

Microsoft Network Access Protection

A technológia bemutatása

A Microsoft a hálózat hozzáférés védelmi technológiáját a Windows Server 2008 kiszolgáló oldali operációs rendszerében mutatta be először. Ez a funkció a kor elvárásainak kíván megfelelni, hiszen ma már fontos igény, hogy csak ellenőrzött körülmények között kerülhessenek be számítógépek egy vállalati infrastruktúrába.

A megoldás nem csak az ellenőrzés mechanizmusát tartalmazza, hanem emellett kitér a karantén vezérlés és az automatikus javítás folyamataira is. Azonban ez a platform is hordoz magában néhány korlátot, melyek alapján ez elsősorban a vállalathoz tartozó mobil munkaállomások ellenőrzésére került kifejlesztésre.

Nagyon fontos azonban azt is kiemelni, hogy a Microsoft NAP technológiája az operációs rendszer és a kapcsolódó szerverszerepek alap képességeinek a része, így külön szoftvervásárlásra, ezáltal többletberuházásra nincs szükség!

A technológiával kapcsolatos aktualitások az alábbi weboldalon olvashatóak:

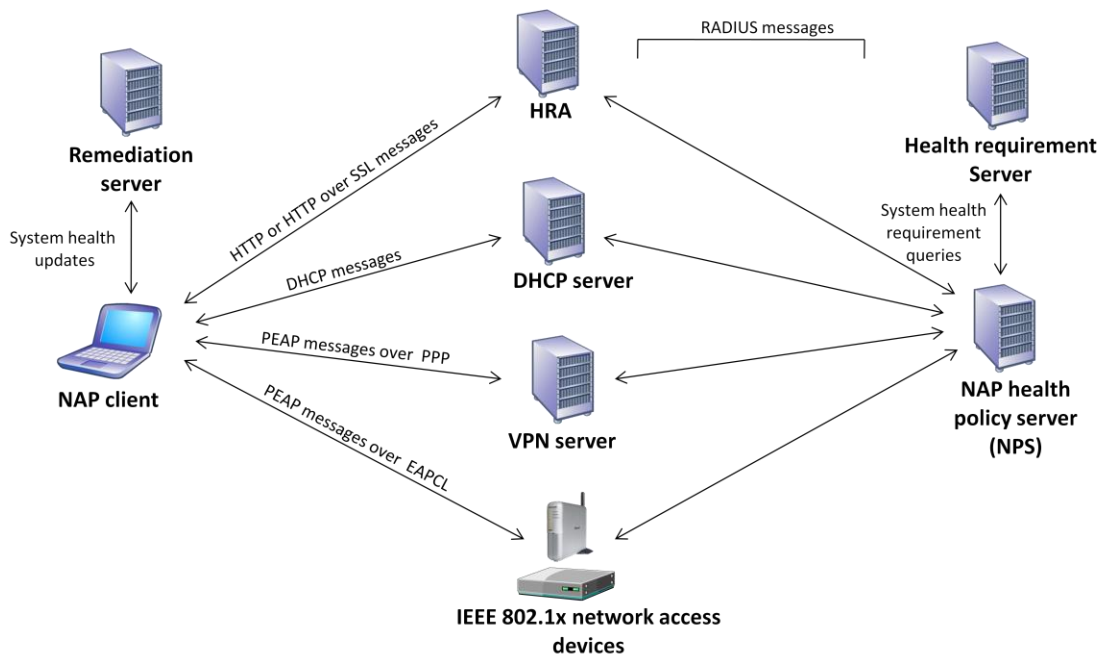
<http://www.microsoft.com/windowsserver2008/en/us/nap-main.aspx>

NAP főbb képességei

Ahhoz, hogy a technológiát megértsük, először sorra kell venni azokat a lehetőségeket, hogy milyen módon lehet egy vállalati infrastruktúrához kapcsolódni. A Microsoft 5 kapcsolódási lehetőséget definiált, ahol a NAP képes vizsgálni a számítógépeket.

Ezek a területek a következők:

1. DHCP kiszolgálótól kért IP cím és további IP opciók
2. IEEE 802.1x → Vezetékes (Wired) és vezeték nélküli (Wireless) kapcsolódások
3. VPN alapú hálózati hozzáférés
4. RDP over HTTPS → Terminal Server Gateway szerepkörrel felépített terminál kapcsolat
5. HRA → IPSec alapú védett hálózati forgalom



NAP egy nagyon fontos rendszereleme az előírt egészségi állapot. Ez egy általunk sablonokból összeállítható szabálycsomag, melyben előírhatjuk például különböző programok jelenlétét a kapcsolódó gépen, programok speciális paramétereit, vagy akár a frissítések naprakészen tartását. A gyártó már a technológia korai stádiumától kezdődően azon dolgozott, hogy minél több hardver és szoftver gyártóval közösen kifejlesszen előre definiált szabály csomagokat (System Health Validators), melyeket az adott gyártó oldaláról letöltve és a rendszerbe importálva könnyedén használatba vehetünk. Jelenleg több, mint 100 gyártó rendelkezik a NAP-hoz szükséges ellenőrző csomaggal (SHV), melyet a legtöbb esetben ingyenesen elérhetővé tettek.



Ahhoz, hogy a kapcsolódó számítógép képes legyen fogadni az előírt egészségi állapot feltételéhez kötődő szabályokat, azokat saját magán le tudja ellenőrizni és az eredményt vissza tudja küldeni, szükséges egy kliens oldali ügynökalkalmazás. Az ügynök komponens a Vista, Windows 7, és a Windows Server 2008 operációs rendszerekben alapértelmezett, az XP kliensben az SP3

telepítésével válik elérhetővé. Korábbi, vagy más operációs rendszerek nem támogatottak, így nem létezik hozzájuk ügynök komponens.

