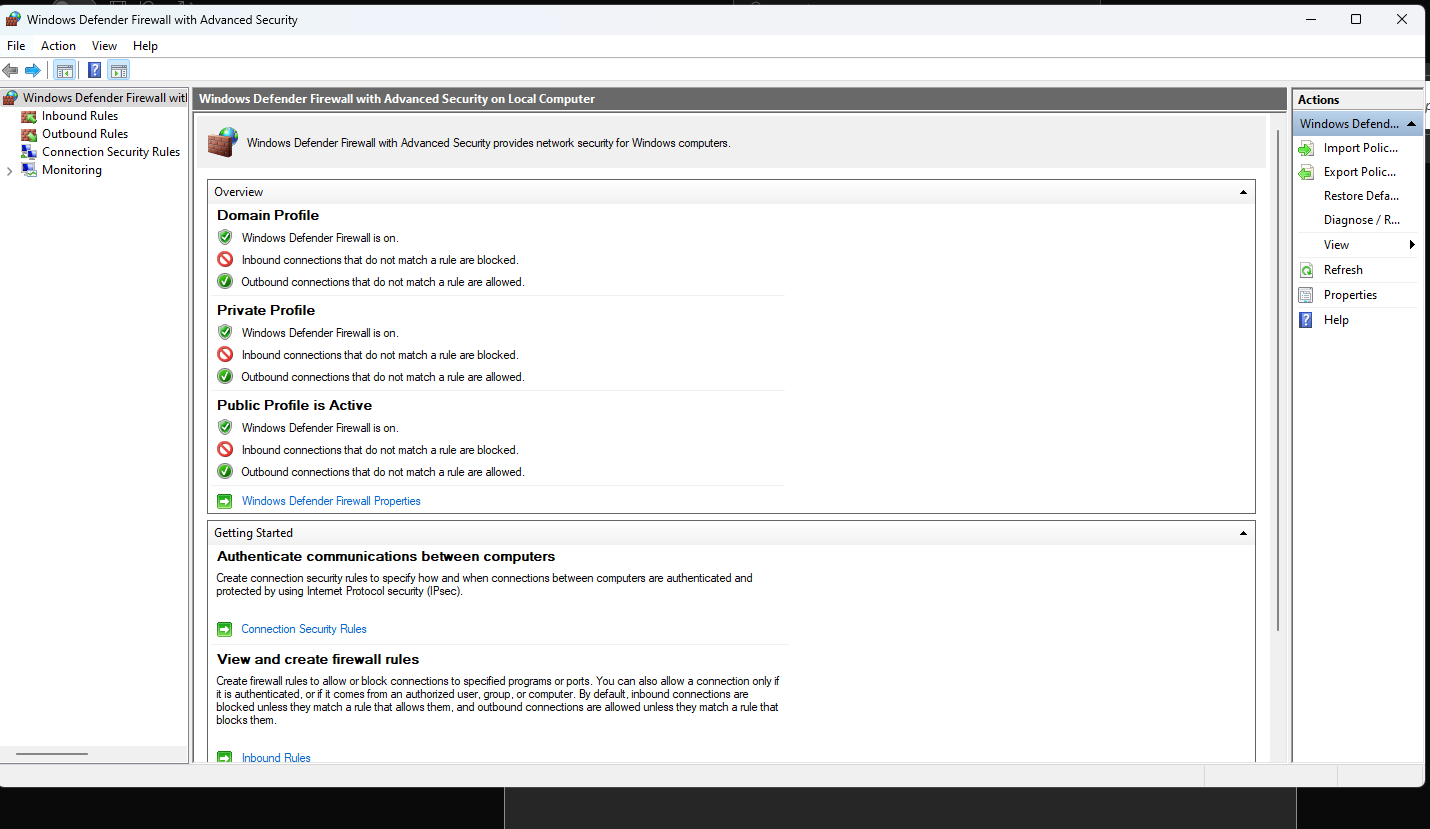
Task 4 –

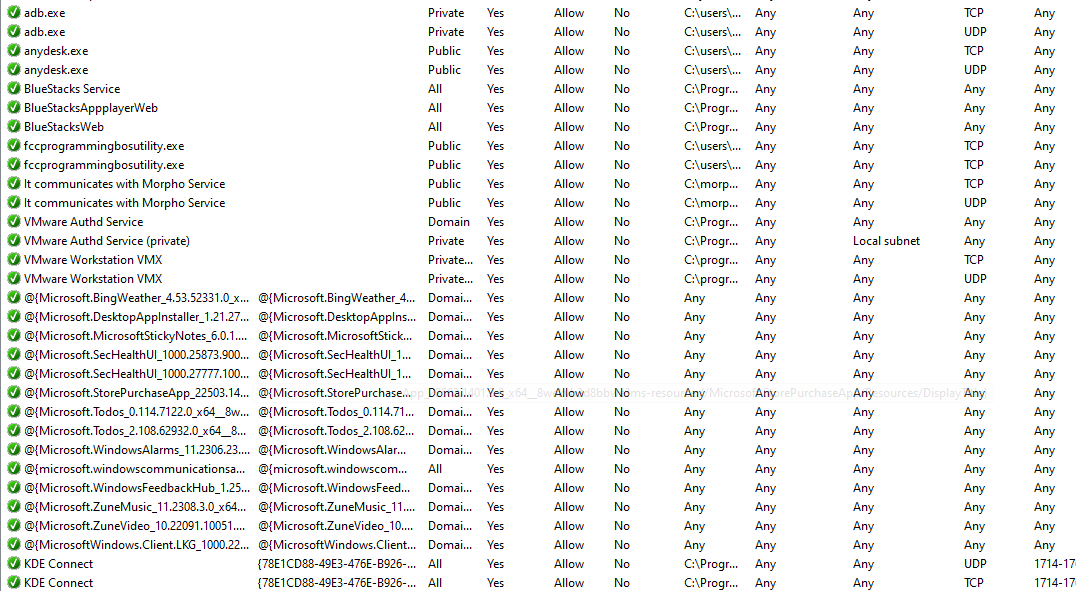
Configure a firewall on local system.

