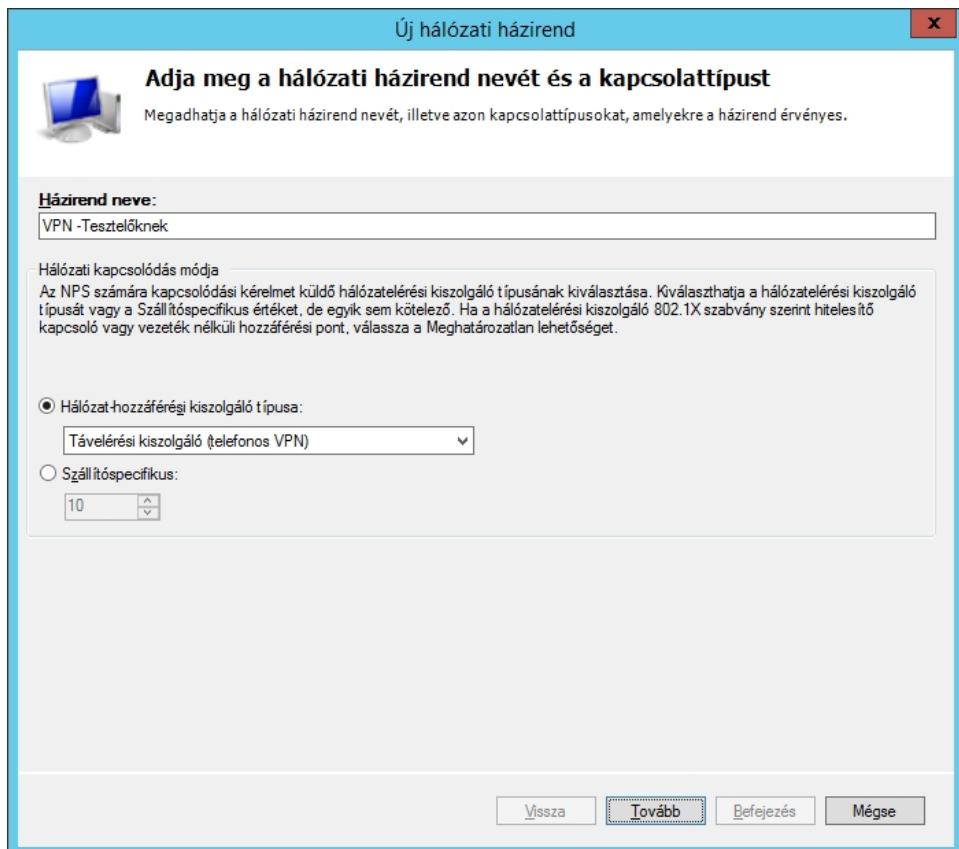
Figyeljük meg, a tiltó házirendekkel ellentétben ez a házirend 1-es sorszámot kapott. Először ezt értékeli a rendszer:



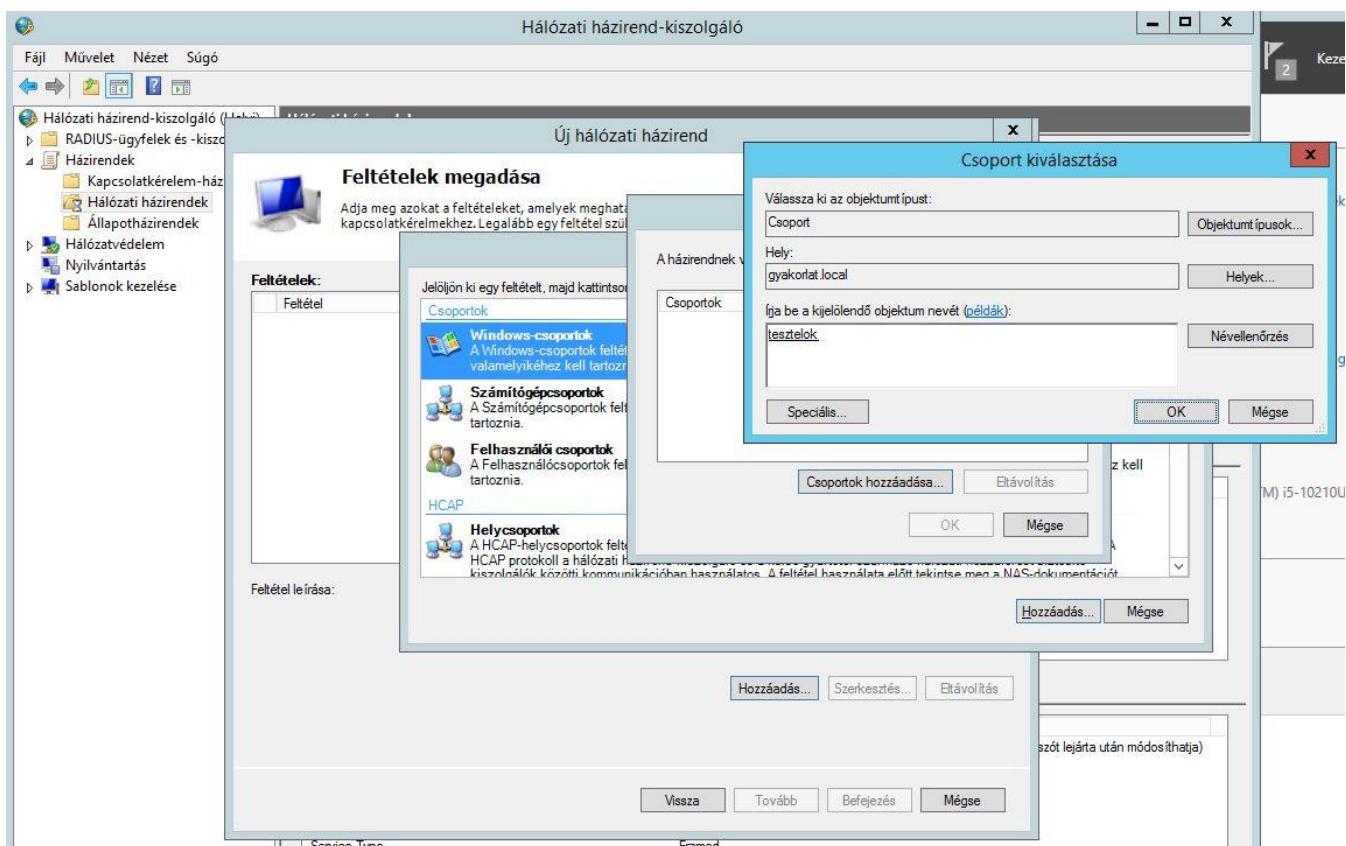
Hozzunk létre egy új hálózati házirendet a **Tesztelők** csoportunknak, **csak L2TP protokoll** és **EAP hitelesítési módszer** legyen használható



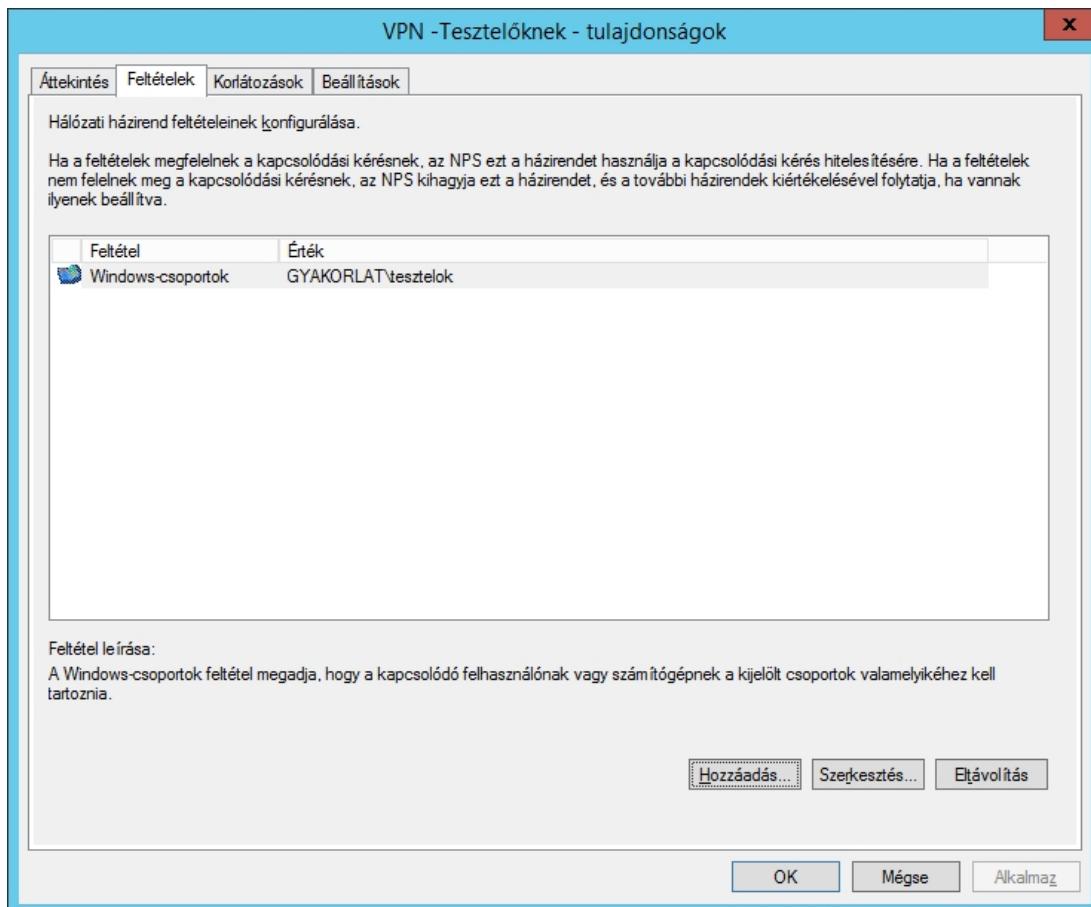
Adjunk nevet a házirendünknek és válasszunk hálózat-hozzáférési típust:



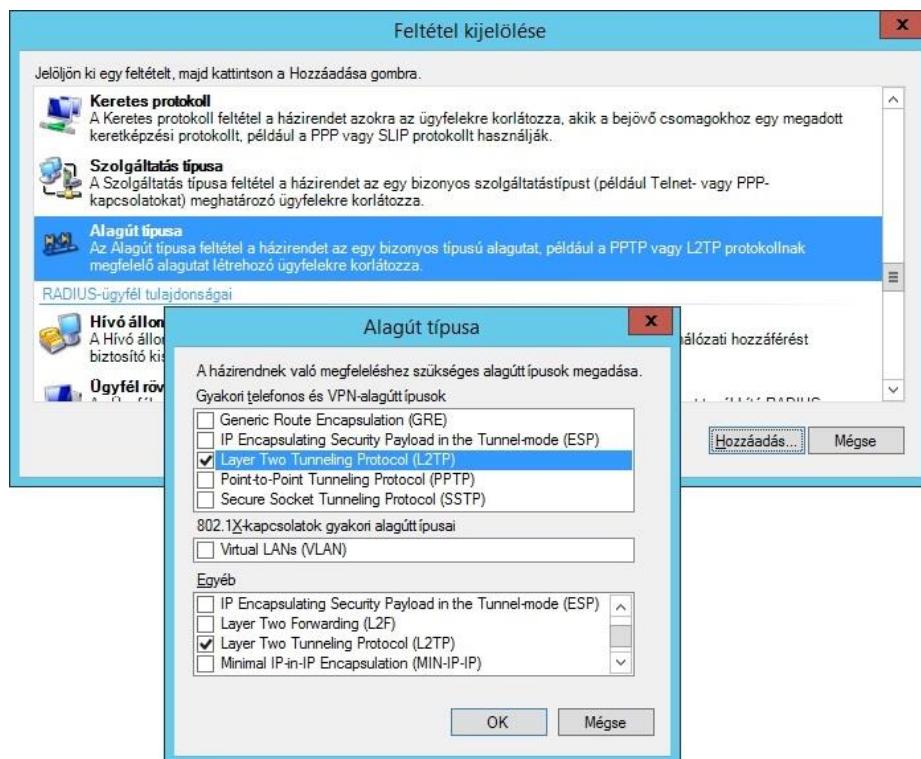
Feltételként adjuk meg Windows csoportunkat: **tesztelok**



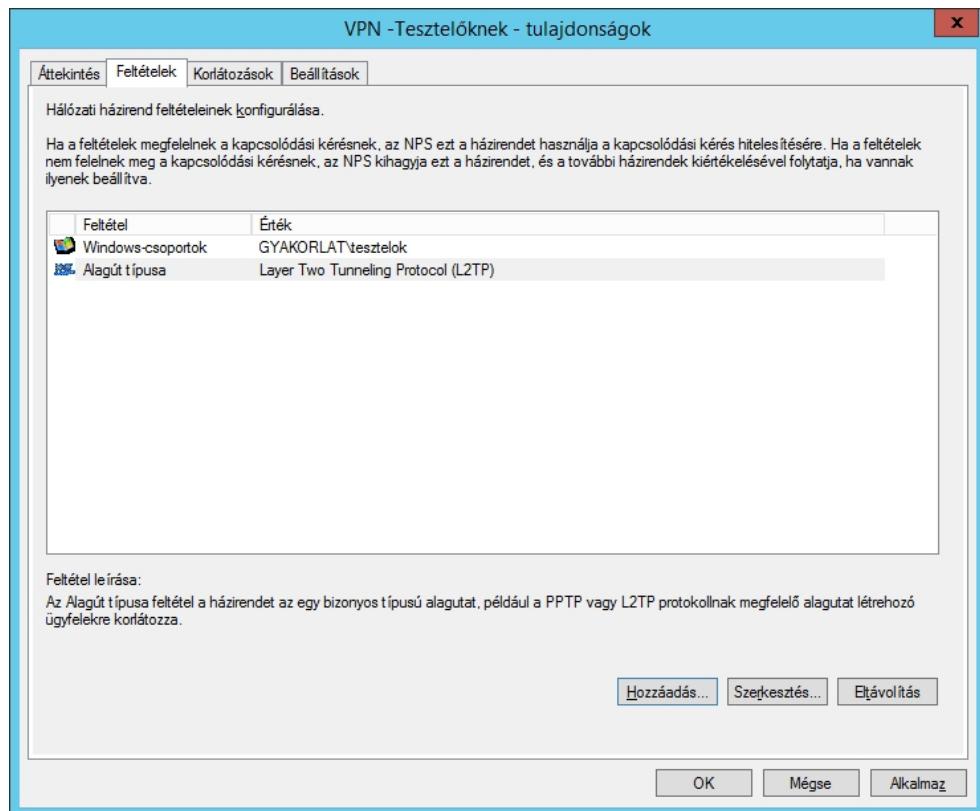
Azonban most vegyük fel további feltételt:



Adjuk meg az **Alagút típusát**, esetünkben ez L2TP protokoll használatát jelenti:

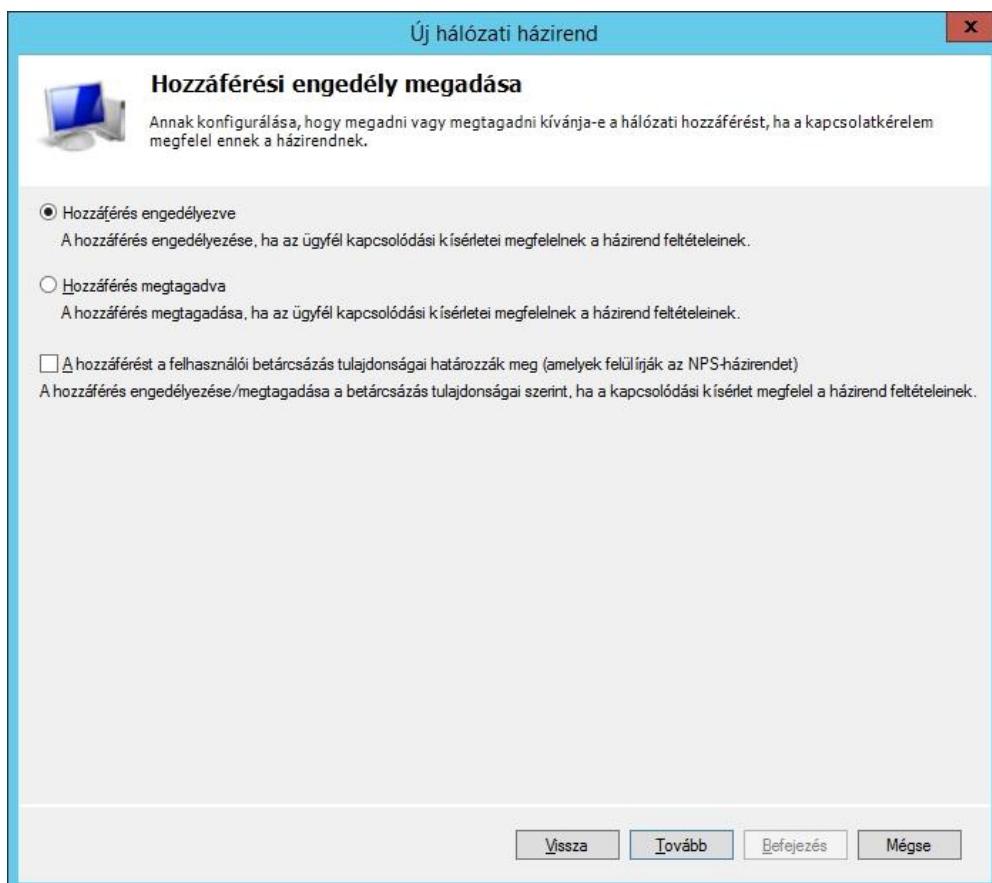


Feltételek megadva:

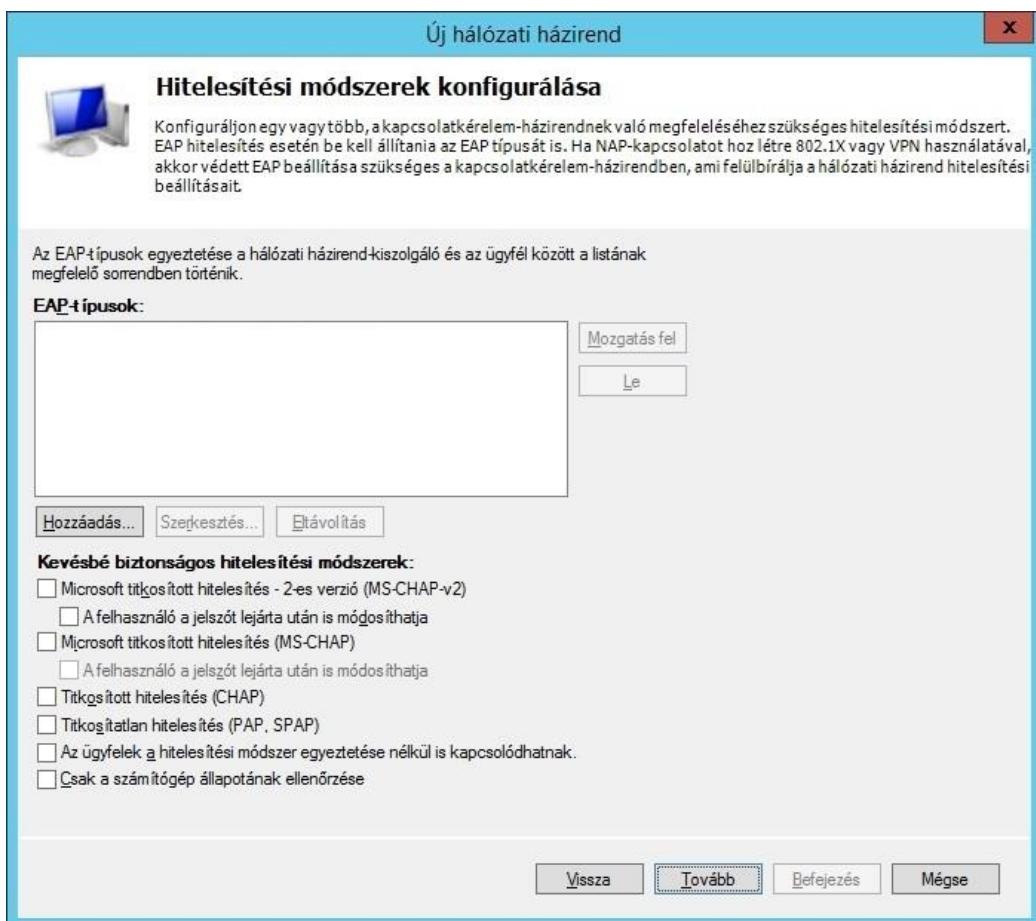


Engedélyező házirendet hozunk létre!

