

What to do when you are prompted by the F-Secure firewall?



Picture this, there is no such thing as a front door. Each family / person has the option of hiring a sentry to guard the front entrance of their home or not. You apparently have chosen to do so and his full name is F-Secure Internet Shield or as some refer to him as "Firewall". He has been paid by you to inform you each time a person (in this case since we are referring to computers) a program / application tries to **exit** or **enter** your PC.


Scenario 1

Moments after hiring the Firewall he prompts you with something like this:



The next question is "What do I do"?

Good question, so let's break this down so that we can determine the proper decision to make. At the very top of this screen capture it states "Application control" . This is one of several features that the Firewall offers and it is the one most users find perplexing. "Application Control" basically means a program (i.e. application) is trying to **enter** your computer or **exit** from your computer to the Internet. In the screen shot above you will note the **GREEN**  pointing to the outside world hence this indicates the program is inside your computer and trying to **exit**. The Firewall did its job and caught this "person" (i.e. program/application) trying to exit your house (Computer) but does not recognize who this person (Program) is. In essence you are being asked by the Firewall "Is this person OK to exit your house (computer)?"

If you recognize this  icon or the name "Internet Explorer" then you will note this is perhaps the program you use to access the Web.

So in this case you should make a firm decision by checking the Check Box


Do not show this dialog for this program again

and then choose the ALLOW button.

The Firewall will then permanently retain your decision and not prompt you any longer when Internet Explorer attempts to **exit** your PC. Please note, I stated "exit your PC". If the firewall catches Internet Explorer **entering** your PC you will of course be prompted and should make the same decision.

Scenario 2

Okay, let's try a slightly different scenario where you do NOT recognize the Application or Icon displayed in the [Application Control](#) pop-up window.

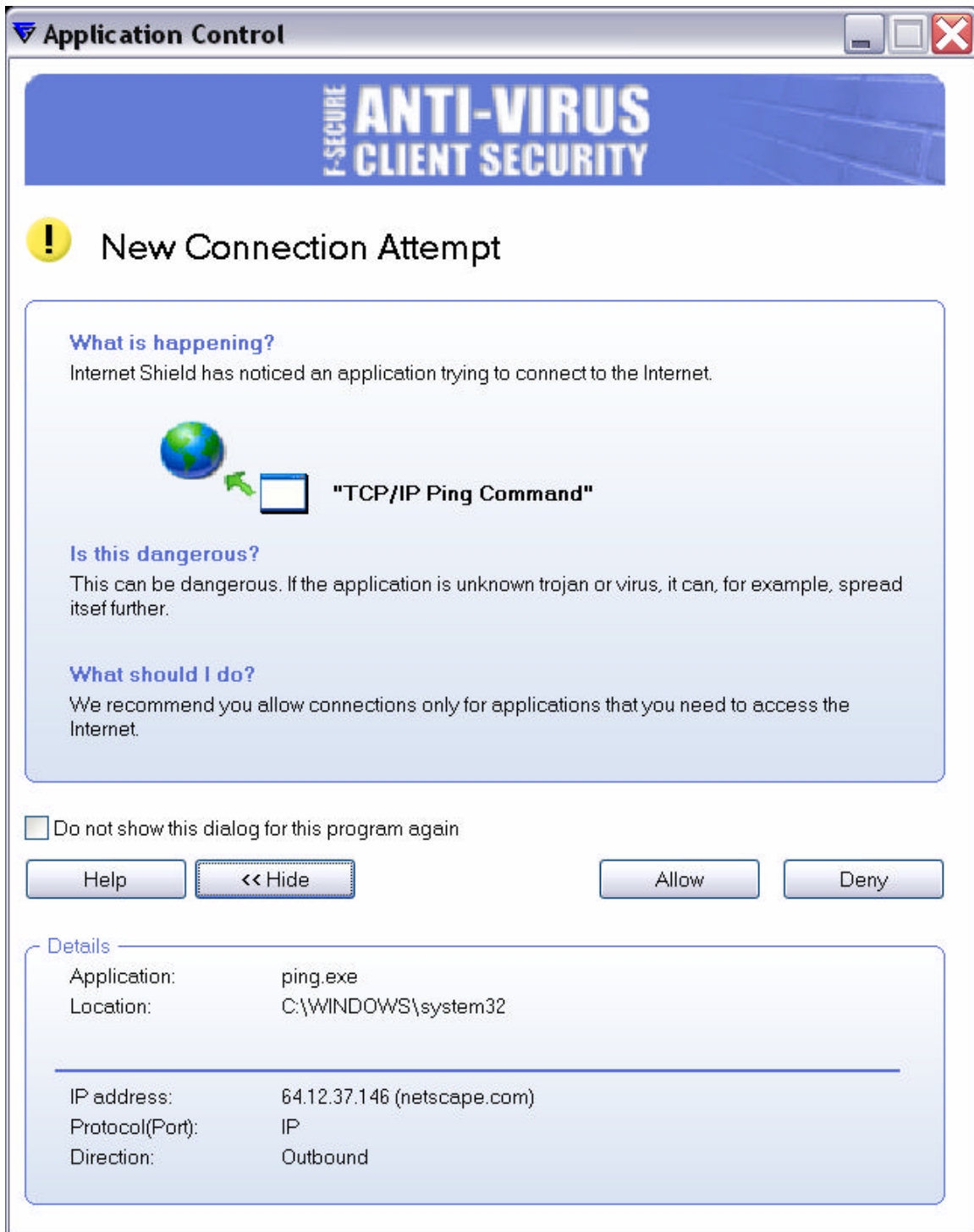
Instead of Internet Explorer or the Blue  icon you see the firewall popup looking like this:



Your obvious question once again is “What Should I Do” or “Who is TCP/IP Ping Command?”

