MailXServer

Securing your E-mail

Complete email management and security solution

Overview

Email has changed the way we communicate. It increases productivity, saves cost and has become an integral part of business. However, the masses of Email messages, viruses, unsolicited Email, legislation and policy regulation has forced us to start managing electronic communication in a more comprehensive way.

MailXServer can act as a stand-alone Email system or can seamlessly be incorporated into any existing environment as a gateway Email security and management system. The server is compatible with any SMTP server including GroupWise, Microsoft Exchange, Lotus Domino, Mercury and Sendmail.

Unlike many other systems, MailXServer is a complete Email management and security tool. It supervises and controls Emails, and records a complete audit trail of messages passing through the server.

Key Benefits:

- Stops security threats at the gateway before any damage is caused.
- Assists with legal compliance to company and government regulations.
- Drastically reduces internet bandwidth and costs.
- Reduces Email administration time and resources.
- Improves employee productivity.
- Accurate usage reporting and logging for multiple Email systems in one place.
- Individual user access to specified pages and rules.

Legal Compliance

Management of Email is not only a crucial part of business to ensure employee productivity, but is also a legal issue. Many countries are implementing electronic communication regulations. Organizations can be faced with costly lawsuits due to offensive material, no proof of Email transactions or the lack of disclaimers. MailXServer can assist companies in adhering to these regulations by allowing header logging of all Email messages, archiving specific or all Email messages, blocking of offensive material and, the attachment of Email legal disclaimers to outgoing Emails.

Improves efficiency

MailXServer includes the most advanced spam and blocking capabilities of malformed Email. Many of the methods employed will stop spam before the data part of the message is received. The rejection of these messages drastically reduces usage of internet bandwidth, improving employee productivity and reducing costly IT support time.

Up to three concurrent virus scanners can be used to block or quarantine virus-infected Emails. Specified attachments can also be blocked to ensure even higher security. This drastically reduces the risk of downtime due to malicious Email attacks.

IT helpdesk support time is reduced due to the single point of management for multiple Email systems. Individual users can be granted limited rights to manage their own rules or domains.

Reporting

Multiple reports can be generated to ensure that the system administrator or delegated individual can ascertain by quick overview any system performance or irregularities.

User Access

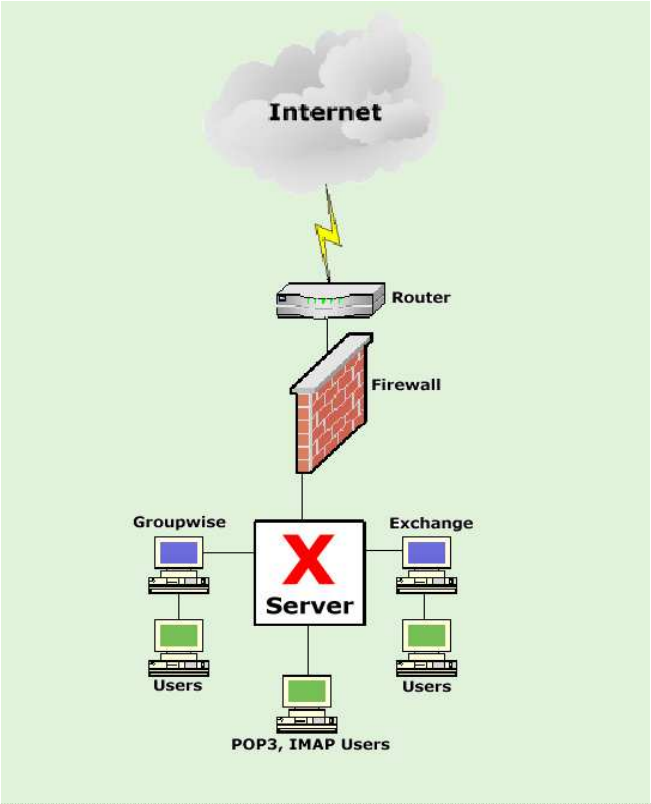
Individual users can be assigned specific page and rule rights to allow management of their own content and rules. Rules can be assigned to both Email addresses and domains. Using this feature, ISP's can assign relevant management rights to customer domains.

