

Könnyű álmok (4. rész)

A hálózati határvédelem alapjai

E cikk keretein belül két témát érintünk: a hálózati védelem kialakításának alapidokumentumát, a határvédelmi tervet (általában a security policy kifejezés használatos), valamint kissé közelebbről megismerkedünk a csomagszűrők tulajdonságaival.

Sokan rutinból állnak neki egy biztonsági rendszer kivitelezésének. Ha azonban nemcsak a lélek megnyugtatása a cél, hanem a valós védelem, akkor a védelmi rendszert beállítás előtt meg kell tervezni. Miután felmértük mit akarunk megvédeni és mitől, ezeket az ismereteket valamilyen félreérthetetlen szabálykönyvbé rögzíteni kell. Ennek egy lehetséges formáját mutatjuk meg.

A Linux rendszer mag számtalan hasznos és biztonságot növelő lehetőséget ad, például a Linux csomagszűrője sok tekintetben felülmúlja a pénzes rendszereket. Segítségével szabályozhatjuk az átáramló forgalmat annak feladója és célja szerint, kialakíthatunk olyan belső hálózatot, melynek teljes forgalma az útválasztó másik oldalán egyetlen számítógépnek látszik (masquerade), így a teljes hálózatnak csak egyetlen közismert hálózati címre van szüksége. Mivel az útválasztó Linux-alapú, szükség esetén futtathatunk rajta levélszolgáltatót, webgyorsítót vagy akár hálózati forgalom-elemzőt.

A jobb érthetőség kedvéért állítsunk fel egy olyan példát, melyen keresztül elmagyarázható, hogy a rendszer mire képes, és mire nem.

Egy képszerű példa

Képzeljünk el egy bolygót városokkal, azokban házakkal, bennük lakásokkal. Minden háznak egyedi címe van. A házak lakói gyakran küldenek egymásnak csomagokat postán, akár másik városba. Minden városban van legalább egy postahivatal, ahol a más városokból érkező, vagy azok felé induló csomagok útját meghatározzák, sőt nagyobb városokban akár több ilyen hivatal is lehet. Az egyes csomagokat postahivatalok döntenek el, hogy merre kell továbbszállítani. Mi történik akkor, ha más városokban rosszindulatú emberek unalmukban bombákat küldözgetnek csomagjaikban? Együtt élhetünk a dologgal vagy megpróbálhatjuk megakadályozni. Ennek kézenfekvő módja a postahivatalokban a csomagok továbbításának valamilyen szabályozása, a veszélyes csomagok kiválogatása és megsemmisítése. Mivel a csomagok a városokba csak postahivatalokon keresztül juthatnak be, itt könnyen megmondhatjuk, hogy mely városokból nem fogadunk el csomagokat, mert tudjuk, hogy az adott város lakói általában rosszindulatúak, vagy bizonyos lakók csomagjait tiltjuk ki, mondván, ők megbízhatatlanok. A csomagokat fel is bonthatjuk, és csak akkor tiltjuk meg a továbbításukat, ha azok valóban bombát tartalmaznak, ehhez természetesen több postásra lesz szükségünk. Most fordítsuk le a fenti példát hálózatokra. A példabeli bolygó megfelel a Föld óriáshálózatának, az Internetnek, a városok az Internet egyes alhálózatait. A házak a hálózaton lévő számítógépek, a lakások a kapuknak, a lakók pedig a kapukon figyelő démonoknak felelnek meg. Ebben az esetben egy kapuban egyszerre csak egy lakó lehet. Minden hálózat bejáratánál van egy útválasztásra alkalmas hálózati elem, ez a példánkban említett postahivatal. Ha a saját hálózatomat (a város) fenyegetve érzem (korábbi cikkeinkben igyekeztünk bemutatni, hogy együgyűség lenne nem félni), akkor annak hálózati kapcsolódási pontjainál (a postahivatalok) érdemes valamilyen védelmet alkalmazni (csomagok kiválogatása). Ehhez előre



