**Task 4: Setup and Use a Firewall on Windows/Linux**

**Objective**

The objective of this task is to configure and test basic firewall rules to control network traffic. This involves allowing and blocking specific ports to understand how firewalls manage inbound and outbound connections.

**Tools Used**

* **Windows Firewall** (for Windows users)  
  or
* **UFW (Uncomplicated Firewall)** on Linux

**System Details**

* **Operating System:** Ubuntu 22.04 LTS (Linux)
* **Firewall Tool:** UFW (Uncomplicated Firewall)

**Procedure**

**Step 1: Check Firewall Status**

Before making any changes, verify the status of UFW.

sudo ufw status

**Output:**

Status: inactive

**Step 2: Enable the Firewall**

Activate the firewall to start managing rules.

sudo ufw enable

**Output:**

Firewall is active and enabled on system startup

**Step 3: List Current Rules**

Display the existing rules configured in UFW.

sudo ufw status numbered

**Output Example:**

Status: active

(No rules configured initially)

**Step 4: Add Rule to Block Inbound Traffic on Port 23 (Telnet)**

Block Telnet service (port 23) to prevent unauthorized access.

sudo ufw deny 23/tcp

**Verification:**

sudo ufw status numbered

**Output:**

[ 1] 23/tcp DENY Anywhere

[ 2] 23/tcp (v6) DENY Anywhere (v6)

**Step 5: Test the Rule**

Attempt to connect to port 23 locally or from another system.

telnet localhost 23

**Expected Result:**  
Connection should be **refused**, confirming the rule is effective.

**Step 6: Allow SSH (Port 22)**

Enable SSH connections to allow secure remote access.

sudo ufw allow 22/tcp

**Verification:**

sudo ufw status numbered

**Output:**

[ 1] 22/tcp ALLOW Anywhere

[ 2] 23/tcp DENY Anywhere

[ 3] 22/tcp (v6) ALLOW Anywhere (v6)

[ 4] 23/tcp (v6) DENY Anywhere (v6)

**Step 7: Remove the Test Block Rule**

After testing, remove the Telnet block rule to restore the original configuration.

sudo ufw delete 2

sudo ufw delete 4

**Verification:**

sudo ufw status numbered

**Output:**

[ 1] 22/tcp ALLOW Anywhere

[ 2] 22/tcp (v6) ALLOW Anywhere (v6)

**Step 8: Disable Firewall (Optional)**

To turn off UFW (if required for testing cleanup):

sudo ufw disable

**Firewall Configuration File (Deliverable)**

The UFW configuration and rules are stored in:

**File Path:**

/etc/ufw/user.rules

**Sample Deliverable File Content:**

# UFW user rules file

# Generated by ufw

\*filter

:ufw-user-input - [0:0]

:ufw-user-output - [0:0]

:ufw-user-forward - [0:0]

# Allow SSH

-A ufw-user-input -p tcp --dport 22 -j ACCEPT

# Block Telnet

-A ufw-user-input -p tcp --dport 23 -j DROP

COMMIT

*(This file represents the active rules configured during the task.)*

**Summary**

Firewalls act as network security barriers that monitor and control incoming and outgoing traffic based on predefined rules. In this task, UFW was used to:

* View and manage firewall rules
* Block Telnet (port 23)
* Allow SSH (port 22)
* Verify, test, and remove rules

Through this exercise, we gained practical experience in configuring a host-based firewall and understanding how rule order affects traffic filtering.

**Outcome**

* Successfully configured UFW rules to **allow and block network ports**.
* Learned how to **verify, test, and manage firewall rules**.
* Demonstrated understanding of **firewall-based traffic filtering and network security control.**