Date:07/11/2020

**Practical no 9**

**AIM:** Configure windows firewall to block

1) A port 2) An Program 3) A Website

**Different Types of Profiles available/ When does this rule applies**

**Domain:** Applies when computer is connected to corporate domain

**Private:** Applies when computer is connected to a private network location, such as a

home or workplace.

**Public:** Applies when computer is connected to public network connection.

**Different types of actions available/What action should be taken when a connection**

**matches the specified the conditions**

**Allow the connection:** This includes connections that are protected with IPsec as well as

those are not

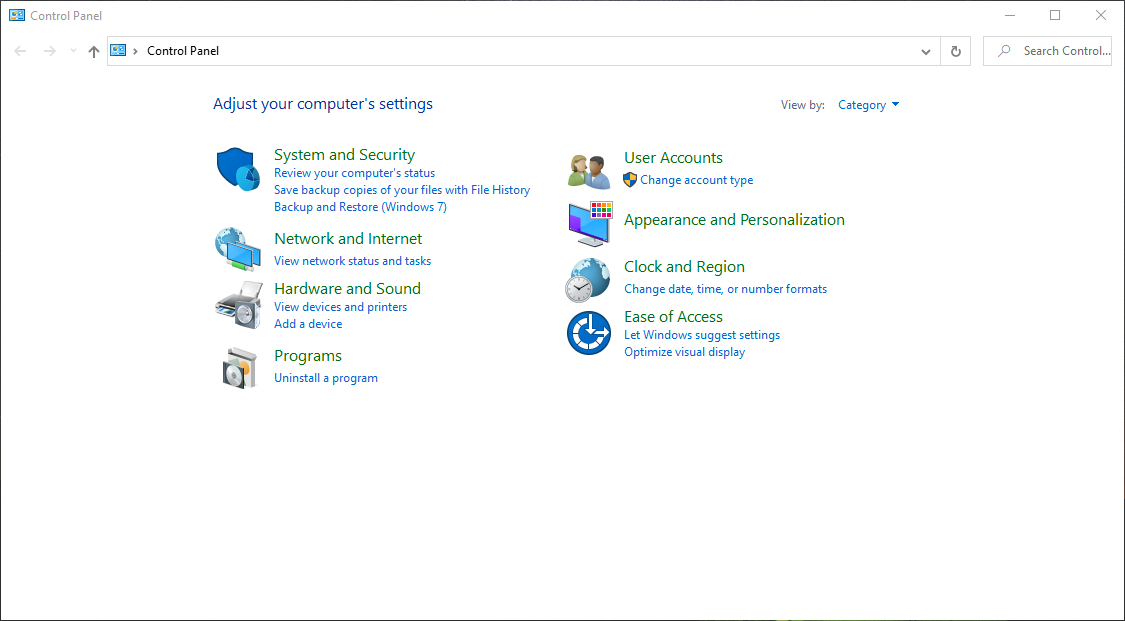
**Allow the connection if it is secure:** This includes only connections that have been

authenticated by using IPsec. Connections will be secured using the settings in IPsec

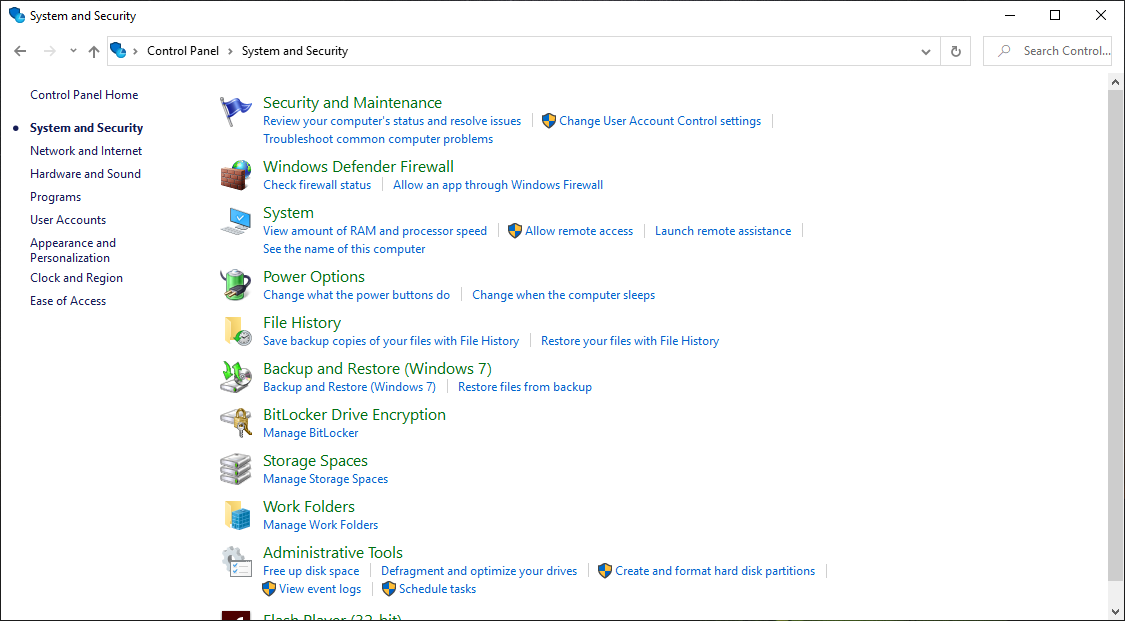
properties and rules in the Connection Security Rule node. Block the connection.

