



FOXHUB TROUBLESHOOTING

Setting Up Your FoxHub

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

Table of Contents

What is FoxHub?	3
Before You Start	3
Configuring Your FoxHub Machine	4
Configuring Your FoxBot Machine(s)	11
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.

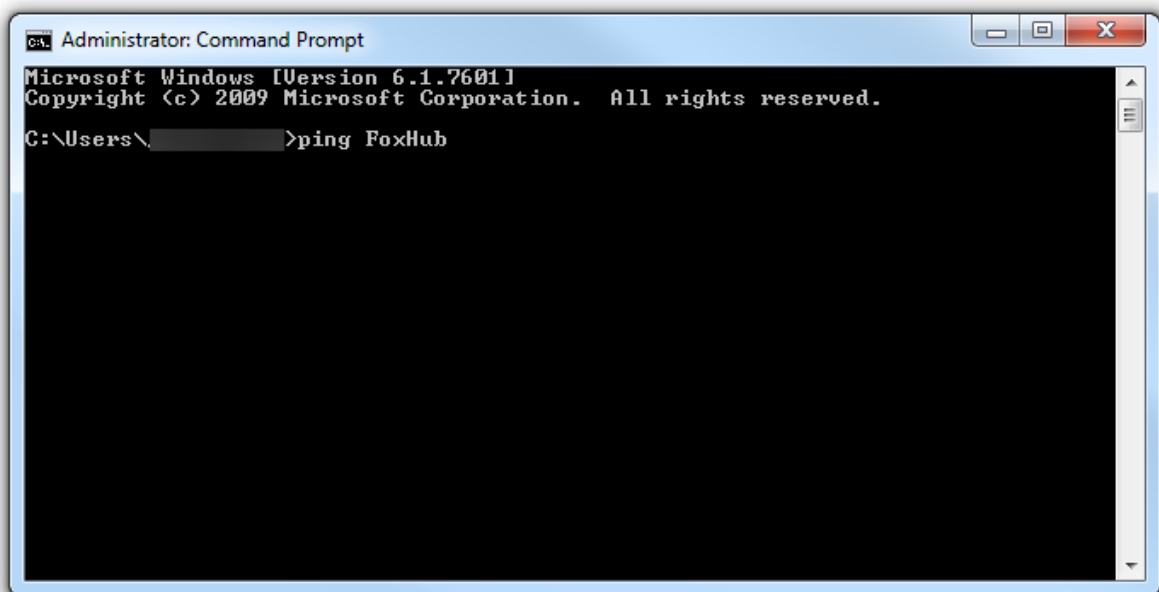
Before starting, please ensure the "FoxService.exe" Service is running on all troubled machines. If this is not running, FoxHub will not be able to communicate with any FoxBot machines.

Configuring Your FoxHub Machine

FILE & PRINTER SHARING RULES

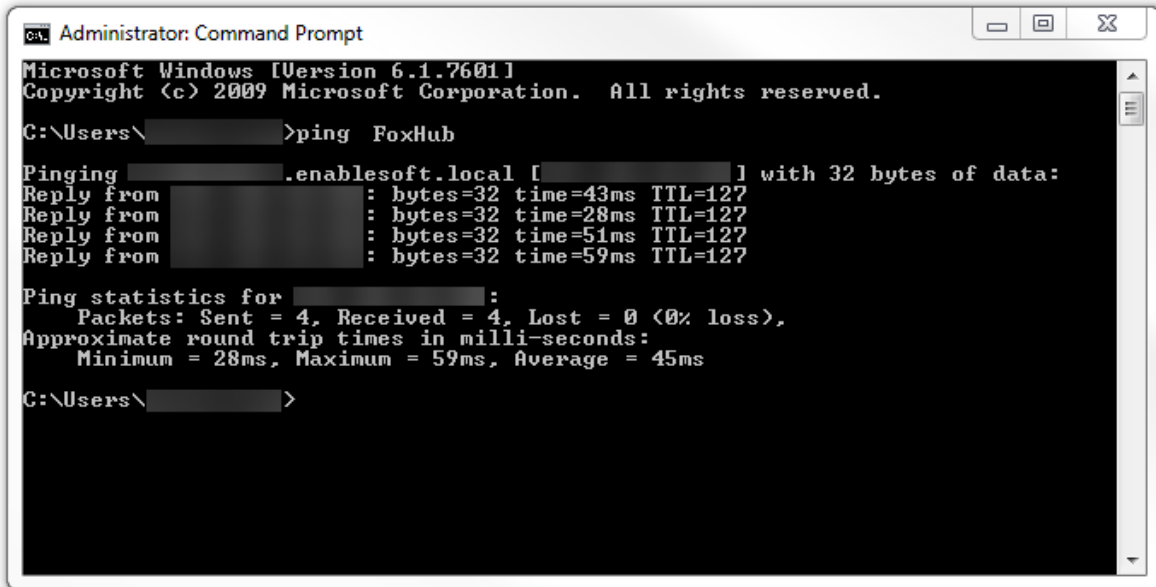
The first thing to check is basic communication from the FoxBot to the FoxHub machine. To do this, we will want to ping the FoxHub machine from one of the FoxBot computers.

1. Open Command Prompt on your FoxBot machine. 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 computer. In this example, it is “FoxHub”



