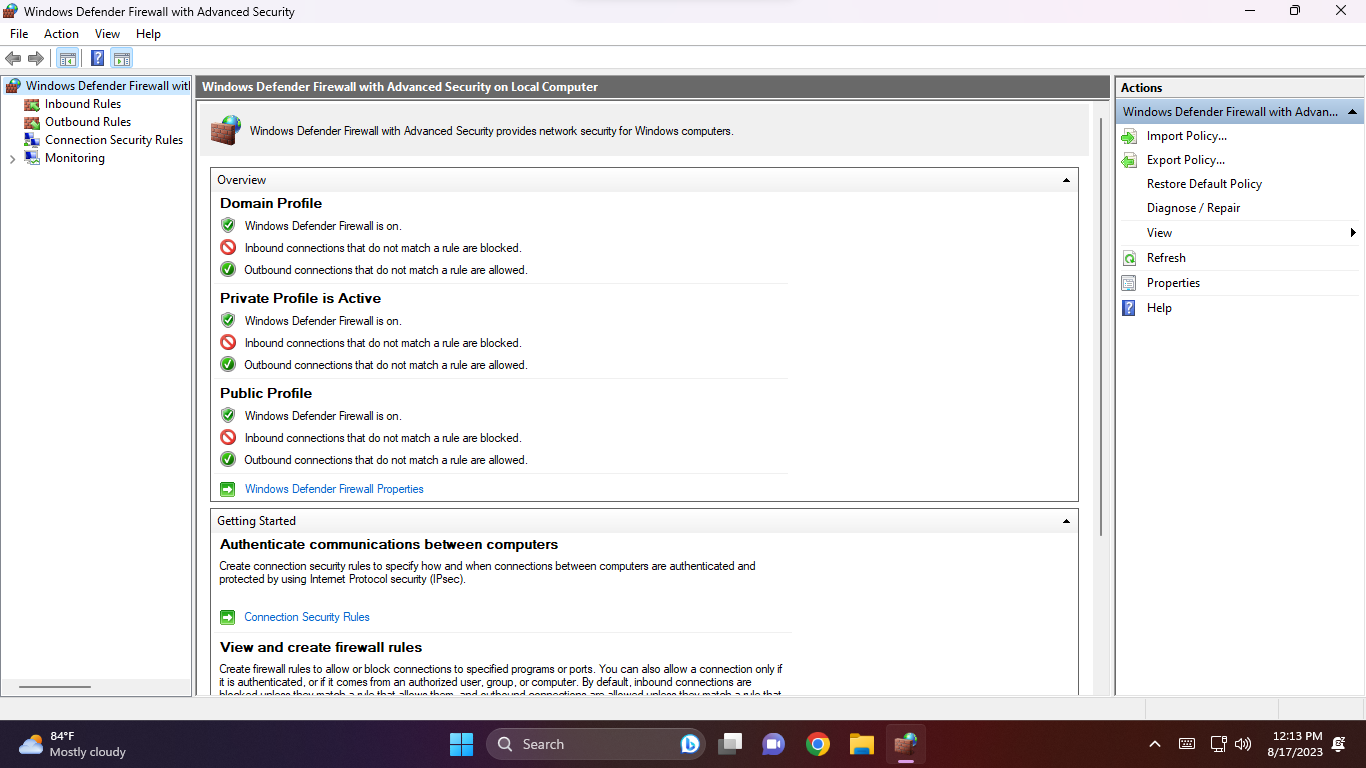
**Firewall Configuration and Rule-based Filtering**

