

A kapun túl

Microsoft Forefront Threat Management Gateway 2010



Gál Tamás

Microsoft Magyarország – technetklub.hu

*A kapun túl, ha oda bemegyek,
tér nyílik, egyszerre közel-távol,
előre, vissza bármit nézhetek,
minden kitárul, minden kitárul.*

Fetykó Judit

© 2010, Gál Tamás

Első kiadás

Minden jog fenntartva.

A könyv írása során a szerző és a kiadó a legnagyobb gondossággal és körültekintéssel igyekeztek eljárni. Ennek ellenére előfordulhat, hogy némely információ vagy például hivatkozás (link) nem pontos vagy teljes, esetleg elavulttá vált.

A példákat és a módszereket mindenki csak saját felelősségére alkalmazza. Felhasználás előtt próbálja ki és döntse el saját maga, hogy megfelel-e a céljainak. A könyvben foglalt információk felhasználásából fakadó esetleges károkért sem a szerző, sem a kiadó nem vonható felelősségre.

A cégekkel, termékekkel, honlapokkal kapcsolatos listák, hibák és példák kizárólag oktatási jelleggel kerülnek bemutatásra, kedvező vagy kedvezőtlen következtetések nélkül.

Az oldalakon előforduló márká- valamint kereskedelmi védjegyek bejegyzőjük tulajdonában állnak.

Lektor: Harmath Zoltán (Architect, Microsoft Magyarország)

A könyv anyaga teljes terjedelemben és ingyenesen letölthető a Microsoft TechNetKlub portálról (<http://technetklub.hu/content/tmgkonyv.aspx>).

Microsoft Magyarország

2010

Köszönetnyilvánítás

Több embernek is tartozom köszönetnyilvánítással, illetve a „tartozom” talán nem is eléggé szép szó, ahhoz, hogy valójában mennyire szeretném megköszönni a segítségüket.

Budai Péter és Lippé Szabolcs azok a kollégáim a Microsoft-nál, akikkel a legtöbbet „gyűrjük” egymást. Petivel 2006 és 2010 között próbáltunk rengeteg hasznosat elkövetni a hazai rendszergazdák és üzemeltetők okításáért, egy váltás után pedig Szabolccsal 2010 nyár eleje óta „pörgünk” együtt ugyanezen a területen. Mindkettőjüknek lett volna elég oka rá, hogy piszkáljon a könyv elkészültével vagy az írás sebességével kapcsolatban, de ezt sosem tették, bíztak bennem. Mivel engem amúgy is egy eléggé független és öntudatos embernek ismernek, duplán hálás vagyok, hogy ez így alakult, így alakulhatott.

A lektornak, azaz *Harmath Zoltánnak* extra köszönet jár. Egy nagyon rövid határidő alatt, félig Budapesten, félig Redmondban, a jetlag-gel küzdve nézte át ezt a rengeteg oldalt, és több lényeges és praktikus javítás mellett, még belső érdekességekkel is szolgált az ISA és a TMG szerverek készítési folyamatáról, a dilemmákról és a döntésekről.

Persze, ennyi segítség még mindig kevés lenne, de nekem olyan „hátszágom” van, amellyel egész földrészeket igazhatnék le, ha úgy alakulna ☺. Ez a hátszág a családom, és főképp a *feleségem*. Ugye, semmi sincs ingyen, ellenben a „csillogás” sokszor csak nekem jut, míg az árát Ő fizeti meg. Ez egy megfelelő alkalom arra, hogy valamit méltó módon visszaadjak ebből. Köszönöm.

Egyébként egyetlen ember(ke) biztosan van, aki már most is utálja ezt a könyvet. Ő az én 9 éves *kisfiam*, akit 2010 augusztusában annyiszor lepattintottam a kosárlabdázás, a focizás, vagy bármi más közös tevékenység kapcsán erre a könyvre hivatkozva, hogy szerintem esténként a szobájában kicsi voodoo könyveket szurkált már, várva hogy végre-végre befejezzem....

TARTALOMJEGYZÉK

1	Bevezetés	9
2	Múlt és jelen	11
2.1	Így kezdődött...	11
2.2	Miért FOREFRONT és miért TMG?	17
2.3	Hány TMG van?	20
3	A telepítés és előzményei	23
3.1	A rendszerkövetelmények	23
3.2	A hálózati viszonyokról	25
3.2.1	A hálózati kártyák kötési sorrendje	26
3.2.2	A hálózati kártyák finomhangolása	27
3.2.3	DNS és NetBIOS	30
3.3	TMG forgatókönyvek	32
3.3.1	Edge firewall	33
3.3.2	3-Leg perimeter	34
3.3.3	Back-end firewall	35
3.3.4	Branch Office Firewall	35
3.3.5	Single network adapter	36
3.4	A kliensek	37
3.5	Telepítsünk végre	43
3.6	Ha nem sikerül, nyomozunk	53
3.7	Migráció, export-import	55
3.8	Virtuális környezetben?	58
3.9	Jó ha megszívleljük...	61
3.9.1	Néhány ökölszabály	62
3.9.2	Tartomány vagy munkacsoport?	63
4	Vegyük birtokba!	66
4.1	A konzol felfedezése	66
4.2	Az új varázslók	77
4.3	Hogyan lesz TMG admin a saját gépeden?	79

5	A tűzfal	81
5.1	Az alapok és némi történelem	81
5.1.1	A csomagszűrés	82
5.1.2	Az állapottartó-vizsgálat (és szűrés)	84
5.1.3	Az alkalmazás szűrés	85
5.1.4	A TMG helye a tűzfalak között	87
5.2	Multi (nem level) networking	88
5.2.1	Mit is jelent ez?	89
5.2.2	Az alapértelmezett hálózatok	89
5.2.3	A hálózatok tulajdonságai	93
5.2.4	A hálózati szabályok	98
5.3	Azok a csodálatos szabályok	103
5.3.1	A szabályok alapanyagai, azaz a hálózati objektumok	103
5.3.2	Hogyan épül fel egy hozzáférési tűzfalszabály?	108
5.3.3	És hogyan működik?	109
5.4	A System Policy	112
5.5	Behatolás detektálás, IP szűrés	120
6	A tűzfal a TMG-ben	124
6.1	Egy nagyágyú: a NIS	124
6.1.1	NIS részletek	128
6.1.2	A szignatúrákról még egy kicsit	132
6.2	ISP Redundancy	135
6.2.1	Típusok és működés	136
6.2.2	A kapcsolat tesztelése	138
6.2.3	Állítsuk be!	140
6.3	Enhanced NAT	146
7	A proxy szerver	149
7.1	Mit csinál egy proxy szerver?	149
7.2	Proxy típusok	150
7.3	Szerver oldali beállítások	154
7.4	Hitelesítési metódusok	158

7.5	Auto Discovery megoldások	162
7.6	Cache avagy tárazzunk gyorsan	169
7.6.1	Hogyan működik a web proxy cache?	170
7.6.2	A gyorsítótár finomhangolása	173
8	A web proxy a TMG-ben	185
8.1	Enterprise Malware Protection	185
8.1.1	Hogyan csinálja?	186
8.1.2	Az EMP konfigurálása	188
8.2	A HTTP filter	199
8.2.1	Hogyan érjük el?	200
8.2.2	A HTTP filter konfigurálása	202
8.3	HTTPS Inspection	208
8.3.1	A következmények és a követelmények	210
8.3.2	A HTTPSi konfigurálása	211
8.4	URL-F	219
8.4.1	Hogyan működik?	220
8.4.2	Amit az URL-F-ből látunk	222
9	Kit és hogyan engedünk be?	228
9.1	A szimpla szerver publikálás	229
9.1.1	Egy példa: FTP szerver közzététel	230
9.2	A webszerver publikálás	235
9.2.1	Egy nagy falat: a web listener	236
9.2.2	További webszerver publikálási opciók	247
9.2.3	Egy másik példa: Webszerver SSL-el	253
9.3	Speciális publikálás: az Exchange Server	260
9.3.1	Az SMTP szerver publikálás	261
9.3.2	SMTP védelem, vírus- és spamszűrés	264
9.3.3	A klasszikus e-mail protokollok publikálása	272
9.3.4	A webes kliensek	274
10	Távoli elérés: VPN és nem VPN	281
10.1	Hogyan faragjunk VPN szerver a TMG-ből?	281

10.2	Site-to-Site VPN	293
10.3	A nagy durranás: DirectAccess támogatás	302
10.3.1	DirectAccess alapok	302
10.3.2	DA vs. TMG	305
11	Ellenőrizzünk és javítsunk	308
11.1	Naplózás	308
11.2	Riasztások	315
11.3	A legjobb barátaink: Session Monitor és a realtime napló	320
11.4	Egy újabb barát: a Connectivity Verification	323
11.5	Jó barátokból sosem elég: a BPA	325
12	A ráadás: az SP1	328
12.1	BranchCache, RODC, Sharepoint 2010	328
12.2	URL szűrés változások	330
12.3	Újdonságok a jelentéseknél	332
13	Zárszó	335

1 BEVEZETÉS

"Körülbelül 6 éve szeretnék könyvet írni az ISA-ról. Számtalan oka van annak, hogy eddig miért nem sikerült, legfőképpen az, hogy egy könyv az egy egész embert kíván, ami egy bizonyos pörgésszám felett majdnem lehetetlen feladat. De most már nem halogathattam tovább (bár a 2010-es év első másfél hónapja mégiscsak ezzel telt ☺), hiszen újra lett aktuális értelme, a TMG megjelenése kapcsán."

Mindezt 2010 februárjának közepén írtam le. Hosszú habozás után ugyanis ekkor végre tényleg hajlandó voltam leülni, hogy elkezdjem. Aztán 10 nap folyamatos írás után, összehoztam kb. 120 oldalt. Nagyon büszke voltam magamra, de ez aztán elmúlt.

Merthogy ezután félévig semmi sem történt. Semmi. A nyár elején írtam egy pár oldalt, de aztán gyakorlatilag az egészet kikukáztam. Mondhatnánk, hogy anyagot gyűjtöttem, elegáns is lenne, de nem igaz. Az viszont igaz, hogy nem unatkoztam, de írni nem voltam hajlandó – az ember kiválóan képes meggyőzni magát arról, hogy amit nem akar, arra nincs is szükség. Aztán augusztus közepe felé nagyon elkezdett égni a lábam alatt a talaj, és kb. 20 kemény munkanap alatt összehoztam a maradék 215 oldalt. Durva, mert mondhatjuk, hogy 7 hónapig készült a könyv, pedig csak egyig, de az milyen volt. Durva.

Nos, ezen anyag *betű szerinti* elsajátítása sok-sok hasonló vastagságú okosság illetve jó pár év gyakorlat nélkül kissé nehezen fog menni. Azt viszont már a legelején megígértem magamnak, hogy minden lehetőség szerint és minden rendelkezésre álló eszközzel maximálisan arra fogok törekedni, hogy ne legyen lehetetlen¹ ebből a könyvből megérteni egy ilyen komplex, nagy tudású, és többféle környezetben is praktikusán használható szoftver működését és főképp működtetését, mint a *Forefront Threat Management Gateway 2010*. De azért alapozunk sokrétűen, mert ez a termék valóban igényli ezt.

De most, hogy kész bátran kijelenthetem, hogy ez nem egy 120%-osan Forefront TMG könyv, az az nem "csak" egy frissítés, hanem inkább átfogó jellegű. Több okból is:

- Rengeteg újdonság van benne (ahogyan a termékben is), de azért vannak olyan részek is, amelyek ISA 2006 vagy esetleg az ISA 2004 óta nem változtak, viszont kihagyhatatlanok.
- A stateful inspection az ISA és a TMG nélkül is stateful inspection.

¹ Az elmúlt 15 évben (azaz kb. mióta üzemeltetek) egy szép terjedelmes méretű

A KAPUN TÚL

Remélem, sokak számára okoz majd legalább annyi örömet e fércmű elolvasása, mint nekem - leszámítva a kezdeti kínlódást, meg néha a fonal elvesztését övező pánikhangulatot - a lekörmölése. És persze az okos ember legutoljára írja meg az előszót, és ilyenkor már, a befejezéstől elkábulva, minden megszépül, kék az ég, zöld a fű, és a szívemben kicsi virágok nyílnak... fúj.

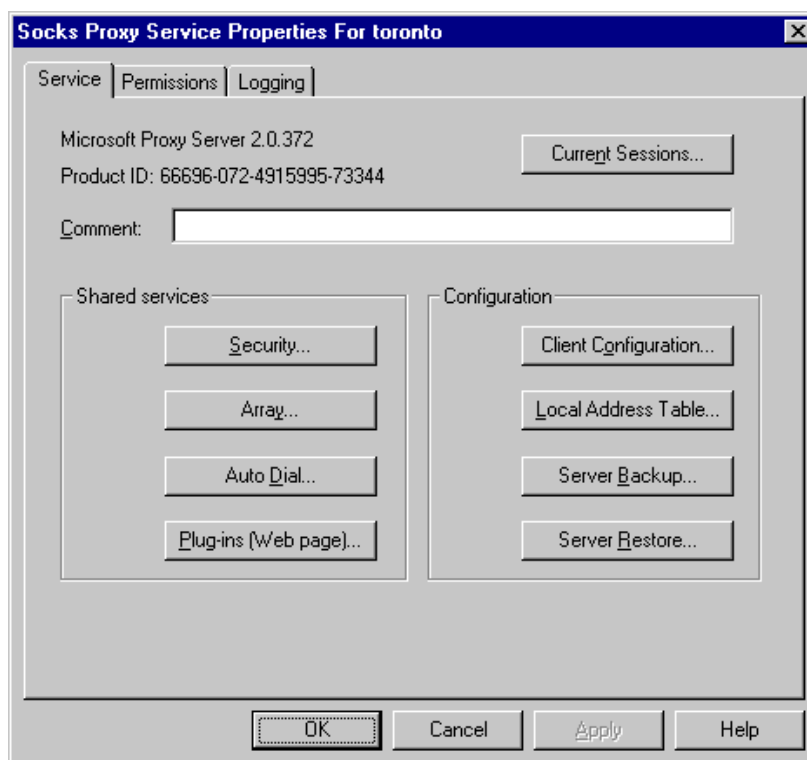
De hogy már az első oldalakon is legyen valami értelmes tartalom, azonnal eszközölök egy praktikus rövidítést a hivatalos, de kissé hosszú elnevezésen: mi TMG-nek fogjuk hívni innentől az új fiút, az elődjét pedig egyszerűen ISA-nak. Három betű mindkettő, de "mecsoda különbség"...

2 MÚLT ÉS JELEN

2.1 ÍGY KEZDŐDÖTT...

A Microsoft első próbálkozása a hálózatot védő komplexebb alkalmazások terén (direkt nem írok tűzfalat) a Proxy Server 1.0 volt, méghozzá 1997 januárjában. Abban az időben egy ilyen típusú termék igencsak ritkaság volt, gondoljunk bele (de ha kb. 30 év alatt van az életkorunk ez biztosan nem fog menni) a megjelenés pár hónappal a Windows NT 4.0 kiadása után történt – ami még éppen nem tartalmazta a TCP/IP-t, hanem csak külön eljárás keretében lehetett rátelepíteni. Szóval a Proxy Server 1.0 igencsak korlátozott képességű volt, és erősen behatárolt támogatással rendelkezett az internetes protokollok viszonylatában.

A szerző ezzel a változattal még nem, ellenben a gyorsan megérkező utóddal a Proxy Server 2.0-vál (1997. december) már dolgozott a mindennapokban is. És nem annyira élvezte, mivel még itt is volt jó csomó korlát és érthetetlen működés, főképp, ha szembeállítottuk az ekkor már bőven éledező/élő konkurenssekkel.



2.1 ÁBRA A PROXY SERVER 2.0

Ám egy nagy előnye a Microsoft termékének már akkor is volt: képes volt a szintén Microsoft termék, a hálózati operációs rendszer felhasználói adatbázisát használni (nincs még Active Directory, ez a ugye még mindig a Windows NT 4.0), ami vállalati környezetben lényegesen egyszerűbbé tette a felügyeletet. Sőt, ekkor már működött a

A KAPUN TÚL

csomagszűrő (packet filtering), sőt ebben a verzióban debütált a web cache, azaz a gyorsítótár szolgáltatás. De azért az összkép még mindig inkább fájdalmas volt, mint élvezhető.

Nagy változás történt 2001 márciusában, mivel megszületett az új nevű, és akkoriban nagyszerű és meghökkentő újdonságokat hozó ISA 2000. Először is rögtön két változat jelent meg, a Standard és az Enterprise. Az ISA Server 2000 eleinte csak Windows 2000 Server-en futott (de csak az SP1-től, viszont bármelyik kiadáson), ám később már a Windows Server 2003-ra is feltelepíthető lett.

Ezt a terméket már nevezhattük tűzfalnak, a sima csomagszűrésen kívül már a stateful szűrést is ismerte, és megjelentek az egyedi alkalmazás- és webszűrők is. Működött az RRAS-ra épülő (ez azóta is változatlanul így van) VPN támogatás, volt dinamikus IP szűrés, és egy pici IDS (Intrusion Detection System).

Az IDS képességek a következő ismert támadási formákat ismerték fel és adott esetben automatikusan tiltották is a problémás forrás IP-t: WinNuke, Ping of Death, Land, UDP bombs, POP Buffer Overflow, Scan Attack (portscan).

Az ISA szerverek első minősítési tanúsítvány:

ISA Server Earns ICSA Labs Certification, Industry's de Facto Standard for Firewall Security

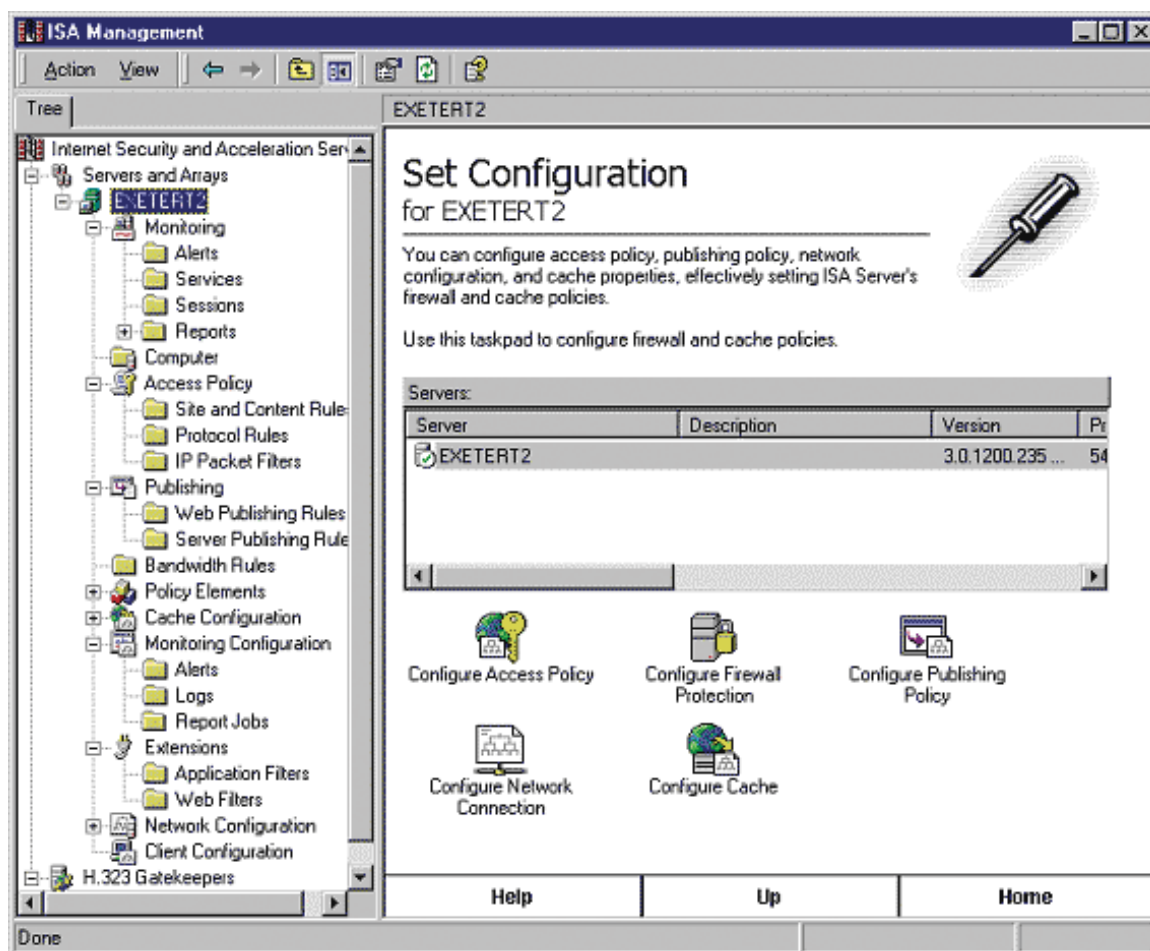
<http://www.microsoft.com/presspass/features/2001/feb01/02-14isaserver.mspix>

A cache már reverse irányban² is hajlandó volt dolgozni, valamint gyárthattunk időzített letöltésre vonatkozó kéréseket is.³ Megjelentek a már akkor is jól variálható és időzíthető jelentések, és volt Gatekeeper H.323 támogatás is, valamint a zéró konfigurálást megkívánó Secure NAT kliens alkalmazására is sort keríthettünk (immár a web proxy és a tűzfal kliens mellett). És volt sávszélesség szabályzás (!), de annyira, gyengére és használhatatlanra sikerült, hogy - bár igény az lenne rá - azóta se került be semelyik ISA vagy TMG verzióba.

² Azaz a reverse cache eredményeként egy publikált portál esetében előfordulhat az, hogy a böngésző kliensnek visszaadott tartalom nem közvetlenül a webszerverről, hanem az ISA gyorsítótárából jön.

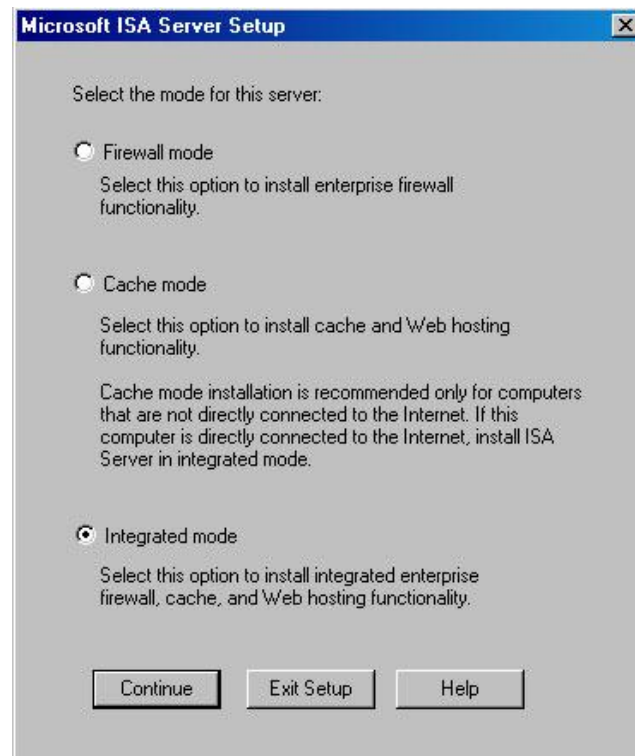
³ ...és volt automata letöltés is (Active Caching), azaz frekvenciált oldalakat önállóan lehúzta éjjel a cache-be, így pl. a szerző az első napokban a logok böngészése közben idegbeteggé vált, a userneveket nem tartalmazó, ám folyamatos letöltési bejegyzésektől ☺

A Gatekeeper H.323 elviekben lehetővé tette az ISA Server számára az IP telefonálás felügyeletét, illetve a H.323 alapú VoIP alkalmazások használatát (pl. Microsoft NetMeeting 3.0). De ehhez még DNS SRV rekordot is kellett regisztrálni, szóval nem volt egyszerű móka.



2.2 ÁBRA AZ ISA SERVER 2000

A számtalan újdonság egyike a mára már egységessé vált tűzfal szabályok elődjének a megjelenése volt, de kissé máshogy, mint napjainkban. Az Access Policy gyűjtőnév alatt külön szabályok vonatkoztak a Local Host gépre (IP Packet Filters), a weboldalak elérésére (Site and Content Rules) és külön az engedélyezett protokollokra (Protocol Rules), plusz külön elágazás volt a publikálásra (Published Rules). De ha pl. a hálózatkezelést néztük, akkor volt összesen egy, azaz 1 db Internal nevű hálónk (kizárólag a belső címtartományt tartalmazó LAT, azaz Local Address Table alapján), meg 1 db External és kész. A belső és a külső hálózat között minden forgalom NAT-olt volt, a belső hálózathoz tartozók között pedig minden forgalomterelés a tradicionális útválasztással (route) történt.



2.3 ÁBRA ÜZEMMÓDVÁLASZTÁS TELEPÍTÉS KÖZBEN AZ ISA SERVER 2000-BEN

A névből már kiderül, hogy az Enterprise kiadás a nagyobb rendelkezésre állás, a magasabb igényű elvárások miatt készült, és érkezett vele 1-2 olyan technológia is, ami miatt a mai napig is ezt választják a nagyvállalati ügyfelek (további részletek a 13. fejezetben):

- Az ISA tömb (array) alkalmazását, és így például a tömbben lévő ISA szerverek működésének központi, házirend alapú kényelmes szabályzását.
- Az NLB (Network Load Balancing) módszer alkalmazását, ami pl. a webszervereink folyamatos elérhetősége és magas rendelkezésre állása miatt vezettünk be
- Már akkor is jelen volt az Enterprise változatnál a CARP protokoll, amely az esetleges nagyobb mértékű, több szerverre elosztott web gyorsítótár kialakítását is lehetővé tette
- Nem került korlátozásra a használható CPU-k száma (ti. a Standard változatnál maximum 4 CPU volt a limit)

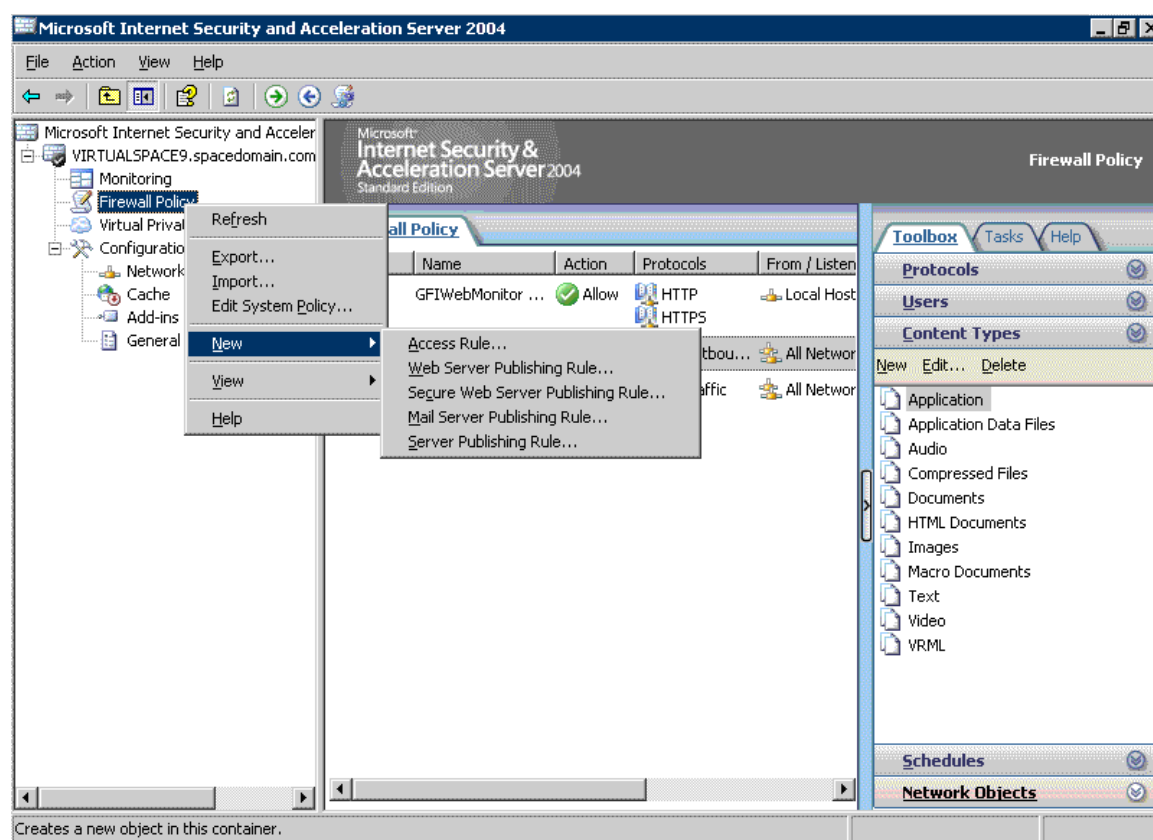
Az ISA Server 2000 Enterprise csak és kizárólag tartományvezérlőn működött és - azóta is példátlan módon - sémabővítést is igényelt!

Kiadástól függetlenül az ISA 2000 hozott még egy rémisztő változást: a telepítés után azonnal lezárt minden kifelé- és befelé tartó forgalmat, azaz nekünk kellett engedélyezni adott esetben gépenként, protokollonként, vagy felhasználói fiókonként

(és még jópár paraméter segítségével) a hozzáférést. Egyetlen szabály volt csak a rendszerben alapértelmezés szerint, az pedig mindent letiltott! Az elv helyes volt és ma is az, de akkoriban ez azt jelentette, hogy sokaknak újra kellett tanulni a tűzfal szakmát.

Még súlyosabb következmény volt, hogy RDP-n keresztül a telepítés bár ment, de a sikeres telepítés után egy „game over” következett. Az ajánlás akkor az volt, hogy húzd le a hálózatról az ISA-t és úgy telepítsd, konfiguráld be, majd tedd fel a hálózatra.

A későbbi ISA-k és a TMG viszont ebben is maradandót alkotott: a telepítéskor ha RDP-n vagy bent, észreveszi és forrás IP címedet automatikusan engedélyezi.



2.4 ÁBRA AZ ISA SERVER 2004

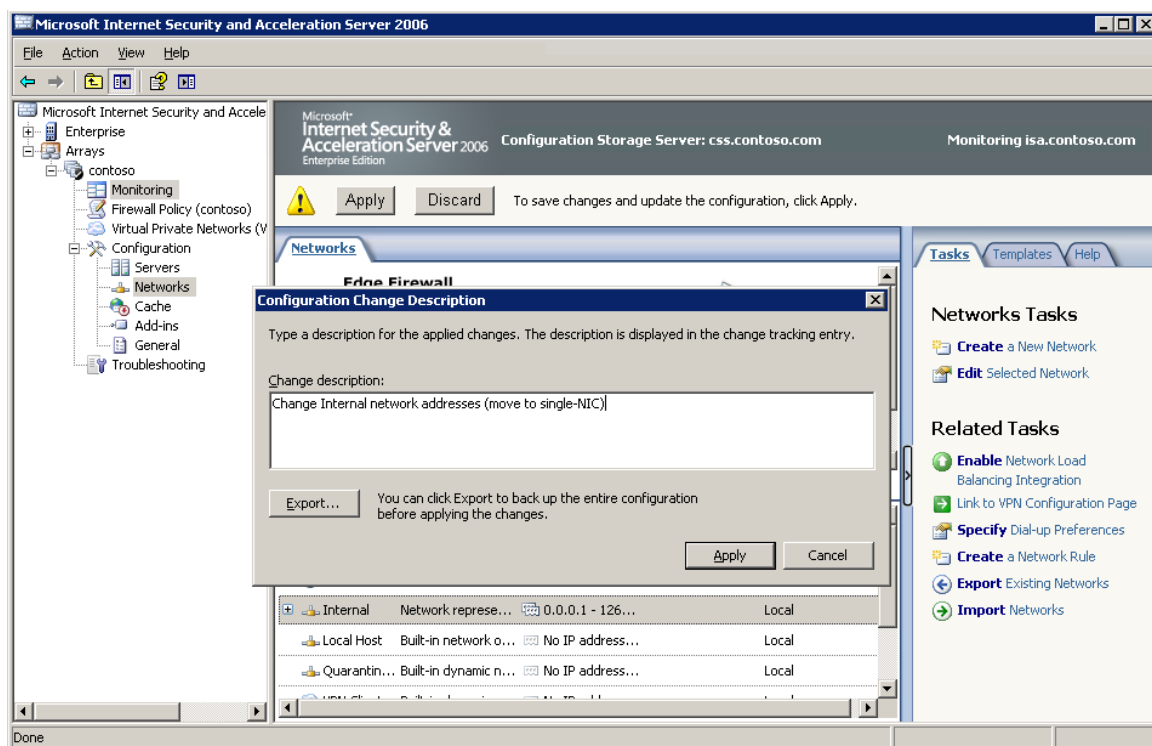
Aztán pontosan 3,5 év múlva újra újratanultuk.

Ugyanis 2004 szeptemberében megérkezett az ISA Server 2004. A felület teljes egészében megváltozott, tényleg eltévedtünk benne az elején. Belépett a multi-networking támogatás (az 5 alap hálózaton kívül akárhány logikai hálózatot kiépíthettünk), egységesedtek, ám összetettebbek lettek a tűzfalszabályok, megváltozott a VPN szerver szerepkör, immár lett VPN karantén támogatás is, változott a felhasználói csoportok kezelése, a hitelesítési metódusok, a felügyeleti módszerek, és megjelent az eleinte igencsak rejtélyesnek tűnő System Policy. Óriási változások történtek a szimpla és a webszerver publikálásban, a tanúsítványok

A KAPUN TÚL

használatában (azért itt még ráfért volna), a TCP és az UDP mellett az IP szintű és az ICMP protokollokat is támogatta az ISA 2004. Egyúttal újra változott a tartományi tagsággal kapcsolatos ajánlás: a RADIUS támogatással a közvetett hitelesítés lehetővé vált, így a tartományi tagság (különösen az Enterprise kiadásnál) már nem volt feltétel, sőt. Az RSA SecurID névtér használata egyszerűvé vált, és kaptunk egy remek, ám azóta is méltatlanul háttérbe szorult HTTP filter-t is, meg egy csudajó online naplót, és megjelent a széleskörű Exchange támogatás is, beépítve.

Azt hiszem, ez nem egy akármilyen lista, pedig most már próbálok szűkszavú lenni, mivel ezek a témák konkrétan és részletesen visszaköszönnék majd a következő fejezetekben. De - hogy más oldalról is említsünk meg példákat - eltűnt a termékből a már emlegetett sávszélesség-szabályzás, valamint pl. az Active Caching (ami valójában ott maradt a UI-n, de nem működött, csak az SP1 radírozta ki végleg ☺).



2.4 ÁBRA AZ ISA SERVER 2006

Na de, a történetnek (lásd: az ISA saga) nincs vége, alig ocsúdtunk fel, máris itt volt a nyakunkon a legújabb trónkövetelő, az ISA Server 2006 (2006 októberében). A kétéves intervallumból bizonyára az avatlan szemlélőnek is kiderül, hogy itt óriási, az alapokat is érintő változások már nem történtek, de sok okos és praktikus finomítás viszont igen. Ahol nagy változások történtek, az a hitelesítés, ezen belül is a hitelesítés-delegálás, a űrlap alapú hitelesítés (mobil eszközökre is kiterjesztve), valamint a különböző névterek (AD, Windows, RADIUS, SecurID, OTP) változatos használhatósága, az SSO (Single-

Sign On), és a Link Translation lehetőségek soha nem látott magasságokba emelkedtek. Az Exchange mellett integrált Sharepoint publikálást is kaptunk, kibővült az NLBS támogatás, valamint (végre) átláthatóbbá vált a tanúsítványkezelés.

Az ISA Server 2006 már nem volt telepíthető Windows 2000 Server-re, ellenben használhattuk a Windows 2003 R2-n is.

Én nem unatkoztam 2006-ban sem, azaz volt mit elsajátítani az ISA Server kapcsán, és a végén annyit még hozzátennék, hogy az azóta elérhető - nem elsősorban biztonsági⁴ - javítócsomagokban (Supportability Upgrade, valamint az SP1) is kaptunk számos kellemes meglepetést okozó segédeszközt.

2.2 MIÉRT FOREFRONT ÉS MIÉRT TMG?

A historikus áttekintés után nem árt megjegyezni rögtön az elején, azt a tényt, hogy a TMG-ben minden "benne van" ami az SP1-es állapotú ISA Server 2006-ban megtalálható volt. Ahogy láttuk a korábbi ISA változatoknál voltak változások, volt, ami kiesett, volt, ami visszajött, de itt most nem, a jelentős számú újdonság mellett minden eddigi ISA tudás benne lakozik a termékben.

Ezt az elvet követem ebben a fércműben is, sok-sok helyen, amikor a TMG egy-egy olyan szolgáltatásáról lesz szó, ami az ISA-ban is megvolt, ezt nem fogom külön kihangsúlyozni. Így viszont a dörzsölt szakiknak is át kell futni mindent – de talán ez nem lesz akkora fájdalom.

Más kérdés, hogy a felület változásai miatt, ha a jó régi megszokott helyen keresünk pl. bizonyos beállításokat vagy funkciókat, akkor időnként orra bukunk, de ez csak navigáció illetve megszokás kérdése, idővel menni fog. Erről még lesz bőven szó egyébként a 4. fejezetben.

Egy másik lényeges elem a név. A Microsoft termékeknél időnként eléggé szofisztikusan változnak a terméknevek, az "átnevező kommandó"⁵ lelkesen működik. Így aztán - ahogyan látható -, a TMG esetében is történt változás, méghozzá kettő is, de azért egy rövid kitekintés után ezek várhatóan mindenki számára logikusnak és érthetőnek tűnnek majd.

⁴ Az ISA nem arról ismert, hogy gyárilag tele lenne lyukakkal, de ez így is van rendben.

⁵ A jogok BK tulajdonába tartoznak ☺..

Érdekes belső sztori az, hogy 2003-ban amikor Redmondban dolgoztunk az ISA 2004-en, akkor a team egyértelműen a Microsoft Firewall Server nevet akarta adni a terméknek, viszont ezt a marketing a végén áthúzta.

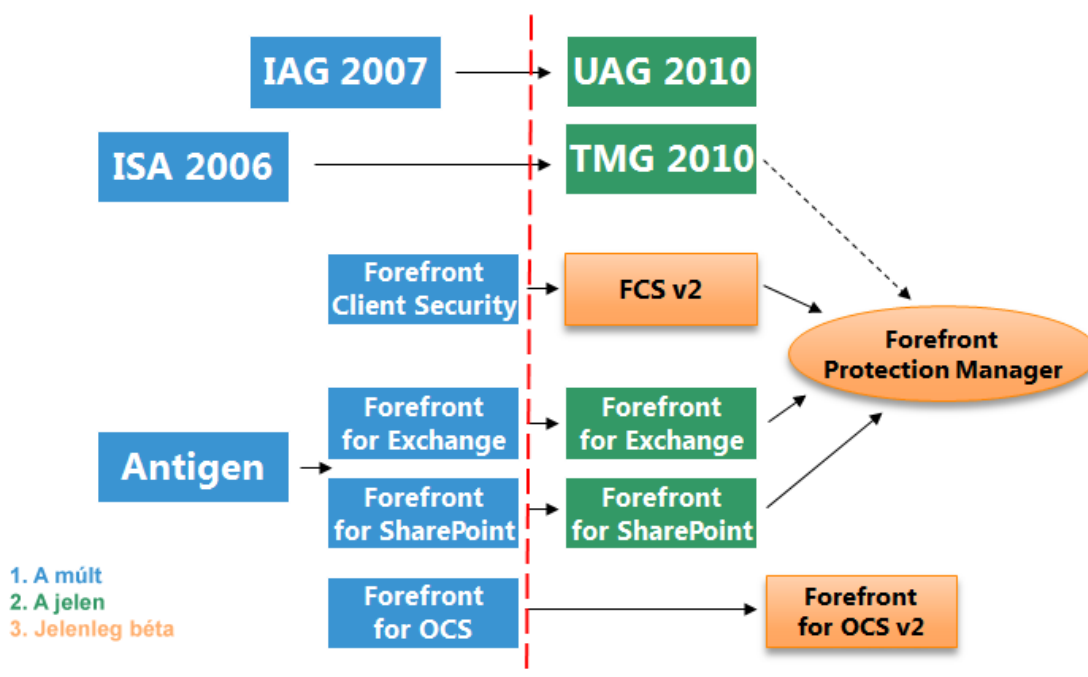
Ennek két üzenete lett volna: 1, szakítani az ISA névvel, mert rossz ómen volt a tűzfalak körében az ISA 2000; 2: fő üzenet az, hogy ez a termék NEM web caching termék elsősorban, hanem tűzfal, ami mellesleg tud gyorsítótárazni is (a mai napig alapértelmezés szerint a cache ki van kapcsolva). Az idő bennünket, azaz a team-et igazolja sajnos, mert sokszor még mindig elsősorban web caching proxy-nak tekintik a terméket, pedig nem az. *(A lektor megjegyzése.)*

A Forefront előtag a családot jelenti. Ez egy népes család, és egy népes, és rendes családhoz illően a tagjai szoros, időnként egészen intim kapcsolatban állnak egymással. A család tagjai értelemszerűen a biztonsági megoldásokhoz kötődnek, a legfrissebb Forefront Endpoint Protection nevű kliens oldali antimalware (a vírusok és spyware-k összefoglaló neve) terméktől a speciális kiszolgáló szoftverek (Exchange, Sharepoint, OCS) védelmén keresztül az olyan komplex tagokig, mint a TMG vagy az UAG.

És ne feledkezzünk meg a skála abszolút nagyvállalati oldalán álló olyan aktív elemről, sem mint a Forefront Protection Server (lánykori nevén Stirling, jelenleg még béta), már csak azért sem, mert ez lesz az a termék, amely pont a család összes, vagy majdnem összes elemét összefogja, és közös munkára bírja majd.⁶

Egyébként ez a család különleges gyökerekkel bír, mivel a tagok jelentős része kamasz vagy éppen felnőttkorában váltak teljes jogú családtaggá, azaz nem a Microsoft eredeti fejlesztése mindegyikük (lásd az Antigen illetve pl. az IAG kulcsszavakat), ám mostanra, azaz az olvasztótégelybe történő alapos és többszörös megmerülés után, ez már nem számít. Közös a cél és egységben az erő.

⁶ 2010 januárjában ez még igaz volt, de augusztusban már nem, ez a termék bizonytalan ideig kimarad a közeli fejlesztésekből, de azért benne hagytam a szövegben (úgy ahogy a TMG MMC-ben is láthatjuk jópár helyen)



2.5 ÁBRA A FOREFRONT CSALÁD TAGJAI
 EGY RÉSZTVEVŐ HIÁNYZIK, EZ PEDIG A FOREFRONT IDENTITY MANAGER 2010 (FIM)⁷
 (AZ FPM APROPÓJÁN LÁSD A LÁBJEGYZETET)

A fejezetindító kérdés második felét tekintve imho a "Threat Management Gateway" név is erősen indokolt, mivel az "Internet Security és Acceleration" nevű megoldás egy másik, lassan letűnő korszak képviselőjét mutatta. *Internet Security? Acceleration?* Ez az általánosítás illetve egyszerűsítés még az ISA 2000-re igaz lehetett, de hogyan lehetne ma már az Acceleration-nal a cache utalni a névben, mikor ez a termékben megjelenő képességek olyan kb. 2 %-át takarja. Ma már kissé mások a kihívások, a TMG-be kerülő új megoldások jelentős része valóban az direkt incidensek (*threat*) elkerülésére illetve megelőzésére szolgál (Antimalware, NIS, HTTP és HTTPS vizsgálat, spam és víruszűrés az Exchange számára és stb.). És a "Gateway" hívószó sem kevésbé jelentős, azt sugallja, hogy itt, az Edge (perem?) ponton kell megfogni mindent. Idáig jönnek a vírusok, idáig jönnek a támadások, idáig jönnek az autentikációs kísérletek – innen viszont a TMG lerendezi a problémát, teljhatalmú Úr Ő⁸ a hálózati forgalom tekintetében, és ha korrekt módon "uraljuk", akkor a hatalma valóban bennünket szolgál.

Kissé talán magasztos bekezdés volt ez, de a lényegét lefedi.

⁷ 2010 áprilisában aztán meg is jelent.

⁸ Randa dolog megszemélyesíteni a termékeket, én előszóban utálom is ezt, de most elnéztem magamnak.

2.3 HÁNY TMG VAN?

Összesen 2 db.

Eddig erről egy szó sem esett, pedig ez egy alapinformáció. És muszáj írni erről a témáról, mert sok a félreértés, jártamban-keltemben még azoktól is hallok fura vélekedéseket, akik elvileg "*benne vannak az iparban*". Szóval a könyv fő témájaként emlegetett TMG verzió mellett létezik egy ún. TMG MBE változat is, amelynek a publikus históriája a régebbi, azaz 2008 novemberének környékére datálódik (a nagy TMG RTM 2009 novemberében jelent meg), és eleinte elválaszthatatlanul kötődött az EBS-hez (Essential Business Server), azaz az SBS szerver nagytestvéréhez. Az EBS-ben megjelenő három fő szerepkör és szerver (Management, Security és Messaging) egyikeként a Microsoft a TMG akkori állapotában lévő változatát adta hozzá ehhez a csomaghoz, amelyet ugyanúgy a Threat Management Gateway névvel illetett, de emellett a Medium Business Edition tagot is szerepeltette a nevében. Ennek a cuccnak amellett, hogy az ISA Server 2006 RTM (ez fontos, lásd később) minden tudását lefedte, a két fő újdonsága volt.

Az egyik az, hogy fel lehetett telepíteni Windows 2008-ra, pontosabban a 64 bites Windows 2008-ra is (az EBS-ben minden szerver x64-es gyárilag), és ebből következik, hogy pl. Hyper-V alá is. A másik előny a majd a későbbiekben részletezett Malware Inspection részleges integrálása.

A Malware Inspection TMG és TMG MBE közötti különbségekről már írtam a TechNet blogon:

TMG Malware Inspection - szűrés ezerrel - I. rész

<http://www.microsoft.com/hun/technet/article/?id=30d3d111-4cb9-4f82-b9f7-d8167624ecfb>

TMG Malware Inspection - szűrés ezerrel - II. rész

<http://www.microsoft.com/hun/technet/article/?id=255b9f92-89d6-42dd-9bcc-189ffd68227b>

Ez a két újdonság csak töredéke a "nagy" TMG számos nagy durranásának, de azért és főleg akkor nagyon hasznos volt.

Na de folytassuk a sort a további MBE hiányosságokkal illetve eltérő tulajdonságokkal, immár felsorolás szerűen:

1. Hangsúlyoztam korábban az ISA 2006 RTM verzióját, nos, ez azért lényeges, mert az ISA 2006 SP1-gyel (2008.03.) pár praktikus újdonság "beleesett" a termékbe, és

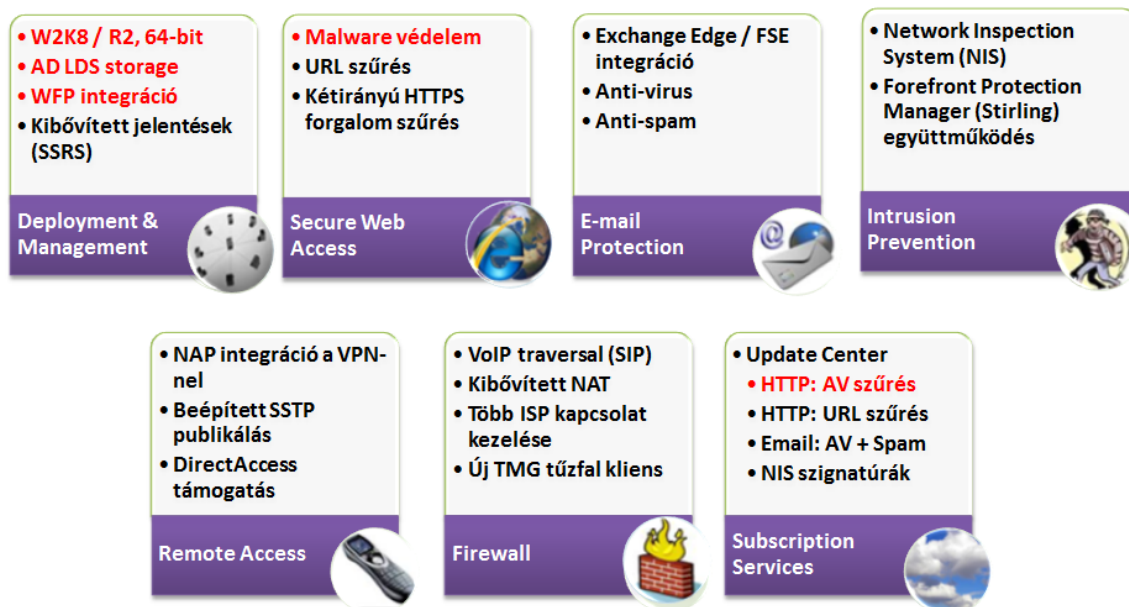
hát ezek az MBE változatból viszont kimaradtak (de ebből a könyvből nem fognak), nézzük meg melyek:

- Configuration Change Tracking (egyébként a TMG-ben ez már automatikus)
- Web Publishing Rule Test Button (ez különösen fájhat, tesztelésnél remekül mutatja a hibákat)
- Traffic Simulator (ez is fáj, teljesen praktikus)
- Diagnostic Logging Query (ez már nem annyira, hiszen gyakorlatilag csak egy link gyűjtemény, többek között pl. a BPA-ra utalva)

ISA Server 2006 SP1 újdonságok

<http://blogs.technet.com/isablog/archive/2008/05/23/isa-server-2006-service-pack-1-features.aspx>

2. Ha már itt tartunk az SP1 előtt, 2007 novemberében megjelent ISA 2006 Supportability Update "jóságait" (mint pl. a log színezés), az MBE is ismeri.
3. Igaz, hogy 64 bites OS alatt működik, de ha jól benézünk a Task Managerbe, akkor azt láthatjuk, hogy az MBE processzei mind-mind 32 bitesek.
4. Abszolút nem SA (Software Assurance) kompatibilis, sem lefelé, sem felfelé, tehát kissé nehézkes csomagban hozzájutni, úgyis mondhatnám, hogy lehetetlen.



2.6 ÁBRA TMG VS. TMG MBE (A PÍROSSAL KIEMELTEK AZ MBE-RE IS VONATKOZNAK)

5. Később az MBE életében annyi változás történt, hogy az EU-ban külön is kaphatóvá vált, azaz az EBS nélkül is megvásárolható. Jómagam vettem is egy cég számára egy rendszerépítés apropóján, mivel tudtam, hogy amikorra "beélesedik" a terv,

már szükség lesz egy Windows Server 2008 x64 alatt is működő tűzfalra, és akkor a nagy TMG még sehol sem volt. Nincs is vele baj, szépen működik azóta is. De sajnos a telepítésnél kiderült egy számomra is meglepő körülmény, azaz, hogy sajnos nem Windows Server 2008 R2 kompatibilis, és kis nyomozás után megtudtam - egyenesen Jim Harrisontól⁹ -, hogy nem is lesz az. Szóval ez egy érdekes helyzet, és persze ma már nincs értelme MBE-t venni külön¹⁰, és be kell látni, hogy ez egy köztes állapotot jelentett csak, ebben a nagyjából 1 éves intervallumban.¹¹

⁹ A szakma egyik kimagasló alakja, a Microsoft Forefront Edge Security Team tagja

¹⁰ 2010 szeptemberében már nem is lehet.

¹¹ Egyébként a kiadásának egyik oka az volt, hogy az antimalware képességet élesben is lássuk működni, mivel sok aggály volt a teljesítménnyel, de szerencsére ezek alaptalannak bizonyultak (A lektor megjegyzése).

3 A TELEPÍTÉS ÉS ELŐZMÉNYEI

Tipikusan ez az a rész, amelyet a rutinos (de nem elég rutinos) rendszergazdák át szoktak lépni. De én (és főleg a Microsoft) erősen ajánlom, hogy egy ilyen extra érzékeny helyzetű termék esetén ezt ne tegyék. A TMG szervergép(ek) teljesítményét, stabilitását és főképp megbízhatóságát mindenki fogja érezni a hálózat mindkét (vagy inkább összes) oldalán. Ebben a fejezetben többek között tehát nemcsak a szoftveres és hardveres követelményekről, hanem a hálózattal kapcsolatos elvárásokról, a TMG alkalmazásának forgatókönyveiről, a virtualizáció használatáról, és magáról a telepítésről is szó lesz. Anélkül hogy bagatellizálnám a telepítést, valószínűleg a rutinos szakik is tudják, hogy az "előzmény" szó a címben a 95%, míg a telepítés a sikeres beüzemelésnek csak töredék része, mondhatnánk a gyümölcse.

3.1 A RENDSZERKÖVETELMÉNYEK

A hardveres követelmények részletezésénél általában csak a minimum követelményeket kapjuk meg, ami érthető, hiszen például a feladat és/vagy a terhelés az, ami meghatározza a hardver elemek elvárt teljesítményét. Értelemszerűen a 15 k-s, SAS RAID lemezekről, vagy a 4x4 magos CPU-król itt nem lesz és nem is lehet szó, maximum majd a "megszívlelős" fejezetben. A minimumszint tehát a következő:

- 64-bit-es CPU, akár Intel (Extended Memory 64) vagy akár AMD64 ízlés szerint, a hitvitába semmiképpen nem mennék bele, viszont csak és kizárólag 64 bit, a TMG-nek nincs 32 bites változata, még próbaváltozat sem¹²
- Windows Server 2008 x64, Windows Server 2008 R2 x64 (Standard, Enterprise, és Datacenter kiadás, a Web, a Server Core és a Foundation nem)
- 2 GB RAM
- 2.5 GB HDD hely (ez csak a rendszer, ebben sem a cache, sem pl. a malware védelem karanténja nincs benne)
- Minimum egy hálózati kártya (hogyan is milyen azon is sok múlik, lásd később)
- További hálózati kártyák a tervezett szkenárió függvényében (3.3 fejezet)
- NTFS fájlrendszer

E mű elkészítése közben jelent meg az ISA-nál már megismert ún. *Capacity Planning Tool* TMG-re passzoló változata. A tervezett sávszélesség, a felhasználók száma illetve a TMG kiválasztott szolgáltatásainak ismeretében viszonylag egyszerűen kiszámolhatjuk azt, hogy milyen és mennyi hardverre, pl. milyen CPU-ra, mennyi RAM-ra, stb. lesz szükségünk a Microsoft ajánlása alapján. Ráadásul a korábbi változathoz képest egy

¹² A Management MMC konzol egy másik kérdés, de erre még visszatérünk

örvendetes változás az, hogy a könnyen feledhető flash-es változat után visszatértünk a jó kis Excel táblákra :)

Forefront Threat Management Gateway 2010 Capacity Planning Tool

<http://go.microsoft.com/fwlink/?LinkId=182886>

Microsoft®
Forefront™
Threat Management Gateway

Capacity Planning Tool v1.0

Deployment Details

Steps

1. **Scenarios** - Select the main deployment scenario for the site you are planning.
2. **Usage** - Select the user Internet activity profile for the expected traffic during peak usage hours.
3. **Features (optional)** - Select specific product features for the site.

1 Scenarios

Select the main deployment scenario for the site

- **Secure Web Gateway:** Outbound access with maximal protection capabilities.
- **Forward Web Proxy and Firewall:** Outbound access with minimal protection.
- **Mail Protection:** Mail server traffic with spam filtering and malware protection.
- **Web Publishing:** Remote access to internal network resources.
- **Free Selection:** Select a mix of features from the **Features** list.

*Note - you can override any or all of the individual features set with any scenario.

☒ Secure Web Gateway
☐ Forward Web Proxy and Firewall
☐ Mail Protection
☐ Web Publishing
☐ Free Selection

2 Usage

Select User Internet Activity Profile

- **High:** Heavy usage (80 Kbps per user)
- **Medium:** Normal usage (60 Kbps per user)
- **Low:** Low usage (40 Kbps per user)

Usage Profile

3 Features (optional)

Select product features for the site
Each of the applications and protection mechanisms listed below. Select only those features you anticipate will be enabled.

- ☒ Forward Web Proxy
- ☒ HTTP Malware Inspection
- ☒ HTTPS Inspection
- ☐ Mail Protection
- ☒ Network Inspection System
- ☒ URL Filtering
- ☐ VoIP
- ☐ VPN Remote Access →
- ☐ VPN Site-to-Site →
- ☒ Web Caching
- ☐ Web Publishing →
- ☐ Load Balancing
- ☐ Virtualization

Back to Welcome **Go to Step 2: Choose Calculation Method**

3.1 ÁBRA RÉSZLET TMG CAPACITY PLANNING TOOL-BÓL, HASZNÁLJUK BÁTAN

A szoftveres követelmények viszont lényegesen árnyaltabbak, pl. a Windows Server 2008 szolgáltatásai és képességei közül az alábbiakra lesz szükség:

- Active Directory Lightweight Directory Services (a korábbi ADAM, azaz a TMG a Standard változatnál is szakított a registry-ben tárolt konfiguráció elvével)
- Network Policy and Access Services Server
- Web Server (IIS)
- Network Load Balancing Tools
- Windows PowerShell

Rutinos szemmel az IIS-en meglepődhetünk, hiszen eddig arról volt szó, hogy a tűzfalra webszervert semmiképp se tegyünk, mert különben csúnya halált

halunk, meg a családjuk és még a szomszédok is, de az idők változnak. És azért ez nem egy közönséges a 80-as porton figyelő webszerver, hanem egy a 8008-asra bedrótozott példány, amin nem is tudunk változtatni.

Egyéb szükséges, de nem integrált összetevők:

- Microsoft SQL Express 2008 vagy
- Microsoft SQL Server Native Client
- Microsoft SQL Server Volume Shadow Copy Service (VSS) Writer
- Office Web Components (része az SQL Server Express telepítésnek)
- Microsoft .NET Framework 3.5 SP1.
- Windows Web Services API.
- Microsoft Windows Installer 4.5.

Amit még tudni kell, hogy a TMG eltávolítása során a Windows Server 2008 szerepkörökön és képességeken valamint az Office Web Components alkalmazáson kívül minden más automatikusan lekerül a rendszerről, ám ezeket viszont kézzel kell eltávolítanunk, ha nincs rá szükség a továbbiakban.

És ami a legjobb: a számos feltétel ellenére gyakorlatilag semmilyen manuális teendőnk nem lesz a szoftveres komponensekkel, mivel a telepítő része egy speciális eszköz, az ún. Preperation Tool (a telepítésnél majd megemlékezünk erről bővebben), ami nagyon praktikus. De itt is van kivétel, ugyanis ha az Exchange-ünket kisegítő e-mail védelem TMG-re illesztését is óhajtjuk, akkor az ahhoz szükséges komponenseket viszont már manuálisan kell telepíteni.

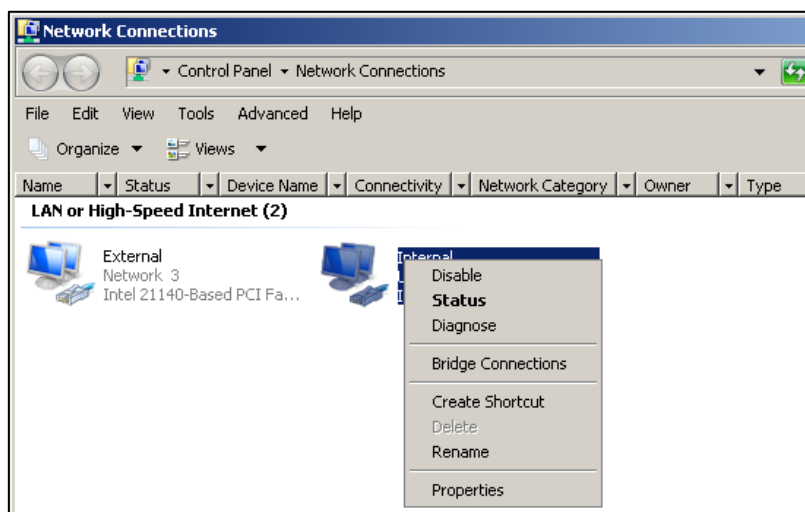
3.2 A HÁLÓZATI VISZONYOKRÓL

Az ISA/TMG szerverek telepítése előtti egyik kulcsfontosságú kérdés (sokan el is hasálnak ezen, ez kiderül a fórum/levlista kérdésekből), a hálózati kártyák beállítása. A kötési sorrend, a külső hálókártya szigorú beállítása, a DNS és NetBIOS beállítások, mind-mind olyan terület, ami adott esetben lehetetlenné, vagy rosszabb esetben¹³ kiszámíthatatlanná, illetve teljesítmény pazarlóvá teheti a működést. Nézzük sorban a helyes elveket és teendőket.

Ha több hálókártyánk, azaz több hálózatunk van (lehetne egy is, lásd 3.3.5), akkor van néhány praktikum illetve arany szabály, amit célszerű betartanunk:

¹³ Szerintem ha valami nem működik, akkor általában könnyebb kinyomozni az okot, mintha csak részlegesen, vagy nem kellő teljesítménnyel, vagy ideiglenesen teszi ugyanezt.

- Nevezzük el a hálókártyákat egy egyértelmű, az adott hálózatra utaló névvel (Internal, External, egy ADSL kapcsolathoz pl. az ISP neve, stb.)



3.2 ÁBRA AZ ÁTNEVEZÉS EGYSZERŰ, ÉS PRAKTIKUS

- Számoljunk azzal, hogy egy és kizárólag egy alapértelmezett átjárónk lehet¹⁴. Ez egy tipikus két hálókártyás rendszerben mindig a külső interfészen állítjuk be (vagy automatikusan beállítja az ISP DHCP-je). A belső hálózat TCP/IP beállításai között biztosan nem szerepelhet egy DG.
- Csak egy interfész TCP/IP tulajdonságai között állítsunk be DNS szervereket. Ez tipikusan a kötési sorrend tetején helyet foglaló kártya lesz, és tipikusan (főképp ha tartományban van a TMG) az AD eléréséhez szükséges DNS szerver(ek) címei lesznek.
- A nem szükséges protokollokat és adapter kötések minden hálókártyáról tüntessük el (interface hardening). Ez különösen a külsőnél lesz fontos, de erről még beszélünk.
- A hálózati interfészek kötési sorrendjének (Network Binding Order) kialakítása kritikus teendő.

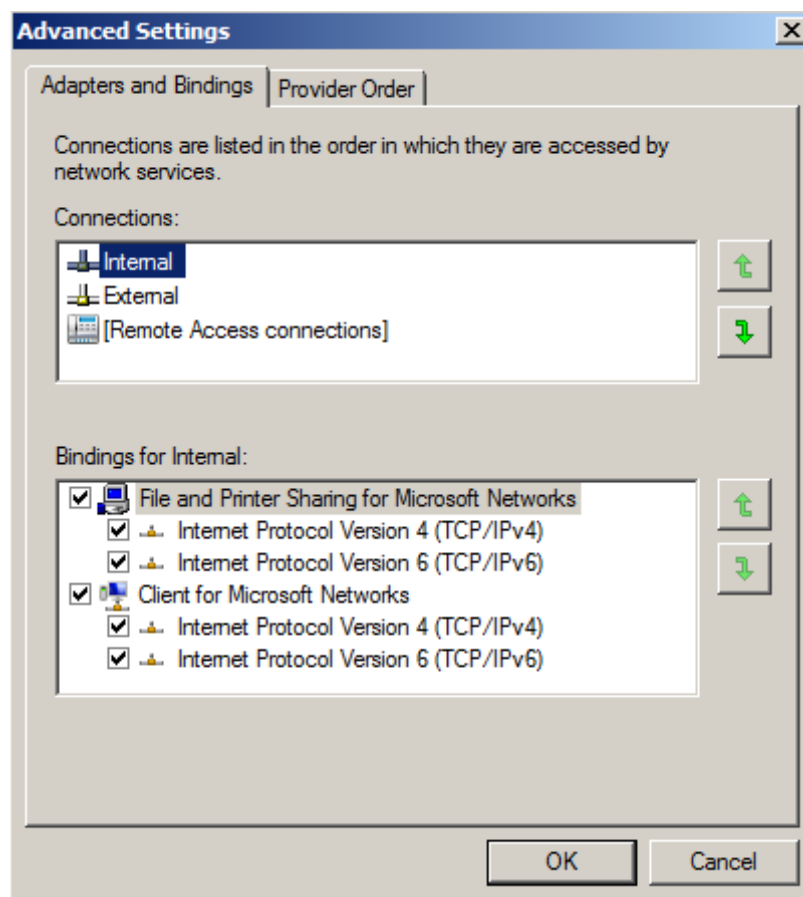
3.2.1 A HÁLÓZATI KÁRTYÁK KÖTÉSI SORRENDJE

Ha több kártyánk van, mindig van kötési sorrend, ergo ezzel foglalkoznunk is kell, mert könnyen lehetséges, hogy az alapértelmezett beállítás nem megfelelő.

Ha az előző ábrára nézünk, akkor a kötési sorrendet az Advanced/Advanced Settings/Adapter and Bindings fül alatt találjuk meg. A TMG teljesítményét erőteljesen befolyásolja ez a sorrend, hiszen itt derül ki, hogy milyen névfeloldási mechanizmust használ az operációs rendszer elsősorban, majd másodsorban és így tovább.

¹⁴ Vagy majd nem, lásd 6.3.

Az ajánlás az, hogy ahol a *legnagyobb* hálózati forgalmat várjuk az legyen az első helyen. Két hálózati kártyás környezetben azonos forgalmat, vagy közel azonos forgalmat várunk mindkét kártyán, ezért a belső hálózat interfésze legyen a legelső helyen. Viszont több hálózat esetén ez már nem mindig egyértelmű, ergo legyen a forgalmi mértéke az irányadó.



3.3 ÁBRA EZ EGY HELYES SORREND

3.2.2 A HÁLÓZATI KÁRTYÁK FINOMHANGOLÁSA

Ha az adott kártya a megfelelő helyen van a kötési sorrendben, illetve ha a nem megfelelő adapter kötések eltávolítottuk a hálókártyáinkról, akkor még mindig van teendők: a TCP/IP konfiguráció. Ez adapterenként erősen különbözhet, és elsősorban attól függ, hogy mire használjuk az adott adaptert.

A belső, azaz a LAN felé mutató hálókártya ajánlott beállításai:

- File and Print Sharing for Microsoft Networks: ez vitatéma lehet, ha nagyon szigorúak vagyunk akkor letiltjuk, ám ha szükség van többek között pl. a fájlmegosztások elérésére a TMG szerveren, akkor muszáj engedni.
- Client for Microsoft Networks: engedélyezve (lásd előző pont).

TCP/IP:

- Default Gateway: nincs
- DNS kiszolgálók: van, az AD-hoz használt, tipikusan a tartományvezérlők
- Register this connection's address in DNS: engedélyezve
- NetBIOS over TCP/IP: engedélyezve

A DNS illetve a WINS fülön szereplő egyéb beállítások egyediek lesznek, így azokat igény szerint használjuk.

Egy külső, azaz az Internet felé mutató hálókártya ajánlott beállításai:

- File and Print Sharing for Microsoft Networks: szigorúan csak letiltva
- Client for Microsoft Networks: szigorúan csak letiltva

TCP/IP:

- Default Gateway: nincs
- DNS kiszolgálók: nincs
- Register this connection's address in DNS: letiltva
- NetBIOS over TCP/IP: szigorúan csak letiltva

A külső interfésznél még vannak további teendőink is. Először is tipikusan tényleg minden kötést leszedünk a TCP/IP protokollok IPv4-es és IPv6-os (ez megint csak vitatéma lehet, lásd mindjárt) képviselőin kívül erről a kártyáról. Ha már van telepített TMG-nk, akkor a *Forefront TMG Packet Filter*-t nem tudjuk egyik interfészről sem, de ez rendben is van így.

Adott esetben az IPv6-ot is leszedhetjük, de tudnunk kell hogy ezzel még nem tiltjuk le teljesen, ehhez registry turkára is szükség lesz. Ám most eljött az ideje, hogy leleplezzem a fájdalmas titkot: a TMG nem rendelkezik IPv6 támogatással. Limitált forgatókönyvekben igen (pl. DirectAccess), de alapértelmezés szerint nem. Az IPv6 forgalom szűrése tehát nem megy a TMG számára, annyira nem, hogy alapértelmezésben blokkolja is ezt.

Ezután az eddig felsorolásban nem szereplő következő tételeket is kapcsoljuk ki, biztos, ami biztos:

- Append parent suffixes of the primary DNS suffix
- DNS suffix for this connection
- Enable LMHOSTS lookup (és nyilván WINS szerver sincs)

Később lesz még szó részletesen a Perimeter hálózatról, de most anélkül hogy részletekbe belemennénk, a teljesség kedvéért lejegyzem az ide passzoló, ajánlott beállításokat is:

- File and Print Sharing for Microsoft Networks: letiltva
- Client for Microsoft Networks: letiltva

TCP/IP:

- Default Gateway: nincs
- DNS kiszolgálók: nincs
- Register this connection's address in DNS: letiltva
- NetBIOS over TCP/IP: letiltva

A hálózati kártyák ügyében egy téma még mindig van, és ez pedig a különböző speciális az új hálózati hardver technológiák támogatása. ISA Server esetén, a Windows Server 2003 SP2-ben egy megújult hálózatkezelési csomaggal szembesülhettünk (ez Scalable Networking Pack, lásd a linket később), amely arra volt hivatott, hogy megfelelő hálózati kártya és meghajtó program esetén támogassa a hálózati csomagok feldolgozásának áthelyezését magára a hálózati kártyára, ami hasznos megoldás, mivel processzor kapacitás szabadítható fel így. Szintén újdonság volt, hogy a megfelelő NDIS miniport driver használata esetén (v6.0) a csomagok feldolgozása már megoszlott a rendelkezésre álló processzorok között. Viszont az ISA Server-nél eleinte ez komoly, a későbbi változatoknál kisebb problémákat okozott, a BPA (Best Practice Analyser, lásd a 11.4 fejezetet) sikított is emiatt, és követelte, hogy tiltsuk le az SNP csomag részeit (pl. a TCP Chimney offload-ot, vagy a Receive Side Scaling-ot).

Napjainkban viszont a lényeg az, hogy mivel a Windows Server 2008-tól ezen összetevők natív állapotban beépítésre kerültek a TCP/IP stack-be, ezért ilyen problémánk a TMG-vel már nem lehet, úgy ahogy az Explicit Congestion Notification-nel kapcsolatos sem jellemző¹⁵, már persze, ha a hálózati hardverlánc minden eleme részéről megvan a támogatás.

Scalable Networking Pack (a Windows Server 2003-hoz)

[http://support.microsoft.com/default.aspx?scid=kb;\[LN\];912222](http://support.microsoft.com/default.aspx?scid=kb;[LN];912222)

Részletes infók az ECN-ről:

Petrényi József: TCP/IP alapok, 1. kötet v2.0

¹⁵ De azért még ma is hibáznak a driverek, ergo ezt alaposan tesztelni kell és probléma esetén kikapcsolni.

<http://www.microsoft.com/hun/technet/article/?id=3effd5d3-139c-471a-adeb-a71a6885562f>

3.2.3 DNS ÉS NETBIOS

Újabb kritikus területre tévedtünk. A névfeloldás mindig az, hiszen rengeteg minden függ ennek a helyes működésétől, aminek persze nem mindig csak egy jól betöltődő weboldal, vagy egy pingelhető cím a pozitív végeredménye, hanem egy felesleges terheléstől megóvott DNS vagy TMG szerver.

Miért is függ ennyire pl. a DNS-től a TMG? Számos okot kinyomozhatunk, de megemlítenék egy nem tipikus példát. Ha szeretnénk egy olyan tűzfalszabályt kreálni, amellyel általunk kiválasztott internetes oldalakat tiltunk vagy engedünk név szerint, akkor a szabály érvényre jutásakor a TMG egy DNS név- és reverse IP¹⁶ lekérdezést is végez egymás után. Ha sok ilyenünk van, akkor mindannyiszor. Nyilván a DNS cache nem ismeretlen fogalom a TMG számára sem, ám ennek ellenére is erősen függ az alap operációs rendszer névfeloldási mechanizmusától, ha más nem addig, amíg az információ nem kerül be a saját DNS cache-be.

De mondok még egy példát a NetBIOS névfeloldás apropóján, immár lépésekbe szedve:

1. A TMG alatt futó Windows tipikusan úgy működik a névfeloldás során, hogy mindegy, hogy hogyan, de valahogy végül legyen valamilyen névfeloldás.
2. Ezért alapesetben a Windows-ok a hybrid node (HNode) típusú NetBIOS névfeloldást részesítik előnyben. Ez azt jelenti, hogyha az OS-ben DNS és WINS szerver(ek) is be vannak állítva, de ezek valamiért nem válaszolnak, akkor az OS kétségbeesetten a klasszikus, és gyűlölt NetBIOS broadcast megoldást választja.
3. Tény: a TMG névfeloldási kéréseinek jelentős része internetes host-ok felé megy.
4. Ha egy publikus reverse DNS lekérdezés nem sikerül (Mindenki kitölti a reverse zónáját? Dehogysis.), akkor végül a NetBIOS broadcast lekérdezés lesz az alapértelmezett.
5. Tény: a TMG alapértelmezés szerint blokkolja a NetBIOS broadcast üzeneteket (nagyon helyesen), de a Windows nem.
6. Kb. mennyi idő amíg kiderül, hogy a végső NetBIOS broadcast sem megy az interneten? Rengeteg, akár 1 teljes perc is. Észveszejtő.

¹⁶ Ez utóbbi egyébként egy TMG újdonság, régebben nem volt ilyen.

javaslat: tiltsuk le a TMG alatti OS-ben a NetBIOS broadcast forgalmat (azaz álljunk át PNode-ra), és egyben növeljük a TMG teljesítményét a következő registry kulcs alatti machinációval:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters

Name: NodeType

Type: REG_DWORD

Value: 2

Mivel ez a változás a Windows egyik kernel módú hálózati komponensét érinti, (konkrétan a NetBIOS over TCP/IP-t), ezért az újraindítás kötelező.

Most egy kicsit beelőzöm magam, és a munkacsoport/tartomány témát egy kicsit előre hozom, de csak a DNS apropóján. Ha ugyanis tartományban vagyunk, a belső kártya DNS szervereinek beállítása nem kérdéses, értelemszerűen a tartomány alapjául szolgáló DNS szervereket kell bejegyeznünk, és gondoskodnunk arról, hogy ez rendesen be is legyen állítva¹⁷. Ha viszont valamilyen okból egy munkacsoportban van a TMG, akkor is szükség van ugyanúgy a belső és a külső host-okkal kapcsolatos névfeloldásra, ez alap mindig. De mi van akkor, ha a céges előírások nem engedik tartományi tagság nélkül a belső DNS szerver(ek) elérését?

Két eshetőség adódik ekkor:

1. Találunk vagy telepítünk külön egy olyan nem tartományi tag DNS szervert, amely képes a "Conditional Forwarding" módszert használni, azaz a TMG-től pl. a belső tartomány felé menő kéréseket mint DNS szerver továbbítani és választ szerezni.
2. DNS szervert telepítünk a TMG-re és ezt használjuk "Conditional Forwarding" DNS szerverként a belső hálózat felé, és sima forwarder-ként a külső hálózat felé.

Mindkét megoldásnak van előnye és hátránya, ha például arra gondolunk hogy a TMG-re egy plusz szolgáltatást kell telepítenünk, az fájdalmas, ám egy külön szervert erre használni szintén az. Na de hagyjuk is ezt a munkacsoportos felállást... ..de erről majd később.

Végül és negyedik esetként a névfeloldás versus TMG ügyben, egy abszolút hibás konfigurációra hívnám fel a figyelmet. Magam is láttam, de olvastam is már olyat, hogy az üzemeltető az ISA szerveren a külső és a belső lábra is beállított DNS szervereket, ráadásul mindkettőre egyformán egy-egy külső és belső DNS szerver IP címét is

¹⁷ De ez nem TMG specifikus téma, ezt nélkül is meg kell oldanunk, pl. a külső feloldást a forwarder-ekkel vagy ha más nincs, akkor a root-dns-ekkel.

bevéste, merthogy biztos, ami biztos. Nos, ugyan ezzel nem állította meg az ISA működését, de halálosan lelassította, mivel néha az egyik ment sikeresen, néha a másik, néha elsődlegesnek használta a belsőt és így OK volt, de ha ez mégsem volt elérhető, akkor próbálkozott a belső címeznél is a külső DNS szerverrel, szóval eléggé kaotikus volt a helyzet, és eléggé izzadt az ISA szerver is.

Hááát, van ilyen is, ergo ha nem vagyunk teljesen tisztában a DNS működésével, akkor kiindulásként olvassuk el ezt a régi, de örökérvényű cikket:

Best practices for DNS client settings in Windows 2000 Server and in Windows Server 2003
<http://support.microsoft.com/kb/825036>

3.3 TMG FORGATÓKÖNYVEK

Kezdjük azzal, hogy nézzünk át egy végső ellenőrzési listát, mielőtt nekiesünk a telepítésnek.

3.1 TÁBLÁZAT

Feladat	Részletek
Az operációs rendszer biztonsági állapota	A telepítés előtt és után is szükség lesz arra, hogy a Microsoft Update szerverekről lehúzzuk a frissítéseket. Erről gondoskodunk kell valahogy (akár egy helyi WSUS, vagy SCCM is jó persze).
Meghajtóprogramok	Különös tekintettel a hálózati kártyákra!
Hálózati kártyák	Sorrend, kötések, TCP/IP - már tudunk mindent.
Névfeloldás	Mely DNS szerver(ek) segítenek majd a TMG-nek a névfeloldásban? Szükség van NetBIOS névfeloldásra is?
Belső címtartomány	Az alapértelmezett belső hálózat IP tartománya
Hálózati sablon	Milyen hálózati forgatókönyvre lesz szükség? Milyen körülmények között fog dolgozni a TMG?
A TMG gép helye	Tartomány vagy munkacsoport?

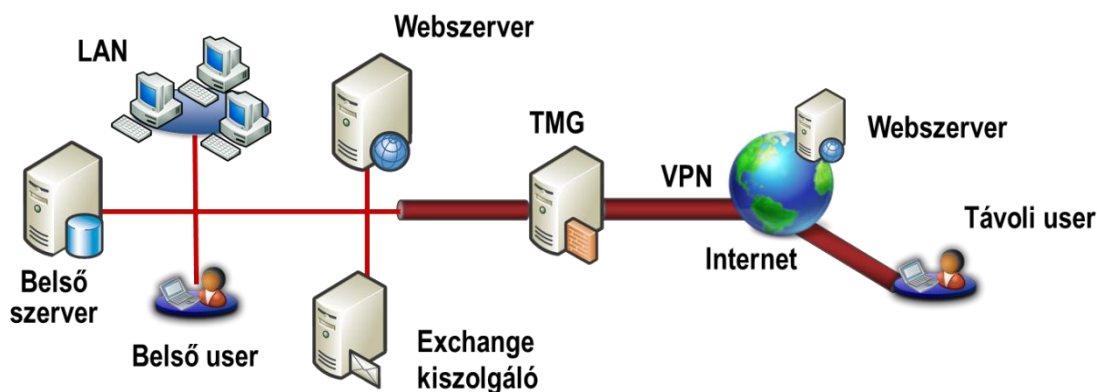
Az utolsó két kérdésre még nem tudjuk a választ, pedig ezeket mindenképpen ki kell találnunk a telepítés előtt. A tartomány vs. munkacsoport kérdéssel később foglalkozunk, viszont a helyes hálózati sablon kiválasztása most aktuális.

Persze ezt a valóságban nem 2 oldallal előbb jön, mint a telepítés, hanem nyilván jóval korábban, hiszen gyakorlatilag ez lesz az első igazán komoly része a tervezésnek. Az alábbiakban a következő öt, kiemelt forgatókönyvről fogok beszélni:

- Edge firewall (kétféle is)

- 3-Leg perimeter
- Back-end firewall
- Branch Office Firewall
- Single network adapter

3.3.1 EDGE FIREWALL



3.4 ÁBRA AZ EDGE FORGATÓKÖNYV

Talán ez a legtipikusabb, legtöbbet használt felállítás, legalábbis a Standard változatú TMG-nél biztosan. Egy tűzfalunk van, két hálózati kártyával, egy belsővel és egy az Internet-re mutató külsővel, amelynek egy publikus, fix IP-je is van. Ebben a felállásban a TMG blokkol minden nem engedélyezett forgalmat kívülről, illetve elrejti a belső hálót a nyilvános hálózatok felé. A tűzfal, a web proxy, a cache, a publikálás és a VPN szerver szerepkörök biztosan működhetnek – már ha van mindegyikre igény. Látható módon egy belső hálózatunk van, ebben közösen foglalnak helyet a kliensek, és a publikálandó szerverek is, ennek előnye, hogy a belső hálózatban a kliensek a szerverek szolgáltatásaihoz (Exchange, IIS, Sharepoint, stb.) egyszerűen hozzáférnek. Persze a hátránya is ugyanebből fakad – ha valaki átjut a TMG-n, akkor minden belső erőforrást elérhet. Természetesen ennek kivédésére ebben a topológiában is sokat tehetünk, azaz szó nincs róla, hogy védtelenek lennénk, de erről majd később.

A belső szervereinket egyszerűen publikálhatjuk az Internet felé, illetve a távoli elérést is biztosíthatjuk pl. az TMG-ban beállított VPN szerver segítségével.

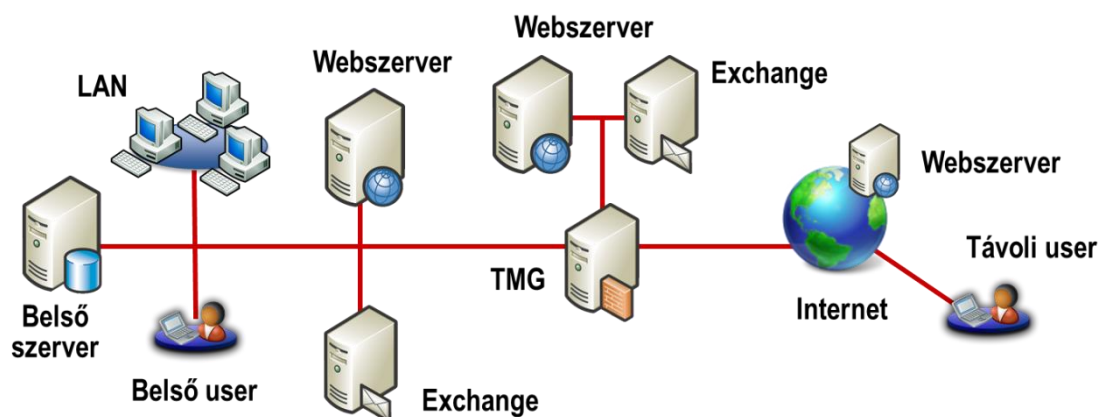
Ennek a megoldásnak létezik egy "B" variánsa is, amikor is egy kisebb cégről, kisebb hálózatról beszélünk. Ennek a cégnek nincs belső, publikálandó szervere, vagy van, de nem akarják publikálni. Az elektronikus levelezés a szolgáltatónál van, a webszerver szintén, másra, azaz pl. a távoli elérésre meg nincs szükségük. Így aztán marad az Edge felállítás, azaz a proxy, tűzfal és cache szolgáltatást használják, de pl. nincs szükség fix IP címre, illetve a TMG-ben gyakorlatilag semmilyen befelé jövő forgalmat nem kell

A KAPUN TÚL

engednünk (tiltani nem kell, a nem engedélyezés explicit tiltást jelent). Jó kis biztonságos megoldásnak tűnhet ez, persze kompromisszumokkal az, hiszen nincs Exchange, ám az SMTP-t és a POP3-at meg kell majd engednünk az összes Outlook user számára. Brrr.

3.3.2 3-LEG PERIMETER

A következő felállítás egy sokkal biztonságosabb, ergo magasabb igények esetén ezzel sűrűbben találkozhatunk.



3.5 ÁBRA A 3-LEG PERIMETER FORGATÓKÖNYV

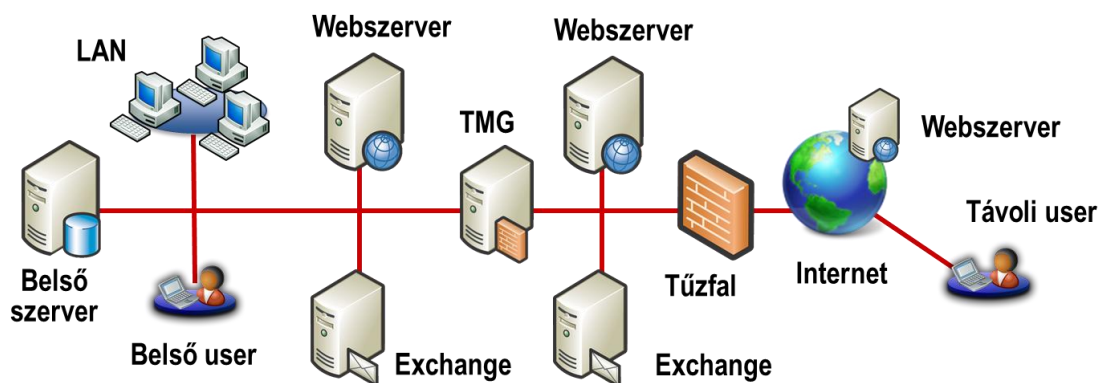
Továbbra is egy tűzfalunk van, de most már három hálózati kártyával, egy belsővel és egy az Internet-re mutató külsővel, illetve egy a Perimeter¹⁸ hálózatra mutatóval. Ekkor mindent használhatunk amit az Edge típusnál, de a publikálás változik. A belső hálózatban lévő szervereket (Exchange, Web Server) csak a belső hálózatból érjük, ha kívülről jön valaki, akkor a Perimeter felé fogjuk irányítani, ahol szintén van egy webszerver, amely ekkor a publikus webszerverünk lesz. És van itt egy Exchange is, ami az SMTP gateway lesz, azaz elfogadja a leveleket (ha rendesen csináljuk, akkor vírust is írt, és spam-et is szűr), majd a maradék hasznos tartalmat betolja a belső Exchange felé és vice versa.

A Perimeter hálózatnak van még egy komoly előnye: az ISA vagy a TMG nem fogad el innen kéréseket előzmény nélkül. Azaz nincs olyan, hogy egy támadó innen próbálkozik, még ha be is jut ide (hiszen ezek a szerverek valóban kapcsolatban vannak az internettel), innen a belső háló felé nem tud kezdeményezni. A Perimeter hálózat elérése a felhasználóink számára viszont kérdéses, és változó megítélésű, de a legjobb, ha nincs (a forgalmi hurkok elkerülése miatt adott esetben a külső webszerver és a belső webszerver szinkronját valahogy meg kell oldanunk).

¹⁸ A Microsoft szóhasználata alapján a Perimeter = DMZ.

3.3.3 BACK-END FIREWALL

Bekeményítünk. Szakítsunk az eddigiekkel, és legyen két tűzfalunk. A kettő között lesz egy Perimeter hálózatunk is, de e lényeg nem ez. Hanem az, hogy az belső tűzfalunk és a külső tűzfalunk nem egyforma típus. Ezzel jól összezavarjuk ☺, a támadót, hiszen adott esetben két teljesen eltérő tűzfal feltörését is meg kell oldania.



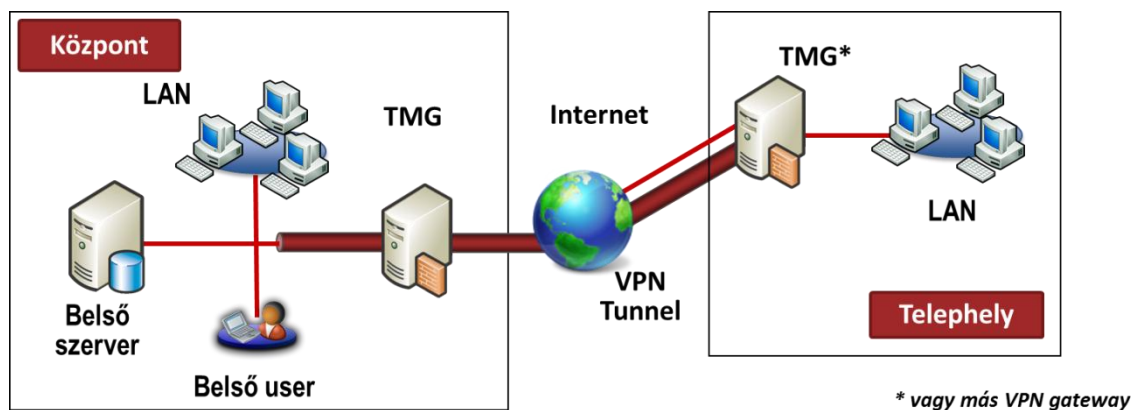
3.6 ÁBRA A BACK-END FIREWALL FORGATÓKÖNYV

Az viszont nem véletlen, hogy a belső tűzfal a TMG (mert éppen lehetne egy front-end forgatókönyvünk is), hiszen ez az, amelyiknek közelebb kell állnia a belső, mondjuk szintén Microsoft kiszolgálókhoz és az AD-hoz, hogy minél jobban kiaknázhassuk az ebből fakadó előnyöket (hitelesítés, publikálás, stb.).

Más kérdés, hogy ilyenkor tipikusan a TMG-nek nincs publikus IP-je, azaz VPN szervert kissé nehezebb fabrikálni, illetve a két eltérő tűzfal között is adódhatnak forgalom/port/stb. továbbítási és egyéb problémák, de hát a tétel örök: kényelem x biztonság = 1.

3.3.4 BRANCH OFFICE FIREWALL

Induljunk ki abból, hogy van egy telephelyünk, ez ugye nem egy szokatlan körülmény, tipikusan bizonyos cégméret felett alapértelmezés.



3.7 ÁBRA A BRANCH OFFICE FIREWALL FORGATÓKÖNYV

Erre a helyzetre is van forgatókönyvünk, amely egy állandó, vagy igény szerint felépülő (on-demand) VPN csatornán alapszik. A csatorna két végén, a hídfőállás a két TMG kiszolgáló, a két LAN felhasználói számára az egész felállás jó esetben viszont transzparens, azaz maximum a sebesség különbségből derül ki, hogy az a megosztás, amelynek parancsikonzára Gipsz Jakab kattintott nem is helyben van Csajágröcsögén, hanem Szegeden a cég központi irodájában. Ilyenkor mindenre használhatjuk a TMG szerverünket, amire eddig, a Site-to-Site VPN kapcsolatok mellett a TMG univerzális használata nem probléma. A VPN lehet PPTP és L2TP is, sőt adott esetben tiszta IPSec is (ha valamilyen elvetélt okból nem TMG-t akarunk a telephelyre tenni, akkor akár egy IPSec-et tudó hálózati eszköz is, akár egy SOHO cucc is, de azért csak óvatosan.)

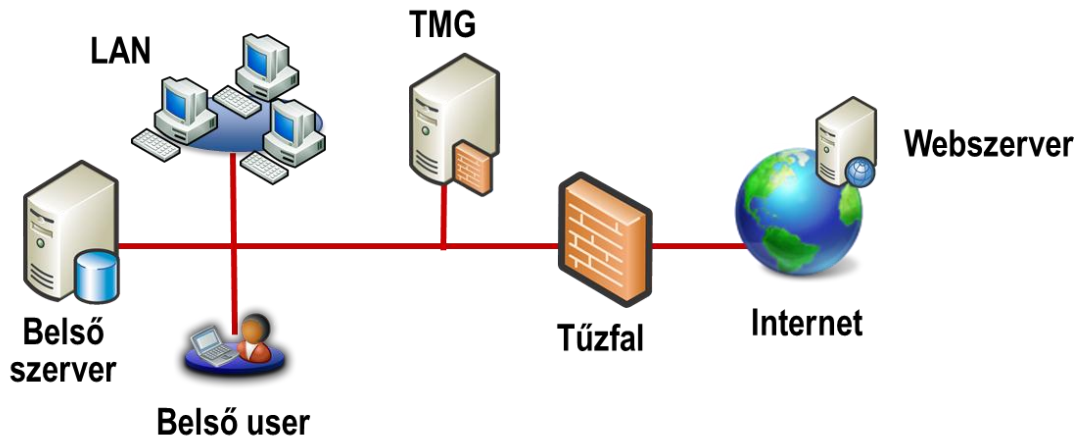
Na de bármilyen is a VPN kapcsolat, a telephelyek (mivel persze számtalan S2S kapcsolatunk lehet) internetes forgalmának ellenőrzése és korlátozása terén komoly előrelépésre számíthatunk (figyelem, ehhez nem szükséges az Enterprise kiadás!). Azaz van lehetőség arra, hogy a teljes telephelyi forgalmat a központi TMG-nk szűrje meg, sőt arra is hogy a nagy-nagy, központi gyorsítótárunkat megosszuk, és szélsőséges esetben még arra is, hogy a központi cache tartalmán kívül mást nem érjen el a telephelyi felhasználó.

3.3.5 SINGLE NETWORK ADAPTER

Ez egy pofonegyszerű forgatókönyv, erős korlátokkal és a TMG alacsony szintű kihasználásával. Ebben az esetben egy hálózati kártyánk van, és gyakorlatilag a web proxy és a cache szerepkör az ami működhet. Ilyenkor a TMG egy másik tűzfal kiegészítéseként dolgozik, és mondjuk a web proxy-n keresztül a felhasználók egyszerű azonosítása (ha mondjuk van AD-nk, akkor pl. lehet ez a fő szerepe) így viszont, "béna kacsaként" a következő feladatokat illetve szolgáltatásokat nem tudja ellátni:

- Firewall és SecureNAT kliens használata
- VPN szerver

- IP csomagszűrés
- Multi-network tűzfal szabályok
- Szerver publikálás
- Alkalmazás rétegbeli szűrés



3.8 ÁBRA AZ EGYKÁRTYÁS FORGATÓKÖNYV

Ennél több okosságot erre a forgatókönyvről nem lehet részletezni, de jó ha tudunk róla, hiszen adódhat olyan helyzet, amikor erre van szükség.

3.4 A KLIENSEK

Eredetileg ezt az alfejezetet lényegesen későbbre szántam, aztán rájöttem, hogy nem-nem, a kliensek típusának ismertetése erősen a tervezéshez tartozik, ergo bárhogy is lesz, muszáj bepasszírozni ebbe a giga-mega hosszú fejezetbe.

Tisztázzuk az elején: a TMG kliensei alatt a hálózat összes maradék gépét értjük, a tartományvezérlőktől kezdve, Jucika a titkárnő asztali PC-jén keresztül a CNC gépbe pakolt beágyazott operációs rendszerig. Sőt, maga a TMG gép is kliens.

Három típust különböztetünk meg, mindegyiknek vannak előnyei illetve hátrányai egyaránt, én most aszerint taglalom őket, hogy mennyi teendőnk van a beállításukkal. Fogjuk látni, hogy minél kevesebb a konfigurációs kényszer, annál kevesebb szolgáltatást is nyújtanak, ami egyébként józan paraszti ésszel végiggondolva logikus is.

Secure NAT (SNAT) kliens

Ez a legegyszerűbb kliens. Semmit sem kell telepíteni, bármilyen OS-en használható (nem csak a Windows platform különböző operációs rendszereire gondolok). Egyetlen követelmény van: az ügyfél OS-ben az alapértelmezett átjáró a TMG szerver belső lába kell hogy legyen. Egy egyszerű hálózatban ez nem kunszt, pl. a DHCP szerverrel könnyedén beállíthatjuk ez alapértelmezésben. Egy összetett, több alhálózattal és

útválasztóval ellátott rendszernél pedig az lesz a lényeges, hogy a TMG-hez legközelebbi útválasztó alapértelmezett átjárója a TMG legyen¹⁹.

Ahhoz, hogy a TMG támogassa a SNAT klienseket, szintén egyetlen alapfeltétel kell: a szerverben legyen 2 hálózati interfész, és használjuk is ezeket, azaz minimum az Edge forgatókönyv működjön. Annál is inkább, mivel az SNAT kliensekkel a tűzfal szolgáltatás (firewall service) tartja a kapcsolatot, a TMG NDIS miniportján illetve a csomagszűrőn keresztül. Miután tehát a csomagszűrő átengedte (azaz ha van egy passzoló engedélyező szabály, ergo nem kell hogy legyen tiltó), kiderül az is, hogy kell-e izzítani a cache-t, azaz szükség van-e a cache tartalmára, vagy arra, hogy beletöljük a megszerzett tartalmat²⁰.

Ezek után még - igény szerint - az alkalmazás- és webfilterek is átgyalogolnak ezen a forgalmon, és adott esetben engednek vagy tiltanak, vagy segítenek mondjuk egy komplex protokollnál (pl. passzív FTP, ami ugye két csatornával, hosszas egyeztetés után épül csak fel). Ezután jön a NAT, azaz a címfordítás a kliens privát és a TMG publikus címe használatával. A TMG mindkét oldal (azaz a pl. a külső webszerver és a belső kliens) felé hazudik magáról, de a szekér halad, sőt, csak így halad.

Az SNAT kliens és a TMG közötti forgalom nincs titkosítva, valamint a DNS névfeloldásban sem segít a TMG ezeknek a klienseknek, magukra (azaz a saját TCP/IP-ben beállított DNS szerverekre) vagy egy optimálisabb esetben a belső DNS szerverre vannak utalva. Viszont az SNAT kliens egy újabb előnye, hogy a nem TCP/UDP protokollokat is támogatja, mint pl. az ICMP (a 6-os IP protokoll), vagy a GRE (a PPTP egyik szükséges "kelléke", a 47-es IP protokoll). Kifejezetten fontos körülmény, hogy azok a szervereink, amelyeket publikálunk (gondoljunk egy Exchange-re vagy Sharepoint-ra, vagy egy FTP-re), azok kizárólag SNAT kliensek lehetnek²¹, pl. a tűzfal klienst tilos telepíteni ezekre.

Az SNAT kliensek óriási hátránya viszont, hogy a TMG és a kliens közötti hitelesítési folyamatban nem lehetnek résztvevők. És mivel nem tudnak hitelesítési adatokat küldeni a TMG-nek nem követelhetünk meg tőlük olyan alap lehetőségeket, mint pl. a kötelező proxy bejelentkezés vagy a "névre, csoportra" szóló tűzfalszabályok, vagy pl. a kliens forgalom felhasználói név szintű naplózása. Szóval ilyenkor muszáj a sokkal

¹⁹ Pontosabb kifejezés az, hogy a forgalomnak át kell jutnia a TMG-n. Ez nem feltétlenül az alapértelmezett átjáróval oldható meg. Sok esetben source routing-al bizonyos forgalmak a TMG felé mennek pedig az alapértelmezett átjáró ekkor nem is a TMG.

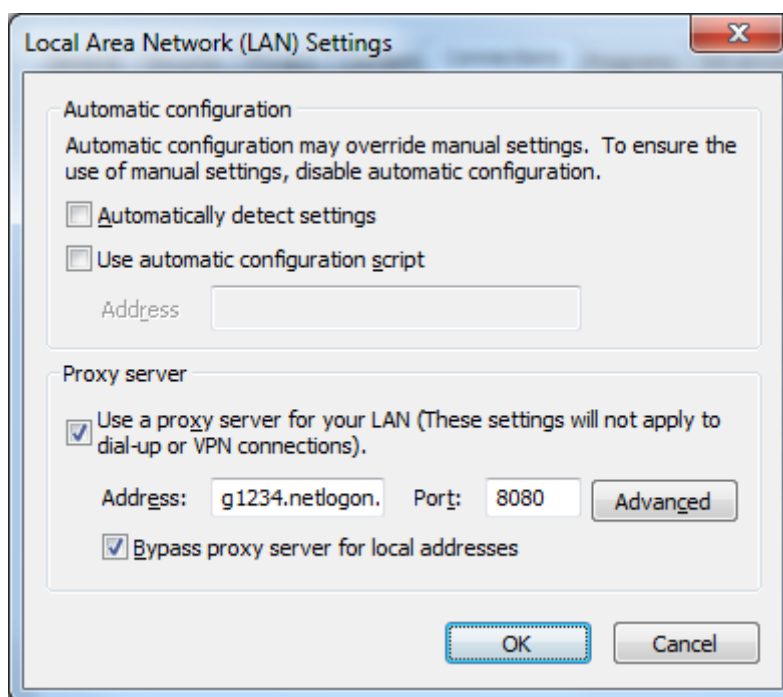
²⁰ Ez az ISA Server 2000-nél még nem volt így, ergo nem is használhatták a cache-t ezek a kliensek.

²¹ Ez nem feltétlenül igaz. Full-NAT esetében (lásd később) amikor a forrás IP nem az eredeti IP hanem a TMG IP-je, nem kell hogy a publikált szerver SNAT kliens legyen.

kevésbé flexibilis IP alapú korlátozást alkalmazni, ami amellet, hogy egyáltalán nem tökéletes megoldás, egy DHCP szervertes környezetben újabb problémákat vet fel.

Web proxy kliens

A középő. Sok szempontból. Kicsivel több konfigurációt igényel, de telepíteni mégsem kell semmit, és mondjuk a Csoportházirendből (tartományban, Windows OS esetén) el tudjuk végezni a beállítását vagy akár WPAD (Web Proxy Autodiscovery Protocol) infó segítségével. Bármilyen platformon használható, mert böngészők, webes kliens alkalmazások mindenhol vannak²², de nem mindegyikkel képes azonos szintű együttműködésre.²³ A web proxy kliens tud hitelesítést végezni (Basic, Digest, Kerberos, NTLM), de csak korlátozott protokollkészlettel (HTTP, HTTPS és a HTTP-be ágyazott FTP). Szóval középő, de mégis nagyon fontos, azaz millió esetben szükségünk van rá.



3.9 ÁBRA A PROXY BEÁLLÍTÁSOK EGY BÖNGÉSZŐBEN

A működését egy böngészőből nézzük meg, mivel tipikusan tényleg ez a szoftverkategória az amiből a legtöbbet használjuk (bár az MSN, a Skype és a társaik is jönnek fel, főképp a fiatal generációt tekintve). Elsőként beütjük a címsorba a <http://www.microsoft.hu/technet> címet. Amellet, hogy végül egy rendkívül érdekes, átfogó és izgalmas tartalommal rendelkező oldalra jutunk (☺) a háttérben kezdésként a

²² És ami az egyetlen követelmény: a legnagyobb részük képes CERN kompatibilis kéréseket intézni a proxy szerver felé.

²³ Kitaláljuk melyik böngészőhöz passzol a legjobban? (lásd később).

böngésző egy HTTP GET kérést küld a beállított proxy szerver adott portjára, azaz jelen esetben egy TMG-nek.

Az adott port az az ISA és a TMG esetében a 8080-as, és alapértelmezés viselkedés szerint a proxy működik és be is van állítva a telepítés után.

A tűzfal szolgáltatás kikeresi ekkor azt a rendszerben lévő ránk vonatkozó engedélyező (vagy tiltó) szabályt, amelyben a HTTP-ről (azaz a 80-as portról) van szó. Közben - szintén a tűzfal szerviz által - lemegy egy klasszikus DNS kérés a célpont felé, azért, mert elképzelhető, hogy egy IP alapú tiltás van a rendszerben az adott távoli host felé. Ha nem, és van engedélyünk, akkor a tűzfal szerviz továbbdobja a kérést a web proxy filternek, ami aztán elkullog a távoli host - alapesetben - 80-as portjára. No de várjunk még kicsit, ezelőtt még két kirívóan fontos dolog történik vagy történhet a beállítástól függően: az egyik a hitelesítés, ez az opcionális, de erről majd a 7. fejezetben fogok mesélni. De mi a másik? Hát az alkalmazás rétegben dolgozó szűrők, ergo pl. a HTTP forgalom esetén (de a TMG-nál, ha akarjuk már a HTTPS-nél is!) pl. a HTTP filter. Ha ezeken mind átjut a kérés, akkor megy ki a web proxy filter, és kedvező válasz esetén visszakapja a 200-as HTTP válaszüzenetet, és mehet az oldal tallózása.

Szóval a lényeg, hogy számtalan ellenőrzésre és szűrésre, illetve pl. a hitelesítésre és ennek kapcsán az auditálásra (a kliens forgalom nevesített naplózására) is van ekkor lehetőségünk. Egy másik fontos dolog, hogy a web proxy kliensről és a hozzá kapcsolódó web proxy szolgáltatásról még visszatérünk, főképp a szerver oldal kapcsán.

TMG (volt tűzfal) kliens²⁴

A legtöbb lehetőséget adó kliens ez. A legszorosabb kapcsolatot is a tűzfal kliens tudja megvalósítani a kliens alkalmazások és a TMG között. De egyúttal ez a legszűkebb környezetben is használható, mivel csak Windows OS-re passzol. És a legbonyolultabban is ez fog felkerülni a kliensre, mivel ez egy alkalmazás, amelyet telepíteni kell (a TMGC a telepítő DVD-n, a Client mappában található, és mivel .msi formátumú akár a Csoportházirenddel is telepíthetjük).

Több automatizmust is beépítve tartalmaz, pl. a TMG szerver automatikus detektálása a WPAD infók elérése céljából többféle módon is történhet (további részletek a 7.1.4 fejezetben). Egy további előnynek számít, az a lehetőség is, hogy amennyiben egy tűzfal kliens van a gépünkön, és pl. ez egy notebook, és már otthon vagyunk vele, akkor a detektálás során kiderül, hogy nincs TMG szerver a közelben. Erre a tűzfal kliens

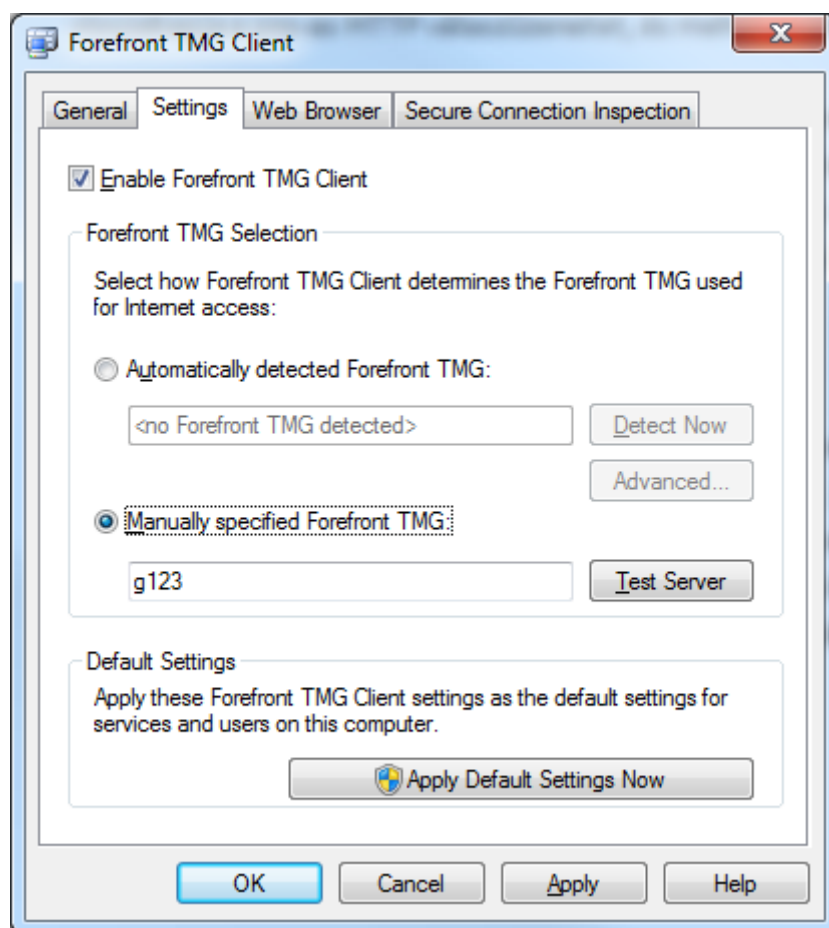
²⁴ Ugyanis terminológiai váltás történt e névvel kapcsolatban.

automatikusan "kilövi" magát, ergo a gép (és pl. az IE) mehet az otthoni eszköztől kapott default DHCP infók alapján, direktben az internetre.

Szerkezetileg a tűzfal kliens három részből áll:

- Winsock plug-in: A Windowsba integrált winsock kliens lehetőségeinek kiterjesztése, és a hatalom átvétele is egyben, azaz az alkalmazások a tűzfal kliens telepítése után kizárólag ezen a bővítményen keresztül kommunikálnak a gépen kívülre – anélkül, hogy erről tudnának. Ráadásul, alapértelmezés szerint minden forgalom csak és kizárólag a TMG felé megy, olyan mintha egy láthatatlan cső alakulna ki, vasbeton burokkal.
- Agent service: Egy rendszerszolgáltatás (Forefront TMG Client Agent, fwcagent), amely észleli és konfigurálja a winsock bővítményt, valamint folyamatosan tartja a kapcsolatot a tűzfal kliens a felügyeleti eszközzel.
- Management applet: A Tálcn is megtalálható segédeszköz, amely egyrészt mutatja a tűzfal kliens állapotát, valamint mi magunk konfigurálhatjuk manuálisan is (persze van automatikus konfigurálás is a TMG-ről), ezen keresztül beállításait.

Winsock azaz a Windows Sockets, a BSD-ből, azaz egy Unix alapú OS-ből származó API Microsoft-os implementációja, amely a hálózati kapcsolatok megteremtésével, kezelésével és felügyeletével foglalkozik. Többek között névfeloldást, adatátvitelt és egyéb hálózati feladatokat végez a Windows alkalmazások számára, azért hogy levegye a vállukról ezt a terhet. Az általános Windows hálózati modellben a Winsock a TCP/IP felett működik.



3.10 ÁBRA A TMGC – HA 4 FÜLE VAN, AZ A JÓ (AZ ISA TŰZFAL KLIENSÉNEK CSAK 3 VAN)

Természetesen képes használni a hitelesítést, sőt korlátok nélkül, azaz ebből szerkezeti felépítésből adódóan bármely alkalmazás hitelesítése a TMG felé megoldható (tartományban Kerberos, ezen kívül NTLM). A háromból egyetlen kliensként képes a forgalom titkosítására, azaz miután a TMGC az 1745-ös TCP porton felépítette a kontroll csatornát a TMG-vel, egy hitelesítés után - igénytől függően - kezdődhet is a titkosítás.

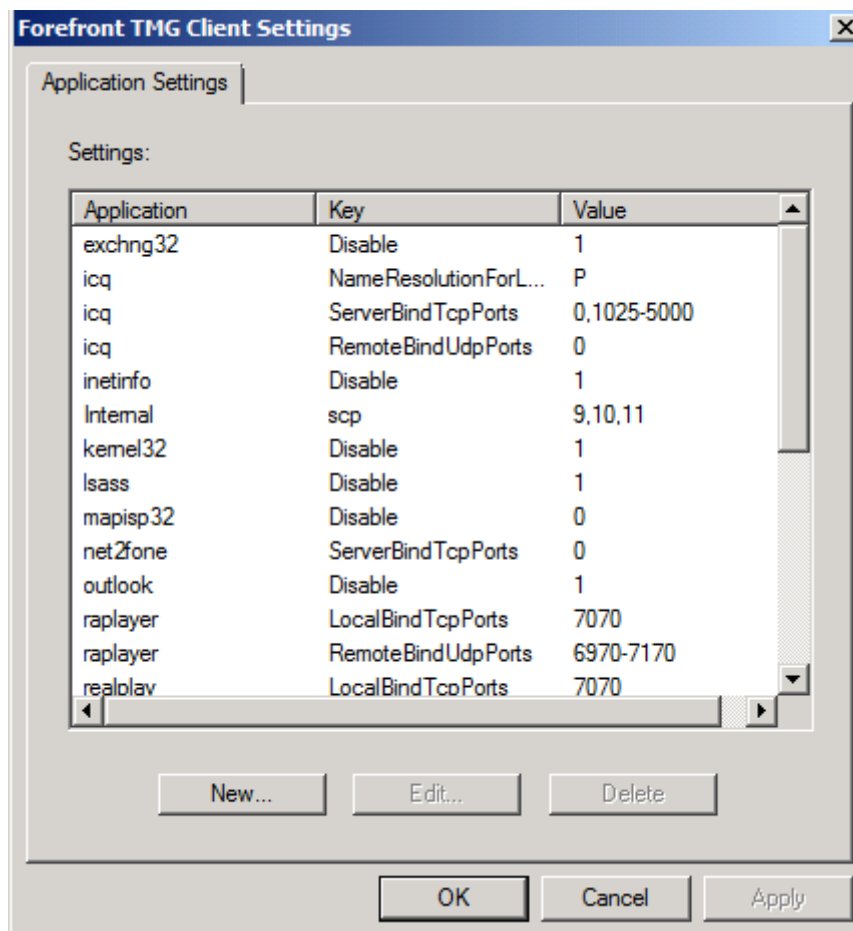
Egy másik előnye az, hogy a web proxy klienssel együtt is használható, sőt a képes automatikusan konfigurálni a proxy beállításokat is (ez persze a szerver oldali beállítástól is függ).

Kapcsolódó írások a TechNet blogon

[RDP vs tűzfal kliens](#)

Még egy dolgot meg kell említenünk a tűzfal kliens kapcsán, és ez pedig a központi konfiguráció lehetősége. Ennek egyik lehetősége az előbb említett a tűzfal kliensre és a tűzfal kliens által vezérelt böngésző beállításaira vonatkozik (lásd 5.2.3 fejezet), míg a másik a winsock alkalmazások és a tűzfal kliens viszonyára.

A TMG-ben ezeket a beállításokat a Networking \ Tasks \ Configure a Forefront TMG Client Settings alatt találjuk és következő ábrán tekinthetjük meg.



3.11 ÁBRA A TMGC SZERVER OLDALI BEÁLLÍTÁSAI

Minden paraméter amit itt beállítunk hat az összes tűzfal kliensünk működésére, azaz ezen konfig alapján működik majd együtt a kliensoldali alkalmazásokkal, amelyekből jópár már eleve szerepel ebben a listában.

Szóval, most hogy a TMG kliensekkel kapcsolatos tudományának egy részét megismerhettük, látható, hogy a megfelelő kiválasztás nem könnyű döntés. A beállítási lehetőségek, az OS, vagy böngésző típusa, a hitelesítés, a naplózás, a kapcsolat biztonsága mind-mind szempont kell, hogy legyen a döntésnél.

3.5 TELEPÍTÜNK VÉGRE

Ha eddig átrágtuk magunkat, és meg is értettük, akkor már sok gondunk nem lehet a telepítéssel, ami egyébként is (és hagyományosan) egy majdnem next-next-finish típusú művelet. De azért kövessük le lépésről-lépésre mi történik közben.

A KAPUN TÚL

Manuális telepítésről beszélünk, mivel ugyan lehet telepíteni a TMG-t is csendes (unattended) módban is²⁵, de nem gondolnám, hogy ez a tipikus, sem a nem mindennapos termék, sem az egyszerű telepítés miatt. Várni így is kell majd közben, szóval találjunk ki más teendőt is a munkavégzés idejére.

No és még két dolog:

1. Még ha van is már aktív internet kapcsolatunk, akkor ha a konzol előtt ülünk, akkor az értelemszerűen a telepítés közben lőjük le. Ha távolban vagyunk, akkor ne ☺. Ha mégis szükséges, akkor a Windows Server 2008 integrált tűzfalát mindenképpen kapcsoljuk be, vagy tegyük egy másik tűzfal mögé ideiglenesen a leendő gépünket.
2. Ha távolból egy Remote Desktop kapcsolaton telepítünk, akkor logikusan várhatjuk, hogy a TMG tűzfalának indulása után végünk lesz. De szerencsére erre a fejlesztők is gondoltak, ezért a telepítés egy adott pontján kapunk egy kérdést arról, hogy a TMG látja, hogy az RDP-n lógunk, ugyan akarjuk-e, hogy ez a cím azonnal bekerüljön a Remote Management Computers csoportba (ez egy System Policy objektum lesz), és így megkapja azt a kivételezett lehetőséget, hogy elérhessük továbbra ezen a módon.

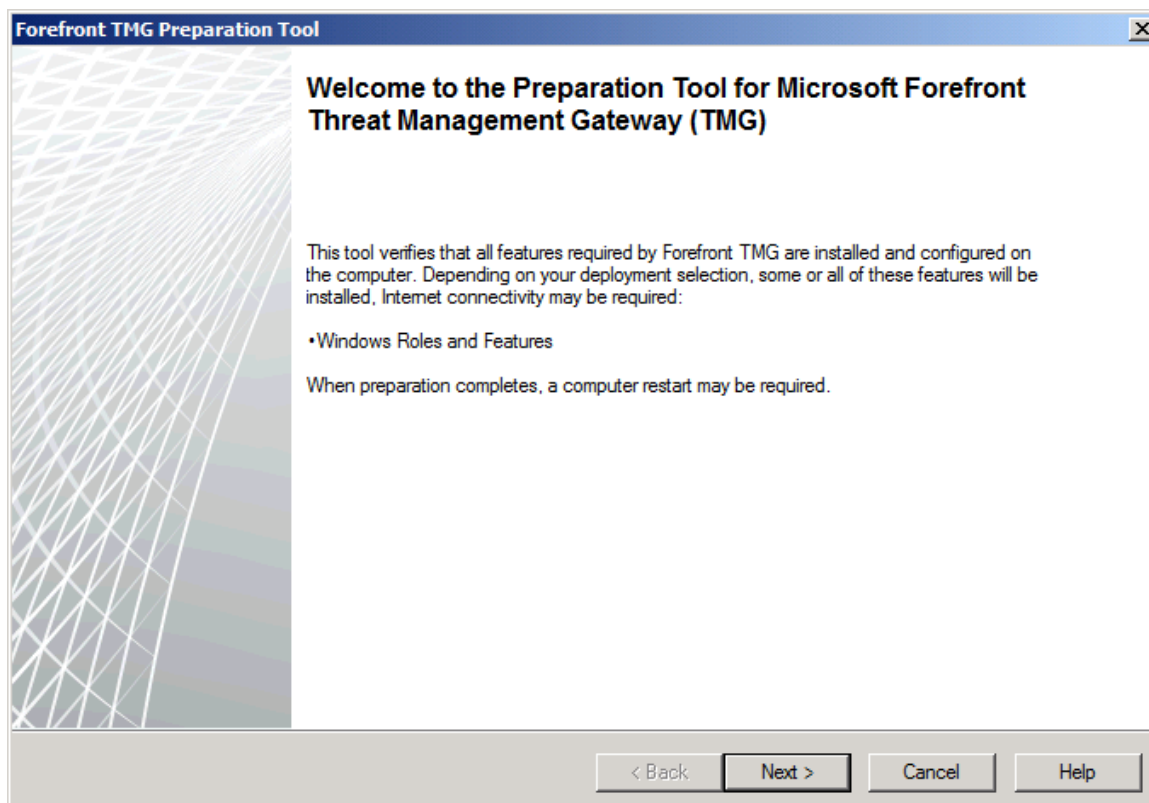
Szóval telepítő DVD be, autorun indul, ha nem akkor indítsuk kézzel az autorun.hta-t. Az alábbi képernyő fogad bennünket, és kivételesen – a jó admin szokás szerint - ne ugorjunk át azonnal, hanem keressük meg az egyik legfontosabb menüpontot, azaz a "Run Preparation Tool"-t.

²⁵ Sőt, négyféle példa .ini fájl is találunk a DVD FPC\Unattended_Setup_Sample mappájában, bár az egyik kakuktojás, mivel az uninstall-ra vonatkozik.



3.12 ÁBRA INDULHAT VÉGRE A TELEPÍTÉS!

Erről a mankóról már volt szó, és tényleg sokat segíthet, ugyanis automatikusan felpakol mindent, de mindent, ami kell, és amivel fárasztottam a Kedves Olvasót a 3.1-es fejezetben.

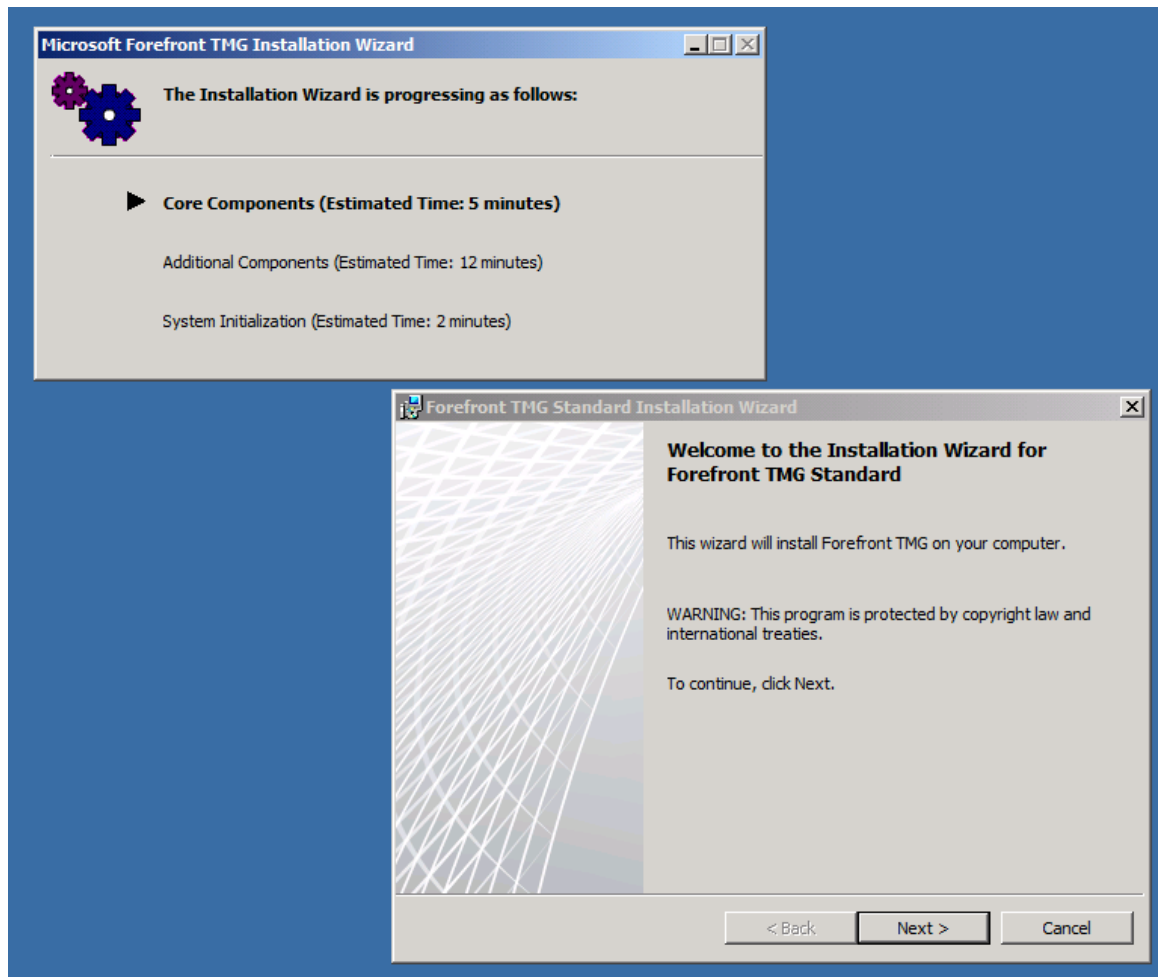


3.13 ÁBRA SZERETJÜK PREPARATION TOOL-T

Menetközben az informális képernyők után azért egy kérdést meg kell válaszolnunk, azaz hogy mit szeretnénk telepíteni: az egész TMG-t vagy csak az MMC konzolt? Az másodikat nyilván akkor választjuk, ha pl. az admin gépre óhajtjuk felpakolni ezt az MMC-t (erről később még lesz szó.) Ide tartozik még az is, hogy előfordulhat, hogy mégis szükségünk lesz a netre a Prep Tool futása közben, de erre figyelmeztet is.

Amíg fut a Prep Tool, nézzünk vissza újra a főmenübe, ahol láthatjuk, hogy 1-2 útmutató is rendelkezésre áll, illetve alul a Forefront család egy másik tagját a Forefront Protection for Exchange Server trial változatát is telepíthetjük – persze csak majd sokkal később, ahogyan a könyvbe is erről majd sokkal később lesz szó (8. fejezet).

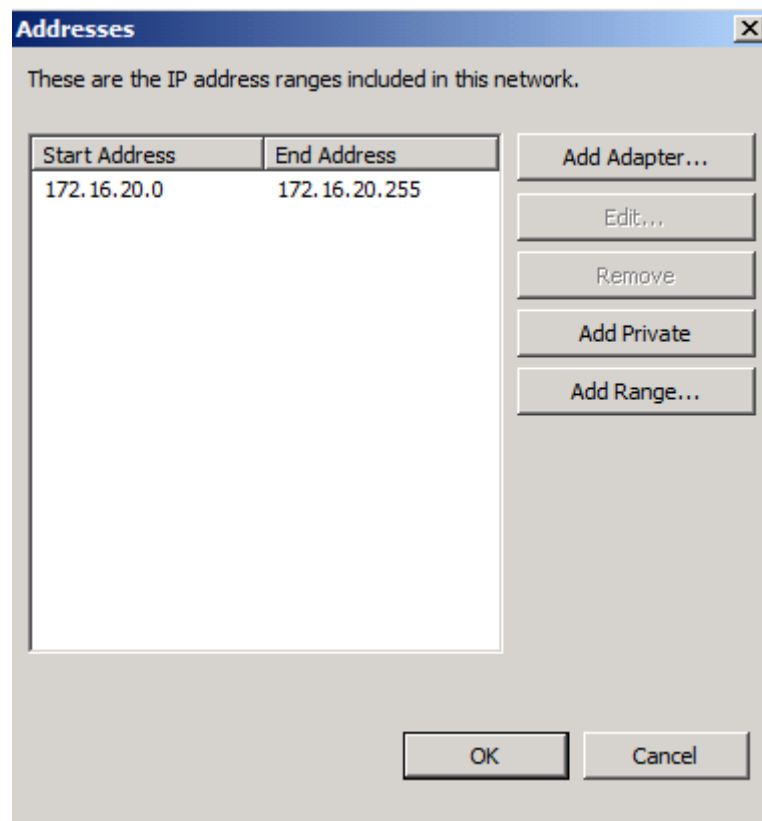
Ha kész a preparálás, akkor indulhat maga a telepítő, pl. a főmenüből, (de a Prep Tool utolsó lépéseként ki is választhatjuk ezt).



3.14 ÁBRA KIS ABLAKOK EZEK NEKÜNK, DE...

A telepítő két részből áll, van egy varázslónk, ami eleinte csak informál, licenszerződést mutat, megint megkérdezi, hogy mit szeretnénk telepíteni, telepítési útvonalat ajánl fel, illetve fent megjelenik egy műveleti ablak, amelyben a háromrészes telepítés pontjai illetve a becsült időtartam (időnként nagyon alábecsüli) mellett két animált fogaskerék teszi élvezetessé a folyamatot.

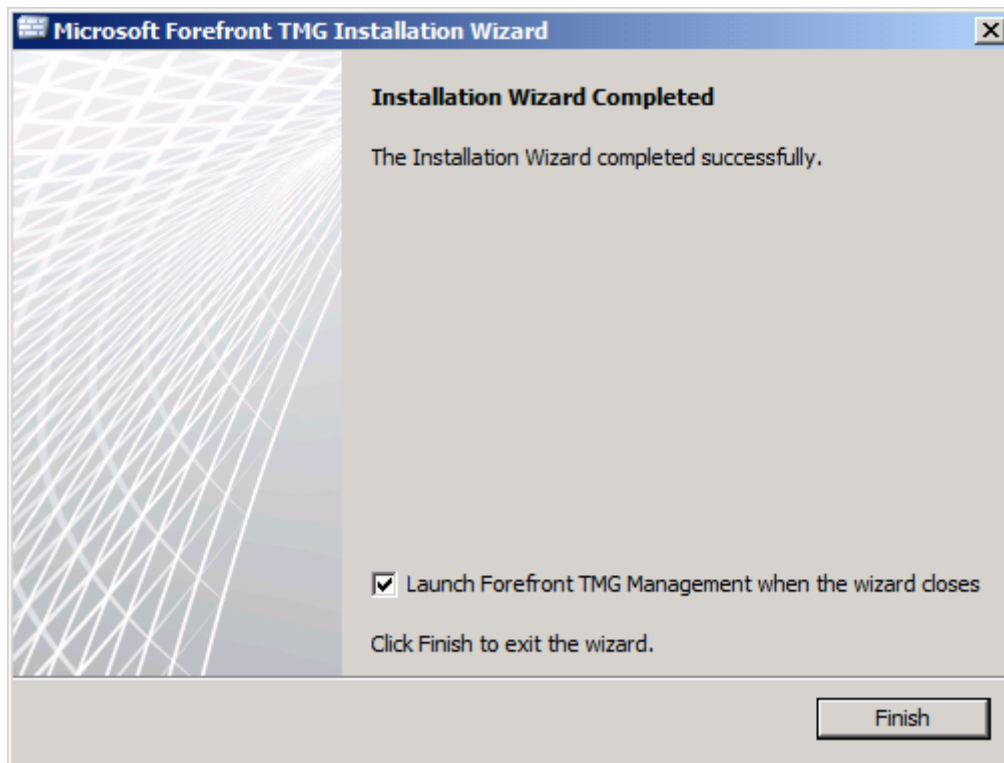
Úgyhogy lépkedjünk tovább szépen vizuálisan lenyűgözve a nagyobb ablakban, egészen addig amíg nem kéri, hogy határozzuk meg a belső hálózatot.



3.15 ÁBRA EZ AZ ÉN BELSŐ HÁLÓM, MAGAM CSOMÓZTAM

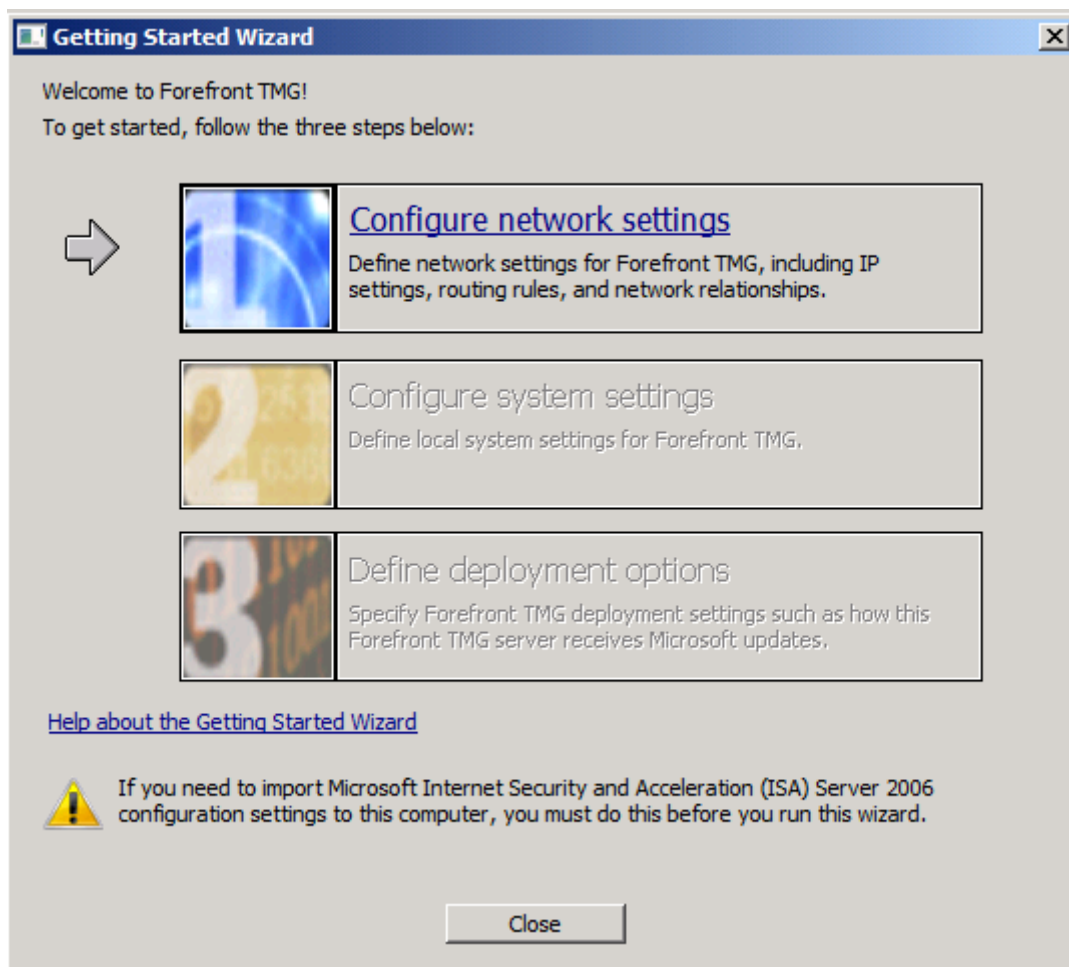
Később majd látni fogjuk, hogy nincs olyan, hogy egyetlen belső hálózat, végtelen számú lehet ebből a típusból, de egyet (főleg ha csak egy van) adjunk meg most az Add... gombbal. Hálózati kártyát, ismert privát hálózatokat, vagy tetszőleges értékhatárt is megadhatunk, igény szerint.

