Mail filtering examples

These are snippets of configuration for an Exim-based MTA. They have had some simple testing but are intended mainly as a starting point for building your own customised configurations. Test them for yourself, and read the related parts of the documentation.

---

1. RBL blacklists with opt-in/opt-out

Here we will configure Exim to check incoming mail against DNS RBLs, but individual users can have a different set of RBLs which apply to their account (which can be empty, in which case they have opted out of filtering altogether).

Customised RBLs can help improve the accuracy of your filtering. For example, if a particular user knows that they will never receive any legitimate mail from a particular country, then they can use an RBL which lists all IP addresses in that country (see http://blackholes.us/), without affecting any other users on your system.

Firstly, create a file `/usr/local/etc/exim/dnslists` containing E-mail addresses (one per line), followed by a space or tab and the list of RBLs to use for that user. If you want a default policy to apply to all other users, put a line starting "*". For a policy which applies to all users in at domain.com, use "*@domain.com". If someone wants no RBL filtering at all, leave the right-hand side blank.

```
fred@flintstone.org      korea.blackholes.us : china.blackholes.us
wilma@flintstone.org
*                        sbl.spamhaus.org : ordb.relay.org : bl.spamcop.net
```

Now edit the configuration file `/usr/local/etc/exim/configure`. In the section 'begin acl' locate the following lines:

```
  # deny    message       = rejected because $sender_host_address is in a black list at $dnslist_domain\n$
  #         dnslists      = black.list.example
```

Uncomment these two lines and change the second line as shown here:

```
  deny    message       = rejected because $sender_host_address is in a black list at $dnslist_domain\n$dn
          dnslists      = ${lookup{${lc:$local_part@$domain}}lsearch*@{/usr/local/etc/exim/dnslists}}
```

How does this work? Instead of having a static list of dnslists, which is the same for everyone, we perform a file lookup to decide which dnslists to use for this particular recipient. This is using Exim's "string expansion" facility.

${lookup{key}lsearch*@{file}}
: Lookup the value "key" in the file "file". The result of the expansion is the rest of the line in the file.

lsearch*@
: We perform a linear search (top to bottom) through a plain text file. If the key "foo@bar" is not found, then we look a second time for "*@bar", and if still not found, look a third time for "*".

${lc:some-string}
: Expands "some-string" and converts it to Lower Case. This is because incoming mail might be using uppercase characters for some or all of the address, so we need to convert to all lower-case to find the key.

$local_part@$domain
: The E-mail address which we are currently processing

You can test and debug string expansions like this using exim's `-be` (expression testing) mode.

```
# /usr/local/sbin/exim -be '${lookup{fred@flintstone.org}lsearch*@{/usr/local/etc/exim/dnslists}}'
korea.blackholes.us : china.blackholes.us
```

To test whether the policy works use exim's -bh mode which simulates an SMTP connection from a particular IP address. The address 61.32.0.1 is included in the korea.blackholes.us list, so:

```
# /usr/local/sbin/exim -bh 61.32.0.1

**** SMTP testing session as if from host 61.32.0.1
**** This is not for real!
220 noc.t1.ws.afnog.org ESMTP Exim 4.34 Wed, 19 May 2004 15:18:30 +0000
mail from:<>
250 OK
rcpt to:<wilma@flintstone.org>
250 Accepted
```

```
rcpt to:<fred@flintstone.org>
550-rejected because 61.32.0.1 is in a black list at korea.blackholes.us
550 Korea blocked by korea.blackholes.us
quit
221 noc.t1.ws.afnog.org closing connection
```

If the `/usr/local/etc/exim/dnslist` file gets big, then it will be slow to search. In this case, you can convert it into an indexed .db file:

```
# /usr/local/sbin/exim_dbmbuild /usr/local/etc/exim/dnslists /usr/local/etc/exim/dnslists.db
```

You'll have to run this command every time you change dnslists. Then make another change to the configure file:

```
change          ....lsearch*@{/usr/local/etc/exim/dnslists}}
to              ....dbm*@{/usr/local/etc/exim/dnslists.db}}
```

For more information read the Exim manual, which is `doc/spec.txt` inside the source directory, or online at www.exim.org

