2. rész: Hálózati biztonság

Tartalomjegyzék

Bevezetés

A számítógépes hálózatok óriási fejlődésen mentek keresztül az elmúlt években, évtizedekben. Nem csupán a hálózatok fizikai alkotóelemei fejlődtek az egyre modernebb gyártástechnológiának köszönhetően, hanem az eszközök együttműködését lehetővé tevő és szabályozó protokollok is. Ennek eredményeképpen ma már nincs az életnek olyan szegmense, ahol eredményesen, hatékonyan lehetne boldogulni megfelelő hálózati támogatás nélkül. Az egyik vezető hálózati eszközöket gyártó cég vezetője foglalta össze találóan, hogy a hálózat megváltoztatta mindazt, ahogy dolgozunk, élünk, játszunk és tanulunk. A változás különösen szembetűnő a webes felületeken, illetve a közösségi oldalakon, hisz a fiatal generáció tagjai ennek segítségével beszélik meg az iskolai felkészülést, szervezik meg a közös programokat, majd ide töltik fel az ott készült fotókat és videókat. Jelenleg is óriási mennyiségű adat halad az információs szupersztrádán, és ez a mennyiség a videokommunikáció folyamatos előretörésével exponenciálisan emelkedik. 2015-re várhatóan a hálózati forgalom 91%-át videoanyagok továbbítása teszi ki, továbbá kb. 30 millió munkavállaló legalább heti egy napot otthonról fog dolgozni.

A hálózati infrastruktúra általánosságban készen áll a megnövekedett adatforgalom kiszolgálására, de mi a helyzet a hálózat és az azon keresztülhaladó adatok védelmével? Szerencsére egyre nagyobb hangsúlyt kap a megfelelő hálózatbiztonság kialakítása kis- és nagyvállalatoknál egyaránt. Ennek eredményeképpen használunk jogosultságkezelést, tűzfalat, demilitarizált zónát (DMZ), behatolás-érzékelő (IDS) vagy -megelőző (IPS) rendszereket.

A számítógépes bűnözés fejlődésével viszont a hálózat elleni támadások is egyre kifinomultabbá váltak. Már nem feltétlenül igényelnek felhasználói interakciót, inkább a hálózat alsóbb rétegeit célozzák. Az itt működő irányító- és szállítási protokollok felelnek az összes áthaladó adat megfelelő irányba történő, legjobb szándékú továbbításáért. Ha egy támadás sikerrel jár, akkor az összes áthaladó információ eltéríthető.

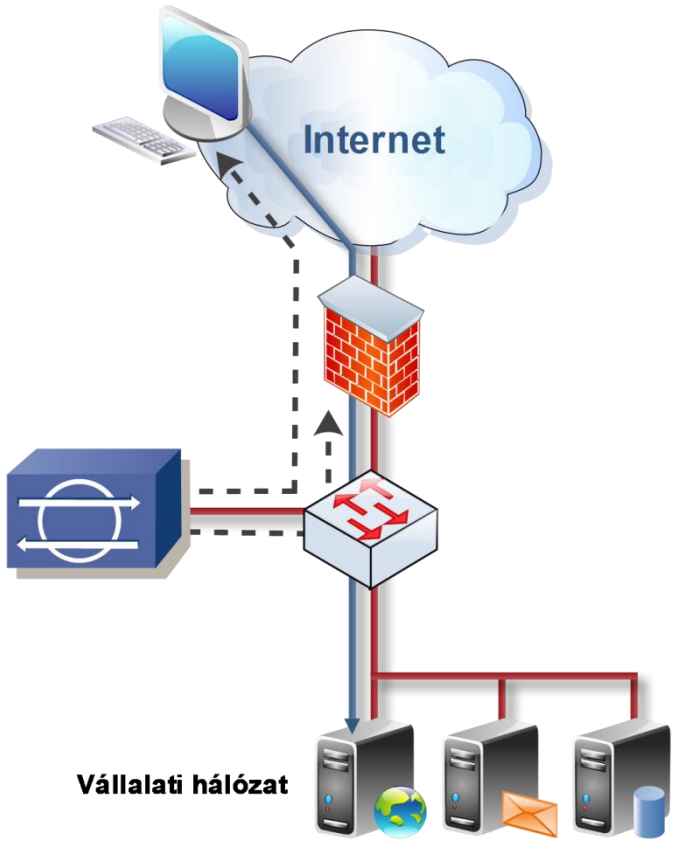
Az alábbi alfejezetek a hálózati biztonság négy kiemelkedő területével foglalkoznak. Az 1. fejezet a behatolás-érzékelő és –megelőző rendszerekkel foglalkozik. A 2. fejezet a VPN technológiákat tekinti át. A 3. fejezet a hálózatbiztonsági architektúrákat veszi számba, különös tekintettel a tűzfal megoldásokra. A 4. fejezetben pedig a napjainkban igencsak népszerű vezeték nélküli hálózatok biztonsági kérdéseit taglalja. A lista természetesen nem teljes körű, de ez terjedelmi korlátok miatt nem is lehetett cél. Az olvasóról feltételezzük, hogy bizonyos szintű informatikai és hálózati ismeretekkel rendelkezik. Az itt esetlegesen nem részletezett hálózati alapfogalmak leírása megtalálható az [1]-ben.

1. Behatolás-érzékelő és -megelőző rendszerek

Mi az a behatolás-érzékelő rendszer?

A behatolás-érzékelő rendszer (IDS, Intrusion Detection System) olyan hardveres, illetve szoftveres megoldás, amely a hálózati forgalomba történő beavatkozás nélkül, válogatás nélkül figyeli az áthaladó csomagokat. A részletes definíció, sok más hasznos információval együtt megtalálható a [2]-ben és a [3]-ban. Passzív működési jellege miatt az IDS csak korlátozott válaszadási képességekkel rendelkezik. Ilyen például, ha rosszindulatú forgalmat érzékel, akkor egy figyelmeztetést küld a hozzá kapcsolódó

felügyeleti állomásnak. Habár adott esetben arra is biztosít lehetőséget, hogy megakadályozza további rosszindulatú forgalom áthaladását a hálózati eszközök (pl.: útválasztók) beállításainak aktív megváltoztatásával, a riasztás kiváltó rosszindulatú forgalom addigra már áthaladt a hálózaton, akár el is érhette tervezett célját. Problémás TCP-kapcsolat esetében az IDS küldhet TCP-reset kérést a végállomásnak, amely ezáltal bontja a TCP-kapcsolatot. A behatolás-érzékelő rendszer általános működése az 1. ábrán látható.

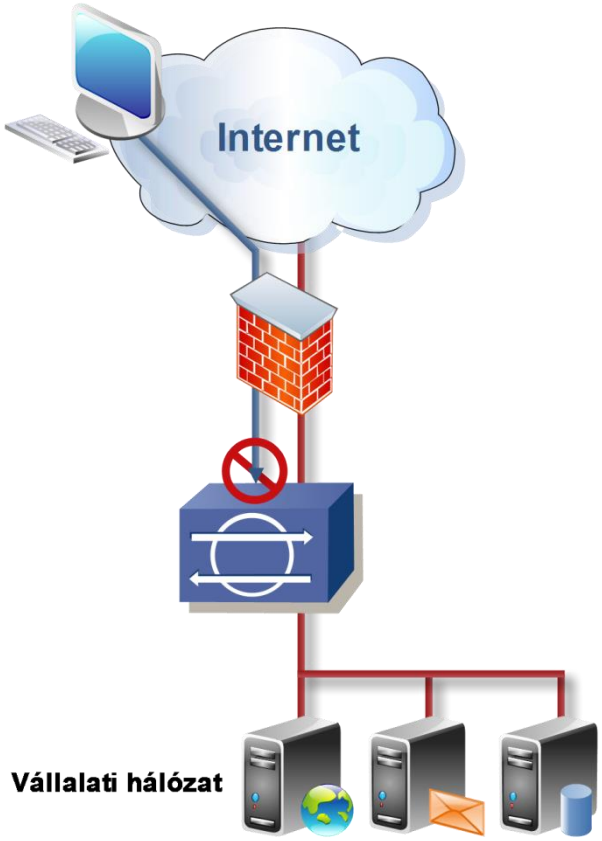


1. ábra: Általános behatolás-érzékelő rendszer

Mi az a behatolás-megelőző rendszer?

A behatolás-megelőző rendszer (IPS, Intrusion Prevention System) olyan aktív, a hálózat forgalmát áteresztő és vizsgáló eszköz, amely a hálózatba érkező csomagokat átengedi vagy eldobja. Elhelyezésénél ügyelni kell arra, hogy lehetőség szerint minden forgalom áthaladjon az IPS-en.

Amennyiben az IPS rosszindulatú forgalmat érzékel, lehetősége van az azonnali beavatkozásra. Riasztást küld a hozzá kapcsolódó felügyeleti állomásnak, majd a beállítások megváltoztatásával azonnal blokkolja a rosszindulatú forgalmat. Működése ezáltal proaktív, mivel a riasztást kiváltó, majd az ezt követő forgalmat egyaránt képes blokkolni. Működése a 2. ábrán látható.



2. ábra: Általános behatolás-megelőző rendszer

Az egyre kifinomultabb támadási módszerek ezt meg is kívánják, a kártékony kódok, illetve a sebezhetőségek elleni harcban.

Az IDS és az IPS kombinált használata

A látszattal ellentétben az IDS és az IPS egymással jól megférő technológiák, ezért nem ritka, hogy vállalati környezetben mindkettőt párhuzamosan alkalmazzák. Az IPS aktív működése révén blokkolja a nemkívánatos forgalmat, ezáltal egyfajta tűzfal-rendszernek is tekinthető. Ezért úgy érdemes beállítani, hogy kizárólag az ismert rosszindulatú forgalmat szűrje ki a kapcsolódási problémák elkerülése érdekében. Az IDS ezáltal ellenőrzi az IPS megfelelő működését, ugyanakkor riasztást küldhet a „szürke zónába" sorolható forgalomról. Ide soroljuk mindazon adatokat, amelyek nem egyértelműen rosszindulatúak, de legitimnek sem tekinthetők. Ha az IPS blokkolja az ilyen típusú forgalmat, fennáll a kockázata, hogy a szabályos forgalmat is megszakítja. Rosszindulatú forgalom esetében viszont az IDS által küldött riasztás értékes információt szolgáltat a lehetséges problémákkal, illetve a támadási módszerrel kapcsolatban.

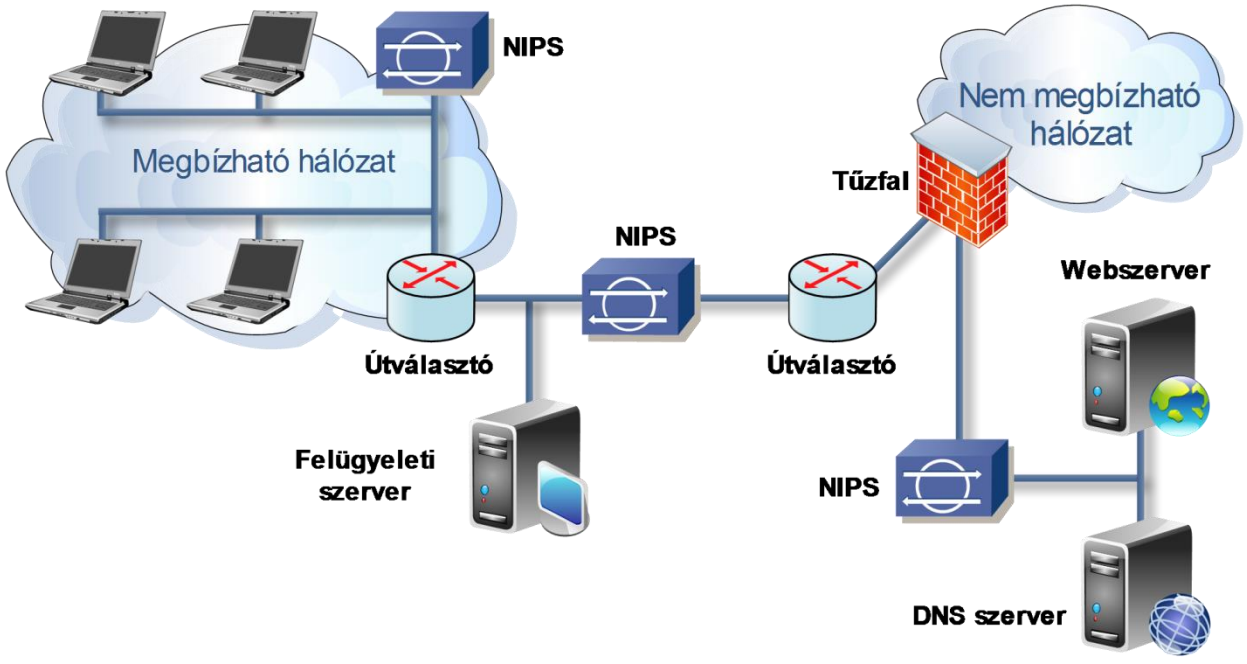
Az IDS és IPS rendszerek típusai

Az IDS és IPS megoldások típusainak csoportosítása a hálózatban elfoglalt helyük, valamint a rosszindulatú forgalom azonosítására használt módszerük alapján lehetséges. Az előbbi alapján beszélhetünk hálózat alapú, illetve állomás alapú rendszerekről, az utóbbi alapján pedig négy technikát különböztetünk meg:

- szignatúra alapú
- házirend (policy) alapú
- anomália alapú
- „mézescsupor” alapú

Az állomás alapú IPS (HIPS) minden egyes számítógép és állomás tevékenységét külön vizsgálja. Teljes hozzáféréssel rendelkezik a végberendezés belső adataihoz, ezáltal a bejövő forgalmat az állomás tevékenységeinek viszonylatában vizsgálja. VPN környezetben, ahol az adat titkosítva halad át a hálózaton, a HIPS az egyetlen módja, hogy a célállomáson a valódi forgalmat megvizsgáljuk. Hátránya, hogy jellemzően egy adott operációs rendszert támogat, és nem véd az alacsonyabb szintű – az OSI rétegmodell első és harmadik rétegét érintő – támadások ellen. További hátránya, hogy kellő felderítés után a támadó tudni fog az állomás létezéséről, sőt arra is rájöhet, hogy az állomást HIPS védi.

A hálózat alapú IPS (NIPS) a hálózaton áthaladó minden egyes csomagot analizál, ezáltal olyan rosszindulatú csomagok felismerésére is alkalmas, amelyek egy tűzfal egyszerű szűrési szabályain átjutnak. A NIPS hálózatban történő elhelyezésénél ügyelni kell arra, hogy lehetőség szerint a teljes, de legalább a kritikus forgalom vizsgálható legyen. A NIPS képes kiszűrni az alacsonyabb szintű támadásokat, de a szenzoron áthaladó titkosított forgalmat nem tudja vizsgálni. A NIPS a támadásokat kizárólag a hálózat szemszögéből, kontextus nélkül analizálja, ezért előfordulhat, hogy az amúgy ártalmatlan forgalmat is támadásnak véli. Ebbéli hiányosságai miatt mindig fenntartásokkal kell a NIPS következtetéseit kezelni. A NIPS működési elve a 3. ábrán látható.



3. ábra: A NIPS működési elve

A fenti csoportosítás analóg módon az IDS rendszerekre is alkalmazható.

A HIPS és a NIPS összehasonlítása

Mivel a NIPS nem az állomások szintjén vizsgálja az áthaladó forgalmat rosszindulatú tevékenység után kutatva, kizárólag a jellemzők (szignatúrák) alapján dönti el, hogy a csomagokat továbbengedi vagy blokkolja. Rendkívül nehéz, de még inkább lehetetlen, hogy a hálózat alapú IPS felmérje, hogy egy adott támadás sikerrel járt-e. Az ilyen rendszerek kizárólag a rosszindulatú tevékenység jelenlétét érzékelik.

A HIPS ellenben a helyi állomást, illetve operációs rendszert vizsgálja. Lehet összetett, amely tényleges rendszerhívásokat vizsgál, vagy egyszerű, amely mindössze a rendszernaplózást és a naplóállományok elemzését teszi lehetővé az állomásokon. Van olyan HIPS, amelyik a támadást még azelőtt elhárítja, hogy az végbement volna, más rendszerek viszont csak jelentik, ha valami már megtörtént.

Általánosságban elmondható, hogy a HIPS a puffer-túlcsordulások, webkiszolgálók elleni támadások, hálózati felderítések, valamint elárasztásos, más néven szolgáltatás-megtagadásos (DoS) támadások detektálására alkalmas, míg a HIPS az alkalmazások és állomások által használt erőforrásokat óvja.

Komoly előny a HIPS javára, hogy tudja monitorozni az operációs rendszer folyamatait és védeni a kritikus rendszererőforrásokat. A HIPS a viselkedés alapú elemzést a szignatúra alapú szűrésekkel kombinálja, ezáltal a vírusirtók, valamint a hálózati és alkalmazás rétegbeli tűzfalak legjobb tulajdonságait ötvözi egy csomagban.

NIPS tulajdonságok

A NIPS a hálózat különböző pontjain található eszközök és szenzorok monitorozásával képes a forgalom elfogására és elemzésére. A szenzorok valós időben detektálják a rosszindulatú vagy jogosulatlan tevékenységeket, és szükség esetén beavatkozhatnak. Mivel a szenzorok a hálózat meghatározott pontjain helyezkednek el, bármilyen esemény kapcsán a támadás céljától függetlenül figyelemmel kísérhető a hálózati forgalom alakulása.