Jön még egy figyelmeztetés arról, hogy mely rendszerszolgáltatásokat stoppolja majd le a telepítő ideiglenesen és végleg (ez az RRAS lesz), majd indul a másolás és a telepítés. Közben majd a nagy ablak megunja és becsukódik végleg, de a kicsiben csak pörögnek, zörögnek a fogaskerekerek tovább és tovább, optimális esetben addig, amíg meg nem jelenik a szumma, hogy minden kész. Íme:



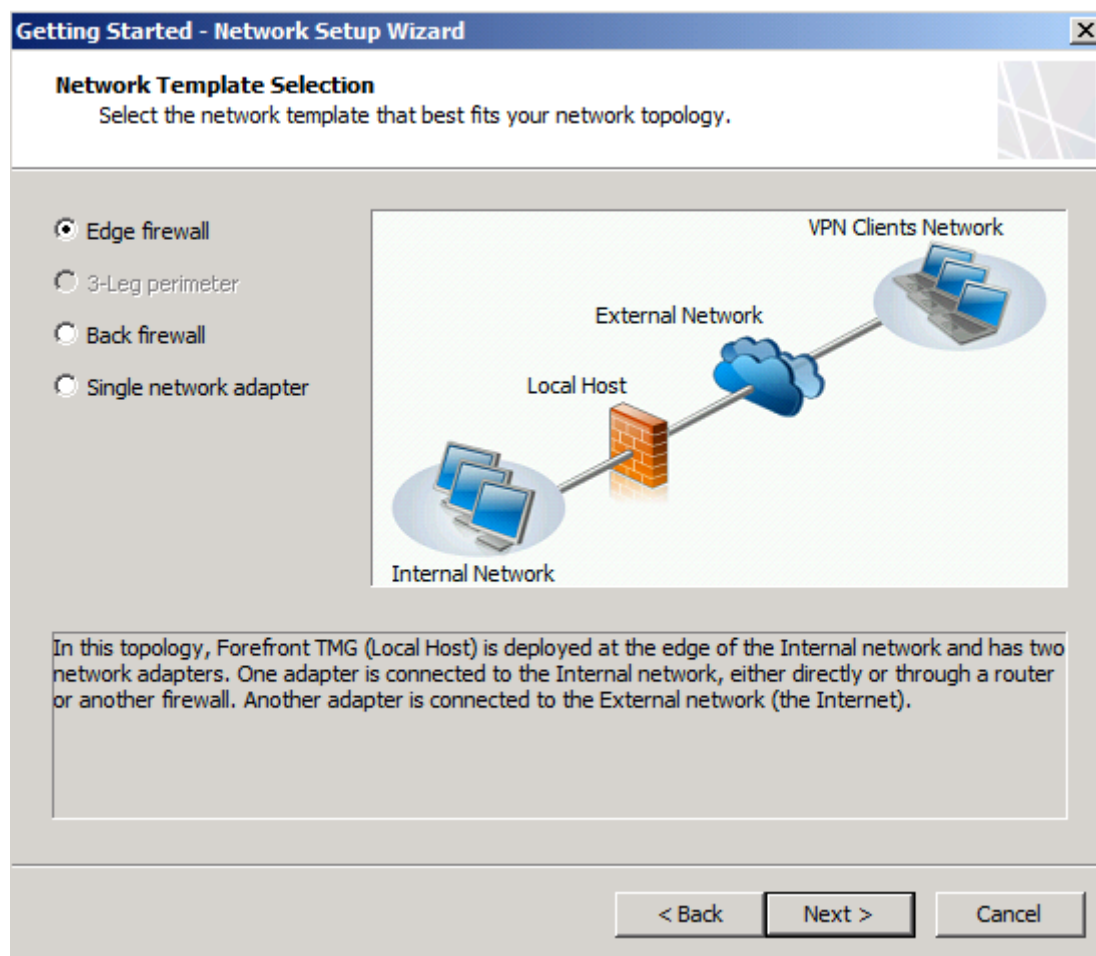
3.16 ÁBRA VÉGRE, VÉGE.

De még nincs igazából vége, azonnal síkit, hogy essünk neki a Getting Started varázslónak (ilyen az ISA-nál nem volt), hát tegyük meg. Elmondom előre, hogy itt úgyis szinte csak azokat az egyébként fontos részleteket kérdezi meg, amelyekre mi már jól felkészültünk, és mindent tudunk, vagy már be is állítottunk. A varázsló egyébként három körös, és az első lépésben hálózati beállítások jönnek.



3.17 ÁBRA KEZDJÜK A HÁLÓZATTAL.

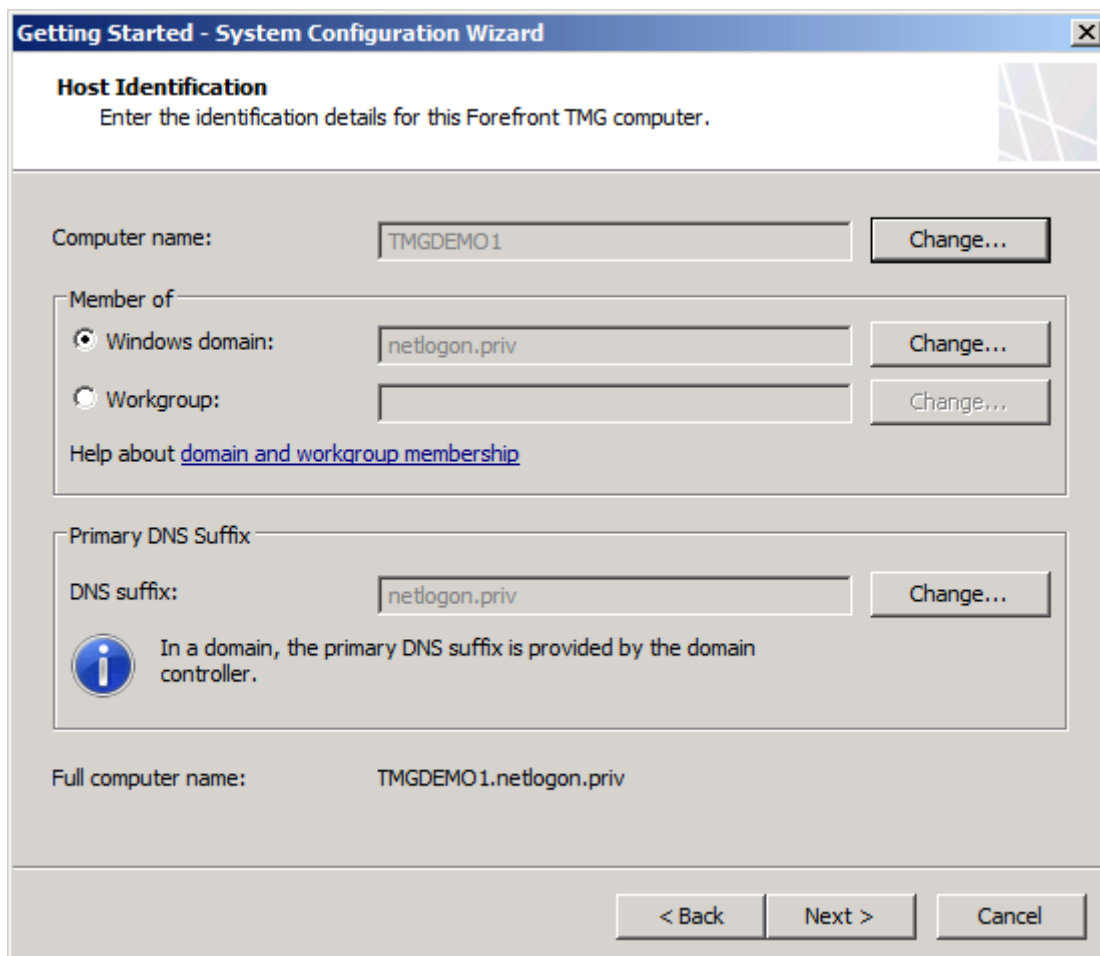
Rögtön ki kell választanunk a megfelelő hálózati forgatókönyvet, értelemszerűen a telephelyes megoldás itt még sehol sincs.



3.18 ÁBRA MARADOK EGYELŐRE AZ EDGE TÍPUSNÁL (KÉSŐBB MAJD VARIÁLUNK)

Ezután következik az belső hálózat interfészének egyszerű kiválasztása a listából (újdonság, hogy már itt is megadhatunk plusz útválasztási szabályokat), majd a következő ablakban jöhet az External hálózat definiálása (ha van Perimeter hálózatunk is, akkor az is sorra kerül). A szumma után átsétálhatunk a rendszerbeállítások varázslóba, ahol ha előzetesen beléptettük a gépet a tartományba, illetve ha jól beállítottuk a DNS utótagot, akkor semmi más teendőnk nem lesz, mert a telepítő varázsló ezeket az adatokat felismeri, jól.

Megint egy szumma jön, majd haladunk tovább a "Deployment" szakaszba, ahol már van egy-két érdekesebb rész is. Például rögtön meg kell adnunk, hogy akarjuk-e a Microsoft Update-et használni, ez ugye a különböző malware, spam és NIS szignatúrák automatikus letöltéséhez is jól jön majd, tehát érdemes a MU-t választani (persze később finomíthatunk, adott esetben majd sorrendet is felállítva, amibe egy WSUS is befurakodhat, de ne siessünk ennyire előre).



3.19 ÁBRA DOMAIN VAGY NEM, EZ ITT A KÉRDÉS

A következő lépésben (két egymást követő ablakban is) csupa olyan kérdést tesz fel a telepítő, amelyet jelenlegi tudásunk alapján egyelőre nem tudunk eldönteni, de bármit is jelölünk be, később könnyedén megváltoztathatjuk, úgyhogy szabad a vásár!

Komolyra fordítva a szót, az imént említett rendszeres frissítésre szoruló komponensek aktiválásáról illetve bekapcsolásáról van szó ezen ponton, de többet itt és most még nem árulok el.

Ezzel a javaslattal nem sodrok veszélybe senkit és semmit, mivel a telepítés közben a régi jó ISA-s szokás szerint minden forgalom, minden irányból, minden irányba le lett tiltva²⁶, egy darab alapértelmezett szabállyal.

²⁶ Kivételt képeznek a System Policy szabályai (lásd 5.4).

Getting Started - Deployment Wizard

Forefront TMG Protection Features Settings
Use this page to activate licenses required for receiving updates and to enable Forefront TMG protection mechanisms.

Network Inspection System (NIS)
License: Activate complementary license and enable NIS
[What is NIS?](#)

Web Protection
License: Activate evaluation license and enable Web Protection
Key: Evaluation Expiration date: 2010.06.17.
☒ Enable Malware Inspection
☐ Enable URL Filtering
 The URL Filtering feature queries Microsoft Reputation Service for URL categorization. The full URL string is sent to the service, using a secure connection.

[Learn about updating license agreements](#)
[Read our Privacy Statement](#)

< Back Next > Cancel

3.20 ÁBRA EZ MEG A KÖVETKEZŐ ABLAK, JELEN PILLANATBAN ÉRDEKTELEN SZÁMUNKRA

A Customer Experience Improvement programba is bejelentkezhettünk ha ez szándékunkban van, illetve a Microsoft Telemetry Reporting programba is, mindezekkel különböző szintű információkat szolgáltatunk a Microsoft-nak termék viselkedéséről, igény szerint használjuk ki ezeket a lehetőségeket vagy sem. Viszont ezután már tényleg végeztünk, habár ha nem figyelünk (bal alsó sarok) óhatatlanul belekerülünk egy hosszas varázspálca forgatásba a Web Access varázslóval (4.2 fejezet). Ha importálni fogunk később, akkor különösen felesleges ezen a varázslón végigmenni. Szóval most tényleg végeztünk, immár megkapjuk a várva-várt konzolt. Uff.

3.6 HA NEM SIKERÜL, NYOMOZUNK

Ha kész van a telepítő és sikerült, örülünk, és akár azonnal elkezdhettük nézegetni az MMC-t, de ha nem, akkor is akad azért pár lehetőségünk kideríteni, hogy miért nem koronázta az erőfeszítéseinket siker.

A KAPUN TÚL

A telepítés alatt, a TMG telepítője részletes információkat naplóz a %systemroot%\temp mappába, számtalan különböző fájlba (ezt egyébként jelzi is, egy sikertelen telepítés szummájaként). Mindezen fájlok tartalma a Windows Installer naplózáson alapszik, és igazából a hiba után rögtön, egyébként Getting Started varázsló működése alatt kerül végleges mentésre. Egyetlen kivétel viszont van: ha az Exchange-re passzoló SMTP védelemmel kapcsolatos telepítési információk a %systemdrive%\ExchangeSetupLogs mappába kerülnek, plusz ha a Forefront Security for Exchange Server komponenst akarjuk használni, akkor jó ha tudjuk, hogy a FssSetupLogYYMMDDTimeStamp.txt fájl lesz az infók gyűjtője, ami viszont a %systemdrive%\Users\All Users\Microsoft\Forefront Security for Exchange Server mappába kerül

Sok esetben viszont maga a hibaüzenet is mindent elmond, pl. az AD LDS-sel kapcsolatosak (ezt személyesen is sikerül már tapasztalnom²⁷), egészen egyértelműek, ha nem akkor nézzük meg a naplófájlokat. A mappa tartalma önmagában eléggé frusztráló tud lenni, ergo nézzük meg, hogy a fontosabbak mire valóak?

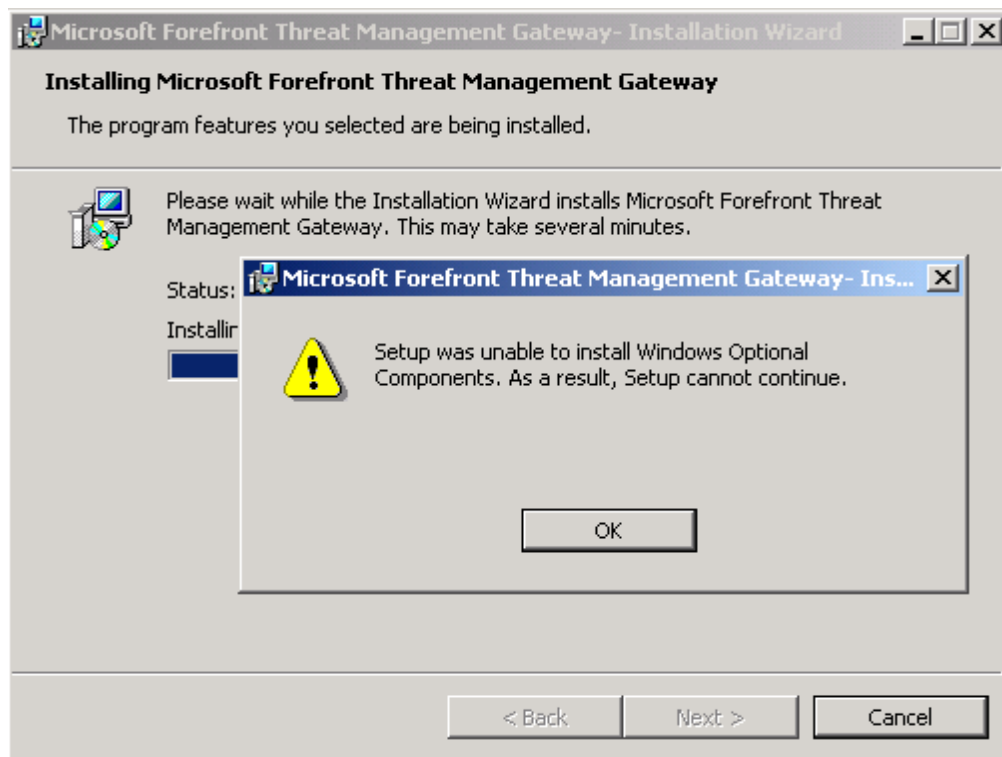
3.2 TÁBLÁZAT (AZ XXX-EK TIPIKUSAN EGYEDI SZÁMOK)

A naplófájl neve	Leírás
ISAWRAP_XXX.log	Általános infók, a telepítésről szól, de csak főbb vonalakban.
ISAFWSV_XXX.log	Nagyon részletes üzenetek a telepítésről (egy szimpla telepítésről 10-12000 sor), amelyek nagyon is fontosak lehetnek. Ha valami nem specifikus, vagy extra hibába futunk, ezt kell nagyon alaposan megnézegetni.
ISAFWUI_XXX.log	Contains information recorded by the MSI UI with events logged during the installation process.
ISAADAM_INSTALL_XXX.log	Az AD LDS telepítésével kapcsolatos történéseket és hibákat tartalmazza.
ISAADAM_IMPORTSCHEMA_XXX.log	Elégge magáért beszél a fájl neve, ugyanis az AD LDS séma importjával kapcsolatos sikeres változtatásokat találjuk meg ebben a jó nagy fájlban.
ISA_GettingStarted_XXX.log	Ha a Getting Started varázsló futása közben történik valami probléma, akkor az ebben a fájlban lesz rögzítve.
IsaUpdateAgent.log	A TMG frissítő ügynökének jelzései ebbe a fájlba kerülnek, de nemcsak a telepítés,

²⁷ Volt már olyan a béta verziók cserélése közben, hogy nem sikerült rendesen egy AD LDS instance eltávolítása, és ez rögtön kibukott a telepítés elején. Némi takarítás után viszont megoldódott.

	pontosabban a Getting Started varázsló alatt, hanem később is.
ServerManager*.log	Minden infó a Windows Server szerepkörök és képességek telepítéséről (amit ugye e Prep Tool végez)

Találunk még itt egy nagy halom *.etl fájlt is, de ezeket mi nem tudjuk értelmes információként felhasználni, mert ezek a különböző tracing naplófájlok, amelyek a Microsoft felé elküldhetünk, ha megengedjük pl. a Customer Experience Improvement programban részvételt.



3.21 ÁBRA ITT VALAMI BIBI VAN, ÉS MIVEL EGY OS KOMPONENST ÉRINT, AZ ESEMÉNYNAPLÓBAN IS LESZ RÓLA BEJEGYZÉS

Egyébként még annyit erről a témáról, hogy abban az esetben ha a telepítő hibába fut bele, akkor ezt tipikusan értelmesen közli, és ha tudomásul vettük az üzenetet, akkor azonnal egy roll-back jön, azaz visszaállít mindent, és leszedi a "szemetet". Ez a tapasztalatom szerint pontosan működik.

3.7 MIGRÁCIÓ, EXPORT-IMPORT

Az esetek jelentős százalékában szükségünk lesz a migrációra. Azaz már van valamilyen kiadású ISA serverünk, amelyet már felruháztunk az évek során számtalan okossággal, hálózati objektumokkal, szabályokkal, szóval elképzelhető, hogy egy évek alatt kicsiszolt konfigurációt nem szeretnénk eldobni és mindent újratekdeni. Már csak azért

sem, mert a *"Ki tudja a 47-es szabályt mikor és miért hoztuk létre?"*, *"Mi az oka hogy a 22-es System Policy szabályban be van állítva a Kőfaragók csoport?"* és más hasonló kérdések egy átálláskor aktuálisak lehetnek²⁸. És van még egy tuti apropója a migrálásnak: az ISA 200x-ek és a TMG között biztosan nem tudunk helyben frissítést (in-place upgrade) végezni, mivel az egyik csak Windows Server 2003 x86-on megy, a másik pedig kizárólag Windows Server 2008 / R2 X64-en. Ez eléggé behatárolja a lehetőségeinket, szóval éljen a migráció.

Ha szabad személyes tartalmat belecsempészni ebbe a fércműbe, akkor el kell mondanom, hogy történelmi okokból jómagam a migrációtól kb. úgy tartok mint a egy fúrómániás fogorvostól, szóval nagyon. Volt lehetőségem (a kényszerről már ne is beszéljünk) az ISA 2000 és a 2004, valamint a 2004 és a 2006 verziók között sokszor migrálni, és akadtak negatív tapasztalataim is (sőt). Mióta .xml alapú a konfiguráció mentése, exportálása, visszaállítása, stb. azóta a helyzet sokat javult, de miután egyszer-kétszer könyékig merültem az .xml fájlba, hogy működhessen az import²⁹, azóta beleremeg a billentyűzet, ha ilyesmibe kezdek.

ISA Server 2006 frissítés - vegyes élmények I.

<http://www.microsoft.com/hun/technet/article/?id=517752bc-6d76-4471-b102-365c7e7dc213>

ISA Server 2006 frissítés - vegyes élmények II.

<http://www.microsoft.com/hun/technet/article/?id=cf71adf5-5ac1-49a7-9171-e63ccc0dc2b4>

Rendszerfrissítés - majdnem tőszavakban

<http://www.microsoft.com/hun/technet/article/?id=48b5fc18-563a-420f-9c6f-729d43fd904a>

Aztán, pár éve, az ISA Server 2006-ok egymás közötti migrálása kapcsán már alig volt problémám, és a dolog látványosan a TMG bétáknál javult fel, könnyedén ment keresztbe kasul a folyamat az ISA 2006 vs. TMG témakörben, illetve a béták között is (erre sokáig nagy szükség volt, mivel a béta fázisok között sokáig nem volt helyben frissítés, és aztán a végső RC-k és az RTM között sem lett, de ez most más kérdés). Szóval amióta TMG-kkel dolgozom, és két TMG között, vagy ISA 2006-ról kell átállni, azóta a migráció gond nélkül megy. De azért van pár előzetes teendő, amivel sokat

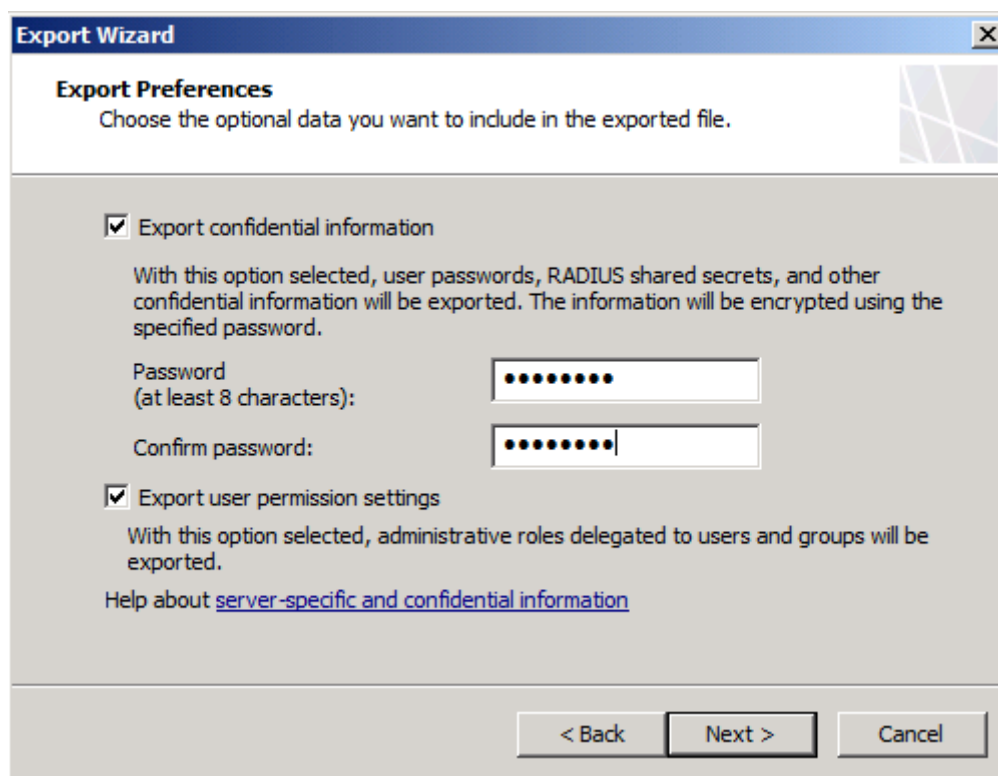
²⁸ Nyilván egy tökéletesen dokumentált rendszerben ilyen nem fordulhat elő, na de tegyük a szívünkre a kezünket...

²⁹ Érdekes módon az exporttal sosem volt gond ☺.

segíthetünk azon, hogy ne kelljen falat rugdosni a sikertelen migráció közben, vagy után.

Először is, a migráció gyakorlatilag az ISA 2006-os konfiguráció lementését (Backup) jelenti, majd a visszatöltését (Restore). De, emellett van még export/import lehetőségünk is, amivel finomíthatunk a lementeni kívánt materián, azaz csak a tűzfalszabályokat, vagy éppen csak a hálózati környezet beállításait szeretnénk átvinni.

Mindez az .xml formátum térhódítása óta van így, az ISA 2000-nél ez még igencsak másképp volt, na de feledjük el a negatív emlékeket. A lényeg, hogy használjuk ki ezeket a rugalmas lehetőségeket, jómagam pl. amit csak lehetséges (tűzfal szabályok, sőt a lényegesebb szabályokat akár egyesével is, VPN konfiguráció, cache szabályok, stb.) kiexportálok .xml-be, több részletben, majd megkoronázom egy hagyományos mentéssel is és időnként még screenshot-okat is készítek, főleg ha tényleg összetett a konfiguráció. Sőt csináltam már nagyjából ugyanolyan virtuális környezetet is a modellezés miatt, de ez utóbbi talán már tényleg extra példa, legalábbis egy kisebb hálózat esetén.



3.22 ÁBRA EZ A BACKUP, DE VALÓJÁBAN EGY "EXPORT ALL"

A probléma megoldása néha nagyon egyszerű. Nézzük meg, hogy milyen, kevésbé a szemünk előtt lévő objektumaink vannak a régi rendszerben. Van-e pl. valahol egy eldugott az automatikus tárcsázáshoz szükséges ADSL kapcsolatunk integrálva az ISA szerverbe. Ha van, és az új gépen nincs ilyen kapcsolat (mert pl.

nem is lehet), akkor ennek kitakarítása a régi gépen, majd egy újabb mentés után, a visszaállítás máris sikeres lesz. Vagy pl. gondoskodtunk-e a privát kulcsokkal ellátott tanúsítvány átviteléről az új gépre? Ezeken sok múlhat.

Egy nagyon fontos jószág, hogy a mentéssel, vagy az exporttal az alkotóelemek, azaz a különböző objektumok (pl. egy saját definiálású protokoll, vagy egy URL gyűjtemény) is eltárolódik és a visszaállítás vagy az import után az új helyre is bekerül.

És, van arra is lehetőségünk, hogy a tanúsítványok beállításai (maga a tanúsítvány nem!), a jogosultságok, és az egyéb szenzitív információk is "átmenjenek", de ezekhez többnyire egy jelszavas védelmet is kell rendelnünk majd, de annyi baj legyen.

Nos, akkor végül a sok-sok csapongás után foglaljuk össze a lényeget egy felsorolás formájában A-tól Z-ig:

- A TMG nem telepíthető a 32-bites OS-eken.
- A TMG nem telepíthető a Windows Server 2003-ra.
- A TMG nem támogatott minden Windows Server 2008-on (Server Core/Web/Foundation kiadások)
- Az ISA Server 2004/2006-ről TMG-re történő helyen frissítés nem támogatott (ez az első két sorból egyébként is kiderül).
- Ilyenkor az eljárás a következő: alapos ISA export > új telepítésű WSo8 SP2, vagy WSo8 R2, TMG telepítés, import.
- Ha van egy TMG-nk egy Windows Server 2008-on, akkor nem lehetséges egy az egyben az R2-re frissíteni. Ilyenkor: alapos TMG export > TMG eltávolít > Windows Server 2008 R2-re frissítés > TMG telepítés > import a helyes megoldás.

Egy teljesen részletes, sok-sok képernyőképpel illusztrált migrációs dokumentumot az alábbi linken nézhetünk meg.

How to migrate Microsoft ISA Server 2006 to Microsoft Forefront TMG
<http://www.isaserver.org/tutorials/How-migrate-Microsoft-ISA-Server-2006-Microsoft-Forefront-TMG.html>

3.8 VIRTUÁLIS KÖRNYEZETBEN?

Igen, igen, nincs mit tenni, 2010-re ez a témakör is bőven aktuálissá vált. Sőt, már korábban, az ISA Server 2006 életében is eljött ez a változás (a TMG-nél pedig a Beta 2-től). Mindez annak ellenére, hogy jó ideig nem volt ajánlott virtuális környezetbe rakni ezeket a szervereket.

Jim Harrison 28 perces előadása: Virtualize your ISA or Forefront TMG servers
<http://edge.technet.com/Media/Virtualize-your-ISA-or-Forefront-TMG-servers/>

Két fő – a virtualizáció specialitásaiból fakadó – szempontot emelnék ki részletesebb magyarázatra, a host (parent) gép biztonságát, illetve a hálózati sajátosságokat, különös tekintettel a hálózatok kapcsolódási forgatókönyvére.

A host géppel szemben támasztott kritériumok közül az első a jól megválasztott OS. Ha pl. valamelyik Server Core operációs rendszert választjuk, akkor máris nyugodtabban alhatunk, hiszen ez a kiadás – a behatárolt képességek miatt – biztonságosabb, kevesebb biztonsági frissítést igényel és kevesebb felügyeletet vár el. Ellenben azzal viszont a speciális körülmények miatt (a Server Core nem alkalmazásplatform) számolnunk kell, hogy az esetleges a hostra szánt alkalmazások tekintetében kompromisszumot kell vállalnunk. Mindezek ellenére sosem válasszunk a host gép operációs rendszerének nem kifejezetten hálózati kiszolgáló operációs rendszert és hardvert, azaz pl. egy munkaállomást. De még akkor is ha server, nagyon oda kell figyelni a szülő partíció hozzáférésekre (felhasználói fiókok, fájlrendszer, stb.), hiszen megint csak ez a partíció lesz a legkönnyebben kijátszható "átjáró" a host gépek felé. Így aztán adott esetben a Bitlocker és társai hasznos szolgálatokat tehetnek a biztonság érdekében.

A szülő partíciónak mindenképpen up-to-date állapotúnak kell lennie a biztonsági frissítések szempontjából (is). Ez farkastörvény, hiszen ebben a helyzetben nem csak egy gépet veszélyeztetünk, hanem minden guest gépet is. Egy másik fontos szabály, hogy biztonsági szempontból az ugyanazon a hoston futó guest gépek legyenek egy súlycsoportban, egy erősen sarkított példával élve, pl. Exchange és SQL szerverek ugyanazon a Hyper-V szerveren ne legyenek internetes játékszerverek.

A host gép hálózati védelmével kapcsolatban az integrált tűzfalat célszerű elsőként megemlíteni. Mivel a Windows Server 2008 Filtering Platform már egy tűrhetően izmos, teljesen kétirányú és jól konfigurálható tűzfalat ad a kezünkbe integráltan, használjuk bátran és szigorúan, nem fog ütközni a guest gép(ek)en futó TMG-vel. Belülről kifelé haladva, természetesen a fizikai gépet a fizikai rétegben működő eszközökkel (router, switch, tűzfal) is védhetjük és védjük egy plusz körös védelem részeként.

A hálózati kapcsolatok témakörben a szülő és a gyermek partíciók, a külső hálózat (Internet) valamint a valós fizikai hálózat közötti hálózati forgalom irányát és szabályait kell megfelelő alapossggal lefektetni. A legfontosabb hogy értelemszerűen kerüljük el

A KAPUN TÚL

a tipikusan internetes (External típusú) hálózatunk mérték nélküli hozzárendelését. Sem a host, sem a guest gépek nem kaphatnak ebből, csak és kizárólag a TMG.

Így hát induljunk ki abból, hogy a TMG guest gépnek (mivel mondanom sem kell, hogy a TMG-t célszerű egy guest gépre rakni és abszolút nem a host-ra) virtuális gép mivolta ellenére direkt fizikai hálózati elérése van, dedikált hálókártyával. Ekkor ezen keresztül történik minden külső hozzáférés, azaz a további guest gépek és a fizikai LAN elérése is és fordítva is (egyelőre elméletben a host gépe is, de nem sokáig). Ha így alakítjuk ki a rendszert, akkor egy esetleges támadó feladatát is megnehezítjük, hiszen az összes géphez hozzáférést szerezni csak a TMG-n átjutva lehet. Ez egyúttal azt jelenti, hogy a TMG belső lábához csatlakozik a többi guest gép, LAN és a host gép (a szülő is).

Emellett a monitorozásnak, a felügyeletnek még nagyobb súlya lesz, mint egy fizikai hálózat esetén, hiszen a virtuális hálózati forgalom az adott esetben a fizikai hálózaton megtalálható felügyeleti eszközök számára tipikusan kevésbé átlátható, tehát erre extra figyelmet kell fordítanunk.

Ez egy viszonylag egyszerű megoldás volt, de most elkezdjük bonyolítani.

Ha még okosabban tervezünk és van rá lehetőség, akkor mindhárom belső hálózat (guest-ek, host és a LAN) külön-külön virtuális interfésszel rendelkezve az TMG-be csatlakozhat, azaz immár az egymás közötti és egyúttal a kifelé tartó forgalmukat is a TMG tartja kézben.

De még közel sincs vége.

Ha lehetséges (és miért ne lenne az?) éles működés közben ne kapcsoljuk össze a szülő partíció hálózati kapcsolatát a gyermek partíciók hálózati kapcsolataival, azaz sem a guest gépek, sem a LAN gépei semmilyen körülmények között ne lássák a host gép saját, privát hálózatát, izoláljuk el.

Ha az eddigi példát nézzük, akkor ezt úgy tudjuk teljesíteni, hogy az eddigi három virtuális hálózatból kettő marad, és a host sem a TMG-hez, sem a guest, sem a LAN gépekkel nem áll összeköttetésben, hanem egy dedikált felügyeleti interfészen keresztül fogjuk piszkálni, ami minden más géptől független. Ilyenkor egy kábelezés könnyítő megoldás az, ha készítünk egy olyan hálózatot is a TMG segítségével, amelyben csak a host gép és a felügyeleti gép van IP szinten kizárólag és ekkor fizikailag nem, csak logikailag zártuk össze ezt a két gépet, illetve izoláltuk.

Azonban, ha a host gépet mégis el kell érünk valahogyan és adott esetben ez nem oldható meg egy cross kábellel, vagy egy logikai hálózattal és egy dedikált munkaállomással (gondoljunk arra pl. hogy az egész hóbelevanc egy szerverhotelben van), akkor marad a közbülső megoldás (persze nyilván ilyenkor LAN nincs).

Nem tudom figyeljük-e a párhuzamot a klasszikus fizikai hálózatokkal összevetve, merthogy van bőven, gyakorlatilag a célok ugyanazok, még akkor is, ha a virtualizációval másképp, azaz kissé "bedobozolva" kapjuk meg a gépeket.

A virtualizáció kapcsán, a hálózati kártyák viszonylatában még egy kis adalék:

- Mindig a legfrissebb, és kizárólag aláírt meghajtó programot használjunk. Ezzel sokkal többet használunk az idegrendszerünknek, mintha ugyanezt a fizikai gépek esetén tennénk.
- Használjuk előzetesen és alaposan a megfelelő tesztsoftvereket a speciális szerver szoftverek (Exchange / SharePoint, SQL, stb.) esetén, a hálózati teljesítmény kivizsgálása apropóján.
- Ha lehet (de ebben mondjuk 30 guest gép esetén van egy kis túlzás), rendeljünk a virtuális hálózatokhoz dedikált hálózati kártyát, külön-külön. Többek között pl. a hálózati teljesítmény szempontjából is ez az igazán nyerő megoldás.
- Az MS Loopback kártya nem számít sem igazi dedikált, sem megfelelő teljesítményű interfésznek.

Ezt a részt Lepenye Tamás kollégám egy korábban (még az ISA vs. Virtual Server kapcsán) elkövetett megállapításával zárom, mivel továbbra is teljesen életszerű:

"Virtuális környezetben futó tűzfal akkor egyenértékű biztonság szempontjából a fizikai gépen futó tűzfallal, ha:

1. A host operációs rendszer üzemeltetése biztonsági szempontból ugyanolyan vagy szigorúbb, mint a tűzfal rendszeré, minden egyes tűzfalat érintő kockázati tényezőre vonatkozóan.
2. A gazdagép üzemeltetői személyzetének megbízhatósága ugyanolyan, vagy jobb, mint a virtualizált rendszerek üzemeltetői személyzetéé."

3.9 JÓ HA MEGSZÍVLELJÜK...

Ebbe a fejezetbe megpróbálok bezsúfolni jó néhány eddig le nem jegyzett ötletet, ökölszabályt, tippet és ismert korlátot a tervezéshez és a telepítéshez. Kicsit zajos lesz, de talán kevesebbszer kerül a Kedves Olvasó zsákutkába, ha elolvassa.

3.9.1 NÉHÁNY ÖKÖLSZABÁLY

- Lehetőleg semmi mást nem telepítünk a TMG gépre, a TMG-n és a megkövetelt szoftver összetevőkön kívül. De tényleg semmit, még egy WinRAR-t sem. Ez a TMG pozíciójának következménye, mivel ez a rendszer véd bennünket, valamint tipikusan ennek a rendszernek kell folyamatos kapcsolatban lennie a külső hálózatokkal, és így rosszul jön ki, ha azért lyukas a rendszerünk mert az egyéb szoftverek lyukasak, vagy azért kell újraindítanunk, mert a plusz szoftverek ezt igénylik. De itt kell megemlíteni az esetleges port/protokoll konfliktusokat is.
- Sosem telepítjük a TMG-t tartományvezérlőre (már az SBS-en sincs!). Csak három okot említek: terhelés, biztonsági problémák, szenzitív információk.
- Bármilyen furán hangzik, de nem használjuk együtt más tűzfalakkal együtt sem. Ebbe beletartoznak a személyi tűzfalakkal rendelkező AV szoftverek is. A Windows integrált tűzfala kivételnek számít, egyrészt a TMF fel van készítve az együttműködésre, másrészt kikapcsolja.
- Csak bizonyos korlátokkal rakhatunk vírusirtót a TMG-re. Erre rendelkezünk hivatalos ajánlással is, lásd a következő link.

Considerations when using antivirus software on ISA Server

<http://technet.microsoft.com/en-us/library/cc707727.aspx>

- A gyári telepítési útvonal megtartása ajánlott, de ha mégis variálunk, akkor egyedi, extra NTFS jogokat ne definiáljunk a célhelyre (ha nem így teszünk, a telepítő hibaüzenete majd figyelmeztet bennünket erre).
- Az R2-ben a .Net Framework 3.5.1 bent van, a Server Managerben megtaláljuk, a Prep Tool ezt meg is teszi nekünk. Ám, ha a Windows Server 2008-nál a Prep Tool-nak ezt először le kell töltenie. Ráadásul kötelező proxy autentikációval ezt nem tudja megtenni. Tehát vagy kapcsoljuk ki ezt a jelenlegi proxy szerverben, vagy töltjük le és tegyük fel kézzel.
- Vegyük figyelembe, hogy a TMG (ahogyan az ISA is) egyrészt leállítja az RRAS-t, másrészt ha beüzemeljük az TMG konzolban a VPN szerver, akkor ciklikusan felülírja az RRAS konfigot TMG-ben beállított értékekkel. ez igaz az interfészekre is (pl. a demand-dial interfészt speciel törli).
- Ha NLB-t szeretnénk használni, akkor ne kezdjük el kialakítani az NLB-t a TMG telepítése előtt.
- Ahogy már korábban is jeleztem, az IPv6 támogatás erősen behatárolt. Az IPv6 blokkolás viszont konkrét:
 - o Az ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) és a 6to4 interfészek letiltásra kerülnek, tehát az IPv4-es csomagokba terelt IPv6 forgalom megáll.

- Ugyan a Forefront TMG Control rendszerszolgáltatás az IPv4-es DNS "A" rekordját mindig beregisztrálja automatikusan, AAAA (IPv6) rekordot viszont sohasem készít és így nem is frissít. Sőt, adott esetben a DNS, az ARP és a Neighborhood Discovery³⁰ cache-k IPv6-os tartalmát is törli.

Ma még (2010 február) nem³¹, de idővel bizonyára szükségünk lesz a telepítő komponenseinek előzetes frissítésére (pl. rollup csomagok vagy szervizcsomagok), azért hogy a telepítés közben is már a megfelelő fájlokkal dolgozzunk. Ehhez a következő pár lépésre lesz szükség:

1. Másoljuk be a DVD tartalmát egy tetszőleges mappába a merevlemezre (pl. C:\TMGInstall).
2. Töltsük le a frissítést, és másoljuk be ugyanide.
3. Nyissunk egy parancssort, és navigáljunk el ebbe a mappába: C:\TMGInstall\FPC.
4. Futtassuk a következő parancsot: `msiexec /a MS_FPC_Server.msi /p afrissitesneve.msp`
5. Indítsuk a telepítést ebből a mappából, az immár frissített fájlokkal³².

3.9.2 TARTOMÁNY VAGY MUNKACSOPORT?

Kerülgetjük már ezt a témát egy jó ideje³³, mivel muszáj volt már 1-2 esetben utalni rá, de most megpróbálom közös nevezőre hozni az érveket és az ellenérveket. Egy biztos, akárhogyan is volt korábban, a Microsoft ajánlása a TMG esetén a tartományi tagság, a Standard és az Enterprise kiadás esetén egyaránt. Ez persze nem azt jelenti, hogy nem oldható meg a tartományi tagság elhárítása, hanem szó szerint az hogy ez az ajánlás.

Ezekon a fórumokon tipikusan a konzervatív, "régi játékos" szakemberek érvelnek úgy, hogy a tartományi tagságon többet veszítünk mint nyerünk, hiszen ha a támadó leküzdötte adott esetben a TMG-t, akkor a tartomány erőforrásainak elérése már egyszerű feladat lesz. Nos, ez egy erősen vitatható megállapítás, amely abból indul ki, hogy a TMG-t kell megtörni. Pedig nem, és nem is ez a tipikus, hanem a TMG-n keresztüli behatolás, az alkalmazásszerverek felé. Hiszen ezek azok, amelyeket publikálunk és így elérhetővé tesszük, és így máris egy elvi előnyt adunk a nyilvános hálózatok felől érkező behatolási kísérleteknek³⁴.

³⁰ Az ARP IPv6-os verziója

³¹ Most már 2010 szeptember igen, a 13. fejezetben szó is lesz erről.

³² Ez hivatalosan nem támogatott egyelőre. (A lektor megjegyzése.)

³³ De ez még semmi, az ISA adminok hosszú évek óta vitáznak arról a különböző fórumokon, hogy melyik forgatókönyv az előnyösebb

³⁴ Abba már főképp ne menjünk bele, hogy a belső próbálkozások aránya kb. 2x akkora mint a külsőké.

Ezek után sorakoztassunk fel érveket mindkét verzió mellett és ellen, először a tartományi tagság jön:

Előnyök

- A tartomány eleve egy jól körbebástyázott zárt kör, bejáratott biztonsági megoldásokkal, és pl. olyan extrákkal mint a Csoportházirend, ami egy plusz helyzetelőnyt jelent a biztonsági vonalak meghúzásánál (is).
- Sokkal részletesebb kontroll a felhasználói hozzáférések elbírálásánál a meglévő tartományi fiókok és csoportok alapján a különböző proxy forgatókönyvekben (ez az érv egyébként amivel überelni lehet azt a kérdést is, hogy miért jobb egy ISA / TMG pl. egy közepes tudású hardveres tűzfalnál).
- A kliens tanúsítványok teljes körű támogatása, ez a hitelesítésnél sokat számíthat.
- Maradva a tanúsítványoknál: az Enterprise változatnál nem szükséges a tanúsítvány az EMS-hez (lásd 13. fejezet).
- A publikálásnál különböző kibővített lehetőségek használata, pl. a Kerberos hitelesítés delegálás.

Hátrányok:

- Ha a TMG szerverünk pl. a Perimeter hálózatban van, egy másik tűzfal előtt, akkor számos protokollt engedélyeznünk kell a tartományi kapcsolatok fenntartása miatt.

A munkacsoportos felállás előnyei:

- Ha a tűzfal mégis kompromittálódik, akkor a tartományi szolgáltatások nem.
- Fordítsuk meg: ha az Active Directory-t töri meg egy ráérő munkatársunk, akkor a tűzfalat nem fogja tudni, hiszen nincs a tartományban.

Hátrányok:

- Az összes a tartományban elérhető (és fentebb említett) megoldás és szolgáltatás nem használható. Nincs korrekt felhasználói hitelesítés és tanúsítványhasználat, nincs jól megtámogatott szerverpublikálás, csoportházirend és egyebek.
- A tűzfal kliensek hitelesítése lényegesen problémásabb.

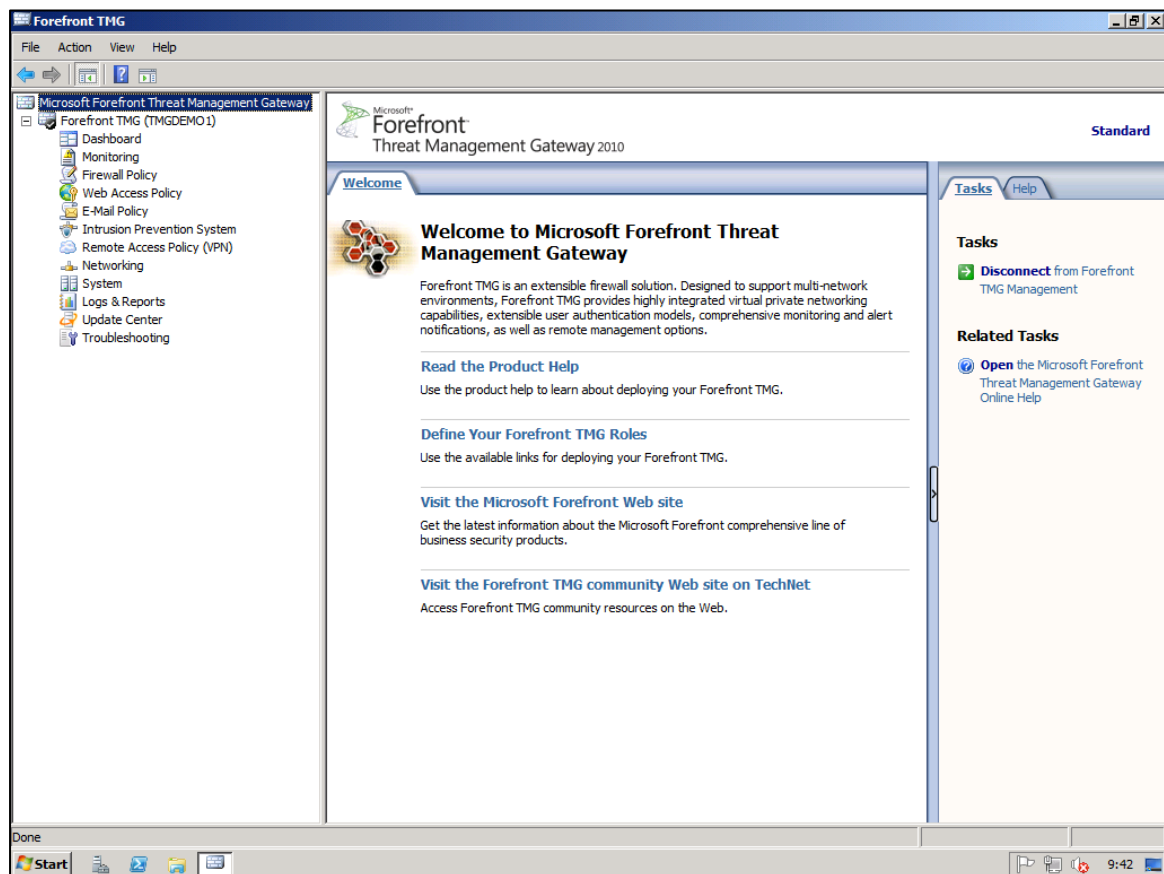
- A felhasználói adatbázis, amelyből táplálkozhatunk tipikusan (de a RADIUS és az LDAP azért jelen van) egy szimpla Windows OS felhasználói adatbázisának felel meg (gondoljunk arra, hogy mennyivel könnyebb egy lokális admin fiókot feltörni, mint egy tartományit).

Nos, ezek voltak az érvek és az ellenérvek, ám a döntés értelemszerűen mindig a helyi viszonyok és a helyi biztonsági házirend alapján történik, ergo szerencsére nem nekem kell itt és most megmondani a frankót.

4 VEGYÜK BIRTOKBA!

4.1 A KONZOL FELFEDEZÉSE

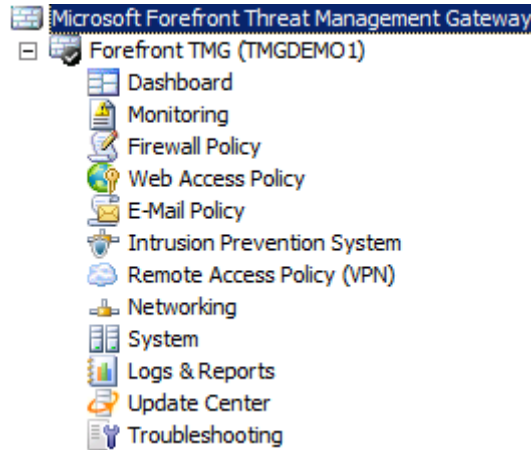
A konzol, azaz a felhasználói felület az egy olyan a hely, ahol az életünk jelentős részét töltjük. Ezért nagyon nem mindegy, hogy mennyire stabil, mennyire áll kézhez, mennyire nehéz kiismerni, és mennyire tér el mondjuk az előző verziónál megszokotthoz képest. Nos a TMG új konzolja kb. közepesen tér el az ISA-hoz képest, vannak új elágazások és vannak új helyre került komponensek, valamint el is tűnt néhány dolog a szokásos helyről, viszont azért sok-sok hasonlóság is van. Egy biztos, a kiismeréséhez nem kell úrhajós vizsga, pár nap és menni fog. No de nézzük sorban az indítókép alapján a felépítést.



4.1 ÁBRA A TELEPÍTÉS UTÁN EZ A KÉP FOGAD BENNÜNKET

Az ablak 3 részre oszlik, a baloldali faszervezetre (akár főmenünek is hívhatjuk, mert van ugyan egy menüsorunk is az ablak tetején, de nagyon ritkán használjuk), a középső az adott menüponthoz tartozó, tartalmi részre, míg az aktuális képen sokat nem mutató, de egyébként szintén rengeteget használt Task Pane-re.

Ha vetünk egy gyors pillantást a faszerkezetre, akkor az ISA négy, vagy egy idő után öt (a Troubleshooting pl. nem volt még meg az ISA 2004 RTM-ben), elágazásához képest itt rögvest 12 van. Ez adódik egyrészt az újdonságokból, másrészt a jobb tagoltság miatt van olyan ISA menüpont, amelyet 2 vagy akár 3 részre is szétszedtek, azért, hogy vertikálisan nem legyen nagyon sok a tartalom. Nézzük meg akkor ezeket is egyesével:



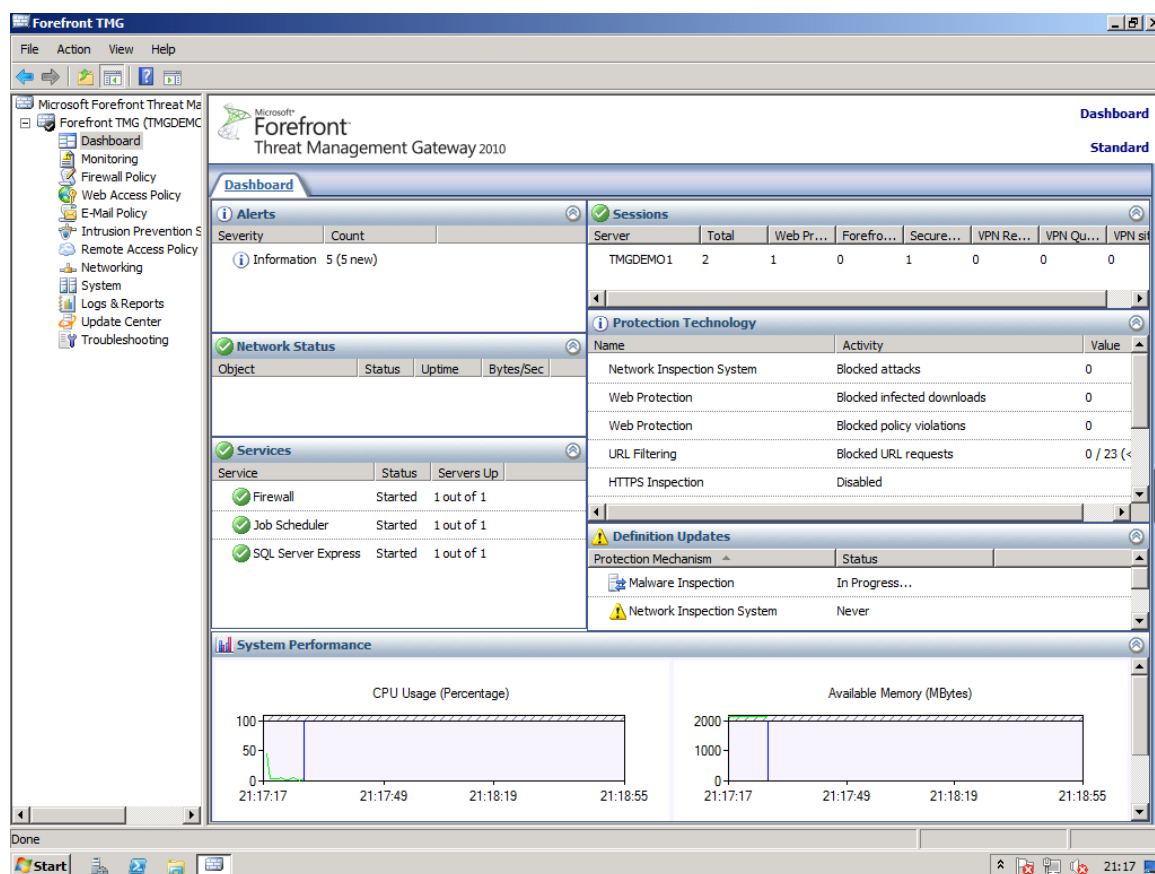
4.2 ÁBRA 3X ANNYI ÚTELÁGAZÁS MINT AZ ISA-BAN

A faszerkezet legtetején csak a különböző TMG példányokhoz kapcsolódást megvalósító Connect/Disconnect parancs található meg (magán a szerveren ez automatikusan megtörténik a telepítés utáni első indítástól számítva).

A szerver NetBIOS nevét is tartalmazó sorban már több minden elérhető, ezek a globális adminisztrációs műveletek, mint pl. az Export/Import, vagy az leválás az Enterprise hálózatról, illetve belépés egy TMG tömbbe. A szerverünk alapszintű jellemzői (Properties), ahol pl. majd a jogosultságokat is megtaláljuk.

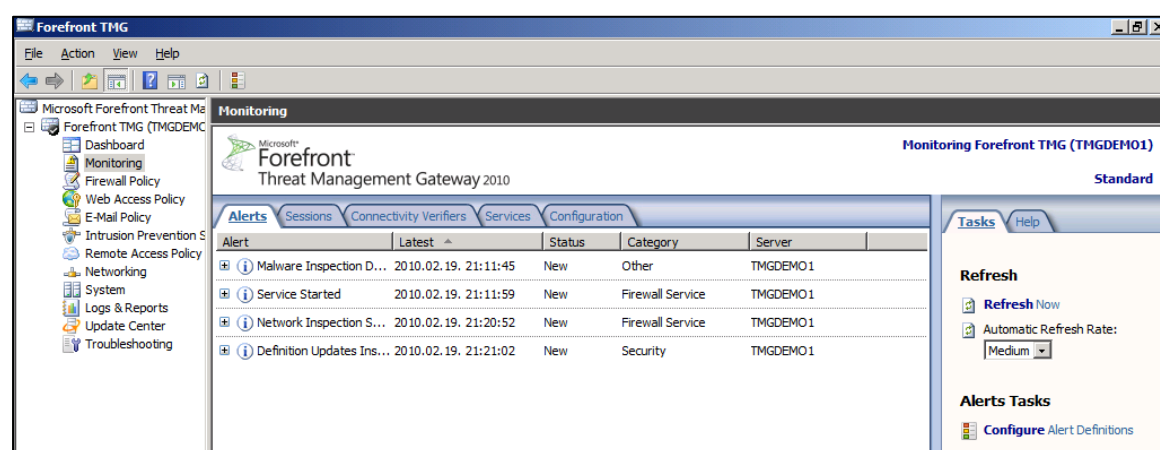
Leválás az Enterprise hálózatról, illetve belépés egy TMG tömbbe? Ez nem egy Standard változat? De. De van magyarázat, a 4.2-es fejezetben megkapjuk.

A következő elágazás egy képernyős ugyan, de tartalom az van benne bőven. Ez a Dashboard, azaz a "Műszerfal", ami az ISA-ban a Monitoring alatt volt, de itt már nem.



4.3 ÁBRA A MŰSZERFALUNK

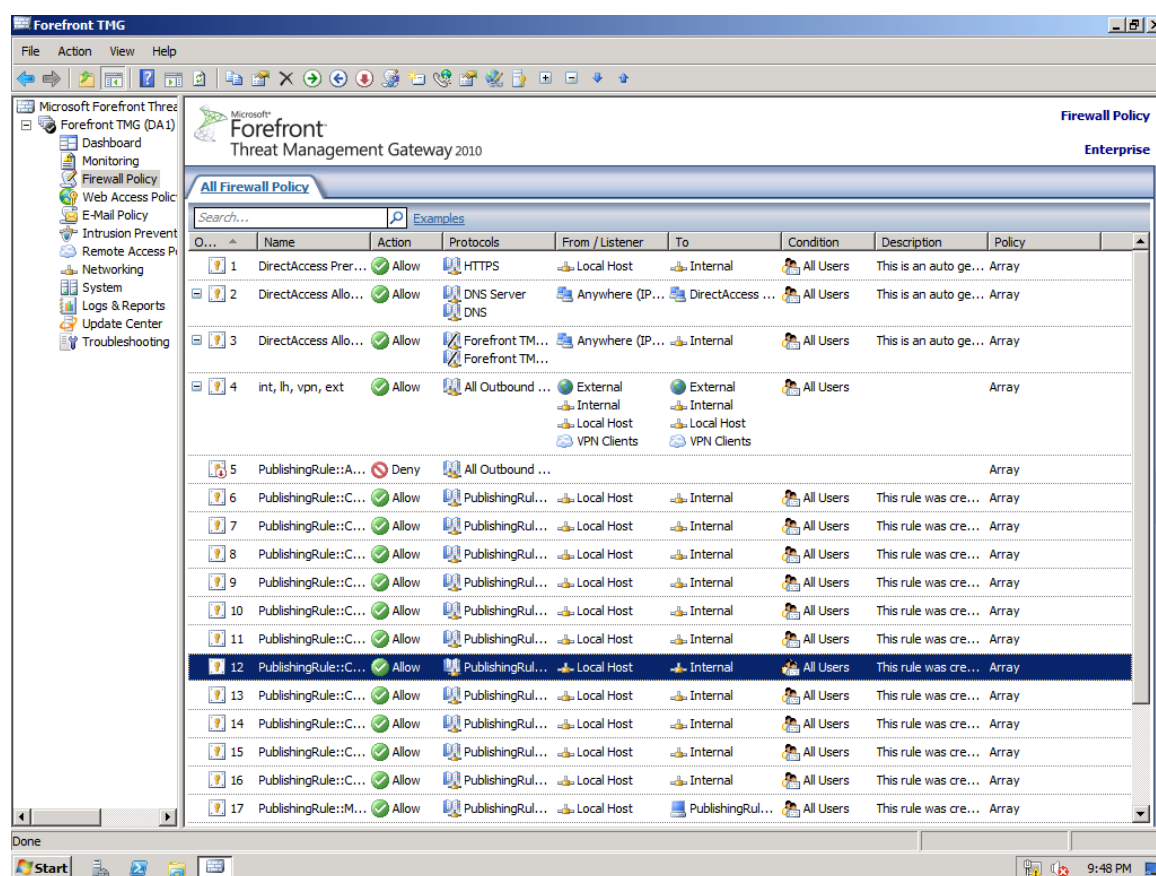
Ebben a riasztások, az aktuális session-ok, a hálózat, a TMG szervizek és a különböző adatbázisok (malware, NIS, spam) állapota, illetve némi statisztika, és egy kicsi teljesítmény ábrázolás (CPU, RAM) is látható. Ebből már kiderül szerintem, hogy ez nem egy interaktív szakasz, hanem elsősorban a passzív információszerzésre alkalmas.



4.4 ÁBRA AZ ÉG KÉK, A FŰ ZÖLD, A MONITORING MONITOROZ

Ha továbblépünk, akkor a kissé megkurtított Monitoring alá esünk be. A kurtítás oka egyrészt a Dashboard, másrészt az online napló és a jelentések elköltözése. De azért általános áttekintésre továbbra is megfelel ez a rész (az részleteket lásd a 12. fejezetben.)

A következő rész már igazi ínycsalat, ugyanis Firewall Policy az egyik legnépszerűbb és egyben legfontosabb hely is számunkra. Ennek megfelelően talán itt található meg a legtöbb beállítás, akár ha csak rákattintunk a nevére a jobb gombbal (pl. a "New" menüpont alatt az összes szerver publikálás típust megtaláljuk), vagy majd ha már feltöltöttük szabályokkal a szerverünket, akkor ezeket a középső keretben konfigurálhatjuk.



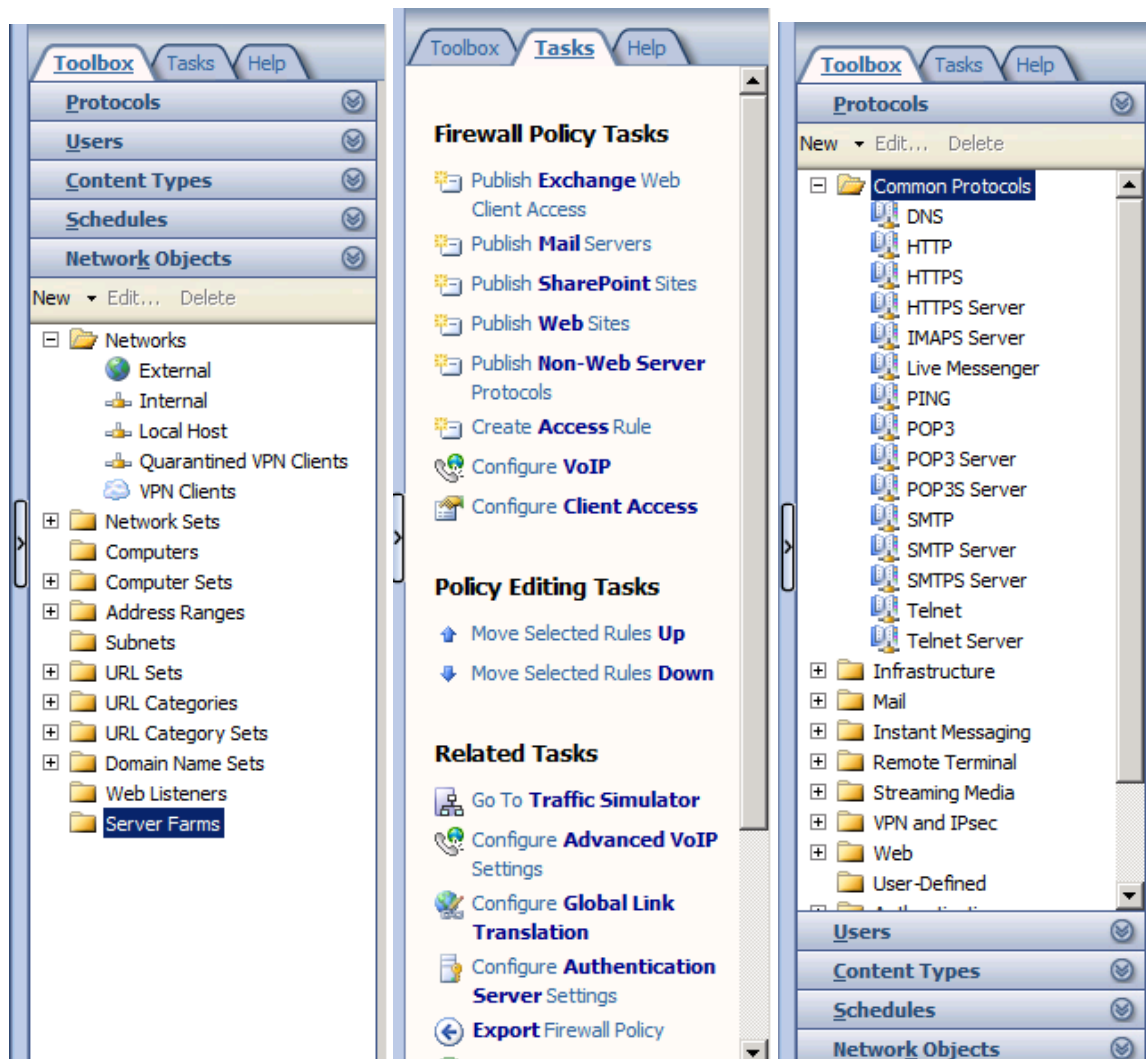
4.5 ÁBRA EGY UAG ALATTI TMG-T LÁTHATUNK, MERT SZERETTEM VOLNA SOK, DE NEM SZENZITÍV SZABÁLYT MUTATNI³⁵

De egy további lényeges helyre is felhívnám a figyelmet, és ez a jobb oldali keret, a Task Pane, amely most először mutatja ki a foga fehérjét, és nagyon sok foga van. Itt már három füle is van, a már eddig is látható Tasks (csak éppen rengeteg tartalommal), a

³⁵ Mint látható, a Task Pane-t becsuktam, ezt a félképernyő magasságában lévő speciális gombbal tudom összehozni, amely működés közben szépen animál, persze van aki gyűlöli ezt, pl. a kedves szerzőtársam ☺, és igaza is van, egy 256K-s vonal végéről várni erre már nem is akkora élvezet.

A KAPUN TÚL

szokásos Help, és a lényeg, a rengeteg, kategóriába szervezett objektum (ezeket használjuk a szabályok létrehozásánál), a Toolbox, azaz kb. egy szerszámoszláda.



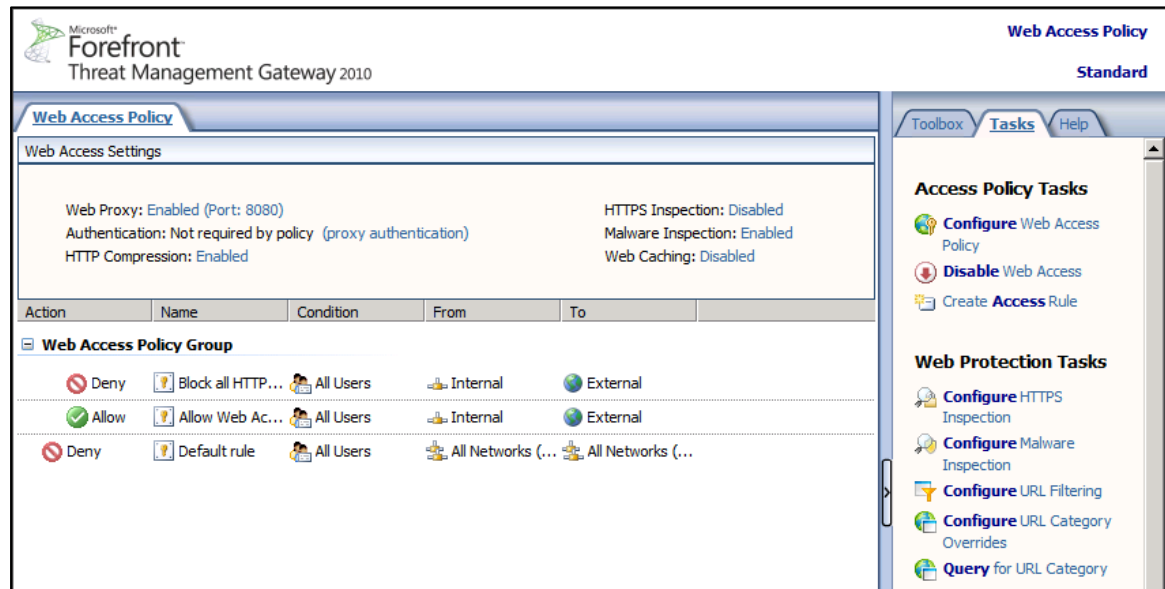
4.6 ÁBRA KÉT TOOLBOX RÉSZLET KÖZÖTT EGY TASKS - ÉS EZ MÉG NEM MINDEN

Nyugodtan nézegessük egy kicsit ezt az elágazást, ellenben én továbbmegyek. Méghozzá egy teljesen új pontba ami a Web Access Policy. Gyakorlatilag ez egy logikai csoportosítása azon tűzfalszabályok kiemelésére, amelyeknek köze van az elsődleges webes protokollokhoz (HTTP/HTTPS). És van még két újdonság, egyrészt a keresés opció a szabályok között, a másik pedig a szabályok csoportosíthatósága, ami egy nagyon kellemes újdonság, és amelyről már részletesen írtam a TechNet portálon.

Egy apró UI változás a TMG-ben

<http://www.microsoft.com/hun/technet/article/?id=7b4d9c93-0a5e-4d92-9760-23e21711bf5b>

Ez még úgy egyébként magában nem is minősülne nagy kunsztnak, na bumm, csoportosítunk, ám emellett a Web Access Settings részben található meg szinte az összes újdonság ami a webes forgalom szűrését, irányítását végzi majd az instrukcióink alapján. Ami innen kimarad, az meg az Action Pane lehetőségei között kapott helyet (mint például az URL szűrés).

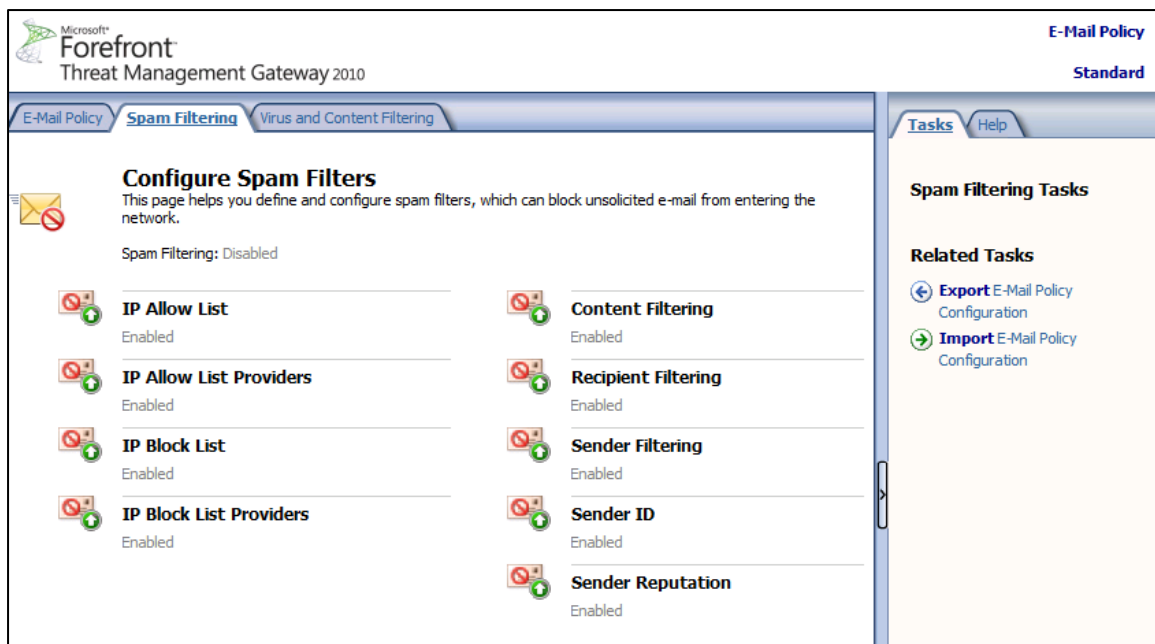


4.7 ÁBRA A WEB ACCESS POLICY-BAN LÁTSZIK A LEGTÖBB ÚJDONSÁG

Egyébként sem a Firewall, sem a Web Access Policy szakaszban nincsenek további fülek vízszintesen, de ez érthető, így is zsúfolt a képernyő. És most ragadnám meg az alkalmat arra, hogy az ISA rendszergazdáknak jelezzem, hogyha valamit nem találunk meg a faszervezetben, vagy a helyi menüben (jó példa erre a hajdanvolt Caching menüpont), akkor mindig nézzék meg az Action pane-ből, a Tasks tartalmát, biztosan ott lesz a keresett opció, vagy szolgáltatás.

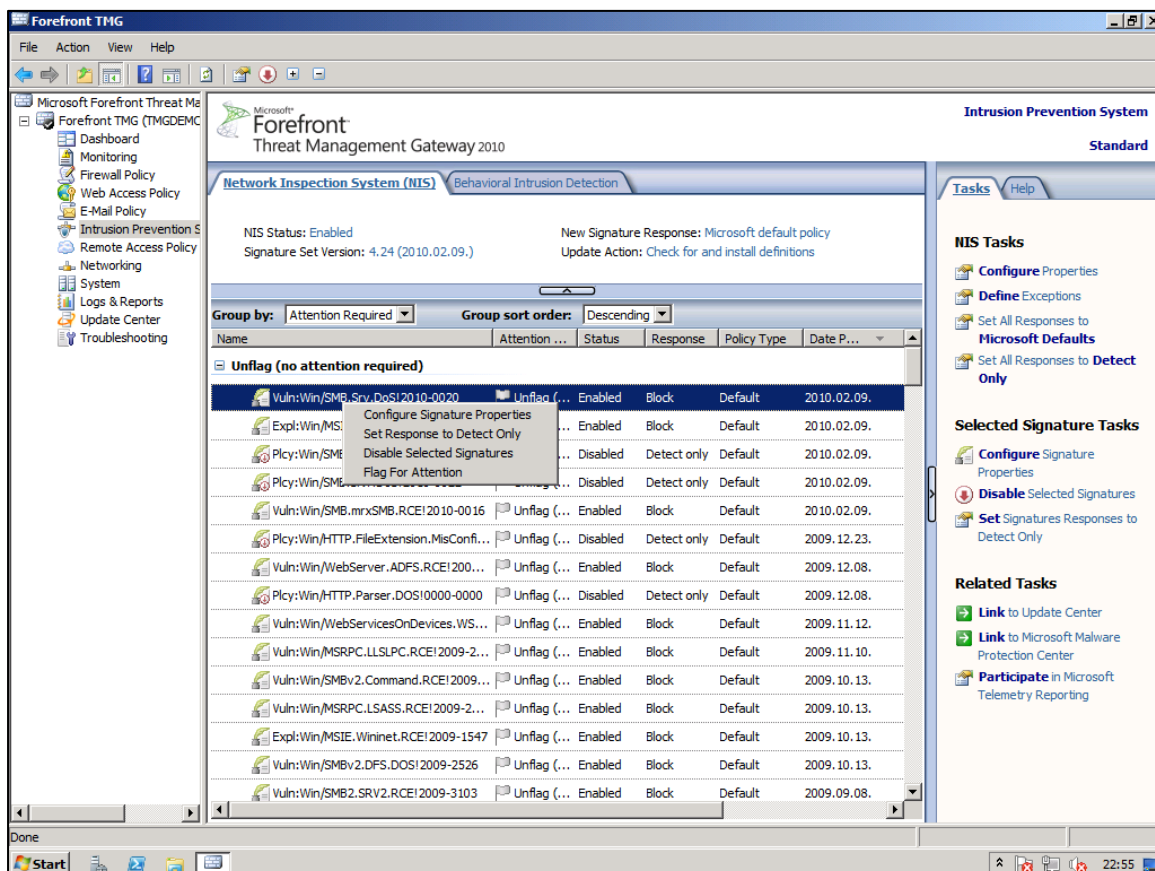
Haladjunk tovább.

Jöjjön az eddig szintén soha sem látott E-Mail Policy. A telepítés utáni alapállapotban a középső ablak első füle alatt semmit nem látunk, de ha pedig beizzítjuk az Exchange Edge szerepkört, vagy a Forefront Exchange-hez passzoló komponensét (Forefront Protection for Exchange Server), akkor a második és a harmadik fül (Spam Filtering, Vírus and Content Filtering) nemcsak színes-szagos lesz, hanem konfigurálható és működő.



4.8 ÁBRA EXCHANGE RENDSZERGAZDÁK FIGYELEM, ISMERŐS?

Biztos nehéz egyszerre ennyi újdonsággal szembesülni, pedig ez még csak a felület, és még nincs is vége, ugyanis a faszervezet középső része erősen innovatív.

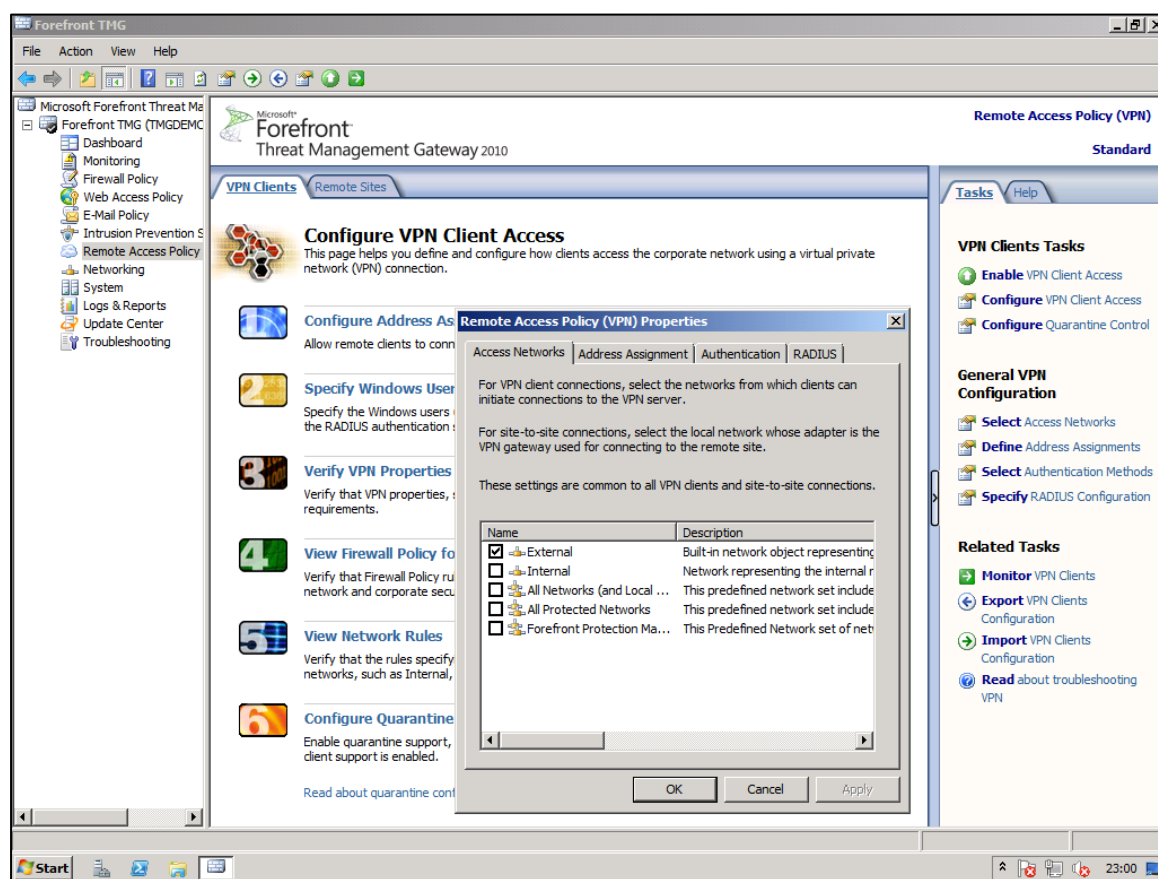


4.9 ÁBRA A NIS EGY ÜTŐS ÚJDONSÁG

A következő elem, az Intrusion Prevention System a TMG tűzfal komponensének egyik figyelemre méltó újdonságát tartalmazza. Ez a NIS (Network Inspection System), amely részleteit a 6.1-es fejezetben taglaljuk. Ha már frissítettük legalább egyszer a NIS-t (lásd később), akkor a középső ablakban a TMG számára ismert és felhasználható sérülékenységek listáját látjuk.

A NIS mellett láthatunk egy második fület is, ami viszont sokaknak ismerős lesz, ez a Behavioral Intrusion Detection, amely a Flood Mitigation Settings-et, az IP szűrést, és a szokásos Intrusion Detection beállításokat tartalmazza. Ezeket eddig az ISA-ban a General\Additional Security Policy elágazásban találtuk meg.

Most is egy ismerős rész jön a korábban az ISA-t ütügetőknek, bár a neve azért új: Remote Access Policy.

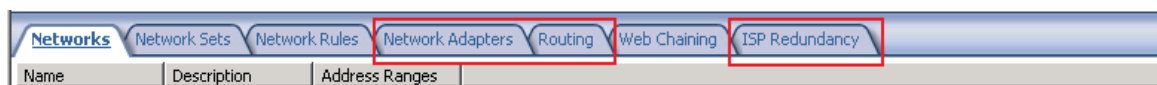


4.10 ÁBRA A REMOTE ACCESS POLICY CSAK EGY KICSIT TÖBB MINT A VIRTUAL PRIVATE NETWORK

Két fül van, egy a szóló VPN kapcsolatok számára, egy pedig a Site-to-SiteVPN (pl. telephelyek közötti VPN) kapcsolatoknak. Az 1-6-ig tartó színes, szagos ikonok számozástól ne várjunk sokat, gyakorlatilag az 1-3-ig tartó rész az alap VPN panel beállítására mutat, a többi meg más ismert részekre (Firewall Policy, Network Rules és a VPN karantén).

A KAPUN TÚL

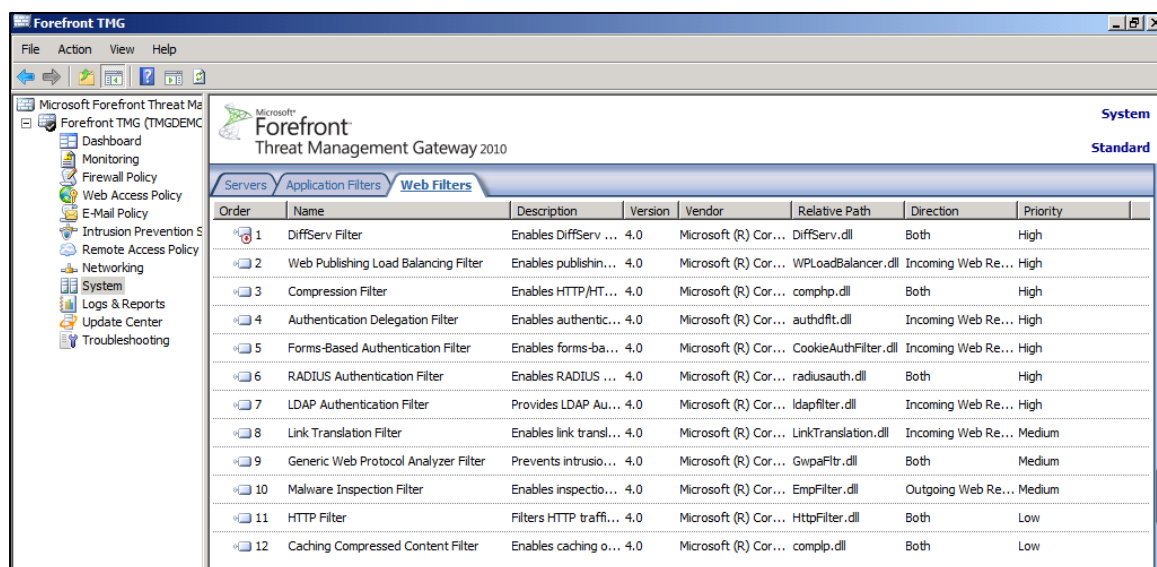
A Networking elágazás sűrű mint a januári kód Lajosmizsénél. 7 darab fül van, ez rekord a TMG-n belül, és bár ebből van ismerős is, de pl. a pirossal jelöltek nem.



4.11 ÁBRA A 4-BŐL 7 LETT

Ezekről a hálózatos fülekről (főképp az elejéről) rengeteget fogok beszélni a következő nagy fejezetben, addig is elégedjünk meg azzal, hogy a Network Adapters alatt a hálózati kártyáink alapbeállításait találjuk, a Routing alatt a gépünk route tábláját (amelyet kiegészíthetünk itt is manuálisan további route bejegyzésekkel, amelyeket úgy hívunk, hogy Network Topology Routes). Valamint abban az esetben ha két internet elérésünk van, akkor az utolsó fül alatt sokat fogunk varázsolni, hogy egy terheléelosztós (Load Balancing), vagy éppen a feladat-átvételes (Failover) konfigurációt összehozzunk.

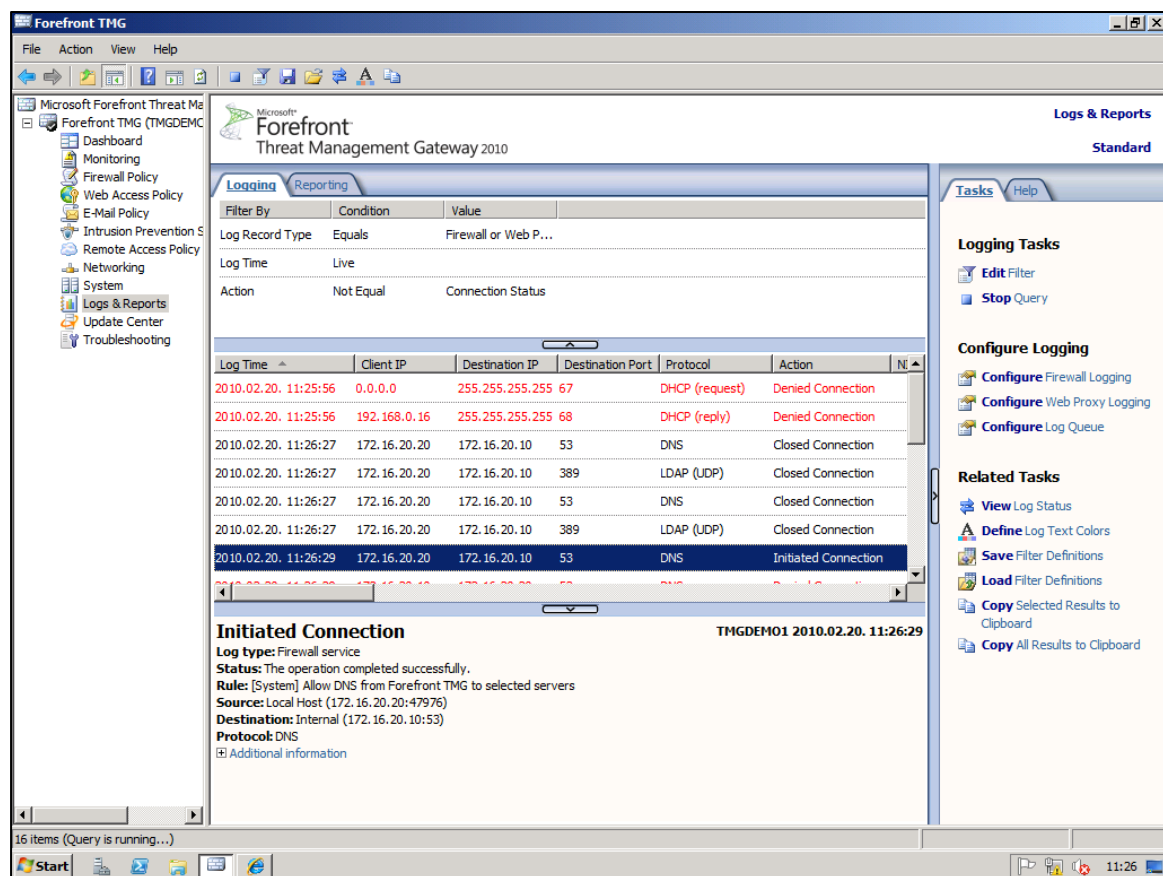
A System teljesen új elágazás a TMG-ben, de mindjárt meglátjuk, hogy tartalomra nem annyira. Három része van, a Servers, amely adminisztrációs alapadatokat tartalmazza³⁶, illetve itt található az Enterprise változatra történő áttérés egyszerű lehetősége is, azaz csak a megfelelő kulcsot kell beírunk ehhez és készen vagyunk. A második és a harmadik fülön az ISA Configuration/Add-Ins szakasz tartalma található meg, azaz a szintén nagyon fontos alkalmazás és web filterek.



4.12 ÁBRA SZÜRŐ SZÜRŐ HÁTÁN

³⁶ De pl. itt van elrejtve az Enterprise változatra történő frissítés lehetősége is – amire reinstall nélkül sort keríthetünk.

Már nincs sok hátra, de tartsunk ki, mert van még fontos rész. A Monitoring szakaszból kiszakadt Logs & Reports tartalmazza a realtime naplót³⁷, illetve a jelentések beállításának, generálásának, időzítésének részleteit. Mindkettő kulcsfontosságú, ám az első kiemelkedően, ez a TMG admin egyik legjobb barátja, azaz ha valami forgalmi, jogosultsági, működésbeli problémába ütközünk és ennek kinyomozására van szükség, akkor ide jöhetünk bátran, a szemünk előtt fognak pörögni a történések, amelyeket majd jól megszűrve, akár villámgyorsan is rájöhetünk egy probléma okára. A jelentések pedig napokra, hetekre, hónapokra visszatekintve adnak granuláris részletességű információt a rendszer illetve pl. az internet használatról.



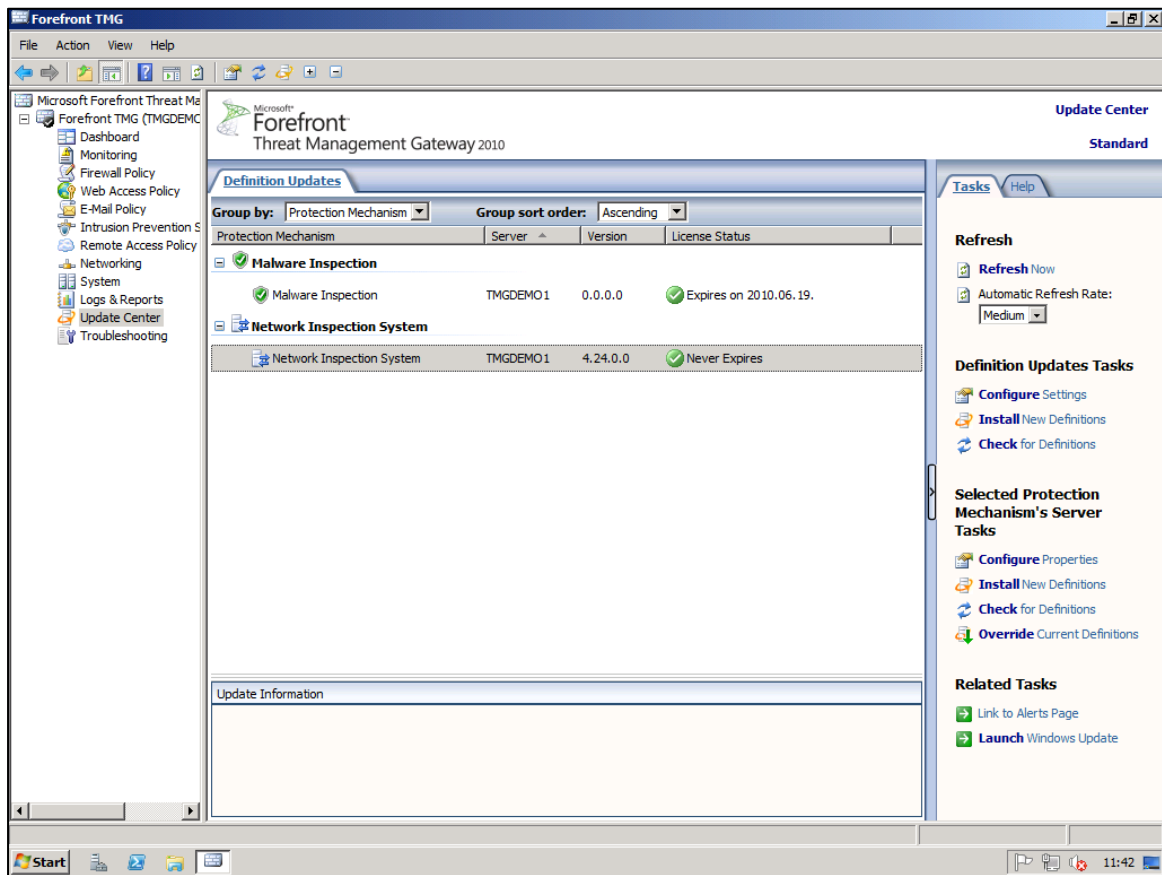
4.13 ÁBRA A PIROS JELENTHET JÓT ÉS ROSSZAT EGYARÁNT

Az Update Center-t már említettem és fogom is még párszor mert több komponens működését is érinti. Itt találhatóak, egy helyre összefogva a különböző olyan szolgáltatásokhoz tartozó adatbázisok frissítési lehetőségei, amelyeket – előfizetés birtokában – ténylegesen frissíthetünk a Microsoft Update szerverekről, vagy adott esetben a WSUS-unkról. A következő képen látszik, hogy a demó szerveremen a e-mailekre vonatkozó spam és vírusfrissítés nálam még nincs beélesítve, ezért nyilván az

³⁷ Nem ez a hivatalos neve, de én így hívom.

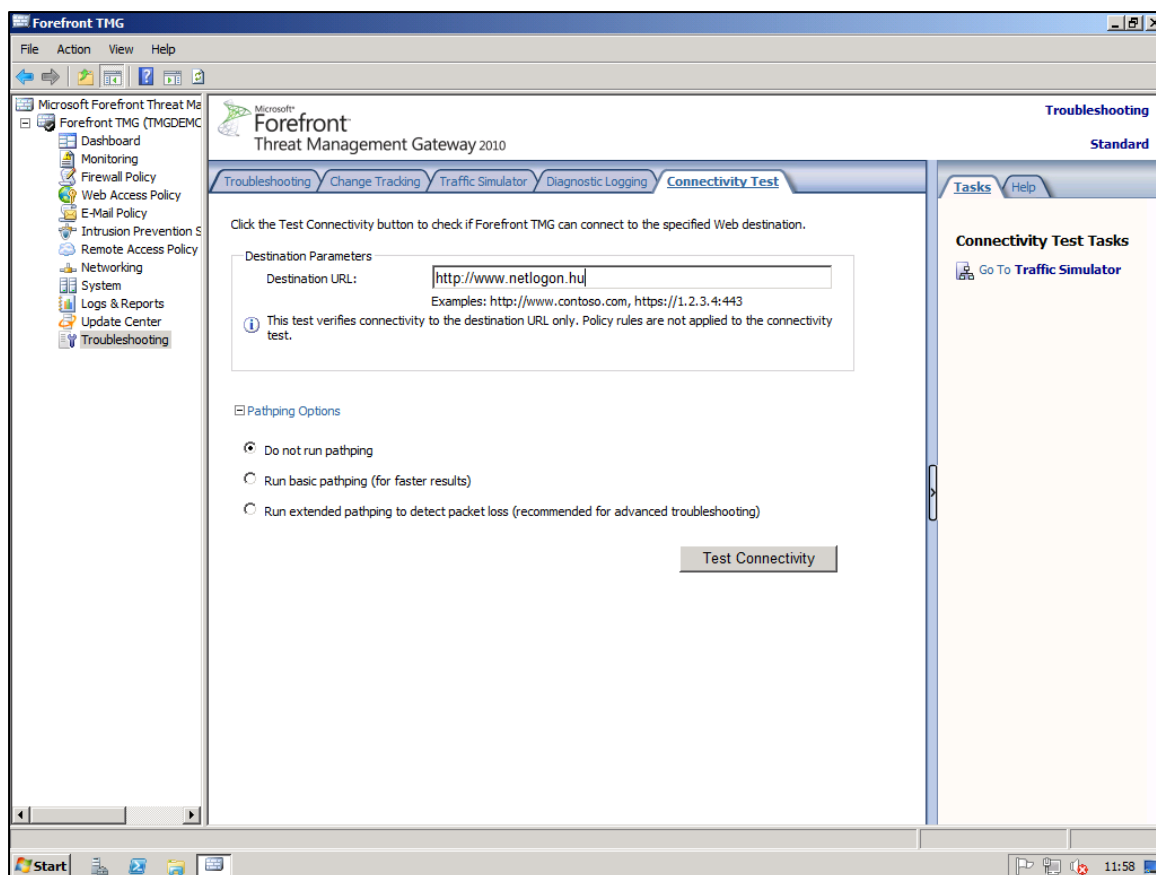
A KAPUN TÚL

adatbázisaikat sem frissíthetem, viszont a Malware védelem és a NIS igen. Ami még szót érdemel, az a Task Pane, ahol szépen ki van vezetve az összes lehetséges opció.



4.14 ÁBRA AZ EGYIK FRISS, A MÁSIK PONT MOST FRISSÜL

Elérkeztünk a faszerkezet utolsó eleméhez, amely nevében hordozza a funkcióját, ez pedig a Troubleshooting, azaz a hibakeresés (angolul mennyivel képletesebb e név). Az ISA 2006 SP1-ből sok-sok ismerős lesz itt, és bár az első oldal csak a tippek, linkek és a többi fül tartalmának ismertetése, azért a többi valós lehetőségeket tartalmaz. Az 5 fülből egy a Monitoring-ból jön (Change Tracking), három már az ISA-ban is itt volt, és van egy teljesen új is, a Connectivity Test.



4.15 ÁBRA ÉL, VAGY ÉL?

Ezzel a sor (a faszerkezet) végére értünk, időnként több volt ez mint egy szimpla UI leírás, de nyilván kevesebb is. De a passzoló fejezetekben nyilván nem mulasztom majd el az ott és akkor aktuális, a felülettel kapcsolatos praktikus információk közlését.

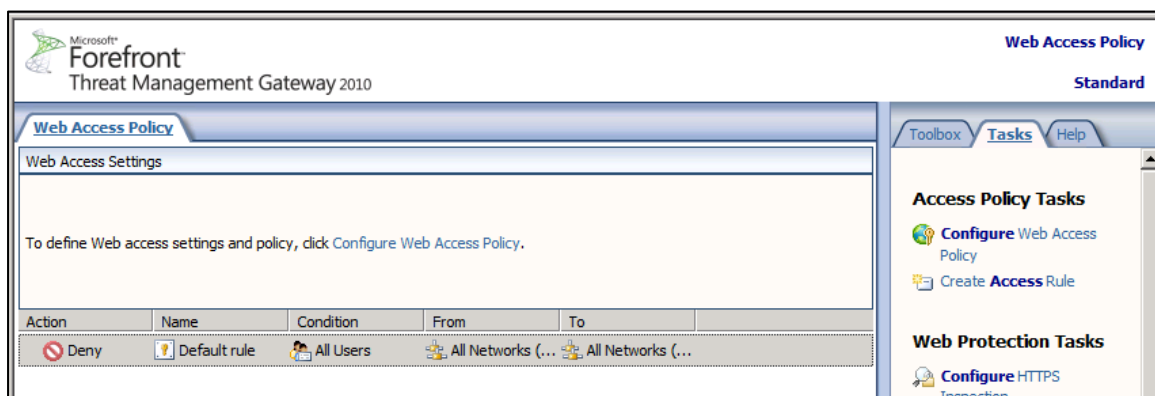
4.2 AZ ÚJ VARÁZSLÓK

Kötelességemnek érzem, hogy erről a témáról is beszámoljak, mert ugyan én általában nem szeretek varázslókat használni, de itt muszáj, mert van amit máshogy nem is lehet. konfigurálni, legalábbis indításképp. Meg aztán annak, akinek még nincs rutinja (mindenki így kezd) óriási segítség akár 1-2 segítő mondat, vagy az, hogy adott esetben konkrétan milyen opciókat választhat, vagy ami még jobb: melyeket nem. Szóval pár sorban csak emlékezzünk meg az új, a TMG-ben bevezetésre kerülő varázslókról (mindamelllett, hogy a régi ismerősökről is lesz még szó bőven).

1. **Web Access Policy varázsló:** erről már volt szó, mivel a Getting Started varázsló részeként is működhet. Végig is a Getting Started-en a telepítés részeként, azonban akkor az utolsó részt, azaz a Web Access Policy varázslót kihagytuk. Márpedig, amíg ezt nem tesszük meg, akkor pl. az előző részben megismert Web Access Settings alatt nem látszanak a lehetőségek.

A KAPUN TÚL

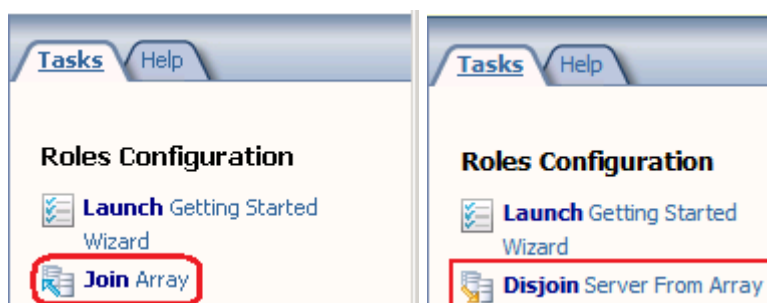
A Getting Started varázslót később is elérhetjük a faszerkezetben a szerver nevére kattintva és a Task Pane-ből kiválasztva, de gyakorlatilag nem lesz rá szükség. Ha pl. kieszdjük a TMG gépet a tartományból, akkor a változás a konfigurban automatikusan megtörténik.



4.16 ÁBRA VARÁZSOLNI, VAGY NEM VARÁZSOLNI – EZ NEM KÉRDÉS

Szóval ezt a varázslót egyszer végig kell csinálnunk, legalábbis akkor, ha nem rögtön egy importtal kezdjük a TMG használatát. A varázslói lépések között érintjük az URL szűrést, a Malware és a HTTPS vizsgálat beállításait, és egyszerűen létrehozhatunk egy alapértelmezett cache szabályt.

2. **Join Array varázsló:** szintén volt már szó érintőlegesen erről, és mivel a Standard kiadás része, ezért most kell beszélnünk róla. De milyen tömb ez, ha mi most a Standard verzióval küzdünk? Egyszerű, a TMG kisebb változata ugyanis csatlakoztatható egy (általában csak az Enterprise változatnál működő) EMS-hez (Enterprise Management Server), újratelepítés nélkül.

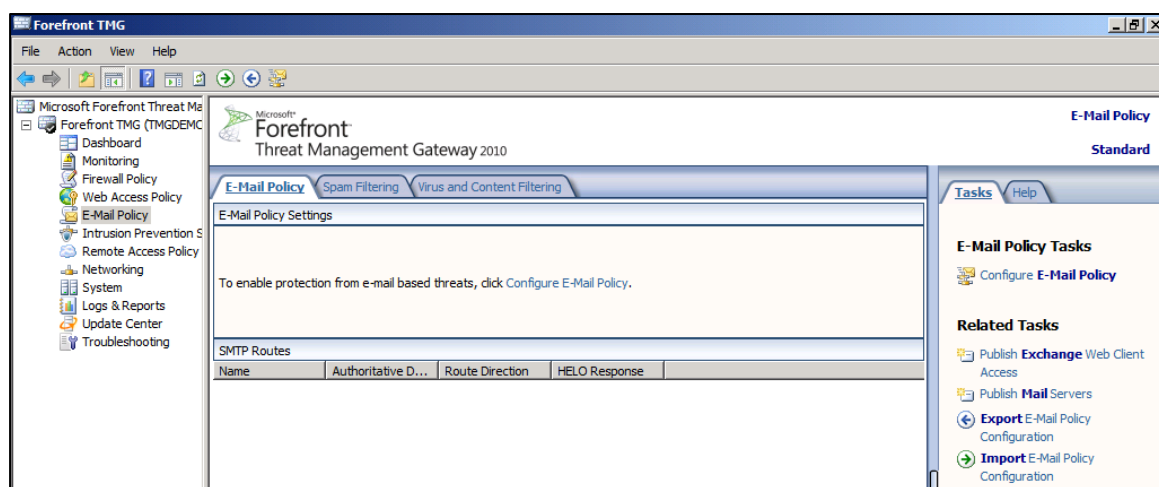


4.17 A TÖMBÖSÍTÉS ONNAN INDUL, AHONNAN A GETTING STARTED

3. **Configure SIP varázsló:** A Firewall Policy szakaszból érhető el (Tasks / Configure VoIP), és ezzel engedélyezhetjük a TMG-n a SIP (Session Initiation Protocol) forgalom használatát, eldöntve hogy pl. közvetlen vagy indirekt kapcsolódásról lesz szó, illetve egyébeket is. Ha már itt tartunk, ezen a ponton (Tasks) lejjebb

találunk még más VoIP-re vonatkozó beállításokat (Configure Advanced VoIP Settings).

4. **Configure E-Mail Policy varázsló:** Értelmszerűen az E-Mail Policy szakaszban találjuk, és SMTP route-okat gyárthatunk vele, azaz definiálhatjuk az SMTP külső és belső listener-eket (még nem tudhatunk róla, de fogjuk fel a listenert egy olyan fülként, amelyen a TMG "hallgatózik"), az autoritativ e-mail tartományok neveit. Mindez azért történik, hogy aztán a varázsló vége felé engedélyezhessük a spam és víruszűrést³⁸.



4.18 ÁBRA A CONFIGURE E-MAIL POLICY VARÁZSLÓ LELŐHELYE

5. **Enable ISP Redundancy varázsló:** Ezzel zárjuk a sort, a Networking részben található, és ahogyan korábban említettem, egy terheléelosztásos (Load Balancing), vagy éppen a feladat-átvételes (Failover) módszert ad a kezünkbe két internet hozzáférés kombinálására (lásd következő nagy fejezet).

4.3 HOGYAN LESZEL TMG ADMIN A SAJÁT GÉPEDEN?

Könnyedén. Inkább a miért a kérdés. De az sem feltétlenül. Ugyanis nincs mindig lehetőség RDP-n kapcsolódni a TMG-hez. Meg aztán egy fizikai hálózaton illetve egy tartományon belül nem is biztos, hogy van értelme, mivel teljesítményt és sávszélességet takarítunk vele, ha a konzol a mi gépünkön fut, és a szokásos távoli MMC módszerrel érjük el a szerveret. Ehhez három dolgot kell megtennünk, nézzük sorban ezeket:

1. Telepítés: A konzol telepítése ugyanúgy kezdődik ahogy a szerveré, mind a Prep Tool, mind a telepítő megkérdezi hogy mit szeretnénk majd használni, és ha

³⁸ Na persze az Exchange Edge vagy a Forefront Protection Manager for Exchange komponensekre még szükség lesz ezek működéséhez

csak a Management Console-t választjuk, akkor ennek megfelelően pakolgatja fel mindkét segédeszköz a szükséges holmikat a gépünkre. De azért van egy jelentős különbség, ugyanis a konzolnak 32 bites telepítője is van.

A telepítő DVD-n ez nincs ugyan rajta, viszont letölthető a Microsoft Download Centerből (egy Passport-os regisztráció után) a 203 MByte-os TMG_ENU_Management_x86.exe nevű csomag. Ha 32 bites OS-ünk van, akkor ezt telepítsük fel a rendszergazdai munkaállomásra.

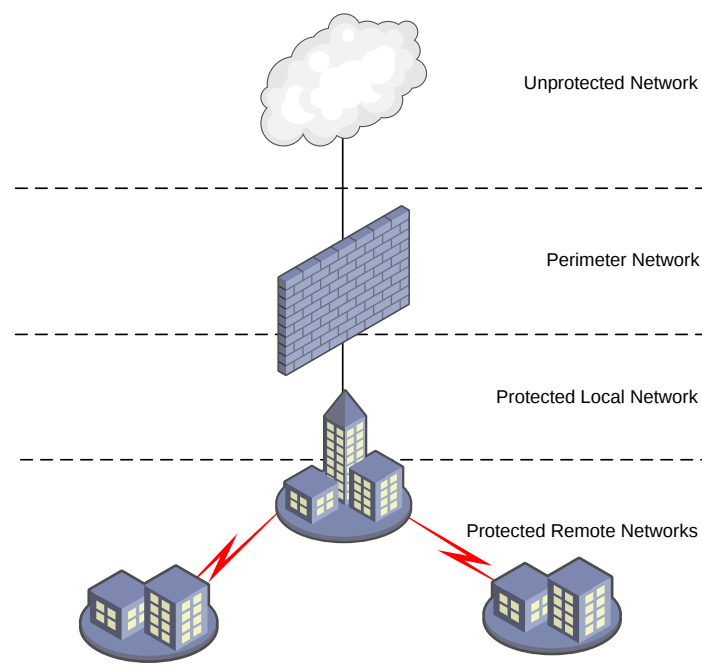
2. Ezután ha elindítjuk a TMG konzolt a gépünkről, akkor egy csúnya Access Denied üzenetbe fogunk futni, ugyanis legalább két helyen még engedélyeznünk kell a hozzáférést. Az első az ún. System Policy (lásd következő fejezet) ahol engedélyezzük a gépünk IP-jét az MMC elérésénél, azaz kerüljön be valahogy ez az IP a Remote Management Computers csoportba, ami alapértelmezés szerint mind az RDP, mind az MMC elérést lehetővé teszi.
3. Ha ez is kész, nézzük meg, hogy van-e jogunk is a TMG-t elérni, azaz a szerveren nézünk be a tulajdonságainál az Assign Roles alá, és ha itt van olyan csoport amelynek tagjai vagyunk, akkor akkor mehet a 32 vagy a 64 bites kliensről is egyaránt a csatlakozás.

A 32 bites Forefront TMG Management MMC telepítőjének letöltése
<http://www.microsoft.com/downloads/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&displaylang=en>

5 A TŰZFAL

5.1 AZ ALAPOK ÉS NÉMI TÖRTÉNELEM

Sokszor elhangzott már a tűzfal szó, de nem mindig pontosan arra utalt, mint ahogyan ebben a fejezetben tárgyaljuk majd. A hétköznapiakban is sokszor használjuk ezt a szót az egész ISA-ra, vagy TMG-re, pedig ahogyan már kapisgálhatjuk az eddigiekből, sokkal több ennél, de mégis, valószínűleg ez a legmarkánsabb megfelelés, ez a legjobb (rövid) jelző. A tűzfalak működésének lényege viszonylag egyszerűen összefoglalható: a lehető legteljesebb körű forgalom ellenőrzés és szűrés, két vagy több kommunikáló fél között. A hálózatbiztonság ezen szereplői egy-két évtizedes történetükben³⁹ komoly evolúciós fejlődésen mentek át. Azért utaltam az evolúcióra, mert nyilvánvalóan a kihívások (mint pl. a legnagyobb nyilvános hálózat, azaz az Internet), jelentősen hatottak és hatnak ma is a védekező típusú megoldások fejlődési irányára. A következő rövid áttekintésben én a Microsoft tűzfal termékein keresztül szeretném bemutatni a generációs különbségeket illetve az ezekkel együtt járó szűrés típusokat, ami nem biztos, hogy tökéletes mintavétel (és biztos hogy nem a legátfogóbb), viszont egy egyszerű szemléltetésre azért alkalmas.



5.1 ÁBRA A TŰZFAL MÖGÖTT MINDEN HÁLÓZAT VÉDETT

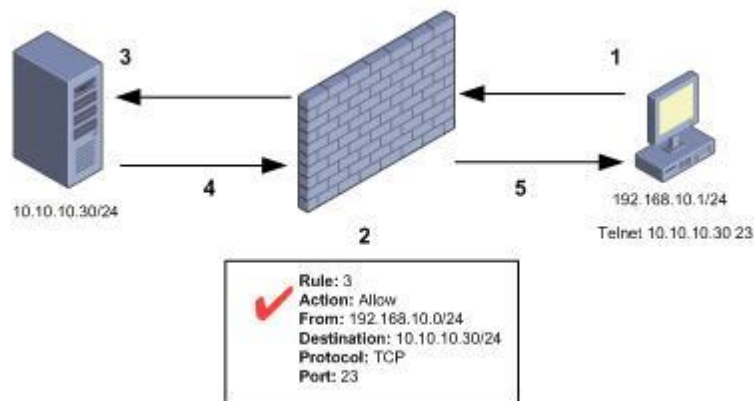
³⁹ 2000 októberére datálódik az első RFC dokumentum (RFC 2979) az internetes tűzfalak működésével szemben támasztott elvárásokról, ami persze nem azt jelenti, hogy előtte nem léteztek

5.1.1 A CSOMAGSZŰRÉS

A tűzfalak első generációs fő megoldása az ún. csomagszűrés (packet filtering), amelyet pl. az első ISA kiszolgálóban is megtalálhattunk (és egyébként máshol már úgy kb. a 80-as évek végétől fellelhető volt), mint alap üzemmódot. Ez gyakorlatilag az IP (vagy internet) és a transzport rétegben történő csomagok engedélyezését, vagy tiltását jelenti nagyjából az általunk definiált szabályok illetve némi automatizmus alapján. Amikor a tűzfal ezt a módszert használja, akkor csak az IP csomagok fejléceit vizsgálja, ezen belül a forrás és cél információt, az irányt, valamint protokoll és a port értékeket. Ezeket bontsuk ki kicsit:

1. Cél cím (Destination Address): A forgalom céljának számítógép címe, ez a hálózataink viszonyától függően lehet pl. a TMG szerverünk külső, publikus címe (NAT esetén), vagy pl. a TMG-n definiált két belső hálózat és egy szimpla route esetén az egyik hálózatban lévő számítógép címe.
2. Forrás cím (Source Address): Ezt most már egyszerűbb lesz megérteni, ugyanúgy lehetséges egy publikus cím is, mint ahogyan egy privát, a lényeg, hogy a kezdeményező címe lesz ez.
3. Az IP protokoll és a száma: Csomagszűrőt definiálhatunk tetszőlegesen a TCP, az UDP vagy akár az ICMP számára is. A számuk az azonosítójuk, mondjuk a TCP esetén a 6, míg a speciális, és időnként a hálózati eszközökben gondot okozó GRE (Generic Route Encapsulation, ez ugye a PPTP VPN alap protokollja) esetén a 47-es.
4. Irány (Direction): A csomag iránya a tűzfal szempontjából. Lehetséges értékek a bejövő (inbound), a kimenő (outbound), ám adott esetben (pl. az UDP-nél, vagy akár az FTP-nél) a Receive only, Send only megjelölésekkel is összefuthatunk.
5. A port száma (Port numbers): A TCP és az UDP csomagszűrésben helyi és távoli port számoknak kell szerepelni, ebből a helyi általában egy 1024 feletti bármilyen magas port szám lehet, míg a távoli az egy fix, és közzismert port lesz (pl. TCP 80 a HTTP-hez, vagy a TCP 23 a Telnet-hez). Mindkét portszám típus lehet fix értékű, vagy dinamikus.

A csomagszűrés folyamatához az alábbi ábra illetve az ábra alatti magyarázat ad segítséget. De még előtte, nem árt tudnunk azt, hogy az ISA 2004-től kezdve mi nem direktben csomagszűrőket definiálunk, hanem tűzfal szabályokat (lásd két fejezet múlva), amelyek alapján a tűzfalunk csomagszűrőkkel érvényesíti az akaratunkat.



5.2 ÁBRA A CSOMAGSZŰRÉS EGYSZERŰ, MINT A FAÉK

1. A kliensünk egy telnet-tel próbál kapcsolódni próbál a cél címhez, de ehhez először a tűzfalhoz lesz muszáj folyamodnia.
2. A csomagszűrő üzemmódban működő tűzfal megvizsgálja a kérést, azaz összehasonlítja a konfigurációjában található szabályokkal (vagy inkább egy hozzáférési listával, lásd ACL).
3. Ha a forgalom megengedettnek minősül, akkor a kérés a cél címen lévő cím felé továbbítódik.
4. A cél címen fellelhető gép válasza elindul a kérő felé.
5. A csomagszűrő tűzfal újra felvonja a szemöldökét, és újra megvizsgálja a feltételeket, és ha mindent rendben talál, akkor továbbít.

Beszéltem néhány automatizmusról az elején, valóban van ilyesmi, ide tartozik pl. az ún. ingress és egress szűrő. Az elsőként említett a külső interfészen blokkol minden olyan kapcsolódási kísérletet, amelynek a forrás címe elvileg a belső hálózatunkhoz tartozna, hiszen ez normális esetben nem lehetséges. Az egress szűrő pedig azt nem engedi meg, hogy egy olyan csomag hagyja el a hálózatunkat, amelynek a forráscíme nem egyezik meg az általunk használt cím tartományokkal.

A csomagszűrés egyszerűsége mellett egy további előny, hogy mivel csak a IP és a transzport rétegben működik, és csak a fejléceket vizsgálja meg, ezért nagyon gyors.

No de nemcsak előnyei vannak, nézzük a hátrányokat is:

6. A csomagszűrő általában véve nem egy úrhajó, komplex protollokat, összetett folyamatokat, nyomon követést képtelen ellátni.
7. Abszolút nincs alkalmazás-érzékenység. Ha a támadó meg tudja oldani, pl. hogy a mi hálózatunkban futó Telnet szerver a 80-as porton fusson, akkor a 23-as klasszikus Telnet port tiltása fabatkát sem ér.

8. A csomagszűrő nem képes tiltani az IP address spoofing-ot, azaz a forrás IP megbízhatóként feltüntetését, azaz egy megbízható címre cserélését.
9. A source-routing információ hamisításától, azaz a csomag elterelésétől sem véd meg a csomagszűrő.
10. Az IP fragmentálás tiltása sem megoldható. Mivel a legtöbb csomagszűrő tipikusan csak a csomag első szakaszát ellenőrzi, ha egy szétdarabolt, és a későbbi darabokban ártó tartalmat akarunk átpasszirozni a csomagszűrőn, akkor ezt simán megtörténhet.

5.1.2 AZ ÁLLAPOTTARTÓ-VIZSGÁLAT (ÉS SZÜRÉS)

A következő generációs, azaz a *circuit-level* néven emlegetett tűzfalak legerősebb ütőkártyája az ún. stateful packet inspection, azaz az állapottartó-vizsgálat. Kiindulva a szimpla csomagszűrő gyengeségeiből, ez a típus már nemcsak a fejléc információkat, hanem a tartalmat is vizsgálja és ami még ennél is fontosabb az az, hogy a csomagokkal kapcsolatos állapotinformációkat is tárolja. Azaz lehetővé válik a nyomon követés, az összetartozó forgalom együttes elemzése illetve szűrése is. Tömören: egy a külső interfészen válaszként megjelenő csomag esetében például mindig kideríthető, hogy az valóban egy válasz-e egy korábbi kérésre. Ha nem, akkor eldobandó, hiszen egy válasz csak egy kérésére érkezhethet normális esetben.

További előnye ennek a megoldásnak, az hogy szemben a packet filter típusú eszközökkel a válasz csomagok engedélyezésére nincs szükség, ami egy nagy áttörés számít a tűzfal technológiában.

Kicsit tudományosabban:

1. Egy TCP session esetében az engedélyezéshez (vagy a blokkoláshoz) a tűzfal információkat tárol az adott session állapotáról.
2. A TCP forgalom elején egy speciális ellenőrzés történik a felek között, amelyet "háromujjas kézrázásnak" (three-way handshake) hívunk, és amely módszer lényege, hogy a forgalomban résztvevő kliens és a szerver (kivételesen nem az OS-re értem ezt most) SYN és ACK flag-ek értékével játszva, kölcsönösen elhiszik a másiktól, hogy az akinek mondja magát⁴⁰.

Petrényi József: TCP/IP alapok, 1. kötet v2.0

<http://www.microsoft.com/hun/technet/article/?id=3effd5d3-139c-471a-adeb-a71a6885562f>

⁴⁰ És ezt persze eljuttassák a kapcsolat bontásakor is.

3. Ezt az információt az SPI tűzfalak is átveszik, és használják az állapottartó szűréshez, mégpedig a (belső hálózaton lévő) kliens által küldött első SYN-re érkező választól kezdve, gyakorlatilag beépülve a folyamatban. Azaz, ha nem megfelelő SYN, vagy nem egy SYN-ACK jön vissza, akkor eldobják a kapcsolatot, kész, passz.

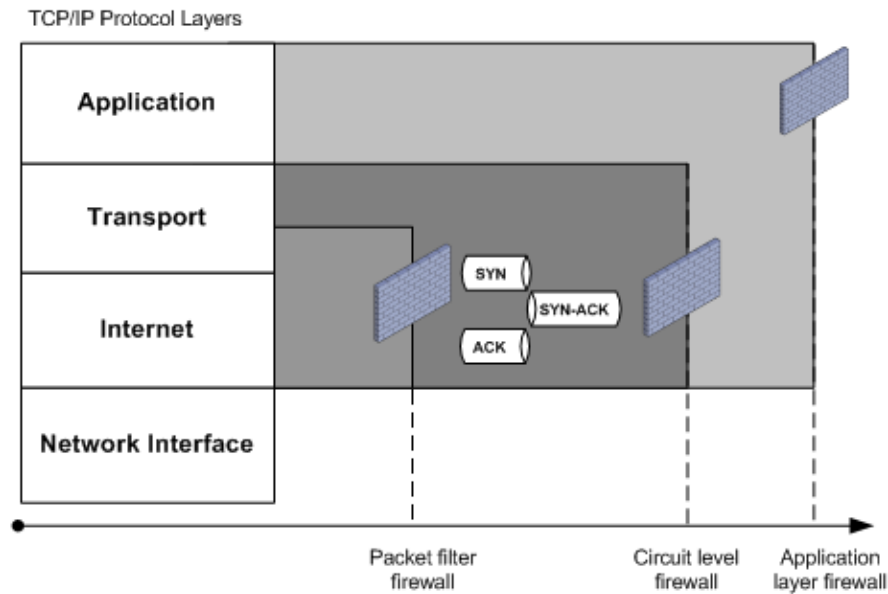
Más, a TCP sessionok karakterisztikájára jellemző részleteket is felhasználhat egy SPI tűzfal, pl. amikor a kliens kezdeményezésére elindul egy session, akkor a tűzfal elindít egy stoppert és addig hagyja nyitva a sessiont amíg van forgalom, és amíg ez az intervallum nem haladja meg pl. az általunk beállított értéket (ezt egy TMG web proxy kapcsolatnál 1 mp-től 27 óráig állíthatjuk be, az alapértelmezés 1800 másodperc). De bizonyos egyszerű esetekben az alkalmazás szintű forgalomban⁴¹ is élhet ez a fajta szűrés, pl. a HTTP esetén a GET metódusban szereplő URL meglétének az ellenőrzése megtörténhet, és a valótlan vagy a hiányos kérések mehetnek a kukába. Plusz amiről eddig még nem volt szó: a változó port számokkal és/vagy több csatornán dolgozó protokollok (pl. FTP, RPC, stb.) forgalma is nyomon követhető, illetve a dinamikus csomagszűrés (csak addig figyel a tűzfal az adott porton, amíg él a kapcsolat) is megvalósítható.

Szerintem mostanra már világossá vált, hogy az állapottartó szűrés lényegesen széleskörűbben használhatóbb, rugalmasabb, és intelligensebb mint a csomagszűrés. De azért vannak hátrányok itt is, pl. több erőforrás szükségeltetik az állapotinformációk tárolásához és kezeléséhez, illetve tipikusan még mindig csak az elsőbb rétegekben szűrtünk eddig, az alkalmazás rétegben sem a csomagszűrés, sem az állapottartó szűrés nem jeleskedik.

5.1.3 AZ ALKALMAZÁS SZŰRÉS

Több esetben az alkalmazás rétegben működő szűrést tekintik a második generációnak, míg más vélemények szerint ez inkább a harmadik. Nálam azért a harmadik, mert ugyan bizonyos alkalmazás és webszűrők már megjelentek az ISA 2000-ben is, de pl. a HTTP filter csak az ISA 2004 kiadása óta áll a rendelkezésünkre.

⁴¹ Illetve pl. a VPN kapcsolatoknál is képes működni - az ISA 2004-től kezdve.

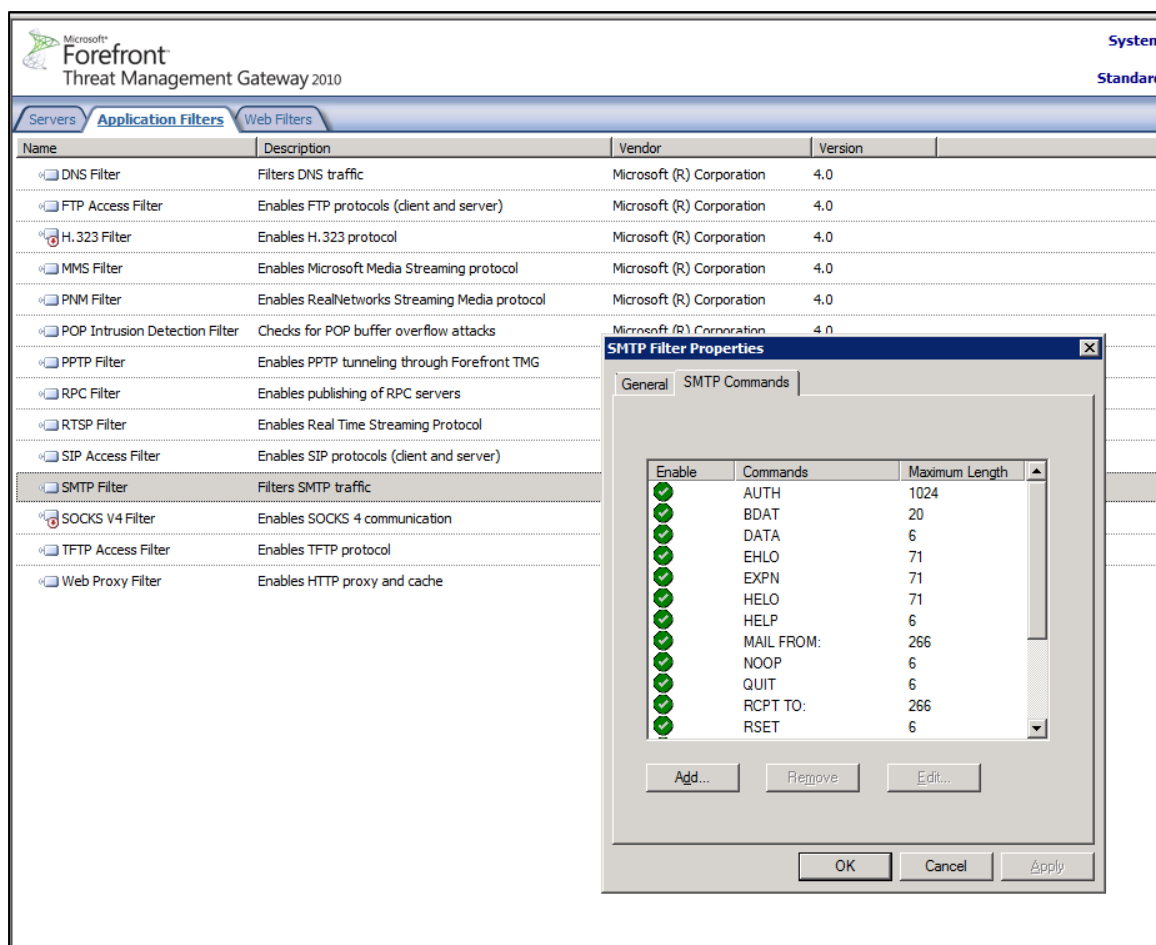


5.3 ÁBRA 4 RÉTEG - 3 SZŰRÉSTÍPUS - 1 ÁBRA

A fontosságának megértéséhez képzeljük el, hogy egy HTTP tartalomban egy rosszindulatú kód vagy egy vírus kódja került elhelyezésre (ez ma már simán tekinthető egy mindennapos esethez). Ez ellen a csomagszűrő vagy az állapottartó szűrő semmit nem tehet, hiszen az ő szemszögükből (és a működési rétegeikben) a csomagok fejlécei rendben vannak, a kapcsolatfelvétel a nagykönyvben megírtak szerint történt, viszont a tartalomhoz hozzá sem képesek szagolni, így ezen forgalom gond nélkül jön és megy át a tűzfalunkon. Az alkalmazás szűrés viszont a tűzfal számára teljes körű lehetőséget ad az egész TCP/IP csomag megnyitására, és az alkalmazások adatainak, parancsainak és kommunikációjának részletes, mélyreható vizsgálatára.

Hadd említsek csak három továbbra is egyszerű példát:

1. Egy SMTP szűrő képes a 25-ös porton minden forgalmat meglesni, az összes SMTP parancs formátumát, szabványosságát (pl. hogy MAIL FROM: mező valóban maximum 266 byte?) csekkolni, illetve adott esetben a kommunikáció megszakítani - még mielőtt a belső Exchange-ünkhöz beérne mindez.
2. Egy HTTP filter akár a metódusok tiltását (nincs POST, nincs több űrlap kitöltés különböző weboldalakon ☺), akár adott alkalmazások működését (torrent kliensek, webes csevegőprogramok, stb.) is képes stoppolni az adott alkalmazásra jellemző, a fejlécben tárolt egyedi szignatúra tiltása alapján.
3. Illetve a fenti példa alapján a HTTP tartalom malware (spyware-ek + vírusok) alapú vizsgálata és megtisztítása, majd a tiszta forgalom továbbítása akár evidens is lehet.



5.4 ÁBRA AZ SMTP FILTER ÉS A TÖBBIEK

Ez csak pár egyszerű példa (később lesznek részletek is), és persze előljáróban még az is érdekes, hogy az alkalmazás szűrés nem mindig a restrikciónak van kihegyezve, hanem a protokollok és session-ok megsegítésére is alkalmas. Viszont azt is tudnunk kell, hogy mindhárom szűrést elszámoltatva, egyértelműen az alkalmazás szűrés az, ami a legmagasabb erőforrás igényvel lép fel.

5.1.4 A TMG HELYE A TÚZFALAK KÖZÖTT

Ahogy már szó volt erről, az ISA Server 2000 tűzfala elsősorban csomagszűrőként és állapotartó szűrőként működött némi alkalmazás szűrő integrációval. Az ISA 2004-ben az utóbbi szerepkör is kiteljesedett, azaz a dedikált alkalmazás és webszűrők mennyisége erősen megnőtt. Ez az ISA 2006-ban alapjaiban nem, mennyiségben viszont változott. Mindezek miatt az ISA Server 2004 és a 2006 is elnyerték a Common Criteria EAL₄₊ (Evaluation Assurance Level 4+) tanúsítványt, amely a tűzfalak megítélésében egy fontos mérföldkő.

Az EAL₄₊ a legmagasabb szintű tűzfal tanúsítvány fokozat a Common Criteria (CC - Közös Követelmények) szabálygyűjteményben, ami azt jelenti, hogy az

adott termék egy kifejezetten magas biztonsági elvárásoknak megfelelő rendszer, ennek megfelelően igazán komoly rendszerekben is bátran használható, valamint bármilyen környezetben is alkalmazzuk, maga a termék is szavatolhatja rendszerünk biztonsági szintjének növelését.

A tanúsítvány kiadója egy független, állami szervezet, konkrétan a német "Bundesamt für Sicherheit in der Informationstechnik". Ez is fontos, de az még jobban, hogy a CC esetén a nemzetközi szerződések miatt a különböző országok kölcsönösen megbíznak egymás professzionális szervezetei által kiadott tanúsítványokban, azaz elvileg ez a tanúsítvány a Föld összes országában érvényesnek tekinthető.

Az ISA 2006 EAL 4+ tanúsítványa (2009. februárban kapta meg, a TMG-é folyamatban van):

<http://download.microsoft.com/download/A/3/3/A33D3307-025E-49AD-A276-DCF0F29E28B0/isa2006-cc-certificate.pdf>

Ezen alfejezet zárásaként csendben jelezném, hogy a TMG-t többek között a Malware Inspection, a HTTPS Inspection, és pl. a Network Inspection System alkalmazás szűrő képességek a hálózatunk határán működő, kártevőket, rosszindulatú kódokat, és a kliensek sérülékenységet kihasználó támadásokat egyaránt legyilkoló, T-100000-es típusú terminátorrá változtatják. Ezek és a további társaik jelentik azt a pluszt, ami miatt az ISA és a TMG tűzfalai között legalább egy fél, de talán egy egész generációs különbség is észrevehető.

5.2 MULTI (NEM LEVEL) NETWORKING

Itt az ideje, hogy tisztázzunk egy olyan témakört... ..amely tisztázásának már régóta itt lett volna az ideje⁴². Ugyanis szó volt már a TMG hálózati forgatókönyveiről, szó volt arról is, hogy a konzolban hol vannak ezek a konfigurációs lehetőségek.

Azt is tudjuk, hogy az ISA 2000-ben még ez nem volt egy komoly probléma, hiszen volt két, rögzített hálózat (Internal és External) és pontum, de az ISA 2004-ben jött a csodaszer, a multi-networking és... ..ennyi. Most már csak azt nem tudjuk, hogy minek ennyi hálózat, hogyan lehet ezeket összekötni, melyek az alapértelmezettek, és milyen elvek mentén kezeljük ezeket a hálózatokat a TMG-ben. Nos, erről lesz szó most.

⁴² A szerző örült tempóban ír, de közben muszáj zsönglőrködni a fejezetekkel is.

5.2.1 MIT IS JELENT EZ?

A multi-networking (nem tudok rá megfelelő magyar kifejezést) véleményem szerint legalább öt alapvetően fontos dolgot jelent:

1. Tetszőleges számú hálózatot definiálhatunk (5 darab alapértelmezettet kapunk), és ezeket csoportokba is szervezhetjük (Network Set)
2. Ezek lehetnek fizikai alapúak (amikor is van hozzá külön interfész) valamint logikaiak is (ugyanazon az interfészen egy vagy több IP tartomány, vagy akár egyetlen IP cím is alkothat egy hálózatot)
3. A hálózatok közötti kapcsolatokat két lépcsőben is szabályozzuk
 - a. A hálózatok közötti alapszabályok (network rules) kizárólag NAT vagy Route lehetnek
 - b. A hálózatok között még ezek után sincs ténylegesen engedélyezett forgalom a tűzfalszabályok nélkül
4. A kliensek hálózatba kerülése automatikus és dinamikus, azaz tennivalót nem igényel, még akkor sem, ha változik pl. a kliens IP címe és így egy másik hálózatba kerül
5. Minden hálózat számára egyedi, akár teljes mértékben eltérő tűzfalszabályokat kreálhatunk (gyakorlatilag ez az oka, hogy adott esetben pl. több "belső" hálózatot is létrehozunk)

A "belső" azért idézőjeles, mert ha jól belegondolunk nincs értelme. A tetszőleges hálózat és hálózati csoport mennyiség és az egyedi tűzfalszabály alkotás miatt Nincs extrán megkülönböztetett belső hálózat (az ISA 2000-nél még volt), a telepítő is csak rutinból kérdezi meg az Internal hálózat. Lehet akár 200 db belső hálónk is (akár egy-egy IP-vel hálózatonként), ergo jön a logikus kérdés: melyik lesz a "legbelső"?

Ezek után nézzük sorban, az alapértelmezett hálózatokat, egyes hálózatok beállítási lehetőségeit, illetve az egymás közötti viszonyukat leíró szabályokat.

5.2.2 AZ ALAPÉRTTELMEZETT HÁLÓZATOK

Öt darab ilyen hálózatunk van a telepítés után, mármint akkor ennyi, ha minimum az Edge forgatókönyvet használjuk.

A KAPUN TÚL

Name	Description	Address Ranges
 External	Built-in network object representing t...	 IP addresses external to the Forefront ...
 Internal	Network representing the internal net...	 172.16.0.0 - 172.16.255.255
 Local Host	Built-in network object representing t...	 No IP addresses are associated with this...
 Quarantined VPN Clients	Built-in dynamic network representing...	 No IP addresses are currently assigned ...
 VPN Clients	Built-in dynamic network object repre...	 No IP addresses are currently assigned ...

