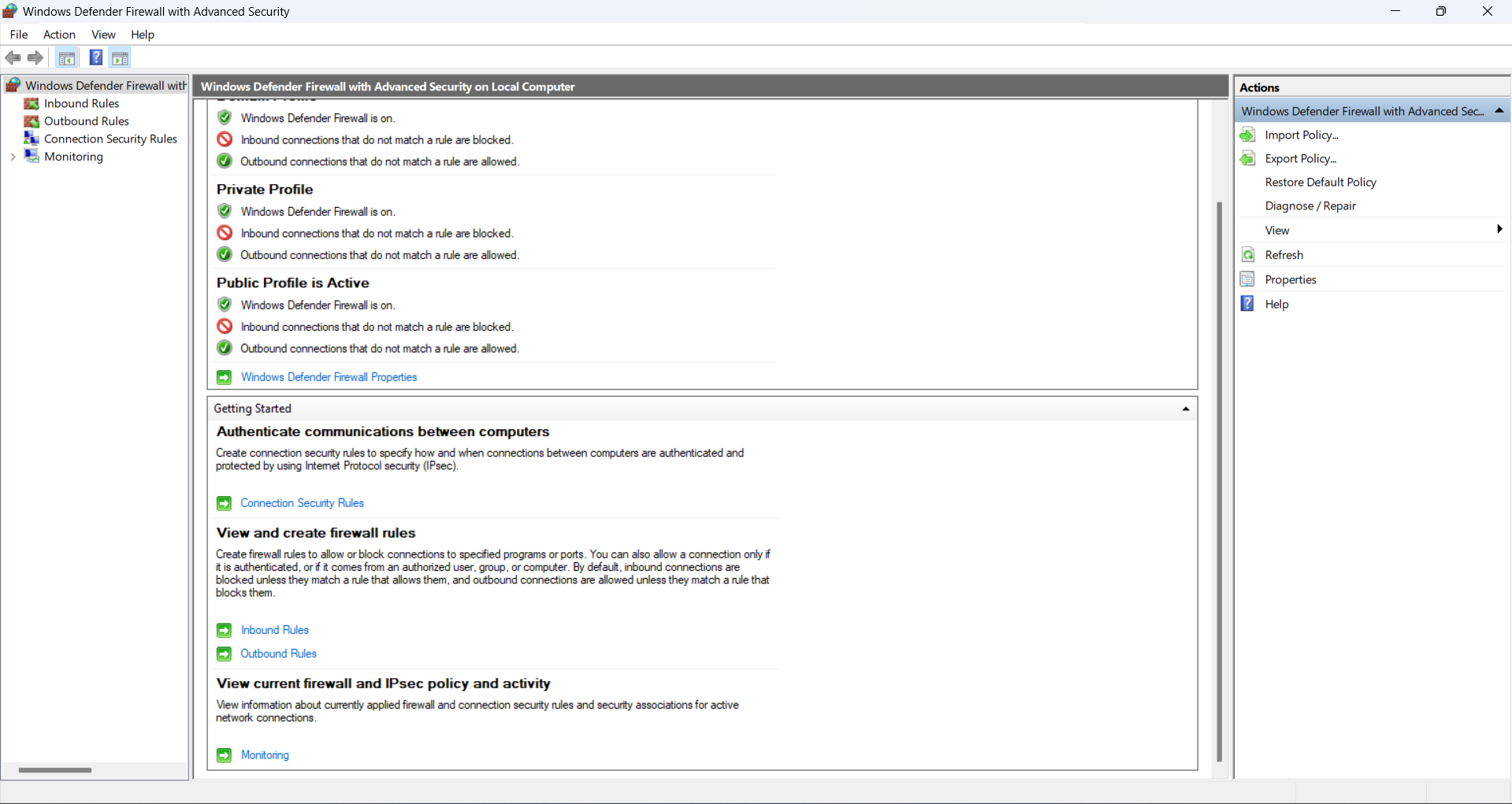
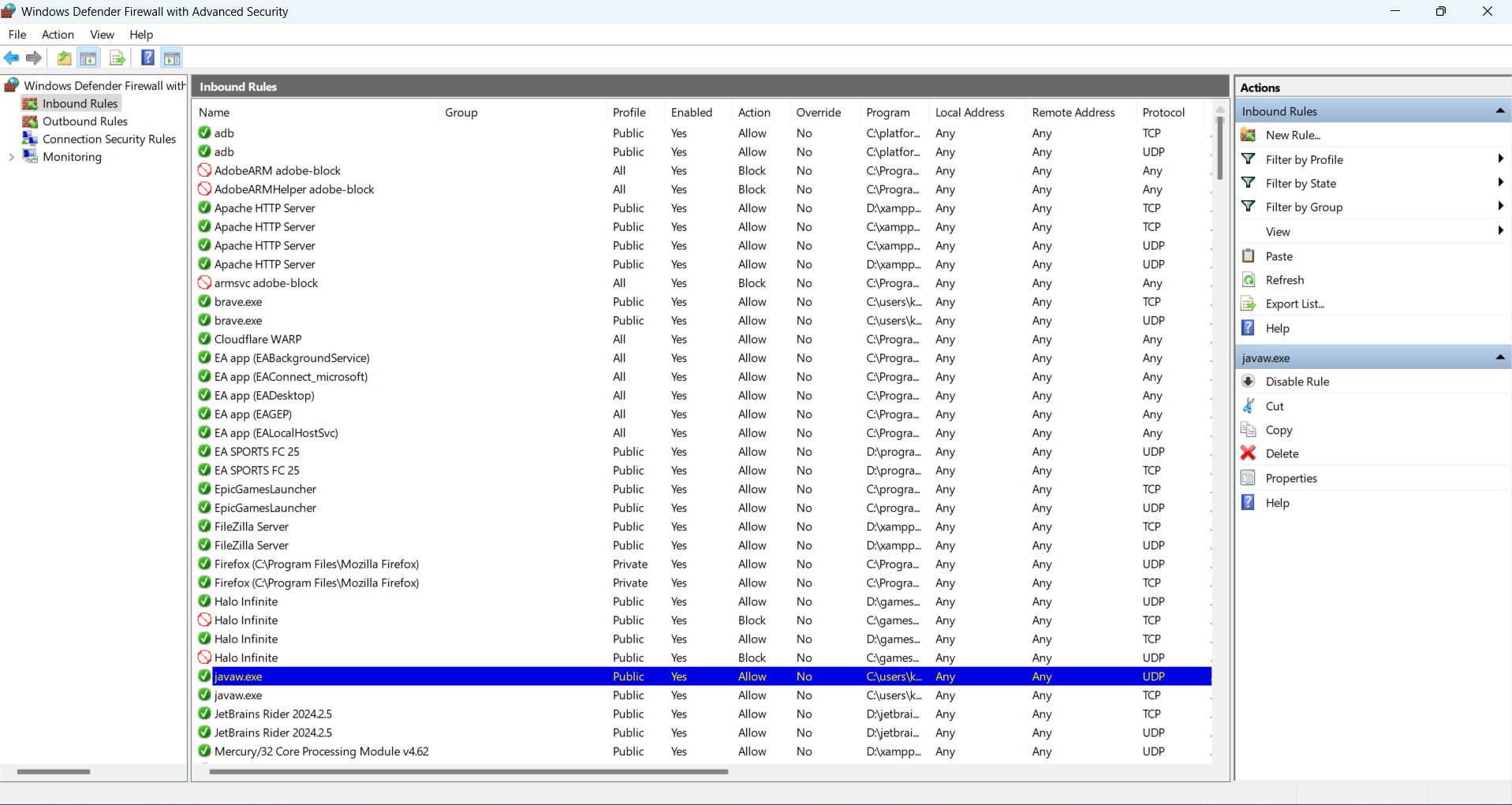
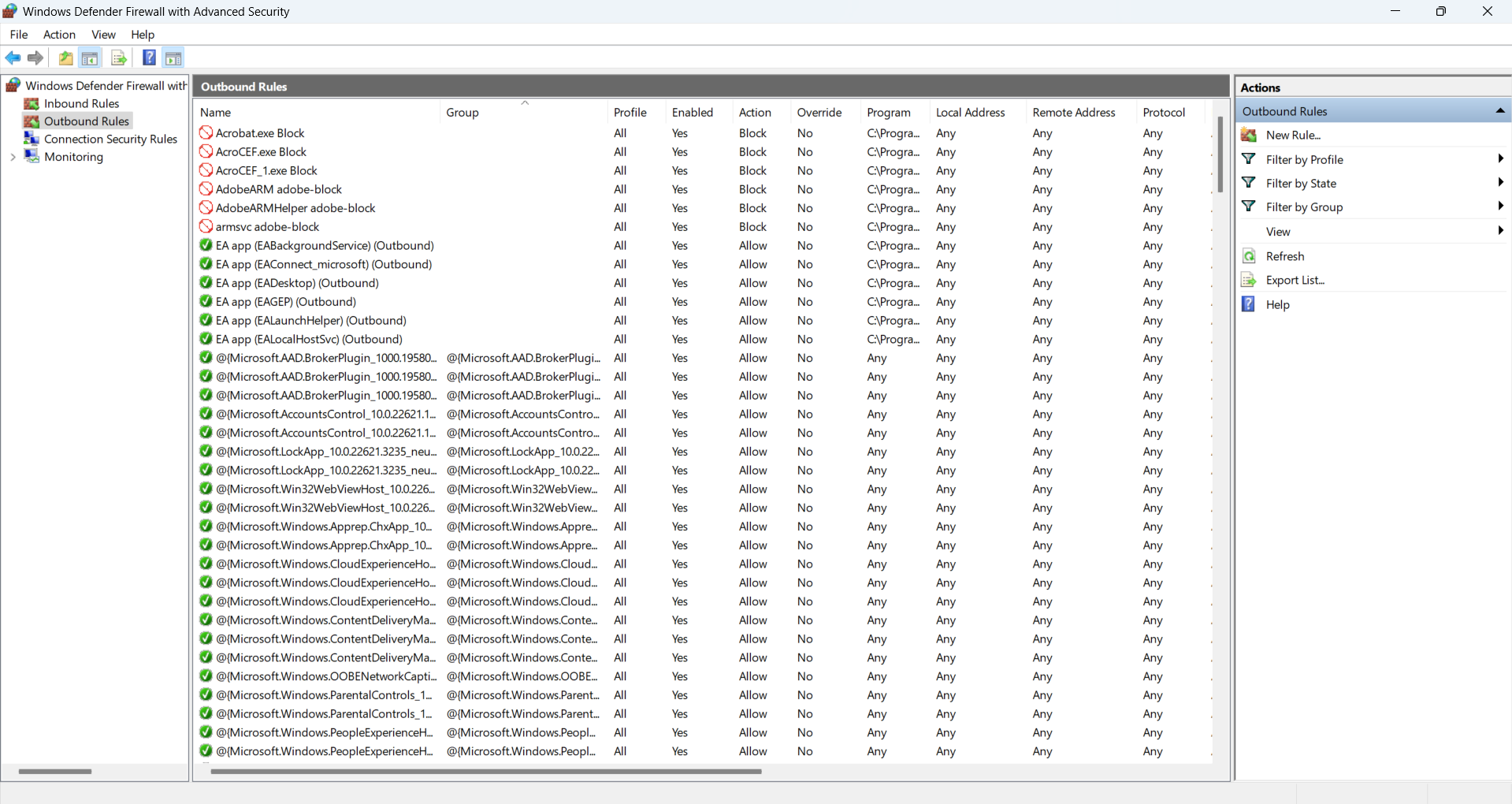
**FIREWALL STATUS**  
  


