

Re: SPF = Sender Policy Framework (was: Microsoft spam solution<snip>)

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.misc/2004-09/1939.html>

From: Norman L. DeForest (af380_at_chebucto.ns.ca)

Date: 09/21/04

Date: Mon, 20 Sep 2004 23:27:28 -0300

On Mon, 20 Sep 2004, Randolph Richardson wrote:

> *"Dave Uhring <daveuhring@yahoo.com>" wrote in news.admin.net-abuse.email:*

>

>> *On Mon, 20 Sep 2004 05:02:55 +0000, Randolph Richardson wrote:*

>>

>>> *Regardless of how I configure my DNS zone to return a different IP*

>>> *address for "netware.inter-corporate.com," the root servers will*

>>> *override this by providing the information specified in the host*

>>> *record. This also seems to speed up DNS resolution a little bit, by the*

>>> *way, because the root servers don't have to take additional steps to look*

>>> *up external NS records.*

>>

>> *I also think that someone is putting something over on you:*

>>

>> *Non-authoritative answer:*

>> *Name: netware.inter-corporate.com*

>> *Address: 24.87.56.253*

>>

>> *Authoritative answers can be found from:*

>> *inter-corporate.com nameserver = netware.inter-corporate.com.*

>> *inter-corporate.com nameserver = oc48.inter-corporate.com.*

>> *inter-corporate.com nameserver = fast01.inter-corporate.com.*

>> *oc48.inter-corporate.com internet address = 64.251.89.8*

>> *fast01.inter-corporate.com internet address = 64.251.89.88*

>>

>> *Suppose you turn off those three DNS servers and then attempt to resolve*

>> *some host whose zone records are maintained there.*

>

> *I'm aware of how this is all configured. Of course, if I turn off my*

> *DNS servers and wait for caches to expire, the only items that will resolve*

> *are the registered name servers.*

>

> *I know it works this way too because I've run across a few registered*

> *host names that resolved in the past, yet the IPs they resolved to weren't*

comp.os.linux.misc: Re: SPF = Sender Policy Framework (was: Microsoft spam solution<snip>)

- > *running any DNS servers (queries against them simply timed out). The only*
- > *reason I discovered these was when I was troubleshooting eMail delivery*
- > *problems for clients.*

Did you make the queries from your own system or did you use a web-based DNS lookup that started the DNS query from outside your (and your customer's) system?

One catch is that your system has to start querying **somewhere** and the IP address for the nameserver that answers that first DNS query has to be entered into your system configuration. (One of the entries I had to make for my PPP connection is enter the IP addresses for the primary and secondary nameservers to use.) If the IP address of **that** nameserver is still present in your system configuration and the machine at that IP address is still providing DNS service (including serving information from its own zone files), it can still answer your queries even if the DNS entries for that nameserver are no longer in the root servers or any server accessible through the root servers. You may have been querying an otherwise unreachable nameserver that contained the zone files for your customer's systems.

So even if ns1.foo.somplace.invalid no longer resolves for others, if you have the IP address for the ns1.foo.somplace.invalid nameserver in your configuration and ns1.foo.somplace.invalid still thinks it's OK, then ns1.foo.somplace.invalid will return the DNS for itself or any other otherwise unreachable system in its zone files that it thinks it's authoritative for. Or your secondary nameserver elsewhere (if you had one) may have been answering the queries.

One advantage of this is that, even if a major datapipe is cut and the main DNS servers are unreachable for you (cutting you off from the rest of the Internet until things are fixed), you can still access other machines on your own network using the local DNS server in your system configuration.

One disadvantage is that you may need some way to bypass that nameserver when you have to in order to troubleshoot DNS problems — including the possible need to know the IP addresses of the root nameservers in order to query them (something that may have to be looked up in advance of problems and something that may have to be done on a regular[1] basis to ensure you have correct info).

[1] Since I don't know how often root nameservers change IP addresses, "regular" could mean once per week, once per year, once per decade, or once per century. (/me off to read some more and try to eliminate some more ignorance.)

--
Norman De Forest <http://www.chebucto.ns.ca/~af380/Profile.html>
af380@chebucto.ns.ca [=| |=] (A Speech Friendly Site)
"One suspects that by now even **Nigerians** have Nigeria blacklisted ;)."
-- Jim Seymour on 419 scams, news.admin.net-abuse.email, Tue, Nov 19, 2002

Re: SPF = Sender Policy Framework (was: Microsoft spam solution<snip>)