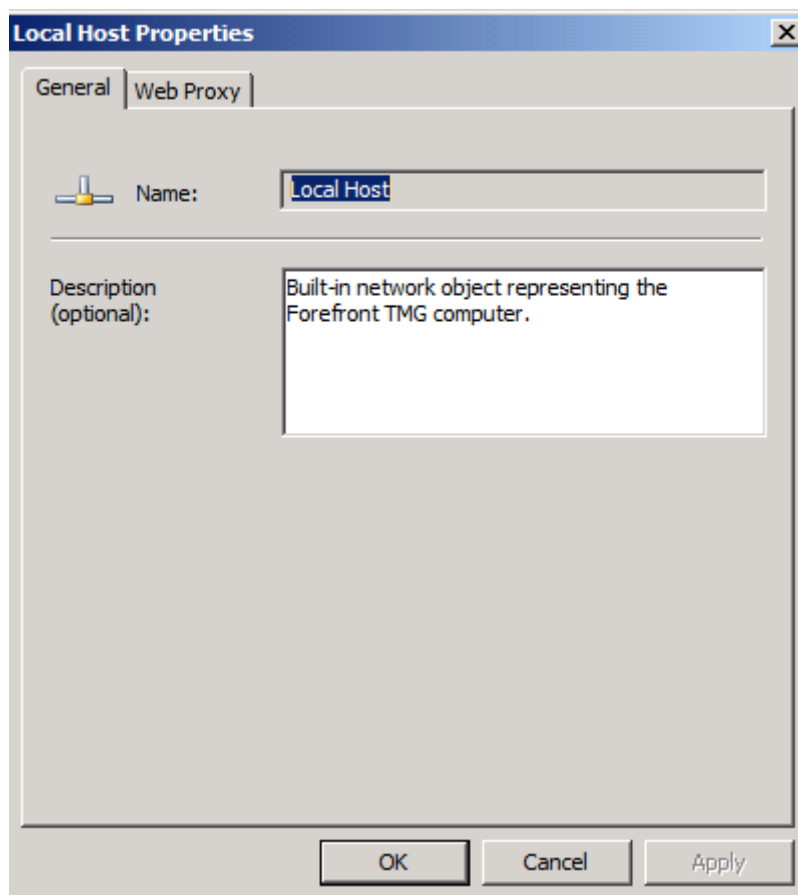
5.5 CSAK EGY ALAPÉRTELMEZETT HÁLÓZATNAK VAN IP TARTOMÁNYA

Az ISA Server 2004 óta pontosan ugyanazok ezek a hálózatok, azaz itt nincs semmilyen változás. Kezdjük egy meglepővel, ami nem egy tipikus hálózat lesz.

A Local Host hálózat

Ez egy kis hálózat, mivel csak egy tagja van: maga a TMG szerver. Azaz ennek a belső interfészén található IP cím, esetleg címek, bár tipikusan csak 1 db. Viszont nem kell és nem is lehet megadni ezt a címet, automatikus. Azért szenzációs ennek a hálózatnak a megléte (szemben pl. a versenytársaival), mert így nagyon egyszerűen és elegánsan tudjuk a TMG szerver felé, illetve felől áramló forgalmat a hálózati szabályokkal illetve a tűzfalszabályokkal kezelni. Sőt, mivel pl. egy tartományba léptetett TMG esetén már telepítés után is szükség van bizonyos belső hálózati hozzáférésére (DC, belső DNS, stb.) ezért a Local Host és az Internal hálózat között már ekkor is léteznek tűzfalszabályok, csak nem látjuk ezeket.

Belegondoltunk már pl. abba, hogy ha az alapállás, hogy a TMG-n nincs semmilyen forgalom engedélyezve a telepítés után, akkor hogyan lépünk be tartományba? Az 5.4 fejezetben elmondom.



5.6 ÁBRA A LOCAL HOST HÁLÓZAT NEM BŐVELKEDIK KONFIGURÁLÁSI LEHETŐSÉGEKBEN

Az External hálózat

Nagyon egyszerű elképzelni ennek a hálózatnak az IP tartományát. Azt szoktuk mondani, hogy minden cím ide kerül, ami nem szerepel máshol. Az előző példánál maradva van három interfészünk, abból két privát címtartománnyal rendelkező Internal (plusz most már tudjuk, hogy a Local Host is) az egyik hálókártyán, a Perimeter egy másikon (ami lehet egy privát tartomány, de akár publikus is).

Ezek IP tartományait majd definiáljuk az adott hálózatok tulajdonságainál, ellenben a harmadik hálókártyán is beállítunk egy, azaz egy darab címet (ha pl. egy darab hardveres router-rel kapcsolódunk, akkor valószínűleg szintén egy privátot, de nyilván teljesen más tartományból mint a többi), és ekkor automatikusan ez lesz az az alapértelmezett External⁴³.

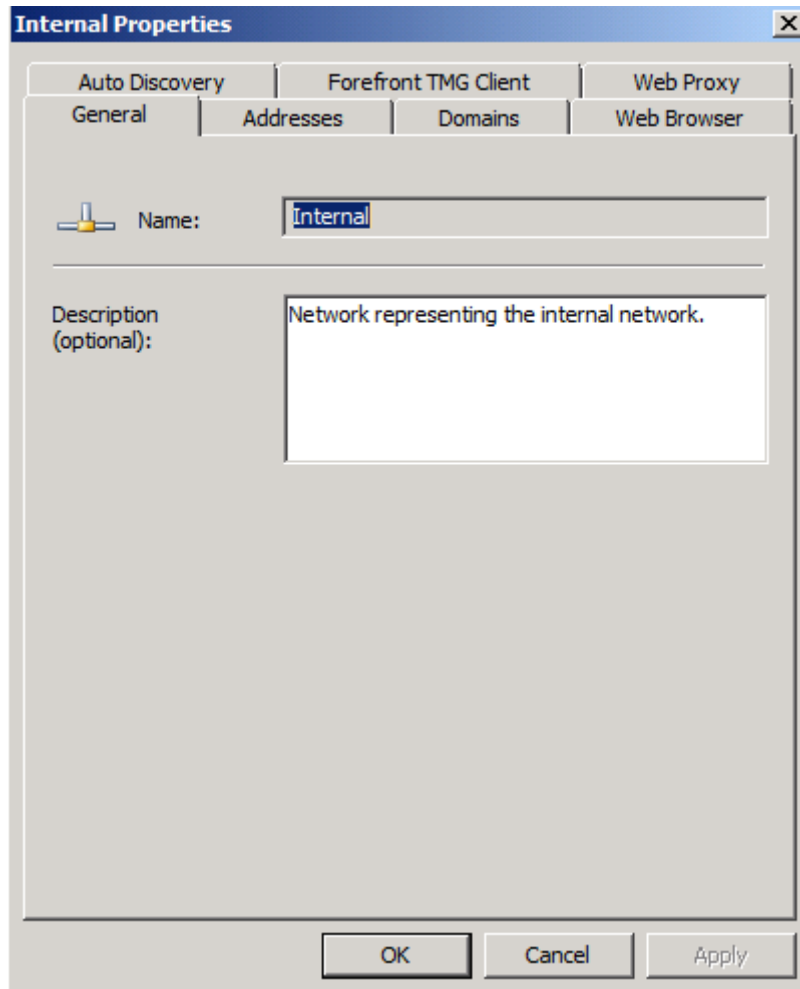
Annyira nincs mit konfigurálni ezen a hálózaton, hogy nem is csináltam róla képernyőképet, majd ha egyszer arra járunk a konzolon, nézzük meg.

⁴³ Igazából nem teljesen automatikusan, mert a TMG-ben már varázsoltunk ezzel kapcsolatban a telepítés után.

A KAPUN TÚL

Az Internal hálózat

Ez a hálózat viszont elkényeztetet bennünket opciókkal (a következő alfejezetben ezeket majd szépen ki is bontjuk). Tipikusan ez a "belső", amelynél viszont kötelező egy IP tartomány megadni – már a telepítéskor. Ezt persze bármikor változtathatjuk, hozzátehetünk, elvehetünk belőle, akár teljesen eltérő IP tartományokat is belevehetünk a hatókörébe, nem gond.



5.7 ÁBRA AZ INTERNAL HÁLÓZAT TULAJDONSÁGAINÁL "FÜLERDŐ" VAN

A VPN Clients hálózat

A neve önmagáért beszél, ellenben arról nem szól, hogy mely gépek az alkotói, illetve hogyan lesz ennek a hálózatnak címtartománya. Nos, a tagok automatikusan kerülnek be ide, és csak és kizárólag azok a gépek lehetnek ebben a hálózatban, amelyek VPN végpontja a TMG szerver. Ezek viszont csak ide kerülhetnek. Így aztán semmit nem kell tennünk azért, hogy egy adagban alkothassunk majd szabályokat a VPN kliensekre, illetve csak annyit, hogy a Remote Access Policy alatt be kell állítanunk egy VPN

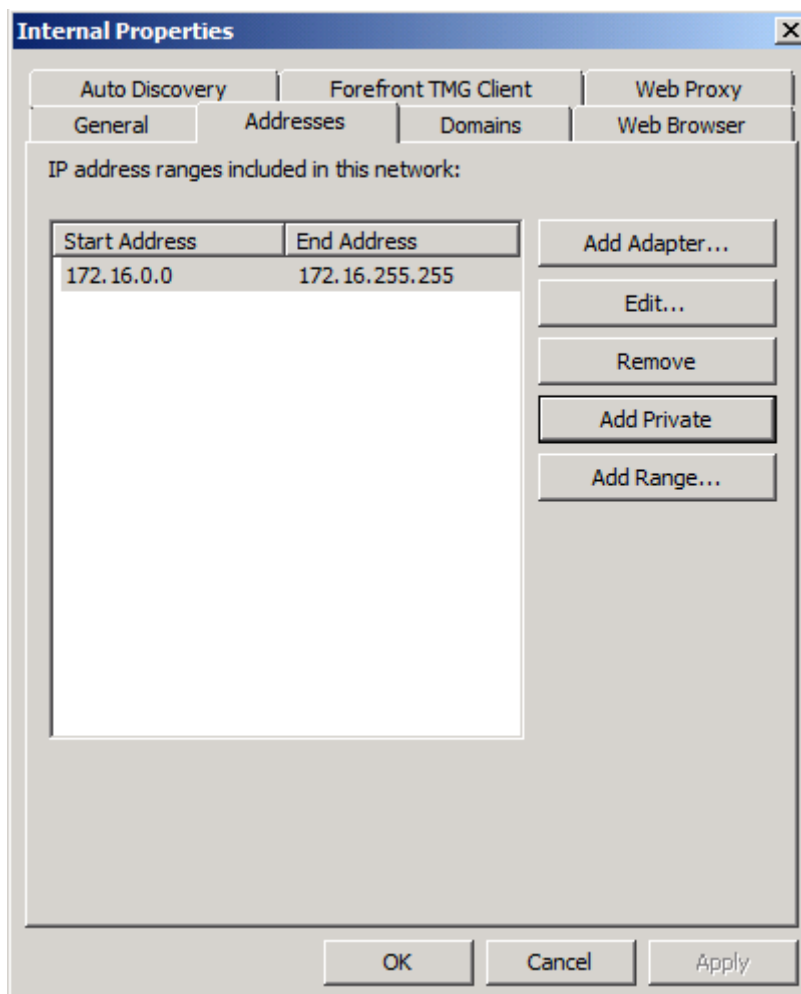
szervert. Mivel ekkor IP tartományt is meg fogunk adni (vagy statikust, vagy egy DHCP-t kérünk majd meg erre), ez lesz ennek a hálózatnak a kijelölt IP tartománya.

A Quarantined VPN Clients hálózat

Az előbb csúnyán hazudtam, amikor azt mondtam, hogy a VPN kliensek csak a VPN Clients hálózatba kerülhetnek. Egy kivétel van, ha beüzemeljük a VPN karantén szolgáltatást, akkor minden VPN kliens (hacsak nem teszünk kivételt egy-egy) géppel, ebbe a hálózatba, azaz egy karanténba kerül először és csak az általunk megkövetelt elvárások (pl. legyen bekapcsolva a tűzfala, legyen frissítve az OS, és stb.) teljesítése után lép át a szimpla VPN hálózatba. Ellenkező esetben kérhetjük majd a kapcsolat bontását. Ez a hálózat ekkor és csak ekkor működik, az IP tartománya megegyezik az szimpla VPN hálózatokéval, illetve még egy közös tulajdonáguk van: semmit nem lehet beállítani a tulajdonságuknál, ezért képernyőkép sincs. Punktum.

5.2.3 A HÁLÓZATOK TULAJDONSÁGAI

Az Internal hálózat adatlapja lesz a példa, mivel itt van a legtöbb elérhető beállítás, ez a legnagyobb halmaz. Ahol lehet címtartományt állítani, ott a második fül tartalmaz azonos lesz a következő ábrán láthatóval.



5.8 ÁBRA A TELEPÍTÉSNÉL BEADOTT IP TARTOMÁNY ITT JELENIK MEG

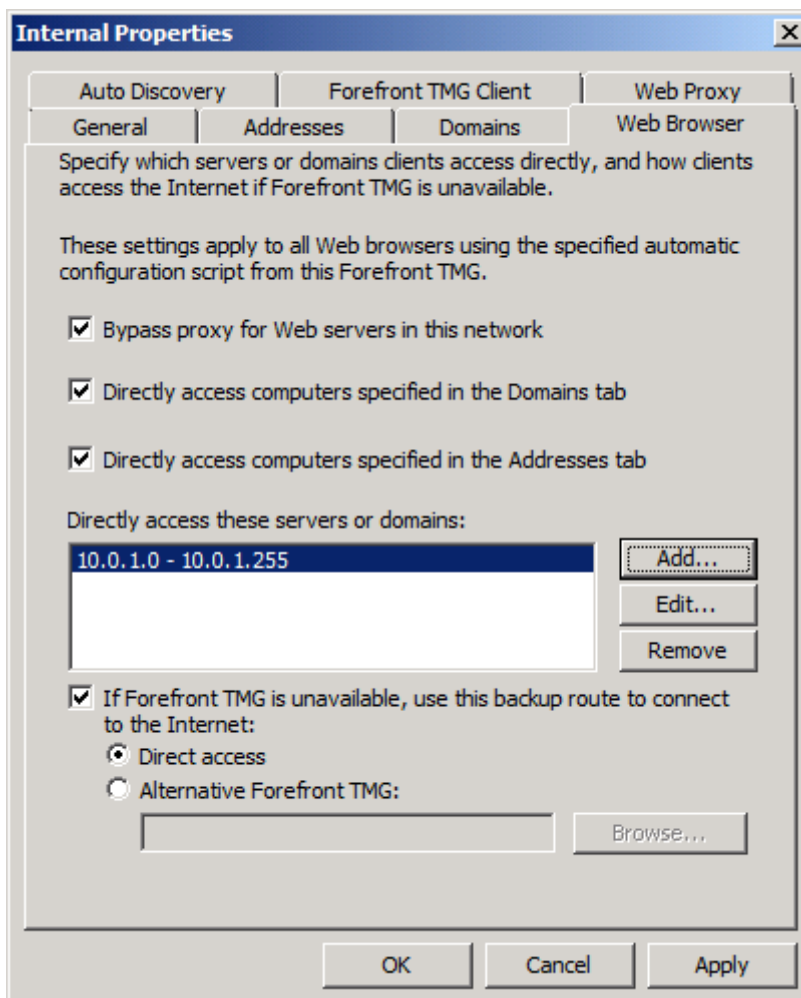
Az automatikus kliens "bekerülés" miatt az IP tartomány megadása kulcsfontosságú, és ezen a helyen kapunk is bőven segítséget ehhez. Hozzáadhatjuk egy már létező és beállított adapter címtartományát, hozzáadhatjuk szabványos privát tartományok bármelyikét (Add Private, 4 ilyen van, ugye egy "A", és egy "C" osztályú, valamint 172.16.0.0 – 172.31.255.255 és az APIPA), illetve egyedi tartományokat is (Add Range).

Ha tovább lépünk, akkor a Domains fülbe botlunk, de ide tartozik szorosan a következő azaz a Web Browser fül is. Tudjunk róla, hogy ezek a beállítások azokra a böngészőkre vonatkoznak, amelyek WPAD-dal kapják majd meg az automatikus konfigurációs szkriptet. Tehát itt, az ebben a szkriptben „letolt” változók (pl. a Domains alatt a „MakeNames()” a Web Browser alatt pedig a „UseDirectForLocal”, a „MAKEIPS ()”, stb.) értékeit konfiguráljuk (7.5 fejezet).

A Domains alatt tehát a hálózatunkhoz tartozó tartománynevet vagy esetleg neveket vehetjük fel, útmutatás gyanánt. A direktíva lényege az, hogy ha egy kliens kérésében egy ebből a tartományból származó gép neve merül fel, abba a TMG (alapértelmezés

szerint) ne piszkáljon bele, hiszen meglesz az direktben is. Itt egyébként csak az információt adjuk meg (úgy ahogy a címtartománynál is), a TMG kényszerítése a kivételezésre a következő fülön történik majd meg.

A Web Browser fülön tovább finomítjuk tehát az eddig útmutatást, jelezhetjük pl., hogy nem kell proxy az ezen a hálózaton dolgozó webszerverekhez (így nem lesz kötelező pl. a hitelesítés sem), valamint itt mondjuk meg, hogy tényleg legyen közvetlen elérés az eddigi füleken megadott értékekhez, sőt pluszban is felvehetünk IP címeket, számítógép vagy tartományneveket. Ez adott esetben igencsak fontos is lehet, azaz ha bármilyen okból nem akarjuk, hogy a megadott gép/tartomány felé a kliensünk ne a web proxy klienssel dolgozzon, hanem pl. egy SNAT klienssel, akkor ez ügyben itt kell lépünk.

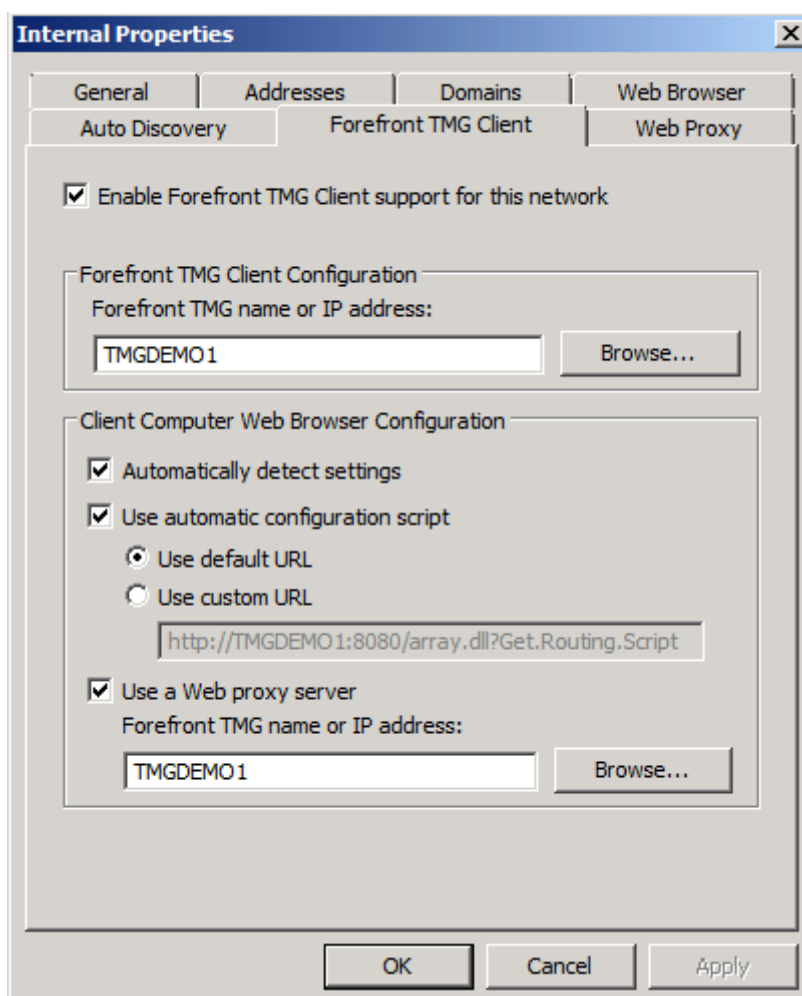


5.9 ÁBRA A WEB BROWSER FÜL

Van itt még egy lehetőség, azaz ezen a panelen legalul a TMG és így a web proxy működésképtelensége esetére tervezhetünk alternatívákat a klienseink számára, azaz a

közvetlen hozzáférést (SNAT vagy tűzfal klienssel) vagy a proxy kérések átdobását egy másik TMG (ISA) szerverre („BackupRoute” a szkriptben).

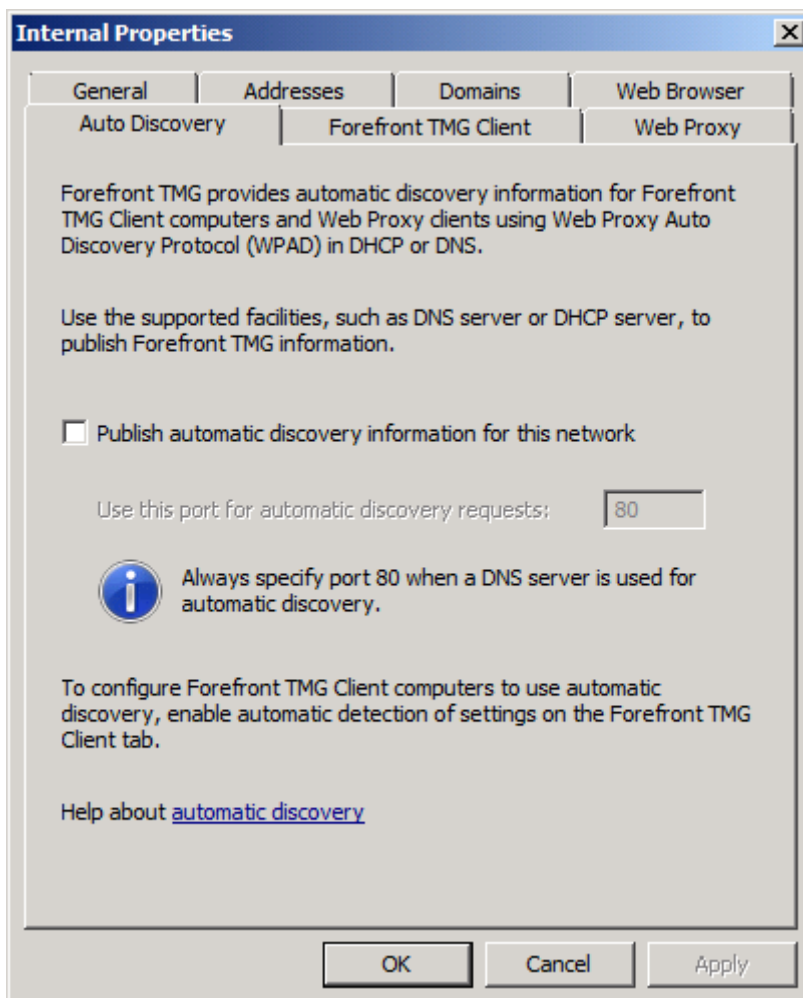
Lépünk ismét tovább, ám nem a Web Proxy fülre, ezt most kihagyjuk, mert erre lesz egy teljes fejezet később, hanem a Forefront TMG Client rész következik. Itt az Internal hálózat tűzfal klienseire vonatkozó beállítások szerepelnek, először is maga az engedélyezés és a TMG konkrét nevének vagy IP címének megadása (ha név, akkor a TMG-nek tudnia kell ezt helyesen feloldani, ha IP, akkor viszont majd ha IP-t váltunk ne felejtjük el itt is átállítani). A panel többi része a tűzfal kliens által a kliens gépen beállítható böngésző konfigurációra vonatkozik. Ez ugye gyakorlatilag majdnem teljesen ugyanúgy néz ki, mint pl. az IE proxy beállításai (3.4 fejezet, első ábra).



5.10 ÁBRA A WEB BROWSER FÜL

Lehetséges automatikus konfiguráció detektálást kérni, amely egy bonyolultabb, elágazásos proxy konfigurációnál történhet egy szkripttel is. Illetve a panel legalján történik meg az beállítás („Use a Web Proxy szerver”), amit a tűzfal kliens felhasznál a kliensoldali böngésző automatikus konfigurálásakor.

Az utolsó fül az Auto Discovery, amelyen ugyan csak egyetlen dolgot állíthatunk (gyakorlatilag ez a ki- vagy bekapcsolás), ám a szakirodalma mégis terjedelmes. Bővebben is kifejtjük, de mivel teljesen a web proxy szolgáltatáshoz kapcsolódik, majd csak a 7.5-ös fejezetben.

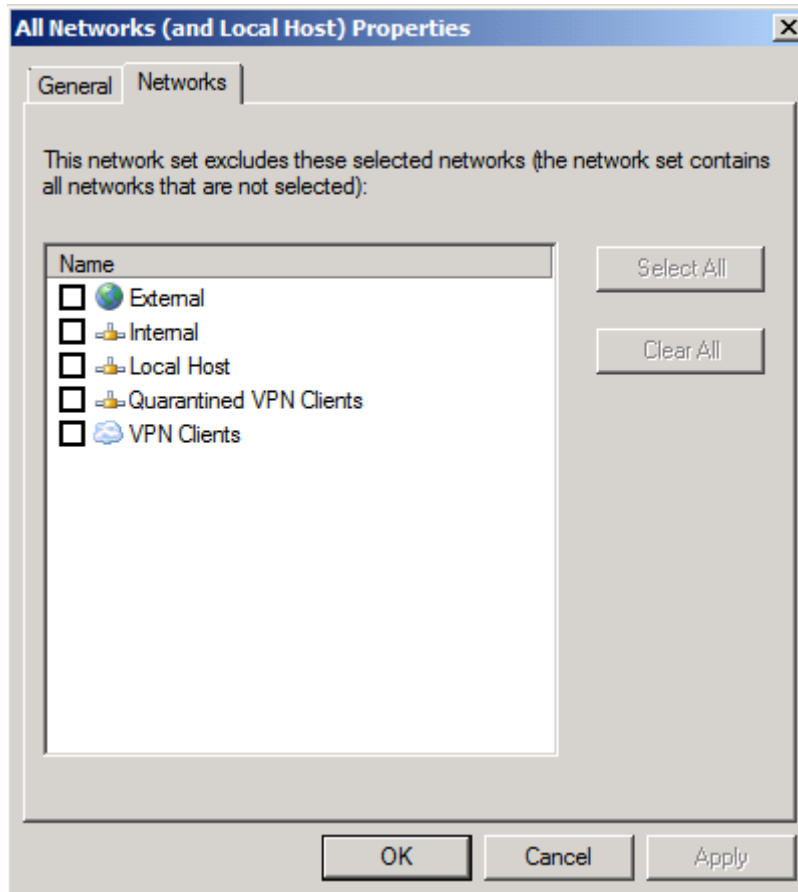


5.10 ÁBRA KEVÉS CSEKKBOX, DE SOK LEHETŐSÉG

A hálózatok logikai csoportosítása nem érdemel külön alfejezetet, de azért megemlékezni meg kell erről a témáról is. Egy hálózatcsoport mindig logikai csoportosítást jelent, elsősorban praktikus okokból, azaz, hogy kevesebb majdnem teljesen azonos szabályt kelljen legyártanunk. A TMG konzolban a Networking \ Network Sets fül alatt érhetőek el, azaz innen elindulva annyit kreálhatunk amennyi jólesik (Tasks \ Create New Network Set), de egy TMG-ben már három alapértelmezettel is összefuthatunk.

1. All Networks (and Local Host): a ténylegesen összes hálózat.
2. All Protected Networks: mind kivéve az External.

3. Forefront Protection Manager Monitored Networks: az FPM által monitorozható hálózat, alapértelmezésben szintén az összes (jelenleg teljesen hatástalan, lásd korábban).



5.11 ÁBRA FURA, DE ÍGY, ÜRES CSEKBOXXAL VAN BENNE MINDEN HÁLÓZAT EBBEN A KÉSZLETBEN

5.2.4 A HÁLÓZATI SZABÁLYOK

A hálózatok közötti alapviszonyt, azaz a két hálózat közötti forgalom áramlás típusát a hálózati szabályokkal írjuk le. Ha van ilyen viszony (ha nincs, minden kérés eldobódik), akkor a típusa kizárólag kétféle lehet, Route avagy NAT.

A Route kapcsolattípus az egyszerűbb, amely szerint a forrás hálózatból induló kliens kérések közvetlenül a cél hálózatban elérhető szerverekhez érkeznek be, és vice versa. A forrás kliens kérése tartalmazza a saját címét is, és a visszairánnyal sem lesz gond, a kapcsolat automatikusan kétirányú.

A NAT (Network Address Translation) már komplexebb dolog, és a mi esetünkben pedig arról szól, hogy a két hálózat között a TMG nemcsak szabályokat érvényesít, hanem aktívan be is kapcsolódik a hálózatok közötti alapszintű kommunikációba.

Röviden: hazudik. Csúnyán becsapja mindkét oldalt, de ez egy kegyes hazugság, enélkül ugyanis nem lehetne megoldani a privát és a publikus címek közötti átjárást.

Szóval ha egy NAT kapcsolatban vagyunk (legjobb példa erre az Internal és az External hálózat kapcsolata), akkor a TMG a forrás hálózathoz érkező kliens kérésében kicseréli a kliens privát IP címét a saját publikus címére, és ezt küldi tovább mondjuk a távoli webszervernek⁴⁴ (ez az első hazugság). A webszerver erre az IP-re küldi a választ, mert azt gondolja jól becsapva, hogy a TMG-nk az eredeti kérő. De nem, de amikor megjön a válasz, akkor a TMG felismeri, hogy ez a belső kliens által küldött kérésre jött, ergo megint csak kamuzik, és úgy tálalja a dolgot a kliens felé, mintha az direktben a távoli webszervertől érkezne. De ebből, sem a kliens, sem a webszerver nem vesz észre semmit (azaz transzparens számukra), a dolog viszont működik. Persze egy speciális esetben, mint pl. akkor, ha egy olyan csomag megy ki, amelyben elvileg nem változhat semmilyen szinten, semmilyen az információ (pl. IPSEC VPN), akkor újabb trükkökre van szükség (konkrétan itt majd a NAT-Traversal segít), de az esetek nagy többségben a NAT nem okoz gondot.

A telepítés után a következő alap hálózati szabályokat láthatjuk a Networking \ Network Rules pont alatt:

1. Local Host Access: Route kapcsolat a Local Host és az összes többi hálózat között⁴⁵
2. VPN Clients to Internal Network: Route kapcsolat a két VPN hálózathoz a belső felé
3. Internet Access: NAT kapcsolat a belső, valamint a két VPN hálózat illetve a külső hálózat között

Nos, ültessük át az elméletet a gyakorlatba, és ezek után képzeljük el a következő helyzetet:

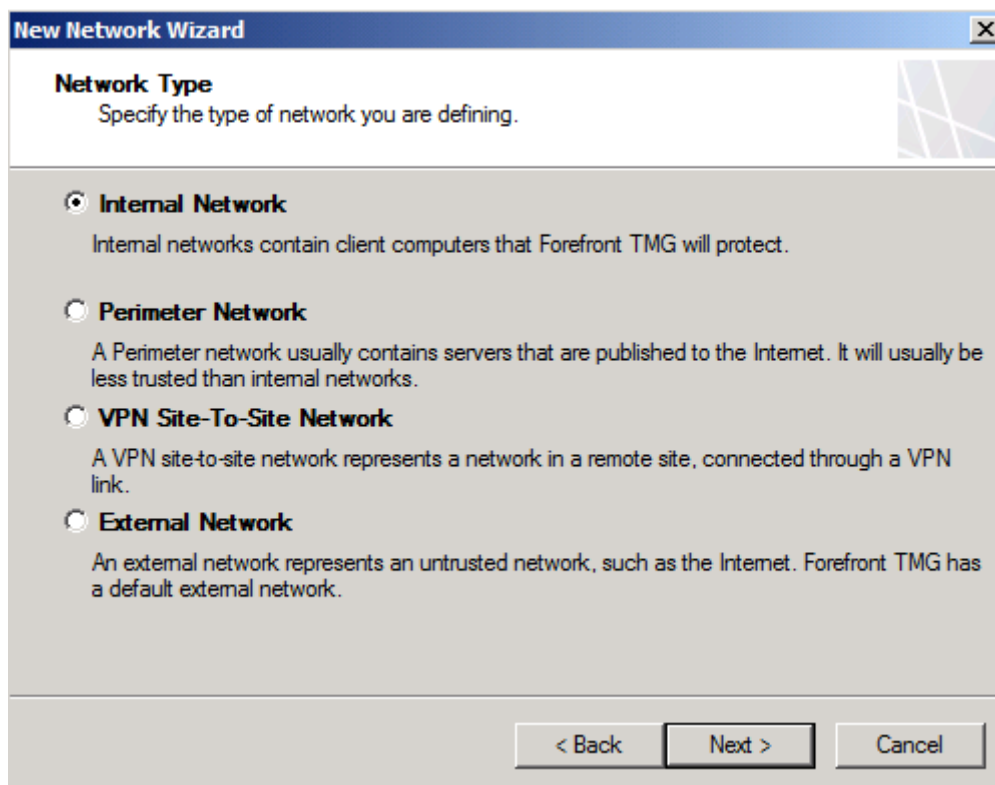
- A rendszerünkben vannak szimpla, irodai klienseink a munkatársaink számára, akiknek az internethez és a belső alkalmazás szerverekhez hozzá kell férniük, de máshoz nem, és természetesen ez egy privát IP címmel rendelkező hálózat.

⁴⁴ Muszáj is ezt megtennie, mivel a NAT kapcsolat egyirányú, közvetett jellegű, ergo alapértelmezés szerint kell valami (ez lehetne az RRAS is, vagy egy hardvereszköz), ami ilyenkor fordít.

⁴⁵ Ne ijedjünk meg, amíg nincsenek tűzfalszabályok addig az External felé és felől semmi nem jöhet.

- Van egy pár gép, ami publikusan bárki számára, de csak kizárólag az internethez elérhető (pl. egy egyetem vagyunk és a folyosón is felállítottunk gépeket), szintén privát címekkel.
- Vannak belső szervereink, amelyek alkalmazásszerverek (fájl, Exchange, printer, stb.), internet elérés azért kell nekik, plusz az 1. pont szerint a belső hálózat kliensei is el szeretnék érni ezeket és privát címeik vannak.
- Vannak olyan szervereink (web, ftp, extranetes kiszolgálók), amelyeket kifejezetten csak az internet felől lehet kérésekkel elérni, minden más hálózattól nagyjából elszigetelve (nyilván egy SMTP átjárónak kapcsolatban kell lennie a belső hálózat Exchange szerverével, de ezt most hagyjuk). Ez a hálózat publikus IP címekkel rendelkezik.
- Az ötödik hálózat az internet, hiszen ezt is elérhetővé kell tennünk az összes eddigi hálózat számára.

Az ISA és a TMG szerverek egy ilyen felállást könnyedén támogatnak. Összesen 4 hálózatra lesz szükségünk (Internal, Internal2, Perimeter, és External, ebből kettő kéznél is van⁴⁶), egyet meg most legyártunk ízibe:



5.12 ÁBRA HA NINCS KÉZNÉL, GYÁRTSUNK LE EGYET

⁴⁶ De a harmadik, Perimeter is kéznél lesz, ha már rögtön ezt választjuk a kezdeti varázslóban, persze ezt utólag is megtehetjük.

Mivel egy belső, privát címekkel rendelkező hálózatunk hiányzik, ezért válasszuk az első pontot. Készíthetnénk egy Perimeter-t is (más szóhasználat: DMZ), illetve egy S2S VPN hálózatot pl. telephelyek között, vagy akár egy második External hálózatot is.

Eddig kevés okunk lehetett rá, hogy egy második External hálózatot kreáljunk, de a lehetőség adott volt már régóta. A cél lehet a megtévesztés kifelé, esetleg egy tartalék képzése, illetve egy új és fontos ok azért akad: a TMG-ben az ISP Link Redundancy használata.

Mindenesetre ha ez az óhajunk, akkor pl. a befelé irányuló publikáló szabályoknál majd nagyon oda kell majd figyelniünk, hogy melyik hálózaton figyel majd a listener, azaz az TMG füle.

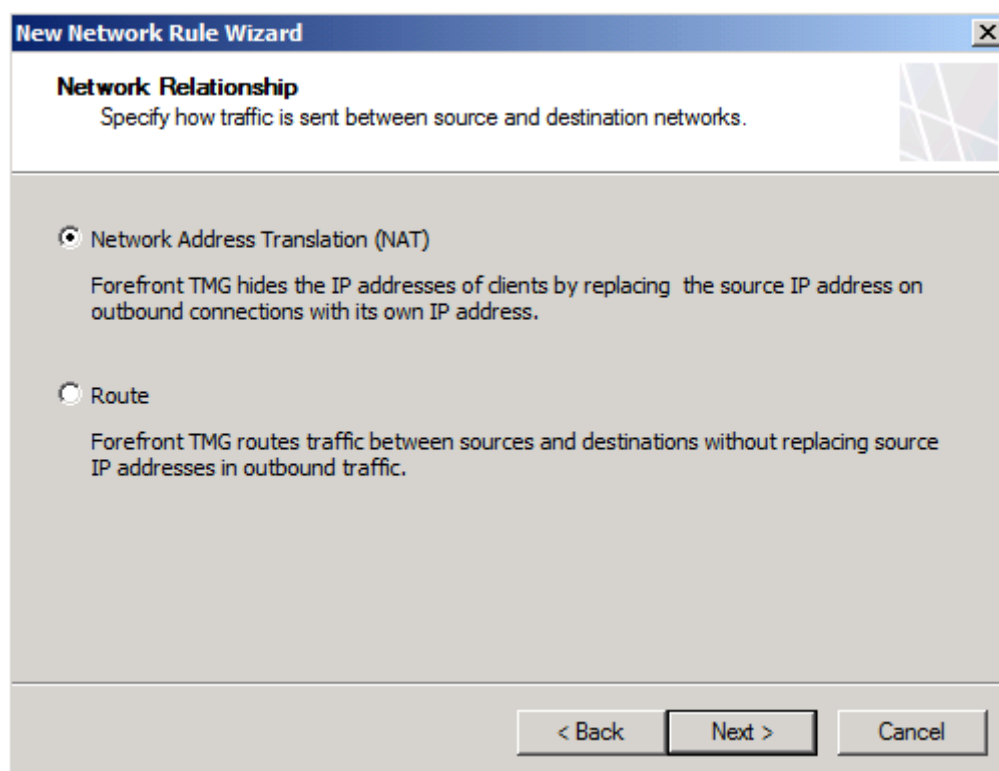
A típus kiválasztása után a többi már rutinmunka, mert már csak címtartományt kell létrehoznunk, amiről már mindent tudunk. Ezután persze jöhet az adott Internal2 hálózat beállítása (lásd az előző alfejezetet).

Így vagy úgy, de mostanra már kész van a négy darab hálózat, így gondoskodhatunk az ezek közötti hálózati szabályokról. Az új hálózatok esetén mindezt a Network Rules rész alatt tehetjük meg, de előbb nézzük meg a következő táblázatot, mert ennek megfelelően kell lépniünk.

5.1 TÁBLÁZAT (X= NEM RELEVÁNS, 0 = NINCS KAPCSOLAT)

	Intranet	Internal2	Perimeter	External
Internal (irodai kliensek és belső szerverek)	X	0	0	NAT
Internal2 (folyosói gépek)	0	X	0	NAT
Perimeter (web, ftp szerver)	0	0	X	Route
External (Internet)	NAT	NAT	Route	X

Szóval a feladat most az, hogy a friss Intranet2 hálózat és az External között egy NAT kapcsolatot hozzunk létre. Ehhez lépünk a Network Rules szakaszba, és válasszuk a Create New Network Rule opciót a Tasks Pane-ből. Adjunk meg egy ráutaló nevet, majd tallózzuk be a forrás hálózatot (Internal2), aztán a célhálózatot az Add... gombbal, majd válasszuk a Network Relationship panelen a NAT opciót.



5.13 ÁBRA ELDÖNTENDŐ KÉRDÉS

Ezek után lesz még egy újabb eldöntendő kérdés, ami az ISA rendszergazdák számára sem lesz ismerős, és ez pedig az ún. Enhanced NAT képességből adódik (6.3 fejezet). Most mi válasszuk az alapértelmezést (Use the default IP address), és zárjuk le a varázslót. Ééés készen is volnánk, mivel kész az új hálózat, amely tagjai NAT-tal el is érik majd az Internetet.

Order	Name	Relation	Source Networks	Destination Net...	NAT Addresses	Desc
1	Local Host Access	Route	Local Host	All Networks (...)		
2	VPN Clients to Int...	Route	Quarantined ... VPN Clients	Internal		
3	Internet Access	NAT	Internal Quarantined ... VPN Clients	External	Default IP address	
4	Internet Access2	NAT	Internal2	External	Default IP address	

5.14 ÁBRA SZÉPÜLÜNK, BŐVÜLÜNK

Amellett, hogy az előző táblázatban egy amőba állást rajzoltam fel (a betűk engem is zavarnak benne ☺), szépen látható, hogy a kétféle hálózati szabályból illetve a "nem kötelező összekötni" elvből szépen kirajzolódik a megoldás. Ha hálózati interfészben gondolkodunk, akkor ez minimum 3 kártya (a két intranet címtartománya lehet egy kártyán). Ha később, úgy döntünk, hogy egy újabb Intranet szegmenst kössünk rá a

TMG-re annak sem lesz akadálya (persze a beállításokat erre vonatkozóan is meg kell tennünk majd), és ha pl. a folyosói gépekből egyet beviszünk az irodába, mert muszáj, elég lesz csak a TCP/IP konfigját átírni. Ilyen egyszerű.

Ha jól megfigyeljük, akkor a hálózati szabályok számozottak. Ez nem statisztika miatt van így, ez valóban egy prioritási sorrend, és változtathatunk is rajta (nézzünk jobbra a Tasks Pane-re). Amikor két, külön hálózaton lévő gép között megindulna a kommunikáció, akkor a TMG megkeresi az első megfelelő hálózati szabályt amely ezekre a hálózatokra passzol, és ennek megfelelően teszi a dolgát. Ha történetesen az egyik hálózatban egy konkrét gépre, vagy egy szűkebb IP tartományra is van egy definiált szabályban egy ellenkező típus, akkor ez nem fog teljesülni. Ahhoz hogy ez mégis működjön, a kisebb halmazzal felölölő szabályt feljebb kell mozgatnunk a sorrendben.

Egy működő felálláshoz ezek után viszont már csak a megfelelő engedélyező tűzfalszabályokat (no és persze a szervereket publikáló tűzfalszabályokat) kell létrehozni azon hálózatok között, amelyeknél nem az X, és nem egy o szerepel.

Ez következik most.

5.3 AZOK A CSODÁLATOS SZABÁLYOK

A TMG legjobban variálható része a tűzfalszabályok világa. Egyúttal ez is az a rész, amelyet a legnehezebben lehet teljes mértékben elsajátítani, pontosan azért mert igen mély és összefüggő ismereteket igényel. Mindent tudnunk kell a hálózati objektumokról, a protokollokról és portokról, a hálózatokról, ráadásul egy nagy halom esetben azokról az eszközökről is, amelyek számára ezeket a szabályokat készítjük. És akkor még a tűzfalszabályok működéséről, vagy pl. a sorrendről nem is beszéltünk...

Viszont szögezzük le: minden tűzfalszabálynak számít, amelyet a faszerkezet Firewall Policy ágában létrehozunk (most a csak logikai csoportosításként funkcionáló Web Access Policy-t figyelmen kívül hagyjuk), pl. a publikáló szabályok is, mi viszont ebben a fejezetben elsősorban a hozzáférési tűzfalszabályokkal játszunk majd.

5.3.1 A SZABÁLYOK ALAPANYAGAI, AZAZ A HÁLÓZATI OBJEKTUMOK

A TMG-ben egy-egy szabály elkészítése olyan mint a főzőcskézés⁴⁷, azaz mint egy jó leves elkészítése, összedobálunk egy kis ezt, egy kis azt, egy kis amaszt, majd megfőzzük és ha jól csináltuk, hatalmas élvezettel megesszük. Egy biztos, nem árt előre

⁴⁷ Nem vagyok egy konyhatündér, sőt a konyhában max. egy sima user vagyok, de TV-n szeretem nézni az ilyen típusú műsorokat, tehát értek hozzá ☺

A KAPUN TÚL

megtekinteni, beszerezni és előkészíteni a kellékeket, mielőtt nekiesünk a műveletnek. Ez itt is így van, szóval kezdjük azzal hogy kiismerjük az alapanyagokat, mert van belőlük igen sokféle. A Firewall Policy szakaszban, a Task Pane Toolbox fül alatt találjuk meg ezeket, a következő fő kategóriákban:

1. Protocols: Számtalan protokoll, előkészítve és csoportosítva
2. Users: Összesen 3 darab gyári csoport a hitelesítéshez
3. Content Types: 11 kategóriában rengeteg MIME típus, vagy kiterjesztés
4. Schedules: 2 db gyári időzítés
5. Network Objects: a legösszetettebb rész, részletek lejjebb

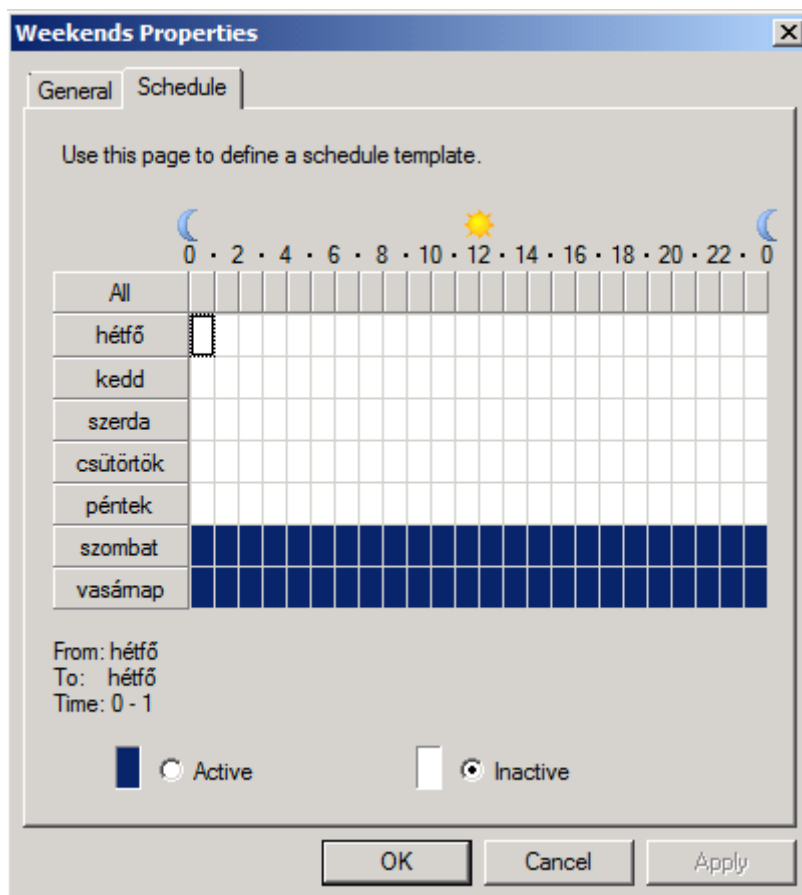
Mielőtt bűnnek eresztenénk a fejünket a gyári kis létszámú felhasználói csoport vagy az időzítések gyűjtemény miatt, természetesen tudnunk kell, hogy mindegyik szerszámoszláda kategória tetszőleges mennyiségű elemmel bővíthető, exportálható, importálható, stb..

Nézzük viszont részletesebben az utolsó kategória elemeit, mert itt aztán van "anyag" bőven, bár az első kettő máris ismerős lesz:

- Network: Egy-egy hálózat, beleértve a gyáriakat, és az általunk definiáltakat is.
- Network Sets: Hálózatcsoportok, szintén ismerősek már.
- Computers: Egyetlen számítógép, IP címmel megjelölve.
- Computer Sets: Számítógép csoport, mely tagja lehetnek egyedi számítógépek, egy egész alhálózat, vagy akár egy tetszőleges IP tartományba tartozó gépek, de nem lehetnek az előző csoport tagjai, azaz a computer objektumok.
- Address range: Kifejezetten egy IP tartományba tartozó gépek
- Subnets: Alhálózat, címmel és maszkkal ellátva
- URL sets: Megdöbbentő lesz, de URL címek összességét jelenti ☺, úgymint pl. a <http://www.microsoft.com> vagy http://www.netlogon.hu/*
- URL Categories: A TMG egyik új szolgáltatásához tartozó URL kategóriák (összesen 91 db)
- URL Category Sets: Az előzőben említett összes kategória szűkítése (11 db)
- Domain Name Sets: Tartománynevek, vagy részeik úgymint pl. *.netlogon.hu
- Web listener: No, ez egy komplex dolog, a publikálásnál sok szó esik már róla, addig is elégedjünk meg annyival, hogy a TMG szerver HTTP vagy HTTPS portokon figyelő "fülei" szerepelnek majd itt
- Server Farms: Szintén a publikáló szabályokban szereplő szerver farm objektum gyártása, a farm elemeinek definiálásával, IP cím vagy név alapján

A hálózati szabályoknál értelemszerűen csak az első kettő kategória elemeit használhatjuk majd, a tűzfalszabályoknál viszont mindent, viszont az utolsó kettőt majd csak a webserver publikálásnál.

Most pedig kiemelnék 1-2 objektumot, azért hogy lássuk, hogy vannak egyszerűbbek és természetesen bonyolultabb, részletesebb jellemzőkkel bírók is. Kezdjük két egyszerűvel, először is egy időzítéssel.

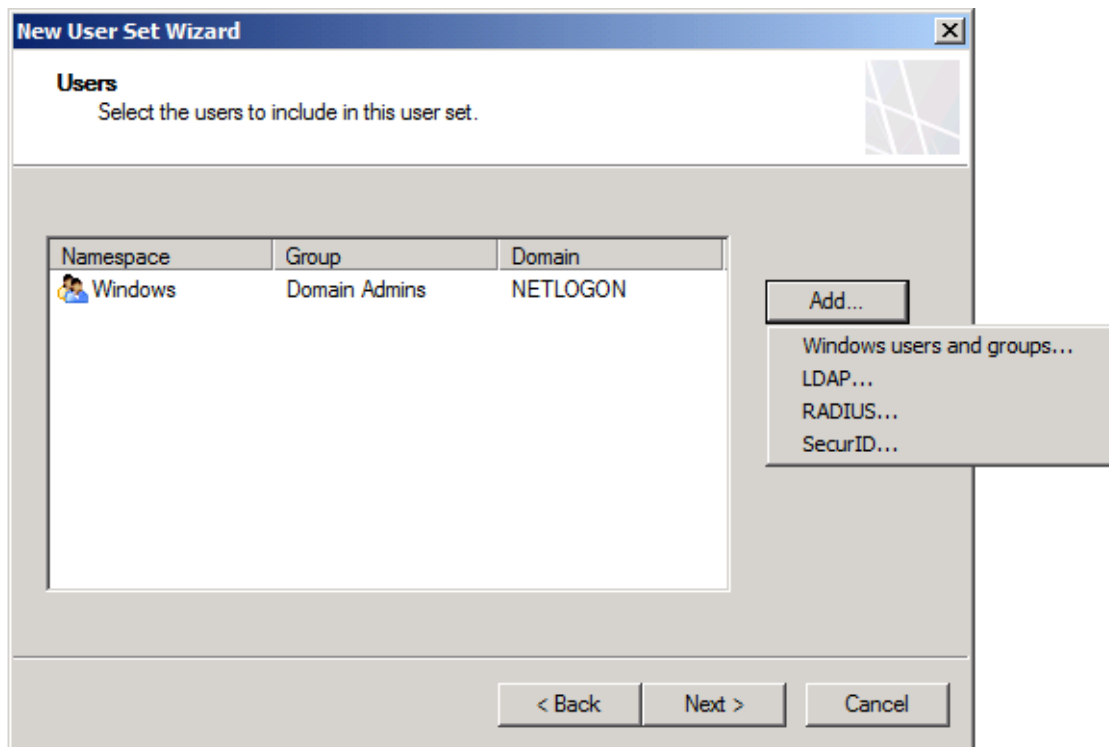


5.15 ÁBRA VÉGRE LESZ NET AZ IRODÁBAN A HÉTVÉGÉN

Ezeket az elemeket időbeli korlátozására használhatjuk a tűzfalszabályokban. Csak két dolgot állíthatunk benne, 1-1 órás részletekben: az egyik az lesz amikor érvényes lesz az adott szabály (kék részek), a másik pedig amikor nem⁴⁸.

Aztán itt egy másik is, a felhasználói csoportok létrehozása, amelyek kulcsfontosságúak lehetnek egy-egy tűzfalszabályban, hiszen a kötelező hitelesítéssel kombinálva felhasználói fiókok szerint különböző szabályokat gyárthatunk, amelyekben pl. különböző csoportoknak, különböző protokoll használatot engedünk vagy tiltunk meg.

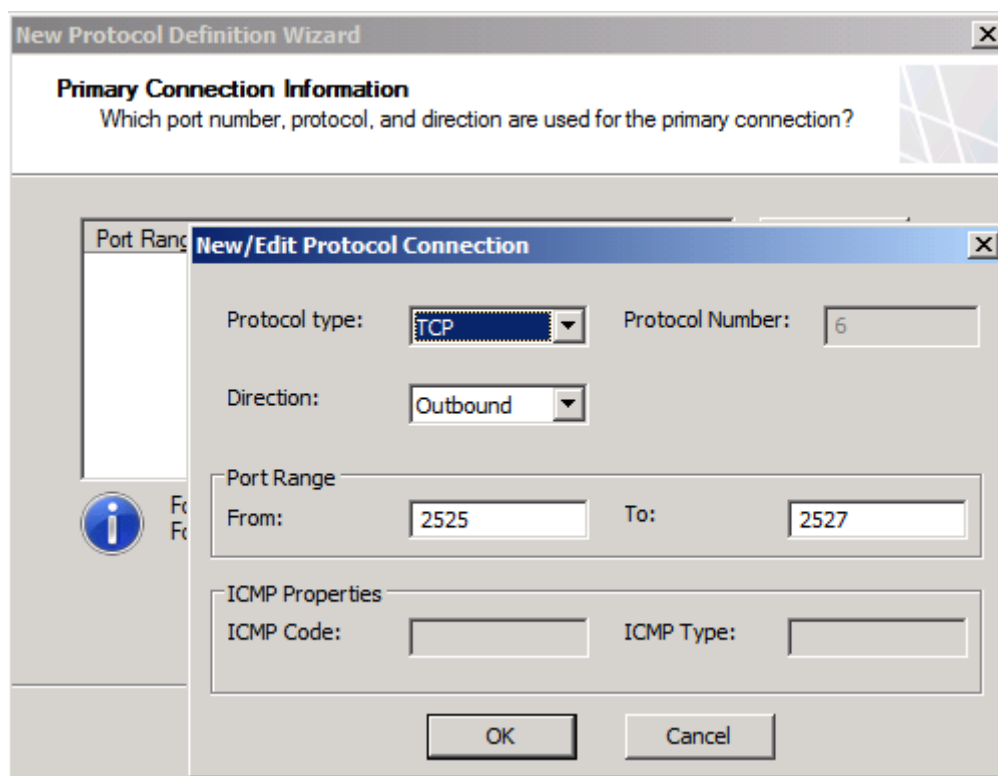
⁴⁸ Figyeljük meg a Hold és a Nap piktogramokat az óra tengelyen: a Microsoft mindenre gondol ☺



5.16 ÁBRA NÉVTÉR, NÉVTÉR HÁTÁN

Ez a mini varázsló gyakorlatilag olyan mint bármelyik fiók kiválasztó panel az OS-ben, annyi kivétellel, hogy míg egy tartományi gépen helyi és tartományi fiókokat és csoportokat tállózzhatunk, itt még plusz három névtér is a rendelkezésünkre áll (LDAP, RADIUS, SecurID).

Nos, nézzünk egy összetettebb objektumot is, pl. egy egyéni protokoll létrehozást. Keressük meg a Protocols legördülő menüt, majd a New / Protocol menüt. Újabb mini varázslót indítunk, ahol először az elsődleges kapcsolat első protokollját állítjuk be.



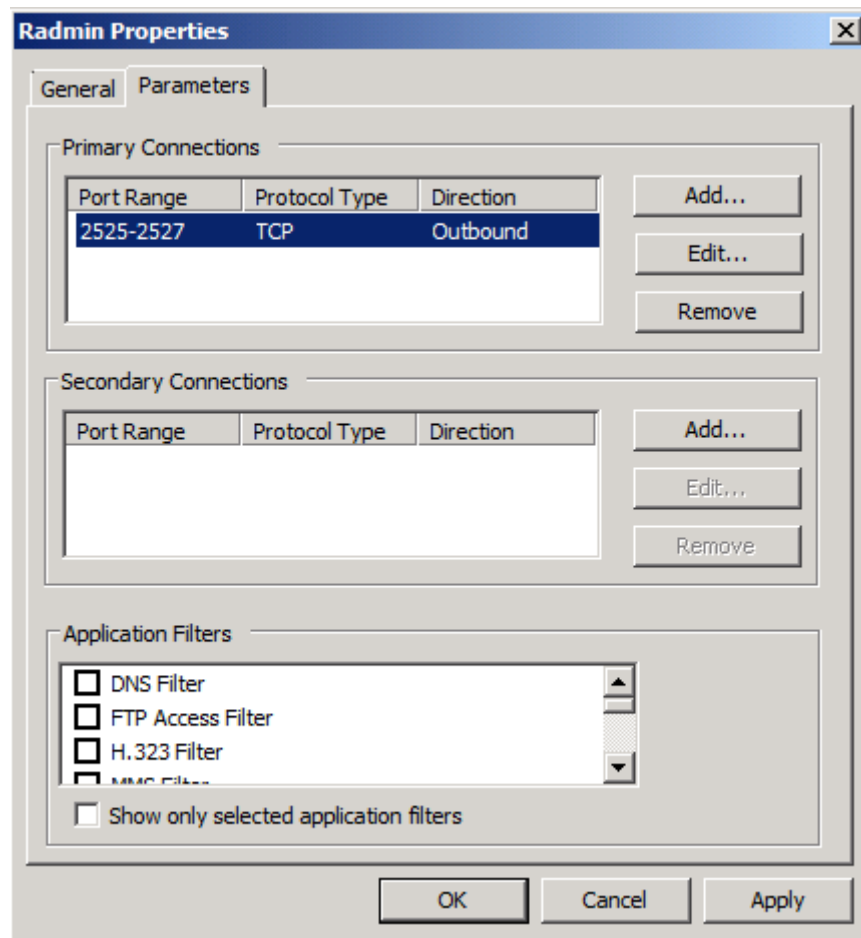
5.17 ÁBRA A SPÉCI ALKALMAZÁSUNK EZT A PORT TARTOMÁNYT HASZNÁLJA

Ezt úgy kezdjük, hogy először is eldöntjük, hogy mely protokoll típust választjuk (TCP / UDP / ICMP / IP), aztán pedig az irányt, majd a port szám intervallumot is. Ha ICMP-t választunk, akkor a megfelelő ICMP kódot és a típust is meg kell adnunk. Ha kell még az elsődleges kapcsolathoz másik port is, akkor azt is fel kell vennünk, ha nem, mehetünk másodlagos kapcsolat⁴⁹ paraméterezéséhez, ahol ugyanezt a panelt találjuk. Csak ezután leszünk készen teljesen, illetve a kész protokollon még további változtatásokat is megtehetünk, pl. egy másik ismert protokoll hozzárendelését (ezt csak a TMG-ben), vagy éppen egy megfelelő alkalmazásfilter hozzárendelését.

Irányok:

- TCP esetén Inbound/Outbound, azaz bejövő/kimenő
- UDP: Send (egyirányú, csak küldés); Receive (egyirányú, csak fogadás); Send-Receive (2 db egyirányú, előbb van küldés aztán a fogadás), Receive-Send (2 db egyirányú, előbb van fogadás aztán a küldés)

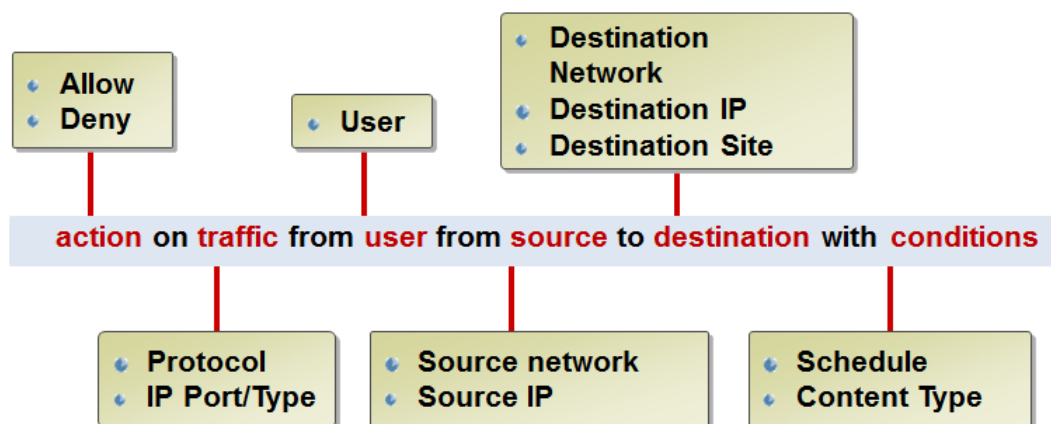
⁴⁹ Port intervallum, protokoll illetve iránybeállítási lehetőség további kapcsolatokhoz vagy csomagokhoz egy már kiépült kapcsolatban. Jó példa erre az FTP kapcsolat, a maga két csatornájával.



5.18 ÁBRA UTÓLAG IS VARIÁLHATUNK

5.3.2 HOGYAN ÉPÜL FEL EGY HOZZÁFÉRÉSI TŰZFALSZABÁLY?

A belépőnk már megvan, sőt már a hálózatokkal, és a felhasználható objektumokkal is tisztában vagyunk, most jön a cylinder és a nyúl.



5.19 ÁBRA TELJESEN EGYÉRTELMŰ

A fenti ábra mutatja egy tűzfalszabály készítésének a menetét, gyakorlatilag a szabály varázsló letükrözéséről van szó.

5.3.3 ÉS HOGYAN MŰKÖDIK?

A policy engine a TMG talán egyik legbonyolultabb része, de kimagaslóan fontos is. A feladata az, hogy meghatározza egy a tűzfalhoz beérkezett kérés sorsát.

Most vegyük azt a példát, amikor egy belső kliens egy internetes webszervert szeretne elérni, azaz a böngészőjével egy weboldalt. Ez a mi rendszerünkben csak és kizárólag a TMG szerveren keresztül történhet, így amikor egy kérés megérkezik a TMG-re, leegyszerűsítve három dolog történhet:

1. Van passzoló szabály és ez engedélyező: a kérés továbbításra kerül és a választ fogadja majd szintén továbbítja a TMG vissza a kliens felé
2. Van passzoló szabály, de tiltó: ekkor vagy megjelenik a böngészőben egy a TMG számos HTML hibaüzenetéből, pontosan jelezve a hiba okát és körülményeit, vagy a kliens a tiltó szabály beállításai alapján átirányításra kerül.
3. Nincs passzoló szabály: ekkor az alapértelmezett mindent tiltó szabály lép életbe, és persze lesz hibaüzenet is.

Igazából nem is egy, hanem két különböző szabálytípus dolgozik majd minden egyes kérés alkalmával (és az eredménybe beleszólhat még az E-NAT (6.3), az ISP-R (6.2) és a Web chaining (7.2.) is), egyrészt az 5.2 fejezetben említett hálózati szabályok illetve az éppen most tárgyalt tűzfalszabályok.

Nézzük tehát a konkrét lépéseket:

1. A belső kliens elküldi kérést a TMG-nek.
2. Az első lehetséges válaszlépés a TMG részéről a hitelesítés kérése. Ez lehet kötelező (pl. általunk manuálisan előírt) és opcionális, illetve történhet transzparens módon is. Ha nem tud transzparens módon hitelesíteni a kliens, akkor a TMG elkéri ezt az infót a felhasználótól (további infó a 7. fejezetben). Ha egy SNAT kliensről van szó, akkor hitelesítés nem lesz, mert nem lehet, de a hálózati és tűzfalszabályok azért vadul dolgoznak tovább – a forrás IP cím alapján.
3. Ha tehát a kliens jogosult egyáltalán elérni a TMG web proxy-ját, akkor jöhet a hálózati szabály ellenőrzés: lehet-e abból a hálózatból ahol a kliens van, elérni azt a hálózat ahova szeretne eljutni? Azaz van-e definiált kapcsolat a két hálózat között? Ha nincs, itt vége a dalnak, van viszont itt még két fontos dolog:
 - Azt is ellenőrizzük, hogy olyan forrás IP-vel érkezett-e a csomag, ami a fogadó interfésszel azonos TMG logikai hálózathoz van-e rendelve. Ha nem, akkor „spoof packet” lesz belőle.

- Ha nincs hálózati szabály, akkor a log viewerben a „Rule” mező üres lesz. Tehát nem a „Default rule” tilt ilyenkor, hanem a firewall engine jóval hamarabb lezárja a kiértékelést.
 - A cél ellenőrzése is megtörténik, és ha nem passzol egyik hálózatra sem, akkor a cél az External, és így a NAT, és megyünk tovább.
4. És csak most jönnek a hozzáférési tűzfalszabályok. Az előző ábrán szépen látszik, hogy egy szabály kezdődhet engedélyezéssel, vagy tiltással. A tiltás egyértelmű, az engedélyezésnél pedig a szabály részletei implicit módon tiltanak, azaz ha azt állítjuk be, hogy csak 11.00-12.00 közötti intervallumban van HTTP engedélyezés, akkor bármilyen más időpontban tiltva van. De - mivel sok-sok tulajdonságra szűr a TMG – előfordulhat hogy ennek végeredménye, az, hogy nemcsak egy szabály passzol majd egy adott pillanatban hanem több is. Rengeteg korábbi ábrán látható, hogy szabályok tucatjai is „élnek” egy rendszerben, és ezek között lehetnek átfedések egy kérés apropóján. Ezért fontos a prioritási sorrend. A TMG tűzfal szabály motorja fentről (illetve az 1. számútól, mert lehet ám, hogy véletlenül fordított, vagy más sorrendben állnak a szabályok) kezdi átfésülni a gyűjteményt, és ha talál egy az adott helyzetre passzoló szabályt, akkor nem kötözködik tovább.

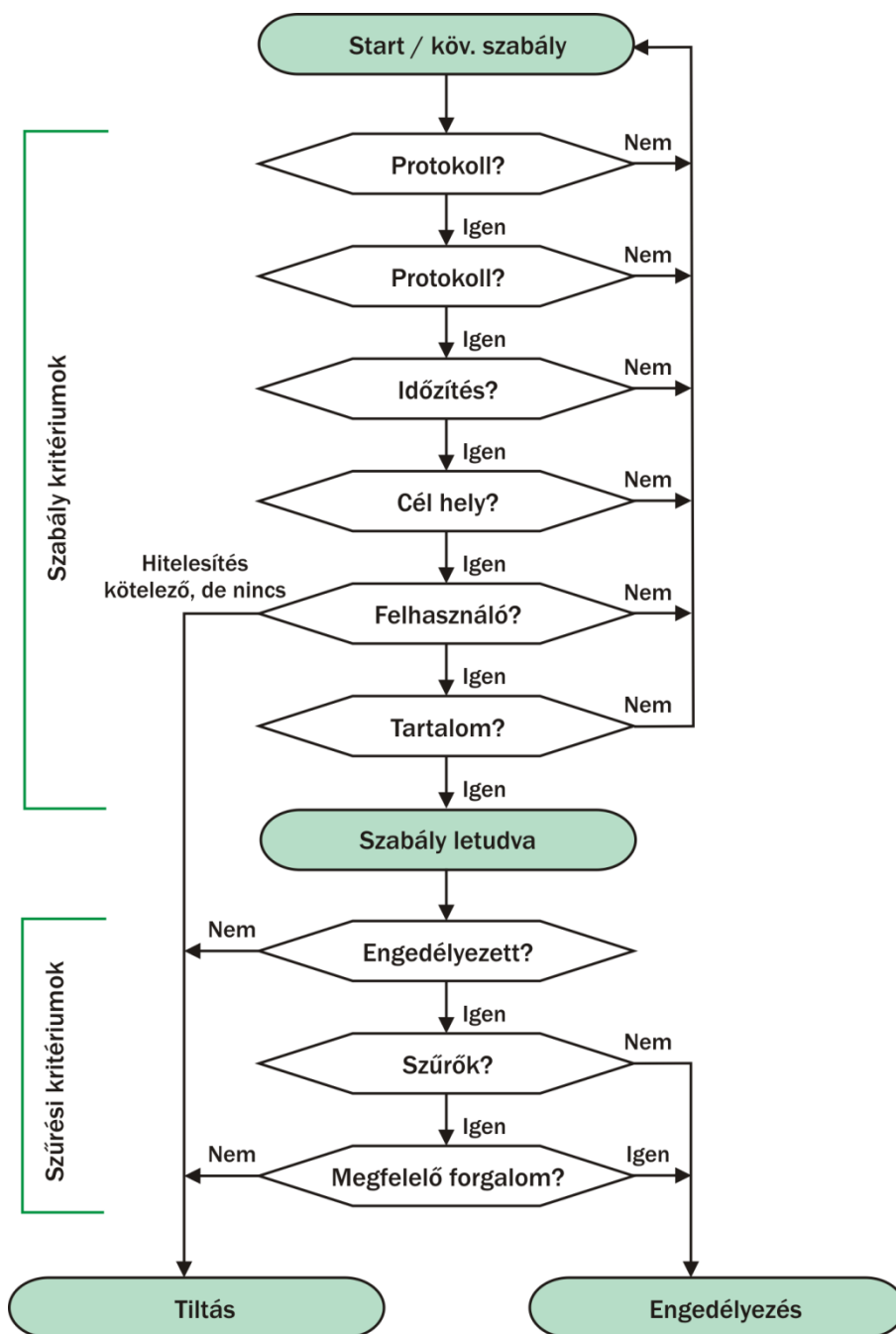
Ezért aztán az ajánlott szabály sorrend a következő:

1. szerver illetve webszerver publikáló szabályok
2. hitelesítést nem igénylő tiltó szabályok
3. hitelesítést nem igénylő engedélyező szabályok
4. hitelesítést igénylő tiltó szabályok
5. hitelesítést igénylő engedélyező szabályok

5. Még nincs vége. Ha egy kérés rendben van a hozzáférési szabályok alapján, akkor a TMG egyrészt elkészíti a connection object-et (ezt az egyszerűség kedvéért pl. egy táblázatként, mondjuk mint a NAT tábla, képzeljük el), másrészt most használja fel a már korábban felfedezett hálózati viszonyt, mivel a folytatásban nem lesz mindegy, hogy NAT avagy Route a két hálózat közötti viszony, mert ha pl. NAT lesz, akkor most kell megváltoztatnia a forrás IP-t.
6. De még mindig nincs vége, most jöhetnek a szabályhoz illő és bekapcsolt alkalmazás és webszűrők (pl. a HTTP filter az példánk esetén).
7. Nos, ha eddig nem állította meg semmi a kérést, akkor ezek után már továbbításra kerül, a TMG VIA header-jével együtt (lásd 8.2).
8. Ezek után a webszerver válaszol. A TMG fogadja ezt, ellenőrzi, hogy a forrás IP valóban az External-ből jön-e (ha nem, akkor spoof packet), és ha szükséges a

cache szabályoknak megfelelően elhelyezi a gyorsítótárban. A NAT miatt újabb IP cím csere történik

9. Továbbítja a választ a kliensnek (+ VIA header újra).
10. A TMG megváltoztatja a connection object állapotát (mivel további csomagot már nem vár), majd 2 percig még él a connection object és ha nincs további kommunikáció, akkor eldobódik. Konyec.



5.20 ÁBRA VAN AKI ÍGY ÉRTI MEG KÖNNYEBBEN

A KAPUN TÚL

Egyetlen dologról kell itt még beszámolni és ez az ún. *Policy Re-Evaluation*, azaz, hogy a változások egy szabály esetén mikor jutnak érvényre. Lényegesen sokat változott ez ügyben a helyzet az elmúlt 10 évben.

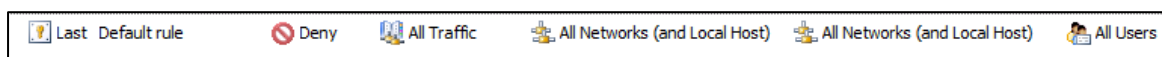
1. Az ISA 2000 esetén egy service újraindítás kellett hozzá.
2. ISA 2004-2006: egy új connection object érvényre jutása kellett hozzá.
3. TMG: *azonnal* megtörténik jut a változás.

Az utóbbiról még annyit, hogy ez egész pontosan azt jelenti, hogy az *Apply* után minden új és minden meglévő anonymous kapcsolatnál azonnal érvényre jut és akkor ha a következő elemek valamelyike vagy mindegyike változik a szabályban:

- Forrás cím és / vagy port
- Cél cím, név, URL stb.
- Időzítés
- User set
- Content Type

5.4 A SYSTEM POLICY

Az alap szentencia az, hogy az ISA és a TMG szervereken a telepítés után minden zárva van, se ki, se be, nincs semmilyen forgalom a telepítés után, még a belső hálózatba se (ez alól kivétel volt az ISA 2000, amely egy teljes körű nyitással megkülönböztette már alapból is az egyetlen, a telepítés közben kiválasztott IP tartományú belső hálózatot). A telepítés után tehát egyetlen látható szabályunk van (ha nem futtatjuk a Web Access Policy Wizard-ot), amely egy minden tiltó szabály.



5.21 ÁBRA MINDEN KAPU BEZÁRVA?

De akkor:

- Miért éri el az TMG a címtárat a telepítés után (azaz pl. beléptethetjük illetve be tudunk lépni rajta a tartományba) ha láthatóan nincs is engedélyező tűzfalszabály a listában?
- Hogyan lehetséges, hogy tudjuk böngészni a <http://www.microsoft.com> címet a TMG gépen egy HTTP engedélyező szabály nélkül?
- Hogyan működhet a Microsoft Update a TMG gépen?

Jópár hasonló kérdést feltehetünk, a válasz minden esetben a System Policy lesz, azaz a gyári, a telepítés után már rögvest életbe lépő szabályok gyűjteménye. Hogyan tekinthetjük meg ezeket? Lépünk a Firewall Policy pontra az MMC-ben, és válasszuk a

View menüből a "Show System Policy Rules" opciót. Ekkor jelentős számú tűzfalszabályt láthatunk, amelynek kb. a fele engedélyezve is van. Ez a titok nyitja.

Persze, pánikra nincs ok, nem "lyukas" gyárilag a rendszerünk, egy-két ártatlan kivételtől (pl. DNS) eltekintve az engedélyezett szabályok maximum a belső hálózatra érvényesek, ezenkívül vannak olyanok is, amelyek bizonyos csoporttagság meglététől függnék (és alapesetben üres ez a csoport). Viszont fontos tudnunk azt is, hogy némely letiltott szabály automatikusan érvényesül, ha a hozzá tartozó funkciót élesítjük, ilyen pl. a szimpla VPN eléréssel kapcsolatos.

A következőkben lépésről lépésre, egyesével átvesszük, hogyan működnek ezek a szabályok, mi mindent engednek vagy tiltanak, és például mely protokollokat használják. Az ISA 2006 Standard változathoz képest igencsak megnőtt ezen szabályok mennyisége, a TMG szintén Standard kiadásánál konkrétan 30-ról 51-re.

5.2 TÁBLÁZAT 51 SZABÁLY KÖVETKEZIK MOST

Ssz.	Alapértelmezés	Szabály neve	Protokoll	Leírás
1	Működik	Allow access to directory services for authentication purposes	LDAP, LDAP (UDP), LDAP GC, LDAPS, LDAPS GC	A címtár és a globális katalógus protokolljainak elérése
2	Működik	Allow remote management from selected computers using MMC	Microsoft Firewall Control (TCP 3847), NetBIOS datagram, NetBIOS Name Service, NetBIOS Session, RPC	Az TMG elérése a telepített MMC bővítménnyel, tipikusan a rendszergazda gépéről. Bár engedélyezve van, de amíg az TMG-n a gyárilag definiált Remote Management Computers csoportba nem tesszük be megfelelő gépet, nem működik.
3	Működik	Allow remote management from selected computers using Terminal Server	RDP	Az TMG elérése RDP-vel, szintén Remote Management Computers csoporttagság kell hozzá.
4	Letiltva	Allow remote management from selected computers using a Web application	TCP 2175	Ugyanaz mint az előző kettő, viszont a hatókör webes alkalmazásokra vonatkozik. Ellenben van még egy különbség: ez a szabály csak az ISA 2006-tól található meg.
5	Letiltva	Allow remote logging to trusted servers using	NetBIOS Datagram, NetBIOS Name	Az SQL szerverbe történő naplózás esetén lesz rá szükségünk

		NetBIOS	Service, NetBIOS Session	
6	Működik	Allow RADIUS authentication from Forefront TMG to trusted RADIUS servers	RADIUS (UDP 1812), RADIUS Accounting (UDP 1813)	A RADIUS hitelesítés engedélyezése adott kiszolgálók felé, az Internal hálózat az alapértelmezett hatókör.
7	Működik	Allow Kerberos authentication from Forefront TMG to trusted servers	Kerberos-Sec (TCP), Kerberos-Sec (UDP)	A Kerberos hitelesítés használatának szabályozása
8	Működik	Allow DNS from Forefront TMG to selected servers	DNS	A DNS protokoll használata az TMG "felől", alapértelmezés szerint a hatókör az All Networks.
9	Működik	Allow DHCP requests from Forefront TMG to all networks	DHCP (Request)	Az TMG DHCP kliensként működéséhez szükséges.
10	Működik	Allow DHCP replies from DHCP servers to Forefront TMG	DHCP (Reply)	Az előző szabály tükörképe.
11	Működik	Allow ICMP (PING) requests from selected computers to Forefront TMG	Ping (ICMP 8)	Az TMG "pingelhetősége", alapesetben csak a Remote Management Computers csoportba tartozó gépeknek. Ha szükség van rá, hogy kívülről is pingelhessük TMG-t ki kell terjesztenünk a hatókört.
12	Működik	Allow ICMP requests from Forefront TMG to selected servers	ICMP Information Request (15), ICMP Timestamp (13), Ping	Különböző hálózati szolgáltatásokhoz szükséges ICMP protokollok és a ping használata az TMG gépen.
13	Letiltva	Allow VPN client traffic to Forefront TMG	Beállításfüggő	A hagyományos VPN kliensek használatára vonatkozik, alapesetben le van tiltva, de amikor az a TMG MMC-ben - első alkalommal - bekonfiguráljuk a VPN elérést, automatikusan engedélyezésre kerül.
14	Letiltva	Allow VPN site-to-site traffic to Forefront TMG	Beállításfüggő	Az VPN S2S szolgáltatásra érvényes, az első élesztése után szintén automatikusan engedélyezésre kerül.

15	Letiltva	Allow VPN site-to-site traffic from Forefront TMG	Beállításfüggő	Az előző tükörképe.
16	Működik	Allow Microsoft CIFS from Forefront TMG to trusted servers	MS CIFS (TCP 445), MS CIFS (UDP 445)	A CIFS protokoll (fájlrendszer) használatának szabályzása
17	Letiltva	Allow remote SQL logging from Forefront TMG to selected servers	MS SQL (TCP 1433) MS SQL (UDP 1434)	Az SQL szerverbe történő naplózás esetén lesz rá szükségünk
18	Letiltva	Allow all HTTP traffic from Forefront TMG to all networks (for CRL downloads)	HTTP	Kivételesen egy az All Networks hálózatra vonatkozó szabály, amely megengedi az TMG kiszolgálónak hogy letöltse a CRL-eket (Certificate Revocation Lists = Tanúsítvány visszavonási lista). Fontos tudnunk, hogy ezzel az TMG-n a HTTP protokollt is megengedtük - minden hálózat felé.
19	Letiltva	Allow HTTP/HTTPS requests from Forefront TMG to selected servers for connectivity verifiers	HTTP/HTTPS	A Connectivity Verification szokatlan, de hasznos bővítmény az TMG szerverekben. A belső hálózat kiszolgálóinak figyelését oldhatjuk meg vele (Ping, HTTP kérések, lekérdezés adott TCP porton, stb.). A hatókör az All Networks, de alapesetben le van tiltva.
20	Letiltva	Allow remote performance monitoring of Forefront TMG from trusted servers	NetBIOS Datagram, NetBIOS Name Service, NetBIOS Session	Ha szándékunkban áll a Performance Monitort használni az TMG-ra kapcsolódva egy másik gépről, akkor kell bekapcsolni ezt a szabályt. Emellett Remote Management Computers csoporttagság is kell hozzá.
21	Működik	Allow NetBIOS from Forefront TMG to trusted servers	NetBIOS Datagram, NetBIOS Name Service, NetBIOS Session	Ha az TMG-ról szeretnénk a belső hálózati fájlszervereket elérni, és ezt máshogyan nem szabályozzuk (pl. egy klasszikus tűzfal szabállyal), akkor ezen az úton megoldható.

22	Működik	Allow RPC from Forefront TMG to trusted servers	RPC	Az RPC protokoll használatának szabályzása
23	Működik	Allow HTTP/HTTPS from Forefront TMG to specified Microsoft error reporting sites	HTTP/HTTPS	Az előredefiniált, ún. Microsoft Error Reporting csoportba tartozó oldalak (*.watson.microsoft.com) böngészése válik lehetővé ezzel a szabállyal.
24	Letiltva	Allow SecurID authentication from Forefront TMG to trusted servers	SecurID (UDP 5500)	A SecurID hitelesítés engedélyezése az TMG-től az RSA ACE kiszolgálók felé (alapból csak az Internal hálózaton).
25	Letiltva	Allow remote monitoring from Forefront TMG to trusted servers, using Microsoft Operations Manager (MOM) Agent	MOM Agent (TCP/UDP 1270) SCOM Agent (TCP 5723)	Az TMG kiszolgálóra telepített MOM/SCOM Agent és a MOM/SCOM szerver közötti kapcsolat engedélyezése (alapból csak az Internal hálózaton illetve egyéb speciális csoportok számára).
26	Működik	Allow installation of System Center Operations Manager Agent	TCP 5724	Az TMG kiszolgálóra szánt SCOM Agent telepítésének engedélyezése, csak speciális csoportok számára
27	Működik	Allow HTTP/HTTPS requests from Forefront TMG to specified sites	HTTP/HTTPS	Ha engedélyezve van, akkor az ún. System Policy Allowed Sites és a MRSS csoportba tartozó oldalakat tudjuk tallózni az TMG szerveren. Ebbe a csoportba tartozik pl. a .microsoft.com, a windows.com és a windowsupdate.com is.
28	Működik	Allow HTTP/HTTPS requests from Forefront TMG to specified sites	HTTP/HTTPS	Ez a szabály a válasz a Microsoft Update-tel kapcsolatos kérdésre. Ha engedélyezve van, akkor az ún. MU-hoz tartozó oldalakat tudjuk használni az TMG szerveren. De ebbe a csoportba tartozik pl. a download.microsoft.com is.

29	Működik	Allow NTP from Forefront TMG to trusted NTP servers	NTP (UDP 123)	Az internetes idősinkronizáláshoz szükséges NTP protokoll engedélyezése. Mivel alapból ez is csak az Internal hálózatra érvényes, érdemes készíteni egy új csoportot a netes időszerverek IP címeivel, majd ennek a csoportnak is engedélyezni.
30	Működik	Allow SMTP from Forefront TMG to trusted servers	SMTP	Az SMTP protokollt engedi meg az TMG-n, de csak az Internal hálózat felé. Erre azért van szükség, mert a különböző figyelmeztetéseket (Alerts) konfigurálhatjuk úgy is, hogy szükség esetén e-mailt küldjön mondjuk az üzemeltetőnek az TMG. Ehhez viszont muszáj, hogy a belső SMTP szervert használni tudja.
31	Letiltva	Allow HTTP from Forefront TMG to selected computers for Content Download Jobs	HTTP/HTTPS	Az TMG szerverek hagyományos szolgáltatása a gyorsítótárba történő időzített HTTP/S Alapesetben le van tiltva ez a szabály, de ha elindítjuk ezt a szolgáltatást, akkor automatikusan engedélyezésre kerül. Az érdekessége még az, hogy szinte ez az egyetlen szabály, amely a felhasználói fiókoktól függetlenül a System és a NetworkService szolgáltatásfiókkal működik.
32	Működik	Allow MS Firewall communication to selected computers	Minden protokoll	Az TMG szerver MMC-n keresztüli eléréshez szükséges, feltétele a Remote Management Computers csoporttagság.
33	Működik	Allow remote access to configuration storage server	TCP 3847, TCP 2171, 2172 és 2174	A TMG-től a Configuration Storage Server felé menő LDAP/LDAPS és a Firewall Access Configuration Control protokollok

34	Működik	Allow access from trusted servers to the local configuration storage server	IKE Client, CIFS (UDP és TCP is), illetve TCP 3847, TCP 2171,2172 és 2174 portok	A tömb tagjai, a Remote Management gépek és pl. a többi CSS gép felől a TMG felé történő forgalom protokolljainak engedélyezése
35	Működik	Allow replication between configuration storage servers	TCP 2173, illetve RPC	A CSS gépek közötti RPC replikáció és szinkronizáció engedélyezése
36	Működik	Allow intra-array communication	SQL, CIFS (UDP és TCP is), illetve TCP 3847 + az RPC	Az Array Server csoport tagjai közötti forgalom engedélyezése
37	Letiltva	Allow IPv6 traffic from Forefront TMG to IPv6 networks	Számtalan ICMPv6 típus	TMG-től az IPv6 hálózatok felé tartó forgalom engedélyezése / tiltása
38	Letiltva	Allow IPv6 traffic from IPv6 networks to Forefront TMG	Számtalan ICMPv6 típus	Az előző tükörképe (mindkettő csak a belső hálózatot érinti)
39	Működik	Allow notifications from Local Host to client computers	TCP 1745	A tűzfal kliens "buboréküzeneteinek" használata
40	Működik	Allow access from Local Host to Forefront Protection Manager server	TCP 9988	A TMG és a Forefront Protection Manager közös használatából fakadó szabály (jelenleg nem igazán használjuk ki)
41	Letiltva	Allow access between Local Host and Forefront Protection Manager gateway	TCP 1961	A TMG és a Forefront Protection Manager közös használatából fakadó szabály (jelenleg nem igazán használjuk ki)
42	Letiltva	Block access from the Blocked Access Computers to the External network	Minden protokoll	A TMG és a Forefront Protection Manager közös használatából fakadó szabály (jelenleg nem igazán használjuk ki)
43	Letiltva	Restrict access from Forefront Protection Manager Limited Access Computers to the External network	Minden protokoll	A TMG és a Forefront Protection Manager közös használatából fakadó szabály (jelenleg nem igazán használjuk ki)

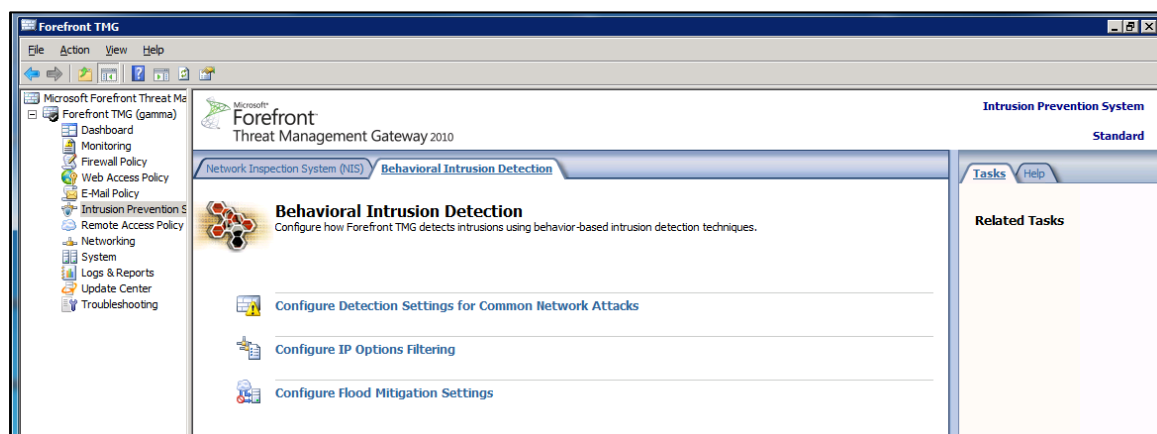
44	Működik	Allow SMTP traffic to the local host for mail protection and filtering	SMTP	Az SMTP forgalom engedélyezése a nyilvános hálózat felől a TMG-nek az Antispam, a Content filtering és a Malware protection szolgáltatások apropóján
45	Működik	Allow SMTP traffic to the Internet for mail protection and filtering	SMTP	Az előző tükörképe (és mindkettő csak a Local Host-ot érinti)
46	Letiltva	SSTP Publishing	-	Érdekes szabály, mert publikálás, méghozzá a Vista SP1/Windows 2008 óta velünk élő speci VPN, az SSTP egyszerű publikálása
47	Letiltva	Allow LDAP/LDAPS traffic to the local host for the Exchange Server EdgeSync synchronization process	LDAP/LDAPS	Az EdgeSync szinkronizálás engedélyezése a TMG-n futó Exchange Edge és belső hálózatban futó Exchange szerver között
48	Letiltva	DirectAccess mode: Allow limited set of IPv6 protocols to Local Host	Számtalan ICMPv6 típus, DHCPv6, LLMNR, IKE Client	IPv6 protokollok engedélyezése a DirectAccess kapcsán
49	Letiltva	DirectAccess mode: Allow IPv6 transition technologies traffic to Local Host	HTTPS, Teredo, IPv6 Over IPv4 Tunnel	IPv6 tranzíciós megoldások engedélyezése a DirectAccess kapcsán
50	Letiltva	Direct Access mode: Allow IPv6 transition technologies traffic from Local Host	Teredo, IPv6 Over IPv4 Tunnel	Az előző tükörképe (és mindkettő csak a Local Host-ot érinti)
51	Letiltva	Direct Access mode: Allow IPv6 traffic from Local Host	Minden protokoll	A TMG és az Anywhere - IPv6 csoport (amelyben minden IPv6 cím benne van) közötti teljes forgalom átengedés
+1	Letiltva	Allow access from trusted computers to the Firewall Client installation share on Forefront TMG	MS CIFS (TCP), MS CIFS (UDP), NetBIOS Datagram, NetBIOS Name Service, NetBIOS Session	Csak az ISA 2004-ben van meg ez az opció, amely ott a 19-es sorszámot viseli. A tűzfal kliensek telepítő mappájának megosztásához (MSPCLNT) szükséges elérést biztosítja, de csak

ha feltelepítjük az ISA ezen szolgáltatását.

5.5 BEHATOLÁS DETEKTÁLÁS, IP SZŰRÉS

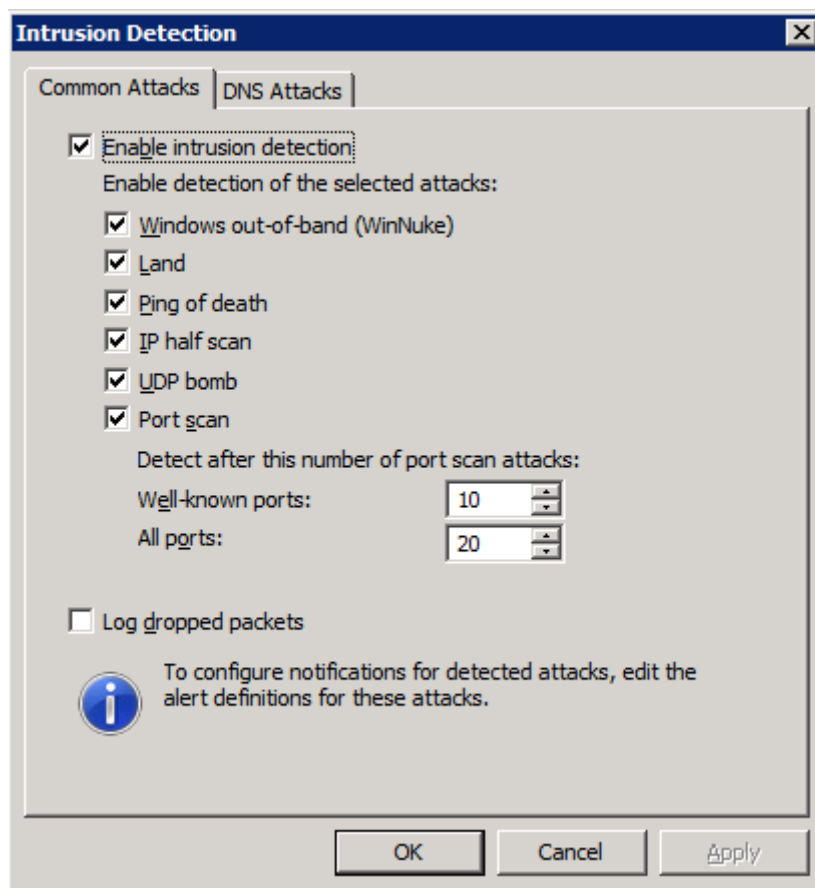
Az általános, ISA 2000-től elérhető képességek közé tartozik a címben szereplő két tétel. Az újabb verziók során történt bővülés a lehetőségekben (pl. a Flood Mitigation az ISA 2006-ban), de az igazán nagy durranás ezen a területen a TMG-ben jött el, ezekkel a következő fejezetben foglalkozunk is részletesen.

De addig is nézzünk bele a faszerkezet Intrusion Prevention System szakaszának második füle alá.



5.22 ÁBRA EZ EGY KEVÉSBÉ LÁTOGATOTT HELY

Az első pontban a TMG behatolás detektálással kapcsolatos tudásának konkrét formáit láthatjuk, nos, ez ügyben nem történt változás 10 év alatt (ez nem azt jelenti, hogy csak ezek ellen véd, hanem azt, hogy ezeket konkrétan felismeri a forgalom elemzésekor). Amikor ezt a listát először láttam (2001), még tetszett és reméltem, hogy egyszer majd, sok-sok frissítés után olyan hosszú lesz ez a lista, hogy vadul kell majd a gördítő sávot használni, de nem ez történt, máshol és máshogy teljesedett ki ez a szakasz. A port szkennelés opciói miatt azért ide is van értelme benézni az indító konfigurálás közben, illetve az eldobott kapcsolatok naplózásának engedélyezése is egy eldöntendő kérdés lesz majd.

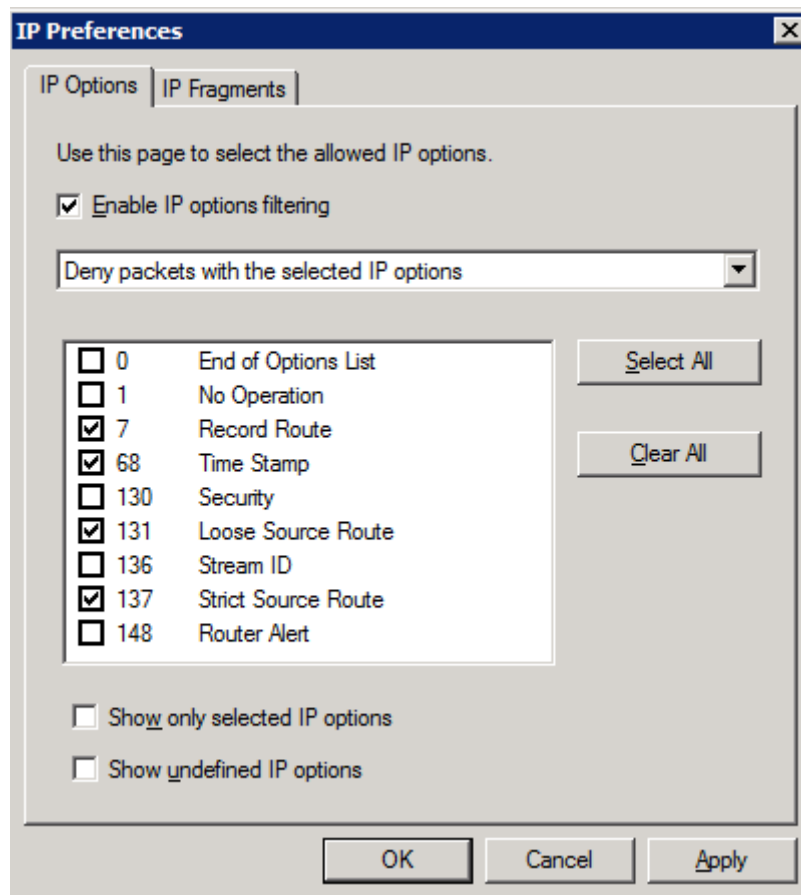


5.23 ÁBRA EZ EGY KEVÉSBÉ LÁTOGATOTT HELY

Ha engedélyezzük, majd bepipáljuk ezeket az ismert támadási típusokat, akkor ezek észlelésekor azonnal egy riasztás keletkezik, amely riasztás tulajdonságai között szerepel majd az is, hogy mi legyen a reakció (pl. kapcsolat bontás, szerviz terminálás, e-mail küldése, sima naplózás, stb.).

A panel második füle alatt a DNS alapú támadási típusokkal kapcsolatos védekezési módszereink láthatóak. Itt viszont az esetleges publikus DNS szerverünket tudjuk térdre kényszeríteni, ha pl. nem engedélyezzük pl. a zónaátvitelt.

Egy másik biztonságfokozó lehetőségcsokor a "Configure IP Options Filtering" szakaszban táruel élénk. Ez a rész a TMG IP csomagkezelésének részleteibe ad betekintést, ami azért egy jóval komplikáltabb és nagyobb erőforrást igénylő dolog, mint ismert támadási típusok elleni védekezés. Ez a panel is két szakaszból áll.

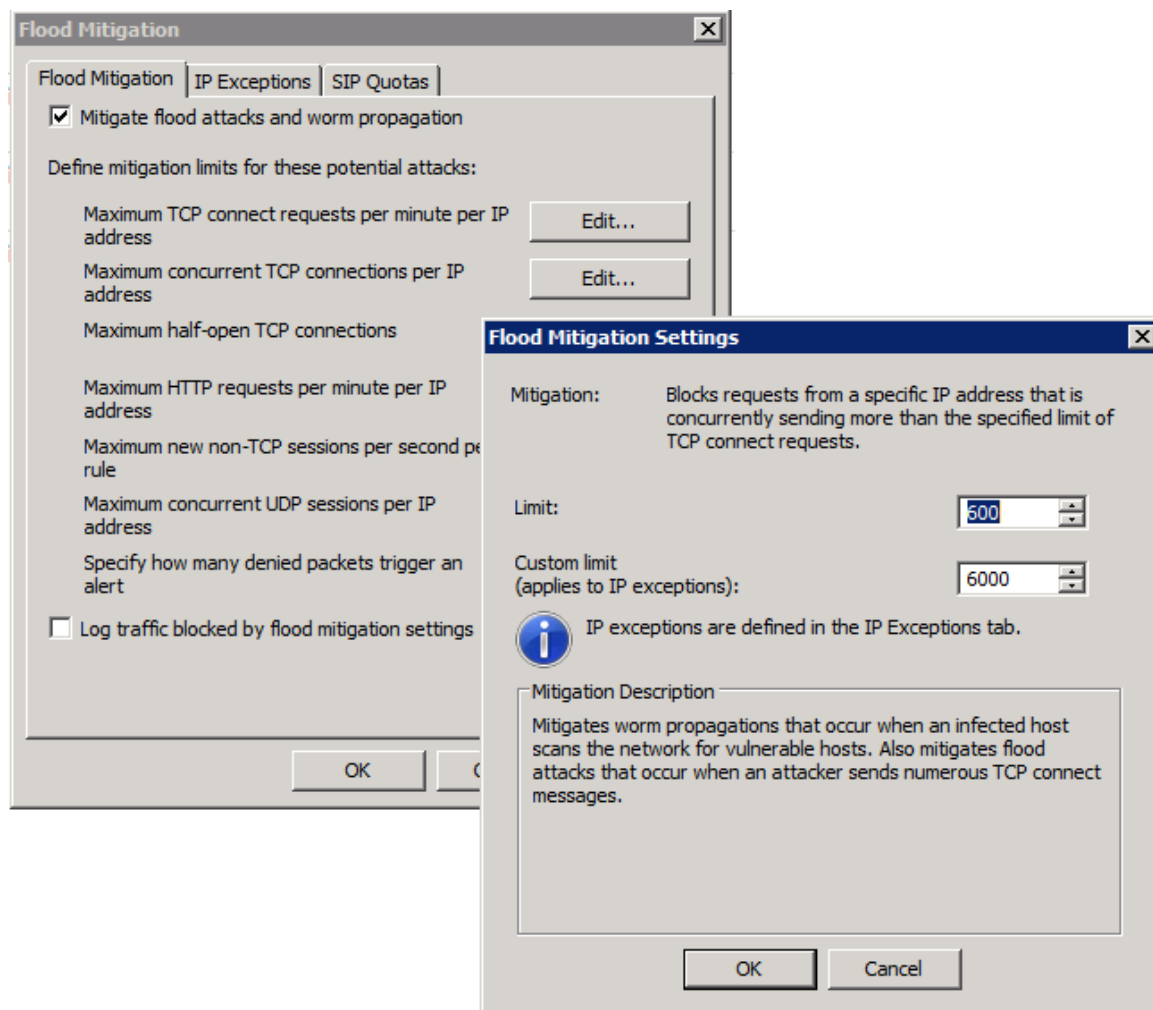


5.24 ÁBRA AZ IP OPCIÓK SZÜRÉSE

Az "IP Options" fül alatt bármilyen a csomag fejlécekben megtalálható opciót megengedhetünk, vagy akár szortírozhatunk is, és ekkor a beállításunk alapján a TMG el fogja dobni azokat a csomagokat, amelyek tartalmazzák a megjelölt IP opciókat. Példának okáért a "source routing" (az IP csomag küldője által meghatározott útvonal kijelölés) hamisítása elleni védekezés lehetősége is itt van. A támadó ugyanis képes a forrás és a cél routerek közötti normális útválasztási döntéseket hamisítani, mi meg képesek vagyunk ezt letiltani (Strict Source Route).

A másik rész, azaz az "IP Fragments" alatt kérhetjük, hogy a TMG az összes széttördelt részeket tartalmazó csomagot eldobja. Elvileg ugyan ezek a töredékek nem károsak, és csak azért kerülnek tördelésre, mert túl nagyok, és így egyetlen csomagba nem férnek bele. Azonban létrehozhatóak olyan töredékek is, amelyek önmagukban, első látásra ártalmatlannak tűnnek, ellenben összerakva már nem egészen, vagy jobb esetben az összerakás során csak az derül, ki róluk, hogy szabálytalanok/hibásak, és ezért pl. túlterhelést okoznak (teardrop). A dolog másik oldala viszont az, hogy streaming audio és video vagy pl. L2TP over IPSec esetén magunknak okozhatunk problémát, ha blokkoljuk a töredék csomagokat.

Már csak egyetlen rész maradt, a Flood Mitigation. Itt granulárisan szabályozhatjuk a TCP/UDP és HTTP kérések percenkénti számát, ráadásul két fokozatban.



5.25 ÁBRA FLOOD MITIGATION RÉSZLETEK

Egyrészt létezik egy általános kör, ezenkívül az IP Exceptions alatt megadhatjuk azokat az IP címeket (számítógép-csoportok formájában), amelyek kivételek, és amelyekre külön értékeket állíthatunk be (de csak globálisan, nincs további differenciálás). Ha pl. azt látjuk, hogy a belső hálózatban egy-egy kliens indokolható módon több kapcsolatot akar kiépíteni, mint amennyit általában megengedünk, akkor kivételt tehetünk vele – de nem muszáj akármeddig elengednünk azért, egy felső határt egyszerűen kijelölhetünk ebben az esetben is.

6 A TŰZFAL A TMG-BEN

6.1 EGY NAGYÁGYÚ: A NIS

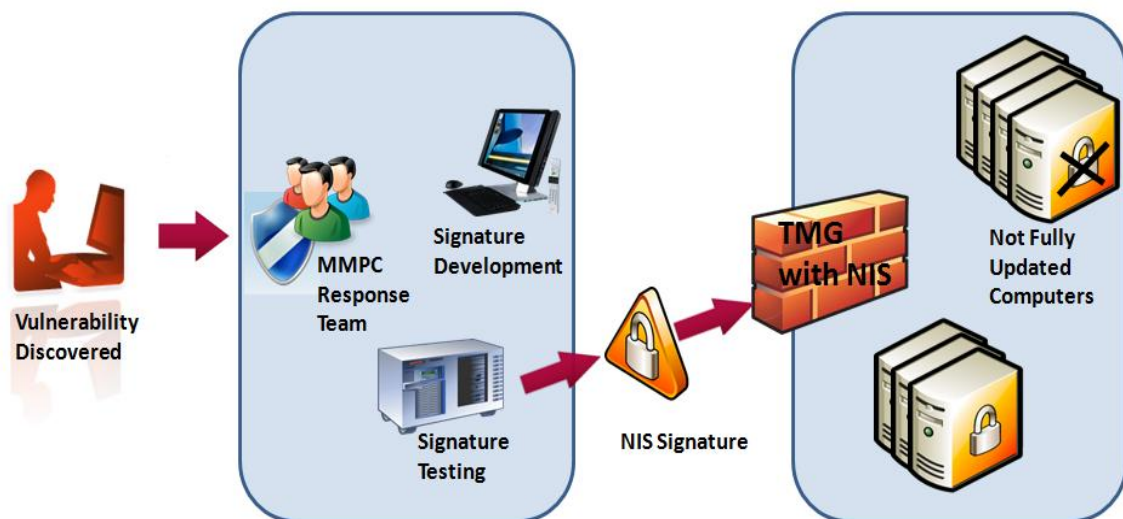
Sok-sok újdonság van a TMG tűzfal szerepkörének háza táján, de ezek közül is kiemelkedik egy teljesen innovatív megoldás, amely ott segít, ahol a „legjobban fáj”, azaz a hálózat gépeinek biztonsági állapotának fokozásában. A frissítések gyors terítése és alkalmazása kötelező feladat minden hálózatban, de ennek sikerességébe sok tényező beleszólhat, most ez a sok, eggyel csökkenhet a TMG révén. Ahhoz, hogy a rendszergazdák, folyamatosan up-to-date állapotban tartsák a védett hálózat operációs rendszereit illetve alkalmazásait régóta vannak megfelelő eszközök egy Windows hálózatban, a Windows/Microsoft Update-től kezdve a WSUS-on át olyan komplex rendszerfelügyeleti eszközökig, mint a kisvállalatok számára készült System Center Essentials, vagy éppen nagyvállalatok számára alkalmas System Center Configuration Manager.

De sajnos van több aktuális probléma is ezen a területen. Az egyik első az, hogy a frissítések tesztelése és korrekt alkalmazása már egy közepes méretű hálózaton is jelentős időbe kerülhet, ergo elképzelhető, hogy egy-egy munkaállomásra vagy kiszolgálóra csak jelentősen késve kerül a javítás. Egy másik probléma az, hogy a másik oldalon, azaz a Microsoftnál is előfordul, hogy a javítás tökéletesítése és tesztelése (amely - értelemszerűen - lényegesen alaposabb mint a felhasználói oldalon), szintén jelentős időt emészt fel, így előfordulhat, hogy a sérülékenységi felfedezése után csak hetekkel érkezik meg (azaz válik nyilvánossá!), és válik letölthetővé az adott javítás. Mindeközben - a versenyfutás részeként-, a sérülékenységi kihasználásra történő exploit fejlesztése közel sem vesz el ennyi időt, és aztán sok esetben így sikeresen alkalmazható, akár rövid határidőn belül is.

Egy másik probléma az, hogy előfordulhat az az eset, amikor az iparági egyezményektől eltérő módon egy sérülékenységet annak felfedezője nem a gyártóval, esetünkben a Microsofttal - közöl először, hanem nyilvánosságra hozza, még hozzá azonnal. A sérülékenységek felfedezéséről és annak javításáról az iparág egyöntetűen gondolkodik. A korábban említett szándék minden esetben ártó szándék. Ezeket az eseteket hívjuk o napos sérülékenységeknek. Bizonyos esetekben o napos exploit-ról is beszélhetünk, amikor a nyilvánosságra hozás során úgy nevezett *proof of concept* kódot is közöl a támadó. Hogy értsük miért baj ez, értenünk kell a rosszfiúk működését. Három kategóriája van a sérülékenységeket kihasználó kódok készítésének (figyelem, ez iparági trend, nem csak a Microsoft-ra igaz):

- Egy biztonsági kutató talál egy hibát, amit jelez a gyártónak. A gyártó elkészíti a javítást, amit nyilvánosságra hoz, a kutatónak fejet hajtva. Hogy lesz ebből támadásra alkalmas kód? Úgy, hogy a hotfix csomagot amit kiad a gyártó, azt a támadók elemzik, abból megállapítják, hogy mit javított a gyártó és azt hogyan lehet a még javítatlan gépeken kihasználni. Ennek az ideje napjainkra erősen lecsökkent. Pár óráról beszélünk csak, míg ez a 2001-2002-es CodeRed, Nimda Blaster, Sasser időszakában több hétben mértük.
- A biztonsági kutató talál egy hibát, amit kihasználó kártékony kódot készít és azt nyilvánosságra hozza. Ebben az esetben nem javító hanem ártó szándék vezérli a kutatót.
- A biztonsági kutató talál egy hibát, amit kihasználó kártékony kódot készít, de azt nem hozza nyilvánosságra, hanem célzott támadásokat hajt vele végre. Ha ügyes, soha nem derül ki. Ha közepesen ügyes, akkor egyszer kiderül (a közelmúlt egyik ilyen emlékeztető eseménye amikor a Google rendszereihez fértek hozzá egy böngésző sérülékenységen keresztül). *(A lektor megjegyzése.)*

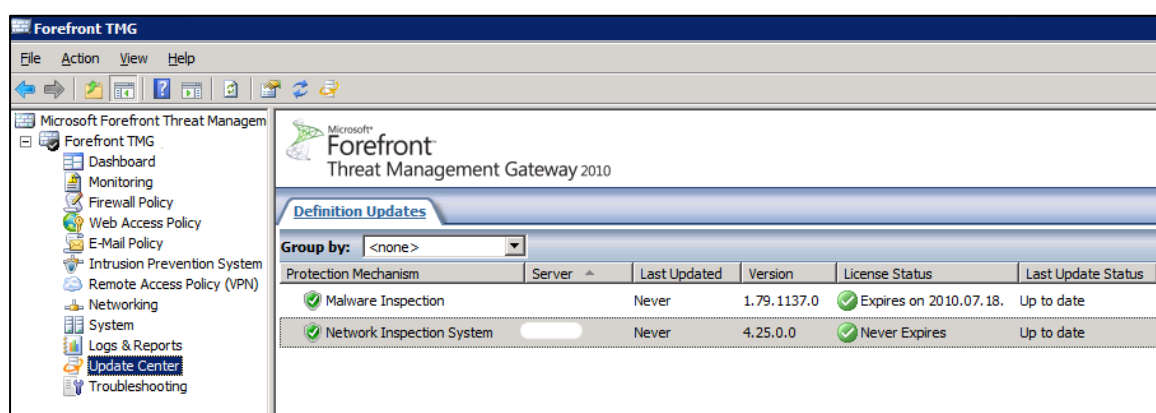
A TMG-be integrált NIS (Network Inspection System) pontosan itt segít, mivel képes arra, hogy az tűzfalon átmenő forgalom alapos elemzése során⁵⁰ felismerje az ismert sérülékenységet kihasználó támadásokban alkalmazott jellemző szignatúrákat, és ezek után blokkolja az adott host felé menő forgalmat. Azaz egy támadó akkor sem képes kihasználni egy adott hibát, ha még nem frissítettük a host gépet, hiszem a kísérlet már a hálózatunk határán robotoló TMG szervernél elakad.



6.1 ÁBRA EZ EGY KÖR, CSAK NEM ÚGY NÉZ KI

⁵⁰ És persze a TMG protokoll engine illetve az alkalmazás- és webfilterek áldásos tevékenysége után.

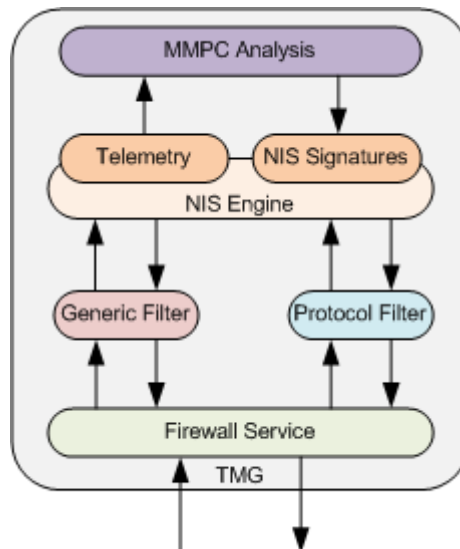
De mi a helyzet a NIS esetén a gyorsasággal? A hetek helyett itt órákról beszélünk, azaz a sérülékenység felfedezése után a Microsoft Malware Protection Center (MMPC; <http://www.microsoft.com/security/portal/>) munkatársai azonnal hozzáfesznek a jellemző lenyomat elkészítéséhez, ellenőrzéséhez és teszteléséhez, és még aznap bizonyosan ki is adják a szignatúrát. A NIS frissítési mechanizmusa pedig lehetővé teszi, hogy akár direktben a Microsoft Update, akár a rendszerünkben már megtalálható WSUS/SCE/SCCM segítségével frissüljön helyben is a NIS adatbázisa, és blokkolható legyen a rosszindulatú forgalom. Erre már több konkrét esetet is felhozhatunk bizonyítékképpen, például a sansnál (<http://www.sans.org/>) 2009. szeptember 8-én megjelent SMBv2 sérülékenység apropóján kiadott lenyomat kevesebb mint 8 óra alatt bekerülhetett a TMG NIS adatbázisba (pedig ekkor még béta állapotú volt a termék).



6.2 ÁBRA A NIS FRISSÍTÉS NEM ELŐFIZETÉSHEZ KÖTÖTT, AZAZ INGYENES ÉS SOSEM JÁR LE

Az MMPC egyébként nyomoz is, tehát a felfedezés folyamatának is lehet részese és igazából - tetszés szerint - a TMG üzemeltetők is, hiszen a Telemetry Reporting Service engedélyezésével a malware vagy egyéb támadási típusokról, illetve a hálózati forgalommal kapcsolatos működési anomáliákról egyaránt szolgáltatható információ a Microsoft felé (természetesen SSL kapcsolaton keresztül), minden egyes a TMG-t futtató gépről.

A NIS „motorháztetejét” felnyitva egyébként egy bonyolult, sok komponensből álló rendszer részeként a GAPA protokoll elemző platformra (és benne a GAPAL protokoll leíró nyelvre) bukkanunk, amely a Microsoft Research (<http://research.microsoft.com/en-us/>), azaz a Microsoft házon belüli tudományos-kutató részlegének „találmánya”. Ezt aztán a TMG fejlesztőcsapata egészítette ki és tökéletesítette, illetve beleillesztette és beleilleszti most is szinte minden Forefront termékbe.



6.3 ÁBRA A NIS MŰKÖDÉSI MECHANIZMUSA

A GAPA keretrendszer a klasszikus protokoll elemzőkkel szemben számos előnnyel rendelkezik, és például az egyszerű protokoll parser fejlesztést is segíti, így az ellenőrző szabályok és a szignatúrák alkalmazása nagyságrendekkel gyorsulhat.

Network Intrusion System (NIS) Behavioral Intrusion Detection

NIS Status: Enabled
Signature Set Version: 4.25 (2010.04.01.)

New Signature Response: Microsoft default policy
Update Action: Check for and install definitions

Group by: Attention Required Group sort order: Descending

Name	Attention ...	Status	Response	Policy Type	Date P...	Related Bulletins
Unflag (no attention required)						
Exploit:Win/HTTP.URL.XSSI0000-0000	Unflag (...)	Enabled	Detect only	Default	2010.03.30.	NA
Exploit:Win/HTTP.URL.SQLInj0000-0000	Unflag (...)	Enabled	Detect only	Default	2010.03.30.	NA
Vuln:Win/SMB.mrxSMB.RCE!2010-0016	Unflag (...)	Enabled	Block	Default	2010.02.09.	MS10-006
Exploit:Win/MSIE.ActiveX.RCE!2010-0252	Unflag (...)	Enabled	Block	Default	2010.02.09.	MS10-008
Plcy:Win/SMB.NegotiateResponse.RC...	Unflag (...)	Disabled	Detect only	Default	2010.02.09.	MS10-006
Vuln:Win/SMB.Srv.DoS!2010-0020	Unflag (...)	Enabled	Block	Default	2010.02.09.	MS10-012
Plcy:Win/SMB.SRV.DoS!2010-0022	Unflag (...)	Disabled	Detect only	Default	2010.02.09.	MS10-012
Plcy:Win/HTTP.FileExtension.MisConfi...	Unflag (...)	Disabled	Detect only	Default	2009.12.23.	
Plcy:Win/HTTP.Parser.DoS!0000-0000	Unflag (...)	Disabled	Detect only	Default	2009.12.08.	NA
Vuln:Win/WebServer.ADFS.RCE!200...	Unflag (...)	Enabled	Block	Default	2009.12.08.	MS09-070
Vuln:Win/WebServicesOnDevices.WS...	Unflag (...)	Enabled	Block	Default	2009.11.12.	MS09-063
Vuln:Win/MSRPC.LLSRPC.RCE!2009-2...	Unflag (...)	Enabled	Block	Default	2009.11.10.	MS09-064
Vuln:Win/MSRPC.LSASS.RCE!2009-2...	Unflag (...)	Enabled	Block	Default	2009.10.13.	MS09-059
Exploit:Win/MSIE.Wininet.RCE!2009-1547	Unflag (...)	Enabled	Block	Default	2009.10.13.	MS09-054
Vuln:Win/SMBv2.Command.RCE!2009...	Unflag (...)	Enabled	Block	Default	2009.10.13.	MS09-050
Vuln:Win/SMBv2.DFS.DoS!2009-2526	Unflag (...)	Enabled	Block	Default	2009.10.13.	MS09-050
Vuln:Win/SMB2.SRV2.RCE!2009-3103	Unflag (...)	Enabled	Block	Default	2009.09.08.	MS09-050
Exploit:Win/MSIE.HelpActiveX.RCE!200...	Unflag (...)	Enabled	Block	Default	2009.08.10.	MS02-055
Exml:Win/MSIE.FlexGrid.RCE!2008-4254	Unflag (...)	Enabled	Block	Default	2009.08.07.	MS08-070

NIS Tasks

- Activate Latest NIS Signature Set
- Configure Properties
- Define Exceptions
- Set All Responses to Microsoft Defaults
- Set All Responses to Detect Only

Selected Signature Tasks

- Configure Signature Properties
- Disable Selected Signatures

Related Tasks

- Link to Update Center
- Link to Microsoft Malware Protection Center

6.4 ÁBRA A NIS AZ IPS SZAKASZON BELÜL: EGY SOR, EGY ISMERŐS ATTAK

Felmerülhetnek még további kérdések is, azaz hogy vajon minden protokoll védelmére felkészült-e a NIS, illetve, hogy csak a Microsoft által kiadott frissítések „előszavának”

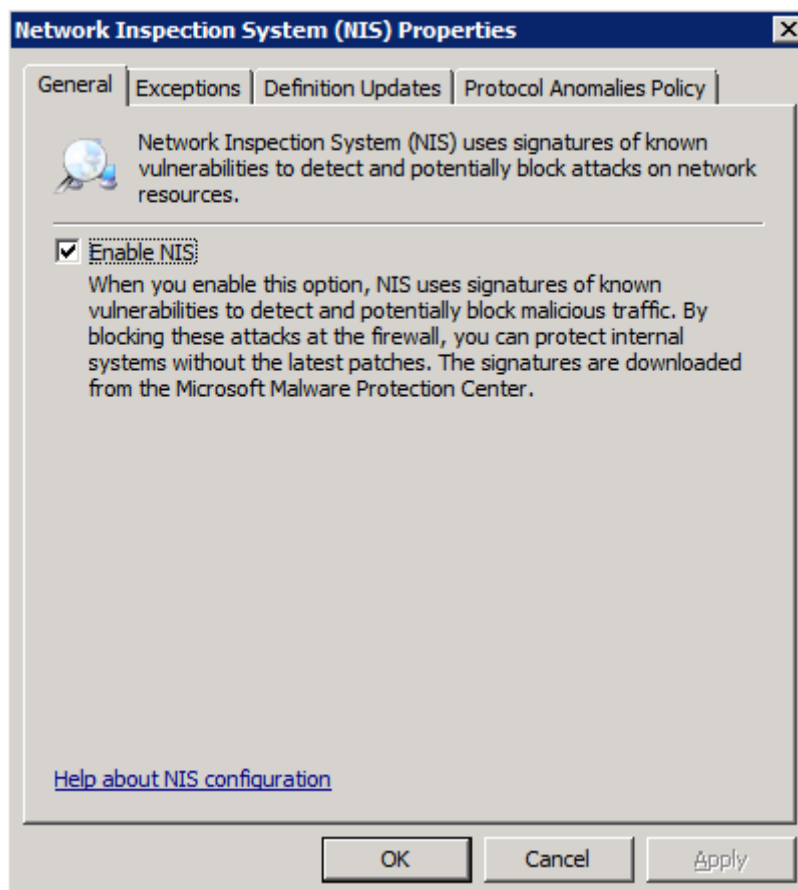
tekinthető-e? A válasz egyrészt az, hogy az közismert protokollok jelentős részét lefedi ez a megoldás (konkrétan: HTTP/S, DNS, SMB, SMB2, NetBIOS, MSRPC, SMTP, POP3, IMAP, MIME), illetve a kérdés második felét illetően pedig azt kell tudnunk, hogy a TMG *jelen* verziójában (SP1, 2010. szeptember) szereplő NIS, egyelőre valóban csak a Microsoft által kiadott frissítésekhez passzol, azaz csak a vállalat szoftvereire érvényes a hatása. Nos, a röpke áttekintés után viszont nézzük meg a konkrét részleteket.

Azt viszont ki kell emelni, hogy a NIS egy GAPA csomagot kap amikor frissíti önmagát. A GAPA csomag azonban nem csak a sérülékenységek leírását tartalmazza, hanem a Protocol par ser objektumokat is. Tehát egy egyszerű NIS update segítségével:

1. Frissülnek a már fent levő par ser objektumok.
2. Érkezhetnek új protokollok - és érkezni is fognak folyamatosan.

6.1.1 NIS RÉSZLETEK

Ha az MMC-ben betallózzuk a NIS ablakát, akkor a konkrét támadási formákat leíró sorok uralják a képernyőt. Ezek felett a TMG-ben már más helyen is látható, fejlécszerűen elhelyezkedő legfontosabb jellemzők találhatók meg, a jobboldali keret meg szintén szokásos: az aktuálisan végrehajtható feladatok (NIS Tasks) sorakoznak itt. Ugorjunk a fejlécbe, és nyissuk meg a "NIS Status: Enabled" hivatkozást.

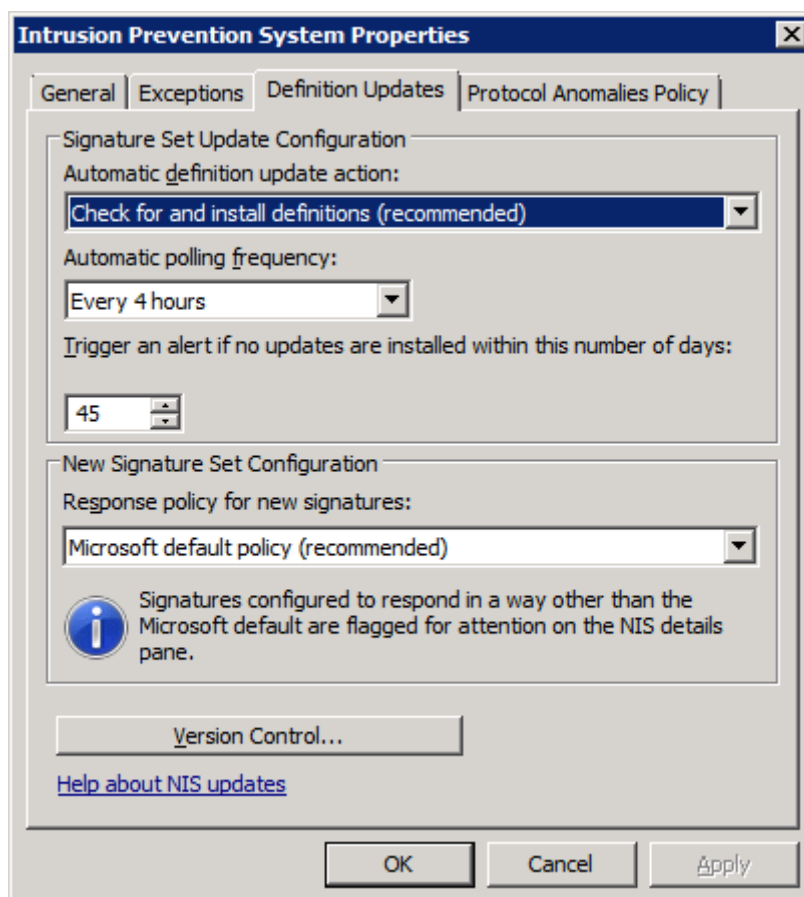


Az elején egyszerű a dolgunk, engedélyezhetjük a NIS-t, vagy nem. Ehhez maximum arra a háttérinfóra van szükségünk, hogy a NIS (a GAPA miatt) azért generál plusz terhelést. A hivatalos dokumentációk szerint egy átlagos típusú forgalom⁵¹ esetén a NIS kb. 30%-nyi plusz elvárást jelent a CPU-tól (abban az esetben ha a Malware Inspection is engedélyezve van). Persze ez sok mindentől függhet, pl. a hardver konfigurációtól, a NIS beállításaitól és persze még attól is, hogy mi mindent csinál az OS a TMG alatt. De kiindulásnak mindenképpen jó érték ez, vegyük figyelembe a tervezésnél mindenképpen.

A következő fül az Exceptions, amely szintén nem okozhat komoly gondot, mivel a kivételekről szól, azaz ha bármilyen okból ki szeretnénk vonni bizonyos gépeket a NIS hatása alól, akkor ezt pl. domain nevek formájában megtehetjük. Vagy éppen felhasználhatjuk az alapértelmezett "Sites Exempt from NIS" csoportot is erre (amelyben a megszokott *.microsoft.com címek már megtalálhatóak). Vagy – pl. ha belső gépekről van szó – akkor egy IP címtartományt is felvehetünk.

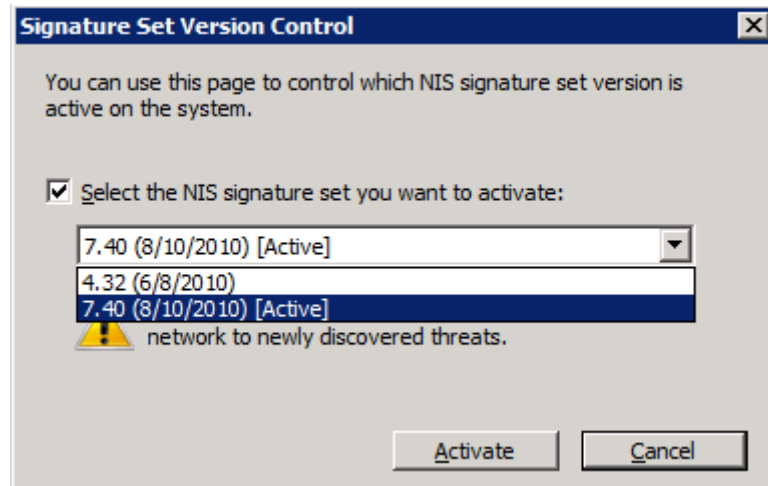
A következő rész viszont már sokkal izgalmasabb. Ez a Definition Updates, és itt már rengeteg mindent beállíthatunk.

⁵¹ Csak az érdekesség kedvéért az átlagos forgalom megoszlása a Microsoft szerint a következő: HTTP: 80%; SIP: 8%; FTP: 5%; DNS: 5%; SMTP: 2%.



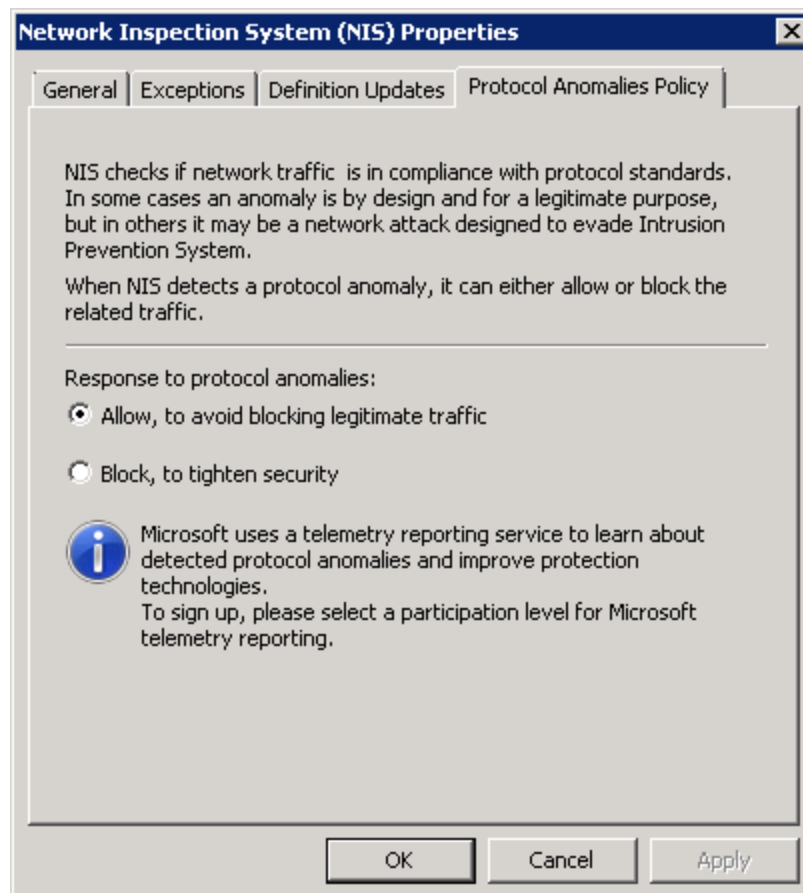
6.6 ÁBRA FRISSÍTÉSEK, REAKCIÓK ÉS VERZIÓK

- **Automatic definition update action:** Hogyan történjen a NIS szignatúra adatbázisának frissítése? Azaz automatikusan figyelje-e és telepítsen, vagy csak figyelje (de nincs letöltés és telepítés sem), vagy éppen ne legyen semmilyen automatizmus.
- **Automatic Polling Frequency:** Milyen sűrűn történjen meg a frissítések ellenőrzése? Ez az intervallum 15 perctől 4 óráig állítható, több fokozatban.
- **Response policy for new signatures:** Mi legyen a NIS reakciója, akkor ha a forgalom ellenőrzése során belefut egy ismert szignatúrába?
 - o Csak detektálás és naplózás, de nincs blokkolás
 - o Microsoft Default Policy: ez az alapértelmezés (később kifejtem)
 - o No Response: nincs reakció
- **Version Control:** Az aktuálisan letöltött és telepített szignatúra csomag automatikusan aktiválásra kerül, azonban adódhat olyan eset (pl. tesztelés), amikor egy régebbi állapotra van szükség. Itt visszamehetünk az időben és aktiválhatunk egy régebbi csomagot, figyelmen kívül hagyva a jelenlegit.



6.7 ÁBRA UNDO?

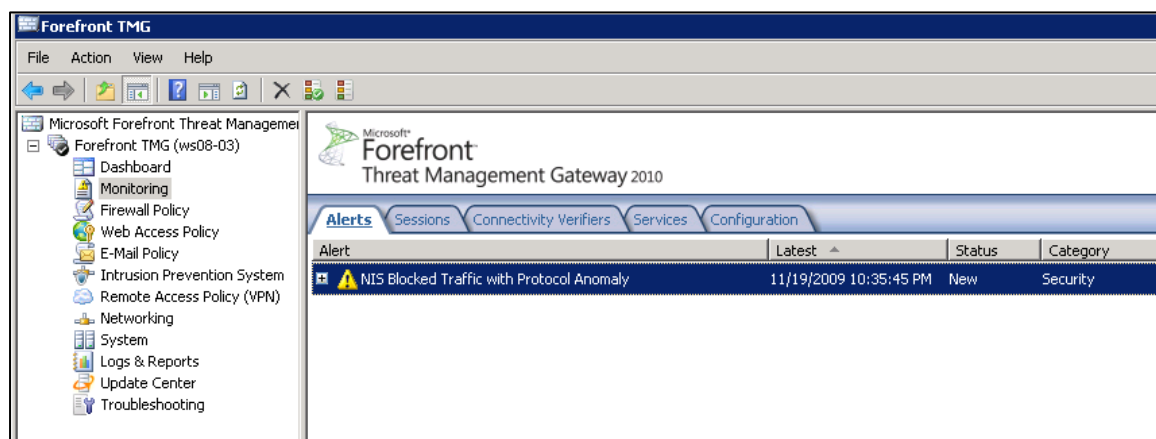
A következő fül a "Protocol Anomalies Policy", ami megint csak egy érdekes, kifejezetten innovatív, és a GAPA-nak köszönhető megoldást takar. A dolog lényege, hogy ha már úgyis az összes forgalmat bitenként és valós időben figyeli a TMG, akkor miért ne figyelje azt is egyúttal, hogy minden kommunikáció a protokolldefiníciókban meghatározott teljesen szabályos módon történik-e?



6.8 ÁBRA BE TETSZIK TARTANI PÉLDÁUL AZ RFC AJÁNLÁSOKAT?

A KAPUN TÚL

Azaz, vannak-e olyan anomáliák, amelyek ugyan nem ismert ártó kódok, de azért gyanúsak? Mondok egy egyszerű és sarkított példát: ha bekapcsoljuk ezt a lehetőséget (az alapértelmezett állapot nem ez!), akkor ha egy HTTP forgalomban egy GET kérés után a HTTP verzió "1.2", akkor a NIS blokkolja ezt a forgalmat (mivel a szabvány szerint az 1.1-nél tartunk) és dob egy riasztást.



6.9 ÁBRA ITT NEM SIKERÜLT...

6.1.2 A SZIGNATÚRÁKRÓL MÉG EGY KICSIT

Ahogy mostanra már bizonyára kiderült, a NIS működési kereteit a szignatúrákkal határozzuk meg. Ezek az MMPC szakemberei által kreálható lenyomatok gyakorlatilag forgalom karakterisztikai leírások⁵², és kizárólag ebből a forrásból érkehetnek, méghozzá a Microsoft Update (vagy a WSUS) segítségével, viszont az ún. "Signature set"-ek formájában. A 6.7-es ábrán ezekből láthatunk kettőt.

Name	Attention Required	Status
Plcy:Win/XMLCore.Location.RCE!2006-4685	Flag for attention	Disabled
Plcy:Win32/NIS.Signature.Test!		Enabled
Vuln:Win/ActiveX.DXImgTransfo		Enabled
Vuln:Win/ASP.NET.InfoDisc!2007-		Enabled
Vuln:Win/ASPNET.URI.InfoDisc!2006-1300	Flag for attention	Enabled

6.10 ÁBRA KÜLÖN-KÜLÖN IS SZABÁLYOZHATÓAK, DE A SHIFT ÉS A CTRL IS MŰKÖDIK

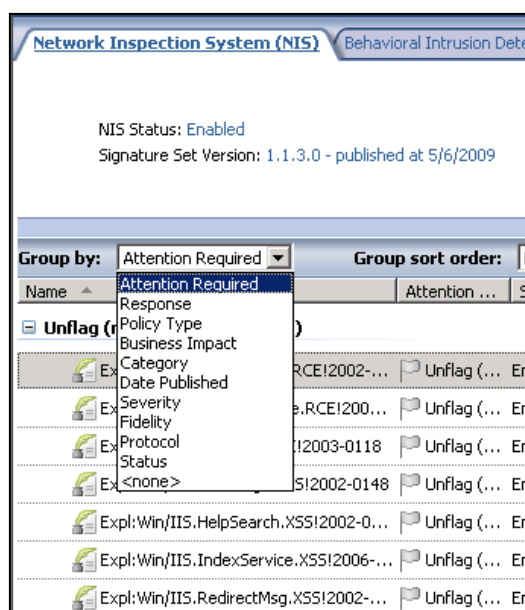
A szignatúrák négyfélék lehetnek, és hogy a NIS listájában melyik milyen, az az adott sor legelső karaktereiből egyértelműen kiderül:

1. A vulnerability típus (Vuln), amelyek az adott sérülékenységet kihasználó kód legtöbb, általános formáját detektálja.

⁵² Például ha jön egy GET kérés, ami a default.ida fájlt hívja és a mérete nagyobb mint X és a második paraméter mérete nagyobb mint Y, akkor az CodeRed.

