## 概述

本设置试图实现DNS完全自主定义和日志追踪效果，以及实现基础国内外上网功能。

设置流程基于《EzOpWrt Ipv6-Mini-Vip-R2023.07.16 by Sirpdboy》固件，仅为adguard+ passwall+ smartdns设置流程。软路由设置是否成功和正确，从日志判断是最准确的，这也是本设置流程的依据。

本设置会让DNS数值看起来很好，但0.02ms和200ms看似1万倍差距，其实感觉不出来差异，故实际意义有限，实际设置时不用太纠结。

因为新旧固件差异很大，此教程主要讲述原理，实际设置只要架构对就可以，绝大部分默认设置其实也不需要变动。

## 架构解析



架构设置完毕，主机建议用 ipconfig /flushdns 方式清空缓存DNS。手机则可以开飞行模式，恢复后清空DNS缓存。

此架构搭建时，除基本网络接口设置外，建议从后向前设置，即先设置SMARTDNS，再设置PASSWALL，能成功出墙后再设置ADG更新内核。

此架构会导致所有DNS从路由器走，即使指定了114DNS也会由路由器劫持和解答，故从根本上避免了手机内置DNS的污染。

## 设置流程

玩家需要知道，各DNS应用设置不当都可能导致DNS架构崩塌，故原则上系统中的任何APP只允许设置自己的部分而不应该强制去变动DNSMASQ。

### 光猫桥接

以联通某光猫为例，记住VLAN号，增加桥接设置为PPP，如下：



桥接后，所有IPV6配置中，关闭所有RA通告和DHCPV6服务。DHCPV4的建议保留，以方便维护。



### 分区扩容

如果要扩容开docker，就第一时间搞，不要设置完了想搞把配置弄丢了。

//也可以用命令行分区和挂载，但不建议，容易出错。

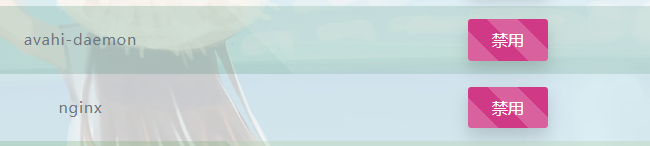


### 计划任务&任务设置

简单看一下，没事别释放内存和重启机器，固件中很少发现内存泄漏软件，释放内存和重启只会让机器变慢。

### 系统->启动项

普通用户Nginx和avahi服务，点击为禁用状态。Nginx会占用80&443端口导致冲突，avahi的mDNS组播服务可能导致FE80的IPV6每20分钟被回收和重新注册而触发PASSWALL重启。若使用ipad隔空打印，则建议/etc/avahi/avahi-daemon.conf 中设置 use-ipv6=no

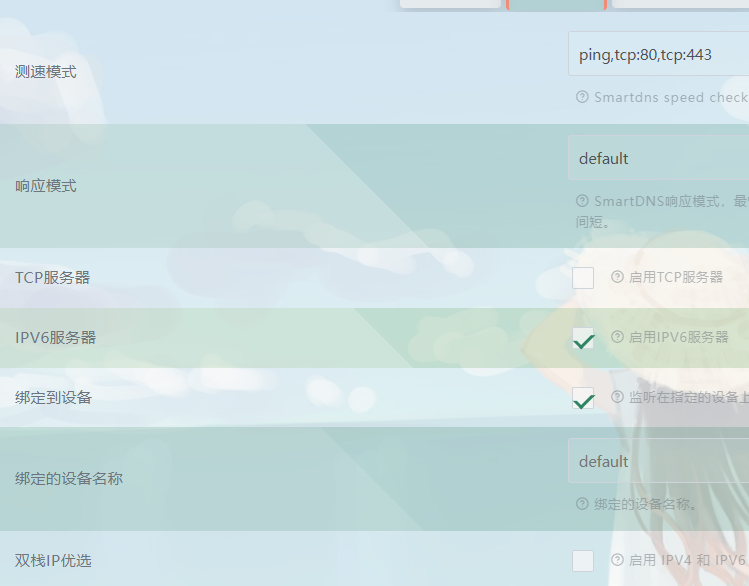
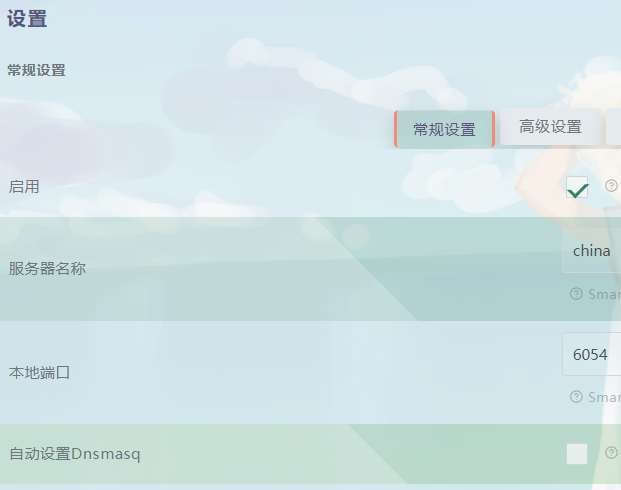


