Az internet a barangolások és felfedezések számára nagyszerű terepet biztosít. Hasonlították már a vadnyugathoz és az emberiség más nagyszabású felfedezéseihez. A valóságban az internet csupán a szerverek és útválasztók (routerek) óriási halmaza, amelyek együtt az írott történelem legnagyobb nagy kiterjedésű hálózatát *(WAN – Wide Area Network)* alkotják. A hálózati kütyük ezen halmazában megtalálhatók a levelezőszerverek, a webhelyek és más információtároló és -lekérdező rendszerek, amelyek mind az internethez csatlakoznak, s amelyek a szintén az internethez csatlakozó emberek számára elérhetők. Szokták azt is mondani, hogy az internet az emberiség összegyűjtött általános tudásának egészét tartalmazza.

Micsoda hatalmas lehetőség! Az emberiség évezredek alatt összegyűjtött teljes ismeretanyaga ott tárolódik a mágneses adathordozókon, és várja azokat, akik letöltik és megtanulják. Már könyveket írtak az internet hatalmas lehetőségeiről, és az életünkre tett kihatásairól. Ebben a könyvben azonban a biztonsággal foglalkozunk, ezért az érdekel minket a legjobban, hogy miként védhetjük meg ezt a hihetetlen mennyiségű információt.

Vannak-e olyan szervezetek, amelyek fenntartják a rendet az interneten, ahogy a rendőrség tartja azt fenn a közutakon? Létezik-e olyan világszervezet, amely mindenbe beleüti az orrát, és alaposan ellenőrzi az internetre kapcsolódó valamennyi eszközt? Ezekre a kérdésekre csak nemleges válasz adható, nincs olyan szervezet, amely az internet védelméért felelne. Az internet termeiben felhalmozott tudás biztonsága és a termekbe vezető bejárók karbantartása arra a személyre vagy személyekre tartozik, akinek vagy akiknek az adott információ publikálása eleve a feladata. Minden egyes webhelyhez egy vállalati internetkapcsolaton vagy egy internetszolgáltatón keresztül vezet az út. Az ő feladatuk megakadályozni a kalózokat abban, hogy a webhelyen található fáradságos munkával összeállított és katalogizált információt tönkre ne tehessék. S miként lehet megvédeni az internetről elérhető webhelyet, levelezőszervert, FTP-szervert vagy más információforrást? Egy szóval megadható a válasz: tűzfallal. Ezeket a hardvereszközöket kifejezetten azzal a céllal tervezték, hogy a hálózat számára védelmet nyújtsanak.[1]

A tűzfal *(firewall)* egy olyan biztonsági berendezés, amely a védett hálózat internetcsatlakozásaként működik, határátlépőként védve a mögötte elhelyezkedő tartományt. Mindkét irányban állandóan figyeli a ke-

1 Soha ne essünk abba a hibába, hogy túlbecsüljük a tűzfal által nyújtott védelmet. A tűzfal csupán egy eszköz, amely mit sem ér az e könyvben is többször hangsúlyozott komplex, többrétegű biztonsági rendszer nélkül. Ha a tűzfalat önmagában használjuk, csupán hamis biztonságérzetbe ringatjuk magunkat. *(A lektor megj.)*

resztülhaladó forgalmat, miközben az előre rögzített szabályoknak megfelelően bizonyos részeit feltartóztatja vagy visszafordítja. A tűzfal a törvények nélküli teljes web számára maga a törvény és a védelem. Mindig éberen védi a hozzá csatlakoztatott belső hálózati erőforrásokat.

Az internet a felhasználók számára olyan mennyiségű információk elérését tette lehetővé, hogy az évek során ez a hozzáférési lehetőség mind az egyének, mind a vállalkozások számára gyakorlatilag nélkülözhetetlenné vált. A saját információink internetről elérhetővé tétele azonban lehetővé teszi, hogy bizalmas vagy kritikus adatainkat bármikor és bárhonnan a világból megtámadhassák – az internet szó szerint egy világméretű hálózat. Ez azt jelenti, hogy Budapestről csatlakozva az internethez, kiteszem magam az Amerikából, Ázsiából, a Közel-Keletről és a világ más részeiről érkező támadásoknak. A helyesen használt tűzfalak védhetik meg az egyes számítógépeket vagy akár az egész vállalati hálózatot attól, hogy az internetről ellenséges behatolók törjenek be rájuk. Helyesen használni azonban csak alapos megismerésük után lehet őket.

Ennek az évi 365 napon keresztül napi 24 órás szolgálatot teljesítő elektronikus „robotzsarunak" nagyon fontos feladata van: tartsa távol a rossz fiúkat, azonban ne akadályozza a jókat a munkájukhoz szükséges erőforrások elérésében. Tulajdonképpen egyszerűnek hangzik, igaz? Így papíron leírva valóban olyan könnyűnek tűnik, mint az egyszeregy, a valóságban azonban egy tűzfal megfelelő beállítása sok tervezést igénylő, felelősségteljes, nehéz feladat.

Bizonyos esetekben egy rosszul beállított, vagy nem megfelelő jellemzőkkel rendelkező tűzfal nagyobb bajt okozhat, mintha egyáltalán nem lenne tűzfal. Nehéz elhinni, ugye? Sajnos mégis igaz. Ebben a fejezetben sorra vesszük a tűzfal feladatait, működésének mikéntjét megértendő.

5.1. Gyakran ismételt kérdések a tűzfalakkal kapcsolatban

Mielőtt megkezdenénk a tűzfal általános működésének vizsgálatát, megvizsgáljuk és megválaszoljuk az őket körülvevő leggyakrabban feltett alapvető kérdéseket.

5.1.1. Kinek van szüksége tűzfalra?

Ez egyike a talán leggyakrabban feltett biztonsággal kapcsolatos kérdéseknek. Amennyiben terveink között szerepel az internethez való kapcsolódás, akkor szükségünk van a tűzfalra. Teljesen mindegy, hogy otthonról

csatlakozunk vagy a vállalatunk hálózata csatlakozik – szükségünk van a tűzfalra, és pont. Az otthonok egyre nagyobb számban rendelkeznek állandó szélessávú internetkapcsolattal, ami az otthoni gépek védelmét egyre fontosabbá teszi.

5.1.2. Miért van szükségem a tűzfalra?

Szinte naponta hallani a hírekben vagy olvashatunk az újságokban új biztonsági kockázatokról: vírusokról, férgekről, szolgáltatásmegtagadási *(DoS – Denial of Service)* támadásokról, gépfeltörésekről és számítógépeink egyre újabb, felismert hiányosságairól. A közelmúltból nyilván mindenkinek ismerősek a SoBig, Blaster, LovSan, Nimda és MyDoom nevek, amelyek mind szerepeltek a hírekben. Még ha nem olvasnánk újságot és néznénk vagy hallgatnánk a híreket, akkor is legalább egyikük neve szinte bizonyosan ismerősen csengene.

Nem titok: a gépkalózok működnek, és állandóan el akarnak kapni minket. Gyakran nem tudjuk, hogy pontosan kik ők, de tudjuk, hol lapulnak, akárcsak azt, hogy hol nem akarjuk őket látni (a hálózatunkon!). A régmúlt kalózai állandóan a tengereket rótták, manapság pedig a gépkalózok állandóan az interneten kóborolnak. Nyilván nem akarjuk őket beengedni a saját hálózatunkba, hogy az azt alkotó gépek között kóborolhassanak.

Tudjuk tehát, hogy meg akarjuk védeni a hálózatunkat ezektől a támadóktól, ennek pedig egyik leghatékonyabb módja éppen a tűzfal beüzemelése. Alapértelmezés szerint bármelyik jó tűzfal képes arra, hogy megakadályozza a védett hálózat és az internet közötti forgalmat. Ez nem azt jelenti, hogy a tűzfal minden forgalmat megtilt – ez az internetcsatlakozás célját és szükségességét kérdőjelezné meg. Sokkal inkább azt jelenti, hogy beállítása értelmében például csupán a webszerver (HTTP/port 80) (illetve más engedélyezett szolgáltatás) érhető el az internetről. Ennek érdekében a tűzfal minden egyes beérkező csomag esetén állapotteljes csomagvizsgálatot *(SPI – Stateful Packet Inspection)* végez, amelyet a 2. fejezetben már tárgyaltunk.

A tűzfal beüzemelésének egyetlen alternatívája az, hogy a hálózatunkba irányuló minden csatlakozási kísérletet jóváhagyunk, miközben még csomagvizsgálatot sem végzünk, így nem deríthetjük fel azt sem, hogy nem zajlik-e a csomagokba rejtve valamilyen külső támadás. Ezért egyáltalán nem tanácsos a tűzfal kihagyása, amelynek hatására gyakorlatilag bárki által sebezhetővé válunk, akinek van internetkapcsolata.

5.1.3. VANNAK-E MEGVÉDENDŐ ÉRTÉKEIM?

Gyakran hallhatjuk másoktól: „Megértem, hogy ha lenne bármi értékes, megvédendő a hálózatomon, akkor feltétlenül szükségem lenne egy tűzfalra. Nincs azonban semmi olyasmim, amire egy támadónak szüksége lehetne, miért aggódnék hát a tűzfal hiánya miatt?"

A hálózatok és a hálózati erőforrások ugyancsak fontosak a társadalom működése és az üzlet általános lebonyolítási módjai szempontjából. Gyakorlatiasabban megfogalmazva ez azt jelenti, hogy a hálózatunk és erőforrásai, illetve hatékony működésük önmagában is érték. A hálózatok megnövekedett szerepe azt jelenti, hogy valamilyen mértékben határozottan van mit féltenünk, amint az a következő felsorolásból is látható.

- **Közvetítői felelősség** – Úgy hangzik, mint valami ostoba tévéműsor címe, pedig valójában az internet jogi szabályozottságához szükséges következő nagy lépést takarja. Alapvetően arról van szó, hogy egy támadónak sikerült hozzáférést szereznie egy számítógéphez (a miénkhez), amit egy harmadik fél megtámadására használt fel. Tegyük fel, hogy a támadó a vállalatunk számítógépére tört be. Ebben az esetben a vállalat elmarasztalható lehet azért, hogy elmulasztotta kellőképpen védeni a saját rendszereit, így közvetve hozzájárult a harmadik félnek okozott kárhoz. A támadó fegyverként használhatta fel a vállalatunk számítógépét. A vállalat tehát felelős azért, mert nem tett meg mindent az ismert kockázat elleni védekezésül – például mert nem üzemelt be egy tűzfalat. A körültekintő embernek ugyanis kötelessége az elvárható óvintézkedések megtétele: „az üzleti élet minden szereplőjétől megkövetelhető, hogy bizonyos magatartási szabályoknak megfelelően viselkedjék, megkímélve így másokat az elkerülhető kockázatok jelentette veszélytől".[2]
- **Elveszett adatok** – Bizonyára mindenki tud arról, hogy egyes vállalatok minden adatukat elvesztették a szeptember 11-i támadás során, és közülük sok nem is volt képes helyreállítani azokat. Mi lenne akkor, ha a vállalatunk elveszítené minden adatát azért, mert nincs tűzfalunk, és egy támadó valamennyi adatunkat letörli? Mi történne ebben az esetben a céggel? Pénzbe kerülne-e, ha mindent újra létre kellene hozni? Eredményezhetné-e az adatok elvesztése a bevételek csökkentését, az üzletektől való elesést?
- **Bizalmas adatok kikerülése** – Minden szervezetnek vannak bizalmasnak minősülő adatai, amelyek elvesztése gazdasági problémákat, jogi nehézségeket, különösen kínos helyzeteket okozhatnak. Ezen adatok lehetnek például a vevők hitelkártyaszámai vagy egy új fogyási módszer

2 Prosser, Wade és Schwartz: Cases and Materials on Torts, 2001.

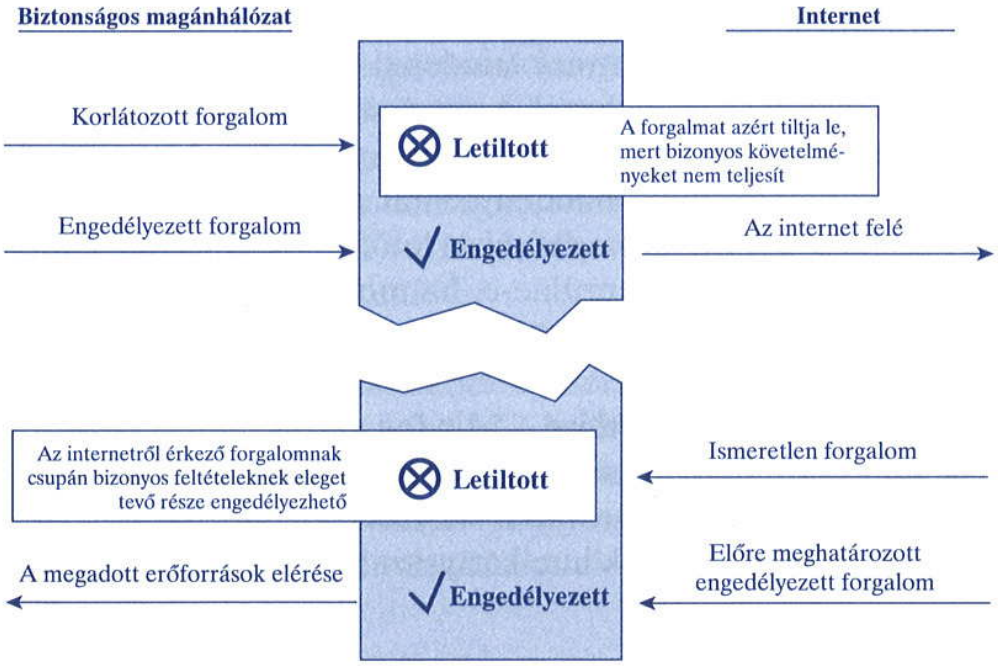
titkos tervei. Előfordulhat, hogy jövőbeli terveink egy versenytárs kezébe kerülnek. A lehetőségek még hosszan folytatódnak, de egy támadás bekövetkezése esetén a legrosszabbakat kell feltételeznünk. Lehet, hogy sokan ezért nem jelentik be a számítógépes bűncselekményeket.

- **Hálózati időkiesés** – Mindennapos dolog a pénzkiadó automatából készpénzt felvenni, vagy vásárolni a hitelkártyánkkal. Az ehhez szükséges eszközök folyamatos működését is egy hálózat teszi lehetővé, amely az esetek többségében kifogástalanul üzemel. Ha azonban nem lennének védve, akkor egy támadó hosszabb-rövidebb időre akár üzemen kívül is helyezhetné őket. Ezen hálózatok üzemkiesése nagyon gyorsan növekvő jövedelemkiesést okoz. Bármely hálózat üzemszünete csapást jelent, amelynek mindig van költsége.

Végezetül még azt tehetjük hozzá, hogy mindenkinek vannak megvédendő dolgai, így a védelem elmulasztása erősen ellenjavallt: csak idő kérdése, hogy mikor következik be valamilyen nem kívánatos esemény. A következő logikus kérdés tehát az, hogy valójában mit is tesz a tűzfal a hálózat védelme érdekében.

5.1.4. Hogyan működik a tűzfal?

A tűzfal állandóan vizsgálja a hálózati interfészeken beérkező forgalmat, és az előre definiált szabályok alapján feldolgozza azt – dióhéjban megfogalmazva, e szabályok alapján engedélyezi vagy letiltja. Amint az 5.1. ábrán látható, a tűzfal mind a kifelé, mind a befelé irányuló forgalmat szűri.



5.1. ábra. A tűzfal működése

A tűzfal a hozzáférés-vezérlő listákhoz (ACL) hasonlóan a cél és a forrás IP-címe, a protokoll és a kapcsolat állapota szerint képes szűrni a forgalmat. Példaként tegyük fel, hogy (a tűzfalon keresztül) a hálózatba irányuló FTP-forgalom általában le van tiltva, ha viszont egy belső felhasználó kezdeményez egy FTP-kapcsolatot, akkor azt a tűzfal mégis engedélyezi, hiszen az adott munkamenet egy belülről kifelé irányuló kezdeményezés hatására jött létre. Alapértelmezés szerint a tűzfalak a megbízható hálózatból (belülről) a megbízhatatlan hálózat felé (kívülre) kezdeményezett kapcsolatokat átengedik.

A tűzfal arra is képes, hogy bizonyos szabályok szerinti kapcsolódási kéréseket naplózzon, illetve bekövetkezésük esetén riasztást adjon le. Végezetül képesek hálózaticím-fordítást (NAT) végezni a belső (privát) címekről nyilvános címekre. A tűzfal működésének áttekintése részben részletesebben ismertetjük az általa betöltött szerepköröket, előbb azonban visszautalunk a 2. fejezetben tárgyalt biztonsági politikára, megvizsgálandó, hogy a tűzfal mennyiben alkalmas ezen szabályok betartatására.

5.2. A TŰZFAL MAGA A BIZTONSÁGI HÁZIREND

Milyen jellegű forgalom engedélyezett befelé a hálózatba és onnan kifelé? Miként védhetjük meg a hálózatunkat a támadásoktól? Mi a biztonsági politikánk? Mi történjék azokkal az emberekkel, akik nem akarják betartani a biztonsági házirendekben foglaltakat? Kinek a felelőssége a biztonsági házirendek írása és frissítése?

Ezek mind fontos kérdések, amelyekre választ kell találni. A hálózat tűzfalon keresztüli internetre csatlakoztatása csak az első lépés a biztonság felé. Mostanra már világosan kell látnunk, hogy a biztonsági házirendek jelentik annak alapját, hogy miként lehet ezeket a szabályokat működőképessé tenni.

Bizonyára mindenki ismeri a szólást: semmilyen munka nincs addig befejezve, amíg a papírmunka nincs készen. Biztonsági megoldás esetén ez úgy módosul, hogy közel sem lehet befejezettnek nevezni mindaddig, amíg a szervezet biztonsági helyzetét meghatározó szabályok és előírások írásos gyűjteménye el nem készül. A szabályok és előírások ezen írásos gyűjteményét nevezzük összefoglaló néven biztonsági házirendnek. A házirend teljesen más természetű és más céllal jön létre, mint a biztonsági terv. Nagyon világosan meg kell értenünk ezt a különbséget, amely a házirendet megkülönbözteti a szervezet által használt más biztonsági dokumentumtól. Pontosan mi is ez a különbség?

A büntetés! Bizony, a biztonsági házirend tartalmazza egyrészt azt, hogy mit szabad és mit nem, de azt is pontosan leírja, hogy mi fog történni azokkal, akik ezeket a szabályokat nem tartják be. A büntetés lehet

- elbocsátás,
- alacsonyabb beosztásba helyezés,
- alacsonyabb beosztásba helyezés és pénzbüntetés,
- lenyakazás,
- golyó általi halálra ítélés,
- nyomban és helyben felkoncolás,
- a fentiek együtt.

A viccet félretéve, a biztonsági házirend köznapi nyelven, érthetően leírja, hogy mik a szabályok, ki tartatja be azokat, és mi történik a szabályokat be nem tartó személyekkel. Összefoglalva tehát alapvetően a felhasználó cselekedeteinek következményéről szól.

A fentiek ismeretében miért állíthatjuk, hogy a tűzfal maga a biztonsági házirend? Egyszerű: a tűzfal minden egyes műveletét a hálózati mérnök vagy az informatikai biztonsági szakember által beállított szabályok alapján végzi. Ezen szabályoknak pontosan meg kell felelniük a biztonsági házirendben leírtaknak. Vegyük elő a szerverszoba hátuljában porosodó nyolccollos cserélhető mágneslemez csomag alól, vagy valamelyik igazgató billegő páncélszekrényének a lába alól azt a régen ott porosodó irattartót, poroljuk le, és győződjünk meg róla! Azt kellene látnunk, hogy a biztonsági házirend a hálózati szabályok listáját tartalmazza, amint arról a 2. fejezetben már esett szó. A házirendben foglalt valamennyi szabályt be kell állítani a tűzfalon is.

Az előző bekezdésben a biztonsági házirend fellelhetőségére vonatkozó tréfásnak látszó helymeghatározás sajnos csak félig tekinthető viccesnek. A szomorú tény az, hogy a legtöbb vállalatnak vagy egyáltalán nincs biztonsági politikája (és így biztonsági házirendje sem), vagy csak régen elavult, még a dinoszauruszok idejéből származó változatai vannak.

A tűzfalnak megadott konfigurációs szabályoknak pontosan meg kell felelniük a vállalat biztonsági házirendjeiben foglalt előírásoknak. Ha megvizsgáljuk a tűzfal konfigurációs állományát, akkor az 5.1. példában látható parancsokat találunk benne (a példában egy Cisco PIX-tűzfal konfigurációjának részlete látható).

A `conduit permit` (átjutási engedély) utasítások szinte bizonyosan megfelelnek a biztonsági házirendben található valamelyik állításnak, amely név szerint felsorolja a védett hálózatba beengedhető protokollo-

kat, és azokat a céleszközöket, amelyekre ez a forgalom eljuthat. Ezen állítások alkotják a vállalati hálózat biztonsági tervét, és a biztonsági házirend definiálja őket.

5.1. példa. PIX-tűzfalszabályok

```
conduit permit tcp host 216.186.xx.xxx eq smtp any
conduit permit tcp host 216.186.xx.xxx eq www any
conduit permit tcp host 216.186.xx.xxx eq pop3 any
conduit permit tcp host 216.186.xx.xxx eq ftp any
```

Napjainkban az átjutási engedélyek egyre inkább átadják a helyüket a hozzáférés-vezérlő listának, mivel a Cisco igyekszik egy adott megoldáshoz közelíteni valamennyi eszközét. A hozzáférés-vezérlő listát a 3. fejezetben tárgyaltuk. A teljesség kedvéért mutatjuk be az átjutási engedélyeket is.

A tűzfal és a házirend hasonlóságának további bizonyítására vizsgáljuk meg a házirendek néhány jellemzőjét, illetve hogy azok mennyiben jellemzik a tűzfalakat:

- A biztonsági házirend leírja, milyen cselekedetekre kerüljön sor bizonyos körülmények bekövetkezése esetén.
- A biztonsági házirend a biztonsági követelményekkel összhangban állandóan változik.
- A biztonsági házirend megadja mind az engedélyezhető, mind az elfogadhatatlan használat jellemzőit.

Ha a biztonsági házirend fenti jellemzőit összehasonlítjuk a tűzfalkonfiguráció képességeivel, akkor pontos egyezést tapasztalunk, amint azt az 5.1. táblázat is szemlélteti.

5.1. táblázat. A biztonsági házirend és a tűzfalkonfiguráció összehasonlítása

	Biztonsági házirend	Tűzfalkonfiguráció
A változó körülményekhez való alkalmazkodás képessége	igen	igen
Állandóan fejlődik, változik	igen	igen
Meghatározza a viselkedést	igen	igen

A jelen fejezet célja természetesen nem az, hogy a tűzfalak biztonsági házirend helyetti alkalmazását ösztönözze. Ehelyett azt kívánja megvilágítani, hogy a biztonságra mint a tervek, szabályzatok és biztonsági eszközök együtteseként, egy egységként tekintsük. A teljes megoldás érdekében gondosan kell tervezni és kivitelezni, nem elegendő a hálózati védelem egyetlen összetevőjére bízni a feladatot. Amikor a tervezés során eljutunk a forgalmat engedélyező és megtiltó tűzfalszabályok meghatározásáig, a korábban elkészített biztonsági szabályzatokból kell kiindulnunk. A tűzfalak tehát a biztonsági házirendek fizikai és logikai megtestesítői.

5.3. A TŰZFAL MŰKÖDÉSÉNEK ÁTTEKINTÉSE

Még a leghosszabb utazás is az első lépéssel kezdődik. Mielőtt belevetnénk magunkat a biztonsági berendezések viselkedésének megismerésébe, mindenekelőtt a tűzfal mágiájának lényegét kell megértenünk.

