

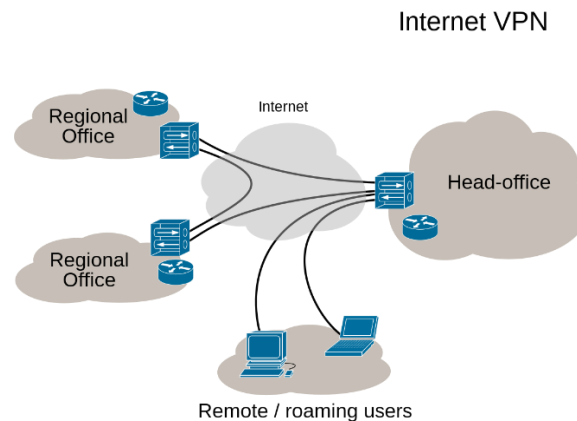
# VPN

## Mi a VPN?

A VPN (Virtual Private Network) magyar fordításban "virtuális magánhálózatot" jelent. Ez egy olyan technológia, amely lehetővé teszi egy biztonságos és titkosított kapcsolat létrehozását az interneten keresztül. A VPN segítségével az internetezők olyan, mintha egy privát hálózathoz csatlakoznának, még akkor is, ha éppen egy nyilvános hálózatot használnak.

Amikor a VPN aktív, akkor a felhasználó valódi IP címe elrejtésre kerül, olykor egy teljesen más országból vagy kontinensről érkezőnek látják bizonyos, "kíváncsiskodó" weboldalak.

VPN nélkül az alábbi módon működik a folyamat: Normál felhasználóként először az internetszolgáltató (ISP) rendszeréhez csatlakozik a számítógép (okostelefon vagy tablet), ami kioszt a készüléknek egy dinamikus IP címet. Ezután eljuttatja a felhasználót a weboldalhoz, amit meg szeretne tekinteni. A megnyitott weboldal látja a dinamikus IP címet, a szolgáltatója pedig látja, hogy milyen szerverek felé indította a forgalmat, ezáltal közvetetten megismerheti, hogy milyen oldalakat nyit meg. Azaz, hogy mit is csinál a neten.



## Mire használjuk a VPN-t?

Sokan használnak VPN-t, hogy anonim módon és biztonságosan letöltsenek és megosszanak fájlokat a torrent hálózaton. A VPN használható olyan országokban, ahol az internetes tartalmakhoz való hozzáférés korlátozott vagy cenzúrázott. A VPN segíthet ezeket a korlátozásokat megkerülni.

## Mik a VPN fő funkciói?

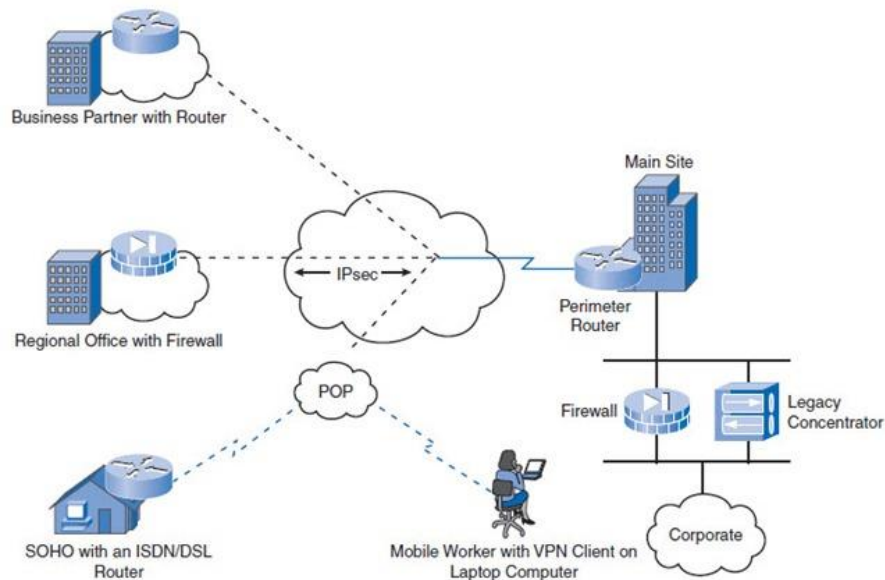
**Biztonságos adatküldés:** A VPN titkosítja az internetes forgalmat, így az küldött és fogadott adatok védettek lesznek a külső, rosszindulatú harmadik felekkel szemben.

**Adatvédelem és anonimitás:** A VPN elrejtí az internetező IP-címét, ezáltal nehezebbé teszi az online tevékenységek nyomon követését. Ez növeli az internetezők adatvédelmét és anonimitását.

**Geográfiai korlátozások feloldása:** A VPN segítségével a felhasználók olyan szervereken keresztül csatlakozhatnak az internethez, amelyek különböző földrajzi helyeken találhatók.

**Nyilvános Wi-Fi kapcsolatok biztonságának növelése:** A VPN segít abban, hogy a felhasználók biztonságosan csatlakozhassanak nyilvános Wi-Fi hálózatokhoz, minimalizálva a külső támadások kockázatát.

**Távoli hozzáférés:** A vállalatok gyakran használják a VPN-t, hogy lehetővé tegyék az alkalmazottaik számára a biztonságos távoli hozzáférést a vállalati erőforrásokhoz



## Mi a VPN használat előnye?

Az azonosságunk elrejtése sok országban az egyetlen opció a blokkolt tartalmak elérésére. Ha egy állam blokkolja a hozzáférést bármilyen "nem kívánatos" weboldalhoz, VPN segítségével megkerülhető ez a tiltás, ezáltal hozzáférhetővé válnak a nagyvilág hírei, a távoli ismerősök, stb. Cenzúra és megfigyelés nélkül.

Maradjunk rejtettek a VPN használatával, ami nem csak biztonságos, titkosított kapcsolatot nyújt, de segít elkerülni a földrajzi elhelyezkedés alapján működő tartalmi korlátozásokat is. Néhány ilyen helyzet például:

- ❖ Olyan szolgáltatásokat szeretnél igénybe venni, amit esetleg korlátoznak földrajzilag, és nálunk nem elérhető.
- ❖ Szeretnél olyan weboldalakat megnézni, amelyek tartalma régióként, országonként eltérő.
- ❖ Szeretnél olyan sorozatokat és filmeket online megnézni, amelyek esetleg a régióban nem érhetőek el.
- ❖ Egy másik előnye a VPN használatának az internet kapcsolat titkosítása. A kliens ugyanis egy titkosított csatornát hoz létre az eszközön és a VPN szerver között, így a külső támadásoktól is aránylag védettek vagyunk. Jól jön ez a védelem, amikor egy nyilvános Wi-Fi hálózatra csatlakozunk, pl. a repülőtéren vagy egy kávézóban.

*Fontos: ha bejelentkezel az adott webes szolgáltatásba a fiókkal pl. Gmail-be, és VPN-en keresztül böngészel, a Google követni tudja a netes tevékenységedet. Ezért inkognitó módot kell használni mellé, így a böngésződben mentett cookie-k (sütik) alapján nem tudnak majd követni.*

## Mik a VPN használat hátrányai?

A VPN (Virtuális Magánhálózat) számos előnyt kínál, de fontos tudni a hátrányait is. Itt vannak a VPN használatának potenciális hátrányai:

**Sebességcsökkenés:** A VPN használata általában lassabb internetkapcsolathoz vezethet, mivel az adatok kiegészítő szintű titkosítás és átirányítás miatt haladnak át.

**Költségek:** Bár léteznek ingyenes VPN-szolgáltatások, a jobb minőségű, megbízhatóbb szolgáltatásokért gyakran fizetni kell. Az előfizetési díjak és egyéb költségek hozzáadhatók.

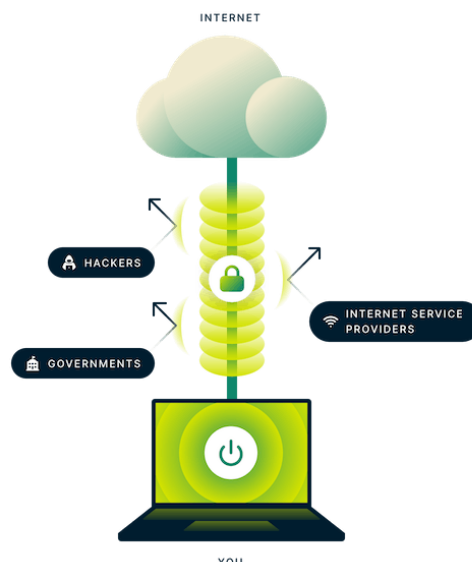
**Adatbiztonsági kockázatok:** Ha nem választasz megbízható VPN-szolgáltatót, az adataidat akár rosszindulatú szándékkal működő szolgáltatókhoz juttathatja el. Fontos alaposan megvizsgálni a választott szolgáltatót, különösen, ha az ingyenes szolgáltatásokat részesít előnyben.

**Korlátozott tartalomhoz való hozzáférés:** Néhány internetes szolgáltatás vagy weboldal blokkolhatja a VPN-t használó felhasználók hozzáférését. Például, egyes streaming szolgáltatók kikapcsolhatják a VPN-eket, hogy megakadályozzák a tartalom területi korlátozások kijátszását.

**Nyomkövetés:** Míg a VPN növelheti az anonimitást, nem garantálja a teljes névtelenséget. Egyes VPN-szolgáltatók még mindig naplózhatják a felhasználói tevékenységeket, és ezeket az adatokat harmadik felekkel megoszthatják.

**Konfigurációs bonyodalmak:** A VPN beállítása és konfigurálása némi technikai jártasságot igényelhet. Az átlagos felhasználóknak ezért lehetnek nehézségeik a megfelelő konfigurációval és beállításokkal.

**Bizalmatlanság:** A VPN szolgáltatóval való teljes bizalom nélkül a felhasználók kénytelenek adataikat egy harmadik félre, a VPN-szolgáltatóra bízni. Ha a szolgáltató nem megfelelően védi az adatokat, az biztonsági problémákat eredményezhet.