### SmartDNS

实现的功能只有一个：屏蔽不需要IPV6解析的网址。另一功能测速和选择较快DNS，开不开其实没意义。

除红色部分外绝大部分设置其实不需要变动，此处仅为理论分析协助玩家理解。

基本设置





各选项解释如下：

//TCP服务器：用于TCP查询DNS；普通用户不需要

//IPV6服务器，监听IPV6本机地址[::1]:6054的请求；

//双栈IP优选：若IPV4/IPV6其中一个延时太长，则直接丢弃DNS解析，目前大陆网络IPV6已全面提速，此项建议取消。

//域名预加载：缓存的DNS过期即TTL=0时，自动向上查询更新；这个理论上效果最好，但也在理论上会加重路由器负担，并导致频繁向上游查询DNS和连接代理查询国外DNS，长期连接代理或许更容易导致节点被封

//缓存过期服务：当DNS过期即TTL为0时，回复TTL=5的短周期DNS给客户端

以防止等待

//缓存大小，设置为0即可，因为后续有ADG的乐观缓存，等同于此处的缓存过期服务，故SMART不开启缓存，仅作为一个查询过程使用。

//解析本地主机名：按本架构DNSMASQ其实会直接回复客户机，开不开都一样

//停用IPV6解析，不返回IPV6解析地址，此项一般会取消，以返回IPV6地址。

//停用HTTPS地址解析：过滤掉 HTTPS 类型65的查询 ，避免iOS设备绕过常规DNS服务

//TTL时间，默认即可，一般不需要额外设置。

第二DNS服务器



第二DNS服务器建议 跳过测速并停用IPV6地址解析。

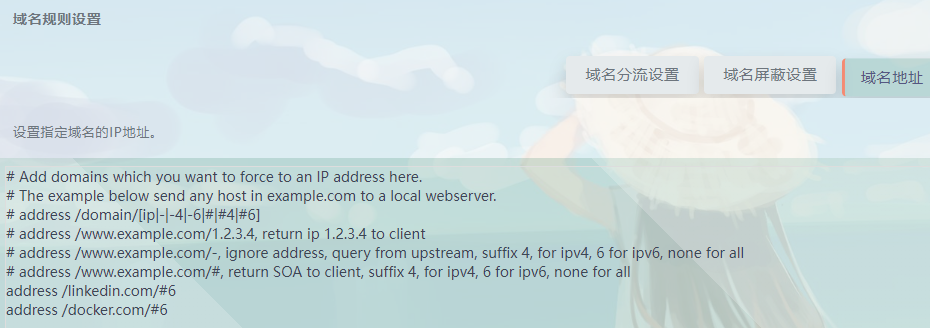
测速ping是路由器本身测量的，而实际流量则是从VPS中转的；例如日本VPS开启测速后可能返回美国的IP地址。IPV6则建议直接停用。



上游服务器：

国内为：223.5.5.5, 223.6.6.6, UDP

国外为：8.8.4.4，8.8.8.8，DOT，其它DOH和DOT节点亦可。若使用DOT（tls），请记得passwall的TCP转发端口增加853，不然DNS会直连请求导致被墙干扰。



此栏为特色设置，例如禁用国际版领英的IPV6以强制其走代理；另可设置WIN默认时间同步为路由器地址（DNS劫持建议都做在DNSMASQ，尤其劫持为内网地址会被重绑定保护丢弃）。

