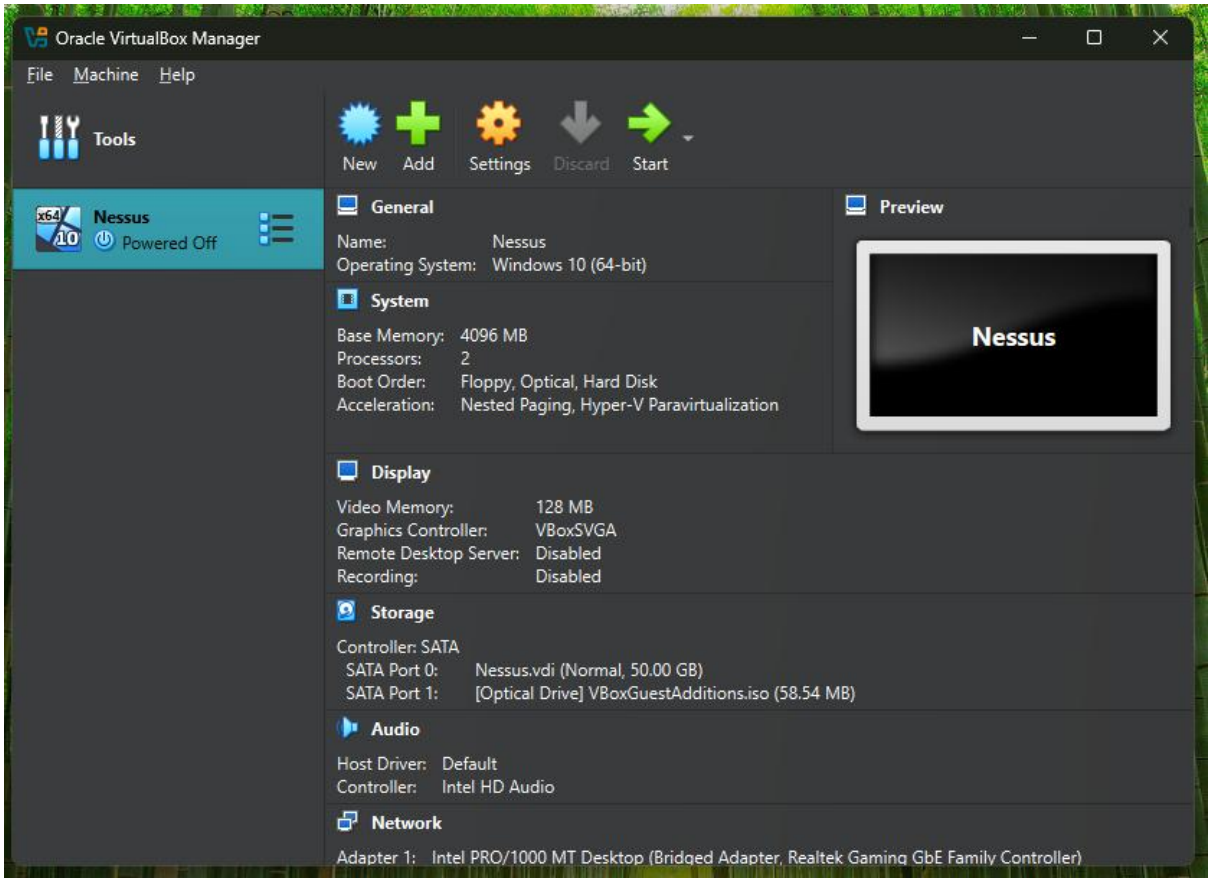
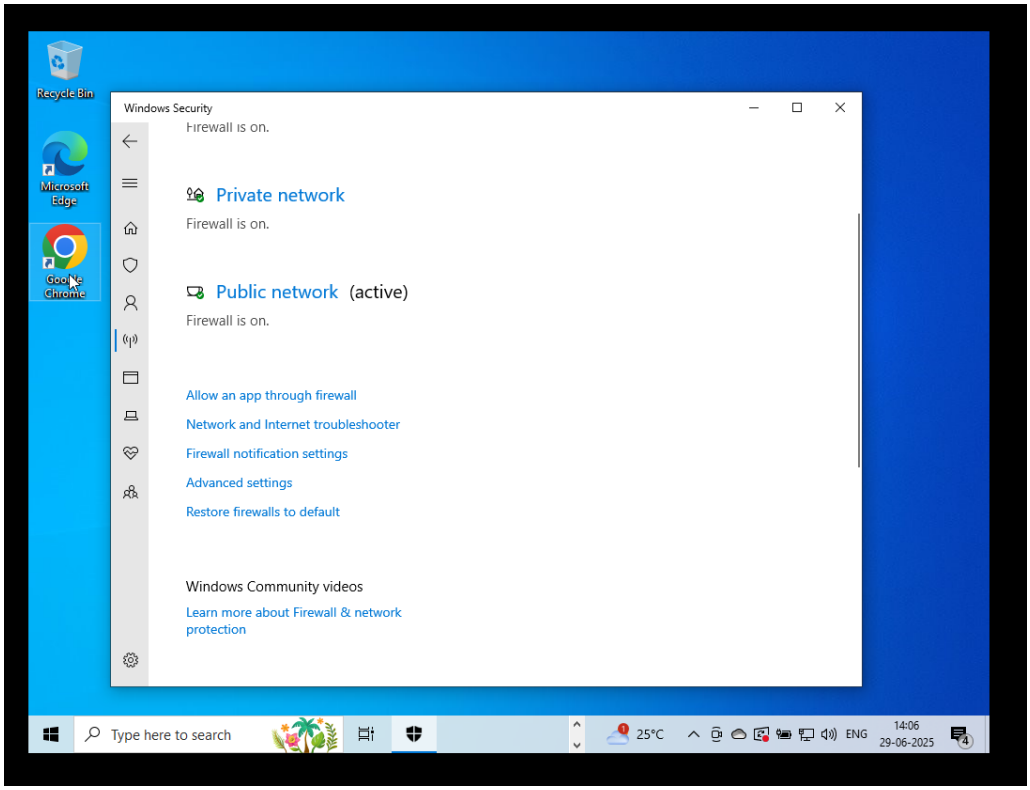
Steps to Perform(using Windows Defender)

