Greylisting za postfix: postgrey

Na portalu za sistemce postoji članak (http://sistemac.carnet.hr/node/101 [1]) gdje je opisan način rada i implementacija greylistinga za sendmail. Ovdje ćemo opisati greylisting za postfix, postgrey.

Postgrey nema posebnu konfiguracijsku datoteku, osim /etc/default/postgrey. U principu, ovdje se nema što ni mijenjati, osim eventualno vremena usporenja za inicijalni primitak maila, --delay. U CARNetovom paketu je ova vrijednost podešena na 58 sekundi:

```
POSTGREY_OPTS="--delay=58 --inet=127.0.0.1:60000"
```

Ostatak retka govori da postgrey daemon sluša na lokalnom mrežnom sučelju na portu 60000. Naravno, odgovarajuća vrijednost mora postojati i u postfixu u main.cf (pored ostalih opcija):

```
smtpd_recipient_restrictions = check_policy_service inet:127.0.0.1:60000
```

Da se podsjetimo, greylisting radi na način da za svaku SMTP sesiju (session, sjednicu) zabilježi tri parametra: IP adresu udaljenog računala, envelope adrese pošiljatelja i primatelja, takozvani triplet. Svaki put kad vidi jedinstvenu kombinaciju ova tri parametra, odnosno jedinstveni triplet, greylista odbije mail (uz standardnu poruku "450 <netko@negdje.hr> [2]: Recipient address rejected: Greylisted for XX seconds") i zabilježi triplet u svoju whitelistu.

Ukoliko u navedenom periodu od XX sekundi udaljeni poslužitelj opet bude pokušao isporučiti mail, on će biti odbijen, ali se vrijeme odbijanja (delaya) i dalje smanjuje. Kad to vrijeme istekne, mail će uredno biti zaprimljen.

Razlog ovakvog ponašanja ovog filtera je jednostavan: svaki (ispravno podešeni) mail poslužitelj ***mora*** pokušavati isporučiti mail nekoliko puta, često i nekoliko desetaka puta u periodu od nekoliko sati do nekoliko dana, u ovisnosti o postavkama udaljenog poslužitelja. Spammeri rabe posebne programe, koji ne poštuju sve konvencije te se ni ne trude protumačiti poruke o greškama koje dobivaju od udaljenih poslužitelja. Njima je jedino bitno isporučiti što više spamova u što kraćem vremenu.

Zbog ove činjenice efikasnost greyliste je čak oko 97%, iako se može očekivati ovo smanjenje čim se spammeri budu prilagodili. Do danas ta prilagodba nije primijećena u znatnijoj mjeri.

Jedan manji problem kod greylistinga je zaustavljanje svih mailova koje sustav susreće po prvi put. Kako bi se ovo ponašanje ublažilo, defaultno je uključena opcija --auto-whitelist-clients=5. Ona jednostavno omogućava da se nakon 5 uspješno propuštenih mailova ta IP adresa stavi u whitelistu i na taj način trajno omogući primanje mailova s te adrese, bez ikakvih usporavanja. Da bi --auto-whitelist-clients opcija proradila, treba zadovoljiti dodatni uvjet da je IP adresa s koje je poslan mail "viđena" u zadnjih --max-age dana (default je 35).

Slična se operacija može napraviti i ručno (što je puno fleksibilnije), što ćemo obraditi u nastavku članka.

Kako ne bi bespotrebno usporavali e-mail promet unutar Hrvatske, paket postfix-cn donosi popis većine MX poslužitelja u CARNetu. Ovi se poslužitelji nalaze u datoteci /etc/postgrey/whitelist_clients(.local). Ovdje možete dopisati MX poslužitelje s kojih vam dolazi

znatnija količina pošte. Primjerice:

```
negdje.nesto.hr
161.53.xxx.yyy
/.*\.carnet\.hr/
```

Dakle, moguće je koristiti ime udaljenog računala, njegovu IP adresu ili regularni izraz koji opisuje poslužitelje koje želite propuštati bez zastoja.

U istom direktoriju postoji datoteka whitelist_recipients. Kako samo ime govori, radi se o datoteci gdje možete upisati primatelje na lokalnom računalu za koje se greylista neće primjenjivati. Ovo ne znači da se mail neće dalje provjeravati u SpamAssassinu, te je moguće da mail bude odbijen (jer je spam) iako je prošao greylistu!

U obje datoteke možete upisati nazive poslužitelja, IP adrese, e-mail adrese, regularne izraze i slično. Potpuni popis potražite u man stranicama (man postgrey).

Nakon bilo kakve promjene u ovim (dodatnim) whitelistama, napravite reload postgreya:

```
# /etc/init.d/postgrey reload
```

U mail.logu će se moći vidjeti sljedeći redak:

```
Mar  8 21:42:02 po postgrey[16648]: HUP received: reloading whitelists...
```

Fizički, baza tripleta (whitelista) se nalazi u /var/lib/postgrey i ne briše se između restarta računala. Ne morate (ni nemojte!) ovdje ništa dirati.

Više informacija imate na URL-u http://projects.puremagic.com/greylisting [3] i naravno, u manualu (man postgrey).

- Logirajte [4] se za dodavanje komentara

pet, 2007-03-09 10:41 - Željko Borš**Kuharice:** Za sistemce [5]
Kategorije: Servisi [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/107

Links
[1] http://sistemac.carnet.hr/node/101
[2] mailto:netko@negdje.hr
[3] http://projects.puremagic.com/greylisting
[4] https://sysportal.carnet.hr/sysportallogin
[5] https://sysportal.carnet.hr/taxonomy/term/22

[6] https://sysportal.carnet.hr/taxonomy/term/28