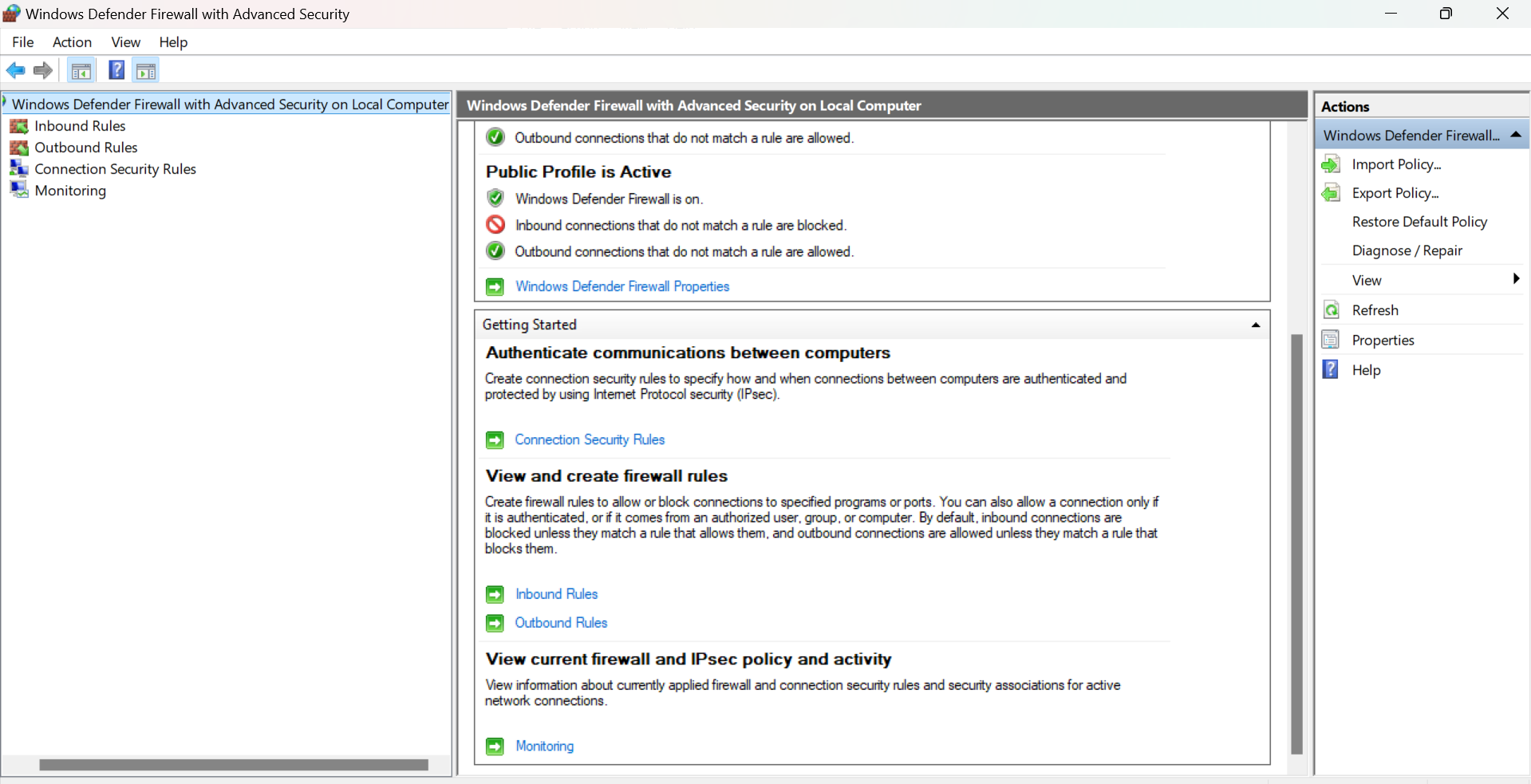
**Task 4 : Setup and Use a Firewall on Windows/Linux**

