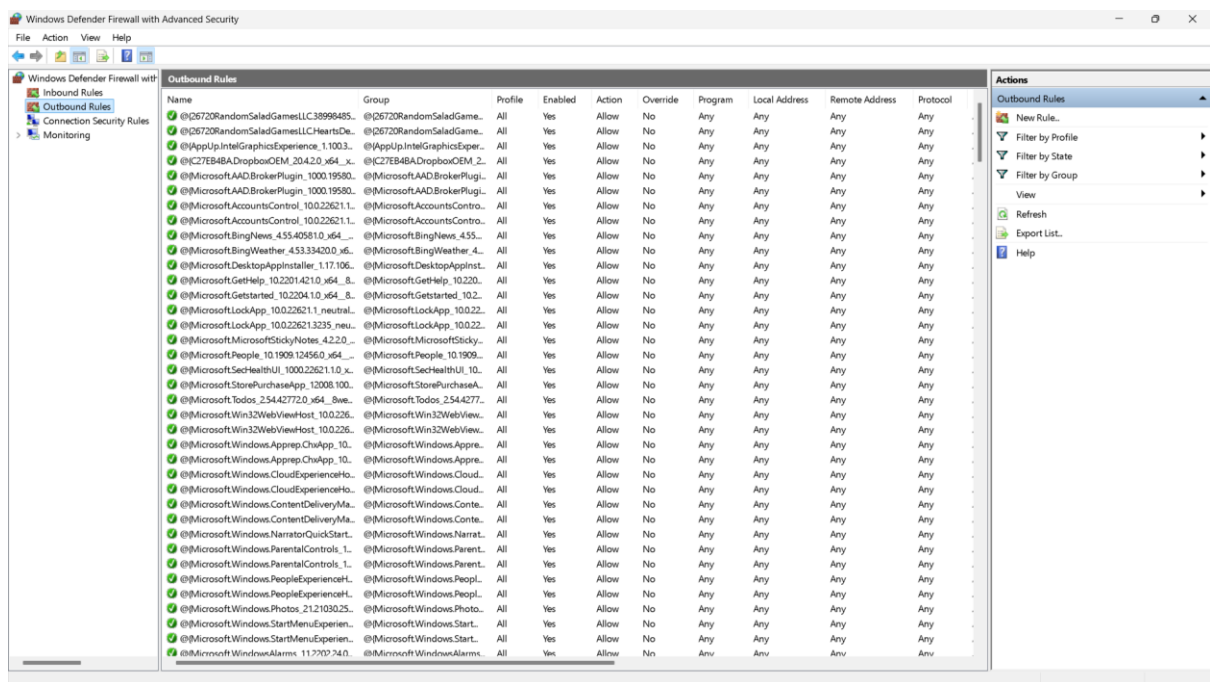
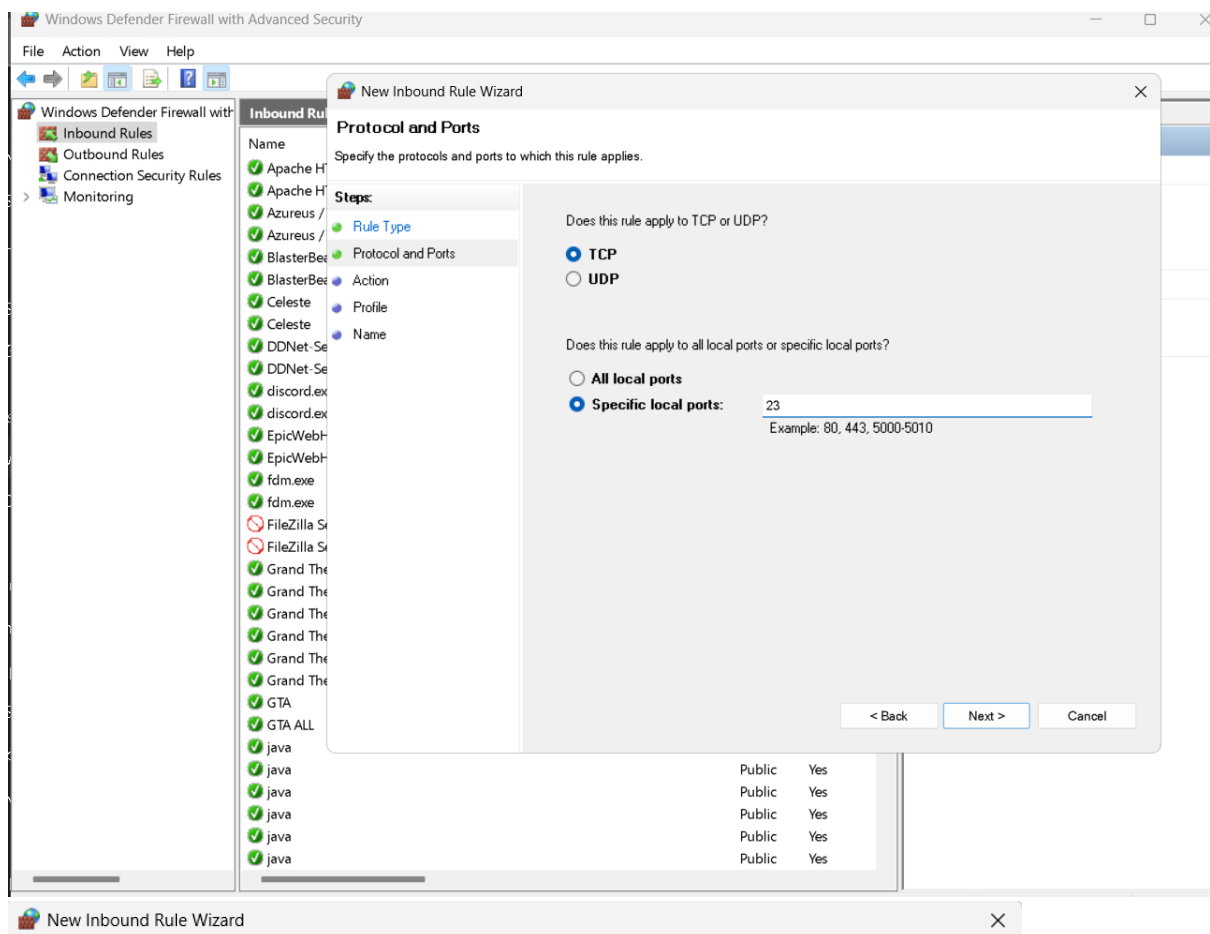