meg kell határozni, hogy mely hálózatrészek között milyen forgalom haladhat át. Ezt a tervet a gyakorlatban hálózati határvédelmi tervnek, vagy az adott hálózat határvédelmi politikájának hívják (security policy). Lásd a mellékletben (58. oldal). Ha okos jelelosztónk van, ami a forgalmat a csomagok forrása és célja szerint szűri, akkor a rendszert csomagszűrő rendszernek (Packet Filter) hívják. Ha a csomagszűrő képes a csomagok által kifeszített kapcsolatot egységként kezelni (akár UDP-n is!), akkor az már állapotartó csomagszűrő (Stateful Packet Filter – SPF). Ez példánkban a több csomagból álló kapcsolat. Az SPF rendszerek ezenkívül gyakran képesek a csomagok tartalmát is megvizsgálni, és valamilyen szinten a protokollok vizsgálatát is elvégzik. A teljes protokollelemző rendszereket alkalmazásszintű tűzfalnak (Application Level Firewall – ALF) hívják. Ez példánkban azt jelentené, hogy a postahivatal kibont minden egyes csomagot, és azok tartalma alapján dönti el, hogy továbbítható-e. Az alkalmazásszintű tűzfalak általában minden átvitt protokollra egy-egy különálló szűrő-programot tartalmaznak, ezek az úgynevezett alkalmazásátjárók (application gateway vagy egyszerűen csak gateway). Egy jól tervezett alkalmazásátjárón a protokoll minden eleme finoman szabályozható. Ezekről a rendszerekről a későbbiekben bővebben is lesz szó.

Határvédelmi politika (HP)

A HP tartalmazza, hogy ki, mivel, hogyan, mikor és mihez férhet hozzá. Minél pontosabban le tudjuk írni a rendszer szabályos működését, annál biztosabb, hogy az ettől eltérő eseteket ki tudjuk zárni. Leírható benne például, hogy a cég pénzügyi rendszerét kizárólag Bogár Elek használhatja, csak a saját munkaállomásáról és a cég által adott azonosító alrendszerrel használva. Délután öt órától reggel nyolcig nem léphet be, ilyenkor ugyanis szórakozik vagy alszik. A HP-t kétféle hozzáállással lehet megalkotni, az egyik a „mindent szabad, ami nem tilos”, a másik az ellenkezője, „minden tilos, amit nem engedélyezek”. Biztonsági rendszerek tervezésénél általánosan elfogadott hozzáállás, hogy az utóbbi szerint kell eljárni. Így nem fordulhat elő az, hogy valami elkerüli a biztonsági politika kialakítóinak figyelmét, és lehetőséget hagy a visszaélésre. Mivel minden tilos, amit nem engedélyezünk, csak a valóban engedélyezett forgalom juthat át. A továbbiakban figyelmeztetés nélkül ezt tekintjük alapértelmezettnek. Az otthoni felhasználók esetén célszerű tudatosan védekezni, a cégek hálózati védelménél viszont szinte kötelező HP-t készíteni, mivel a védelemnek mindenképpen jól meghatározottan kell lennie. A védelem alanyai gyakran nem örülnek túlzottan a védettségeknek, mivel ez gyakran eddigi jogaik csorbulásával és szokatlan kényelmetlenségekkel járhat. A rendszer védelmi szintje és kényelme között nagyjából fordított arányosság áll fenn. Ilyenkor a vezetőség által elfogadott, aláírt HP nagyon sokat segíthet. Egy cég védelmi elveit mindig a cég vezetőinek bevonásával kell kialakítani, hiszen ők azok, akik a HP-t be nem tartó alkalmazottakkal szemben felléphetnek.

Fontos szerepe van a HP-nak a védelmi eszközök megválasztásában

1. lista /etc/ipchains.conf

```
# /etc/ipchains.conf - csomagszűrő beállító állomány az ipchains rendszerhez
#
# Azbesztkabát 1.0.0 - készítette a Könnyű álom szabadcsapat
# az Úr 2001. évének február havában
#

:input DENY
:forward DENY
:output ACCEPT
:modem_be

-A input -i lo -j ACCEPT
-A input -p tcp -i ppp0 ! -y -d __modemip__ -j modem_be
-A input -p udp -i ppp0 -d __modemip__ -j modem_be
-A input -p icmp -i ppp0 -d __modemip__ -j modem_be
-A input -p tcp --dport auth -j REJECT

# minden, ami eddig nem került engedélyezésre, azt elutasítjuk és naplózuk
-A input -j DENY -l

# innen a modem bejövő csomagjait vizsgáljuk
-A modem_be -p icmp --source-port destination-unreachable -j ACCEPT
-A modem_be -p udp -s x.y.z.s3 domain --destination-port 1024: -j ACCEPT
-A modem_be -p udp -s x.y.z.s3 ntp --destination-port ntp -j ACCEPT
-A modem_be -p tcp -s x.y.z.s1 smtp --destination-port 1024: -j ACCEPT
-A modem_be -p tcp -s x.y.z.s1 pop3 --destination-port 1024: -j ACCEPT
-A modem_be -p tcp -s x.y.z.s2 3128 --destination-port 1024: -j ACCEPT
-A modem_be -p tcp --source-port www --destination-port 1024: -j ACCEPT
-A modem_be -p tcp --source-port https --destination-port 1024: -j ACCEPT
-A modem_be -p tcp --source-port ssh --destination-port 1024: -j ACCEPT
-A modem_be -j DENY -l
```