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

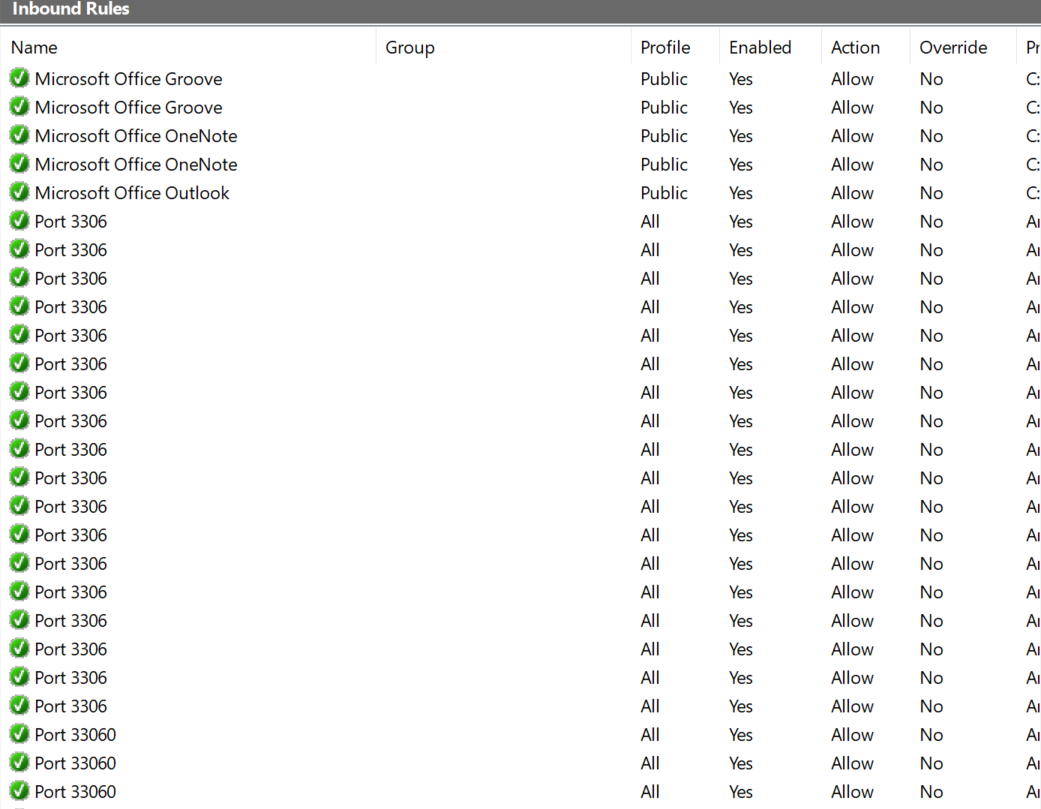
**Tools:** Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

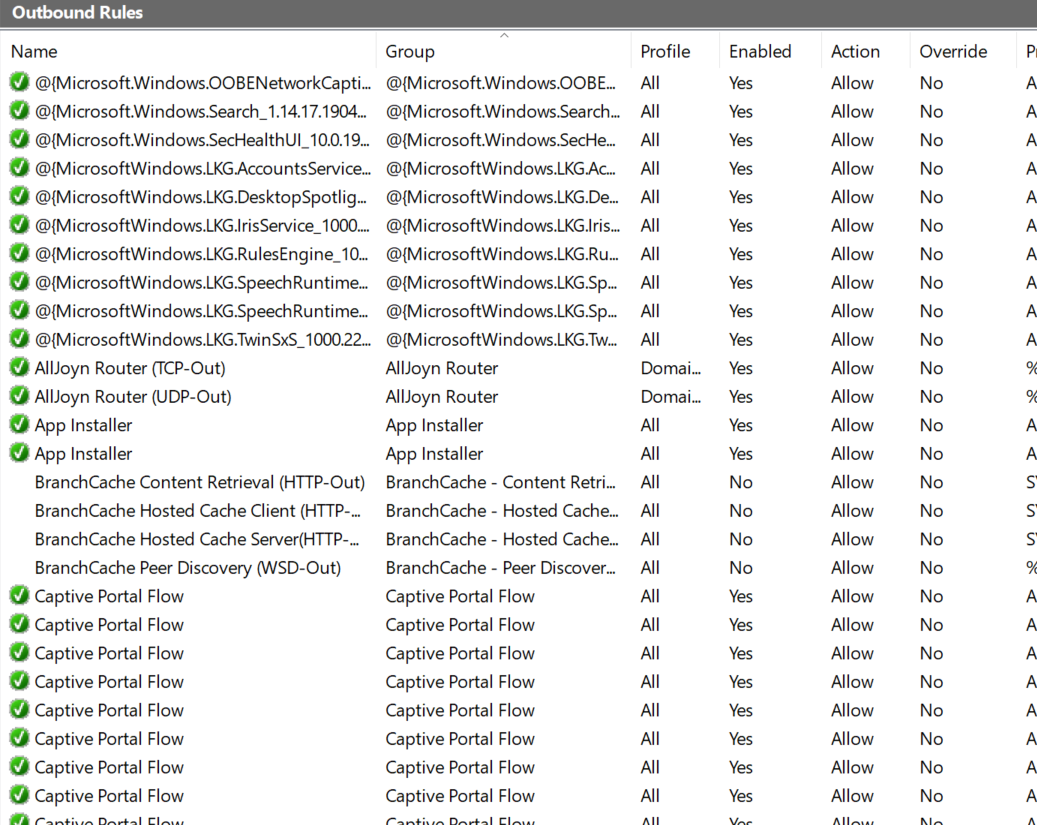
**Deliverables:** Screenshot/configuration file showing firewall rules applied

