Debreceni Egyetem

Informatika Kar

A Windows 7 hálózati újításai

Témavezető:

dr. Krausz Tamás

Egyetemi adjunktus

Készítette:

Berna Tibor

Mérnök Informatikus

Debrecen

2010

Tartalomjegyzék

I. Bevezető

A személyi számítógépek mára az egész világon emberek milliói életének szerves részévé váltak. Életünk különféle területein megszámlálhatatlanul sok funkcióra használjuk őket, jóval többre, mint néhány éve bárki is gondolta volna. Az informatika mai világunk egyik leggyorsabban fejlődő tudományágává nőtte ki magát.

A számítógépek beférkőztek otthonainkba, munkahelyeinkre, és szinte bárhova, ahol valamilyen módon hasznosítani lehet képességeiket. Egyre inkább elképzelhetetlen egy otthon számítógép és internet-elérés nélkül, mely emberek millióinak szinte napi szükségletévé vált.

A világ majdnem összes számítógépe mára már egy hálózat része. Az interneten rendelkezésre álló, valamint a magán és vállalati hálózatainkon tárolt információk léte szinte megköveteli egy mindenre kiterjedő, mindenki számára elérhető, univerzális kapcsolat kialakítását. A vezeték nélküli hálózati képességek bővülése növeli a mobilitásunkat anélkül, hogy aláásná a számunkra szükséges információhoz való hozzáférési képességünket.

De ebben az univerzális kapcsolatban nagy veszélyek is rejlenek. A kapcsolódás könnyedsége, amely a jogosult felhasználók számára elérhetővé teszi a kívánt erőforrásokat szinte bárhonnan, bármikor, a jogosulatlan felhasználók és károkozó programok számára is lehetőséget ad a támadásra, mindezt viszonylag nagy sebességgel, és a támadó kilétének titokban maradásával.

A hálózatok fejlődése mind a nagyvállalatok, mind az otthoni és kisvállalkozások körében megmutatkozott. Talán nem is létezhet ma már olyan nagyvállalat, amelynek nem képezik szerves részét a számítógépek és a hálózatok, valamint az Internet. Itt is egyre nagyobb szerepet kapott a biztonság kérdése is.

Újabb és újabb technológiák látnak napvilágot, javítva, vagy lecserélve a korábbi technológiákat, egyre több lehetőséget biztosítva a hálózatokat használó társadalomnak. Egyre nagyobb teret hódítanak a vezeték nélküli hálózati megvalósítások, melyek előnye mobilitásukban, hátrányuk elérhetőségükben, biztonságukban és talán sebességükben rejlik. Ezeket a hátrányokat egyre inkább sikerül leküzdeni, teret hódítanak a wireless megoldások.

A felhasználói igényeket a versengő operációs rendszerek igyekszenek kielégíteni. A legsikeresebb ilyen operációs rendszerek a Microsoft fejlesztésében készülnek már évek óta.

Habár nem kifejezetten hálózati operációs rendszer, a sorozat tagjaként nemrégiben megjelent legújabb verzió, a Windows 7 hálózati képességeinek, felvonultatott technológiáinak és újdonságainak bemutatását, valamint a fentebb említett bővülő és fejlődő hálózati szolgáltatások Windows-os megvalósításának bemutatását tűztem ki célul. Azért választottam ezt az operációs rendszert, mert a Windows XP óta ez az első sikeresnek ígérkező kliens operációs rendszer, valamint ez jelképezi a Microsoft jelenlegi csúcstechnológiáját, ezért a hálózatok kezelésének újdonságainak bemutatására remek példaként szolgál.

A Microsoft a Windows 7-ben új hálózati eszközöket vezetett be, amelyek javítják vagy felváltják a Windows előző kiadásainak mára már elavult eszközeit. Habár nagyon sok változás történt, a korábbi funkcionalitás megmaradt, és további tulajdonságokkal és funkciókkal bővült.

II. Microsoft Windows 7

A Windows a világ egyik legnépszerűbb termékcsaládja, melynek több százmillió vásárlója van világszerte. A Windows technológiáit folyamatosan fejlesztik, frissítik, az újabb és újabb kiadott verziók mindig a legfrissebb technológiákat ötvözik, hogy kielégítsék a fejlődő felhasználói igényeket, és hogy megőrizzék a Microsoft operációs rendszereinek piacvezető szerepét.

A **Windows 7** a Microsoft Windows termékcsaládjának legújabb tagja. Fejlesztési időszakának elején Blackcomb, aztán Vienna kódnéven fejlesztették. 2009 októberének végén került kereskedelmi forgalomba, kevesebb, mint 3 évvel elődje, a Windows Vista megjelenése után. A Windows 7 szerverekre szánt megfelelője, az azonos kódbázisra épített Windows Server 2008 R2 ugyanebben az időben került a boltok polcaira.

A Windows drámai változásokon ment keresztül a Windows XP és korábbi verzióinak megjelenésétől a Windows 7 megjelenéséig. Bár hasonló a Windows Vista-hoz, A Windows 7 nagyon fontos változtatásokat hozott, melyek mind az interfészen, mind a mögöttes architektúrában, a rendszer működésében megmutatkoznak. Elődeivel ellentétben, melyek mindig nagy mennyiségű új funkciót és egyéb újításokat vonultattak fel, a Windows 7-et inkább úgy készítették, hogy javítsa elődje, a Windows Vista hibáit, pótolja hiányosságait, továbbfejlessze funkcióit, így járulva hozzá a Windows vonal továbbfejlődéséhez, de kompatibilis maradjon minden szoftverrel és hardverrel, amellyel a Windows Vista kompatibilis volt. Persze azért nem állt meg a Microsoft egy sima javításnál, új funkciók is implementálásra kerültek legújabb operációs rendszerükben.

Folytatva a Windows XP-vel indult trendet, a Windows 7 is különböző otthoni és üzleti felhasználásra készült kiadásokat nyújt. De eltérően a Windows XP-től, ezek a kiadások nem hadver típus vagy processzor architektúra szerint kerültek csoportosításra.

A **Windows 7** termékcsaládja négy fő tagból áll:

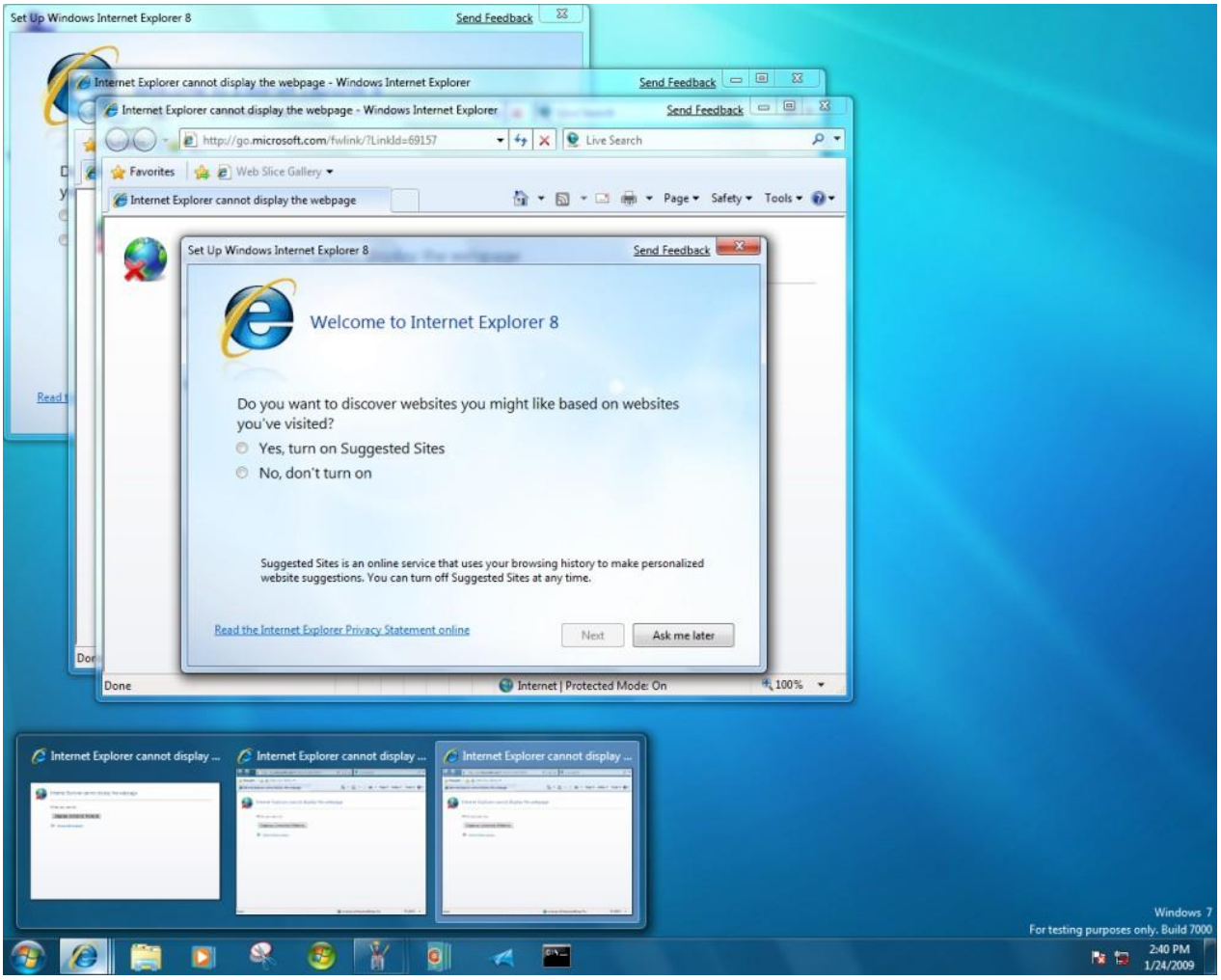
- *Home Basic Edition*, az átlag felhasználó számára: alapszintű belépési pontot biztosít a Windows 7 használatához.
- *Home Premium Edition*, haladó felhasználók számára: túllép az alapszintű szolgáltatásokon, elérhetővé teszi a Windows Aero felület használatát, a Mobility Center és Tablet PC támogatást laptopok számára, és a Windows Media Centert, mely eltérően a korábbi Windows operációs rendszerektől, beépített szolgáltatásként szerepel a Windows 7-ben.
- *Professional Edition*, üzleti célokra és haladó felhasználóknak: abban módosult a Home Premium Edition-höz képest, hogy magasabb szintű hardver védelmet, üzleti hálózat-kezelést, és távoli asztali elérést biztosít, és kivették belőle a Windows Media Centert.
- *Ultimate Edition*, mely az egész csomagot magába foglalja: minden funkciót és szolgáltatást egyesít az összes elérhető kiadásból.

Két másik kiadás is elérhető, melyek speciális célokra készültek:

- *Starter edition*, az abszolút kezdő személyi számítógép és Windows használóknak, fejlődő piacoknak. (főleg új laptopokra telepítik a gyártók)
- *Enterprise Edition*, nagyvállalatok számára készült, azok magasabb szintű adatvédelmi, kompatibilitási és nemzetközi támogatási igényeit igyekszik kielégíteni.

A Windows 7 néhány új funkciót foglal magába, mint például a multi-touch és a kézírás-felismerés, támogatja a virtuális merevlemezeket, javítja a több processzormagos rendszerek teljesítményét, a boot teljesítményt, továbbfejlesztett kernellel rendelkezik. Nagyban javították az energiagazdálkodást. A Windows XP külön kiadással rendelkezett a Windows Media Center használatához, de a Windows 7-ben már beépített funkcióként szerepel annak egy újabb verziója. A vezérlőpult is nagy változásokon ment keresztül, sok új elem került ide. A biztonságért felelős Windows Security Centert Windows Action Center-ré avanzsálták, mely a számítógép biztonságát és karbantartását öleli körül. Továbbá úgy tervezték a rendszert, hogy sokkal gyorsabban kerüljön alvó állapotba, és gyorsabban álljon vissza a rendszer alvó állapotból.

A Tálca ment át a leglátványosabb változáson, immár a ’Superbar’ nevet viseli. A Gyorsindítás eszköztárat felváltotta az alkalmazások „feltűzése” (pin), rögzítése a tálcán. A rögzített alkalmazások a tálca részévé válnak, a gombok az alkalmazás futását reprezentáló gombbal integrálódnak. Ezek a gombok teszik lehetővé továbbá a Jump List funkció használatát, mely megkönnyíti a futó alkalmazások közötti tallózást. Az Asztal megjelenítése gomb a tálca jobb oldalára került, és segítségével elérhető az Aero Peek, mely felé húzva a kurzort szó szerint átnézhetünk az épp megnyitott ablakokon, azok átlátszóvá válnak így látható lesz az asztal. Az Aero Snap funkcióval könnyebben kezelhetőek az ablakok. A képernyő különböző részeire húzva egy ablakot különböző helyzetekbe kerülnek, például a képernyő jobb szélére húzva a képernyő jobb felét fogja elfoglalni, míg ha felülre húzzuk, teljes képernyőssé válik az ablak. Ez csak az Aero nyújtotta lehetőségek töredéke. Nagyban megkönnyíti a nagyobb mennyiségű ablakok kezelését.



A Windows 7 asztal, a Superbar-al és Jump list menüvel.

A felhasználóknak sokkal több Windows komponens kikapcsolására van lehetőségük, mint a Windows Vista esetében. Ilyenek például az Internet Explorer, Windows Media Player. A microsoft Virtual PC új néven, Windows Virtual PC-ként került be a Professional, Enterprise, és Ultimate változatokba. Egyazon gépen többféle Windows környezet futtatását teszi lehetővé. Ebbe tartozik a Windows XP Mode, mellyel teljes kompatibilitást élvezhetünk a Windows XP-vel. A Windows XP ilyenkor virtuális gépen fut, és ha egy program azon fut, annak kimenetét a Windows 7 asztalára irányítja, így az ott jelenik meg.

A Windows 7 Remote Desktop Protocol-ja (RDP, Távoli Asztali Protokoll) szintén sokat fejlődött, támogatja a valós idejű multimédiás alkalmazásokat, például a videó lejátszást, 3D játékokat, tehát engedélyezi a DirectX 10 használatát távoli asztali környezetekben.

III. Hálózati újítások

A Windows Server 2008 R2 és a Windows 7 operációs rendszerek olyan hálózati újításokat tartalmaznak, amelyek megkönnyítik a felhasználóknak, hogy csatlakozzanak, és csatlakozva is maradjanak, mindegy, hogy hol vannak vagy milyen típusú hálózatot használnak. Ezek az újítások lehetővé teszik az IT szakembereknek, hogy üzleti igényeiket biztonságos, megbízható és rugalmas módon elégítsék ki.

- **DirectAccess**, mely lehetővé teszi, hogy egy felhasználó belépjen egy vállalati hálózatba anélkül, hogy plusz lépésként egy virtuális magánhálózati kapcsolatot (virtual private network, VPN connection) létrehozna.

- **VPN (**Virtual Private Network): **VPN Reconnect**, mely azonnal automatikusan újra kialakítja a VPN kapcsolatot, amint helyreáll az Internet kapcsolat, így a felhasználónak nem kell újra hitelesíteniük magukat és újból létrehozni a VPN kapcsolatot.

- **BranchCache**: ez az alkalmazás folyamatosan figyeli, és egy fiókirodában vagy a központban gyorsítótárazza a fájl vagy Web szerverekről érkező frissített tartalmakat egy WAN-on, így csökkenti a WAN forgalmát.

- **URL-alapú QoS (Quality of Service)**: lehetővé teszi, hogy prioritási szintet rendeljünk az adatforgalomhoz az alapján, hogy mely URL az adott adatforgalom forrása.

