

Re: GPO controlled firewall incorrectly ON due to Standard instead of Domain Profile

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2004-12/0028.html

From: Andy Vaya (*herbwarrior_at_mmecpa.com*)

Date: 11/30/04

Date: Tue, 30 Nov 2004 15:32:47 -0500

I have exactly this same problem in a much simpler site with one domain, one site, a single SBS2k DC, 3Com switch with independent cable runs from switch to each desktop (nil latency). I get this (sporadically, as described by Erik) behavior on laptops AND DESKTOPS (which have never been removed from the LAN). Group Policy has worked on these machines in the past to install software, prescribe other "lock down" policies, etc. I only noticed aberrant behavior with WinXP SP2 firewall policies.

My understanding from the (scant) documentation on "network discovery" (for lack of a better term) for the purpose of switching between Standard and Domain GP settings for the firewall is that the machine checks to see that it's on a network that has the same DNS suffix it found when it got it's last GP update. That seems like it should be very robust (as clients get this early in boot from DHCP).

Right? Wrong? Am I missing something?

Thanks,
Andy

BTW, I'll run rsop.msc next time the behavior appears and send it with a "normal domain" rsop result.

"Rebecca Chen [MSFT]" <v-rebc@online.microsoft.com> wrote in message news:pRaY0iq1EHA.2732@cpmsftngxa10.phx.gbl...

> *Hi Erik,*

>

> *I am a little unclear the paragraph and have a couple of questions below:*

> "

> *We do have two DCs in our small domain (50 computers, Windows Server 2003 on the DCs), one of which is at another location, but the connectivity is good (around 40ms ping)".*

>

> *1. What is the relationship of two DCs, they are in the same domain but*

> *two*

> *sites, or they are in the different domains?*

- > 2. Where is the workgroup to implement the standard profile?
- > 3. Could you provide the detailed steps to reproduce this issue? For example, if you connect the laptop to the domain, do you hibernate the laptop and resume it, or turn off/turn on the machine when you connect to the domain or workgroup?
- > 4. Do you have applied logon/logoff or startup/shutdown script in the domain? Please temporarily remove the script and test this issue.
- >
- > According to your description, since "gpupdate /force" can fresh the GPO, I believe the GPO has not correctly applied to the problematic machine.
- >
- > I suggest you take your laptop as the test machine and use the following steps to isolate this issue:
- > 1. Refer to the following KB to perform a Clean Boot and always keep in clean boot.
> Q310353 How to Perform a Clean Boot in Windows XP
> <http://support.microsoft.com/support/kb/articles/q310/3/53.asp>
- >
- >
- > 2. Turn off the machine and connect to the domain. What is the result?
- >
- > 3. Issue "rsop" in CMD, can you see the GPO has applied to the machine? Save the rsop result and called it "domain".
- >
- > 4. Turn off the machine and connect to the workgroup, what is the result? Issue "rsop" in CMD, does the GPO has been successfully applied? Save the rsop result and called it "workgroup".
- >
- > If the issue persists, please send me (v-rebc@microsoft.com) two rsop result for research. In addition, please download the MPS report tool from the following link and send the result (CAB) file to me. This log file can help me clarify the computer configuration.
- >
- > <http://download.microsoft.com/download/b/b/1/bb139fcb-4aac-4fe5-a579-30b0bd915706/MPSRPT_SETUPPerf.EXE>
- >
- > 1. Double click this file to run it.
- > 2. After that, please go to C:\windows\MPSReports\Setup\Reports\Cab
- > .
- > 3. Find a file named [COMPUTERNAME]_MPSReports.CAB
- > 4. Send this cab file to me at v-rebc@microsoft.com
- >
- >
- >
- > Any update, let us get in touch!
- >
- > Best regards,
- >
- > Rebecca Chen
- >

> MCSE2000 MCDBA CCNA
>
>
> Microsoft Online Partner Support
> Get Secure! – www.microsoft.com/security
>
> =====
>
> When responding to posts, please "Reply to Group" via your newsreader so
> that others may learn and benefit from your issue.
>
> =====
> This posting is provided "AS IS" with no warranties, and confers no
> rights.
> -----
>>From: "Erik" <umetricsdev@umetrics.com>
>>Subject: GPO controlled firewall incorrectly ON due to Standard instead of
> Domain Profile
>>Date: Mon, 29 Nov 2004 16:41:35 +0100
>>Lines: 49
>>X-Priority: 3
>>X-MSMail-Priority: Normal
>>X-Newsreader: Microsoft Outlook Express 6.00.2900.2180
>>X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
>>X-RFC2646: Format=Flowed; Original
>>Message-ID: <#WCJqni1EHA.2180@TK2MSFTNGP10.phx.gbl>
>>Newsgroups: microsoft.public.windows.group_policy
>>NNTP-Posting-Host: mail.umetrics.com 194.165.228.114
>>Path:
> cpmsftngxa10.phx.gbl!TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP10
> phx.gbl
>>Xref: cpmsftngxa10.phx.gbl microsoft.public.windows.group_policy:10832
>>X-Tomcat-NG: microsoft.public.windows.group_policy
>>
>>I have setup a GPO to configure the XP SP2 Windows Firewall to work
>>differently while connected to the domain (Domain profile) and when now
>>(Standard profile). This basically works as intended but unfortunately not
>>always:
>>
>>
>>
>>Sometimes the firewall on a client is incorrectly ON and the profile used
> is
>>"Standard" (from netsh firewall show state) when it in fact should be OFF
>>and the profile "Domain" since the computers are connected to the domain.
> A
>>reboot or "gpupdate /force" on a command prompt fixes the problem but is
>>more of a workaround than a solution.
>>
>>
>>

microsoft.public.windows.group_policy: Re: GPO controlled firewall incorrectly ON due to Standard instead of Domain P

>>*The problem occurs only sometimes, not always. I have found nothing wrong*
> *on*
>>*the clients that have the problem (same IP settings, and network*
> *connection*
>>*domain name for example). Nothing in the event log. Happens to both*
> *laptops*
>>*and desktops (that are always at the office).*
>>
>>
>>
>>*We do have two DCs in our small domain (50 computers, Windows Server 2003*
> *on*
>>*the DCs), one of which is at another location, but the connectivity is*
> *good*
>>*(around 40ms ping). But still; could it be temporary connectivity problems*
>>*to the other DC that are causing the GPO problems? How can I try this*
>>*theory?*
>>
>>
>>
>>*Any other ideas how I narrow the problem down further?*
>>
>>
>>
>>*I have googled but all I've found is a similar post "Windows Firewall by*
>>*Group Policy fails to detect domain network" from 2004-10-29 by Andy Vaya*
>>*(herbwarrior@mmecca.com) in microsoft.public.backoffice.smallbiz2000, but*
>>*there were no replies there. (and I thought that posting here might be*
>>*better.).*
>>
>>
>>
>>*/ Erik*
>>
>>
>>
>>
>>
>>
>>
>>
>