A legtöbb tűzfal (a legtöbb, és nem mindegyik) az **állapotteljes csomagvizsgálat** *(SPI – Stateful Packet Inspection)* módszerét alkalmazza a kimenő csomagok nyomon követésére, és az ezen csomagokra érkező esetleges válaszok felismerésére. A védett hálózat kimenő csomagokat előállító gépeinek nyilvántartása megakadályozza a csaló vagy kéretlen WAN-csomagok bejutását egy külső hálózati interfészen keresztül.

Úgy is mondhatjuk, hogy a 3. fejezetben tárgyalt SPI-t használó tűzfal felismeri a belső gépek kapcsolatfelvételi csomagjait, nyomon követi a célgéppel folytatott ezt követő forgalmat, és biztosítja, hogy az ettől a céltól érkező válaszcsomagok háborítatlanul visszajussanak a párbeszédet kezdeményező belső géphez.

Azt a tűzfalat, amely tervezése vagy konfigurációja miatt nem végez állapotteljes csomagvizsgálatot, félkésznek nevezhetjük, amelyet nem célszerű a hálózatunk védelmére használni. Ebben a fejezetben elsősorban a kapcsolat állapotát is figyelő tűzfalakra összpontosítunk. Hivatkozásként a Cisco PIX-tűzfalait említhetjük, amelyek mindegyike állapotteljesnek vehető.

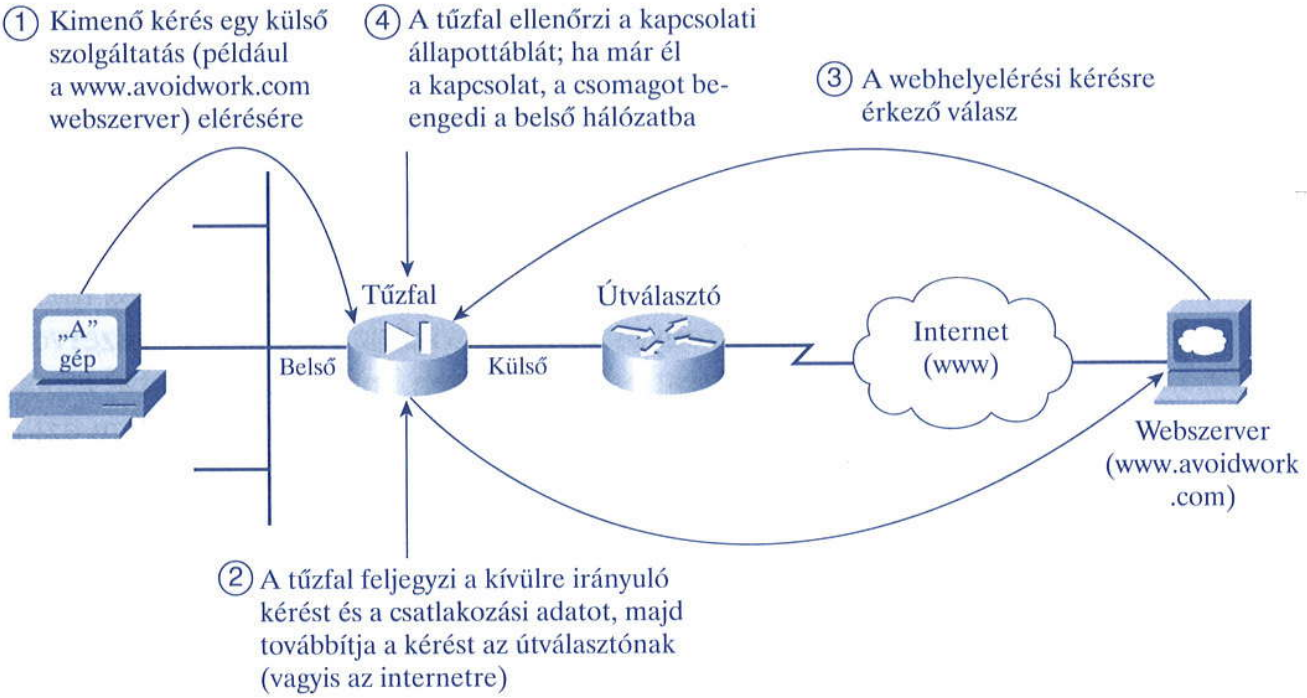
A csomagvizsgálat és csomagszűrés kettős célja a tűzfal egyik legalapvetőbb felelőssége. Az alábbiakban felsoroljuk a tűzfalak leggyakoribb jellemzőit és szabályait:

- **Cél- vagy forráscím alapján a beérkező hálózati forgalom szűrése** – A nem kívánt beérkező forgalom szűrése a tűzfal egyik leggyakoribb jellemzője, és egyben alkalmazásának legfőbb célja is: a nem kívánt forgalom védett hálózatba való bejutásának megakadályozása. A nem kívánatos forgalom általában támadóktól származik, ezért van szükség a kívül tartására.
- **A cél- vagy forráscím alapján a kimenő hálózati forgalom szűrése** – Sok tűzfal a belső hálózatból az internetre irányuló forgalmat is figyeli. Szükség lehet például arra, hogy megakadályozzuk az alkalmazottak számára bizonyos weboldalak elérését, esetleg a belülről induló támadásokat, vagy akár az információ kijuttatását.
- **A hálózati forgalom tartalomszűrése** – A jobb minőségű tűzfal képes a hálózati forgalom tartalmának vizsgálatára. Egy vírusvédő szoftverrel is rendelkező tűzfal például megakadályozhatja a vírusokat tartalmazó állományok bejutását a belső hálózatba. Léteznek e-levelezési szolgáltatást nyújtó tűzfalak is, amelyek a nem kívánatos e-leveleket tudják távol tartani.
- **A belső erőforrások tehermentesítése** – Jóllehet a tűzfal elsődleges célja a nem kívánatos forgalom bejutásának megakadályozása, számos tűzfal beállítható úgy is, hogy bizonyos erőforrásokhoz (például webszerverhez) csak szelektív hozzáférést engedélyezzen, míg az internetről a belső hálózatba irányuló többi forgalmat megtiltja. A legtöbb esetben ezt a demilitarizált zóna (DMZ) megfelelő használatával lehet megvalósítani. A webszerver ilyenkor a DMZ-tartományban helyezhető el. (A DMZ fogalmát részletesebben kifejtjük a fejezet egy későbbi részében.)
- **A belső hálózathoz való kapcsolódás engedélyezése** – Az alkalmazottak belső hálózatra csatlakozásának elterjedt módja a virtuális magánhálózatok *(VPN – Virtual Private Network)* használata. Ezek a vállalati hálózat internetről történő biztonságos elérését teszik lehetővé. Például az ingázók vagy a kereskedelmi utazók is így csatlakozhatnak a vállalati hálózathoz, de használhatók a fiókirodák összekapcsolására is. Bizonyos tűzfalak képesek a VPN-szolgáltatás biztosítására, könnyebbé téve ezen kapcsolatok létrehozását.
- **A hálózati forgalom és a tűzfal tevékenységének naplózása** – Az internetről érkező, illetve az oda irányuló forgalom figyelése során rendkívül fontos lehet a tűzfal pillanatnyi tevékenységének ismerete. Így tudhatjuk meg, hogy ki próbált betörni a hálózatba, és ki akart az interneten meg nem engedett tartalomhoz hozzáférni. A legtöbb tűzfal valamilyen módon biztosítja az ilyen jellegű lekérdezés lehetőségét. A minőségi tűzfalak képesek működésükről naplót is vezetni, vagy a rendszernaplóba, vagy valamilyen archív tárolóterületre. A naplók alapos áttanulmányozása egy támadás felismerése után egyike a rendelkezésünkre álló vizsgálati eszközöknek.

5.3.1. A TŰZFAL MŰKÖDÉSE

A folyamat még pontosabb megértését segítendő érdemes áttanulmányozni az 5.2. ábrát. Célszerű azt összevetni az alábbi listával, amely a működés egyes lépéseit némileg részletesebben ismerteti.

Mielőtt megkezdenénk az ábra és a lista összehasonlítását, fontos felidézni, hogy a legtöbb tűzfalnak két hálózati interfésze van, és ezek 99 százalékban Ethernet-alapúak. Ezen interfészekre belső (védett) és külső (nem védett) névvel hivatkozunk, a hálózatban elfoglalt helyüknek megfelelően. A gyakorlatban tehát a külső interfész csatlakozik az internetre, a belső pedig a megvédendő saját belső hálózatunkra.



5.2. ábra. A tűzfal működése

1. Az „A" gépen a felhasználó megnyit egy webböngészőt, és meg akarja nézni vele a www.avoidwork.com webhelyen található oldalt. A gép elküldi ezirányú kérését a tűzfalon keresztül.
2. A tűzfal észleli az „A" gépről érkező, a www.avoidwork.com irányába küldendő kérést.
   a) A tűzfal megjegyzi a kimenő kérést, és feltételezi, hogy a válasz kizárólag a www.avoidwork.com webszervertől érkezhet.
   b) A tűzfal a munkamenet állapot-nyilvántartó táblájába (amelynek segítségével a kapcsolat a megnyitásától a lezárásáig figyelemmel kísérhető) bekerül a munkamenet azonosítója.
   c) A kapcsolat jellemzői szintén bekerülnek az ezen párbeszédet felügyelő tűzfal által elhelyezett munkamenet-azonosítóba.

3. Az „A" géptől érkező kérésre a www.avoidwork.com webszerver visszaküldi a választ a tűzfalon keresztül.
4. A tűzfal megvizsgálja az állapottábláját azt ellenőrzendő, hogy megtalálható-e benne a befelé irányuló csomaghoz tartozó kapcsolat munkamenet-azonosítója. Ha a munkamenet-azonosítóban tárolt valamennyi jellemző megegyezik, akkor a csomag folytathatja útját a belső hálózatba.

Az állapotteljes tűzfalakkal kapcsolatban még egy utolsó általános megjegyzést érdemes tenni. Amennyiben a tűzfal a kifelé és befelé irányuló kapcsolatok állapotát mindig nyilvántartja és figyeli, akkor a támadó számára rendkívül nehézzé válik a hálózatra való behatolás érdekében a csomagok meghamisítása vagy mesterséges előállítása. Amikor a támadó megkísérli a csomagot átküldeni a tűzfalon, a helytelen vagy hiányzó kapcsolati állapotinformáció azt okozza, hogy a munkamenet lezárul, és nagy valószínűséggel a későbbi vizsgálódások céljára naplózódik.

Számos tűzfal a forrás IP-címét vizsgálja meg annak eldöntéséhez, hogy a csomagot beengedheti-e. A támadó azonban végrehajthat IP-címhamisító (IP spoofing) *támadást is, megváltoztatva a tűzfalnak küldött csomagokban a feladó IP-címét. Ha a tűzfal ezáltal azt hiszi, hogy a csomag egy megbízható gépről származik, hiszen látszólag annak az IP-címéről érkezik, a tűzfal átengedheti ezeket a csomagokat még akkor is, ha más feltételek esetleg nem teljesülnek. Ez a tény ismét megerősíti azt az állítást, hogy önmagában a technológia nem képes valamennyi biztonsági probléma megoldására. Ehhez szükség van a vállalat igazgatóságának közreműködésére is a biztonsági politika kialakításához. A Cisco-tűzfalak önbeállító biztonsági algoritmust* (ASA – Adaptive Security Algorithm) *használnak, dinamikusan hozzácsatolva egy számot a továbbított munkamenetekhez, így a támadó számára még nehezebbé válik ezek feltörése. Bővebb információk (a Cisco-témaszámmal rendelkezők) az alábbi webhelyen találhatók: http://www.cisco.com/en/US/partner/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278b.html#29996.*

5.3.2. A TŰZFAL ALKALMAZÁSA

Manapság zavarbaejtően nagy számú megoldás létezik a tűzfalakra, mindenféle méretben, formában és paraméterekkel kaphatók. Amikor tűzfalat kell üzembe helyezni valahol, elsőként azt kell megfontolni, hogy pontosan milyen elvárásoknak kell megfelelnie.

Az üzembe helyezni kívánt tűzfal típusa a kezelhetőségével és az általa nyújtott biztonsággal kapcsolatos igényektől, valamint az általa védeni

kívánt hálózat méretétől függ. Alapvetően az alábbi kétféle tűzfalmegoldás jöhet szóba:

- **Személyi tűzfal** – A személyi tűzfal *(personal firewall)* alatt általában az egyetlen számítógép védelmére az adott gépen installált valamilyen szoftveres megoldást értjük. Ezekkel leginkább a szélessávú csatlakozással rendelkező otthoni vagy távoli munkahelyként üzemelő gépeket védjük. Egy tűzfal üzembe helyezése persze mindig hasznos. A legismertebb személyi tűzfalak az alábbi helyeken találhatók: http://www.zonelabs.com, http://www.tinysoftware.com, http://www.firewallguide.com.

  Az operációs rendszerek gyártói, például a Microsoft és az Apple úgy válaszoltak az ezzel kapcsolatos megnövekedett igényekre, hogy beépítették rendszereikbe a személyi tűzfalat. Az Apple cég OS X (panther) rendszerébe be van építve egy IP-tűzfal, és a Microsoft Windows XP szintén rendelkezik egy hasonlóval (inkább csak az SP2 óta).
- **Multifunkciós tűzfal** – A multifunkciós tűzfal *(all-in-one firewall)* széles körben elterjedt a szélessávú (DSL vagy kábel) internet-előfizetők körében, hiszen így egyetlen eszközben mindent megtalálnak: útválasztót, Ethernet-kapcsolót *(switch)*, drót nélküli elérési pontot *(access point)* és tűzfalat. Ha az ilyen típusú tűzfal elsőre lenyűgöző is lehet, mindig meg kell győződni a tényleges képességeiről, és gyártótól függetlenül érdemes némileg kételkedni az általa nyújtott biztonságban.

A kábelmodemek a kábeltévé-hálózaton keresztül egy állandó elérésű, nagyon gyors internetkapcsolatot biztosítanak. Ugyanahhoz a kábelhez köthető a tévé és a kábelmodem, és így egy csapásra rendelkezésünkre állhat a nagy sebességű internet-hozzáférés. A DSL ugyenezen előnyöket nyújtja, azonban kábeltévé-hálózat helyett a telefonvonalakat használja az átvitelre.

- **Kisebb-közepes irodai tűzfal** – Az ilyen tűzfalak (például Cisco PIX 501 és 506) a kisebb irodák biztonsági igényeit hivatottak kielégíteni.[3]
- **Vállalati tűzfalak** – Az ilyen típusú tűzfalak (például Cisco PIX 515) az akár több ezer felhasználóval is rendelkező nagyobb vállalkozások

3 Érdemes megemlíteni a több hálózati interfésszel ellátott személyi számítógépre telepített, általában Linux-alapú szoftveres tűzfalakat is. A közepes irodák igényeit ezek is bőven képesek kielégíteni, áruk viszont csupán töredéke a kifejezetten tűzfalnak tervezett hardvereszközökének. *(A lektor megj.)*

számára lettek kifejlesztve. Éppen ezért további lehetőségekkel és nagyobb kapacitással, például nagyobb memóriával és extra-interfészekkel rendelkeznek.

A Cisco-tűzfalak mindegyikén típustól függetlenül ugyanazon operációs rendszer fut, amelynek ugyanazon naplózási/listázási és kezelési lehetőségei vannak. A nagyobb modelleket akkor érdemes választani, ha nagyobb kapacitásra és az egyidejűleg kezelt kapcsolatok nagyobb számára van szükség.

Hagyományosan a tűzfalak a belső hálózat internetes kapcsolódási pontján helyezhetők el. A nagyobb vállalatok esetleg a több különböző biztonsági igényű részre tagolt belső hálózatok kapcsolódási pontjain is elhelyezhetnek tűzfalakat, a legtöbb tűzfal mégis egy belső hálózat és az internet közötti forgalmat védi. Ha mondjuk egy nagyobb vállalat lehetővé teszi a partnerei számára a saját hálózatához való közvetlen csatlakozást, akkor a csatlakozási pont és a hálózat között általában található egy tűzfal is, amely a partnerek számára megengedett és meg nem engedett forgalmat vezérli. Az ilyen és hasonló feladatokat ellátó belső tűzfalak üzembe helyezését bízvást tekinthetjük a hálózatvédelem ajánlott módszerének.

Akármilyen tűzfalat választunk is, meg kell határozni a szűrőket, amelyek a biztonsági politikát támogatják.

5.3.3. A BEJÖVŐ FORGALOMRA VONATKOZÓ SZABÁLYZAT MEGHATÁROZÁSA

Mivel a hálózati forgalom a tűzfalon halad keresztül, így ez a forgalom a tűzfalon beállított szabályoknak van alávetve. Mivel a hálózatok 99 százaléka saját IP-címeket használ a belső hálózatában, így csaknem mindegyik tűzfalról feltehető a 3. fejezetben ismertetett hálózaticím-fordítás *(NAT – Network Address Translation)* módszer használata.

Amennyiben a helyi hálózat teljes forgalma az internetre irányulna, a bejövő forgalomra vonatkozó szabályok kialakítása is nyilvánvaló lenne. A tűzfal csak a belső hálózatból küldött kérésekre válaszként érkező bejövő forgalmat engedné át. A tűzfal ehhez a kimenő kéréseket jegyzi fel az állapottáblában, amint arról már volt szó.

Előfordul azonban, hogy bizonyos kívülről érkező kéréseket szintén át kell engedni a tűzfalon. Ez persze nem jelenti azt, hogy ez a módszer ajánlatos lenne, vagy hogy ezt kellene megvalósítani.

A helyi számítógépekről (felhasználóktól) küldött kérésekre érkező válaszcsomagok a tűzfal külső interfészének vannak címezve. A tűzfal végzi el a címfordítást, miközben mindegyik belső felhasználói kérés hatására létrejött kapcsolat állapotát nyilvántartja. A címfordító tűzfal dinamikusan allokálja a külső interfészen a végpontszámot (port number). *A hálózaticím-fordítás lényege tehát az, hogy több felhasználó az internetre irányuló kéréseihez egy (esetleg néhány) nyilvános IP-címet használhasson. Az egyetlen IP-címen különböző végpontszámokkal történő címfordítást nevezzük végpont-cím címfordításnak* (PAT – Port Address Translation). *A belső címhez tartozó végpontok gyakran változnak, megnehezítve a támadó számára az éppen használt vagy használni kívánt végpontszámok kitalálását.*

Valós élethelyzetben a vállalatok gyakran azt akarják, hogy a saját e-levelező vagy webszerverük kívülről elérhető legyen anélkül, hogy egy DMZ-interfészszel is rendelkező új tűzfalat kelljen vásárolniuk, ami pedig a kívülről elérhető szerverek elhelyezésének ajánlott módszere lenne. Később bővebben is kifejtjük a DMZ-interfész célját és szerepét.

A tűzfalon keresztül engedélyezni az internet felőli közvetlen forgalmat ugyan veszélyes, de elterjedt gyakorlat. Az ilyen jellegű beállítások esetén a biztonság kulcsa az engedélyezett forgalomtípus és a végpontszám szigorú szabályozása. Nem helyes például valamennyi belső IP-cím elérésének engedélyezése. Ha mondjuk egy webszervert kívánunk elérhetővé tenni, akkor elegendő a HTTP-forgalom (80-as végpont) engedélyezése, de kizárólag akkor, ha az a webszerverre (például 10.10.10.10 IP-címre) irányul. Elegendő ez a védelem?

Természetesen nem elegendő, hiszen mostanra már ki kellett alakulnia a hálózat mélységi, többrétegű védelmére vonatkozó szemléletnek, amelynek a fenti megoldás nem felel meg. Számos támadás használja a HTTP-végpontot, és több sérülékeny pontja is ismert, a tűzfal azonban ezek közül sokat nem képes felismerni, hiszen keresztülengedjük rajta az ilyen típusú forgalmat. Ez tehát amolyan „22-es csapdája". Melegen ajánlott tehát további védelmi rétegeket üzembe helyezni, például személyi tűzfalat, behatolásjelző rendszert *(IDS – Intrusion Detection System)* és vírusvédelmet. Az ilyen konfigurációk beüzemelése előtt arról is érdemes meggyőződni, hogy a biztonsági szabályzataink megfelelnek-e az ajánlott

gyakorlatnak, és milyen lépésekre van szükség a kellő biztonság fenntartásához. Ha még nem rendelkeznénk biztonsági szabályzatokkal, itt egy újabb ösztönző a kialakításukra.

5.3.4. A KIMENŐ FORGALOMRA VONATKOZÓ SZABÁLYZAT MEGHATÁROZÁSA

Minden tűzfal figyeli és korlátozza a befelé irányuló forgalmat, a jól tervezett és helyesen beüzemelt tűzfal azonban a kifelé irányuló felhasználói forgalmat is figyeli.

Korábban már volt szó a közvetítő *(proxy)* szerverekről, és a hálózatból kifelé irányuló forgalom ellenőrzésében és szabályozásában betöltött szerepükről. Ott egyben kitűnő példáját láthattuk a kimenő forgalomra vonatkozó szabályzat meghatározására is.

Esett már szó a saját hálózatunk és a hozzá csatlakozó üzleti partnerek közötti tűzfal szerepéről is. Ezt most kiegészíthetjük azzal, hogy ugyanezen a tűzfalon valószínűleg a hálózatunkból a partnerekébe irányuló forgalom figyelésére és szabályozására szolgáló előírásokat is alkalmazni kívánunk.

Felmerülhet olyan igény is, hogy a tűzfal csak bizonyos IP-című gépeknek tegye lehetővé a kifelé irányuló forgalmat. Ennek egyik formája, hogy kizárólag a belső hálózatban valóban megtalálható IP-címekről érkező forgalmat engedjük ki, erősen megnehezítve így az IP-cím hamisítását.

Lehetnek olyan internethelyek, amelyek elérését lehetetlenné akarjuk tenni a felhasználók számára. Ennek erősebb formája, ha csak bizonyos helyek elérését engedélyezzük, és minden más hely meglátogatását automatikusan megtiltjuk.

A továbbiakban a most ismertetett gyakorlat biztonságosabb alternatíváját ismertetjük, bemutatva a DMZ (demilitarizált zóna) mibenlétét és szerepét.

5.4. ELSŐKÉNT AZ ALAPELVEK: ÉLET A DMZ-BEN

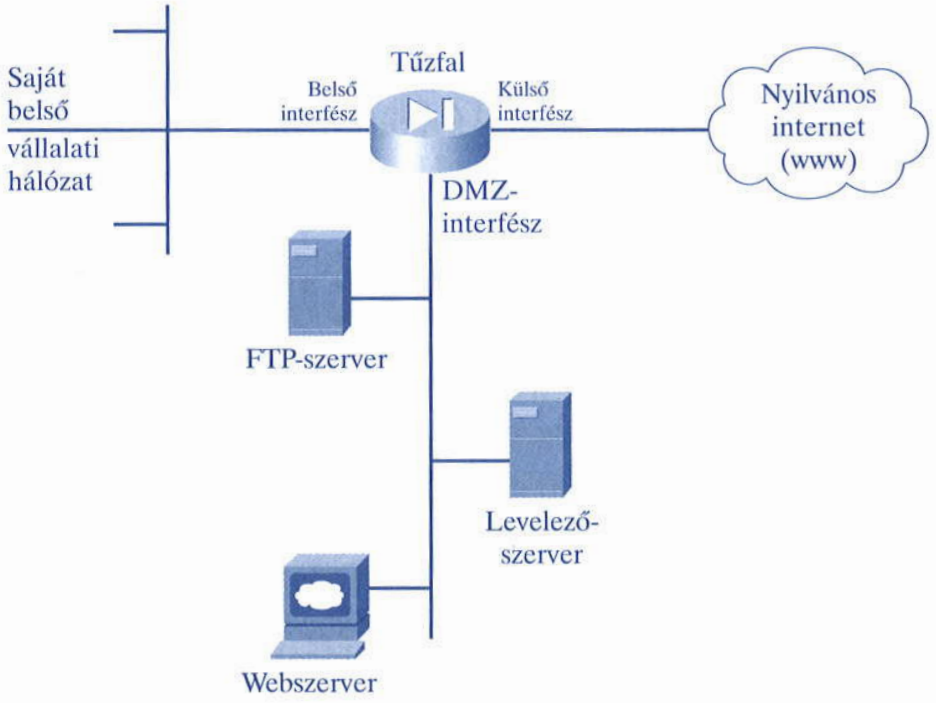
A demilitarizált zóna *(DMZ – demilitarized zone)* a katonai harcászatban használt fogalom a két ellenség közötti ütközőterület definiálására. A világ talán legismertebb demilitarizált zónája az Észak- és Dél-Korea között húzódó övezet, amely elválasztja a két államot, amelyek a koreai háború óta még nem kötöttek békét. Lehet persze, hogy ez csupán egyike a némileg érdekes, ám jobbára jelentéktelen politikai és katonai tényeknek, de miként segíthet ez bennünket a hálózati biztonság növelésében?