**A) Blocking a port:**

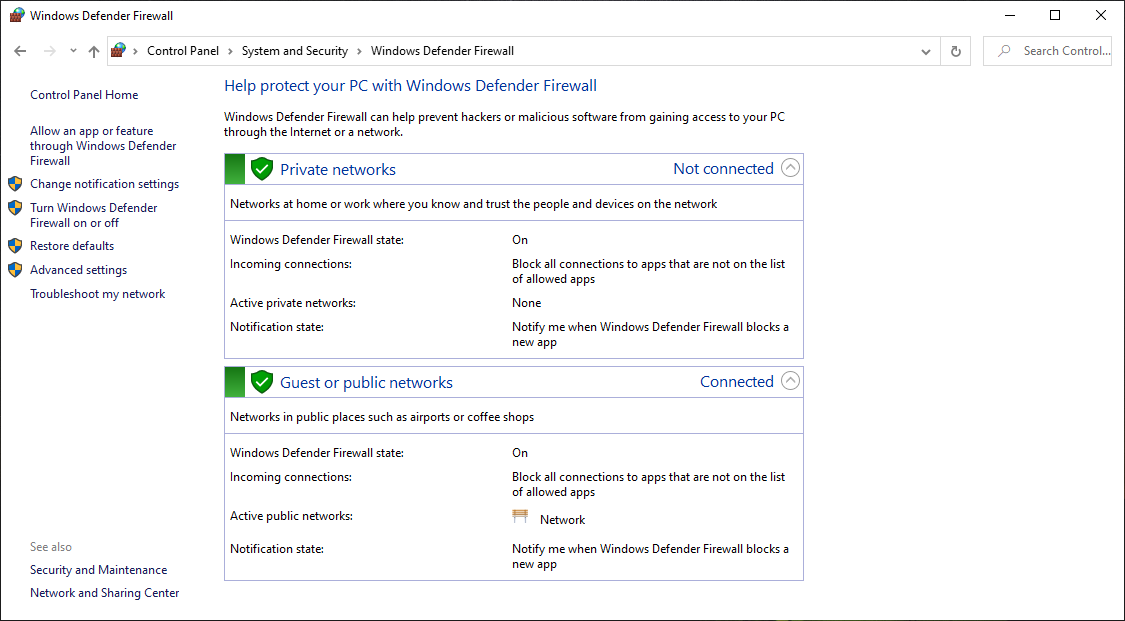
**Step 1:** Open control panel and go to System Security



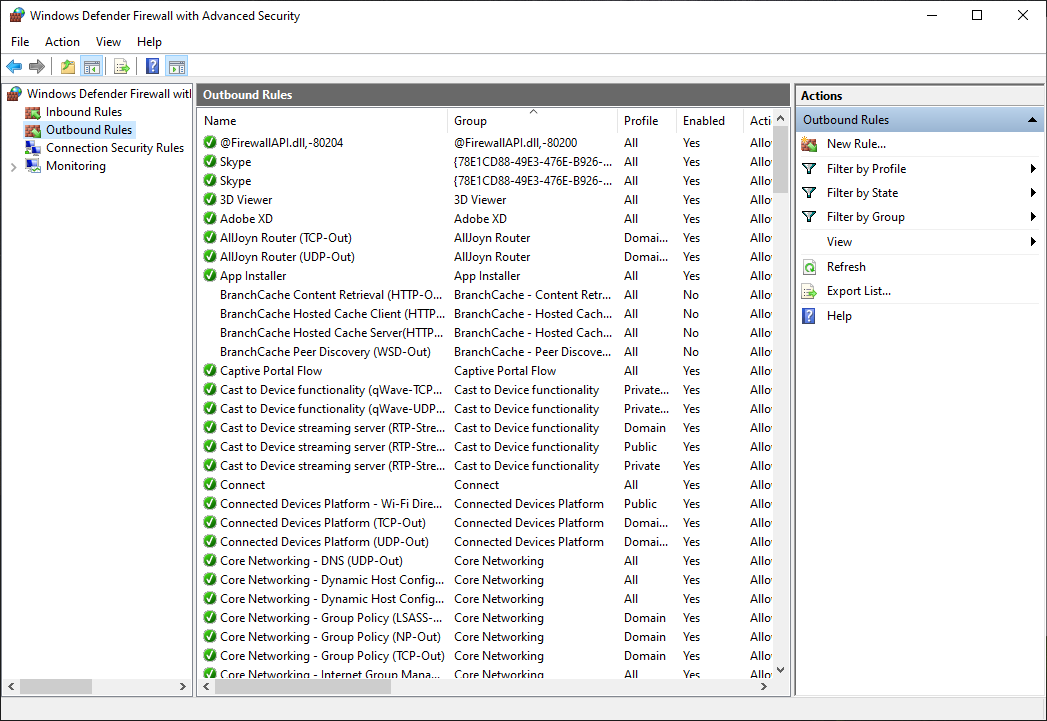
**Step 2:** Now Select Windows Defender Firewall.



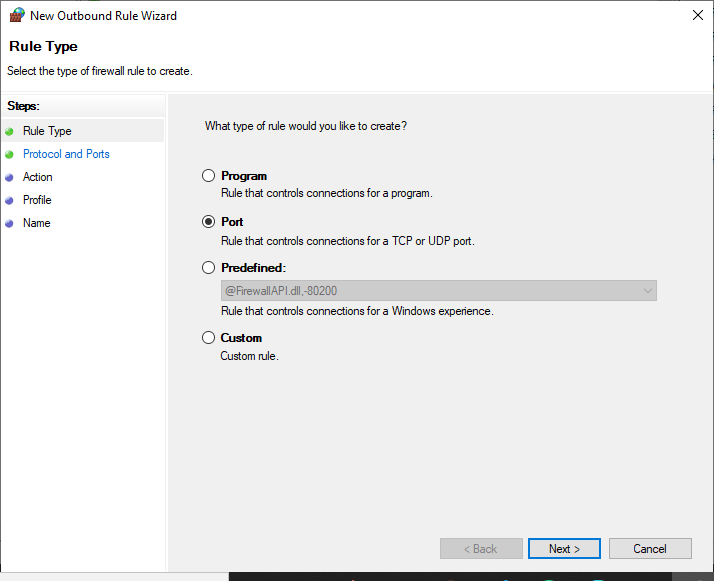
**Step 3**: Now you need to select Advanced setting.



