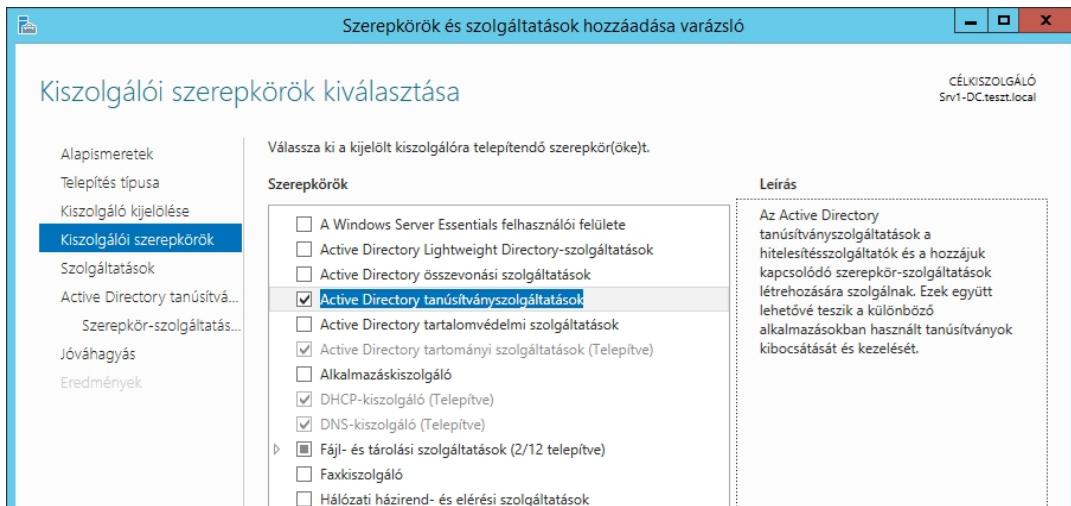


SSL tanúsítvány kérése AD-ban

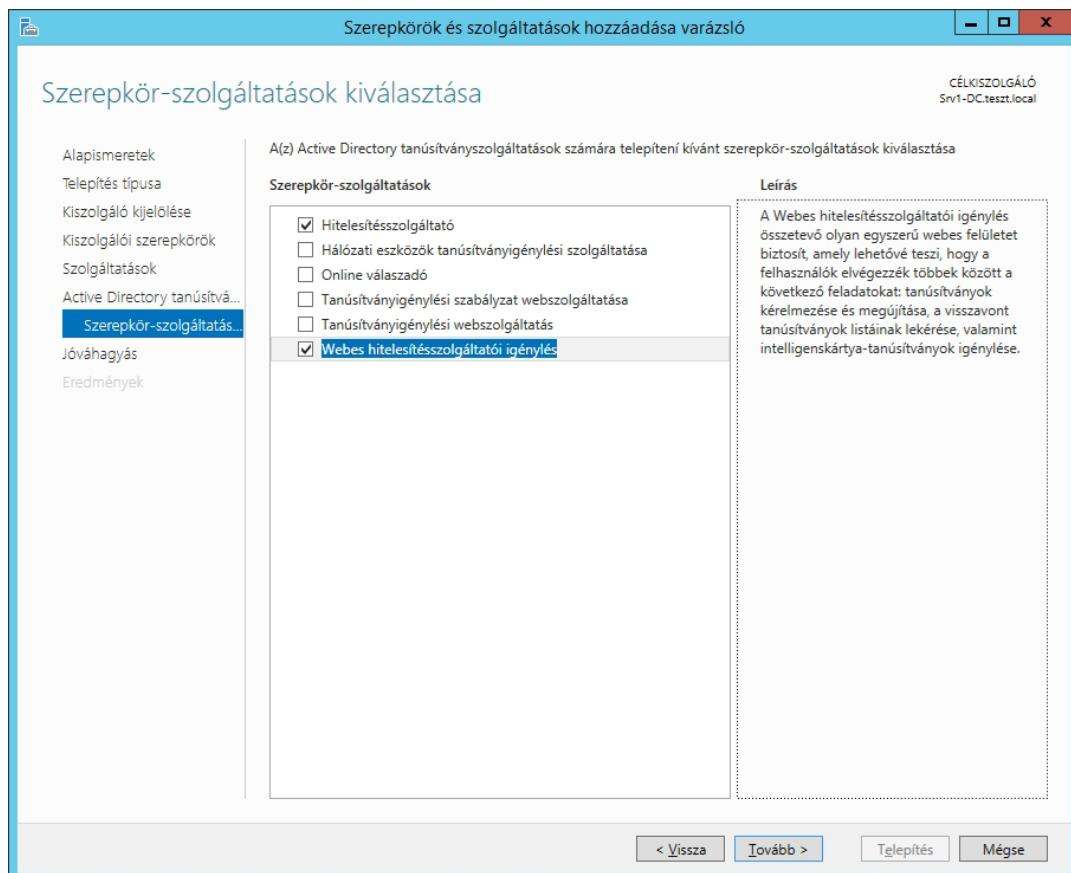
A kliens gépet léptessük be az Active Directory-be, a szerveren és a kliensen is kapcsoljuk be a tűzfalat a bejövő forgalomnál. A webhely működéséhez a 80-as és a 443-as portokat engedélyeznünk kell a bejövő forgalom esetén. A tűzfalról és annak beállításairól még nem volt szó, ez csak egy kis bemelegítésképpen van most benne a leírásban.

Weblapok biztonságos eléréséhez szükség van SSL tanúsítványra (HTTPS elérés). Ebben a feladatban Active Directory használatával valósítjuk meg a tanúsítvány kérését. Ehhez szükségünk van a megfelelő szerepkörökre.

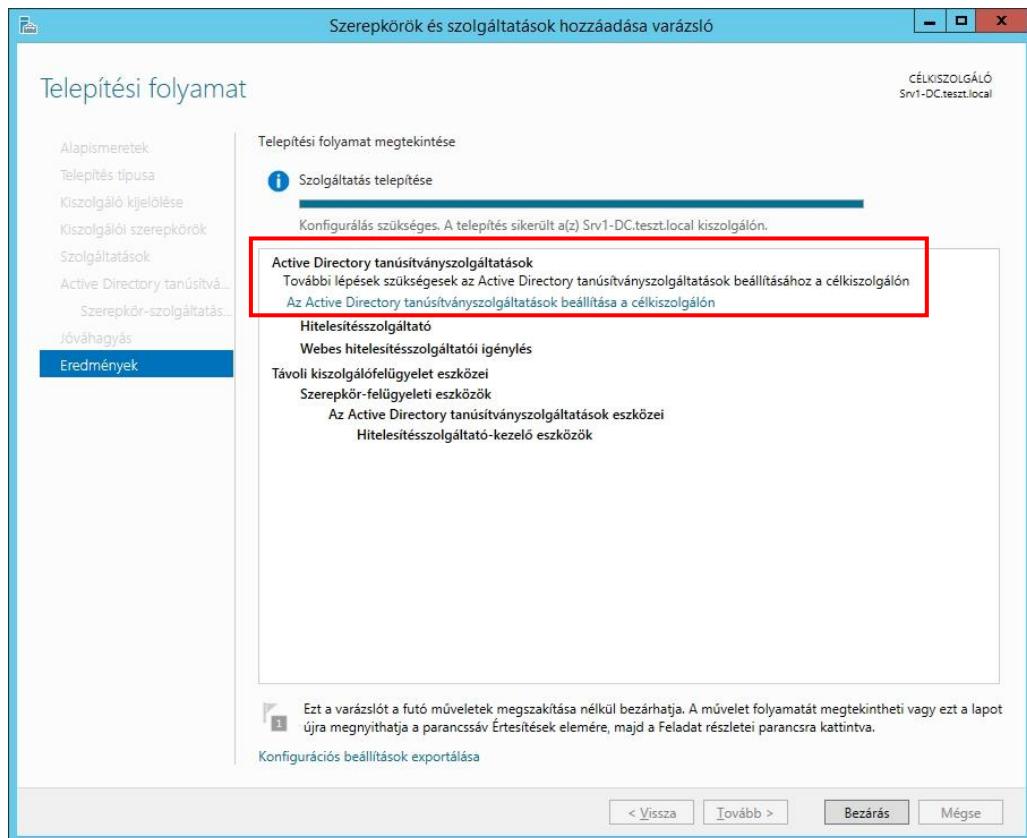
Telepítünk az **Active Directory tanúsítványszolgáltatások** szerepkört:



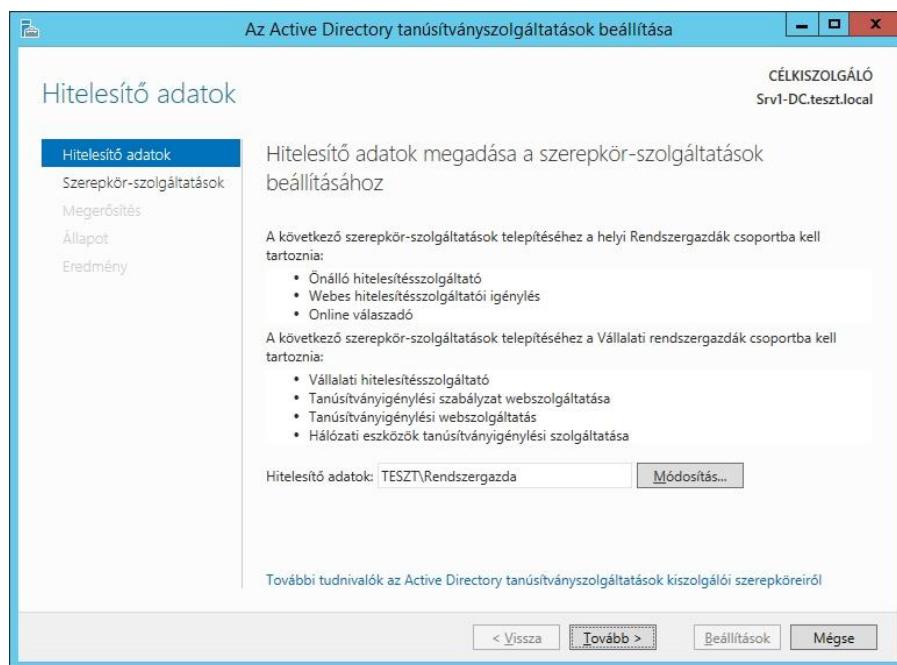
A következő ablakban kiválasztjuk a telepíteni kívánt szolgáltatások közül a **Hitelesítésszolgáltató** és a **Webes hitelesítésszolgáltatói igénylés** nevű szerepkör-szolgáltatásokat. Kattintsuk a **Tovább** gombra.



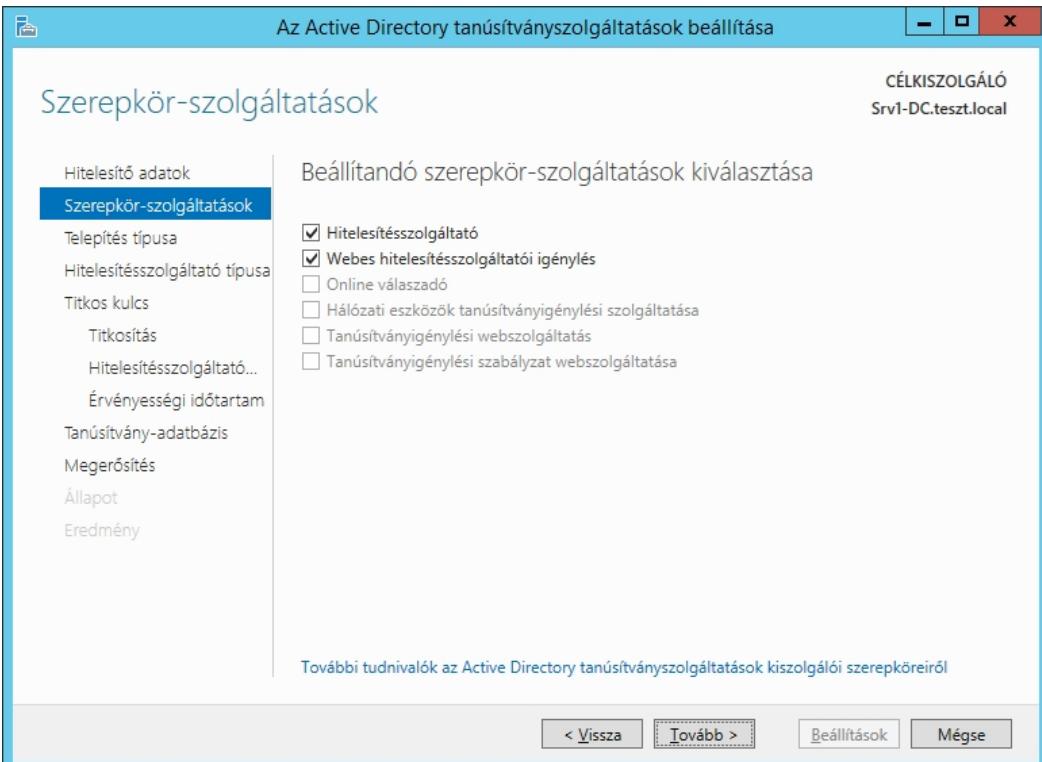
Elkészült a telepítés, következhet a Tanúsítványszolgáltatások beállítása: (kattintsunk a linkre)



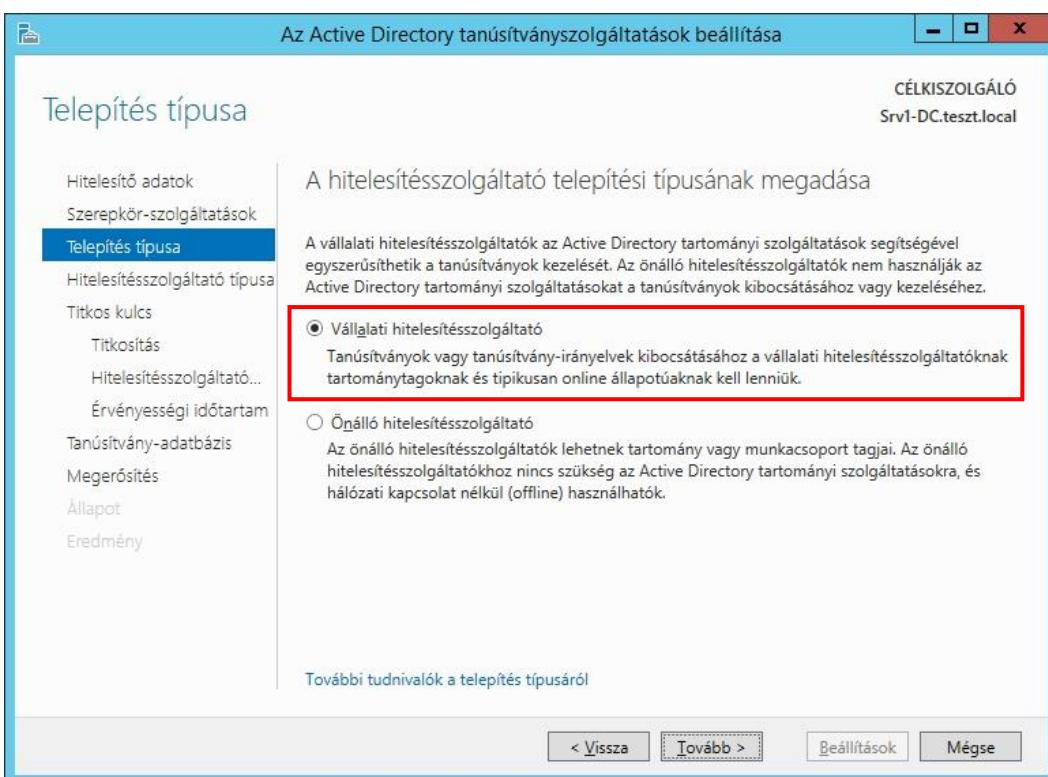
A Rendszergazda fiókot adjuk meg, mint hitelesítő felhasználót