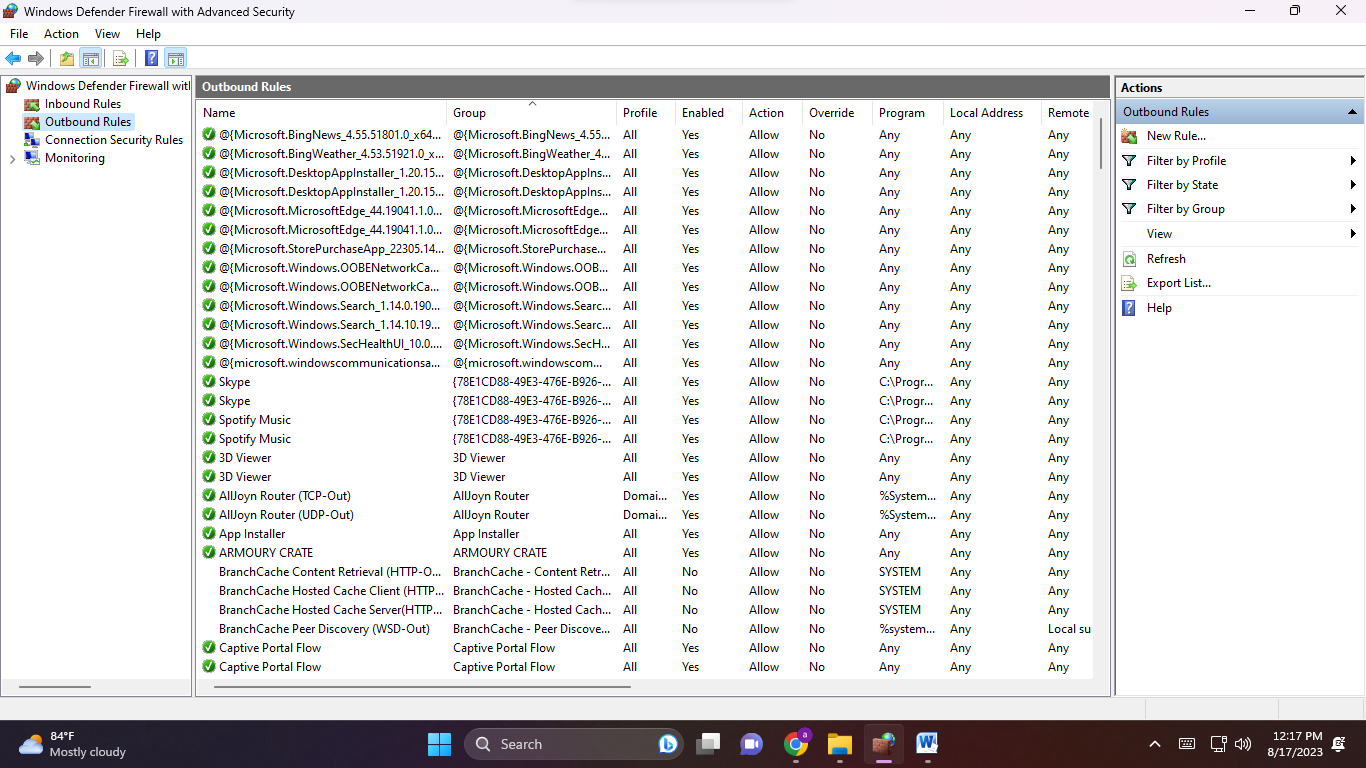
**Rule for Outbounds**

**Firewall Interface**



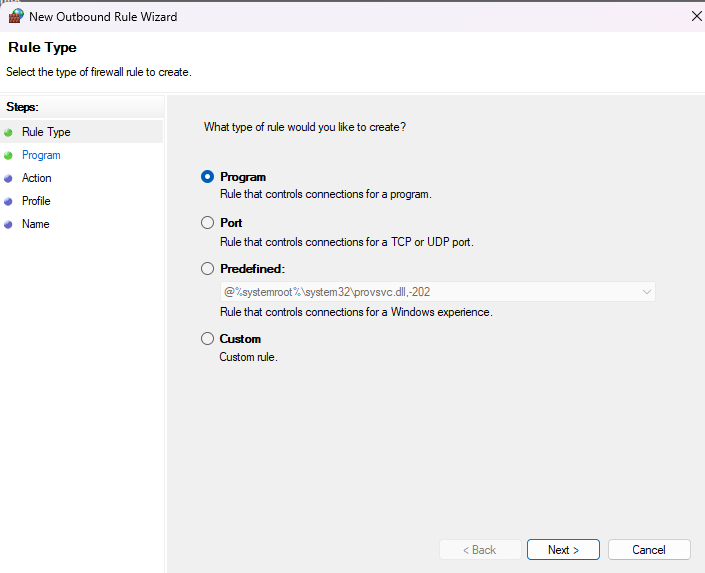
**Write a rule for Outbound**

**Select Outbound rules**



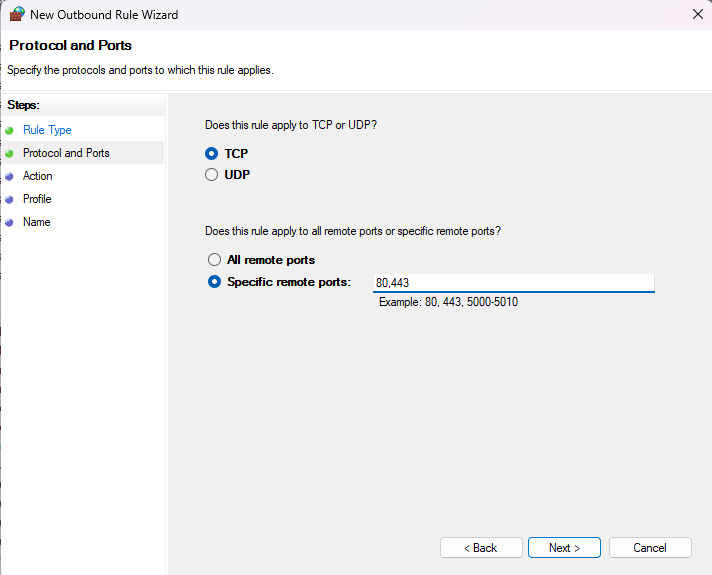
**Select the rule type:either rule for any Program /Port/Predefine/Custom**