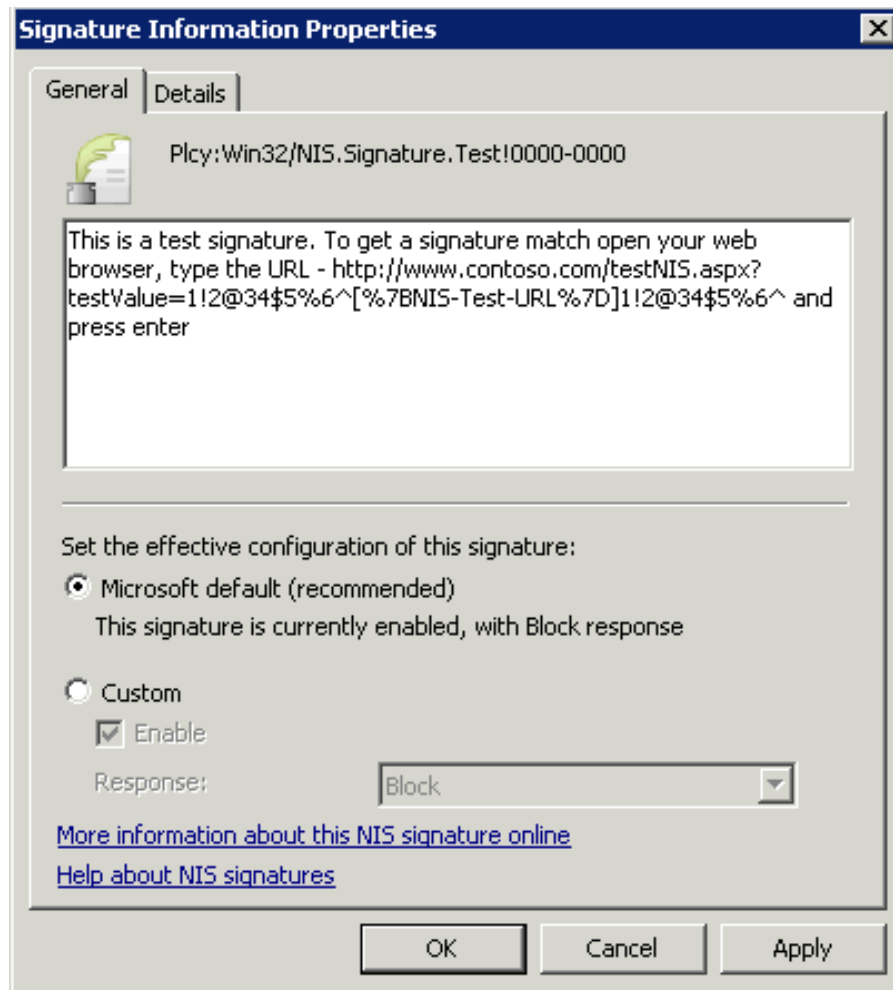
2. Az exploit típus (Expl:), amely egy adott sérülékenységre passzoló egyedi kódot detektálja.
3. A policy típus (Plcy), amelyek általában az auditálási előny miatt kerülnek be a gyűjteménybe (de később követheti majd egy exploit vagy vulnerability típusú blokkoló szignatúra), és amelyek kivétel nélkül le is vannak tiltva.
4. A teszt típus (Test), amelyek nevükhöz híven a NIS tesztelést segítik, és amelyekből összesen 3 db van (két SMB és egy HTTP).

A NIS sokoldalúan és granulárisan enged meg nekünk szabad kezét a szignatúrákkal kapcsolatos műveletekben, mind a kulcsint, mind a működést illetően .



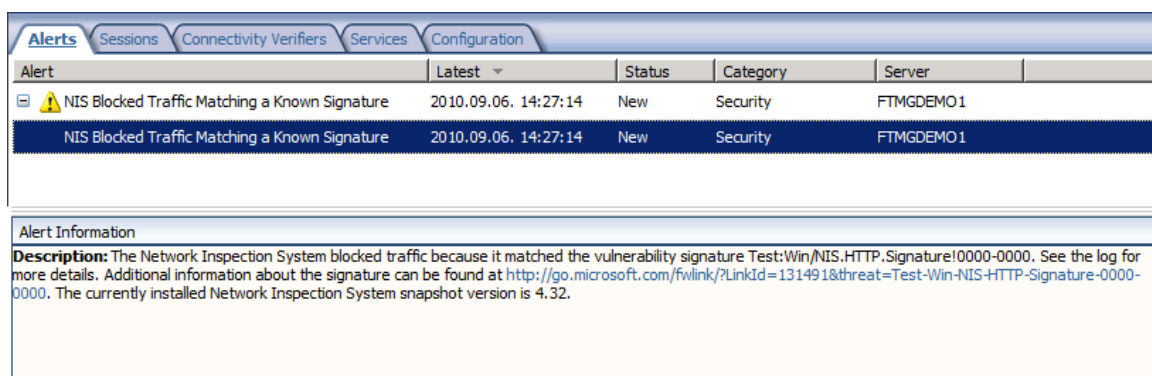
6.11 ÁBRA KÜLÖN-KÜLÖN IS SZABÁLYOZHATÓAK, DE A SHIFT ÉS A CTRL IS MŰKÖDIK

A NIS Tasks alatt lehetőségünk van aktiválni, egyetlen paranccsal az összes jelenlegi és jövőbeni szignatúra kapcsán a NIS reakcióját befolyásolni (pl. csak detektálásra behangolni). Mindegyik lenyomat egy ajánlott érvényesítéssel érkezik az MMPC-től, de akár egyesével, akár többenél is egyszerre felülbírálhatjuk ezt (ami - ha úgy gondoljuk - semmilyen módon nem befolyásolja majd a később érkező lenyomatok gyári ajánlását).

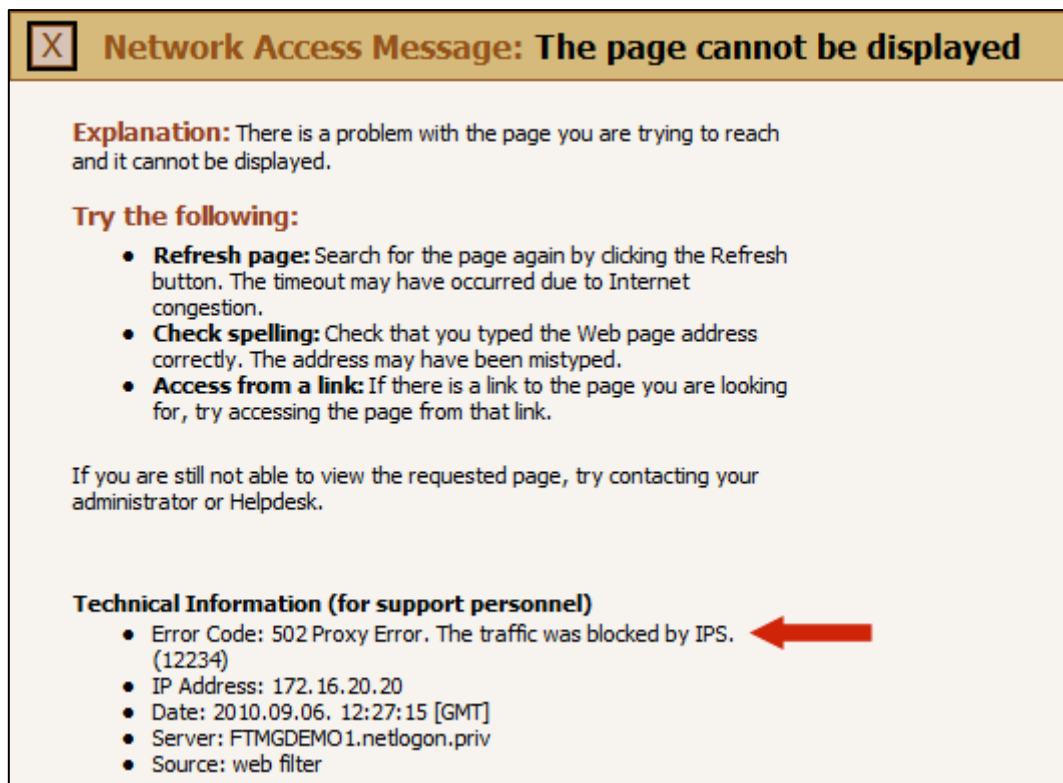


6.12 ÁBRA EZ EGYIK RENDHAGYÓ, TESZT SZIGNATÚRA

Nézünk meg most egymásután két darab ábrát, amelyeken egyrészt azt rögzítettem, hogy mi történik a felhasználó böngészőjében ha belefut a NIS hatókörébe, másrészt milyen nyoma lesz ennek a TMG riasztások között.



6.13 ÁBRA EGY NIS RIASZTÁS



6.14 ÁBRA ÉS AMIT A USER LÁT A NIS-BŐL

E fejezet lezárása alkalmából még ismerkedjünk meg a NIS Encyclopedia-val, amely gyakorlatilag egy webes adatbázis a Microsoft Malware Protection Portal-on (<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Browse.aspx>).

Itt viszonylag egyszerűen utánanézhethetünk a NIS szignatúrákkal kapcsolatos információknak is, amit egyébként egyszerűbben is megtehetünk, ugyanis minden egyes lenyomatra duplán kattintva az előző képen is látható "More information about this NIS signature online" link is rendelkezésre áll.

6.2 ISP REDUNDANCY

Ismerjük a www.isaserver.org oldalt? Esetleg a fórumot is tallóztattuk régebben? Ha igen, akkor biztosan emlékszünk a "Wish List" szálra, amelyben (mint a mesében) maximum hármat lehetett leírni azok közül a képességek és szolgáltatások közül, amelyeket szeretnénk majd viszontlátni a következő ISA szerverben. No nem mintha ezen múlna (és ma már ez a fórum se pörög), de az biztos, hogy az amit ISP-R néven rövidítve pakolt bele a Microsoft a TMG-be, az mindig benne volt a Top3 kívánságban.⁵³

⁵³ Emlékeim szerint a másik két többnyire vezető kívánság a sávszélesség szabályzás (no nem az ISA2000-es, és nem is a DiffServ, hanem egy tényleg használható), illetve a frissülő, kategorizált URL szűrés volt. De a SIP támogatásnak is sokan szurkoltak. E három pluszból is megvan még kettő, ergo haladunk ☺

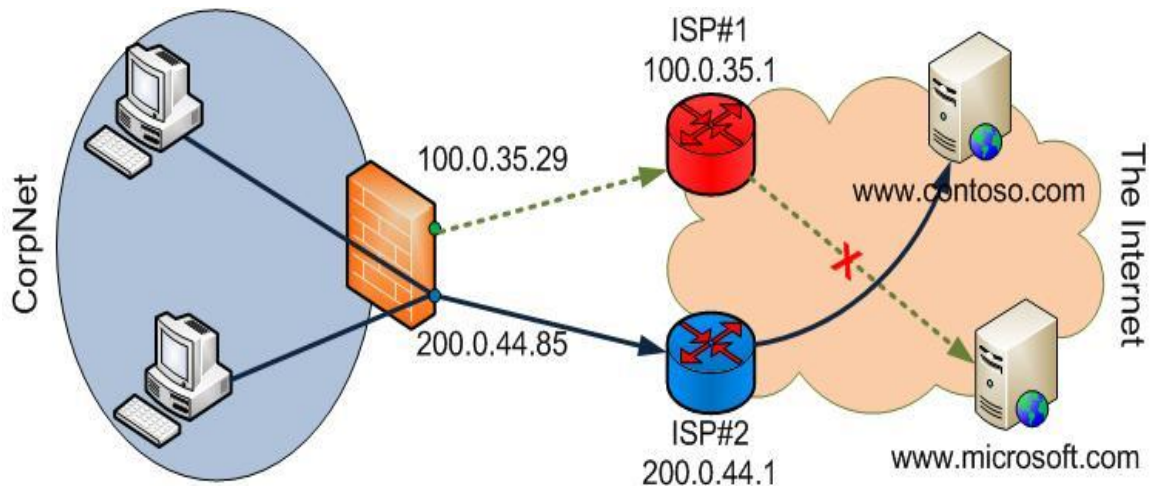
Szóval igen régóta várunk már arra, hogy a különböző netes kapcsolatainkat (azaz több External hálózatot, azaz maximum kettőt!) kezelni tudja az ISA Server-ünk. Nos az már nem fogja, de a TMG igen, és ez nem valami plusz nagyvállalati képesség, hiszen a Standard kiadás is tartalmazza ezt a lehetőséget.

Használati előfeltétel nem sok van, legyen két vonal (célszerűen routerekkel, tehát nem modemekkel, PPPoE alapon ugyanis nem megy), tudjuk ezek alapadatait, default gateway, netmask (ezeknek teljesen különbözőeknek kell lenniük), tudjuk, hogy adott esetben majd melyiket szeretnénk elsődlegesnek, illetve a második kapcsolat előzetes beállításaképp egészítsük ki a hálózati listánkat, mondjuk egy External2 nevűvel, amelyhez természetesen a hálózati szabály(oka)t is el kell készítenünk (Route vagy NAT, stb).

6.2.1 TÍPUSOK ÉS MŰKÖDÉS

Két, eltérő típust különböztetünk meg, először is a **"Failover"**, amikor is a két beállított kapcsolat között automatikus váltás történik - abban az esetben ha az egyik (konkrétan az elsődleges) megáll. Ehhez természetesen be kell állítanunk, hogy melyik legyen az elsődleges, és melyik a tartalék (nyilván ez utóbbi a lassúbb és vagy a drágább lesz). Ezután sok teendő nincs, a váltás tényleg megtörténik. Ha később az elsődleges kapcsolatunk visszatér a tetszhalálból, akkor természetesen megint változik a helyzet, csak fordított előjellel, de szintén automatikusan. Egyszerűen lehetséges bármikor változtatni az elsődlegességet (lehet menetközben is konfigurálni, variálni, ezért nem kell a varázslót a nulláról kezdeni).

A másik típus a **"Load balancing"** (a két fő típus között is lehet váltani egyébként menetközben), amikor is a megoszthatjuk a két kapcsolat között a használat arányát, amelyet egy ún. "load balancing factor" csúszkán, százalékosan állíthatunk be. Ez az egyetlen különbség egyébként a típusok között, a beállítás és a feltételek azonosak mindkét esetben. Pontosabban nem, van még egy különbség, mégpedig az ún. explicit route-ok bevitelének lehetősége, ami csak a terheléelosztásnál van, és a kapcsolatonként (nyilván) különböző, saját DNS/Time vagy egyéb szerverek felé tereli az odatartozó forgalmat. Így aztán nem fordulhat elő az, hogy az ISP2 DNS-ét kérdezi le a TMG akkor, ha az ISP1 kapcsolatot használja.



6.15 ÁBRA A LOAD BALANCING EGYBEN FAILOVER IS

Általában a magas rendelkezésre állási szolgáltatások zéró vagy ehhez nagyon közeli intervallum alatt megoldják az "átkapcsolást", azaz a felhasználói oldalról nézve a kiesésmentes működés garantált. Ez most a mi esetünkben azt jelentené, hogy ha pl. egy oldalletöltés közben áll meg az egyik vonal, akkor az oldal töltődése zökkenőmentesen folytatódik (stateful failover). Nos az azért itt nem így van, lásd később.

Amit még mindenképpen tudnunk kell, az az, hogy az ISP-R-t elsősorban a "belülről kifelé" irányra szánták a tervezői, azaz a hozzáférési tűzfalszabályokkal kapcsolatos forgalom fenntartásán van a fókusz. De ez nem azt jelenti, hogy a belső web- vagy más szervereink felé menő forgalomban nem lehetne elérni ezt a lehetőséget, dehogynem. Csak, ha ez a célunk, akkor gondoskodnunk kell arról, hogy a web- vagy más szervereink elérhetőek legyenek a másik, éppen működő ISP-n keresztül is (DNS).

A TMG az ISP varázslóban általunk megadott ISP hálózati adatait használja mindkét vonal fenntartására, amely mindkét esetben minimum az alhálózat és az alapértelmezett átjáró⁵⁴. Ha például egy kapcsolat mondjuk a belső hálózattól éppen kiépülne, akkor a TMG kiválasztja az ISP-R konfigurációját, hogy melyik hálózatot fogja használni. Ezt mindig a TMG dönti el, azaz én nem tudok userek/gépek/protokollok alapján elsődleges illetve másodlagos hálózatot kijelölni (pedig ez is jó lenne), ez a termék jelenlegi állapotában egy értelmezhetetlen kívánság. A döntés két dologon múlik: az adott kapcsolat rendelkezésre állásán, valamint a "stickiness"-en, azaz a (talán ez egy jó szó) "folytonosságon"⁵⁵.

⁵⁴ Mivel ezekből kettő darab van, így egy kicsit olyan, mintha egy tömbösített konfigurációt használna, de mégis csak egy szerverrel.

⁵⁵ A „stickiness”, azaz a szó szerint „ragadosság” sok helyen előjön a mi iparunkban (fürtöknél, terminálszervereknél, de még a tartományvezérlőknél is), de mindig

Meg aztán még egy dolgon, a 6.3-as fejezet témakörén, az Enhanced NAT (E-NAT) képességen, ugyanis ha ezt beizzítottuk, akkor az E-NAT dönt, mégpedig keményen: adott esetben felül is írhatja az ISP-R konfigot. Szóval így vagy úgy, de ha megvan a döntés, akkor az új kapcsolat az immár meglett NAT címet felhasználva, elkezd kiépülni. A TMG felülírja a TCP/IP útválasztási adatokat az aktuálissal, majd route-ol tovább lefelé, a Layer2-be a megfelelő linken keresztül.

Talán ebből már azt is ki lehetett találni, hogy a ISP-R csak és kizárólag a NAT kapcsolatoknál képes működni. Ebből meg azt, hogy a Local Host hálózatban, azaz magán a TMG-n ezt nem fogjuk tesztelni. Viszont ami a web proxy filteren keresztül megy (pl. HTTP), az NAT-tal megy, tehát finomítsuk a tételt: a Local Host esetén, ha nem a web proxy filtert használjuk, akkor nem elérhető az ISP-R.

6.2.2 A KAPCSOLAT TESZTELÉSE

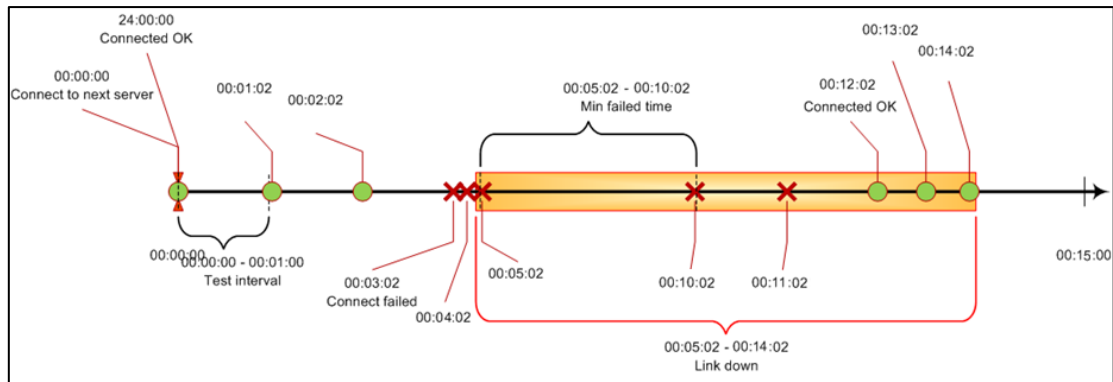
Nem kevésbé lényeges tudnunk azt is, hogy hogyan teszteli a TMG a kapcsolatokat, milyen intervallumokban történik meg mindez, és mikor vált oda- vagy vissza ha pl. a failover üzemmódban vagyunk.

Szóval elsődlegesen DNS lekérdezésekkel (UDP53) bombázza a root DNS szervereket a TMG, alapértelmezésben 60 másodpercenként.

13 root DNS szerver van szétosztva a Földön, minden földrészen van az Antarktisz kivételével, és ezekre a DNS sajátosságai miatt majdhogynem jobban vigyáznak, mint Fort Knox-i aranyra, további info: <http://www.root-servers.org>.

Váltogatva kérdezi le ezeket a TMG, de egyszerre azért mindig csak egyet. Ha egy alkalommal több root DNS szerver sem válaszol, akkor még 2x próbálkozik a TMG, tehát összesen 3 sikertelen kísérlet, és így 3 perc kell a váltáshoz. Ha váltott a második kapcsolatra, az első azért nem nagyjá békén, minden 300-ik másodpercben újra teszteli. Ha visszatér a tetszhalálból az első kapcsolat, akkor még 2x újra teszteli (szinten percenként), majd ha OK, akkor visszavált.

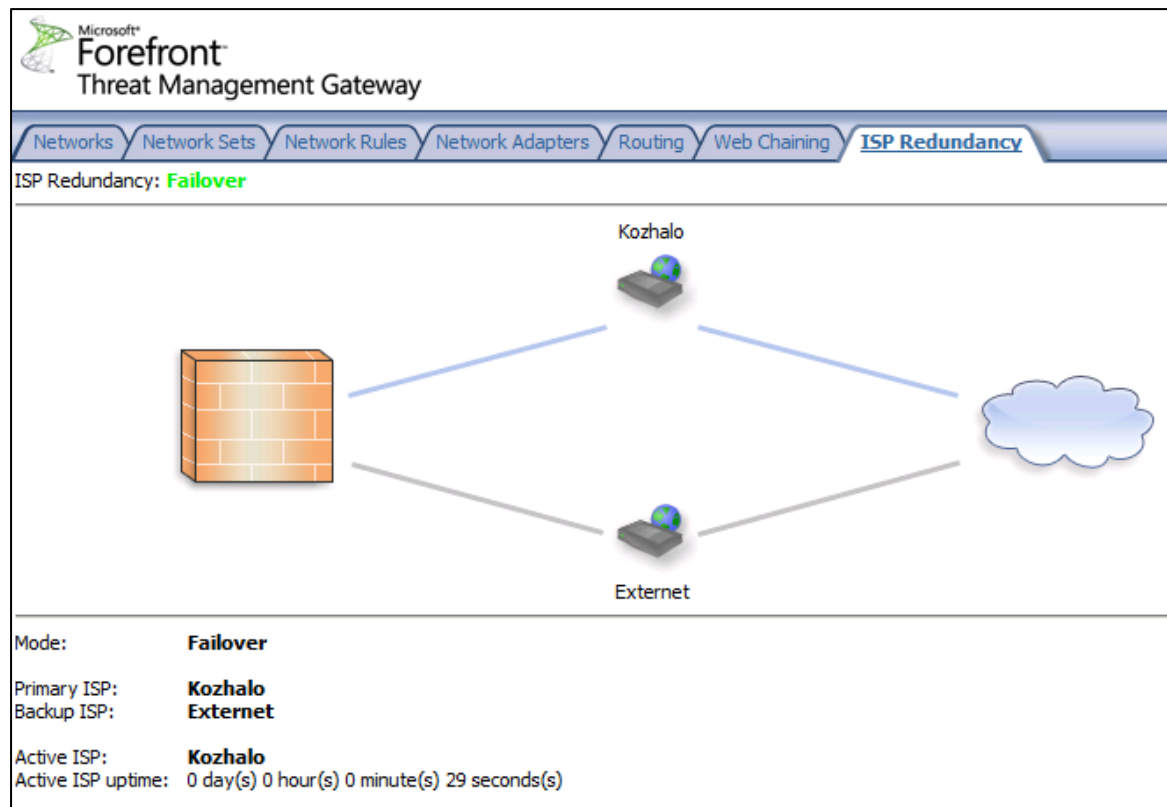
nagyjából ugyanazt jelenti: a kliens-szerver viszonylatban a kapcsolatok „szeretnek” ugyanazzal a géppel/IP-vel stb. kézenfogva megmaradni, vagyis folytatni a működést.



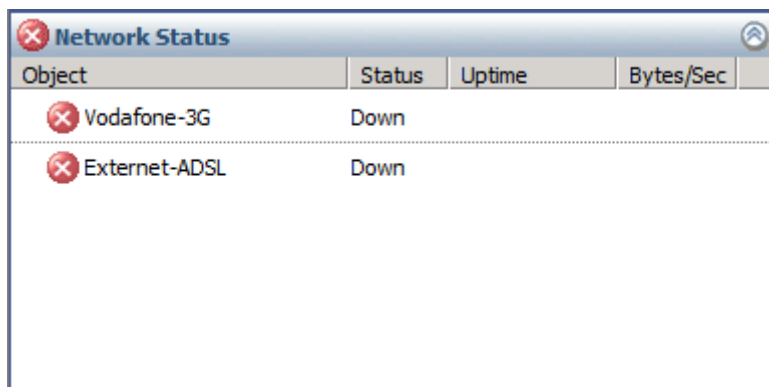
6.16 ÁBRA 3,5,3: EZEK A KULCSSZÁMOK

Az ISP-R szolgáltatáshoz különböző riasztások is tartoznak, egész konkrétan 10 új elemet találhatunk a listában, ezek közül kiemelnék párat:

- ISP-R - Link Connection Address Missing: Nincs IP cím beállítva az adott External hálózathoz tartozó NIC-en
- ISP R - Connection Active: Ha működik a kapcsolat az ISP felé (és ha újra működik is)
- ISP-R - Connection Unavailable: Ha elérhetetlen vagy bontott az adott kapcsolat
- ISP-R - Connections Unavailable: Csak egy betű az előzőhöz képest, de nagy a különbség: ilyenkor már mindkét ISP elérhetetlen, és ez ellen nem véd már meg minket senki.



6.17 ÁBRA ILYEN VOLT (MÉG A VONALAK SZÍNE IS SZÁMÍTOTT), DE AZTÁN EZ AZ RTM-RE KIHALT

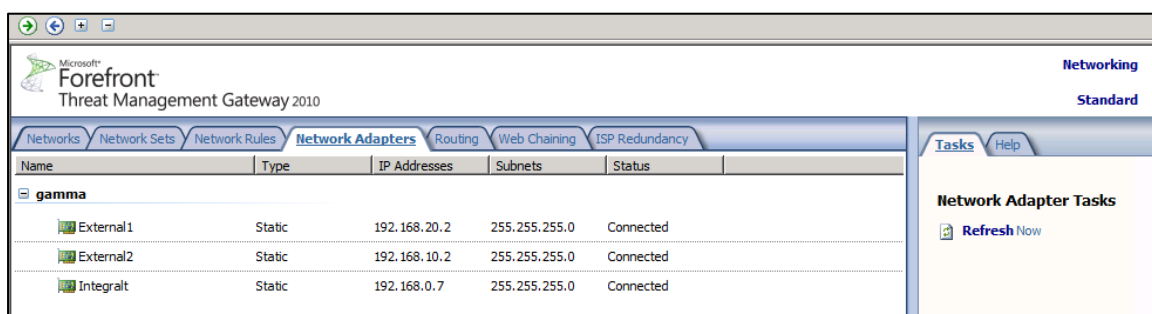


6.18 ÁBRA MOST ÉPPEN EGYIK SEM MŰXIK (A DASHBOARD EGYIK RÉSZE EZ AZ ABLAK)

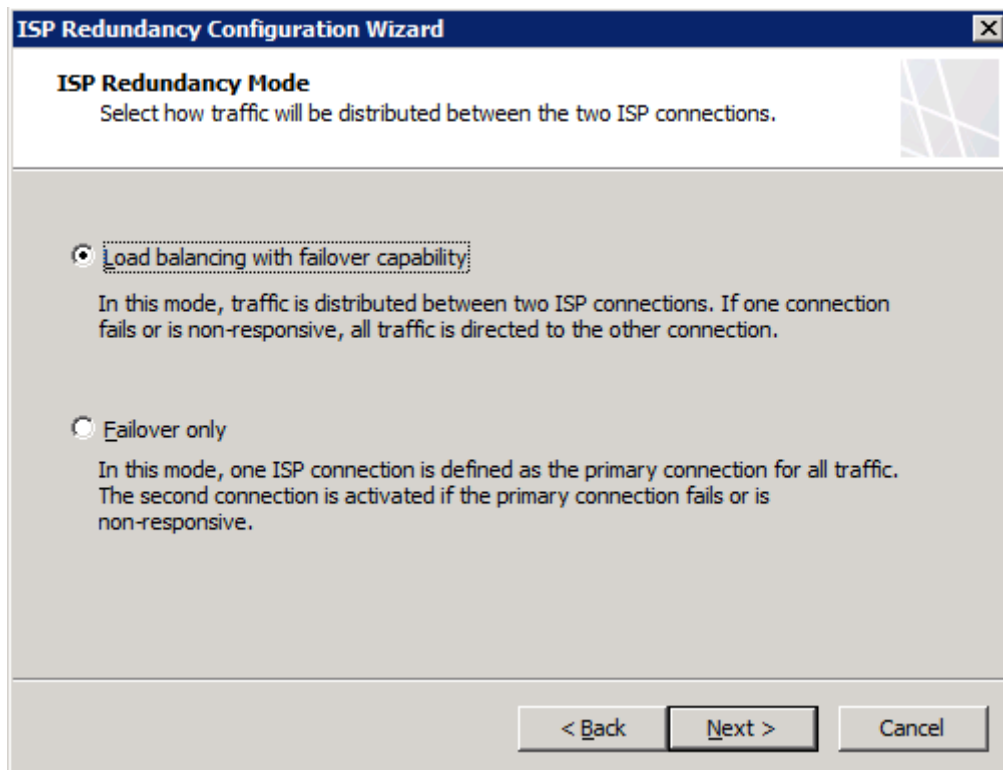
Vizuálisan is kaphatunk visszajelzést, bár a bétához képest kissé szegényes a helyzet, az előző két ábra magáért beszél.

6.2.3 ÁLLÍTSUK BE!

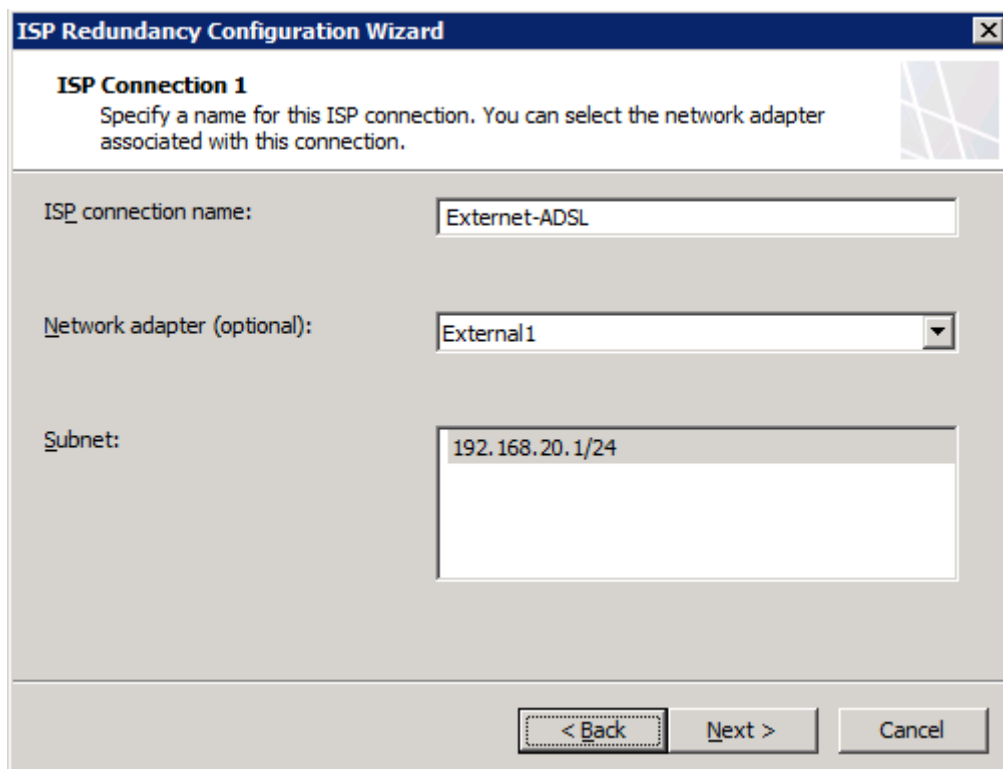
Képes beszámoló következik, minimális szövegmennyiséggel.



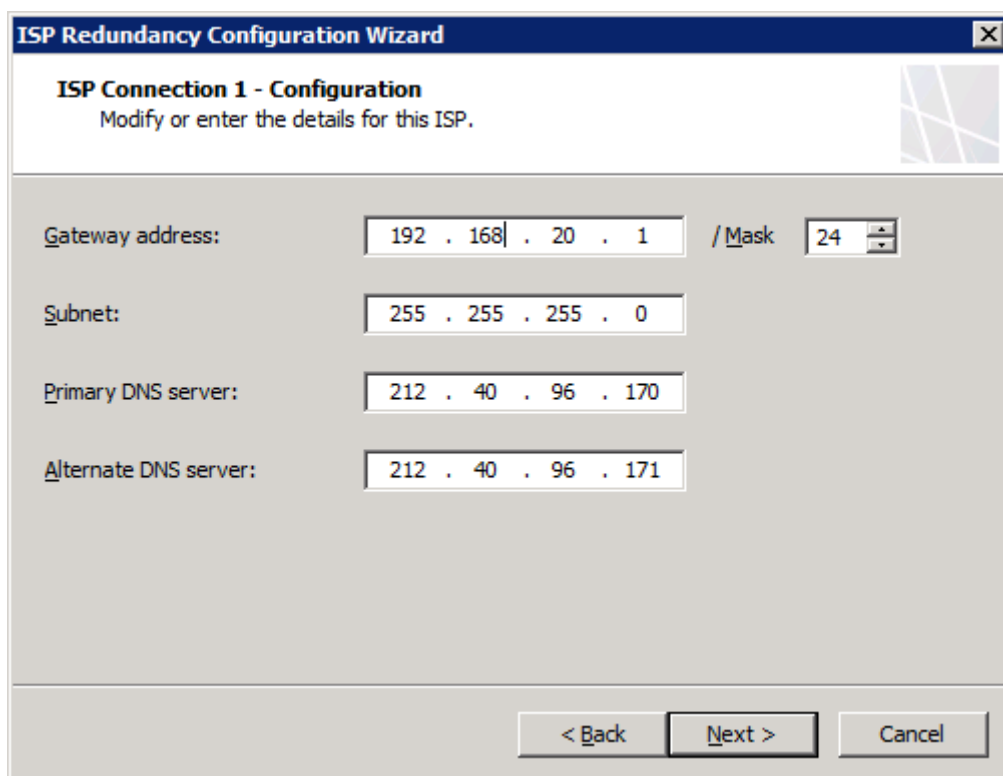
6.19 ÁBRA MEGVAN MINDEN FELTÉTEL



6.20 ÁBRA A TERHELÉSELOSZTÁST VÁLASZTJUK MOST, MERT EZ A KOMPLEXEBB



6.21 ÁBRA AZ EGYIK HÁLÓZAT KIJEÖLÉSE



ISP Redundancy Configuration Wizard

ISP Connection 1 - Configuration
Modify or enter the details for this ISP.

Gateway address: 192 . 168 . 20 . 1 / Mask 24

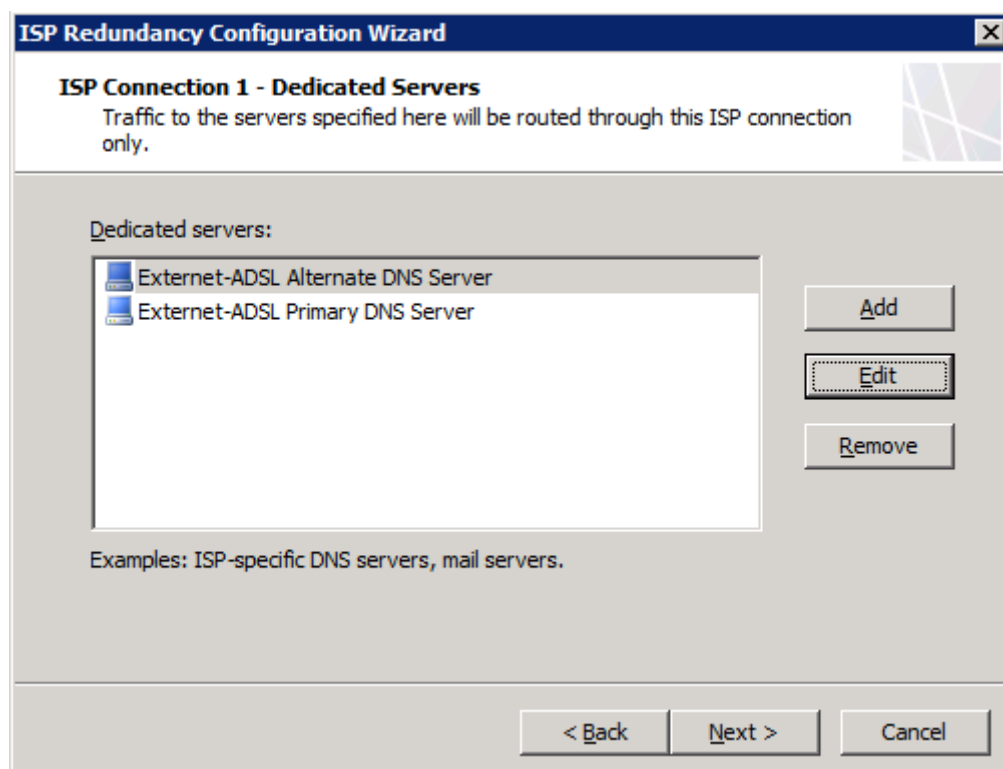
Subnet: 255 . 255 . 255 . 0

Primary DNS server: 212 . 40 . 96 . 170

Alternate DNS server: 212 . 40 . 96 . 171

< Back Next > Cancel

6.22 ÁBRA A DNS ADATOK TISZTÁZÁSA MÉG AZ ELSŐ KAPCSOLATNÁL



ISP Redundancy Configuration Wizard

ISP Connection 1 - Dedicated Servers
Traffic to the servers specified here will be routed through this ISP connection only.

Dedicated servers:

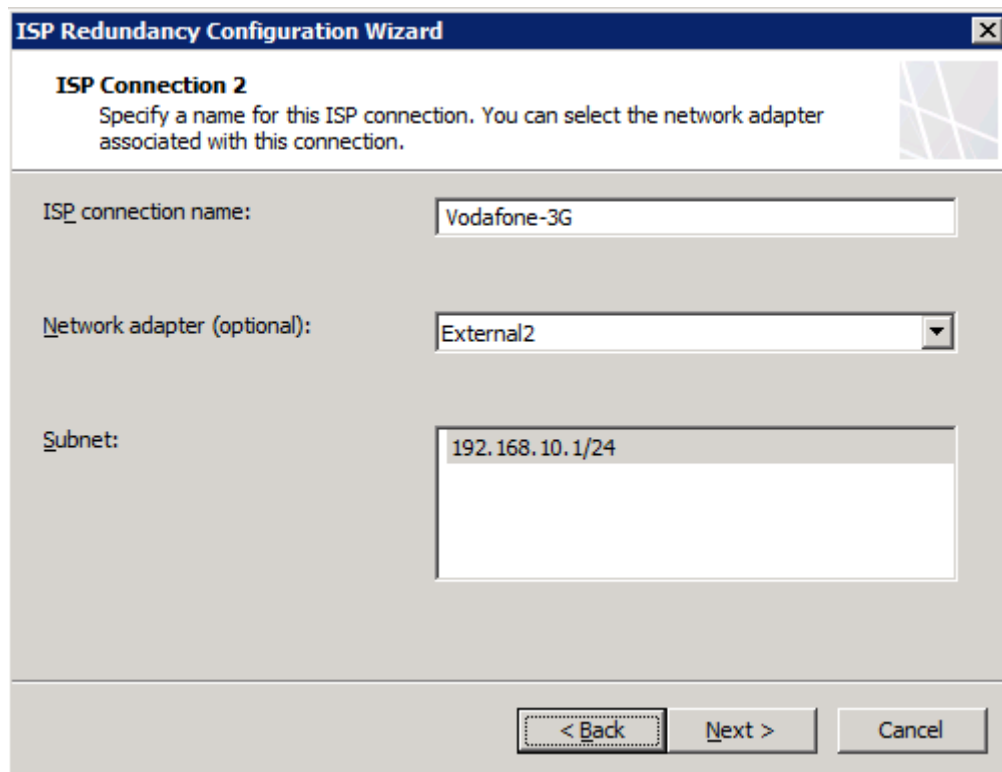
- Externet-ADSL Alternate DNS Server
- Externet-ADSL Primary DNS Server

Add Edit Remove

Examples: ISP-specific DNS servers, mail servers.

< Back Next > Cancel

6.23 ÁBRA KÉSŐBB AKÁR VARÁZSLÓ NÉLKÜL IS VARIÁLHATJUK ÍGY



ISP Redundancy Configuration Wizard

ISP Connection 2
Specify a name for this ISP connection. You can select the network adapter associated with this connection.

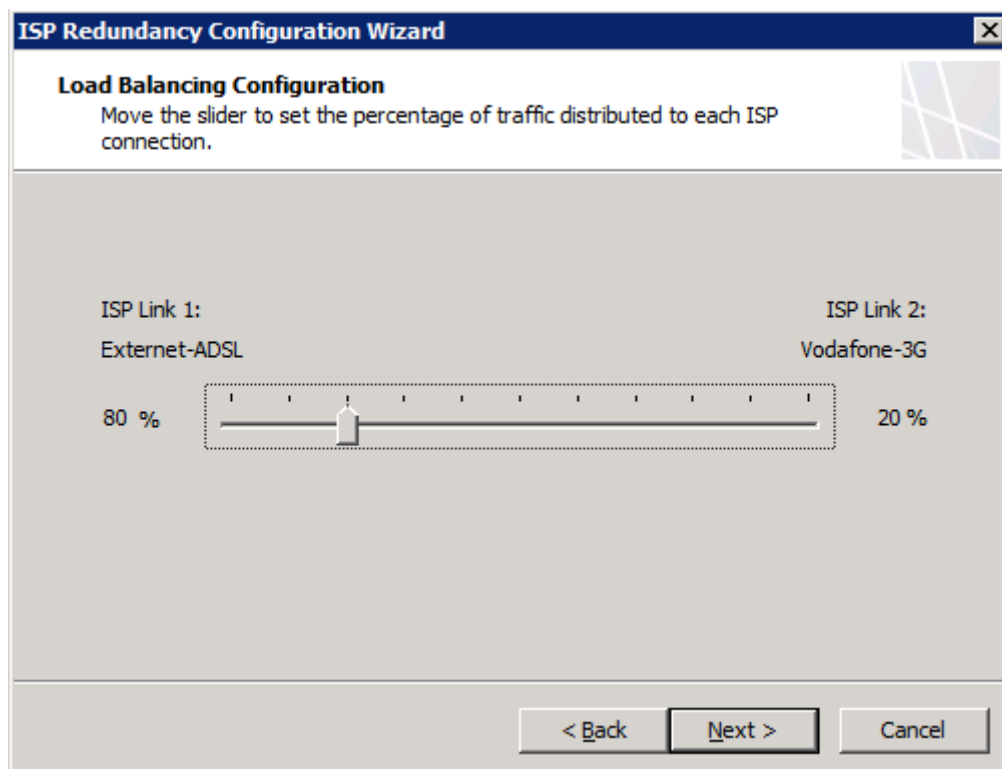
ISP connection name:

Network adapter (optional):

Subnet:

< Back Next > Cancel

6.24 ÁBRA A MÁSIK HÁLÓZAT (IGEN, 3G-S ROUTEREM IS VAN)



ISP Redundancy Configuration Wizard

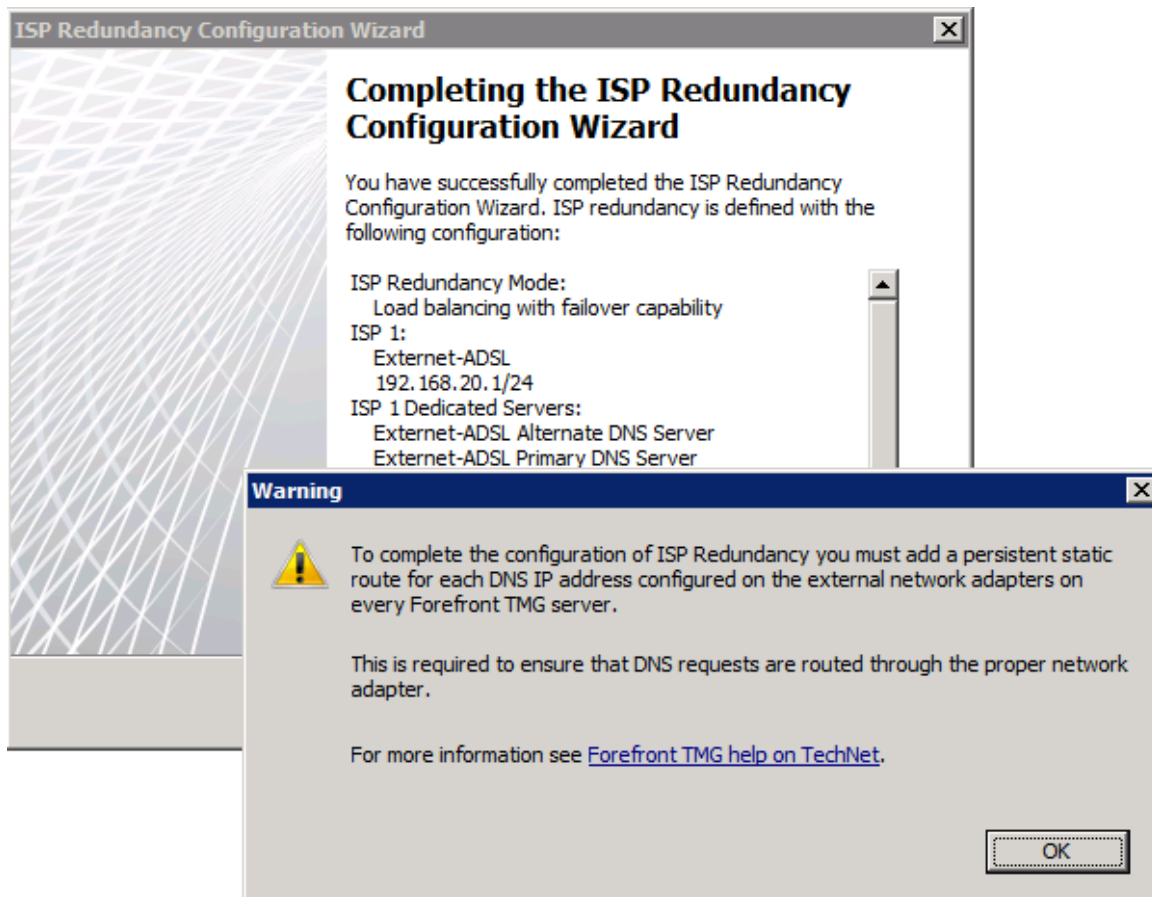
Load Balancing Configuration
Move the slider to set the percentage of traffic distributed to each ISP connection.

ISP Link 1: Externet-ADSL ISP Link 2: Vodafone-3G

80 % 20 %

< Back Next > Cancel

6.25 ÁBRA A MOBILNET DRÁGA
(KÉT KÉP KIMARADT, DE AZOK MÁR ISMERŐSEK)



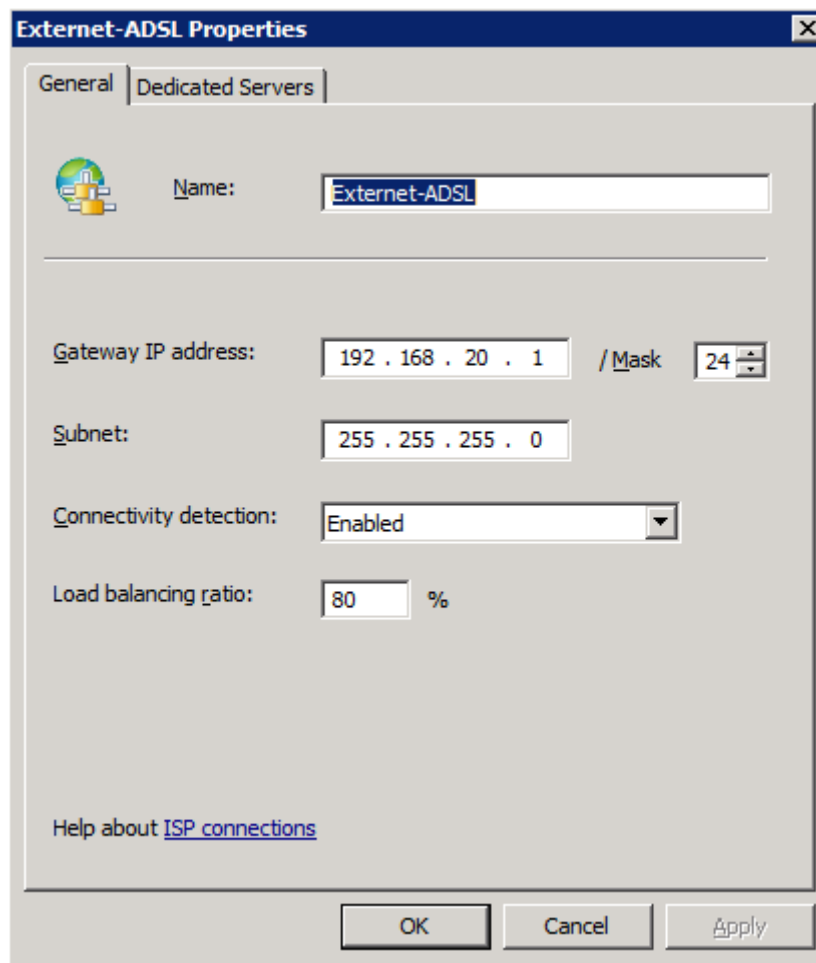
6.26 ÁBRA JÓL DOLGOZTAM, MINDEN RENDBEN, DE EGY TEENDŐNK MÉG VAN

A plusz üzenet lényege, az hogy mint tudjuk az OS nem szívesen támogatja a többszörös alapértelmezett átjáró konfigurációt (erről szoktunk is megjegyzést kapni ha több kártya TCP/IP konfigurációjánál ezt elszúrjuk), és különösen nem, ha mindezt DHCP kapcsolatokkal óhajtjuk megvalósítani. Ha viszont az ISP-től csak így kaphatunk (még ha fix is) IP-t, akkor kézzel ki kell egészítenünk a varázslást a következő a route táblába bekerülő adatokkal (ezt persze még a varázsló előtt is megtehetjük). Az én esetemben a parancsok a következő módon néznek ki:

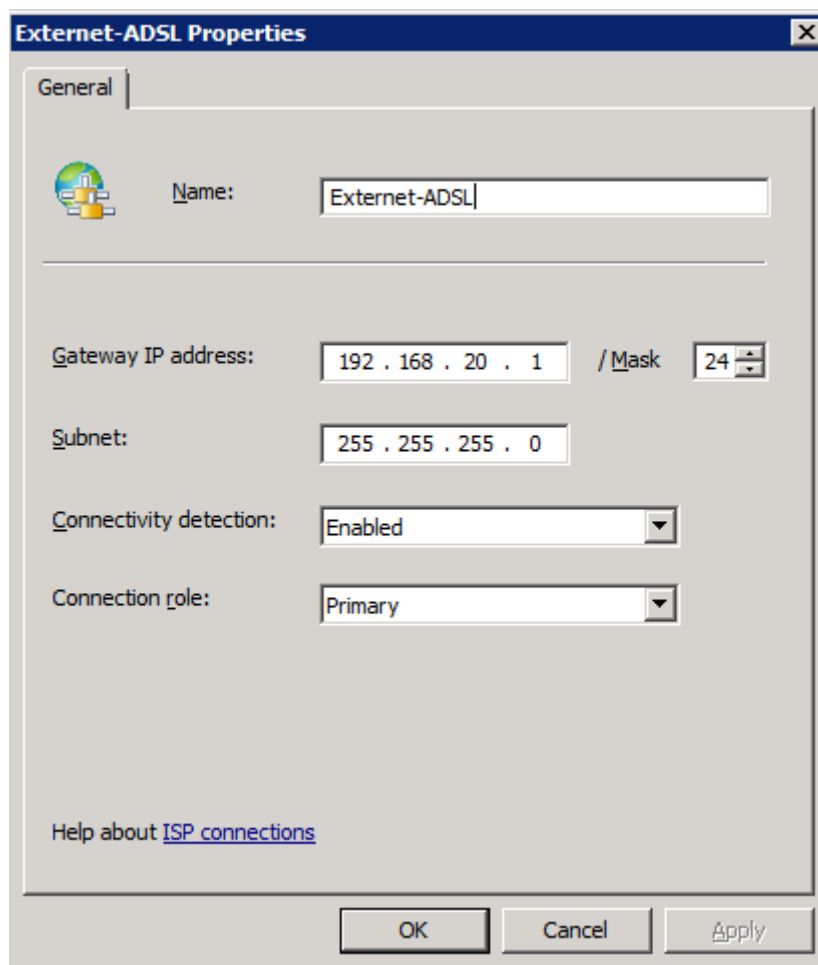
```
route -p add 0.0.0.0 mask 0.0.0.0 192.168.10.1
```

```
route -p add 0.0.0.0 mask 0.0.0.0 192.168.20.1
```

Készen is vagyunk, tekintsük meg most a kapcsolatok állapotát, majd váltsunk.



6.27 ÁBRA AZ ISP1 KAPCSOLAT A VARÁZSLÁS UTÁN

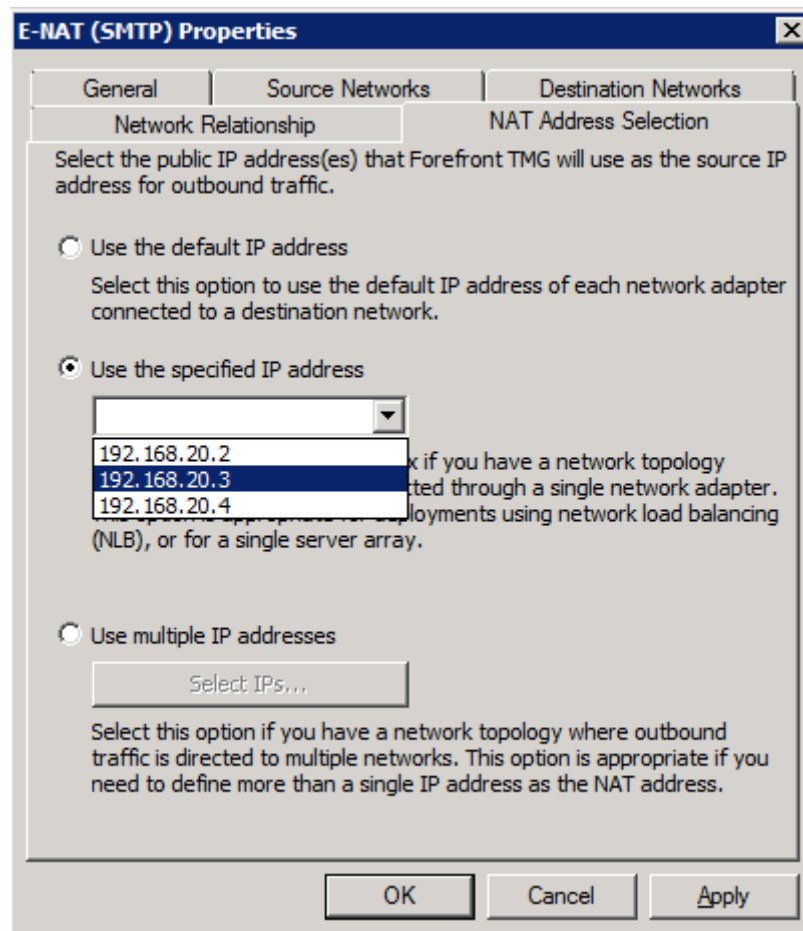


6.28 ÁBRA EGYSZERŰEN ÁTKAPCSOLTAM FAILOVER MÓDBA (ISP-R TASKS AZ ACTION PANE-N)

6.3 ENHANCED NAT

A legtöbb esetben elég egyetlen publikus IP cím ahhoz, hogy olyan levelezőszervert üzemeltessünk, amely fogad is e-mail-eket. Ezen feladatra az ISA Server-ek is tökéletesen megfeleltek már, az egyetlen külső hálózatunkon egyetlen külső IP-vel képesek voltunk olyan SMTP szerver publikálást csinálni, amely befogadta a (publikus) DNS-ben elhelyezett pontos MX rekord alapján a szervezetünknek szánt üzeneteket, majd szépen továbbította is a belső Exchange-nek. A probléma abban a pillanatban kezdődött, amikor bármilyen okból több IP-re volt szükség (vagy lesz, mert pl. a TMG-nél a DirectAccess-t is szeretnénk használni), amelyeket szépen fel is vettünk a külső hálózat adapterébe. Ekkor ha két SMTP tartományunk van, akár csinálhatunk két MX rekord bejegyzést is, és két reverse-et is, mindig az alapértelmezett IP lesz a forrás cím.

Az E-NAT egyik előnye éppen itt mutatkozik meg, hiszen az eddig megszokott "egy NAT-bármelyik IP" megszorítást feloldja. Kézzel beállíthatjuk, hogy melyik hálózat esetén melyik IP lesz az, amelyiket a TMG-nek használnia kell, ergo a tűzfal mindig a megadottat használja majd forrás címként és nincs probléma.



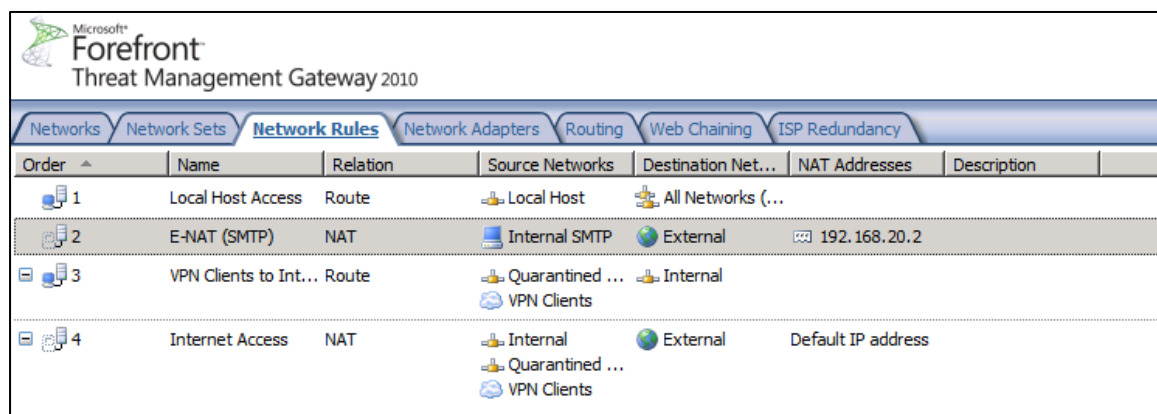
6.29 ÁBRA OKOS DOLOG VÁLASZTANI

Az E-NAT okos⁵⁶ használatához hozzunk létre egy új hálózati szabályt (Networking - New - Network Rule), amelybe forrásként az SMTP szerverünk belső címét rakjuk, célként az External hálózatot, majd varázsló NAT Address Selection ablakában (6.27-es ábra), a megfelelő, kívültre szánt IP-t jelöljük ki.

Ezután a helyes működés kedvéért rakjuk ezt a szabályt közvetlenül a gyári "Local Host Access" nevű után a második helyre, mivel ha ezt nem tesszük meg hatástalan maradhat a szándékunk, mivel pl. az Internet Access nevű gyári hálózati szabályban (szintén NAT) a legelső IP az alapértelmezett lesz, így ez a szabály – ha előbb jut érvényre – simán felülírhatja a szándékunkat.

⁵⁶ Miért mondom hogy „okos”? Csak azért, mert ha pl. az Internet Access hálózati szabályon állítjuk be az E-NAT használatot, akkor egy aktív FTP szerver alapértelmezett első IP-s publikálásába könnyedén belebukhatunk. Ugyanis az aktív FTP használatkor a második (az adat) csatorna kezdeményezése nem a külső kliens, hanem a mi FTP szerverünk dolga lesz, de mivel mi globálisan használjuk az E-NAT képességet, lehet hogy az alapértelmezett és a másodikként kapott IP cím eltér, a külső kliens pedig erre csak széttárja a kezét és terminál. Az SMTP remekül fog működni, de az FTP szerverünk nem. Ha szétválasztjuk a dolgot egy külön SMTP E-NAT hálózati szabállyal, akkor nem lesz ilyen problémánk.

A KAPUN TÚL



Order	Name	Relation	Source Networks	Destination Net...	NAT Addresses	Description
1	Local Host Access	Route	Local Host	All Networks (...)		
2	E-NAT (SMTP)	NAT	Internal SMTP	External	192.168.20.2	
3	VPN Clients to Int...	Route	Quarantined ... VPN Clients	Internal		
4	Internet Access	NAT	Internal Quarantined ... VPN Clients	External	Default IP address	

6.30 ÁBRA A SORREND ABSZOLÚTE NEM MINDEGY

Kimaradt egy fontos dolog. Ez pedig az, hogy nem tudjuk protokoll szinten szabályozni. Csak forrás és cél hálózati objektumok között szabályozható. Tehát nincs olyan, hogy Internal - External SMTP esetében „A” IP cím, POP3 esetében „B” IP cím.

7 A PROXY SZERVER

7.1 MIT CSINÁL EGY PROXY SZERVER?

A proxy a tűzfal szerepkör mellett egy másik nagyon fontos és komplex összetevője az ISA és a TMG szervereknek. Egy hétköznapi proxy szerver a kliens alkalmazások (pl. egy böngésző) és a távoli szerver közötti kapcsolatban kap szerepet, mivel minden kliensoldali kérés és minden válasz a proxy szerveren keresztül történhet csak⁵⁷, azaz teljes rálátása van erre a forgalomra. A biztonság és a teljesítmény a két legfontosabb terület, ahol érvényesülhetnek a proxy szerverek, és ha csak azt nézzük, hogy az összes forgalom kb. 4/5-e HTTP, ezért a szerepük valóban óriási jelentőséggel bír.

Taglaljuk most kicsit részletesebben hogy hol egészíti ki az ISA/TMG szerverek működését a proxy szerver:

- Felhasználói hitelesítés: Erről már többször szó esett eddig is, legutoljára például a hozzáférési tűzfalszabályok kapcsán. A háromból kétféle klienssel lehetséges az Internet felé menő kéréséknél hitelesítést kérni a felhasználótól vagy a géptől (gondoljunk egy szoftverre, pl. WSUS). A hitelesítés történhet a háttérben, történhet rejtve, és történhet pl. az eltárolt hitelesítési csomagok alapján is. Az értelemszerűen elsődleges feladat, a kérés engedélyezése vagy megtagadása mellett pl. a naplózás egyértelművé tételét is megoldhatjuk a proxy hitelesítéssel.
- Szűrés: Azonkívül, hogy már a kapcsolódás is lehet engedélyköteles, utána sem kell feladnunk az ellenőrzést, sőt, több szinten, valóban rengetegféle jellemző alapján tudjuk szűrni a forgalmat a proxy szerverrel. IP, protokoll, port, időpont és még sorolhatnám, hogy mi minden tartozik az alapszintű szűrési módszerek közé.
- Tartalom vizsgálat: Szintén teljes körű ki- és bemenő szűrést jelent, és itt több szintet meg tudunk különböztetni, az egyszerűbb, MIME típus alapján történő szűréstől, a HTTP filter képességein keresztül egészen a teljes következő fejezetig, azaz mint pl. a malware vagy az kategorizált URL filterig.
- Ahogyan említettem, mivel a proxy kéz alatt tart mindent, értelemszerű, hogy "lát" is mindent, így a granulás naplózás illetve az ezen alapuló jelentések generálása sem okoz gondot.
- A belső hálózat "eltüntetése": Akár bentről kifelé, akár kintről befelé tart a forgalom, a proxy szerver gondja lesz a belső, védett hálózat adatainak teljes elrejtése. Ez nagyon kevés kivételtől eltekintve tökéletesen meg is oldható.

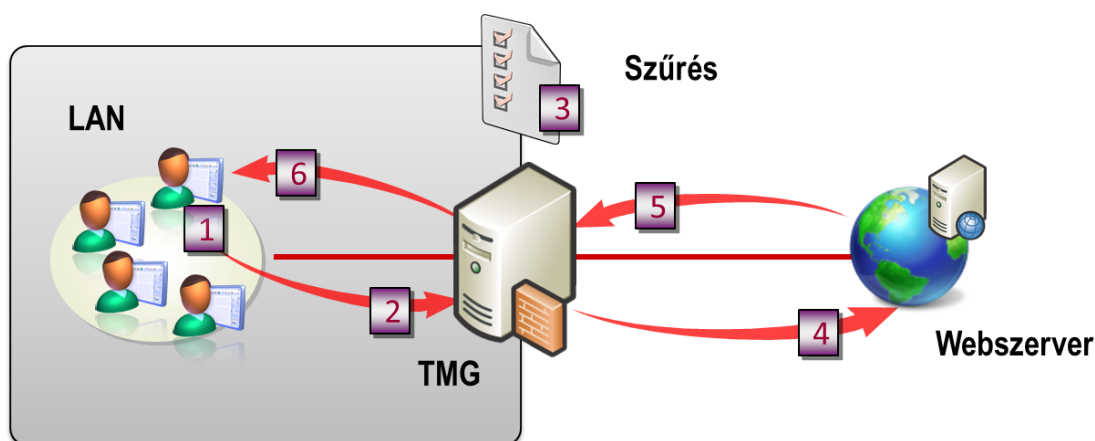
⁵⁷ A tűzfal pedig a proxy szerver és a külső hálózat között található pl. az ISA/TMG szervereknél.

- A biztonság mellett a teljesítményfokozásban is van aktív szerepe a proxy szervereknek. Ez az ISA/TMG szervereknél egy harmadik fő alkotóelemben, a gyorsítótárzásban (cache) teljesedik ki, amelyet én annyira lényegesnek tartok, hogy külön alfejezetet (7.6) szántam erre a témakörre.
- Tartalom tömörítése: a modern böngészők képesek a tömörített http tartalmat renderelés és feldolgozás előtt kitömöríteni. A TMG a forward és reverse proxy esetében is képes tömörített tartalmat küldeni a kérőnek. Ezzel sávszélességet, csomagszámot takaríthatunk meg.

7.2 PROXY TÍPUSOK

Három alapvető típust különböztetünk meg, az irány (forward, reverse) illetve a proxyzásban résztvevők kapcsolódása alapján (web chaining, ami csak forward irányú lehet). Az ISA/TMG szerverek mindhárom típust egyaránt beépítve tartalmazzák és használják.

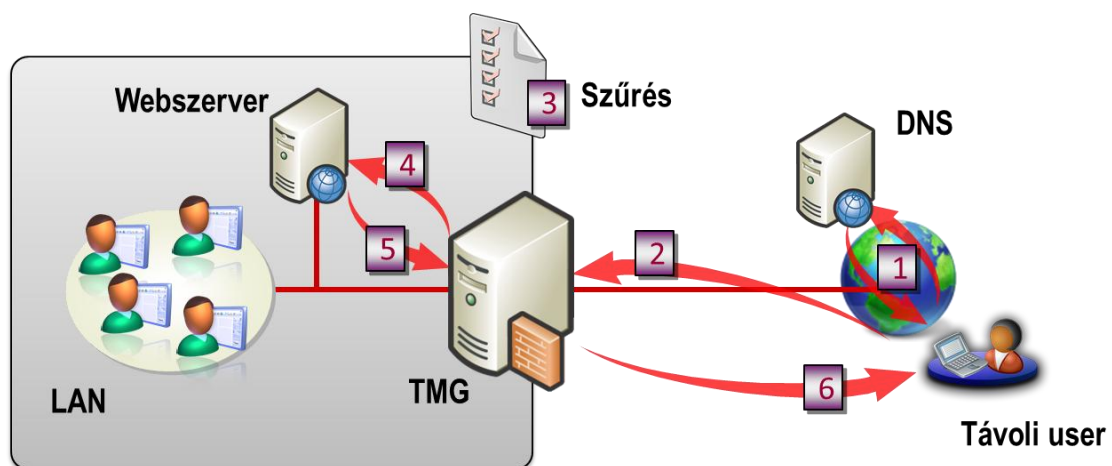
A **forward proxy** az a típus, amelyről a legtöbb szó esik, mert ez az elsődleges irány (bentről kifelé), ezt szűrjük a legalaposabban, és itt zajlik a legtöbb forgalom. Sokszor ezt az típust illetik a "web proxy" kifejezéssel is. A belső, védett hálózathoz, a privát IP című források alkalmazásaitól (böngészők, üzenetküldő és egyéb programok) a publikus, nyilvános hálózatok felé menő irány forgalmát kezeli a forward proxy. Éppen ezért valamilyen automatikus módszerrel (pl. Csoportháztirend, tűzfal kliens), vagy végső esetben manuálisan gondoskodnunk kell arról, hogy ezek az alkalmazások lássák is a reverse proxyt. A javasolt irány a flexibilitás miatt valamilyen automatikus detektálási módszer (CERN Proxy client esetében a WPAD, TMG Client esetében a WPAD vagy az SCP alapú detektálás).



7.1 ÁBRA A FORWARD PROXY MŰKÖDÉSE 6 LÉPÉSBEN

1. A felhasználó a böngészőjéből indít egy kérést egy webszerver felé. A böngésző megtekintti a saját web proxy beállításait, és ellenőrzi, hogy talál-e az adott webszerverre egy konkrét utalást (mint kivétel).
2. Ha nincs a kivételek között az adott cím (mert pl. *nem* a belső hálózatban van az adott webszerver), akkor a kérés elmegy a proxy szervernek. A kérés specialitása az, hogy a kérelemben az eredetileg beírt URL, URI mezője szerepel. Vagyis a CERN proxy kliens nem próbálkozik a névfeloldással.
3. A proxy szerver ellenőrzi, hogy adott kérés a definiált szabályok és beállítások alapján engedélyezett-e?
4. Egyúttal a gyorsítótár tartalmát is csekkolja, mert ha az adott cél vagy annak legalább bizonyos és érvényes objektumai a helyi cache-ben megtalálhatóak, akkor ezeket elküldi a kliensek. és ha ez netalántán maradéktalanul kielégíti (bármilyen nagy is a cache, azért ez egészen ritka) a klienst, akkor vége is a folyamatnak. Ha nem, a proxy továbbküldi a saját nevében a külső webszervernek.
5. A webszerver válaszol, a proxy pedig a beizzított filtereknek megfelelően ellenőriz.
6. Ha nem kell blokkolni, akkor a ISA/TMG egy másolatot elhelyez a gyorsítótárban, majd kiszolgálja a klienst.

A **reverse proxy** elvileg ugyanúgy működik mint a nagy testvére, csak az irány más, ugyanis ennek a proxy típusnak a segítségével a külső kliensek szeretnék elérni a belső erőforrásainkat, pl. a webszerverünket.

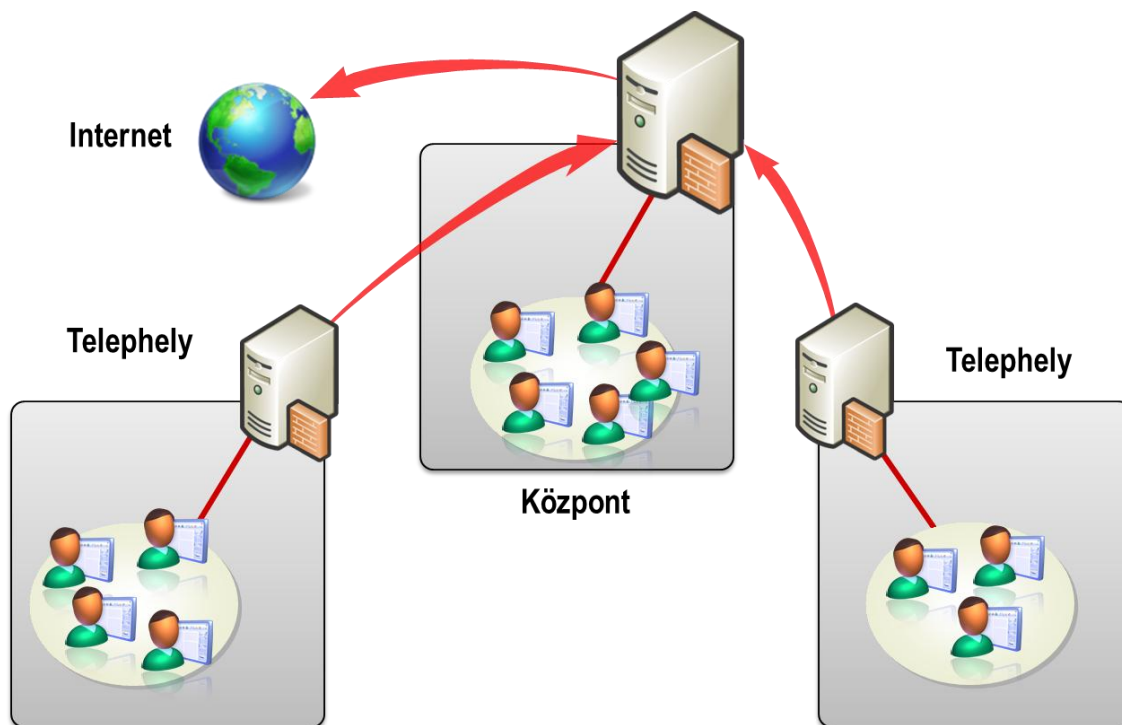


7.2 ÁBRA A REVERSE PROXY IS 6 LÉPÉS

1. A távoli felhasználó a böngészőjével a weboldalunkat óhajtja megnézni. A kliens értelemszerűen DNS egy lekérdezéssel kezd, és ha minden jól megy, akkor a proxy szerverünk publikus IP-jét kapja meg.

2. A kliens elküldi erre az IP-re a kérést, amelyet először a proxy szerver kezel le.
3. A proxy szerver először azt ellenőrzi, hogy az URL rendben van-e⁵⁸, majd azt is hogy adott kérés a definiált szabályok és beállítások alapján engedélyezett-e az elérés?
4. Egyúttal a gyorsítótár ellenőrzésére is sor kerül, ugyanis ez a fajta tartalom is elérhető ily módon. Ha nincs benne a kívánság, vagy már nem érvényes, akkor a proxy továbbküldi a kérést a belső webszervernek.
5. A webszerver válaszol (a proxynak természetesen).
6. A proxy elküldi a távoli kliensek a tartalmat.

A **web chaining (láncolás)** az utolsóként említett a proxy típusok sorában, ami nem véletlen, mert nem is mindennapos használatú. Először is általában több proxy szerver kell hozzá, mivel az ezek közötti proxy kérések terelgetéséről van szó. A használatának oka lehet biztonsági és a teljesítménnyel kapcsolatos, valamint szóba jöhet az infrastrukturális ok is. Az előbbiek azért fontosak, mert a proxyk egymás között a különböző protokollokat különböző biztonsági rétegekben kezelik le, az utóbbira pedig jó példa a telephelyek-központ viszonylat.

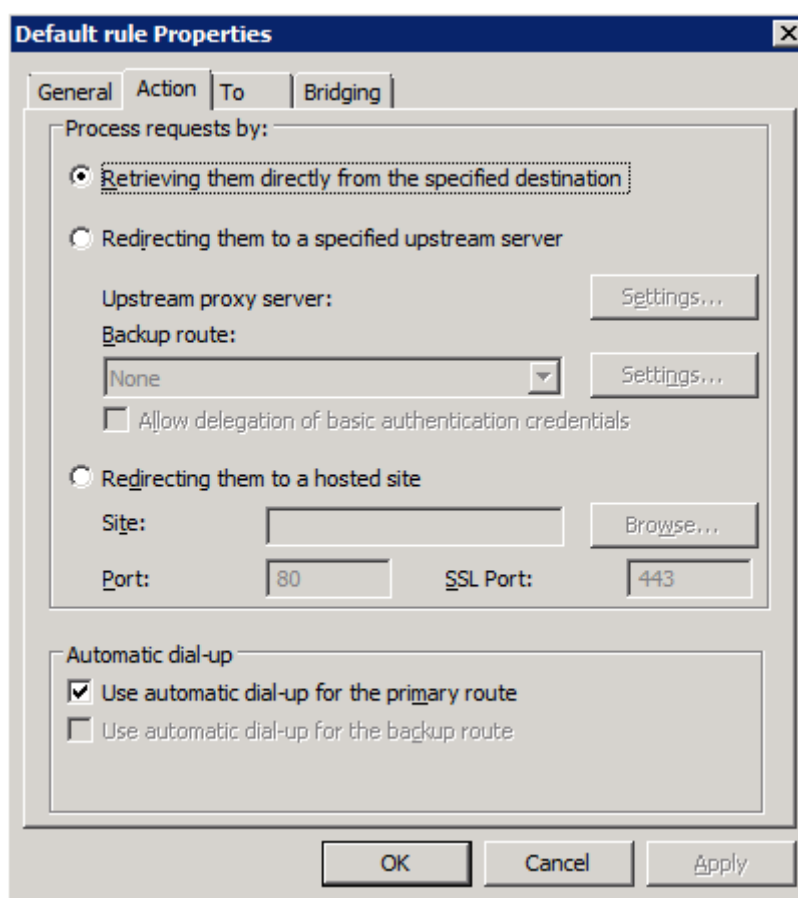


7-3 ÁBRA 3 SZEMŰ LÁNC

⁵⁸ Egyáltalán URL-e, ami kap? Ti. ha pl. a külső IP címünkkel jön a kérés, és nem egy URL-lel, akkor (a publikáló tűzfalszabálytól függően) a proxy akár el is dobhatja a kérést.

Ebben a felállásban pl. az egy lehetséges használati módszer, hogy a telephelyeken levő TMG az érvényes (szabályokba nem ütköző) HTTP forgalmat egy- az-egyben elküldi egy további ellenőrzésre és engedélyezésre a központi TMG-nek (vagy más esetben láncban következőnek). De tehetünk kivételt is, ha pl. a telephelyen van internet hozzáférés, akkor az is szabályozható hogy bizonyos domain nevek esetén használja a saját TMG-jét proxynak, míg minden más esetben a központi TMG proxyja mondja ki a végső szót. Azaz technikailag a lánc bármelyik eleme kiszolgálhatja, megtagadhatja, vagy továbbküldheti a többitől érkező kéréseket.

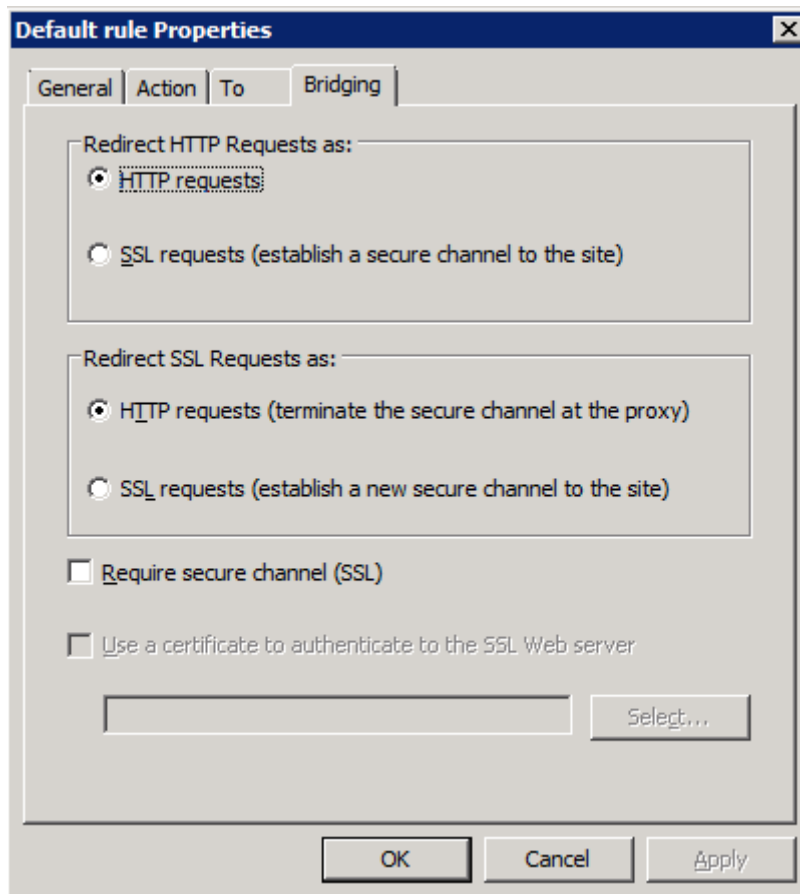
Egy a való élet szülte példa: egy kutató cég több országban telephellyel rendelkezik. A cégvezetés elektronikus könyvtárakhoz és folyóiratokhoz megvásárolt egy előfizetést. Az előfizetés azonosítása IP cím alapján történik. Hogy minden telephelyről használhassák a kutatók a folyóiratot, ezért a központi telephely IP címére fizettek elő. A külföldi telephelyek proxy kiszolgálói az adott elektronikus folyóiratok irányába menő kéréseket továbbítják a központi telephely proxy kiszolgálójának. Így minden telephelyről az összes kutató elérheti az előfizetett tartalmat. *(A lektor megjegyzése.)*



7.4 ÁBRA ÁTIRÁNYÍTÁSI VARIÁCIÓK (NETWORKING\WEB CHAINING)

Ilyenkor a cache szabályzás is működhet úgy, hogy a telephelyi TMG-k először a lokális cache-ben, majd a központiban kutakodnak, de akár úgy is, hogy csak és kizárólag a központiban. És persze, az is elképzelhető, hogy – mondjuk a hierarchia felállástól eltekintve – hogy egy Enterprise verziójú TMG-kből álló, cache tömbre irányítjuk át a felhasználóink kéréseit.

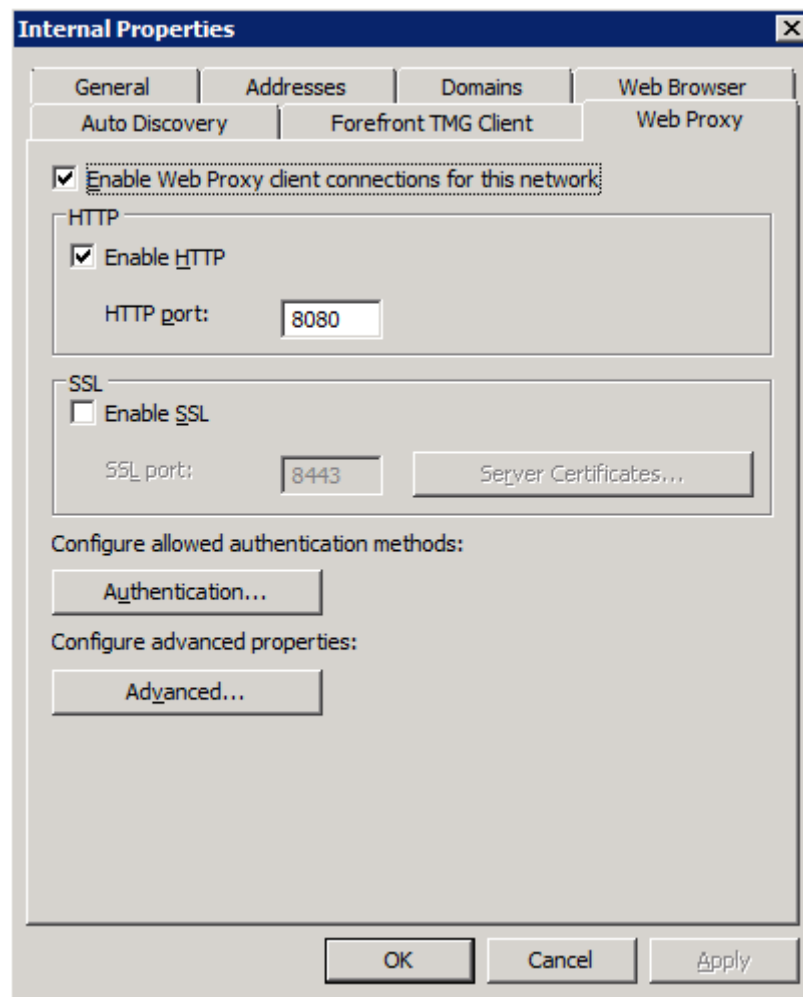
Speciális átirányításokat is kiötlhetünk a web chaining szabályokkal (egy alapértelmezett már létezik, de tetszőleges számút kreálhatunk az igényeink alapján), pl. másodlagos útvonalakkal, de pl. DSL esetén az automatikus tárcsázás beállításainak egy része is itt található. A Bridging fül alatt pedig a HTTP/S oda-vissza irányítást állíthatjuk be.



7.5 ÁBRA ÁTIRÁNYÍTÁSI VARIÁCIÓK (HTTP VS. SSL)

7.3 SZERVER OLDALI BEÁLLÍTÁSOK

A címben ugyan nem került megjelölésre a terméknév, mert gyakorlatilag nincs változás a TMG-ben ezen a területen. A proxy szerver beállításai mindkét esetben a hálózatok egy-egy jellemző tulajdonsága, de nem mindé, hanem igazából csak az Internal és a Local Host típusú hálózatoké, a VPN és az External ebből kimarad.



7.6 ÁBRA A PROXY SZERVER FŐ BEÁLLÍTÁSAI

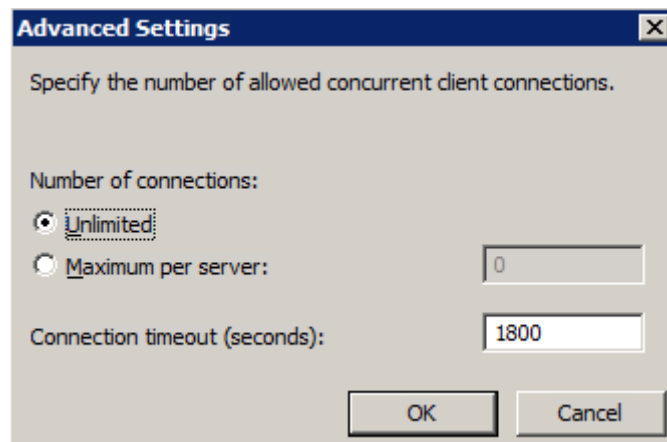
Ezen a panelen első körben engedélyezhetjük/tilthatjuk a proxy szerver működést, valamint el kell döntenünk, hogy HTTP vagy SSL alapon és milyen porttal valósítjuk majd meg. A 8080 az alapértelmezett illetve a 8443 az SSL-nél. Ez utóbbi esetén a megfelelő tanúsítványra is szükség lesz, a hitelesítéshez és a titkosításhoz. A böngészők ezzel a módszerrel nem nagyon tudnak mit kezdeni, de pl. ha a web chaining használata felmerül, akkor hasznos lehet.

A 8080-as portra figyeljünk oda, és ne járjunk úgy mint az egyszeri rendszergazda, aki még a netstat -ano | find ":8080" paranccsal sem találta meg az adott szerver hardvergyártójának egy korábban feltelepített RAID vezérlő felügyeleti programját, amelynek egy apró komponense szintén a 8080-as porton működött, csak nem volt hajlandó ezt elárulni magáról.

A részletek:

<http://www.microsoft.com/hun/technet/article/?id=ebf85f41-cc1d-4d98-9b2a-69f8bf8fa5e4>

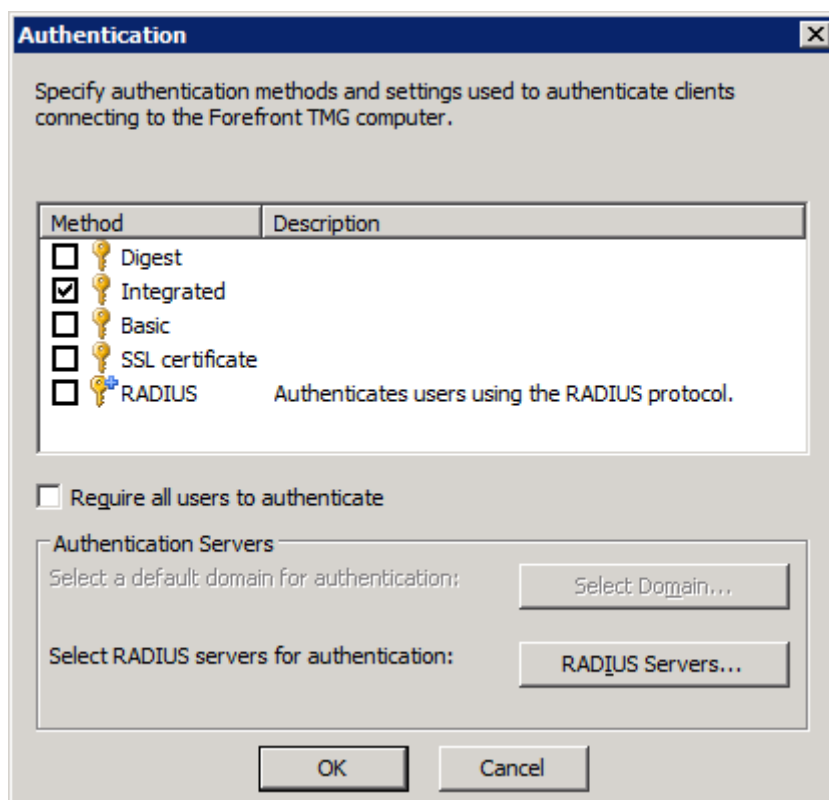
A "Authentication" gombot most ugorjuk át, ellenben tekintsük meg az "Advanced" alatti lehetőségeket.



7.7 ÁBRA

Itt két dolog az, amit konfigurálhatunk, egyrészt a kapcsolatok számának korlátozása, másrészt egy-egy kapcsolat időtúllépési értéke. Sosem gondoltam volna, de egyszer muszáj volt egy kérés alapján utánanézni, hogy mennyi itt a maximum érték, ugyanis egy speciális alkalmazásnak minimum 24 óráig állandóan tartania kellett a proxyval a kapcsolatot, nem szakadhatott le, akkor sem ha nem volt forgalom. Kiderítettem, hogy 99999 sec, ami kb. 27 óra lehet a maximum.

Lépünk tovább illetve vissza, és térjünk rá a hitelesítés beállítására. Ez egy nagyobb lélegzetű témakör, de mindig azzal kezdődik, hogy ki kell derítenünk, hogy milyen klienseink vannak (böngészők, Java, egyéb alkalmazások, más platformokon is, stb.), és ennek megfelelően milyen típusú hitelesítési metódusra (vagy többre) lesz szükségünk, hogy működjön is a dolog.



7.8 ÁBRA

A hitelesítés lehet kötelező ("Require all users to authenticate") vagy opcionális, és ahogy már elhangzott a 3 féle kliensből csak az Secure NAT típusnál nem működhet. A kötelezővé tételnek számos előnye van, pl. az AD-ból vagy más névtérből megszerzett felhasználó vagy csoportinfó alapján így egyszerűen tudunk hozzáférési tűzfalszabályokat generálni, ami lényegesen hatékonyabbá teszi ennek a rendszernek a kialakítását, pl. egy csak az IP-ken alapuló szabályrendszerrel szemben. De a korrekt, felhasználónév alapján történő naplózás, és az ezekre támaszkodó riportok teljessége is múlhat ezen.

Azonban gondoljuk végig, ha kötelezővé tesszük a hitelesítést, 1-2 további kötelezettséget is vállalnunk kell:

1. Az összes szoftver, amelynek bármilyen internetes kapcsolata is van/lesz, csak olyan lehet, ahol a proxy infót lehetséges beállítani. Ez vonatkozik a "Jézus Szíve" Kft. könyvelőprogramjára is, amit pl. csak az internetről lehet frissíteni. És persze vonatkozik a Microsoft termékeire is, mondjuk egy WSUS-ra is, de ebben az esetben egyszerűen lehet proxy auth infót közölni, csak ehhez és a többi alkalmazáshoz kreálnunk kell egy felhasználót, akinek lesz engedélye átjutni a proxyn.
2. Mindezt kikerülhetjük a tűzfal klienssel, ami transzparens módon megoldja ezt a problémát, ahogyan már a 3.4 fejezetben volt is erről szó, de ez ugye csak

Windows kliensre telepíthető, és ekkor amúgy is oda kell figyelnünk pár dologra (pl. VPN kapcsolatok a belső hálózathoz kifelé, és egyebek).

7.4 HITELESÍTÉSI METÓDUSOK

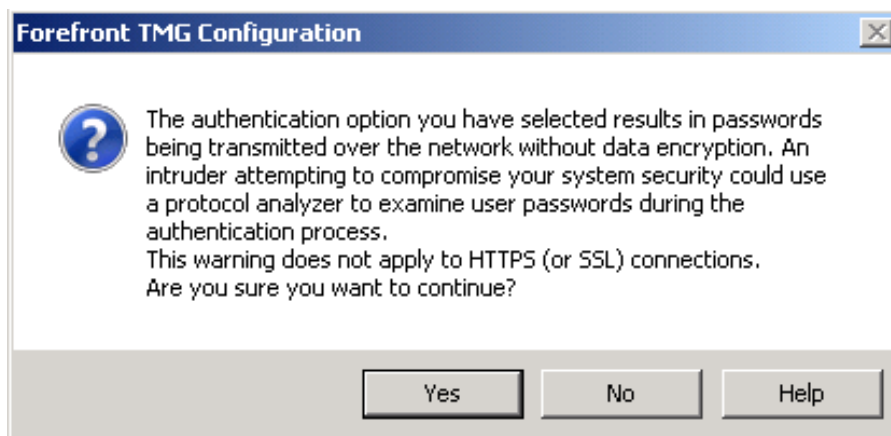
A hitelesítési metódusoknál áttekintésénél nem sorban haladunk, hanem a felhasználási gyakoriság alapján:

Integrated

Ha pl. a böngészőnk minimum IE2 (igen!), akkor az Integrated hitelesítés működhet a háttérben és NTLM-mel, Kerberos-sal⁵⁹, vagy Negotiate alapon (kölsönösen egyeztetve). Ha tartományunk van, és a felhasználó be is lépett az OS-en keresztül, akkor az IE az ekkor megszerzett infót küldi el a TMG kérésére, azaz ezzel hitelesít alapértelmezés szerint. A TMG pedig ennél a típusnál használhatja az érvényesítésre a Windows Security Support provider-t (SSP). Ezekből is látható, hogy miért ez az alapértelmezett hitelesítési módszer: biztonságos, a jelszó sosem megy át a hálózaton, és kézenfekvő is használni.

Basic

Ha más böngészőnk van mint az IE, akkor nem biztos, hogy működik majd az Integrated típus, és még az is lehet, hogy nem a háttérben, azaz a felhasználó egy felugró hitelesítő ablakkal találkozik, de azért szerencsére nem weboldalanként, hanem session-onként eggyel. Ha a Basic metódust használjuk, akkor a hitelesítési adatok enkódolva (Base64), de nem titkosítva utaznak a hálózaton, ami nem túl megnyerő, mivel a Base64 pillanatok alatt, komoly erőfeszítés nélkül megfejthető. E metódus előnye tehát a teljes körű kompatibilitás, az alkalmazásokkal és a böngészőkkel, de ennek ellenére – pl. SSL nélkül – nagyon nem ajánlott. Ha mégis ezt választjuk, a következő figyelmeztetést kapjuk a TMG-től:



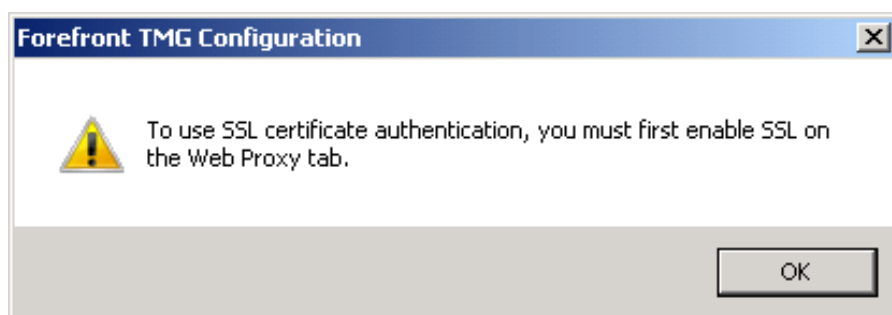
⁵⁹ Ezzel akkor, ha minimum IE7-ről van szó.

7.9 ÁBRA A TMG SÍKIT

A Basic hitelesítésről még annyit, hogy az ugyanezen ablakban látható „Select Domain” gomb csak akkor használható, ha a Basic hitelesítést is kiválasztottuk. E gomb alatt az alapértelmezett tartomány mellett egy alternatívát is megadhatunk.

SSL Certificate

A TMG ebben az esetben a kliens oldali tanúsítvánnyal történő hitelesítést preferálja. Ehhez tipikusan egy intelligens kártyán vagy egy mobil eszközön (pl. PDA vs. ActiveSync) megtalálható tanúsítványra lesz szükség.



7.10 ÁBRA A TMG MEGINT SÍKIT

Ha ezt a hitelesítést akarjuk használni, akkor muszáj a proxy szerver fő beállító ablakában (7.4 ábra) be kell állítanunk a web proxy portját az SSL-re (és a tanúsítványt is mellékelni kell), erre figyelmeztet ez a felugró ablak.

Digest

A Digest egy érdekes "állatfajta", mert ugyan a nevéből ez nem derül ki, de egy típus mögött valójában kettő van. A klasszikus típus a HTTP 1.1-et használja, azaz a böngészőnek ezt ismernie kell, valamint minimum Windows 2000 tartomány is kell hozzá (erre figyelmeztet a következő ábrán látható üzenet).



7.11 ÁBRA A SÍKÍTÁS KONSTANS A DIGEST-NÉL IS

A KAPUN TÚL

No meg a legnagyobb problémára: a működéséhez a felhasználók *jelszavait* (és nem a hash-eket) kell tárolnunk az AD-ban ☺. Ezt ugye a felhasználó tulajdonságai között, vagy a Csoportházirendben tudjuk beállítani ("Store password using reversible encryption"), de szigorúan tilos, és azt hiszem nem kell magyarázni az okot.

Ellenben, ha az ISA2004/2006/TMG minimum Windows Server 2003 tartományban van, akkor az alapértelmezés a Digest esetén a WDigest lesz. Ezt sehol sem látjuk az UI-n, de higgyük el⁶⁰. Ami még fontosabb: ekkor már nem kell a jelszavakat közprédának kitennünk. De azért maradt egy-két furcsaság továbbra is, pl. a tartomány/usernév páros megadása nagybetű/kisbetű érzékeny, ami semmilyen más hitelesítési módszerre nem jellemző.

RADIUS

A Remote Authentication Dial-In User Service (RADIUS) egy hálózati protokoll (RFC 2865), ami központosított hitelesítésre kérdését képes megoldani. Több helyen is használhatjuk, pl. munkacsoporti tagsággal tartományba történő hitelesítéshez (lásd ISA 2004/2006 Enterprise szerverek), tartományi felhasználók WLAN Access Point-kon keresztüli belépése, és még sorolhatnánk.

A TMG tehát képes RADIUS kliensként viselkedni és pl. a más platformról kapott RADIUS felhasználói hitelesítő adatokat fogadni és továbbküldeni a belső RADIUS szervernek⁶¹, amely viszont az AD-val van kapcsolatban, így bezáródik a kör, és működik a hitelesítés a RADIUS névtérből is.

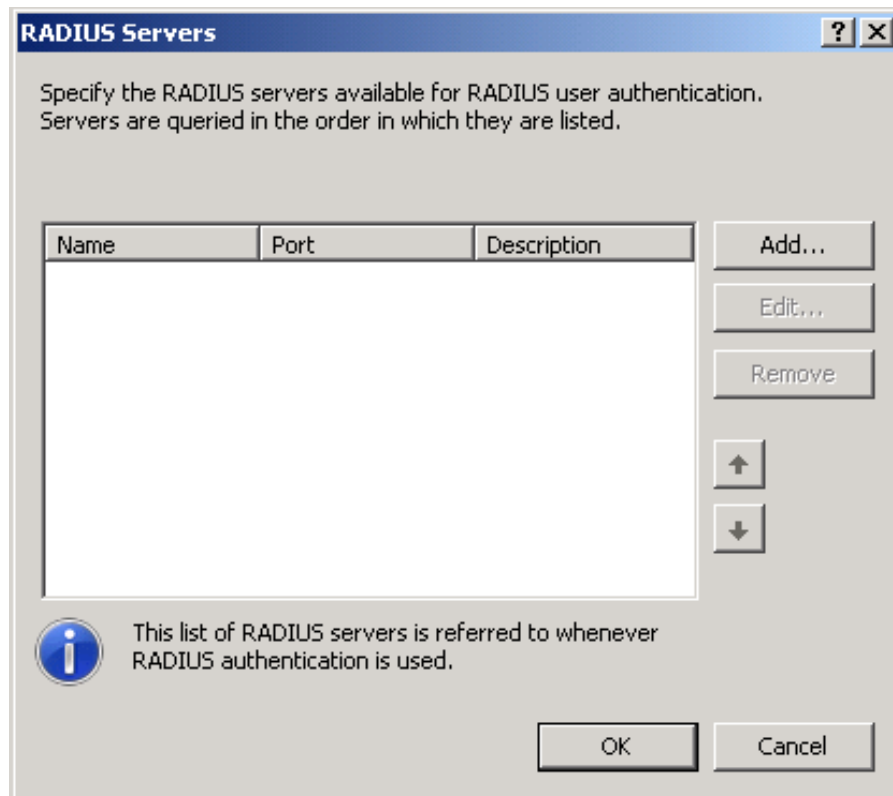
A működést tekintve egy további fontos információ, hogy ha a RADIUS hitelesítést használjuk, akkor a forgalom a kliens alkalmazások (pl. a böngészők) és a TMG között megint csak a Basic módszer, annak összes ismert hátrányával. Illetve itt érdemes megemlíteni, hogy a RADIUS forgalomban a RADIUS kliens (esetünkben a TMG) elküldi egy kérést a RADIUS kiszolgálónak, vagy egy RADIUS Proxy-nak. A kérés úgy hangzik nagyon leegyszerűsítve, hogy XY felhasználónak van-e hozzáférése. A RADIUS kiszolgáló a RADIUS házirendek alapján megválaszolja a kérdést, egy határozott IGEN vagy NEM-el. mi nincs itt ami egyéb azonosítás esetén van? Sok dolog, de pl. nincs információ a felhasználó csoporttagságáról. Vagyis, ha készítünk egy TMG szabályt, amiben azt mondjuk, hogy tartomány\csoportnak van joga az adott szabályon és RADIUS-t használunk akkor a felhasználónk hiába tagja a csoportnak, a TMG ezt nem

⁶⁰ Ha nekem nem hisszük el, akkor:

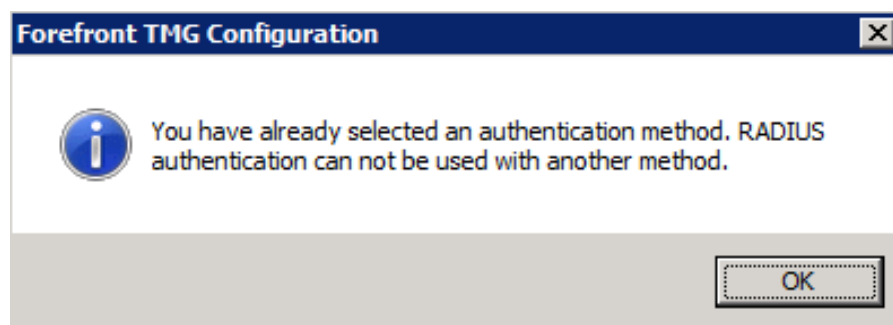
[http://technet.microsoft.com/en-us/library/cc780170\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780170(WS.10).aspx)

⁶¹ Methogy a Windows szerverekben is van egy RFC kompatibilis, teljesértékű RADIUS szerver, amit a Windows Server 2003-ig IAS-nak (Internet Authentication Server) hívtak, a Windows Server 2008 óta pedig az NPS (Network Policy Server) része.

„látja”. Így vagy egyesével felvesszük a felhasználókat egy User Set-be a RADIUS névtérből, vagy használjuk az All Authenticated Users előre létrehozott csoportot., ami tartalmazza az összes elérhető névtér köztük a RADIUS névtér sikeresen azonosított felhasználóit.



7.12 ÁBRA IDE KELL FELVENNÜNK A RADIUS SZERVEREKET, NÉVVEL, PORTTAL ÉS A SHARED SECRET KULCCSAL



7.13 ÁBRA A SÍKÍTÁS EGY VÉGTELEN DOLOG

A RADIUS bekapcsolásakor a figyelmeztetés (7.8 ábra) arra a célra szolgál, hogy rájöjjünk, hogy a RADIUS csak és kizárólag önmagában használható hitelesítési módszernek számít.

Viszont a RADIUS használatánál két dolgot feltétlenül a Kedves Olvasó lelkére kell kötnünk:

A RADIUS kliens (esetünkben a TMG) és a RADIUS kiszolgáló között van egy pre-shared key alapú azonosítás. Ezt a pre-shared key-t rendszeres időközönként illik cserélni, mint a fogkefét. És egy igazán komplex jelszót használunk erre a célra. Igazán komplex jelszó erős technikai felhasználók esetében minimum 32 karakter hosszú pass-phrase, amiben speciális karakterek is vannak. Személyes kedvencem a GUIDGEN-el generált több GUID összefűzése 😊.

A RADIUS kliens (még mindig TMG) és a RADIUS szerver közötti forgalmat a RADIUS protokoll nem védi. Ezért az iparági szabvány az, hogy ezt a forgalmat egyéb megoldással kell védeni. Vagy IPSec, vagy fegyveres őrrrel védett lengőkábel amin keresztül eléri a RADIUS kliens a RADIUS szervert. Azt hiszem az IPSec egyszerűbben implementálható, és tegyük is meg. Ne ringassuk magunkat abba a hitbe hogy ezt nem kell védeni. *(A lektor megjegyzése)*

7.5 AUTO DISCOVERY MEGOLDÁSOK

Az előző két alfejezet a proxy szerver oldali beállításairól szólt, a 3.4 fejezetben pedig ugyanezt taglaltuk a klienseknél is. Ez szép és jó, de sok esetben azt is meg kell oldanunk, hogy a szerver és a kliens automatikusan egymásra találjon. Persze manuálisan is be lehet gépelni a proxy címét⁶² (de nem mindig és mindenhol), de ez egyrészt nem elegáns, másrészt nem praktikus ha pl. sok gépünk van, illetve akkor sem, ha változik a TMG címe vagy adott esetben egy másik TMG-t kell használniuk a klienseknek. És van még egy olyan foratókönyv is, amikor nehéz a kliensek élete, és ez pedig az a helyzet, amikor valamilyen okból az alapértelmezett átjáró nem lehet a TMG-n belső lába, de azért a klienseknek muszáj látni a proxy is, ilyenkor is.

Nos, három eszközünk is van, ami igazából csak kettő, mert az első kettő gyakorlatilag szoros rokonságban van, egymás nélkül nem is működnek, és mindkettő egy hálózati megközelítést jelent, a maradék pedig egy TMG újdonság és az Active Directory-t használjuk majd hozzá.

WPAD

Tehát egészen a TMG-ig, a web proxy és a tűzfal kliensek számára csak a Web Proxy Automatic Discovery (WPAD) jelentette az egyetlen megoldást. Ez egy olyan protokoll, amely segítségével a kliens képes önállóan, a háttérben felfedezni a proxyt, majd egy szkriptet használva az alkalmazások értesére tudja hozni ezt az információt.

⁶² Most a Csoportházirendbe beírt proxy információkat vegyük ki a képből, mert először is ezt is változtatnunk kell, ha a változik a TMG címe/neve, másrészt nem használhatjuk csak az IE-hez, harmadrészt ez ugyan sokat segít, de végül is mégiscsak egy manuális megoldás, ami pl. egy laptop hazavitele esetén máris problémát okoz.

A WPAD protokoll a Microsoft "találmánya, és az IE5 óta használható. Ugyan a Microsoft bejegyezte az IETF-hez a szabványosítás érdekében, de a benyújtás elévült 1999-ben, az eredmény, azaz az ajánlás elfogadása nélkül. Ettől függetlenül természetesen használható maradt, és az IE mellett pl. a Firefox böngészőkben is alkalmazható.

A detektáláshoz először is elő kell készítenünk a TMG-t, majd pedig a két közvetítő szolgáltatást. Ezek a közvetítők az DHCP illetve a DNS szerver lesznek. A kliens (ebben a sorrendben) ezekhez fordul majd a WPAD bejegyzésért, majd ennek értelmében az adott TMG-hez, alapértelmezésben a TCP 80-as portot használva (de ha a DNS a közvetítő, akkor amúgy is csak és kizárólag ez a port jöhet szóba). Ezután a kliens a kapott konfigurációs fájlban lévő infót felhasználva beállítja önmagát (majd le is cache-eli a tartalmát), és nyertünk.



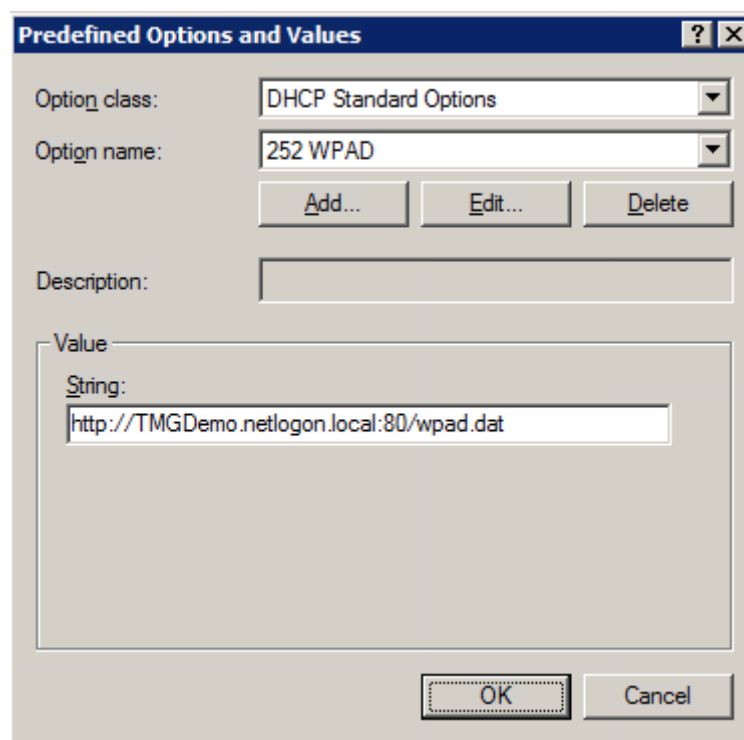
7.14 ÁBRA A PUBLIKÁLÁS RÉM EGYSZERŰ

A KAPUN TÚL

A TMG hálózatonként engedélyezi számunkra az automatikus észlelés beállítását (na persze a VPN-ek és a Local Host itt is kimarad), ergo csak azokban a hálózatokban kell ezt beállítani, ahol ezt a lehetőséget elérhetővé óhajtjuk tenni. Ezt a panelt egyébként az adott hálózat tulajdonságai között, az Auto Discovery fül alatt találjuk.

Ez még csak a bemelegítés volt, nézzük meg tehát elsőként DHCP szervert. A konzolban a szerverünk neve alatt az IPv4-es szakaszban⁶³ a tulajdonságok közül válasszuk a Predefined Options pontot (de lehetséges csak egy adott szkópban is, ha csak ezek a gépek érintettek).

1. A Predefined Options and Values ablakban > Add.
2. Az Option Type alatt a név legyen a "WPAD", a Data type: String, a Code pedig: 252, majd jöhet az OK.
3. A Value/String mezőbe írjuk be a TMG-nk címét, a portot és a fájl nevét, a következő ábrát mintául véve, majd OK.
4. Nyissuk ki a szkópunkat, majd Scope Options > Configure Options.
5. Keressük meg (könnyű lesz, ez az utolsó) és kattintsuk be a 252 WPAD opciót és készen is vagyunk.



7.15 ÁBRA A ÍGY NÉZ KI EGY WPAD OPCIO A DHCP-BEN

⁶³ Itt az egyetlen különbség az ISA-hoz képest: a TMG-ben IPv6 alapon is beállíthatjuk mindezt, hiszen a konfigurációs fájl támogatja ezt.

A DNS szerver felkészítése egyszerűbb. A címkeresési zónánkban (az összes érintettben, még a delegált zónákban is) hozzunk létre egy új Alias (CNAME) rekordot amelynek az aliasa a "wpad" sztring legyen, az FQDN-je pedig a TMG szerverünk komplett domain neve.

Két dolog, az amivel adós maradtam ebben a fejezetben:

1. Bármilyen meglepő, a DHCP használható statikus IP beállítású klienseken is, pl. a fejezet tárgyaként szolgáló feladatra. Ezt úgy kell elképzelni, hogy egy alkalmazás kérheti a Windows-t arra, hogy egy ún. DHCP Inform üzenetet küldjön. Ilyenkor a DHCP Inform tartalmazza azt, hogy melyik DHCP options-t (esetünkben a 252-t) kéri a kérő. A DHCP server válaszként az adott DHCP options-t visszaküldi és készen is vagyunk. Ez statikus beállítású kliensen is működik.
2. A másik pedig az, hogy Windows Server 2008-tól felfelé a DNS szerver (kiszolgálónként külön-külön!) a WPAD és az ISATAP rekordot alapértelmezés szerint egy ún. global query block listre teszi⁶⁴, és ha ezzel nem vagyunk tisztában, nem fog működni a WPAD rekordunk. Győződjünk meg ezen rekordok tiltásáról vagy engedélyezéséről a „dnscmd . /info /globalqueryblocklist” paranccsal.

A WPAD szkript és protokoll

Az egész eddig játék azt a célt szolgálta, hogy megszerezzük a wpad.dat konfigurációs fájlt, a leghitelesebb forrástól, magától a TMG szervertől.

Érdekességszámba megy, hogy eme szkript eredeti specifikációja a Netscape-től származik, 1996-ból. Aki minimum 30 éves, még simán emlékezhet erre az akkor remeknek számító böngészőket és más internetes klienseket fejlesztő cégre (no és persze volt egy nagyvállalati proxy szerverük is, ám pl. a szkriptjük a .pac kiterjesztést használta).

<http://web.archive.org/web/20080208114016/http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html>

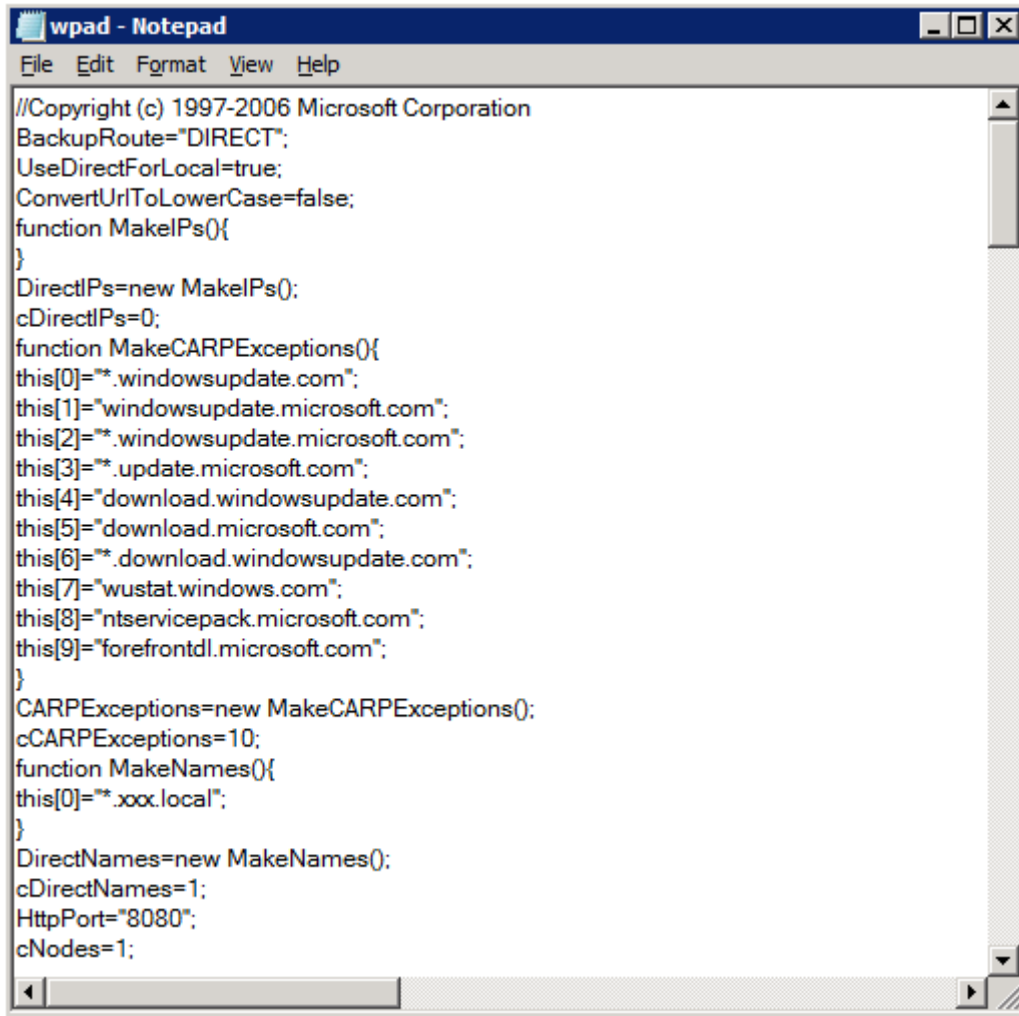
A szkript Jscript formátumú (ezt univerzálisan értik a böngészők), alapértelmezés szerint kb. 5 Kbyte, és jópár dologra fény derülhet a tartalmából a kliensek előtt. Konkrétan: mi történjen akkor pl., ha egy kért protokoll nem támogatott a web proxy által? Vagy melyek azok a célcímek, amelyek proxy nélkül is elérhetőek? Vagy mi történjen akkor ha a TMG nem elérhető? Vagy melyek azok a címek, amelyeket a CARP

⁶⁴ Pl. a DirectAccessnél is fel kell ezt oldanunk az ISATAP apropóján.

A KAPUN TÚL

(Cache Array Routing Protocol, a nagyvállalati, "tömbösített" gyorsítótár) nem gyorsítótár?

Egyébiránt a fájl tartalmaz egy TTL bejegyzést is, amely lejártá után a kliens törli a letöltött tartalmat, majd kér egy újat. Így alakul ki a korrekt, mindig pontos tartalom, és egyben ez a változások érvényesítésénél is alapvetően lényeges körülmény.



```
//Copyright (c) 1997-2006 Microsoft Corporation
BackupRoute="DIRECT";
UseDirectForLocal=true;
ConvertUrlToLowerCase=false;
function MakeIPs(){
}
DirectIPs=new MakeIPs();
cDirectIPs=0;
function MakeCARPExceptions(){
this[0]="*.windowsupdate.com";
this[1]="*.windowsupdate.microsoft.com";
this[2]="*.windowsupdate.microsoft.com";
this[3]="*.update.microsoft.com";
this[4]="download.windowsupdate.com";
this[5]="download.microsoft.com";
this[6]="*.download.windowsupdate.com";
this[7]="wustat.windows.com";
this[8]="ntservicepack.microsoft.com";
this[9]="forefrontdl.microsoft.com";
}
CARPExceptions=new MakeCARPExceptions();
cCARPExceptions=10;
function MakeNames(){
this[0]="*.xxx.local";
}
DirectNames=new MakeNames();
cDirectNames=1;
HttpPort="8080";
cNodes=1;
```

7.16 ÁBRA CSAK AZ ELEJE ILYEN ÉRTHETŐ

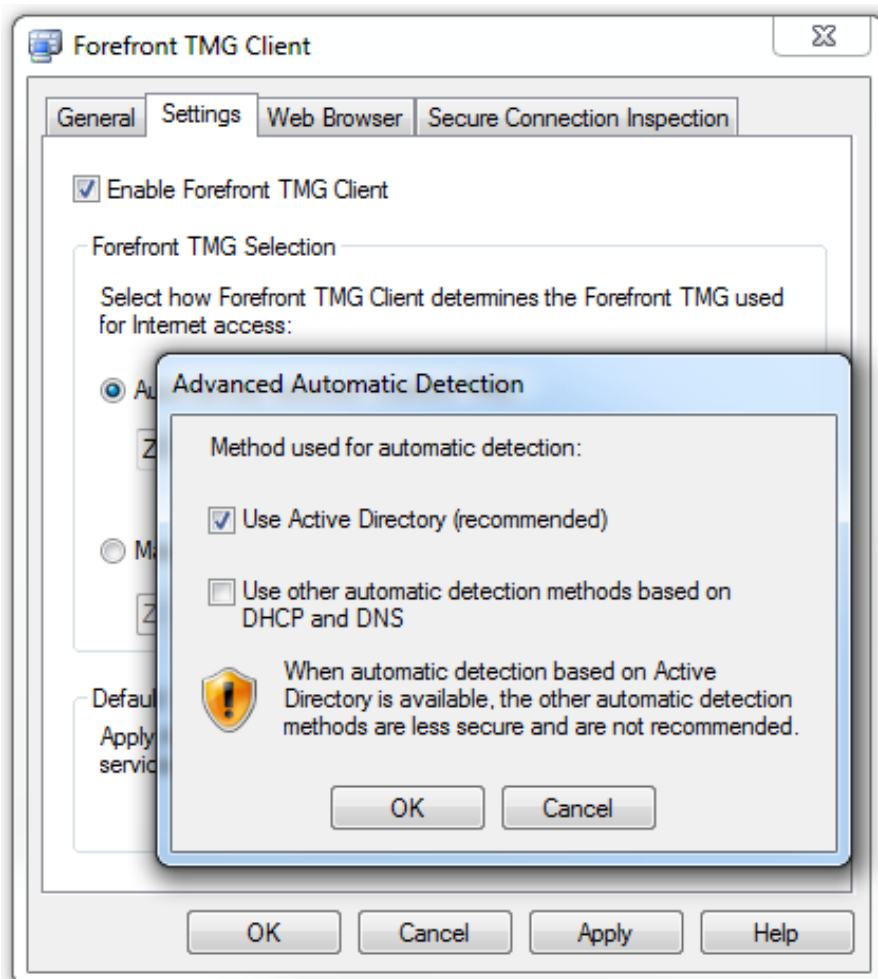
Bár igen izgalmas téma ez, további részletekbe itt már nem megyünk bele, ellenben találunk bőven forrást a neten, pl. itt:

<http://technet.microsoft.com/en-us/library/cc713344.aspx>

Forefront TMG Auto Discovery Configuration Tool

A TMG-vel és az új tűzfal klienssel egy tisztább, szárazabb megoldást is kapunk. Ugyanis innentől az Active Directory-t használhatjuk is a wpad.dat lelőhelyének tárolására (gyakorlatilag ez egy SCP, azaz Service Connection Point, mint az Exchange AutoDiscover-nél), ami egyrészt biztonságosabb, másrészt lényegesen kézreállobb a

kivitelezése. Az új megoldás nem zárja ki a régieket, csak éppen optimális esetben (ez még lényeges lesz!) a sorban hátrébb taszítja, értelmesebben szólva tartalék módszerre fokozza le.



7.17 ÁBRA AZ ÚJ TŰZFAL KLIENSZEN ILYEN IS VAN⁶⁵

A manőverről:

1. A tűzfal kliens LDAP lekérdezéssel az AD-ből kizsedi a TMG elérési útját illetve a portját.
2. Ha bármilyen ok miatt nem tud kapcsolódni az AD-hoz, akkor nincs failover (erre hoztam fel az előbb az optimális esetet), azaz ilyenkor egyáltalán nem érdekli az esetleges DHCP/DNS infó, hanem bont.
3. Ha van AD kapcsolat, de üres a WPAD infó, akkor jöhet először a DHCP, majd a DNS módszer.

Hogy érjük el ezt? Nem is bonyolult.

⁶⁵ Nézzük csak meg alaposan a tűzfal klienst: van egy negyedik füle! De erről majd a 9.2 fejezetben lesz szó.

A KAPUN TÚL

1. Töltsük le a TMG 2010 Tools & Software Development Kit-ből a Auto Discovery Configuration Tool for Forefront TMG 354 Kbyte-os kis csomagját (a bétában még ezt AD Marker Tool-nak hívták).
2. Telepítsük fel a TMG szerveren.



7.18 ÁBRA MÁR TELEPÜL IS

3. Goto admin parancssor (sortörés nélkül):
tmgadconfig add -default -type winsock -url
http://a.szerverünk.fqdn.neve:port/wspad.dat⁶⁶
4. Kész.

Háromféle módon győződhetünk meg a sikerről (a harmadik az igazi, az első kettő csak érdekes):

1. Indítsunk a tartományvezérlőn egy ldp.exe-t és a szokásos módon navigáljunk el az utolsó képen látható helyre.
2. Kliens OS > parancssor > C:\Program Files (x86)\Forefront TMG Client, majd "fwctool testautodetect"

⁶⁶ Kicsi furcsaság: a tmgadconfig.exe elérési útja nem a szokásos TMG mappa, hanem a \Program Files (x86)\Microsoft Forefront TMG Tools\AdConfig

3. Telepítsük fel az új tűzfal klienst, és ha a telepítés elején bepipáljuk az automatikus beállítást, a végén meg kell jelennie a tűzfal kliensben a szerverünk nevének (a sorrend beállítását lásd az első képen).



7.19 ÁBRA AZ LDP.EXE-VEL MINDIG MINDEN KIDERÜL

Microsoft Forefront Threat Management Gateway (TMG) 2010 Tools & Software Development Kit

<http://www.microsoft.com/downloads/details.aspx?FamilyID=8809cfda-2ee1-4e67-b993-6f9a20e08607&displaylang=en>

7.6 CACHE AVAGY TÁRAZZUNK GYORSAN

Azt vettem észre az elmúlt - kb. egy évtizedet felölelő ISA és TMG tanulmányaimban -, hogy kissé mostoha téma ez a különböző könyvekben és tanfolyamokon (és magában a termékben is hátraszorult kissé az évek során), pedig komoly előnyökre tehetünk szert e témakör megfelelő ismeretével és alkalmazásával.

A TMG webes gyorsítótárával akár feltűnő teljesítménynövekedéshez (azaz jelentős válaszidő csökkentéshez) is juthatunk, ugyanis lehetséges úgy hangolni a proxyt, hogy a gyakran lekért objektumokat tárolja el, és a felhasználókat "helyben", a TMG szolgálja ki. Ezt a technikát ismerhetjük a böngészők hasonló módszeréből is, csak hogy ez egy lényegesen összetettebb megoldást takar, granuláris szabályzással, nem beszélve arról, hogy már két felhasználó esetén is 100%-kal több lehet a hasznos, eltárolt tartalom (na jó, csak akkor ha sosem nézik ugyanazokat az oldalakat ☺).

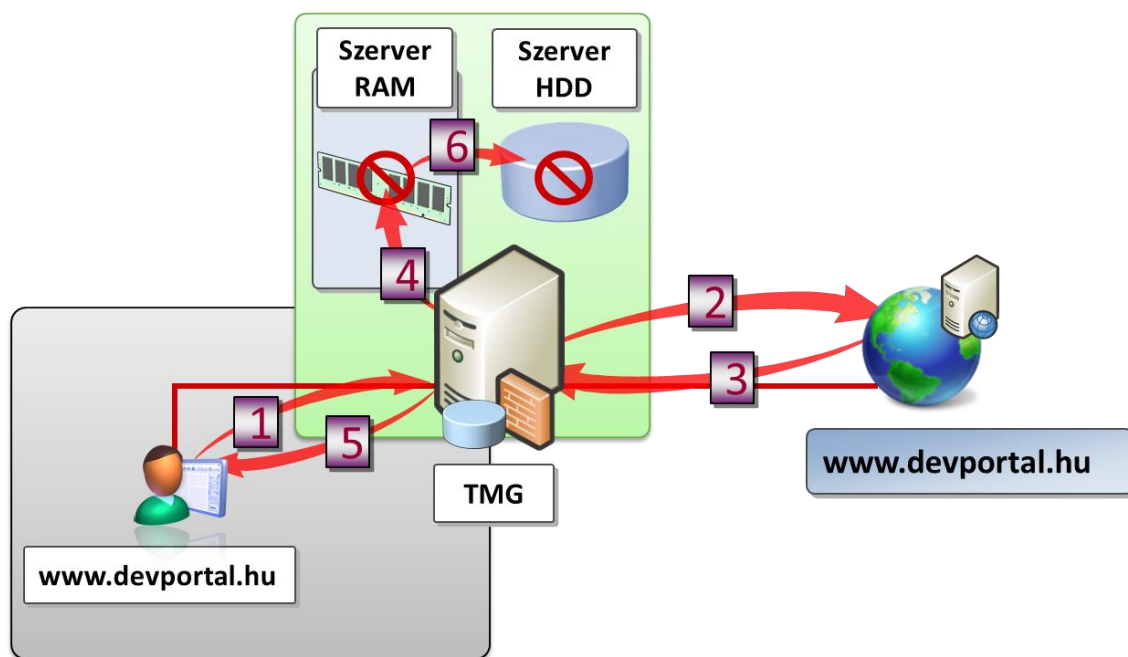
Persze a "sosem elég" típusú sávszélesség nem fog fizikailag nőni, de a felhasználók komfortérzete viszont biztosan, nem beszélve pl. a mindenképpen szükséges letöltések (pl. biztonsági frissítések) használatának kérdéséről.

Bevezetésként még annyit megemlítenék, hogy ugyan már a TMG Standard verziójában is egy kifinomult cache fájl- és tartalom szabályzást kapunk, de ez semmi az Enterprise verzióban használható CARP (Cache Array Routing Protocol) megoldáshoz képest. Az egy nagyágyú, de az alapverzióval is azért lehet nagyokat lőni.

7.6.1 HOGYAN MŰKÖDIK A WEB PROXY CACHE?

Az ISA és a TMG szerverek a HTTP és az FTP objektumok gyorsítótárazását képesek elvégezni, RAM-ba és lemezre (ebben a sorrendben), és a forgalom szempontjából mindkét irányba.

A **Forward Caching** a tipikus irány, hiszen valószínűleg a belső hálózathoz több webszerver tartalmat tekintenek meg a felhasználók, mint amennyi külső kérés a saját webszerverünk felé áramlik. Nézzük meg először, hogy hogyan történik a gyorsítótár feltöltése.

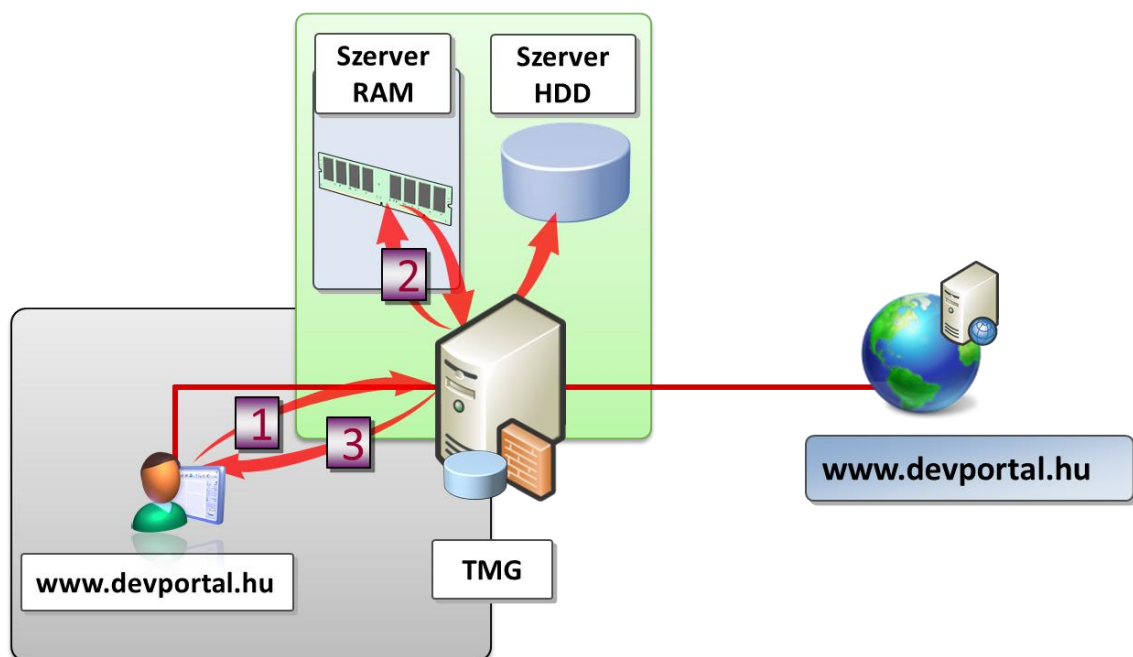


7.20 ÁBRA A FORWARD CACHE MŰKÖDÉSE, I RÉSZ.

1. Szóval, amikor a felhasználó a saját gépéről egy HTTP/FTP objektumot szeretne elérni, a web proxy kliens odafordul a proxy szerverhez, és kezdődik a násztánc. De, alapértelmezés szerint a Firewall szervíz a tűzfal és a SecureNAT kliensektől származó HTTP kéréseket is forwardolja, ergo minden kliens élvezheti a gyorsítótár áldásos működését, de mindig csak a web proxyn keresztül.

2. Az első lépésben a TMG ellenőrzi, hogy esetleg nincs benne-e ez a tartalom a gyorsítótárban. Ha nincs, vagy ha az érvényessége már lejárt (ez pl. a fejléc infó alapján kiderülhet), akkor a TMG továbbküldi a kérést a távoli webszerver felé.
3. A TMG megkapja a választ (és a tartalmat) a webszervertől.
4. A Web proxy elhelyezi ezt a tartalmat a memóriába (RAM). Ez az első lépcső, ami ide bekerül, az villámgyorsan kiszolgálható lesz, de nyilván nem korlátlan ideig és méretben.
5. A TMG kiszolgálja a felhasználót, azaz elküldi neki is a tartalmat.
6. Egy idő után a web proxy a RAM-ból átmásolja a merevlemezre ezt a tartalmat. Ha nincs sűrűn használva, akkor a RAM-ból ki is kerül végelegesen, azaz innentől csak a lemeztől lesz elérhető.

