**Setup and Use a Firewall on Windows/Linux**

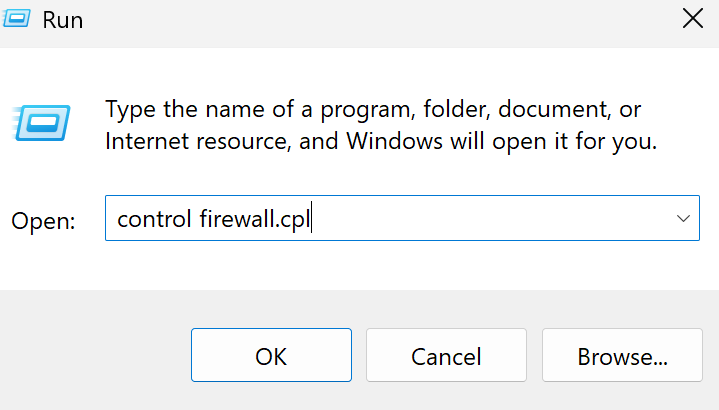
**Objective: Configure and test basic firewall rules to allow or block traffic.**

**Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.**

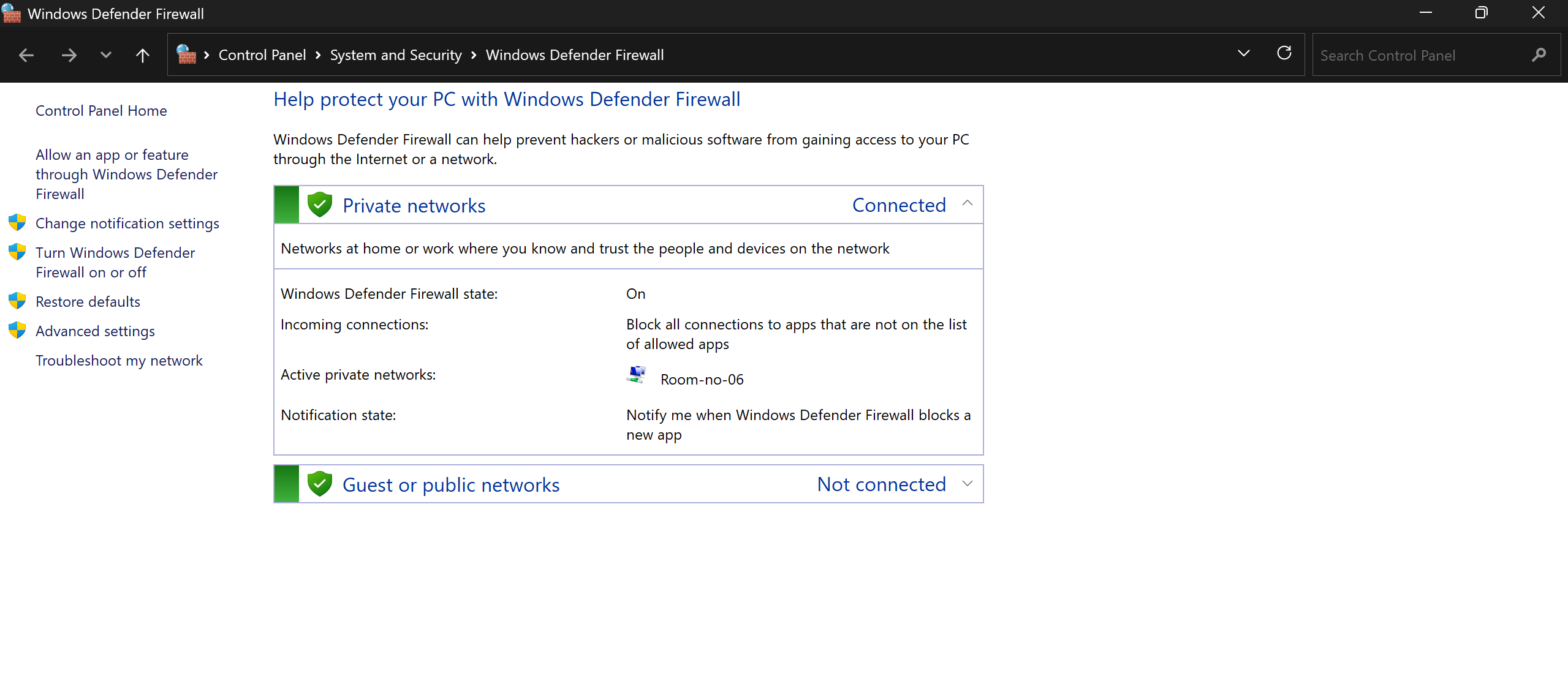
**Deliverables: Screenshot/configuration file showing firewall rules applied.**

**commands or GUI steps used.**

We are using here windows defender firewall and configure the rules.