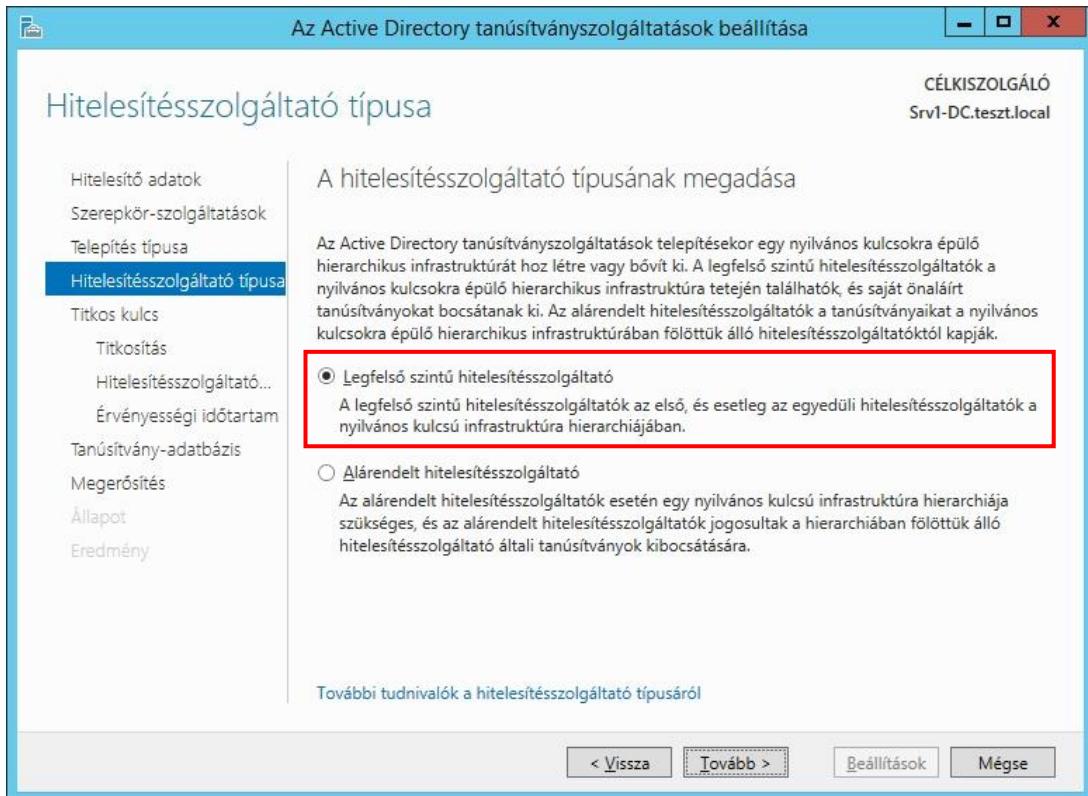
Válasszuk ki az ábrán látható szerepkör-szolgáltatásokat



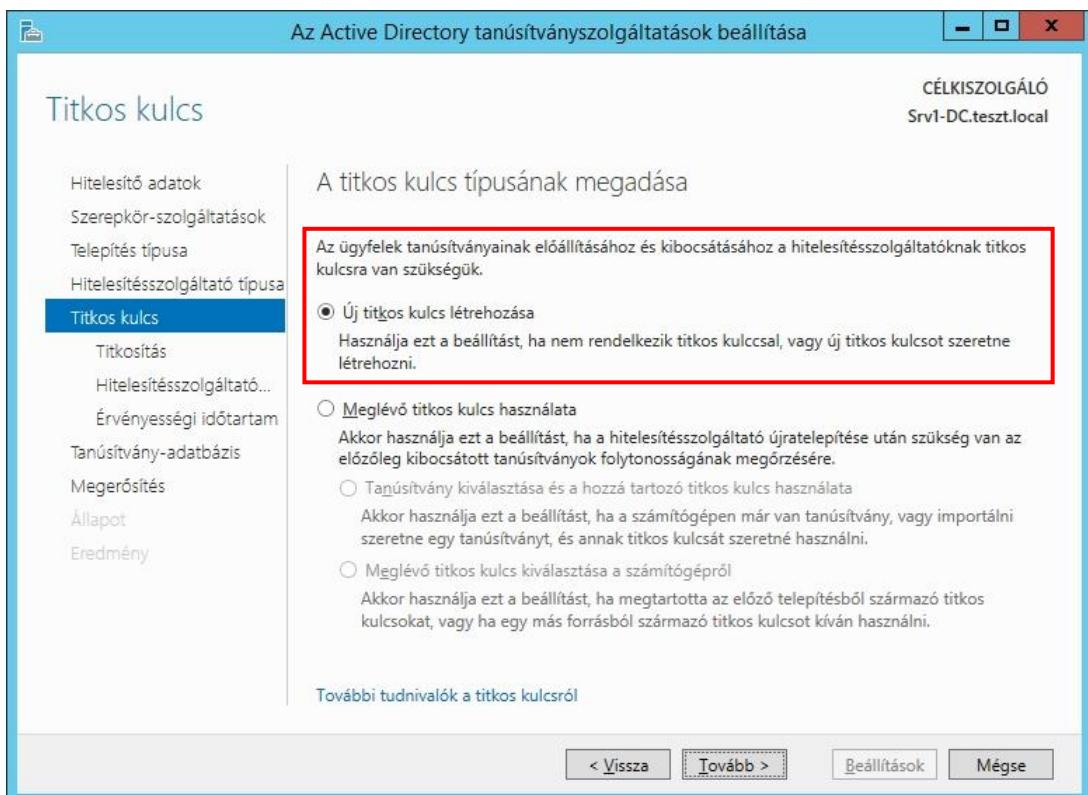
Active Directory esetén (és csak ekkor) választhatjuk a **Vállalati hitelesítésszolgáltató** telepítési típust:



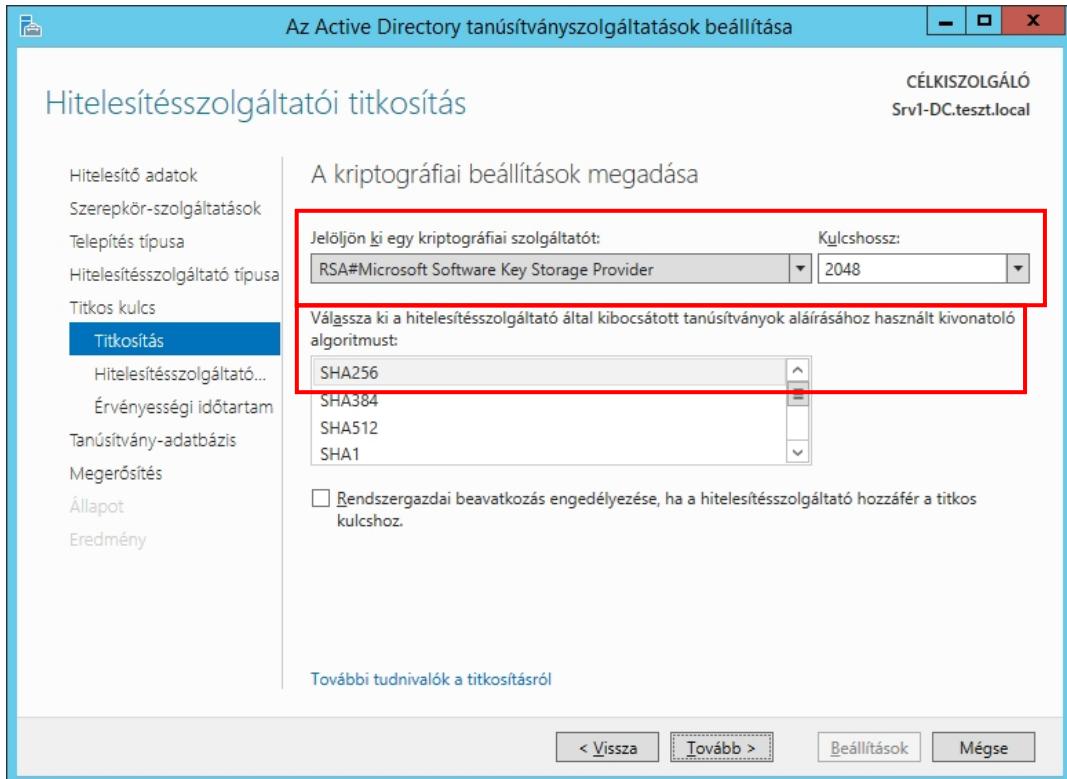
Az kiszolgálónk az első a tartományon belül, mindenkorban **Legfelső szintű hitelesítésszolgáltató** legyen



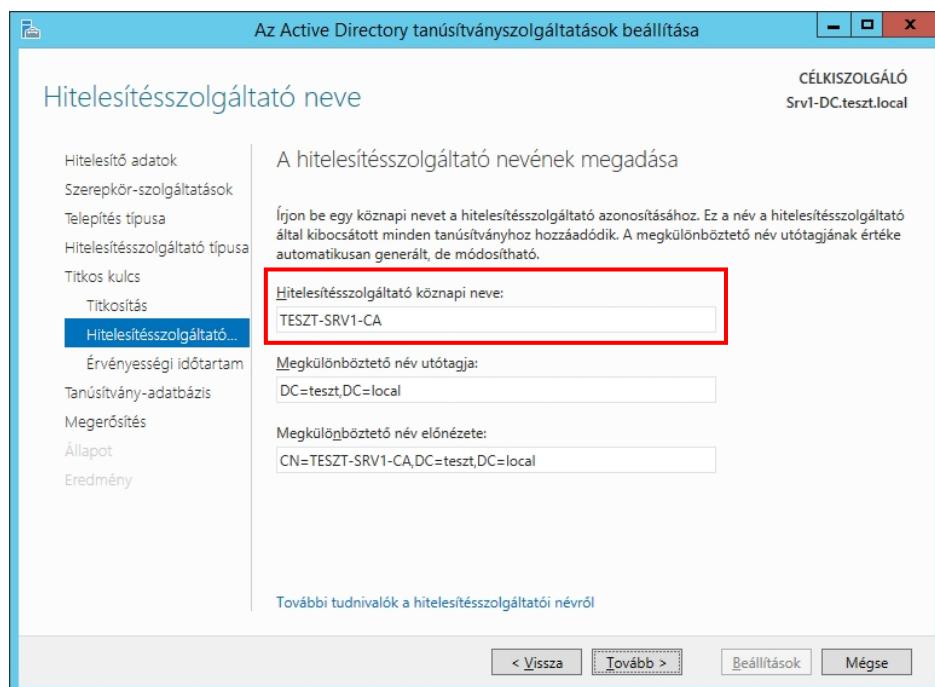
A tanúsítványokhoz szükség van egy kulcs létrehozására és mivel most telepítünk elsőnek tanúsítványszolgáltatást, nincs létező kulcsunk, **új titkos kulcsot kell létrehoznunk.**



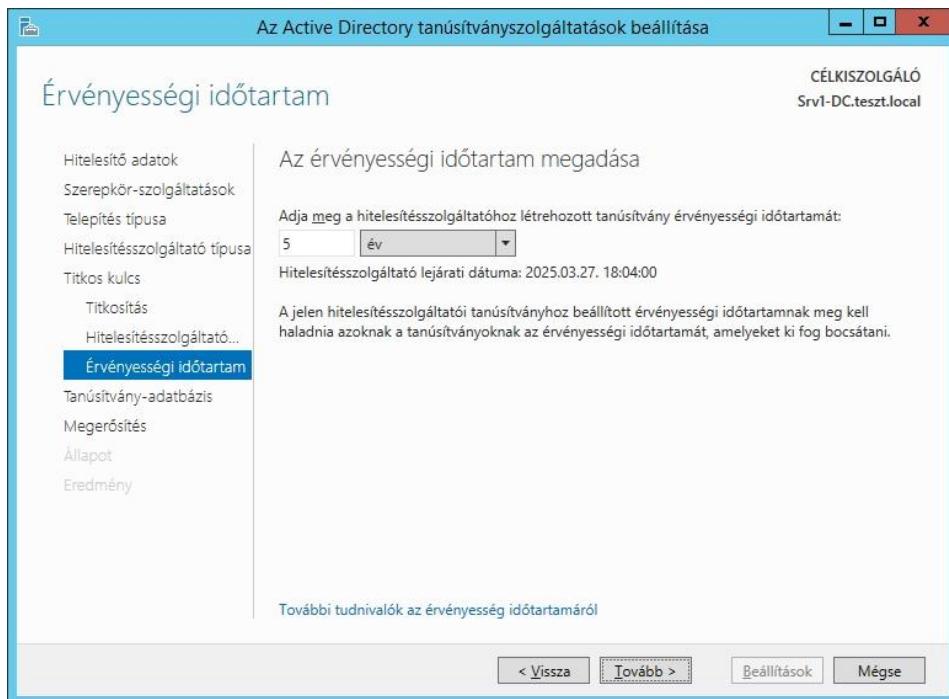
A kriptográfiai beállításokat az ábra szerint végezzük



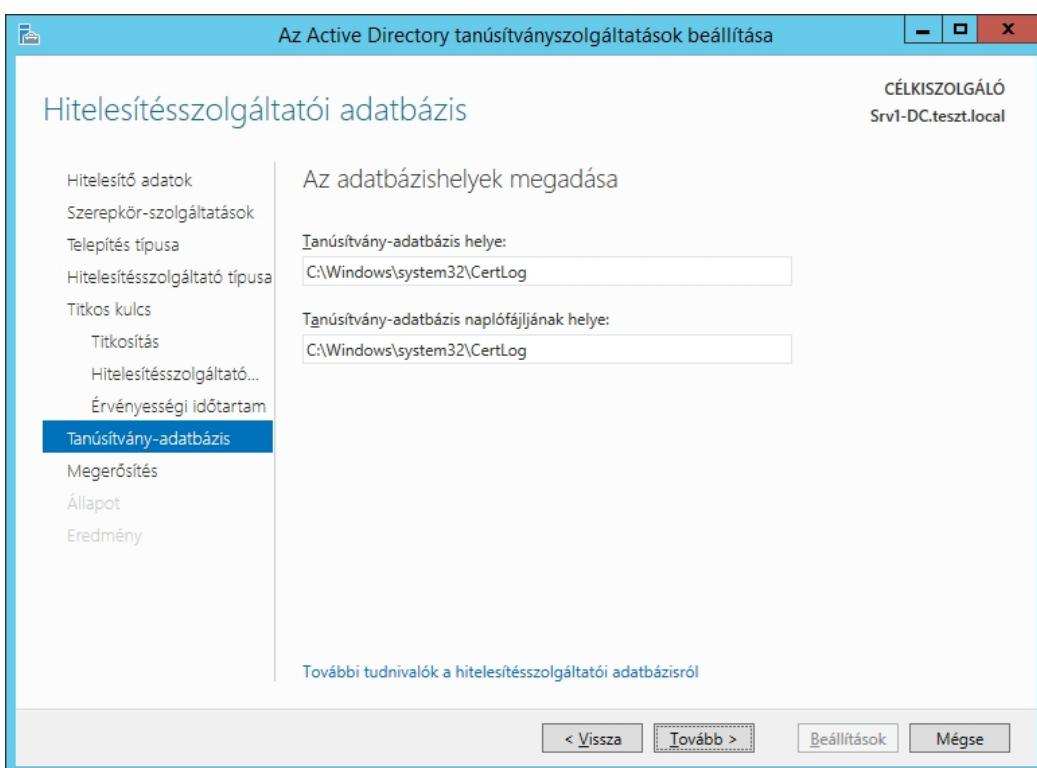
A köznapi nevet megváltoztathatjuk, de nem szükséges



