راهنمای کامل SlipNet (فارسی)

> کانال رسمی: @SlipNet_app سورس‌کد: SlipNet https://github.com/anonvector/SlipNet در گوگل‌پلی، اپ‌استور یا هیچ مارکت دیگری نیست. فقط از کانال رسمی یا گیت‌هاب دانلود کنید.

فهرست

---

۱. SlipNet چیست و چرا ساخته شده

SlipNet یک ابزار رایگان و **source-available** (سورس‌کدش قابل مطالعه است، اما اجازه‌ی توزیع مجدد ندارد) برای دور زدن سانسور و بازرسی شبکه است. نسخه‌ی اصلی برای اندروید است و یک کلاینت CLI هم برای مک، لینوکس و ویندوز ارائه می‌شود. SlipNet ترافیک اینترنت شما را از داخل پروتکل‌های متفاوتی مثل VLESS، HTTPS، SSH، QUIC، DNS یا Tor عبور می‌دهد تا حتی در شبکه‌هایی که اینترنت در آن‌ها فیلتر، محدود یا با DPI بازرسی می‌شود، بتوانید آزادانه به وب دسترسی پیدا کنید.

برخلاف یک VPN معمولی که تنها یک پروتکل دارد، SlipNet چند **حامل (transport)** مختلف ارائه می‌کند تا متناسب با شرایط شبکه‌ای که در آن گیر افتاده‌اید بتوانید بهترین مسیر را انتخاب کنید:

- اگر ISP فقط ترافیک DNS را عبور می‌دهد، از تونل‌های DNS مثل NoizDNS، DNSTT یا VayDNS استفاده کنید.
- اگر فقط HTTPS کار می‌کند، می‌توانید به سراغ NaiveProxy یا VLESS از پشت CDN (مثل Cloudflare) بروید.
- اگر شبکه به‌شدت بازرسی می‌شود و الگوی ترافیک شما را تشخیص می‌دهد، می‌توانید روی هر کدام از این تونل‌ها یک لایه‌ی SSH هم اضافه کنید تا نشت DNS صفر شود و ترافیک رمزنگاری بیشتری داشته باشد.
- در سخت‌ترین شرایط، می‌توانید از Tor همراه با Snowflake، obfs4 یا Meek استفاده کنید (فقط در نسخه‌ی Full).

از نظر فلسفه، SlipNet در همان خانواده‌ی پروژه‌های ضد سانسور قرار می‌گیرد که Psiphon، Tor و Outline VPN متعلق به آن هستند؛ با این تفاوت مهم که SlipNet **فقط کلاینت** است: شبکه یا سرور مرکزی متعلق به یک سازمان خاص وجود ندارد و سرور را یا خودتان راه‌اندازی می‌کنید (با SlipGate فقط چند دقیقه طول می‌کشد) یا از طریق فردی مورد اعتماد دریافت می‌کنید. این مدل سه مزیت اصلی دارد:

- **حریم خصوصی**: ترافیک شما از سروری عبور می‌کند که خودتان یا کسی که می‌شناسید کنترل می‌کند، نه یک شرکت ناشناس.
- **مقیاس‌پذیری و دوام**: چون هیچ زیرساخت متمرکزی برای فیلتر کردن وجود ندارد، حتی اگر یک سرور بلاک شود، یک IP جدید و تغییر یک رکورد DNS کافی است.
- **انعطاف**: می‌توانید پروتکل، CDN، دامنه و حتی کشور سرور را خودتان انتخاب کنید — چیزی که هیچ VPN تجاری به شما نمی‌دهد.

سورس‌کد SlipNet به‌صورت کامل روی گیت‌هاب در دسترس است (تحت لایسنس source-available — قابل مطالعه و مشارکت، اما بدون اجازه‌ی توزیع مجدد یا انتشار در استورها) و در هیچ مارکت اپ (گوگل‌پلی، اپ‌استور و...) منتشر نمی‌شود؛ تنها منبع رسمی، کانال @SlipNet_app و مخزن گیت‌هاب پروژه است.

---

۲. تونل‌های پشتیبانی‌شده

تونل	پروتکل	کارش	برای چه شبکه‌ای
DNSTT	DNS (KCP + Noise)	ترافیک را در کوئری DNS می‌فرستد	شبکه‌هایی که فقط DNS باز است
NoizDNS	DNS (KCP + Noise)	DNSTT با مقاومت در برابر DPI (انکودینگ base36/hex، حذف پیشوند CDN)	شبکه‌های تحت بازرسی شدید
VayDNS	DNS (KCP + Curve25519)	تونل DNS بهینه و قابل تنظیم	کاربران حرفه‌ای
Slipstream	QUIC	تونل پرسرعت QUIC	شبکه‌های سالم
SSH	SSH	تونل SSH ساده و رمزنگاری‌شده	امنیت ساده، بدون نشت
NaiveProxy	HTTPS (Caddy + اثرانگشت TLS کروم)	HTTPS با اثرانگشت اصیل کروم	عبور از DPI روی HTTPS
VLESS	WebSocket (روی TLS یا plain)	VLESS روی WebSocket پشت CDN (مثل Cloudflare)	فرانتینگ CDN، بسیار رایج در ایران
DOH	DNS over HTTPS	فقط DNS را رمزنگاری می‌کند	عبور از فیلترینگ DNS
Tor	Tor + Snowflake/obfs4/Meek	شبکه‌ی ناشناس	ناشناسی بالا
+ نسخه‌های SSH	SSH + (DNSTT/NoizDNS/VayDNS/Slipstream/NaiveProxy/VLESS)	یک لایه‌ی SSH اضافه — نشت	حداکثر امنیت

تونل	پروتکل	کارش	برای چه شبکه‌ای
		DNS صفر	

کدام را انتخاب کنم؟

- تازه‌کار و گیج؟ → **DNSTT** (پیش‌فرض).
- DPI سخت؟ → **NoizDNS** یا **NoizDNS + SSH**.
- می‌خوای پشت CloudFlare قایم شی؟ → **VLESS** یا **NaiveProxy**.
- سرعت خام روی شبکه‌ی تمیز؟ → **Slipstream**.
- ناشناسی؟ → **Tor** (فقط نسخه Full).

---

۳. نسخه‌ها: Full و Lite

SlipNet در دو نسخه عرضه می‌شود — تفاوت در حجم APK و پروتکل‌های موجود است.