**Here we are write rule for Port .**

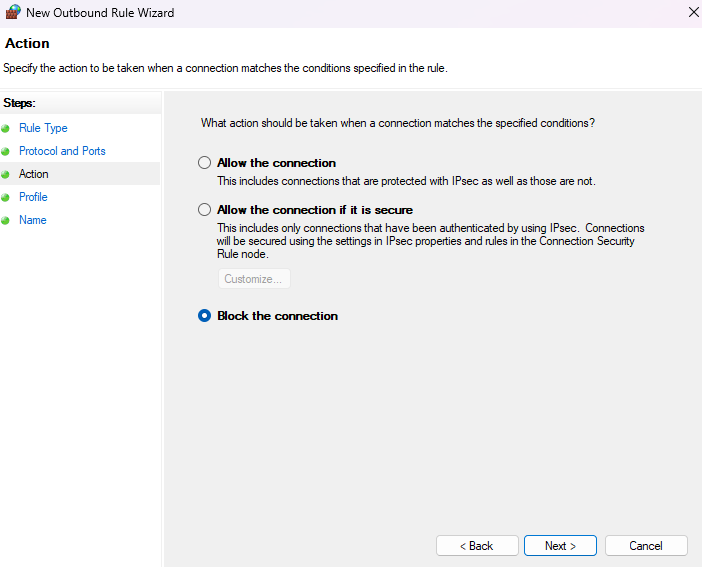


**After Selecting the port choose Either TCP or UDP . we are choosing TCP**

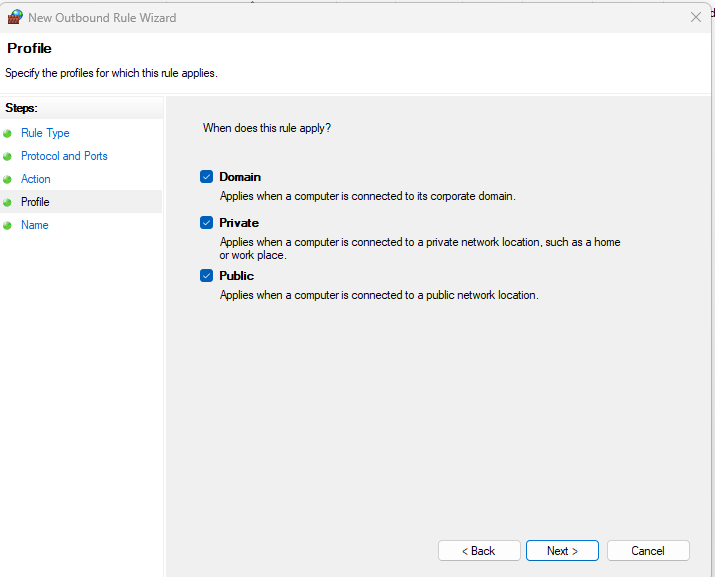
**Select TCP Protocol and Ports: Assign the for which port you want to apply the rule we are selecting 80 port**



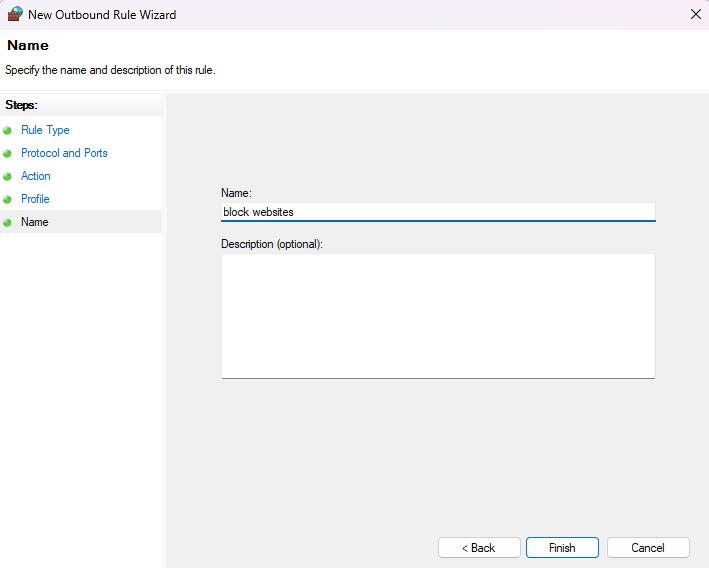
**Specify action for the rule: either you want to Allow the connection or block the connection. In this case we are block the connection**