is. Ha a HP csak a hozzáférés irányát határozza meg, akkor elegendő lehet egy csomagszűrő alkalmazása, ha azonban megköveteli a kapcsolat protokollszintű szűrését, módosítását vagy az erős azonosítást a tűzfalon való áthaladáshoz, akkor nem kerülhető el az alkalmazás-szintű tűzfalak használata.

A határvédelmi politika tartalma

Vizsgáljuk meg, mit kell egy HP-nak tartalmaznia. Mindenekelőtt meg kell határozni a rendszer számára értelmezett hálózatokat. A határvédelem szempontjából kiemelt rendszereket is egyedi – egy-címes – hálózatokként érdemes kezelni. A hálózatok leírását láthatjuk a példa HP első részében. Ahol nincs megadva hálózati maszk, ott az 32 bites. Ez azt jelenti, hogy nem egy valódi hálózatról van szó, hanem egy hálózati címről, például a szolgáltató levélkiszolgálójáról. A későbbiekben így tudjuk majd megadni azt a szabályt, hogy oda és csakis oda fogjuk engedélyezni a levelek továbbítását. Ezek után a hálózatok logikai neveit használva a lehető legpontosabban le kell írni, hogy milyen forgalom engedélyezett az egyes alhálózatok között. Ezt a példánkban bemutatott megoldásnál szabályokban adjuk meg. Egy szabály mindenképpen tartalmazza a forrás és célhálózat logikai nevét, az átvitt protokoll meghatározását és a célkaput (néhány esetben az utóbbi kettő megadása nehéz, vagy nem lehetséges). Ha lehetséges, a forráskaput is meg kell határozni. Általában itt csak tartományt tudunk megadni, de ez is segít a szabályos működés pontosabb leírásában. A biztonsági rendszerek arany-szabálya szerint az utolsó szabály mindig a „minden más tilos”

(catch all). Az egyes protokollok átvitelének általában külön lefektetett szabály-rendszere van, ezt egy külön dokumentumban rögzítik. Innen derül ki, hogy a HP-t milyen védelmi eszköz tudja megvalósítani. Ha például az elvárás az, hogy a nyilvános webkiszolgáló típusát ne lehessen meghatározni, akkor látszik, hogy egy tiszta csomagszűrő rendszerrel ezt nem lehet megvalósítani. Ha az általánosan kívül még valamilyen megszorítást tudunk tenni az adott kapcsolatra, akkor azt megjegyzésként érdemes az adott szabályba illeszteni. Ilyen lehet például az, hogy a cég általános levélto-vábbítási szabályozása nem ír elő semmilyen különleges eljárást a csatolt állományokkal kapcsolatban, de a pénzügyi rendszerbe menő levelekből el kell távolítani a futtatható állományokat. Például határvédelmi tervünk egy későbbi személyi tűzfal kialakításához lett kitalálva, azokat a kapcsolatokat engedélyezi, melyek egy jellemző otthoni Internet-felhasználónál szükségesek.

Csomagszűrő rendszerek

A HP-k elvárásainak az egyszerű csomagszűrő rendszer gyakran nem felel meg, mivel a legkisebb protokollon belüli beavatkozáshoz is alkalmazás-szintű szűrésre van szükség. Ebből arra következtethetnénk, hogy a csomagszűrő felesleges, de ez nem igaz. Az alkalmazás-szűrő tűzfalak első védelmi vonala csomagszűrő, így mindenképpen meg kell ismerni helyes beállításának alapjait. Alkalmazás-szűrő tűzfal esetén a csomagszűrő alrendszer hárítja el a támadások jelentős részét, mivel csak az olyan kapcsolatok létrejöttét engedélyezi, amelyek a HP által engedélyezettek. Így az átjárókhoz csak az engedélyezett kapcsolatok juthatnak el, ezzel nehezítve a rendszer megbénítását (DoS).

