```
root@proxy-ops:~# ./deploy_blueprint.sh
```

现代代理系统架构蓝图与部署实录

面向 DevOps 与 AI Agent 的全生命周期自建指南

KERNEL	sing-box
PROTOCOLS	VLESS-Reality | Hysteria2 | TUIC-v5
CLIENT	Clash Verge Rev
STATUS	Automated & Hardened

协议“裸奔”的代价：Shadowsocks 秒封复盘

Step 1: 部署 (Deploy)

shadowsocks-rust

```
Port:   8388
Cipher: aes-256-gcm
```

Step 2: 拦截机制 (GFW Kill Chain)

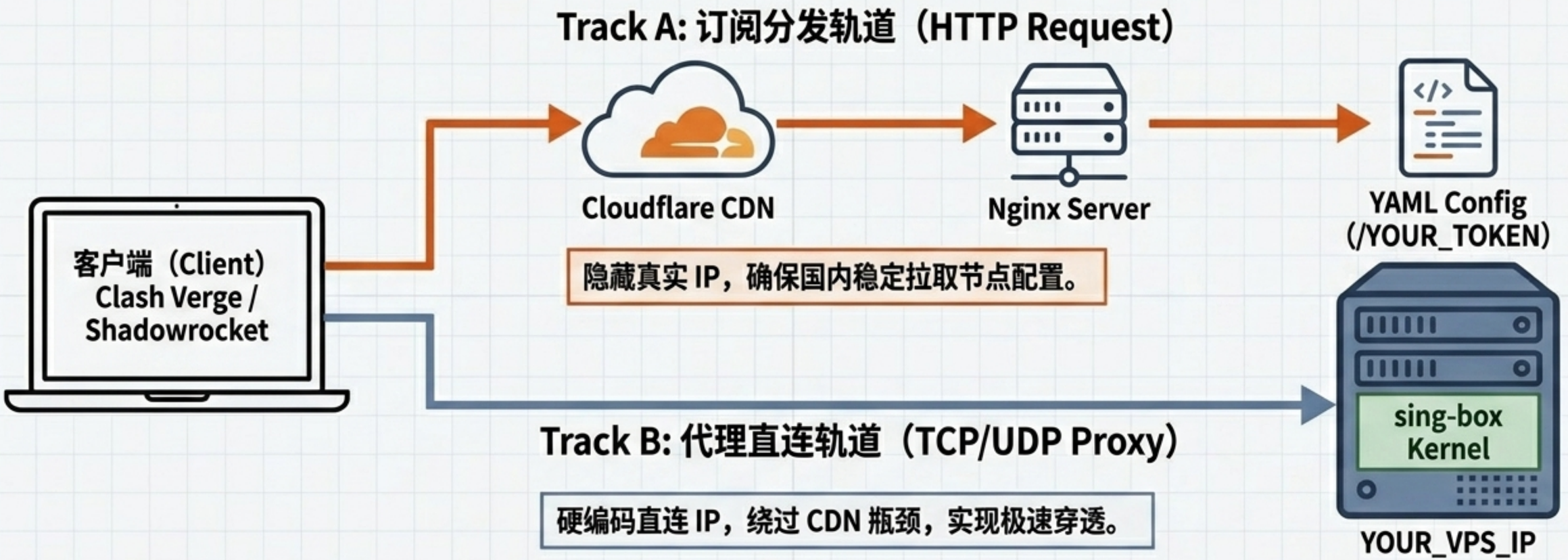
1. 主动探测 (Active Probing)：针对可疑端口
2. 熵值分析 (Entropy Analysis)：锁定高熵加密流量
3. 特征比对 (Signature Matching)：识别裸协议

Step 3: 结果 (Outcome)

Connection Timeout.
IP Blocked.

