Cyber Security Internship – Task 4 Report

Task: Configure and test firewall rules using Windows Defender Firewall.
Objective: Block inbound traffic on port 23 (Telnet), verify the rule, and remove it.

Detailed Firewall Rule Configuration Steps

Step 1: Open Windows Defender Firewall with Advanced Security

Press **Win + S** and search for **Windows Defender Firewall with Advanced Security**.
Alternatively, press **Win + R**, type **wf.msc** and press **Enter**.
This will open the advanced firewall management window.

Step 2: Create Rule to Block Port 23

In the left panel, click **Inbound Rules**. In the right panel, click **New Rule…**

In the New Inbound Rule Wizard:

Prompt	Select/Type
Rule Type	Port
TCP / UDP	TCP
Specific Local Ports	23
Action	Block the connection
Profile	Check ALL (Domain, Private, Public)
Name	Block Telnet

Click **Finish** to apply the rule.
■ *Screenshot 2 should show the final step before clicking 'Finish'*

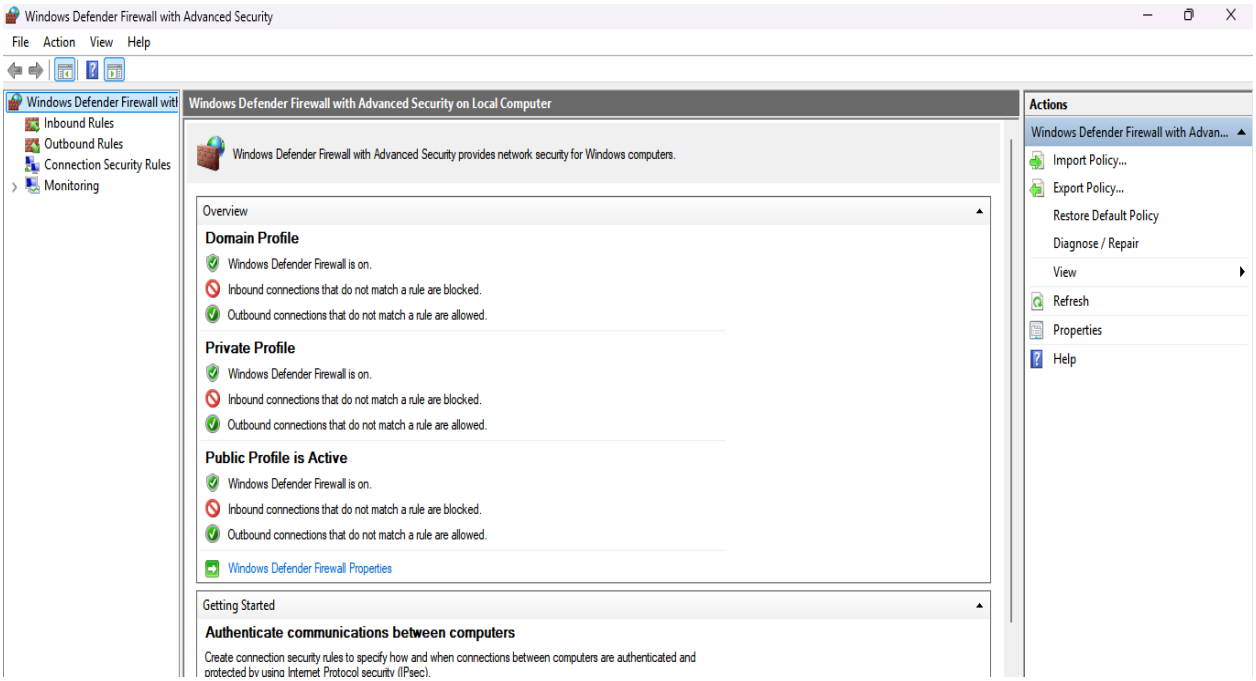
Step 3: Verify Rule Exists

After clicking **Finish**, you'll be back to the Inbound Rules list.
Look for a rule named **"Block Telnet"**
■ *Screenshot 3 should show the rule in the list*

