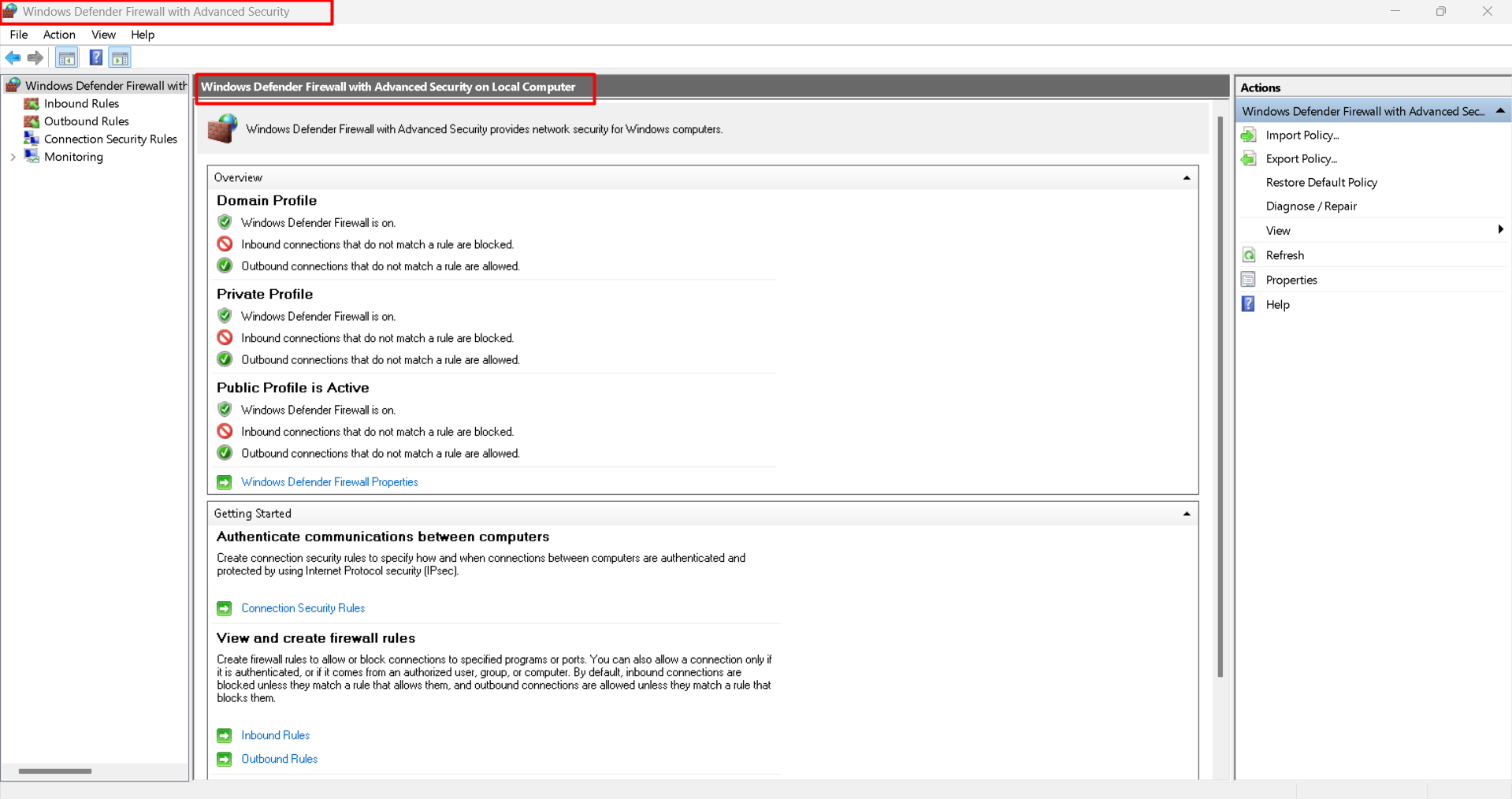
# Windows Firewall Configuration - Step by Step

## 1. Open Firewall Configuration Tool

GUI:

1. Press Win + R → type wf.msc → press Enter.

2. The Windows Defender Firewall with Advanced Security window will open.



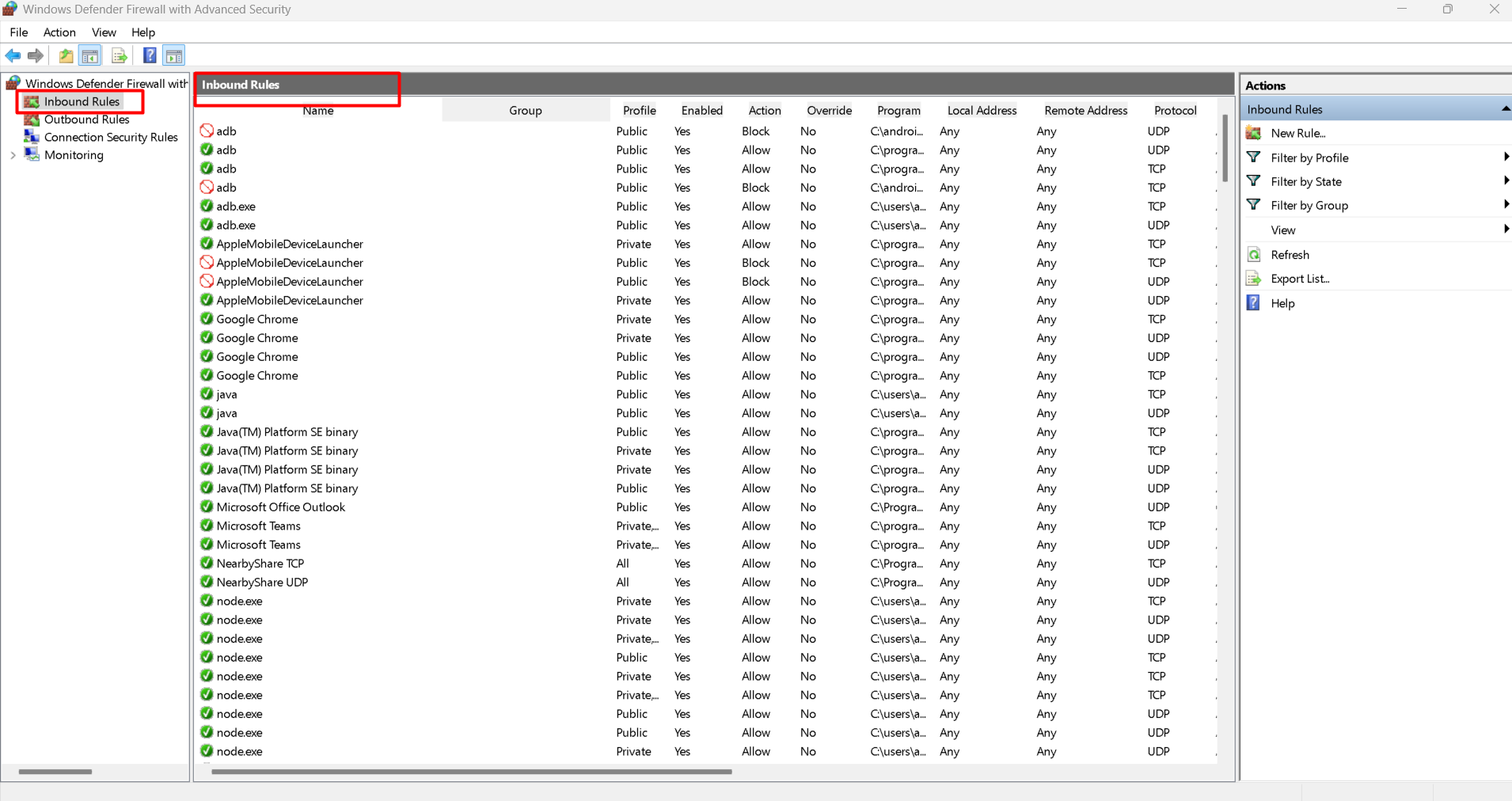
PowerShell:

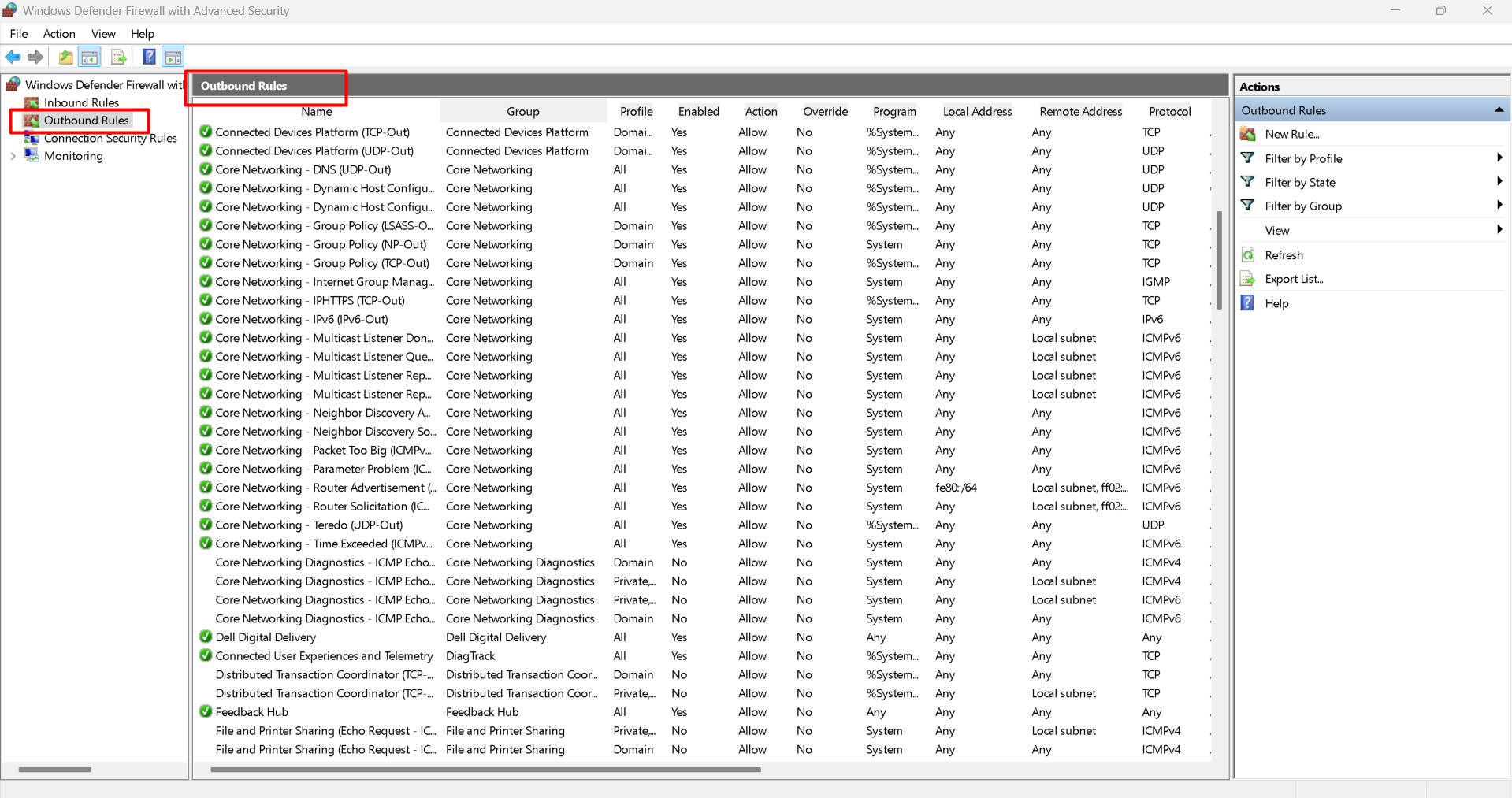
Run: Get-NetFirewallRule

## 2. List Current Firewall Rules

GUI:

In Windows Defender Firewall with Advanced Security, click Inbound Rules or Outbound Rules to view the configured rules.





PowerShell:

Get-NetFirewallRule | Format-Table Name, DisplayName, Enabled, Direction, Action

## 3. Add a Rule to Block Inbound Traffic on Port 23 (Telnet)

GUI:

1. Go to Inbound Rules → New Rule (right-hand side).

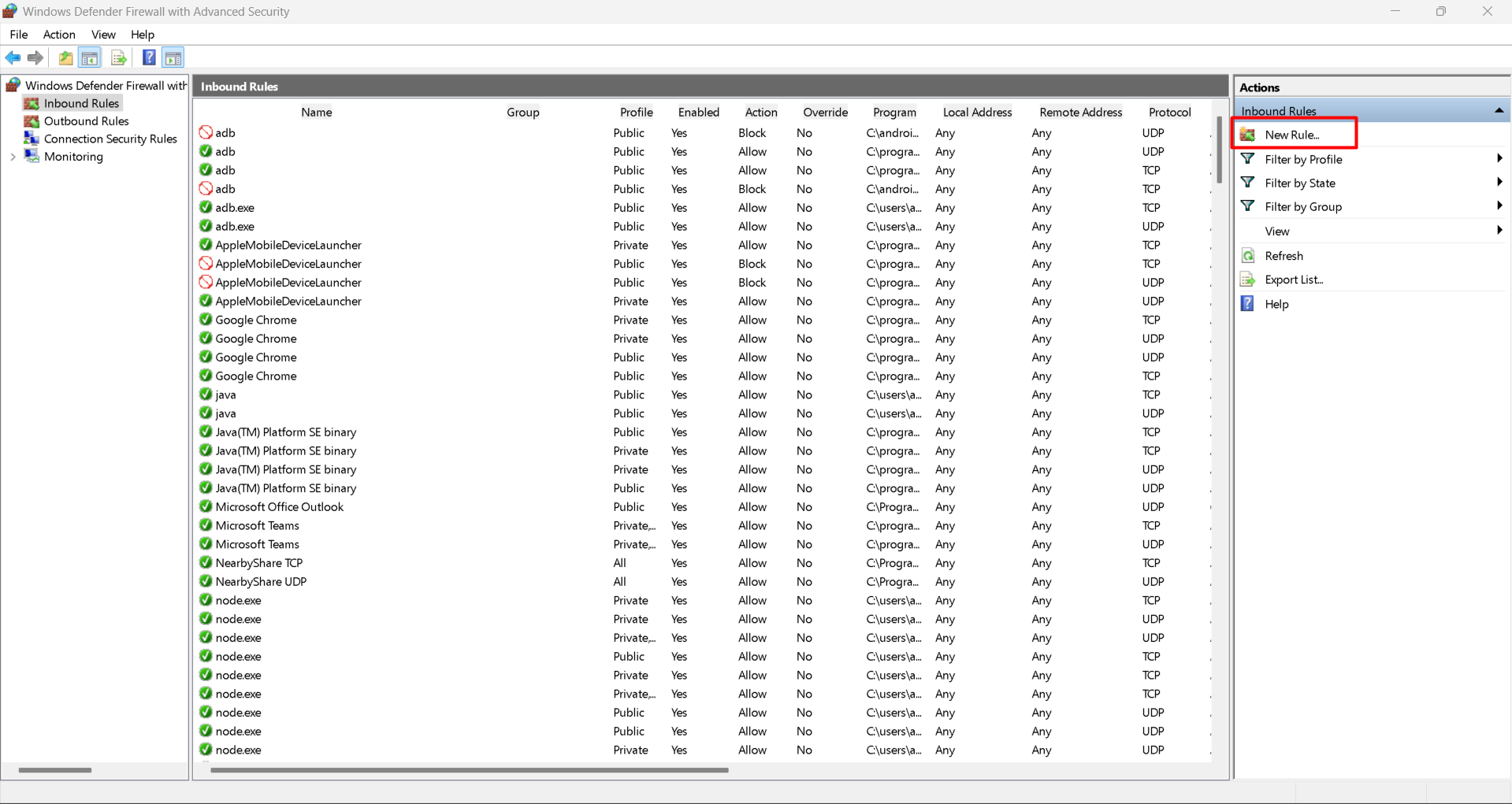
2. Select Port → Click Next.

