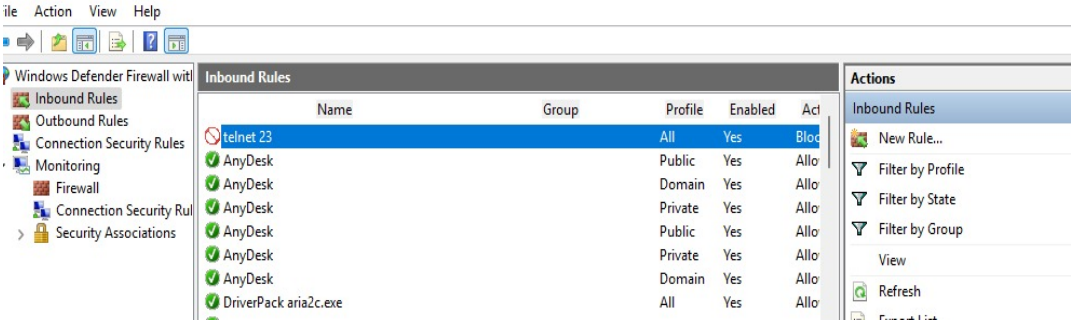
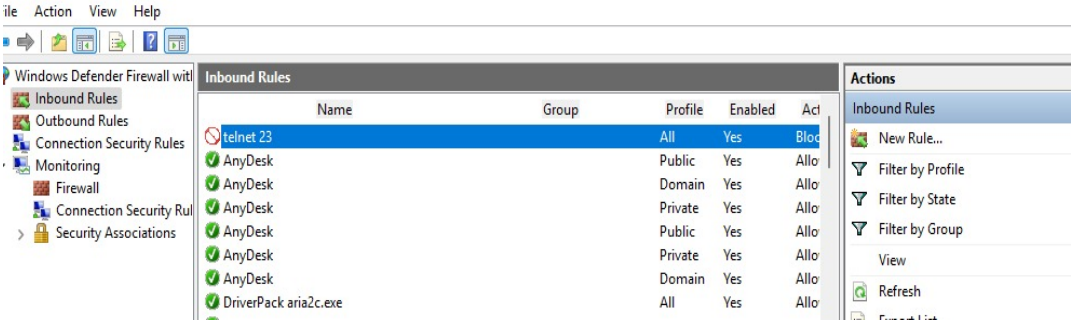
Complete Report: Configuring Windows Firewall Inbound Rule to Block Port 23 and Testing

This report documents the step-by-step procedure for configuring a Windows Firewall inbound rule to block TCP port 23 (Telnet) and verifying its functionality. Telnet is an outdated and insecure protocol that transmits data in plaintext, making it vulnerable to interception and misuse. Blocking it helps enhance system security.

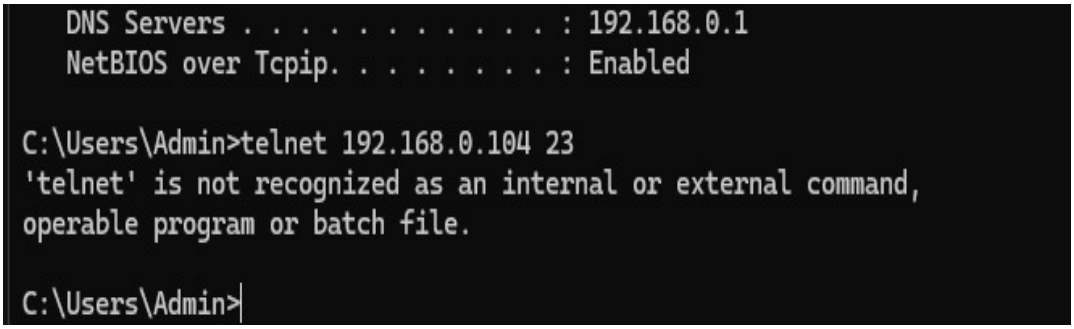
Step 1: Checking Current Network Settings
Before configuring the firewall, the current network configuration was reviewed using the *ipconfig* command. This shows the DNS server, gateway, and other network details.



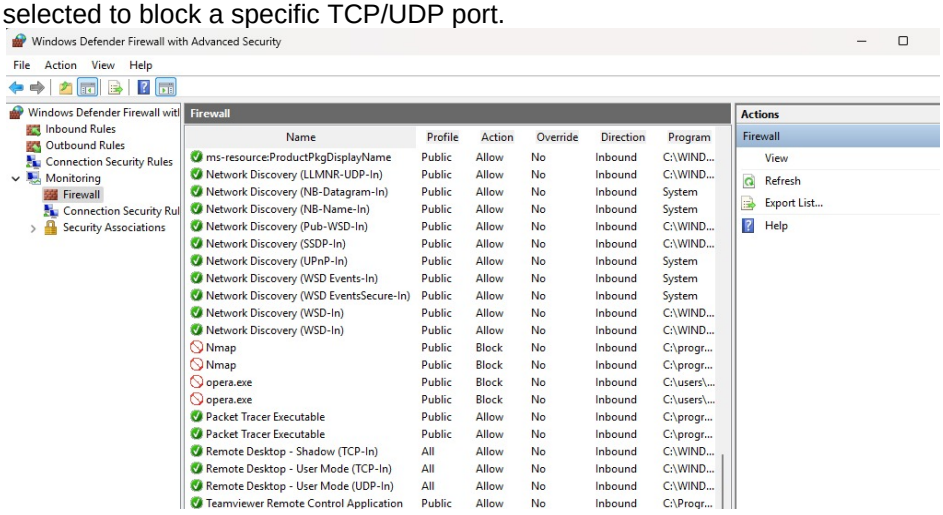
Step 2: Attempting to Use Telnet
An attempt was made to connect to another machine on TCP port 23 using the Telnet client. However, the system returned an error: *'telnet' is not recognized as an internal or external command*. This means the Telnet client is not installed by default.



