Subject: HELO and IP Matching?
Posted by smorris on Thu, 03 Mar 2005 19:05:34 GMT
View Forum Message <> Reply to Message

Is there a way to test whether the HELO/EHLO domain name match the IP address and PTR record that are coming in?

Subject: Re: HELO and IP Matching?

Posted by support on Fri, 04 Mar 2005 09:32:46 GMT
View Forum Message <> Reply to Message

What should we compare? SMTP does not require that the HELO name and the real hostname have anything to do with each other, so rejecting a mail if they do not match would block lots of legit mail as well.

So some small positive spam score would be in order, and this seems is exactly what SpamAssassin is doing already. It looks as if the rules in the file 20_fake_helo_tests.cf do RDNS lookups. They have scores in the range of 1 to 2 points.

Subject: Re: HELO and IP Matching?

Posted by smorris on Fri, 04 Mar 2005 13:41:19 GMT
View Forum Message <> Reply to Message

I don't care about the real hostname. What I care about is whether the IP address that is actually talking to me matches the HELO entry... this is an important thing for folks who are spamming where the PTR entries often don't give the same information as the HELO.

I suppose I could also just up the points on that entry... Just gotta remember to do it again with every upgrade! :)

Subject: Re: HELO and IP Matching?

Posted by smorris on Fri, 04 Mar 2005 14:05:43 GMT
View Forum Message <> Reply to Message

Ok... So where do I modify that score?

Subject: Re: HELO and IP Matching?

Posted by support on Fri, 04 Mar 2005 14:15:41 GMT
View Forum Message <> Reply to Message

All scores are set in 50_scores.cf, but you can override them in other files. If you put your overrides into local.cf, they will even survive upgrades. Like this:

```
score   FAKE_HELO_AOL       5.6
score   FAKE_HELO_YAHOO_CA  27.0
...
```

Subject: Re: HELO and IP Matching?

Posted by smorris on Fri, 04 Mar 2005 23:17:02 GMT
View Forum Message <> Reply to Message

Yeah... Ok, found that... but looking at the CD with the HELO items in it, those are each for specific domain structures of places that shouldn't really house e-mail servers.

It's not really anything about a basic IP-level check for whether the HELO given resolves back to the IP address that shows up in the source field of IP packets for the current connection. (Or PTR of the IP matching the HELO name)

Hmmmm...