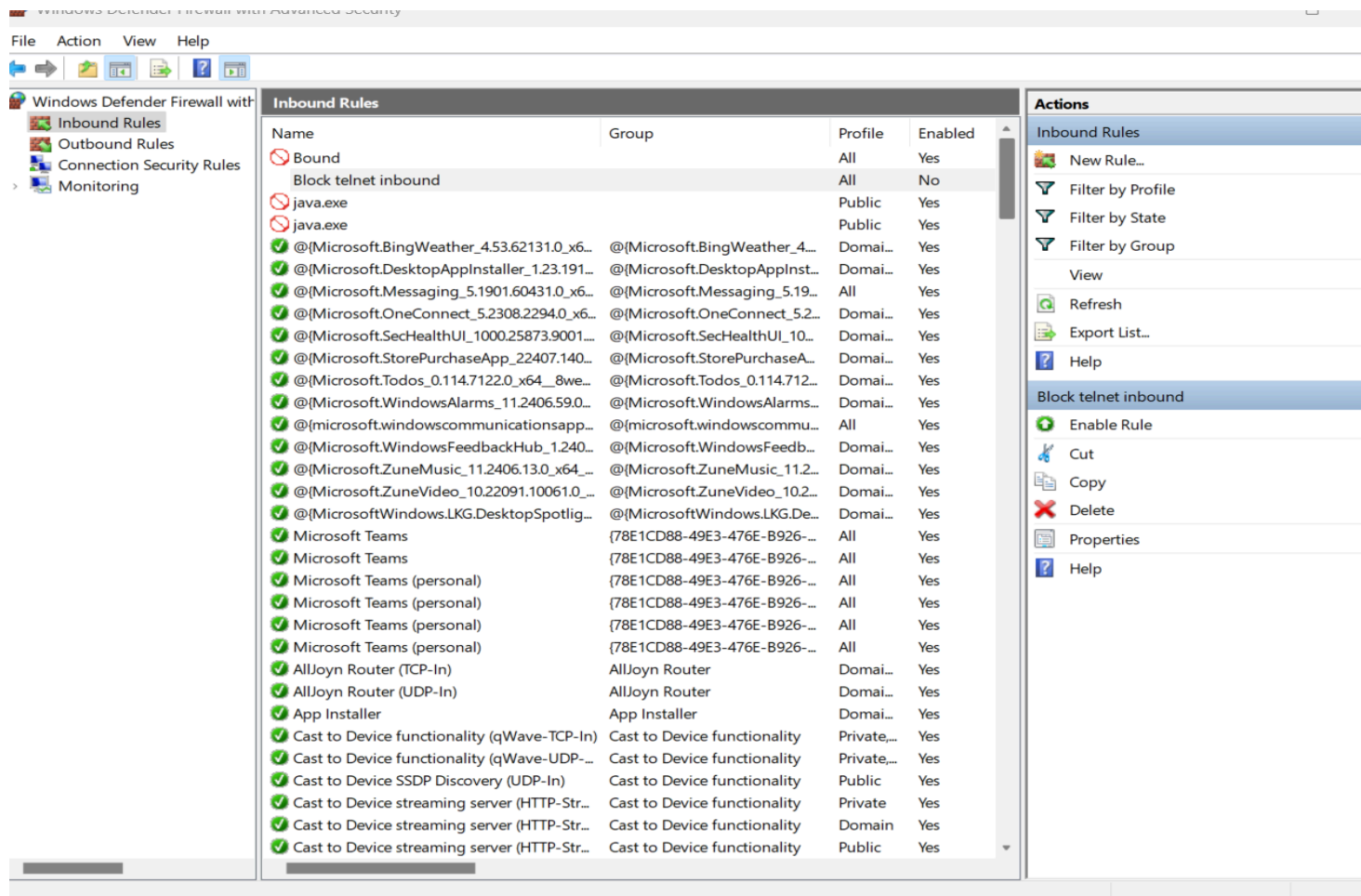


Firewall Setup and Testing Report

This report documents the steps taken to configure, test, and remove a basic firewall rule on a Windows system.

I. Firewall Rule Creation

1. **Open Configuration Tool:** Opened **Windows Defender Firewall with Advanced Security** (\text{wf.msc}) and navigated to **Inbound Rules**.




