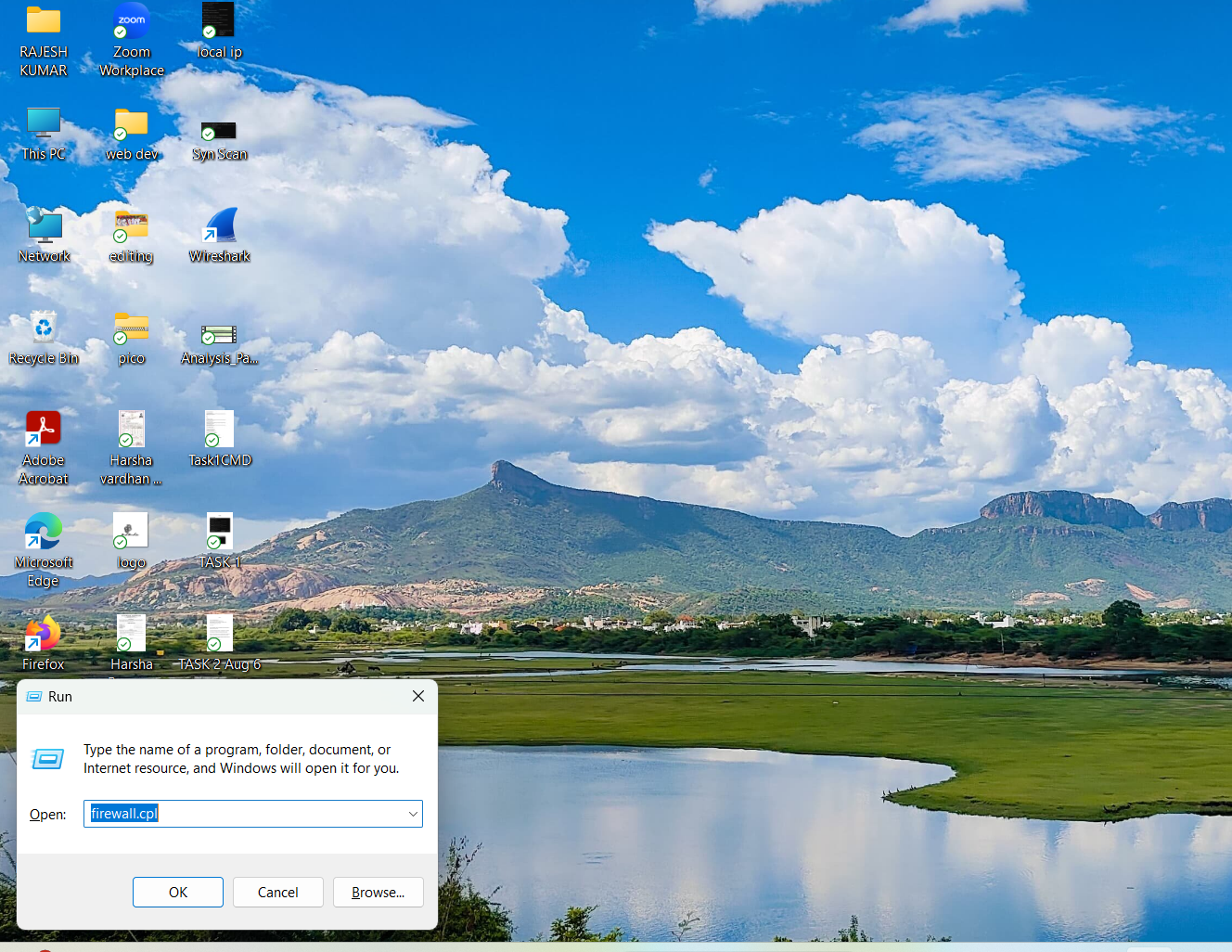
**TASK-4**

For Windows Firewall

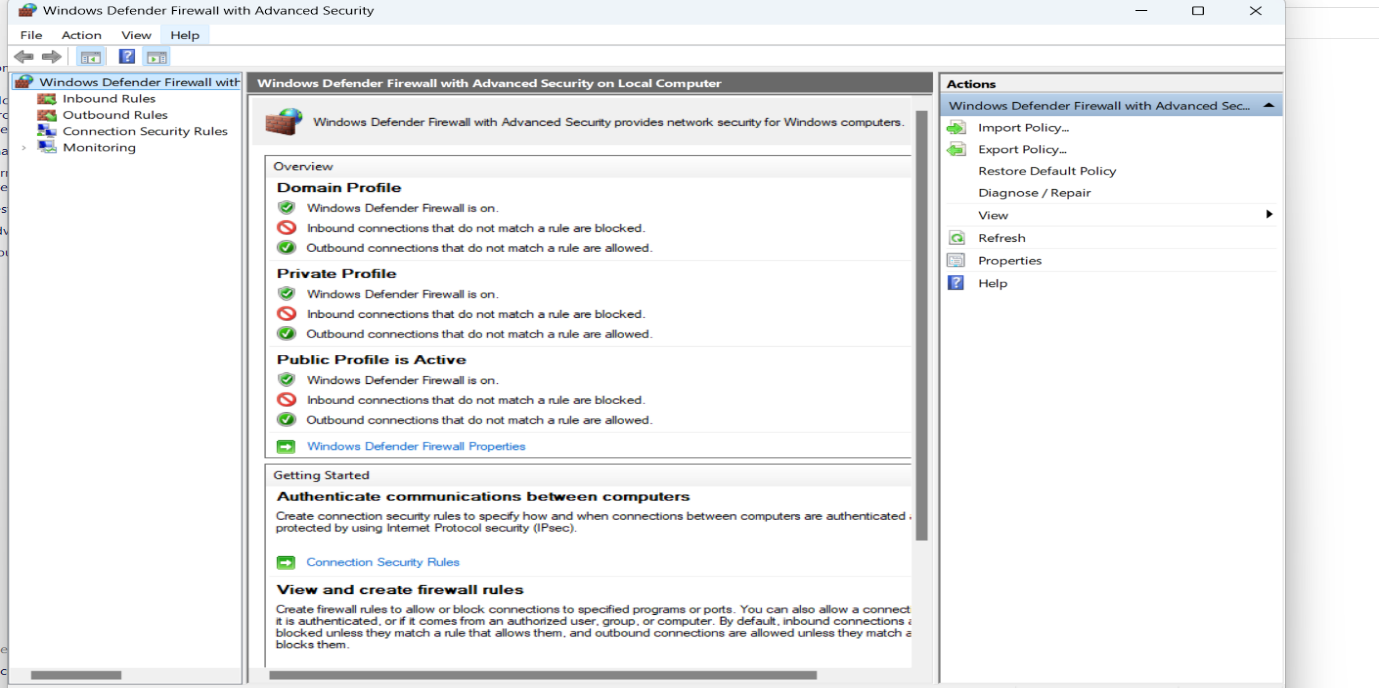
1. Open Firewall Configuration Tool

* Go to Windows press Win + R, type firewall.cpl, and Enter.



2. List Current Firewall Rules

* In the left pane, click Advanced Settings.
* This opens Windows Firewall with Advanced Security.
* Click Inbound Rules to view existing rules.



3. Add Rule to Block Port 23

* In Inbound Rules, click New Rule .
* Choose Port → TCP → Specific local ports: 23
* Select Block the connection
* Apply to Domain, Private, Public
* Name it like Block Telnet Port 23

4. Test the Rule

* Try connecting to port 23
* telnet localhost 23
* we observe a connection failure.

5. Remove the Test Block Rule

* Go back to Inbound Rules, find Block Telnet Port 23 rule.
* Right-click → Delete

**Summary:**

**Firewalls Filter Traffic**

Firewalls act as **gatekeepers** between your device and the network. They filter traffic based on rules that define:

* Direction: Inbound (coming in) or Outbound (going out)
* Protocol: TCP, UDP, ICMP, etc.
* Port: Specific services (e.g., 22 for SSH, 80 for HTTP)
* IP Address: Source or destination filtering

**Filtering Logic**

* Allow Rule: Permits traffic that matches criteria
* Deny/Block Rule: Prevents traffic from passing through
* Default Policy: If no rule matches, the firewall applies a default (usually deny)

**Interview Questions**

**1. What Is a Firewall?**

A firewall is a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet).

* Can be hardware-based, software-based, or both
* Filters traffic based on IP addresses, ports, protocols, and more
* Helps prevent unauthorized access, malware, and data breaches

**2. Difference Between Stateful and Stateless Firewall**

| Feature | Stateful Firewall | Stateless Firewall |
| --- | --- | --- |
| Traffic Awareness | Tracks the state of active connections | Treats each packet independently |
| Security Level | More secure and intelligent | Faster but less secure |
| Performance | Slightly slower due to connection tracking | Faster due to simplicity |
