Spam Wars Episode III - Revenge of the SPF

Posted At : November 3, 2005 11:47 AM | Posted By : Mark Kruger
Related Categories: Hosting and Networking

Yesterday and today I've joined the SPF bandwagon. SPF or "Sender Policy Framework" is a way of trying to back track an e-mail's domain and figure out if the server is legitimate . It does this by adding what is essentially a mask or pattern to a simple text record in the DNS server. For example, you can specify that all mail from a domain should be rejected *unless it originates from a particular server or domain*. You might dictate that mail must come from servers listed as MX records, or you can specify an "A" record. If your data center has just a few subnets you could specify a range of IP addresses. Pretty neat huh?

Sample SPF record

If you are worried about fiddling with DNS records don't panic. SPF records (for the time being) are strings that are added as part of a long standing but little used DNS record type called "TXT". Here's a sample DNS record from my BIND 9 server (with a few edits).

```
@   IN   SOA   ns1.cfwebtools.com. webadmin.cfwebtools.com. (
         2005060901
         7200
         3600
         604800
         86400 )
;
          IN NS   ns1.cfwebtools.com.
          IN NS   nic.tekindustries.com.

mail IN A 66.37.232.195
www IN A   66.37.232.205
cfwebtools.com.    IN A   66.37.232.205
cfwebtools.com.    IN MX 10 mail.cfwebtools.com.
.... bunch of other hosts....
cfwebtools.com.   IN TXT   "v=spf1 ip4:66.37.232.199 ip4:66.37.232.195 -all"
```

That last record with the string *"v=spf1 ip4:66.37.232.199 ip4:66.37.232.195 -all"* says that cfwebtools.com mail is only supposed to come from 1 of 2 IPs. There are lots of other ways to do this, but if you have a relatively small operation like ours, this works well.

The Downside

Ok, so I added SPF records what now? The truth is that a mail server must be configured to honor SPF records and go check them. That means people can still send out forged emails that are passed through servers that are not "SPF Aware". Since this is very simple code and email servers already do lots of DNS querying, the good news is that many of them already support SPF. Our inexpensive mail server made by Argosoft supports it, as does our more expensive mail ap by smartertools. Spam Assassin has an SPF module you can add as well. Still, it will require everyone in the business to "climb aboard" and make use of the technology before it is adopted.

AOL is one very large player that is already configured to use SPF. They are requiring white list premier partners to add SPF records to DNS in order to send mail to their

domains. That usually means that other big players will follow suite shortly (yahoo, hotmail etc).

Competing Technologies

There is another technology called the "sender ID" framework that is billed as a "competing" technology. I do not know anything about it, but I assume it has more to do with employing something on the client. I like the fact that I can support SPF by making server configuration changes alone and avoid instructing users of email on how to configure a client - a daunting and money losing proposition.

Additional Resources

Probably the best, most readable explanation of SPF can be found in **Mark Minasi's Newsletter** this month. You have scroll past all the stuff at the top. It's about half way down (Mark hasn't learned to use named anchors yet :). Another great Site is **http://spf.pobox.com/** which I suppose is one of the major players behind the effort - and their site doesn't look like it was designed by a guy in a bath robe in his mom's basement (..source forge - cough cough). They have a nifty "**wizard**" that can create a DNS record for you - handy if you are DNS challenged. There are also some nice **instructions** for configuring mail headers to be SPF compliant. See my **previous blog** on working with mail headers for a bit more on that. James Moberg has some nice tips in the comments.