

Re: Spam in Mail Queue

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2007-11/msg00881.html>

- *From:* "Rich Matheisen [MVP]" <richnews@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 12 Nov 2007 10:24:02 -0500
-

Andel <Andel@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Many thanks Rich... however,

To prevent your server from accepting email that it can't deliver, enable "Recipient filtering" at the global level (check the box that says "Filter recipients who are not in the directory". Then enable recipient filtering on the SMTP Virtual Server.

RF is selected. Spam still sits there...

Recipient filtering won't prevent spam from being delivered to addresses that exist in your directory, just as connection filtering won't prevent spam.

Spam comes from many places. It's most commonly identified by content, not by source. The only time "source" prevents spam is when you make a policy decision that you're not going to accept connections from someplace, no matter what. That means you won't accept "ham" from that source, either. Sometimes that's a good policy, sometimes it's a not so good policy. But, either way, it's not going to prevent spam from being delivered to your system.

You said, in your original post, "they're spam aimed at non-existent users within the company". That shouldn't happen if recipient filtering is correctly enabled. Remember, you must enable recipient filtering in two places. One is in the "Global settings", the other is on the SMTP Virtual Server. It's a common mistake to just enable it in the Global settings and forget the virtual server.

can i adjust the expiry at all?

Sure. It done from the SMTP Virtual Server's property page, on the

Re: Spam in Mail Queue

"Delivery" ab.

If there is spam in the queue to be sent out but is not from or to my domain and yet the server is not SMTP relay, what does that mean?

Well, forget spam for a moment. If your server is accepting email that is for a domain that isn't in one of your Recipient Policies then your server is either 1) allowing unrestricted SMTP relays, or 2) it's allowing authenticated users to relay and you have a weak password on one of the common users (administrator, postmaster, iusr_<server>, etc.), or a "regular user's password has been cracked, or 3) you're allowing IP addresses or address ranges to relay and you've incorrectly entered one of the values (most commonly that would be an incorrect network mask), or 4) you have the "Guest" user enabled in the AD, 5) you have a SMTP connector with "*" as the address space and you checked the box labeled "Allow messages to be relayed to these domains".

If it's an authenticated user that's relaying you have two choices. 1) disallow authenticated users from relaying, or 2) immediately change all your passwords — and use something that not easy to guess.

If you allow relaying for IP address ranges, verify that what you've configured is correct — or remove them altogether.

If the "Guest" user is enabled, disable it.

If you allowed relaying on a SMTP connector, uncheck the box.

You can also run the Exchange Best Practices Analyzer (ExBPA). It may point out other problems.

—

Rich Matheisen

MCSE+I, Exchange MVP

MS Exchange FAQ at http://www.swinc.com/resource/exch_faq.htm

Don't send mail to this address <mailto:h.pott@xxxxxxxxxxxxxx>

Or to these, either: <mailto:h.pott@xxxxxxxxxxxxxx> <mailto:melvin.mcphucknuckle@xxxxxxxxxxxxxx>
<mailto:melvin.mcphucknuckle@xxxxxxxxxxxxxx>

.