Spamszűrés a gyakorlatban Postfix és Postgrey

Előző cikkemben (Linuxvilág 2005. október) bemutattam a leggyakrabban használt spamszűrési elveket. Ebben az írásban egy konkrét példát mutatok be arra, miként valósítható meg egy szürkelista együttműködése a Postfix levélkiszolgálóval.

Többféle megoldás létezik erre a funkcióra (➲ *http://www.postfix.org/addon.html*). Azért esett a választásom a postgrey nevű programra, mert egyszerűen és könnyen telepíthető, nincs szükség külső alkalmazásra, például adatbázisra, stb.

Az úgynevezett ***szürkelista*** szerveroldali – ***MTA*** szinten megvalósított – spamszűrő módszer, amely úgy működik, hogy az ***SMTP*** szerver a kapott levelet először átmeneti hibával elutasítja, majd amikor egy bizonyos idő múlva a küldő oldal újból próbálkozik ugyanazzal a levéllel, akkor már elfogadja azt szerverünk. A spammerek azonban nem sokat foglalkoznak ideiglenes hibakódokkal, ha egy levél nem megy el az első alkalommal, akkor veszik a következő „áldozat" email címét. A módszer előnye, hogy nincs téves pozitív azonosítás, a rendszer önműködő, nem igényel folyamatos karbantartást.

A ***postgrey*** nevű alkalmazás valójában egy ***Perl*** nyelven készített úgynevezett ***policy démon***, amely ***Berkeley DB*** adatbázisban tárolja a feladó/címzett/kliens adatokat. Képes mind ***unix domain socket***-en, mind pedig ***TCP*** porton át kommunikálni. Ha ugyanazon a gépen futtatjuk, mint a ***Postfixet***, akkor az előbbit javaslom.

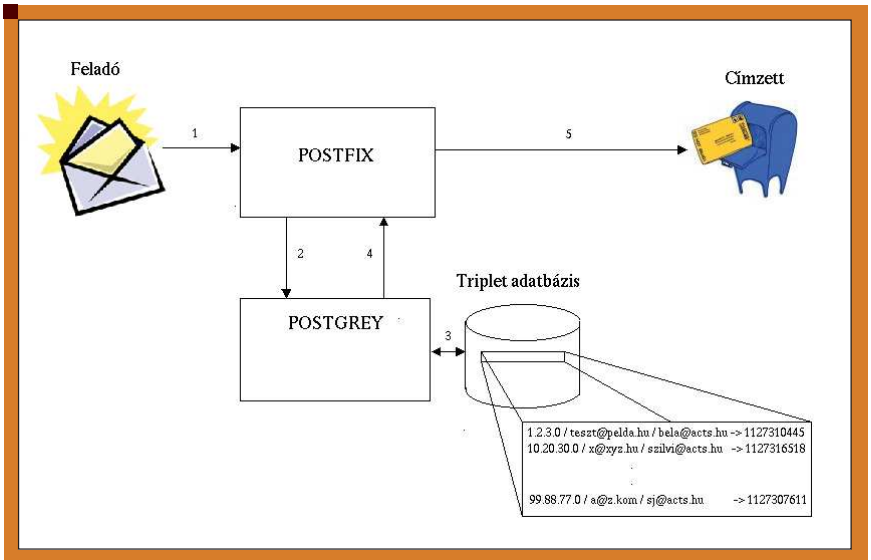
A postgrey működése

Az *1. ábrán* követhetjük nyomon, hogyan működik együtt a ***Postfix*** és a ***postgrey***. A levelet először megkapja a ***Postfix*** (1), majd konzultál a policy démonnal (2). Ez megvizsgálja, hogy a feladó ***IP***-címe (alapértelmezésben a C-osztályú hálózati maszkot nézi), a feladó-, ill. a címzett email címe szerepel-e az adatbázisban (3). Ha nem, vagy a hozzárendelt időbélyeg 5 percnél (konfigurálható érték) frissebb, akkor ***„ideiglenesen elutasítva"*** (`DEFER_IF_PERMIT`), ellenkező esetben ***„tőlem mehet"*** (`DUNNO`) választ ad a ***Postfix*** kérdésére (4). Ez alapján dönti el a ***Postfix***, hogy átmeneti hibával elutasítja az ***SMTP*** kapcsolatot (valójában a kliens `RCPT TO` parancsára ad vissza hibakódot), ellenkező esetben továbbítja a levelet a címzett postafiókjába (5).