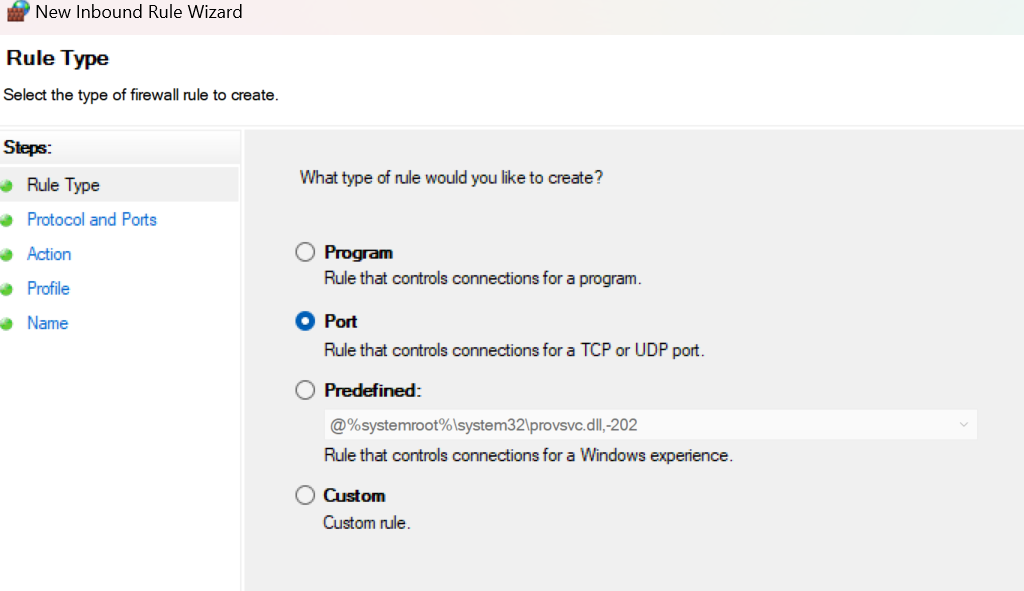
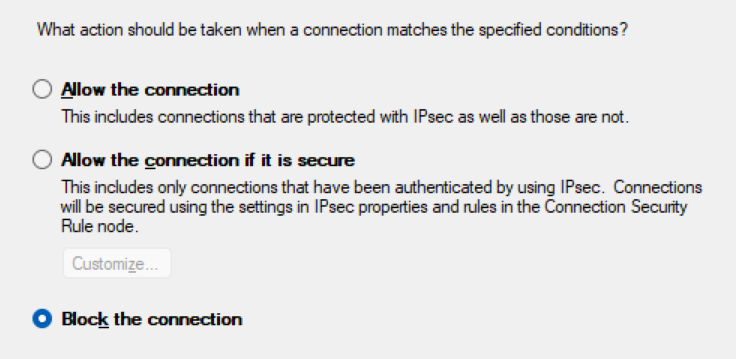
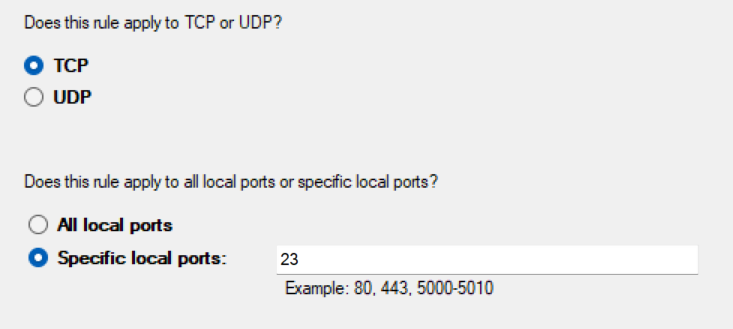
1. **Open firewall configuration tool (Windows Firewall or terminal for UFW).**