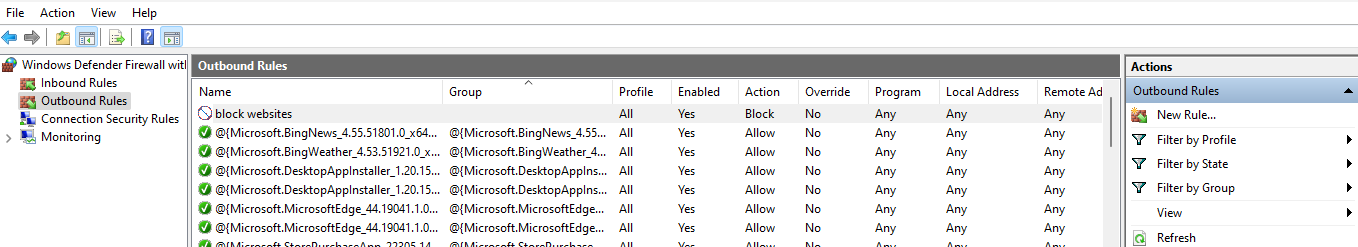


**Select the Profile to apply the rule:**



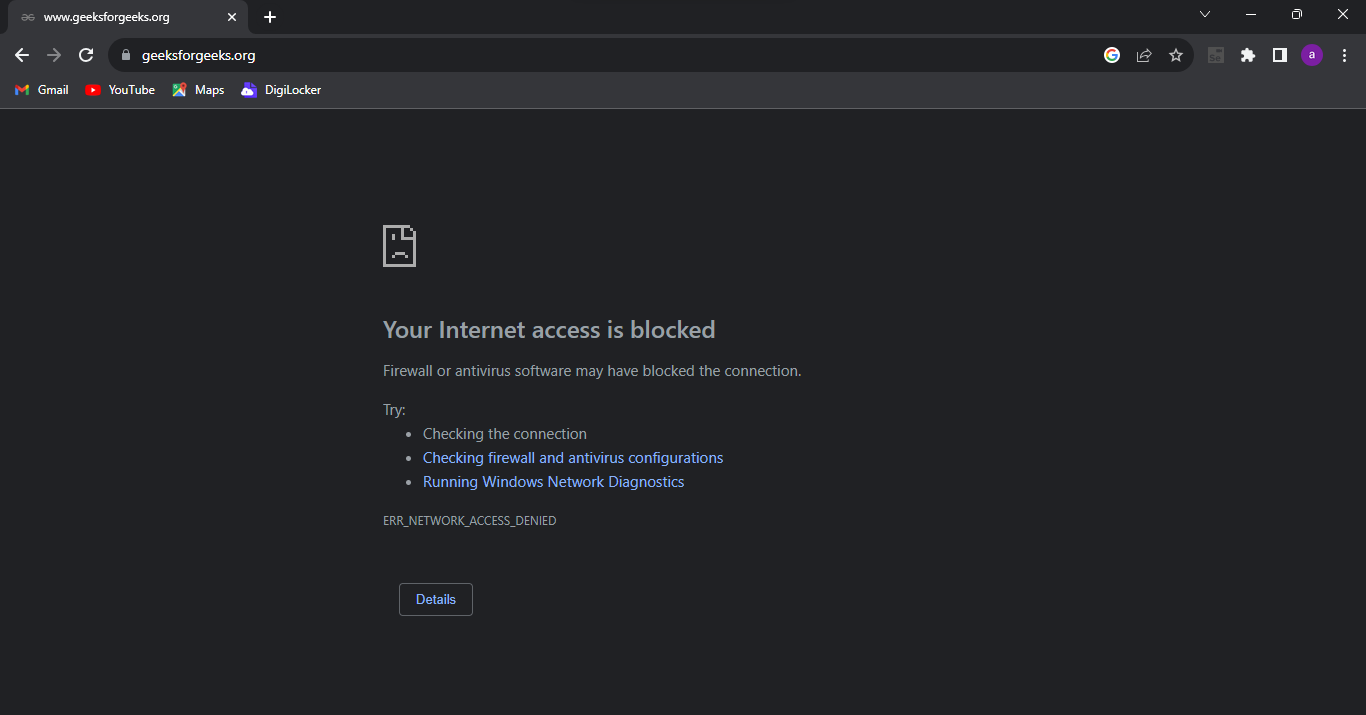
**Specify name for the rule:**



