

RE: Exchange SMTP Queue's full – not receiving external email

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-05/msg04188.html>

- *From:* v-chacez@xxxxxxxxxxxxxxx (chace zhang)
 - *Date:* Wed, 24 May 2006 05:32:26 GMT
-

Hi Andy,

Thanks for posting here.

According to your description, I understand that you found many emails were stuck in queues. Please let me know there were Junk mails or NDRs?

From the symptom, it appears that you exchange server may under spam attack, Reverse NDR attack or some internal workstations are infected by virus. Please perform the following steps to narrow down this issue.

Step 1.

This issue can occur if your exchange server is being used as a relay server. Please double check you configured smtp virtual server correctly.

To do so:

1. In Exchange System Manager, expand Servers , expand the container for your server, expand Protocols , and then expand SMTP .
2. Right-click the SMTP virtual server, and then click Properties.
3. Click the Access tab of the SMTP virtual server, and then click Relay.
4. Click Only this list below and keep the following list blank.
5. Clear Allow computers which successfully authenticate to relay check box.
6. Restart SMTP Virtual Server.

Normally, after performing the steps above, your Exchange server will prevent message relaying including open relay and authenticated relay. At this point, I would ask you how you determine your Exchange server is being used to relay messages. I would suggest you perform the tests in the articles below to examine if your Exchange 2003 server is configured as relay.

SMTP relay behavior in Windows 2000, Windows XP, and Exchange Server
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;304897>

RE: Exchange SMTP Queue's full – not receiving external email

How To Examine Relay Restrictions for Anonymous SMTP Connections and Filter Unsolicited E-mail Messages in Exchange 2000 Server
<http://support.microsoft.com/default.aspx?scid=KB:EN-US:313395>

Step 2. Clean Queue.

1. Stop SMTP Virtual Server.
2. Go to C:\Program Files\Exchsrvr\mailroot\vs1 and rename the Queue folder as Queue.old
3. Restart the SMTP Virtual Server and refresh queues in Exchange System Manager.
4. Then you can delete the Queue.old folder as you want.

Step 3. Please go to Queue viewer. Double click to open the Properties of the stuck emails. Please check the sender of the emails. Are the problematic emails sent from certain internal user?

Are these emails NDR emails? If so, please check the following:

(Do NOT use these steps unless you are under this kind of attack) Nowadays spammers have a new means to avoid filters built into many systems. They take advantage of a mail systems sending of a non-delivery report (NDR) when a message cannot be delivered as addressed and returns the original contents. Since this follows the RFC standard, most all mail servers will function this way. This is what is called a "Reverse NDR attack" (RNDR). This form of attack is becoming increasingly widespread. Some users get it so badly that over 33% of their Internet messages are attributed to this type of spam. The end result is the spammer has attained a new form of mail relaying. Your server's resources are being stolen to deliver spam.

How does a " Reverse NDR" attack work?

Step 1 Spam email is created with the intended spam victim's address in the sender field and a random, fictitious recipient, at your domain, in the To: field.

Step 2 Your mail server cannot deliver the message and sends an NDR email back to what appears to be the sender of the original message, the spam victim.

Step 3 The return email carries the non-delivery report and possibly the original spam message. Thinking it is email they sent, the spam victim reads the NDR and the included spam.

What are the symptoms of a RNDR attack?

1. Sluggish email delivery
2. Outbound queues full of non-delivery notices

RE: Exchange SMTP Queue's full – not receiving external email

RE: Exchange SMTP Queue's full – not receiving external email

3. Excessive admin time to clear outbound queues
4. Badmail folder's size grows quickly

If you are experiencing any of the above, chances are good your mail server is under attack.

To stop the RNDR from happening, follow the following steps:

To Configure Recipient Filtering

When you enable recipient filtering (if you are using SMTP for incoming emails) on the SMTP virtual server, e-mail messages that are received from anyone on the recipient filter are not accepted. Recipient filtering is set globally, but you enable it on a per-Virtual Server basis on each SMTP virtual server.

To create a recipient filter:

1. Click "Start", point to "Programs", point to "Microsoft Exchange", and then click "System Manager".
2. Expand "Global Settings", right-click "Message Delivery", and then click "Properties".
3. Click the "Recipient Filtering" tab, and then click the checkbox at the bottom (Filter recipients who are not in the directory).
4. Specify any additional filter options that you want to configure, Select Apply, and then click "OK".

To enable recipient filtering on the SMTP virtual server:

1. Click "Start", point to "Programs", point to "Microsoft Exchange", and then click "System Manager".
2. Expand "Servers", expand "<ServerName>", and then expand "Protocols".
3. Expand "SMTP", right-click "Default SMTP Virtual Server", and then click "Properties".
4. Click the "General" tab, and then click "Advanced".
5. In the "Address" list, click the IP address where you want to apply the recipient filter, and then click "Edit".
6. Click to select the "Apply Recipient Filter" check box, click "OK", and then click "OK".

Note: Recipient filter rules apply only to anonymous connections. Authenticated users and Exchange servers bypass these validations.

Also I provide the following methods of protecting Exchange:

1. Disable the Guest account in your SBS 2003 server and enable Strong Password Protection. Everytime when you run CEICW you will be asked for enabling password policies after it ends. I suggest you enable it. You can also do that in Server Management\Users->Configure Password Policies. For more information, see:

RE: Exchange SMTP Queue's full – not receiving external email

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx>

2. We can block unsafe attachments in emails by running through CEICW and enable Internet Email on the wizard. You should see a page named "Remove E-mail Attachments" where you can choose to block all or some of the unsafe attachments. For more information, you can search "Remove E-mail Attachments" (without the quotes) in SBS 2003 Help and Support Center.

3. If you are using SMTP for incoming emails, you can install IMF (Intelligent Message Filter):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=C1B08F7B-8CAF-4147-B074-8C9C8F277071&displaylang=en>

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy..mspx>

Please feel free to let me know if you have any further questions or concerns.

I appreciate your time and look forward to hearing from you.

Best regards,

Best Regards,

Chace Zhang (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

=====
This newsgroup only focuses on SBS technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner.

You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the "Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

RE: Exchange SMTP Queue's full – not receiving external email

RE: Exchange SMTP Queue's full – not receiving external email

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

=====

This posting is provided "AS IS" with no warranties, and confers no rights.

.