Step 1: Initialize VMware

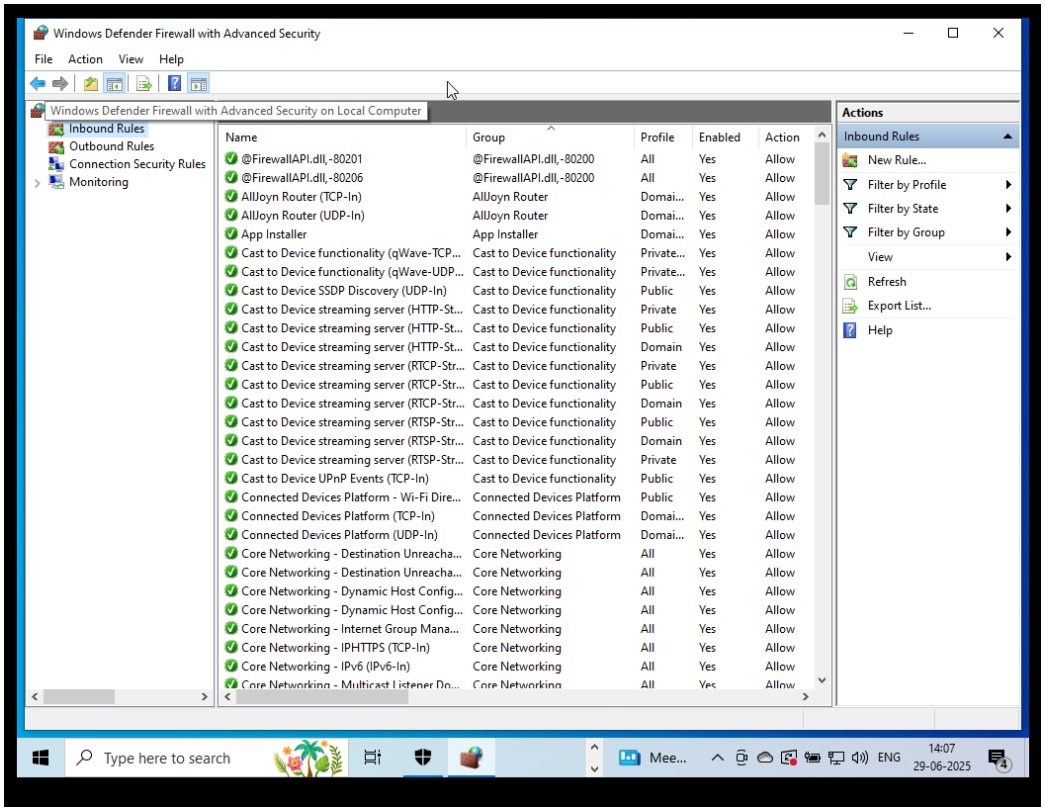
- Setup vmware and open windows on vm



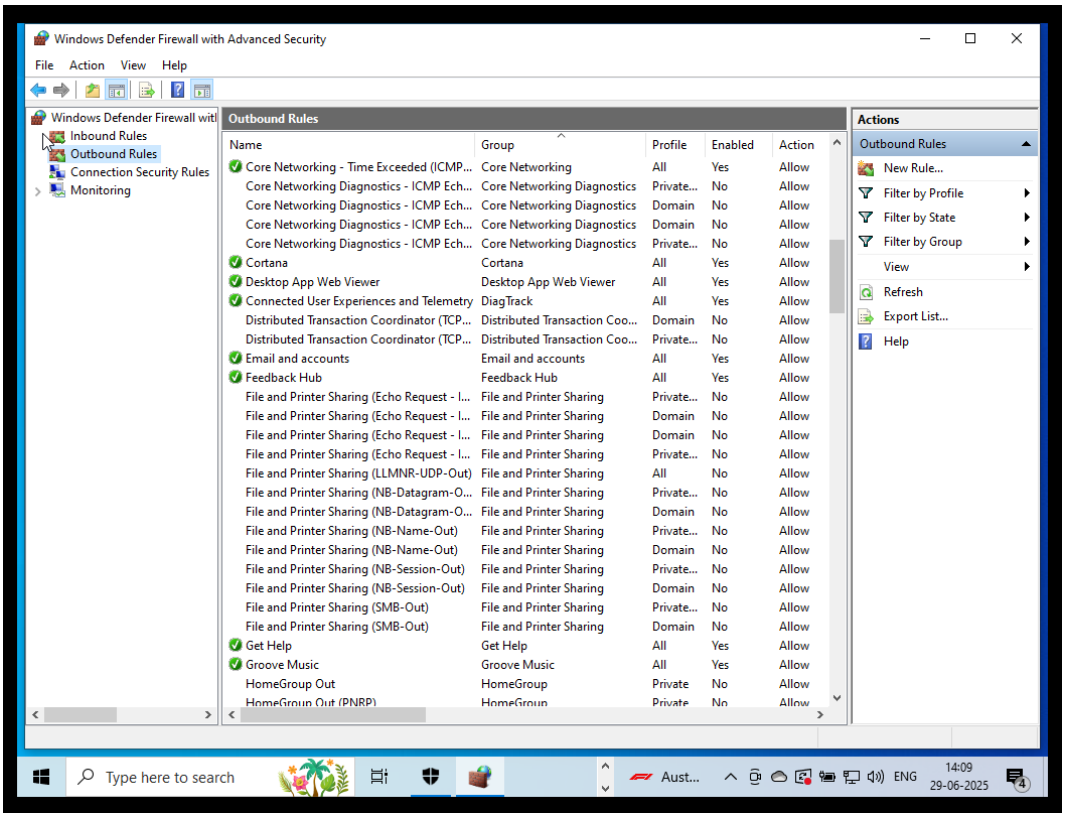
- Open Windows Defender Firewall with Advance Settings