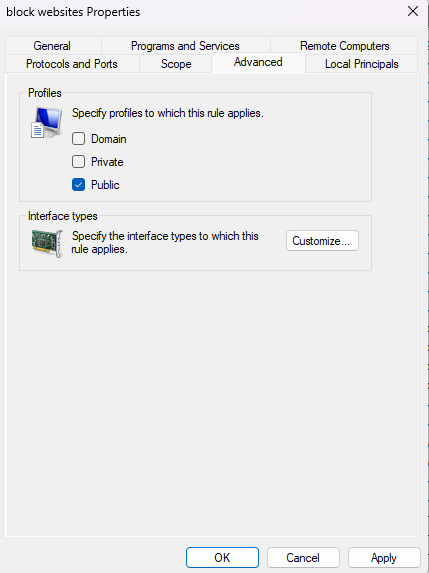


**Output:**

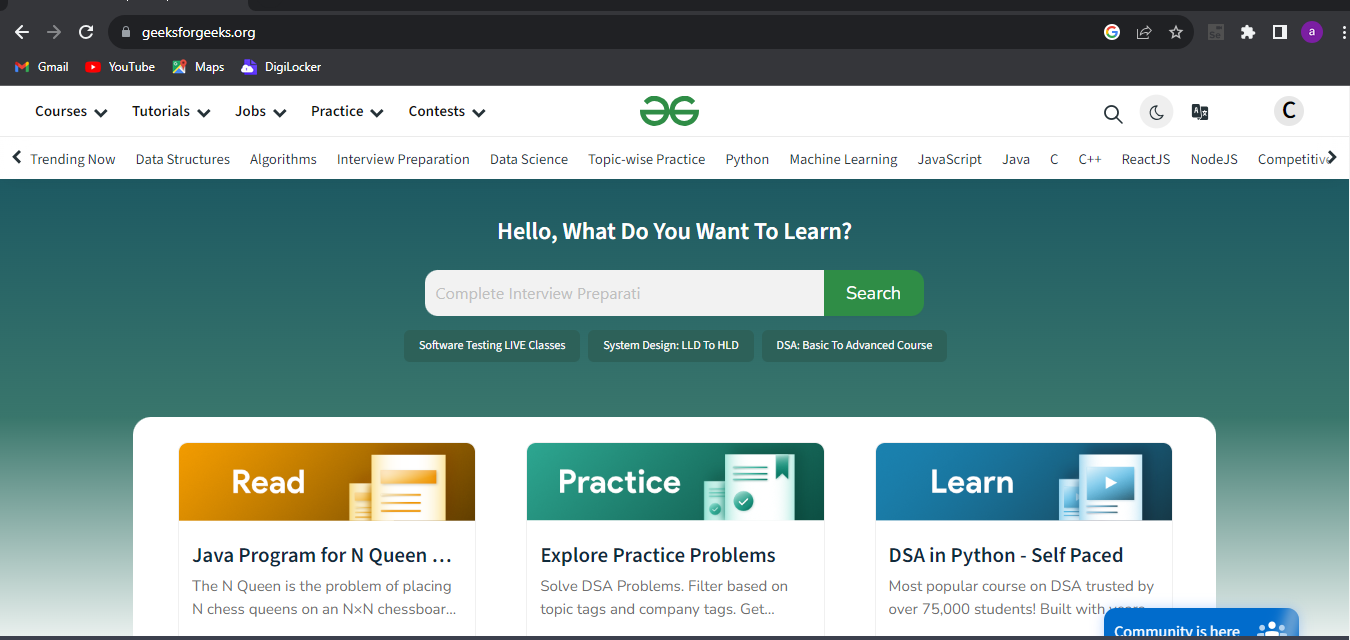
**After applying rule you want to open any website of port 80 it gives you following output**



