2013

fort systems ltd

configuring setup for barricademx & access map

documentation for system and domain administrators

BarricadeMX Plus

This short document will show you how to use the BarricadeMX Plus System and Domain Administrators' interface to configure BarricadeMX level 1 filtering. This BarricadeMX Plus processing is performed by the smtpf daemon so the term BarricadeMX Plus as used in this document is synonymous with the term SMTPF (Simple Mail Transfer Protocol Filtering).

The BarricadeMX Plus interface is accessed using a Web Browser window. We currently support the latest versions of Internet Explorer on Windows, Safari on Mac OS X and Firefox on Windows, Mac OS X and Linux systems. You will need to have login credentials supplied to you by the administrator of the BarricadeMX system to be able to use this interface.

Accessing BarricadeMX Configuration

The BarricadeMX configuration for the entire site is modified by using the web interface.

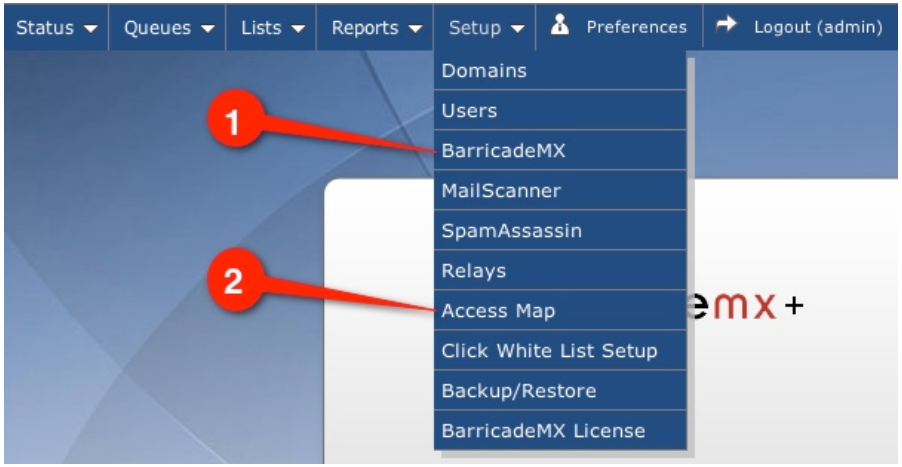

Figure 1. Setup Menu

Select 1. **Setup -> BarricadeMX** to modify the configuration of the BarricadeMX spam testing, virus testing, DNSBL configuration, caching and logging. (**Modifying SMTPF the Configuration** below).

Select 2**. Setup -> Access Map** to modify the configuration of the BarricadeMX white / black listing, message size limits, connection limits, message and attachment filtering. (**Modifying the Access Map Configuration** below).

Modifying the SMTPF configuration

If **Setup -> BarricadeMX** is selected, the screen shown below will be displayed.