A web-, e-levél- és FTP-szerverek internetre csatlakoztatása veszélyes, és bizonyos esetekben egyáltalán nem javasolt. Ha vállalatunk rendelke-

zik saját maga által fenntartott webhellyel, amelyhez még az e-levelezés is társul, akkor célszerűnek tarthatjuk a két interfésszel (külső és belső) rendelkező tűzfal beüzemelését, amelyen a beérkező kéréseket a megfelelő szerverhez irányító szabályokat állítunk be. Jóllehet első pillantásra ez a megoldás biztonságosnak tűnhet, mégis katasztrofális hatása lehet, ha egy képzett támadó célpontjának választja az így védett hálózatot. Szerencsére már régóta létezik jobb megoldás is: beteszünk egy harmadik interfészt is a tűzfalba, és az ahhoz csatlakozó hálózatot elnevezzük DMZ-nek. Ez a megoldás egyrészt egyszerűbbé teszi a tűzfalon keresztüli forgalmat vezérlő szabályok kialakítását, másrészt némileg nagyobb biztonságot ad, ha internetről is elérhető szervereket és szolgáltatásokat kívánunk üzemeltetni.

Az internetről érkező forgalom közvetlenül a hálózatunkba irányítása egyáltalán nem jó gondolat. Valójában annyira hibás, hogy meglepő, mégis milyen sok vállalat gondolkodik a bevezetésén. Ha kisvállalkozóként a saját házunkban számítógépeket árusítanánk, akkor sem akarnánk azt, hogy a vevők az egész lakásunkon végigcsörtessenek vásárláskor, ehelyett kinevezünk egy (önálló bejárattal rendelkező) helyiséget, mondjuk a garázst boltnak, megakadályozva az ismeretlen embereket a lakás többi részébe való bejutásban. Így tesszük lehetetlenné számukra, hogy a lakásunkban kóboroljanak, és tapogassák féltve őrzött könyvgyűjteményünket.

A DMZ egy olyan interfész, amely a megbízható hálózati szegmenstől (a saját belső hálózatunktól) és a megbízhatatlan külső hálózattól (az internettől) egyaránt elválasztja a szintén megbízhatónak tartott szolgáltatási hálózati szegmenst (a szervereket). A hálózatokat egymástól fizikai-



5.3. ábra. A DMZ elhelyezése és funkciója

lag elkülöníti, a közöttük zajló forgalmat pedig a tűzfalon beállított kapcsolati szabályok sora vezérli. Ennek a biztonsági modellnek fontos része a DMZ fizikai elkülönítése a belső hálózattól, hiszen így az internetről csak a szerverekhez lehet hozzáférni, nem pedig a teljes belső hálózathoz. Ezt a megoldást szemlélteti az 5.3. ábra.

Az 5.3. ábrán a DMZ-interfészhez csatlakozó hálózat ad otthont az FTP-, levelező- és webszervernek. A DMZ-interfészen való átjutás szabályai nem teszik lehetővé, hogy az internetről érkező forgalom a DMZ határain túl terjeszkedhessék.

A DMZ legnagyobb előnye az, hogy az ismeretlen internetes forgalmat legfeljebb a DMZ-ben található szerverekre korlátozza, megakadályozva a belső hálózatba való bejutását. Másként megfogalmazva, a kívülről is elérhető szolgáltatásokat nyújtó gépek, külön alhálózatban lévén elhelyezve, sokkal nehezebben szolgálhatnak ugródeszkaként a belső hálózatba. Van azonban a DMZ-nek néhány más előnye is, amelyek segítségünkre vannak abban, hogy jobban figyelemmel kísérhessük, mi történik a hálózatunkban, ezáltal is növelve a hálózatunk biztonságát:

- A DMZ-forgalom auditálása.
- A behatolásjelző rendszer DMZ-ben való elhelyezhetősége.
- A három interfész közötti útválasztási frissítések korlátozása.
- A névszerver (DNS) DMZ-ben való elhelyezhetősége.

Ezzel megtárgyaltuk, hogy mi is az a DMZ, és egy általános példán keresztül bemutattuk használatának módját is. A következő esettanulmányban a DMZ-vel szemben támasztott követelményeket vizsgáljuk meg, ezzel is szemléltetve, hogy bármely adott szempontrendszer esetén miért célszerű az alkalmazása.

5.5. Esettanulmányok

Ebben a fejezetben eddig számos érdekes szemszögből megvizsgáltuk a tűzfalakat, működésüket és beüzemelésük lehetőségeit. A továbbiakban az így megszerzett tudást igyekszünk elmélyíteni azzal, hogy valós élethelyzetekből vett példákon keresztül keresünk választ az esetleg homályban maradt kérdésekre, jobban megvilágítva egyúttal az eddig tárgyalt fontos elveket is.

5.5.1. Demilitarizálni vagy nem demilitarizálni?

A Kárpáti Vállalat elhatározza, hogy a továbbiakban nem kíván az internetszolgáltatójának fizetni a webtárhelyért és a levelezőszolgáltatásért. Az IT-részleg úgy dönt, hogy két régebbi szervert kíván használni arra, hogy ezeket a szolgáltatásokat nyújtsák a kliensek és a vállalat dolgozói számára. Ezeket a szervereket a hivatali irodában kívánják elhelyezni, azonban még nem döntöttek arról, hogy üzembe helyezésükhöz szükség van-e egy DMZ-interfésszel is rendelkező tűzfal beszerzésére.

Amennyiben a Kárpáti Vállalat valóban tovább akar haladni a megkezdett úton, és a jövőben saját maga akarja biztosítani ezeket a szolgáltatásokat, akkor alaposan fel kell mérnie a javasolt megoldások biztonsági kockázatát. Ezen az úton az első helyes lépés annak felmérése, hogy milyen biztonsági következményekkel kell egyáltalán számolnia. A vállalat IT-részlegének tehát gondosan meg kell határoznia a saját internetszolgáltatások (web és e-levelezés) biztosításával kapcsolatos biztonsági kockázatokat. A következő kérdések merülnek fel.

- **1. biztonsági témakör** – Engedélyezni kell-e a saját hálózatra csatlakozó szerverek internetről történő elérését, vagy van más lehetőség is?

  Válasz: A levelező- és a webszerver a DMZ-interfészre is csatlakoztatható. Nincs szükség a külön hálózatban való elhelyezésükre, és implementációjuk nem jelent biztonsági problémát.
- **2. biztonsági témakör** – Miként tudja az IT-részleg azt biztosítani, hogy a bejövő forgalom kizárólag a levelező- és webszervert tartalmazó hálózati szegmensre korlátozódjék?

  Válasz: A DMZ-interfész beállított szabályai természetüknél fogva nem engedélyezik, hogy a külső forgalom bejuthasson a saját hálózatba. Így tehát a beérkező internetforgalom kizárólag a DMZ-szegmensre fog korlátozódni.
- **3. biztonsági témakör** – Milyen műveletekre van szükség ahhoz, hogy a saját hálózatot elrejthessük a beérkező forgalom elől?

  Válasz: A DMZ-interfész útválasztási szabályai nem teszik lehetővé a bejövő forgalom saját hálózatba jutását.

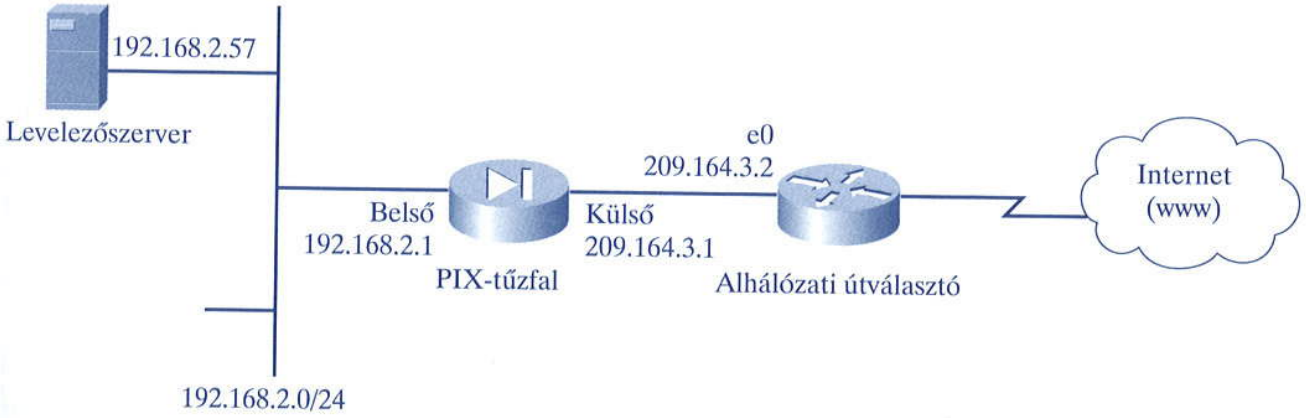
A vállalat IT-részlege tehát végiggondolta a „mi az a DMZ és miért van rá szükségünk" kérdését. A válaszok nyilvánvalóan egyetlen irányba mutatnak: harmadik, vagyis DMZ-interfésszel is rendelkező tűzfalat kell használni. Az eddigiekben már megismerhettük a DMZ-interfész alapvető működését, és láthattunk egy tipikus konfigurációt is.

5.5.2. Levelezőszerver a tűzfallal védett belső hálózatban

A fejezetben már esett szó arról, hogy a vállalatok a belső hálózatukban is telepíthetnek levelezőszervert, s megemlítettük az ezzel kapcsolatos veszélyeket is. A levelezőszerver belső hálózatban való elhelyezése azonban viszonylag elterjedt gyakorlat, így az ilyen megoldásra is kell vetnünk egy pillantást.

Ha megnézzük a Cisco Systems eszközeihez kínált konfigurációs állományokat, akkor számos beállítási lehetőséget találhatunk bennük. Az alábbi esettanulmányban számos ilyen beállítási lehetőséget mutatunk be. Az esettanulmány jobb követhetősége érdekében a lehetőségek között magyarázó sorokat helyezünk el, azonban nem kíséreljük meg minden egyes parancs bemutatását, mivel ez meghaladná ennek a könyvnek a kereteit. Bővebb információkat a Cisco.com webhelyen lehet találni.

A bemutatott esetben egy kis/közepes vállalati hálózatot mutatunk be (5.4. ábra). Amint az 5.2. példában található konfigurációs állomány is bizonyítja, jelenleg csak egy levelezőszerver van a hálózatban, de lehetne egy webszerver vagy a DNS-szerver is ott.



5.4. ábra. Tűzfal telepítése belső levelezőszerver esetén

5.2. példa. PIX-tűzfal belső levelezőszerverhez konfigurálva

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

```
!--- Ezek a parancsok nevezik meg és állítják be az egyes PIX-interfészek
biztonsági szintjét. Ezen parancsok következtében a tűzfal képes felis-
merni, hogy melyik interfészt tekintjük megbízhatatlannak (külsőnek), és
melyiket megbízhatónak (belsőnek).

enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SECURE-FIREWALL
domain-name noplace.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
no names

access-list smtp permit tcp any host 209.164.3.5 eq smtp

!--- Az SMTP- (e-levelezés) forgalmat engedélyező hozzáférési lista
létrehozása úgy, hogy a bárhonnan érkező forgalmat a 209.164.3.5 IP-címre
(levelezőszerver nyilvános címe) beengedje. Ezt a listát elnevezi smtp-
nek. Amennyiben web- vagy DNS-szerverek is lennének, ehhez a listához
kell további sorokat hozzáadni. Amennyiben szükség van arra, hogy egy
adott címre irányuló, kívülről érkező forgalmat beengedjünk a belső
hálózatba, akkor mindenekelőtt ezt a listát kell létrehozni.
Megjegyzés: irányonként és interfészenként csupán egyetlen egy lista
létrehozása engedélyezett (például „külső interfész beérkező forgalma"
lista). Ezen korlátozás miatt a hozzáférési listához adandó valamennyi
további sort itt kell megadni. Ha a kérdéses szerver nem SMTP, akkor
előfordulásait ki kell cserélni a www, pop3, dns, vagy más szükséges
protokoll nevére. Ezt a parancsot a PIX-szoftver 5. kiadása vezette be;
a példában a conduit utasítás helyett szerepel.

pager lines 24
logging on
logging timestamp
no logging standby
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging
no logging history
```

```
logging facility 23
logging queue 512

interface ethernet0 auto
interface ethernet1 auto

!--- Mindegyik Ethernet-interfészt úgy állítja be, hogy automatikusan
felismerje a csatlakozó médiatípust.

mtu outside 1500
mtu inside 1500
ip address inside 192.168.2.1 255.255.255.0
ip address outside 209.164.3.1 255.255.255.0

!--- Az egyes interfészek IP-címének beállítása

no failover
arp timeout 14400

global (outside) 1 209.164.3.129
nat (inside) 1 192.168.2.0 255.255.255.0

!--- Megadja, hogy a belső hálózatból érkező 192.168.2.x forráscímű, az
internetre irányuló csomagokon a külső interfészen való áthaladáskor cím-
fordítást kell végezni úgy, hogy az új forráscím a 209.164.3.129 legyen.

static (inside, outside) 209.164.3.5 192.168.2.57 netmask
255.255.255.255

!--- Az előző parancs statikus címfordítást végez a külső interfészen
látható 209.164.3.5. nyilvános cím és a belső (RFC1918 szerint hasz-
nált) 192.168.2.57 (saját) cím között. A tűzfal mögött ugyanis a levele-
zőszerver a saját címen látszik, míg kívülről a nyilvános címén érhető
el. Régebbi PIX-tűzfalak esetén egy conduit és egy static parancspárra
van szükség a beérkező forgalom esetén; a conduit parancs megnyitotta
az ajtót, és a static parancs meghatározta az útvonalat. Éppen ezért
általában egyik a másik nélkül soha nem állt.

access-group smtp in interface outside

!--- Az smtp nevű hozzáférési listát hozzárendeli a külső interfész
bejövő forgalmához. A static utasítással együtt ettől kezdve működőképes
a konfiguráció. Mivel a hozzáférési lista (smtp) a bejövő forgalomhoz
```

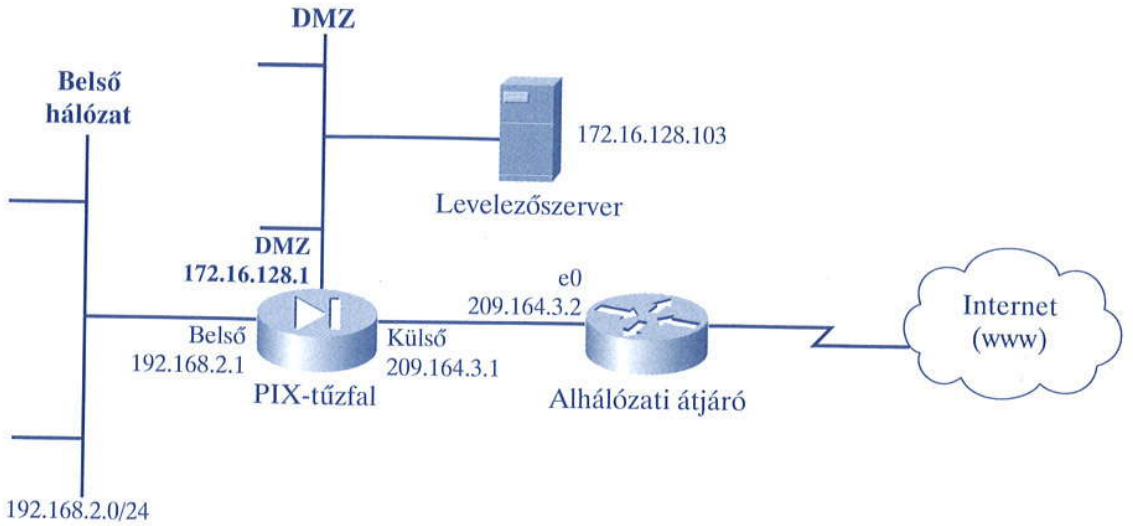
```
lett hozzárendelve, így a PIX minden beérkező csomagot ezen lista alapján
fog megvizsgálni, eldobva mindazokat, amelyekhez nem talál külön megadott
engedélyt.

route outside 0.0.0.0 0.0.0.0 209.164.3.2 1

!--- Az alapértelmezett útvonal a külső interfészen keresztül vezet, és a
következő állomás a megadott 209.164.3.2 IP-című eszköz. A PIX azt
feltételezi, hogy ez az útválasztó címe.

timeout xlate 1:30:00 conn 1:00:00 half-closed 0:10:00 udp 0
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
terminal width 200
Cryptochecksum: d66eb04bc477f21ffbd5baa21ce0f85a
: end
```

5.5.3. A TŰZFAL BEÁLLÍTÁSA (LEVELEZŐSZERVER A DMZ-BEN)

A fejezetben már esett szó arról, hogy a biztonságra nézve milyen következményei lehetnek a levelezőszerver belső hálózatban való elhelyezésének. Mindazonáltal ez egy meglehetősen elterjedt megoldás, így érdemes közelebbről is megvizsgálnunk a leggyakoribb megvalósítását.

A Cisco Systems az eszközeihez a konfigurációs beállítások széles skáláját sorolja fel. A következő esettanulmányban a különböző konfigurációs állományok csak a jobb megértést hivatottak elősegíteni. Az alapvető fontosságú utasítások köré magyarázatokat helyeztünk el, minden egyes utasítás ismertetése azonban meghaladja ezen könyv kereteit. További információkat a Cisco.com webhelyen lehet találni.

Példánk egy kis, vagy közepes méretű vállalkozás legyen, amelyet az 5.5. ábrán szemléltetünk. Amint az 5.3. példa is mutatja, csak a levelezőszerver található a DMZ-ben, bár el lehetne itt helyezni a webszervert, vagy a névszervert is.



5.5. ábra. Tűzfal telepítése DMZ-ben lévő levelezőszerverhez

5.3. példa. PIX-tűzfal beállítása DMZ-ben lévő levelezőszerverhez

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50

!--- Az egyes PIX-interfészek biztonsági szintjeit beállító parancsok. A
tűzfal ezek segítségével képes azonosítani, hogy melyik hálózati
interfésze minősül külsőnek (megbízhatatlannak), belsőnek (megbízhatónak),
és DMZ-nek. Figyeljük meg a példában látható értékeket. A legkevésbé
biztonságos interfészhez a 0 biztonsági értéket rendeljük (egyáltalán nem
biztonságos). A belső interfészhez a 100 biztonsági érték tartozik
(biztonságosnak feltételezett interfész). A DMZ nagyjából a kettő között
van, így értéke 50.

enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SECURE-FIREWALL
domain-name noplace.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 ras 1718-1719
fixup protocol h323 h225 1720
fixup protocol ils 389
fixup protocol rsh 514
```

```
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
no names

access-list smtp permit tcp any host 209.164.3.5 eq smtp

!--- Létrehozza a hozzáférési listát, amely a bárhonnan érkező,
209.164.3.5 címre (a levelezőszerver nyilvános címére) irányuló SMTP-
(levelezési) forgalmat engedélyezi. Ezt a listát elnevezi smtp-nek.
Amennyiben webszerver, vagy DNS-szerver is van a hálózatban, akkor további
sorokat kell adni a listához. A hálózatunk adott IP-címére irányuló
forgalom engedélyezésének ez az első lépése.

pager lines 24
logging on
logging timestamp
no logging standby
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging
no logging history
logging facility 23
logging queue 512

interface ethernet0 auto
interface ethernet1 auto
interface etherner2 auto

!--- mindegyik Ethernet-interfészre beállítja, hogy automatikusan ismerje
fel a csatlakozó eszköz protokoll-típusát.

mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address inside 192.168.2.1 255.255.255.252
ip address outside 209.164.3.1 255.255.255.252
ip address dmz 172.16.128.1 255.255.255.0

!--- Mindegyik interfésznek beállítja az IP-címét.
```

```
no failover
arp timeout 14400

global (outside) 1 209.164.3.129
nat (inside) 1 192.168.1.0 255.255.255.0

!--- megadja, hogy a 192.168.1.x tartományból érkező forgalmat
címfordítani kell a 209.164.3.129 címre, amennyiben az adott forgalom a
külső interfészen keresztül akar kijutni az internetre.

static (dmz,outside) 209.164.3.5 172.16.128.103 netmask 255.255.255.255

!--- A fenti parancs a szerver külső, nyilvános IP-címéről (209.164.3.5) a
belső, nem nyilvános 172.16.128.103 címre történő statikus címfordításra
ad parancsot. Ezek a DMZ-ben található szerver külső, illetve belső címei.

static (inside,dmz) 192.168.1.0 192.168.1.0 netmask 255.255.255.0

!--- Ezzel a statikus címfordítási utasítással megakadályozható, hogy a
belső címeket a DMZ irányába is címfordítsa. Szó szerinti értelemben a
192.168.1.x címet a 192.168.1.x címre „fordítja".

access-group smtp in interface outside

!--- Az smtp-nek elnevezett hozzáférési listát rendeli a külső interfészen
beérkező csomagokhoz. A static parancsok jelenléte és az interfészhez
rendelt smtp lista együtt teszi lehetővé a tervezett működést. Mivel a
listát a beérkező csomagokhoz rendeli, így a tűzfal minden beérkező
csomagot e szerint a lista szerint engedélyez vagy tilt le.

route outside 0.0.0.0 0.0.0.0 209.164.3.2 1

!--- Beállítja, hogy az alapértelmezett irány a külső interfész legyen,
mégpedig a 209.164.3.2 eszköz irányába. A tűzfal ezt a címet tekinti
alapértelmezett átjárónak.