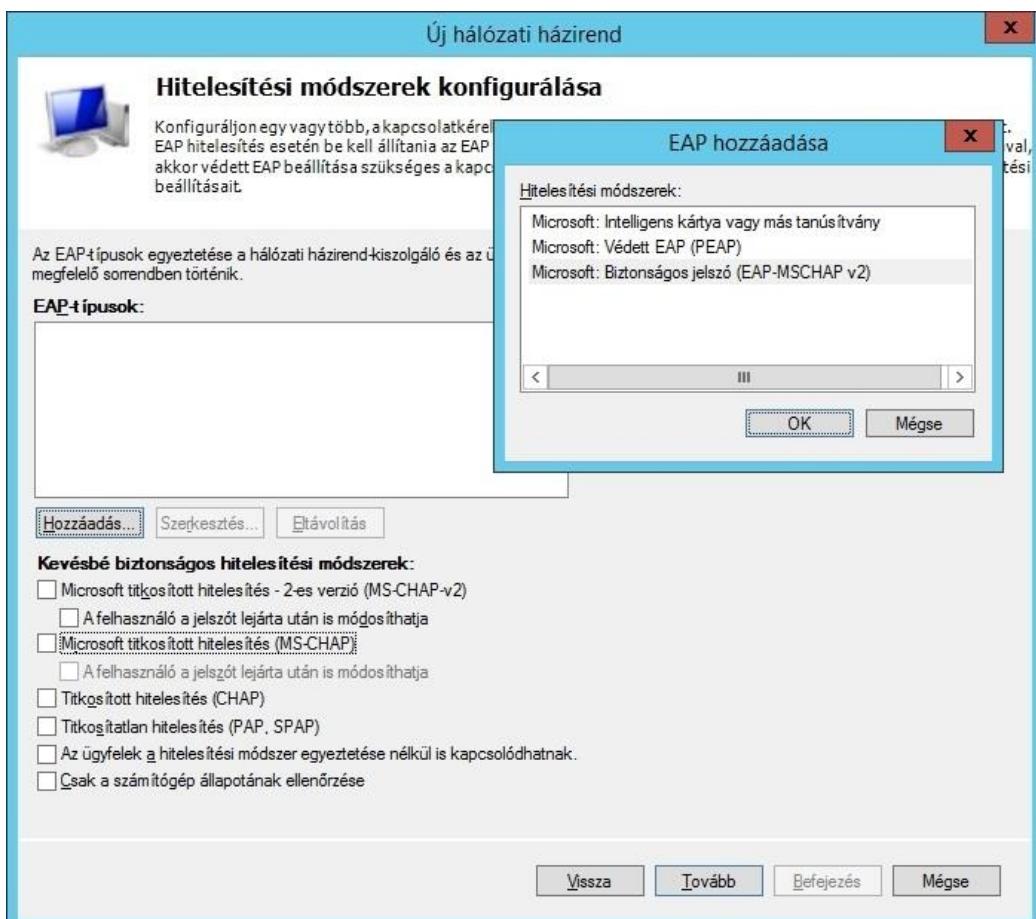
A jelölő négyzet üresen hagyásával biztosítjuk, hogy a Hálózati házirend-kiszolgáló (NPS) beállításai határozzák meg, kapcsolódhat-e egy adott felhasználó vagy sem. A felhasználói adatlap / behívás lapon található beállításokat így figyelmen kívül hagyja:



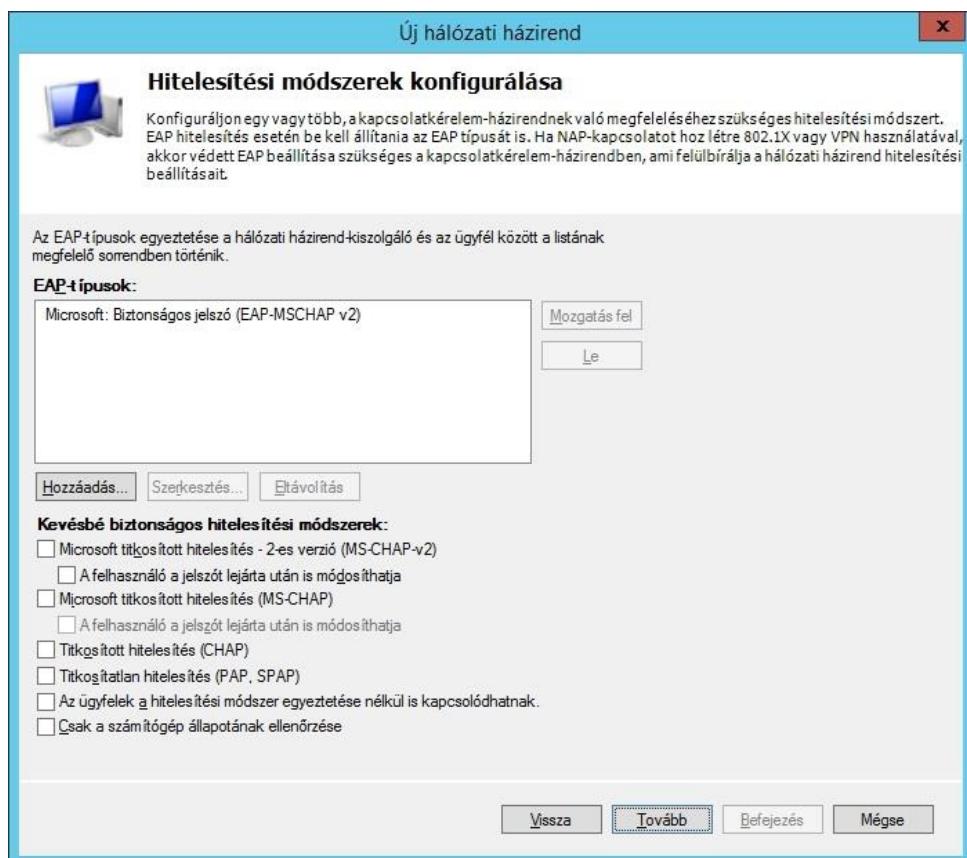
Ebben az esetben csak az EAP-típusokat fogadjuk el a klienstől: Töröljük a kevésbé biztonságos módszereket:



Adjuk hozzá az EAP-MSCHAPv2 hitelesítési módszert:



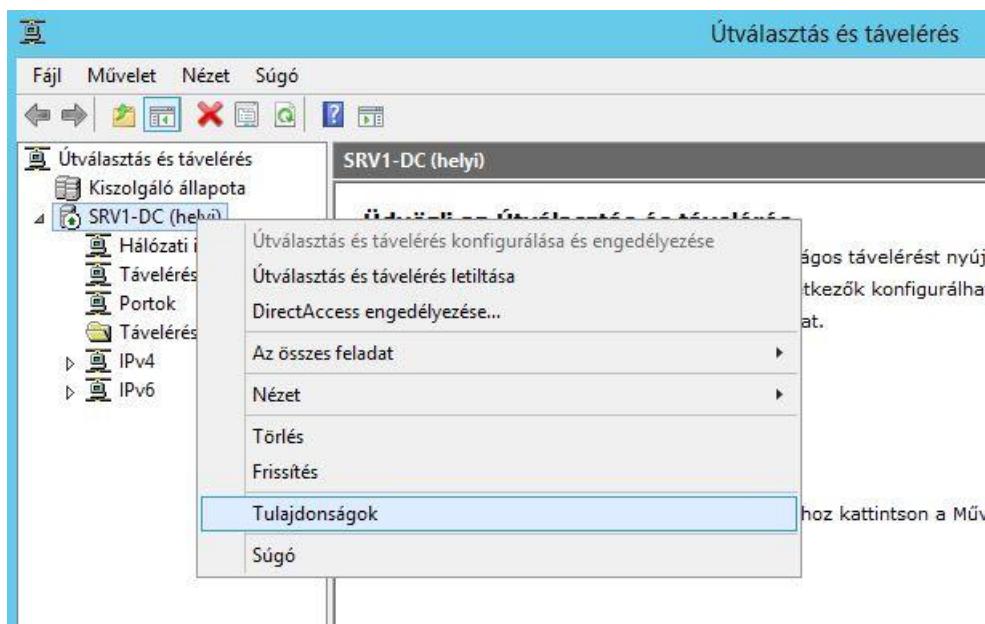
A felhasználó által használni kívánt hitelesítési módszernek az általunk itt megadott típussal meg kell egyeznie:



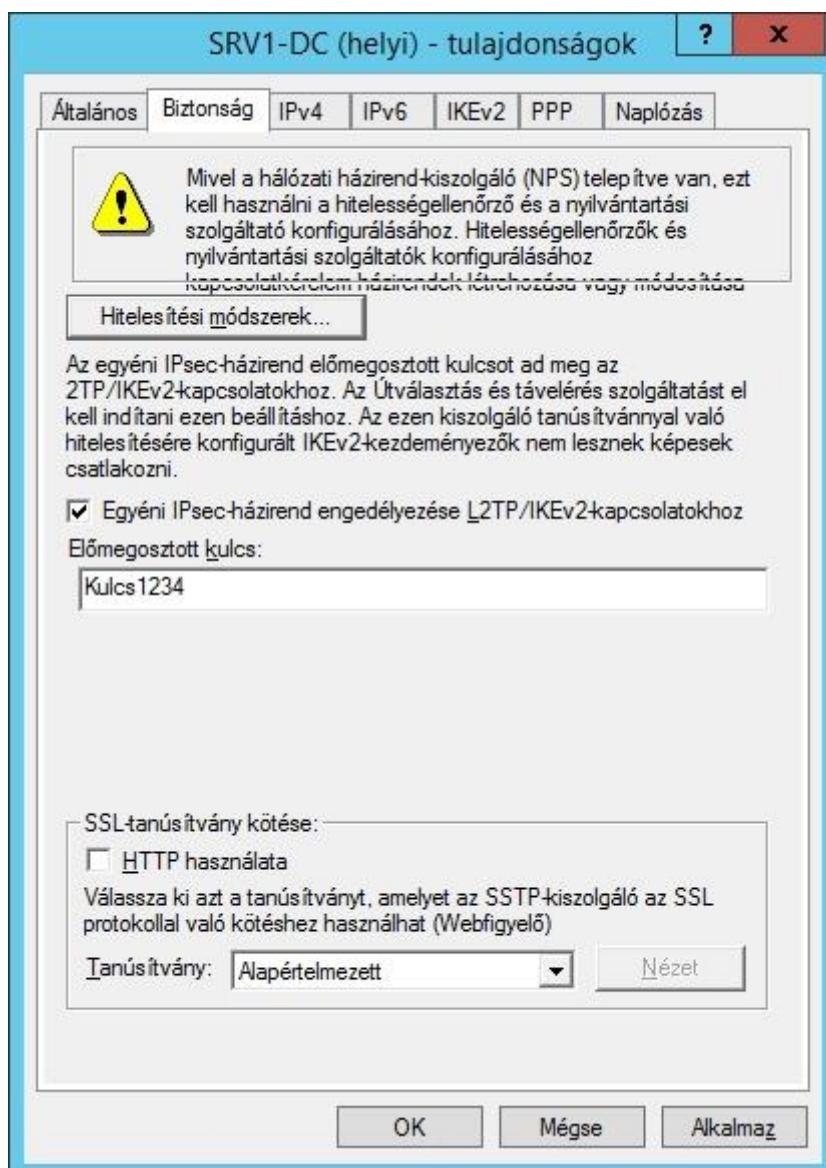
Itt nem adtunk meg **korlátozást** és egyéb **beállítást** sem.