Az egyszerű csomagszűrő rendszerek alapvető tulajdonságai:

- nagyon gyors, mivel alkalmazás-szinten nem elemez
- átlátszó (transparent) – a felhasználóknak nem kell tudniuk róla
- olcsó, hiszen szinte minden útválasztásra alkalmas eszköz tartalmazza – így az ingyenes operációs rendszerek is. Érdekes tény, hogy néhány pénzért kapható operációs rendszer nem tartalmaz csomagszűrési lehetőséget.
- nagyon nagy terhelésnél olcsóbb megoldás a vas cseréje, mint több rendszer használata – nehezen méretezhető
- nagy rendszereknél a beállítás nehezen áttekinthető
- a már beállított csomagszűrő esetleges hibáit nehéz meghatározni
- bizonyos protokollok szűrése nehézkes (például FTP, NFS).

2. lista /etc/ppp/ip-up.d/ipchains

```
#!/bin/sh
# /etc/ppp/ip-up.d/ipchains - csomagszűrő
# élesítő script
#
# Azbesztkabát 1.0.0 - készítette a Könnyű álom
# szabadcsapat
#          az Úr 2001. évének február havában
#

modemdev=ppp0
ipchainsconf=/etc/ipchains.conf

modemip='ifconfig $modemdev | perl -ane 'print \
        ((split(/:/, $F[1]))[1]) if /ine/'
# Debiannál
modemip=$PPP_LOCAL

tmpdir=.tmp.'date +%Y.%m.%d'
mkdir -m 700 /tmp/$tmpdir
if [ $? != 0 ]; then
    echo "Hiba: Az átmeneti könyvtárat nem \
        sikerült létrehozni."
    echo "          A csomagszűrő beállítása \
        sikertelen."
    exit 1
fi
sed s/___modemip___/$modemip/ $ipchains.conf > \
    /tmp/$tmpdir/ipchains.conf
ipchains -F
ipchains -I input 1 -j DENY
ipchains -X
egrep -v '^s*(#.*)?$' /tmp/$tmpdir/ \
    ipchains.conf | ipchains-restore
ipchains -D input 1
rm -rf /tmp/$tmpdir
```

3. lista /etc/ppp/ip-down.d/ipchains

```
#!/bin/sh
# /etc/ppp/ip-down.d/ipchains - csomagszűrő
# leállító script
#
# Azbesztkabát 1.0.0 - készítette a Könnyű
# álom szabadcsapat
#          az Úr 2001. évének február havában
#

ipchains -F
ipchains -X
ipchains -P input ACCEPT
ipchains -P forward DENY
ipchains -P output ACCEPT
```

- A méretezhetőség tűzfalakkal is azt jelenti, hogy a rendszer kis és nagy terhelés esetén is hatékonyan használható. Amennyiben a nagy áthaladó forgalom miatt a szűrést nem lehet egy géppel megvalósítani, akkor a szolgáltatások külön gépekre bontásával oldható meg. Ettől erősebb terhelés esetén, az egyes szolgáltatásokon belül is osztható a forgalom, például forráscím szerint. Így szélsőséges forgalom mennyiség is szűrhető. Ennek a megoldásnak alkalmazásszűrő rendszereknél van igazán értelme, hiszen azon rendszerek lényegesen erőforrás-igényesebbek. A tiszta csomagszűrőknél ennek csak akkor van értelme, ha a csomagszűrő szabályrendszere nagyon sok szabályból áll, és azokat nem lehet egyszerűsíteni. A csomagszűrő rendszereknél mindig arra kell törekedni, hogy egy csomag a lehető legkevesebb vizsgálaton essen át, így kevesebb időt kell a rendszernek egy csomag feldolgozásával töltenie. Ennek egyszerű módja a csomagok bejövő láb szerinti válogatása, ahogy azt a későbbi példában látjuk.
- Bizonyos protokollok szűrése azért nehézkes, mert a protokoll tevézői úgy álmodták meg rendszerüket, hogy sem a forrás, sem a célkapu nem előre meghatározott. Így ha például az A hálózathoz a B hálózatba át akarjuk engedni az NFS protokollt a hozzá tartozó csingilingikkal, akkor nem tehetünk mást, át kell engednünk szinte a teljes hálózati forgalmat. Erre a gondra csak egy alkalmazásszűrő nyújthat megnyugtató megoldást, az is csak abban az esetben, ha ő maga kezelheti folyamatosan a csomagszűrőt. Ha tehát az átmenő kapcsolat azt követeli, hogy a 2317-es kaput nyissuk ki, akkor a rendszer a csomagszűrőben engedélyezi a csomagok bejövetelét erre a kapura, de kizárólag az adott ügyfélről.

