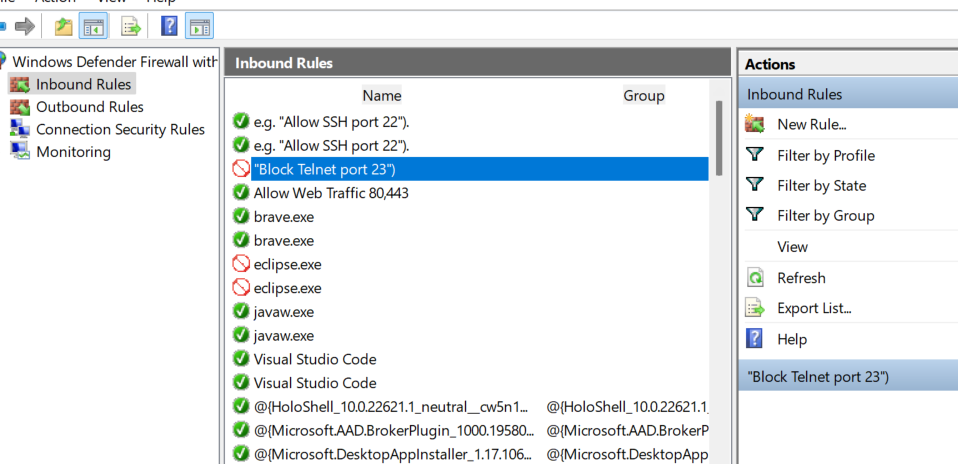
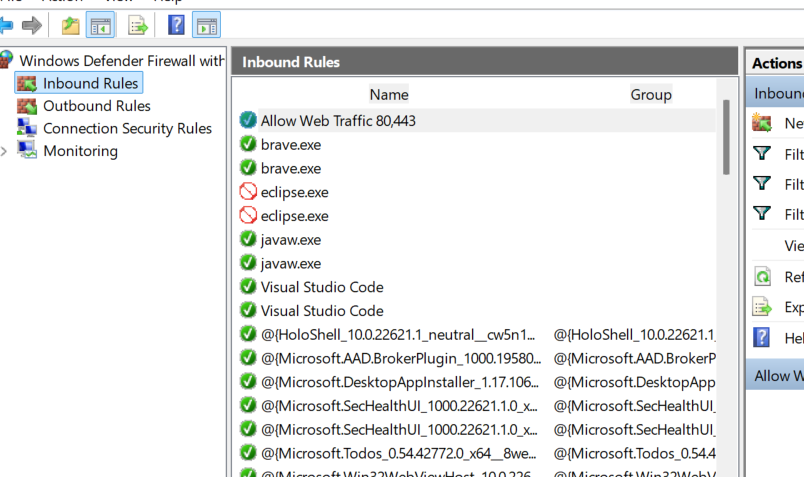
Task 4 : Setup and Use a Firewall on Windows/Linux:



**1. Document Commands or GUI Steps Used**

**For Windows Firewall (GUI steps):**

1. Open Windows Defender Firewall with Advanced Security from the Start menu.
2. Select Inbound Rules from the left panel to list current rules.
3. To block inbound traffic on port 23 (Telnet):
   * Click New Rule…
   * Choose Port, click Next.
   * Select TCP and enter 23 in "Specific local ports", click Next.
   * Choose Block the connection, click Next.
   * Select the network profiles where this applies (Domain, Private, Public), Next.
   * Name the rule (e.g., "Block Telnet port 23") and Finish.
4. Test the blocking rule by attempting to connect to port 23 locally or remotely.
5. To allow SSH traffic (port 22):
   * Repeat steps 3 but select Allow the connection and specify port 22.
   * Name this rule (e.g. "Allow SSH port 22").
6. To remove the block rule:
   * In Inbound Rules, find the “Block Telnet port 23” rule.
   * Right-click and select Delete or Disable.



**2. Summary: How Firewall Filters Traffic**

A firewall filters network traffic by using a set of predefined rules that determine whether to allow or block data packets based on their attributes. Key points include:

* Inspection of packets: Each incoming or outgoing packet is examined, focusing on parameters such as source and destination IP addresses, protocol (TCP, UDP), and port numbers.
* Rule matching: The firewall compares the packet's details against its configured rules.
* Decision making: If the packet matches a rule to allow traffic, it passes through; if it matches a rule to block, it is dropped or rejected.
* Default policy: If no rule matches, the firewall’s default behavior applies (usually blocking unsolicited inbound traffic).
* Additional inspection: More advanced firewalls may inspect packet contents (deep packet inspection), check for malicious patterns, apply proxy or URL filtering, and log traffic for monitoring.
* Profiles and contexts: Firewalls can apply different rules based on network profiles (public, private, domain) or the direction of traffic (inbound/outbound).

This mechanism provides a controlled gateway ensuring only authorized and safe traffic passes, protecting systems from unauthorized access and potential threats.