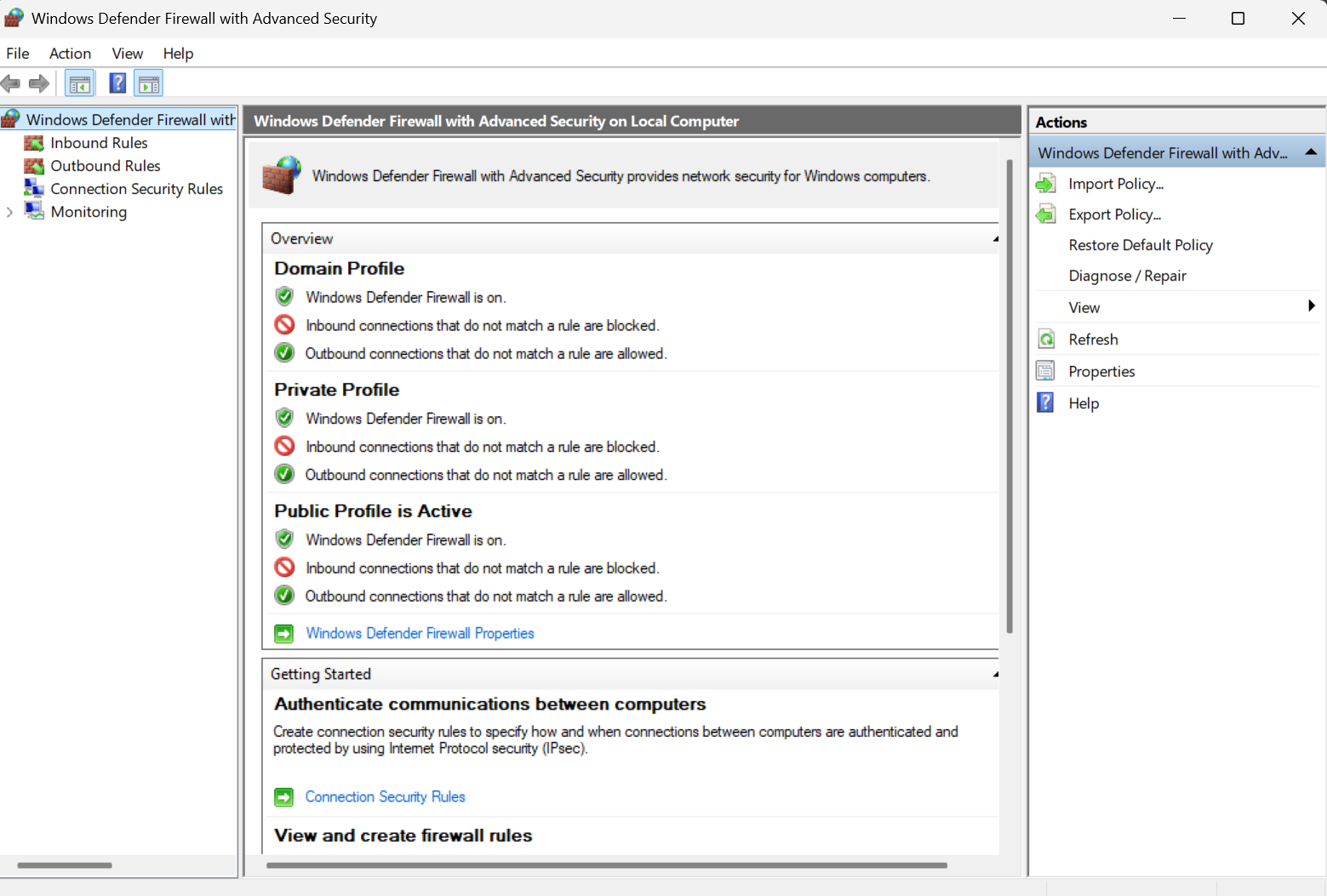
Cyber Security Internship Task 4.