- **Mobil Szélessávú Eszköz Támogatás** (Mobile Broadband Device Support): driver-alapú modelt biztosít olyan eszközök számára, amelyeket mobil szélessávú hálózatra való kapcsolódáshoz használunk.

- **Több aktív tűzfal profil**: a Windows 7 azt a tűzfal profilt alkalmazza, amely szabályai alapján a legjobban illik ahhoz a hálózathoz, amelyhez éppen csatlakozik számítógépünk.

- **Hálózati energiagazdálkodási lehetőségek**:
  - **Wake on Lan** (WoL), mellyel egy alvó állapotban lévő számítógép bizonyos hálózati aktivitás hatására felébreszthető.
  - **Low Power on Media Disconnect**: Ez az új Windows 7 funkció lehetővé teszi a számítógép számára, hogy a hálózati adaptert alacsony áramfelvételi állapotba helyezze, ha a LAN kábel ki van húzva és a számítógép be van kapcsolva.

- **Network Driver Interface Specification - NDIS 6.20**: Az NDIS egy standard interfészt határoz meg kernel-módú hálózati driverek és az operációs rendszer között, valamint meghatároz egy standard interfészt rétegelt hálózati driverek között, ezáltal absztraktálva alacsonyabb szintű drivereket amelyek magasabb szintű driverekhez tartozó hardvereket kezelnek.

- **Natív WWAN** támogatás

- **Background Intelligent Transfer Service 4.0**: Fájlokat továbbít (feltöltés és letöltés is) egy kliens és szerver között, és információt szolgáltat a folyamat állapotáról. Valamint egy peer-ről is lehet fájlokat letölteni.

- **DNSSEC:** A Windows 7 az első kliens operációs rendszer, amely tartalmazza a szükséges eszközöket, hogy ellenőrizze, hogy biztonságosan kommunikál egy DNS szerverrel, és igazolja, hogy a szerver végrehajtott egy DNSSEC érvényesítést helyette.

- **Wireless hálózati lehetőségek:**
  - **Virtual WiFi:** lehetővé teszi egy vezeték nélküli hálózati adapter számára, hogy két különböző kliens eszközként viselkedjen. Valamint virtuális eszközünket access point-tá tehetjük, így más WiFi eszközök csatlakozhatnak rá. Egyelőre ez a funkció (támogató driver híján) nem elérhető.

- **HomeGroup**

- **Ipv6, IPsec**

- **Távoli Segítségnyújtás (Remote Assistance):** Easy Connect funkció.

IV. IPv6 és a Windows 7

A Windows 7-el és a Windows Server R2-vel a Microsoft továbbra is támogatja az IPv6 támogatását egy protokoll stack-el, amely támogatja az ipari szabványokat, beépített alkalmazásokat és szolgáltatásokat. Mindkét operációs rendszerben alapértelmezettként engedélyezve van a beépített IPv6 támogatás.

A következő fejezetekben a Windows 7 olyan részeiről lesz szó, amelyek kihasználják az IPv6 adta lehetőségeket.

Néhány szervezet kikapcsolja az IPv6 támogatást Windowst futtató számítógépeiken. Sokan azért, mert úgy gondolják, hogy nem használnak olyan alkalmazásokat, amelyek használnák azt, míg mások talán azért, mert úgy vélik, hogy ha IPv4 és IPv6 is engedélyezve van, akkor az megduplázza a DNS és Web forgalmukat. De ez nem így van. Az interneten is sokfelé találkozunk oldalakkal, amelyek az IPv6 kikapcsolására adnak útmutatást.
A Microsoft meglátása az, hogy az IPv6 szerves része a Windows operációs rendszereknek, és az operációs rendszer és az alkalmazások fejlesztésekor és tesztelésekor is engedélyezve voltak. Így, mivel a Windows-t IPv6 használata mellett tervezték, kikapcsolásával néhány funkció és komponens nem fog működni. Így például olyan alkalmazások, amelyekről nem is gondolnánk, hogy használjuk – például a távoli segítségnyújtás, OtthoniCsoport, DirectAccess. Ezért a Microsoft az IPv6 bekapcsolva hagyását javasolja, még akkor is, ha nem áll rendelkezésünkre olyan hálózat, amely IPv6-ot használ. Így működhetnek az IPv6-ot használó alkalmazások (például a HomeGroup és a DirectAccess a Windows 7-ben csakis IPv6-al működnek).

IPv6

A Windows újabb verzióiba, mint például a Windows 7, Windows Server 2008 R2, és néhány korábbi verzió, már be van építve az Internet Protocol version 6 (IPv6) támogatása. A protokollba implementálva van az IP Security (IPSEC), mely a titkosításért és az authentikációért felelős, így nagyobb biztonságot nyújt, mint az IPv4.

Azért hozták létre az IPv6-ot, mert az IPv4-el kapcsolatban tervezésekor előre nem látott gondok merültek fel, mint például a címtartomány kimerülése, a címek elfogyása, illetve

azon terv miatt, hogy további funkcionalitást nyújtson a modern eszközöknek, és ezzel az Internetet megfeleljen a 21. század követelményeinek.

Tulajdonságai:

- Új fejrész formátum
- Nagy címtartomány
- Hatékony és hierarchikus címzési és útválasztási infrastruktúra
- Beépített biztonsági szolgáltatások
- Jobban támogatja a prioritással rendelkező kézbesítéseket
- Új protokollal rendelkezik a szomszédos csomópontok közötti együttműködéshez
- Bővíthetőség

V. Vállalati hálózatok elérése bárhonnan: DirectAccess

Egyre több felhasználó válik mobillá, hogy produktív maradhasson amíg a munkahelyen és az irodán kívül tartózkodik. Az IDC információi alapján 2008 harmadik negyedéve volt az a pont, amitől kezdve a gyártók világszerte több mobil számítógépet forgalmaztak, mint asztali számítógépet.

A mobil felhasználók száma várhatóan növekedni fog. Azonban a mód, ahogy a felhasználók elérik a hálózati erőforrásokat nem változott. Habár az otthoni szélessáv, vezeték nélküli szélessáv és a Wi-Fi lehetővé teszi, hogy az irodán kívül is csatlakozzanak az internetre, a vállalat tűzfalai meggátolják őket, hogy elérjék az intraneten található erőforrásokat. Azokat csak olyan felhasználók érhetik el, akik fizikailag csatlakoznak a szervezet vagy vállalat hálózatához. Ez sok gondot okoz a rendszergazdáknak, mivel csak olyankor tudják frissíteni a számítógépeket, amikor azok az intranetre csatlakoznak. Hogy ezt a korlátozást megkerüljék, sok szervezet használ VPN-t.

VPN

A Windows 7 támogatja a fejlett hálózati megoldásokat, például az IPsec-et és a VPN-t. Ezek a protokollok már egy ideje léteznek, de a Windows 7-ben könnyebben elérhetőek és használhatóbbak, mint a Windows korábbi kiadásaiban.

Számos szervezetnél használnak VPN kapcsolatokat, hogy alkalmazottaik beléphessenek a belső hálózataikba. Ezek a VPN kapcsolatok titkosítást használnak, hogy megvédjék a felhasználó és a hálózat között átvitt adatokat, továbbá távoli elérést biztosítanak a hálózathoz, így a felhasználó az internet segítségével bárhonnan beléphet a munkahelyi hálózatba, hozzáférhet a hálózati erőforrásokhoz, például a megosztott fájlokhoz, e-mail szerverekhez.

A VPN szabvány protokollokat használ (TCP/IP, SSL) a nyilvános hálózaton történő adattovábbításra, ezért nagyon könnyű használni. Háromféle típusú VPN létezik: Secure VPN, Trusted VPN és Hybrid VPN, ezek különböző folyamatokat használnak arra, hogy kapcsolatot építsenek ki egy távoli hálózattal. A Secure VPN kriptografikus bújtatás protokollt használ erre. Az adat továbbításakor annak titkosítására IPsec-et is képes használni, de támogatja az SSL-t is az adattitkosításra. A Point-to-Point Tunneling Protocol (PPTP), a VPN eredeti protokollja mára elavulttá vált, így már nem védi úgy az adatokat, mint a Layer 2 Tunneling Protocol (L2TP). Ezen felül az L2TP 3-as verziója (L2TPv3) szintén működik Windows 7 alatt.

A Trusted VPN nem használ kriptografikus készletet a bújtatás (tunneling) engedélyezésére. Helyette a szolgáltató hálózatát használja az adat titkosítására.

A legtöbb hálózat, amely támogatja a VPN-t rendelkezésre bocsát egy VPN klienst is, amelyet a kliens számítógépre kell feltelepíteni. Ha a hálózatban Routing and Remote Access Service-t (RRAS) használunk, akkor a Windows 7-ben lehetőségünk van a beépített kliens használatára.

VPN Reconnect

A VPN Reconnect egy új szolgáltatás az RRAS-ben, amely a felhasználóknak problémamentes és folyamatos VPN kapcsolatkészséget biztosít, automatikusan helyreállítja a VPN kapcsolatot, ha átmenetileg megszakad a felhasználó internet kapcsolata. Azok a

felhasználók fognak a legjobban profitálni ebből a képességből, akik vezetéknélküli mobil szélessávot használnak. A Windows 7 a VPN Reconnect segítségével automatikusan azonnal helyreállítja az aktív VPN kapcsolatot, amint újra elérhető lesz az internetkapcsolat. Bár az újrakapcsolódás néhány másodpercet azért igénybevehet, ez a felhasználók számára észrevétlen marad.

A kliens számítógépnek Windows 7 operációs rendszert kell futtatnia, hogy a VPN Reconnect funkciót képes legyen használni.

DirectAccess

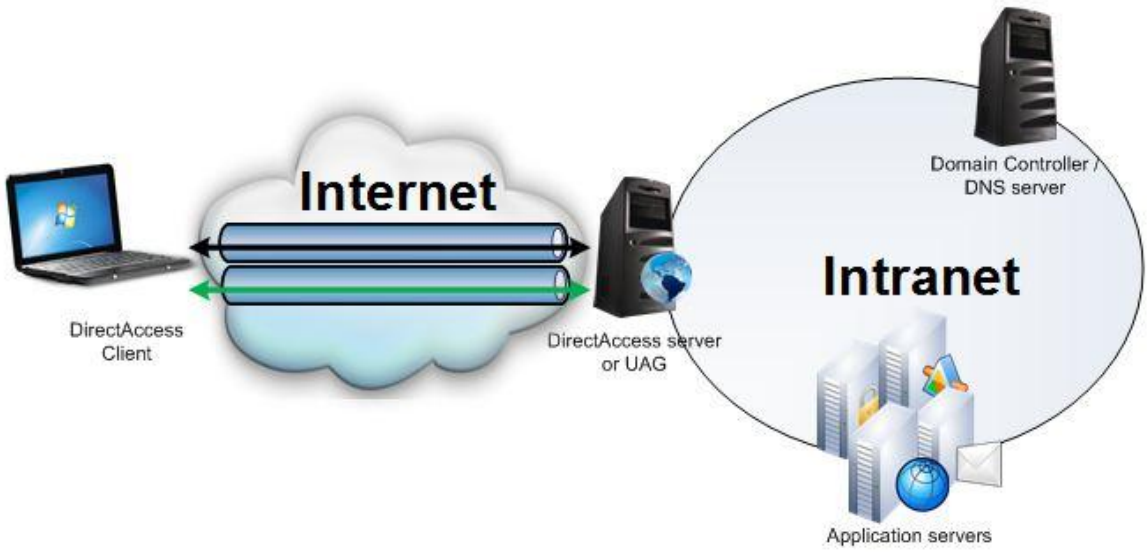
Tehát hagyományosan a felhasználók VPN (Virtual Private Network) segítségével kapcsolódnak intranet erőforrásokhoz. Azonban ez a következő okok miatt sokszor nem kifizetődő:

- Egy VPN kapcsolat kialakítása számos lépést igényel, és a felhasználónak várnia kell a hitelesítésre. Olyan szervezeteknél, amelyek a hálózatukba való belépés előtt ellenőrzik a kapcsolódó számítógép állapotát („egészségét”, hogy vírusok vagy egyebek miatt jelent-e valamilyen veszélyt a hálózatra), egy VPN kapcsolat kialakítása akár több percet is igénybe vehet.
- Bármikor, amikor a felhasználó elveszti az Internet kapcsolatot, újra kell kapcsolódniuk a VPN-nel is.
- A VPN kapcsolatok problémásak lehetnek olyan környezetekben, amelyek kiszűrik a VPN forgalmat.
- Az internetkapcsolat teljesítménye csökken, ha az intranetes és az internetes forgalom is a VPN-en keresztül bonyolódik le.

Ezen kényelmetlenségek miatt több felhasználó is elkerüli a VPN kapcsolatok használatát. Helyette inkább alkalmazás átjárókat használnak, mint például a Microsoft Outlook Web Access (OWA), hogy az intranetes erőforrásokat elérjék. Az OWA segítségével a felhasználó a belső levelezéséhez hozzáférhet ugyan, de az intraneten megosztott fájlokhoz és az e-mailek csatolt fájljaihoz nem képesek VPN nélkül hozzáférni.

A Microsoft nemrég egy kézenfekvő megoldással állt elő a VPN-el kapcsolatos problémák kiküszöbölésére.

A Windows Server 2008 R2 által bevezetett DirectAccess segítségével, a tartományi tag Windows 7 operációs rendszert futtató számítógépeknek lehetőségük van csatlakozni nagyvállalati hálózati erőforrásokhoz bármikor, amikor az Internetre csatlakoznak, és ehhez nincs szükségük VPN kapcsolatra sem. Ezekhez a hálózati erőforrásokhoz való hozzáférése alatt az internetre csatlakozott felhasználó gyakorlatilag ugyanazokat a lehetőségeket élvezheti, mintha közvetlenül a szervezet helyi hálózatára (LAN-jára) csatlakozna. Továbbá az IT szakemberek számára a DirectAccess az irodán kívüli mobil számítógépek menedzselését, kezelését is lehetővé teszi. Minden alkalommal, amikor egy tartományi tag számítógép csatlakozik az internetre, még mielőtt a felhasználó bejelentkezne, a DirectAccess létrehoz egy kétirányú kapcsolatot, amely lehetővé teszi a kliens számítógép számára, hogy naprakész maradjon a vállalat házirendjét illetően, és szoftverfrissítéseket fogadjon.



A DirectAccess biztonsági és teljesítménnyel kapcsolatos tulajdonságai többek között a felhasználó hitelesítés, titkosítás, és a hozzáférés-szabályozás. Beállítható, hogy az egyes felhasználók mely hálózati erőforráshoz kapcsolódhatnak, ezáltal akár teljes hozzáférés is adható, vagy csak néhány szerverre vagy hálózatra korlátozhatjuk az elérést. Van egy olyan lehetőség is, hogy csak az olyan forgalom halad át a DirectAccess szerveren, amelynek célja a

vállalati hálózat. Az internetes forgalmat forgalmat eltereli, hogy az a kliens számítógép által használt internet átjárón keresztül haladjon. Ez a lehetőség opcionális, úgy is konfigurálható a DirectAccess, hogy az összes forgalmat a vállalati hálózaton keresztül engedje.

A DirectAccess segítségével egy vállalat hálózati szakembere úgy kezelheti az irodán kívüli mobil számítógépeket, hogy frissíti a csoportházirendeket, és terjeszti a szoftverfrissítéseket, bármikor, amikor a mobil számítógép az internetre csatlakozik, még akkor is, ha a felhasználó nincs bejelentkezve.

Megszorítások

A DirectAccess szervernek mindenképpen Windows Server 2008 R2 operációs rendszert kell futtatnia, tartományi tag kell, hogy legyen, és két fizikai hálózati adapterrel kell rendelkeznie. A szervernek csakis DirectAccess szerverként kell létezni, nem szolgáltathat más elsődleges funkciót. A tartományi tag klienseknek Windows 7 operációs rendszert kell futtatniuk.

