Configure Sendmail Server :Controlling SPAM Part-3

Author : Vikas Debnath

Categories : Mailserver

Date : May 17, 2015

- Facebook
- Twitter
- Google+
- Gmail

Using Realtime Blackhole lists

When running Sendmail, one can take advantage of Realtime Blackhole Lists. These are lists of hosts known to be sending out spam, and kept up to date by whoever maintains these lists. When using such features, Sendmail will drop the connection before receiving the e-mail, with the appropriate error message. Isn't that sweet? Not only are you reducing the amount of spam you're getting, but there's very little bandwidth wasted along the way.

In order to use this feature, you'll need to make changes to the configuration of Sendmail. The use of a macro config file (.mc) makes this a lot easier. By adding the following line to /etc/mail/sendmail.mc, you should start noticing a reduction of spam.

> FEATURE(dnsbl', ipwhois.rfc-ignorant.org',"550 Mail from " $&{client_addr} " refused. Rejected for bad WHOIS info on IP of your SMTP server - see http://www.rfc-ignorant.org/"')

FEATURE(dnsbl', proxies.blackholes.easynet.nl', “550 5.7.1 ACCESS DENIED to OPEN PROXY SERVER “$&{client_name}” by easynet.nl DNSBL (http://proxies.blackholes.easynet.nl/errors.html)”‘, ')dnl

FEATURE(dnsbl', bl.spamcop.net', “450 Mail from ” $'&{client_addr} " refused - see http://spamcop.net/bl.shtml"')

FEATURE(dnsbl',sbl.spamhaus.org',Rejected – see http://spamhaus.org/')dnl

Using Access Database

Sendmail checks with a database to see who has what access. One of the features here is using the REJECT keyword. With this, you can reject connections from the specified IP address, IP subnet or domain name! Tired of getting spammed from Korea? You can block out all IP addresses from Korea, and the problem is gone. However, in order to use this, you need to make sure that the use of the Access Database is enabled in Sendmail. This is done with the following line in the /etc/mail/sendmail.mc file.

FEATURE(access_db',hash -o /etc/mail/access.db')dnl

Once that’s in there, and the macro config file has been compiled, Sendmail is ready to use the access database. If I recall correctly, this feature is enabled by default. There’s also a minor difference in how this entry is listed (by default) in the sendmail.mc file between 8.11.x and 8.12.x. In 8.12 there’s an addition “-T” parameter to the “hash” command. Just leave the line as it is, it’s listed above just so you know what to look for.

Also by default, there should be a couple of entries in the /etc/mail/access file. It should look something like this:

```
localhost.localdomain        RELAY
localhost                    RELAY
127.0.0.1                    RELAY
```

This is just to allow the local host (the server itself) to send and receive mail.

In order to block mail, you’ll need to add some rejects… Recently, I’ve been getting a lot of spam from a certain ISP in china, so, I’m blocking all of it with the following line:

```
xing.com.cn                  REJECT
```

This one line will reject all connections from all hosts within the “xing.com.cn ” domain. You can achieve the same effect (more or less) with the following line:

147.171.39. REJECT

Note that once you have added entries in the /etc/mail/access file, you need to re-create the actual database. This can be done with the following command, entered while in the /etc/mail directory:

make all

The only thing you need to do now, is figure out who to block out. I simply add hosts or domains when I receive spam from them. It’s easy enough to find the IP address and/or domain name of the sender by checking the headers of the message. You can also search through the /var/log/maillog file to find the offender, and the real IP address of the sending mail server is bound to be in there.

Don’t accept mail from unresolvable domains!

One of the “tricks” that spammers use, is to send mail from made up domains. You can easily refuse mail from such domain with Sendmail. I don’t recall what the default setting was, but at the bottom of the sendmail.mc file, there should be an entry looking like this:

dnl FEATURE(accept_unresolvable_domains')dnl

The "dnl" in front indicates that the line should not be included when re-creating the configuration file, thus disabling the feature. Check your /var/log/maillog file for the following error message "reject=451 4.1.8", and you should see a nice list ...

