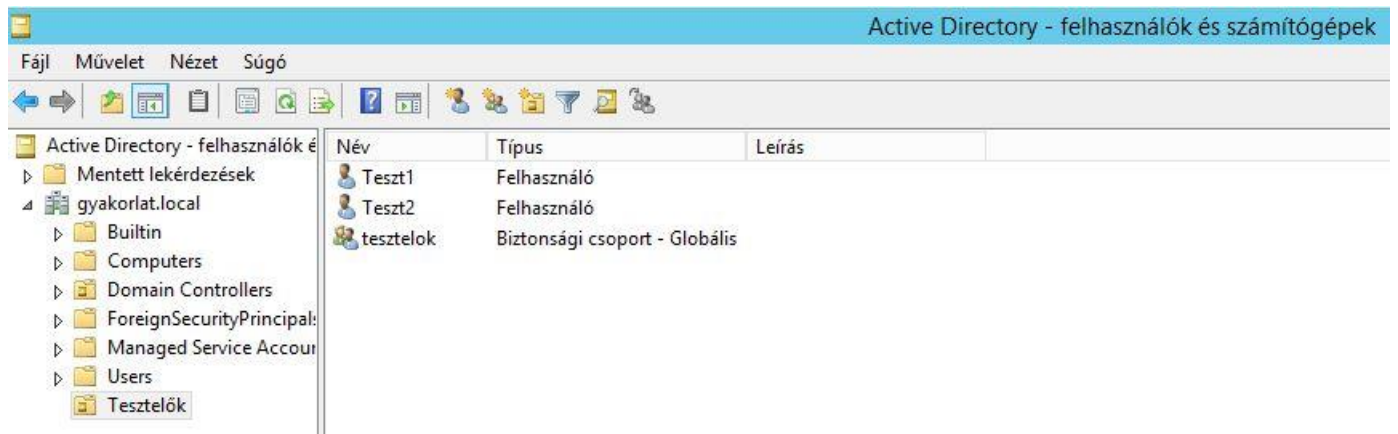
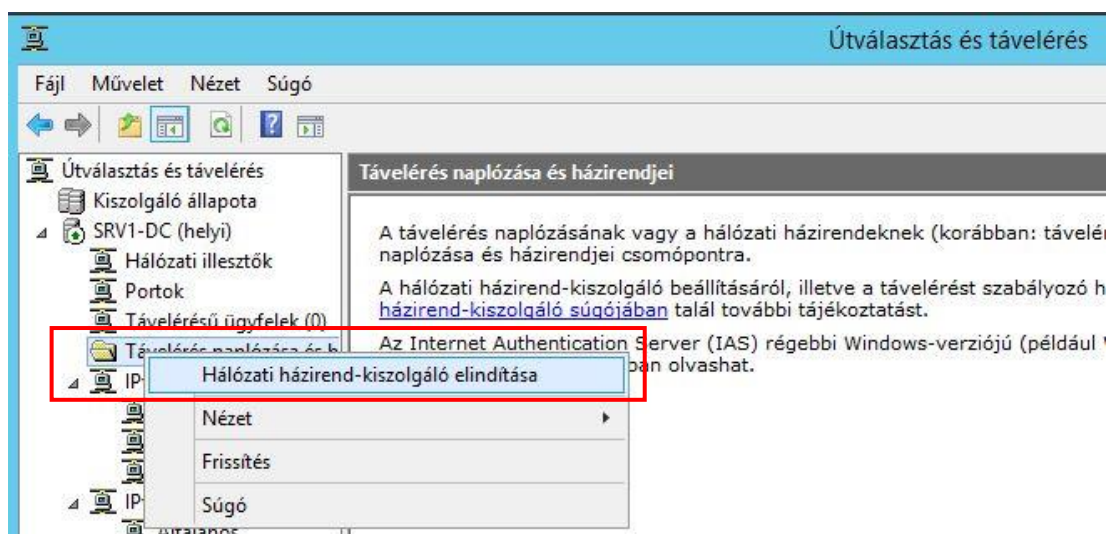


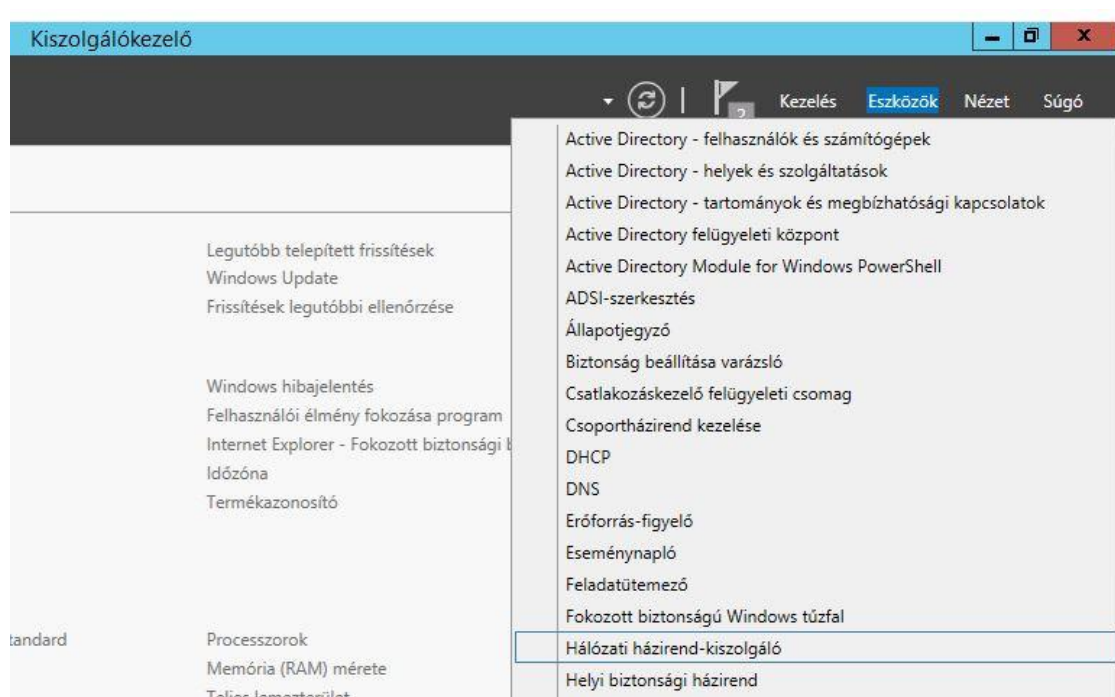
A **Hálózati házirend-kiszolgáló** konfigurálása előtt hozzunk létre néhány **teszt** felhasználót:



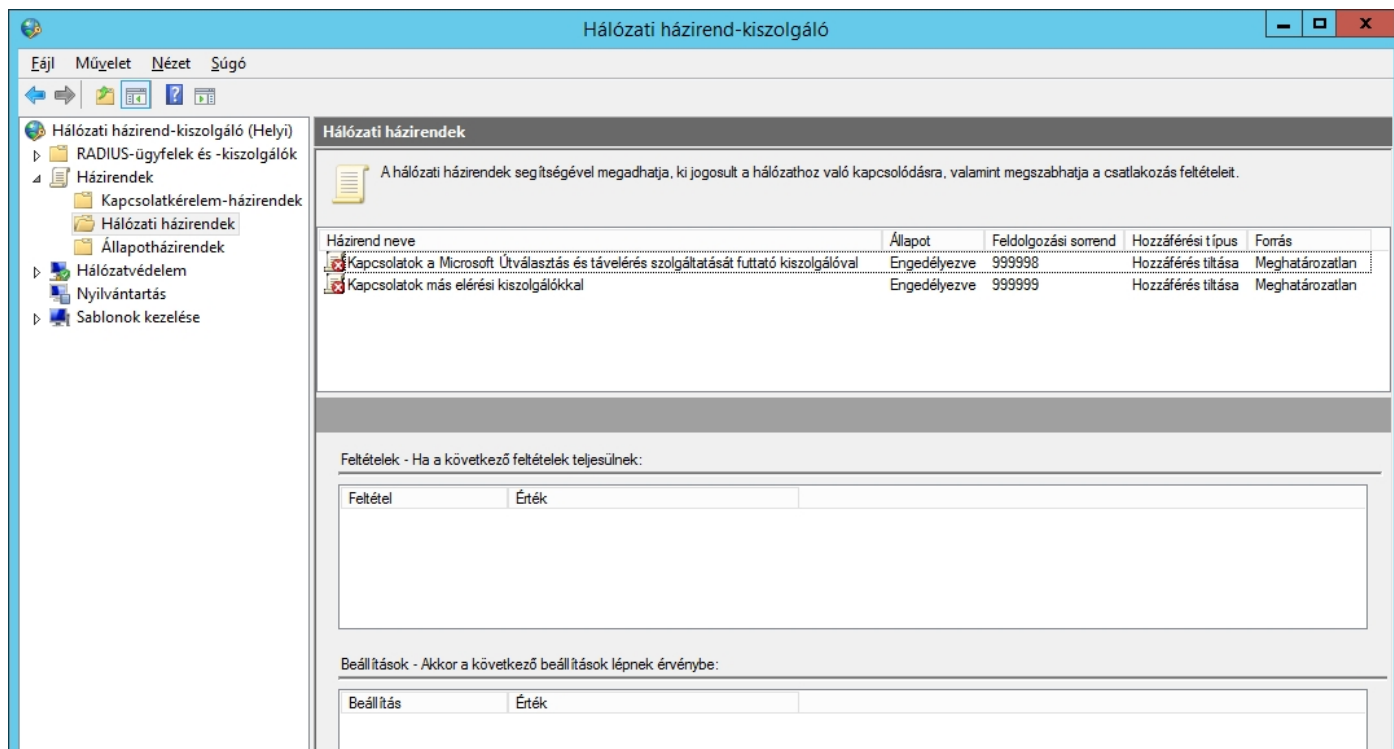
A Hálózati házirend-kiszolgáló kezelőjét elindíthatjuk közvetlenül a *Útválasztás és távelérés kiszolgáló kezelőből* is. A **Távelérés naplózása és házirendjei** konzolra részről: ez esetben *csak a Táveléréshez szükséges nézetben* indul el:



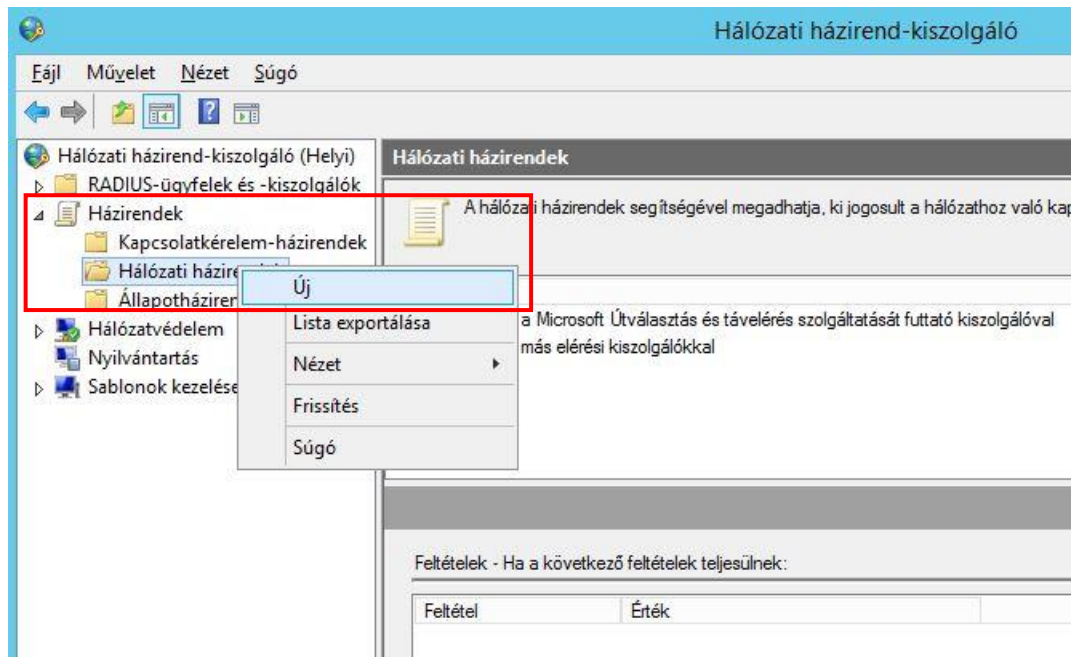
Azonban, ha minden funkciót szeretnénk elérni a Hálózati házirend-kiszolgáló kezelőjében akkor indítsuk a **Kiszolgálókezelő / Eszközök / Hálózati házirend-kiszolgáló kezelő**:



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




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



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:**

**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.

☒ Hálózat-hozzáférési kiszolgáló típusa:

☐ Szállítóspecifikus:

Vissza

Tovább


Befejezés

Mégse

### Feltételek:

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

Új hálózati házirend



### Feltételek megadása

Adja meg azokat a feltételeket, amelyek meghatározzák, hogy a hálózati házirend ki lesz-e értékelve a kapcsolatkérelmekhez. Legálább egy feltételt kell megadni.

Feltétel	Érték
----------	-------

Feltétel leírása:

Hozzáadás...

Szerkesztés...

Elávolítás

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

szombat

vasárnap

hétfő - péntek, 8:00 - 18:00

OK

Mégse

☒ Engedélyezve

☐ Megtagadva


Egy feltétel megadva (minden VPN kapcsolat létrejöhet, ha ennek a feltételnek megfelel). Azonban, ha nem teljesül ez a feltétel, a rendszer már nem is vizsgálja a további feltételeket, a következő házirend szabályra ugrik:

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
 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

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... Szerkesztés... 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:

Új hálózati házirend

### Hozzáférési engedély megadása

Annak konfigurálása, hogy megadni vagy megtagadni kívánja-e a hálózati hozzáférést, ha a kapcsolatkérelmek 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.

Vissza Tovább Befejezés Mégse



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

Új hálózati házirend

### Hitelesítési módszerek konfigurálása

Konfiguráljon egy vagy több, a kapcsolatkérelem-házirendnek való megfeleléséhez szükséges hitelesítési módszert. EAP hitelesítés esetén be kell állítania az EAP típusát is. Ha NAP-kapcsolatot hoz létre 802.1X vagy VPN használatával, akkor védett EAP beállítása szükséges a kapcsolatkérelem-házirendben, ami felülbírálja a hálózati házirend hitelesítési beállításait.

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 lejártá után is módosíthatja
- ☒ Microsoft titkosított hitelesítés (MS-CHAP)
- ☒ A felhasználó a jelszót lejártá után is módosíthatja
- ☐ Titkosított hitelesítés (CHAP)
- ☐ Titkosítatlan hitelesítés (PAP, SPAP)
- ☐ Az ügyfelek a hitelesítési módszer egyeztetése nélkül is kapcsolódhatnak.
- ☐ Csak a számítógép állapotának ellenőrzése

Vissza Tovább Befejezés Mégse

Adjuk hozzá a megbízhatóbb EAP-MSCHAPv2 hitelesítési módszert:

Új hálózati házirend

### Hitelesítési módszerek konfigurálása

Konfiguráljon egy vagy több, a kapcsolatkérelem-házirendnek való megfeleléséhez szükséges hitelesítési módszert. EAP hitelesítés esetén be kell állítania az EAP típusát is. Ha NAP-kapcsolatot hoz létre 802.1X vagy VPN használatával, akkor védett EAP beállítása szükséges a kapcsolatkérelem-házirendben, ami felülbírálja a hálózati házirend hitelesítési beállításait.

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

**EAP-típusok:**

Hozzáadás...

Szerkesztés...

Eltávolítás

**Kevésbé biztonságos hitelesítési módszerek:**

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

Vissza Tovább Befejezés Mégse

**EAP hozzáadása**

Hitelesítési módszerek:


- Microsoft: Intelligens kártya vagy más tanúsítvány
- Microsoft: Védett EAP (PEAP)
- ☒ Microsoft: Biztonságos jelszó (EAP-MSCHAP v2)

< III >

OK Mégse

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

Új hálózati házirend



### Hitelesítési módszerek konfigurálása

Konfiguráljon egy vagy több, a kapcsolatkérelem-házirendnek való megfeleléséhez szükséges hitelesítési módszert. EAP hitelesítés esetén be kell állítania az EAP típusát is. Ha NAP-kapcsolatot hoz létre 802.1X vagy VPN használatával, akkor védett EAP beállítása szükséges a kapcsolatkérelem-házirendben, ami felülbírálja a hálózati házirend hitelesítési beállításait.

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

**EAP-típusok:**

Microsoft: Biztonságos jelszó (EAP-MSCHAP v2)

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.
- ☐ Csak a számítógép állapotának ellenőrzése

Vissza Tovább Befejezés Mégse

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

Új hálózati házirend



### Korlátozások konfigurálása

A korlátozások a hálózati házirend olyan további paraméterei, amelyeknek a kapcsolatkérelmeknek meg kell felelniük. Ha egy korlátozásnak a kapcsolatkérelmek nem felelnek meg, a hálózati házirend-kiszolgáló automatikusan visszautasítja azokat. A korlátozások megadása nem kötelező. Ha nem kíván korlátozásokat konfigurálni, kattintsan a Tovább gombra.

Hálózati házirend korlátozásainak konfigurálása.  
Ha a kapcsolódási kérelem nem felel meg minden megkötésnek, a hálózati hozzáférés meg lesz tagadva.