Postgrey telepítése

0Ha gépünkön nincsenek meg az alábbi ***Perl*** modulok, akkor installáljuk fel az ***IO-Multiplex***, a ***BerkeleyDB*** és a ***Net-Server*** modulokat a ***CPAN***-ról (➲ *ftp://ftp.cpan.org/*). Töltsük le a ***postgrey*** legutolsó verzióját (a cikk írásakor 1.21) az alkalmazás honlapjáról (➲ *http://isg.ee.ethz.ch/tools/postgrey/pub/*). Csomagoljuk ki, majd másoljuk át a programot egy tetszőleges könyvtárba:

```
tar zxvf postgrey-1.21.tar.gz
cp postgrey-1.21/postgrey /usr/local/bin
```



1. ábra A postgrey működése

Hozzunk létre egy felhasználót, akinek a nevében a ***postgrey policy démon*** futni fog:

```
groupadd postgrey
useradd -g postgrey -d /var/postgrey postgrey
usermod -L postgrey
```

Hozzuk létre az adatbázis könyvtárát, és állítsuk be a megfelelő jogosultságokat:

```
mkdir /var/postgrey
chown postgrey:postgrey /var/postgrey
chmod 700 /var/postgrey
```

Itt az idő, hogy elindítsuk a policy démont, adjuk ki az alábbi parancsot:

```
/usr/local/bin/postgrey -d -u /tmp/postgrey \
--user=postgrey \
--group=postgrey \
--dbdir=/var/postgrey \
--delay=600 \
--greylist-text="Szerverunkon a postgrey
➥spamszuro mukodik. Kerjuk, kuldje ujra
➥a levelet 10 perc mulva"
```

A Postfix beállítása

Most már csak a Postfix tudomására kell hozzuk, hogy használja a policy démonunkat. Szerkesszük a */etc/postfix/main.cf* fájlt, és módosítsuk (vagy hozzuk létre) az `smtpd_recipient_restrictions` változót, amellyel az *SMTP* kapcsolat `RCPT TO` szakaszára alkalmazunk korlátozásokat. Ez a paraméter az én gépemen így néz ki:

```
smtpd_recipient_restrictions = permit_mynetworks,
➥reject_unauth_destination,
➥reject_non_fqdn_recipient, check_policy_service
➥unix:/tmp/postgrey
```

Ezzel a beállítással a *main.cf* `mynetworks` változójában szereplő gépek automatikusan fehérlistára kerülnek, azokra a *Postfix* egyáltalán nem alkalmaz korlátozást. Ha elkészültünk a *main.cf* módosításával, akkor indítsuk újra a *Postfixet* a

```
postfix reload
```

paranccsal, és készen vagyunk, a spammerek egy jó részétől megszabadultunk. Legalábbis egyelőre.

Kóstoljuk meg a pudingot!

Ha levelet kapunk, akkor a szerverünk 25-ös portján az *1. listában* látható kommunikáció folyik.
Látható, hogy a *Postfix* `450`-es kóddal (ideiglenes hiba) utasítja el a levelet. A feladó oldalon pedig hibaüzenetként megjelenik a beállított szöveg, amely megnyugtatja a küldőt, miszerint csak egy átmeneti korlátozásról van szó; és ha a levelet 10 perc múlva újraküldi, akkor az rendben el fog jutni a címzetthez.
Ha 10 perc múlva újra próbálkozik a feladó ugyanezzel a levéllel, akkor egy a *2. listában* látható kommunikációt láthatunk.