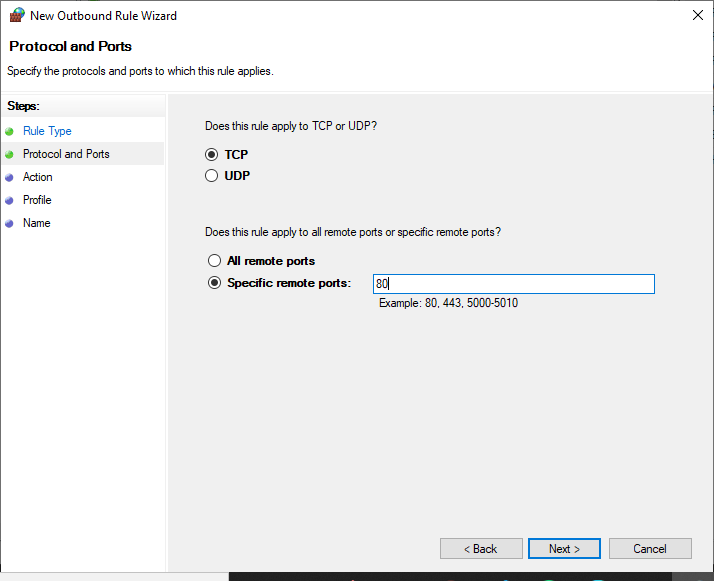
**Step 4:** Now Select Outbound Rules.



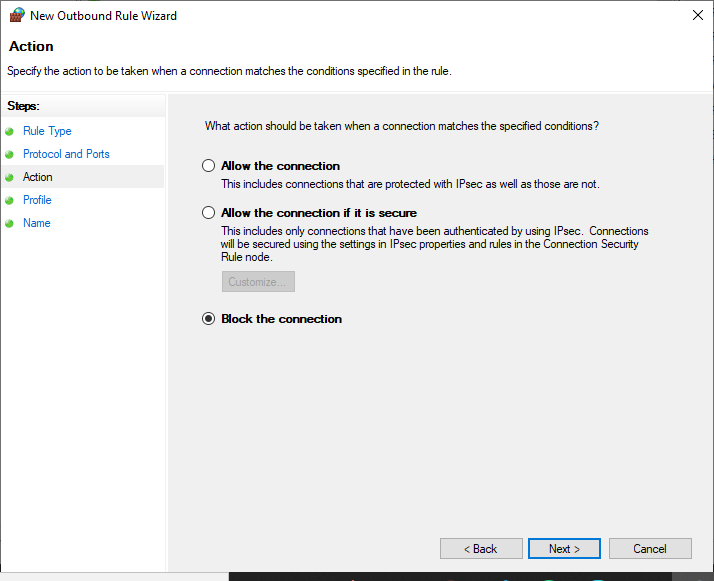
**Step 5:** Inside Outbound rules -> Select New Rules -> select Port and then click on next.



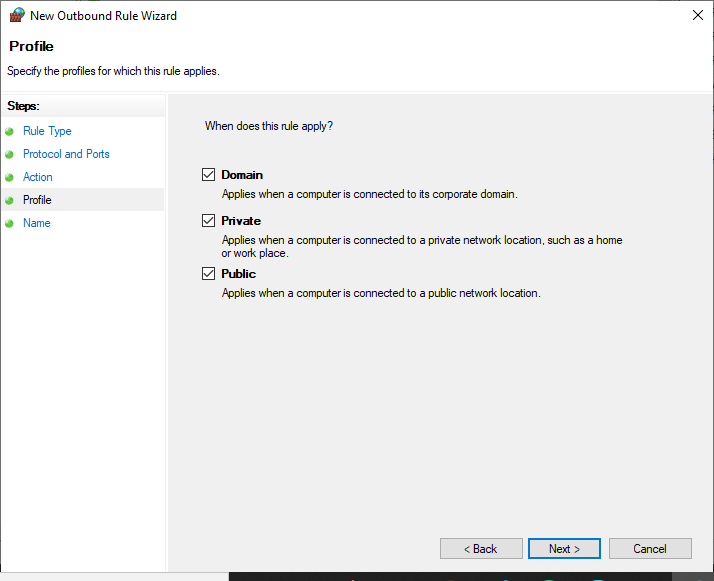
**Step 6**: Select the protocols and enter the port that you want to want to block



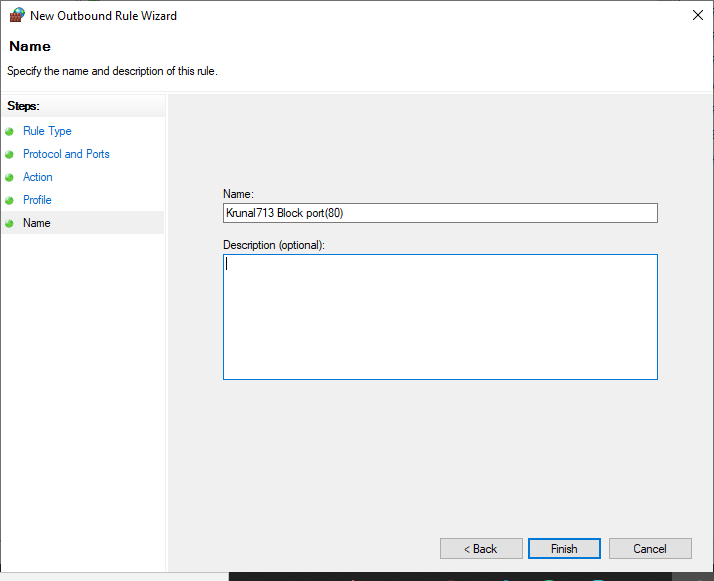
**Step 7:** Select the action block the connection for blocking a port