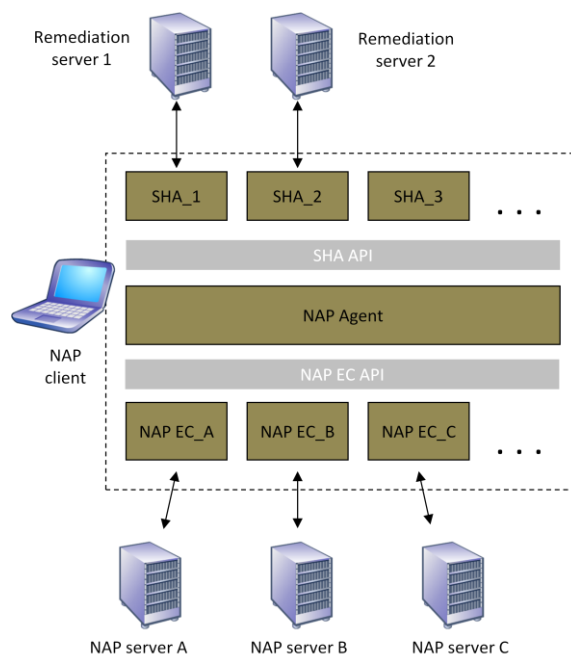
A fent felsorolt 5 kapcsolódási területből négyénél működik a karantén vezérlés (az RDP over HTTPS alapú kapcsolódásánál nincs karantén logika). Bár a karantén a kapcsolódó számítógép számára a belső hálózat védett erőforrásainak elérését nem engedélyezi, de biztosítja a szintre hozatalhoz szükséges szerverszerepek és erőforrások elérését. Korlátozhatjuk, hogy egy gép maximálisan mennyi időt tölthet el a karanténban, így ha záros határidőn belül nem képes magát megjavítani, akkor megszüntethetjük vele a kapcsolatot. Mindez persze akkor igazán érdekes, ha a javítási folyamat automatikusan történik (Auto Remediation).

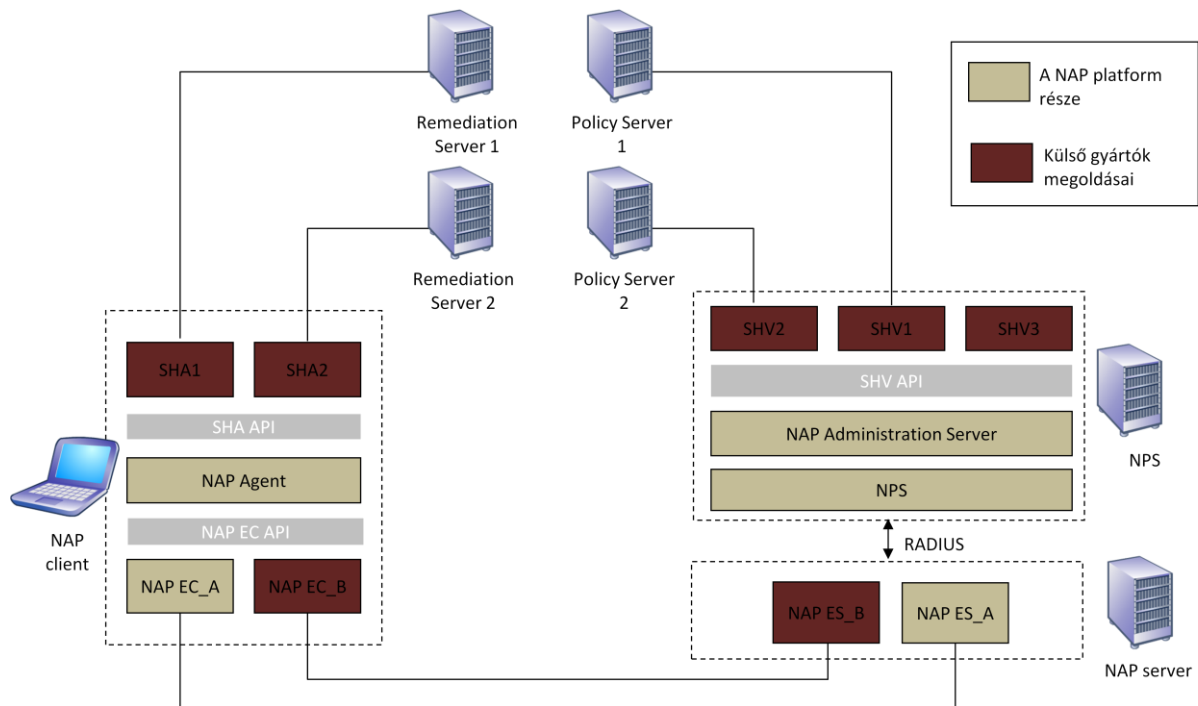
És végül, de nem utolsó sorban, a rendszer képes folyamatosan figyelni a kapcsolódó gép egészségállapot változásait. Ez a gyakorlatban annyit jelent, ha a gép a számára előírt állapottól eltér, akkor automatizált folyamatok szerint azonnal kikerül a karantén hálózatba, ahonnan csak akkor kerülhet vissza a belső hálózatba, ha maximálisan teljesíti az előírt feltételeket.

NAP architektúra felépítése

A rendszer három fő kategóriára osztható:

- Áll egyrészt a kapcsolódó számítógépből, a rajta futó Network Access Protection Agent (napagent) szolgáltatásból, illetve az ehhez tartozó Enforcement Client komponensekből.
- Másrészt a kliensek kapcsolódását fogadó komponensekből (5 különböző kapcsolódási terület).
- Harmadrészt pedig a háttér infrastruktúrából, ahol előírjuk az egészségi állapotot, azt publikáljuk az Active Directory-ba, és szükség esetén megjavíthatjuk a nem megfelelő szinten lévő számítógépet.