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
```

```
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
terminal width 80
Cryptochecksum: d66eb04bc477f21ffbd5baa21ce0f85a
: end
```

5.6. A TŰZFALAK KORLÁTAI

A tűzfalak a hálózatbiztonság szempontjából alapvető fontossággal bírnak. A forgalom (állapotteljes csomagvizsgálat segítségével történő) ellenőrzésére, az adat sértetlenségének ellenőrzésére és (a címfordítás segítségével) a belső hálózat bizalmas voltának megőrzésére lettek kialakítva. Ezek az előnyök úgy érvényesíthetők a hálózatban, hogy mindkét irányú forgalma a tűzfalon halad át. A tűzfal szerepe a biztonsági stratégiában nyilvánvaló. Soha nem szabad azonban elfelejteni, hogy a tűzfalakra az alábbi korlátok vonatkoznak:

- A tűzfal nem képes megakadályozni egyes felhasználókat vagy támadókat abban, hogy a tűzfalat megkerülve létesítsenek kapcsolatot a külvilággal (például modemjükkel kitelefonáljanak vagy hívást fogadjanak, esetleg drót nélküli elérési pontot telepítsenek).
- A tűzfalak nem tartatják be a jelszószabályzatot, és nem akadályozzák meg a jelszavakkal való visszaéléseket. A jelszóházirendnek kritikus szerepe van, mivel az határozza meg az elfogadható viselkedést, és határozza meg a megszegéséért járó büntetéseket.
- A nem technikai jellegű biztonsági kockázatok (például az 1. fejezetben említett pszichomérnöki tevékenység) ellen a tűzfalak nem védenek.
- A tűzfal adja a forgalom szűk keresztmetszetét, hiszen mindkét irányban a teljes forgalomnak át kell rajta haladnia, kapacitása pedig nyilván véges. Ezzel egyidejűleg ráadásul elhelyezünk a hálózatunkban egy olyan kockázati tényezőt, ahol egyetlen eszköz (nevezetesen a tűzfal) meghibásodása is a hálózat kifelé (DMZ esetén pedig még a szerverek felé) irányuló kapcsolatának elvesztését jelenti. A szerverek elérhetetlensége pedig akár a teljes hálózat működésképtelenségéhez is vezethet.

Az FBI a „phone masters" nevű gépkalóz társaság 1999-ben bekövetkezett letartóztatása után számos hasonló biztonsági problémára derült fény. A kalózok végső célja az volt, hogy az Egyesült Államok egész telekommunikációs hálózatát képesek legyenek uralni, így betörtek számos telefonhálózatba, beleértve az AT&T, a British Telecom, a GTE, az MCI WorldCom, a Sprint, a Southwestern Bell és több állami és szövetségi ügynökség hálózatát. Betörtek továbbá több hitelminősítő cég (Equifax Inc, TRW Inc.), valamint a Nexis/Lexis és a Dun & Bradstreet vállalatok adatbázisaiba. Hozzáfértek az USA erősáramú hálózatának egyes részeihez, egyes légiforgalom-irányító rendszerekhez, sőt a Fehér Ház nem nyilvános telefonszámokat tartalmazó digitális gyorsítótárát is feltörték. Ezen közben a társaság tagjai egyáltalán nem végeztek különösebb tudást vagy felszerelést igénylő tevékenységet. A kukabúvárkodás és a pszichomérnöki tevékenység segítette ezeket a műszakilag meglehetősen gyengén felkészült kalózokat a fenti céljaik eléréséhez.

5.7. Összefoglalás

A fejezetben a tűzfalak világával ismerkedtünk meg, és megértettük a hálózatban játszott szerepüket. Vannak, akik nem hisznek ezen eszközök értékében, és a fejezet egyes eszmefuttatásai ezen tűzfaltagadókkal szembeni érveket igyekeztek bemutatni, amelyekkel érveik ostoba volta megmutatható. A tűzfalak fontosságával kapcsolatban további bizonyítékokat sorakoztattunk fel a tisztán technikai szempontból történő bemutatásuk során is, miközben arra az alapvető igazságra is rá kívántunk mutatni, hogy a tűzfalak tulajdonképpen a vállalat biztonsági politikájának megtestesítői.

A fejezet bemutatta a tűzfalak működését, hol és hogyan kell őket elhelyezni, és miként kell megtervezni a hálózat korlátozott eléréséhez szükséges hozzáférési szabályokat. Bemutatta továbbá a DMZ-interfészt, amely a fejlettebb tűzfaltechnológia elengedhetetlen része, s amely a különböző szerverek számára biztosít különleges helyet a hálózatban. A fejezet végén a tűzfalak gyakorlati alkalmazását szemléltető esettanulmányok állnak, majd a tárgyalást a tűzfalak korlátainak bemutatása zárja.

5.8. Összefoglaló kérdések

Az alábbi kérdések megválaszolása a fejezetben tárgyalt ismeretek alaposabb megértését segíti.

1. Kinek van szüksége a tűzfalra?
2. Nekem miért van szükségem tűzfalra?
3. Egyáltalán, van szükségem tűzfalra?
4. A tűzfal miként nevezhető a biztonsági politika kiterjesztésének?
5. Mi a neve a tűzfalban a kapcsolatokat nyomon követő táblázatnak?
6. Mi a DMZ alapvető szerepe?
7. Mi a DMZ kialakításának négy legfontosabb előnye?
8. Képesek-e a tűzfalak a jelszóházirend betartatására, vagy a felhasználók által elkövetett jelszavakkal való visszaélés megakadályozására?

6. fejezet Útválasztók

Légy magad a változás,
amit a világban látni akarsz.
(Mahatma Gandhi)

A fejezet elolvasása után érteni kell, és el kell tudni magyarázni az alábbi témákat:

- ***a tartalom alapú hozzáférés-ellenőrzés* (CBAC – Content-Broad Access Control) *legfontosabb elemei;***
- ***az IOS-alapú behatolásjelző szolgáltatás és a Cisco-tűzfalkészlet* (FFS – Firewall Feature Set) *használatának előnyei;***
- ***az útválasztó biztonságossá tételére használt technikák és céljaik.***

Mindenki szeretne olyan gyorsan csatlakozni az internetre, amilyen gyorsan csak lehetséges. A kedves olvasót, aki e könyvet most olvassa, valószínűleg a családja jelölte ki arra, hogy „állítsa be" a család számára az internet-hozzáférést. A legjobb póló, amit valaha láttam, a ThinkGeek.com cégtől származott, felirata pedig így szólt: „Nem, én nem fogom beállítani a te számítógépedet" (lásd 6.1. ábra).

6.1. ábra. „Nem, én nem fogom beállítani a te számítógépedet"

A fentiekkel csak arra akartam kitérni, amit a legtöbben nem tudnak: az internetet az útválasztók éltetik. Sokan úgy vélik, hogy az egyes emberek biztonsága és beavatkozási lehetősége nagyobb, hiszen az ő gépük csatlakozik az internetre. Valójában azonban a helyzet egészen más – az interneten nincsenek biztosítékok, az egy vad és száguldó hely. Mindenki megpróbál helyesen cselekedni, de balesetek mindig történnek.

Amikor az emberek megkísérlik az internet páratlan kommunikációs lehetőségeit kihasználni, akkor olyan megoldásokat kell biztosítaniuk, amelyek

- megvédik a belső hálózatokat a behatolástól;
- biztonságos internetes és távoli hozzáférést tesznek lehetővé;
- lehetővé teszik a hálózati kereskedelmet a világhálón keresztül.

Napjainkban az internet olyan új, rendkívül hatékony technológiák gyűjtőhelye, amelyek hihetetlen módon megnövelik a távoli fogyasztókkal, beszállítókkal, partnerekkel és alkalmazottakkal folytatott kommunikáció lehetőségét. A felhasználóknak meg kell bízniuk abban, hogy – különösen a nyilvános – hálózaton keresztül zajló ügyletek biztonságosak.

Az internet gerinchálózatát alkotó útválasztók 80%-ánál is több futtatja a Cisco IOS-szoftverét, és az internethez csatlakozó kereskedelmi hálózatok útválasztóiban ez a szoftver hasonlóan magas arányban fut. Ez a szoftver a hálózati szolgáltatások teljes készletét biztosítja, és lehetővé teszi a hálózatos alkalmazások futtatását is. Az IOS biztonsági szolgáltatásai számos módon lehetővé teszik az internettel, intranettel és a távoli elérésű hálózatokkal kapcsolatos biztonsági megoldások testreszabását, kialakítva így a végpont-végpont közötti biztonságos hálózati összekötetést.

A teljes biztonsági megoldások kritikus pontja a hálózati tűzfal, amely a hozzá csatlakozó hálózatok közötti forgalmat figyeli és a biztonsági po-

litikának megfelelően korlátozza. Amint arról már az 5. fejezetben esett szó, a tűzfalak nem útválasztók, jóllehet az internethez való csatlakozás kizárólag rajtuk keresztül lehetséges. Az alhálózat legkülső elemét azonban a peremi útválasztó *(edge router)* alkotja (fordító megjegyzése: itthon ez a szóhasználat nem terjedt el, inkább az átjáró *(gateway)* nevet használjuk, utalva arra, hogy az alhálózatból csak ezen az útválasztón – mint egyetlen „ajtón" – keresztül juthatnak ki a csomagok a külvilágba).

Az átjárók tehát minden hálózat határán megtalálhatók, például a saját hálózat, az intranet, az extranet és az internet között, vagyis az egyes alhálózatokat az útválasztók kötik össze. A tűzfalak viszont általában a belső (saját) hálózat, és a külső (nyilvános) hálózat között találhatók.

A Cisco IOS-tűzfalkészlet *(firewall feature set)*, amely a Cisco-útválasztó szoftverének (IOS) opcionális része, olyan megnövelt biztonsági megoldást jelent, amely a hálózatot védi a biztonsági kockázatokkal szemben. Ezen integrált útválasztó-biztonsági megoldás egyik eleme a Cisco Systems cég által szállított biztonsági megoldások rendszerének.

Ebben a fejezetben az útválasztók használatát mutatjuk be, beleértve a tűzfalkészlet célját és mibenlétét is. Hol kell a hálózatunkban alkalmazni ezt a típusú védelmet? A fejezet erre a kérdésre is választ ad, és bemutatja ennek a biztonsági technológiának az előnyeit és a hátrányait is.

A tűzfal olyan biztonsági eszköz, amely az internetkapcsolatunk határán áll, és szigorú határőrként állandóan figyeli a befelé és kifelé irányuló forgalmat, amelyet az előre beállított szabályoknak megfelelően átenged, leblokkol vagy visszautasít. A törvényen kívüli globális web világában a tűzfal képviseli a rendet és a törvényt, állandóan éberen ügyelve és megvédve a hozzá csatlakozó belső hálózati erőforrásokat.

A peremi útválasztó ezzel szemben a vállalkozás internethez csatlakozását biztosítja. A legtöbben úgy tekintenek rá, mint a csatlakozáshoz feltétlenül szükséges eszközre.

A tűzfal azonban nem cserél más útválasztókkal az útvonal megválasztásához szükséges információkat, ez a feladat a peremi útválasztóra marad. Ezért van szükség mindkét eszközre a hálózat határán.

Az útválasztó léte azonban azt jelenti, hogy a hálózatba belépni vagy onnan távozni kívánó minden egyes csomagnak át kell haladnia rajta. A tűzfal szerepe annak megállapítása, hogy ezek közül melyik haladhat át és melyik nem. Ha már azonban a tűzfal és a külvilág közé odatettünk egy útválasztót, akkor nem használhatnánk ezt is a mélységi védelem egyik (legelső) vonalaként?

Természetesen használhatjuk, és célszerű is használnunk. Az útválasztóért súlyos pénzeket adtunk ki, értékes órákat töltöttünk a beállításával, és súlyos hiba lenne vakon megbíznunk biztonságos voltában. Ha a vállalat milliókat költ is más biztonsági megoldásokra, sokszor mégis elhanyagolja az útválasztó, és ezen keresztül a hálózat védelmének kiépítését.

Megjegyzés

A legtöbb védett hálózat egyetlen ponton csatlakozik az internethez. Ezen az egyetlen ponton helyezkedik el az útválasztó. Szerepe az, hogy biztosítsa a kapcsolatot a külvilág és a belső hálózat között. Maga az internet tekinthető úgy is, mint egy útválasztókból álló hálózat. Minden egyes útválasztó egy vagy több másik útválasztóval van összekötve. Amennyiben több másikkal áll kapcsolatban, akkor legfontosabb feladata a forgalomirányítás: minden egyes áthaladni kívánt csomagról eldönti, hogy melyik másik útválasztó (vagy az általa kiszolgált hálózat) irányába haladjon tovább.

A peremi útválasztók, vagyis átjárók általában két kapcsolódási ponttal rendelkeznek: egyik a belső (védett) hálózat felé, a másik a külvilág (vagyis az internetet alkotó valamelyik útválasztó) felé néz. A belső hálózatban minden olyan csomagot, amely nem egy másik, szintén belül elhelyezkedő eszköznek van címezve, mindig az átjárónak kell elküldeni, és az átjáró gondoskodik arról, hogy azt kiküldje a külvilágba, ahol az útválasztók láncán keresztül előbb-utóbb megtalálja a címzett eszközt. Az útválasztók egymás között információkat cserélnek, hogy mindig tudják, egy adott cím megtalálásához milyen irányban kell továbbítani a csomagot.

Önmagában az útválasztó eredetileg semmiféle védelmet nem nyújtott. Ezért vezették be a tűzfalat, amely alapvetően szintén két irányba nyújt kapcsolatot: egyik irány a külvilág (amelyet ezúttal az átjáró képvisel), a másik irány pedig a belső hálózat (amelyet véd). Mint arról már volt szó, lehetnek további kapcsolódási pontjai, például a DMZ irányába. Mindenképpen igaz az, hogy egyetlen pontján a külvilág felé, a többi pontján pedig az egyes belső, védett hálózatok felé néz. Ezen védett hálózatok számára úgy viselkedik, mint az átjáró – a kifelé irányuló csomagokat tehát a tűzfalnak kell eljuttatni, és a tűzfal gondoskodik arról, hogy a külső interfészén azt az útválasztó (a hálózat tényleges átjárója) felé továbbítsa.

Számos útválasztó a gyári beállítást használja. Tegyük fel, hogy egy támadó képes átvenni az uralmat az útválasztónk felett. Mivel az útválasztó minden egyes kifelé irányuló vagy onnan érkező csomagot lát, menynyi információt gyűjthet ebből össze egy támadó? Mire lesz képes ezzel az információval? Az útválasztó tehát egy sokat tudó, kulcspozícióban lévő eszköz, amely alapvető fontosságú információt kezel. A hálózati biztonság alatt sokszor a szerverek, tűzfalak, virtuális magánhálózatok, és az IT-erőforrások védelmét értjük. Ebben a fejezetben arról lesz szó, hogyan kell megvédeni az útválasztót, majd miként lehet megnövelni a képességeit a Cisco-tűzfalkészlettel úgy, hogy a hálózat védelmének egy újabb rétegét képviselje.

Az útválasztó biztonságossá tételével, s így a hálózat biztonságosabbá tételével a következő célok érhetők el:

- Megakadályozhatjuk, hogy az útválasztók a támadók számára értékes információkat szivárogtathassanak ki.

- Megakadályozhatjuk, hogy a támadó, esetleg egy hibás félrekonfigurálás működésképtelenné tegye az útválasztót (és ezáltal a belső hálózat külvilági kapcsolatát elvágja).
- Megakadályozhatjuk, hogy egy támadó az útválasztóinkat belső célpontok, esetleg mások támadásának eszközeként használhassa.
- Csökkenti a belső hálózat, illetve a tűzfal terhelését azáltal, hogy az eredendően hibás csomagokat, és az ilyenek felhasználásával indított támadásokat be sem engedi, hanem rögtön a hálózatunk legkülső határán leblokkolja.
- Gyorsan felállíthatjuk így a hálózat védelmének egy újabb rétegét.

Ezen eredmények mind a hálózat és az útválasztó biztonsága és működése körül forognak. Ezek persze csak az általános képet alkotják, az útválasztókhoz megvásárolható tűzfalkészletnek azonban további biztonsági előnyei is vannak.

Nem mindenki akarja pénzét, idejét, erőfeszítéseit, valamint tudását az útválasztó tűzfalkénti működésének beállítására fecsérelni. A valóságban számos vállalat a tűzfalát állapotteljes csomagvizsgáló eszközként használja. Az útválasztót azonban mindenkinek a hálózat első védelmi vonalaként kellene használnia. Nem az a kérdés, hogy az útválasztó be legyen-e állítva csomagszűrőként, hanem az, hogy miként kell így beállítani. A peremi útválasztót háromféleképpen használhatjuk:

- **Alapbeállítású útválasztó** – Fogjuk az útválasztót, rátesszük az alapbeállítást, rácsatlakoztatjuk az internetre és a belső hálózatra, és ezzel készen is vagyunk. Ebben semmi trükk nincs, viszont a hálózat számára semmilyen biztonsági értéket nem is hoztunk létre.
- **Ellenőrző pontként használt útválasztó** – Amint arról a 3. fejezetben már volt szó, minden útválasztó rendelkezik a hozzáférés-vezérlő lista (ACL) segítségével történő forgalomirányítási képességgel. A hozzáférés-vezérlő lista a forgalmat cél és típus szerint képes szűrni, így az útválasztó ellenőrző pontként üzemelhet: ha az adott forgalomnak nincs külön engedélye, akkor meg kell tiltani. Ez a minimálisan elérendő cél.
- **Csomagvizsgálóként használt útválasztó** – Az útválasztó bonyolultabb szűrés elvégzésére is képes, ha feltesszük rá a tűzfalkészletet. A három közül ez a legjobb útválasztó, azonban ezt a legbonyolultabb beállítani. Az életben az értékes dolgokat soha nem kapjuk ingyen, mindig meg kell értük dolgozni.

Ebben a fejezetben az alapbeállítású útválasztó által nyújtott védelemről vagy biztonságról egyáltalán nem beszélünk, mivel ez semmit nem tesz hozzá a hálózati védelemhez. Ehelyett előbb megvizsgáljuk, hogy a

hozzáférés-vezérlő listák segítségével miként működik az útválasztó ellenőrző pontként, majd rátérünk arra, hogy az ellenőrző listák kiterjesztésével hogyan képes figyelni a forgalmat.

6.1. A PEREMI ÚTVÁLASZTÓ MINT ELLENŐRZŐ PONT

Az **ellenőrző pont** *(choke point)* az internet katonai örökségének részeként származott át a hálózat világába. Az ellenőrző pont egy olyan adott helyet jelent, amelyen mind a befelé, mind a kifelé irányuló forgalomnak egyaránt át kell haladnia. A kifejezés ilyen értelmű használata esetén ez maga az útválasztó. A peremi útválasztó jelenti azt az eszközt, ahol az internetes forgalom bejuthat a belső hálózatba. Ez persze azt is jelenti, hogy meghibásodás szempontjából ez kritikus pont, de ez a téma már más tárgykörbe tartozik.

Az ellenőrző pontként üzemelő útválasztók a belső hálózat biztonságát azáltal növelik meg, hogy a hálózat és az internet (vagy más hálózat) közötti adatáramlást megszűrik.

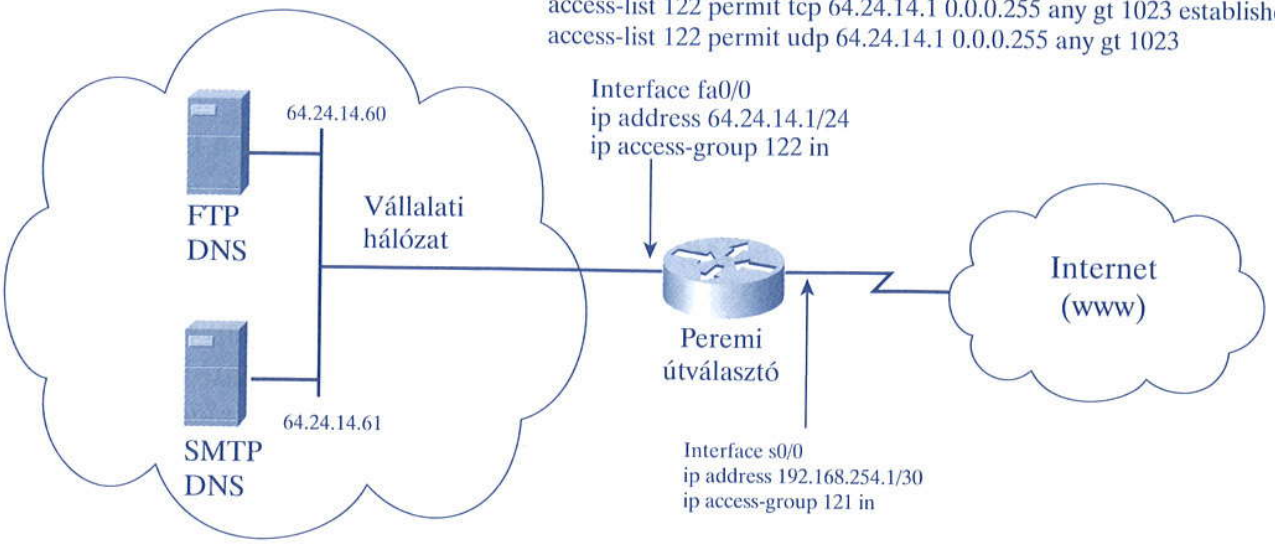
A hálózati biztonság sikeres megvalósítása annak megértésén alapszik, hogy mi is történik a hálózatban. Ezen tudás alapján dönthető el, hogy mit kell használni a hálózati forgalom szűrésére, hogy a nem kívánt tevékenység azonosítható legyen. A hálózati tevékenységet kizárólag az elfogadható szolgáltatásokra kell korlátozni. Az ellenőrző pont kitűnő módja az ellenőrzés durva megvalósításának, amit intelligens szűrők, például állapotteljes tűzfalak és közvetítők *(proxy)* segítségével tovább lehet majd finomítani.

Az ellenőrző pontként beállított peremi útválasztók értéke az, hogy bizonyos eszközök és alkalmazások elérése teljesítményoptimalizáltan valósítható meg. A biztonság ilyetén növelését általában az alap és a kiterjesztett hozzáférés-vezérlő listák *(ACL – Access Control List)* segítségével érjük el, amelyek az OSI hivatkozási modell második, harmadik és negyedik rétegében megjelenő forgalmat képesek ellenőrizni. Maga az a tény, hogy a teljesítmény *általában* nem romlik, abból ered, hogy az útválasztónak a továbbítási döntés meghozatalához amúgy is meg kell vizsgálnia az IP-csomagot, és ehhez képest nem jelent többletmunkát egy egyszerű döntés meghozatala, hogy a csomagot el kell-e dobni, vagy átengedhető-e.

A hozzáférés-vezérlő listák az útválasztón áthaladó csomagok szűrésének és ellenőrzésének lehetőségét nyújtják a hálózatmérnök számára. A 6.2. ábrán az ellenőrző pontként használt útválasztó elhelyezkedését és a rajta alkalmazott szabályokat szemléltetjük. Mellékfeladatként azt kérjük a kedves olvasótól, hogy próbálja meg kitalálni, milyen hálózati eszköz hiányzik az ábráról.

ACL 122: az fa0/0 interfészen érkező forgalomra vonatkozik

```
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq 22
access-list 122 permit udp 64.24.14.1 0.0.0.255 any eq domain
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo-reply
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq ftp
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq http
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any gt 1023 established
access-list 122 permit udp 64.24.14.1 0.0.0.255 any gt 1023
```



ACL 121: az s0/0 interfészen érkező forgalomra vonatkozik

```
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14. 61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```

6.2. ábra. Ellenőrző pontként működő peremi útválasztó

A vállalati hálózat ezen ellenőrző pontként működő peremi útválasztója csupán a következő forgalmat engedi be a belső hálózatba:

- A beérkező elektronikus levélforgalmat a 64.24.14.61 IP-címen található SMTP- (levelező-) szerverre.
- A 64.24.14.60 IP-címen található FTP-szerverre irányuló FTP-forgalmat.
- A 64.24.14.61 IP-címen található névszerverre irányuló zónatranszfer *(zone transfer)* UDP-kéréseket.
- Az 1023 fölötti végpontokra a belső hálózatból kifelé irányuló TCP- és UDP-forgalmat teszi lehetővé.
- Bizonyos típusú ICMP-kéréseket.
- A peremi útválasztó minden más forgalmat letilt.

A vállalati hálózat felhasználójaként a peremi útválasztó az internet irányába csupán az alábbi forgalmakat engedélyezi:

- SSH (22. végpont),
- DNS (53. végpont),
- FTP (20. és 21. végpont),
- HTTP (80. végpont).

