

What is BarricadeMX?

BarricadeMX is a high-performance and highly scalable, multi-threaded SMTP proxy. It was written with e-mail security in mind and is designed to handle connections as quickly and efficiently as possible.

We believe that BarricadeMX is the most efficient, accurate and cost effective email security solution available.

Target Markets

- Organizations requiring a simple, cost-effective yet comprehensive, configurable email solution.
- Organizations that are having scalability or accuracy issues with their existing solution.
- Organizations looking for a product that can be easily integrated into an existing control panel.

Unique Sender Notifications

BarricadeMX's totally unique design ensures that that ALL messages are either accepted, tagged if possible spam (both header and subject) or rejected at the SMTP phase. There are many advantages to this approach:

No Quarantine is required because legitimate senders should be notified immediately of delivery failures and can use our unique 'click white listing' feature (described below) to white list themselves automatically in the case of a false-positive. This unique design:

- Removes inherent delays caused by quarantines and the potential for a human to miss a valid e-mail in all the other quarantined spam.
- Requires little maintenance by avoiding the overhead of managing, centralizing and backing up the quarantine
- Considerably simplifies and improves support, system administration and overall efficiency.

- Requires far less disk space. Since quarantine messages are typically stored as one-file-per-message, they can require considerable storage space.
- Substantially reduces network bandwidth requirements since 90% of messages are rejected before the message data is transmitted.

Quarantine types of filtering are really best handled by the users e-mail software where personal preferences are best controlled.

The very small amount of "tagged" email that might contain a false positive can easily be filtered and filed for further examination by the users e-mail software. All modern e-mail software has Junk Mail folders where the user can easily and automatically store any tagged messages for later review.

Pricing

Per-domain pricing model - unlike our competitors who charge on per-user basis, we charge based on the number of domains and CPU cores of the server that runs BarricadeMX.

The base cost of the software includes 100 domains and additional packs of 100, 500, 1,000 or 10,000 domains can be added as your business grows. This additional cost can be as little as \$1 per domain per year. There are no bandwidth or total message limits imposed in the software license.

Clustering

Clustering – BarricadeMX uses a proprietary Multicast / Unicast cache sharing algorithm which allows multiple systems to share persistent data without the need for a centralized SQL database. This provides for fully resilient operation by avoiding any single point of failure.

Cluster dashboard – The web based interface shows the status of each cluster member participating in the cache sharing group. It monitors latency, time offset, cache packet volume, basic message statistics, load, traffic and capacity.

Message Testing

All incoming messages are subject to a series of standard and proprietary tests. The principal design goal for BarricadeMX was to improve SpamAssassin and other types of Post Content (after DATA is accepted) filtering by clever application of Pre-Content (before DATA is accepted) tests.

The unique design of the type and sequence of these tests typically results in BarricadeMX accurately rejecting over 90% of all messages on a typical site.

DNS Lists – BarricadeMX implements traditional IP blacklists (DNSBLs) but also checks the IP white lists, IP grey lists, e-mail, name-server IP, attachment digest and URI blacklists. There are several free public services available for implementing these features or we can provide subscriptions to the popular Spamhaus and URIBL lists at favorable rates. It is also possible to create in-house DNS zones to centralize and simplify management of local RBL lists.

Recipient Verification – BarricadeMX allows the gateway to reject invalid recipients using a "call-ahead" technique, thus improving efficiency and avoiding back-scatter.

Sender Policy Framework – BarricadeMX Provides protection against forged domain names by implementing SPF checks. See <http://www.openspf.org> for further information.

RFC compliance tests – BarricadeMX checks for deliberate or accidental mis-configurations common to spam and virus e-mails.

Enhanced Greylisting – BarricadeMX is designed to distinguish between mail servers that implement RFC compliant retry queues and spam bots that typically do not. Our implementation of greylisting is superior to others, avoiding the pitfalls and excessive delays inherent in other implementations.

Anti-Virus – BarricadeMX supports ClamAV, Avast!, F-Prot and Sophos anti-virus engines via highly efficient daemon interfaces for maximum performance and throughput. This design even allows the anti-virus scanning services to be run on remote servers for maximum scalability.

Attachment Filtering – BarricadeMX supplements Anti-Virus checks to prevent zero-day viruses and enforces local attachment policies by disallowing attachments by filename extension and MIME type.

URI Blacklisting – BarricadeMX prevents the use or inclusion of blacklisted domains or email addresses in the body or headers of a message.

SpamAssassin – BarricadeMX implements the spamd protocol and may be configured to filter messages using “by domain” or “by user” settings in conjunction with SpamAssassin’s virtual user facility.

Electronic Watermarks – BarricadeMX can include a “secret” in the header of each outbound message. All replies to these message can be recognized as valid replies to messages that originated from the BarricadeMX site. This allows for quick and easy filtering of bogus back-scatter due to forged sender addresses and also provides automatic white listing of valid replies.

Customization and Monitoring

Web interface – Customization and monitoring of the BarricadeMX configuration is easily accomplished using a simple, intuitive web interface.

Access Controls – The web interface allows for creation of local white or black lists by IP address, Hostname, HELO, Sender, Recipient or any combined pair of these parameters.

Message Tracking – the web interface also simplifies message tracking and trouble shooting by automating the search and assembly of information from the mail

logs. You only need to enter the information to locate, such as the From or To address and the dates of the logs to search. Log entries matching the search criteria will be quickly displayed.

Protection Limits – The web interface also allows limits to be configured for concurrent connections and rate limits (connections allowed / per unit of time) by IP, Hostname, HELO, Sender or Recipient to prevent Denial of Service and dictionary attacks. Limits can also be configured for the size of messages that will be accepted by IP address, Hostname, Sender, Recipients.

Automated White Listing

Click White Listing allows a valid sender, whose email has been rejected by policy based tests, to white list themselves using a clickable link in the Non-Deliver Receipt and then passing a CAPTCHA test (see <http://recaptcha.net>)

Outbound Filtering

BarricadeMX can easily be configured to automatically detect and block questionable outbound messages from compromised systems, accounts or customers before your email gateways are blacklisted.

System Requirements

Red Hat Enterprise Linux or CentOS version 5 or later.
Minimum 1Gb RAM and Pentium 4 class CPU or better with 200Mb disk space required for installation.
We recommend 1Gb RAM per CPU core and server-class hardware with SCSI/SAS disks for optimum performance.

A typical new Dual CPU, Dual Core server with fast disks and 2GB RAM can easily handle over a million connection attempts per day.

Please contact FSL for further information if you are interested in running BarricadeMX on other platforms (e.g. other UNIX, Windows or MacOS).

Support Options

Basic Support – Available week days from 8am to 5pm US EST (email and web)

Platinum Support – Available 24x7 coverage (telephone, web and email)

fort systems ltd

Fort Systems Limited (FSL) was founded in 2001 to provide the best email security solutions at a reasonable cost. We have sales and development offices in the USA, Canada and UK.

We develop and support both open source and commercial software. FSL delivers expert, dependable and timely support for your open source or commercial email management solution.

FSL is committed to providing our customers with an easily manageable, highly accurate and scalable e-mail security solution.

CONTACT INFORMATION



ZMA - ESET Argentina
Larrea 1011 piso 8° C1117ABE
Ciudad de Buenos Aires - ARG
Tel: 011 4825 1602 - Fax: 011 4825 7692
www.zma.com.ar / info@zma.com.ar