Firewall Configuration Assignment Report (Detailed Version)

1. Open Firewall Configuration Tool

- Press **Win + R**, type `wf.msc`, and press **Enter**.
- Windows Defender Firewall with Advanced Security opens.
- The console has three main sections:
  - **Inbound Rules**: Controls incoming traffic.
  - **Outbound Rules**: Controls outgoing traffic.
  - **Monitoring**: Shows applied firewall rules and their status.

2. List Current Firewall Rules

- Navigated to **Inbound Rules** to see all current inbound traffic rules.
- Verified rules using PowerShell:

```
Get-NetFirewallRule
```

- Observed properties:
  - **DisplayName**: Name of the rule.
  - **Direction**: Inbound or Outbound.
  - **Enabled**: Whether the rule is active.
  - **Action**: Allow or Block.
  - **Profiles**: Domain, Private, Public.

3. Add Rule to Block Inbound Traffic on Port 23 (Telnet)

GUI Steps: 1. In **Inbound Rules**, right-click → **New Rule...**
2. **Rule Type:** Select **Port** → Click **Next**.
3. **Protocol & Ports:** - Protocol: **TCP** - Specific local ports: `23` → Click **Next**
4. **Action:** Select **Block the connection** → Click **Next**
5. **Profile:** Check **Domain, Private, Public** → Click **Next**
6. **Name:** `BlockTelnet` → Click **Finish**

- The rule now blocks all inbound traffic on TCP port 23, preventing Telnet connections.

4. Test the Rule Using PowerShell

1. Open **PowerShell as Administrator**.
2. Run:

```
Test-NetConnection -ComputerName localhost -Port 23
```

3. Observed Output:
   - `PingSucceeded: True` → machine is reachable on the network.
   - `TcpTestSucceeded: False` → port 23 is blocked by the firewall.

Explanation: - The firewall successfully blocks TCP connections on port 23. - Even without Telnet installed, this test confirms the rule is active.

5. Remove the Test Block Rule

GUI Method: - In **Inbound Rules**, find **BlockTelnet** → Right-click → **Delete**.

PowerShell Method:

```
Remove-NetFirewallRule -DisplayName "BlockTelnet"
```

- Restores original firewall configuration for port 23.

6. Document Commands / GUI Steps Used

Task	Method / Command
List firewall rules	`Get-NetFirewallRule`
Create block rule (GUI)	Windows Firewall → Inbound Rules → New Rule → TCP 23 → Block → Domain/Private/Public → BlockTelnet
Test port	`Test-NetConnection -ComputerName localhost -Port 23`
Remove rule	`Remove-NetFirewallRule -DisplayName "BlockTelnet"` or GUI delete

7. Summary: How Firewall Filters Traffic

- Firewall inspects all network packets based on rules.
- **Inbound packets** are checked against **Inbound Rules**:
  - **Allow rule** → packet is permitted
  - **Block rule** → packet is dropped
- **Outbound packets** are checked against **Outbound Rules** similarly.

- Default behavior in Windows:
    - Inbound: mostly blocked unless allowed.
    - Outbound: mostly allowed unless blocked.
- Custom rules (like BlockTelnet) give administrators control over which ports and services are accessible.
- Testing with PowerShell confirmed the firewall is correctly blocking and allowing traffic as expected.

Conclusion

- Successfully created a new inbound firewall rule to block port 23.
- Tested the rule safely using PowerShell and observed expected results.
- Removed the test rule to restore the original firewall configuration.
- Demonstrated understanding of firewall operation, rule creation, testing, and removal.
- Assignment completed successfully without installing Telnet.