//此时SMART进入服务状态，实际并未被任何服务使用。

### 接口

在2023的固件中有设置向导，原则上设置后不需要变更细节。此章节引导手动设置，尽量少改动默认值为妙。

全局网络选项

IPv6 ULA 前缀 建议删除好了，直接用公网前缀即可。

一般建议外网口新增城域网接口，MAN口：//和WAN共用一个口

1. 传输协议用DHCP客户端。这样就可以直接用IP访问上游的光猫。
2. 防火墙设置，选择WAN/MAN。

~~~~

WAN6接口设置

如果用路由器拨号，物理设置改为@WAN，即可看到前缀等信息。如果是猫拨号并下发前缀则用WAN口即可。



LAN口->IPV6设置

检查一下DNS，有可能是错误的。::1地址的前缀会导致问题，此处直接留空即可。



观察IPV6 WAN的分发前缀，例如：

IPv6-PD: 2408:\*::/60

//若没有前缀，则联系供应商下发前缀。/64前缀也可下发，但会是最小子网。

IPV6的/64子网无法进行2级路由下发而只能采用通告和中继模式，设置很容易出问题，所以网络中不建议使用2级路由。若非要2级路由，则建议主路由下发整个WAN口的/60长度且主路由支持dhcp前缀下发，2级路由下发/62或/64才行。具体设置较为复杂且作者没有这方面的实战经验。

### DHCP/DNS（Dnsmasq）

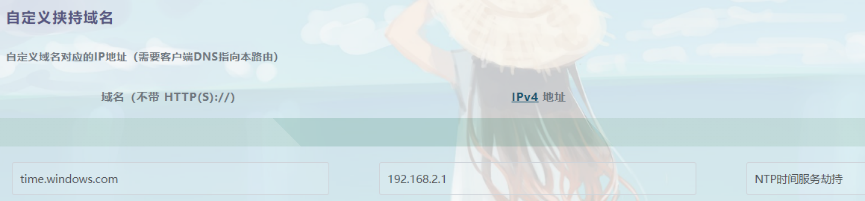
基本设置：

DNS转发，填写127.0.0.1#6054 //#不要错误写成冒号

重绑定保护，在校园网这种有内网解析的环境中要取消。

也可劫持域名，以便内网同步时间。





高级设置：

禁止解析 IPv6 DNS 记录，取消勾选，启用IPV6解析。

DNS 服务器端口：保持默认的53

最大并发查询数，建议加大为9999 //其实意义不大

DNS查询缓存大小，建议设置为0 //其实意义不大





//至此，所有DNS会进入路由器，之后被转发到SMARTDNS的6054口，即阿里DNS。

//此时并没有分流！也就是会存在DNS污染。

### ACC网络加速设置

建议除FULLCONE(全锥形NAT)外全部取消，DNS加速必须取消。

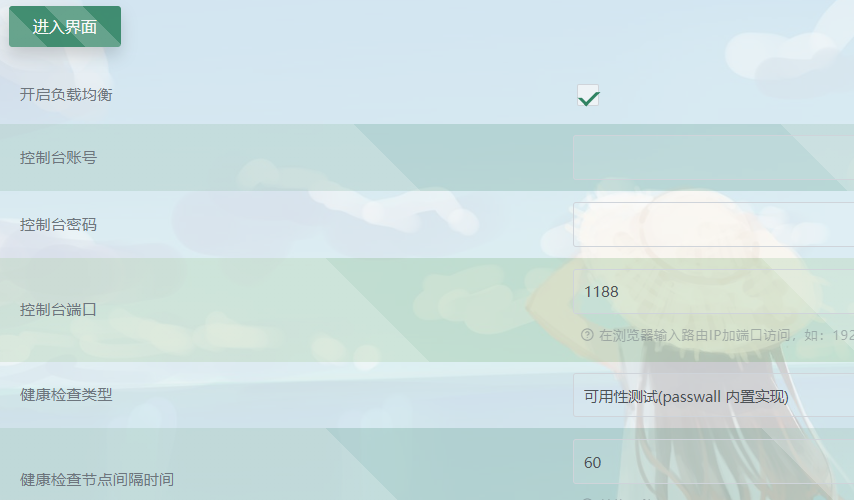
注意：在新版本固件中，FullCone-NAT在“防火墙”设置中。



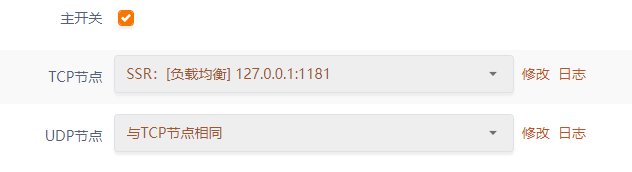
### PASSWALL

新版可直接添加本地SOCKS节点127.0.0.1：1181，以开启负载均衡：建议健康检查1小时即可，1分钟其实有点过于频繁。//IPV6节点其实不会被封





注意旧版的PASSWALL，其类型、密码、加密方式等，必须与“负载均衡”中的所有节点一模一样！否则无法工作。