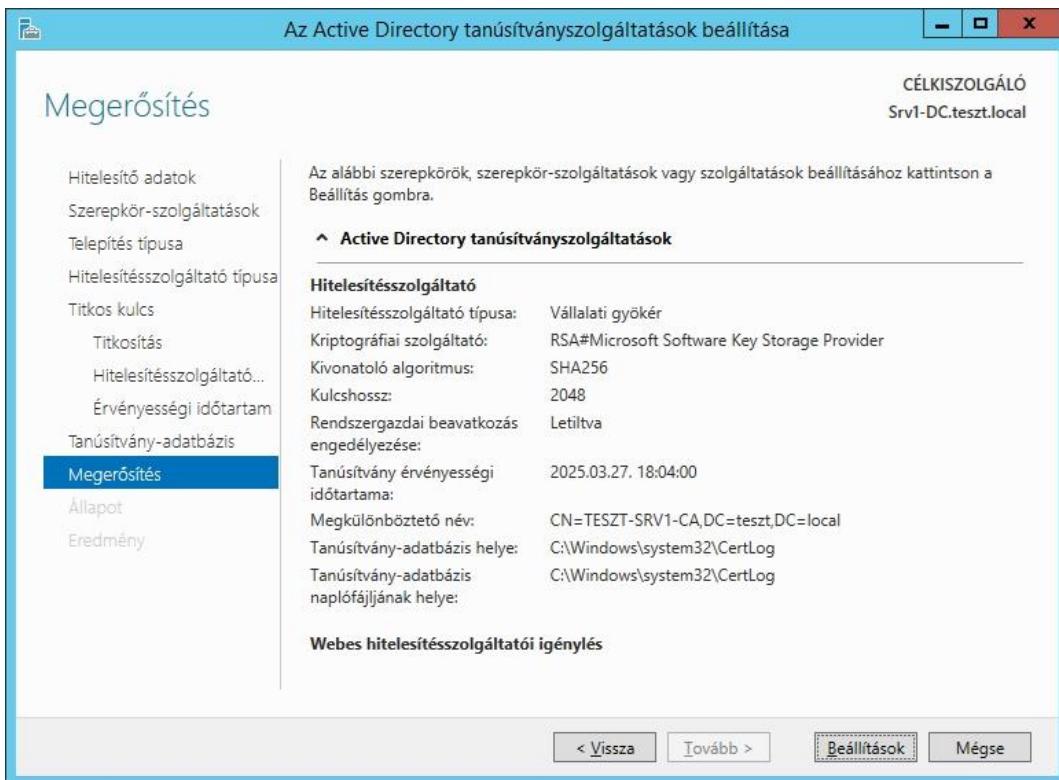
Adjuk meg az érvényességi időtartamot



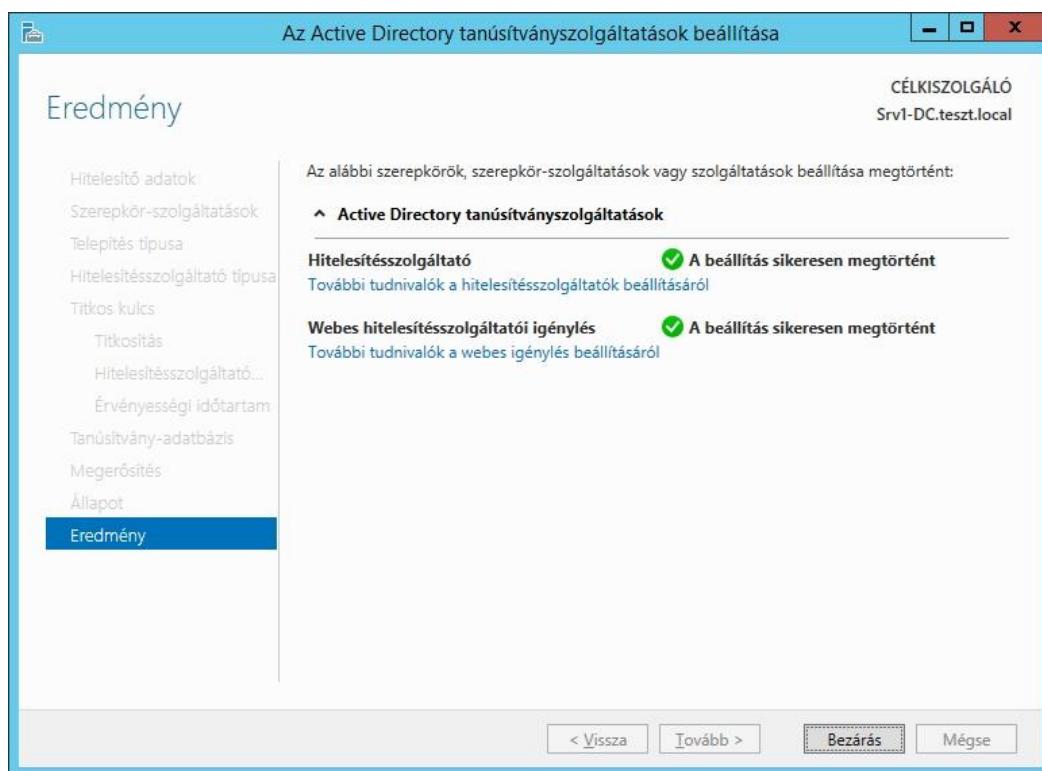
Tovább az alapértelmezésekkel beállítva



Elkészült a konfiguráció. Kattintva **Beállítások** gombra, kész is vagyunk.

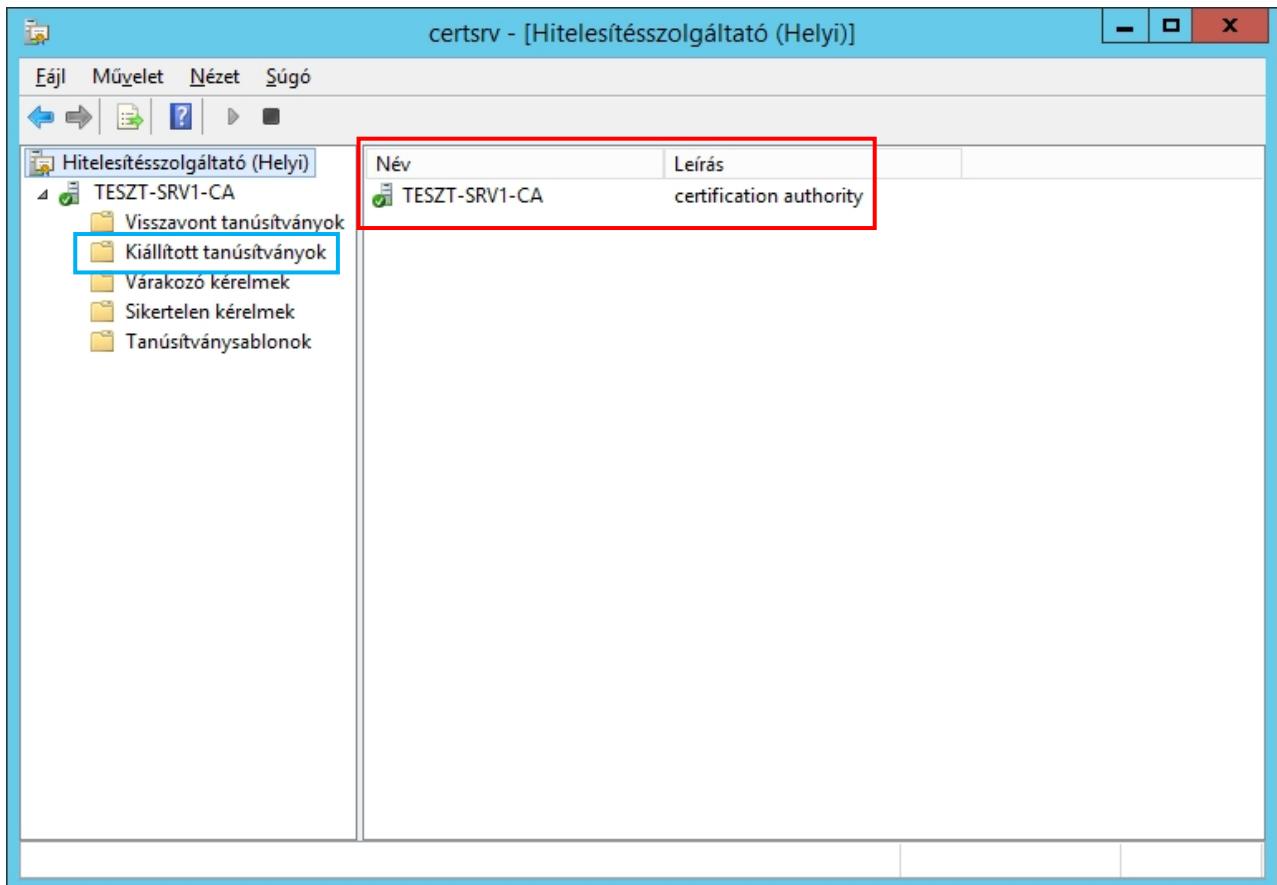


Sikeressé vált beállítani a Tanúsítványszolgáltatásokat.



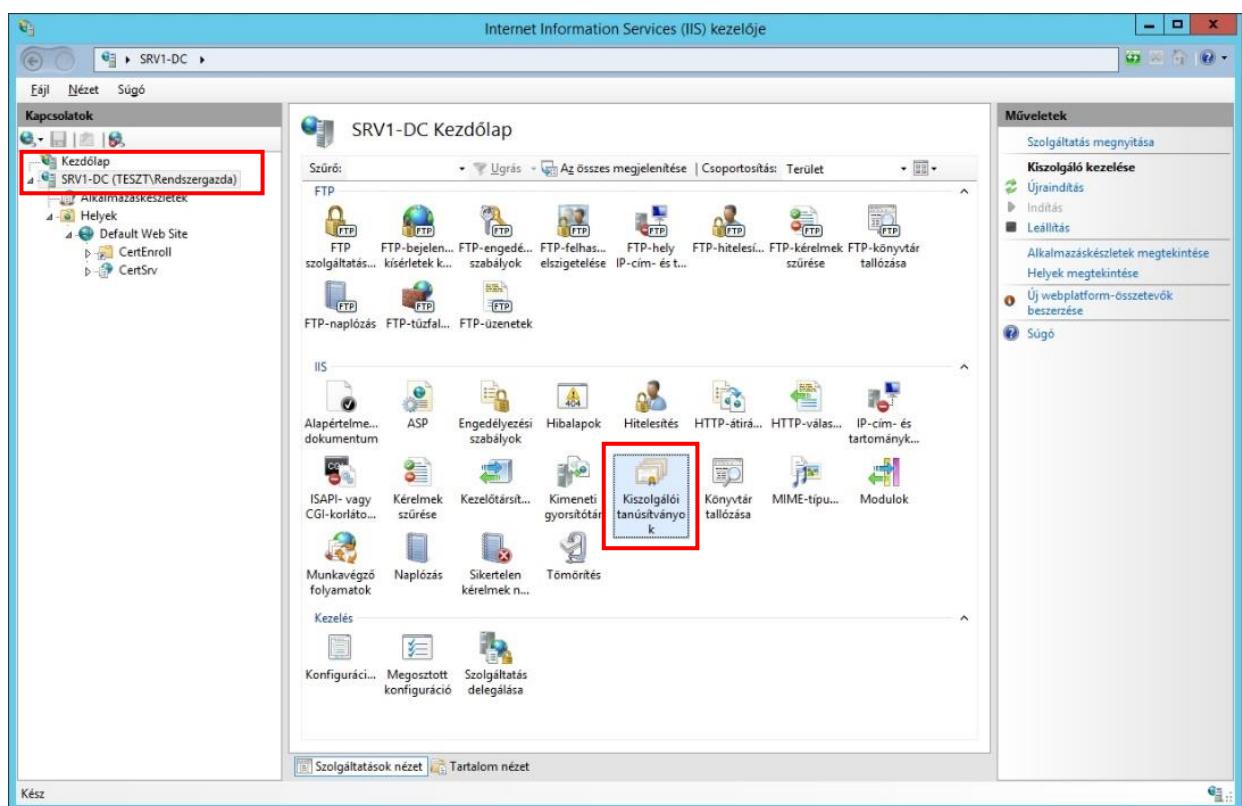
A Hitelesítésszolgáltató saját tanúsítványát megnézhetjük a Hitelesítésszolgáltató kezelőben.

Megnyitás után lényegi beállítást nem kell végeznünk. A zöld pipával jelzett név a **Hitelesítő szerver**, benne 5 mappa található, a nevük alapján tudjuk mire szolgálnak. Ha **AD nélkül** telepítjük akkor a **Tanúsítványsablonok** mappa nem található meg itt. A **Tanúsítványsablonok** csak tartományi (vállalati) hitelesítésszolgáltató esetén jön létre!



