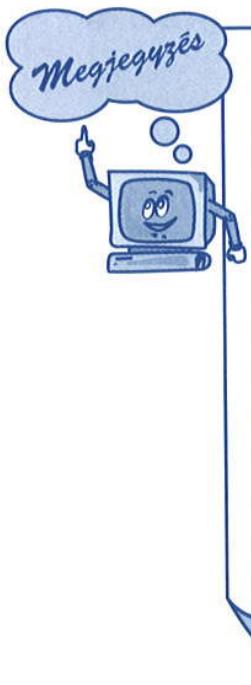


Amint a csatlakozók száma növekszik, amihez még a felhasználók egyre nagyobb utazási kedve is társul, a különböző szolgáltatásokat nyújtó hálózatok iránti igény is egyre nagyobb. A felhasználók jellemzően nincsenek tisztában az általuk a nagyobb hatékonyság érdekében megkövetelt helyfüggetlen távoli szolgáltatások biztonsági problémáival. A más országokba utazó felhasználók a repülőtereken, de a vásárlóik telephelyén is megkövetelik, hogy munkájuk hatékonyabb végzése érdekében képesek legyenek hozzáérni a vállalati erőforrásokhoz. A repülőtereken egyre nagyobb számban elérhető kábeles és vezeték nélküli hozzáérések, a Wi-Fi pontok és a nagy sebességű kapcsolattal rendelkező felhasználók számának növekedésével a hálózatok karbantartásáért felelős szakemberek számos nehéz döntési helyzettel szembesülnek. Miként biztosíthatják a felhasználók által megkövetelt szolgáltatásokat biztonságos és ésszerű módon úgy, hogy azok függetlenek legyenek az elérés földrajzi helyétől?

A technológia természetesen követi a kívánalmakat, és a fenti követelések kielégítésére létrejött az Internet Protokoll Biztonságos Protokollja (*IPSec – Internet Protocol Security Protocol*) segítségével titkosított **virtuális magánhálózat** (*VPN – Virtual Private Network*). Időnként előfordul, hogy egy technológia neve tükrözi a tényleges funkcióját, s ez a VPN esetén is így van.



Az USA Nemzeti Szabvány- és Technológiaügyi Hivatala (NIST – National Institute of Standards and Technology) létrehozta az AES-t, amit az új szövetségi információfeldolgozási szabvány (FIPS – Federal Information Processing Standard) rögzít mint titkosítási módszert. Az AES az IPSec és az internetes kulcs-csere (IKE – Internet Key Exchange) titkosítása, amely a korábbi adattitkosítás szabvány (DES – Data Encryption Standard) lecserélésere lett létrehozva. Az AES sokkal biztonságosabb a DES-nél: [http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\\_feature\\_guide0918-6a0080110bb6.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide0918-6a0080110bb6.html)

Az NIST várta az AES végső elfogadását, amit 2003 végén az USA Védelmi Minisztériuma végül meg is adott. Ennek hatására a közeljövőben az AES-sel valószínűleg egyre többet találkozhatunk majd.

Ebben a fejezetben a VPN használatával ismerkedünk meg: hogyan működik, milyen titkosítást nyújt az IPSec és miként lehet ezen technológiák segítségével fenntartani a hálózat biztonságát, miközben megnövelt szolgáltatásokat nyújthatunk a felhasználók számára. Mindenkinek vannak felhasználói, akiknek bizonyos mértékű szolgáltatást kell nyújtaní, függetlenül az adott területtől. A VPN esetén a felhasználót úgy defi-

niálhatjuk, mint azon személyt, akinek biztonságosan hozzá kell férnie a vállalati hálózat bizonyos erőforrásaihoz. Lehetnek mozgó felhasználók (ügynökök, rendszermérnökök), vezetőségi tagok, akik a vállalat ügyeit intézik, kiemelt felhasználók, akik bármikor csatlakozhatnak, vagy üzleti partnerek, akik fontos információkat kapnak vagy adnak. Az *erőforrások* a fenti értelemben olyan eszközök lehetnek, amelyek nem közvetlenül csatlakoznak az internethez; ilyenek lehetnek állomány- és levelezőszerverek vagy hálózati eszközök.

Manapság a biztonság témakörében a legnagyobb figyelem a VPN-t övezi, amelyek az alacsony költséget, megnövelt méretezhetőséget és alkalmazhatóságot ígérik az üzlet számára, miközben biztosítják a kommunikáció biztonságát is.

### Megjegyzés



*A Gartner Dataquest technológiai iparkutató vállalat 2002 májusában jelentette be, hogy „a bizonyított IP VPN implementációknak 2006-ra a feltételezett piaci volumene a 4,7 milliárd dollárt is meg fogja haladni.” Ugyanez 2002-ben kissé 3 milliárd alatt volt, 2001-ben pedig még a kétnyolcadot sem érte el. Az ilyen nagyságú növekedés (45,7% 2001-ről 2002-re) magáért beszél, és jól mutatja a VPN mai piaci részesedését.*



Hogy pontosan mit is csinál a VPN, és milyen kihatással van az üzleti folyamatokra – csökkenti a költségeket, mérsékli a kockázatot és növeli a bevételt. A VPN népszerűsége közvetlenül visszavezethető a befektetés megtérülésére mutatott jelentős kihatására. A vállalkozások gyakran hihetetlen összegeket fizetnek ki a bérelt vonalakon vagy átjátszókon keresztül megvalósított privát kapcsolatokért, így az ezeket helyettesítő VPN bevezetésével jelentős megtakarítás érhető el. Jobban megérthetjük, hogy milyen értéke van a VPN-nek a vállalkozás szempontjából, ha megvizsgáljuk az általa kiváltott más technológiákat:

- A telephelyközi VPN helyettesítheti a költséges nagy kiterjedésű hálózati (WAN) eszközöket, a magánvonali szolgáltatások helyett az internet használva az összeköttetésre.
- A távoli elérésű VPN megszünteti a távolsági hívásokkal elért modernes kapcsolatokat, amelyekkel korábban a kihelyezett irodák vagy elárusítóhelyek csatlakoztak a vállalathoz.

Amennyiben a vállalatunknak ismétlődő költségei vannak akár a WAN telekommunikációs vonalak, akár a távolsági hívások díjai miatt, akkor

a VPN alternatív megoldást kínálhat ezek helyett, miközben a költségek csökkentésén kívül még növeli a rugalmasságot is.

Mielőtt megkezdenénk a VPN telepítési lehetőségeinek és az ehhez szükséges alkotóelemek vizsgálatát, fontos megismerni a VPN-elv lényegét. Ezt hasonlatok segítségével próbáljuk meg bemutatni, mivel a különböző előzetes elméleti tudással rendelkező olvasók így könnyebben értik meg ezt az összetett problémát.

## 7.1. A VPN A BIZTONSÁGOS ÖSSZEKÖTTETÉS

A hálózatok, vagyis a rendet, ésszerűséget és felhasználói szolgáltatásokat jelentő szigetek partjait verdesi az internet kiismerhetetlen óceánja. Tudjuk, hogy ezer más sziget is található benne. Amikor az egyik szigetről a másikra akarunk eljutni, egy kompra kell felugranunk, így érhetjük el például a másikon található webhelyeket.

Tehát az óceánon (internet) keresztül úszó kompon (TCP/IP) vagyunk, hogy elérjünk valamit egy másik szigeten (LAN), amely valamilyen szolgáltatást nyújthat (webhely). Ésszerűen hangzik, ugye? A kérdés az, hogy ugyanezen a kompon háyan utaznak még – csak néhányan, vagy esetleg több ezren? Az alapvető probléma az, hogy a szigetről szigetre utazás közben magánéletünk sincs, és biztonságról sem beszélhetünk; minden ember láthat minden, amit csak teszünk. Mármost ha csupán az index.hu oldal legfrissebb híreit olvasgatjuk, akkor egyáltalán nem zavaró, hogy mások is beleolvashatnak. Ha viszont a vállalatunk webhelyének egy privát zónájában található információkat kívánjuk látni, akkor a nyilvánosság már igencsak zavaró, sőt káros lehet.

Mivel az internetet alkotó világtengeren utazunk, így nincs befolyásunk arra, hogy az ezt alkotó mely kábeleken, útválasztókon vagy kapcsolókon haladunk keresztül. Semmiféle garanciával sem rendelkezünk: általában elérhetjük a más szervereken lévő webhelyeket, de nincs garancia az elérésükre. Ne feledjük, az internethez való csatlakozás nem jog, hanem kiválltság! Ha viszont nincs rá befolyásunk, akkor eleve gyanakvóan kell hozzáállnunk valamennyi biztonsági kérdéshez. Különösen így van ez akkor, ha két magánhálózatot akarok összekötni a nyilvános internetkapcsolaton kereszül.

A szigetek összekötéséért felelős személyként azt az utasítást kapjuk, hogy a saját szigetünket kössük össze egy újonnan megvásárolt másik szigettel. Elhatározzuk hát, hogy építünk egy hidat a két sziget között, amely az utazók számára egyszerűbb, biztonságosabb és közvetlen összekötést jelent. A híd megépítése és fenntartása rendkívül költséges, jóllehet



*Amikor egy megrendelőm hálózatát kellett felmérniem, meglepve tapasztaltam, hogy a négy telephely egyikén sincsenek tűzfalak beállítva, pedig mind a négy csatlakozott az internethöz. Önmagában ez a tény is meglehetősen komoly biztonsági kockázatot jelent, de igazán megrázó felismerésnek az bizonyult, hogy mindegyik helyen egy Microsoft-szerver volt úgy beállítva, hogy a többi helyen lévő szerverekkel bizalmi viszonyt épített ki – mindez a nyilvános interneten keresztül! Egy támadónak elegendő ezt a bizalmi viszonyt felderítenie, s ezzel márás feltörte az egész hálózatot! Valójában ez többször be is következett. Hitelenül ráztam a fejemet – soha ne engedje, hogy ugyanez önnel is megtörjenek! Használjon VPN-t!*

a két sziget nagyon közel van egymáshoz. A megbízható, biztonságos útra azonban olyan nagy szükség van, hogy mindenkiéppen megvalósítjuk azt.

Ez a helyzet hasonló ahhoz, amikor kiépítünk egy saját nagy kiterjedésű hálózatot (WAN). A hidakon (bérelt vagy saját kiépített vonalakon) zajló forgalom elkülönül az óceán (internet) forgalmától, mégis képesek a szigetek (LAN) összekötésére. Számos vállalat választotta ezt a megoldást, mivel a kihelyezett irodák és a központ között biztonságos és megbízható összeköttetést akartak.

Újabb igény merül fel: ezúttal azonban egy sokkal távolabbi szigettel kell összeköttetést teremteni. Alapos felmérés után kiderül, hogy a híd megépítésének költségei túlságosan nagyok lennének. Meg kell értenünk, hogy a távolabbi irodák esetén a költségek nagyon gyorsan növekedni kezdenek, akárcsak a nagy távolságot átívelő hidak esetén. Az összeköttetés iránti igény azonban továbbra is fennáll.



*Számos vállalat esetén megfigyelhető, hogy az IT vezéri a vállalkozás növekedését. Jóllehet ez a megközelítés néhány vállalatnak elfogadható, a legtöbb cég esetén azonban éppen fordítva kellene lennie – a vállalkozás növelésének kell vezérelnie az IT-infrastruktúra növekedését. Ez alapvető igazság, hiszen a vállalatok célja nem az, hogy nagyméretű IT-részleget vagy hálózatot növesszenek maguknak. Az e-vállalkozások nemrég bekövetkezett erőteljes visszaesése figyelmeztet bennünket arra, hogy a már bevált üzleti modellhez kell visszatérni.*

Kíváncsi lenne arra, hogy a VPN-re miként illik ez a hasonlat? Leszögeztük, hogy szükségünk van a biztonság növelésére, és az első lehetőség egy híd építése volt; ez azonban túlságosan drágának bizonyult. Másik le-

hetőséggént adhatnánk mindenkinék, aki a két sziget között kíván közlekedni, egy saját és biztonságos tengeralattjárót. Ez a tengeralattjáró meg lehetősen jól példázza a VPN-t, mivel mindenki rendelkezik az alábbi jellemzőkkel:

- nagyon gyorsak is lehetnek,
- könnyen rendelkezésünkre állnak,
- képesek mások elől elrejteni minket,
- az első üzembe helyezést követően a költségeik minimálisak,
- védelmeznek minket utazás közben.

Ehhez kapcsolódóan a VPN-piacon mostanában kezdenek megjelenni a VPN képességeivel is rendelkező kézi számítógépek (*PDA – Palmtop Digital Assistant*). Egyre több cég használja a technológiát, például a Cisco VoIP SoftPhone alkalmazása is kitűnően üzemel a VPN felett, a gépünket biztonságos telefonná alakítva.

Nem feltétlenül könnyű állandóan egy tengeralattjárót hordani magunkkal, mindenkorral a fenti hasonlat segít minket a megértésben. A VPN beüzemelésének számos különböző módszere van. A következőkben a három alapvető típust fogjuk megvizsgálni. Ugyancsak jó hasonlat lenne a csillagkapu-kikötő. A működéséhez rendelkezni kell a használat jogával, és a másik oldalon is lennie kell egy csillagkapu-kikötőnek, amelyen a hiperűr-csatorna végződik.

## 7.2. A VPN ÁTTEKINTÉSE

A virtuális magánhálózat (VPN) egy kódolt hálózati összeköttetés, amely az interneten, vagy más hálózaton (például WAN) keresztül biztonságos csatornával köti össze a végpontokat. A modemes behívócsatlakozások, illetve a bérelt vonalak helyett az internetszolgáltató, vagy más szolgáltató jelenléti helye (*POP – Point of Presence*) által biztosított helyi kapcsolatot használjuk. A távoli, kis irodákban és az otthonokban is megtalálható szélessávú internetkapcsolatok egyre növekvő száma az internetet az olcsóbb elérés miatt egyre vonzóbbá teszi. Amint arról már esett szó, a VPN kezdeti kiépítése után a helyek vagy felhasználók növelésének csak minimális költségvonzata van.