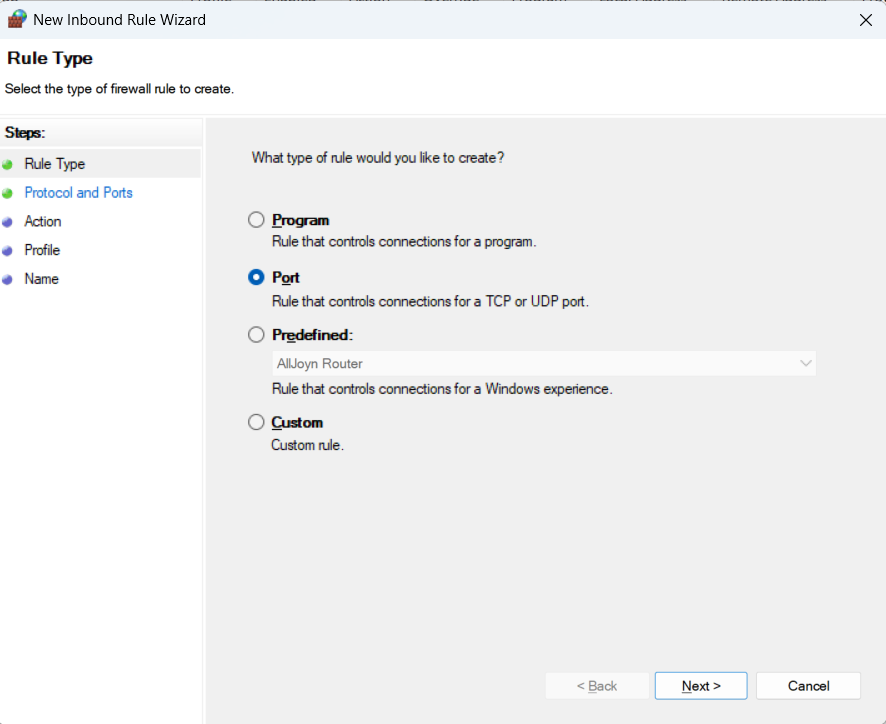
INBOUND RULES

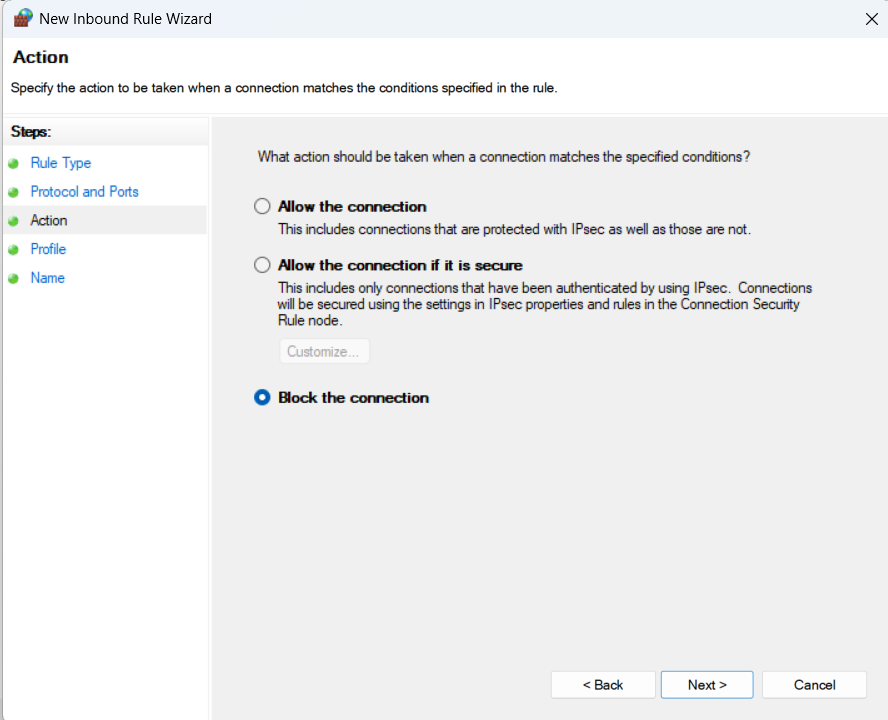
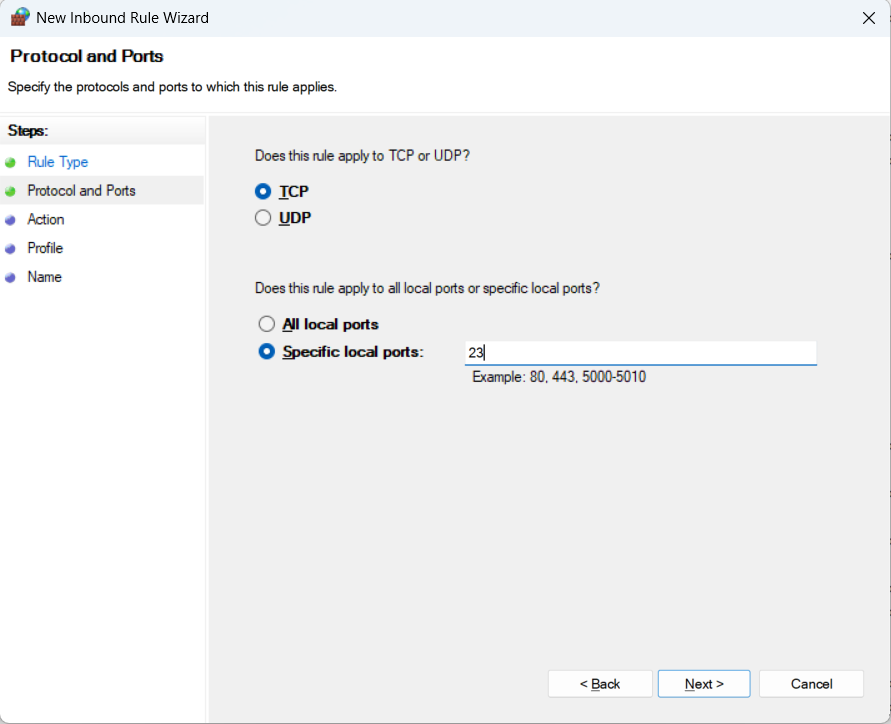


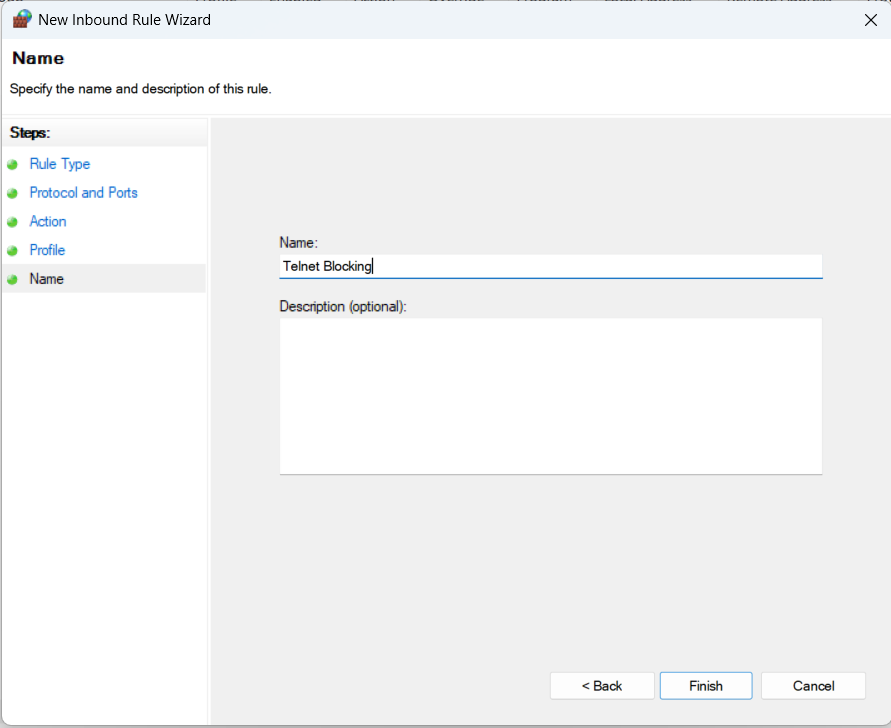
