

BarricadeMX / SMTPF 2.0 RELEASE NOTES

With the release of BarricadeMX / smtpf 2.0, come many improvements. Below are the principal highlights concerning new options and significant changes:

Improved Performance

smtpf has re-implemented the server connection handling using a collection of pre-spawned server threads that are reusable and grow or shrink as load varies. This change in the server design reduces the effect of constantly creating and destroying threads by maintaining an active pool of waiting threads. New options for this are:

- server-min-threads
- server-new-threads
- smtp-accept-timeout

Delay Checks

Sendmail and Postfix MTAs have a concept called "delay-checks", which essentially allows for recipient white listing to override possible rejections that might occur due to tests early in the SMTP session. smtpf 2.0 now supports a similar concept with the new option:

- smtp-delay-checks

When enabled, all the policy based tests leading up to the recipients being specified are still performed, but any rejection or drop result is delayed and a "250 2.0.0 proceed" reply given. As each recipient address is specified, it is checked whether it is black or white listed, in which case the recipient is rejected or accepted (and subsequent tests by-passed). Recipient addresses that are neither black nor white will either be rejected if there is a previously delayed rejection/drop result or simply accepted.

New Access-Map (Combo) Tags

smtpf borrows some concepts from Sendmail and Postfix, in particular the access key-value map used for access control and some configuration by domain and/or mail address through the use of tagged entries. The original set of tags allowed for black or white listing of a connecting host, a sender's address or domain, or a recipient's address or domain. However, the original tags Connect:, From:, and To: can sometimes be too broad or open to falsification (From:).

So we've added an additional mechanism that allows for finer control over black and white listing in the access-map called "combo tags", where it is possible to join two previously independent tag entries into one to provide lookups based on:

- Connect:From:
- Connect:To:
- From:To:

Combo tag syntax is explained in detail in the access-map documentation section.

New Access-Map Action

Spammers typically use false sender addresses of either legitimate or unknown users within some domain, such as hotmail.com or yahoo.com and others. Use of a From:domain OK access entry might be a quick fix, but can result in spam messages getting white listed and slipping past smtpf. To improve the From: tag, we have added a new SPF-PASS action, that can be used in place of OK, which only white lists a sender domain that has passed an SPF check.

New Administration Commands

smtpf implements SMTP command extensions that are used for administration on the local host machine either directly via telnet or via the web user interface. Some new commands have been added to aid in diagnosis and server management. They are:

CONN	list active session
KILL	kill a session
STAT WINDOW	last 60 minute window view, different from STAT HOURLY

Grey Listing Enhancements

A. Late builds of smtpf 1.0 silently introduced an experimental option that we found to be very effective and have now officially added the option:

grey-content

This option alters grey-listing slightly to take into account the message body of the first message from a never seen before host. A one-way hash of the message is computed, saved, and the message temporarily rejected. Grey-list is applied as before until the temporary fail period expires, after which each message from the unknown host is checked and temporarily rejected until the original first message is sent back thus confirming that a retry queue is used.

This technique has been found to be effective against botnet spam that uses varying templates and/or random generated "hash/bayes busting" text.

B. In addition, a new informational X-Grey-Report header is added to the first message that successfully passes from a host after the grey listing period providing information such as age, grey-key used, and time when grey-listing started.

C. When the grey-list key contains IP or PTR elements, we drop the connection after reporting the temporary failure, because it has been observed that some spammers remain connected and repeatedly attempt to send a message for the same sender/recipient pair or even different pairs. The options smtp-drop-after and/or smtpf-reject-delay would eventually catch this abuse, but this is a time and resource saving measure.

Slow Replies

Some research results reported by the anti-spam community demonstrated that spammers are impatient, such that many will drop a connection that takes too long, the majority within 10 seconds:

MIT Spam Conference 2007 - Pres11

Part A: <http://www.youtube.com/watch?v=bBwdWQfaskI>

Part B: <http://www.youtube.com/watch?v=0pGncfRZqm0&mode=related>

smtpf, Sendmail, Postfix, and other MTA already have options equivalent to smtp-greet-pause and/or smtp-command-pause, which are helpful in catching certain types of bad SMTP behavior (i.e. pipelining commands when such support is disabled).

In some of the late smtpf 1.0 builds, we added an experimental option that we found effective and have now officially added the option:

`smtp-slow-reply`

This option will slow down all the SMTP responses sent to a connected SMTP client. The impatient spammers typically go away, while legitimate senders will continue to send.

Well Behaved Host Enhancement

While the slow reply delays have proven effective, they can also be a burden on legitimate high volume senders and so we added an automated way of disabling some, but not all delaying options, once we know that a sending host is well behaved. We use the results of successful grey-listing by proven good hosts to disable smtp-greet-pause and smtp-slow-reply whenever they connect.