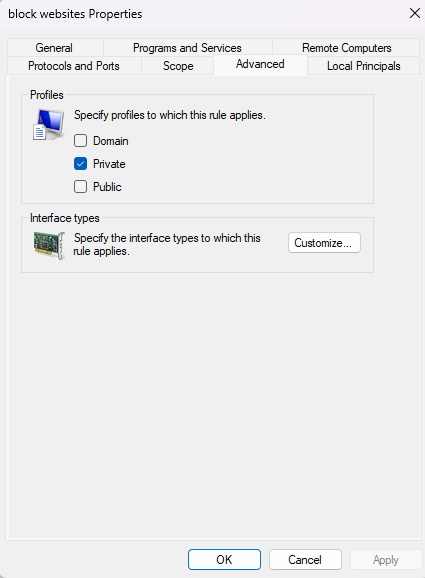
**Apply rule for public:**



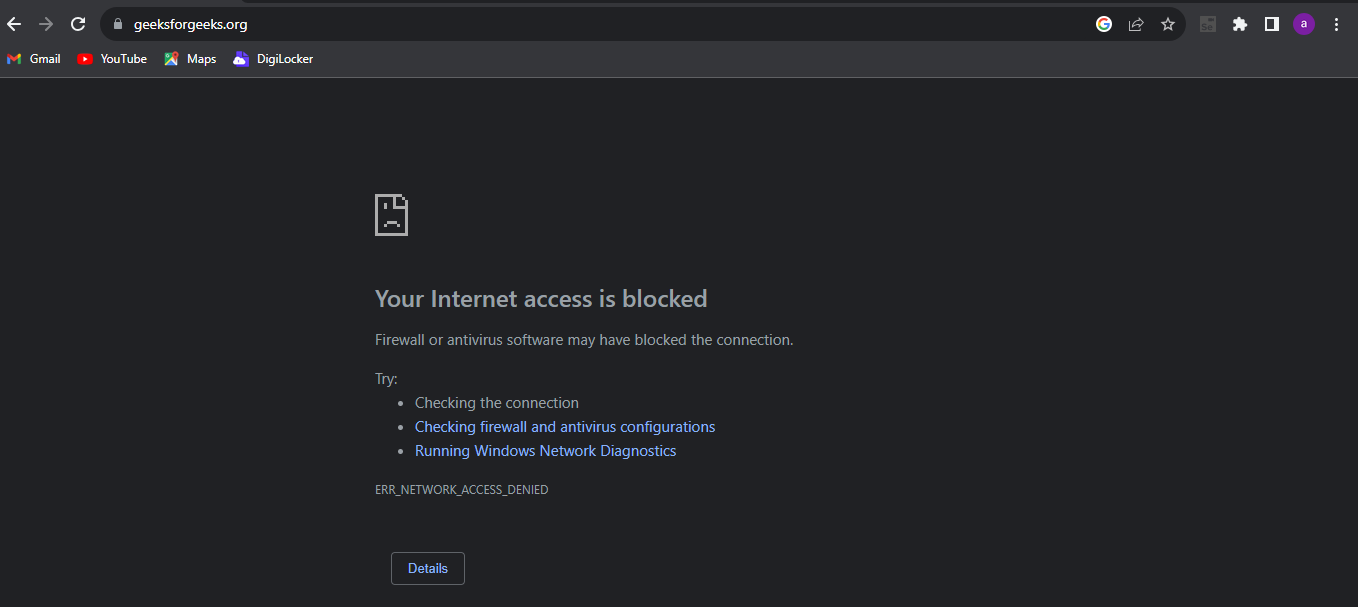
**Output:**



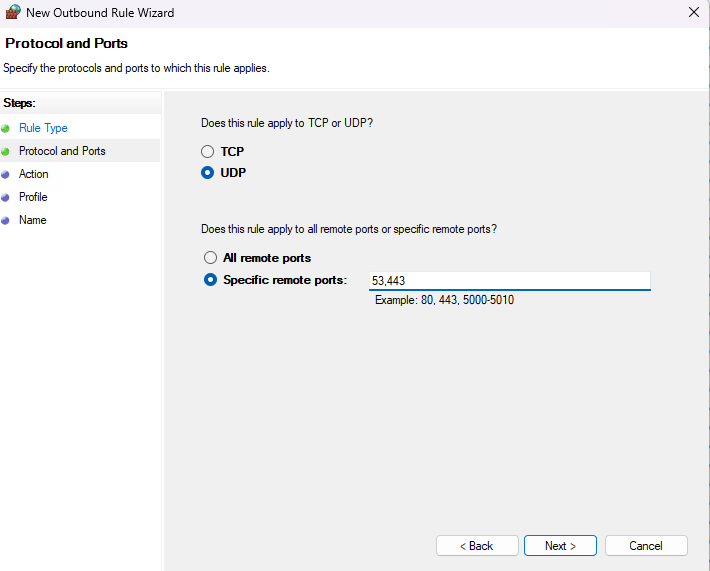
**Apply rule for Private:**



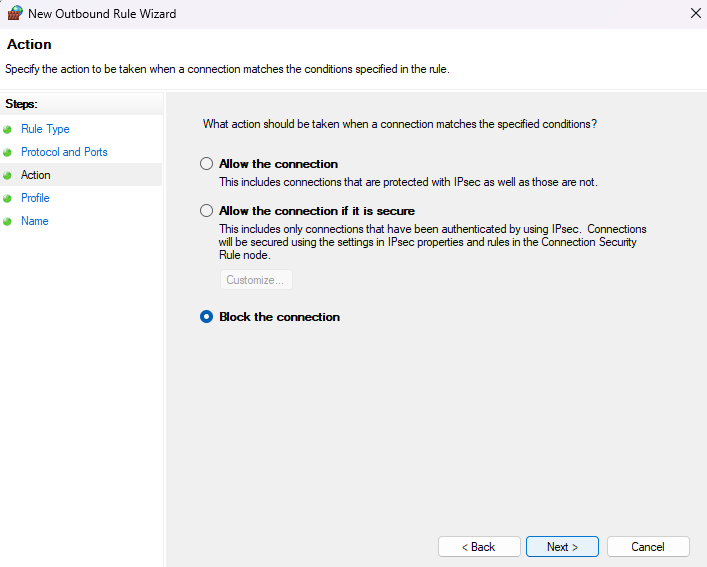
**Output:**



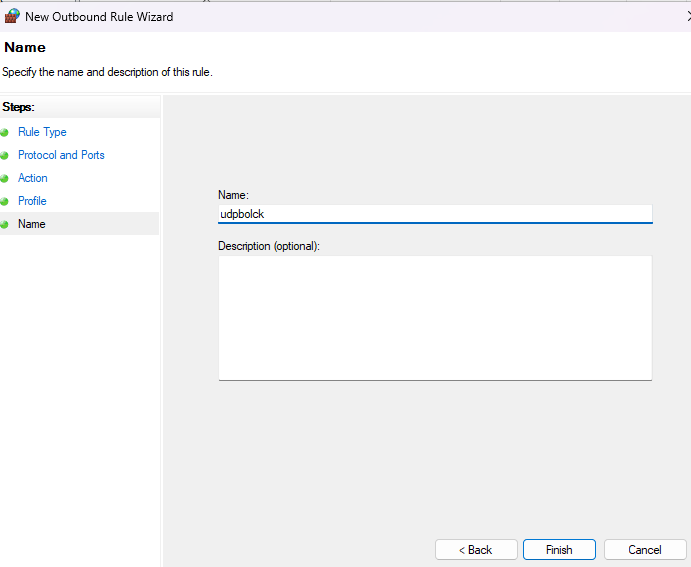
**After TCP we are Apply rule for UDP: Select UDP protocol and Ports:**



