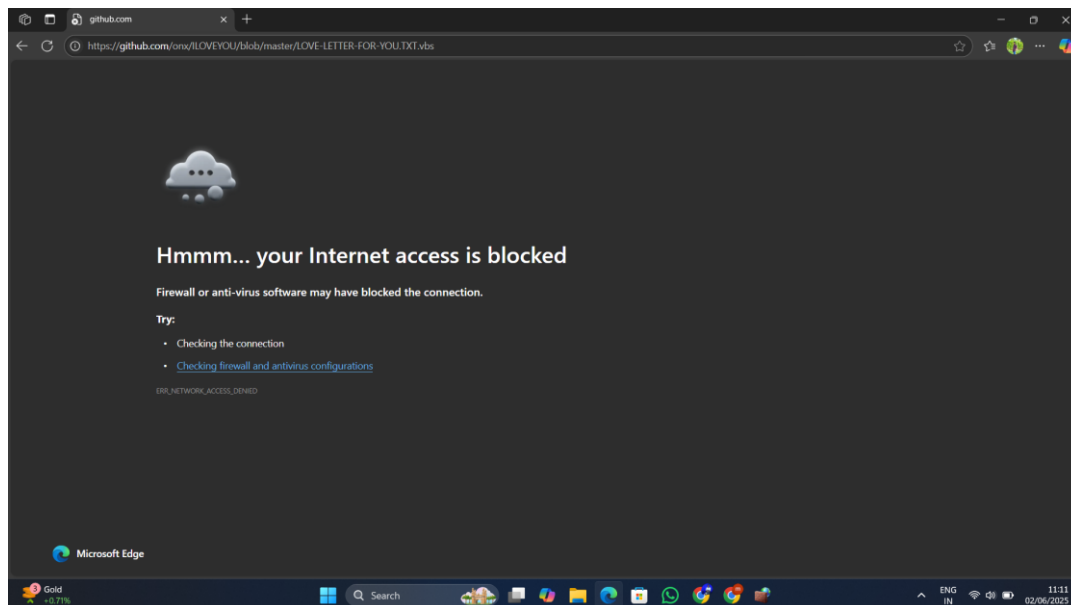
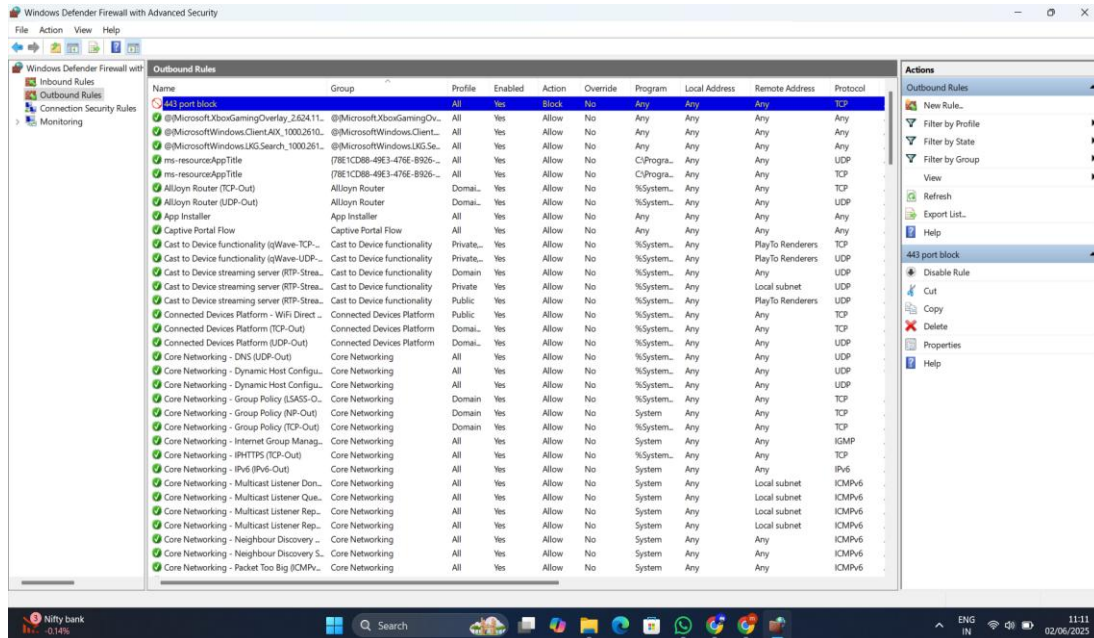