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\>ping FoxHub
```

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



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

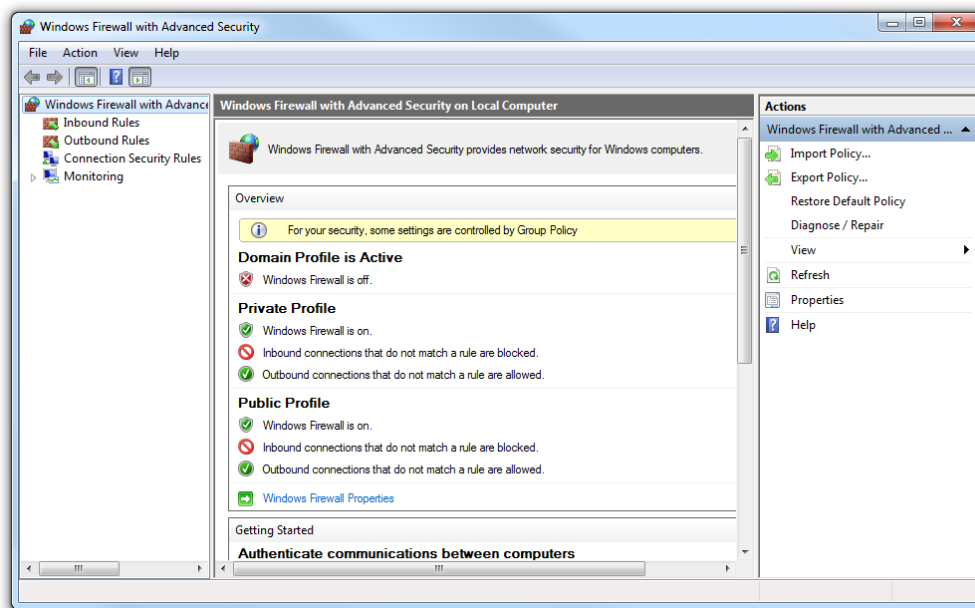
C:\Users\>ping FoxHub

Pinging .enablesoft.local [ ] with 32 bytes of data:
Reply from : bytes=32 time=43ms TTL=127
Reply from : bytes=32 time=28ms TTL=127
Reply from : bytes=32 time=51ms TTL=127
Reply from : bytes=32 time=59ms TTL=127

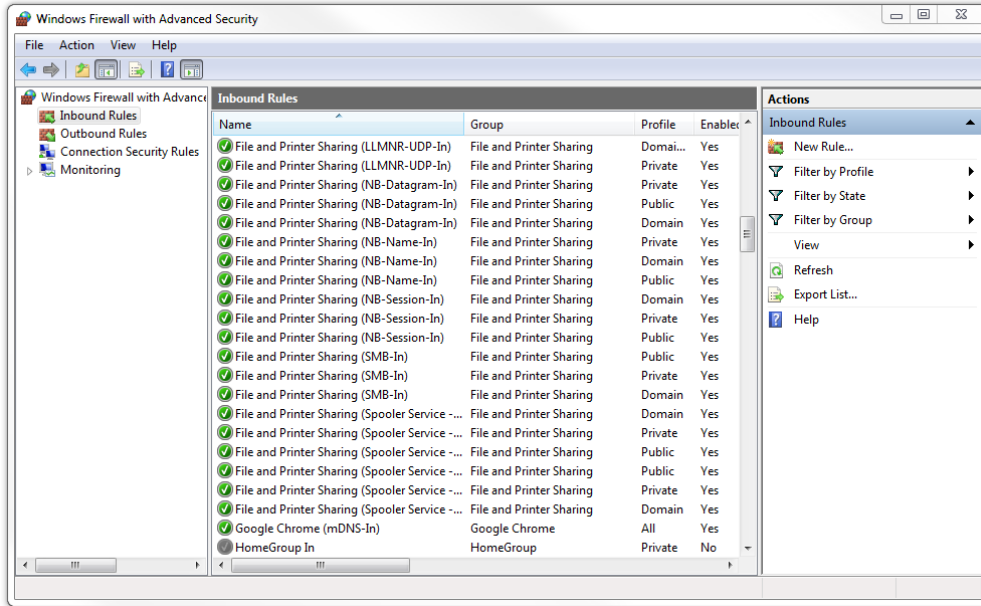
Ping statistics for :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 59ms, Average = 45ms

C:\Users\>
```

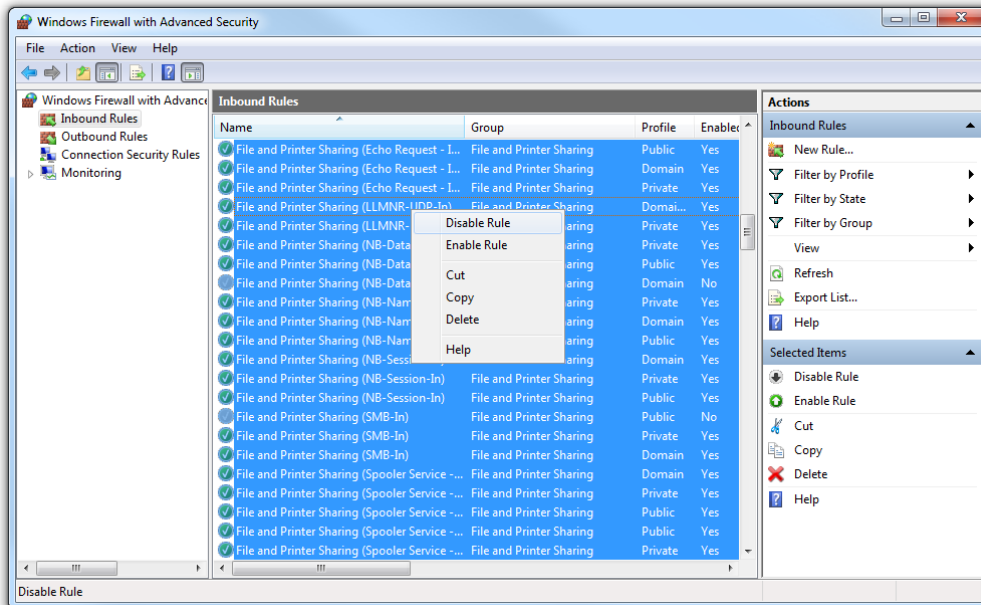
- If there is a negative result after the ping command is run, you will need to enable your ‘File and Printer Sharing’ firewall rules on the FoxHub machine. Begin by opening Windows Firewall with Advanced Security, on your FoxHub machine.



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



- 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.

