



## Release of MailXServer 4.1a

Release 4.1a is a complete rebuild of MailXServer on the Red Hat Enterprise Linux 4 (RHEL4) platform. This will ensure a life span without requiring a system rebuild up to 2010, allowing for Linux security updates during this period.

In addition version 4.1a of MailXServer specifically focused on spam prevention. In the test environment, that currently handles around 30000 emails per day, spam was virtually eliminated.

1. **Global Rules→Graylist Settings (& Graylist Delay Pool & Graylist Whitelist)**  
Added support for gray listing. Currently gray listing is arguably the most effective spam stopping method available. All valid email servers must comply with the RFC 821 standard. In the RFC 821 it is specified that when an email server is not available or mail is temporarily failed the sending server should retry mail delivery. Due to the huge amount of emails a spam server needs to deliver it normally uses a fire once method for mail delivery, not retrying delivery of email.

When gray listing is enabled it will temporarily fail (tempfail) all new incoming email messages for a fixed period of time. If the same message is received after the tempfail time expired the message will be allowed and white listed for a fixed period. The suggested whitelist time should be around 40 days.

### Disadvantages of grey listing

- a. Unless the relay server is statically white listed the first valid email from a specific host will be delayed, for a short period, every 40 days (depending on your settings).
- b. When grey listing is widely used, spammers will adapt (with cost and time implications)

### Advantages of grey listing

- a. Amazing results stopping spam with no valid emails dropped.
- b. Places a burden on spammers, especially if they need to adapt.
- c. It is relatively transparent.

2. **Global Rules→Edit Static Server Blacklist & Whitelist**

When email is received the following tests are done before the data part of the message is delivered:

- RBL
- SPF
- FL (Forward email lookup)
- Graylist

If a sending server is statically blacklisted the email will be dropped without doing any tests.

If the server is statically whitelisted all above tests will be skipped except for the Forward Lookup test.

\*NOTE: The Static RBL Whitelist & Blacklist settings where replaced with the above.

3. **Global Rules→Custom Spam Rules**

Custom rules can be created as a very powerful way to stop specific spam. Rules can be defined as body, header, URI or raw body rules. Body rules will only search the body of an email while header rules will analyze the header fields. The raw body rule will search the complete message in raw format. URI rules should be used to detect blacklisted websites.

Regular expressions are used to detect rule hits in a message. Simplified rules can automatically be created using the supplied interface. Power users can modify (update) the created rules using regular expressions.

4. **Global Rules→Custom Spam Scores**

All scores assigned to spam rules can be modified using this feature.

5. **Global Rules→General Settings**

Added support for Bayes spam filtering. Using Bayes the filter has the ability to learn spam and ham and score the email accordingly. Bayes can be taught manually or automatically.

6. Added support for SURBL scanning

SURBL will search the body of an email message for references to know spam website links. By default a score of 4 will be added to the spam score is the rule is triggered. The score can be changed using the Custom Spam Score option.

7. Added support to add HTML disclaimers to an email message.