A VPN lehetővé teszi a hálózatunkhoz csatlakozó valamennyi felhasználó számára a belső hálózathoz való biztonságos és megbízható hozzáférést a nyilvános interneten keresztül. A VPN könnyebben méretezhető át több felhasználó vagy hely fogadására, mint a bérelt vonalak. Tüljönképpen a bérelt vonalakkal szembeni legnagyobb előny éppen az átméretezhetőség. Ráadásul a távolság növekedésével nem jár együtt az



Léteznek nem titkosított VPN-ek is, amelyek a biztonságot valamilyen más szinten zajló titkosítással vagy útválasztással kívánják megvalósítani. Ilyen például az MPLS VPN. Ezen VPN-ek csupán meglehetősen különleges esetekben alkalmasak a hálózathoz való távoli csatlakozásra. Az ajánlott gyakorlat mindenkorban az, hogy a VPN-en zajló forgalmat mindig kódoljuk. Ennek elmulasztása katasztrófához vezethet, és minden ezzel kapcsolatos vagy ebből fakadó felelősséget a mi vállunkon fog nyugodni.

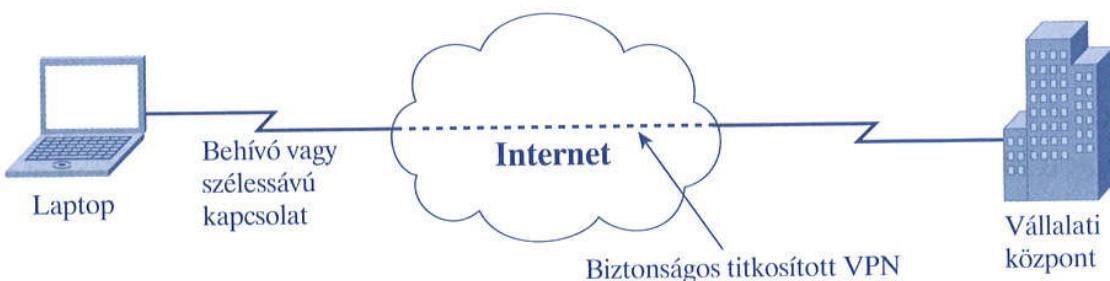
üzemeltetési költség drámai növekedése sem, mint a bérelt vonalak esetén járna.

A VPN lehetővé teszi, hogy a belső intranetet az IPSec-kódolás felhasználásával a nyilvános interneten vagy más hálózati szolgáltatáson keresztül biztonságosan kiterjessük, biztonságos e-kereskedelmet és extranet lehetőséget valósítva meg az utazó ügynökök, üzleti partnerek, beszállítók és felhasználók számára. A VPN alábbi három típusa létezik:

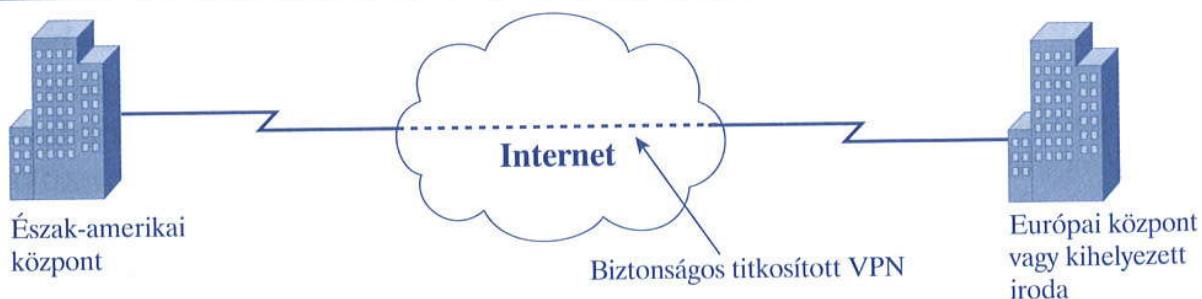
- **Távoli elérésű VPN** – Lehetővé teszi az egyéni behívó felhasználóknak, hogy biztonságosan kapcsolódjanak az interneten vagy más nyilvános hálózaton keresztül egy központi helyhez. A VPN ezen típusa egy felhasználó–helyi hálózat jellegű kapcsolat, amely a telephelyen kívülre távozó felhasználók számára teszi lehetővé a vállalati hálózat elérését. Az ilyen felhasználók rendszerén különleges VPN-szoftver fut. Ez a szoftver teszi lehetővé a közöttük és a vállalati hálózat között létesített biztonságos kapcsolatot. A nagyméretű távoli elérésű VPN-t beüzemelni szándékozó vállalkozás általában egy szolgáltatóval karoltve valamilyen behívó internetelérést kínál a felhasználónak. A távoli felhasználók az internethez csatlakozásra valamelyen díjmentes vagy csökkentett díjú modemes hozzáférést használnak, és a saját VPN-kliens szoftverük segítségével érik el a vállalat hálózatát. Egy ilyen vállalkozásra jó példa lehet egy több száz utazó munkatársat foglalkoztatónak nagyobb cég, amelynek munkatársai távolról el akarják érni a vállalat hálózatát. A távoli elérésű VPN-t időnként „puha” (*soft*) vagy szoftveralapú, esetleg virtuális magán-behívóhálózatnak (*VPDN – Virtual Private Dial-In Network*) vagy egyszerűen behívó VPN-nek is nevezzük. A felhasználók alacsony, állandó összegű díjat fizetnek a helyi internetszolgáltatónak a kapcsolatért. Ennek során helyi hívást használnak, nincs szükség távolsági hívásra sem a szolgáltató, sem pedig a vállalat eléréséhez. A felhasználó ezt a helyi kapcsolatot használhatja arra, hogy fölötté egy VPN-csatornát hozzon létre. A vállalat pénzügyi vezetősége előnyben

részesei az alacsony, állandó összegű költségeket az állandóan növekvő távolsági hívások díjával szemben.

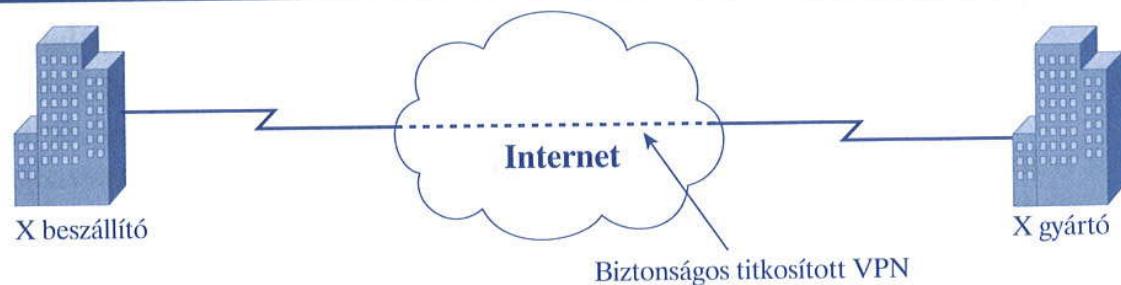
- **Telephelyközi VPN** – A vállalat létező hálózatának a kifejezetten erre szolgáló eszközök segítségével más épületekbe és helyekre való kiterjesztésére használjuk, így az ottani távoli felhasználók is ugyanazon hálózati szolgáltatásokat érhetik el. Az ilyen jellegű VPN-t állandó hozzáférést biztosító virtuális magánhálózatnak tekintjük. A telephelyközi VPN-t néha „kemény” (*hard*) vagy hardveralapú VPN-nek, intranetnek vagy hálózat–hálózat VPN-nek is nevezzük.
- **Extranet VPN** – Lehetővé teszi az üzleti partnerekkel, beszállítókkal és fogyasztókkal az elektronikus kereskedelem érdekében kialakított biztonságos kapcsolatot. A külső VPN a belső VPN kiterjesztése a helyi hálózatot védő tűzfalakon kívülre. Felhasználására jó példa a beszállítókkal és más partnerekkel szorosan együttműködő vállalat, amelynek érdekében áll a szoros kínálat/kereslet kapcsolat kezelése – például ha az alacsony raktárkészletet fenntartani kívánó vállalat igényeit a beszállító az igényeknek megfelelő módon, folyamatosan kívánja kielégíteni.



Távoli elérésű VPN



Telephelyközi VPN



Extranet VPN

7.1. ábra. A VPN lehetséges típusai

A kiterjesztett hálózaton keresztül ez a két vállalat gyorsabban tud adatokat cserélni.

Ezen VPN-ek mindegyike a hagyományos WAN-hálózatok megbízhatóságát, teljesítményét, szolgáltatásának minőségét és biztonságát kívánja nyújtani, de jóval alacsonyabb költségek és sokkal rugalmasabb szolgáltatói háttér mellett. A 7.1. ábra szemlélteti a fent ismertetett háromféle VPN-t.

A 7.1. ábrán látható minden VPN az interneten keresztül működik. A VPN-technológia azonban használható a saját hálózaton belül is a biztonság egy újabb szintjének bevezetése érdekében, ezzel is nehezítve az érzékeny információhoz, rendszerekhez vagy erőforrásokhoz való illetéktelen hozzáférést. A VPN-technológia segítségével például a pénzügyi rendszerekhez való hozzáférés csak bizonyos felhasználókra korlátozható, vagy arra, hogy az érzékeny vagy bizalmas adatok csak biztonságos módon legyenek elküldhetők. A következő fejezetben a VPN elhelyezkedését és az ahhoz tartozó különböző előnyeit tárgyalja.

## 7.2.1. A VPN ELŐNYEI ÉS CÉLJA

A jól megtervezett VPN nagy előnyt jelent a vállalat számára, például az alábbi célok érdekében:

- A VPN-technológia kifejlesztése előtt a távoli helyeken tartózkodó alkalmazottak távolsági hívás segítségével érhették csak el a vállalati hálózatot. Ha le akarjuk csökkenteni ezeket a hívási költségeket, akkor a távolsági hívás helyett helyi hívás segítségével az adott körzet internetszolgáltatóját kell elérni, és rajta keresztül használhatjuk a VPN-klientet. Az utazó alkalmazottak számától függően az így megtakarított költség jelentős összeg is lehet. A kisebb pénzügyi mozgástérrel rendelkező kis- és középvállalatok esetén ezért a VPN jelentheti a gyakorlati megoldást.
- Meg akarjuk növelni a felhasználók termelékenységét azzal, hogy földrajzi helyzetüktől függetlenül lehetővé tesszük számukra a hálózati erőforrásaink elérését.
- Csökkenteni akarjuk a bérelt WAN-kapcsolatok jelentette működési költséget azáltal, hogy üzleti célra alkalmas, szélessávú közvetlen internetkapcsolattal helyettesítjük, amelyen keresztül a távoli helyek a telephelyközi kapcsolatot biztosító VPN segítségével kapcsolódnak.
- Egyszerűsíteni akarjuk a hálózatunk topológiját azzal, hogy a hálózat stratégiai pontjain VPN-hozzáférést biztosítunk.

- A helyi hálózatunk csatlakoztatására viszonylag szerényebb a sávszélesség iránti igényünk. A VPN használata esetén gyorsabb befektetésmegterülést érhetünk el, mint a hagyományos WAN-megoldások esetén.
- A mobil számítástechnika, távkommunikáció és kihelyezett irodai hálózat nagymértékben rugalmas létesítésére, az üzleti partnerekkel, beszállítókkal és vevőkkel könnyebb e-kereskedelmi és extranet-hálózatok ki-alakítására van szükség, illetve a belső intranet- és a külső extranetelérést egyetlen biztonságos kapcsolaton keresztül kívánjuk megoldani.
- Csökkenteni akarjuk az irodai költségeket azzal, hogy a munkatársak munkaidejük egy részében otthonról dolgozzanak. Az otthoni dolgozók általában termelékenyebbek, és kisebb stressz alatt állnak.

Mielőtt implementálnánk a VPN-t, körültekintően és minden részletre kiterjedően meg kell terveznünk, mit várunk el a VPN-től. Ez alatt az idő alatt – még a szállító vagy a hardver és szoftver kiválasztása előtt – ki kell választani a számunkra legfontosabb jellemzőket. A VPN tervezése során a biztonság, amiről később még lesz szó, mindig az egyik legfontosabb szempont kell legyen.

## 7.2.2. VPN IMPLEMENTÁCIÓS STRATÉGIÁK

A VPN implementációs stratégiák nagymértékben eltérhetnek egymástól, hiszen manapság minden szállítónak van egy saját VPN „megoldása” számunkra. Ezek némelyike valóban megfelel az általuk hirdetettnek, míg másokat a biztonsággal foglalkozó szakemberek erősen megkérdőjeleznek, amint azt a hatodik fejezetben, az útválasztó biztonsága kapcsán is említettük már. Mivel a VPN implementálásának nincs elfogadott szabványa, így számos cég dolgozta ki a saját megoldását.<sup>1</sup> Ebben a fejezetben a Ciscónál elérhető különböző lehetséges komponenseket mutatjuk be, valamint azt, hogy az egyfunkciós berendezések, például tűzfalak miként tudják betölteni a VPN-beli szerepüket:

- **Tűzfalak** – Ha nem is lett volna tűzfala az 5. fejezet elolvasásáig, mostanra már nyilván beszerzett egyet. A tűzfalaknak alapvető szerepük van a hálózat biztonsága szempontjából. Manapság a Cisco-tűzfalak mindegyike egyszerre támogatja az állapotteljes csomagvizsgálatot és a virtuális magánhálózatot. A megoldások a szabványalapú telephelyközi VPN-től az internetkulcscsere (*IKE – Internet Key Exchange*) és az

---

<sup>1</sup> Ma már az IPsec, az SSL, az L2TP és a PPTP szabványos megoldásnak tekinthető. (A lektor meg.)