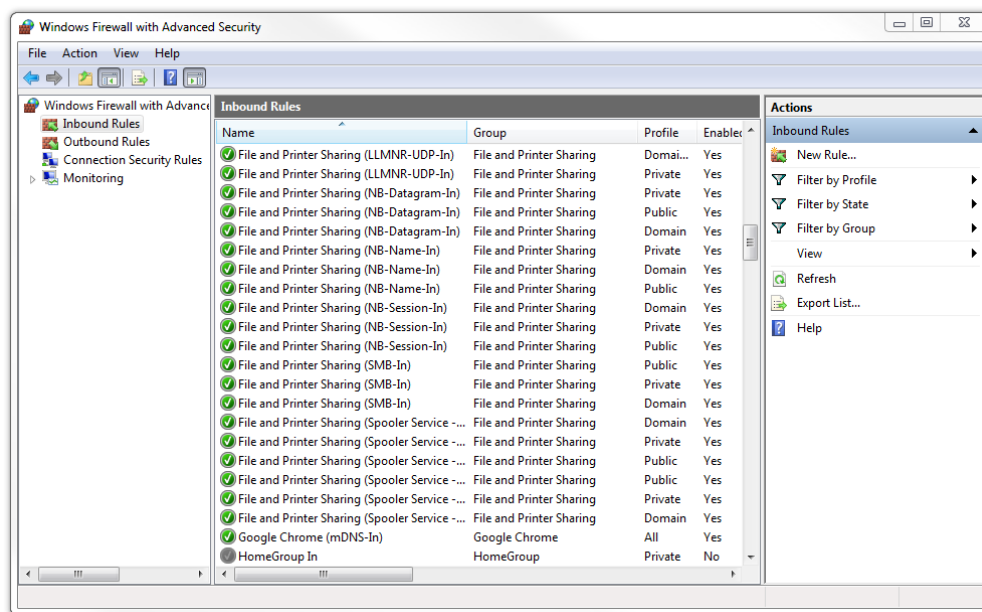


7. Right click on this selection, and select ‘Enable Rule’.
8. After enabling all the File and Printer sharing firewall rules, return to step 1 of this section to run a ping command again. If the command fails again, you will have to contact your network administrators or IT department for further assistance.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

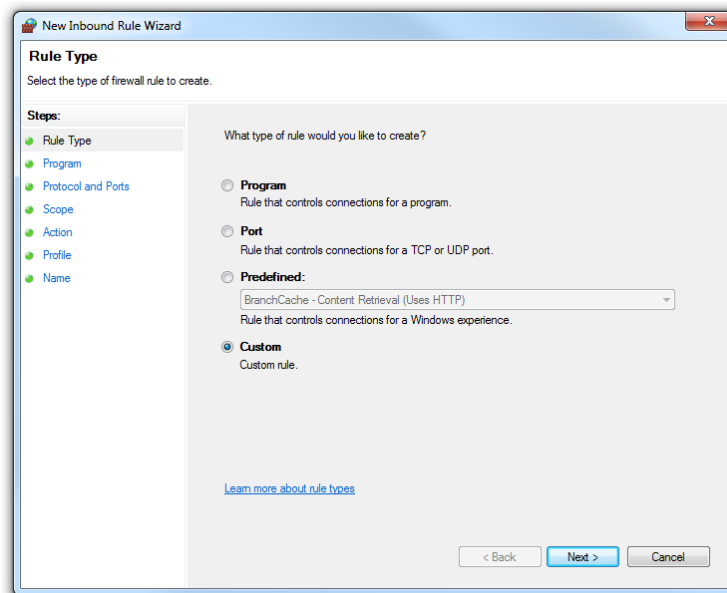
OTHER FIREWALL CONFIGURATIONS

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. These changes will take place on your FoxHub machine.

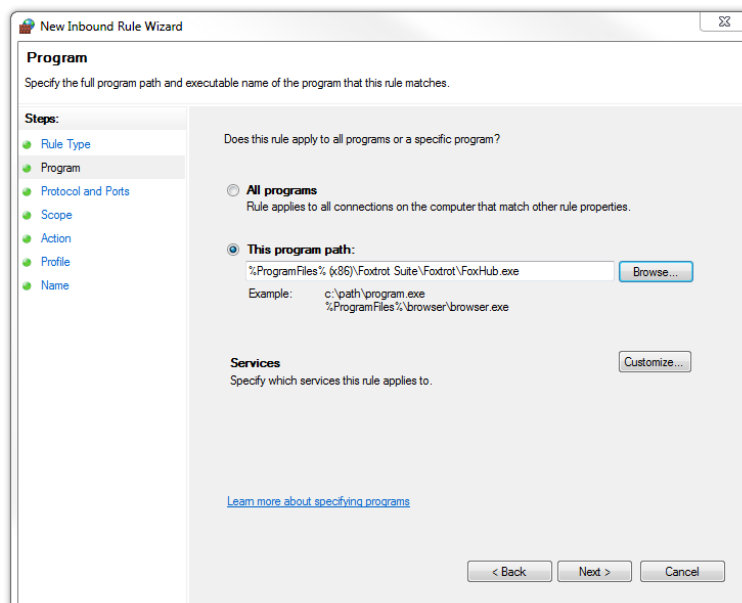
1. Begin by opening Windows Firewall with Advanced Security. Click on the ‘Inbound Rules’ section on the left hand side.



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



- 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)\Foxrot Suite\Foxrot\FoxHub.exe*. Click ‘Next’ to continue.



- The 'Protocol type' dropdown should be set to "TCP". 'Local port' should be set to "Specific ports" with "12650" in the field below it. 'Remote port' should remain on the "All Ports" option. Click 'Next' to continue.

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' sidebar lists: Rule Type, Program, Protocol and Ports (highlighted), Scope, Action, Profile, and Name. The main area asks 'To which ports and protocols does this rule apply?' and contains the following fields:

- Protocol type: TCP (dropdown)
- Protocol number: 6 (spin box)
- Local port: Specific Ports (dropdown) with a text input field containing '12650'. Below it is an example: 'Example: 80, 443, 5000-5010'.
- Remote port: All Ports (dropdown) with an empty text input field below it and the same example: 'Example: 80, 443, 5000-5010'.
- Internet Control Message Protocol (ICMP) settings: with a 'Customize...' button.