**Korlátozások:**

**Korlátozások**

- Üresjárat időkorlátja
- Kapcsolat-időtűllépés
- Hívott állomás azonosítója
- Nap és időpont korlátozásai
- NAS-porttípus

Adja meg azt a maximális időt percben, amelyet a kiszolgáló üresjáratban tölthet a kapcsolat bontása előtt

☐ A kapcsolat bontása a maximális üresjárat idő letelte után

1

Vissza Tovább Befejezés Mégse

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!*

Új hálózati házirend

### Beállítások konfigurálása

A hálózati házirend-kiszolgáló akkor alkalmazza a beállításokat a kapcsolatkérelemre, ha a hálózati házirend feltételei és korlátozásai teljesülnek.

A hálózati házirend beállításainak konfigurálása.  
A beállítások érvénybe lépnek, ha a feltételek és korlátozások megfelelnek a kapcsolódási kérelemnek, és a házirend engedélyezi a hozzáférést.

**Beállítások:**

- RADIUS-attribútumok**
  - Szabványos
  - ☒ Szállítóspecifikus
- Hálózati védelem**
  - NAP-kényszerítés
  - Kiterjesztett állapot
- Útválasztás és távélérés**
  - Multilink és BAP protokoll
  - IP-szűrők
  - Titkosítás**
  - ☒ IP-beállítások

A titkosítási beállításokat a Microsoft Útválasztás és távélérés szolgáltatását futtató számítógépek támogatják.

Ha más hálózati hozzáférést biztosító kiszolgálókat használ a telefonos vagy virtuális magánhálózati kapcsolatokhoz, győződjön meg arról, hogy a kiszolgálók támogatják a kijelölt titkosítási beállításokat.

Ha csak a Nincs titkosítás lehetőséget jelöli be, az ügyfelek és a hálózati távélérési kiszolgáló adatforgalma nem lesz titkosítva. Ez a konfiguráció nem ajánlott.

- ☒ Alapszintű titkosítás (MPPE 40 bites)
- ☒ Erős titkosítás (MPPE 56 bites)
- ☒ A legerősebb titkosítás (MPPE 128 bites)
- ☒ Nincs titkosítás

Vissza Tovább Befejezés Mégse

Elkészült a házirendünk 😊

Új hálózati házirend

### Új hálózati házirend befejezése

Sikeresen létrehozta a következő hálózati házirendet:

**VPN - mindenkinek**

**A házirend feltételei:**

Feltétel	Érték
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

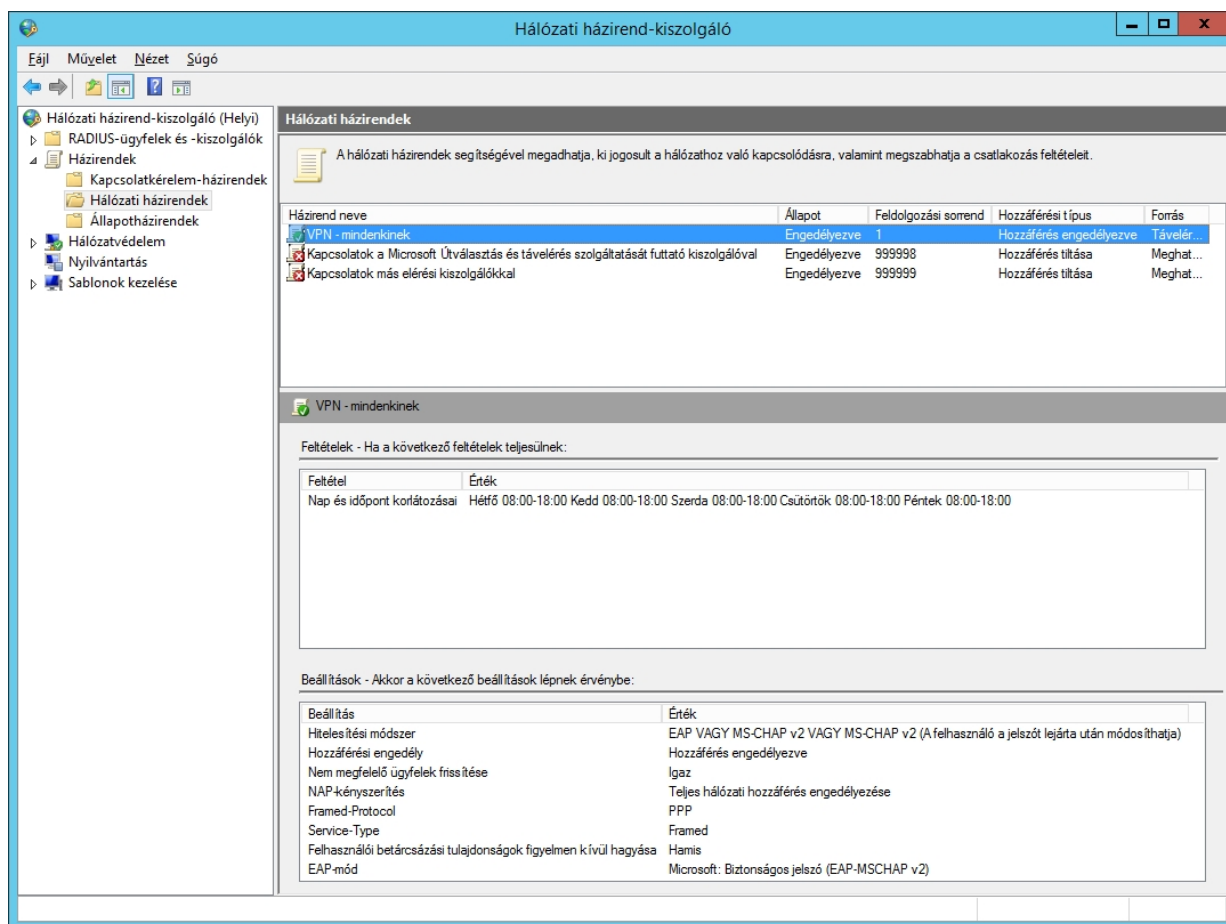
**Házirend beállításai:**

Feltétel	Érték
Hitelesítési módszer	EAP VAGY MS-CHAP v2 VAGY MS-CHAP v2 (A felhasználó a ...
Hozzáférési engedély	Hozzáférés engedélyezve
Nem megfelelő ügyfelek frissítése	Igaz
NAP-kényszerítés	Teljes hálózati hozzáférés engedélyezése
Framed-Protocol	PPP
Service-Type	Framed