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

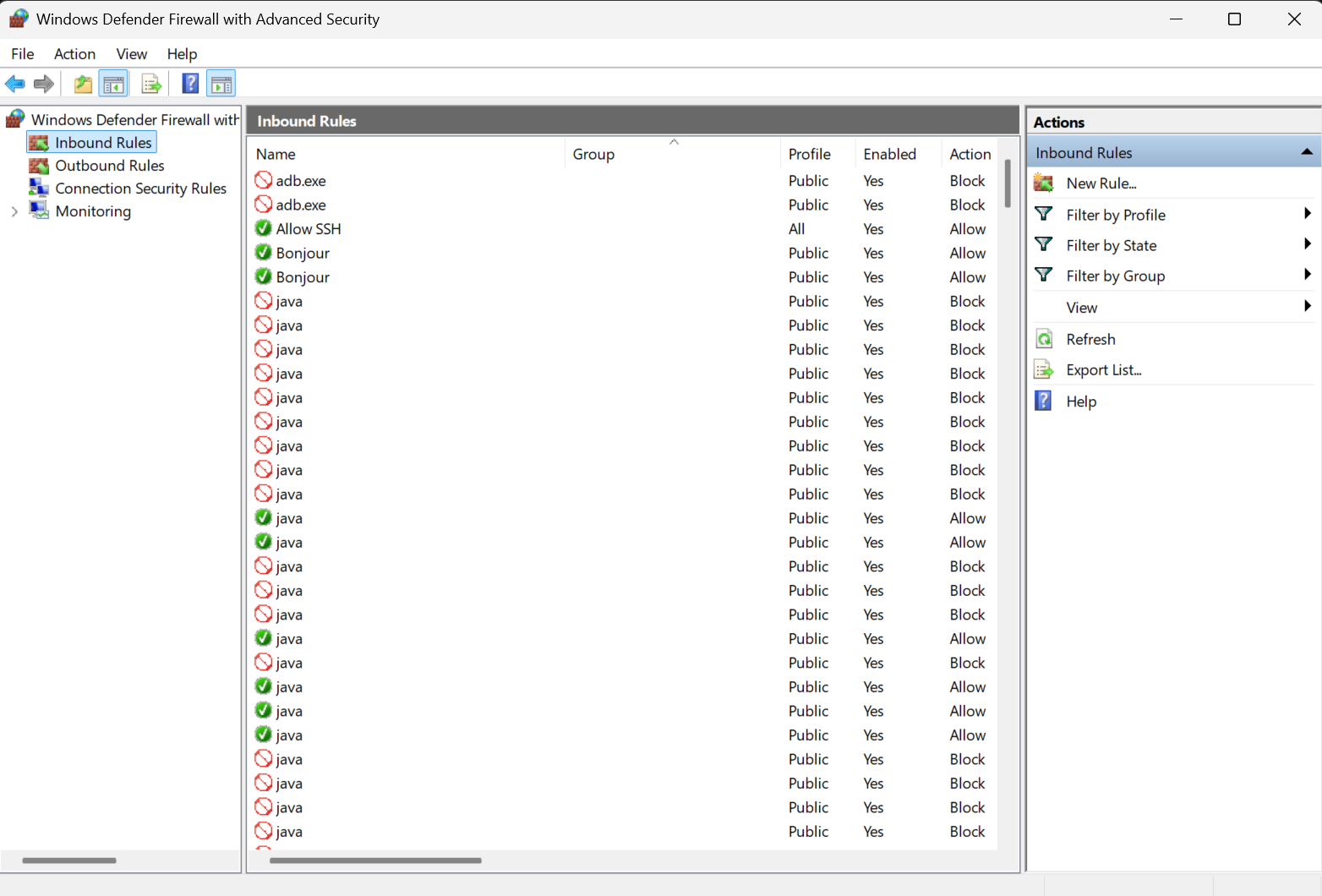
1. Open firewall configuration tool.

I opened the **Windows Defender Firewall with Advanced Security** console by pressing **Win + R**, typing wf.msc, and hitting **Enter**.



2.List current firewall rules.

Once in the console, I clicked **Inbound Rules** in the left pane. This displayed all existing firewall rules for inbound traffic (including name, enabled/disabled, action, ports, etc.).



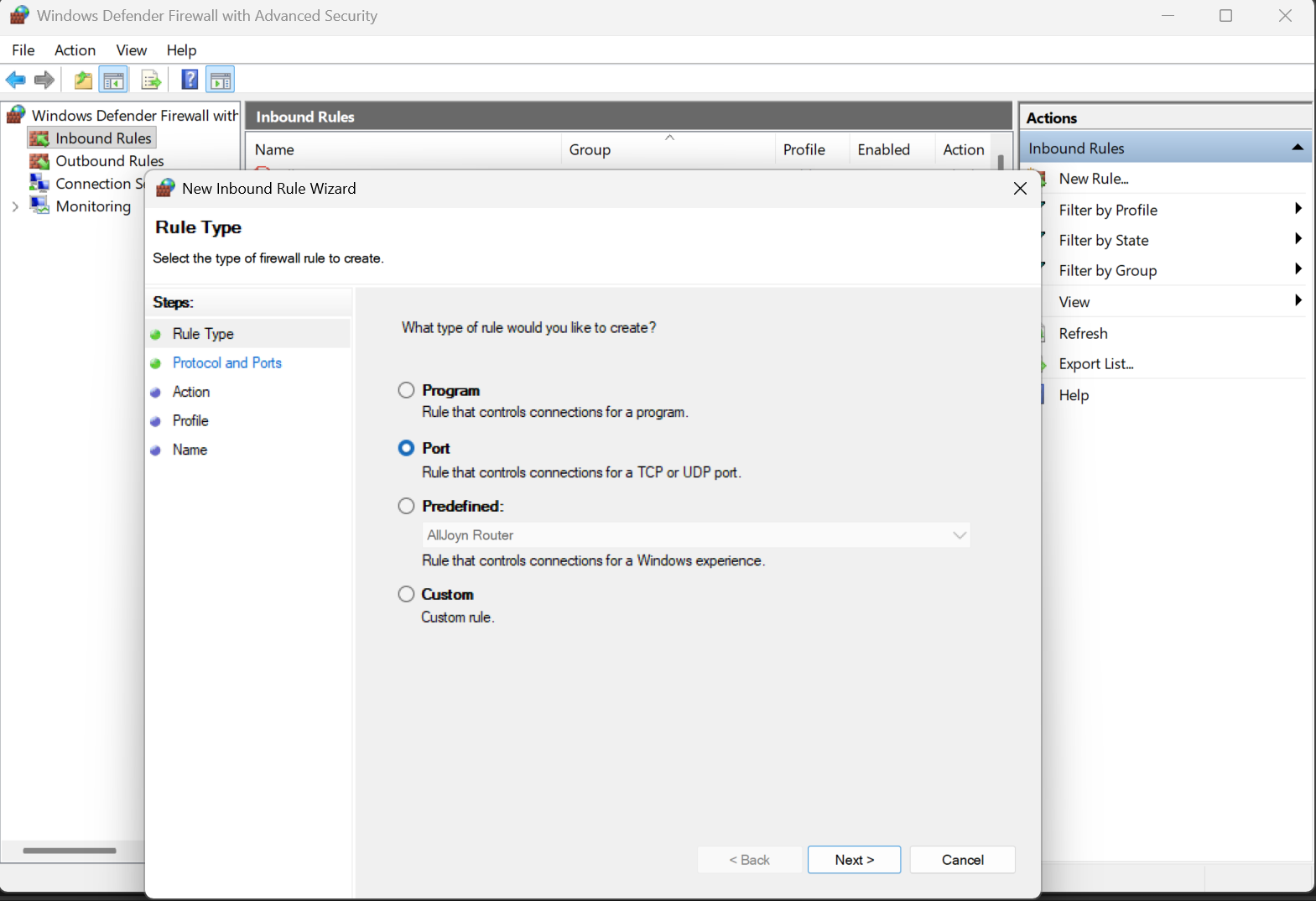
-------------------------------------------------------------------------

