
Greylisting

An anti-spam measure

Safeserve.com Ltd.



Contents

Safeserve Greylisting 4

 What is Greylisting? 4

 Why use it? 4

 How is it used? 4

 Who gets greylisted and when? 5

Safeserve Greylisting

What is Greylisting?

Greylisting is a relatively new anti-spam technique used to block a high proportion of spam before it is even transferred to the mail server, thus not only reducing spam delivery rates, but also saving valuable network and CPU resources on the mail server and improving performance for genuine emails.

Why use it?

Spam now accounts for a huge proportion of all email, with some estimates putting it over 90%. Conventional anti-spam techniques are not perfect, and so any additional anti-spam measure is always welcome. Greylisting also has the advantage that it blocks spam before it has even been delivered to a mail server. This reduces the volume of email that needs to be processed with traditional anti-spam devices that are very CPU intensive, and it also saves network bandwidth, as the bulk of the email is never transferred to the server. The net result is increased performance by the mail server, and thus an increased quality of service to clients.

How is it used?

Emails are sent using something called Simple Mail Transfer Protocol (SMTP). When a machine (from now on referred to as the client) has an email it wishes to send, it opens an SMTP dialogue with a mail server (from now on referred to as the server) to facilitate the sending procedure. Exactly how that machine came to have this email (be it a client workstation, or another mail server), and which server it is trying to send to are irrelevant and beyond the scope of this document.

The first thing that happens during this dialogue is the two machines exchange data regarding their identity, set some options regarding the sending procedure, and then the client informs the server who the email is from, and who the email is to. If this stage is passed, the data (i.e. the actual email) is transferred, and then the connection is closed.

Greylisting works by detecting whether an email is spam or not during this initial exchange of information. It does this by tracking who the email is claiming to be from, and who it is being sent to. When the to and from information have been exchanged, if there is no previous record of the sender successfully sending an email to the recipient, then the email is rejected with an SMTP code 451, which means "Requested action aborted: local error in processing". This is known as a 'soft' failure. 'Hard' failures are failures which are permanent, e.g. a domain not existing. 'Soft' failures are regarded as temporary failures, and the client should respond to such a failure by trying to send the email again after a short pause. This is detailed in the RFCs, with increasing emphasis over time. Originally RFC 821 stated that a client "should" reattempt delivery at a later time. This was later

clarified with RFC 2119, which clarifies that “should” is a strong recommendation to be ignored at the client’s risk. RFC 821 was finally replaced with the current standard (at time of writing), RFC 2821, which states that “the SMTP client retains responsibility for delivery of that message” and “mail that cannot be transmitted immediately **MUST** be queued and periodically retried by the sender”.

After a short pause (the exact length is configured on the client), the mail will be resent. At this point, the mail will be accepted for delivery by the server, and processed as normal (including traditional spam and virus checking).

The reason this blocks spam is because the vast majority of spam is sent from what are known as Zombies. These are hacked machines that are then programmed to send out spam without the user being aware of it. Unlike proper mail servers, which are always on, Zombies are usually on people’s workstations which may be turned off at any moment, and as such have little time for the niceties of sticking to proper conventions. They tend to be more concerned with sending out in bulk, and are usually not very sophisticated. As such, if they receive a ‘soft’ failure, in the vast majority of cases they give up and continue sending to other addresses, unprotected by greylisting. This has been vindicated by the fact that over 80% of all spam blocked by Safeserve is blocked by greylisting. Tests have shown that the vast majority of this would subsequently be caught by our other anti-spam measures, however some may not be and the subsequent barrage of email to process would certainly have reduced the service to our clients.

Who gets greylisted and when?

So exactly how does the server decide who does and does not get greylisted?

The first thing to consider is the initial block. An email is blocked if and only if there is **NO RECORD OF THIS SPECIFIC SENDER SENDING TO THIS SPECIFIC RECIPIENT IN THE LAST 90 DAYS**. If the email is sent to several people, some of whom there is a record of this sender sending to previously and some of whom there is not, then the email will be accepted for delivery to some recipients and not to others. Greylisting is carried out on a per-recipient basis, not a per-email basis. If no email sent from a given sender to a given recipient for 90 days, then the record expires and the next time an email is sent from that sender to that recipient, greylisting will occur again.

After the initial greylisting, the sending mail server must wait **ONE MINUTE** before the redelivery will be accepted. After this period of one minute, if the server receives another email between the same sender and recipient, the email will be allowed through, and this sender-recipient combination will be added to the database to allow subsequent emails.

After this period of one minute, the server will accept delivery of the email for **UP TO 25 HOURS AFTER THE INITIAL DELIVERY ATTEMPT**. If no attempt to resend the email is encountered within this period, then the next email between this sender and recipient will be greylisted again.

Experience shows that the redelivered delay varies from company to company. Most attempt redelivery after about 10 minutes. Some attempt

after only one or two. Others (though these are rare) can wait up to three hours. All reputable email providers will attempt redelivery at some point.

The net result of this measure is that the first time you receive an email from a new sender (or the first time an old sender sends you an email in 90 days) that email will arrive with a short delay. After that, emails between you will arrive as normal. If a sender sends to a colleague regularly, but has never sent to you, then an email to both of you may arrive at different times as one is delayed and one is not. This is normal.

It is possible, though *extremely* unlikely, that a genuine email may be blocked by greylisting. Emphasis has been placed on the extremely, because as shown above Internet standards very clearly state that an email that could not be delivered on the first attempt due to a 'soft' failure MUST be resent. No reputable email provider will fail to resend in such circumstances.

In the unlikely event of this happening, the sender should contact their email provider to inform them of the problem, and enquire why they are not abiding by RFC 2821. If the problem is not fixed immediately, then we strongly recommend that the sender change email provider, as this may be causing problems sending to a large number of companies, not just Safeserve's clients.

Unlike our other antispam measures, Safeserve cannot archive spam emails blocked by greylisting, as the email itself is never transferred to our server. If you understand the risks and would prefer to have greylisting disabled for your domain, then please inform us; however be aware that we reserve the right to levy a charge for such a change, as it may result in a significant increase in use of our resources.