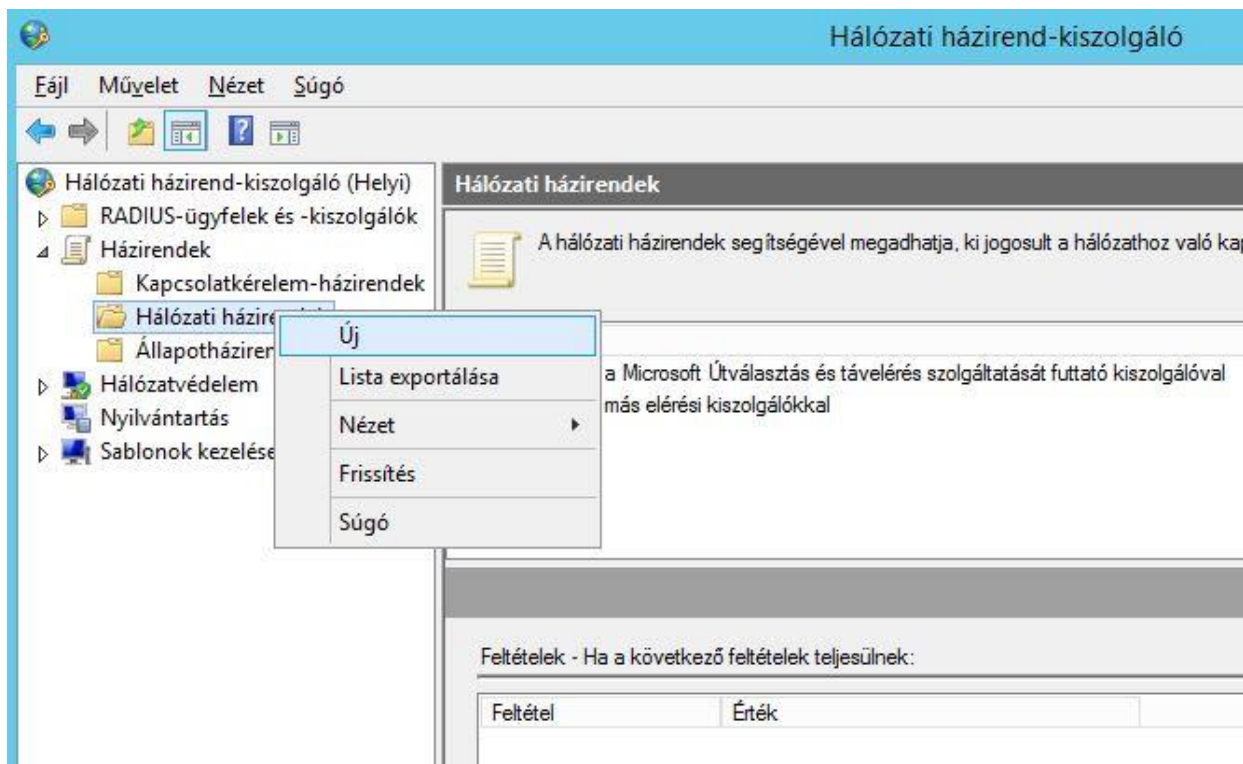
A varázsló bezárásához kattintson a Befejezés gombra.