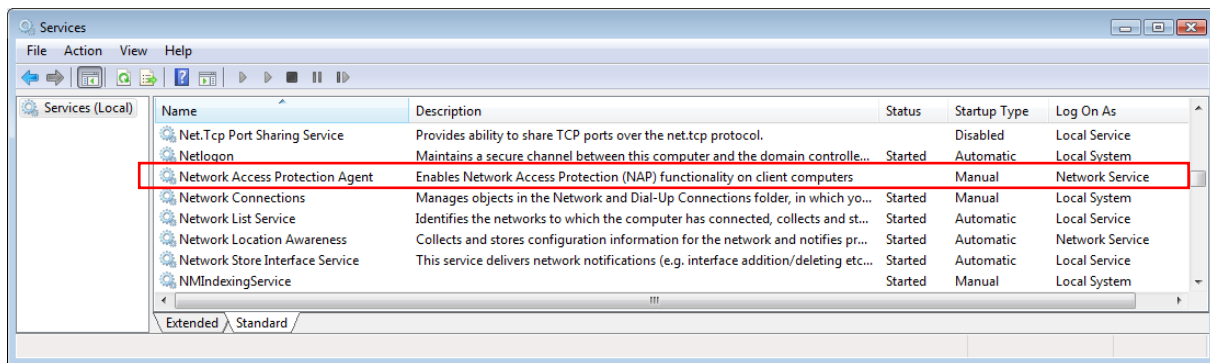




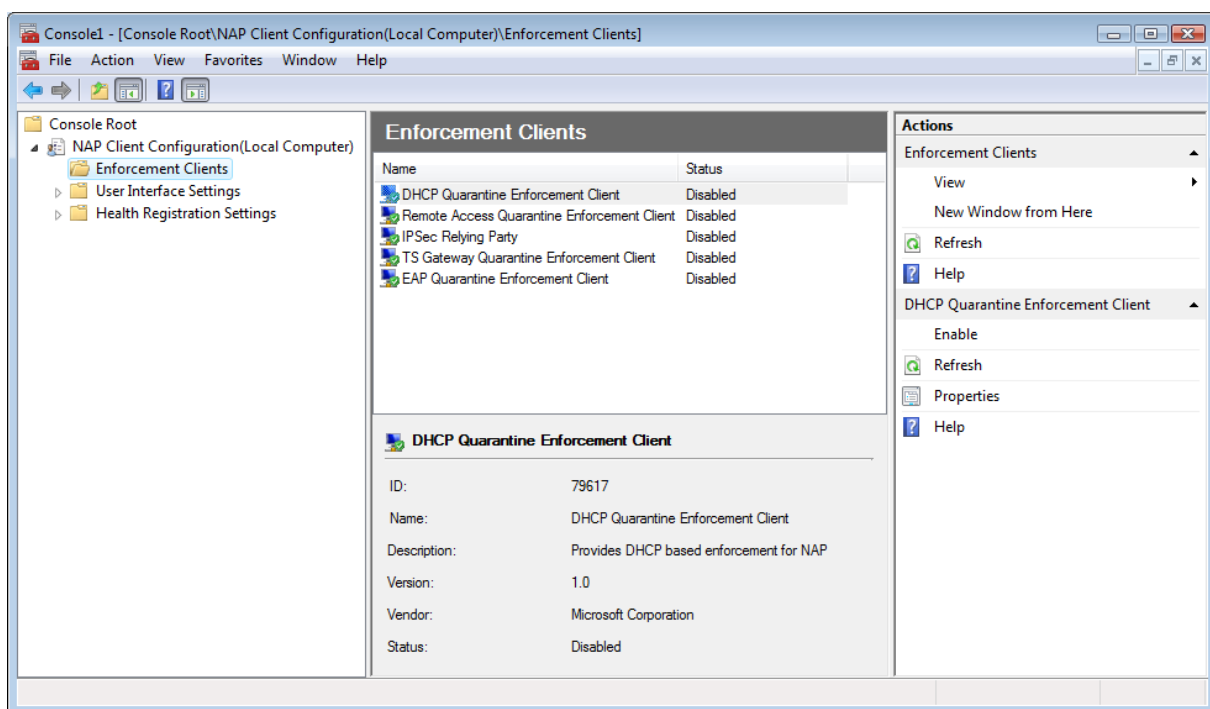
A kapcsolódó géppel szembeni elvárások

Fontos tudnunk, hogy nem minden operációs rendszer verzió támogatott a NAP-ban! Ez a megoldás nem kezeli az a helyzetet, ha egy gépen nincs ügynök, illetve ha az nem került megfelelő bekonfigurálásra. Ez mindenképpen erősen lekorlátozza a lehetőségeinket. Az állítás első részével nem sokat kezdhethünk, meg kell oldanunk, hogy legyen *nagent* a gépen! Ha valaki Vista, vagy Windows 7 kliens operációs rendszerrel dolgozik, akkor nem lesz ezzel külön teendője, XP esetében azonban csak a Service Pack 3 csomag telepítésével kerül be ez a funkció. Szerver oldalon még korlátozottabbak a lehetőségek, mivel csak a Windows Server 2008 része az említett ügynök. A 2003 szerverekhez a Microsoft nem tervezi az ügynök kiadását.

De hiába van fent az ügynök, mivel az alapértelmezett beállítás szerint az nem fut. Ennek viszonylag egyszerű az oka: a „Secure by Default” szemlélet szerint minden felesleges szolgáltatást ki kell kapcsolni. És mivel egyáltalán nem biztos, hogy be akarja mindenki alapértelmezettként vezetni a NAP-ot, ezért inkább kikapcsolták ezt a szolgáltatást. Ha azonban nem fut a szolgáltatás, akkor nem lesz semmilyen egészségállapot vizsgálat, így az ilyen gépek valószínűleg még a karanténba sem fognak bekerülni, a rendszer nem fog velük szóba állni. Bár ez az állítás csak akkor igaz, ha ilyen szabályokat készítünk, de nagy valószínűséggel így fogunk eljárni.

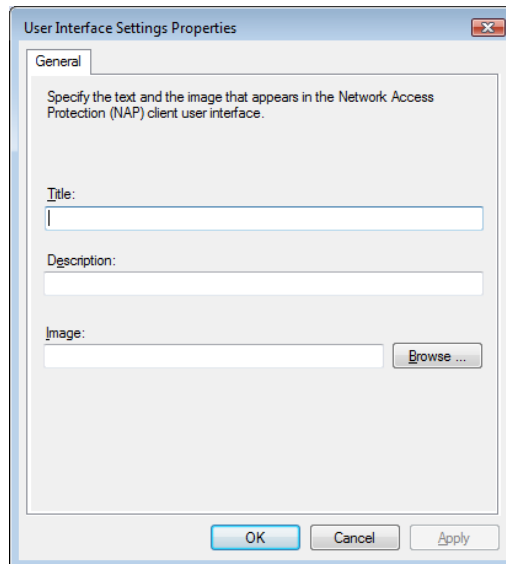


És ha esetleg fut is a szolgáltatás, az sem fog sokat számítani abban az esetben, ha nem konfiguráltuk megfelelően a részterületi ügynököket (Enforcement Client). De mivel alapértelmezettként az előbb említett szolgáltatás sem fut, így az EC-k sincsenek engedélyezve.



