



Tarragon Solutions Ltd – SMTP Feed with SPAM + Virus Filtering

http://www.tarragon.co.uk/Website_Hosting.asp?ID=7

SMTP Feed with SPAM + Virus filtering has been designed to filter out junk for those customers that route email to their own mail servers, a typical example of which is a Microsoft Exchange server on an ADSL line or a dedicated server.

SMTP Feed with SPAM + Virus filtering works on our powerful spam filtering servers to provide your network with the ultimate protection against harmful Spam and malicious virus email, without the need to invest in expensive software or network management tools. This includes filtering of an unlimited number of recipient addresses and emails for 1 domain (e.g. @YourCompany.co.uk).

Creating SPAM Filtering Account

We will need the following information:

- External IP address/Hostname.
- Domain Name.
- List of all the email address's that you want to except email for.
- How do you want SPAM to be treated?
 - Redirected to a specific email address. (Must be the same domain.)
 - Indicated in the Subject line and delivered to the original recipient.
 - Deleted

Note that virus mail is deleted automatically, regardless of the method selected above.

NOTE: It is important that the destination mail server has TCP Port 25 Open and accepts mail for the selected domain. It is also advised your server's Internet connection is provided with a Static IP Address.

Post Installation

Once SMTP Feed with SPAM + Virus filtering has been setup for you, you must alter the domain's DNS MX record to take advantage of the facility.

spam0.interdns.co.uk	PRIORITY 0
spam1.interdns.co.uk	PRIORITY 0
spam.interdns.co.uk	PRIORITY 0
spamsec.interdns.co.uk	PRIORITY 20

If your systems are locked down to except email from specified IP addresses please find them below:

83.170.96.20
83.170.96.21
83.170.96.22
83.170.96.23
83.170.96.24
83.170.124.50
83.170.124.51

83.170.124.52
83.170.124.53
83.170.124.54
208.43.81.187
174.36.195.11
174.36.195.12
174.36.195.13
174.36.195.14
174.36.195.15

SPAM + Virus Filtering Options

White + BlackLists

In the unlikely event of an email being considered spam incorrectly, you can add the user's from address in the whitelist so all future mail from that source will be allowed through, regardless of its content. Likewise with the 'Blacklist', senders specified in here will always be considered spam regardless of their content.

How SPAM Filtering works

SPAM Filtering is based on the world renowned SpamAssassin software. This essentially works on a combination of 'tests'. Each email is checked against a series of tests where points are scored. This scoring system combined with the quantity and diversity of tests performed means that unlike most competing products, the likelihood of SPAM Filtering incorrectly identifying a message as spam is negligible and makes it nigh on impossible for spammers and virus writers to craft their messages to bypass the filters.

You can adjust the sensitivity of the Spam Filter to suit your needs. Generally the default settings are suitable for the majority of users. However, should you be seeing an increase in spam that has not been caught, consider increasing the 'Sensitivity' of the Spam Filter as described on the settings page.