Elkészült a hálózati házirendünk:

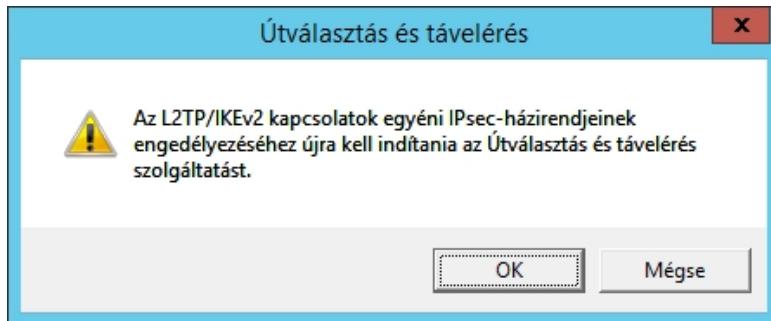
Konfiguráljuk a **Távelérés kiszolgálót (RAS)**, hogy kapcsolódhassunk **L2TP** protokollt használva is:  
(ez esetben előmegosztott kulcsot használva)



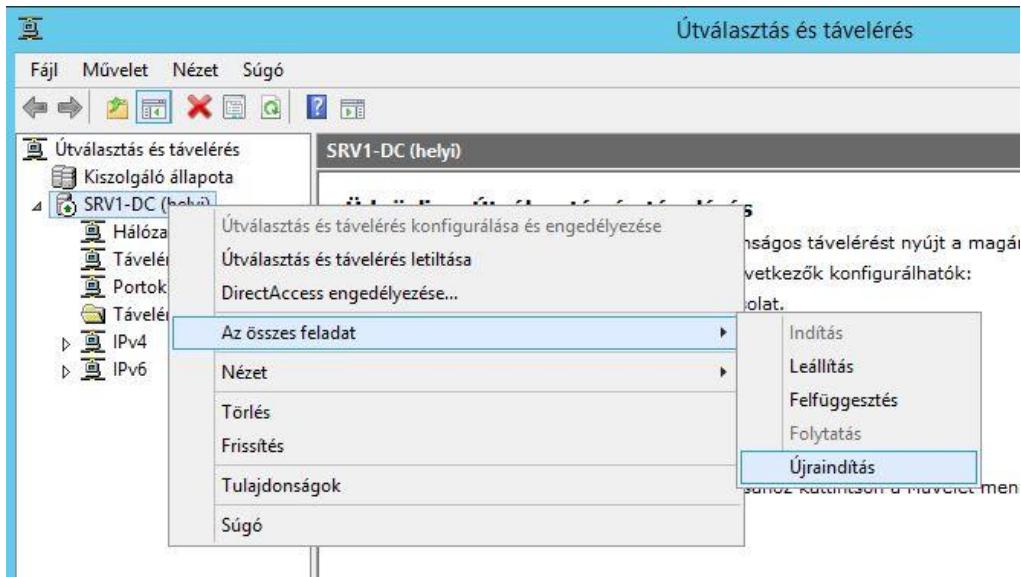
A Távelérés kiszolgáló tulajdonságait megnyitva, a Biztonság fülön az Egyéni IPsec-házirend engedélyezése L2TP/IKEv2-kapcsolatokhoz jelölőnégyzet kiválasztásával megadhatjuk az Előmegosztott Kulcsot:



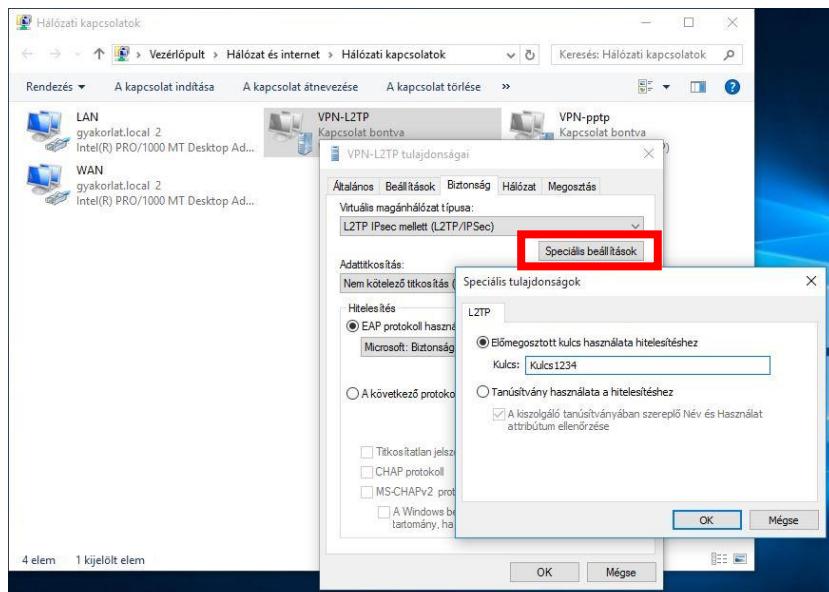
A Távelérés kiszolgálót újra kell indítanunk, **csak figyelmeztet!**



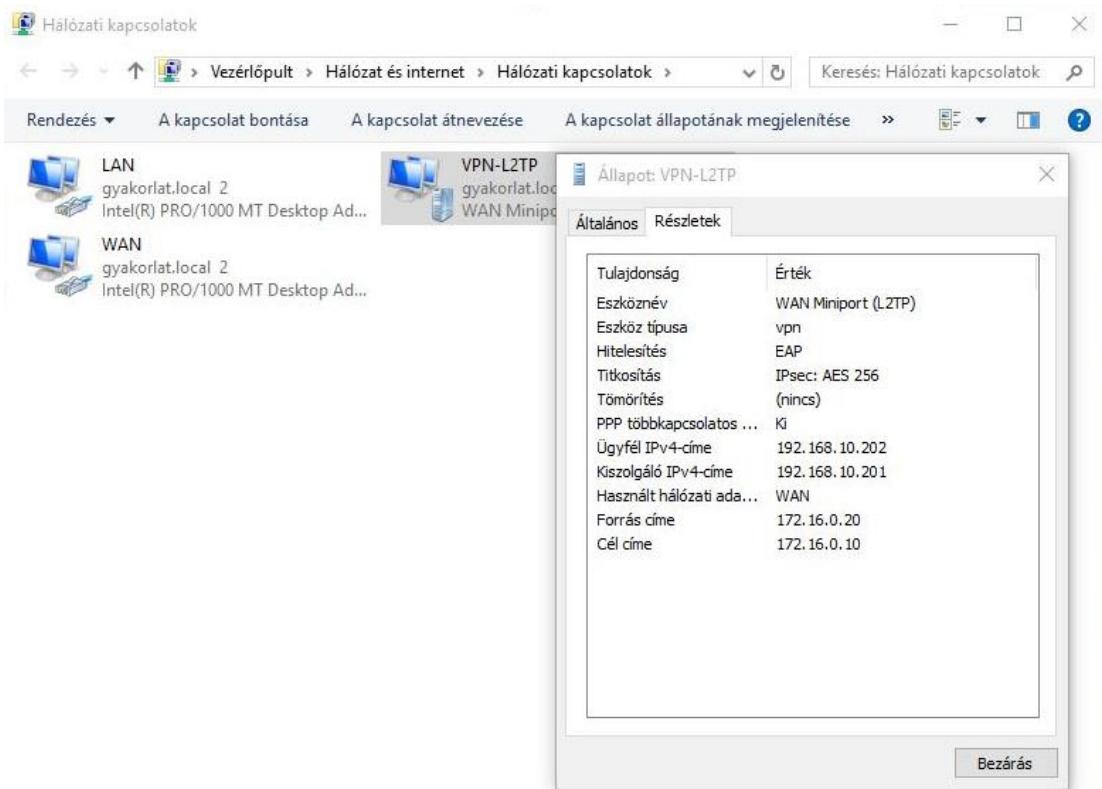
**Indítsuk újra a Távelérés kiszolgálót: újraindítás nélkül nem működik az L2TP!**



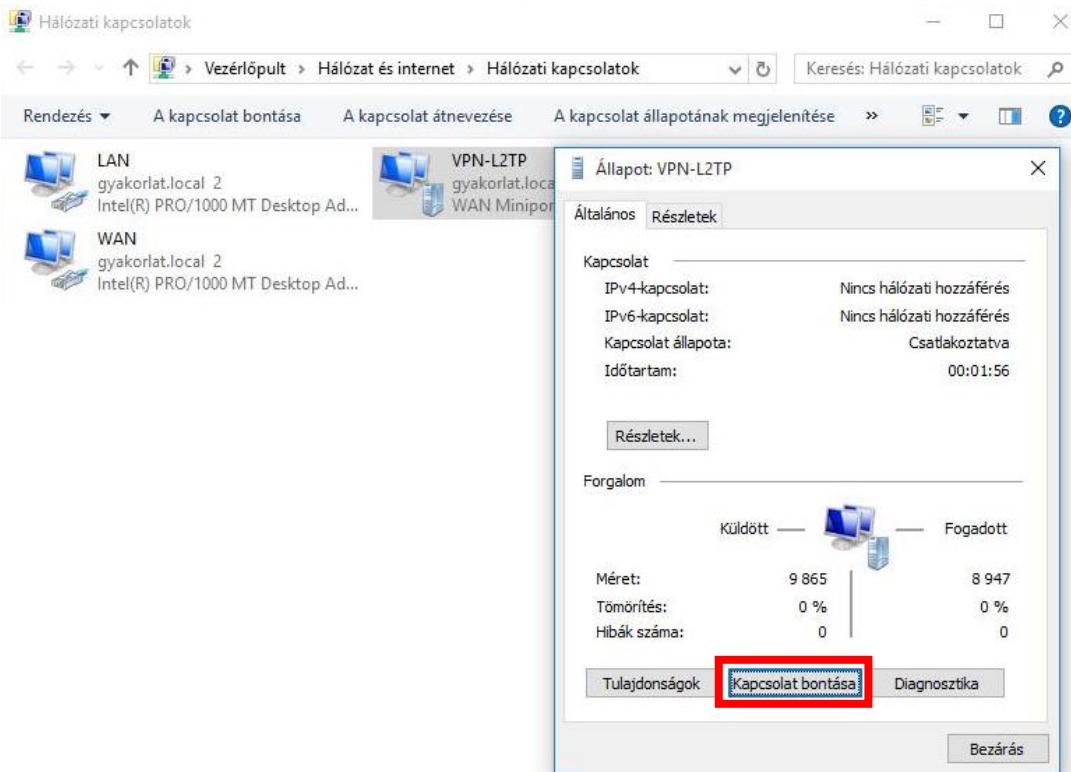
A kliensen (Windows 10) a **PPTP** protokoll esetén megismert módon kell létrehozzuk a **VPN-L2TP** kapcsolatot, aztán a kapcsolat tulajdonságait az alábbiak szerint módosítsuk:



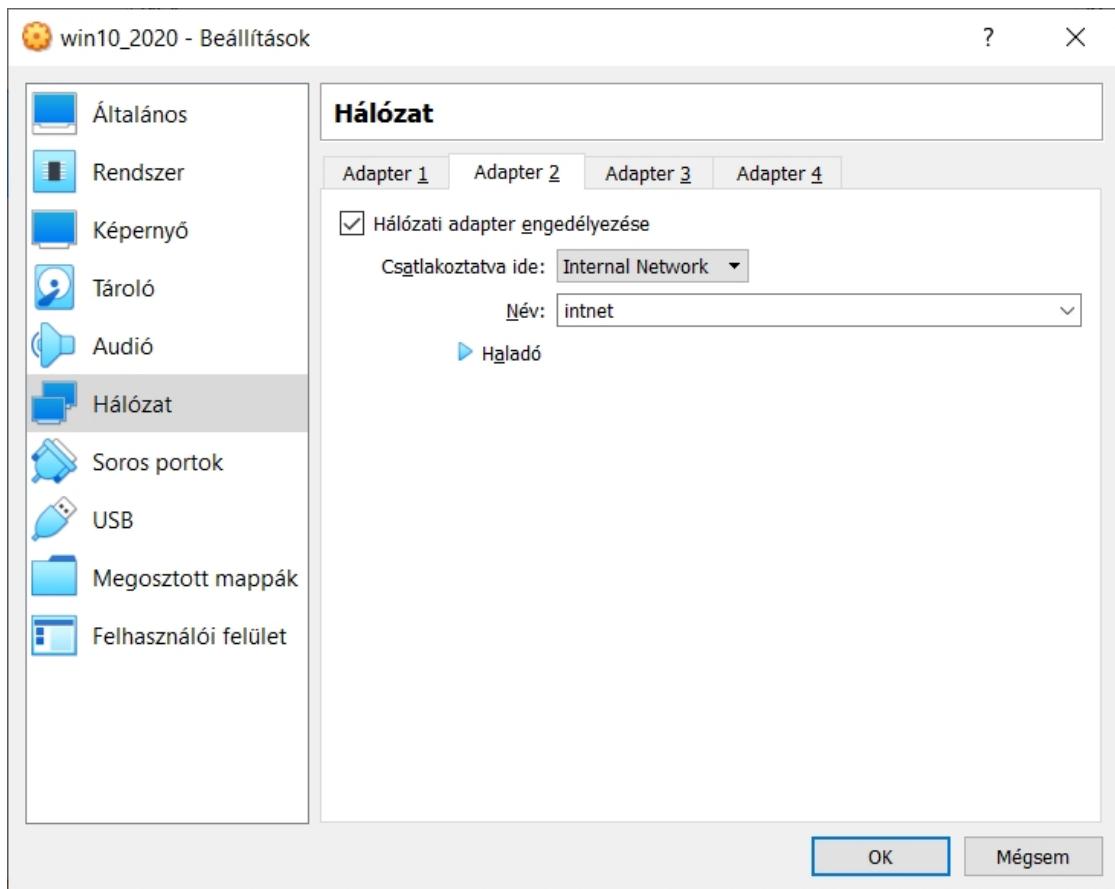
A létrejött VPN kapcsolatunk ellenőrzésére nézzük meg a kapcsolat állapotát, ott a részletek fülre kattintva láthatjuk: **L2TP protokollt** használ és **EAP hitelesítési módszert, titkosított kapcsolaton** keresztül.



A VPN kapcsolatunkat bonthatjuk az Állapot lapon kezdeményezve is:

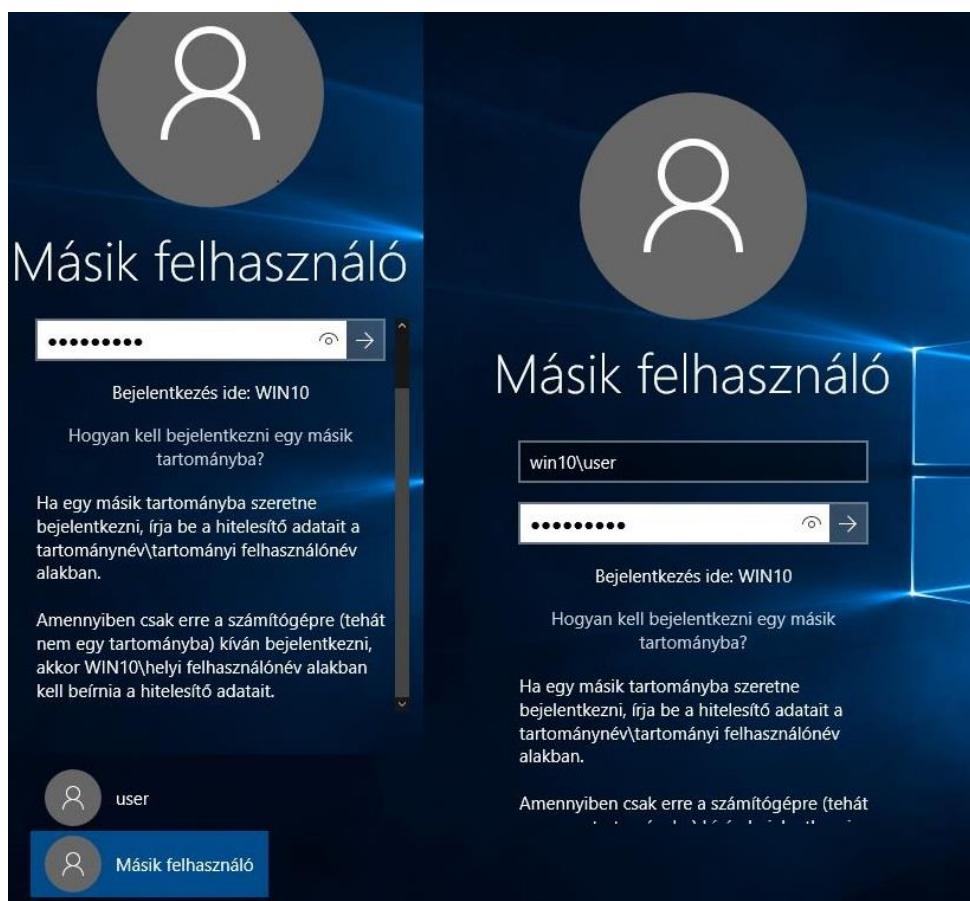


A kliens géphez is adjunk hozzá egy második hálózati kártyát (Internal network / belső csatoló):

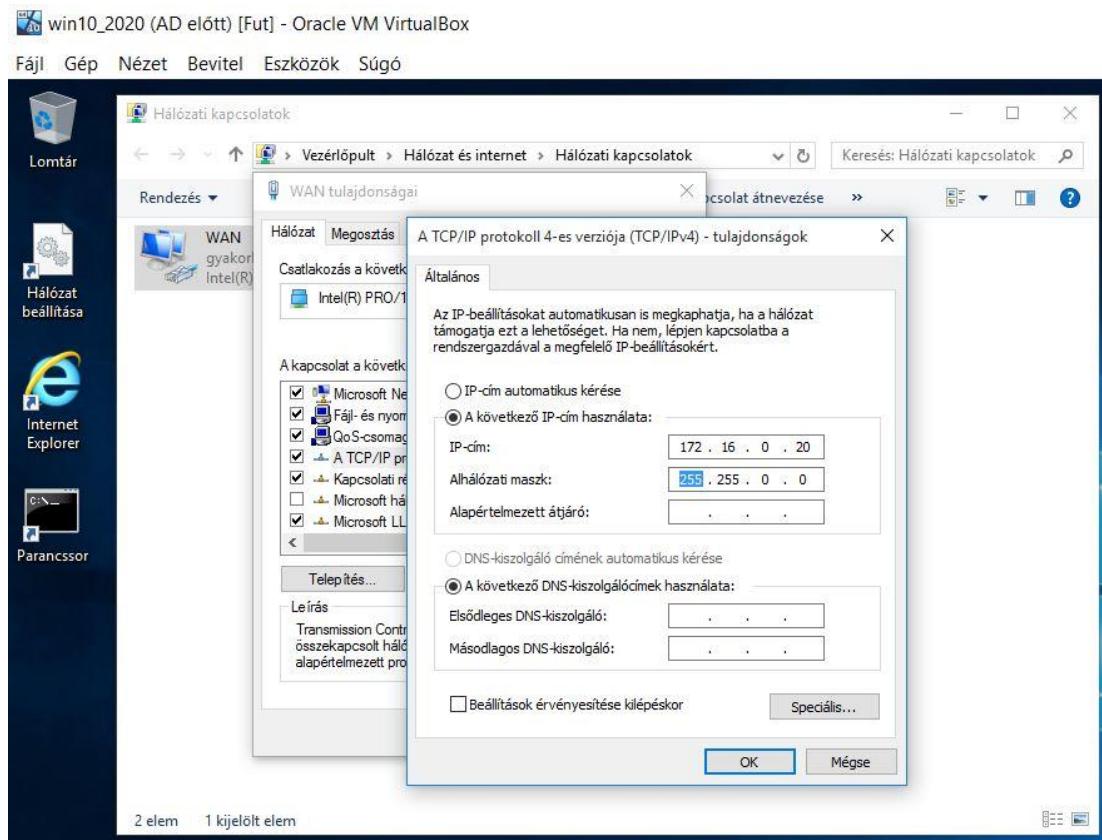


A beállításokat helyi rendszergazda jogú felhasználóként végezhetjük el

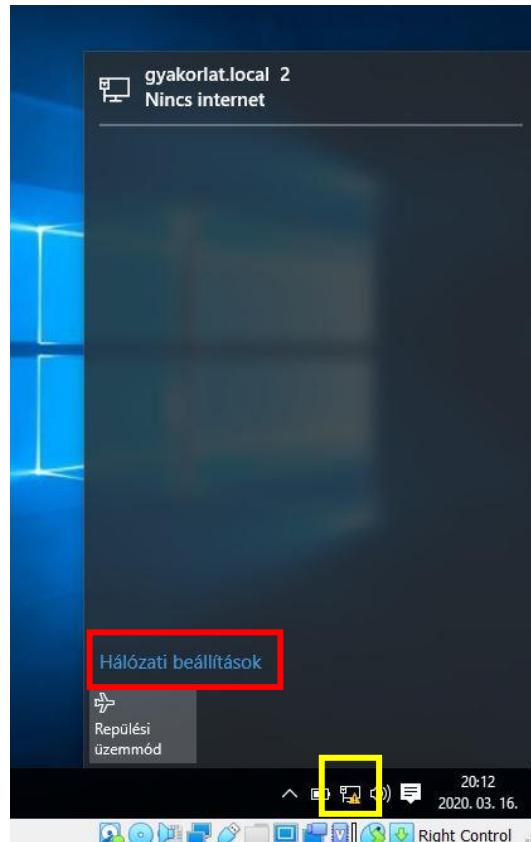
(pl. a telepítéskor megadott helyi felhasználói fiókot használva):