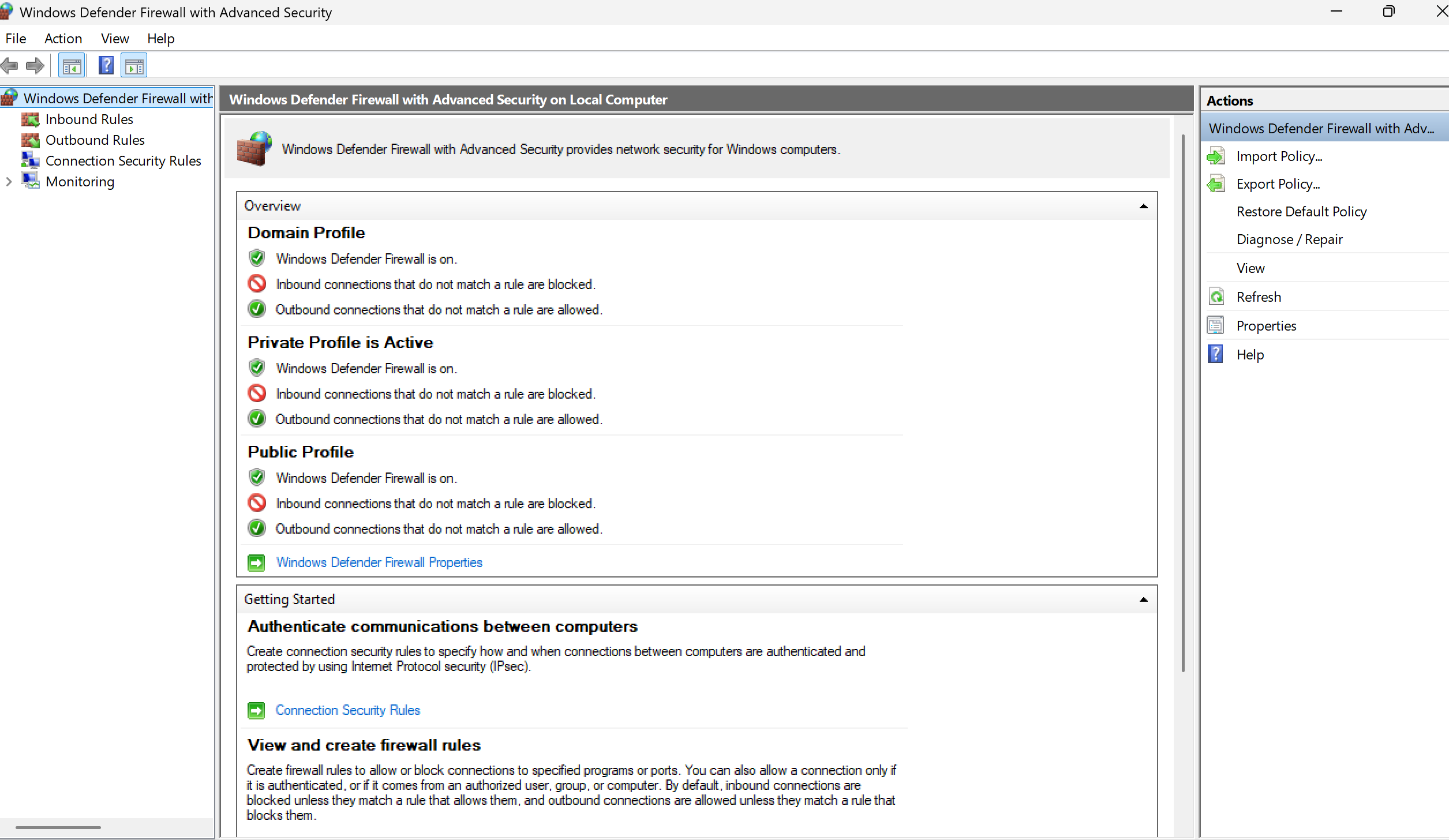


After running a command: control firewall.cpl we get this window. now click on advance settings >



