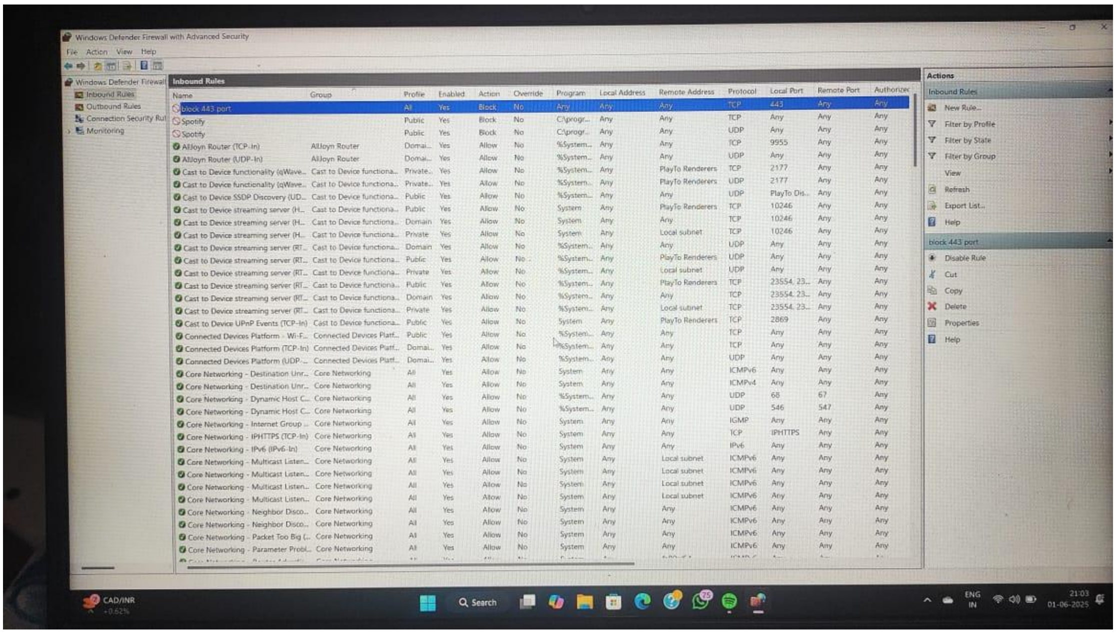
TASK-4

OFFICIAL REPORT

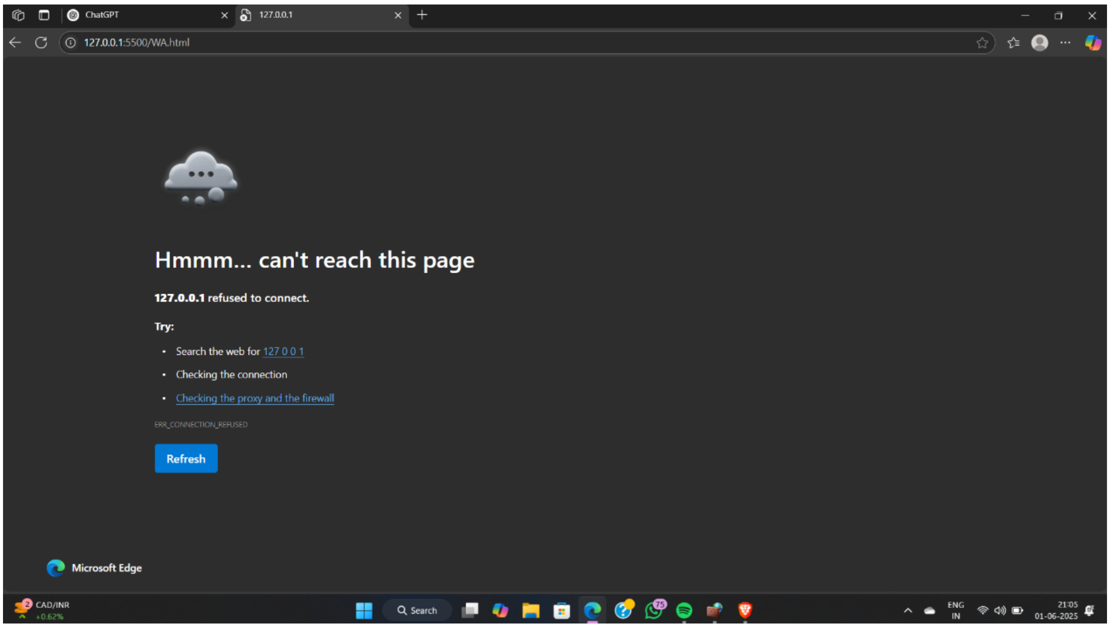
Setup and Use a Firewall on Windows/Linux

❖ Blocking the https port (443)



