**Windows Firewall Configuration**

**1. Open Windows Firewall**

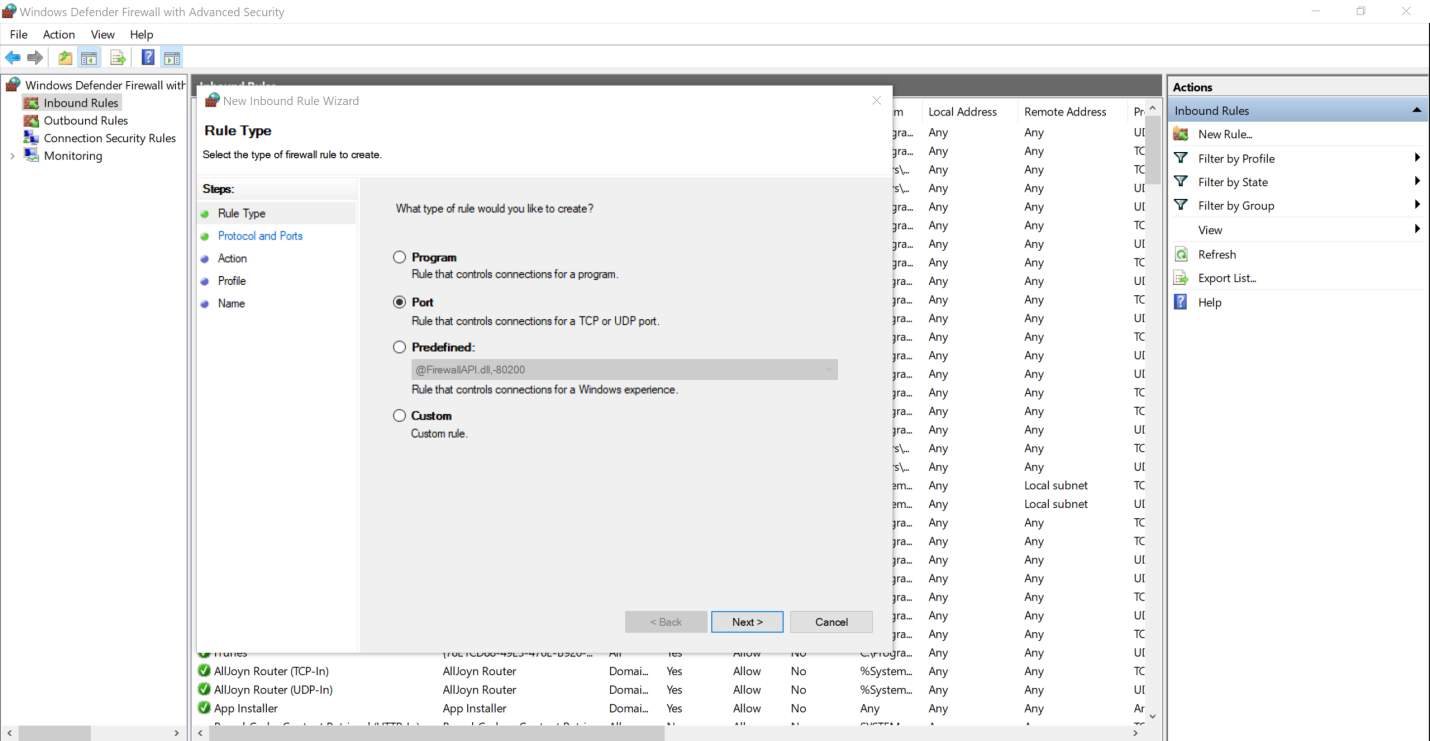
* Go to **Start Menu** → Search **“Windows Defender Firewall with Advanced Security”**
* Open the **Advanced Security** interface.