Az útválasztó ellenőrző pontként való használata (mind a befelé, mind a kifelé irányuló forgalom szűrésére), amennyiben az csak az alsó 1023 (ismert szolgáltatások) végpontra korlátozódik a hálózatot nagymértékben védtelenül hagyja. Mivel napjaink alkalmazásainak többsége az 1023 fölötti végpontokat használja, és mivel nem minden IP-rétegbeli alkalmazás tartja be a 49152-65535 végpontokra előírt szabályokat, így az 1023. végpont feletti szűrés érinthetné azon alkalmazásokat, amelyek működését biztosítani akarjuk, így nem tilthatjuk le ezen végponttartományt.

Volt-e hiányérzete az útválasztó fenti bemutatása során? Amennyiben hiányolta az állapotteljes csomagvizsgálatot *(SPI – Stateful Packet Inspection)* és a hálózaticím-fordítást *(NAT – Network Address Translation)* végző tűzfalat, akkor önnek teljesen igaza van, és már kezd biztonsági szakértővé válni.

6.1.1. Az ellenőrző pontként működő útválasztók korlátai

Az elmondottak alapján az ellenőrző pontként működő útválasztó hasznos, és képes a hálózat valamilyen szintű védelmére, tudásuk azonban csupán arra elegendő, hogy egy szkriptcsávót távoltartsanak. Egy gyakorlottabb támadó vagy a jelen könyv olvasója azonban már képes felmérni, hogy a hálózat ezáltal még nincs teljesen védve. Az ellenőrző pontként működő útválasztók korlátai az alábbiak:

- Az ilyen útválasztók nem képesek az OSI-modell magasabb (5–7) rétegeiben szűrni. Az IOS néhány bővített lehetősége lehetővé teszi a hálózati alkalmazás felismerését *(NBAR – Network Based Application Recognition),* amely az útválasztó számára a legtöbb ismert féreg felismerését és blokkolását lehetővé teszi. Lásd a http://certcities.com/editorial/columns/story.asp?EditorialsID=76 cikket.
- Az ilyen útválasztók nem teljesen kielégítő módon foglalkoznak az alkalmazási, illetve a protokoll biztonsági problémáival, így például nem képesek felfedni azt, hogy a kapcsolatokat hamisítják.

- Az ilyen útválasztók komoly bővítések nélkül nem képesek állapotteljes csomagvizsgálatot végezni.

Jóllehet az ellenőrző pont a fenti problémák megoldására képtelen, a hálózati és a szolgáltatási elérés szabályozásának (vagyis hogy az internetről érkező felhasználók mihez férhetnek hozzá) azonban kellően jó megoldását jelentik.

A statikus hozzáférés-ellenőrző listák (ACL) létrehozása némi gondolkodást, és hosszas ellenőrzést kíván. A nem kellően átgondolt módon megfogalmazott ACL jelentős kihatással lehet a hálózat teljesítményére és a szolgáltatások elérhetőségére nézve. Ne akarjuk elérni a hálózat védelme érdekében kitűzött célokat sem anélkül, hogy előtte végig ne gondoltuk volna – minden ACL végén ott van az alapértelmezett elutasítása minden olyan csomagnak, amely nem volt külön engedélyezve. A Cisco TAC (a Cisco terméktámogatási ügyfélszolgálata) külön megköszöni, ha ezt a követelményt is megadjuk, mivel mindenki elfelejti – néha még a könyv szerzője is!

6.2. Csomagvizsgáló útválasztó

Mostanra már látni kell, hogy a peremi útválasztó hálózati biztonság részeként való felhasználásának vannak előnyei. Az útválasztó ellenőrző pontként való felhasználása nyilvánvaló előnyökkel jár, ennek azonban van számos olyan korlátja, amely számunkra fontos lehet. Lehet, hogy a vállalata a kormányzat számára készít anyagokat, ezért a legmagasabb elérhető biztonságra van szüksége. Mindettől függetlenül a biztonság következő szintjét a Cisco tűzfalkészlet használata jelenti a peremi útválasztón.

A tűzfalkészlet lelkét a **környezetfüggő hozzáférés-vezérlés** *(CBAC – Context Based Access Control)* jelenti. A CBAC egy olyan állapotteljes csomagvizsgáló motor, amely az útválasztó szűrési képességét az OSI-referenciamodellnek egészen a hetedik (alkalmazási) rétegéig kiterjeszti. Mindezt a CBAC hozzáférés-vezérlő lista segítségével éri el. (Kezdjünk hozzászokni a hozzáférés-vezérlő listákhoz, mivel ezekre mindig szükség van, legfeljebb az újabb technológia újraértelmezi ezeket.)

A tűzfalkészlet nyomon követi a TCP-, az ICMP- (a Cisco IOS 12.2.15T verziótól kezdődően), valamint az UDP-alapú alkalmazási csomagokat. A CBAC az útválasztó mindkét oldalán figyel, megvalósítva így az állapotteljes csomagvizsgálatot, vagyis a nevében szereplő „tűzfalkészlet" jogosan kapta a nevét; mindazonáltal ez az IOS semmiképpen sem tekinthető a kifejezetten állapotteljes tűzfalként üzemelő eszköz lecserélésének.

A tűzfalszerű működést is megvalósító útválasztókat néha „útfal" (routerwall) *néven is emlegetjük. Jelen esetben a kulcsszó a „tűzfalszerű", ami azt jelenti, hogy képes ugyan a tűzfal bizonyos funkcióit ellátni, de semmiképpen sem alkalmas a kifejezetten tűzfal célokat szolgáló eszköz cseréjére.*

A CBAC nem egy egyszerű, tiszta megvalósítás a hálózati architektúrában, mint például a kifejezetten tűzfalnak készített eszköz lenne, hanem egy hibrid. Ez a hibrid architektúra adja a tűzfalkészletes IOS-nek azt a rugalmasságot, ami lehetővé teszi számára azt, hogy tűzfalként és útválasztóként egyaránt működjék. Így növelheti meg a hálózat legszélén a biztonságot. Az ilyen biztonsági technológia legjobb helye valóban a hálózat szélén van.

A tűzfalkészletet csaknem minden Cisco-útválasztó támogatja. Az ilyen verziójú IOS üzemeltetéséhez általában szükség van arra is, hogy megnöveljük az eszközben rendelkezésre álló memória méretét. A legtöbb esetben a Cisco-útválasztónak két dolgot kell teljesítenie ahhoz, hogy fusson rajta a tűzfalkészlet: legyen benne megnövelt méretű memória, és a megfelelő licencű IOS. Valamilyen oknál fogva a Cisco-eszközökben használható memóriamodulok ára nem csökkent le úgy, mint a PC-memóriáké, így növekvő költségekre lehet számítani. Ennek ellenére erősen javasolt olyan Cisco-csomag vásárlása, amely tartalmazza az útválasztót, a megnövelt méretű memóriát, és a megfelelő IOS-licencet.

6.2.1. A TŰZFALKÉSZLET ELŐNYEI

Jóllehet ennek a könyvnek nem célja, hogy mindenféle kereskedelmi reklámszövegeket szajkózzon, jelen technológia esetén mégis kivételt kell tennünk, mivel ez az IOS-ek Mercedese.

A tűzfalkészlet különösen hasznos azon vállalatok számára, amelyek a hálózat határain keresztül költséghatékony módon ki akarják terjeszteni a határok biztonságát, különösen az irodai, az intranet, és az extranet határain. Ugyancsak hasznos azon kisebb és közepes méretű vállalkozások számára, amelyek behatolásérzékeléssel ellátott költséghatékony útválasztóra vágynak. A Cisco-tűzfalkészlet néhány előnye:

- **Dinamikus szűrés** – A CBAC lehetővé teszi a visszatérési útvonal szerinti TCP-, ICMP- és UDP-szűrést, amely dinamikus állapotteljes bejegyzéseket készít a kétirányú kommunikációs munkamenetekről, amikor a párbeszéd először létrejön. A CBAC ezek létrehozását teszi lehetővé, amennyiben az egyedi hozzáférési listákban vannak hozzájuk tartozó engedélyek. Így nincs szükség egyetlen végpont nyitva tartására sem, mivel a CBAC akkor nyitja ki a megfelelő végpontot, ha az ACL engedélyezi azt a forgalmat. A dinamikusan nyitott végpontok élettartama korlátozott (a párbeszéd időtartamára érvényes), és csak adott gépekre korlátozódik, ezzel is csökkentve a külső támadások lehetőségeit. A szűrési képességek között megtalálható például:
  - **Alap és kiterjesztett hozzáférés-vezérlő lista (ACL)** – adott hálózati szegmensek hozzáférését vezérli, definiálva, hogy a hálózati szegmensen vagy az útválasztón milyen forgalom haladhat át, védve így a hálózatot.
  - **„Zár és kulcs" dinamikus ACL** – a tűzfalakon keresztül a felhasználói azonosítás (felhasználónév/jelszó) alapján biztosítja az ideiglenes hozzáférést.
  - **Felhasználónkénti azonosítás és feljogosítás** – a biztonsági házirendben megfogalmazott IP-címek és interfészek alapján nyújtja a felhasználói hozzáférés vezérlésének képességét. Ezt nevezzük hitelesítő közvetítőnek *(authentication proxy)*.
- **TCP-sorszám követése** – A CBAC figyeli a TCP által használt kifelé irányuló munkamenet-sorszámokat, és a befelé jövő forgalmat, nyomon követve így az adatfolyam állapotát. A sorszámkövetés véd a beékelődéses, és más munkamenetet elfogó támadások ellen, mivel a hibás sorszámú csomagokat eldobja. Amint a korábbi fejezetekben már esett róla szó, ez alkotja az SPI lényegét.
- **A kommunikációs munkamenetek állapotának követése** – A CBAC nyomon követi a félig megnyitott, a nyitott, és a zárt TCP-munkameneteket, védve ezáltal a TCP-SYN szolgáltatásmegtagadási támadások ellen. A percenkénti munkamenetszámok és átvitelek száma a rendszergazda által megadott legkisebb és legnagyobb számok alapján történik.
- **UDP- és ICMP-kapcsolat követése** – Ezt a két protokollt elég nehéz megfigyelni, mivel nincs olyan jellemzőjük, amelynek alapján állapotteljesek lehetnének, mint például a TCP. Ettől még persze szükség van az állapotteljes nyomkövetésükre, így a CBAC dinamikus szűrők és időzítők segítségével kísérli meg a kapcsolat állapotának nyomon követését. A könyv nyomtatásakor valószínűleg ez tekinthető az ilyen protokollok átvitelének érvényesítését végző technikák közül a legfejlettebbnek.
- **Munkamenet-naplózás** – Elsőként és leginkább a tűzfalnak mint biztonsági eszköznek kell védenie. Rögtön a védelem után következik azonban a naplózás képessége és a napló rendszeres felülvizsgálata. A mun-

kamenetnaplók egyik fontos lehetősége, hogy a tranzakciókról tartalmazzanak részleteket – a kommunikáció befejeződését, időbélyegeket, a forrás- és célgép címét és végpontjait, valamint az átvitt bájtok számát. Ez az információ rendkívül hasznos lehet, amelyet számos célra fel lehet használni. A CBAC támogatja az alkalmazásonkénti valós idejű felülvizsgálatokat. A naplókról tájékoztatókat lehet készíteni a hagyományos IOS naplózási mechanizmus segítségével, amely mind a helyi, mint a távoli rendszernapló *(syslog)* szervert használhatja a naplózásra.

- **Alkalmazásfüggő monitorozás** – A CBAC számos alkalmazásfüggő protokollt ismer, és folyamatosan vizsgálja a TCP-, UDP- és ICMP-csomagfolyamot, kiszűrve a specifikációtól való eltéréseket. Amennyiben a protokoll szempontjából hibás csomagra bukkan, a párbeszédet blokkolja, és a hozzá tartozó csatornákat lezárja. Az alkalmazásszintű csomagvizsgálatot az alábbi, számos ismert sérülékenységet tartalmazó protokollok esetén képes elvégezni:
  - *CU-SeeMe (7648. végpont)* – Pont-pont videokonferencia.
  - *FTP (21. végpont)* – Kliens-szerver állományátviteli protokoll.
  - *H.323 (1720. végpont)* – Csomag-alapú multimédiás kommunikációs protokoll (VoIP), amely a Q931 és H.245 vezérlő üzeneteket figyeli, további UDP-csatornákat megnyitva a hang- és képadatok számára; ide tartozik továbbá az 5060. végponton a SIP *(Session Initiation Protocol)*.
  - *ICMP vizsgálata* – Jelen könyvben több helyen is láthattuk, hogy az ICMP-t (amely részben a hálózati hibakeresésre szolgál) sok támadó használja a hálózat topológiájának megismerésére, a hálózaton lévő eszközök felderítésére. A tűzfalkészlet ezért ellenőrzi ezeket a csomagokat, és közülük csak a belső hálózatból érkezőket engedélyezi.
  - *MCGP (2427. végpont)* – Médiavezérlő átjáró protokoll *(Media Control Gateway Protocol)* (VoIP)
  - *MSRPC (135. végpont)* – Microsoft távoli eljáráshívási protokoll *(Microsoft Remote Procedure Call Protocol),* amely a rendszerközi folyamatkommunikációt teszi lehetővé.
  - *Net show (1755. végpont)* – A Microsoft médiafolyam platformja.
  - *R-Exec (512. végpont)* – A UNIX-rendszerben használt Berkeley távoli parancs protokoll *(Berkeley remote command protocol).*
  - *R-Shell (514. végpont)* – A UNIX-rendszerben használt Berkeley távoli parancsértelmező protokoll *(Berkeley remote shell protocol).*
  - *RTSP (544. végpont)* – Valós idejű folyamprotokoll *(Real-Time Streaming Protocol)* a multimédia és VoIP-átvitelhez.
  - *SMTP (25. végpont)* – Elektronikus levelezés protokollja *(Simple Mail Transfer Protocol);* a tűzfalkészlet képes az érvénytelen SMTP-parancsok felismerésére, így nincs szükség a demilitarizált zónában a külső levélközvetítő *(mail relay)* használatára.

- *SQLnet (1521. végpont)* – A kliens–adatbázis és adatbázis–adatbázis kommunikációban használt kliens-szerver köztesréteg protokollja. A tűzfalkészlet az Oracle figyelő *(listener)* folyamataitól érkező átirányított üzeneteket vizsgálja, megnyitva a kliens számára a végpontot a szervercsatlakozáshoz.
- *Stream Works (1558. végpont)* – Médiafolyam platform (jelenleg a Real Networks cég tulajdonát képezi).
- *SUNrpc (111. végpont)* – A Sun Microsystems cég távoli eljáráshívás protokollja, melyet a hálózati állományrendszer (NFS) is használ.
- *Real Audio (7070. végpont)* – A Real Networks cég médiafolyam platformja.
- *Telnet (23. végpont)* – Virtuális terminál protokoll.
- *TFTP (69. végpont)* – Trivial File Transfer Protocol.
- *VDOlive (7000. végpont)* – Médiafolyam protokoll.

• **Java-appletek blokkolása** – A peremi útválasztón be lehet állítani a Java kisalkalmazások (appletek) elleni védelem szintjét. Beállítható úgy, hogy kiszűrje vagy teljesen megtagadja a Java-appletek áthaladását, hacsak nincsenek archívumba vagy tömörített állományba csomagolva.

• **Virtuális magánhálózatok** – Az interneten keresztüli biztonságos adatátvitelt teszi lehetővé, miközben csökkenti a kihelyezett irodákkal, valamint a mobil felhasználókkal és alkalmazottakkal kapcsolatos kezelési és üzembe helyezési költségeket, növeli a szolgáltatás minőségét és megbízhatóságát, ráadásul a jobb együttműködési képesség érdekében teljesen szabványos. A virtuális magánhálózatok (VPN) az elfogadható árú szélessávú internet-hozzáférés terjedésével egyre népszerűbbé válnak. A 7. fejezetben részletesebben is tárgyaljuk ezt a témakört.

A helyes és többrétegű biztonsági politika a tűzfal létesítésénél sokkal többet jelent. A tűzfalkészlettel bővített Cisco IOS-szoftver ideális módja a hálózat legelső belépési pontján a biztonság növelésének, így könnyebben betarthatóvá teszi a biztonsági politikát, és növeli a hálózat biztonságát. A tűzfalkészlet ráadásul lehetővé teszi a kapcsolatok átfogó elemzését is, amennyiben egy biztonsági incidens (vagy ennek gyanúja) ezt szükségessé tenné.

6.2.2. TARTALOMALAPÚ CSOMAGVIZSGÁLAT

Amint arról már az 5. fejezetben is szó volt, számos kifejezetten tűzfalként üzemelő eszköz a fizikai interfész szintjén képes a biztonsági ellenőrzésre. Másként megfogalmazva, a tűzfal képes a hálózatunkat a külvilághoz csatlakoztató interfészén definiálni a biztonságot – miközben a belső hálózat felé néző interfészen különösebb korlátozásokat nem vezet

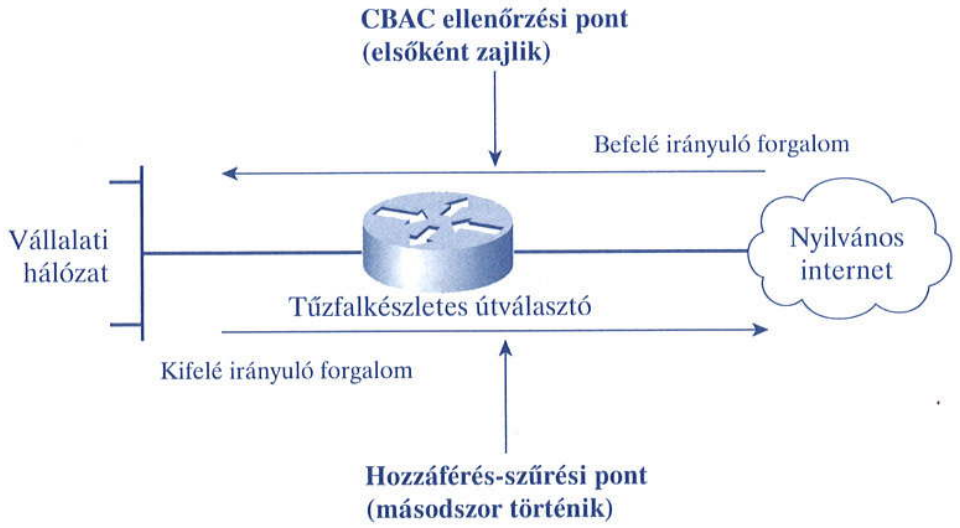
be. A nyilvános internet felé néző interfész nyilván sokkal veszélyeztetettebb, a támadásoknak sokkal jobban ki van téve, és így sokkal inkább védendő, mint a belső interfész. Ez a hiedelem minden típusú tűzfal esetén tetten érhető. Idézzük fel az első fejezetben elhangzottakat: fontos tudni, hogy kiben bízhatunk és kiben nem.

A Cisco-tűzfalkészlettel bővített IOS azonban egy útválasztón üzemel, és a San Jose városában dolgozó szürkeállomány egy különösen ihletett pillanatában vette az útválasztót (a csomagok irányítóját) és a tűzfalat, majd bizalmi függőségek nélkülivé téve összegyúrta ezeket. A tűzfal eredendően kénytelen a bizalomra hagyatkozni, hiszen van külső és belső interfésze. A tűzfalkészletes útválasztón viszont kézzel kell beállítani a bizalmi viszonyokat. Elhatározhatjuk például, hogy nem engedélyezzük a bejövő (vagyis a kívülről befelé irányuló) Telnet-kapcsolatokat, így a hozzáférés-vezérlő listán leblokkoljuk a 21. (telnet) végpontot. Ugyanígy letilthatjuk az internetből a hálózatunkba irányuló SNMP-forgalmat is.

Ez azt jelenti, hogy a tűzfalkészlet nem pontosan ugyanúgy viselkedik, mint egy tűzfal, de ez mostanra már bizonyára nyilvánvalóvá vált.

A tűzfalkészlet lehetővé teszi a csomag tartalmának vizsgálatát, ami szerfelett hatékony módja a hálózat biztonságossá tételének. Ha engedélyezzük a nyolcvanas (HTTP) végponton befelé irányuló forgalmat, de csak a webszerver irányába, akkor a biztonság nem sérül, ugye? *Nem igaz! Ez csupán hamis biztonságérzetet nyújt!* A támadók tudják, ha van egy webhelyünk, akkor eléréséhez engedélyeznünk kell a HTTP-forgalmat, ezért olyan HTTP-csomagokat küldenek, amelyek kifejezetten a webszerver gyenge pontjait támadó rosszindulatú kódot tartalmaznak. Nem kell azonban kétségbeesni – a CBAC ez ellen is véd.

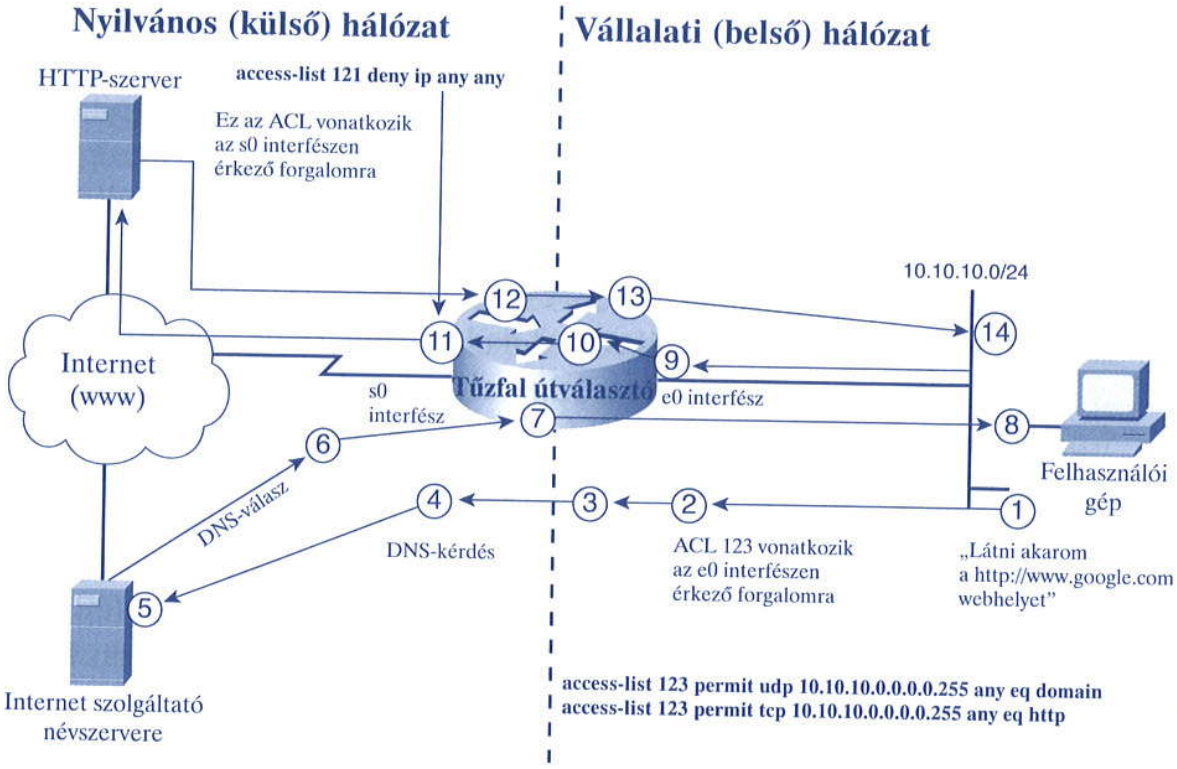
A CBAC a csomagok tartalmának vizsgálatát egyszerű alapelv szerint végzi: az ellenőrzés megelőzi az engedélyezést. Az ellenőrzés eredményétől függően szűrhetjük a csomagot, amint azt a 6.3. ábra mutatja.