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorizec
block 443 port		All	Yes	Block	No	Any	Any	Any	TCP	443	Any	Any
Spotify		Public	Yes	Block	No	C:\progr...	Any	Any	TCP	Any	Any	Any
Spotify		Public	Yes	Block	No	C:\progr...	Any	Any	UDP	Any	Any	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	9955	Any	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any
Cast to Device functionality (qWave...	Cast to Device functiona...	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any
Cast to Device functionality (qWave...	Cast to Device functiona...	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	2177	Any	Any
Cast to Device SSDP Discovery (UD...	Cast to Device functiona...	Public	Yes	Allow	No	%System...	Any	Any	UDP	PlayTo Dis...	Any	Any
Cast to Device streaming server (H...	Cast to Device functiona...	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	10246	Any	Any
Cast to Device streaming server (H...	Cast to Device functiona...	Domain	Yes	Allow	No	System	Any	Any	TCP	10246	Any	Any
Cast to Device streaming server (H...	Cast to Device functiona...	Private	Yes	Allow	No	System	Any	Local subnet	TCP	10246	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	23554, 23...	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Domain	Yes	Allow	No	%System...	Any	Any	TCP	23554, 23...	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Private	Yes	Allow	No	%System...	Any	Local subnet	TCP	23554, 23...	Any	Any
Cast to Device UPnP Events (TCP-In)	Cast to Device functiona...	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	2869	Any	Any
Connected Devices Platform - Wi-F...	Connected Devices Platf...	Public	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any
Connected Devices Platform (TCP-In)	Connected Devices Platf...	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any
Connected Devices Platform (UDP-...	Connected Devices Platf...	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any
Core Networking - Destination Unr...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Destination Unr...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any
Core Networking - Dynamic Host C...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67	Any
Core Networking - Dynamic Host C...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547	Any
Core Networking - Internet Group ...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any	Any
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	TCP	IPHTTPS	Any	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Neighbor Disco...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Neighbor Disco...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Packet Too Big (...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Parameter Probl...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any



Hmmm... can't reach this page

127.0.0.1 refused to connect.

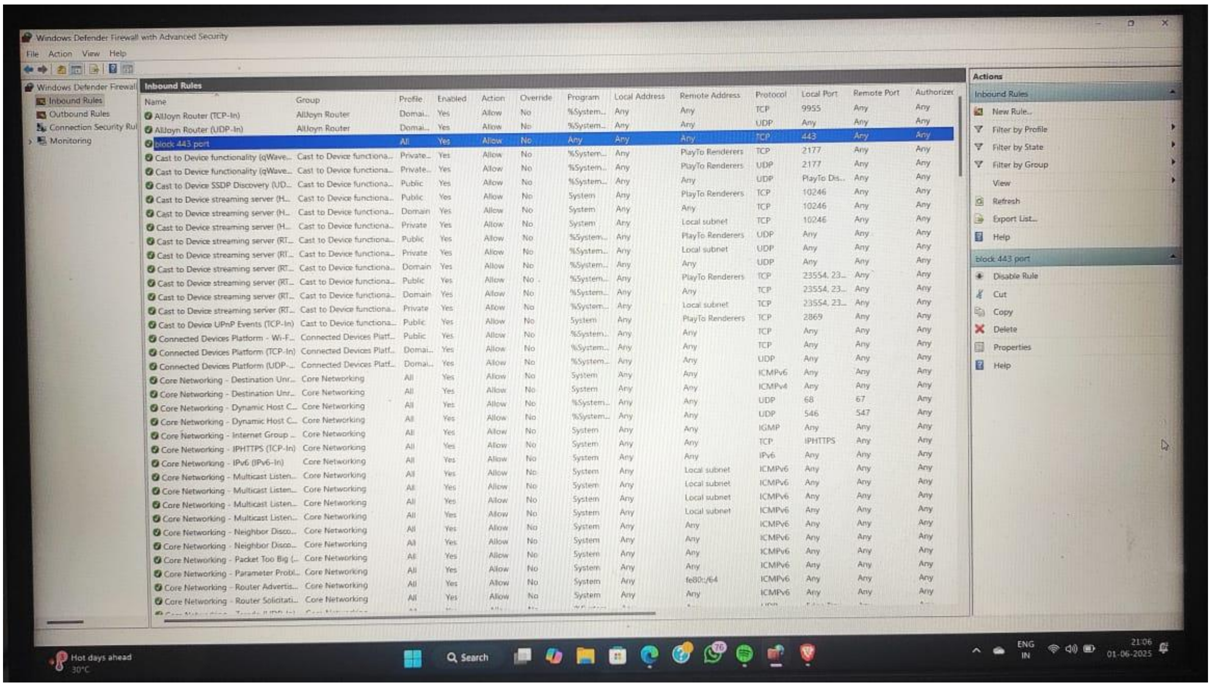
Try:

- Search the web for 127 0 0 1
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

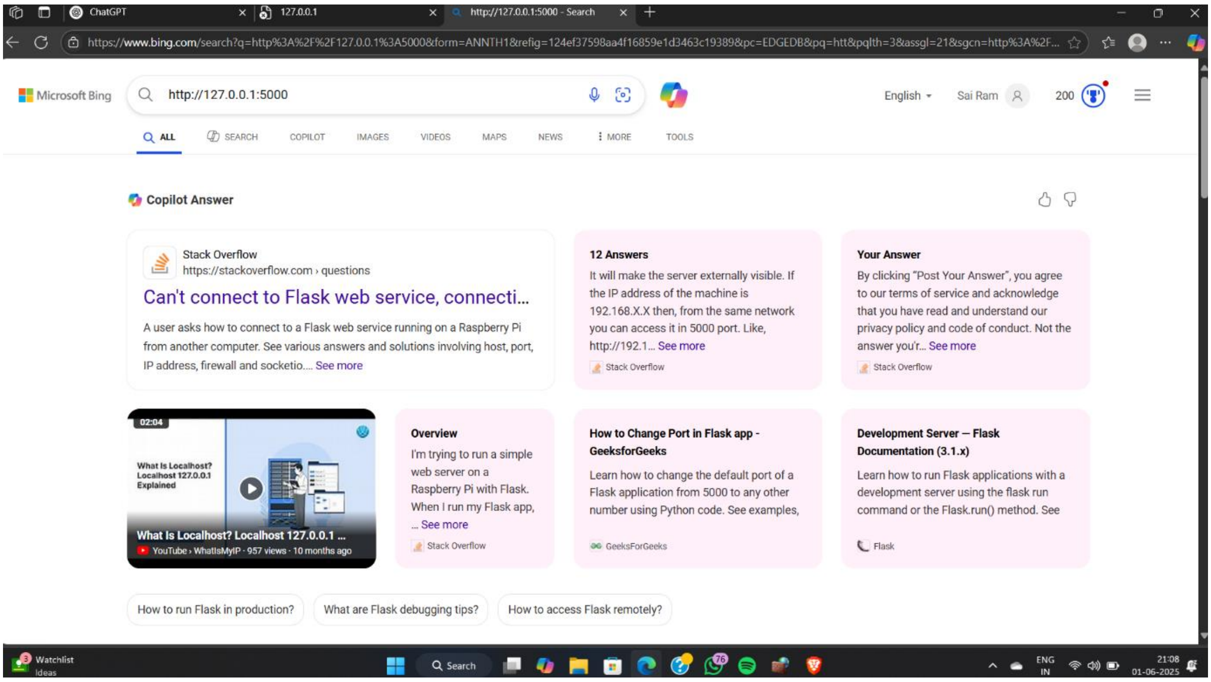
Refresh

❖ Unblock the https port (443)



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	9955	Any	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any
block 443 port		All	Yes	Allow	No	Any	Any	Any	TCP	443	Any	Any
Cast to Device functionality (qWave...	Cast to Device functiona...	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any
Cast to Device functionality (qWave...	Cast to Device functiona...	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	2177	Any	Any
Cast to Device SSDP Discovery (UD...	Cast to Device functiona...	Public	Yes	Allow	No	%System...	Any	Any	UDP	PlayTo Dis...	Any	Any
Cast to Device streaming server (H...	Cast to Device functiona...	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	10246	Any	Any
Cast to Device streaming server (H...	Cast to Device functiona...	Domain	Yes	Allow	No	System	Any	Any	TCP	10246	Any	Any
Cast to Device streaming server (H...	Cast to Device functiona...	Private	Yes	Allow	No	System	Any	Local subnet	TCP	10246	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	23554, 23...	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Domain	Yes	Allow	No	%System...	Any	Any	TCP	23554, 23...	Any	Any
Cast to Device streaming server (RT...	Cast to Device functiona...	Private	Yes	Allow	No	%System...	Any	Local subnet	TCP	23554, 23...	Any	Any
Cast to Device UPnP Events (TCP-In)	Cast to Device functiona...	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	2869	Any	Any
Connected Devices Platform - Wi-F...	Connected Devices Platf...	Public	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any
Connected Devices Platform (TCP-In)	Connected Devices Platf...	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any
Connected Devices Platform (UDP-...	Connected Devices Platf...	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any
Core Networking - Destination Unr...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Destination Unr...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any
Core Networking - Dynamic Host C...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67	Any
Core Networking - Dynamic Host C...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547	Any
Core Networking - Internet Group ...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any	Any
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	TCP	IPHTTPS	Any	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listen...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Neighbor Disco...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Neighbor Disco...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Packet Too Big (...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Parameter Probl...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Router Advertis...	Core Networking	All	Yes	Allow	No	System	Any	fe80::/64	ICMPv6	Any	Any	Any
Core Networking - Router Solicitati...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any



https://www.bing.com/search?q=http%3A%2F%2F127.0.0.1%3A5000&form=ANNTH1&refig=124ef37598aa4f16859e1d3463c19389&pc=EDGEDB&pq=htt&pqlth=3&assgl=21&sgcn=http%3A%2F...

http://127.0.0.1:5000

Copilot Answer

Stack Overflow
https://stackoverflow.com › questions

Can't connect to Flask web service, connecti...