Ez volt bekerülés menete, idáig még nem segítettünk semmit a klienseken, de most akkor nézzük meg, hogy hogyan szolgálja ki a TMG az ugyanezen tartalom felől érdeklődő *második* klienst.



7.21 ÁBRA A FORWARD CACHE MŰKÖDÉSE, II. (BEFEJEZŐ) RÉSZ.

1. A második jelentkező az eddig megismert folyamatnak megfelelően felkeresi a TMG-t a kérésével, a TMG pedig rutinból letolja azt a web proxynak.
2. A web proxy megtekinti a gyorsítótár két részben előforduló tartalmát (RAM, diszk) majd ha talál megfelelő tartalmat, akkor annak érvényességét is. Ha minden rendben van, akkor elkezd kiszolgálni a klienst
3. A kliens böngészőjébe megérkezik a tartalom, anélkül hogy az ábra jobb szélén lévő külső webszervert zargattuk volna.

A másik fő típus, a **Reverse Caching** lényege a webserverek tartalmának gyorsítótárazása. Ha egy kérés érkezik a belső, vagy a Perimeter hálózatban lévő webserverekhez, akkor az először valószínűleg a TMG-hez érkezik meg. Az adott publikáló szabálynak megfelelően a TMG továbbküldi a kérést a webservereknek, amely aztán válaszol, először megint csak a TMG-nek. Ekkor az éppen jelen lévő tartalom "lemásolódik" a gyorsítótárba a már ismert lépésekben, és így újból kiszolgálható lesz az esetleges ismételt külső kérések apropóján.

A kényelmi szolgáltatások szintjét tovább emelhetjük, az ún. **Content Download Job** megoldással, amely segítségével időzített letöltések elvégzésére, majd az eredmény gyorsítótárba pakolására utasíthatjuk a TMG-t. A cache finomhangolása során erre még visszatérünk.

A működéshez hozzá tartozik még a cache kezelése is, optimalizálása is. Például több szó is esett már az érvényességről, ami kifejezetten fontos, egy szögletes példát említve, egy tőzsdei adatokat tartalmazó weboldal legtöbb objektumát nem tárolhatjuk el örökké, és nem adhatjuk oda a felhasználónak, mint egy új tartalomként. Éppen ezért, bármilyen objektum is kerül be a TMG cache-ébe, rögtön egy Time-to-Live (TTL) értékkel lesz ellátva, amely lejáratáig szabad csak kiszolgáltatni a klienseknek. A TMG maga is képes ezt az értéket belőni pl. a létrehozás és a változtatás dátumának alapján, illetve mi is tudjuk ezt az értéket változtatni globálisan és egy-egy cache szabályon keresztül is. És persze egy lényeges dolgot ne felejtsünk el, ha az adott weboldal egy meta tagja szerint már van gyárilag beállított lejárat az oldalnak, akkor azt a TMG elsődleges jelleggel veszi figyelembe.

Egyébként sem történik meg minden tartalom automatikus gyorsítótárazása, a kivételek listájában a következők biztosan benne vannak:

A HTTP response header alapján: Cache-control: no-cache; Cache-control: private; Pragma: no-cache; www-authenticate; Set-cookie

A HTTP request header alapján: Authorization, Cache-control: no-store

A cache optimalizálása egy sok tényezős feladat, amelyben a TMG a következő dolgokat veszi figyelembe:

- A tárolási sorrendről volt már szó, azaz először a gyors RAM, majd a merevlemez a sorrend. De emellett a RAM-ban tárolt tartalom egy mappaszerkezet szerű formátumban történik, így gyorsítva az elérés és főleg a megtalálás időtartamát.
- A TMG egyetlen fájlban tárolja a merevlemezen a gyorsítótár tartalmát, amelyet a létrehozásakor előre le is foglal fájlrendszerben, az általunk beállított méret

alapján. Párhuzamosan, több partícióra is elpakolhatjuk a gyorsítótárat, ilyenkor partíciónként egyetlen fájlban leledzik majd a tartalom. Ez szintén az elérés gyorsítását jelenti, hiszen nem 10.000 fájlt kell nyitni-zárni, hanem mondjuk egyet.

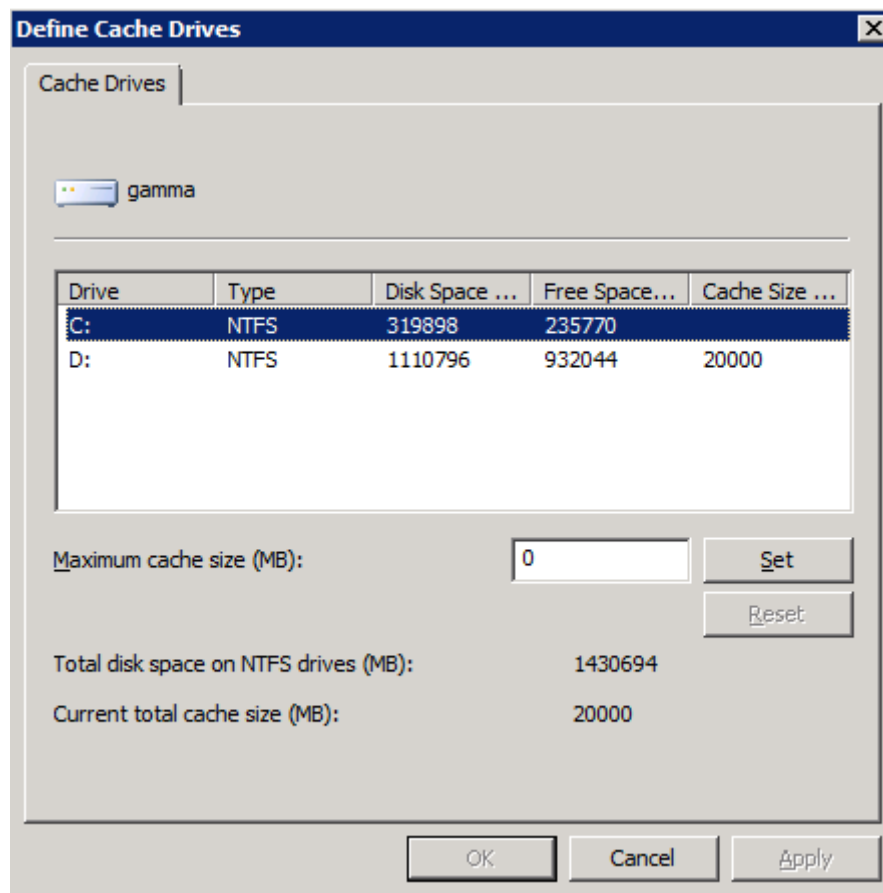
- A TMG villámgyorsan képes a gép indításakor felépíteni a gyorsítótárat (a szerkezettel együtt, mert a lemezen is ilyen formában tárolódik az adott fájl belsejében), akkor is, ha valamilyen zűr támadt a fájlrendszerben, vagy pl. egy nem tervezett leállás után.
- Mind a RAM, mind a merevlemez esetén a TMG automatikusan eltávolítja a nem sokat vagy nem sűrűn egymás után elérni kívánt tartalmat – és akkor mindenképpen, ha a mindkét esetben beállítható mérethatárhoz közelít a gyorsítótár.

7.6.2 A GYORSÍTÓTÁR FINOMHANGOLÁSA

Ennyi elmélet után nézzük meg a TMG gyorsítótár beállítható tulajdonságait és pl. a cache szabályok létrehozását és működését. A TMG-ben a cache beállítások kikerültek a faszerkezet legfelső szintjéről és immár a legegyszerűbben a Web Access Policy-ból érhetőek el (Web Caching a középső keret fejlécében). Ha engedélyezve van (alapértelmezés szerint nincs) és ezt megnyitjuk, egy öt füllel rendelkező panel kapunk, amelyből az első csak az összegző, azonban a második (Cache Drives), a különböző partíciókon már lefoglalt cache jellemzőit sorolja fel.

Ha itt a konfigurálást választjuk, akkor szintén partíciónként létrehozhatunk lefoglalásokat a cache számára. A cache törlése is csak innen működik, ti. ha megkeressük a fizikai megjelenését a fájlrendszerben (pl. D:\urlcache\Dir1.cdat), akkor ott hiába próbálkozunk a törléssel, a TMG nem engedi⁶⁷. Ha viszont itt nullára állítjuk a "Set" gombbal vagy használjuk a "Reset" gombot, akkor töröltük is. Ha ez volt az egyetlen partíció, amelyen a cache-t tároljuk, akkor a Web Access Policy keretben is "Disabled" állapotúra vált a gyorsítótár állapota.

⁶⁷ Amíg megy a Firewall szerviz, ha viszont leállítjuk, sima ügy a törlés.



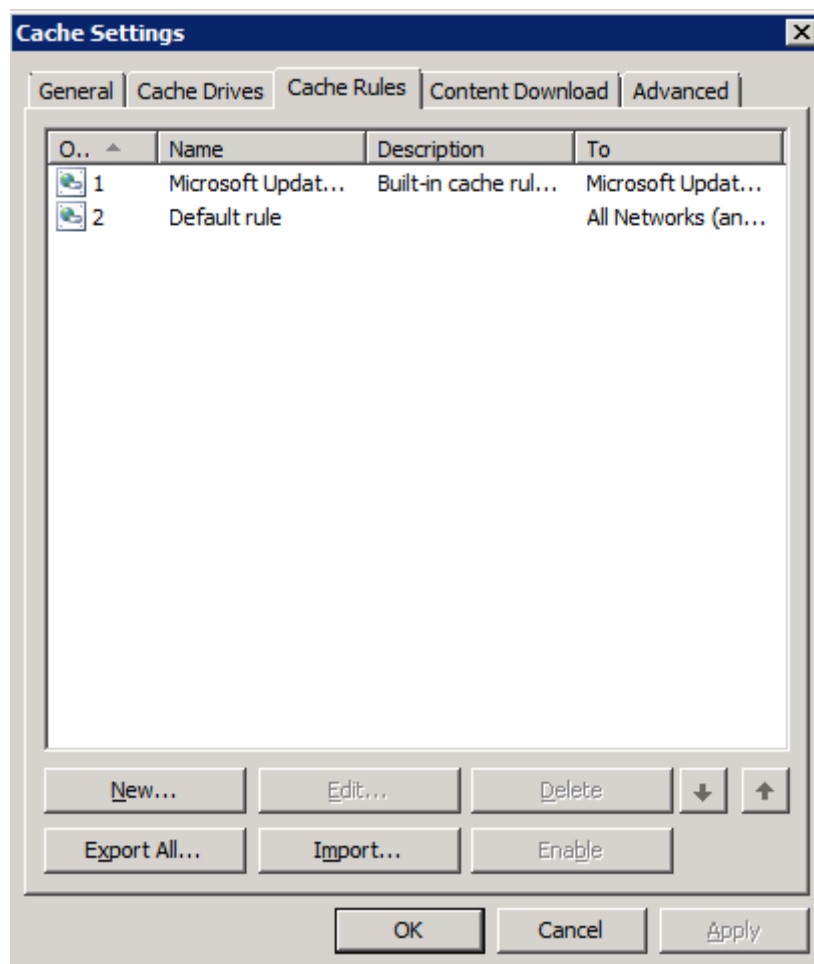
7.22 ÁBRA A MENNYISÉG SZÁMÍT

Ha viszont már itt tartunk, nézzünk meg egy-két megszorítást illetve ajánlást a cache tárolásával kapcsolatban:

- Kizárólag egy helyi NTFS partíció jöhet számba a cache tárolására.
- Partíciónként maximum 64 GB lehet a cache mérete.
- Ha van víruskereső, akkor hatása alól vegyük ki a cache helyét.
- Nagyon célszerű egy külön lemezre elhelyezni a cache-t, lehetőleg egy olyanra, amelyet mással nem is terhelünk, és ami nagyon gyors eléréssel rendelkezik⁶⁸.
- Rendszerlemezre és arra a lemezre/partícióra amelyen a pagefile van, szintén nem ajánlott a cache-t tervezni – amelynek elsősorban megint csak teljesítmény okai vannak.
- Cache méret kiszámítása = méret + (user*0,5MB) = 4000MB + (100*0,5) = 4050MB
- Lemezek száma = (Peak request / sec * Cache Object hit ratio)/100 = 1500*0,4 / 100 = 6 lemez

⁶⁸ Best Practices for Performance in ISA Server 2004 (benne pl. a cache méretezés, képletrel, egyébekkel): <http://technet.microsoft.com/en-us/library/cc302518.aspx>

Ha továbblépünk, a Cache Rules fülre akkor a cache működését alapvetően befolyásoló szabályokat tudjuk megtekinteni. A TMG esetén kettővel már rendelkezünk is a telepítés után, egy alapértelmezettel, illetve a Microsoft Update Cache Rule nevűvel. Vegyük figyelembe hogy sorszámokat is látunk itt, ami nem véletlen: a szabályok végrehajtásának sorrendje a hozzáférési tűzfalszabályokénak felel meg és a jobb alsó sarokban levő nyilakkal variálhatjuk.



7.23 ÁBRA A KÉT ALAPSZABÁLY

Az alapértelmezett szabály (Default rule) egy alig módosítható szabály a gyári alapbeállításokkal (hogyan akkor is működjön a cache), ha megnyitjuk, minden opció szürke. Ugyanez a helyzet ez 1. számúval is, ami viszont az ISA szerverekben még nem volt gyárilag működő, de itt már igen. Ez a szabály az összes Windows/Microsoft Update oldal tartalmát gyorsítótárazza. Ennek komoly előnye lehet akkor, ha nincs WSUS, vagy SCCM a rendszerben, hiszen akkor a kliensek biztosan többször és viszonylag sűrűn látogatják ezeket a szervereket. Amennyiben ez nekünk felesleges akkor törölhetjük, letilthatjuk vagy akár módosíthatjuk is ugyanitt, de az is látható hogy az export/import is innen indulhat.

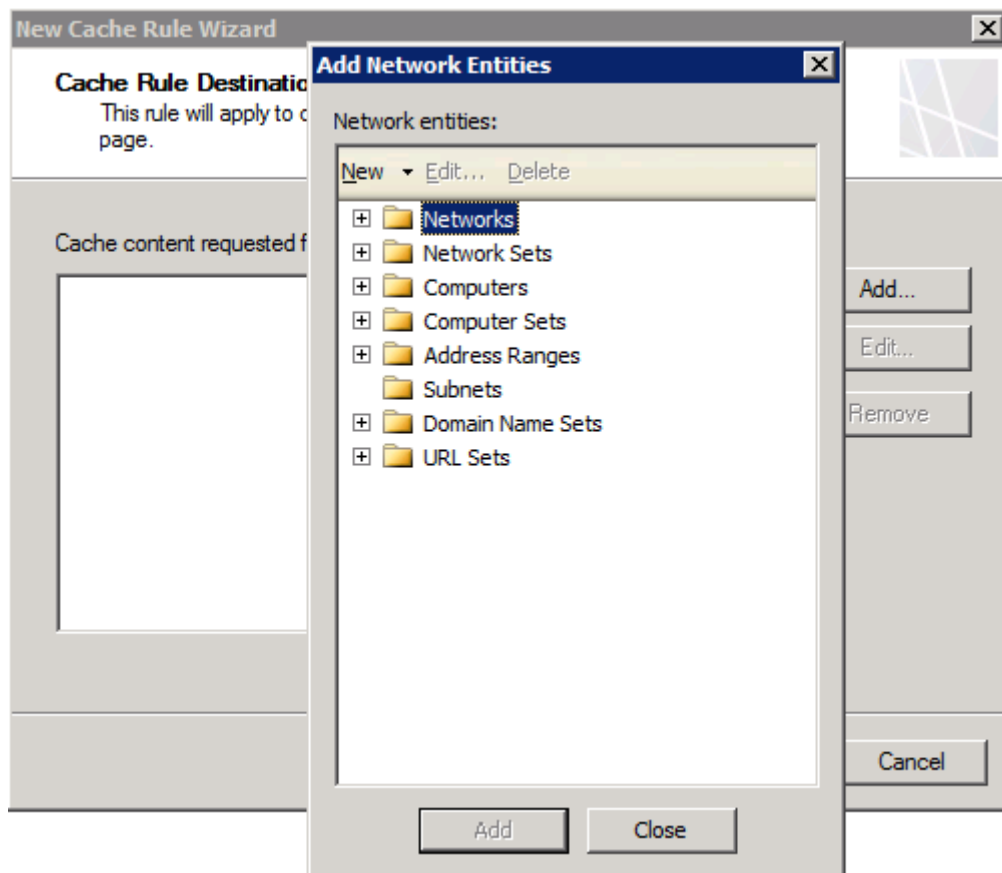
A KAPUN TÚL

De most hozzunk nézzük meg egy cache szabály létrehozása közben, hogy milyen részleges lehetőségeink vannak e területen.



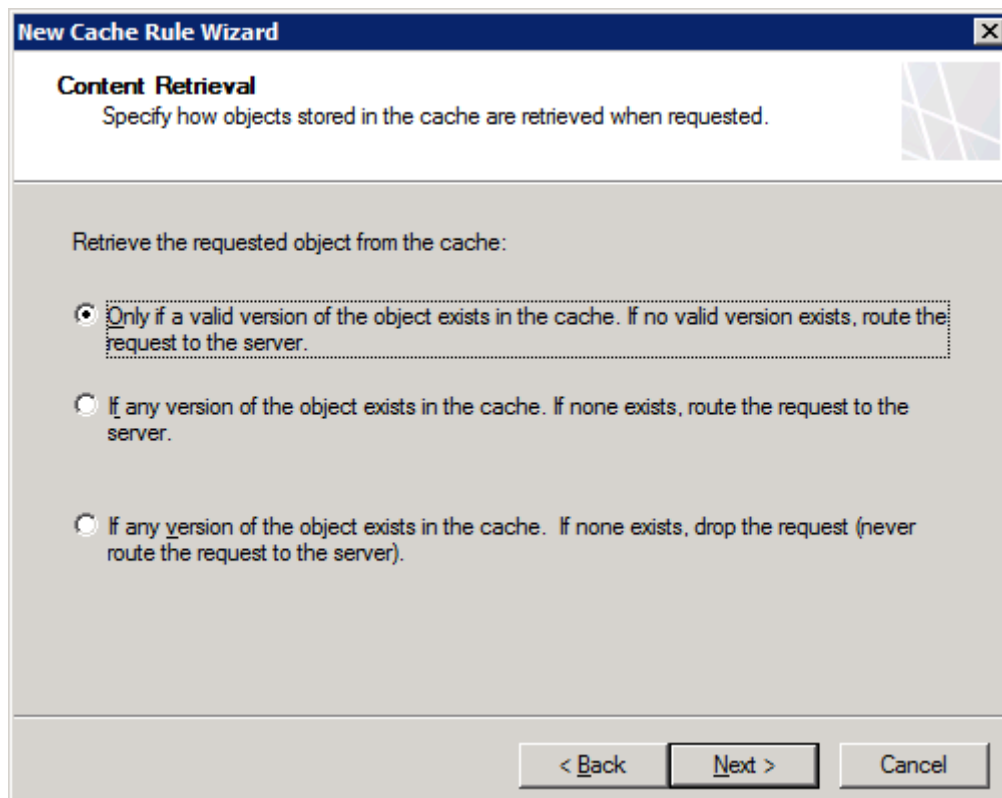
7.23 ÁBRA EZ EGY NÉV

A név meghatározása meg kell határozni a kérés alanyát. Az itt meghatározott alanyhoz érkező kérésekre fog vonatkozni a létrehozott gyorsítótár konfigurációs szabályunk. Mint az a következő ábrán látható, a lehetőségek száma a forrás kijelölésére egészen tágas.



7.24 ÁBRA RETTENTŐ SOKFÉLE HELYRE ÉRTELMEZHETŐ A CACHE

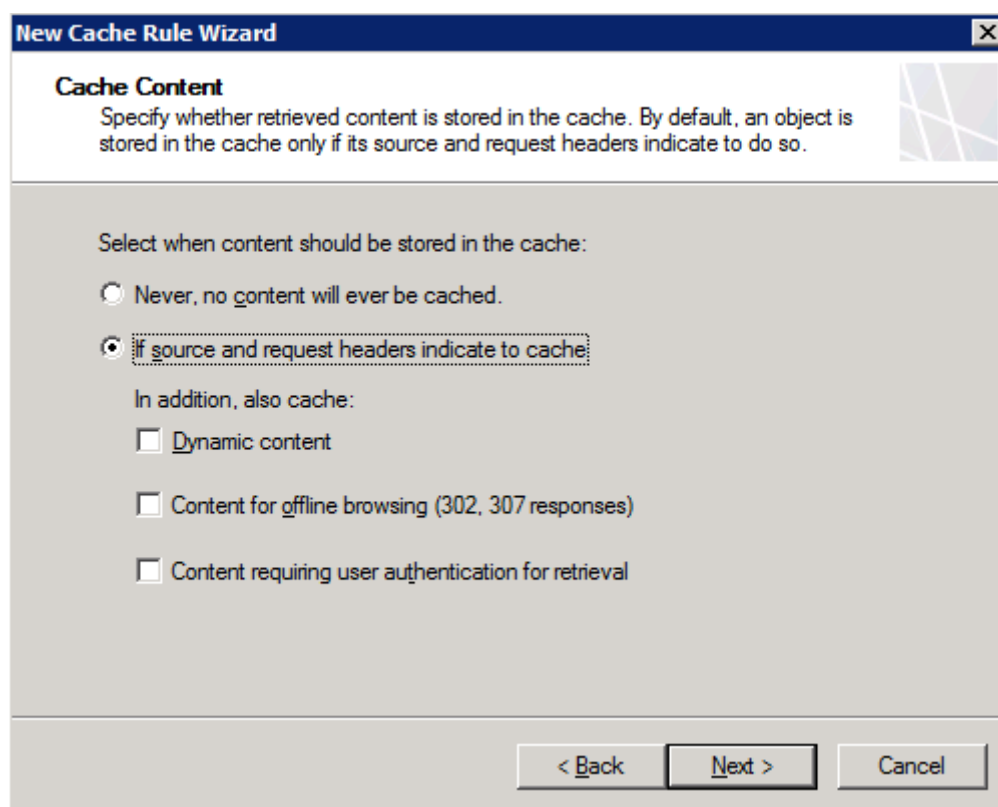
Válasszuk ki pl. a belső hálózatot, aztán lépünk tovább.



Nos, ez itt már egy komolyabb dolog, mint az eddigiek. Azokat a feltételeket szabjuk itt meg, amelyek alapján megkaphatja a felhasználó az adott tartalmat.

- *Only if a valid version of the object exists in the cache. If no valid version exists, route the request to the server:* Csak akkor kapjuk meg, ha még érvényes a tartalom. Ha nem, a kérés továbbítódik a cél kiszolgálóhoz.
- *If any version of the object exists in the cache. If none exists, route the request to the server:* Ha van bármilyen passzoló tartalom a cache-ben, akkor azt kiadja a TMG.
- *If any version of the object exists in the cache. If none exists, drop the request (never route the request to the server):* A különbség az előzővel szemben az, hogy az ha ezt választjuk, akkor ha nincs bármilyen passzoló tartalom, akkor sohasem küldi tovább a felhasználót a cél kiszolgálóhoz a TMG.

Kicsit nehéz ennek a pontnak az értelmét megtalálni, de talán az egy elképzelhető eset, hogy egy korábban már letöltött tartalmat akarunk megmutatni mondjuk egy tanítási óra keretében, de a netre semmiképpen nem mehetünk ki eközben. Illetve akár a Schedule Download Job segítségével egyszer, egy számunkra kedvező pontban letöltöttük a cache-be az adott tartalmat és így csak azt szabad böngészni.

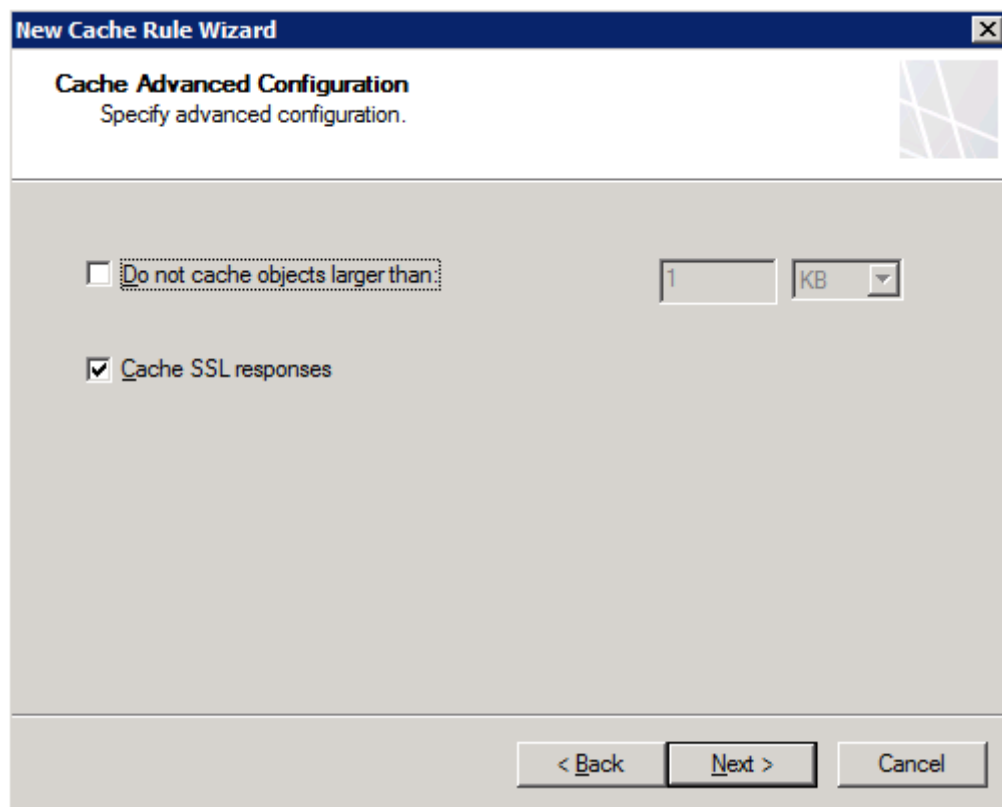


7.26 ÁBRA MI KERÜLJÖN BELE?

A most következő beállítások a cache-be kerülés feltételeivel foglalkoznak.

- *Never, no content will ever be cached:* Ez egy kifejezetten fontos opció. Ha egy vagy több oldalt egyáltalán nem akarunk gyorsítótárazni, akkor készíthetünk rá olyan szabályt, amelyben itt kérjük a tiltást. Persze, akkor a mostani példában a legelején említett Internal hálózat helyett egy URL Set-et vegyünk fel (és ebbe tegyük bele a kívánt webcímeket).
- *If source and request headers indicate to cache:* Minden tartalom mehet a cache-be, ha meg van jelölve erre.
- *In addition, also cache: Dynamic content:* Mehet azok a dinamikus tartalmak is, amelyeket pont azért nem szoktunk eltárolni, mert változnak (az URL-ekben az első kérdőjel (?) utáni következő sztring szakasz jelöli ezt általában).
- *In addition, also cache: Content for offline browsing (302, 307 responses):* Még azok az oldalak is mehetnek a cache-be, amelyek ezekkel a HTTP státusz kódokkal jelöltek (ideiglenesen áthelyezve, illetve átirányítva)
- *In addition, also cache: Content requiring user authentication for retrieval:* Nos, ez a lehetőség tűnhet feleslegesnek is, hiszen a hitelesítéshez kötött tartalom letárolásáról szól.

Nos, ha nem egy adott URL Set tiltását kérjük, akkor van még tovább is.



7.27 ÁBRA KÉT HALADÓ OPCIÓ

Itt elsőként szabályozhatunk méretre, azaz megtilthatjuk azt, hogy egy bármekkora objektum is bekerüljön a cache-be. Ennek a HTTP letöltések, vagy az FTP tartalom apropóján lesz igazán értelme. De - és ez szintén furának tűnik elsőre – kérhetjük az SSL tartalmak tárazását is. Da ha tudjuk, hogy mindezt csak az SSL Bridging-re vonatkozik (lásd 9.3 fejezet), akkor már nem is olyan fura.

New Cache Rule Wizard

HTTP Caching
Unless the source specifies an expiration time, HTTP objects stored in the cache are updated according to the time-to-live (TTL) settings.

☒ **Enable HTTP caching**
TTL is the amount of time content remains in the cache before it expires. Content age is the amount of time since an object was created or modified.

Set TTL of objects (% of the content age):

TTL time boundaries:

No less than: Minutes

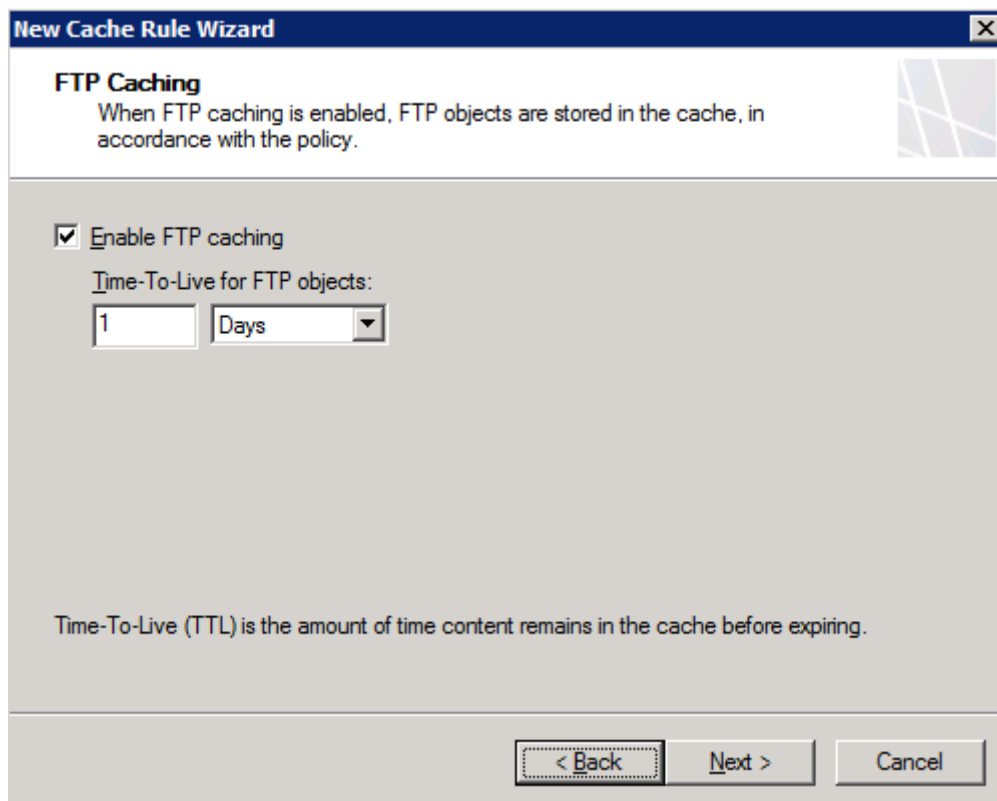
No more than: Days

☐ Also apply these TTL boundaries to sources that specify expiration

< Back Next > Cancel

7.28 ÁBRA A HTTP GYORSÍTÓTÁRAZÁS FELTÉTELEI

Most ismét egy komplexebb beállításcsokor jön. Először is engedélyezhetjük a HTTP tartalom eltárolását, és ha szeretnénk ezt, akkor konfigurálhatjuk a már ismerős elévülési időtartamot, amely alapesetben 20%-kal van megnövelve az eredeti tartalom TTL-jéhez képest. De további finomhangolás is lehetséges a következő részben, ahol a "nem kevesebb" és a "nem több" értékeket is beállíthatjuk. Sőt, a "Also apply these TTL boundaries to sources that specify expiration" bepipálásával felülírhatjuk az oldallal érkezett érvényességi jelzéseket, az itt megjelöltekre, ami egy kicsit már veszélyesnek is tűnik számomra, de ezt mindenki önállóan dönti majd el.

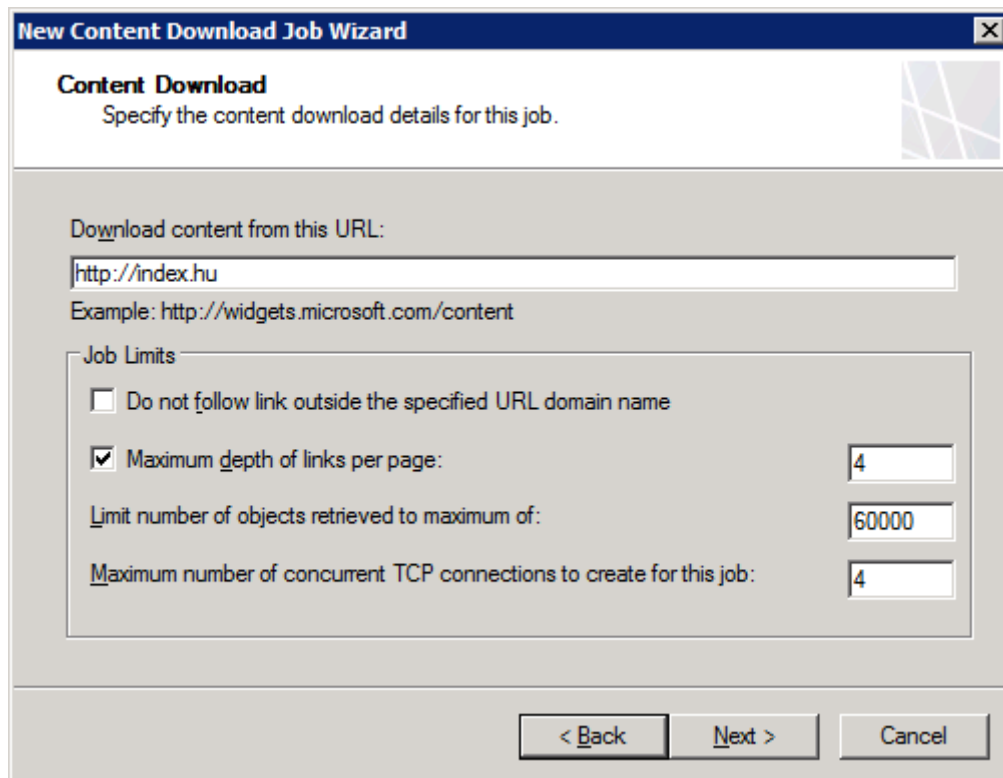


7.29 ÁBRA AZ FTP-NÉL KEVESEBB OPCIÓ VAN

A következő beállítás valószínűleg segít abban, hogy megértsük az iménti HTTP-re vonatkozó tiltást értelmét, ti. itt külön választhatjuk az FTP forgalom gyorsítótárazását, és a HTTP-től független szabályt is legyárthatunk az FTP-re, külön TTL-lel.

Gyakorlatilag készen is vagyunk, ezután már csak az összegző képernyő jön, majd az érvényesítés, illetve az adott szabályunk igény szerinti sorrendbe állítása.

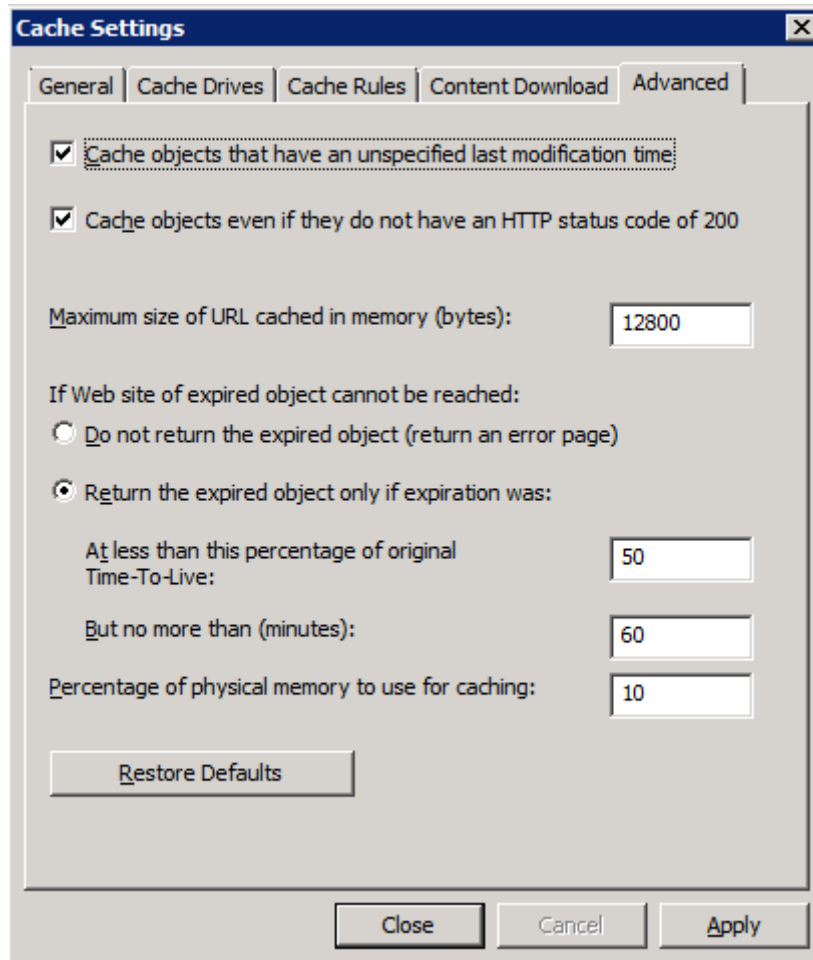
Térjünk vissza a fő ablakba, ahol a negyedik fül az időzített letöltések (Content Download Job) szintén érdekes területére vezetnek el bennünket. Egy-egy feladat varázslásából csak egy képet mutatok meg, ahol a letöltendő oldal címét, a letöltés adott webszerveren belüli "mélységét", illetve az objektumok és a letöltéshez használt párhuzamos TCP kapcsolatok korlátait állíthatjuk be.



7.30 ÁBRA AKÁR MINDEN REGGEL 8.55-KOR LETÖLTHETJÜK

Már csak egyetlen fül maradt (Advanced), de ez ismét globális jelentőséggel bír, és néhány nagyon fontos beállítás is helyet kapott itt.

- *Cache objects that have an unspecified last modification time:* Mi legyen azokkal az oldalakkal, ahol nincs beépítve a fejlécbe TTL érték? Ha bepipáljuk, akkor az cache szabályokban szereplő TTL opciók lesznek érvényesek az ilyen oldalakra.
- *Cache objects even if they do not have an HTTP status code of 200:* Az ún. negatív gyorsítótárazás engedélyezése. Ugyanúgy mint a DNS-nél itt is van lehetőség arra, hogy a különböző okokból hibás oldalak (HTTP 203, 300, 301, 410 státuszkódok) eredménye el legyen tárolva. Így időt takaríthatunk meg, mert csak a TTL lejártakor vizsgálja meg a TMG, hogy él-e a korábban nem működőnek jelölt oldal.
- *Maximum size of URL cached in memory (bytes):* Az URL-ek maximális száma, amelyet eltárolhat a TMG a memóriában.
- *If Web site of expired object cannot be reached: Do not return the expired object (return an error page):* Mi legyen akkor, ha a kérés egy oldalra vonatkozik, amit már letároltunk, de közben már lejárt az érvényessége, viszont online elérhetetlennek bizonyult? Az első opció azt mondja, hogy szó sem lehet róla, legyen egy hibaüzenet, a maradék kettő viszont engedélyezi, de tovább finomítja a dolgot azzal, hogy feltételekhez köti a tárolt verzió bemutatását.



7.31 ÁBRA JÓPÁR NAGYON FONTOS BEÁLLÍTÁS

- *Percentage of physical memory to use for caching:* A gyorsítótárazásra felhasználható RAM mennyiségét szabályozhatjuk itt. Csak érdekességképpen, az ISA 2000-ben, a RAM-ban lefoglalt cache mennyisége alapértelmezés szerint 50% volt. Ez durván befolyásolhatta a gép teljesítményét, és ha ezt nem tudtuk, akkor sokáig kereshettük a rejtélyesnek tűnő okot. Aztán ez változott, a következő verziókban és így a TMG-ben is ez az érték már csak 10%. Ha nagyon kevés a RAM-unk, akkor korlátozzuk le a belső webszerverünk méretére, és akkor legalább ennyit le tud majd tárolni a memóriában a TMG.

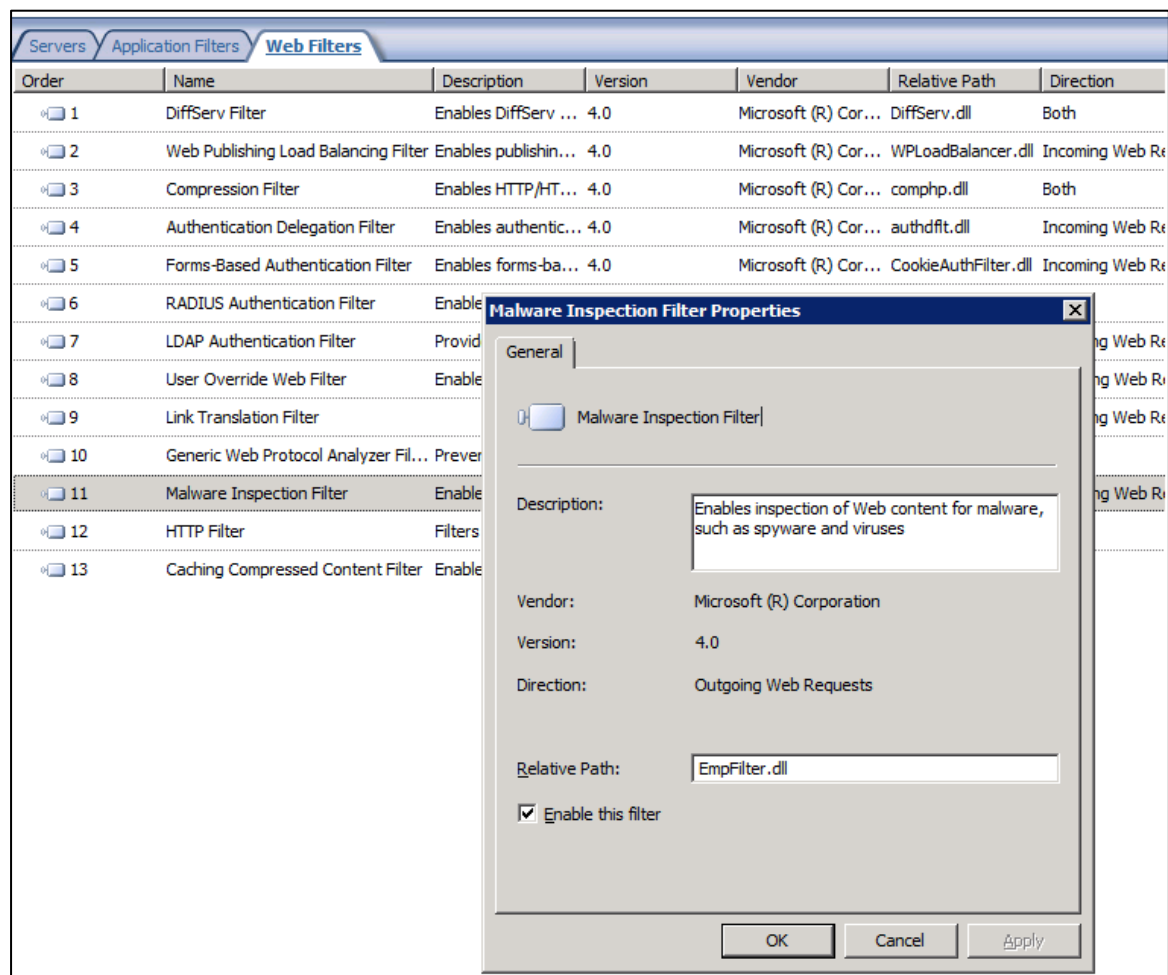
Ezzel a gyorsítótár fejezetnek és egyben a proxy szerver általános ismertetésének vége szakad, de most következik a TMG újdonságainak egy jelentős része, úgyhogy azért ne csüggedjünk.

8 A WEB PROXY A TMG-BEN

Ebben a fejezetben a TMG a web proxy filterhez kapcsolódó újdonságait vesszük számba, azaz a HTTP/S forgalom ellenőrzésével és szűrésével foglalkozunk. Egyetlen kivétel lesz, a HTTP filter, amely már ugyan az ISA 2004 óta velünk van, de kicsit kevesen ismerik és kevesen is használják ki az előnyeit, én viszont úgy éreztem, hogy szorosan kötődik az újdonságokhoz, ergo egy ilyen integrált tartalmú könyvben ennyi kivételezés bőven belefér.

8.1 ENTERPRISE MALWARE PROTECTION

Tömören összefoglalva a TMG⁶⁹ ezen új megoldása a HTTP folyamat figyeli és szűri, méghozzá az integrált és frissíthető adatbázisa segítségével.



8.1 ÁBRA A MIF A WEB FILTEREK KÖZÖTT

⁶⁹ Kivételesen ez a megoldás a TMG MBE változatában is megtalálható, persze némiképp csökkentett lehetőségekkel.

(<http://www.microsoft.com/hun/technet/article/?id=30d3d111-4cb9-4f82-b9f7-d8167624ecfb>).

A TMG illetve a szintén új Malware Inspection Filter (MIF) képes detektálni és izolálni a veszélyes forgalmat (malware = spyware-ek + vírusok), így már a határvédelem részévé tenni az Internet felől érkező kártevők semlegesítését.

Mindezt csak akkor teszi meg a TMG, ha az adott forgalomra vonatkozó szabályban be van kapcsolva ez a vizsgálattípus, merthogy ez egyrészt globálisan, másrészt szabályonként is ki- vagy bekapcsolható illetve forrás és cél alapján is szabályozható. A vizsgálat több részből áll, a folyamat legelején a mi kliensünktől induló kérés is már szűrésre kerülhet, majd az engedélyezés után a visszatérő forgalomba is képes beavatkozni a TMG proxy szervere, azaz ellenőrzi, pontosabban ellenőrzésre küldi az adott választ.

8.1.1 HOGYAN CSINÁLJA?

A működésről szólva, az előző ábrán is látható MIF szűrő az ami átnézi a proxy által megjelölt http kérés törzsét (body). A 64K-nál kisebb anyagok⁷⁰ ellenőrzése a memóriában történik meg, azaz a MIF villámgyorsan meggyötri az anyagot, rendbe rakja a letöltés időzítését, majd visszaadja a proxynak, és ha nincs gond, akkor mehet minden tovább a felhasználó felé. Ha viszont nincs rendben a tartalom, akkor a TMG megpróbálja megtisztítani (a mechanizmus alapja a Forefront Client Security / Windows Defender / MSE által is használt MPE, azaz Microsoft Malware Protection Engine), ha tudja, remek, ha nem akkor erről a felhasználó egy HTML oldal formájában kap egy értesítést, amiből az is kiderül, hogy sajnos (illetve nem is sajnos) ez a forgalom blokkolásra került. No és persze a fertőzött tartalom azonnal eltűnik minden háttértárolóról és a memóriából is.

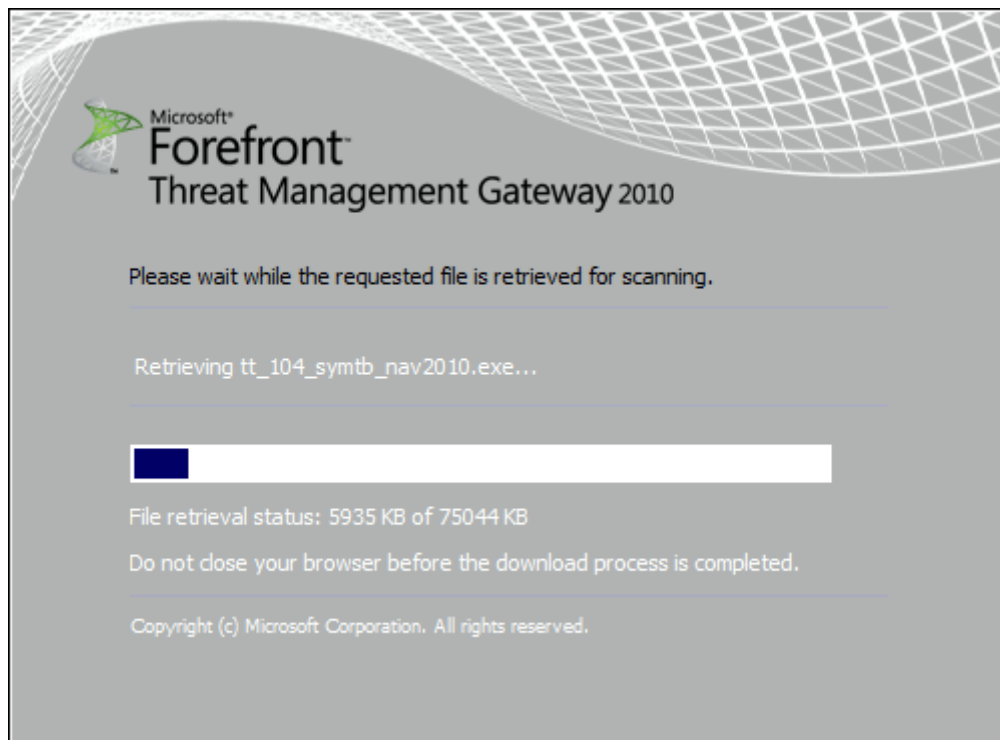
Természetesen a TMG arról is gondoskodik, hogy az AV motor és a szignatúra mindig friss legyen. Ezeket közvetlen frissíthetjük a Microsoft Update szerverekről, vagy egy saját WSUS-ról – értelemszerűen teljesen automatikusan és bármilyen leállás, kiesés nélkül.

Az persze hogy egy komplett AV alrendszer működik a TMG-ben még nem azt jelenti, hogy a belső hálózaton, vagy éppen a mobil gépeinken nincs szükség a klasszikus vírus/spyware irtókra. Természetesen van, ha másért nem akkor a fájlrendszerek, a fix és a leválasztható háttértárak kontrollja meg kell hogy maradjon a TMG bevezetése után is, nem beszélve arról, hogy a Malware

⁷⁰ A statisztikák szerint a szimpla http letöltések, kérések 98%-a kisebb mint 64K, ergo így a szűréshez a legtöbb esetben nem is kell semmilyen klasszikus I/O művelet.

Protection nem képes igény szerinti víruskeresésre, hanem "csak" a valósidejű, a web proxyn átmenő forgalom vizsgálatára.

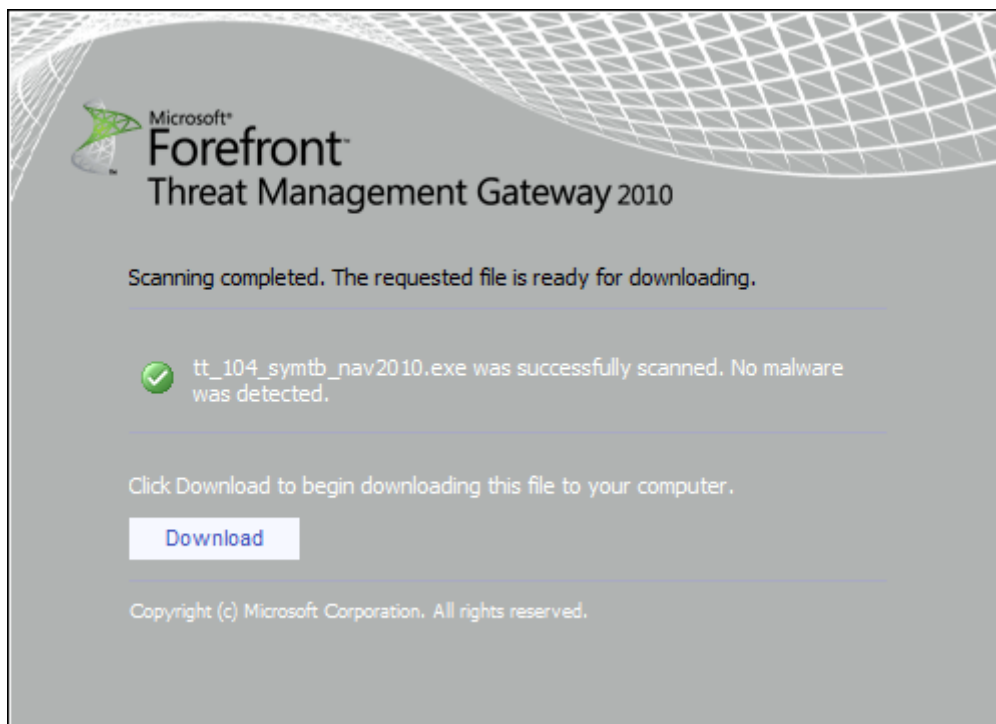
A működés megértéséhez hozzátartozik az is, hogy a felhasználó a TMG mögött mit lát ebből a szokásos internet használat közben. A TMG észrevétlenül vizsgálódik mindaddig, amíg egy-egy objektum letöltése 10 másodpercen belül megtörténik. Ha a TMG azt észleli, hogy az aktuális letöltés tovább tart majd mint ez az időkeret, akkor a felhasználó egy ún. progress bar-t kap majd a fájl helyett.



8.2 ÁBRA MOST VIZSGÁLÓDIK A TMG (A FELHASZNÁLÓ BÖNGÉSZŐJÉBEN EZ LÁTSZIK KÖZBEN)

Ez ugye az a "csík", ami "megy előre" :), pl. egy fájl másolásnál, vagy éppen a letöltésnél, vagy éppen most majd a felhasználó böngészőjében (8.2 ábra). Ezt tilthatjuk, illetve szintén a tartalomtípus alapján behatárolhatjuk⁷¹, hogy látható legyen-e, vagy sem. Ez az egész folyamat a letöltés kezdetétől a végéig az ún. trickling (szivárogtatás, csepegtetés), amelyről még lesz szó később a konfigurálás közben.

⁷¹ Értelemszerűen egy Youtube videó közben ez nem uralhatja a képernyőt.



8.3 ÁBRA EZ RENDBEN VAN ÉS MOST MÁR LETÖLTHETŐ



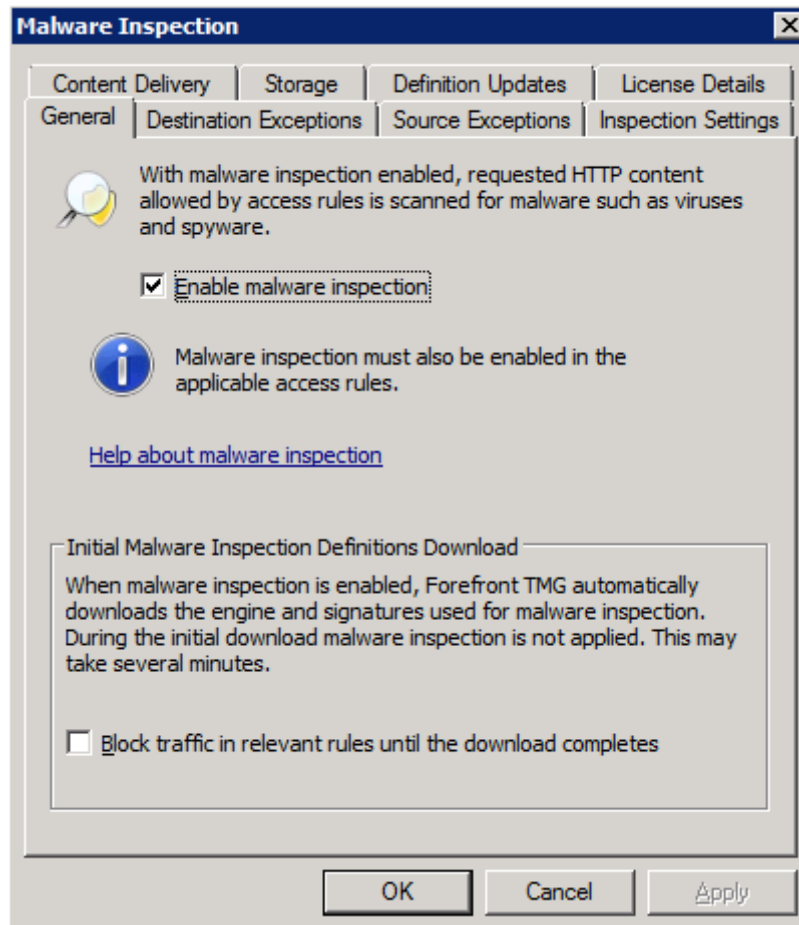
8.4 ÁBRA ITT VISZONT BIBI VAN⁷²

8.1.2 AZ EMP KONFIGURÁLÁSA

Egy kicsit már belemártottuk magunkat ebbe a témakörbe, hiszen a Web Access Policy varázsló futtatásakor már találkozhattunk az EMP-vel. Ha ott és akkor engedélyeztük,

⁷² De nyugalom ez csak teszt (<http://www.eicar.org/download/eicar.com>)

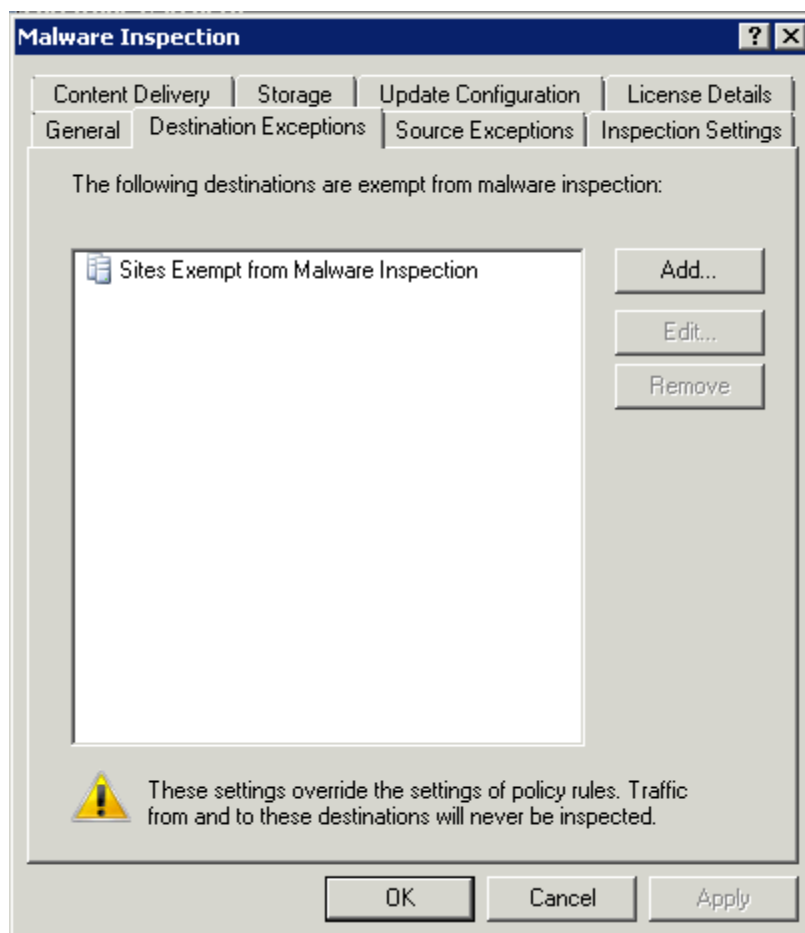
vagy esetleg letiltottuk, akkor az egy globális műveletnek minősült és minden szabályunkra egyformán vonatkozott. Úgyhogy most nézzük meg először ezeket a globális beállításokat.



8.5 ÁBRA ITT KEZDŐDIK MINDEN

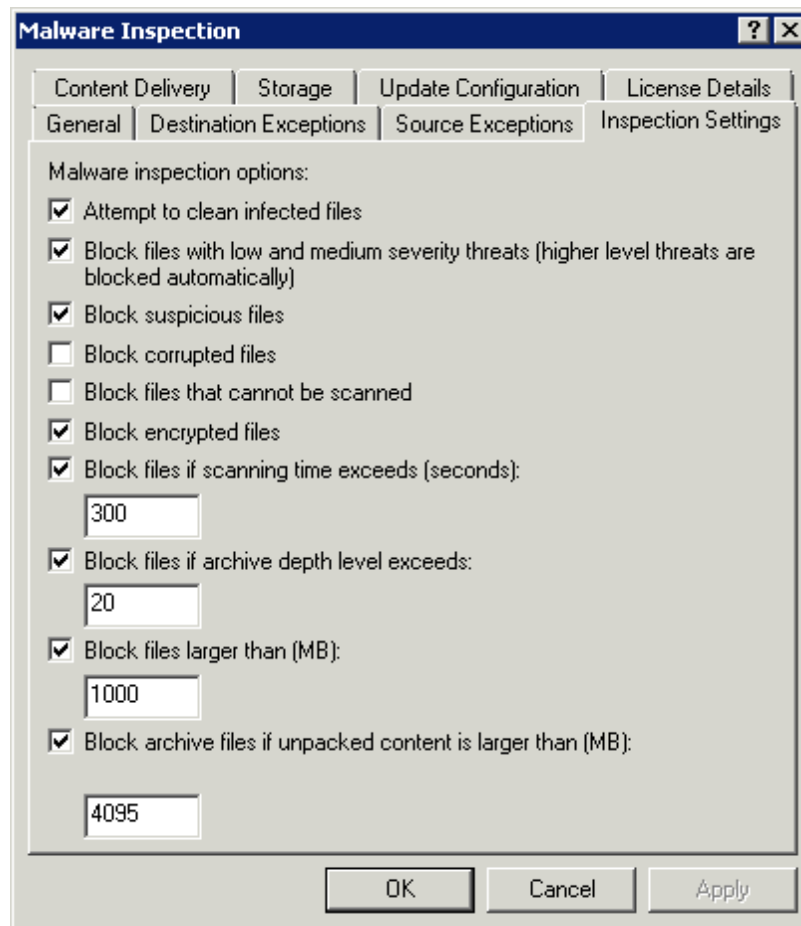
A globális engedélyezést/tiltást a faszervezet Web Access Policy pontja alatt, a már ismert fejléc részben a Malware Inspection linkre kattintva érjük el. Ami ezen a panelen lentebb van, az is érdekes, ugyanis biztonsági okból letilthatjuk az egész forgalmat a legeslegelső sikeres EMP frissítés befejezése előtt.

A következő két fül a kivételekről szól, akár cél, akár forrás alapján kivonhatunk bizonyos hálózatokat, gépcsoportokat, URL gyűjteményeket, stb. az EMP hatása alól. A Destination Exception fül alatt azonnal találunk is egy gyári kivételt (Sites Exempt from Malware Inspection), amelybe a NIS-nél vagy a System Policy-nál már megismert *.microsoft.com oldalakat találjuk. A forrás rész (Source Exceptions) alapértelmezés szerint üres, azonban itt vehetjük fel pl. egy IP tartomány alapján azokat a belső gépeket, amelyeket ki akarunk venni az EMP hatása alól.



8.6 ÁBRA VANNAK/LEHETNEK KIVÉTELEK

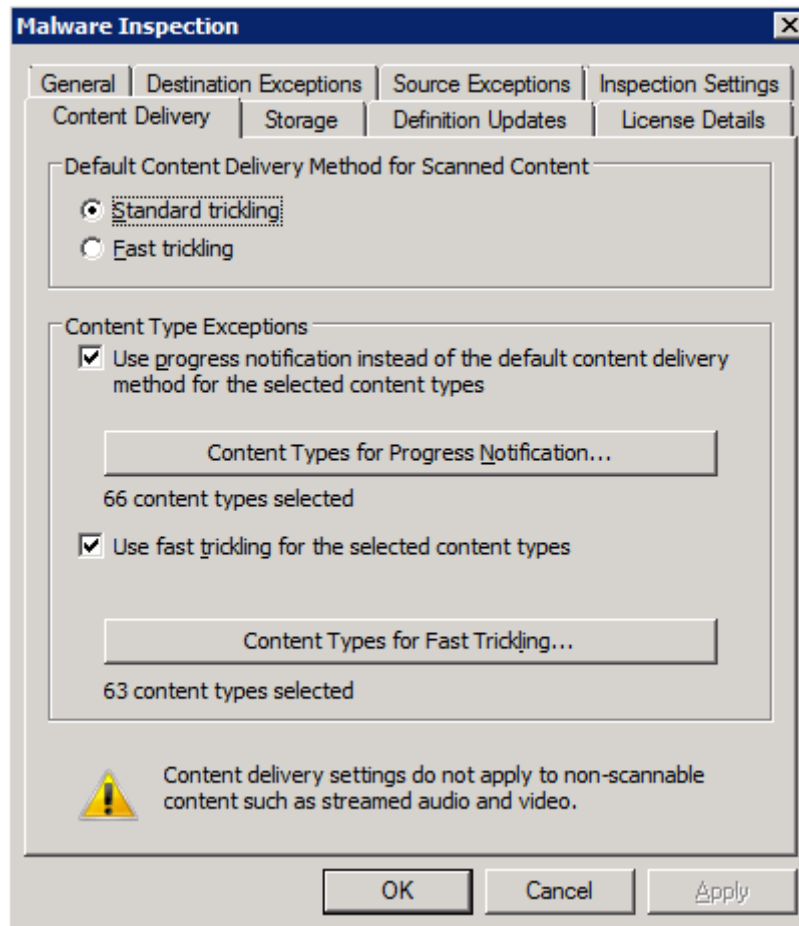
Ami viszont most jön az a lényeg, azaz milyen feltételek mellett szűrjön az EMP. A malware vizsgálat és keresés mellett ezen a helyen ugyanis egy jó nagy csokor más restriktiót is beiktathatunk.



8.7 ÁBRA ITT MINDEN VAN, AMI SZEM-SZÁJNAK INGERE

- **Attempt To Clean Infected Files:** Itt kapcsoljuk be azt, hogy egy malware esetén legyen-e kísérlet az irtásra. Ha bekattintjuk két eset lehetsége: 1; a TMG sikeresen elvégzi a tisztítást, 2; Ha nem akkor blokkolja a hozzáférést az oldalhoz és értesíti a felhasználót.
- **Block Files With Low And Medium Severity Threats (Higher Level Threats Are Blocked Automatically):** Alapértelmezés szerint az EMP gyári érzékenysége csak a legmagasabb szintű incidensek blokkolására van belőve, itt ezt az érzékenységet lényegesen komolyabbra is vehetjük.
- **Block Suspicious Files:** Az EMP kategorizálja a fájlokat az ellenőrzés során, és amelyeket fertőzöttnek ítél, azokat blokkolja is, de azokat is megjelöli, amelyekben nem képes azonosítani egy ismert vírust, de azért felettébb gyanúsak. Ha szeretnénk, akkor ezek a gyanús fájlok is blokkolásra kerülhetnek.
- **Block Corrupted Files:** Ha egy fájl sérültnek tűnik, az is lehet gyanús, és ha úgy gondoljuk, akár blokkolhatjuk is. De a nem teljes fájlokat, azaz „fragmented” fájlokat is ideértjük érte (például egy több szeletes .rar-t. Hogy kiderüljön, hogy tartalmaz-e kártékony kódot, kellene az egész fájl. Bár a .rar fájl önmagában egy egész, de ami benne van az egy zagyvaság. Ha bekapcsoljuk ezt az opciót akkor minden fragmented tartalmat kidobunk.

- **Block Files That Cannot Be Scanned:** Lehetséges olyan helyzet is, amikor a TMG nem tudja ellenőrizni a fájlokat. Így aztán kérhetjük azt, hogy ilyenkor is viselkedjen úgy a TMG, mint egy malware esetén. Viszont mivel ekkor lehet egy halom téves blokkolás, ezért alapértelmezés szerint ez nincs engedélyezve.
- **Block Encrypted Files:** A titkosított fájlok (pl. EFS) blokkolása érhető el ezzel, mivel a TMG ezeket sem tudja megvizsgálni, alapértelmezés szerint is blokkolja.
- **Block Files If Scanning Time Exceeds (Seconds):** A türelmetlen felhasználók ☺ (de igazából a korlátozott számú thread-ek, és így a problémás teljesítmény) miatt létezik és konfigurálható egy alapértelmezett vizsgálati idő is, amely letelte után a TMG nem húzza tovább az időt, hanem szintén blokkol.
- **Block Files If Archive Depth Level Exceeds:** Ugye mi is ismerjük a sokszorososan, azaz újra és újra tömörített fájlokat? Nos, ezek használatának véget vehetünk ezzel a beállítással. Szerintem az alapértelmezett 20 kissé elnéző, de szerencsére ezt mindenki önállóan dönti majd el. Alapvetően azért kerül bele kivétel nélkül minden víruskeresőbe ez az opció, hogy legyen egy fékrendszer. Ugyanis, ha nincs fék, akkor egyszerűen DoS támadást lehet indítani így a szolgáltatás ellen, egy ezerszeresen egymásba ágyazott tömörített fájlal.
- **Block Files Larger Than (MB):** A letölthető fájlok méret szerinti korlátozása is egy lehetőség, alapértelmezés szerint 1 GB-nál húzza meg a határt az EMP, ami szintén elsősorban teljesítmény okokkal magyarázható.
- **Block Archive Files If Unpacked Content Is Larger Than (MB):** Mivel a TMG úgyis kibontja majd a tömörített fájlokat az ellenőrzés alkalmával, van arra is lehetőségünk, hogy ezeknél is szabjunk mérethatárt. Teljesítmény szempontból megfontolandó, hogy ne engedjünk ily módon óriási fájlokat is letölteni.



8.8 ÁBRA HOGYAN CSURGASSUNK?

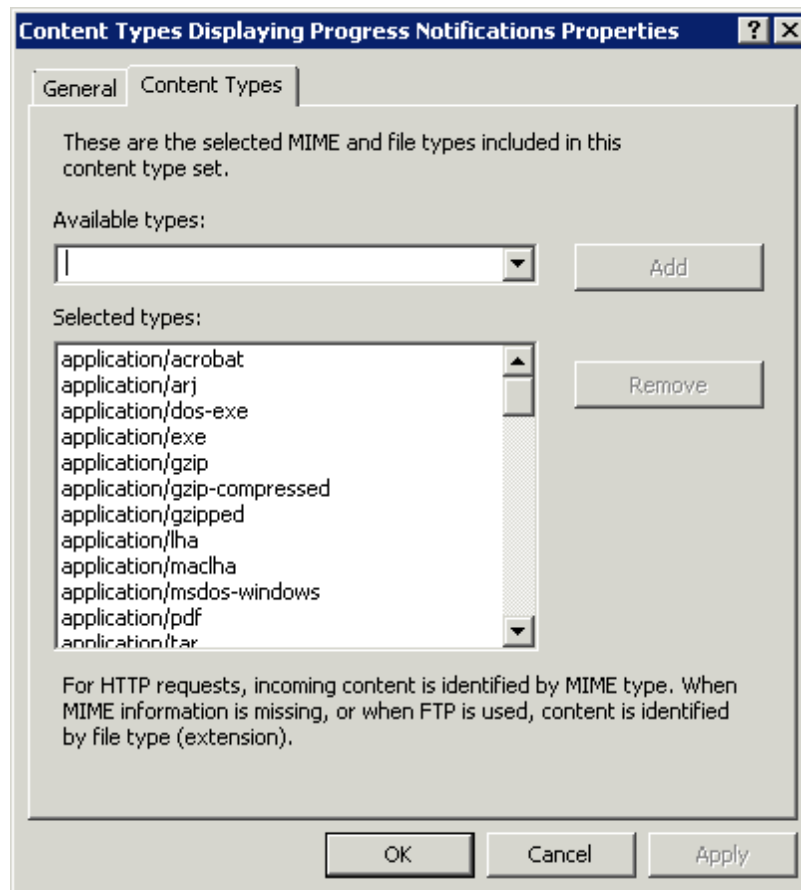
Ha ezután az opcióorgia után továbblépünk a második "fülsorba", akkor először a már említett trickling-gel kapcsolatos beállításokat (Content Delivery) láthatjuk.

Két lehetőségünk van a Standard és a Fast trickling, de némiképp variálhatjuk is ezeket.

Ahhoz, hogy megértsük miért is merült fel ez a kérdés egyáltalán, előbb gondoljuk végig a következő kérdést: *mikor tudjuk megállapítani egy fájlról azt, hogy az kártékony kód?* A válasz egyszerű: akkor ha a teljes fájl a birtokomban van. Ez egy fájlrendszerben implementált víruskeresés esetén nem akkora kihívás, mint egy átmenő forgalom esetén, mint amilyen például egy letöltési forgalom. Ugyanis ha kellően nagy a fájl amit szeretne a felhasználó letölteni és/vagy a hálózat képessége sem határtalan, akkor lesz olyan időszelhet amikor a proxy-n még csak a fájl töredéke van meg.

A kérdés az valójában, hogy mit adjunk a felhasználó alkalmazásának vissza addig, amíg nem tudtuk ellenőrizni a letöltendő fájlt. Ha 1 órán keresztül tart a letöltés, akkor a TMG biztosan csak a 60. percben tudja ellenőrizni a fájlt. 60 percig azonban egyetlen alkalmazás sem fogja kibírni, de a felhasználó sem. Nos ennek a problémának a kezelésére van az alábbi két megoldás:

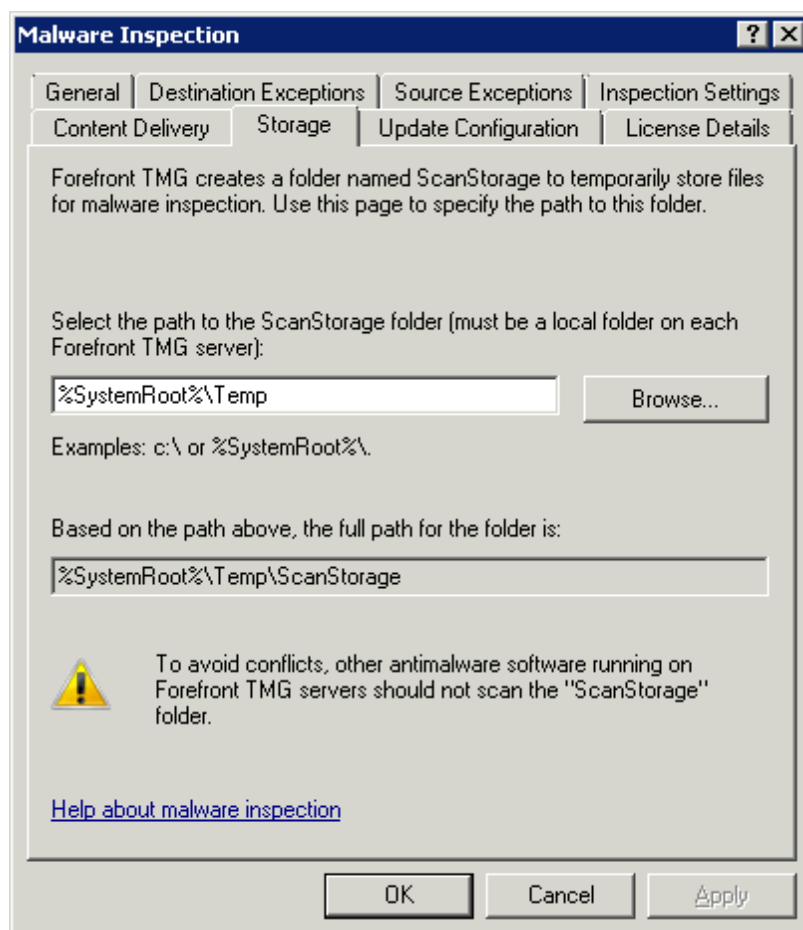
- Standard: ebben az esetben a TMG letölti a kért fájl egy kis darabját (néhány kb), és ezt ellenőrzi. Ha nem tartalmaz kártékony kódot, akkor ezt elküldi a felhasználó alkalmazásának folyamatosan, addig amíg a tartalmat biztosító célkiszolgálótól nem érkezik meg a teljes fájl. Ha megérkezik a teljes fájl, akkor ezt ellenőrzi. Ha nem tartalmaz kártékony kódot, akkor a teljes tartalmat átadja a felhasználó alkalmazásának. Ha tartalmaz, akkor egy RST csomaggal lezárja a kapcsolatot és a felhasználónál a letöltés megszakad.
 - o A Standard csepegtetés két legfontosabb jellemzője az, hogy a TMG teljesítményét negatívan nem befolyásolja, illetve a felhasználói élményt alaposan rontja. Ugyanis a teljes letöltési idő jelentős részében a felhasználó azt látja, hogy csak „vánszorognak” a bitek, ugyanis folyamatosan kis apró darabokat kap az alkalmazása. Ez egy IE esetében jelentheti azt is, hogy a felhasználó kb. 340 byte/sec-es letöltési sebességet lát. Aztán a folyamat végén minden felgyorsul és megkapja hirtelen a teljes fájlt. és ez nos, problémás lehet a felhasználók felé. Éppen ezért a Standard módszernél is ki van jelölve 63 fájltypus (Content Types for Fast Trickling), amikor a Fast módszert használja a TMG, automatikusan. Ide kerültek be pl. az audio/video és streaming fájltypusok.
- Fast: ez a kifejezés kissé becsapós. Azt várjuk, hogy ez egyértelműen a jobb és a gyorsabb. Azonban ha megértjük hogyan működik, meglátjuk hogy nem biztos, hogy (a TMG szempontjából pedig biztosan nem) ez a jobb megoldás. A Fast „csepegtetés” típus esetében a TMG letölti a fájl egy részét, azt ellenőrzi és átadja a felhasználónak. Majd letölti a fájl egy második szeletét és ellenőrzi azt. A kérdés az, hogy mit ellenőriz. Csak a második szeletet? Vagy az első és a második szeletet? A helyes válasz az, hogy az első és a második szeletet. És ez így folytatódik addig amíg a teljes fájl nem érkezik meg. Ha a folyamatban bármikor kártékony kódot talál a szűrő, akkor megszakítja a letöltést. Összehasonlítva a Standard csepegtetési módszerrel, itt a teljes fájl letöltési ideje alatt használjuk a szűrőt és minden fájl részletet indokolatlanul sokszor ellenőrzünk. Cserébe a felhasználó a fájl valós tartalmát és valós sebességgel kapja meg, azonban ennek a módszernek lényegesen nagyobb a CPU igénye.



8.9 ÁBRA MIKOR LEGYEN CSÍK?

Ugyanitt szabályozzuk azt is, hogy mikor legyen csík, azaz a "Progress bar" (Content Types for Progress Notification). Ez a forgalomban résztvevő fájlok típusától függ és alapértelmezés szerint 66 típus van erre kijelölve, de akár ezt, a listát, akár a következőt, teljesen szabadon variálhatjuk, a saját elképzelésünk alapján.

Még nincs vége az EMP opcióknak, most jön az, hogy hol legyen az átmeneti tároló (ha nem a RAM-ban történik a tárolás, hanem a merevlemezeken). Ez alapesetben a %systemroot%\temp\ScanStorage mappá, ami nekem kicsit vakmerőnek tűnik, de hát ilyen a paranoia.

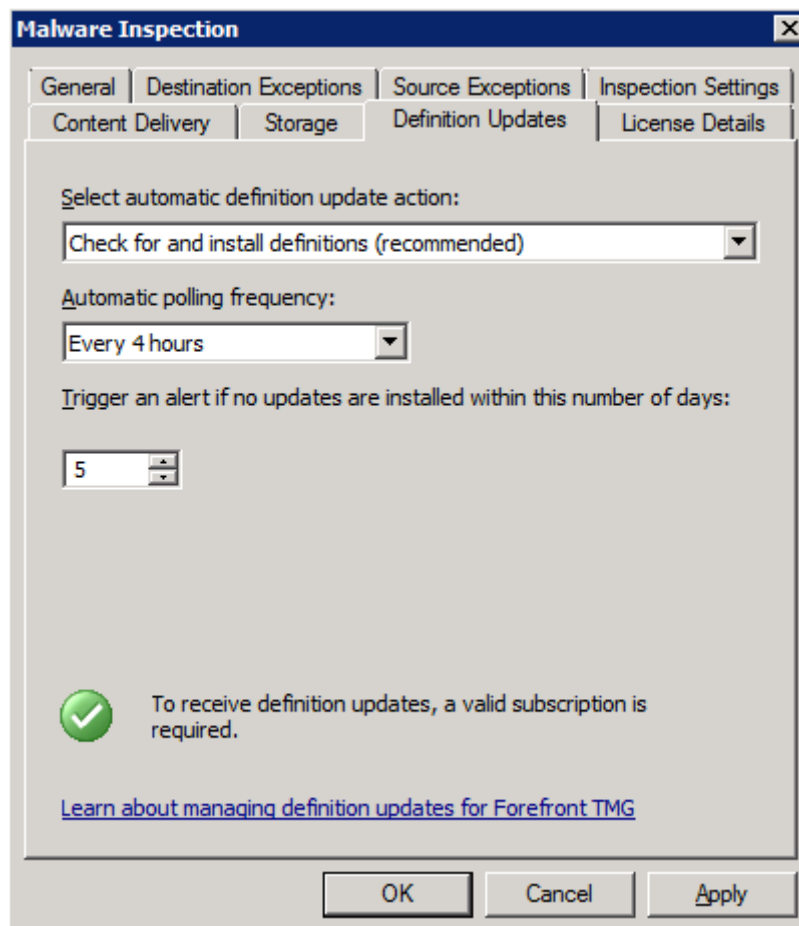


8.10 ÁBRA MIKOR LEGYEN CSÍK?

Mindenesetre, ha netalántán van egy klasszikus AV szoftverünk is a TMG-n (mert lehetséges, de feltétlenül tartsuk be az ajánlásokat⁷³), akkor ennek a mappának mindenképpen benne kell lennie az ellenőrzési kivételekben. Ezen mappa gyári, NTFS jogosultsági beállításával se játszunk, ha lehetséges.

A következő fül a frissítéssel kapcsolatos beállításokat tárolja. Legyen-e ellenőrzés és telepítés, vagy csak ellenőrzés, vagy semmilyen akcióra nincs szükség? Valamint 15 perctől 4 óráig tartó intervallumban állíthatjuk be a frissítések ellenőrzési ciklusát.

⁷³ <http://technet.microsoft.com/en-us/library/cc707727.aspx>

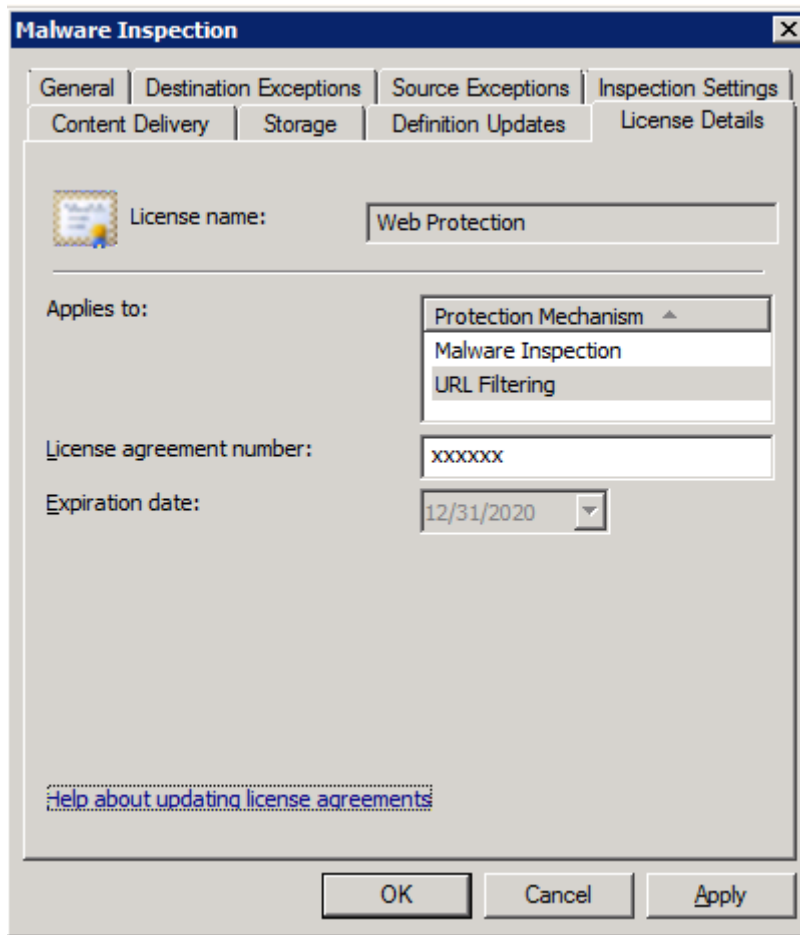


8.11 ÁBRA A FRISSÍTÉSEKRŐL MINDEN

Ami még itt érdekes (és pl. a bétához képest egy újdonság volt), az a szintén beállítható riasztási korlát, azaz ha pl. az alapértelmezés szerint 5 napig nem volt frissítés, akkor a TMG generál egy riasztást.

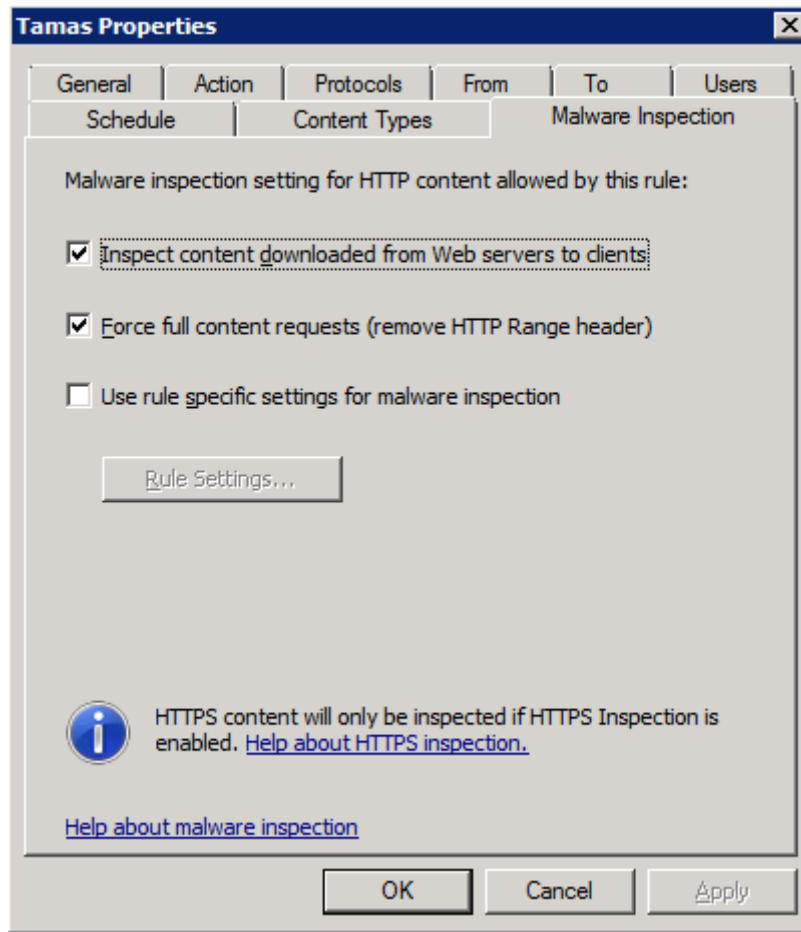
Arról, hogy hogyan állnak a különböző adatbázis frissítések, azaz pl. a Malware Inspection-é, a TMG-n belül, a faszervezetben az Update Centerben találunk infót, illetve itt kezdeményezhetjük az ellenőrzést, és magát az adatbázis frissítést is, manuálisan.

Az viszont, hogy a frissítésre jogosultak vagyunk-e, az az utolsó fülön, a License Details alatt derül majd ki. A TMG telepítése után kapunk egy 120 napos, ingyenes lehetőséget, de ezután vagy marad ez az állapot azaz működik az EMP, csak nem frissül, vagy meg kell vennünk és be kell táplálnunk a rendszerbe a frissítésre jogosító kódot. Ezt egyébként első alkalommal nem itt, hanem Web Access Policy varázsló futtatása közben leszünk csak képesek megtenni, akkor is ha éppen most telepítettük a TMG-t, és akkor is ha a 120 napos trial időszak után/közben akarjuk a licenst érvényesíteni.



8.12 ÁBRA A LICENSZ ADATOK (A LEJÁRAT AZÉRT SZÜRKE, MERT KISZEDTEM A HELYES KÓDOT)

A konfigurálásból már csak egyetlen dolog maradt ki, a nem globális szabályzás, azaz a tűzfal szabályokban elérhető EMP lehetőségek. Ehhez nézzünk be pl. a Firewall Policy szakaszba, válasszunk ki egy megfelelő, a HTTP protokollt tartalmazó szabályt (vagy ha a Web Access Policy részbe megyünk még gondolkodnunk sem kell ezen).



8.13 ÁBRA SZABÁLYONKÉNT MÁS ÉS MÁIS IS LEHET

- **Inspect Content Downloaded:** Bekapcsoljuk vagy nem? Nyilván csak akkor, ha globálisan is be van kapcsolva az EMP. Erre egy diszkrét sárga háromszög + fekete felkiáltójel kombinációval figyelmeztet is a TMG.
- **Force full content requests (remove HTTP Range header):** A vizsgálat apropóján a teljes tartalom elkérésére utasítjuk ezzel a tűzfal motort.
- **Use rule specific settings for malware inspection:** Ha ezt kérjük, kaphatunk egy ugyanolyan beállító panelt, mint amelyet a 8.7-es ábrán láthatunk. Azaz teljesen testreszabhatjuk az adott szabálynál ezeket a jellemzőket is.

Egy dologra még figyelmeztet bennünket a TMG itt, mégpedig arra, hogy csak akkor lesz HTTPS vizsgálat is, ha ezt engedélyezzük, nos ez egyrészt logikusan hangzik, másrészt egy tökéletes átvezetés a következő fejezetekbe.

8.2 A HTTP FILTER

Az 5.1.3 fejezetben már szoltunk az alkalmazás szűrésről, sőt az integrált HTTP filterről is. Most itt egy kicsit jobban kibontjuk majd, mivel a HTTP a domináns protokoll jelenleg az internetes forgalom összességét tekintve, és hát (hasonlóan a POP3-hoz,

vagy az SMTP-hez, meg a többi klasszikus protokollhoz) amikor “elkészült”, akkor senki nem gondolta volna, hogy az internet olyan veszélyeket hordoz majd magában, mint amelyet most. Tegyük egymás mellé három, statisztikákkal bizonyított tény:

1. Az átlagos forgalom megoszlása a következő: HTTP: 80%; SIP: 8%; FTP: 5%; DNS: 5%; SMTP: 2% (forrás: Microsoft)
2. A sikeres betörések 75%-a ezekben a protokollokban jön össze (forrás: Gartner).
3. A sebezhetőségek 92%-a szintén itt fordul elő (forrás: NIST).

Ráadásul a HTTP használat tendenciája egy ideje még egyértelműbb. Ennek okai között szerepel az, hogy egyrészt a klasszikus szoftverek közül is egyre több képes a 80-as vagy a 443-as porton működni (gondoljunk az üzenő- és kommunikációs alkalmazásokra), másrészt egy olyan irányvonal is megfigyelhető, amely arról szól, hogy amit csak lehet tuszkoljunk bele a HTTP-be illetve HTTPS-be. Outlook Anywhere (lánykori nevén RPC over HTTPS), RDP over HTTPS (Remote Desktop Services Gateway), SSTP (Single Socket Tunneling Protocol, azaz egy SSL VPN típus, ami a Vista SP1 óta érhető el) de még az IPv4 is (IPHTTPS). Ezek mind, tűzfalbarát módon, konkrétan a 443-as porton érhetőek tetten, ami jó nekünk, hiszen egy idegen hálózatban (szállodák, partnerek, stb.) is biztosak lehetünk abban, hogy működni fognak, másrészt plusz problémákat okoznak, hiszen egyszerűen nem tilthatjuk le a HTTP-t vagy a HTTPS-t a forgalom blokkolása miatt (pedig a malware-ek miatt ezt kellene tennünk), hiszen univerzálisan kell, hogy ezeket használják a felhasználók, ráadásul többnyire alig látunk bele ezekbe az adatfolyamokba, főképp ha SSL-el támogatottak.

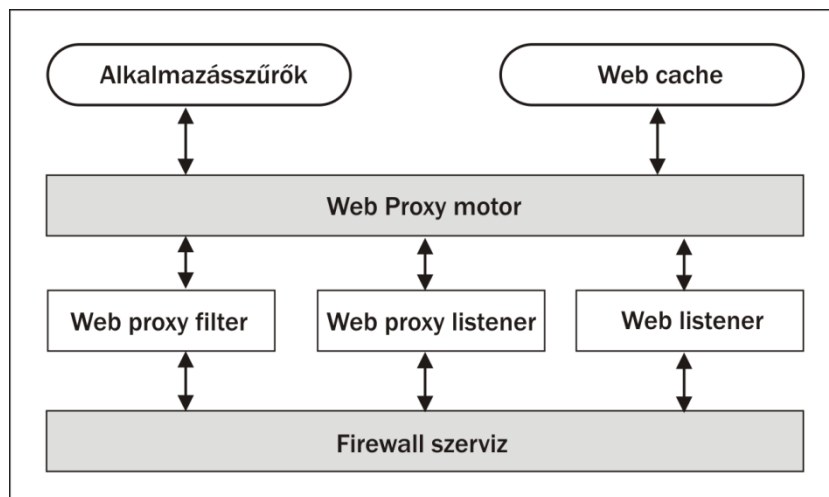
Bizonyára feltűnt, hogy konzekvensen és folyamatosan a HTTPS-ről is beszélek. A következő fejezetben majd látni fogjuk, hogy miért, egyelőre csak annyit, hogy ha szeretnénk, akkor pl. a HTTP filter, vagy akár a Malware Filter szempontjából a TMG-ben teljesen mindegy, hogy HTTP vagy HTTPS a forgalom, képesek leszünk egyenértékűen szűrni.

8.2.1 HOGYAN ÉRJÜK EL?

És most a már ismert recept szerint beszéljünk egy kicsit a működésről. Az előzmény apropóján először menjünk vissza a web proxy motorhoz, amelyhez többféle módon is érkezhetnek a kérések, egész pontosan háromféle módon:

1. **A web proxy filteren keresztül:** Ahogyan ez már kiderült az előző nagy fejezetből, ez egy komplex alkalmazás szűrő, amely fő feladata a HTTP/S forgalom bonyolítása, ezt a tömörítéssel, a hitelesítéssel és a gyorsítótárazással is támogatja (úgy hogy ezekhez a különböző webes szűrőket használja). Egyben

a web proxy filter az egyik belépési pontja a web proxy motornak is, azaz pl. ha az adott tűzfalszabályban a HTTP/S-hez a web proxy filter hozzá van rendelve, akkor ez lekezeli a bejövő kérést, és továbbküldi a web proxy motornak. Ennek a filternek nincs köze a web proxy kliensekhez (amelyek attól válnak azzá, hogy beírjuk a proxy címét és portját, pl. egy böngészőben), hanem az SNAT és a tűzfal kliensek kapcsolódnak hozzá.



8.14 ÁBRA ÉS EZ MIND USER MÓDBAN VAN

2. Az előző pontban zárójelben említett web proxy kliensek viszont egy másik irányból kommunikálnak, még hozzá a **web proxy listener**-ekkel (pl. a 8080-as alapértelmezett porton), amelyeket egy-egy hálózat tulajdonságainál engedélyezhetünk (vagy nem). Egy ilyen listener teljes forgalmát szintén a web proxy motor kapja meg, és így a web proxy kliensek az alkalmazásszűrők képességeit ugyanúgy ki tudják használni.
3. A harmadik eset a **web listener**-eké, amelyek a publikáló tűzfalszabályokban használatosak (ez ugye a bejövő forgalom a szervereink felé), kötelező jelleggel. Ekkor a kérés útja szintén a Firewall szervíznél kezdődik, és a web listener-eren keresztül a web proxy motorhoz vezet, és ugyanúgy az alkalmazásszűrők hatása is érvényesül rajtuk.

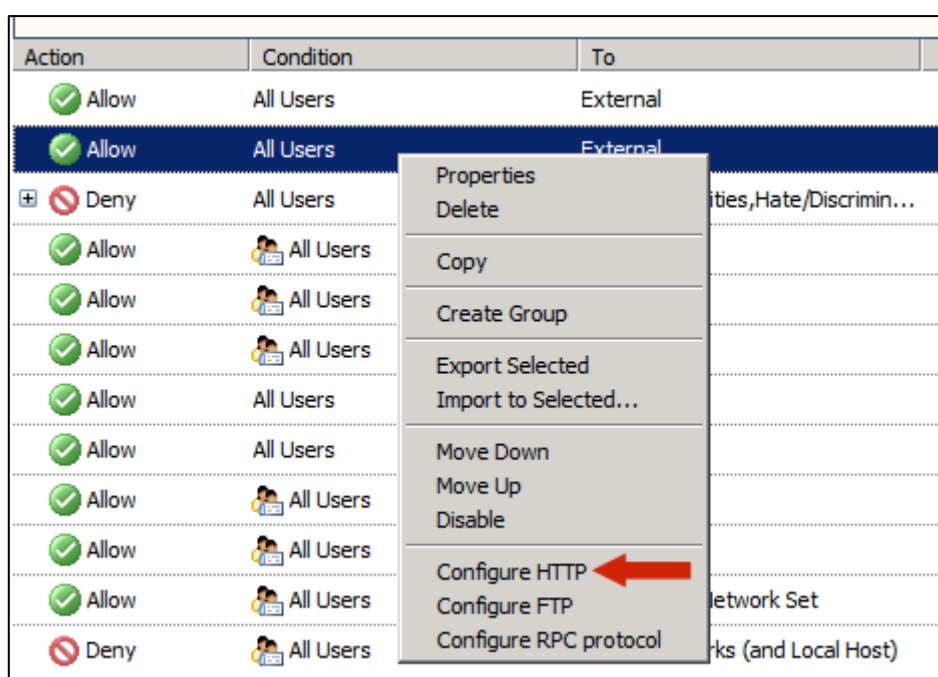
Az ábrából tehát jól látható, hogy, teljesen mindegy, hogy hogyan jut el a web proxy motorhoz a kérés, ha HTTP/S van "benne"⁷⁴, akkor ráereszti az alkalmazásszűrőket, majd a feldolgozott és ellenőrzött tartalom mehet vissza a Firewall szervizhez, majd végül jóval "lejjebb" a Firewall Engine-hez (ez már nincs az ábrán), ami viszont már egy

⁷⁴ Ha (például egy SNAT kliens esetén) nincs hozzárendelve a web proxy filter, akkor azért továbbmehet a kérés, csak a web proxy funkcionalitás illetve ellenőrzés kimarad.

kernel módú komponens. Tehát konklúzióként megállapítható, hogy ezen alkalmazásszűrők egyikéként a HTTP filter állandóan dolgozik (dolgozhat) a TMG-ben, már csak az a kérdés, hogy miért éri meg használni?

8.2.2 A HTTP FILTER KONFIGURÁLÁSA

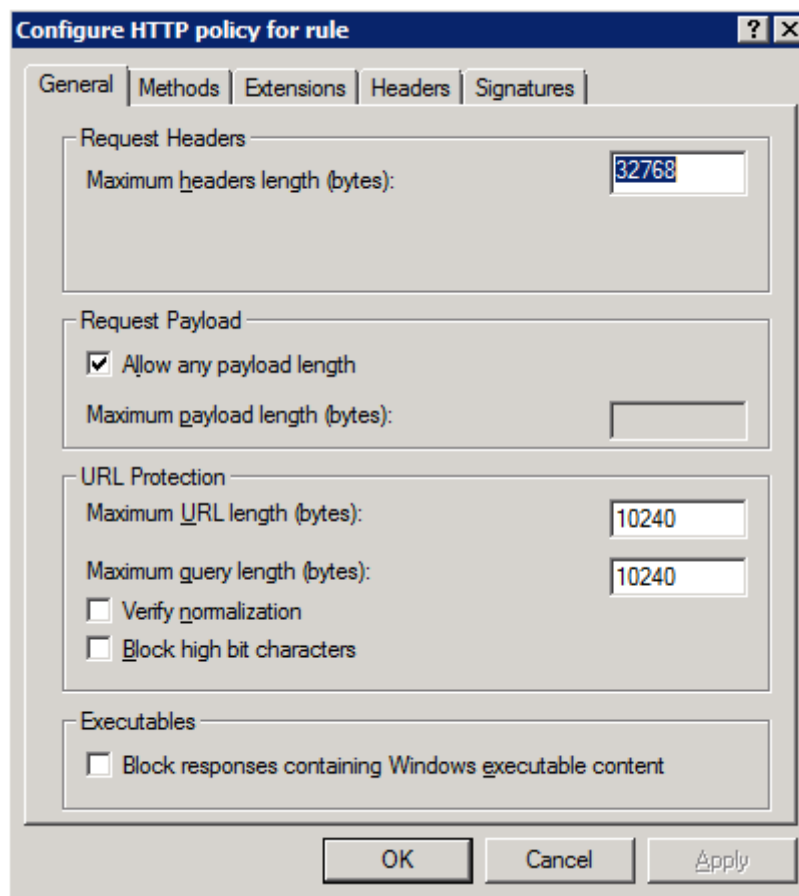
Ennek szűrőnek a beállításait minden egyes tűzfalszabályban, amelyben szerepel a HTTP vagy HTTPS protokoll elérhetjük. Ez egyúttal azt is jelenti, hogy lehetséges egyesével is, és teljes mellszélességben változtatni is az összes opciót - szabályonként. Meg még azt is jelenti, hogy akár ki- vagy be is kapcsolhatjuk szabályonként, külön-külön is a szűrést.



8.15 ÁBRA INNEN INDULUNK

Másrészt azonnal ellent is mondok önmagamnak, a legeslegelső opció, ami szembe jön velünk, ha megnyitjuk a HTTP filter konfigurációs paneljét, az máris globális, tehát ha egyszer átállítjuk, az összes szabályunkra érvényes lesz.

- **(Request Headers) Maximum Headers Length (Bytes):** A túl hosszú fejlécek és URL-ek buffer overflow módszerrel történő felhasználása ellen védekezhetünk ezzel a byte-ban megadott mérettel.
- **(Request Payload) Allow Any Payload Length:** Ezzel az értékkel limitálhatjuk a POST metódussal feltölthető adatmennyiséget. Ez a módszer egy lehetséges támadási forma is, de a korlátozása okozhat legális esetekben is elakadásokat, úgyhogy csak óvatosan.
- **(URL Protection) Maximum URL Length (Bytes):** Értelemszerű, az URL-ek hosszának korlátozása, az alapértelmezett érték a legtöbb esetben megfelelő.



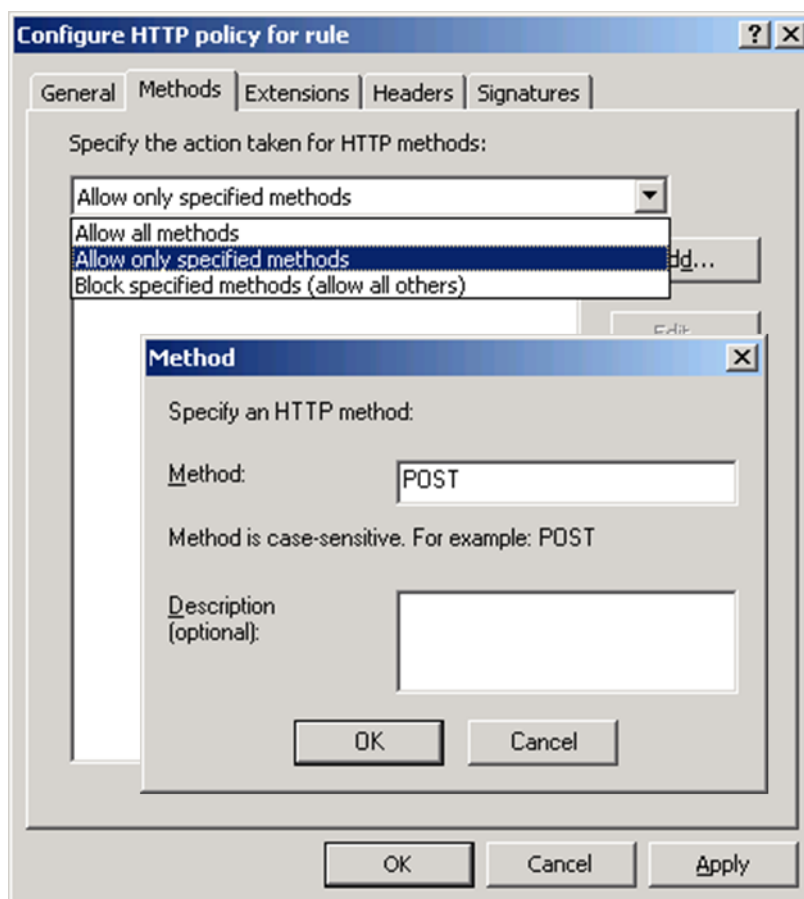
8.15 ÁBRA

- **(URL Protection) Maximum Query Length (Bytes):** Az URL-ben a lekérdezéshez használt kérdőjel (?) utáni hossz korlátozása.
- **(URL Protection) Verify normalization:** Ez egy érdekes dolog, valószínűleg mindannyian találkoztunk már az URL-ekben pl. szóközök helyett a %20 kombinációval, ami ugye természetes dolog, az enkódolás következménye. De ez egyben lehet egy speciális rosszindulatú kód része is, amit a TMG úgy tud kiszűrni, hogy kétszer is próbálja normalizálni az URL-t, és ha ezek után sem tűnnek el - a példánál maradva - a százalékjelek, és ha be is állítottuk ezt a restriktiót, akkor blokkolja a forgalmat.
- **(URL Protection) Block high bit characters:** Nos, kis hazánk esetén ez egy különösen fontos opció, hiszen ennek a bejelölésével bizonyos karakterkészletek⁷⁵ használatát tilthatjuk az URL-ekben, azaz ezeket a címeket egy- az-egyben kiszűri a HTTP filter. Ez nem olyan vicces, hiszen gondoljunk egy OWA-ra, amelyben megnyitunk egy ékezetes karaktereket tartalmazó tárgyú e-

⁷⁵ Az ún. Double-Byte Character (DBCS) illetve a Latin 1-es karakterkészlet elemeiről van szó, részletek itt: <http://support.microsoft.com/kb/837865>

mailt. Illetve nem nyitjuk meg, mert a TMG majd szépen blokkolja. És ugyanígy járhatunk egy Sharepointtal is.

- **(Executables) Block responses containing Windows executable content:**
Ezzel az opcióval a webszerverek válaszaiban esetlegesen megbúvó Windows futtatható tartalmakat blokkoljuk.

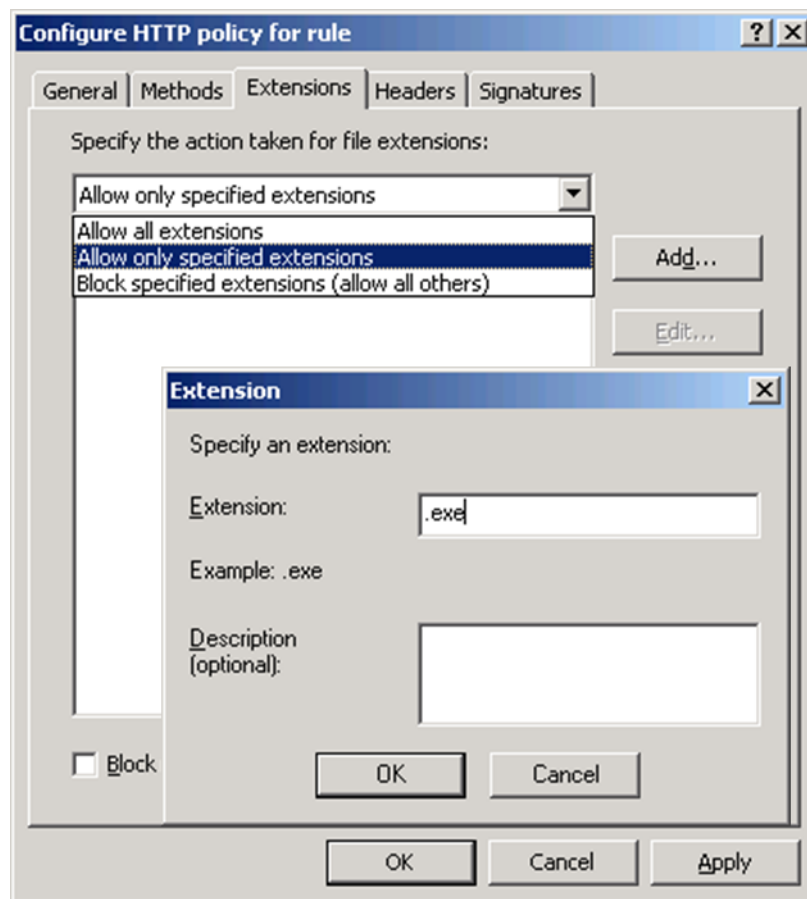


8.16 ÁBRA METÓDUSOK SZŰRÉSE

Ha átlépünk a következő fülre, akkor a HTTP metódusokkal (verbek) kapcsolatos részbe jutunk el, ahol alapesetben minden metódust engedélyezünk, de ki is választhatunk párat, amit (és csak ezeket) megengedünk, vagy éppen azokat jelöljük meg amelyeket blokkolunk és egyúttal minden mást megengedünk. Az ábrán látható POST-tal pl. az adott esetben a belső hálózatunk felhasználói számára a webes űrlapok kitöltését, pontosabban ezen űrlapok elküldését tiltjuk meg. A GET metódus blokkolásával pedig extra sávszélességhez jutunk, persze nem ez a legjobb módszer ☺

Emlékszünk a 2001 nyarán először megjelent Code Red-re? Ez egy olyan féreg volt, amely a fejlécében mindig megtalálható volt a "GET http://<ipaddress>/default.ida?" szakasz, ergo a .ida kiterjesztésével simán tudtuk szűrni az ISA 2004 HTTP filterével.

Az Extensions fülnél a kiválasztási módszer ugyanaz mint az előzőnél, az Add... gombbal viszont a konkrét kiterjesztéseket adhatjuk meg, pl. .exe, .bat, .cmd, stb. (MIME típus választás itt nincs). Ellenben a "Block Requests Containing Ambiguous Extensions" bepipálásával arra kényszerítjük a TMG-t, hogy minden olyan fájlkiterjesztést blokkoljon, amelyet nem képes felismerni és azonosítani.



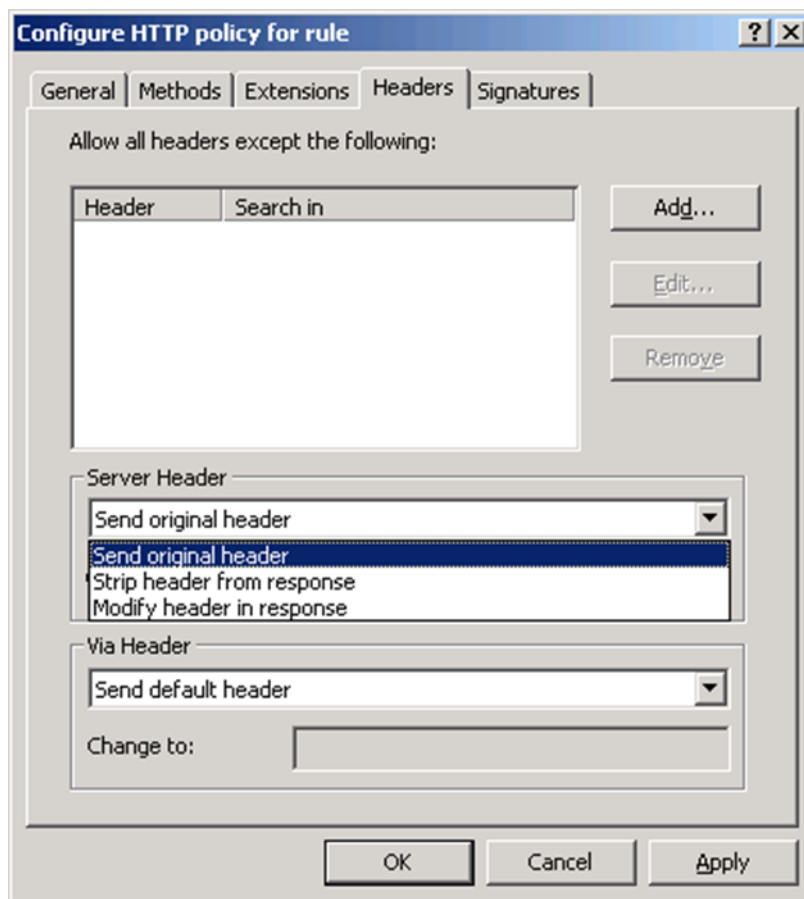
8.17 ÁBRA AZ .EXE NEM KÍVÁNATOS MÁR EGY IDEJE A HTTP-BEN

Akár egy HTTP kérésről, akár egy válaszról van szó, fejléc mindig van a kliens és a webszerver közötti forgalomban. OS, böngésző és alkalmazás adatok, formátum típusok és engedélyezési információk, ergo sok-sok minden utazik a fejlécekben. A Headers fül alatt viszont több szinten is bele tudunk nyúlni ebbe az adatcserébe. Az Add... gombbal például felvehetjük külön-külön a Request vagy a Response fejléc azon lehetséges részletét, ami alapján tiltani akarunk.

A Server Header rész kissé összetettebb, és a mi webszerverünk válaszába tudunk beleavatkozni a HTTP filter segítségével.

- **Send original header:** Ez az alapértelmezés, azaz nincs változtatás, az eredeti fejléc infó utazik, pl. a "Microsoft-IIS/7.0" sztring.

- **Strip header from response:** Teljesen lecsípjuk ezt az infót.
- **Modify:** Változtatunk, az általunk itt beírt szövegre (pl. "Secure Web Server" vagy "Apache/2.2.3 (Unix) mod_ssl/2.2.3 OpenSSL/0.9.7g") cseréljük az eredetit. Script kiddie-k és az amatőr verzió detektáló programjaik ellen talán még jó is lesz, egyébként ez egy kissé "Security by obscurity", azaz a szabad fordításom szerint kb. egy "ál-biztonsági" megoldás.



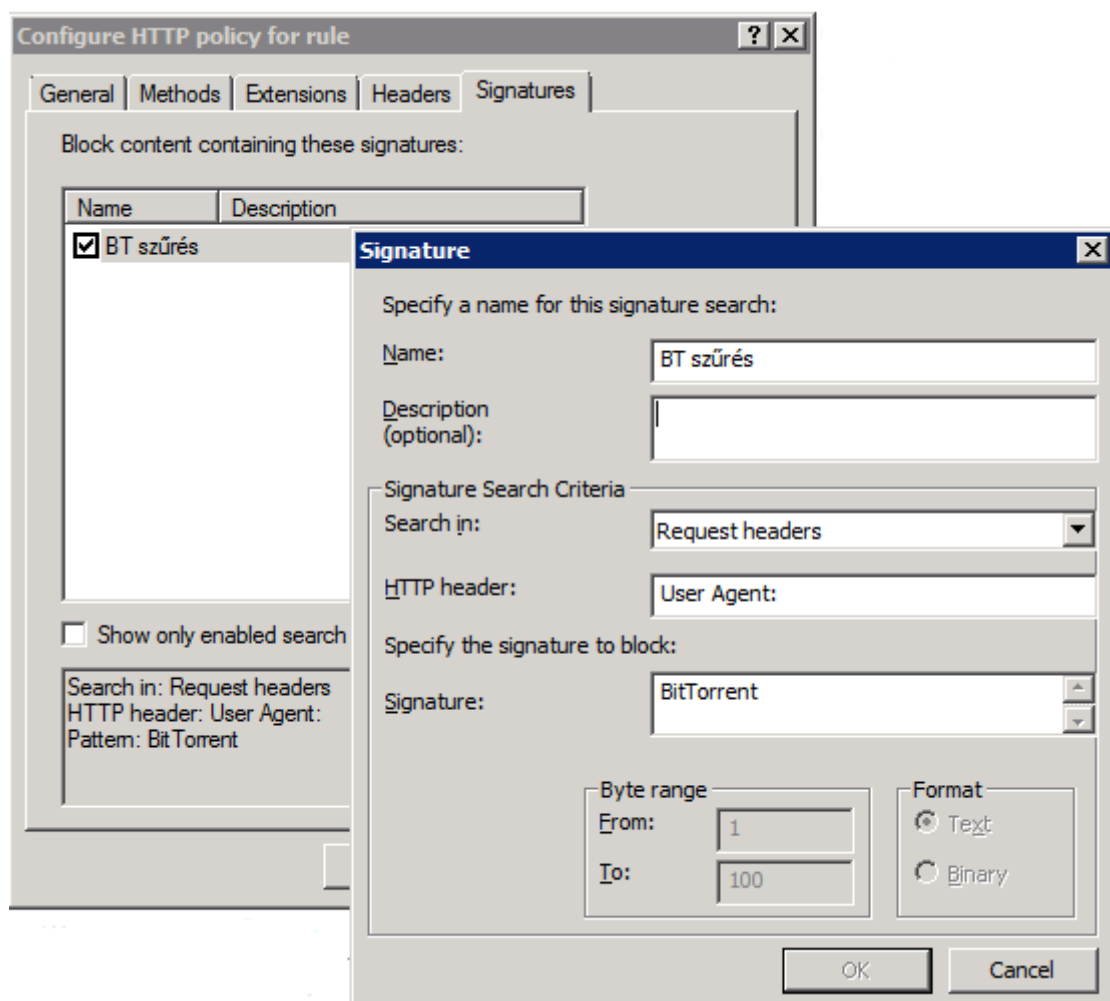
8.18 ÁBRA MI LEGYEN A SERVER HEADER?

Script kiddie: "Cracker wannabe, azaz valaki, aki szeretne cracker lenni, de túl lusta vagy túl hülye hozzá. Általában mások által megírt backdoorokat, rootkit-eket, már közismert exploitokat használ számítógépes rendszerekbe való illegális bejutáshoz. Jellemzően gyengén védett rendszereket támad meg. Az elnevezés eredetileg tizenévesekre vonatkozik, akik könnyen kihasználható hibákra vadásznak, hogy átvegyék a rendszer irányítását, vagy például webserverek tartalmát módosítsák, címdalát lecserélik (Lásd: deface). Manapság a kifejezés nem feltétlenül az életkorra utal, inkább a tudás hiányára.

Nem valódi crackerek, a biztonsági hibákhoz alig értenek, Ők a "szakma kukabúvárai".⁷⁶

Maradt itt még egy opció: ez az ún. Via Header. Ebbe tipikusan a proxy szerverek/alkalmazások pakolják bele a saját neveiket (pl. a TMG a gép NetBIOS nevét), a HTTP verzióval egyetemben, egy egyszerű azonosság ellenőrzése miatt, a kérés/válasz alapján. Ha nem akarjuk ezt az infót viszontlátni a fejlécekben, akkor szintén cserélhetjük ezt is, egy általunk választott tetszőlegesre, mindkét típusúnál egyaránt.

Most jön a HTTP filter befejezése, ami egyben talán a leghasznosabb alkalmazási területe is. A Signatures fül alatt járunk, ahol a TMG az általunk beállított egyedi lenyomatok alapján képes blokkolni, akár a fejlécek, akár pl. a törzs teljes tartalma alapján.



⁷⁶ Ez annyira kerek, hogy teljes tartalmában ide kellett másolnom, méghozzá innen: http://wiki.hup.hu/index.php/Script_kiddie

Hogy ez mit jelent? Nagyon sokat, de egyben nagyon óvatosan is kell bánnunk ezzel az eszközzel. Az ábrán pl. a Bittorent kliens teljes használatát tesszük tönkre (amennyiben HTTP-vel üzemel). Ezt az User Agent: infó alapján tudjuk megtenni, ami alkalmazásonként (de sokszor verzióként változva) egy teljesen egyértelmű, az adott alkalmazásra jellemző sztringet tartalmaz. Ezeket kinyomozhatjuk egy a belső hálózatra belőtt Network Monitorral, de számos szignatúra publikálva is van az interneten.⁷⁷

De nemcsak az alkalmazásokra jellemző gyári szignatúrák játszanak, emlékszünk a nem is régen példátlan módon sikeres Conficker féregre? Nos, ugyanitt a Request URL-t választva és a "search?q=%d&aq=7" sztringet beírva ezt is kiszűrhetjük/kiszűrhetjük (állítólag még mindig rengeteg helyen fertőz).

Szóval a HTTP filter ezen részébe felvihetünk számtalan szignatúrát, a TMG meg szépen ezek alapján megfogja majd az adott forgalmat. Kísérletezhetünk a törzsbe beírt tetszőleges sztringek használatával is, ezekkel is lesz eredmény, meg élmény.

Még egy utolsó dolog a HTTP filterrel kapcsolatban: láthattuk, hogy sok helyen, sok mindent konfigurálhatunk, amit aztán jó lenne lementeni is, és például egy másik TMG-re is átvinni. Nos, ehhez az ISA 2004-2006-ban volt egy httpfilterconfig.vbs szkriptünk, ami a telepítő anyagban megtalálható volt. Ez a TMG-ből eltűnt, de ettől függetlenül használható export/import feladatokra.

A probléma viszont ezzel a szkripttel az, hogy nem tud kiegészíteni egy meglévő állapotot egy beemelni kívánt HTTP filter konfigurációval. Na de erre is van egy kiegészítő megoldás, amihez el kell ballagnunk a népszerű, és rendkívül tartalmas <http://isatools.org> oldalra⁷⁸, hogy aztán a Jim Harrison által írt szkripteket alkalmazhassuk.

8.3 HTTPS INSPECTION

Azt már látjuk, hogy mi mindent szűrhetünk a HTTP folyamaban, de feltenném a költői kérdést: ez elég? Nem, ma már nem. Ma, amikor már a felhasználó is tud egy SSL tunnell képezni egy nyitott, a neten működő anonymous proxy-hoz, és így kihagyni az ellenőrzésből a mi proxy szerverünket, illetve amikor akár HTTPS-ben is jöhetnek a káros tartalmak, nem. Tehát szűrjünk, ha a proxynk képes erre. De van egy másik oldala

⁷⁷ Például itt: <http://technet.microsoft.com/en-us/library/cc302520.aspx>

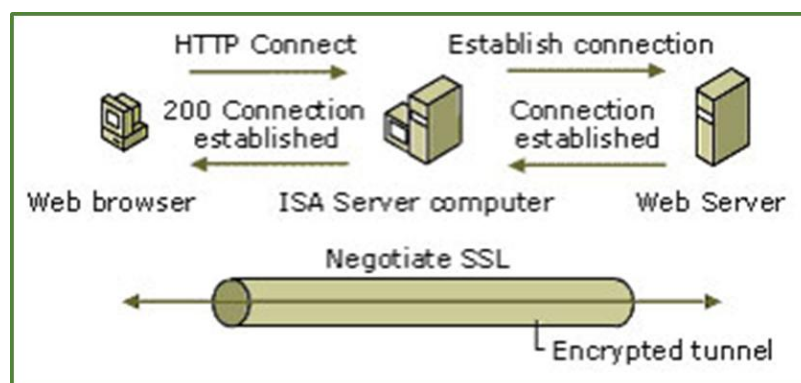
⁷⁸ http://isatools.org/tools/block_hcp.vbs és http://isatools.org/tools/block_lnk.vbs

is a HTTPS ellenőrzésnek. Szabad ezt? Az integritás és az eredetiség megőrzése, mint fő elvek nem sérülnek? Végül is de, ám a "valamit valamiért" elv is ott van a mérleg másik serpenyőjében.

Az egyik legelső TMG előadásomban szűk körben az MVP-kkel, miután elmagyaráztam, hogy hogyan működik, az egyik kolléga azonnal nekem szegezte a kérdést: "- Akkor az OTP-s banki műveleteimet is fogod így látni?" Nos, igen, csak ezt tudtam válaszolni. Azonban, – az én véleményem szerint – megfelelően lefektetett szabályzással, kivételekkel, a megbízhatónak ítélt oldalak ellenőrzésének kihagyásával, egy vállalati környezetben azért mindenképpen bevállalható.

Illetve azt azért lássuk be, hogy bár technikailag lehetséges, a TMG nem ad erre egyszerű felületet a TMG üzemeltetőnek. Tehát az online log viewerben nem fogom látni a teljes http body-t clear-text-ben. Igazán felkészülten, mély műszaki ismeretekkel rendelkezve, egy debugger segítségével kitudom szedni a forgalmat clear text-ben, de ezt egy átlagos TMG üzemeltető nem fogja ezt megtenni. Ha pedig képes rá, akkor másik öt egyszerűbb módon fogja megszerezni tőlünk a banki adatainkat. (A lektor megjegyzése.)

De ha nem morális, hanem technikai szemszögből közelítek akkor a lényeg az, hogy a TMG-ben a HTTPS forgalom terminálása és a TMG-től a felhasználóig zajló szimpla HTTP teljes körű ellenőrzése (EMP, HTTP filter, URL filter és minden más) immár a rendelkezésünkre áll. Plusz – és ezt sokan elfelejtik – egy több részes, konfigurálható feltételeket tartalmazó tanúsítványvizsgálatot is rejt a HTTPS Inspection.



8.20 ÁBRA EZ EGY RÉGI RAJZ, DE A LÉNYEG NEM VÁLTOZIK: A CSŐBEN BÁRMI MEHET(ETT)

De hogyan csinálja ezt a TMG? Nyilván nem a "HTTPS törésével", hanem egy nagyon elegáns trükkel, ami alapján viszont a TMG-t simán tekinthetjük egy "Man in the

Middle”-vel operáló támadónak, a külső webservert és a belső kliens közötti forgalomban ☺. Szóval amikor a kliens felépítene az SSL kapcsolatot, a TMG ezt nyomban elkapja, és le is ellenőrzi távoli szerver tanúsítványát. Ezután lemásolja a webservert tanúsítványának részleteit, majd legyárt egy új tanúsítványt ezekkel a részletekkel, és a sajátjával (mint Certificate Authority⁷⁹) írja alá! Ezt kapja a kliens, így két különböző SSL session alakul ki, és a “rövidebben” már nem lesz akadálya a teljes körű ellenőrzésnek. Gyakorlatilag outbound SSL inspection nélkül az SSL handshake a felhasználó alkalmazása és a cél kiszolgáló között történt meg. Outbound SSL inspection esetében a TMG amikor észreveszi az SSL handshake üzenetet, akkor indít el egy SSL handshake-t a cél kiszolgálóval. Ha a handshake sikeres, akkor válaszol is a célkiszolgáló helyett, kvázi proxy-zva annak válaszát a klienshez. A kliens és a TMG között pedig az előző sorokban említett tanúsítványt használja a TMG, a handshake során.

Egyébiránt félig meddig nem számít újdonságnak ez a dolog, hiszen aki már az ISA 2004-et is üttögette, az tudja hogy a saját webszervereink felé menő forgalomban az ún. SSL Bridging technikával már képes volt az ISA is terminálni az SSL kapcsolatot (bár technikailag kicsit egyszerűbb a kivitelezés, lásd következő fejezet), majd ellenőrizni a forgalmat. A HTTPSi viszont bármilyen a felhasználók felől/felé menő forgalomban képes ezt produkálni.

8.3.1 A KÖVETKEZMÉNYEK ÉS A KÖVETELMÉNYEK

Bármilyen szenzációsan is működik az ellenőrzés, azért számolnunk kell pár következménnyel illetve követelménnyel a HTTPSi bevezetése kapcsán:

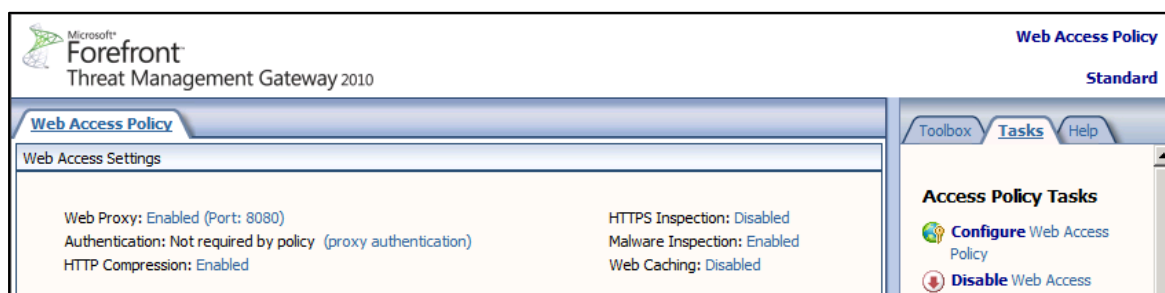
- Itt ugye egy klónozott tanúsítványról van szó, ami nem biztos hogy tetszik mondjuk annak a banknak vagy webáruháznak, amellyel a kliens kapcsolatba lép. De lehet kivételezni, globálisan, akár az URL kategóriák segítségével is.
- A web proxy naplókba a teljes URL kerül ilyenkor, ami ugye szenzitív is lehet.
- Akár az egész tartalom bekerülhet a cache-be, ami megint csak nem biztos, hogy szimpatikus következmény, persze cache kivételeket is lehet kreálni.
- Ha a HTTPSi-t szeretnénk használni, akkor a tanúsítványokkal és/vagy tanúsítványkiadókkal is bűvészkednünk kell. Két alapeset lehetséges:
 - Ha a TMG által generált önaláíró tanúsítványt akarjuk használni, akkor a kliensek meg kell bízzanak a TMG-ben, mint tanúsítványkiadóban. Ennek a megoldására több lehetőségünk is lesz majd (automatikus is).

⁷⁹ Amelyben persze a kliens vakon megbízik, erről gondoskodnunk kell majd előre.

- Ha egy bármilyen más tanúsítványt akarunk felhasználni a TMG-ben ehhez (értsd: már van pl. egy magunk által üzemeltet PKI alrendszerünk), akkor annak a kiadójában kell hogy megbízzanak a kliensek, de a TMG is!
- A TMG saját magát leszámítva nem szereti a "Man in the Middle" módszerrel támadókat, ergo a külső tanúsítványok vizsgálata nagyon alapos lesz – alapértelmezés szerint is, valamint ne felejtjük el, hogy ez az ellenőrzés akkor is működhet, ha HTTPS-i ki van kapcsolva. A következő szempontok alapján ellenőriz a TMG:
 - A kapcsolatban lévő külső gép nevének meg kell egyeznie a tanúsítvány Subject mezőjében, vagy a SAN (Subject Alternative Names) mezőben szereplő egyik elnevezéssel.
 - Szerver hitelesítési (Server Authentication) típusúnak kell lennie a tanúsítványnak.
 - Mind a kiadás, mind a lejáratnak érvényesnek kell lennie.
 - A TMG meg kell hogy bízson a tanúsítvány kiadójában.
 - A tanúsítvány visszavonási listának (CRL, Certificate Revocation List) elérhetőnek kell lennie, és nem szerepelhet a szerver tanúsítványban.

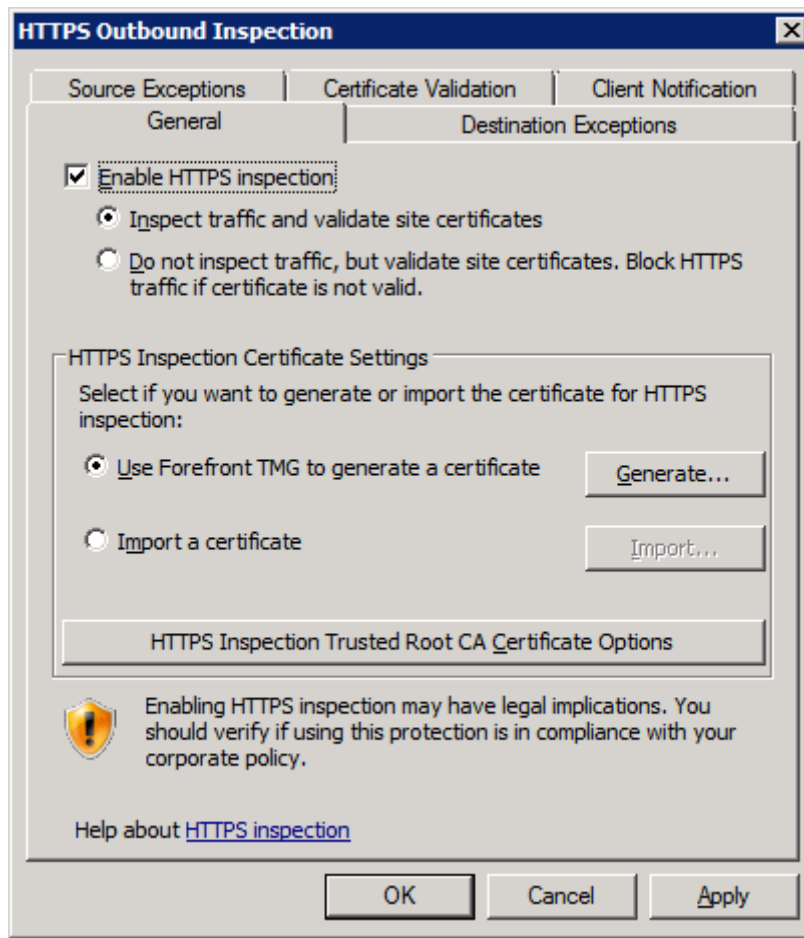
8.3.2 A HTTPS-I KONFIGURÁLÁSA

Nagyjából ez a fejezet a tanúsítványok és a tanúsítványkiadók konkrét kezeléséről szól, azaz szinte mindenhol visszaköszön majd, hiszen az ezekkel történő konfigurálás az alapja a HTTPS-i-nek. A 8.20 ábrán látható, immár szokásos helyről indulunk.



