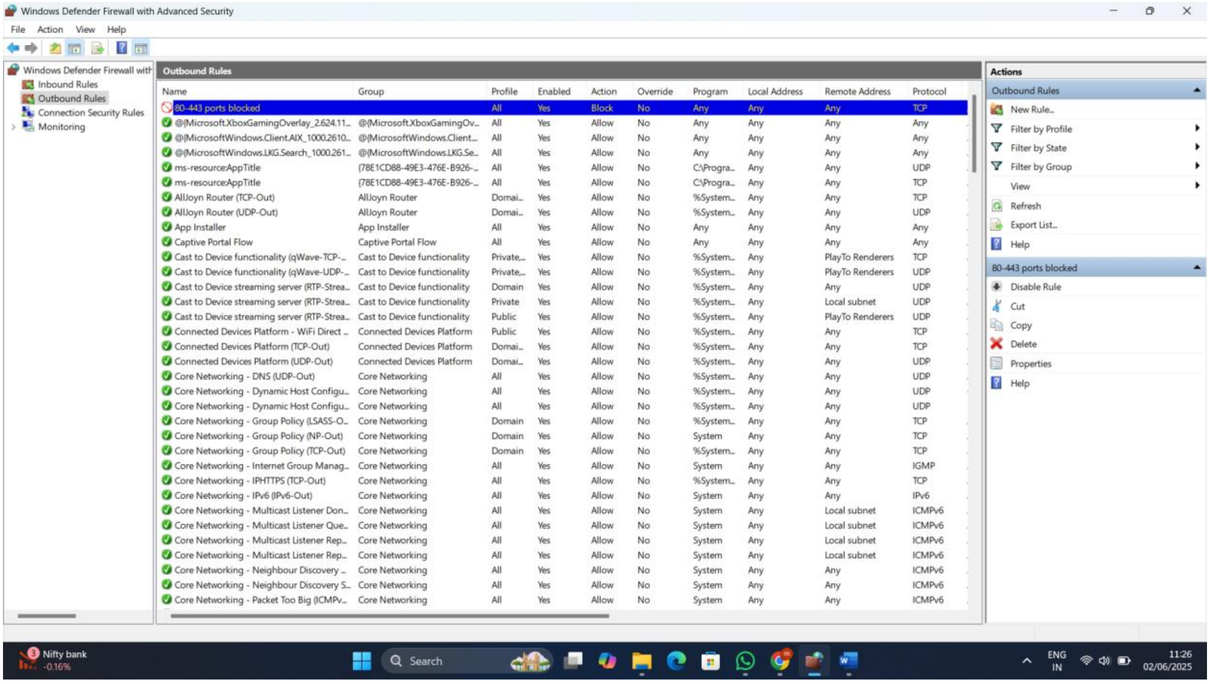
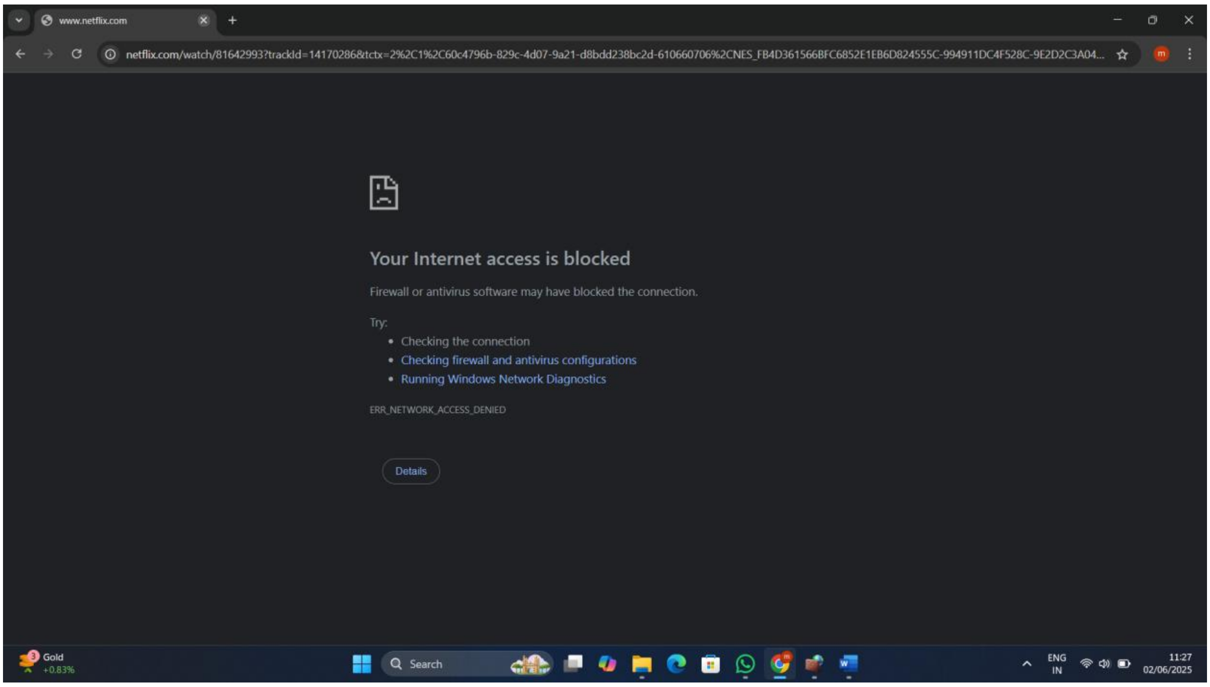
REPORT ON TASK-4