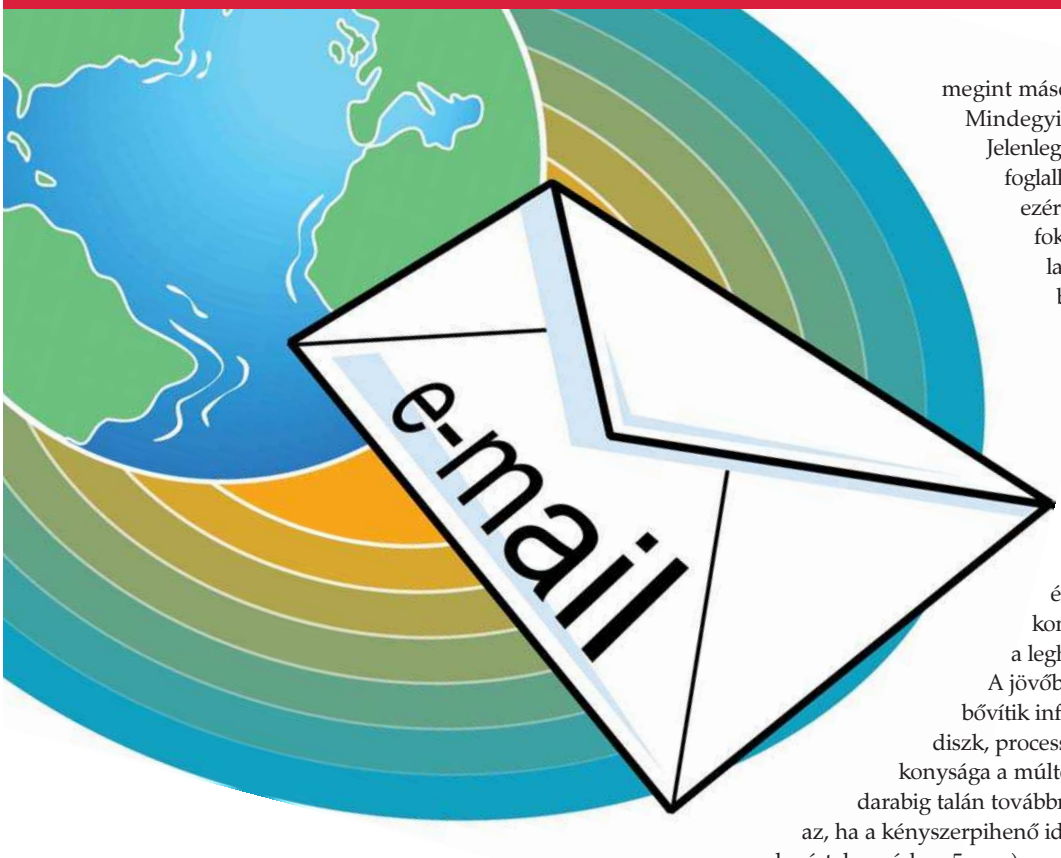
1. lista Kommunikáció a szerver 25-ös portján

```
telnet 10.2.2.2 25
220 rhodium.acts.hu ESMTP Please don't spam
HELO pelda.hu
250 rhodium.acts.hu
MAIL FROM: <teszt@pelda.hu>
250 Ok
RCPT TO: <bela@acts.hu>
450 <bela@acts.hu>: Szerverunkon a postgrey
➥spamszuro mukodik. Kerjuk, kuldje ujra
➥a levelet 10 perc mulva
QUIT
```

2. lista Tíz perc múlva ...

```
telnet 10.2.2.2 25
220 rhodium.acts.hu ESMTP Please don't spam
HELO pelda.hu
250 rhodium.acts.hu
MAIL FROM: <teszt@pelda.hu>
250 Ok
RCPT TO: <bela@acts.hu>
250 Ok
DATA
...
```

Látható, hogy most a `RCPT TO` után már nem utasította el a levelet a *Postfix*, így az mehetett tovább a `DATA` fázisba. Ha ezután ismét levelet akar küldeni az említett feladó ***Bélának***, akkor már nem utasítja el a policy démon, alapesetben 35 napig őrzi meg az ehhez a kapcsolathoz tartozó adatokat – amely érték még a havi hírlevelek szempontjából is megfelelő. De mi van akkor, ha ezúttal nem Bélának, hanem Mártának szeretnének levelet küldeni? Ebben az esetben ismét 450-es hibaüzenettel el fogja utasítani a feladót a *Postfix*. Miért?
Azért, mert a *postgrey* a kliens *IP*-cím/feladó email cím/címzett email cím formátumú úgynevezett ***tripletekben*** (hármasokban) tárolja el az információt. Ha megváltozik pl. a címzett, akkor a *postgrey* ismét egy 10 perces várakozásra kényszeríti a feladót.
Tegyük fel, hogy van néhány megbízható levelezőpartnerünk, akiket nem akarunk ezzel az átmeneti visszautasítással fárasztani. Őket ún. fehérlistára vehetjük fel. Alapértelmezésben az ő *IP*-címüket a */etc/postfix/postgrey_whitelist_clients* fájlban keresi a *postgrey*, de természetesen ez módosítható a `--whitelist-clients` parancssori kapcsoló megadásával. Ha itt megadunk egy *IP*-címet, akkor az onnan érkező összes levelet „fárasztás" nélkül átveszi a *Postfixünk*. Ebben a fájlban sorolhatjuk fel (1 cím – 1 sor) például *Fontos Üzleti Partnerünk* levelező szervereit, így az ő összes levelüket azonnal megkapjuk:




```
# cat /etc/postfix/postgrey_whitelist_clients
1.2.3.4
172.16.88.31
```

