

RPC Connection problems with XP Firewall, despite proper exceptions

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-01/2558.html

From: Robert (*jemimus_at_xs4all.nl*)

Date: 01/31/05

Date: Mon, 31 Jan 2005 15:42:22 +0100

So there seems to be a problem with DCOM or RPC over the Windows XP SP2 firewall.

The problem above manifests itself when you use MSinfo32.exe to collect info on an external computer. And also appears when you try access the disk manager of the remote pc, via the Computer Management Snap-in. Also the Resultant Set of Policy: – "RPC Server is Unavailable"

Discounted all other things, as RSoP and all of the above works just fine with the firewall turned off.

Also note, that all the firewall settings are being pushed via Group Policy, and that the policy is not being overridden by anything above it, the application of the correct settings can be observed live on the client.

Now via Group Policy, you can set some settings that are suppose to open up all the management ports you could need within your lan/domain:

Windows Firewall: Allow local program exceptions

This will open up the following ports on the client machines:

TCP Port 135 for (DCOM) (DCE/RCP Endpoint Mapper)

TCP Port 445 for (RPC)

Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). This policy setting also allows SVCHOST.EXE and LSASS.EXE to receive unsolicited incoming messages and allows hosted services to open additional dynamically-assigned ports, typically in the range of 1024 to 1034.

If you enable this policy setting, Windows Firewall allows the computer to

receive the unsolicited incoming messages associated with remote administration. You must specify the IP addresses or subnets from which these incoming messages are allowed.

If you disable or do not configure this policy setting, Windows Firewall does not open TCP port 135 or 445. Also, Windows Firewall prevents SVCHOST.EXE and LSASS.EXE from receiving unsolicited incoming messages, and prevents hosted services from opening additional dynamically-assigned ports. Because disabling this policy setting does not block TCP port 445, it does not conflict with the "Windows Firewall: Allow file and printer sharing exception" policy setting.

Note: Malicious users often attempt to attack networks and computers using RPC and DCOM. We recommend that you contact the manufacturers of your critical programs to determine if they are hosted by SVCHOST.exe or LSASS.exe or if they require RPC and DCOM communication. If they do not, then do not enable this policy setting.

Note: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (the message sent by the Ping utility), even if the "Windows Firewall: Allow ICMP exceptions" policy setting would block them. Policy settings that can open TCP port 445 include "Windows Firewall: Allow file and printer sharing exception," "Windows Firewall: Allow remote administration exception," and "Windows Firewall: Define port exceptions."

Then you also have this one:

Windows Firewall: Allow File and Print Sharing exception

This will open up the following ports on the client machines:

- TCP Port 139 (Netbios Session Service)
- TCP Port 445 (RPC)
- UDP Port 137 (Netbios Name Service)
- UDP Port 138 (Netbios Datagram Service)

Allows file and printer sharing. To do this, Windows Firewall opens UDP ports 137 and 138, and TCP ports 139 and 445.

If you enable this policy setting, Windows Firewall opens these ports so that this computer can receive print jobs and requests for access to shared files. You must specify the IP addresses or subnets from which these incoming messages are allowed. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is selected and administrators cannot clear it.

If you disable this policy setting, Windows Firewall blocks these ports, which prevents this computer from sharing files and printers. If an administrator attempts to open any of these ports by adding them to a local port exceptions list, Windows Firewall does not open the port. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared and administrators cannot select it.

If you do not configure this policy setting, Windows Firewall does not open these ports. Therefore, the computer cannot share files or printers unless an administrator uses other policy settings to open the required ports. In

microsoft.public.windowsxp.security_admin: RPC Connection problems with XP Firewall, despite proper exceptions

the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared. Administrators can change this check box. Note: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo requests (the message sent by the Ping utility), even if the "Windows Firewall: Allow ICMP exceptions" policy setting would block them. Policy settings that can open TCP port 445 include "Windows Firewall: Allow file and printer sharing exception," "Windows Firewall: Allow remote administration exception," and "Windows Firewall: Define port exceptions."

But unfortunately, this doesn't seem to help.

Now MS KB article 875605 (How to troubleshoot WMI-related issues in Windows XP SP2) also tells me to

- Create a program exception for unsecapp.exe – Done, no dice
- Explicitly open port 135 – Done, still no dice.
- Edit the DCOM remote launch permissions. – Done, officer, I still don't have any dice.

I really can't think of anything else at this point. I guess I will have to dig into DCOM and pull out the network monitor for this. *sigh*

Consulted sources so far:

<http://www.ntcompatible.com/thread28557-1.html> – SP2 Windows Firewall programs exceptions list issues...

<http://support.microsoft.com/kb/q204279/> – Direct Hosting of SMB Over TCP/IP

<http://support.microsoft.com/default.aspx?scid=kb;en-us;840634> – You receive an "Access denied" or "The network path was not found" error message when you try to remotely manage a computer that is running Windows XP Service Pack 2

<http://www.microsoft.com/technet/prodtechnol/winxp/opro/maintain/sp2maint.mspx#EEAA> – Changes to Functionality in Microsoft Windows XP Service Pack 2

http://www.911cd.net/forums/index.php?showtopic=5999&hl=mmc_sp2 – Diskpart And Nu2menu Problem

<http://www.microsoft.com/technet/prodtechnol/winxp/opro/maintain/mangxpsp2/mngdepgp.mspx> – Managing Windows XP Service Pack 2 Features Using Group Policy

If anyone has any ideas, it would be appreciated!