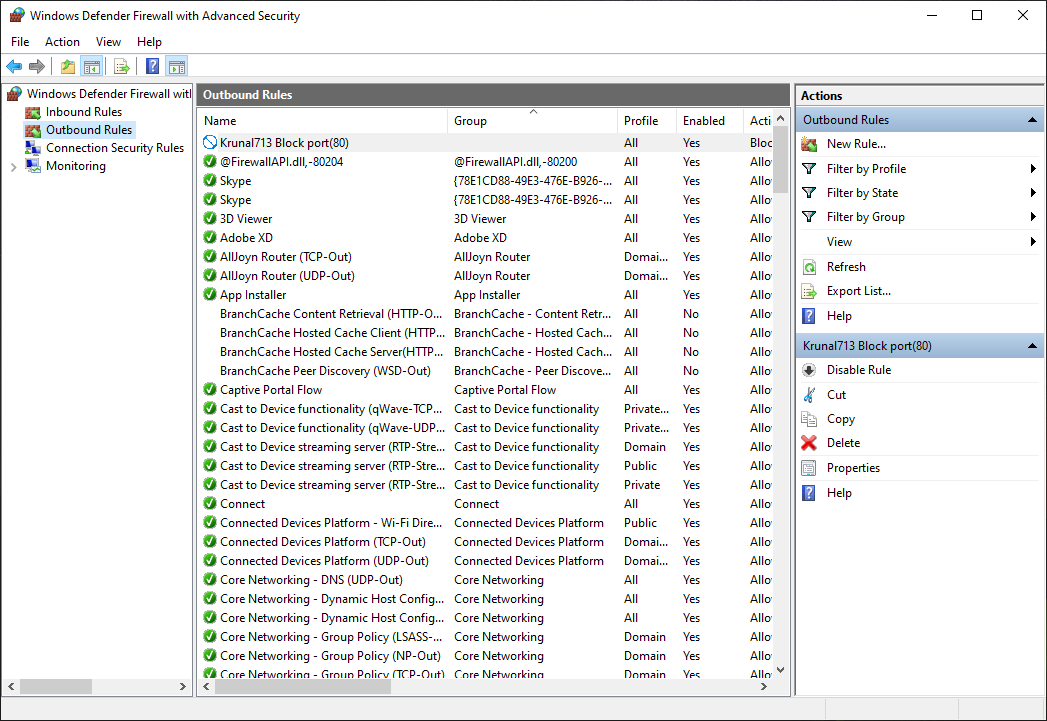
**Step 8:** Select the profiles domain private or public.



**Step 9:** Give a name to our new set rule and click on finish.



**Output:**

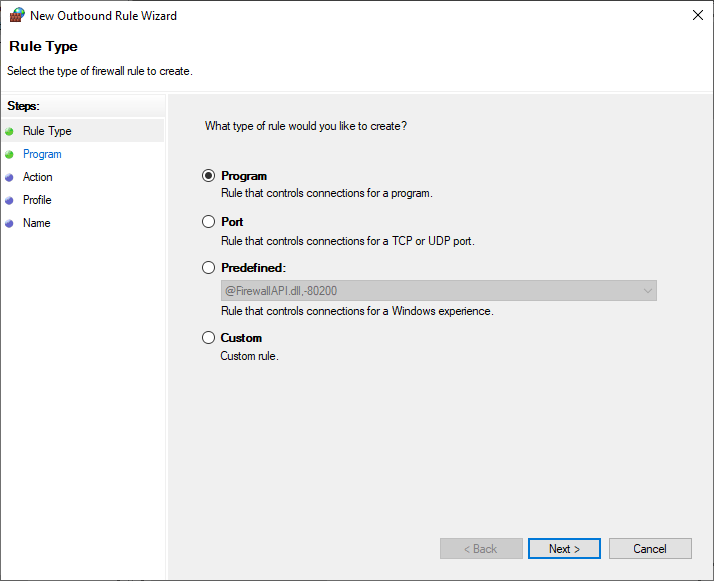
****

**B) Blocking a program:**

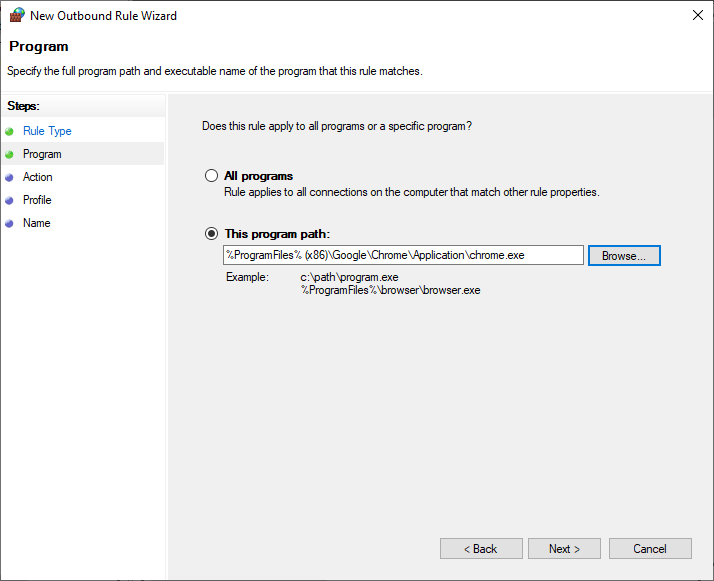
**Rule that controls the connection of a program**

**Step1: Repeat PartA Step1 to Step4.**

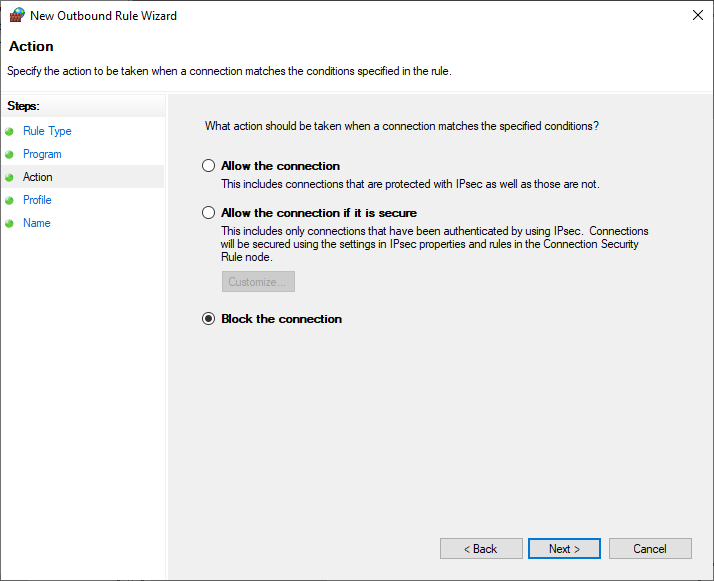
**Step 5:** Inside Outbound rules -> Select New Rules -> select a program and then click on next.



