Bot Traffic Analysis and Mitigation Strategy

Eren Cengiz

July 17, 2025

Analysis of 432,096 log entries over four days showed heavy bot traffic that overloaded the service. There were 40,887 unique IPs, averaging 10.6 requests each. However, 16 suspicious IPs made 34,500 requests, about 8% of total traffic, showing clear bot-like behaviour. Normal users make 1 to 50 requests in four days, while bots made between 1,400 and 5,400 requests. The threshold of 1,400 was chosen because the next highest request count after the bots is 47, a dramatic decrease.

The suspicious IPs mainly came from the UK (14,400 requests from 10 IPs), Russia (12,240 requests from 3 IPs), the US (3,640 requests from 2 IPs), China (2,880 requests from 2 IPs), and Iran (2,880 requests from 2 IPs). Applying the potential prevention methods, which will be introduced shortly, primarily to traffic coming from these countries would help the company focus resources effectively and keep spending accurate.

Recommended solutions include setting rate limits on requests per IP over time, blocking or throttling suspicious IPs, and using bot filtering software. These methods reduce bad traffic while allowing legitimate users access.

The costs for these protections are moderate but manageable. Implementing rate limiting and IP blocking can be done with existing server tools at no extra cost. Bot filtering services like Cloudflare or Akamai cost between $20 and $500 per month depending on the traffic. Monitoring and alerting tools might add $50 to $150 monthly. Overall, investing about $70 to $650 monthly would improve performance, reduce server load, and protect against attacks, making it a cost-effective solution for the startup.