2. **Rule Definition:** Created a new **Inbound Rule** named "**Block telnet inbound**".
- **Rule Parameters:** The rule was configured to block **TCP** traffic specifying **Local Port 23** (Telnet).

Block telnet inbound Properties

General Programs and Services Remote Computers

Protocols and Ports Scope Advanced Local Principals Remote Users

Protocols and ports

 Protocol type: TCP

Protocol number: 6

Local port: Specific Ports

23

Example: 80, 443, 5000-5010

Remote port: All Ports

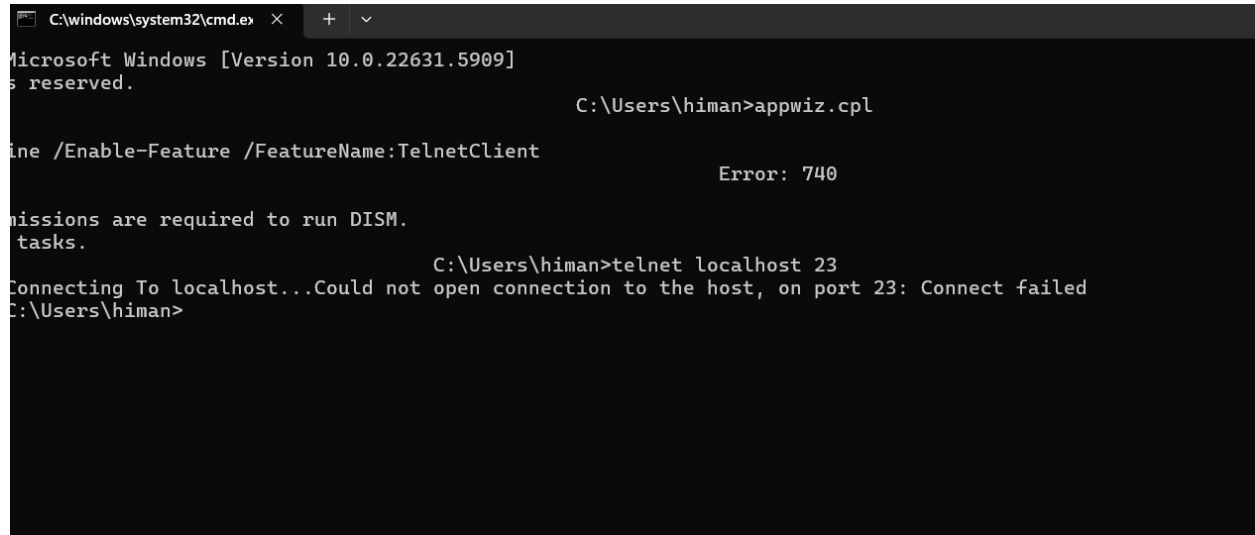
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: [Customize...](#)

