fort systems ltd

RBL Use and Configuration with BarricadeMX

This file contains our best interpretations of the permitted "Terms of Use" for using Realtime BlackHole (RBL) DNSBL lists on systems that use BarricadeMX. However, you are strongly advised to visit the original list sites to view the actual "Terms of Use" for each list that you use on your systems.

For the complete Spamhaus Usage Policy Statement please see:
http://www.spamhaus.org/organization/dnsblusage.html

For the complete SURBL Usage Policy Statement please see:
http://www.surbl.org/usage-policy.html

For the complete URIBL Usage Policy Statement please see:
http://www.uribl.com/about.shtml#abuse

At the time of this writing, the following lists are freely available for use:

cbl.abuseat.org	http://cbl.abuseat.org/tandc.html
bl.spamcop.net	http://www.spamcop.net/fom-serve/cache/297.html
list.dnswl.org	This is a whitelist; see http://www.dnswl.org/

While we have done our best to understand and explain the "Terms of Use" for each of the lists below, we cannot be responsible for misinterpretations or changes that have occurred since this document was written.

USE THIS INFORMATION AT YOUR OWN RISK !

Using RBL Lists with BarricadeMX

If your site can meet all of these conditions:

1. Your use of the Spamhaus DNSBLs is commercial*
2. Your email traffic is less than 100,000 SMTP** connections** per day
3. Your DNSBL query volume is less than 300,000** queries per day.

*Definition: "non-commercial use" is use for any purpose other than as part or all of a product or service that is resold, or for use of which a fee is charged. For example, using our DNSBLs in a commercial spam filtering appliance that is then sold to others requires a data feed, regardless of use volume. The same is true of commercial spam filtering software and commercial spam filtering services.

**This would equate to approximately 3,500 mail boxes.

It would be considered a smaller site as described below and you would need to purchase subscriptions to use the Spamhaus and SURBL RNL lists. This is because BarricadeMX is considered commercial spam filtering software.

Smaller sites can use the black.uribl.com (URIBL) list and the bl.spamcop.net (SPAMCOP) RBL lists at no charge. You will need to purchase subscriptions to use the zen.spamhaus.org (SPAMHAUS) and the multi.surbl.org (SURBL) RBL lists if:

1. Your use of the Spamhaus DNSBLs is commercial*
2. Your email traffic is more than 100,000 SMTP connections per day
3. Your DNSBL query volume is more than than 300,000 queries per day.

Your site would be considered a larger site as described below and you would need to purchase subscriptions to use the Spamhaus, URIBLACK and SURBL RBL lists.

For Smaller Sites that use BarricadeMX

A. BarricadeMX configuration:

Block at the SMTP level using bl.spamcop.net. We also recommend blocking at the MTA level using zen.spamhaus.org but you will need to purchase a Spamhaus license to use this feed. Please contact info@fsl.com for a price quote to use this list.

If you can use the spamhause, feed configure BarricadeMX to use the spamhaus list as well as the free bl.spamcop.net list. In the file/etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

dns-bl=zen.spamhaus.org,bl.spamcop.net

If you have not purchased a Spamhaus feed, use the free bl.spamcop.net list. In the file /etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

dns-bl=bl.spamcop.net

You should also block at the SMTP level based on "spammy" URI/URLs in the body of the message using the black.uribl.com list. You can also block at the MTA level for suspect URI/URLs using multi.surbl.org but you will need to purchase a subscription for this feed from http://www.surbl.org/

Unless you have purchased the SURBL list, configure the system to use only the black.uribl.com which is free to use for smaller sites. In the file /etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

uri-bl=black.uribl.com

If you have purchased a subscription to use the SURBL list, in the file /etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

uri-bl=multi.surbl.org,black.uribl.com

B. SpamAssassin rule configuration:

Unless you have a subscription to Spamhaus or SURBL, you will need to disable the relevant SpamAssassin rules to prevent them from being queried. The following lines should be added to your local SpamAssassin configuration file (typically /etc/mail/spamassassin/local.cf).

Unless you have a subscription to spamhaus, disable Spamhaus:

```
score __RCVD_IN_ZEN 0
score RCVD_IN_SBL 0
score URIBL_SBL 0
```

With Spamhaus disabled; you can then enable checks to the CBL by adding:

```
header RCVD_IN_CBL eval:check_rbl('cbl-lastexternal','cbl.abuseat.org.')
describe RCVD_IN_CBL Received via a relay in the CBL
score RCVD_IN_CBL 4.0
tflags RCVD_IN_CBL net
```

Unless you have a subscription to SURBL, disable SURBL:

```
score URIBL_AB_SURBL 0
score URIBL_JP_SURBL 0
score URIBL_OB_SURBL 0
score URIBL_PH_SURBL 0
score URIBL_SC_SURBL 0
score URIBL_WS_SURBL 0
```

For Larger sites that use BarricadeMX

A. MTA configuration:

Block at the SMTP level using bl.spamcop.net. We also recommend blocking at the MTA level using zen.spamhaus.org but you will need to purchase a Spamhaus license to use this feed. Please contact info@fsl.com for a price quote to use this list.

If you can use the spamhaus feed, configure BarricadeMX to use the spamhaus list as well as the free bl.spamcop.net list. In the file /etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

```
dns-bl=zen.spamhaus.org,bl.spamcop.net
```

If you have not purchased a Spamhaus feed, use the free bl.spamcop.net list. In the file /etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

```
dns-bl=bl.spamcop.net
```

You should also block at the SMTP level based on "spammy" URI/URLs in the body of the message using the black.uribl.com list. You can also block at the MTA level for suspect URI/URLs using multi.surbl.org but you will need to purchase a subscription for this feed from http://www.surbl.org/

Unless you have purchased the SURBL list, configure the system to use only the black.uribl.com which is free to use for smaller sites. In the file /etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

```
uri-bl=black.uribl.com
```

If you have purchased a subscription to use the SURBL list, in the file /etc/smtpf/smtpf.cf or the BarricadeMX web interface configure:

```
uri-bl=multi.surbl.org,black.uribl.com
```

B. SpamAssassin rule configuration:

Unless you have a subscription to Spamhaus, URIBL or SURBL, you will need to disable the relevant SpamAssassin rules to prevent them from being queried. The following lines should be added to your local SpamAssassin configuration file (typically /etc/mail/spamassassin/local.cf).

Unless you have a subscription to spamhaus, disable Spamhaus:

```
score __RCVD_IN_ZEN 0
score RCVD_IN_SBL 0
score URIBL_SBL 0
```

With Spamhaus disabled, you can then enable checks to the CBL by adding:

```
header RCVD_IN_CBL eval:check_rbl('cbl-lastexternal','cbl.abuseat.org.')
describe RCVD_IN_CBL Received via a relay in the CBL
score RCVD_IN_CBL 4.0
tflags RCVD_IN_CBL net
```

Unless you have a subscription to URIBL, disable Spamhaus:

```
score URIBL_BLACK 0
score URIBL_GREY 0
score URIBL_RED  0
```

Unless you have a subscription to SURBL, disable Spamhaus:

```
score URIBL_AB_SURBL 0
score URIBL_JP_SURBL 0
score URIBL_OB_SURBL 0
score URIBL_PH_SURBL 0
score URIBL_SC_SURBL 0
score URIBL_WS_SURBL 0
```

Prepared :
Mon Apr 27 13:09:46 EDT 2009