 At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

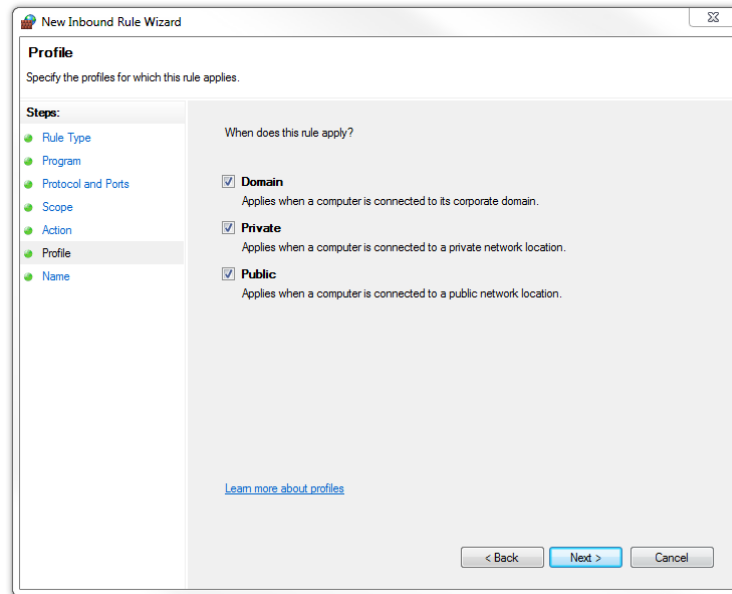
- On the 'Scope' page, nothing needs to change. For both questions, the radio button will stay on "Any IP address". Click 'Next' to proceed.
- Select the option to "Allow the connection" on this page. Click 'Next' to continue.

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, the 'Steps' sidebar lists: Rule Type, Program, Protocol and Ports, Scope, Action (highlighted), Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?' and contains the following options:

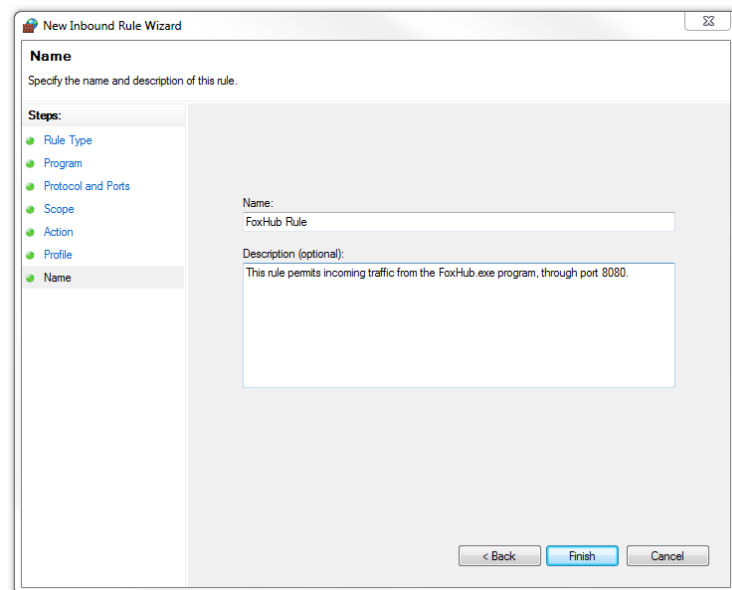
- Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Below this is a 'Customize...' button.
- Block the connection**

 At the bottom left is a link: [Learn more about actions](#). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

- 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.



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



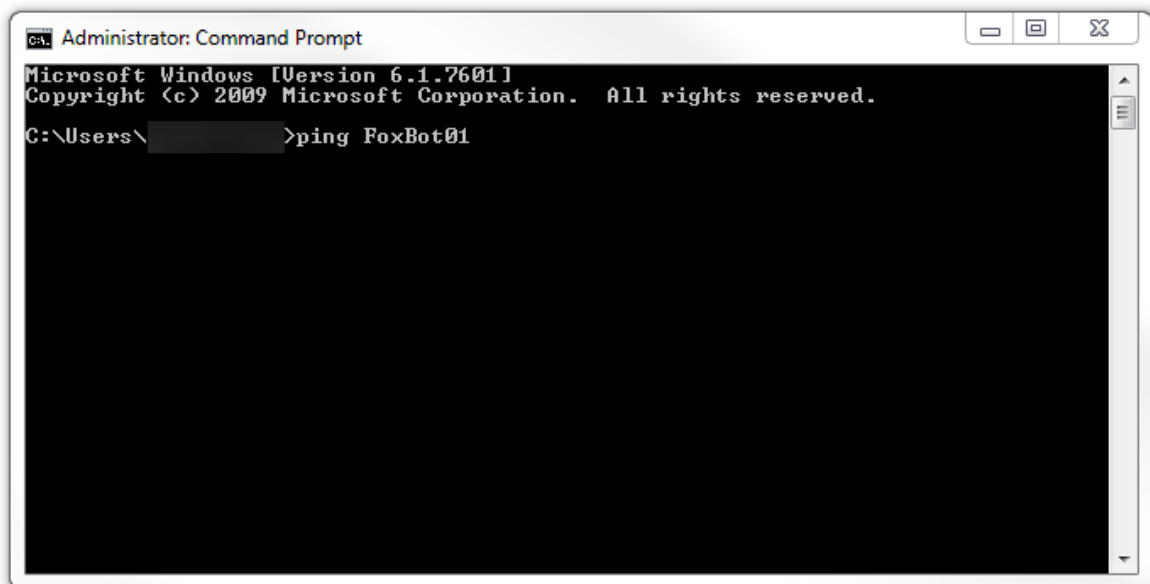
After these rules have been set up, check FoxHub to see if the issue has been resolved. If there are still communication issues (such as your Bots showing offline), then continue on with this guide.

Configuring Your FoxBot

FILE & PRINTER SHARING RULES

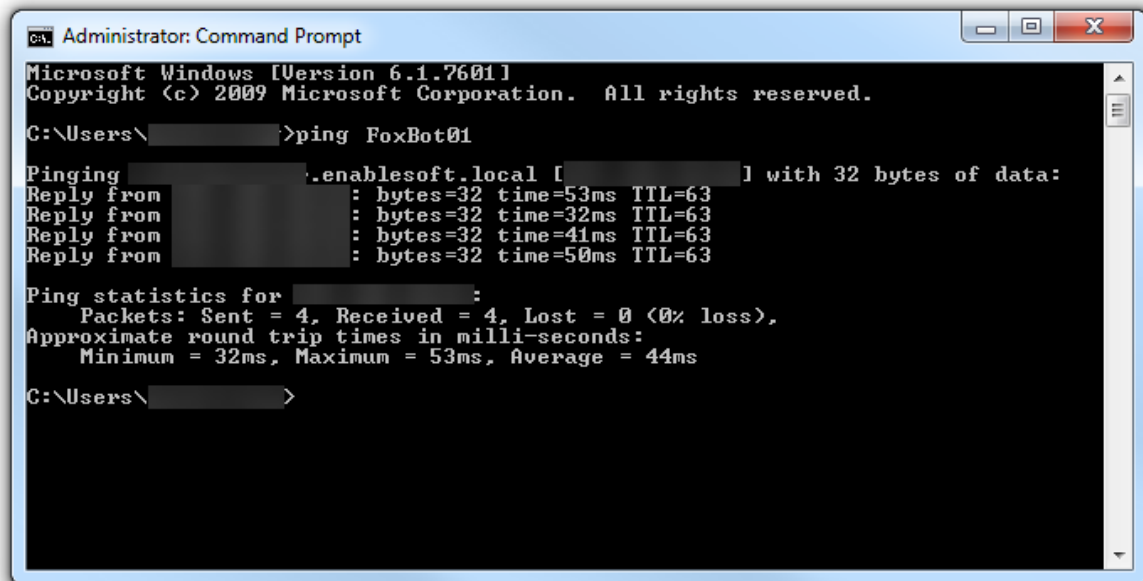
The first thing to check is basic communication from the FoxHub to the FoxBot machine. To do this, we will want to ping the FoxBot machines from the FoxHub computer.