Mivel a NIPS szenzor feladata a behatolások elemzése, az alatta futó operációs rendszerről el kell távolítani az összes szükségtelen szolgáltatást, a működéshez nélkülözhetetlen szolgáltatásokat viszont be kell biztosítani. A NIPS szenzor hardvere az alábbiakból áll:

- hálózati adapter, amellyel a NIPS csatlakoztatható bármilyen (leggyakrabban Ethernet jellegű) hálózatra
- processzor, amely elegendő számítási teljesítményt nyújt a behatolás-érzékeléshez szükséges protokollok, illetve mintaegyezések vizsgálatához.
- memória, melynek elegendő mennyisége teszi lehetővé a támadások hatékony és pontos detektálását

A NIPS kiváló skálázhatóságot biztosít egy védett hálózat számára, hisz új állomások hozzáadásával nem szükséges további szenzorok kihelyezése. Új alhálózatok esetében is csak akkor szükséges további szenzorok kihelyezése, ha a meglévő szenzor(ok) vizsgálati kapacitását meghaladja a megnövekedett forgalom, teljesítménye nem éri el a kívánt szintet vagy a biztonsági házirend felülvizsgálata indokolja azt.

Az NIDS és az NIPS esetében a szenzorok helye a hálózatban kulcsfontosságú, általában a hálózat – kritikus szegmenseit védő – belépési pontjainál kell elhelyezni azokat.

A hálózat alapú IPS és IDS előnyei közé sorolható, hogy könnyedén érzékeli a teljes hálózat ellen irányuló támadásokat, segítségével világosan látszik, hogy milyen mértékű a hálózatot ért támadás. További előnye, hogy mivel kizárólag a hálózati forgalmat vizsgálja, nem szükséges a hálózati állomásokon használt különböző típusú operációs rendszereket támogatnia.

Hátrányai közé sorolható, hogy a titkosított adatfolyammal nem tud mit kezdeni a szenzor, de rendkívül nehéz problémát okoz számára a töredezett forgalom helyreállítása is. A legnagyobb hátrány azonban az egyre nagyobb méretű hálózatokból adódik; egyre nehezebb úgy elhelyezni egy szenzort, hogy az lehetőleg az összes csomag elfogását lehetővé tegye. A problémát ugyan megoldja további szenzorok kihelyezése, de ez jelentősen megnövelheti a költségeket.

Szignatúra alapú IDS és IPS

A szignatúra alapú megközelítésmód viszonylag merev, ellenben egyszerűen alkalmazható. A mintaegyezéshez előre meghatározott, fix bájtszekvenciákat keres a csomagok fejlécében és adattartalmában. A legtöbb esetben csak akkor beszélhetünk mintaegyezésről, ha a gyanús csomag bizonyos szolgáltatásokhoz (még inkább konkrét portokhoz) van társítva. Ezzel a módszerrel csökkenthető a vizsgálatból adódó hálózati terhelés, ugyanakkor lényegesen nehezebbé válik az alkalmazása olyan rendszerekben, amelyek nem a jól ismert portokhoz társított protokollokat használnak.

Eleinte viszonylag nagy számban előfordulhatnak hamis riasztások, de a rendszer behangolását követően ez a szám kevesebb lesz, mint a házirend alapú megközelítésmód esetében.

A szignatúra bizonyos környezetben (kontextusban) előforduló bájtsorozat. Ilyen környezet lehet a szekvencia adatfolyamban elfoglalt pozíciója vagy egy alkalmazásrétegbeli protokoll érvényes parancsának részlete.

Íme néhány példa:

- A webkiszolgálók ellen irányuló támadások jellemzően speciálisan összeállított URL-eket használnak, így az IDS és az IPS olyan szignatúrákat keres az adatfolyam elején, amelyek kliens-oldali HTTP kéréssel kezdődnek.
- Az SMTP kiszolgálók ellen irányuló támadások jellemzően puffer-túlcsordulást próbálnak előidézni az SMTP menet MAIL FROM parancsának segítségével, ezért az IDS és az IPS az SMTP menetek MAIL FROM paranccsal kezdődő sorában keres egy bizonyos támadási mintát.
- A levelezőkliensek ellen irányuló támadások jellemzően a tényleges üzenet MIME fejlécébe rejtett puffer-túlcsordulásra építenek, ezért az IDS és az IPS olyan bájtszekvenciákat keres, amelyek azonosítják az üzenetbe rejtett új MIME részeket, és puffer-túlcsordulást idéznek elő az üzenet olvasását követően.

A fenti példák is jól illusztrálják, hogy a szignatúra alapú IDS és IPS kizárólag olyan támadások detektálására képes, amelyek már előzőleg rendelkezésre állnak egy – a gyártó által biztosított vagy a rendszergazda által karbantartott – mintaadatbázisban. A szignatúra alapú IDS és IPS nem képes a még nem ismert és nem jelentett, ún. nulladik napi támadások detektálására, ezáltal nagyobb terhet ró a rendszergazdára, akinek folyamatosan ügyelnie kell a mintaadatbázis naprakészen tartására, amennyiben a gyártó ezt nem teszi meg. További információ a szignatúra alapú rendszerekről a [4]-ben található.

Házirend alapú IDS és IPS

A házirend alapú megközelítésmód roppant egyszerűen működik; a házirend megsértése esetén az IDS és az IPS blokkolhatja a forgalmat vagy riasztást küldhet az eseményről. A riasztás szükségességéről egy algoritmus alapján dönt. A módszer azért is rendkívül népszerű, mert képes a még nem ismert támadásokat is detektálni.

A házirend alapú IDS és IPS esetében mindig pontosan tisztázni kell, hogy a házirend milyen célt szolgál, és pontosan mit takar. Amennyiben a hálózati hozzáférést akarjuk házirend segítségével szabályozni, pontosan meg kell adni az engedélyeket, mely hálózatok érhetik el egymást, és milyen protokollok használatával.

Példaként vegyük azt az esetet, amikor portpásztázás (port sweep) jellegű tevékenységet akarunk detektálni. Ekkor a házirendben meg kell határozni egy küszöbértéket, hogy egy bizonyos számítógép vagy eszköz esetében hány egyedi port szkennelése lehetséges. A házirend további korlátozásokat is tartalmazhat, így meghatározhatja a házirend szempontjából „érdekes” (pl.: SYN) csomagokat, de azt is rögzítheti, hogy minden kérésnek azonos forrásból kell származnia. A megfelelő küszöbértékek meghatározása sokszor nem egyszerű feladat, mindig figyelembe kell venni a vizsgált hálózat forgalmi sajátosságait.

Léteznek olyan biztonsági házirendek, amelyek nagyon nehezen építhetők be az IDS és az IPS rendszerekbe. Ha például nem engedélyezett a „felnőtt” vagy warez tartalmak böngészése, kapcsolatot kell biztosítani egy ún. feketelistát működtető adatbázishoz, amely alapján eldönthető, hogy megsértették-e a házirendet.

Anomália alapú IDS és IPS

Az anomália alapú rendszerek általában a „normáltól” eltérő hálózati forgalmat keresik. Ebből adódik a fő problémájuk is: mit tekintünk „normálnak”? Anomáliának tekintjük például bizonyos típusú forgalom szokatlan mértékű növekedését, a vizsgált hálózaton jellemzően nem előforduló típusú forgalom megjelenését, de akár egy ismert protokoll deformált üzenetét. Léteznek olyan rendszerek, amelyekbe bele van kódolva a normál forgalom mintája, míg más rendszerek megtanulják, hogy mi számít normál forgalomnak. Ez utóbbinál felmerül annak a lehetősége, hogy nem megfelelő csoportosítással a normáltól eltérő forgalmat is normálnak tekinti. Ennek eredményeképp kisebb méretű környezetben relatíve jól használható, de nagyobb – főleg vállalati – hálózatok esetében alkalmazása nehézkes, nem váltja be a hozzá fűzött reményeket.

Az anomália alapú IDS és IPS két típusát különböztetjük meg:

Statisztikai alapú anomáliadetektálásról akkor beszélünk, ha a rendszer bizonyos idő alatt megtanulja a vizsgált hálózat „profilját”, vagyis az azon áthaladó forgalom mintáját. Ezt követően a vizsgált forgalom statisztikai vizsgálatával dönti el, hogy az kellően eltér-e a szokásostól. Amennyiben igen, riasztást küld.

Nem statisztikai alapú anomáliadetektálás esetében az ismert, normál viselkedés jellemzői előre rögzítve vannak, bármilyen ettől eltérő forgalmi minta riasztást vált ki.

Az alábbiakban található néhány példa a rosszindulatú, nem statisztikai alapon detektálható anomáliákra:

- IPX kommunikáció előfordulása két olyan eszköz között, amelyek kizárólag TCP/IP protokollt használó hálózatban működnek
- Felhasználói eszközről származó útvonalfrissítés előfordulása
- Szórási vihar (broadcast storm), illetve a hálózat végigpásztázása
- Olyan ellentmondásos csomag, amelyben az összes TCP jelölő bit be van állítva, esetleg megegyezik a TCP szegmens forrás és cél IP-címe vagy a TCP forrás- és célportja

Mézescsupor alapú rendszerek

A mézescsupor alapú megközelítésmód azon az ötleten alapul, hogy a támadást minél messzebbre kell terelni a valódi hálózati eszközöktől. A mézescsupor tulajdonképpen nem más, mint egy speciálisan erre a célra kialakított – az éles hálózat többi eszközétől teljesen elszigetelt – eszköz, amely irányított körülmények között lehetővé teszi a bejövő támadások és rosszindulatú forgalmi minták elemzését, és elegendő időt biztosít a felkészülésre, mielőtt a forgalom elérné a valódi eszközöket. Fontos, hogy soha ne bízzunk meg a mézescsuporként funkcionáló eszközökben, hisz előfordulhat, hogy a tudomásunk nélkül már feltörték azt, és ugródeszkaként használják az éles hálózat ellen indított támadásokhoz!

Kétféle módon foghatunk mézescsupor építéséhez:

Készíthetünk olyan mézescsuprot, amely bizonyos fokig valóban sebezhető a támadásokkal szemben. Így a mézescsupor ellen indított támadások általában sikerrel járnak, de a rendszergazdának időt és lehetőséget ad, hogy naplózza és nyomon kövesse a támadó minden lépését, anélkül hogy az éles rendszerek veszélybe kerülnének.

Ugyanakkor a mézescsupor lehet olyan érdekesnek tűnő célpont, amely megfelelően fel van vértezve a támadásokkal szemben, ugyanakkor sokkal sebezhetőbbnek és áthatolhatóbbnak tűnik a támadó számára. Íme két trükk, amellyel elérhetjük, hogy rendszereink sebezhetőbbnek tűnjenek:

- Több kapcsolódási lehetőség (vagy kevésbé védett hozzáférés) biztosítása a mézescsuporhoz
- A ténylegesen használt alkalmazások verziószámának megváltoztatása, ezáltal a támadó egy korábbi sérülékenység kihasználásával próbálkozhat

Néhány példa:

- A klasszikus mézescsupor egy olyan UNIX rendszer, amely például gyenge jelszavak használatával engedi, hogy a támadó bejelentkezzen valamiféle hamis környezetbe, ahol a rendszergazda nyomon követheti minden lépését.
- A levélszemét elleni harcban sem ismeretlen a mézescsupor fogalma. Itt jelenthet olyan levelező-kiszolgálót, amely nyílt relének tűnik, de valójában odavonzza és összegyűjti a levélszemetet küldő címeket, majd eldobja ezeket a leveleket. Az összegyűjtött címek vagy a küldő IP-címe ezután felkerül egy ún. szürke- vagy feketelistára, amelyek használatával a levelező-kiszolgálók tovább szűkíthetik a levélszemét mozgásterét.

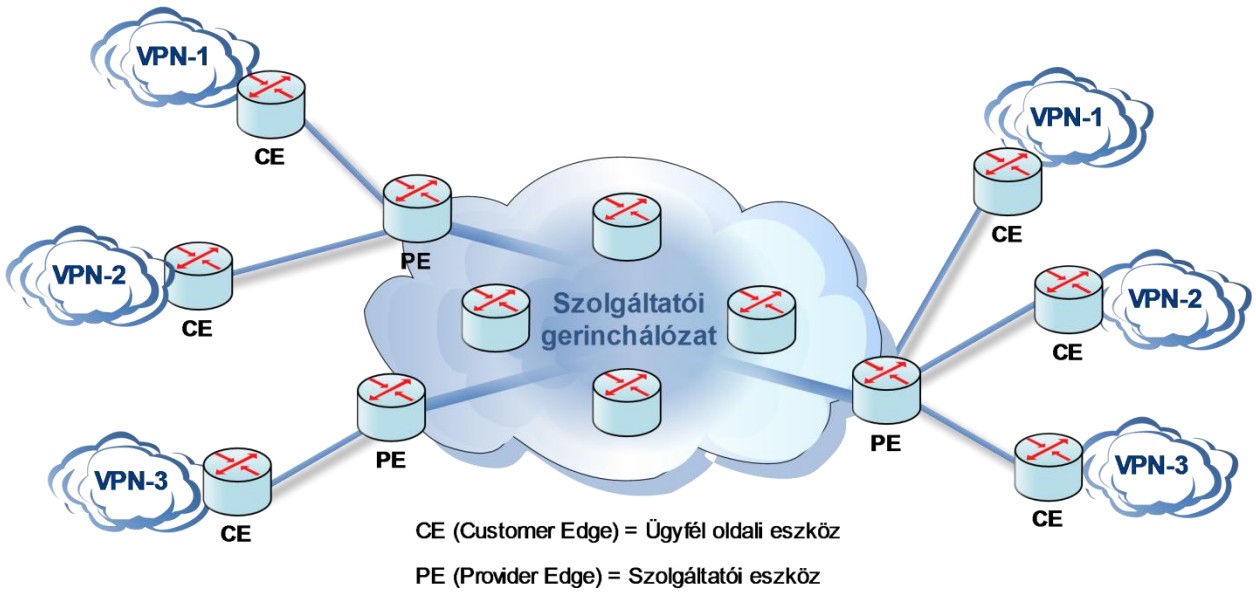
További információ a mézescsupor alapú rendszerekről az [5]-ben található.

2. Virtuális magánhálózatok biztonsága

Mi az a virtuális magánhálózat?

A virtuális magánhálózat (VPN, Virtual Private Network) fejlett titkosítási és alagúttechnikák segítségével lehetővé teszi, hogy biztonságos, végponttól végpontig terjedő hálózati kapcsolatot hozzunk létre harmadik fél által üzemeltetett – alapvetően nem megbízható – hálózatokon (pl.: az interneten) keresztül. Jelen fejezet főként a VPN elméleti hátterét tárgyalja, a VPN megoldások gyakorlati oldalát a [6] mutatja be részletesen. A biztonságos kapcsolat azt jelenti, hogy a küldő hiteles azonosítása mellett, az üzenet sértetlensége (integritása) és bizalmas kezelése is ellenőrizhető. A VPN beágyazással, titkosítással vagy a kettővel együtt gondoskodik az adatok védelméről. Azt sem árt leszögezni, hogy beágyazás (más néven alagutazás) alatt az adatok transzparens módon történő átvitelét értjük megosztott hálózatok fölött. A VPN megoldások az OSI rétegmodell második (L2), harmadik (L3), illetve negyedik (L4) rétegében implementálhatók.

Alapvetően kétféle VPN modell létezik: átlapolódó (overlay) és egyenrangú (peer-to-peer) rendszerekről beszélhetünk. Az átlapolódó VPN a 4. ábrán látható.



4. ábra: Az átlapolódó VPN struktúrája

A szolgáltatók a legtöbb esetben átlapolódó VPN modellt használnak, ahol még a tényleges forgalom megkezdése előtt megtörténik a virtuális áramkörök (VC) megtervezése és kiosztása a gerinchálózaton keresztül. Ez IP-hálózat esetében azt jelenti, hogy bár az alapvető technológia kapcsolat nélküli, a szolgáltatás nyújtásához kapcsolatorientált megközelítésmód szükséges. A módszer nem túl skálázható, mivel jelentős mennyiségű áramkört és alagutat kell felügyelni és kiosztani a felhasználói berendezések között. Az átlapolódó modell L2 és L3 rétegbeli VPN-eket is tartalmaz:

Az L2 rétegbeli átlapolódó VPN független az ügyfél által használt hálózati protokolltól, így a VPN nincs kizárólag IP-forgalom továbbítására korlátozva.

Az L3 rétegbeli átlapolódó VPN leggyakrabban az „IP az IP-ben” alagútsémát használja PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), illetve. IPsec technológiák alkalmazásával.