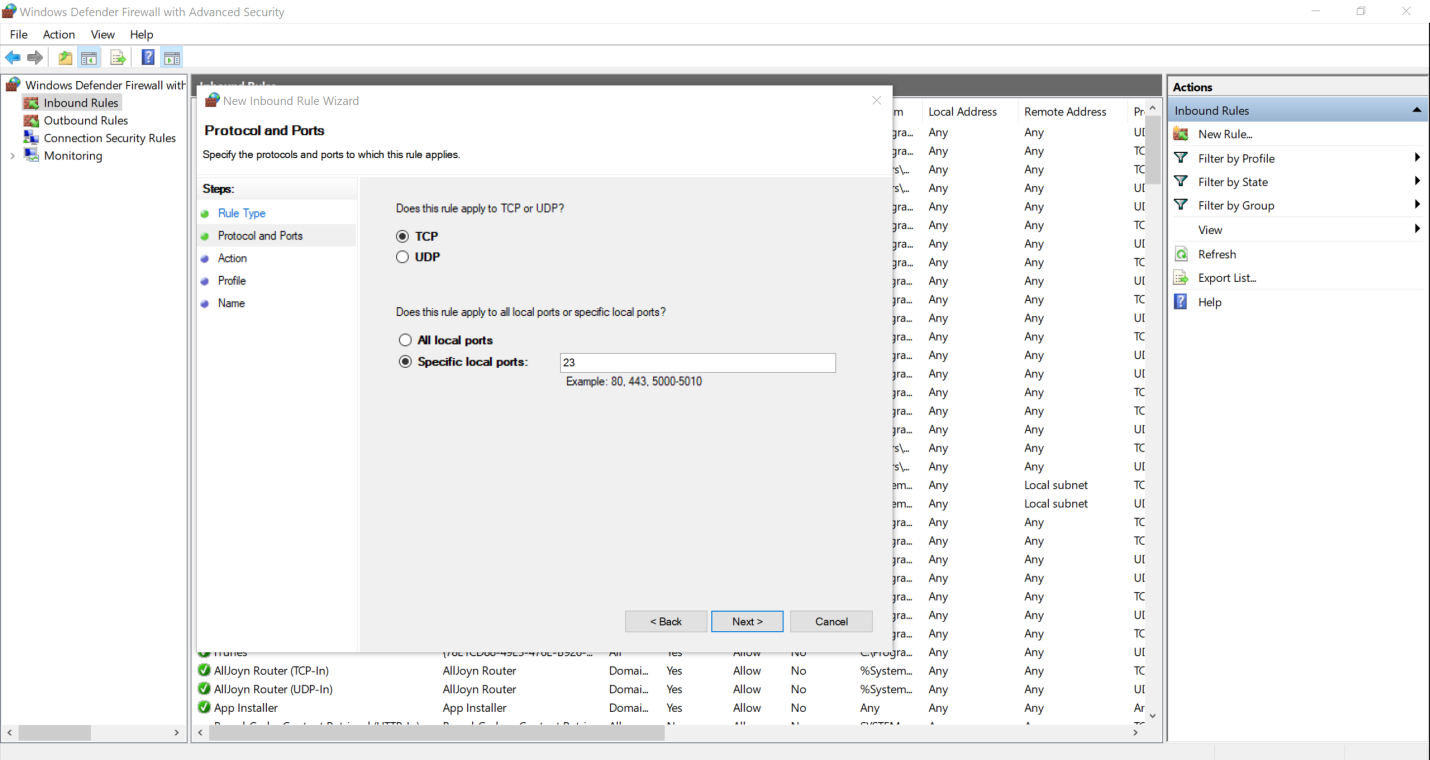
**2. List Current Rules**

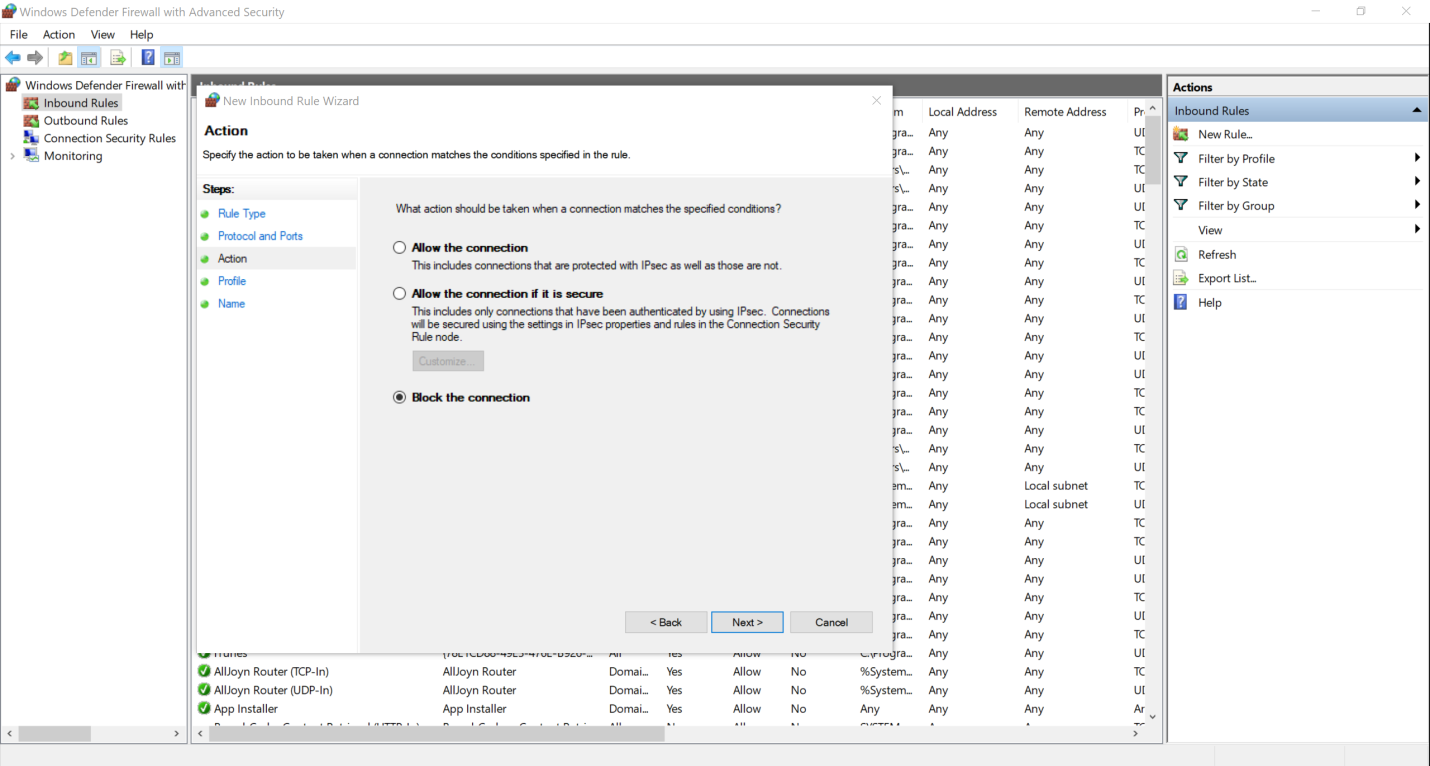
* On the left panel: Click **Inbound Rules** and **Outbound Rules**
* Observe the current rules listed