## Mit kell előzetesen beállítani a VPN-hez?

A VPN beállítása általában viszonylag egyszerű folyamat, és a konkrét lépések a használt eszköz és operációs rendszer függvényében változhatnak. Általánosságban elmondható, hogy a következő lépéseket kell követni:

### **Számítógépen (Windows 10 példája):**

- ❖ Válasszunk egy megbízható VPN-szolgáltatót, és regisztrálj egy fiókot.
- ❖ Töltsük le és telepítsük a VPN-szolgáltató által kínált kliensalkalmazást.
- ❖ Nyissuk meg a VPN-kliens alkalmazást, és jelentkezzen be a fiókjába a kapott bejelentkezési adatokkal.
- ❖ Válasszuk ki a kívánt szerverhelyet. Ezt általában az alkalmazás felhasználói felületén vagy a beállítások menüjében teheti meg.
- ❖ Indítsuk el a VPN-kapcsolatot az alkalmazásban található "Connect" vagy "Start" gomb megnyomásával.

### **Számítógépen (Mac példája):**

- ❖ Regisztráljunk egy VPN-szolgáltatónál, majd töltsd le és telepítsd az általa kínált alkalmazást.
- ❖ Nyissuk meg az alkalmazást, és jelentkez be a fiókodba.
- ❖ Válasszuk ki a szükséges szerverhelyet az alkalmazás felhasználói felületén.
- ❖ Indítsuk el a VPN-kapcsolatot az alkalmazásban található "Connect" vagy hasonló gomb segítségével.

### **Okostelefonon vagy táblagépen (iOS példája):**

- ❖ Töltsük le a kiválasztott VPN-szolgáltató alkalmazását az App Store-ból.
- ❖ Nyissuk meg az alkalmazást, és jelentkez be a fiókodba.
- ❖ Válasszuk ki a kívánt szerverhelyet az alkalmazásban.
- ❖ Indítsuk el a VPN-kapcsolatot az alkalmazásban található "Connect" gombbal vagy hasonlóval.

### **Okostelefonon vagy táblagépen (Android példája):**

- ❖ Töltsük le a kiválasztott VPN-szolgáltató alkalmazását a Google Play Áruházból.
- ❖ Nyissuk meg az alkalmazást, és jelentkez be a fiókodba.
- ❖ Válasszuk ki a kívánt szerverhelyet az alkalmazásban.
- ❖ Indítsuk el a VPN-kapcsolatot az alkalmazásban található "Connect" gombbal vagy hasonlóval.

A fenti lépések csak egy általános útmutatást nyújtanak. Minden VPN-szolgáltatónak saját alkalmazása és beállítási folyamatai vannak, tehát érdemes elolvasni az adott szolgáltató által nyújtott útmutatót vagy támogatási dokumentációt is.

### **Forrás:**

<https://www.hwsz.hu/hirek/56755/android-biztonsag-vpn-kapcsolat-titkositas.html>

[https://www.expressvpn.com/hu/go/home?gad\\_source=1&gclid=Cj0KCQiA6vaqBhCbARIsACF9M6I4Z9U-](https://www.expressvpn.com/hu/go/home?gad_source=1&gclid=Cj0KCQiA6vaqBhCbARIsACF9M6I4Z9U-)

[AXma2\\_xjKKecep46sWrFfWKU\\_9qVALkoZdaS9Iyp19R1KrwMaAqSJEALw\\_wcB](https://www.expressvpn.com/hu/go/home?gad_source=1&gclid=Cj0KCQiA6vaqBhCbARIsACF9M6I4Z9U-AXma2_xjKKecep46sWrFfWKU_9qVALkoZdaS9Iyp19R1KrwMaAqSJEALw_wcB)

<https://privadovpn.com/hu/what-is-a-vpn/>

# VPN Gyakorlat

## Gyakorlati megvalósítás

### Lépések

#### I. Előkészületek

##### 1. IP-címek

Windows 11

### IP-beállítások szerkesztése

IP-cím

192.168.0.30

Alhálózati maszk

255.255.255.0

Átjáró

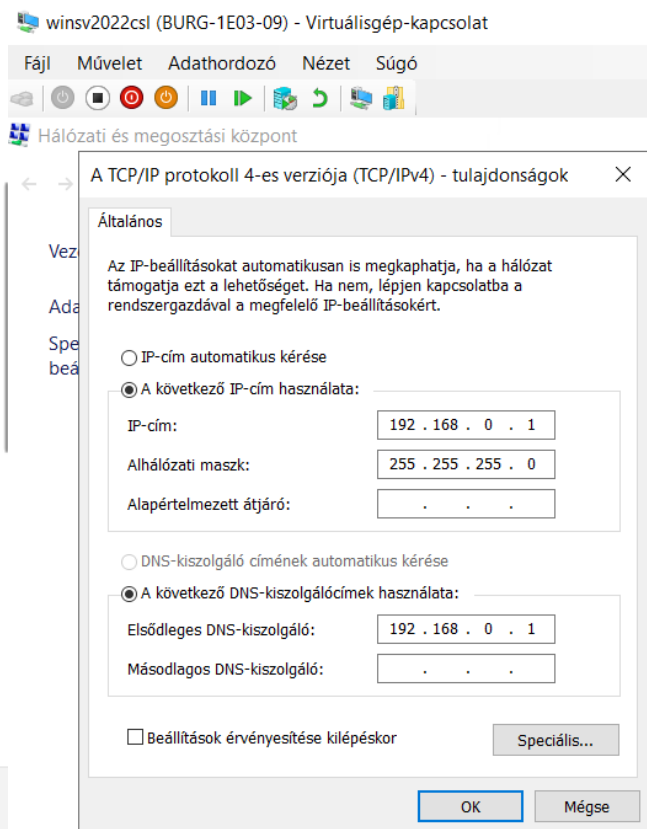
192.168.0.1

Előnyben részesített DNS

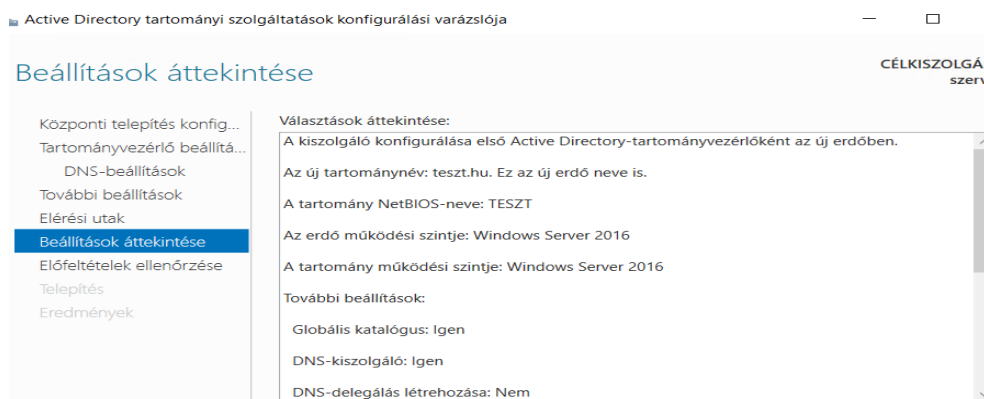
192.168.0.1

HTTPS-on keresztüli DNS

Windows Server 2022



A VPN feltelepítése és konfigurálása előtt fel kell telepíteni az „Active Directory tartományi szolgáltatások”, „DNS” és a „DHCP” szerepkört!



## Új hatókör varázsló

### Hatókör neve

Az azonosításhoz meg kell adnia egy hatókörnevet. Ha akarja, megadhat egy leírást is.

Írja be a hatókör nevét és leírását. Ez az információ segít annak gyors azonosításában, hogy miként történik a hatókör használata a hálózatban.

Név:

Leírás:

## Új hatókör varázsló

### IP-címtartomány

Hatóköri címtartományt úgy definiálhat, hogy megad egy egymást követő IP-címekből álló halmazt.

A DHCP-kiszolgáló konfigurációs beállításai

Adja meg azt a címtartományt, amelyet a hatókör terjeszt.

Kezdő IP-cím:

Záró IP-cím:

A DHCP-ügyfélre is érvényes konfigurációs beállítások

Hossz:

Alhálózati maszk:

## Új hatókör varázsló

### Kizárások és késleltetés hozzáadása

A kizárások olyan címek vagy címtartományok, amelyeket a kiszolgáló nem terjeszt. A késleltetés az az időtartam, amellyel a kiszolgáló késlelteti a DHCP OFFER üzenetek továbbítását.

Írja be a kizárandó IP-címtartományt. Ha egyetlen címet szeretne kizárni, akkor ezt a címet csak a Kezdő IP-cím mezőbe írja be.

Kezdő IP-cím:

Záró IP-cím:

Hozzáadás

Kizárt címtartomány:

192.168.0.1-192.168.0.5

Eltávolítás

Alhálózati késleltetés  
ezredmásodpercben:

0

## Új hatókör varázsló

### Címberlet élettartama

A bérlet élettartama azt adja meg, hogy az ügyfél mennyi ideig használhatja a hatókörből.

A címberlet időtartamának tipikus esetben egyenlőnek kell lennie az amennyit a számítógépek az adott fizikai hálózathoz csatlakozva tölt hordozható számítógépekből álló) hálózatok vagy telefonos ügyfelek lehet rövidebb címberleti időtartamot megadni.

Stabil (azaz főleg rögzített helyen levő, asztali számítógépekből álló) hosszabb bérleti időtartamot érdemes megadni.

Állítsa be a kiszolgáló által terjesztett hatókörbérletek időtartamát.