First open the wf.msc firewall configuration in start menu

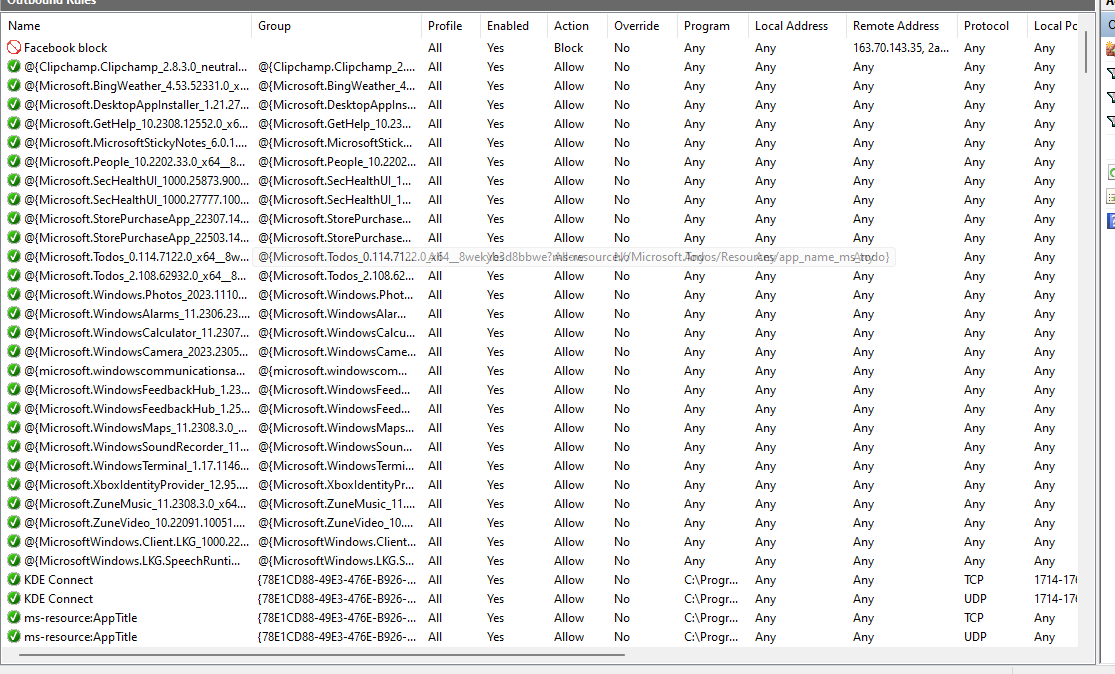


Now 2 rules are showing on left hand side.

