What is Greylisting?

Greylisting is a method of blocking spam by temporarily rejecting emails coming from unknown senders. If the email is legitimate, the originating server in most cases will re-attempt to send it, which will then be accepted by the recipient mail server. It is observed that most spamming servers do not try to resend the email in case of a first time rejection.

How does Greylisting works in MailScan?

The MailScan Greylist feature will record the following triplet information from each incoming email message:

1. IP address of the Host
2. Sender email ID
3. Recipient email ID

The triplet is checked against the record maintained by the MailScan Greylist feature. If this triplet has never been seen before, the e-mail is rejected and the triplet information is stored. Based on the retry interval set, the sending server will attempt to deliver the e-mail.

On the next hit MailScan will once again check for the triplet information present in its records. If an email, whose triplet matches with the stored record, is received within 5 minutes of its first rejection MailScan will once again reject it. MailScan will accept emails only if the triplets match and are received after 5 minutes of its first rejection.

MailScan accepts an email if the above criteria are met and the triplet information of such emails will be cached to the Greylisting Whitelist database in MailScan. This information will remain in the MailScan database for 30 days. After every 30 days, the Greylisting Whitelist is refreshed.

Similarly, the Triplet information, which contains IP address of the host, sender and recipient email ID, is temporarily stored in the MailScan server cache for 7 hours. After every 7 hours, the Triplet information list is refreshed.