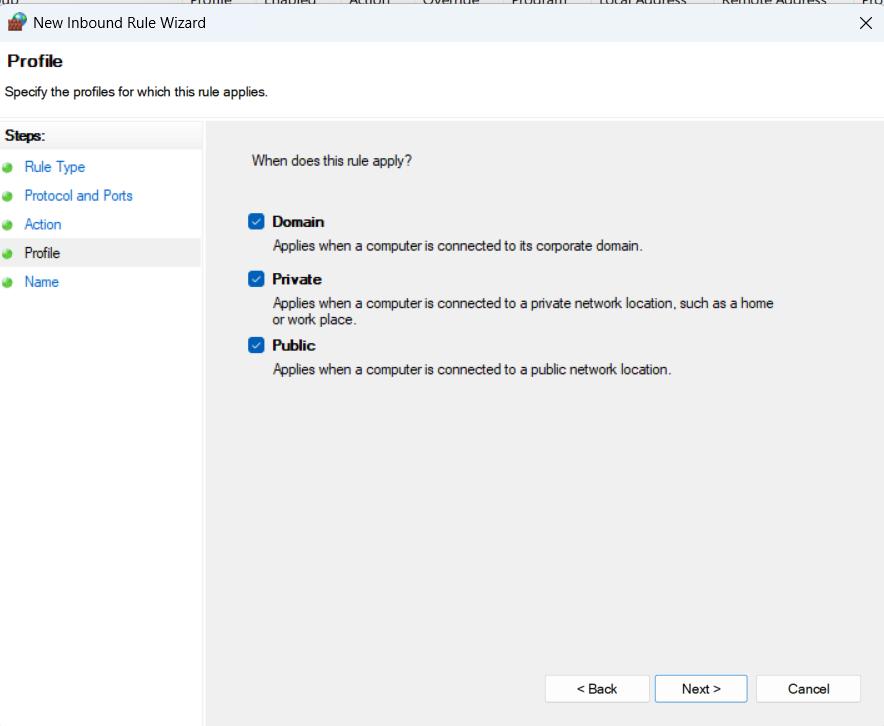
OUTBOUND RULES



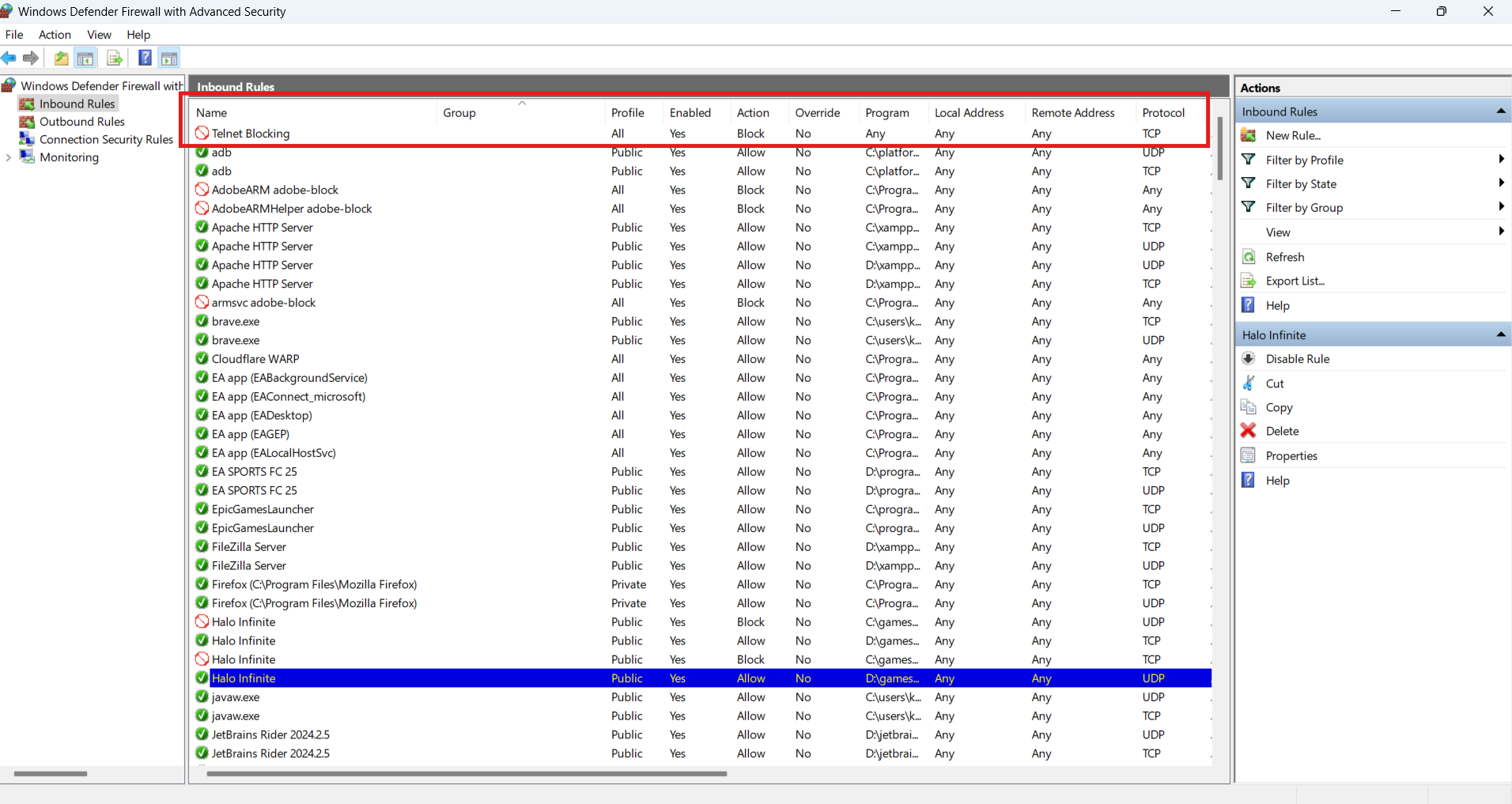
Blocking Port 23 (Telnet)



