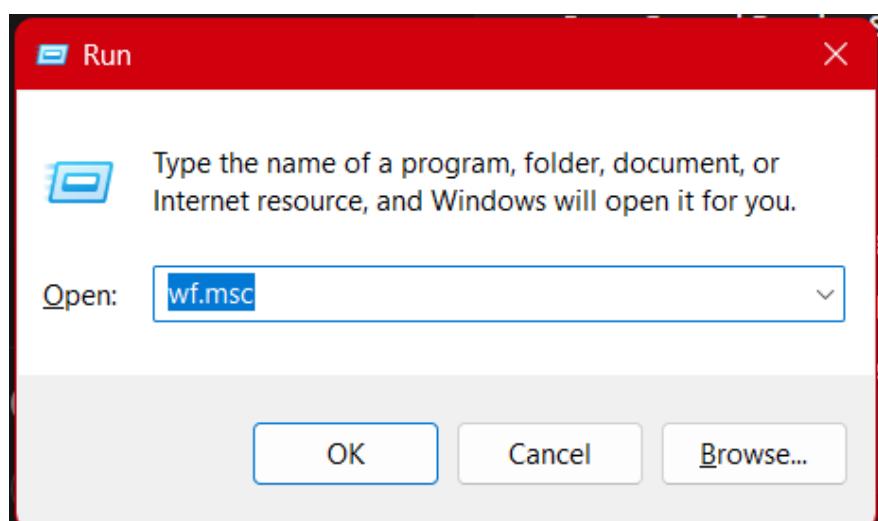


# Firewall Configuration & Testing Report (Windows Firewall)

Objective: Configure and test basic firewall rules  
in Windows Firewall.

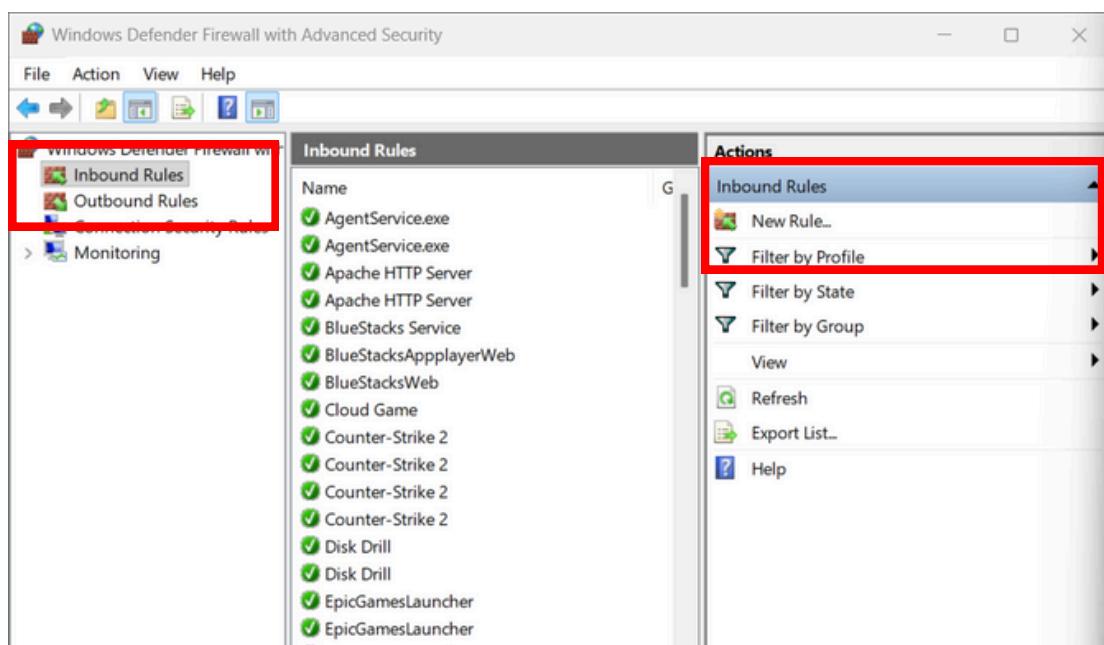
## Steps 1:

Open Windows Firewall (wf.msc).