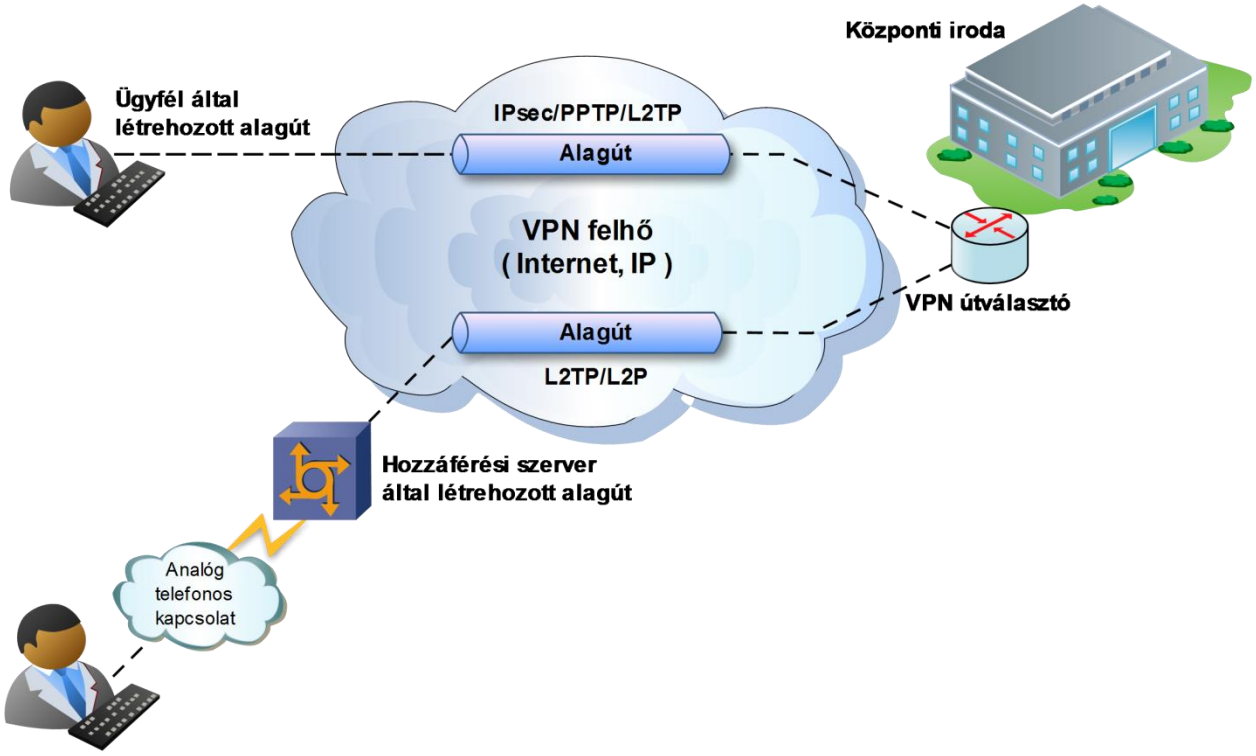
VPN topológiák

A VPN megoldások topológia szerint három csoportba sorolhatók:

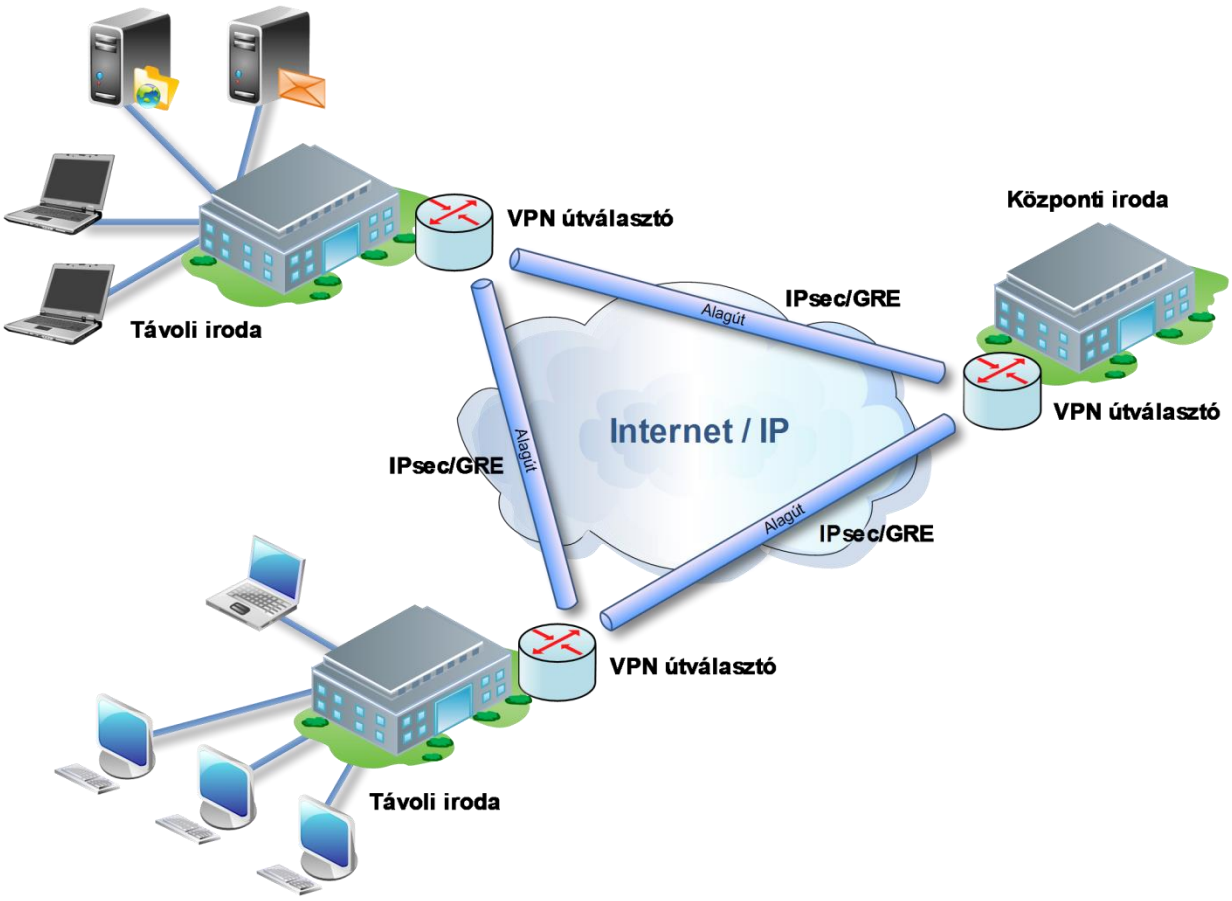
- Távoli elérésű VPN-t elsősorban az otthon vagy folyamatos mozgásban lévő dolgozók használnak, akik megosztott infrastruktúrán keresztül (DSL, ISDN, mobil- vagy kábelnet segítségével) férnek hozzá a vállalati intranethez vagy extranethez. A távoli elérésű VPN-hez mindössze egy VPN átjáró szükséges. A biztonságos kapcsolatot kezdeményező félnek VPN kliensszoftver segítségével kell a VPN átjáróhoz kapcsolódnia. A VPN kliens teszi lehetővé, hogy a központi hálózathoz csatlakozva elérhesse az – akár különböző helyszíneken található – erőforrásokat (pl.: adatközpontokat). Az alagutak létrehozásához az IPsec, a PPTP (pont-pont alagútprotokoll), az L2TP (második rétegbeli alagútprotokoll), esetleg az L2F (második rétegbeli továbbítás) használható.
  Előnyei: Nem kell magas híváskölségekkel kalkulálni, mint a betárcsázós esetben. Javítja a

termelékenységet, hisz a dolgozó a tényleges helyzetétől függetlenül végezhet érdemi munkát. Példa a távoli elérésű VPN-re az 5. ábrán látható.

- A telephelyek közötti intranet VPN a vállalati központok, telephelyek, kihelyezett irodák és a belső hálózat között biztosít dedikált, állandó kapcsolatot, megosztott infrastruktúrán keresztül. Az intranet VPN és az extranet VPN közötti fő különbség, hogy előbbi kizárólag a megbízható munkatársak részére biztosít hozzáférést. Az intranet VPN esetében egyazon vállalat különböző földrajzi helyszínei között – az internet segítségével – alakítanak ki biztonságos alagutakat, a felhasználók felé pedig úgy tűnik, mintha mindannyian ugyanabból a belső hálózatból csatlakoznának. Az ilyen hálózatokkal szemben az erős titkosításon túl szigorú elvárások vannak a teljesítménnyel és sávszélességgel kapcsolatban is. Az alagutak létrehozásához IPsec vagy IPsec/GRE protokoll használatos. Példa a telephelyek közötti intranet VPN-re a 6. ábrán látható.
  Előnyei: Komoly költségek takaríthatók meg a hagyományos bérelt vonalakkal szemben.
- A telephelyek közötti extranet VPN külső ügyfeleket, beszállítókat kapcsol össze a vállalati ügyfélhálózattal. Általában tűzfalakkal egészül ki az alagutak használata, hogy a külső felhasználók csak bizonyos információkhoz és erőforrásokhoz férhessenek hozzá.
  Előnyei: A teljes partnerhálózat azonos házirend, biztonsági és QoS beállítások szerint üzemelhet.



5. ábra: Távoli elérésű VPN



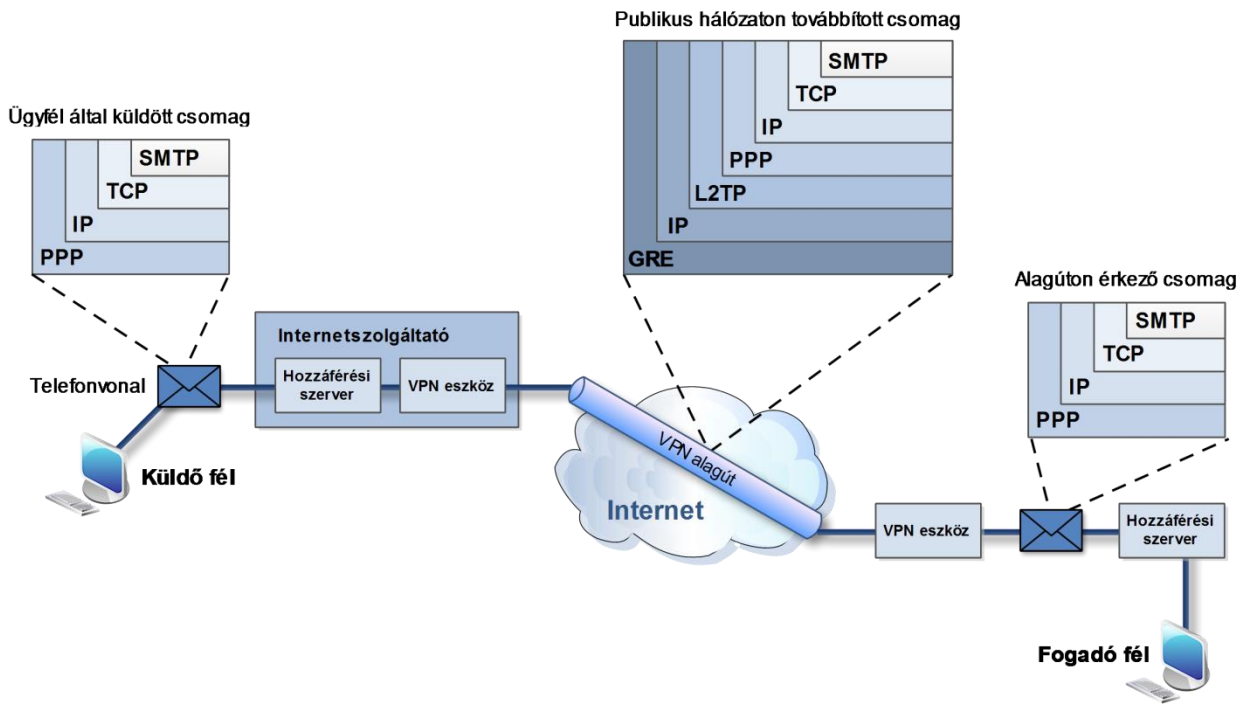
6. ábra: Telephelyek közötti intranet VPN

A biztonságos VPN sajátosságai

A VPN-t használó adattovábbítás megfelelő biztonságáról egyrészt a beágyazás, másrészt a titkosítás gondoskodik. Beágyazásnak (más néven alagutazásnak) nevezzük azt a folyamatot, amelynek során a teljes csomagot egy másikba beágyazva az összetett csomagot továbbítjuk egy (akár publikus) hálózaton. Az alagutazáshoz az alábbi protokollok szükségesek:

- Átviteli (carrier) protokoll, ami az információt szállítja.
- Beágyazási protokoll (pl.: GRE, IPsec, L2F, PPTP, L2TP), amellyel az eredeti adat becsomagolásra kerül. Nem mindegyik protokoll képes ugyanazt a biztonságot garantálni.
- Utasprotokoll (passenger protocol), amely tulajdonképpen az eredeti adat (IPX, AppleTalk, IPv4, IPv6).

A beágyazás folyamata a 7. ábrán látható.



7. ábra: A beágyazás (alagutazás) folyamata

A VPN biztonsága: az IPsec és a GRE

Az alagútprotokollok jelentős mértékben különbözhetnek az átvitt adatok számára kínált szolgáltatások, a kezelhető problémák és a biztonsági szint tükrében.

Az IPsec önmagában megbízható magánhálózatot kínál, de csak egyedi címzésű (unicast) IP-csomagok számára. Amennyiben az IPsec és a GRE protokollt kombináljuk, lehetőség nyílik a csoportcímzésű (multicast) IP-csomagok, a dinamikus IGP irányítóprotokollok és az IP-től eltérő szállítási protokoll használatára is.

Az IPsec két titkosítási módot ismer: az alagútmódot és a szállítási módot.

Alagútmódban mind a fejléc, mind pedig az adattartalom titkosítva lesz, szállítási módban viszont kizárólag az adattartalom titkosítása történik meg. Fontos, hogy a szállítási módhoz teljesen IPsec-kompatibilis rendszer szükséges. Emellett elengedhetetlen a közös kulcs és a tűzfalak nagyon hasonló házirenden alapuló beállítása is. Az IPsec többféle eszköz (útválasztó-útválasztó, tűzfal-útválasztó, PC-útválasztó, PC-kiszolgáló) között képes az adatokat titkosítani.

A GRE becsomagolja a csomagok IP-fejlécét és adattartalmát, és kiegészíti azt a GRE-beágyazás fejlécével. A hálózattervezők előszeretettel használják ezt a módszert a csomagok IP-fejlécének elrejtésére, méghozzá a GRE-beágyazás adattartalmi részébe.

Alagutazás telephelyek közötti VPN használatával

A telephelyek közötti VPN esetében a GRE felel azért, hogy az utasprotokollt alkalmassá tegye az átviteli (jellemzően IP-alapú) protokoll feletti szállításra.

Alagutazás távoli elérésű VPN használatával

A távoli elérésű VPN esetében az alagutazáshoz használt protokoll jellemzően a PPP és társai. Amikor létrejön a hálózati kapcsolat a kliens számítógép és a távoli elérésű rendszer között, a PPP lesz az átviteli protokoll. A távoli elérésű VPN esetében is használhatók az alábbi – a PPP alapstruktúráját használó – protokollok: L2F, PPTP, L2TP.

A hitelesítés kérdése

Amennyiben hálózaton keresztül dolgozunk vagy bonyolítunk üzletet, nagyon fontos, hogy tudjuk ki van a vonal, email vagy fax másik végén. Ugyanez igaz VPN használata esetén, tehát a VPN alagút túlsó oldalán lévő eszközt hitelesíteni kell, mielőtt a létrejövő kapcsolatot megbízhatónak tartanánk. Az alábbi módszerek állnak rendelkezésre, hogy a felek meggyőződjenek arról, hogy a megfelelő partnerhez kapcsolódnak-e:

- Felhasználói név és jelszó
- Egyszeri jelszó (OTP, One Time Password)
- Biometrikus azonosítás
- Digitális tanúsítvány
- Publikus/privát kulcspár
- Közös titok (shared secret)

Távoli elérésű VPN környezetben sokkal biztonságosabb hozzáférést tesz lehetővé az ún. AAA szerverek használata. Az AAA betűszó az angol hitelesítés (authentication), jogosultság- (authorization) és fiókkezelés (accounting) szavak rövidítése. Egy kliensoldalról kezdeményezett kapcsolat esetében a kérés automatikusan egy AAA szerverhez kerül továbbításra, amely ellenőrzi, hogy ki az ügyfél, milyen jogosultságokkal rendelkezik, majd naplózza a felhasználó minden tevékenységét. Ez utóbbi különösen hasznos egy esetleges biztonsági probléma felmerülése során.

Az IPsec biztonsági funkciói

Az IPsec egy szabvány, amely az IP-hálózaton történő biztonságos adatátvitel menetét határozza meg, biztosítja az adatok bizalmasságát, sértetlenségét és a nem megbízható hálózatok feletti kommunikáció hitelességét. Az IPsec egy olyan protokollkészlet, amely egyik titkosítási vagy hitelesítési algoritmushoz, kulcsgenerálási technikához vagy biztonsági társításhoz (SA, security association) sem kötődik. Az IPsec tulajdonképpen csak biztosítja a szabályokat, míg a létező algoritmusok adják a titkosítást, hitelesítést vagy kulcskezelést.

Az adatok megbízhatóságáról az IPsec titkosítással gondoskodik, amely megakadályozza a nyilvános vagy vezeték nélküli hálózatokon átvitt adatok elolvasását vagy lehallgatását, mivel az elfogott csomagok nem dekódolhatók. A titkosításhoz többek között az alábbi algoritmusok használhatók: DES, 3DES, és AES.