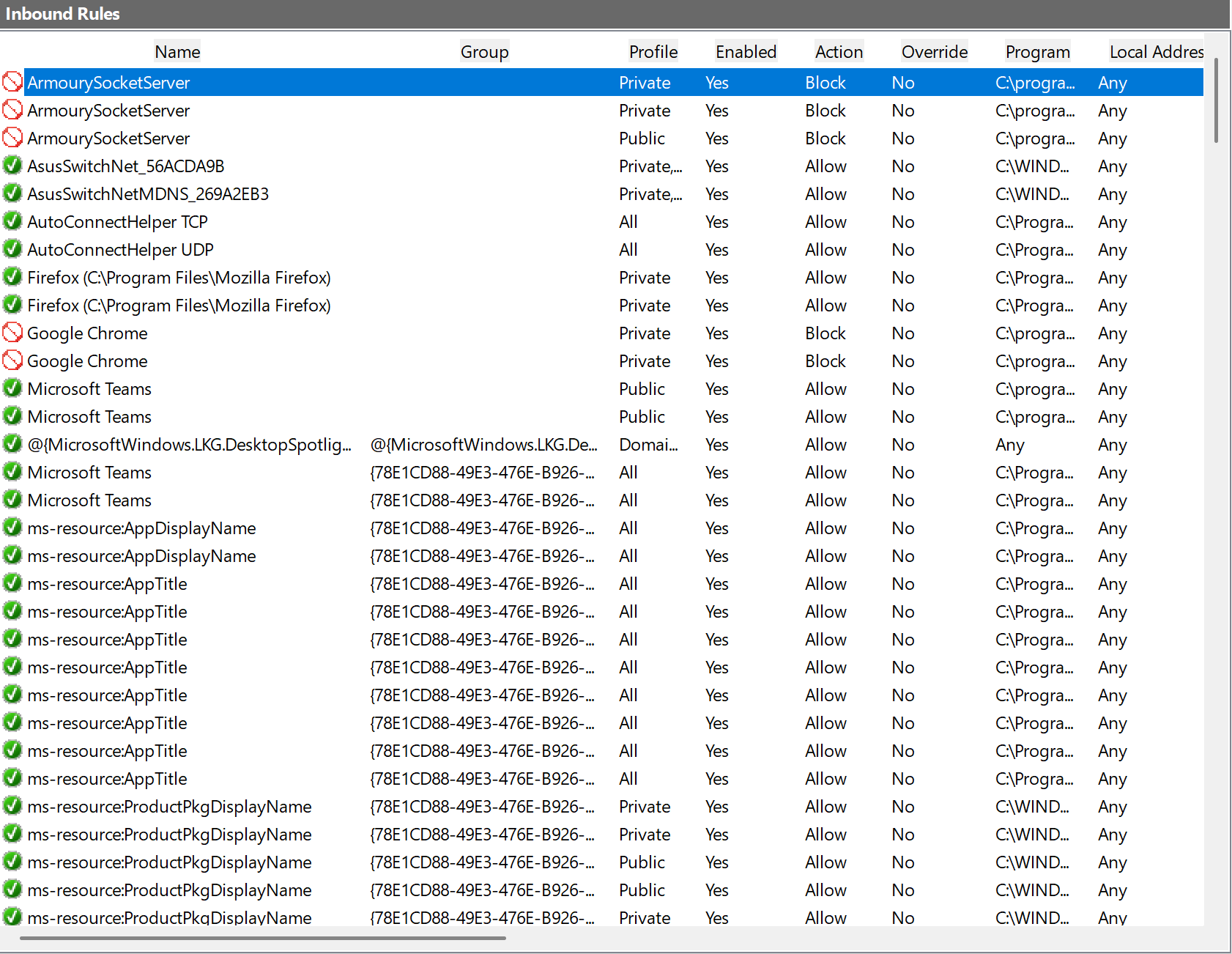


Then we get the below window that show inbound and outbound firewall rules.