基本设置->DNS：（不要开启chinadns-NG为上游）

若为其它版本，此画面会不同，但原则不变：

国内为DNSMASQ解析，前方设置中已转发到SMART的6054国内端口；

过滤模式为UDP，地址可能为127.0.0.1:7054，用冒号或者#号取决于不同版本，设置成功后看日志即可确认是否正确。





高级设置/（其它设置）：

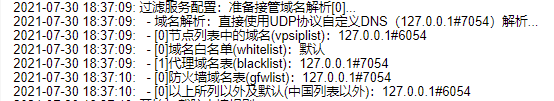
TCP转发端口，若使用了DOT的DNS，请记得常用端口只有（22,25,53,143,465,587,993,995,80,443），853在旧版固件中并没有在常用端口中，一定要手动添加853。

IPv6透明代理(TProxy)，开启后国外IPV6分流到代理，实测会导致卡顿，还不如禁用第2DNS的IPV6更好。

直连/代理名单管理->代理列表：

已默认dns.google，doh.opendns.com和IP（8.8.8.8，8.8.4.4，208.67.222.222， 208.67.220.220）走代理表，若没有请自行添加。若有其它国外DNS，也一并把域名和IP地址添加到表内。//一般建议把github.com也添加进代理。建议把linkedin.com也添加进去。

检验设置是否成功，请在启动后查看PASSWALL日志，若有以下信息即为正确：



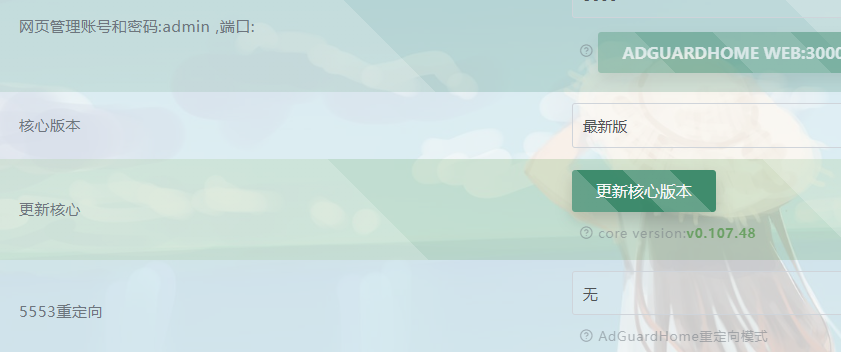
此时系统应该能正常出墙。

### AdGuard Home

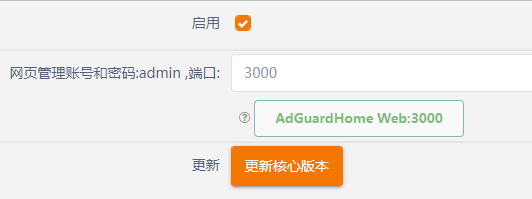
先更新内核，由于系统已将github走代理，很容易成功。

此处不需要重定向端口了，因为后一章节防火墙规则会把所有DNS支持到这里了。此处端口要和防火墙对应。

开机后网络准备好时重启，这个因为是防火墙转发，不需要判断内网地址范围，故不再需要勾选。

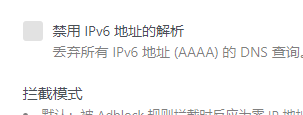


点击管理界面的绿色区域“Web:3000”进入管理器：



设置->DNS设置:

1. 上游DNS服务器，127.0.0.1:53 //指向系统的Dnsmasq端口  
   
2. 禁用IPV6，取消



1. 若此处DNS缓存建议直接设置大值并开启乐观缓存，TTL则建议留空。



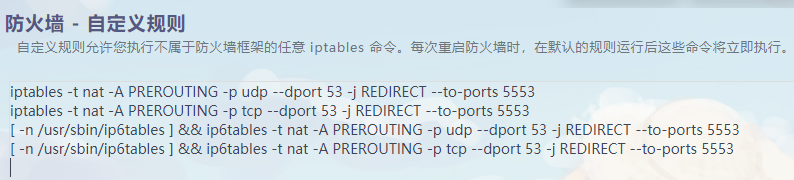
//此处乐观缓存DNS解析数据为0.1毫秒左右，很漂亮。但也只是看起来漂亮。

//每个DNS约605字节，此处约10万+缓存，基本够用了。



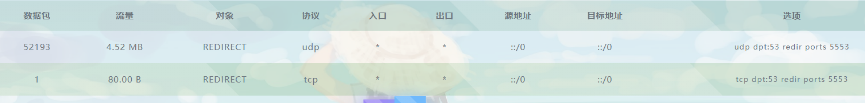