8.21 ÁBRA A 6-OS LISTÁBÓL MÁR CSAK A TÖMÖRÍTÉST NEM PISZKÁLTUK

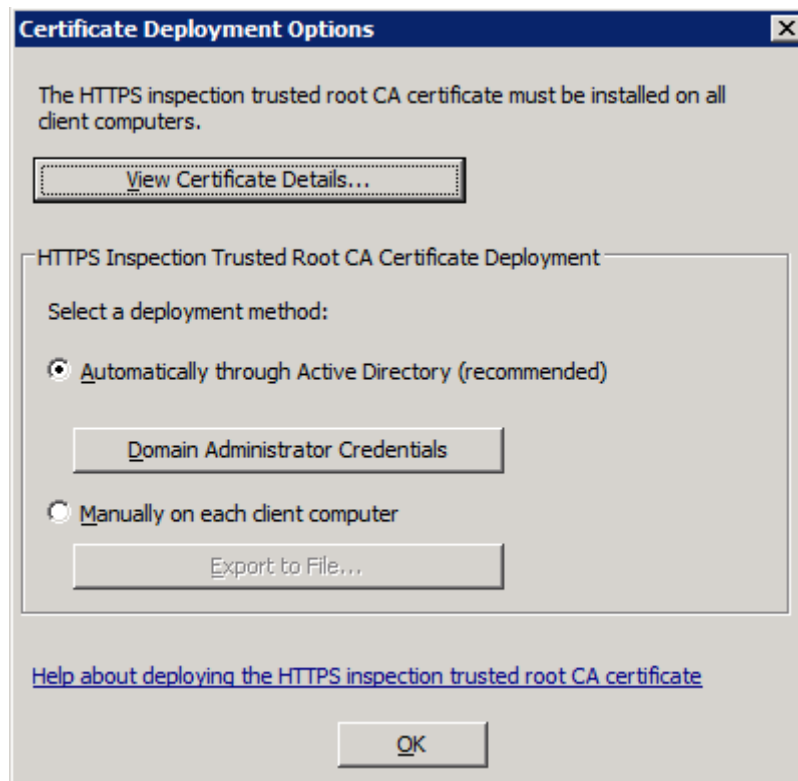
A General fül egyből mélyvíz. Az "Enable HTTPS Inspection" alatt máris két választási lehetőségünk is lesz:



8.22 ÁBRA

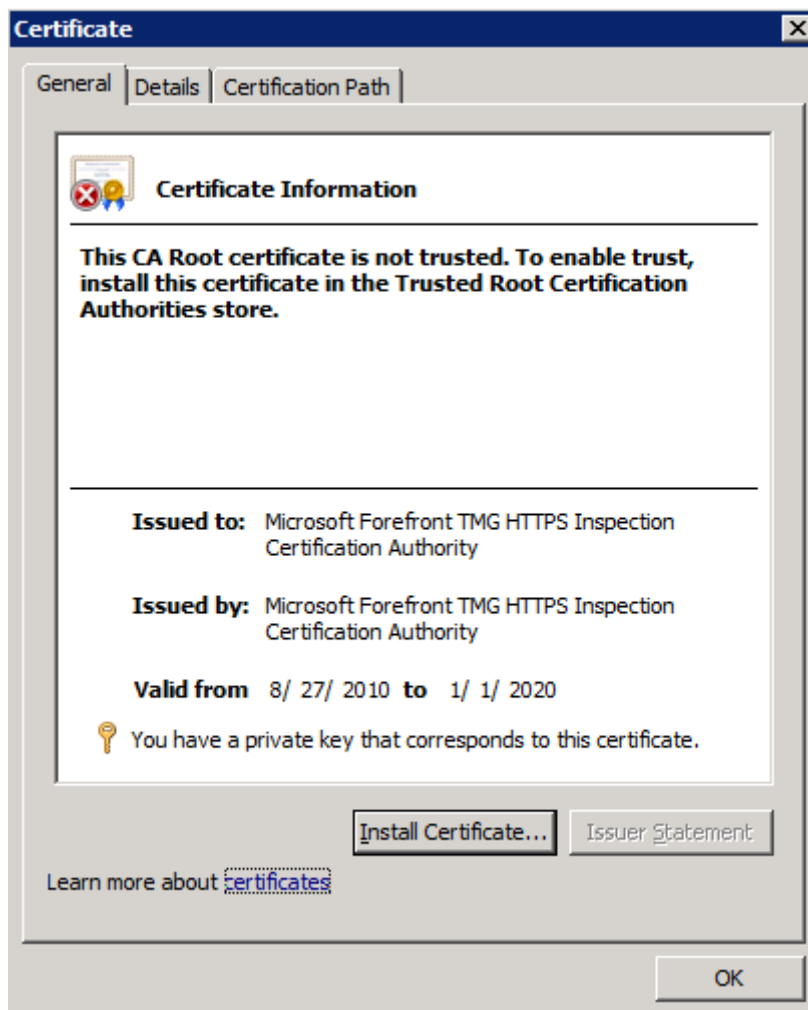
- **Inspect HTTPS traffic and validate HTTPS site certificates:** a komplett HTTPS forgalom ellenőrzés + a tanúsítványok ellenőrzése is.
- **Do not inspect HTTPS traffic, but validate the HTTPS site certificate:** csak a tanúsítványok ellenőrzése.

A középső rész a tanúsítványok generálásával/importálásával kapcsolatos lehetőségekkel foglalkozik. Először is eldönthetjük, hogy egy a TMG által kreált tanúsítványt használunk-e majd az aláírásra, vagy már meglévőt importálunk be. Ha az első választás a favorit, akkor a "Generate" gomb alatt a kiadó nevét illetve az érvényességet is be tudjuk állítani (a "Soha le nem járó", azaz a "Never" opció 2049.01.01-et jelent). Ha viszont importálunk, akkor egy privát kulccsal ellátott tanúsítványra lesz szükség (.pfx). Ezzel megvan a TMG tanúsítványa, de van még egy fontos feladat, amelynek hatására a 8.20-as ábra jelenik meg.



8.23 ÁBRA AKÁR AUTOMATIKUSAN IS TERJESZTHETŐ

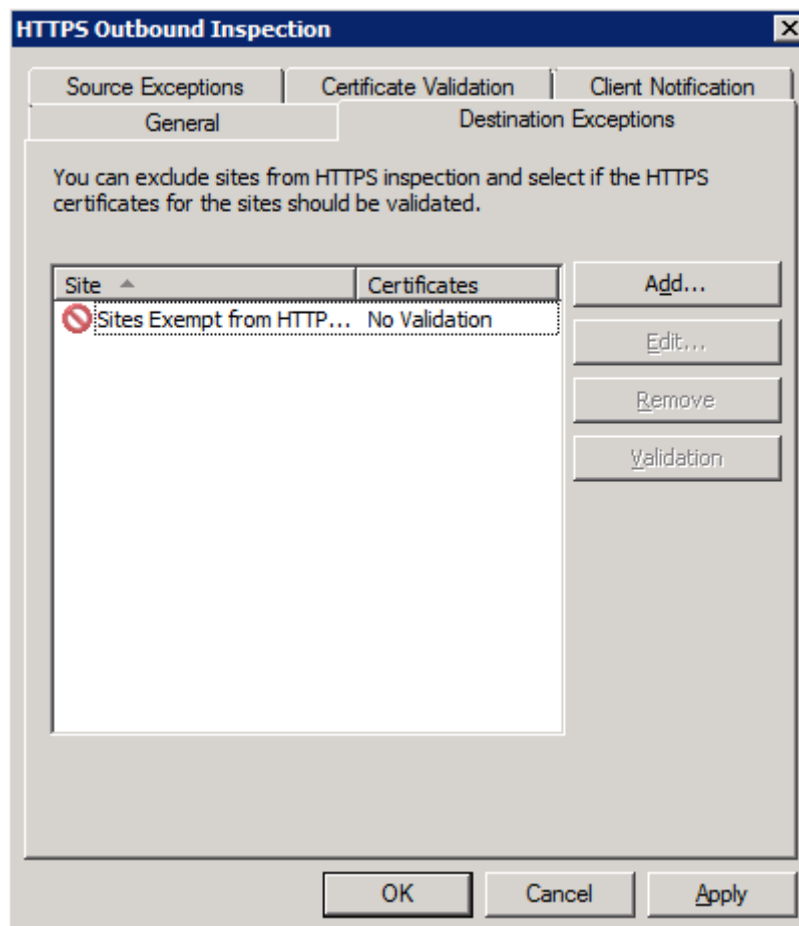
Ez a "HTTPS Inspection Trusted Root Certificate Options" nevű, jó széles gomb, amely alatt egyszerűen megnézhetjük (View Certificate Details) a TMG Root CA tanúsítványát (8.24 ábra). Az ábrán még az is látszik, hogy jelen pillanatban ez a tanúsítvány még nem megbízható, mivel még nem szerepel számítógép megbízható tanúsítványkiadóinak listájában (Trusted Root Certification Authorities).



8.24 ÁBRA MÉG NEM SZÁMIT MEGBÍZHATÓNAK

Épp ezért kanyarodjunk vissza az előző ábrához (8.23), ahol a TMG Root CA tanúsítvány automatikus terjesztését is kérhetjük az Active Directory segítségével (ehhez egy Domain Admins csoporttagságú felhasználó jogosultsága kell majd), illetve akár ki is exportálhatjuk az előbb említett root tanúsítványt a manuális terjesztéshez.

Az AD segítségével? Igen, ha ezt választjuk, akkor a TMG Root CA bekerülhet a Domain Enterprise Trusted Root Store-ba, ahonnan minden tartományi tag a következő Csoportházirend frissítéskor (15 perc múlva) megkaphatja, vagy a gpupdate /force-szal manuálisan és azonnal. Ezt aztán például a "certutil -store -enterprise root" paranccsal ellenőrizhetjük is.

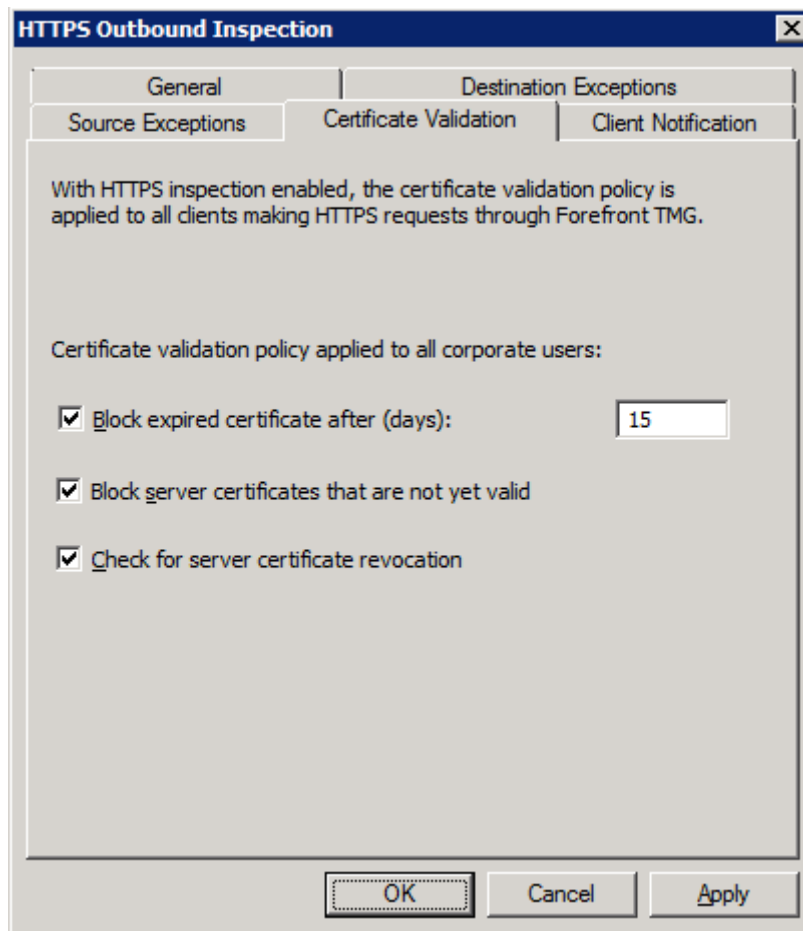


8.25 ÁBRA

Végeztünk a HTTPSi működéséhez kapcsolódó tanúsítványkezeléssel, de nem végeztünk a HTTPSi-vel. A "Source Exceptions" és a "Destination Exceptions" fül tartalma a forrás (belső háló) vagy a cél (Internet) típusú kivételek listája lesz, amelyeket csoportokba szervezhetünk (illetve a gyári, szokásos csoport is létezik).

De - ahogyan a képen is látszik - akár az itt megjelenő kivételeknél is kérhetjük a "Validate" gombbal egyesével a tanúsítvány vizsgálatot - annak ellenére, hogy a forgalom ellenőrzés szempontjából valóban kivételekről van szó. A cél kivételnél természetesen a könyv későbbi fejezetében tárgyalt URL kategóriákat is használhatjuk. Így anélkül hogy fel kellene sorolni az összes online bank elérési útját, egy kényelmes mozdulattal mondhatjuk azt, hogy a banki oldalak irányába nem kérjük a HTTPSi-t.

De ha még ezt sem akarjuk, akkor hagyjuk meg a "No Validation" állapotban, illetve vissza is állhatunk az első érvényesítés után a "No Validation" gombbal.



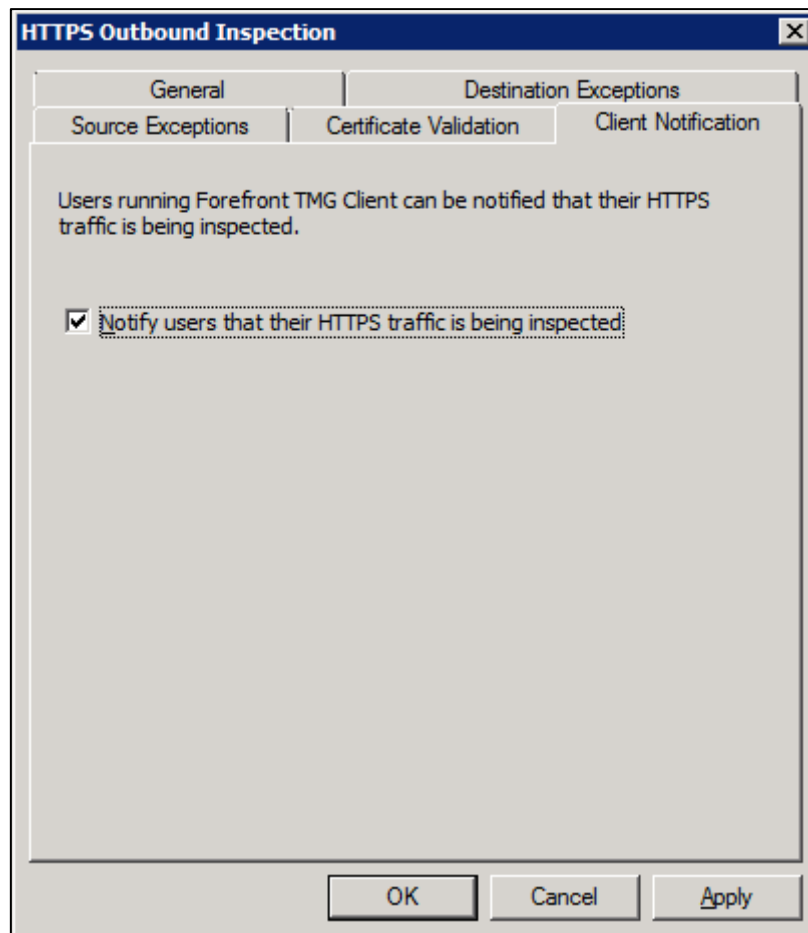
8.26 ÁBRA SZÖRÖSSZÍV

A "Certificate Validation" fül tartalmára már utaltam a 8.3.1 fejezetben. A lejárt vagy bármilyen okból nem érvényes tanúsítványok illetve a visszavonási tanúsítványlisták elérhetősége (illetve egyáltalán a léte) ellenőrzése és adott esetben az ilyen szerver blokkolása állítható be itt. Érdemes megfigyelni ezt a dialógus ablakot. Mi hiányzik róla? Korábban említettük, hogy a tanúsítvány ellenőrzésénél a TMG-nek fontos szempont az, hogy megbízzon a cél kiszolgáló által használt tanúsítványt kiadó tanúsítványkiadóban. Ez a funkció itt nem konfigurálható és rossz hírem van: ez a funkció nem is kapcsolható ki. Tehát ha a certification validation-t használjuk és a felhasználó egy önálírt tanúsítvánnyal rendelkező cél kiszolgálót szeretne elérni, akkor a TMG azt nem fogja engedélyezni. Hogy megoldjuk ezt a problémát a következő lehetőségeink vannak:

- Meg kell bízunk a tanúsítványt kiadó tanúsítványkiadó hivatalban. Hol kell megbízunk benne? Természetesen a TMG-n (gondoljunk arra, hogy két SSL handshake zajlik és a TMG találkozik a cél kiszolgáló tanúsítványával).
- Az adott felhasználó által használt eszközt felvesszük a forrás kivétel listára.
- Az elérni kívánt kiszolgálót felvesszük a cél kivétel listára.
- Tudomásul vesszük hogy nem bízunk meg a tanúsítványban és a forgalmat nem engedélyezzük.

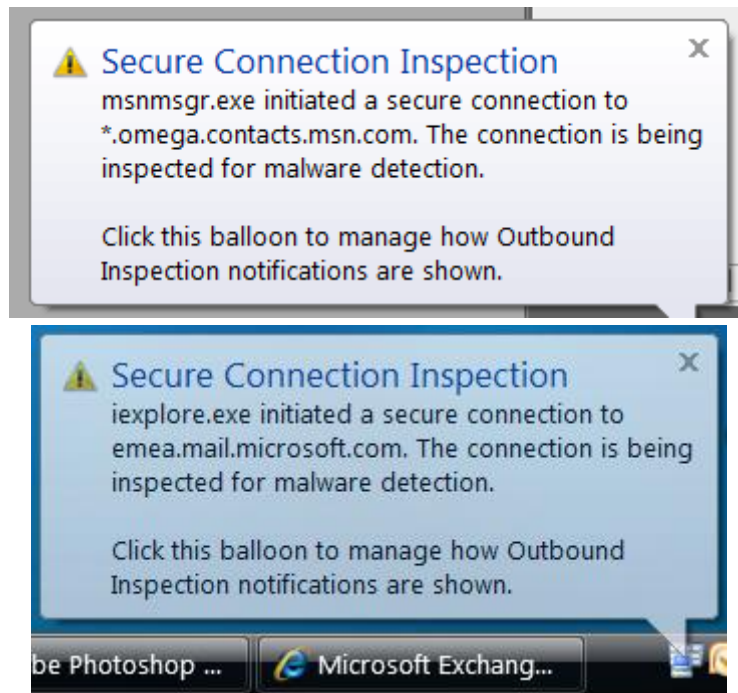
Az utolsó fül a tűzfal kliensen keresztüli kommunikáció lehetőségét szabályozza, azaz a felhasználók kaphatnak értesítést arról, hogy annak ellenére, hogy HTTPS-ben folyik a forgalom, az adott oldalt a TMG-n keresztül vizsgáljuk.

Természetesen ehhez minimum a TMG RTM telepítési csomagban lévő (Build 07.00.7734.100) verziószámú tűzfal szükséges, csak ezzel klienssel működik az "üzengetés", a régi ISA kliensekkel nem, de annyira nem, hogy azokban nincs is negyedik fül.



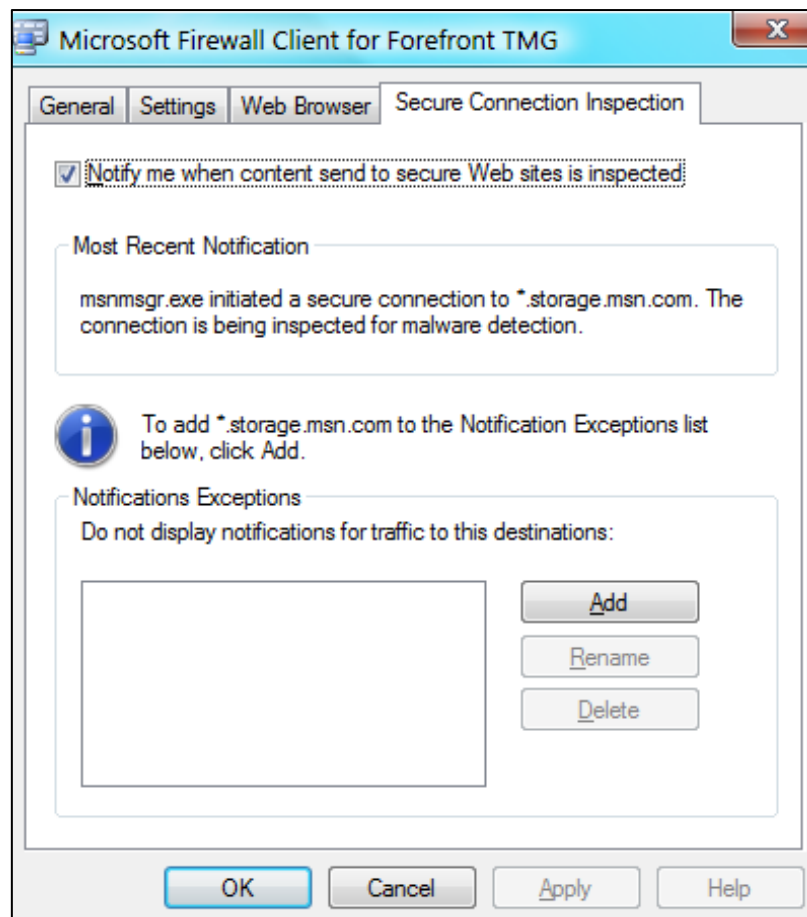
8.27 ÁBRA CSAK EGYETLEN OPCÍÓ, DE SOKAT SZÁMÍT

Végezetül nézzük meg az új tűzfal kliens idekapcsolódó új beállításait, illetve először a két különböző buborékot is, amelyben szépen látszik az értesítések formátuma.



8.28 ÁBRA A BUBORÉKOK (A MÁSODIK MÁR HALVÁNYODOTT MIKORRA ELKAPTAM)

A tűzfal kliens egyébiránt a "Most Recent Notification" alatt jegyzi is a legutolsó értesítést, amelyet így nagyon egyszerűen fel is tud venni a felhasználó a kivételek közé, mármint nem az ellenőrzés alóli kivételről van szó, hanem csak az értesítésekre gondolunk.



8.29 ÁBRA ÜZEN, DE TÁROL IS A TÚZFAL KLIENS

Érdemes mindenkit megnyugtatni azzal kapcsolatban, hogy a TMG Client nem fogja minden egyes https kérés /válasznál a felhasználót kiértékelni, mert akkor valószínűleg a buborék folyamatosan kint lenne. Alapértelmezésben cél kiszolgálónként 12 óránként egy értesítést jelenít meg a TMG kliens. A 12 óra egy változtatható paraméter, amit ha módosítani szeretnénk akkor a munkaállomás rendszerleíró adatbázisában az alábbi elérési úton tehetjük meg: `HKLM\SOFTWARE\Microsoft\RAT\Stingray\Debug\FwcMgmt FWC_MGMT_HTTPS_TEMPORARY_DISABLED_TIMEOUT` (A lektor megjegyzése).

8.4 URL-F

Technikai szempontból ezen nagy fejezet legkevésbé bonyolult megoldása jön, azonban a fontossága megkérdőjelezhetetlen. Az ISA szerverekben az URL-ek tartalom alapján történő szűrésére nem, illetve csak manuális módszerrel vagy külső segítséggel volt lehetőség. Kézzel pl., lelkesen készítettem én egy "Pornó" nevű URL csoportot, amelybe hosszas kutatással (☺), bevihettem a megfelelő webcímeket, de ez egy statikus, és finoman szólva sem tökéletes módszer. Léteztek emellett kicsit profibb,

“maszek” módszerek is, amikor egy szkripttel már többféle és jelentős mennyiségű, mások által összegyűjtött URL-eket beimportálhattunk, majd a szabályokhoz hozzá rendelhattunk, és így a tiltó szabályok már jobban működtek. De ez még mindig statikus módszer volt, ráadásul rengeteg fals találattal.

Így aztán jobb híján maradtak a 3rd party szoftverek, amelyekből volt bőven, jómagam is üzemeltettem anno pl. a Websense tartalomszűrő szoftverét (amely azóta a legnagyobb riválisával a SurfControl-lal egyesülve egészen naggyá nőtt), amely már korrekt volt, automatikus, és dinamikus – viszont kifejezetten drága, még vállalati környezetben is.

A TMG Beta3-tól viszont kaptunk egy beépített megoldást, amely végre megoldotta a problémánkat és így a céges vagy éppen iskolai/oktatási szabályzatoknak megfelelően az URL Filtering (URL-F) távol tudja tartani a belső felhasználóinkat a tiltott weboldaltól. Nézzük meg, hogyan.

8.4.1 HOGYAN MŰKÖDIK?

Az URL-F 79 beépített kategóriával és 11 fő csoporttal, illetve rettenetes méretű, sok tízmillió URL-lel segíti a célok behatárolását, amelyet a Microsoft Reputation Service (MRS) tart formában és tölt fel, és így a TMG minden kérés alkalmával a web service-n keresztül az MRS-től tölti majd le.

Az MRS létrehozását a Microsoft a 2009-es RSA konferencián jelentette be, egyben jelezve, hogy a gyűjtemény forrása több beszállító partnertől érkezik majd. Ami még érdekes, hogy a TMG az első Microsoft termék, amely használja az MRS lehetőségeit.

Az MRS egy felhő alapú kategorizáló rendszer, ami a Microsoft adatcentereiben tárolódik, és amelyet a TMG online lekérdezésekkel ér el. Már hallom is a felszisszenést, hogy akkor internet nélkül nem működik ez a képesség? Dehogynem. Az elérési sebesség és a sávszélesség optimalizálás miatt a TMG gyorsítótárazza mind az URL-eket, mind a kategóriákat. Természetesen minden eltárolt objektum rendelkezik egy TTL értékkel, amely alapján rendszeresen frissíteni kell, de ezen kívül a TMG csak akkor nyúl online az MRS-hez, ha egy kérést abszolúte nem tud kiszolgálni a cache-ben tárolt adatok alapján⁸⁰.

⁸⁰ És természetesen egy biztonságos kapcsolaton keresztül teszi mindezt.

Az URL-F használata nagyon egyszerű, mivel abszolúte belesimul az engedélyező tűzfal szabályokba. Gyakorlatilag a teendők csak annyi, hogy engedélyezzük globálisan, majd a kívánt kategóriát vagy egyszerre többet is, egy új tiltó szabályba belehelyezzük. A szabály célja már ismert módszerekkel lehet egy felhasználó vagy egy csoport, vagy hitelesítés nélkül pl. egy IP intervallum. Innentől a felhasználó a tiltott URL-eket nem éri el, és mivel az adatbázis dinamikusan frissül, ez az újonnan bekerült címekre is vonatkozik. Erről egy némiképp testreszabható HTML üzenet formájában is tájékoztatjuk a felhasználót. Egy további fontos előnynek számít az URL szűréshez kapcsolódó jelentések és napló bejegyzések is, amelyekkel egy kerek képet kaphatunk a szervezetünk internet használatáról, beleértve azt is, hogy milyen oldalakat (és pontosan kik is?) szeretnének megnézni a felhasználók, ha nem lennének tiltások.

De van még egy kiaknázzható előny, amelyet az URL-F nyújt, és ez pedig a maguk a címgyűjtemények, amelyeket pl. a Malware Inspection vagy pl. a HTTPS Inspection alkalmazása során is felhasználhatunk korrekt kivételezés apropóján.

Végezzünk el egy érdekes vizsgálatot, ez itt egy példa cím:

www.microsoft.com/pathA/pathB

Ez ugye simán felbontható több részre.

- .com – unknown
- microsoft.com – General business
- www.microsoft.com – unknown
- www.microsoft.com/pathA - Phishing (not inherited)
- www.microsoft.com/pathA/pathB - Portal

A „not inherited” azt jelenti, hogy nem öröklődik a subpath-ra (pathB), ergo a végeredmény:

- General business
- Portal

Még néhány tipp és illetve információ a működéssel kapcsolatban:

- Lokálisan felülírhatjuk, azaz kiegészíthetjük a kategóriákat az általunk hasznosnak vélt címekkel.
- Lekérdezhetőek az adatbázisban szereplő címek, ami egyrészt érdekes (sajnos magyar címeknél nem mindig pontos, vagy ismert a valódi kategória), másrészt előzetesen fontos is lehet.
- Kihasználhatjuk az URL szűrést a reklámok és hirdetések (ad) blokkolására is.

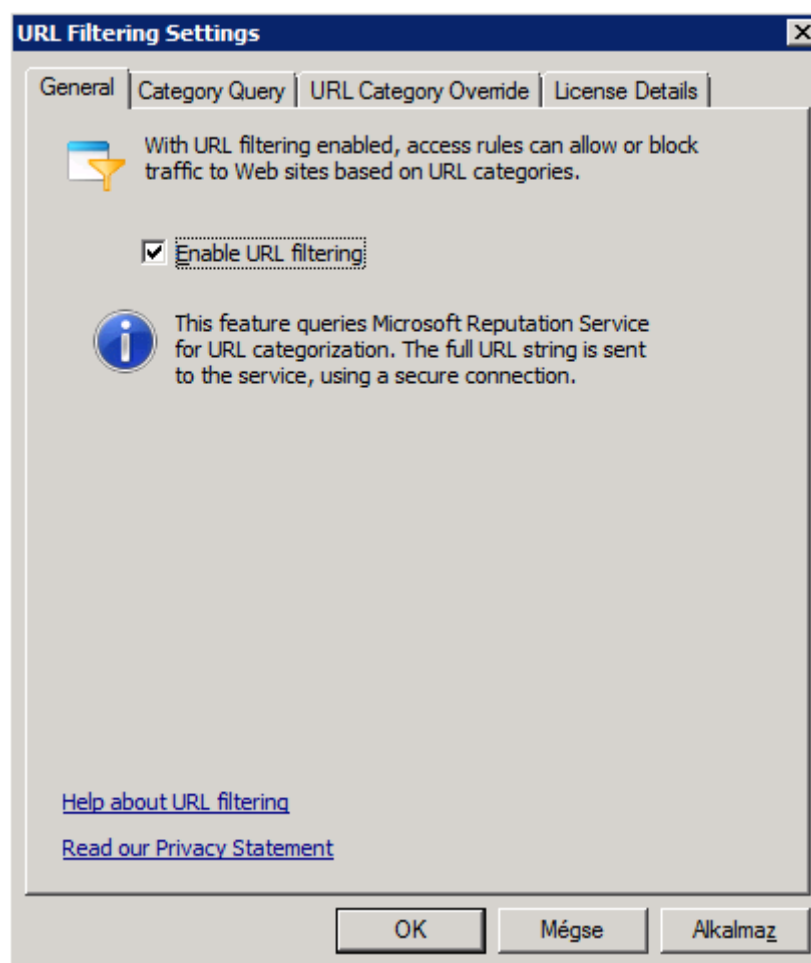
A KAPUN TÚL

- Az URL szűrés frissítése feliratkozás alapú, az EMP-hez hasonlóan egy licenz kell hozzá az első 120 nap után, de a kettő kombinálva van a TMG-ben, ahogyan az a 8.12 ábrán látható is.
- A TMG SP1-ben talán ez a terület, ahol a legtöbb pozitív változás történt. Erről majd a 13. fejezetben bővebben beszámolok.

8.4.2 AMIT AZ URL-F-BŐL LÁTUNK

Két különböző helyen érjük el a TMG-ben az URL szűréssel kapcsolatos beállításokat, ebből az egyik a globális, a másik pedig az adott tiltó tűzfalszabályon belül. Nézzük először a globális beállításokat, amelyek kivételesen nem a már sokat emlegetett Web Access Policy keret felső részéből, hanem az Action Pane\Tasks füléből érhető el.

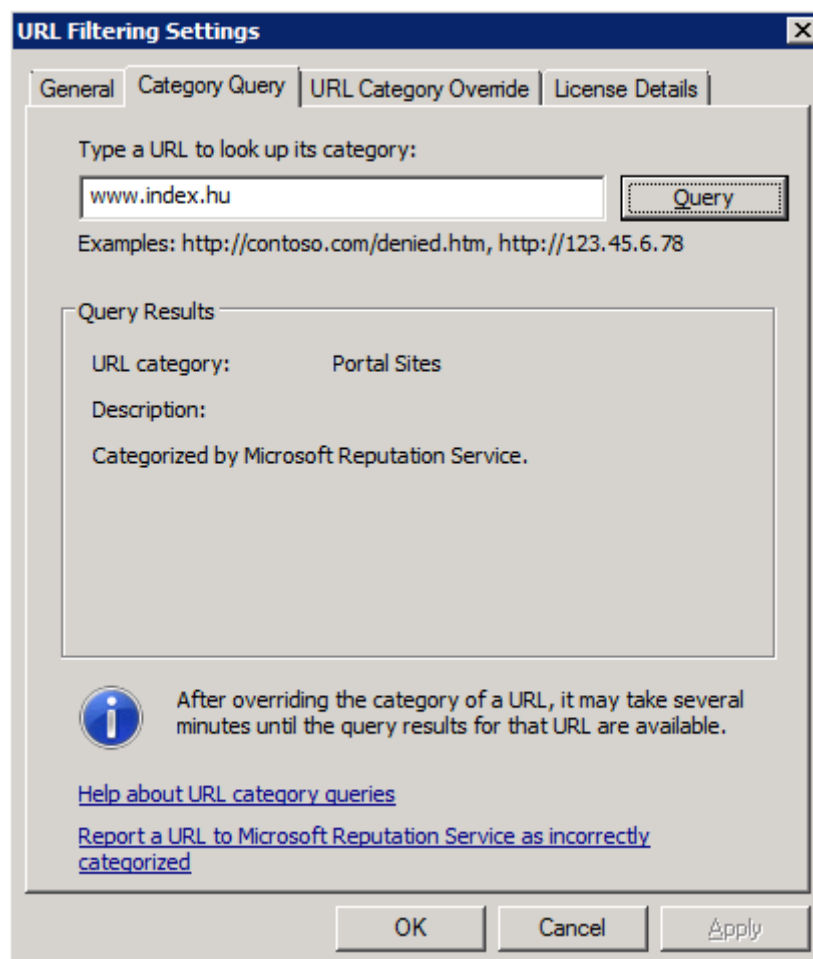
Az eleje nem bonyolult, egyszerűen engedélyezünk, ami esetleg lényeges lehet, hogy egészen az első szabály elkészítéséig (vagy egy meglévő módosításáig) a hatása nem érvényesül, ellenben a teszteléshez muszáj bekapcsolni, sőt a változást véglegesíteni is (Apply).



8.30 ÁBRA

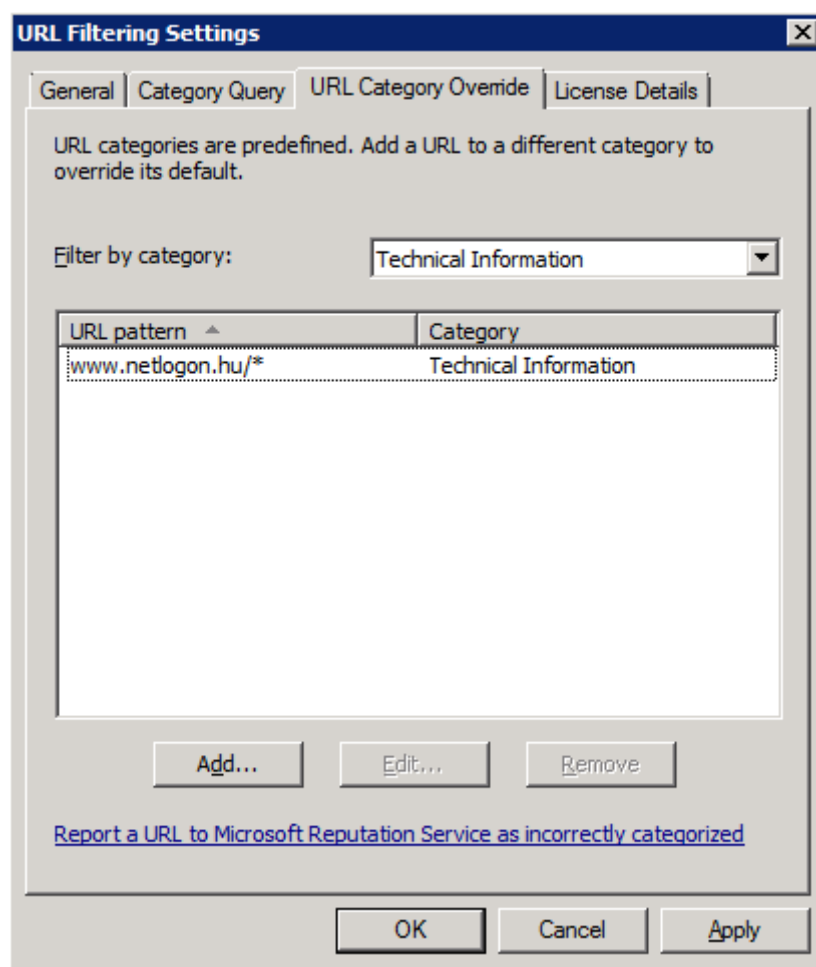
Ez a tesztelés az, ami elérhető a második, Category Query fül alatt. Nem fogja nagyon megdolgoztatni az agyunkat, de azért azt is tudnunk kell, hogy már ehhez is kell az érvényes (vagy a trial) licenz.

Ha viszont ezen a fülön a "Report to URL..." linket választjuk, akkor az MRS Feedback and Error Reporting (<https://www.microsoft.com/security/portal/mrs/default.aspx>) oldalra jutunk el, ahol egy űrlap formájában ugyanúgy lekérdezhethetünk, illetve javasolhatunk is oldalakat a megfelelő kategória megjelölésével. Bízgatunk is mindenkit arra, hogy használják ezt a lehetőséget.



8.31 ÁBRA

A következő fül alatt (URL Category Override) viszont direktben vehetünk fel kiegészítéseket egy-egy már létező kategóriába.



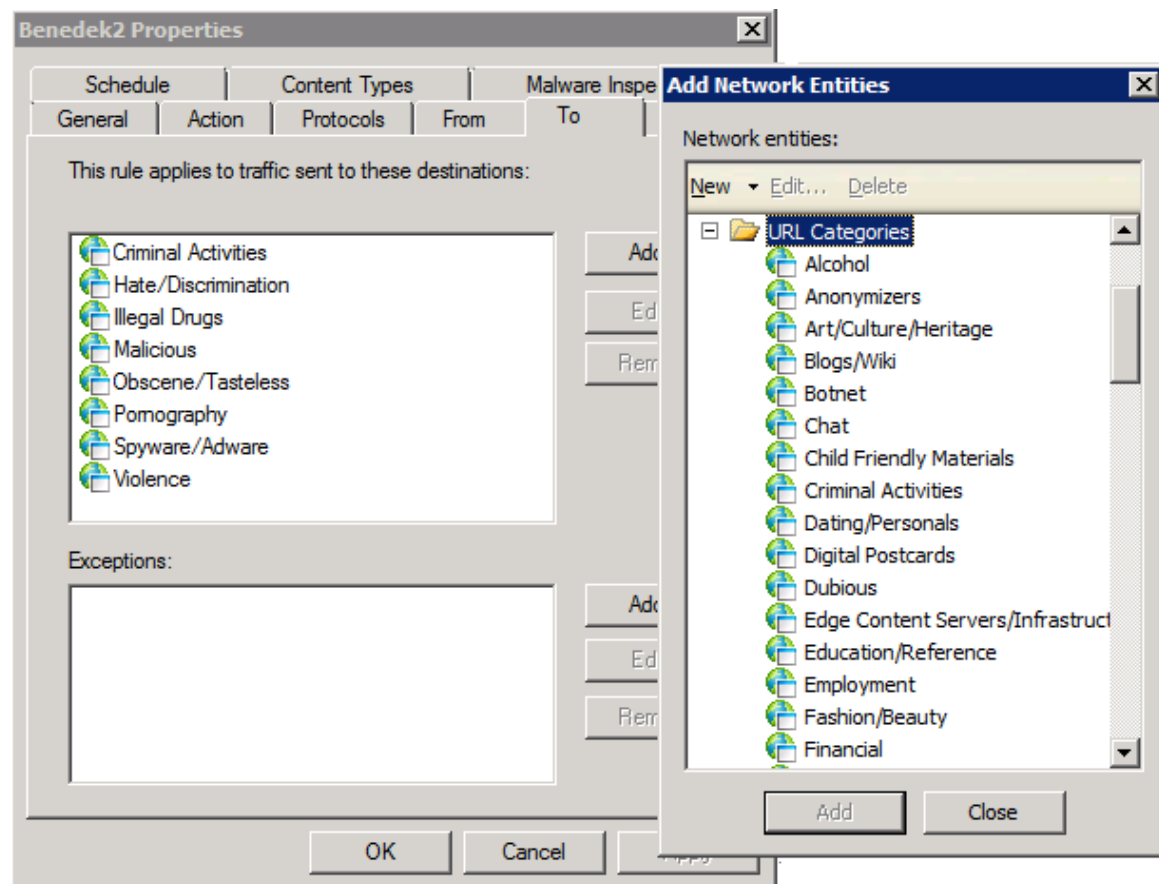
8.32 ÁBRA

Talán itt érdemes megemlíteni azt is, hogy az MRS adatbázis nem exkluzívan a TMG részére van. A Microsoft középtávú stratégiája szerint sok egyéb termék is használni fogja. Amiért ez fontos az az, hogy az MRS-ben már most sokkal több van, mint amit a TMG használ és ezzel a különbséggel mint gyakorló TMG üzemeltetők találkozni is fogunk. Ugyanis az MRS adatbázisban jelenleg egy URL akár öt kategóriába is tartozhat. Amikor a TMG elküldi a kérését az MRS adatbázis felé, akkor az MRS helyesen megválaszolja a kérdést és visszaküldi az összes kategóriát amibe az URL tartozik. Azonban a TMG, csak az első kategóriát fogja felhasználni. Tehát ha egy oldal a Technical Information és a Hacking / Criminal Activities kategóriába is tartozik és az elsőszámú kategória a Technical Information, akkor ebből lehetnek érdekes működések. Hiába tiltjuk a Hacking / Criminal Activities kategóriát, a TMG szerint az adott oldal a Technical Information-be tartozik. Ilyenkor csak a local override segít. Illetve a TMG termékfejlesztő csapat aktívan dolgozik ennek a kezelésén és várható hogy ez a viselkedési mód megváltozik. Addig is érdemes ezt szem előtt tartva tervezni és hibakeresni adott esetben a rendszerünket. *(A lektor megjegyzése.)*

Ami maradt az a licenz információk megtekintése, de ehhez már nincs kép, mert itt változtatásra amúgy sincs lehetőség, a licenz kulcs bevitele az EMP-nél már megismert módon, azzal együtt történik.

És most nézzük meg, hogy a szabályokba foglalás hogyan zajlik. Egy URL szűrő szabály készítésénél az első különbség az, hogy tipikusan tiltó (Deny) szabály készítünk. A második pedig az a protokoll HTTP/S kell, hogy legyen. A harmadik pedig az, hogy a célunk (To) az egy vagy több URL kategória lesz.

És itt jönnek be a képbe a csoportok. Ugyanis rendelkezünk 11 db előredefiniált csoporttal (URL Category Sets), amelyben már előzetesen beválogatták a 79 kategória összefüggő elemeit. Ezeken persze mi már nem változtathatunk, de tetszőleges számú új csoportot azért létrehozhatunk.



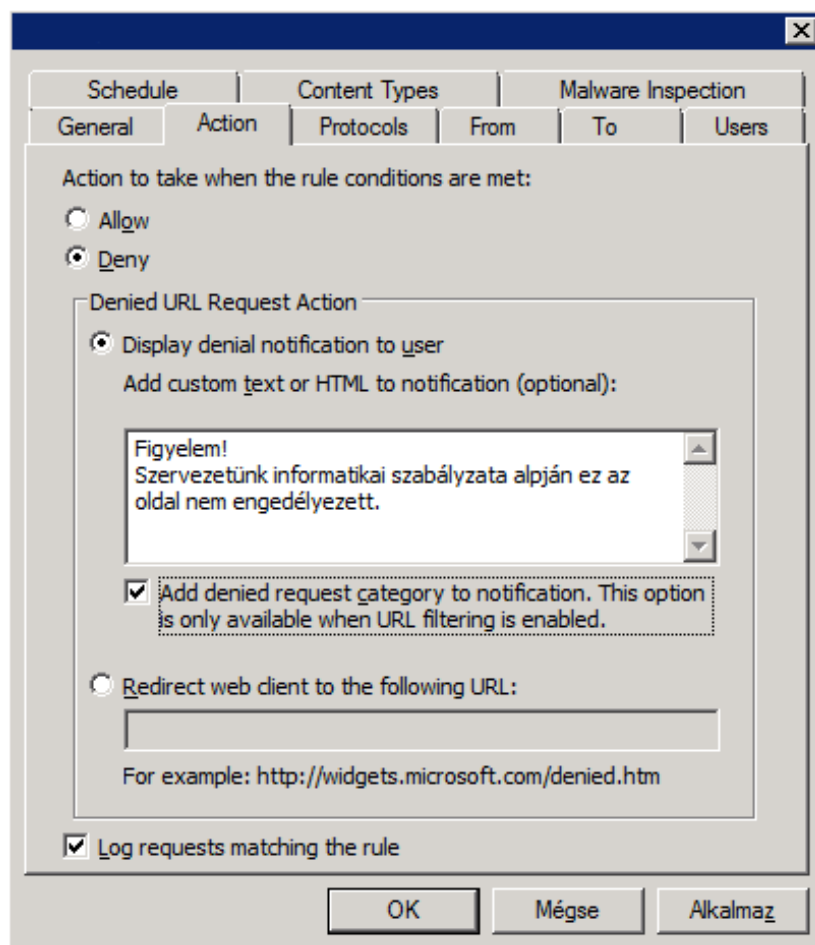
8.33 ÁBRA

Ezek alapján már könnyedén elkészíthető lesz egy-egy URL szűréssel rendelkező szabály, de van még egy rész, amely említést érdemel, és ez pedig a felhasználó számára az oldal helyett érkező hibaüzenetek konfigurálása.

A KAPUN TÚL

Ehhez az adott szabályban menjünk az Action földre, majd a "Denied URL Request Action" szakaszba, majd "Display Denial Notification To User" alatti mezőbe beírhatjuk a szépséges információ üzenetünket (lásd következő ábra).

Ugyanitt célszerű az "Add denied request category to notification..." opciót is bejelölni, ez amely hatására a felhasználó látni fogja, hogy mely kategóriába tartozik az az oldal amit blokkolunk.⁸¹

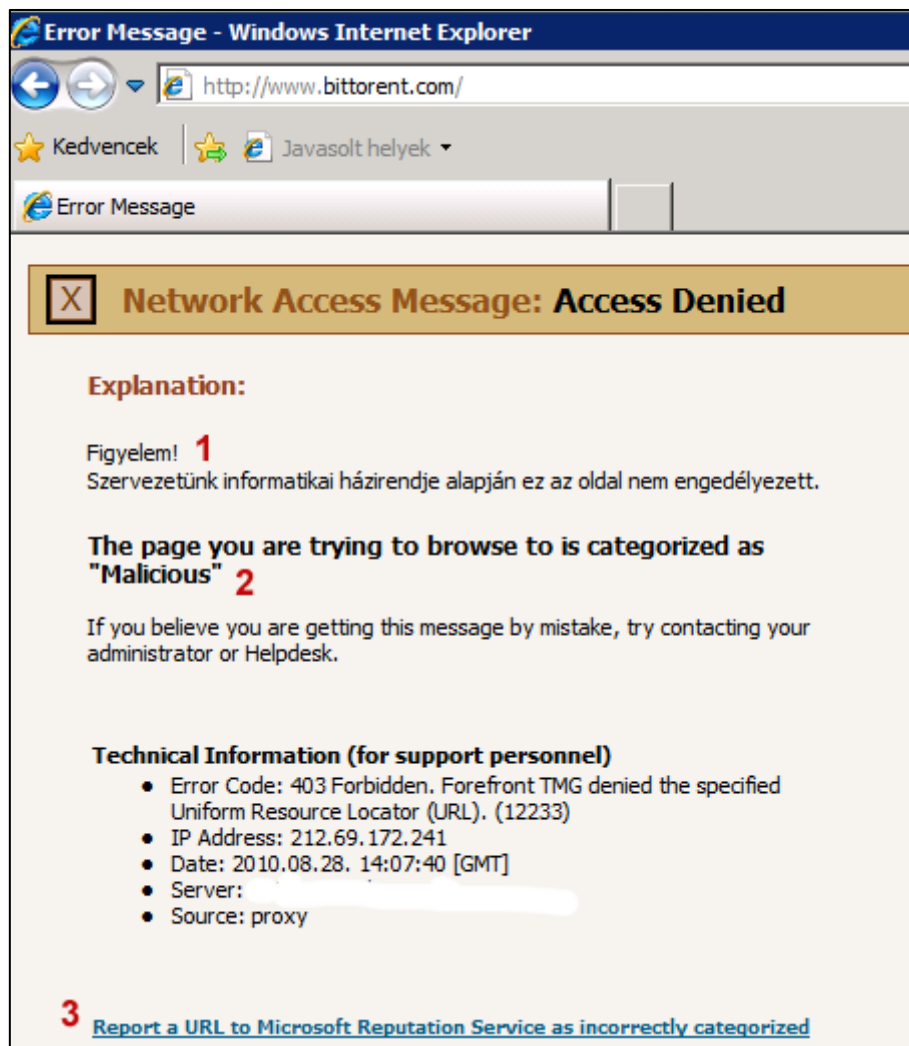


8.34 ÁBRA

Ez az üzenet ennél is jobban testreszabható, pl. olyan HTML kódokkal, amelyeket az oldalak <body> részében használhatunk. Viszont pl. nyelvi variációk nem játszanak, azaz maximum az a szöveg lehet magyar nyelvű, amelyet itt begépelünk.

És most nézzük meg a végeredményt, azaz azt a hibaüzenetet, amelyet a felhasználó kap ha netalántán rossz útra téved. (8.35 ábra).

⁸¹ Az átirányításra utaló legalsó opció ("Redirect web client...") általános a tiltó szabályoknál, az URL szűréshez nincs köze.



8.35 ÁBRA A VÉGEREDMÉNY

Némi magyarázat a számozáshoz:

1. Az általunk a szabályban begépelte hibaüzenet, itt pl. bármiféle formázás nélkül.
2. A kategória megnevezése (igen, a bittorent.com a Malicious kategóriában van)
3. Ugyanaz a riportolási lehetőség (MRS Feedback and Error Reporting), mint amelyről a már szó volt korábban.

Ezzel egy igen-igen tartalmas rész végére értünk, amely tele volt újdonsággal, valamint pl. a HTTP filter vagy a HTTPS Inspection kapcsán talán némiképp nehezebben emészthető, ám rendkívül fontos tartalommal is. Valamint ezzel észrevétlenül be is fejeztük azt a több, nagy fejezetből álló részt is, amelyekben elsősorban a klienseink hozzáférését és védelmét szabályoztuk. Ami most jön az pontosan a fordítottja lesz az eddigieknek: megvizsgáljuk azt, hogy kívülről kit és hogyan engedünk hozzá a belső hálózat erőforrásaihoz.

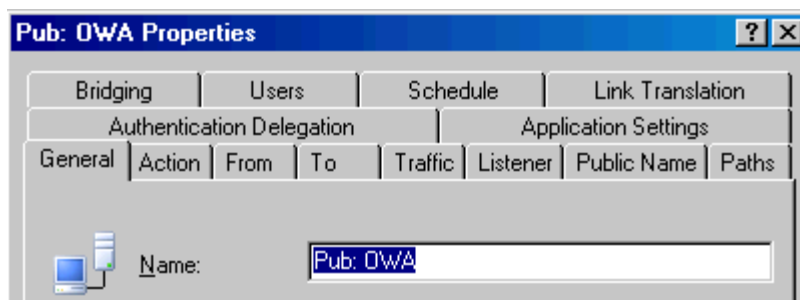
9 KIT ÉS HOGYAN ENGEDÜNK BE?

Most sok-sok oldalon keresztül tipikusan arról a folyamatról lesz szó, amely során a TMG kiszolgáló beépített eszközeivel a védett belső, vagy az elkülönített Perimeter (DMZ) hálózat különböző szervereinek szolgáltatásait elérhetővé tesszük az internet vagy egy másik hálózat felé.

A „tipikusan” kifejezés nem véletlen, hiszen ugyanezzel a módszerrel természetesen a belső kiszolgálókat is publikálhatjuk a belső hálózat ügyfelei számára is, csak nem ez a „tipikus”. Pedig nincs ennek túl sok akadálya, és igazán van értelme is, hiszen miért is van alapértelmezés szerint mindenkinek aki csak fellép a hálózatunkra (akárcsak egyszer is, mondjuk a laptopjával egy másik cégtől egy tárgyalás során) jogosultsága a például a webszerverekhez, a SharePoint kiszolgálókhoz, stb.? Jó kérdés, de most mégsem ez a lényeg, egyelőre maradunk a publikálás hagyományos eseténél.

Két csoportba oszthatjuk a szerver publikálás „alanyait”, először egy kicsit kevesebbet fogunk beszélni az egyszerűbb, szimpla szerver publikálásról, majd ezután sokkal több szó esik majd a webszerver publikálásról (HTTP/S). A különbség valóban számottevő, egy Windows hálózatban rettentő sok és fontos webszerverre épülő szolgáltatás van, amelyeket értelemszerűen a hálózaton kívülről is el szeretnénk érni. Melyek ezek?

- Maga a webszerver (például az IIS), statikus vagy dinamikus oldalakkal és az egyéb, akár speciális, webes célalkalmazásokkal együtt.
- Az Exchange szerverek webszerverre épülő szolgáltatásai (például az OWA, az OA, az ECP és még az ActiveSync).
- SharePoint/MOSS kiszolgálók

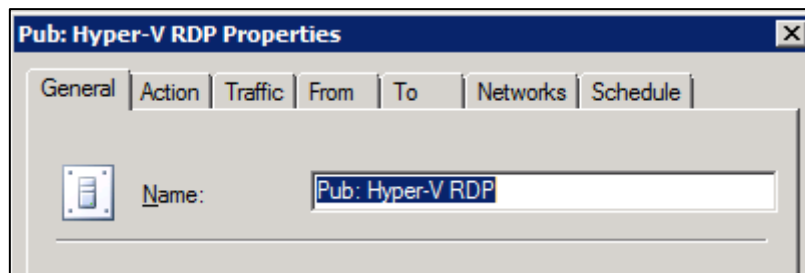


9.1 ÁBRA SOK EXTRA OPCIÓ – WEBSZERVER PUBLIKÁLÁS

Könnyen belátható tehát, hogy a webszerver publikálás valóban jelentős területet fed le egy Windows alapú hálózat üzemeltetési feladatain belül, nem véletlen tehát az hogy a TMG is jóval több publikálási lehetőséggel, választható bővítménnyel kecsegteti az

üzemeltetőket. A felsorolás helyett nézzük meg az előző ábrát az elérhető beállításokról és szolgáltatásokról (később persze részletesen ki is vesézzük ezeket).

E felosztás szerint a másik csoportba tartozik a szimpla szerver publikálás, amit a legkönnyebben talán úgy tudunk meghatározni, hogy minden ami nem webszerver publikálás. Persze az így közzétett kiszolgálók, szolgáltatások száma is lehet jelentős a helyi igények függvényében, viszont a konfigurálási lehetőségek száma mindenképpen kevesebb, ahogyan az alábbi képen ez szépen látható is.



9.2 ÁBRA KEVÉS EXTRA, DE SOKFÉLE TÍPUS – SZIMPLA SZERVER PUBLIKÁLÁS

Még két fontos, és inkább technikai különbség is van a két típus között. Először is a webszerver publikálás kizárólagosan a web proxy filtertől függ, míg a szerver publikálás a maradék (nem webes, FTP, PPTP, streaming, stb.) alkalmazásfiltereket használhatja csak. A másik alapvető különbség pedig az, hogy szimpla szerver publikáló szabályok a bejövő (incoming) értelmezésben használják a protokollokat, míg a hozzáférési és web publikáló tűzfalszabályoknál ez a kimenő (outbound) irányt jelent.

9.1 A SZIMPLA SZERVER PUBLIKÁLÁS

Tisztázzuk az elején, csak én használom a "szimpla" kifejezést, egyébként a terminológia szerint "szerver publikálásnak" hívjuk ezt a típust.

Egy szerver publikáló tűzfalszabály a kliens kérésének az adott protokollon történő továbbítását jelenti. A TMG egy IP:port párost (socket) rendel össze a saját külső lábától a publikált belső szerver szintén IP:port párosáig. Így aztán ha kívülről e portra érkezik egy kérés, már mehet is befelé, a megfelelő szerver megfelelő portjára.

Nos, ez egy újabb különbség a két publikálási típus között: míg a webszervernél lehet hogy csak egy virtuális mappát publikálunk, addig itt a teljes portra irányuló forgalmat "beküldjük". Még egy tudnivaló: még ha route-olás is van beállítva a TMG és adott hálózat között, a szerver publikálás során a mindig NAT-olva lesz, de ennek két típusa is van, amelyet majd szabályszinten definiálhatunk (lásd később: Requests for the published server).

A belső erőforrások ilyen módon működő publikálása a TMG részéről a következő támogatásban részesül:

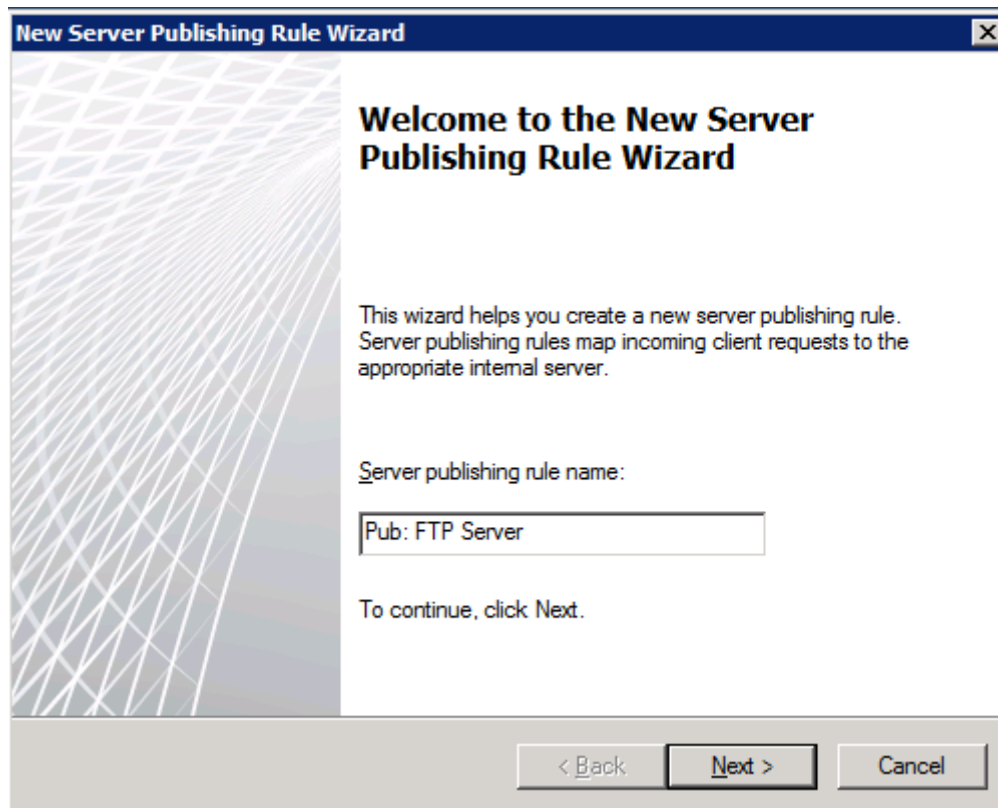
- Többszörös protokoll használat: Egyrészt rengeteg előredefiniált TCP és UDP protokoll elérhető (míg a webesnél összesen 2 darab), másrészt mi magunk is készíthetünk (és sokszor muszáj is) egyéni protokollokat, amelyeket aztán majd egyszerűen fel tudunk használni a szerver publikáló szabályokban. Egy a lényeg: az irány mindig csak a bejövő lehet (erre figyelmeztet is a TMG egyébként).
- A alkalmazási rétegben történő szűrés: Gyárilag 13⁸² db alkalmazásszűrő használható a szerverpublikáló szabályokban (nézzünk vissza az 5.4 ábrára). Ezeket többségében alig konfigurálhatjuk, nem is kell, egy POP filterben már benne van az ismert POP3-mal kapcsolatos támadási formák elhárítása. Míg másoknál, pl. az FTP filternél a hangsúlyt pl. az aktív illetve főképp a bonyolultabb portokat és csatornákat variáló passzív FTP elérés megsegítése van beépítve a szűrőbe.
- A titkosítás támogatása: Itt arra gondolunk, hogy a szerver publikálásban használhatjuk az egyes protokollok titkosított változatát is, pl. SMTPS, POP3, IMAPS, stb. A TMG képes továbbítani a titkosított adatforgalmat a kliens és a szerver között, de ezek esetében nincs Bridging, vagyis a tűzfal számára ez transzparens forgalom.
- IP cím naplózás: Amikor publikálunk egy belső szervert, akkor elvileg ez a szerver naplózza pl. a hozzáférő kliens IP-jét. De ha mindez egy ISA vagy TMG mögött történik, akkor a belső szerver (és a kliens is) mindig csak a "köztes elemmel" van kapcsolatban, azaz pl. a TMG személyesíti meg mindkét fél számára a másikat. Épp ezért egy belső szerver naplójában ebben az esetben mindig csak az TMG IP-je jelenne meg, hiszen mindig ez a gép a kliens. De kérhetjük, hogy ez ne így legyen, a szerver publikálásban is van lehetőség az eredeti IP továbbküldésére is a belső szerver felé.

9.1.1 EGY PÉLDA: FTP SZERVER KÖZZÉTÉTEL

A feladat egyszerű, a belső hálón már működő IIS7.5 (pontosabban FTP 7.5, mivel egy ideje ugye külön is letölthető) publikálása a nagyvilágba.

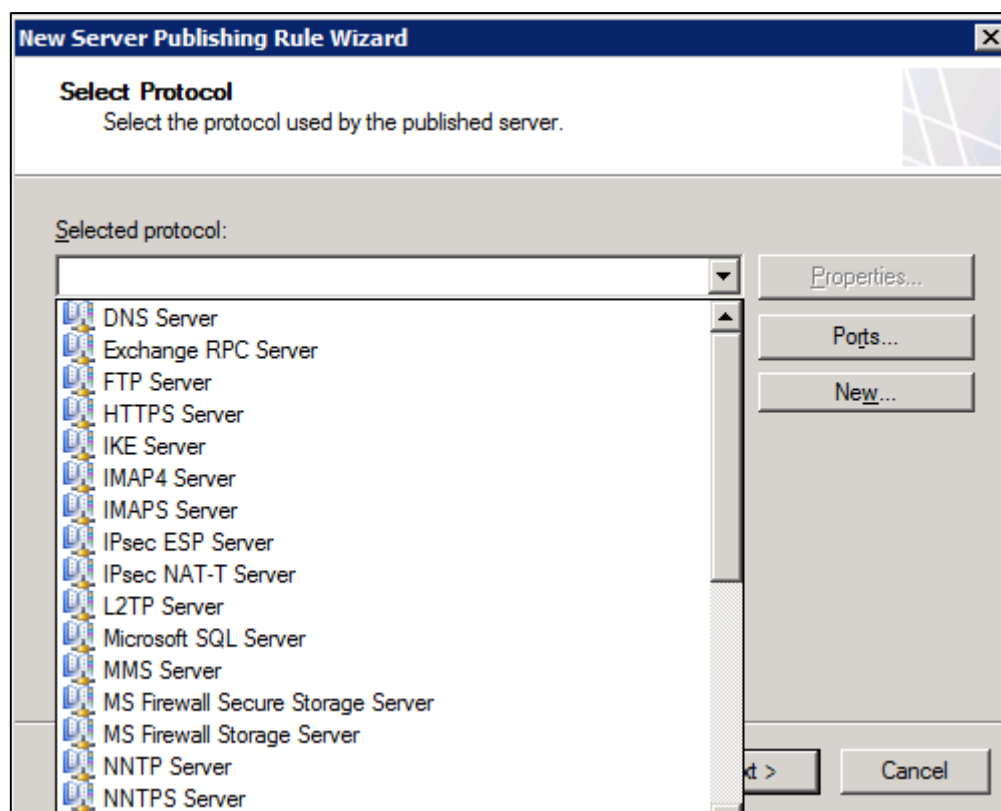
Ehhez induljunk el a Firewall Policy\Tasks\Publish Non-Web Server Protocols pontból.

⁸² Valójában 14 van a képen, de a web proxy filtert nem számoljuk ide.



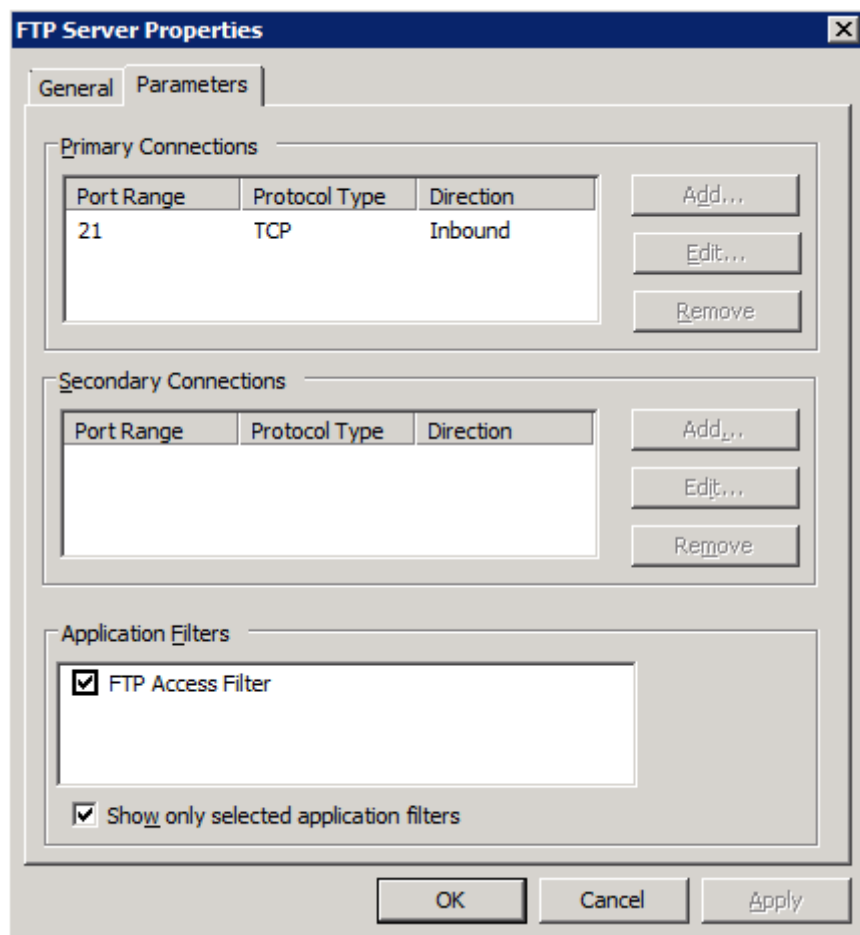
9.3 ÁBRA BÁRMIT ÍRHATUNK BELE, DE ÉN A PUB: RÉSSZEL JELÖLÖM A PUBLIKÁLÓ SZABÁLYOKAT MINDIG

A következő panelen a belső szerver IP címét kell megadnunk, mást nem is tehetünk.



9.4 ÁBRA A VÁLASZTÉK

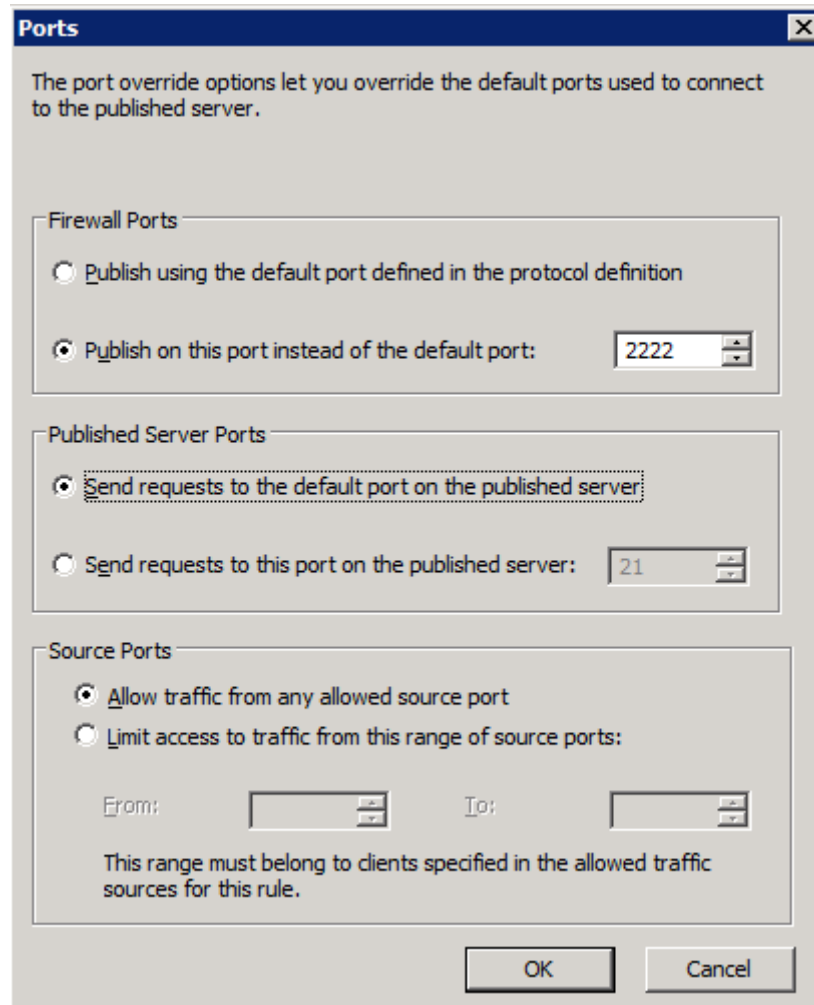
Ezután viszont kicsit komplikáltabbá válik a helyzet. Ki kell választanunk az előredefiniált szervertípusok közül a megfelelőt, azaz a mi esetünkben az FTP Server-t. Ezután megtekinthetjük ennek a tulajdonságait, sőt itt a paraméterek alatt a gyárilag definiált portot és (ha van) a megfelelő alkalmazásszűrőt is.



9.5 ÁBRA ELSŐDLEGES ÉS MÁSODLAGOS PROTOKOLLOK ÉS A SZŰRŐ(K)

Ha visszamegyünk az előző ábrához akkor a "Ports" gomb is érdekes lehet, hiszen ez alatt tudjuk a belső és külső portokat variálni.

Az ábrán nem véletlen az első port szám. Az FTP alapesetben a TCP 21-es porton figyel, de tegyük fel, hogy nekem ezen a TMG-n keresztül már van egy FTP szerver publikálva, ami egy másik belső gépre mutat. Ezért egy másik portot választottam, ami egyben azt is jelenti, hogy a külső kliensnek is majd így ezt kell beírni az FTP kliens programban. A belső port viszont változatlan, mivel ezen a belső szerveren nem fut másik FTP szerver szolgáltatás (ha ott is más a port, mint az alapértelmezett, akkor viszont itt is változtatni kell). Legalul még a dinamikus forrás (vagy helyi) portokat is korlátozhatnám, de most ezt nem tesszük.

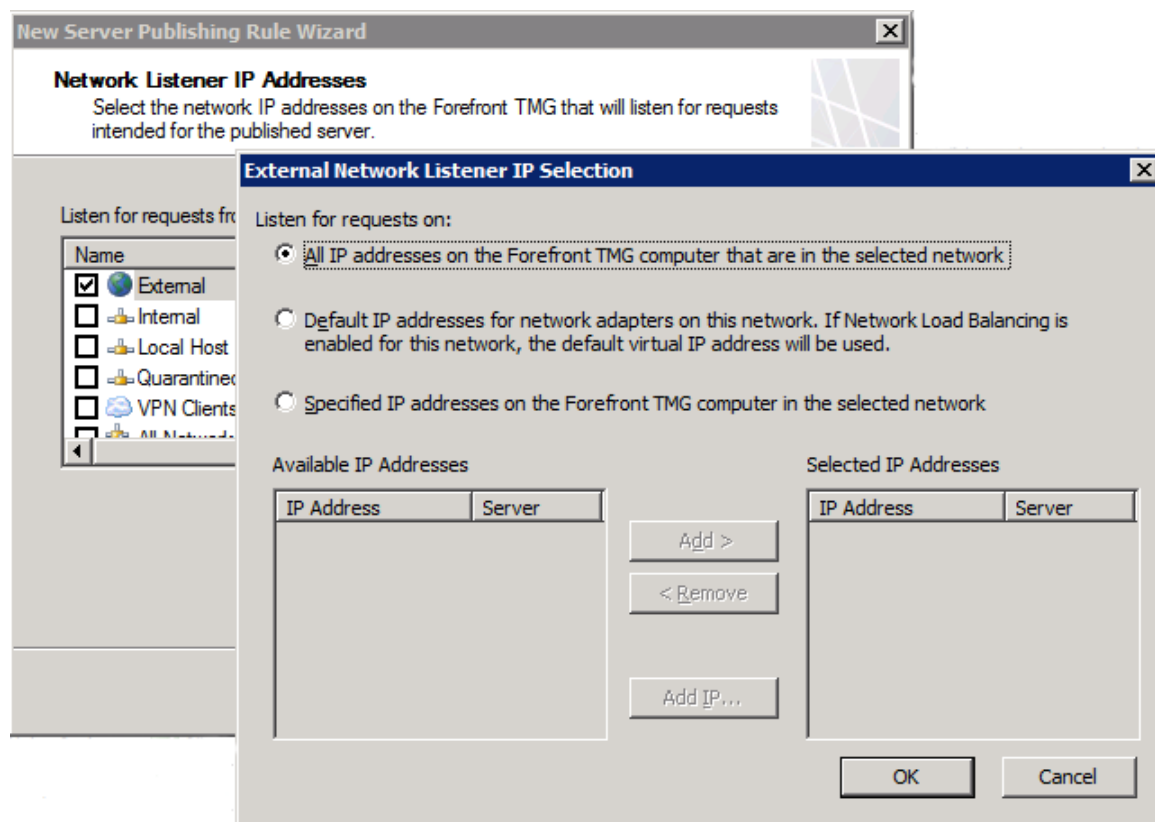


9.6 ÁBRA PORTVARIA

Hadd említsek meg egy másik hasznos trükköt is ezzel kapcsolatban. Ha a belső gépeket (tipikusan a szervereket) szeretném VPN nélkül RDP-vel elérni, akkor alapesetben a tűzfalam RDP portjára be tudok menni, de tovább értelemszerűen nem. Ellenben ha készítek egy-egy RDP publikáló szabályt a belső szerverek IP-jével, és egy másik, nem használt TCP porttal (legyen mondjuk most a TCP10000), amit itt beállítok a "Firewall ports" alatt, akkor kívülről a tuzfalgep.cegnev.hu:10000-ra kapcsolódva a belső szervert érem el az RDP kliensemben. Persze ezzel nyitottam egy portot a tűzfalban, ami nem biztos hogy kívánatos, viszont működik.

Ha megint csak visszanezünk a 9.4 ábrára, akkor azt látjuk, hogy eddig kimaradt a "New..." gomb, amely alatt viszont egy új portot létrehozva egy speciális porton működő szervert tudok majd publikálni.

Most erre nincs szükség, az FTP Server nekünk jó, ergo menjünk tovább. A következő lépésben ki kell választanunk, hogy mely hálózatokhoz és esetleg azon belül mely IP-hez legyen hozzárendelve a publikálás.



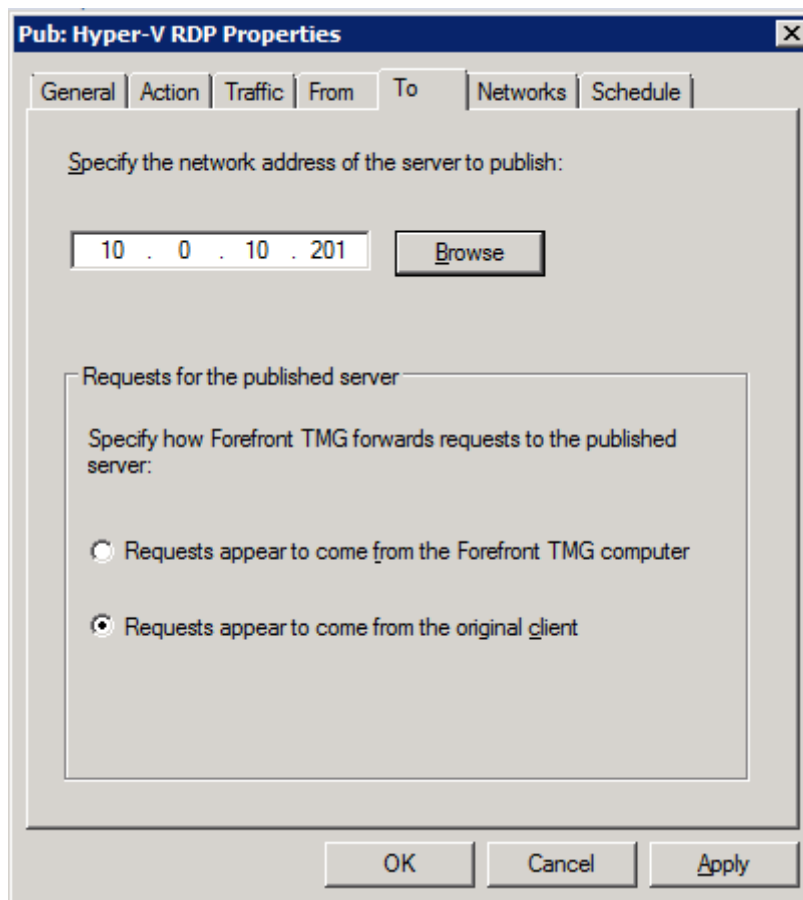
9.7 ÁBRA PORTVÁRIA

A három lehetőség közül a két alsónak csak akkor van értelme, ha több IP-nk van. Ha 1 db van, akkor viszont teljesen mindegy, hogy az első kettő közül melyiket választjuk. Ellenben ha több IP-nk van, akkor mindenképpen komolyan fontoljuk meg hogy melyiket választjuk a háromból. Az első esetén mindegyiken működik majd, ami pl. egy nem megfelelő DNS beállítás esetén problémás lesz. A középső lehetőség az alapértelmezett (NLB-nél is) IP választása, míg a harmadiknál konkrétan ki kell választanunk egyet, de hogy még jobban zavaros legyen, lehet többet is.

Ha csak egy IP-nk van, akkor semmiképp ne variáljunk, jó lesz az első opció, vagy esetleg úgy járunk mint a szerző, aki egy publikus IP váltáskor 2 órát konfigurált, miután beindította az SMTP szerver forgalmát egy korábbi idióta miatt, aki beírkálta az egyetlen publikus IP-t minden szabályba ☺

Nos, ha a "Network Listener IP Addresses ablakban" választottunk, jelen esetben pl. az External hálózatot, akkor már csak egy összegző képernyő jön és már készen is vagyunk. Ha érvényesítünk az FTP szerverünk már él is, kívülről is. De van még három

dolog, amelyet meg szeretnék említeni a már kész publikáló szabályban a teljesség igénye miatt, viszont egyetlen ábrán belül.



9.8 ÁBRA MILYEN IP-T KÜLDJÜNK TOVÁBB?

A "Requests for the published server" rész az érdekes, és nemcsak a korábban említett naplózás miatt. Ha itt meghagyjuk az alapértelmezett alsó opciót, akkor a naplózás nem szenved majd csorbát, mert egyúttal itt válik el a korábban már említett „*mindig NAT-olás*” útja, egyrészt az ún. half-NAT típusra (a forrás, mindig az eredeti IP), és full NAT-ra (ez a TMG módszere, amikor a routing topológia is egyszerűbb, mert a válasz garantáltan a TMG-nek fog visszamenni, tehát akár lehet más alapértelmezett átjárója a publikált kiszolgálónak). A fűlek közül a "From" további hely szerinti korlátozást jelent, a "Schedule" pedig időzíthetővé teszi a publikáló szerver elérhetőségét.

És most térjünk át a nagyobb falatra, azaz a webszerver publikálásra.

9.2 A WEBSZERVER PUBLIKÁLÁS

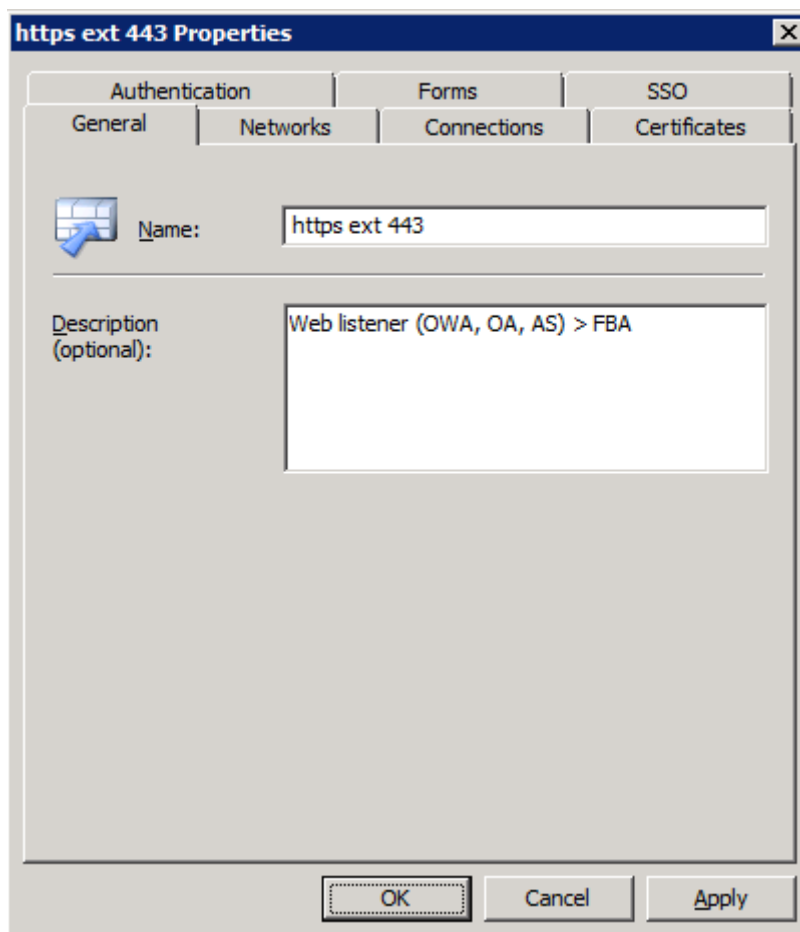
Amikor 2006 szeptemberében megjelent az ISA kiszolgálók harmadik generációs képviselője, az ISA Server 2006, akkor első ránézésre drasztikus változást nem láttunk az előző verzióhoz képest, de ha kicsit alaposabban megvizsgáltuk, akkor azért több

fontos, hasznos és nagyléptékű újítást is felfedezhetünk. Az újdonságok nagyon nagy százaléka a webszerver publikálás témakörét érintette, drasztikusan megnövelve a lehetőségeinket. A TMG-ben viszont ezen a területen nagyon sok változás nem történt, úgyhogy ez a rész a még ISA rendszergazdák számára is teljesen releváns lesz. A következő három szakasz első két részében sorra vesszük a lehetőségeket, majd a harmadikban egy SSL-el működő webszerver publikálást fogunk végrehajtani, lépésről-lépésre.

9.2.1 EGY NAGY FALAT: A WEB LISTENER

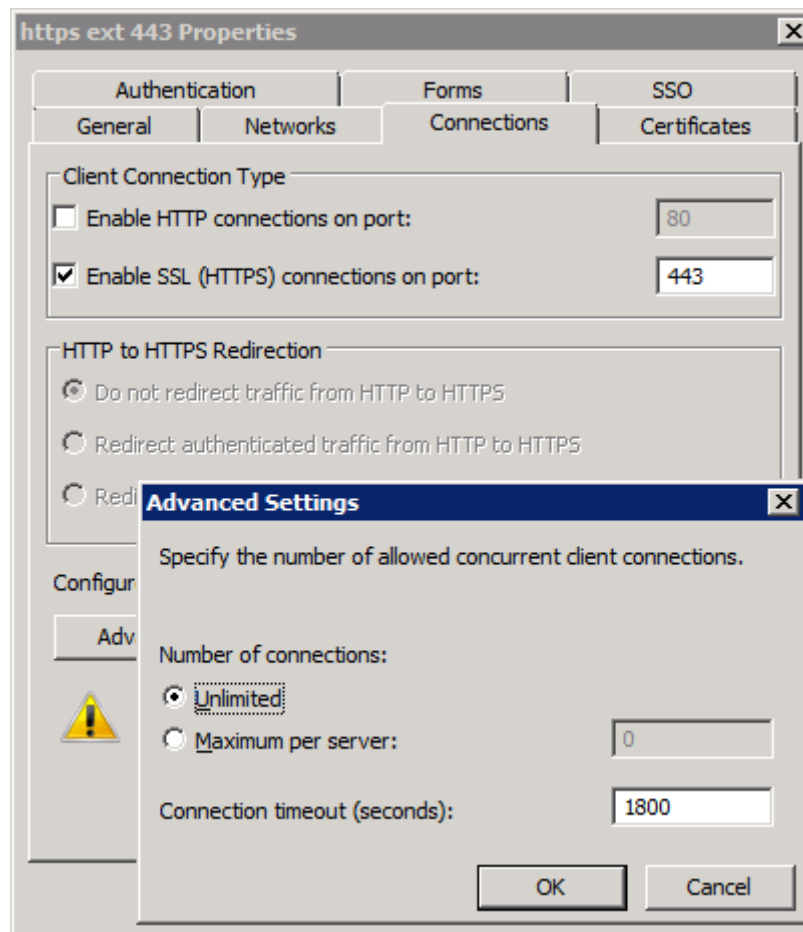
Ezt a témakört muszáj kiemelni egy külön és szélesebb áttekintésre, mert annak ellenére, hogy csak egyetlen fül egy webszerver publikálási szabályban azért igen bonyolult és félelmetesen granuláris. A web listener-ről már többször szó esett, legutoljára a proxy szerver és a HTTP filter kapcsán, idézzük csak fel:

*"A harmadik eset a **web listener**-eké, amelyek a publikáló tűzfalszabályokban használatosak (ez ugye a bejövő forgalom a szervereink felé), kötelező jelleggel. Ekkor a kérés útja szintén a Firewall szervíznél kezdődik, és a web listener-eren keresztül a web proxy motorhoz vezet, és ugyanúgy az alkalmazásszűrők hatása is érvényesül rajtuk."*



Szóval ha szeretnénk közzétenni egy belső webszervert, akkor a feladat azzal kezdődik, hogy le kell gyártanunk egy megfelelő "fület" hozzá a TMG-n, azért hogy "meghallja" ha majd valaki keresi. Ez az a komponens, amellyel a külső felhasználó először találkozik, amikor mondjuk a vonatkozó publikáló szabály alapján böngészni próbálja a belső webszerverünket. Ha még nem nincs web listener-ünk, akkor a publikáló szabály varázslása közben is létrehozhatjuk ezt egy külön varázslóval, de lehet a szabálytól függetlenül teljesen külön is. Mi most egy már kész listener beállításait nézzük végig, ugyanis ebben már minden lehetőséget látunk, míg a varázslónál csak a létfontosságúakat.

Ha az előző ábrát megnézzük alaposan, akkor láthatjuk, hogy ezen belül az első fül (General) csak informális, a második (Networks), arra a célra szolgál, hogy kiválasszuk azt a hálózatot, ahol ez a fülünk figyelni fog (ez más ismerős lesz a szimpla szerver publikálásból), de a harmadik, azaz a "Connections" már újdonság.

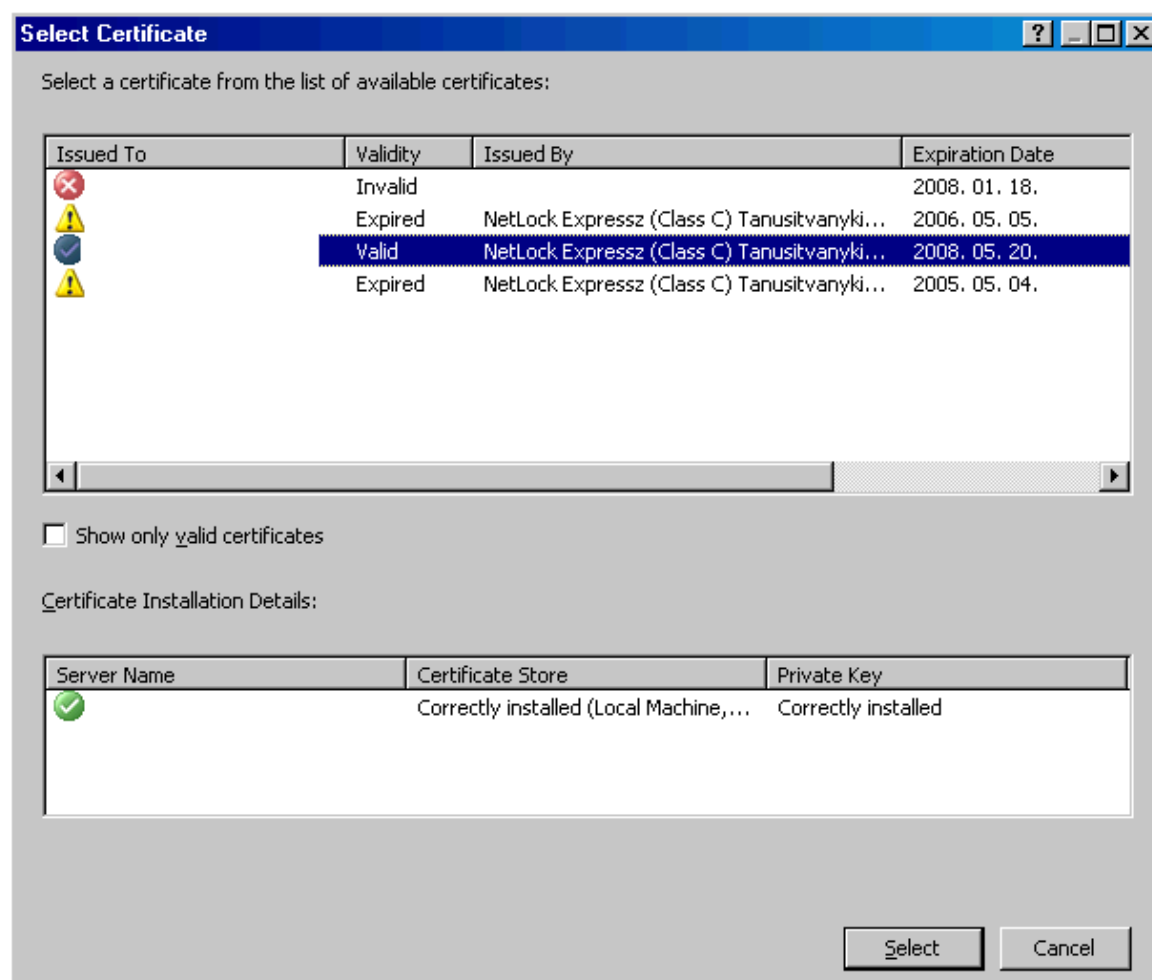


9.10 ÁBRA AZ ADVANCED GOMB KINYITVA A JOBB ALSÓ RÉSZBEN

A KAPUN TÚL

Itt először is definiáljuk, hogy HTTP avagy HTTPS lesz majd a listener érvényességi területe, illetve ha esetleg mindkettő (ezt szinte sosem így használjuk), akkor mi legyen az átirányítási opciókkal. Az ábrán kiemelt haladó beállításoknál mindkét lehetőség fontos, hiszen a kapcsolatok korlátja illetve az időtúllépés is lényeges lehet egy adott helyzetben (erről már szintén volt szó korábban, igaz a proxy szerver kapcsán).

Ezután átjutunk a "Certificates" szakaszra, ami anno az ISA 2006-ban szintén sokat változott, és mondhatjuk igazán kellemes újdonság volt. Korábban ugyanis a szükséges tanúsítvány kiválasztása bármilyen probléma esetén egy kissé rémálom volt. Nem kaptunk semmilyen információt a rendszerben lévő tanúsítványok lehetséges problémáiról, csak egy ronda, piros keresztes, legorombító üzenet érkezett. Most viszont egy külön ablakban, áttekinthető módon kapjuk az információt, ergo könnyebb kitalálni mi a probléma ezen a ponton. A következő ábra tartalmát a "Select Certificate..." gomb alatt találjuk.



9.11 ÁBRA TANÚSÍTVÁNY-KEZELÉS TMG MÓDRA (A KÉP HIÁNYOS, PÁR ADATOT KIRADÍROZTAM)

A megfelelő tanúsítvány kiválasztása a megfelelő előkészületek után nem lesz nehéz, azonban ehhez gondoskodnunk kell arról, hogy:

- Legyen egy megfelelő külső (pl. Netlock, Verisign, stb.) vagy belső tanúsítványkiadótól (ha egy saját Windows szervert alkalmazunk tanúsítványkiadóként) származó tanúsítvány, amelynek a "Common Name" mezője ugyanaz legyen mint amellyel majd publikálni fogjuk, azaz amellyel majd elérhető lesz kívülről.⁸³
- A TMG gép megfelelő tanúsítvány tárolójában legyen (azaz a helyi számítógép tárolójában).
- A tanúsítvány kiadójának a tanúsítványa szintén szerepeljen a helyi gép Trusted Root Certificate Authorities tárolójában.
- Csak olyan tanúsítvány jöhet szóba, amelyben a privát kulcs is benne van, azaz az előzetes exportnál vagy az igénylésnél erre oda kell figyelni.
- A CDP (CRL Distribution Point) és az AIA (Authority Information Access) mezők tartalma is lényeges lehet⁸⁴, mivel ezek az adott tanúsítványkiadó visszavonási listájának elérési útjait tartalmazzák. Ha vásárolunk egy tanúsítványt, akkor ezzel nem lesz gond, ha sajátunk van, akkor viszont a pontos, és élő elérési út megadására még az első tanúsítványok igénylése előtt, azaz a CA indító konfigurálása közben kell nagyon odafigyelni.

Ha nemcsak egy külső IP-vel rendelkezünk, akkor ugyanitt akár IP-nként külön-külön tanúsítványt is megadhatunk, de ehhez előzetesen a Networks fülön is külön-külön meg kell adnunk az IP-ket.

És most az amúgy is bonyolult listener konfigon belül, egy ritka összetett részhez értünk, jöjjön az "Authentication" azaz a hitelesítés szakasz. Kezdeként nézzük meg azt, hogy a webszerver hitelesítési procedura milyen fő szakaszokra osztható:

- A kliens jogosultságainak elfogadása.
- A jogosultságok érvényesítése, amelyhez egy hitelesítés szolgáltató szükséges (pl. Active Directory, RADIUS, SecurID),
- A hitelesítési adatok delegálása egy a TMG „mögött” működő szerver (pl. egy SharePoint) közreműködésével.

Az első két komponenst az adott listener segítségével konfiguráljuk, míg a harmadikat majd a vonatkozó publikáló szabályban (lásd a 9.2.3 alfejezetben). Ez egyúttal azt is jelenti, hogy ugyanazt a listener-t természetesen használhatjuk majd több publikáló

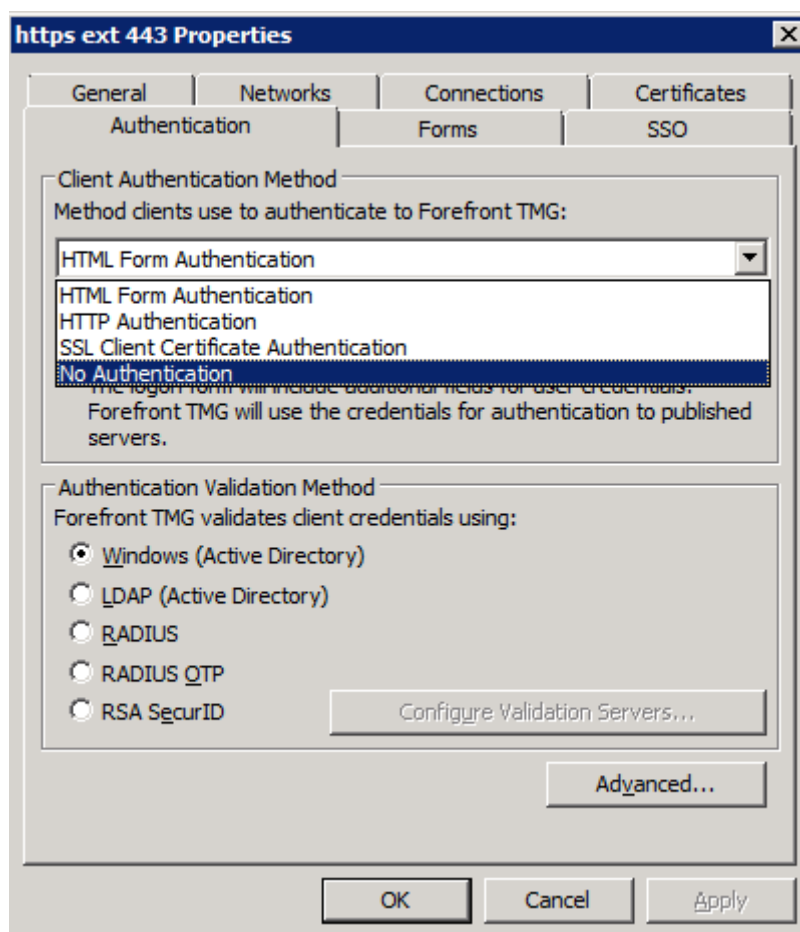
⁸³ És persze például egy Exchange publikálás esetén mindenképpen oda kell figyelni az adott tanúsítvány alternatív neveinek tartalmára is, azaz amikor egy SAN (Subject Alternate Name) tanúsítványt kell használnunk, akkor a megfelelő plusz neveknek is benn kell lennie a tanúsítványban.

⁸⁴ Példának okáért a TMG is ellenőrizheti ezeket, lásd HTTPS Inspection.

A KAPUN TÚL

szabályhoz is (lásd a 9.9 ábrát), sőt esetenként változó delegálási típusokkal is. Ezek után viszont tekintsük át csoportokba szedve az összes, a TMG-ben megtalálható hitelesítési technológiát és módszert.

- 1) Nincs hitelesítés
- 2) HTML űrlap alapú kliens hitelesítési módszer
 - a) Windows (Active Directory)
 - b) LDAP (Active Directory)
 - c) RADIUS
 - d) RADIUS OTP
 - e) RSA SecureID
- 3) HTTP alapú kliens hitelesítési módszer
 - a) Basic
 - b) Digest / wDigest
 - c) Integrated
- 4) SSL kliens tanúsítványon alapuló hitelesítés



9.12 ÁBRA A HITELESÍTÉSI METÓDUSOK

Ezek közül a "Nincs hitelesítés" nem vicc, nem mindig van szükség hitelesítésre, viszont a 3.⁸⁵ és a 4. pont módszereit a web proxy hitelesítésnél már kiveséztük⁸⁶, ergo jöjjön a kakukktójs, azaz a második metódus.

Az űrlap alapú hitelesítés (Forms-Based Authentication)

Egyre több olyan webes alkalmazás, szolgáltatás jelenik az intranet/internet/extranet hálózatokban, amelyet miatt biztonságos, részletesen szabályozható és testreszabható hitelesítési formákat kell(ene) alkalmazni. Az intranet szó nem elírás, tényleg komolyan el kell gondolkoznunk azon, hogy a belső felhasználók valamint a vezetékes vagy vezeték nélküli „alkalmi” kapcsolódók (szállítók, vendégek, ügyfelek, a laptopokkal, dpa-kkal, stb.) azonosítás és hitelesítés nélkül érthessék-e el a belső hálózat eddig semmilyen módon nem korlátozott erőforrásait (webszerverek, portálok, stb.).

Az ilyen típusú igények megjelenése miatt a TMG-ben gyakorlatilag bármilyen webszerver publikálásánál használhatjuk az FB A-t, három fő csoportba osztva:

- Jelszó űrlap: felhasználónév/jelszó, az Active Directory, az LDAP, és a RADIUS jogosultságok ellenőrzésére.
- Passcode űrlap: felhasználónév/passcode, a SecureID és a RADIUS hitelesítésnél.
- Passcode/jelszó űrlap: felhasználónév/passcode a hitelesítésre ÉS felhasználónév/jelszó a delegálás céljából.

Az űrlapos hitelesítés további újdonságai közül az egyik legfontosabb a jelszókezelés. Ez azt jelenti, hogy újra van⁸⁷ lehetőségünk a felhasználók számára megengedni, hogy akár távolból is megváltoztassák a jelszavukat, valamint azt is elérhetjük, hogy az általunk beállított időhatáron belül a jelszóváltoztatás szükségességéről értesítést (és ennek apropóján rögvést egy jelszóváltoztató űrlapot is) kapjanak. A két opció nem szükségszerűen jár együtt, szerencsére külön-külön is szabályozhatóak.

További megjegyzések és tudnivalók az űrlap alapú hitelesítésről

- A TMG (és az ISA is) képes ezt a hitelesítési formát a mobil kliensek számára is nyújtani, persze csak akkor ha a mobil eszközről beérkező kérés User-Agent fejléce alapján megfelelően detektálta a klienst. Az ide tartozó űrlapok az TMG telepítési mappájának Templates\CookieAuthTemplates\ISA mappájában találhatóak meg.

⁸⁵ Itt maximum azt érdemes még megjegyezni, hogy ha ezt a módszer választjuk, akkor az Advanced alatt a „Allow client authentication over HTTP” pipát mindenképpen be kell kattintani.

⁸⁶ Az SSL kliens hitelesítésnél van fallback, azaz tartalék megoldás, méghozzá több is: a Basic, a Digest és az Integrated.

⁸⁷ Mert volt régebben is, pl. az Exchange-nél.

9.13 ÁBRA EGY SZIMPLA WEBOLDALHOZ TARTOZÓ HITELESÍTÉS JELSZÓ VÁLTOZTATÁSI KÉRÉSSSEL

- Közvetlenül ide tartozik az is, hogy a szimpla HTML űrlapok is teljesen testreszabhatóak, a telepítési mappa `CookieAuthTemplates\HTML` könyvtárában találunk meg ehhez mindent, pl. az összes szöveges részt a `Strings.txt`-ben.
- A TMG 26 különféle nyelven képes ezeket az űrlapokat megjeleníteni, szintén egy vizsgálat, azaz a böngésző nyelvi beállításai alapján. Természetesen ettől eltérő beállítást is megtehetünk a publikáló szabályn belül (`Listener/Properties/Forms`), azaz elképzelhető olyan felállítás is, hogy más lesz az űrlap és más a böngésző nyelve.

A multifaktoros hitelesítésről

Teljesen egyértelmű, hogy a hitelesítési folyamatnak igazán biztonságosnak kell lennie, de hogyan lehet még jobban fokozni a biztonságosságot? Erősebb titkosító kulcsokkal, bonyolult, gyakran változó jelszavakkal, publikus és privát környezetben eltérő módon működő környezeti beállításokkal? Igen-igen, de mégsem csak így. Ha viszont másfelől közelítünk és a többszörös hitelesítést, vagyis az ún. multifaktoros módszert alkalmazzuk, akkor valószínűleg nagyobbat lépünk előre. Miről van szó?

Például az először az ISA Server 2004-ben bemutatkozó multifaktoros hitelesítésről, amely a felhasználót kettős hitelesítésre kényszerítheti, azaz egy user/password kombináció ÉS egy hardver eszköz vagy egy tanúsítvány „bemutatására”. A lehetséges variációk szerint a felhasználónak rendelkeznie kell:

- Egy tanúsítvánnyal.
- Vagy egy egyszeri jelszót/kódot (One-Time Password, OTP) generáló szoftveres modullal/hardver eszközzel.
- Vagy egy SecurID eszközzel, amely minden szükséges esetben (hosszú érvényességi időben, pl. 2-3 évig) egy ún. passcode-ot (nagyon rövid lejáratú számkombináció) képes generálni.

9.14 ÁBRA PASSCODE ÉS PASSWORD, UGYANAZZAL A USERREL

Jelenleg valószínűleg az első a tipikus példa, amikor is a felhasználó rendelkezik egy smartcard-on elhelyezett személyes tanúsítvánnyal.

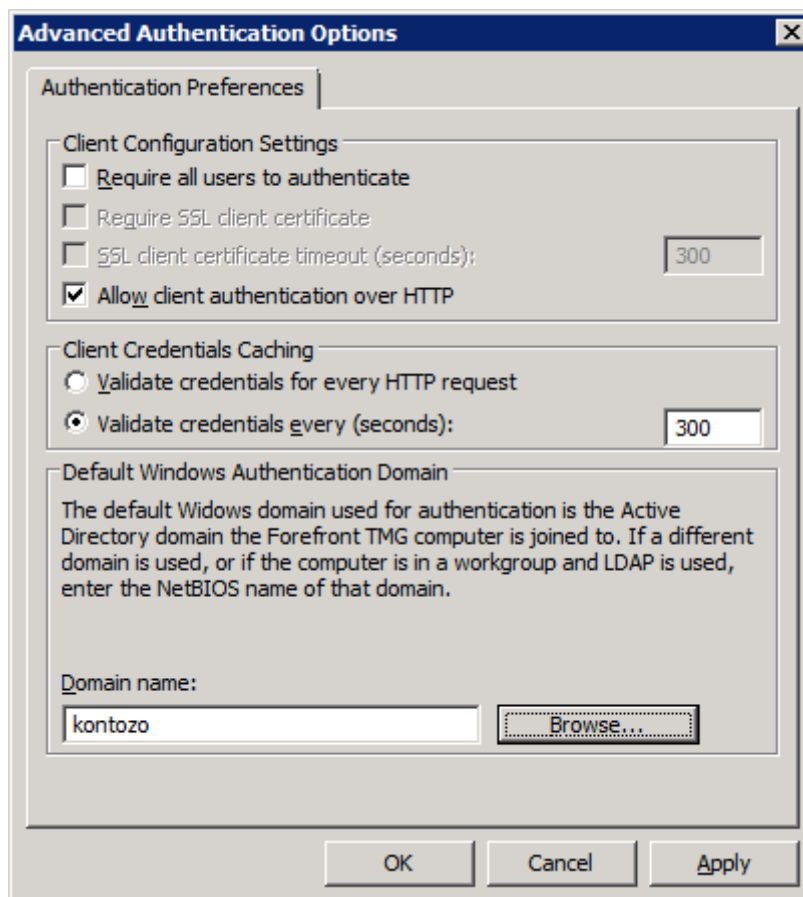
A KAPUN TÚL

A multifaktoros hitelesítés alkalmazásához tartozik még két gondolat:

- Az űrlapos hitelesítés simán együtt használható ezzel a módszerrel (lásd 9.14 ábra).
- Az OTP az ISA 2004-ben maximum az SecurID megoldáshoz volt alkalmazható, az ISA 2006-tól kezdve viszont a RADIUS hitelesítésénél is támogatott.

A jogosultságok tárolása

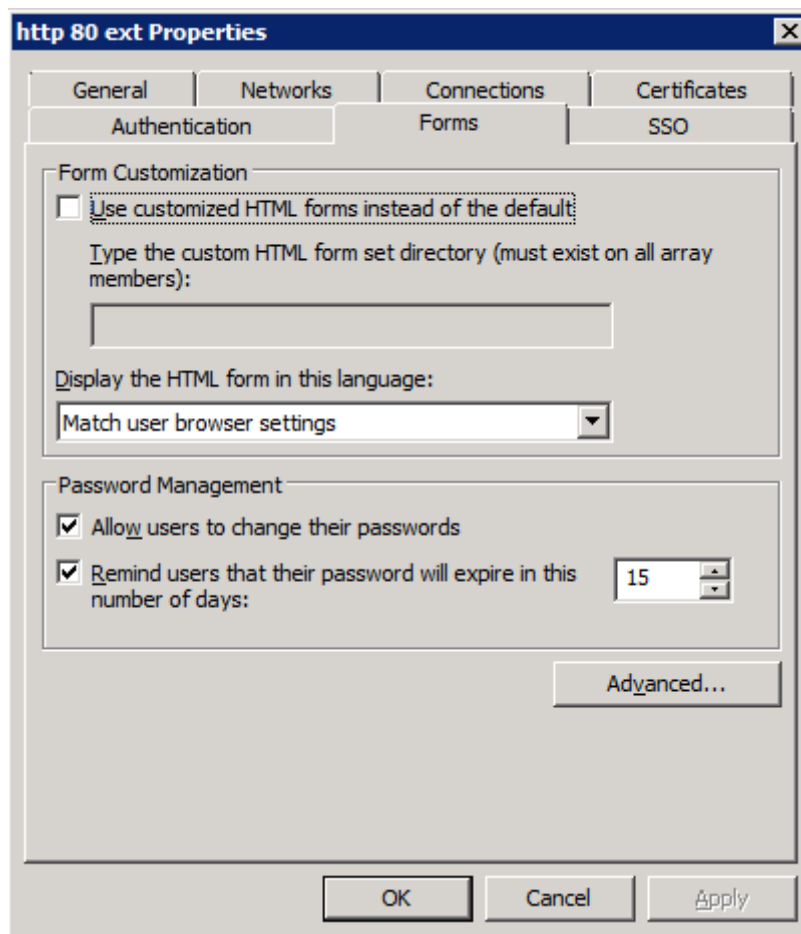
A TMG képes tárolni a Basic és az űrlap alapú hitelesítésnél használt felhasználói adatokat. Ha kérjük ezt a lehetőséget (alapértelmezésben tiltva van), akkor a TMG egy TCP session-ben egyszer, a legelső HTTP kérés alkalmával követeli meg csak majd ezeket az adatokat, és utána csak x időnként, az x értéke pl. a következő ábrán 300 mp. Ezt a módszert az Integrated (az AD és az LDAP féle egyaránt) és a RADIUS hitelesítés mód is támogatja.



9.15 ÁBRA A KÖZÉPSŐ (CLIENT CREDENTIALS CACHING) RÉSZ A LÉNYEG⁸⁸

⁸⁸ Ha az ábrával ellentétben egy olyan listener-ről lenne szó, amelyben SSL kliens hitelesítés is van, akkor további fülek állnának rendelkezésre (Client Certificate Trust List; Client Certificate Restrictions), és így további restriktciókat is bevezethetnénk a tanúsítvány elfogadásával kapcsolatban.

Közben az űrlapos hitelesítés apropóján szépen csendben átvezetünk a Forms földre is, hiszen ezt illetve ennek a paramétereit itt állítjuk be.

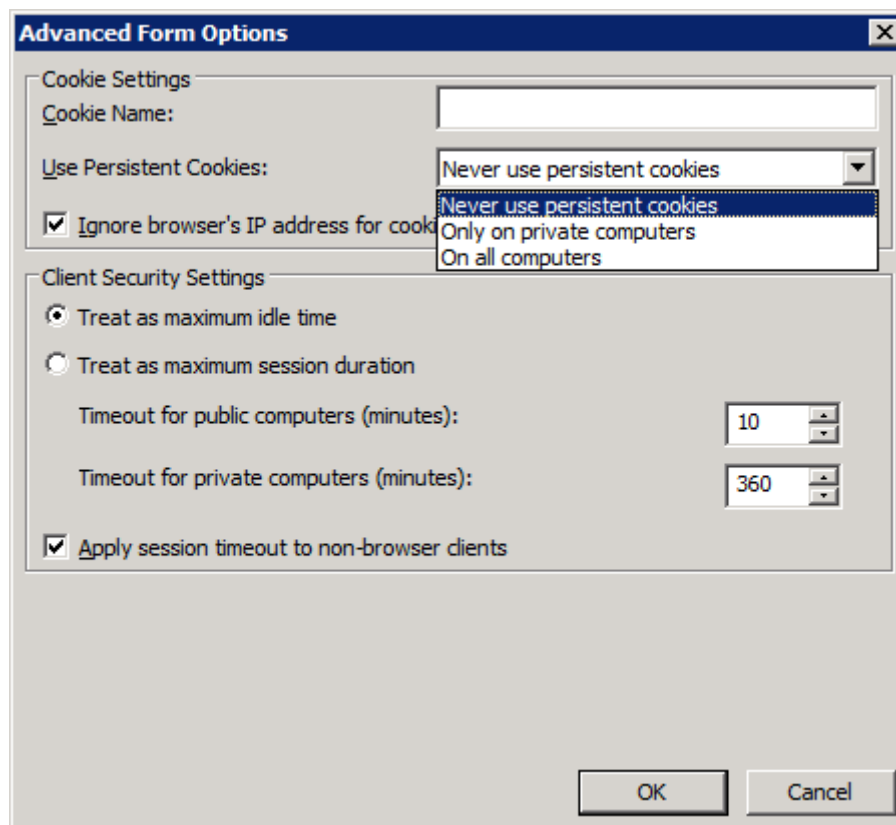


9.16 ÁBRA MI LEGYEN AZ ŰRLAPON?

Ha egyéni űrlapot szeretnénk, akkor a TMG sablonjai alapján elkészített űrlapunk helyét, azaz egy mappát kell megadnunk a panel tetején. A középső részben (“Display the HTML form in this language”) állítjuk be, hogy milyen nyelvű legyen az űrlap. Alapesetben meghagyjuk a felhasználó böngészőjében található nyelvi beállítást (Match user browser settings), de kiereszközhathatunk egy eltérő nyelvet is – és ez kötelezően felülírja majd a böngésző beállításait. Legalul pedig a korábban már említett jelszókezelés részletei látszanak.

Kicsit el van dugva, de ennek ellenére nagyon fontos az “Advanced” gomb tartalma is, ahol a cookie kezelés részleteit állítjuk, azaz pl. azt, hogy mikor lehessen egyáltalán perzisztens, azaz állandó sütitet használni. Ezek ugye szenzitív tartamúak is lehetnek, ergo ha a felhasználó egy publikus helyen (pl. egy internet kávézó) lép nem, akkor nem okos dolog, ha eltárolásra kerülnek. Jó, hogy szóba jött, ugyanis pontosan a belépést emlegetve lépünk át a következő részbe, azaz hogy meddig éljen egy felhasználói session. Ennek ideje lehet korlátlan, vagy függhet attól, hogy a felhasználó milyen

biztonsági beállítást választ az űrlap nyitólapján. Nézzünk vissza egy tetszőleges űrlapos ábrára (pl. 9.14), azt fogjuk látni, hogy mindig van egy "Public or Shared" és egy "Private" opció, amelyek beállításai, pl. itt az időtartamokban (vagy az előbb a cookie-knál) eltérnek. Azonban ez a lehetőség, csak akkor ér valamit, ha a felhasználó tudatosan választ, azaz tisztában van vele, hogy egy nyilvános helyen nem a "Private" opció a nyerő.

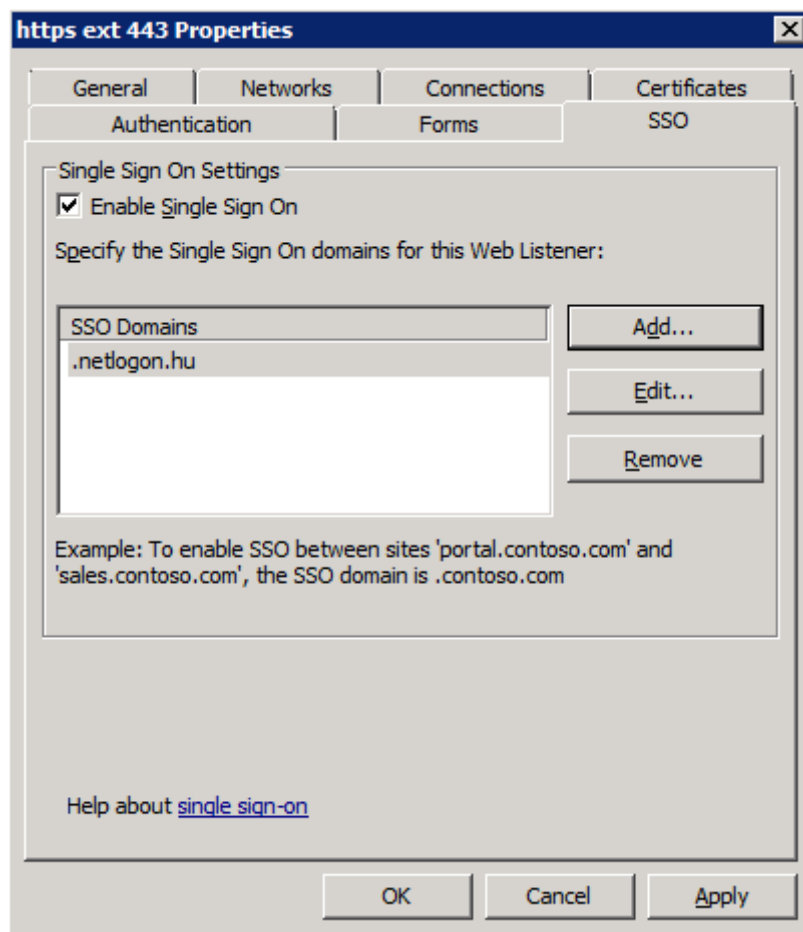


9.17 ÁBRA TOVÁBBI ŰRLAP OPCIÓK (A "NON-BROWSER" KLIENSEK PL. A PDA-K LEHETNEK)

A web listener beállításainak utolsó szakasza az SSO-val kapcsolatos. Mivel egyre nő a publikált szolgáltatások száma, könnyen elképzelhető, hogy egy szervezeten belül több különböző erőforrást is szeretnénk „megmutatni” a külső felhasználóknak. Ez rendben is lenne, de azonnal adódik egy probléma is ennek kapcsán, mégpedig az újra bejelentkezések szükségessége.

Ezzel el is értünk az SSO (Single Sign-On, egyszeri belépés) módszer alkalmazásához, amelynek a lehető legtöbb esetben célszerű együtt használni a különböző hitelesítési megoldásokkal (de csak az űrlaposnál működik), mert különben – elsősorban a felhasználók számára - nagyon fárasztóvá válhat egy-egy belépési folyamat. Ha itt beírjuk a tartományunk kívülről elérhető DNS névterét (.netlogon.hu), akkor a felhasználó amikor pl. az OWA-ból egy e-mailben kattint egy hivatkozásra, amely egy

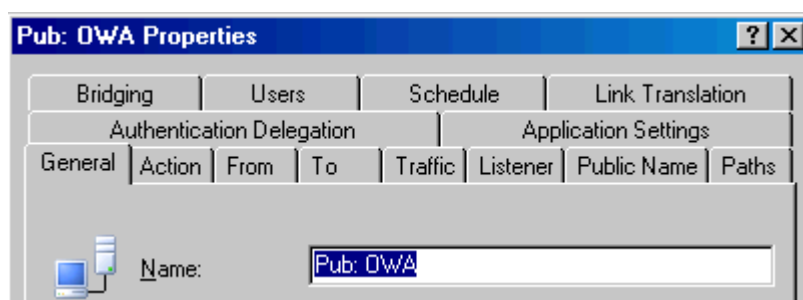
belső Sharepoint oldalra mutat, akkor nem kell majd újra belépnie a Sharepoint-ba, hanem a TMG "belép" majd felhasználó helyett a háttérben.



9.18 ÁBRA AZ SSO ENGEDÉLYEZÉSE

9.2.2 TOVÁBBI WEBSZERVER PUBLIKÁLÁSI OPCIÓK

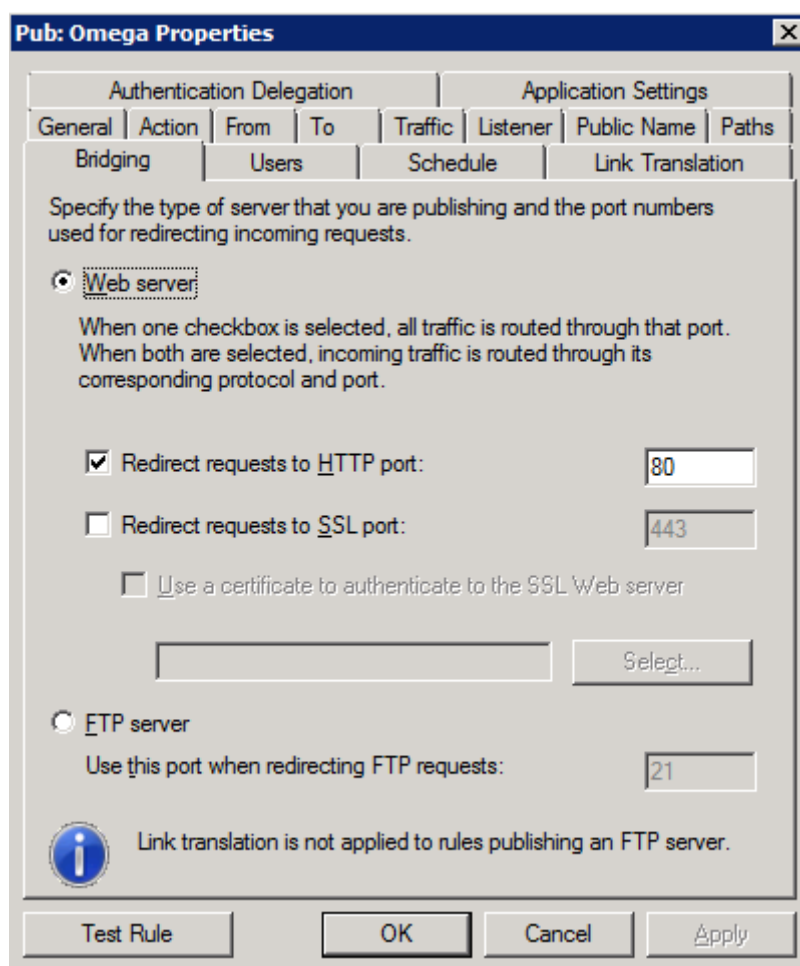
Itt és most már nem törekszem a teljesség igényének maximális kielégítésére, hanem csak az érdekesebbeket illetve a fontosabbak emelem ki. A három sornyi fülből egyet, azaz a Listener-t már alaposan kivégeztük, és később az Exchange publikálásnál egymásra egyébként is fény derül majd.



9.19 ÁBRA ISMÉTLÉS GYANÁNT: A KÜLÖNBÖZŐ FÜLEKEN A WEBSZERVER PUBLIKÁLÁS FINOMHANGOLÁSI LEHETŐSÉGEI ÉRHTŐEK EL

Bridging

A Bridging fül az, ahol a web- illetve egyúttal az FTP szerver⁸⁹ portátírányítási lehetőségei találhatók. Itt akkor fogunk sűrűn járni, ha történetesen a TMG kiszolgálón helyeztük el a webszervert is - ami nem a legbiztonságosabb szkenárió, de például egyetlen szerver esetén (lásd korábbi SBS verziók) nincs túl sok választási lehetőség.



9.20 ÁBRA ÁTIRÁNYÍTÁS

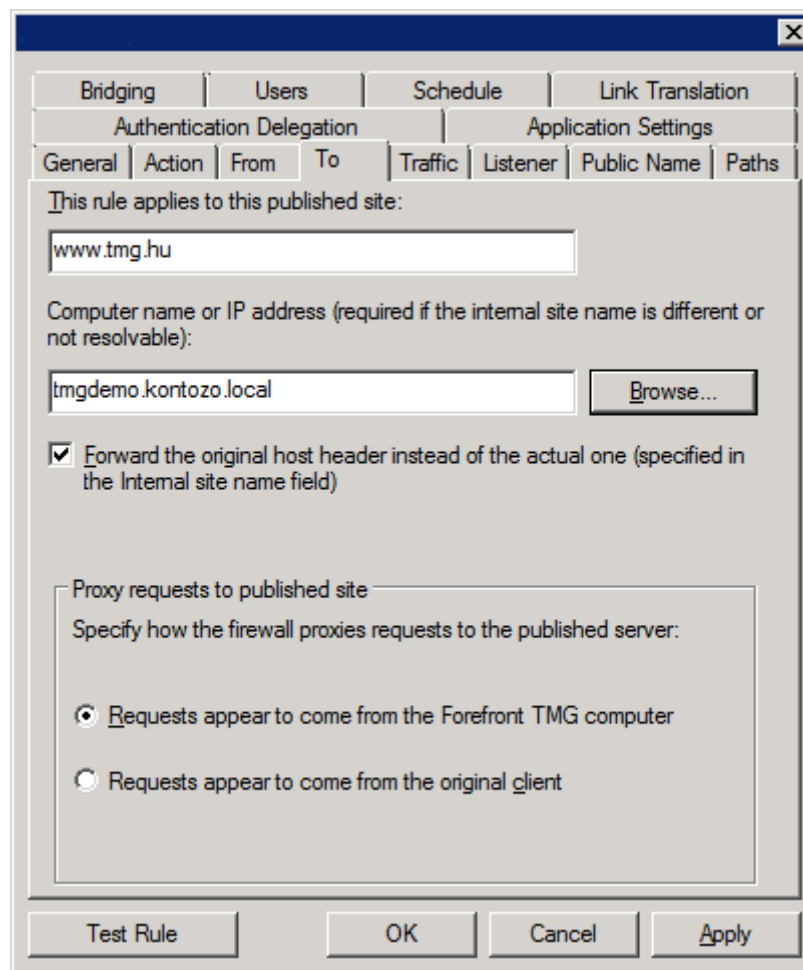
Ez esetben tehát a webszerver szeretné a hagyományos HTTP portot magáénak tudni, de erről a szándékáról az TMG villámgyorsan le fogja beszélni. Működő IIS esetén a várható konfliktusra már a telepítő is figyelmeztet, mert a TMG-nek kerek-perec, óhatatlanul szüksége van a 80-as portra. Teljesen logikus, hogy miért, a külső (de a belső ügyfeleknek is) a TMG kell, hogy legyen az egyes számú kapcsolat, ezért a 80-as porton a web listenerek kell figyelnie, hogy aztán már továbbadhassa a kéréseket és válaszokat a webszerver illetve az ügyfél felé. A megoldás nem a kissé nehézkes a

⁸⁹ FTP szerver? Azon már túl vagyunk, nem? Nos, itt beállíthatjuk azt is, hogy a HTTP/S kérések FTP kérésekként továbbítódjanak a webszerver felé.

`http://www.ceg.hu:8181` formula, azaz egy alternatív port használata, hanem az átirányítás. Az ügyfél böngészője a 80-as porton közelít, a TMG elkapja, és a Bridging fülön beállított tetszőleges porta továbbítja a kérést. Ehhez már csak a webszerver tulajdonságainál kell ugyanezt a portot beállítani. Természetesen ha nincs webszerver a TMG szerveren (ne is legyen), akkor erre nincs szükség, mert ekkor egy másik gép, a belső szerver 80-as portját használjuk (de ha nem, akkor ugyanúgy átirányíthatunk), nem zavarva az TMG listener-jét.

To

Rövid és velős neve van ennek a fülnek, nem is sejtetve, hogy egészen fontos dolgok rejtőznek mögötte. Kötelezően itt a publikált webhely nevét, esetleg alatta a belső nevét vagy IP címét (ha nem egyező) kell megadnunk. Ha SSL-t használunk ez csak olyan név lehet, amely a tanúsítványon is szerepel, más esetekben viszont elképzelhető hogy a TMG nem tudja feloldani az adott nevet, ezért kell a második mező pl. az IP címmel.



9.20 ÁBRA HÁROM LÉNYEGES DOLOG IS HELYET KAPOTT EZEN A PANELEN

A „Forward the original host header instead of the actual one” opció pl. az OWA publikálásnál hasznos, annyira, hogy az Exchange publikáló varázsló automatikusan be is kattintja. Ennél a pontnál a kérdés az, hogy az TMG továbbítsa-e az eredeti host header információt vagy kicserélje? Alapértelmezésben kicseréli a már említett második mező tartalmára, mert ez a biztos megoldás, viszont nem feltétlenül jó nekünk, pontosabban az adott alkalmazásnak.

A következő opció (Proxy requests to published site) viszont a szimpla webszerverek esetén is él és számít. Az alapfelállítás szerint a belső webszerver minden kívülről érkező kérés esetén csak a közvetítő felet, az TMG-t látja (mivel a fejlécben az TMG kicseréli a forrás IP-t), azaz gyakorlatilag csak a TMG belső hálózati kártyájának IP címével szembesül. Ez egyszerűvé teszi a webszerver választát, hiszen a cím ismerős alhálózaton van, benne van a routing táblában, közvetlenül elérhető, összesen annyi dolga van, hogy egy ARP kérést küld, és ha megjön a válasz, mehet a forgalom.

Ha viszont az alsó opciót választjuk, akkor annyi a különbség, hogy a webszerver egy idegen IP-vel találkozik, amelyről nem lesz információ a routing táblában, ezért az ARP kérést az alapértelmezett átjárónak küldi el, oldja meg az a problémát. Mivel általában a TMG belső „lába” az alapértelmezett átjáró (ebben az esetben muszáj is, hogy az legyen), megjön a válasz és indul a forgalom. Ha valaki ezt már harmadszor is elolvasta, biztosan azt fogja kérdezni, hogy minek bonyolítani a dolgot az alsó opcióval??? Hiszen a folyamat több időbe kerül valamint plusz terheléssel is jár. Van értelme, ha más nem az, hogy az IIS naplóban nem egyetlen IP cím kerül be (a TMG belső lába), és vezeti majd a naplóból képzett statisztikát toronymagasan, hanem a valódi kliensek címei. Az első opció viszont akkor kötelező, ha nincs lehetőségünk arra, hogy a TMG legyen az alapértelmezett átjáró (azaz valamilyen okból nem lehet SNAT kliens a belső webszerver), hiszen ekkor a webszerver és a TMG közötti kapcsolat e nélkül is töretlen lesz.

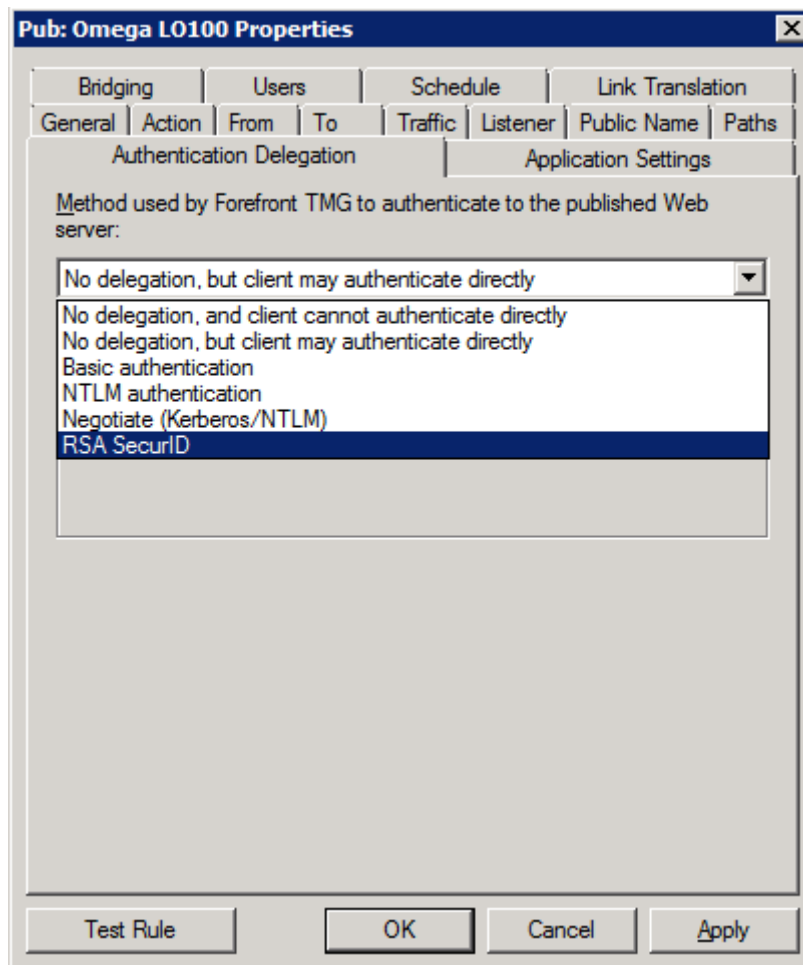
Egy az életből merített példa, azaz miért fontos még az eredeti IP cím: sok helyen a TMG mögött levő web kiszolgálók valamilyen terheléelosztási megoldással rendelkeznek. Legtöbb esetben ez kis hazánkban a Windows Network Load Balancing. A WNLB affinitás beállításainak eredményeként egy kliens mindig ugyanahhoz a WNLB taghoz megy, amíg azzal a taggal nem történik valami hiba. Ha minden bejövő kérésünk 1, legfeljebb 2 IP címtől származik, akkor a TMG mögött levő WNLB-t akár le is kapcsolhatjuk, mert az összes kliens kérés ugyanahhoz a WNLB taghoz fog érkezni. *(A lektor megjegyzése.)*

Hitelesítés-delegálás

Egyre több esetben fordul elő az a helyzet, hogy a hálózatokat elválasztó elemnek, azaz a tűzfalnak kell az elsődleges ellenőrzést elvégeznie, azért is, hogy a belső hálózatban működő kiszolgálót ne terheljük, és ne kockáztassuk az állapotát, például egy „próbálgató” kedvű, az OWA-ba jogosultság nélkül belépni óhajtó internetes vendég miatt. Maradva a példánál: sokkal jobb ha a TMG egy Exchange szervernek „hazudja be” magát, és már a határvonalon visszautasítja a jogosulatlan elérést, mintha minden hitelesítési csomagot előzetes vizsgálat nélkül, nyomban továbbítana az Exchange szervernek. Ezért van az, hogy egy - a TMG kiszolgálón keresztüli - hitelesítési folyamatban csak a jogosultságok érvényesítése után következik jogosultsági adatok végleges ellenőrzése, amelyet delegál a TMG a megfelelő belső szerver felé. Viszont itt is van fontos változás, mert míg az ISA Server 2004-ben csak a Basic hitelesítésénél élt ez a lehetőség, a 2006-os verziótól kezdve gyakorlatilag minden egyes hitelesítési metódusnál alkalmazható. Sőt, a publikáló szabályoknál a következő lehetőségeink vannak még ezeken kívül is:

- Nincs delegálás és a kliens nem hitelesíthet közvetlenül (biztonsági okokból akár ki is kapcsolható a komplett delegálás)
- Nincs delegálás, de a kliens hitelesíthet közvetlenül (a TMG nem avatkozik be)
- A Basic hitelesítés delegálása
- Az NTLM hitelesítés delegálása
- A Negotiate (megegyezőes) módszer, azaz NTLM/Kerberos hitelesítés delegálás
- Kikényszerített Kerberos delegálás⁹⁰ (pl. ha kliens tanúsítványon alapuló hitelesítésre vágyunk)
- A SecurlD hitelesítés delegálása

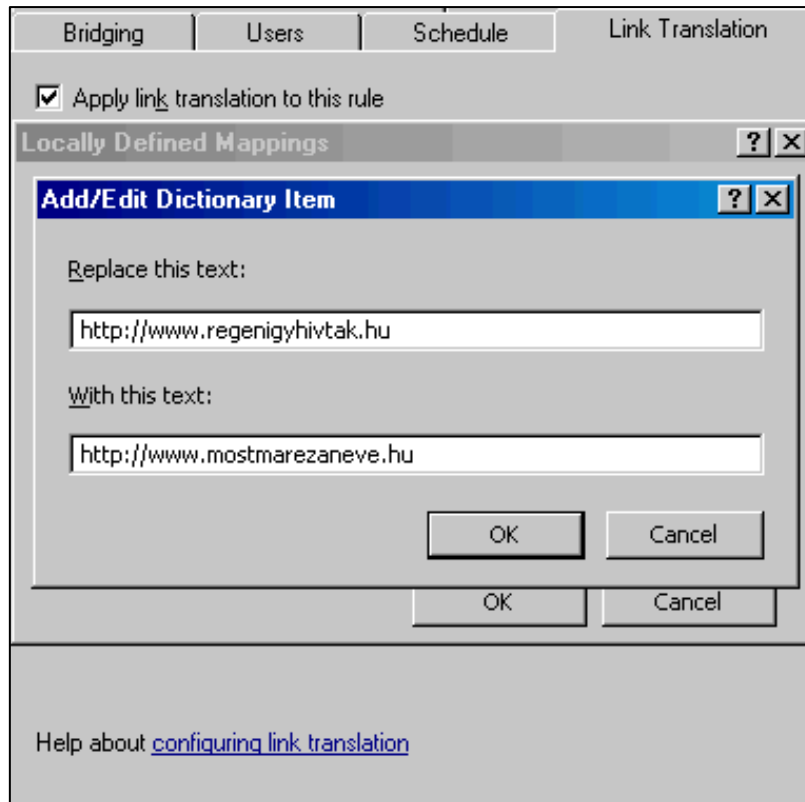
⁹⁰ Minimum Windows Server 2003-as tartományi működési szint szükséges hozzá.