Az infrastruktúra felépítéséhez szükségesek a következők:

- **Active Directory Domain Services (AD DS).** Legalább egy Active Directory domaint létre kell hozni. A munkacsoportok nem támogatottak.

- **Csoportházirend (Group Policy).** A kliens beállítások alkalmazásához ajánlott csoportházirend beállítása.

- **Tartományvezérlő (Domain controller).** Legalább egy, a felhasználói fiókokat tartalmazó tartományvezérlő a tartományban Windows Server 2008-at (vagy újabb szerver operációs rendszert) kell, hogy futtasson.

- **IPsec házirendek.** A DirectAccess IPsec-el szolgáltat felhasználó azonosításra (authentikáció) és titkosításra az interneten keresztül történő kommunikációhoz.

- **IPv6.** Az Ipv6 szolgáltatja a szükséges végponttól-végpontig címzést a kliensek számára, hogy bármikor kapcsolódhassanak a vállalati hálózathoz. Azok a szerezetek, amelyek még nem képesek teljes mértékben alkalmazni az IPv6 címzést, különböző technológiákat használhatnak (ISATAP, Teredo, 6to4), hogy csatlakozzanak az IPv4-et használó interneten keresztül, és elérjenek IPv4 erőforrásokat a vállalati hálózatban.

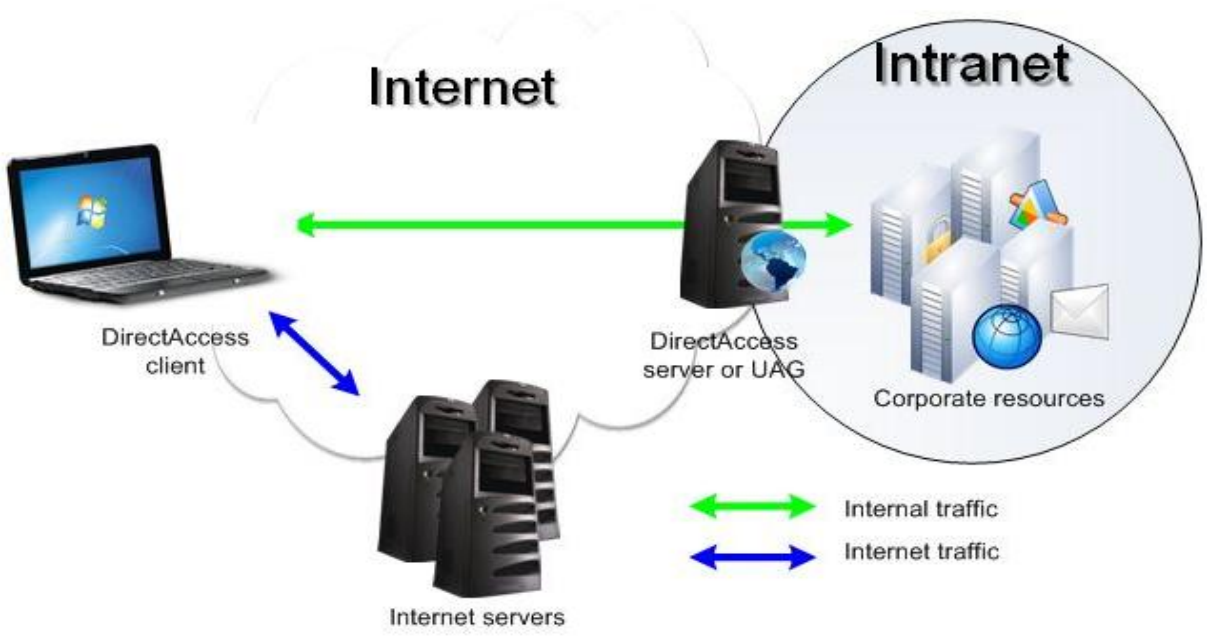
Az IPv6, vagy ezek az átalakítási technolgóiák elérhetőek kell, hogy legyenek a DirectAccess szerveren.

A DirectAccess kapcsolódási mechanizmusa

A DirectAccess kapcsolódási folyamata automatikusan történik, nincs szüksége a felhasználó beavatkozására.

Az internetes és intranetes forgalom szétválasztása

A DirectAccess képes megkülönböztetni és szétválasztani az internetes és az intranetes forgalmat, hogy csökkentse a vállalati hálózatra nehezedő felesleges forgalom okozta terhet. A legtöbb VPN az összes forgalmat (még azt is, amelynek célja az Internet) a VPN kapcsolaton keresztül küldi, így lassítja mind az internetes, mind az intranetes kapcsolatot. Mivel az internetre irányuló kommunikációnak nem kell a vállalati hálózaton keresztül kijutnia az internetre, a DirectAccess nem lassítja ily módon az internetelérést.



Beállítható továbbá, hogy az összes forgalmat, kivéve a helyi alhálózat forgalmát, a DirectAccess szerveren és az intraneten keresztül irányítsuk. Ha ez a funkció engedélyezve van, akkor az összes kommunikáció az IP_HTTPS protokollt használja, mely IP csatornákat épít ki a HTTPS protokollon belül, így azok átjuthatnak tűzfalakon és proxy szervereken.

Egyesítve ezt az opciót a Windows Tűzfallal, az IT adminisztrátorok teljes irányítással rendelkeznek afelett, hogy mely alkalmazások bonyolíthatnak forgalmat, és mely alhálózat kliens számítógépeit érhetik el.

Network Access Protection (NAP)

Annak érdekében, hogy elkerüljük a rosszindulatú programok (vírusok, férgek, kémprogramok) terjedését a hálózaton, és hogy elősegítsük a kapcsolódó számítógépek együttműködését a biztonsági és egészségi követelményekkel és a házirendekkel, a nem-együttműködő klienseket kizárhatjuk az intranetből, korlátozhatjuk a hálózati erőforrásokhoz való hozzáférésüket illetve a házirenddel együttműködő számítógépekkel való kommunikációjukat. A Network Access Protection és a DirectAccess együttes használatával az IT adminisztrátorok a DirectAccess kliens számítógépeitől megkövetelhetik, hogy együttműködjenek a vállalat előírásaival a vírusmentességet illetően. Például egy kliens számítógép csak akkor csatlakozhat a DirectAccess szerverre, ha rendelkeznek a legfrissebb biztonsági frissítésekkel, káros programok elleni védelemmel, és egyéb biztonsági beállításokkal.

Ahhoz, hogy együtt használhassuk a NAP-ot és a DirectAccess-t, a kezdeti kapcsolat kialakításakor a NAP-ot használó DirectAccess klienseknek be kell nyújtaniuk egy egészségi bizonyítványt hitelesítésre a DirectAccess szervernek. A bizonyítvány tartalmazza a számítógép azonosításához szükséges információkat, és bizonyítékot a rendszer vírus- és kémprogram mentességéről. Ezt a bizonyítványt a kapcsolat kiépítése előtt az internetről szerzi be a kliens számítógép úgy, hogy információkat küld állapotáról egy interneten lévő szervernek, mely kiállítja a bizonyítványt.

A DirectAccess-t NAP-al használva egy nem-együttműködő kliens számítógép, amely esetlegesen ártó programmal van megfertőzve, nem csatlakozhat az intranetre a DirectAccess segítségével, így csökkentve a vírusok és egyebek terjedését.

Nem szükséges ugyan a NAP használata, de erősen ajánlott, mivel nagyban növeli a vállalat hálózatának biztonságát.

DirectAccess hitelesítés

A DirectAccess hitelesíti a számítógépet, mielőtt a felhasználó bejelentkezik. Általában a számítógép-hitelesítés csak tartományvezérlőkhöz és DNS szerverekhez biztosít hozzáférést.

Miután a felhasználó bejelentkezik, a DirectAccess hitelesíti a felhasználót, így az hozzáférhet bármilyen erőforráshoz, amihez jogosultsággal rendelkezik.

A DirectAccess támogatja az alapszintű – jelszóval és felhasználóval történő – felhasználó hitelesítést. Magasabb szintű védelem érdekében kétfaktorú hitelesítést is implementálhatunk smartcard segítségével. Ez a fajta konfiguráció ugyan lehetővé teszi a felhasználóknak, hogy hozzáférjenek internetes erőforrásokhoz smart cardok nélkül, de intranetes erőforrásokhoz való kapcsolódáshoz smart card szükségeltetik.

Tehát a felhasználónak a felhasználóneve és jelszava megadása mellett be kell helyeznie egy smart card-ot is. A smart card-os authentikáció meggátolja olyan támadók belépését a vállalat hálózatába, akik megszerezték a felhasználó felhasználói nevét és jelszavát, de a smart card-ot nem. Hasonlóan, ha csak a smart card-al rendelkezik a támadó, de nem tudja a felhasználónevet vagy a jelszót, akkor nem képes a hitelesítésen átjutni.

IPsec

Az Internet Protocol security (IPsec, IP biztonság) nyílt szabványok internetes kommunikáció védelmére szolgáló kerete Internet Protocol (IP) hálózatok felett, kriptografikus biztonsági szolgáltatások használatával. Az IPsec támogatja a hálózati szintű peer azonosítást, adatszármazás hitelesítést, adatintegritási, adat bizalmassági (titkosítási), és ismétlési védelmet. Az IPsec Microsoft általi implementációja az Internet Engineering Task Force (IETF) IPsec munkacsoportja által kifejlesztett szabványokra épül.

Az IPsec-et támogatja a Microsoft Windows 7, Windows Server 2008 R2, Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP és a Windows 2000 operációs rendszerek, és integrált része az Active Directori Domain Services-nek. IPsec házirendeket csoportházirendeken keresztül állíthatunk be, amely lehetővé teszi az IPsec beállítások magas (pl. tartomány, szervezeti egység, biztonsági csoport) szintű konfigurálását.

A Windows 7-ben az IPsec viselkedését a Fokozott biztonságú Windows tűzfal (Windows Firewall with Advanced Security) beépülő modullal konfigurálható.

IPsec és DirectAccess

A DirectAccess túllép a VPN korlátain azzal, hogy automatikusan létrehoz egy kétirányú kapcsolatot a kliens számítógép és a vállalati hálózat között. A DirectAccess két nagyon

fontos, szabványokon alapuló technológia által létrehozott alapra épült: Internet Protocol security és IPv6.

A DirectAccess IPsec-et használ a számítógép és a felhasználó hitelesítésére, ezzel lehetővé téve a rendszergazdáknak, hogy anélkül igazgassák a mobil számítógépet, hogy a felhasználó bejelentkezne. Opcionálisan elvárható a smart card használata a felhasználó hitelesítéséhez.

A DirectAccess az interneten keresztül folytatott kommunikáció titkosítására is hasznosítja az IPsec-et. Olyan IPsec titkosítási módok használhatók, mint a Triple Data Encryption Standard (3DES) és az Advanced Encryption Standard (AES).

A kliensek létrehoznak egy IPsec csatornát az IPv6 forgalom számára a DirectAccess szerverhez. Ez a csatorna átjáróként szolgál az intranetbe. A kliensek akkor is képesek csatlakozni, ha tűzfal mögött vannak.

A DirectAccess kliens két IPsec alagutat alakít ki:

IPsec Encapsulating Security Payload (ESP) alagút, számítógép tanúsítvány használatával. Ez a csatorna egy intranetes DNS szerverhez és egy tartományvezérlőhöz biztosít hozzáférést, így lehetővé téve a számítógép számára, hogy Csoportházirend objektumokat töltsön le, és hogy hitelesítést kérjen a felhasználó számára.

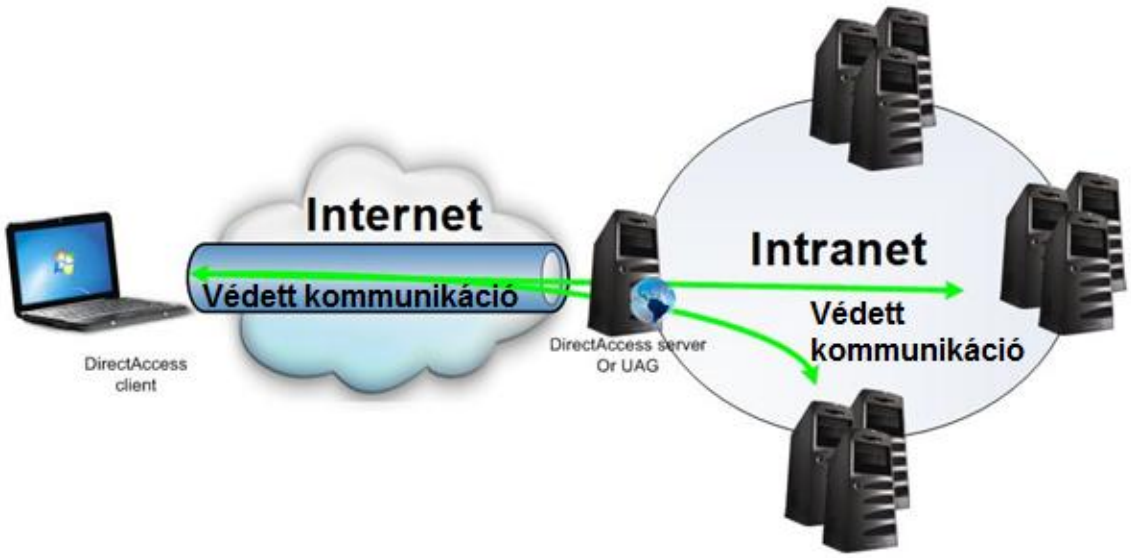
IPsec ESP tunnel, tanúsítvány és felhasználói hitelesítő adatok használatával. Ez a tunnel hitelesíti a felhasználót, és biztosítja az intranetes erőforrások és alkalmazásszerverek elérését. Például ezt az alagutat létre kellene hozni, mielőtt a Microsoft Outlook leveleket tölthetne le az intranetes Microsoft Exchange Serverről.

Miután létrejöttek a csatornák a DirectAccess szerverhez, a kliens azokon keresztül küldhet adatokat az intranetre. A DirectAccess szerveren beállíthatjuk, hogy a távoli felhasználók mel yalkalmazásokat futtathatják, és mely erőforrásokhoz férhetnek hozzá.

A kliensek kétféle IPsec védelmet használva csatlakozhatnak a vállalati hálózathoz: end-to-end és end-to-edge.

Végponttól-végpontig (End-to-end) védelem

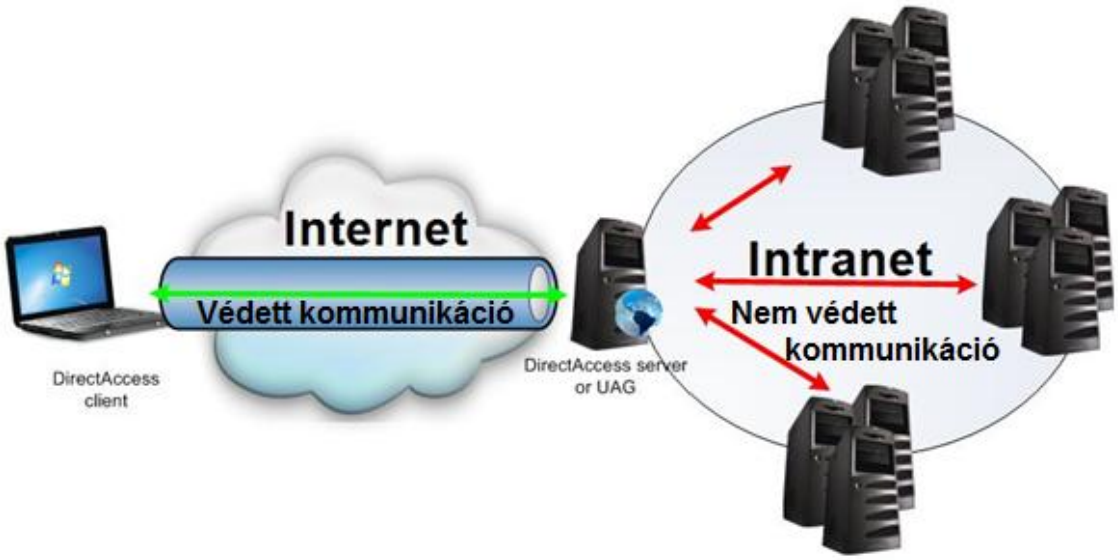
Ezzel a fajta védelemmel a DirectAccess kliensek létrehoznak egy IPsec session-t a DirectAccess szerveren keresztül minden alkalmazás szerverhez, amelyhez csatlakoznak. Ez a legmagasabb szintű védelmet nyújtja, mert a DirectAccess szerveren konfigurálható a hozzáférés-szabályozás. Azonban ez az architektúra csak akkor működik, ha a szervereken Windows Server 2008 vagy Windows Server 2008 R2 operációs rendszer fut, és IPv6-ot és IPsec-et is használnak.



