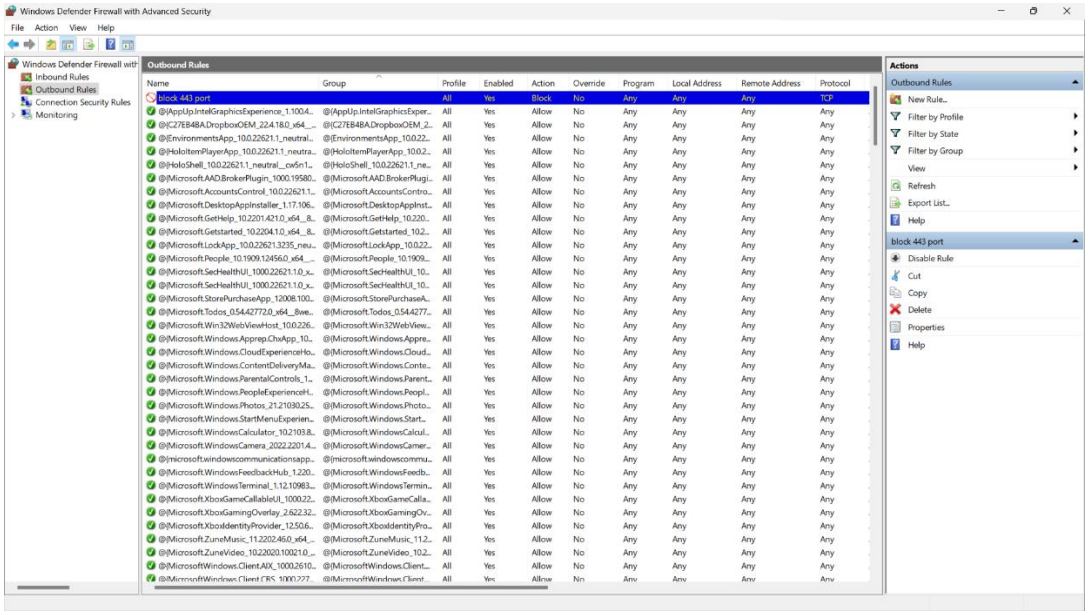
Task-4

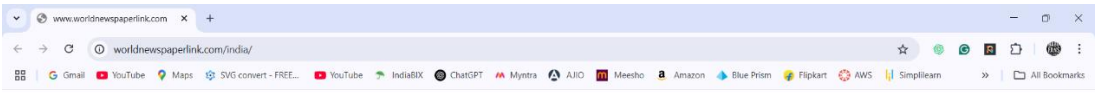
OFFCIAL REPORT ON

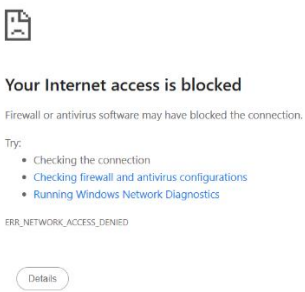
Setup and use a Firewall on Windows/Linux

Firewall Traffic Filtering Summary Report
Operating System: Windows 11
Date: [June 1 2025]
Prepared by: [Sandeep]

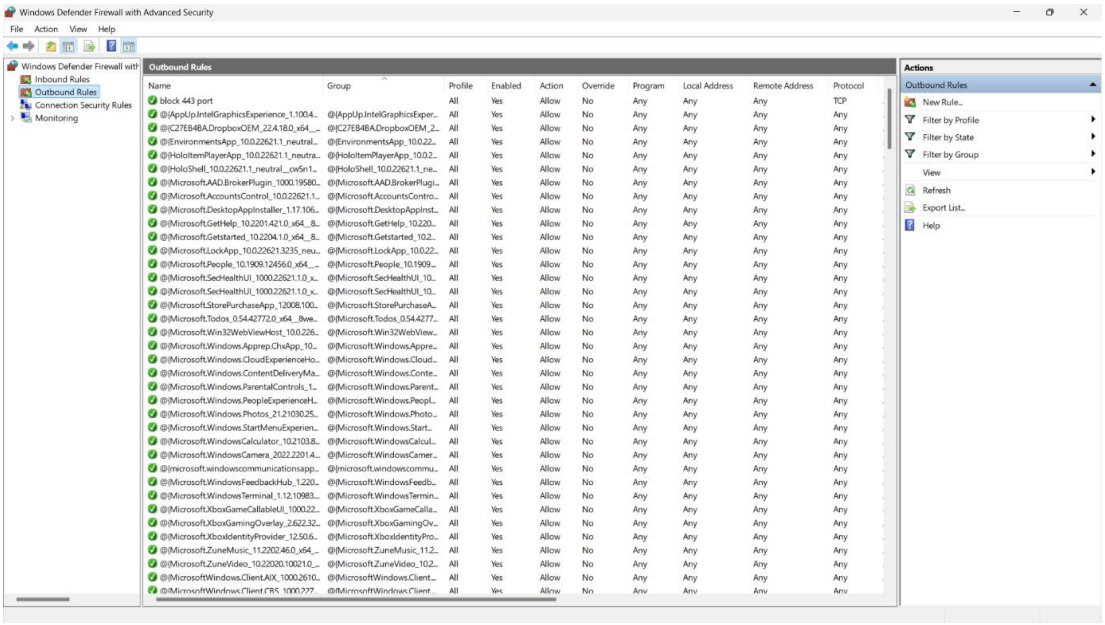
- Block 443 port (HTTPS)