### 防火墙：

自定义规则，53端口的条目全部转发到ADG的端口，例如5553或6060，具体看ADG监听的哪个端口。此处为关键步，可支持所有外网DNS，如114或8.8到ADG，并统一分流和解析，避免泄露给其它DNS。也就是说，即使客户端指定外部DNS也是无效的，这个对于非常规应用的客户端可能会有问题，还需要慎重考虑。



防火墙的NAT表中包括IPV6的DNS请求可看到已转发：





## 检查客户端

不再需要检查客户端，手机内置114的也没问题了。

## 关于IPV6

路由器的::1为IPV6地址，与IPV4的127.0.0.1是无缝互通的；adguard也会处理IPV6流量，开启后从防火墙规则可以看出来；SMART作为最终DNS服务器可实现IPV6的完美解析和访问。

## 关于DNS缓存

根据架构，DNS时会经历ADG，DNSMASQ，SMART三个流程，此3项皆可设置缓存。显然，从理论上分析，ADG即最底层做DNS缓存和乐观缓存会更有效加快DNS解析。

但实质上软路由处理此3项流程都是瞬间完成的，无论SMART或是ADG带有缓存并返回过期服务，就能实现软路由的最快解析。

## 关于重启

正常情况下没有内存泄漏的软件，软路由设置好后解析和服务会越来越快，不建议重启。新版固件重启后PASSWALL延迟1分钟启动，此时ADG缓存会出现被污染的DNS解析，解决方法为进入3000端口WEB，设置DNS部分清空缓存或者等待TTL时间结束。

//WAN口变动时/etc/hotplug.d/iface/下防火墙等会重启和自动适应。

//路由器若不稳定，则应该从系统日志中找原因，重启并不能解决问题。

## 关于配置备份

实测发现大部分配置能恢复，但adguard内部设置，以及docker无法恢复。

## 关于打印机

存储->打印服务，可开启打印机，但只适应于windows安装驱动后使用；

另一服务CUPS可供安卓和苹果使用，建议使用以下docker:

docker run -d -p 631:631 --privileged=true -v /dev/bus/usb:/dev/bus/usb -v /var/run/dbus:/var/run/dbus --name cupsd olbat/cupsd

驱动程序较多，密码和用户名为print/print,地址格式示例为：

192.168.2.1:631/printers/HP\_DeskJet\_1200\_series

CUPS依赖于AVAHI服务，建议此服务按前文方式禁用IPV6而保留IPV4。

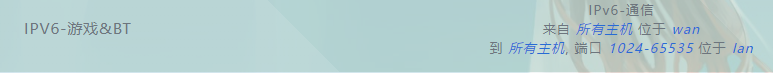
## 游戏设置

游戏设置理论上会导致端口暴露，增加风险，但实质上问题不大。

### 防火墙

启用fullcone-nat为高性能模式，一般上运营商上游设备也有此设置，即可允许外界玩家联接本机。

