

Postfix: kako zabraniti primanje određenih dolaznih poruka?



Postfix podržava filtriranje poruka u bilo kojoj fazi SMTP sjednice (sessiona), dakle može blokirati ili propustiti mail na osnovu adrese pošiljatelja, IP adresi ili domeni s kojom se udaljeni poslužitelj predstavlja, kao i po drugim, manje korištenim parametrima. Filtriranje po adresi pošiljatelja može zvučati kao dobro mjerilo, no u realnosti to nije tako. Ova se adresa bez ikakvih problema može lažirati, pa nema smisla blokirati prema ovom mjerilu ukoliko mislimo spriječiti spam. No, ipak u određenim situacijama ima smisla rabiti ovo mjerilo.

Obično prepuštamo kombinaciji Amavis/SpamAssassin da se brine o spamu, koji to u velikom postotku uspješno i čini. No, zbog određenih postavki ili njihovih kombinacije ([poput ovog primjera](#) [1]), moguće je da uporni korisnik ili korisnici s iste domene mogu slati spam. Obično se to događa kod korisnika unutar Hrvatske ili iz regije jer nisu pisani na engleskom pa izbjegnu standardnu detekciju.

Moramo napomenuti da je ovakve slučajeve najbolje prijaviti nadležnim Abuse službama, a tek nakon njihove eventualne neaktivnosti pribjeći ovakvim rješenjima. Dovoljno je da pošiljatelj promijeni odlaznu adresu i spam će proći, čineći ovu metodu neefikasnu kao sredstvo zaštite od spama. S druge strane, može uštedjeti nešto resursa, jer će odbiti mail odmah na ulazu u sustav i neće ga se proslijediti u Amavis/SpamAssassin.

Sve što vam treba je access datoteka s unosima adresa, cijelih ili djelomičnih, te s akcijama koje trebaju biti poduzete nad njima. Ovaj tip datoteka Postfix rabi u svim drugim načinima filtriranja koje podržava, a više o formatu datoteke pročitajte u [man](#) stranici sa "**man 5 access**".

Pojednostavljeno, datoteka izgleda ovako:

@domena.hr	DISCARD domena.hr spam message discarded
root@domena.hr	OK
netko@spam.hr	REJECT Odbijeno zbog spama.

U prvom stupcu se nalazi puna e-mail adresa ili njen dio, a u drugom akcija koja će se provesti ako dolazni mail odgovara adresama navedenim u access datoteci.

U primjeru, svi mailovi u obliku "domena.hr" će biti ignorirani (udaljeni poslužitelj će vidjeti kao da je mail uredno zaprimljen), a poruku iza naredbe "DISCARD" ćete moći vidjeti u logovima. Poruka, inače, nije obavezna. No, poruke od root korisnika ("root@domena.hr") će biti propuštene.

Ukoliko netko pošalje mail s adrese "netko@spam.hr", mail će mu biti odbijen (zato što rabimo "REJECT"), i moći će vidjeti našu poruku.

U prvom stupcu, osim pune adrese možete rabiti i sve druge načine koji su uobičajeni u postfix access datotekama. Izdvojit ćemo najčešće (ostale oblike možete naći s "**man 5 access**"):

korisnik@

U ovom slučaju, domena se ne gleda, nego samo koji je korisnik poslao poruku

domena.hr

Sve poruke s "@domena.hr" će biti obrađene. Podrazumijevano, ovo ne znači i poddomene, primjerice "@studenti.domena.hr". Ukoliko želite da se obrađuju i poddomene, stavite točku ispred .domena.hr. Ukoliko je postavljena varijabla `parent_domain_matches_subdomains`, točka ispred naziva domene nije potrebna, nego će se obrađivati i poddomene. Više o tome pročitajte u članku na <http://sistemac.carnet.hr/node/569> [2].

Akcija koje mogu biti provedene ima mnogo (DEFER, BCC, FILTER, REDIRECT...), no već smo naveli najčešće iz prakse. Mogli bi navesti još jedan čest primjer:

```
domena.hr          554 Spam not welcomed here
```

Gornji redak će, osim tekstom, poruku popratiti i standardnim SMTP kodom, pa ćemo time udaljeni poslužitelj ljubazno obavijestiti o čemu se radi, a on na osnovu toga odraditi njemu definirane akcije.

Kad jednom složite svoju access listu, tu datoteku nazovite prigodnim imenom (primjerice, `/etc/postfix/sender_access`), te u `/etc/postfix/main.cf` upišite redak:

```
smtpd_sender_restrictions = check_sender_access  
    hash:/etc/postfix/sender_access
```

Ostaje još samo konvertirati datoteku u binarni hash:

```
# postmap /etc/postfix/sender_access
```

i restartati, odnosno *reloadati* postfix:

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

Više o svim ostalim načinima limitiranja unutar SMTP sesije pročitajte na adresi http://www.postfix.org/SMTPD_ACCESS_README.html [3].

- [Logirajte](#) [4] se za dodavanje komentara

uto, 2010-03-30 21:56 - Željko BorošKuharice: [Linux](#) [5]

Kategorije: [Servisi](#) [6]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/735>

Links

[1] <https://sysportal.carnet.hr/node/734#primjer>

[2] <https://sysportal.carnet.hr/node/569>

[3] http://www.postfix.org/SMTPD_ACCESS_README.html

[4] <https://sysportal.carnet.hr/sysportallogin>

[5] <https://sysportal.carnet.hr/taxonomy/term/17>

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