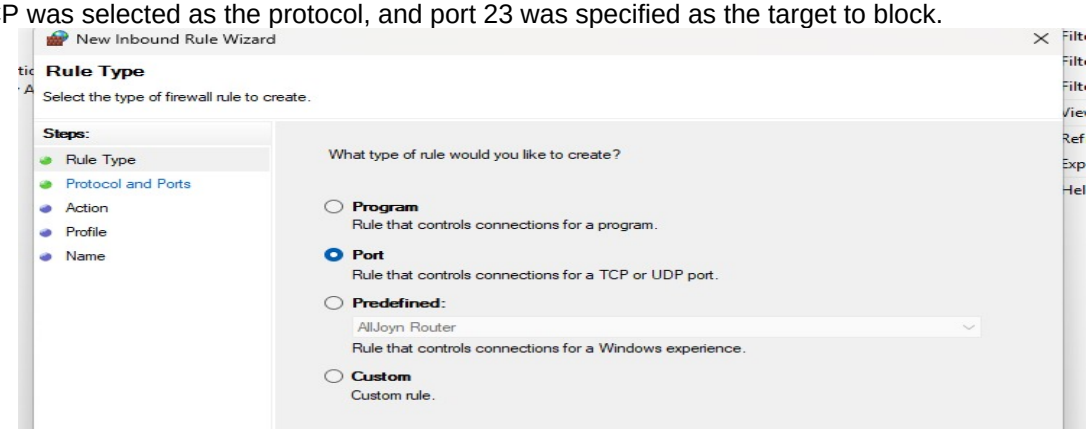
Step 3: Accessing Windows Defender Firewall with Advanced Security
The Windows Firewall with Advanced Security was accessed from the Control Panel to configure inbound rules.



Step 4: Creating a New Inbound Rule
From the left pane, *Inbound Rules* was selected and *New Rule...* clicked. In the rule type window, **Port** was selected to block a specific TCP/UDP port.



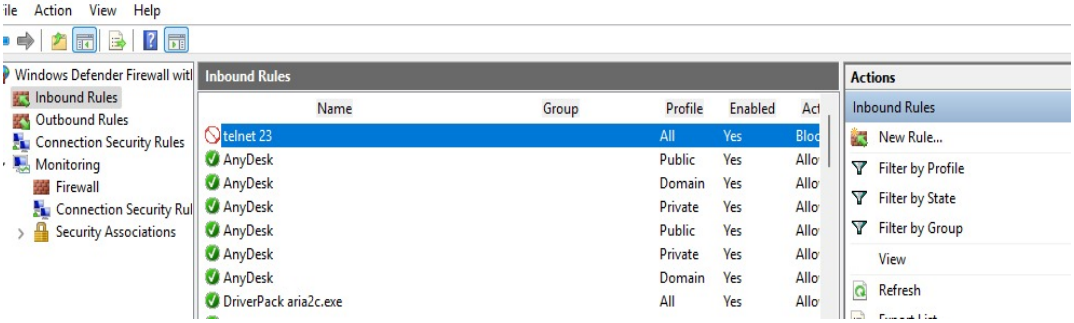
Step 5: Configuring Port and Protocol
TCP was selected as the protocol, and port 23 was specified as the target to block.



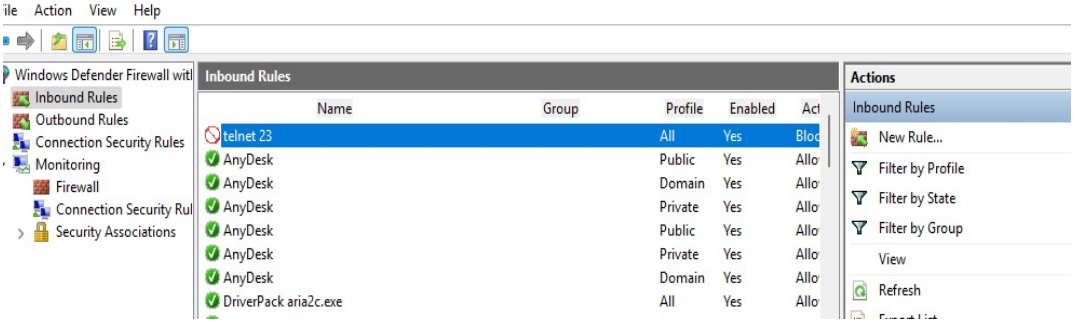
Step 6: Choosing Block Action
The option **Block the connection** was selected to ensure that any attempt to connect over port 23 would be denied.

Step 7: Applying to All Profiles
The rule was applied to all network profiles (Domain, Private, and Public) for complete coverage.

Step 8: Naming and Saving the Rule
The rule was named "telnet 23" for easy identification and saved.



Step 9: Verifying the Rule
The inbound rules list confirmed the new rule "telnet 23" with the action set to **Block**.



Step 10: Testing the Firewall Rule
Although the Telnet client was not installed, any connection attempt to port 23 would now be blocked by the firewall. This prevents any Telnet-based remote access to the machine.

Conclusion:
Blocking port 23 via Windows Firewall is a proactive security measure to prevent the insecure Telnet protocol from being used. Even without Telnet installed, the firewall rule ensures that no communication over this port is allowed.