流量规格，则建议转发WAN口至LAN的IPV6高位端口的TCP/UDP转发，以优化IPV6游戏体验。这样会导致端口暴露，但/64子网数量巨大，并不担心外界扫描子网地址。



### VPS主机

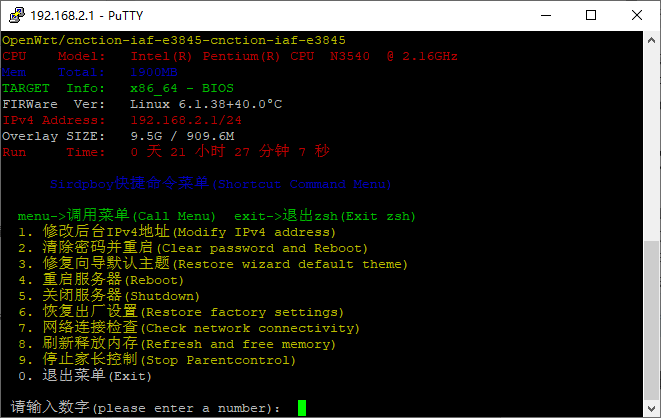
PASSWALL默认代理国外UDP流量，此时需要关闭PASSWALL的负载均衡，以保证UDP流量会代理到同一主机。

VPS方面则建议直接开启高位的UDP端口，以允许其它玩家连接。

firewall-cmd --permanent --add-port=1024-65535/udp

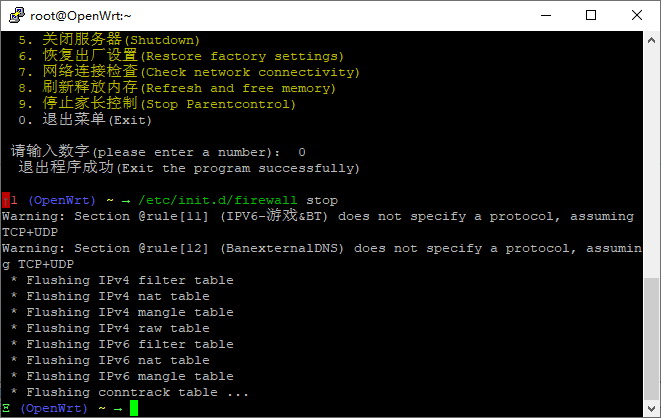
## 临时禁用防火墙

如果规则设置错误，则可能导致LAN口无法连接路由器造成问题；此时若有外接屏幕可接触路由器，可按以下方式尝试：



按0退出菜单，输入 /etc/init.d/firewall stop

出现Flushing字样就代表防火墙iptables规则被清除了。



此时防火就已经关闭了，可LAN口访问，请尽快重新设置规则；完成后/etc/init.d/firewall start 即可启动防火墙正常使用。

//转发也是防火墙功能，所以防火墙不要关闭，会导致DNS查询等转发生效。

## 更新日志

202501修订防火墙顺序在ADG之后，以便先更新ADG的核心；新增IPV6 QUIC直连设置

2024.6 修订ADG的TTL细节以减少路由器重启后DNS污染时间

2024.4 劫持所有DNS解析到路由器，根本上杜绝手机DNS泄漏给114

2024.4 增加禁用防火墙的临时措施，以方便设置错误的朋友及时修正规则

2024.4 增加防火墙指定路由器为惟一DNS，解决国内手机艹墙DNS污染问题。

2024.3 增加SMARTDNS的UDP设置解释，不建议新手尝试；增加VPS设置建议

2023.12 禁用第二DNS的测速，增加第二DNS的UDP方式和设置细节

2023.9 更新Avahi为禁用IPV6，解决CUPS隔空打印问题，增加游戏设置

2023.8 增加光猫桥接示例，建议清除nginx和avahi，修订WAN6物理设置

2023.7 因刷新固件，PASSW负载均衡等按新版更新为SOCKS

2023.6 更正重绑定保护的认识错误，删除IPV6NAT网，实际发现NAT没有意义

2023.4 尝试新固件后进行细节更新，添加打印机设置。

2022.11 根据新固件更新图片界面和部分细节描述。

2022.10 取消LAN网关设置，更正对IPV6前缀的理解以及2级路由架构说明，增加客户端检验，以及重启描述章节

2022.8 设置惟一缓存到ADG以实现理论最快DNS解析

2022.7 增加配图以方便新手设置，同时对于新的固件也利于对照。