MailXServer

Detailed Features

- The Server can handle **multiple domains and/or Email addresses** (called rules), each with their own set of rules for incoming and outgoing Emails. Rules can be added for internal or external users or domains.
- Groups can be created with unlimited members. Every group will have a configured domain connected to the group. Multiple groups can share the same domain, allowing the creation of feature specific groups. The group domain can be any local or external domain.
- Set the Email size limit per rule.
- The **Recording** of message headers for incoming and outgoing Email can be enabled and logged in a database, ensuring a complete audit trail.
- The server will automatically check on a daily basis if new spam rules are available and update the server accordingly.
- Intelligent **Spam filtering** can be enabled. Mail classified as Spam is discarded or quarantined. The weight of the spam filter can be configured per rule.
- **Bayes** spam filtering can be enabled to allow for automatic or manual learning of spam or ham.
- Powerful custom "regular expression" spam rules can be created to enhance spam filtering.
- Custom scores can be assigned to existing rules.
- ***Static relay **whitelist or blacklist** entries can be specified.
- ***Support for multiple RBL** (real-time block list) databases. A specific weight can be specified for every individual RBL database. If the sum of the weights are bigger than the specified threshold the mail will be rejected. To increase server performance **RBL queries can be temporarily cached**.
- **Support for SURBL** databases. SURBL's will score a message on known spam Uri's in the body of the message.
- *Comprehensive **Graylist testing** can be enabled with complete control over time settings. Graylisting is arguably the most effective anti-spam technique. Entries in the Graylist Delay pool can be manually placed in the Graylist Whitelist.
- ***SPF** (sender policy framework) **testing** can be enabled, ensuring the legitimacy of senders. To increase server performance, **SPF queries can be temporarily cached.**
- ***Email address forward lookup** can be enabled to test for valid recipients before accepting Email and the ability to do forward lookups for valid recipients on flat text files.
- **Disclaimer insertion** on all outgoing Email messages. This signature is unique per rule and can be inserted at the bottom or top of an Email. The disclaimer can be in HTML, text or text attachment format. Email addresses for recipients can be defined to not receive disclaimers.

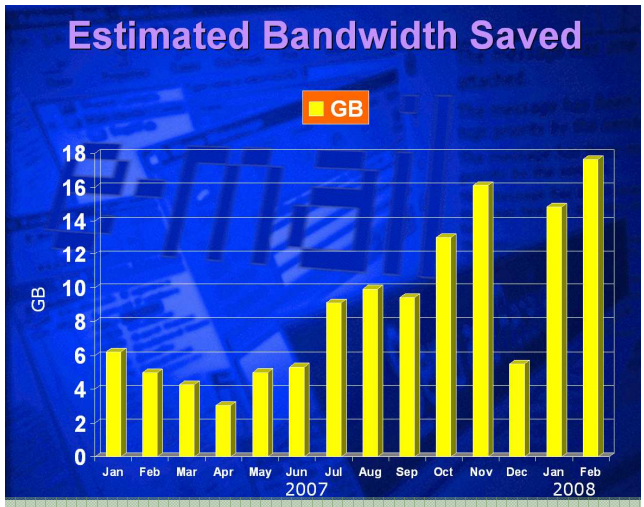
** Email will be rejected before the data part of the message is received, saving internet bandwidth and cost.*



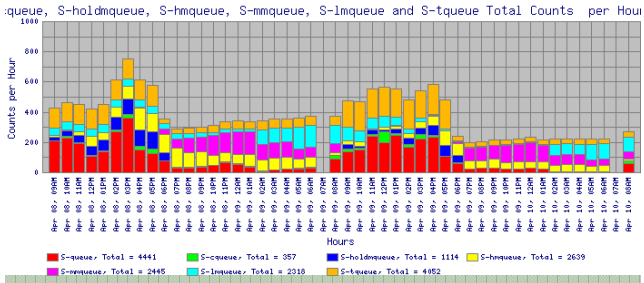
Typical network connection using MailXServer in a mixed environment.