1. Open Command Prompt on your FoxHub machine. 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 computer. In this example, it is “FoxBot01”.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\>ping FoxBot01
```

- 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.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

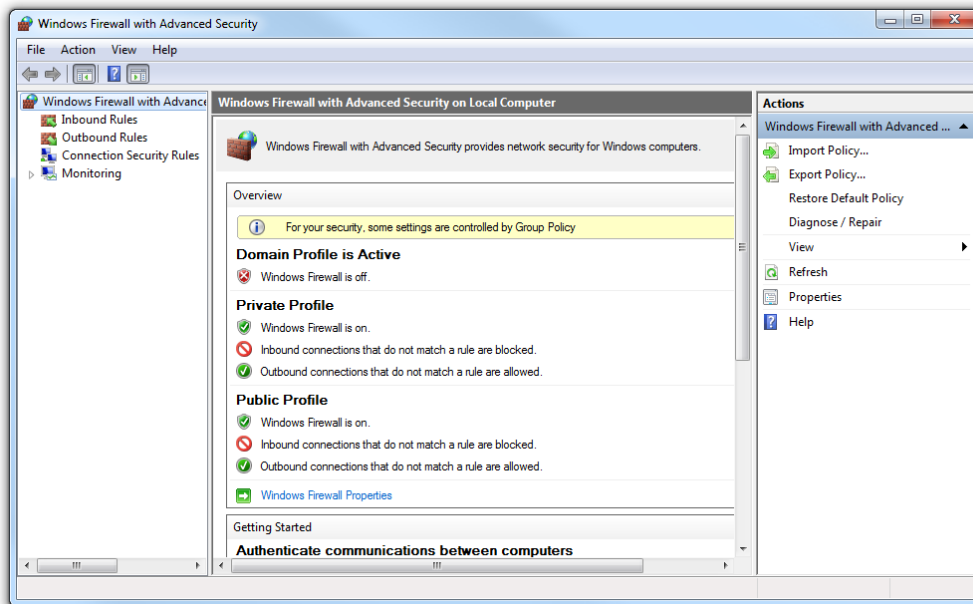
C:\Users\>ping FoxBot01

Pinging .enablesoft.local [ ] with 32 bytes of data:
Reply from : bytes=32 time=53ms TTL=63
Reply from : bytes=32 time=32ms TTL=63
Reply from : bytes=32 time=41ms TTL=63
Reply from : bytes=32 time=50ms TTL=63

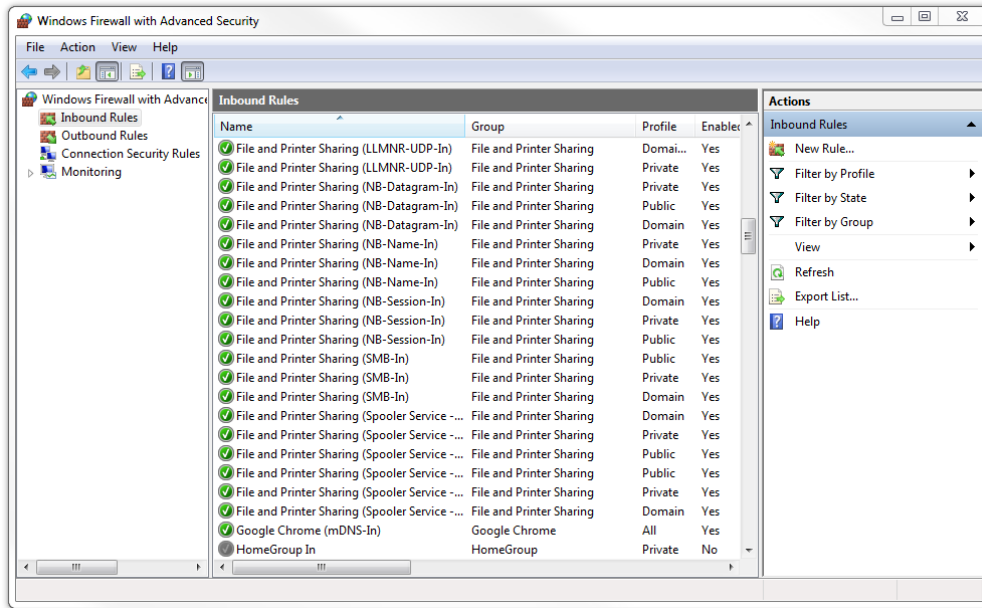
Ping statistics for :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 53ms, Average = 44ms

C:\Users\>
```

