Ruslpóstsían Spam Assassin er eins og nafnið gefur til kynna vægðarlaus við ruslpóstinn. Ýmsir möguleikar bjóðast í uppsetningu þessarar þjónustu en allar stillingar fara fram í gegn um stjórnborðið (cpanel - sjá Spam Assassin undir E-Mail hlutanum).

Byrjað er á að virkja (enable) kerfið en sú aðgerð er það fyrsta sem blasir við þegar það er opnað.

HOME
LOGOUT
cPanel X
CPANEL 10
Spam Message Filter Configuration
Current Status
SpamAssassin is currently: Disabled
Spam Box is currently: Disabled
SpamAssassin
SpamAssassin is an automated mail filter that uses a wide range of heuristic algorithms on email headers and message bodies to identify "SPAM" (unsolicited email). SpamAssassin is designed to identify and mark emails that score beyond your threshold value. An email's SpamAssassin score is the sum of values given to certain known spam characteristics.
For more information, please visit the developers' website: http://www.spamassassin.org
To simply have the server DELETE and NOT deliver emails that are tagged as spam by SpamAssassin, click here now.
Enable SpamAssassin
Disable SpamAssassin
Configure SpamAssassin (required to rewrite subjects)
Spam Box
This feature allows emails identified as spam by SpamAssassin to be delivered to a seperate mail folder named "spam". If this folder is not regularly checked and emptied, it may cause your email or filesystem quotas to be exceeded, resulting in a failure to receive legitimate messages. You can easily use IMAP or Horde/IMP to check messages that are routed to this box. If you wish to use pop3 to check the spam box, just add "/spam" (without the quotes) to the end of your pop3 login. (Example: user@domain.tld/spam)
This feature's use is generally discouraged in favor of sorting and deleting spam messages using your mail client. Without Spam Box you can configure SpamAssassin to mark your email with an identifying subject (e.g. ***SPAM***), which can then be filtered out into an appropriate location.
Enable Spam Box
Disable Spam Box
Clear Spam Box
[Go Back]

blacklist_from	
blacklist_from	
blacklist_from	

Used to specify addresses which send mail that is often tagged (incorrectly) as non-spam, but which the user doesn't want. Same format as whitelist_from.

required_score	3

Set the number of hits required before a mail is considered spam. "n.nn" can be an integer or a real number. 5.0 is the default setting, and is quite aggressive; it would be suitable for a single-user setup, but if you're an ISP installing SpamAssassin, you should probably set the default to be more conservative, like 8.0 or 10.0

rewrite_header subject	****SPAM****

Text added to the Subject: line of mails that are considered spam. _HITS_ in the tag will be replace with the calculated score for this message. _REQD_ will be replaced with the threshold.

score	
score	
score	
score	
score	

Assign scores (the number of points for a hit) to a given test. Scores can be positive or negative real numbers or integers. "SYM-BOLIC_TEST_NAME" is the symbolic name used by SpamAssassin for that test; for example, 'FROM_ENDS_IN_NU'. If only one valid score is listed, then that score is always used for a test. If four valid scores are listed, then the score that is used depends on how SpamAssassin is being used. The first score is used when both Bayes and network tests are disabled. The second score is used when Bayes is disabled, but network tests are enabled. The third score is used when Bayes is enabled and network tests are disabled. The fourth score is used when Bayes is enabled and net-work tests are enabled. Setting a rule's score to 0 will disable that rule from running.

whitelist_from	*.is
whitelist_from	*@edal.net
whitelist_from	
whitelist_from	
whitelist_from	

Used to specify addresses which send mail that is often tagged (incorrectly) as spam; it also helps if they are addresses of big companies with lots of lawyers. This way, if spammers impersonate them, they'll get into big trouble, so it doesn't provide a shortcut around SpamAssassin. Whitelist and blacklist addresses are now file-glob-style patterns, so friend@somewhere.com, *@isp.com, or *.domain.net will all work. Specifically, * and ? are allowed, but all other metacharacters are not. Regular expressions are not used for security