6.3. ábra. CBAC biztonsági ellenőrzés

Az ACL formájában persze számos helyen nyílik lehetőség az ellenőrzésre. A tűzfalkészlet és a CBAC által támasztott egyetlen követelmény az, hogy a szűrésnek a vizsgálat után kell megtörténnie. Mivel a tűzfalkészlet is a beszélgetés irányától függően határozza meg a hozzáférést, így az útválasztó elsődlegesen továbbra is útválasztóként működhet.

A tervezési nézőpontból vizsgálva a CBAC üzembe helyezése előtt gondosan végig kell gondolni a hatásait, és elemezni kell a forgalmat, különösen a „kifejezett engedély szükséges" jellegű hozzáférési modell szerint kialakított környezetben. Most vizsgáljuk meg a tűzfalkészlettel bővített IOS-szoftvert használó útválasztó biztonsági folyamatait egy példán keresztül. A 6.4. ábrán szintén nyomon követhetők az egyes lépések.



6.4. ábra. A tűzfalkészlettel bővített Cisco IOS működése

1. A vállalati hálózatban, vagyis a belül lévő felhasználó a saját gépén begépeli a böngészőjének a http://www.google.com útnevet, és megnyomja az Enter gombot.
2. Mielőtt a google webhelyével létrejöhetne a kapcsolat, a felhasználó gépének mindenekelőtt fel kell oldania (IP-címmé kell alakítania) a megadott nevet, ezért elküld egy névfeloldási (DNS) kérést az őt kiszolgáló névszervernek. A DNS névfeloldási kérés megérkezik a peremi útválasztó belső ethernet interfészére. A csomag, egy UDP-távadat *(datagram)*, az ACL 123 (vagyis a belső interfészre érkező forgalmat szabályozó lista) szerint kiértékelésre kerül.
3. Amennyiben ez a hozzáférési lista megengedi a DNS névfeloldási kérések áthaladását, akkor a csomag továbbhaladhat a külvilág felé; ha nem

engedi meg, akkor viszont az útválasztó automatikusan eldobja azt (alapértelmezett megtagadás).

Amennyiben a hozzáférés-ellenőrző lista szerint a DNS-kérés áthaladása engedélyezhető, akkor a csomagot a CBAC is megvizsgálja, és állapotinformációit, nevezetesen a forrás IP-címét és végpontszámát, a cél IP-címét és végpontszámát, valamint a protokollt feljegyzi a saját táblájába.

4. A CBAC ebből a kigyűjtött adatból az ACL 121-ben (az útválasztóra kívülről érkező valamennyi csomagot ellenőrző listában) készít egy ideiglenes engedélyező utasítást. A hozzáférési lista új **permit** (engedélyező) utasítása kizárólag a forgalmat kezdeményező felhasználói gépre irányuló, és a cél címéről (jelen példában a névszerverről) visszaérkező forgalmat engedélyezi, amennyiben az ugyanazon végpontszámokat és protokollt használja, mint a kimenő csomag. Ez az ideiglenes lista az ACL 121 elejére (a lista által már tartalmazott összes statikus engedély elé) kerül bejegyzésre. Ne feledjük, az UDP nem kapcsolatorientált protokoll, így a TCP-kapcsolatoktól eltérően némi trükkre van szükség ahhoz, hogy képesek legyünk mégis nyilvántartani az ilyen párbeszéd állapotát.
5. A DNS névfeloldási kérés (UDP 53. végpont) kijut az útválasztó külső interfészén, majd a névszerver a feldolgozása után a felhasználó gépének címezve visszaküldi a választ. Az előző lépésben dinamikusan felvett új engedélyező utasítás öt másodpercig marad a hozzáférés-ellenőrző listában. Ha az útválasztó ezen idő alatt nem kap választ, akkor az ezen kapcsolathoz tartozó ideiglenes bejegyzés megszűnik.
6. Amikor a névszerver (DNS) válaszüzenete megérkezik az útválasztó külső interfészére, a továbbhaladási engedély megadásához mindenekelőtt megvizsgálja az ACL 121 listát. Mivel a lista élén megtalálja az engedélyező utasítást, így a csomagot egy korábban már felépített kapcsolathoz tartozónak tekinti, és engedélyezi az áthaladását.
7. A csomag az útválasztóba való bejutás után a CBAC-hez kerül, amely megvizsgálja a DNS-választ, majd továbbengedi azt a felhasználó gépe felé. Mivel a munkamenet UDP-alapú, így a feljegyzett állapot az alapértelmezett időzítés szerinti ideig a táblában marad, majd törlődik, akárcsak az ideiglenes ACL-bejegyzés.

A tűzfalkészletet futtató útválasztó esetén használt terminológia szerint az első csomag folyamatkapcsolt (process-switched), míg az azonos munkamenethez tartozó minden további csomag gyorskapcsolt (fast-switched).

8. A DNS-válasz megérkezik a felhasználó gépére, amely ezáltal megismeri a google webszerver IP-címét. Ezen cím alapján létrehozható a HTTP-munkamenet. Mivel a HTTP (www) TCP-t használ, ezért az első elküldött csomag a TCP SYN (szinkronizálás) kérése lesz, amely a gépek közötti háromutas kézfogás protokoll első lépése.
9. A HTTP-csomag megérkezik az útválasztó belső Ethernet interfészére. Az útválasztó megvizsgálja a kifelé menő forgalmat vezérlő 123-as lista alapján, s mivel ez egy HTTP- (nyolcvanas végpontra irányuló) csomag, így áthaladása engedélyezhető.
10. Mivel az ACL 123 szerint a HTTP-csomag engedélyezhető, így a csomagot a CBAC is megvizsgálja, és állapotinformációit, nevezetesen a forrás IP-címét és végpont-számát, a cél IP-címét és végpont-számát, valamint a protokollt feljegyzi a saját táblájába.
11. A csomagot továbbítja a webszerverhez, miközben az állapottábla-bejegyzés alapján az ACL 121 elejére a visszafelé irányuló forgalom számára elhelyez egy engedélyező utasítást. Mivel a HTTP-protokoll TCP-átvitelt használ, így az ideiglenes bejegyzés 30 másodpercig teszi lehetővé a megcímzett gépről a SYN-ACK (kapcsolatfelvételi kérés elfogadva) válaszcsomag megérkezését. Ha a válasz ezen időtartamon belül nem érkezne meg, akkor a dinamikusan létrehozott engedély, valamint az állapottábla-bejegyzés is törlődik.
12. Amikor a válasz megérkezik az útválasztó külső interfészére, akkor az ACL 121 szerint ellenőrzésre kerül. Mivel az ideiglenes engedélyt a CBAC korábban már beírta ezen lista elejére, így a válasz áthaladása engedélyezhető.
13. Miután az útválasztó beengedte a válaszcsomagot, a CBAC megvizsgálja a protokoll szintaxisa szerinti megfelelőségét. Amennyiben a csomag fejléce, vagy maga az adat nem felel meg a szintaxisnak, a CBAC eldobja a csomagot és lezárja a kapcsolatot. Ha a csomag hibátlan, akkor továbbítódik az eredeti kezdeményező gép felé.
14. A HTTP és más többmenetes protokollok esetén, amelyek végrehajtásához több kommunikációs munkamenetet kell létrehozni, a CBAC folyamatosan frissíti az állapottábláját, és a külső interfészre érkező hozzáférés-vezérlő listát.

Valamennyi, a CBAC által készített ideiglenes engedélyező utasítás törlődik akkor, amikor a hozzá tartozó minden egyes kommunikációs munkamenet befejeződik, mégpedig a protokolltól függően:

- AZ ICMP- és UDP-munkamenetek akkor törlődnek, amikor az adott párbeszéd az útválasztó beállításakor meghatározott ideig szünetel.
- A TCP-munkamenetek a FIN-csomagok cseréje utáni ötödik másodperc elteltével törlődnek. Amennyiben megérkezne egy RST-csomag,

akkor a munkamenet azonnal lezárul, és a hozzá tartozó ACL-engedélyek is törlődnek.

- A CBAC alapértelmezésben:
  - A félig megnyitott kapcsolatokat elkezdi lezárni, amennyiben számuk meghaladja az ötszázat.
  - A félig nyitott kapcsolatok lezárását félbehagyja, amikor számuk négyszáz alá csökken.
- A félig nyitott kapcsolatok nagy száma azt jelentheti, hogy egy DoS (szolgáltatásmegtagadási) támadás kezdődött valamilyen portletapogató, vagy más felderítő módszerrel, amely félbemaradt kapcsolatfelvételi (félig nyitott) munkamenetek segítségével kíván információt gyűjteni.[1]

6.2.3. A behatolás érzékelése a Cisco IOS segítségével

A Cisco IOS behatolásjelző **kiegészítő csomagja** *(IDS – Intrusion Detection System)* úgy működik, mint egy betörésjelző készülék, folyamatosan figyelve az útválasztón áthaladó csomagokat és kommunikációs munkameneteket, kutatva az esetleges behatolási kísérleteket jelző jellegzetes minták után.

A Cisco a behatolásjelző kiegészítést a tűzfalcsomagban úgy helyezte el, hogy fő céljának a rugalmasságát tartotta, így az egyedi támadásnyomok kivehetők a figyeltek közül, amennyiben nem nyernek megerősítést. Jóllehet a hálózati biztonság növelése érdekében javasolt a CBAC biztonsági motornak mind a tűzfalcsomag, mind a behatolásjelző lehetőségét aktiválni, ezek azonban egymástól függetlenül, és akár az útválasztó külön interfészein is bekapcsolhatók.

A tűzfalcsomag a behatolásjelző technológiát az alapvető tűzfalszolgáltatások kiegészítéseként nyújtja. Korlátozott képességű állandó betörésjelzőként működik, amely az útválasztón áthaladó csomagokat és munkameneteket vizsgálja (működése ezért állandó – minden egyes csomagot megvizsgál annak eldöntésére, hogy a készlet által ismert valamelyik betörési kísérlet nyomait hordozza-e). Amennyiben gyanús tevékenységre utaló nyomot talál – vagyis amikor úgy véli, hogy egy csomag egy támadás mintázatának felel meg –, akkor azonnal közbelép, még mielőtt a hálózat biztonsága sérülne, egyidejűleg feljegyezve a gyanús tevékenységet

1 A SYN támadás egy nagyon elhíresült szolgáltatásmegtagadási (DoS) támadás volt, a támadott rendszerek különböző táblái gyorsan beteltek a félig nyitott kapcsolatokkal, így nem tudtak újabb kapcsolatokat létesíteni. *(A lektor megj.)*

a *syslog* használatával, és bejelentve azt a Cisco biztonságos betörésjelző szoftverét *(Cisco secure IDS)* futtató szervernek is.

A rendszerüzenet naplózása (syslog – system message logging) a rendszer és futó folyamatai számára azt teszi lehetővé, hogy a rendszer állapotüzeneteinek különböző típusai naplózhatók legyenek. Alapvetően háromféle állapotüzenet van: hiba, tájékoztató és hibakereső. A Cisco IOS-szoftver egy meglehetősen átfogó naplózó és hibafeljegyző eszközt is tartalmaz. Összesen ötszáznál is több szolgáltatásazonosító segítségével kategorizálja a rendszer állapotait. A rendszernapló nagyon fontos szerepet játszik a problémák diagnosztizálása során, a kiegészítő csomagok, például a tűzfalkészlet által készített naplóbejegyzések pedig az események észlelését könnyítik meg.

A tűzfalkészlet korlátozott behatolásészlelési képességgel rendelkezik, mivel a támadások jellemző mintái bele vannak égetve az IOS-be, s így nem változhatnak, hacsak az IOS újabb verzióját nem hozzuk létre, amelyet be kell tölteni az útválasztóba. Ezzel szemben az önálló IDS-eszközbe az új minták viszonylag könnyen betölthetők. A gyakorlatban persze ez azzal jár, hogy a hálózat biztonságáért felelős szakembereknek állandóan biztosítaniuk kell azt, hogy a jellemző támadási minták minél frissebbek legyenek. A hálózat rendszergazdája be tudja állítani az IDS-csomaggal kiegészített útválasztón azt, hogy a különböző fenyegetésekre milyen választ adjon. Amennyiben egy munkamenet csomagjai megfelelnek valamelyik támadási mintának, az útválasztó az alábbi módon viselkedhet:

- riasztást küld a naplózó szervernek, vagy a Cisco biztonsági IDS-vezérlőnek (központosított vezérlés esetén),
- eldobja az érintett csomagot,
- lezárja a TCP-kapcsolatot.

A javasolt biztonsági eljárás az, hogy a csomag eldobását és a kapcsolat lezárását egyszerre végezzük. A gyakorlatban ez azt jelenti, hogy amikor a tűzfalkészlet IDS-modulja az IDS támadási mintáknak megfelelő csomagot kap, eldobja azt, így az nem tud bejutni a védett hálózatba. A támadások azonban általában több csomagban érkeznek, ezért közülük egynek az eldobása nem lenne elégséges védelem. Az IDS-modul ezért a támadó csomagot küldő eszköznek küld egy TCP-lezárás *(reset)* csomagot, amelynek hatására a kapcsolat véget ér. Így tehát az adott támadócsomagot eldobja, a támadásban érintett kommunikációs csatornát pedig lezárja, ezzel biztosítva a leghatékonyabb védelmet.

6.2.4. Mikor használjuk a tűzfalkészlet IDS-modulját?

A Cisco IOS-tűzfalkészlet behatolásérzékelő moduljának képességei kiválóan megfelelnek az intranet, extranet, és a kihelyezett irodai hálózatok bejáratának őrzésére. Bármilyen méretű és összetettségű hálózat védelme sokkal erősebbé válik vele, hiszen automatikusan képes elhárítani a belső és külső gépektől érkező támadásokat egyaránt.

A Cisco IOS-tűzfalkészlet behatolásérzékelő modulja valamennyi vásárló biztonsági elvárásainak kielégítésére lett kifejlesztve, és a következő helyzetekben különösen hasznos:

- Vállalati felhasználók, akik a hálózati átjárók biztonságát az alhálózati határokon átívelő, költséghatékony módon akarják megoldani – különösen a kihelyezett irodák, intranet és extranet határok védelme során.
- Kis- és középvállalkozások, amelyek költséghatékony módon akarnak behatolásérzékelő tűzfalkészlettel is ellátott útválasztót vásárolni.
- Azon szolgáltatók, akik felügyelt szolgáltatásokat akarnak nyújtani úgy, hogy ügyfeleiket ellátják tűzfalas védelemmel és behatolásérzékelővel egyaránt, mindezeket beépítve az egyébként is szükséges útválasztóba.

6.2.5. A tűzfalkészlet IDS-moduljának működése

Mostanra világossá kellett válnia, hogy a csomagok megértése nagyon fontos a hálózatokban. Egyesekhez nehezen jut el ez a felismerés, az igazság elfogadása után azonban a hálózati fogalmakat sokkal könnyebb megérteni. Minden a csomag, és valamennyi hálózati eszközt arra terveztek, hogy a csomaggal tegyen valamit. Ez lehet a csomag továbbküldése a célja felé, lehet a megvizsgálása, vagy akár a valamilyen cél érdekében végzett megváltoztatása. Számos kalóz is rájött erre az igazságra, bár ők ezt a tudást a sötét oldal szolgálatába állították. Ez drámaian hangzik, de sajnos igaz, hiszen egyáltalán nem mulatságos egy szervert hajnali háromkor újra beállítani csak azért, mert valaki feltörte azt; még kevésbé vidám egy féktelenül szaporodó vírussal küzdeni, amelyik térdre kényszerítette a hálózatunkat. Ez a könyv nem kíván senkit a csomagok szakértőjévé varázsolni, azonban bemutatja a hálózati biztonsággal kapcsolatos alapvető igazságokat, amelyek a mindennapi műveletek megértésének biztos alapját adják. Ha ennél többre lenne szükség, akkor elölről kell kezdeni a megismerést. Mindezzel együtt nem kell leereszkednünk a csomagok szintjére; elég, ha tudjuk, hogy vannak csomagok, s hogy azok alkotják a *hálózati működés* lelkét.

A csomagok szintével kapcsolatos tudás átadására véleményem szerint Laura Chappell a legalkalmasabb. Számos anyaga állandóan megtalálható a http://www.packet-level.com honlapon. Látogassa őt meg!

A behatolásérzékelővel kiegészített tűzfalkészletet a Cisco rugalmasnak tervezte, így a hamis találatok esetén az érintett támadási minták kikapcsolhatók a figyelésből. Ráadásul, jóllehet ajánlott mind a tűzfalkészletet, mind a behatolásérzékelést egyszerre bekapcsolni, hiszen a hálózat biztonságát így növelhetjük a legjobban, ezek mégsem függnek össze, és külön-külön is engedélyezhetők, vagy akár külön útválasztó interfészenként ki- és bekapcsolhatók.

Az IDS úgy működik, mint egy állandó behatolásjelző érzékelő, állandóan figyelve az útválasztó interfészein áthaladó csomagokat, és ezek alapján cselekedni képes egy előre beállítható módon.

Az IDS a leggyakoribb támadásokat deríti fel azzal, hogy felismeri a hálózati forgalommal való visszaélés leggyakoribb módjait (a **támadási mintákat**). Ezeket a mintákat az ilyen jellegű támadások széles készletéből választották ki, és tartalmazzák a legnagyobb biztonsági rések kihasználásának, a leggyakoribb hálózati támadásoknak és az információgyűjtő letapogatási kísérleteknek a mintáit.

A Cisco IDS által használt mintákat négy csoportba sorolhatjuk:

- **Elemi információs minta** – Az elemi minták olyan egyszerűek lehetnek, mint egy adott gépen egy adott port elérése, például egy portletapogatás.
- **Összetett információs minta** – Az összetett minták bonyolult támadások kivédésére valók, mint például a műveletek meghatározott sorrendje, amelyek tetszés szerinti időtartamban különböző gépek között vannak megosztva. Általánosságban megfogalmazva, mindkét típusú információs minta a támadó információgyűjtő tevékenységére utal.
- **Elemi támadási minta** – Olyan minták, amelyekkel egy támadó egy gépet kíván elérni.
- **Összetett támadási minta** – Olyan minták, amelyek bonyolult támadásokra jellemzők, és amelyek tetszés szerinti időtartamban több gépet is érintve következnek be.

A Cisco IDS a működő hálózatban általában be nem következő tevékenységre utaló mintákat képes felismerni.

A következő URL a Cisco IDS hálózatbiztonsági adatbázisában található sorszámuk szerinti sorrendben tartalmazza a támadási mintákat. Mindegyik minta neve után megtalálható a típusa is (a fenti négy egyike): http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/ products_configuration_guide_chapter09186a00800ca7c6.html.

A Cisco IDS-csomag felülvizsgálati módszere az alábbiak szerint zajlik:

1. A felhasználó létrehoz egy felülvizsgálati szabályt, amely meghatározza a csomagforgalomra vonatkozó támadási mintát, és az egyezés esetén végrehajtandó intézkedést. A felülvizsgálati szabály annyira rugalmas és határozott lehet, amennyire csak szükséges ahhoz, hogy a biztonsági politika előírásainak megfelelhessen. Az alábbi példa segítségével az e-levelek „szemétforgalma" *(spam)*, pontosabban ennek egy része akadályozható meg úgy, hogy az IDS-t utasítjuk valamennyi SMTP-forgalom vizsgálatára, és nem engedjük meg azon leveleket, amelyek száznál több címzettet tartalmaznak:
   ```
   ip audit smtp spam 100
   ```
2. Alkalmazzuk az útválasztó megfelelő interfészén a felülvizsgálati szabályt, egyben megadva a kívánt forgalmi irányt is (befelé vagy kifelé). A következő példa az útválasztóra irányuló minden SMTP-forgalom felülvizsgálatát írja elő:
   ```
   ip audit smtp in
   ```
3. Amennyiben a felülvizsgálati szabályt az interfész befelé irányuló forgalmára alkalmazzuk, akkor a beérkező csomagokat még azelőtt megvizsgálja, hogy a tűzfal ACL eldobhatná azokat. Támadás vagy információgyűjtő tevékenység bekövetkezése esetén ez lehetővé teszi a rendszergazda figyelmeztetését még akkor is, ha az útválasztó egyébként eldobja az érintett csomagokat. Mindenképpen javasolt ezért a felülvizsgálati szabályokat alkalmazni a beérkező csomagokra.
4. Amennyiben a felülvizsgálati szabályt az interfész kifelé irányuló forgalmára alkalmazzuk, a csomagokat akkor vizsgálja meg, amikor egy másik interfészen beérkeznek az útválasztóba. Ebben az esetben a másik interfész beérkező szűrési szabályait tartalmazó lista alapján egyes csomagok még az előtt eldobásra kerülhetnek, hogy megvizsgálná azokat. Ennek eredményeként bizonyos támadási kísérletek esetleg felderítetlenek maradhatnak, jóllehet a kísérletet vagy az információgyűjtést a csomagok eldobásával meghiúsította.
5. Az interfészen áthaladó, a felülvizsgálati szabályoknak megfelelő csomagokat különböző modulok ellenőrzik. Elsőként az IP-, majd a típusnak

megfelelően az ICMP-, TCP- vagy UDP-modul, végül az alkalmazásszintű modul ellenőriz.

6. Amennyiben a csomag megfelel valamely támadási mintának, akkor a felhasználói beállítástól függően az alábbi akciók következhetnek be:
   - Amennyiben az előírt művelet a **riasztás** *(alarm)*, akkor a modul befejezi a vizsgálatot, riasztást küld, majd átadja a csomagot a következő modulnak.
   - Ha az előírt művelet az **eldobás** *(drop)*, akkor a modul a csomagot eldobja, és nem adja át a következő modulnak.
   - Az **elbontás** *(reset)* művelet előírása esetén a modul a csomagot továbbítja a következő modulnak, és TCP-átvitel esetén mindkét kommunikáló félnek egy TCP reset csomagot küld a kapcsolat elbontása érdekében.

Amennyiben a modul több mintával is egyezőnek találhatná a csomagot, akkor csak az első megfelelés szerinti műveletet végzi el. A más modulok által talált egyezés további műveletek elvégzéséhez is vezethet, de modulonként mindig csak egy művelet kerül elvégzésre. A behatolásérzékelő modul a kapcsolatot kizárólag a TCP-protokoll esetén tudja elbontani, mivel ez rendelkezik a SYN ACK, és az igen erélyes RST *(reset)* utasításokkal, amelyeket az IDS visszaküldhet a támadó gépnek, lezárva ezzel a csatornát és valószínűleg bezárva a támadó alkalmazást. Az UDP nem kapcsolatorientált protokoll, így ott nincs semmi, ami elbontható lenne – ezért van szükség az útválasztóhoz vagy a PIX-tűzfalhoz hasonló blokkoló eszközökre.

6.2.6. A TŰZFALKÉSZLET KORLÁTAI

A környezetfüggő hozzáférési vezérlés (CBAC) megnöveli az IOS-útválasztók biztonsági eszközként való üzemeltetésének hatásosságát. Az IOS-útválasztók a csomagtovábbításnál sokkal többre is képesek, megnövelve így használhatóságukat, és lehetővé téve a rendszergazdák számára a biztonságosabb hálózatok költséghatékony kialakítását. Természetesen tökéletes biztonsági eszköz nincs. Van azonban néhány olyan működési kérdés, és a CBAC-nek néhány olyan korlátja, amelyre figyelemmel kell lenni:

- A behatolásérzékelő okozta esetleges teljesítményromlás a minták beállításától, az útválasztón keresztül haladó forgalom nagyságától, az útválasztó szoftverétől, és az útválasztón beállított más egyedi lehetőségek (például titkosítás stb.) mennyiségétől függ. Az egyes minták engedélyezése vagy tiltása nem módosítja a teljesítményt észrevehető mértékben; a hozzáférés-vezérlő listákat használó mintáknak azonban

jelentős kihatása van a teljesítményre, hiszen minél alaposabban vizsgáltatjuk az útválasztóval a csomagokat, annál hosszabb időre van ehhez szükség.

