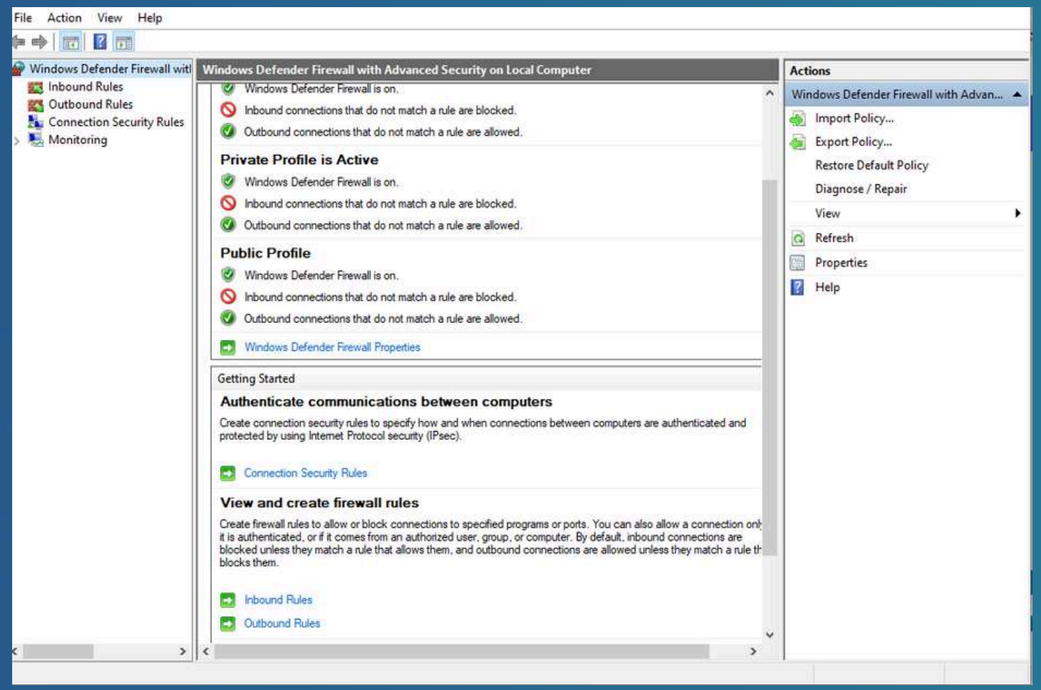
TASK 4 : SETUP AND USE A FIREWALL ON WINDOWS/LINUX

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

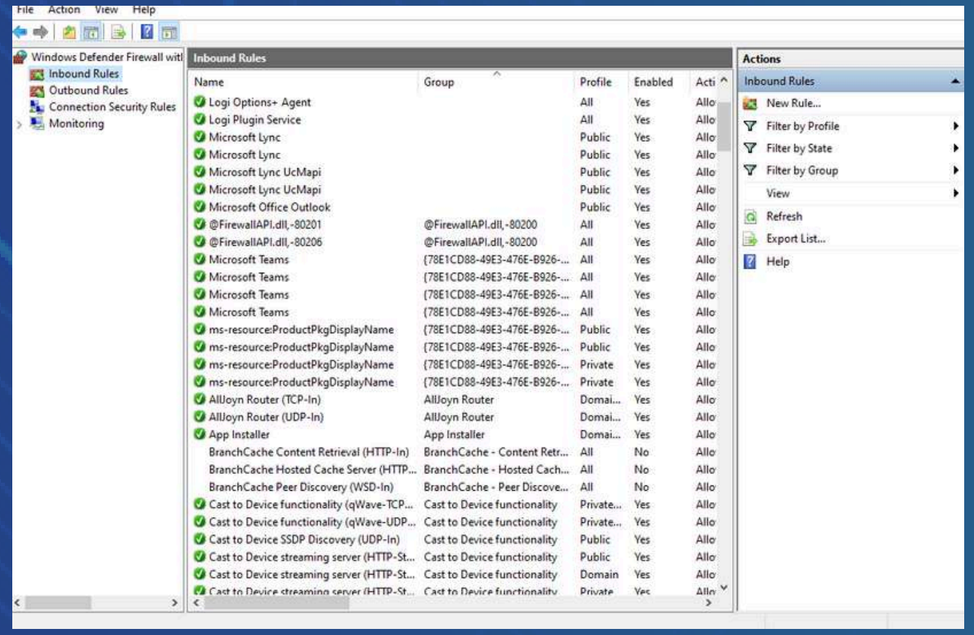
1.Open firewa l configuration tool (Windows Firewal or terminal for UFW).

I opened Windows Defender Firewall with Advanced Security by searching for “wf.msc” in the Start menu.

