Firewall Rule Configuration Task Report

\*\*Internship Task Title:\*\* Firewall Rule Configuration — Block Telnet, Allow SSH

\*\*Intern Name:\*\* Naveen Kumar

\*\*Date:\*\* May 30, 2025

\*\*System Used:\*\* Windows PowerShell (Run as Administrator)

# Objective

The goal of this task was to enhance system security by:  
1. Blocking all inbound Telnet connections (TCP Port 23).  
2. Allowing all inbound SSH connections (TCP Port 22).

# Steps Performed

## 1. Created Firewall Rule to Block Telnet

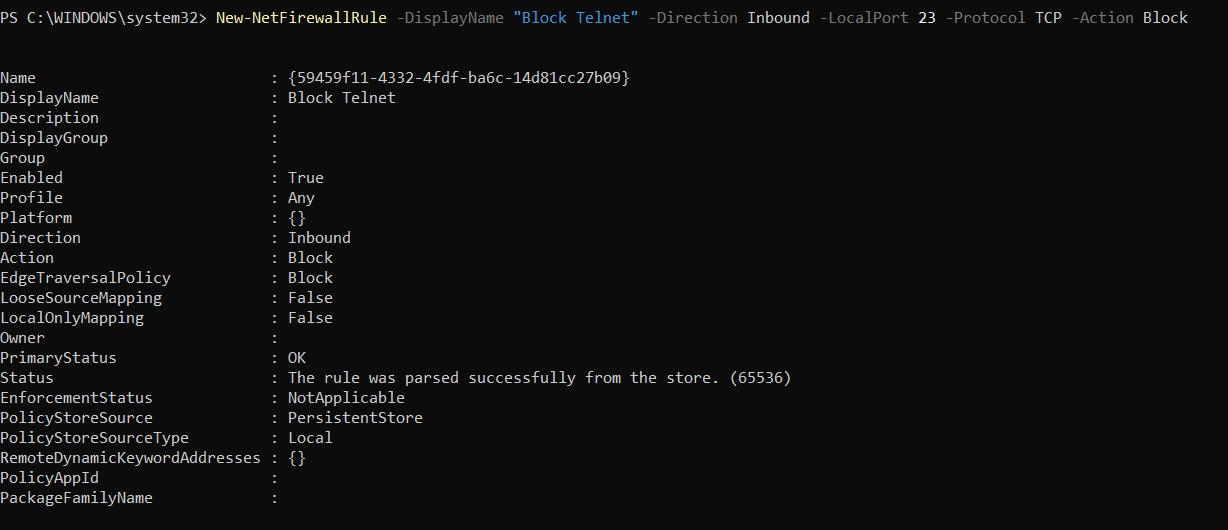
Command Used:

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

Result:

- Rule named "Block Telnet" was successfully created.  
- Action: Block  
- Port: 23  
- Direction: Inbound

Screenshot Evidence:



## 2. Tested the Block Telnet Rule

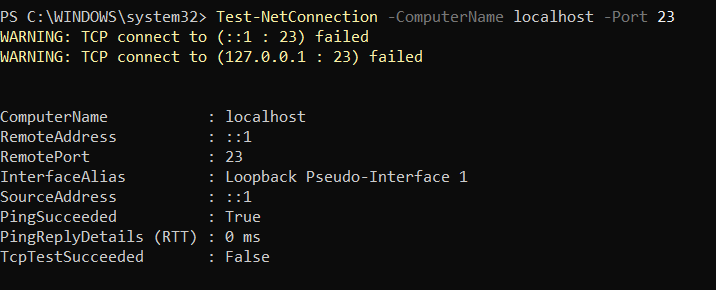
Command Used:

Test-NetConnection -ComputerName localhost -Port 23

Result:

- Connection to port 23 failed as expected.  
- TcpTestSucceeded: False confirms the port is blocked.

Screenshot Evidence:



## 3. Created Firewall Rule to Allow SSH

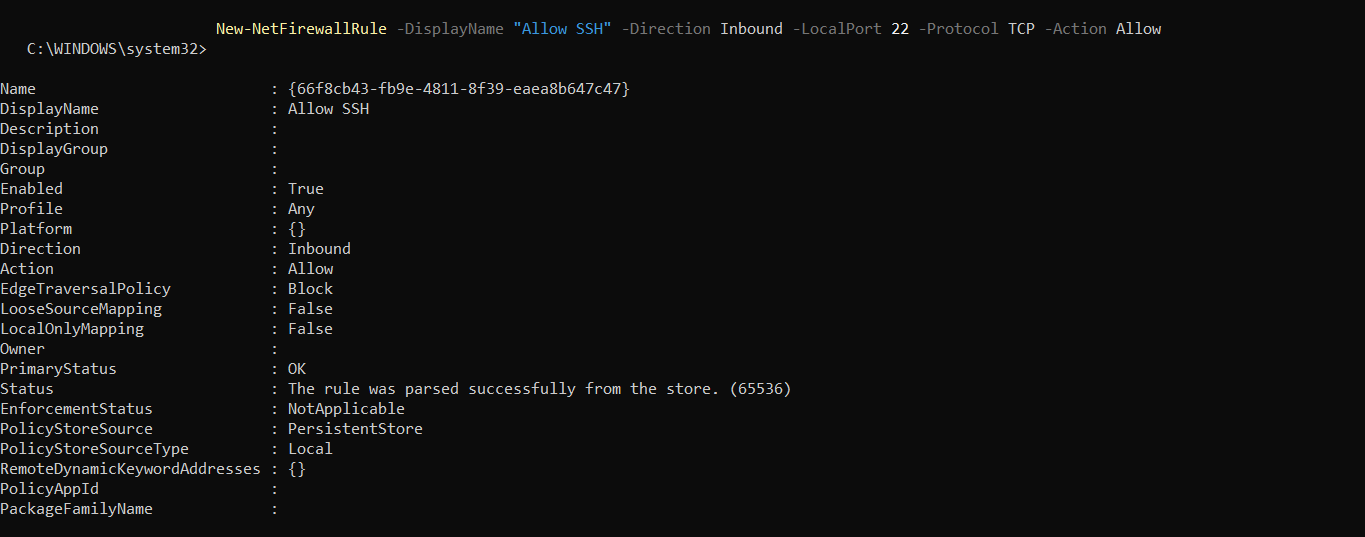
Command Used:

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

Result:

- Rule named "Allow SSH" was successfully created.  
- Action: Allow  
- Port: 22  
- Direction: Inbound

Screenshot Evidence:



## 4. Verified Firewall Rules

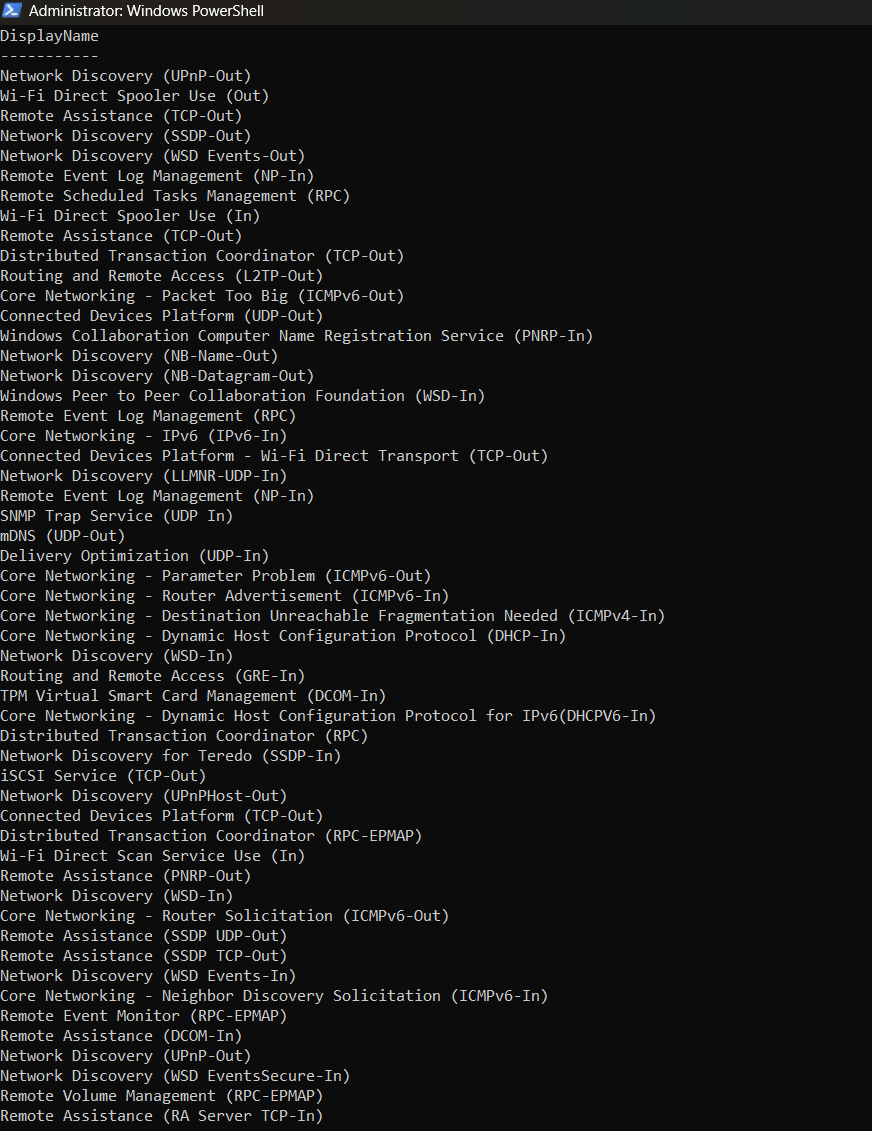
Command Used:

Get-NetFirewallRule | Where-Object DisplayName -like "\*Telnet\*"  
Get-NetFirewallRule | Where-Object DisplayName -like "\*SSH\*"

Result:

- Both "Block Telnet" and "Allow SSH" rules were listed successfully.

Screenshot Evidence:



# Conclusion

The task objectives were successfully met.  
Telnet connections are now blocked, improving security.  
SSH access is permitted through the firewall.  
All configurations were tested and verified via PowerShell.