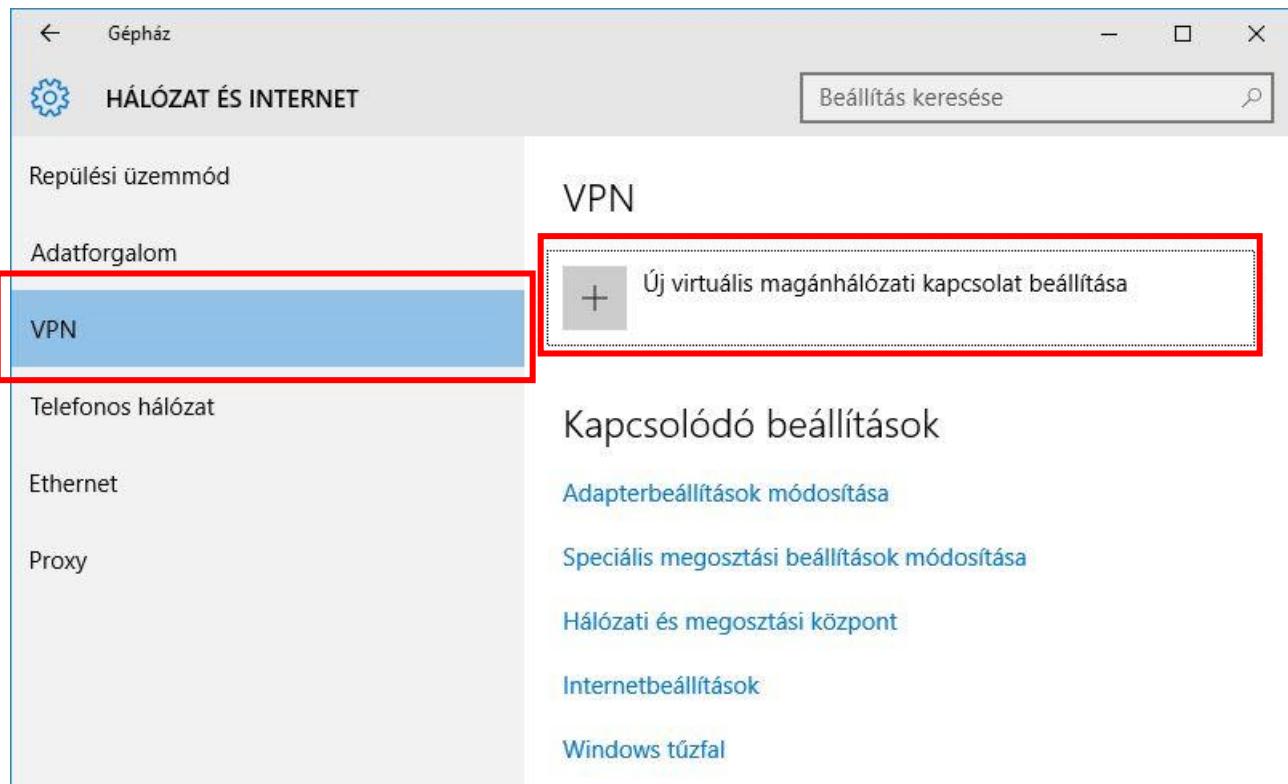
Állítsuk be a második hálózati kártya IP-címét és nevezzük át a könnyebb azonosításhoz:



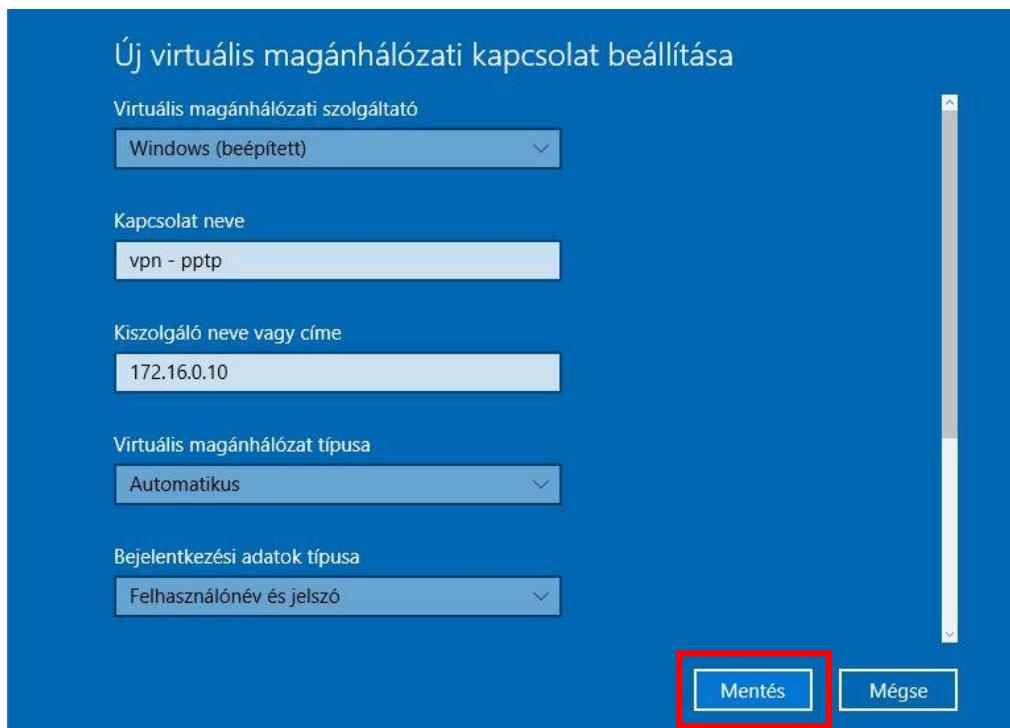
A VPN kapcsolatot létrehozhatjuk, ha a tálcán lévő Hálózatok ikonra kattintunk, majd a Hálózati beállításokat választjuk:



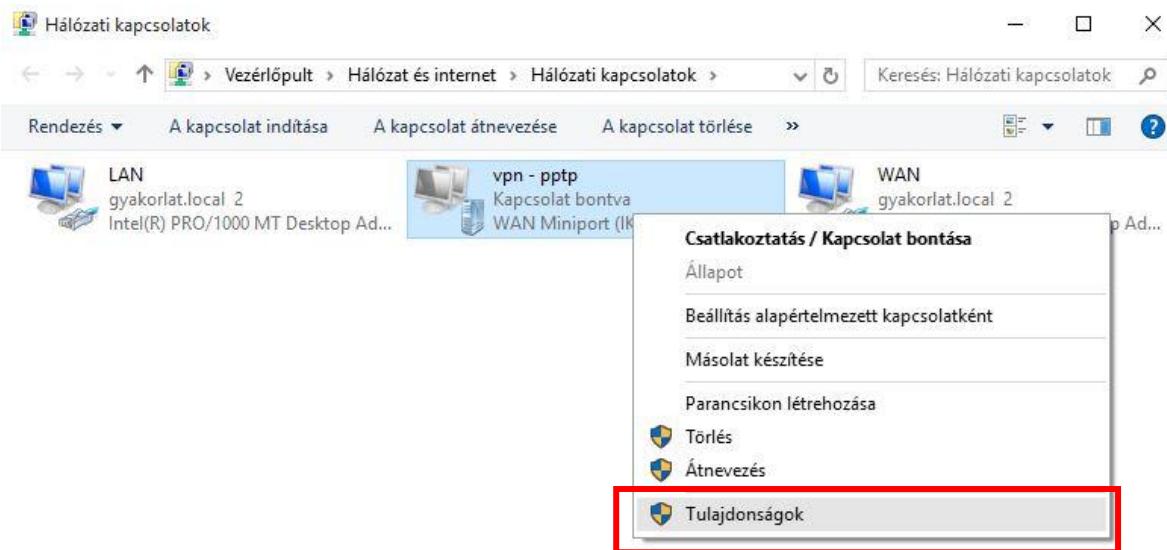
Jelöljük ki a VPN-t és egy Új magánhálózati kapcsolat beállítását válasszuk:



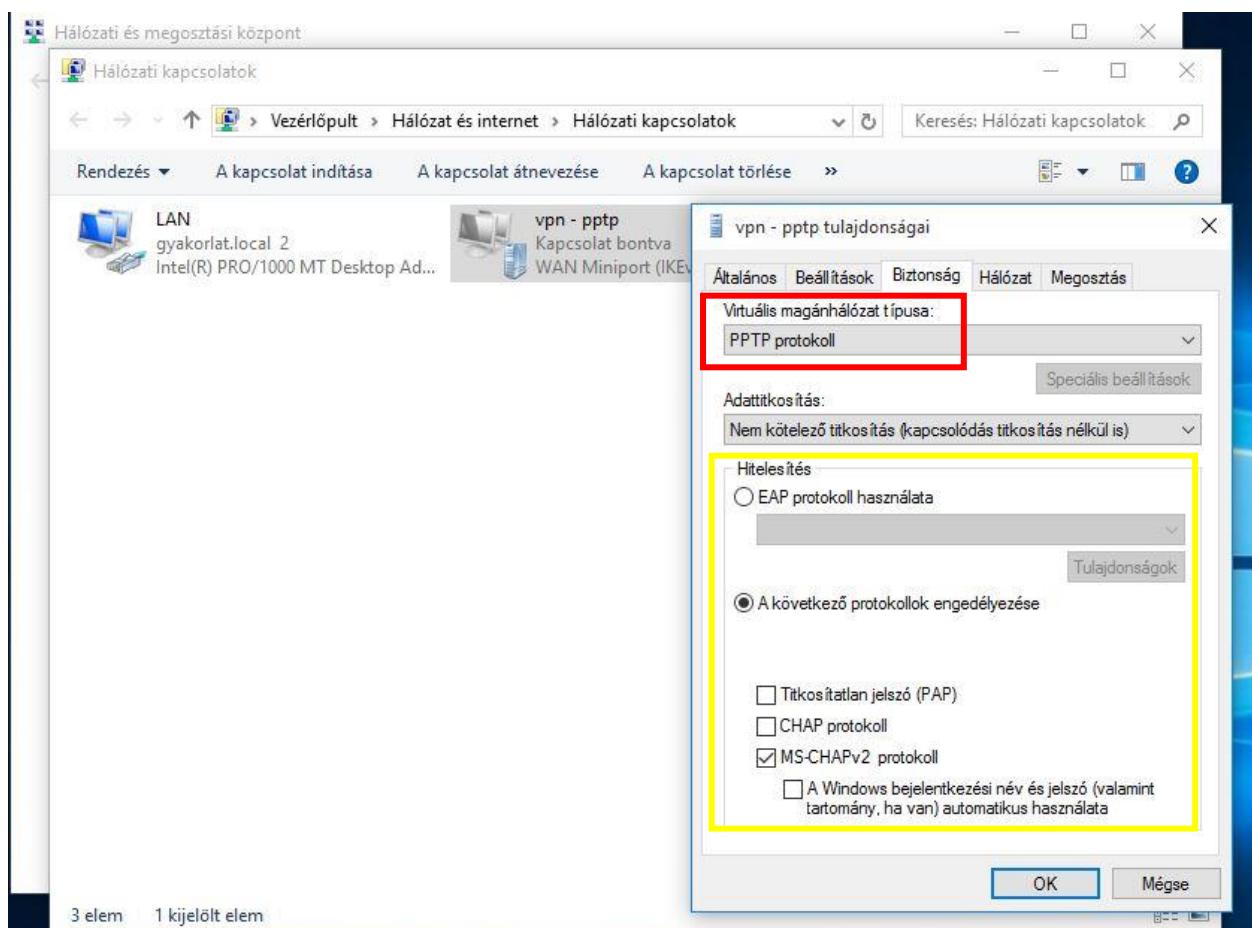
A beállítások végezzük az ábra szerint és mentsük el:



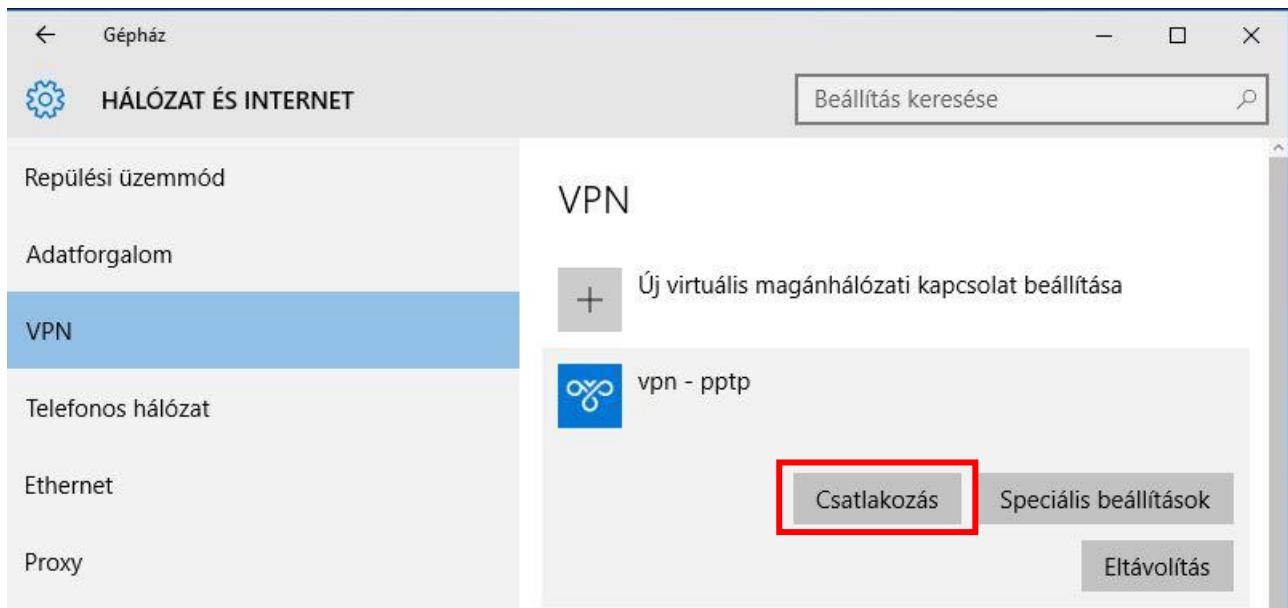
A hálózati kapcsolatok között létrejött új kapcsolatunk tulajdonságait hangoljuk:



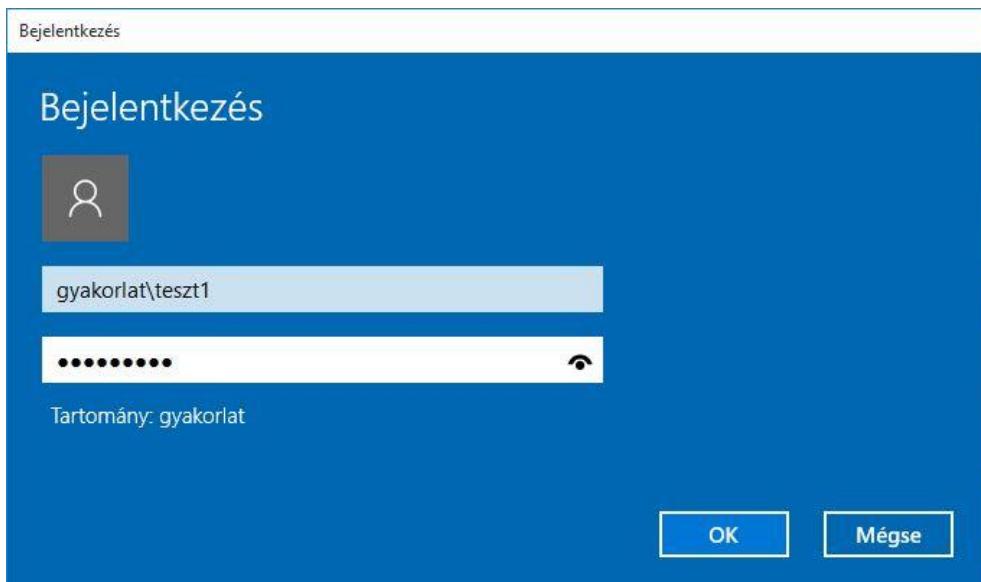
Állítsuk be a **virtuális magánhálózat típusát** és használni kívánt **hitelesítési protokollt**:



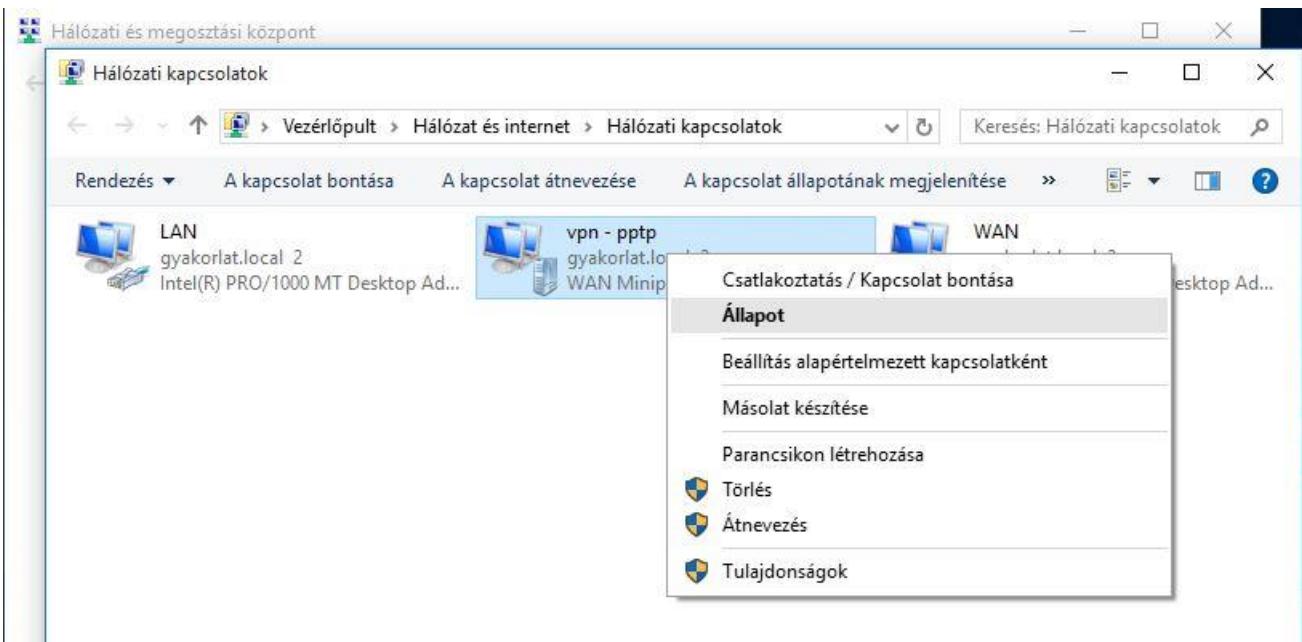
Teszteljük a létrejött kapcsolatunkat, csatlakozzunk a szerverhez:



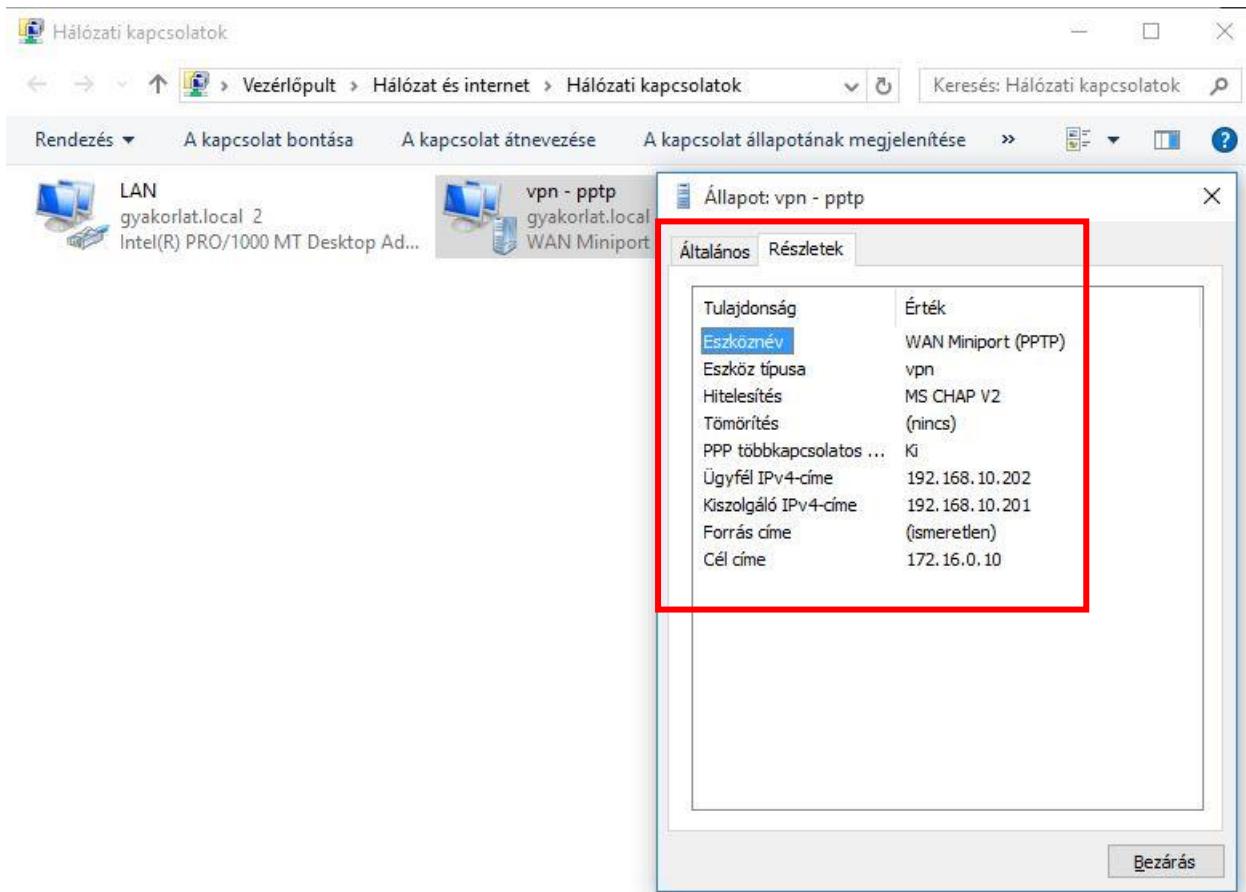
Adjuk meg a hitelesítési adatainkat (tartományi felhasználóként):