Végponttól-végpontig védelem

Végponttól-peremig (End-to-edge) védelem

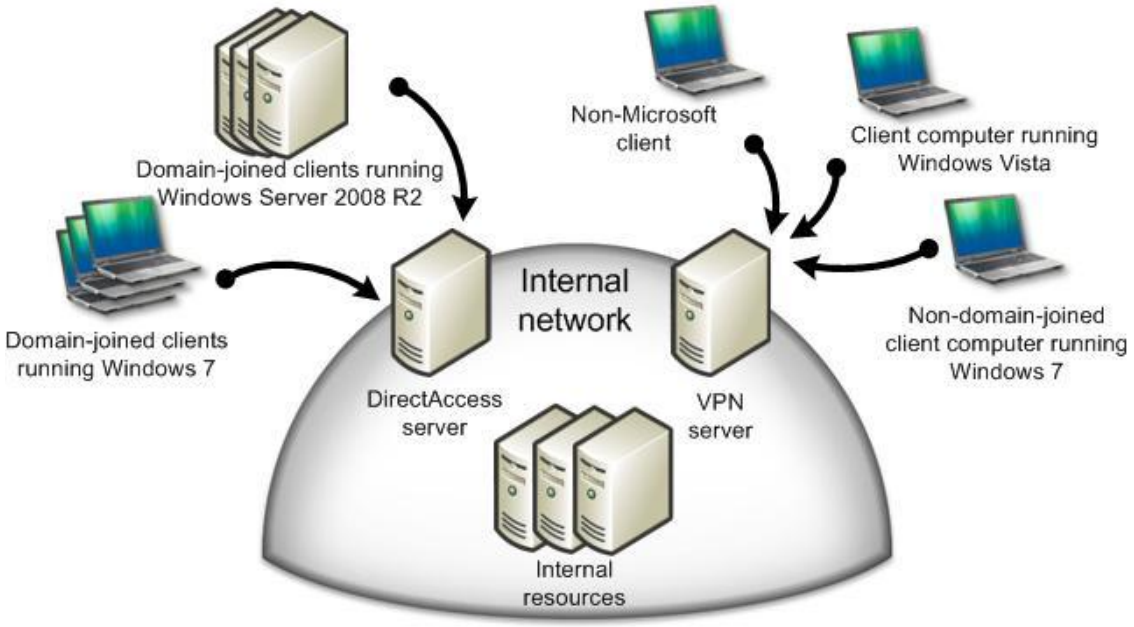
A DirectAccess kliensek létrehoznak egy IPsec session-t egy IPsec gateway szerverhez (amely alapértelmezésként egyezik a DirectAccess szerverrel). Az IPsec átjáró szerver ezután védelem nélküli forgalmat továbbít az alkalmazásszervereknek az intraneten. Ez a felépítés nem igényli az IPsec használatát az intraneten belül, és bármely IPv6 használatára képes alkalmazásszerverrel működik.



Végponttól-peremig védelem (pirossal jelölve a nem védett forgalom az intraneten belül)

DirectAccess és VPN párhuzamos működése

A legtöbb szervezet DirectAccess-t és VPN-t párhuzamosan fog használni, hogy az összes kliens számára biztosítsa a távoli elérést. Azon a klienseknek, amelyek képesek DirectAccess-t használva kapcsolódni, ajánlott kihasználni ezt az észrevétlenül működő, rugalmas és nagyon biztonságos belépési módot. Azok a kliensek, amelyek nincsenek a tartományhoz csatlakoztatva, vagy még nem rendelkeznek Windows 7-el, továbbra is használhatnak VPN-t. Továbbá azok a távoli irodák, amelyek nem rendelkeznek Windows Server 2008 R2 operációs rendszert futtató számítógéppel, hogy DirectAccess szerverként szolgáljon, biztosítsanak VPN szervert a távoli kapcsolódás megoldásához.

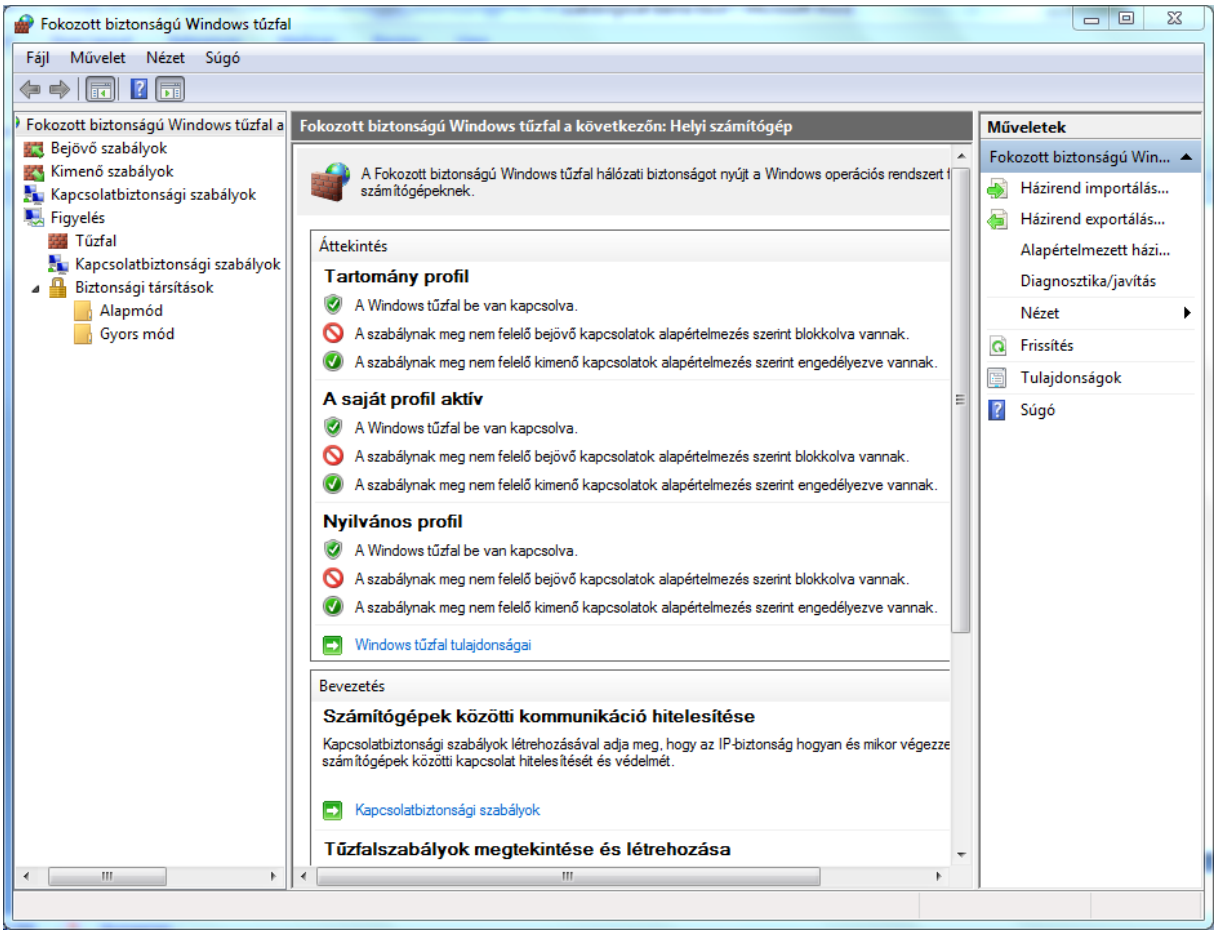


DirectAccess és VPN párhuzamos működése

VI. Fokozott biztonságú Windows tűzfal (Windows Firewall with Advanced Security)

A hálózatunk és adataink védelme egy rétegelt, mélységében védelmet nyújtó biztonsági modellt kíván meg. Nem csak az internet irányából érkező jogosulatlan felhasználóktól és programoktól kell megvédenünk hálózatba kötött számítógépeinket, de az intranet hasonló veszélyforrásaitól is óvnunk kell azokat. Egy rétegelt felépítésű biztonsági rendszer védelmet képes biztosítani jogosulatlan, kezeletlen, és nem-együttműködő számítógépektől, függetlenül attól, hogy ezek hogyan csatlakoznak a hálózatra.

A Fokozott biztonságú Windows tűzfal (Windows Firewall with Advanced Security) a rétegelt biztonsági modell fontos része. Azzal, hogy host-alapú, kétirányú hálózati forgalom szűrést biztosít a számítógépnek, a Fokozott biztonságú Windows tűzfal blokkolja a helyi számítógépbe be-, illetve az onnan kiirányuló jogosulatlan hálózati forgalmat. Továbbá együttműködik a Network Awareness-el (hálózatfigyelés), hogy olyan biztonsági beállításokat alkalmazhasson, amely a legjobban illik azokhoz a típusú hálózatokhoz, amelyekhez a számítógép éppen csatlakozik.

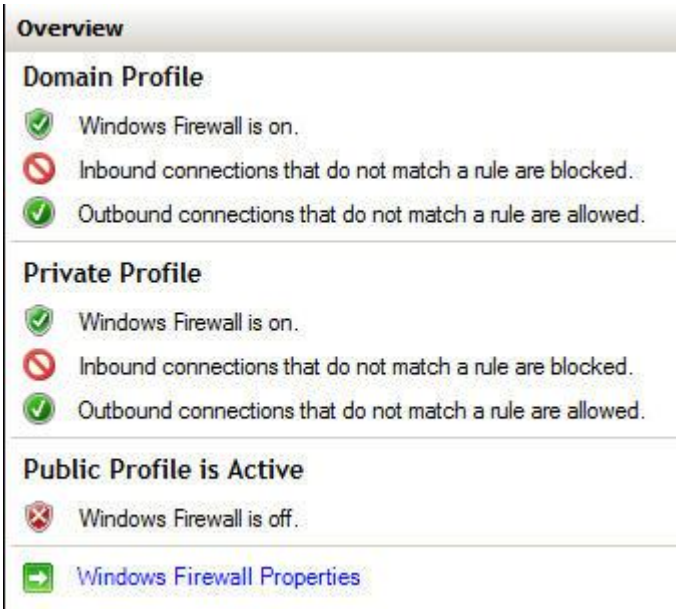


A Fokozott biztonságú Windows tűzfal kezdőképernyője.

Most, hogy a Windows tűzfal és az Internet Protokoll Biztonság (IPsec) konfigurációs beállításai egyetlen Microsoft Management Console-ba (MMC-be), a Fokozott biztonságú Windows tűzfalba lettek integrálva, a Windows Tűzfal fontos részévé válik a hálózatok izolációs stratégiájának.

Újdonságok a Windows 7-ben

Több aktív profil. A Windows Vista-ban és a Windows Server 2008-ban csupán egyetlen tűzfal profil lehet aktív egy időben. Ha egy számítógép egynél több hálózatba is be van kötve, akkor az a profil kerül alkalmazásra a számítógépen az összes kapcsolatra, amely a legtöbb megszorító szabályt tartalmazza. A Nyilvános profil (Public profile) a legbiztonságosabb, ez tartalmazza a legtöbb megszorítást, ezt követi a saját profil (Private Profile), majd a Tartomány profil (Domain profile).