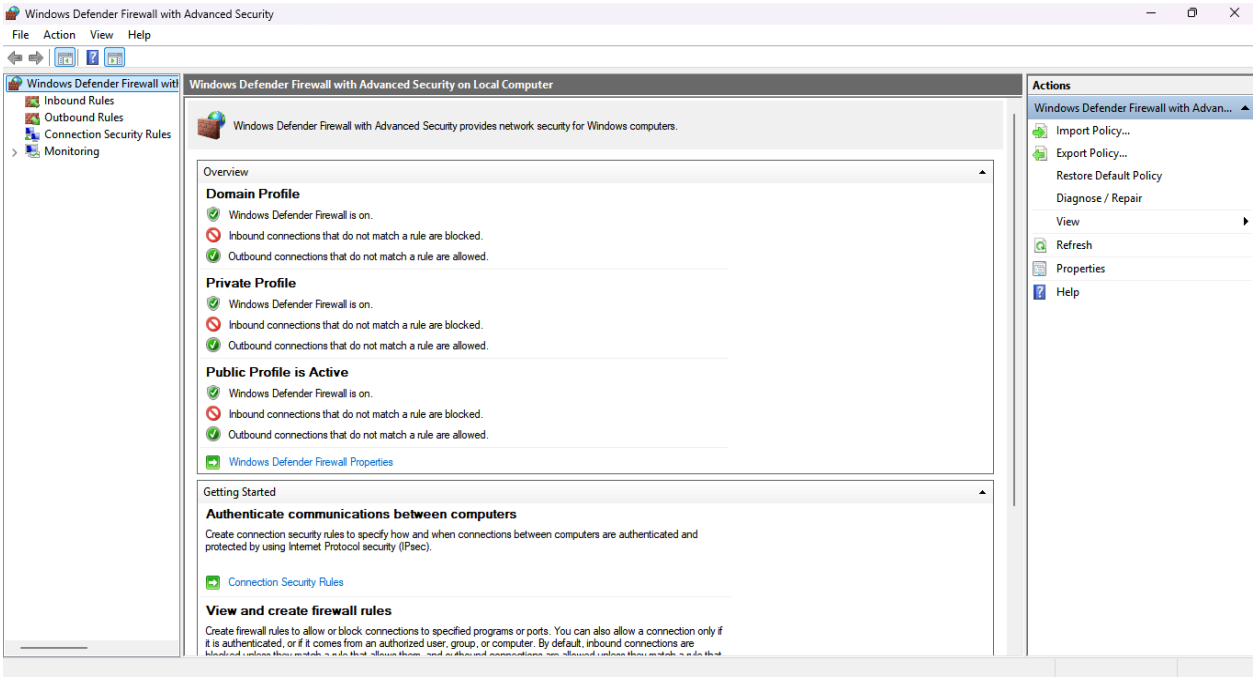
Step 4: Delete the Rule (Cleanup)

Right-click on the rule **Block Telnet** and click **Delete**
■ *Screenshot 4 should show the delete confirmation dialog*