IPsec biztonsági protokollalapú VPN-szabványokig terjednek. A Cisco PIX-tűzfal az 56 bites adattitkosító szabványt (*DES – Data Encryption Standard*), a 168 bites háromszoros DES-t (3DES), vagy akár a 256 bites javított titkosító szabványt (*AES – Advanced Encryption Standard*) képes használni. Fejlett technológiájából adódóan a Cisco PIX-tűzfal egyesíti magában a dinamikus hálózaticím-fordítás (NAT), a csomagszűrő proxy szerver, a tűzfal és a VPN-végállomás módszereket, mindenzt egyetlen hardveregységen. A Cisco IOS-szoftver használata helyett ebben az eszközben egy rendkívül modern operációs rendszer kapott helyet, amely a nagyszámú protokoll kezelésének képességét nagyfokú megbízhatósággal és hatalmas teljesítőképességgel ötvözi.

- **VPN-képességekkel felszerelt útválasztók** – A Cisco-útválasztóhoz elérhető a VPN használati képesség is. Az ehhez szükséges frissítések az alábbiak egyikeként érhetők el, a szóban forgó útválasztótól függően: IOS, memória vagy külön VPN-hardver. Bizonyos egyedi jellemzők érhetők el azáltal, hogy biztosítja az átméretezhetőség, útválasztás, biztonság és szolgáltatásminőség lehetőségét. A Cisco IOS-szoftverre alapozva bármely feladatra található alkalmas Cisco-útválasztó, a kis irodai/otthoni használatra tervezettől a nagyméretű vállalatok igényeinek is megfelelő, központi helyen üzemelő VPN-gyűjtőig.
- **VPN-koncentrátor** – Magában foglalva az elérhető legfejlettebb titkosítási és hitelesítési technikákat, a Cisco VPN-koncentrátor kifejezetten a távoli elérést igénybe venni kívánó felhasználók igényeihez lett kifejlesztve. Biztosítja a nagyfokú elérhetőséget, teljesítményt és rugalmasságot. Tártalmazza a méretezhető titkosítás-végrehajtó (*SEP – Scalable Encryption Processing*) modulokat, amely a hálózati mérnökök számára lehetővé teszi a növekvő kapacitásigényekhez és átvitt adatmennyiséghoz való könnyű illesztést. A VPN-koncentrátorok a VPN-ek követelményeinek kezelésére készültek, és a legfeljebb néhány száz felhasználót tartalmazó kisebb vállalkozásoktól akár a tízezres nagyságrendű számban egyidejűleg csatlakozó nagyvállalatokig bármit kiszolgálni képes többféle modell érhető el.
- **Kliensszoftver** – A könnyen telepíthető és működtethető Cisco VPN-kliens biztonságos végpont–végpont közötti titkosított csatornákat biztosít az itt felsorolt VPN-eszközök számára. Ez a vékonyréteg-tervezésű IPsec-hez illeszkedő szoftver előkonfigurálható a nagytömegű telepítéshez, és a kezdeti bejelentkezések kevés felhasználói beavatkozást igényelnek. A kliensszoftver az alábbi platformokon érhető el: Windows 95, 98, Me, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc-32 bit) és Mac OS X 10.x.

A VPN típusától függően (távoli elérésű vagy telephelyközi típusú), külön hardvereszközök használatára lehet szükség a VPN kiépítéséhez. Mindenesetre az alábbi megfontolásokra is figyelemmel kell lenni:

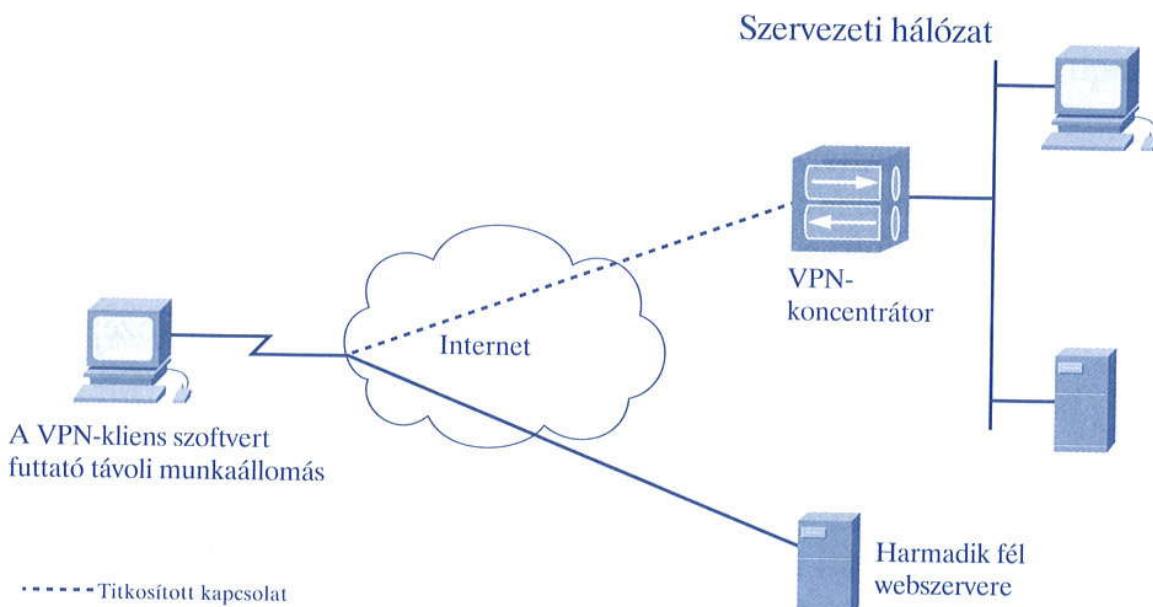
- **Menedzselhetőség** – A VPN menedzselhetősége a létrehozott hálózati csatlakoztathatóság sikeres kezeléséhez szükséges erőfeszítések menyiségét jelenti. Adott esetben a PC Magazine folyóirat a menedzselhetőséget a „távoli és helyi kezelési lehetőségek könnyű vagy nehéz volta” alapján ítéli meg, amelybe beleérti azt is, hogy az „adott eszköz rendelkezik-e böngészőalapú interfésszel vagy parancssori hozzáféréssel” (PC Magazine, 2002).
- **Megbízhatóság** – Ha a VPN-szoftver vagy -hardver nem elérhető, amikor szükség lenne rá, nyilván csökken a termelésünk, és valószínűleg valamennyi pénzt is veszítünk. Amikor kiválasztunk egy megoldást, érdemes megvizsgálni és összehasonlítani a szóba jöhető lehetőségek üzemidejével és kiesési idejével kapcsolatos statisztikákat.
- **Méretezhetőség** – Amint a vállalat üzleti volumene növekszik, általában ennek mértékében növekszik az IT-infrastruktúrával szemben támiasztott követelmények listája is. A VPN gyors és költséghatékony növelésének egyszerűsége érdekében a megoldások közötti válogatás során érdemes figyelemmel lenni az átméretezhetőségre is. Az IT-vezető a legkevésbé sem akarna később minden teljesen előlről kezdeni, és kicsérélni a teljes VPN-infrastruktúrát csak azért, mert az üzleti növekedésnek ez válik a korlátjává.

Amikor kiválasztjuk a hálózat VPN-szolgáltatását nyújtani képes megfelelő eszközt, akkor figyelemmel kell lenni a korlátaira is. Így például egy útválasztó IOS-szoftvere is lehet VPN-végződés, de ennek beállítása kizárolag kézzel történhet, és a téma sokkal mélyebb ismeretét igényli, mintha a PIX-tűzfalat használnánk a grafikus felületén elérhető saját VPN-beállító varázslójával. Elérhető továbbá a Cisco VPN-koncentrátör is, amely grafikus beállítási lehetőségeit tekintve valahol félúton van a PIX és az IOS között, viszont megkönnyíti a nagymennyiségű VPN-szabály beállítását. A koncentrátör könnyen érhető utasításaival jól be lehet állítani a különböző szabályokat és csoportokat, így a hálózathoz csatlakozó különböző felhasználók csoportba sorolásával más és más elérési jogosultságok adhatók. A koncentrátör elsősorban akkor ajánlható, ha a vállalkozásnak korlátozott létszámu munkatárs áll rendelkezésére, azonban számos különböző VPN-szabályra lenne szüksége. A PIX és az IOS némileg bonyolultabban állítható be és kezelhető ilyen különleges kívánsgág esetén, és az átméretezhetőségről sem szabad megfeledkeznünk.

### 7.2.3. MEGOSZTOTT ALAGÚT

Számos VPN-felhasználó már eleve túzfal mögött van, és az erőforrásokhoz való hozzáférésre kizárolag VPN-en keresztül van szükségük. A hagyományos VPN nem teszi lehetővé, hogy a felhasználók a saját helyi hálózati szegmensüket és a VPN segítségével a vállalat hálózatát egyidejűleg elérjék. Ez az igény azonban felmerülhet például akkor, ha a felhasználónak el kell érnie a vállalati hálózatot, és közben képesnek kell lennie a hálózati nyomtatóna való nyomtatásra is. Ezen valós igény kielégítésére bevezetett megoldást nevezzük „megosztott alagútnak” (*split tunneling*).

Az alagút megosztása akkor következik be, ha egy távoli felhasználónak vagy helynek a magánhálózattal egyidőben a nyilvános internetet is el kell érnie anélkül, hogy a nyilvános hálózati forgalmat is a VPN-csatornán keresztül akarná lebonyolítani. Ezt a lehetőséget nem minden jó ötlet bekapcsolni, mivel megkönnyíti a behatoló számára a minden hálózathoz csatlakozó számítógép feltörését. A 7.2. ábra mutatja be, hogy miként is történik az alagútmegosztás.



7.2. ábra. Az alagútmegosztás vázlata

7.

### 7.3. Az IPSec VPN Áttekintése

Az IPSec a hálózati iparban a VPN létrehozásának hallgatólagos szabványává vált. Számos gyártó implementálta, s mivel az IETF több RFC-t is kiadott az IPSec-ről, így a különböző gyártók eszközei közötti együttműködési képesség miatt ez a VPN kiépítésének a legjobb módja. Az IPSec a végpontok közötti hitelesítésre és titkosításra kínál szabványos megoldást. Témánk szempontjából az IPSec-végpontok a VPN-csatorna minden-

két végén megtalálhatók. Az IPSec az OSI-modell szerinti hálózati réteget alkotja,<sup>2</sup> amely a kommunikációban részt vevő IPSec-eszközök, például Cisco-útválasztók és tűzfalak közötti IP-csomagokat hitelesíti és védi. Az IPSec hálózatbiztonsági szolgáltatásai a következők:

- **Adat bizalmassága** – Az IPSec küldő oldal a hálózaton való átvitel előtt titkosítja a csomagokat. Ha egy támadó nem tudja elolvasni az adatot, akkor hasznát sem veheti.
- **Adat sértetlensége** – Az IPSec fogadó oldal az IPSec-küldő által küldött minden egyes csomagot hitelesíti, így döntve el, hogy az nem változott-e meg az átvitel során.
- **Adatforrás hitelesítése** – Az IPSec fogadó oldal az IPSec-csomagokat küldő felet képes azonosítani. Ez a szolgáltatás az adatsértetlenségi szolgáltatástól függ.
- **Visszajátszás elleni védelem** – Az IPSec fogadó oldal képes felismerni és eldobni a visszajátszott csomagokat.

Az IPSec a nem védett hálózatokon továbbított adatokat képes megvédeni. A biztonsági szolgáltatásokat a hálózati réteg nyújtja, így nincs szükség az egyedi munkaállomások, számítógépek vagy alkalmazások beállítására. Ez az előny önmagában is jelentős költségmegtakarítást eredményezhet. Ahelyett, hogy a biztonsági szolgáltatásokat számítógépenként és alkalmazásonként egyedileg kellene telepíteni és beállítani, inkább a hálózati infrastruktúrát változtatjuk meg olyanra, amely az igényelt biztonsági szolgáltatásokat nyújtaná képes. Ez a támogatás teszi lehetővé az IPSec-megoldások viszonylag egyszerű átméretezését közepes vagy nagyméretű és növekvő hálózatokra, ahol számos eszköz között kell biztosítani a biztonságos kapcsolatot.

Az IPSec fejlett biztonsági jellemzőkkel bír, például jó minőségű titkosító algoritmusokkal és aprólékos hitelesítéssel. Az internethoz csatlakozó vállalati hálózatokon rugalmas és biztonságos VPN-hozzáférés engedélyezhető az IPSec használatával. Az IPSec technológiával a felhasználók az internetet használó VPN-t helyezhetnek üzembe, amely a kábel lehallgatása és a magánkommunikációt fenyegető más támadások ellen biztonságos titkosítással védekezik.