Use SpamAssassin

Once sendmail receives an e-mail message, it hands the message over to procmail, which is the application that actually places the e-mail in user mailboxes on the mail server. You can make procmail temporarily hand over control to another program, such as a spam filter. The most commonly used filter is spamassassin.

spamassassin doesn't delete spam, it merely adds the word "spam" to the beginning of the subject line of suspected spam e-mails. You can then configure the e-mail filter rules in Outlook Express or any other mail client to either delete the suspect message or store it in a special Spam folder.

```
[root@mail1 spamassassin]# rpm -q spamassassin
spamassassin-3.2.5-1.el5
```

if not there use **yum install spamassassin**, go the the folder **/etc/mail/** there is a folder

```
[root@mail1 mail]# ls
access          local-host-names  sendmail.cf.bak  trusted-users
access.db       mailertable       sendmail.mc      virtusertable
```

```
domaintable     mailertable.db    spamassassin     virtusertable.db
domaintable.db  Makefile          submit.cf
helpfile        sendmail.cf       submit.mc
[root@mail1 mail]#
```

[root@mail1 mail]# cd spamassassin/

```
[root@mail1 spamassassin]# ls
init.pre  spamassassin-default.rc  spamassassin-spamc.rc  v312.pre
local.cf  spamassassin-helper.sh   v310.pre               v320.pre
```

[root@mail1 spamassassin]# vi local.cf

```
# These values can be overridden by editing ~/.spamassassin/user_prefs.cf
# (see spamassassin(1) for details)

# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.

required_hits 5
report_safe 0
rewrite_header Subject [SPAM]
whitelist_from  mr.vivekpal@gmail.com
blacklist_from *@comcast.net
```

where :

To explain what we are doing and why we are doing this, we will need a short run-down on the above lines.

Required_hits: This determines the filter balance; the lower the score the more aggressive the filter. A setting of 5.0 is generally effective for a small organisation or a single user. Adjust the strictness score to your organization's needs - a large medical organisation might want to let email items through that are trying to sell pharmaceuticals, so we might increase the level to a more modest 8.0.

Report_safe: This line determines whether to delete the item or to move the item to the inbox whilst appending a spam notice to the subject line. The levels for this line are set to either a 1 or 0. A score of 1 will delete the spam item, whereas a score of 0 will send the item to the inbox and rewrite the subject line. For this guide we shall use 0 as the score.

Required_score: This line sets the spam score for all email alllowed through to your domain,

with levels of certainty set from 0 to 5. Zero would be classified as a legitimate email item, whereas 5 would be an definite ‘SPAM’ item. If we set the score to 3 we would catch a lot of unsolicited emails but quite a few false positives would still get through. For our example email server we will use the score of 5, but you can of course set this value according to your preference.

Rewrite_header: This line does exactly what it implies, that is, any message caught as ‘SPAM’ will have the subject line rewritten to include this header. For this guide we will use the default subject header of [SPAM].

whitelist_from: Some time genuine mails will land in junk box, we need to whitlist it to land it in inbox for the next time.

blacklist_from: Some time Spam Mails are landed into Inbox, we need to blacklist this to not landed into inbox again.

Now that we have the spam variables set up we will now move on to creating the spamd function.

Using Procmail

we can use /etc/procmailrc to control spam for examples

procmailrc spam death_____

/etc/procmailrc

```
:0 wh: msgid.log
| formail -D 1008192 $HOME/msgid.cache
:0
* MensHealth.com
/dev/null
:0
* Subject: {Spam?}
/dev/null
:0
* From: viagra
/dev/null
:0
* From: Viagra
/dev/null
:0
* MensHealth.com
* Rosalyn Bass
/dev/null
```

```
:0
* From: Mail Delivery System
/dev/null
:0
* From: CIALIS.COM
/dev/null
:0
* Subject:Pharmacy
* Subject:watches
* From:Internet Mail Delivery
* Subject:Your credit card balance limit
* Subject:Credit limit exceeded
/dev/null
:0
* MAILER-DAEMON@host.ddppl.in.com
* Subject:SALE
* Subject:sale
/home/spamreport1/mail/
:0
* From:MensHealth.com
/dev/null
:0
* From:VIAGRA
* From:Pfizer
/dev/null
:0
* Subject:Have I disappointed you?
* Subject:Bank account overdraft
* Subject:credit card
* Subject:  Personal loan
* Subject:% 0FF
* Subject:more %
/dev/null
:0fw
| /usr/bin/spamassassin
:0
* ^X-Spam-Status: Yes
/home/spamreport/mail/
DEFAULT=$HOME/mail/
```

