**Setup and Use a Firewall on Windows**

**Objective**

To configure and test basic Windows Firewall rules to allow or block specific network traffic. The task focuses on applying security policy via port-based filtering and verifying the effects through testing.

**Tools Used**

\* Windows Defender Firewall with Advanced Security

\* Command Prompt (cmd)

\* Telnet client (enabled via DISM command)

**Steps Performed**

**1. Opened Windows Firewall Configuration**

\* Accessed firewall interface using `wf.msc`.

\* Navigated to "Inbound Rules" to view and manage incoming traffic rules.

**2. Listed Current Firewall Rules**

\* Observed existing rules for commonly used services.

\* Verified no pre-existing rule blocking TCP port 23.

**3. Created a Rule to Block Telnet (Port 23)**

Created a new inbound rule:

\* Rule Type: Port

\* Protocol: TCP

\* Port: 23

\* Action: Block the connection

\* Profiles: Domain, Private, Public

\* Name: Block Telnet (Port 23)

**4. Tested the Block Rule**

\* Used the command:

Cmd

telnet localhost 23

**Result:**

Connecting To localhost...Could not open connection to the host, on port 23: Connect failed

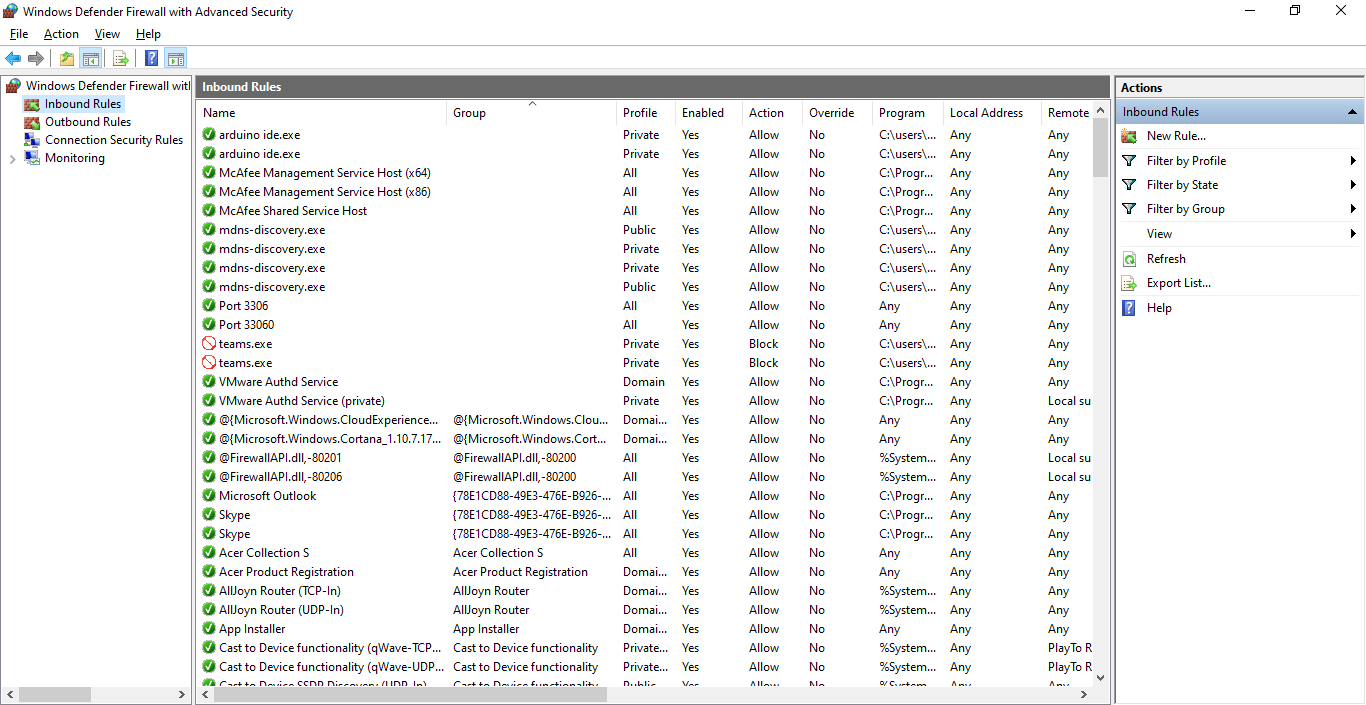
\* Confirmed firewall successfully blocked access to the Telnet service on the specified port.

