Windows Defender Firewall Project

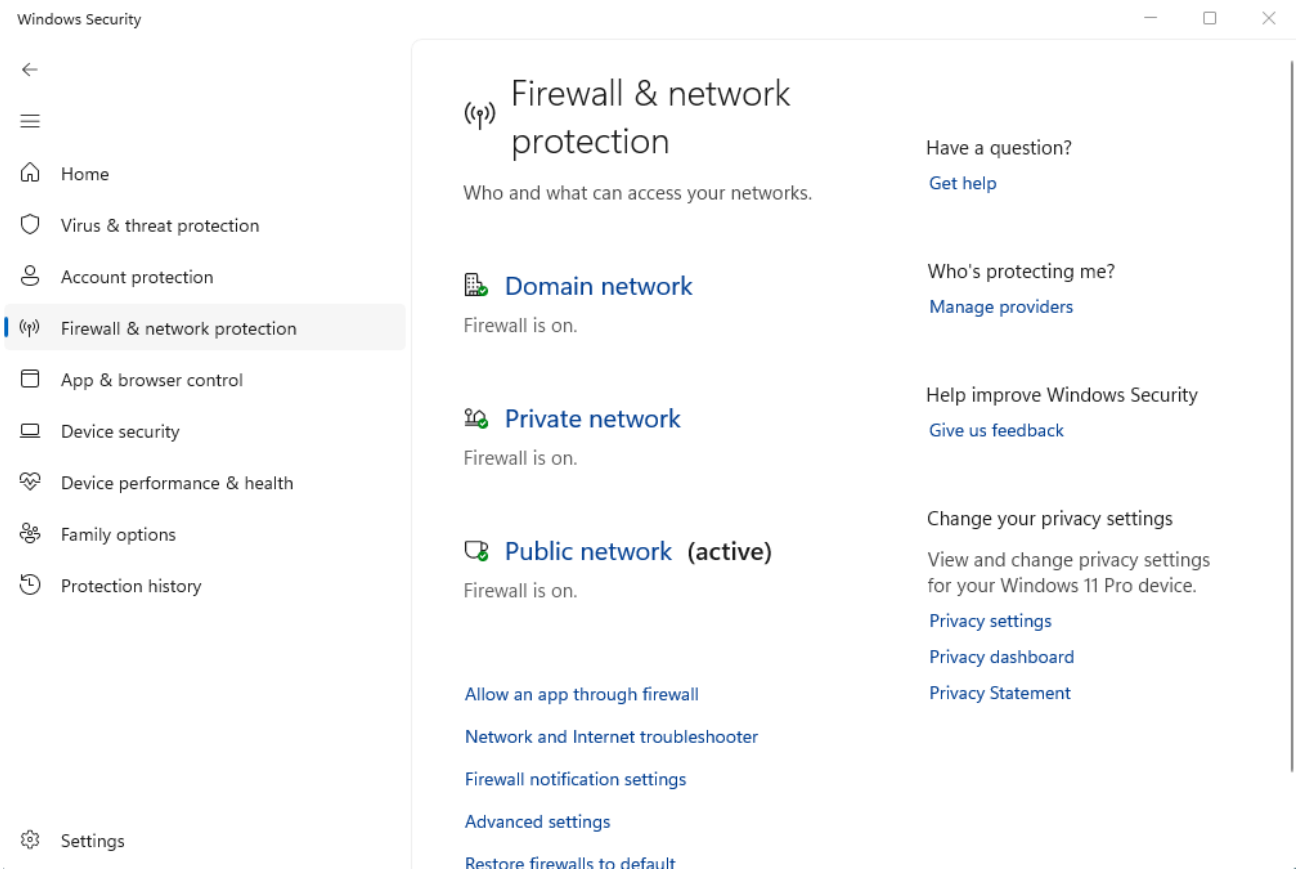
Scenario:

I configured a custom firewall rule that blocked access to my GitHub webpage from any device connected to my network using Windows Defender.

