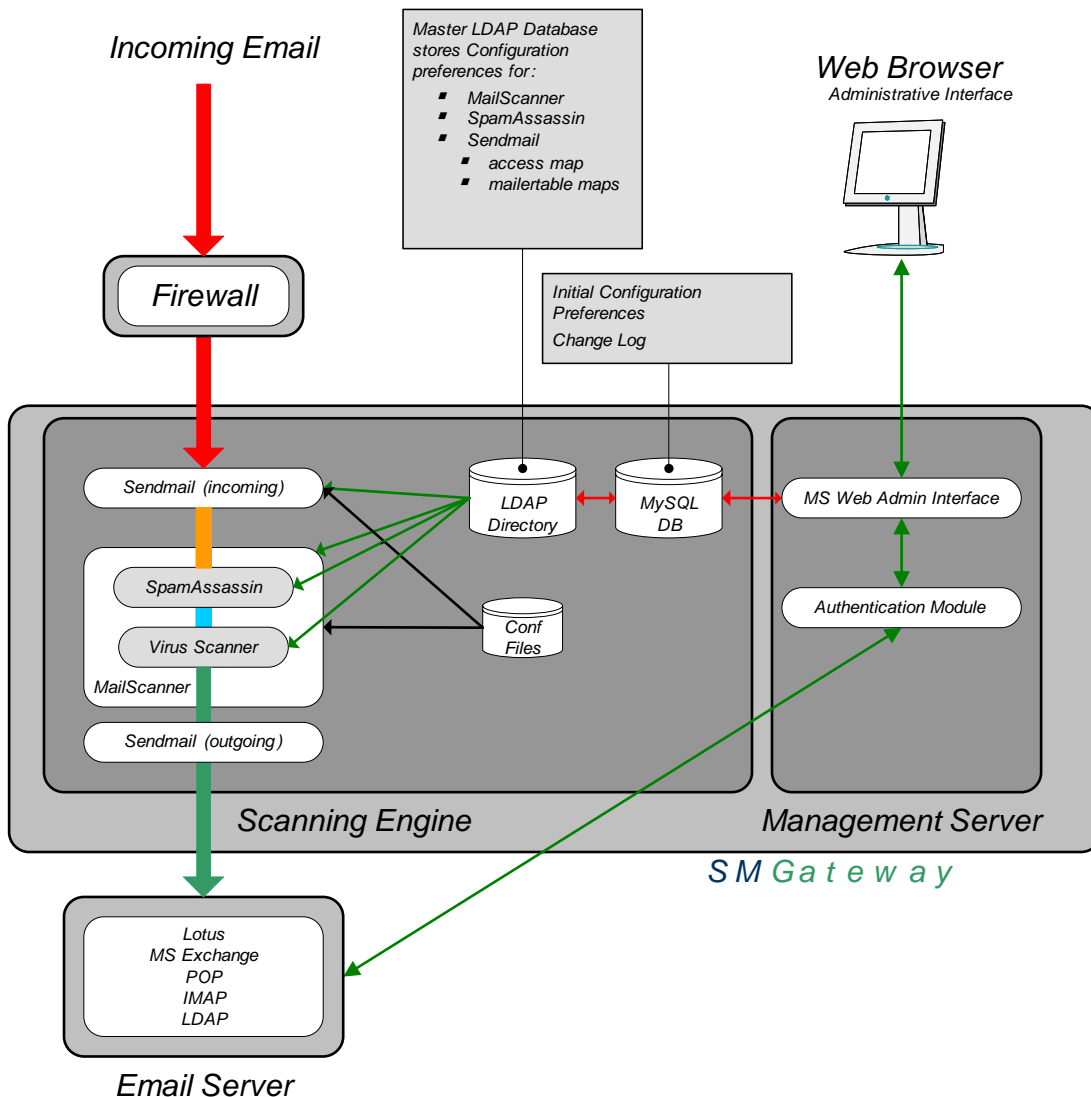


# Fort Systems DefenderMX Architecture Diagram

A typical DefenderMX Installation consists of:

- A Firewall configured to pass all email traffic through to the email gateway
- The DefenderMX which is configured to scan all email for security breaches, viruses and mark spam and the pass the email to an email server
- An Email Server which receives the sanitized email and stores or forwards the email to the user's email program.
- A web interface for configuring DefenderMX and real-time monitoring of email traffic and processing.