ویژگی	Full	Lite
DNSTT، NoizDNS، VayDNS	✓	✓
Slipstream (QUIC)	✓	✓
SSH	✓	✓
DoH	✓	✓
VLESS	✓	✓
NaiveProxy	✓	—
Tor (Snowflake / obfs4 / Meek)	✓	—
حجم تقریبی APK	حدود ۵۰ MB	حدود ۲۰ MB

پیشنهاد پیش‌فرض **Full** است. **Lite** برای اینترنت کند، گوشی با حافظه‌ی کم، یا وقتی Tor و NaiveProxy لازم نیست.

---

۴. نصب APK

۱. کانال رسمی @SlipNet_app یا صفحه‌ی Releases در گیت‌هاب را باز کنید. ۲. APK مناسب CPU گوشی‌تان را دانلود کنید. اکثر گوشی‌های جدید `arm64-v8a` هستند. اگر مطمئن نیستید، APK نسخه‌ی **universal** را بگیرید. ۳. در گوشی: **تنظیمات → امنیت → نصب از منابع ناشناس** را برای مرورگر یا تلگرام فعال کنید. ۴. روی APK دانلودشده بزنید و نصب

کنید. ۵. اپ را باز کنید. در اولین اجرا، اندروید مجوز VPN می‌خواهد — **OK** را بزنید. ۶. تنظیم پیشنهادی یک‌باره: **تنظیمات** → **بهینه‌سازی باتری** → **SlipNet** → **را بهینه نکن** تا اندروید آن را در پس‌زمینه نکشد.

> ⚠️ اگر SlipNet را در گوگل‌پلی، اپ‌استور یا هر مارکت دیگری دیدید، **مال ما نیست**؛ نصب نکنید.

---

۵. سرور لازم است — از SlipGate استفاده کنید

SlipNet *کلاینت* است. برای کار به یک **سرور** نیاز دارد که تونل سازگار را اجرا کند.

روش رسمی و پشتیبانی‌شده برای راه‌اندازی سرور **SlipGate** است — یک نصاب لینوکسی تک‌دستوری که سمت سرور تمام پروتکل‌های SlipNet را راه می‌اندازد.

> https://github.com/anonvector/slipgate

راهنمای جداگانه‌ی SlipGate در کنار همین سند منتشر شده است. خلاصه: یک VPS ۵ دلاری بگیرید، دامنه‌اش را به آن وصل کنید، یک دستور نصب اجرا کنید، یک کاربر بسازید، و SlipGate یک لینک `slipnet://` می‌دهد که مستقیم در اپ پیست می‌شود.

اگر سرور خودتان را راه نمی‌اندازید، می‌توانید:

- از دوستی که SlipGate دارد لینک `slipnet://` بگیرید، یا
- از لینک تستی عمومی که گاهی در @SlipNet_app منتشر می‌شود استفاده کنید.

---

۶. اولین پروفایل

سه راه برای ساخت پروفایل وجود دارد.

الف) چسباندن لینک `slipnet://` (ساده‌ترین)

۱. SlipNet را باز کنید → دکمه‌ی **+** پایین سمت راست. ۲. **Import from URI** را انتخاب کنید. ۳. لینک `slipnet://...` را پیست کنید. ۴. تمام — پروفایل به لیست اضافه می‌شود.

ب) ایمپورت فایل JSON

اگر دوستی پروفایل‌هایش را خروجی گرفته (رمزشده یا ساده):

۱. منوی سه‌نقطه (⋮) صفحه‌ی اصلی → ۲. **Import Profiles**. فایل `.json` را انتخاب کنید. ۳. اگر رمزشده است، رمز را وارد کنید.

پ) ساخت دستی پروفایل

وقتی به‌جای URI، مقادیر خام (دامنه + کلید) داده شده.

۱. روی **+** بزنید ← ۲. **Add Profile**. یک **Name** بگذارید. ۳. **Tunnel Type** را انتخاب کنید (بسته به نوع، فیلدها فرق می‌کند — به بخش ۱۱ نگاه کنید). ۴. فیلدهای موردنیاز را پر کنید. ۵. **Save** بزنید.

---

۷. اتصال و قطع

۱. روی پروفایل دلخواه در لیست بزنید (یک تیک می‌آید). ۲. دکمه‌ی بزرگ **Connect** را بزنید. ۳. اولین بار اندروید مجوز VPN می‌خواهد ← ۴. **OK**. وقتی آیکن سبز شد و آمار آپلود/دانلود زنده دیده شد، متصل هستید. تمام ترافیک از تونل عبور می‌کند.

برای قطع، دوباره **Connect** را بزنید. برای تعویض پروفایل، اول قطع کنید، پروفایل دیگر را انتخاب و دوباره وصل کنید.

سوییچ سریع بدون باز کردن اپ:

- نوار اعلان را پایین بکشید ← **کاشی Quick Settings** SlipNet را بزنید (اولین بار باید از پنل کاشی‌ها اضافه‌اش کنید).
- یا از **ویجت صفحه‌ی اصلی** برای اتصال یک‌ضربه‌ای استفاده کنید.

تست پینگ زنده: پس از انتخاب پروفایل، روی **Real Ping** یا **Simple Ping** بزنید. **Sort by Ping** لیست را از سریع‌ترین مرتب می‌کند.

---

۸. اسکنر DNS

پروفایل‌های تونل DNS (DNSTT، NoizDNS، VayDNS) فقط از طریق ریزالورهایی کار می‌کنند که چند رفتار RFCای را رعایت کنند و در پاسخ‌ها دست‌کاری نکنند. خیلی از ریزالورهای ISPها در یک یا چند مورد از این تست‌ها مردود می‌شوند — NXDOMAIN را hijack می‌کنند، EDNS را حذف می‌کنند، نام‌های طولانی را رد می‌کنند، یا ترافیک شبیه‌تونل را در DPI می‌بندند. **اسکنر** ریزالورهایی را پیدا می‌کند که از این تست‌ها رد می‌شوند.

باز کردن: **منو** ← **DNS Resolver Scanner**.