---

2. Content filtering: exiscan-acl

Exim has some hooks which allow other people to write extensions which perform content scanning. One of these is "exiscan-acl". You need to apply the exiscan-acl patch before you compile exim, but this is already done for you if you build exim from the FreeBSD port. Check this using the -bV flag:

```
# /usr/local/sbin/exim -bV
Exim version 4.43 #0 (FreeBSD 5.3) built 18-Nov-2004 14:16:42
...
Contains exiscan-acl patch revision 28 (c) Tom Kistner [http://duncanthrax.net/exiscan/]
```

Exiscan needs options in the configure file to enable it; until this is done, exim will continue to work just as it did before. To do useful filtering you will need to install SpamAssassin and/or clamav first. The Exiscan documentation is in **doc/exiscan-acl-spec.txt** and **doc/exiscan-acl-examples.txt** in the source directory once you've applied the exiscan patch.

---

3. SpamAssassin

This is a content-based filtering system. Warning: it's written in Perl, and is very CPU-intensive; it can also perform a number of network-based lookups which can take a long time to complete. It may therefore not be suitable for high-volume mail systems. It's also complex to configure well, although the initial installation is easy enough using the ports system:

```
# cd /usr/ports/mail/p5-Mail-SpamAssassin
# make
# make install
# make clean
```

In the directory `/usr/local/share/doc/p5-Mail-SpamAssassin`, files INSTALL and USAGE give more detailled information.

Now you need to create the configuration file, `/usr/local/etc/mail/spamassassin/local.cf`. There was a web-based configuration generator at http://www.yrex.com/spam/spamconfig.php but unfortunately it has not been updated for SpamAssassin-3.x yet. So for now we will do it by hand and disable the most expensive network-based tests:

```
# cd /usr/local/etc/mail/spamassassin
# cp local.cf.sample local.cf
# vi local.cf
... Add the following lines ...
use_dcc 0
use_pyzor 0
use_razor2 0
skip_rbl_checks 1
use_bayes 0
```

Now start the spamassassin daemon:

```
# vi /etc/rc.conf
...
spamd_enable="YES"
# /usr/local/etc/rc.d/sa-spamd.sh start
Starting spamd.
```

You can test it manually using "spamc", a client program which sends mail to spamd for analysis:

```
$ spamc -R
Subject: penis enlargement

Great new pills available!!!!!!!
Ctrl-D
Content analysis details:   (-2.0 points, 5.0 required)

 pts rule name              description
 ---- ----------------------
--------------------------------------------------
 0.0 MISSING_DATE           Missing Date: header
 -2.8 ALL_TRUSTED            Did not pass through any untrusted hosts
  0.8 BODY_ENHANCEMENT2      BODY: Information on getting larger body parts
```

Clearly, there is some additional work to do here; this has been strongly tagged as 'not spam', because it has not been through any 'untrusted' hosts. Type `perldoc Mail::SpamAssassin::Conf` to get the full documentation on this file, and how to set your internal/trusted networks.

Finally, you need to configure exiscan-acl to pass each message to spamd as it is received during the DATA phase, and tag or reject if it's spam. The following additions to /usr/local/etc/exim/configure come from the samples included in the configure file.

```
Add the following line in the top section of the file; a good place would
be next to the existing extry for acl_check_rcpt

acl_smtp_data = acl_check_content

The ports system installs an ACL called acl_check_content in the
section 'begin acl'. You will need to modify it to comment out the
anti-virus section as we don't have that running yet:

acl_check_content:

  # Reject virus infested messages.
#  deny  message = This message contains malware ($malware_name)
#        demime  = *
#        malware = *

  # Always add X-Spam-Score and X-Spam-Report headers, using SA system-wide set
  # (user "nobody"), no matter if over threshold or not.
  warn  message = X-Spam-Score: $spam_score ($spam_bar)
        spam = nobody:true
  warn  message = X-Spam-Report: $spam_report
        spam = nobody:true

  # Add X-Spam-Flag if spam is over system-wide threshold
  warn message = X-Spam-Flag: YES
       spam = nobody

  # Reject spam messages with score over 10, using an extra condition.
  deny  message = This message scored $spam_score points. Congratulations!
        spam = nobody:true
        condition = ${if >{$spam_score_int}{100}{1}{0}}

  # finally accept all the rest
  accept
```