Most often the **DefenderMX** is simply installed between an existing firewall and email server. After the **DefenderMX** is installed, configured and tested, the DNS Mail Exchanger (MX) record(s) for the existing email server are changed to point to the IP address of the new **DefenderMX**. Mail will then start flowing to the **DefenderMX** and after scanning, will be forwarded to the existing email gateway.

## Fort Systems Ltd. **DefenderMX** Scanning Engine

The Scanning engine initiates email scanning by starting two instances of sendmail. The first sendmail instance is started in daemon mode to accept incoming email. Email is accepted and simply delivered to an incoming queue directory. The second sendmail instance is also started in daemon mode and watches an outgoing queue directory for scanned and processed messages that need to be delivered.

To accomplish these scanning and processing tasks, **DefenderMX** starts a configurable number of MailScanner child processes. Typically there are five child processes which examine the incoming queue at five second intervals and select a number of the oldest messages in the queue for batch processing. The number of child processes and the time interval between them is configurable and is dependent on the gateway system's speed, memory, number of processors and other application loading.

Once a MailScanner child process has found a batch of emails in the incoming queue, it first runs a series of Real-time Black List (RBL) tests on each message. If the IP address of the sender matches a definable number of RBLs, the message may be marked as definitely spam and no further tests are performed to processing time. If the message passes the MailScanner RBL tests it is passed to SpamAssassin which uses heuristic, Bayesian and other tests to determine the spam level of the message (see Figure 2)

SpamAssassin actually assigns a numerical value to each test that is used on the message. SpamAssassin also examines the site specific white lists (not spam) and black lists (is spam). If the sender, system or domain of the message sender is on either list, a very high (black list), or very low (negative score) is assigned to the message. SpamAssassin calculates the final spam score for each message at the end of these tests.