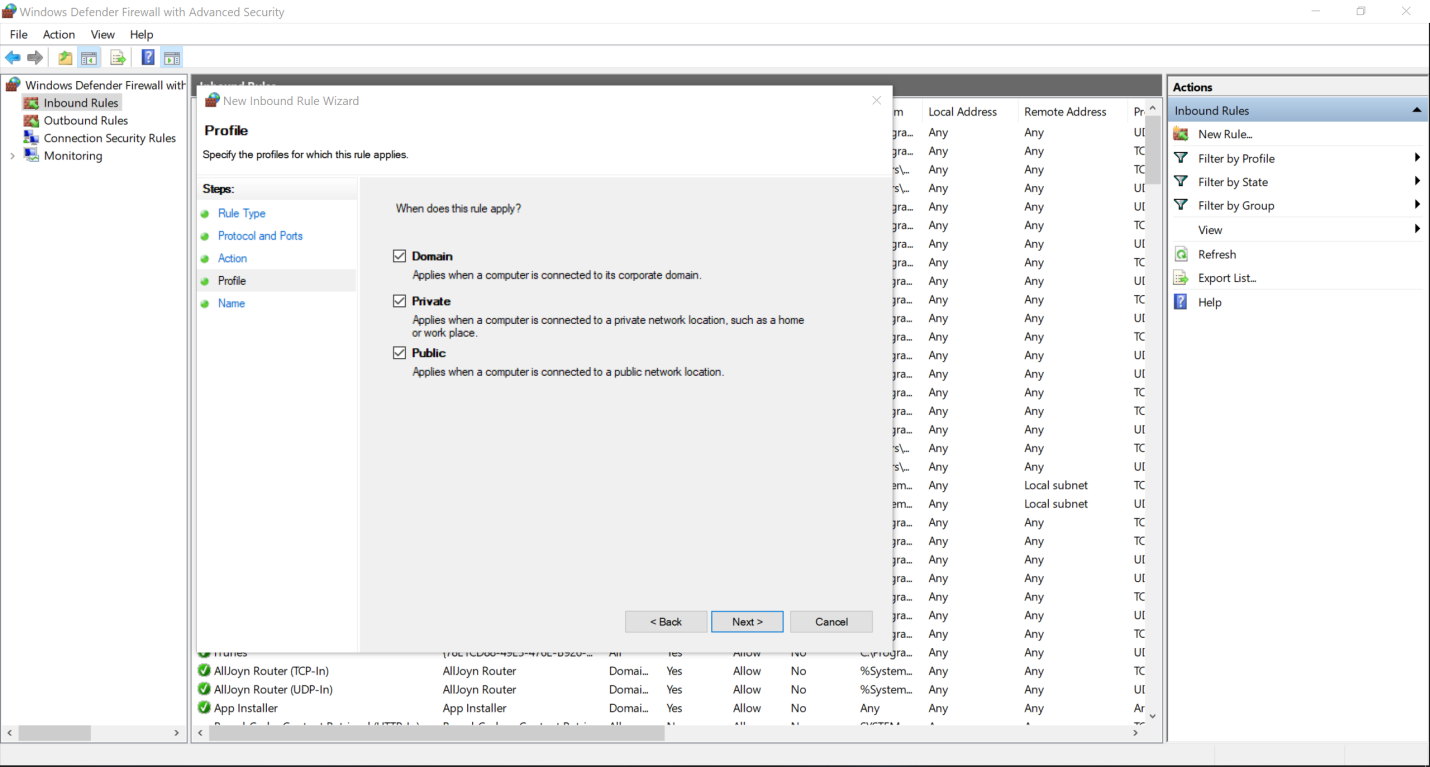
### 3. ****Create a Rule to Block Inbound Traffic on Port 23 (Telnet)****

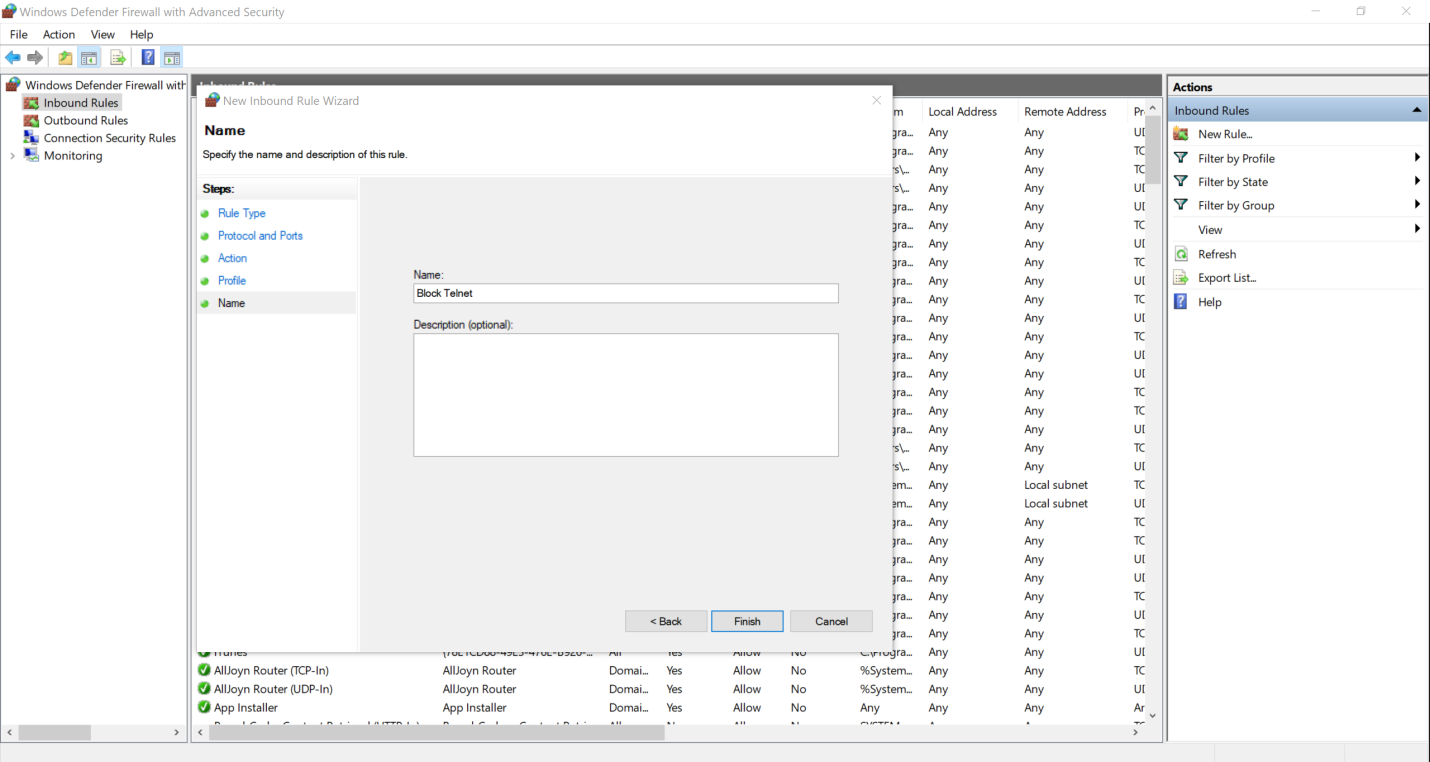
* In **Inbound Rules**, click **“New Rule…”**
* Choose: **Port** → Click **Next**
* Choose: **TCP** → Enter port: 23 → Click **Next**
* Choose: **Block the connection** → Click **Next**
* Apply to **Domain, Private, Public** → Click **Next**
* Name the rule: Block Telnet → Click **Finish**

