

Re: SBSServer processes Port 80 blocked

Source:

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz2000/2004-12/0133.html>

From: Eugene Tan (*insights-[drophthis]*)

Date: 12/02/04

Date: Fri, 3 Dec 2004 03:07:02 +0800

hi Fred,

First, I shd qualify that I'm no expert in ISA, just what i know from experience and observation.

Second, from your last post, you should not install the FW client on the SBS server. ISA rules will apply anyway.

I believe you are trying to understand why is something blocked (or not). Well, we need to be very sure of all of our facts in the situation we're trying to understand. Perhaps you can provide more precise info abt the acct used as the service acct for the various apps. But for now, let's assume that you're using "administrator" which as default root has all the privileges needed.

I've found that certain Windows apps don't work properly because they get blocked; the common factor was that these apps sent out some data. In my case, there was even a permit rule, LDAP389 any any. I found the Windows app was unable to authenticate with ISA, although the user could. Perhaps it only works with apps which are able to authenticate with ISA.

I guess ISA functions at the network level so one needs to understand the protocol involved. What does it mean to send over port 80? Is it HTTP or FTP over port 80? (assuming you don't open your web to the world) port80 permits sending a particular request (HTTP) and then receives the response to the request. But if you start beaming out over port 80, shd that be allowed (using the current rules)?

Above, I was thinking of your custom app. I don't know how McAfee works, perhaps it is sending more than just HTTP. Symantec LU d/l with no problem, nothing else to config for version 9. I believe the earlier ver8

had a problem with scheduled liveupdate, but when administrator logs in and initiates LU, there's no problem.

I've not tried running OE on the SBS and trying to get NG over NNTP119.
Will give it a try and see what happens.

HTH,
Eugene Tan

=====
"Fred Blum" <h.f.blum@marketconnectnospam.nl> wrote in message
news:Ojaq1dE2EHA.3000@TK2MSFTNGP15.phx.gbl...

>
> *Your explanation is in line with my understanding of how ISA works. I
> can't check McAfee Auto Update architects service account settings (i'm
> sure it was administrator member of the Backoffice Internet users group,
> proxy settings and auth provided for the AutoUpdate client). as we
> replaced it with Sophos. This works fine with the proxy settings provided.*
>
> *McAfee autoupdate client used HTTP port 80 to downlad the latest update
> information and data files. This showed up as blocked outbond on port 80
> in my logs. Only creating the allow packet rule made it work. The
> developed sync app has the same problem (proxy settings and auth provided
> in Vbasic code), sending flat txt via xml works but binary data send via
> xml port 80 and reassambled at the other site not. Porbably McAfee used
> the same method. This sync app is scheduled in task scheduler and provided
> with the administrator auth. Is this normall protection behaviour to
> block?*
>
> *On the server connecting to this newsgroup on port 119 is also not allowed
> for the adminsitator logged on locally. He is in the BackOffice internet
> users group allow all protocols rule. The only difference with a
> workstation is the firewall client.*
>
> *I'm trying to understand the basic undelying principle of what is normally
> allowed on the server and what is not.*
>
> *TIA,*
>
> *Fred*
>
>
> *"Eugene Tan" <insights-[dropthis]@post1.com> wrote in message
> news:%23DcCv8\$1EHA.1260@TK2MSFTNGP12.phx.gbl...*
>> *hi Fred,*
>>
>> *At first, I didn't understand the situation in your original post.*
>> *Now, I think I've got the issue...*
>>
>> *In SBS2000, the default settings define a rule which permits only members
>> of SBS Internet Users access to the Internet. This means not all users
>> have access to the Internet, just those you permit. If you create user
>> accts
>> using the SBS wizard, you can choose the Internet users template which*

>> will make the user account a member of SBS IU. If you use ADUC to
>> create a user account, the default is DomainUser which doesn't have any
>> access to the Internet.
>>
>> Now, if you login at the server as administrator, no doubt you can surf
>> the Internet. What process is running McAfee etc which doesn't have
>> access? You probably need another rule or modify the existing rule to
>> provide access by either another user account or group, or by IP addr
>> (Client address set).
>>
>> As for the apps issue, Steve is right, XML is today all plain text, no
>> binary involved. However, your apps may be doing a FTP or something
>> like that, perhaps over port 80. In this case, you need to create an
>> allow outbound rule. You don't have to provide an IP destination but
>> it is better as this would limit the permission to just this IP addr.
>>
>> Hope this helps,
>> Eugene Tan
>>
>> =====
>> "Fred Blum" <h.f.blum@marketconnectnospam.nl> wrote in message
>> news:OuxX9B41EHA.304@TK2MSFTNGP11.phx.gbl..
>>>
>>> I had the problem in the past that processes running on the SBS server
>>> could not connect outbound on port 80 and would show up in the log as
>>> Blocked.
>>> According to Marina everything running on the server would be allowed
>>> outbound port 80 and was it my ISA configuration.
>>> For example McAfee Autoupdate would not connect (even with option use
>>> explorer proxy settings or manually entered proxy configuration) or
>>> programs connecting to the internet for a software update.
>>>
>>> Marina has reinstalled ISA and configured it out of the box. I still
>>> have this problem now with our application using XML to sync with a
>>> providers SQL database. Normal XML flat txt data uploads work fine but
>>> in case of binary data (product pictures) uploaded via xml port 80, will
>>> be blocked and only an allow rule with destination IP address will make
>>> it work. The program is set to use and authenticate with the proxy, but
>>> it seems that tunneling is detected by ISA and blocked by default. This
>>> seems logical as a leak and trojan protection.
>>>
>>> Is this the case? Are allow rules the only solution? This problem is
>>> only at the SBS server itself. Workstations running Firewall client will
>>> work fine. (moving it to a workstation is not an option due to 24h sync)
>>>
>>> TIA,
>>>
>>> Fred
>>>
>>>
>>>

microsoft.public.backoffice.smallbiz2000: Re: SBSServer processes Port 80 blocked

>>>
>>>
>>
>>
>
>