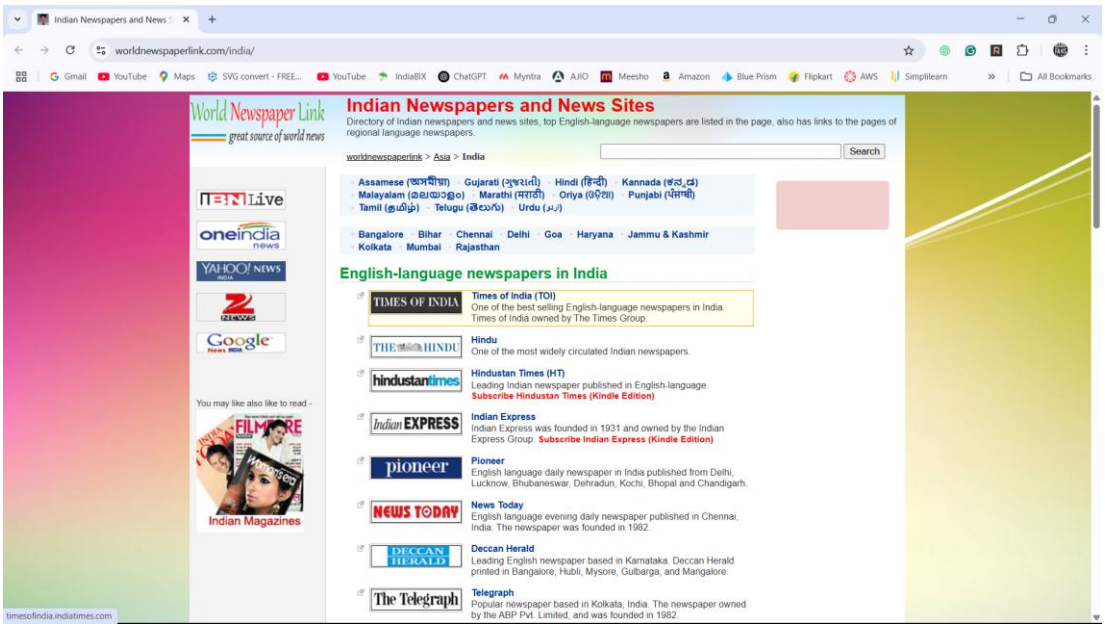






- Unblock 443 port (Https)





---

1. Introduction

This report provides a summary of firewall traffic filtering on Windows 11 systems. Windows Defender Firewall is integrated into Windows Security and plays a critical role in managing inbound and outbound traffic to enhance system security.

---

2. Firewall Overview

Windows Defender Firewall uses a rule-based engine to filter network traffic. Rules can be configured for programs, ports, services, and IP addresses. It operates in three profiles:

- **Domain Profile** – For systems connected to an Active Directory domain.
- **Private Profile** – For trusted networks such as home or work.
- **Public Profile** – For untrusted networks such as public Wi-Fi.

---

3. Traffic Filtering Components

Component	Description
Inbound Rules	Control traffic allowed **into** the system.
Outbound Rules	Control traffic **leaving** the system.
Connection Security Rules	Define how and when IPsec is used to protect traffic.
Monitoring	Provides logs and real-time monitoring of allowed/blocked connections.

---

4. Filtering Mechanisms

- **Application-Based Filtering:** Rules can allow or block specific executable files.
- **Port-Based Filtering:** Specific TCP or UDP ports can be allowed or blocked.
- **Protocol-Based Filtering:** Filters by IP, ICMP, or custom protocols.
- **IP Address Filtering:** Allows or blocks based on source or destination IPs/subnets.
- **Network Profile Filtering:** Rules apply based on network trust levels (Domain, Private, Public).

---

5. Configuration Methods

- **Windows Security App:**
  Settings > Privacy & Security > Windows Security > Firewall & Network Protection
- **Control Panel:**
  Control Panel > System and Security > Windows Defender Firewall
- **Advanced Security MMC Snap-in:**
  wf.msc command for detailed rule management.

- **PowerShell:**
  Examples:

powershell

CopyEdit

Get-NetFirewallRule

New-NetFirewallRule -DisplayName "Block FTP" -Direction Outbound -Protocol TCP -RemotePort 21 -Action Block

- **Group Policy (Enterprise):**
  Used to enforce standardized rules across multiple endpoints.

---

6. Logging and Monitoring

- **Log File Location:**
  %SystemRoot%\System32\LogFiles\Firewall\pfirewall.log
- **Event Viewer Logs:**
  Applications and Services Logs > Microsoft > Windows > Windows Firewall With Advanced Security
- **Real-Time Alerts:**
  Can be configured via third-party SIEM tools or custom scripts.

---

7. Common Use Cases

Scenario	Action
Block unauthorized remote access	Create inbound rules to block RDP, SMB, etc.
Allow corporate VPN	Permit traffic on required ports/IPs.
Prevent malware C2 communication	Use outbound filtering to block suspicious IPs/domains.

---

8. Recommendations

- Regularly audit and review firewall rules.
- Use least privilege principles – deny by default, allow only necessary traffic.
- Monitor logs for unusual patterns or blocked attempts.
- Deploy group policies for enterprise-wide rule enforcement.

---

9. Conclusion

Windows 11 Firewall provides robust, flexible, and easily configurable traffic filtering capabilities. Proper management of firewall rules helps minimize attack surfaces and enforces strong endpoint security practices.

[Signature]
Name: Y.sandeep
Signature: Sandeep
Date: June 1 2025