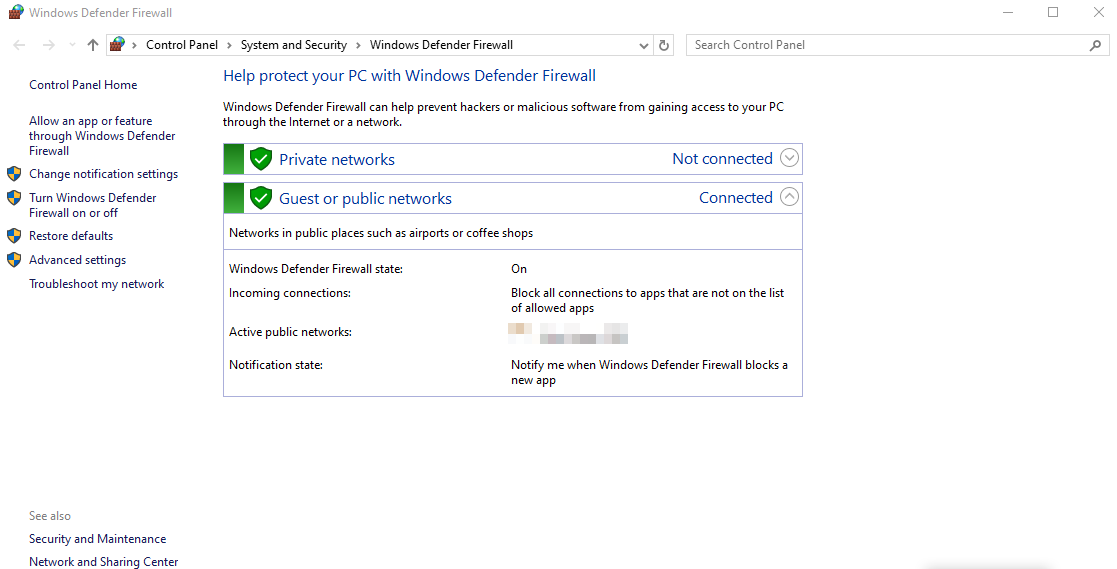
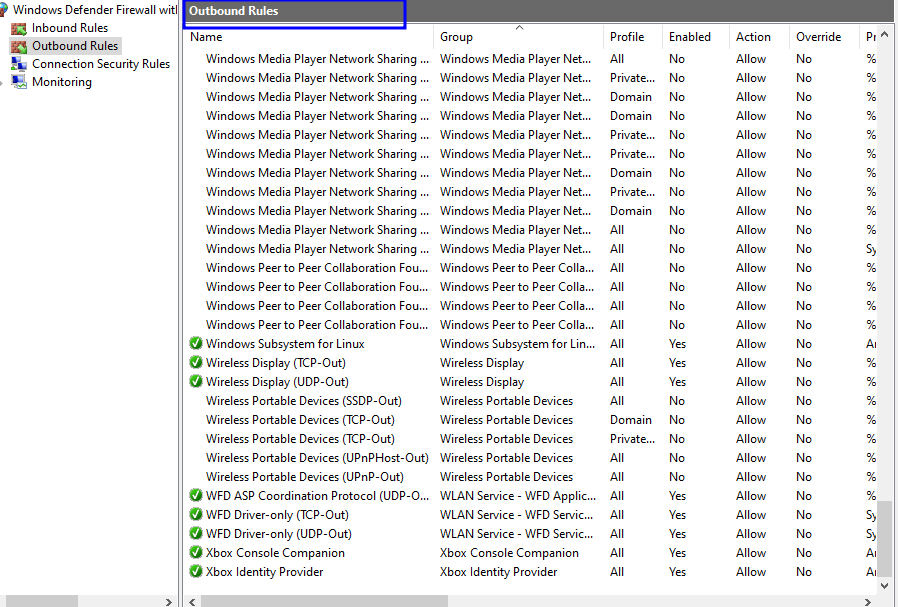
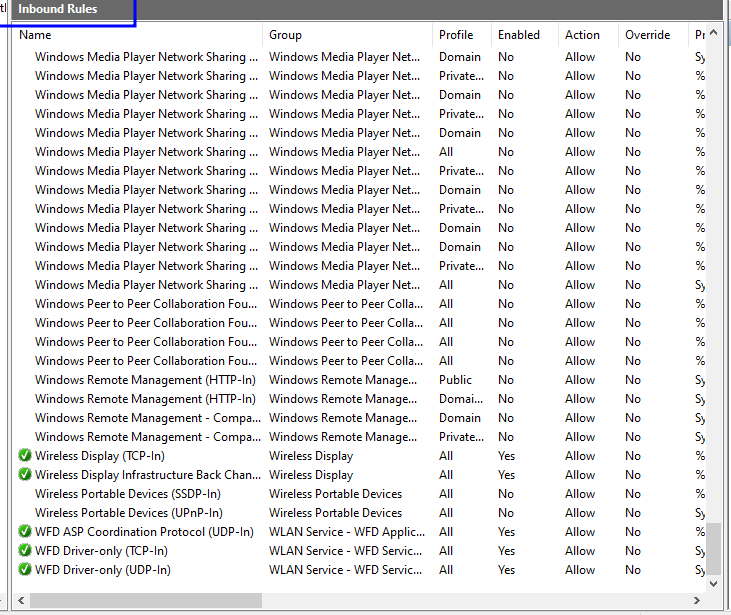
1. Open firewall configuration tool