9.21 ÁBRA MIVEL EZ EGY SECURID-S HITELESÍTÉSSSEL OPERÁLÓ PUBLIKÁLÁS, EZT IS DELEGÁLHATJUK

Link Translation

A Link Translation, szintén nem keveset fejlődött a kezdetek, azaz az ISA 2004 óta. Ez a szolgáltatás arra a célra van beépítve a publikáló szabályokba, hogy az adott website oldalain belül elhelyezett hivatkozások mindig pontosak legyenek. Mivel a külső ügyfelek számára a TMG az egyetlen kapcsolat, ezért ennek a szolgáltatásnak az ISA kiszolgálón kell működnie. Konkrétan ez azt jelenti, hogy a TMG korrigálja a felhasználó felé pl. a HTML kódban rövid névvel (<http://kiszolgalo/kep.gif>) megnevezett hivatkozásokat, az FQDN névre (<http://www.kiszorgalo.hu/kep.gif>). Ez az alapszintű, automatikusan bekapcsolt művelet, de emellett mi magunk is felvehetünk több hasonló szabályt is.



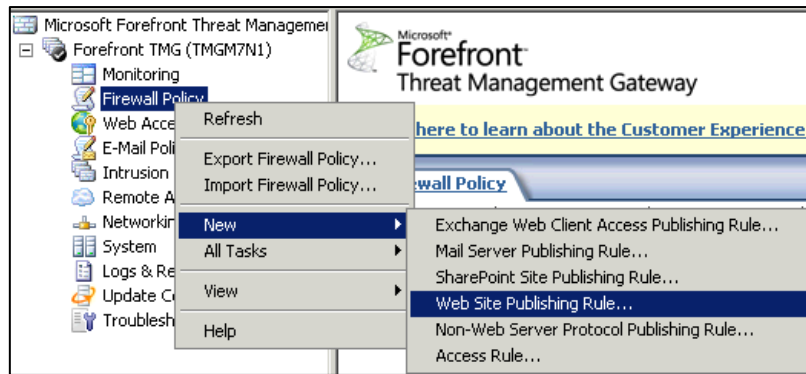
9.21 ÁBRA LINK TRANSLATION – EGYSZERŰ ÉS NAGYSZERŰ

Miért van erre szükség? Példának okáért vegyünk egy olyan webalkalmazást, amelyben több helyen is rögzítve van a kiszolgáló korábbi neve, de azóta sajnos ezt a szervert már átneveztük. Ekkor csak felveszünk egy új és lokális szabályt a régi és az ezt lecserélendő új névvel, és a TMG megteszi a változtatást. Egyszerű és nagyszerű szolgáltatás ez, ami az ISA 2006-tól kezdve annyival bővült, hogy az elnevezésekhez extra karakterkészleteket is rendelhetünk (az UTF-8 mellett). Sőt, az összes hozzárendelést és ezek részleteit megtekinthetjük egy külön weblapon a „Mappings...” gombra kattintva.

9.2.3 EGY MÁSIK PÉLDA: WEBSZERVER SSL-EL

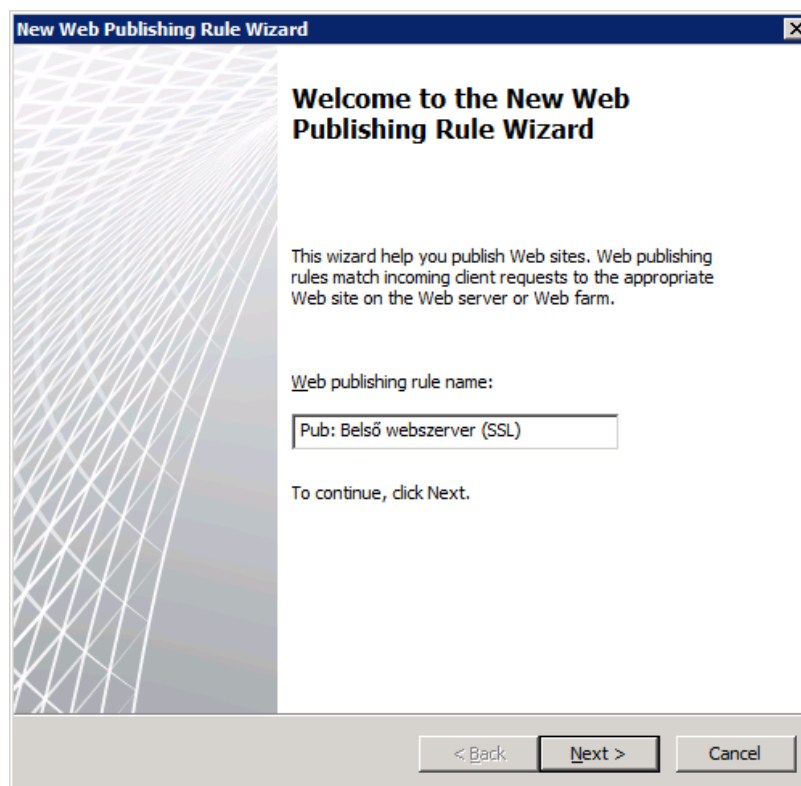
Immár jó néhány alapfogalommal tisztában vagyunk, jöjjön tehát a gyakorlat. A feladat egy SSL-el működő, de minden másban szimpla webservert közzététele, majd néhány extra opció beállítása. A webservert a belső hálózatban van és egy IIS-ről van szó, tehát egyszerűen használjuk a beépített varázslót a TMG MMC-ből.

1. Az első lépés a Firewall Policy nézetben a feladatok (Tasks) közül kiválasztani a „Publish a Web Site” pontot, de a következő ábrán látható módon is elérjük.



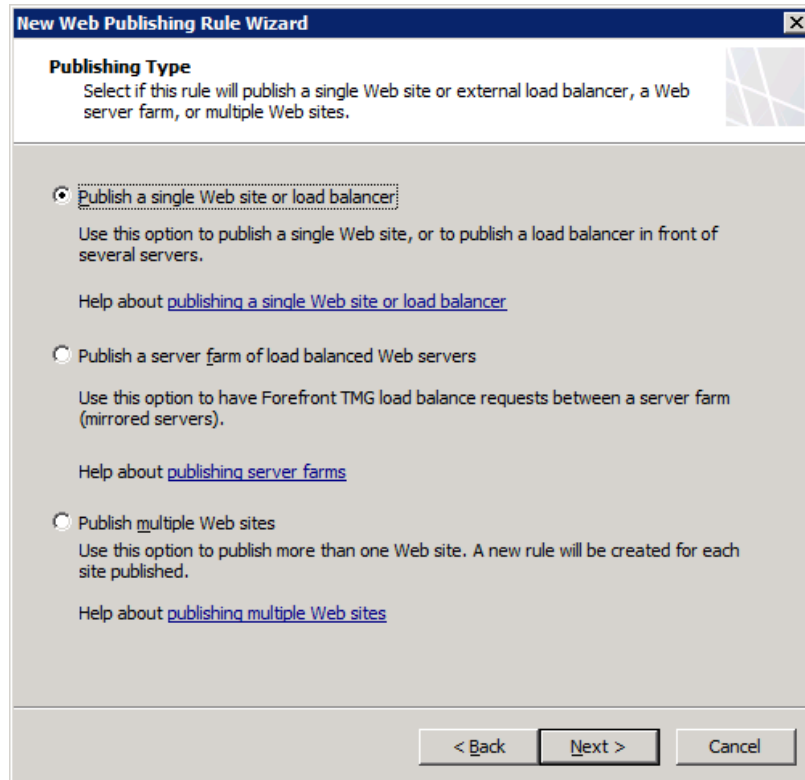
9.22 ÁBRA LINK TRANSLATION – EGYSZERŰ ÉS NAGYSZERŰ

2. Az üdvözlő képernyő és a szabály elnevezése következik.



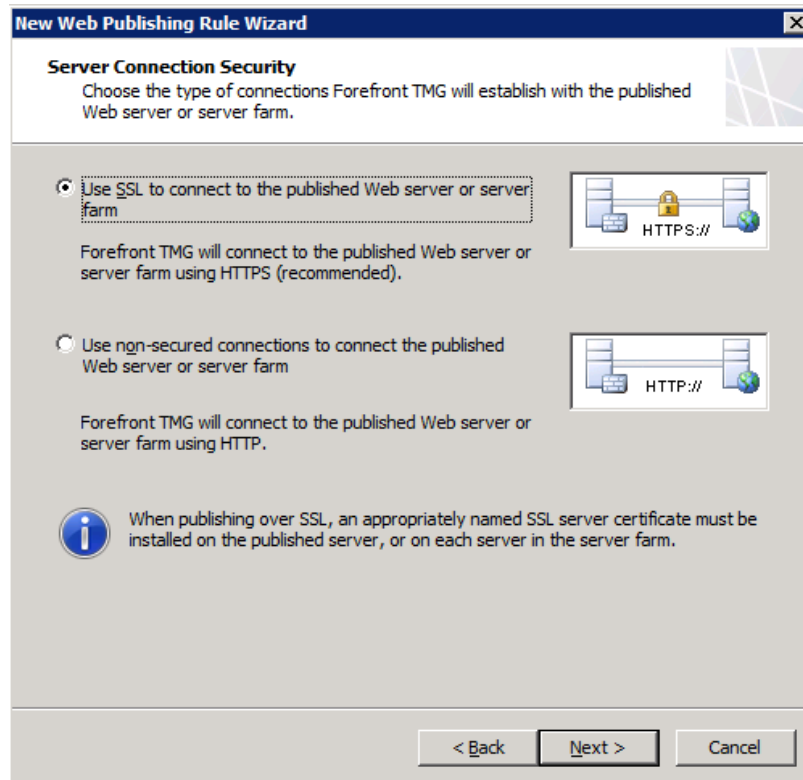
9.23 ÁBRA ADJUNK ÉRTELMES NEVET A SZABÁLYNAK, ÉS KÖNNYEBB LESZ 6 HÓNAP MŰLVA ÉRTELMEZNI

3. Az engedélyezés kiválasztása után el kell döntenünk, hogy milyen típusú webservert publikálásról van szó.



9.24 ÁBRA VÁLASSZUK KI A WEBSZERVERT TÍPUSÁT

4. Az első eset egy egyszerű website (jelen esetben ez kell nekünk), vagy éppen egy olyan speciális „load balancer” server publikálása, ami egy webszerver farm (kettő vagy több webszerver, amelyen ugyanaz a website vagy alkalmazás fut) előtt helyezkedik el. Az ajánlás szerint ha ez utóbbi publikálása a célunk, akkor célszerű inkább a második pontot választanunk. Ha tehát történetesen egy webszerver farm felállítása és publikálása a feladat, akkor a TMG MMC-ből lesz lehetőségünk néhány speciális terheléelosztási tulajdonság hangolására is – a publikálás mellett. A harmadik választási lehetőség akkor segít bennünket, ha több website publikálása a feladat, egyetlen varázslóval.
5. Ha továbblépünk akkor el kell döntenünk, hogy használunk-e kötelezően titkosítást (SSL) a webszerver elérésére. Mi most igen, ehhez teljesítenünk kell majd később néhány kritériumot, de egyelőre még csak választunk, más teendőnk nincs.



9.25 ÁBRA MI AZ SSL-T VÁLASZTJUK

6. A következő lépésben nevezzük meg a belső szervert a belső nevén, és ha szükséges a NetBIOS neve, vagy az IP címe is megadható. Itt egyébként - némiképp előregondolva az SSL miatt - arra is kell figyelnünk, hogy a tanúsítványban szereplő webszerver névnek (vagy egy SAN típusnál valamelyik alternatív névnek) és ennek a névnek meg kell egyeznie.

New Web Publishing Rule Wizard

Internal Publishing Details
Specify the internal name of the Web site you are publishing.

Internal site name:

The internal site name is the name of the Web site you are publishing as it appears internally. Typically, this is the name internal users type into their browsers to reach the Web site.

The internal site name must match the common or subject alternative name (SAN) on the certificate bound on the Web site that you are publishing.

If Forefront TMG cannot resolve the internal site name, Forefront TMG can connect using the computer name or IP address of the server hosting the site.

☒ Use a computer name or IP address to connect to the published server

Computer name or IP address:

< Back Next > Cancel

9.26 ÁBRA BELSŐ NEVEK MEGADÁSA

7. Az elérési út megadása opcionális, mert alapesetben elég az előző szervernév, de lehetséges behatárolni mappa szinten az adott website tartalmának elérését. És itt adhatjuk meg a korábban már kitárgyalt host header továbbítást.

New Web Publishing Rule Wizard

Internal Publishing Details
Specify the internal path and publishing options of the published Web site. You can publish the entire Web site, or limit access to a specified folder.

Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use /*. Example: folder/*.

Path (optional):

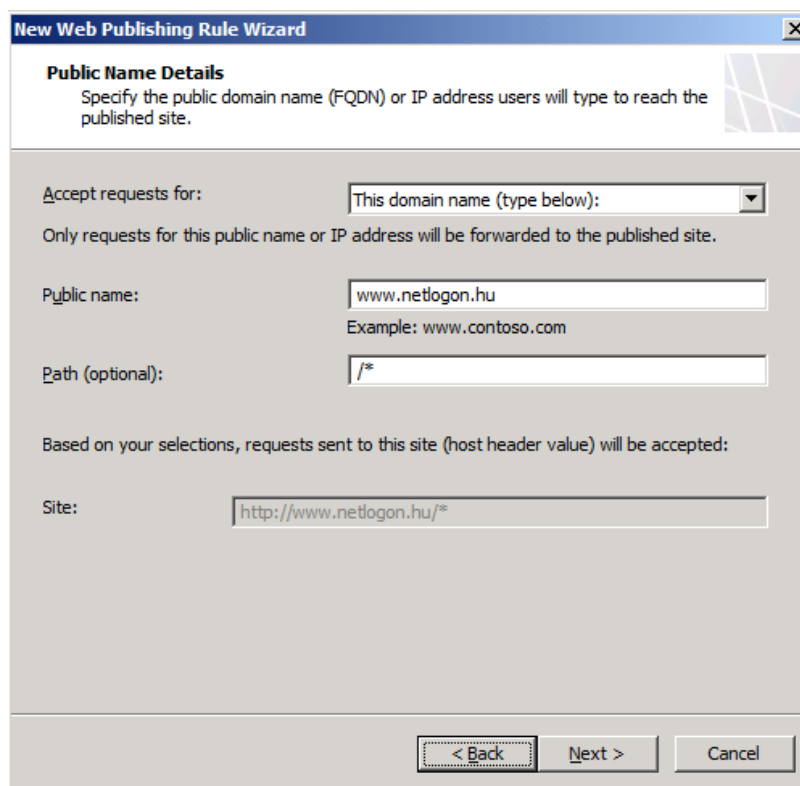
Based on your selection, the following Web site will be published:

Web site:

☐ Forward the original host header instead of the actual one specified in the Internal site name field on the previous page

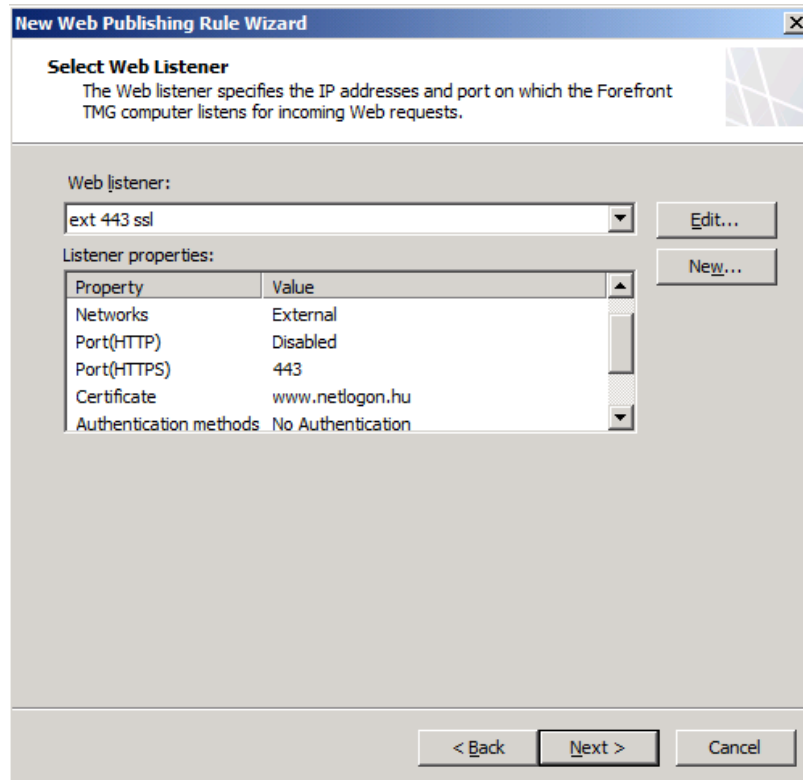
< Back Next > Cancel

8. Még mindig az elnevezésen rágódunk, hiszen a következő panelen jöhet a publikus név és az elérési út rögzítése. Ebből is látszik, hogy az a névadás abszolút rugalmas, hiszen bátran lehetséges egy a 23. szinten lévő mappa tartalmát egy szimpla URL-el helyettesíteni. Az `www.netlogon.hu` „Accept request for...” mező viszont szintén említést érdemlő, ugyanis ha a „This domain name (type below)” lehetőséget választjuk, akkor a TMG csak az általunk megadott névre irányuló kérést dolgozza fel, azaz ha bármilyen más (ha élő, ha nem) névvel, vagy IP-vel próbálkozunk, akkor azt megtagadja majd.



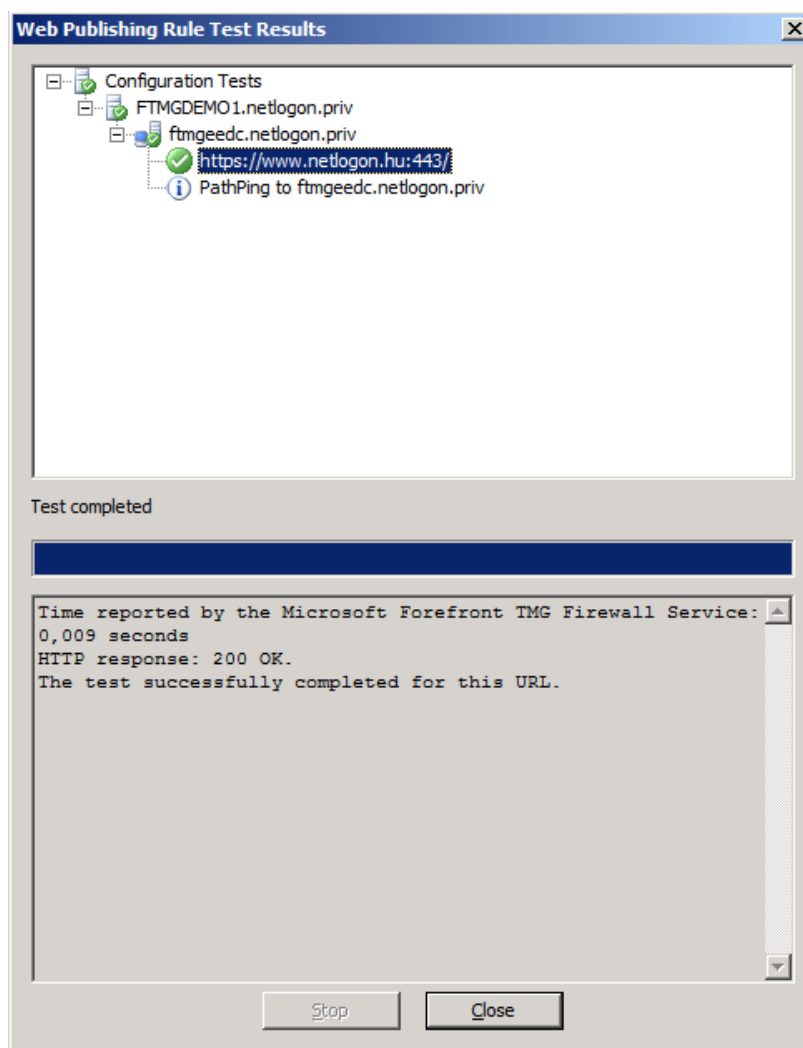
9.28 ÁBRA KÍVÜLRŐL HOGYAN LEHET MAJD ELÉRNI?

9. A következő lépés a már sokat emlegetett listener létrehozása, vagy éppen kiválasztása ha már rendelkezünk egy megfelelővel. Itt ez most részleteiben kimarad, mivel a 9.2.1-ben mindent elmondtam már erről, de annyit azért tudnunk kell, hogy ennél a publikálásnál mi a „Nincs hitelesítést” választjuk, valamint a megfelelő tanúsítványra is szükségünk volt.



9.29 ÁBRA HA MEGVAN A LISTENER MEHETÜNK IS TOVÁBB

10. Ezután a hitelesítés-delegálás lépés következik, amelyről már szintén esett szó, viszont a mi esetünkben most nincs szükség erre, mivel ugye hitelesítés sincs.
11. Egy speciális felállásban akár még felhasználók és csoportjaik szerint is szűrhetnénk az elérésre, de egy publikus website esetén (még ha SSL-el is működik) erre nem lesz szükség, így meghagyjuk az alapbeállítást a következő lépésben, és az összegző, ellenőrző ablak után végeztünk is a webszerver publikálással.
12. Nos, innentől elvileg működik a webszerverünk HTTPS-el működő külső elérése, de azért még nem végeztünk, próbáljunk ki egy remek dolgot, azaz az integrált tesztelést, a publikáló szabály bal alsó sarkában lévő "Test Rule" gombbal. Ez rengeteget segíthet, mivel az esetleg hibaüzenet(ek)ből rögtön kitalálhatjuk, hogy mit szűrtünk el.



9.29 ÁBRA MŰKÖDIK!

9.3 SPECIÁLIS PUBLIKÁLÁS: AZ EXCHANGE SERVER

Ez a témakör is hatalmas. Elsősorban azért, mert rengeteg féle forgatókönyv szerint használhatjuk kívülről is az Exchange szerver szolgáltatásait, másrészt azért, mert az ősidők óta nagyon szoros kapcsolat van e két nagy kiszolgáló között. Kezdjük azzal, hogy egy rövid áttekintést adunk az Exchange szerverek szerepeiről.

9.1 TÁBLÁZAT EXCHANGE SZERVER SZEREPEKÖRÖK

Szerepkör	Leírás
Mailbox Server	Back-end kiszolgáló, amely a postafiókokat és a nyilvános mappákat tárolja.
Client Access Server	OWA és ActiveSync, POP3 és IMAP valamint pl. az Autodiscover és egyéb webes szolgáltatások támogatása.
Unified Messaging Server	A PBX (Private Branch eXchange) rendszerekhez kapcsolható szerepkört, amellyel telefonon

	keresztül férhetünk hozzá a postaládánkhoz, és pl. hangvezérléssel irányíthatunk kattintgatás helyett.
Hub Transport Server	A levelek továbbítását végzi (ez egy klasszikus SMTP szerver) az Exchange organizáción belül.
Edge Transport Server	A Perimeter (DMZ) hálózatban elhelyezett levél továbbító szerver, amely a belső Hub Transport-tal együttműködve fogadja és küldi az e-mailjeinket (SMTP-vel szintén).

Ha csak a publikálást tekintjük (és elsősorban az Exchange 2010 + TMG párosra fókuszálunk), akkor nagyjából négy eltérő területre oszthatjuk fel az Exchange szerverrel végzendő feladatainkat, persze nem egyenlő részben:

1. Az SMTP szerver publikálása (két módszerrel is)
2. SMTP, vírus és spam védelem (Exchange Edge / FPE Server)
3. A klasszikus e-mail protokollok (POP3, IMAP) publikálása
4. Webes kliensek (OWA, OA, ECP, ActiveSync) publikálása

9.3.1 AZ SMTP SZERVER PUBLIKÁLÁS

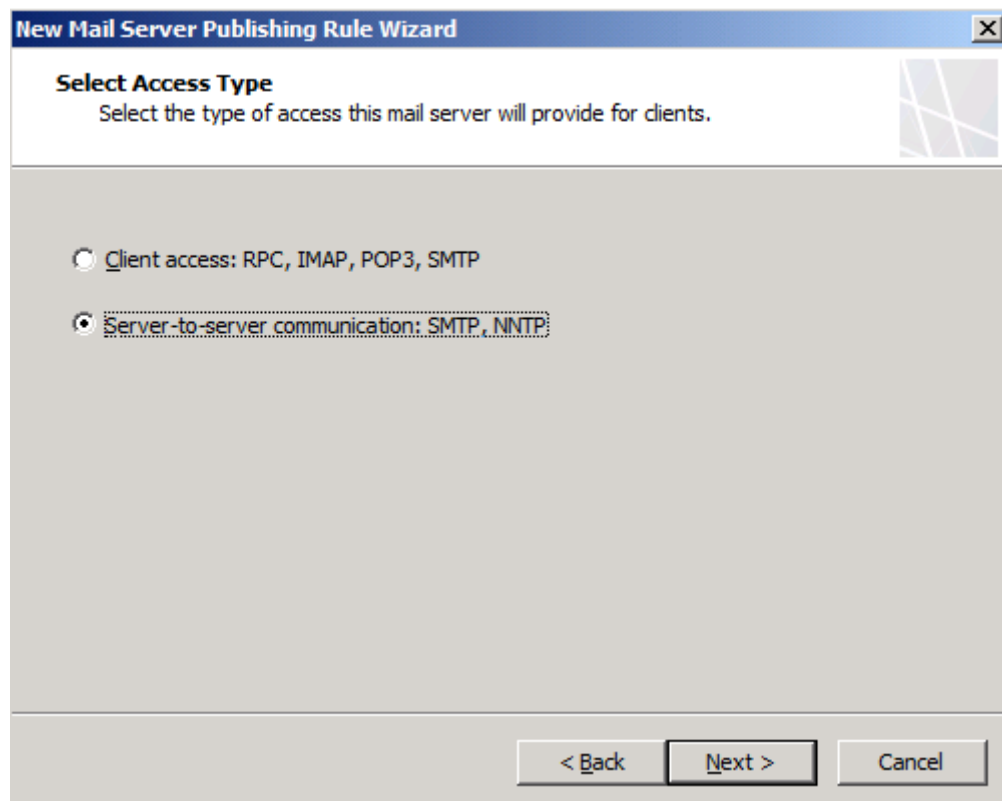
Ez egy egyszerű szkenárió, a kevés komforttal és innovációval - de a legkevesebb munkával is. Vegyünk egy szolid, egyszerű környezetet alapul, Perimeter, Edge Server és minden más extra nélkül, azaz az egyetlen Exchange szerverünk a belső hálózatban SNAT kliensként tengeti hétköznapiit, és szeretnénk ha a TMG-n keresztül SMTP szerverként működne. Az egyéb működési feltételeket (pl. az MX, PTR esetleg az SPF rekord) már mind megteremtettük, sőt az Exchange-ben is konfiguráltuk már a megfelelő konnektorokat.

Ezek után pl. a Firewall Policy pontra a jobb gombbal kattintva, egy új publikáló szabályként válasszuk a "Mail Server Publishing Rule..."-t a régi jól bevált ISA serveres módszer szerint.



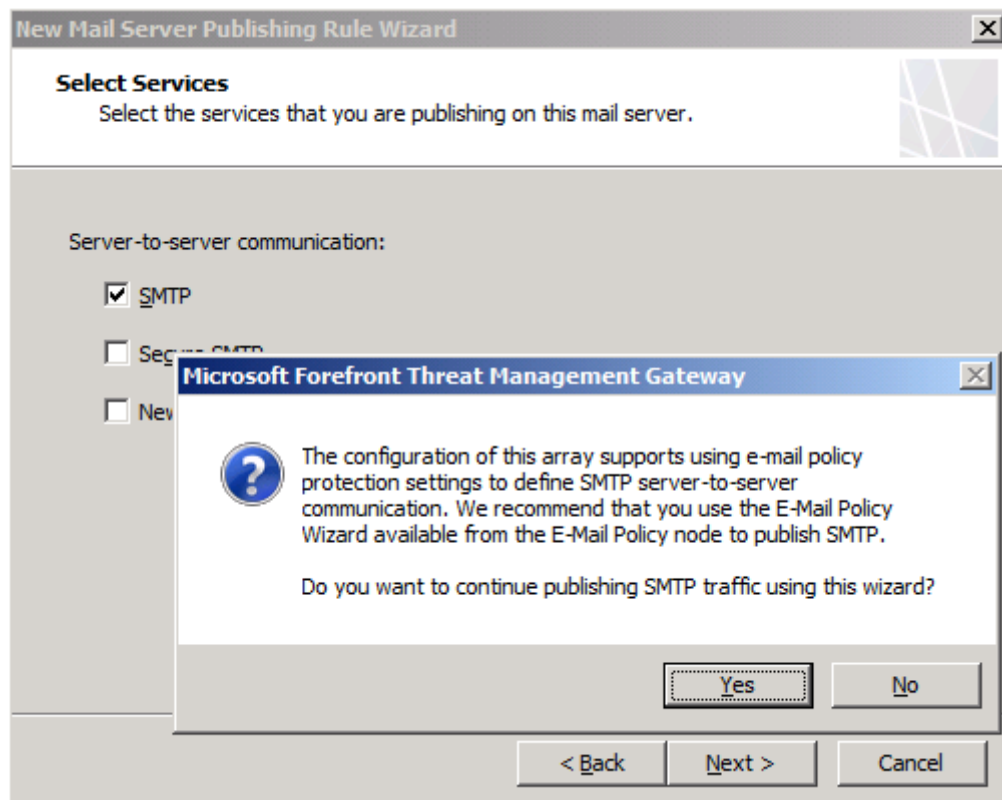
9.30 ÁBRA ITT MÉG BÁRMI LEHET

A varázsló következő ablaka az amelyben elválik majd a következő fejezet témájától a jelenlegi, ugyanis most mi a szerverek közötti kommunikációt akarjuk erősíteni, ezért ezt válasszuk.



9.31 ÁBRA

A következő lépésben finomítunk, azaz választhatunk, hogy SMTP, SMTPS, illetve NNTP szerver publikálást óhajtunk.



Most jön a meglepetés, ugyanis ha kiválasztjuk az SMTP-t, akkor egy felhívás formájában tudatja velünk a TMG, hogy van már ennél újabb módszer is, hagyjuk ezt. Nos hagyjuk is, de azért ha mégis folytatnánk, akkor jelzem, hogy ezután már csak az Exchange Hub Transport kiszolgáló IP-jét kell megadni, valamint azt a hálózatot kell kiválasztani ahol figyelnie kell majd az SMTP listener-nek - ez tipikusan az External lesz.

Na de akkor térjünk rá az ajánlott megoldásra, de előtte szeretném jelezni, hogy az ajánlás oka a TMG részéről egy teljesen más hozzáállást jelent majd.

9.3.2 SMTP VÉDELEM, VÍRUS- ÉS SPAMSZŰRÉS

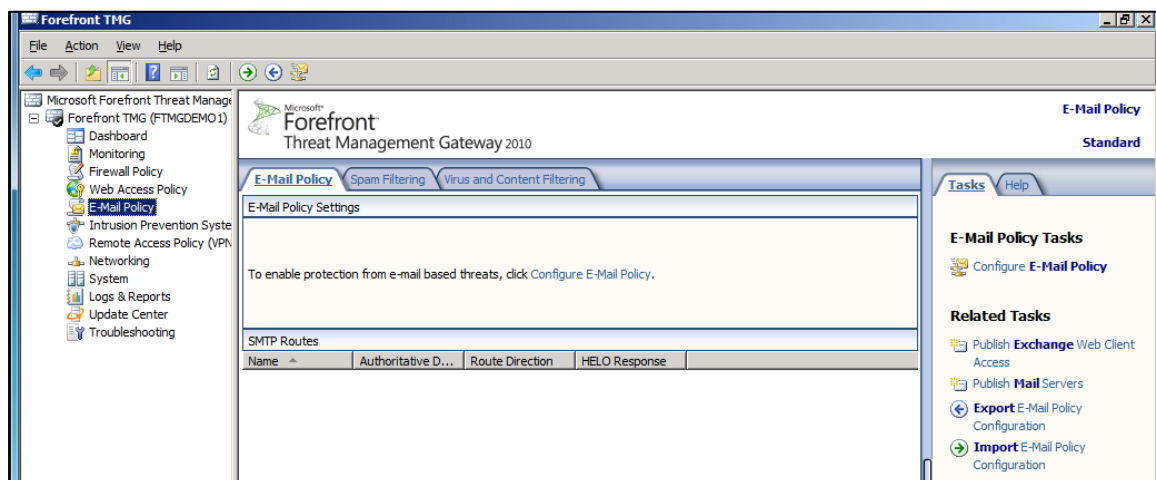
Az ISA 2004-ben szerepelt egy érdekes komponens, amely neve SMTP Message Screener volt, és egy második SMTP szerver beillesztésével képes volt az ISA és az Exchange szerverek közötti forgalomban, az e-mailek fejlécében és törzsében a vírusokat és a kéretlen leveleket kiszűrni, általunk bevitt sztringek és szignatúrák alapján. Teljesen jól működött, sok egyéb dolgot is lehetett benne állítani, viszont minden szűrőnivaló elemet csak manuálisan lehetett bevinni, és minden ilyen alkalommal kötelező volt az SMTP szerver restart. Ez így 2010-ben már nem tűnik azért nagy számnak, de már korábban sem volt az: a Microsoft az ISA 2006-ból ki is vette ezt a komponenst, és a már Exchange 2003-ban is használható, az Exchange szerverre telepíthető "Intelligent Message Filter" mellett tette le a voksát.

Aztán az Exchange 2007-ben már egy igen kellemes komponenst kaptunk a spamek szűrésére - beépítve az Exchange-be. Egész pontosan egy külön szerepkörrel (Edge) működő szerverrel a Perimeter hálózatban, SMTP gateway-ként kiválóan működhetett a spamszűrés (plusz a Connection/Content/Sender/Recipient filtering, a Sender ID és pl. a Sender Reputation), és a hozzátartozó adatbázisok pedig egyszerűen frissülhettek pl. a Microsoft Update szerverekről vagy egy WSUS-on keresztül is. Ha magasabb elvárásaink voltak, akkor használhattunk egy nagyobb tudású eszközt, pl. a Forefront Protection For Exchange Server-t.

A TMG színrelépésével a változás a spam, vírus és SMTP védelem tárgykörben egész jelentős, mivel az Exchange Edge szerepkör és/vagy a Forefront Protection For Exchange Server 2010 immár magára a TMG gépre telepíthető, és helyben működik⁹¹. Ez egyszerűbb, olcsóbb és gyorsabb feldolgozást jelent, valamint nemcsak helyben működik, helyben is konfiguráljuk. Ez egyben az SMTP szerver egy újfajta publikálását

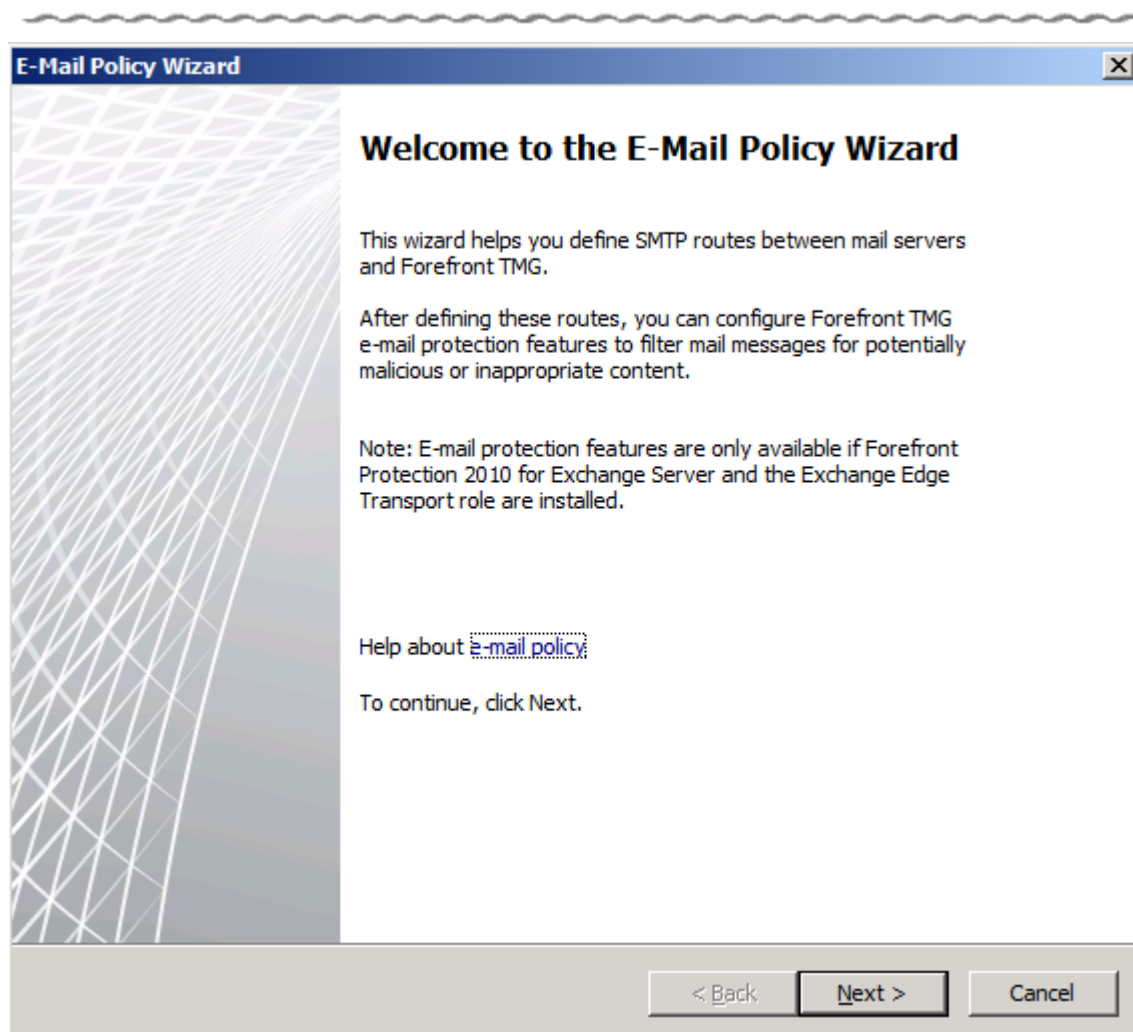
⁹¹ Jó lett volna ez már korábban is, csak hogy az ISA-ból csak 32 bites volt, az Exchange 2007-ből meg csak 64 bites.

is lehetővé teszi, és ezt a TMG-ben egy ún. E-Mail Policy varázslóval hozzuk létre. Nézzük meg akkor, hogy hogyan történik mindez.



9.33 ÁBRA ITT KEZDŐDIK MINDEN

Az előző ábrán is látható E-Mail Policy pontra kattintva egy üres képernyőképet kapunk, viszont a középső keret fejlécében ott virít a "Configure E-Mail Policy" varázsló indító linkje, amellyel az SMTP route-okat fogunk létrehozni a TMG és a levelezőszerverünk (vagy szervereink) között.



9.34 ÁBRA VARÁZSOLJUNK KAPCSOLATOKAT

Ha elindítjuk, rögtön kapunk egy figyelmeztetést, amely arról szól, hogy ez az egész védelem csak és kizárólag akkor működik, ha minimum egy Exchange Edge szerepkör már megtalálható a TMG-n, illetve akkor is, ha ez kiegészül a FPE2010-el (amelynek 120 napos változata megtalálható a telepítő médián).

És ami még fontos, az Edge és/ vagy az FP2010 telepítésére előbb kell sort kerítenünk mint a TMG-re. Sőt, az FPE-t csak az Exchange Edge után tehetjük fel. És persze tisztázzuk: az Exchange Edge megköveteli a saját licenszét, úgy ahogyan az FPE is pénzbe kerül majd 120 nap után. Sőt az FPE-t viszont érdemes feltenni a többi Exchange szerverünkre is, hiszen a TMG-n lévő példány csak az átmenő forgalom ellenőrzésére használható. Az FPE 2010-ről rengeteget megtudhatunk a Szirtes István kollégám által készített kitűnő screencastokból: <http://www.microsoft.com/hun/technet/article/?id=a8985983-6e4d-4267-bc3b-cc2b50e7d5e6>

Ez egyébként nem azt jelenti, hogy az SMTP publikálás nem működik, meg az, csak a védelem nem elérhető. Szóval lépünk tovább, és tekintjük meg a varázsló első paneljét.

E-Mail Policy Wizard

Internal Mail Server Configuration
Specify your internal mail servers and the domains from which these servers accept mail messages (accepted authoritative domains).

Internal mail servers:

Computer Name	IP Address
FTMGEEEDC.netlogon.priv	172.16.20.10

Add...
Remove

Accepted authoritative domains:

*.netlogon.hu

Add...
Remove

< Back Next > Cancel

9.35 ÁBRA AZ ELSŐ LÉPÉSEK

Adjuk meg amit kér, azaz a Hub Transport szerver nevét és IP címét, illetve azt a domaint, amelybe szánt e-maileket elfogadhatja a TMG. Ezután jöhet a már sokadszor látott beállítás (már nem is készítek hozzá képet, lassan fejből lerajzolhatja bárki), amikor is kiválasztjuk, hogy mely hálózat az, amelyiken a TMG az Exchange Hub Transport-tal kommunikál (tipikusan az Internal, ugye).

A következő lépés majdnem ugyanez, de mégsem. Itt is hálózatot választunk, azonban azt amelyen az Internetre vagyunk kötve. De emellett még meg kell adnunk azt az FQDN nevet is, amelyen majd az SMTP szerverünk válaszol a HELO vagy az EHLO parancsokra. Ez ugye egyúttal az a név is, amelyre egy reverse DNS feloldással válaszként a külső IP-nket kapjuk.

E-Mail Policy Wizard

External E-Mail Listener Configuration
The external e-mail listener accepts inbound mail traffic from the networks and IP addresses specified here.

Networks:

Name	Selected IPs
☒ External	<All IP addresses>
☐ Internal	<All IP addresses>
☐ Local Host	<All IP addresses>
☐ Quarantined VPN Clients	<All IP addresses>
☐ VPN Clients	<All IP addresses>

Select Addresses...

Specify the public domain name or IP address the e-mail listener provides in response to SMTP session initiation messages (HELO, EHLO).

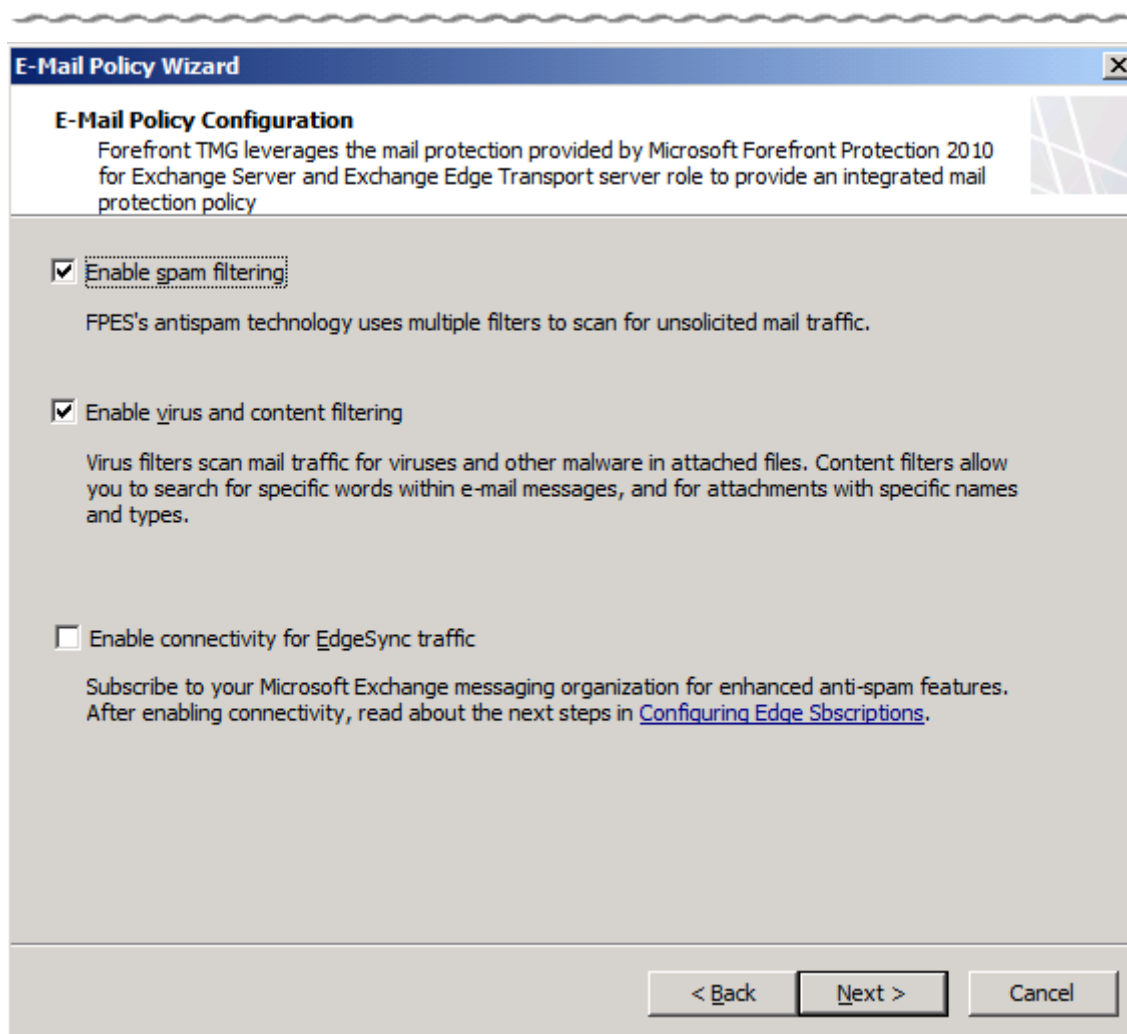
EQDN or IP address:
mail.netlogon.hu

Examples: mail.contoso.com, 192.168.10.10

< Back Next > Cancel

9.36 ÁBRA A KÜLSŐ FÜL BEÁLLÍTÁSA

Ez volt a java, most már a kényelmesebb dolgok jönnek. Elsőként is, a védelem összetettségét határozhatjuk meg.

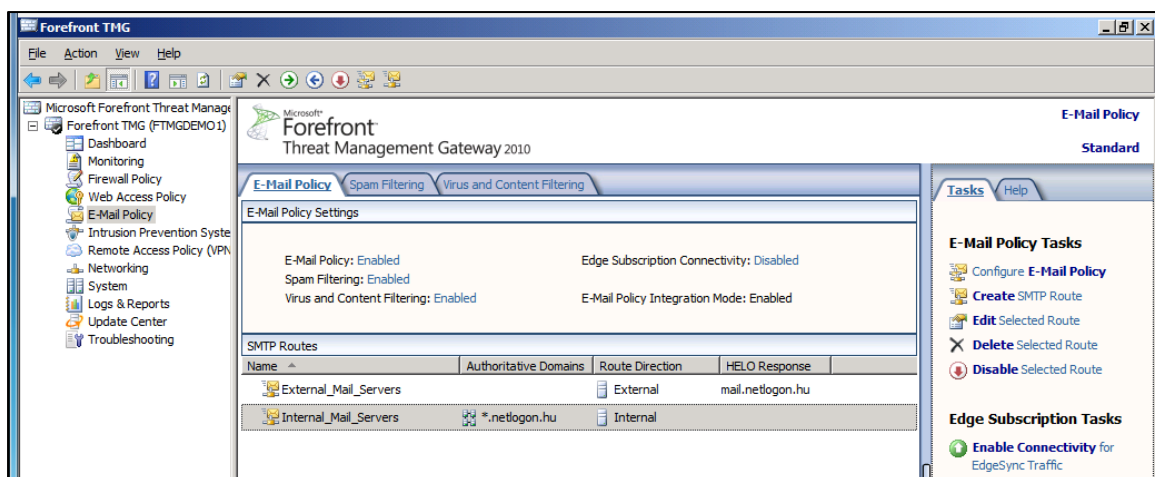


9.37 ÁBRA HÁROMBÓL MENNYI? MOST CSAK KETTŐ.

Itt azonnal bekapcsolhatjuk a spam és a vírus/tartalom szűrést⁹², valamint az EdgeSync kapcsolódást a belső Exchange Hub Transport szerver felé. Ezzel egy teljesen automatikus és biztonságos (kölsönös TLS) replikációs kapcsolatot hozunk létre, és így a Transport szerveren fogjuk konfigurálni az Edge szerverünk lehetőségeit, pl. a route-olással vagy az elfogadható e-mail tartományokkal kapcsolatban. Ellenben jó ha tudjuk, hogy amit itt beállíthatunk, azt később bármikor megváltoztathatjuk, ezért most az EdgeSync belövésére nem kerítünk sort.

Ezzel egyébként készen is vagyunk, csak az összegzés jön (és a System Policyban szereplő SMTP szabály automatikus élesítése), és a végeredmény, amely így néz ki a TMG-ben:

⁹² De az Exchange Edge önmagában még nem ad a kezünkbe egy vírusirtót, csak az FPE-vel együtt: <http://technet.microsoft.com/en-us/library/aa997658.aspx#Filters>

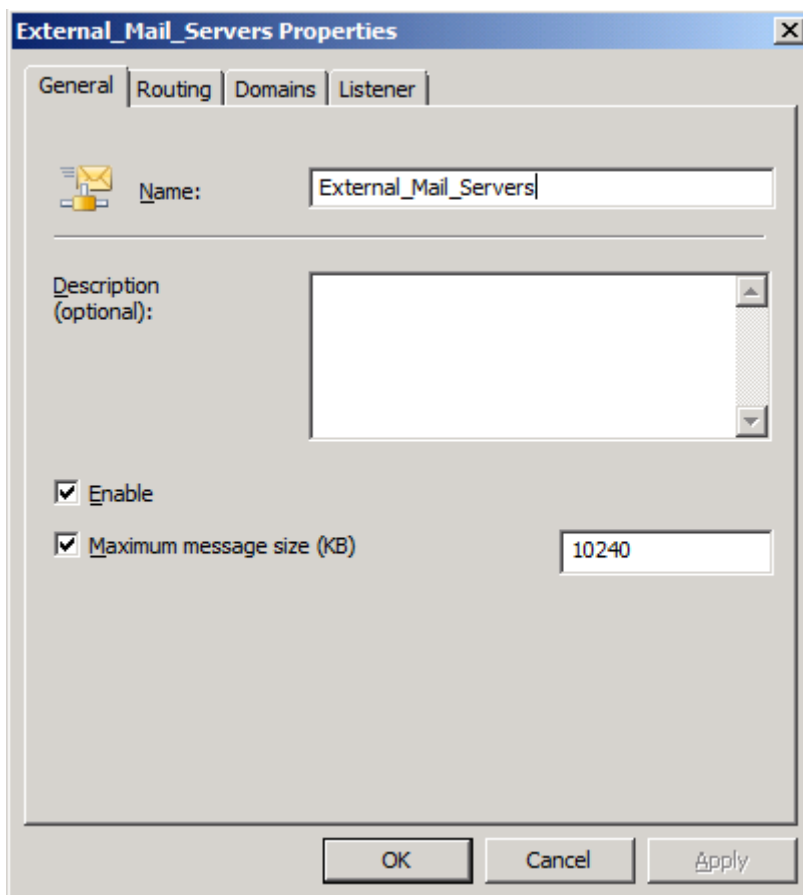


9.38 ÁBRA KÉSZ

Feature	Exchange Edge Role	FPE 2010
IP Allow / Block Lists	☒	☒
IP Allow / Block List Providers	☒ (custom)	☒ (FF DNSBL)
Sender / Recipient Filtering, Sender ID	☒	☒
Sender Reputation	☒	
Basic Content Filtering (SmartScreen)	☒	
Premium Antispam (Cloudmark)		☒
File Filtering		☒
Message Body Filtering		☒
Antivirus and Antispyware		☒

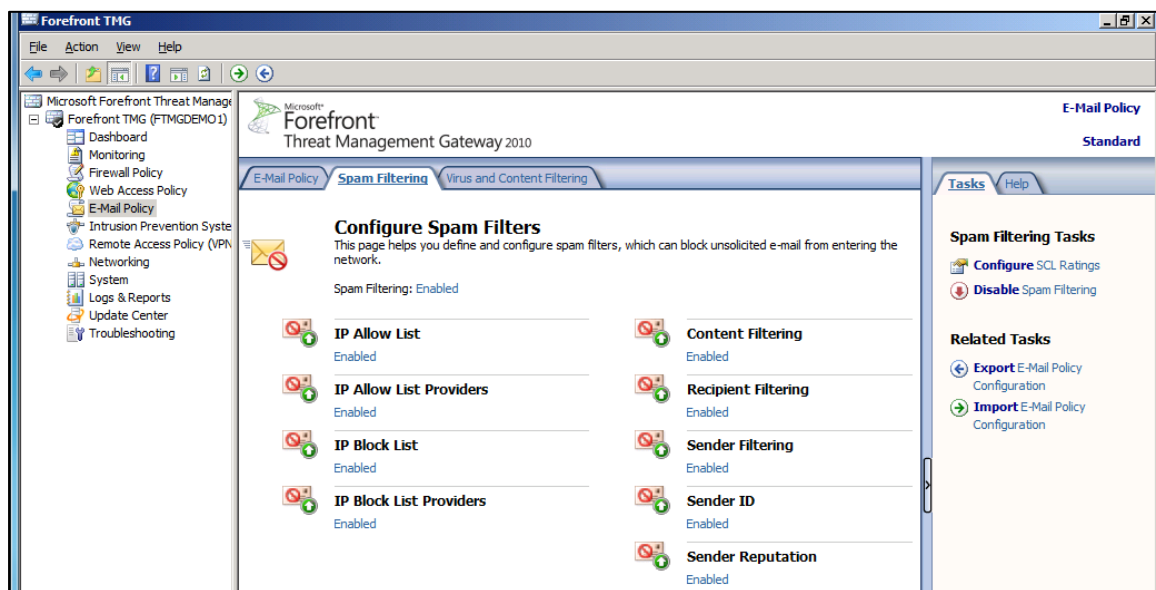
9.39 ÁBRA A KÉPESSÉGEK TÖMÖRÍTETT ÖSSZEHASONLÍTÁSA

Egyébiránt még nincs vége, egyrészt egy az Action Pane-ben látható paranccsal (Enable Connectivity for EdgeSync Traffic), majd utána egy .xml fájl legyártásával és ennek a Hub Transporton történő beimportálásával összehozhatjuk a korábban említett replikációt. Másrészt bármelyik SMTP route nevére kattintva behozhatjuk annak tulajdonságait, ahol megint csak kismillió opciót találunk, négy különböző fülön keresztül.



9.40 ÁBRA AZ SMTP ROUTE-OK IS KONFIGURÁLHATÓAK

És akkor a spam és vírus szűrés beállításairól nem is beszéltünk, ezeket a középső keret fejlécében találjuk a "Spam Filtering" és a "Vírus és Content Filtering" fülök alatt. Itt és most nem is fogunk, ez inkább Exchange Server tananyag, nézzük meg a következő ábrát: teljes tükörképe a közismert Exchange szakasznak.



9.41 ÁBRA MINTHA EZT MÁR LÁTTUK VOLNA VALAHOLO...

Ezzel ennek a fejezetnek vége is szakad, ellenben lépünk vissza most időben egy kicsit, és folytassuk valami olyannal, amelyre a fiatalabb versenyzők már nem is emékezhettek.

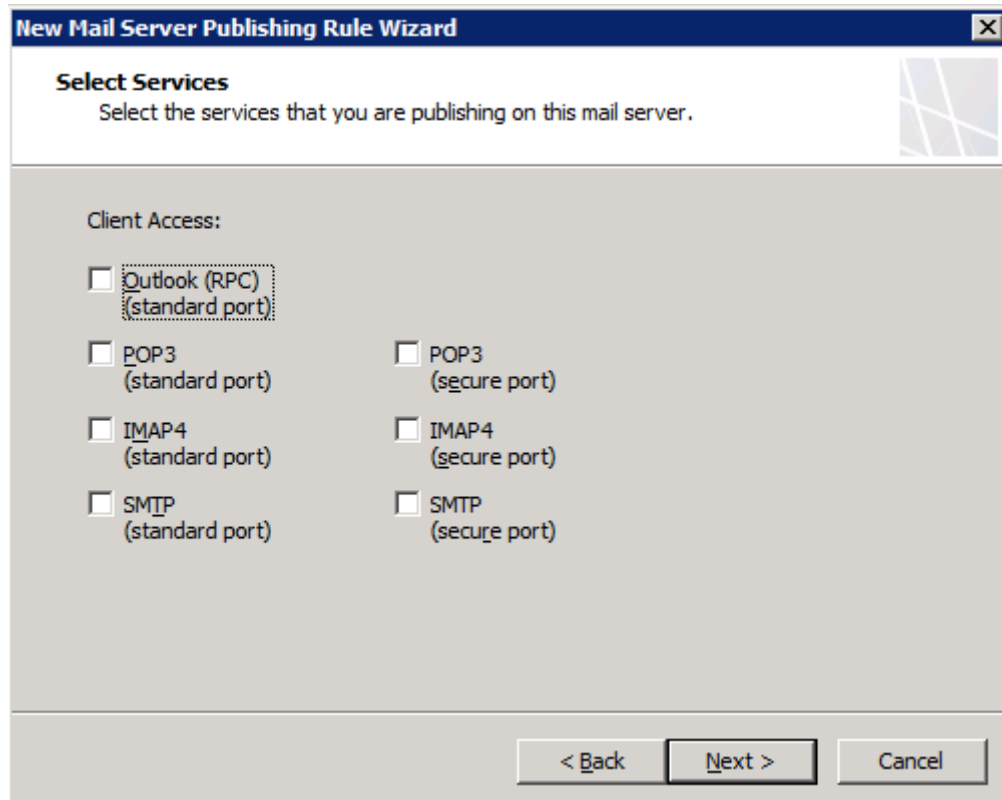
9.3.3 A KLASSZIKUS E-MAIL PROTOKOLLOK PUBLIKÁLÁSA

POP₃, IMAP, NNTP, mind mind velünk van az 1970-es évek eleje óta, de ma már (induljunk ki abból hogy Exchange-ünk van) szerencsére a háttérbe szorultak. A "szerencsére" arra vonatkozik, hogy ezekkel a protokollokkal és a rájuk épülő kliensekkel szinte csak a baj van, nem eléggé biztonságosak (persze van mindegyikből S-es, azaz SSL-el használható változat is, POP₃S, IMAPS), kis tudásúak és kevésbé praktikusak, különösen ha az implementációs kulcsszavak között a "vállalati" és a "csoportmunka" is szerepel⁹³.

De azért, van mikor muszáj használnunk ezeket a protokollokat is egy belső mail szerver kedvéért (ami persze lehet egy Exchange is) miatt. A TMG ahogyan az ISA szerverek is, ezekre a helyzetekre is fel van készítve, nosza publikáljunk hát klasszikus protokollokat.

Ehhez pontosan úgy indulunk, mint az SMTP szervernél (9.31 ábra), csak a második lépésnél válik el az utunk, azaz itt majd a "Client Access: RPC, IMAP, POP₃, SMTP" opciót választjuk. Ha ez megvan, akkor válogatunk.

⁹³ És nem véletlen, hanem jelzésértékű az is, hogy pl. az Exchange 2007-től kezdve a telepítés után a POP₃ és az IMAP szervízek alapesetben nincsenek is engedélyezve.



9.42 ÁBRA A KLASSZIKUS PROTOKOLLOK KIVÁLASZTÁSA
(AZ OUTLOOK RPC IS AZ, DE HASZNÁLNI VPN NÉLKÜL TILOS)

A baloldali oszlop és a jobboldali oszlop között az SSL támogatás a különbség, illetve az Outlook (RPC). Ez utóbbit mostanra már valószínűleg sokan elfelejtették, de ez nem is olyan nagy baj.

Pár mondatot azért mégér: nagyjából az ISA 2000 Feature Pack 1-től kezdve kísérletezett a Microsoft a MAPI kapcsolatok (Exchange vs. Outlook a belső hálón) kiterjesztésével a nagyvilágon, azaz az Interneten keresztül. Ez az elején kissé körülményes volt (az RPC UUID-k alapján történt) és rengeteg pl. dinamikus portot kellett hozzá kitárni a tűzfalban. Mindez a remekül működő "RPC over HTTPS" (ma már Outlook Anywhere) előtt volt, ezért nem nagy baj, ha már elfelejtettük.

Ha bejelöljük a szükséges protokollokat, akkor a következő lépésben már csak meg kell adnunk pl. a belső POP3 szerver IP-jét (ami lehet egy Exchange is) meg a megfelelő hálózatot, ahova figyel majd a TMG, és végeztünk is.

Ezután a TMG automatikusan elkészíti a szükséges tűzfalszabályokat - pont annyit, amennyi protokollt kijelöltünk - és már működik is a belső POP3 szerver. Ha lehetséges, ne kapcsoljuk ki a passzoló alkalmazásfiltereket (POP3, SMTP), mert hasznosak, de más okossággal nem nagyon szolgálhatunk, mert nincs is, ez ilyen egyszerű.

Illetve egy kicsit kapcsolódó dolog azért mégis eszembe jutott: előfordulhat az a rendkívül szélsőséges helyzet is, hogy a klienseink számára az SMTP-t is engedélyeznünk kell egy tűzfalszabállyal (mert pl. a levelezésünk kiszolgáltatását nem mi oldjuk meg helyben, hanem mindezt rábízuk a szolgáltatónkra).

Ekkor ha tűzfal klienset használunk és SMTP-t is adunk a klienseknek, és ezt egy Outlook-kal használják, akkor a tűzfal kliens központi beállításai között (Network\Configure Forefront TMG Client Settings) keressük meg az "Outlook" paramétert és állítsuk a "Disable" értéket o-ra. Amíg ezt nem tesszük meg, az Outlook nem fog leveleket küldeni, hiába kapott lehetőséget az SMTP használatára.

9.3.4 A WEBES KLIENSEK

Elérkeztünk egy komolyabb, népszerűbb és nagyon fontos részhez. És itt már webszerver publikálásról van szó, és nem is akármilyenekről.

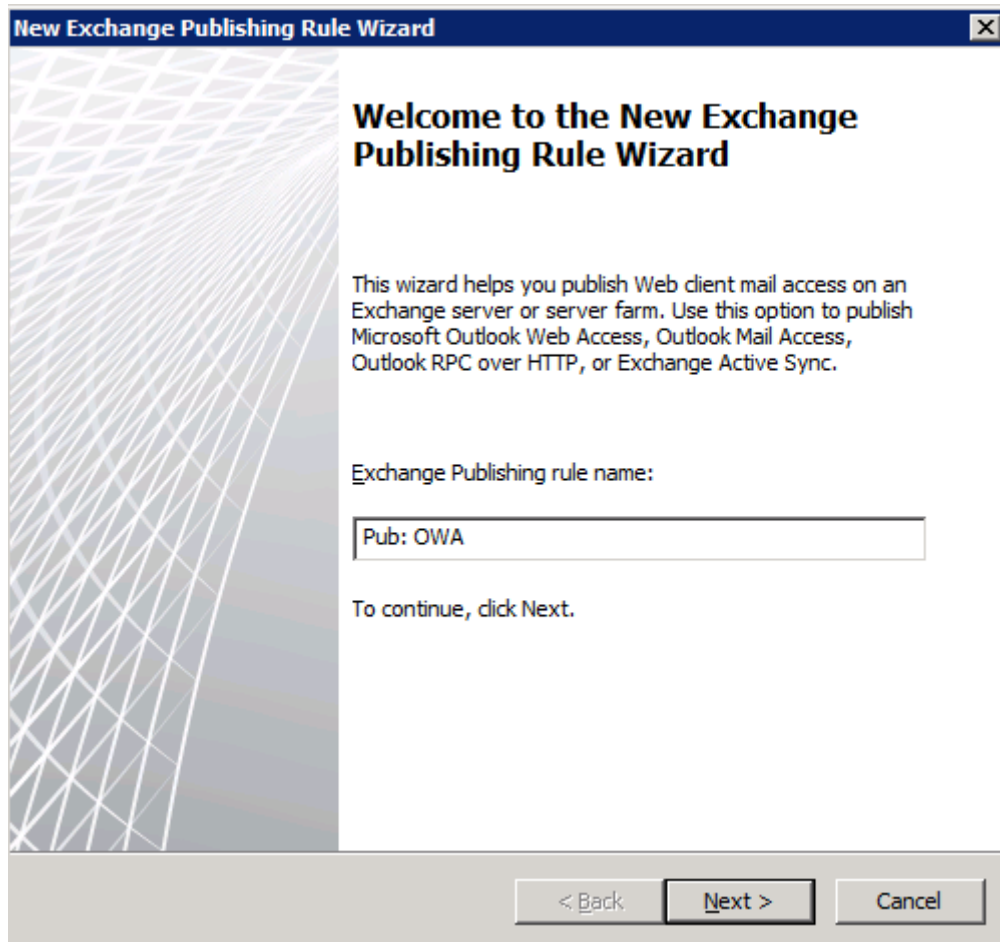
A kliensek típusa alapján újabb három csoportra oszthatjuk tovább a publikáló szabályokat. Szó eshet egyrészt a PDA-k, Smartphone-ok és egyéb kütyük csoportjára vonatkozó elérésről, valamint a webes levelezést megoldó Outlook Web Access-t érintő publikálásról. A harmadik körben az asztali Outlook-ot érintő lehetőségekről kell beszélnünk, a maximálisan ajánlott RPC over HTTP/S-ről vagy ahogyan már egy ideje hívjuk: az Outlook Anywhere-ről.

Egy fontos dokumentum a webes kliensek méretezéséről:

White Paper: Outlook Anywhere Scalability with Outlook 2007, Outlook 2003, and Exchange 2007

[http://technet.microsoft.com/en-us/library/cc540453\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/cc540453(EXCHG.80).aspx)

Ezekhez a megoldásokhoz egy teljesen külön publikáló varázsló áll a rendelkezésre, amelyet például a Firewall Policy helyi menüjéből, vagy a Tasks részből is elérhetünk, a neve: "Publish Exchange Web Client Access". Szaladjunk át ezen most, egyelőre egy OWA publikálás apropóján.



9.43 ÁBRA MOST EGY OWA ELÉRÉST FOGUNK VARÁZSOLNI

Ezután jön a lényeg, el kell döntenünk, hogy az Exchange 2000-től a 2010-ig mely szerveret választjuk, azaz melyik szolgáltatásait szeretnénk használni. Mindent nem lehet egyszerre, pl. egy Exchange 2010 esetén, az OWA, az OA, és az AS az három különböző szabályt, azaz háromszori nekifutást jelent majd ezzel a varázslóval.

Viszont mindháromnál választhatjuk majd ugyanazt a listenert (ugyanazzal a helyesen előkészített tanúsítvánnyal, lásd pl. SAN) és az űrlapos hitelesítést is, de ezt azért beszéljük meg, mert felvet egy-két kérdést.

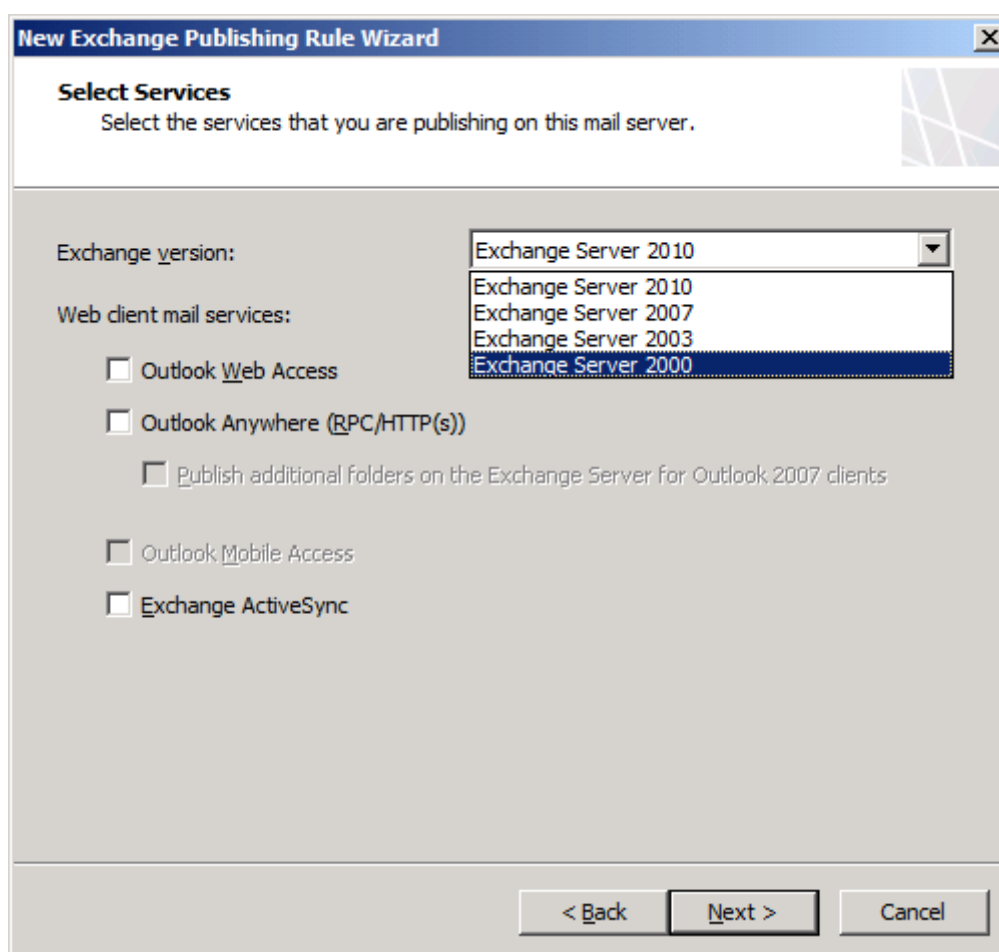
Ahogy már szó volt róla, az űrlap alapú hitelesítés egy nagyon sokrétű, sok extrát felvonultató módszer. Használhatjuk immár multifaktoros hitelesítésre, kontrollálhatjuk a csatolások használatát, felajánlhatunk a felhasználóknak kétféle megjelenítést (basic és premium), alkalmazható az SSO, és beépíthető egy biztonságos jelszó változtatási lehetőség is. A mobil klienseknél különösen jól jöhet, hogy teljesen testreszabhatjuk a felületet, és ezt teljesen automatikusan a fejléc tartalmától függően kaphatják meg a kijelzőre. Kierőszakolhatunk a böngésző beállításaitól független nyelvi támogatást (26

A KAPUN TÚL

féle nyelvből választva), a cookie-kkal kapcsolatban is kapunk jópár lehetőséget, és ha bevállaljuk, akár gyorsítótárazhatjuk is a jelszavakat. Ezek mind-mind olyan megoldások, amelyeket bármelyik Exchange kliens publikálásnál jól jönnek.

Az Outlook Anywhere esetén viszont ez a fajta kliens hitelesítési metódus csak részben lesz tökéletes, mivel egy űrlap kitöltése egy Outlook esetén értelmezhetetlen, viszont ha mégis ezt az utat választjuk, akkor a TMG automatikusan vált a Basic hitelesítésre, ami már jó megoldásnak számít. Így egy csapással három legyet is leütünk.

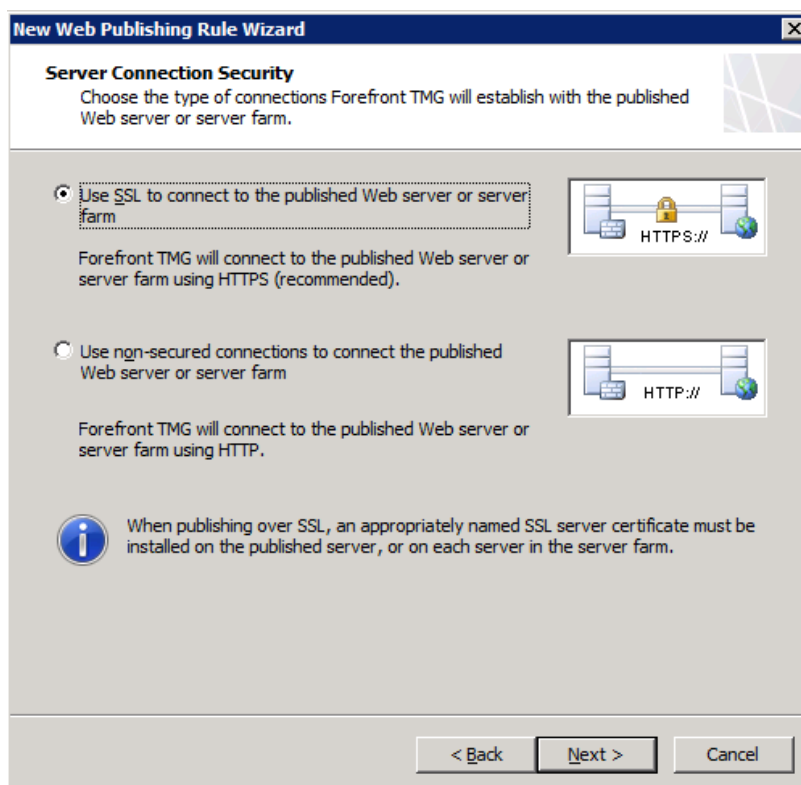
Nos, ennyi kitérő után kanyarodjunk vissza és először válasszuk az OWA-t a varázslóból.



9.44 ÁBRA 4 GENERÁCIÓBÓL VÁLOGATUNK

A listener-rel és az űrlapos hitelesítéssel kicsit előreszaladtunk egyébként, mivel a varázslóban ezek után még a webszerver típusát kell megadnunk (egyszerű webszerver, load balancer vagy farm) majd pedig el kell döntenünk, hogy használunk-e kötelezően titkosítást (SSL) a webszerver elérésére, ami nyilván erősen megfontolandó minden Exchange elérés esetén.

Az SSL alkalmazására az TMG és a belső webszerver között kétfajta, manuális választható módszerünk volt az ISA 2004-ben (Tunneling és Bridging, azaz szimpla továbbítás ellenőrzés nélkül illetve a „szűrési” módszer), és nem maradt egy sem az ISA 2006-ban, de ez kivételesen előrelépésnek számít. Tudniillik ennek az opciónak a beállítása automatikussá vált, és minden esetben - tehát az OWA-val is, - működik a szűrés, ha kérjük a tikosítást.⁹⁴



9.45 ÁBRA AZ ISA 2006-TÓL KEZDVE VÁLASSZUK AZ SSL-T ÉS MEGKAPJUK VELE AUTOMATIKUSAN A LEGJOBB MÓDSZERT

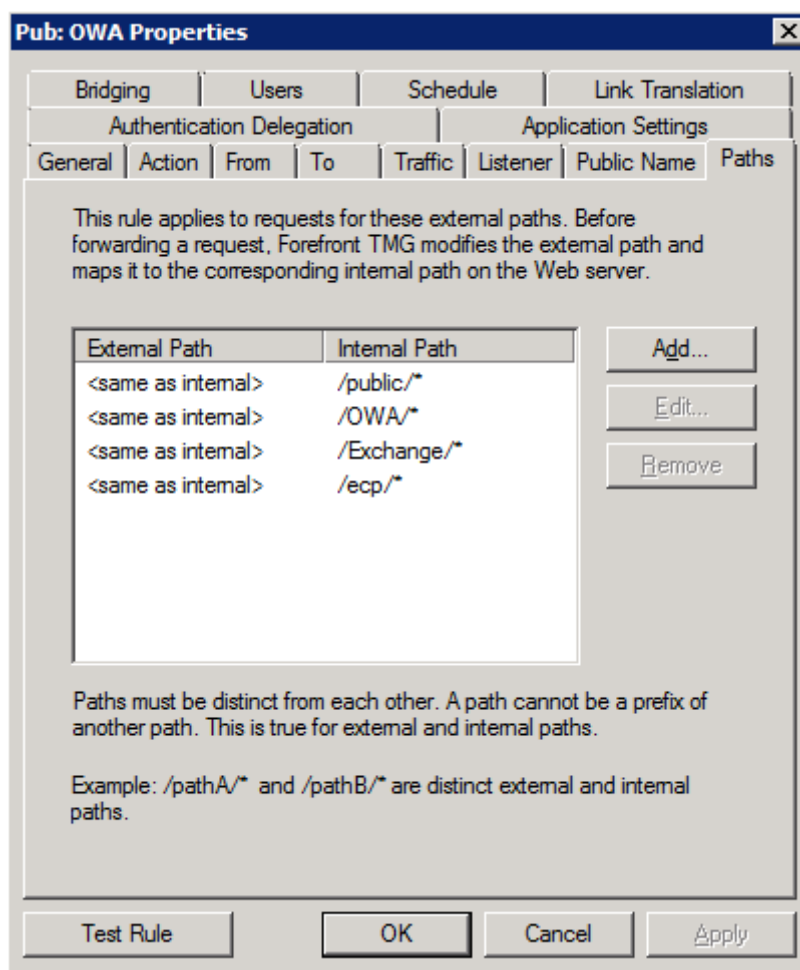
Az SSL Bridging (ne keverjük össze a webszerver publikáló szabályban látható Bridging füllel) megértéséhez tudnunk kell, hogy ez gyakorlatilag a HTTPS Inspection előzménye, amellyel viszont a TMG előtt csak a saját publikált webszervereinkkel operálhattunk. Egy SSL alapú OWA forgalom esetén a felhasználó böngészőjét futtató gép és a TMG között felépül egy SSL kapcsolat és egy ettől független egy második SSL kapcsolat is a TMG és a publikált Exchange CAS kiszolgáló között. A böngésző és TMG kapcsolatában a böngésző lesz az SSL kliens a TMG kiszolgáló pedig az SSL szerver. A TMG kiszolgáló és az Exchange kapcsolatában pedig a TMG kiszolgáló lesz az SSL

⁹⁴ És az igazán szép a dologban az, hogy a minimum ISA 2006 + a régi-régi Exchange 2003 SP2 esetén ez az ActiveSync-kel is működött, tanúsítvány alapú hitelesítéssel. De az már régi történet.

A KAPUN TÚL

kliens és az Exchange kiszolgáló az SSL szerver. Ezután a publikáló szabály típusától függően újra titkosít (vagy nem, azaz adott esetben http-ként küldi tovább) és csak ezután kapja meg az Exchange szerver a kérést. Ha minden rendben van most is, akkor mehet a csomag a távoli kliens felé (természetesen anélkül, hogy ez ebből bármit észlelne).

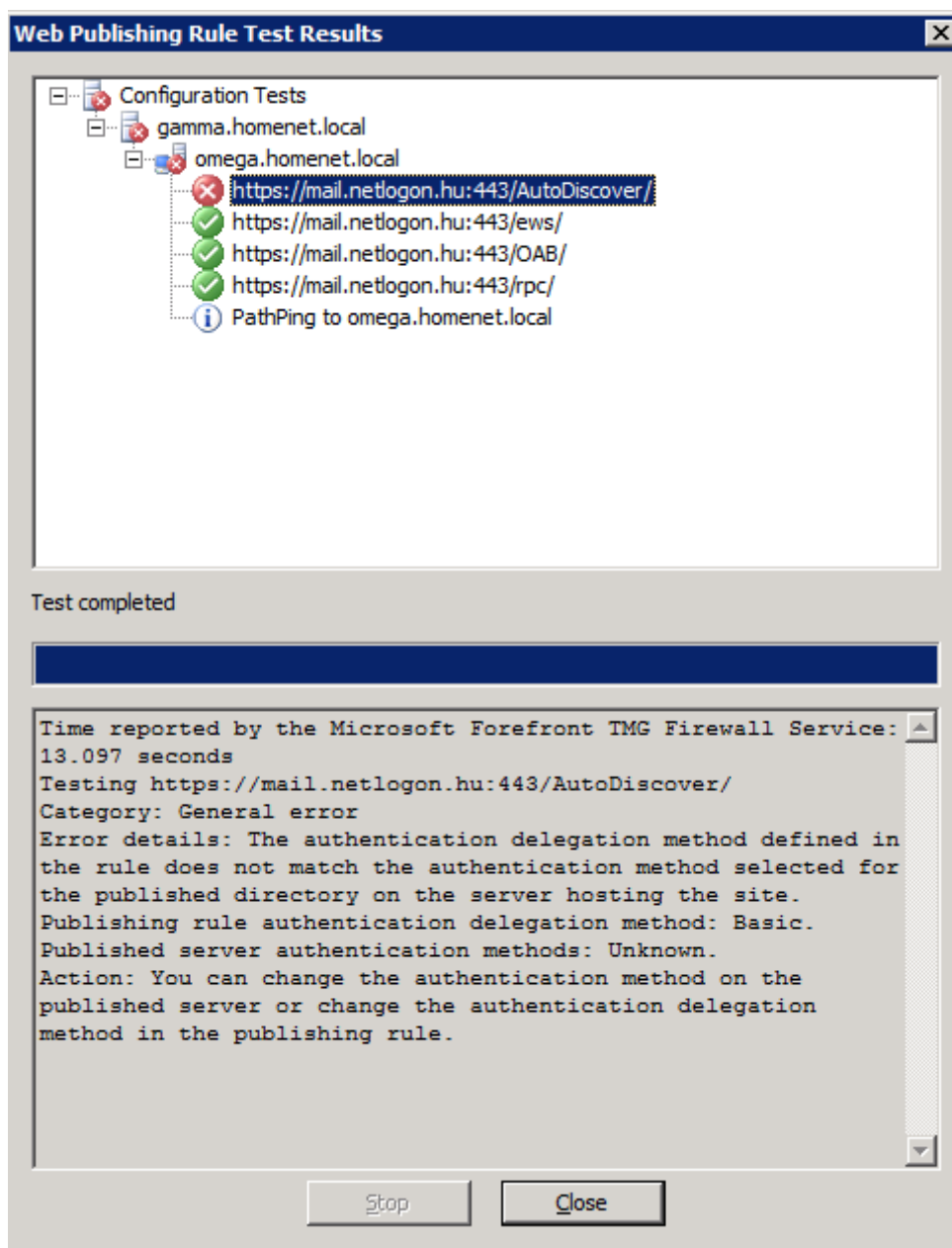
Nos, ezek után térjünk vissza a varázslóra, de már csak azért, hogy megállapítsuk, hogy innentől nincs új opció, minden a normál (az előző részben ismertetett) webszerver publikáláshoz hasonlóan megy végbe. A végeredmény pedig a sima SSL webszerver publikáló szabályhoz nagyon hasonló lesz, 1-2 eltéréssel. Az egyik eltérés a következő ábrán látható.



9.46 ÁBRA A VIRTUÁLIS MAPPAK AZ OWA PUBLIKÁLÓ SZABÁLYBAN

Az Outlook Anywhere és az ActiveSync publikálás lépései teljesen hasonlóak, ergo további kifejtést nem nagyon igényelnek. Ellenben a tesztelés ezeknél itt is sokat segíthet, például abban, hogy kiszűrjük a listener-ünk és az Exchange alatt futó IIS hitelesítési metódusainak pontosabban ezek delegálásának eltérő beállításait. A

következő ábrán az Outlook Anywhere publikáló szabály tesztelése (és persze így az ehhez passzoló virtuális mappák is) látható.



9.47 ÁBRA DIREKT RONTOTTAM EL AZ IIS-BEN A HITELESÍTÉST, ÉS JÓL LÁTSZIK A PROBLÉMA

És végül ez Exchange webes kliensek fejezet lezárásaképp a következő táblázat szolidan összefoglalja az Exchange 2000-től kezdve az összes elérhető Exchange szolgáltatást illetve ezek kötelezően publikálandó virtuális mappáit. Igazából csak az ellenőrzés miatt van ennek értelme, hiszen a TMG pontosan tudja, hogy mely verziónál és szolgáltatásnál mely virtuális mappákat kell belepakolni a publikáló szabályba.

9.2 TÁBLÁZAT MINDEN AMI SZEM SZÁJNAK INGERE

	Exchange 2000	Exchange 2003	Exchange 2007	Exchange 2010
Outlook Web Access	/public/* /exchweb/* /exchange/*	/public/* /exchweb/* /exchange/*	/owa/* /public/* /exchange/* /exchweb/*	/owa/* /public/* /exchange/* /exchweb/* /ecp/*
RPC over HTTPS (OA)	/rpc/*	/rpc/*	/rpc/*	/rpc/*
Outlook Mobile Access	Not Supported	/OMA/*	Not Supported	Not Supported
Exchange Active Sync	/Microsoft- Server- ActiveSync/*	/Microsoft- Server- ActiveSync/*	/Microsoft-Server- ActiveSync/*	/Microsoft- Server- ActiveSync/*
RPC over HTTP with Publish additional folders on the Exchange Server for Outlook 2007 clients selected	Not Supported	Not Supported	/unifiedmessaging/* /rpc/* /OAB/* /ews/* /AutoDiscover/*	/rpc/* /OAB/* /ews/* /AutoDiscover/*

Nos, ezzel végére értünk ennek a monstre nagy fejezetnek. 52 oldal, 47 ábra, és 2 táblázat kísért a publikálás témakörét. Ezek után ismét csak azzal fogunk foglalkozni, hogy kit és hogyan engedünk be, de egészen más körülmények között.

10 TÁVOLI ELÉRÉS: VPN ÉS NEM VPN

Bevezetésképpen hadd ékeskedjek idegen tollakkal. A szerzői jogok megsértése nélkül, hadd közöljek egy részletet egy régi-régi inetpubos és MVP kollégám Petrényi József legújabb hálózatos könyvéből (a forrás linket lásd később).

"El sem hiszed, de megint csatornázni fogunk.

Azért ejtsünk előtte pár szót arról, hogy mit is értünk Virtual Private Network, azaz VPN alatt.

Hát, alapvetően azt, amit az angol név is sugall. Van egy védett (private) hálózatunk és van ezen kívül a vad külső világ. A védett hálózatunkban mindenki barát, a social engineering művelőit már a portás főbe lövi a bejáratnál, szóval itt tényleg magunk között vagyunk, sokkal lazábbak lehetünk.

De ójaj, embereink időnként kénytelenek kimerészkedni a nagyvilágba. természetesen a laptopjaikkal meg a mindenféle kutyüikkel együtt. Mondtam már, hogy nekünk borzasztó perverz embereink vannak? Képesek arra, hogy egy fárasztó nap után a távoli szállodából is szeretnének a belső hálózat ólmelegében lubickolni egy cseppet. Nem is beszélve azokról az embereinkről, akik akár munkaidőn kívül, akár azon belül a kényelmes otthonukból szeretnének dolgozni.

Nyilván felmerül az igény, hogyan lehetne a belső biztonságos hálózat határait úgy kihúzni, hogy távoli pontokra is elérjen. Úgy, hogy a két pont között a kiszámíthatatlan közeg, az internet jelenti az átviteli közeget."

Finoman szólva is eltérő stílust képviselünk, ha az írásról van szó ☺, de a probléma vázolásában viszont nincs különbség. Adott egy belső hálózat, amelyet akár teljes egészében el kell érni a külsőből. Előfordulhat, hogy csak egyetlen gépről, és az is, hogy két hálózatot kell összekötnünk. És immár az is, hogy nem használhatjuk a klasszikus VPN protokollokat (PPTP, L2TP), hanem valami újabbra, egy tűzfalbarátabb megoldásra van szükségünk. Sőt, a legeslegújabb és a mostanság a legelképesztőbb technológiát, az "észrevétlen" VPN-t, a DirectAccess-t akarjuk használni. Nos, minden esetben segíthet rajtunk a TMG. Az ISA Server is, de csak egy darabig tartja a lépést, ugyanis ezen a területen ismét sok újdonsággal számolhatunk.

10.1 HOGYAN FARAGJUNK VPN SZERVERT A TMG-BŐL?

A TMG (és az ISA) nem "a" VPN szerver. Az alap VPN szerver tudást az operációs rendszer adja. Ez elsősorban akkor lesz majd fontos, ha nem működik rendesen, ilyenkor az RRAS szerverünket kell sűrűn nézegetnünk. A TMG a VPN szerepkörhöz

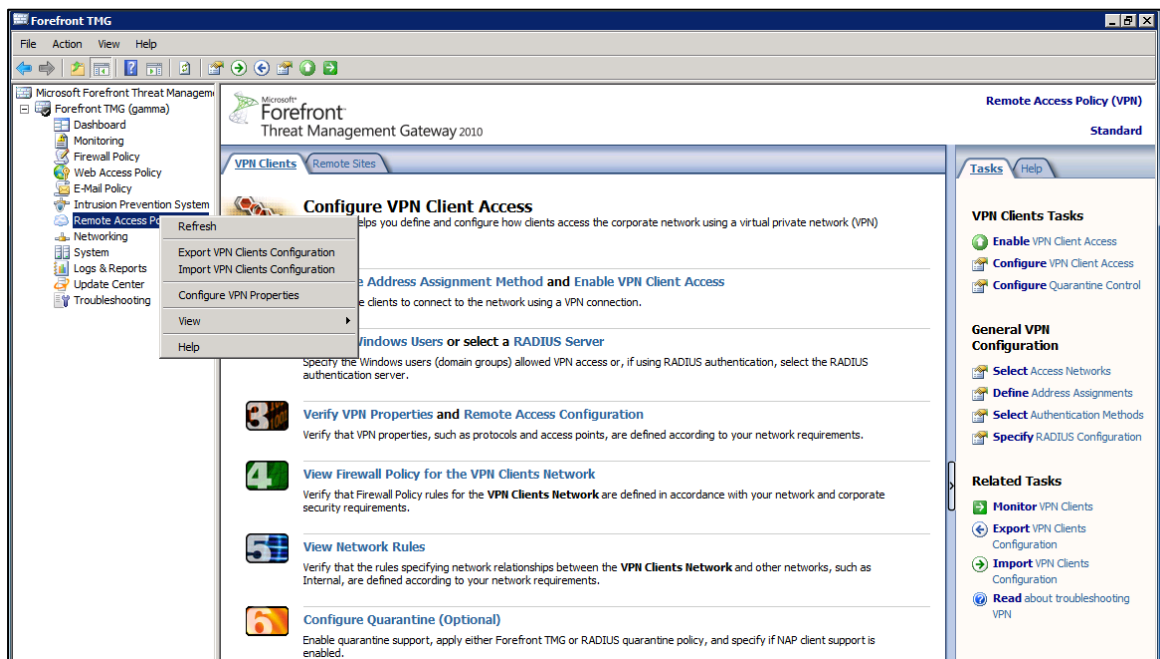
A KAPUN TÚL

egyrészt a komplex kezelőfelületet adja (szóló és telephelyek közötti kapcsolatoknál is), másrészt a saját jóságait, azaz pl. a speciális hálózatokat (VPN Clients, Quarantined VPN Clients) és a hálózatok kezelésben rejlő rengeteg lehetőséget (pl. egy VPN kliensre vonatkozó hozzáférési tűzfalszabályok), valamint a tűzfal és a web proxy által nyújtott már eddig is sokszor említett szolgáltatásokat.

Mondok egy egyszerű példát: az ISA Server 2004 óta a stateful inspection, a "háromujjas kézfogással" a VPN kliensekre is működik.

Kezdjünk el konkretizálni és a VPN kliensek típusainak illetve a VPN szerverek működésének áttekintése nélkül (ezeket a fenti linken megtaláljuk am PPTP-től kezdve az SSTP-n át egészen a legújabb a Windows 7-ben debütáló IKEv2 kliensig) tekintsük meg, hogy a TMG-ből hogyan faragunk gyorsan és egyszerűen egy VPN szervert.

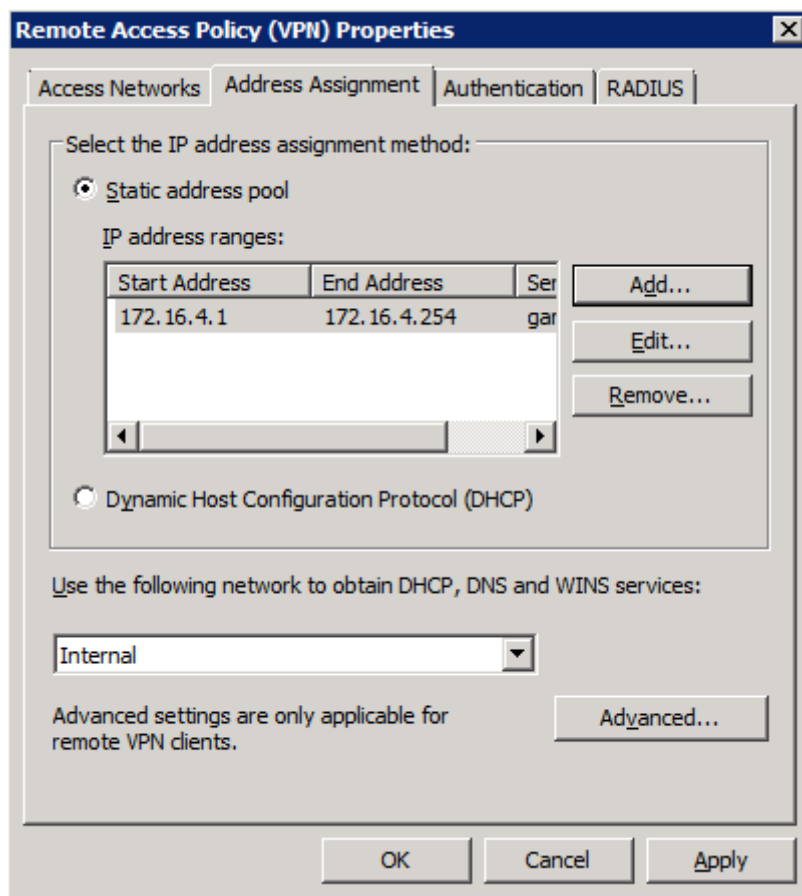
Akármilyen VPN kliens fogadásra készülünk, először a közös VPN szerver beállításokat kell rendbe raknunk. Ezt a szakaszt a TMG-ben a baloldali keret egy dedikált pontjában érhetjük el, amely neve: Remote Access Policy (VPN). Ha erre kattintunk, akkor a középső keretbe megérkezik egy színes-szagos 6 lépéses konfigurálási útmutató, amit most hagyjunk (már csak azért is mert nagyjából 1 panel összes opciója van ide kivezetve), e helyett kérjük a helyi menüt ezen a ponton és nézzünk be a "Configure VPN Properties" pont alá.



10.1 ÁBRA BALRA, JOBBRA ÉS KÖZÉPEN – MINDENHOL VPN VAN

A már unalmas "Access Networks" fül alatt azokat a hálózatokat pipáljuk be, ahonnan lesz majd lehetőség a VPN használatára (elégge egyértelműen az External vezet itt, de

azért nem mindig van egyedül). A következő azaz az "Address Assignment" fül már több mindent megenged.



10.2 ÁBRA HOGYAN ÉS KITŐL KAP MAJD IP-T A KLIENS?

Az nyilvánvaló, hogy a VPN kliens egy megfelelő a belső hálózatba "belátó" IP nélkül nem sokat ér, dehogya ahhoz pl. a különböző névfeloldási mechanizmusok is biztosan megfelelően működjenek, itt bele kell piszkálnunk kicsit a konfigurációba.

Először is ha van DHCP szerverünk, akkor akár kijelölhetjük arra a feladatra, hogy a VPN klienseknek is ossza ki a jól megérdemelt IP konfigurációt⁹⁵. De a statikus címzés lehetősége is előttünk áll, ekkor két dologra kell nagyon oda figyelnünk:

1. Semmilyen a TMG-ben már szereplő IP tartományt nem használhatunk, ergo válasszunk ki egy szomszédost, és az útválasztást a TMG majd elintézi.
2. Minimum annyi cím és még 1 db kell, mint amennyi darab VPN klienst engedélyezünk majd később.

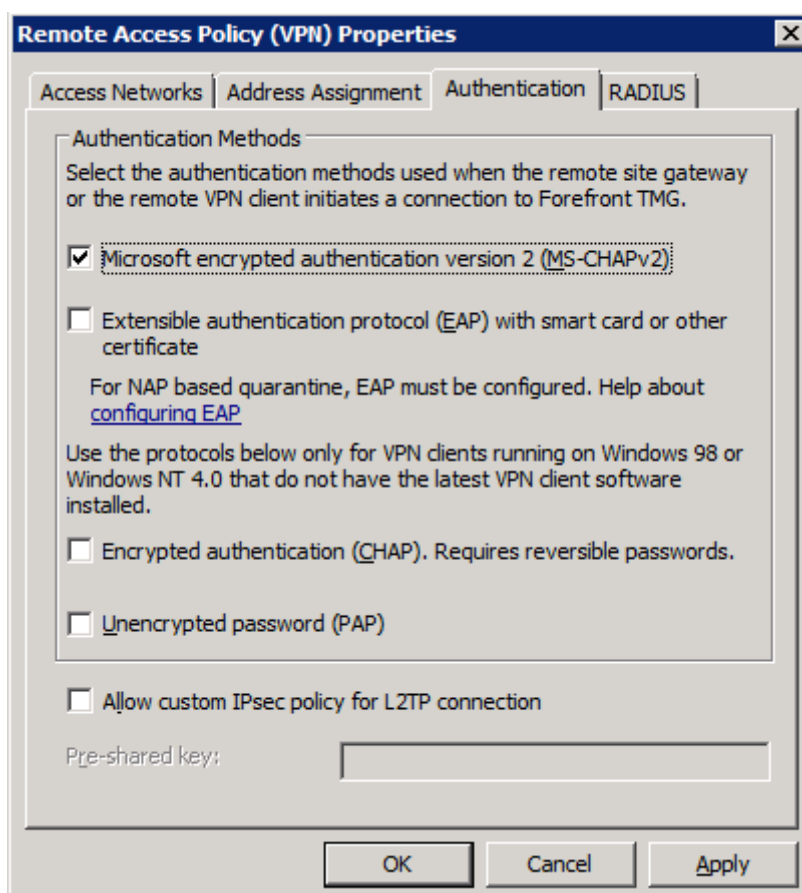
A DHCP használat előnye az egyszerűség, nincs gond a route-olással, és az eléréssel, ilyenkor a VPN kliensek teljes mellszélességgel a belső hálózat IP tartományának tagjai

⁹⁵ De nem mindig, ha az Enterprise verziót és így pl. tömböket használunk, akkor nem.

lesznek, a TMG pedig egy ARP proxyként működik ezen kliensek szempontjából, pl. abból az apropóból amikor is a belső hálózat gépei ARP kérésekkel bombázzák majd a VPN klienseket. A másik eset akkor él, ha pl. nincs DHCP szerverünk, vagy éppen nem használható erre a célra.

A "Use the following network to obtain DHCP, DNS, and WINS services" pont alatt közölhetjük a TMG-vel, hogy melyik hálózati interfész felé tolja tovább a DHCP kérést, (ez ugye tipikusan az Internal lesz), aztán ezt az "Advanced" gomb alatt tovább finomíthatjuk, azaz az alternatív DNS és WINS szerverek címeit itt vehetjük fel.

Az "Authentication" fül is kötelező pont a látogatásunkkor, bár az alapértelmezés is megfelelő, így ha nem nyúlunk hozzá, akkor is rendben leszünk.

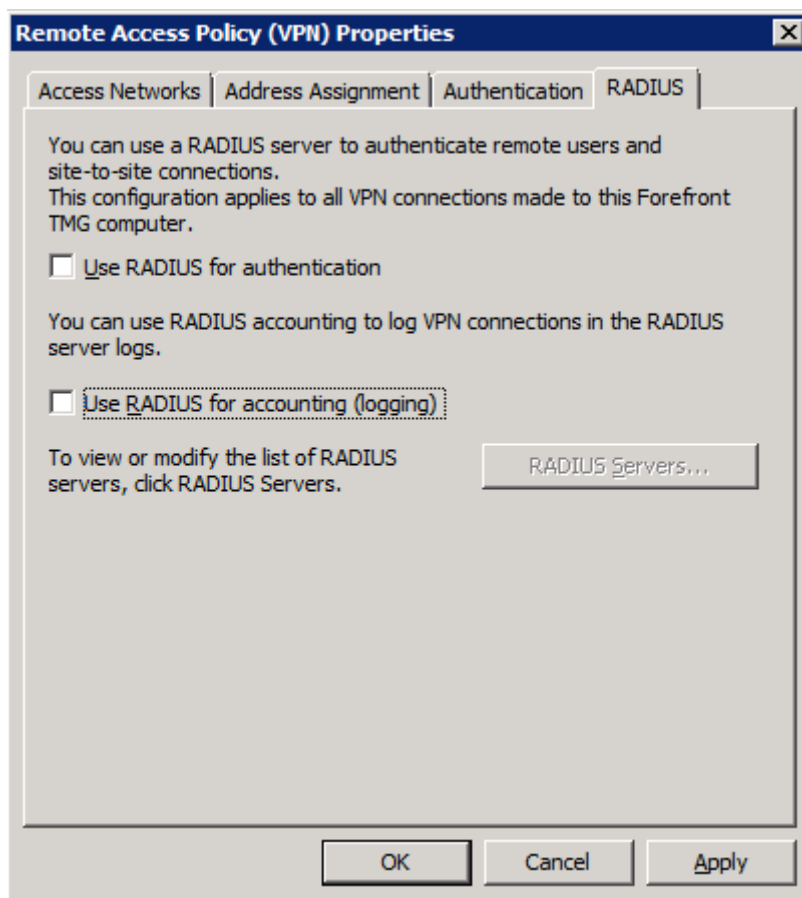


10.3 ÁBRA A HITELESÍTÉSI METÓDUSOK ITT IS JELEN VANNAK

Itt ugyanis a kapcsolódáskor szükséges hitelesítési metódusok között választunk. Normál, azaz nem multifaktoros hitelesítés esetén az MS-CHAPv2 megfelelő, az EAP akkor lesz a barátunk, ha smartcard-os vagy egyéb tanúsítványos megoldást tervezünk a klienseink számára. Ennél lejjebb viszont en adjuk, bár a kompatibilitás miatt (Apple, Linux, Unix) szükség lehet a CHAP, vagy a legrosszabb esetben a PAP metódusra, tudunk kell, hogy ezek ma már abszolút nem megfelelőek biztonsági szempontból, és ezért abszolút módon hanyagolandóak is.

Ami még itt szerepel, az az "Allow custom IPSec policy for L2TP connection. Erre akkor lesz szükség, ha egy olyan L2TP/IPSec VPN szervert kreálunk, amely nem a megszokott módon tanúsítványokkal működik, hanem egy lényegesen alacsonyabb biztonsági szinten, egy előre megosztott jelszóval. Nos, ez gépeljük be itt.

A következő lépésben egy általában nem mindennapos módon oldjuk meg a kliensek hitelesítését. Amellett, hogy a RADIUS névteret használhatjuk a webes publikálásnál és a web proxy hitelesítésénél is, a VPN felhasználók számára is rendelkezésre áll. Ha ez a megkívánt felállás, és nem a megszokott, az Active Directory-ban leledző adatok alapján szeretnénk a hitelesítést lebonyolítani, akkor ennek az engedélyezéshez be kell állítani a RADIUS szerverek címét és portját a "RADIUS Servers... gomb alatt" (ez ugye Windows OS esetén egy belső IAS, vagy mostanság már NPS szerver lesz, amelyek egy teljesen RFC kompatibilis RADIUS szervereknek számítanak), és ilyenkor a TMG-nk egy RADIUS kliensként szépen továbbítja is a beérkező autentikációs csomagokat, aztán fogadja a visszajövő utasításokat, és ennek megfelelően engedi vagy tiltja a VPN kliens csatlakozási kérelmét.



10.4 ÁBRA HA EZT A MÓDSZER VÁLASZTJUK, MÁST NEM LEHET!

A KAPUN TÚL

Van azért még több más előnye is a RADIUS-nak a hitelesítés lebonyolításán kívül, mégpedig a "számlázás" (azaz az Accounting), azaz a rendszerben eltöltött idő mérése, valamint pl. a "User Mapping", amelyről hamarosan szó lesz.

Ezen hitelesítési metódusokról a következő oldalon további részleteket is megtudunk ([http://technet.microsoft.com/en-us/library/cc785072\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc785072(WS.10).aspx)), de Petrényi József különböző TCP/IP könyveiben is rengeteg helyen (és szemléletesebben is mint itt) előfordulnak - beleértve a RADIUS-os részeket is.

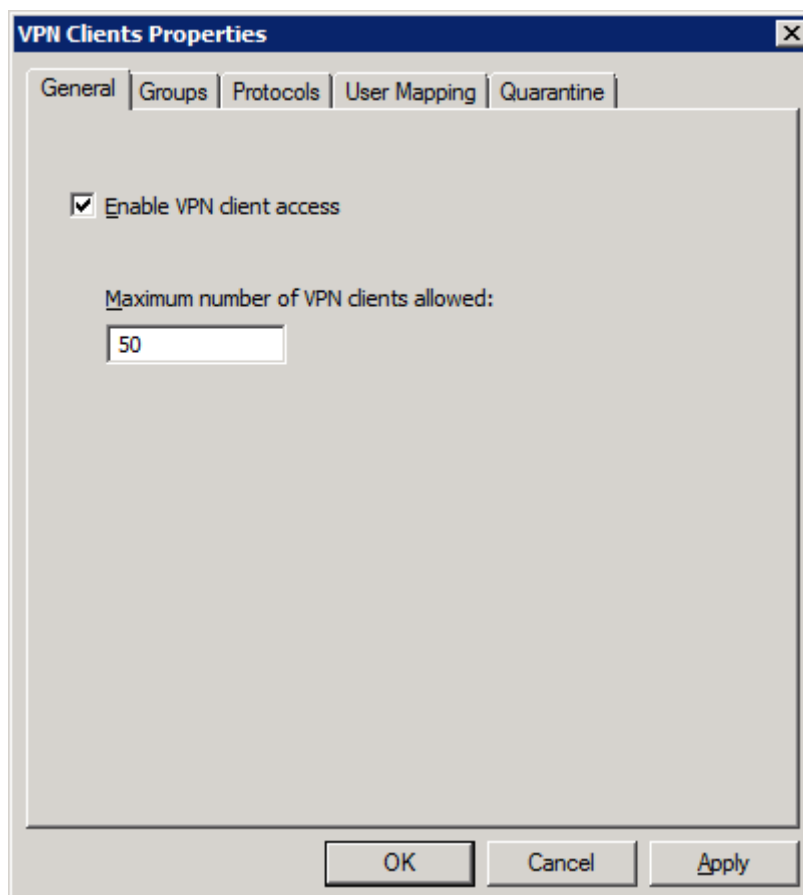
Petrényi József: TCP/IP alapok, 1. kötet v2.0

<http://www.microsoft.com/hun/technet/article/?id=3effd5d3-139c-471a-adeb-a71a6885562f>

Petrényi József: TCP/IP Alapok, 2. kötet v1.0

http://download.microsoft.com/download/5/8/8/5886EEBo-BFB5-4854-9D17-AAEDE66825D3/tcpip_v2/tcpipalapok-1-v2o.pdf

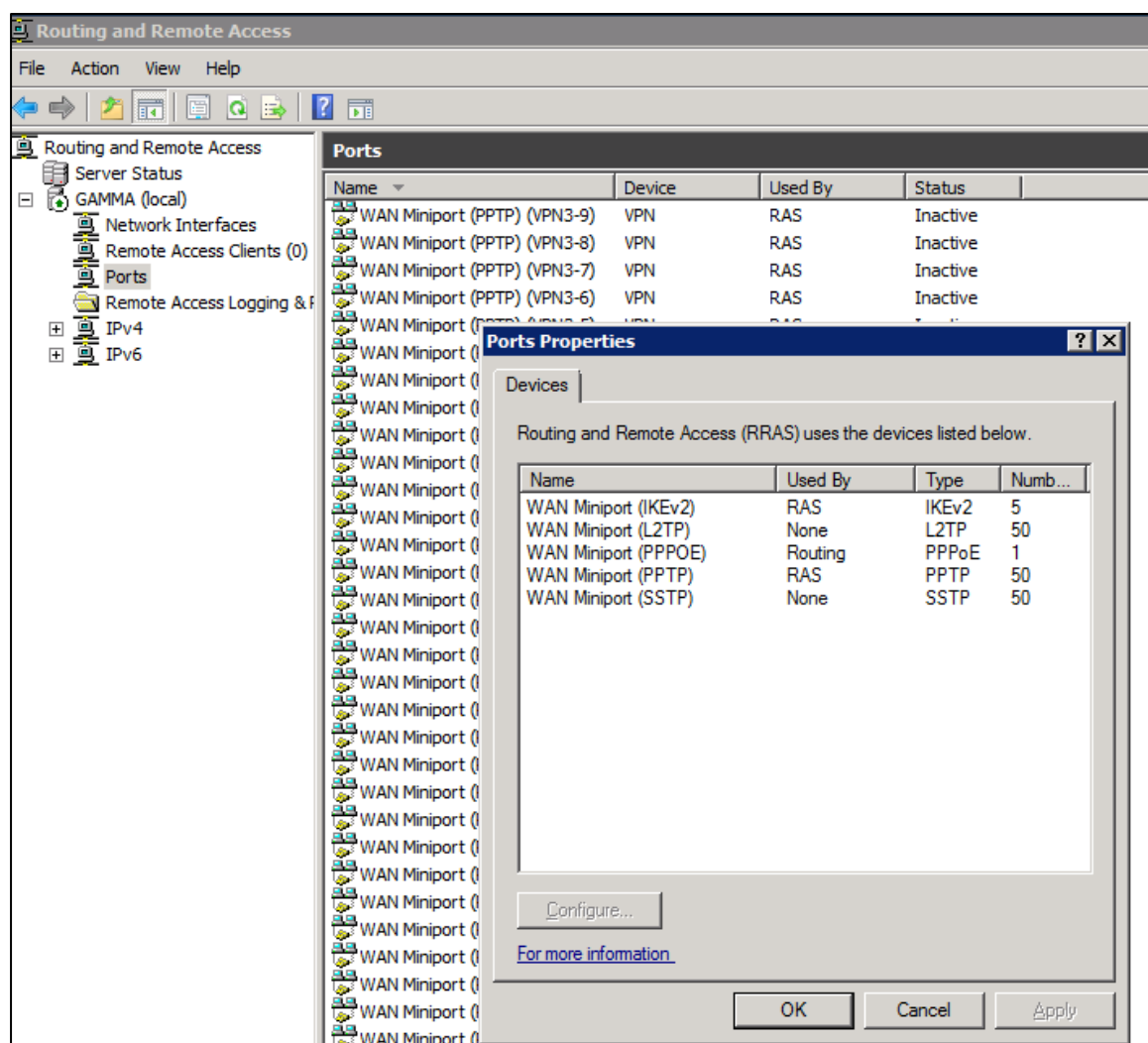
De még mindig nem működik a TMG VPN szerverként, ehhez még egy adag beállításon túl kell esnünk, méghozzá a kliensekkel kapcsolatos közvetlen beállításokon.



10.5 ÁBRA EZ EGYSZERŰ MINT A 6-OS CSAVAR

Ezt a faszerkezetben ugyanonnan indítjuk mint az előbb a globális beállításokat, azaz a "Remote Access Policy (VPN)" keretből, de nem ennek a helyi menüjéből, hanem az Action Pane "Configure VPN Client Access" pontja alól.

Az előző ábra tanúsága szerint az első szakasz valóban nem bonyolult, azt viszont tudnunk kell, hogy ha pl. 50-et írok be a kliensek számához, akkor az 50 db PPTP, L2TP, SSTP és 5 db IKEv2 VPN portot jelent majd, ha 500-at, akkor 3x500-at plusz ugyanúgy 5 IKEv2-t (már persze ha WSo8 R2-ről van szó, mert ha csak WSo8-ról, akkor a legutóbbi VPN típus nincs is). Mindezt itt nem, ellenben az RRAS-ban megtekinthetjük.

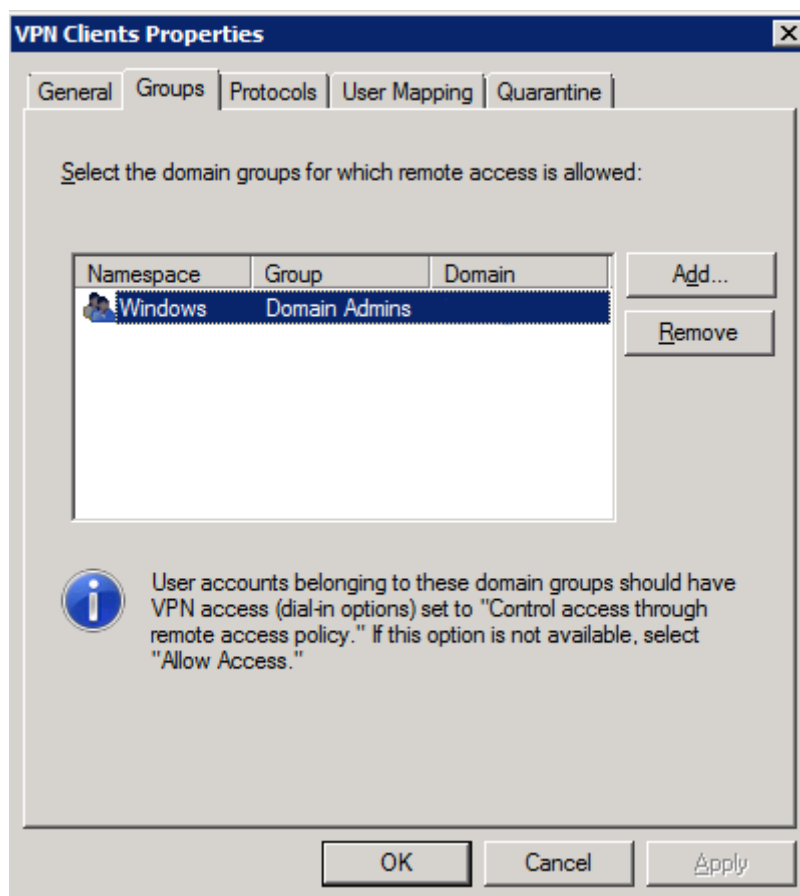


10.6 ÁBRA RRAS ÉS A VPN PORTOK

Még valamit a számokról: tudtuk azt pl., hogy a Standard verziójú Windows szerver OS-ekben van egy felső limit a bejövő VPN kapcsolatokra? Van bizony, és ez pedig konkrétan 250, és ez akkor is él, ha a TMG-vel bonyolítjuk a VPN-t. Az Enterprise-ban már nincs ilyen korlát.

A KAPUN TÚL

Na de próbáljunk meg nem nagyon eltérni a témától. A "Groups" fül jön, ami szintén nem őrült bonyolult, itt adjuk meg azokat a csoportokat vagy szélsőséges esetben felhasználói fiókokat, akik jogosultak VPN kapcsolatot összehozni.

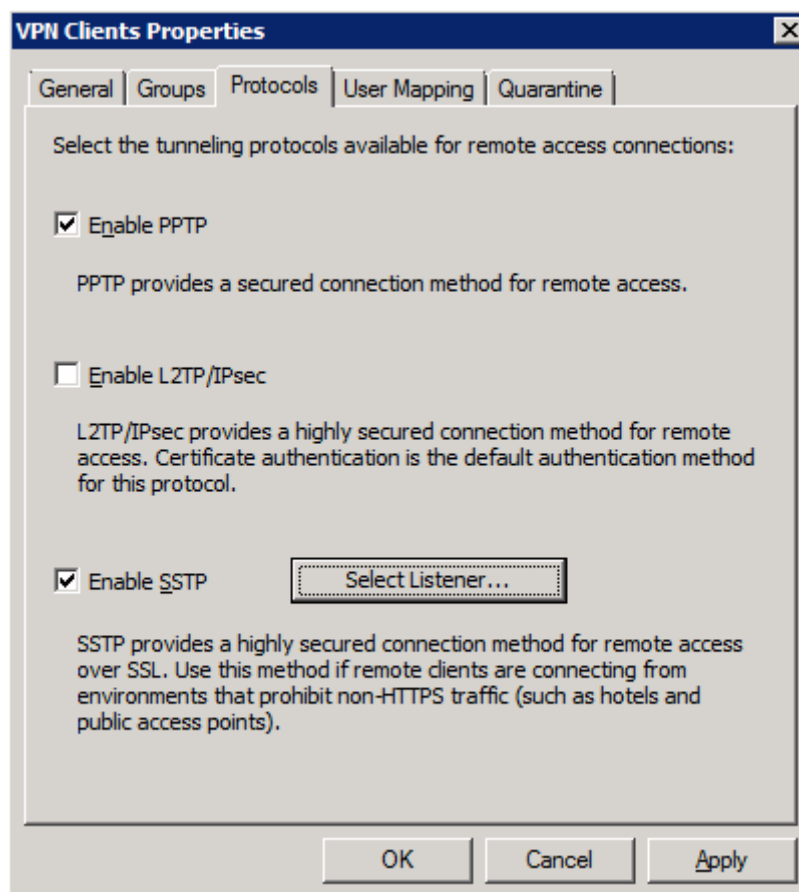


10.7 ÁBRA RRAS ÉS A VPN PORTOK

Tipikusan ez egy AD csoport⁹⁶, amely tagsági ellenőrzése könnyű lesz, hiszen a TMG is bent van a tartományban. Persze felvehetjük a TMG helyi felhasználói adatbázisából a megfelelő fiókokat is, de ez a kevésbé praktikus módszer. Ám van még egy fontos tudnivaló az AD-s csoport esetén: az ADUC-ban az adott felhasználó tulajdonságlapján a "Dial-in"fül alatt, a "Network Access Permission" szakaszban mindenképpen a "Control access through NPS Network Policy" gombnak kell bekattintva lennie. Nagyon azért ne aggódjunk emiatt a Windows Server 2003-as erdő működési szinttől ez az alapértelmezés, de ha nem, akkor ez legyen (vagy persze az "Allow Access" is megfelelő).

Most jön a számunkra megfelelő VPN protokollok kiválasztása, itt egy újdonsággal rögtön szembesülhetünk az ISA 2006-hoz képest, ugyanis lett egy SSTP opció is.

⁹⁶ a következő ábrán is az, csak a domain nevét kiradiroztam ☺



10.8 ÁBRA PPTP/L2TP/SSTP?

Sőt, nemcsak egy választási lehetőség, hanem a tervezett használat esetén azonnal egy HTTPS listener-t is hozzá kell rendelnünk. Még hozzá egy olyat, amelyben egy megfelelő tanúsítvány van, amely egyik legfontosabb tulajdonsága - a szokásos kritériumokon kívül - a CRL információk helyes és pontos lelőhelye kell hogy legyen⁹⁷. Ugyanis az SSTP kapcsolat felépülése során ez az egyik kritikus pont ez az ellenőrzés. Egyébként a TMG előtt az ISA-val egy akkor már létező SSTP server publikálása (ez ugye a WSo8 <> Vista SP1 verziók óta működhet) nem volt éppen egy egyszerű folyamat.

Ha ebben a kényszerhelyzetben vagyunk, akkor ez a segítség jól fog jönni:
 Publishing a Windows Server 2008 SSL VPN Server Using ISA 2006 Firewalls
<http://www.isaserver.org/tutorials/Publishing-Windows-Server-2008-SSL-VPN-Server-Using-ISA-2006-Firewalls-Part1.html>

Most viszont az, gyakorlatilag itt az engedélyezésen illetve a listener megadásán kívül mással nincs dolgunk (ti. a System Policy-ban az SSTP szabály ekkor automatikusan

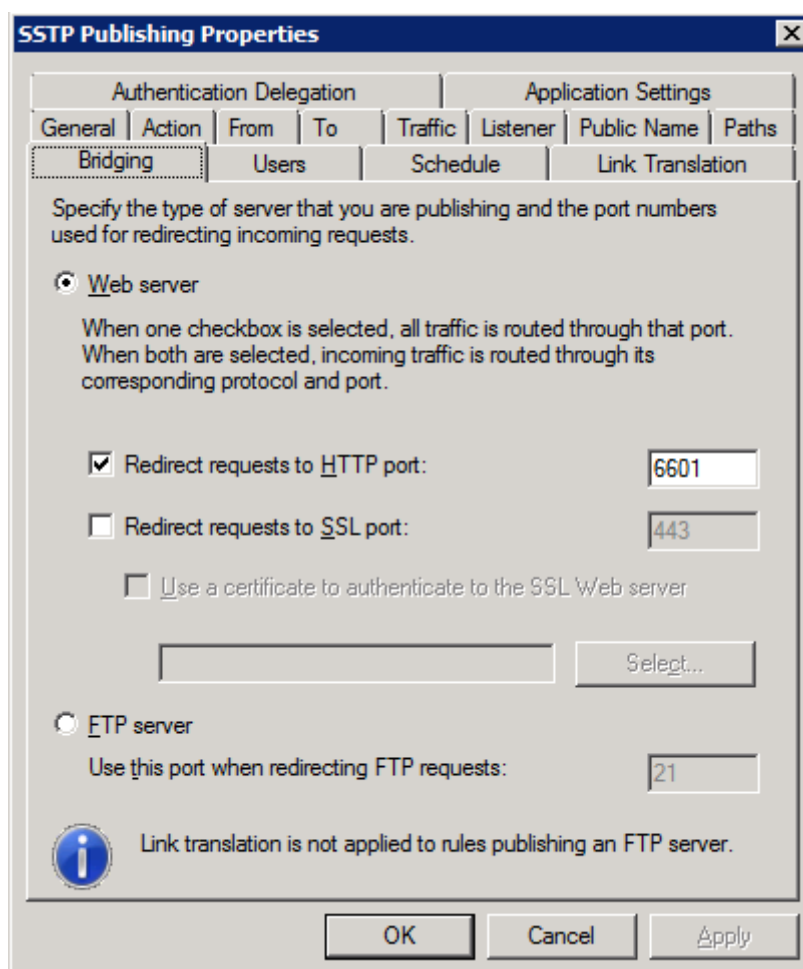
⁹⁷ A megfelelő hitelesítési metódus viszont ebben a listenerben a „No Authentication”.

A KAPUN TÚL

élesedik). És ez öröndetes változás, mert így könnyedén kihasználhatjuk az SSTP előnyeit.

A SSTP konfiguráció egyébként két nagy komponensre épül: az RRAS-ra és a HTTP.SYS-re, a TMG pedig a következőképpen használja ezeket:

- RRAS: elfogadja az SSTP kapcsolatokat és pl. definiálja - a már látott módon - az ilyen típusú kapcsolatok számát.
- HTTP.SYS: a TCP 6601-s porton figyel, azaz a TMG egy SSL terminátorként működve továbbítja a 443-as portra érkező forgalmat a 127.0.0.1-re és az említett 6601-es portra.⁹⁸



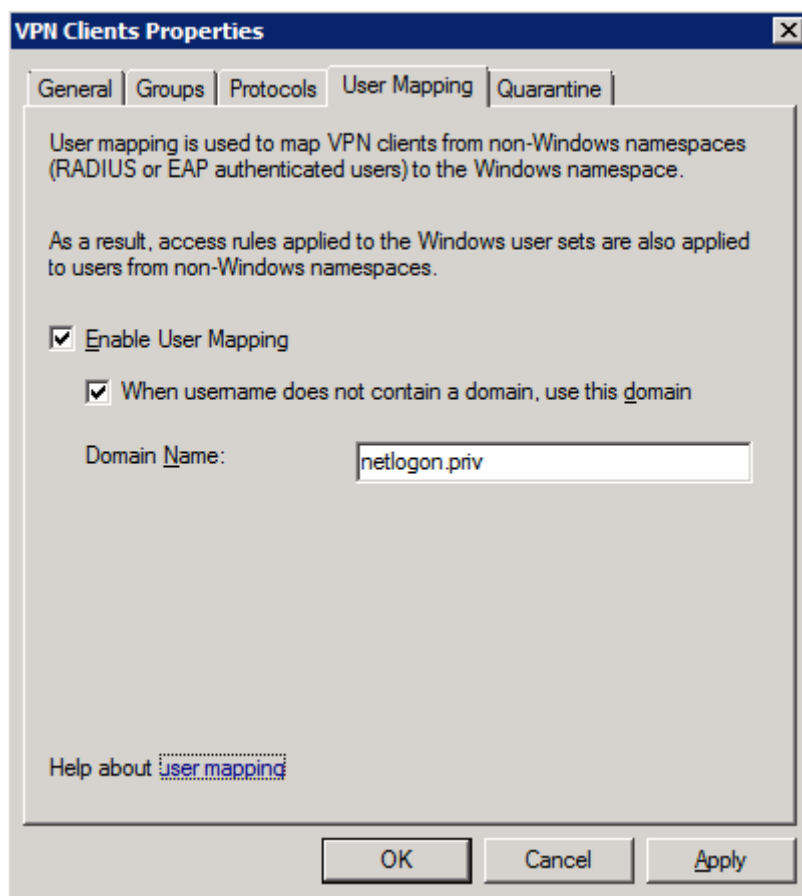
10.9 ÁBRA SSTP ÁTIRÁNYÍTÁS

Csakhogy kicsit mögé lássunk, itt egyébként még a "Path" fül tartalma is érdekes, ti. ez egy érdekes URL lesz, konkrétan ez: "/sra_{BA195980-CD49-458b-9E23-

⁹⁸ És ezt mind kiválóan lekövethetjük a 10.9-es ábrán is látható 46. számú SSTP System Policy szabályban

C84EEoADCD75}/.⁹⁹ És ez az, amely egy SSTP kérésbe becsomagolva érkezik a VPN klientsztől, és erre indul be TMG ezen System Policy szabálya az átirányítással.

Érdekes dologra bukkanhatunk rá a "User Mapping" fül alatt. Ha spéci RADIUS vagy EAP kliensekről van szó, és ha engedélyezzük és előkészítjük, akkor egy nem tartományi fiókkal megszemélyesíthetünk egy tartományit – annak minden előnyével együtt. Azaz megszemélyesítjük a VPN kapcsolatot felépítő felhasználót és így a VPN kapcsolaton is szűrhetünk anélkül, hogy további azonosítást kellene végezni a felhasználónak.



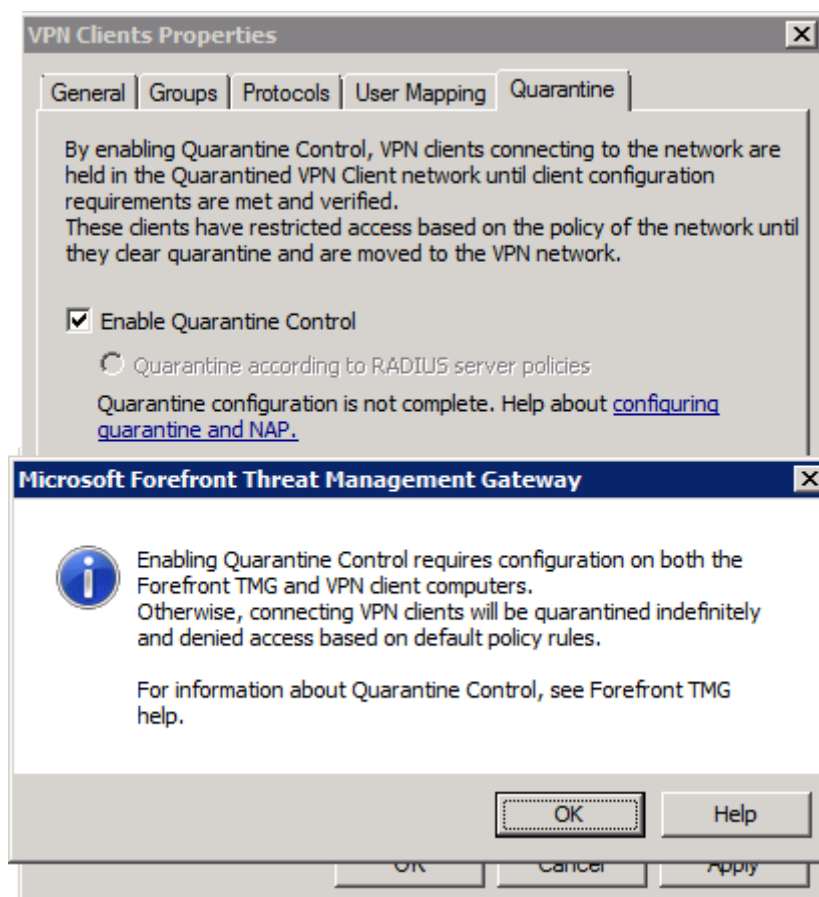
10.10 ÁBRA ÁTJÁRÁS A NÉVTEREK KÖZÖTT: EZ A USER MAPPING

Ehhez az AD-ban létre kell hoznunk egy pl. a RADIUS névtérből közeledő fiók nevével és jelszavával azonosat, itt be kell lőnünk a tartományunk nevét és készen is vagyunk, működik az átjárás. Cool, nem?

Aztán egy kicsi időutazásban is lehet részünk, ugyanis az utolsó fülön a VPN karantén mára már kissé letűnt világába jutunk el. Ha ezt használtuk, akkor lehetőségünk volt rá

⁹⁹ Többek között ennek a speciális URL rezervációnak a jellemzőit is megnézhetjük a "netsh http show urlacl" paranccsal.

hogy a VPN kient bizonyos vizsgálatok (pl. van-e AV szoftver a gépen, be van-e kapcsolva a tűzfal, és stb.) alá vessük még a kapcsolódás közben, de még a belső hálózat elérése előtt. Aztán vagy beengedtük, vagy elküldtük a VPN Quarantine hálózatba, hogy összeszedje magát, vagy egyszerűen lebontottuk. Mindezt már az ISA 2004 előtt is kipróbálhattunk, hiszen a Windows Server 2003 a Resource Kit Tools-sal és az RRAS-sal felturbózza kínált egy megoldást.



10.11 ÁBRA EZEN MÁR TÚL VAGYUNK EGY KICSIT

Ám az ISA 2004-gyel egy egyszerűbb, az ISA konzolba beépített módszerhez jutottunk (és ez maradt meg változás nélkül a TMG-ben is), ami azért így is rengeteg előkészületet és feladatot jelentett valamint komoly programozói tudást feltételezett, és közel sem volt egy tökéletes megoldás.

Így aztán amikor a NAP (Network Access Protection) beköszöntött a Windows Server 2008-cal, akkor ezt egy pillanat alatt el is felejtettük. De azért itt megvan még, sőt figyelmeztet is az engedélyezés után rögtön arra, hogy kliens oldalon is van ám előkészület, a szimpla VPN klienssel nem fog menni a kapcsolódás, akkor sem ha minden feltétel egyébként adott ehhez, szóval csak óvatosan kapcsolgassuk be.

A faragás véget ért, a TMG most már készen áll a VPN kapcsolatok fogadására, mármint akkor ha a felhasználóknál is be van állítva egy-egy VPN kapcsolat. Ha ezt manuálisan indítják, megkapják a helyes IP konfigurációt, működni fog a névfeloldás, kialakul a gépük és a TMG segítségével egy virtuális magánhálózat – és ezzel vége is. Egyáltalán nem fognak elérni semmilyen protokollal, semmilyen erőforrást a belső hálón....

Miért nem? A válaszhoz kanyarodjunk vissza az 5. fejezethez. Van számukra hálózati szabály? Igen van, alapesetben, azaz a TMG telepítése után létrejön egy NAT típusú szabály az Internal és a VPN hálózat között (ahová ugye automatikusan bekerülnek a csatlakozás után), de ez még kevés.

Egy vagy több külön hozzáférési tűzfalszabályt is létre kell hoznunk, attól függően, hogy mit, mikor, milyen feltételek mellett engedünk meg ezeknek a felhasználóknak. És ez a szép ebben az egészben, és ez az egyik dolog, amit az RRAS-ban nem, vagy csak nehézkesen tudunk összekalapálni, míg a TMG-ben ezen tűzfalszabályok rugalmasságát a végletekig kiaknázhadjuk – a VPN felhasználók esetén is.

10.2 SITE-TO-SITE VPN

Érthető, hogy nemcsak szóló VPN kapcsolatokra vágyunk, remek dolog lenne, ha komplett hálózatokat köthetnék össze, valamely VPN protokollal, gondoljunk bele, mennyire nagyszerűen alkalmazható lenne ez a telephelyek/központ viszonylatban, az interneten vagy más nyilvános vagy éppen nem nyilvános hálózatokon keresztül is..

Valóban remek dolog, és az ISA-val és TMG-vel egyaránt kiválóan működik is ez a kívánság Site-to-Site VPN néven, már sok-sok éve. Még hozzá nem is kell hozzá feltétlenül mindkét oldalon egy-egy TMG mint VPN átjáró, hanem akár egy megfelelő hardver eszközzel (VPN router) is képes összefütyülni a TMG, tipikusan úgy, hogy a kisebb értékű, kevesebb felügyeletet igénylő célhardver eszközök a telephelyeken kerülnek telepítésre, míg a TMG a központban. De nem Microsoft által készített szoftveres VPN szerverekkel is kialakítható ez a fajta kapcsolat.

Háromféle¹⁰⁰ VPN protokollt használhatunk ha egy S2S kapcsolatot szeretnénk kreálni:

- PPTP
- L2TP over IPSec
- IPSec tunnel mode

¹⁰⁰ Az SSTP-t nem lehetséges e célból használni.

A KAPUN TÚL

A harmadik a kakkuktojás, egyrészt azért mert ezt a szülő VPN-eknél nem használjuk, másrészt azért mert a hardveres VPN routerek esetén legjobban ezt preferáljuk.

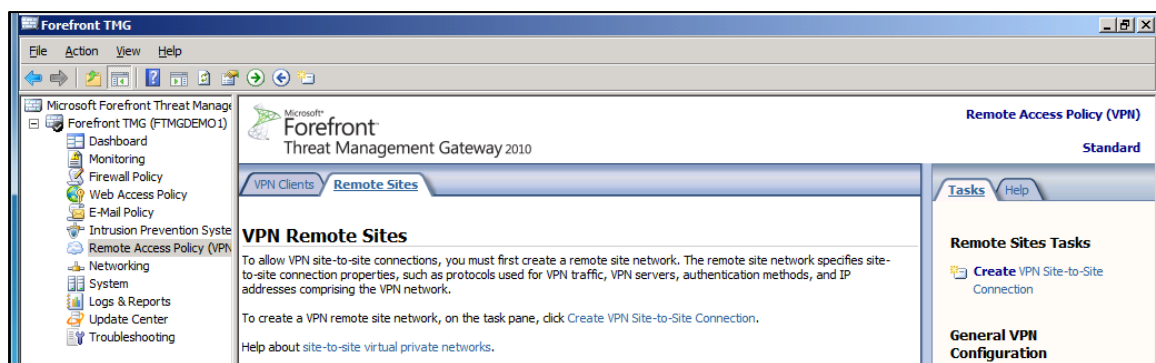
Persze sok más jellemző és körülmény is befolyásolhatja, hogy végül mely típus mellett döntünk, nos ebben segíthet a következő összefoglaló táblázat.

