

Re: SQL Server Specific Windows Firewall Exception

Source:

<http://www.tech-archive.net/Archive/SQL-Server/microsoft.public.sqlserver.connect/2007-08/msg00020.html>

- *From:* Andrew Hayes <AndrewHayes@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 5 Aug 2007 22:36:01 -0700
-

Generally. That is true. And I'm quite happy with the default out-of-box configuration. At least for local machine purposes.

However, if I've gone into the Surface Area Configuration and enabled remote Named Pipes and TCP/IP connections then obviously something is going to be connecting to it remotely (otherwise, why would I bother?).

At this point it should install the Exceptions that are needed, even if it doesn't enable them, so when I go to Windows Firewall I don't have to mess about browsing for EXE's or adding new ports, and ending up with a mess of exceptions that are a pain to deal with.

I spend far too much time trawling through "HOWTO: blah blah blah through Windows Firewall" articles than I would like.

Why introduce a firewall that is so complicated to configure in a corporate environment that most SE's I know just turn it off?

And no. Using the GPO isn't a realistic approach as you would have to have several policies to open different ports and/or point at different EXE's depending on what the server is used for, and then setup WMI filtering so that the policies only apply to the correct servers.

"Sue Hoegemeier" wrote:

You generally don't want something that installs and automatically opens up ports – that's been a huge problem in the past. So things are intentionally designed to be secure by default now with the newer Microsoft services. There are applications that use only local, nonremote connections to SQL Server so automatically opening up ports in such cases would unnecessarily increase the surface area of exposure to threats, hacks.

–Sue

Re: SQL Server Specific Windows Firewall Exception

On Sun, 29 Jul 2007 18:30:01 -0700, Andrew Hayes

<AndrewHayes@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

If you edit File and Print Sharing in Windows Firewall, you'll see that it lists 2 UDP ports and 2 TCP ports.

This is something that cannot be done normally but is offered through the XPSP2 resource DLL. You can see this by looking at the registry entry for GloballyOpenPorts under HKLM.

```
"137:UDP"="137:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22001"  
"138:UDP"="138:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22002"  
"139:TCP"="139:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22004"  
"445:TCP"="445:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22005"
```

My question is – when will such a DLL or other method become available for SQL Server 2005 so that we don't have to add a number of different program and port exceptions to get remote connections and administration to work through Windows Firewall?

Or possibly have it install the exceptions for us, such as Office 2007 does for Groove, OneNote and Outlook? The SQL Server Surface Area Configuration tool is the best place for such firewall changes to be chosen.