اسکنر چهار چیز اصلی را در اختیار شما می‌گذارد:

۱. **حالت اسکن (Scan Mode)** — چه نوع تستی اجرا شود ۲. **پنل پیکربندی (Configuration)** — دامنه تست، پورت، تایم‌اوت، موازی‌سازی ۳. **منبع IP (IP source)**ـهای کاندید از کجا بیایند ۴. **نتایج و اعمال (Results & Apply)** — مرور و push کردن به پروفایل

۸.۱. حالت‌های اسکن

یک تاگل بالای صفحه یکی از چهار حالت را انتخاب می‌کند. هر کدام trade-off متفاوتی بین سرعت، عمق و قطعیت دارد.

Simple

«ریزالورهای DNS را اسکن می‌کند و خودکار هر کدام را از تونل تست می‌کند. فقط ریزالورهایی که از تست تونل رد می‌شوند نمایش داده می‌شوند.»

حالت یک‌ضربه‌ای برای همه. اسکنر هم پروب سازگاری DNS و هم تست end-to-end تونل را در یک pipeline اجرا می‌کند و فقط ریزالورهایی را نشان می‌دهد که واقعاً ترافیک را می‌رسانند. اگر نمی‌خواهید فکر کنید، این را انتخاب کنید.

نیاز به پروفایلی با کلید عمومی معتبر دارد (تا تست تونل سرور واقعی برای حرف زدن داشته باشد).

Advanced

«اول ریزالورها را اسکن کن، بعد در صورت نیاز تست تونل را جدا اجرا کن.»

جریان دو-مرحله‌ای کلاسیک. مرحله ۱ پروب DNS است و به هر ریزالور امتیاز ۰ تا ۶ می‌دهد (به ۸.۵ نگاه کنید). می‌توانید نتایج را مرور، مرتب و فیلتر کنید، و بعد در صورت نیاز یک تست تونل E2E روی ریزالورهای رد شده اجرا کنید. وقتی می‌خواهید جزئیات پروب را ببینید یا هنوز پروفایل ندارید، این مفید است.

E2E

«هر ریزالور را مستقیم از تونل تست می‌کند، بدون چک سازگاری DNS. کندتر است ولی اتصال واقعی را تست می‌کند.»

پروب DNS را کامل رد می‌کند. برای هر IP کاندید فقط یک تونل واقعی باز می‌کند و یک درخواست HTTP می‌فرستد. وقتی از قبل لیست IPهای «شناخته‌شده‌ی تونل-سازگار» دارید و فقط می‌خواهید بدانید کدام در حال حاضر سریع به سرور خاص شما می‌رسد، این را انتخاب کنید.

Prism

«اسکن سرور-تأییدشده: فقط ریزالورهایی نمایش داده می‌شوند که به‌صورت رمزنگاری‌شده اثبات کنند به سرور خاص شما می‌رسند. به نصب SlipGate روی سرور نیاز دارد.»

قوی‌ترین حالت. پروب‌های HMAC-authenticated می‌فرستد که فقط یک سرور SlipGate واقعی می‌تواند درست امضا کند، پس ریزالوری که «کار می‌کند» اما در واقع ترافیک را به یک middlebox مهاجم می‌رساند، در این چک رد می‌شود. هر ریزالور N بار پروب می‌شود؛ ریزالورهایی که ≤ *threshold* پاسخ امضاشده می‌گیرند، عبور می‌کنند. وقتی به transparent-proxy interception شک دارید یا می‌خواهید جلوی hijacking تونل را بگیرید، این را انتخاب کنید.

فقط وقتی پروفایل انتخاب‌شده‌تان کلید عمومی معتبر دارد و سرور شما SlipGate اجرا می‌کند، در دسترس است.

۸.۲. پنل پیکربندی

این فیلدها بالای دکمه‌ی اسکن می‌آیند. اکثرشان مقدار پیش‌فرض درستی دارند — فقط وقتی اسکن نتیجه نمی‌دهد دستکاری کنید.

مشترک Simple / Advanced

- **Test Domain** — اسمی که پروب می‌پرسد. *دامنه‌ی تونل خودتان* را بگذارید (مثل `t.example.com`)؛ ریزالوری که می‌تواند زیردامنه‌های تصادفی طولانی زیر آن را روت کند، همان است که می‌تواند تونل واقعی را حمل کند. در پروفایل‌های قفل‌شده به دامنه‌ی خود پروفایل برمی‌گردد.
- **Port** — معمولاً `53`. اگر سرورتان روی پورت غیراستاندارد است، عوض کنید.
- **Timeout (ms)** — تایم‌اوت پروب DNS برای هر ریزالور. پیش‌فرض ۳۰۰۰. اگر لیست کاندیدتان عظیم و پر از IP مرده است، روی ۱۵۰۰ بگذارید.

- **Workers** — تعداد پروب موازی. پیش‌فرض ۵۰. روی شبکه‌ی ناپایدار کم کنید تا drops نداشته باشید.

فقط E2E

- **Resolver Port** — پورتی که ریزالور گوش می‌دهد (۵۳ مگر تغییر داده باشید).
- **E2E Timeout** — تایم‌اوت تست تونل هر ریزالور. پیش‌فرض ۱۵۰۰۰ ms.
- **E2E Concurrency** — تعداد تست تونل موازی. ۱ تا ۱۰. **Slipstream حداکثر ۱** چون تونل‌های QUIC نمی‌توانند پورت را به اشتراک بگذارند.
- **Test URL** — چیزی که تونل برای اثبات اتصال می‌گیرد. پیش‌فرض `http://www.gstatic.com/generate_204` (پاسخ No Content 204 — کوچک، سریع، به DNS داخل تونل وابسته نیست).
- **Full Verification** — وقتی روشن است، URL تست را از تونل زنده می‌گیرد؛ وقتی خاموش، فقط تأیید می‌کند که handshake تونل کامل شد.

فقط Prism

- **Probes** — تعداد درخواست‌های HMAC-signed به هر ریزالور. پروب بیشتر = اطمینان آماری قوی‌تر، اسکن کندتر. پیش‌فرض ۵.
- **Pass threshold** — حداقل تعداد پروبی که باید درست امضاشده برگردد. پیش‌فرض ۲.
- **Timeout (per resolver)** — بودجه‌ی کلی که بین پروب‌ها تقسیم می‌شود. اپ تنظیماتی را که زمان هر پروب زیر ۲۰۰ ms می‌شود رد می‌کند.
- **Response size** — بایتی که سرور باید پاسخ‌ها را تا آن پد کند (0 = پیش‌فرض سرور). اگر سرورتان برای اندازه‌ی پاسخ خاصی پیکربندی شده، مفید است.
- **Pre-filter dead resolvers** — اول یک چک سریع DNS اجرا می‌کند تا IPهای مرده را قبل از مصرف بودجه پروب حذف کند. برای لیست‌های بزرگ پیشنهاد می‌شود.