Az adatok sértetlenségét az IPsec hash segítségével biztosítja. A hash pusztán redundancia-ellenőrzés, melynek során az IPsec összeadja az üzenet összetevőit (jellemzően a bájtok számát), majd eltárolja az összeget. A megérkezett csomagon az IPsec megvizsgálja az ellenőrzőösszeget, és összehasonlítja az eredeti, hitelesített értékkel. Amennyiben az értékek megegyeznek, biztosak lehetünk benne, hogy a kérdéses adatot nem manipulálták. Az adatok sértetlenségét a HMAC (hash-alapú üzenethitelesítési kód,

Hash-based Message Authentication Code) függvény biztosítja, amely az alábbi algoritmusokat támogatja: MD5, illetve SHA-1.

Az IPsec adatok forrásának hitelességét mindig a fogadó fél ellenőrizheti. Az IPsec felhasználók és eszközök hitelesítésére egyaránt alkalmas. Az adatforrás hitelesítésének minőségét az adatok sértetlenségét biztosító szolgáltatás határozza meg.

A visszajátszás elleni (anti-replay) védelem ellenőrzi, hogy minden egyes csomag egyedi, nem pedig duplikált. Az IPsec úgy gondoskodik a csomagok védelméről, hogy minden beérkező csomag sorszámát összehasonlítja a meglévőkkel, valamint csúszóablakot (sliding window) is alkalmaz. Ha egy csomag sorszáma a csúszóablak értékénél korábbi, azt későnek tekinti. A duplikált, illetve késő csomagok eldobásra kerülnek.

Az IPsec protokolljai

Az IPsec szabvány hitelesítési és adatvédelmi módszert kínál a biztonságos adatátvitelben résztvevő (akár több) partnerek számára. Az IPsec része az IKE (Internet Key Exchange) kulcsok cseréjére használt protokoll, valamint két IP-alapú protokoll: az ESP (Encapsulating Security Payload) és az AH (Authentication Header).

Az IPsec három fő protokollja biztosítja a biztonságos keretet az alábbiakhoz:

- Az IKE felelős a biztonsági paraméterek egyeztetéséért, valamint a hitelesített kulcsok létrehozásáért. Az IPsec szimmetrikus titkosítási algoritmusokkal valósítja meg az adatok védelmét, amelyek sokkal hatékonyabbak és könnyebben alkalmazhatók hardveres környezetben, mint az egyéb típusú algoritmusok. Az IKE biztosítja az ezen algoritmusok számára szükséges biztonságos módszert a kulcscseréhez.
- Az AH, vagyis az IP hitelesítési fejléce biztosítja az IP-adatcsomagok számára a kapcsolat nélküli sértetlenséget, illetve az adatforrás hitelesítést, valamint opcionális védelmet a visszajátszások ellen. Az AH-t a védeni kívánt adatba kell beágyazni, de mára szinte teljesen felváltotta az ESP.
- Az ESP felelős az adatok titkosításáért, hitelesítéséért és védelméért. Az ESP nem csupán adatvédelmi szolgáltatásokat vagy opcionális adathitelesítést, hanem visszajátszás elleni szolgáltatásokat is kínál. A védeni kívánt adatokat az ESP csomagolja be, a legtöbb IPsec megvalósítás ezt használja.

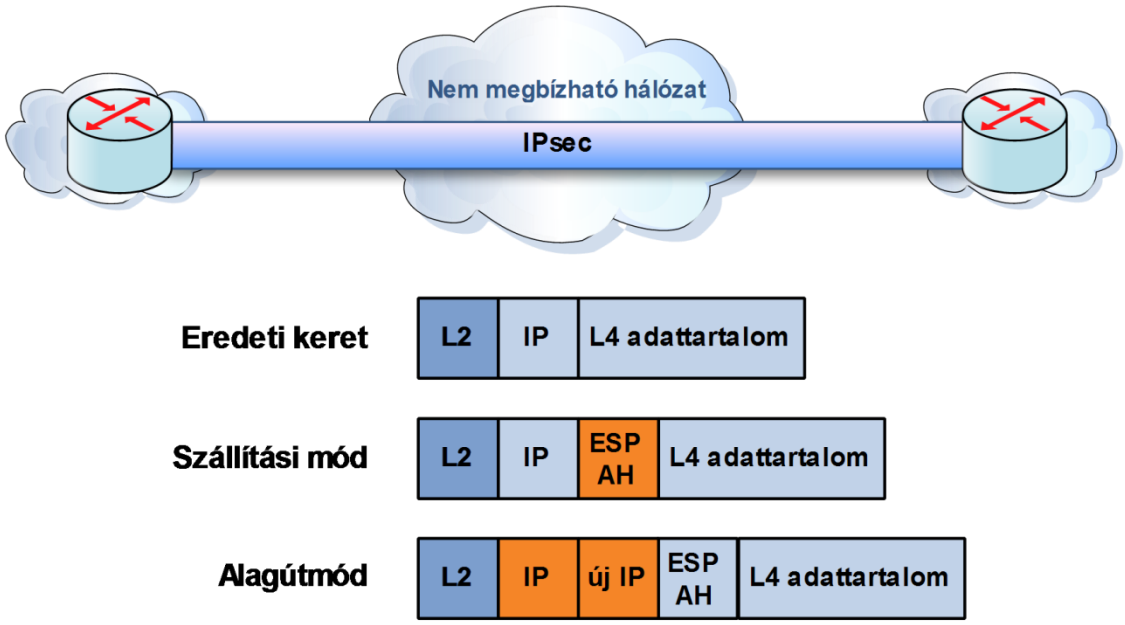
Az IPsec fejlécei

Az IPsec a hitelesítésről, az adatok sértetlenségéről, valamint a titkosításról az IP-adatcsomagba beszúrt AH vagy ESP fejléccel, esetleg mindkettővel gondoskodik.

Az AH lehetőséget biztosít az IP-adatcsomag hitelességének, illetve. sértetlenségének ellenőrzésére, az ESP ezen felül információt tartalmaz az adattartalom titkosításáról is. Az AH és az ESP két állomás (pl.: végberendezés vagy átjáró) között használható.

Az AH és az ESP megoldások szabvány alapú módszert kívánnak meg az adatok manipulációja és illetéktelen olvasása elleni védelemhez. Az IPsec az alábbi, különböző erősségű titkosításokat támogatja: DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) és az AES (Advanced Encryption Standard). Az IPsec számos, különböző erősségű hash módszert is támogat: HMAC (Hash-based Message Authentication Code), MD5 (Message Digest 5) és az SHA-1 (Secure Hash Algorithm 1).

Az IPsec által használt fejlécek a 8. ábrán láthatóak.



8. ábra: IPsec fejlécek

Az IKE protokoll

A titkosított VPN megoldásoknál rendszeres időközönként szükségessé válik a titkosítási kulcsok cseréje. Ennek elmaradása esetén a hálózat kiszolgáltatottá válhat a kipörgetéses (brute-force) támadásokkal szemben. A probléma kiküszöbölésére az IPsec az IKE protokollt alkalmazza, amely további protokollok (pl.: DH kulcscsere) segítségével biztosítja a résztvevő felek hitelesítését, illetve a kulcsok generálását. Az IKE az 500-as UDP portot használja.

Az IPsec az IKE protokoll használatával az alábbi funkciókat biztosítja:

- A biztonsági társítások jellemzőinek egyeztetése
- Automatikus kulcsgenerálás
- Automatikus kulcsfrissítés
- Felügyelhető (menedzselhető) kézi beállítások

A biztonsági társításhoz az alábbiak szükségesek:

- Az ISAKMP (Internet Security Association and Key Management Protocol) egy olyan protokoll-környezet, amely megadja a kulcscseréhez használt protokoll, valamint a biztonsági házirend egyeztetésének menetét. Az ISAKMP bármelyik szállítási protokoll felett alkalmazható.
- A SKEME egy olyan kulcscseréhez használt protokoll, amely megadja, hogy gyors kulcsfrissítéssel hogyan származtathatók hitelesített kulcsok.
- Az OAKLEY egy olyan kulcscseréhez használt protokoll, amely megadja hogyan szerezhetők be hitelesített kulcsok. Az OAKLAY alapértelmezés szerint a DH kulcscsere algoritmust használja.

Az IKE automatikusan egyezteti az IPsec biztonsági társításait, és költséges előkészítés nélkül teszi lehetővé a biztonságos IPsec kommunikációt. Az IKE az alábbi tulajdonságokkal rendelkezik:

- Szükségtelenné teszi az IPsec összes biztonsági paraméterének megadását mindkét oldalon (félnél).
- Meghatározhatja az IPsec biztonsági társításainak élettartamát.
- Lehetővé teszi az IPsec kapcsolat ideje alatti kulcscserét.
- Lehetővé teszi a visszajátszás elleni védelmet az IPsec számára.
- Biztosítja a hitelesítés-szolgáltató (tanúsítvány-kibocsátó) támogatását a felügyelhető, skálázható IPsec implementációkhoz.
- Lehetővé teszi a résztvevők dinamikus hitelesítését.

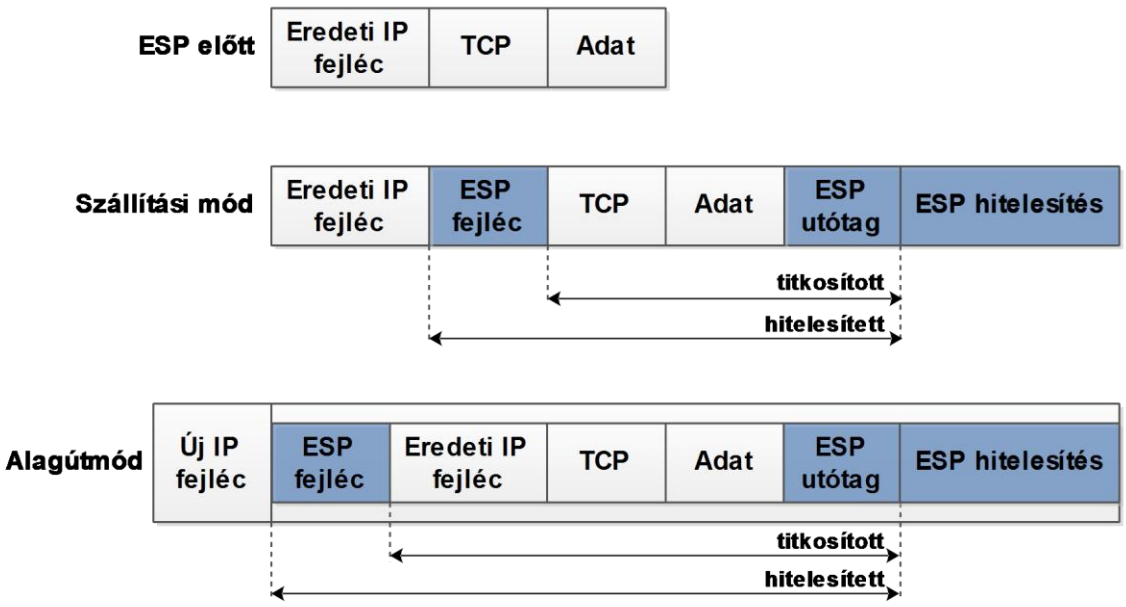
Az IKE lépéseinek részletes leírása a telephelyek közötti VPN működésénél található.

Az ESP és az AH protokoll

Az IPsec protokoll magját az ESP fejléc adja, amely megfelelő titkosítással és transzformációs készlettel gondoskodik az adatok visszafejthetetlenségéről. Az ESP kizárólag a csomag adatrészét védi, opcionálisan gondoskodhat a védett adatok hitelesítéséről is.

Az IPsec másik fontos eleme, az AH protokoll nem a hagyományos értelemben – az adatokat elrejtve – védi a kommunikációt, hanem egyfajta pecséttel látja el az adatcsomagokat. Így tulajdonképpen az IP-fejléc mezőit – ideértve a címmezőket – is védi. Az adatok megbízhatóságát önmagában azonban nem képes garantálni.

Az IPsec két módban továbbíthatja az adatokat a hálózaton keresztül: alagútmódban, illetve szállítási módban. A két mód nem csupán a használatukban, hanem az „utazó” csomaghoz adott többlet mennyiségében is eltér egymástól. Az ESP működési elvét a 9. ábra illusztrálja.



9. ábra: Az ESP működési elve

Az alagútmód a teljes IP-csomagot becsomagolja és védi. Mivel az alagútmód becsomagolja vagy elrejti az IP-csomag címét, a sikeres továbbításhoz a csomagnak egy új – kb. 20 bájtos – fejlécet kell kapnia. Alagútmódban egyaránt használható az ESP és az AH, vagy a kettő kombinációja.

Teljesítmény szempontjából a jellemzően kisméretű csomagokat használó átvitel költségesebb, mint ha ugyanazt az adatmennyiséget nagyobb csomagok szállítanák, ezért lehetőség van az ún. szállítási mód használatára is. Az IPsec szállítási módja az ESP fejlécet az IP-fejléc és a csomag szállítási rétege közé szúrja be, ezáltal a biztonságos adatforgalmat bonyolító mindkét hálózati csomópont címe látható marad. Ez ugyan kevésbé biztonságos megoldás, viszont nem keletkezik új IP-fejléc, ezért a méret sem nő. Szállítási módban egyaránt használható az ESP és az AH, vagy a kettő kombinációja. A szállítási mód különösen jól tud együttműködni a GRE protokollal, amely egy IP-fejléc beszúrásával már eleve elrejti a végberendezések címeit.

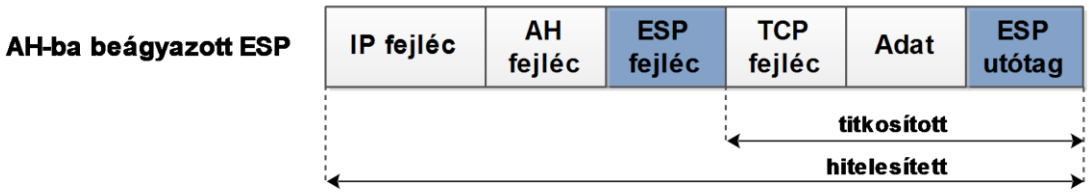
Az ESP titkosítási algoritmusai önmagukban nem tudják garantálni az adatok hitelességét vagy sértetlenségét. Az ESP a problémát az adatok hitelességét és sértetlenségét biztosító szolgáltatásokkal kiegészítve, kétféleképpen oldhatja meg:

- Hitelesített ESP formátummal
- Az AH-ba beágyazott ESP-vel

A hitelesített ESP esetében az IPsec először szimmetrikus kulcs segítségével titkosítja az adattartalmat, majd egy második szimmetrikus kulcs, valamint a HMAC-SHA1 vagy a HMAC-MD5 használatával kiszámol egy hitelesítési értéket a titkosított adatra. Ezt a hitelesítési értéket a csomag végéhez fűzi. A fogadó fél először kiszámítja a titkosított csomaghoz tartozó hitelesítési értéket a második szimmetrikus kulcs és

ugyanazon algoritmus használatával. Amennyiben a kiszámolt érték megegyezik a csomaghoz kapott hitelesítési értékkel, akkor az első szimmetrikus kulcs segítségével kikódolja az eredeti adatot.

A másik megoldás, hogy az ESP csomag beágyazható egy AH csomagba is. Először az adattartalom kerül titkosításra, majd a titkosított adatokra kell ráereszteni egy hash-függvényt (pl.: MD5 vagy SHA-1). A továbbiakban a hash biztosítja a forrás hitelességét, valamint az adattartalom sértetlenségét. Erre példa a 10. ábrán látható.



10. ábra: AH-ba beágyazott ESP

Az AH által biztosított hitelesség és sértetlenség

Az AH függvény a teljes adatcsomagra alkalmazandó, kivéve az IP-fejléc olyan mezőit, amelyek az átvitel során módosulhatnak. Ennek tipikus példája az útválasztók által folyamatosan módosított TTL mező.

Az AH működése az alábbi lépésekből áll:

1. Az IP-fejléc és az adattartalom hash-értékének kiszámítása
2. Az AH fejléc felépítése a hash alapján, amely az eredeti csomaghoz lesz hozzáfűzve.
3. Az „új” csomag továbbítása az IPsec partner útválasztója felé.
4. A partner útválasztó kiszámítja a kapott IP-fejléc és az adattartalom hash-értékét.
5. A partner útválasztó az AH fejlécből kivonja a kapott hash-értéket.
6. A partner útválasztó összehasonlítja a két hash-értéket, amelyeknek pontosan meg kell egyezniük.