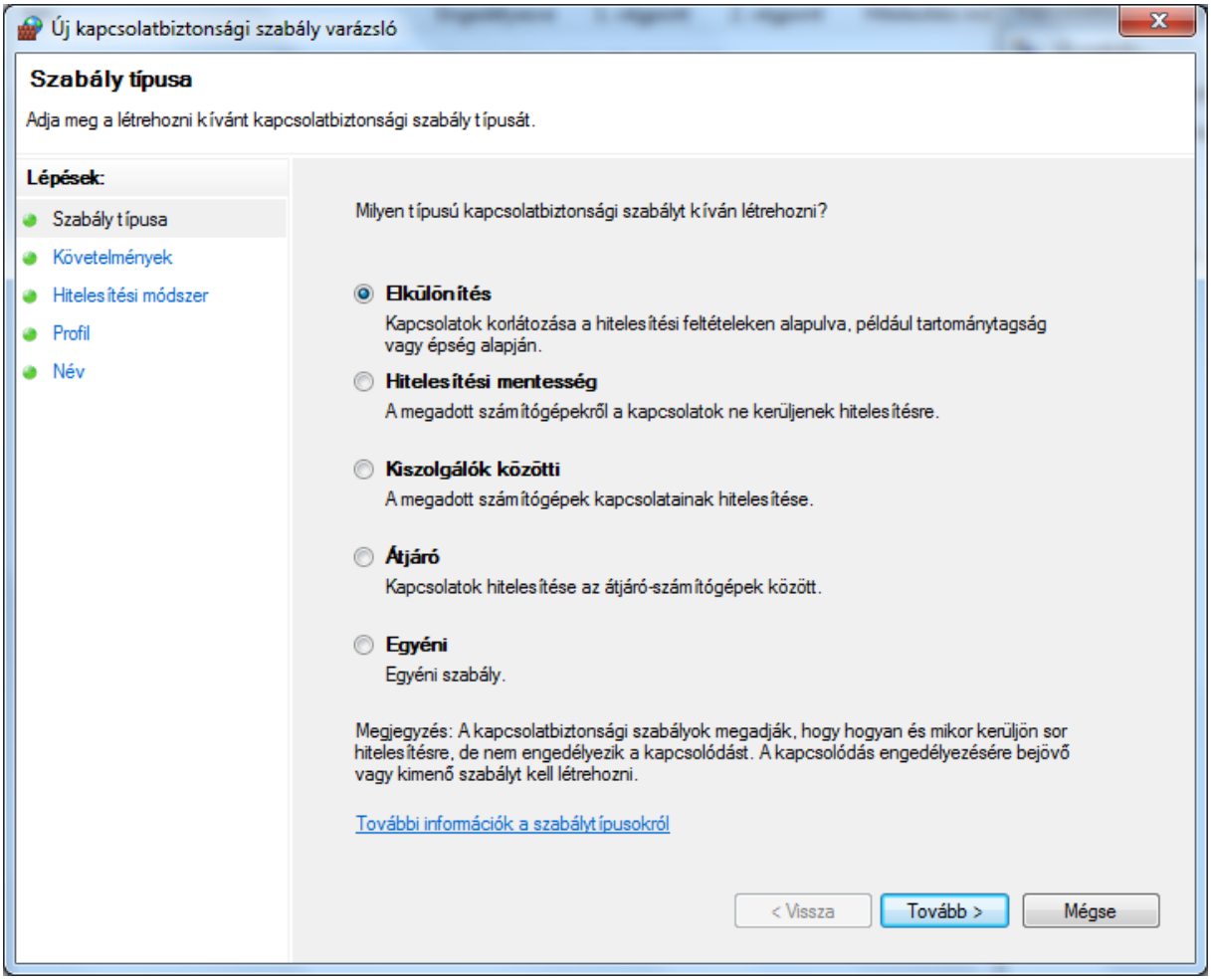


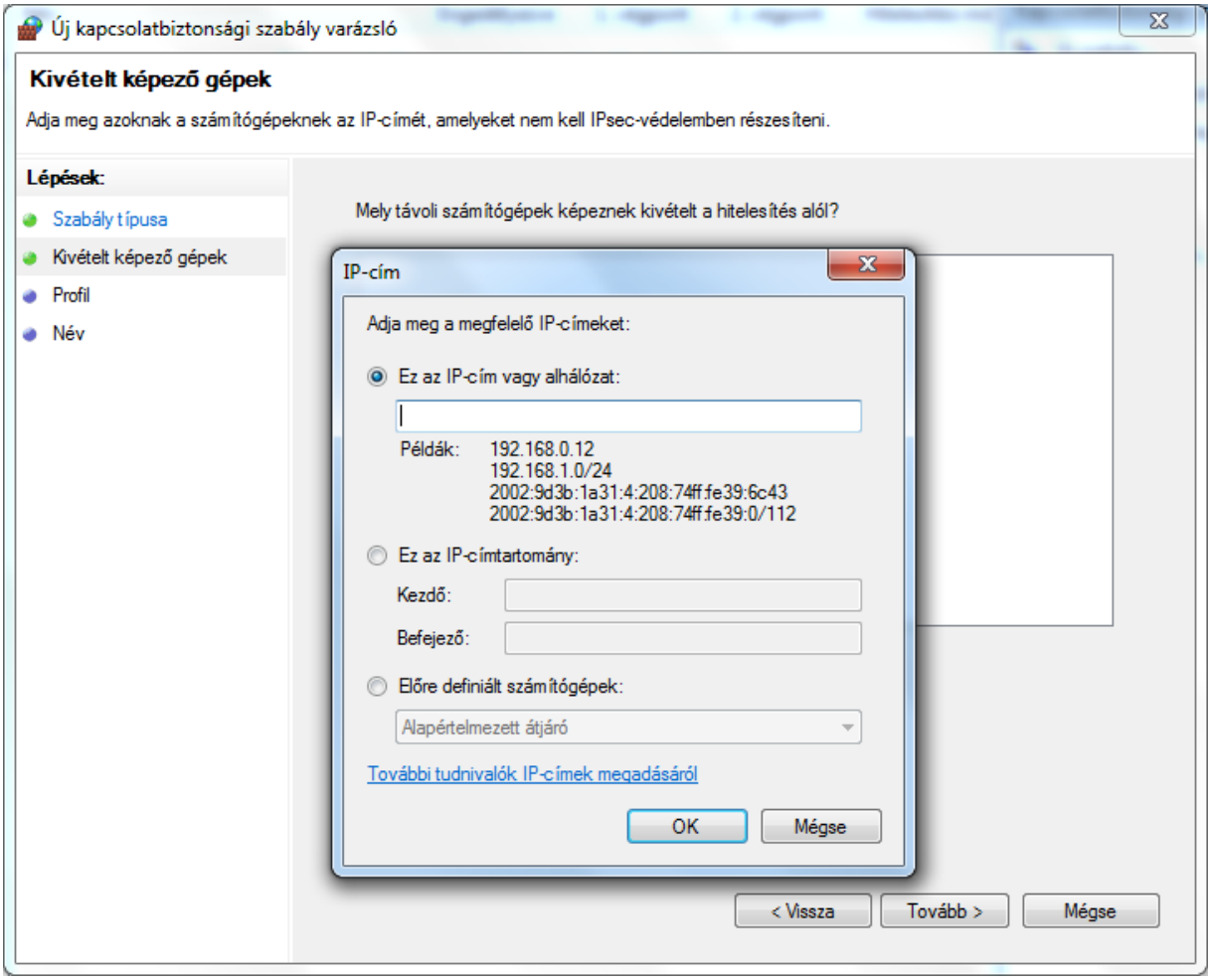
A Windows 7-ben és a Windows Server 2008 R2-ben minden hálózati adapterhez a megfelelő profilt rendelhetjük (tartományi, saját vagy nyilvános), függetlenül minden más hálózati adaptertől a számítógépen. Az egyes hálózatok forgalma a hálózat típusának megfelelő szabályok alapján kerül feldolgozásra.

Más gyártó tűzfala mellett is működhet. A Fokozott biztonságú Windows tűzfal egy sor olyan szolgáltatásból áll, amely sokkal többet nyújt, mint egy hagyományos tűzfal. Több tűzfal program problémás lehet a konfliktusok miatt, ezért ha harmadik gyártótól származó tűzfal programot telepítünk, ki kell kapcsolni a Windows Tűzfalat. A Windows korábbi verzióiban a tűzfal kikapcsolása azt is jelentette, hogy az összes hozzá kapcsolódó szolgáltatást is kikapcsoljuk. Ha a telepített program nem kínál ugyan olyan funkcionalitást, akaratlanul is kitehetjük magunkat olyan veszélyeknek, amelyek ellen immár nincs védelmünk. A Windows 7-ben a Fokozott biztonságú Windows tűzfal részegységeit és szolgáltatásait specifikusabban van lehetőségünk kikapcsolni. Ha egy harmadik gyártótól származó tűzfal programot telepítünk, akkor a telepítést végző felhasználónak lehetősége van a Fokozott biztonságú Windows tűzfal csupán azon részeit kikapcsolni, amely ütközik a

telepített program által nyújtott szolgáltatásokkal. A többi szolgáltatás bekapcsolva marad, és továbbra is védi a számítógépet.

Engedély kivételek. Ha olyan bejövő tűzfal szabályt hozunk létre, amely meghatározza, hogy mely számítógépek vagy felhasználók felhatalmazottak arra, hogy a hálózaton keresztül belépjenek a számítógépbe, a Windows 7 támogatja azt a képességet, hogy kivételeket határozzunk meg a felhatalmazottak listájához. Például azonosíthatunk egy csoportot engedélyezettekként, de erre a listára vonatkozólag meghatározhatunk egy számítógépet vagy egy felhasználót, amely tagja az engedélyezettek csoportjának. A mindkét listán szereplő számítógépek vagy felhasználóktól megtagadjuk a hozzáférést. Az ezektől érkező hálózati forgalmat a tűzfal blokkolja.





Létrehozhatunk olyan kimenő szabályt, amely meghatározza mind az engedélyezett számítógépek listáját, mind azon számítógépeket, amelyek e lista kivételei.

Az MMC beépülő modulban létrehozott kapcsolat szabályokban szereplő portok és protokollok specifikációja. A Fokozott biztonságú Windows tűzfal Microsoft Menedzsment Konzol (MMC) beépülő modul használatával a Windows 7-ben létrehozhatunk olyan kapcsolatbiztonsági szabályokat hozhatunk létre, amelyek portszámokat és protokollokat határoznak meg. Csak az olyan hálózati forgalom lesz alanya az IPsec által igényelt kapcsolatbiztonsági szabályoknak, amelyek ezekre a portokra irányulnak, vagy ezekről a portokról indulnak, vagy a meghatározott protokollt használják. A Windows Vista-ban és a Windows Server 2008-ban ezek a szabályok csak a **netsh** parancssori eszköz segítségével hozhatók létre.

Port intervallumok. A Windows 7-ben és a Windows Server 2008 R2-ben a tűzfal szabályok portszámok intervallumai is képesek meghatározni (például egy program a hálózatba csak az 5000 és 5010 közötti portok használatával léphet be. Ugyanezt megtehetjük az olyan kapcsolatbiztonsági szabályoknál, amelyek hitelesítési kivételeket határoznak meg.

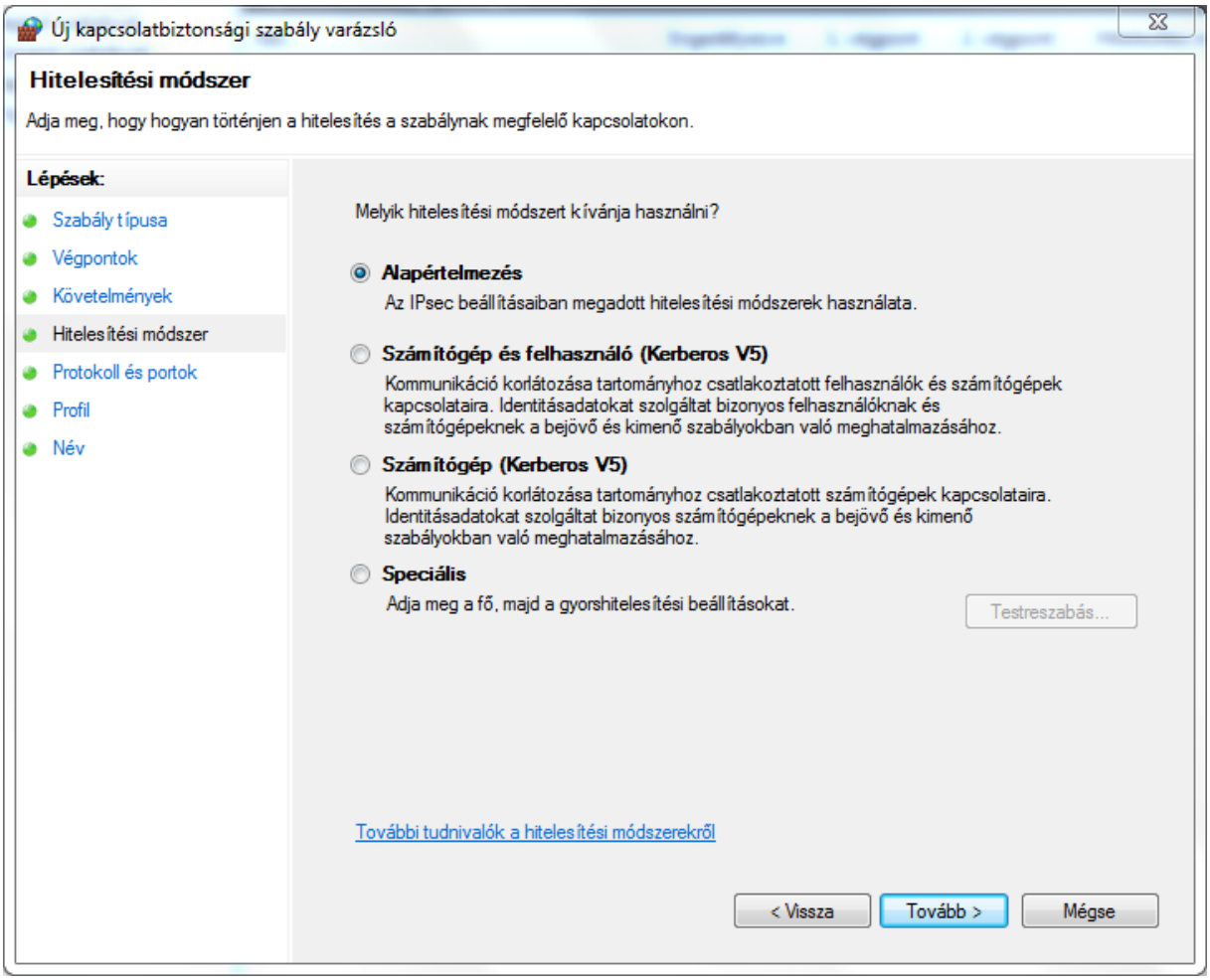
Suite B algoritmusok. Azok a kapcsolatbiztonsági szabályok, amelyek fejlettebb hitelesítési és titkosítási algoritmusokat határoznak meg (ezeket nevezzük „Suite B" algoritmus készleteknek), a Fokozott biztonságú Windows tűzfal MMC beépülő modullal segítségével létrehozhatók. A Windows korábbi verzióiban ezek a szabályok csak a **netsh** parancssori eszköz segítségével hozhatók létre.

Dinamikus titkosítás. A tűzfal szabályok támogatják a dinamikus kódolást, ezzel egyszerűsítve olyan IPsec kapcsolatbiztonsági szabályok létrehozását, amelyek portonkénti titkosítási beállításokat igényelnek. Alapvetően így egy adminisztrátornak nem kell kettő vagy akár annál is több kapcsolatbiztonsági szabályt beállítani mind a kliens számítógépen, mind a szerveren, hogy elérje a portonkénti titkosítást. Helyette elég létrehoznunk egy olyan kapcsolatbiztonsági szabályt a szerveren és a kliens számítógépen, amely IPsec védelmet igényel a szerver és az összes kliens között. A folyamatot azzal tesszük teljessé, hogy létrehozunk egy új tűzfal szabályt a szerveren, amely meghatározza azt a portot, amely forgalmát titkosítani kell. Ezen szabály miatt a szerver elindít egy gyors módú tárgyalást a klienssel, amint a hálózaton megérkezik az első csomag a meghatározott porttal.

Hitelesítés null enkapszulációval. Létrehozhatunk olyan kapcsolatbiztonsági szabályokat, amelyek meghatározzák a hitelesítést, de nincs meghatározva Encapsulating Security Payload (ESP) vagy Authenticated Header (AH) védelem az adatcsomagokon. Ez lehetővé teszi a hitelesítéses védelmet oylan környezetekben, ahol a hálózati felszerelés nem kompatibilis az ESP-vel vagy AH-val, mint például a behatolás érzékelő vagy védelmi rendszerek, még akkor is, ha a forgalom nem titkosított. Mielőtt adat továbbítódna a kapcsolatban, hitelesítés történik, de az egyéni csomagok az adatfolyamban nem kapnak IPsec védelmet.

Dinamikus csatorna végpontok. Létrehozhatunk olyan tunnel mód kapcsolatbiztonsági szabályokat, amelyek a tunnelnek csak az egyik végpontja számára határoz meg egy címet.

Tunnel mód hitelesítés. Meghatározhatjuk, hogy csak a jogosultsággal rendelkező számítógépek és jogosult felhasználók állíthatnak fel bejövő csatornát egy IPsec átjáró szerver felől. Főleg akkor kell biztosítani, hogy csak a jogosult felhasználók léphessenek be a vállalati hálózatba, ha dinamikus csatorna végpontokat használunk.