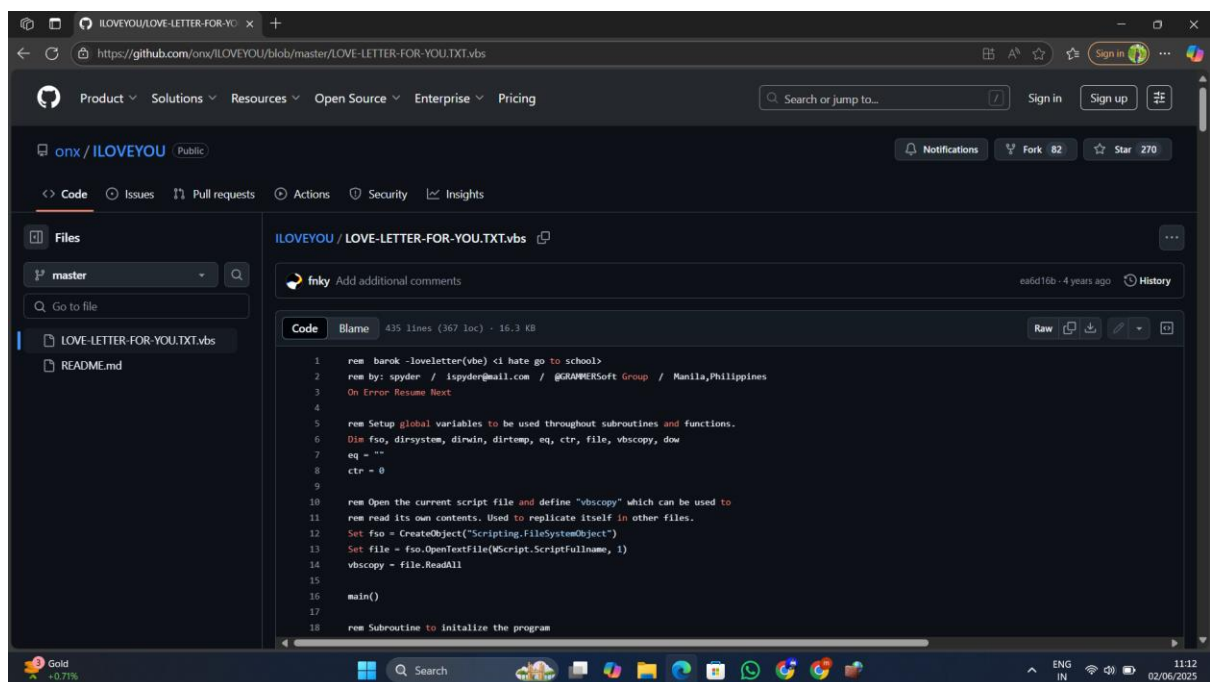
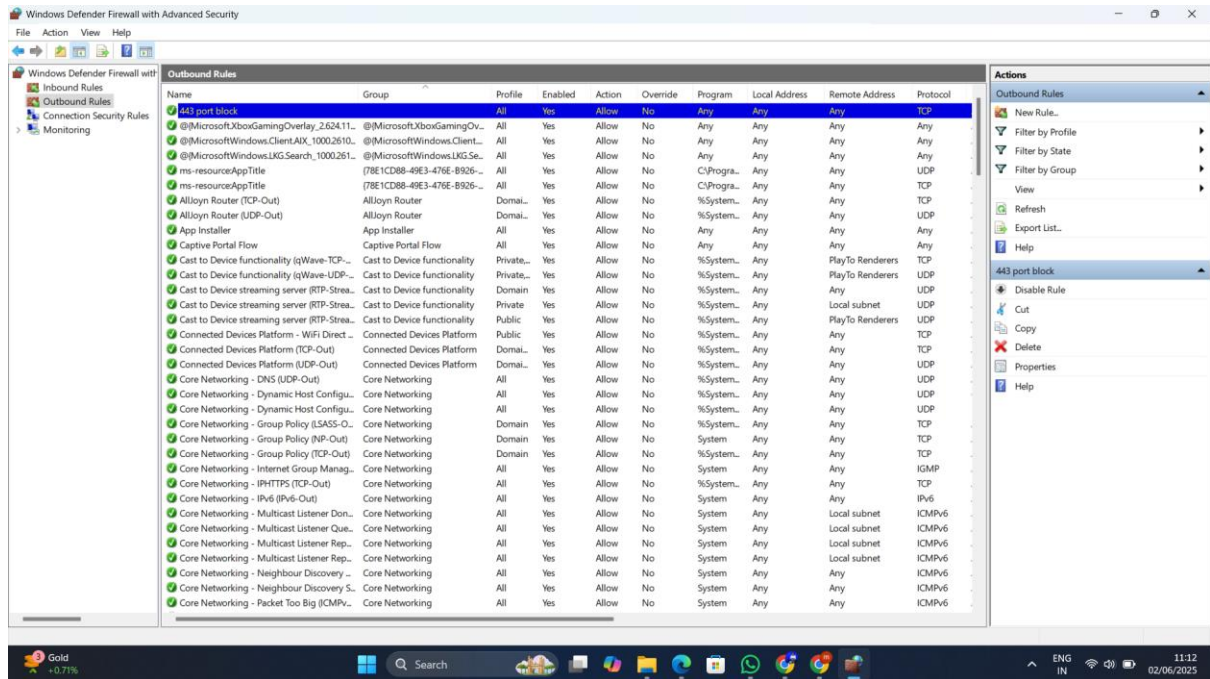