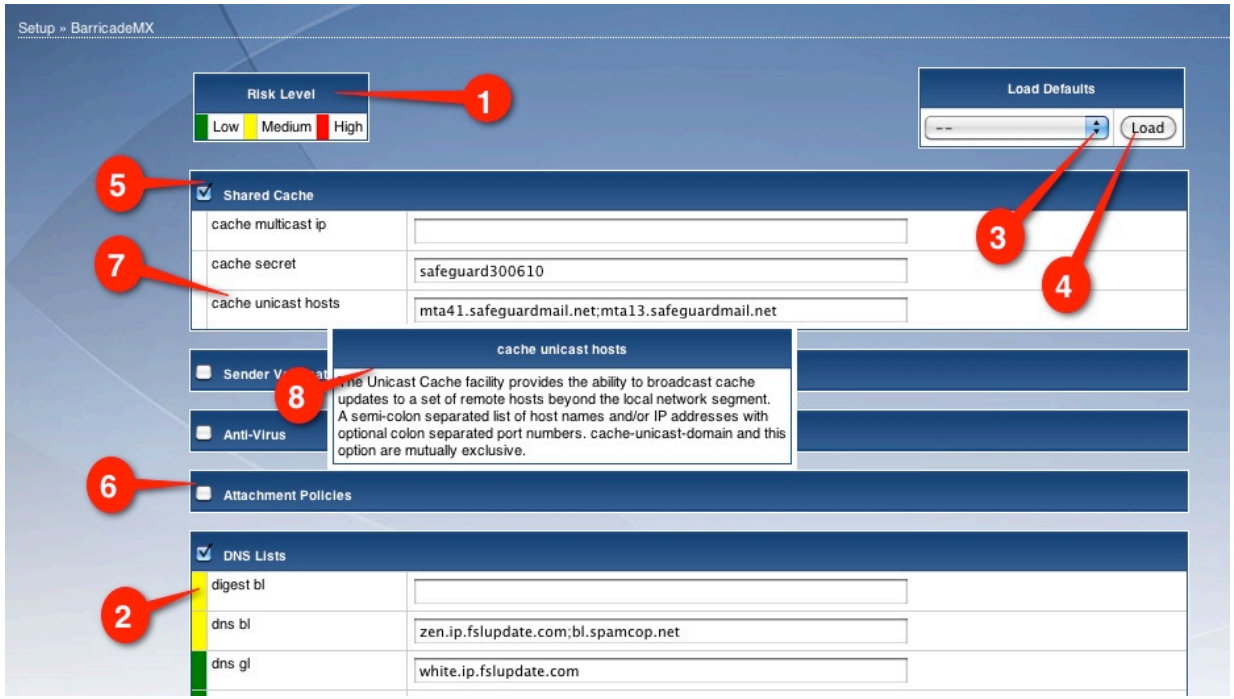

Figure 2. Setup - BarricadeMX Menu

The **1**. **Risk Level Legend** displays the color legend for the **2. Risk Level Color** assigned to some **7**. **Configuration Parameters**. Note that not all **Configuration Parameters** are assigned Risk Level Colors. Risk levels are associated with the potential for False Positives if that test is enabled.

The **3. Load Defaults** text box allows the selection of one of three initial System Default configurations, Low Risk, Medium Risk or High Risk. The **4**. **Load button** changes the system's SMTPF configuration to the selected Risk Level.

Important: These defaults are typically used for the initial system configuration and should **NOT** normally ever be reloaded.

The **5**. **Configuration Grouping** heading shows an "expanded" system configurations grouping. An "expanded" grouping will show one or more **7**. **Configuration Parameters** listed below it.

Clicking on the **7**. **Configuration Parameters** will display the **8**. **Help Tip** associated with the Configuration Parameter. Clicking again will hide the Help Tip.

Important: SMTPF configurations **RARELY** need to be changed. If you are not absolutely sure that you understand the results of a planned configuration change, please contact support@fsl.com before making the change.

Access Map Syntax

The Access Map Database contains records that can determine what actions are taken on an incoming e-mail message. Each Record is composed of a **Key**:**Value** and **Action** pair. Very complete, detailed information of the structure and syntax used in the Access Map database may be found at http://www.snertsoft.com/smtp/smtpf/access-map.html. Only a brief overview of the syntax and structure is given here.

Note: This documentation refers to the first part of the Database Record pair as the **Tag** while the Documentation at www.senertsoft.com refers to the first part of the Database Record pair as the **Key**. The terms **Key** and **tag** are synonymous.

There are three types of **Keys** used in the access-map.

IP Address Lookups

An IP address lookup is typically applied to the connected SMTP client. It will start with a complete IPv4 or IPv6 address and break it down on delimiter boundaries from right to left.

IPv4 Lookup [Key:Value]	IPv6 Lookup [Key:Value]
Key:192.0.2.9	**Key**:2001:0DB8:0:0:0:0:1234:5678
Key:192.0.2	**Key**:2001:0DB8:0:0:0:0:1234
Key:192.0	**Key**:2001:0DB8:0:0:0:0
Key:192	**Key**:2001:0DB8:0:0:0
	Key:2001:0DB8:0:0
	Key:2001:0DB8:0
	Key:2001:0DB8
	Key:2001

Note: that the compact form of an IPv6 address, "2001:0DB8::1234:5678", *cannot* be used. Only the full IPv6 address format, with all intervening zeros, is currently supported.

Domain Name Lookups

A domain lookup may be applied to either the connected SMTP client, where the client's host name found through a **DNS PTR** record is searched for, or using the domain portion of an mail address (see below). A domain lookup will try the IP-domain literal if applicable, continue with the **FQDN**, breaking it down one label at a time from left to right.

[Key:Value]
Key:[ipv6:2001:0DB8::1234:5678]
Key:[192.0.2.9]
Key:sub.domain.tld
Key:domain.tld
Key:tld

Key:

Note:

1. The bare **Key** (a **Key:** without a Value) is often used to specify system wide defaults.
2. "tld" refers to a Top Level Domain

Mail Address Lookups

A mail address lookup is similar to a domain lookup, but the search first starts with a complete mail address, before trying the address's domain, and finally only the local part of the address.