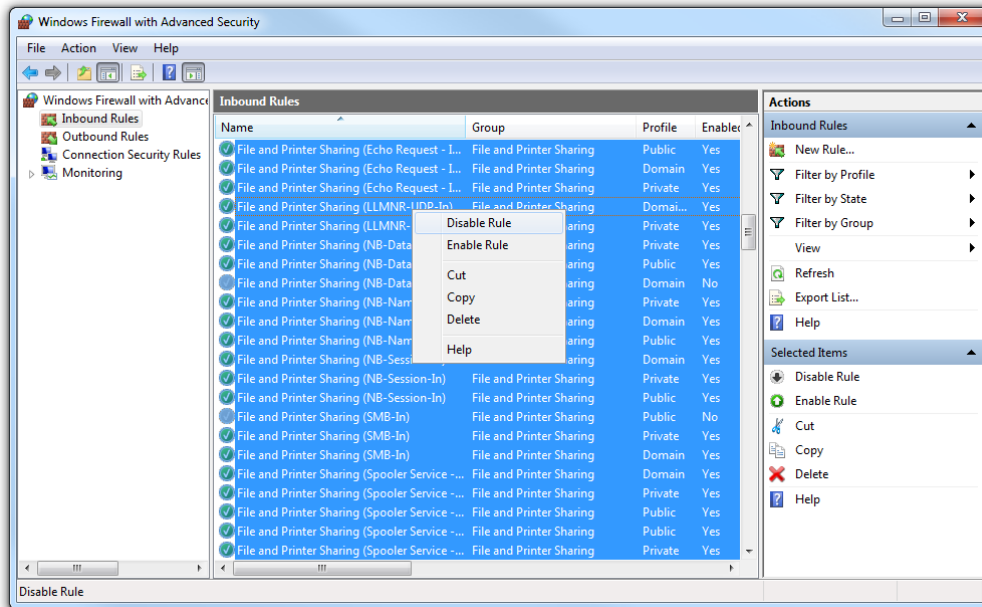
- If there is a negative result after the ping command is run, you will need to enable your 'File and Printer Sharing' firewall rules on each FoxBot machine. Begin by opening Windows Firewall with Advanced Security on your FoxBot.



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



- 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.

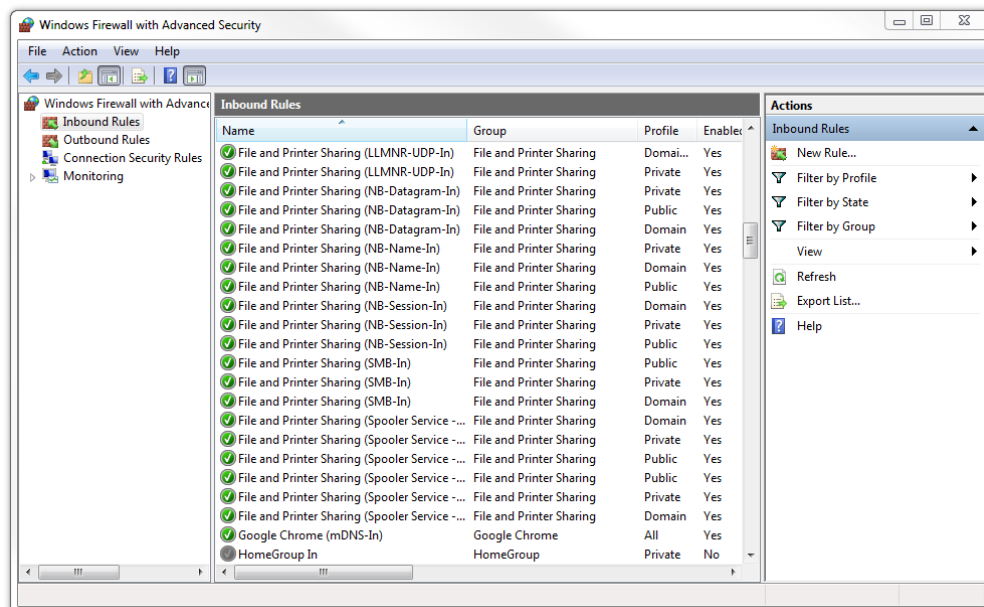


7. Right click on this selection, and select ‘Enable Rule’.
8. After enabling all the File and Printer sharing firewall rules, return to step 1 of this section to run a ping command again. If the command fails again, you will have to contact your network administrators or IT department for further assistance. If the command is successful, please continue on to the next section “Other Firewall Configurations”.

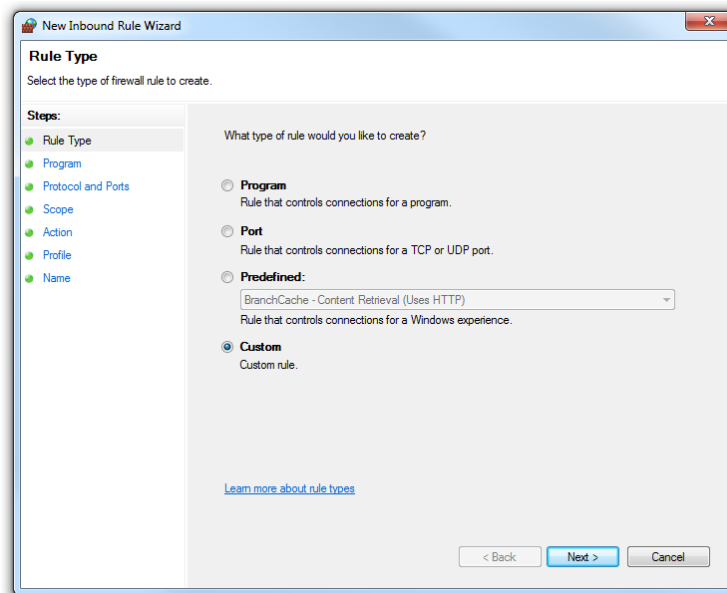
OTHER FIREWALL CONFIGURATIONS

Now that basic file sharing has been confirmed, additional firewall rules can be setup on the FoxBot machines. This involves opening specific ports to allow traffic through from our applications.

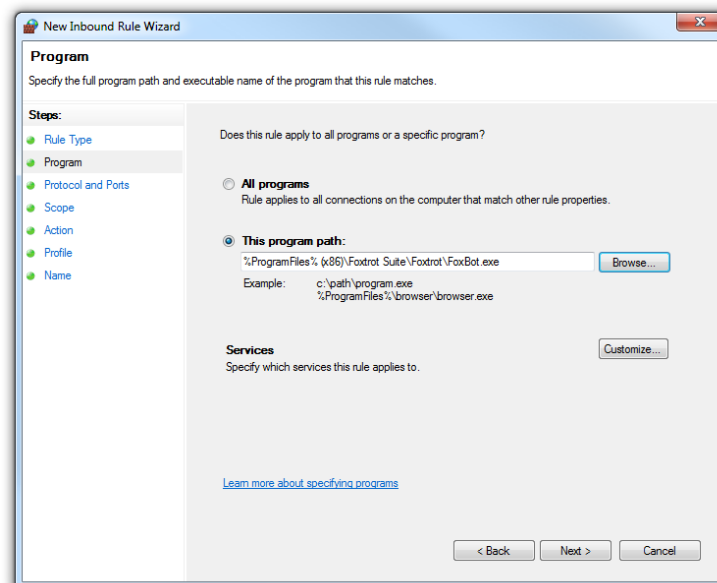
1. On your FoxBot machine, begin by opening Windows Firewall with Advanced Security. Click on the ‘Inbound Rules’ section on the left hand side.