Ahhoz, hogy az egészségállapot ellenőrzés folyamata rendkívül gyors legyen, minden ügynök a saját cache-ében tartja a gép aktuális állapotát, amit a kapcsolódáskor azonnal el is tud küldeni az ellenőrzést végző NPS kiszolgáló felé. Minden kapcsolódási területnek megvan a maga részterületi ügynöke, hiszen más-más formátumban kell küldeni az egészségi állapotot, illetve a karantén vezérlés logikája is máshogy működik. Itt csupán annyi a teendőnk, hogy bekapcsoljuk azt az EC komponenst, amelyen keresztül a kliensünk képes lesz kommunikálni az ellenőrzést végző szerverszereppel. Tehát, ha DHCP kiszolgálón keresztül kér a kliens IP címet, akkor a DHCP Quarantine Enforcement Client komponensre lesz szükségünk.

Természetesen Active Directoryval felügyelt rendszer esetében lehetőség van ezen beállítások házirenden keresztüli szabályozására is. Akár testreszabott üzenetek formájában tájékoztathatjuk a felhasználókat arról, hogy mit kell tenniük abban az esetben, ha az ellenőrzés szerint nem megfelelő a számítógépük. Ez főleg akkor igazán hasznos, ha egy külsős felhasználó gépét kellene az előírt egészségi szintre hozni, de itt nem alkalmazható az automatikus javítás folyamata.



Talán a NAP platform legfőbb korlátját éppen az jelenti, hogy a külsők gépére nem fog érvényre jutni az a házirend, ami bekapcsolná az említett komponenseket, és mivel a rendszernek nincs joga az automatikus javításhoz sem, ezért a felhasználó képességein múlik az, hogy megtud-e birkózni a különböző beállításokkal. Az is gondot okoz, ha a külsős felhasználó nem rendelkezik adminisztrációs jogokkal a gépén, mivel ebben az esetben nem állíthat szolgáltatásokat, nem telepíthet programokat. De ha esetleg ezek a jogosultságok adottak is, akkor hamar egy másik problémával találjuk szemben magunkat: előírtuk a Forefront Client Security programot, illetve annak definíciós frissítéseinek naprakészen tartását, de a kapcsolódó gépen nincs telepítve az alkalmazás. Ha ez egy vállalati számítógép, akkor egy központi szoftvertelepítési módszer alkalmazásával (pl.: SCCM) könnyedén orvosolhatjuk ezt a problémát. De mi a helyzet egy külsős gép esetén? Arra nem akarjuk feltelepíteni a vállalati alkalmazásainkat, hiszen ez licenelési problémákhoz vezetne. Így viszont nem tud kapcsolódni az ilyen számítógép a védett rendszerhez.

És ezzel el is érkeztünk a termék legfontosabb bevezetési korlátjához! Mivel ez a technológia nem képes kivételek kezelésére (de ennek nem is lenne túl sok értelme), ezért ha megfogalmazzuk az előírt egészségi állapot feltételrendszerét, illetve megadjuk, hogy mi legyen azokkal a gépekkel, melyek ezt nem teljesítik, akkor az minden a rendszerhez kapcsolódó gépre egységesen vonatkozni fog. A bevezetés előfeltételeként szükséges egy olyan felsővezetői szabályozás, hogy a külsős gépek nem érhetnek el védett, belső erőforrásokat. Tehát ki kell alakítani egy olyan hálózatot, ahol a külsős gépről csak például Internet hozzáférést biztosítunk.

A fogadó komponensek

A kliensek kapcsolódását fogadó komponensek nem közvetlenül döntenek arról, hogy a hozzáférést kérő gép állapota megfelelő-e vagy sem, ezt az információt az NPS kiszolgáló adja meg számukra. A fogadó komponensekkel kapcsolatos általános elvárás az, hogy mielőtt befogadnának egy hozzáférési kérést, továbbítsák a kliens egészségi állapotát az ellenőrzést végző NPS felé, aki azt visszaigazolvva megmondja az adott kiszolgálónak, hogyan járjon el a kapcsolódó géppel szemben.

Az NPS három féle választ adhat:

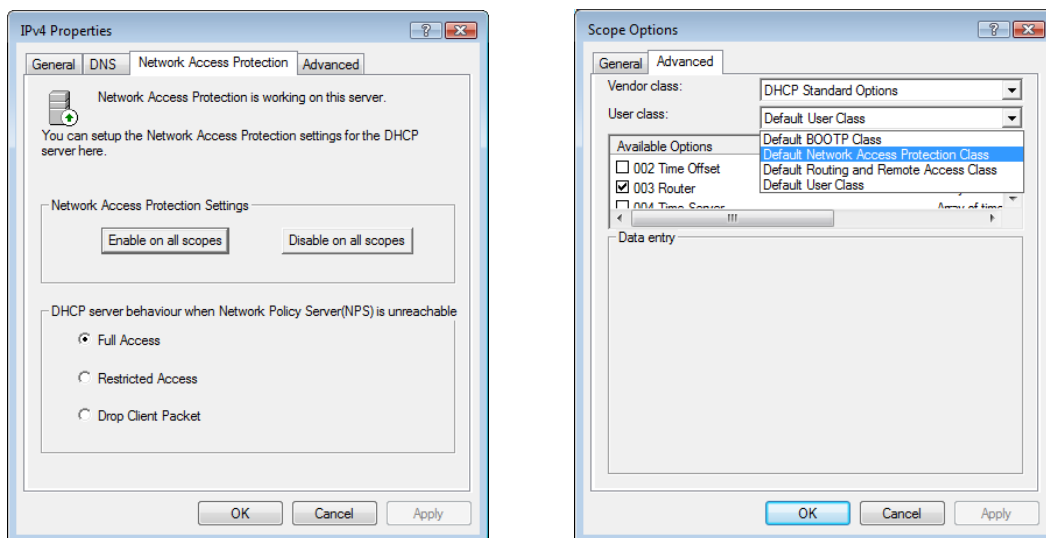
- a kapcsolódó gépet fogadd be, helyezd őt a belső, védett hálózatba,

- a kapcsolódó gép nem teljesítette az előírt egészségi állapotot, ezért helyezd őt a karanténba,
- a kapcsolódó gép nem teljesítette az előírt egészségi állapotot, ezért utasítsd vissza a hozzáférési kérését.

