

What is BarricadeMX Plus?

BarricadeMX Plus extends the powerful core technologies present in BarricadeMX by adding a user and domain level web interface and additional monitoring interfaces.

These additional features allow your customers full control of their e-mail filtering and quarantine while providing substantially enhanced reporting capabilities.

BarricadeMX Plus has all the features and advantages of BarricadeMX and More!

Target Market

- Organizations that require a multi-level user accessible interface.
- Organizations that require extensive per-domain configuration.
- Organizations that require a quarantine facility.
- Organization that delegate access and support to customers

Features

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 running BarricadeMX Plus. 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.

Enhanced Web Interface – Can authenticate your users against Active Directory, POP3, IMAP or SMTP servers and allows domain administrators or users to manage their quarantines, train the filters, modify white and black lists and configure their filtering preferences.

Advanced Dashboard – The MailWatch interface shows messages as they are received in real-time and

provides a window on the current day's statistics, monitor queues, machine performance and top senders/recipients.

System Node Monitor provides a real-time view of all on-line gateways and analyze current processing statistics and predicts probable performance and capacity.

Enhanced Message Tracking – The complete message header is available in the searchable MailWatch database for tracking and trouble shooting. Drill-down, clickable links provide easily accessible complete information on the sender, recipient, servers and domains that are part of the message track.

Enhanced Reporting – Users can elect to receive quarantine reports and administrators can run numerous reports against their mail traffic.

Forwarding and / or Archiving – of messages is possible by specifying any combination of Sender, Recipient, Domain or other header parameter.

Before Accepting the Message

Before a message is accepted all of the standard BarricadeMX tests are run:

- Denial of Service Protection
- Message Size Limits
- DNS List
- Concurrent connection Limit
- Rate Control Limits
- Black Listing
- Recipient Verification
- Sender Policy Framework
- RFC compliance
- Enhanced Greylisting
- Basic Virus check (up to 4 engines)
- Click Auto White Listing

SpamAssassin tests may be run before DATA is accepted if no quarantine is desired or after DATA is accepted if Quarantine is required.

Product Comparison

Features	barricademx	plus
Anti-spam	Yes	Yes
Anti-spoofing	Yes	Yes
Anti-phishing	Yes	Yes
Anti-spyware	Yes	Yes
Denial of Service Protection	Yes	Yes
Administrator based login	Yes	Yes
User based login	No	Yes
User based filtering	Yes	Yes
User based Spam Actions	Yes	Yes
Individual Spam Scoring	Yes	Yes
Domain Administrator login	No	Yes
Domain based filtering	Yes	Yes
Domain based Spam Actions	Yes	Yes
Individual Spam Scoring	Yes	Yes
Spam and Antivirus Auto-update	Yes	Yes
Multiple User Authentication Methods - POP- IMAP- LDAP	No	Yes
Domain Based User Authentication	No	Yes
Archive Mail Option	No	Yes
Enhanced Reporting Module	No	Yes
Works with any Mail Server and Network	Yes	Yes
Clustering	Yes	Yes
Active Directory and LDAP integration	Yes	Yes
Outlook-Lotus Notes Integration	Yes	Yes
Log and Graphical Reports	Yes	Yes

	barricademx	plus
Number of Virus Scanners Available	4	26
Enhanced Notification Configuration	No	Yes
Notices Editor	Yes	Yes
Backup Configuration and Settings	No	Yes
Multiple Configuration Rollback Ability	No	Yes
Users licensed	Unlimited	Unlimited
Web interface	Yes	Yes
Integrated help	Yes	Yes
Spam Message tagging	Yes	Yes
Blocked recipient can white list self	Yes	Yes
	Yes (by domain or user)	Yes (by domain or user)
Block on message size	Yes	Yes
Set Spam score by user or domain	Yes	Yes
Fully automated application updates	Yes	Yes
View Log Via Web Interface	Yes	Yes
Multilingual User Interface	Yes	Yes
No Per User or Per Domain Charges	Yes	Yes
Install on your Tested & Certified Hardware	Yes	Yes
Time to Re-deploy in case of Server Failure	Under 1 Hour	Under 1 Hour
Quarantine Attachments	No	Yes
Quarantine Spam	Not Needed	yes
Attachment filtering by user or domain	No	Yes (by domain or user)
Signatures	No	Yes (by domain or user)
MailWatch monitoring	No	Yes
Message Archiving	No	Yes
Server Reboot from Web Interface	Yes	Yes

After Accepting the Message

Attachment Filtering - filter attachments by filename extension or by MIME type to prevent unwanted content (e.g. audio or video) and to prevent zero-day virus attacks.

Additional Anti-Virus checks – BarricadeMX Plus supports 26 different virus scanners and allows multiple scanners to be run for additional protection.

Mail Archiving and Forwarding

Electronic Watermark

Click White listing – BarricadeMXplus 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

MailScanner Roots – BarricadeMX is based on the popular and highly configurable open source MailScanner email gateway software but configuration data is stores in a PostgreSQL database rather than text files. Modifications are done via web interface versus editing text files.

By Domain Configuration – The web interface allows for any configuration parameters such as Spam Scoring, Delivery Options, Message tagging, Reports or signatures to be easily customizable by domain.

Clustering

Adding capacity is as simple as adding identical gateways to a cluster. Each server contains a replica of all configuration data needed to process and deliver messages, ensuring that there is no central point of failure.

Clustered servers may be geographically remote without impacting the clusters performance.

System Requirements

Red Hat Enterprise Linux or CentOS version 5. 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 can easily handle over a million connection attempts per day.

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