Firewall Configuration Report - macOS (M1)

1. Commands and GUI Steps Used

1. Enabled macOS Firewall via System Settings > Network > Firewall.

2. Clicked 'Options' to block incoming connections for selected apps.

3. Created custom packet filter rule to block port 23 (Telnet):

   sudo nano /etc/pf.anchors/blocktelnet

   (Added: block in proto tcp from any to any port 23)

4. Included the rule in main config file /etc/pf.conf:

   anchor "blocktelnet"

   load anchor "blocktelnet" from "/etc/pf.anchors/blocktelnet"

5. Reloaded and enabled pf firewall:

   sudo pfctl -f /etc/pf.conf

   sudo pfctl -e

6. Tested the block using:

   telnet localhost 23

7. Created rule to allow SSH (port 22) in a similar way.

8. Removed test block rule by deleting/commenting anchor line and reloading config:

   sudo pfctl -f /etc/pf.conf

2. Summary: How Firewall Filters Traffic

macOS uses a powerful tool called 'pf' (Packet Filter) to manage firewall rules. Firewall rules inspect and control incoming and outgoing network packets. Each rule defines whether to allow or block traffic based on conditions such as port, protocol, or IP address. In this task, we blocked Telnet traffic (port 23) to prevent insecure remote connections and allowed SSH (port 22) to enable secure access. This process demonstrated how firewalls help enforce network security policies by controlling traffic flow into and out of the system.