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



- 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.



- The 'Protocol type' dropdown should be set to "TCP". 'Local port' should be set to "Specific ports" with "12652" in the field below it. 'Remote port' should remain on the "All Ports" option. Click 'Next' to continue.

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' sidebar lists: Rule Type, Program, Protocol and Ports (highlighted), Scope, Action, Profile, and Name. The main area asks 'To which ports and protocols does this rule apply?' and contains the following fields:

- Protocol type: TCP (dropdown)
- Protocol number: 6 (spin box)
- Local port: Specific Ports (dropdown) with a text field containing '12652' and an example '80, 443, 5000-5010' below it.
- Remote port: All Ports (dropdown) with an example '80, 443, 5000-5010' below it.
- Internet Control Message Protocol (ICMP) settings: with a 'Customize...' button.

 At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

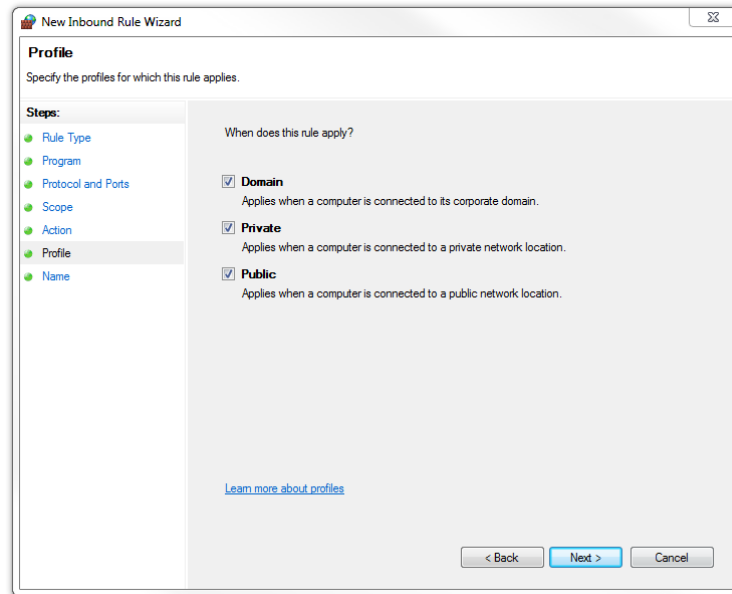
- On the 'Scope' page, nothing needs to change. For both questions, the radio button will stay on "Any IP address". Click 'Next' to proceed.
- Select the option to "Allow the connection" on this page. Click 'Next' to continue.

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps' sidebar lists: Rule Type, Program, Protocol and Ports, Scope, Action (highlighted), Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?' and contains the following options:

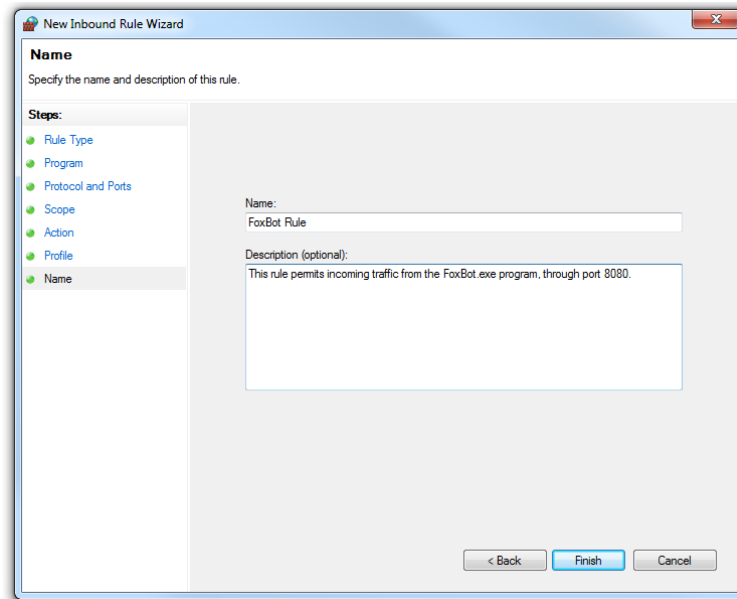
- Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. (Includes a 'Customize...' button)
- Block the connection**

 At the bottom are '< Back', 'Next >', and 'Cancel' buttons. A link 'Learn more about actions' is also present.

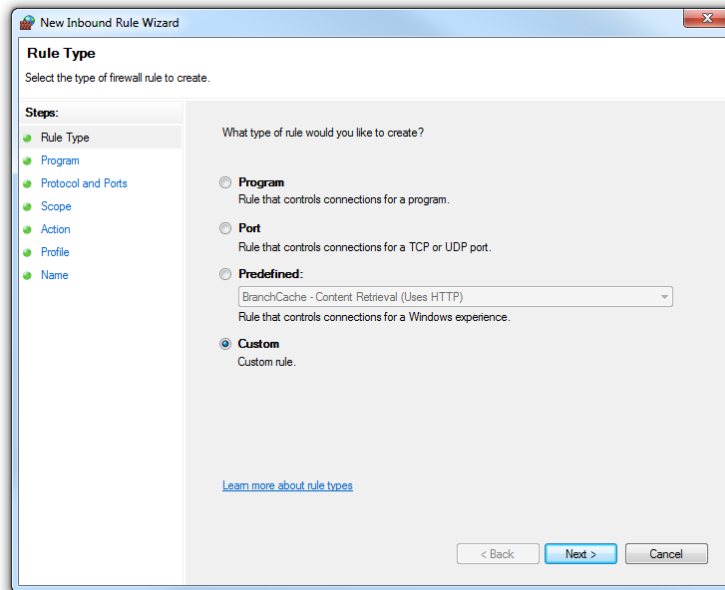
- On the Profile page, select which option will apply. If the FoxBot machine is on a domain, choose the 'Domain' checkbox but if it is on a public network, choose the 'Public' checkbox. If you're unsure, select all the boxes. Click 'Next' to move on.