## Step 2:

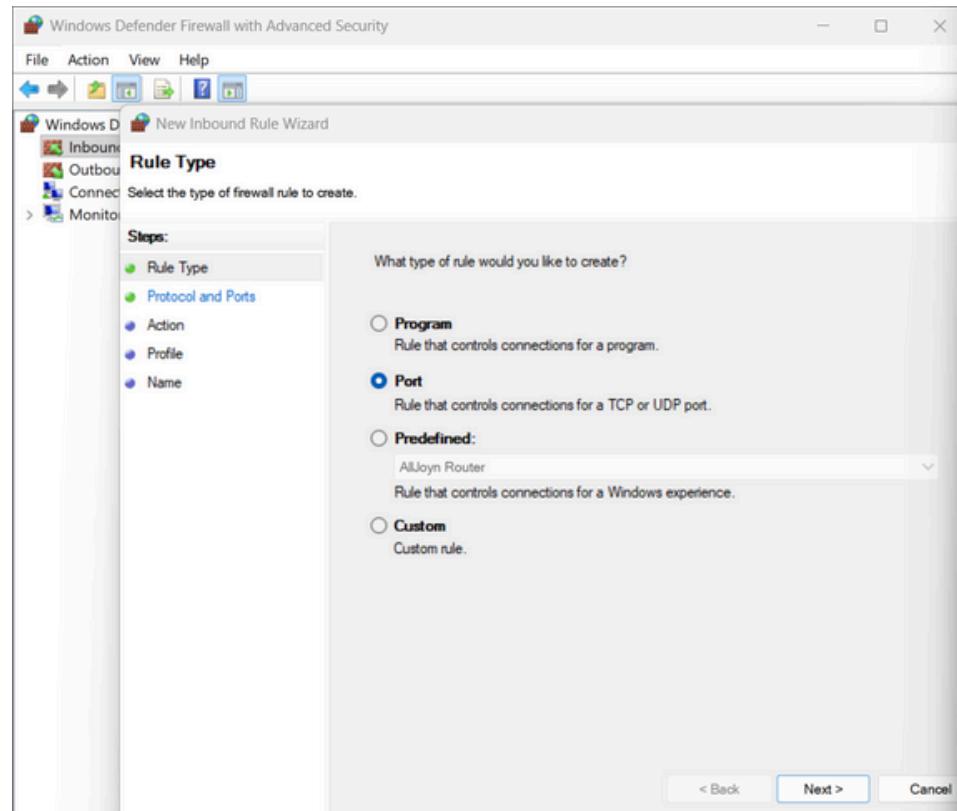
View current inbound and outbound rules.