- Az elemi minták felülvizsgálata nem igényli a forgalomfüggő memória meglétét. Az összetett minták vizsgálatához azonban a CBAC memóriát allokál, hogy minden egyes kapcsolat minden egyes munkamenetének állapotát követhesse, hiszen az összetett minták – definíciójukból adódóan – a több géppel való kapcsolattartást definiálják. Ugyancsak szükség van memóriára a konfigurációs adatbázis és a belső gyorsítótár céljaira is.
- A CBAC nem vizsgálja az útválasztó interfészének címzett, vagy az onnan feladott csomagokat. Ez kétféleképpen is érinti az útválasztó működését:
  - A virtuális terminál *(telnet)* munkamenetet a kezelő és az útválasztó között nem vizsgálja.
  - A kezelési, feljogosítási és naplózási (TACACS/RADIUS) forgalmat nem vizsgálja, mivel ezek is az útválasztónak vannak címezve.
- A csomagok rejtjelezett tartalmát (például amit a virtuális magánhálózat használ) nem vizsgálja, hacsak nem az útválasztó a kapcsolat egyik kódoló végpontja.

Általában véve minél fejlettebb lehetőségekkel rendelkezünk, annál jobban növelhetjük az útválasztó és a hálózat biztonságát. Ezek a lehetőségek azonban nem vonatkoznak magának az útválasztónak a biztonságossá tételére, ami pedig erősen javallt lenne. A következő pontban ezért az útválasztó biztonságosabbá tételéről beszélünk, mivel a tűzfalkészlet ára és beállításainak nehézsége miatt szinte bizonyosan csak a hálózat határán fogjuk azt üzembe helyezni; ezért tehát a későbbiekben a belső eszközök biztonságosabbá tételéről beszélünk.

6.3. Biztonságos IOS-sablon

Mind ez idáig a fejezetben arról beszéltünk, hogyan tehetjük biztonságossá az útválasztónkat, és miként használhatjuk azt tűzfalként. Ebben a pontban azt taglaljuk, miként lehet tovább növelni az útválasztó biztonságát, ismertetve annak a hálózaton belüli biztonságosabbá tételével kapcsolatos ajánlott módszereket. A rövidség kedvéért nem fogunk a biztonságosabbá tétel érdekében kiadott minden egyes ACL-parancsot külön értelmezni. Ennek a döntésnek két oka van:

- A könyv fizikai terjedelme nem teszi ezt lehetővé, így a fontosabb kérdésekre kell szorítkoznunk. A kihagyott elemek egyébként is bizonyos

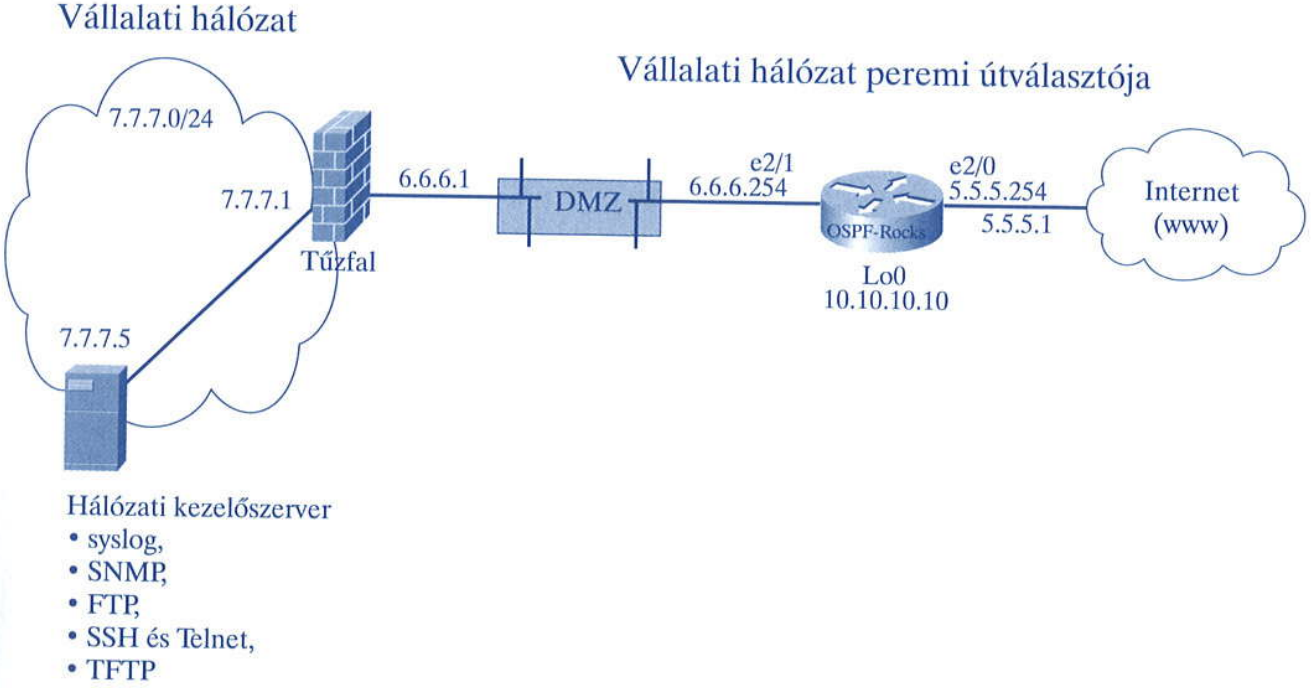
hálózati vállalkozások (például internetszolgáltatók) számára fontosak; a legtöbb hálózatban a többi beállítást könnyen felhasználhatjuk.

- Bizonyos részeket, így például a TACACS és RADIUS kérdéskörét a korábbi fejezetekben már tárgyaltuk, így nincs szükség ezek megismétlésére.

Ezt a pontot nem arra szánjuk, hogy a rövid magyarázatok segítségével megmagyarázzuk, miként tehető biztonságossá az útválasztó, csupán lehetővé tesszük annak eldöntését, hogy a saját hálózatunkban melyik parancsokra van szükség.

A teljes biztonságos IOS-sablon megtalálható az INRGI webhelyen: http://www.inrgi.net/security/secure_ios_template.htm. Ezen a webhelyen a legfrissebb parancsok és magyarázatok találhatók, mivel a biztonság egy állandóan változó probléma.

A Cisco SDM biztonsági eszközkezelő egy természetes, megbízható grafikus szoftver, amelyet a biztonsági/VPN útválasztókkal együtt szállítanak. Ez a CBAC és VPN megbízható telepítő- és beállítóeszköze; tartalmaz útválasztó analizátort is, továbbá lezárja az útválasztót. A felhasználónak ad javaslatot arra nézve is, hogy miként használja az útválasztót: http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html.



6.5. ábra. Biztonsági sablon hálózati topológiája

A 6.1. példában a beállító parancsokat vastagon szedtük, így azok élesen elválnak a magyarázatoktól, amelyeket a jobb olvashatóság kedvéért *eltérő háttérszínnel* is kiemeltünk. A biztonsági sablon a 6.5. ábrán látható hálózati topológiát feltételezi.

6.1. példa. Biztonsági sablon

```
!
A nagle torlódásvezérlő algoritmust számos vállalat bekapcsolja, hogy
megnövelje az útválasztó felé irányuló telnetforgalom teljesítményét. A
hagyományos telnet TCP alapú. Amikor gépek között billentyűlenyomásokat
akarunk átvinni, a TCP hajlik arra, hogy minden egyes parancsot külön
csomagként vigyen át. A nagyobb hálózatokban a sok kicsiny csomag
elhasználja a sávszélességet, s így kialakul a torlódás. John Nagle
algoritmusa (RFC 896) a TCP ezen problémáját van hivatva kiküszöbölni.
Általánosságban az alábbiak szerint működik: A kapcsolat létrehozása után
az első lenyomott karaktert önálló csomagban viszi át, de minden további
karaktert visszatart mindaddig, amíg a fogadó nem nyugtázza a karakter
megérkezését. Ekkor egy második, nagyobb csomagot küld, és a további
karaktereket szintén visszatartja, amíg erre a csomagra is válasz nem
érkezik. Ennek az a hatása, hogy a karaktereket nagyobb csomagokba gyűjti
össze, amelyeket a kapcsolatra jellemző válaszidő szerint postáz. Az
ébrentartó csomagok biztosítják azt, hogy a TCP-kapcsolat nem szakad meg.
!
service nagle
!
Engedélyezi az ébrentartó csomagok küldését a beérkező kapcsolatok esetén,
így biztosítva azt, hogy a távoli rendszer összeomlása vagy
szétcsatlakozása nem okozza az útválasztó hozzáférhető telnet
végpontjainak blokkolódását vagy elhasználódását.
!
service tcp-keepalives-in
service tcp-keepalives-out
!
Alapértelmezés szerint a naplóbejegyzések nem kapnak időbélyeget, ami pe-
dig lehetővé tenné azt, hogy az esemény bekövetkezésének időpontját ismer-
jük. Célszerű ezért kézzel bekapcsolni a hibakereső és a naplózó bejegyzé-
sekhez az időbélyegzést egészen ezredmásodperces pontossággal, gondoskodva
egyúttal az útválasztó órájának pontos beállításáról is, így minden üzenet
friss volta egy szempillantással ellenőrizhető. A következő beállítás min-
den üzenet elé elhelyez egy időbélyeget, ami a következőképpen néz ki:

Sep 4 23:58:11.437: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed
state to up
```

A timestamp utasítás parancssori kapcsolói az alábbiak:
-debug: minden hibakereső információt időbélyegezni kell
-log: minden naplózási információt időbélyegezni kell
-datetime: a dátum és az idő is szerepel a syslog üzenetekben
-localtime: az útválasztó a saját helyi idejét írja a napló üzenetekbe
-show timezone: az útválasztó saját órája szerinti időzóna is szerepeljen az időbélyegben (hasznos lehet, ha a hálózat több időzónára is kiterjed; ebben az esetben azt javasoljuk, hogy egyetlen időzóna legyen beállítva)
- -msec: az időt ezredmásodpercben adja meg - hasznos lehet, ha NTP van beállítva.

```
!
service timestamps debug datetime msec show-timezone localtime
service timestamps log datetime msec show-timezone localtime
!
```

Alapértelmezésben a syslog üzenetek az útválasztó elhagyására használt interfész IP-címét tartalmazzák. Beállíthatjuk azonban úgy is, hogy minden syslog üzenet ugyanazon IP-címet tartalmazza, függetlenül a használt interfésztől. Számos nagyvállalat vagy internetszolgáltató cég a loopback interfész címét állítja be, hogy könnyebben azonosíthatóvá tegye a hálózata útválasztóit. Ez egységessé teszi a syslog naplókat, és segíti őket a syslog szerver biztonságának növelésében. Amennyiben nem lenne beállítva a loopback interfész, akkor az útválasztó bármely aktív interfészének címe is beállítható.

```
!
logging source-interface loopback0
!
```

Az alábbi parancs a felhasználó számára minimális biztonságot nyújt az IOS konfigurációs állományban tárolt jelszavak számára. A parancs hatására a konfig állományban lévő jelszavakat visszafejthető titkosítással kódolja, ami megakadályozza az embereket abban, hogy a konfigurációs állományra vetett egyetlen pillantással megtudhassák a jelszavainkat. Megjegyezzük, hogy ez a titkosítás nem jelent valódi védelmet, ezért ajánlatos a titkos jelszavak, vagy a TACACS/RADIUS felügyelte bejelentkezés használata helyette.

```
!
service password-encryption
!
```

Alapértelmezés szerint a Cisco bekapcsolja az útválasztók DHCP szolgáltatását. Ez azonban tulajdonképpen nem egy szükséges szolgáltatás, így érdemesebb kikapcsolni. Győződjünk meg arról is, hogy a TCP és UDP kis szolgáltatások ki vannak kapcsolva. Egyik ilyen kis szolgáltatás például a „Chargen", egy karaktergenerátor szolgáltatás , amely hibakeresési céllal képes karaktersorozatokat előállítani. Létezik az „echo"

szolgáltatás, amely a neki küldött valamennyi karaktert egyszerűen visszhangozza. Amennyiben a „chargen" szolgáltatást az „echo"-ra irányítjuk, akkor egy olyan hurkot hozhatunk létre, amely hatalmas forgalmat generál az útválasztón, nyilvánvalóan túlterhelve annak CPU- és RAM-kapacitását. Így tehát komoly szolgáltatásmegtagadási (DoS) támadást lehet kivitelezni. Az ilyen támadások megakadályozásának legegyszerűbb módja, ha letiltjuk ezeket a szolgáltatásokat.

```
!
no service udp-small-servers
no service tcp-small-servers
no service dhcp
!
```

Nem minden szolgáltatás rossz. Az alábbi szolgáltatás is hasznosnak bizonyul a gyakorlatban. Engedélyezésével a syslog bejegyzések számozását kapcsoljuk be, ezzel is megnehezítve azok meghamisíthatóságát.

```
!
service sequence-numbers
!
hostname OSPF-Rocks
!
```

A naplózás szinte minden esetben kötelező, így kapcsoljuk be! A beállítással megkövetelt naplózások miatt továbbá hasznos lehet a másodpercenként küldhető naplóbejegyzések számának korlátozása, nehogy túlterheljük a szervert, mivel az ACL-ek naplózása során az üzenetek száma gyorsan megnövekedhet!

```
!
logging 7.7.7.5
logging buffered 16384 debugging
logging rate-limit ?
!
```

Amikor az útválasztó konzol bemenetére üzenet érkezik, ez egy CPU-megszakítást eredményez, és a konzolra menő további naplózó üzeneteket letiltja, amíg újra szükség nem lesz rájuk. A konzolra menő naplózás nagyon hatékony eszköze a hibakeresésnek; amikor fizikailag csatlakozunk az útválasztóhoz, fontoljuk meg ezen parancs megváltoztatását.

```
!
no logging console
!
```

A Cisco IOS konfigurációs állományban szinte minden jelszó és más azonosító karaktersor egy gyenge, visszafejthető titkosítás segítségével kódoltan található. Egy adott jelszó kódolási módszerének megismerésére a konfigurációs állományban látható kódolt karaktersort megelőző számot kell megvizsgálni. Ha ez a hetes számjegy, akkor a jelszót a gyenge titkosítás

védi. Az ötös számjegy azt jelzi, hogy az erősebb MD5 kivonatoló algoritmussal kódolt. Jóllehet az „enable secret" paranccsal az engedélyező jelszót adhatjuk meg, nem szabad azonban elfelejteni a „service password-encryption" parancs kiadását sem, hogy a jelszavak ne nyílt szövegként, hanem kódolva szerepeljenek a konfigurációs állományban. A legbiztonságosabb jelszótípus természetesen az „enable secret" segítségével kódolt jelszó, használjunk ezért nagybetűket és számokat is hozzá, így a puszta erővel történő jelszótörés nehezebbé válik. A gyengébb titkosítási módszer az engedélyező jelszót visszafejthetően kódolja. Nagyobb biztonságot nyújt egy nem visszafejthető titkosítási módszer használata. Az erősebb titkosításra elsősorban olyankor van szükség, ha a jelszónak a hálózaton keresztül kell közlekednie, vagy ha egy TFTP-szerveren tároljuk azt.

```
!
enable secret <JELSZÓ>
no enable password
!
```

Használjon TACACS+ vagy AAA belépési hitelesítést. Biztosítja, hogy a helyi témaszám kisbetű-nagybetű érzékeny, így az erőből feltörési kísérletek nehezebbek.

```
!
aaa new-model
aaa authentication login default group tacacs+ local-case
aaa authentication enable default group tacacs+ enable
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting network default stop-only group tacacs+
tacacs-server host 7.7.7.5
tacacs-server key OSPF-rOck2
!
```

Amennyiben a TACACS+ meghiúsul, használjon betűméret-függő helyi hitelesítést, illetve - amennyiben a TACACS+/RADIUS nem elérhető a hálózatban - helyi AAA-t. A helyi hitelesítés a támadókat bizonytalanságban hagyja, miáltal az útválasztó biztonságosabb lesz; emlékezzünk rá, a biztonságot a minél több rétegű védelem jelenti.

```
!
username <FELHASZNÁLÓNÉV> password <JELSZÓ>
!
```

A beépített webszerver kikapcsolását mostanra már remélhetőleg nem is kell indokolni. Néha a Cisco is túl sokat akar beépíteni az eszközeibe, de ez egy útválasztó, nem pedig egy webkiszolgáló.

```
!
```

```
no ip http server
!
Osztály nélküli és a nullás alhálózatok használatát teszi lehetővé.
!
ip subnet-zero
ip classless
!
Senki nem érti, hogy ezek a szolgáltatások miért részei még mindig az IOS-
nek, azt pedig még kevésbé, hogy miért vannak alapértelmezésben
bekapcsolva. Mindenesetre a józan ész azt diktálja, hogy a biztonság
érdekében legyenek kikapcsoltak. A Cisco IOS fejlődése során némelyiket
már alapértelmezésben kikapcsolták, de legjobb erről saját magunknak
gondoskodni.
!
no service pad
no ip source-route
no service finger
no ip bootp server
no ip domain-lookup
!
A TCP-elfogás a TCP-kapcsolati kérések elfogásával és ellenőrzésével segít
megakadályozni a TCP SYN elárasztásos támadást. Elfogó módba kapcsolva a
szoftver a kliensektől a szervereknek küldött, és egy kiterjesztett
hozzáférési listának megfelelő SYN-csomagokat elfogja. Ezekre az
útválasztó válaszol, így a tényleges kommunikációt nem akadályozza.
!
ip tcp intercept list 120
!
Az IOS alaphelyzetben 24 óráig figyeli és kezeli a TCP-kapcsolatot. Senki
nem tudja, miért ilyen hosszan, mindenesetre vegyük rövidebbre.
!
ip tcp intercept connection-timeout 60
!
A félig nyitott kapcsolat csomagjai esetén az alapértelmezett 30 másodperc
helyett elegendő 10 másodpercig várakozni a válaszra.
!
ip tcp intercept watch-timeout 10
!
Az alábbi beállítások azt határozzák meg, hogy mikor kell aktiválni és
deaktiválni az elfogást. Az alapértelmezett 900 és 1100 nem túlságosan
valószerű.
!
ip tcp intercept one-minute low 1500
```

```
ip tcp intercept one-minute high 6000
!
```

A Cisco beépítette a memóriakiírás (core dump) eszközt az IOS-be. Ez ugyanúgy működik, mint számos hasonló rendszer azonos szolgáltatása. Amikor az útválasztó összeomlik, a memóriaképről készül egy másolat, amelyet az újraindításkor kiír egy külső szerverre. Ehhez ott egy FTP-, TFTP- vagy RCP-témaszámot kell létrehozni, és elegendő lemezterületről kell gondoskodni. A memóriaképek elmentése nagyon fontos lehet egy biztonságos útválasztó esetén, mert ha egy szolgáltatásmegtagadási (DoS) támadás miatt összeomlana, a memóriaképből ki lehet deríteni, mi is történt. Az alábbiakban azzal a feltételezéssel élünk, hogy a hálózatkezelő szerveren létrehoztunk egy FTP-témaszámot, amely az útválasztó kapcsolatfelvételi kéréseit fogadja. Arról is meg kell bizonyosodni, hogy a memóriakép állományok önálló nevet kapnak, amint arról lentebb gondoskodunk is. Ajánlatos persze ezt a „Cisco memóriakép témaszámot" annyira biztonságossá tenni, amennyire csak lehetséges. Többek között ellenjavallt olyan FTP-szervernek küldeni a memóriaképeket, amelyek nyilvános FTP-kéréseket is fogadnak, vagy amelyeken vannak más FTP-felhasználók.

```
!
ip ftp username <FTP-SZERVER FELHASZNÁLÓNÉV>
ip ftp password <JELSZÓ>
exception core-file <EGYEDI ÁLLOMÁNYNÉV>
exception protocol ftp
exception dump 7.7.7.5
!
```

Az IOS-frissítések vagy konfigurációk feltöltésének leggyakoribb eszköze a TFTP. A TFTP-szerver biztonságának kritikus szerepe van. Ez jelenti például a forrás IP-címe alapján azonosított TFTP-kapcsolatok kizárólagos engedélyezését. A Cisco IOS lehetővé teszi, hogy egy adott IP-címet használjon a TFTP-hez. Így létrehozható egy rögzített ACL a TFTP-szerveren, amely az útválasztó címét tartalmazza. Ez a rögzített IP-cím általában egy loopback interfész címe, mivel az útválasztó kezelésére gyakran ilyen interfészt választunk. Ha azonban ezt tennénk, akkor a TFTP-szerverhez legközelebbi loopback interfész címét kell megadni az alábbi paranccsal. Az FTP-t hasonlóan állítjuk be, mivel azt korábban már szintén beállítottuk.

```
!
ip tftp source-interface <FORRÁS INTERFÉSZ>
ip ftp source-interface <FORRÁS INTERFÉSZ>
!
```

A CEF egy harmadik rétegbeli bővített kapcsoló technológia az útválasztóban. Ez a leggyorsabb módja a bejövő interfészről a kimenőre

továbbítani a csomagokat. Az alábbi parancs bekapcsolja ezt a lehetőséget. Nem mindegyik útválasztó támogatja azonban, ezért meg kell nézni a dokumentumban a létezését.

```
!
ip cef
!
```

Beállítja az időzónát. A legjobb, ha minden szerveren és útválasztón egy időzónát állítunk be, hogy a hibakeresés egyszerűbb legyen.

```
!
clock timezone GMT 0
!
```

Az NTP a legtöbb hálózat leginkább elnagyolt lehetősége. A hálózati időprotokoll (NTP - network time protocol) a hálózati gépek óráinak szinkronizálására szolgál. Ez adja a munkaállomások, kiszolgálók és más eszközök pontos időjelzését. Az NTP az UDP-t használja, amely az IP fölötti protokoll. Az NTP-hálózat a pontos időt egy hiteles időforrástól veszi, amely lehet például egy rádiószignál- vagy atomóra-vezérelt időszerver. Az NTP ezt az időt szolgáltatja a hálózatnak. A protokoll rendkívül hatékony, percenként alig egy csomagra van szükség ahhoz, hogy két gépet ezredmásodpercnél jobb pontossággal szinkronizáljunk.
A legtöbb rendszergazda a szervereket még összehangolja, de a többi hálózati elemet már nem. Ha azonban mindegyik hálózati eszköz syslog bejegyzéseit összehasonlíthatóvá akarjuk tenni, akkor ezekre is be kell állítani az időszinkront. Márpedig a különböző naplók összehasonlítása alapvető fontossággal bír különböző hibakereső, hibaanalizáló és a biztonsági eseményt követő tevékenység során. A különböző naplózó, kezelő, AAA és biztonsági műveletek pontos időszinkronjának hiányában az ilyen összehasonlításra nincs lehetőség. Amikor aktiváljuk az NTP-t, akkor az útválasztó óráját hozzáigazítjuk egy helyi (megbízható és hitelesített) NTP szerveréhez. Megjegyezzük, hogy a szinkron felvétele lassabb, mint a megtartása; ez egy Cisco-sajátosság, így legyünk türelmesek.

```
!
ntp authentication-key 6767 md5 <TITKOS KULCS>
ntp authenticate
ntp update-calendar
ntp server 7.7.7.5
!
```