Inbound rule

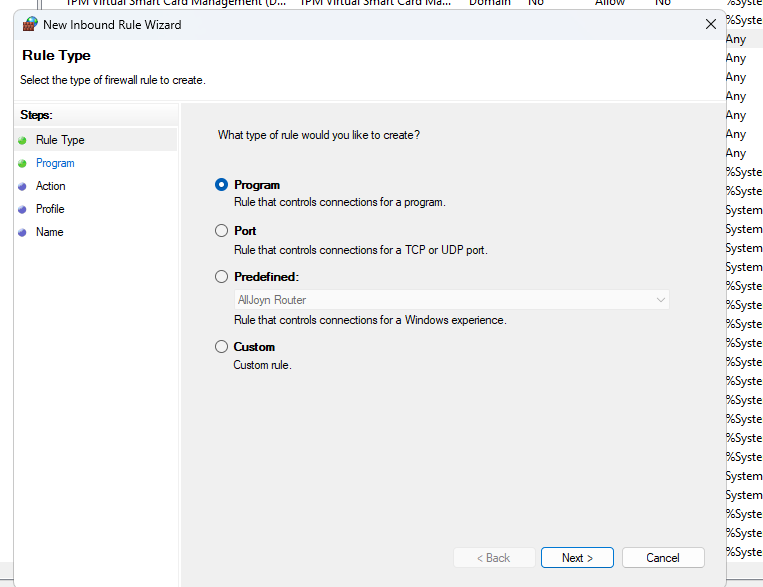


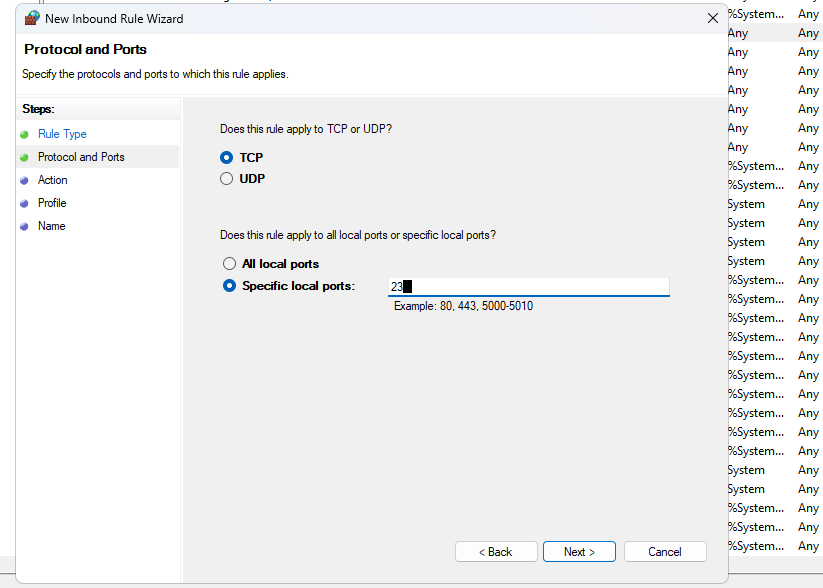
Outbound Rules -



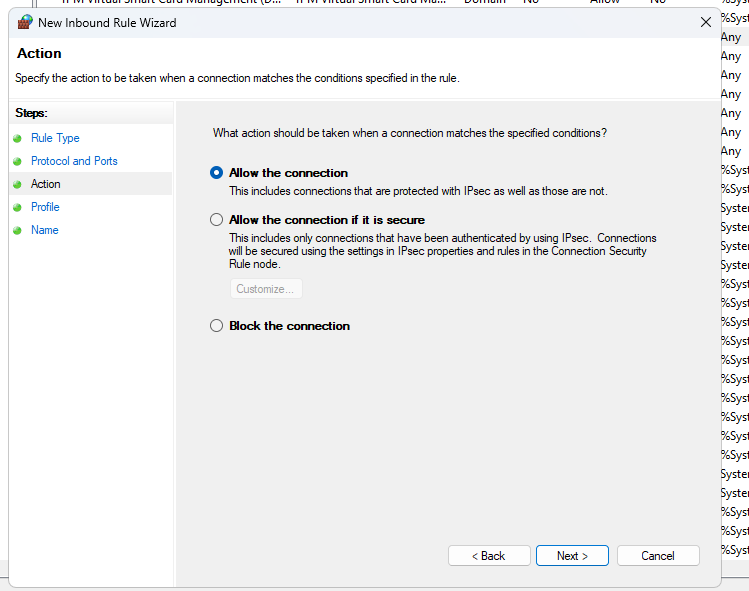
Now configure a rule for blocking telnet protocol