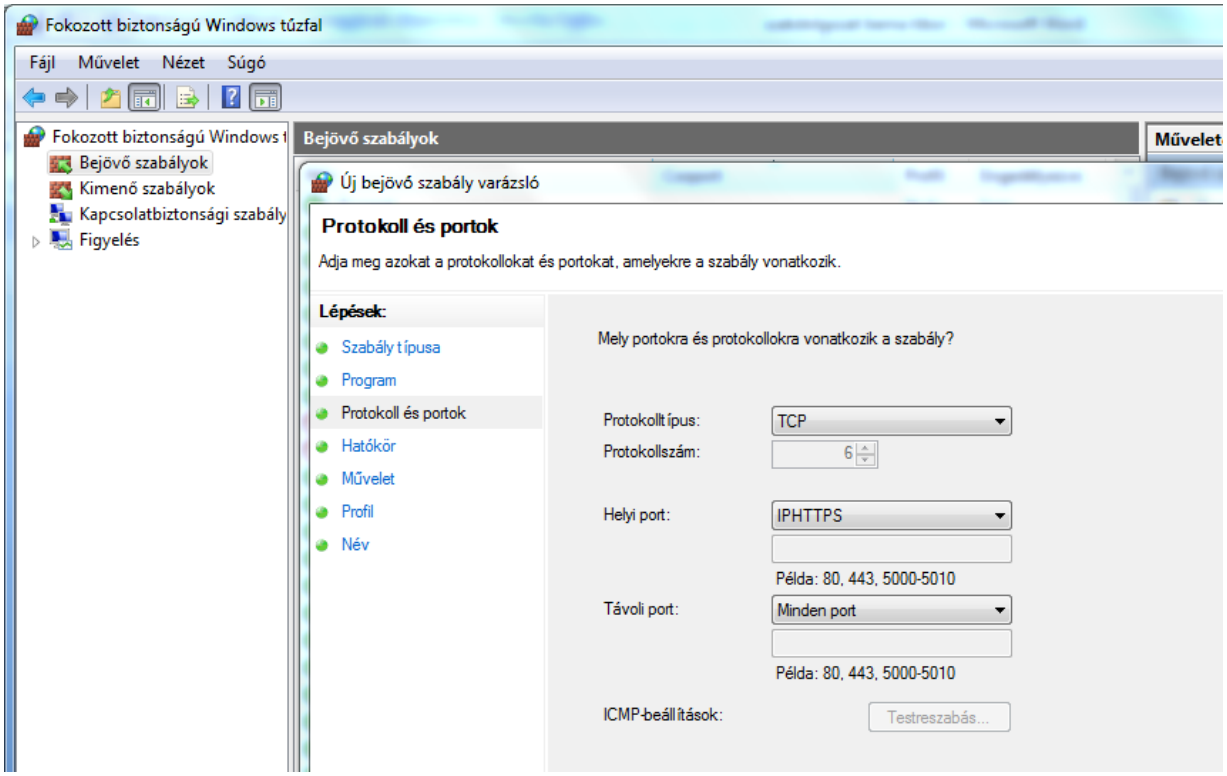
A Windows 7-ben és a Windows Server 2008 R2-ben felhasználók vagy számítógépek csoportját is meghatározhatjuk, akik jogosultak létrehozni egy tunnelt a helyi számítógéphez. Létrehozhatunk olyan csatorna-módú kapcsolatbiztonsági szabályokat, amelyek meghatározzák, hogy hitelesítés szükséges a tunnelhez, amelyeket a szabály hozott létre.

A tunnel mód szabály meg kell hogy adjon olyan hitelesítést, amely képes azonosítani a távoli számítógépet vagy felhasználót, és aztán a hitelesítési adatokat átadja a helyi számítógép számára. A számítógép vagy felhasználó adatai ezután összehasonlításra kerülnek a jogosultak listájával, és ha van egyezés, akkor a tunnel létrejön és adatcsere történhet. Ha a kapcsolódást végző számítógép vagy felhasználó nincs a helyi számítógép hozzáférésére

jogosultak listáján, akkor a kapcsolódás sikertelen lesz és a tunnel nem jön létre. Továbbá meghatározhatunk kivételeket a jogosultak listájához, így könnyen kreálhatunk „mindenki kivéve XY felhasználó” típusú szabályokat. A tunnel mód hitelesítés csak bejövő, IPsec átjárónál végződő tunneleknél működik, kimenő csatornákra nem alkalmazható.

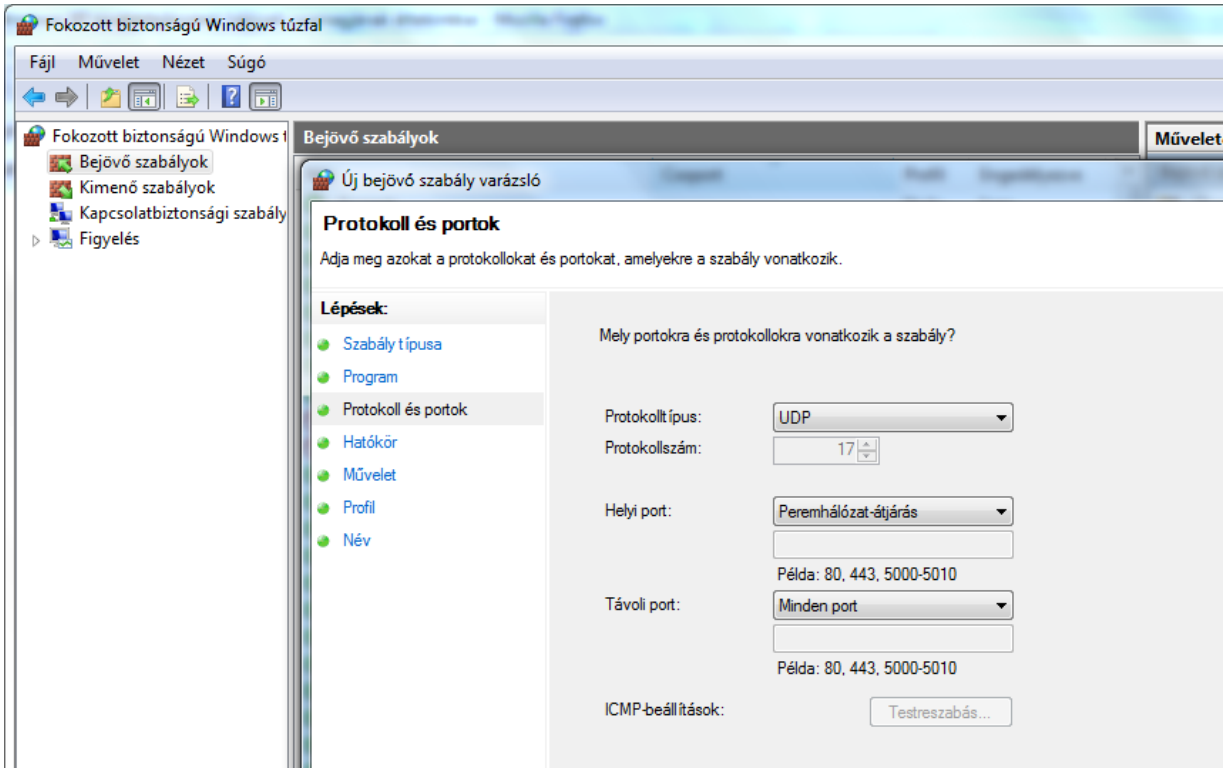
Diffie-Hellman használata az AuthIP-hez. Ha olyan kapcsolatbiztonsági szabályt hozunk létre, amely olyan tulajdonsággal rendelkezik, amelyet nem támogat az Internet Key Exchange version 1 (IKEv1), mint például felhasználó hitelesítés kérése, akkor IKE helyett AuthIP-t (Authenticated IP), azaz Hitelesített IP-t használunk. Alapértelmezésként az AuthIP a kért hitelesítési módszer által generált titkos kulcsot használja. Például, ha a Kerveros V5 hitelesítést választjuk, akkor a Kerberos titkos kulcsát fogja használni, a Diffie-Hellman csere által generált helyett. A Windows 7-el és Windows Server 2008 R2-vel kezdődően megadható, hogy az IPsec az összes alapmódú kommunikációban Diffie-Hellman-t használjon, még akkor is, ha AuthIP-t használ.

Az IPv6 átviteli protokollok állapottartó tűzfalak általi kezelésének támogatása. A Windows 7 és a Windows Server 2008 R2 támogatja az IP over HTTPS (IPHTTPS) nevű átviteli technológiát. Az IPHTTPS egy olyan bújtatás protokoll, amely egy IPv6 csomagot épít be egy HTTPS datagramba egy IPv4 csomagon belül. Az IPHTTPS lehetővé teszi néhány olyan IP proxi átjárását, amely nem támogatja az IPv6-ot, vagy a többi IPv6 átviteli



technológiát, mint például a Teredo vagy a 6to4. Egy Windows Tűzfal bejövő vagy kimenő szabályban beállíthatjuk a TCP portot IPHTTPS-re egy szám helyett, hogy a Windows Tűzfal automatikusan felismerje és megfelelően kezelje a kapcsolatot.

Továbbá a Windows 7 és a Windows Server 2008 R2 támogatja a *Teredo* IPv6 átviteli technológiát. A *Teredo* egy olyan bújtatás protokoll, amely IPv6 csomagokat ágyaz be egy UDP datagramba egy IPv4 hálózati csomagon belül. Egy Windows Tűzfal bejövő szabályként az UDP portot **Peremhálózat-átjárásra (Edge Traversal)** állíthatjuk egy specifikus port szám helyett, hogy a Windows Tűzfal automatikusan felismerje és megfelelően kezelje a kapcsolatot.



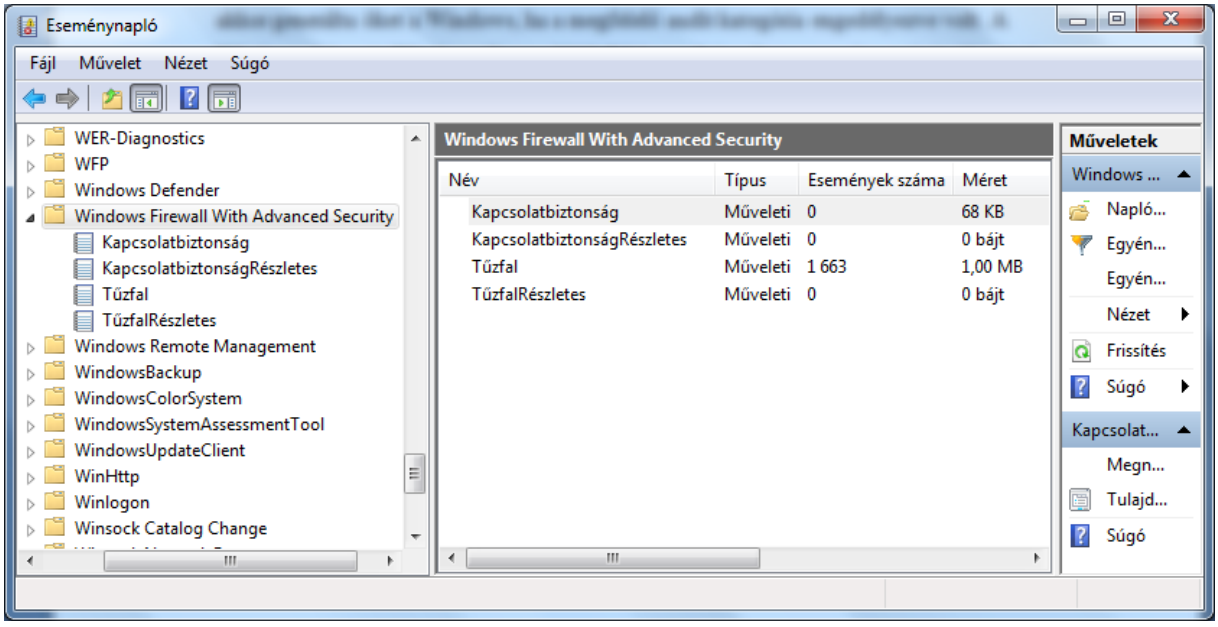
IPsec szabályok alól mentes DHCP. A Windows 7-ben és Windows Server 2008 R2-ben egy parancssori paranccsal mentesíthetjük az összes DHCP hálózati forgalmat IPsec követelmények alól (*netsh advfirewall set global ipsec defaultexemptions*, DHCP paraméterrel).

Blokkolási szabályok felülírása kimenő forgalomnál. Megadható, hogy egy kimenő Engedélyező (Allow) szabály felül tud írni egy blokkolási szabályt, ha IPsec kapcsolatbiztonsági szabály által van védve.

Mentesített IPsec által védett forgalom egy alagútból. Ha a már eleve IPsec-védett forgalmat egy IPsec csatornán keresztül küldjük, akkor az mégegy IPsec-be és IP fejrészbe lesz csomagolva. Ehelyett a Windows 7 lehetővé teszi, hogy egy tunnel-mód szabályban meghatározzuk, a hálózati forgalom, amely már IPsec által védett, mentesül az alagútból, és helyette a fölösleges enkapszuláció nélkül halad át a tunnel végponton.

Több alapmód konfigurációs készlet. Windows Vista és Windows Server 2008 operációs rendszerekben csak egyféle alapmód kezdeményezés készletet határozhatunk meg, amelyet az összes bejövő vagy kimenő IPsec kapcsolat használ. A Windows 7 és a Windows Server 2008 R2 egy új **netsh** parancs kontextust támogat, a „mainmode”-ot, amely olyan parancsokat tartalmaz, amelyekkel meghatározott forrás és cél IP címekhez vagy hálózati hely profilokhoz hozhatunk létre alapmód kezdeményezéseket.

Tűzfal és IPsec események elérhetőek az Eseménynaplóban. A Windows Vista-ban és a Windows Server 2008-ban a tűzfal események ’audit’ eseményeknek számítottak, és csak akkor generálta őket a Windows, ha a megfelelő audit kategória engedélyezve volt. A Windows 7-ben és Windows Server 2008 R2-ben néhány ilyen esemény már ’működési’ esemény, és megjelennek az Eseménynaplóban (Event Viewer) anélkül, hogy be kellene kapcsolnunk.



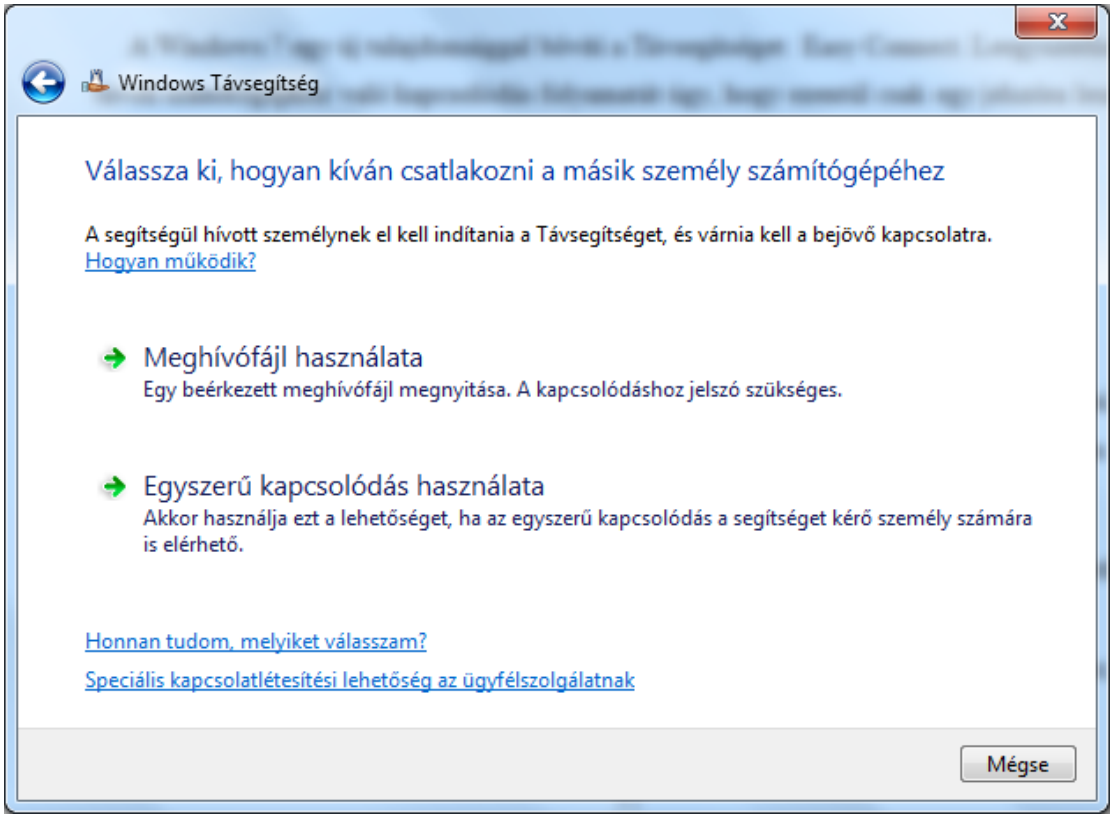
VII. Remote Assistance

Bizonyára minden informatikával foglalkozó emberek életében, így az enyémben is, többször előfordult már, hogy egy ismerős, kolléga, családtag számítógépén felmerült problémája miatt segítséget kért – telefonon. Habár a probléma egyszerűen megoldható lenne akár néhány kattintással, ha személyesen én ülhetnék le a számítógép elé. Így azonban csak azt látom, amit a segítségre szoruló lát, csak azt vagyok képes megtenni, amit ő képes megtenni az én irányításom alatt, és ez nem mindig vezet eredményre. Azonban van egy kézenfekvő megoldás, mely már évek óta jelen van a Microsoft operációs rendszereiben.