A fenti kijelentésekhez érdemes néhány megjegyzést fűzni.

- Az átlátszóság pontosabban azt jelenti, hogy sem az ügyfeleknek, sem a kiszolgálóknak nem kell tudniuk, hogy tűzfal választja el őket. Ha a tűzfal nem átlátszó, akkor az ügyfélnek erre fel kell készülnie, mivel nem a célkiszolgáló címére kell kapcsolódnia, hanem a tűzfal egy meghatározott kapujára, és a tűzfal itt kérdezi meg tőle, hogy ma hová szeretne menni. Ez természetesen az ügyfél módosítását, illetve további beállítást követel. Az ügyfél módosítása azt jelenti, hogy az eredeti protokollt kiegészítik olyan elemekkel, aminek segítségével a rendszer a tűzfalal közölni tudja eredeti úti célját, szükség esetén az áthaladó azonosítását is itt teszi lehetővé.
- A hálózatok építői gyakran feledkeznek meg róla, hogy majd minden útválasztó tartalmaz csomagszűrési lehetőséget. Ezt általában nem állítják be, vagy nem elég körültekintően, így a rendszer beállítása mindenhol nem módosítható. Pedig egy ilyen rendszernél célszerű meghatározni, hogy honnan fogad el módosítási kéréseket. Ez a legkevesebb, amit minden útválasztóban be kellene állítani, de ha már az útválasztónál meg tudjuk akadályozni a tiltott forgalmak áthaladását, akkor ésszerű megtenni, hisz így a tiltott forgalom nem terheli feleslegesen a mögöttes hálózatot.

Hogyan varrjunk Azbesztkabát?

Az informatikában egyre általánosabbá válik az üldözési mánia. Sokszor nem tiszta, hogy mitől félünk, mennyire félünk, egy azonban biztos: félünk. A számítógépet otthon használók is tudnak már a veszélyekről, és a világháló számos olyan fórumot kínál, amely tájékoztat a rendszerre leselkedő veszélyekről, és megoldásokat kínál. Ezen megoldások összefoglaló neve (personal firewall) azbesztkabát, és számtalan változata létezik. Lényege, hogy rendszerünk kap egy olyan tűzfalat, amely nem egy mögöttes hálózatot véd, hanem saját gépünket. Megvédi viselőjét – innen az elnevezés. A tapasztalatlanabb Linux-felhasználók bizonyos szempontból rosszabb helyzetben vannak, mint más operációs rendszereket használó társaik. A nagyobb tapasztalattal rendelkezők hajlamosak a kérdést a következő kijelentéssel elintézni: Nincs szükség azbesztkabát fejlesztésére, itt van a csomagszűrő. Ez a kijelentés igaz ugyan, de két dolgot nem vesz figyelembe. Egyrészt a csomagszűrő helyes beállítása némi tapasztal-

talatot kíván, másrészt csak a kívülről induló támadások ellen nyújt védelmet. Nem segít akkor, ha a rendszert szabályos forgalomnak álcázva támadják meg. Például ha egy webkiszolgáló azután, hogy arra valaki a rendszerről csatlakozott, visszatámad. Ez a HP szempontjából szabályos, engedélyezett kapcsolatnak minősül, így nem szűrhető ki pusztán csomagszűrő segítségével. Hajlamosak lennénk azt gondolni, hogy egy ilyen támadást szinte lehetetlen kivitelezni, de sajnos nem ez a helyzet. Sok olyan támadást tartanak számon, amit trójai kiszolgálók követtek el a mit sem sejtő ügyfelek ellen. Az azbesztkabát határvédelmi politikája (AHP) egy hétköznapi ember felhasználási szokásaihoz lett idomítva. Ettől szükség esetén természetesen el lehet térni, ehhez azonban célszerű elolvasni legalább az IPCHAINS-HOWTO-t [1.] [2.], és segítséget kérni tapasztaltabbaktól. Bátorabbak kezdek rögtön az engedélyezni kívánt protokoll RFC-jének elolvasásával és a **tcpdump** vagy az **ethereal** programok lehetőségeinek tanulmányozásával. Segítségükkel figyelni lehet a hálózati forgalmat, és meg lehet állapítani, hogy az adott protokoll hogyan engedhető át a lehető legkisebb lyuk megnyitásával.

