DnsBlocklists

DNS Blocklists

Introduction

DNS Blocklists are a common form of network-accessible database used in spam detection. They're also referred to as "DNSBLs", "DNS Blacklists" and "RBLs". (The latter usage is incorrect; see RBL.)

SpamAssassin includes support for many of the bigger DNSBLs, with optimal scores (or at least, optimal as determined by the GeneticAlgorithm).

To implement DNS Blocklists, it is heavily recommended to run your own CachingNameserver

SpamAssassin Policy for DNSBL Inclusion

The SpamAssassin Policy for DNSBL Inclusion is available at DnsBlocklistsInclusionPolicy

Block Lists

Support for the following DNSBLs is built-in, and shipped in the default configuration.

- **Mailspike** http://www.mailspike.net/ Mailspike has a few components: in the sense of blacklists Mailspike has a blacklist and a zombie-list (participants of current spam waves).
- **SORBS** http://www.sorbs.net/ Note: most zones are included except the actual spam zone due to a $50 delisting fee. You can enable it manually it desired.
- **SpamCop** http://www.spamcop.net/ SpamCop accepts (automatic) submissions and sends abuse mail in your behalve. SA has a plugin for reporting.
- **Spamhaus ZEN** http://www.spamhaus.org/zen/ NOTE: *Spamhaus is enabled as a "free for most" provider.* See: http://www.spamhaus.org/organization/dnsblusage.html.
- **SURBL** http://www.surbl.org/ NOTE: *SURBL is enabled as a "free for most" provider.* See: http://www.surbl.org/usage-policy.
- **URIBL** http://www.uribl.com/ NOTE: *URIBL is enabled as a "free for most" provider.* See: http://www.uribl.com/about.shtml.
- **Validity** http://www.validity.com/ NOTE: *Validity is enabled as a "free for most" provider.*.

Reputation

The following DNS checks have diverse levels of reputation:

- **Mailspike** http://www.mailspike.net/ Mailspike has a reputation list of 10 different levels between a good and bad reputation. The top and bottom define their white and blacklists.

Whitelists

The following DNS checks are actually for WHITE lists, or sites which are certified by someone to be a reasonable sender.

- **DNSWL** http://www.dnswl.org/ NOTE: *DNSWL is enabled as a "free for most" provider.* See http://www.dnswl.org/license.
- **ISIPP Accreditation Database** (IADB) http://www.isipp.com/email-accreditation/
- **Mailspike** http://www.mailspike.net/
- **Sender Score Certified & Sender Score Safe List** http://www.senderscorecertified.com/ (formerly Ironport Bonded Sender & Habeas Safelist)

URIBLs

The following DNS checks are for URI's (eg http links).

- **Spamhaus** http://www.spamhaus.org/dbl/ Checking for spamvertized/phishing/malware/botnet/abused redirector sites. Also checking for NS and A records.

Other Lists

Other places to find out about DNS blacklists / blocklists:

- Wikipedia on DNSBLs http://wikipedia.org/wiki/DNSBL
- Dr. Jørgen Mash's DNS database list checker http://moensted.dk/spam/
- Weekly Blacklist Statistics (including hit rate and false positive rate) http://www.intra2net.com/en/support/antispam/

Note that it's extremely important to compare false positive rates (nonspam messages marked as spam), as well as spam hit-rates, when evaluating any anti-spam system, include DNS blocklists. (For example, a blocklist that returned a match for every single mail would 'catch all the spam', but would also mark every nonspam mail too.) Some of the above pages omit this information, so take with a pinch of salt.

Questions And Answers

Q: My queries to a DNS-blocklist were blocked. What does this mean?

A: DNS-Blocklists often run on the "free for some" model and/or they may limit the number of queries you can perform to maximize resources.

If you were directed to this link from a rule description, then you have a DNS-Blocklist that is purposefully blocking your queries.

Resolving the block might be as simple as using your own non-forwarding caching nameserver to avoid being lumped together with other users queries; setting up your own mirror of the DNS-blocklist; or paying to use the blocklist. The choice is up to the DNS-Blocklist administrator.

