

## الوكيل خادم حذر تحليل

الاناري الجدار حذر تجنّب الوكيل خوادم في `iptables` التطبيقات برمجة لواجهات يمكن هل `iptables` العظمى؟

التالي: الكود باستخدام بي الخاص `iptables` مثيل على بسيط خادم بتشغيل أقوم

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

app = Flask(__name__)
CORS(app) # CORS

@app.route('/bandwidth', methods=['GET'])
def get_bandwidth():
    # vnstat 5 eth0
    result = subprocess.run(['vnstat', '-i', 'eth0', '-5', '--json'], capture_output=True, text=True)
    data = result.stdout

    # JSON
    return jsonify(data)

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

أدناه: موضح هو كذا 443 المنفذ لتقديم `iptables` وأستخدم

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

    ssl_certificate /etc/letsencrypt/live/www.some-domain.xyz/fullchain.pem; #
    # ...

    location / {

        proxy_pass http://127.0.0.1:5000/;
```

```

    # ...
}
}

```

الاتصال حالة بعرض لي يسمح مما ولكيل، كخادم الخادم وأستخدم الشبكة، بيانات الخادم البرنامج هذا يوفر الشبكة. بيانات باسخدام مدونتي على بالإنترنت

في أخرى تحكّم أنظمة أي أو `os` العنظم الناري الجدار قبل من حظره يتم لم الخادم أن هو للاهتمام المثير يعمل يومين. أو يوم غضون في بإعداده أقوم الذي ولكيل خادم حظر يتم عادةً، الآن. حتى أيام لعدة الشبكة `os` مرور حركة مع يعمل فهو لذا، 51939 مثل من فذ على `os` برنامج تشغيل على الخادم ولكيل خادم ليس الخادم بأن الاعتقاد إلى الناري الجداري قود المزيج هذا أن يبدو العادية. `os` مرور حركة مع مختلطة `os`. عنوان حظر من يمنعه مما عادي، خادم بل مخصص،

الوكيل مرور حركة بين للتمييز محدّدًا من طقًا يستخدم الناري الجدار أن يبدو للاهتمام. مثيرة الملاحظة هذه العديد تظل الصين، في `os` `os` مثل المواقع من العديد حظر يتم بينما العادية. المرور وحركة للوصول. قابلية `os` الدولية والشركات الجاعمات مواقع مثل `os` الأجانبية المواقع من

العادية `os` مرور حركة بين تميز قواعد على بناء الأرحح على يعمل الناري الجدار أن إلى هذا يشير يتم بينما الحظر، تتجنب المرور حركة من النوعين لكلا مع تتعامل التي الخوادم أن يبدو ولكيل. مرور وحركة ولكيل. مرور حركة مع فقط تتعامل التي الخوادم حظر

ساعة. أو يومًا كان سواء `os` للحظر البيانات لتجميع الناري الجداري استخدمه الذي الزمني النطاق هو ما هو واحد سؤال عنوان حظر يتم لذلك، كانت إذا ولكيل. من حصريًا تأتي المرور حركة كانت إذا ما يكتشف الزمني، النطاق هذا خلل `os` بالخدام. الخاص `os`

من بدلًا أخرى مهام إلى تركيزي سينتقل القادمة، الأسابيع في ولكن كتبت، ما لمراجعة مدونتي أזור ما غالبًا إذا. 443 المنفذ عبر bandwidth التطبيقات برمجة واجهة إلى وصولي من هذا سيقول المدونة. منشورات كتابة الناري. الجدار لخداع بانظام الواجهة هذه إلى للوصول برنامجًا أكتب أن يجب أخرى، مرة للحظر أتعرض أنني وجدت

## `os`. العنظم الناري الجدار عمل كفي

### الطلبات تسجيل: 1 الخطوة

```

import time

#
request_log = []

#
def log_request(source_ip, target_ip, target_port, body):

```

```

request_log.append({
    'source_ip': source_ip,
    'target_ip': target_ip,
    'target_port': target_port,
    'body': body,
    'timestamp': time.time()
})

```

منفذ الهدف، عنوان المصدر، عنوان مثل أساسية معملومات مع الواردة الطلبات log\_request دالة تسجل الزمن. والطابع الطلب، نص الهدف،

عناوين وحظر التحقق: 2 الخطوة

```

# IP
def check_and_ban_ips():
    banned_ips = set()

    #
    for request in request_log:
        if is_illegal(request):
            banned_ips.add(request['target_ip'])
        else:
            banned_ips.discard(request['target_ip'])

    # IP
    ban_ips(banned_ips)

```

بأنشطة المرتبطة عناوين وتحظر وتحدد المسجلة، الطلبات جميع عبر check\_and\_ban\_ips دالة تكرر قانونية. غير

قانوني غير الطلب يجعل ما تحدي: 3 الخطوة

```

#
def is_illegal(request):
    #
    #
    return "illegal" in request['body']

```

ليشمل هذا توسيع يمكن. كلاً على يحتوي الـ IP. إذا ما is\_illegal دالة تتحقق من،  
قانوني. غير نشأ يـ عتبر ما على اعتماً إذا تطوراً أكثر من طبقاً

المدد عن اوين حظر: 4 الخطوة

```
# IP
def ban_ips(ip_set):
    for ip in ip_set:
        print(f"IP: {ip}")
```

أو به الاضافة عن اوين طباعة طريق عن حظره ban\_ips دالة تقوم القانوني، غير عن اوين تحديد بمجرد  
بحظره. تقوم أن يمكن حقيقي، نظام في

القانوني غير الـ IP 80 على بناء عن اوين وحظر للتحقق بدلة طريق: 5 الخطوة

```
# IP 80%
def check_and_ban_ips():
    banned_ips = set()
    illegal_count = 0
    total_requests = 0

    #
    for request in request_log:
        total_requests += 1
        if is_illegal(request):
            illegal_count += 1

    # 80%
    if total_requests > 0 and (illegal_count / total_requests) >= 0.8:
        for request in request_log:
            if is_illegal(request):
                banned_ips.add(request['target_ip'])

    # IP
    ban_ips(banned_ips)
```

والمجلس التنفيذي للمؤسسات الخيرية غير الربحية من التحقق تحسني :6 الخطوة  
المجلس

```
# Shadowsocks )
if request['target_port'] == 443:
    if is_trojan(request):
        return True
    elif is_shadowsocks(request):
        return True
return False
```

### القانونية الطلبات على مثال: 7 الخطوة

الوكيل خادم مرور حركة خصائص: 8 الخطوة

الذكي للكشف الاصطناعي والذكاء الآلي التعلّم نماذج: 9 الخطوة

5

## تحديث

باعتخدام بديل حل بتن في ذمت هذا، من لتخفيف بي. الخاص الوليل خاد حطري ست م ر ج هودي، من الرغم على حطر. حدث لكل ما بسرعة جدي د عن وان بت عي ين لي تس م ح وال تي، ، من الم عكوس مي زة