Dealing with API Behind Cloudflare CDN

If your API is behind Cloudflare and you're experiencing issues like rate-limiting, CAPTCHA, or other blocks,

there are several strategies you can try to resolve or work around these problems:

1. Check Cloudflare's Security Settings:

Cloudflare may block requests based on:

- Request Methods: Cloudflare may block or challenge certain HTTP methods, like POST.
- Firewall Rules: Specific firewall rules might be configured to block unauthorized traffic.
- Bot Fight Mode: If enabled, this feature can block automated requests, even if they are legitimate.

Solution:

- Log into your Cloudflare dashboard.
- Navigate to the Firewall section.
- Check Firewall Rules and Security Levels to see if any rules are configured to block or challenge POST requests

or requests from your origin.

2. Add Headers to Mimic a Browser:

Cloudflare often treats non-browser traffic as suspicious, so try adding headers that mimic browser behavior.

Along with the Authorization header for Basic Authentication, you can add:

Example Headers:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124

Safari/537.36

Authorization: Basic <your_base64_encoded_credentials>

3. Whitelist Your API Client:

If you control the Cloudflare settings for your API, you can whitelist the IP or user agent of your API client.

Solution:

- Go to Firewall > Tools in the Cloudflare dashboard.
- Add your server's IP address to the whitelist.

4. Adjust Cloudflare's WAF Rules:

Cloudflare's Web Application Firewall (WAF) might be blocking POST requests with Basic Auth due to its default

security settings.

Solution:

- Go to Firewall > WAF in Cloudflare.
- Check if any specific rules are being triggered.

5. Use Cloudflare Page Rules:

If your API is being blocked by Cloudflare, you can set up Page Rules to bypass certain checks for your API.

Solution:

- Go to Page Rules in your Cloudflare dashboard.
- Create a new rule for your API path.

6. Verify SSL/TLS Settings:

Cloudflare enforces strict SSL/TLS policies. Make sure the TLS version is compatible with your server settings.

7. Use Cloudflare Bypass Services (Optional):

If none of the above works and you're still blocked by Cloudflare, look into using libraries like cloudscraper

or Cloudflare Scrape.

Python Example:

```
import requests
import base64

# API URL
url = "https://your-api-domain.com/endpoint"

# Basic Authentication
username = "your_username"
password = "your_password"
credentials = f"{username}:{password}"
encoded_credentials = base64.b64encode(credentials.encode()).decode()
```

```
# Headers
headers = {
    "Authorization": f"Basic {encoded_credentials}",
      "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36",
    "Accept": "application/json",
}

# Data for POST request
data = {
    "key1": "value1",
    "key2": "value2"
}

# Send POST request
response = requests.post(url, headers=headers, json=data)
```