Vissza Tovább Befejezés Mégse

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

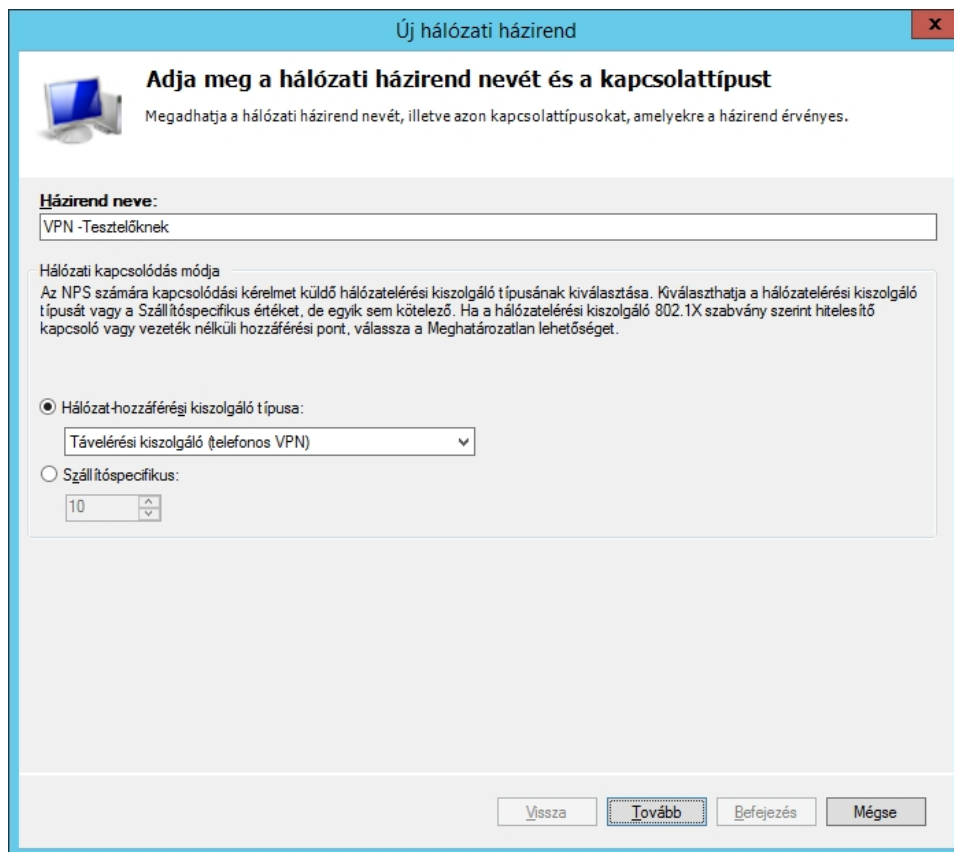


Hozzunk létre egy új hálózati házirendet a **Tesztelők** csoportunknak, **csak L2TP protokoll** és **EAP hitelesítési módszer** legyen használható