Ennyi ideig:

nap:

óra:

perc:

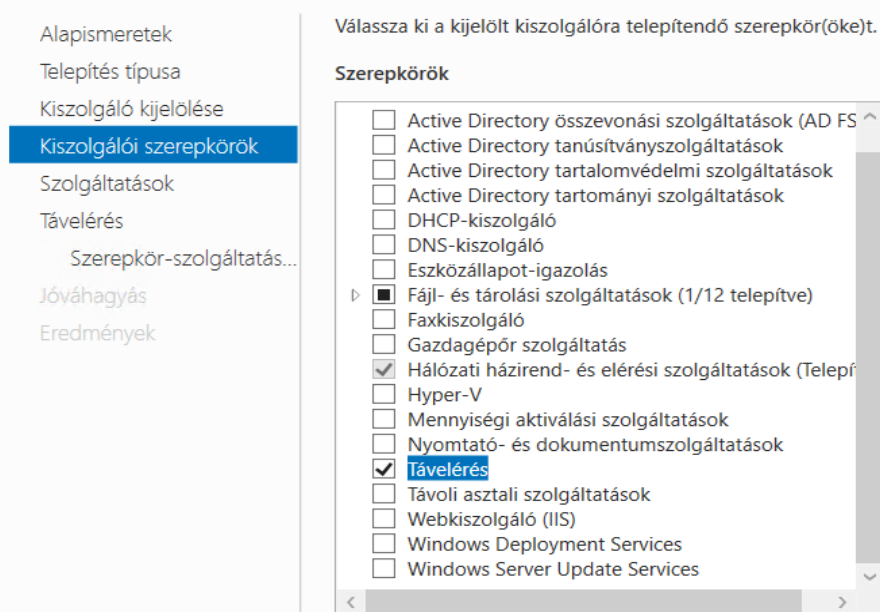


## II. A VPN létrehozása

### 1. Feltelepítés

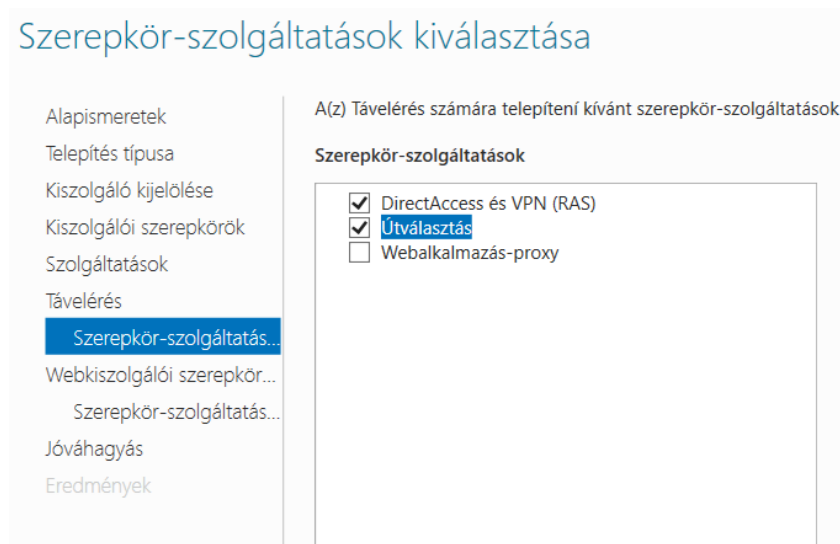
A szolgáltatás „Távelérés” néven található meg,” ezt a szerepkört telepítsük fel.

#### Kiszolgálói szerepkörök kiválasztása



A „Távelérés” szerepkörön belül válasszuk ki az „Útválasztás” és a „DirectAccess és VPN (RAS)” lehetőségeket.

#### Szerepkör-szolgáltatások kiválasztása



A Kiszolgálókezelőben a „Távelérés-kezelés” szerepkörre kattintunk, majd ezen belül a DirectAccess és VPN-t opciót választjuk a konfiguráción belül.



Távélés kezelési konzolja

Konfiguráció

DirectAccess és VPN

szerver

## Távélés telepítése

Távélés (például DirectAccess és VPN) konfigurálása.

### Távélés beállítása

A DirectAccess és a virtuális magánhálózat beállításai még nincsenek konfigurálva. Válassza ki a kívánt beállításai közül.

→ [Az Első lépések varázsló futtatása](#)

A varázsló alapértelmezett beállításaival gyorsan konfigurálhatja a DirectAccess és a virtuális magánhálózat beállításait.

→ [A Távélés telepítése varázsló futtatása](#)

A varázslóban egyedi beállításokkal is konfigurálhatja a DirectAccess és a virtuális magánhálózat beállításait.

**Az „Első lépések varázsló futtatása” menüpontban csak a VPN-t telepítjük fel.** (Ezt egyébként rögtön a feltelepítés utáni ablakban is megtaláljuk szintén „Első lépések varázsló futtatása” címmel.)

Távélés beállítása

### Távélés beállítása

Első lépések varázsló

Üdvözlő a Távélés szolgáltatás

A lap beállításai konfigurálhatja a DirectAccess szolgáltatást és a virtuális magánhálózatot.

→ **DirectAccess és VPN telepítése (ajánlott)**

A DirectAccess és a VPN konfigurálása a kiszolgálón és a DirectAccess-ügyfélszámítógépek engedélyezése. A DirectAccess szolgáltatáshoz nem támogatott távoli számítógépek virtuális magánhálózaton keresztüli csatlakozásának engedélyezése.

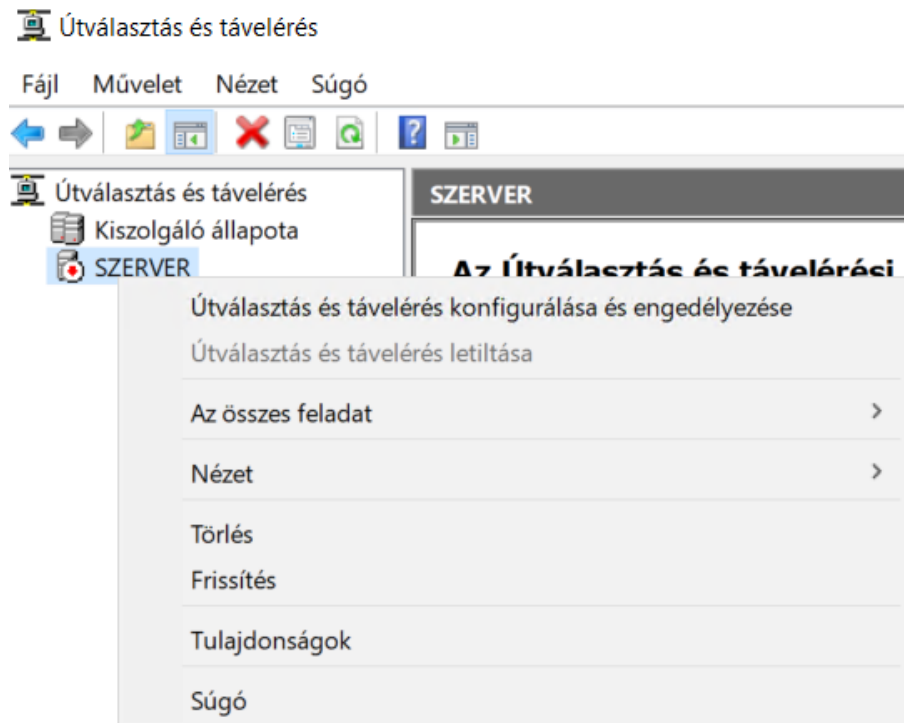
→ **Csak a DirectAccess telepítése**

DirectAccess konfigurálása a kiszolgálón és a DirectAccess-ügyfélszámítógépek engedélyezése.

→ **Csak a VPN telepítése**

Virtuális magánhálózat konfigurálása az Útválasztás és távélés konzolról. A távoli ügyfélszámítógépek csatlakozhatnak virtuális magánhálózaton keresztül, és több hely köthető össze a virtuális magánhálózati pont-pont kapcsolatokkal. A VPN-t használhatják a DirectAccess szolgáltatáshoz nem támogatott távoli számítógépek.

A Szerverre jobb egérgombbal kattintunk, majd engedélyezzük az útválasztást és konfiguráljuk.



Az Egyéni konfiguráció lehetőséget választjuk.

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

Kiválasztjuk a VPN-t, azaz a „Virtuális magánhálózat” lehetőséget, és ezzel elindítjuk a szolgáltatást.

## Útválasztás és távelérési kiszolgáló - telepítővarázsló

### Egyéni konfiguráció

Miután a varázsló bezárul, a kiválasztott szolgáltatásokat az Útválasztás és távelérés konzolban lehet beállítani.

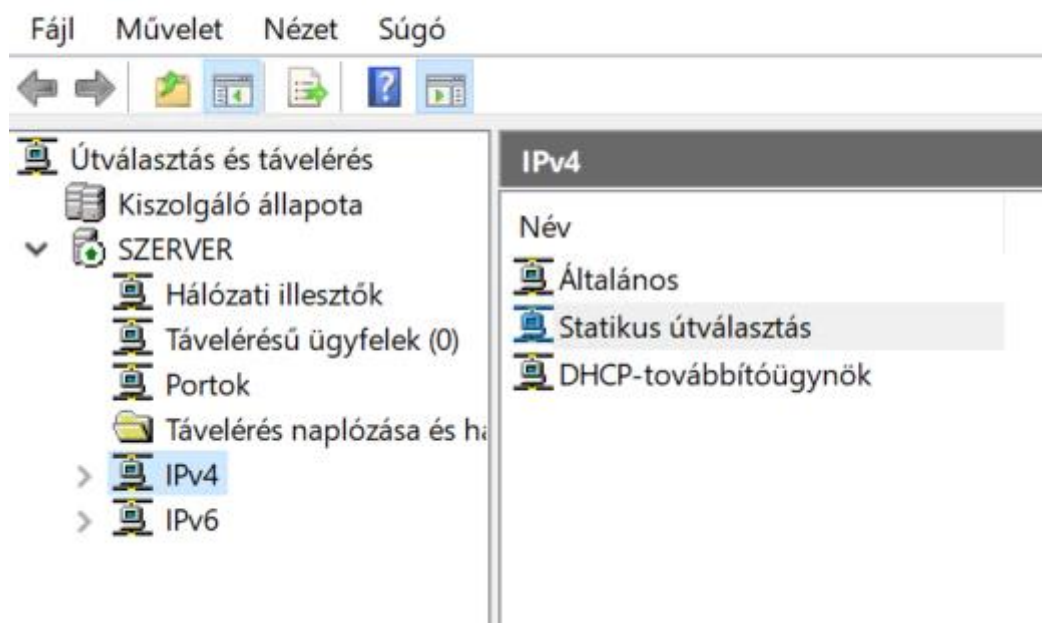
Válassza ki azokat a szolgáltatásokat, amelyeket engedélyezni szeretne ezen a kiszolgálón.