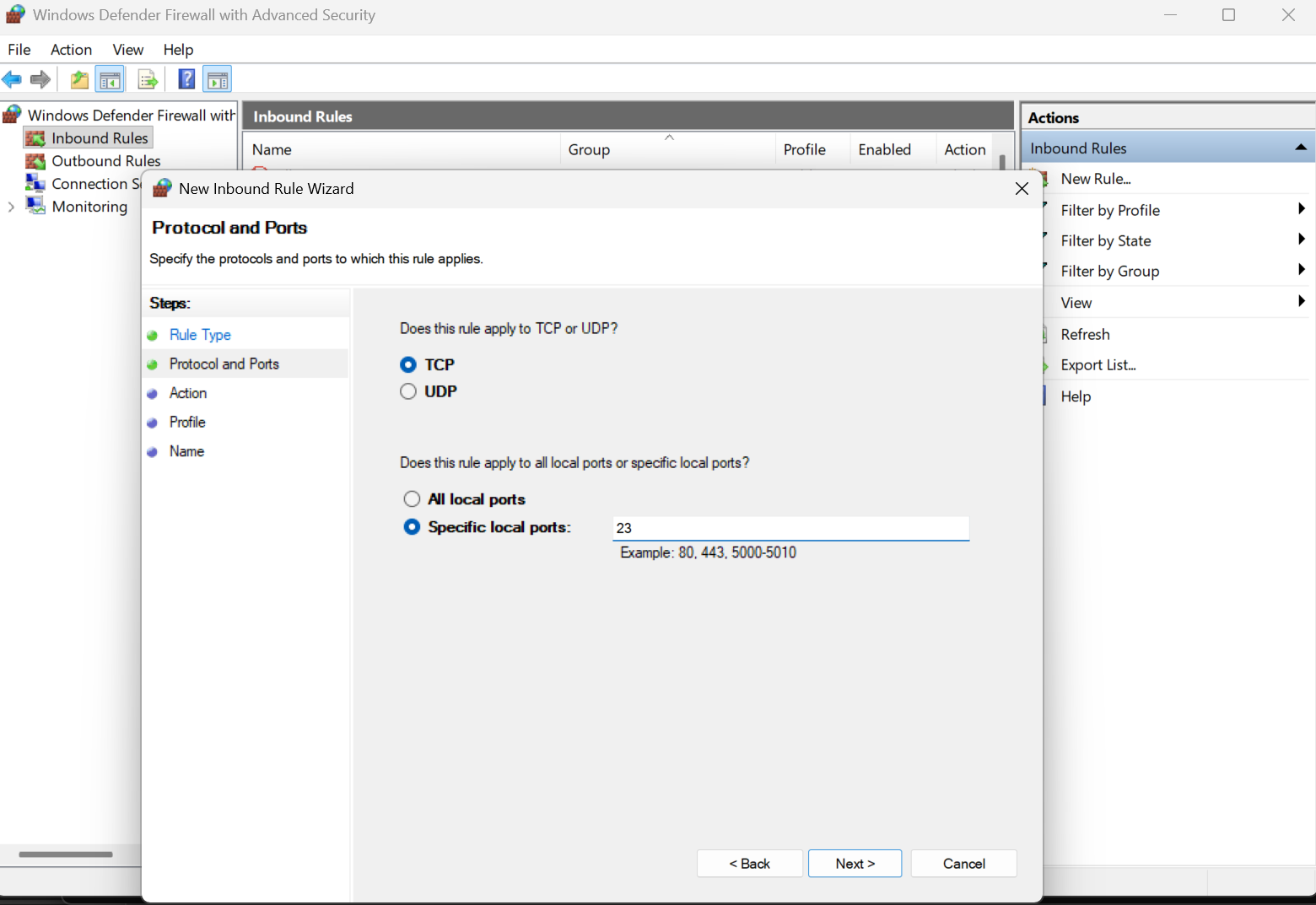
3.Add a rule to block inbound traffic on a specific port (port 23 – Telnet).

