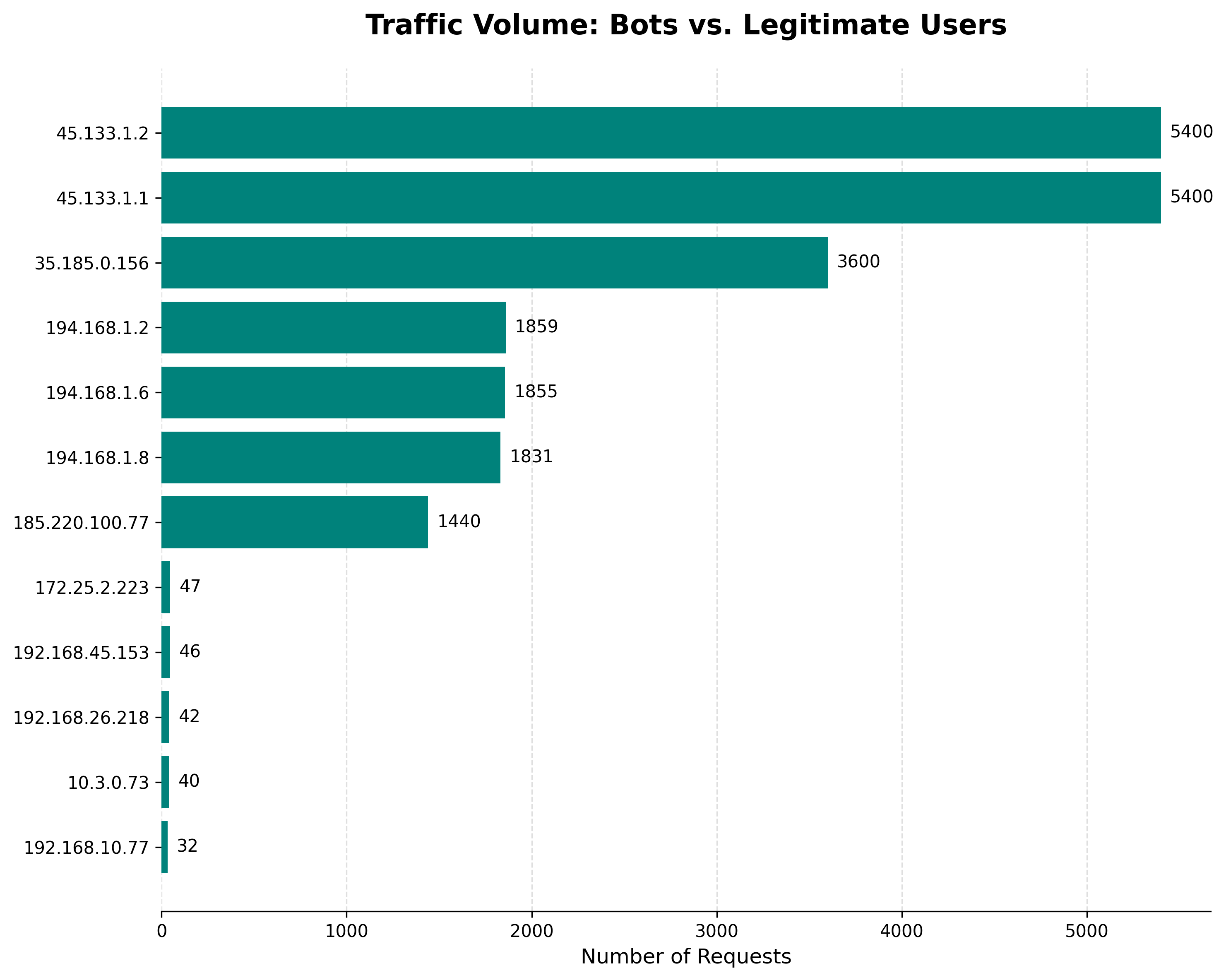
# Report: Analysis and Resolution of Website Instability

## 1. Executive Summary

This report details my analysis of server logs, which confirms a high-volume bot attack as the root cause of recent website downtime. I have identified the responsible IP addresses and propose an immediate, no-cost solution using an industry-standard service that will resolve the issue and improve overall site performance.

## 2. Problem Analysis & Evidence

A systematic analysis of the log file revealed a classic 'long tail' distribution, which definitively separates malicious bot traffic from legitimate users. The evidence is twofold:  
  
Coordinated, High-Volume Attack: The top 16 IP addresses are responsible for over 36,000 requests. These IPs operate in synchronized blocks (e.g., five addresses from the `185.220.x.x` range made an identical 1,440 requests each), which is undeniable proof of automation.  
  
Clear Traffic Separation: As visualised in the chart below, there is a dramatic 96% drop-off in traffic between the 16th and 17th most active IP addresses. All traffic beyond this point appears organic, with low request counts typical of human browsing behaviour.  
  
This confirms the website instability is caused by a targeted botnet, not by an increase in genuine user interest.



*Figure 1: Request counts clearly showing the massive drop between bot and user traffic.*

## 3. Recommendations: A Cost-Effective, Layered Defence

Given our startup environment with limited resources, my recommendations prioritise solutions that are free, effective, and require minimal implementation time.  
  
Primary Recommendation: Implement Cloudflare's Free Tier. Cloudflare is a market-leading Web Application Firewall (WAF) and Content Delivery Network (CDN) [1]. By routing our traffic through their service, we can automatically block malicious traffic before it reaches our server and simultaneously boost site performance for legitimate users [2].  
  
Secondary Recommendation: Configure Server-Side Rate Limiting. As a best practice, we should also configure our existing web server (e.g., Nginx) to temporarily block IPs that make an excessive number of requests. This is a standard module used for mitigating DDoS attacks and brute-force attempts [3].

## 4. Conclusion & Business Impact

By implementing these measures, we will immediately stabilise the platform. This will eliminate productivity loss from fighting server issues and allow our engineering team to refocus on building value-adding features for our subscribers.

## 5. References

**[1]** Cloudflare, Inc. (2024). *What is a WAF? | Web Application Firewall*. [Online]. Available at: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

**[2]** Cloudflare, Inc. (2024). *Cloudflare Free Plan*. [Online]. Available at: https://www.cloudflare.com/plans/free/

**[3]** Nginx, Inc. (2024). *Module ngx\_http\_limit\_req\_module*. [Online]. Available at: http://nginx.org/en/docs/http/ngx\_http\_limit\_req\_module.html