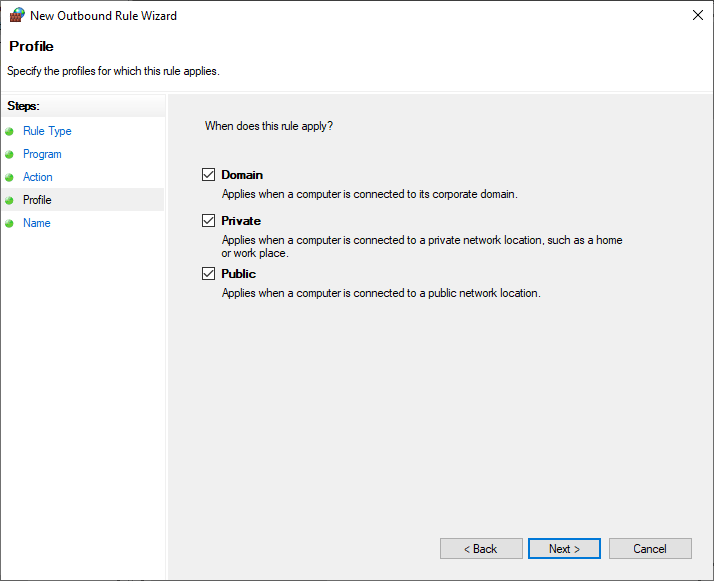
**Step 6:** Choose the path of the program from the directory.



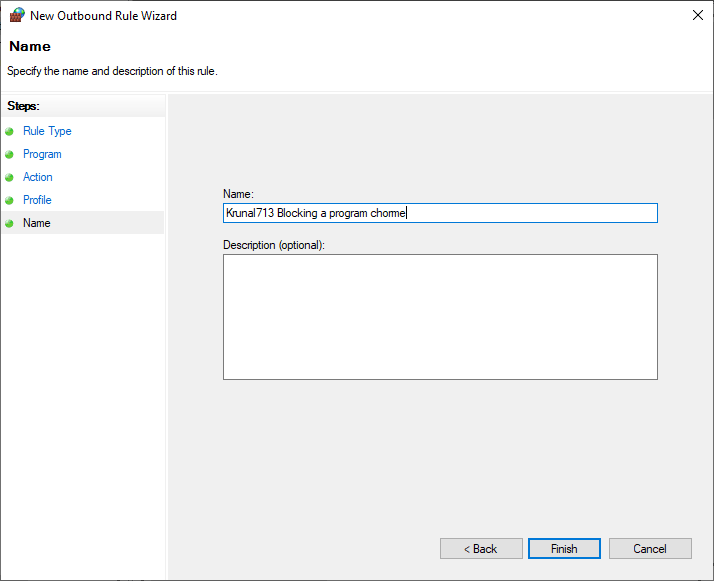
**Step 7:** Click on Block the connection.



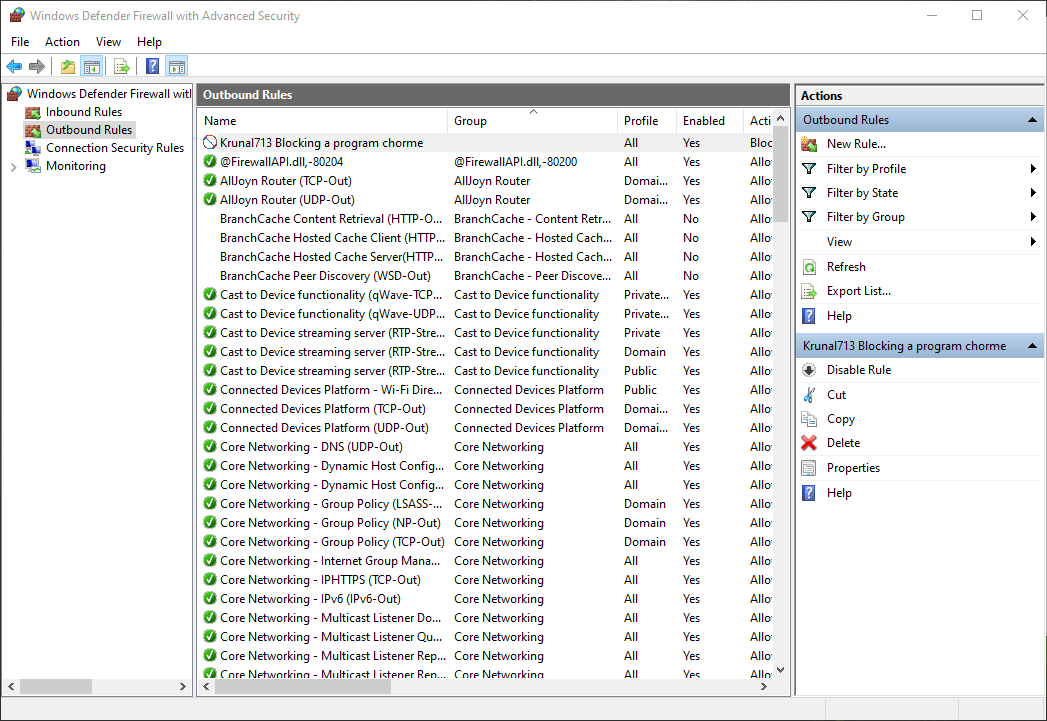
**Step 8**: Select the profiles domain private or public.



