Release notes for MailXServer 4.4a

MailXServer 4.4a is available for online update. The following new features are included:

1. **Firewall Rules**:

   Rules → Firewall Rules

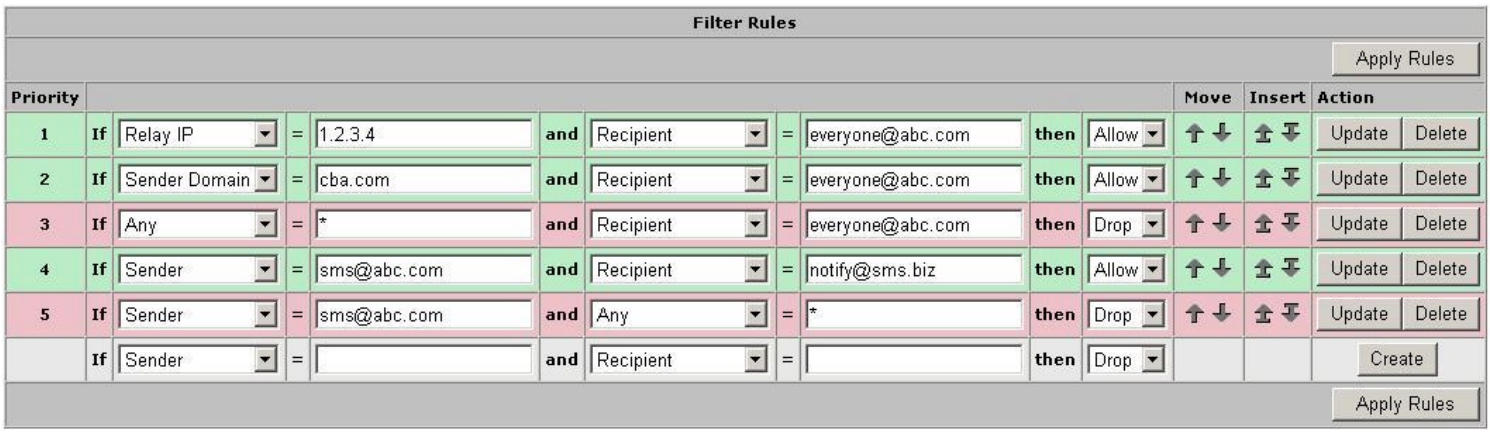
   The e-mail firewall can allow or deny any message based on Relay IP, sender, recipients, sender domain and recipient domain. Incoming and outgoing e-mail will be tested against the rule set before any other testing is done. To save bandwidth, messages will be rejected before the data part of the e-mail is received. The firewall uses a very powerful algorithm to ensure that even a large number of rules (thousands) will have very little impact on server performance.

   The recipients of messages will be tested separately. This will ensure that if multiple recipients receive an e-mail the mail will only be denied for specified users. The sender of the e-mail will receive a single delivery failure message with the rejected recipients listed.

   Rules will always be executed from top to bottom. When a rule match is made no further firewall testing is done and the relevant action is executed against the e-mail. If no rule is supplied or no match is made the default action is to allow the email.

   If possible always try to use the Replay IP as the source of a rule instead of the sender, since it is far more difficult for malicious users to fake an IP address.

   Example: Your company abc.com has a distribution e-mail address named everyone@abc.com. You only want to allow users on your local server with IP 1.2.3.4 and a partner company with e-mail domain cba.com to send e-mail to the everyone@abc.com address. You also have a SMS warning account (sms@abc.com) that is not allowed to send e-mail to anyone, but notify@sms.biz. All other e-mail must pass the firewall rules. The rules for above scenario are as follows:



2. E-mail Proxy Server

Rules → Create New Rule, Rules → Edit Sender Rules, Rules → Edit Recipient Rules, Rules → Group Management

The proxy server can be used to save internet bandwidth by removing attachments bigger that a specified size from the e-mail and replacing it with a URL. If used in conjunction with HTTP proxies (like squid) it can have a huge impact on bandwidth depending on the organization structure.

The same attachment will not use up duplicate storage space on the web (URL) server even if it has a different attachment name. The attachments will automatically be deleted once the specified expiry date is reached. Once a duplicate attachment is received the expiry date will be updated. E-mail proxy rules forms part of the general MailXServer rule set, which means that different settings can be applied to different rules.

The recipient of an e-mail with a removed attachment will receive a message at the bottom of the e-mail similar to this:

```
The attachment was larger than 100000 bytes.
It was removed, but may be accessed at this URL:

https://server.domain.com/proxy/7418668b657d6e1f795b717b71d6a85cc4f22517/Eng2006.pdf
The attachment will be deleted within 10 days
```

3. E-mail Audit Log

Reports → View Log DB, Reports → Query Wizard

E-mail audit logging will ensure that the e-mail administrator can trace exactly what happed to an e-mail. The log will for example clearly show if an e-mail was placed in the Hold Queue, if it was denied or temporarily denied by the remote server, if it was delivered successfully, etc.