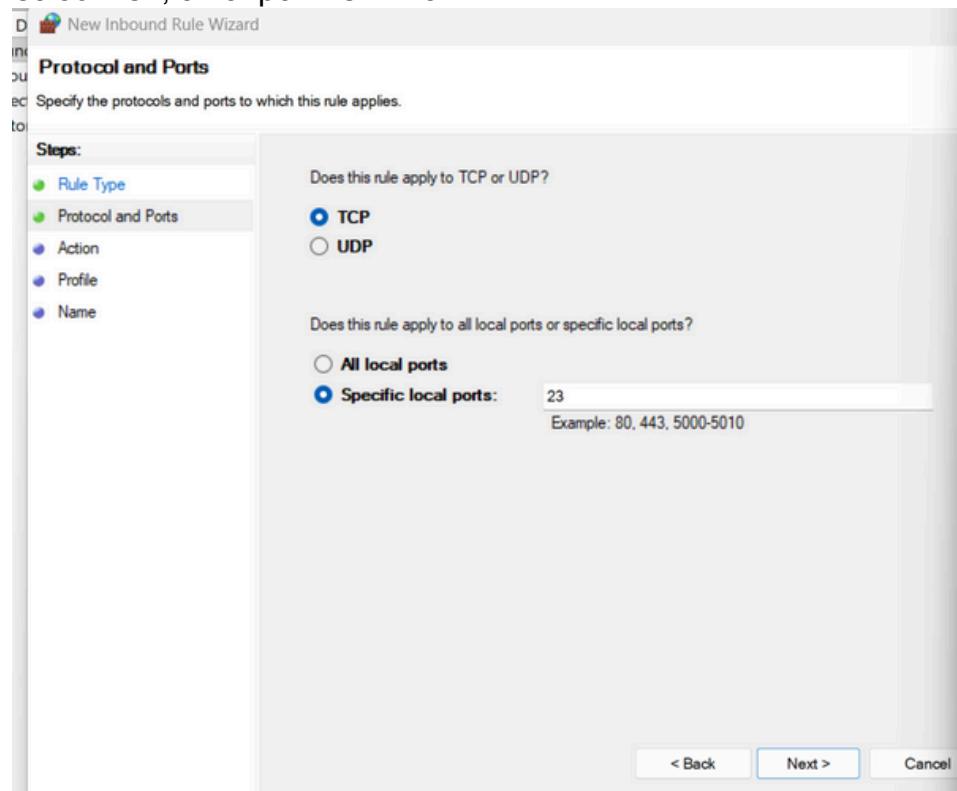
### Step 3:

Add Rule to Block Inbound Traffic on Port 23 (Telnet)