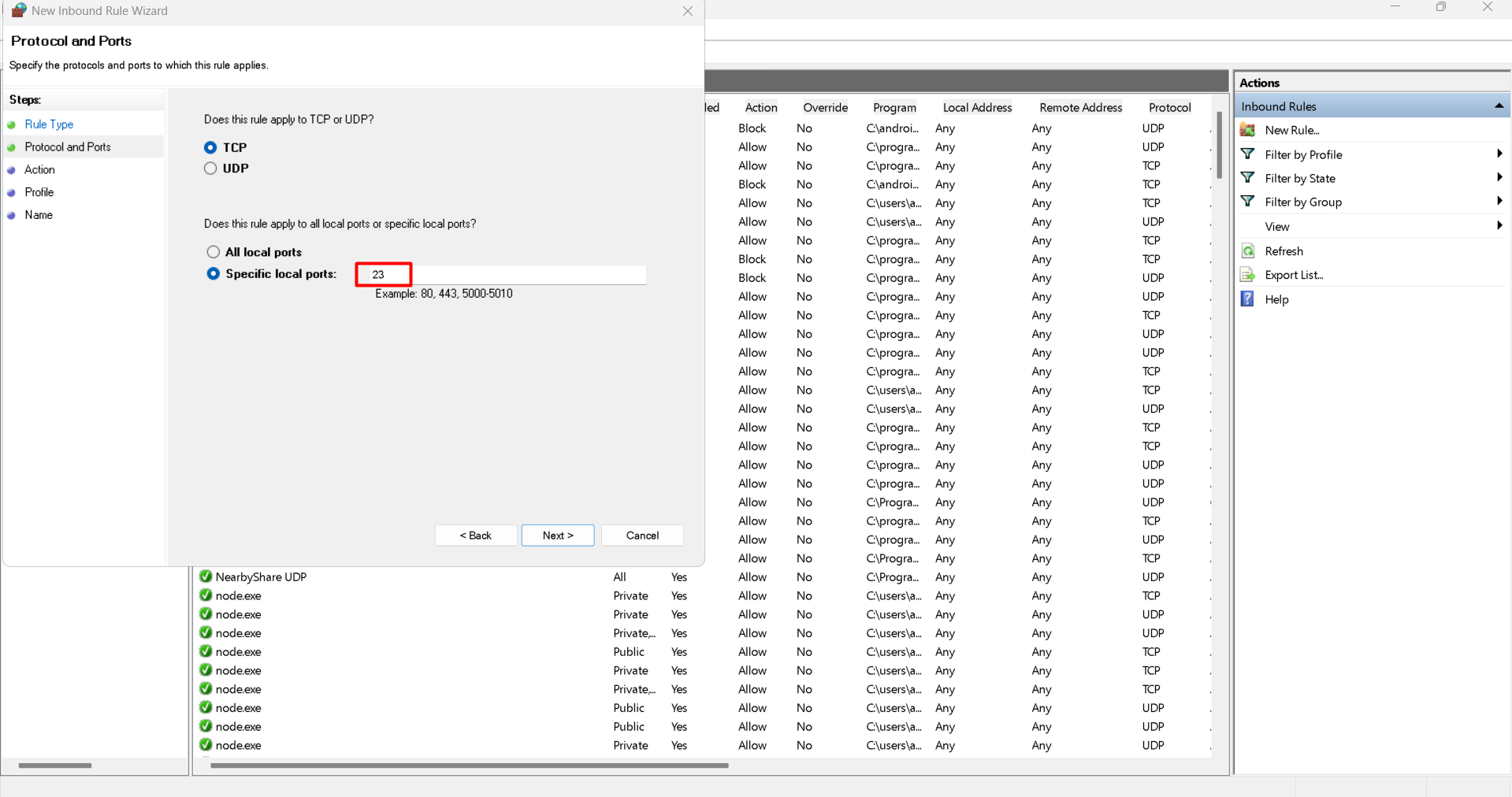
3. Choose TCP and enter 23 in the Specific local ports field → Click Next.

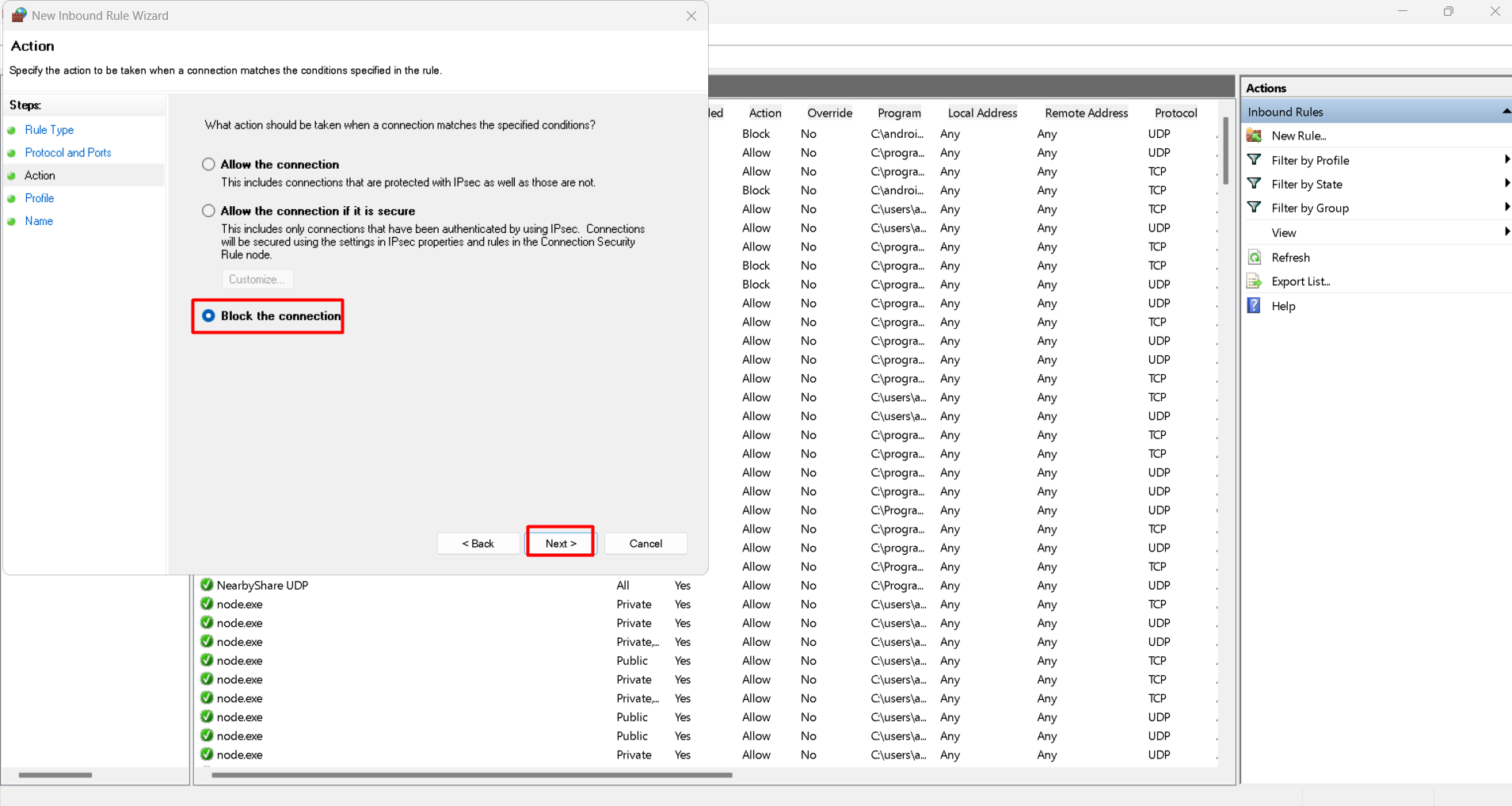
4. Select Block the connection → Click Next.