OK Cancel Apply

II. Rule Testing

1. **Command Used:** To test the effectiveness of the block rule, the following command was executed in the Command Prompt:
 - **Command:** telnet localhost 23
2. **Verification:** The command immediately failed to connect, proving the firewall rule was correctly implemented and functional.
 - **Expected Output:** Could not open connection to the host, on port 23: Connect failed



```
C:\windows\system32\cmd.exe X + v
Microsoft Windows [Version 10.0.22631.5909]
(c) 2025 Microsoft Corporation. All rights reserved.

C:\Users\himan>appwiz.cpl

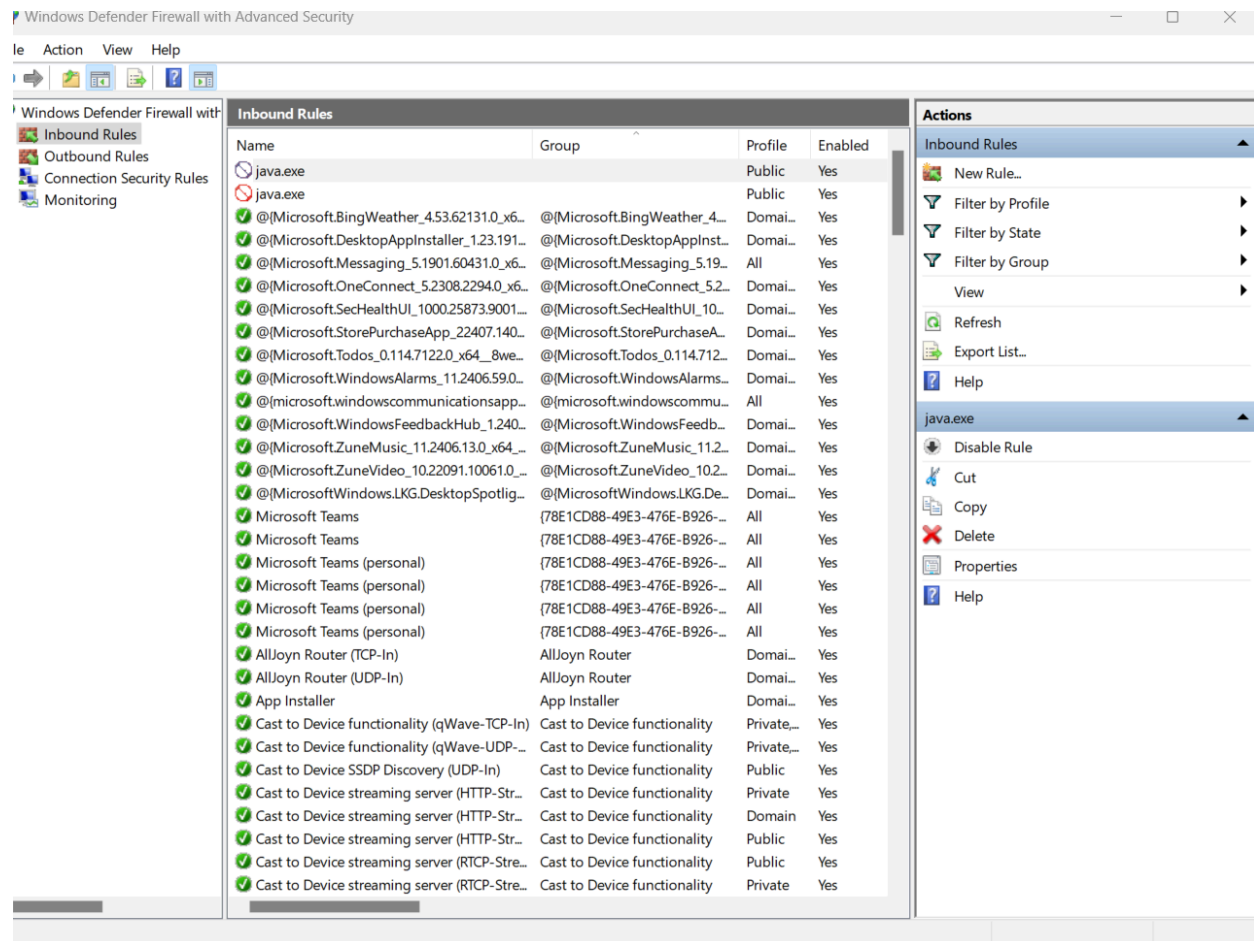
C:\Users\himan>DISM /Online /Enable-Feature /FeatureName:TelnetClient
Error: 740

Administrative permissions are required to run DISM.
For more information, see the help topics for DISM tasks.

C:\Users\himan>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed
C:\Users\himan>
```

III. Cleanup and Documentation

1. **Restore Original State:** The test rule was removed using the Graphical User Interface (GUI) to restore the system's default firewall configuration.
 - **GUI Action:** The rule "**Block telnet inbound**" was located in the Inbound Rules list, right-clicked, and **Deleted**.
 - **(Alternative Command for Documentation):** `netsh advfirewall firewall delete rule name="Block telnet inbound"`



IV. Summary of Firewall Function

1. **Firewall Filtering Summary:** A firewall acts as a security checkpoint, filtering network traffic based on configured rules. The process demonstrated here shows:
 - **Block Action:** An explicit **Block** rule takes precedence, immediately dropping traffic (Telnet packets on port 23) that matches its criteria.
 - **Defense Mechanism:** By filtering incoming traffic, the firewall successfully protected the system from unauthorized access attempts on that specific port.
 - **Restoration:** The ability to easily remove the temporary rule ensures the system's operational state is restored without persistent changes.