Scan Transport (فقط Advanced و Simple) — `UDP` ، `TCP` یا `Both` . **Both** اول UDP اجرا می‌کند، بعد فقط ریزالورهایی که نگذشتند را روی TCP دوباره تست می‌کند. در شبکه‌هایی که UDP DNS rate-limit یا فیلتر می‌شود مفید است، چون بعضی ریزالورها روی TCP خوب پاسخ می‌دهند. هر نتیجه نشان `UDP` و `TCP` نشان می‌دهد که از کدام عبور کرده.

۸.۳. پنل منبع IP

تب‌های پایین تعیین می‌کنند *IPهای کاندید از کجا بیایند*. هر بار فقط یک منبع.

- **Default** — لیست ازپیش‌منتخب اپ از ریزالورهایی که در گذشته جواب می‌دادند. کوچک‌ترین و سریع‌ترین اسکن؛ شروع خوب.
- **Import** — IP از فایل بارگذاری کن (`.txt` ، یکی در خط یا با کاما). برای اسکن لیست دیگران یا نتایج خودتان مفید است.
- **Country** — IP تصادفی از تخصیص آدرس یک کشور تولید می‌کند. کشور و sample count را انتخاب کنید (پیش‌فرض ۲۰۰۰، حداکثر ۱۰۰,۰۰۰). برای کاربران ایران معمولاً معدن طلاست — ریزالورهای داخلی معمولاً برای تونل

بهتر از خارجی‌ها هستند، چون DPI داخلی به اندازه‌ی کافی روی آن‌ها حساسیت ندارد.

- **Custom** — یک CIDR (`5.144.0.0/14`)، یک رنج (`5.144.0.1–5.147.255.254`)، IPهای کاما-جداشده یا تک IP پیست کنید. پیش‌نمایش شمارش نشان می‌دهد چند IP در صف اسکن قرار می‌گیرد.
- **IR DNS Ranges** — تخصیص DNS ایرانی گروه‌بندی‌شده با `/8` اول. انتخاب کنید کدام گروه‌ها باشند (نشان شماره روی هر گروه تعداد IP کل آن را می‌گوید). سنگین‌تر از IR DNS Lite ولی جامع‌تر.
- **IR DNS Lite** — زیرمجموعه‌ی ازپیش‌منتخب از رنج‌های DNS ایرانی، کوچک‌تر و سریع‌تر از کامل. پیش‌فرض خوبی برای کاربران ایران.
- **Recent DNS** *(دکمه‌ی پایین)* — IPهای آخرین اسکن را دوباره استفاده می‌کند، برای تنظیم پارامترها بدون تولید مجدد لیست کاندید.
- **Load Last Scan IPs** — ریزالورهایی را که در اجرای قبلی قبلاً قبول شده‌اند برمی‌گرداند («Working IPs») را از «E2E Passed IPs» جدا نگه می‌دارد تا فقط لیست اثبات‌شده را دوباره تست کنید).

تاگل‌هایی که برای اکثر منابع کار می‌کنند:

- **Shuffle** — ترتیب اسکن را تصادفی کن. پیش‌فرض روشن. کمک می‌کند روی یک ISP خاص متمرکز نشوید.
- **Expand neighbours** — موقع اسکن یک رنج سفارشی، چند IP اطراف هر hit را هم پروب کن، چون ریزالورها معمولاً خوشه‌خوشه هستند.

۸.۴. نتایج و اعمال

پس از اتمام اسکن، **View Results** را بزنید. هر سطر ریزالور این‌ها را نشان می‌دهد:

- IP ریزالور و امتیاز (۰ تا ۶) از پروب DNS.
- یک نشان تفکیکی: `NS✓ TXT✓ RND✓ DPI✓ EDNS✓(1232) NXD✓` — به ۸.۵ نگاه کنید.
- در حالت Simple/E2E: زمان setup تونل، تأخیر HTTP، کل round-trip.
- در حالت Prism: `Probes 4/5` (موفق/کل) و نشان `Verified` .
- نشان transport (`UDP` ، `TCP`) که از کدام رد شده.
- وضعیت `WORKING` / `CENSORED` / `TIMEOUT` / `ERROR` .

می‌توانید:

- **مرتب** کن بر اساس امتیاز، تأخیر یا موفقیت E2E.
- **فیلتر** بر اساس تعداد پروب رد شده (Prism)، رنج امتیاز (Advanced)، یا «همه‌ی working».
- **سرچ** بر اساس بخشی از IP.
- **کپی** یا **خروجی** IPهای دیده‌شده (فقط E2E-passed / فقط Stage-1 working / انتخاب خودتان).
- **Re-test Tunnel** روی یک نتیجه — وقتی شبکه عوض شده مفید است.
- **Apply Selected** — ریزالورهای انتخاب‌شده را روی پروفایل فعال اعمال می‌کند (حداکثر ۸). دفعه‌ی بعد که وصل می‌شوید، همان ریزالورها استفاده می‌شوند.

اسکن قطع‌شده را می‌توانید resume کنید (اپ هنگام ورود مجدد می‌پرسد). تست‌های E2E را می‌توانید وسط اجرا pause/continue کنید.

۸.۵. شرح امتیاز ۰ تا ۶

امتیاز سازگاری DNS برابر است با تعداد تست‌هایی از این شش پروب که ریزالور با موفقیت پشت سر می‌گذارد. هر پروب یک امتیاز دارد (موفق یا ناموفق).

