

Re: Fully spam/virus filtered mail, and reliable outbound relay

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2004-06/2012.html>

david20_at_alpha2.mdx.ac.uk

Date: 06/14/04

Date: Mon, 14 Jun 2004 12:23:20 +0000 (UTC)

In article <40cd4c4d\$0\$62725\$ee9da40f@news.wanadoo.nl>, Frank Slootweg <this@ddress.is.invalid> writes:

>Barry Margolin <barmar@alum.mit.edu> wrote:

>> In article <40cb421a\$0\$227\$4a441750@news.wanadoo.nl>,

>> Frank Slootweg <this@ddress.is.invalid> wrote:

>>

>>> For the record, I do not expect them to allow me to *run my own
>>> server*, but I do expect them to allow me to *access other servers*.
>>> After all what I 'buy' is mainly *Internet* access (as in the "I" of
>>> ISP). Suddenly they decide that Internet access excludes other mail
>>> servers. What's next? That they decide that I can no longer access
>>> other (or specific) websites? Or other News servers? Or (specific)
>>> Newsgroups? Or ...

>>

>> If people bypassing their ISPs' news servers were causing a major
>> problem for almost all Internet users, I would expect them to take some
>> action.

>>

>> This stuff is all "necessary evils", due to the enormous problem of spam
>> and email-borne malware. Do you think ISPs are implementing these
>> blocks capriciously?

>

> Well, IMO, *too* capriciously. I am more is Chris' camp, i.e. only
> block those who actually cause problems, but I also understand Leythos
> economic arguments (I just don't (want to) agree with them! :-)).

>

> Anyway, ss I've shown, they do not really stop the (virus/spam)
> problem, they just re-direct it via their mailservers. I have yet to
> see that they take any action against the culprits (both the spammers/
> virus-writers and the ISP customers who do not (sufficiently) protect
> their systems).

Any ISP (or any other company) that is blocking port 25 to force mail through their mail servers should be running anti-virus software on their mail servers.

Blocking Spam is more problematic since often one recipient's spam is another

recipient's important mail message.

I'm not aware of this rate limiting software for port 25 connections but would have thought that the ideal way to implement that would be on the ISPs central mailhub limiting the number of connections from internal users sending mail rather than on the ISP's external firewall which is where you would have to limit it if allowing direct connection to external sites on port 25.

Generally I think blocking access to port 25 on external sites and forcing users to send through the organisations mail server is a good idea. However forcing the user to use the ISPs from/return address is not a good idea. Most ISPs had experimented with and dropped that idea years ago.

However with the rise of SPF and similar schemes the idea has gained a new respectability. One of the problems with SPF is the employee sending from home through the ISP who currently forges his from/return-address to be his employee mail address so that replies go to his works account. (If instead he sends directly through his works mail server by connecting to it on port 25 he will not be able to send to anyone outside his organisation because of anti-relaying rules.) SPF suggests that to get around this problem the employer configure his mail server to use SASL so that the user authenticates before sending his mail and is thus allowed to bypass the anti-relaying rules. However this depends on the user being able to connect directly to his employers mailhub on port 25 from his ISP.

In other words you can implement either

Banning of forging from addresses (with or without SPF)

or

Banning of connection to external hosts port 25

You should not do both !!!

If SPF takes off then banning of connections to port 25 on External hosts will no longer be possible which in my opinion will make stopping the spread of viruses more difficult.

David Webb
VMS and Unix team leader
CCSS
Middlesex University

*>Also I understand from a posting somewhere (in this
>thread? or cmm?) that it is possible to rate-limit (i.e. maximum X
>messages (SMTP sessions?) per hour) access to (external) outbound port
>25. IMO, *that* would be the sensible thing to do (in *addition to*
>taking action against the culprits).*