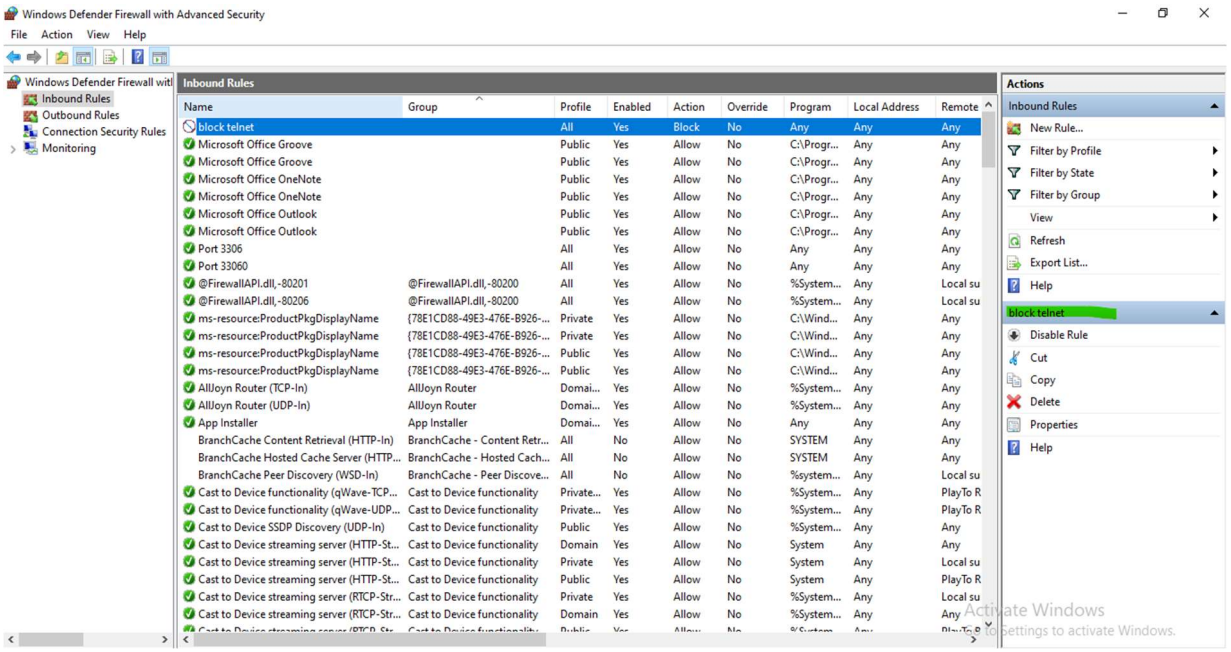
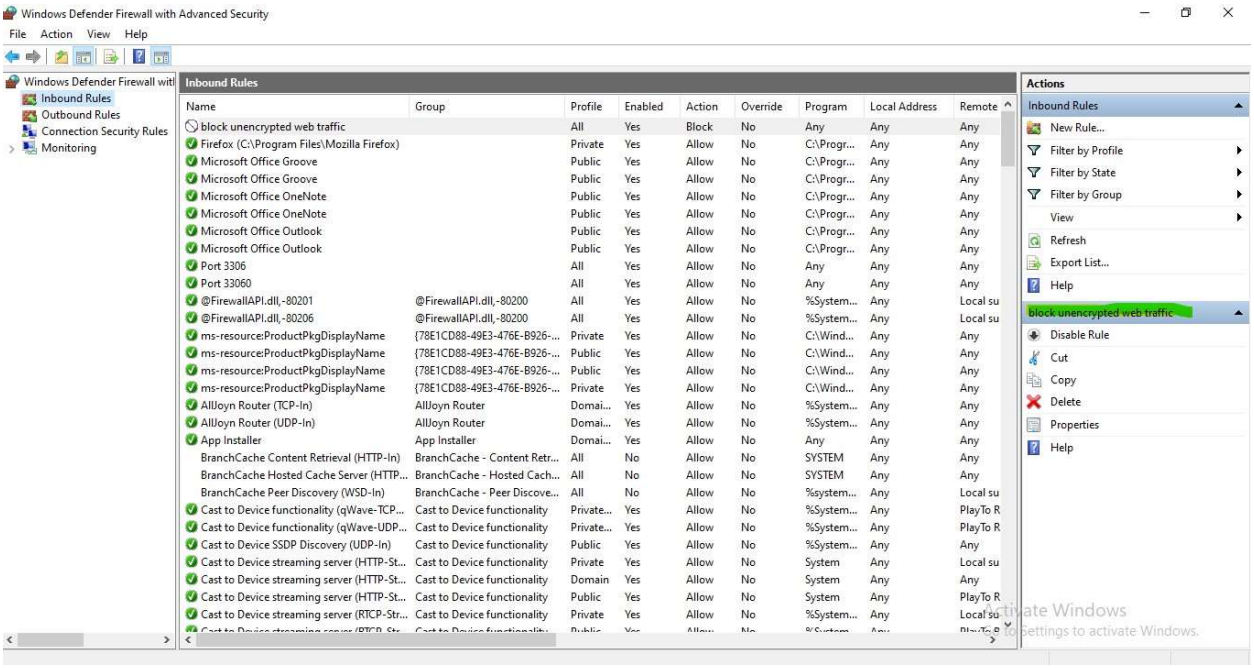
1. List of current firewall rule
    - Inbound rules
    - Out bound rules
    - Connection security rules