Nézzük ezeket a komponenseket részletesebben:

DHCP szerver

A dhcp alapú kapcsolódáskor a kliens IP címet és további IP opciókat kér a DHCP kiszolgálótól. A Windows Server 2008 (és csak ez a verzió) felkészített a NAP technológia támogatására, így képes eltérő IP opciókat adni a nem megfelelő gépeknek. Ehhez szükség van a standard IP opciók mellé alternatív paramétereket is definiálni Scope, vagy akár szerver szinten.



Természetesen a kliensnek átadott IP cím nem változik a karanténból a belső hálózatba való bekerüléskor, vagy akár fordítva, mivel ez szakadást okozna a folyamatos kommunikációban, viszont a háttérben egy IPconfig /renew parancsnak megfelelő IP opciók megújításával járó folyamat zajlik le. Ennek eredményeképpen a kliens az állapotának megfelelő User Classhoz definiált opciókat fogja megkapni.

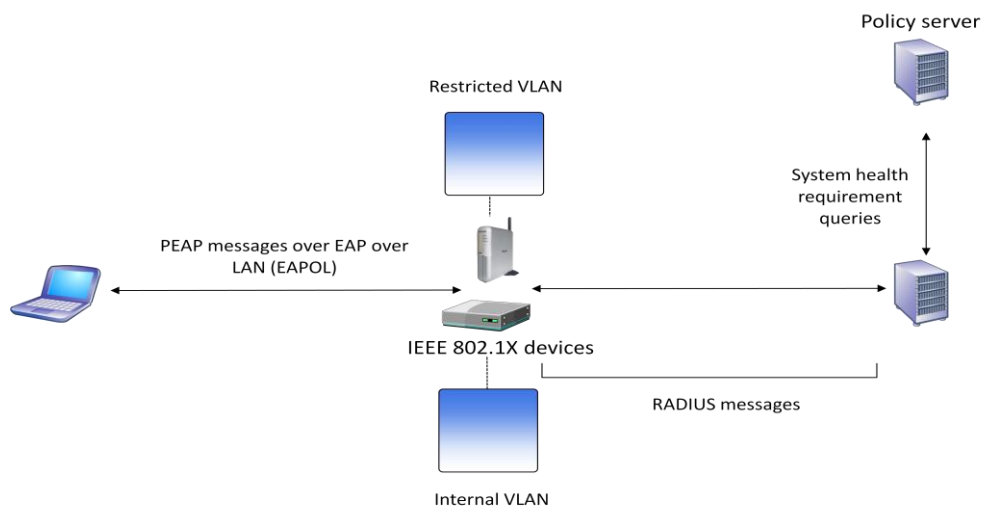
Bár látszólag bármilyen IP opciót definiálhatunk a NAP Classhoz is, de valójában korlátozott, hogy mit fog ténylegesen megkapni a kapcsolódó gép, például átadhatjuk a DNS szerver címét (006-os opció), vagy a DNS tartományi utótagot (015-ös paraméter), de az átjáró címét (003-as opció) nem fogja megkapni, ha nem teljesíti az előírt feltételeket. Tehát itt a karantén vezérlés az alternatív IP opciók kiadásával került megoldásra, ami csak akkor lesz igazán hasznos, ha a kliensek által elérhető hálózatot és a szervert infrastruktúra hálózatát fizikailag is kettéválasztjuk egymástól. Ezzel el tudjuk rejteni a felhasználók elől a belső hálózatban használt névteret, a névfeloldásért felelős kiszolgálókat és egyéb fontosabb információkat.

IEEE 802.1x

Ebben a komponensben található a vezetékes és vezeték nélküli hálózati kapcsolódást fogadó eszközök halmaza. Ezeknek az eszközöknek képesnek kell lenniük a kliensektől érkező egészségi

állapotot befogadni, és azt továbbítani az NPS kiszolgáló felé. Az NPS válaszána k függvényében a kapcsolódó gépet vagy a rendes VLAN hálózatba, vagy egy izolált VLAN-ba kell helyezniük. Ez utóbbi a karantén vezérlés logikája. A kapcsolódó gép és az aktív eszköz között EAP (Extensible Authentication Protocol) vagy PEAP (Protected Extensible Authentication Protocol) alapú kommunikáció zajlik le. Ebből kiderül, hogy az eszközzel szemben is van elvárás: támogatnia kell a NAP technológiát. A Microsoft éppen emiatt kötött egy megállapodást a Ciscoval, hogy legalább egy gyártó legyen, aki az eszközeit felkészíti a NAP-pal való együttműködésre. Persze sok más hardvergyártó is elkészítette az eszközeihez az újabb firmware-t, hogy versenyben maradjanak.

javasolt úgy konfigurálni az eszközt, hogy az izolált VLAN-ban legyen olyan szerverszerep, melyen keresztül a kliens képes magát megjavítani.

