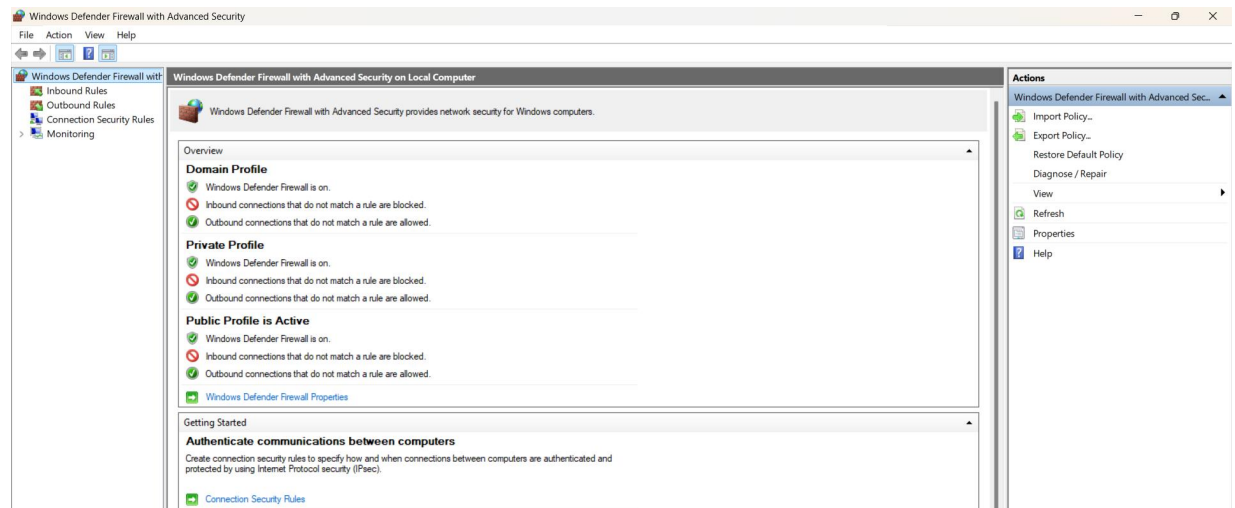


TASK - 4

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

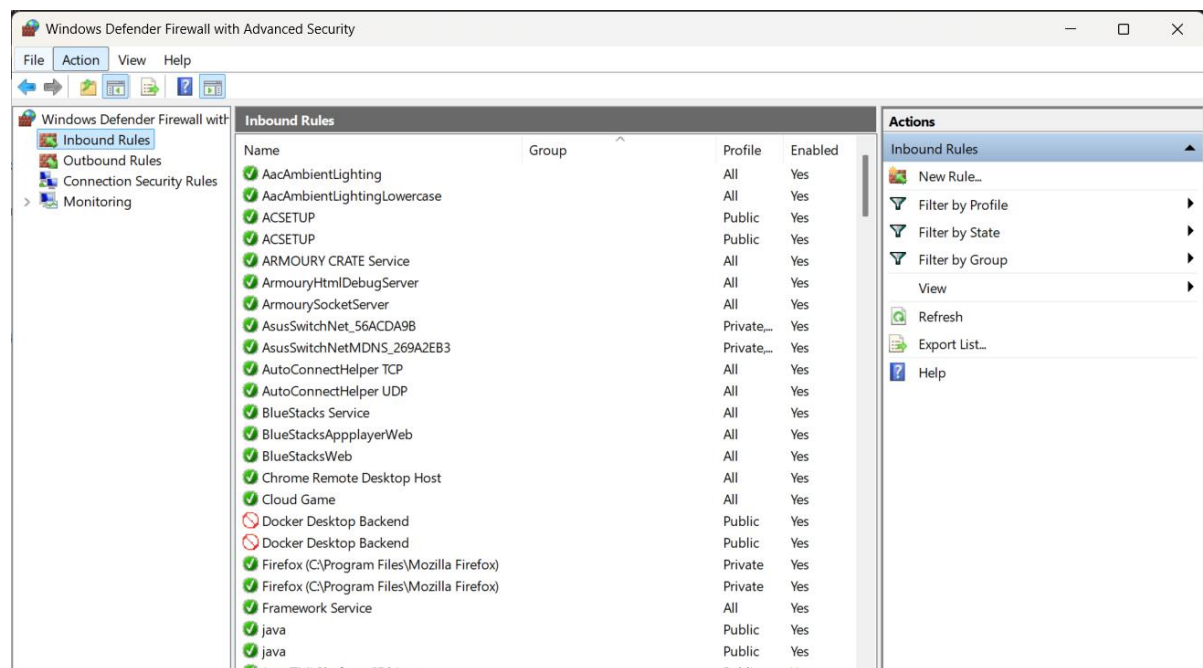
1. Open Firewall Configuration Tool

Access the firewall management interface to begin security configuration. Use Windows Firewall GUI.



