

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

Steps on Windows (Windows Defender Firewall)

- 1 Open Firewall Configuration Tool: Press Win + R → type wf.msc → press Enter.
- 2 List Current Rules: In the left pane, click Inbound Rules to view existing rules.
- 3 Add Rule to Block Port 23 (Telnet): Right-click Inbound Rules → New Rule → Port → 23 → Block the connection → Apply.
- 4 Test the Rule: Try 'telnet localhost 23' (if Telnet client installed). It should fail.
- 5 Add Rule to Allow SSH (Port 22): New Rule → Port → 22 → Allow connection.
- 6 Remove Test Block Rule: Right-click the Block Telnet rule and delete.

Take Screenshot:

1.Capture the firewall rules showing Block Telnet

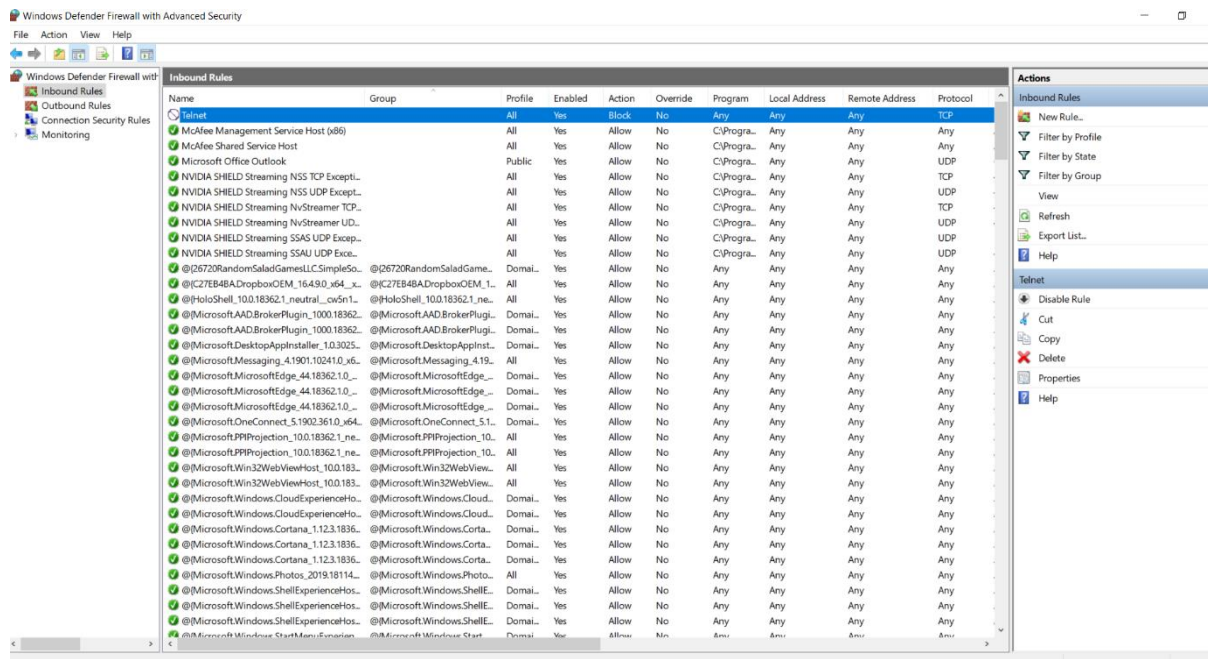


Figure 1 Telnet Block Screenshot

2.Capture the firewall rules showing Allow SSH

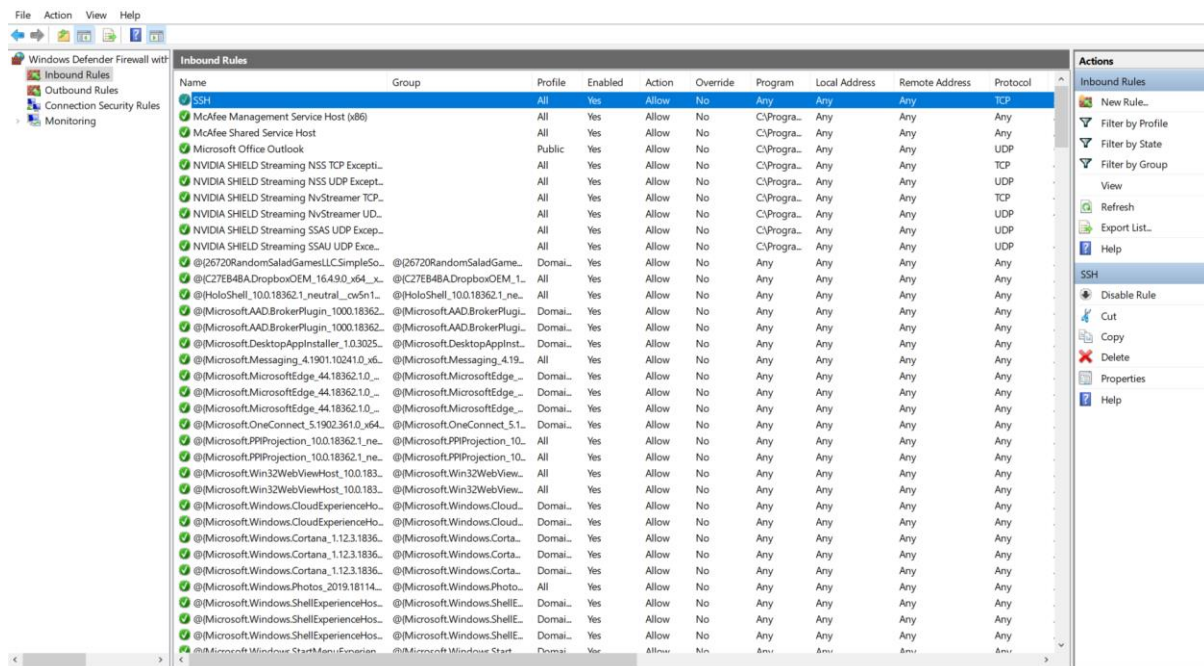


Figure 2 SSH ALLOW Screenshot

Summary:

- Firewalls filter network traffic based on defined rules (port, protocol, IP).
- Allow rules explicitly permit traffic; Deny/Block rules reject or drop traffic.
- Blocking Telnet (23) prevents insecure access while allowing SSH (22) enables secure remote login.
- This exercise provides basic firewall management skills and traffic filtering understanding.

Outcome:

Basic firewall management skills were practiced by blocking and allow ports, verifying rules, and restoring settings.