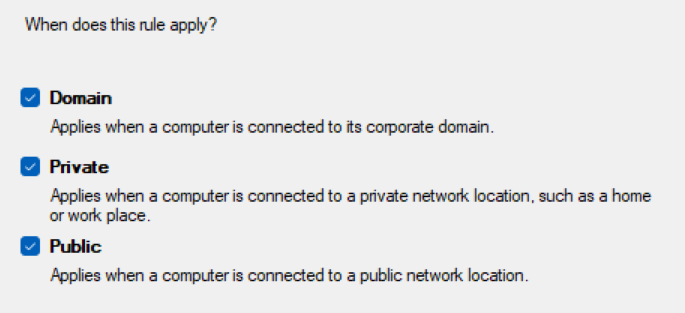
****

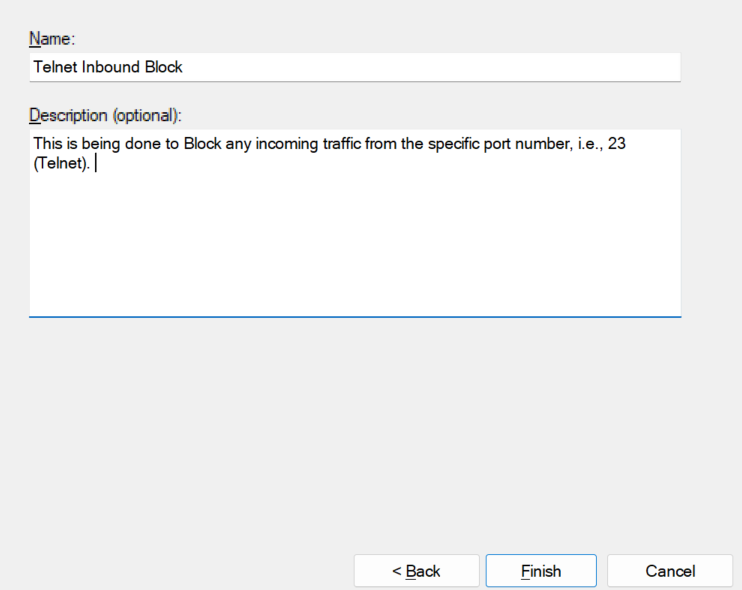
1. **List current firewall rules.**

****

****

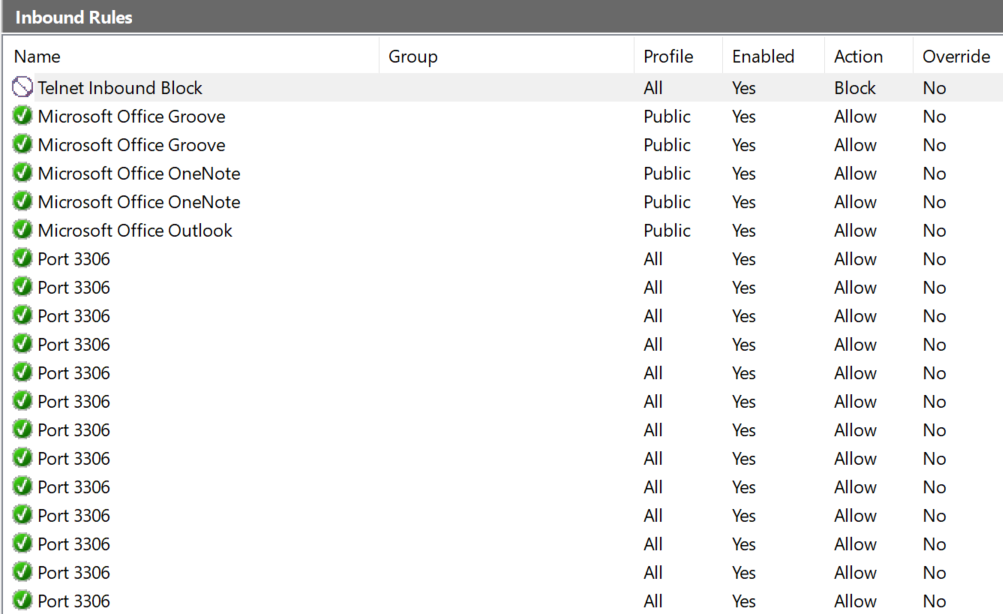
1. **Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).**

****

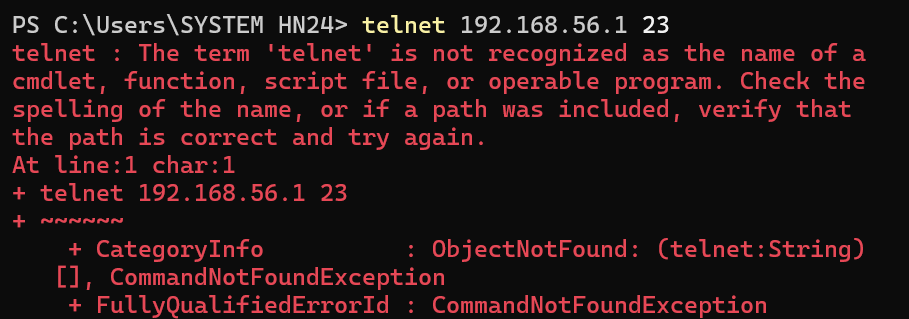
****

and click *FINISH* in the end to finally apply it.

In the below screenshot, we can see that a new rule named- **“Telnet Inbound Block”** has been added with **action** as **“Block”** which ensures no incoming traffic from port number- **23** enters our Network System.



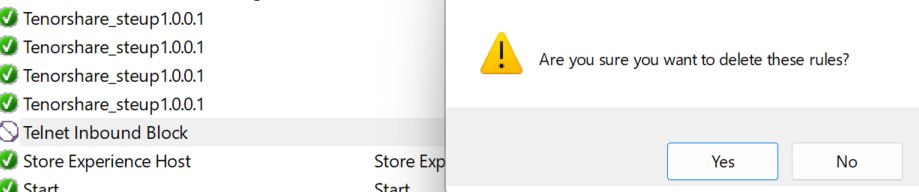
1. **Test the rule by attempting to connect to that port locally or remotely.**

****

1. **Add rule to allow SSH (port 22) if on Linux.**

Not applicable (Using Windows Operating System).

1. **Remove the test block rule to restore original state.**

****

1. **Document commands or GUI steps used.**

**GUI steps used:-**

Windows Defender Firewall with Advanced Security> Inbound Rules> New Rule…> Rule Type> Protocol and Ports (Port selection eg. 23) > Action (Block the Connection)> Profile (Domain/ Private/ Public) > Name>

**Commands used-**

Used command- **telnet <ip address> 23** to check if port is working or not.  
If it is working then shows blank, otherwise shows NotFound.

1. **Summarize how firewall filters traffic.**

It examines the data packets and compares them against predefined security rules.  
  
There are various security rules such as:  
1. source and destination IP addresses,

2. port number,

3. protocol,

4. Type of Network our computer system is using,

5. Action (if it allows or blocks)

Based on the match, the firewall decides whether to allow the packet to pass through, or to block or discard it.