- ☒ Virtuális magánhálózat
- ☐ Telefonos hálózat
- ☐ Igény szerinti kapcsolat (irodai útválasztáshoz)
- ☐ Hálózati címfordítás (NAT)
- ☐ LAN-útválasztás

Ha a SZERVER kiszolgálónál zöld felfele nyíl jelenik meg, akkor az azt jelenti, hogy a szolgáltatás működésbe lépett.



### Útválasztás és távelérés



Ezután a „SZERVER”-en jobb egérgombra kattintva, „Tulajdonságok” menüpontot nyitjuk meg, ezen belül a „Biztonság” menüpontot.

Általános Biztonság IPv4 IPv6 IKEv2 PPP Naplózás

A hitelességellenőrző érvényesíti a távelérésű ügyfelek és az igény szerinti útválasztók hitelesítő adatait.

Hitelességellenőrző:

Windows-hitelesítés Beállítás...

Hitelesítési módszerek...

A nyilvántartási szolgáltató kezeli a csatlakozási kérelmek és munkamenetek naplóját.

Nyilvántartási szolgáltató:

Windows-nyilvántartás Beállítás...

Az egyéni IPsec-házirend előmegosztott kulcsot ad meg az 2TP/IKEv2-kapcsolatokhoz. Az Útválasztás és távelérés szolgáltatást el kell indítani ezen beállításhoz. Az ezen kiszolgáló tanúsítvánnyal való hitelesítésére konfigurált IKEv2-kezdeményezők nem lesznek képesek csatlakozni.

☒ Egyéni IPsec-házirend engedélyezése L2TP/IKEv2-kapcsolatokhoz

Előmegosztott kulcs:

Vizsga2023

SSL-tanúsítvány kötése:

☐ HTTP használata

Válassza ki azt a tanúsítványt, amelyet az SSTP-kiszolgáló az SSL protokollal való kötéshez használhat (Webfigyelő)

Tanúsítvány: Alapértelmezett Nézet

OK Mégse Alkalmaz

Az „Egyéni IPsec-házirend engedélyezése L2TP/IKEv2-kapcsolatokhoz” lehetőség legyen engedélyezve, az előre megosztott kulcs a „Vizsga2023” legyen.

Ezután újraindítjuk a szolgáltatást.

A „Kiszolgálókezelő”-ben feltelepítjük a „Hálózati házirend- és elérési szolgáltatások” szerepkört.

**FONTOS!!!!**

**A feltelepítése előtt, mindenképpen a Távelérés szolgáltatást fel kell telepíteni és konfigurálni kell, különben a szolgáltatás nem fog elindulni!**

## Kiszolgálói szerepkörök kiválasztása

Alapismeretek

Telepítés típusa

Kiszolgáló kijelölése

**Kiszolgálói szerepkörök**

Szolgáltatások

Hálózati házirend- és elér...

Jóváhagyás

Eredmények

Válassza ki a kijelölt kiszolgálóra telepítendő szerepkör(öke

### Szerepkörök

- ☐ Active Directory Lightweight Directory-szolgáltatás
- ☐ Active Directory összevonási szolgáltatások (AD FS)
- ☐ Active Directory tanúsítványszolgáltatások
- ☐ Active Directory tartalomvédelmi szolgáltatások
- ☒ Active Directory tartományi szolgáltatások (Telepítve)
- ☒ DHCP-kiszolgáló (Telepítve)
- ☒ DNS-kiszolgáló (Telepítve)
- ☐ Eszközállapot-igazolás
- ▶ ☒ Fájl- és tárolási szolgáltatások (2/12 telepítve)
- ☐ Faxkiszolgáló
- ☐ Gazdagépőrző szolgáltatás
- ☒ **Hálózati házirend- és elérési szolgáltatások**
- ☐ Hyper-V
- ☐ Mennyiségi aktiválási szolgáltatások
- ☐ Nyomtató- és dokumentumszolgáltatások

(Célkiszolgáló automatikus újraindítása, ha szükséges) legyen bejelölve!

## Telepítendő összetevők megerősítése

Alapismeretek

Telepítés típusa

Kiszolgáló kijelölése

Kiszolgálói szerepkörök

Szolgáltatások

Hálózati házirend- és elér...

**Jóváhagyás**

Eredmények

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

- ☒ Célkiszolgáló automatikus újraindítása, ha szükséges

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

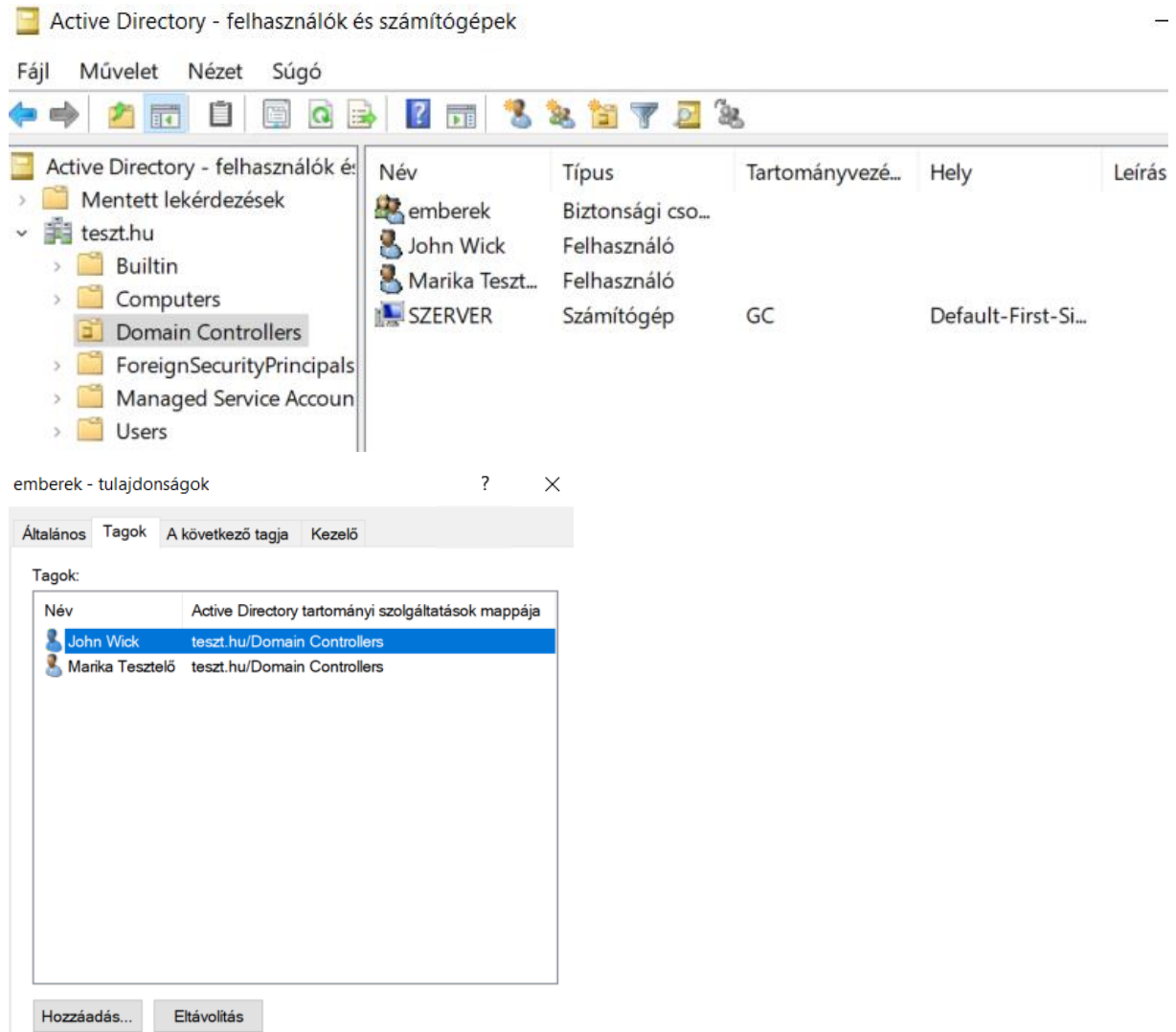
Hálózati házirend- és elérési szolgáltatások

Távoli kiszolgálófelügyelet eszközei

Szerepkör-felügyeleti eszközök

A Hálózati házirend- és elérési szolgáltatások eszközei

A Hálózati házirend kialakítása előtt létre kell hoznunk a felhasználókat, és ezt egy csoportba vesszük fel az ábrán látható módon. A felhasználók már fel vannak véve az emberek csoportba. Ezt az „Active Directory – Felhasználók és számítógépek” szerepkörön belül tehetjük meg.



Megvannak a felhasználók, hozzá láthatunk a VPN szabály kialakításához.

Először is engedélyoznünk kell az elérést a két felhasználó számára.

A „Felhasználó”-ra jobb egérgombbal kattintva a „Tulajdonságok” fülben a behívás menüpontban engedélyezzük az elérést a felhasználók számára.



Marika Tesztelő - tulajdonságok

Távvezérlés    Távoli asztali szolgáltatások profilja    COM+

Általános    Cím    Fiók    Profil    Telefonszámok    Szervezet

A következő tagja    Behívás    Könyezet    Munkamenetek

Hálózati hozzáférési engedély

☒ Elérés engedélyezése

☐ Elérés letiltása

☐ Hozzáférés-vezérlés NPS-hálózati házirend alapján

☐ Hívóazonosító ellenőrzése:

Visszahívási beállítások

☒ Nincs visszahívás

☐ Hívó által megadott számon (csak útválasztás és RAS)

☐ Mindig ezen a számon:

☐ Statikus IP-címek hozzárendelése

IP-címek megadása ehhez a behívásos kapcsolathoz.

☐ Statikus útvonalak alkalmazása

Útválasztás megadása ehhez a behívó kapcsolathoz.

OK    Mégse    Alkalmaz    Súgó

Ugyanezt megcsináljuk a „John Wick” felhasználóval is.

Hálózati házirend kialakítása:

A „Hálózati házirend- és elérési szolgáltatások” szerepkörbe kattintva a „Hálózati házirendek” menüpontra jobb egérgombbal kattintva létrehozunk egy új „Hálózati házirendet”.

Hálózati házirend-kiszolgáló

Fájl    Művelet    Nézet    Súgó

Hálózati házirend-kiszolgáló (H)

> RADIUS-ügyfelek és -kiszolgálók

▼ Házirendek

    Kapcsolatkérelem-házirendek

    Hálózati házirendek

        Új

        Lista exportálása

        Nézet

        Frissítés

        Súgó

Hálózati házirendek

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

	Állapot	Feldolgozó
... a Microsoft Útválasztás és távérlés szolgáltatását futtató kiszolgálóval	Engedélyezve	999998
... más elérési kiszolgálókkal	Engedélyezve	999999





## Adja meg a hálózati házirend nevét és a kapcsolattípust

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

**Házirend neve:**

VPN

**Hálózati kapcsolódás módja**

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

☒ Hálózat-hozzáférési kiszolgáló típusa:

Meghatározatlan

☐ Szállítóspecifikus:

10

## Hozzáadunk egy új feltételt:



### 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

**Feltétel leírása:**

**Feltétel kijelölése**

Jelöljön ki egy feltételt, majd kattintson a Hozzáadása gombra.

Csoportok

- Windows-csoportok**  
A Windows-csoportok feltétel megadja, hogy a kapcsolódó felhasználónak vagy számítógépnek a kijelölt csoportok valamelyikéhez kell tartoznia.
- Számítógépcsoportok**  
A Számítógépcsoportok feltétel megadja, hogy a kapcsolódó számítógépnek a kijelölt csoportok valamelyikéhez kell tartoznia.
- Felhasználói csoportok**  
A Felhasználói csoportok feltétel megadja, hogy a kapcsolódó felhasználónak a kijelölt csoportok valamelyikéhez kell tartoznia.

Nap és időpont korlátozásai

**Nap és időpont korlátozásai**  
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... Mégse






Hozzáadás... Szerkesztés... Eltávolítás

Kiválasztjuk a megfelelő hitelesítéstípust, jelen esetben MS-CHAP v2.

Feltétel kijelölése

Jelöljön ki egy feltételt, majd kattintson a Hozzáadása gombra.

**Kapcsolat tulajdonságai**

-  **Hozzáférési ügy**  
A hozzáférési ügy feltétel megadja az ügyfél számítógép hozzáférést kér.
-  **Hozzáférési ügy**  
A hozzáférési ügy feltétel megadja az ügyfél számítógép hozzáférést kér.
-  **Hitelesítés típusa**  
A hitelesítés típusa feltétel a házirendet az egy bizonyos hitelesítési módokra korlátozza.
-  **Engedélyezett EAP-típusok**  
Az Engedélyezett EAP-típusok feltétel megadja azokat az EAP-típusokat, amelyek a házirendben engedélyezettek a hitelesítéshez.
-  **Keretes protokoll**  
A Keretes protokoll feltétel a házirendet azokra az ügyfelekre korlátozza, amelyek keretképzési protokollt, például a PPP vagy SLIP protokollt használnak.

**Hitelesítési módszer**

A házirendnek való megfelelés megadása.

- ☐ Bövítő
- ☐ CHAP
- ☐ EAP
- ☐ MS-CHAP v1
- ☐ MS-CHAP v1 CPW
- ☒ **MS-CHAP v2**
- ☐ MS-CHAP v2 CPW
- ☐ Nem hitelesített
- ☐ PAP
- ☐ PEAP

Alagút protokollt állítunk be, jelen esetben L2TP azaz Layer Two Tunneling Protocol-t.

Feltétel kijelölése

Jelöljön ki egy feltételt, majd kattintson a Hozzáadása gombra.

**Engedélyezett EAP-típusok**  
Az Engedélyezett EAP-típusok feltétel megadja azokat az EAP-típusokat, amelyek a házirendben engedélyezettek a hitelesítéshez.

**Keretes protokoll**  
A Keretes protokoll feltétel a házirendet azokra az ügyfelekre korlátozza, amelyek keretképzési protokollt, például a PPP vagy SLIP protokollt használnak.

**Szolgáltatás típusa**  
A Szolgáltatás típusa feltétel a házirendet az egy bizonyos típusú szolgáltatásokra korlátozza.

**Alagút típusa**  
Az Alagút típusa feltétel a házirendet az egy bizonyos típusú alagútakra korlátozza.

**RADIUS-ügyfél tulajdonságai**

**Alagút típusa**

A házirendnek való megfeleléshez szükséges alagúttípusok megadása

Gyakori telefonos és VPN-alagúttípusok

- ☐ Generic Route Encapsulation (GRE)
- ☐ IP Encapsulating Security Payload in the Tunnel-mode (ESP)
- ☒ **Layer Two Tunneling Protocol (L2TP)**
- ☐ Point-to-Point Tunneling Protocol (PPTP)
- ☐ Secure Socket Tunneling Protocol (SSTP)

802.1X-kapcsolatok gyakori alagúttípusai

- ☐ Virtual LANs (VLAN)

Egyéb

- ☐ Ascend Tunnel Management Protocol (ATMP)
- ☐ Bay Dial Virtual Services (DVS)
- ☐ Generic Route Encapsulation (GRE)
- ☐ IP-in-IP Encapsulation (IP-IP)

OK Mégse

Hozzáadás... Szerkesztés... Eltávolítás

Nap és időpont korlátozások az ábrán látható módon:

**Nap és időpont korlátozásai**

Jelöljön ki egy feltételt, majd kattintson a Hozzáadás gombra

- Windows-csoportok**  
A Windows-csoportok feltétel megadja, valamelyikéhez kell tartoznia.
- Számítógépcsoportok**  
A Számítógépcsoportok feltétel megadja, tartoznia.
- Felhasználói csoportok**  
A Felhasználócsoportok feltétel megadja, tartoznia.

**Nap és időpont korlátozásai**  
A nap- és időkorlátozások adják meg a engedélyezettek vagy nem engedélyezett házirend-kiszolgáló található.

**Nap és időpont korlátozásai**

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

Minden

hétfő

kedd

szerda

csütörtök

péntek

szombat

vasárnap

OK

Mégse

☒ Engedélyezve

☐ Megtagadva

hétfő - péntek, 8:00 - 17:00

Majd felvesszük azt a csoportot, akikre ezt érvénybe akarjuk léptetni, jelen esetben az előbb létrehozott „emberek” csoportot vesszük fel a VPN-szabályba.

**Felhasználói csoportok**

Jelöljön ki egy feltételt, majd kattintson a Hozzáadás gombra

**Csoport**

- Windows-csoportok**  
A Windows-csoportok feltétel megadja, h valamelyikéhez kell tartoznia.
- Számítógépcsoportok**  
A Számítógépcsoportok feltétel megadja, tartoznia.
- Felhasználói csoportok**  
A Felhasználócsoportok feltétel megadja, tartoznia.

**Nap és időpont korlátozásai**  
A nap- és időkorlátozások adják meg a engedélyezettek vagy nem engedélyezett házirend-kiszolgáló található.

**Csoport kiválasztása**

Válassza ki az objektumtípust:

Csoport

Hely:

teszt.hu

Írja be a kijelölendő objektum nevét (példák):

emberek

Névellenőrzés

Speciális...

OK

Mégse



## 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/megtagadása a betárcsázás tulajdonságai szerint, ha a kapcsolódási kísérlet megfelel a házirend feltételeinek.

Új hálózati házirend



## Hitelesítési módszerek konfigurálása

Konfiguráljon legalább egy hitelesítési módszert, amellyel a kapcsolatkérelmek esetén be kell állítania az EAP-típust is.

Az EAP-típusok egyeztetése a hálózati házirend-kiszolgáló és az ügyfél között a listának megfelelő sorrendben történik.

**EAP-típusok:**

Mozgatás fel

Le

Hozzáadás...

Szerkesztés...

Eltávolítás

**Kevésbé biztonságos hitelesítési módszerek:**

- ☒ Microsoft titkosított hitelesítés - 2-es verzió (MS-CHAP-v2)
  - ☒ A felhasználó a jelszót lejárta után is módosíthatja
- ☒ Microsoft titkosított hitelesítés (MS-CHAP)
  - ☒ A felhasználó a jelszót lejárta után is módosíthatja
- ☐ Titkosított hitelesítés (CHAP)
- ☐ Titkosítatlan hitelesítés (PAP, SPAP)
- ☐ Az ügyfelek a hitelesítési módszer egyeztetése nélkül is kapcsolódhatnak.

Tovább → Tovább → Tovább

Láthatjuk, hogy a VPN szabály sikeresen létrejött.

Házirend neve	Állapot	Feldolgozó
VPN	Engedélyezve	1

A „Kapcsolatok a Microsoft Útválasztás és távelérés szolgáltatását futtató kiszolgálóval” jobb egérgombra rákattintva a „Tulajdonságok” menüpontban, engedélyezzük ezt a szabályt.

Hálózati házirend-kiszolgáló

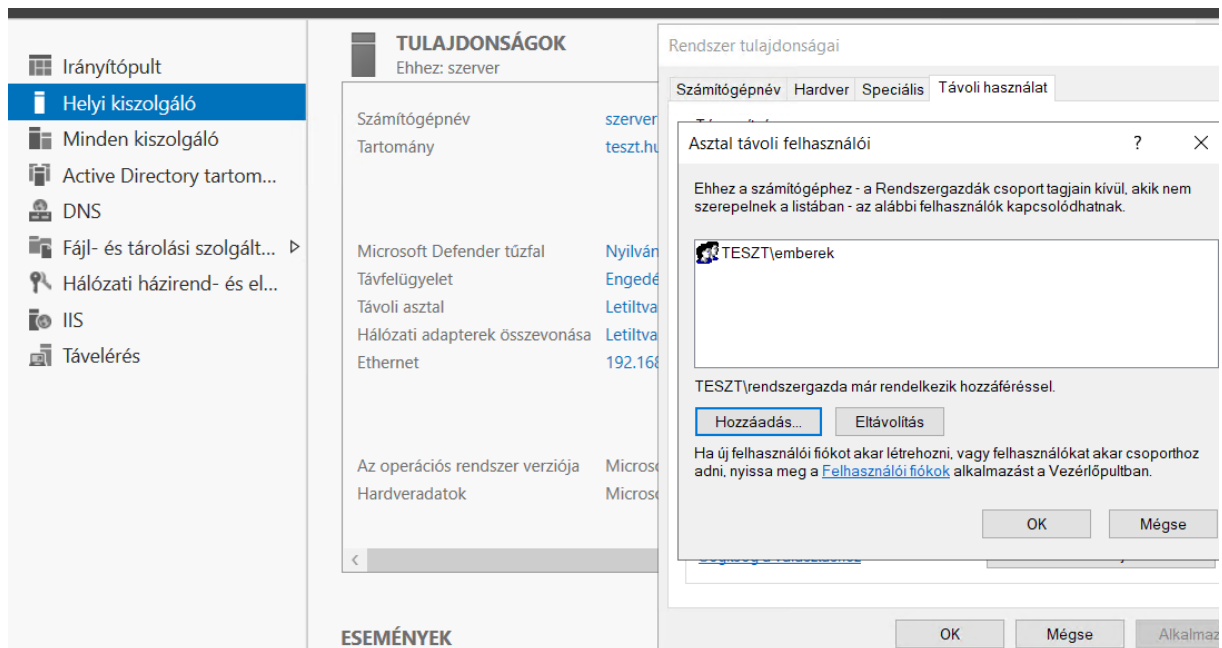
Fájl Művelet Nézet Súgó

Hálózati házirendek

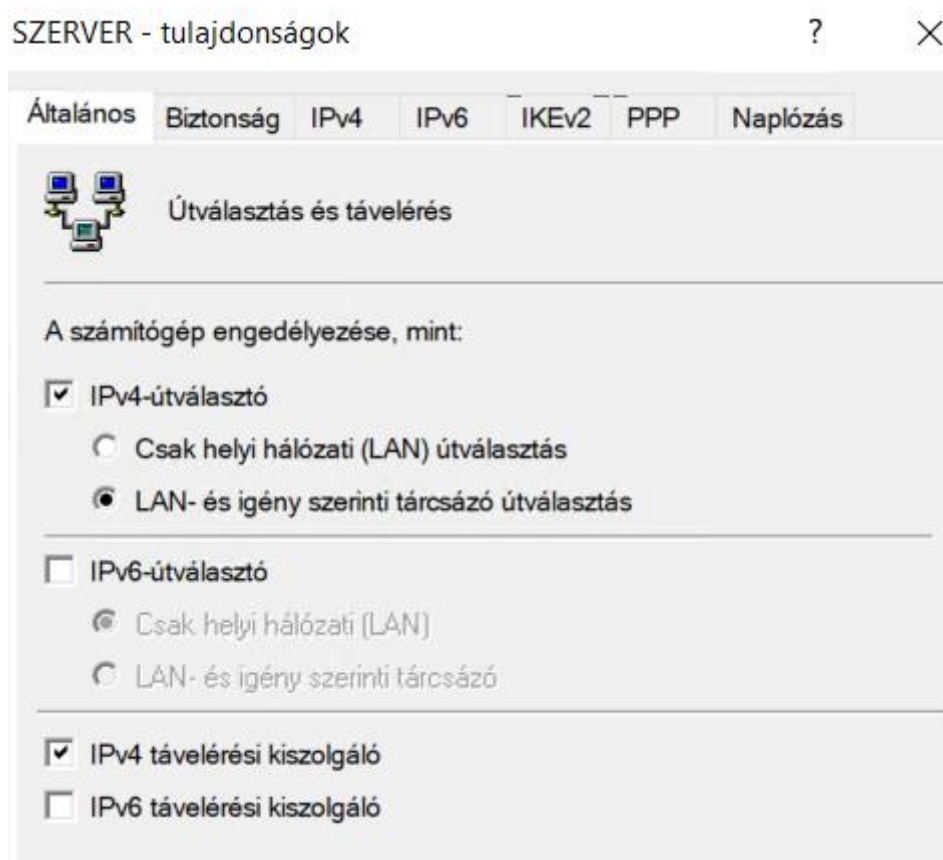
A hálózati házirendek segítségével megadhatja, ki jogosult a hálózathoz való kapcsolódásra, valamint megszabhatja a csatlakozás feltételeit.

Házirend neve	Állapot	Feldolgozó
VPN	Engedélyezve	1
Kapcsolatok a Microsoft Útválasztás és távelérés szolgáltatását futtató kiszolgálóval	Engedélyezve	999998
Kapcsolatok más elérési kiszolgálókkal	Engedélyezve	999999

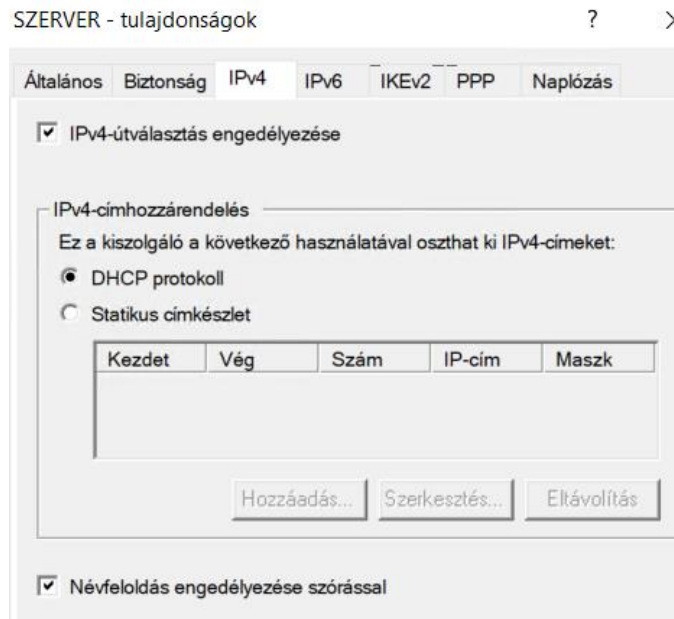
A Szerveren engedélyoznünk kell a Távoli asztal elérését! A Kiszolgálókezelőn belül a helyi kiszolgáló fülön belül a „Távoli asztal” menüpontra kattintva, engedélyezzük a Távoli elérést a „Távoli használat” fülön belül, majd felvesszük azt a csoportot, akire szeretnénk a beállítást alkalmazni, jelen esetben az „emberek” csoportot.



A „Távélerés” menüpontra kattintunk → „Szerver” részen jobb klikk → „Távélerés-kezelés” -  
 → bal oldalt a Konfiguráció alatt „virtuális magánhálózat”-ra kattint → majd „Az RRAS-  
 kezelőkonzol megnyitása” pontra kattintva kiválaszthatjuk jobb egérgombbal kattintva a  
 Tulajdonságok fülön belül az IP-címzés típusát. Jelen esetben most IPv4-et használunk.

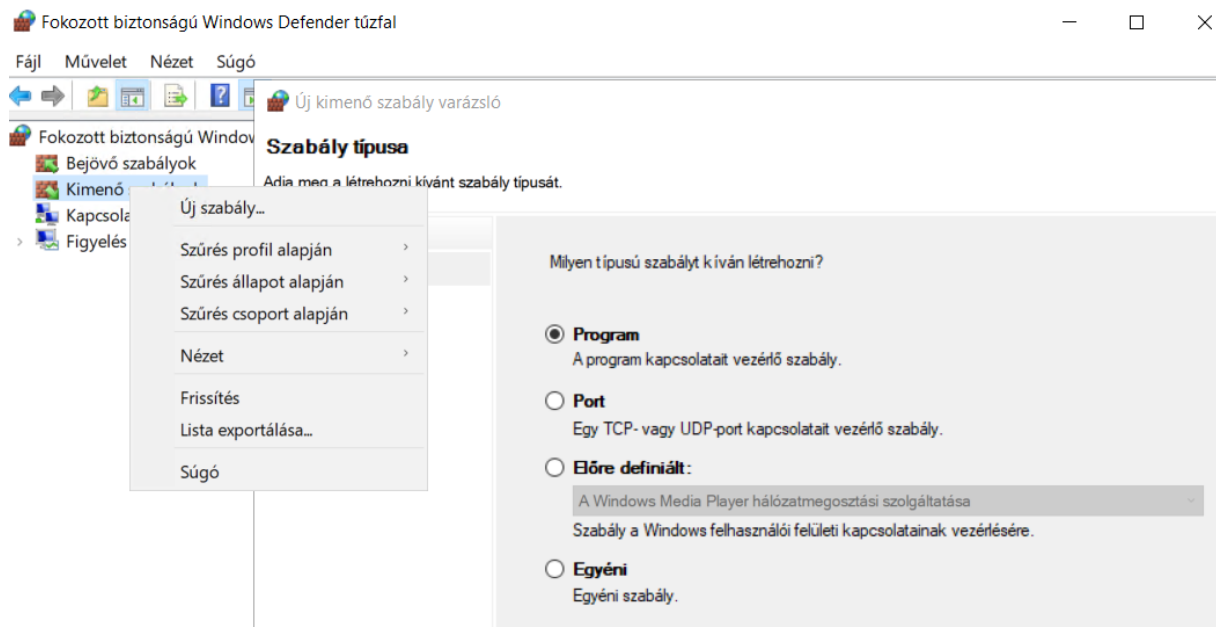


Az „Útválasztás és távelérés” menüpontban a Tulajdonságok fülön belül beállítható DHCP és statikus címkészlet is. Jelen esetben DHCP szolgáltatást használunk.