BLOCKED PORT :



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
80-443 ports blocked		All	Yes	Block	No	Any	Any	Any	TCP
@{Microsoft.XboxGamingOverlay_2.624.11...	@{Microsoft.XboxGamingOv...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Client.AIX_1000.2610...	@{MicrosoftWindows.Client...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.Search_1000.261...	@{MicrosoftWindows.LKG.Se...	All	Yes	Allow	No	Any	Any	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Connected Devices Platform - WiFi Direct ...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Group Policy (LSASS-O...	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any	Any	TCP
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Core Networking - Internet Group Manag...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	TCP
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6
Core Networking - Multicast Listener Don...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Multicast Listener Que...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Neighbour Discovery ...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Neighbour Discovery S...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Packet Too Big (ICMPv...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6



netflix.com/watch/81642993?trackId=14170286&tctx=2%2C1%2C60c4796b-829c-4d07-9a21-d8bdd238bc2d-610660706%2CNES_FB4D361566BFC6852E1EB6D824555C-994911DC4F528C-9E2D2C3A04...

Your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

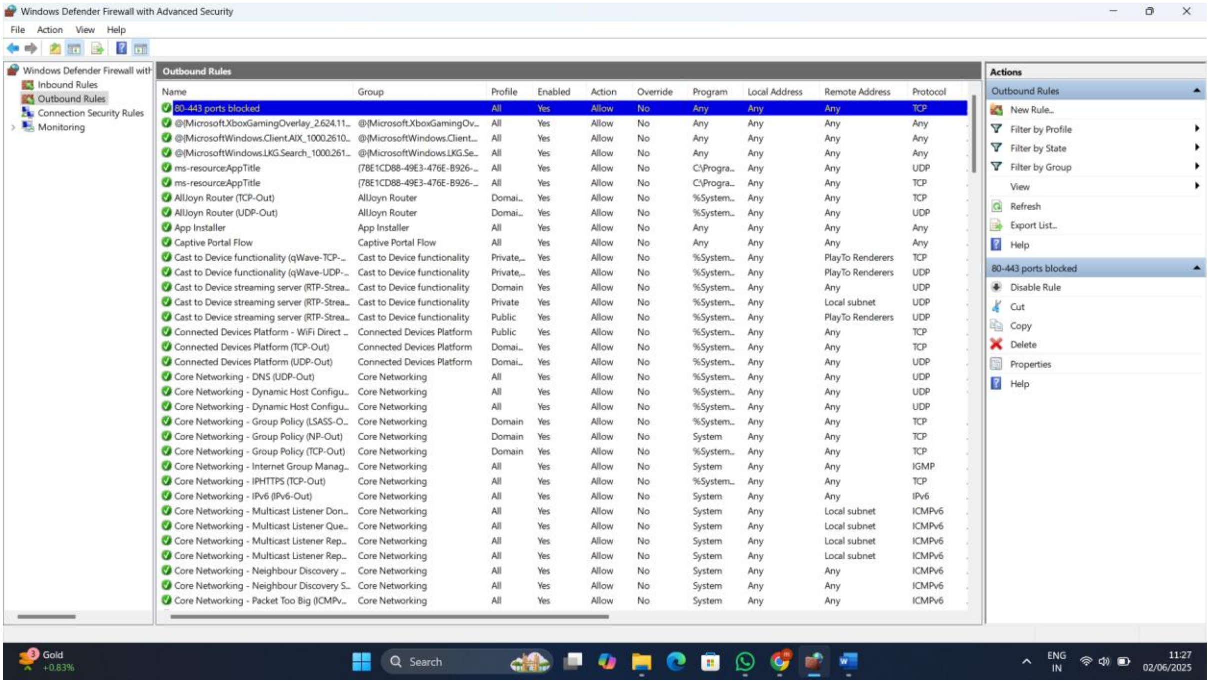
Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