For testing purposes, you can change {100} to {10} in the above condition; this will reject mail with a spam score of 1.0, rather than 10.0. Now test:

```
# /usr/local/sbin/exim -bh 1.2.3.4
mail from:<>
250 Accepted
rcpt to:<username@pcnn.presanog.org.bt>
250 Accepted
data
354 Enter message, ending with "." on a line by itself
Subject: penis enlargement

Dear friend,

Do you have bad credit? Have you been turned down for a mortgage? Would
you like a free cellphone? Place your confidential order now.
This is not spam!!!
.
550 This message scored 1.5 points. Congratulations!
```

If you want to change spam scores in either exim's configure file or local.cf, then remember to restart spamd after editing.

```
# /usr/local/etc/rc.d/sa-spamd.sh restart
```

---

4. ClamAV

The documentation is on-line at http://clamav.sourceforge.net/doc/ and the important thing to note is you need a 'clamav' user and group before starting to compile, and the 'clamav' user must be in the 'mail' group so that it can access spool files. However the ports system, as ever, takes care of this for you.

```
# cd /usr/ports/security/clamav
# make
At this point a dialog box pops up; hit TAB to move to 'OK' then hit ENTER.
# make install
```

Now start the daemons. Note that there are two: one is the actual virus scanner, and the other updates the virus database automatically over the Internet. The configuration files are `/usr/local/etc/clamd.conf` and `/usr/local/etc/freshclam.conf`, but the ports system installs suitable defaults.

```
# vi /etc/rc.conf
...
clamav_clamd_enable="YES"
clamav_freshclam_enable="YES"

# /usr/local/etc/rc.d/clamav-clamd.sh start
Starting clamav_clamd.
# /usr/local/etc/rc.d/clamav-freshclam.sh start
Starting clamav_freshclam.
```

The clamav source directory includes some test virus signatures which you can use to check that the scanner is working correctly; as long as you did not do 'make clean' then those files should still be available inside the 'work' subdirectory.

```
# cd /usr/ports/security/clamav
# cd work/clamav-0.80
# clamdscan
/usr/ports/security/clamav/work/clamav-0.80/test/clam.cab: ClamAV-Test-File FOUND
/usr/ports/security/clamav/work/clamav-0.80/test/clam.exe: ClamAV-Test-File FOUND
/usr/ports/security/clamav/work/clamav-0.80/test/clam.zip: ClamAV-Test-File FOUND
/usr/ports/security/clamav/work/clamav-0.80/test/clam.exe.bz2: ClamAV-Test-File FOUND
/usr/ports/security/clamav/work/clamav-0.80/contrib/clamdwatch/clamdwatch.tar.gz: Eicar-Test-Signature FOU

----------- SCAN SUMMARY -----------
Infected files: 5
Time: 2.962 sec (0 m 2 s)
```

Now to configure exim:

```
# vi /usr/local/etc/exim/configure

Add this line somewhere in the top section
av_scanner = clamd:/var/run/clamav/clamd

Using the spamassassin ACL from earlier, uncomment these lines
which were previously commented out

 deny message = This message contains malware ($malware_name)
      demime   = *
      malware = *
```

To test, you can use one of the test virus-infected files in the 'test' subdirectory of the source - send one to yourself as an attachment. Or you can do this using copy-paste:

```
$ cd /usr/ports/security/clamav
$ cd work/clamav-0.80
$ uuencode test/clam.exe test/clam.exe
begin 644 test/clam.exe
M35I0``(````$``\`__\``+@````A````0``:``````````````````````
... etc
`
end

$ /usr/local/sbin/exim -bh 1.2.3.4
220 noc.t1.ws.afnog.org ESMTP Exim 4.34 Thu, 20 May 2004 10:33:17 +0000
mail from:<>
250 Accepted
rcpt to:<fred@flintstone.org>
250 Accepted
data
354 Enter message, ending with "." on a line by itself
Subject: test

< Paste everything from 'begin' to 'end' in here >
.
550 This message contains malware (ClamAV-Test-File)
LOG: 1CltpX-000Gpu-Cl H=(wombat) [1.2.3.4] F=<> rejected after DATA: This
message contains malware (ClamAV-Test-File)
```