Adept

Managed ICT Services & Solutions

Introduction to Greylisting

The term Greylisting is meant to describe a general method of blocking spam based on the behaviour of the sending server, rather than the content of the messages.

Greylisting is a method that is being used all over the world as the first line of defense against spam. It is a simple yet effective way to eliminate most of the spam emails reaching a recipient.

1. What is Greylisting and how does it work?

Greylisting is set up on mail servers to temporarily reject sender email addresses and mail server IP addresses that it does not recognise. The reason for this is when a spammer sends out an email to however many recipients it is normally only sent once. If an email reaches our mail servers and the sender/IP is not recognized, we temporarily "defer" the email. If the sending server does not resend the message, then the spam will not reach the recipient email address. This is why Greylisting is so effective and why it filters out most spam emails.

Legitimate mail servers should be configured to receive the temporarily deferred message, add the message to their mail queue, and resend the email within a few minutes (if you ever see a Greylisting error message sent back to you it means the mail server you used for sending email is not set up correctly).

Once the email is sent again our mail servers will recognise the sender/IP and allow the email to go through. Our servers keep record of valid senders/IP's for 30 days, so if you send an email again within that time you will be recognised and your email will go through without being greylisted again. If you only send an email again after 31 or more days, you will be greylisted again. Whenever you send an email, your email address is stored as a valid sender for 30 days.

Adept Internet's mail servers are set up to greylist a sender/IP for 2 minutes. If the sending mail server tries to resend the email after 1 minute it will be greylisted again. This will happen until the sending mail servers waits the required 2 minutes before resending the email, at which point our servers will accept the email and store the sender/IP in the database of valid senders/IP's which will be kept for 30 days.

2. Examples of Greylisting errors

Greylisting errors will always have an error code of 4xx with the most common code being 450. Note that any error code starting with 4xx is always a temporary error.

Below is an example of a Greylisting notification generated by our mail server:

- example@adept.co.za
- SMTP error from remote mail server after RCPT TO:<example@adept.co.za>:
- host mail.adept.co.za [x.x.x.x]: 450 4.7.1 <example@adept.co.za>:
- Recipient address rejected: Policy Rejection- Greylisting. Please retry in 2 minutes.: retry timeout exceeded.

Below are other examples of Greylisting notifications that you might encounter:

- <mail.example.co.za #4.0.0 smtp;450 <example@example.co.za>: Recipient address rejected: Greylisting in action, please try again later>
- 450 4.7.1 <address>: Recipient address rejected: Greylisted
- 450 4.7.1 <address>: Recipient address rejected: Policy Rejection.
- 451 Message temporarily deferred - [160]

Email support@adept.co.za
Tel +27 (0)21 888 6500
Fax +27 (0)21 888 6600

2nd Floor DataVoice House, 16 Elektron Avenue
Techno Park, Stellenbosch, 8301
www.adept.co.za

Adept Internet (Pty) Ltd.
Directors: J. Pietersen, G. le Grange
Reg. 1984/001310/07

3. Information we need to troubleshoot Greylisting problems

In order to troubleshoot Greylisting problems we will require the same information as with other email errors:

- Sender address (the address that you sent from)
- Recipient address (the address or addresses that you sent to)
- Date sent (If you are overseas, we preferably need a time stamp/zone too, for example GMT +4)
- SMTP server
- Error message
- Email headers

4. FAQ: What happens if the sending mail server doesn't try sending the message again?

If a sending mail server receives a 450 temporary rejection error code, it is required by Internet standards to retry sending the message (mail servers that are not configured to resend emails are faulty and needs to be corrected). This is very important because any mail server that will not retry to send the message will not be able to deliver emails to any server that uses Greylisting.

This will normally be one of the few times you will actually see a Greylisting error message sent back to you as the sender.

This will also cause problems with other temporary errors so it is not just Greylisting that will have problems with incorrectly configured mail servers.

5. FAQ: Where do Internet standards say that retrying is required?

The technical explanation of why retrying is required is that RFC 2821** defines a 450 error code as a "Transient Negative Completion reply" in section 4.2.1. Then, in section 4.2.5, it specifies that if an SMTP mail server receives such a reply, it must continue "retrying delivery some reasonable number of times at intervals as specified in section 4.5.4." Finally, section 4.5.4 says "mail that cannot be transmitted immediately MUST be queued and periodically retried by the sender", and that retrying should continue for "at least 4-5 days".

** Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviours, research, or innovations applicable to the working of the Internet and Internet-connected systems. See http://www.rfc-editor.org/rfc.html

6. FAQ: I run a mail server, and some users say we are being blocked. How do I get off your list?

Greylisting does not use a "blacklist". There is no centralised list to request checking of your server, or to request removal from. The reason your mail server is getting blocked is most likely that it does not properly handle 4xx SMTP error codes, and does not retry delivery within a reasonable amount of time after receiving such a code. Please see RFC above where it states that your mail server MUST be set up to resend emails.

7. FAQ: My email provider uses Greylisting, and a few people are reporting mail to me is bouncing. What's happening?

There are a few mail systems that do not properly follow the email protocols as defined by the RFC standards specifications. Due to this failure to follow the standards, bounces may be generated from their sending server when they shouldn't. This could be due to the mail server being configured incorrectly or the mail server software being outdated.

The best solution is to have the people getting the bounces get in contact with the system administrators of their email system, and have them upgrade to a version that is standards compliant.

8. FAQ: Can I use Greylisting on my personal mail account?

Because Greylisting methods are designed to work at the mail server level, unless you have control of your own mail server, or your ISP has installed a Greylisting implementation for you, you will not be able to take advantage of Greylisting.

9. FAQ: I do not want Greylisting, can you remove it from my email address?

Please send an email to support@adept.co.za requesting that we remove Greylisting from your address(es).

10. FAQ: I use Adept's Authenticated SMTP, will my emails get greylisted?

If you send emails to Adept hosted email addresses you will not be greylisted by our mail servers. However, other ISP's might still greylist you on their mail servers.

11. FAQ sources

http://projects.puremagic.com/greylisting/index.html
http://support.tigertech.net/error-grey

Links to other Greylisting sites for further explanations and information:

- http://en.wikipedia.org/wiki/Greylisting
- http://www.greylisting.org/
- http://projects.puremagic.com/greylisting/index.html