- Open Inbound Rules

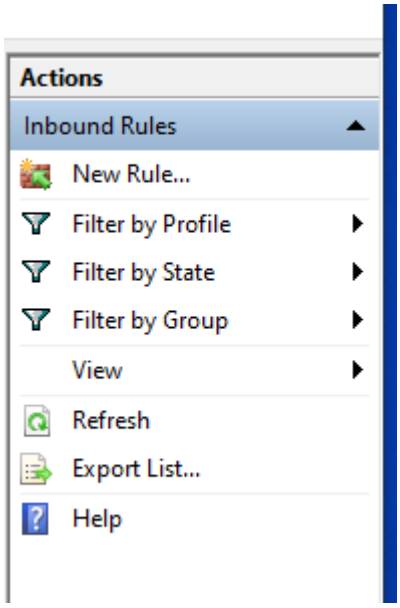


- Open Outbound Rules

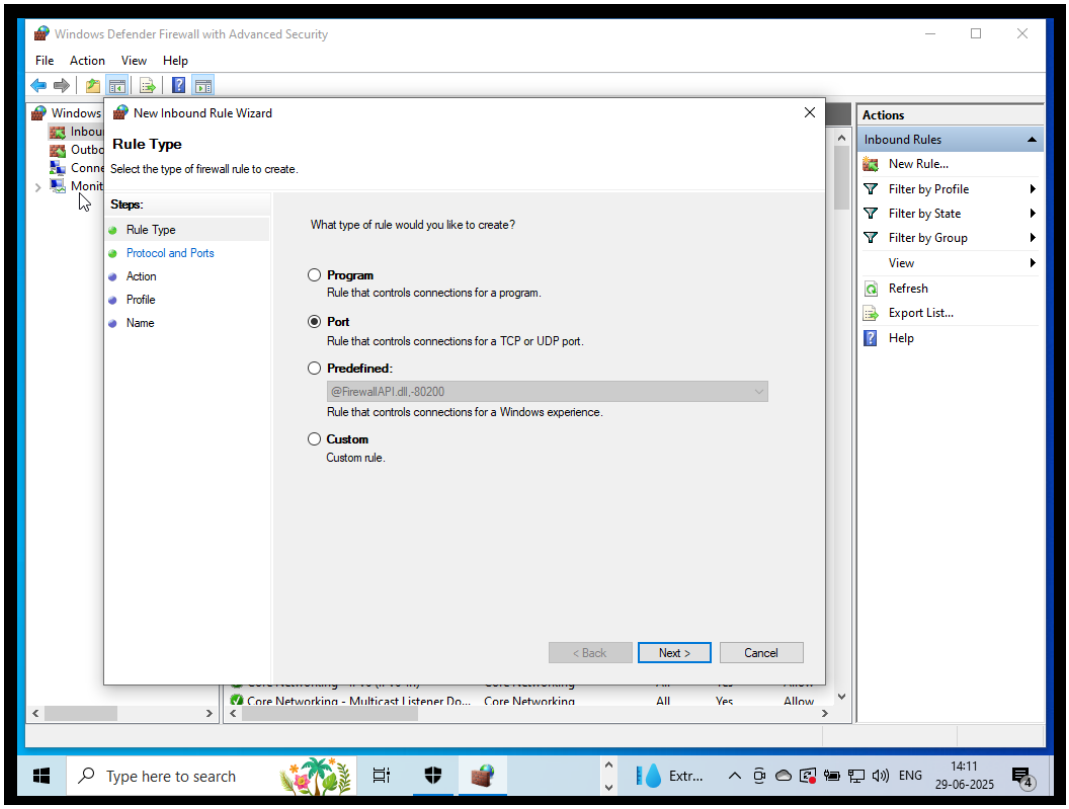


Step 3: Block Inbound Traffic on Port 23 (Telnet):