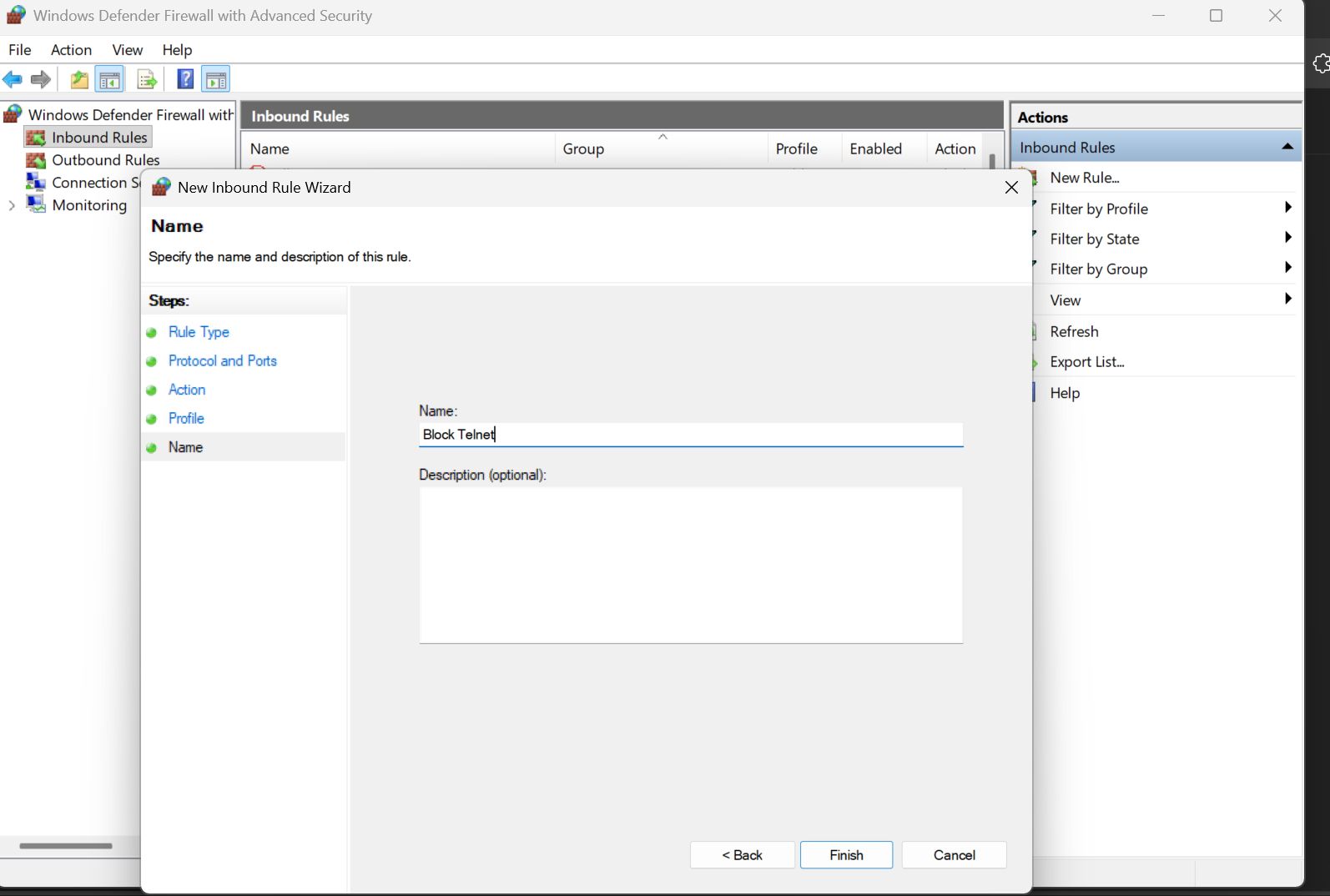
Steps I used:

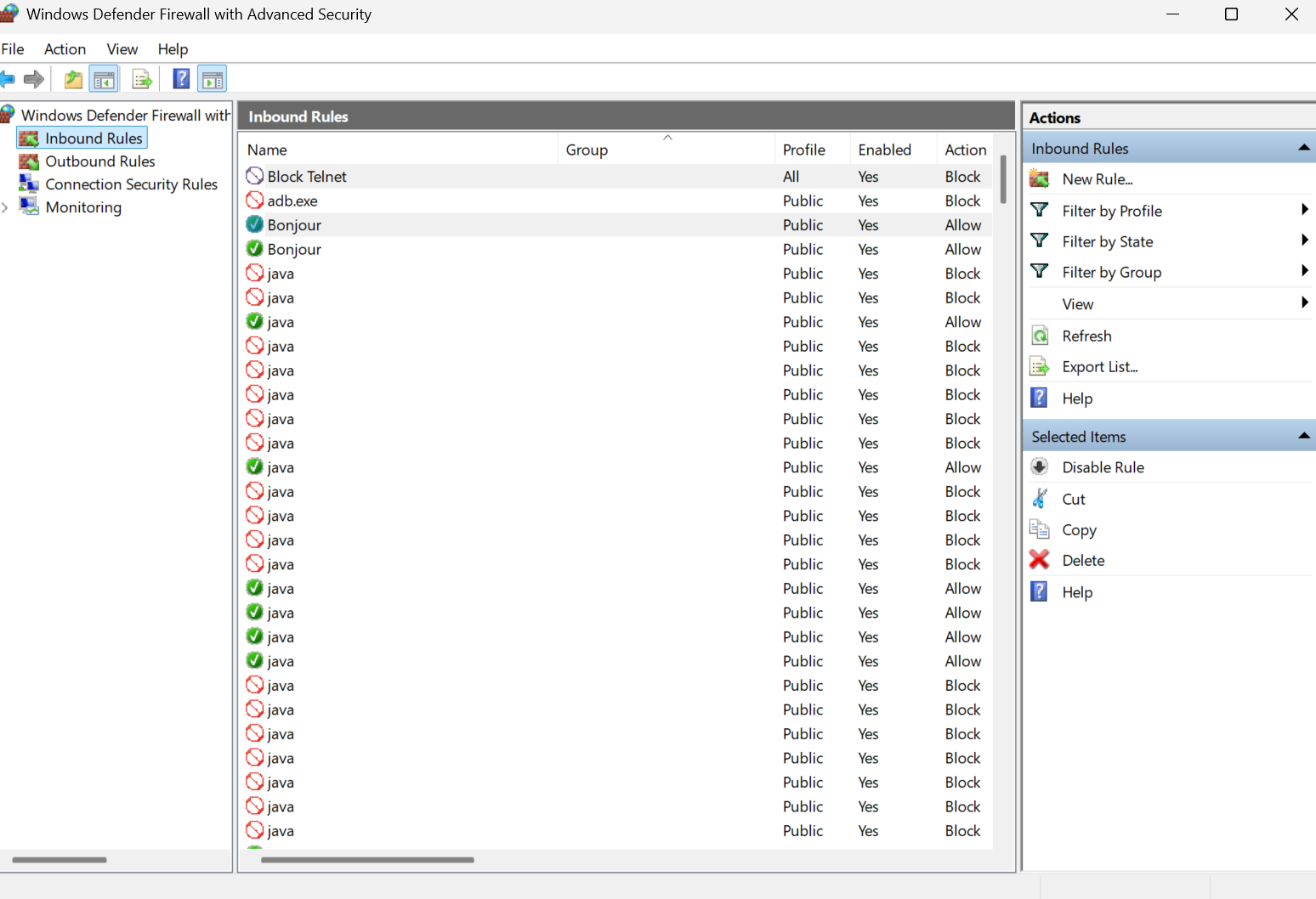
1. In **Inbound Rules**, click **New Rule…** in the right Actions pane.
2. Choose **Port** → Click **Next**.
3. Select **TCP**, then **Specific local ports**, and enter 23.
4. Choose **Block the connection** → **Next**.
5. Apply to **Domain, Private, Public** → **Next**.
6. Give the rule a name, e.g. **Block Telnet**, and click **Finish**.

This rule ensures any inbound attempt to open port 23 (Telnet) will be denied.