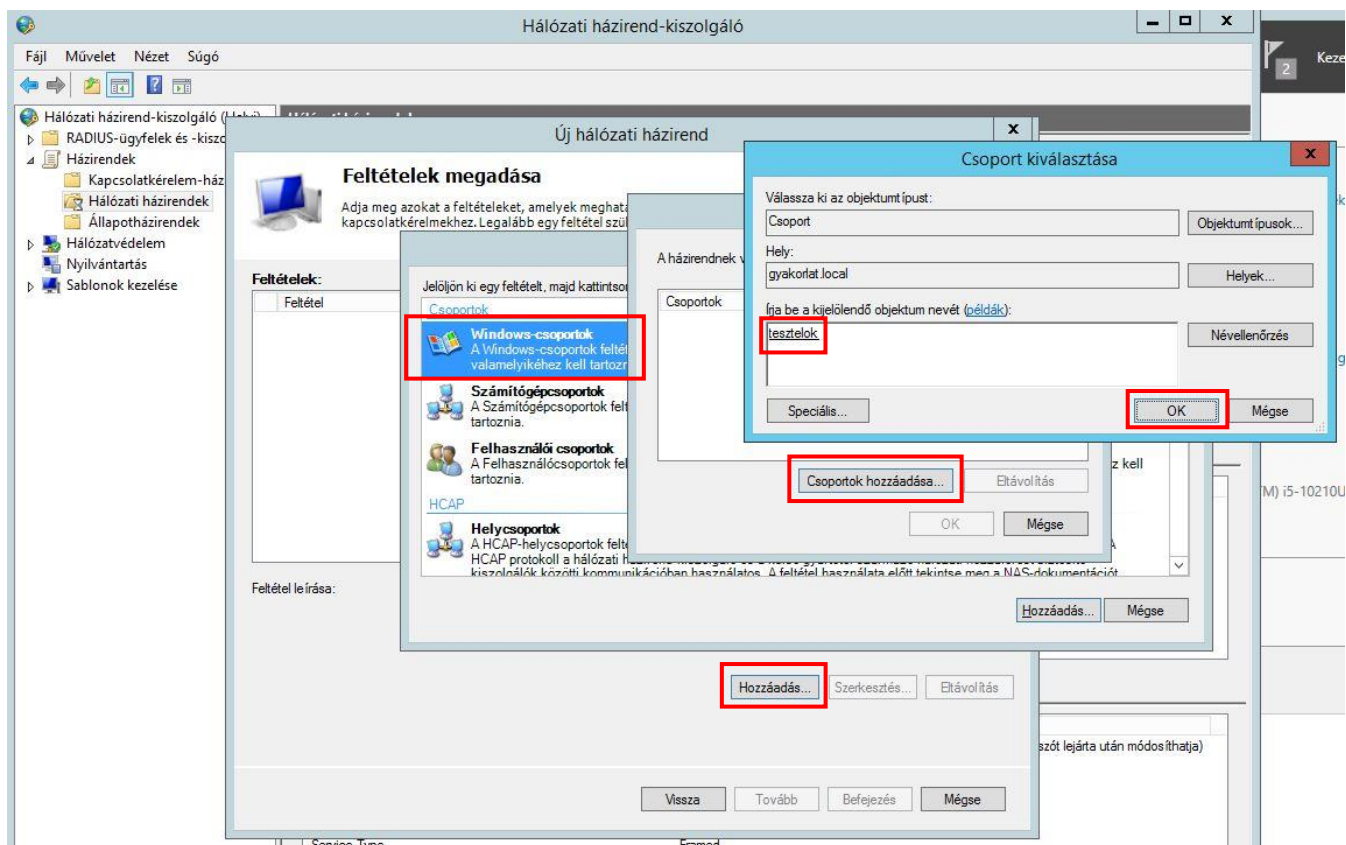




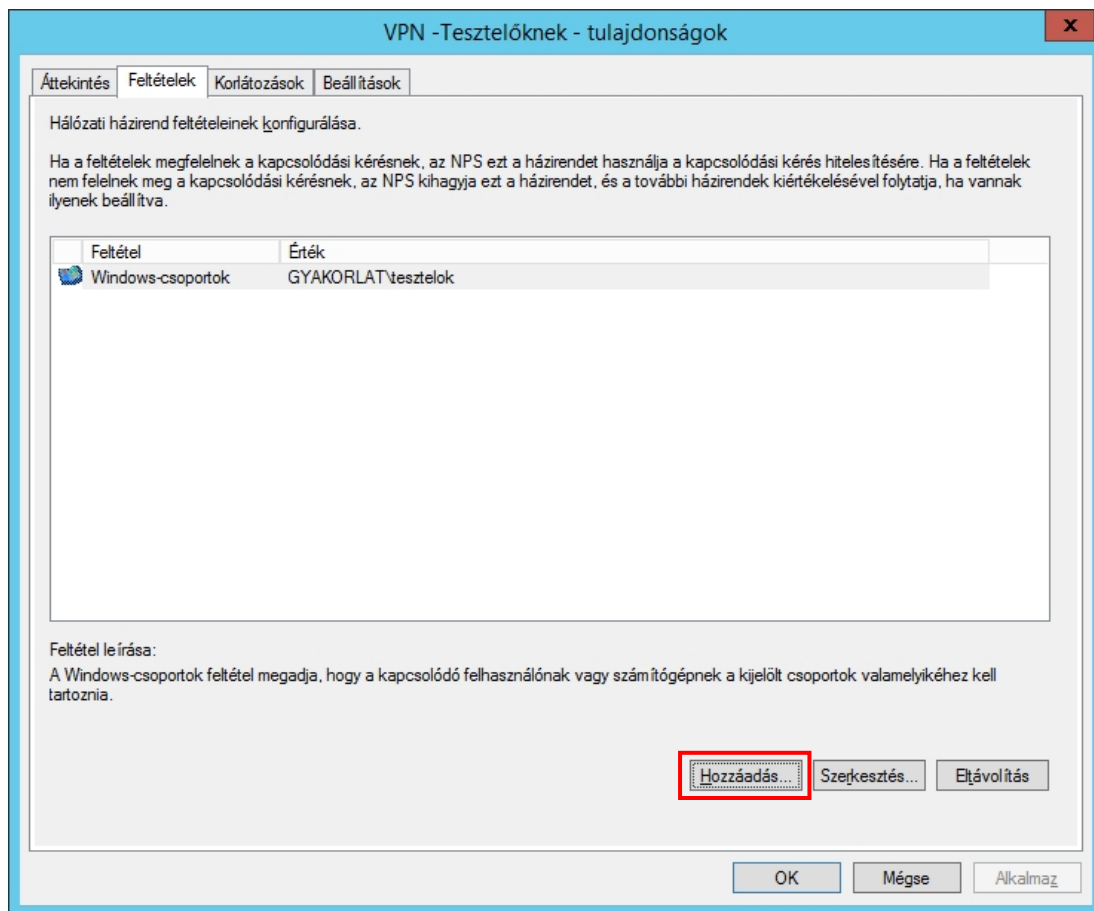
Adjunk nevet a házirendünknek és válasszunk hálózat-hozzáférési típust:



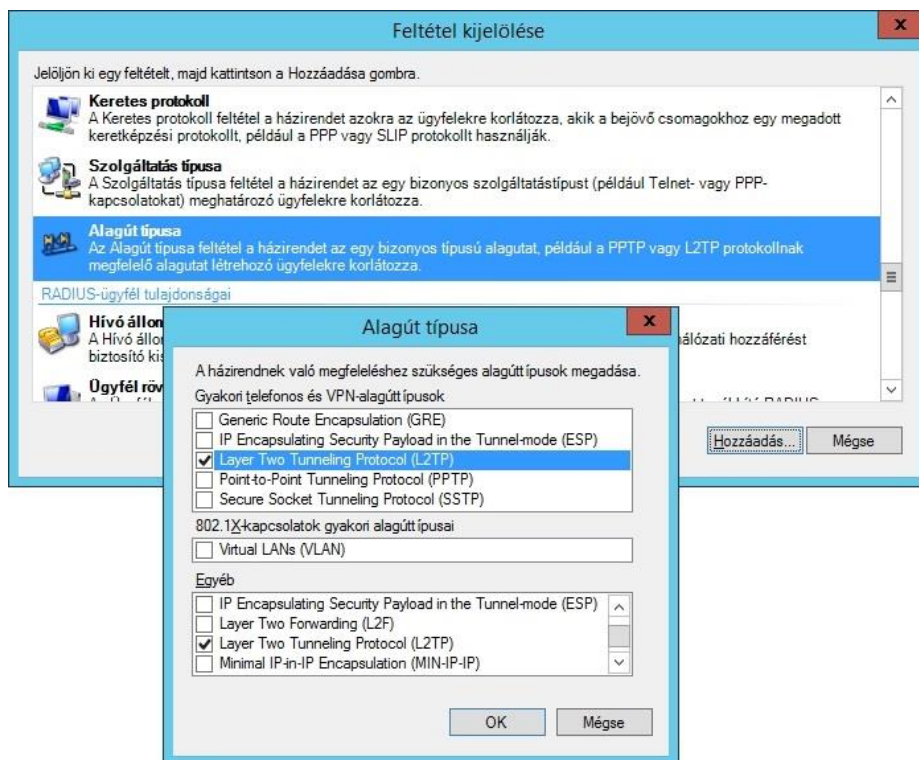
Feltételként adjuk meg Windows csoportunkat: **tesztelok**



Azonban most vegyünk fel egy további feltételt:



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



Feltételek megadva:

The screenshot shows the 'VPN - Tesztelőknek - tulajdonságok' (VPN - For Testers - Properties) dialog box, specifically the 'Feltételek' (Conditions) tab. The window title is 'VPN - Tesztelőknek - tulajdonságok'. The tab bar at the top includes 'Áttekintés', 'Feltételek', 'Korlátozások', and 'Beállítások'. The main text area contains the following information:

Hálózati házirend feltételeinek konfigurálása.

Ha a feltételek megfelelnek a kapcsolódási kérésnek, az NPS ezt a házirendet használja a kapcsolódási kérés hitelesítésére. Ha a feltételek nem felelnek meg a kapcsolódási kérésnek, az NPS kihagyja ezt a házirendet, és a további házirendek kiértékelésével folytatja, ha vannak ilyenek beállítva.

Feltétel	Érték
Windows-csoportok	GYAKORLAT\tesztelők
Alagút típusa	Layer Two Tunneling Protocol (L2TP)

Feltétel leírása:  
Az Alagút típusa feltétel a házirendet az egy bizonyos típusú alagutat, például a PPTP vagy L2TP protokollnak megfelelő alagutat létrehozó ügyfelekre korlátozza.

Buttons at the bottom: Hozzáadás..., Szerkesztés..., Eltávolítás, OK, Mégse, Alkalmaz.