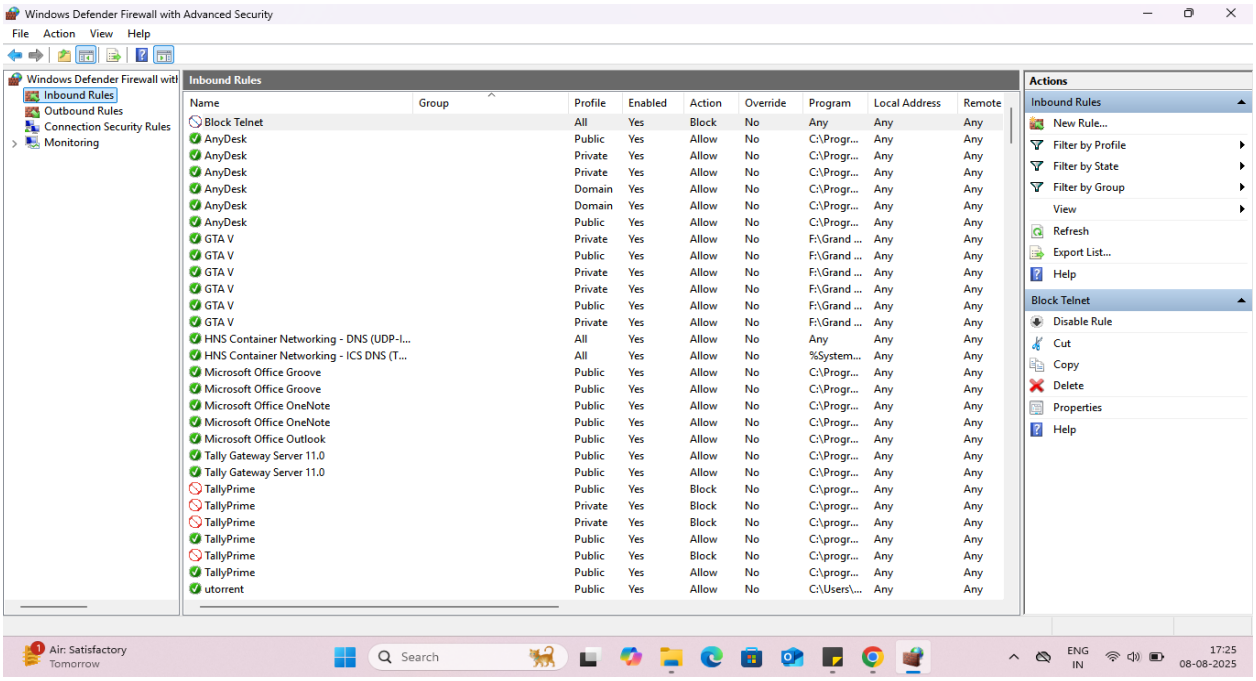
Step 1 – Firewall Overview



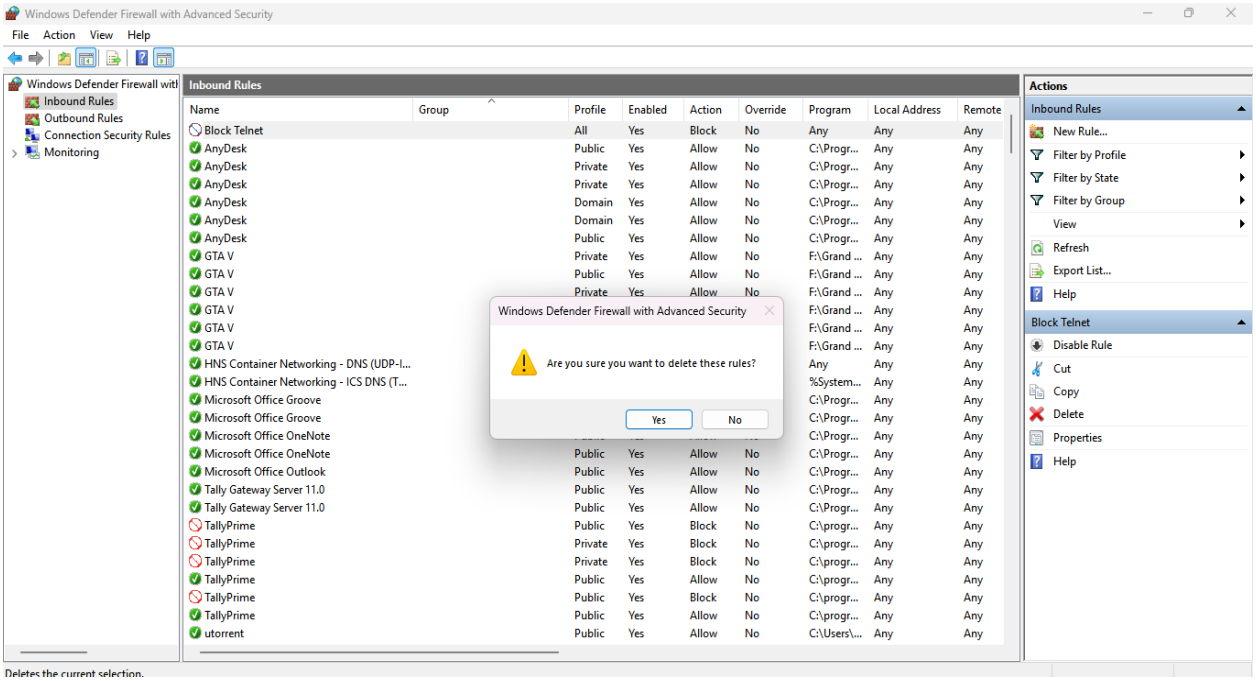
Step 2 – Creating Rule (Final Wizard Step)



Step 3 – Inbound Rules with 'Block Telnet'



Step 4 – Delete Confirmation



Conclusion

Conclusion:
Through this task, basic firewall rule management was performed using Windows Defender Firewall. A custom inbound rule was created to block traffic on Telnet port (23), confirmed in the rule list, and then safely removed. This demonstrated practical understanding of port-based traffic filtering and security rule configuration.