The Firewall has informed us “TCP/IP Ping Command” is trying to (Exit or Enter?) your computer.

If you said ***Exit*** (this is correct) your computer than you right. However you don't recognize that white generic looking icon or the name “TCP/IP Ping Command”. Your next question is how do I make a decision. You could go to a search engine like Google and type in “TCP/IP Ping Command” and review some of the links to help you make a well informed decision as to what or who this is. You could dig a bit further within the Application Control popup window by choosing Details which would then look like this:

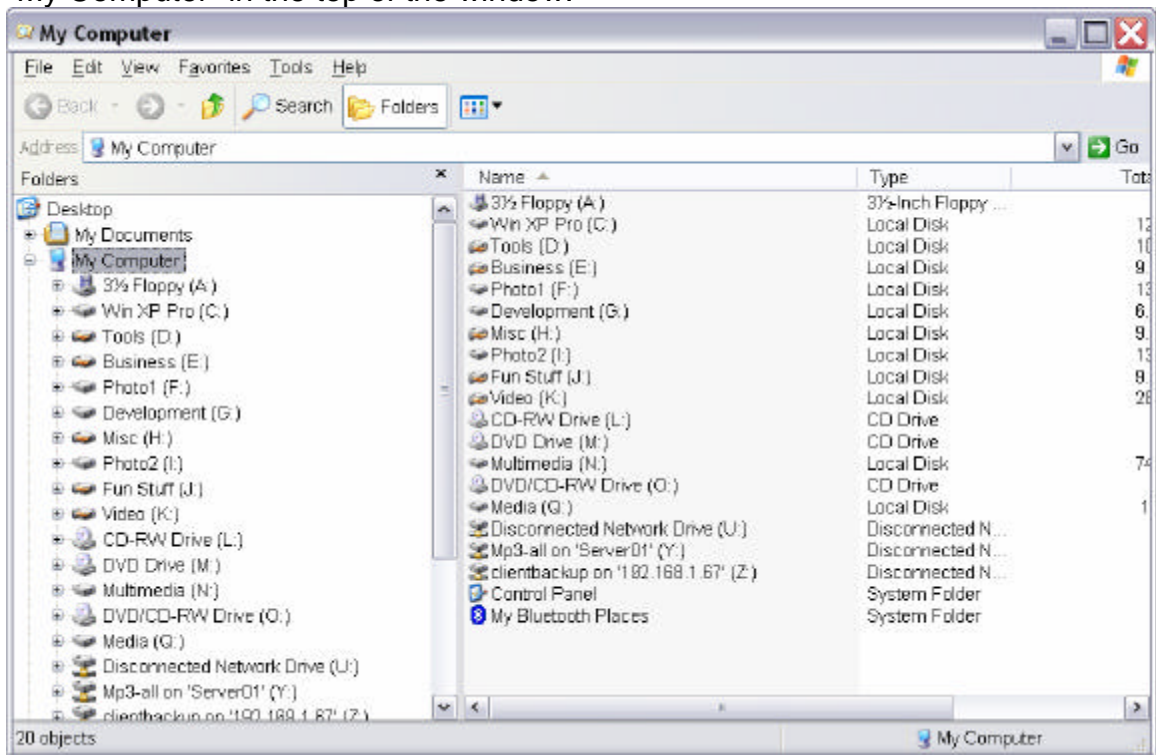


Note the DETAILS section. The Application Control Popup window tells us the full name of the Application that is trying to access the Internet and its true name is "ping.exe". It also tells us the exact location (also known as "the path") of this file on your computer which is **C:\windows\system32** (this will come in handy later). Furthermore, the Details section tells us the web site it is trying to access which is netscape.com and lastly the direction of the call which is Outbound or

“exiting your computer”. With this additional information you can now go to your favorite search engine such as Google or AOL and search out “ping.exe”. This will give you more accurate information on the exact application/program that is exiting your PC than just searching the word “ping”.