**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:

The screenshot shows the 'Új hálózati házirend' (New Network Policy) dialog box, specifically the 'Hozzáférési engedély megadása' (Access Permission) tab. The window title is 'Új hálózati házirend'. The tab bar at the top includes 'Hozzáférési engedély megadása'. The main text area contains the following information:

Hozzáférési engedély megadása

Annak konfigurálása, hogy megadni vagy megtagadni kívánja-e a hálózati hozzáférést, ha a kapcsolatkérellem 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.

Buttons at the bottom: Vissza, Tovább, Befejezés, Mégse.

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

Új hálózati házirend

### Hitelesítési módszerek konfigurálása

Konfiguráljon egy vagy több, a kapcsolatkérelem-házirendnek való megfeleléséhez szükséges hitelesítési módszert. EAP hitelesítés esetén be kell állítania az EAP típusát is. Ha NAP-kapcsolatot hoz létre 802.1X vagy VPN használatával, akkor védett EAP beállítása szükséges a kapcsolatkérelem-házirendben, ami felülbírálja a hálózati házirend hitelesítési beállításait.

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 lejártá után is módosíthatja
- ☐ Microsoft titkosított hitelesítés (MS-CHAP)
  - ☐ A felhasználó a jelszót lejártá után is módosíthatja
- ☐ Titkosított hitelesítés (CHAP)
- ☐ Titkosítatlan hitelesítés (PAP, SPAP)
- ☐ Az ügyfelek a hitelesítési módszer egyeztetése nélkül is kapcsolódhatnak.
- ☐ Csak a számítógép állapotának ellenőrzése

Vissza Tovább Befejezés Mégse

Adjuk hozzá az EAP-MSCHAPv2 hitelesítési módszert:

Új hálózati házirend

### Hitelesítési módszerek konfigurálása

Konfiguráljon egy vagy több, a kapcsolatkérelem-házirendnek való megfeleléséhez szükséges hitelesítési módszert. EAP hitelesítés esetén be kell állítania az EAP típusát is. Ha NAP-kapcsolatot hoz létre 802.1X vagy VPN használatával, akkor védett EAP beállítása szükséges a kapcsolatkérelem-házirendben, ami felülbírálja a hálózati házirend hitelesítési beállításait.

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 lejártá után is módosíthatja
- ☐ Microsoft titkosított hitelesítés (MS-CHAP)
  - ☐ A felhasználó a jelszót lejártá után is módosíthatja
- ☐ Titkosított hitelesítés (CHAP)
- ☐ Titkosítatlan hitelesítés (PAP, SPAP)
- ☐ Az ügyfelek a hitelesítési módszer egyeztetése nélkül is kapcsolódhatnak.
- ☐ Csak a számítógép állapotának ellenőrzése

**EAP hozzáadása**

Hitelesítési módszerek:

- Microsoft: Intelligens kártya vagy más tanúsítvány
- Microsoft: Védett EAP (PEAP)
- Microsoft: Biztonságos jelszó (EAP-MSCHAP v2)**

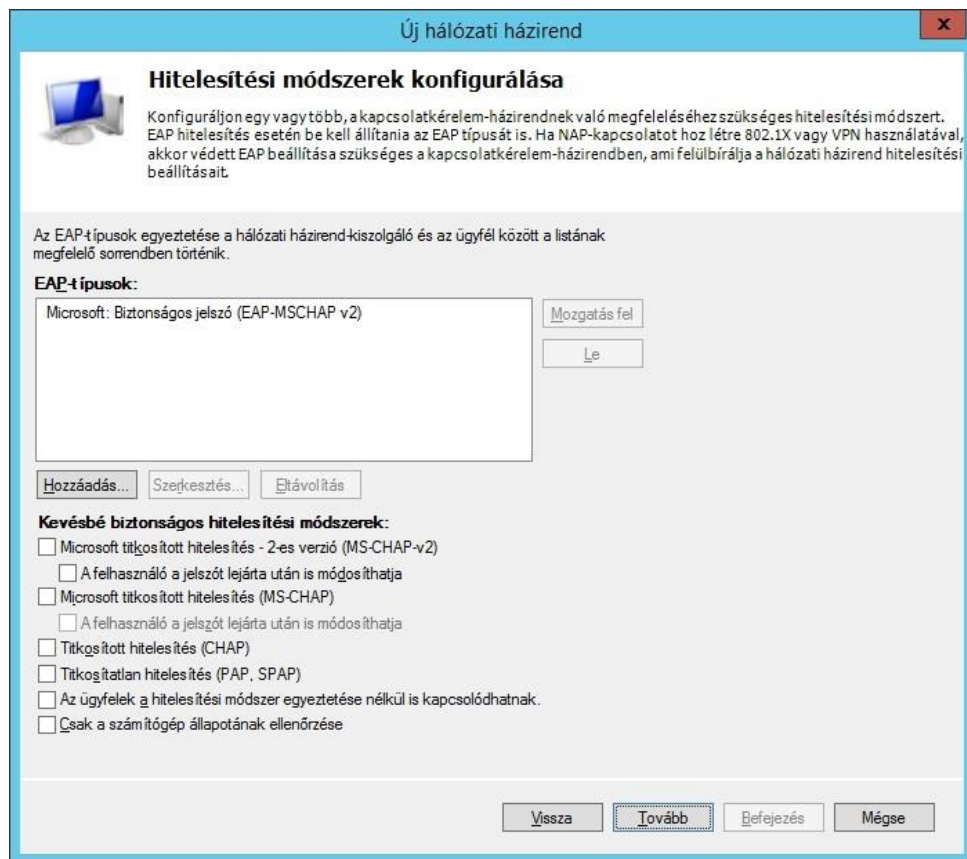
< III >

OK Mégse

Vissza Tovább Befejezés Mégse



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



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

Elkészültek az **engedélyező** hálózati házirendjeink:

