Foxtrot® powered by ENABLESOFT

FOXHUB DEPLOYMENT GUIDE

Setting Up Your FoxHub

Intended for administrators in charge of planning, implementing and maintaining the deployment of Foxtrot, FoxBot and FoxHub in an organization.

Table of Contents

What is FoxHub? 3
Before You Start 3
Configuring Your FoxHub 4
Configuring Your FoxBot 14
Wrap Up & Further Troubleshooting 21
Contact Us 22

What is FoxHub?

FoxHub is our newest application allowing you to centrally control your FoxBot deployment. View all of your Bots and know what they are doing at all times. Put them to work by adding a job for an individual bot, or by adding a team job for multiple bots to complete. FoxHub is installed with the Foxtrot Suite, and does not require any other installation to function. Some considerations to take into account before using FoxHub:

- Each bot requires a FoxBot license to run.
- The number of bots that can participate is limited to the number of your FoxBot licenses
- Bots can be set up on either a virtual or physical machine
- All machines must reside on the same network
- FoxHub must be running in order to send work to your bots.
- If FoxHub is closed, all bots will stop their work.

Before You Start

For full installation and licensing instructions, please refer to our Deployment Guide. This guide assumes everything is installed and licensed already. All FoxHub and FoxBot machines must be on the same version of the Foxtrot Suite to communicate properly.

If there are communication issues between the FoxHub and FoxBot machines, in certain cases, you will have to make changes to your firewall settings. Examples of this are:

- A Bot showing a status of 'Offline' after being added to the FoxHub
- A Bot not starting the FoxBot client after a Job is Run
- A Bot unable to receive a project after a Job is Run

This guide will outline the steps that need to be taken to ensure your FoxHub and FoxBots are configured optimally.

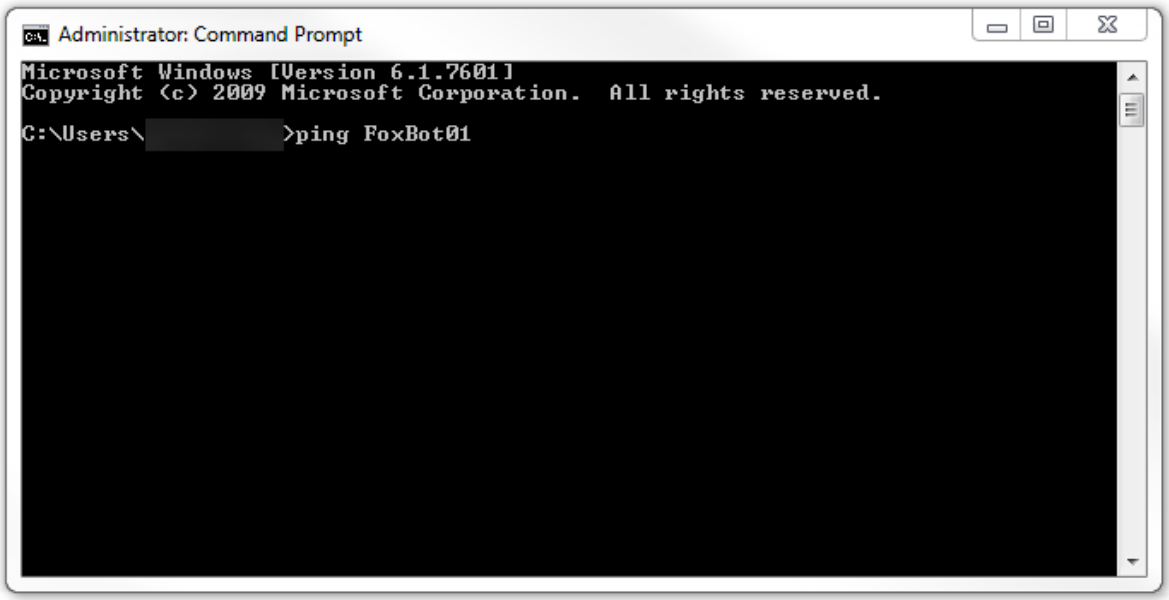
Configuring Your FoxHub

FILE & PRINTER SHARING RULES

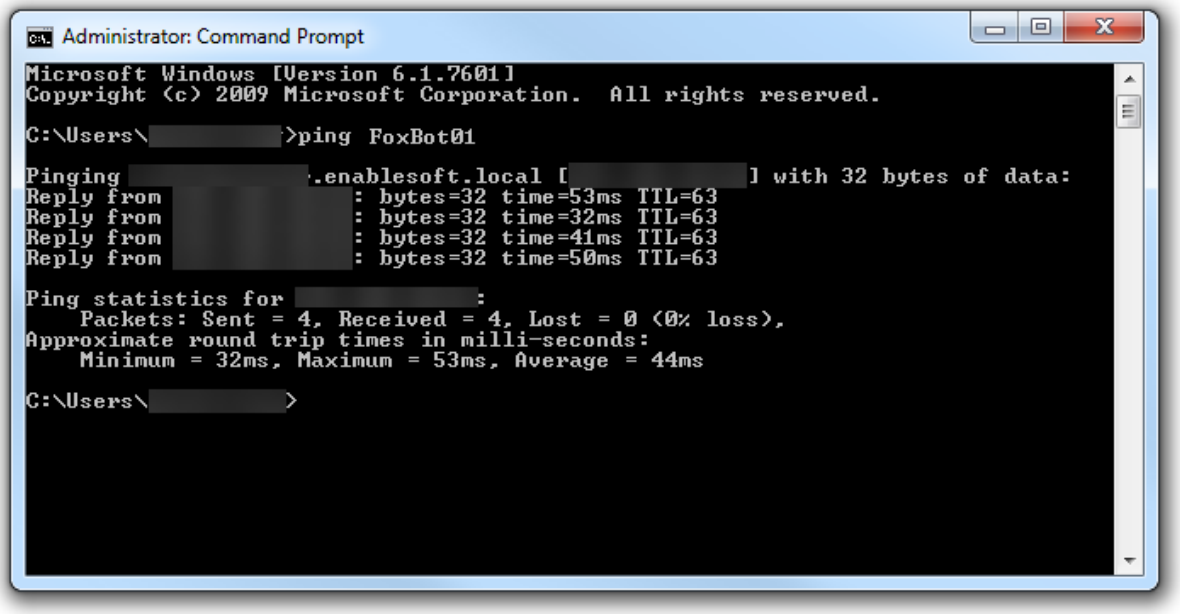
The first thing to check is basic communication from the FoxHub to the FoxBot machines. To do this, we will want to ping the other machines from the FoxHub computer.

1. Open Command Prompt. You can do this by searching in your Start Menu for “cmd.exe” or “Command Prompt”.

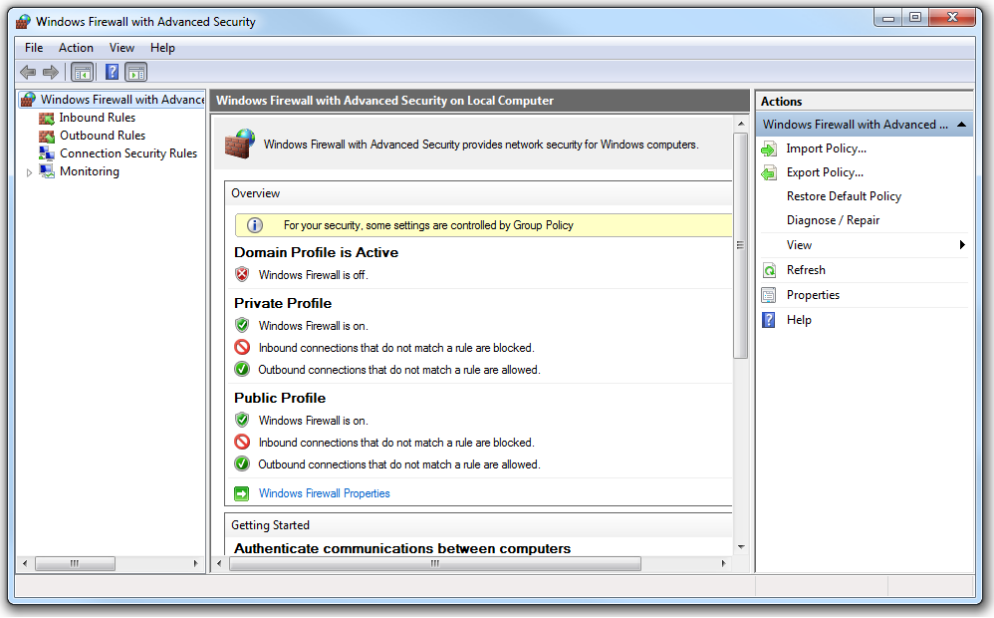
2. Input the command “ping <MachineName>”. Replace <MachineName> with the name of your FoxBot computers. In this example, it is “FoxBot01”



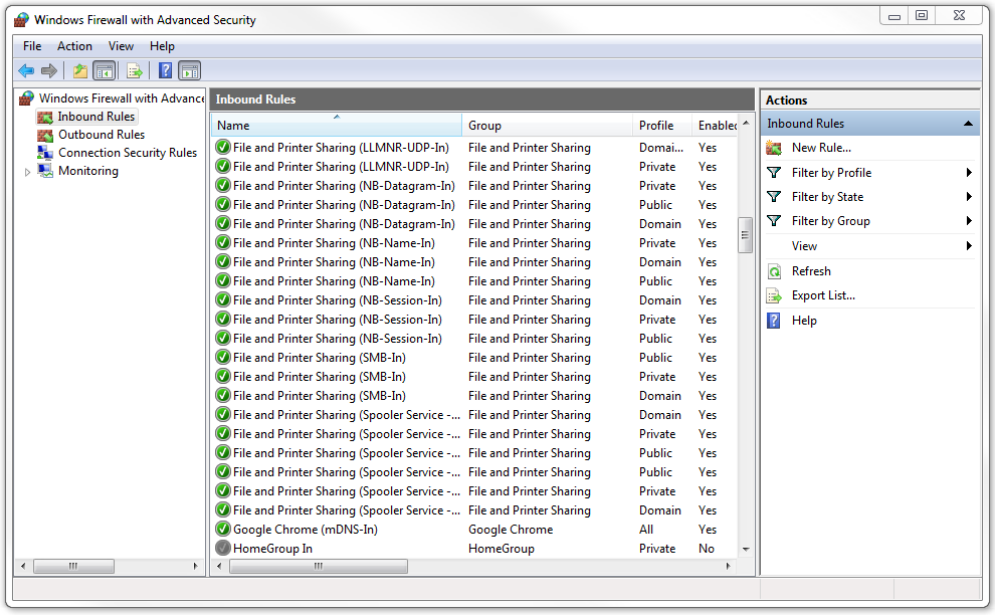
3. If the command returns similar to the screenshot below, you can skip to the next section. Otherwise, communication is being blocked between the two machines and you will need to continue in this section.



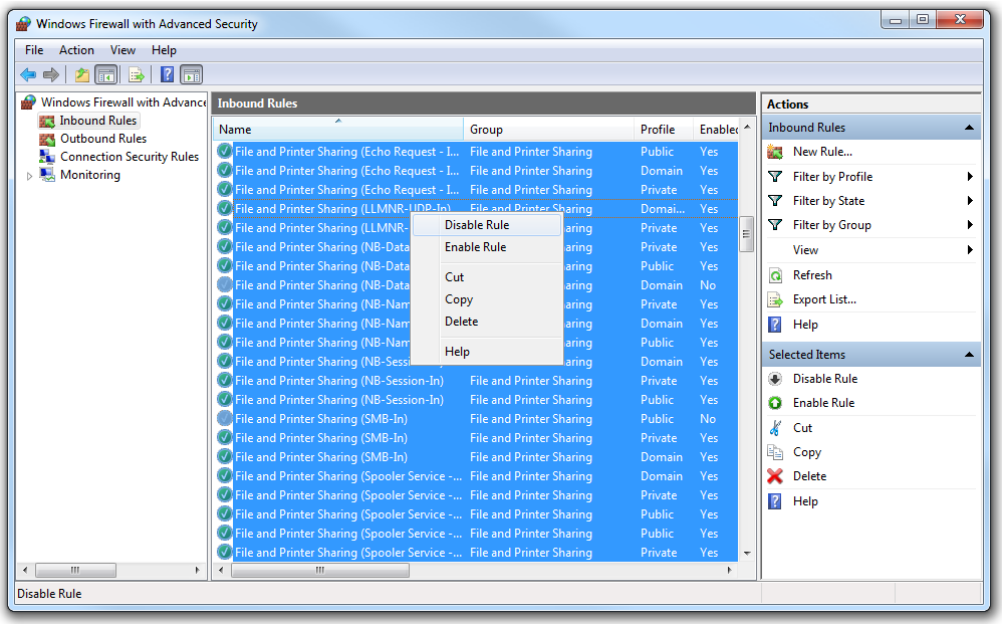
4. If there is a negative result after the ping command is run, you will need to enable your 'File and Printer Sharing' firewall rules. Begin by opening Windows Firewall with Advanced Security.



5. On the left panel, click the Inbound Rules section. This will pull up a list of firewall rules.



6. Find the block of all 'File and Printer Sharing' rules. Select them all by clicking on the first in the list, then holding shift and clicking on the last item.

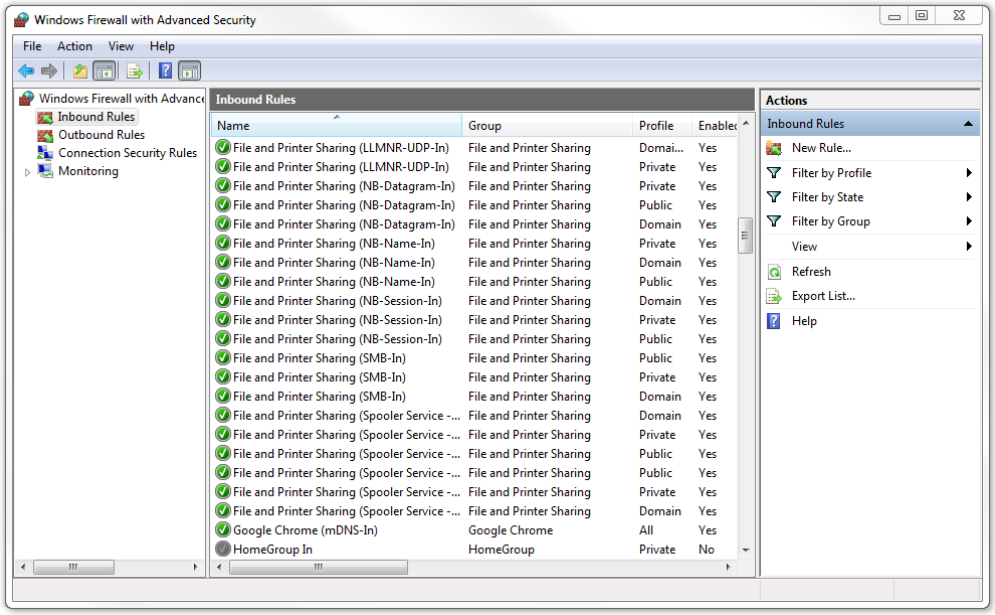


7. Right click on this selection, and select 'Enable Rule'.
8. After enabling all the File and Printer sharing firewall rules, return to step 1 of this section to run a ping command again. If the command fails again, you will have to contact your network administrators or IT department for further assistance.

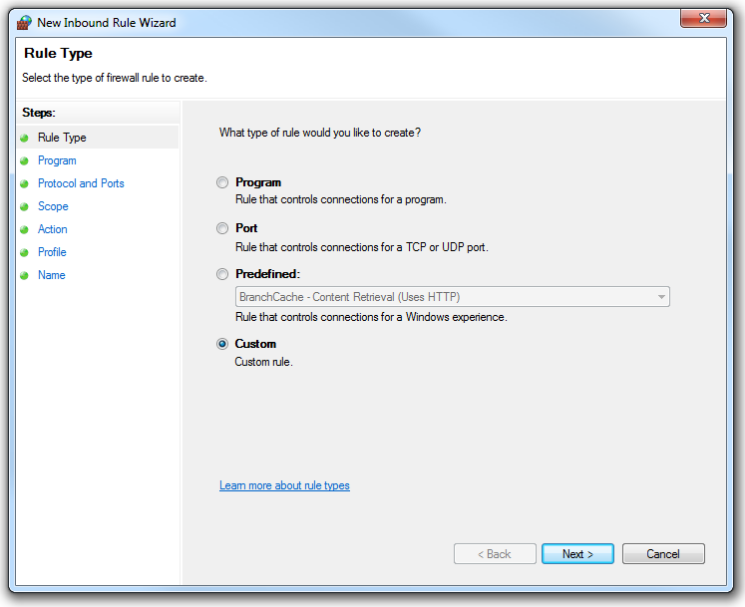
OTHER FIREWALL CONFIGURATIONS

If you are still experiencing communication issues between your FoxHub and FoxBot, there are some additional steps we can take. Now that basic file sharing has been confirmed, additional firewall rules can be setup. This involves opening specific ports to allow traffic through from our applications.

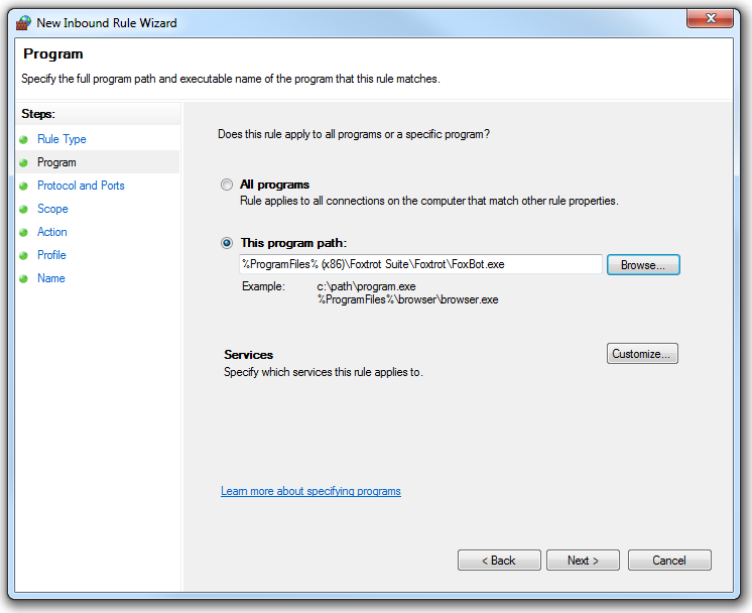
1. Begin by opening Windows Firewall with Advanced Security. Click on the 'Inbound Rules' section on the left hand side.



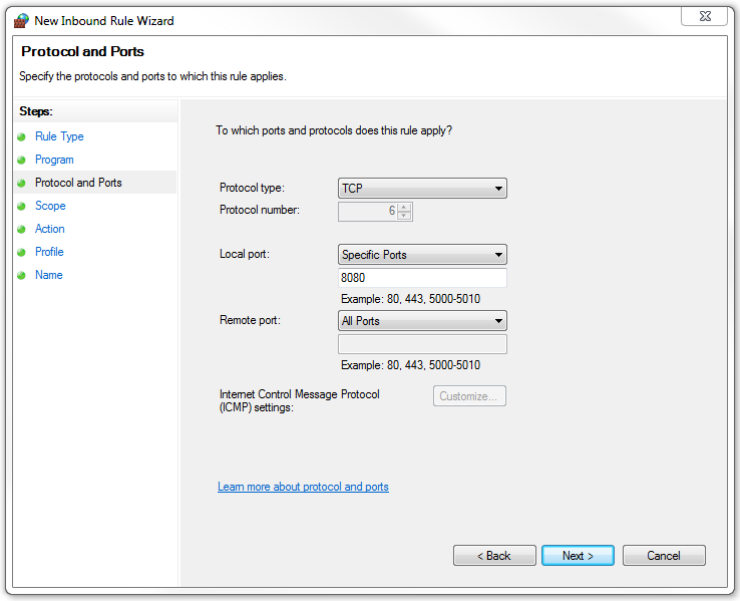
2. On the right hand menu, click the 'New Rule' button. We will be creating a Custom rule. Click 'Next' to proceed.



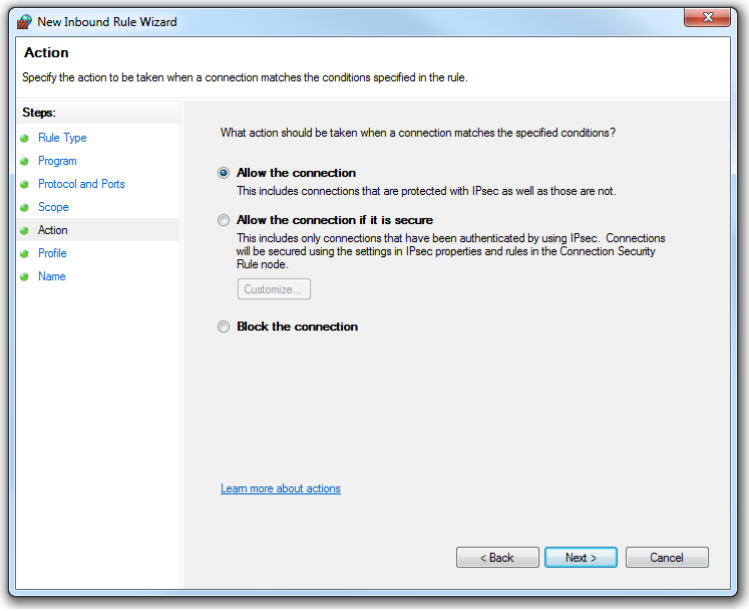
3. Choose the radio button for "This program path:". Click the 'Browse' button and navigate to where FoxBot is installed. By default this is *C:\Program Files (x86)\Foxtrot Suite\Foxtrot\FoxBot.exe* . Click 'Next' to continue.



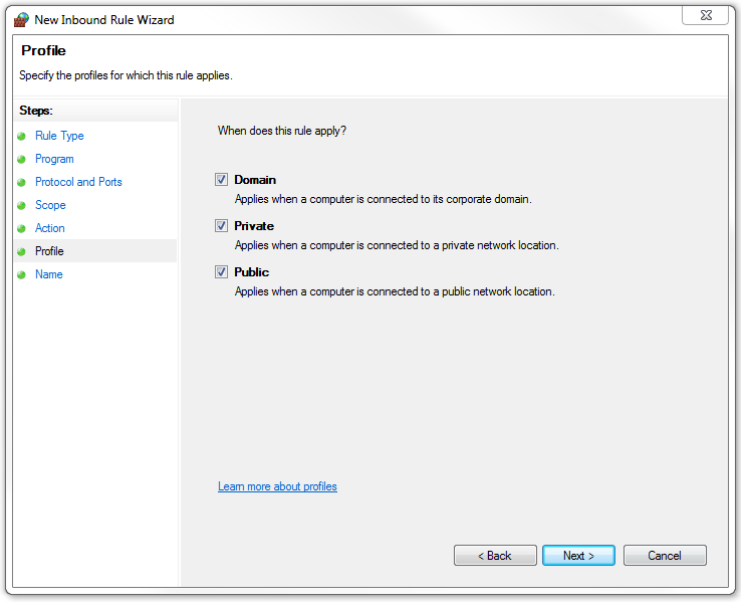
4. The ‘Protocol type’ dropdown should be set to “TCP”. ‘Local port’ should be set to “Specific ports” with “8080” in the field below it. ‘Remote port’ should remain on the “All Ports” option. Click ‘Next’ to continue.



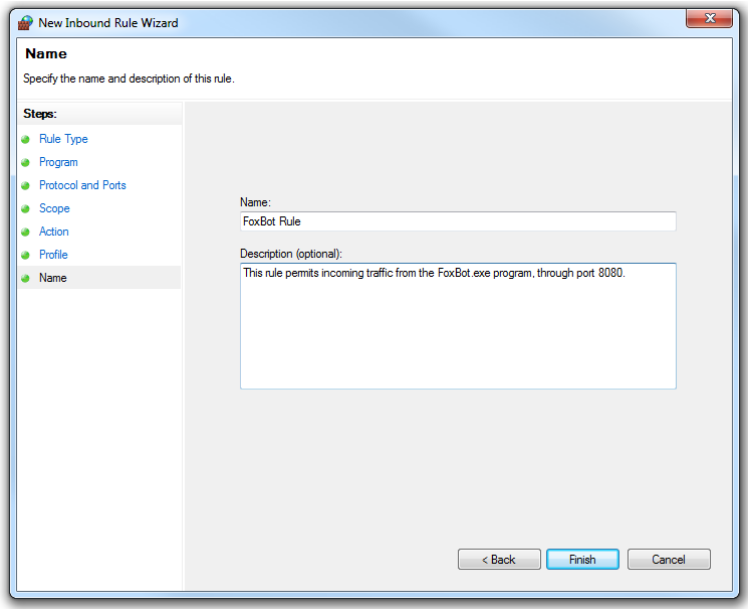
5. On the ‘Scope’ page, nothing needs to change. For both questions, the radio button will stay on “Any IP address”. Click ‘Next’ to proceed.
6. Select the option to “Allow the connection” on this page. Click ‘Next’ to continue.



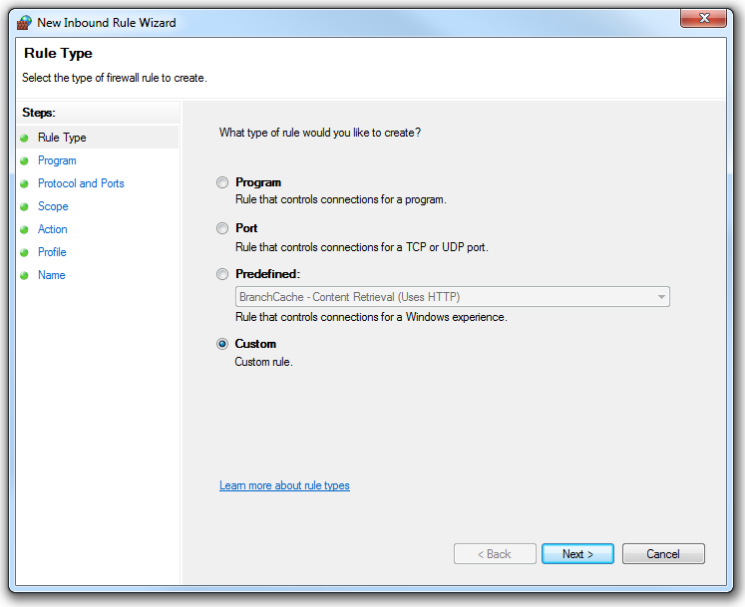
7. On the Profile page, select which option will apply. If the FoxBot machine is on a domain, choose the 'Domain' checkbox but if it is on a public network, choose the 'Public' checkbox. If you're unsure, select all the boxes. Click 'Next' to move on.



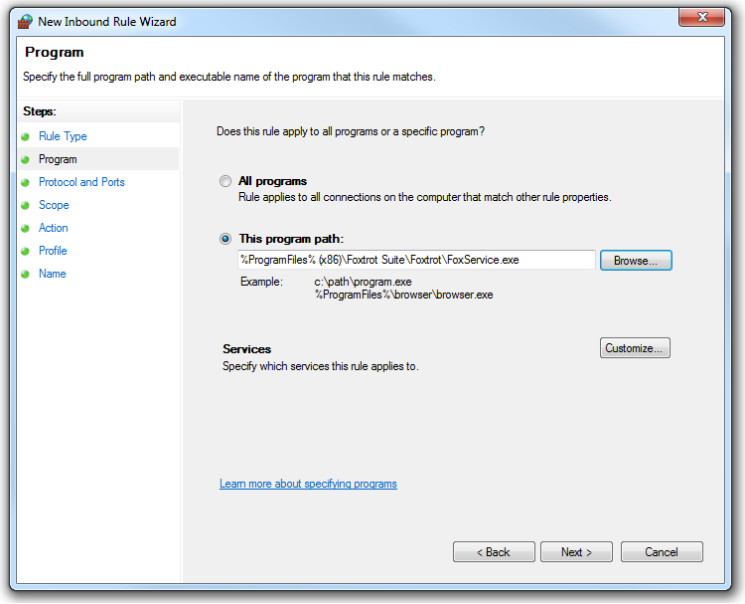
8. Input a friendly name for this rule, and an optional description. A good name would be 'FoxBot Rule'. Click 'Finish' to create the rule. Continue the steps on the next page to create the next inbound rule.



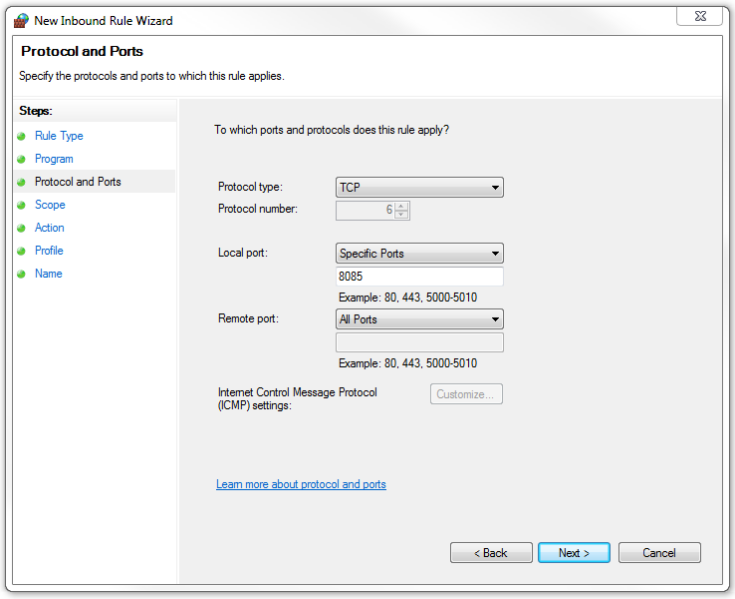
9. On the right hand menu of the Windows Firewall window, click the 'New Rule' button. We will be creating a Custom rule. Click 'Next' to proceed.



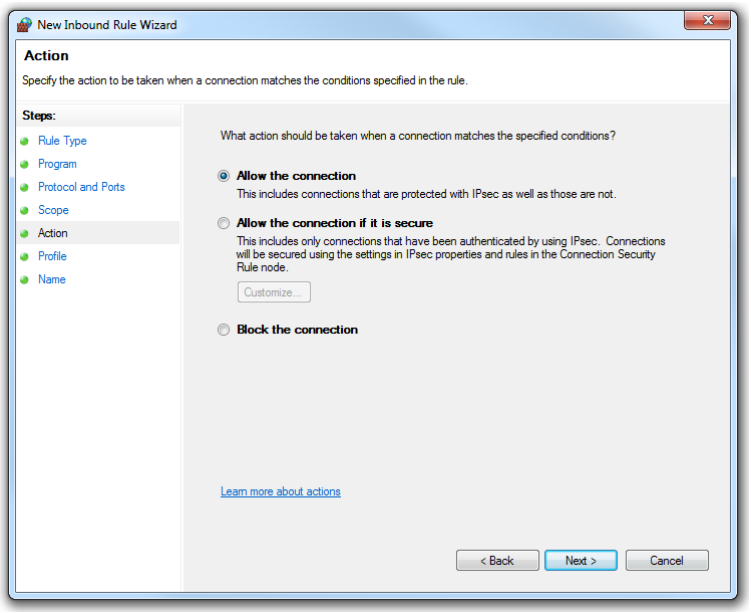
10. Choose the radio button for "This program path:". Click the 'Browse' button and navigate to where FoxService is installed. By default this is *C:\Program Files (x86)\Foxtrot Suite\Foxtrot\FoxService.exe* . Click 'Next' to continue.



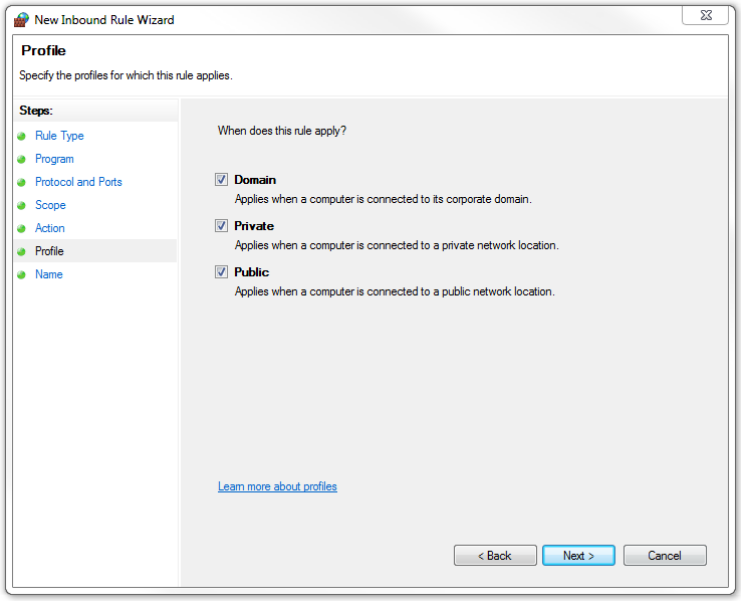
11. The ‘Protocol type’ dropdown should be set to “TCP”. ‘Local port’ should be set to “Specific ports” with “8085” in the field below it. ‘Remote port’ should remain on the “All Ports” option. Click ‘Next’ to continue.



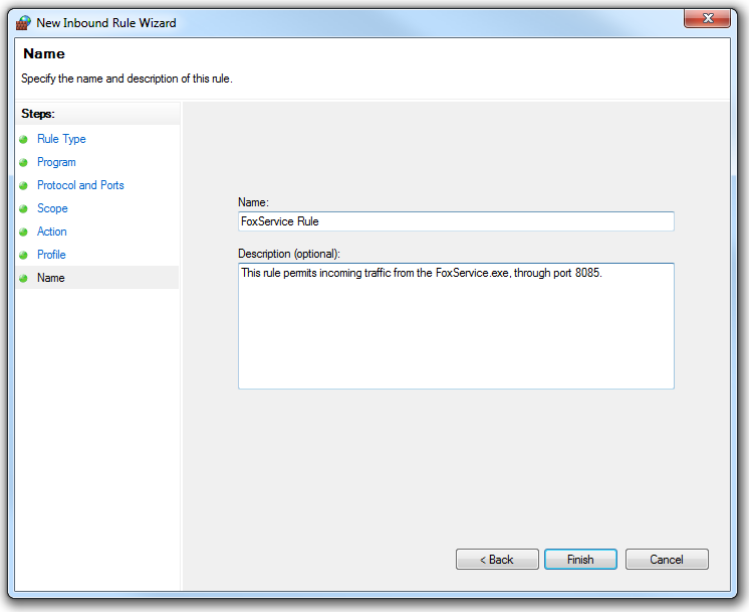
12. On the ‘Scope’ page, nothing needs to change. For both questions, the radio button will stay on “Any IP address”. Click ‘Next’ to proceed.
13. Select the option to “Allow the connection” on this page. Click ‘Next’ to continue.



14. On the Profile page, select which option will apply. If the FoxBot machine is on a domain, choose the 'Domain' checkbox but if it is on a public network, choose the 'Public' checkbox. If you're unsure, select all the boxes. Click 'Next' to move on.



15. Input a friendly name for this rule, and an optional description. A good name would be 'FoxService Rule'. Click 'Finish' to create the rule.



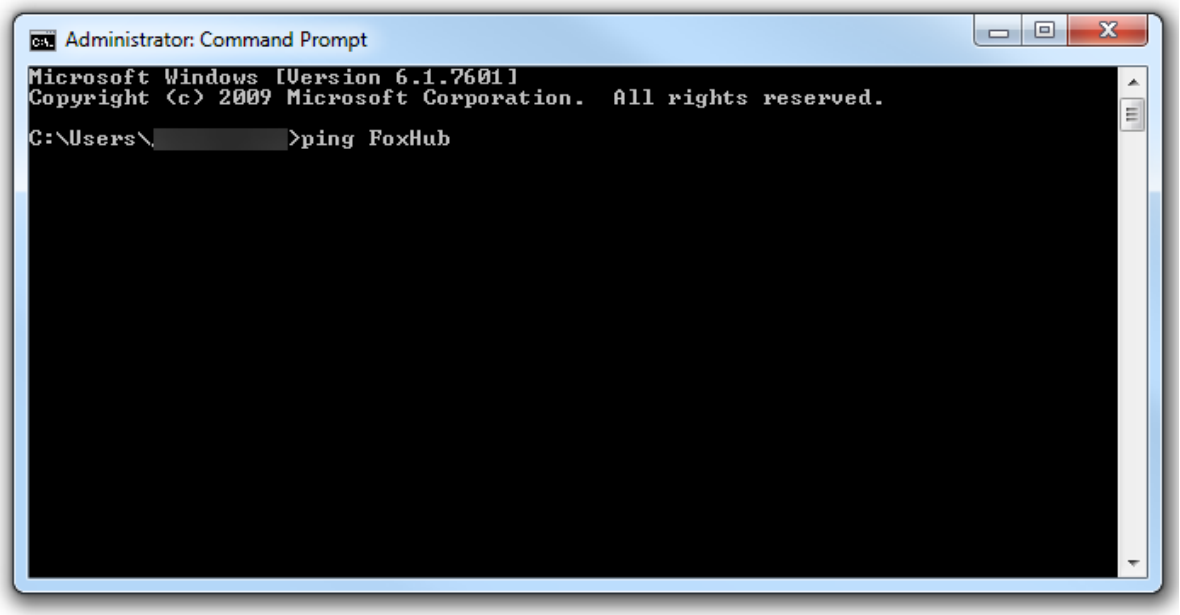
After these rules have been set up, check FoxHub to see if the issue has been resolved. If there are still communication issues (such as your Bots showing offline), then continue on with this guide.