- **Duplication or archiving** of complete Email messages per rule basis can be enabled. The archiving process will be completely transparent to the recipients of the Email.
- All messages can be **scanned for known viruses and Trojans** using multiple, updated virus scanners**.** Infected attachments can be dropped or quarantined. Only infected body parts will be stripped from the message. Notifications can be generated for the sender, recipients and administrator. Viruses that generate fake headers can be blocked without notification.
- **Mime attachments can be blocked** per extension type. This is configurable per rule basis on both send and receive rules.
- The **MIME type of a file will remain the same** even if users rename the file extension.
- Emails can be **blocked**, per rule base, **based on subject** for both sending and receiving rules.
- Emails can be **blocked** based on source **domain or Email address**, e.g. baddomain.com or baduser@baddomain.com
- All suspect or illegal mail can be quarantined. **Quarantined mail can be released** by the administrator or authorized users at any time either to the original recipient or another recipient. Email messages can be released via a link from administrator quarantine notification Email messages. The release page will also state the reason why the message was quarantined.

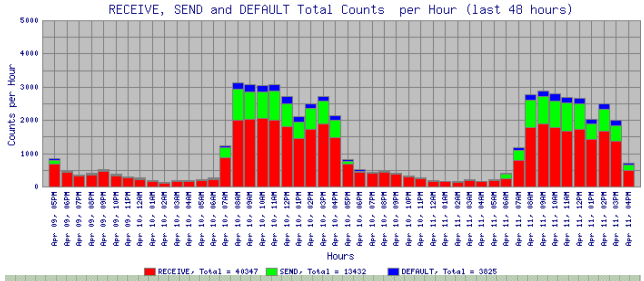
- **Users** can be assigned **rights** to manage their own rules. Multiple rules can be assigned to a single user.
- **Rights to individual management pages** can be assigned to users allowing for unique rights per user as required.
- **Built-in reports** can be generated summarizing spam, viruses, top senders, top entries, and recipients to name a few.
- Generate summary reports with custom senders or recipients. A report can now be generated for any user, group or domain.
- Graphs are generated for hourly, daily and monthly statistics. Dynamic graphs can also be generated.
- Automatically executed scripts at user defined times, containing the relevant procedures to ensure the stable running of MailXServer.
- The **query wizard** feature allows for quick extraction of relevant records from the database. Top entry queries can be generated on a cycled database.
- **Multiple queues with different priority settings** are available to lessen the load on MailXServer. The Mail Queue will ensure that email that cannot be delivered will automatically be moved down the priority queue scale according to configured delivery failure values. Email that fails to be delivered after an amount of time will be moved to the Trash Queue. Warning messages from the MailXServer will be placed in the Client Mail Queue, and emails that can be delivered at a later stage are placed in the Hold Queue.
- Messages in the **Email queue can be managed**, allowing for the release or deleting of individual messages or multiple selected messages.
- Support for **Domain Masquerading**. This allows you to make all outgoing messages appear to be from the same domain.
- Full **Domain Routing** support.
- **Domain Mapping** support. This feature allows you to remap all To and From addresses for a domain to another domain.
- ESMTP support can block **oversized messages** before the data part is received.
- Full **POP3 and IMAP** support for stand-alone use.
- The **management console is web based**, allowing management from anywhere.
- Server operation settings like Early Rejection filter, Minimum/Maximum slaves, Busy/Idle timeout, Slave Startup delay, Local Host Connections, Log Events and Multiplexer Queue Size/Timeout can be **configured through a GUI**.
- The MailXServer can be **configured to do basic monitoring functions** like Server load and Disk Space and, sending an Email to a configured address to warn the administrator of any possible problems.
- **Firewall rules** can allow or deny any message based on Relay IP, sender, recipients, sender domain and recipient domain. Incoming and outgoing Email will be tested against the rule set before any other testing is done.
- The **Email Proxy Server can be used to save internet bandwidth** by removing attachments larger that a specified size from the Email and replacing with a URL that can be accessed by the recipient.
- The **Email Detail Audit Log** will ensure that the Email administrator can trace exactly what happed to an Email. The log will for example clearly show if an Email was placed in the Hold Queue, if it was denied or temporarily denied by the remote server, if it was delivered successfully, etc.
- **XUsers** is an completely separate interface to allow normal Email users to view quarantined Email, view audit reports, release and analyse Email with limited rights. User Authentication can be done on a MailXServer or via a LDAP Service.