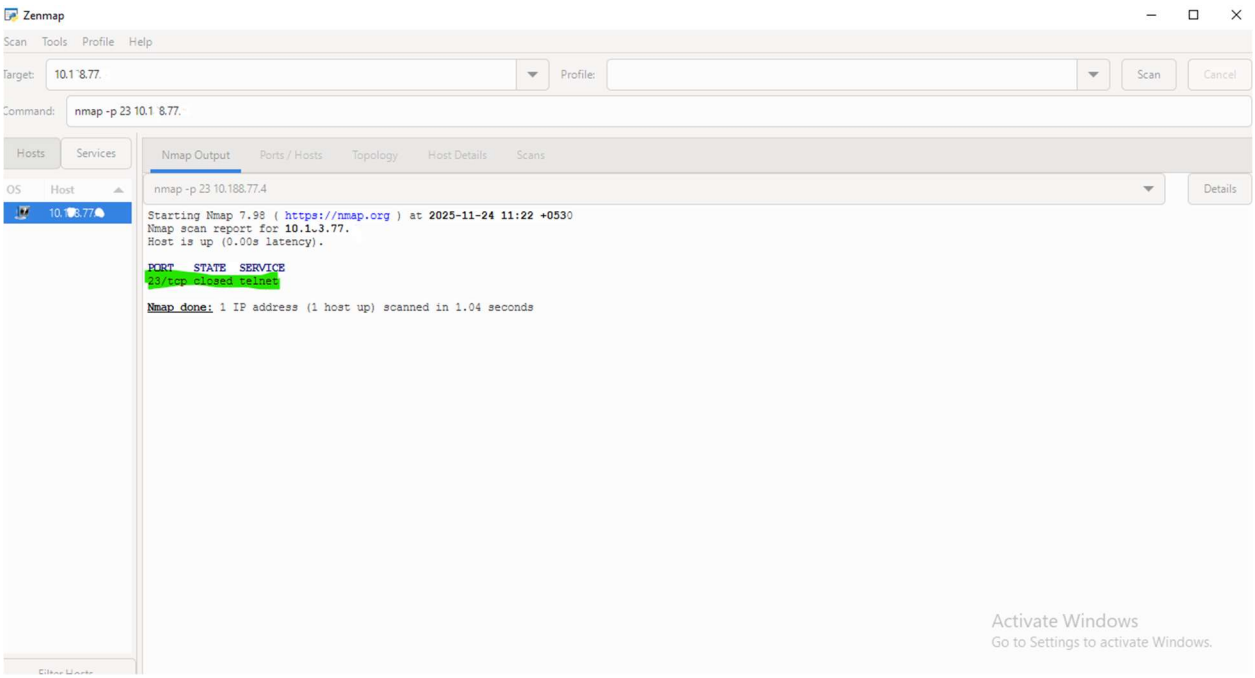
2. Add a rule to block inbound traffic on a specific port
    - Open Windows Defender Firewall and go to Advanced Security
    - Firewall → Advanced Settings
    - Inbound Rules → New Rule
    - Select Port
    - Choose TCP
    - Enter Port: 23
    - Select Block the connection
    - Apply on Domain, Private, Public
    - Name the rule:-Block Telnet
      Port number:- 23



Port numer:-80



3. Testing the rule by using Nmap :- tcp/23 closed

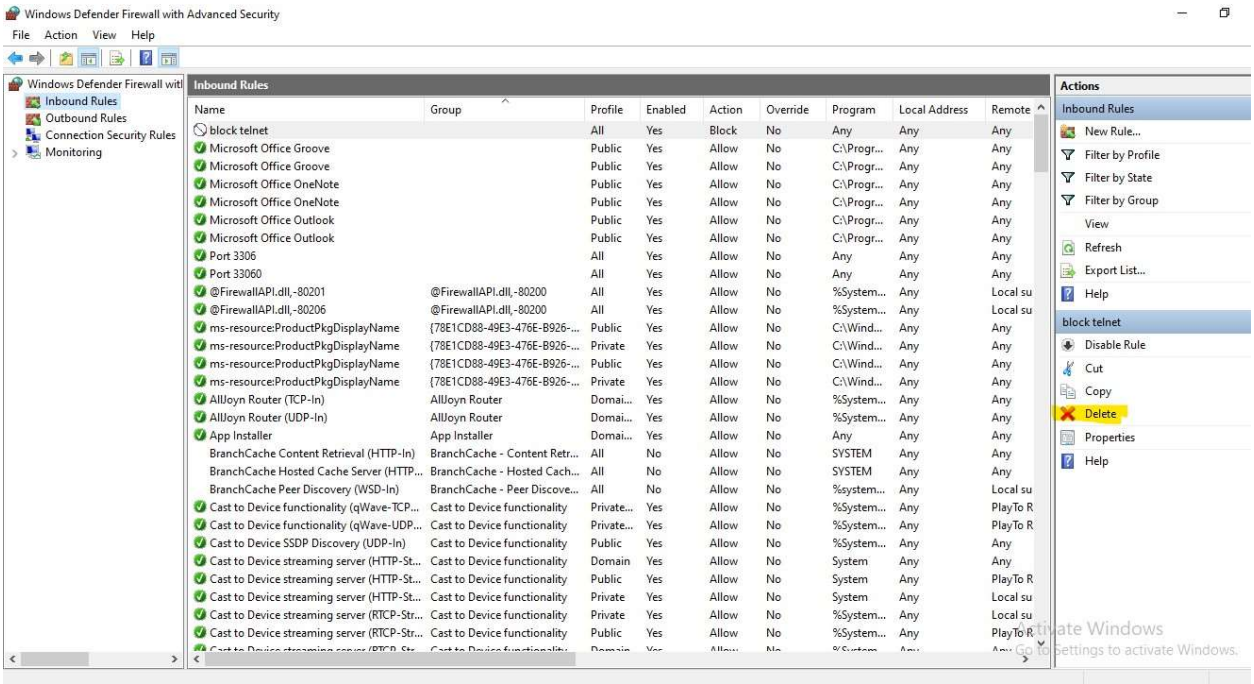


(PowerShell Test-NetConnection -ComputerName localhost -Port 23

Expected Output:

- TcpTestSucceeded : False → port is blocked
- TcpTestSucceeded : True → port is open/allowed)

4. .Removing the test block rule to restore original state :-
    - Advanced Settings → Inbound Rules
    - Right-click Block Telnet → Delete



5. summary
   A firewall controls network traffic by comparing each packet against security rules (based on IPs, ports, protocols, and direction) and then allowing or blocking it accordingly.