Note: Last red lines show , procmail will deliver mails with spam status yes (spam mails) to a separate user here spamreport (you have to create this user)

Some Other Options Embedded with Sendmail just have a look

```
define(confPRIVACY_FLAGS',goaway')dnl
```

```
FEATURE(smrsh)dnl
define(confMAX_HEADERS_LENGTH',16384)dnl
define(confMAX_MESSAGE_SIZE',2097152)dnl
define(confCONNECTION_RATE_THROTTLE',3)dnl
define(confMAX_DAEMON_CHILDREN',12)dnl
define(confSMTP_LOGIN_MSG', $j server ready at $b')dnl
define(confMAX_RCPTS_PER_MESSAGE,25)dnl

FEATURE(relay_entire_domain')
FEATURE(relay_based_on_MX')
FEATURE(relay_local_from')
FEATURE(relay_mail_from')
FEATURE(loose_relay_check')
FEATURE(accept_unresolvable_domains')
FEATURE(access_db')
FEATURE(relay_hosts_only')
FEATURE(blacklist_recipients')
FEATURE(dnsbl')
FEATURE(`delay_checks')
```

We can use this features as per our situations

_____-

The primary anti-spam features available in sendmail are:

Relaying is denied by default.
Better checking on sender information.
Access database.
Header checks.

Relaying (transmission of messages from a site outside your domain to another site outside your domain) is denied by default.

If you use

FEATURE(relay_entire_domain)

then any host in any of your local domains will be relayed.

You can also allow relaying based on the MX records of the host portion of an incoming recipient address by using

FEATURE(relay_based_on_MX)

For example, if your server receives a recipient of user@domain.com and domain.com lists your server in its MX records, the mail will be accepted. Note that this will stop spammers from using your host to relay spam but it will not stop outsiders from using your server as a relay for their site. Along the same lines,

FEATURE(relay_local_from)

will allow relaying if the sender specifies a return path (i.e. MAIL FROM:) domain which is a local domain. This a dangerous feature as it will allow spammers to spam using your mail server by simply specifying a return address of user@your.domain.com. It should not be used unless absolutely necessary.

If source routing is used in the recipient address (i.e. RCPT TO:), sendmail will check user@site.com for relaying if othersite.com is an allowed relay host in either class 'R', class 'm' if **FEATURE(relay_entire_domain)** is used, or the access database if **FEATURE(access_db)** is used. To prevent the address from being stripped down, use:

FEATURE(loose_relay_check)

If you think you need to use this feature, you probably do not. This should only be used for sites which have no control over the addresses that they provide a gateway for. Use this FEATURE with caution as it can allow spammers to relay through your server if not setup properly.

As of 8.9, sendmail will refuse mail if the MAIL FROM: parameter has an unresolvable domain (i.e., one that DNS, your local name service, or special case rules in ruleset 3 cannot locate). If you want to continue to accept such domains, e.g. because you are inside a firewall that has only a limited view of the Internet host name space (note that you will not be able to return mail to them unless you have some "smart host" forwarder), use

FEATURE(accept_unresolvable_domains)

sendmail will also refuse mail if the MAIL FROM: parameter is not fully qualified (i.e., contains a domain as well as a user). If you want to continue to accept such senders, use

FEATURE(accept_unqualified_senders)

View video for more explanation

Vikas Debnath

CEO, KV IT-Solutions Pvt. Ltd. | vikas@kvit.in | 9810028374|
Linux Professional and an Industrial Trainer | 20 + years Experience in IT Industry

” We are born free, No Gate and Windows can snatch our freedom “

- Facebook
- Twitter
- Google+
- Gmail