Az ESP protokoll

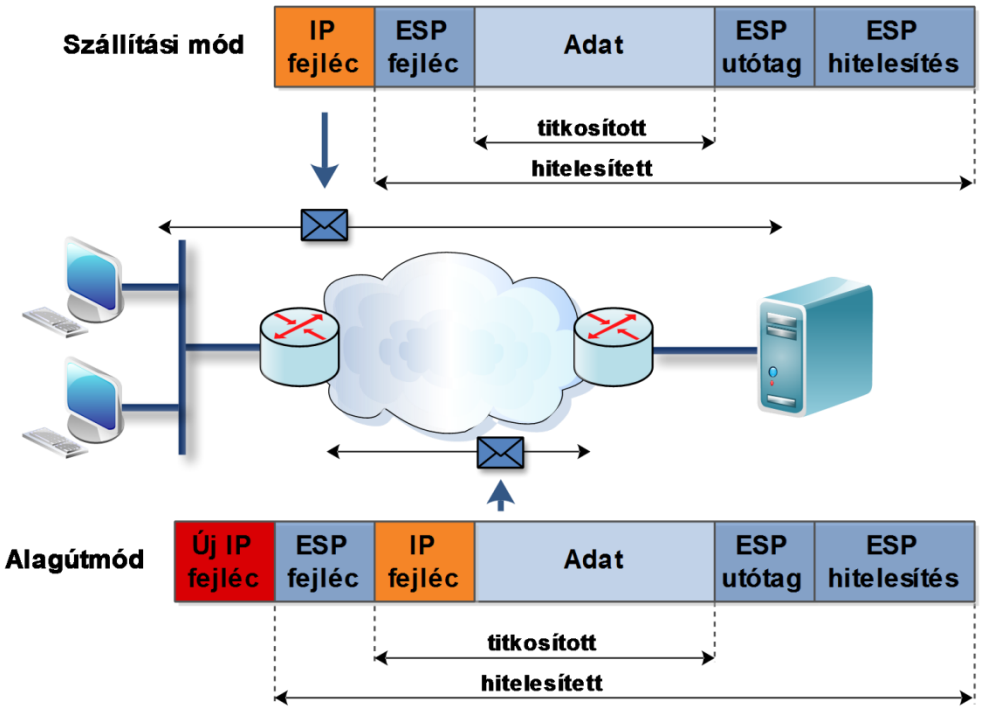
Amikor az ESP végzi a hitelesítést és a titkosítást egyaránt, először a titkosítás történik meg. Ezt a sorrendet az indokolja, hogy a fogadó fél így gyorsabban tudja detektálni és eldobni az ismételt vagy hamis csomagokat. Mivel a fogadó fél még a kikódolás előtt ellenőrizheti a bejövő csomagok hitelességét, csökkentheti egy esetleges elárasztásos (DoS) támadás káros hatásait.

Az IPsec alapértelmezés szerint a szállítási módot használja, amely kizárólag a csomag adattartalmát, valamint a magasabb rétegbeli protokollokat védi, de az eredeti IP-címet védtelenül hagyja. Ez teszi lehetővé, hogy a célhoz vezető útvonalat a csomag az eredeti IP-címe alapján találja meg. Az ESP szállítási módja mindig két állomás között használható.

Az IPsec alagútmódjának használata esetén mind az IP-fejléc, mind pedig az adattartalom titkosítva lesz. Az alagútmód biztosítja a teljes IP-csomag védelmét, amelyet AH vagy ESP adattartalomként kezel.

(Tulajdonképpen a teljes IP-csomag kap egy AH vagy ESP fejlécet, majd a beágyazott csomag egy újabb IP-fejlécet.) Az ESP alagútmód általában egy állomás és egy biztonsági átjáró, esetleg két biztonsági átjáró között használható. Távoli elérésű hozzáférésnél általában az ESP alagútmód használata jellemző.

Az ESP szállítási, illetve alagútmódját a 11. ábra illusztrálja.



11. ábra: Az ESP működési módjai

A telephelyek közötti VPN működése

Az IPsec működése öt pontban foglalható össze, amelyet a 12. ábra is illusztrál:

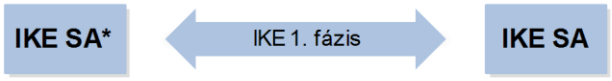
1. Ha a VPN eszköz védelmet igénylő forgalmat érzékel, az „érdekes” forgalom elindítja az IPsec folyamatot.
2. Az IKE első fázisa, amelynek során az IKE hitelesíti az IPsec partnereket (előre megosztott kulcsok, RSA tanúsítványok vagy RSA-val titkosított, egyszer használatos kulcsok segítségével), majd egyezteti az IKE biztonsági társításait, megteremtve ezzel a következő fázishoz szükséges biztonságos kommunikációs csatornát. Az IKE első fázisa kétféle módban lehetséges: normál (main) vagy agresszív módban. Normál módban a felek között három kétirányú üzenetváltás zajlik. Az elsőben a két fél egyezteti, hogy milyen algoritmust és hash-t használnak az IKE kommunikáció biztonságossá tételéhez. A másodikban egy Diffie-Hellmann által generált megosztott kulcs, illetve egyszer használatos kulcs (nonce) segítségével ellenőrzik egymás kilétét. Miután létrejön a megosztott kulcs, ezzel generáljuk az összes további titkosítási és hitelesítési kulcsot. A harmadikban mindegyik fél

hitelesítéssel ellenőrzi a másik fél kilétét. Agresszív módban kevesebb üzenetváltás, ezáltal kevesebb csomag szükséges, szinte minden az első fázisban történik, a végeredmény ugyanaz.

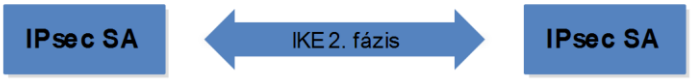
3. Az IKE második fázisa, amelynek során az IKE egyezteti az IPsec biztonsági társítások paramétereit, majd beállítja az egymással megegyező IPsec biztonsági társításokat a partnereknél. Ezek a paraméterek határozzák meg az átvitt adatok és üzenetek védelmét a végpontok között. Két pont közötti biztonságos kapcsolat létrehozásakor szükséges a biztonsági protokoll által használt algoritmusok ismertetése. Ezeket nem egyenként, hanem ún. transzformációs készletekbe szervezve lehet összevetni. A transzformációs készlet tartalmazza a titkosítási algoritmust, a hitelesítési algoritmust, módot, valamint a kulcs hosszát is. Amennyiben nincs egyezés a partnerek transzformációs készletei között, az alagút megszűnik. Pont-pont környezetben elég, ha egyetlen IKE házirendet határoz meg minden végpont. Küllős (hub-and-spoke) környezetben viszont a központi szerepet betöltő helyszínhez több IKE házirendet is szükséges lehet megadni, hogy az összes partner igényeinek meg tudjon felelni. Mivel a biztonsági társítás élettartama véges, ezért szükség lehet annak (és persze a kulcsok) megújítására.
4. Adatátvitel, a biztonsági társítás biztonsági házirend-adatbázisban (SPD, Security Policy Database) tárolt paraméterei és kulcsai alapján történik.
5. Az IPsec alagút megszüntetése törlés vagy időtúllépés miatt. Időtúllépést eredményezhet bizonyos mennyiségű idő eltelése vagy bizonyos adatmennyiség átvitele. Ha a folyamatos átvitel biztosításához új IPsec biztonsági társítás szükséges, az IKE második – vagy szükség esetén az első – fázisa hajtódik végre, jellemzően még az érvényben lévő biztonsági társítás lejárta előtt.

1. **Az "A" munkaállomás "érdekes" adatforgalmat küld a "B" munkaállomás felé.**

2. **Az "A" és "B" útválasztó elvégzi az IKE első fázisához tartozó lépéseket.**



3. **Az "A" és "B" útválasztó elvégzi az IKE második fázisához tartozó lépéseket.**



4. **Információcsere történik az IPsec alagúton keresztül.**

5. **Az IPsec alagút megszűnik.**

*SA (Security Association) = Biztonsági társítás

12. ábra: A telephelyek közötti IPsec VPN működésének lépései

A telephelyek közötti IPsec VPN beállítása

A telephelyek közötti VPN beállítása az alábbi lépések szerint történik:

1. Az IKE alagút létrehozásához szükséges ISAKMP házirend beállítása, amely kitérhet a kulcs terjesztési módjára, a titkosításhoz használt algoritmusra, a hash algoritmusra, hitelesítési módra, a kulcscsere menetére, valamint az IKE társítás időtartamára.
2. A transzformációs készlet (transform set) megadása, amely rögzíti az IPsec alagút paramétereit (pl.: a titkosítást, illetve az adatok sértetlenséget biztosító algoritmusokat)
3. Egy kripto hozzáférési lista (ACL) létrehozása, amely meghatározza az IPsec alagúton áthaladó forgalmat. A szabályra nem illeszkedő csomagok természetesen nem kerülnek eldobásra, hanem titkosítás nélkül, az irányítóprotokoll normál működésének megfelelően kerül továbbításra.
4. Kripto-leképezés létrehozása, amely az előzőekben beállított paramétereket kombinálja, illetve megadja az IPsec partnereszközt (peer). A bejegyzések az alábbiakra terjedhetnek ki:
   - Mely forgalmat kell az IPsec-kel védeni (a kripto-ACL alapján)?
   - Milyen a védett adatfolyam finomsága (a biztonsági társítások alapján)?
   - Hova kell az IPsec által védett forgalmat továbbítani (vagyis ki az IPsec partner)?

- Mi az IPsec forgalomhoz használt lokális cím (opcionális)?
- Milyen IPsec biztonságot válasszunk a kérdéses forgalomhoz (a transzformációs készletből kiválasztva)?

5. A kripto-leképezés alkalmazása a VPN eszköz kimenő interfészére.
6. Az ACL létrehozása és interfészre történő alkalmazása. A határ-útválasztók jellemzően korlátozó ACL-eket használnak, amelyek akaratlanul is blokkolhatják az IKE és IPsec protokollt.

Tippek, trükkök:

- Amennyiben az interfészen dinamikus irányítóprotokoll működik, annak forgalmát is engedélyeznünk kell.
- Amennyiben az IPsec forgalom áthalad cím- vagy portfordítást (NAT, illetve PAT) használó eszközökön, szükség van az IPsec NAT-T (Network Address Translation Traversal) funkciójára, amely az IPsec csomagot egy UDP fejléccel kiegészítve csomagolja be. A megfelelő működéshez szükség lehet a tűzfalszabályok további módosítására (kiegészítésére).

A GRE protokoll

A GRE (Generic Routing Encapsulation) egy olyan alagútprotokoll, amely sokféle protokoll- és csomagtípus beágyazását teszi lehetővé az IP-alagutakon belül, egyfajta virtuális pont-pont kapcsolatot létrehozva az IP-hálózaton két útválasztó között. Ezáltal a GRE-t alkalmazó IP-alagúttechnika lehetővé teszi a hálózat bővülését mindössze egyetlen protokollt támogató gerinchálózatok fölött is. Így az alagútban használt irányítóprotokollok is küldhetnek és fogadhatnak útvonal-frissítési információkat a virtuális hálózatban. Ehhez mindössze annyi szükséges, hogy az adattartalmi rész és az alagutazáshoz használt IP-fejléc közé beszúrjunk egy GRE fejlécet is. A GRE fejléc tartalmaz egy protokolltípus (protocol type) mezőt, amely bármilyen L3 rétegbeli protokoll beágyazását támogatja. A GRE nem állapottartó, és nem biztosít különösebben erős biztonsági mechanizmust sem az adattartalom védelmének érdekében. Az eredeti, alagúton átutazó csomaghoz képest legalább 24 bájtnyi többletet jelent a GRE, illetve. az alagutazáshoz használt fejléc.

A GRE fejlécében előforduló alagútkulcs (tunnel key) kétféle célra használható:

Egyszerű, titkosítás nélküli szövegként hitelesíthető vele minden áthaladó csomag a GRE végpontok között, ugyanakkor a csomagok útvonalán bárki könnyen megtekintheti a kulcsot, és meghamisíthatja az alagútcsomagokat is.

Sokkal elterjedtebb a kulcs használata olyan környezetben, ahol két útválasztó között ugyanarról az IP-címről induló alagutat kell kialakítani. Ekkor a különböző alagutakhoz tartozó GRE csomagok a kulcs segítségével válnak megkülönböztethetővé.

Biztonságos GRE alagutak

A GRE legfőbb előnye az erőteljes, ugyanakkor egyszerű alagúttechnika biztosítása. A GRE bármilyen L3 rétegbeli protokollt elfogad adattartalomként, és azok számára virtuális pont-pont összeköttetést biztosít. A GRE segítségével az irányítóprotokollok használata is lehetővé válik az alagút felett.

A GRE fő hiányossága, hogy szegényes a biztonsági készlete. Kizárólag egyszerű, titkosítás nélküli szöveges kulcsot használ a hitelesítéshez, amely nem tekinthető biztonságosnak. A csomagok útvonalán gyakorlatilag bárki könnyen megtekintheti a kulcsot, és meghamisíthatja az alagútcsomagokat is. A biztonságos VPN által megkövetelt alábbi feltételeknek a GRE önmagában nem felel meg.

Erős titkosítás:

- az adatforrás hitelesítése, amelyet nem lehet kijátszani beékelődéses (man-in-the-middle) támadással
- az adat sértetlenségének biztosítása úgy, hogy ne lehessen kijátszani beékelődéses támadással

A GRE alagutak biztonságossá tétele az IPsec segítségével

Az IPsec gyakorlatilag biztosítja a GRE-ből hiányzó összes alagútjellemzőt:

- szimmetrikus algoritmust (pl.: 3DES-t vagy AES-t) használó titkosítás
- Az adatforrás hitelesítése hash-alapú üzenethitelesítési kódok (HMAC) (pl.: MD5 és SHA-1) segítségével
- Az adat sértetlenségének ellenőrzése HMAC segítségével

Az IPsec fenti szolgáltatásai viszont eredetileg kizárólag IP-forgalomhoz készültek. Több protokoll egyidejű támogatásához mindig szükség van további alagútprotokollra.

GRE az IPsec fölött

A pont-pont alapú „GRE az IPsec fölött” legtöbb megvalósítása a küllős topológiát használja, mivel a VPN helyszínek közötti teljes kapcsolat létrehozásához ez igényli a legkevesebb alagutat. A küllős topológia minimalizálja az IPsec alagutak karbantartásához szükséges felügyeleti felesleget (többletet).

OpenVPN – alternatíva virtuális magánhálózat megvalósításra

Az OpenVPN egy GNU GPL alatt kiadott multiplatformos virtuális magánhálózatot megvalósító szoftver. Elérhető többek közt Linux, BSD, Windows, Solaris, Android rendszerekre. Alkalmas telephelyek közti és távoli elérésű VPN kiépítésére is. Egy bináris openvpn programot tartalmaz, ami kliensként és szerverként is tud viselkedni. Konfigurációját egy szöveges állományon keresztül lehet beállítani. Egyes rendszerekre elérhető hozzá grafikus konfiguráló segédprogram, de tudja kezelni a Linux világban népszerű Network-manager is. Tud működni inicializálás után felhasználói térben (userspace) rendszergazdai jogosultság nélkül is. Az alagút titkosítását az OpenSSL szoftver valósítja meg teljes egészében, így használható bármilyen titkosító algoritmussal, amit az OpenSSL ismer és használni képes. Egy virtuális hálózati kártyát hoz létre, melynek két típusa lehet: TUN vagy TAP. TUN típus esetén IP-forgalom szállítására lesz használható. TAP típus esetén bármely ethernet forgalom továbbítható lesz rajta keresztül. Ennek köszönhetően működhet TAP felett minden olyan protokoll is, ami szórási címre

küldött csomagokat is használ a működéséhez. Ilyen például a Windows rendszereken a fájl- és nyomtatómegosztásra használt SMB (server message block) protokoll. A felek azonosítása történhet előre kiosztott kulcspárok és tanúsítványok felhasználásával, de az hitelesítési motorja kiegészíthető beépülő modulokkal, így az azonosítás elvégezhető PAM-on vagy RADIUS szerveren keresztül is. Tartalmaz egy szkriptgyűjteményt a gyors és egyszerű kulcspár és tanúsítvány generáláshoz. Ha kulcsos azonosítást választjuk, akkor minden kliensnek szüksége lesz a szerver tanúsítványhoz, valamint saját kulcspárra. A kulcspárban megjelölt név (CN, common name) mező segítségével megkülönböztethetjük a klienseket csatlakozáskor, és a közös, mindenkire vonatkozó beállítások mellett kliensre szabott beállításokat is eljuttathatunk a távoli eszközhöz, így például egyedi útválasztó szabályokat. Egy OpenVPN folyamat több kliens egyidejű csatlakozását is tudja kezelni.

3. Hálózatbiztonsági architektúrák (terheléselosztás, azonnali helyreállítás)

A tűzfal célja

Tűzfalak alkalmazása többes céllal történhet. Céljuk egyfelől, hogy forgalomszabályozási pontot képezzenek a szervezet belső hálózata és az internet között mindkét irányba. Az internet vagy a szervezet szemszögéből nézve bármely, külső hálózatnak minősülő irányból csak a szervezet házirendjének megfelelő, és csak a szükséges hálózati forgalmat szabad beengednie. Másfelől saját szervezetünk kifelé irányuló hálózati forgalmát is szabályozhatjuk tűzfalakkal. Ennek megvalósításához a tűzfalat a hálózat határán kell elhelyezni.

Ugyanakkor alkalmazhatunk tűzfalakat szerverekre és munkaállomásokra telepítve is. Ezek célja, hogy kikényszerítsék az adott szerverre vagy munkaállomásra vonatkozó házirendet, valamint védjék azokat mind a külső, mind pedig a belső hálózat felől érkező támadások ellen. Tipikusan elhárítandó jelenségnek számít egy adott hálózat gépein futó szolgáltatások miatt futtatott portszkennelés (port scan) vagy a különböző elárasztásos támadások. Ne feledjük, hogy egy adott hálózat állomásai nem csupán kívülről, hanem belülről is támadhatók, ha a támadó már sikeresen hozzáférést szerzett valamely géphez vagy belső eszközhöz.

Fontos szem előtt tartani, hogy a tűzfal nem tud védelmet nyújtani a felhasználók gondatlansága vagy rosszhiszemű viselkedése, valamint a megtévesztéses támadások (social engineering) ellen!