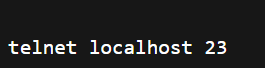


-------------------------------------------------------------------------

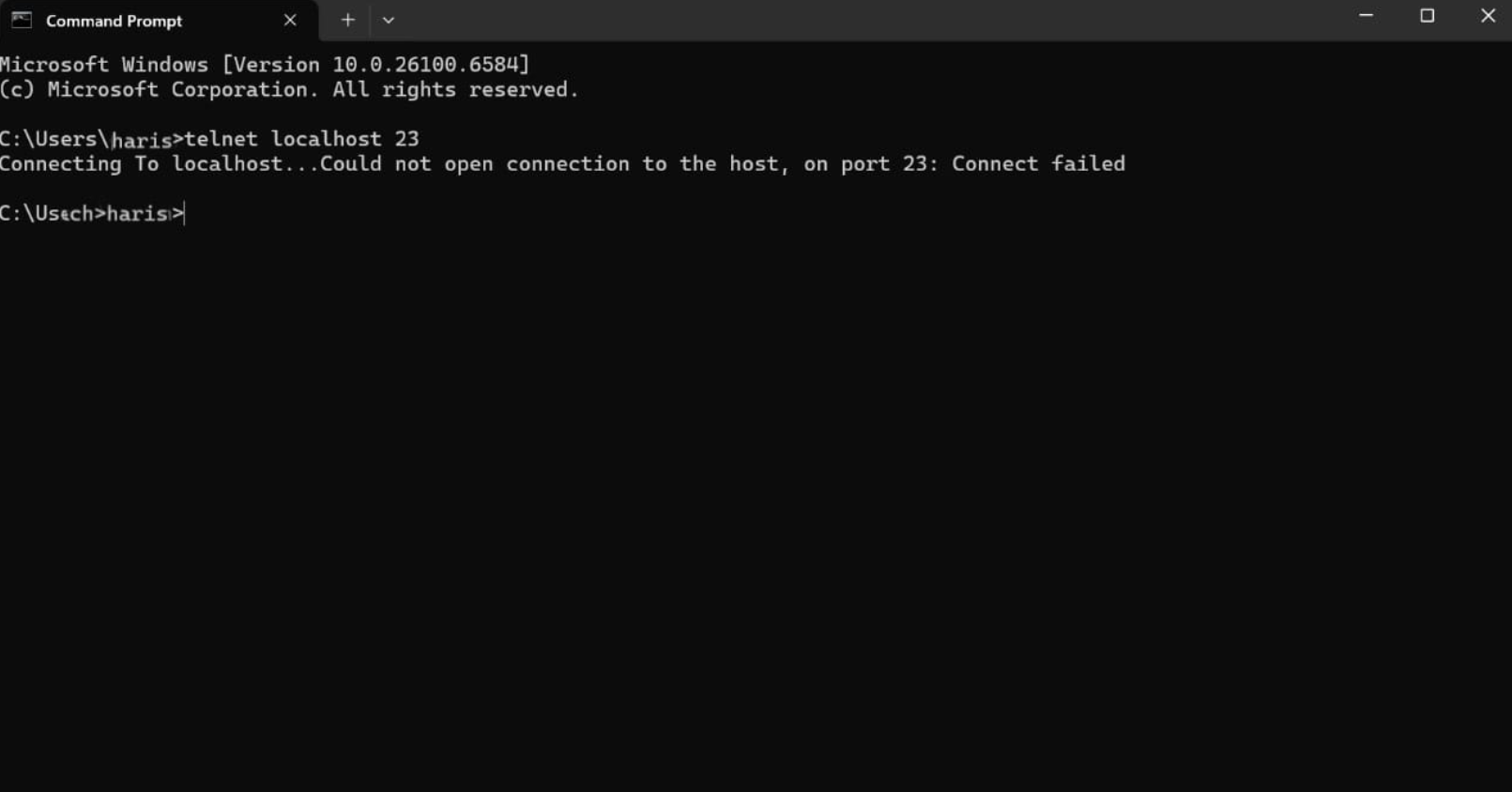
4. Test the Rule with CMD.

Since Telnet is not installed by default:

1. First, install Telnet Client (one-time):
   * Press **Win + R** → type optionalfeatures → Enter.
   * Check **Telnet Client** → OK.
2. Open **Command Prompt** (cmd).  
   Run:



If the firewall block is active, you’ll see:



-------------------------------------------------------------------

5. Add a Rule to Allow SSH (Port 22).

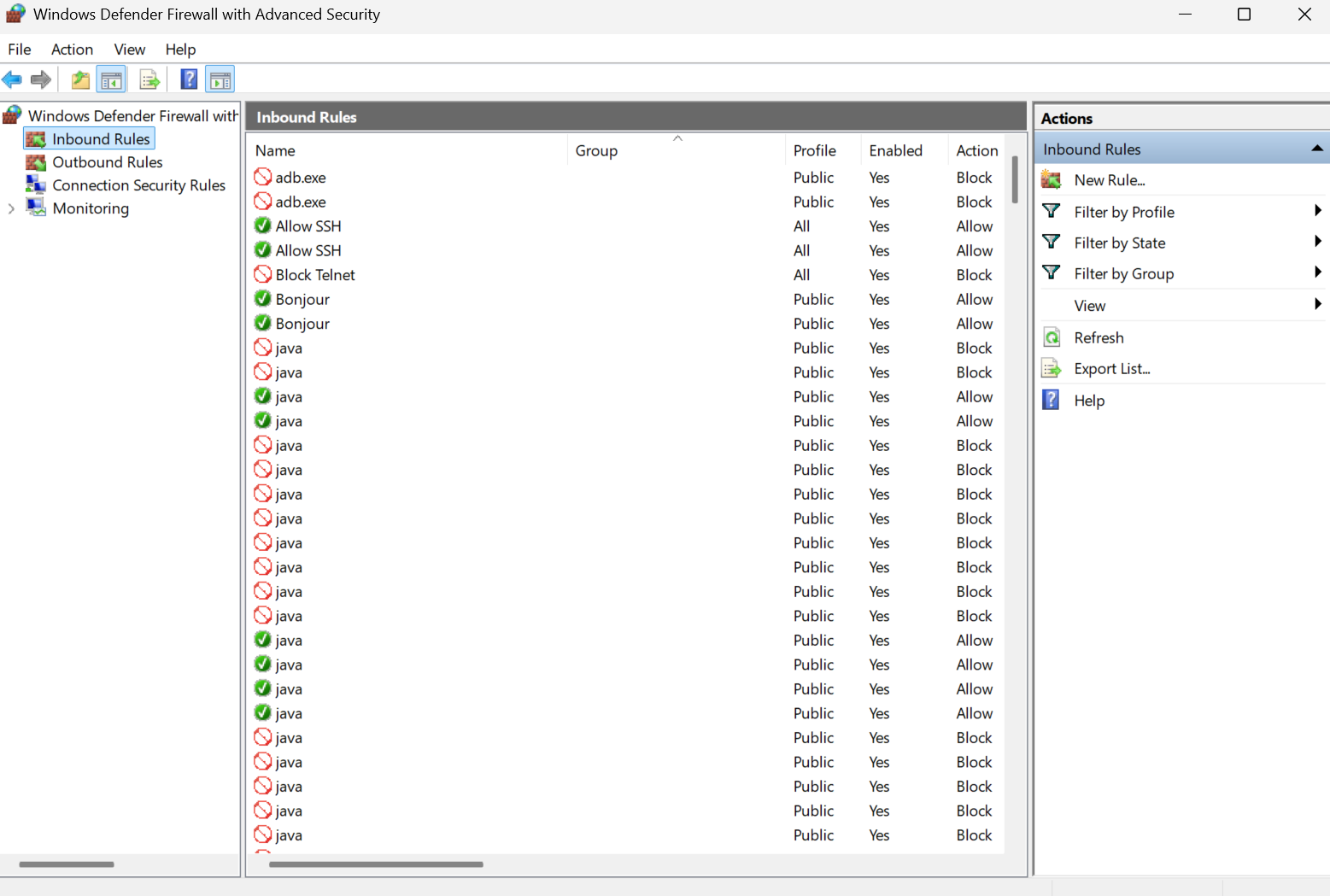
\* Go back to **Inbound Rules → New Rule**.