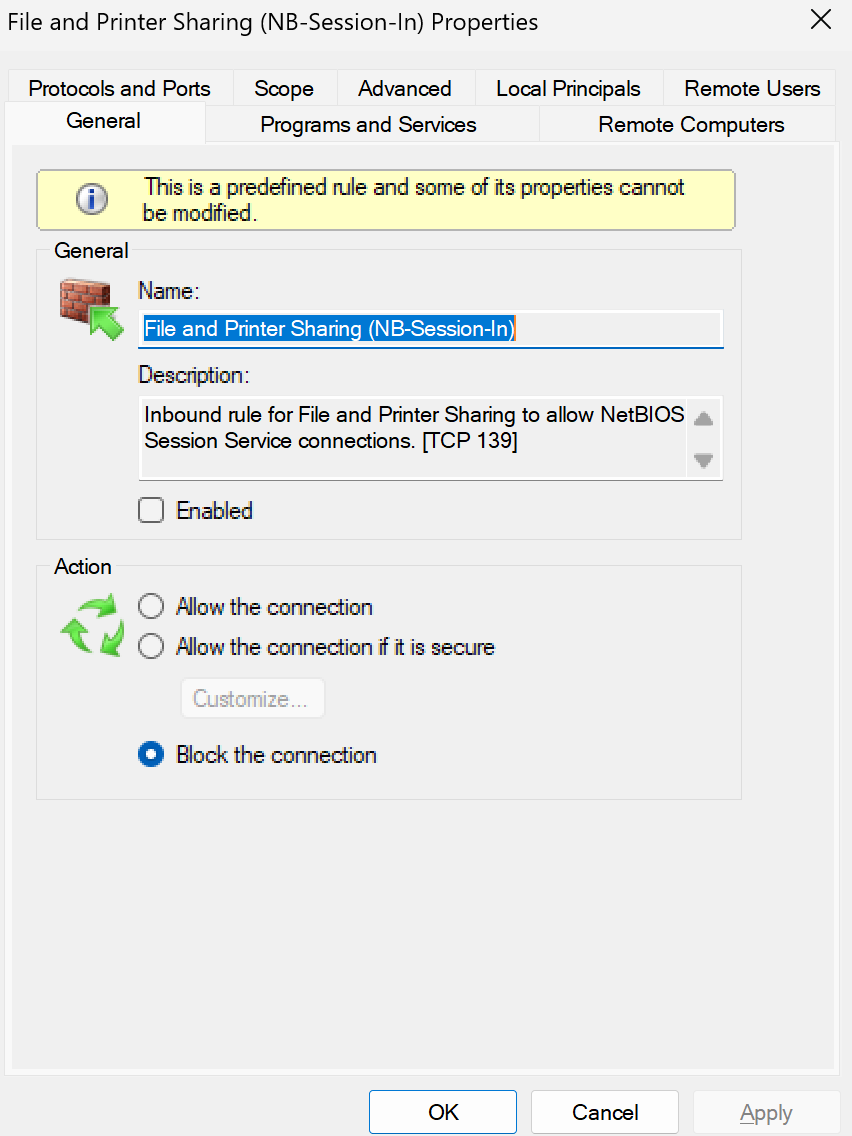




List of inbound current firewall rules.

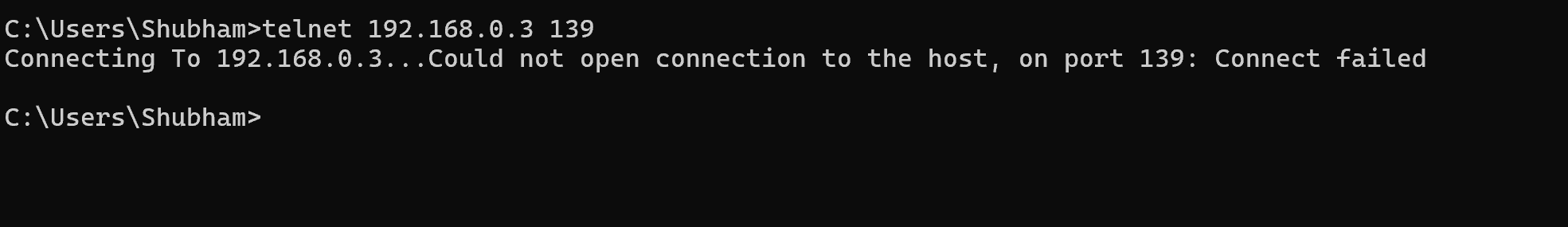


Now we set a rule to block a port 139 on firewall for inbound traffic. click ok to apply changes.





Then we check for the open port using command line, weather the rule is applied or not.

If the port is open then we get a blank screen with cursor, if it is closed we get a “connection failed” message. 

Hence the inbound rule is applied for the port 139 to block it.

Summary how firewall filters traffic

A firewall filters network traffic by examining data packets and comparing them to predefined security rules. These rules determine whether to allow or block the traffic based on criteria like source and destination IP addresses, port numbers, and protocols. Essentially, the firewall acts as a gatekeeper, controlling which data can enter and leave a network based on these rules, ensuring only safe and legitimate traffic is permitted.