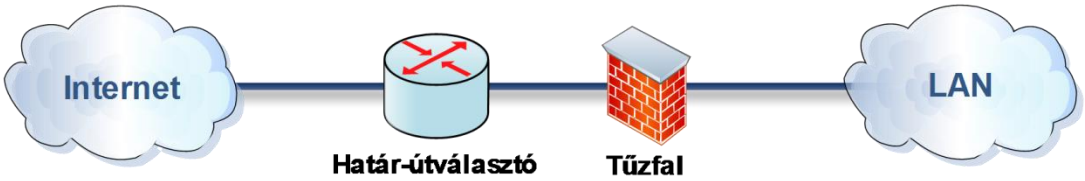
Megvalósítás

Tűzfalat szoftveres és hardveres eszközökkel egyaránt megvalósíthatunk, ahol a hardveres megvalósítás tartalmaz szoftverkomponenst is. Lássuk most ezeket egyenként!

Hardveres megvalósítás

Ebben az esetben a tűzfal szerepét egy célhardver látja el, mely rendelkezik a hálózat forgalmához mért áteresztőképességgel, akár több hálózati interfésszel, saját operációs rendszerrel, csomagszűrő vagy proxy szoftverrel, konfigurációs felülettel, melyen keresztül beállíthatók a hálózati paraméterek, valamint kialakíthatók a szabályrendszerek.

Ezen kívül lehetséges olyan hálózati kapcsolók telepítése is, melyek képesek egyszerű hozzáférési szabályok (access control list) alkalmazására switch-portonként, vagy belső, csak a switch szoftvere által létrehozott hálózati interfészenként. A hardveres tűzfal struktúrája a 13. ábrán látható.



13. ábra: Tűzfal hardveres megvalósítással

Szoftveres megvalósítás

Olyan megoldások is szóba jöhetnek, melyeknél a tűzfalszoftver telepítése a szervezet határ-útválasztójára, illetve a szerverekre és munkaállomásokra történik. Ekkor az operációs rendszer, a hálózati interfészek már adottak, a tűzfalszoftver kiegészíti az útválasztó vagy a munkaállomás képességeit. A hardveres tűzfal struktúrája a 14. ábrán látható.

Szoftveres tűzfalra példa a Linux kernellel szállított Netfilter csomagszűrő, valamint a hozzá kapcsolódó, konfigurációs lehetőséget biztosító iptables szoftvercsomag.

14. ábra: Tűzfal szoftveres megvalósítással

A tűzfalak szabályrendszerei

A szabályrendszerek határozzák meg a tűzfal működését. A tűzfal kétféle döntést hozhat: adott forgalmat engedélyez vagy sem. A döntés meghozatala előre meghatározott szabályok szerint történik. A szabályoknak sorrendjét mi határozzuk meg. A szabályok fentről lefelé (top-down) értékelődnek ki. Minden szabálynál megvizsgálja a tűzfal, hogy a szabályban rögzített feltételeknek megfelel-e a beérkező forgalom. Addig folytatódik a szabályok kiértékelése, amíg olyan szabályhoz nem ér, ami illeszkedik a beérkező csomagra. Ekkor a szabály eldöntheti, hogy a forgalom áthaladhat, visszautasításra kerül, de akár utasíthatja a tűzfalat további szabálycsoportok kiértékelésére. Ha egyik szabály esetén sem volt illeszkedés, akkor a beállított alapértelmezés szerinti akció hajtódik végre, azaz a tűzfal mindent visszautasít vagy mindent elfogad.

Külön szabálycsoportok is létrehozására is van lehetőség. A szabálycsoportok lehetővé teszik, hogy a vizsgált forgalomnak kevesebb szabályon kelljen végighaladnia, lerövidítve a kiértékeléshez szükséges időt és erőforrásigényt, valamint segíti a szabályrendszer olvashatóságát és áttekinthetőségét. Például a kiértékelési folyamat elején elágazást iktathatunk be, külön szabálycsoportra irányíthatjuk a

TCP/UDP/ICMP forgalmat, és ezekben folytathatjuk a szabályozást. De a csoportosítás történhet a forrás- vagy célcímek osztályai szerint is.

Azt sem szabad elfelejteni, hogy napjainkban történik az IPv6 protokoll széleskörű bevezetése, ami azt jelenti, hogy nem csak IPv4, hanem IPv6 címtartományainkra is ki kell alakítanunk szabályrendszerünket.

Tűzfalak csoportosítása

A tűzfalakat csoportosíthatjuk az alapján, hogy az OSI rétegmodell mely rétegében működnek. Ez alapján a következő típusokat különböztethetjük meg:

- Csomagszűrő tűzfalak
- Nem állapottartó (stateless) működés
- Állapottartó (stateful) működés
- Proxy tűzfalak

Csomagszűrő tűzfalak

A csomagszűrő tűzfalak az OSI rétegmodell adatkapcsolati (L2), hálózati (L3) és szállítási (L4) rétegében működnek. A tűzfal megkap minden csomagot az operációs rendszer kernelétől, és azokat egyesével vizsgálja, legyen az kintről befelé, vagy bentről kifelé irányított csomag. A tűzfal dönti el, hogy adott csomag áthaladhat vagy eldobásra kerül, esetleg a megfelelő ICMP válaszüzenet küldésével egy kapcsolat visszautasítása vagy – már felépült kapcsolatok esetén – bontása történjen meg.

A szabályok a csomag egy vagy több paraméterét is vizsgálhatják. Ilyen lehet például a forrás- vagy célcím, a forrás- vagy célport, a szállítási protokoll (pl.: TCP/UDP/ICMP), IP-verzió (IPv4, IPv6), fizikai cím (MAC address), esetleg valamely TCP/UDP jelzőbit (flag).

A csomagszűrő tűzfalak általában nem vizsgálják a csomagok adattartalmát, kizárólag a csomagok fejléceiben található információk alapján hoznak döntést.

Nem állapottartó működés

Ebben a működési módban a csomagszűrő tűzfal nem tart fenn saját adatbázist az új, már felépült vagy lezárásra váró kapcsolatokról. Nincs úgynevezett kapcsolatkövetés (connection tracking), így nincs információ egy adott adatfolyam állapotáról. A döntés mindig kizárólag a kapott csomag fejléceinek vizsgálata alapján történik. Sok hálózati protokoll esetén ez a mechanizmus elegendőnek bizonyulhat, főleg olyanoknál, ahol egy szolgáltatás csak egy portot használ. A webszervereknél elterjedt HTTP protokoll például tipikusan a 80-as TCP portot használja. Amennyiben egy publikus IP-címen hallgató szerver webes szolgáltatásának elérését engedélyezni kell az internet felől, akkor két szabály megadása szükséges. Egyfelől engedni kell a kapcsolat létrejöttét külső címek felől, másfelől engedélyezni kell, hogy a szerver válaszolhasson kifelé, a kezdeményező állomás irányába. Így a szerverenként minden egyes szolgáltatáshoz tartozó két szabály a szabályrendszerünk gyors hízását eredményezi.

Állapottartó működés

Több olyan, napi szinten használatos protokoll létezik, amely nem csak egy portot használ. Ilyen például az FTP protokoll, amely tipikusan a 21-es TCP porton figyel. Ezen a porton működik a protokoll működéséhez szükséges kontroll csatorna, viszont az adatátvitel a 20-as TCP porton megy végbe. Ebben

az esetben viszonylag egyszerű a helyzet, viszont léteznek olyan protokollok, amelyeknél a különböző segédfolyamok portszáma nem előre definiált. Ilyen például az NFS protokoll, vagy a VoIP hívásoknál a SIP/RTP protokollpáros. Látható, hogy ezekben az esetekben megoldás lehet a tűzfalon áthaladó kapcsolatok nyomon követése. A tűzfal feljegyzi az engedélyezett kapcsolatokat, az abban résztvevő állomások IP-címeit, a portszámokat, a kapcsolat állapotát (új kapcsolat, felépült kapcsolat, bontásra váró kapcsolat). Így megadhatók olyan szabályok is, amelyek megengedik, hogy a feljegyzett kapcsolatok további ellenőrzés nélkül átjussanak a tűzfalon. Az előző példában szereplő webszerver esetén elegendő lenne egy szabályt definiálni, ami átengedi a feljegyzett kapcsolatot, és egyet, ami engedi a webszerver elérését. Minden további szolgáltatás engedélyezéséhez elegendő egy új szabály felvétele. Hasonlóan, az FTP esetében is elegendő a 21-es TCP port engedélyezése, a nyilvántartás miatt az adatátvitel is menni fog.

Proxy tűzfalak

A proxy tűzfal az OSI rétegmodell alkalmazási rétegében (L7) működik. Nem egyszerűen csak a csomagok fejléceiben szereplő paramétereket vizsgálja, hanem az adatrészt is. Ismer több hálózati protokollt, sokszor transzparens módon működik a felhasználók szemszögéből nézve. Az ismert protokollok szabályos működése is vizsgálható proxy tűzfalakkal, amellett, hogy eszközt biztosít a hozzáférés-szabályozáshoz is. Tipikus példa proxy tűzfalra a webes forgalom szabályozására használt webproxy. A HTTP kérést a kliens gépek valójában a proxy irányába továbbítják. A proxy feldolgozza a kérést, a meghatározott szabályok alapján engedélyezi vagy visszautasítja azt. Engedélyezés esetén a webtartalmat a proxy tölti le a megadott célcímről, majd továbbítja a kérést indító kliens felé. Ez a technika használható egyfelől a szervezet gépeinek kifelé irányuló kéréseinek szabályozására, de lehetőséget ad a webszerver külső támadások elleni védelmére is az úgynevezett fordított proxy (reverse proxy) mód használatával, amely kikényszeríti a protokollszabályok pontos betartását, valamint védhet az elárasztásos próbálkozások ellen is.

Hátránya, hogy nagyobb az erőforrásigénye és késleltetése a csomagszűrő tűzfalalakkal szemben, mivel nem csomagonként történik a vizsgálat, hanem több csomag bevárása, az adatmezők összefűzése után.

Előnye, hogy naplózhatóvá teszi a tevékenységeket, szűrhető, szabályozható lesz az adatfolyam az alkalmazási rétegben. A csomagszűrő tűzfal csak azt tudja szabályozni, hogy egy adott szervezet munkatársai elérhessék az interneten levő FTP szerverek 21-es TCP portját. Azt viszont csak a proxy tűzfal képes kiszűrni, hogy egy tetszőleges irányba indított, 21-es TCP portra irányuló kapcsolat valóban egy FTP szervert ér-e el, és nem pedig a cég munkatársa próbál olyan protokollt használni, amelynek az alapértelmezett portja a házirend szerint tiltott, és kizárólag a tűzfal megkerülése a cél.

Manapság szinte minden szerveren beállítható, hogy adott szolgáltatás mely porton figyeljen, ezért a rendszergazdának megfelelő technikákat kell alkalmaznia, hogy az elképzelt szabályrendszer valóban a kívánt szabályozást biztosítsa.

Helyreállítás áramszünet után

Évente pár alkalommal szinte mindenhol elfordulnak rövidebb-hosszabb ideig tartó áramszünetek. Fontos, hogy a hálózat központi tűzfala minél magasabb rendelkezésre állást biztosítson! Ezért fontos,

hogy a tűzfalként szolgáló eszköz szünetmentes tápellátással legyen felszerelve, ami át tudja hidalni az átlagos hosszúságú áramszüneteket. Hogy milyen az átlagos hosszúságú áramszünet, azt tapasztalat útján tudjuk megállapítani, egy adott környezetre nézve. Ugyanakkor az áthidalandó idő hosszúságát meghatározhatják a szervezettel szemben támasztott elvárások is. Kis iroda esetén elfogadható lehet, ha az áram visszakapcsolása után a tűzfal üzemkész állapotáig el kell telnie egy-két percnek, és nem okoz gondot, ha az áramszünet alatt a tűzfal legfeljebb 30 percig üzemel, hisz az irodai asztali gépekhez csatlakoztatott szokványos szünetmentes tápok 15-30 perces intervallumot tudnak áthidalni. Egy internetszolgáltató vagy irodaház gerinchálózati eszközei, illetve tűzfala esetén azonban jogosan elvárható a hosszabb tartásidő, hiszen a kliensek nagy területen való elhelyezkedése miatt előfordulhat olyan szituáció, amikor csak a szerverszoba környékén – illetve internetszolgáltató esetén csak a központi eszközöknél – van áramszünet, de az épület más részein vagy akár a teljes felhordó hálózatban nincs áramkimaradás.

Általánosságban elmondható, hogy minél nagyobb tudással, feldolgozási és áteresztőképességgel rendelkezik egy tűzfaleszköz, annál több időbe telik kikapcsolt állapotból az üzemi állapot elérése. Azt is figyelembe kell venni, hogy újraindítás után a tűzfal elveszíti állapotterét! A kapcsolatokról nyilvántartott minden információ elveszik az állapottartó és proxy tűzfalak esetén egyaránt, így a klienseknek újra fel kell építeniük a hálózati kapcsolataikat, ami löketszerű terhelést jelenthet a tűzfal számára.

Tűzfal-architektúrák

A tűzfalépítési feladat komplexitása, az elvárt rendelkezésre állás és a megkövetelt biztonsági szint határozza meg, hogy milyen architektúrát alkalmazunk. Az alábbiakban néhány építkezési mód leírása olvasható.

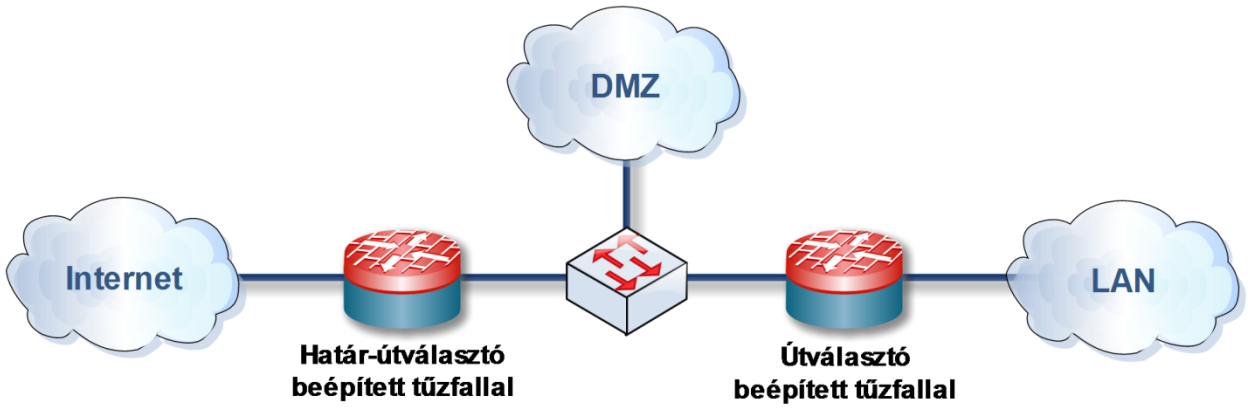
Egyedülálló tűzfal

Egyedülálló tűzfal esetén a belső hálózat és a külső hálózat között csak egy tűzfal helyezkedik el, amely minden irányból szabályoz. Előnye, hogy alacsony a kialakítás költsége, egy eszközt kell konfigurálni és üzemeltetni. Hátránya, hogy csak egy védelmi vonalat teremt, azaz kritikus meghibásodási pontnak (single point of failure) tekinthető. A tűzfal sikeres feltörése vagy szabályainak kijátszása a külső támadó számára direkt hozzáférést biztosít a belső hálózathoz. Az egyedülálló tűzfal struktúrája a 15. ábrán látható.

15. ábra: Egyedülálló tűzfal

Kettős (szendvics) tűzfal

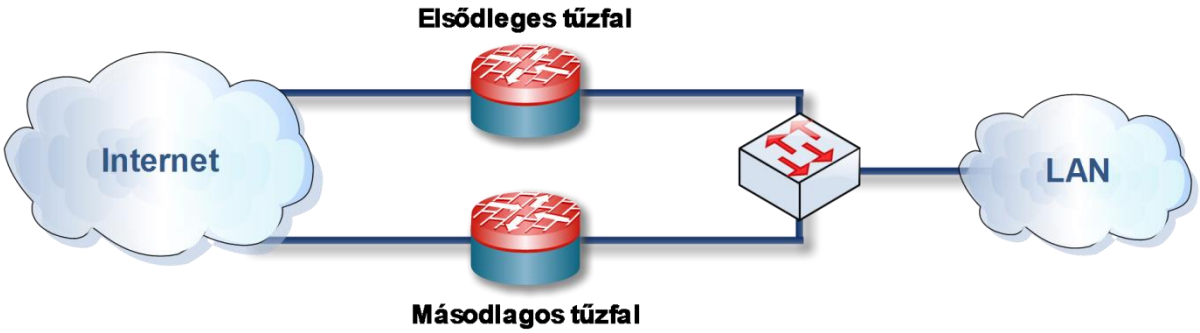
Kettős tűzfalról akkor beszélünk, ha külön tűzfal szűri a külső hálózat forgalmát, amelynek a belső hálózat felé néző hálózati interfésze egy demilitarizált zónához (DMZ) csatlakozik. A DMZ-ben található szerverek kommunikálhatnak külső hálózatokkal, megbíznak egymásban, a belső hálózat felé külön kapcsolattal rendelkeznek, valamint forgalmuk – a teljes befelé irányuló forgalommal együtt – áthalad egy belső tűzfalon, mely mögött húzódik a belső hálózat. Hátránya, hogy implementációja költségesebb, több tűzfal- és hálózati eszközt igényel. Fontos, hogy kettős tűzfal esetében két helyen kell a szabályrendszerünket felépíteni és karbantartani! Előnye, hogy a külső tűzfal kompromittálása csak az első védelmi vonal elestét jelenti, a rendszer-üzemeltetőnek detektálási lehetőséget és időt ad a támadás megállításához, a szükséges lépések megtételéhez. A támadó nem jut direkt hozzáféréshez a belső hálózat irányába, mivel a DMZ-ből csak erősen korlátozott kommunikáció indítható a belső hálózat irányába. A kettős tűzfal struktúrája a 16. ábrán látható.