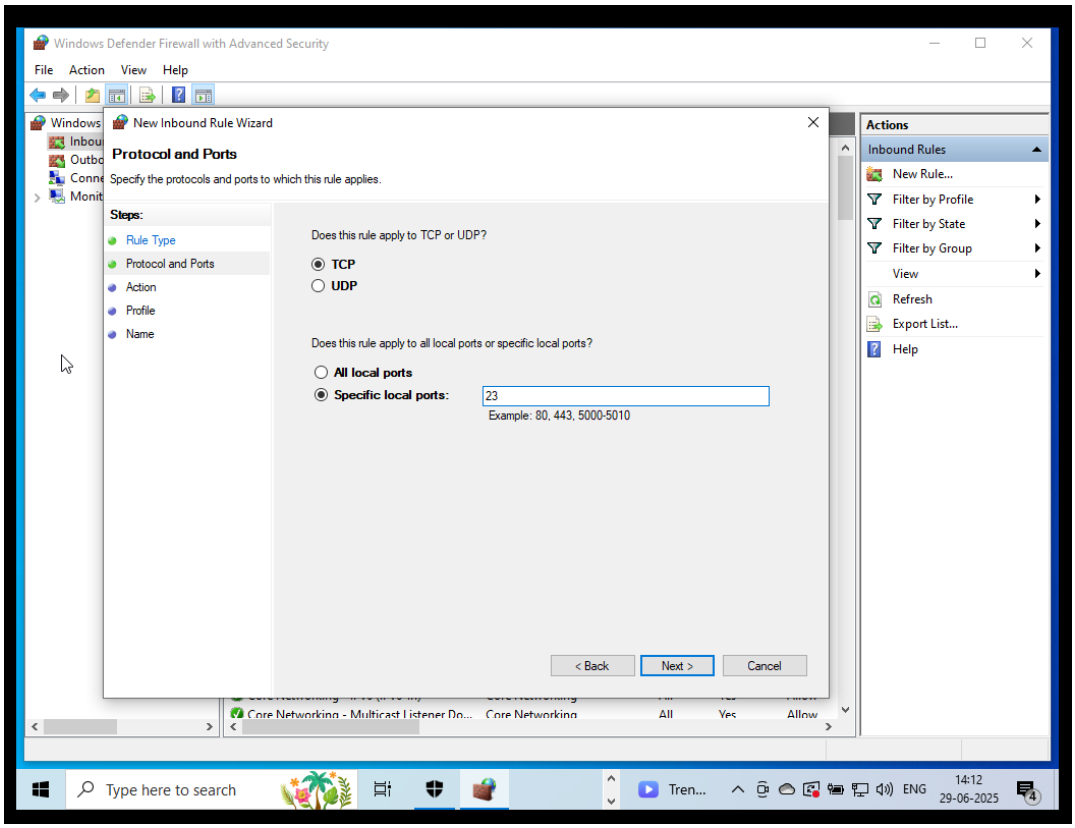
- Open New Rules in Action Menu



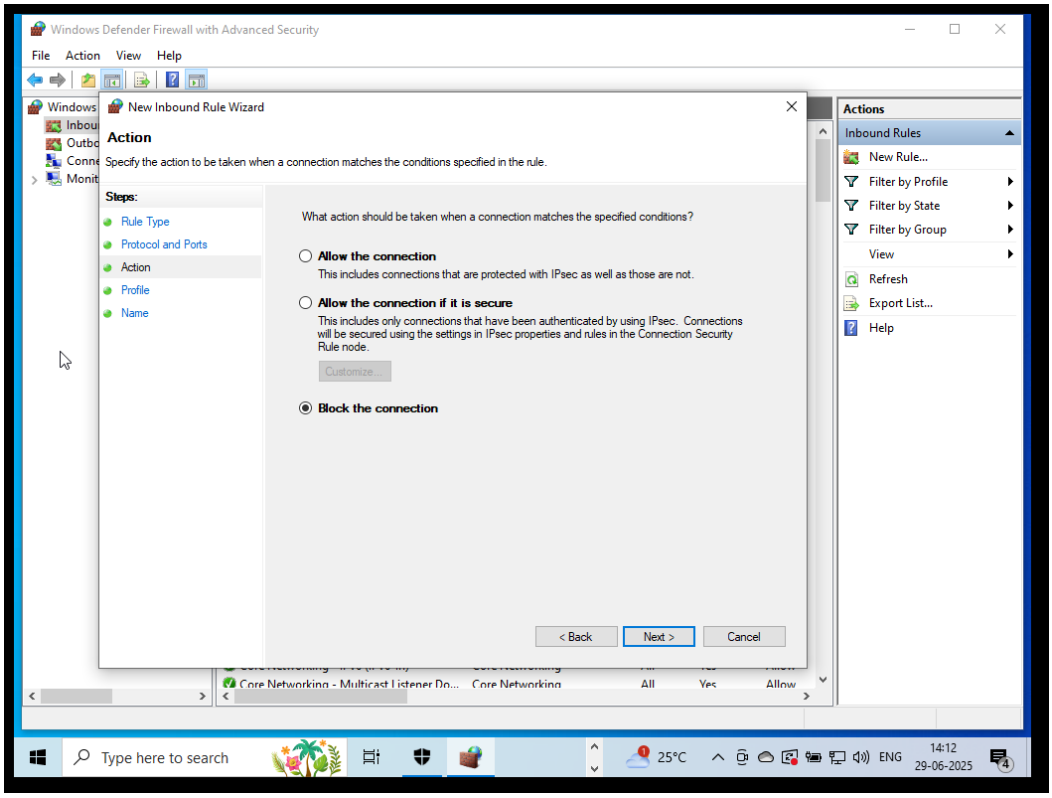