Végül létrehozzuk a Windows tűzfalban belül azt a szabályt, amely átengedi a szükséges portokat. Ez megtalálható a Windows tűzfal → Speciális beállítások → Kimenő szabályok(jobb klikk) → Új szabály...

Majd a „Port” rádiógombot válasszuk ki!










 Új kimenő szabály varázsló

## Protokoll és portok

Adja meg azokat a protokollokat és portokat, amelyekre a szabály vonatkozik.

<b>Lépések:</b>	
 Szabály típusa	
 <b>Protokoll és portok</b>	
 Művelet	
 Profil	
 Név	

A TCP vagy az UDP protokollra vonatkozik ez a szabály?

☒ **TCP**


☐ **UDP**

Minden távoli portra vonatkozik ez a szabály, vagy csak bizonyos távoli portokra?

☐ **Minden távoli port**






☒ **Adott távoli portok:**

Példa: 80, 443, 5000-5010

 Új kimenő szabály varázsló

## Művelet

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

<b>Lépések:</b>	
 Szabály típusa	
 Protokoll és portok	
 <b>Művelet</b>	
 Profil	
 Név	

Milyen tegyen 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.

☐ **Tiltsa le a kapcsolatot**




 Új kimenő szabály varázsló

## Profil

Adja meg azokat a profilokat, amelyekre ez a szabály vonatkozik.

Lépések:	
<ul style="list-style-type: none"><li>● Szabály típusa</li><li>● Protokoll és portok</li><li>● Művelet</li><li>● Profil</li><li>● Név</li></ul>	<p>Mikor lép érvénybe ez a szabály?</p> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> <b>Tartomány</b> A számítógép vállalati tartományához való csatlakozásakor alkalmazandó.</li><li><input checked="" type="checkbox"/> <b>Személyes</b> A számítógép magánhálózati (például otthoni vagy munkahelyi) helyhez való csatlakozásakor alkalmazandó.</li><li><input checked="" type="checkbox"/> <b>Nyilvános</b> A számítógép nyilvános hálózati helyhez való csatlakozásakor alkalmazandó.</li></ul>

 Új kimenő szabály varázsló

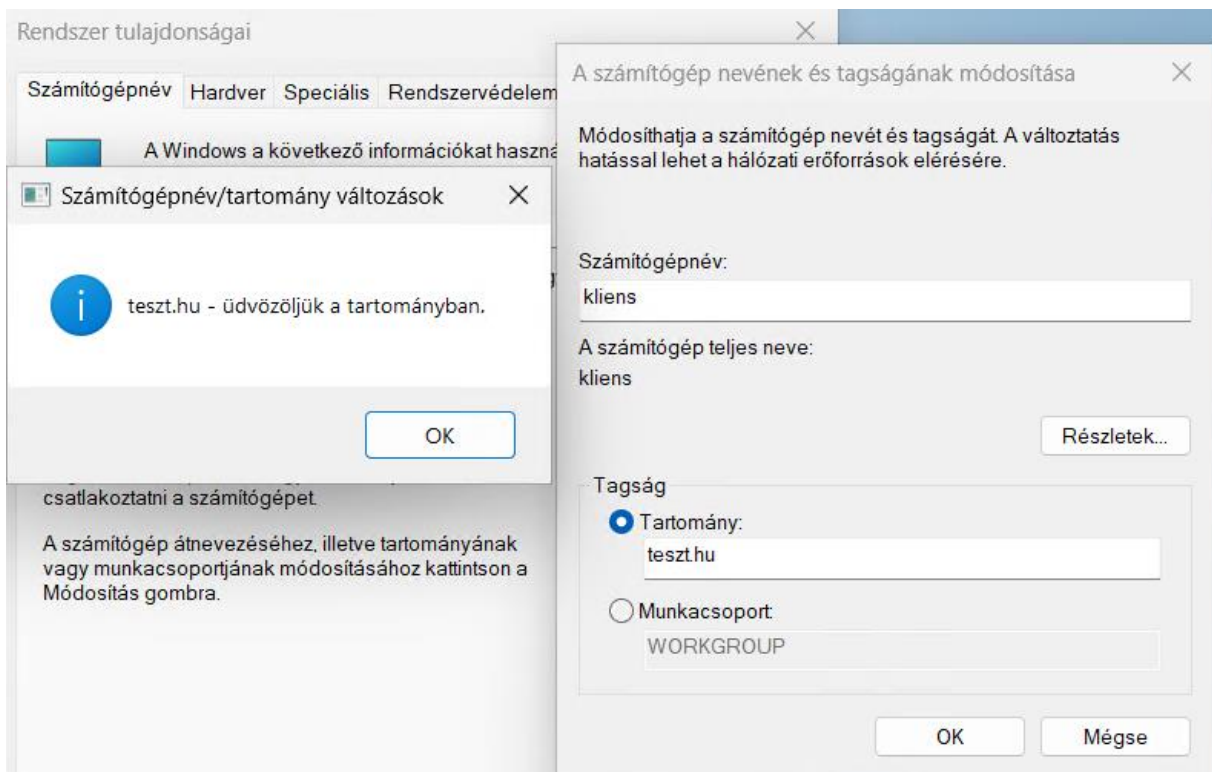
## Név

Adja meg a szabály nevét és leírását.

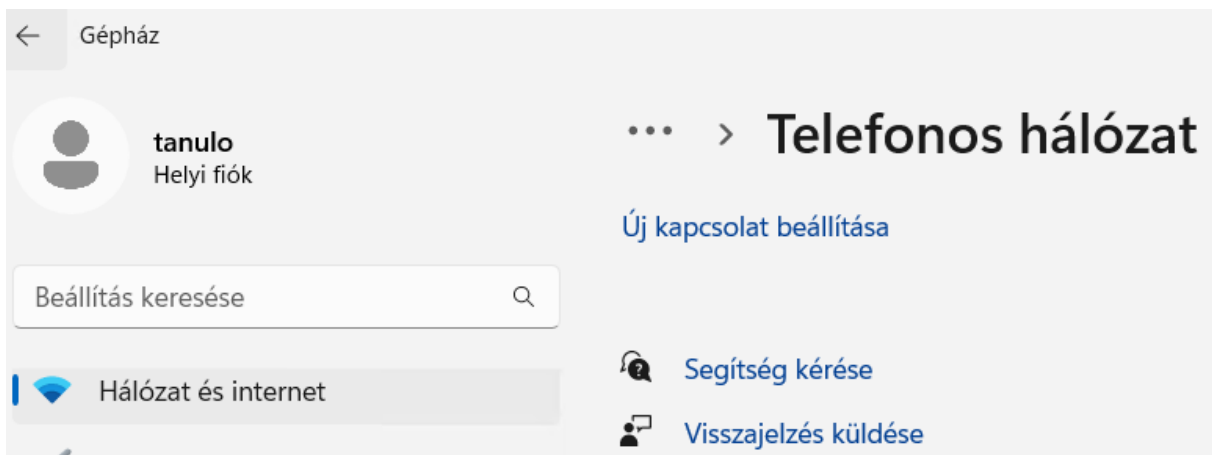
Lépések:	
<ul style="list-style-type: none"><li>● Szabály típusa</li><li>● Protokoll és portok</li><li>● Művelet</li><li>● Profil</li><li>● Név</li></ul>	<p>Név:</p> <p>1723 és 47 kimenő szabály</p> <p>Leírás (nem kötelező):</p>

Így a szerveren az összes beállítást elvégeztük. Áttérhetünk a Kliens-re. Beléptetjük a „teszt.hu” Active Directory tartományba.

## A kliens beállítása és tesztelése




A kapcsolatot hozzáadjuk a "Hálózat és internet" résznél (jobb aluli hálózat ikonon jobb klikk) → „Hálózat és internetkapcsolat” kattint → „Telefonos hálózat” menüpont





A Kapcsolódási lehetőségek közül a – Kapcsolódás munkahelyhez – lehetőséget válasszuk, saját internetkapcsolaton keresztül (magánhálózat – VPN).


Az internetkapcsolatot majd később állítjuk be.


-  Kapcsolat vagy hálózat beállítása

## Kapcsolódási lehetőség kiválasztása

 **Csatlakozás az internethez**  
Szélessávú vagy telefonos internetkapcsolat beállítása.

 **Új hálózat beállítása**  
Új útválasztó vagy elérési pont beállítása.

 **Kapcsolódás munkahelyhez**  
Telefonos vagy virtuális magánhálózati kapcsolat beállítása munkahelyhez.

- ←  Kapcsolódás munkahelyhez

## Hogyan szeretne csatlakozni?

→ **Saját internetkapcsolat (magánhálózat) használata**  
Csatlakozás virtuális magánhálózati internetes kapcsolattal (VPN).



→ **Közvetlen hívás**  
Közvetlen csatlakozás egy telefonszámhoz az internet nélkül.



- ←  Kapcsolódás munkahelyhez


## Beállítja az internetkapcsolatot a folytatás előtt?

A virtuális magánhálózati kapcsolatok használatához internetkapcsolat szükséges.

→ **Internetkapcsolat létrehozása**

→ **Internetkapcsolat beállítása később**


Itt internetcímnek a SZERVER IP-címét adjuk meg!

