

Re: two winxp home machines, varied results

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2005-08/msg02113.html

- *From:* Chuck <none@xxxxxxxxxxx>
 - *Date:* 26 Aug 2005 10:58:04 -0500
-

On 26 Aug 2005 06:51:46 -0700, "Brian McCabe" <briansmccabe@xxxxxxxxxxx> wrote:

>Thanks for being so willing to help out. I appreciate it!!
>
>I was gonna address this last, but I think I had a bit of a
>breakthrough at the end of my research so this info is getting bumped
>to the top.
>
>The only firewall I have on my machine *aside* from the Cisco VPN
>client (more on that in a minute) is Windows Firewall that came with
>SP2. Oh yeah, that reminds me: both machines are WinXP Home with the
>latest updates installed. Anyway, regarding the Cisco VPN client –
>there was a setting in there called "stateful firewall (always on)"
>that was CHECKED. I unchecked it and have tried a few things.
>NEWSFLASH: I can now ping "brian" from "heidi" by name and by IP. Also,
>port requests on my router that are set up to forward to "brian" are
>working again as well. Finally, I attempted to map a drive on "heidi"
>to a shared dir that resides on "brian" and was able to do so. To me,
>that accomplishes everything I have been trying to keep stable. BUT
>that raises another question or two: is it safe to disable the
>"stateful firewall" on my VPN client? Perhaps I should check with the
>IT guys at work?

Brian,

You're asking a very interesting question here. One that must be analysed in TWO directions. Most firewalls are used to protect one environment against another. But which environment do you trust? Are you protecting your home LAN from your work LAN, or vice versa?

As networks become more complex, and more common, bidirectional protection becomes more significant.

So what protection does a VPN bundled firewall provide? What is intended to provide? What happens when it is disabled, for convenience? These are all issues which I have yet to think about. Please do discuss this with the IT guys, and please please do let us know what they say.

Re: two winxp home machines, varied results

>I'll go ahead and include the remainder of my findings in this post in
>case you want to see them and / or there's something else I need to be
>aware of. If you consider the problem solved and do not have the time
>to review this info, I understand.

I'm here to learn. If there's anything else to learn, I'll keep posting. If
you keep posting, I will too.

>Ok, here's what I found with regards to the restrictanonymous presence
>in the registry.
>
>on "brian", the following registry dirs had keys named either
>"restrictanonymous" or "restrictanonymousSAM." In each case, the value
>for "restrictanonymous" was 0 and the value for restrictanonymousSAM was
>1.
>
>HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa
>HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Control\Lsa
>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

That is called a Registry "Key". The "CurrentControlSet" key is the relevant
one. The others were current at some previous time. Only adjust
"CurrentControlSet".

>Furthermore, there were also a pair of dirs that had my search criteria
>("restrictanonymous") in the name of the dir itself.

The leaf elements are called "values". The "value" named "restrictAnonymous"
(please note the small "r" in the name!) (Microsoft named this thing) must be
"0". This is all Microsoft terminology.

Please don't confuse "restrictAnonymous" and "restrictAnonymoussam". Those are
two separate values! Please don't change "restrictAnonymoussam", only
"restrictAnonymous", IFF necessary!

>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
>NT\CurrentVersion\SeCEdit\Reg
>Values\MACHINE\System\CurrentControlSet/Control/Lsa/RestrictAnonymous
>
>which has the following keys and their corresponding values:
>
>(Default) REG_SZ (value not set)
>DisplayName REG_SZ Network access: Do not allow anonymous
>enumeration of SAM accounts and shares
>DisplayType REG_DWORD 0
>valueType REG_DWORD 4
>
>
>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
>NT\CurrentVersion\SeCEdit\Reg
>Values\MACHINE\System\CurrentControlSet/Control/Lsa/RestrictAnonymousSAM

Re: two winxp home machines, varied results

>
>which has the following keys and their corresponding values:
>
>(Default) REG_SZ (value not set)
>DisplayName REG_SZ Network access: Do not allow anonymous
>enumeration of SAM accounts (NOTE: does NOT say "and shares" at the
>end)
>DisplayType REG_DWORD 0
>valueType REG_DWORD 4
>
>
>The registry findings for "heidi" were identical to that of "brian".
>
>Here is the IPCONFIG and BROWSTAT listings for each machine. NOTE: The
>"browstat" command does not appear to have worked.

<SNIP>

>BROWSTAT info for "heidi"
>
>'browstat' is not recognized as an internal or external command,
>operable program or batch file.
>
>
> So there you have it. All I have done here is compile information; I
>did not edit any registry entries because from following the guide you
>provided on the restrictanonymous aspect of the registry, it did not
>look like editing anything was necessary. I included the search
>findings here in case you needed to peruse them.

Please read instructions about using the Path properly. Or run browstat directly from the folder where you copied it.

<<http://nitecruZR.blogspot.com/2005/05/using-path-and-making-custom-program.html>>

<<http://nitecruZR.blogspot.com/2005/05/browstat-utility-from-microsoft.html>>

<<http://nitecruZR.blogspot.com/2005/06/command-window.html>>

But based upon what you say above about the VPN firewall, this point may be moot.

At any rate, I suspect the problem may be identified, and based upon what you get from the IT guys at work, may be solved. Please do let us know what they say about their needs. I provide advice so I may learn, and may instruct others. Your situation is one which should be of interest to many – WHO is being protected by a VPN firewall?

Some background: AOL customers, using AOL purely as a portal, but providing their own ISP, access the AOL servers thru a VPN. Some time ago, the effectiveness of this setup became embarrassingly obvious:

<<http://nitecruZR.blogspot.com/2005/12/todays-security-alert.html#7/28>>

The AOL situation may be relevant to yours. In both directions. Please keep us

Re: two winxp home machines, varied results

Re: two winxp home machines, varied results

updated on this.

—

Cheers,

Chuck, MS-MVP [Windows – Networking]

<http://nitecruze.blogspot.com/>

Paranoia is not a problem, when it's a normal response from experience.

My email is AT DOT

actual address pchuck mvps org.

.

• **Follow-Ups:**

◆ **Re: two winxp home machines, varied results**

◇ From: Brian McCabe

• **References:**

◆ **two winxp home machines, varied results**

◇ From: briansmccabe

◆ **Re: two winxp home machines, varied results**

◇ From: Chuck

◆ **Re: two winxp home machines, varied results**

◇ From: Brian McCabe

• Prev by Date: **RE: Mystery Problem**

• Next by Date: **Re: Can't connect to the internet on WinXP using a wireless connection**

• Previous by thread: **Re: two winxp home machines, varied results**

• Next by thread: **Re: two winxp home machines, varied results**

• Index(es):

◆ **Date**

◆ **Thread**