پروب	چه چیزی را می‌سنجد	چرا مهم است
NS	آیا ریزالور رکورد `NS` را دنبال می‌کند و رکورد A زون والد را برمی‌گرداند	سرور تونل معمولاً به‌صورت زیردامنه به سرور شما واگذار (delegate) می‌شود؛ ریزالوری که از این واگذاری پیروی نکند، اصلاً نمی‌تواند سرور تونل را پیدا کند
TXT	آیا ریزالور رکوردهای TXT را به‌درستی برمی‌گرداند	NoizDNS، DNSTT و VayDNS داده‌ی بازگشتی را داخل رکوردهای TXT (یا انواع دیگر در تنظیمات VayDNS) رمزگذاری می‌کنند؛ اگر TXT کار نکند، هیچ ترافیکی از سرور به کلاینت نمی‌رسد
RND	آیا ریزالور برای زیردامنه‌ای که قبلاً ندیده، واقعاً از سرور بالادست (upstream) سؤال می‌کند	برخی ریزالورها بیش از حد کش می‌کنند یا نام‌های ناشناس را بدون پرسش رد می‌کنند؛ تونل DNS برای هر درخواست یک زیردامنه‌ی جدید می‌سازد، پس این رفتار باید درست باشد
DPI	آیا یک کوئری TXT طولانی base32 به سبک `dnstt` از فیلترینگ DPI عبور می‌کند	برخی شبکه‌ها با شناسایی الگوی DNS-tunnel (طول، آنتروپی یا نوع رکورد) آن را می‌بندند؛ اگر این تست رد شود، کوئری‌ها بی‌سر و صدا حذف می‌شوند
EDNS	آیا ریزالور پاسخ‌های EDNS0 بزرگ‌تر از ۵۱۲ بایت را پشتیبانی می‌کند (و حداکثر اندازه‌ی payload — مثلاً ۵۱۲ یا ۹۰۰ یا ۱۲۳۲)	سرعت تونل مستقیماً به اندازه‌ی پاسخ بستگی دارد؛ ۱۲۳۲ مقدار توصیه‌شده‌ی dnsflagday.net است و ریزالورهایی که روی ۵۱۲ گیر کرده‌اند بسیار کند خواهند بود
NXD	آیا ریزالور برای دامنه‌ی نامعتبر، پاسخ صحیح `NXDOMAIN` می‌دهد یا آن را به یک IP جعلی هدایت می‌کند	ریزالورهایی که NXDOMAIN را hijack می‌کنند پاسخ ساختگی می‌فرستند و این کار قاب‌بندی تونل را خراب می‌کند؛ چنین ریزالوری امتیاز `NXD✗` می‌گیرد و عملاً غیرقابل‌استفاده است

امتیاز **۶** یعنی ریزالور کاملاً با تونل سازگار است. امتیاز **۵** معمولاً قابل قبول است — اغلب تنها امتیاز ازدست‌رفته مربوط به اندازه‌ی payload EDNS است که فقط روی سرعت اثر می‌گذارد. امتیاز **۳ یا کمتر** معمولاً ارزش استفاده ندارد. با فیلد Pass threshold می‌توانید حداقل امتیاز قابل قبول را تعیین کنید.

۸.۶. دستورهای کاربردی

- **کاربر ایران، پروفایل پیش‌فرض، فقط می‌خواهی وصل شی**: حالت Simple → منبع Start → IR DNS Lite.

- **کاربر ایران، جستجوی همه‌جانبه**: حالت Simple → منبع IR DNS Ranges → همه‌ی گروه‌ها را انتخاب کن → sample count را روی ۵۰۰۰ ببر.
- **تست‌کننده‌ی خارجی**: حالت Advanced → منبع Country → کشور را انتخاب کن → score threshold روی ۵.
- **شک داری ISP intercept می‌کند**: حالت ۵ probe / threshold ۸ → IR DNS Lite → Prism.
- **لیست کارا داری، فقط سرعت را تأیید کن**: حالت E2E → آن لیست را Import کن → concurrency بالا.
- **UDP DNS rate-limit شده**: هر حالتی → Scan Transport را روی `Both` بگذار.

---

۹. زنجیره‌ی پروفایل (Chains)

تب **Chains** اجازه می‌دهد چند پروفایل را پشت سر هم بگذارید. مثال‌ها:

- `NoizDNS → SSH → مقصد` — حمل‌کننده‌ی مقاوم در برابر DPI با SSH روی آن، نشت DNS صفر.
- `VLESS (Cloudflare) → SSH` — فرانتینگ CDN به‌علاوه آخرین‌گام رمزنگاری‌شده.
- `Tor → NaiveProxy` — ناشناسی + خروجی HTTPS.

ساخت زنجیره: ۱. تب **Chains** را باز کنید. ۲. **+ New Chain** را بزنید. ۳. پروفایل‌ها را به ترتیب اضافه کنید — اولین گام بالا، آخرین گام پایین. ۴. ذخیره و انتخاب مثل یک پروفایل عادی.

موقع اتصال، اپ سازگاری زنجیره را اعتبارسنجی می‌کند (transportهای سازگار، بدون حلقه) و زنجیره را به‌عنوان یک تونل اجرا می‌کند.

---

۱۰. مرجع تنظیمات

با باز کردن **Settings**:

Connection

- **Auto-connect on boot** — با روشن شدن گوشی خودکار وصل شو.
- **Auto-reconnect** — اگر VPN قطع شد دوباره وصل شو.
- **Auto-disconnect after** — بعد از مدت بی‌مصرفی قطع شو.
- **Block all if VPN drops** — کلید قطع اضطراری (بدون نشت).
- **VPN MTU** — کم کن (مثلاً 1280) اگر بعضی سایت‌ها لود نمی‌شوند.
- **DNS Workers** — کمتر = پایدارتر روی شبکه‌های محدود؛ "per-query" برای هر لوک‌آپ یک کانکشن جدید.
- **Disable QUIC** — اپ‌ها را به TCP مجبور می‌کند؛ معمولاً روی تونل سریع‌تر است.

Routing

- **Split Tunneling** — انتخاب اپ‌هایی که از VPN رد می‌شوند (allow / bypass).
- **Domain Routing** — فقط دامنه‌های خاصی از تونل عبور کنند.

- **Geo-bypass** — ترافیک مربوط به IPها/سایت‌های کشور انتخاب‌شده را *بیرون* از تونل می‌فرستد تا سایت‌های داخلی سریع و بدون اثر تونل بمانند.
- **Bypass VPN** — اپ‌هایی که VPN را دور بزنند.
- **Append HTTP Proxy to VPN** — یک پراکسی HTTP محلی هم می‌سازد.

DNS

- **Global DNS Resolvers** — جایگزینی ریزالورها برای همه‌ی پروفایل‌ها.
- **Remote DNS Server** — DNS سمت سرور تونل.
- **DNS Resolver Scanner** — به بخش ۸ نگاه کنید.