ERR_NETWORK_ACCESS_DENIED

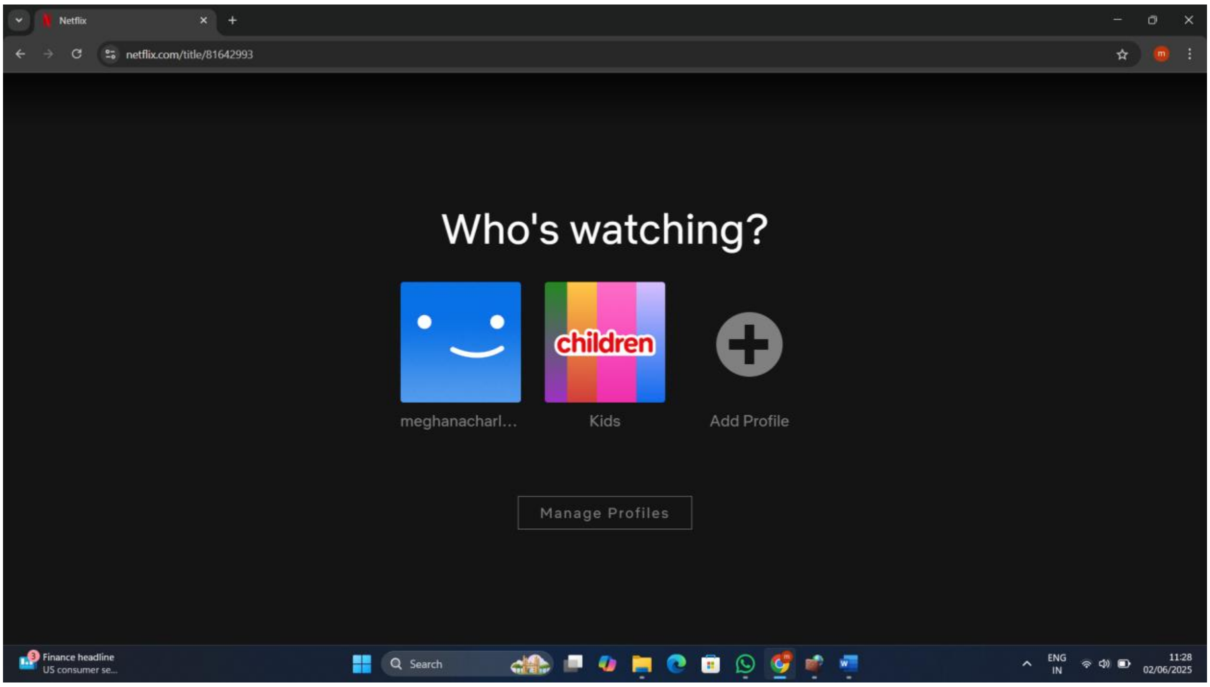
Details

UNBLOCKED PORT:



Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
80-443 ports blocked		All	Yes	Allow	No	Any	Any	Any	TCP
@{Microsoft.XboxGamingOverlay_2.624.11...	@{Microsoft.XboxGamingOv...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.Client.AIX_1000.2610...	@{MicrosoftWindows.Client...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.Search_1000.261...	@{MicrosoftWindows.LKG.Se...	All	Yes	Allow	No	Any	Any	Any	Any
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Connected Devices Platform - WiFi Direct ...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Group Policy (LSASS-O...	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any	Any	TCP
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Core Networking - Internet Group Manag...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	TCP
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6
Core Networking - Multicast Listener Don...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Multicast Listener Que...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking - Neighbour Discovery ...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Neighbour Discovery S...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Packet Too Big (ICMPv...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6



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.
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
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.