- Select port



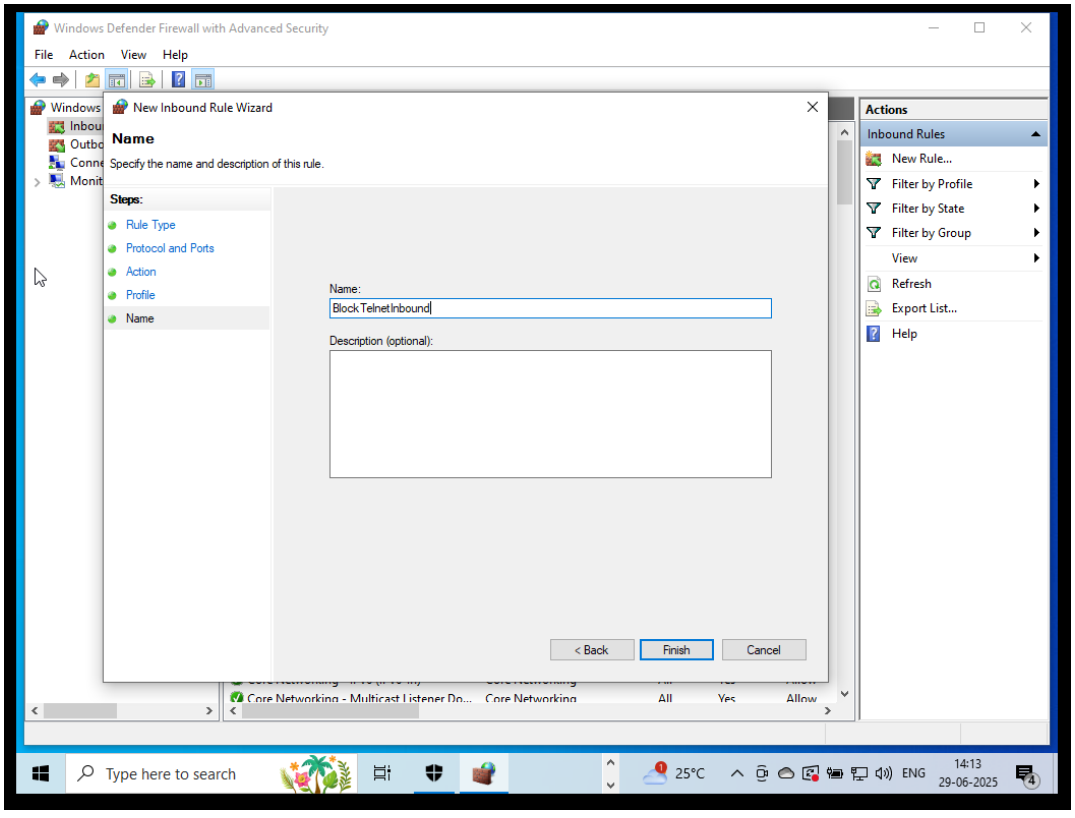
- Select TCP