Security

- **SSH Cipher** — AES-128-GCM / ChaCha20 / AES-128-CTR (legacy).
- **Bandwidth Limit** — سقف آپلود/دانلود.
- **Hotspot mode** — تونل را با دستگاه‌های دیگر روی Wi-Fi به اشتراک بگذار.

Appearance

- **Dark mode** — Dark / AMOLED Dark / Auto.

Diagnostics

- **Debug logging** — لاگ پرجزئیات برای پشتیبانی.
- **Device ID / IP** — برای درخواست پشتیبانی کپی کنید.
- **Check for updates** — آخرین نسخه را می‌گیرد.

---

۱۱. مرجع سریع هر تونل

وقتی پروفایل را به‌صورت دستی می‌سازید، هر نوع تونل به این فیلدها نیاز دارد:

DNSTT / NoizDNS

- **Domain** — زیردامنه‌ی تونل، مثل `t.example.com`
- **Public Key** — کلید Curve25519/Noise سرور (هگز)
- **DNS Transport** — UDP / TCP / DoT / DoH
- **DNS Resolvers** — IPهای ریزالورها
- **Stealth Mode** — *NoizDNS:* کندتر اما سخت‌تر برای تشخیص

VayDNS

- Domain + Public Key (مثل بالا)
- **Record Type** — TXT / CNAME / A / AAAA / MX / NS / SRV

- **Max QNAME Length** — حجم سیمی هر کوئری
- **Rate Limit (RPS)** — تعداد کوئری در ثانیه
- **Idle Timeout / Keep-Alive / UDP Timeout**
- **ClientID Size** — باید با سرور یکی باشد (پیش‌فرض ۲؛ در حالت DNSTT-compat برابر ۸)

Slipstream

- Domain + Public Key
- **Congestion Control** — BBR / DCUBIC
- **Keep-Alive Interval**
- **Authoritative Mode**, **GSO**

SSH (مستقل یا به‌عنوان آخرین گام)

- **SSH Host / Port** (پیش‌فرض ۲۲)
- **Username + Password** *یا* **Private Key** (با passphrase)
- **Cipher** — AES-128-GCM / ChaCha20 / AES-128-CTR

گزینه‌های transport برای SSH (روی هر تونل SSH-base کار می‌کند):

- **SSH over TLS** — SSH را در TLS با SNI سفارشی بپوشاند (domain fronting).
- **HTTP CONNECT proxy** — مسیر از پراکسی HTTP CONNECT با Host سفارشی.
- **SSH over WebSocket** — `ws://` یا `wss://` با path و Host سفارشی (سازگار با Cloudflare).
- **SSH Payload** — قبل از handshake بایت خام بفرست تا کانکشن استتار شود. placeholder: `[host]` ، `[port]` ، `[crlf]` ، `[cr]` ، `[lf]` .

NaiveProxy

- **Server hostname** + **port** (معمولاً ۴۴۳)
- **Proxy username / password**

VLESS

- **UUID** — شناسه‌ی کاربر VLESS (`xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`)
- **Domain** — هاست پشت CDN؛ به‌عنوان TLS SNI و WS Host
- **Security** — `tls` (پیشنهادی) یا `none`
- **Transport** — فقط WebSocket (TCP خام در اپ پشتیبانی نمی‌شود — VLESS در SlipNet به‌عنوان تونل پشت CDN در نظر گرفته شده)
- **WS Path** — مثلاً `/` ، `/vless`
- **CDN IP / Port** — یک IP تمیز Cloudflare اگر فرانتینگ CF می‌کنید (وگرنه IP مستقیم سرور، پورت ۴۴۳)
- **TLS SNI** — چیزی که در ClientHello می‌رود (موقع روتینگ روی CDN باید با گواهی CDN بخواند)

- DPI-evasion — **SNI Fragmentation** سمت TLS: split / pad کردن ClientHello (اگر ISP شما VLESS را تشخیص می‌دهد، روشنش کنید)
- **Header obfuscation** *(فقط WS)* — هدرهای تصادفی مرورگری

SOCKS5 (زنجیر کردن به یک پراکسی SOCKS5 ریموت)

- **Host / Port** پراکسی SOCKS5 ریموت
- **Username / Password** (اختیاری، RFC 1929)
- **DNS Server** برای DNS-over-TCP داخل تونل (پیش‌فرض `8.8.8.8`)

⚠️ چرا SOCKS5 ممکن است «Connected» نشان دهد ولی واقعاً کار نکند

حالت SOCKS5 در SlipNet یک **passthrough** ساده است — فقط یک listener محلی روی گوشی باز می‌کند و هر درخواست را به پراکسی SOCKS5 ریموت زنجیر می‌کند. **هیچ تست end-to-end اولیه‌ای انجام نمی‌شود.** وضعیت «Connected» فقط دو چیز را تأیید می‌کند:

1. listener محلی SOCKS5 روی گوشی شما با موفقیت bind شده، و
2. یک کانکشن downstream توانسته handshake (CONNECT + auth) را با پراکسی ریموت کامل کند.

این **تأیید نمی‌کند** که پراکسی ریموت واقعاً به اینترنت آزاد دسترسی دارد. پراکسی می‌تواند بی‌سروصدا ترافیک خروجی را drop کند، پاسخ CONNECT جعلی برگرداند، پشت یک فایروال ابری باشد که فقط CIDR داخلی را اجازه می‌دهد، یا خودش پشت uplink سانسورشده گیر کرده باشد — و SlipNet هیچ راهی برای تشخیص این‌ها از روی پروتکل SOCKS5 ندارد، چون SOCKS5 **نه هویت سرور را تأیید می‌کند، نه key exchange سرتاسری دارد، نه سیگنال liveness**.

مقایسه‌ی SSH و SOCKS5

برقراری تونل SSH شامل این مراحل است که همه باید موفق شوند تا instance خودش را connected اعلام کند:

- TCP connect به endpoint سرور SSH
- تبادل بنر نسخه‌ی SSH
- Key Exchange (ECDH/DH) و تولید کلید نشست مشترک
- احراز هویت کاربر (password یا public-key) — توسط سرور اعتبارسنجی می‌شود
- باز شدن یک channel واقعی روی نشست رمزنگاری‌شده

اگر هر کدام از این مراحل fail شود، SSH هرگز به وضعیت سبز نمی‌رسد. بنابراین وقتی SSH می‌گوید «connected»، یعنی واقعاً یک کانال رمزنگاری‌شده و احراز هویت‌شده وجود دارد و در حال انتقال بایت است. به همین خاطر **تونل‌های مبتنی بر SSH وقتی چیزی خراب باشد صدای بلندی در می‌آورند**، در حالی که SOCKS5 ساده می‌تواند یک وضعیت سبزِ دروغی نشان دهد.

