7 Tips to Keep in Mind When Choosing an Anti-Spam Solution

Ask any administrator who is responsible for ensuring a company's email infrastructure is as spam free as possible what they're job is like, and they will answer that it is like fighting an ongoing battle.

Just like in a regular battle, you can expect some collateral damage. Collateral damage in an anti-spam solution context is when legitimate emails end up classified as spam, thus never reaching their intended recipient. This means that any server anti-spam solution you employ has to be tweaked to only stop real spam. This is achieved by applying the right technologies and the right settings.

However, no amount of technology and tweaking will give you 100% accuracy. Therefore, you will almost certainly end up with some legitimate mails being erroneously classified as spam. In the event this happens, you need to ensure you have a system in place to allow administrators or users to quickly and safely check for legitimate emails that have been misclassified and action them.
There are several technologies that can be useful in detecting actual spam emails, as well as keeping the rate of false positives to a minimum.

Here is a list of some of the most effective features to help you to decide which ones are most important for you:

1. Whitelisting: Whitelisting allows you to provide your anti-spam solution with either a list of emails or domains. Any email that matches those criteria will never be marked as spam. Some advanced server anti-spam solutions will automatically whitelist the email addresses of recipients you send email to.
2. Databases: Some solutions maintain databases that they regularly update which contain finger print data and other information that can be used by the anti-spam solutions to detect spam.
3. Greylisting: This system will reject any email from a new source with a temporary error. Many spam mailing systems do not follow email standards and will not try to resend the email again, as legitimate email servers will.
4. SPF (Sender policy framework): This system depends on an email's source domain to list the email servers that are authorized to send

on its behalf. This can be very helpful, especially when combating phishing emails that generally try to spoof legitimate domains to create a false sense of security. When an email for a domain is received from an unauthorized source, it is marked as spam.

5. DNSBL (DNS blocklist): This is a system maintained by various third parties that use the DNS system as a database of sorts. Different providers provide different functionality, but essentially they all will allow the solution to query the database and check if the IP address which an email originates from has ever been caught sending spam.
6. Bayesian: Bayesian is a technology where a statistical analysis is run on an email to determine if it is spam or not based on its content. This technology requires training with spam and legitimate emails to keep it up to date with the latest spam trends. This training can either be performed by the vendor, or even by your organization itself.
7. Quarantine System: A quarantine system is a kind of vault in which spam is kept when caught. This can then by reviewed by either administrators, or in some solutions you can also allow review by the recipients themselves. The email can then be marked as legitimate if it was wrongly classified.

These are some of the most popular advanced technologies that can be used to detect spam. Choosing which one, or which combination, to deploy can help ensure your server anti-spam solution is an effective tool for the constant battle against spam.