For new rule

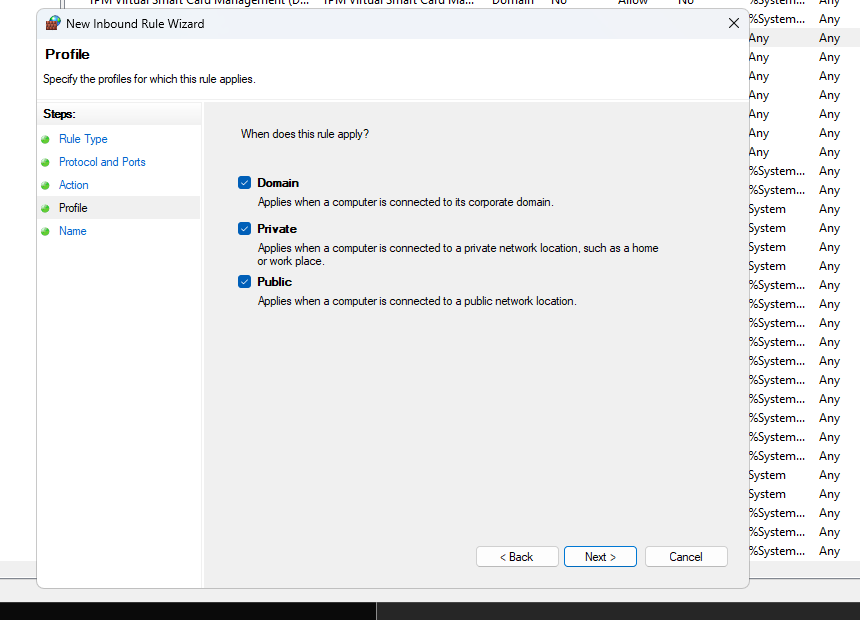




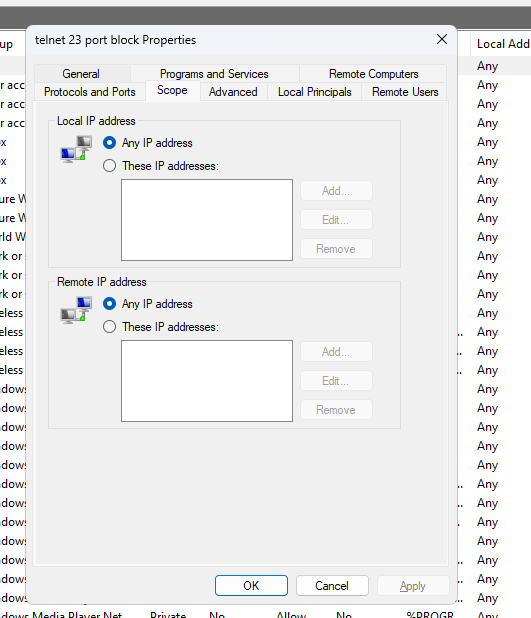
Now block all connections



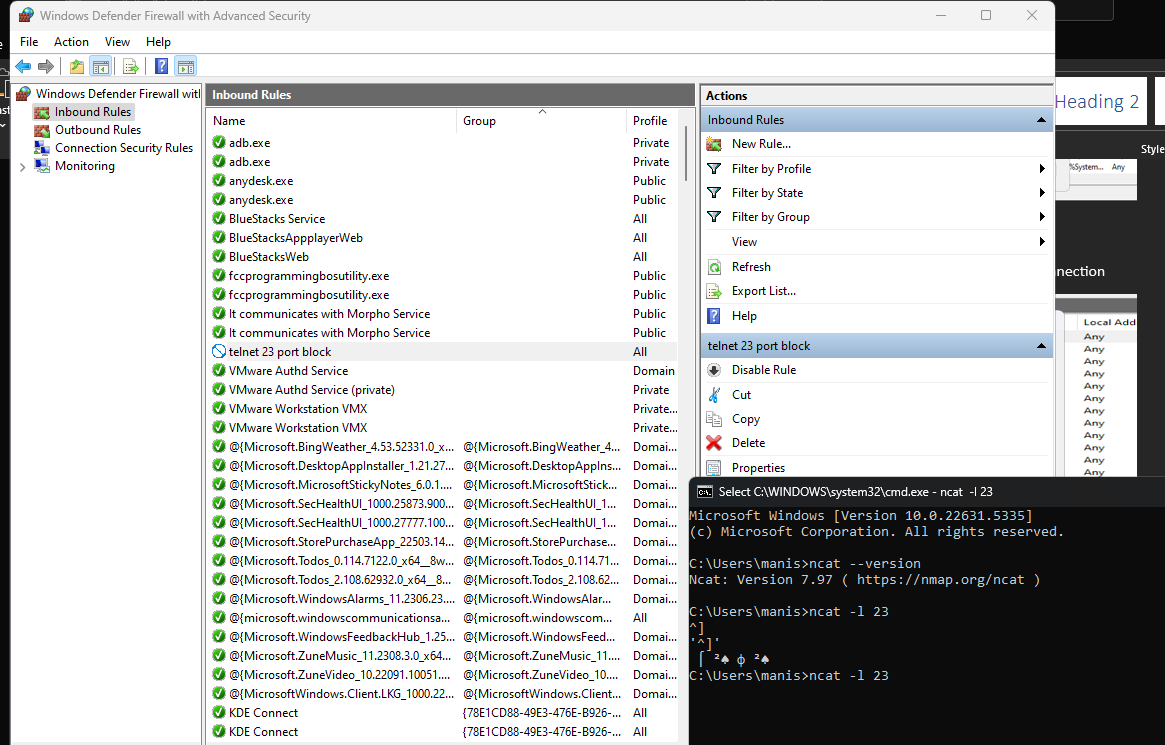
For all domain now block

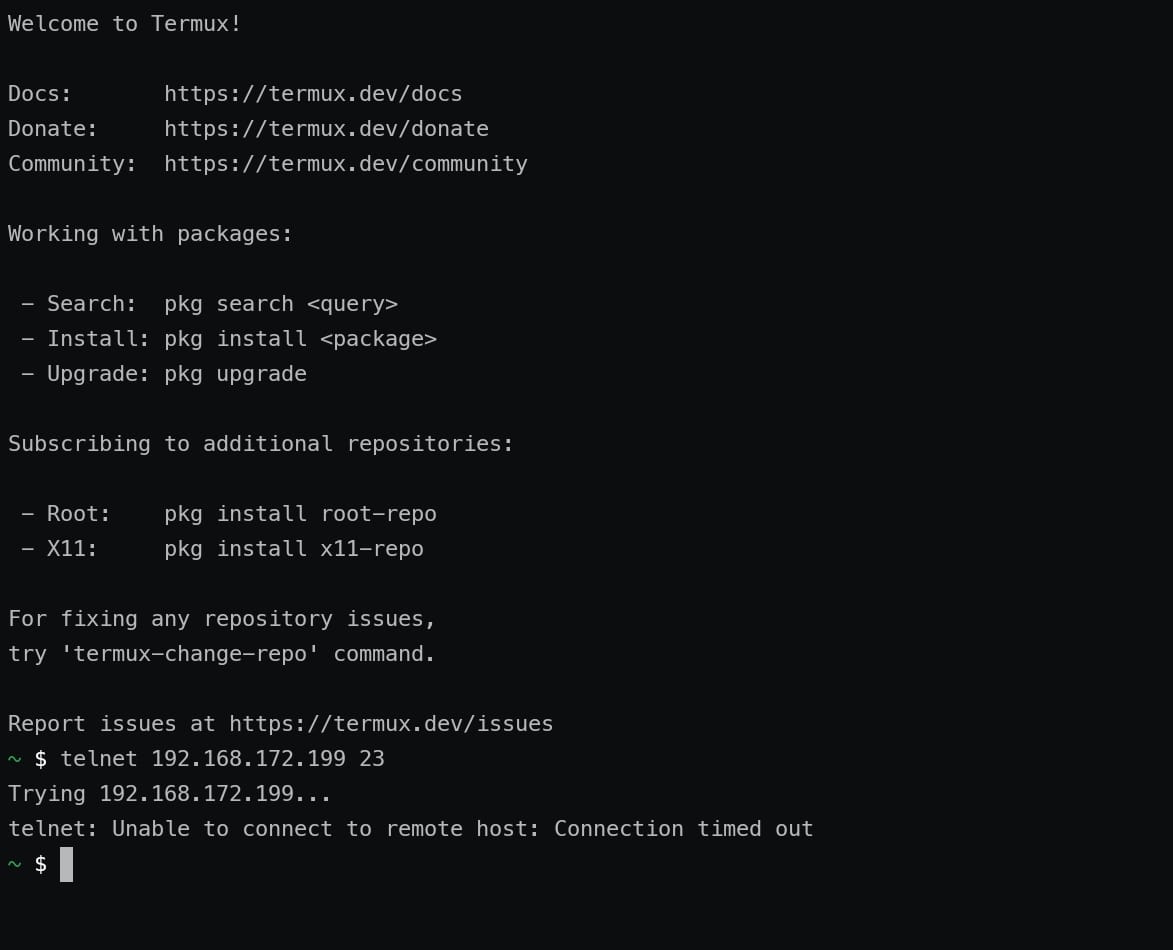


We can define the particular ip address for accessing or blocking connection

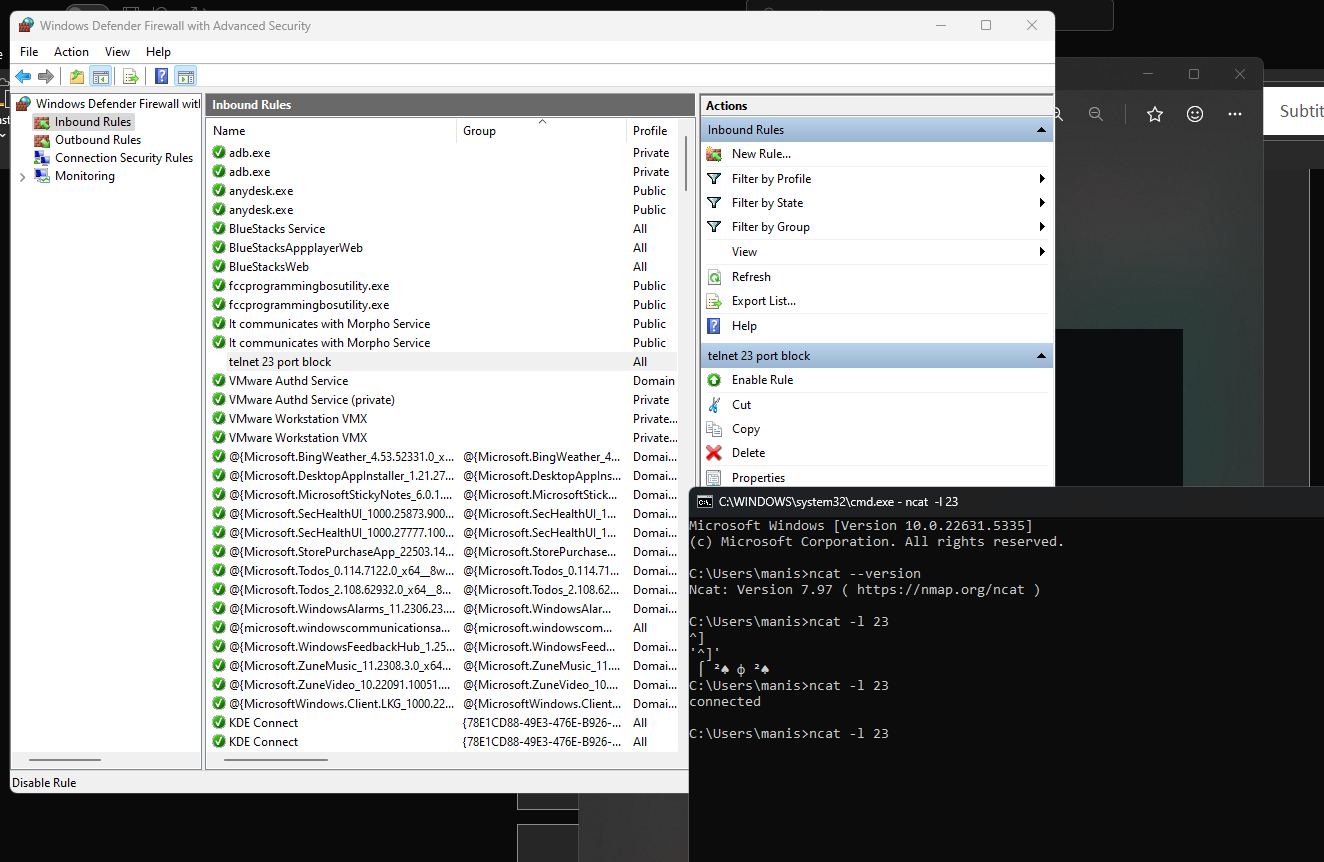


Now testing with blocked 23 port





Now disable firewall and try to connect 23 port





Above image showing connected with 23 port connection established

A firewall acts as a security guard for a network, positioned between a trusted internal network (like your home or office network) and an untrusted external network (like the internet). Its primary function is to **monitor and filter incoming and outgoing network traffic based on a predefined set of security rules**, allowing non-threatening traffic to pass through and blocking dangerous traffic.

Here's a breakdown of how firewalls filter traffic:

**1. Rule Examination:** Every data packet attempting to traverse the firewall is evaluated against a set of established rules. These rules are configured by network administrators and dictate what traffic is allowed or blocked based on various criteria. If a packet doesn't comply with any of the rules, it's typically discarded.

**2. Key Filtering Mechanisms:**

* **Packet Filtering (Stateless Inspection):** This is the most basic and oldest form of firewall filtering.