Opening windows firewall and listing the inbound and outbound rules:



3. now adding a rule to block inbound traffic on port 23.



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☐ Allow the connection

This includes connections that are protected with IPsec as well as those are not.

☐ Allow the connection if it is secure

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

[Customize...](#)

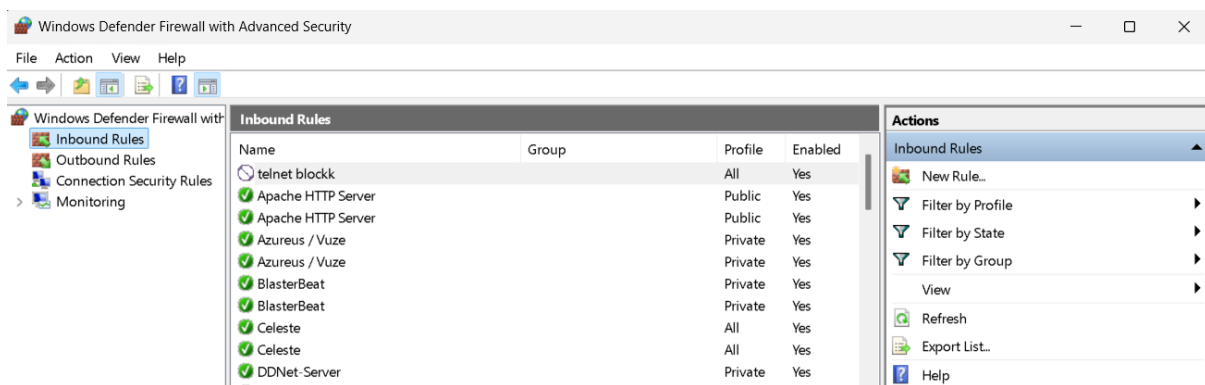
☒ Block the connection

< Back

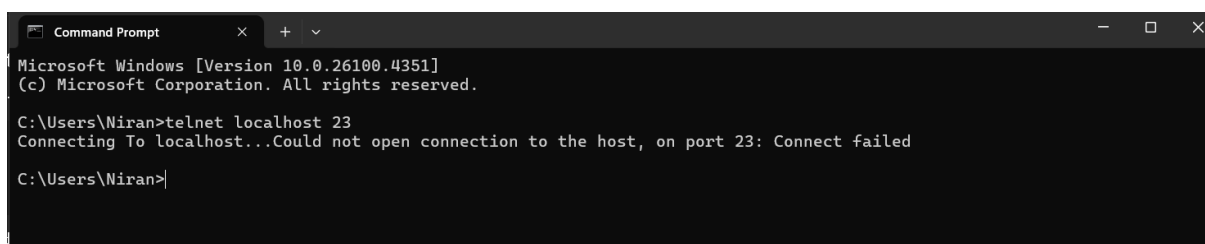
Next >

Cancel

It is now a new inbound rule:

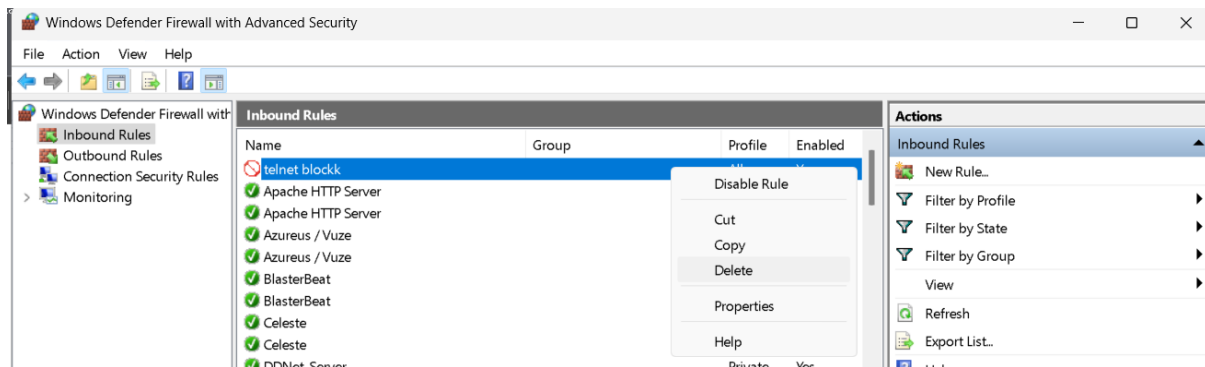


Now to test the rule:



The rule has been applied.

Now we delete this rule



So to summarize a firewall checks incoming and outgoing network traffic and decides who to allow or block based on defined security rules as seen above where blocking port 23 stops us from remotely connecting to it.