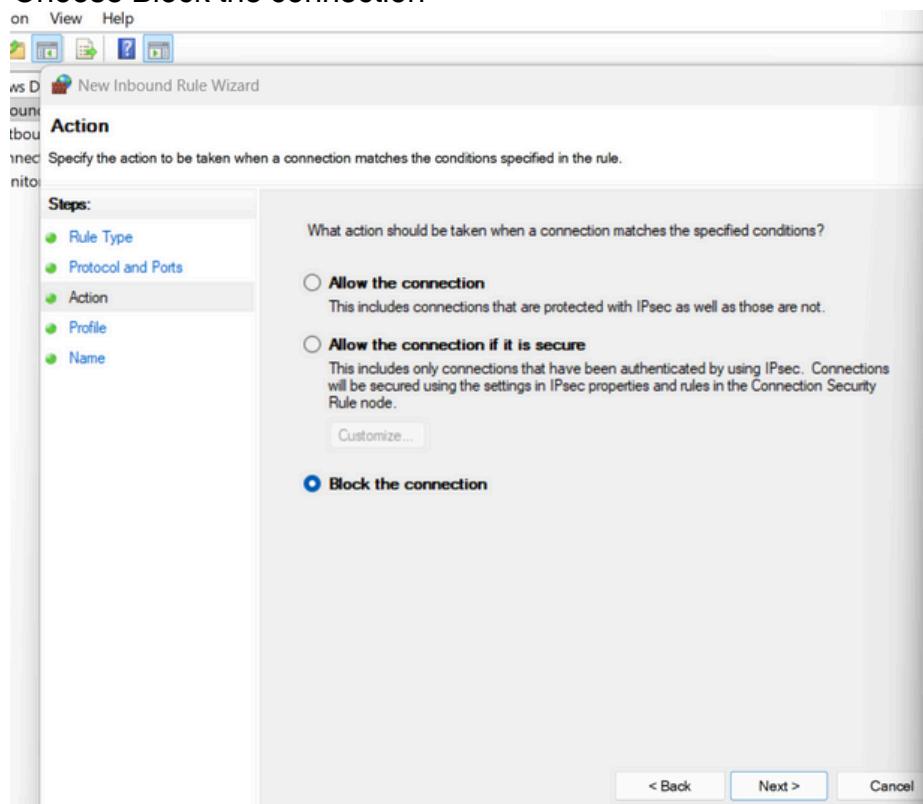
Choose Port → Next



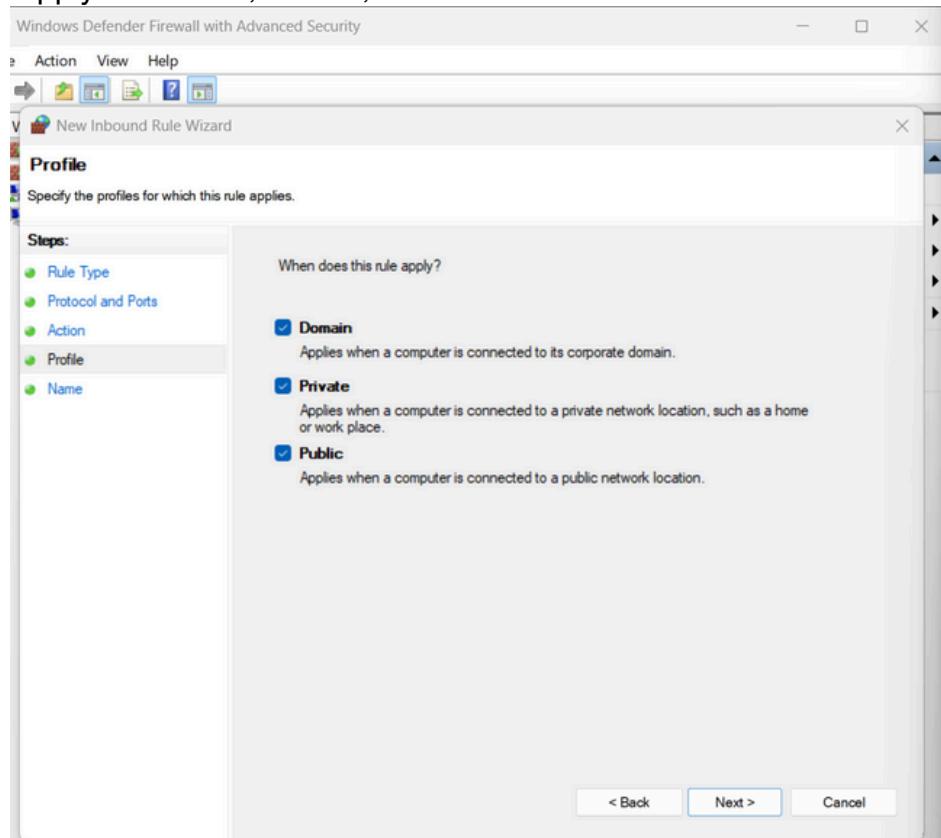
select TCP, enter port:23 → Next



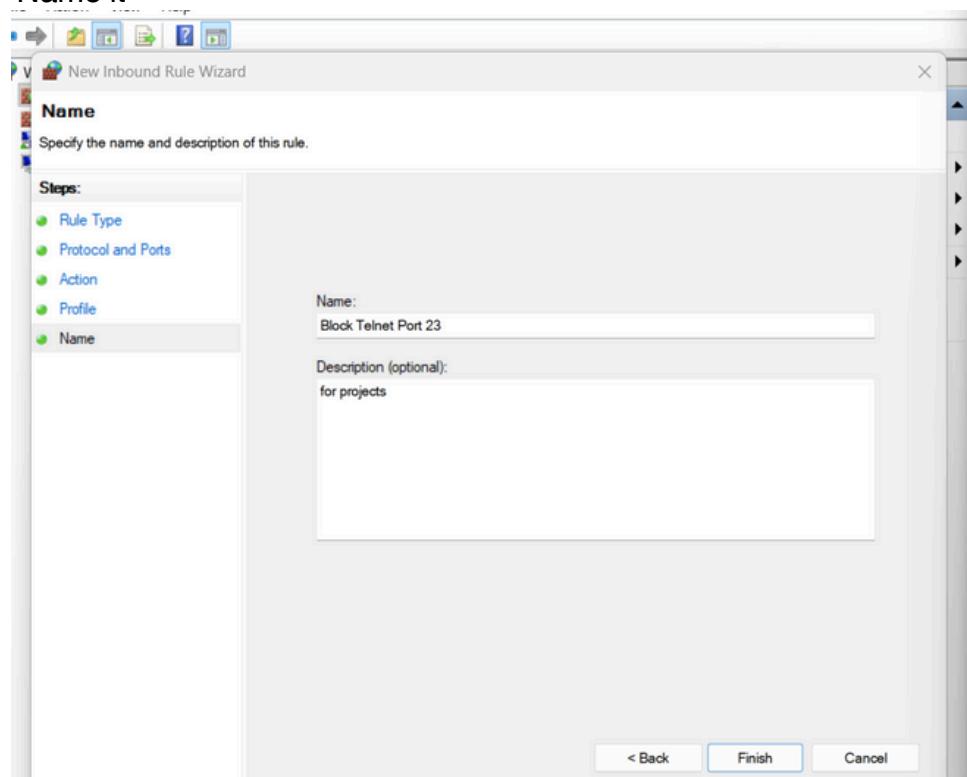
## Choose Block the connection



## Apply to Domain, Private, Public → Next



## Name it



## Enable Telnet Client: using command

```
Administrator: Command Prompt - dism /online /Enable-Feature /FeatureName:TelnetClient
Microsoft Windows [Version 10.0.26200.7019]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>dism /online /Enable-Feature /FeatureName:TelnetClient

