

Re: Connecting to XP sp2 machines by VPN

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-05/msg04017.html>

- *From:* "Bill Sanderson" <bill_sanderson@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 30 May 2008 17:54:28 -0400
-

Sorry for losing track of this thread.

For PPTP VPN, you need two protocols: TCP, port 1723—which you know all about, and GRE. GRE is protocol 50, I believe, but don't confuse that number with a port number—it isn't one.

As I understand it, both the XP firewall and the Windows firewall (the first is what existed before SP2, and the latter what is in SP2 on, as I understand it)—only require that you open port 1723—they then take care of the GRE stuff automagically.

This may not be the case with third-party firewalls or suite protective products. And it definitely isn't the case with the average home nat/router device, which will use a variety of non-standard names for GRE.

Don't open up any of those other protocols you see being dropped, unless there is clear evidence of functionality you need thich is connected to those ports.

"Jim Behning SBS MVP" <jimbehning@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:8uoe24dbqmecl48msmet56kt4ovbq2eg0@xxxxxxxxxx

No thinking cap on today. We have had issues with Trend's PCCillin firewall. I did call them once when I could not get the right click to get the vpn to work properly.

You might want to do a google search on th eport numbers. One or two of those are netbios ports.

That article of mine is poorly format right now. I guess the format was goofed up with various blog updates. Send me an email if you want me to copy and paste the whole article. It apears in my browser to be missing some words. You just delete the stuff between the @ and the m of mindspring

On Fri, 9 May 2008 06:19:01 -0700, Leigh <Leigh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Hi Jim

Re: Connecting to XP sp2 machines by VPN

Thanks for your input I found both articles very interesting. however I have no idea what values to put into the scope parameters. That being so I opted to use * as the easy no brain every thing allowed. But next problem Which port to modify ???

Is this the same as changing the scope in fire wall set up for Print and file sharing. If so I allready plumped for the "Any computer (including those on the internet)

I have no idea which parts of the connections the firewall is blocking. I have looked at the firewall log and googled the ports that have DROP in the dialogue. That has scared me to death. PORTS 445 138 139 68 67 13518 13504 13502 13503 13477 what ever happened to good old "you only need 1723" I dont have a clue what all the other ports are or if the word DROP indicates them causing my problem (please see previous posts) any guidance here gratefully recieved.

incidentally the software I am using makes no difference to my problem. If I connect by VPN manually from SBS2003 into XPsp2 I cannot see shared folders unless I switch off the firewall :-(

"Jim Behning SBS MVP" wrote:

I think I have seen this before. You probably need to add other networks to allow foreign ips in. Here is my long story from a few years ago. I hope it is relevant.
<http://msmvps.com/blogs/bgb/archive/2006/05/16/95140.aspx>

On Fri, 9 May 2008 02:25:01 -0700, Leigh
<Leigh@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

>Hello Bill
>
>I have allowed the print and file sharing to be accessed by any >computer
>(including those on the internet) previously and still no luck.!!
>I also created a log file "pfirewall" previously which I have copied >into
>here. Unfortunately it doesnt fit very well and looks a mess in this >post.
>Perhaps you can cast your eye over it and make some observations that >may
>help as I do not really understand all the information contained.

Re: Connecting to XP sp2 machines by VPN

>
>81.140.65.54 is the SBS external static .192.168.16.41 is
the XP >internal
>fixed IP 192.168.0.1 is the internal SBS ip
>I can see a lot of DROPS in the log which seem to involve
TCP and UDP >ports
>
>In all the research I have done I understood I only need to
make sure >to
>open port 1723 so what are all the others, are they to do
with the VPN
>connection I am trying to make and do I need to open them.
>I dont want to open them if that will cause me other
problems. Can you >advise
>
>Thanks for your help
>
>2008-04-25 14:15:42 OPEN-INBOUND TCP
81.140.65.54 192.168.16.41 13477 >1723 -
>- - - - -
>2008-04-25 14:15:46 DROP UDP 192.168.0.174
255.255.255.255 68 67 >328 - - - -
>- - - RECEIVE
>2008-04-25 14:15:50 DROP UDP 192.168.0.174
255.255.255.255 68 67 >328 - - - -
>- - - RECEIVE
>2008-04-25 14:16:03 DROP TCP 192.168.16.41
192.168.0.174 445 13502 48 >SA
>3084194260 1133350834 9520 - - - SEND
>2008-04-25 14:16:03 DROP TCP 192.168.0.1
192.168.16.41 13503 139 48 S
>804954720 0 65535 - - - RECEIVE
>2008-04-25 14:16:03 DROP TCP 192.168.16.41
192.168.0.174 139 13504 48 >SA
>369768440 2327057425 9520 - - - SEND
>2008-04-25 14:16:06 DROP TCP 192.168.16.41
192.168.0.174 445 13502 48 >SA
>3084194260 1133350834 9520 - - - SEND
>2008-04-25 14:16:06 DROP TCP 192.168.16.41
192.168.0.174 139 13504 48 >SA
>369768440 2327057425 9520 - - - SEND
>2008-04-25 14:16:06 DROP TCP 192.168.0.1
192.168.16.41 13503 139 48 S
>804954720 0 65535 - - - RECEIVE
>2008-04-25 14:16:06 DROP TCP 192.168.16.41
192.168.0.174 445 1350240 A
>3084194261 1133350834 9520 - - - SEND
>2008-04-25 14:16:06 DROP TCP 192.168.16.41
192.168.0.174 139 13504 40 A
>369768441 2327057425 9520 - - - SEND
>2008-04-25 14:16:12 DROP TCP 192.168.16.41

