Email bouncebacks with server rejection error (or: SPF Records and You)

The Symptoms Exhibited by the Patient

With the never ending fight against the ocean of spam, email providers are increasingly tightening their standards that mass emails need to follow. We are seeing increasing amounts of bounce back emails due to this.

When a client is having issues with bounce backs, the important thing to do is to segment the reasons and tackle them one at a time. The main reasons you will see in bounce back messages are these:

a) "A connection attempt failed because the connected party did not respond properly after a period of time" or something similar. The receiving server was offline for some reason. This is beyond any control of ours or the clients.

b) "Too many connections" or something similar. If too many emails are sent simultaneously to the same recipients, the receiving server will but up a temporary block to thwart potential spam. Only send one eNotification at a time to prevent this.

c) Receiving email address does not exist. Obviously that email address has been deleted. These need to removed right away as repeatedly sending to non-existent emails can get you blacklisted

d) 553 - Rejected. There are other numbers and messages, but they will frequently mention an authentication or permission fail. This is the reason this article will focus on

The Cause

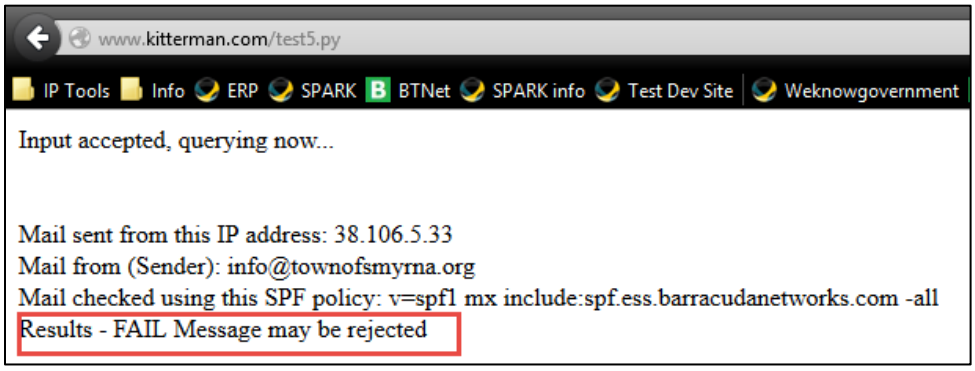
When we host a client's website and they use the eNotifications the emails are sent out from our servers. This will be noted in the header of the emails, but the "From" line in the body of the message will say it is coming from the client domain.

This means that an email that begins like this:

From: info@townofsmyrna.org
Sent: Tuesday, January 27, 2015 8:28 AM
To: John Doe
Subject: Town Centre Lunch Menu

This message will have buried out of sight in the header the fact that this message was actually sent by enotification.visioninternet.com but claims to have been sent by townofsmyrna.org. As you would imagine, this would potentially raise a red flag at the email provider who receives this message. This is good practice because many scam emails are sent out that claim to be from bankofamerica.com, but in the header the ISP sees that it actually was sent by scamallyourmoney.scam.

Here is an example how what happens when an email such as this is sent by our servers and the SPF record does not authorize us:



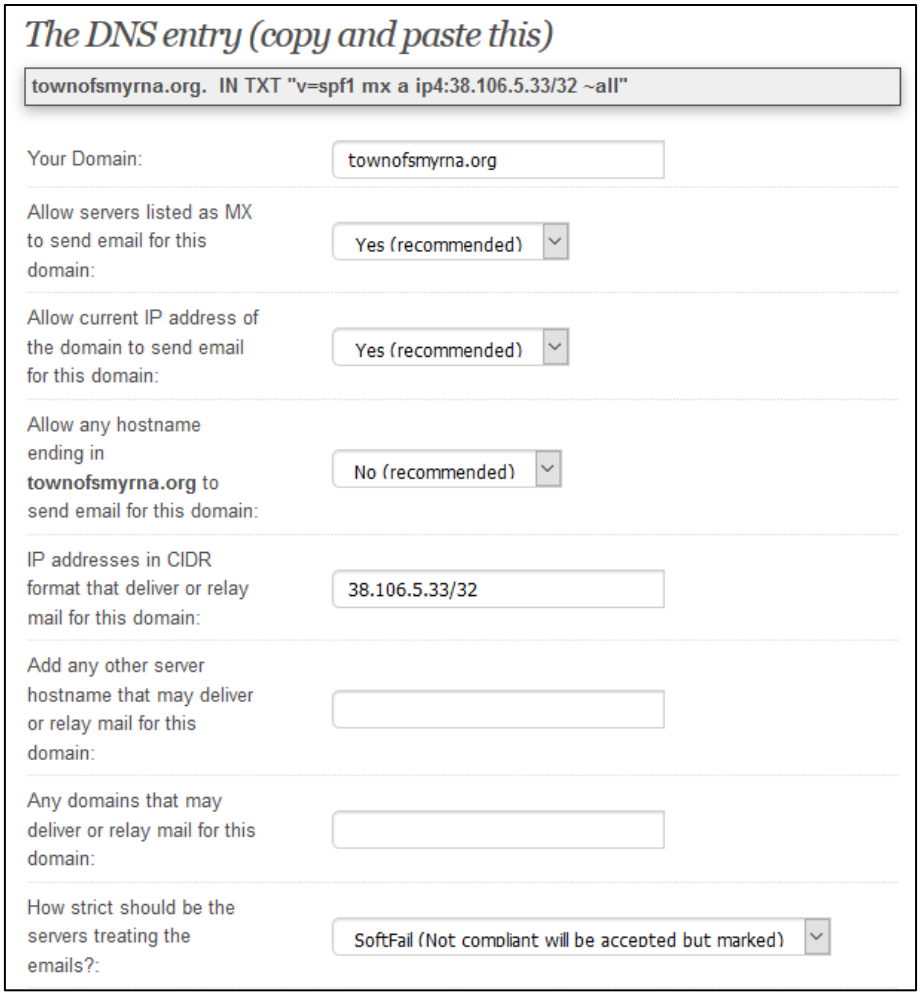
The SPF record in this example does not authorize our eNotification server, and the "-all" at the end tells the receiving email server to fail a message that does not pass.

The Cure

Sprucing up the SPF text entry is actually much easier than you would expect. The entry is nothing more than a little string of text that instructs anyone reading how to treat incoming emails.

There is an incredibly handy site called spfwizard.net where you can quickly enter your settings and the site will build the SPF entry for you. Now you just pop over to your DNS provider and tell them to use the new text for the SPF entry.

The easiest way to add our email server as an authorized sender on your behalf is to add this in the "IP address in CIDR" field: 38.106.5.33/32



Now that our server has been added you will get this happy result!

Finally, this super useful site can test the SPF record to confirm it:
http://www.kitterman.com/spf/validate.html