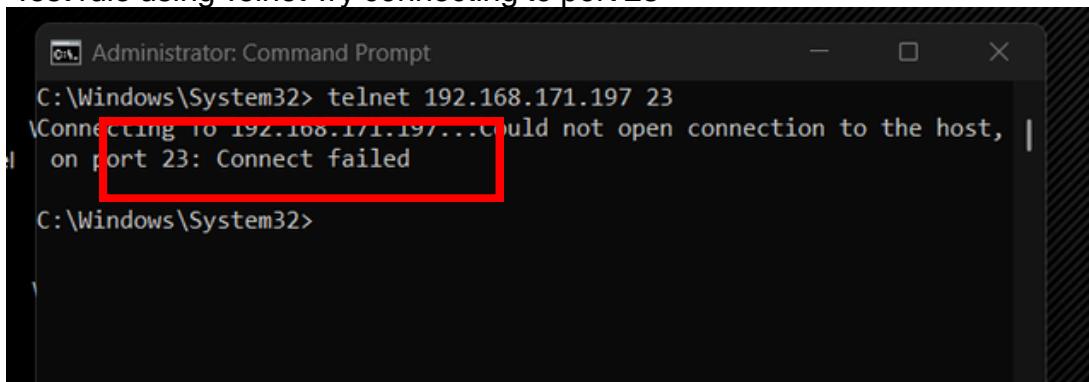
Deployment Image Servicing and Management tool
Version: 10.0.26100.5074

Image Version: 10.0.26200.7019

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Restart Windows to complete this operation.
Do you want to restart the computer now? (Y/N)
```

#### Step 4:

Test rule using Telnet Try connecting to port 23



C:\Windows\System32> telnet 192.168.1.197 23  
!Connecting to 192.168.1.197... could not open connection to the host,  
on port 23: Connect failed  
C:\Windows\System32>