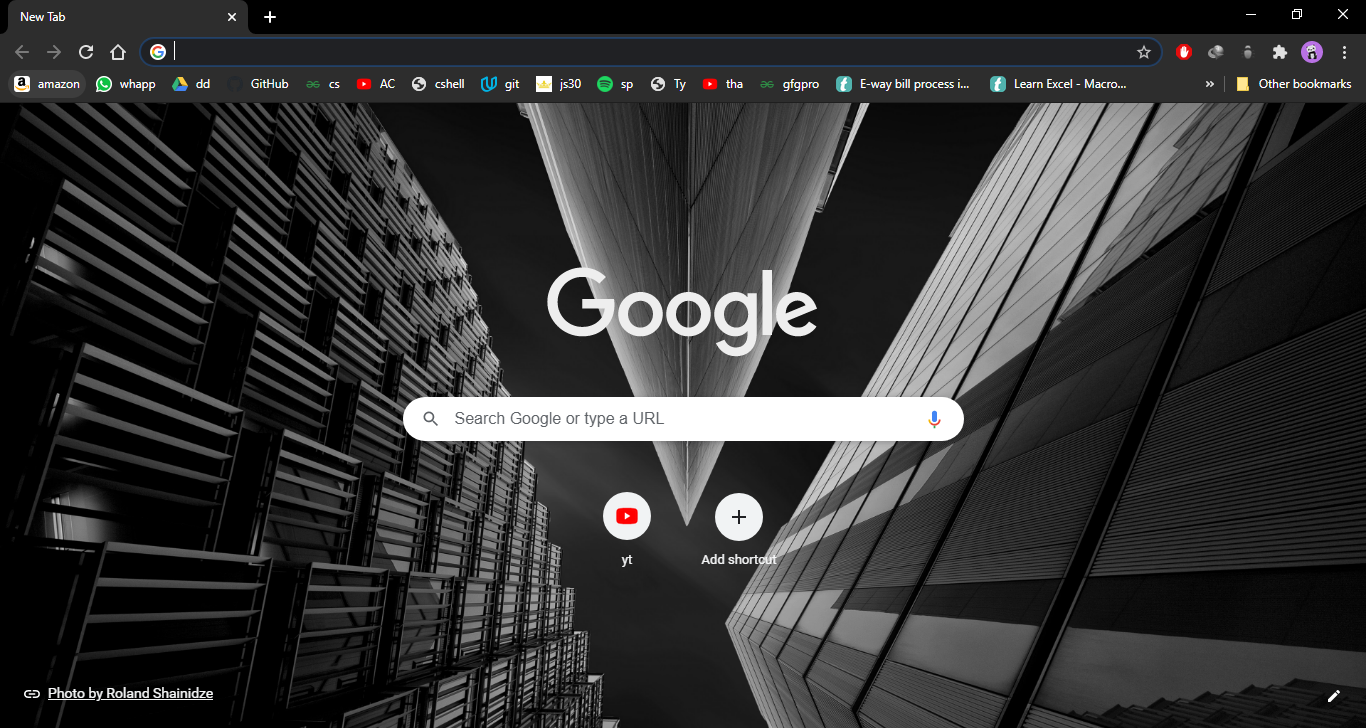
**Step 9:** Give a name to your new set rule and click on finish.