Firewall Configuration:

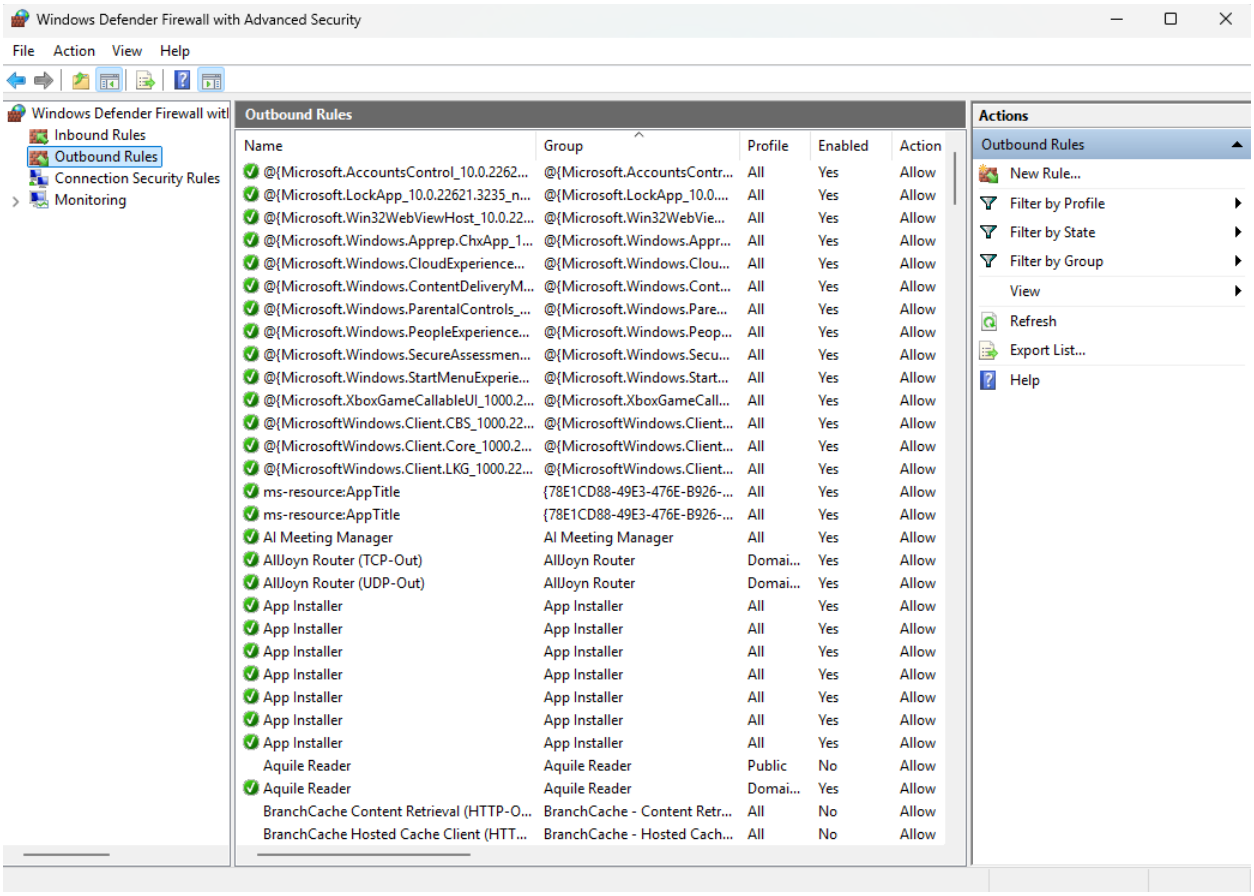
I opened Windows Security, selected 'Firewall & network protection', and then selected 'Advanced settings'.

Figure 1: Opening Windows Security and Navigating to Advanced Settings



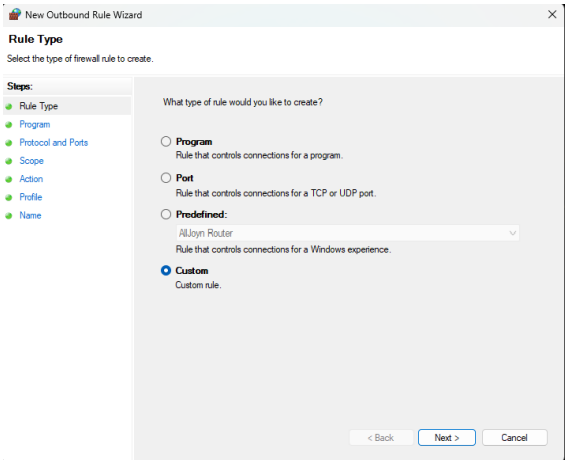
I selected ‘Outbound Rules’ and then selected ‘New Rule’.