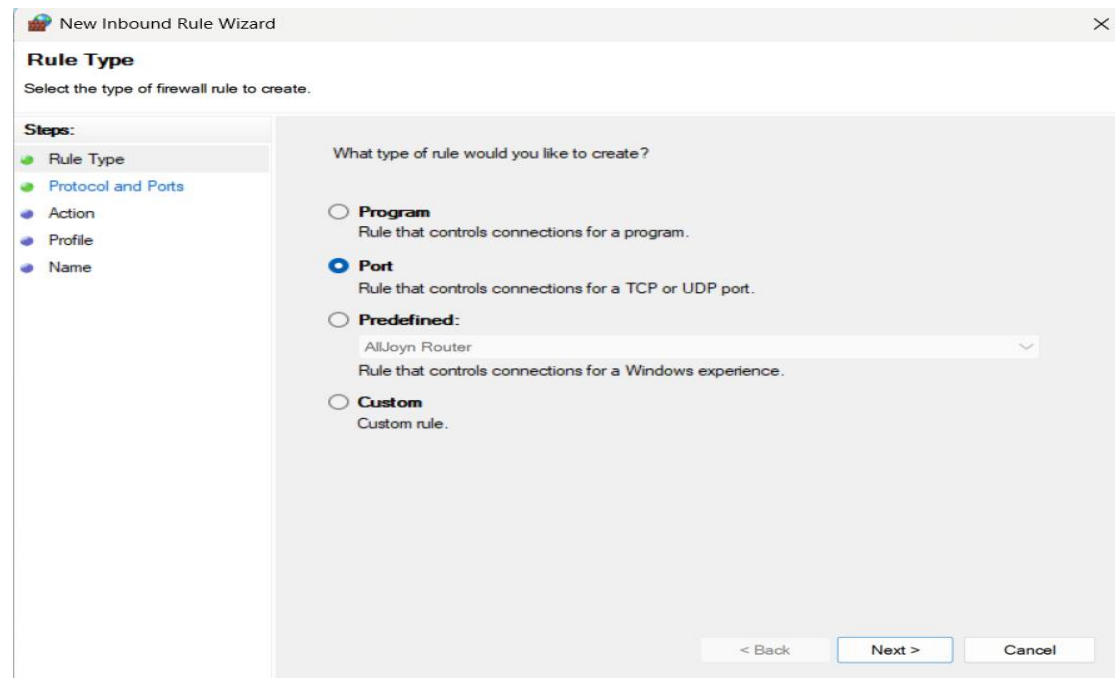
2. List Current Firewall Rules

Display all active firewall rules to understand current traffic permissions. This baseline assessment helps identify existing allowed and blocked services.

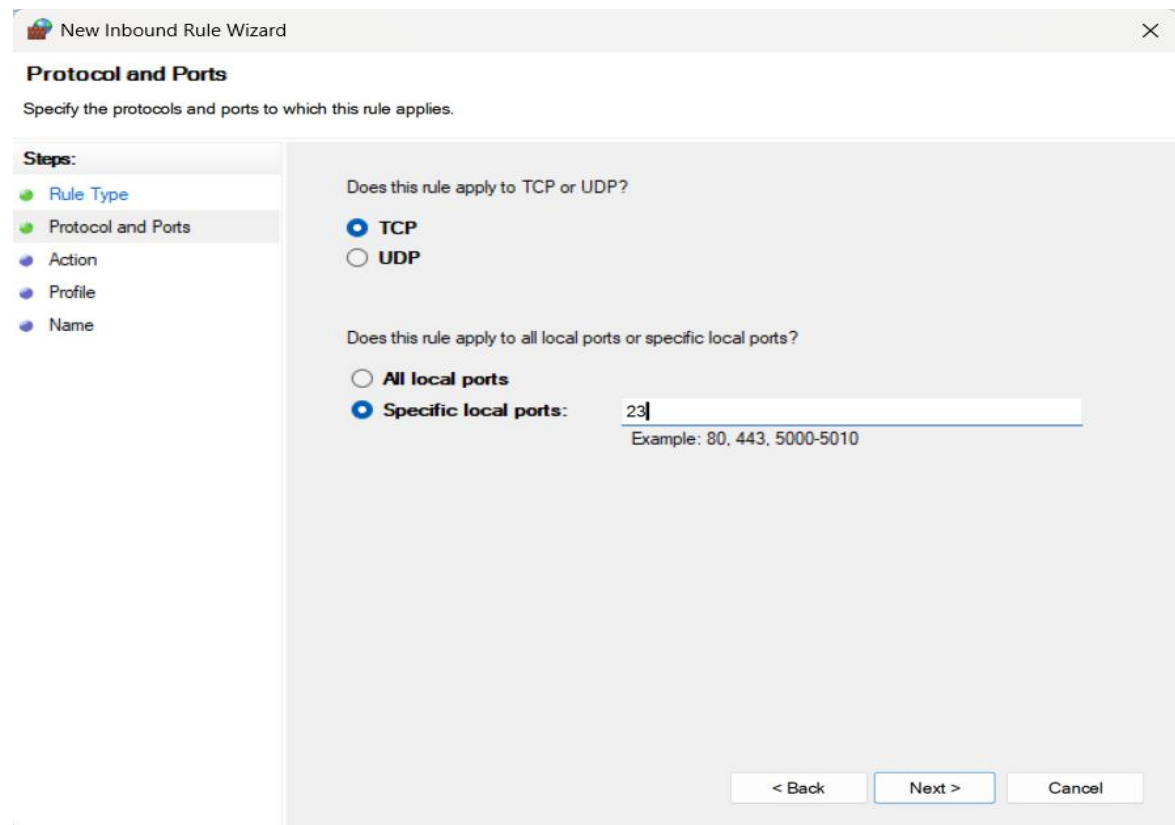


3. Add Rule to Block Telnet (Port 23)

Create a new inbound rule explicitly blocking TCP port 23 to prevent Telnet access. This enhances security by closing an unused network service port.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Rule Type' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps:' pane lists 'Rule Type' (selected), 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?' with four radio button options: 'Program' (Rule that controls connections for a program.), 'Port' (selected, Rule that controls connections for a TCP or UDP port.), 'Predefined:' (with a dropdown menu showing 'AllJoyn Router' and the description 'Rule that controls connections for a Windows experience.'), and 'Custom' (Custom rule.). At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports' (selected), 'Action', 'Profile', and 'Name'. The main area has two questions. The first is 'Does this rule apply to TCP or UDP?' with radio button options for 'TCP' (selected) and 'UDP'. The second is 'Does this rule apply to all local ports or specific local ports?' with radio button options for 'All local ports' and 'Specific local ports:' (selected). Below 'Specific local ports:' is a text input field containing '23' and a hint 'Example: 80, 443, 5000-5010'. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☒ **Block the connection**

< Back

Next >

Cancel

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

< Back

Next >

Cancel

4. Test the Block Rule


Verify the blocking rule's effectiveness by attempting Telnet connections to the secured port. Confirm connection failures to validate proper firewall functionality.

Port Checker

Free DNSEmail CheckerShow My IPPort Scanner

Port Checker

Check for open ports and verify port forwarding setup on your router.



Smooth-sailing through 20+ apps. [Learn more](#) **Adobe Creative Cloud Pro**

Your IP Address

Port Number

Port 23 is *closed*.

Summary of How the firewall filters traffic:

Firewalls act as security guards for computer networks by monitoring and controlling incoming and outgoing traffic. They examine data packets based on predefined rules to determine whether to allow or block communication.

Key Filtering Methods:

Packet Inspection: Analyzes source/destination IP addresses, port numbers, and protocols

Rule-Based Filtering: Follows configured rules in sequence (allow/deny specific services)

Stateful Tracking: Remembers active connections and only allows legitimate response traffic

Default Security: Typically blocks all traffic by default, only permitting explicitly allowed services