

Re: How to allow client to disable firewall on XP/sp2 machine

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-12/msg03514.html>

- *From:* Tony Su <TonySu@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 29 Dec 2007 13:33:00 -0800
-

If the work relates to VoIP, many of those protocols are fundamentally Peer to Peer and may be a problem because they use dynamic ports and create secondary sessions across a wide range of ports. This causes problems for ISA which for anything that isn't configured with a protocol filter restricts by port.

If the laptop is on the LAN with ISA, you <may> be able to configure firewall exceptions both on the client but more preferably on the ISA server. I'd recommend trying to create an exception for the application rather than the ports because of the issues I described above.

Otherwise, if you're working remotely,

1. You can usually disable the ISA FW client by rt-clicking on the icon in the tray and selecting "disable"
2. The following Registry entries will disable the Windows Firewall (not the ISA FW client), just create a reg file that enables and another one that disables so that you only have to double click on the appropriate file to enable or disable.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall=0 (DWORD data type)
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\EnableFirewall=0 (DWORD data type)
```

—
Tony Su
www.su-networking.com
ISA
SBS
Enterprise Mobile Solutions Architect

"Dave Nickason [SBS MVP]" wrote:

Re: How to allow client to disable firewall on XP/sp2 machine

My first question would be this: instead of disabling the firewall, can you have someone with local admin rights log onto the laptop, and manually configure exceptions to accommodate your software application? It'll retain the manually configured exceptions, while still using everything that's set in group policy.

Aside from the fact that doing it that way would be more secure than completely disabling it, it'll be a fair amount of work to allow disabling only on certain machines. There are a number of ways of doing it, but I have not been able to think of a very elegant one. You could move the laptops in question to their own OU, then apply the existing policy to the other PCs instead of domain wide, creating a second set of policies for the laptop OU. You could use security filtering to apply the existing policies only to a security group that does not include the laptops. I'm sure there are other ways – I'm just not crazy about any of the ones I've been able to think of.

The specific setting that allows you to turn off the firewall is (not surprisingly) in the policy called Small Business Server Windows Firewall. It's under Computer Config -> Administrative Templates -> Network -> Network Connections -> Windows Firewall. It's under both the Domain and Standard Profiles, and it's called "Protect all network connections." All of these settings have additional information if you open the setting, which might be enough information for you to make decisions about which settings you want (use Extended View in the GP editor to see it). You can set it in either the domain or standard profile – standard applies when not connected to the domain at login.

"Barry B." <BarryB@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:6AADED42-0632-4E9D-8BCB-DA4ACC98AE54@xxxxxxxxxxxxxxxxxxxx

We have a laptop running XP-SP2 that needs to be able to turn off the Windows Firewall when using the laptop for some PBX software installation tasks that we do on a regular basis. The laptop also has MS Firewall Client for ISA 2004 installed. The server is SBS2003. Are there any articles or other instructions available to help me change the GP settings that control this?
Thanks for any suggestions.

Barry Brown
Mountain Telecom