←  Kapcsolódás munkahelyhez

Írja be az internetcímet, amelyhez csatlakozni szeretne

Ezt a címet a rendszergazdától tudhatja meg.

Internetcím:	<input type="text" value="192.168.0.1"/>
Cél neve:	<input type="text" value="VPN-kapcsolat"/>


- ☐ Intelligens kártya használata
- ☒ Jegyezze meg a hitelesítő adataimat
-  ☐ A kapcsolat használatának engedélyezése más felhasználók számára  
A beállítás eredményeként a számítógéphez hozzáféréssel rendelkező felhasználók mindegyike használhatja a kapcsolatot.

Létrehozás

Mégse

Láthatjuk a „Vezérlőpult → Hálózat és internet → Hálózati és megosztási központ → Adapterbeállítások módosítása” menüpontot belül, hogy létrejött egy VPN-kapcsolat.

Ennek a tulajdonságait állítjuk be. Jobb klikkel a létrejött „VPN-kapcsolat”-ra kattintunk, majd „Tulajdonságok” menüpont, ezen belül a „Biztonság” része.


 Hálózati kapcsolatok


← → ▾ ▴

« Hálózat és internet » Hálózati kapcsolatok ▾ ↻

Keresés: Hálózati kap

Rendezés ▾ A kapcsolat indítása A kapcsolat átnevezése A kapcsolat törlése » ▢ ▾

 Ethernet 2  
teszt.hu  
Microsoft Hyper-V Network Adap...

 VPN-kapcsolat  
Kapcsolat bontva  
WAN Miniport (IKEv2)


Csatlakoztatás / Kapcsolat bontása


Állapot


Beállítás alapértelmezett kapcsolatként

Másolat készítése

Parancsikon létrehozása

 Törlés

 Átnevezés

 Tulajdonságok

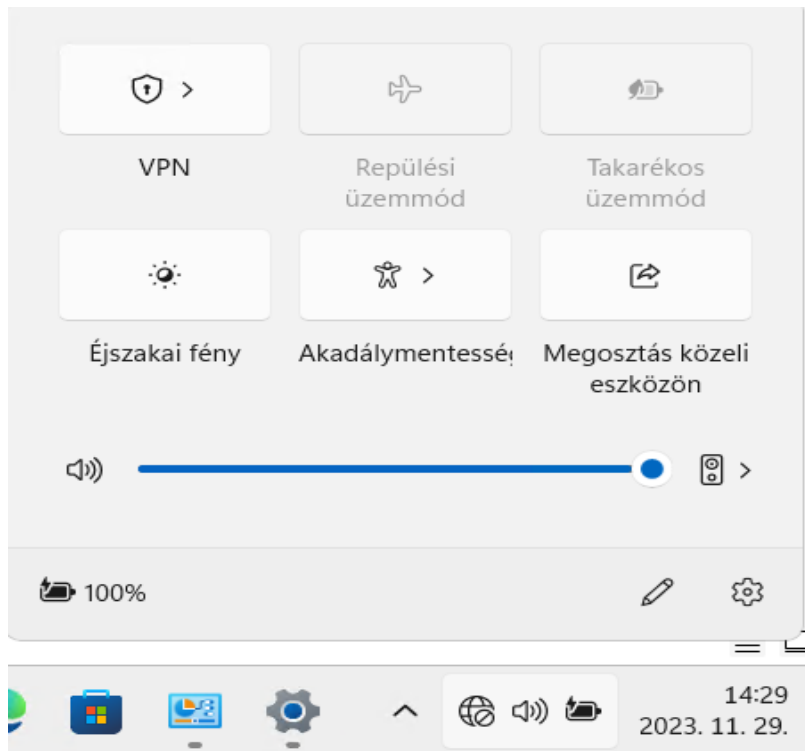
Mivel L2TP hitelesítést állítottunk be, ezért L2TP típus állítunk be a kliens oldalon is, valamint a protokollok típusai is ugyanazok legyenek, mint a szerveren!

The screenshot shows the 'VPN-kapcsolat tulajdonságai' (VPN Connection Properties) dialog box with the 'Biztonság' (Security) tab selected. The 'Virtuális magánhálózat típusa:' (Virtual Private Network type:) dropdown is set to 'L2TP IPsec mellett (L2TP/IPSec)'. The 'Adattitkosítás:' (Data encryption:) dropdown is set to 'Nem kötelező titkosítás (kapcsolódás titkosítás nélkül is)' (No mandatory encryption (connection encryption optional)). Under the 'Hitelesítés' (Authentication) section, the 'A következő protokollok engedélyezése' (Allow the following protocols) radio button is selected. The 'MS-CHAPv2 protokoll' (MS-CHAPv2 protocol) checkbox is checked, while 'EAP protokoll használata' (Use EAP protocol), 'Titkosítatlan jelszó (PAP)' (Unencrypted password (PAP)), 'CHAP protokoll' (CHAP protocol), and 'A Windows bejelentkezési név és jelszó (valamint tartomány, ha van) automatikus használata' (Automatic use of Windows logon name and password (and domain, if any)) are unchecked. The 'Speciális beállítások' (Advanced settings) button is visible. At the bottom are 'OK' and 'Mégse' (Cancel) buttons.

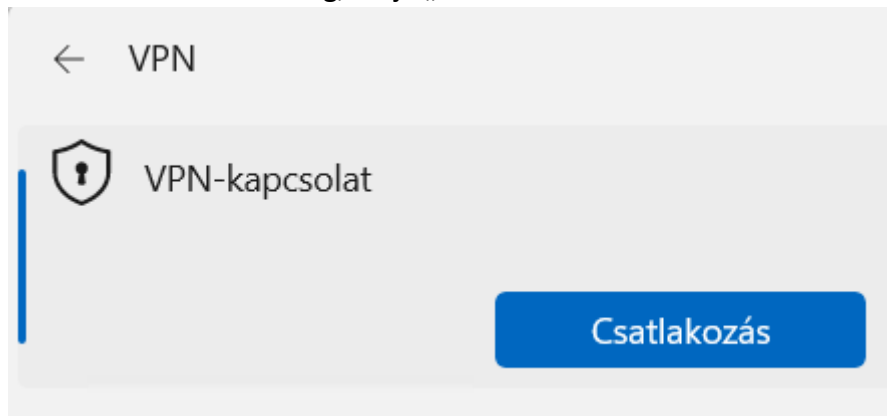
Rákattintunk a „Speciális beállítások”-ra, majd az „Előre megosztott kulcs használata hitelesítéshez” pontot bejelölve, megadjuk a Szerveren megadott kulcsot!

The screenshot shows the 'Speciális tulajdonságok' (Advanced properties) dialog box with the 'L2TP' tab selected. The 'Előmegosztott kulcs használata hitelesítéshez' (Use pre-shared key for authentication) radio button is selected. The 'Kulcs:' (Key:) text box contains the value 'Vizsga2023'. The 'Tanúsítvány használata a hitelesítéshez' (Use certificate for authentication) radio button is unselected. The checkbox 'A kiszolgáló tanúsítványában szereplő Név és Használat attribútum ellenőrzése' (Check Name and Usage attributes in the server's certificate) is checked. The background shows the 'Biztonság' tab of the 'VPN-kapcsolat tulajdonságai' dialog box.

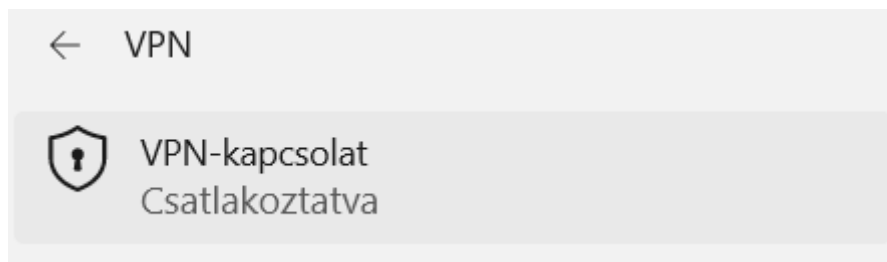
Ezek után a VPN kapcsolatot felépítjük.



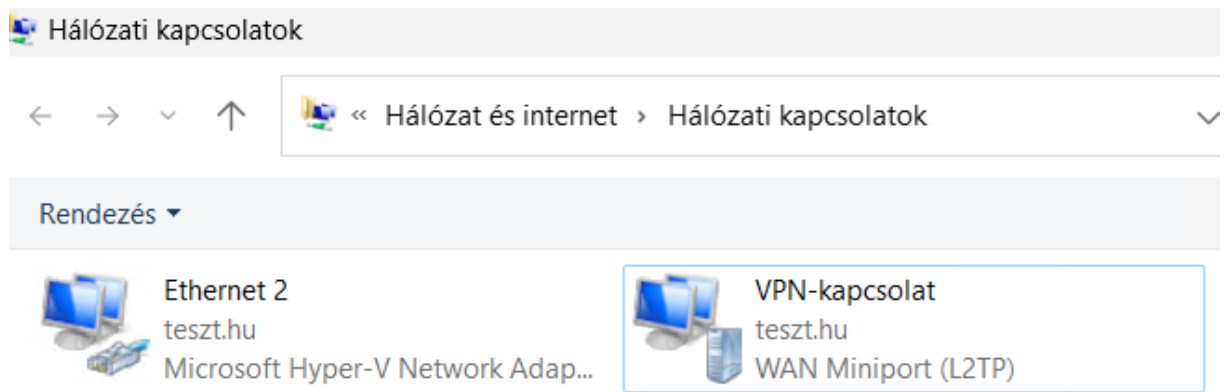
Ezen belül VPN lehetőség, majd „Csatlakozás”.



A „Rendszergazda” fiókjával és jelszavával hozzuk létre a VPN-kapcsolatot!



A kapcsolat létrejött!



**Készítették:**

- **Fülöp Gergő**
- **Csobi László**
- **Nagy János**