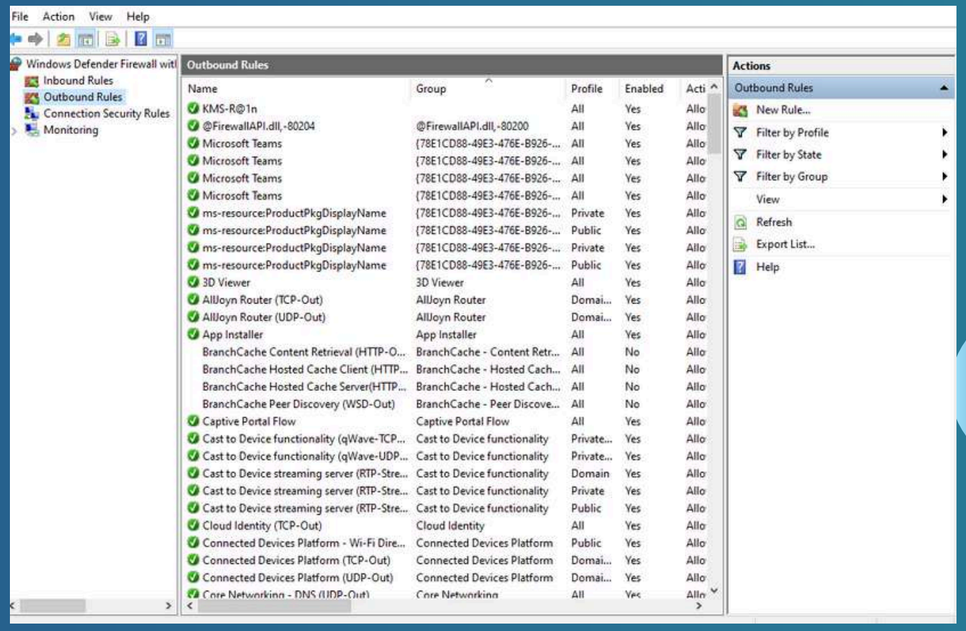


2.List current firewal rules.

Inbound



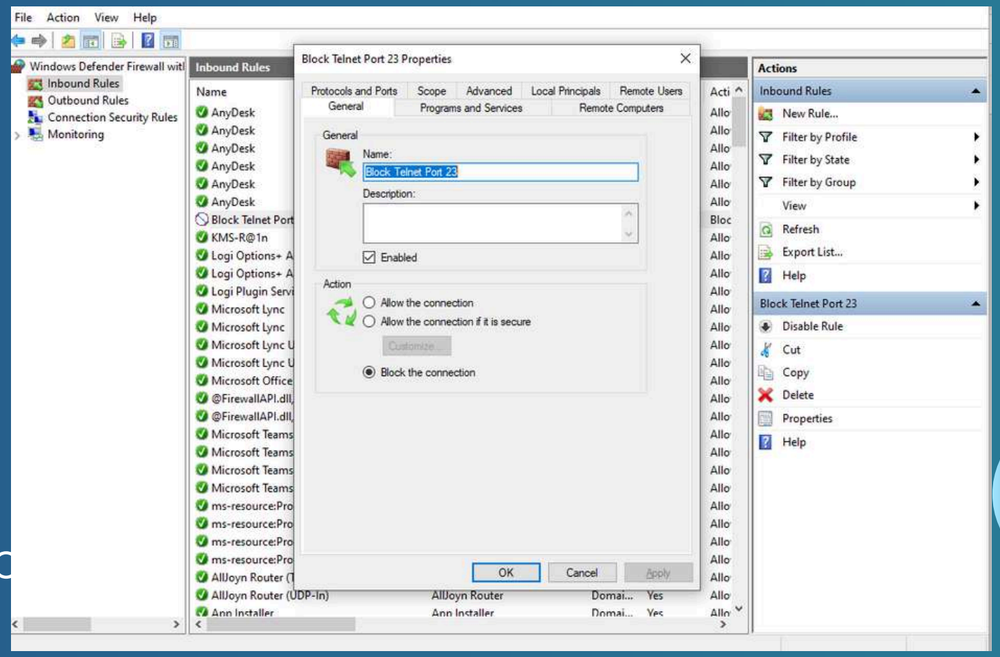
Outbound



3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet)

Created a New Inbound Rule to Block Port 23 (Telnet):

- Went to Inbound Rules → New Rule
- Selected Port
- Chose TCP
- Entered port 23
- Selected Block the connection
- Applied rule to Domain, Private, and Public
- Named it “Block Telnet Port 23”

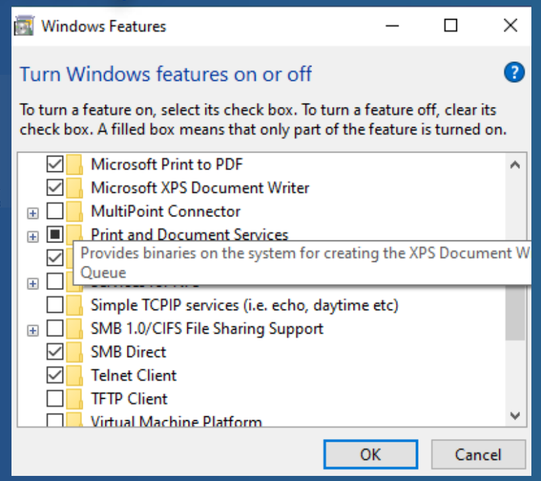


4.Test the rule by attempting to connect to that port localy or remotely.

