

Re: Questions About Windows Firewall and Domain Policy Enforcement

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.group_policy/2005-01/0456.html

From: Benjamin Gay [MSFT] (*bengay_at_online.microsoft.com*)

Date: 01/20/05

Date: Wed, 19 Jan 2005 18:12:48 -0800

Hi Leo,

Can you please provide me with more detail with what you mean by connecting to the domain? Are you saying that the machines are always joined to your domain (i.e. the computer belongs to your domain) but happen to connect to other networks? Also can you provide me with a bit more information on how they connect to your domain (i.e. are they wired, wireless, VPN etc)?

As I'm sure you are aware there are several ways that your users can configure the firewall, namely group policy, net shell scripts, manual configuration and through an application using the relevant firewall configuration API's.

Let me see if I can answer your questions now:

1. You should enable the firewall on all your machines. Create exemptions based on your applications requirements. For example file and print etc.
2. You can do this through group policy or a login script. Group policy would probably be the better way to go. You can force policy by performing a `gpupdate /force`
3. I'm not quite sure what you are saying here. Can you please explain in more detail.
4. What do you mean by disable the firewall locally? Are you stopping the `sharedaccess` service or setting the operation mode of the firewall? Please provide me with some more information on how this machine is configured.

Q1. Group policy overrides local policy. Please explain what you mean by activating locally.

Q2. This should be happening. If you can give me some more information on this I can help diagnose what is happening.

Regards

--

Benjamin Gay
Microsoft Corporation

This posting is provided "AS IS", with NO warranties and confers NO rights

"Leo Alls" <Leo_Alls@ncauditor.net> wrote in message
news:OG77cpj\$EHA.2032@tk2msftngpl3.phx.gbl...
>I have a Windows 2000 domain that has 200 workstations most of which are
>still only running XP w/SP1. We haven't been able to move everyone to SP2
>because of the problems that have arisen.
>
> Problem 1: 90% of the workstations need to have the firewalls activated
> because of the way they travel around and the networks that they are
> subject to attach to.
>
> Problem 2: The workstations need to be able to be managed on all the
> workstations when they are connected to the domain.
>
> Problem 3: If we enable the firewall locally on the workstations then the
> domain policies do not over ride the local setting.
>
> Problem 4: If we disable the firewall settings locally then the domain
> policy Domain Profile settings takes over and functions properly as long
> as there is no Standard Profile configured. If you created a Standard
> Profile in the policy then it applies that setting over the Domain
> Profile. This problem doesn't matter whether you are on the domain network
> or not.
>
> Question 1: Is there a way to enforce the domain policy firewall settings
> even if the firewall was activated locally?
>
> Question 2: Is there a way to enforce the Domain Profile to work over the
> Standard Profile when connected to the domain and the Standard to be the
> default when not connected to the domain?
>
> TIA,
> Leo
>