

BarricadeMX

Overview

BarricadeMX is a new light weight, small footprint computer-based anti-spam application available. The development of BarricadeMX development started when Anthony Howe¹ and Steve Freegard² with assistance from Julian Field³, started studying the behavior of the compromised systems (bots) that send out the majority of spam. Trend Micro estimates there are 70 million subverted computers worldwide and that 8 million to 9 million are used to send spam in a given month⁴. Using the Fort System Ltd. live spam trap, they developed techniques to analyze, in detail, the Mail Transfer Agent (MTA) connection between the bots and other spammer systems and the receiving MTA. The result of this analysis enabled them to develop techniques that are extremely effective in determining that an incoming email is spam well before the bulk of the message is accepted for delivery.

BarricadeMX is designed to sit in front of one or more Mail Transfer Agents on SMTP port 25. It acts as a proxy, filtering and forwarding mail to one or more MTAs, which can be on the same server or different servers. BarricadeMX supports a variety of well blended anti-spam filtering techniques that can be individually enabled or disabled according to the rigors of the postmaster's local filtering policy. Some of the tests available are:

- ClamAV anti-virus support
- "Client-Is-MX" heuristics for PTR and IP in name checks
- Concurrent connection limits
- Connection rate throttling
- DNS real-time blacklists
- Drop on N bad SMTP commands
- Enhanced grey-listing (patent pending)
- HELO claims to be us
- Local black/white list by IP, host name, domain, MAIL, RCPT
- Message limit controls
- Message size controls
- Recipient verification using call-ahead
- Sender verification using call-back
- SIQ protocol support for reputation services
- SMTP command & greet pause
- SpamAssassin anti-spam support
- SPF Classic support
- Tar pitting negative SMTP responses
- URI blacklist test of PTR & HELO
- URI blacklist testing of message content
- White wash & backscatter prevention using RET-ID (patent pending)

Most tests are optional and many are configurable by Domain

If the existing receiving MTA is running on the same system as BarricadeMX, the existing MTA is simply reconfigured to listen for messages on another port, typically port 26. If BarricadeMX is running as a standalone email gateway it can be configured to connect to the receiving MTA on another system.

BarricadeMX can be simply configured to route mail for individual domains to different port and other systems. BarricadeMX also supports both IPv4 and IPv6 routing and addressing.

BarricadeMX may be configured to run on multiple gateways which share multicast or unicast cache. This cache provides a fast, simple, and efficient means to share cache updates across the multiple gateways on the same network segment or to a set of remote hosts. Both the multicast and unicast caches use a broadcast-and-correct model and support IPv4 and IPv6.

By using an independent SMTP pre-filter in the form of a proxy BarricadeMX avoid portability differences and limitations of MTA extension methods (milters, plugins, rule sets, etc.) and can more tightly couple & integrate certain tests to improve performance and message throughput. It may be configured to run as a proxy for any MTA, Sendmail, Postfix, Exim, Qmail, etc. This allows BarricadeMX to be used in front of any existing anti-spam application to enhance spam detection and reduce loads on existing mail servers, gateways and mail hubs.

Efficiency

BarricadeMX is a small (4 MB resident memory), lightweight, multi-threaded C program that is much more efficient than the typical MTA so it can gracefully handle many more simultaneous incoming connections. A single CPU system has been seen to handle over 600 concurrent MTA connections without failing. Many servers that are in production routinely handle 60 to 70 incoming simultaneous connection without the load on the system exceeding 3.0.

BarricadeMX case study

This case study is based on a real life implementation of BarricadeMX. Before installing BarricadeMX five gateways were handling between 1.2 million and 1.4 million messages per day. The servers were all overloaded and regularly falling behind with a +30 minute delay in message delivery at busy times of the day.

After installing BarricadeMX there are now three gateways, any two of which can easily handle all of the incoming messages with a typical delay of less than 1 minute. The load average on any of these servers rarely exceeds two and usually runs below 1.0.

System configuration (three servers):

- Intel(R) Pentium(R) D CPU 3.00GHz
- 2 GB memory
- BarricadeMX and MailScanner software installed

Results:

- Average Connections / Day: 323,446
- Average Connections / sec: 3.74

- Load Average: Under 1
- Accepted through DATA Phase: 9.93%
- Rejected before DATA Phase: 90.07%

Notice that over 90% of the messages are rejected at the MTA level. This is most all of the spam and viruses. These are typical results for all BarricadeMX sites.

Another strange effect that we are seeing is that the total number of messages processed by all gateways is now dropping. After installation each of the three servers was processing approximately 500,000 messages per day. Now each server is processing less than 350,000 messages per day. We are seeing this effect at all BarricadeMX sites but cannot explain why yet.

There have been very few instances of “good” email being rejected. In all cases the mail was rejected because of very poorly configured servers that were not RFC compliant and these servers were easily detected and white listed where appropriate. The most common errors were:

- Non-existent DNS records for the sending MTA
- Unqualified hostnames for the sending MTA. i.e., localhost not “mail.abc.com”, a FQDN

The rules we enforce for delivery are no more stringent than those enforced by AOL⁵:

More Information

Please contact info@fsl.com or visit our web site at www.fsl.com.

Footnotes

1. Anthony Howe is a respected and well known developer of sendmail milters. His website is www.snertsoft.com.
2. Steve Freegard is the developer of MailWatch, a graphical front to MailScanner. His web site is mailwatch.sourceforge.net.
3. Julian Field is best known for his creation of open source MailScanner, the world’s most popular anti-spam gateway software. His web site is www.mailscanner.info.
4. [Beware the Bots](#), Information Week, October 9, 2006
5. AOL email restrictions
<http://www.postmaster.aol.com/guidelines/standards.html>