Az engedélyezett forgalom

Most nézzük meg röviden, mi miért van a példa határvédelmi tervben. Mit szeretne egy átlagos otthoni felhasználó csinálni a nagy Interneten? Lássuk:

- webböngészés; ha webezne, akkor használni akarja az Interneten lévő rendszereket és szolgáltatójának webgyorstárát (webcache).
- ftp-állományok átvitele; ha ftp-zne, ezt megteheti szolgáltatójának webgyorstárán keresztül – így azonban csak letölteni tud (ekkor ehhez nem kell újabb beállítás), vagy közvetlenül, ekkor azonban némi terhet vesz a vállára (ezt a problémát jelenleg nem vesszük figyelembe, de az ip-filter későbbi tárgyalásakor megoldjuk).
- levelezés; ha levelezne, akkor a leveleit el akarja tölteni levelezési kiszolgálójáról (POP server), küldeni pedig postakiszolgálóján (SMTP server) keresztül fog.
- egyéb szükséges szolgáltatások; minden szolgáltatás igénybevételehez szüksége lesz az Internet névfeloldásának használatára (DNS-kiszolgálók), és ha rendszerének óráját az Internet atom-óráihoz akarja hangolni, akkor szüksége lesz az időszolgáltatók (ntp servers) elérésére is.

Azbesztkabátunk mindezt a lehetőséget megadja. Mitől szeretné megvédeni magát egy átlagos Internet-felhasználó? Nem szeretné, ha illetéktelenek lépnének be a gépére, vagy használnák valamire, amit ő nem szeretett volna. A rendszerek telepítőjének jelentős része azonban olyan szolgáltatóprogramokat is telepít, melyre valójában nincs szüksége, és aminek a hibájából azonban gyakran lehetségessé válik a rendszerre való behatolás. Mivel az AHP-ben megengedett forgalmak között nincs a rendszerbe befelé irányuló forgalom, így annak helyes megvalósítása esetén hiába van hibás kiszolgáló a gépre telepítve, a csibészek nem tudnak azon keresztül behatolni. Jelen cikk tartalmaz egy csomagszűrő beállítást, ami kielégíti a példa HP követelményeit (1. lista). A cikk megírása idején a 2.4-es rendszermagso-rozat még nem mondható megbízhatónak, így a beállítások a 2.2-es sorozat csomagszűrő rendszeréhez megfelelőek. A beállításban szereplő *x.y.z* kezdetű példa címeket természetesen le kell cserélni a szolgáltató valós levelező, posta és webgyorstár kiszolgálójának hálózati címére. A `__modemip__` betűsorozatot a beállítóállomány betöltő parancsfájl fogja kicserélni a modem pillanatnyilag érvényes hálózati címére, mivel ez általában behívásonként változik. A 2. és 3. lista két egyszerű parancsfájlt tartalmaz, melyek feladata, hogy a csomagszűrőt élesítsék, illetve kikapcsolják. Ha a két parancsfájlt a megadott könyvtárba helyezzük el, és nem feledkezünk meg a futtathatóvá tételükről, akkor a védelem tárcsázás után önműködően éle-

sedik, a kapcsolat lezárultakor pedig leáll. Ez igaz a Debian Potato rendszerre, más Linux-változatokban azonban más lehet a helyzet. Ennek kiderítését az olvasóra bízuk.

A csomagszűrő beállításaiiban néhány dolgot érdemes megmagyarázni. Ha valami az alábbi bekezdésben nem világos, akkor javasolt elolvasni az ipchains leírását [2.]. Ennek ismertetése ezen cikk kereteit meghaladja, ezenkívül található hozzá jól érthető magyar leírás is. Az egyes lábakra (csatoló) érkező forgalmat célszerű különválasztani, ezért használjuk a `modem_be` láncot (`chain`). Ennek a módszernek akkor fogjuk igazán hasznát látni, ha egy 12 lábú tűzfalát kell beállítanunk, és a csomagszűrő valahol hibázik. Itt a hibát egyszerűen megtalálni már csak akkor lehet, ha a csomagokat döntés előtt gondosan osztályoztuk.

