

Exchange issues

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.admin/2005-07/msg00275.html>

- *From:* "Ashi" <Ashi@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 21 Jul 2005 04:39:05 -0700
-

Hi,

I have a very strange problem.

Environment: SBS 2000, 25 users, Exchange is configured with an SMTP feed. ADSL is connected through a firewall then a router. The Firewall has a live IP address that the MX record points, port forwarding is configured to route all traffic on port 25 to the SBS Exchange server. Groupshield and Virusscan Enterprise are installed.

All has been fine for months but as from last Friday they reported the internet being slow and intermitent times, I managed to narrow it down to the server that was using all the bandwidth. I suspected SMTP relaying because when I shutdown the information store the bandwidth resumes although I am confused because SMTP was locked down and configured to only relay mail from authenticated users?? Things I have tried;

- Confirmed that the default SMTP vurtual server is locked down (no SMTP connector installed)
- Disabled groupshield – no effect
- Scaned for virus – no effect
- Scaned with stinger – no effect

All was fine last night and this morning until Exchange stopped working altogether. Users can login and see there in box but can't send or receive mail. All the Exchange services are running and all looks fine. The MX record is pointing to the correct IP and I can externally connect to port 25. When I try and send mail locally sometimes it works (although I have to log in and out of outlook) and other times not. I am completly stumpped!! Not sure where else to look and really don't want to have to reload the server!! Any suggestions would be greatly appreciated.

Thanks

Send to a Friend Printer Friendly

Exchange issues

Comment from gpriceee

Date: 07/20/2005 09:45AM PDT

Comment

Hi.

You should verify that the server really isn't an open relay:

<http://support.microsoft.com/default.aspx?scid=kb;en-us:324958>

Also, about half way down, pay particular attention to "Clean up the Exchange Server's SMTP queues."

You might have some issues remaining.

Comment from eholland99

Date: 07/20/2005 09:48AM PDT

Comment

It definitely sounds like relay is either turned on or was turned on. Your SMTP queues are probably clogged with SPAM. I once saw a single Exchange server with relay turned on that after 12 hours had half a billion email messages in it's queue.

You will need to clear out the queues...there are a couple of tools that can do this for you. Make sure, however, that you've disabled relay before you start doing that or you'll be chasing your tail.

It is also possible that you are getting attacked by a relay on the internet. I would try to determine if the traffic is coming from inside your organization or outside.

Here is a good article from Microsoft on how to lock yourself down and clean up your SMTP queues.

<http://support.microsoft.com/?id=324958>

Comment from eholland99

Date: 07/20/2005 09:48AM PDT

Comment

gpriceee...get off my back! LOL...we seem to be on the same wavelength.

Comment from gpriceee

Date: 07/20/2005 09:51AM PDT

Comment

Exchange issues

:~)

Ha! LMAO

Comment from Dejan_Foro

Date: 07/20/2005 12:11PM PDT

Comment

My sound stupid, but do you have a file system antivirus installed ? Such things happen when you have antivirus for Exchange but no file system antivirus and your server gets infected. A Virus on the file system could send through your server (becasuse it is on the local network) and consumpt your bandwith.

Regards,

Dejan Foro

Exchange MVP

dejan.foro@xxxxxxxxxxxxxxxxxxxxxx

www.exchangemaster.net

Comment from capitalpro

Date: 07/20/2005 01:10PM PDT

Your Comment

Thanks all, I will try emptying the queues.

Dejan, there is McAfee Enterprise V. 7.0.0 installed for filesystem protection.

Comment from capitalpro

Date: 07/20/2005 02:55PM PDT

Your Comment

I have deleted the queues and have ensured the SMTP virtual server is configured not to relay messages. Now I can send and receive internal mail and I can send out but no mail is getting in. I can't even telnet to port 25 from the server it's self. I get a 'connection to host lost' error although I can telnet to port 110.

How do I fix the 'unable to telnet to port 25' issue? I presume this is the cause of it not receiving mail from the SMTP feed? I have checked the MX record is pointing to the correct address.

Another thing is that earlier I disabled the SMTP service as a test to see if it would increase the bandwidth but still the server is hogging all the bandwidth??? Something on the server is sending out sh*t loads of cr*p!! If I disconnect the server from the network the bandwidth is ok.

Exchange issues

Comment from eholland99

Date: 07/20/2005 03:00PM PDT

Comment

Well if you disabled the SMTP service you're not going to be able to telnet to port 25. You're also not going to be able to receive external email.

If something is still hogging all the bandwidth after you shut down SMTP, then it's not a relay problem. I would start shutting down services one at a time until you find the culprit.

Comment from Dejan_Foro

Date: 07/20/2005 03:15PM PDT

Comment

The fact that your server is sending out data consuming bandwidth is quite a good reason to believe that your computer might be infected with a virus. This can happen although you have an antivirus installed.

Did you try to do a check with another antivirus for example Norton Antivirus?

I would also suggest you run some antispyware tools to make sure that your server is not hacked and used for attacks on other computers on the Internet because this would quickly get you filtered and/or blacklisted.

Regards,

Dejan Foro

Exchange MVP

dejan.foro@xxxxxxxxxxxxxxxxxxxxx

www.exchangemaster.net

Comment from gpriceee

Date: 07/20/2005 06:38PM PDT

Comment

hi.

Did you have a chance to verify all of the settings in

<http://support.microsoft.com/default.aspx?scid=kb:en-us:324958>

Comment from capitalpro

Exchange issues

Exchange issues

Date: 07/21/2005 12:26AM PDT

Your Comment

gpriceee: I did verify the setting in the link you provided....thanks.
Although part of the tests were to telnet to port 25 which I was unable to do, so I carried on to the next part which was to lock down relaying and clean the queues. As a result of this I can now send and receive locally and send externally but not receive external mail (I think it has something to do with that fact that I can't telnet to port 25, not even from the server it's self!). MX record is ok.

eholland99: I was not trying to telnet to port 25 when SMTP was disabled, disabling SMTP was a separate test to find out what is consuming all the bandwidth.

Dejan Foro: I have run Adaware Pro which couldn't find any problems, I will try another antivirus.

My main concern is to get the exchange server to receive mail, once exchange is back I will try and sort out the bandwidth problem.

Thanks for your suggestions people.....I will battle on!

Comment from capitalpro

Date: 07/21/2005 01:07AM PDT

Your Comment

I can now telnet to port 25. I had to add the subnet in to the SMTP virtual connection but I still can't get the server to receive external mail.

Comment from capitalpro

Date: 07/21/2005 02:45AM PDT

Your Comment

Now I think it is an SMTP relaying problem although I have checked that SMTP is locked down. I have disabled SMTP when the internet is slow and it instantly speeds up. I am in the process of setting up a POP box to download all the mail using a POP connector, this way I can close port 25 (as a temp fix)

.

-
- *Follow-Ups:*
 - ◆ *Re: Exchange issues*

Exchange issues

◇ *From:* John Oliver, Jr. [MVP]

- Prev by Date: ***Re: Out Of Office replies from specific Users***
- Next by Date: ***Re: Event Viewer Errors, I need help!***
- Previous by thread: ***Out Of Office replies from specific Users***
- Next by thread: ***Re: Exchange issues***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***