

Whitepaper – Spamfiltering

MailSafe's spamfilter uses a combination of contextual filters and sender reputation (domains, ip addresses and mail routing). Most common antispam and -virus solutions uses a serial model where the filters are used subsequent, in contradiction to MailSafe where the filters are used simultaneously and where the results are mutual dependent.

This method creates more reliable results, but demands more calculations, which in MailSafe is solved by caching of results and other optimizations, and mails therefore passes the filter in less than one second.

This subsequent model creates less false positives, and therefore MailSafe is using more filters than most common solutions which again creates more reliable results.

Our spam filter automatically eliminates "junk" e-mail or "spam" from each user's mailbox, protecting them from unwanted distractions and interruptions. With the ever-increasing amount of unsolicited e-mail arriving daily, protection is an important means of saving time and staying focused on important work at hand.

As e-mail passes through our mail switches, our proprietary spam filter automatically scans inbound e-mail and separates out any spam found.

Our junk mail filter is a system that we have developed in house. We filter spam in a three-step process.

1. Firstly, we use what we call "bait" e-mail addresses. We have hundreds of e-mail addresses that we use to actively look for spam. We take those spam messages and run them through a process that we have created, in which we create a fingerprint for each message. Those fingerprints are added to our database.

2. Secondly, when new e-mail enters our network, we fingerprint each message and cross-reference to our database to see if there is a match. If there is a match, the message is marked as spam.

3. If there is no match, we then run the message through a series of tests in which we look at different aspects of the message including the header, subject, and content of the message. These tests give the message a score and if that score hits a certain threshold, we mark that message as spam.

This whole process takes less than a second to perform.

What happens with the spam? As the administrator, you have four options in regards to the spam.

1. The first, and most popular, option is to leave the junk e-mail on our network. As we catch the junk e-mail, we create a temporary junk e-mail box for each of your users. We then notify each user that they have junk e-mail on our server and we give them a link to a web-based control panel where they can check it. As the administrator, you can set the notification interval. We hold the junk e-mail on our network for 30 days before it is deleted.

2. The second option is to redirect all the junk mail to a single e-mail address. For example, spam@yourcompany.com.

3. The third option is to have Armada insert an x-header. The junk e-mail is delivered to your mail server giving you the ability to reroute the e-mail via the x-header variable.

4. The fourth option is to modify the subject. For example, you could insert the word JUNK before the subject so that the individual users could set up their own filters at the e-mail client level.

Benefits:

- Unique 3-step filtering process catches 98% of all junk e-mail
- Automatic filtering with no maintenance headaches
- Reduces the time-distraction of clearing out unwanted e-mail
- Far less expensive than maintaining own onsite spam filtering system
- Implementation in minutes with a simple change in DNS configuration
- Reduced load on IT staff and mail servers