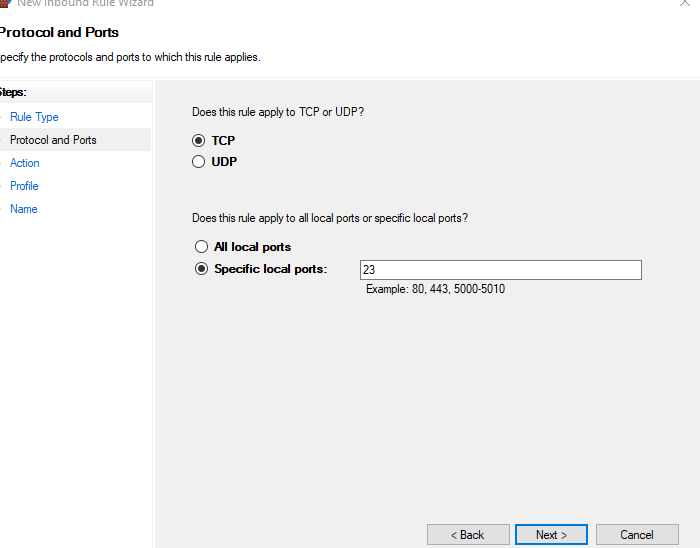
2. Outbound Rules



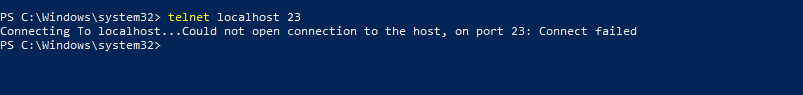
3. Inbound Rules



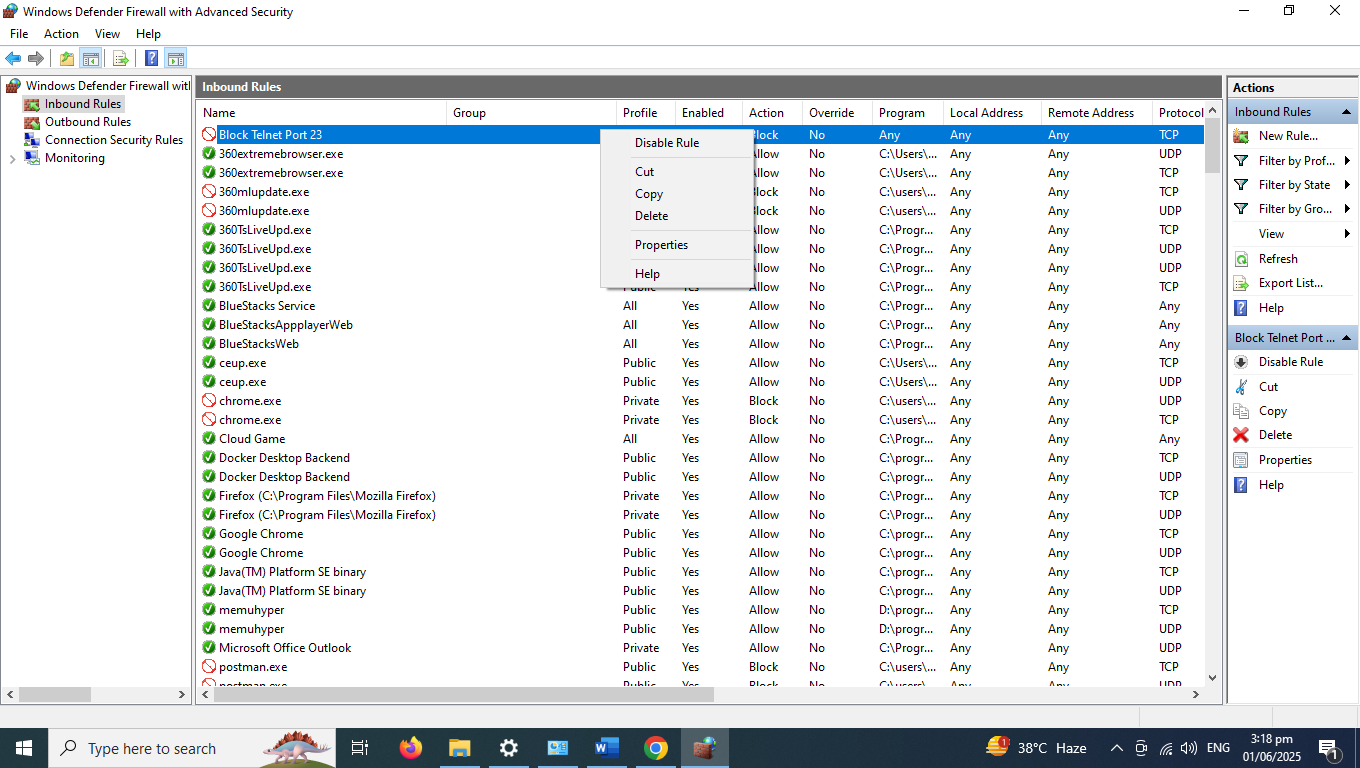
4. Rule to block inbound traffic on a specific port (e.g., 23 for Telnet).



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



6. Deleting test block rule to restore original state.



**7. Summary: How Firewalls Filter Traffic**

Firewalls inspect network traffic based on defined rules to allow or block data packets. They work on:

* Ports: Specific service channels (e.g., port 80 for HTTP, 22 for SSH).
* Protocols: TCP/UDP.
* IP Addresses: Source and destination filtering.

**Types:**

* Inbound Filtering: Controls what enters your system.
* Outbound Filtering: Controls what leaves your system.

Rules are processed top-down; once a match is found, the action is taken (allow/deny), and the rest are skipped.