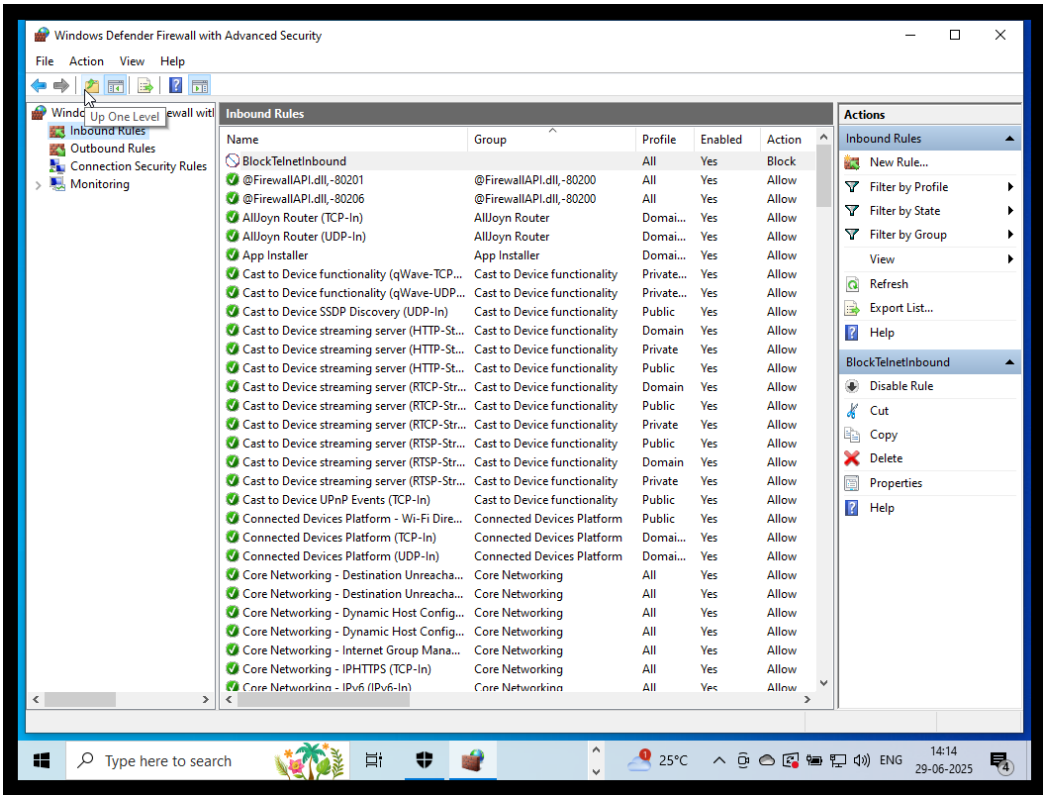
- Block the Connection



- Give name



- Finish