	SOCKS5	SSH
تأیید هویت سرور	ندارد	ضمنی از طریق احراز هویت (و host-key اگر pin شده باشد)
Key exchange سرتاسری	ندارد	بله (ECDH/DH)
«Connected» یعنی ترافیک رد می‌شود	خیر	بله
رمزنگاری تا سرور	خیر (متن ساده تا پراکسی)	بله
تشخیص MITM / drop خاموش	ندارد	دارد

همین مشکل روی تونل‌های DNS هم می‌تواند رخ دهد. NoizDNS، DNSTT و VayDNS در حالت **مستقل** (یعنی بدون wrapper `SSH +`) از یک listener محلی SOCKS5 به‌عنوان رابط downstream استفاده می‌کنند. خودِ تونل DNS سرتاسری احراز هویت می‌شود (handshake مبتنی بر Noise / Curve25519 — پس لینک تونل واقعاً برقرار است)، اما آنچه **بعد از** ترمیناتور سمت سرور اتفاق می‌افتد — یعنی forwardکردن واقعی به اینترنت آزاد — یک SOCKS5 / فورواردِ ساده‌ی بدون تست end-to-end است. بنابراین یک پروفایل DNSTT/NoizDNS/VayDNS هم می‌تواند **«Connected» نشان دهد در حالی که ترافیک واقعی بی‌سروصدا fail می‌شود** اگر forwardکننده‌ی سمت سرور خراب یا جغرافیا-محدود باشد. حالت‌های **`SSH +`** (یعنی DNSTT+SSH، NoizDNS+SSH، VayDNS+SSH) این موضوع را حل می‌کنند: یک نشست واقعی SSH از *داخل* تونل DNS رد می‌کنند و handshake SSH فقط زمانی کامل می‌شود که سرور واقعاً بتواند ترافیک را به مقصد برساند — به این ترتیب گارانتی liveness بازمی‌گردد.

نتیجه‌ی عملی:

- حالت SOCKS5 را یک **آداپتور انتقال** برای پراکسی‌ای که از قبل به آن اعتماد دارید بدانید، نه یک تست تونل. اگر پراکسی خراب یا جغرافیا-محدود باشد، «Connected» سبز می‌بینید بدون اینکه یک بایت رد و بدل شود.
- برای یک تونل واقعیِ ضد سانسور، **SSH** یا یکی از حالت‌های SSH-wrapped (NoizDNS+SSH، Slipstream+SSH، NaiveProxy+SSH، VLESS+SSH و …) را ترجیح دهید — این‌ها وقتی چیزی خراب است شکست را آشکار اعلام می‌کنند.
- اگر مجبورید SOCKS5 ساده استفاده کنید، تا حد ممکن **SSH را روی آن سوار کنید** — خانواده‌ی `SSH +` از پراکسی SOCKS5 به‌عنوان transport استفاده می‌کند و یک نشست واقعی SSH از داخلش رد می‌کند. به این ترتیب گارانتی‌های احراز هویت و liveness بازمی‌گردند.

DOH

- **DoH Server URL** — مثل `https://cloudflare-dns.com/dns-query`
- *(DOH فقط DNS را رمزنگاری می‌کند — ترافیک معمولی شما عوض نمی‌شود.)*

Tor (نسخه Full)

- **Bridge type** — Snowflake / obfs4 / Meek / Direct / لاین‌های bridge سفارشی
- **Auto-detect Best Bridge** — اپ بهترین را خودش انتخاب می‌کند

---

۱۲. عیب‌یابی

نشانه	راه‌حل
اصلاً وصل نمی‌شود	**اسکنر** را اجرا کن، ریزالورها را عوض کن؛ DNS Transport را عوض کن (UDP → DoT → DoH)؛ به‌جای DNSTT از **NoizDNS** استفاده کن
وصل می‌شود ولی چند ثانیه بعد قطع می‌شود	**VPN MTU** را پایین بیار (1280)، **DNS Workers = 1** یا حالت *per-query*
وصل است ولی اینترنت نیست	**Disable QUIC** را روشن کن؛ **Auto-reconnect** را تست کن
اندروید SlipNet را در پس‌زمینه می‌کشد	تنظیمات → **بهینه‌سازی باتری** → SlipNet را بهینه نکن
یوتیوب / استریم بافر می‌کند	**Disable QUIC**؛ **Max Query Size** را روی تونل DNS کم کن؛ **Slipstream** یا **VLESS** را امتحان کن
محیط DPI سختگیر	از **VLESS + SNI Fragmentation**، **NoizDNS + SSH**، یا (Full) **Tor + Snowflake** استفاده کن
VLESS از Cloudflare تایم‌اوت می‌شود	**CDN IP** را روی یک IP تمیز معروف Cloudflare بگذار؛ **TLS SNI** باید با گواهی CF تو بخواند
SOCKS5 می‌گوید «Connected» ولی اینترنت نیست	پراکسی ریموت واقعاً به اینترنت آزاد دسترسی ندارد — SOCKS5 تست end-to-end ندارد. پراکسی را مستقل تست کنید، یا با SSH دور آن را بپیچید (از حالت `SSH +` استفاده کنید) تا خرابی آشکار شود.
می‌خوام لاگ به پشتیبانی بدم	تنظیمات → **Debug logging** → ریپروی مشکل → **Export logs**

---

۱۳. اشتراک‌گذاری و پشتیبان

- **اشتراک یک پروفایل**: روی پروفایل بزنید → منو → URI → **Export** `slipnet://` یا JSON.
- **خروجی همه**: منوی صفحه‌ی اصلی → **Export All Profiles** (ساده) یا **Export All (Encrypted)** با رمز.
- **بکاپ تنظیمات**: تنظیمات → منو → **Export Settings**.
- **اشتراک APK** با دوستان از طریق بلوتوث از منوی صفحه‌ی اصلی (مفید موقع قطعی اینترنت).

