

## Re: Windows Firewall Config for Symantec AV Corp version 9

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-01/4739.html>

---

**From:** neo [mvp outlook] ([neo\\_at\\_online.mvps.org](mailto:neo_at_online.mvps.org))

**Date:** 01/17/05

Date: Mon, 17 Jan 2005 11:00:26 -0800

Actually you need to create 2 UDP port exceptions for Corporate Edition. Those 2 ports are 2967 and 38293. These two ports do the majority of the work. (e.g. Virus Definition Transport Method (VDTM), reporting back on status, .etc) You don't have to worry about making a hole if clients are using FTP to acquire definitions from Symantec or your own internal liveupdate server. (so you can skip the lucomserver unless using a 3rd party firewall software package like Symantec's firewall.)

As for the remainder of ports, the question is: will you be doing a push install from the server to client? If yes, then you have to allow file/print. If you always go to the client and run the installer from the VPHome share, then you don't need to open file/print on the desktops. (FWIW, I do open file/print so I can do central management of workstations from the server segment(s).)

"epigram" <nospam@spammy.com> wrote in message

news:1105986353.a4c94aea91b930fc954756052d04fc5e@bubbanews...

> I'm trying to define custom exceptions in the Windows XP firewall from my  
> SBS to allow my Symantec AV Corp (version 9) clients and servers to  
> communicate correctly. I have documents from MS and Symantec that talk  
> about how to do this, but I'm having trouble with the Symantec docs. The  
> symantec doc is

>

<http://service1.symantec.com/SUPPORT/ent-security.nsf/c9b1ac1936fbf63488256e77006521df/7346c9f9933898dd88>

> This document has a link to two other documents where they explain which  
> ports and programs you need to create exceptions for.

>

> It looks like I've got to do create two types of exceptions. Some for the  
> Symantec EXEs and some for the ports the clients/server use to communicate  
> with each other.

>

>

> The program exceptions that I plan to put in "Windows Firewall: Define  
> program exceptions" in the Windows Firewall/Domain Profile (in the Group  
> Policy Object Editor) are:

>  
> *"%PROGRAMFILES%\Symantec*  
> *AntiVirus\VPC32.exe:localsubnet:enabled:Symantec\_Client\_UI" – This one*  
> *isn't listed in the symantec document, but it is the client app that is*  
> *running on all the PCs. Not sure if I need this or not.*  
>  
> *"%PROGRAMFILES%\Symantec*  
> *AntiVirus\Rtvscan.exe:localsubnet:enabled:Symantec\_Client\_Scan" – This one*  
> *is listed in the symantec document.*  
>  
>  
> *"%PROGRAMFILES%\Symantec\LiveUpdate\Lucomserver.exe:localsubnet:enabled:Symantec\_LiveUpdate\_Client"*  
> *– This one is listed in the symantec document.*  
>  
>  
> *The ports are really what are confusing me. The port exceptions that I*  
> *plan to put "Windows Firewall: Define port exceptions" Windows*  
> *Firewall/Domain Profile are:*  
>  
> *"2967:UDP:localsubnet:enabled:Symantec\_Client\_RtvScan\_Port" – This is the*  
> *port that allows Symantec System Center to manage the Symantec Client*  
> *Security clients and also what Rtvscan uses*  
>  
> *"137:UDP:localsubnet:enabled:Symantec\_Remote\_Client\_Install\_Port1" – This*  
> *is one of the ports required to remotely install the Symantec Client*  
> *Security client from the server*  
>  
> *"138:UDP:localsubnet:enabled:Symantec\_Remote\_Client\_Install\_Port2" – This*  
> *is one of the ports required to remotely install the Symantec Client*  
> *Security client from the server*  
>  
>  
> *Any feedback on my approach (or a better one to take) would be much*  
> *appreciated!*  
>  
> *Thanks*  
>