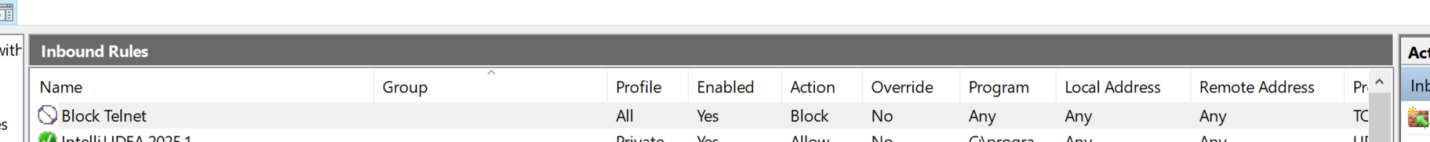






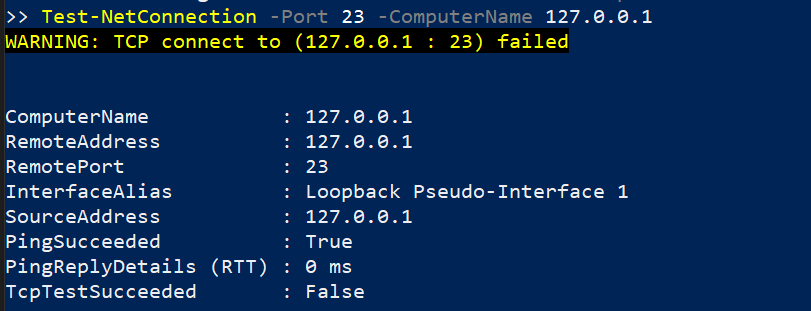






### 4. ****Test the Rule****

* Try connecting to localhost:23



## How Firewalls Filter Traffic

A firewall works by filtering **incoming and outgoing traffic** based on pre-configured rules. Each rule controls access to specific **ports**, **protocols**, or **IP addresses**.

* **Inbound Rules**: Control what external traffic can reach your computer
* **Outbound Rules**: Control what your computer can send to the network
* **Allow Rules**: Let traffic pass
* **Deny/Block Rules**: Drop or reject traffic

Firewalls protect systems by **blocking unwanted or harmful traffic**, such as Telnet (often abused by attackers), while **allowing trusted services** like SSH for remote administration.