Az IPSec hitelesítő- és titkosítószolgáltatásokat nyújt, amelyek a saját vagy a védelem nélküli külső hálózatban mozgó adatok jogosulatlan elolvasása vagy módosítása ellen védenek. Az IPSec különböző eszközök közötti adatforgalom titkosítására képes, beleértve

2 ESP-mód esetén az IPSec inkább az adatkapcsolati réteget alkotja. (A lektor meg.)

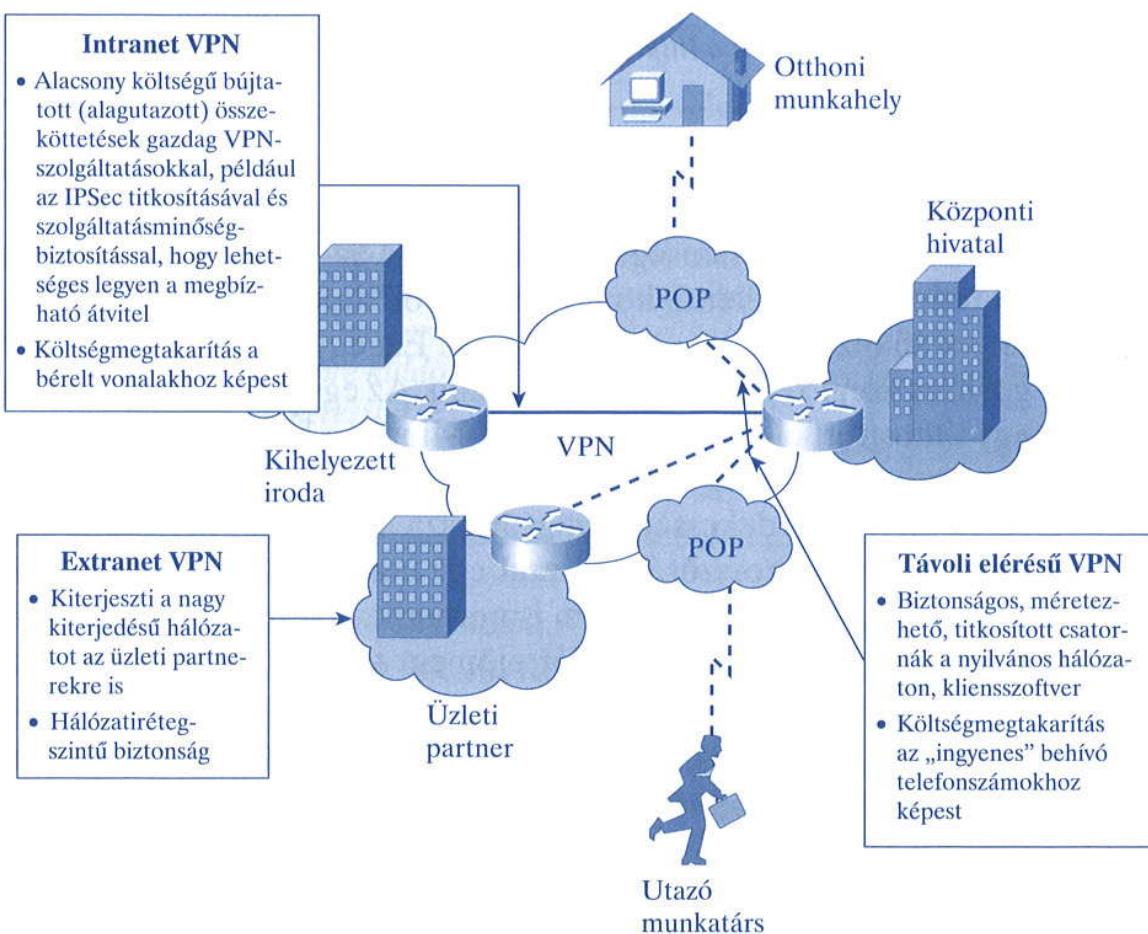


Ezt a protokollt kizárolag az IPSec felhasználására felkészített rendszerek képesek kihasználni. Valamennyi eszközökhez hozzá kell továbbá rendelni egy közös kulcsot, és minden tűzfalat hasonló biztonsági szabályokkal kell ellátni.

- útválasztótól útválasztóig,
- tűzfaltól útválasztóig,
- tűzfaltól tűzfalig,
- felhasználótól az útválasztóig,
- felhasználótól a tűzfalig,
- felhasználótól a VPN-koncentrátorig,
- és a felhasználótól a szerverig.

mozgó adatokat.

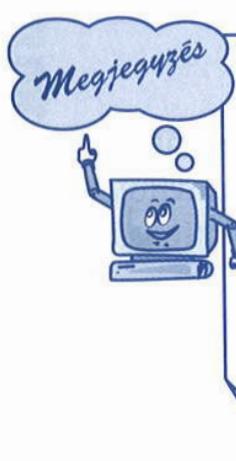
Az IPSec az IETF által definiált nyílt keretszabvány. A védetlen hálózatokon (például internet) keresztsüli érzékeny adatok biztonságos átvitelét teszi lehetővé. A 7.3. ábra mutatja be a VPN három leggyakoribb típusát.



7.3. ábra. A VPN-kapcsolatok áttekintése

### 7.3.1. AZ ADATOK HITELESÍTÉSE ÉS SÉRTETLENSÉGE

Ahhoz, hogy meglegyen a bizalom, a hitelesítés nevű folyamat során el- lenőrizni kell minden két VPN-végpont és a VPN-en keresztül adatot kül- dő felhasználó azonosságát. A végpont lehet egy VPN-kliens, VPN-kon- centrátor, tűzfal vagy útválasztó. A hitelesítés az IPSec egyik folyamata, amely az adat titkosítása után és a másik oldali visszafejtése előtt hajtódik végre. Ez az IPSec kötelezően végrehajtott művelete, amely biztosítja, hogy minden két oldalnak kézzel be kell állítani egy korábban kicse- rélt kulcsot (amelyet a felek általában nem hálózati átvitellel adnak meg egymásnak), valamint a fogadható végpontok listáját. Ezzel az útválasz- tóban lefoglalunk egy valószínűleg nagyméretű táblát, amely a memória- erőforrásokat erősen terhelheti.



*A felhasználók digitális tanúsítványok segítségével is hitelesíthetők, vagy meg- követelhetjük azt is, hogy a gépeknek legyen digitális azonosítójuk ahoz, hogy a kapcsolatot egyáltalán megkezdhessék kiépíteni; ezután következhet a fel- használó hitelesítése, amellyel a kapcsolatkiépítés be is fejezhető. Ennek to- vábbi tárgyalása meghaladja jelen könyv kereteit, a hitelesítésről további infor- mációkat azonban a <http://www.netsol.com> helyen is találhat.*

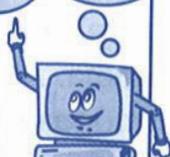
Az adatok sértetlenségének biztosítása az IPSec másik szolgáltatása. A sértetlenség azt jelenti, hogy a fogadó oldalon megkapott csomag az átvitel során biztosan nem változott meg. Ezt egyirányú kivonatoló (*hash*) algoritmus segítségével lehet ellenőrizni. Az egyirányú kivonatolás megfelel egy titkosított ellenőrző összegnek. Miután a küldő fél titkosítja és hitele- síti a csomagot, még az egyirányú kivonatolást is elvégzi a teljes csomag- ra. A kivonat érdekessége, hogy hossza a bemenet méretétől függetlenül minden azonos hosszúságú. Ezzel egy újabb biztonsági mechanizmushoz jutunk, hiszen a támadók nem ismerhetik a bemeneti adatok méretét. Az egyirányú kivonatolás során létrejön egy titkosított mező, amelyet az üze- net végéhez csatol. A fogadó oldalon a kivonatot leválasztja a csomagról, és a maradékban a fogadó is elvégzi a kivonatolást. Mivel a kivonat értéke csak a csomagban található változó adatok, például a küldés időpontjá-nak értékétől, a bájtok számától stb. függ, így minden két oldalon azonos ki- vonatot kell kapunk. Ha ez teljesül, akkor a csomag a küldés során nem változott meg. Amennyiben a kapott kivonatok különböznének, a csoma- got eldobja, majd az IPSec újra beállítja a biztonsági paramétereit.

### 7.3.2. ALAGÚTTECHNIKA

A VPN a nyilvános interneten keresztül az alagúttechnika segítségével valósítja meg a magánhálózatot. Ez tulajdonképpen egy olyan folyamat, amikor vesszük a teljes csomagot, és a hálózaton keresztülküldése előtt elhelyezzük azt adatként egy másik csomag belsejében. A hálózatnak csak a külső csomag protokollját kell ismernie a továbbításhoz. Az alagút működéséhez három különböző protokollra van szükség:

- **Utasprotokoll** – Az eredeti adatcsomag, általában egy IP-csomag, amelyet titkosítani kell a VPN-en keresztül. Amennyiben arra lenne szükség, más protokollok, például IPX vagy NetBEUI is használható.
- **Csomagoló protokoll** – Az eredeti csomagot becsomagoló (magába foglaló) protokoll (például GRE, IPSec, L2F, PPTP, L2TP). Jelenleg az IPSec az erre szolgáló, hallgatólagosan szabványként elfogadott protokoll, amely lehetővé teszi az egész utacsomag titkosítását és védelmét. Ehhez az IPSec protokollt minden alagút interfésznek támogatnia kell.
- **Hordozó protokoll** – A hálózat által a továbbításhoz használt protokoll. Az eredeti (utas) csomagot előbb bezárjuk a csomagoló protokollba, majd ezt a hordozó protokoll (általában IP) fejrészébe helyezzük a nyilvános hálózaton kereszti átküldéséhez.

#### Megjegyzés



*A csomagoló protokoll gyakran elvégzi még az adat titkosítását is. Amint látható, az IPX vagy NetBEUI protokollok, amelyeket általában nem küldünk az interneten keresztül, szintén biztonságosan átvihetők így. Lehetséges olyan csomag átküldése is, amely magán (nem irányítható) IP-címet tartalmaz a befogadó, nyilvános címre küldött csomagon belül, kiterjesztve így a magánhálózatot az interneten keresztül.*

Az alagúttechnikát jól hasznosítja a VPN, hiszen az internet által nem támogatott protokollokat küldhetünk így át az IP-csomagok belsejében, ráadásul biztonságos módon. A VPN alagútátvitel kezdetén a forráshálózatból származó adatcsomagot becsomagoljuk és új fejlécinformációkkal látjuk el, amely lehetővé teszi a köztes hálózatokon való átküldését. Miután ez megtörtént és az átvitel befejeződött, az alagútprotokoll fejlécét levágjuk, és az eredeti csomagot a célhálózatnak adjuk át továbbításra.

Jóllehet az alagút lehetővé teszi az adatok harmadik fél hálózatán kereszti átküldését, maga az alagúttechnika önmagában nem biztosítja a tit-

kosságot. A lehallgatás és módosítás elleni védelem érdekében a VPN-en keresztül küldött minden forgalmat titkosítani is kell. A VPN ráadásul további szolgáltatásokat is nyújt, például tűzfalakat használhatunk a szélein.

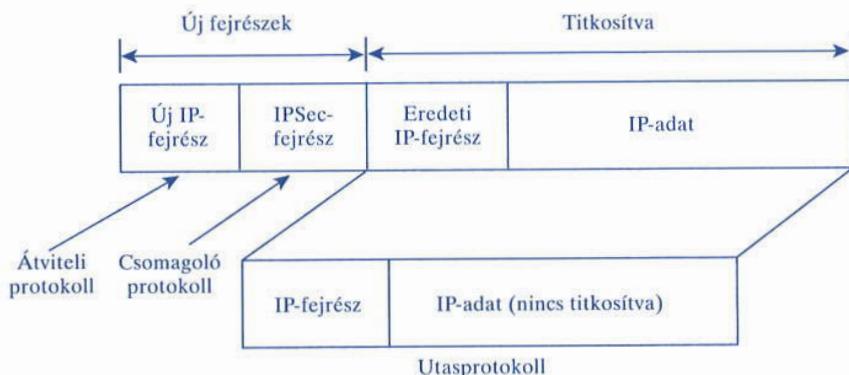
A telephelyközi VPN esetén a csomagoló protokoll általában az IPSec vagy GRE (*generic routing encapsulation*). Ez utóbbi a becsomagolandó csomag típusára és a kliens és a szerver közötti kapcsolatra jellemző információkat is tartalmaz. A kettő közötti választás attól függ, hogy milyen szintű biztonságra van szükség az összeköttetésben, mivel az IPSec biztonságosabb, a GRE viszont szolgáltatásokban gazdagabb protokoll. Az IPSec az IP-csomagokat képes titkosítani és alagúton keresztül elküldeni, míg a GRE az IP- és a nem IP-csomagok alagúton keresztüli küldésére egyaránt képes. Amikor nem IP-csomagok (például IPX) átküldésére van szükség, az IPSec és a GRE együttes használata ajánlatos.

### 7.3.3. TITKOSÍTÓ MÓDSZEREK

Az IPSec-nek két titkosító módja van: alagút és átviteli. A két mód eltérően van megvalósítva, és különböző mennyiségű többletterhet jelent az utacsomag számára. A két módot röviden úgy jellemzhetjük, hogy az alagúttitkosítás a csomagoknak a fejrészét és az adatrészét egyaránt titkosítja, míg az átviteli titkosítás csak az adatrészet rejtelezeti.

#### Alagúttitkosítás

Nem megbízható hálózaton, például a nyilvános interneten keresztül összekötött két PIX-tűzfal (vagy más biztonsági eszköz) között az alagúttitkosítás (vagy alagút mód) az IPSec alapértelmezett titkosítási módja. A további tárgyalás során minden azt feltételezzük, hogy ebben a módban használjuk az IPSec-et. Az alagúttitkosítás során a teljes csomagot védjük és becsomagoljuk. Mivel a sikeres továbbításhoz a teljes csomagot elrejti egy másikban, így a befogadó IP-csomagba, vagyis az új fejrészbe a titkosító útválasztók IP-címei kerülnek. A titkosítás kiegészíthető az AH- vagy

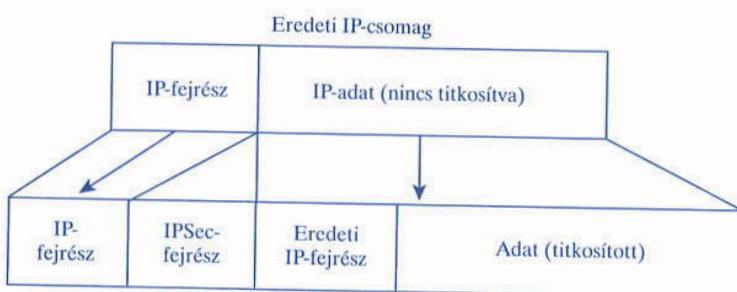


7.4. ábra. Alagúttitkosítás

ESP-szolgáltatással is (lásd később). A módszer használata egy körülbelül húsbajtnyi IPSec-fejrész és az új IP-fejrész hozzáadásával jár, amint azt a 7.4. ábra mutatja.

