

Re: problems with KB951746

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-08/msg01544.html>

- *From:* "Cliff Galiher" <cgaliher@xxxxxxxx>
 - *Date:* Fri, 15 Aug 2008 20:28:57 -0600
-

Depends on how aggressive the firewall is with its intrusion prevention measures. Blocking legitimate IP addresses responding on ports the firewall doesn't expect will cause problems. And three or more people using the net will cause the firewall to block IPs more rapidly. Never *assume* that the problem isn't somewhere. Test and verify...test and verify... :)

-Cliff

"Gary Karasik" <gkarasik@xxxxxxx> wrote in message
[news:u7%23gyc0\\$IHA.3756@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:u7%23gyc0$IHA.3756@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Also, if this were a firewall issue, I think it would be there all the time, not just when the system is under load.

--

GaryK

"Cliff Galiher" <cgaliher@xxxxxxxx> wrote in message
news:I5OdnRWuYKkGijvVnZ2dnUVZ_uqdnZ2d@xxxxxxxxxxxxxxxx

Gary,

I doubt the patch, or SBS, is the problem here. What I suspect is happening is that the patch is doing what it is supposed to do. But one of the things the patch does is cause the source port to be randomized. If your firewall is not configured to allow DNS traffic from a random source port then your recursive DNS requests are being stopped at the firewall...and you'll get the symptoms you describe. It is also possible, but less likely, that your ISP's DNS servers are misconfigured and are unable to reply on odd source ports.

So this is where I'd start....look at your network perimeter and see if you can verify there is a firewall issue.

Then, if you are CONFIDENT that you are okay there and the speed issue remains, reconfigure SBS (CEICW) and point it to another DNS server that is known to be patched and working (openDNS is a good option here).

Let me know if that helps,

Re: problems with KB951746

-Cliff

I'm fairly confident you'll be able to fix the issue from there.
"Gary Karasik" <gkarasik@xxxxxxx> wrote in message
news:%236rvj2y\$1HA.5660@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi,

I can't decide how to proceed with getting this problem solved. When the server-side DNS-vulnerability patch (951746) is installed, all my SBS2K3 systems are exhibiting the same problem: extremely slow internet access when the system is under load, meaning when three or more clients are trying to access the internet at once.

With the patch uninstalled everything returns to normal. This is not resolved by reserving ports as one fix suggests.

The problem seems to be that DNS can't resolve quickly when the patch is installed. Sometimes it is so slow that the system times out. I've tried different forwarders, different DNS servers, and root hints only. If the patch is installed, nothing helps.

Someone has posted a message about this in the SBS private forum, but he isn't getting much help.

My indecision stems from the fact that no symptoms show if there is no load, so if I call CSS after hours I can't show them any symptoms, and I don't want to load the patch during a work day because access is so slow that client work slows to a virtual standstill, the remote branches connections to Exchange server stop responding, and local clients can't do any work that involves the internet.

I think I'm just going to have to live with this and hope that MS comes up with a fix for someone else and I hear about it.

Maybe someone here can suggest an approach, because I'm stumped as to how to proceed.

--

GaryK

Re: problems with KB951746