

Re: SP2 and Firewall

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-09/18485.html>

From: Torgeir Bakken \ (MVP) (Torgeir.Bakken-spam_at_hydro.com)

Date: 09/14/04

Date: Tue, 14 Sep 2004 23:36:59 +0200

Scott Micale wrote:

> *Ok, I have downloaded and installed XP SP2 and my firewall is enabled. I
> can no longer use remote desktop to connect to another machine nor connect
> into my machine. I have looked at the exceptions list and remote desktop is
> checked for my local connection so it should allow it through. Is there
> something else I am missing? If I turn off the firewall then I can use
> remote desktop like before.*

Hi

You could set "Allow remote administration exception" for the firewall and see if that helps.

Using netsh.exe, you can configure this from command line, like this:

```
netsh.exe firewall set service type=remoteadmin mode=enable scope=subnet  
profile=domain
```

If not a domain computer, you need to change to 'profile=standard' (or 'profile=all'). Scope can also be set to 'custom' and then you can add ip ranges to the command line as well, or 'all' (not recommended for security reasons).

The netsh.exe syntax is documented in WF_XPSP2.doc.

WF_XPSP2.doc "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" is downloadable from

<http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1>

An alternative to netsh.exe:

This can be done with gpedit.msc for a local computer, or push it out with a AD GPO if possible.

From PolicySettings.xls available here:

Group Policy Settings Reference for Windows XP Professional Service Pack 2

<http://www.microsoft.com/downloads/details.aspx?familyid=ef3a35c0-19b9-4acc-b5be-9b7dab13108e&displaylang>

<quote>

Administrative Templates\Network\Network Connections\Windows Firewall
\<some> Profile

Windows Firewall: Allow remote administration exception

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.

</quote>

--
--

torgeir, Microsoft MVP Scripting and WMI, Porsgrunn Norway
Administration scripting examples and an ONLINE version of
the 1328 page Scripting Guide:

<http://www.microsoft.com/technet/scriptcenter/default.aspx>