10.1 TÁBLÁZAT S2S VPN PROTOKOLLOK

Protokoll	Mikor használható?	Biztonsági szint	Megjegyzések
IPSec tunnel mode	Külső VPN szerver (hardveres/szoftveres)	Magas ¹⁰¹	Külső (nem Microsoft) VPN szerverhez így kapcsolódhatunk.
L2TP over IPSec	Másik TMG-hez vagy ISA 2000/2004/2006-hoz kapcsolódva vagy akár egy Windows RRAS-hoz	Magas	RRAS lesz ez minden esetben, csak valamikor a TMG-n vagy az ISA-kon keresztül. Megfelelően biztonságos, főképp ha nem előre megosztott kulccsal, hanem tanúsítványokkal használjuk. Ez egyben a hátránya is, ami miatt közepesen bonyolult a kiépítése (az előző még összetettebb is lehet).
PPTP	Másik TMG-hez vagy ISA 2000/2004/2006-hoz kapcsolódva vagy akár egy Windows RRAS-hoz	Mérsékelt	Ez is RRAS, de nem IPSec, mint az előző, ezért kevésbé biztonságos, viszont nagyon egyszerű összekalapálni.

Tehát a most következő részben az lesz a feladatunk, hogy egy telephelyi hardveres VPN routert illetve a TMG-t egy állandó, azaz igény szerint felépülő (on-demand) IPSec VPN kapcsolattal kössük össze. A TMG-vel kezdünk.

¹⁰¹ Egy megfelelően kiválasztott IKE auth mentén magas. Egy pre-shared key esetén nem az.



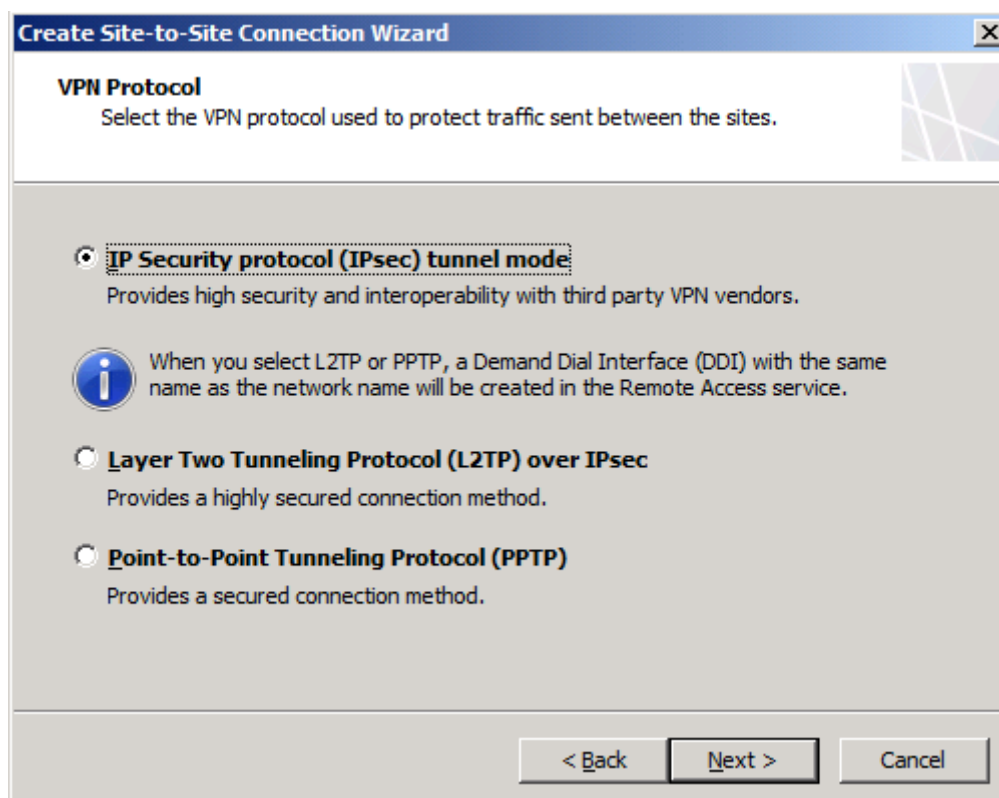
10.12 ÁBRA MÉG ÜRES

Vagy a már ismerős VPN elágazás második fülének (Remote Sites) középső keretéből, vagy az Action pane "Create VPN Site-to-Site Connection" pontja alól indul a varázslás.

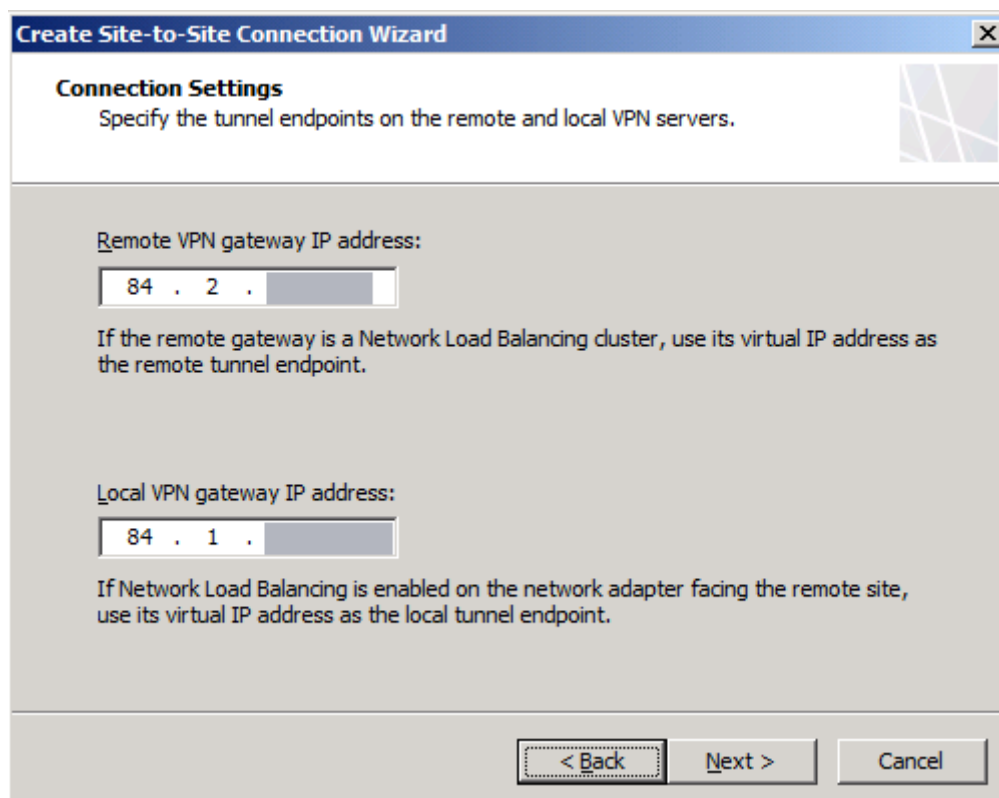


10.13 ÁBRA EZ MÉG CSAK EGY NÉV

A második lépésben rögzest el kell döntenünk, hogy mely VPN protokollokat használjuk majd.

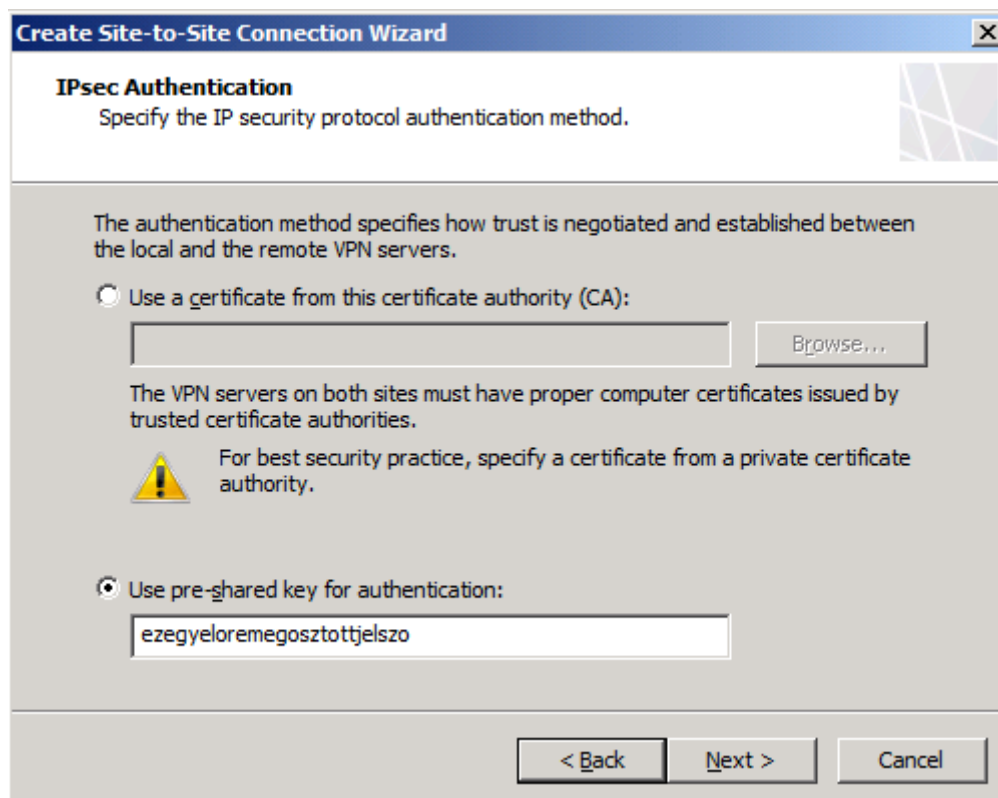


10.14 ÁBRA NEKÜNK AZ IPSEC-RE VAN SZÜKSÉGÜNK



10.15 ÁBRA A TÁVOLI ÉS A HELYI ÁTJÁRÓ CÍMEI

A következő lépés a hitelesítési metódus meghatározása, mi most mivel ez egy teszt megoldás, választhatjuk az előre megosztott jelszót, egyébként nem ez az ajánlott.



Create Site-to-Site Connection Wizard

IPsec Authentication
Specify the IP security protocol authentication method.

The authentication method specifies how trust is negotiated and established between the local and the remote VPN servers.

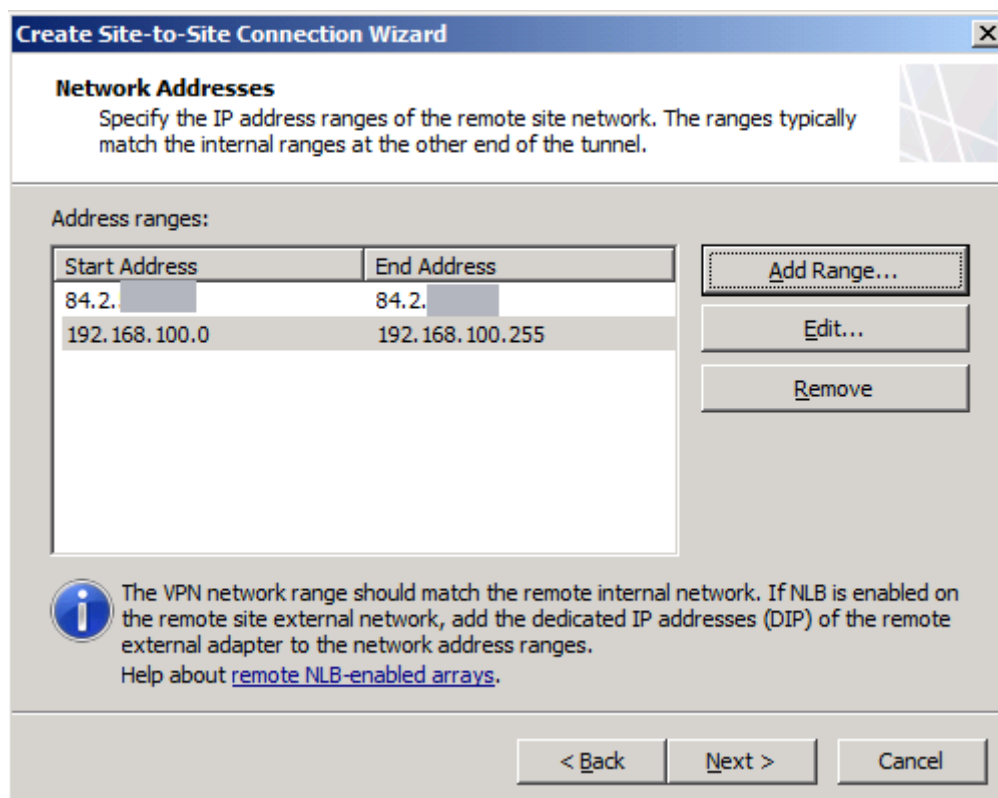
☐ Use a certificate from this certificate authority (CA):

The VPN servers on both sites must have proper computer certificates issued by trusted certificate authorities.

 For best security practice, specify a certificate from a private certificate authority.

☒ Use pre-shared key for authentication:

10.16 ÁBRA EZ CSAK TESZT LESZ



Create Site-to-Site Connection Wizard

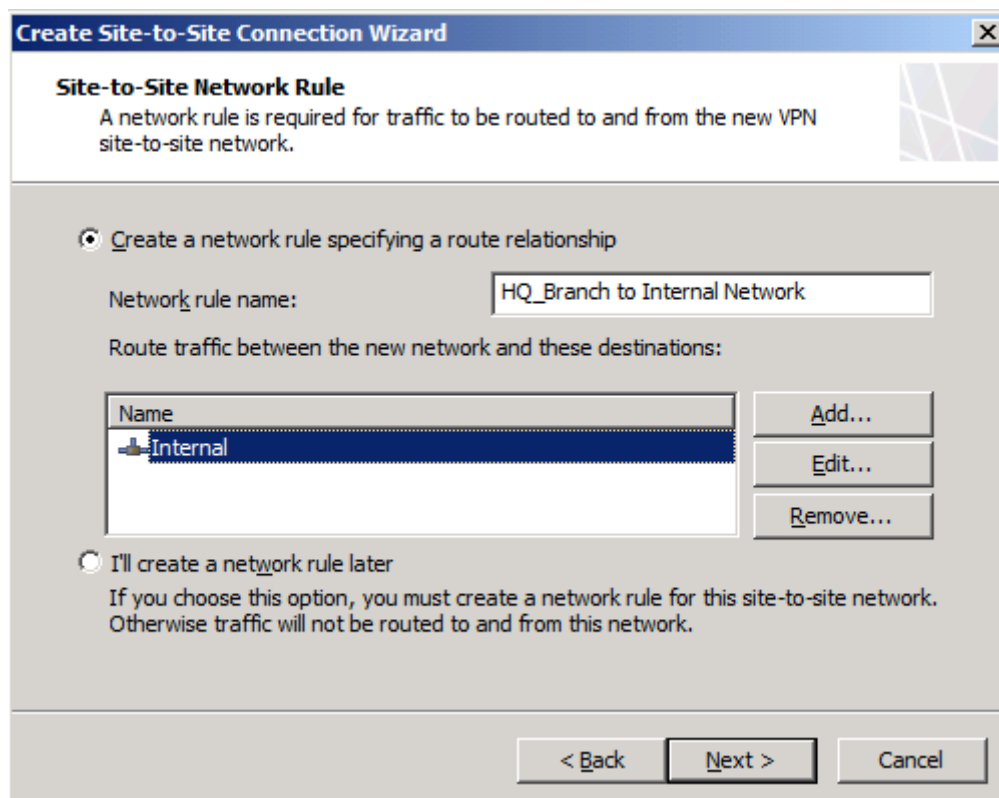
Network Addresses
Specify the IP address ranges of the remote site network. The ranges typically match the internal ranges at the other end of the tunnel.

Address ranges:

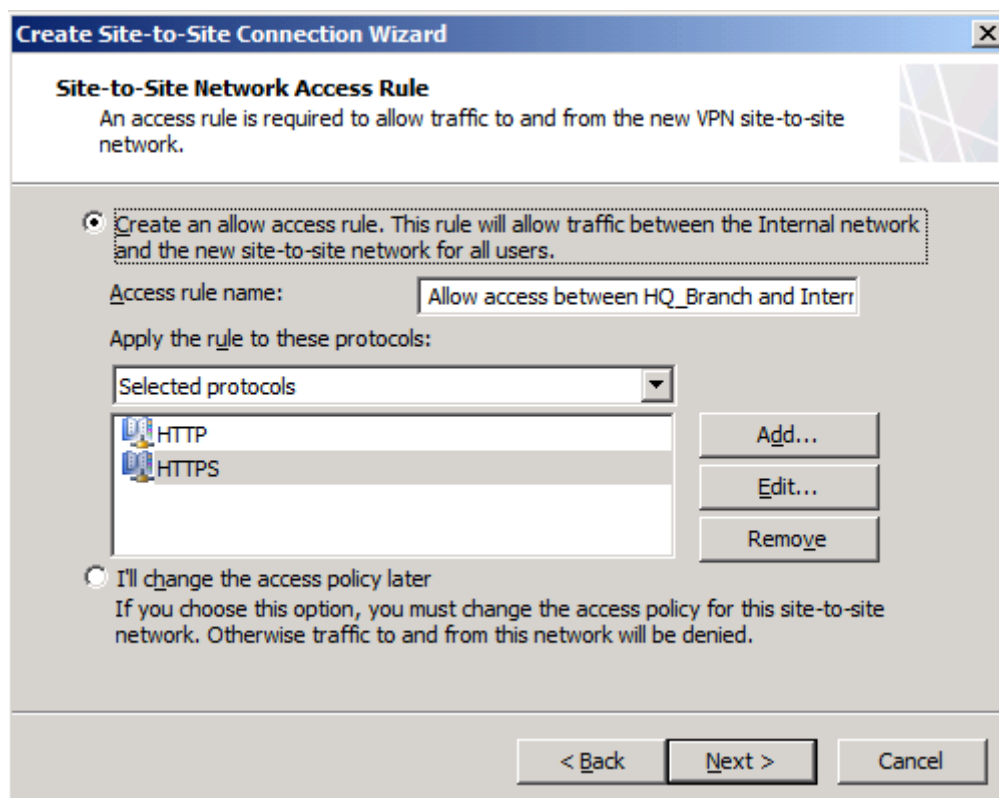
Start Address	End Address
84.2.	84.2.
192.168.100.0	192.168.100.255

 The VPN network range should match the remote internal network. If NLB is enabled on the remote site external network, add the dedicated IP addresses (DIP) of the remote external adapter to the network address ranges.
Help about [remote NLB-enabled arrays](#).

10.17 ÁBRA AZ ÁTJÁRÓ MELLETT A MÁSIK HÁLÓZAT BELSŐ IP TARTOMÁNYÁRA IS SZÜKSÉG VAN

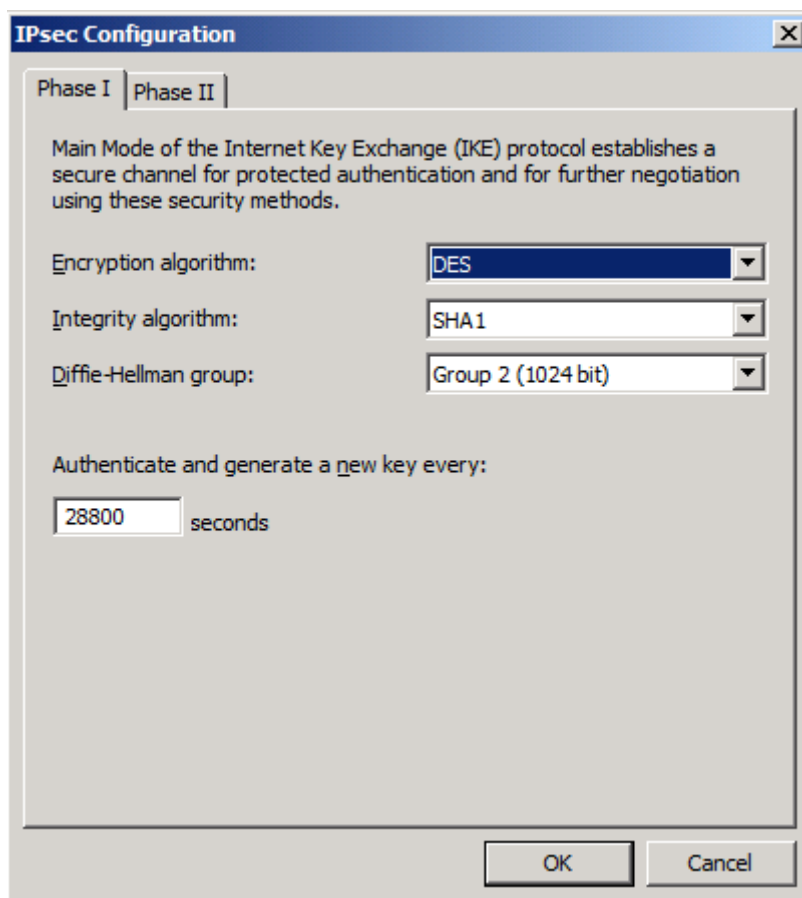


10.18 ÁBRA AKÁR AZONNAL ELKÉSZÜLHET EGY HÁLÓZATI SZABÁLY A KÉT HÁLÓZAT KÖZÖTT



10.19 ÁBRA SÓT, TÚZFALSZABÁLYOKAT IS KREÁLHATUNK IZIBE

Ezután már csak az összegző képernyő jön, és az egyik oldal már készen is van. Most nézzük meg a speciális IPSec beállításokat, azért hogy a hardveres oldalt már könnyebb legyen összerakni.



10.20 ÁBRA EZ MÁR NEM AZ ALAPBEÁLLÍTÁS

Vagy fordítva, azaz adott esetben a TMG IPSec beállításait kell módosítani, hogy aztán egymásra találjon a két eszköz. Éppen ezért az előző ábrán pontosan ezért már nem az alapbeállítás látszik (ráadásul a Phase2 fül alatt sem), hanem egy olyan konfiguráció, amelyet a másik oldalon egy Draytek Vigor 2910-es dual WAN-os, VPN routerrel meg tudtam etetni.

Vigor2910 Series
Dual-WAN Security Router

Quick Start Wizard
Online Status

WAN
LAN
NAT
Firewall
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
▶ VPN Client Wizard
▶ VPN Server Wizard
▶ Remote Access Control
▶ PPP General Setup
▶ IPsec General Setup
▶ IPsec Peer Identity
▶ Remote Dial-in User
▶ LAN to LAN
▶ VPN Backup Management
▶ Connection Management
Certificate Management
USB Application
System Maintenance
Diagnostics

Status: Ready

All Rights Reserved.

Profile Index: 1

1. Common Settings

Profile Name: []
☒ Enable this profile

VPN Dial-Out Through: WAN2 Only

Netbios Naming Packet: ☒ Pass ☐ Block

Multicast via VPN: ☐ Pass ☒ Block
 (for some IGMP, IP-Camera, DHCP Relay..etc.)

Call Direction: ☒ Both ☐ Dial-Out ☐ Dial-In

☐ Always on

Idle Timeout: 300 second(s)

☐ Enable PING to keep alive

PING to the IP: []

2. Dial-Out Settings

Type of Server I am calling

☐ ISDN
☐ PPTP
☒ IPsec Tunnel
☐ L2TP with IPsec Policy [None]

Server IP/Host Name for VPN.
 (such as draytek.com or 123.45.67.89)
 []

Link Type: 64k bps

Username: ???

Password: []

PPP Authentication: PAP/CHAP

VJ Compression: ☒ On ☐ Off

IKE Authentication Method

☒ Pre-Shared Key

IKE Pre-Shared Key: []

☐ Digital Signature(X.509)

[None]

IPsec Security Method

☒ Medium(AH)
☐ High(ESP) [DES without Authentication]

Advanced

Index(1-15) in Schedule Setup:
 [] [] [] []

Callback Function (CBCP)

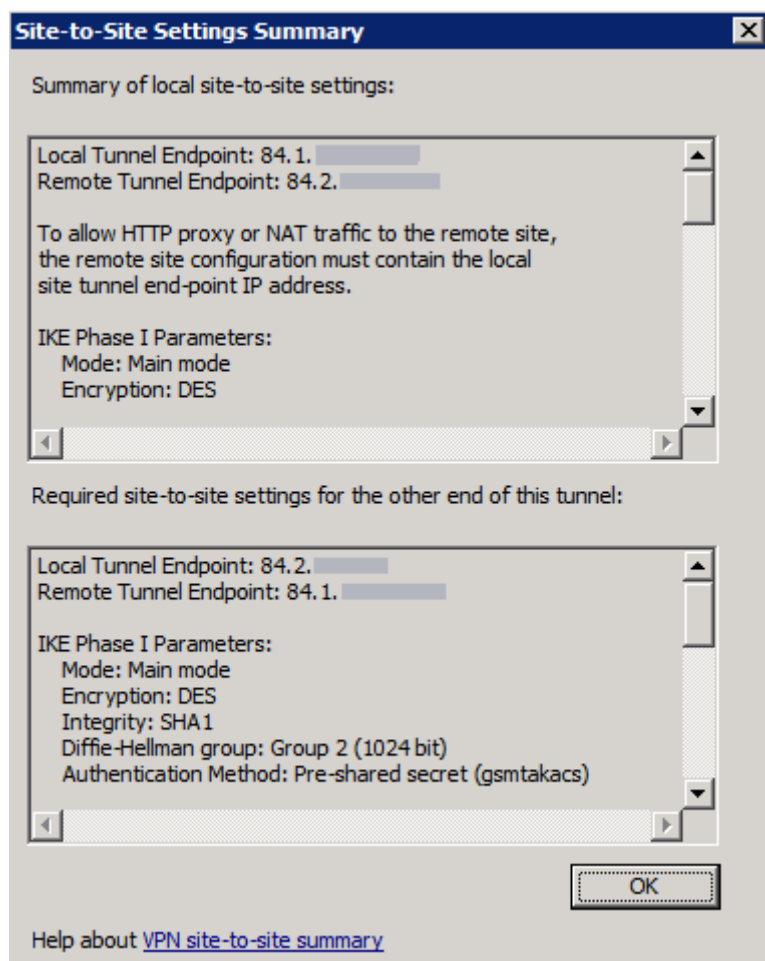
☐ Require Remote to Callback
☐ Provide ISDN Number to Remote

3. Dial-In Settings

Allowed Dial-In Type: []

10.21 ÁBRA ÍGY NÉZ KI A MÁSIK OLDAL BEÁLLÍTÁSAINAK EGY RÉSZE

Ha viszont sikerült az IPsec beállításokat közös nevezőre hozni, akkor a TMG-ben kérhetünk egy részletes összegzést ezekről.



10.22 ÁBRA AZ ÖSSZEGZŐ STATISZTIKA (EGY DARABJA)

Egy kész IPSec S2S kapcsolatot nem válthatunk át pitty-putty mondjuk PPTP-re, ehhez egy új varázslásra lesz szükség. Ha PPTP-vel szeretnénk összehozni pl. két TMG-t, akkor talán a legfontosabb különbség a protokoll típusán kívül az, hogy szüksége lesz egy felhasználói fiókokra (egy olyanra, aminek van dial-in joga) mindkét oldalon (a kapcsolat beindításához), amelyeknek ráadásul meg kell egyezniük az általunk helyben kreált hálózat nevével (lásd 10.13-es ábra).

Nem kell, hogy ez a fiók rendszergazda jogosultsággal bírjon, csak ezek a követelmények. Sőt még a varázslás közben sem lesz ennek a fióknak a hiányából baj, a kapcsolat viszont biztosan nem működik majd addig, amíg nem kreálunk egy ilyen fiókot - mindkét oldalon.

Az L2TP kapcsolatoknál a fióknév ügyben teljesen ugyanez a helyzet, itt még a különbség az is értelemszerűen, hogy a megfelelő biztonsági szint érdekében egy megfelelő tanúsítványra is szükségünk lesz.

Ezek után viszont tetszőleges S2S kapcsolatunk lehet a TMG-ben, leszámítva az előzőekben említett licenz különbséget. Ami még számíthat, az nyilvánvalóan a Internet felé menő vonalunk sávszélessége, hiszen bármilyen csodafegyver a kezünkben a VPN, azért egy hátránya biztosan lesz: erőforrásba kerül (a kulcsszó a Capacity Planning, 3.1 fejezet).

10.3 A NAGY DURRANÁS: DIRECTACCESS TÁMOGATÁS

10.3.1 DIRECTACCESS ALAPOK¹⁰²

A 2007-es RSA konferencián beszélt Bill Gates először arról a vízióról, hogy VPN vagy bármilyen más távelérési módszer nélkül is el kellene tudnunk érni biztonságosan a belső hálózatunk erőforrásait, instant módon, azaz bármilyen manuális teendő nélkül, gyakorlatilag teljesen automatikusan. Ez remekül hangzott az elképzelés szintjén, hiszen akár rendszergazda vagyok, akár felhasználó, ezzel az eléréssel csak a probléma van. A VPN bonyolult (is tud lenni, főképp, ha szimpla felhasználók vagyunk), ha komolyan vesszük kell a Smartcard\PKI, sokszor egy automatikus default gateway átirányítással is jár (a split tunnel-t nem szeretik általában a céges környezetben), vannak olyan hálózatok (pl. hotelek, vagy egyéb szigorú céges hálózatok), ahonnan nem használható, vagy csak PPTP, és sorolhatnám még a problémákat. Szumma szummárum: nem igazi az élmény.

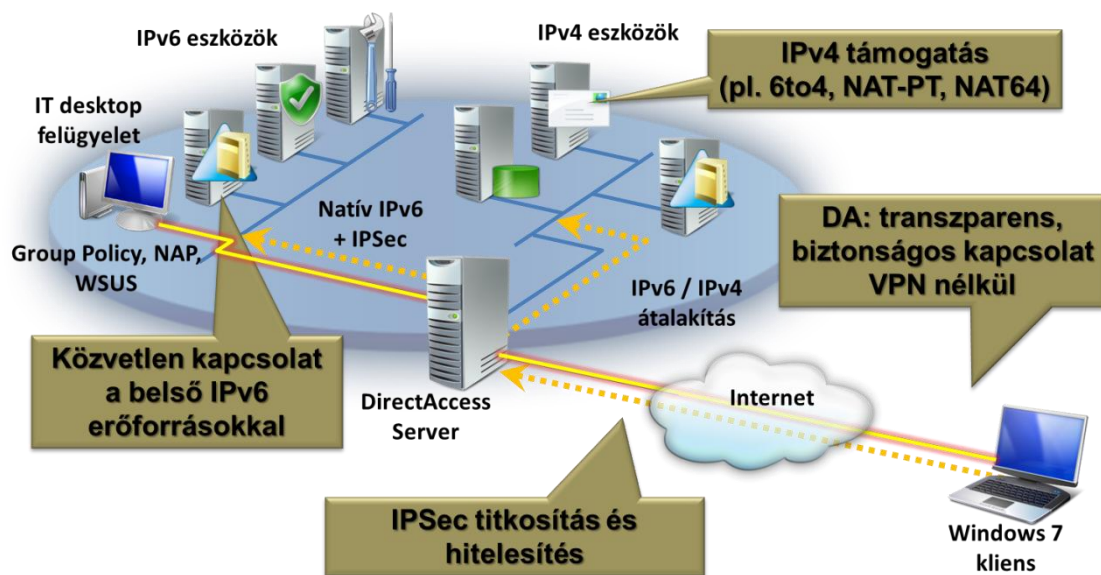
A DirectAccess azaz a Windows Server 2008 R2-vel és a Windows 7-tel megvalósított közvetlen elérés viszont az. Most már rutinos DA felhasználó vagyok, a Microsoftnál már több mint 1,5 éve használom és mondhatom, hogy függő lettem ☺

Mivel jómagam rendkívül sokat vagyok távol az irodától, a távoli elérés az első pillanattól kezdve fontos volt. Anno minden gépemhez beszereztem a smartcard olvasót (a Dell Tablet PC-hez nem volt egyszerű), mindenhol használtam a CMAK-kal csomagolt IT Connection Manager-t az összes kritériummal együtt (a részletek nem publikusak). Működik, de mindez csak kínládás a DA-hoz képest.

Ugyanis most már semmit nem kell tárcsázni, semmit nem kell elindítani (kritériumok persze ugyanúgy vannak, hiszen pl. a NAP itt is van, sőt BitLocker-rel kombinálva is), csak indítom a böngészőt és beírom az intranetes szerver nevét, vagy pl. a fájlszervert a Start/Run-ba. Nincs hosszú ellenőrzés, terjedelmes karantén vizsgálat, csak egy internet kapcsolat kell.

¹⁰² Tisztázzuk: ezek csak alapok, ennyiből nyilván nem tudunk komplett DA-t építeni, itt csak egy rövid áttekintést kapunk majd és persze a TMG függő részeket.

Ráadásul, mivel már a belépés előtt éled, a céges környezetben kötelező frissítések és házirendek letöltése sem csak a VPN kapcsolat után indulhat, hanem ettől függetlenül, azaz bármikor, ha van a gépnek net elérése. Persze nem arról van szó, hogy az összes "internetes" forgalom "befelé" megy (de ezt is lehet, ha szükséges), a normál forgalom továbbra is az ISP-nken keresztül zajlik, csak az a különbség, hogy mivel rögvest kapcsolatban lehetünk pl. a cégünk Perimeter hálózatában lévő DA szerveren keresztül a belső WSUS/SCE-vel/SCCM-el, stb, nem kell ehhez megvárni a klasszikus VPN csatlakozást. Ez jó az üzemeltetőknek, és végül is jó nekem is, mint felhasználónak.



10.23 ÁBRA EGY (MAJDNEM) TELJES DA INFRASTRUKTÚRA

Mindeme "csoda" alapja több hálózati technológia együttes alkalmazása, úgymint IPSec (hitelesítés és titkosítás) illetve az IPv6, a kétirányú kapcsolat felépítéséhez, ideális esetben tökéletes point-to-point security kialakítása a NAT, a NAT-T és az egyéb NAT problémák nélkül.

Viszont ha még nincs teljes IPv6 infrastruktúránk¹⁰³, akkor az ISATAP-ra, a Teredo-ra, a 6to4-re is szükségünk lehet az IPv4/v6 átalakításhoz szerver illetve kliens oldalon¹⁰⁴. Kis segítség ezek értelmezéséhez:

- Teredo: NAT Traversal

¹⁰³ Alapértelmezés szerint a Vista, WSo8, Windows 7, WSo8 R2 OS-ekben natív módon implementálva van, a hálózati hardver eszközök persze még egy külön kérdést képeznek.

¹⁰⁴ Vagy egy NAT-PT (RFC 2766) képes Layer2/3 hálózati eszköz, azaz switch vagy router (mivel az R2 ezt nem nyújtja), vagy egy Forefront UAG 2010, ami szintén képes a teljes átalakítást elvégezni.

- IPv4 tunneling: ISATAP (IPv6 átalakítás), 6to4 (publikus IPv4 címekhez), Teredo (privát IP címekhez)
- Split DNS és a DA használat "követése": Name Resolution Policy Table

Az NRPT-hez még egy mondat, mivel ez egy érdekes újdonság, amely a Windows 7-ben debütál. Az NRPT elsődleges célja az, hogy szeparálni tudjuk a kliens oldalon a Internet/Intranet forgalmat, tehát abban az esetben, ha a kliens az interneten lóg, az első DNS infó keresés helye a NRPT lesz - és ha egy DA-n keresztül, belső hálózati név/cím eléréséről van szó, akkor ott kell lennie ebben a táblában a mi megfelelő DNS szerverünknek (Csoportházirend > Name Resolution Policy) és már indulhat is a titkosított DNS lekérdezés vagy mehet titkosítás nélkül is - pl. az élő DA kapcsolaton keresztül.

Plusz, itt van még nekünk egy új, jelen pillanatban még szabványosítás alatt álló, a Microsoft által fejlesztett protokoll, az IP-HTTPS. Csak a Windows 7 illetve a WSo8 R2 esetén, a proxy vagy tűzfal mögött elhelyezett hostok képesek az IPv6 csomagokat IPv4 alapú HTTPS session-okba "gyömöszölni". Ezzel még akadnak teljesítmény gondok, a Microsoft keresi is a megoldást, éppen ezért ez csak a tartalék forgatókönyv, arra az esetre ha a kliens szimpla IPv6 alapon (illetve a fentebb említett átalakítási megoldásokkal) nem tud kapcsolódni.

No és persze a különböző hitelesítési protokollok is szükségesek, ezek közül jelen pillanatban elsősorban a Smartcard, azaz egy multifaktoros hitelesítés a kíváncsi. A gépnek értelemszerűen muszáj tartományi tagnak kell lennie, illetve jó tudni azt is, hogy az üzemeltetők megszabhatják a belső erőforrások elérését, azaz adhatnak elvileg korlátlan hozzáférést, vagy csak bizonyos szerverek/gépek elérését, nagyjából ahogyan pl. egy Remote Desktop Gateway-nél.

E rövid áttekintés után még egy dologba gondoljunk bele: azok a klienseink, akik használják a DA-t, azon kívül, hogy a belső hálózatba csont nélkül beeláthatnak, egymással is kommunikálhatnak majd, amelyet elsősorban a különböző P2P alkalmazásokkal fognak tudni igazán összehozni, de a lista szélesíthető. Ezek között vannak/lesznek olyanok, amelyeknél nincs szükség plusz lépésekre a biztonságos kommunikációhoz, a többi esetben (pl. Remote Assistance, Remote Desktop, File/Printer Sharing, stb.) viszont - nekünk üzemeltetőknek - gyakorlatilag IPSec transzport szabályokkal kell majd engedélyeznünk alkalmazásonként külön-külön vagy éppen mindent megengedve, vagy adott esetben tiltani a kapcsolódás lehetőségét.

Mindezek után nézzük meg a DA telepítés többségében szoftver, de némiképp hardver követelményeit is:

- Active Directory (minimum egy Windows 2008 vagy újabb DC), sőt ha smartcardot akarunk használni, akkor csak R2-es AD jöhet szóba.
- PKI infrastruktúra (AD CS), EKU-s kiszolgáló tanúsítvány, autoenrollment, illetve olyan CRL publikálás, amely elérhető kívülről, azaz a netről is.
- Egy dedikált WSo8 R2 DirectAccess kiszolgáló (nem DC) két hálózati kártyával (intranet/internet), sőt a külsőn két statikus, publikus és szomszédos IPv4 címmel.
- IIS7, ami lehet a DA szerveren is, vagy más kintről elérhető kiszolgálón, a lényeg, hogy a DA kliensek számára biztosítani kell az ún. "Network Location Server" szerepet, amely segítségével kiderül, hogy a DA kliens az intraneten vagy az interneten van éppen.
- Csak a tartományi fiókkal rendelkező Windows 7 kliensek használhatják a DA-t.
- AD biztonsági csoport a DA-t használni óhajtó kliens gépfiókok számára.
- Illetve a korábban ismertetett szoftveres IPv4 <> IPv6 átalakítási technikák, vagy a NAT-PT hardver.

10.3.2 DA vs. TMG

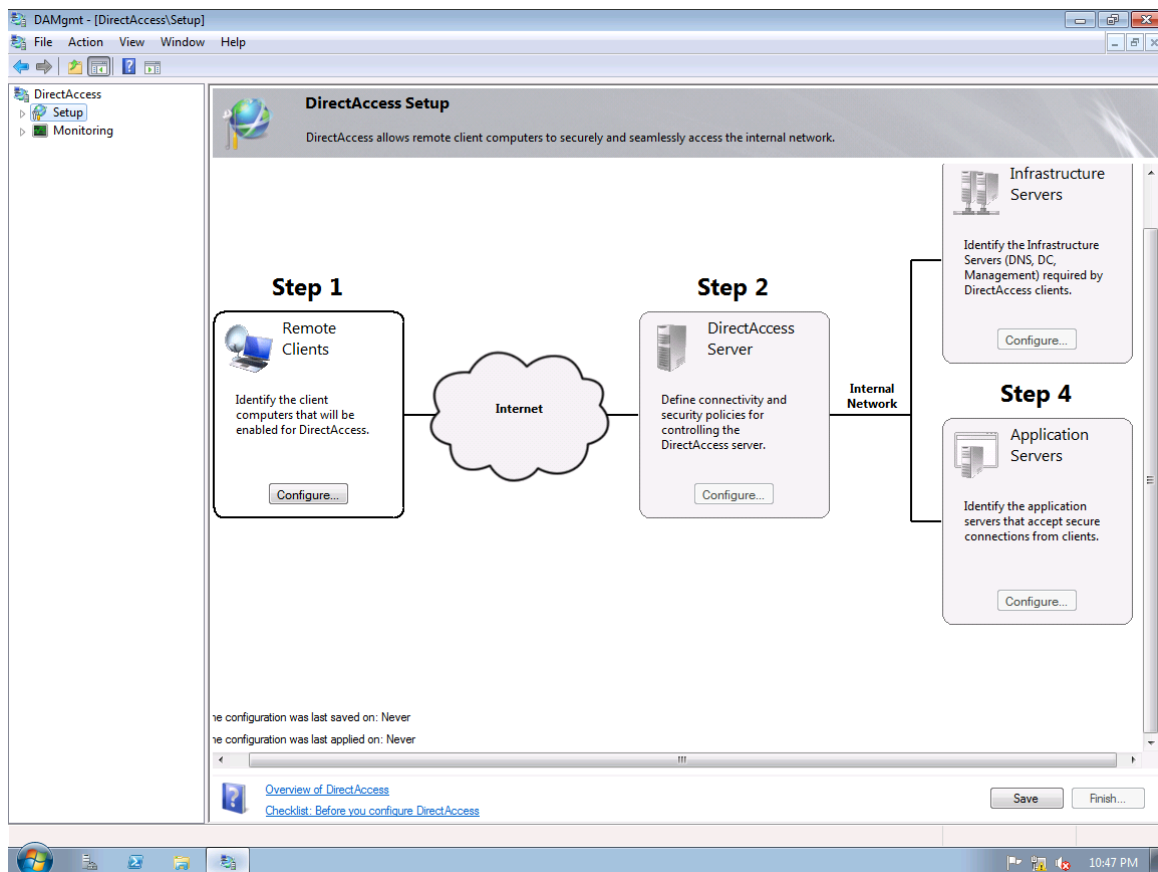
Nos, minden szép és jóóó, a DA egy remek találmány, de ezek után jöhet a kérdés, hogyan fogjuk összehozni mindezt a TMG-vel amely elvileg nem is támogatja az IPv6-os szcenáriókat, pl. egy RDP elérést sem tudok vele, illetve rajta keresztül elkészíteni?

Hát úgy, hogy a DirectAccess kivétel, a TMG fel van készítve erre, csupán pár trükköt kell bevetnünk, ahhoz hogy működjön. Ez egyik legfontosabb tudnivaló, az hogy a DirectAccess-t még a TMG telepítése előtt fel kell raknunk a gépre, és tökéletesen be is kell konfigurálnunk, minden részletével egyetemben.

Szerintem egy nagyon jó segítség ehhez a "Test Lab Guide: Demonstrate DirectAccess".

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=8d47ed5f-d217-4d84-b698-f39360d82fac>

Ez egy step-by-step típusú dokumentum, amelynek egy korai változatából építettem fel annak idején én is az első tesztrendszeremet.



10.24 ÁBRA ÉPP A DA MMC-BEN TEVÉKENYKEDÜNK

Ezután egy .reg fájl segítségével (amelyet be kell importálnunk a registry-be), a TMG által majdan letiltandó IPv6-os tranzíciós technikák feloldását előre elvégezhetjük. A .reg fájl tartalma a következő kell hogy legyen:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RAT\Stingray\Debug\ISACTRL]
"CTRL_SKIP_DISABLE_IPV6_PROTOCOLS"=dword:00000001
```

Ezt követheti a TMG normál telepítése. Ha ez rendben lemegy, akkor már csak egy szkript lefuttatására lesz szükség, ami a következőképpen néz ki:

```
set o = createobject("fpc.root")
set arr = o.Arrays.Item(1)
set policy = arr.ArrayPolicy
set IPV6Settings = policy.IPv6Settings
IPV6Settings.DirectAccessEnabled = vbTrue
arr.save
```

És ezzel el is készültünk, a TMG leszinkronizálja a konfigurációját, és egyúttal már DA szerverként is működik. Ezt részben leellenőrizhetjük a System Policy-ban is, ahol 48-51-ig felsorakozott szabályok mind a TMG és a DA kapcsolatával foglalkoznak.

Még 1-2 apró adalék a témához¹⁰⁵, amelyek közül az első a tervezés apropóján fontos. Ugyanis a Microsoft részéről az ajánlás nem ez a forgatókönyv a DirectAccess bevezetéséhez, hanem a Forefront Unified Access Gateway 2010 (UAG)¹⁰⁶, amely egy sokkal nagyobb ágyú ebben az esetben, sokkal tökéletesebb és granulásabb megoldás a távoli elérésre és a különböző trancíziós kényszerhelyzetekre.

Egy másik kérdés arra vonatkozik, hogy csak és kizárólag a TMG telepítése előtt lehet-e felpakolni a DirectAccess szerepkört? Igen, ez lenne az ajánlott, de ha nagyon muszáj, akkor a "net stop fweng" paranccsal le tudjuk lőni a Forefront TMG drivert¹⁰⁷, majd jöhet a DA telepítés, és utána a "net start wpsrv"-vel a TMG indítása. A .reg fájlra és a szkriptre persze ekkor is szükség van.

Jó tudni azt is, hogy egy DA szervert lehet-e a TMG mögé tenni, illetve hogy az is, hogy a TMG elé, azaz az internet és a TMG közé lehet-e tenni ezt a szervert? Mindkettőt lehet. A korábban említett útmutató tartalmaz egy "Firewall Exception" szakaszt, amely alapján kiderül, hogy a TMG mögött elhelyezett DA szerver esetén milyen portokat kell kinyitni. A másik esetben a válasz azért már nem ilyen egyértelmű: a TMG "gyári" IPv6 inkompatibilitása miatt ez csak akkor működhet, ha a belső hálón csak és kizárólag az ISATAP-ot használja minden kliens és szerver.

Nos, ezzel a kellemesen alakuló témájú befejező résszel a távoli elérés fejezet végére is értünk, és most ezzel a lendülettel egy összetett részre ugrunk, amely viszont nem a képességek további tallózását, hanem az eddigiekkel kapcsolatos ellenőrzéseket és vizsgálódásokat szerepelteti majd.

¹⁰⁵ A forrás ezen kérdések és válaszok esetén a következő:

<http://blogs.technet.com/b/isablog/archive/2009/09/23/forefront-tmg-and-windows-7-directaccess.aspx>

¹⁰⁶ <http://www.microsoft.com/uag>

¹⁰⁷ Ilyenkor persze minden védelem megszűnik, ergo ezt offline állapotban tegyük meg a TMG-vel.

11 ELLENŐRIZZÜNK ÉS JAVÍTSUNK

Nem nagyon hiszem, hogy a nyeretlen kétéveseken kívül van olyan üzemeltető, aki ne tudná, hogy ugyan a munka fontos része a tervezés, a bevezetés, a képességek elsajátítása, de az ördög a részletekben rejtőzik, és ezek a részletek ezután jönnek. Egész pontosan hogyan működik? Miért ezt csinálja? Miért nem úgy csinálja? Miért csinálja ezt csak nálunk? Hol is tudnám ezt lekövetni? És még fokozhatnánk. A már emlegetett "koszos" hétköznapi világában ezért is kulcsfontosságú, hogy képben legyünk e fejezet témaköreivel kapcsolatban is.

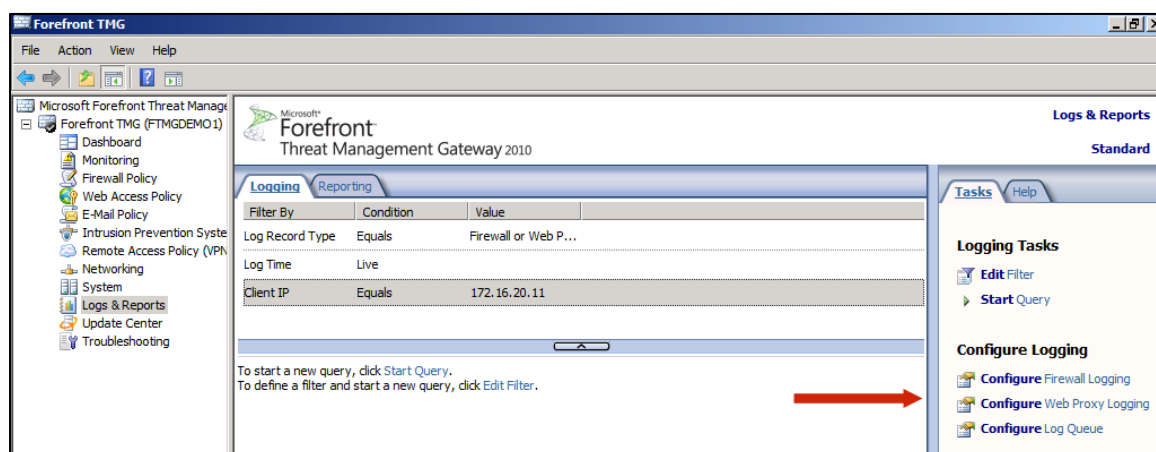
11.1 NAPLÓZÁS

Naplózni tehát muszáj. Egy tűzfal esetében kritikusan muszáj. Muszáj, mert tudnunk kell, hogy milyen változások történnek, milyen felhasználói aktivitás zajlik, milyen támadási kísérleteket hárít el a TMG, és minden más, azaz bármilyen más történést is részleteiben kell megismernünk, mert az ördög nem alszik.

Sokszor hibakeresési céllal használjuk fel a naplót, máskor csak dokumentálni szeretnénk az adott konfigurálási folyamatot, és megint máskor a kiszolgálónk "egészségi" állapotának az ellenőrzése a cél. Jelentéseket és statisztikákat is készítenünk kell a naplófájlok alapján, illetve értesülnünk kell a rendszer elemeinek aktuális állapotáról is, úgy, hogy közben ezek is dokumentálva legyenek természetesen.

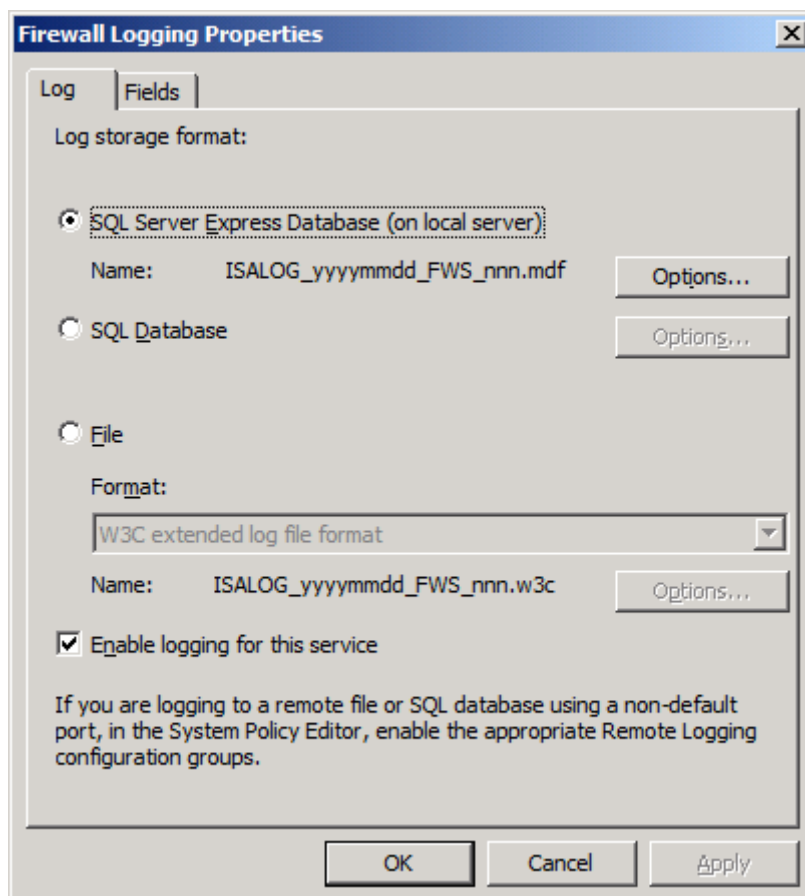
Szóval nincs itt kérdés, naplózunk és kész. De hova, mit és mennyit? Mindjárt kiderül.

Ahhoz, hogy elkezdjük a beállításokat válasszuk a baloldali faszerkezetből a "Logs And Reports" pontot, majd az Action Pane alatt válasszuk először a háromból a "Configure Firewall Logging" linket.



11.1 ÁBRA A NAPLÓZÁS KONFIGURÁLÁSA ITT KEZDŐDIK

A tűzfal illetve a web proxy napló beállításai szinten semmiben sem térnek el, elég az egyiket most jól megnéznünk. A "Log" fülön kiválóan látszik, hogy három fő módszerünk lehet a naplózásra, a tárolás típusától függően.



11.2 ÁBRA ALAPESETBEN EGY HELYI SQL EXPRESS-BE DOLGOZIK

Érdekes módon legalul kapcsoljuk be-, vagy ki a naplózást (Enable logging for this service), viszont utána rögtön három lehetőségünk is akad.

- Az első az alapértelmezés, ma SQL Express-nek hívják (ez már a 2008-as változat), régebben MSDE néven futott (aztán lett WMSDE, de az annak az ISA-hoz már nem volt köze volt). Helyben fut (csak helyben futhat), és minden haladó módszer (pl. az realtime napló) esetén is alkalmazható. A telepítő konfigurálja és alapértelmezett policy szerint csak a "Shared Memory" protokollal érhető el, sem a Named Pipes, sem a TCP/IP protokollokkal nem¹⁰⁸.
- A középső típus a "nagy" SQL Database használata, amely funkcionálisan elvileg nem ad többet mint az első módszer, ám egyrészt nem helyben van, másrészt és valószínűleg kapacitás problémákat sem vet fel¹⁰⁹.

¹⁰⁸ A System Policy alapértelmezés szerint a távoli SQL kapcsolatokat tiltja.

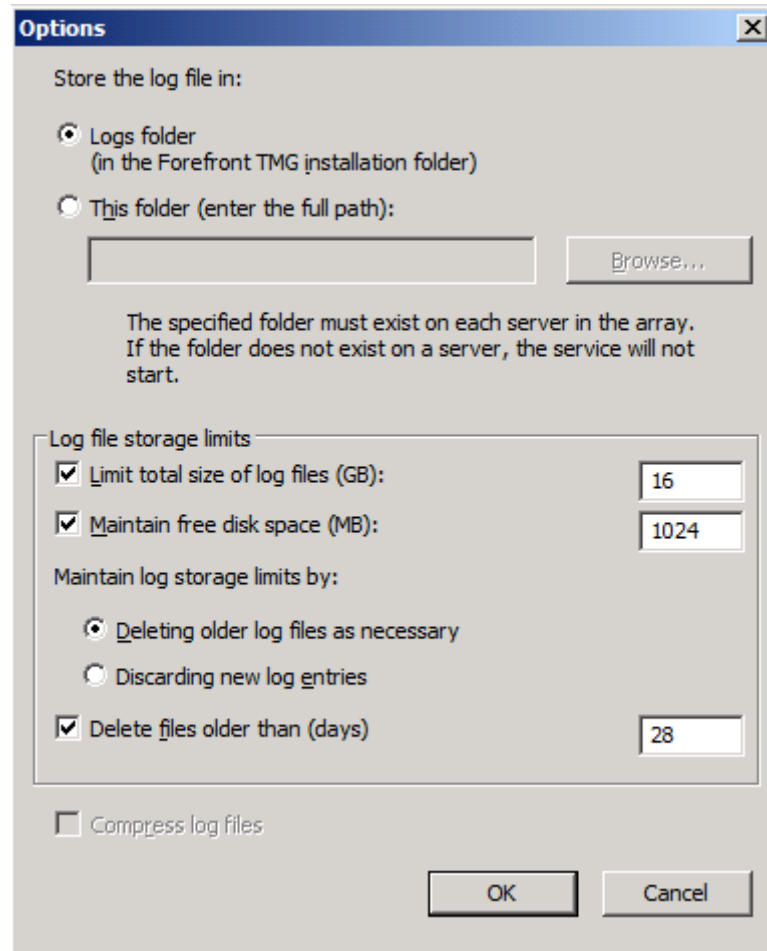
¹⁰⁹ Abból a feltételezésből kiindulva, hogy egy önálló SQL szerver alatt valószínűleg több hely van, mint az SQL Express-t használó TMG esetén.

- A fájl típusú naplózás eléggé szegényes módszer, több korláttal, az előnye gyakorlatilag a kis helyfoglalás és erőforrás-takarékosság, valamint a kompatibilitás (találkoztam már olyan 3rd party naplóelemző és statisztika készítő alkalmazással, ami csak ezt a típust ismerte). Mivel elesünk jópár előnytől, ez a típus nem szokott favorit lenni.

Mindegyik módszernek vannak előnyei és hátrányai, pl. ha az erőforrások kihasználását nézem, a helyi SQL sokkal izmosabb igényekkel bír, mint a másik kettő. A távoli SQL-be naplózás adott esetben akár jelentős hálózati forgalmat is képes generálni, lassítva a feldolgozást, ami a torlódás miatt megint csak lassít, és erőforrást is igénybe vesz, és még sorolhatnánk. Éppen ezért, az, pl. hogy mit naplózunk, ez mekkora terheléssel jár, mekkora kapacitást igényel, azt alaposan meg kell terveznünk és meg is kell figyelnünk menetközben, folyamatosan is. Számtalan olyan szituáció ismert, amikor rejtélyesnek tűnő problémák (pl. net lassulás, ideiglenes elérési hibák, stb.) megoldása a naplózás korrektebb beállítása lett.

Valamint az ehhez a témához (is) érzékenyen hozzátartozó hardver elemek (diszk, CPU, RAM) méretezése sem egy elhanyagolható rész.

Nos ennyi kitérő után folytassuk az ismerkedést. Ha az előző ábrának alapján, ugyanitt belemegyünk pl. az első típus további lehetőségeibe, akkor már kissé már ömlesztve tárul elénk több lehetőség is.



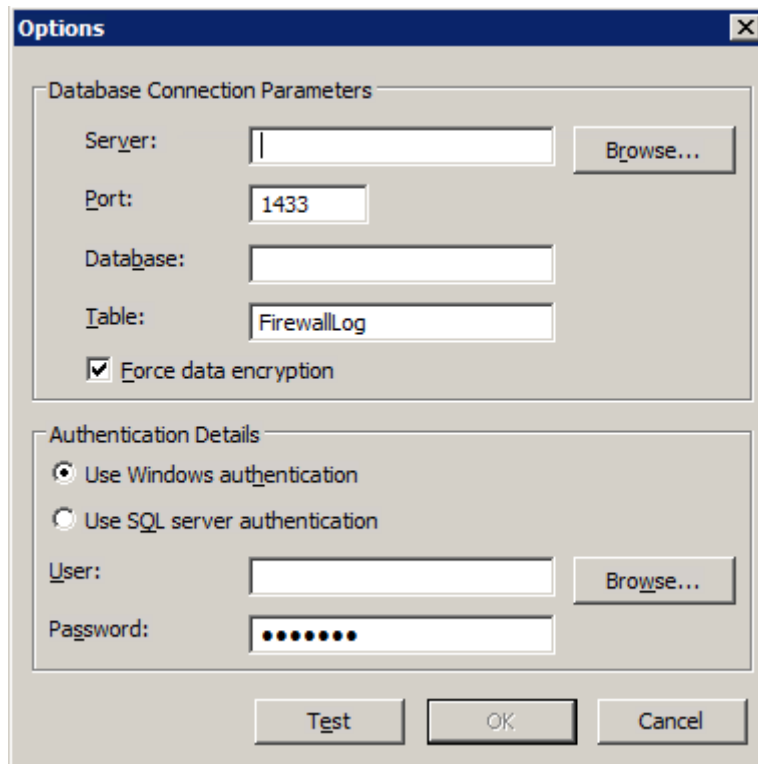
11.3 ÁBRA NAPLÓ OPCIÓK

Először is, akár naplónként (kettő van ugye, a tűzfal és a web proxy), külön-külön az alapértelmezéstől (%ProgramFiles%\Microsoft Forefront Threat Management Gateway\Logs) eltérő helyen is tárolhatjuk a naplóállományokat ("Store the log file in"), aztán a "Log file storage limits" alatt először a naplók maximális helyigényét állíthatjuk be, illetve azt is egyúttal a biztonság kedvéért, hogy minimum mennyi hely maradjon az adott diszken (Maintan free disk space (MB)).

Aztán el kell döntenünk, hogy hogyan tudjuk betartatni a korlátokat a TMG-vel. Törölje-e a régieket, ha elfogyni készül a hely (Deleting older log files as necessary), vagy ne legyenek új naplófájlok, ha elfogy a hely (Discarding new log entries). Ez utóbbi azért veszélyes dolog, hiszen ilyenkor egyáltalán nincs naplózás, és utólag sem tudjuk sehogy sem megszerezni ezeket adatokat. Végül napokban kell megadnunk azt az értéket, amelyeknél régebbi naplófájlok biztosan nem lesznek meg a lemezen (akkor sem ha van hely).

A KAPUN TÚL

Ha a fájlformátumú naplózást választjuk, akkor csupán kettő különbséget veszünk észre az opcióknál az SQL Express-hez képest. Egyrészt kétféle formátum is a rendelkezésre áll (a klasszikus W3C, illetve az TMG sajátja), plusz ha beljebb megyünk az "Options..." gomb alá, akkor mivel fájl formátumról van szó, kérhetünk tömörítést. Természetesen az SQL Database választás esetén teljesen más helyzet áll elő, hiszen ekkor a lényeg a kapcsolat felállítása és pl. a hitelesítés meghatározása, a többi dolog, pl. a napló mérete majd az SQL-től függ.

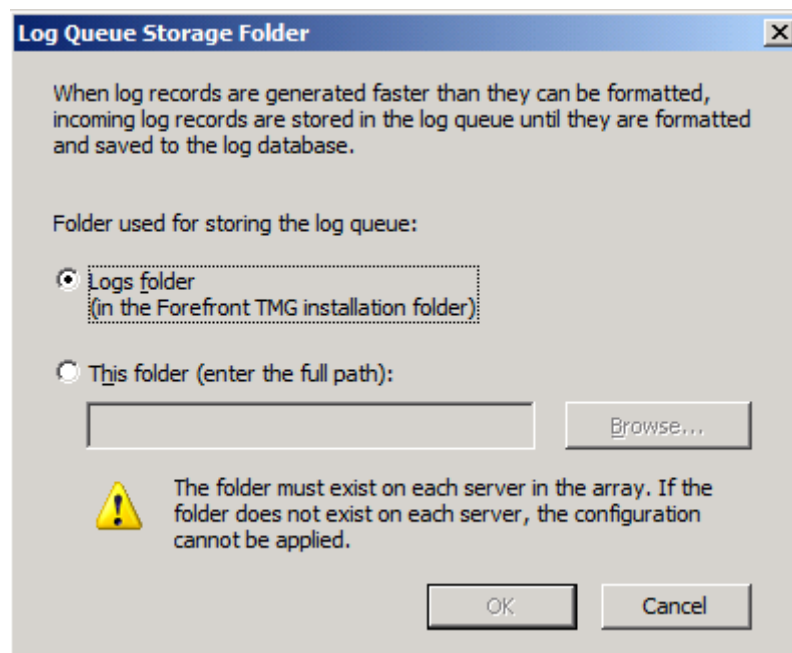


11.4 ÁBRA CÉL A "NAGY" SQL

Ha viszont a innen visszalépünk egyet, akkor egy másik fület is kiszúrhatunk, ami a "Fields" nevet viseli, és amely alatt pipálással azokat a mezőket jelöli meg a TMG, amelyek tartalma bekerülhet a naplófájlokba.



Az első ábrán ebben a fejezetben láthatunk még egy harmadik linket, ami eddig nem volt az ISA szerverekben. Ez a "Configure Log Queue", amely tipikusan egy akkor használatos, kisegítő jellegű megoldás, ha valamiért a TMG nem képes megfelelő sebességgel feldolgozni, azaz pl. formattálni a beérkező, a naplókba szánt adatokat. Így gyakorlatilag az a hely amit itt megadunk (az alapértelmezés a szokásos mappa), egy pufferként szolgál majd.

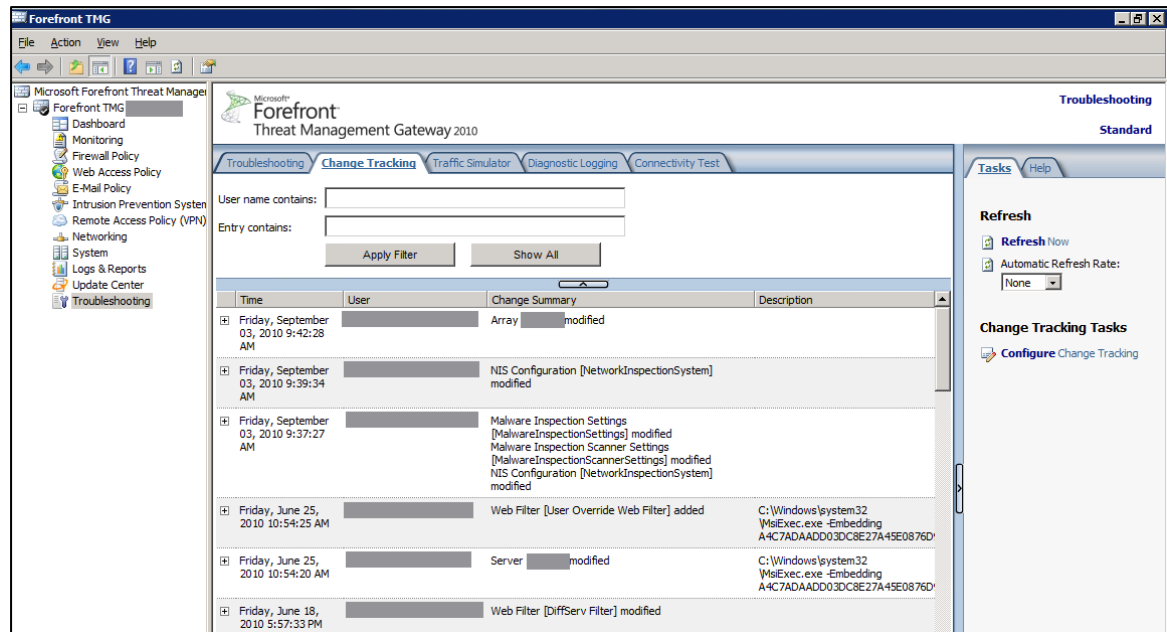


11.6 ÁBRA EGY ABSZOLÚT ÚJDONSÁG: A LOG QUEUE

Az a helyzet, hogy amit most szeretnék csak röviden bemutatni, az csak kicsit egy kapcsolódik a naplózáshoz, de azért fontos, főképp több felhasználós környezetben. A "Change Tracking"-ról beszélek, amely naplóz, de nem akármit, hanem a TMG-t ütügetők tevékenységét.

Az ISA 2006 SP1-ben jelent meg, és a TMG-ben már automatikusan be van kapcsolva (a Troubleshooting pont alatt a második fülnél találjuk). Ennek segítségével a TMG minden egyes konfigurálásról bejegyzéseket készít, amelyeket adott esetben (ha engedélyezzük a beállításai között) még egyéni megjegyzésekkel is elláthatunk, sőt kereshetünk is benne.¹¹⁰

¹¹⁰ Az Enterprise kiadással a teljes környezetben, például mindent tömböt tekintve is használhatjuk.

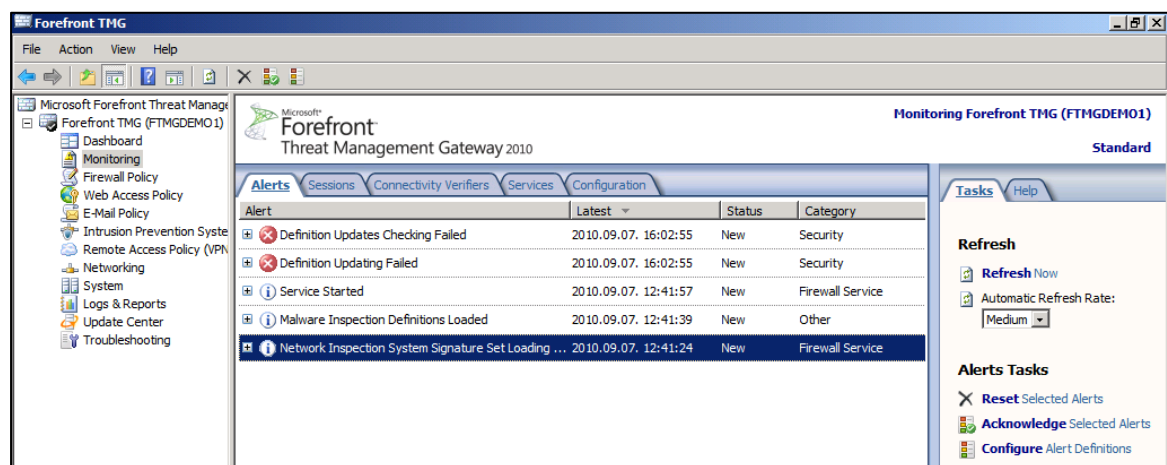


11.7 ÁBRA A CHANGE TRACKING MINDENT MOZGÁST LÁT

11.2 RIASZTÁSOK

A TMG szervereken a naplónál egy lényegesen proaktívabb módszerünk is létezik a funkcionalitás és a biztonsági állapot nyomon követésére illetve adott esetben az automatikus beavatkozásra. Nem is lehetünk meg e nélkül, hiszen a helyzet az, hogy időben tudnunk kell azt pl. hogy esetleg megáll egy TMG szerviz, vagy pl. azt, le fog járni egy tanúsítvány, vagy akár azt, hogy egy behatolási kísérlet történik éppen.

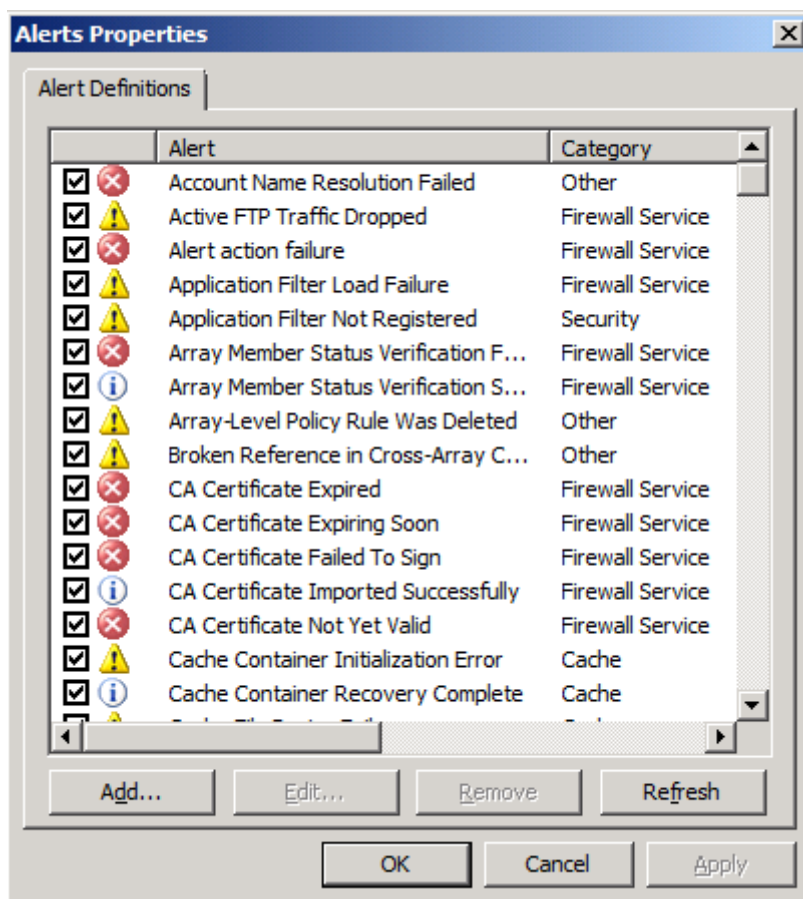
A számos, gyárilag már definiált riasztás¹¹¹ ezeket a célokat valósítja meg, de természetesen mi magunk is gyárthatunk majd egy-egy riasztást, nincs akadálya ennek.



¹¹¹ Már az ISA 2000-ben is voltak riasztások, amelyek később bővültek is, de most a TMG-ben rengeteg újat találhatunk.

Ha egy riasztás megszületik, akkor annak természetes következményeként *valamit* csinál majd a TMG. A valami helyébe beleképzelhetünk egy szkript indítást, egy program futtatást, egy e-mail küldését, illetve alapértelmezés szerint egy bejegyzést az Eseménynaplóba. De súlyosabb következmények is beállíthatóak, pl. egy szerviz indítása vagy leállítása, illetve az ún. "lockdown" mód kikényszerítése.

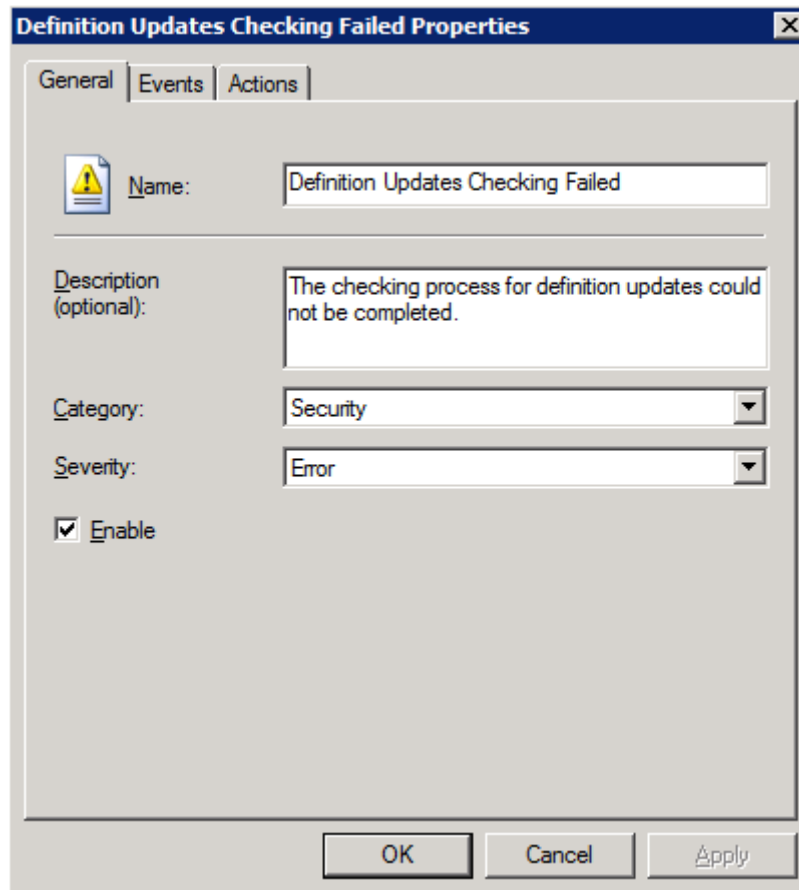
Az előző ábrán az Action pane közepén három utasítást is láthatunk. A "Reset Selected Alerts" töröl egy vagy több bejegyzést, az "Acknowledge Selected Alerts" nem töröl, csak a riasztás státuszát állítja mondhatjuk úgy, hogy "ismert"-re¹¹². A harmadikkal indul a nirvána, a "Configure Alert Definitions" nyitja meg ugyanis a már működő riasztások listáját és ezen keresztül majd a beállításait is.



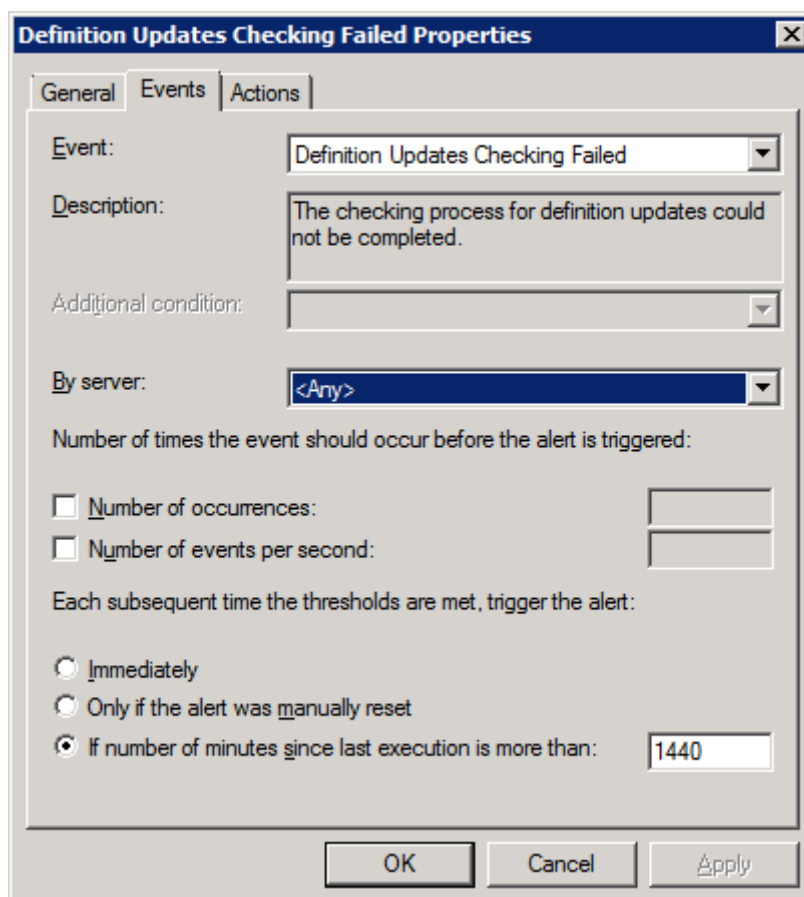
11.9 ÁBRA Kb. 260 RIASZTÁS ÁLL RENDELKEZÉSRE

¹¹² Ennek is akkor lehet értelme, ha pl. többen kezeljük az adott szerveret. Tudunk róla, de azt akarjuk, hogy minden üzemeltető tudja.

Válasszunk ki egyet egy alaposabb vizsgálatra, én most a "Definition Updates Checking Failed" nevűt szűrtem ki, amely neve magáért beszél, ez egy engedélyezett riasztás, tehát permanensen működik a telepítés óta.



11.9 ÁBRA ÁLTALÁNOS INFÓK - A CATEGORY ÉS A SEVERITY
AKKOR LESZ FONTOS, HA MI IS GYÁRTUNK RIASZTÁST



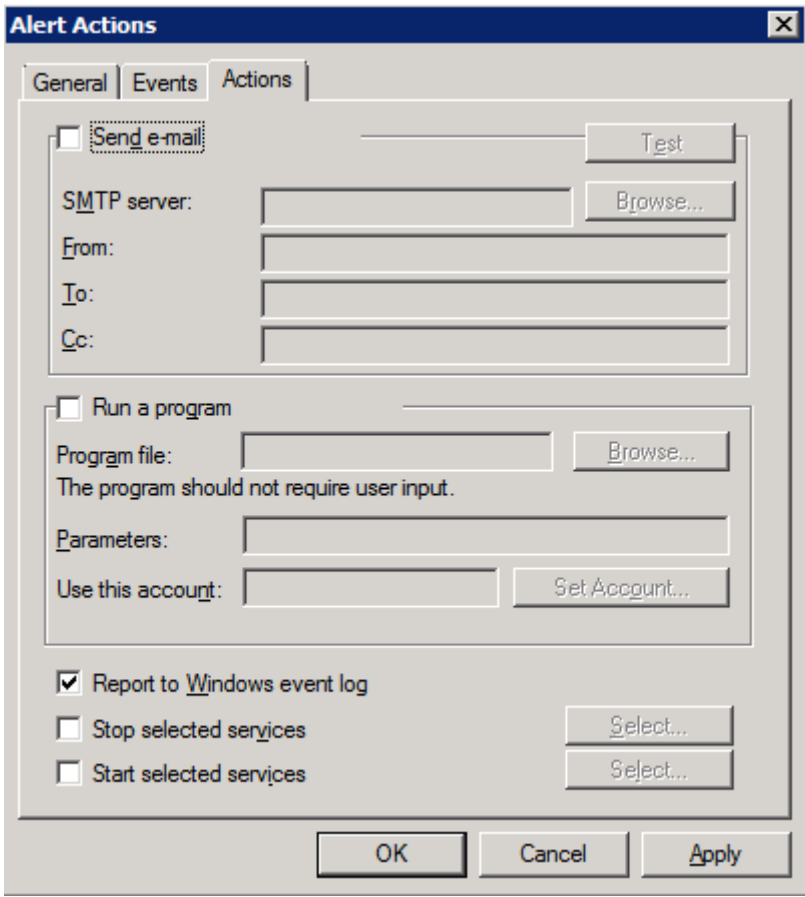
11.10 ÁBRA A TRIGGER FELTÉTELEI

Az "Events" fül alatt már izgalmasabb dolgok jönnek, ezen a panelen többek között a szabályozható a riasztás indítása (Number of times the event should occur before the alert is triggered):

- Number of occurrences: Hányszor kell megtörténnie a riasztást kiváltó eseménynek, hogy valóban riasztás legyen belőle?
- Number of events per second: Hányszor kell megtörténnie *másodpercenként* a riasztást kiváltó eseménynek, hogy valóban riasztás legyen belőle?

Az "Each subsequent time the thereholds are met, trigger the alert" rész opciói:

- Immediately: Ha bekövetkezik a kiváltó ok, azonnal mehet a riasztás.
- Only if the alert was manually reset: Csak akkor mehet a riasztás, ha már kézzel lenulláztuk (ez így gyakorlatilag a tájékoztatás rögzítésének minősül).
- If time since last execution is more than: Csak akkor mehet a riasztás ha minimum a bejegyzett értéknek megfelelő másodperc eltelik (ez ugye a definíciófrissítések hibája kapcsán 24 óra). Ez itt nyilván egy jelentős időintervallum, de ennél a szituációnál nem gond.



11.11 ÁBRA VÁLASSZUNK AKCIÓT

Az előbbi esetén egyébként a TMG egy speciális „Lockdown” módba kerül. Ilvenko

Ezen alfejezet befejezéséig még azt hadd mondjam el, hogy ha egy ennél magasabb szintű monitorozásra van szükség, akkor jöhetnek a kifejezetten nagyvállalati környezetben használatos System Center termékek, hiszen a TMG

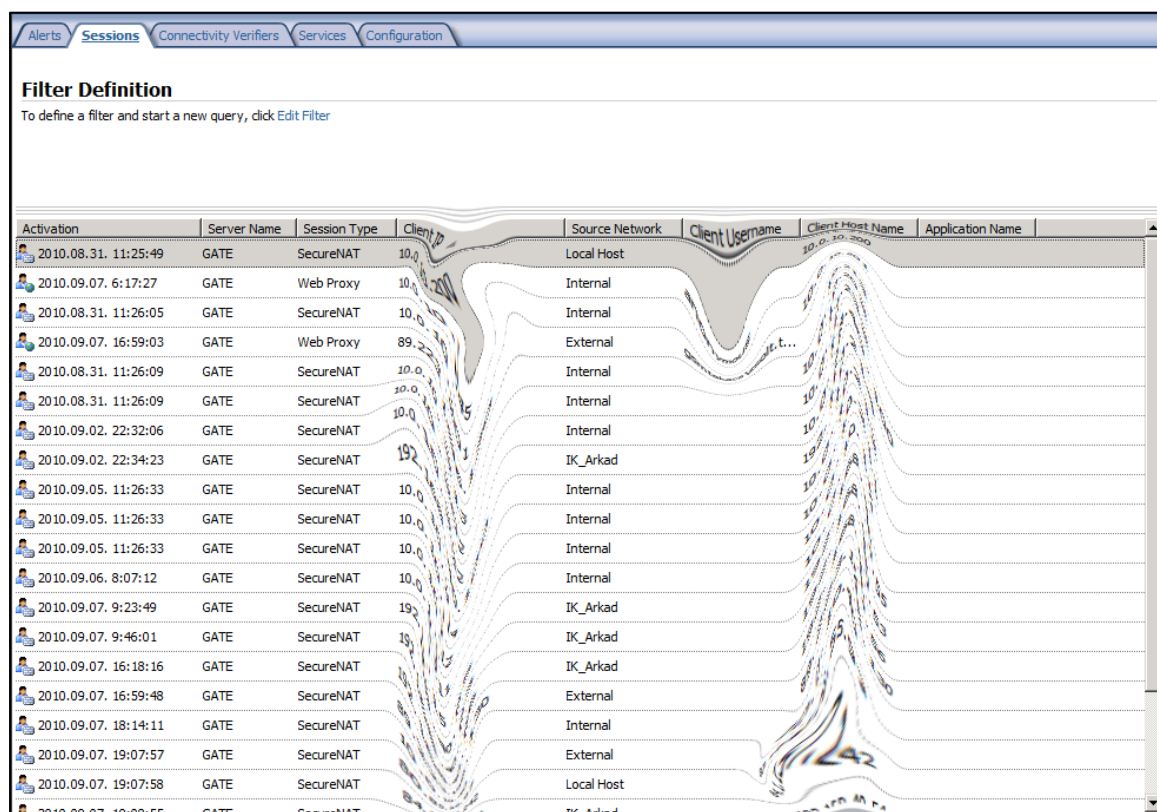
teljesen kompatibilis ezekkel, a megfelelő menedzsment csomag, pl. az SCOM-hoz rendelkezésre állnak.

Microsoft Forefront Threat Management Gateway (TMG) 2010 Management Pack for Operations Manager 2007

<http://www.microsoft.com/downloads/details.aspx?FamilyID=5BFCE6BE-B681-48BF-BDA9-A93D005820DD&displaylang=ru&displaylang=en>

11.3A LEGJOBB BARÁTAINK: SESSION MONITOR ÉS A REALTIME NAPLÓ¹¹³

A felhasználói vagy számítógép session-ok¹¹⁴ megfigyelése, illetve adott esetben megszüntetése alap feladat az TMG üzemeltető számára. A TMG konzolban a Monitoring\Sessions alatt valós képet kapunk az aktuális kapcsolódásokról, ezek típusairól (SNAT, vagy Web proxy, vagy Firewall Client), a kliens IP-jéről, hálózatról, ha hitelesített, akkor ezekről az adatokról, a host nevééről, az adott alkalmazás nevééről, valamint pl. arról, hogy ez a kapcsolat VPN-e?



Activation	Server Name	Session Type	Client IP	Source Network	Client Username	Client Host Name	Application Name
2010.08.31. 11:25:49	GATE	SecureNAT	10.0.0.1	Local Host		10.0.0.1	
2010.09.07. 6:17:27	GATE	Web Proxy	10.0.0.1	Internal			
2010.08.31. 11:26:05	GATE	SecureNAT	10.0.0.1	Internal			
2010.09.07. 16:59:03	GATE	Web Proxy	89.23.254.100	External			
2010.08.31. 11:26:09	GATE	SecureNAT	10.0.0.1	Internal			
2010.08.31. 11:26:09	GATE	SecureNAT	10.0.0.1	Internal			
2010.09.02. 22:32:06	GATE	SecureNAT	192.168.1.1	Internal			
2010.09.02. 22:34:23	GATE	SecureNAT	192.168.1.1	IK_Arkad			
2010.09.05. 11:26:33	GATE	SecureNAT	10.0.0.1	Internal			
2010.09.05. 11:26:33	GATE	SecureNAT	10.0.0.1	Internal			
2010.09.05. 11:26:33	GATE	SecureNAT	10.0.0.1	Internal			
2010.09.06. 8:07:12	GATE	SecureNAT	10.0.0.1	Internal			
2010.09.07. 9:23:49	GATE	SecureNAT	192.168.1.1	IK_Arkad			
2010.09.07. 9:46:01	GATE	SecureNAT	192.168.1.1	IK_Arkad			
2010.09.07. 16:18:16	GATE	SecureNAT	192.168.1.1	IK_Arkad			
2010.09.07. 16:59:48	GATE	SecureNAT	192.168.1.1	External			
2010.09.07. 18:14:11	GATE	SecureNAT	192.168.1.1	Internal			
2010.09.07. 19:07:57	GATE	SecureNAT	192.168.1.1	External			
2010.09.07. 19:07:58	GATE	SecureNAT	192.168.1.1	Local Host			

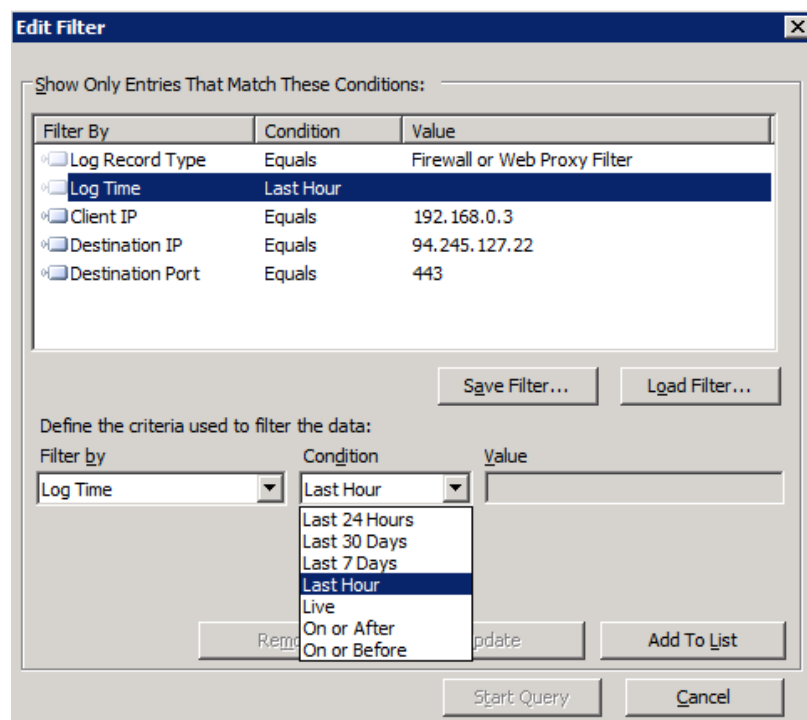
11.12 ÁBRA PÖRGÉS VAN

¹¹³ Jelzem újra, én hívom így, nem tudom mi a neve, ha van egyáltalán.

¹¹⁴ A session helyett sosem tudtam egy frappáns magyar szót írni.

Egyszóval nagyon infó megérkezik ide, de ez a rész elsősorban a megfigyelés terepe, sok teendőnk itt nem lehet. Az Action pane pontjai alapján szűrhetünk kicsit, szüneteltethetjük és leállíthatjuk a monitorozást, illetve pl. kilőhetjük a felhasználó session-két (ami csak az adott folyamat végét jelenti majd, nem végleg tiltjuk le).

Ami viszont az igazán nagy segítség pl. a hibakeresésben, az a faszervezetben kissé lentebb, a "Logs and Reports" szakaszban található a Logging fül alatt. Ez a realtime (de lehet offline is) napló, ahol tengersok jellemző alapján szűrhetünk.



11.13 ÁBRA EZ CSAK A JÉGHEGY CSÚCSA

Nézzük meg például a következő ábrát, amelyet úgy hoztam össze, hogy a "Logging" alatt az Action Pane-ben szereplő (de az ábrán nem látszó) "Edit Filter" parancssal összeválogattam a szűrési szempontokat.

A KAPUN TÚL

Microsoft Forefront Threat Management Gateway 2010

Logs & Reports Standard

Logging Reporting

Filter By Condition Value

Log Record Type Equals Firewall or Web Proxy Filter 1

Log Time Last Hour 2

Client IP Equals 192.168.0.3 3

Destination IP Equals 94.245.127.22 4

Destination Port Equals 443 5

Log Time	Client IP	Destination IP	Dest...	Protocol	Action	Result Code	HTTP Status Code	Log Record T...
9/7/2010 7:28:42 PM	192.168.0.3	94.245.127.22	443	SSL-tunnel	Allowed Connection 6	0x0 SUCCESS	0 The operation compl...	Web Proxy Filter
9/7/2010 7:28:42 PM	192.168.0.3	94.245.127.22	443	BranchCache - Advertise	Initiated Connection	0x0 SUCCESS		Firewall
9/7/2010 7:28:41 PM	192.168.0.3	94.245.127.22	443	SSL-tunnel	Allowed Connection	0x0 SUCCESS	0 The operation compl...	Web Proxy Filter
9/7/2010 7:28:41 PM	192.168.0.3	94.245.127.22	443	BranchCache - Advertise	Initiated Connection	0x0 SUCCESS		Firewall
9/7/2010 7:28:41 PM	192.168.0.3	94.245.127.22	443	BranchCache - Advertise	Closed Connection	0x80074e21 FWX_E_ABORTIVE_S...		Firewall
9/7/2010 7:28:41 PM	192.168.0.3	94.245.127.22	443	BranchCache - Advertise	Closed Connection	0x80074e21 FWX_E_ABORTIVE_S...		Firewall
9/7/2010 7:28:41 PM	192.168.0.3	94.245.127.22	443	BranchCache - Advertise	Initiated Connection	0x0 SUCCESS		Firewall
9/7/2010 7:28:39 PM	192.168.0.3	94.245.127.22	443	BranchCache - Advertise	Initiated Connection	0x0 SUCCESS		Firewall

Allowed Connection

Log type: Web Proxy (Forward)

Status: 0 The operation completed successfully.

Rule: [redacted]

Source: Internal (192.168.0.3:53187) 7

Destination: External (94.245.127.22:443)

Request: - emea.mail.microsoft.com:443

Filter information: Req ID: 0809c0e9

Protocol: SSL-tunnel

User: anonymous

Additional information

- Object source: Internet (Source is the Internet. Object was added to the cache.)
- Cache info: 0x0
- Processing time: 0 MIME type: -

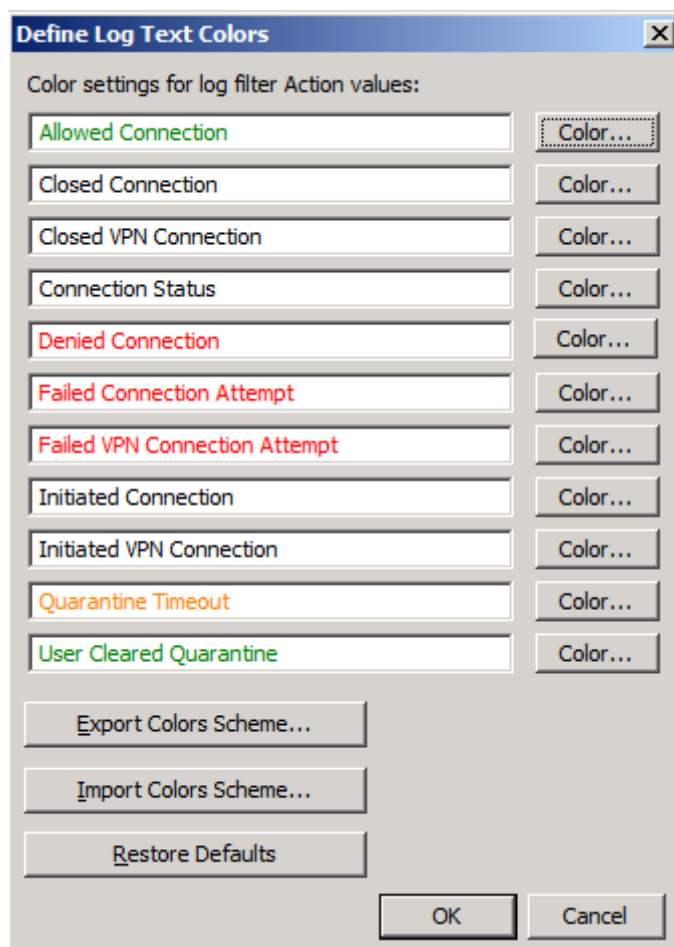
9/7/2010 7:28:41 PM

11.14 ÁBRA A SZŰRÉS EREDMÉNYE

1. Kétféle naplóra is szűrünk.
2. Az elmúlt 1 óra történéseiből válogatunk.
3. Egy adott forrás IP érdekel bennünket.
4. És egy adott cél IP felé menő forgalom.
5. Meghatározott porton.
6. Zölddel jelenek meg a valamely szabály által engedélyezett forgalmak, piros lenne a tiltott, és ha jól megnézzük a vízszintes gördítő sávot, akkor az is kiderül ebből, hogy
7. További részletek kibontva. Itt látszik a szürke csík alatt a vonatkozó szabály neve. Ez óriási segítség tud lenni, hiszen egyből kiderül hogy melyik az amelyik engedélyezi mondjuk a hozzáférést, vagy éppen tiltja.

Kétdimenziós formában nem tudom ennél jobban bemutatni a lehetőségeket, pedig még bőven lenne mit, de javaslom, hogy térjünk be ide rendszeresen, menetközben rengeteget tanulhatunk a forgalom illetően elemzésével.

Zárásképpen még egy dolog: ugyanebben az ablakban (Logging) jobbra, az "Action Pane\Related Tasks" alatt kiegészítő műveleteket is végezhetünk a szűrés kapcsán, mint pl. a színezés beállítása, vagy szűrőfeltételek mentése és betöltése, az eredmények másolása a vágólapra, vagy éppen az IPv6-os forgalom elrejtése.



11.15 ÁBRA MÉG SZÍNEZHETÜNK IS

11.4 EGY ÚJABB BARÁT: A CONNECTIVITY VERIFICATION

Az ISA Server 2004 óta velünk van ez a kissé meglepő, de hasznos szolgáltatás. A Local Host géptől kiindulva ellenőrizhetünk kapcsolatokat, bármely hálózaton (tehát az Interneten is) pl. szerverekhez ennek a szolgáltatásnak a segítségével. Egy további fontos pozitívuma pedig ennek a szolgáltatásnak az, hogy egyszerűen beállíthatjuk, hogy generáljon riasztásokat egy-egy kapcsolat elvesztésekor, illetve az újra kapcsolódásakor is.

Többféle módszer is a rendelkezésünkre áll, a Monitoring harmadik füle alatt:

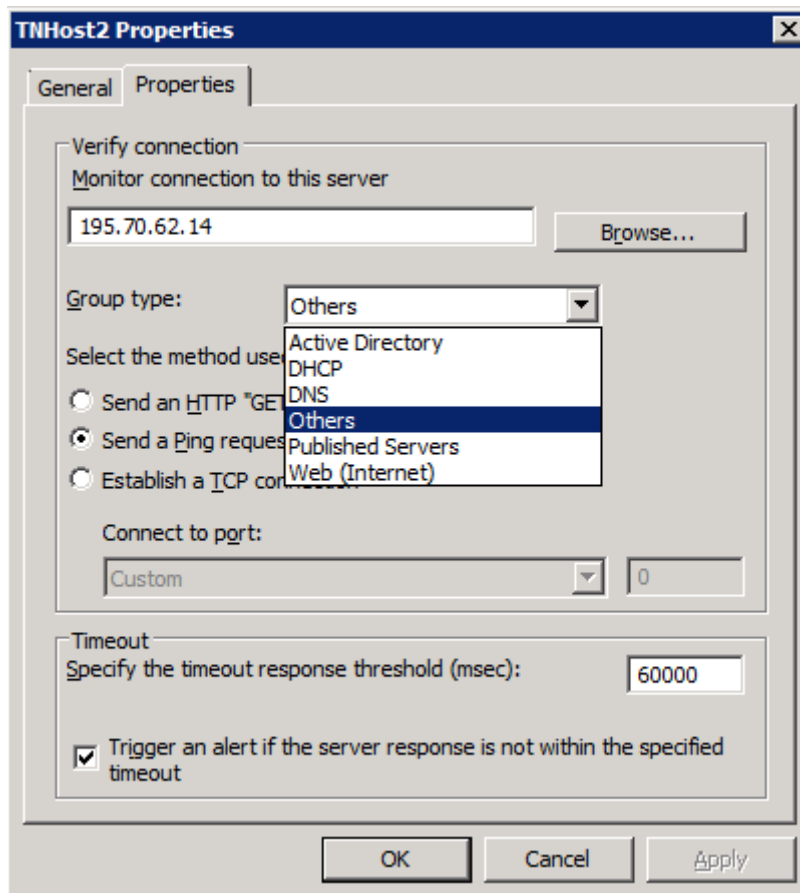
- Ping: A TMG egy ICMP ECHO_REQUEST-et küld és egy ICMP ECHO_REPLY-t vár el cserébe.
- TCP connect: A TMG egy általunk beállítható TCP porton (pl. TCP21 egy FTP szerver esetén) próbál kapcsolódni az adott kiszolgálóhoz.
- HTTP request: Ha ezt választjuk, egy HTTP kérést küld a TMG és vár a válasza (nyilván ez lesz a jó módszer egy webszerver esetén).

A KAPUN TÚL

A Timeout szakaszban beállíthatjuk még azt is, hogy mennyi időnként történjen meg ez az ellenőrzés milliszekundumban, valamint, hogy legyen-e riasztás („Trigger an alert if the server response is not within the specified timeout”). Aztán ehhez a riasztáshoz az „Alerts” szakaszban már könnyű lesz pl. egy e-mail küldést hozzárendelni¹¹⁵.

A frissítési időköz (Refresh Rate) viszont egy másik opció, amire szükségünk lehet, ellenben ez nincs kint a GUI-n. Az alapértelmezése 30 mp, de egyébként maximum 1440 mp-re, azaz 24 percre „húzható fel”, szkripttel:

<http://technet.microsoft.com/en-us/library/cc302480.aspx>



11.16 ÁBRA MŰKÖDIK, VAGY NEM?

- A HTTP/S kérések esetén a System Policy 19-es szabálya engedélyezi a forgalmat - automatikusan, ha használjuk.
- A web farm publikálásnál is létezik, de integráltan, azaz pl. a varázslóba építve is találkozhatunk vele.

¹¹⁵ De a gyári riasztások nevét leírom, mert ezt viszont nem könnyű megtalálni: „No Connectivity” illetve „Connectivity Restored”.

11.5 JÓ BARÁTOKBÓL SOSEM ELÉG: A BPA

A BPA jelentése a Best Practice Analyzer, és szerencsére jó régóta létezik ez az ingyenesen letölthető eszköz a Microsoft szervereihez, eleinte csak Sharepoint-hoz és Exchange-hez, de aztán az ISA kiszolgálókhoz is megjelentek sorra a megfelelő verziók, sőt a Windows Server 2008 R2 óta immár nem egy külön letölthető változatban, hanem pl. a Server Managerbe beépítve is találkozhatunk a BPA tudásával.

A TMG BPA 8.0.1-es változata jelenleg a legfrissebb, innen le is szedhetjük:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=8aa01cbo-dag6-46d9-a50a-b245e47e6b8b>¹¹⁶

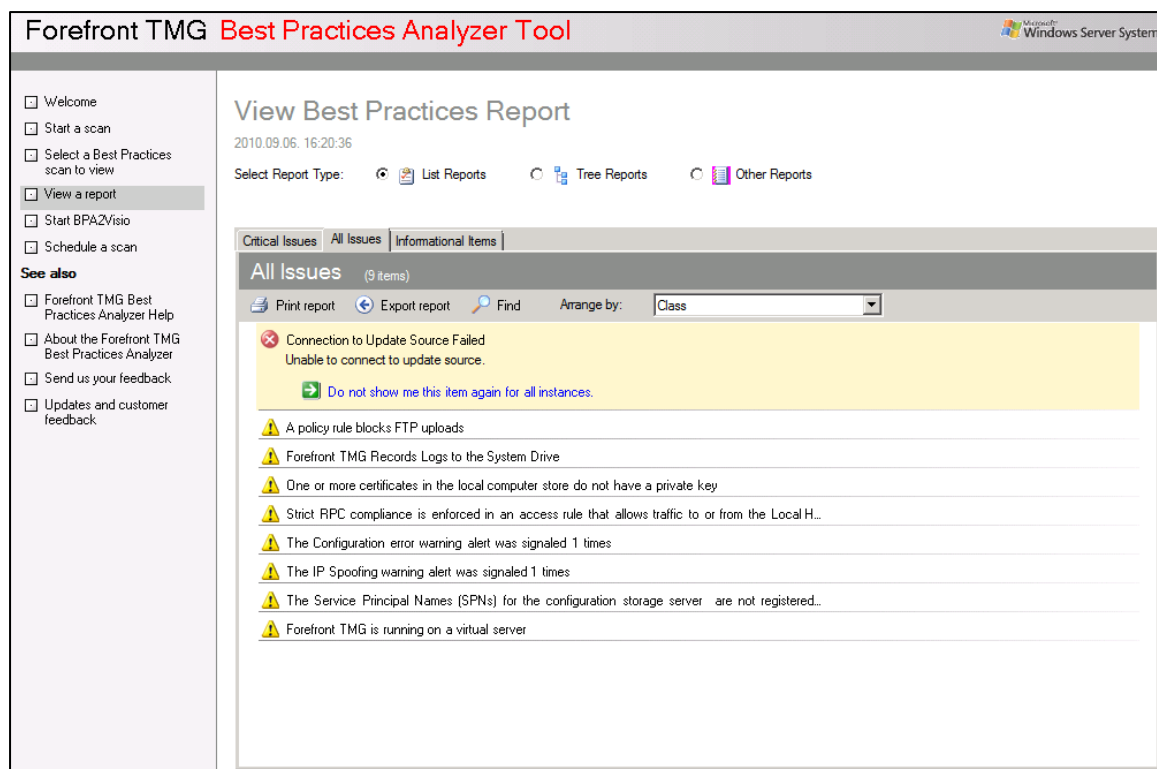
De mit is csinál? Összehasonlít. Egy ideális, optimális konfigurációt ahhoz, amit mi kalapáltunk össze. Ezenkívül felismer még jópár jelenséget a termék működésével kapcsolatban, és a közölnivalóját három kategóriába osztva hibák, figyelmeztetések, vagy egyszerűen csak információs csomagok formájában és összesítve meg is jeleníti..

Ha erről a cuccról van szó, akkor én két dolgot szoktam kiemelni előnyként.

- Ha kezdők vagyunk (mindenki így indul), akkor a tippek, illetve a konfigban per pillanat lévő hibák, vagy hiányosságok listázása egy remek terep a tanuláshoz (arról nem is beszélve, hogy problémákat oldunk meg ☺)
- Ha már rutinos versenyzők vagyunk, akkor ellenőrzésre, 2 év múlva az adott konfig újbóli átvizsgálására is tökéletesen alkalmas az eszköz. Az hogy a 63. szabályban kikapcsoltam-e az FTP upload tiltás opciót, az ránézésre nem nyilvánvaló, de a BPA futtatása után rögtön kiderül, hogy ráadásul az 52.-ben és a 20-asban is ugyanezt ezt tettem.

A használat pofonegyszerű, letöltjük és telepítjük, majd elindítjuk. Nem árt ha megkérjük arra, hogy mindig frissítsen (ugyanis ez egy olyan eszköz, amely tudásanyagát rendszeresen frissítik a beérkező problémák, és hibajelenségek, leírások alapján).

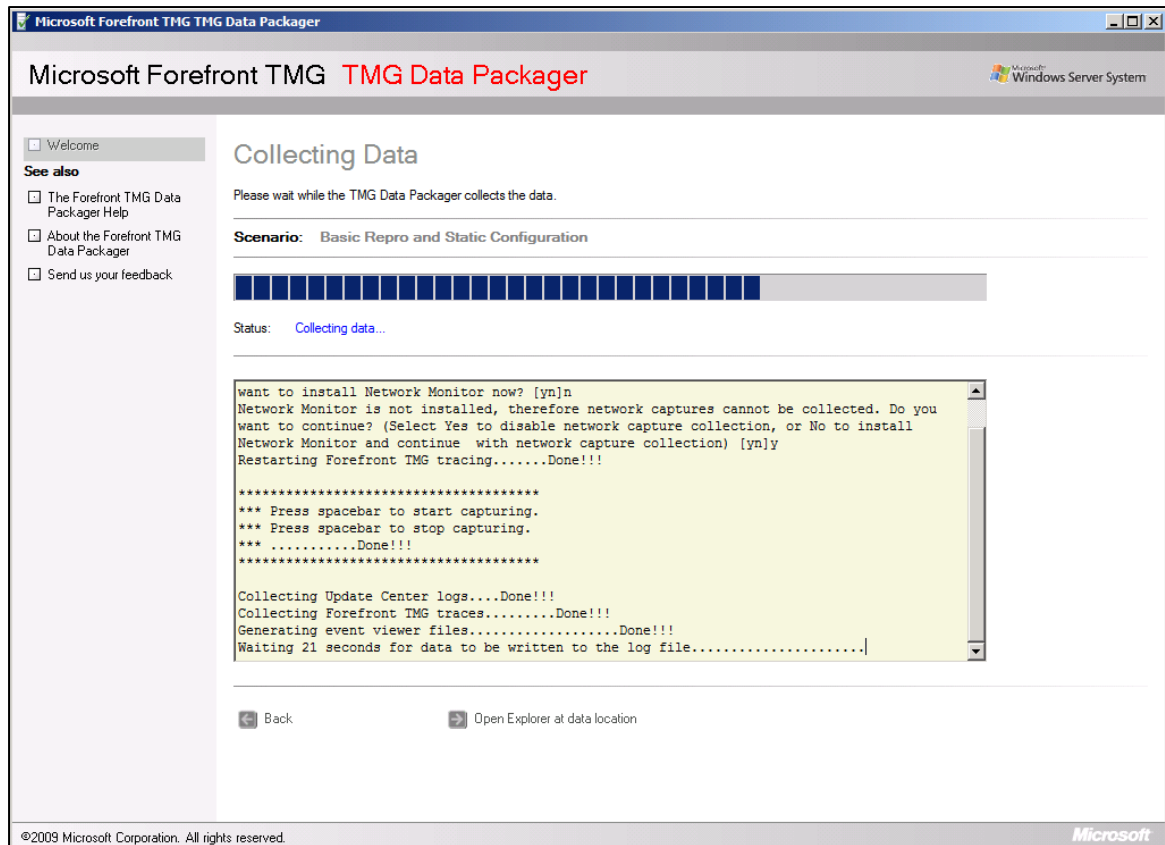
¹¹⁶ De az ISA 2006 SP1-től a baloldali faszerkezetben, a "Troubleshooting" alól is elérjük ezt a linket.



11.17 ÁBRA A BPA FIGYELMEZTET ÉS JAVASOL

Így tehát ha valami rejtélyes gond van a TMG-vel, és ha az Eseménynapló vagy a TMG naplók nem adnak elég segítséget akkor segíthet a BPA.

De van egy alternatív felhasználási területe is, amikor is valaki másnak szeretnénk megmutatni - nagyon részletesen, de egy csomagban – problémát. Ugyanis az már emlegetett szimpla "egészségi" állapotvizsgálat illetve BPA2Visio (Visio-ba importálás) mellett az TMG BPA-nak van egy ún. Data Packager üzemmódja is (külön a Start menüből kell indítani), ahol nagyon részletes beállításokkal és pl. probléma-szűkítő sablonokkal is bővíthetjük a vizsgálatot. Ráadásul menetközben - ha kérjük - a Network Monitort is feltelepíti és használja is.



11.18 ÁBRA MŰKÖDIK A DATA PACKAGER

Ehhez kövessük az itt szereplő, igaz még az ISA-ra vonatkozó részletes, képernyőképekkel illusztrált bemutatót (a második link az igazi, az első viszont a szimpla BPA használatban segít.)

Using ISABPA For Proactive And Reactive Work On ISA Server - Part 1

<http://blogs.technet.com/yuridiogenes/archive/2009/03/13/using-isabpa-for-proactively-and-reactively-work-with-isa-server-part-1-of-2.aspx>

Using ISABPA For Proactive And Reactive Work On ISA Server - Part 2

<http://blogs.technet.com/yuridiogenes/archive/2009/05/07/using-isabpa-for-proactive-and-reactive-work-with-isa-server-part-2-of-2.aspx>

12 A RÁADÁS: AZ SP1

A TMG RTM megjelenési dátuma 2009. november közepére tehető. Eme könyv első adagjának elkészítésekor (2010 februárjában) még csak csendes susogást lehetett hallani az első szervizcsomagról, de azért élénk susogást, rövid határidőkkel. Aztán Forefront MVP mivoltomból fakadóan, áprilisban már kaptam egy példány, amit gyorsan feldobtam a Hyper-V-s gépemre, és nagyon megörültem a csomagnak, mert már akkor látszott, hogy nemcsak a hotfixek és a patch-ek összegyűrásáról van szó¹¹⁷, hanem - bár még csak egy félév telt el az RTM óta - kapunk is újdonságokat.

Aztán jött egy újabb, majd egy még újabb béta, és 2010. június közepére publikusan is megjelent az SP1. És gyakorlatilag nem került ki belőle semmi a bétákhoz képest, nézzük tehát most sorban végig, hogy mit kapunk, ha feltelepítjük.

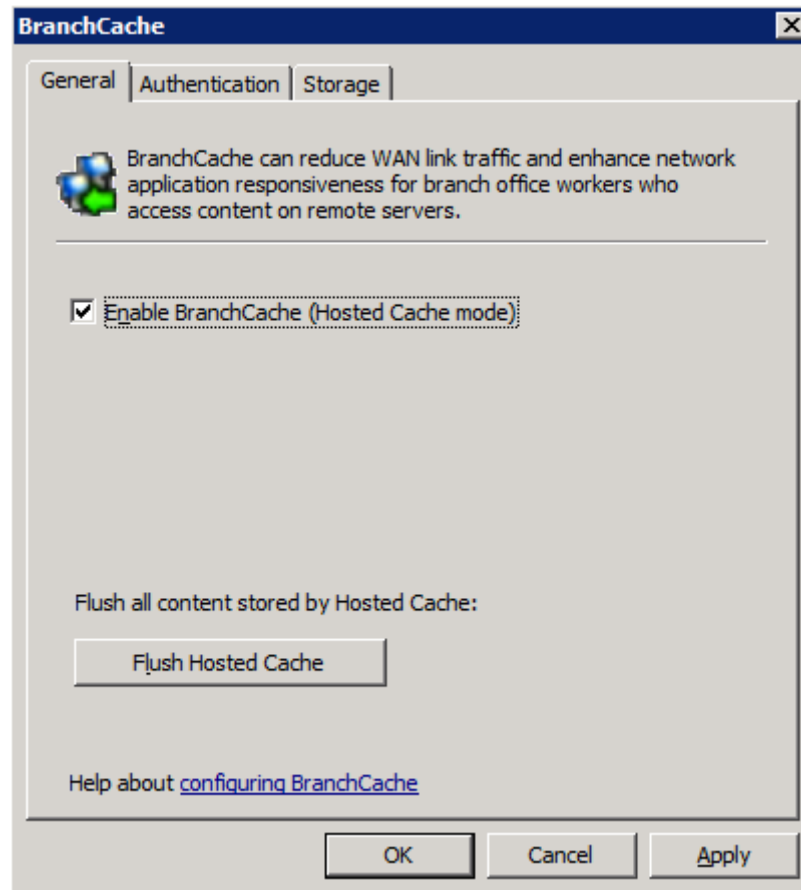
Microsoft Forefront Threat Management Gateway (TMG) 2010 Service Pack 1
<http://www.microsoft.com/downloads/details.aspx?FamilyID=fofd5770-7360-4916-a5be-a88aofd76c7c&displaylang=en>

12.1 BRANCHCACHE, RODC, SHAREPOINT 2010

Az első két képesség kihasználása főképp a telephelyi környezetben érdekes és fontos. Ha pl. már egyébként is van egy TMG-nk a telephelyen (és ugye ez Windows Server 2008 R2 alatt fut), akkor örülni fogunk, hiszen az SP1 telepítése után a TMG konzolból engedélyezhetjük a BranchCache "hosted cache" üzemmódban történő működését. Ráadásul itt a GUI-n, a TMG konzolból gyakorlatilag minden beállítást elvégezhetünk, amelyet pl. a netsh-val tennénk meg egyébként.

A BranchCache-ről rengeteg írtunk és előadtunk már, de a lenti linken, komplett előadás és demó screencastokat is megtekinthetünk erről az újdonságról:
<http://www.microsoft.com/hun/technet/article/?id=aef89148-1f12-4ee3-8f33-8b0df92471b8>

¹¹⁷ Azért vannak ilyenek is benne, egész pontosan 22 db.
<http://technet.microsoft.com/en-us/library/ff686708.aspx>



12.1 ÁBRA BRANCHCACHE KONFIGURÁLÁS

Egy másik érdekes dolog a Windows Server 2008-cal érkezett RODC képesség (Read-Only DC, azaz a csak olvasható tartományvezérlő) egybegyűrása a TMG-vel. Ez megint csak egy kifejezetten a telephelyekre fókuszáló képesség, amelyet immár telepíthetünk a TMG gépre is, pontosabban fordítva, az eddigi receptek szerint előbb a RODC, majd aztán jöhet a TMG.

A klasszikus tartományvezérlők továbbra sem képesek (és tegyük a szívünkre a kezünket: abszolúte nem is okos dolog, és nem is ajánlott) ugyanazon a gépen futni, mint a TMG, telepítés közben szép kerek hibaüzenet kapunk majd, ha ezzel próbálkozunk, és mivel az TMG RTM még ilyen, ezért ha a szándékunk határozott RODC ügyben, akkor össze kell ragasztanunk (slipstream) az eredeti telepítő anyagot az SP1-gyel.

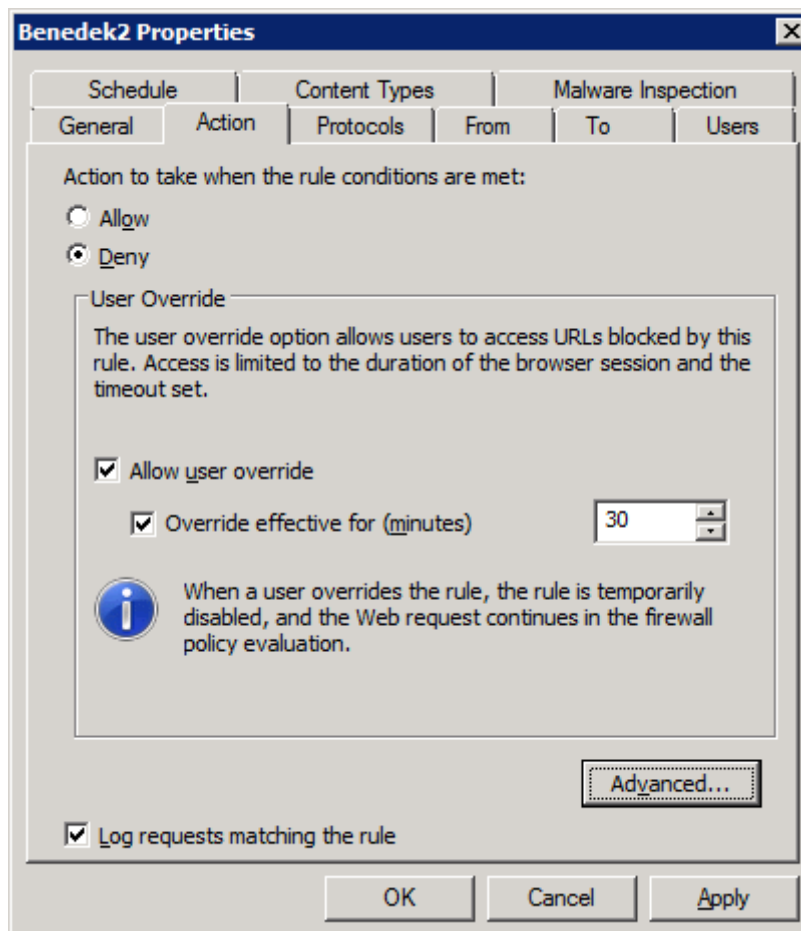
Ennek lépéseit, illetve a RODC/TMG telepítés gyakorlati részleteit megtaláljuk ezen a TechNet oldalon:

<http://technet.microsoft.com/en-us/library/ff808305.aspx>

És végül az SP1-gyel az időközben megjelent Sharepoint 2010 publikálása is egyszerűbbé vált, az immár integrált publikálás varázsló segítségével.

12.2 URL SZŰRÉS VÁLTOZÁSOK

Tegyük fel, hogy úgy érezzük (pl. a felhasználóink szűnni nem akaró nyomása alapján), hogy rengeteg téves blokkolást eredményez az URL szűrés bevezetése. Mivel látgyszívűek vagyunk (brrrr), ezért örülünk annak a lehetőségnek, amellyel az SP1 kecsegtet: a felhasználók manuálisan felülbírálhatják a szűrést!



12.2 ÁBRA USER OVERRIDE

Ezt persze először engedélyeznünk kell (szabályonként), és ekkor még azt is megadhatjuk (de mi és nem ők), hogy mennyi ideig legyen érvényes a feloldás, ha egyáltalán szükséges ez.

Kiválóan működik ez az újdonság, a következő képen meg is lehet tekinteni, hogy milyen formában jelenik meg a böngészőben, illetve az azután következőben azt is, hogy a naplóból azért nyomon követhető, hogy ki és mikor él ezzel a lehetőséggel.

X

Network Access Message: Access Denied

Explanation:

The Web site you are trying to access is categorized as "Pornography"

If you consider this site to be categorized incorrectly, or that you are receiving this message by mistake, contact your administrator or helpdesk.

You can access this Web site by clicking the "Override Access Restriction" button. Note that your access to this Web site will be logged.

Technical Information (for support personnel)

- Error Code: 403 Forbidden. (12240)
- IP Address: [REDACTED]
- Date: 9/5/2010 9:13:58 PM [GMT]
- Server: [REDACTED]
- Source: proxy

[Report a URL to Microsoft Reputation Service as incorrectly categorized](#)

12.3 ÁBRA A GYEREKEM PORNÓT AKAR NÉZNI, ÉS ÉN RÁ BÍZOM A DÖNTÉST

Client IP	Destination IP	Destination Port	Protocol	Action	Overridden Rule	NIS Scan Resu
[REDACTED]	74.125.87.101	80	http	Allowed Connection	-	
[REDACTED]	66.196.65.174	80	http	Allowed Connection	-	
[REDACTED]	66.196.65.174	80	http	Allowed Connection	-	
[REDACTED]	192.221.107.126	80	http	Allowed Connection	Benedek2	
[REDACTED]	80.239.230.179	80	http	Allowed Connection	-	
[REDACTED]	173.192.60.243	80	http	Allowed Connection	Benedek2	
[REDACTED]		8080	HTTP Proxy	Initiated Connection		
[REDACTED]		8080	HTTP Proxy	Initiated Connection		
[REDACTED]		8080	HTTP Proxy	Initiated Connection		

Allowed Connection

Log type: Web Proxy (Forward)

Status: 200 OK.

Rule: Benedek

Source: Internal [REDACTED]

Destination: External (173.192.60.243-static.reverse.softlayer.com 173.192.60.243:80)

Request: GET http://www.youporn.com/

Filter information: Req ID: 080966bd

Protocol: http

User: anonymous

[Additional information](#)

12.4 ÁBRA ÉS DÖNTÖTT

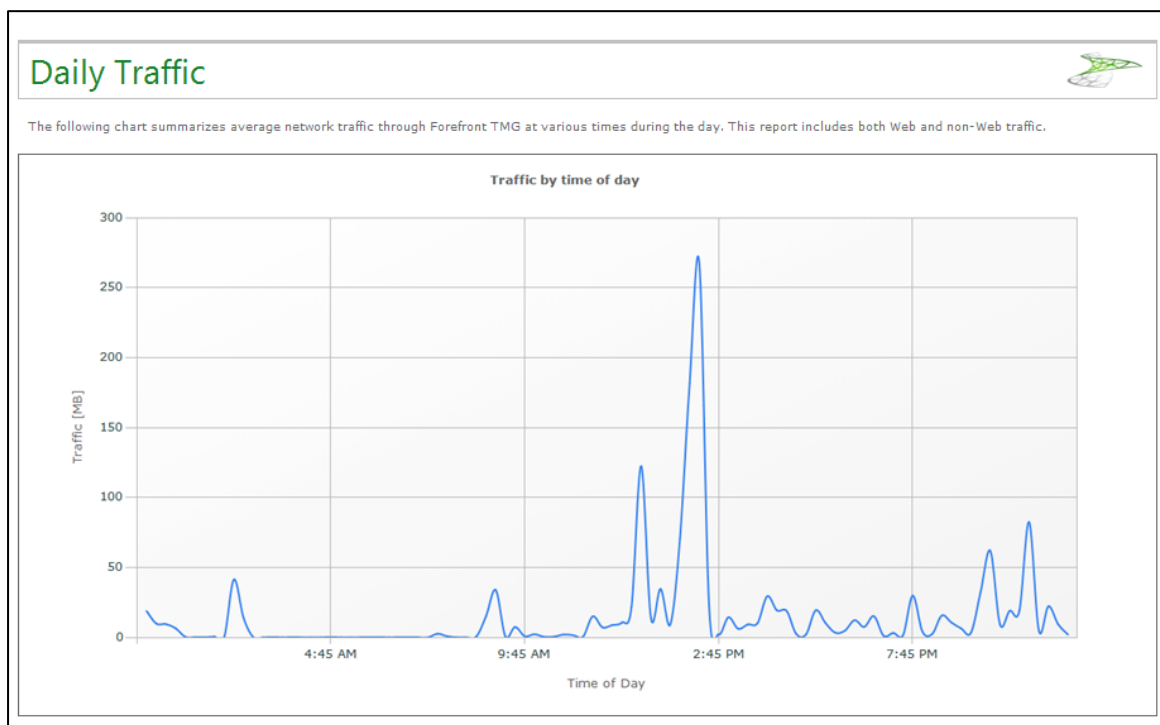
(DE AZÉRT A LOGBÓL MINDEN LÁTSZIK - AZ OVERRIDEN RULE OSZLOPBAN LÁTHATÓ A LÉNYEG)

A KAPUN TÚL

Egyetlen furcsaságot vettem csak észre, amikor beüzemeltem ezt a lehetőséget, egészen addig nem engedte érvényesíteni a megváltozott szabályt a TMG, amíg a HTTPS-t ki nem szedtem a szabályból, mert ezzel nem működik együtt az User Override és ez by design. Ugyanis egy cookie alapú „azonosítás” történik és az IE7/8 például nem engedi azt, hogy a https adatfolyamba belepíszkáljunk ilyen formában.

12.3 ÚJDONSÁGOK A JELENTÉSEKNÉL

A következő szakasz gyakorlatilag csak egy képes beszámoló, hiszen itt ez a lényeg. Egyrészt vizuálisan megújult a jelentések kinézete, másrészt kérhetünk egy ún. User Activity reportot is, az Action Panel\Tasks\Create User Activity Report Job pont alatt (ilyen képem sajnos nincs).



12.5 ÁBRA SZINES-SZAGOS (MÁR ALAPOSAN RÁFÉRT A VÁLTOZÁS)

Top URL Categories



Browsing to the following URL Categories generated the largest amount of network traffic through Forefront TMG during report period. The most popular URL Categories are listed first.

Category	Requests	% of Total Requests	Total Bytes	% of Total Bytes	Bytes In	% of Total Bytes In	Bytes Out	% of Total Bytes Out
Unknown	129,838	85.3 %	138.36 MB	20.4 %	54.99 MB	9.7 %	83.37 MB	75.0 %
Technical Information	7,892	5.2 %	182.70 MB	27.0 %	171.68 MB	30.3 %	11.02 MB	9.9 %
Search Engines	2,301	1.5 %	35.10 MB	5.2 %	33.51 MB	5.9 %	1.59 MB	1.4 %
Online Communities	2,054	1.4 %	27.13 MB	4.0 %	25.83 MB	4.6 %	1.30 MB	1.2 %
Pornography	2,038	1.3 %	86.01 MB	12.7 %	84.61 MB	14.9 %	1.40 MB	1.3 %
Internet Services	1,737	1.1 %	39.16 MB	5.8 %	31.20 MB	5.5 %	7.96 MB	7.2 %
Web Ads	1,205	0.8 %	6.53 MB	1.0 %	5.67 MB	1.0 %	880.25 KB	0.8 %
General Business	917	0.6 %	8.44 MB	1.2 %	7.70 MB	1.4 %	755.55 KB	0.7 %
Blogs/Wiki	691	0.5 %	8.69 MB	1.3 %	8.25 MB	1.5 %	446.38 KB	0.4 %
Education/Reference	587	0.4 %	10.35 MB	1.5 %	10.00 MB	1.8 %	353.35 KB	0.3 %
Free Hosting	273	0.2 %	3.04 MB	0.4 %	2.78 MB	0.5 %	271.49 KB	0.2 %
News	239	0.2 %	3.07 MB	0.5 %	2.95 MB	0.5 %	122.42 KB	0.1 %
Shopping	230	0.2 %	1.82 MB	0.3 %	1.68 MB	0.3 %	141.04 KB	0.1 %
Portal Sites	220	0.1 %	4.07 MB	0.6 %	3.83 MB	0.7 %	245.39 KB	0.2 %
General Entertainment	217	0.1 %	2.67 MB	0.4 %	2.56 MB	0.5 %	118.16 KB	0.1 %
All Others	1,691	1.1 %	120.06 MB	17.7 %	118.82 MB	21.0 %	1.24 MB	1.1 %
Total	152,130	100.0 %	677.21 MB	100.0 %	566.07 MB	100.0 %	111.14 MB	100.0 %

12.6 ÁBRA URL KATEGÓRIÁK SZERINT IS

Top Blocked Users



The following users generated the largest number of requests to access a blocked URL during the report period. Network addresses are presented when user names are unknown to Forefront TMG (unauthenticated Web Proxy clients).

No	User	Requests	% of Total Requests
1		2	100.0 %
	All Others		
Total		2	100.0 %

Top Restricted URL Categories



Restricted Categories are URL Categories for which users should not have access according to the Firewall policy. The report shows the Restricted URL Categories for which access attempts were most frequent during the Report period. Categories with most frequent access attempts are listed first.

No	Category	Requests	% of Total Requests
1	Pornography	2	100.0 %
	All Others		
Total		2	100.0 %

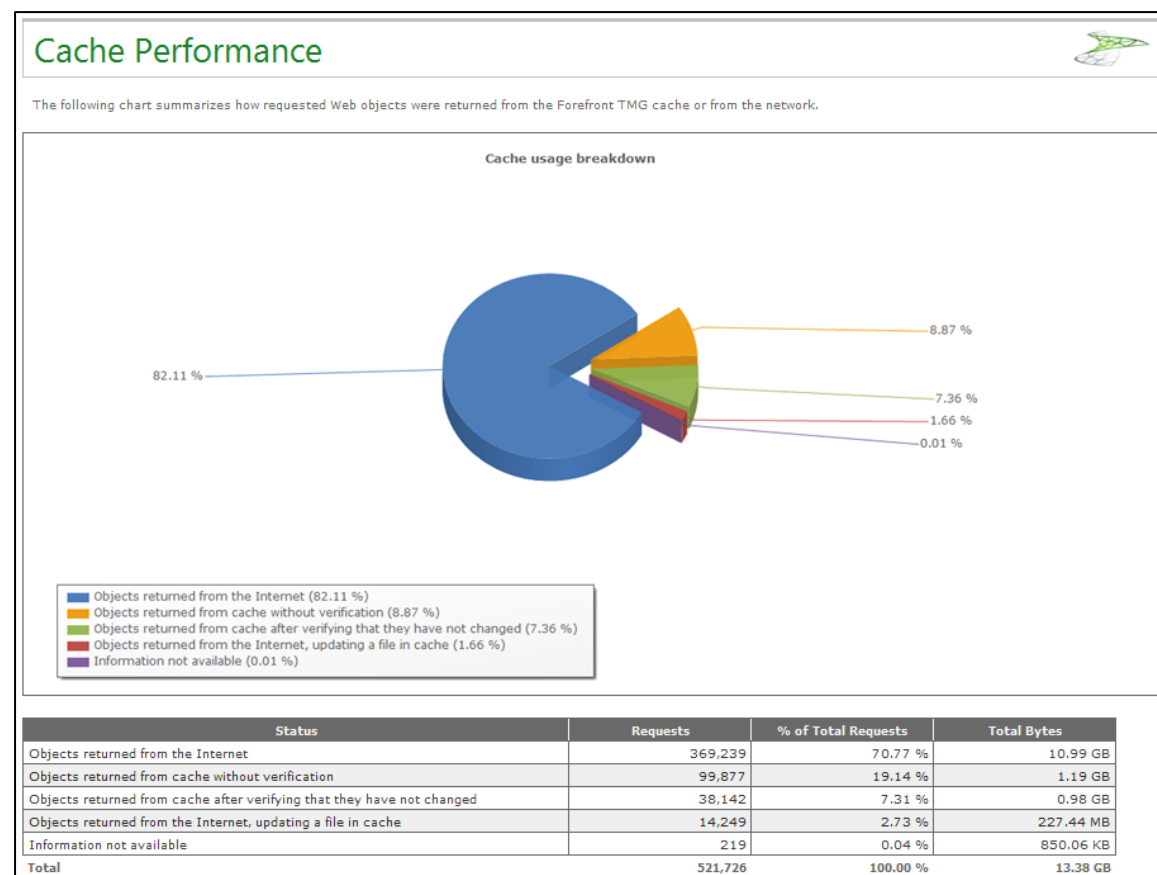
URL Filtering Statistics



The following report shows general statistics summarizing the URL Filtering during the report period.

Total blocked requests	2
Total allowed requests	0
Average number of blocked requests per day	0

12.7 ÁBRA A USER OVERRIDE-DAL KAPCSOLATOS ELŐZŐ TEVÉKENYSÉGEM IS SZÉPEN LÁTSZIK



12.8 ÁBRA JÓ DOLOG A CACHE, AZ TUTI

Ezzel az SP1-es újdonságok felsorolásának vége is szakadt, ahogyan a könyv fejezetei is elfogytak, egy kivételével, ami egy rövid zárszó lesz csak csupán.

13 ZÁRSZÓ

A „Mi maradt ki?” kérdésre tisztán előttem van a válasz. Nem esett szó igazából a terheléelosztásról, viszonylag kevés tartalom kerül bele a migrációs fejezetbe, kimaradt a Sharepoint publikálás, illetve az Enterprise kiadás speciális tudásáról és szépségeiről egyáltalán nem emlékeztem meg. Az elején még egy teljes fejezetet beterveztem a *Forefront Unified Access Gateway 2010* (UAG) szerverről is, legalábbis a különbségekről és a hasonlóságokról az UAG vs. TMG viszonylatban, de ez sem sikerült végül összehozni. Néhány helyen (még) mélyebben is bele lehetett volna menni az anyagba, de hát így is kb. 100 oldallal több lett, mint amire számítottam.

Nos, ez már csak így megy, ráadásul ki tudja mit hoz a jövő (mármint, izé a távoli jövő ☺), de azért beidézném az örökérvényű megállapítást (talán egy Murphy törvény is egyúttal): *„Befejezetlen dokumentum nincs, csak olyan, amelynek meguntuk a módosítását”*. Uff.

Köszönöm a türelmet.

Cegléd, 2010. szeptember

Gál Tamás

v-tagal@microsoft.com

MCP, MCSA, MCSE, MCTS, MCITP SA/EA, MCT, MVP

IT üzemeltetési szakértő

Microsoft Magyarország

<http://www.technetklub.hu>