A **Távoli Hozzáférés** (Remote Access) egy olyan rendkívül hasznos része a Windows-nak, mely már igen régóta elérhető és viszonylag könnyedén használható. A Windows XP megjelenésével a Microsoft két új technológiát mutatott be, a Távoli Asztali elérést (Remote Desktop, RD) és a Távsegítséget (Remote Assistance). **A Remote Desktop** inkább a vállalati felhasználásra fókuszált, valamint integrációra egyéb Microsoft technológiákkal, mint például Terminal Services (Terminál szolgáltatások).

A **Távsegítség** az otthoni felhasználókra összpontosított, bár vállalati környezetben is hasznosnak bizonyulhat segítségnyújtásban a dolgozók számára. A Távsegítség a következőket teszi lehetővé:

- Megosztható az Asztal (Desktop) egy másik felhasználóval
- Megoszthatóak a számítógép perifériái: egér és billentyűzet (további beállításokkal egyéb eszközök is)
- Peer to Peer összeköttetés továbbító szerver nélkül, tehát a Távsegítség ugyanolyan jól működik két számítógép között egy LAN hálózaton, mint Interneten (WAN-on) keresztül.

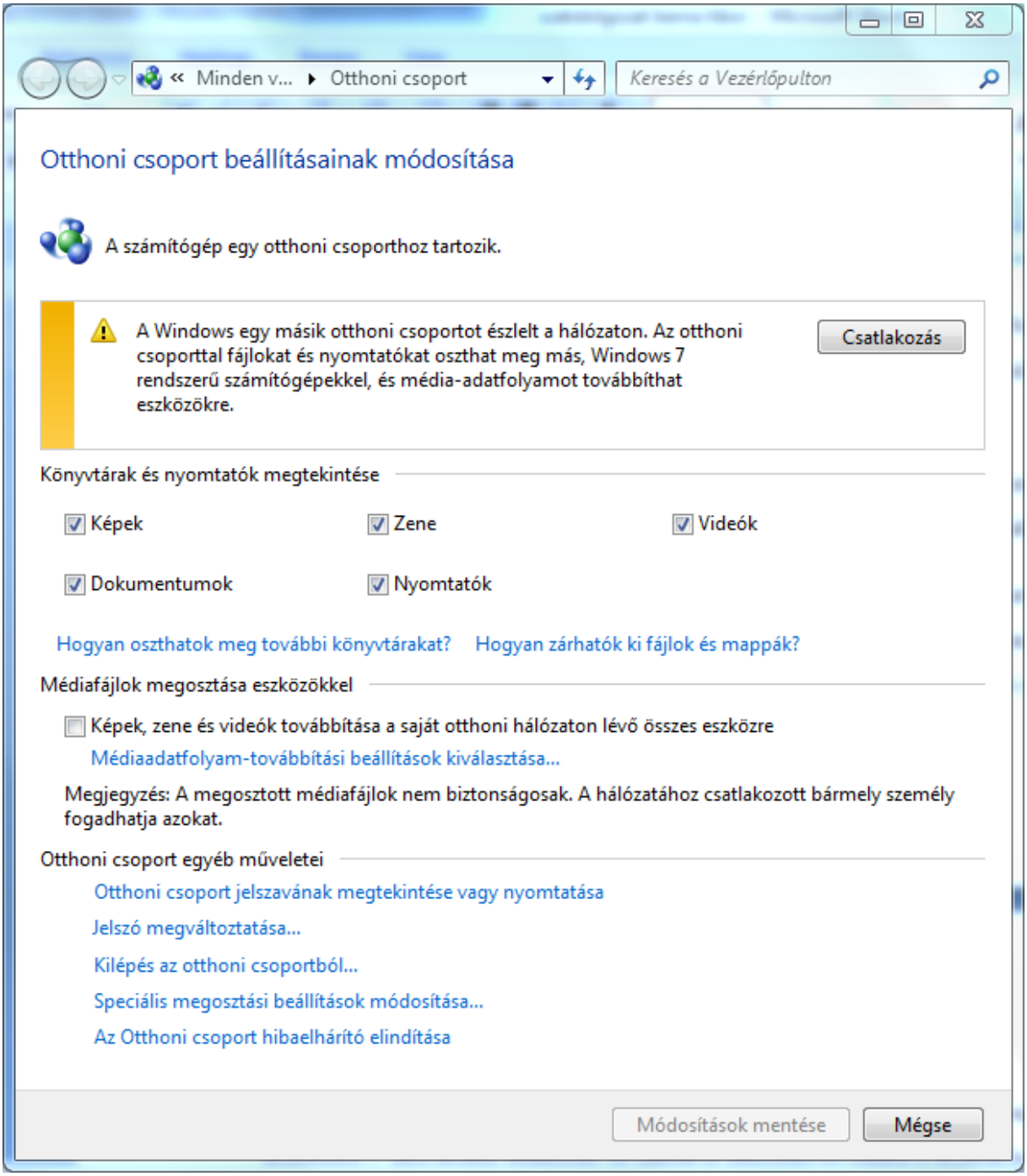


A Windows 7 egy új tulajdonsággal bővíti a Távsegítséget: Easy Connect. Leegyszerűsíti a távoli számítógéphez való kapcsolódás folyamatát úgy, hogy ezentúl csak egy jelszóra lesz szükségünk, fájlokra nem. Amikor létrejön egy kapcsolat mindkét számítógép között, kapcsolati fájlokat cserélnek, így létrejön egy bizalmi viszony. Ez tovább egyszerűsíti a jövőbeni kapcsolódásokat, amelyeket jelszó igénye nélkül fogunk véghezvinni.

VIII. Windows 7 HomeGroup

Bizonyára sokan tapasztalták már, akik otthoni hálózatukon fájlokat próbáltak megosztani, hogy a mappák engedélyeinek és a felhasználói fiókok beállítása és kezelése sokszor igen frusztráló lehet, főleg az átlag otthoni felhasználó számára.

Az Otthoni csoport (HomeGroup) segít leegyszerűsíteni a fájl- és nyomtatómegosztást otthoni hálózatunkban olyan számítógépek között, amelyek Windows 7 operációs rendszert használnak. Tartományba kapcsolt számítógépek is csatlakozhatnak otthin csoportunkhoz, így akár a munkahelyi laptopunkat is hazavihetjük, és elérhetjük megosztott fájljainkat. Otthoni csoportok létrehozása nagyon könnyű, belépéshez csupán egy jelszót kell megadnunk.



Otthoni csoport létrehozása

Otthoni csoport létrehozásához Windows 7 Home Premium, Professional vagy Ultimate verzióval kell rendelkeznünk. Ha egy Windows 7-et futtató számítógépünket egy új hálózatra csatlakoztatjuk, az operációs rendszer megkér minket, hogy azonosítsuk a helyet: otthon, munkahely, vagy nyilvános. Ha otthoni hálózatot választunk, és a számítógép nincs tartományhoz csatolva, és még nem létezik otthoni csoport a hálózaton, akkor a Windows 7

elindítja az Otthoni csoport létrehozása varázslót, így létrehozhatunk egy új otthoni csoportot. Miután megadtuk, hogy mely könyvtárakat szeretnénk megosztani, a varázsló egy jelszót ad meg nekünk, amellyel más számítógépek csatlakozhatnak az otthoni csoporthoz (ez a jelszó megváltoztatható).

Ha már létezik otthoni csoport egy hálózaton, és mi ehhez a hálózathoz csatlakozunk, akkor a Windows 7 felajánlja, hogy csatlakozzunk az otthoni csoporthoz. A Csatlakozás gomb megnyomása után, csak úgy mint otthoni csoport létrehozásakor, a varázslóban megadhatjuk, miket szeretnénk megosztani, majd a csoport jelszavának beírása után már csatlakozva is vagyunk.

IX. BranchCache

A BranchCache a Windows 7 és Windows Server 2008 R2 olyan új szolgáltatása, mely képes csökkenteni a WAN kihasználását, és növeli a hálózati alkalmazások elérhetőségét amikor felhasználók a központi irodában tárolt adatokhoz férnek hozzá a fiókirodákból. Ha engedélyezzük a BranchCache-t, akkor a webszerverekről vagy fájl szerverekről letöltött tartalom másolata a fiókirodában tárolódik. Ha egy másik kliens ebben az irodában ugyanezt a tartalmat igényli, akkor közvetlenül töltheti le a helyi hálózatról anélkül, hogy a WAN-t használná, így csökken a WAN forgalom.

Technikai áttekintés

A kirendelt irodákban a felhasználók gyakran tapasztalnak gyenge teljesítményt, amikor olyan alkalmazásokat használnak, melyek a WAN-on keresztül kapcsolódnak szerverekhez. Például jónéhány másodpercet vagy akár percet is igénybe vehet, míg egy fiókirodában tartózkodó felhasználó megnyit egy nagy fájlt, ami a központi irodában lévő szerveren van megosztva. Hasonlóan, ha egy felhasználó megpróbál egy videót lejátszani a web böngészőjében, sokszor hosszú ideig kell várakoznia, hogy a videó betöltsön.

A BranchCache-t úgy tervezték, hogy a fiókirodai felhasználóknak azt az élményt nyújtsa, mintha közvetlenül lennének csatlakoztatva a központi irodához. A BranchCache segítségével, az első felhasználó, aki tartalmat tölt le egy web szerverről vagy fájl szerverről (ezt nevezik tartalomszervernek), egy másolatot helyez el a tartalomról a helyi hálózatban. Az

utána következő kliensek ezt a chache-elt másolatot töltik le a fiókirodában, miután a tartalomszerver azt hitelesítette és engedélyezte.

A BranchCache-t úgy tervezték, hogy a már meglévő hálózati és biztonsági infrastruktúrával működjön. Támogatja az IPv4-et, IPv6-ot, végponttól-végpontig terjedő titkosítási módszereket, mint például az SSL és az IPsec. A BranchCache biztosítja, hogy a gyorsítótárazott tartalmak legfrissebb verzióját szolgáltassa, valamint, hogy a klienseket a tartalomszerver felhatalmazza, mielőtt azok hozzáférnének az adatokhoz.

A következő rendszerkövetelményeket igényli:

- A kliens számítógépeknek Windows 7-et kell futtatniuk, és a BrancCache funkció engedélyezve kell, hogy legyen.
- A web és fájl szervereknek Windows Server 2008 R2-t kell futtatniuk, engedélyezett BrancheCache funkcióval.

Módok

Attól függően, hogy a cache hol található, a BranceCache a következő két mód valamelyikében képes működni: Központi Gyorsítótáras mód (Hosted Cache mode), vagy Elosztott gyorsítótáras mód (Distributed Cache mode). A Hosted Cache mód úgy működik, hogy ki kell jelölni a fiókirodában egy számítógépet, amelyen Windows Server 2008 R2 fut, ez szolgál majd szerverként.

A kliens számítógépeket a host teljes domain nevével (Fully Qualified Domain Name – FQDM) konfiguráljuk, így bármikor hozzáférhetnek a tartalmakhoz a központi gyorsítótárban, amikor az elérhető. Ha a tartalom nem elérhető Központi gyorsítótáras módban, akkor a forráskiszolgálóról kéri le a kliens a WAN-on keresztül, majd azt felajánlja a központi gyorsítótárnak, így a későbbi kliensek azt használhatják.

Az ötven felhasználónál kevesebbel rendelkező fiókirodáknál a BranchCache beállítható Elosztott Gyorsítótáras módba is. Ebben a módban a helyi Windows 7 kliensek másolatot tartanak a letöltött tartalmakról, és a többi jogosult kliens rendelkezésére bocsátja, ha azok ugyanazt a tartalmat kérik. Így nem szükséges a fiókirodában szervert üzemeltetni. Azonban, ellentétben a Központi Gyorsítótáras móddal, ez a konfiguráció csak egyetlen alhálózaton keresztül működik (emiatt a tartalmat alhálózatonként kell letölteni a WAN-ról). Továbbá

azok a kliensek, amelyek leállnak vagy valami okból nem csatlakoznak a hálózathoz, nem képesek a kérelmező kliensek rendelkezésére bocsátani a kért tartalmakat.

Tartalom metaadat

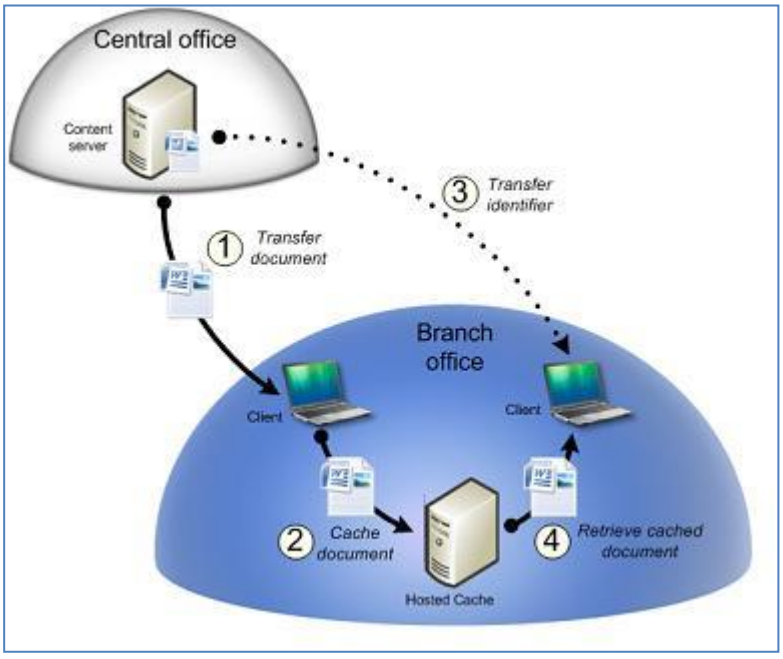
Úgy csökken a sávszélesség-használat, hogy a tartalomról metaadatot (ún. tartalom metaadatot) küldünk a klienseknek, amelyek letöltik a tartalmat a fiókirodán belülről. Ez csökkenti a sávszélességet, mert a tartalom metaadat lényegesen kisebb, mint a tényleges tartalom. Mielőtt a tartalom metaadatot elküldi, a szerver hitelesíti a klienst. Fontos, hogy a tartalomkiszolgáló mindet kliensnek küldjön tartalom metaadatot, hogy biztosítsa, hogy a kliens mindig kapjon hash-eket a legfrissebb tartalmakról.

A legkevesebb tartalom, amit a BranchCache gyorsítótáraz 64 KB méretű. Ha a tartalom ennél kisebb, akkor az adatot közvetlenül a tartalomszerverről töltjük le a WAN-on keresztül.

Központi Gyorsítótáras mód (Hosted Cache mode)

A Központi Gyorsítótár (Hosted Cache) BranchCache használatával működő szerverekről a fiókirodába BranchCache-t használó kliensek által letöltött adatok tárja.

A Központi Gyorsítótáras mód nem igényel dedikált szervert. A BranchCache funkció olyan szervereken működhet, amelyre Windows Server 2008 R2 van telepítve, és olyan fiókirodában van, ami más munkaterheléseket is futtat. Továbbá a BranchCache virtuális munkaterhelésként is beállítható, és más munkaterhelésekkel együtt futtatható egy szerveren (pl fájl, nyomtató).