### Átviteli mód

Az IPSec implementálásának ezt a módját általában az L2TP használata esetén választjuk a távoli Windows 2000 VPN-kliensek hitelesítéséhez. Erről a lehetőségről az 5. fejezetben már esett szó, így most csak az IPSec-re és az alagút módra összpontosítjuk figyelmünket. Ez utóbbi esetén az IPSec a teljes csomagot titkosítja, és egy új IP-fejrészt ad hozzá, elfedve így az eredeti forrás- és célcímeket.<sup>3</sup> Az alagút mód tehát eredendően biztonságosabb (mivel a teljes eredeti csomag titkosított, nem csupán az adat, mint az átviteli módban), amint az a 7.5. ábrán is látszik.



7.5. ábra. Átviteli mód

### 7.3.4. IPSEC PROTOKOLLOK

Az IPSec három kiegészítő protokollt is használ, amelyek együttes használata a VPN-ek számára ideális egységes és biztonságos szabványalapú keretet biztosít. Az IPSec-szabványban leírt három protokoll az alábbi:

**7.**

- **ISAKMP** – Internet biztonságos kapcsolati kulcskezelő protokoll (*Internet Security Association Key Management Protocol*). Leírja az IPSec VPN kiépítésére tett kapcsolatteremtési kísérlet egyeztetési fázisát. Az Oakley protokoll definiál egy módszert a hitelesítési kulcsok cseréjére. E módszer, más kulcscserélő algoritmusokból, például a Diffie–Hellman-módszerből származva számos működési módot tesz lehetővé. Az ISAKMP tartalmazza az IKE (Internet Key Exchange – internet kulccsere) módszert, amely a biztonsági paraméterekre (például titkosítás

3 Ez akkor igaz, ha el akarjuk fedni az eredeti fejrészt. A címek jól használhatók például a forgalomanalízis során, de ha az IPSec-csatorna végén csak egy gép van, akkor ez az információ semmivel nem ad többet. (A lektor meg.)

típusa, biztonsági kapcsolat élettartama stb.) vonatkozó megállapodások keretét adja és biztosítja a kulcsok valódiságát.

- **ESP** – Csomagoló biztonsági protokoll (*Encapsulated Security Protocol*). Az adat bizalmasságát és védelmét nyújtja, opcionális hitelesítő és visszajátszás-feltáró szolgáltatásokkal. Az ESP teljesen becsomagolja a felhasználó adatait. Használható önmagában, vagy az AH-val együtt. Ezt a TCP protokoll szerinti 50 és 51 végpontokat használó protokoltt az RFC 2406 írja le.
- **AH** – Hitelesítő fejléc (*authentication header*). Opcionális hitelesítő és visszajátszás elleni védelmi szolgáltatást nyújt. Az IP normál és bővített fejrészének korlátozott részéhez nyújt szolgáltatást, azonban nem titkosítja az adatot, csupán egyirányú kivonatot készít a csomagról. Az AH beépül a védett adatba (például a teljes IP-csomagba). Használható önmagában, vagy az ESP-vel együtt. Ezt a protokoltt az ESP nagymértékben kiváltotta, és manapság már elavultnak számít.

### Biztonsági kapcsolatok

A biztonsági kapcsolat (*SA – security association*) a gép-gép kapcsolat során a két eszköz közötti bizalmat hozza létre, és lehetővé teszi a VPN-végpontok számára, hogy a lehetséges másik féllel megállapodjanak a használni kívánt átviteli szabályokban. A biztonsági kapcsolatot felfoghatjuk szerződésnek is, amely egyezteti és beállítja a kapcsolat különböző paramétereinek értékét.

A biztonsági kapcsolatot az IP-cím, a biztonsági protokoll azonosító, és egy egyedi biztonsági paraméter index (*SPI – security parameter index*) segítségével azonosítjuk. Az SPI a csomag fejrészében található 32 bites szám. A biztonsági kapcsolatoknak az alábbi két típusa létezik:

- **IKE** – Internet kulccsere (*Internet Key Exchange*). Biztosítja az egyeztetési, végpont-azonosítási, kulcskezelési és kulccserélő szolgáltatásokat. Mint kétirányú protokoll, az IKE a titkosítás, a kivonatképzés, a hitelesítési eljárás vagy más hasonló csoportinformáció algoritmusában megállapodni óhajtó két eszköz között biztosít biztonságos kommunikációs csatornát. A Diffie–Hellman-algoritmus szerinti kulccserét használ, ráadásul a hálózati adminisztrátorok a szabálykezelő rendszerekhez szorosan hozzá tudják kötni. A beékelődéses támadás (amikor egy támadó elfogja az interneten közlekedő csomagokat, módosítja azokat, és újraküldi a módosított csomagokat az eredeti címre) megelőzésére a Diffie–Hellman-algoritmus kibővítése, az állomás–állomás (*STS – station to station*) protokoll még azt is lehetővé teszi, hogy a kulccserére készülő eszközök egymás nyilvános kulccsal olvasható igazolásait és digitális aláírásait ellenőrizhessék.

- **IPSec SA** – Az IPSec biztonsági kapcsolat (*IPSec Security Association*) egyirányú, így az egyes irányokban eltérő IPSec SA-ra van szükség. Ez egy kétfázisú, hárommódszű eljárás. Az 1. fázisban két módon használható: *alapmódban* és *agresszív módban*. A 2. fázisban kizárolag a gyors mód érhető el. A végfelhasználó nem tudja befolyásolni, hogy melyik módot használja, mivel ennek kiválasztása automatikus, és minden két végpont konfigurációs beállításaitól függ.

Mind az IKE, mind az IPSec használ SA-t, azonban ezek egymástól függetlenek. Az IPSec SA egyirányú és minden egyes biztonsági protokollnál egyedi. A biztonsági kapcsolatok határozzák meg, hogy mely protokollok és algoritmusok alkalmazhatók az érzékeny csomagok esetén, és milyen kulcskészletet használnak az egyes végpontok. Az SA egyirányú, és az egyes biztonsági protokollokhoz (AH és/vagy ESP) külön kerülnek meghatározásra. Az IPSec SA kétféle módon építhető ki:

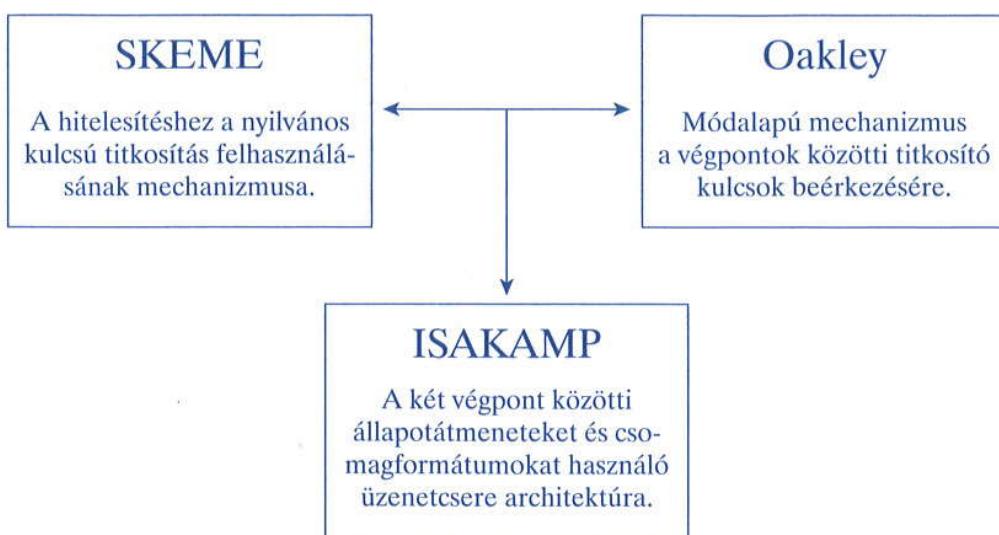
- **Kézi SA előre megosztott kulccsal** – A kézi IPSec SA a PIX-tűzfal és az IPSec-végpont adminisztrátorainak előzetes megegyezését követeli meg. Maga az SA során nincs egyeztetés, így minden rendszerben a beállítási információ az IPSec-forgalom sikeresége érdekében azonos kell legyen. A kézi beállítás egyszerű, azonban a kulcsok előzetes cseréje bonyolult lehet, hiszen ennek során az alagútátvitel kudarcot vallhat, és az is gond, hogy az előre beállított kulcsok nem változtathatók meg.
- **IKE által létrehozott SA** – Amikor az IKE-t használjuk az IPSec SA létrehozására, a végpontok megállapodhatnak azokban a beállításokban, amelyeket az új SA használni fog. Ez azt jelenti, hogy megadhatók listák (például az elfogadható átalakítások listája) is a *crypto map* bejegyzésben.

### Internet kulcscsere (IKE)

Ebben a pontban bemutatjuk az internet kulcscsere (*IKE – Internet Key Exchange*) protokollt, és a VPN jobb skálázhatóságát elősegítő működését. Az IKE egy hibrid protokoll, amely részben az Oakley, részben a biztonságos kulcscsere mechanizmusnak (*SKEME – secure key exchange mechanism*) nevezett protokollt használja az internet biztonsági kapcsolat és kulcskezelő protokoll keretén (*ISAKMP – internet security association and key management protocol*) belül. A 7.6. ábra szemlélteti, hogy az IKE valóban egy hibrid protokoll.

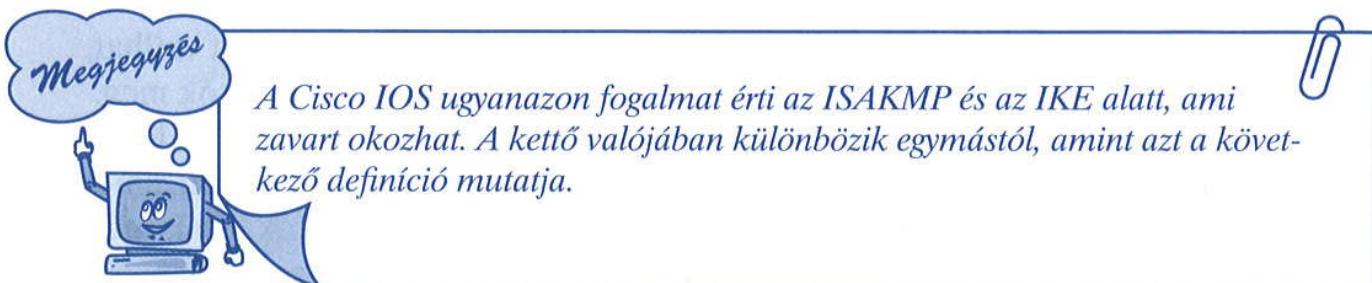
Az IKE a megosztott biztonsági szabályokat, valamint a hitelesítő kulcsokat biztosítja az ezt igénylő szolgáltatások (például IPSec) számára. Mielőtt az IPSec-forgalom áthaladhatna, minden egyik útválasztónak, tűzfalnak és gépnek képesnek kell lennie a végpont azonosítására. Ez megtehető minden két végponton az előre megosztott kulcsok kézi bevitelével,

## IKE (Internet Key Exchange) (RFC 2409) hibrid protokoll



7.6. ábra. Az IKE összetétele

egy tanúsító hatóság (*CA – Certification Authority*) által vagy a biztonságos DNS-sel (DNSSec). Az IKE protokoll korábbi neve az ISAKMP/Oakley volt, és az RFC 2409 definiálta.



Az IKE az a protokoll, amelyet az IPSec az 1. fázis lezárásához használ. Az IKE állapotid meg az SA-ban és rendeli azt hozzá mindegyik IPSec-végponthoz. Így válik lehetővé egy biztonságos csatorna használata az IPSec SA megállapodáshoz a második fázisban. Az IKE az alábbi előnyöket nyújtja:

- Mindkét végponton szükségtelenné teszi az IPSec biztonsági paramétek kézi megadását.
- Lehetővé teszi, hogy az IPSec SA élettartamát meghatározzuk.
- Lehetővé teszi az IPSec titkosító kulcsok megváltoztatását a kapcsolat időtartama alatt.
- Lehetővé teszi az IPSec számára a visszajátszás-megelőző szolgáltatások nyújtását.
- Lehetővé teszi a CA-támogatást egy kezelhető, méretezhető IPSec-implementációhoz.
- Lehetővé teszi a végpontok dinamikus hitelesítését.

Az IKE egyeztetési fázisnak védetten kell lezajlania, így ezek minden egyike azzal kezdődik, hogy a végpontok megegyeznek egy közös IKE szabályban. Ez a szabály vezérli a további IKE-egyeztetések védelmét biztosító biztonsági paramétereket. Miután a két végpont megállapodott a szabályban, létrejön a biztonsági kapcsolat azzal, hogy mindegyik végpont azonosítja a szabály biztonsági paramétereit, és ezek a biztonsági kapcsolatok vezérlik a további IKE-forgalmat az egyeztetés során.

### Az ISAKMP áttekintése

Az ISAKMP adja a kulccsere protokollnak és a biztonsági szabályok egyeztetési mechanizmusának keretét. Ezt használhatjuk mind az SA paraméterek, mind a végpontok közötti privát kulcsok biztonságos cseréjére az IPSec-környezetben, továbbá alkalmas a kulcs létrehozására és kezelésére is.

Az ISAKMP a kulcskezelésre több lehetőséget is nyújt, és a végpontok között lehetővé teszi az IPSec-paraméterek biztonságos átvitelét. Mind-ezt az IPSec által az adat tényleges titkosítására használt algoritmushoz hasonló módon teszi. Akárcsak az IPSec, az ISAKMP sem egy protokoll, hanem a dinamikus kulccsere különböző módszereinek kezelésére szolgáló interfész. Különböző módokat definiál (használhatók például digitális aláírások, bizonyítványok és egyirányú kivonatoló algoritmusok) annak biztosítására, hogy a végpontok közötti SA egyeztetési szakasza biztonságos legyen.

Jelenleg az ISAKMP által támogatott egyetlen protokoll az IKE. Amikor ezt aktívan használjuk a titkosítási eljárás során, az IPSec kommunikációs folyamatnak számos jellegzetessége válik elérhetővé. A nyílt kulcsú titkosítás használatával az IKE az IPSec-feldolgozás megkezdése előtt már egyezteti a biztonsági paramétereket, és elvégzi a kulccszerét.