Configuring Your FoxBot

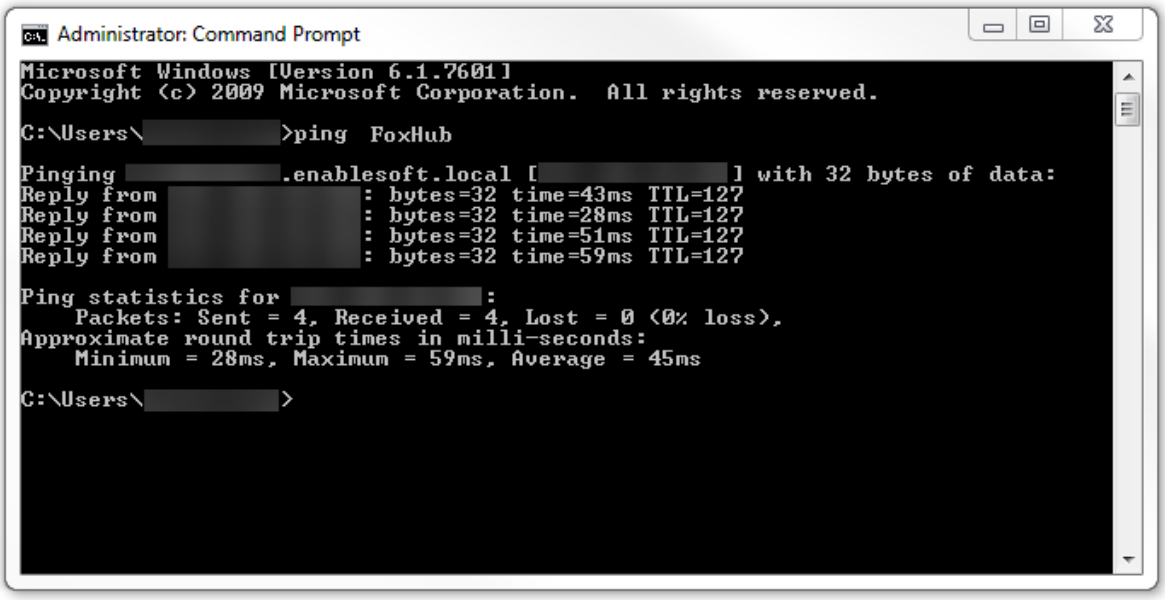
FILE & PRINTER SHARING RULES

The first thing to check is basic communication from the FoxBot to the FoxHub machine. To do this, we will want to ping the other machines from the FoxBot computer.

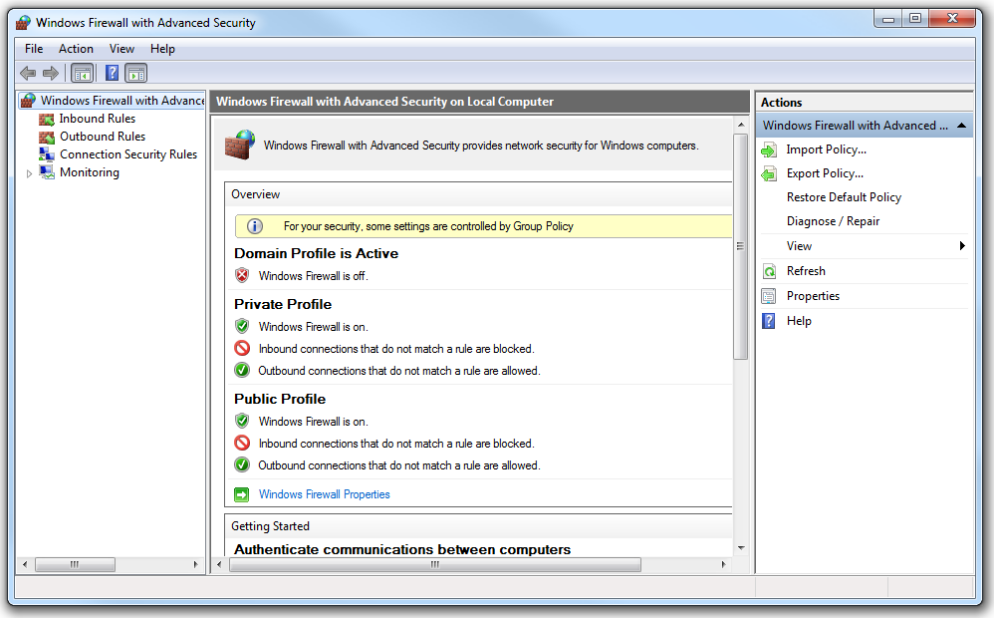
1. Open Command Prompt. You can do this by searching in your Start Menu for “cmd.exe” or “Command Prompt”.
2. Input the command “ping <MachineName>”. Replace <MachineName> with the name of your FoxHub computers. In this example, it is “FoxHub”.



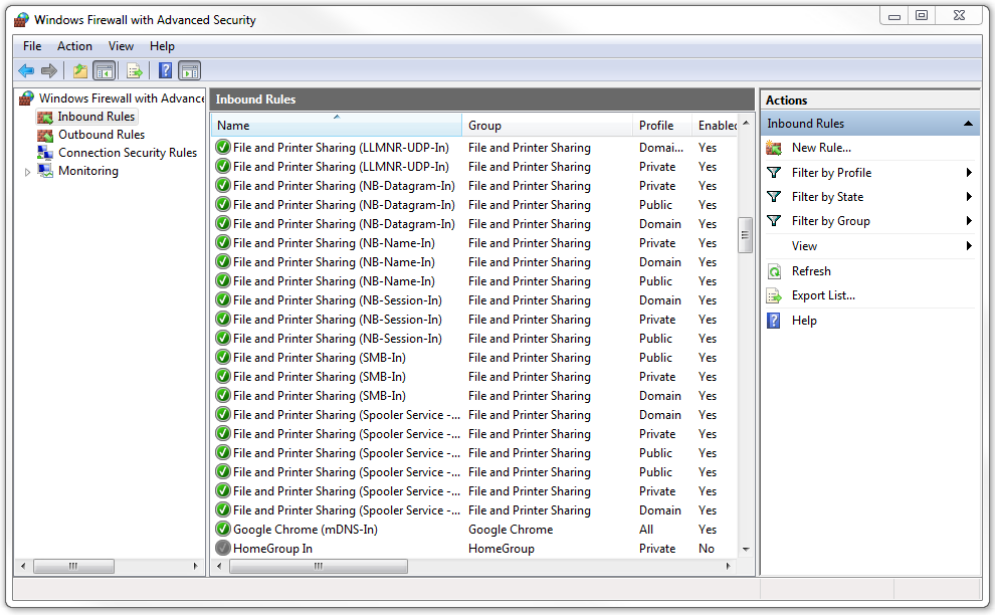
3. If the command returns similar to the screenshot below, you can skip to the next section. Otherwise, communication is being blocked between the two machines and you will need to continue in this section.