Központi Gyorsítótáras mód (Hosted Cache mode)

Részletesebben a Központi gyorsítótáras mód a következő folyamatot használja az adatok gyorsítótárazására és letöltésére:

1. A Windows 7 kliens kapcsolódik a forráskiszolgálóhoz, és kér egy fájlt (vagy egy részét a fájlnak), pontosan úgy, mint ahogy BranchCache nélkül próbálna egy fájlt letölteni.

2. A forráskiszolgáló ezután hitelesíti a klienst és engedélyt ad neki a hozzáférésre. Ha ez sikeres, akkor tartalom metaadatot küld azon a csatornán, amelyen normális esetben az adatot küldte volna.

3. A kliens a metaadatban lévő hash-eket használva és azok alapján a Központi Gyorsítótár szerveren keresi a fájlt. Mivel ez az első alkalom, hogy egy kliens letölti ezt a fájlt, még nincs gyorsítótárazva a helyi hálózaton. Ezért a kliens letölti a fájlt közvetlenül a forráskiszolgálóról.

4. A kliens létrehoz egy SSL kapcsolatot a Központi Gyorsítótár szerverrel, és ezen a titkosított csatornán keresztül felajánlja a tartalom azonosítókat.

5. A Központi Gyorsítótár szerver kapcsolódik a klienshez, és letölti azon blokkokat, amelyek még nincsenek gyorsítótárazva.

6. Egy második Windows 7 kliens ugyanezt a fájlt kéri a tartalomszervertől. A forráskiszolgáló ismét hitelesíti a felhasználót, és tartalom azonosítókat küld neki.

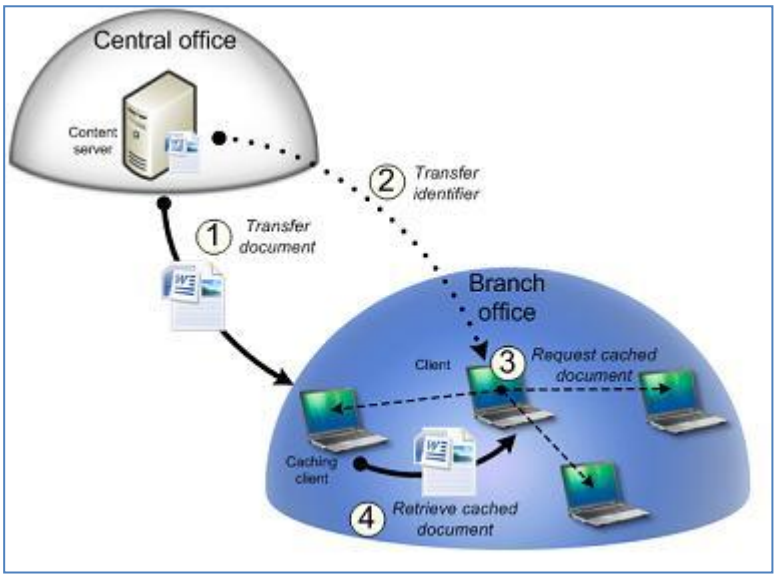
7. A kliens ezeket az azonosítókat használva kéri az adatot a Központi Gyorsítótár szervertől. A Központi Gyorsítótár szerver titkosítja az adatot, és visszajuttatja a klienshez. (Az adatot egy olyan kulcs használatával titkosítja, amelyet a tartalom metaadat részeként a forráskiszolgáló által küldött hash-ekből származtat)

8. A kliens feloldja az adat titkosítását, kiszámítja a hash-eket a Központi Gyorsítótárból kapott blokkokon, és ellenőrzi, hogy egyezik azokkal a blokk hash-ekkel, amelyeket a tartalom metaadat részeként a forráskiszolgáló küldött. Ez biztosítja, hogy a tartalmat nem módosították.

Elosztott Gyorsítótáras mód (Distributed Cache mode)

Elosztott Gyorsítótáras módban, a Windows 7 kliensek gyorsítótárazzák az adatokat, amelyeket a WAN-on keresztül töltöttek le, aztán elküldik ezt a tartalmat közvetlenül a többi jogosult Windows 7 kliensnek, ha azok kérik. Az Elosztott Gyorsítótáras mód olyan fiókirodákhoz illik, ahol ötvennél kevesebb felhasználó van.

Az első kliens, amely letölt egy bizonyos tartalmat egy forráskiszolgálóról WAN-on keresztül, ezen adat forrásává válik a fiókirodán belül más olyan kliensek számára, amelyek ugyanezt a tartalmat akarják letölteni. Ha egy második kliens ugyanezt a tartalmat kéri, letölti a tartalom metaadatot a forráskiszolgálóról. A második kliens ezután küld egy kérelmet a szegmens hash-ekért a helyi hálózatra, hogy megállapítsa, hogy bármely más kliens gyorsítótárazta-e már az adatot. Megtalálja az első klienst, és letölti tőle a tartalmat a helyi hálózaton.



Elosztott Gyorsítótáras mód (Distributed Cache mode)

Az elosztott gyorsítótáras mód folyamata hasonló a központi gyorsítótáras módéhoz, kivéve, hogy a gyorsítótárazott tartalmat a helyi hálózaton keresik a kliensek, és nincs szükség központi gyorsítótár szerverre.

Részletesebben:

1. Egy Windows 7 kliens kapcsolódik a tartalomszerverre, és kér egy fájlt (vagy egy fájl egy részét), ugyanúgy, ahogy BranchCache használata nélkül letöltene egy fájlt.

2. A forráskiszolgáló hitelesíti és jogosulttá teszi a klienst, és a szerver visszaküld egy azonosítót, amivel a kliens a helyi hálózaton keresi a fájlt. Mivel ez az első alkalom, hogy egy kliens megpróbálta letölteni ezt a fájlt, még nincs gyorsítótárazva a helyi

hálózaton. Ezért a kliens letölti a fájlt közvetlenül a forráskiszolgálótól, és gyorsítótárazza azt.

3. Egy második Windows 7 kliens ugyanezt a fájlt kéri a tartalomkiszolgálótól. Ez a kiszolgáló hitelesíti és jogosulttá teszi a felhasználót az adat letöltésére. Ha ez sikerül, akkor tartalom metaadatot küld azon a csatornán, amin keresztül normál esetben az adatot küldené.

4. A második kliens küld egy kérelmet a helyi hálózatra a kért fájlért, a Web Services Discovery (WS-Discovery) multicast protokollt használva.

5. A kliens, amely előzőleg gyorsítótárazta a fájlt, titkosítva elküldi azt a kérelmező kliensnek.

6. A kliens feloldja az adat titkosítását, számítja a hash-eket a blokkokon, amelyeket az első klienstől kapott, és ellenőrzi, hogy egyezik-e a blokk hash-ekkel, amelyeket a tartalom metaadat részeként a forráskiszolgálótól kapott. Ez biztosítja, hogy a tartalmat nem módosították.

Az Elosztott Gyorsítótáras mód lehetővé teszi, hogy a fiókirodában minimális hardverbővítéssel fordítsuk előnyünkre a BranchCache-t. Azonban ha a fiókirodában más infrastruktúra van kialakítva, akkor a Központi Gyorsítótáras mód a következő okokból előnyösebb lehet:

- **Nagyobb gyorsítótár elérhetőség.** A Központi Gyorsítótáras mód növeli a gyorsítótár hatékonyságát, mert a tartalom elérhető akkor is, ha a kliens, amely eredetileg igényelte az adatot, már nem elérhető.

- **Gyorsítótárazás az egész fiókirodának.** Az Elosztott Gyorsítótáras mód csupán egyetlen alhálózaton működik. Ha az elosztott gyorsítótárazást használó fiókiroda több alhálózattal rendelkezik, akkor minden alhálózat egy kliense le kell hogy töltsön egy külön példányt a kért fájlból. Központi Gyorsítótáras módban az összes kliens elérheti a központi cache-t, akkor is, ha különböző alhálózatokon vannak.

X. Összefoglalás

Szakdolgozatomban a Microsoft legújabb kliens operációs rendszerének, a Windows 7-nek a hálózati újításait igyekeztem bemutatni. A rengeteg újítást felsorolni is nehéz, ez mutatja, hogy a Microsoft egy-egy új operációs rendszerrel számtalan új dolgot vezet be, vagy régi dolgot tesz korszerűvé, vált fel újabb és jobb funkciókkal, alkalmazásokkal, eszközökkel. Ám mindezen újítások részletes taglalására több szakdolgozat is kevés lehet, ezért igyekeztem három, a mai viszonyokat tekintve fontos részt kiemelni: távoli elérés, biztonság, és vállalati hálózatok teljesítményének növelése.

Az első nagy fejezet azon a tényen alapszik, hogy a vezeték nélküli hálózatok elterjedése, fejlődése sok új lehetőséget tár a vállalatok mobil alkalmazottai elé. A vállalati hálózatok távoli elérése megkönnyíti munkájukat, felruházza őket azzal a képességgel, hogy a világon szinte bárhonnan dolgozhassanak, vagy elérjék a vállalati hálózat erőforrásait, ahol az internet rendelkezésükre áll. A Microsoft is rég felismerte az ebben rejlő lehetőségeket. DirectAccess szolgáltatása leegyszerűsíti a távoli elérés folyamatát, zökkenőmentessé teszi a szolgáltatást, mindezt a háttérben, komolyabb felhasználói beavatkozás nélkül. Használata lényegesen egyszerűbb és kényelmesebb, mint a VPN kapcsolatoké, ráadásul biztonságosabb is, köszönhetően az IPv6 és az IPsec által biztosított védelemnek. Továbbá a hálózati adminisztrátorok dolgát is megkönnyíti, a távoli gépek menedzselése azok internet kapcsolatától függetlenül történhet. A jogosulatlan felhasználók, károkozók, rosszindulatú programok elleni védelem minden operációs rendszer működésében nagyon fontos szempont. A másik nagy fejezetben arra próbáltam rávilágítani, hogy a Windows tűzfal rengeteg újítással bővült. A Fokozott biztonságú Windows tűzfal elődeinél sokkal hatékonyabb, több beállítási lehetőséggel rendelkezik, így könnyen testre szabható számítógépünk védelme. A több, különálló telephellyel rendelkező vállalatok számára a Windows 7 talán legelőnyösebb újítása a BranchCache. A fiókirodák közötti valamint a központi irodával való kommunikáció sok helyen problémát okoz. Ez főleg a sávszélesség elégtelenségében jelentkezik. Gyakorlatilag nincs az a sebesség, amely mindenkor elég lenne. Nagyobb sávszélesség eléréséhez pedig a cégek vezetőinek igen mélyen a zsebükbe kell nyúlniuk. Ennek híján az idővel megnövekedett forgalom miatt az átvitel a fiókirodák illetve a központ között lassú lesz, ez pedig megmérgezi a mindennapi munkát. Ezen enyhít a BranchCache, a forgalom figyelésével és a letöltött anyagok gyorsítótárazásával. Nincs szükség nagy beruházásra, hogy

a BranchCache-t üzembe helyezzük, Elosztott Gyorsítótáras mód alkalmazásával a fiókirodákban szervergépre sincs szükség, tehát olcsó és könnyen menedzselhető.

Mindezeket egybevetve a Windows 7 remek választás a nagyvállalatok kliens számítógépei számára, szolgáltatásai a mobil alkalmazottak és hálózati adminisztrátorok munkáját és mindennapjait is megkönnyíti. Remélem sikerült erről átfogó képet adnom az olvasónak.

XI. Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Dr. Krausz Tamásnak a munkám során nyújtott állandó támogatásért és segítőkészségéért, valamint a szakdolgozat megírásához szükséges források és egyéb információk biztosításáért.

Irodalomjegyzék, források

http://redqueen.uw.hu/modules.php?name=News&file=article&sid=89 (2010.03.12.)

http://www.packet.cc/files/arpanet-computernet.html (2010.03.12.)

Win7 Product Guide.xps (2010.03.12.)

http://www.windowsitpro.com/article/news2/blackcomb-scrapped-as-microsoft-heads-to-vienna49128.aspx (2010.03.17.)

http://www.microsoft.com/presspass/features/2009/Jun09/06-02SteveGuggenheimer.mspx (2010.03.17.)

http://www.microsoft.com/hun/technet/tc/?id=c11d35f3-8a2a-4801-bdd1-1086e903967a (2010.03.17.)

http://windows.microsoft.com/hu-HU/windows7/products/what-is (2010.03.12.)

http://blogs.msdn.com/e7/archive/2009/03/17/designing-aero-snap.aspx (2010.03.12.)

http://windows.microsoft.com/hu-HU/windows7/products/why-choose?os=other (2010.03.12.)

http://www.msw.hu/cikkek/67/windows_7_informaciok.html (2010.04.05.)

http://blogs.msdn.com/e7/archive/2009/03/06/beta-to-rc-changes-turning-windows-features-on-or-off.aspx (2010.04.05.)

http://www.microsoft.com/windows/virtual-pc/ (2010.04.05.)

Windows XP Mode for Windows 7_brochure.pdf (2010.04.05.)

http://channel9.msdn.com/pdc2008/ES21/ (2010.03.19.)

http://blogs.technet.com/wsnetdoc/archive/2009/04/13/spotlight-on-windows-firewall-multiple-active-firewall-profiles-in-windows.aspx (2010.03.19.)

H. Molnár József: Windows 7 a cégnél: BranchCache (http://www.microsoft.com/hun/technet/article/?id=9a9c4ab0-6f43-41c0-b700-728d910460e5) (2010.03.19.)

http://msdn.microsoft.com/en-us/library/bb968799%28VS.85%29.aspx (2010.02.13.)

http://blogs.msdn.com/openspecification/archive/2009/06/22/smb-2-1-multi-credit-large-mtu-operations.aspx (2010.02.13.)

http://technet.microsoft.com/en-us/magazine/2009.05.win7.aspx (2010.02.13.)

http://www.engadget.com/2009/05/18/microsofts-virtual-wifi-will-make-windows-7-wireless-adapters-d/ (2010.02.13.)

http://www.microsoft.com/windows/windows-7/features/homegroup.aspx (2010.03.19.)

http://windows.microsoft.com/en-us/windows7/help/home-sweet-homegroup-networking-the-easy-way (2010.04.12.)

http://windows7news.com/2009/11/27/windows-7-remote-tools-remote-assistance/ (2010.04.12.)

http://adacosta.spaces.live.com/blog/cns!E8E5CC039D51E3DB!24153.entry (2010.04.12.)

http://technet.microsoft.com/hu-hu/library/bb726944%28en-us%29.aspx (2010.04.15.)

http://itmanagement.earthweb.com/entdev/article.php/3783831/Windows+7+IT+Pro+Feature+Watch+List.htm (2010.04.15.)

http://www.microsoft.com/windowsserver2008/en/us/directaccess.aspx (2010.04.15.)

http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx (2010.04.15.)

http://technet.microsoft.com/en-us/library/dd637767%28WS.10%29.aspx (2010.04.15.)

http://technet.microsoft.com/en-us/network/bb545655.aspx (2010.04.15.)

(IDC Worldwide Quarterly PC Tracker, December 2008).

http://technet.microsoft.com/en-us/library/cc755158%28WS.10%29.aspx#bkmk_7 (2010.02.23.)

http://technet.microsoft.com/en-us/library/ee449421%28WS.10%29.aspx (2010.02.24.)

http://www.biztostu.hu/mod/resource/view.php?id=614 (2010.02.24.)

http://technet.microsoft.com/hu-hu/library/dd759172.aspx (2010.03.13.)

William R. Stanek – Windows 7 The Definitive Guide O'REILLY

Steve Johnson – Microsoft Windows 7 on Demand (2009)

Paul McFedries – Windows 7 Simplified

Ed Bott, Carl Siechert, Craig Stinson - Windows 7 Inside Out (2010)