عبور از CGNAT با Cloudflare Tunnel: داستانی واقعی از یک ماجراجویی فنی

🧭 مقدمه: آغاز یک سفر نه چندان ساده

ماجرا از جایی شروع شد که تصمیم گرفتیم به سیستم Fedora خونه مون از اینترنت دسترسی پیدا کنیم؛ هدف‌های زیادی داشتیم:

- بالا آوردن وب‌سایت تستی با Django یاFlask
- مدیریت سرور از راه دور باSSH
- حتی استفاده از سیستم به‌عنوان گیت‌وی برای عبور ترافیک اینترنت با ابزارهایی مثل WireGuard یا Xray

اما خیلی زود فهمیدیم که قرار نیست همه‌چیز طبق برنامه پیش بره...

🎯 هدف اولیه ما

داشتن یه سیستم لینوکسی همیشه روشن که از بیرون بشه بهش دسترسی داشت. این سیستم باید:

- بتونه یه وب‌سایت رو ارائه بده
- از SSH پشتیبانی کنه برای دسترسی امن
- در حالت ایده‌آل، ترافیک اینترنتی بقیه دستگاه‌ها رو هم عبور بده (VPN خانگی)

خلاصه می‌خواستیم یه سرور کوچیک خفن داشته باشیم.

⛔ مرحله اول: برخورد با CGNAT و سقوط ایده‌آل‌گرایی

تنظیم اولیه با:No-IP

- ساخت ساب‌دامنه در No-IP مثل thegoat.zapto.org
- اتصال دامنه به آی‌پی مودم با Dynamic DNS
- باز کردن پورت‌ها روی مودم :80 برایHTTP ، 22 برای SSH

🚨 **اولین مشکل: پورت‌ها باز نمی‌شن!**

- پورت 80 اصلاً رزرو مودم بود (صفحه ورود مدیریت مودم)
- پورت 22 ظاهراً باز شده بود، اما از بیرون هیچ جوابی نمی‌اومد
- تست با nmap, curl, telnet و ping نشون می‌داد هیچ پکتی به سیستم نمی‌رسه

🤔 **مشکوک شدیم: چرا هیچ پکتی نمی‌رسه؟**

رفتیم IP رو با whatismyip.com چک کردیم. آی‌پی مودم مثلاً 100.96.231.45بود. عجیب بود...

🔍 **کشف:CGNAT**

متوجه شدیم آی‌پی‌مون از رنج 100.64.0.0/10هست؛ یعنی نه Public IP واقعی، بلکه یه آی‌پی داخلی بزرگ ISP یعنی پشت Carrier-Grade NAT گیر افتادیم!

مفهوم:CGNAT

- NATچندلایه‌ای که ISP برای صرفه‌جویی در IPv4 استفاده می‌کنه
- شما پشت یه لایه NAT هستید و آی‌پی‌تون به‌طور مستقیم از اینترنت در دسترس نیست

🎯 **نتیجه :**حتی اگه مودم شما پورت رو فوروارد کنه، بسته هیچ‌وقت به سیستم نمی‌رسه!

🧠 **مرحله دوم: فکر کردن خارج از چارچوب — تونل از داخل به بیرون**

ورود Cloudflare به داستان

Cloudflare یه ابزار خیلی کاربردی به اسم cloudflared داره که می‌تونه از داخل شبکه شما یه تونل امن به بیرون بزنه.

مزایای Cloudflare Tunnel

- نیاز به Public IP نداره!
- حتی اگه پشت CGNAT باشید، چون ارتباط از داخل به بیرونه، تونل برقرار می‌شه
- ترافیک HTTPS رمزنگاری شده و از طریق زیرساخت Cloudflare می‌گذره

نصب cloudflared روی Fedora

```
curl -L https://github.com/cloudflare/cloudflared/releases/latest/download/cloudflared-linux-amd64 -o cloudflared

chmod +x cloudflared

sudo mv cloudflared /usr/local/bin/
```

راه‌اندازی اولیه:

```
cloudflared tunnel login
```

بعد از لاگین، یه پنجره مرورگر باز می‌شه، وارد حساب Cloudflare می‌شیم و دسترسی می‌دیم.

ساخت تونل:

```
cloudflared tunnel create mytunnel
```

فایل config.yml

```
url: http://localhost:8000

tunnel: mytunnel

credentials-file: /home/user/.cloudflared/xxxxxxxx.json
```

اجرای نهایی:

```
cloudflared tunnel run mytunnel
```

✅ حالا سایت لوکال ما با دامنه روی اینترنت باز می‌شه، حتی بدون باز کردن پورت!