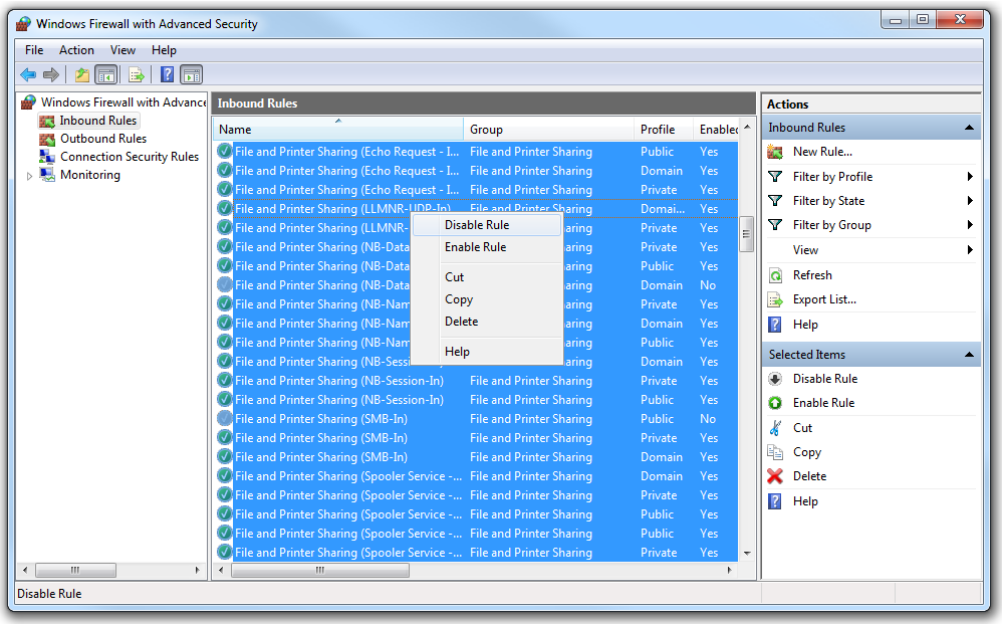
4. If there is a negative result after the ping command is run, you will need to enable your 'File and Printer Sharing' firewall rules. Begin by opening Windows Firewall with Advanced Security.



5. On the left panel, click the Inbound Rules section. This will pull up a list of firewall rules.



6. Find the block of all 'File and Printer Sharing' rules. Select them all by clicking on the first in the list, then holding shift and clicking on the last item.

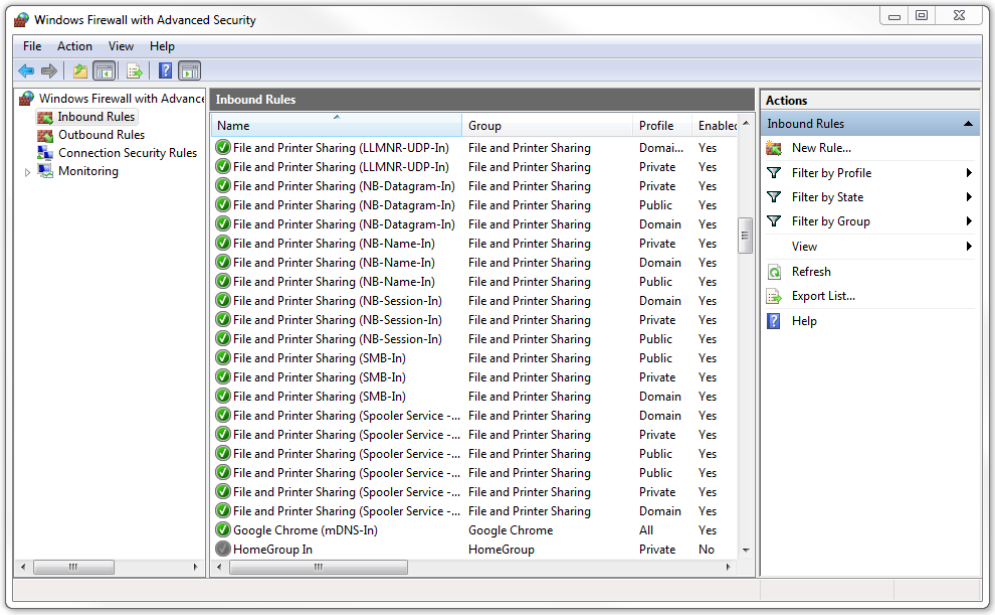


7. Right click on this selection, and select 'Enable Rule'.
8. After enabling all the File and Printer sharing firewall rules, return to step 1 of this section to run a ping command again. If the command fails again, you will have to contact your network administrators or IT department for further assistance.

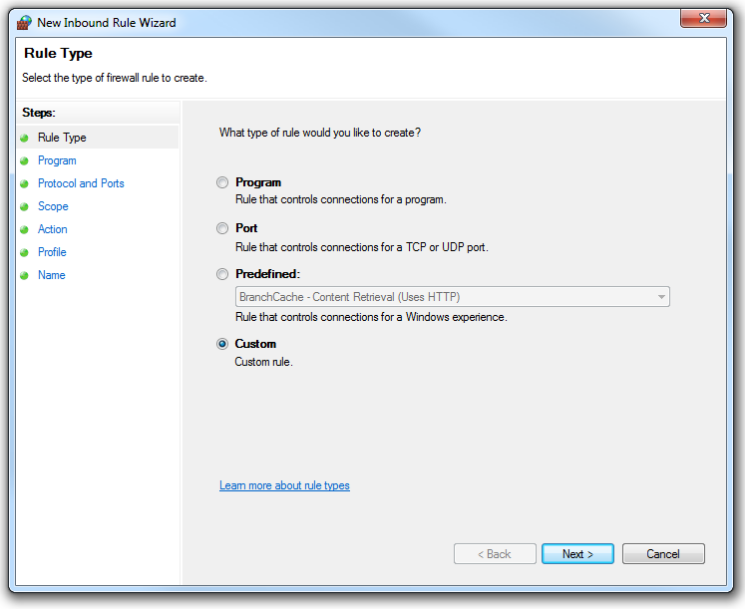
OTHER FIREWALL CONFIGURATIONS

If you are still experiencing communication issues from the FoxBot to the FoxHub, there are some additional steps we can take. Now that basic file sharing has been confirmed, additional firewall rules can be setup. This involves opening specific ports to allow traffic through from our applications.

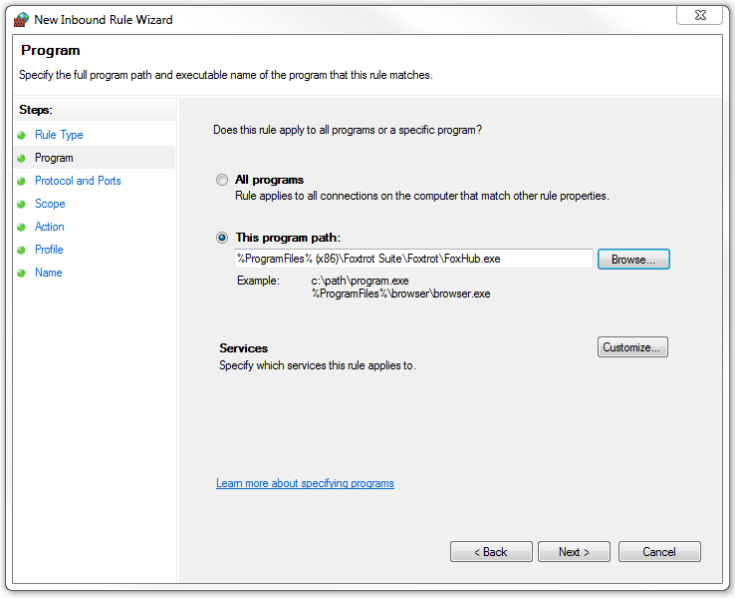
1. Begin by opening Windows Firewall with Advanced Security. Click on the 'Inbound Rules' section on the left hand side.