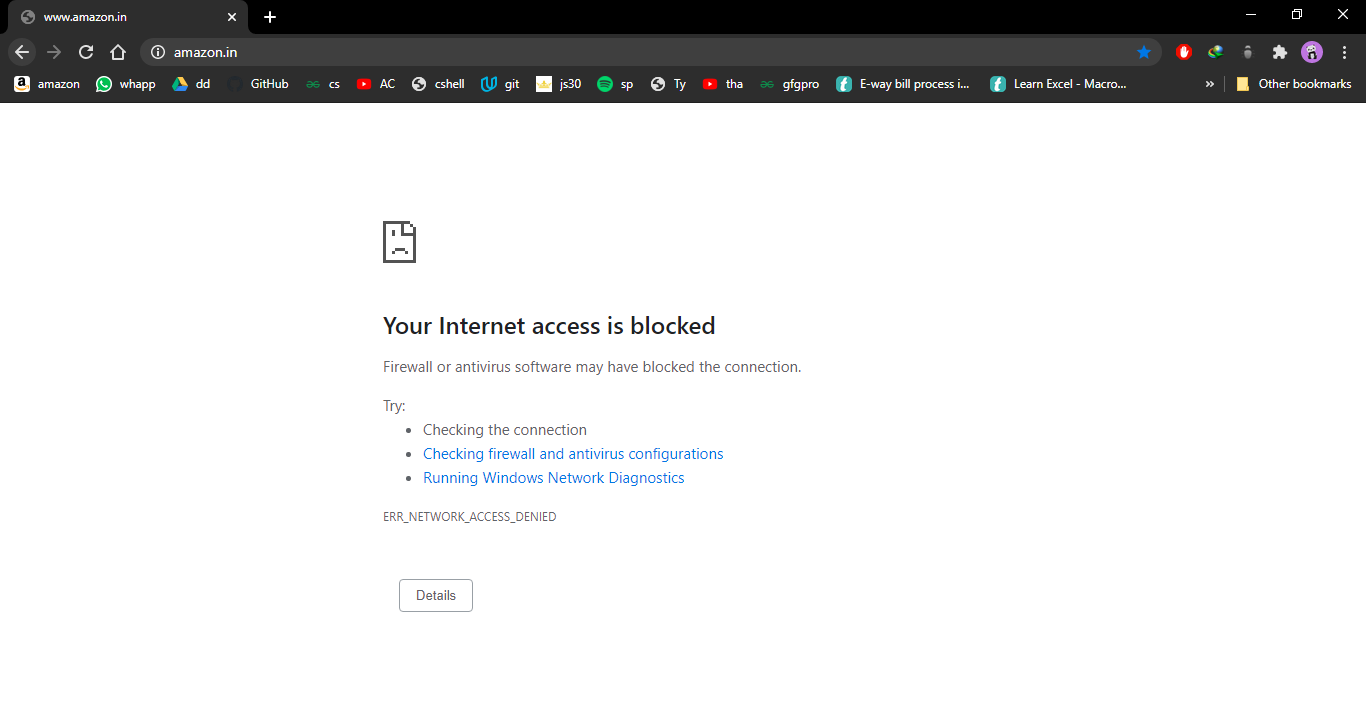
**Output:**



**Before Applying the Rule:**



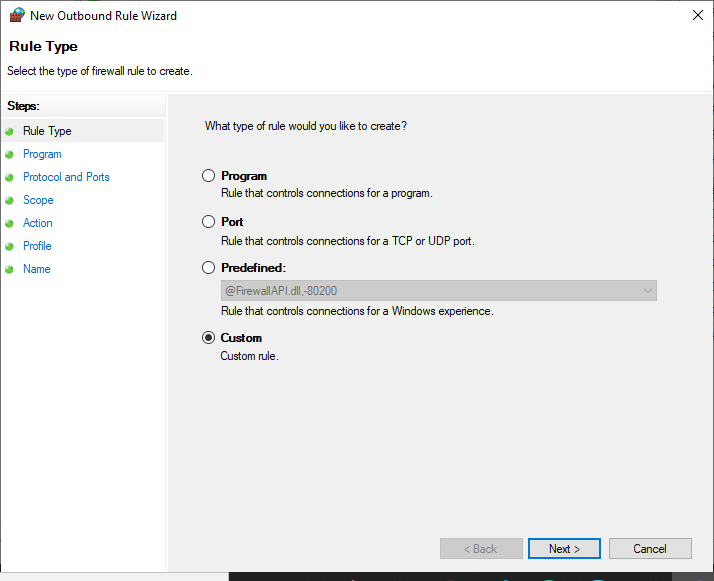
**After Applying the Rule:**

****

**C) Blocking a website:**

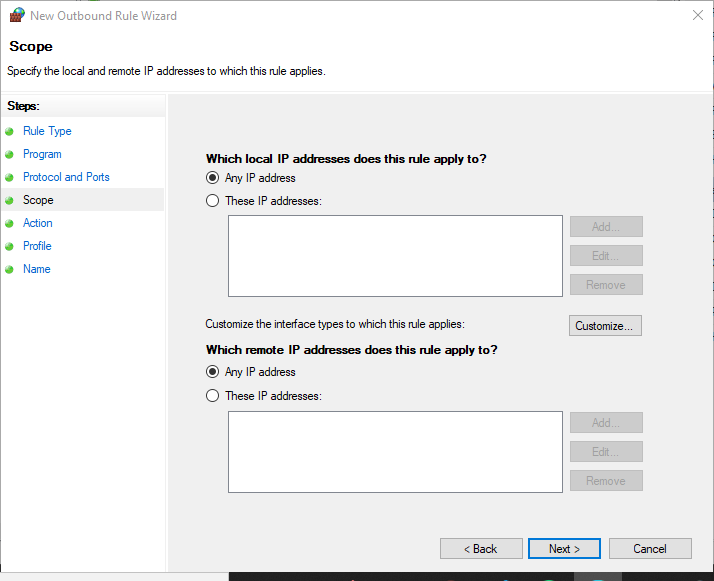
**Step1: Repeat PartA Step1 to Step4.**

**Step 5**: Inside Outbound rules -> Select New Rules -> select custom and then click on next.

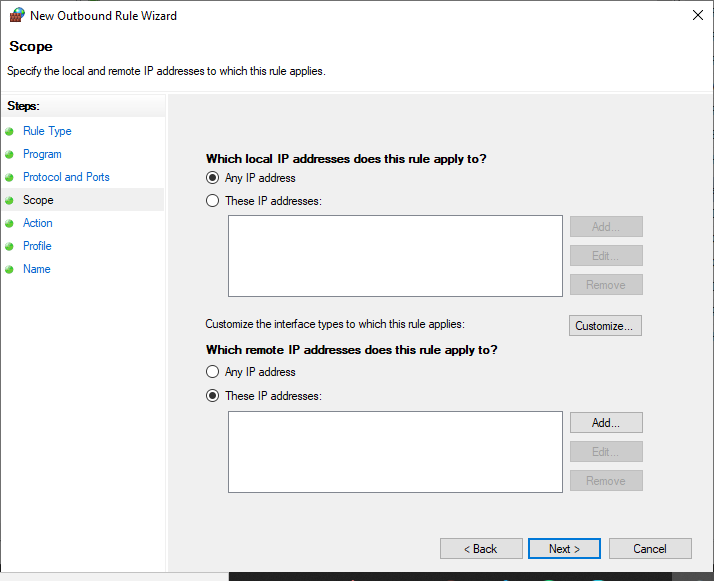


**Step 6**: When you click next you would see a window where you will see “Steps:” on left hand side of the

screen. From that select “Scope”.

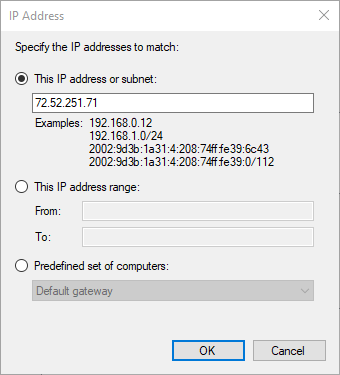


**Step 7**: In scope click on These IP addresses in remote IP

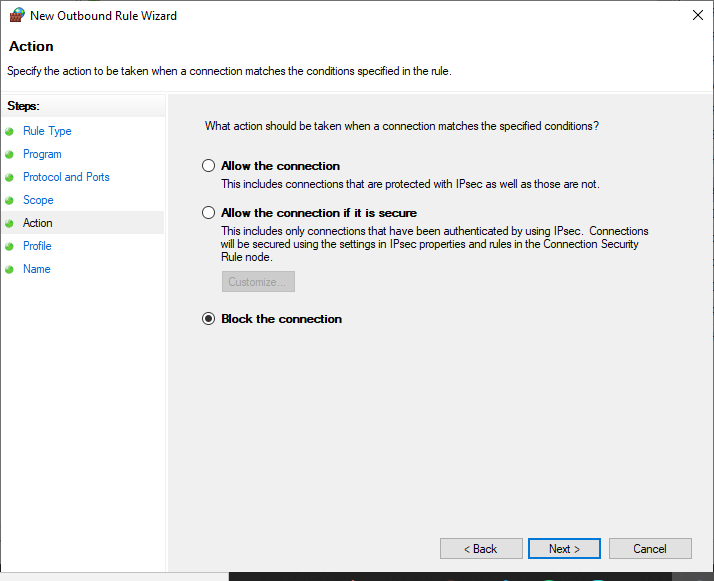


**Step**

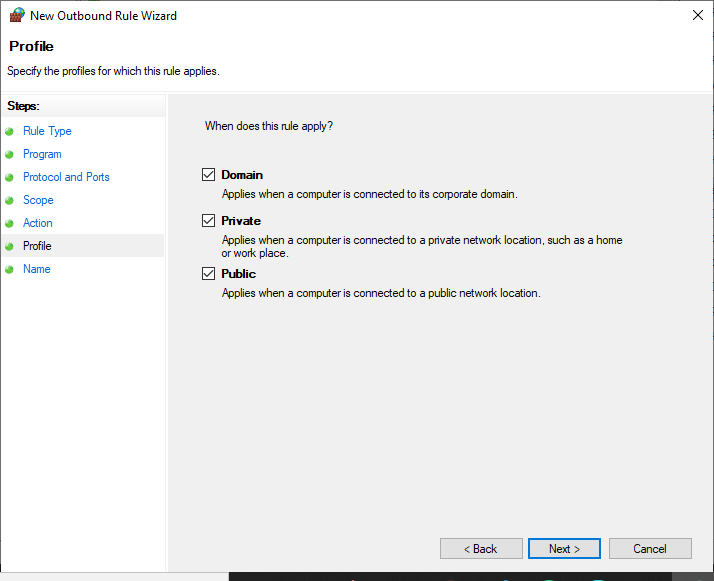
**8:** Click on add and Add the IP address of the website that you want to block and click ok.