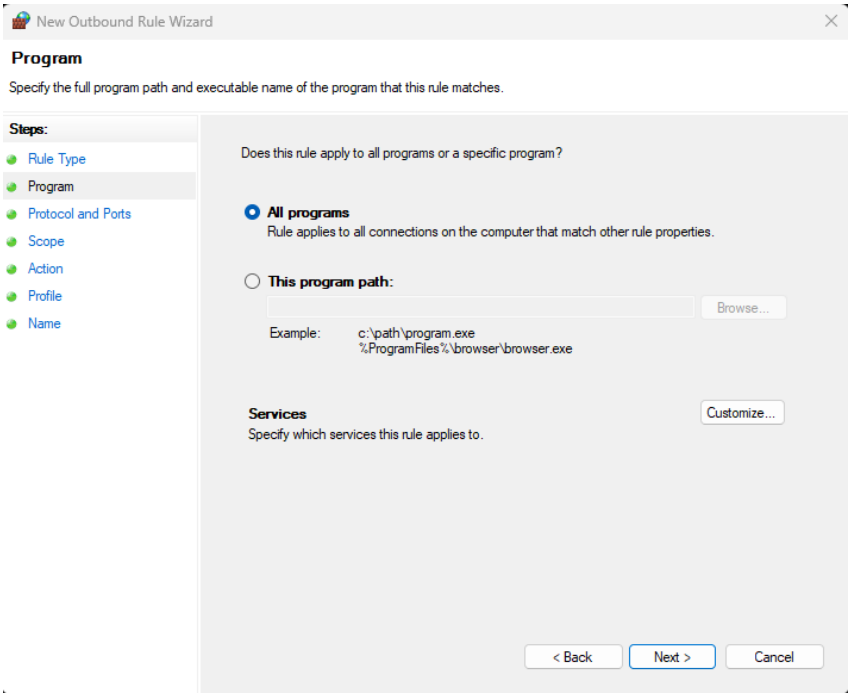
Figure 2: Selecting Outbound Rules and Creating a New Rule

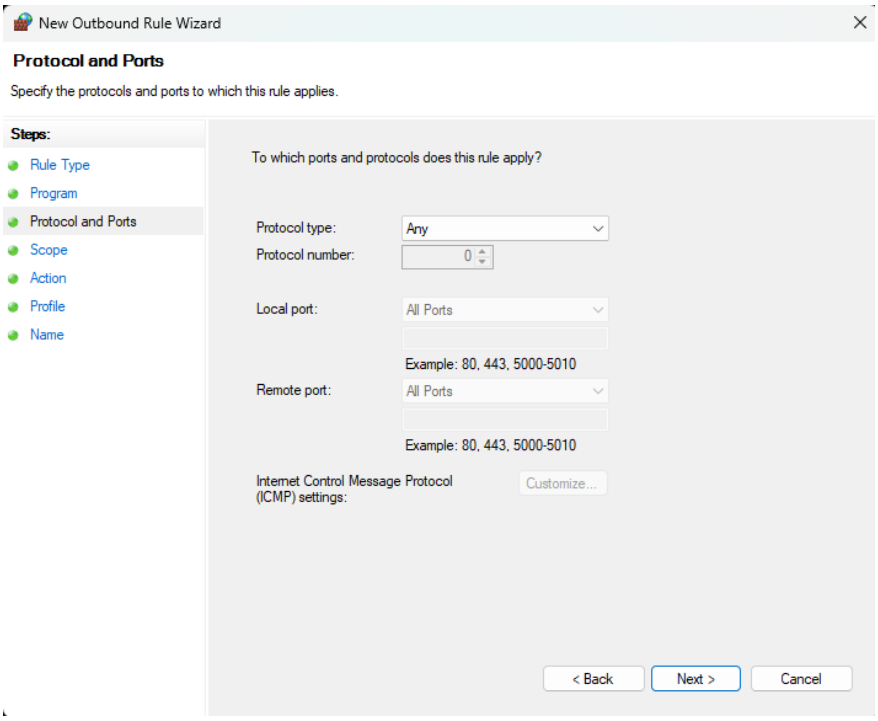


I selected the ‘Custom’ rule type, applying to ‘All programs’, ‘Any Protocol type’, and ‘All Ports’ (local and remote).