\* Choose **Port → TCP → Specific port: 22**.

\* Select **Allow the connection**.

\* Apply to **Domain, Private, Public**.

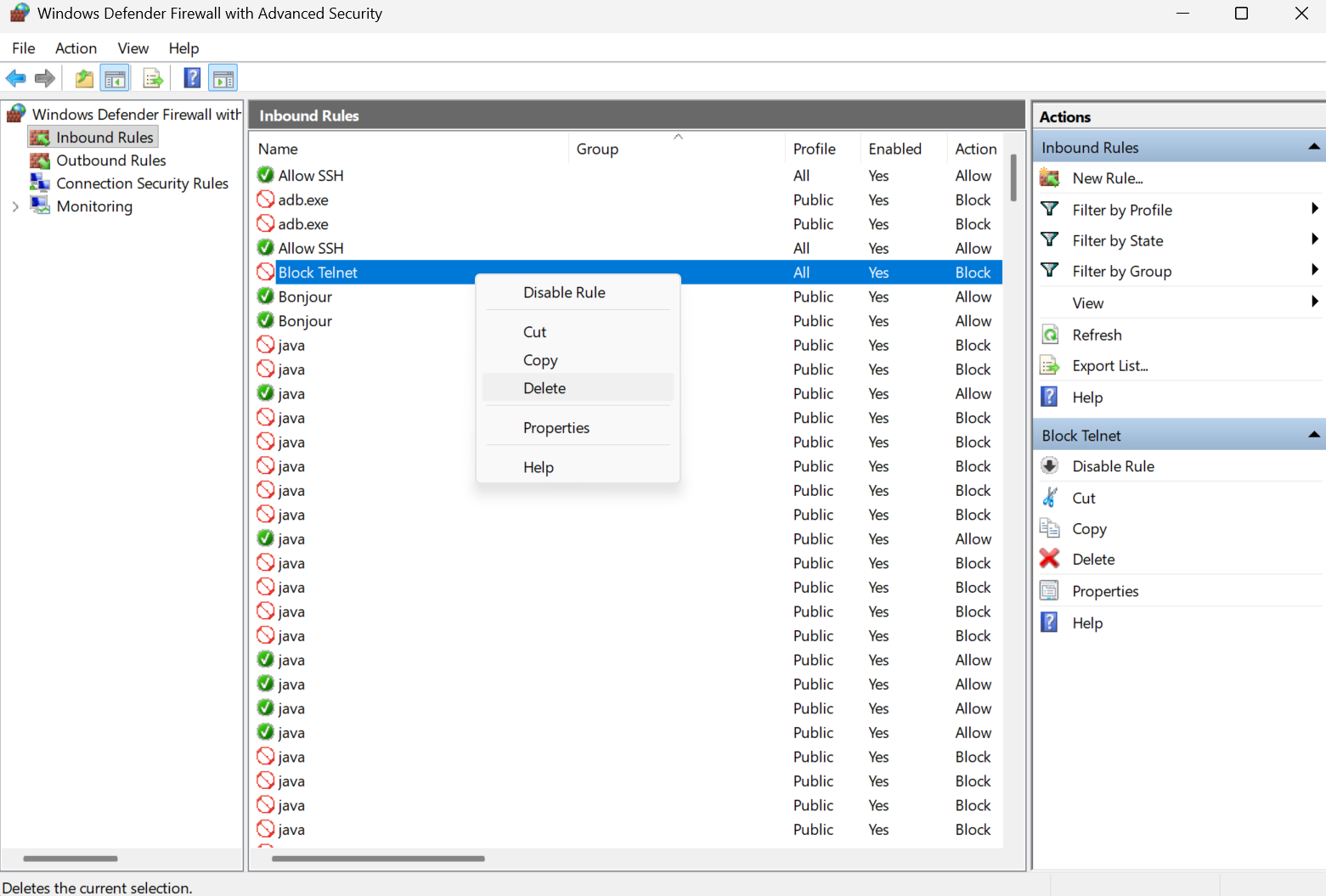
\* Name it **Allow SSH** → Finish.

