OpenWRT路由器上的ShadowSocks+ChinaDNS搭梯子方案

笔记本： default
创建时间： 2016-10-15 20:45
URL： http://blog.chionlab.moe/2016/01/23/openwrt-bypass-gfw-solution/index.html

OpenWRT路由器上的ShadowSocks+ChinaDNS搭梯子方案

在路由器上运行ShadowSocks科学上网是最为优雅的方案。本文将介绍其安装和配置步骤。
首先为智能路由器刷上OpenWRT，博主推荐Pandorabox修改版。本文将实现：连接上路由器的客户端当访问国内主机时，直接连接，而访问国外主机时，自动代理。

安装ShadowSocks

1. 因为本文讨论的是SS+ChinaDNS的翻墙方案，对于部分已集成SS+domain list的固件版本，需要先删除已安装的SS及相关工具。

```
#ssh连接上路由器后运行
$ opkg list_installed | grep shadowsocks #查询已安装的ss和相
# opkg remove shadowsocks-* #删除之
```

2. 下载安装shadowsocks-libev-spec
http://sourceforge.net/projects/openwrt-dist/files/shadowsocks-libev/
经作者测试，最新版在极贰最新OpenWRT固件上会出现iptables规则失效的情况，建议使用 `shadowsocks-libev-spec_2.3.0-1_XXXX` 版本。
以MT7620系列为例，在路由器上运行：

```
# opkg update
# cd /tmp
# wget http://sourceforge.net/projects/openwrt-dist/files/
# opkg install shadowsocks-libev-spec_2.3.0-1_ramips_24kec
```

3. 下载安装luci-app-shadowsocks-spec
   luci-app提供ss的图形化配置界面。
   http://sourceforge.net/projects/openwrt-dist/files/luci-app/shadowsocks-spec/
   如果 `shadowsocks-libev-spec` 使用的版本是本文推荐的 `2.3.0`，请下载 `luci-app-shadowsocks-spec_1.3.2-1_all.ipk`。路由器上运行：

```
# wget http://sourceforge.net/projects/openwrt-dist/files/
# opkg install luci-app-shadowsocks-spec_1.3.2-1_all.ipk
```

安装ChinaDNS

ChinaDNS用于解决国内DNS污染问题，同时可加速国内网站的访问。其原理如下：
提供至少一个国内DNS服务器和一个国外DNS服务器，ChinaDNS收到来自用户的DNS请求后，同时向这两个服务器发DNS请求。如果从国内DNS服务器返回的解析结果为国外IP，则选择国外DNS服务器的解析结果，否则选择国内DNS的解析结果，最后返回给用户。
http://sourceforge.net/projects/openwrt-dist/files/chinadns/

1. ChinaDNS

```
$ wget http://sourceforge.net/projects/openwrt-dist/files/
# opkg install ChinaDNS_1.3.2-3_ramips_24kec.ipk
```

2. luci-app-ChinaDNS
   http://sourceforge.net/projects/openwrt-dist/files/luci-app/chinadns/

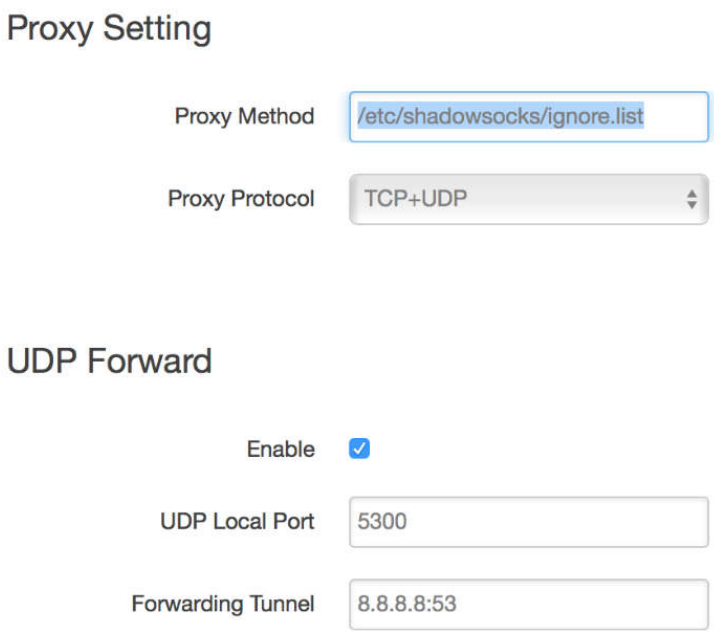
```
$ wget http://sourceforge.net/projects/openwrt-dist/files/
# opkg install luci-app-chinadns_1.3.4-1_all.ipk
```

