## Analysis of Proxy Server Ban

I run a simple server on my Shadowsocks instance with the following code:

```
from flask import Flask, jsonify
from flask_cors import CORS
import subprocess

app = Flask(__name__)
CORS(app)  # Enable CORS for all routes

@app.route('/bandwidth', methods=['GET'])
def get_bandwidth():
    # Run the vnstat command to get the 5-minute interval traffic statistics for eth0
    result = subprocess.run(['vnstat', '-i', 'eth0', '-5', '--json'], capture_output=True, text=True)
    data = result.stdout

    # Return the captured data as a JSON response
    return jsonify(data)

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)
```

And I use nginx to serve port 443 as shown below:

```
server {
    listen 443 ssl;
    server_name www.some-domain.xyz;

    ssl_certificate /etc/letsencrypt/live/www.some-domain.xyz/fullchain.pem; # managed by
    # ...
    location / {

        proxy_pass http://127.0.0.1:5000/;
        # ...
    }
}
```

This server program provides network data, and I use the server as my proxy server, allowing me to display

my online status on my blog using the network data.

What ' s interesting is that the server hasn ' t been banned by the Great Firewall (GFW) or any other network control systems for several days now. Normally, the proxy server I set up would be banned within one or two days. The server runs a Shadowsocks program on a port like 51939, so it operates with Shadowsocks traffic mixed with regular API traffic. This mix seems to lead the GFW to believe the server is not a dedicated proxy, but rather a normal server, preventing it from banning the IP.

This observation is intriguing. It seems that the GFW uses specific logic to differentiate proxy traffic from regular traffic. While many websites like Twitter and YouTube are blocked in China, numerous foreign websites—such as those of international universities and companies—remain accessible.

This suggests that the GFW likely operates based on rules that distinguish between normal HTTP/HTTPS traffic and proxy-related traffic. Servers that handle both types of traffic seem to avoid bans, whereas servers handling only proxy traffic are more likely to be blocked.