Enable Telnet on Windows

- Press Windows Key type “Turn Windows features on or off”
- Scroll down
- Tick Telnet Client
- Click OK

Wait for installation to finish



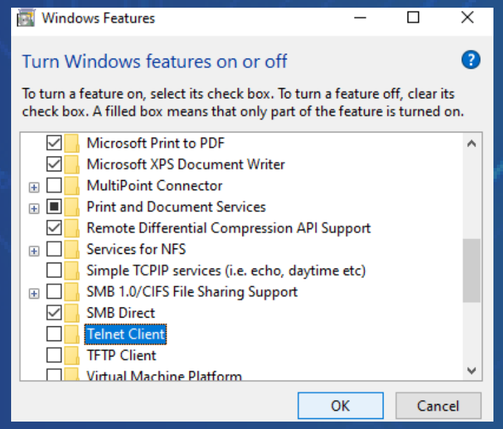
Tested the Rule

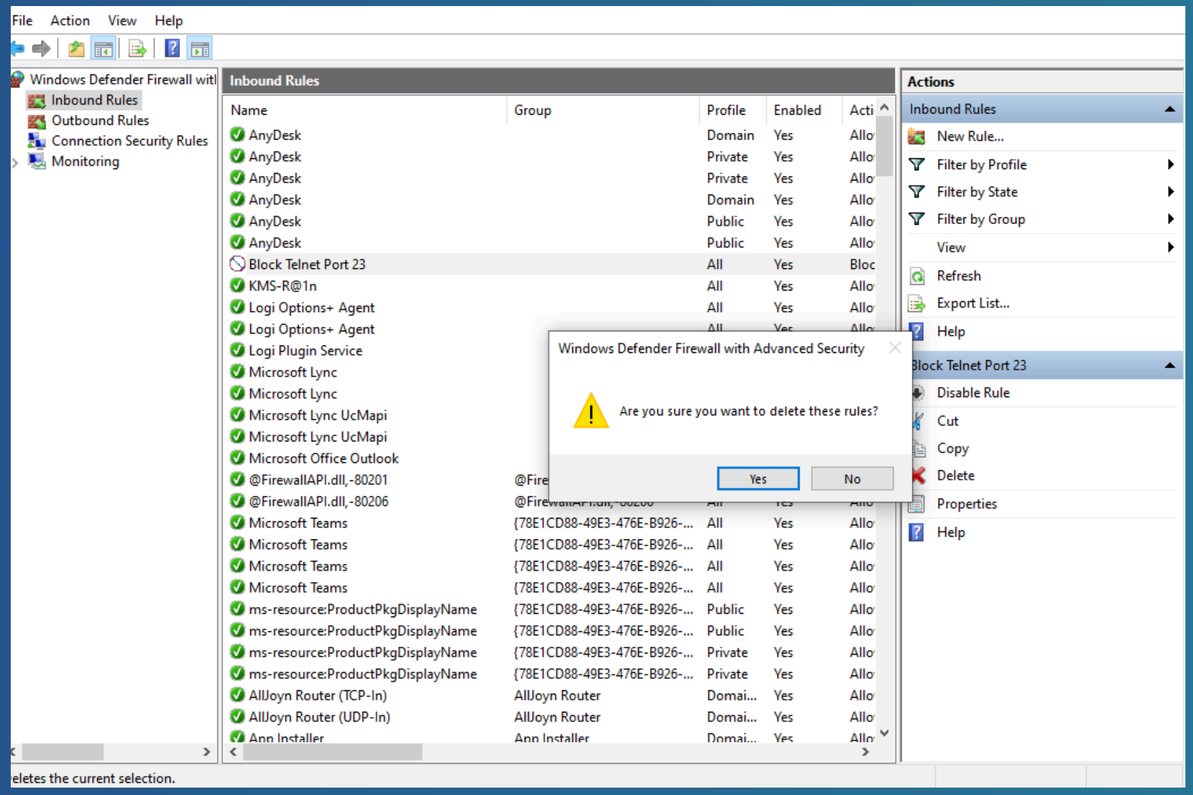
- telnet 127.0.0.1 23
- telnet localhost 23

```
C:\Windows\system32>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed

C:\Windows\system32>
C:\Windows\system32>telnet 127.0.0.1 23
Connecting To 127.0.0.1...Could not open connection to the host, on port 23: Connect failed

C:\Windows\system32>
C:\Windows\system32>
```

6.Remove the test block rule to restore original state.

After completing the test, I returned to Inbound Rules, selected Block Telnet Port 23, and deleted it to restore the firewall to its original state.





8.Summarize how firewal filters traffic.

- A firewall filters traffic by checking each incoming or outgoing packet against defined rules.
- If a packet matches a rule (allow/block), the firewall applies that action.
- This protects the system by controlling which ports, services, and applications can communicate.

THANK YOU!