SpamAssassin supports the "free for some" model since it works for the majority of SpamAssassin installations. However, we do not support methodologies that purposefully return wrong answers and those DNS-Blocklists will be disabled by default.

The following blocklist providers have implemented a Block Notification Rule with SpamAssassin:

- URIBL http://www.uribl.com/ (rule **URIBL_BLOCKED**)
- DNSWL http://www.dnswl.org/ (rule **RCVD_IN_DNSWL_BLOCKED**)
- Spamhaus http://www.spamhaus.org/
- SURBL http://www.surbl.org/ (rule **SURBL_BLOCKED**)
- Validity http://www.validity.com (rule **VALIDITY_BLOCKED**)

Q: This documentation doesn't seem to cover how to configure DNS-Blocklists. It says "Support for these is built-in" but I can't believe that all free BL's is called each time a mail is beeing checked. There must be a way to configure which to use.

A: You're right. You might look at the Mail::SpamAssassin::Conf documentation page which I admit doesn't really say how to configure which DNSBL to use, or the rules file 20_dnsbl_tests.cf, for internal details, but no clear examples of how to configure the inclusion of various DNSBLs either. For the latest list of DNSBLs you want to be using a recent SpamAssassin version (3.4.1 at the time of this correction) and sa-update, for the same reason that you wouldn't use an out-of-date virus scanner, but that also doesn't really have anything to do with the question.

If you don't want *any* DNSBLs used, put a line like

- `skip_rbl_checks 1`

in your local.cf

To eliminate the use of a particular DNSBL, set the score to zero. Put lines like

- `score RCVD_IN_RFCI 0` `score RCVD_IN_ORBS 0` `score RCVD_IN_DSBL 0`

in your local.cf if you don't want certain DNSBLs listed with RCVD_IN_* in 50_scores.cf to be used.

Note: many of the DNSBLs that can return multiple lists with one DNS query are implemented using one, unscored, rule that triggers the DNS lookup and stores the result, and several scored rules that check against that stored result (ie: zen.spamhaus.org). For these sets, if you wish to completely disable the DNS lookup, you will need to disable this rule. It can be found by looking at 20_dnsbl_tests.cf, and find the rule implemented using "check_rbl" instead of "check_rbl_sub".

At present, the query trigger rule for SpamHaus looks like this:

- `header __RCVD_IN_ZEN eval:check_rbl('zen', 'zen.spamhaus.org.')`

So to disable it you'd use:

- `score __RCVD_IN_ZEN 0`

To disable all DNSWL rules, use:

- `score __RCVD_IN_DNSWL 0`

NOTE: As from SpamAssassin version 3.4 you may disable queries for any BL by adding: (local.cf)

dns_query_restriction deny bldomain

for example:

dns_query_restriction deny sorbs.net

Q: The dns-blocklists just don't appear to be used. What is going wrong?

A: First, make sure Net::DNS for perl is installed. Without this the blocklists will not be used.

A: Second, do some tests with Net::DNS to make sure it is resolving names (see the Net::DNS site for examples). A common mistake for client machines (such as Mandrake 9.2) is to have 127.0.0.1 in the </etc/resolv.conf> file – Net::DNS does not check multiple nameservers it appears, so you need to comment this line out for Net::DNS to work. (Anybody with a better solution, other than running a local nameserver?)

A: Third, if your email gateway is behind a firewall make sure that SpamAssassin is resolving the gateway to its external address. If SpamAssassin resolves the gateway to an private IP or can't resolve the name at all, it may mark the sending system as a trusted relay. As a result, some or all of the spammer's systems will not be checked against the DNSBL. (I'm not aware of anyway to specify 'last trusted relay' in SA).

Q. Wouldn't it be a good idea to run a local nameserver anyway? So, you can run caching-nameserver to cache blocklist query results.

1. Yes! In fact, doing this is important to *avoid false results from some DNS lists (e.g. DNSWL) if you have a large ISP* and, if you're running a busy mailserver, this is *essential* for efficiency. See CachingNameserver.

Q: I'd like to penalize certain countries from which I get a lot of spam and almost no real mail. I can't seem to get it working with multiple countries.

1. See RelayCountryPlugin.