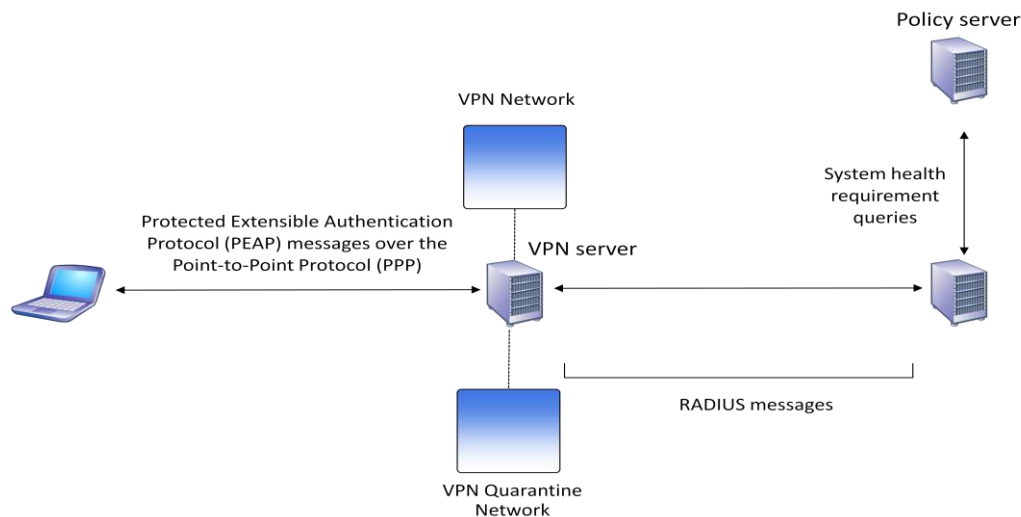


VPN

A VPN karantén vezérlés logikája nem új elem a Microsoft védelmi megoldásaiban, hiszen ennek az első verziója a Windows Server 2003 Routing and Remote Access szerverszerepben megtalálható volt. A működési folyamat gerince nem változott, viszont számos új képességgel bővült a kínálat. Ahhoz, hogy lássuk az új verzió előnyeit, meg kell ismernünk a korábbi megoldás képességeit.

Az előző verzióban nekünk kellett mindenféle ügyes ellenőrző scriptet és exe-t fejleszteni, amiben leírtuk, hogy mit akarunk ellenőrizni. Bár a Microsoft készített ehhez néhány minta scriptet, de a valóságban igen komoly kihívást jelentett ilyen ellenőrző csomagokat készíteni. Az ellenőrzést végző scriptet közvetlenül a VPN kapcsolat felépítése után kellett lefuttatni, és záros határidőn belül (pl.: 1 perc) elküldeni a VPN gatewaynek. Ha ez nem történt meg, akkor a VPN Gateway a megadott idő elteltével bontotta a kapcsolatot a géppel. További probléma volt, ha a gép nem teljesítette az előírt feltételeket, mivel ilyenkor a felhasználónak kellett „megjavítania” a gépét. És végül a gép ellenőrzése csak a kapcsolat felépítésekor történt meg. Miután a gépet beengedtük a VPN hálózatba és a felhasználó úgy döntött, hogy kikapcsolja a gépén lévő tűzfalat, akkor már semmi nem vizsgálta a gépet, hogy még mindig teljesíti-e az előírt állapotot. Sajnos ezzel előállhatott az a helyzet, hogy egyik interfészével védtelenül és közvetlenül kint lógott az Interneten, míg a létrejött PPP adapterével pedig a belső hálózaton figyelt a gép.

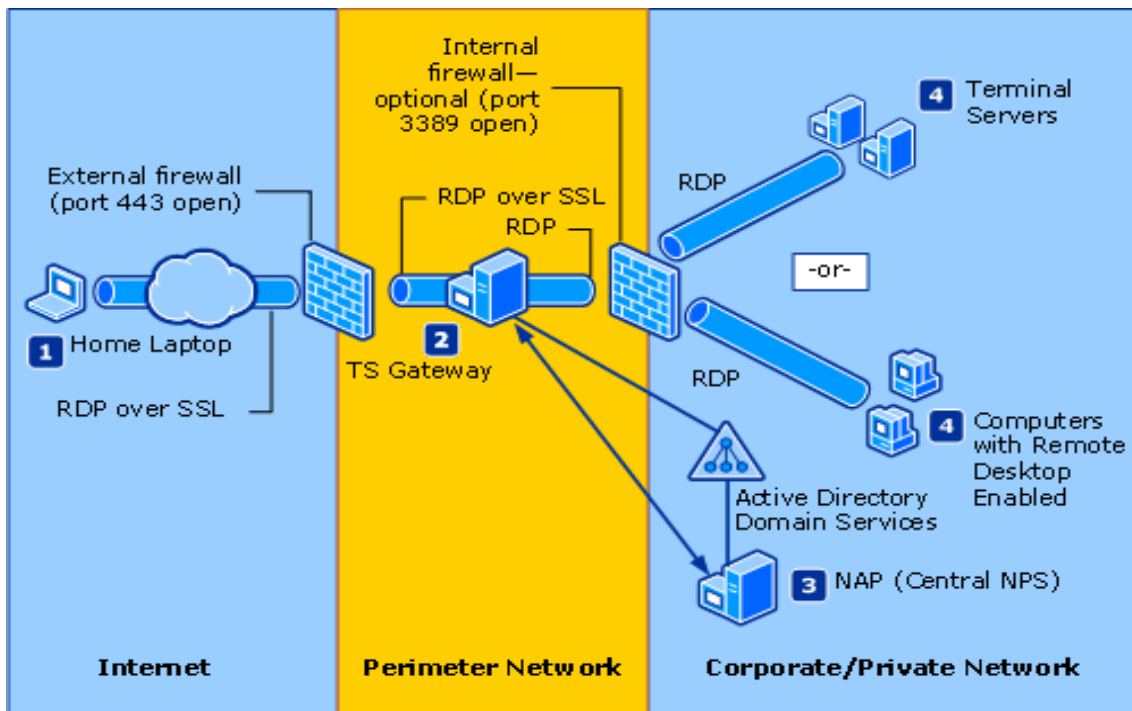
A NAP-ban lévő VPN támogatás a fent leírt összes problémára megoldást ad. Könnyedén előírhatjuk az egészségi állapotot, amit a kapcsolódó kliensen lévő ügynök folyamatosan figyel. Ha tartományi gép kapcsolódik, akkor az automatikus javítás sem lehet probléma, és a kapcsolódás ideje alatt folyamatosan ellenőrzés alatt marad a kliens. A Windows 7-el és a Windows Server 2008 R2-vel megjelenő DirectAccess alapú hálózati elérés esetén is folyamatosan ellenőrzés alatt marad a kapcsolódó munkaállomás.