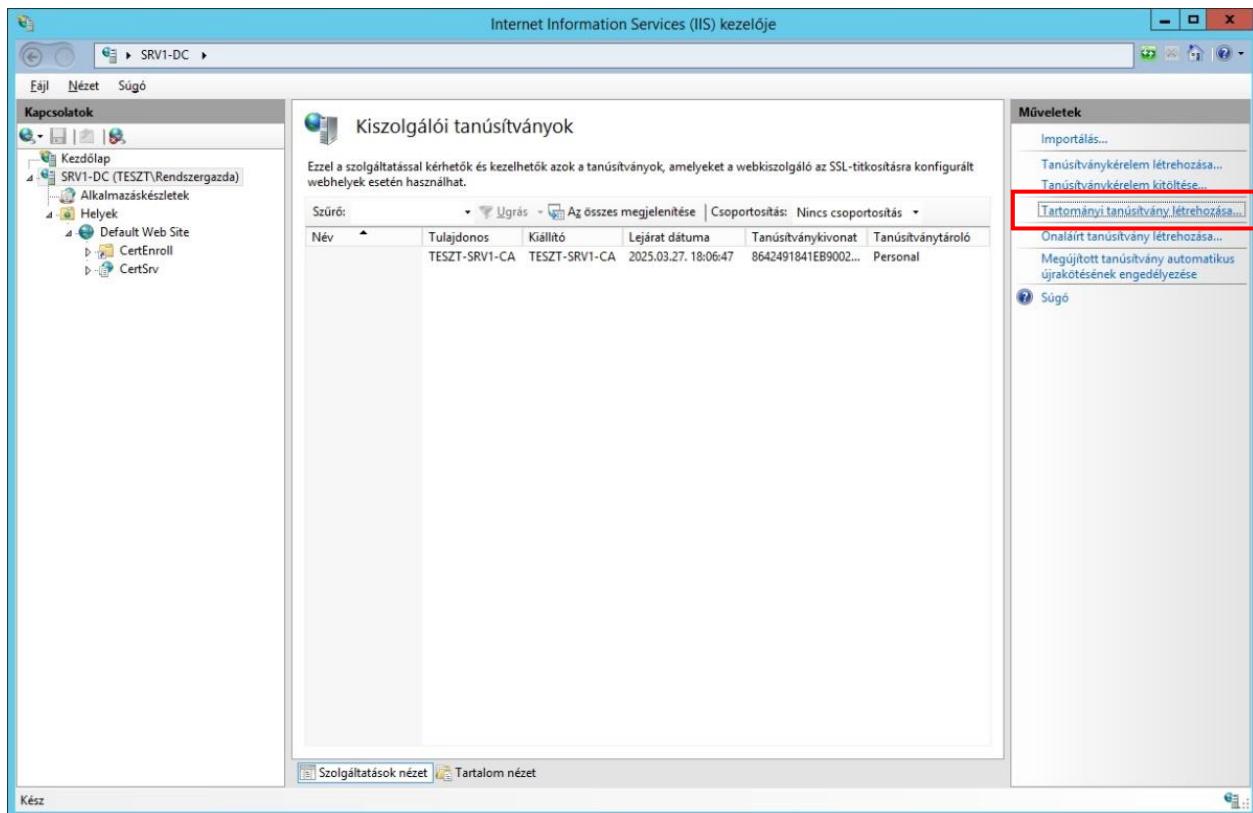
Biztonságos webhely kialakítása

Az alapértelmezett webhelyet fogjuk használni (Default Web Site). Előtte a webkiszolgálónak egy tanúsítványt kell igényelnünk. Első lépésként a legfelső (szerver) szinten a kiszolgálói tanúsítványok beállítás menüjébe lépünk.



A tanúsítványok listájában ott a **Hitelesítésszolgáltató tanúsítványa** (rootCA: TESZT-SRV1-CA).

A **Tartományi tanúsítvány létrehozása** linkre kattintva készítsünk a webszerverünknek tanúsítványt



Adjuk meg a szükséges adatokat, a **Köznapi név**: a webhelyünk kötésében megadott **domain-név** legyen

The screenshot shows the 'Tanúsítvány létrehozása' (Create Certificate) wizard. Step 2, 'Megkülönböztető név tulajdonságai' (Properties of the certificate subject), is displayed. It asks for identifying information: Köznapi név (www.teszt.local), Szervezet (home), Szervezeti egység (home), Település/helység (DB), Állam/megye (HB), and Ország/térulet (HU). The 'Köznapi név:' field is highlighted with a red box. At the bottom, there are buttons for Vissza (Back), Tovább (Next), Befejezés (Finish), and Mégse (Cancel).

A tovább gombra kattintva ki kell választanunk az **online hitelesítési szolgáltatót**:
ez a mi szerverünk, a **Kijelölés gombra** kattintva kiválasztjuk a szolgáltatót.

Tanúsítvány létrehozása

Online hitelesítésszolgáltató

Adja meg a tartományán belüli hitelesítésszolgáltatót, amely alá fogja írni a tanúsítványt. Meg kell adni egy rövid nevet, amelyet célszerű úgy megválasztani, hogy könnyen megjegyezhető legyen.

Adja meg az online hitelesítésszolgáltatót:

Példa: HitelesítésszolgáltatóNeve\Kiszolgálónév

Rövid név:

Vissza Tovább Befejezés Mégse

Jelöljük ki a **CA kiszolgálónkat**:

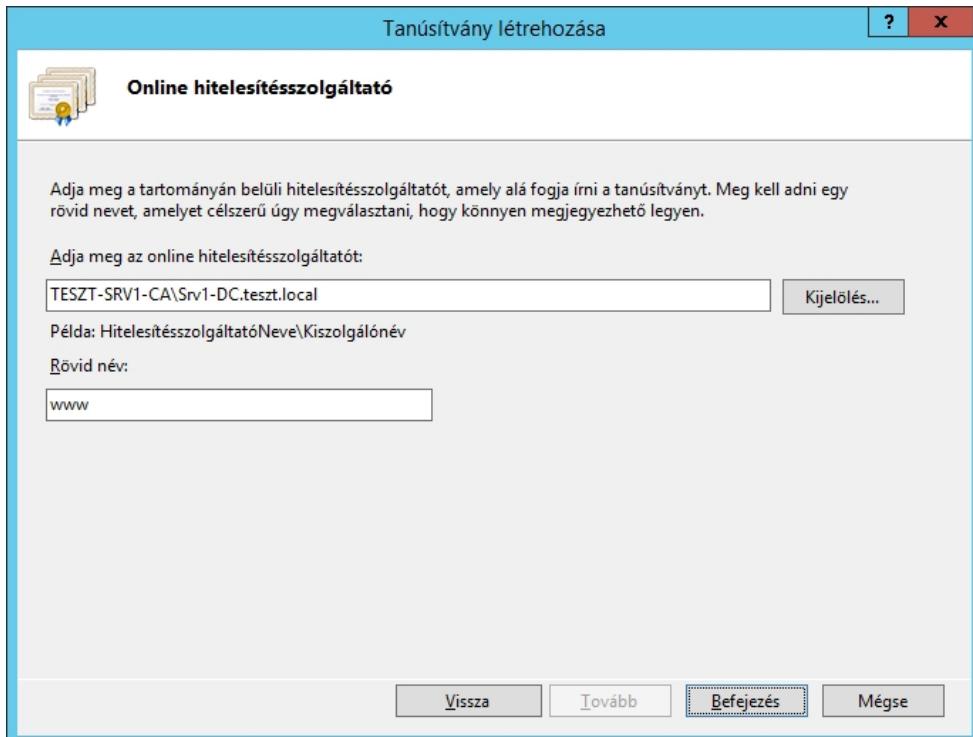
Hitelesítésszolgáltató kiválasztása

Válassza ki a használni kívánt hitelesítésszolgáltatót:

Hitelesítésszolgáltató	Számitógép
TESZT-SRV1-CA	Srv1-DC.teszt.local

OK Mégse

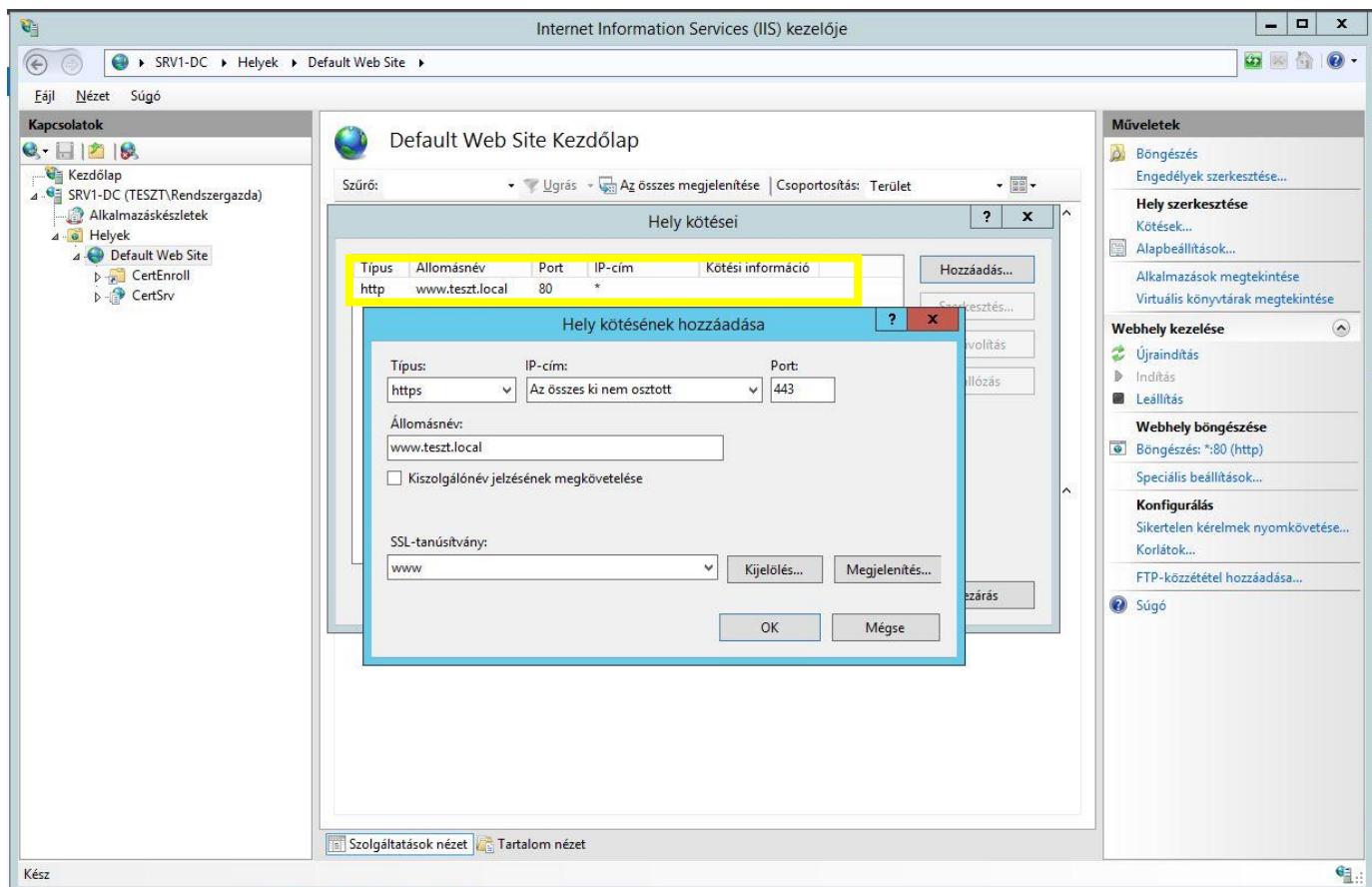
Befejezésre kattintva kész is a tanúsítványunk:



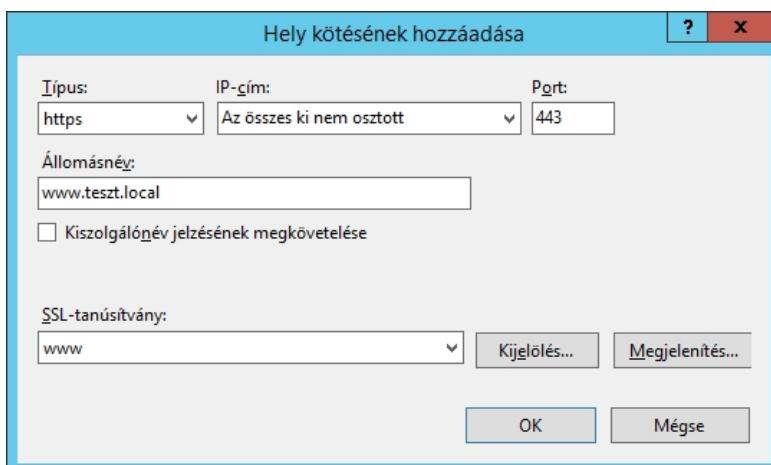
Megjelent a listában a **www** nevű tanúsítványunk, melynek tulajdonosa: www.teszt.local

Név	Tulajdonos	Kiállító	Lejárat dátuma	Tanúsítványkivonat	Tanúsítványtáról	
www	www.teszt.local	TESZT-SRV1-CA	TESZT-SRV1-CA	2025.03.27. 18:06:47	8642491841FB8002	Personal

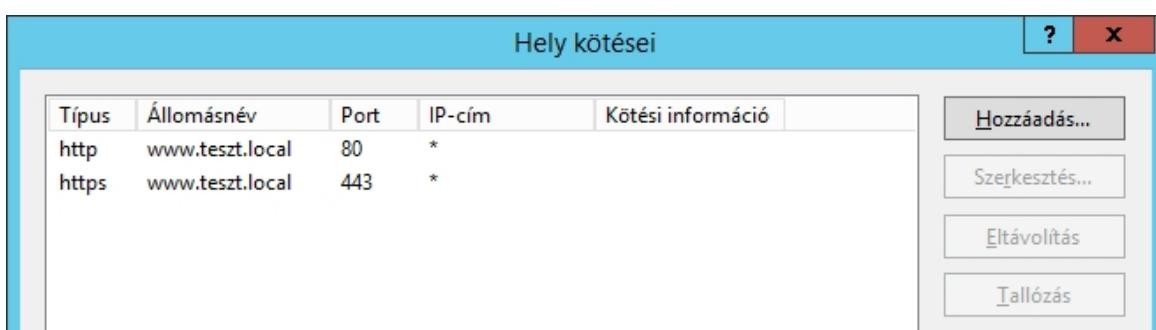
Használjuk fel a tanúsítványunkat a **https** kötés létrehozásához, a **port** esetünkben marad az alapértelmezett **https port: 443** és hozzákötjük az állomásnévhez a www.teszt.local domain-hez:



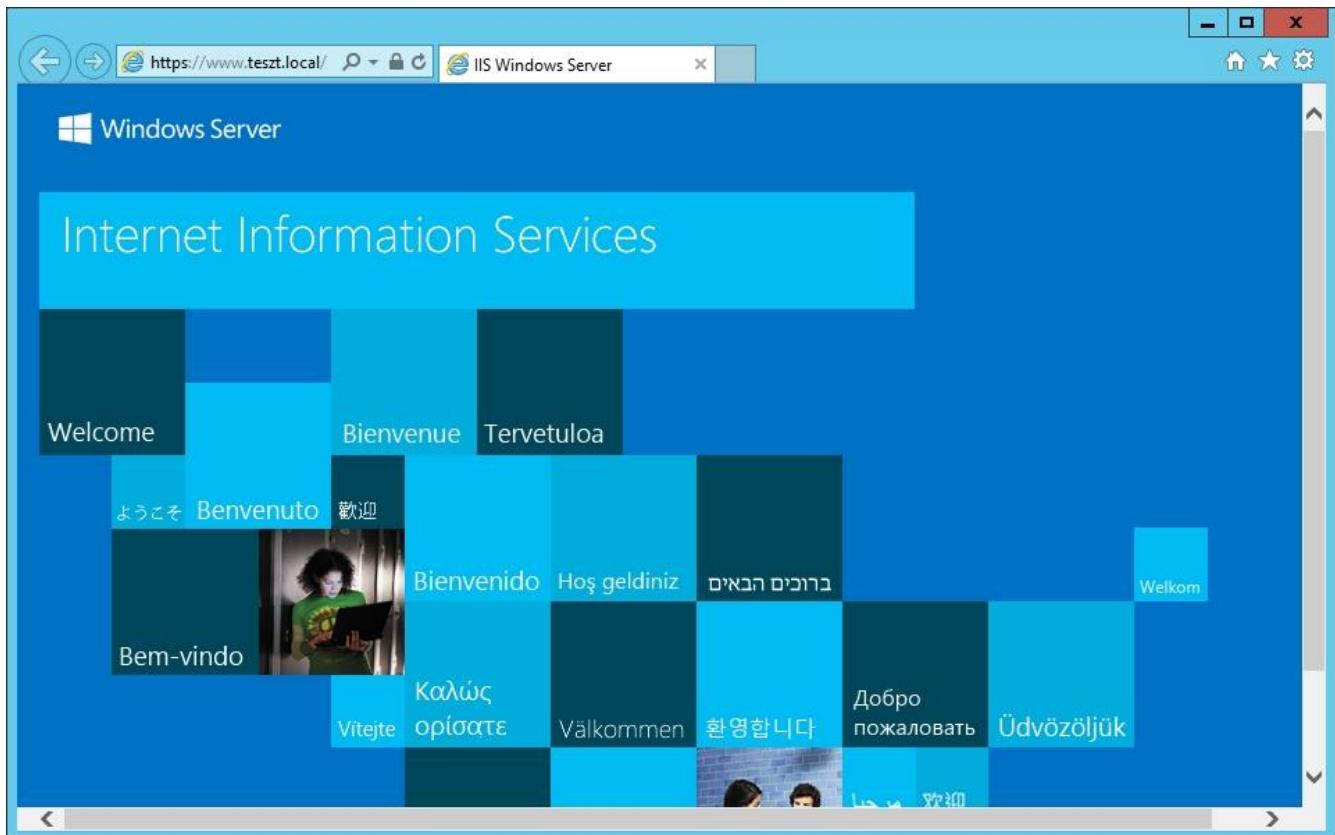
A **https** kötés részletei:



NE töröljük a kötések közül a **http protokollt a **80-as port-on**:**



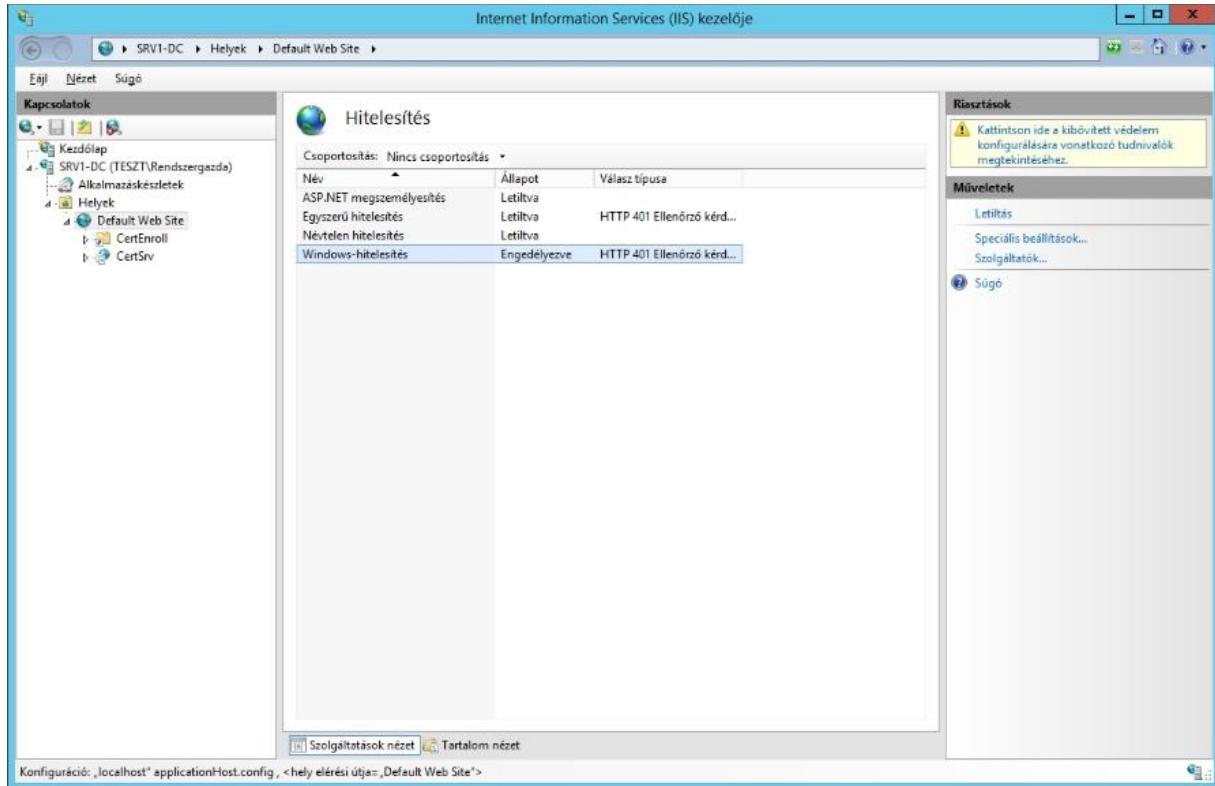
Teszteljük a szerveren elindított **Internet Explorerben** a beállításokat. A kis lakkat zárva ☺



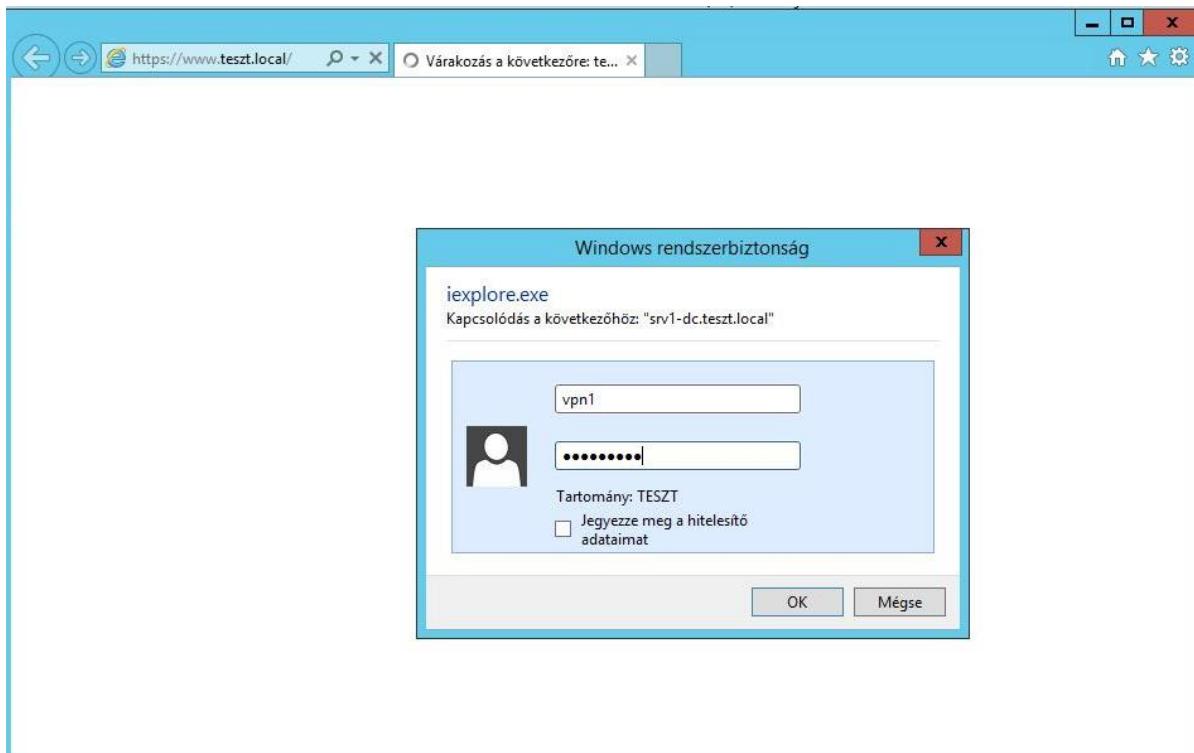
Amennyiben szeretnénk korlátozni a szerverünkhöz történő hozzáférést:

AD alatt engedélyezzük a Windows hitelesítést!

(Feltétel: a webkiszolgálói szerepkör telepítésekor, kijelöltük a **Windows hitelesítés** szerepkör-szolgáltatást!)



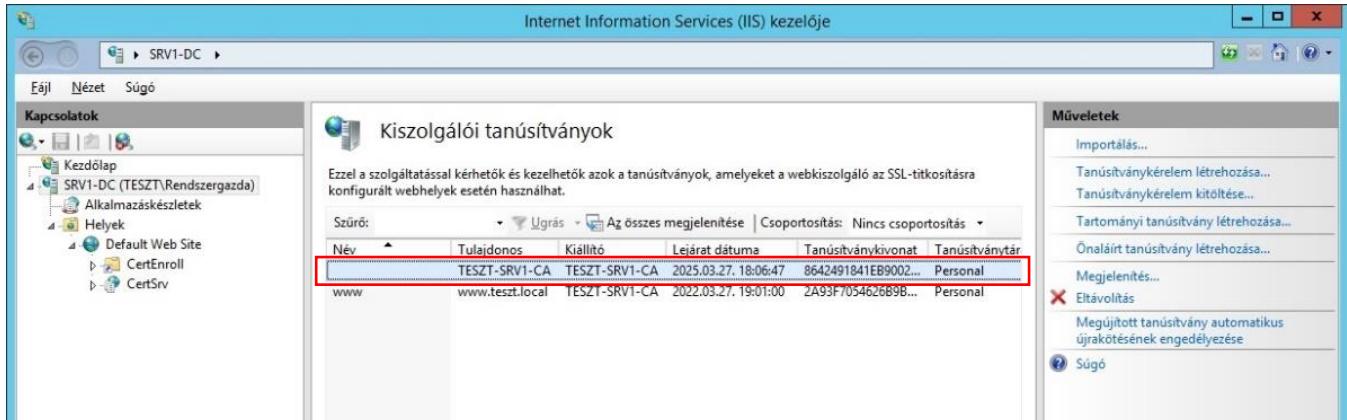
Újra töltve az oldalt a böngészőben, kéri a rendszer, hogy hitelesítsük magunkat:



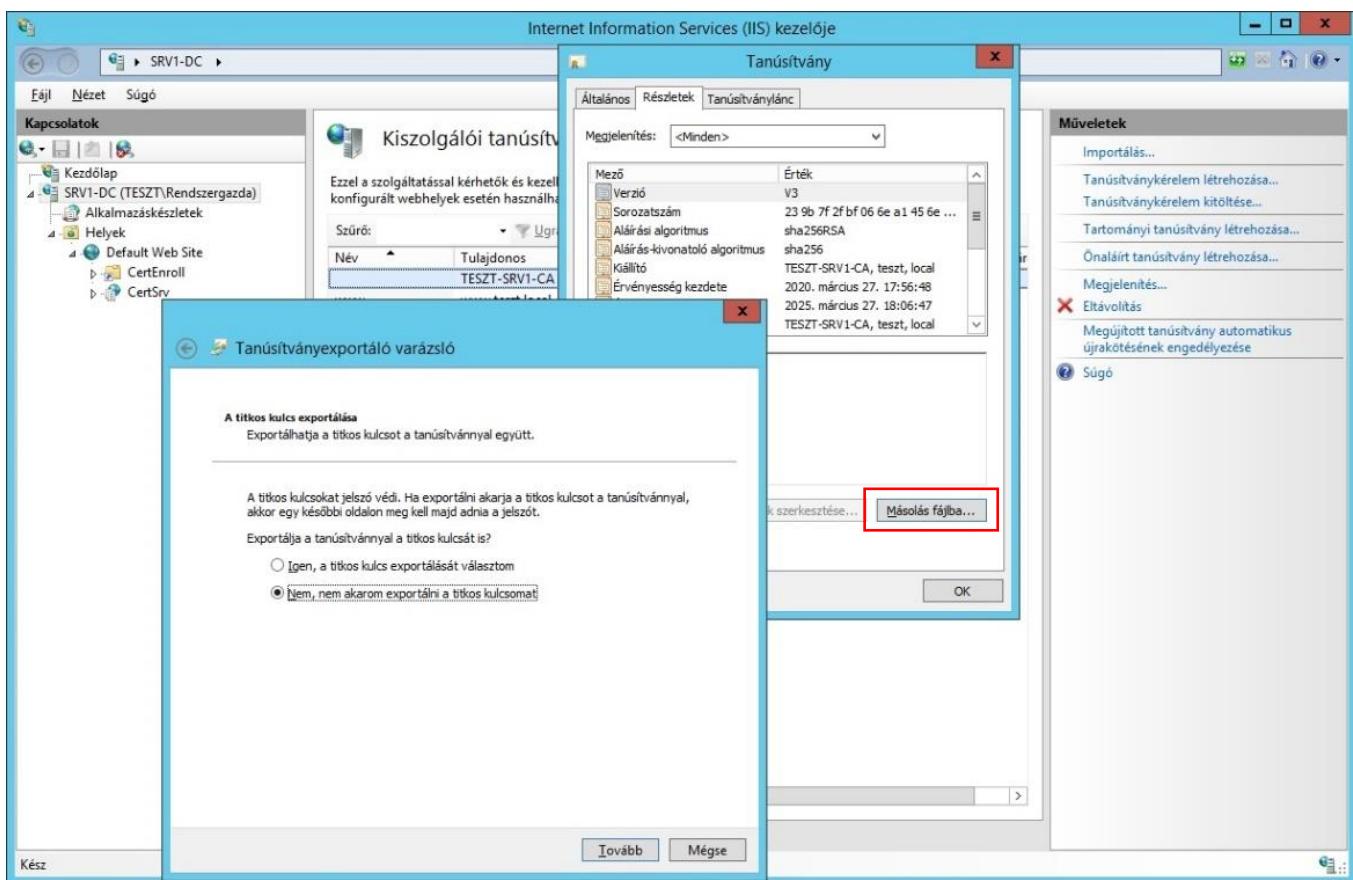
Szeretnénk elérni, hogy a kliensgépeken automatikusan hitelesként fogadja el a webkiszolgálónkat a böngésző. Ehhez a **rootCA** tanúsítványát importálnunk kell a kliens gépekre.

Először szerezzük meg a **Legfelsőbb szintű hitelesítésszolgáltató** tanúsítványát.