[Key:Value]

Key:account@sub.domain.tld
Key:sub.domain.tld
Key:domain.tld
Key:tld
Key:account@

Possible Key : Value combinations

The following list outlines the available tags and their supported key lookups:

Archname

Archname-Connect:IP
Archname-Connect:Domain
Archname-From:Mail
Archname-To:Mail

The right hand side value is a semi-colon separated list of unacceptable file patterns to reject when found in RAR or ZIP attachments. This overrides the global option deny-compressed-name when defined for a specific host, sender, or recipient.

Body

Body: Domain
Body:Mail

Used to black list (REJECT) or ignore (OK) domains that make up mail addresses or URLs found within the header or body content of a message. See uri-bl and uri-dns-bl.

Concurrent

Concurrent-Connect:IP
Concurrent-Connect:Domain

This is used to specify the maximum number of concurrent connections an SMTP client is permitted at any one time. Specify an integer or zero (0) to disable. The bare tag can be used to specify a global setting. If an SMTP client exceeds the allotted number of connections, then the incoming connection is dropped, while existing connections continue.

Connect

Connect:IP
Connect:Domain

Used to black or white list an SMTP client. If black listed (REJECT), the connection will be dropped. If white listed (OK), then the messages from this connection by-passes all the filtering except anti-virus. The connection can also be "grey-listed" (CONTENT), similar to dns-gl, which only white lists a connection as far as, but not including, the data content filters.

Connect:IP**:From:**Mail
Connect:Domain:**From**:Mail

This set of combination tags are used to black or white list sender addresses when sent from a given SMTP client. The sender address can be easily forged and using the From: tag by itself could allow spam with a forged address. By adding the sender's SMTP client as an extra constraint, it is possible to limit such abuse. Note that the lookup variants with blank IP, domain, or mail are not supported.

Connect:IP**:To:**Mail
Connect: Domain**:To:**Mail

This set of combination tags are used to black or white list recipient addresses that a given SMTP client may contact. This allows for finer granularity of control in place of the To: tag. Note that the lookup variants with blank IP, domain, or mail are not supported.

Emew

Emew: Mail

Used to specify an alternative EMEW secret for the sender or sender's domain.

Filename-Connect

Filename-Connect:IP
Filename-Connect: Domain
Filename-From: Mail
Filename-To: Mail

The right hand side value is a semi-colon separated list of unacceptable file patterns to reject when found as MIME attachments. This overrides the global option deny-content-name when defined for a specific host, sender, or recipient.

Filename-Connect

Filename-Connect:IP**Filename-Connect:**Domain
Filename-From: Mail
Filename-To: Mail

The right hand side value is a semi-colon separated list of unacceptable file patterns to reject when found as MIME attachments. This overrides the global option deny-content-name when defined for a specific host, sender, or recipient.

From

From: Mail

Used to black or white list a sender's mail address. If black listed (REJECT), mail from this sender is refused. If white listed (OK), then the messages from this sender will by-pass all the filtering except anti-virus. Black listing using this tag is fine, but white listing is not recommended as it is too easy for someone to fake the sender address.

From: Mail**:To:**Mail

This set of combination tags are used to black or white list a pair of sender and recipient addresses. This allows for finer granularity of control in place of the To: tag. Note that the lookup variants with blank mail elements are not supported.

Grey-Connect

Grey-Connect:IP
Grey-Connect: Domain
Grey-To: Mail

This is the amount of time in seconds a correspondent's grey-list record will be temporarily rejected before being accepted. If several keys are possible for a given message, then the minimum value is used. Specify an integer number of seconds or zero (0) to disable.

Helo

Helo:IP
Helo: Domain

Used to black or white list an SMTP client based on the HELO/EHLO argument. If black listed (REJECT), the connection will be dropped. If white listed (OK), then the messages from this connection by-passes all the filtering except anti-virus. The connection can also be "grey-listed" (CONTENT), similar to dns-gl, which only white lists a connection as far as, but not including, the data content filters.

This tag is not recommended for white listing as the HELO argument as it can be too easily falsified. It is primarily intended for data gathering and diagnostics when used with SAVE, TAG, or TRAP actions. The other actions are supported for completeness.

Length-Connect

Length-Connect:IP
Length-Connect: Domain
Length-From: Mail
Length-To:Mail

Used to limit the maximum length of a message in octets. It is expressed as a number with an optional scale suffix K (kilo), M (mega), or G (giga). If no length is given or is -1, then the message can be any length (ULONG_MAX).