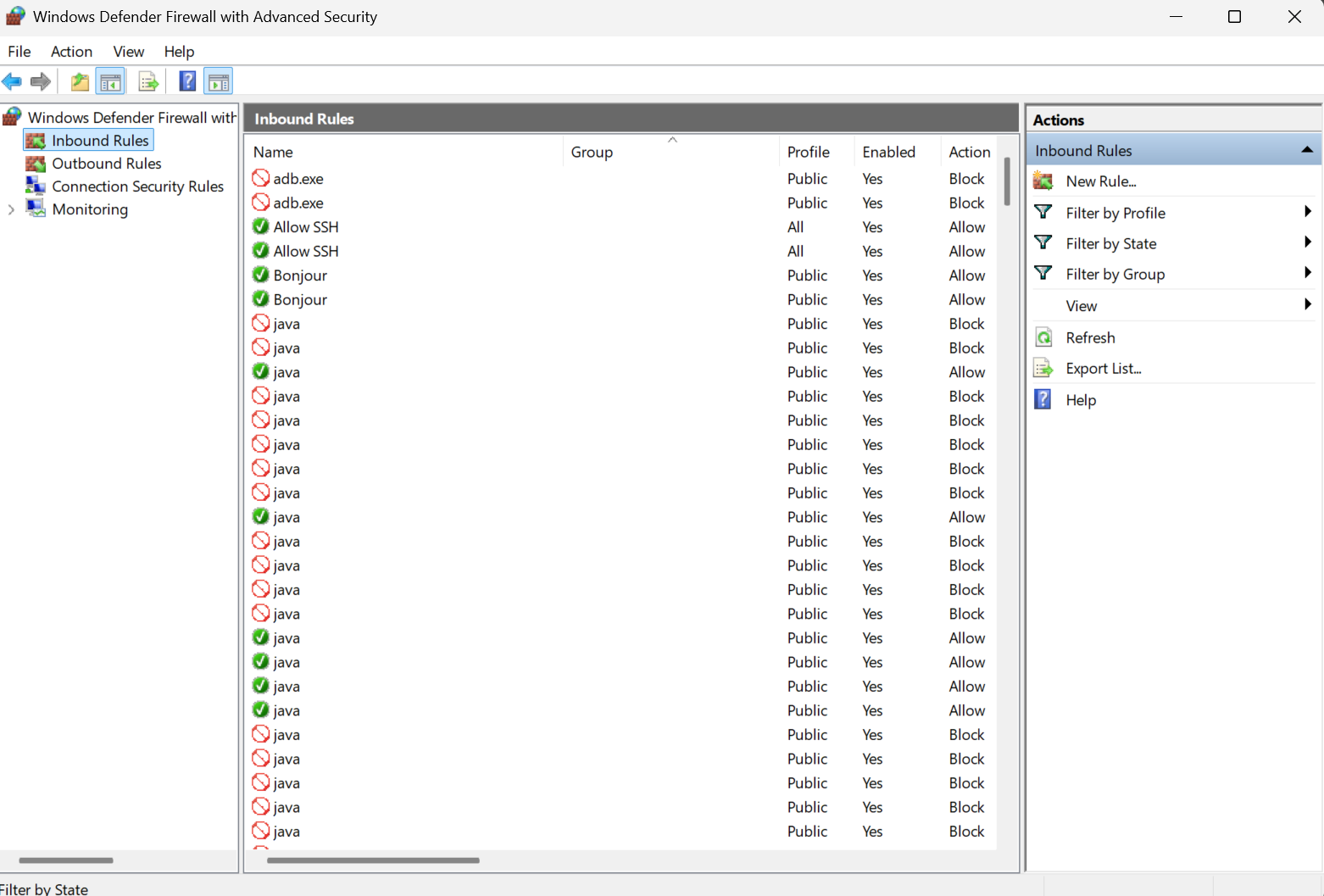


-------------------------------------------------------------------------

1. Remove the Test Block Rule.

In **Inbound Rules**, right-click **Block Telnet** → **Delete** → Confirm.





--------------------------------------------------------

1. Document Steps Used.

For CMD:

* wf.msc → open firewall.
* GUI steps: Inbound Rules → New Rule → Port → Enter port → Block/Allow → Finish.
* Test with:



-------------------------------------------------------------------------

1. Summarize How Firewall Filters Traffic.

* A firewall acts as a gatekeeper between your system and the network. It checks each data packet against predefined rules to decide whether to **allow** or **block** it.
* If traffic matches a **block rule** (e.g., Telnet on port 23), the connection is denied.
* If traffic matches an **allow rule** (e.g., SSH on port 22), it is permitted.
* If no rule applies, the firewall follows its default policy (usually block for inbound).
* In this way, a firewall prevents unauthorized access while allowing safe and necessary communication.

-------------------------------------------------------------------------