| Use Case | Ideal for complex networks | Suitable for simple, high-speed filtering |

**3. What Are Inbound and Outbound Rules?**

* Inbound Rules: Control traffic coming *into* your network or device.  
  Example: Allow HTTP (port 80) traffic to a web server.
* Outbound Rules: Control traffic going *out* from your network or device.  
  Example: Block access to external FTP servers.

**4. How Does UFW Simplify Firewall Management?**

UFW (Uncomplicated Firewall) is a user-friendly frontend for managing iptables on Linux systems.

* Uses simple command-line syntax (e.g., ufw allow 22)
* Automatically handles rule ordering and syntax
* Ideal for beginners and quick configuration
* Supports profiles and logging

**5. Why Block Port 23 (Telnet)?**

Telnet (port 23) is outdated and insecure because it transmits data—including passwords—in plain text.

* Vulnerable to eavesdropping and man-in-the-middle attacks
* Replaced by SSH (port 22), which encrypts communication
* Blocking port 23 helps prevent unauthorized remote access

**6. Common Firewall Mistakes**

* ❌ Allowing too many open ports
* ❌ Misconfigured rules (e.g., overly permissive)
* ❌ Forgetting to block outbound traffic
* ❌ Not updating firewall rules with network changes
* ❌ Disabling logging, making troubleshooting harder
* ❌ Relying solely on firewalls without other security layers

**7. How Does a Firewall Improve Network Security?**

* Filters malicious traffic before it reaches internal systems
* Prevents unauthorized access to sensitive resources
* Enforces network segmentation and access control
* Helps detect and block suspicious activity
* Supports compliance with security policies and regulations

**8. What Is NAT in Firewalls?**

NAT (Network Address Translation) allows multiple devices on a private network to share a single public IP address.

* Purpose: Conserves IP addresses and hides internal network structure
* In Firewalls: NAT is often integrated to route traffic between internal and external networks
* Types: Static NAT, Dynamic NAT, and PAT (Port Address Translation)