When there are multiple message length limits possible, then the limit applied, in order of precedence is:

1. Length-To:. If there is more than one **Length-To:,** then the maximum limit specified will be used.
2. Length-From:
3. Length-Connect:Mimetype-Connect:ip

Mimetype-Connect

Mimetype-Connect: Domain
Mimetype-From: Mail
Mimetype-To: Mail

The right hand side value is a semi-colon separated list of unacceptable attachment MIME types to reject. This overrides the global option deny-content-type when defined for a specific host, sender, or recipient.

Msg-Limit-Connect:

Msg-Limit-Connect:ip
Msg-Limit-Connect:domain
Msg-Limit-From:mail
Msg-Limit-To:mail

Used to limit the number of messages a SMTP client, sender, or recipient can send/receive in a given time period. A message limit is given as:

messages '/' time [unit]

Which is the number of messages per time interval. The time unit specifier can be one of week, day, hour, minute, or seconds (note only the first letter is significant). A negative number for messages will disable any limit.

When there are multiple message limits possible, then the limit applied, in order of precedence is: **Msg-Limit-To**:, **Msg-Limit-From**:, and **Msg-Limit-Connect**.

Null-Rate-To

Null-Rate-To:Mail

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.

smtpf provides another mechanism to help with backscatter situations, where smtpf monitors the rate of DSN or MDN messages (essentially any message from the "null sender" ie. MAIL FROM:<>) arriving per minute and rejects such messages above a certain threshold that can be configured globally, by domain, and by recipient.

The right-hand-side value is a positive number representing the permitted number of messages from the null sender per minute to the given recipient or domain; -1 to disable.

Rate-Connect

Rate-Connect:IP
Rate-Connect: Domain

This is used to specify the number of connections per minute a host is allowed. Simply specify an integer or zero (0) to disable. The bare tag can be used to specify a global setting. If an SMTP client connects too frequently in excess of this limit, then the incoming connection is dropped.

Spamd

Spamd: Mail
Spamd: Domain
Spamd:

Used to specify a SpamAssassin configuration to use. If the message is addressed to a single recipient, then a Spamd:mail lookup is done. If the message is for more than one recipient, all of whom are within the same domain, then a Spamd:domain lookup is done. Otherwise the Spamd: default configuration is used. The right hand side **Action** must be a user name or address to pass to spamd or it can be a pattern list. If the special user name OK is used, then the message is not processed by spamd.

To:

To: Mail

Used to black or white list a recipient's mail address. If black listed (REJECT), mail to this recipient will be refused; the current message transaction is permitted to specify addition recipients or abandon the transaction. If white listed (OK), then the message will by-pass all the filtering except anti-virus.

Top-Mimetype-Connect

Top-Mimetype-Connect:IP
Top-Mimetype-Connect: Domain
Top-Mimetype-From: Mail
Top-Mimetype-To: Mail

The right hand side value is a semi-colon separated list of unacceptable message MIME types to reject. This overrides the global option deny-top-content-type when defined for a specific host, sender, or recipient.

It should be noted that black & white listing with Connect:, Connect:From:, Connect:To:, From:, From:To:, and To: take effect immediately in the SMTP state they apply to. This can be changed by enabling smtp-delay-checks which delays policy rejections until the recipients have been specified with the possibility to white list. The auth-delay-checks option can be used to delay the connection and EHLO related tests until a MAIL FROM: is received allowing for an SMTP AUTH command to be issued.

Possible Actions

When a key lookup matches, then the value returned is a pattern list, which in its simplest and most common form is either an action word like **OK**, **CONTENT**, **DISCARD**, **REJECT**, **IREJECT**, **TAG**, etc; or a numerical value depending on the tag involved. For example:

Connect:192.168.0 OK

Rate-Connect:fsl.com 17

Msg-Limit-From:hotmail.com 150/30m

The supported **Action** words are:

OK	White list, by-pass one or more tests, except anti-virus scanning
CONTENT	White list as far as, but not including, the content filters; used only with Connect: or Helo:.
DISCARD:"log-comment"	Accept and discard message skipping tests; use with care. :"log-comment" is optional
IREJECT:"custom-reply"	immediate REJECT, ignore smtp-delay-checks; applies only to Connect:, Connect:From:, From:, and Helo:. :"custom-reply" is optional
REJECT:"custom-reply"	Black list, either reject or drop. :"custom-reply" is optional
SAVE:"path"	Save a copy of message if delivered and save message to save-dir, unles the optional :"path" is specified
SKIP	Stop lookup and return no result ie. continue testing
SPF-PASS	White list sender if SPF returns Pass; used only with Connect:From: and From:
TAG	If a policy rejection or drop would occur, simply tag the Subject: header and by-pass remaining tests
TEMPFAIL:"custom-reply"	Report a temporary failure condition. :"custom-reply" is optional
TRAP:"path"	Accept and save message, but do not deliver, to trap-dir, unless the optional :"path" is specified

