**Intern Name:** Swapnil Dixit  
**Date:** 26/09/2025  
**Tool Used:** Windows Defender Firewall (on Windows)

**🎯 Objective**

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

**🖥️ Environment Details**

| **Parameter** | **Value** |
| --- | --- |
| Operating System | Windows 10 |
| Scanner Tool | Windows Defender Firewall |

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

**A screenshot of a computer

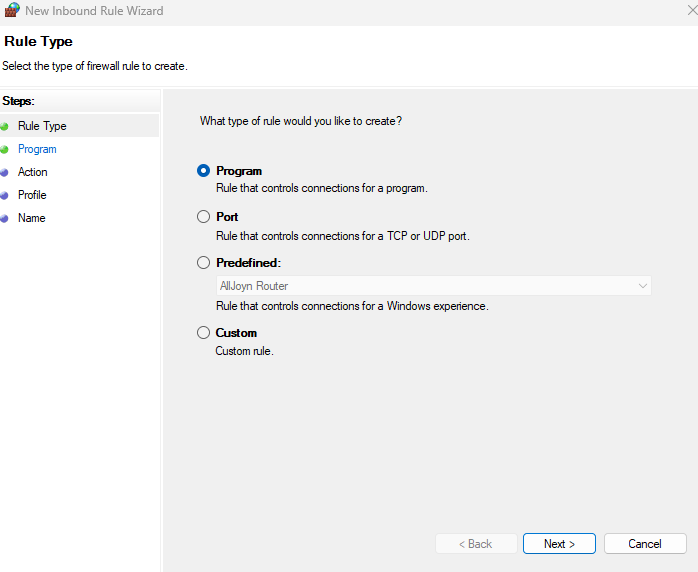
AI-generated content may be incorrect.**

**2.List current firewall rules.**

**A screenshot of a computer

AI-generated content may be incorrect.**

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

****

**A screenshot of a computer

AI-generated content may be incorrect.**

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

While testing Telnet – I got to know my windows are not having Telent installed.  
A screenshot of a computer

AI-generated content may be incorrect.  
Enabled it from windows features and installed.

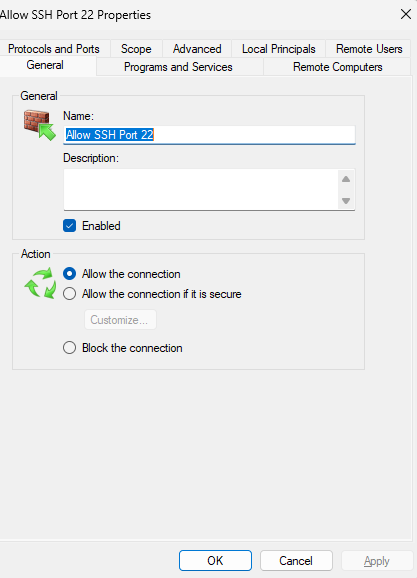
A screenshot of a computer

AI-generated content may be incorrect.

**5.Add rule to allow SSH (port 22).**

**A screenshot of a computer

AI-generated content may be incorrect.**

****

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

**A blue line on a white background

AI-generated content may be incorrect.**

**8.Summarize how firewall filters traffic.**

A firewall filters network traffic based on defined rules that check packet headers, connection states, IP addresses, ports, and protocols. It ensures only authorized traffic passes through while blocking harmful or unauthorized traffic to protect the network from threats like intrusions, malware, and denial-of-service (DoS) attacks. As we saw different filters like Inbound rules, outbound rules. The firewall inspects the **header** information of each packet (e.g., source IP, destination IP, protocol, source and destination ports), then it compares the rules.

**✅ Conclusion**

With the increasing sophistication of cyber threats, firewalls—whether packet-filtering, stateful, or next-gen—serve as a critical line of defense in maintaining the integrity, confidentiality, and availability of a network. Properly configuring and maintaining firewalls is crucial for safeguarding systems against external and internal attacks, ensuring secure communication, and upholding organizational security policies.