Re: Connecting to XP sp2 machines by VPN

```
192.168.0.174 139 13504 48 >SA
>369768440 2327057425 9520 --- SEND
>2008-04-25 14:16:12 DROP TCP 192.168.16.41
192.168.0.174 445 13502 48 >SA
>3084194260 1133350834 9520 --- SEND
>2008-04-25 14:16:12 DROP TCP 192.168.0.1
192.168.16.41 13503 139 48 S
>804954720 0 65535 --- RECEIVE
>2008-04-25 14:16:12 DROP TCP 192.168.16.41
192.168.0.174 445 13502 40 A
>3084194261 1133350834 9520 --- SEND
>2008-04-25 14:16:12 DROP TCP 192.168.16.41
192.168.0.174 139 13504 40 A
>369768441 2327057425 9520 --- SEND
>2008-04-25 14:16:22 DROP UDP 192.168.0.170
255.255.255.255 138 138 >239 ---
>--- SEND
>2008-04-25 14:16:24 DROP TCP 192.168.0.174
192.168.16.41 13518 80 48 S
>1701259848 0 65535 --- RECEIVE
>2008-04-25 14:16:27 DROP TCP 192.168.0.174
192.168.16.41 13518 80 48 S
>1701259848 0 65535 --- RECEIVE
>2008-04-25 14:16:33 DROP TCP 192.168.0.174
192.168.16.41 13518 80 48 S
>1701259848 0 65535 --- RECEIVE
>
>
>"Bill Sanderson" wrote:
>
>> I'm surprised at this result. I'd have thought that the VPN
tunnel >> between
>> the SBS server and the XP workstation would have
bypassed the >> firewall.
>>
>> Here's what I think I would do to try to troubleshoot this:
>>
>> Arrange to be able to connect to one of the XP
workstations via >> Remote
>> Desktop. Open Remote Desktop through the Windows
firewall on that XP
>> machine.
>>
>> You may find that when the VPN tunnel connects, you
lose the RDP >> connection,
>> unfortunately—if that's the case, I'm not sure how to
work around >> it.
>>
>> http://support.microsoft.com/kb/875357
>>
>> is the article I would use to guide your troubleshooting.
```

Re: Connecting to XP sp2 machines by VPN

However, I >> think
>> you
>> could save some time if you can find as much
information about this
>> "inherited software" as possible—particularly—what
executables, if >> any,
>> are involved on the XP end, and what ports and protocols.
>>
>> One thought is to open file and printer sharing through
the firewall, >> which
>> is a simple checkbox—if that is not already enabled.
Another would >> be to
>> modify the scope of that sharing to include not just the
local >> (in-store)
>> network, but also the IP address of the SBS 2003 server
end of the >> VPN
>> tunnel.
>>
>> The firewall on the XP end can be configured to log
dropped packets. >> I'd
>> suggest enabling this logging, and attempting a
connection, and then
>> inspecting the log to see what's happening. That should
give you >> clues
>> about what needs to be allowed through.
>>
>>
>>
>> "Leigh" <Leigh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote
in message
>>
news:B3009467-6D21-4EC4-99C8-BAC6AD48A285@xxxxxxxxxxxxxxxxxxxx
>> >I have Win 2003SBS and several Win XP sp2
standalone remote >> >machines.
>> > I need to collect simple files from the XP machines
using the >> > 2003SBS and
>> > the internet on a daily basis.
>> > I have set XP machines as VPN servers
>> > I can connect to these machines from the 2003SBS by
VPN no problem
>> >
>> > My problem is this.
>> >
>> > When I try to map a drive in 2003SBS to the shared
folder on the XP
>> > machine
>> > I am unable to do so except when the Windows firewall
is switched >> > off on
>> > the
>> > XP machine.
>> > When the XP firewall is off every thing works fine.

Re: Connecting to XP sp2 machines by VPN

>>> What do I have to do to the firewall to allow access to
the shared >>> folder,
>>> because I would rather not leave the firewall turned off
>>> permanently.
>>>
>>> Thanks for any help
>>>
>>
See what SBS support is working on
<http://blogs.technet.com/sbs/default.aspx>
Check your SBS with the SBS Best Practices Analyzer
<http://blogs.technet.com/sbs/archive/tags/BPA/default.aspx>

See what SBS support is working on
<http://blogs.technet.com/sbs/default.aspx>
Check your SBS with the SBS Best Practices Analyzer
<http://blogs.technet.com/sbs/archive/tags/BPA/default.aspx>