Tips Singkat Pada Postfix Untuk Mengurangi SPAM

Raden Mohamad Dikshie Fauzie
dikshie@ppk.itb.ac.id
http://ipv6.ppk.itb.ac.id/~dikshie/

Pada saat ini SPAM adalah fenomena paling menyebalkan di internet, hampir setiap orang pasti pernah mendapatkan email SPAM.

Tulisan berikut ini akan memaparkan tips sederhana untuk mail server berbasis Unix atau Linux dengan menggunakan Postfix sebagai MTA (Mail Transfer Agent) untuk mengurangi SPAM. Tulisan ini dibuat dengan asumsi bahwa pembaca telah terbiasa melakukan instalasi aplikasi pada system operasi Unix atau Linux, terbiasa melakukan sistem administrasi pada sistem operasi Unix atau Linux, terbiasa membaca dan mengerti email header, dan mengerti bagaimana cara kerja mail server.

REVIEW INSTALASI POSTFIX

Jika anda pemakai linux lebih mudah melakukan installasi Postfix menggunakan paket binary yang telah disediakan oleh distro anda, misalnya bila anda menggunakan distro RedHat maka gunakan paket *.rpm, begitu pula untuk distro yang lain seperti Mandrake, Suse, dan lain-lain. Untuk pemakai Debian anda lebih baik menggunakan paket *.deb yang telah disediakan oleh Debian. Untuk anda pemakai Unix BSD seperti FreeBSD atau OpenBSD sebaiknya melakukan installasi melalui mekanisme ports (`/usr/ports/mail/postfix-devel`).
Source postfix sendiri dapat didownload pada: http://www.postfix.org

MENGURANGI SPAM DENGAN CARA MEMERIKSA HEADER DAN BODY EMAIL

MTA Postfix dilengkapi fitur `body_checks` dan `header_checks`. Dengan mengunakan fitur ini mail server dapat langsung menolak email yang datang berdasarkan pola yang dipakai oleh fitur tersebut. Contoh pada file konfigurasi Postfix, main.cf adalah sebagai berikut:

```
body_checks = regexp:/usr/local/etc/postfix/body_checks
```

Dimana file body_checks berisi pola/pattern. Contohnya sebagai berikut:

```
/^Hi! How are you?$/     REJECT
```

Ini artinya bila di body email ada frasa Hi! How are you ? maka postfix akan otomatis melakukan penolakan email tersebut, dan email akan dikirim kembali kepada pengirim.
Hal yang sama berlaku untuk fitur `header_checks.` Contoh pada file konfigurasi postfix, main.cf adalah sebagai berikut:

```
header_checks = regexp:/usr/local/etc/postfix/header_checks
```

Dimana file header_checks berisi pola/pattern.Contohnya sebagai berikut:

```
/^From:.*@sexyfun.net/ REJECT
```

Ini artinya email dari @sexyfun.net akan ditolak oleh postfix mail server, email akan dikembalikan kepada pengirim.

Arti regexp pada file konfigurasi postfix, main.cf diatas artinya bahwa pola/pattern yang akan digunakan adalah pola berdasarkan regular expression atau biasa dikenal dengan regex.
Untuk dapat membuat pola/patern anda harus mengusai regex ini dengan baik, referensi seperti buku *Mastering Regex* karya Jeffry Friedl dari penerbit O'Reilly sangat baik untuk buku pegangan belajar regex. Namun jangan khawatir di internet banyak orang yang membuka file `body_checks` dan `header-checks` untuk umum. Situs berikut ini contohnya:

```
http://www.securitysage.com/guides/postfix_uce.html
http://www.hispalinux.es/~data/postfix
```

Karena pola yang dipakai untuk tiap admin untuk mengurangi Spam berbeda karena itu jangan terlalu berharap bahwa dengan pola regex milik orang lain ini akan bekerja baik 100% pada sistem milik anda.

MENGURANGI SPAM DENGAN CARA MEMERIKSA CATATAN DNS DAN MAP

Postfix mempunyai fitur untuk melakukan restriksi berdasarkan catatan DNS mail server..
Option tersebut adalah :
`smtpd_sender_restrictions`
secara default isi dari parameter `smtpd_sender_restrictions` adalah :
`permit_mynetworks` dan `reject_unauth_destination`
selain isi tersebut anda dapat menambahkan:

`reject_unknown_client`	Menolak permintaan dari client bila hostname client tidak ada/tidak diketahui, atau ketika terjadi kegagalan query terhadap reverse address DNS
`reject_maps_rbl`	Menolak client jika terdapat pada daftar `$maps_rbl_domains` *(penjelasan detail ada diabawah)
`reject_invalid_hostname`	Menolak hostname dengan syntax yang salah
`reject_unknown_hostname`	Menolak hostname tanpa record A atau MX DNS
`reject_unknown_sender_domain`	Menolak domain pengirim tanpa A atau MX record DNS
`check_sender_access maptype:mapname`	Memeriksa alamat pengirim pada map yang didefinisikan dan memutuskan apakah ditolak atau tidak ** (penjelasan detail ada dibawah)
`rject_non_fqdn_hostname`	Menolak HELO dari hostname yang tidak dalam bentuk FQDN

`reject_non_fqdn_sender`	Menolak alamat pengirim yang tidak dalam bentuk FQDN

`*reject_maps_rbl` berhubungan option `$maps_rbl_domains`, dimana option `maps_rbl_domain` isinya kosong. Ada beberapa situs yang menyediakan layanan RBL (Realtime Blackhole List), namun layanan ini biasanya tidak gratis. Contohnya: http://www.mail-abuse.org.
Bila anda ingin layanan ini maka contohnya anda dapat mengisi options `maps_rbl_domain=rbl.maps.vix.com`

**Untuk option `check_sender_access maptype:mapname` contoh penggunaannya seperti berikut ini:

```
smtpd_sender-restrictions=hash:/usr/local/etc/postfix/access
```

dimana file `/usr/local/etc/postfix/access` berisi:

```
spamdomain.com       550    Mail rejected.   Known spam site.
```

Ini artinya mail server kita akan menolak email dari domain spamdomain.com dengan kode error 550.
Jangan lupa setelah membuat file `/usr/local/etc/postfix/access`
Untuk menjalankan program `postmap` untuk membuat atau mengupdate file database `access.db`
Contohnya seperti berikut ini:

```
#postmap /usr/local/etc/postfix/access
```

setelah itu jangan lupa untuk me-restart postfix :

```
#postfix reload
```

Untuk mencegah user tidak bersalah terblok maka file access tersebut dapat dibuat variasi, dengan contoh seperti berikut ini :

```
spamdomain.com               550    Mail rejected.   Known spam site.
tidakbersalah@spamdomain.com OK
```

Jangan lupa kembali untuk mengupdate file access tersebut dengan postmap dan merestart postfix.

BIOGRAFI PENULIS

R Mohamad Dikshie Fauzie. Menamatkan pendidikan S1 dibidang Fisika Oseanografi pada Departemen Geofisika dan Meteorologi ITB tahun 2000. Pada tahun 2001 menjadi mahasiswa magister Teknologi Informasi ITB. Bidang peminataan pada: TCP/IP, IP Multicast, IPv6, dan UDLR. Saat ini penulis sedang menyelesaikan tesis magister dengan topik IPv6. Menggunakan sistem operasi FreeBSD pertama kali pada tengah 1998, FreeBSD-2.2.6

Informasi lebih lanjut tentang penulis ini bisa didapat melalui:
URL: *http://ipv6.ppk.itb.ac.id/~dikshie/*
Email: *dikshie@ppk.itb.ac.id*