Front-line Spam Defense for Mail Services in Mac OS X 10.4.x / Mac OS X 10.5.x

---

DISCLAIMER: The author(s) claim(s) no responsibility for any damage that may occur from the use of any information found here or found on links followed from this document. The author(s) will take credit for the good stuff though.

All items and/or companies mentioned on this and other pages are or may be trademarks, registered trademarks, or service marks of the respective companies or individuals.

---

1. - Introduction

Mac OS X 10.4.x/10.5.x Mail Services are composed of Postfix, Cyrus, Squirrelmail, Mailman, Amavisd-new, Spamassassin & ClamAV. These components come pre-installed and pre-configured. Unfortunately, the configuration is a very basic one and doesn't take advantage of the underlying power and in some circumstances can even cripple a server's performance.

The purpose of this document is to provide instructions on how to improve the mail services configuration to fight spam more efficiently.

This document will require you to use the command line and a text editor (do NOT use Word). If you do not feel comfortable with using the command line, you should find assistance.

This document is written for Mac OS X 10.4.x/10.5.x. It should apply to 10.3.x as well. Be aware though that I have not done any particular testing of this procedure on 10.3.x.

DISCLAIMER: Whatever you do based on this document, you do it at your own risk! Just in case you haven't understood: Whatever you do based on this document, you do it at your own risk!

This tutorial has been tested on a standard Mac OS X 10.4.x/Mac OS X 10.5.x Server installation. If you have already tinkered with your system, be aware that things might differ. It is impossible to foresee all changes that one might have applied to a server.

2. - Who should change her/his configuration?

On a small system with low-traffic you probably do not care, but on a larger scale this can become a problem. If you have heavy incoming traffic, you should consider optimising your configuration.

You should be comfortable with using terminal.

3. - Fortifying your front-line

One of the foremost configuration issues is that spam and virus detection is done very poorly and relies mainly on SpamAssassin and ClamAV. While both these programs are very good at what they do, they also require a substantial amount of processing power.

Mail is processed first by Postfix, then by Amavisd-new which passes it on to ClamAV and SpamAssassin. This results in a very thorough check against spam and viruses. However, truth is, about 50% (or more) of spam can be detected without the need for specialised software like SpamAssassin. Spam often comes from poorly configured servers, has forged headers and does not stick to the same conventions legitimate mail does. Issues that could be detected by Postfix alone, taking 3 out of 4 components out of the equation, thus reducing processor load substantially.

Postfix, if properly configured, will detect and block a great amount of spam based on the aforementioned criteria. Only mail that can not be clearly marked as "bad mail" will need to be further checked by Amavsid-new, ClamAV and SpamAssassin.

Since I have no idea how your server is configured, I must assume a more or less standard OS X 10.3/4/5.x installation. Don't just replace your configuration with my suggestion, but compare it to your actual configuration and adapt accordingly. You may for example already have certain policies in place which you may want to keep and just extend with my configuration tips.

As mentioned before, we are trying to have Postfix reject "bad" mail as soon as possible in the processing chain. In other words, make sure things like mail for unknown users does not hit the content filter or mail with bad addresses is rejected at the first possible contact with your server.

Note: If you use virtual domains and want to reject mail for unknown users before it reaches the content filter you will need to start using postfix style virtual aliases. A tutorial on this topic is available here: http://osx.topicdesk.com/

The following configuration is a suggestion based on experience. A lot more could be done, but my aim is to block as much spam as

possible without risking any legitimate mail being blocked. "If in doubt, let it through". After all, there is still SpamAssassin waiting to be called if needed.

Some may object there is some redundancy. However, once Postfix determines a message needs to be rejected, subsequent checks will not take place. Better be safe than sorry. Everything is listed in the order it's being actually processed by Postfix.

Now let's implement the "front-line" checks for Postfix:

NOTE: Make sure Server Admin is closed while you manually edit the configuration files. Also, make a backup of /etc/postfix/main.cf first!

Edit /etc/postfix/main.cf and add/modify (Lines wrapping without line spacing are a single continuous line):

```
disable_vrfy_command = yes

smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks,
reject_rbl_client zen.spamhaus.org, permit
```

(Above entry will check connecting clients/servers against blacklists)

```
smtpd_helo_required = yes

smtpd_helo_restrictions = permit_sasl_authenticated, permit_mynetworks,
check_helo_access hash:/etc/postfix/helo_access, reject_non_fqdn_hostname,
reject_invalid_hostname, permit
```

(Above entry will check connecting clients/servers for properly formed host-names and against faking your own domain or IP number. To work it also needs the following file (/etc/postfix/helo_access) to be created.)

```
Contents of /etc/postfix/helo_access
xxx.yyy.zzz.xxx REJECT  You are not me.
mydomain.com   REJECT  You are not me.
```

(Replace xxx.yyy.zzz.xxx with your mail server's IP number and replace mydomain.com with your domain name. If you have more than one domain name, add extra lines. Hash files must be "postmapped".
To do so issue "`sudo postmap /etc/postfix/helo_access`" after you create/modify it.)

```
smtpd_sender_restrictions = permit_sasl_authenticated, permit_mynetworks,
reject_non_fqdn_sender, permit
```
(Above entry will check if sender address is properly formed)

```
smtpd_recipient_restrictions = reject_invalid_hostname,
reject_non_fqdn_sender, reject_non_fqdn_recipient,
permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination,
reject_unlisted_recipient, reject_rbl_client zen.spamhaus.org, permit
```
(Above entry will check if recipient address is properly formed and not present in a blacklist)

```
smtpd_data_restrictions = permit_mynetworks, reject_unauth_pipelining,
permit
```
(Above entry will block a data sending technique often used by spammers)

That's it. When done, issue "`sudo postfix reload`" and enjoy.

More information can be found here:
http://www.postfix.org/postconf.5.html
http://www.postfix.org/uce.html

4. - Caveats

The more changes you manually make in /etc/postfix/main.cf the more you increase chances of Server Admin not staying in sync. As a general rule of thumb, once you start advanced configuration of mail services avoid using Server Admin. If you must, make sure you have a backup of /etc/postfix/main.cf first.

There are a couple of parameters in main.cf, which can nullify part of the desired blocks.

-Check to see if you have "`local_recipient_maps =`" in main.cf. If you have and it's empty, either remove it or replace it with "`local_recipient_maps = proxy:unix:passwd.byname $alias_maps`"

Avoid having a catchall address ("`luser_relay`"). It is pointless as 99% of mail to unknown users is spam anyway. Legit mail that wasn't properly addressed should bounce so the sender knows.

That's all folks.
Hope this helps.
Have fun,
Alex

Doc. Version 1.3, 26.10.2007
Athanasios Alexandrides
Lugano, Switzerland
tutorials -at- topicdesk.com

Content contributions:
-