2022.6 增加解释说明以方便使用者选择细节设置。

2022.2 尝试根据防火墙原理暴露IPV6给油管，以达到去广告的目的，旁门左道版

2021.8 更正国内SMART端口格式为#6054

2021.8 取消smardns的“域名预加载”，以减轻软路由负担

2021.6 以元旦版为固件，基本形成系统

2021.1 开展尝试与总结

=============================================//分隔线

## 旁门左道设置

本章节补充一些非常规的设置方式和应用，需要玩家理解原理，并对自己的代理有一定的了解；不需要的玩家请勿尝试。

### SmartDNS的第二DNS用UDP

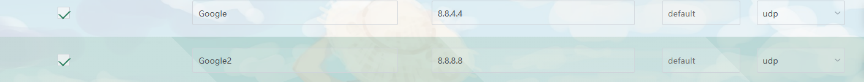
此项设置并没什么意义，只是理论上速度更好，代理节点负荷更小；但因为很依赖节点，所以此设置从标准设置中移除放在了此章节。

若节点支持UDP，其实SMARTDNS的第2DNS也可用UPD；具体设置为：

PASSWALL中的模式，UDP设置为中国以外，这样类似8.8.8.8的DNS以及国外游戏UDP会走代理。



之后smartdns的国外就可以使用UDP，从代理出发去查询并返回正确的结果。



### 关于Quic直接油管IPV6

但这个设置的效果每个人都不一样，有人直连很快，但有的区域则可能连上导致负面作用。直连会有去广告的效果。

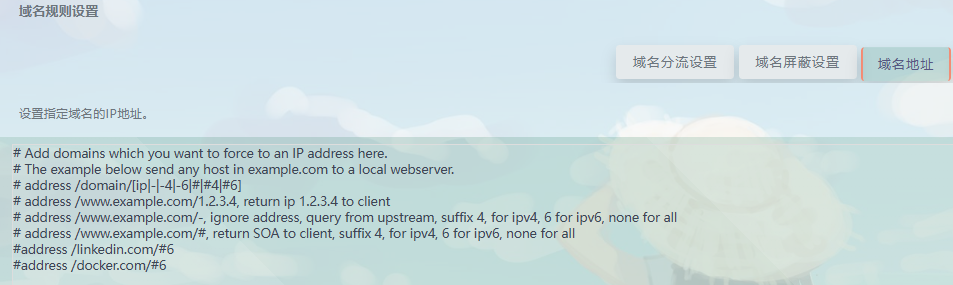
因为IPV6地址很多，其实DNS解析正确时，大陆是可以用QUIC直接油管的IPV6地址的，设置如下：

SMARTDNS部分，取消测速模式，让解析的地址全部返回给主机；

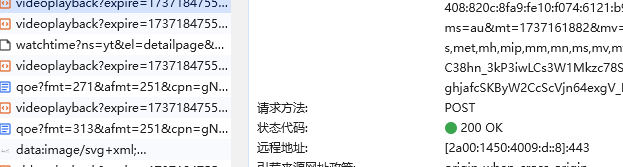


第二DNS，取消“停用IPV6地址解析”，让所有IPV6地址返回给主机，以便挑选能用的地址进行直连；但一些国内能连的网络如领英，必须在规则中禁用IPV6解析，在“域名地址”中设置即可。

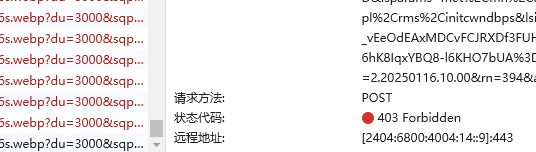




同时passwall的IPV6透明代理不要开，即可主机完成直连。



当然也可能有连不上的，如下图所示，会在延时之后，返回到代理的IPV4进行连接。



### 关于代理的建议

无论软路由是否带AES指令集，常见代理软件都不会调用，而是采用CPU计算来搞定，故AES指令集其实没有意义；在IPV6的节点，用最简单的rc4-md5加密就很稳定了，完全不需要强加密和TSL，也不需要负载均衡。

软路由连接外网虽然不知道具体在看什么，但一定知道是在出墙；如果用左道方式，则会直接发现连接的IPV6视频和网站，从理论上讲不回帖和转发才是自保的最优手段。