16. ábra: Kettős tűzfal topológia

Tűzfalak tartalékolása, hibatűrő elosztott tűzfalak

A rendelkezésre állás növelhető, a szolgáltatás-kiesés pedig csökkenthető, amennyiben tartalék tűzfal(ak) áll(nak) folyamatos készenlétben. Olyan architektúra kialakítása szükséges, amelyben alapértelmezés szerint az elsődleges tűzfal üzemel, de ki van jelölve egy tartalék tűzfal. Ha az elsődleges eszköz meghibásodik vagy tervszerű karbantartáson megy keresztül, akkor a tartalék átveszi a szerepét. Nem állapottartó tűzfalaknál a váltás szinte észrevehetetlen lehet a kliensek szemszögéből. Viszont az állapottartó és proxy tűzfalak esetében ahhoz, hogy az átállás észrevehetetlen legyen, az állapottér folyamatos replikációja, az elsődleges eszközzel való szinkronban tartása lenne szükséges. A nagy hálózati átviteli sebesség, a kliensek nagy száma és a folyamatos kapcsolatnyitási és -lezárási kérések, a magas – akár több tízezer – másodpercenkénti áthaladó csomagszám miatt ez nem kis feladat, implementációja nem triviális, és nagy körültekintést igényel, ezért a legtöbb megvalósítás ezt nem foglalja magába.



17. ábra: Tartalékolt tűzfal topológia

Léteznek megoldások klaszterezett tűzfalakra is, ahol nem egy, hanem több, erre a célra dedikált tűzfal végzi a munkát. A klaszter egy tagjának kiesése esetén a klaszter többi tagja megosztva veszi át a szerepét. Implementációja költséges, csak nagy szervezeteknél használatosak. A tartalékolt tűzfal topológia a 17. ábrán látható.

A tűzfalak ellenőrzése

Tűzfalépítés során kerül meghatározásra a házirend, amelyben megadott paraméterek alapján körültekintően kialakítjuk a szabályrendszerünket. Fontos, hogy ne fogadjuk el ellenőrzés nélkül, hogy a kigondolt logika pontosan fedi a megálmodott házirendet! Munkánkat mindig egészítsük ki ellenőrzésekkel! Vizsgáljuk meg, hogy adott kliens eléri-e a számára szükséges hálózati erőforrásokat, és csakis kizárólag azokat! Ugyanígy ellenőrizzük a szervereknél is, hogy szolgáltatásaik csak a meghatározott kliensek számára elérhetőek! A vizsgálatokhoz az egyszerű kapcsolódási tesztek mellett számtalan ingyenes és fizetős eszköz érhető el. A kapcsolódási teszt egyik legegyszerűbb módjához mindössze egy telnet kliens szükséges. Egy webszerver elérése például szinte bármely operációs rendszer alól tesztelhető a telnet www.example.com 80 parancs kiadásával. Ha a szolgáltatás elérhető, akkor sikeres TCP kapcsolat épül fel a kliens és a szerver között. Ha a szolgáltatást blokkolja a tűzfal, akkor a kapcsolódási kísérlet sikertelen lesz (pl.: időtúllépés miatt).

Ha kíváncsiak vagyunk, hogy egy szerver milyen szolgáltatásai érhetőek el adott gépről, akkor a kliens gépen használhatjuk az ingyenes Nmap programot, amely többek között portszkennelést tesz lehetővé. Képes nem csak a nyitott, de a szűrt – csak bizonyos irányból elérhető – portokat is felderíteni, valamint a kapott válaszcsomagok mintázata alapján megállapítani a vizsgált cél operációs rendszerét. A szoftverrel feltérképezhetők a hálózatban található gépek is. Fontos a körültekintő használat, tanácsos csak saját hálózatunk ellenőrzésére használni, hiszen a portszkennelés sok helyen tiltott tevékenységnek és automatikusan támadásnak minősül!

Hasznos és ingyenes eszköz a Wireshark is. Létezik konzolos és grafikus felülete is, így alkalmazható szervereken és munkaállomásokon egyaránt. A Wireshark a kijelölt hálózati interfész teljes forgalmához hozzáfér, ennek eléréséhez rendszergazdai jogosultsággal kell futtatni. Képes a csomagokat elfogni, azokat elmenteni, fejlécüket és adatrészüket egyaránt elemezni, ismert protokollok esetén a szabályos működést ellenőrizni, teljes analizálást végezni. Az így kapott információk birtokában a rendszergazda képes lehet hálózati kommunikációs hibák felderítésére és megoldási terv kidolgozására.

A hálózati forgalmi adatok és a hálózati hozzáférés auditálása

Előfordulhat, hogy egy támadást már csak akkor veszünk észre, ha már sikeresen lezajlott. Megtörténhet az is, hogy egy rosszhiszemű alkalmazott a biztonsági házirendet meg nem sértve adatokat szivárogtat ki harmadik fél számára. De adatszivárgás előfordulhat akaratlanul is, például kémprogrammal fertőzött gépekről. Az sem ritka, hogy egy oktatási intézmény a hallgatói számára publikus Wi-Fi hozzáférést biztosít, amely esetben a hálózat használata a nap bármely szakában történhet, időtartama eltérő lehet. Ugyanakkor az intézmény elvárja a hallgatóktól, hogy betartsák a házirendet és a hatályos jogszabályokat, törvényeket.

Ezekből az életszerű szituációkból is látszik, hogy a legrészletesebb házirend kidolgozása esetén is történhetnek biztonsági incidensek, vagy kaphat értesítést az intézmény, hogy hálózatából jog- vagy törvénysértő tartalmat tettek közzé (pl.: webes feltöltő űrlap vagy FTP használatával). A hálózat üzemeltetőjének ilyenkor szüksége lenne arra, hogy vissza tudja keresni, mi történt egy adott időszakban a hálózaton. Ezért fontos, hogy minden szerverszolgáltatás naplózva legyen az alkalmazási rétegben. Ha egy szervezet tagjai számára lehetséges a világhálón történő böngészés, akkor webforgalmukat csak a szervezet webproxy eszközén keresztül engedélyezzük, közvetlenül ne érhessenek el külső webszervereket! Az SMTP szerver is jegyezze fel a pontos levélmozgásokat mindkét irányban, levelet küldeni és fogadni csak a kijelölt SMTP szerveren keresztül lehessen! A DNS szerver is rögzítse a feloldási kéréseket! A belső hálózat állandó gépei előre kialakított címzési logika alapján kapjanak IP-címet a szervezet DHCP szerverétől! Az időszakosan megjelenő (pl.: az előbb említett hallgatói) gépek kerüljenek külön hálózatba, mivel nem számítanak megbízhatónak, nincs közvetlen kontroll felettük! Legalább a határ-útválasztó jegyezze fel az összes hálózati kapcsolatot! Egy incidens okainak feltárása és a lezajlás pontos menetének kielemzése akkor lehetséges, ha rendelkezünk megfelelő adathalmazzal a vizsgált időszakról. Ehhez nyújt kiváló segédeszközt a Netflow.

Netflow a hálózati audit segítésére

A Netflow eredetileg egy olyan szoftveres eszköz, amelyet a Cisco fejlesztett ki, de ma már a legtöbb neves gyártó útválasztói és hálózati kapcsolóeszközei ismerik, emellett elérhető Linux, BSD, VMware vSphere 5 rendszerekre is. A Netflow jelenleg használatos verziói már ipari szabvánnyá váltak, működésük többek közt RFC dokumentumokban rögzített irányelvek alapján valósul meg. A Netflow rendszer három részre tagolódik:

- A Netflow Exporter az útválasztóban vagy hálózati kapcsolóban megvalósított adatszolgáltató szoftverkomponens, ami a hálózati folyamokról gyűjt adatokat. Jegyzi a forrás- és célcímeket, forrás- és célportot, protokollt, átvitt adatmennyiséget a kijelölt hálózati interfészen. A Netflow Exporter a beállított időérték leteltével vagy a hálózati folyam befejeztével küldi tovább az adatokat.
- A Netflow Collector veszi át az adatokat a Netflow Exporter-től, majd letárolja megfelelő rekordszerkezetet használva a háttértáron. Általában pár percenként új állományt nyit, mivel kisebb állományokban gyorsabban lehet keresni a későbbiekben.
- A Netflow Analyzer – kérésünkre – kiolvassa a letárolt rekordokat, és megjeleníti a vizsgált hálózati folyamokról kapott adatokat. Így az elemzést végző rendszergazda lekérdezéseket intézhet bármely tárolt paraméterre vonatkozóan, de visszakövetheti egy adott időszak

hálózati történéseit is. Az elemzés időben bármikor történhet, amíg a gyűjtött adatokat megőrizzük.

Fontos látni a hármas tagolás előnyeit, hiszen ennek köszönhetően:

- Az adatgyűjtés kis erőforrásigénnyel megvalósítható nagy forgalmú és nagy sávszélességű kapcsolatokon.
- Az adatok tárolásáról külső tároló gondoskodik, például egy Linuxot futtató PC, így nagy mennyiségű adat olcsón tárolható, az adatok több hónapra visszamenőleg is megőrizhetők, nem a hálózati forgalmat bonyolító eszköz erősen véges memóriaterülete határozza meg a megőrzött adatok mennyiségét.
- Az elemzés a tárolt adatokon végezhetők, nem kell előre meghatározni, hogy mire leszünk kíváncsiak a későbbiekben. Szabadon elemezhetjük a rendelkezésre álló adatokat, ugyanakkor lehetőség van időzített jelentések generálására is.

A Netflow Analyzer kimenete nfdump használatával (példa):

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2012-07-01 16:40:18.941	1.121	TCP	195.39.12.117:80	->	172.21.3.8:49156	3	132	1
2012-07-01 16:40:18.676	0.000	UDP	172.21.3.8:58418	->	193.6.33.2:53	2	122	1
2012-07-01 16:40:18.915	0.000	UDP	193.6.33.2:53	->	172.21.3.8:58418	2	352	1
2012-07-01 16:40:18.941	1.122	TCP	172.21.3.8:49156	->	195.39.12.117:80	5	467	1
2012-07-01 16:40:18.340	0.000	ICMP	172.21.0.1:0	->	172.21.3.8:8.0	1	48	1
2012-07-01 16:40:22.874	1.442	TCP	149.7.241.118:80	->	172.21.3.8:49159	3	132	1
2012-07-01 16:40:22.873	1.444	TCP	172.21.3.8:49159	->	149.7.241.118:80	5	471	1
2012-07-01 16:40:23.713	1.486	TCP	172.21.3.8:49160	->	149.7.241.118:80	5	446	1
2012-07-01 16:40:23.713	1.482	TCP	149.7.241.118:80	->	172.21.3.8:49160	3	132	1

Támadás bármikor érheti a hálózatot. A biztonsági felkészültség szinten tartásához fontos alkalmazni a már rendelkezésre álló biztonsági, naplózási és auditsegítő tehcnológiákat. De ne feledjük el, hogy gyors és robbanásszerű fejlődésen megy keresztül az informatika, ezért nem elég, ha a hálózat biztonsági struktúrája egy adott technológiai fejlettséghez és felhasználói szokásokhoz kerül kidolgozásra. A házirendeket, szabályrendszereket, az alkalmazott IDS és IPS rendszereket folyamatosan hozzá kell igazítani a változó körülményekhez!

4. Vezeték nélküli hálózatok biztonsága

A vezeték nélküli hálózati kommunikációt a vezetékes kommunikáció kiegészítésére kezdték el kidolgozni. Tervezői nem számítottak akkora térhódításra, mint amit elért napjainkra. Kisegítő alternatívának szánták olyan szituációkra, amikor a vezetékes hálózat kiépítése nem volt lehetséges, vagy csak ad-hoc, ideiglenes hálózati hozzáférésre volt szükség. A kezdeti elgondolások nyújtotta szolgáltatási szint hamar szűkösnek bizonyult. Nem csak otthoni környezetben, de nagyvállalati szinten is egyre nagyobb piaci részesedésre tett szert. Kényelmes, gyorsan implementálható hálózati megoldássá, széles körben elterjedt kommunikációs eszközzé vált. A népszerűség és a vállalatok részéről érkező elvárások arra késztették a technológiai újítókat, hogy a vezeték nélküli kommunikációt több lépcsőben fejlesszék. Nézzük végig ezeket az állomásokat a biztonság oldaláról, kezdve a technológia alapjainak rövid áttekintésével!

Betekintés a vezeték nélküli technológia alapjaiba

Ugyan az első próbálkozások 1979-ben indultak infravörös fény alkalmazásával, rövidesen kézenfekvővé vált, hogy az átviteli közeget érdemes levegőben terjedő rádióhullámokra cserélni. Hosszabb előkészítő munka után 1997-ben szabványosította az IEEE (Institute of Electrical and Electronics Engineers) szervezet a 802.11 nevű szabványban azt a fajta vezeték nélküli, rádióhullámokkal működő kommunikációs technológiát, ami napjainkra meghódította a világot, később több utódszabvány követte. A szabványokban közös, hogy mindegyik 802.11 elnevezéssel kezdődik, de kiegészül különböző betűjelölésekkel, így például a kezdeti szabványt követte az IEEE 802.11a, majd az IEEE 802.11b, IEEE 802.11g, és jelenleg az IEEE 802.11n a manapság kapható legfejlettebb megoldás.

Kik kommunikálnak?

Több felállást tesz lehetővé a technológia. Az architektúra építőkövei az állomások. Azokat az eszközöket nevezzük állomásnak, melyek részt vesznek a kommunikációban, rendelkeznek megfelelő rádiós adóvevő komponenssel. Állomás lehet egy vezeték nélküli hálózati kártyával rendelkező munkaállomás vagy laptop, illetve a vezetékes hálózat oldaláról nézve tipikus összekötő elem: a vezeték nélküli hozzáférési pont (AP, Access Point). Manapság elterjedtek már az okostelefonok, tabletek, melyek ugyancsak rendelkeznek a megfelelő képességekkel, hogy egy vezeték nélküli hálózatban állomások lehessenek.

Azon eszközök kommunikálhatnak egymással, akik azonos csatornán tartózkodnak. Ezen eszközök gyűjtőneve a Basic Service Set (BSS). A kommunikáció rögzített protokollt követve zajlik.

Rádióhullámok és az interferencia

A kijelölt frekvenciatartomány a 2.4GHz volt kezdetekben. Az IEEE 802.11n hozott változást ebben, hiszen ez a szabvány megengedi már a 2.4GHz mellett az 5GHz-es tartomány használatát is 20, illetve 40MHz széles csatornákkal.

Fizikai tanulmányainkból ismerős lehet, hogy azonos frekvenciájú rádióhullámok találkozásakor a hullámok csillapíthatják, erősíthetik vagy teljesen kiolthatják egymást. Ezt nevezzük interferenciának. Ez nyilván nem kívánatos jelenség esetünkben. Az interferencia minimalizálása érdekében 20MHz-es csatornákat alakítottak ki. Az Európában érvényes szabályozások szerint 11 darab csatorna áll

rendelkezésre 2.4GHz-en és lényegesen több 5GHz-en, de ez utóbbi tartományban országonként változik a használható csatornák száma.

Ha egy időben több állomás ad, akkor fellép az interferencia jelensége. A küldött csomag sérülhet, nem jut célba, újraküldése szükséges, ami erősen degradálja a hálózat teljesítményét. Ennek csökkentésére a közös osztott közegben időosztásos átviteli technikákat alkalmaznak. De a jelenséget így sem lehet teljesen elkerülni. Mivel azonos földrajzi helyen több, egymástól független hálózat is üzemelhet. Előfordulhat, hogy egymás hatósugarán belül találhatók olyan hálózatok, amelyek azonos csatornán üzemelnek, viszont egymás forgalmát szabályozni nem tudják. Törvényi előírások szerint a vezeték nélküli rádióadók legfeljebb 100mW teljesítménnyel sugározhatnak, hogy a hálózati frekvenciaátlapolódás kisebb területen léphessen fel. Tanácsos telepítés előtt feltérképezni, hogy mely csatornák foglaltak, és a saját hozzáférési pontokat olyan frekvenciára hangolni, amelyen a legkevesebb hálózat „érzékelhető”.

Azt azonban fontos megjegyezni, hogy egy esetlegesen szabad csatorna sem garantálja a zavartalan működést. Egyrészt az elterjedtség miatt bármikor megjelenhetnek új állomások az addig szabad csatornán, másrészt a 2.4GHz-es frekvenciatartományt használja a Bluetooth is, valamint számos háztartási gép (pl.: mikrohullámú sütő) is itt kelt hullámokat. Ezért ha az eszközök támogatják és lehetőség van rá, javasolt az 5GHz-es tartomány használata.