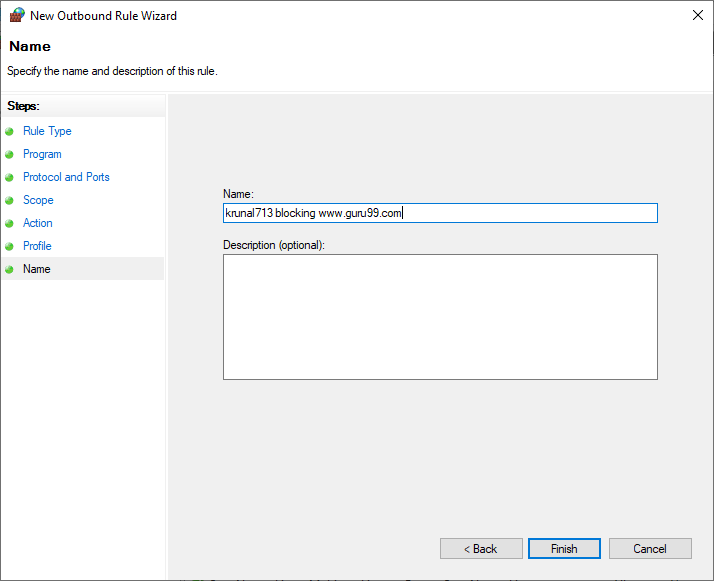
**Step 9:** Click on Block the connection in action



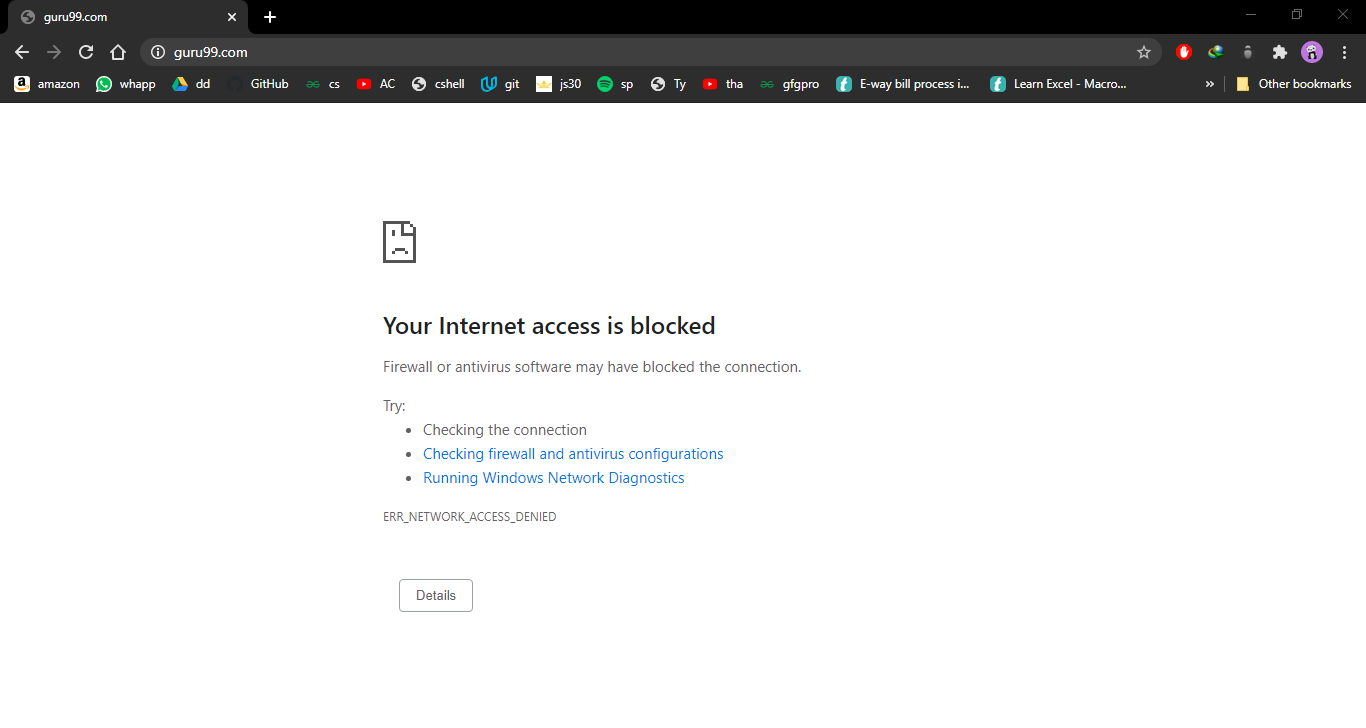
**Step 10:** Select the profiles domain private or public.

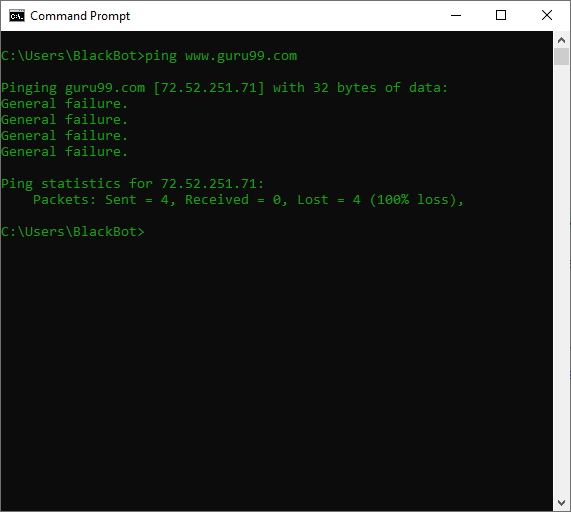


**Step 11:** Give a name to your new set rule and click on finish.



**Output:**

****

****