  + It inspects individual data packets in isolation, looking at information in the packet's header, such as:
    - **Source and Destination IP addresses:** Where the packet originated and where it's trying to go.
    - **Source and Destination Port numbers:** These specify the application or service the traffic is associated with (e.g., port 80 for HTTP web traffic, port 22 for SSH).
    - **Protocols:** The type of communication protocol being used (e.g., TCP, UDP, ICMP).
  + Based on these header details and the predefined rules, the firewall decides to allow or block the packet.
  + **Limitation:** It doesn't remember past packets or the context of a connection, making it less secure against more sophisticated attacks.
* **Stateful Inspection (Dynamic Packet Filtering):** This is a more advanced and common method.
  + It builds upon packet filtering by maintaining a "state table" or "connection table" that tracks active network connections.
  + When an outgoing packet is sent, the firewall records its details. When an incoming response arrives, the firewall checks if it matches an active session in its state table.
  + Only packets that correspond to a valid, previously established outgoing connection are allowed through. This significantly enhances security by preventing unsolicited incoming connections.
  + **Benefit:** More secure than basic packet filtering as it understands the context of a conversation.
* **Proxy Service (Application-Level Gateway):**
  + A proxy firewall acts as an intermediary between the internal network and the external network.
  + Instead of allowing direct communication, the proxy intercepts requests from internal users, establishes its own connection to the external destination, fetches the data, inspects it, and then relays it to the user.
  + Similarly, for incoming traffic, the proxy receives it first, inspects it, and then forwards it to the internal system if it's deemed safe.
  + **Benefit:** Provides an extra layer of isolation, preventing direct access to internal systems and allowing for deeper inspection of application-level content.
* **Next-Generation Firewalls (NGFWs):**
  + These are modern, multi-layered firewalls that combine the capabilities of packet filtering, stateful inspection, and proxy services with additional advanced features.
  + They can perform **deep packet inspection (DPI)**, which examines the actual payload (content) of packets for specific patterns, signatures, or anomalies indicative of malicious behavior (like malware or specific keywords).
  + NGFWs often integrate with intrusion prevention systems (IPS), antivirus software, and other security tools for comprehensive threat protection.
  + They can also control traffic based on specific applications, users, or even content categories.

**3. Decision Execution and Logging:** After evaluating a packet against its rules and applying the relevant filtering mechanism, the firewall makes a decision:

* **Allow:** The packet is permitted to pass through to its intended destination.
* **Block (Reject):** The packet is dropped, and an "unreachable error" message might be sent back to the sender.
* **Drop:** The packet is silently discarded without any notification to the sender.

Firewalls also typically maintain a log of their actions, recording details of accepted and rejected packets. This logging provides administrators with valuable insights into network traffic patterns, potential threats, and helps in troubleshooting.

**4. Continuous Updates:** Firewall rules are not static. Administrators regularly update and refine these rules based on emerging threats, changing network requirements, and security policies to maintain optimal network security. Modern firewalls can also use AI-driven security operations platforms to adapt to new threats.

In essence, a firewall acts as a customizable gatekeeper, meticulously inspecting every piece of data that tries to enter or leave a network, ensuring that only authorized and safe traffic is allowed to flow.