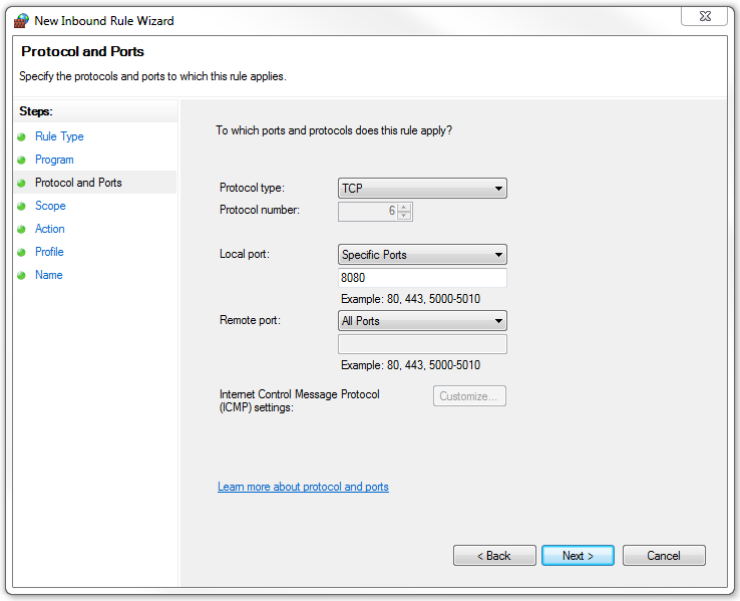
2. On the right hand menu, click the 'New Rule' button. We will be creating a Custom rule. Click 'Next' to proceed.



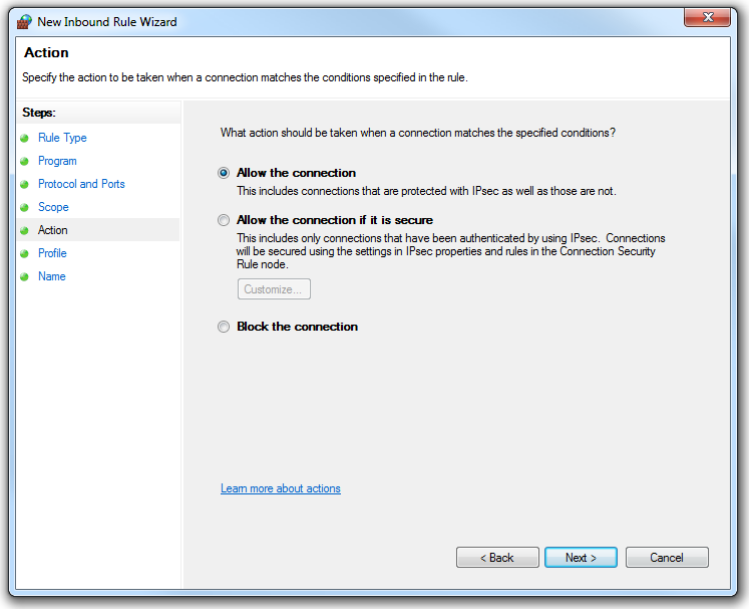
3. Choose the radio button for "This program path:". Click the 'Browse' button and navigate to where FoxHub is installed. By default this is *C:\Program Files (x86)\Foxtrot Suite\Foxtrot\FoxHub.exe* . Click 'Next' to continue.



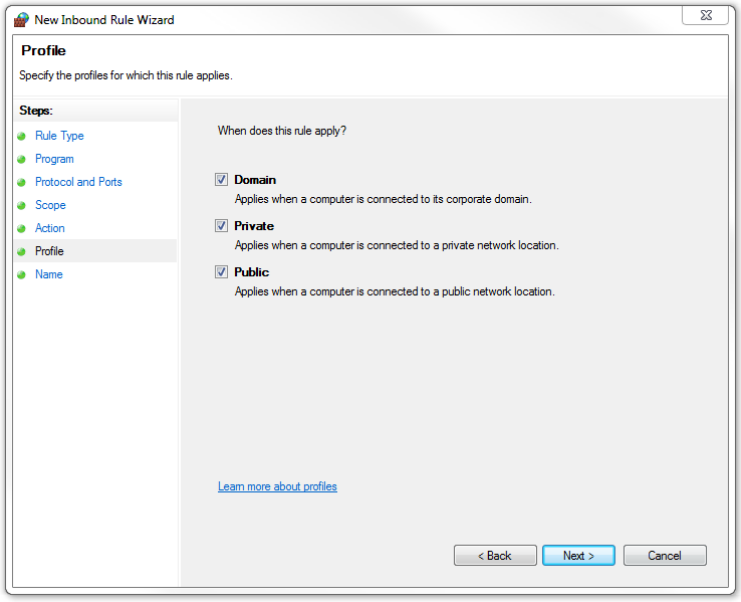
4. The ‘Protocol type’ dropdown should be set to “TCP”. ‘Local port’ should be set to “Specific ports” with “8080” in the field below it. ‘Remote port’ should remain on the “All Ports” option. Click ‘Next’ to continue.



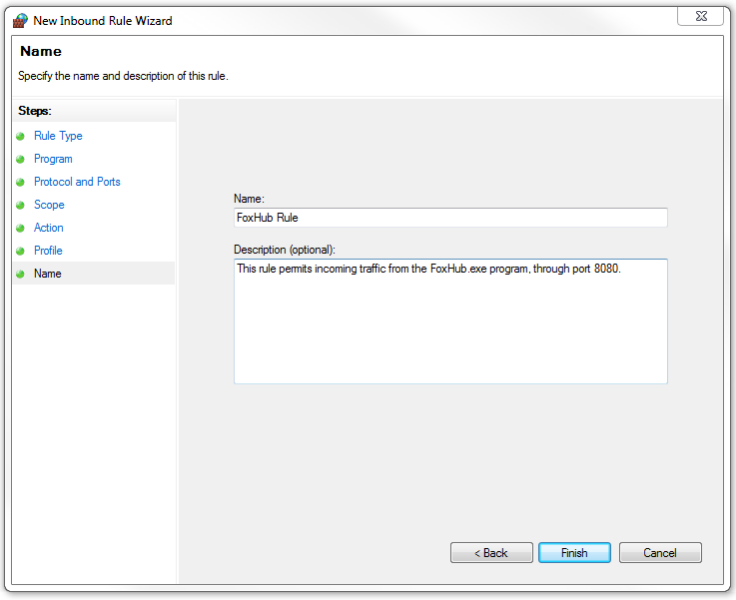
5. On the ‘Scope’ page, nothing needs to change. For both questions, the radio button will stay on “Any IP address”. Click ‘Next’ to proceed.
6. Select the option to “Allow the connection” on this page. Click ‘Next’ to continue.



7. On the Profile page, select which option will apply. If the FoxBot machine is on a domain, choose the 'Domain' checkbox but if it is on a public network, choose the 'Public' checkbox. If you're unsure, select all the boxes. Click 'Next' to move on.



8. Input a friendly name for this rule, and an optional description. A good name would be 'FoxHub Rule'. Click 'Finish' to create the rule. Continue the steps on the next page to create the next inbound rule.



Wrap Up & Further Troubleshooting

After setting up Rules on all required machines, you should be able to start running Jobs with your FoxBots! If you are still experiencing issues, there may be some external forces at play that are interfering with communication. If this is the case, check the following:

- Foxtrot Suite versions on all machines
- Virus protection
- Additional firewall programs
- Port forwarding or blocking
- Network and/or domain policies

These could all potentially affect the communications that are being attempted. Each situation will vary between different environments, and your network or IT team would be most familiar with these external programs.

THANK YOU FOR YOUR TIME.

Contact Us

Customer Success Team

success@enablesoft.com

800-658-1147

www.enablesoft.com