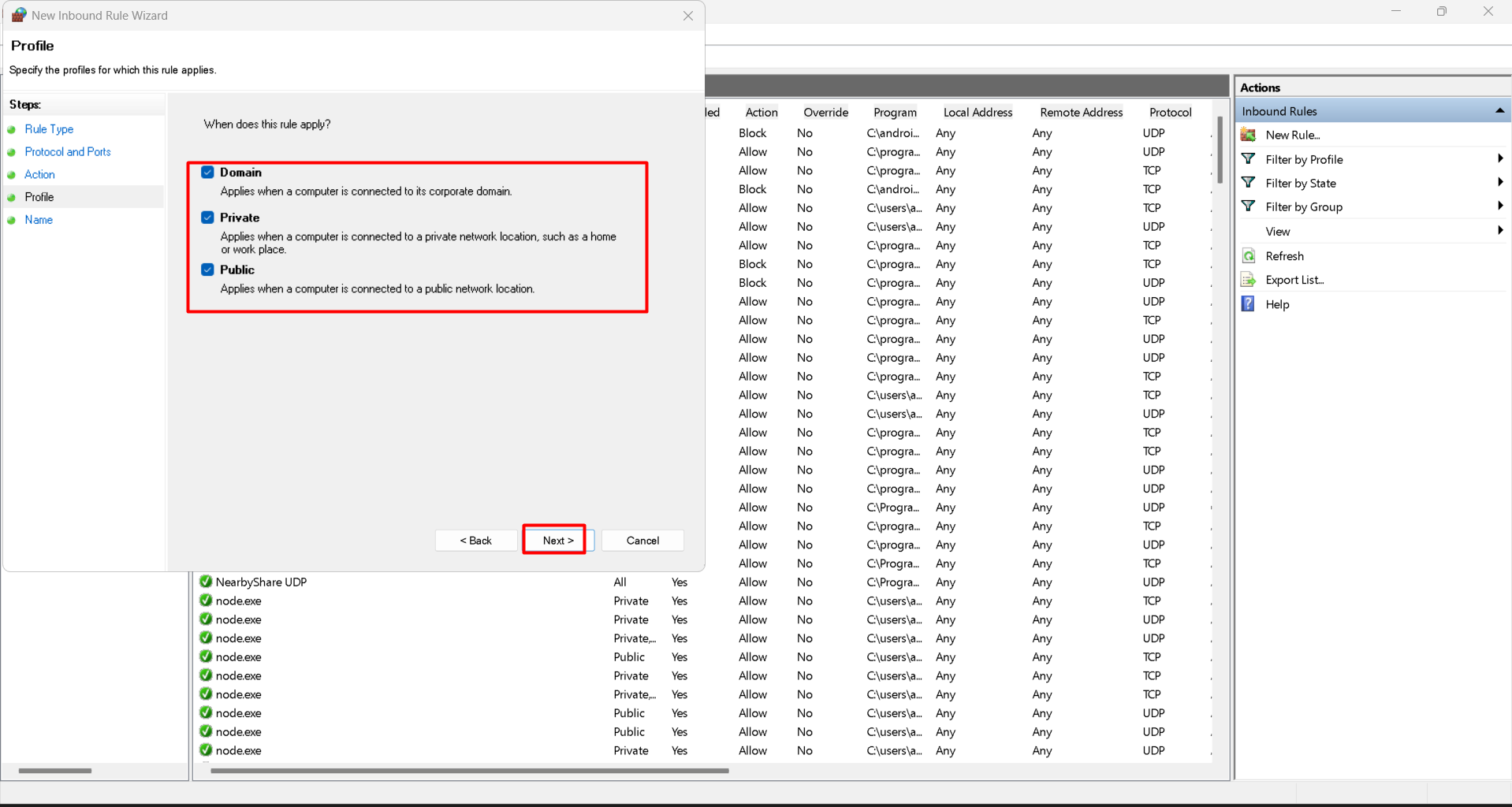
5. Apply to Domain, Private, and Public profiles → Click Next.

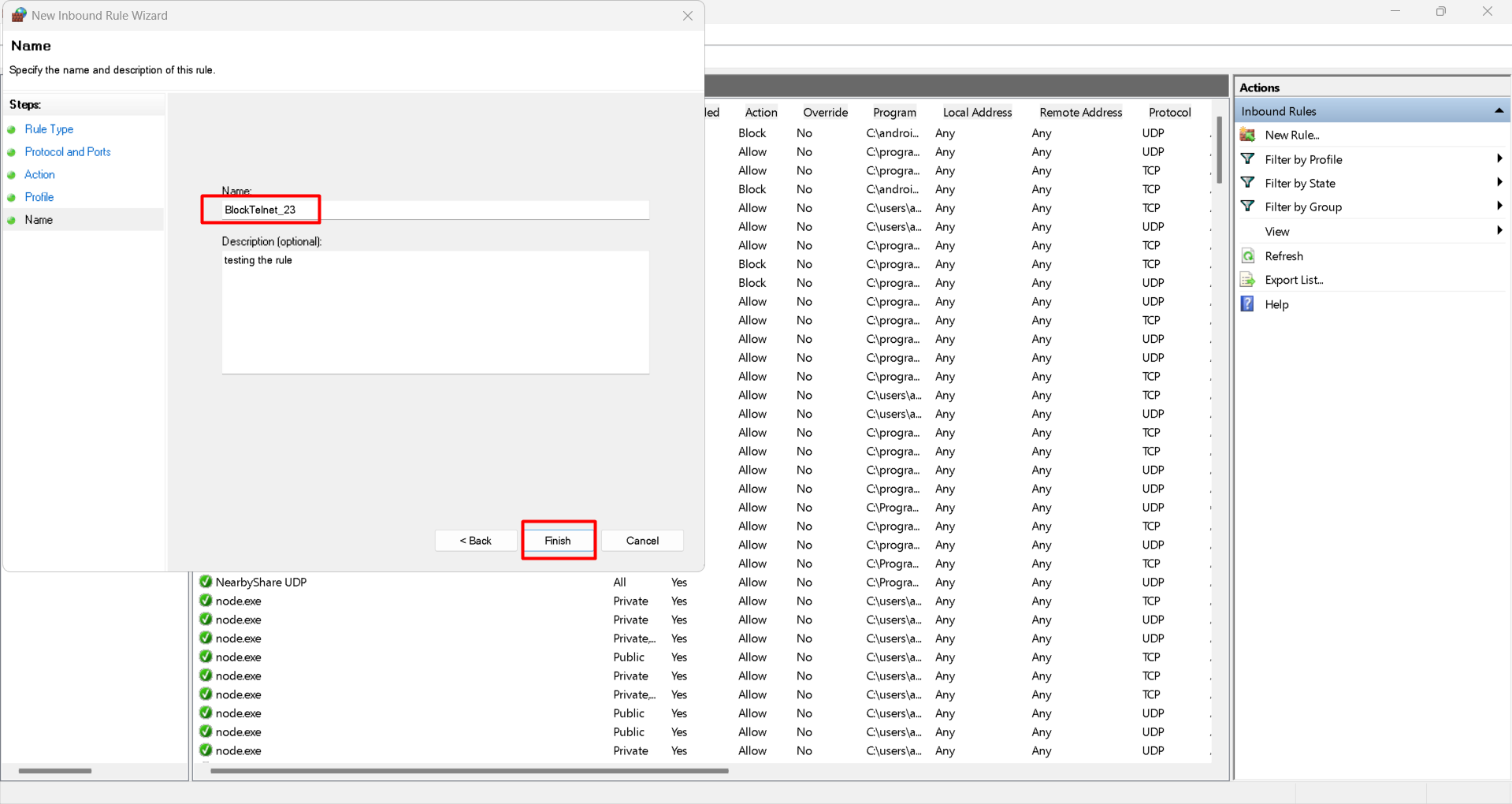
6. Name the rule Block Telnet 23 → Click Finish.











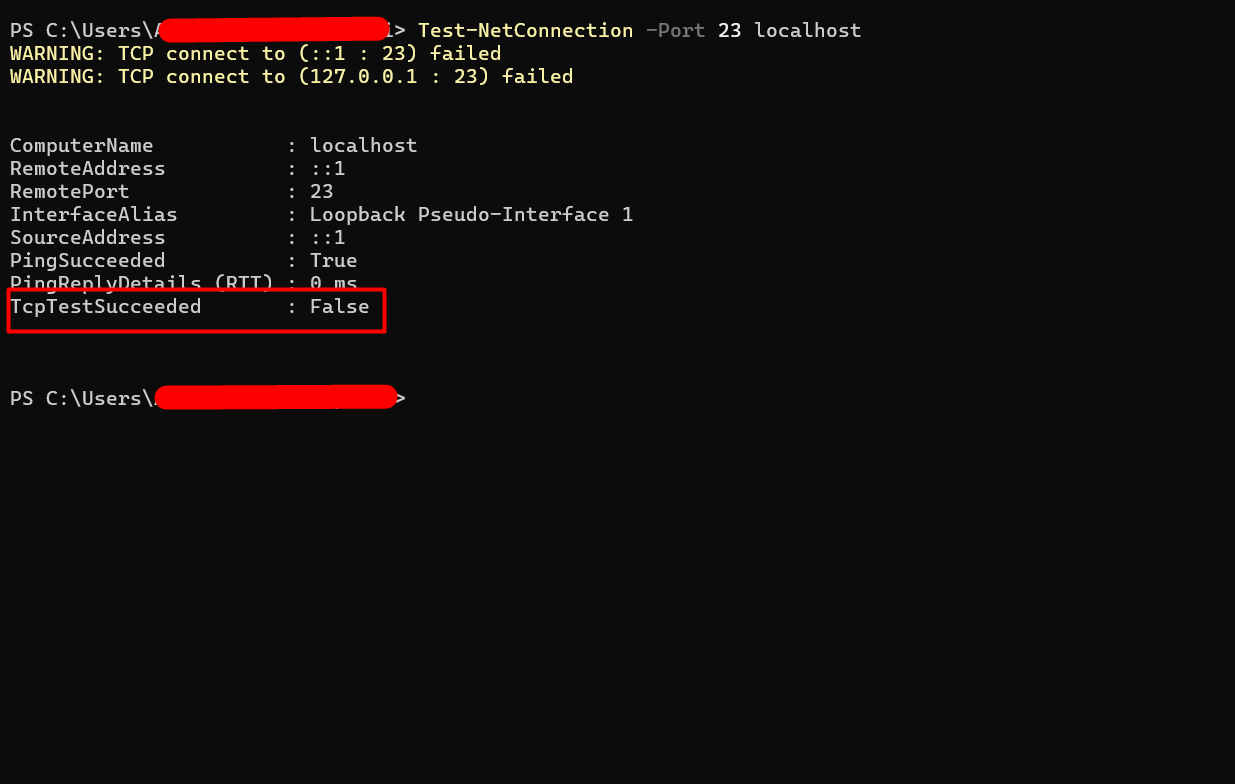
PowerShell:

New-NetFirewallRule -DisplayName "Block Telnet 23" -Direction Inbound -LocalPort 23 -Protocol TCP -Action Block

## 4. Test the Rule

PowerShell:

Test-NetConnection -Port 23 -ComputerName localhost



The result should show TcpTestSucceeded : False if the rule is working.

## 5. Add Rule to Allow SSH (Port 22)

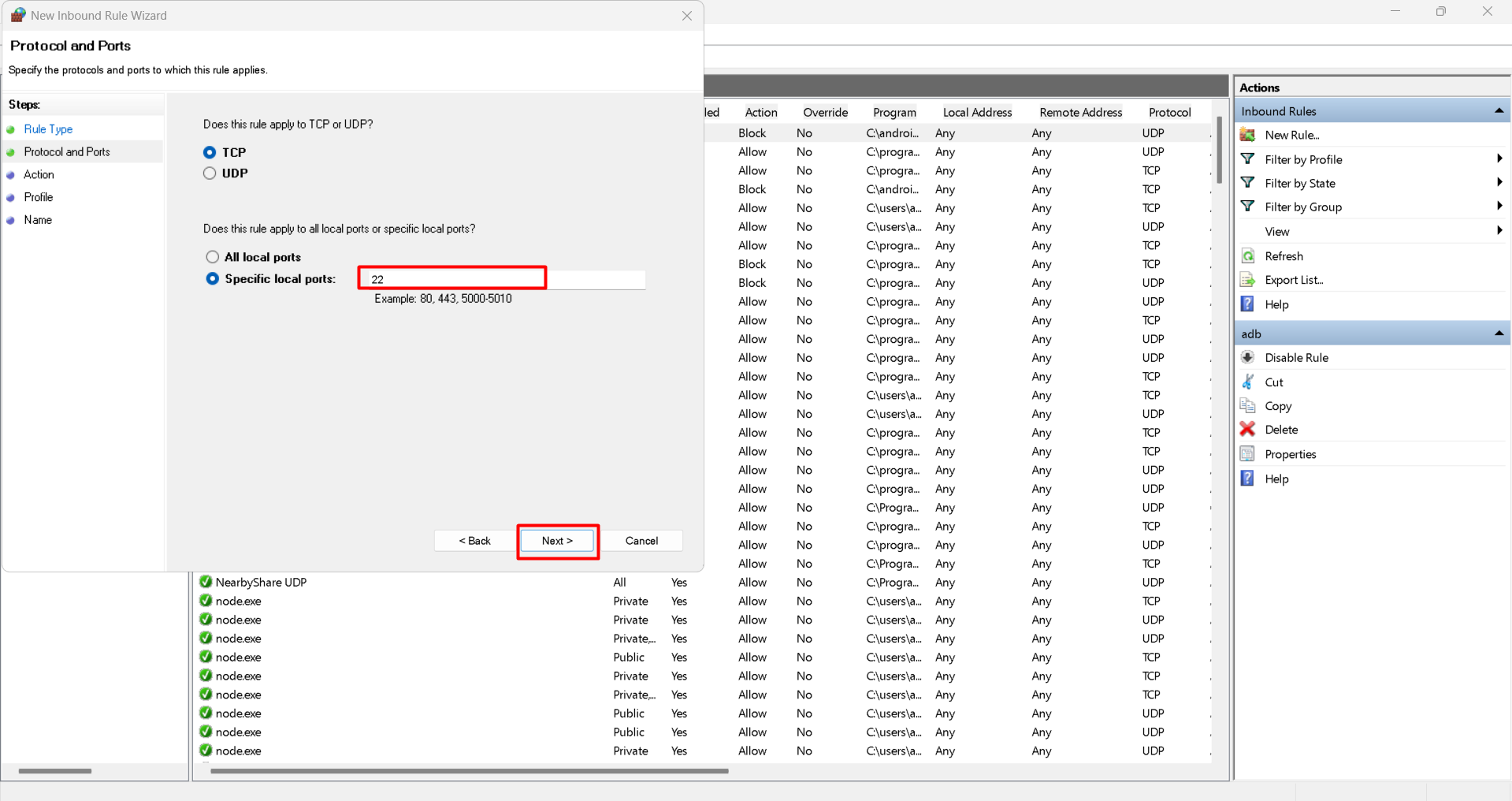
(Only needed if you have OpenSSH server installed on Windows)

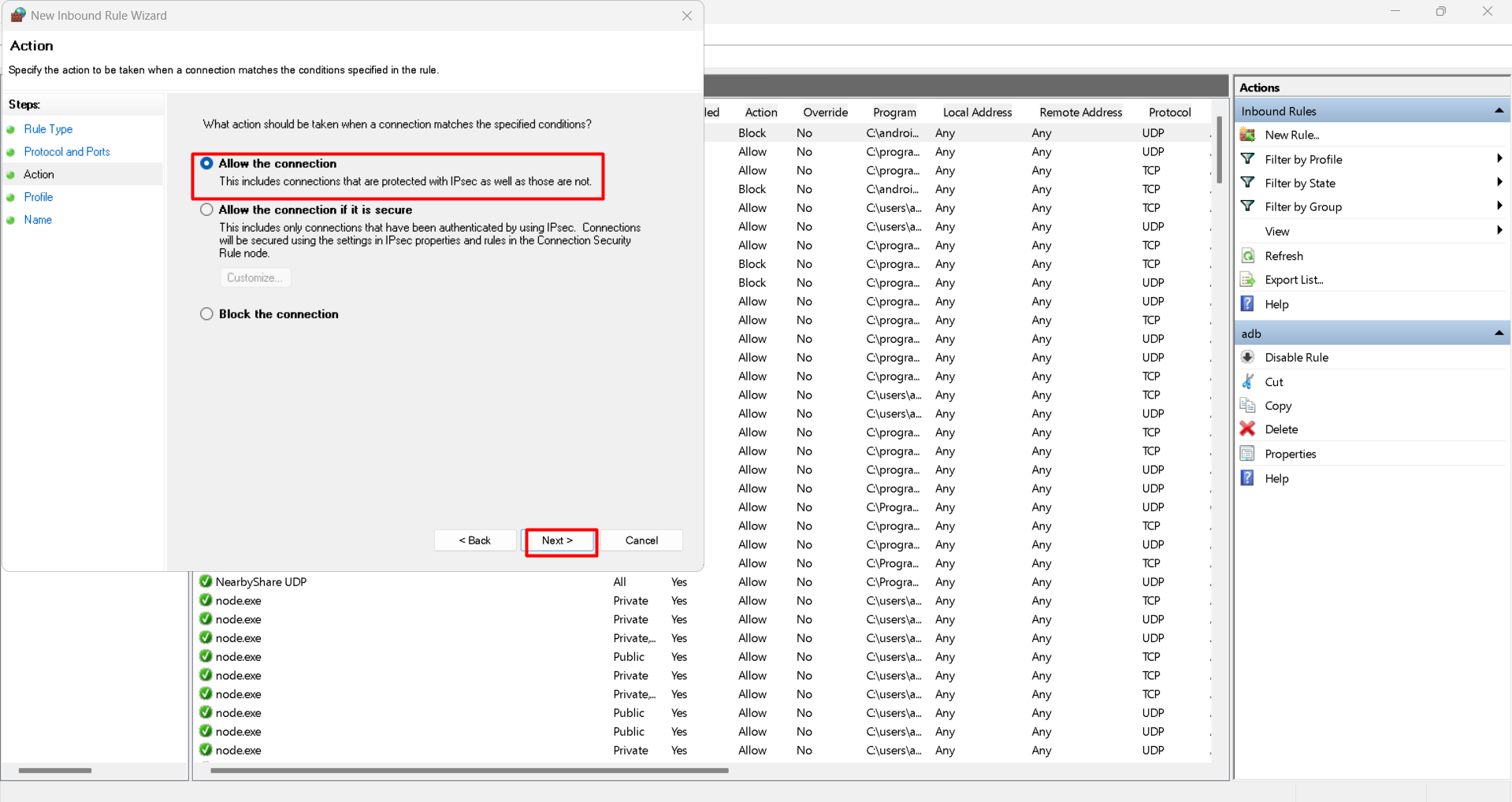
GUI:

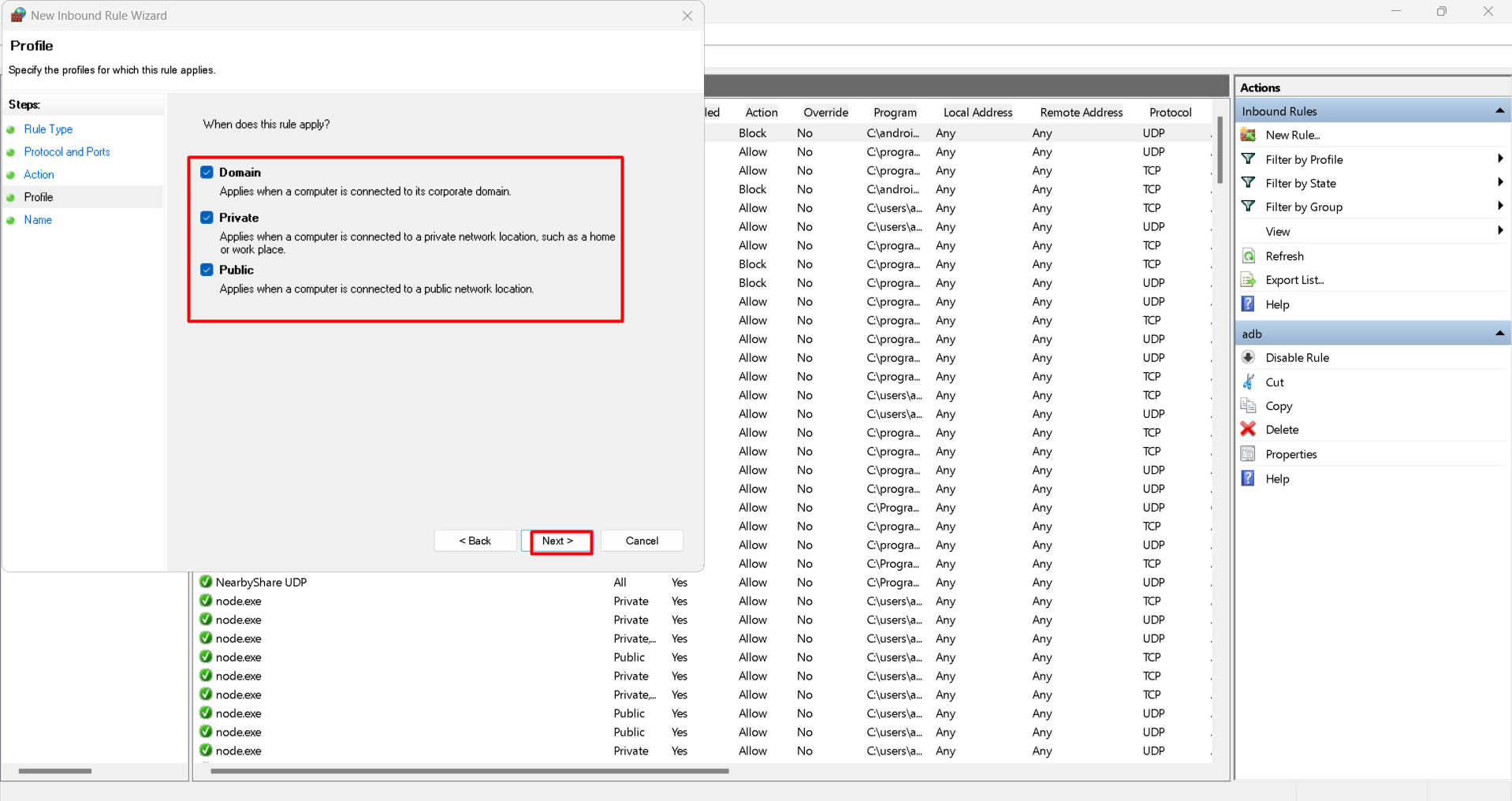
1. Inbound Rules → New Rule.

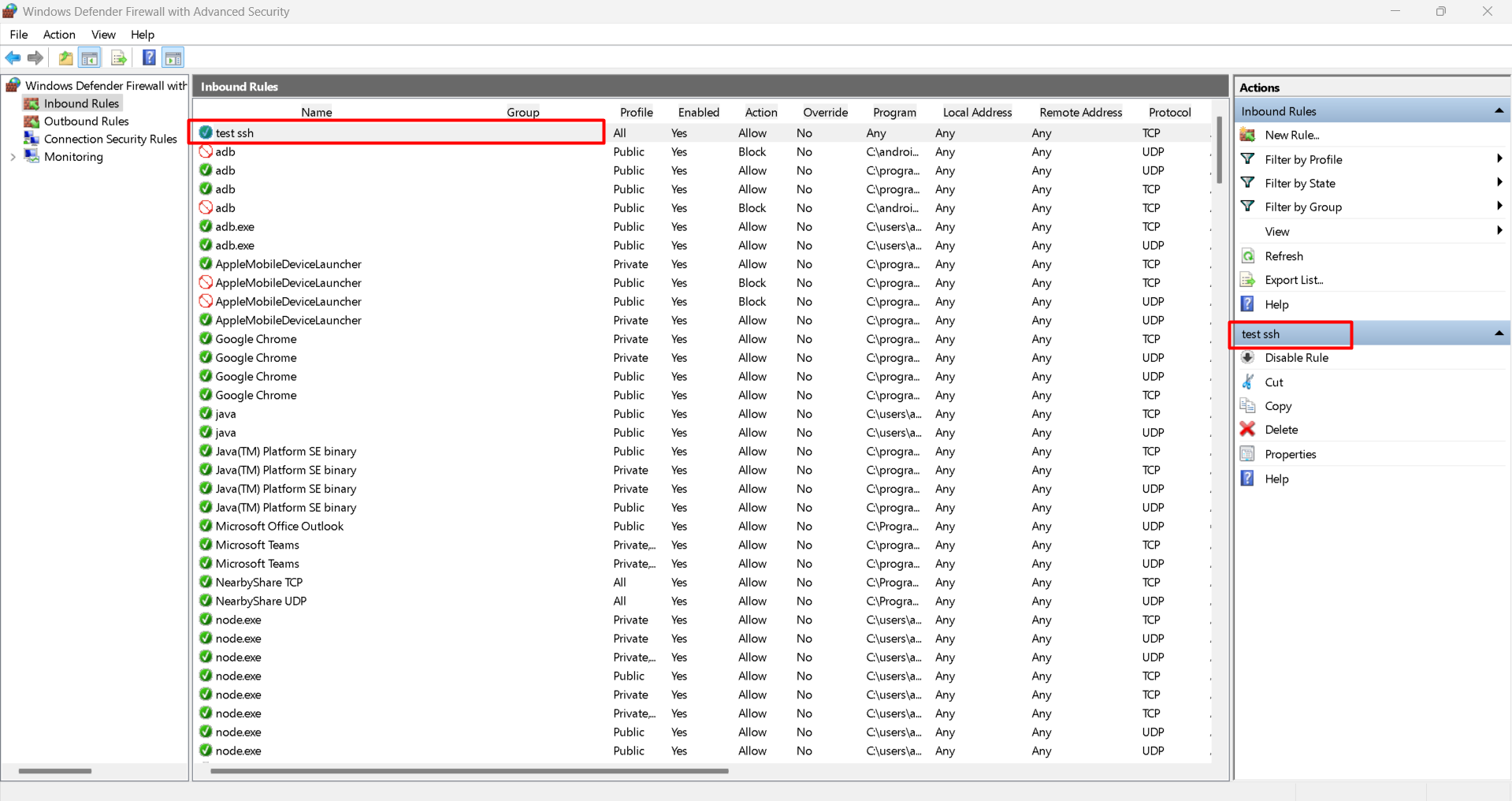
2. Select Port → TCP → enter 22.

3. Select Allow the connection → apply to all profiles → Name it Allow SSH Port 22.

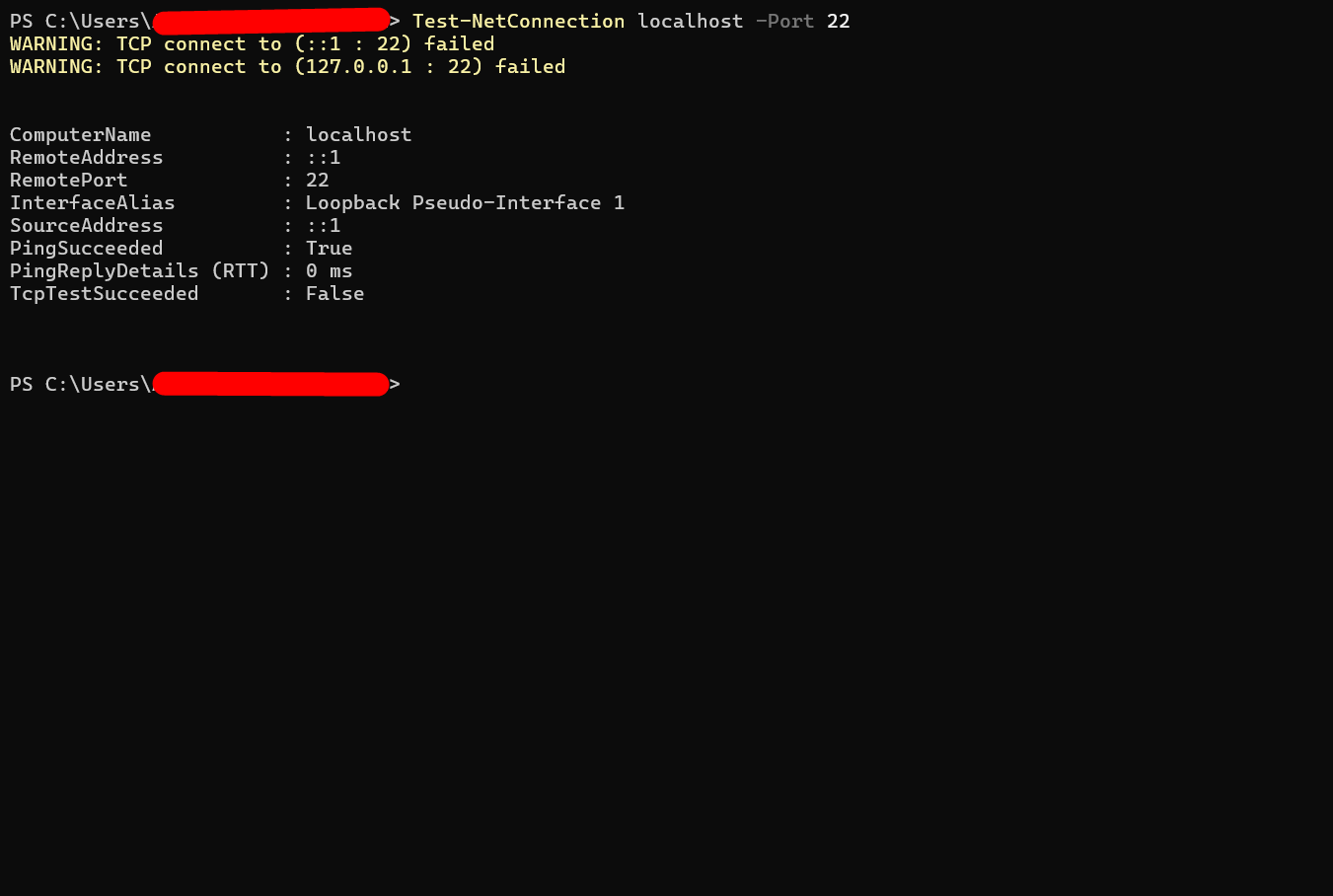








**Test SSH rule**:



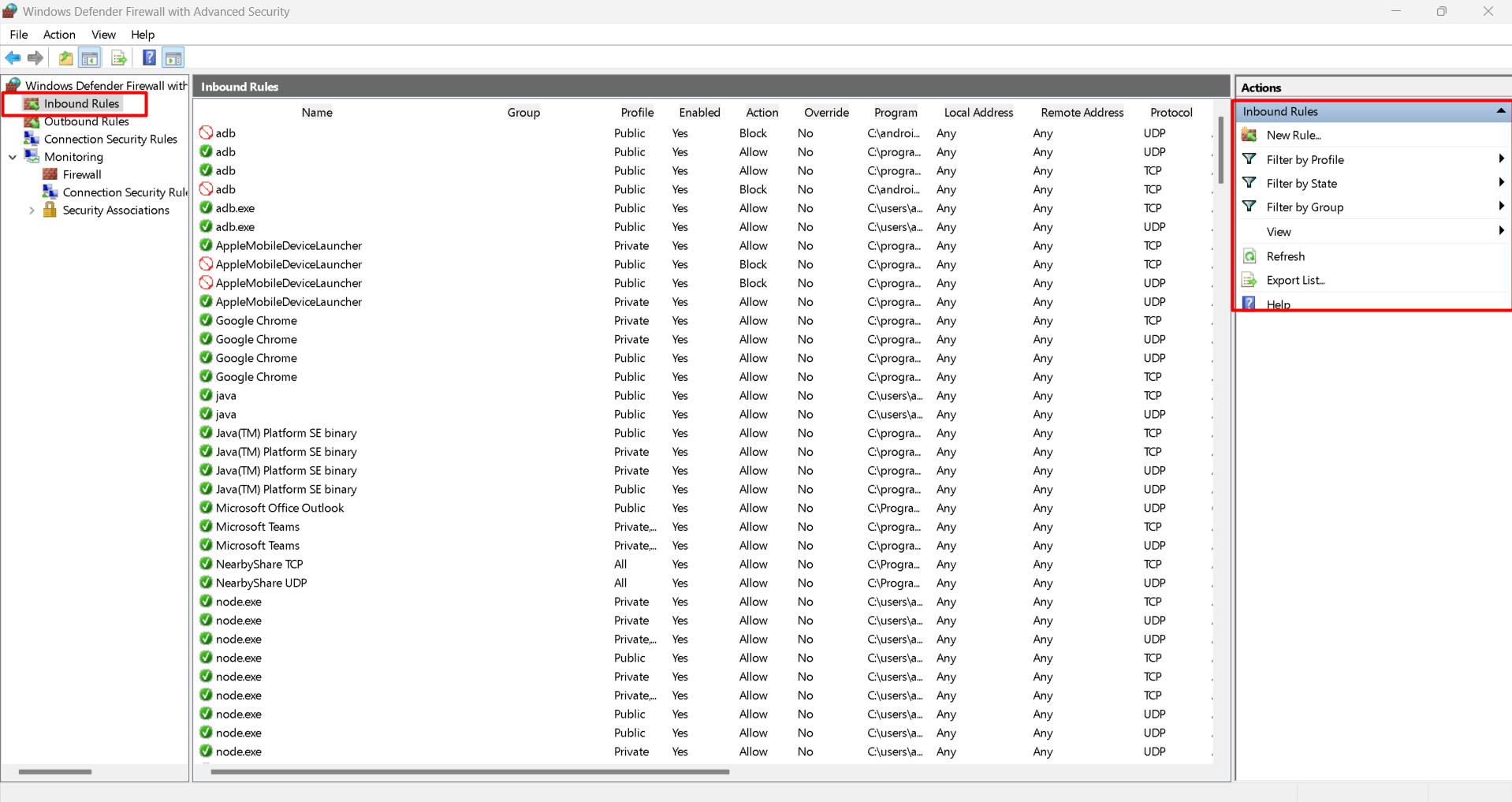
PowerShell:

New-NetFirewallRule -DisplayName "Allow SSH 22" -Direction Inbound -LocalPort 22 -Protocol TCP -Action Allow

## 6. Remove the Test Block Rule

GUI:

In Inbound Rules, find Block Telnet 23 and right-click → Delete.



PowerShell:

Remove-NetFirewallRule -DisplayName "Block Telnet 23"

## 7. Document Commands or GUI Steps Used

Save screenshots of GUI steps (PrtSc key).

Keep a log of commands run in PowerShell.

Example log entry:

2025-08-08 11:00 AM – Added inbound block rule for TCP Port 23

Command: New-NetFirewallRule -DisplayName "Block Telnet 23" -Direction Inbound -LocalPort 23 -Protocol TCP -Action Block

## 8. Summary – How Windows Firewall Filters Traffic

Inbound rules control network connections coming into your PC.

Outbound rules control traffic leaving your PC.

Rules can be based on protocol (TCP, UDP, ICMP), port numbers, application path, or IP addresses.

Windows Firewall checks every network packet against these rules, blocking or allowing based on your configuration.