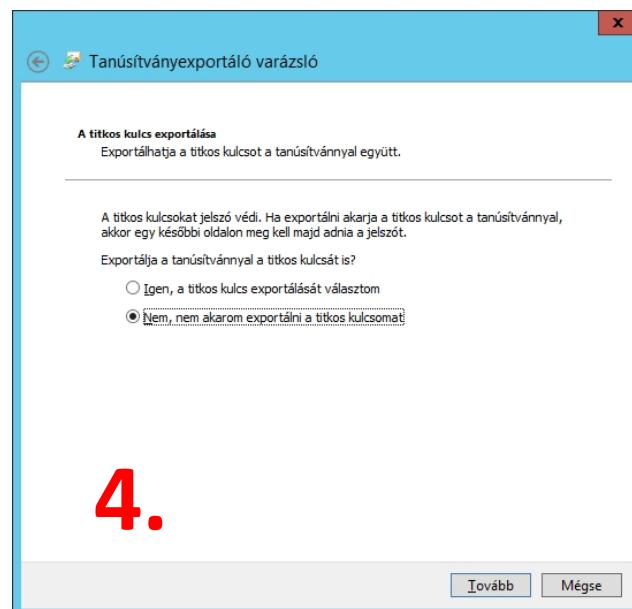
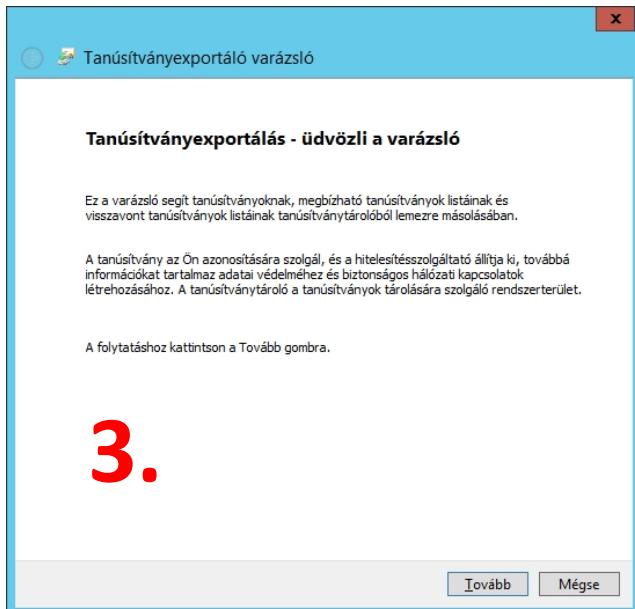
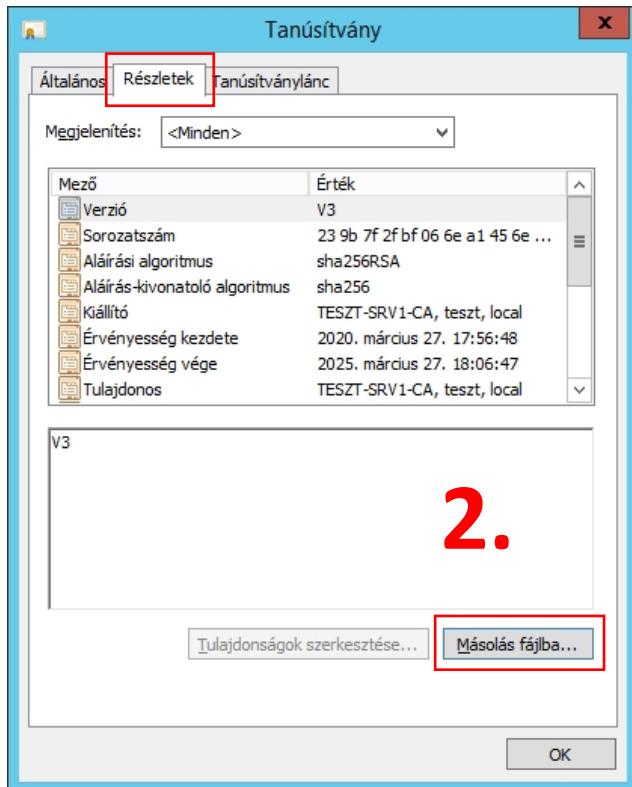
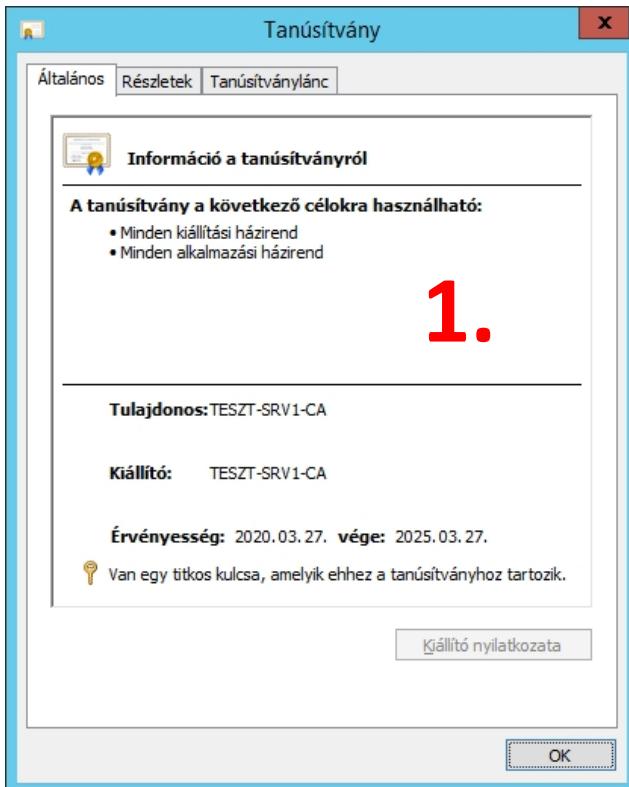
Az IIS kezelőben keressük meg a **rootCA** tanúsítványát, válasszuk ki és nyissuk is meg (dupla katt.)

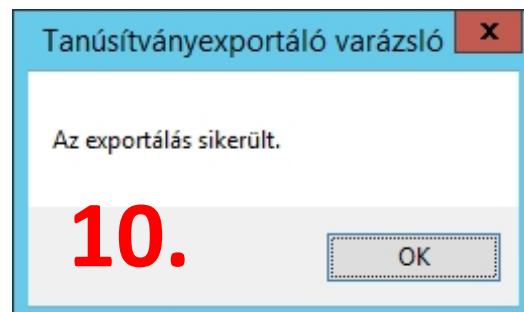
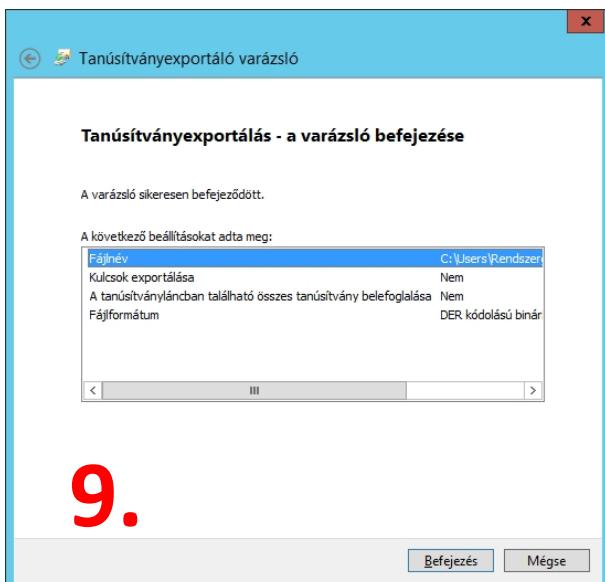
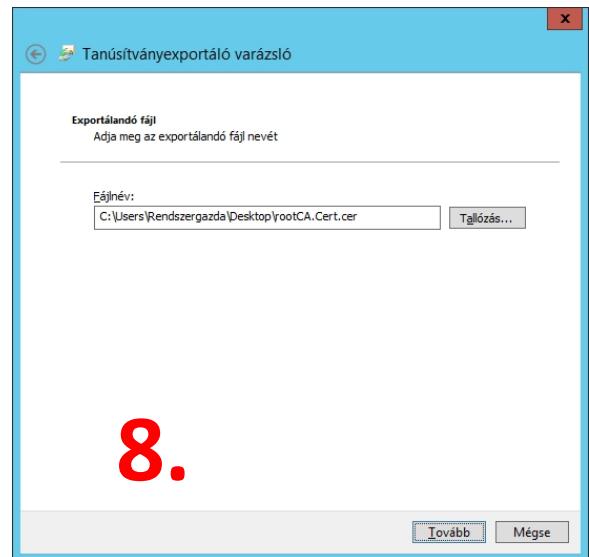
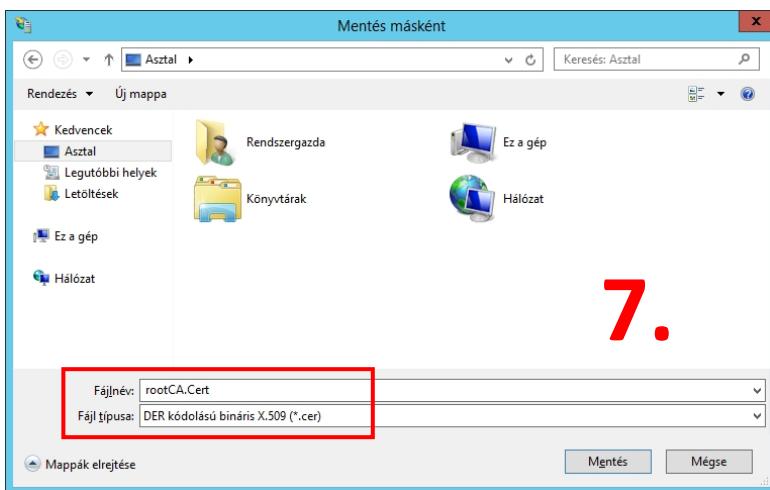
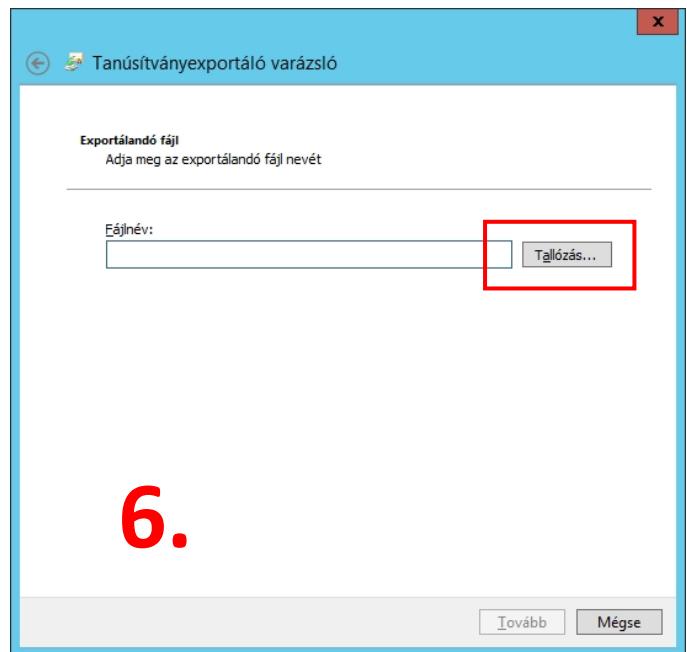
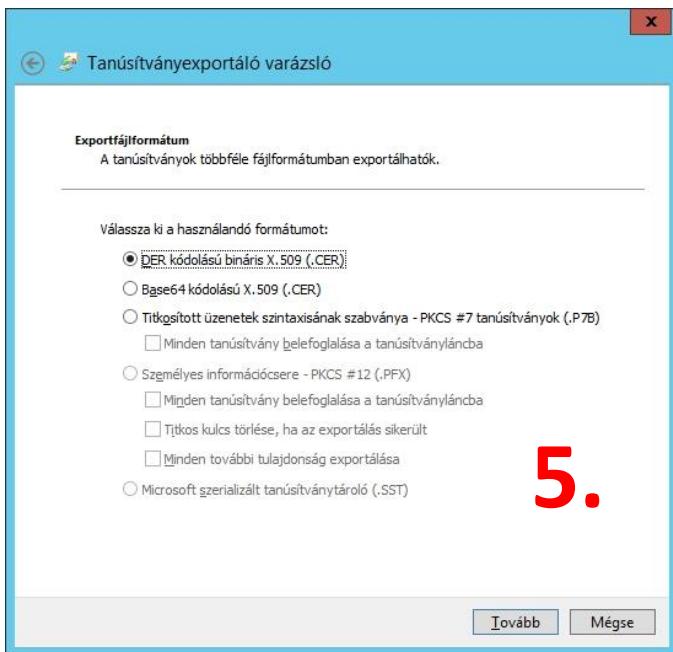


A **Részletek** fülön válasszuk a **Másolás fájlba...** lehetőséget:

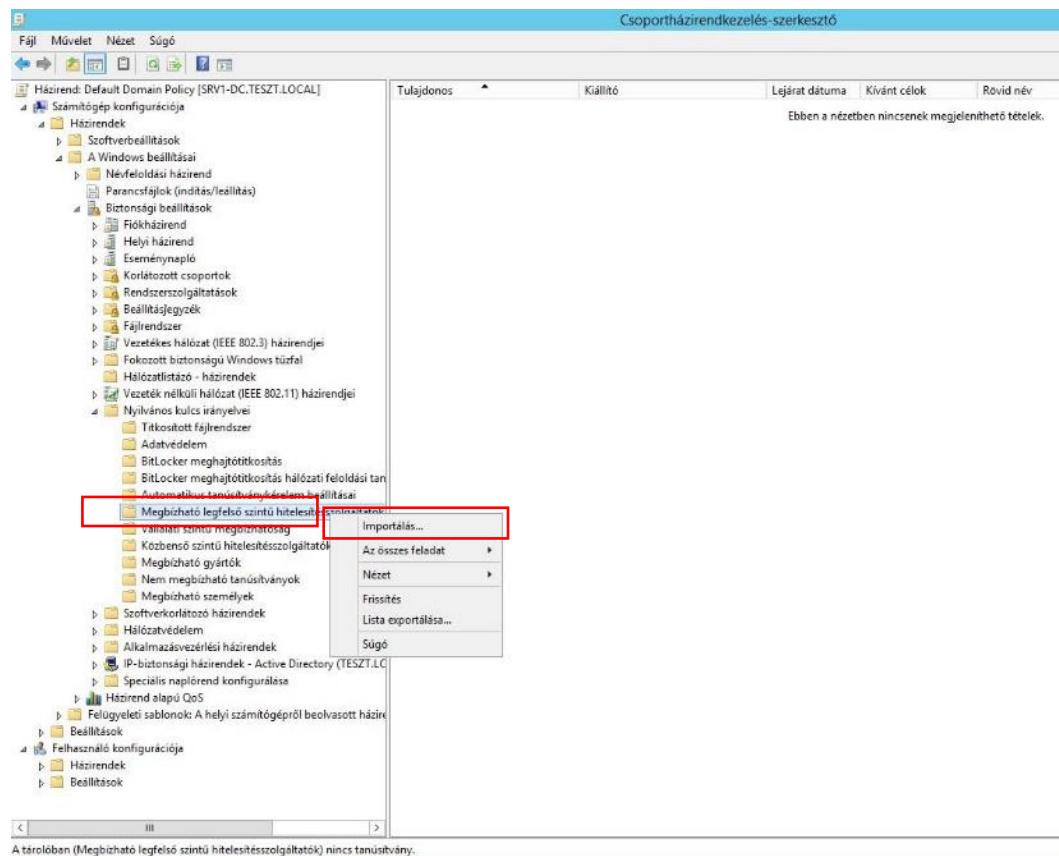


Részletesebben a folyamat képei:

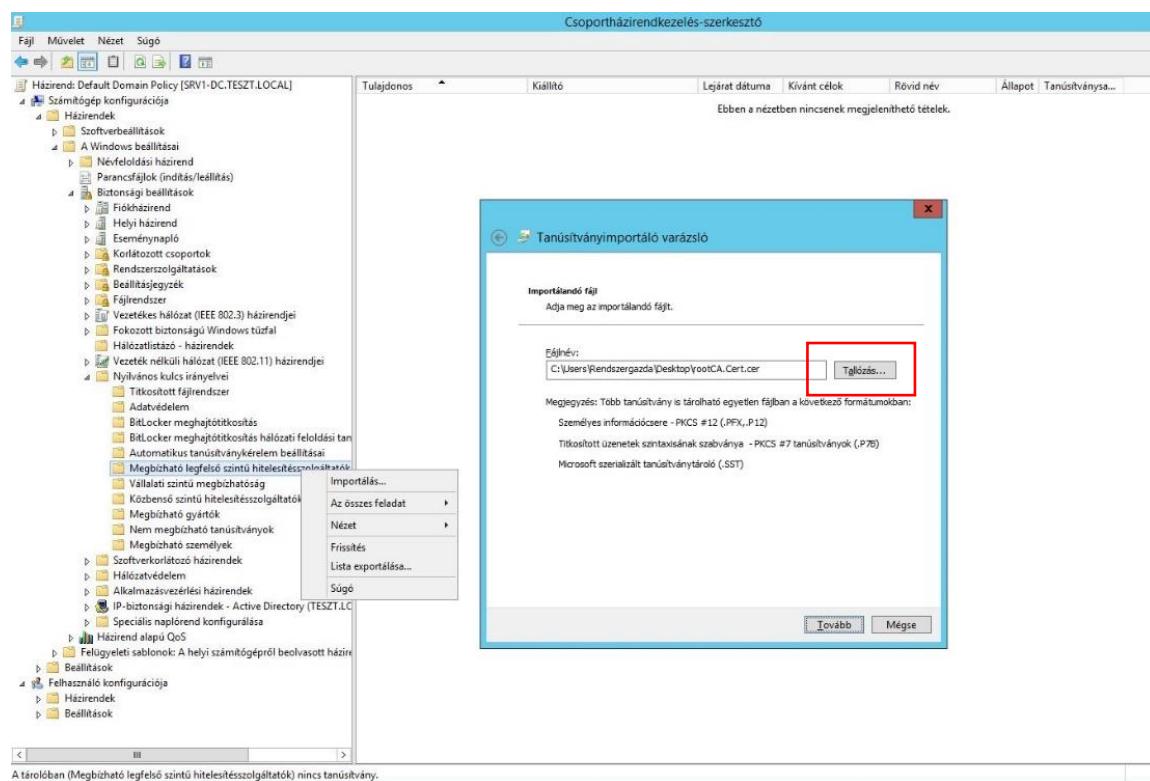




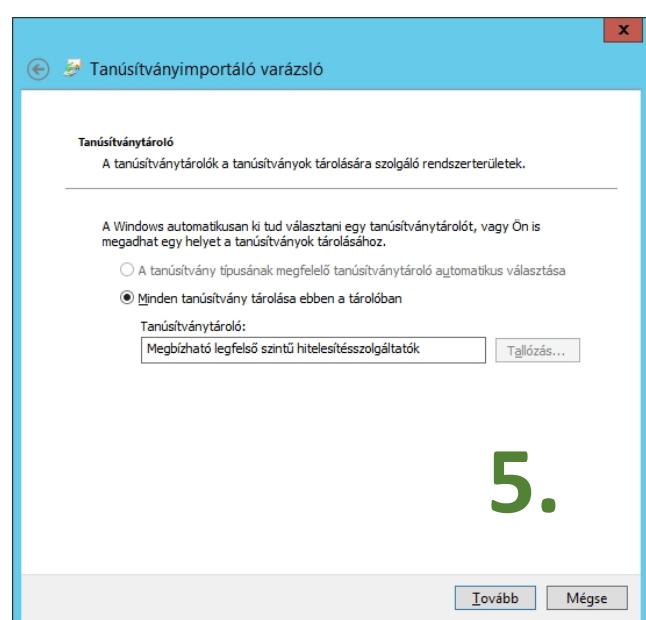
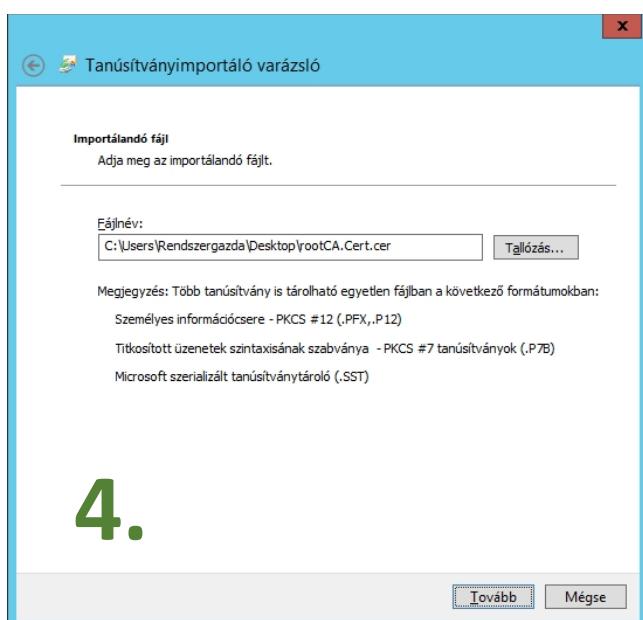
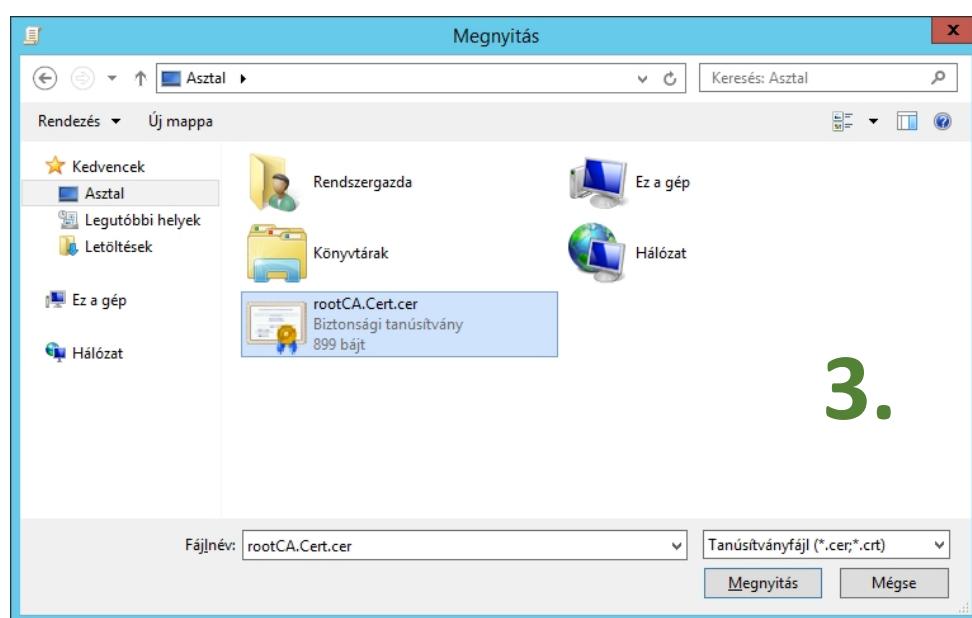
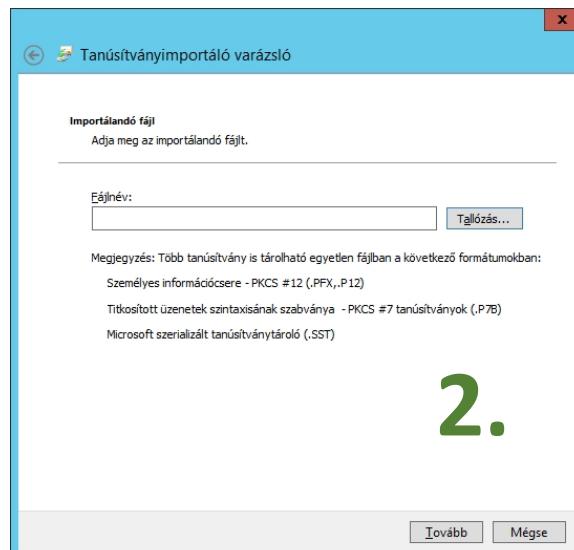
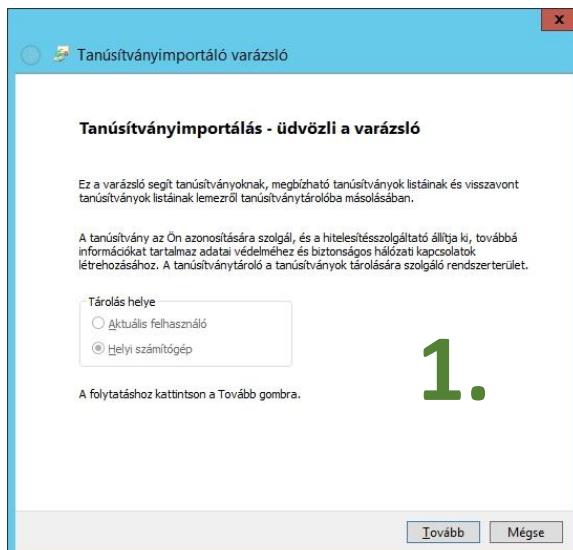
Csoportházirend kezelőben nyissuk meg a **Default Domain Policy**-t szerkesztésre és keressük meg a **Megbízható legfelső szintű hitelesítésszolgáltatók** ágat és a helyimenüből válasszuk az **Importálás-t**:

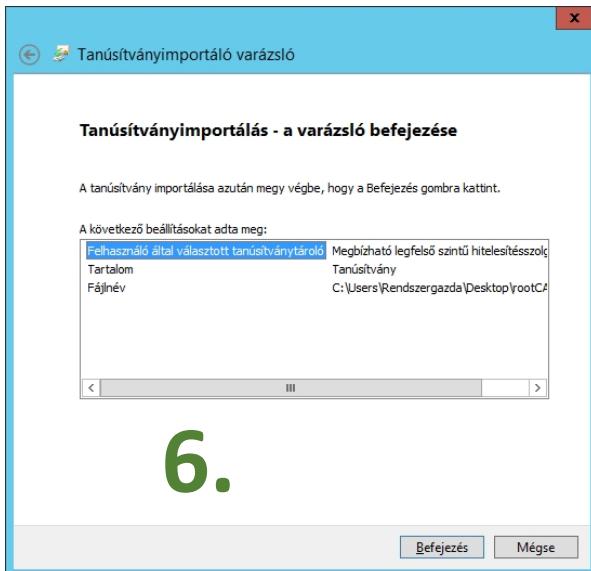


Keressük meg az asztalra mentett tanúsítványunkat:



Részletezve: a Tanúsítványimportáló varázsló lépései:





6.

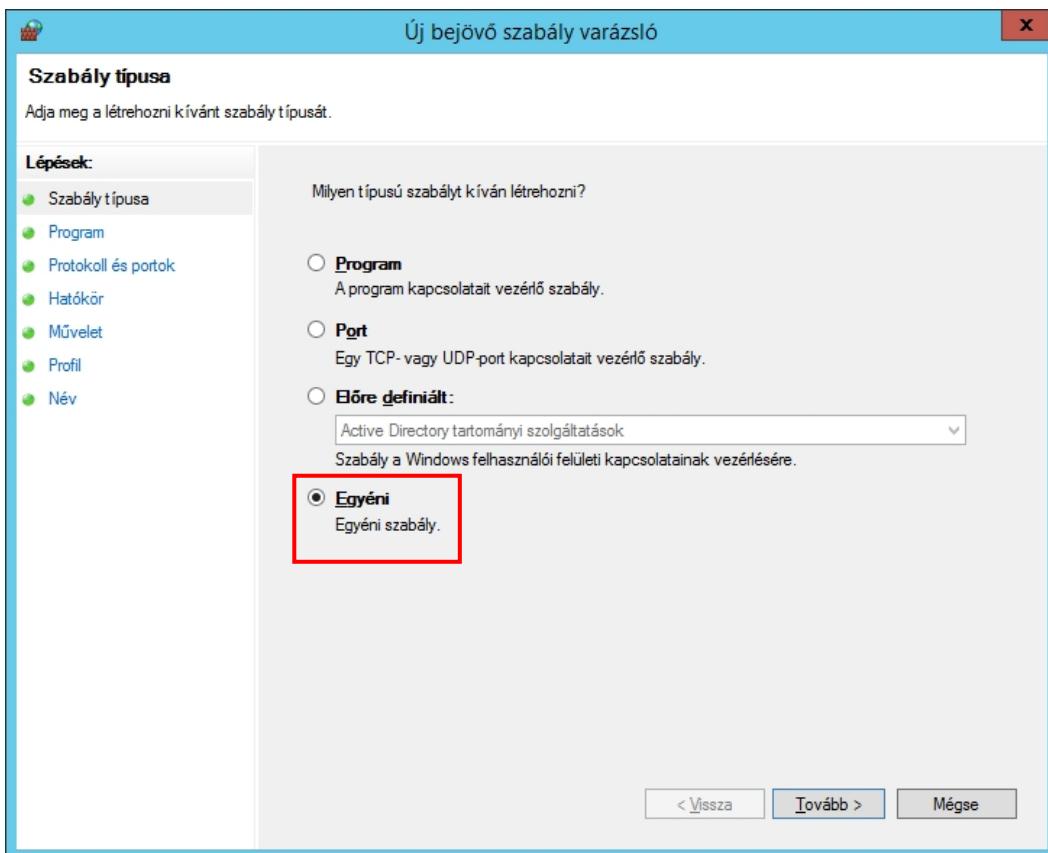
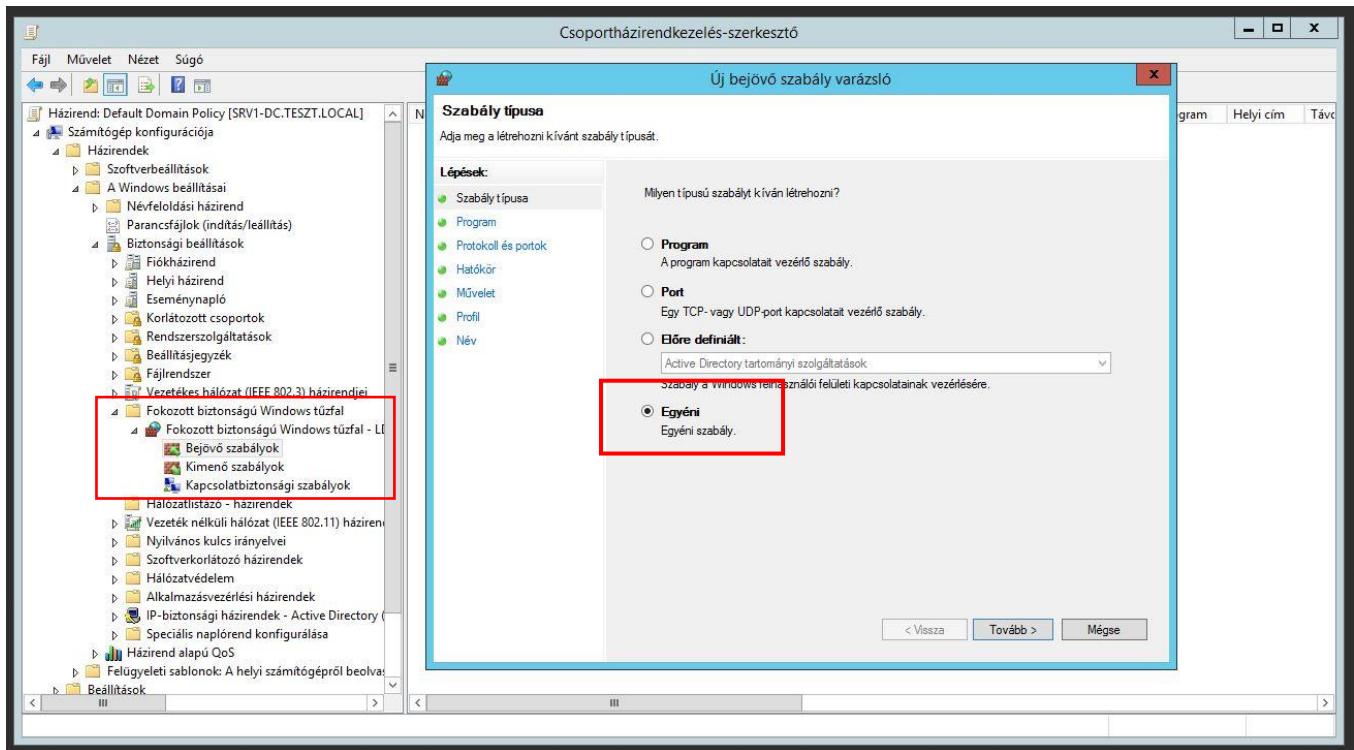
Kész!