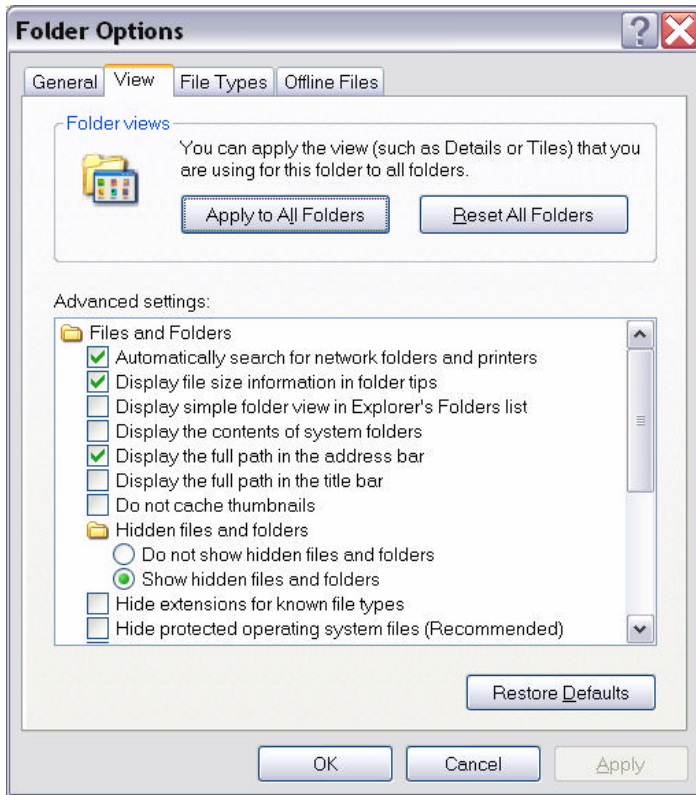
If you recall I stated above we now know the path of the file. How is this helpful you may ask? Just follow these steps and you see who the Owner of this file is:

While keeping the Application control window open, please open Windows Explorer (not Internet Explorer) by pressing the key that looks like a Windows flag on your keyboard + E. A window appears similar but not exact to this with “My Computer” in the top of the window:



At this point, single click on the C drive. Then click on the Windows folder and then finally the System32 folder. (Note if you are unable to see any of these folders or files you will have to enable this type of viewing by choosing within this same window (Tools/Folder Options/View then Select the circular button that says “Show Hidden Files and Folders” and also deselect the check box “Hide Extensions for known file types” as shown in the diagram below.

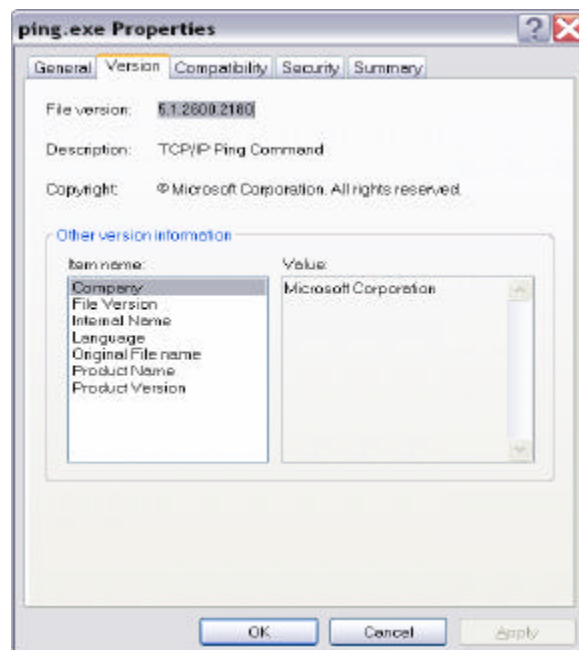
Click Apply then OK.



Now you are back at the previous screen and are able to navigate to
C:
then the Windows folder
then the System32 folder.
Now scroll and look for the file "ping.exe"

Once you see this file, Right Click on Ping.exe (not a left click unless you have reversed your mouse options) and choose Properties. You will see several Tabs at this point so choose "Version".

It should look
this:



something like

Note where it states Company “Microsoft Corporation”. This tells us this file was created by Microsoft so we can therefore determine who the creator is. With this information in hand we are able to Check Do not show this dialog for this program again and then choose the ALLOW button. This is a good methodology to help determine what decision you should make (Allow or Deny) when you are uncertain. In some cases you will not see a Version tab nor will you see a company or corporation listed and the only information you have is the full file name. It is at this point you should review the other criteria found by clicking the DETAILS button as stated above to make a decision as to whether or not you should ALLOW or DENY this particular program.

Most legitimate companies will include proper information under the version tab. I would be more suspicious of the file if information is not included in this section. This however does not mean the file exiting or entering your PC is malicious. It basically means you may have to do more digging to find out further information on this particular file

Scenario 3

If you do not have the time to search out a file you can choose Allow or Deny without checking the box. Once this application attempts to access your computer or the Net a second time you will be prompted again. It is most important to realize if you recognize the name of the application trying to exit or enter than it is probably safe to choose Allow and check the box. Also, if you invoked the execution of an application via the clicking of an icon or the installation of software as an example, and the Firewall prompted you with an Application Control window a moment later, than you should choose Allow and then the check box.

These instructions are not intended to be complete in how to determine a Best decision but rather they are ideas on how to determine “What should I do” when the Firewall prompts you.

Anthony Gliozzo
PC Professional Group Inc.
F-Secure reseller