DnsBlocklistsInclusionPolicy

Apache SpamAssassin PMC Policy for DNSBL Inclusion

Goal:

To produce an objective policy for the inclusion of DNS-Blocklists (DNSBLs) including free, commercial and semi-commercial services that promotes the ability to include more tests in a manner that is fair to the community and the service provider.

Criteria for All DNSBL Services:

All services, including free, commercial or semi-commercial services must meet these criteria for default inclusion in Apache SpamAssassin's rules:

- Must not block queries by returning purposefully wrong answers e.g. from over-quota or abusive IPs.
- May refuse or block queries completely through technologies that must not result in misfiring of rules but may result in minor delays scanning emails due to DNS timeouts.
- Must have an existing or planned infrastructure capable of handling the anticipated query load.
- Must give the Apache SpamAssassin project permission to include the rules by default.
- DNSBLs should only be added to default configuration rules in conjunction with a new major release using version encapsulation so that existing administrators can decide whether to use the new DNSBL manually, if possible, in older installations.
- A formal vote in bugzilla must be taken before a DNSBL is added to a sandbox and enabled including sandbox rules added for testing purposes only.
- Must meet acceptable mass-check scoring criteria to be considered for default inclusion. Testing is mandatory and the higher the S/O ratio, the better. See http://wiki.apache.org/spamassassin/HitFrequencies.
- Must not have significant reliability issues.
- Must have clear rules and procedures that are followed uniformly for listings and de-listings.
- Must not have intent to profit, including optional or required payments, in order to remove, add, expedite or otherwise non-objectively handle entries to their lists.
- Must use Apache SpamAssassin rules that implement lastexternal or firsttrusted testing unless there is an overwhelming benefit to the S/O ratio or similar technical argument.
- May use limits such as DNS query limits per day with daily query limits of at least 100,000 queries per day considered acceptable for default inclusion. A DNSBL may also be approved for default inclusion with lower query limits under certain circumstances such as free access to download zone files to run a local mirror.
- May have licensing that requires an Administrator to sign up for an account / mailing list / etc. for the purpose of notifying Administrators of changes and problems but must not have technical enforcement of the requirement.

Criteria for Semi-Commercial aka “Free for Some” DNSBL Services:

Semi-commercial services aka "Free for Some" must meet these additional criteria for default inclusion in Apache SpamAssassin's rules:

- Must be considered “free for most” Apache SpamAssassin installations with “most” defined loosely to include covering the small businesses, non-profits, personal users, etc. that make up the bulk of our installations.
- Must be free for any kind of person or organization to use including commercial, government, or home user however service providers may impose licensing limitations on use by anti-spam resellers or those directly reselling standalone spam filtering services.
- Must not attempt to retroactively bill users that have exceeded any free limits.
- Must not implement licensing limitations on the service that constitute a trial or limited time offer. However, service providers may still offer trials or limited time offers on Commercial licenses.
- May use a zone specific to Apache SpamAssassin in order to offer licensing to meet the criteria of this Policy.
- Must not place a limit on the number of users or other arbitrary caps that can't be correlated to a direct increase in expenses for the service provider.
- Should use a query response and BLOCKED rule that indicates a system is over query limits *if* query limits are enforced. Scoring on the BLOCKED rule must not materially affect scoring and link only to a generic DNSBL Block page such as http://wiki.apache.org/spamassassin/DnsBlocklists#dnsbl-block.
- Must have a usage policy including any limits or restrictions that is clearly documented and publicly visible using well defined terms. Terms such as "heavy load" are not acceptable.

Criteria for Commercial DNSBL Services:

Services that are completely commercial are not eligible to be enabled by default but can be included for administrator configuration on a case-by-case basis. We encourage you to consider implementing a “Free for Some” DNSBL service to support the anti-spam community.

Caveats:

This policy is subject to change by the Apache Software Foundation SpamAssassin Project Management Committee. We welcome community input.

DNSBLs can be removed or added for reasons not covered in this policy but this policy should: a) form the basis of any discussion on such matters; and b) be updated to account for the decision in a uniform manner.

There is no guarantee a DNSBLs accepted for default configuration rules will remain in the default configuration rules for any period of time.

Services that are administered by or on behalf of the Apache Software Foundation and its projects are exempt from this policy.

Items not Covered by this Policy:

This policy currently only covers DNSBLs. It does not cover network-based anti-spam tests such as Vipul's Razor, Pyzor or the Distributed Checksum Clearinghouses (DCC).

All three of these tests are not suitable to have their rules enabled by default because they require administrator configuration, system registration and software installation. However, support for all three is included with Apache SpamAssassin for easier administrator configuration.

Should these or new tests have underlying technology and/or policy changes allowing them to be work in a default configuration; then this policy should be expanded to cover all network-based tests.