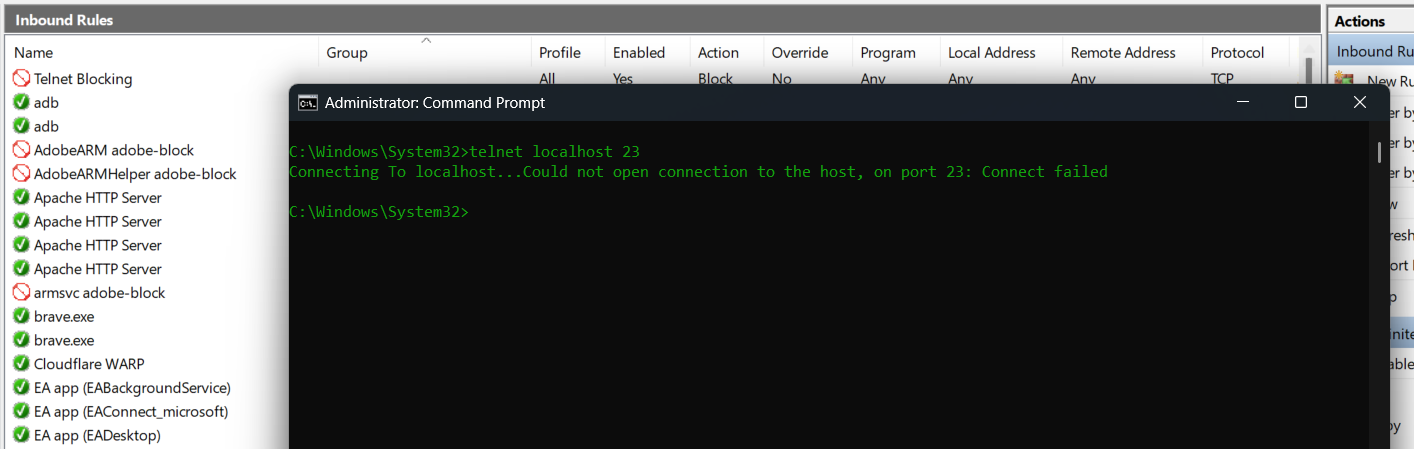




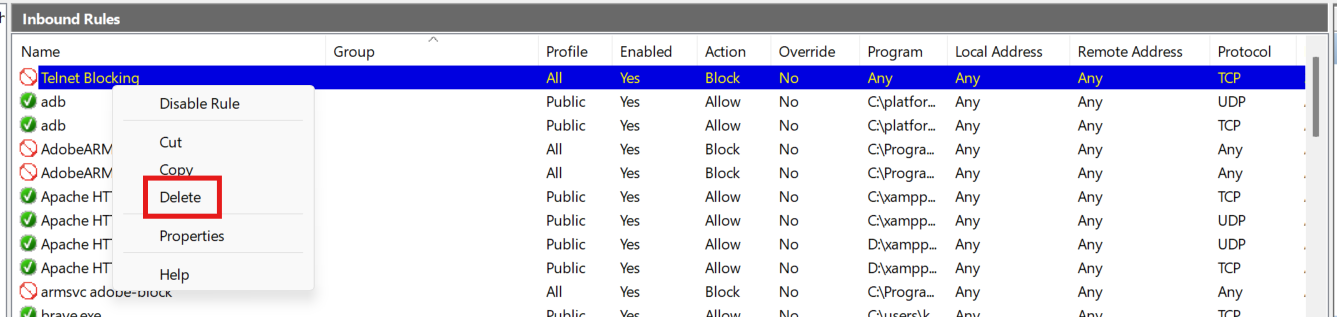
UPDATED INBOUND RULES



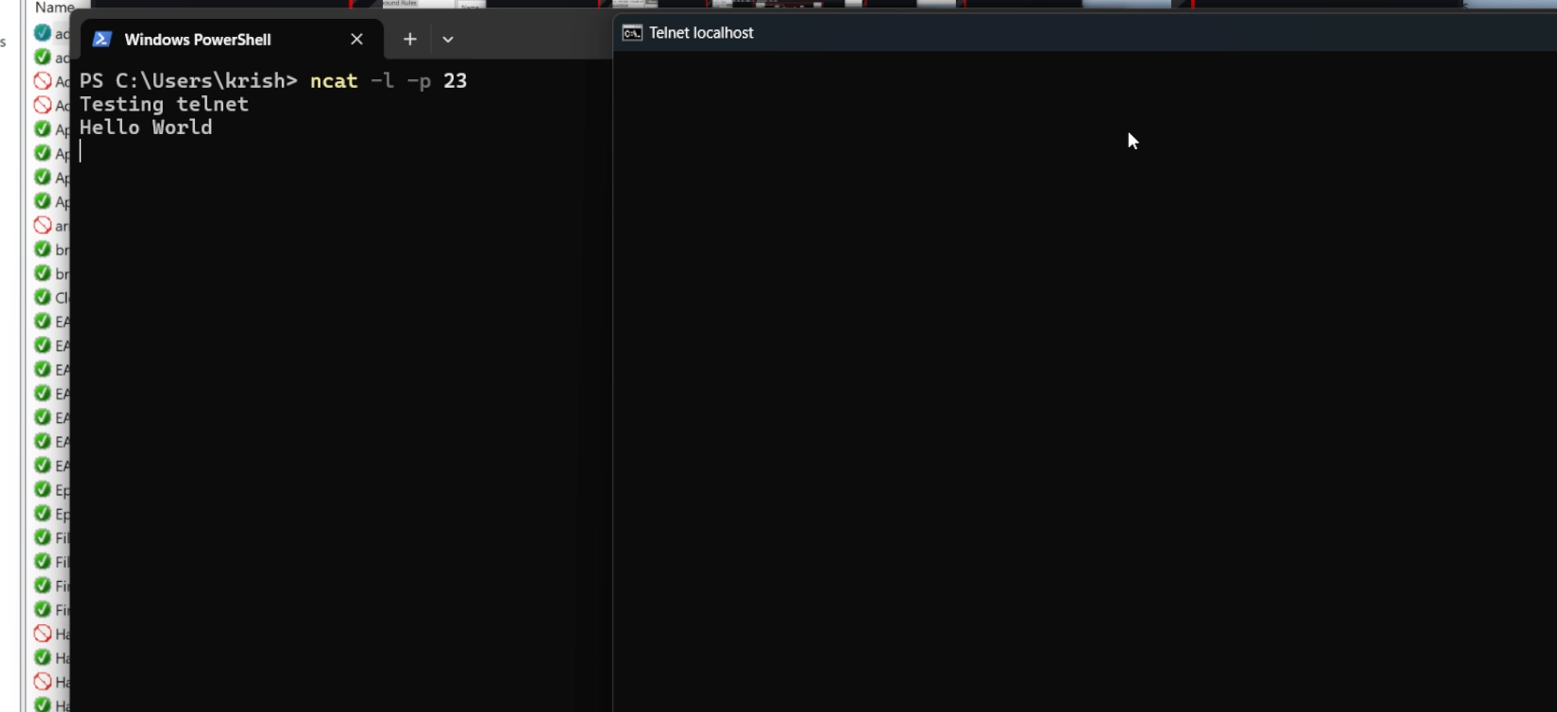
AFTER BLOCKING TELNET



Restoring Original State



AFTER RESTORING ORIGINAL STATE



Summary on How Firewall Filters Traffic:

1. **Inspects Each Packet**: Every data packet trying to enter or leave your system is analysed.
2. **Matches Against Rules:** The firewall checks whether the packet matches any allow or block rules you've set (e.g., block port 23, allow port 22).
3. **Decision Made:**

* If a packet matches an allow rule, it is let through.
* If it matches a block rule, it is dropped (ignored).

1. **Default Behaviour:** If no rule matches, firewalls usually follow a default deny policy (block everything not explicitly allowed).