Actual results from a MailXServer customer



Example: Graph of Mail Priority Queues



Example: Graph of Mails Send and Received

MailXServer

Specifications

Proven Reliability and Scalability

- Built on robust industry standard architectures
- Scales up and down for large, medium or small enterprises
- RAID level disk redundancy
- Online file level Linux backups
- 99.99%+ uptime
- Leverages Linux platform advantages: flexible, reliable and scalable
- High performance mail routing
- Scalable local Linux Email store supporting thousands of users per server

Compliance to Standards

- SMTP/ESMTP
- POP3
- IMAP
- MIME
- HTTP/HTTPS
- RFC 821
- RFC 822
- TCP/IP

Server System Requirements

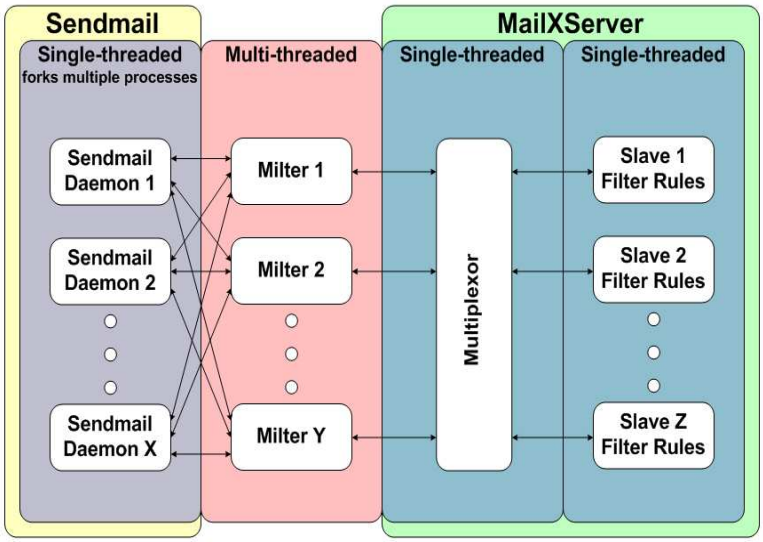
Minimum Hardware

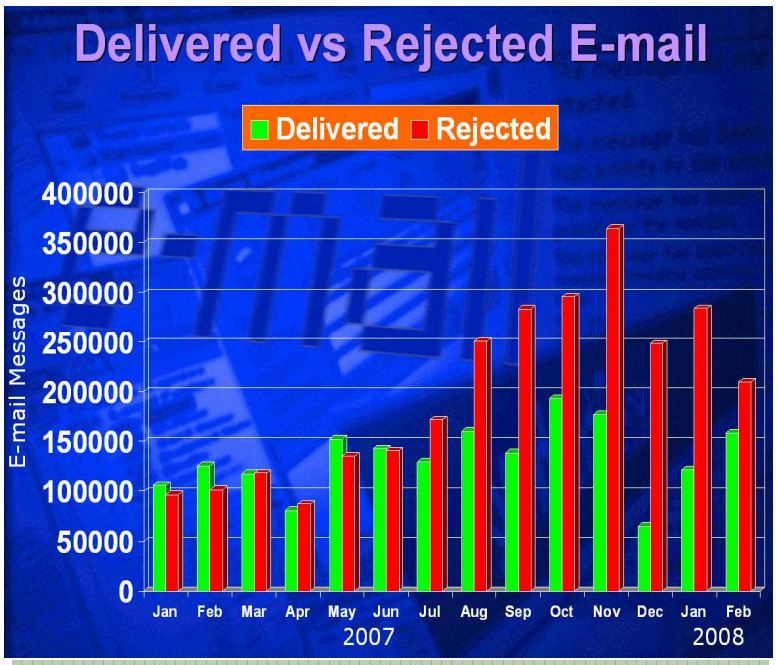
- Pentium 3GHz
- 2 GB RAM
- 80 GB HDD

Software

- Redhat Linux AS,ES 4 (RHEL4)
- Centos Linux 4
- Sendmail 8.14.1
- PHP
- Apache 2
- MySQL or other ADO compliant database

Architecture





Actual results from a MailXServer customer

Contacts:

URL: http://www.mailxserver.com
Email: mailx@mailxserver.com

Support and Distributed by:

NETWORK & COMPUTING CONSULTANTS

Url: http://www.ncc.co.za
Tel: 0861-555444 / +27(0)51-4478589 / +27(0)11-2588740