面向国内的 VPS，不能裸跑 SS/VMess/Socks5。必须采用具备 TLS 伪装或流量混淆的现代协议。

全局架构蓝图：双轨并行分发机制



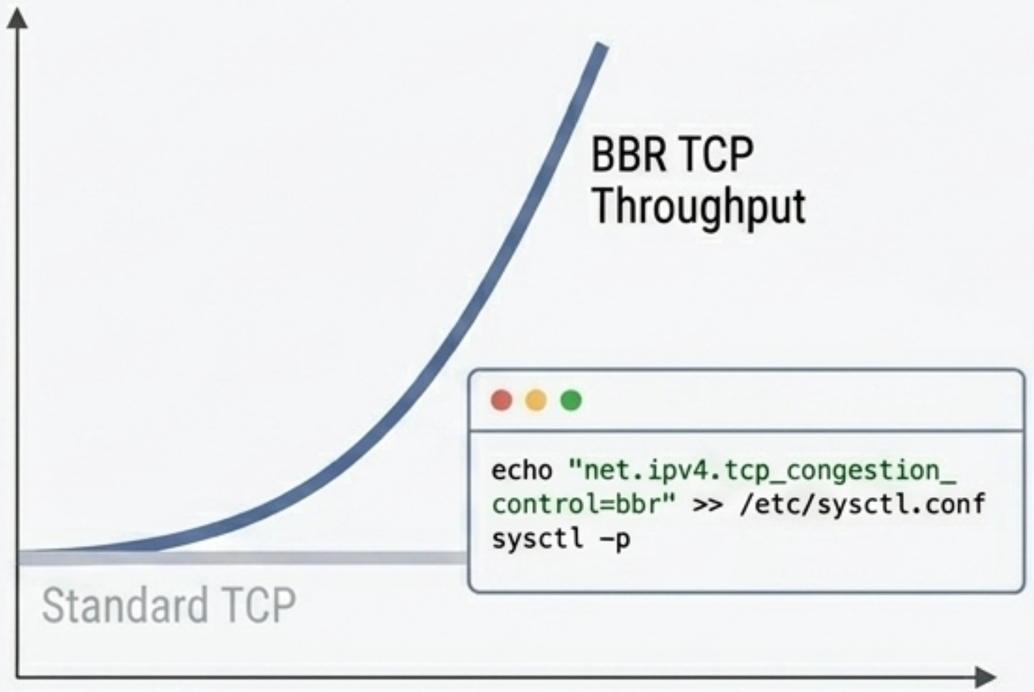
架构核心在于“解耦”——用 CDN 保护订阅分发，用直连保障协议速度。

底层基建：节点选择与 BBR 网络加速

推荐配置矩阵 (Recommended Specs Matrix)

IP 质量	静态住宅 IP (Atlas Networks) > 数据中心 IP (抗封锁性强)
优质路由	AS9929 / CN2 GIA (绕过骨干网拥堵)
最低要求	100Mbps 带宽 / 1TB+ 月流量 / Ubuntu 24.04.1 LTS

BBR 拥塞控制引擎 (BBR Congestion Control Engine)



**Linux 4.9+ 内核原生支持，跨国网络提速核心基石。*

现代代理协议诊断矩阵

协议 (Protocol)	传输层 (Layer)	抗封锁伪装 (Cloak)	推荐指数 (Rating)	核心定位 (Role)
VLESS-Reality-Vision	TCP	伪装 HTTPS	★★★★★	主力：抗封锁天花板
Hysteria2	UDP	QUIC 加速	★★★★	极速：高带宽场景优选
TUIC-v5	UDP	QUIC 加速	★★★★	低延时：交互式应用
Anytls	TCP	TLS 伪装	★★★★	备用：新型伪装
~~Vmess-WebSocket~~	TCP	无强混淆	★★	弃用：易被主动探测识别，需踢出自动组

```
root@proxy-ops:~# ./sb.sh # 一键生成并随机分配上述 5 组独立端口
```

SSL 签发与 CDN 代理的“云朵悖论”

State 1: 部署期（Deployment Phase）

灰色云朵 (Grey Cloud - DNS Only)

申请 Let’s Encrypt 证书

```
acme.sh --dns dns_cf
```

为什么：必须透传真实 IP 以完成 ACME 的 DNS API 验证，开启代理会导致验证失败。

State 2: 交付期（Handover Phase）

橙色云朵 (Orange Cloud - Proxied)