RDP over HTTPS

A terminál alapú kapcsolódás egy új megoldása a Windows Server 2008-ban megjelenő Terminal Server Gatewayen keresztül folytatott RDP over HTTPS kommunikáció. A megoldás lényege, hogy a felhasználó képes Interneten keresztül HTTPS-be ágyazott RDP protokollon keresztül elérni a vállalati szervereket. Ezzel a megközelítéssel a felhasználó ugyanazon a teljes értékű felületen dolgozhat vállalaton belül, mint bárhol máshol, hiszen a jól megszokott terminál kiszolgáló felületét éri el bárholonnan. A megoldás tovább kombinálható a szintén Windows Server 2008-al megjelenő RemoteApp alapú alkalmazások használatával is. Ilyenkor a felhasználó a terminál kiszolgálóra telepített alkalmazás paraméterezett RDP kapcsolati ikonját kapja meg a saját gépének asztalára, de amikor elindítja az alkalmazást, akkor a rendszer detektálja, hogy a vállalati hálózaton belül vagy kívül tartózkodik a számítógép. Ennek függvényében próbálkozik közvetlenül az RDP vagy a HTTPS-be ágyazott RDP hívással. Ahhoz, hogy ez a technológia használható legyen a kliens oldallal kapcsolatosan is van elvárás, mégpedig az RDP 6.1-es kliens program.

A NAP ebben az egy kapcsolódási területben nem képes karantén vezérlésre. Tehát megvizsgálhatjuk a kapcsolódó gép egészségi állapotát, azonban ha az nem teljesíti az előírt feltételeket, akkor itt nem létesül karantén hálózat, ahonnan képes megjavítani magát a gép. Ez persze érthető, ha megvizsgáljuk a TSGateway architektúráis felépítését.

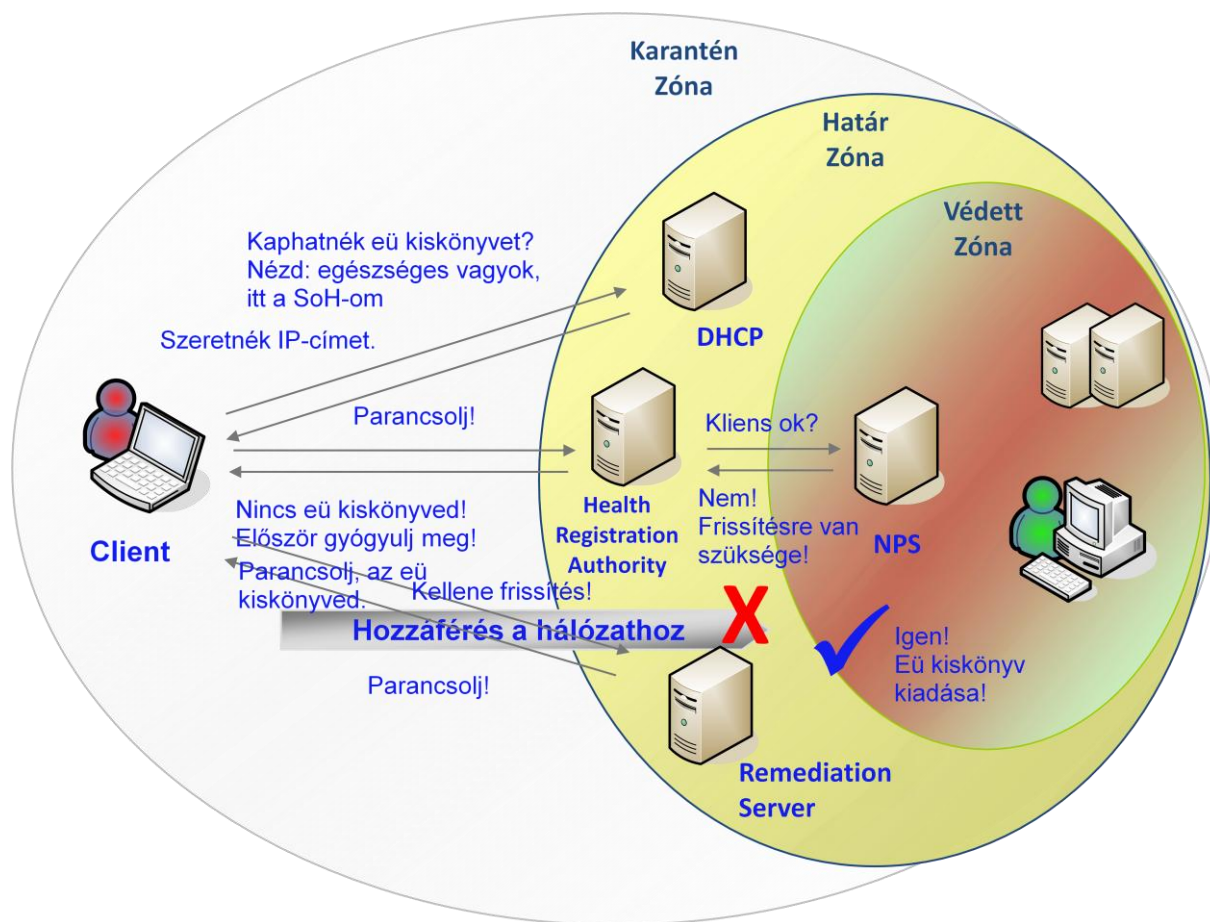


HRA → IPsec védett hálózati kommunikáció

Talán a legbiztosabb védelmet ez a megoldás képes nyújtani a nem megfelelően konfigurált gépekkel szemben. A megfelelő rendszer felépítéséhez alkalmaznunk kell a domain izoláció fogalmát, melynek lényege, hogy a belső hálózatban futó szenzitív információkat tartalmazó kiszolgálókhöz IPsec alapú szabályokat hozunk létre. Az IPsec alkalmazásával nem csupán a hálózati forgalom titkosítását és az adatintegritás védelmet nyerjük, de egyúttal azt is szabályozhatjuk, hogy csak azok a kliensek legyenek képesek kommunikálni a kiszolgálói rendszerrel, akik teljesítik az előírt egészségállapot feltételrendszert.