Figures 2-4: Rule Type, Program, Protocols and Ports Parameters

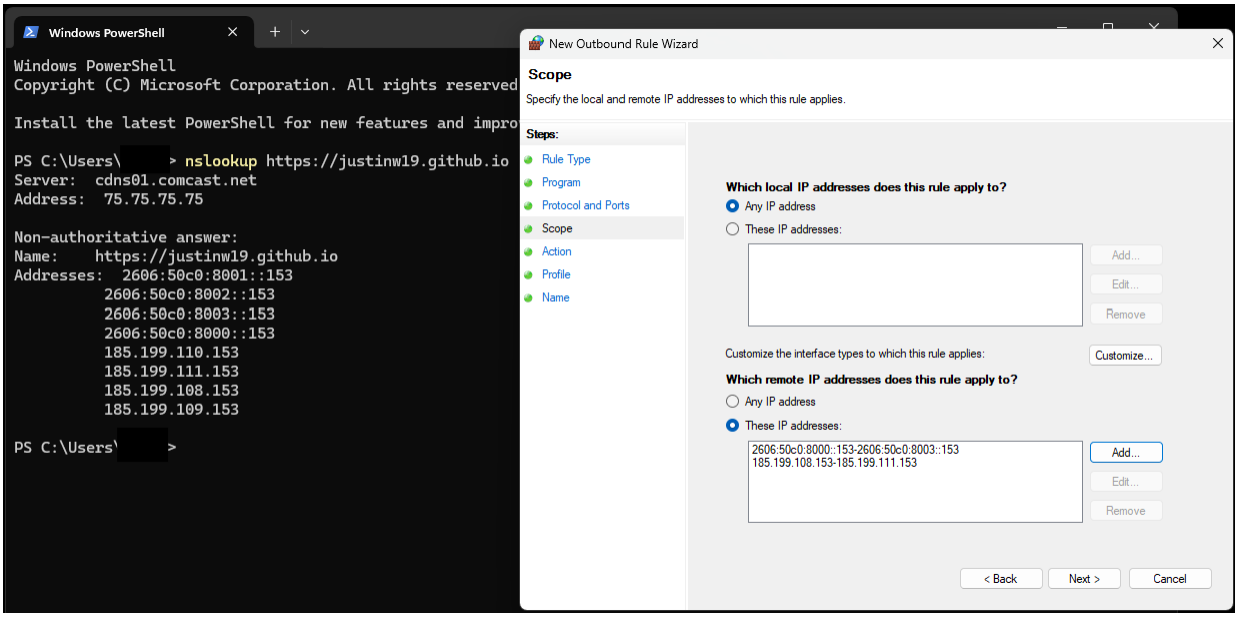



New Outbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
Cancel


New Outbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type:
Any
Protocol number:
0
Local port:
All Ports
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
Next >
Cancel

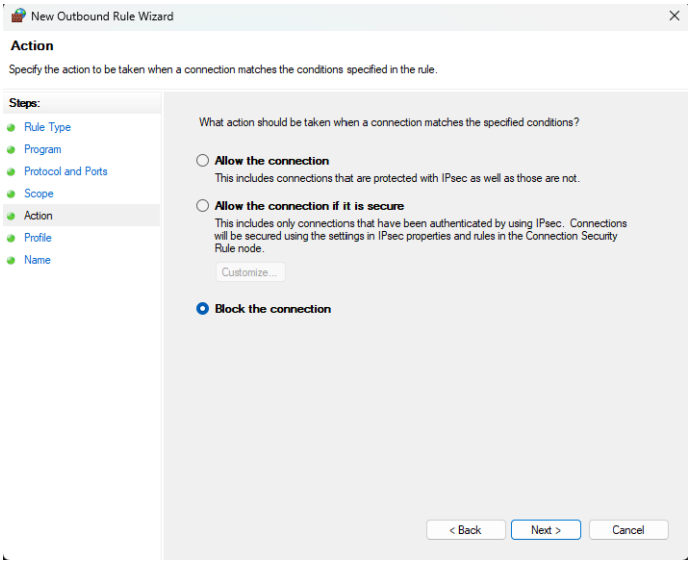
I performed a nslookup command on the domain name (justinw19.github.io) I wanted to block and input those ranges into the ‘Scope’ section of the firewall rule.