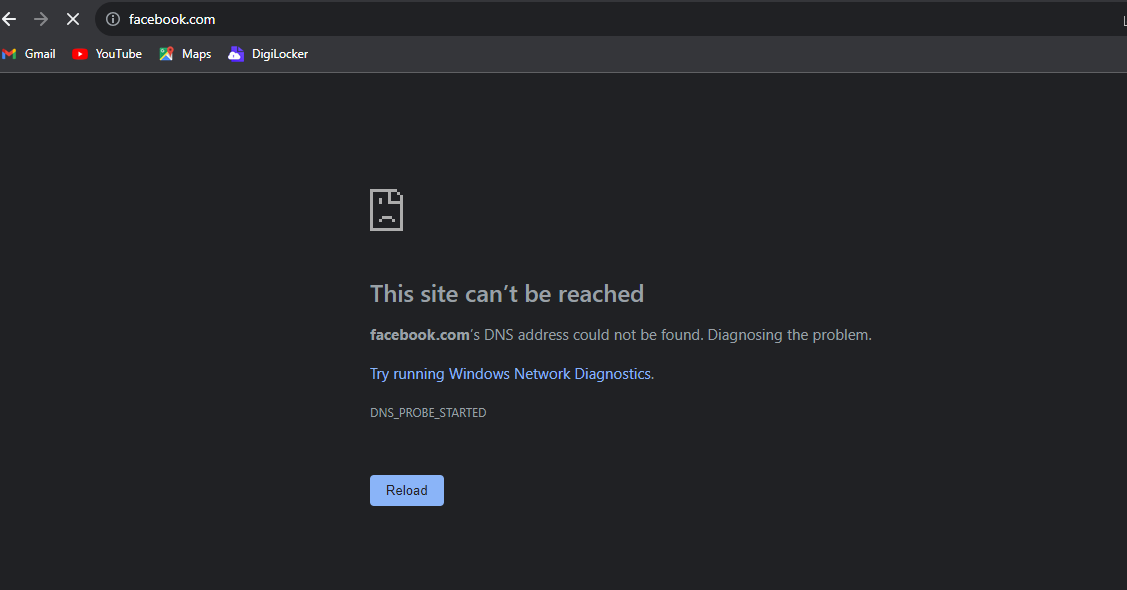
**Specify the action for the rule:**



**Specify name for the rule:**

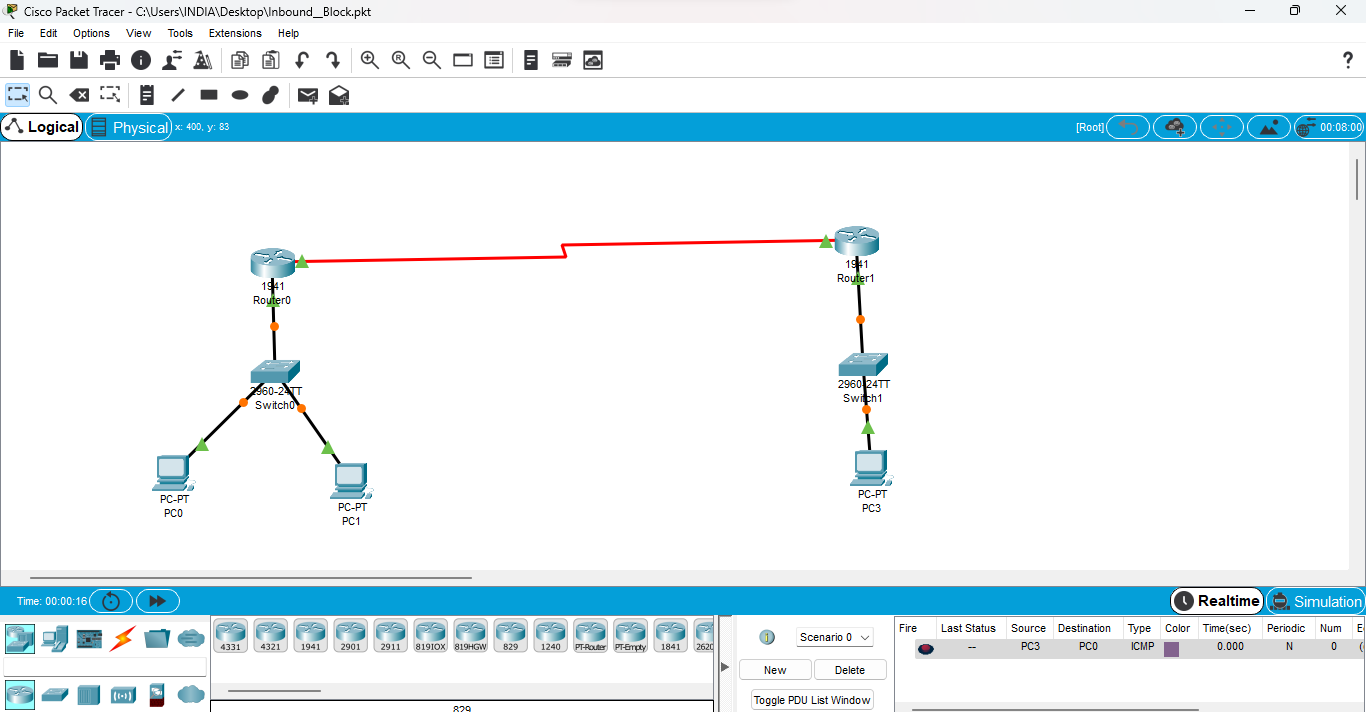


**Output:**



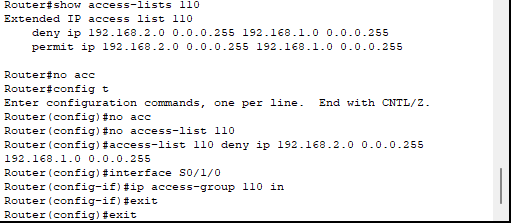
* **Write a rule for Inbound using Cisco packet tracer**

**Make a connection using 2 router (1941) , 2 switch, 3 PC**

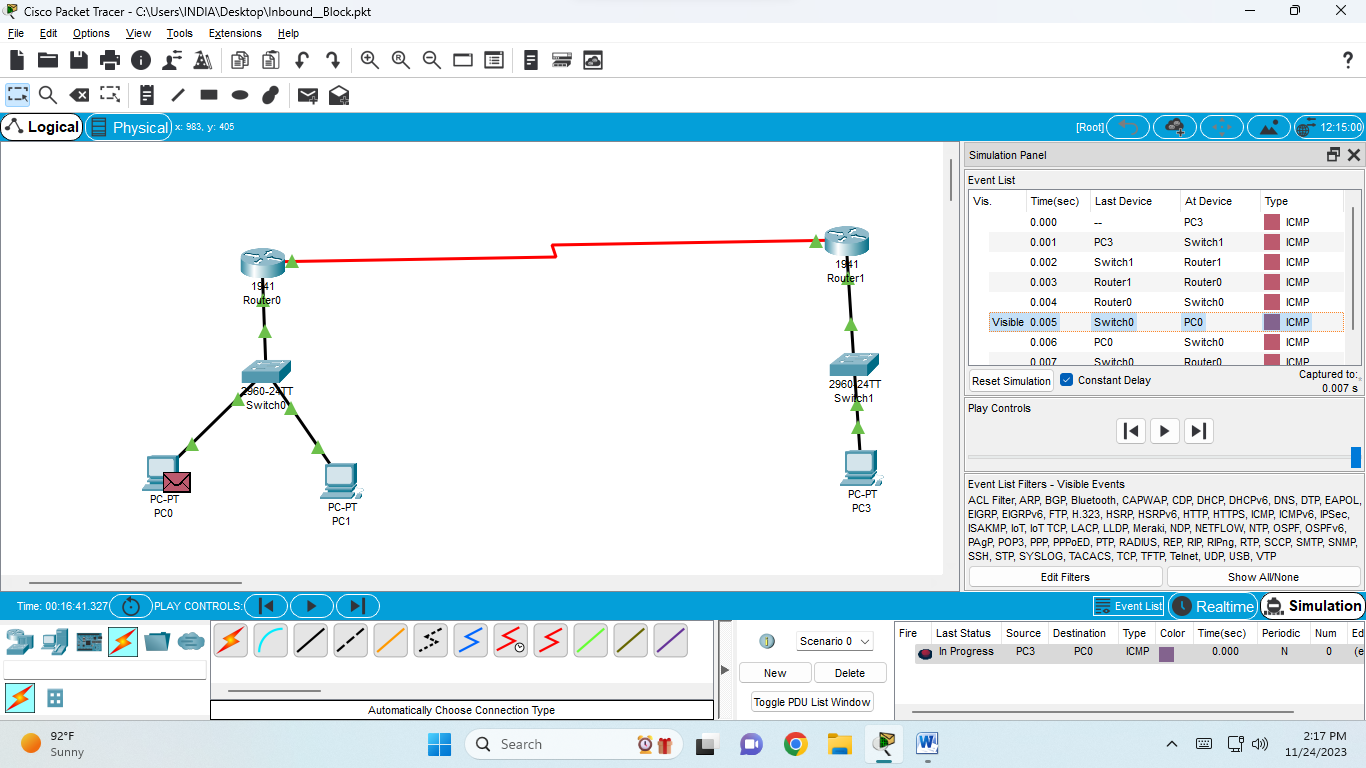


**Then assign the Ip address for the all pc and routers**

**Then give command to Router 1**



**After that send packet 192.168.2.0 to 192.168.1.0 it successfully reach at pc3 to pc0**



**But when it come back to the pc0 to pc3 it is failed at Router1 because we are write a rule for inbound**