Állítsuk be a loopback0 interfészt, hogy az legyen a naplóüzenetek forrása. Ezt gyakran használják az útválasztó protokollok is, mivel egy logikai interfész soha nincs leállítva, így nagyon megbízható. Olyan IP-címet adjunk meg, amely egyértelműen azonosítja az útválasztót.

```
!
int loopback0
```

```
ip address 10.10.10.10 255.255.255.255
no ip redirects
no ip unreachable
no ip proxy-arp
!
```

Állítsuk be és ezzel aktiváljuk a null0 interfészt mint azon célpontot, ahová a rossz csomagokat küldjük. Ez lesz a „börtön" - a csomagok bejöhetnek, de soha nem mehetnek ki.

```
!
interface null0
no ip unreachables
!
interface Ethernet2/0
description Unprotected interface, facing towards Internet
ip address 5.5.5.254 255.255.255.0
!
```

Használunk-e CEF ellenőrzést? A válasz igen, ha az adatút szimmetrikus, de nem, ha aszimmetrikus. Használjuk az alábbi parancsot az útválasztó bejövő interfészén, mint a kapcsolat felső végén. Ezzel az adott interfészen beérkező valamennyi csomagot megvizsgálja. Amennyiben a forrás IP-címe nem található meg az ugyanezen interfészre vonatkozó CEF útválasztó táblában, akkor az útválasztó a csomagot eldobja.

```
!
ip verify unicast reverse-path
!
```

Használjuk a sablon ACL-t (az alábbiakban még szó esik róla). Ez a parancs alapvető fontosságú a sikere érdekében.

```
!
ip access-group 2010 in
!
```

Az útválasztó és az infrastruktúra védelme a forgalom limitálásával alapvető fontosságú. Az értékeket hozzá lehet igazítani a tényleges igényekhez, általánosságban azonban az alábbi számokat javasoljuk. Az UDP 2 MB/s-nál ne legyen nagyobb, bár ha kérésre adott videoszolgáltatást is keresztül kell engedni az útválasztón, akkor ne feledjük, hogy ez is UDP-t használ.

```
!
rate-limit input access-group 150 2010000 250000 250000 conform-action
transmit exceed-action drop
!
```

Az ICMP-nek csak 200 Kb/s sávszélességet engedélyez.

```
!
rate-limit input access-group 160 500000 62500 62500 conform-action
```

```
transmit exceed-action drop
!
A többesküldés legfeljebb 5 Mb/s sávszélességet kap.
!
rate-limit input access-group 170 5000000 375000 375000 conform-action
transmit exceed-action drop
!
Megtiltja az útvonal megismerésére szolgáló ICMP átirányító parancsot;
hadd csodálkozzanak a támadók!
!
no ip redirects
!
Megtiltja az ICMP „gép elérhetetlen" vagy „protokoll elérhetetlen"
válaszainak visszaküldését; semmi okunk nincs arra, hogy a támadók számára
lehetővé tegyük a hálózatunk megismerését.
!
no ip unreachables
!
Az irányított IP-adatszórás (IP directed broadcast) megtiltásának hatására
az útválasztó kevésbé van kitéve a szolgáltatásmegtagadási támadásoknak. A
következő konfigurációs parancs azt jelenti, hogy az irányított adatszórás
fizikai adatszórássá alakítása le van tiltva. Ha engedélyeznénk, akkor egy
adott hálózatba irányuló adatszórást az útválasztó interfészére lehetne
irányítani, ami egyáltalán nem kívánatos, és potenciálisan veszélyes
következményekkel jár. A nem kívánt következmények egyikét jól példázza a
SMURF támadás.
!
no ip directed-broadcast
!
A Cisco IOS-szoftver minden csomagnak megvizsgálja az IP fejlécopcióit.
Támogatja az RFC 791 szerinti szigorú forrásútvonal (strict source route),
laza forrásútvonal (loose source route), útvonalfeljegyzés (record
route), valamint az időbélyeg opciókat. Amennyiben a szoftver egy olyan
csomagot talál, amelyekben ezen opciók valamelyike engedélyezett, akkor
végrehajtja a megfelelő műveletet. Ha érvénytelen opciójú csomagot talál,
akkor a „paraméterhiba" ICMP-üzenetet küldi vissza a forrásnak, és eldobja
a csomagot. Az IP-protokoll lehetővé teszi a forrásgépnek, hogy megadja az
IP-hálózaton belüli követendő útvonalat. Ezt a lehetőséget nevezzük
forrásútvonalnak, amit az IP-fejléc opciójaként lehet megadni. Amennyiben
meg van adva, a Cisco-útválasztó az ennek megfelelő módon továbbítja a
csomagot. Ezt a lehetőséget akkor használjuk, ha egy csomagot
meghatározott útvonalon kívánunk továbbítani a hálózaton keresztül. Az
útválasztó alapértelmezett viselkedése a forrásútvonal végrehajtása.
```

Alapelvként azonban kijelenthetjük, hacsak nincs kifejezetten szükségünk erre a lehetőségre a saját céljaink miatt, akkor kapcsoljuk ki. A forrásútvonal ugyanis egyike az ismert IP-sérülékenységeknek, amelyet a rendszer támadására, vagy egy tűzfal megkerülésére lehet használni.

```
!
no ip source-route
!
```

Az alábbi beállítással letiltjuk, hogy az útválasztó válaszoljon a beérkező ARP-kérésekre az interfészeihez csatlakozó, ismert MAC-című gépek helyett. A csatlakozó hálózatokban a nem kívánatos viselkedést akadályozzuk így meg, egyúttal kiküszöbölve egy lehetséges biztonsági rést is. Másként megfogalmazva megtiltjuk az útválasztónak azt, hogy úgy tegyen, mintha másvalami volna.

```
!
no ip proxy-arp
!
```

Letiltja az ICMP-válaszüzenetek küldését. A Cisco-útválasztók alapértelmezésben nem küldenek ilyet, de semmiképpen sem árthat, ha a biztonság kedvéért kifejezetten letiltjuk.

```
!
no ip mask-reply
!
```

Engedélyezi az IP-nyilvántartást úgy, hogy képes az IP-hozzáférési listáknak meg nem felelő IP-forgalom azonosítására, vagyis az útválasztó minden tiltott kísérletet feljegyez és naplóz. Tessék ezt a naplót gyakran ellenőrizni is!

```
!
ip accounting access-violation
!
```

Amennyiben megengedjük a többescímű küldést, vagy a virtuális alagutak felett kialakított többescímű hálózatban (MBONE) való részvételt, a következő többescímzést szűrő szabályok nyújtanak segítséget a biztonságos többescímű környezet kialakításában. Ezeket mindegyik interfészre alkalmazni kell.

```
!
ip multicast boundary 30
!
```

Az adatfolyamot későbbi vizsgálat számára megtartja. Ha lehetséges, exportáljuk azt egy cflowd szerverre.

```
!
ip route-cache flow
!
interface Ethernet2/1
```

```
description Protected interface, facing towards DMZ
ip address 6.6.6.254 255.255.255.0
Futtatunk-e CEF-ellenőrzést? Igen, ha az adatút szimmetrikus, és nem,
ha aszimmetrikus.
!
ip verify unicast reverse-path
!
Amennyiben használ „reverse path forwarding" lehetőséget, törölje az
alábbi ACL-beállítást.
!
ip access-group 115 in
!
Az alábbi parancsokat korábban már ismertettük, további információért
lapozzon vissza.
!
no ip redirects
no ip unreachable
no ip directed-broadcast
no ip proxy-arp
ip accounting access-violations
ip multicast boundary 30
no ip mask-reply
ip route-cache flow
!
A forrásútválasztás lehetőség megengedi, hogy a továbbítási útvonalat a
csomag megadhassa. Ennek segítségével a csomag például megkerülhetné a
tűzfalat. Tiltsuk le!
!
no ip source-route
!
Ez az internet felé az alapértelmezett útvonal (lehetne helyette egy
útválasztó protokoll is).
!
ip route 0.0.0.0 0.0.0.0 5.5.5.1
!
A tűzfal másik oldalán a hálózat felé vezető útvonal.
!
ip route 7.7.7.0 255.255.255.0 6.6.6.1
!
Az alábbi statikus útvonalak a nyilvános interneten nem továbbítható
hálózatokat „fekete lyukba" irányítják. Nagyon figyeljen oda, ha TCP-
elfogást alkalmazva engedélyezni kívánja őket. A TCP-elfogás parancs az
útválasztót TCP-végpont helyettesként (socket proxy) való működésre
```

utasítja. Amikor az útválasztó megkap egy SYN-csomagot, az útválasztó (a címzett helyett) válaszol egy SYN|ACK-csomaggal. Emiatt jelent problémát a fekete lyukba irányítás és a TCP-elfogás. Amennyiben fekete lyuk útvonalakat állítunk fel, és egy null eszközre (korlátlan nyelő) irányítjuk azokat, majd valaki elindít egy SYN elárasztásos támadást egy tiltott IP-címről, akkor az útválasztó a SYN|ACK-csomagokat a null eszközre küldi (ahonnan persze nem kap választ). Ma (még) nem elég intelligens ahhoz, hogy felismerje ezt a támadást, így a TCP-elfogás várósora gyorsan megtelik, mivel alapértelmezés szerint az időtúllépés nem elég rövid ahhoz, hogy megoldja ezt a problémát.

```
!
<<<A parancsokat lásd:
<<<http://www.inrgi.net/security/secure_ios_template.htm
!
```

A NetFlow-adatokat exportálja a NetFlow-szerverre (7.7.7.5). A NetFlow néhány olyan statisztikát ad, amelyek hasznosak lehetnek egy forrás visszakeresésénél a címhamisításos támadás esetén is. Az ajánlott gyakorlat szerint a loopback interfészt használjuk forrásként.

```
!
ip flow-export source loopback0
ip flow-export destination 7.7.7.5 2055
ip flow-export version 5 origin-as
!
```

Minden érdekeset naplózzon a syslog szerverre. Fogjon el minden, a loopback interfészre irányított naplózó kimenetet, így az útválasztó azonosítója a különböző helyeken feljegyzett adatokban könnyen azonosítható és egyértelmű lesz.

```
!
logging trap debugging
logging source-interface loopback0
logging 7.7.7.5
!
<<<A további parancsokat lásd:
<<<http://www.inrgi.net/security/secure_ios_template.htm
!
```

Ne ossza meg a Cisco Discovery Protocol (CDP) információkat másokkal, mert ez a hálózat topológiájáról, az eszközök konfigurációiról, a használt hálózati eszközökről, IP-címekről és hasonló kritikus információkról adna tájékoztatást. A paranccsal a CDP globálisan letiltható. Ha egy adott interfészen mégis szükség lenne rá, akkor helyette engedélyezze a CDP-t (cdp run), és tiltsa le azt az internet felé néző interfészen (not enable cdp). Másként megfogalmazva a CDP-t csak azon interfészeken használja, ahol tényleg szükség van rá, de soha nem lehet globálisan engedélyezve.

Megjegyezzük, hogy a Cisco a 11.1CA verziójú IOS-től kezdve minden eszközét úgy szállítja, hogy a CDP engedélyezve van.

```
!
no CDP run
!
```

Az SNMP nagyon fontos a hálózat menedzselése szempontjából, különösen ha a felhasználói statisztikák miatt az MRTG-vel együtt használjuk. Az SNMP-hozzáférés biztonságosabbá tételéhez a <COMMUNITY> karaktersor helyén használjunk egy jó jelszót, amelyet a kis- és nagybetűk, valamint számok használatával nehezen kitalálhatóvá teszünk. Végső soron ez a jelszó az SNMP-hozzáférés jelszava, így ennek is követnie kell a vállalat jelszó házirendjét. Erre már csak azért is szükség van, mert ez a jelszó nincs titkosítva. A hozzáférést azonban később tovább nehezíthetjük, ha a hozzáférési listákban beállítjuk azokat a minimálisan szükséges gépeket, amelyeknek joguk van az SNMP-hozzáférésre (persze csak ha tudják a jelszót), a többiekről pedig megtiltjuk azt. Valahogy így nézne ki a többrétegű védelem!

Amennyiben az SNMP-t írható/olvasható módban kívánjuk alkalmazni, nagyon gondosan elmélkedjünk azon, valóban van-e erre szükségünk, mivel az ilyen beállítás meglehetősen sérülékennyé teszi az útválasztót. Magam is láttam, sőt terveztem is olyan eszközöket, amelyek segítségével az SNMP-írás/olvasás segítségével automatikusan alaphelyzetbe állíthattam a jelszavakat, és megváltoztathattam a beállítást. Ha lehet, tegyünk egy ACL-t rögtön a hálózat belépési pontjára, lehetetlenné téve így a támadók számára az SNMP-n keresztüli próbálkozásokat. Számos szabadon vagy a kereskedelemben hozzáférhető eszköz van arra, hogy bármilyen hálózatot végigpróbálgasson az SNMP segítségével. Ezzel egész hálózatokat térképezhetünk fel, és/vagy felfedezhetjük azokat az eszközöket, amelyeken nyitva maradt az SNMP. A biztonsági auditok és a sérülékenységi felmérések során általában gyakran használtam az SNMP-t a hálózat felderítésére, és sokszor voltam képes értékes információtömegre szert tenni a segítségével.

```
!
snmp-server community <COMMUNITY> RO 20
snmp-server location Budapest, Hungary
snmp-server contact INGRI: Kis Pal [kispal@netcerts.hu]
snmp-server host 192.168.254.70 <COMMUNITY>
!
```

A konfigurációban ez az ACL máshol jelenne meg, a teljesség kedvéért azonban itt mutatom be. A 20 jelű ACL akkor engedi meg az SNMP-hozzáférést ehhez az eszközhöz, ha a kérés a 7.7.7.5 IP-című szerverről érkezik, minden más hozzáférést pedig letilt. Megjegyzendő, hogy az általában kihagyott „deny any" parancs is szerepel, mivel a „log" kulcsszóval kiegészítve naplózni is akarjuk a sikertelen SNMP-hozzáférési kísérleteket.

```
!
access-list 20 remark SNMP-hozzáférési lista
access-list 20 permit 7.7.7.5
access-list 20 deny any log
!
Mutassuk be magunkat egy megfelelő üzenettel, amely utal a védelem
mértékére és a megfigyelésre. Fontos, hogy az útválasztót elérni kívánó
felhasználók figyelmét felhívjuk arra is, milyen következményei lehetnek
egy támadásnak. Jóllehet csak a „napi üzenet" (motd - message of the day)
üzenetet mutatjuk, ugyanez megadható a konzol és a tartalék portra, az AAA
bejelentkezésre, és valahányszor a felhasználó végrehajtási (EXEC) módba
kapcsol.
!
banner motd %
Figyelem! Ezt a rendszert kizárólag az arra feljogosított személyek
használhatják, a jogosítványukban szereplő céllal. A rendszer eléréséhez a
felhasználónak rendelkeznie kell az írásos engedéllyel. Használata során
nem várható el a magántitok védelme, és a felhasználók tevékenysége
állandó megfigyelés alatt áll, amelyről feljegyzések is készülnek. A
rendszer használatával Ön kifejezetten hozzájárul ahhoz, hogy
tevékenységét megfigyeljük és rögzítsük, s ezeket bizonyítékként
felhasználjuk Ön ellen, amennyiben a megfigyelés során bármilyen
illegális, nem megengedett használati kísérletre derülne fény. A
feljegyzéseket ilyen esetben a megfelelő hatóságokhoz továbbítjuk, akik a
polgári és a büntető törvénykönyv rendelkezései alapján a törvény
szigorával fognak eljárni.

A rendszer jogosulatlan használata hazai és nemzetközi törvényeket sért,
amelynek következménye pénzbüntetés és/vagy szabadságvesztés lehet. Minden
IP-forgalmat naplózunk, és a törvénysértők ellen megtesszük a
feljelentést.
%
Az „EXEC" üzenet jelenik meg akkor, ha egy felhasználó sikeres
bejelentkezés után „végrehajtási" (exec) módba kapcsol. Ez a mód
egyenértékű a UNIX-rendszerek szuperfelhasználói, illetve a Windows-
rendszerek adminisztrátori témaszámával.
!
banner exec ^
Kérem, vegye figyelembe, hogy ez az útválasztó egy vállalati hálózat
része, és a rajta végrehajtott valamennyi változtatást előzetesen jóvá
kell hagyatni. Minden változtatást fel kell jegyezni, és a korábbi
beállításokat el kell menteni.
^
```

```
!
```

Használjunk jelszót az útválasztó konzol portján is. Ezzel a védelem egy újabb rétegét helyezzük üzembe, hiszen így az eszköz fizikai elérése esetén is csak a jelszó ismeretében lehet ténylegesen parancsokat kiadni. A „transport input" parancs segítségével letiltható a telnet, és a fizikai portok is védhetők a hozzáféréstől.

A kapcsolat alapértelmezett időtúllépési értéke mind a konzolon, mind a tartalék porton 10 perc. Ezt vezérli az „exec-timeout" parancs, amint az alábbi beállítás is szemlélteti. A telnet (vty) kapcsolatokhoz viszont nem tartozik alapértelmezett időtúllépés. Hibás gyakorlatnak számít azonban, ha nem is rendelünk hozzá értéket, mert így az útválasztó néhány elérhető portját gyorsan el lehet fogyasztani, s így vészhelyzet esetén sem tudunk távolról beavatkozni. Megjegyzendő, hogy a nulla értékű időtúllépés azt jelenti, hogy végtelen ideig élhet a kapcsolat.

```
!
line con 0
 exec-timeout 15 0
 transport input none
line aux 0
 exec-timeout 15 0
 transport input none
!
```

A telnet-portokhoz továbbá célszerű hozzáférés-vezérlő listát is hozzárendelni. Ezekkel meghatározható, hogy mely rendszerekből engedélyezett a telnet-hozzáférés. A legtöbb IOS csupán öt telnet-portot támogat. A beállítások között a „line vtty 0 4" jelzi ezt az öt portot, mivel a nulla is egy csatorna (0, 1, 2, 3, 4). A következő parancsokkal a vty-vonalak egy csoportjára (0..3) állítjuk be ugyanazokat a működési paramétereket.

```
!
line vty 0 3
 access-class 100 in
 exec-timeout 15 0
 transport input telnet ssh
!
```

Ezen hozzáférési lista definiálása rendkívül fontos, és valós helyzetben már sokkal korábban szerepelt volna a beállítások között, a könnyebb megértés kedvéért azonban ezúttal itt mutatjuk be. A 100 jelű lista mindenkinek megtiltja a hozzáférést az útválasztóhoz, majd külön engedélyezi a hálózatkezelő szerver (7.7.7.5), illetve a tűzfal (6.6.6.1) irányából érkező kapcsolódási kísérleteket, de csak ha az a telnet- (23) vagy az ssh- (22) porton történik. A sikeres kapcsolódást naplózzuk, így megfigyelhető, hogy ki mikor és hogyan csatlakozott. Természetesen

```
ugyanebből a célból a visszautasított kísérleteket is naplózzuk. A
kiterjesztett ACL segítségével további adatok is naplózhatók, ha erre
szükség lenne.
!
access-list 100 remark Telnet hozzáférés az útválasztóhoz
access-list 100 permit tcp host 7.7.7.5 host 0.0.0.0 range 22 23 log-input
access-list 100 permit tcp host 6.6.6.1 host 0.0.0.0 range 22 23 log-input
access-list 100 deny ip any any log-input
!
Valahányszor lehetséges, engedélyezzük az ssh-forgalmat, mivel az sokkal
biztonságosabb a telnetnél. Természetesen olyan IOS-szoftverre van
szükség, amely támogatja az SSH hozzáférést, s nem szabad elfelejtkezni az
RSA-parancs segítségével történő kulcskészítésről sem.
!
Egy vty-csatornát vészhelyzet esetére hagyjunk meg biztonságosnak. A
7.7.7.8 gép a belső hálózatban található biztonságos gép. Ha minden más
telnet csatorna foglalt lenne, egy csatorna így is mindenképpen szabad
maradhat, így onnan csatlakozva megvizsgálható, hogy mi is történik.
!
line vty 4
 access-class 105 in
 exec-timeout 15 0
 transport input telnet ssh
 ! megjegyzés: az AAA is használható lenne bejelentkezéskor
access-list 105 remark VTY hozzáférési lista
access-list 105 permit tcp host 7.7.7.8 host 0.0.0.0 range 22 23 log-input
access-list 105 deny ip any any log-input
!
```


6.4. Összefoglalás

Ebben a fejezetben azon módszerekről és helyekről beszéltünk, amikor az útválasztót az eredetileg szándékozott felhasználásánál hasznosabban akarjuk alkalmazni. A fejezet ennek érdekében megvizsgálta, hogy egy útválasztót miként lehet a hálózatunkhoz való hozzáférés kötelező ellenőrző pontjaként felhasználni. Következő szintként megnéztük, hogy a behatolás-ellenőrző csomaggal kiegészített Cisco IOS-tűzfalkészlet miként működhet fejlett csomagvizsgálóként is. Ezeknek a fejlett technológiáknak egyike sem szolgálhat azonban a kifejezetten erre a célra létrehozott eszközök helyett, azonban a védelem egy újabb rétegének megvalósításával a hálózat biztonságát még hatékonyabban valósítja meg.

A továbbiakban a fejezet magának az útválasztónak a biztonságossá tételével kapcsolatos alapvető módszereket mutatta be. Ezt az információt egy tényleges beállító (konfigurációs) állomány formájában szemléltettük, amelyet a saját beállítások itt közöltekkel való összevetése során hivatkozásként felhasználhatunk. A következő fejezetben a tárgyalást a hálózatbiztonság megnövelésére kialakított virtuális magánhálózattal folytatjuk.

A biztonsággal kapcsolatos további információkat találhatunk még: „Increasing security on IP Networks" – egy régi, ám alapvető dokumentum, amely az IP-alapú hálózatokkal és biztonságukkal kapcsolatos számos információt tartalmaz: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

„The Cisco Internet Security Advisories" – A Cisco honlapján található élő hivatkozási lista, amely a cég biztonsági tanácsait sorolja fel, beleértve különböző útmutatókat is. Részletesen tárgyalja, hogy az internet legfrissebb sérülékenységei közül a legrosszabbak ellen miként védhetjük meg hálózatunkat (Cisco-témaszámra szükség van az eléréshez): http://www.cisco.com/warp/customer/707/advisory.html

6.5. Összefoglaló kérdések

1. Mivel minden, az internethez csatlakozó vállalatnak van útválasztója, így kell-e védelmi lehetőségeket telepíteni ezekre?
2. Mi a haszna annak, ha a hálózat peremén található útválasztót ellenőrző pontként használjuk, és mennyire hatékonyak ezek a hálózat biztonságának növelésében?
3. Melyik technológia képezi a Cisco IOS-tűzfalkészlet lelkét?
4. Miként hajtja végre a tűzfalkészlet a dinamikus csomagszűrést az ACL segítségével?
5. Képes-e a Cisco IOS behatolásérzékelő csomagja a több helyen történő csomagvizsgálatra?
6. Az ideiglenes hozzáférési listákhoz egy időzítő is van rendelve. Határozza meg ezek működését a különböző protokollok (ICMP, UDP, TCP) alapján!
7. Mi a különbség az elemi és az összetett minta között?
8. Mi történik, ha egy támadó egyszerre használja a visszhang és a karaktergenerátor eljárásokat? Miként lehet ezt kivédeni a Cisco-útválasztó esetén?

7. fejezet Virtuális magánhálózatok

A változás életadás.
Segít minket abban,
hogy többé váljunk,
mint korábban voltunk.
(Successories)

A fejezet elolvasása után érteni kell, és el kell tudni magyarázni az alábbi témákat:

- ***A különböző virtuális magánhálózatok (VPN – Virtual Private Network) közötti eltérések;***
- ***A VPN-technológia céljai és előnyei, valamint alkalmazásának módja,***
- ***Hol használunk titkosítást, és az milyen szerepet játszik a VPN-ben,***
- ***Az IPSec-alapú VPN működésében érintett protokollok.***