**Firewall configaration**

**TASK4:Setup and Use a Firewall on Windows/Linux**

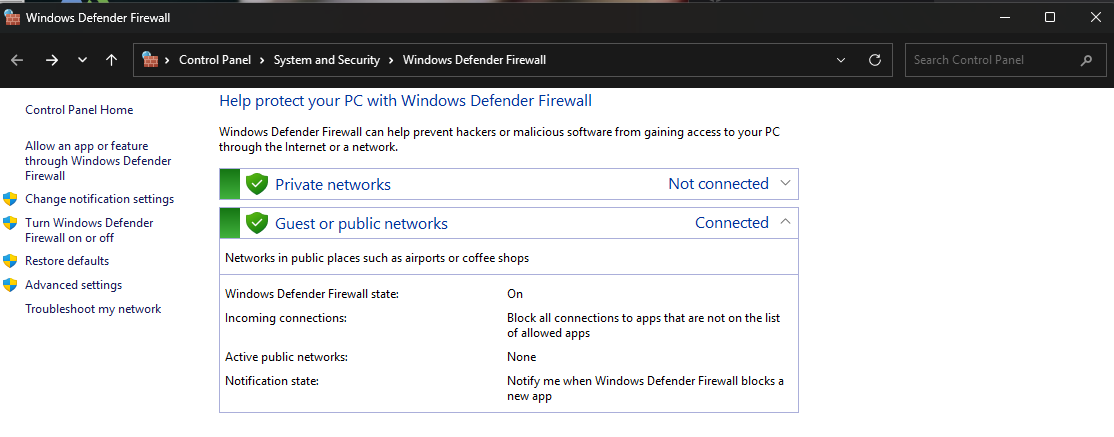
Objective: Configure and test basic firewall rules to allow or block traffic.

Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

Deliverables: Screenshot/configuration file showing firewall rules applied.

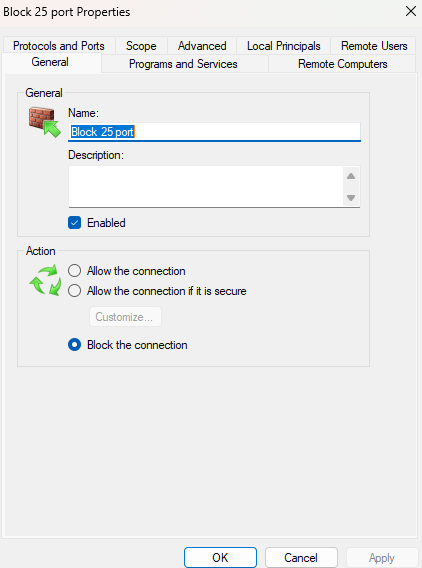
**Process:**

* Open firewall configuration tool
* In the windows, open the windows defender firewall.
* Search in windows /or in the run enter wf.msc



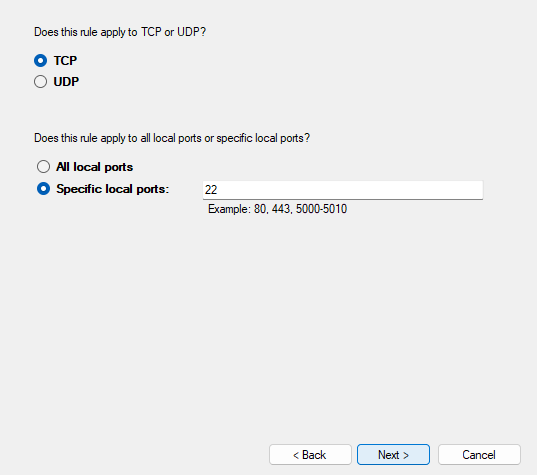
****

* Add a rule to block inbound traffic on a specific port.
* Select the inbound rules go to action write new rule.
* Select the rule type (select the port), enter next.
* Mention the specific local ports (enter 25port (SMTP)).
* Select the Block the connection and enter next.

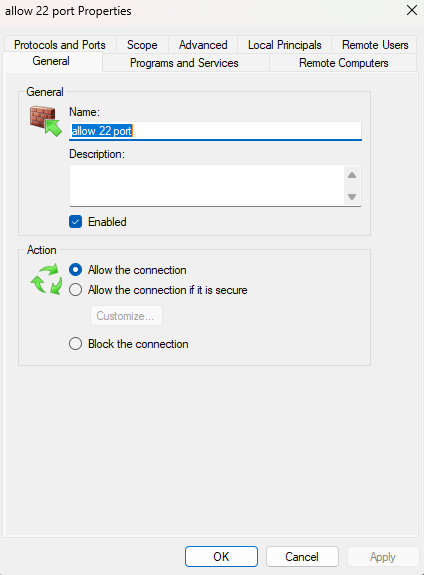


**BLOCK 25 PORT(SMTP)**

* Add rule to allow SSH (port 22)
* Select the inbound rules go to action write new rule.
* Select the rule type (select the port), enter next.

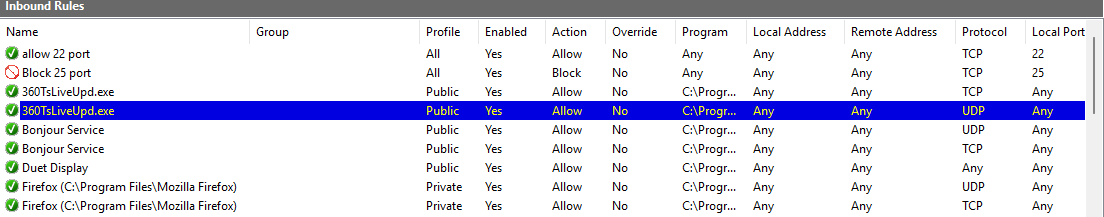


* Mention the specific local ports (enter 22port (SSH)).
* Select the Allow the connection and enter next.

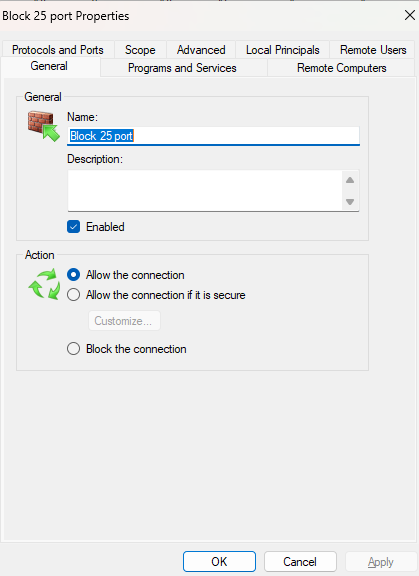


**ALLOW 22PORT (SSH)**

* Finally SMTP( 24) is blocked, and add rule to allow SSH (port 22)



* After that we remove the test block rule to restore original state.



* Allow to the connection