Pattern Lists

In most instances, the above forms of key lookup and values are sufficient. However, there may be times when finer granularity of control is required, in which case pattern lists can be used. A pattern list is a white space separated list of pattern-action pairs followed by an optional default action. The supported types are:

[network/cidr]action Classless Inter-Domain Routing (only with IP address lookups)

!pattern!action Simple fast text matching.

/regex/action Extended Regular Expressions.

The simple pattern matching, !pattern!, uses an asterisk (*) for a wildcard, scanning over zero or more characters; a question-mark (?) matches any single character; a backslash followed by any character treats that character as a literal. This method always tries to match the beginning and end of string. For example:

!abc! exact match for 'abc'

!abc*! match 'abc' at start of string

!*abc! match 'abc' at the end of string

!abc*def! match 'abc' at the start and match 'def' at the end, maybe with stuff in between.

!*abc*def*! find 'abc', then find 'def'

The following is an example using a simple pattern to reject client connections that originate from a range of IP addresses of an ISP assigned to ADSL customers. Using a pattern like this allows you to drop connects from the ISP's ADSL, while still accepting connections from mail and web servers.

Connect:hananet.net !adsl-*-*.usr.hananet.net!REJECT

If you know that an ISP's mail and web servers follow a standard naming convention, you might prefer to only accept mail from those instead. We include web servers here to handle the case where a web server might have to send a mail response based on a form being filled in.

Connect:hananet.net !smtp*.hananet.net!OK !www*.hananet.net!OK REJECT

Note that SPF was designed to help mail servers identify originators of mail, so creating patterns as shown in the above two examples is not normally required. However, SPF is still considered experimental and not as widely deployed as one might hope.

The next example, /regex/, uses Extended Regular Expressions to validate the format of the local-part of an AOL address, which must be between 3 and 16 characters long, can contain dots and RFC 2822 ``atext'' characters except % and /. The NEXT word allows the one regular expression to validate the format of the address and resume key lookup if the pattern matches; otherwise if the regular expression failed to match, REJECT the suspect aol.com address.

From:grandma@aol.com OK

From:aol.com /^[a-zA-Z0-9!#$&'*+=?^_`{|}~.-]{3,16}@aol.com$/NEXT REJECT

The discussion of Extended Regular Expressions is vast and complex, well beyond the scope of this document. There are many on-line tutorials and references available and the book, Mastering Regular Expressions, from O'Reilly covers the topic in depth.

If you need to use a pattern list, then try and follow these suggestions:

A pattern cannot be used as the key in an access-map lookup. Key-value tables work with constants for the keys using a predefined lookup order as outlined above.

Use the key lookup as a selector to find a pattern list.

Use simple !pattern! matching where possible, as it will be faster than Extended Regular Expressions, /regex/.

Avoid using pattern lists with bare tag variants that specify a global default. It will more often than not cause a lot of unnecessary attempts to match a pattern.

Keep your pattern lists short & simple.

Modifying the Access Map

If **Setup -> Access Maps** is selected, the screen shown below will be displayed.

Figure 3. Setup – Access Map Menu

The 1. **Records** window displays the total number of Access Map records with links to the first 5 pages and the last page of the Records. The **2. Search** text box allows you to enter a text string to match in the Access Map **Records**. The 3. **Go!** button is use to initiate the search. The 4. **Alphabetical Index** provides shortcut links to alphabetically sorted groups of the Records.

Each 9. **Record** consist of a **Key**:**Value** and **Action** pairs as described above.

To enter a new **Record**, enter the new Key:Value in the 5. **Key:Value** text Entry box, then enter the Action in the 6. **Action** Text Entry box. Then select the 7. Add button

To delete a 9. **Record,** select the Delete Link on the same line as the Record to be deleted.

To Edit a 9. **Record,** select the Edit Link on the same line as the Record to be Edited.

Getting Help

With over 300 possible configuration settings, configuring BarricadeMX can be intimidating at first. Many possible configuration settings, while quite powerful, can be confusing to modify or revise correctly. If you need assistance with any of the configuration settings, just send a request which describes what you are trying to accomplish to support@fsl.com and we'll try to assist with your site configuration questions.