Az IPsec alapú kommunikációs csatorna kiépítésének első lépése a két fél kölcsönös hitelesítése. A hagyományos IPsec esetében a hitelesítéshez alkalmazható a megosztott titok (preshared key), a Kerberos alapú jegyrendszer és a megbízható, CA által kibocsátott tanúsítvány. A NAP esetében viszont kicsit tekertek a fejlesztők az alap logikán. Itt mindkét félnek egy speciális OID (Object Identifier) mezővel ellátott tanúsítvány sablonból kiállított tanúsítványra van szüksége, amit nem igényelhetnek közvetlenül. Ilyen tanúsítványt a Health Registration Authority (HRA) Windows Server 2008-as szerepkört ellátó kiszolgáló állít ki az előírt egészségi állapotot teljesítő gépek számára.

Ha egy gép nem teljesíti az előírt feltételeket, akkor nem kaphat ilyen tanúsítványt, ha pedig korábban teljesítette azt, de valamilyen oknál fogva menet közben attól elért, akkor a korábban kibocsátott tanúsítványt a kliensen futó nap ügynök eldobja, ezzel megszakad a védett kiszolgálóval felépített IPsec csatorna.



A háttér infrastruktúra komponensek

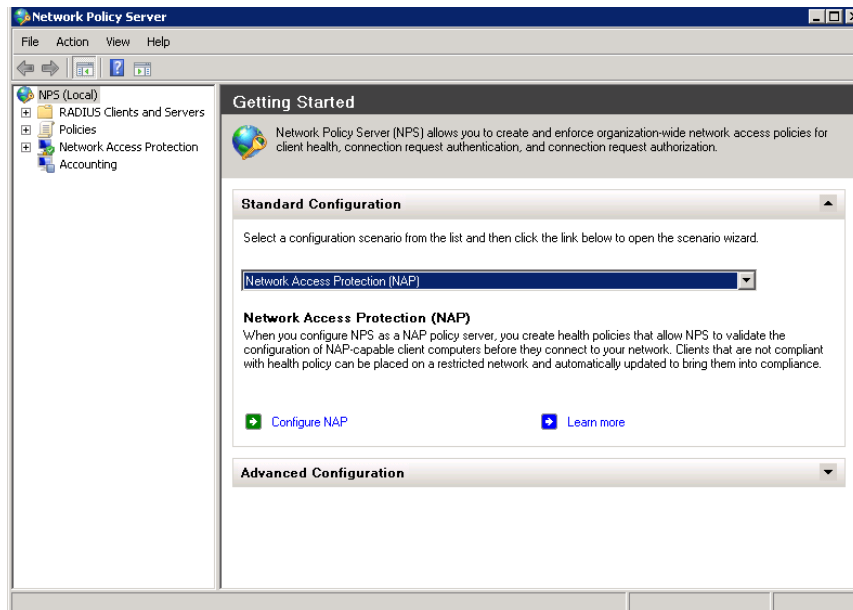
A háttérben lévő szerverszerepek és szolgáltatások működése rendkívül fontos, hiszen ezek nélkül nincs egészségállapot ellenőrzés, sem javítás.

A rendszer lelke, mint sok más alkalmazásnál, itt is az Active Directory. Ide publikálódik az előírt egészségi állapot információ.

Az egészségi állapot előírásokat SHV ellenőrző csomagok formájában telepíthetjük az NPS (Network Policy Server) kiszolgáló alá, ami a Windows Server 2003-ban lévő IAS (Internet Authentication Server) utódja. Az NPS kiszolgáló tartalmaz egy Connection Policy, és egy Network Policy ágat. Ezekben a konténerekben kell szabályokká formálnunk azt, hogy mely gépek kapcsolódhatnak a rendszerünkhöz, és azt milyen feltételek mellett tehetik meg. Rendkívül sok paramétert lehet definiálni kapcsolódási feltételként, beleértve azt is, hogy mit csináljon a rendszer akkor, ha egy egészséges gép érkezik, illetve ha egy nem megfelelő gép küld kapcsolódási kérést.

Ha a cégnek több belépési pontja van (például egy több telephelyes rendszer esetében), vagy ha redundánssá szeretnénk tenni az NPS infrastruktúránkat, akkor érdemes lehet egy központi NPS kiszolgálót üzembe állítani, melyen megfogalmazzuk az említett szabályrendszert. Ezt gyakran Central Policy Storage kiszolgálónak is nevezik. Az NPS kiszolgálók között, illetve a fogadó komponensek és az NPS kiszolgáló között egyaránt RADIUS kommunikáció zajlik. Az architektúrában ki kell neveznünk az

egészségi állapotot küldő kiszolgálót RADIUS kliensnek, míg az NPS szervert (vagy a központi NPS szervert) pedig RADIUS szerverként szükséges konfigurálnunk.



Összefoglalás

Ez is egy olyan újítás a Windows Server 2008-ra épülő infrastruktúrában, ami miatt érdemes lehet átállni a Windows 2003-as rendszerről. A NAP bevezetése előtt mérlegelnünk kell, hogy valóban szükséges-e ez a fajta kontroll a vállalati gépek felett, mivel nincs kivételkezelés. Fontos a management egyértelmű és folyamatos támogatása, mivel ennek hiányában kudarcra van ítélve a projekt.

Tartsuk szem előtt tartani azokat a korlátokat, melyek az operációsrendszerre, a fogadó komponensekre és a vállalaton kívüli gépekre vonatkoznak. Dolgozzunk ki automatizmusokat arra az esetre, ha egy vállalati gép ellenőrzésekor nem megfelelő egészségi állapot eredmény születik. Erre jó megoldás lehet a System Center Configuration Manager szoftvertelepítési és konfiguráció beállítási képessége. Persze ennek előfeltétele, hogy bevezessük az SCCM-et, és a kapcsolódó gépen legyen megfelelően konfigurált SCCM ügynök.

A külső gyártók által elkészített ellenőrző csomagok (SHV-k) sokat segítenek abban, hogy megfelelően testre szabhassuk az egészségi állapot feltételrendszerét.

És végül egy gondolat: használhatjuk akár mind az 5 kapcsolódási terület esetén a NAP platformot, de a felesleges átfedéseket kerüljük, pl.: IEEE 802.1x beállítása a switchen, majd ugyanazon a hálózaton DHCP ellenőrzés együttes használata teljesen felesleges, és ráadásul igen komoly fennforgásokat is okozhat.