انواع URI کانفیگ

SlipNet سه نوع URI برای خروجی دارد. این‌ها **هم‌ارز نیستند** — مدل امنیتی هرکدام فرق می‌کند.

فرمت	چیست	کلید رمزنگاری
`slipnet://`	پروفایل ساده‌ی base64	ندارد — هرکسی می‌تواند بخواند
`slipnet-enc://`	پروفایل تکیِ **قفل‌شده** (مخصوص گیرنده‌ی خاص)	کلید درون‌برنامه‌ای SlipNet
`slipnet-bundle-enc://`	بسته‌ی چندپروفایلی، رمز شده با رمز عبور	از رمز عبور خود شما مشتق می‌شود

`slipnet://` — هرکسی با base64 می‌تواند بخواند. فقط برای گیرنده‌ی مورد اعتماد.

`slipnet-enc://` — وقتی یک پروفایل تکی را با قفل خروجی می‌گیرید (رمز، تاریخ انقضا اختیاری، قید به یک دستگاه، مخفی‌سازی resolverها، عدم اجازه‌ی بازنشر). محتوا با AES-256-GCM رمز می‌شود، **اما کلید AES درون اپ SlipNet جاسازی شده** و از رمز شما مشتق نمی‌شود. رمزی که می‌گذارید توسط اپ گیرنده بررسی می‌شود و فقط **نحوه‌ی استفاده** را کنترل می‌کند (فقط استفاده، عدم ویرایش، انقضا، قید به دستگاه، مخفی‌بودن resolverها). محرمانگی کانفیگ در برابر کسی که اپ را نصب دارد تأمین نمی‌شود. این را یک ابزار **کنترل اشتراک‌گذاری** بدانید، نه محرمانگی واقعی.

`slipnet-bundle-enc://` — توسط **Export All (Encrypted)** ساخته می‌شود. این یکی واقعاً با رمز عبور خودتان رمزنگاری می‌شود و برای پشتیبان‌گیری مناسب است.

⚠️ حتی کانفیگ رمزشده هم نباید در فضای عمومی منتشر شود

رمزنگاریِ بایت‌های کانفیگ، **هویت** سرور، دامنه یا CDN شما را پنهان نمی‌کند. به محض اینکه یک لینک `slipnet-enc://` در کانال عمومی منتشر شود:

- هرکسی که APK SlipNet را داشته باشد می‌تواند آن را باز کند و دامنه، CDN host، SNI، IP و credential را ببیند.
- سامانه‌های سانسور، کانال‌های عمومی را برای کانفیگ‌های جدید رصد می‌کنند و دامنه/IP را در عرض چند ساعت بلاک می‌کنند.
- خود دامنه از این به بعد یک هدف دائمی blocklist است؛ رمزنگاری نمی‌تواند آن را برگرداند.

اگر **VPS یا دامنه‌ی خود را داخل همان کشوری که می‌خواهید سانسورش را دور بزنید خریده‌اید**، خطر دو چندان است:

- ثبت‌کننده‌های دامنه و سرویس‌دهنده‌های هاستینگ داخلی می‌توانند **مجبور به افشای صاحب، توقف سرویس یا تحویل لاگ شوند**.
- دامنه‌های تحت TLD ملی (مثل `.ir`، `.cn`، `.ru` یا هر TLD تحت همان قضاوت قانونی) را می‌توان به‌صورت اداری توقیف کرد، فارغ از اینکه تونل شما چقدر رمزنگاری قوی دارد.
- VPS یا دامنه‌ای که قابل ردیابی به شخصی داخل کشور باشد، علاوه بر کانفیگ، **اپراتور** را هم لو می‌دهد.

قواعد کلی:

- برای پخش گسترده‌تر، روی **VPS خریداری‌شده از خارج کشور** و دامنه‌ی ثبت‌شده در **ریجیسترار خارج از کشور** میزبانی کنید. روی همان VPS، **Warp را از داخل SlipGate فعال کنید** تا ترافیک خروجی سرور از پشت Cloudflare Warp عبور کند و IP واقعی VPS لو نرود.
- کانفیگ را **خصوصی** بفرستید (تک به تک، در چت رمزنگاری‌شده‌ی end-to-end) — نه در گروه، نه در سایت، نه پین‌شده در کانال.
- قابلیت‌های قفل `slipnet-enc://` (انقضا، قید به دستگاه، مخفی‌بودن resolverها، عدم بازنشر) را برای **کند کردن سوءاستفاده** به کار ببرید، نه برای اینکه کانفیگ را عمومی کنید.

> ⚠️ لینک `slipnet://` حاوی اطلاعات حساس شماست؛ هرگز آن را در گروه عمومی نگذارید.
>
> ⚠️ لینک `slipnet-enc://` هم **برای انتشار عمومی امن نیست**: هر کسی که اپ SlipNet را داشته باشد می‌تواند آن را رمزگشایی کند. قفل، فقط *نحوه‌ی استفاده* را محدود می‌کند و **محرمانگی محتوا را تضمین نمی‌کند**. رمزنگاری از credentialها در حین انتقال محافظت می‌کند، اما به محض اینکه لینک علنی شد، **هویت دامنه و سرور شما لو می‌رود** و رمزنگاری نمی‌تواند جلویش را بگیرد.

---

۱۴. حمایت مالی

توسعه‌ی SlipNet داوطلبانه و بدون درآمد است. اگر این اپ به شما کمک کرده، آدرس‌های دونیت (BEP-20 / ERC-20، Monero، Arbitrum / و...) همیشه به‌روز در README پروژه روی گیت‌هاب نگه‌داری می‌شوند:
https://github.com/anonvector/SlipNet#donations

---

۱۵. نکات امنیتی

- SlipNet را فقط از **کانال رسمی تلگرام** یا **گیت‌هاب** دانلود کنید.
- لینک `slipnet://` خود را با غریبه‌ها به اشتراک نگذارید.
- موقع پشتیبان‌گیری از **Export رمزشده** استفاده کنید.
- اصالت سرور را با **Prism** (اسکن سرور-تأییدشده) اعتبارسنجی کنید — با SlipGate کار می‌کند.
- اگر سرور خودتان را اجرا می‌کنید: هیچ‌وقت `root` یا هر اکانت shell را به‌عنوان credential VPN ندهید — همیشه با SlipGate کاربر مخصوص بسازید.

کانال: @SlipNet_app سورس: https://github.com/anonvector/SlipNet