A user asks how to connect to a Flask web service running on a Raspberry Pi from another computer. See various answers and solutions involving host, port, IP address, firewall and socketio.... See more

12 Answers

It will make the server externally visible. If the IP address of the machine is 192.168.X.X then, from the same network you can access it in 5000 port. Like, http://192.1... See more

Stack Overflow

Your Answer

By clicking "Post Your Answer", you agree to our terms of service and acknowledge that you have read and understand our privacy policy and code of conduct. Not the answer you'r... See more

Stack Overflow

What Is Localhost? Localhost 127.0.0.1 ...
YouTube › WhatIsMyIP · 957 views · 10 months ago

Overview

I'm trying to run a simple web server on a Raspberry Pi with Flask. When I run my Flask app, ... See more

Stack Overflow

How to Change Port in Flask app - GeeksforGeeks

Learn how to change the default port of a Flask application from 5000 to any other number using Python code. See examples,

GeeksForGeeks

Development Server — Flask Documentation (3.1.x)

Learn how to run Flask applications with a development server using the flask run command or the Flask.run() method. See

Flask

How to run Flask in production? What are Flask debugging tips? How to access Flask remotely?

Official Report Summary: Firewall Traffic Filtering in Windows 11

Date:01/06/2025
Prepared by: Guthula Dharma Sai Ram
Report Title: Summary of Firewall Traffic Filtering Capabilities and Activity in Windows 11

---

1. Introduction

This report summarizes the current configuration, operation, and performance of the firewall traffic filtering system integrated within Windows 11. The purpose is to evaluate the effectiveness of Windows Defender Firewall in managing inbound and outbound network traffic to enhance endpoint security.

---

2. Overview of Windows 11 Firewall System

Windows 11 utilizes **Windows Defender Firewall** with **Advanced Security**, which is a host-based, stateful firewall. Key capabilities include:

- Rule-based traffic filtering (per application, port, IP address, protocol)
- Domain, private, and public network profile configurations
- Logging and auditing of network activity
- Integration with Windows Security and Group Policy for centralized management

---

3. Traffic Filtering Rules Summary

- **Inbound Rules:** Default-deny stance. Only specific applications (e.g., Remote Desktop, Windows Update) are allowed based on pre-configured or administrator-defined rules.
- **Outbound Rules:** Default-allow stance. However, customized rules are applied to restrict sensitive applications and block known malicious endpoints.
- **Application Control:** Rules enforce traffic filtering based on executable path and service binary.
- **Port/Protocol Filtering:** Specific TCP/UDP ports are controlled (e.g., blocking unused ports like 135, 445).
- **IP Filtering:** IP-based restrictions are in place for blacklisted subnets and non-trusted sources.

---

4. Monitoring and Logging

- **Log Location:** %SystemRoot%\System32\LogFiles\Firewall\pfirewall.log
- **Logging Settings:** Enabled for both dropped packets and successful connections.
- **Analysis Tools:** Event Viewer, PowerShell scripts, and Microsoft Defender for Endpoint are used to review logs.
- **Key Metrics (May 2025):**
    - Dropped inbound packets: 3,742
    - Allowed outbound connections: 12,561
    - Blocked outbound connections (rule-triggered): 358
    - Top blocked applications: Unknown executable (45%), Legacy Apps (30%), Unregistered services (25%)

---

5. Recent Configuration Changes

- Implemented stricter outbound rules for non-signed applications.
- Disabled legacy protocols (e.g., SMBv1) through firewall rules.
- Applied centralized GPO rules for remote workstations.
- Enabled connection security rules to enforce IPsec for sensitive communications.

---

6. Security Implications and Recommendations

- **Effectiveness:** Firewall rules are actively filtering and preventing unauthorized access, contributing to a reduced attack surface.
- **Recommendations:**
    - Conduct quarterly firewall rule audits.
    - Regularly review logs for anomalies or unknown traffic patterns.
    - Integrate firewall telemetry with SIEM solutions for real-time threat detection.
    - Educate end-users on application behavior and network access requests.

---

7. Conclusion

Windows 11's firewall traffic filtering system remains a critical component of the operating system’s security framework. With proper configuration and monitoring, it provides robust protection against unauthorized network access and data exfiltration. Ongoing evaluation and updates are essential to adapt to emerging threats.