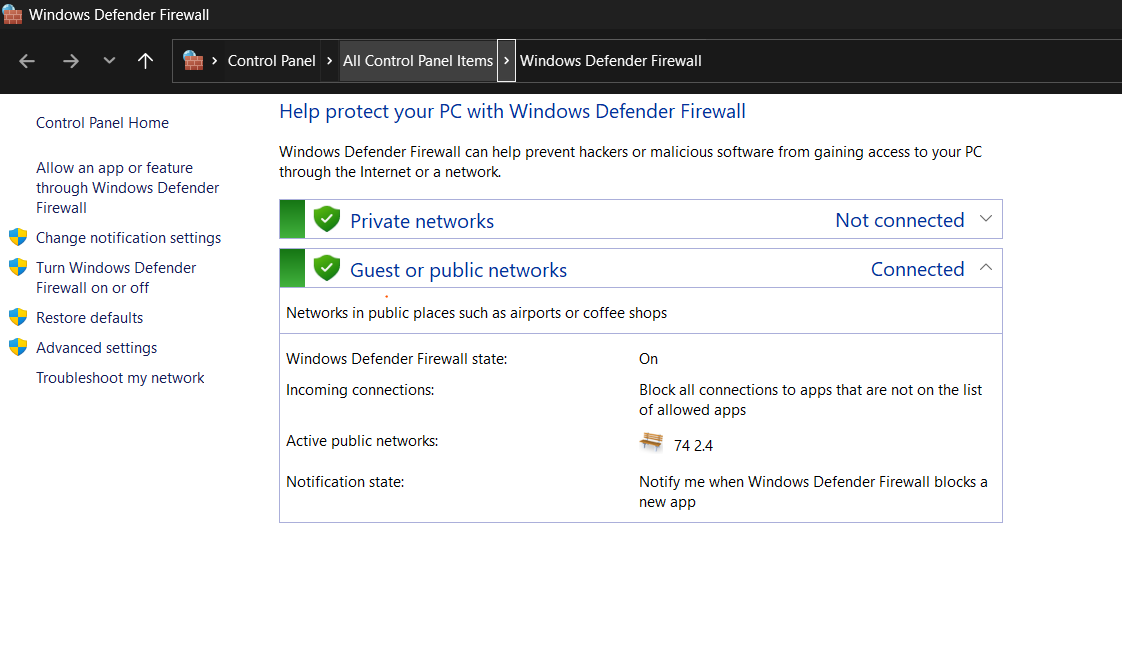
**Task 4: Setup and Use a Firewall on Windows/Linux**

***Objective****: Configure and test basic firewall rules to allow or block traffic.*

**Tools**: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

**1. Interface**



**2. Firewall Rules**

A screenshot of a computer

AI-generated content may be incorrect.

**2.1 Inbound Rules**

A screenshot of a computer

AI-generated content may be incorrect.

**2.2 Outbound Rules**

A screenshot of a computer

AI-generated content may be incorrect.

**3. Add a rule to block inbound traffic on a specific port**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

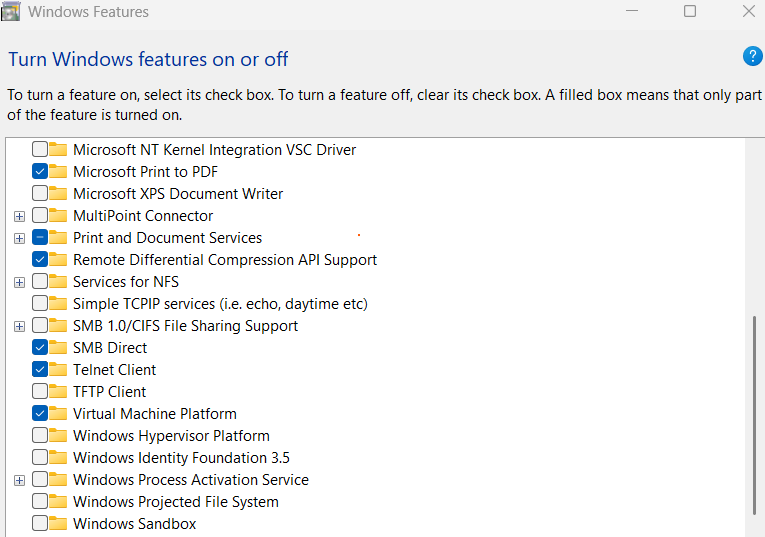
A screenshot of a computer

AI-generated content may be incorrect.



**4. Test the rule by attempting to connect to that port locally or remotely. Test the rule by attempting to connect to that port locally or remotely**

*-> (If Telnet client isn’t installed, enable it: Control Panel → Programs → Turn Windows features on/off → enable Telnet Client).*

**

Then run the command: ***telnet [host ip] 23***

A screenshot of a computer

AI-generated content may be incorrect.



**5. Summarise How Firewall Filters Traffic**

A firewall works like a **security guard** for your computer. It decides whether to **allow or block traffic** based on defined rules:

* **Inbound rules**: Control traffic entering your system (e.g., blocking Telnet on port 23).
* **Outbound rules**: Control traffic *leaving* your system (e.g., preventing an app from accessing the internet).
* Rules are based on **port numbers, protocols (TCP/UDP), IP addresses, or applications**.
* When traffic tries to pass through, the firewall checks the rules:
  + If **allowed** → traffic passes.
  + If **blocked** → traffic is dropped.

In Our test: Blocking port **23** stopped Telnet connections, proving how the firewall filters unwanted access while allowing other safe traffic.