7.

### 7.3.5. Az IPSEC MŰKÖDÉSE

Az IPSec fő feladata a nem biztonságos kapcsolaton keresztül lehetővé tenni a privát információk cseréjét azáltal, hogy a kapcsolat jellemzőit és a titkosító kulcsokat biztonságos módon cseréli. Az információ védelme érdekében titkosítást használ, így akadályozva meg a lehallgatást. A titkosítás hatékonysága érdekében azonban a két félnek egyaránt rendelkeznie kell egy közös titkos kulccsal (jelszóval), amelyet az információ VPN-csatornába küldése előtt, és az onnan való kivétele után kell a rejtjelezésre és a visszafejtésre használni. Az IPSec az IKE segítségével hozza létre a biztonságos kapcsolatot. Magas szinten vázolva, az IPSec-átvitel során bekövetkező események a következők:

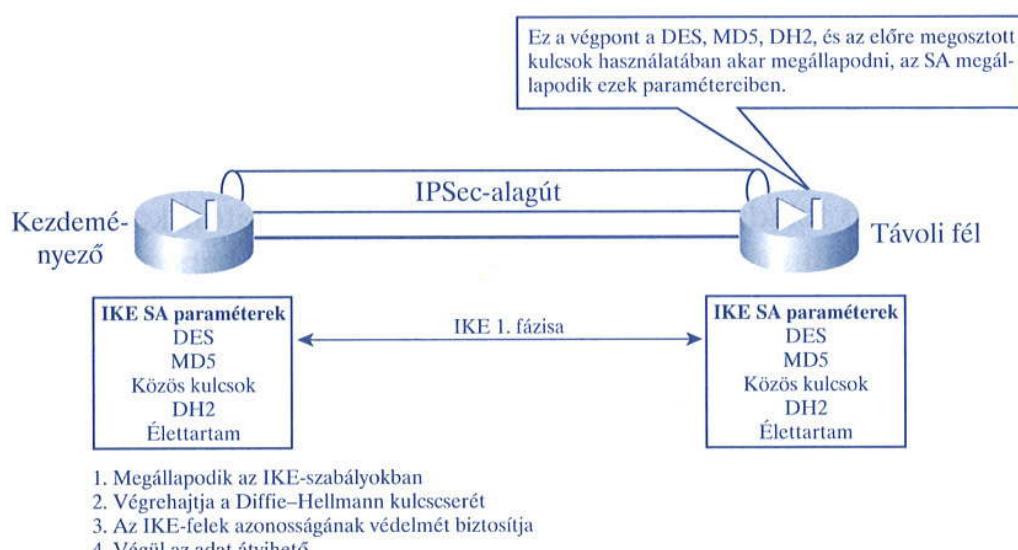
1. Az IPSec-végpontok egyike érdekes forgalmat állít elő vagy kap egy olyan interfészén, amelyet kifejezetten úgy állítottak be, hogy az ilyen típusú érdekes forgalomra egy IPSec-alagút kiépítésével válaszoljon.
2. Az alapmódú vagy agresszív módú egyeztetés a két végpont közötti IKE biztonsági kapcsolat létrehozásához az IKE eredményét használja.
3. A gyors módú egyeztetés az IKE eredményét a két végpont közötti két biztonsági kapcsolat létrehozásához használja.
4. Az adat ESP vagy AH csomagolási technikák valamelyikével történő átvitelle megkezdhető a titkosított csatornán.

Ez a négy, látszólag egyszerű lépés megérdemel némi többlet vizsgálatot. Az IPSec a közös titkos kulcs biztonságos megosztását két fő menetben végzi, amint azt a következő pontban bemutatjuk.

### IKE 1. fázisa

Az IKE 1. fázisa a két IPSec-végpontnak a biztonságos csatorna kialakításához szükséges biztonsági paraméterekkel kapcsolatos megállapodását teszi lehetővé. Általában az IKE protokoll fölött van implementálva, és elsődleges célja az IKE-üzenetek védelmének kialakítása. Ebben a fázisban az alábbi események követik egymást:

1. Mindenekelőtt létrejön az ISAKMP SA, ahol a felek megegyeznek a következőként létrehozandó IPSec SA paramétereikben. Miután ez megtörtént, és a felek között létrejött a biztonságos csatorna, az IKE a 2. fázisba lép tovább.
2. Amennyiben a távoli IPSec nem képes végrehajtani az IKE 1. fázisát, akkor az 1. fázis az előre kiválasztott kulcsok kézi beállításával zárható le.



7.7. ábra. Az IKE 1. fázisának működése

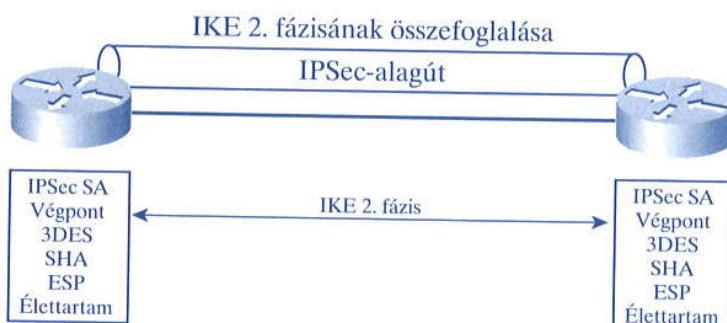
A 7.7. ábra mutatja az 1. fázis paramétereiről való megállapodást az SA használatával.

Az IKE 1. fázisának két működési módja van: az agresszív és a normál mód. Az agresszív módban az IKE kihagyja az azonosítási eljárás egyes részeit, azt csupán három lépésre redukálva, míg a normál módban minden a négy lépés végrehajtásra kerül. Jóllehet az agresszív mód gyorsabb, ám nyilvánvaló okokból kevésbé biztonságos, mint a normál mód. A Cisco-eszközök alapértelmezetten a normál módot használják, de az agresszív módot alkalmazó eszközök kapcsolatfelvételi kísérletére is képesek megfelelően válaszolni.

### Az IKE 2. fázisa

A 2. fázis az elsőben létrehozott biztonságos csatornán keresztül állapodik meg a felhasználói adatok tényleges átviteléhez szükséges további biztonsági paraméterekről, ezzel fokozva a kapcsolat biztonságát (lásd 7.8. ábra).

Ebben a fázisban az IKE létrehozza az IPSec számára a biztonsági kapcsolatokat, a beállított paraméteknek megfelelően. Az 1. fázisban létrehozott ISAKMP SA védi az ennek során generálódó forgalmat.



- Az 1. fáziban létrehozott IKE SA által védett módon megállapodik az IPSec SA paramétereikben.
- Létrehozza az IPSec biztonsági kapcsolatot (SA).
- Periodikusan újraegyezteti az IPSec biztonsági kapcsolatot a biztonság érdekében.
- Ha PFS engedélyezett, opcionálisan végrehajt egy újabb Diffie–Hellman-kulcscserét.

7.8. ábra. Az IKE 2. fázisának működése

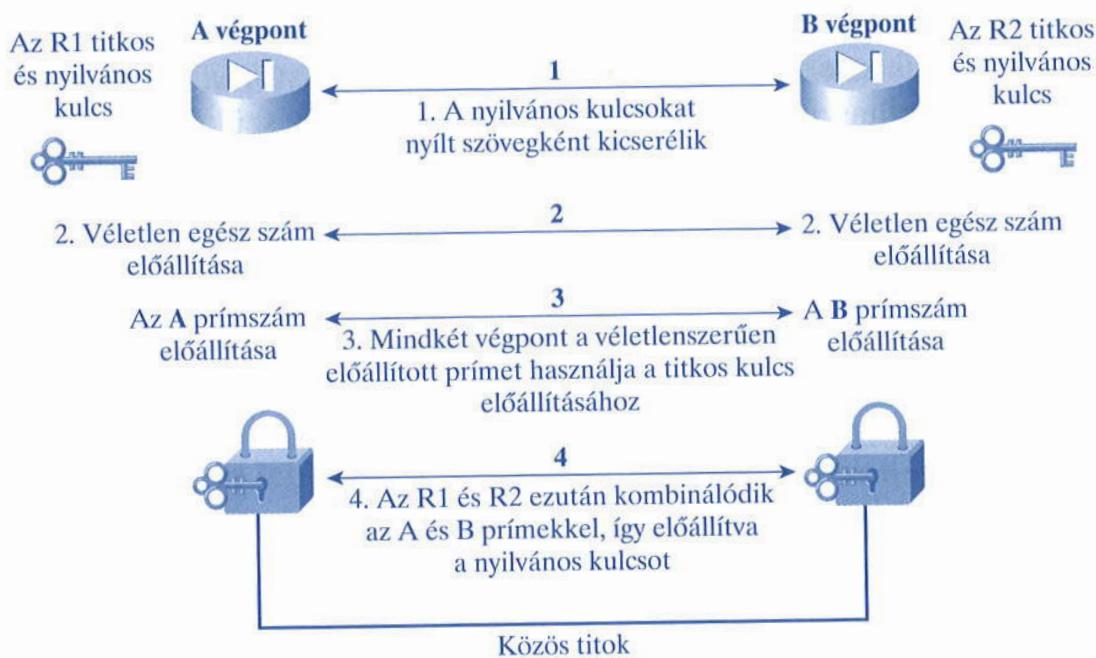
Az IPSec minden fázisában használt biztonsági alagutak az egyes IPSec végpontok által használt biztonsági kapcsolatokon (SA) alapszanak. Az SA írja le azon biztonsági paramétereket, például a hitelesítés típusát és a titkosítás jellegét, amelyek használatában minden két végpontnak meg kell egyeznie.

### A Diffie–Hellman-algoritmus

A Diffie–Hellman volt az első nyilvános kulcsú algoritmus, amelyet még ma is az egyik legjobbnak tartunk. Az IKE a kulcscsere védelmére és a biztonsági paraméterekben való megállapodáshoz egyaránt a nyilvános kulcsú

titkosítást használja. A megállapodás során a Diffie–Hellman-algoritmust használja arra, hogy a két végpont megegyezhessen a közös titokban, vagyis a használni kívánt kulcs előállítása során. Ez az oka annak, hogy a folyamat során a Diffie–Hellman-algoritmus használatát többször is láthatjuk.

Az algoritmus általában a következőképpen működik: mindenek végpontnak van egy saját titkos kulcsa. A Diffie–Hellman-algoritmus veszi ezt a titkos kulcsot, és előállítja a saját és a hozzá tartozó nyilvános kulcsot. A nyilvános kulcsot a titkos kulcs segítségével hozták létre, ám belül a titkos kulcs nem fejthető vissza. A felek ezután kicserélik a nyilvános kulcsaikat, amint az a 7.9. ábrán látható.



7.9. ábra. A Diffie–Hellman-kulcscsere



*A szimmetrikus kulcsú titkosítás során mind a titkosításhoz, mind a visszafejtéshez ugyanazt a kulcsot használjuk. A szimmetrikus kulcsú titkosításnak jelentős előnye van a nyilvános kulcsúakkal szemben. A legnagyobb előny a gyorsaság, mivel a nyilvános kulcsú titkosítás által használt algoritmusok rendően lassabbak. A szimmetrikus kulcsú titkosítás egyetlen problémáját a két végpont közös titkos kulcsban való, a nem biztonságos összeköttetésen keresztüli megegyezése jelenti.*

Amennyiben az A végpont titkosított forgalmat akar eljuttatni a B végpontnak, akkor az A az adatot a B végpont nyilvános kulcsával titkosítja.

A B végpont ezután a saját titkos kulcsa segítségével fejti vissza az üzenetet, mivel a nyilvános kulcsa a titkosból származik. Ez biztosítja egyút-

tal, hogy kizárálag B tudja visszafejteni az üzenetet, hiszen csak ő birtokolja a titkos kulcsot.

Ez a módszer teszi lehetővé, hogy egy biztonságos csatorna (ISAKMP SA) úgy legyen kiépíthető, hogy a további IPSec biztonsági kapcsolatok biztonságosan kicserélhessék a kulcsokra vonatkozó titkos információkat anélkül, hogy minden egyes alkalommal nyilvános kulcsú titkosítást kellene használniuk. A 7.10. ábra mutatja az ISAKMP első és 2. fázisa során használt megállapodási módszer különböző lépéseit.



7.10. ábra. VPN-kapcsolat kiépítése

A 7.10. ábra szemlélteti, hogy az IKE 1. fázisának befejezése előtt a forgalom már titkosítva zajlik. Ez teszi lehetővé az IPSec-kezdeményezések és az IPSec részéről az IKE 2. fázisában végrehajtott kulccsere biztonságos végrehajtását.

Az IPSec biztonsági kapcsolatok és a kulccsere számára nyújtott biztonsági mechanizmuson kívül az ISAKMP más fontos feladatot is ellát. Beállítható arra is, hogy az IPSec SA élettartamát is meghatározza, ami azt vezérli, hogy milyen gyakran kell kulcsokat cserélni a kapcsolat során. Lehetővé teszi azt is, hogy az IPSec SA lebontása és újra létrehozása nélkül a kommunikáció során kulcsot lehessen változtatni. Az önálló IPSec esetén, valahányszor a kommunikáció során kulccserére kerül sor, a létező SA-kat le kell bontani, majd az új kulcsokkal újra fel kell építeni. Mivel az ISAKMP az IPSec számára megállapodik a biztonsági kapcsolatokban, a saját biztonsági kapcsolatával is védve azokat, így a kulcsok menet közben, az SA újraegyeztetése nélkül is kicserélhetők. Ez további előnyét jelenti a magányos IPSec-kel szemben. Lehetővé teszi még a végpontok dinamikus hitelesítését, és az adatok sérülésekének biztosítását is, mindenkor egyirányú kivonatoló algoritmus segítségével.