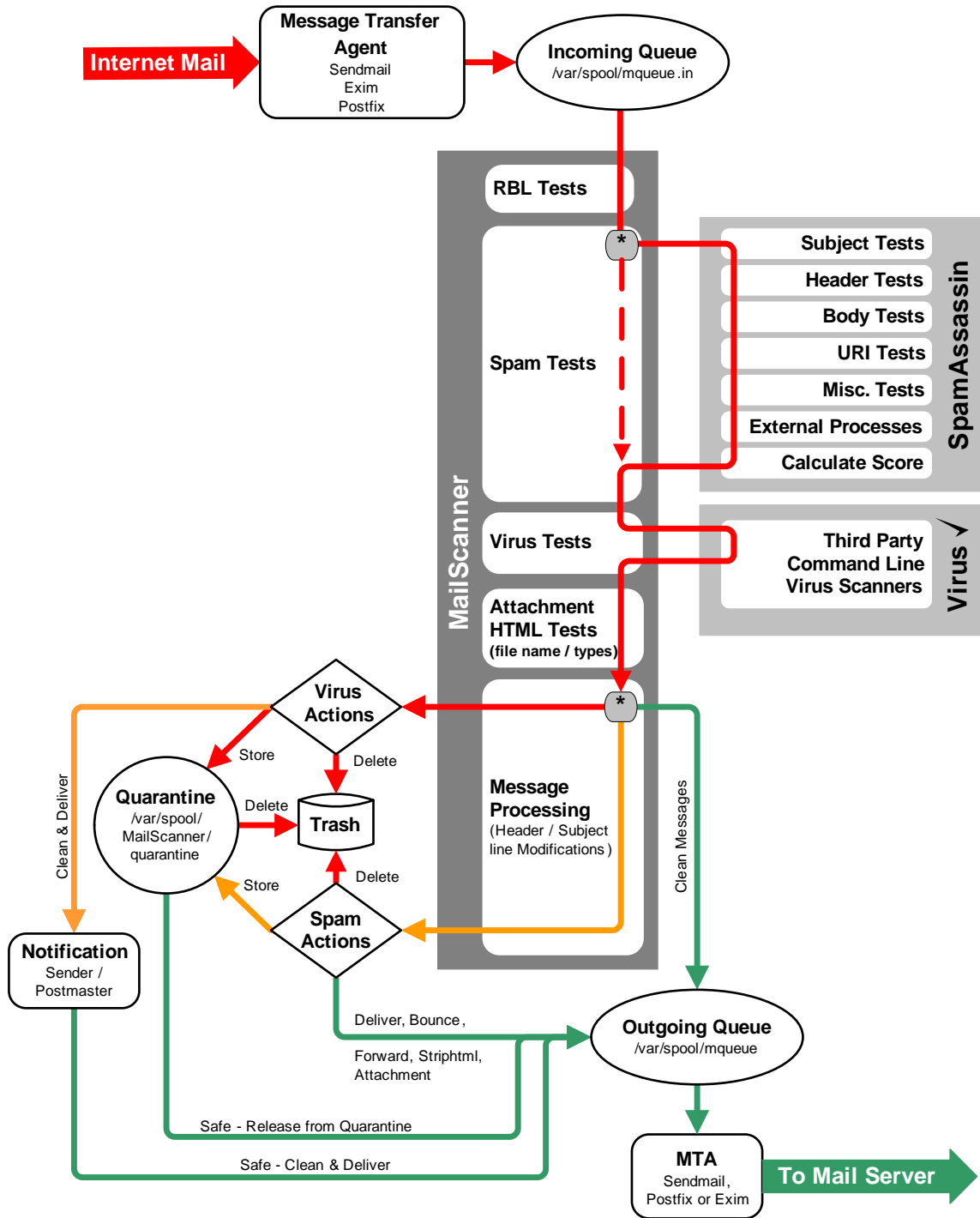


Figure 2

DefenderMX may be configured to use one or more of seventeen commercial or open source virus scanners. If a virus is detected at this point, the message is marked as containing a virus.

Once virus detection is complete, the MailScanner child process examines the filename and file types of any email attachments against site configurable rule sets. Virtually any type or name of attachments can be blocked or passed depending on how MailScanner has been configured. The message is also scanned to see if the body contains possibly dangerous HTML content such as:

- IFrame tags
- <Form> tags
- <Object Codebase=...> tags

Configurable options allow logging, passing, deleting or disarming these HTML content tags.

After this stage of the processing, DefenderMX has all the information needed to modify, deliver, reject or quarantine the message. This final message processing depends on the message content and the DefenderMX configuration settings.

If a virus is detected, DefenderMX can send (or not send):

- A customized message to the sender of the virus
- A customized message to the recipient of the virus
- The disarmed and sanitized message to the recipient
- The message and the virus to quarantine

Every message has now received a “spam score”. DefenderMX can be configured to discern between different levels spam cores:

- Not spam, i.e. spam score < 5
- Spam, i.e. spam score =>5 and <= 10
- High spam, i.e. spam score > 10

For each of the not spam or spam levels listed above, DefenderMX can perform any combination of the following options:

- Delete - delete the message
- Store - store the message in the quarantine
- Bounce - send a rejection message back to the sender
- Forward user@domain.com - forward a copy of the message to user@domain.com
- Strip HTML - convert all in-line HTML content to plain text.

- Attachment - Convert the original message into an attachment of the message.
- Deliver - deliver the message as normal

All mail or mail to specific recipients or domains may also be archived.

These options (and most other message processing options) are configurable by the To: or From: address for specific domains, senders or recipients. Spam and virus detection may be turned on or off depending on the To: or From: address of specific domains, senders or recipients. This granularity is accomplished using simple Rulesets.

Many other alterations may be made to individual messages depending on the site's preferences:

- Various levels and types of spam scores may be added to the header of the message
- Customizable "X-" style messages may be added to the header of the message
- Subject: lines may be customized depending on Virus, attachment or spam score detected
- Messages may be signed with site customized footers
- Reports to administrators, senders and recipients may be customized (standard reports are available in fifteen different languages)

DefenderMX also provides the additional features and functions required for ease of email gateway administration and maintenance:

- Sensible defaults for most sites
- Automated updating of virus definitions for all supported virus scanning engines
- Configurable cleaning options for quarantined messages
- Very simple application updating