Setup And Use a Firewall on Windows/Linux

- List Current Firewall Rules

Name	Profile	Enable
Firefoxc;\program files\Mozilla Firefox	Private	Yes
NVIDIA SHIELD Streaming NSS UDP Exception	All	Yes
Stremio-runtime.exe	Public	Yes
Microsoft Teams(personal)	All	Yes

- To Block Inbound Traffic on Port 23 for telnet

In Inbound Rules go to left side click on New Rules select Rule Types as port next Protocol as TCP next specific local port enter 23 click next Action select Block the connection and next Profile choose all and next for description Enter Block Telnet Port 23.

- Test the rule bu attempting to connect to that port locally or remotely

  ComputerName : 127.0.0.1
  RemoteAddress : 127.0.0.1
  RemotePort : 23
  InterfaceAlias : Loopback Pseudo-Interface 1
  SourceAddress : 127.0.0.1

PingSucceeded : True
PingReplyDetail(RTT) : 0 ms
TcpTestSucceded : False

- Summarize How Firewall Filters Traffic :

  Traffic Monitoring : Every data packet entering or leaving a network is inspected by the firewall.
  Rule Matching : The firewall compares each packet against a set of rules
  Allow or Block Decision : Allowed traffic is forwarded to its destination.
  Blocked traffic is dropped (not delivered).

- Types of Filtering:

  1. Packet Filtering
  2. Stateful Inspection
  3. Application layer Filtering

- **Inbound Filtering** – Controls traffic coming into the system.
- **Outbound Filtering** – Controls what data is allowed to leave.