## 7.4. AZ ÚTVÁLASZTÓ BEÁLLÍTÁSA VPN-VÉGPONTKÉNT

A könyben mindenkorban be akartam mutatni egy útválasztó telephelyközi VPN-ként való beállításának módját. Ezt az adott beállítást azért tartom fontosnak, mert a jelenleg működő útválasztók 80 százalékát a Cisco-útválasztók adják. Úgy éreztem tehát, hogy sok hálózat biztonsága nagymértékben megnövelhető azzal, hogy az útválasztót tessük a VPN végpontjává.

### 7.4.1. AZ ISAKMP BEÁLLÍTÁSA

Az IKE kizárolag az IPSec biztonsági kapcsolatának létrehozásához kell, de mielőtt ez megtörténhetne, meg kell állapodnia a másik végponttal egy biztonságos kapcsolatban (egy ISAKMP SA-ban). Mivel az IKE megállapítja a saját szabályait, így különböző konfigurációs beállításokkal többszörös szabályok is beállíthatók, majd rábízható a végpontokra, hogy a ténylegesen használni kívánt szabályokban megegyezzenek. Az ISAKMP az alábbiakban állapodik meg:

- **Titkosító algoritmus** – A két IPSec-végpont között átvendő felhasználói adatok védelmét szolgálja (DES vagy 3DES).
- **Kivonatoló algoritmus** – Ez a beállítás az adat sérzetlenségét biztosító kivonatoló algoritmust határozza meg (MD5 vagy SHA). Alapértelmezés az SHA-1. Az MD5 hasonlóan kivonatol, azonban kissé lassabbnak tartják az SHA-1 algoritmusnál.
- **Hitelesítés** – RSA-aláírások, titkosított véletlen számok vagy előre megbeszélt kulcsok. Ez a beállítás az egyes IPSec-végpontok azonosságát hitelesítő módszert határozza meg. Az előre megbeszélt kulcsok a hálózat növekedésével egyre nehezebben használhatók, azonban a kisebb hálózatokban könnyebb a beállításuk a többinél.
- **SA élettartama (másodpercben)** – Alapértelmezésben 86 400 másodperc, vagyis 24 óra. Alapvetőként kijelenthető, hogy a rövidebb élettartam (egy adott pontig) biztonságosabb IKE-megállapodást jelent. A hosszabb élettartam esetén a jövőbeli IPSec biztonsági kapcsolatok gyorsabban kialakíthatók.

Minden egyes paraméter kiválasztásánál kompromisszumot kell kötnünk a biztonság és a teljesítmény között. Az alapértelmezett beállítások kellő biztonságot nyújtanak a legtöbb szervezet számára. Amennyiben olyan végponttal kell együttműködni, amely valamelyik paraméternek csupán egyik értékét képes használni, akkor a választhatóság nyilván arra az egyre korlátozódik.

Amikor az IKE megbeszélése elkezdődik, az egyeztetést kezdeményező végpont elküldi a saját paraméter-beállításairól szóló információkat a másik oldalnak, amely megkeresi az egyezőségeket. A távoli végpont az egyezést egy meghatározott prioritás szerint keresi (elsőként a magasabb prioritásúakat), amíg egyezést nem talál.

Egyezőségről akkor beszélhetünk, ha minden fél azonos titkosítást, kivonatolást, hitelesítést és Diffie–Hellman-paraméterértékeket használ, és a távoli fél élettartam-beállítása kisebb vagy legalább egyenlő a kezdeményező által megadott hosszal. Amennyiben az élettartam nem egyezik, a rövidebb (amely csak a távoli fél beállítása lehet) lép életbe.

Amennyiben nem található elfogadható egyezés, az IKE visszautasítja a megállapodást, és az IPSec-kapcsolat nem jön létre. Ha található egyezőség, az IKE befejezi a megállapodást, és az IPSec biztonsági kapcsolatok létrejönnek. Jelenleg az ISAKMP beállítására két módszer létezik:

- Előre megbeszélt kulcsok használata, amelynek előnye a könnyű konfigurálhatóság.
- Egy központi hitelesítő hatóság (*CA – Certificate Authority*) használata. Ez egy olyan harmadik fél, amely bizonyítványok kiadásával és viszszavonásával foglalkozik. minden egyes eszköznek megvan a saját bizonyítvanya és nyilvános kulcsa. Az adott CA valamennyi hozzá tartozó eszköz bizonyítványát és kulcsát képes ellenőrizni és hitelességéről meggyőződni. Ennek a megoldásnak előnye a nagyobb hálózatok igényeihez való jobb alkalmazkodási képesség (átméretezhetőség).

### Megjegyzés

*Az IKE-egyeztetés az UDP 500-as végponton zajlik. Az IPSec az 50 és 51 IP protokollt használja. A sikeres kapcsolat érdekében biztosítani kell, hogy az ezen végpontokra irányuló forgalom a két fél közötti teljes útvonalon engedélyezve legyen.*

A továbbiakban bemutatjuk az előre megbeszélt közös kulcsok használatát, amely az ISAKMP-beállítások túlnyomó többségét adja.

### Előre megbeszélt kulcsok

Amennyiben az IKE hitelesítési eljárása előre megbeszélt kulcsok segítségével történik, akkor a felek mindegyikén be kell állítani ezeket a kulcsokat, vagyis a VPN kialakításához használt eszközök mindeneként kézzel be kell ezeket vinni. Több végpontnak is megadható ugyanaz a kulcs, de sokkal biztonságosabb a végpontpárok mindenekéhez önálló, a töb-

bitől független kulcsot rendelni. Az előre megbeszélt kulcs beállítását a PIX-tűzfalon az alábbi két lépésben kell elvégezni. Jóllehet az IKE ilyen beállítása egyszerű, és nincs szükség hitelesítő hatóságra, azonban a méretezhetősége korlátozott. Az IKE beállítása:

- 1. lépés.** Be kell állítani az ISAKMP-szabálykészletet.
- 2. lépés.** Be kell állítani az ISAKMP-kulcsot.

### Az ISAKMP védelmi készlet beállítása

A következő parancssal lehet létrehozni az ISAKMP-szabályobjektumot. Megadható több szabály is, de ebben a példában csak egyet mutatunk be:

```
INRG1(config)#crypto isakmp policy 1  
INRG1(config-isakmp)#{
```

A következő group parancssal megadható, hogy a Diffie–Hellmann-számítás során milyen méretű legyen a modulus:

```
INRG1(config-isakmp)#group 2
```

Az 1-es csoport 768 bit hosszú, a 2-es 1024. Miért használjuk az 1-eset és nem a 2-eset? Először is, nem minden gyártó eszköze képes használni a 2-es csoportot. Másodszor a 2-es csoportnak jelentősen nagyobb a CPU-igénye, mint az 1-esé. Éppen ezért a kisebb útválasztókon, például a Cisco 2500 (vagy kisebb) sorozat tagjain nem célszerű a 2-es csoport használata. A 2-es csoport azonban nyilván nagyobb biztonságot nyújt.

Mivel jelenleg a legfontosabb tényező a minél nagyobb biztonság, így a példában a 2-es csoportot állítjuk be (persze meg kell győződni arról, hogy a másik végponton szintén a 2-es csoport van beállítva). Az alapértelmezett az 1-es csoport. Amennyiben az alapértelmezett beállításokat választjuk, az 1-es csoportot használó sorok nem jelennek meg a konfigurációs parancs kilistázásánál.

A következő parancssal kivonatoló algoritmusként az MD5-öt állítjuk be. Jóllehet mind az SHA, mind az MD5 implementálása kötelező, nem minden végponton van beállítva mindkettő.

```
INRG1(config-isakmp)#hash md5
```

A következő parancs megadja a biztonsági kapcsolat élettartamát – ebben az esetben 500 másodperct. Amennyiben nem állítunk be külön élettartamot, az alapértelmezett értéke 86 400 másodperc (egy nap). Az élettartam lejártával a biztonság fokozása érdekében a biztonsági kapcsolatban a feleknek újra meg kell állapodniuk.

INRG1(config-isakmp)#lifetime 500

Az alábbi parancssal a hitelesítéshez használni kívánt kulcs adható meg.

INRG1(config-isakmp)#authentication pre-share

Az előre megosztott (pre-share) lehetőségen kívül a hitelesítési kulcs megadására két további lehetőség adódik:

- rsa-enr – Az RSA-titkosítású kitűző (*nonce*) használatát írja elő
- rsa-sig – Az RSA-aláírás használatát írja elő.

Ezek ismertetésétől eltekintünk, elegendő azt megjegyezni, hogy az rsa-sig az alapértelmezés.

### Az ISAKMP-kulcs beállítása

A következő parancs mondja meg, hogy az IKE mely kulcsot használja. Jegyezzük meg, hogy a végpont (jelen esetben a 192.168.10.38 című gép) beállításának ugyanezt a kulcsot (Ita1Automata) kell tartalmaznia.

```
INRG1(config-isakmp)#exit
INRG1(config)#crypto isakmp key Ita1Automata address
192.168.10.38
```

Ezzel befejeztük az IKE beállítását. Nézzük meg egy helyen, hogy milyen parancsokat is használtunk:

```
INRG1(config)#crypto isakmp policy 1
INRG1(config-isakmp)#group 2
INRG1(config-isakmp)#hash md5
INRG1(config-isakmp)#lifetime 500
INRG1(config-isakmp)#authentication pre-share
INRG1(config)#crypto isakmp key Ita1Automata address
192.168.10.38
```

## 7.4.2. Az IPSEC BEÁLLÍTÁSA

Akár előre megbeszélt kulcsokat, akár hitelesítő hatóságot használunk, az IKE beállítása után még be kell állítani az IPsec paramétereit is. Függetlenül a használt IKE-módszertől, az IPsec beállításának lépései ugyanazok:

- 1. lépés.** Létre kell hozni a kiterjesztett ACL-t.
- 2. lépés.** Létre kell hozni az IPSec-átalakításokat.
- 3. lépés.** Létre kell hozni a titkosítási leképzést.
- 4. lépés.** Alkalmazni kell a titkosítási leképzést az interfészre.

### **1. lépés. Kiterjesztett ACL létrehozása**

A következő parancs egy egyszerű ACL, amely lehetővé teszi az útválasztók egymással való kommunikációját (például az egyikről a másikra való Telnet kapcsolatot).

```
INRG1(config)# access-list 101 permit ip host 192.168.10.38  
host 192.168.10.66
```

Egy ennél életszerűbb ACL nagyjából az alábbi parancssal hozható létre:

```
INRG1(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255  
10.3.2.0 0.0.0.255
```

Ez a parancs egy közönséges kiterjesztett ACL, ahol 192.168.3.0 az adott útválasztó mögötti hálózati szegmens, a 10.3.2.0 pedig a másik végpontként funkcionáló útválasztó mögötti hálózati szegmens. Ne feledjük, a hozzáférési listán az engedélyezés ezúttal titkosítást jelent, a tiltás pedig a nem titkosított küldést.

### **2. lépés. IPSec-átalakítások létrehozása**

Az átalakítás egy biztonsági protokollt (AH vagy ESP), és a hozzá tartozó algoritmust írja le. Ilyen például az ESP a DES titkosító algoritmus-sal, és a HMAC-SHA a hitelesítéshez. Az átalakítási készlet a biztonsági protokollok és algoritmusok egy adott készletét jelenti. Az IPSec biztonsági kapcsolatban való megállapodás során a felek egy adott átalakítási készletben egyeznek meg, amellyel az adott adatfolyamot védeni kívánják. Több átalakítási készlet specifikálható, majd ezek egyike, vagy közülük több megadható a titkosítási leképzések bejegyzéseként. Az IPSec a titkosítási leképzési bejegyzésben megadott átalakítási készletet használja az IPSec biztonsági kapcsolatban való megállapodás során az ugyanazon leképzés hozzáférési listájában specifikált adatfolyam védelmére. Az IKE-vel végzett IPSec biztonsági kapcsolatról történő megállapodás során a felek megegyeznek abban a készletben, amely minden két végpontron azonos. Ha találnak ilyen készletet, akkor azt kiválasztják, és az IPSec biztonsági kapcsolat részeként minden két oldalon alkalmazzák. A biztonsági kapcsolatok kézi beállításakor nincs ilyen megállapodás a felek között, így minden két oldalon ugyanazt az átalakítási készletet kell beállítani.

Hozzunk létre három átalakítási készletet a következő parancsokkal:

```

INRG1(config)#crypto ipsec transform-set MedvePapa esp-rfc1829
INRG1(cfg-crypto-trans)#exit
INRG1(config)#crypto ipsec transform-set MedveMama
    ah-md5-hmac esp-des
INRG1(cfg-crypto-trans)#exit
INRG1(config)#crypto ipsec transform-set MedveGyerek ah-rfc1828
INRG1(cfg-crypto-trans)#exit

```

Az első készlet kizárálag az ESP-t használja, a második kombinálja azt az AH-val, a harmadik pedig kizárálag az AH-t specifikálja. Az IPSec SA megállapodás során minden kompatibilitásra felajánlja a másik végpontnak, amelyik kiválaszt közülük egyet. Mindhárom átalakítási készlet az alapértelmezett alagútmódot használja. Az átalakítási mód kizárálag akkor használható, ha a titkosítási végpontok egyben a kommunikációs végpontok is. Az átalakítási készlet beállítása után kiadott mode transport parancssal állítható be az átalakítási mód. A VPN során elsősorban az alagútmódot használja.

Jegyezzük még meg, hogy az esp-rfc1829 és ah-rfc1828 az ezen technológiák eredeti RFC-jén alapulnak, amelyek a visszafelé kompatibilitás érdekében használt, ma már elavult technológiák. Ezeket az átalakítási készleteket már nem minden gyártó támogatja, mások azonban kizárálag ezek használatát engedik. Azt is vegyük észre, hogy a fent megadott három mód nem feltétlenül a legpraktikusabb. Így például mind a „MedvePapa”, mind a „MedveGyerek” kifogásolható átalakítási készlet, ugyanazon készletben mindenkorrel egyszerre kellene használni inkább.