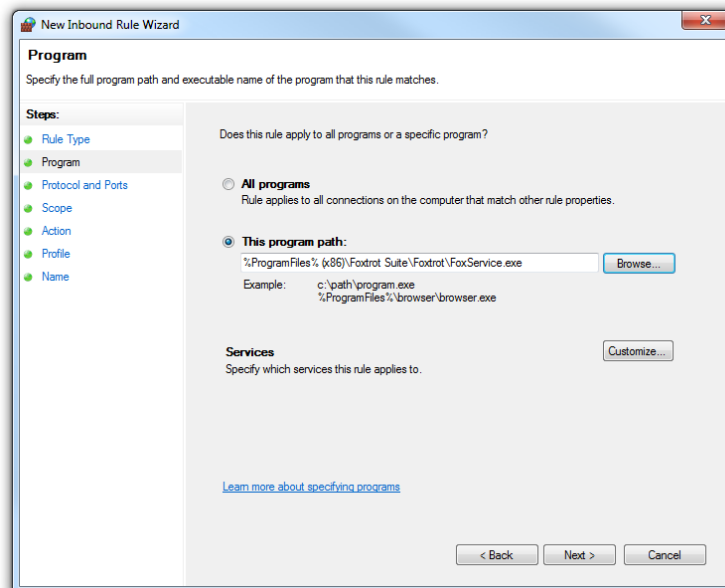
- Input a friendly name for this rule, and an optional description. A good name would be 'FoxBot Rule'. Click 'Finish' to create the rule. Continue the steps on the next page to create the next inbound rule.



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)\Foxrot Suite\Foxrot\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 “12651” in the field below it. ‘Remote port’ should remain on the “All Ports” option. Click ‘Next’ to continue.

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' list includes 'Rule Type', 'Program', 'Protocol and Ports' (highlighted), 'Scope', 'Action', 'Profile', and 'Name'. The main area asks 'To which ports and protocols does this rule apply?' and contains the following fields:

- 'Protocol type': A dropdown menu set to 'TCP'.
- 'Protocol number': A spinner box set to '6'.
- 'Local port': A dropdown menu set to 'Specific Ports' with a text input field containing '12651'. Below it is an example: 'Example: 80, 443, 5000-5010'.
- 'Remote port': A dropdown menu set to 'All Ports' with an empty text input field below it. Below that is another example: 'Example: 80, 443, 5000-5010'.
- 'Internet Control Message Protocol (ICMP) settings:': A 'Customize...' button.

 At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

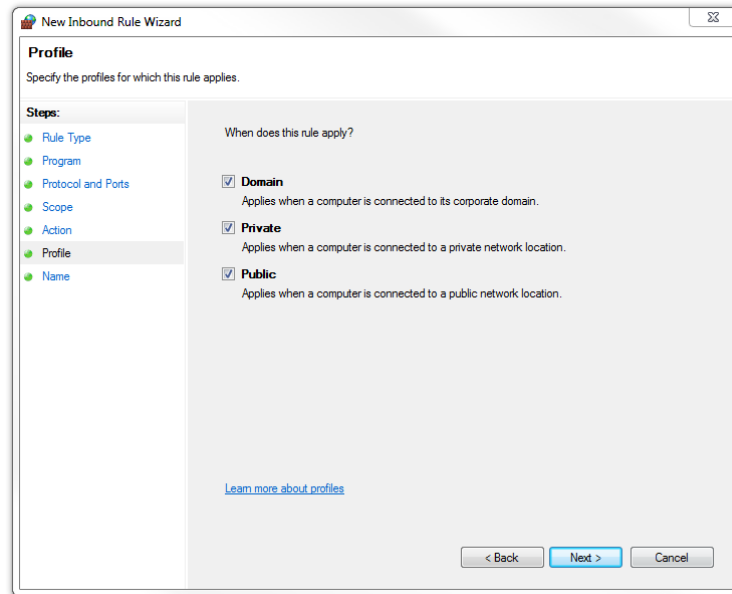
12. On the ‘Scope’ page, nothing needs to change. For both questions, the radio button will stay on “Any IP address”. Click ‘Next’ to proceed.
13. Select the option to “Allow the connection” on this page. Click ‘Next’ to continue.

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps' list includes 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action' (highlighted), 'Profile', and 'Name'. The main area asks 'What action should be taken when a connection matches the specified conditions?' and contains three radio button options:

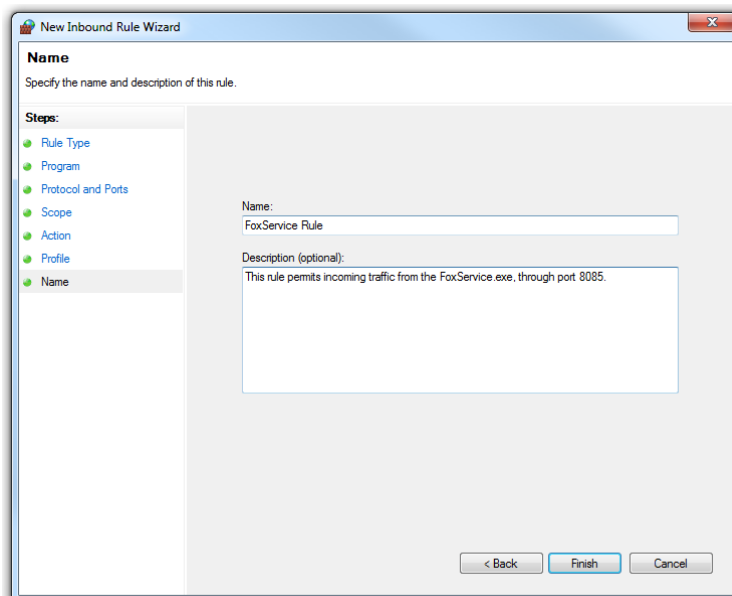
- Allow the connection**: This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**: This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Below this option is a 'Customize...' button.
- Block the connection**

 At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A link 'Learn more about actions' is located at the bottom left of the main area.

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.



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 and policies.

THANK YOU FOR YOUR TIME.

Contact Us

Customer Success Team

success@enablesoft.com

800-658-1147

www.enablesoft.com