Ha egy postakiszolgáló felé kapcsolatot kezdeményezünk, akkor az esetenként az `auth` (113-as) kapun át visszanyit a gépünk felé, a levél feladójának kiderítésére. Mivel a levelezőrendszerek e szolgáltatás nélkül is működnek, ezt mi tiltjuk. Van azonban egy kis bökkenő. Mivel mi minden bejövő SYN-es csomagot válasz nélkül a földre dobunk (a DENY célra), így a postakiszolgáló azt hiheti, hogy a válasz érkezik, csak még nem ért oda. Ebben a helyzetben ezért használunk REJECT célt, így a másik rendszer azonnal visszakap egy ICMP csomagot, amely tájékoztatja, hogy az adott kapu nem érhető el. Így a levél továbbítását azonnal megkezdhetjük. Ha ezt nem használjuk, akkor a kiszolgáló rendszer 90 másodpercig várni fogja a választ, mielőtt a levéltovábbítást megkezdhetnénk.

A `modem_be` láncon belül, ha a csomag valamelyik kitételnek megfelel, akkor továbbítását elfogadjuk, ha nem, akkor végül beleesik a „minden más tilos” szabályba. Amint láttuk, a csomagok érvényességét az input láncból kiindulva vizsgáltuk meg. Amennyiben a rendszeren *kizárólag* átmenő csomagok vannak, akkor szokás még a forward láncban megadni a szabályokat, de ez igen ritka. Ki lehet alakítani teljesen egyéni megoldást is, de a tapasztalatokat nem figyelembe venni a biztonságmodszertanban nem túl hálás hozzáállás.

A csomagszűrő magasabb szintű beállítására még visszatérünk, mikor a hivatalos megbízható rendszermag nem csak nevében lesz megbízható. Akkor már az ip-filter lehetőségeivel ismerkedünk meg, ami a rendszermag új nemzedékének csomagszűrője. A következő alkalommal Bozó megteszi azt, amit már oly régen szeretne, jól beolvas a VLAN-nak. Szóval a hálózatok alacsony szintű támadásairól ejtünk pár keresetlen szót.

Kapcsolódó címek

- [1.] <http://www.math.bme.hu/LDP/HOWTO/IPCHAINS-HOWTO.html>
 [2.] <http://linux.hu.rulez.org/ipchains>



Mátó Péter (atya@andrews.hu), informatikus mérnök és tanár. Biztonsági rendszerek ellenőrzésével és telepítésével, valamint oktatással foglalkozik. 1995-ben találkozott először linuxos rendszerrel. Ha teheti, kirándul vagy olvas.



Borbély Zoltán (bozo@andrews.hu), okleveles mérnök-informatikus. Főként Linuxon futó számítógépes biztonsági rendszerek tervezésével és fejlesztésével foglalkozik. A 1.0.9-es rendszermag ideje óta linuxozik. Szabadidejét barátaival tölti.

Hálózati határvédelmi terv

A rendszer fizikai csatolói

a csatoló logikai neve	a csatoló fizikai neve	a csatoló hálózati címe	egyéb megjegyzés
if_local	lo	127.0.0.0/8	
if_internet	ppp0	interIP/interMASK	gw interGW

A rendszerben ismert hálózatok

logikai megnevezés	hálózati cím	a csatoló neve
helyi_h	127.0.0.0/8	lo
modem	x.z.y.b1	ppp0
internet	0.0.0.0/0	ppp0
out_mail	x.y.z.s1	ppp0
out_cache	x.y.z.s2	ppp0
out_domain	x.y.z.s3	ppp0

A rendszerben engedélyezett hálózati forgalom

szabály	forrás	cél	protokoll	forráskapu	célkapu	művelet
1.	helyi_h	helyi_h	*	*	*	ACCEPT
2.	modem	out_domain	UDP	> 1023	53/domain	ACCEPT
3.	modem	internet	UDP	123/ntp	123/ntp	ACCEPT
4.	modem	out_mail	TCP	> 1023	25/smtp	ACCEPT
5.	modem	out_mail	TCP	> 1023	110/pop3	ACCEPT
6.	modem	internet	TCP	> 1023	80/www	ACCEPT
7.	modem	internet	TCP	> 1023	443/https	ACCEPT
8.	modem	out_cache	TCP	> 1023	3128	ACCEPT
9.	modem	internet	TCP	> 1023	22/ssh	ACCEPT
10.	modem	internet	ICMP	3/dest-unreach	*	ACCEPT
11.	*	*	*	*	*	DENY