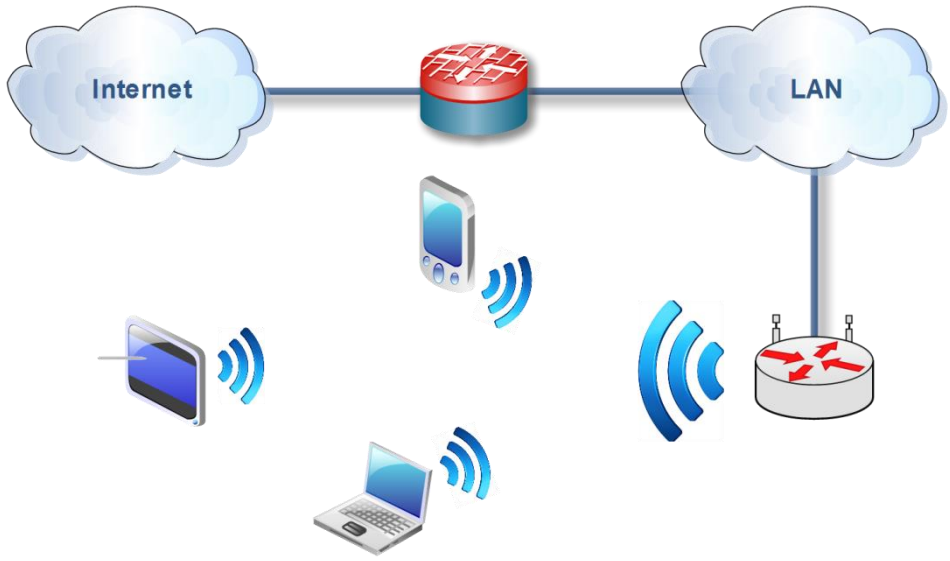
Látható, hogy már az átviteli közeg is számtalan lehetőséget ad a vezeték nélküli hálózat zavarására. A támadó érkezhet olyan eszközzel, ami folyamatosan zavaró jelet sugároz a megfelelő frekvencián, ezzel használhatatlanná téve a hálózatot. Továbbá érkezhet adatgyűjtési szándékkal, hiszen a csomagok a levegőben terjednek, a rádióadók pedig körsugárzó antennával rendelkeznek, így a tér minden irányába indulnak rádióhullámok. A támadónak nincs más dolga, mint elhelyezni eszközét a hatósugáron belül, és lehallgatni a forgalmat.

Topológiák

Alapvetően két topológia létezik: ad-hoc és infrastruktúra kialakítás. Ad-hoc hálózatról akkor beszélünk, amikor az állomások halmazában nem található AP. A kommunikációs partnerek pont-pont kapcsolatokat építenek fel szomszédjaikkal. Ez a topológia tartalmazhat mindössze két állomást, de megengedett több állomás csatlakoztatása is, a felek saját pont-pont kapcsolatot alakítanak ki a közelükben levő résztvevőkkel, a hálózat további tagjait a szomszédokon keresztül éri el. Az ad-hoc vezeték nélküli hálózatok működését a 18. ábra szemlélteti.

18. ábra: Ad-hoc vezeték nélküli hálózati topológia

Az infrastruktúra mód használatához szükséges legalább egy AP, ami egy szöveges hálózati azonosítót hirdet saját interfészének MAC-címével együtt. Az állomások az AP-hez csatlakoznak egy társítási folyamat keretén belül, melynek során egyeztetik a hálózat paramétereit, felépítik munkamenetüket. A hálózat bármely két állomása közti kommunikáció az AP eszközön keresztül történik. Jellemzően az AP kapcsolódik a vezetékes hálózathoz, így kapcsolja össze a vezeték nélküli eszközöket a vezetékes belső hálózattal, illetve az internettel. De nem csupán ez az előnye az AP-k alkalmazásának. Fontos szempont lehet az is, hogy egy AP-hez nem csak azonos szabványt támogató állomások csatlakozhatnak, hanem egyszerre asszociálhatnak a 802.11b, illetve a 802.11g szabványt támogató eszközök is. Az infrastruktúra mód működését a 19. ábra illusztrálja.



19. ábra: Infrastruktúra módban működő vezeték nélküli hálózat

Az infrastruktúra mód egy kiterjesztése a központilag felügyelt vezeték nélküli hálózat, amely kétféle komponensből áll: pehelysúlyú hozzáférési pontok (LWAP, Lightweight Access Point) csoportjából és egy központi irányítóeszközből, a kontrollerből.

Pehelysúlyú hozzáférési pont

A pehelysúlyú hozzáférési pontra jellemző, hogy nem képes önállóan működni, beüzemelése két módon történhet. Az egyik esetben a hálózat üzemeltetője az alapkonfiguráció részeként beállítja vezetékes interfészét, valamint hogy milyen címen és paraméterekkel fér hozzá a kontrollerhez. A másik esetben az eszközt a rendszergazda csatlakoztatja a hálózathoz, az DHCP protokollon keresztül megkapja a hálózati beállításokat és opcionálisan a kontroller fellelhetőségét, esetleg azonos szórási tartományon belül felderíti azt.

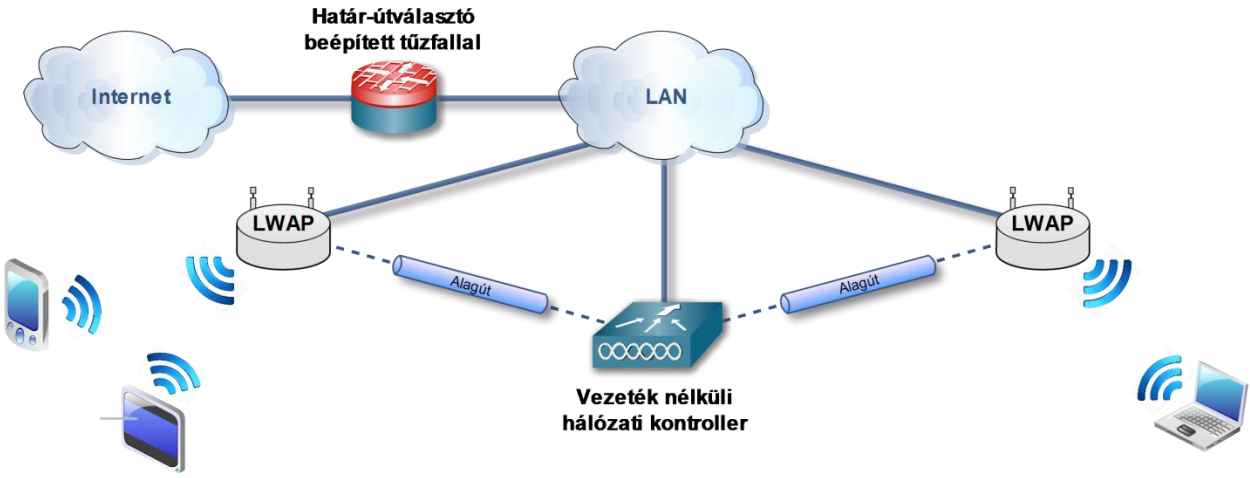
Mindkét esetben a hozzáférési pont kapcsolatot kezdeményez a kontroller irányába, amely egy titkosított alagutat hoz létre a két eszköz között. Az AP és a kontroller közti teljes hálózati kommunikáció ezután az alagúton keresztül történik.

A kontroller

A kontroller a központi vezérlőeszköz. A rendszergazda ezen konfigurálja fel a kialakítandó vezeték nélküli hálózatokat. A pehelysúlyú hozzáférési pontok a kontrollertől kapják meg a konfigurációs állományt, amely az összes, eszközre szabott beállítást tartalmazza. Átjárót valósít meg a vezetékes és a vezeték nélküli hálózatok közt. A forgalom nem a hozzáférési pontokon lép ki a belső hálózatba, hanem az alagúton keresztül továbbítódik a kontrollerig. Az architektúra lehetővé teszi, hogy hozzáférési szabályozást alakítsunk ki ezen a ponton.

Azon túlmenően, hogy egy helyen, egy felületen látható mindegyik eszköz, lekérdezhetővé válik az állapotuk és a hozzájuk csatlakoztatott kliensek, firmware frissítés indítható, naplózásra kerülhetnek központilag a kliensek forgalmi adatai vagy a kliensek vándorlása (roaming). Algoritmizálható az AP-k

adóteljesítményének automatikus állítása és csatornaválasztása. A központilag felügyelt vezeték nélküli hálózat működése a 20. ábrán látható.



20. ábra: Központilag felügyelt vezeték nélküli hálózat

Roaming, az állomások vándorlása

Roamingnak azt nevezzük, amikor egy állomás az AP hatósugarának széléhez érve lecsatlakozik a hálózatról, majd a társítási folyamat keretében csatlakozik egy másik, erősebb jelerősséggel rendelkező AP-hoz, azaz egyik AP-ról átvándorol egy másikra. Központosított rendszer esetén ez a váltás milliszekundumok alatt lezajlódik. A kliens megtartja hálózati konfigurációját, nem szakadnak meg a hálózati kapcsolatai. A váltás gyorsasága különösen a hang- és video-átviteli alkalmazásoknál rendkívül lényeges.

A vezeték nélküli hálózat forgalmának titkosítása

Kezdetekben a vezeték nélküli forgalom titkosítás nélkül haladt az állomások között, melynek következtében a forgalom viszonylag egyszerűen lehallgathatóvá vált. Az adatátvitel nem volt védett a visszajátszásos vagy beékelődéses támadásokkal szemben. Nem állt rendelkezésre olyan mechanizmus, amivel a fogadó fél ellenőrizhette volna, hogy egy csomag adatrésze sértetlen és hiteles. Ez komoly gátat szabott annak, hogy a technológiát olyan környezetben alkalmazzák, ahol fontos az adatok biztonságos továbbítása. A mérnökök első válasza a felmerülő problémára a WEP titkosítási eljárás volt.

WEP

A WEP (Wired Equivalent Privacy) egy titkosítási eljárás, amely a hálózati forgalom biztonságos átvitelét két függvénnyel biztosítja:

- Az RC4 folyamtitkosító (stream cipher) függvény felel a csomagok bizalmas kezeléséért.
- A CRC-32 (Cyclic Redundancy Check) ellenőrzőösszeg-generáló függvény pedig a csomagok sértetlenségét ellenőrzi.

A WEP leírását tartalmazza az első 802.11 szabvány, ami 64 bit hosszú kulcs alkalmazását teszi lehetővé. A 64 bit hosszú kulcs két részből tevődik össze. Egy 40 bit hosszúságú kulcsból, ami tetszőleges karakterlánc lehet, és mi határozzuk meg. Ezt hagyományosan „jelszónak" nevezzük. A másik komponens egy 24 bit hosszúságú inicializáló vektorból áll. Az így kapott kulcsot használja fel az RC4 a kulcsfolyam (key stream) előállításához. A kulcsfolyam és a titkosítani kívánt adatfolyam között bitenként elvégzi a XOR logikai műveletet, így áll elő a WEP által titkosított folyam.

Későbbi törvényi változások lehetővé tették 128 bit hosszúságú kulcsok alkalmazását, ahol a 104 bit hosszúságú „jelszó" mellett 24 bit hosszúságú maradt az inicializáló vektor.

Az alkalmazott RC4 folyamtitkosító függvény rendkívül gyors. Viszont a 64, illetve 128 bit hosszúságú kulcsok alkalmazása, valamint a megkötés, hogy a 40, illetve 104 bit hosszúságú kulcsrész csak az [A-Za-z], valamint [0-9] karakterosztályokból állhatott elő, beszűkíti a generálható kulcsok terét.

Nem kellett sokat várni, és megjelentek az első eljárások a WEP titkosítás feltörésére. Nagyságrendileg elegendő 40-60000 csomag elfogása a kulcs visszafejtéséhez. Ekkora csomagmennyiség percek alatt összegyűjthető, főleg, hogy a vezeték nélküli hálózat protokollja kijátszható, könnyen generálható hálózati forgalom. Ennek következtében a WEP bármely kereskedelmi forgalomban kapható vezeték nélküli hálózati kártya és megfelelő, szabadon elérhető szoftver felhasználásával pár perc alatt feltörhető, az általa védett hálózathoz illetéktelen hozzáférés szerezhető. Épp ezért a WEP használata erősen nem javasolt!

WPA és WPA2

A WPA (Wi-Fi Protected Access) és a WPA2 (Wi-Fi Protected Access II) kívánt megoldást nyújtani a WEP gyengeségeire, ezek kidolgozását a „The Wi-Fi Alliance" vállalta fel.

A WPA áthidaló megoldást nyújtott, hiszen az eszközök felkészíthetőek voltak az új eljárás használatára egy firmware frissítés elvégzésével. A WPA2 alkalmazásához már a rádióeszközök hardverfelépítésén is változtatni kellett.

A WPA az IEEE 802.11i szabvány egy részét valósítja meg, különösképp a TKIP (Temporal Key Integrity Protocol) eljárást. A munkamenetenként statikus WEP kulccsal szemben a TKIP csomagonként generál egy 128 bit hosszúságú titkosítási kulcsot a kulcsfolyam legenerálásához.

A csomagok integritás-ellenőrzésében is történt változtatás, a CRC szerepét a Michael algoritmus vette át, amely sokkal nehezebben kijátszható ellenőrzőösszeget adott, viszont erőforrásigényét kielégítették a piacon akkoriban forgalomban levő vezeték nélküli hálózati kártyák.

A WPA2 újabb algoritmusokat alkalmaz. A csomagok titkosításához és hitelesítéséhez az AES (Advanced Encryption Standard) eljárásra épülő CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) algoritmust alkalmazza. A kereskedelmi termékek mégsem a CCMP megnevezést használják a konfigurációs felületen, hanem az AES megnevezést.

Előre kiosztott kulcsok, WPA-PSK mód

A WPA-PSK (WPA Pre-Shared Key) a WPA, illetve a WPA2 azon működési módja, amikor a kulcs előállításához tetszőleges ASCII karaktereket tartalmazó saját „jelszót” használunk. Ezt a módot WPA-Personal néven is ismerhetjük. Otthoni, kisvállalati telepítések során ez a legszélesebb körben alkalmazott működési mód.

WPA-802.1x mód

A WPA-802.1x mód lehetővé teszi, hogy központi RADIUS hitelesítési szerveren keresztül történjen a kliensek azonosítása. A 802.1x egy olyan folyamat, amelynek során a sikeres azonosítás előtt kizárólag hitelesítési keretek utazhatnak az Ethernet hálózaton. A keretek csak az azonosítandó eszköz és az azonosítást elvégző hálózati eszköz között közlekedhetnek. A központi adatbázisból történő lekérdezést az azonosítást végző eszköz hajtja végre, RADIUS protokollon keresztül.

Mit tanácsos, és mi nem tanácsos?

- Soha ne építsünk olyan vezeték nélküli hálózatot, ami nem védett legalább WPA2-PSK titkosítási móddal.
- Nem tanácsos olyan hálózathoz csatlakozni, ami nem használ titkosítást. Ha mégis elkerülhetetlen, akkor olyan alkalmazások használata javasolt, amik alkalmazási (L7) rétegben gondoskodnak a biztonságos kommunikációról (pl. HTTPS, SSH, IMAPS).
- WEP titkosítást nem tanácsos alkalmazni, mert csak látszólagos biztonságérzetet kelt.
- A vezeték nélküli hálózat olyan csatornán üzemeljen, amelyen a legkevesebb a zavaró jel.
- Törekedni kell az 5GHz frekvenciasáv használatára, amennyiben a csatlakoztatni kívánt eszközök erre felkészítettek.

Bár számos helyen keletkezhet támadási felület a vezeték nélküli hálózatokban, gondos tervezés és körültekintő implementálás esetén a hálózat biztonsággal használható és üzemeltethető. Mégis a rendszer üzemeltetőjének fel kell készülnie arra is, hogy a hálózatot támadás éri, ezért itt is fontos szerepet kap a hálózat naplózása és az audit. Biztonsági kérdésekben a [11] könyv adhat további ismeretanyagot.

5. Irodalomjegyzék

[1] Andrew S. Tanenbaum: Számítógép-hálózatok, Panem Kiadó, 2004.

[2] Ryan Trost: Practical Intrusion Analysis (Prevention and Detection for the Twenty-First Century), Addison-Wesley, 2009.

[3] Stephen Northcutt , Judy Novak: Network Intrusion Detection (3rd Edition), New Riders, 2002.

[4] Matt Fearnow , Stephen Northcutt , Karen Frederick , Mark Cooper: Intrusion Signatures and Analysis, New Riders, 2001.

[5] Niels Provos, Thorsten Holtz: Virtual Honeypots (From Botnet Tracking to Intrusion Detection), Addison-Wesley, 2007.

[6] Jon C. Snader: VPNs Illustrated (Tunnels, VPNs, and IPsec), Addison-Wesley, 2005

[7] J. Michael Stewart: Network Security, Firewalls, and VPNs, Jones & Bartlett Learning, 2010.

[8] Greg Holden: Guide to Firewalls and Network Security (Intrusion Detection and VPNs), Course Technology, 2003.

[9] Michael E. Whitman, Herbert J. Mattord, Andrew Green: Guide to Firewalls and VPNs, Delmar Cengage Learning, 2011.

[10] Oleg Kolesnikov, Brian Hatch: Building Linux Virtual Private Networks (VPNs), Sams, 2002.

[11] John R. Vacca: Guide to Wireless Network Security, Springer, 2006.