🚧 چالش‌های مسیر: چیزهایی که درست پیش نرفت

⚠️ چالش ۱ : دامنه Cloudflare باید DNS خودش رو مدیریت کنه

اگر دامنه‌تون روی Cloudflare نباشه، نمی‌تونید از Tunnel استفاده کنید. باید:

- دامنه‌تون رو روی Cloudflare اضافه کنید
- NameServer ها رو از سمت ثبت‌کننده دامنه مثلاً Namecheap تغییر بدید

⚠️ چالش ۲: با هر بار ری‌استارت باید تونل رو اجرا کنیم

مگر اینکه از systemd استفاده کنیم یا cloudflared رو به‌صورت سرویس راه بندازیم:

```
sudo cloudflared service install
```

⚠️ چالش ۳: عدم پشتیبانی از TCP/UDP خام

Cloudflareفقط برای ترافیک HTTP/HTTPS کار می‌کنه. یعنی:

- VLESS و Xray کار نمی‌کنن
- WireGuard قابل اجرا نیست
- SSH به‌صورت عادی جواب نمی‌ده

🔐 راه‌حل‌های هوشمندانه برای SSH وVPN

Cloudflare Acces ابزاری برای اتصال امن به SSH از طریق مرورگر یا کلاینت خاص:

- تونل رو به پورت 22 می‌زنید
- از دامنه‌ای مثل ssh.mydomain.comاستفاده می‌کنید
- روی کلاینت ابزار cloudflaredنصب می‌کنید و با MFA Uگین می‌کنید

راه‌حلی حرفه‌ای، امن و بدون پورت فورواردینگ!!

✅ **داشبوردهای مدیریتی:**

برای مدیریت WireGuard یا Xray ، می‌تونید داشبوردهایی مثل:

- wg-easy برای WireGuard
- x-ui یا soga برای Xray رو نصب کنید،

روی پورت لوکال اجراشون کنید و از طریق Cloudflare Tunnel بهشون دسترسی بدید.

این روش فقط برای کنترل پنل مناسبه، نه برای اتصال واقعی VPN

📈 **جدول قابلیت‌ها:**

موارد پشتیبانی‌شده:

سرویس	وضعیت	توضیح
وب‌سایت لوکال	✅ عالی	پورت 8000 یا 3000 یا هرچی
داشبورد مدیریتی	✅ کامل	Portainer، Adminer، phpMyAdmin
API REST	✅	Flask, FastAPI, NodeJS

موارد پشتیبانی‌نشده:

سرویس	چرا پشتیبانی نمی‌شه؟
Xray / VLESS	TCPخام لازم داره، Cloudflare فقط HTTP می‌فهمه
WireGuard	پروتکل UDP استفاده می‌کنه
SSH مستقیم	فقط با Access کار می‌کنه نه به‌صورت پیش‌فرض
RDP	پرتکل خاص ویندوز هست، نهHTTP

🏁 **نتیجه‌گیری نهایی: درس‌هایی از یک ماجراجویی واقعی**

اگر پشت CGNAT هستید:

- ❌ فراموش کنید که بخواید پورت باز کنید؛ فایده‌ای نداره
- ✅ از ابزارهایی مثل cloudflared برای وب‌سایت و پنل استفاده کنید
- ✅ برای SSH امن از Cloudflare Access بهره بگیرید
- ❌ برای VPN واقعی، VPS تنها راه چاره است

ما توی این سفر یاد گرفتیم که:

- فهمیدن ساختار شبکه اولین قدم موفقیته
- همیشه راهی هست، حتی اگر مسیر غیرعادی باشه
- Cloudflare یه نعمت برای توسعه‌دهنده‌هاییه که پشت NAT موندن

🧩 راه‌حل ترکیبی Cloudflare Tunnel + VPS + DDNS :

گاهی بهترین جواب، ترکیبی از چند ابزار مختلف است. اگر بخواهیم هم به داشبورد لوکال دسترسی داشته باشیم، هم از SSH و VPN واقعی استفاده کنیم، باید کمی خلاق‌تر عمل کنیم.

سناریوی پیشنهادی:

- از Cloudflare Tunnel برای دسترسی به وب‌سایت و داشبوردهای لوکال استفاده می‌کنیم
- از یک VPS با آی‌پی ثابت به‌عنوان پل بین دنیای بیرون و شبکه داخلی خودمون استفاده می‌کنیم
- از ابزارهایی مثل WireGuard ، VLESS یا حتی SSH Reverse Tunnel برای انتقال ترافیک به سیستم خونه بهره می‌گیریم

🔧 پیاده‌سازی ساده: SSH Reverse Tunnel

روی سیستم Fedora خونه:

```
ssh -R 2222:localhost:22 user@vps-ip
```

حالا روی VPS می‌تونید:

```
ssh -p 2222 user@localhost
```

با این روش، حتی پشت CGNAT هم از طریق VPS به SSH سیستم خانگی وصل می‌شید!

چرا از DDNS هم استفاده کنیم؟

اگر بخوایم از تونل‌های غیر Cloudflare مثل WireGuard یا Xrayاستفاده کنیم و VPS نداریم، می‌تونیم:

- از سرویس DDNS مثل No-IPاستفاده کنیم
- کلاینت DDNS رو روی سیستم اجرا کنیم تا آی‌پی جدید مودم رو آپدیت کنه
- فقط در صورتی مفیده که ISP به شما Public IP داده باشه) نه(!CGNAT

✅ جمع‌بندی ترکیبی:

ابزار پیشنهادی	نیاز
Cloudflare Tunnel	وب‌سایت و پنل مدیریت
Cloudflare Accessیا SSH Reverse Tunnel بهVPS	SSHامن و ساده
VPS + VLESSیاWireGuard	VPNواقعی
DDNSفقط وقتی Public IP دارید	تشخیص IP متغیر

این ترکیب به شما اجازه می‌ده:

- از قدرت Cloudflare برای امنیت و راحتی استفاده کنید
- با تونل SSH یا VPN به دنیای TCP/UDP هم دسترسی داشته باشید
- بدون خرید آی‌پی ثابت، شبکه‌ی خودتون رو مدیریت کنید