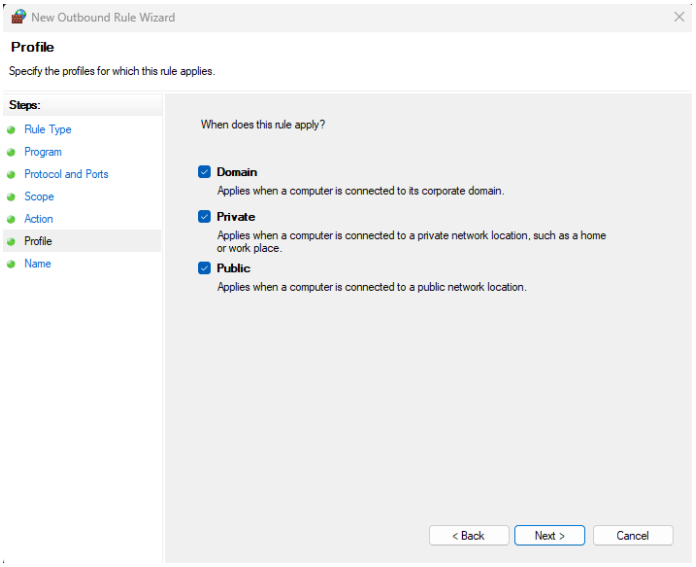
Figure 5: Finding IP Addresses and Writing Them into the Firewall Rule



I set the firewall rule to ‘Block the connection’ across all network types, and all ‘Network Profiles’ (Domain, Private, Public).

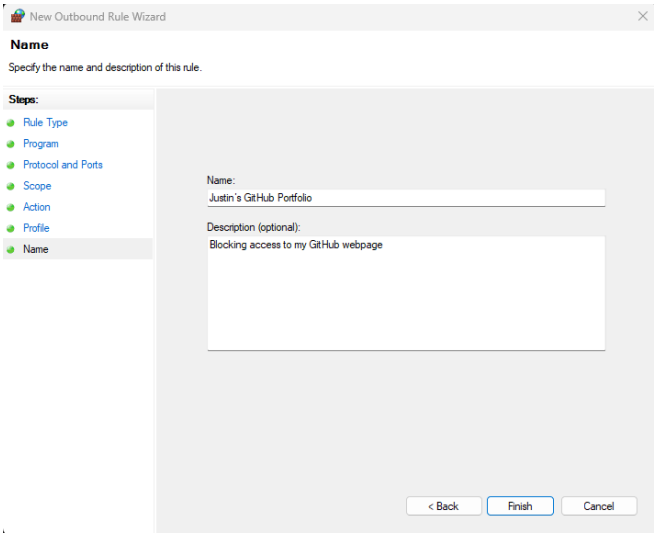
Figure 6-7: Setting Rule to Block Across All Network Profiles





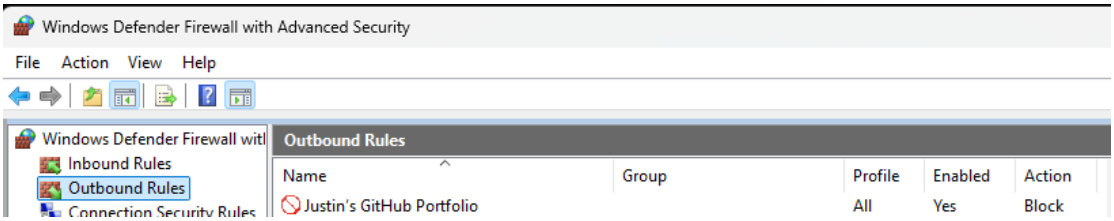
I named my firewall rule 'Justin's GitHub Portfolio'. I wrote a description of what the rule was accomplishing (blocking access to my GitHub webpage from any device connected to my network) and clicked 'Finish'.

Figure 8: Naming and Completing Firewall Rule



I then checked the listing of 'Outbound Rules' and verified that the new rule was enabled

Figure 9: Rule Listed in Outbound Firewall Rules



Lastly, I attempted to access my GitHub webpage and could not due to the firewall rule.

Figure 10: justinw19.github.io Webpage is Successfully Blocked