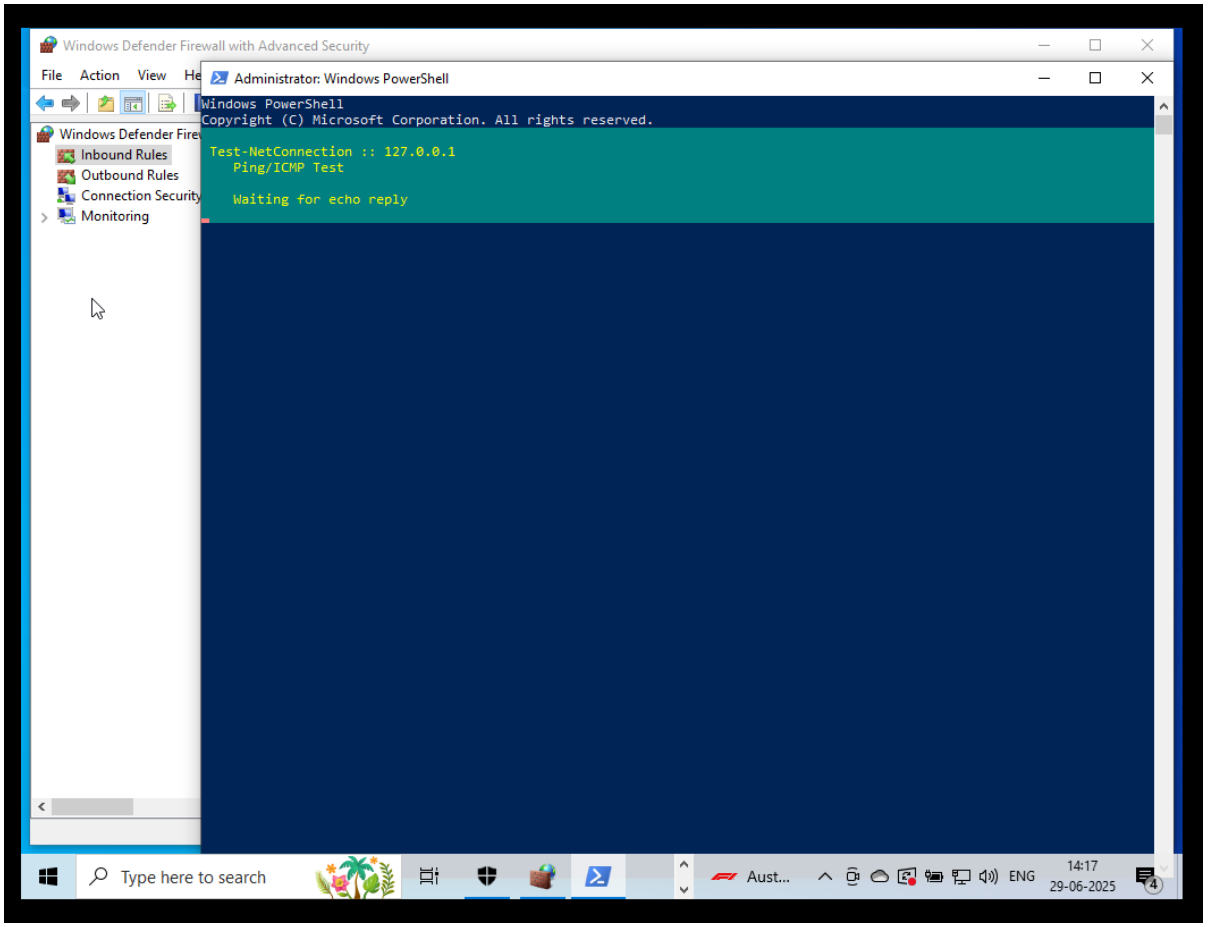


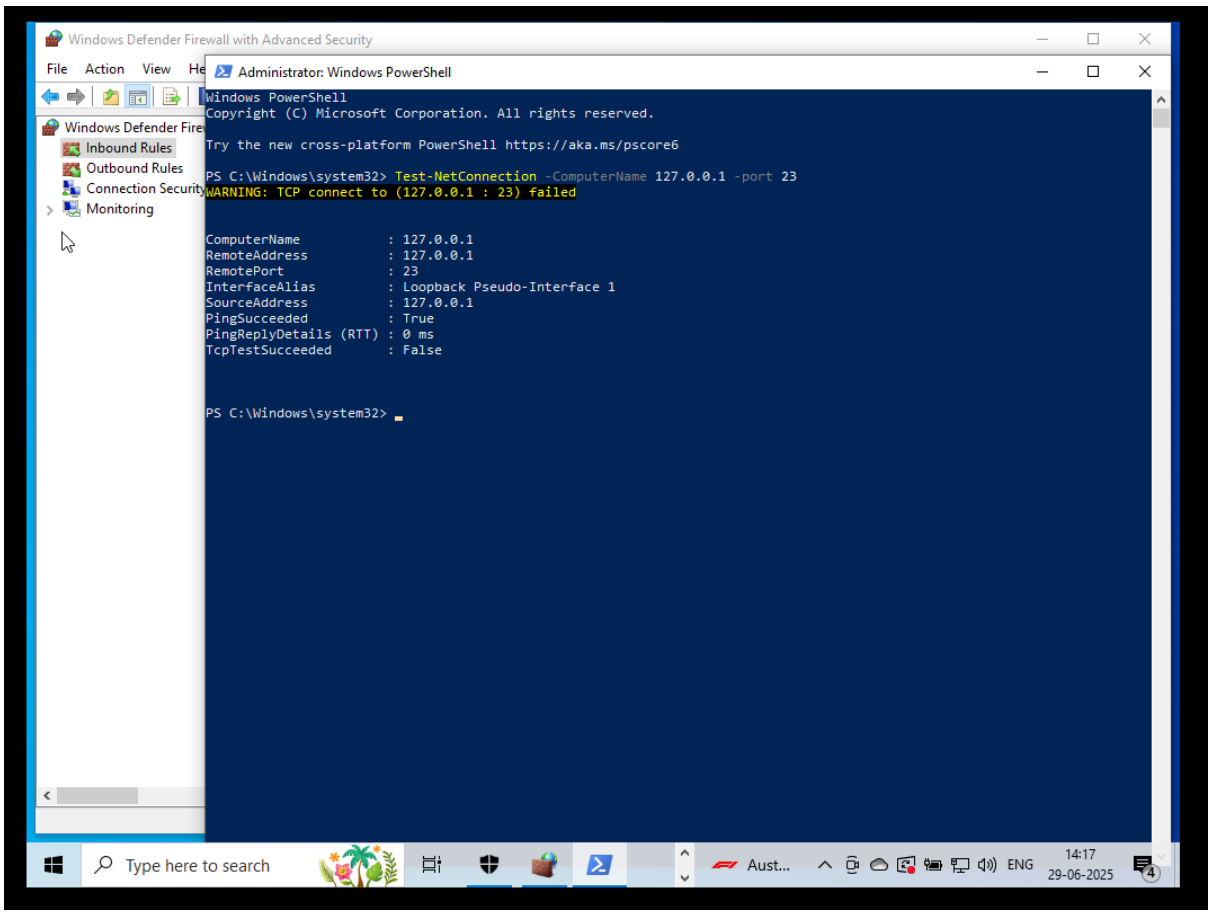
Step 4: Test the Blocked Port:

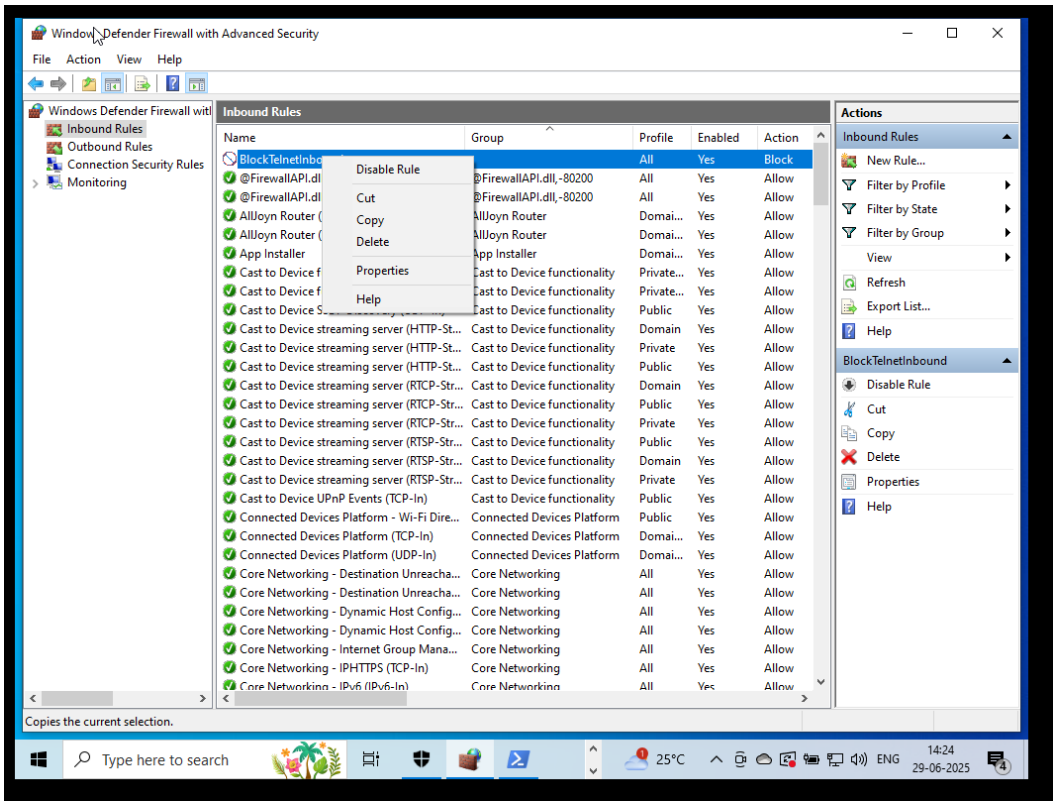
- Open PowerShell and try:

```
Test-NetConnection -ComputerName 127.0.0.1 -Port 23
```

```
PS C:\Windows\system32> Test-NetConnection -ComputerName 127.0.0.1 -port 23
```


Windows Defender Firewall with Advanced Security
File Action View He
Windows Defender Firewall
Inbound Rules
Outbound Rules
Connection Security
Monitoring
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Test-NetConnection :: 127.0.0.1
Ping/ICMP Test
Waiting for echo reply
Type here to search
Aust...
ENG
14:17
29-06-2025


Windows Defender Firewall with Advanced Security
File Action View He
Windows Defender Firewall
Inbound Rules
Outbound Rules
Connection Security
Monitoring
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> Test-NetConnection -ComputerName 127.0.0.1 -port 23
WARNING: TCP connect to (127.0.0.1 : 23) failed
ComputerName : 127.0.0.1
RemoteAddress : 127.0.0.1
RemotePort : 23
InterfaceAlias : Loopback Pseudo-Interface 1
SourceAddress : 127.0.0.1
PingSucceeded : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded : False
PS C:\Windows\system32>
Type here to search
Aust...
ENG
14:17
29-06-2025

Step 5: Remove the Block Rule:

- Click on BlockTelnetIn and select delete