Route Statistics

All of the statistics gathered by smtpf 1.0 have been overall server-wide numbers, helpful in gauging overall performance and behavior of the mail system. However, based on some customer requests, we've added "route statistics", where we gather the ratio of "messages" accepted and rejected daily plus volume in KB for the past 31 days. This allows Postmasters to observe trouble spots on per-domain or per-recipient basis and/or show their customers and management an idea of traffic.

This facility works best when the new smtp-delay-checks is on; when smtp-delay-checks is off, the numbers are still interesting, but need to be interpreted a little differently due to the difference in behavior.

Call-Ahead Enhancements

The call-ahead facility in smtpf has been improved with a "false RCPT" test that checks if the host being consulted is an accept-then-bounce system or the recipient's domain implements a "catch all" rule. For such cases call-ahead is pointless and can be skipped when detected.

Second, in combination with +smtp-delay-checks, when there is a recipient who has not been white listed and for which there is a delayed rejection/drop result from a previous test, we can skip the call-head and report the delayed result.

Null Sender Rate Control

Spammers will often impersonate some random or otherwise false mail address within a legitimate domain like hotmail.com. In some cases when a third party mail system rejects spam or virus mail during the SMTP session, a DSN (bounce message) is generated and sent back to the false sender. Since spammers typically send millions of messages with falsified sender addresses, the mail system of the abused domain can be swamped by the backscatter. smtpf's EMEW facility was designed in part to help with backscatter, but cannot be deployed in some mail system architectures.

So we have implemented another mechanism to help with backscatter situations, where we monitor the rate of DSN or MDN messages (essentially any message from the "null sender") arriving and reject such messages above a certain threshold that can be configured globally, by domain, and by recipient. See the access-map documentation concerning the new tag:

Null-Rate-To:

Additional RFC 2822 Header Tests

smtpf has added some new RFC 2822 conformance tests. First a check for the minimum required message headers Date:, From:, Sender:. The Message-ID: header is also required, though not specified by the RFC as such. Second, date/time stamps in Date:, Resent-Date:, and Received: headers are checked for conformance with the RFC specification. The new options for these tests are:

rfc2822-min-headers
rfc2822-strict-date

Additional URI related tests.

In an effort to deal with "fast-flux" spam, which involve using among other things, several compromised machines to host a spam/phishing web site or act as a redirector to a spam/phishing web site. These hosts used are often on dynamic or residential broadband IP blocks and the spam that refers to these "sites" some time contain links by IP address, host names with IP in name or PTR characteristics, or are missing PTR records. The new options are:

uri-ip-in-name
uri-ip-in-ns
uri-ip-in-ptr
uri-ns-nxdomain
uri-require-domain
uri-require-ptr
uri-reject-unknown
uri-reject-on-timeout

p0f support

Additional p0f support which adds an information X-p0f-Report: header. New options are:

p0f-mutex
p0f-socket

p0f-timeout

Improved spamd support

One of the original design goals for smtpf was to not use any temporary files in an effort to maximize performance of the SMTP proxy. As a result the SpamAssassin spamd support in smtpf 1.0 was limited to rejecting or discarding spam messages; the ability to tag the Subject: header and add result headers was not possible. This meant that a second stage filter such as MailScanner or sendmail with milter-spamc or similar would be required in order to tag messages.

With smtpf 2.0, we altered the design to allow the use of temporary files when using spamd-socket option. Thus it is now possible to tag the Subject: header and add assorted X-Spam-* headers to the message before forwarding. The spamd-policy option has been replaced by the following options:

- spamd-score-reject
- spamd-subject-tag
- save-dir

In addition, some sending sites include "X-Spam-Flag: YES" and/or X-Spam-Status headers that indicate that they already thought the message was spam (why they did not reject it at their end remains a mystery). In such case when the X-Spam-Status score exceeds our spamd-score-reject, we reject the message. Or if there is only a X-Spam-Flag header that states "YES", then we reject the message. Otherwise we discard previous X-Spam-* headers and content filtering proceeds as per usual.

Also we have added support for spamd user configuration selection through the use of a spamd: access map tag. See the spamd documentation for further details.

SMTP AUTH White Listing

Originally, successful SMTP AUTH sessions only allowed you to relay mail and by-pass filters such as SAV and grey-listing, yet content filtering was still applied to protect mail systems from their users who might be infected with a virus or trojan designed to used SMTP AUTH through their relays. Rather than make this a hard rule, we have added a new option to disable this behavior if desired:

- smtp-auth-white

Additional Sender Tests

Similar to the uri-ip-in-ns and uri-ns-nxdomain tests, the NS records of the sender's domain are also tested in a similar manner, i.e. looking for NS hosts that appear to have IP-in-name characteristics and instances of NS records under non-existent domains. These are often traits of "fast-flux" spam. The require sender-mx has been replaced and the new options are:

- mail-ip-in-ns
- mail-ns-nxdomain
- mail-require-mx

SMTP ETRN Support

Added support RFC 1985 SMTP ETRN support, where ETRN commands are simply relayed to the local route, which is responsible for queuing.

Miscellaneous new options

- concurrent-drop
- rate-drop