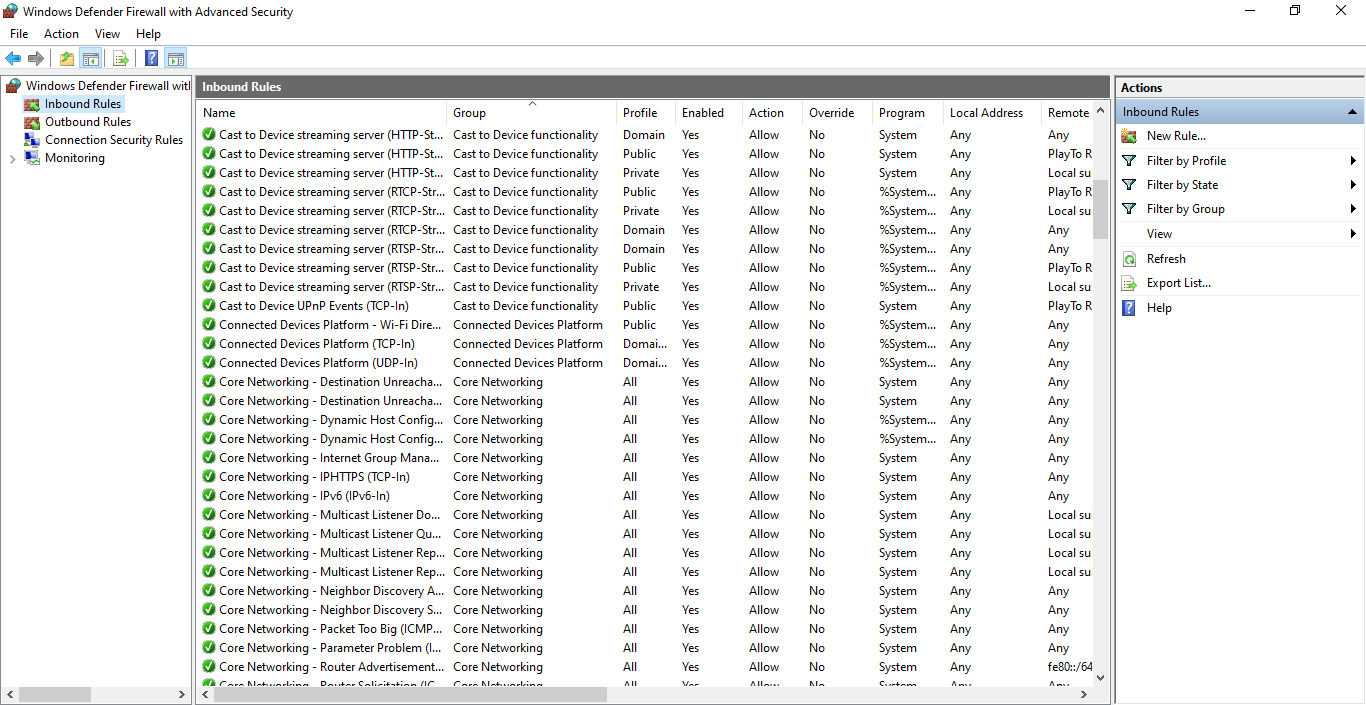
**5.Removed the Test Block Rule**

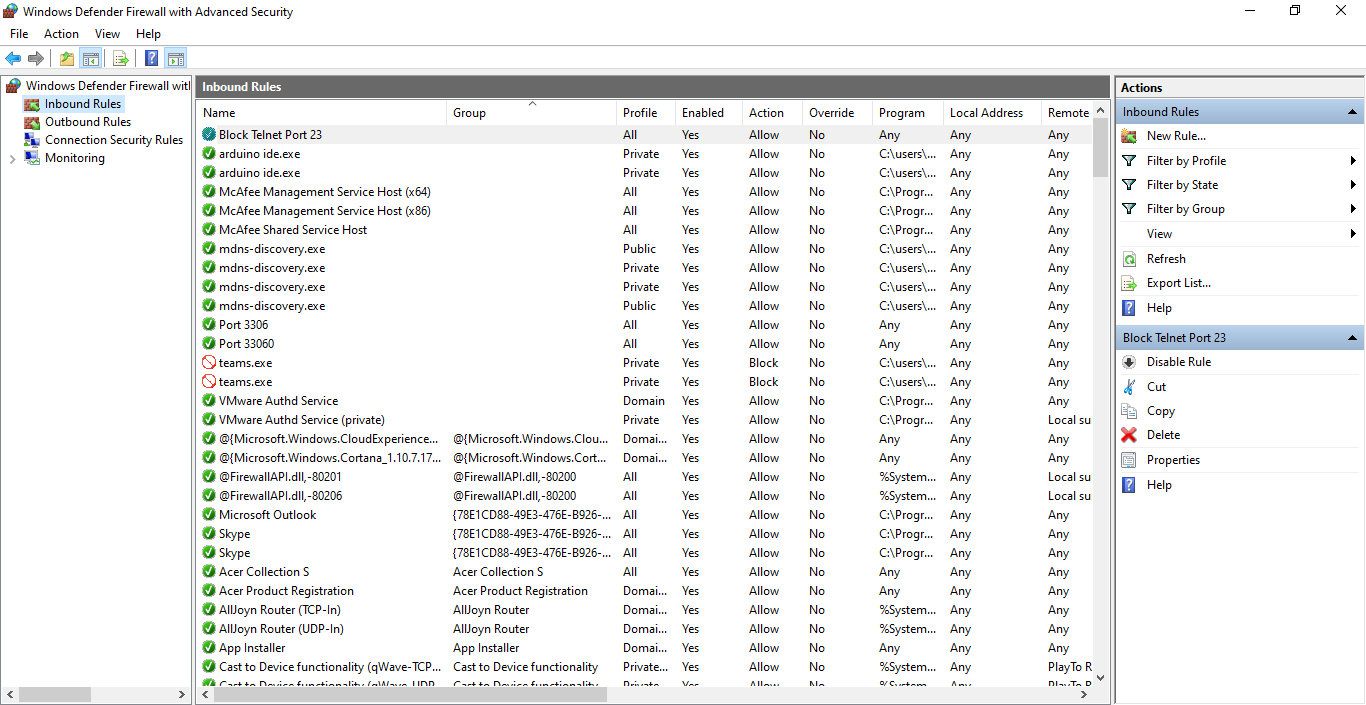
\* Deleted the `Block Telnet (Port 23)` rule to restore the firewall to its original state.

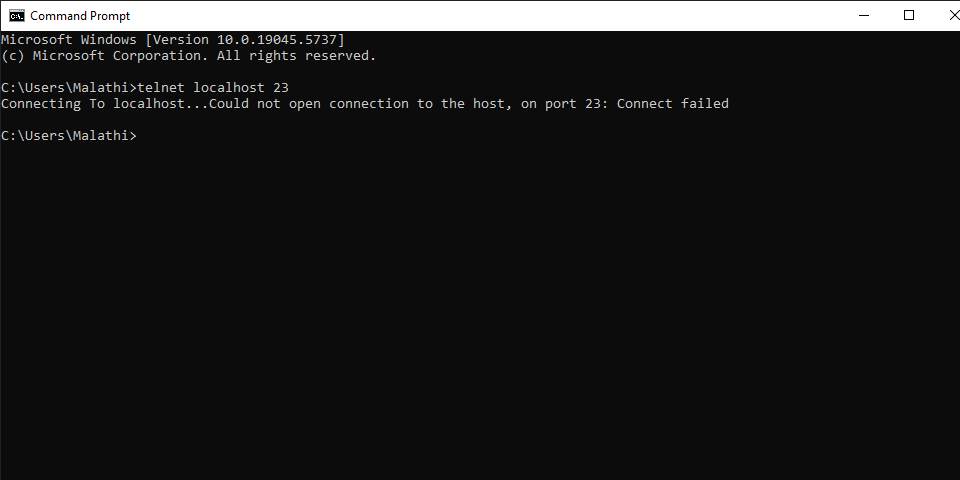
\* Ensured no residual restrictions remained after testing.

**Screenshots Captured**









**Firewall Filtering Summary**

Windows Defender Firewall allows administrators to control how incoming and outgoing network traffic is handled using rule-based configurations. Each rule can filter traffic based on:

\* Port numbers

\* Protocols (TCP/UDP)

\* Application executables

\* Source or destination IP addresses

In this task, port 23 was blocked to simulate restricting a Telnet service. The test confirmed that once the rule was applied, access was denied, demonstrating effective network filtering. This task emphasized the importance of securing unused or insecure ports to reduce the attack surface of a system.

**Outcome**

\* Gained hands-on experience in managing Windows firewall rules.

\* Demonstrated ability to:

\* Block and allow network traffic by port.

\* Verify firewall behavior using local testing.

\* Understand how firewall rules enforce system security policy.