# REPORT ON TASK-4

BLOCKED PORT :



## UNBLOCKED PORT:



# Official Report: Summary of Firewall Traffic Filtering in Windows 11

---

## 1. Overview

This report provides a summary of firewall traffic filtering capabilities and activities within the Windows 11 operating system. Windows Defender Firewall is the built-in solution responsible for regulating inbound and outbound network traffic according to defined security rules.

---

## 2. Firewall Architecture in Windows 11

- **Firewall Component:** Windows Defender Firewall with Advanced Security (WFAS)
  - **Integration:** Deep integration with the Windows Security Center and Group Policy Management
  - **Profiles Supported:**
    - Domain
    - Private
    - Public
- 

## 3. Traffic Filtering Capabilities

Feature	Description
Inbound Rules	Controls traffic coming into the system.
Outbound Rules	Controls traffic leaving the system.
Port-based Filtering	Allows or blocks traffic based on specific TCP/UDP ports.
Program-based Filtering	Enables or blocks traffic based on executable files.
Protocol-based Filtering	Filters traffic based on IP protocols (TCP, UDP, ICMP, etc.).
IP Address Filtering	Permits or denies traffic based on source or destination IP addresses.
Profile Awareness	Applies different rule sets based on the network location profile.

Feature	Description
Connection Security Rules	Enforces IPsec authentication and encryption for secured communications.

---

#### 4. Default Behavior

##### Traffic Direction Default Action

Inbound	Block
---------	-------

Outbound	Allow
----------	-------

- The default settings are designed to minimize attack surfaces while maintaining essential outbound communications.

---

#### 5. Traffic Logging and Monitoring

- **Log File Location:**  
%systemroot%\system32\LogFiles\Firewall\pfirewall.log
- **Loggable Events:**
  - Dropped packets
  - Successful connections (optional)
- **Configuration:**
  - Logging settings adjustable via GUI (WFAS) or netsh / PowerShell
  - Audit Policy integration for log forwarding to SIEM solutions

---

#### 6. Administrative Interfaces

Interface	Usage
Windows Defender Firewall GUI	Basic rule creation, profile management, logging settings
Windows Security App	General status and basic configuration
Group Policy Editor	Enterprise-wide rule enforcement
PowerShell (New-NetFirewallRule)	Advanced rule creation, automation

Interface	Usage
netsh advfirewall	Legacy CLI tool for firewall configuration

---

7. Summary of Active Rules (Example)

Rule Name	Direction	Action	Profile	Enabled	Description
File and Printer Sharing	Inbound	Allow	Private	Yes	Enables sharing resources on LAN
Remote Desktop	Inbound	Allow	Domain	Yes	Allows RDP access in corporate LAN
Block All Unlisted	Inbound	Block	All	Yes	Denies all other unlisted traffic

---

8. Conclusion

Windows 11's firewall offers a robust and flexible framework for controlling network access to and from the system. Through built-in tools, policy support, and advanced features like IPsec, it supports both individual user security and enterprise-grade protection.