配置ShadowSocks

1. 创建国内IP段列表，用于忽略国内目标主机。

```
# mkdir /etc/shadowsocks
# wget -O- 'http://ftp.apnic.net/apnic/stats/apnic/delegat
```

2. 使用luci-app配置ss
   进入路由器管理web页面，用root登录，进入服务(Services)->ShadowSocks。
   勾选启用Shadowsocks，输入ss服务器信息（服务器IP、端口、密码、加密方式）。
   代理方法(Proxy method)选择忽略列表(Ignore list)，并在—custom—中填入 `/etc/shadowsocks/ignore.list` 。代理协议(Proxy protocol)选择 `TCP+UDP` 。
   开启UDP隧道，UDP本地端口5300，目的地址 `8.8.8.8:53` 。UDP隧道用于加密DNS查询包，稍后将会用到。



3. 保存并应用(Save and Apply)

配置ChinaDNS

```
1  wget -O- 'http://ftp.apnic.net/apnic/stats/apnic/delegated-apni
```

在路由器web管理页面，进入服务(Services)->ChinaDNS。
勾选启用ChinaDNS，启用DNS压缩指针。
本地端口写5353，中国路由表(CHNRoute File)
填 `/etc/chinadns_chnroute.txt` 。
上游DNS服务器填 `114.114.114.114,127.0.0.1:5300` 。（可将114.114.114.114改成当前ISP提供的DNS服务器IP）
这里将ss的UDP隧道作为ChinaDNS的国外DNS上游源。
保存并应用

配置路由器DNS(Dnsmasq)

进入网络(Network)->DHCP and DNS。
将DNS转发(DNS forwardings)设置为 `127.0.0.1#5353` 。这将使得路由器将DNS请求经由dnsmasq全部转发至ChinaDNS处理。
这样设置后，从内网主机端发出的国外DNS请求将发送至：dnsmasq->ChinaDNS->ss-tunnel->ss服务器->8.8.8.8，
国内DNS请求则：dnsmasq->ChinaDNS->114.114.114.114
还要记得勾选“忽略解析文件”(ignore resolve file)。

至此，路由器上的梯子已经搭建完毕，如不出意外，你已经可以进youtube了。
但是，受路由器到ss服务器的链路质量影响，可能会出现不稳定的情况。例如某些ISP下会出现境外UDP流量丢包、多TCP并发连接容易建立失败等情况。博主将在下篇文章中介绍优化方案。

关于shadowsocks-libev-spec的原理

通过分析ss的启动脚本，初步确定ss-libev-spec是以以下步骤实现自动翻墙的。

1. 运行 `/usr/bin/ss-rules` ，设置在ipset中建立一个列表 `ss_spec_wan_ac` ，列表中存放了 `/etc/shadowsocks/ignore.list` 中的IP段（即为需要忽略的国内IP段），然后设置iptables，在 `nat` 表的 `OUTPUT` 链中将目标地址 `match-set`

`ss_spec_wan_ac` 的包采取 `RETURN` 处理。然后再在这条规则后增加一条，将全部包 `REDIRECT` 到 `127.0.0.1:1080`

2. 运行 `/usr/bin/ss-redir`， 监听本地端口 `1080`， 负责将收到的包经由ss，加密socks代理至ss服务器。
3. 运行 `/usr/bin/ss-tunnel`， 经由ss服务器建立加密的UDP隧道，隧道一端为本地监听端口 `5300`， 另一端为 `8.8.8.8:53` 。

#openwrt #router

评论 分享