Bizonyos esetekben arra is szükség lehet, hogy némely email címre érkező leveleket is késleltetés nélkül beengedjünk. A ***postgrey*** egy másik fehérlistát is kezel, ahol ezeket a címzetteket adhatjuk meg.
A következő példában késleltetés nélkül beengedjük azokat a leveleket, amelyek bármelyik virtuális tartomány postamesterének, vagy pedig a `bela@acts.hu` címre érkeznek:

```
# cat /etc/postfix/postgrey_whitelist_recipients
postmaster@
bela@acts.hu
```

Ha menet közben módosítjuk valamelyik fehérlistát, akkor azt a ***postgrey***-nek küldött `HUP` jelzéssel adhatjuk tudtára.
A ***postgrey*** az említett fehérlistákon kívül még egyet kezel, amelyet automatikusan tart karban. Erre a listára akkor kerül fel egy kliens, ha már legalább 5 (`--auto-whitelist-clients`) alkalommal sikeresen átjutott a szürkelistán – óránként csak 1 sikeres kézbesítés számít. A ***postgrey*** feltételezi, hogy ebben az esetben legitim levelezőpartnerről van szó, és ezután már nem állítja meg ezt a klienst átmeneti hibával. Ha letelt a 35 nap (`--max-age`), akkor a klienst törli erről a fehérlistáról.

További gondolatok

A ***postgrey Berkeley*** adatbázisban tartja a tripleteket, de nem ez az egyetlen lehetőség. Az adatbázis épsége érdekében tranzakciókat használ. Más megvalósítások például ***MySQL*** adatbázisban tárolják ezeket az információkat, megint mások pedig a fájlrendszerben. Mindegyiknek megvan a maga előnye. Jelenleg a spammerek jellemzően nem foglalkoznak az elutasított levelekkel, ezért a szürkelista nagyon jó hatásfokkal működhet. A ***postgrey*** honlapja szerint, míg a szürkelista bekapcsolása előtt percenként körülbelül 15 vírus és spam került a rendszerbe, addig utána már csak 3. A szürkelista tehát hatékonyan képes csökkenteni az egyéb típusú (például ***Bayesian***, heurisztikus, stb.) spamszűrők terhelését. Amint előző írásomban is említettem, jelenleg a ***Bayesian*** és heurisztikus spamszűrővel kombinált szürkelistát tartom a leghatékonyabb védekezésnek.
A jövőben azonban – ha a spammerek bővítik infrastruktúrájukat (sávszélesség, diszk, processzor, stb.) – a szürkelista hatékonysága a múlté lehet. Ebben az esetben egy darabig talán továbbra is megfelelő védelmet adhat az, ha a kényszerpihenő idejét (ami a ***postgrey*** esetében alapértelmezésben 5 perc) megnöveljük – ***Evan Harris*** (➲ ***http://www.greylisting.org/articles/whitepaper.shtml***) eleve 1 órás beállítást javasol. Mindenesetre ha a spammerek így is tesznek, az számukra megdrágítja az egy levél tényleges elküldésére jutó egységnyi költséget, és ez nekünk jó.
Gyakori az az eset, amikor a spammerek a tartalék (backup) `MX` szervereket célozzák meg a spammel, mert az elsődleges `MX` szerver általában minden további nélkül átveszi a leveleket a tartalék `MX`-ektől. Ezt úgy lehet kivédeni, ha egy tartomány minden `MX` szerverét felruházzák szürkelista védelemmel, ill. közös adatbázisból dolgoznak, és ha az elsődleges `MX` fehérlistájában szerepel az összes tartalék `MX`. A ***postgrey*** ebben a környezetben is megállja a helyét, képes ***TCP*** socket-en is kommunikálni (a `-i` kapcsoló használatával). ***Harris*** szerint, ha a spammerek alkalmazkodnak, akkor nyilván a lehető leghamarabb el akarják küldeni a leveleket, ezért rövid időn belül – minden bizonnyal többször is – próbálkozni fognak, még mielőtt a szürkelista által megszabott idő letelne. Ebben az esetben viszont érdemes módosítani a szürkelista implementációkat úgy, hogy számolják, hány idő előtti próbálkozás történik, és egy bizonyos határ felett (hogy a legitim ***SMTP*** szerverek ne essenek bele) már nem szürke, hanem feketelistára tehetjük ezeket a próbálkozókat. Ha pedig már ez is kevés lesz, akkor új megoldások után kell néznünk, de addig is remélhetőleg lesz még pár napos és spammentes napunk.

Sütő János (jsuto@freemail.hu)
1997 óta használ Slackware Linux-ot. Szabadidejében a postfix clapf nevű vírus- és spamszűrőjét polírozza.