The log will be processed every night when the daily script is run. You can update the log manually during the day, but it can create slight inconsistencies in the report graphs.

An example of the audit log:

id	Date	Audit Trail
3371607	2006-11-27 13:56:45	Milter: to=<user@abc.co.za>, reject=554 5.7.1 E-mail firewall rules determined that sender@pqz.com is not allowed to send e-mail to user@abc.co.za.
3371608	2006-11-27 13:56:46	from=<sender@pqz.com>, size=744970, class=0, nrcpts=1, msgid=<H000491d013ac199.1164628604.pqz.com@MHS>, proto=ESMTP, daemon=MTA, relay=sendcomp.com [192.168.1.120]
3371609	2006-11-27 13:56:46	USER SEND,,,<sender@pqz.com>,<user@xyz.com>,Demo on Audit Log
3371610	2006-11-27 13:56:47	replace_with_warning=1 sm_quarantine=1
3371611	2006-11-27	Milter change (add): header: X-MXID: kARBujj2012401

	13:56:47	
3371612	2006-11-27 13:56:47	Milter add: header: X-Spam-Score: Not Checked - Size exceeded
3371613	2006-11-27 13:56:47	milter=mimedefang, quarantine=Default
3371614	2006-11-27 13:56:47	Milter change: header Content-Type: from multipart/mixed;~n~tboundary=~scalix-part-00591d6e0c=_01~ to multipart/mixed;~n~tboundary=~scalix-part-00591d6e0c=_01~
3371615	2006-11-27 13:56:47	Milter change: header MIME-Version: from 1.0 to 1.0
3371616	2006-11-27 13:56:47	Milter message: body replaced
3371617	2006-11-27 13:56:47	Milter add: header: X-Scanned-By: MailXServer-v4.4a on 192.168.1.121
3371618	2006-11-27 13:56:47	to=<user@xyz.com>, delay=00:00:02, mailer=esmtp, pri=774970, quarantine=Default, **stat=** Hold Queue
3371719	2006-11-27 13:58:05	to=<user@xyz.com>, delay=00:01:20, xdelay=00:00:21, mailer=esmtp, pri=864970, relay=imx01.xyz.com [10.10.10.1], **dsn=** 2.0.0, **stat=** Sent (174040933 message accepted for delivery)

This example clearly illustrates that a user sender@pqz.com send an e-mail to two users nl. user@abc.co.za and user@xyz.com. The e-mail to user user@abc.co.za was immediately rejected by the MailXServer firewall rules. The e-mail of user user@xyz.com was placed in the hold queue. The e-mail was released from the hold queue and was successfully received by server imx01.xyz.com

4. Bayes Database Spam Teaching

Reports → View Log DB, Reports → Query Wizard

Bayes is a result in probability theory, which relates the conditional and marginal probability distributions of random variables. MailXServer uses the Bayes theorem as a spam detection method. The server however needs to understand what spam is. To allow the server to learn spam a setting can be enabled per rule basis to save e-mail that passes the normal spam rules to the local MailXServer file system in encrypted format. Only e-mail that is smaller than the allowed scan spam size will be saved. Normally this will only be enabled for receiving rules. When complaints about spam bypassing the system are received the administrator can learn message as spam by manually clicking on the "Learn as Spam" button in the mail log. It is crucial that the Bayes database is trained ONLY on spam and not ham.

5. Server Health Monitor

Tools → Monitor

The server health monitor was updated with a virus scanner test and database health test. If a fault in the database or a fault in the virus

scanner is detected the administrator can be notified by e-mail and the server can be shutdown. By default these tests are disabled.

6. New Top Entries

Reports → Top Entries

The following new Top Entries was added:

- Sender Domain – To display the top sending domains
- Recipient Domain – To display the top recipient domains
- Sender E-mail Size – To order senders not by e-mail count, but by total e-mail size send.
- Unique recipients – To display the e-mail count of unique recipients
- Unique recipient domain - To display the unique top recipient domains
- Recipient e-mail size - To order recipients not by e-mail count, but by total e-mail size received.

These new queries will only be available in the current e-mail database and subsequent cycled databases, but NOT in old cycled databases.

7. Other

Some other changes include:

- Update to newest release of Sendmail.
- Update filter rules and e-mail scan engine.
- Speed up top entries and database queries.
- Fixed bug to allow for special characters (like ü) to be inserted into the disclaimer by the GUI.
- Added rights to control if users can see the Server Status on authentication.
- Allow for drill downs on Top Enties in cycled databases.
- Fixed bug to allow whitelisting and blacklisting of a x.0.0.x ip range.
- Support for the external perl module FileScan was removed, since it is full of bugs.