

安装教程 —— 把安卓机顶盒变成「去广告 DNS 盒子」(旁路由 / AdGuard Home)

OpenHW Lab · 智能硬件开放实验室 · 面向普通用户 / 开发者。约 30-50 分钟。

用一台吃灰的**安卓机顶盒**，做成一台**局域网 DNS 服务器**：全家设备自动去广告、防跟踪，一次配置、全屋生效，手机/电视/电脑都干净。进阶可当"旁路由"。

本项目在 **B860AV1.1-T2** (中兴微 ZX296715 / **Android 7.1** / **armv8**) 实测通过。

0. 你需要

- 一台**已 root** 的安卓机顶盒 (能开 ADB; **不刷机**)。
- 已搭好的 **Linux 子系统 (chroot Ubuntu)** (参见系列其它教程 / 系统改造手册)。
- 电脑一台 (装 adb; 用 SSH 也行)。
- 路由器能改 **DHCP 的 DNS** (把下发的 DNS 指到盒子)。

总思路：子系统里跑 **AdGuard Home** (DNS :53 + 管理页 :3000)，

把它的**上游 DNS 改成 TCP** (老盒子 UDP 常被封)、加**广告过滤列表**；

再把家里路由器的 **DHCP DNS 指向盒子** → 全家生效。

1. 认清你的盒子 (1 分钟)

```
getprop ro.product.cpu.abi      # armv7 / arm64 (决定下哪个 AdGuard 包)
getprop ro.build.version.release
free -m | head -2
```

AdGuard Home 是**单文件二进制**，很轻，1G 内存的盒子跑它无压力。

2. 控制通道 (ADB / SSH)

盒子开「ADB 调试」→ 电脑：

```
adb connect <盒子IP>:5555 && adb devices  
# 或: ssh root@<盒子IP>    (登录即进子系统)
```

3. 取 AdGuard Home

AdGuard Home 只有 **https 下载**，而老盒子子系统常只通 **HTTP/80** → 在**电脑**上下好再传进盒子：

```
# 电脑上 (有 https): 到 github.com/AdguardTeam/AdGuardHome/releases 下  
#   AdGuardHome_linux_arm64.tar.gz    (armv7 盒子用 ..._linux_armv7.tar.gz)  
# 传进子系统 /root:  
adb push AdGuardHome_linux_arm64.tar.gz /data/linux/root/adg.tgz  
# 或 scp AdGuardHome_linux_arm64.tar.gz root@<盒子IP>:/root/adg.tgz
```

盒子子系统里解压：

```
cd /root && tar xzf adg.tgz && ls AdGuardHome/  
./AdGuardHome/AdGuardHome --version
```

4. 首次配置（用 API 免网页向导）

先后台跑起来（首次是"设置模式"，只开 :3000）：

```
cd /root/AdGuardHome && nohup ./AdGuardHome >/root/adg.log 2>&1 &
```

用 安装文件/adg_setup.py 一步配置（web :3000 / dns :53 / 管理员）：

```
scp 安装文件/adg_setup.py root@<盒子IP>:/root/  
ssh root@<盒子IP> "python3 /root/adg_setup.py 你的密码"
```

（脚本等价于向 `POST /control/install/configure` 提交配置。）

5. ★ 把上游 DNS 改成 TCP（关键！）

老盒子子系统里 **UDP 常被封**（DNS 查询发不出去）→ 必须用 **TCP 上游**，否则解析超时：

```
scp 安装文件/adg_upstream.py root@<盒子IP>:/root/  
ssh root@<盒子IP> "python3 /root/adg_upstream.py 你的密码"
```

它把上游设为 `tcp://223.5.5.5 / tcp://119.29.29.29 / tcp://114.114.114.114`。

验证（在电脑上查盒子）：

```
nslookup example.com <盒子IP>
```

能解析出地址就说明 DNS 服务通了。

6. 加广告过滤列表

AdGuard 的默认列表是 **https**（老盒子下不了）。用 **http** 列表：

```
scp 安装文件/adg_filters.py root@<盒子IP>:/root/  
ssh root@<盒子IP> "python3 /root/adg_filters.py 你的密码"
```

默认加了两个 http 列表：`pgl.yoyo.org`（≈3500 条）+ `someonewhocares.org`（≈1.3 万条）。

验证拦截：

```
nslookup doubleclick.net <盒子IP>      # 应返回 0.0.0.0（被拦）  
nslookup example.com    <盒子IP>      # 应正常解析
```

7. 设为"全家 DNS"

把路由器的 DHCP 设置里，下发的 **DNS 改成盒子的 IP**（如 `192.168.31.161`）。

这样家里所有设备（手机/电视/电脑）自动用盒子做 DNS → 全屋去广告。

- 只做 DNS（推荐起步）：改 DHCP DNS 即可。
- **完整旁路由**（可选进阶）：再把设备**网关**也指向盒子（盒子做转发/分流）——需更多网络配置。

⚠ 盒子是 DNS 单点：建议在路由器里**设备用 DNS**（如 `223.5.5.5`），以防盒子关机时断解析。

⚠ 部分 App 用**硬编码 IP/DoH** 绕过 DNS，拦不到；视频前贴片/YouTube 广告也拦不全。

8. 开机自启

把 安装文件/3-开机自启.sh 并入子系统的启动链（拉起 AdGuard Home）：

```
# 3-开机自启.sh 内容要点：  
pgrep -f "[A]dGuardHome" >/dev/null || ( cd /root/AdGuardHome && nohup ./AdGuardHome >/rc
```

4-开机兜底.sh 是盒子侧（Android）挂载+启动脚本模板，按你盒子的启动链放置。

重启一次验证：盒子重启后能继续解析（nslookup 到盒子）。

9. 使用 / 管理

| 用途 | 地址 |

|---|---|

| **AdGuard Home 管理页**（看拦截统计/规则/设备） | <http://<盒子IP>:3000/>（账号 admin / 你设的密码） |

| **DNS 服务** | <盒子IP>:53（路由器 DHCP 指向它） |

管理页可看：总查询量、**拦截比例**、拦截排行、每台设备的查询、被拦域名；也能加/减规则、设家长控制。

10. 恢复 / 卸载

不刷机、不改固件，全部可逆：

- 停服务：`pkill -f AdGuardHome`
- 路由器 DHCP 的 DNS 改回原样（或自动获取）
- 删 `/root/AdGuardHome` 与启动脚本里那行即可。

有问题先看 [常见问题.md](#)。更多见 [开发者资料/](#)（系统改造手册 / 关键坑与经验 / 源码）。

本项目开源（MIT）——OpenHW Lab • openhwlabs.com