证书部署完毕，启动 Nginx 订阅服务器。

为什么：阻断 GFW 对真实 IP 的 HTTP 嗅探，利用 CDN 节点为国内提供稳定的 YAML 订阅下发。

重要提示：代理流量走硬编码 YOUR_VPS_IP，完全不受橙色云朵的 CDN 速度限制影响！

动态流量溯源：从网卡到客户端的优雅闭环

Step 1：数据抓取

vnstat

抓取 Ubuntu 底层物理网卡的出入站原始流量数据。

Step 2：脚本清洗

bash script

`update_traffic.sh` 计算已用和剩余配额，生成响应头配置。

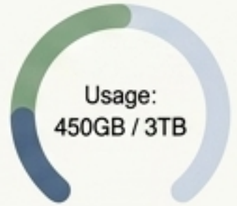
Step 3：头部注入

Nginx

通过 `.traffic_header.conf` 将 Subscription-Userinfo 注入 HTTP 响应头。

Step 4：终端可视化

Clash Verge UI



将底层服务器的生硬监控数据，无缝转化为最终用户的直观可视化体验。

终端控制台：Clash Verge Rev 路由策略

订阅导入：https://your.domain.com/YOUR_TOKEN
（务必点击卡片激活，呈现高亮边框）

代理模式：设定为『规则(Rule)』，实现国内外流量精准分流。

策略组设定：
- GLOBAL 设为『自动选择』
- 自动选择 (url-test) 仅保留 VLESS、Hys2、TUIC，彻底剔除高延迟的 Vmess-WS。

系统接管：开启系统代理（System Proxy）与 TUN 模式。

核心原则：客户端只负责拉取和分流。所有节点重命名、协议删减，均在服务端 YAML 侧完成，避免客户端重启导致修改被覆盖。

排雷矩阵 I：系统与环境基建

异常现象（Symptom）	根本原因（Root Cause）	战术解法（Tactical Fix）
SSH 密钥部署后仍要求输入密码。	供应商默认关闭 PubkeyAuthentication。	修改 `/etc/ssh/sshd_config` 并 `systemctl restart sshd`。
安装 sing-box 后，ufw status 报命令不存在。	sb.sh 脚本执行时默认移除了 ufw 防火墙。	重新安装 ufw 并配置规则，或直接接受原生 iptables 的 ACCEPT 策略。
节点连接测试 UDP 端口显示 Connection refused。	nc -zv 或 telnet 默认仅测试 TCP。Hysteria2/TUIC 是纯 UDP 协议。	使用专用 UDP 测试工具，勿依赖传统 TCP 探针进行网络侦测。

排雷矩阵 II：鉴权与证书流转

异常现象（Symptom）	根本原因（Root Cause）	战术解法（Tactical Fix）
acme.sh 申请证书持续报错，提示邮箱不匹配。	sb.sh 脚本运行时向系统注入了错误的邮箱账户缓存。	执行 `rm -rf ~/.acme.sh/account.conf` 清理缓存，附加 `--force` 重新申请。
证书自动续期成功，但客户端连接依然报证书过期。	acme.sh 默认路径与内核读取路径（/etc/s-box/cert.pem）未发生物理同步。	在 `acme.sh --install-cert` 的 `--reloadcmd` 中注入 `cp` 复制指令后再重启容器。
国内无代理环境下无法获取订阅 URL。	VPS 直连 IP 遭遇阻断或路由劣化。	开启 Cloudflare 橙色小云朵，利用 CDN 节点代理 HTTP 订阅请求。

最终交付清单（Definition of Done）

[ ] 服务端核心状态（Server Core）

- `systemctl status sing-box` 运行正常，5 大协议端口监听中。
- `systemctl status nginx` 运行正常，HTTPS 订阅路由可用。

[ ] 客户端状态（Client UI）

✓ 订阅卡片呈现 高亮边框（已激活）。
✓ 代理页节点列表已剔除 Vmess-WS。
✓ 延迟测试仪成功返回各节点毫秒级 Ping 值。

[ ] 自动化闭环（Automation Loop）

✓ 客户端成功读取并展示 `vnstat` 抓取的流量配额进度条。
✓ Cron 定时任务中包含 `acme.sh` 的证书自动续期与路径同步。

> 架构部署完毕。复制本手册核心参数，交由 Agent 启动执行环境。