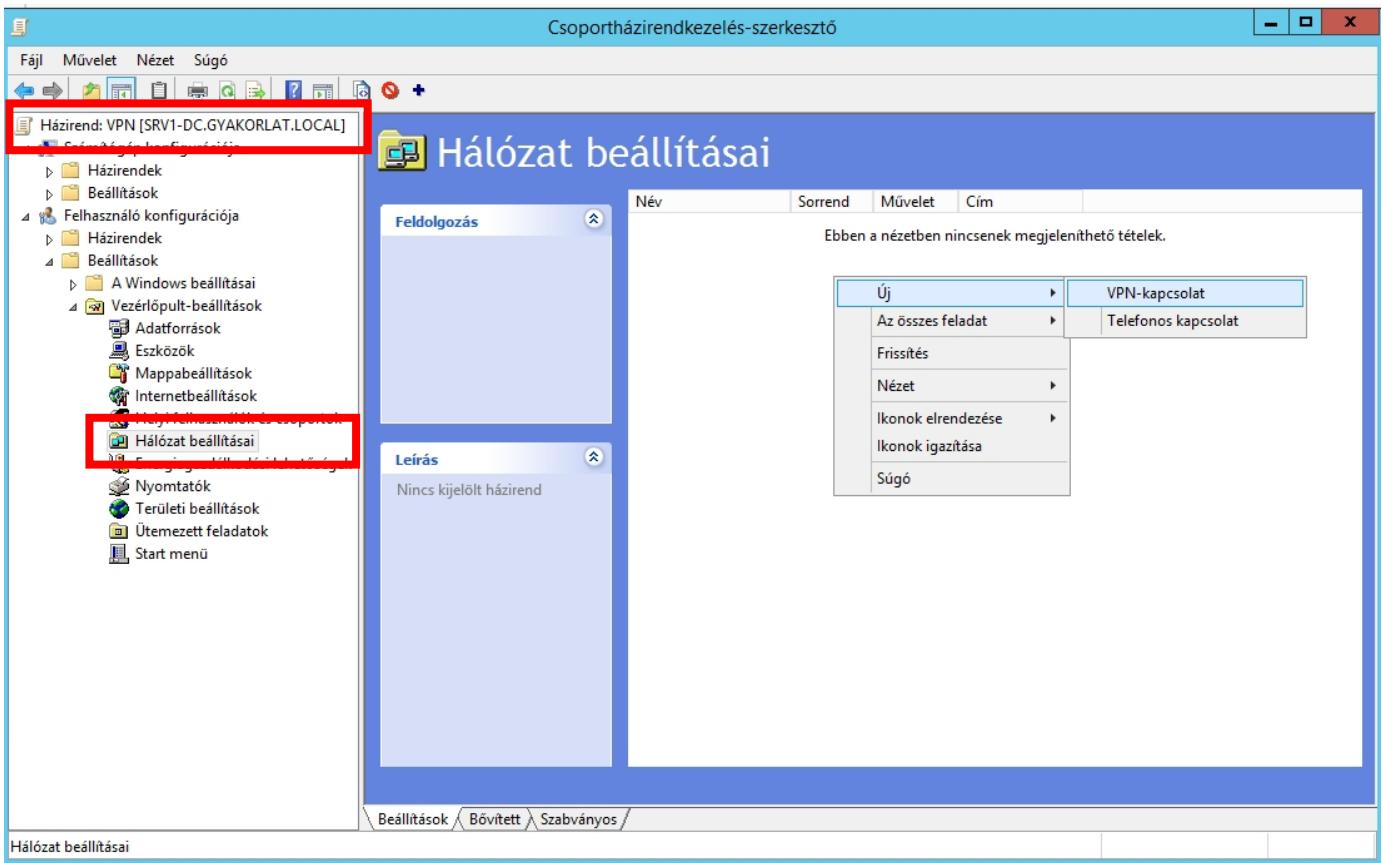
Ellenőrzésképpen, a kapcsolat állapotát lekérve...



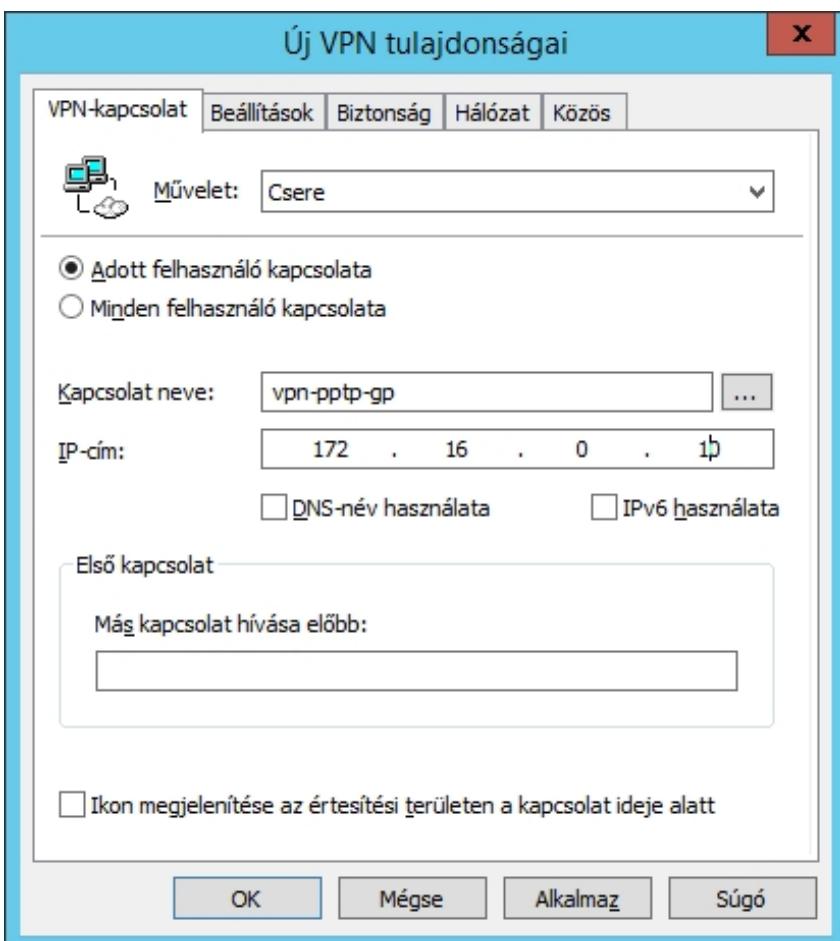
... részletek fülön láthatjuk a használt protokollokat és a kapott IP-címeket is:



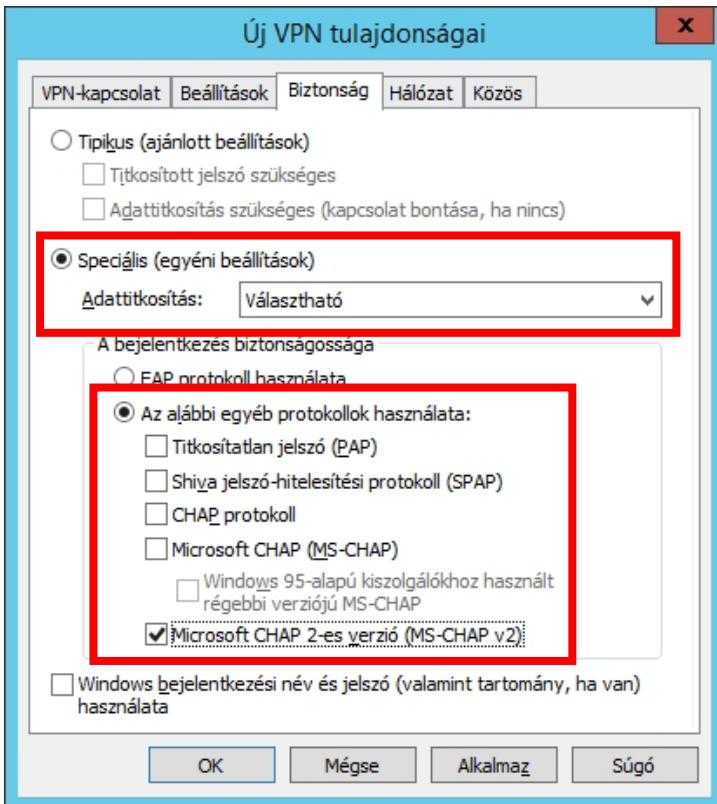
A **VPN** nevű szervezeti egységez rendeljünk egy új házirendet, nyissuk meg szerkesztésre és az ábrán látható helyen létrehozhatunk egy új VPN-kapcsolatot készítő házirend szabályt:



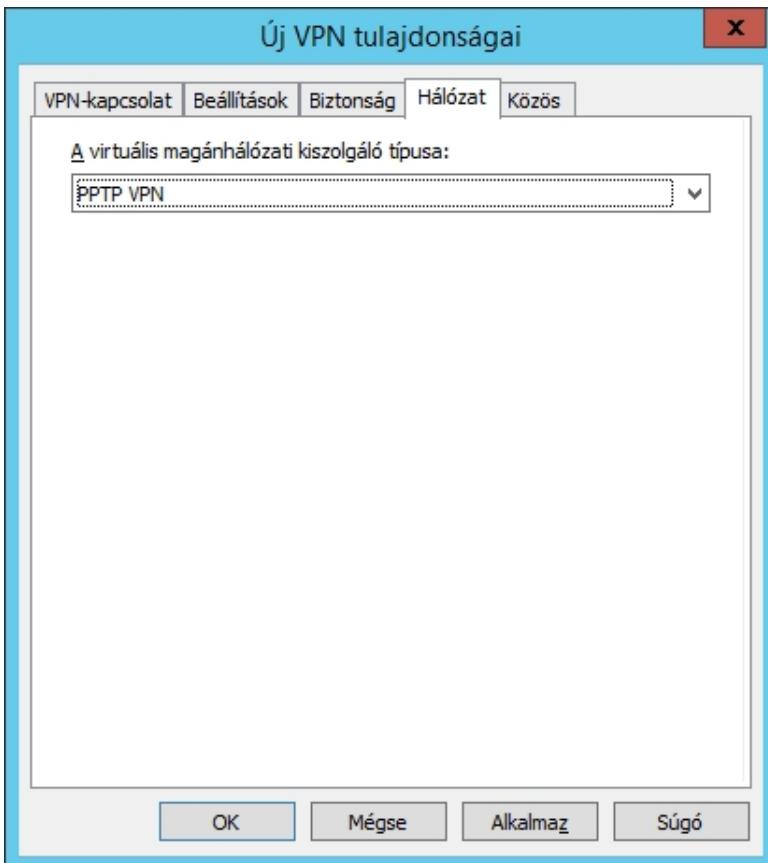
A VPN kapcsolat létrehozásához szükséges adatokat adjuk meg:



A Biztonság fülön állítsuk be a szerver által megkövetelt vagy elfogadott protokollokat:



A Hálózat fülön megadhatjuk a magánhálózat típusát is, esetünkben ez PPTP, ami az alapértelmezés is:



Az elkészült csoportázirendünket ellenőrizzük, frissítsük a csoportázirendet: **gpupdate /force**

Kliensen jelentkezzünk be tartományi felhasználói névvel, ehhez el kell érjük a tartományvezérlőnket, működnie kell a **LAN** nevű kapcsolatnak mind a szerveren, mind a kliensen. Amikor a csoportázirend frissítés eljut a kliensre (bejelentkezünk tartományi felhasználóként) a Hálózati kapcsolatok között automatikusan létrejön a VPN kapcsolatunk, a kliens gépen letiltva a LAN nevű kapcsolatot, a WAN nevűn keresztül (a VPN kapcsolatot használva) továbbra is elérhetjük a 192.168.10.0 /24 hálózat kiszolgálóit. pl. **ping 192.168.10.1** vagy **http://192.168.10.1**