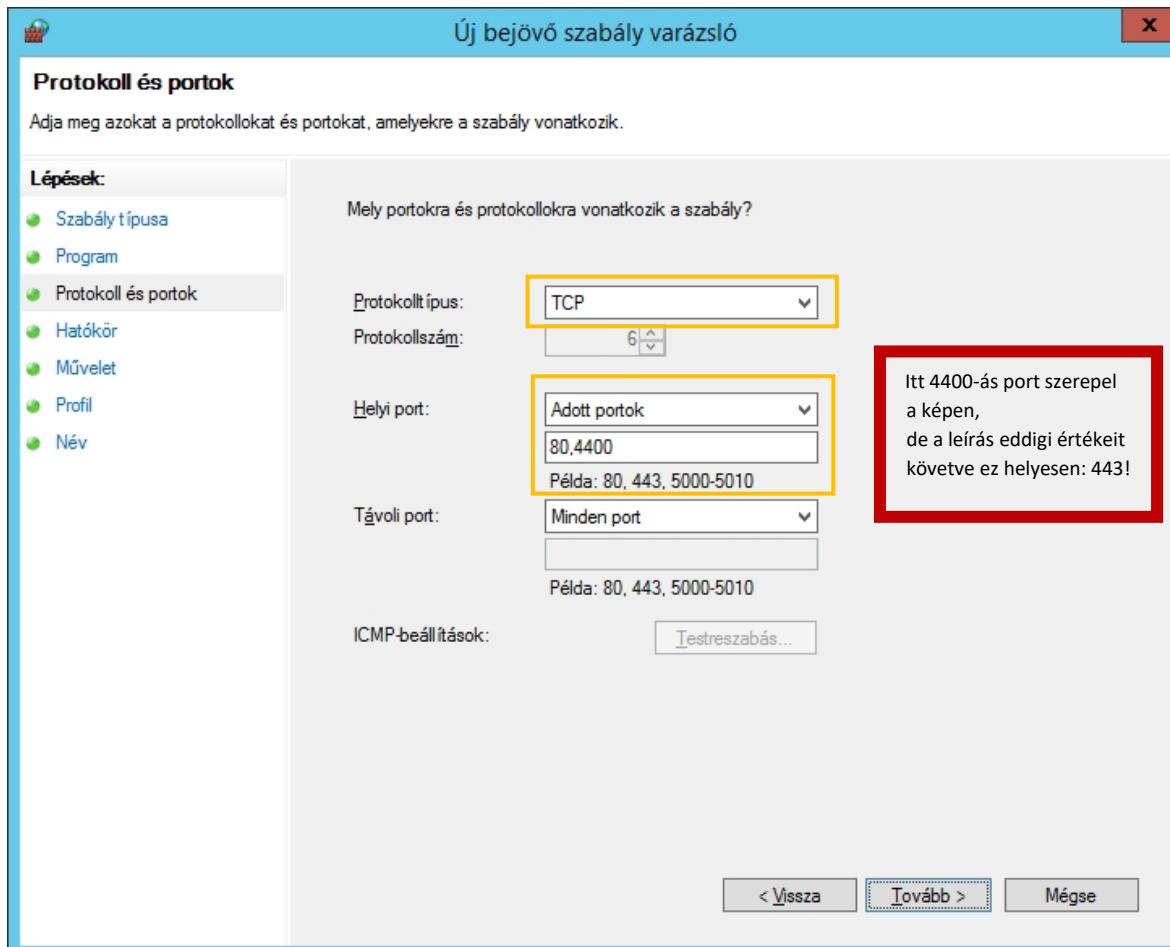
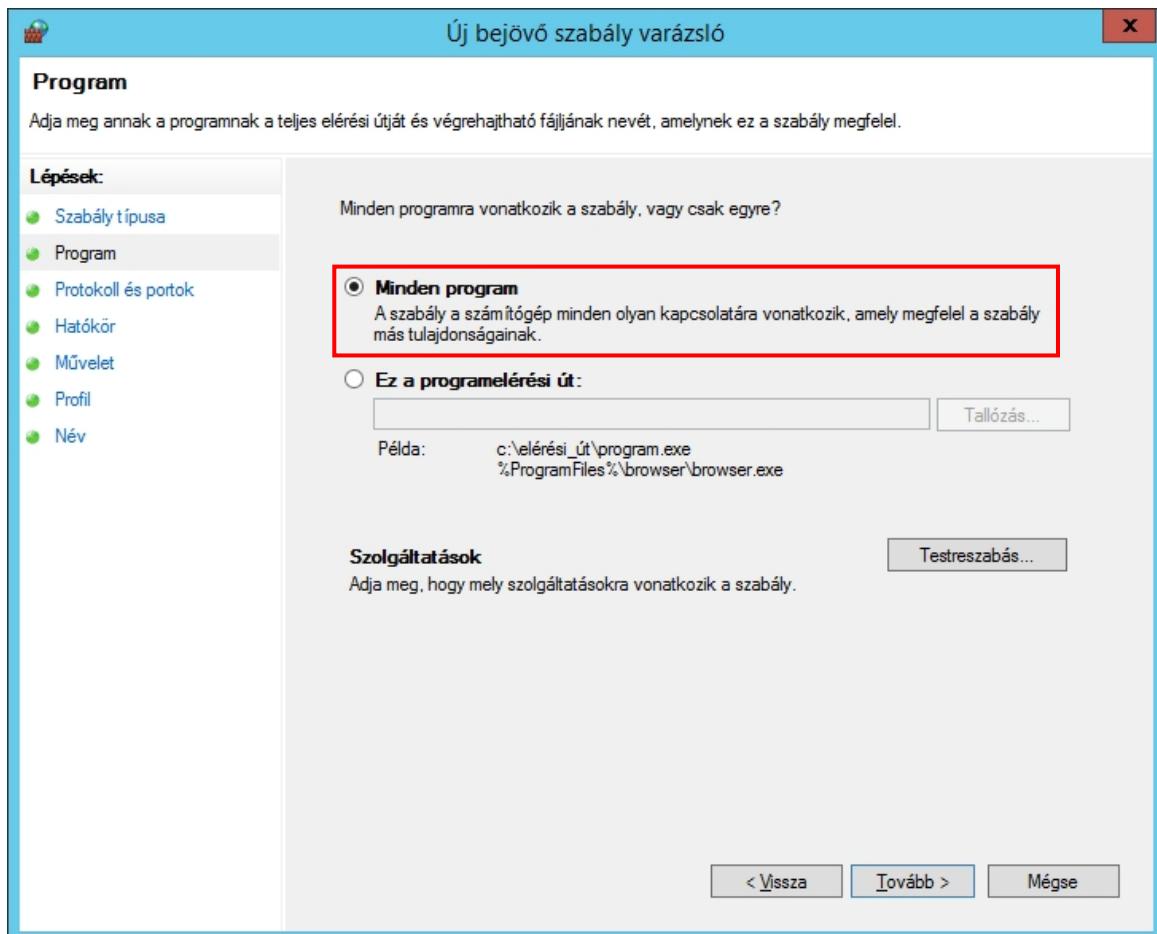
Ha a tűzfal beállításokat nem végezzük el még, akkor kész is vagyunk a csoportüzirend szerkesztővel.

A szerveren jöhet a csoportüzirend frissítés: **gpupdate /force**

Teszteljük a kliensgépről a beállításokat!

Amennyiben a kliens tűzfal beállításait is csoportüzirendekkel szabályozzuk, akkor itt a **Default Domain Policy**-ben megtehetjük: Elsőként hozzunk létre **egy bejövő szabályt**: (tűzfal beállításokról lesz még szó a következő órákon)





Új bejövő szabály varázsló

Hatókör

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

Lépések:

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

Mely helyi IP-címekre vonatkozik ez a szabály?

Bármely IP-cím
 Ezek az IP-címek:

Hozzáadás...
Szerkesztés...
Eltávolítás

Azoknak az adaptertípusoknak a testreszabása, amelyekre ez a szabály vonatkozik: [Testreszabás...](#)

Mely távoli IP-címekre vonatkozik ez a szabály?

Bármely IP-cím
 Ezek az IP-címek:

Hozzáadás...
Szerkesztés...
Eltávolítás

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

Csak az alapértelmezések, tovább...

Új bejövő szabály varázsló

Művelet

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

Lépések:

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

Milyen 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.

[Testreszabá](#)

Tiltsa le a kapcsolatot

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

Új bejövő szabály varázsló

Profil

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

Lépések:

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

Mikor lép érvénybe ez a szabály?

Tartomány
A számítógép vállalati tartományához való csatlakozásakor alkalmazandó.

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

Nyilvános
A számítógép nyilvános hálózati helyhez való csatlakozásakor alkalmazandó.

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

Adjunk a szabálynak nevet:

Új bejövő szabály varázsló

Név

Adja meg a szabály nevét és leírását.

Lépések:

- Szabály típusa
- Program
- Művelet
- Profil
- Név

Itt 4400-ás port szerepel a képen,
de a leírás eddigi értékeit követve ez helyesen: 443!

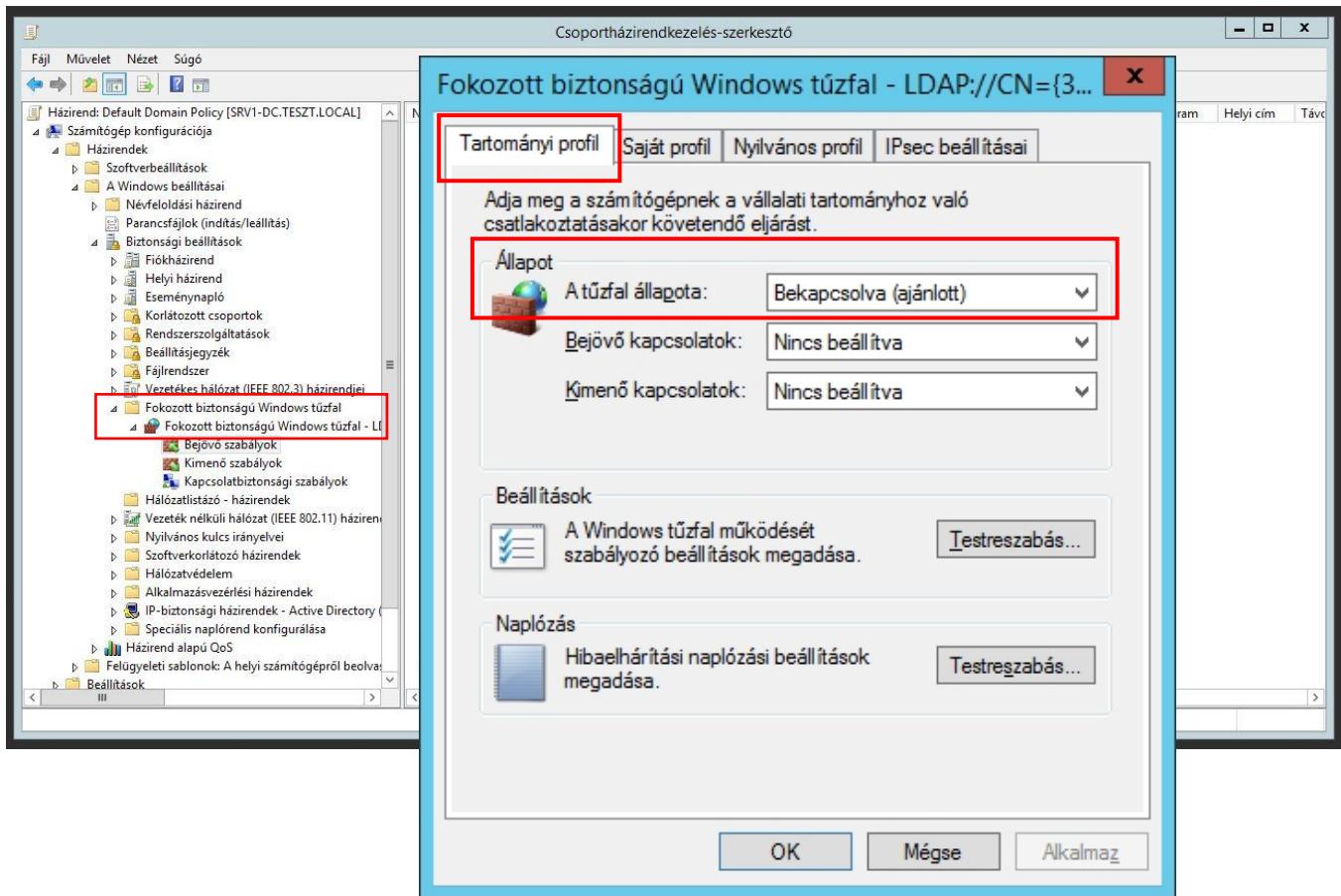
Név:

Leírás (nem kötelező):

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

Legvégül a **Fokozott biztonságú Windows tűzfal** beállításait szerkesztve kérjük, hogy kapcsolja be a Tűzfalat a Tartományi profilban.

A bejövő és kimenő kapcsolatok beállításai az ábrának megfelelően is maradhatnak:



A szerveren jöhet a csoportkörnyezet frissítés: **gpupdate /force**

Teszteljük a kliensgépről a beállításokat!

A számítógépre ható házirendet hoztunk létre, a számítógépet indítsuk el vagy ha már fut indítsuk újra!

Bejelentkezés után (pl. **vpn1** felhasználóként) a kliensen elindított **Internet Explorer** automatikusan fel kell ismerje a webkiszolgálónk tanúsítványát hitelesként (*kis lakat bezárva*), hiszen a csoportkörnyezetben keresztül beállítottuk a **Megbízható legfelsőbb szintű hitelesítésszolgáltatókat**.