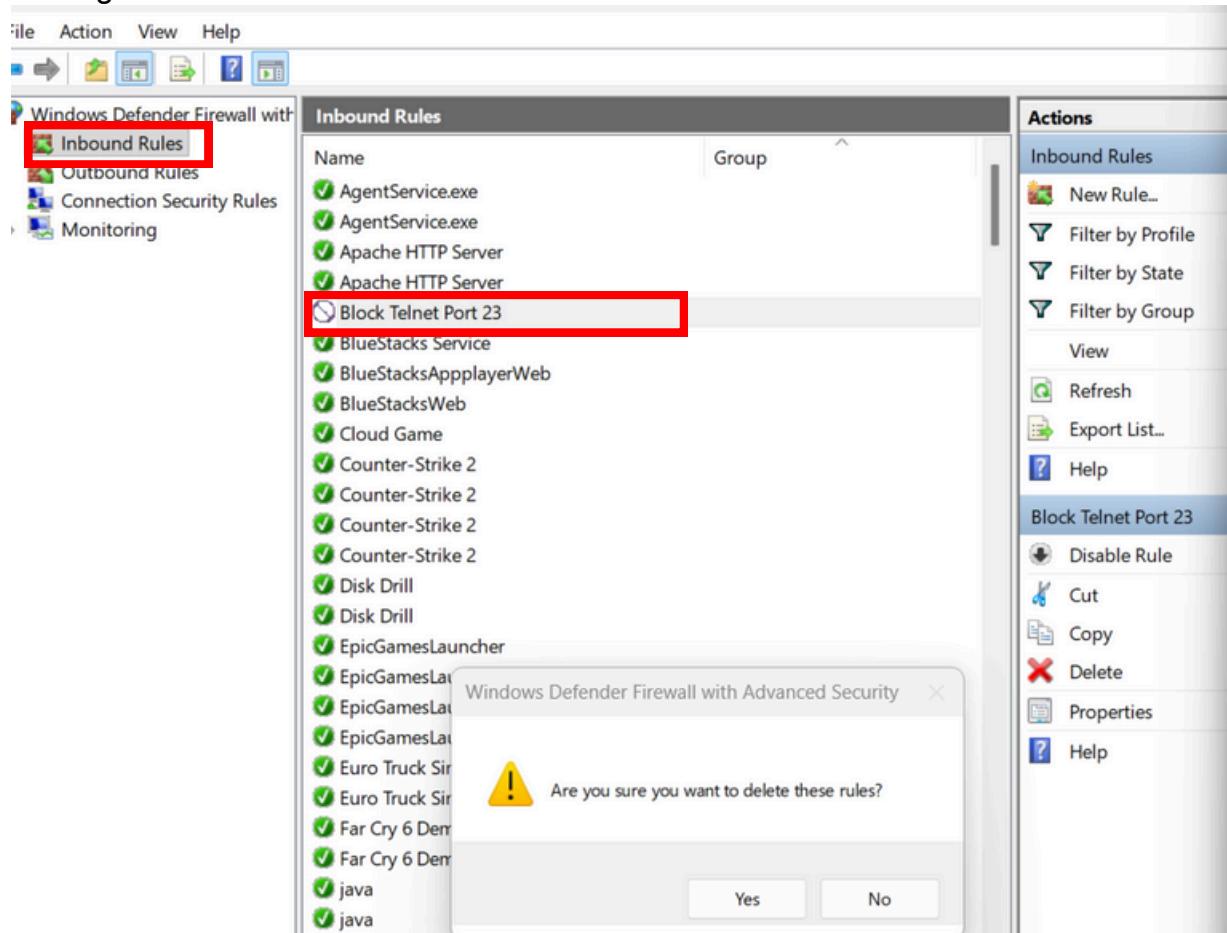
A red box highlights the error message "could not open connection to the host, on port 23: Connect failed".

It must show connection failed or blocked!!!

#### Step 5:

Remove test rule.

1. Go to Inbound Rules
2. Find Block Telnet port 23
3. Right-click → Delete



Summary:

Windows Firewall works by filtering packets based on configured allow/block rules.