### 3. Lépés. Titkosítási leképezés létrehozása

A titkosítási leképezés specifikálja az IPSec-szabályokat. Az IPSec-hez létrehozott bejegyzései egyesítik az IPSec biztonsági kapcsolatok felállításához szükséges különböző biztonsági beállításokat, beleértve a következőket:

- Milyen forgalmat kell védeni az IPSec által (titkosítási hozzáférési listánként).
- Hová kell küldeni az IPSec által védett forgalmat (mi a másik oldal).
- Az IPSec-forgalom során használt helyi cím.
- Milyen IPSec-biztonságot kell használni a forgalom során (az egy vagy több átalakítási lista közül kiválasztva a megfelelőt).
- A biztonsági kapcsolatokat kézzel vagy az IKE által automatikusan hozzuk-e létre.
- Egyéb, az IPSec SA definiálásához fontos paraméterek.

Ahhoz, hogy két végpont között sikeresen létrejöjjön az IPSec-kapcsolat, minden fél titkosítási leképzésének tartalmaznia kell egymással kompatibilis beállításokat. Amikor a két fél megkísérli létrehozni a biztonsági kapcsolatot, legalább egy olyan bejegyzést kell találniuk, amelyik kompatibilis a másik oldali bejegyzés által meghatározott módszerekkel.

Az `ipsec-isakmp` tag használata mondja meg az útválasztónak, hogy az adott titkosítási leképzés egy IPSec-beállítás. Jóllehet a példában csupán egy végpontot deklaráltunk, egy adott leképzési bejegyzés több végpontot is meghatározhat. A kapcsolati kulcs élettartama megadható méretre (kilobájtokban, vagyis adott mennyiségű forgalom után kulcsot kell cserélni), vagy időtartamra, amint az alábbi parancsok is szemléltetik. A cél természetesen az, hogy az esetleges támadó dolgát minél jobban megnehezítsük:

```
INRGI(config)#crypto map armadillo 10 ipsec-isakmp
INRGI(config-crypto-map)#set peer 192.168.10.38
INRGI(config-crypto-map)#set session-key lifetime seconds 4000
INRGI(config-crypto-map)#set transform-set MedveMama
    MedvePapa MedveGyerek
INRGI(config-crypto-map)#match address 101
```

A `set transform-set` parancssal adhatjuk meg a leképzéshez hozzárendelt átalakítási készleteket. A felsorolás sorrendjének is van jelentősége. Ebben a beállításban a MedveMama a leginkább kívánatos készlet, a legkevésbé kívánatos, de még elfogadható a MedveGyerek készlet.

A titkosítási leképezés hozzáférési listát az IPSec-alagútba irányuló IPSec-csomagokat továbbító kimenő interfészhez kell rendelni. Az alagútbeli érkező IPSec-csomagok hitelesítése és visszafejtése az IPSec feladata, amelyet az alagút azonosítójának megfelelően végez.

A `match address 101` parancs csupán azt jelenti, hogy a 101-es számú hozzáférési listát kell használni a megfelelő forgalom kiválasztásához.

Ugyanazon névvel (armadillo), de különböző sorszámmal több titkosítási leképzés is létrehozható (lásd az alábbi parancsok). Ez lehetővé teszi számunkra, hogy a hagyományos és az IPSec-titkosítást vegyesen használjuk. A PFS beállítás még itt is módosítható. A megadott példában a PFS első csoport az alapértelmezett.



*Mi történik, ha egy csomag nem felel meg a titkosításban meghatározott feltételeknek? A válasz egyszerű: az ilyen csomagokat eldobja.*

#### 4. lépés. A titkosítási leképzés interfészhez rendelése

A következő parancssal rendelhető leképezés egy interfészhez. Ne feledjük, hogy a leképzést a kimenő interfészhez kell rendelni, nem a bejövőhöz. Ha ugyanezen interfészhez több leképzést is hozzá akarunk rendelni, akkor a nevét egyszerűen fel kell sorolni a crypto map parancsban.

```
INRGI(config)#int e0
INRGI(config-if)#crypto map armadillo
```

Jegyezzük meg, hogy a titkosítási leképzések és hozzáférési listáik egyaránt irányalapúak (vagy kifelé vagy befelé irányúak). A hozzáférési listának nem megfelelő forgalmat pedig továbbra is titkosítás nélkül fogja továbbítani.

## 7.5. A TŰZFAL VPN-BEÁLLÍTÁSA A KLIENS-HOZZÁFÉRÉS SZÁMÁRA

A Cisco PIX-tűzfalak beállíthatók úgy is, hogy a kliensek számára biztosíták a VPN-hozzáférést, hogy a felhasználók távolról is biztonságosan érhessék el a vállalat erőforrásait.

Az IKE-vel használva a biztonsági leképzések megkönnyítik az IPSec beállítását. Ez a módszer olyan hálózatokban ajánlható, ahol a másik oldali felek nem határozhatók meg előre. A VPN-kliensek (például mozgó felhasználók) és a dinamikusan kapott IP-című útválasztók számára dinamikus titkosítási leképzések használhatók.

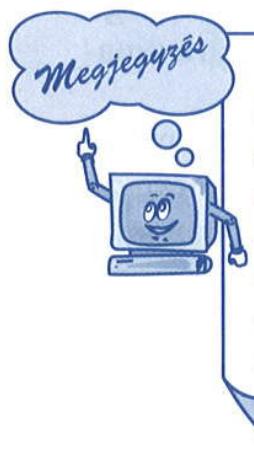
A dinamikus titkosítási leképzések csak a kapcsolatot kezdeményező végponttal folytatott, a biztonsági kapcsolatban a megállapodásra irányuló kommunikáció során használhatók. Nem alkalmazhatók azonban a távoli féllel való kapcsolat kezdeményezésére. A dinamikus leképzés esetén, ha a kimenő forgalom megegyezik a hozzá tartozó hozzáférési lista egy engedélyező utasításával, és a megfelelő biztonsági kapcsolat még nincs kiépítve, a PIX-tűzfal egyszerűen eldobja a forgalmat.

A dinamikus titkosítási leképzés egyszerűen egy olyan bejegyzés, amelynek minden paramétere előre beállítva. Tulajdonképpen szabálysablonként viselkedik, amelyben a hiányzó paramétereket később dinamikusan kell beállítani (az IPSec-megállapodás során), hogy azok megfeleljenek a másik fél kíváncsainak. Ez teszi lehetővé a végpontok számára, hogy a PIX-tűzfal IPsec-forgalmat bonyolíthassanak le még abban az esetben is, amikor az adott tűzfalnak nincs olyan beállítása, amely pontosan megfelelne a végpont valamennyi kívánságának. A dinamikus leképzések a számítógépeken futó VPN-klienseknek állnak rendelkezésre.

Ha a PIX-tűzfal fogadja a végpont kérését, akkor installálja az új IPSec biztonsági kapcsolati beállításokat, valamint egy ideiglenes titkosítási leképzési bejegyzést. Ezt a bejegyzést az egyeztetés eredményének megfelelően tölti ki. Ettől kezdve a PIX-tűzfal a szokott módon üzemel tovább, az ideiglenes bejegyzést hagyományos bejegyzésként kezelve, és az éppen használt biztonsági kapcsolatok élettartamának lejártakor még újakat is képes létrehozni vele (az ideiglenes bejegyzés élettartam-beállításainak megfelelő módon). Amikor az adatfolyam megszűnik (vagyis valamennyi hozzá tartozó biztonsági kapcsolat élettartama lejár), az ideiglenes bejegyzést törli.

Akárcsak a szokásos titkosítási leképzési bejegyzések, a dinamikus bejegyzések is készletekbe vannak csoportosítva. A készleteket az azonos dinamikus leképzési névvel rendelkező bejegyzések alkotják, amelyek azonban különböző dinamikus sorszámmal vannak ellátva. Ha ez van beállítva, akkor a titkosított kapcsolatot kezdeményező IPSec végpont azonosítójának a leképzési készlet hozzáférési listájában szerepelnie kell. Ha ez a beállítás hiányzik, akkor a PIX-tűzfal a végpontok által kezdeményezett bármely adatfolyamot elfogadja.

Az adott dinamikus leképzési készletre hivatkozó bejegyzések útján egy vagy több másik dinamikus készlet is hozzáadható a készlethez. A bejegyzéseket úgy célszerű beállítani, hogy a hivatkozott más készletek kisebb prioritásúak legyenek a tényleges bejegyzéseknel (vagyis alacsonyabb hivatkozási sorszámuk legyen).



*Nagyon figyeljünk oda, ha a dinamikus titkosítási leképzések során a permit bejegyzésben az any kulcsszót akarnánk használni. Amennyiben ez a bejegyzés lefedheti a többesküldésű vagy általános című üzeneteket is, akkor a hozzáférési listának a megfelelő címtartományra deny bejegyzéseket is tartalmaznia kell. A hálózati és alhálózati forgalom számára is be kell állítani a deny bejegyzéseket, és minden olyan forgalomra, amelynek során nem kívánjuk használni az IPSec-biztonságot.*

A dinamikus bejegyzés létrehozására szolgáló eljárás megegyezik a korábban ismertetett módszerrel. Egyetlen kivételként nem statikus titkosítási leképzési bejegyzést, hanem dinamikust kell létrehozni. A statikus és dinamikus bejegyzések vegyesen is használhatók egy adott leképzési készletben. A dinamikus bejegyzés előállítása során az alábbi lépéseket kell megtenni:

**1. lépés.** Rendeljünk egy hozzáférési listát a dinamikus leképezési bejegyzéshez:

```
crypto dynamic-map dinamikus-leképzés-neve dinamikus-sorszám
    match address hozzáférési-lista-neve
```

Ez határozza meg, hogy mely forgalmat kell védeni, és melyet nem. Példa:

```
crypto dynamic-map dyn1 10 match address 101
```

Ebben a példában a 101-es számú hozzáférési listát rendeljük a dyn1 nevű dinamikus leképezési bejegyzéshez. A leképzés sorszáma a 10 lesz.

**2. lépés.** Megadjuk, hogy mely átalakítási készletet engedélyezzük ezzel a dinamikus bejegyzéssel. Több átalakítási készlet is felsorolható prioritásuk sorrendjében (a legmagasabb prioritású szerepel elsőként):

```
crypto dynamic-map dinamikus-leképzés-neve dinamikus-sorszám
    set transform-set átalakítási-készlet-nevel
        [, átalakítási készlet-neve2, ..., átalakítási-készlet-neve9]
```

Példa:

```
crypto dynamic-map dyn 10 set transform-set myset1 myset2
```

Ebben a példában ha a forgalom megfelel a 101 listának, a biztonsági kapcsolat egyaránt használhatja a myset1 és a myset2 készletet attól függően, hogy a végpont beállításai melyiknek felelnek meg. Elsőként a myset1 kerül ellenőrzésre, s csak meghiúsulása esetén ellenőrzi a myset2 készletet is.

**3. lépés.** Megadja a dinamikus bejegyzés élettartamának hosszát. Akkor kell ezt használni, ha az általános beállításoktól el kell térni:

```
crypto dynamic-map dinamikus-leképzés-neve dinamikus-sorszám
    set security-association lifetime {seconds másodpercek |
        kilobytes kilobájtok}
```

Példa:

```
crypto dynamic-map dyn1 10 set security-association lifetime
    seconds 2700
```

A példában a „dyn1 10” dinamikus bejegyzés élettartamát 2700 másodperc-re (45 percre) állítjuk be.

**4. lépés.** Meghatározza, hogy az IPSec-nek kell-e kérnie FPS-t a dinamikus bejegyzés-sel vezérelt új biztonsági kapcsolat létrehozásakor, vagy a végponttól követelje-e meg azt a kérés részeként:

```
crypto dynamic-map dinamikus-leképzés-neve dinamikus-sorszám
    set pfs
        [group1 | group2]
```

Példa:

```
crypto dynamic-map dyn1 10 set pfs group1
```

**5. lépés.** A dinamikus leképzési bejegyzést hozzáadja egy statikus leképzési készlethez. Mindig győződjünk meg arról, hogy a dinamikus bejegyzéseknek legyen a legkisebb prioritásuk (legnagyobb sorszámuk) a készletben.

```
crypto map leképzés-név sorszám ipsec-isakmp dynamic  
dinamikus-leképzés-neve
```

Példa:

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

## 7.6. ÖSSZEFoglalás

Ebben a fejezetben megtárgyaltuk, hogy mi is az a VPN, és milyen általános előnyökkel jár a használata. A VPN implementálásának legnagyobb előnye a költségek csökkentése és az általános gazdasági megtakarítás. A sávszélességi költségek megtakarítása tette a VPN-t az elérhető legjobb megoldássá.

Ebben a fejezetben a legjobb létező VPN-ekre koncentráltunk: az IPSec-alapú VPN-re. Az adatvédelmi képesség megértése érdekében megvizsgáltuk mindeneket a különböző szinteket, meneteket és eljárási típusokat, amelyek az IPSec-alapú VPN-ben az adatok biztonságának megőrzéséhez szükségesek. Ez valóban lenyűgöző feladat volt, hiszen az érintett problémák bonyolultsága gyorsan növekszik.

## 7.7. Összefoglaló kérdések

1. Van-e lehetőség titkosítás nélküli VPN felállítására?
2. Sorolja fel a VPN három típusát!
3. Válassza ki a VPN három jellemzőjét és előnyét, és mutassa meg, hogy az ön vállalata miként tud belőlük használ húzni!
4. A VPN-koncentrátorokat sok felhasználó igényeihez alakították ki. Mutassa be, hogy hány felhasználóhoz és mikor célszerű a használtuk!
5. Mikor következik be az alagút megosztása?
6. Milyen szerepe van a hitelesítésnek az adatfolyam biztonságában?
7. Milyen protokollok játszanak szerepet, amikor az adatot az IPSec-alagútban küldjük?
8. A telephelyközi VPN esetén melyik a két különböző csomagoló protokoll, és mi közöttük a különbség?
9. Nevezze meg az IKE előnyeit!