1. 规则

1.1 什么是规则

配置过防火墙和路由表的人肯定都知道, 这两样东西的行为基本上就是由你配置下去的规则决定的. 比如防火墙, 对哪个地址的访问你想要允许它给你放行的, 哪些端口的访问你是要禁绝的, 都得以规则的形式告诉防火墙. 同样的, 对路由表来说, 系统上哪些地址的访问该怎么走, 有没有网关, 你也得告诉它, 要不然网肯定通不了.

对Postern来说规则的作用也是同理的, 总的来说, Postern会管理设备上所有的对外访问, 当发现有一个APP发起一个新的访问请求时(一个TCP连接), Postern必须做出一个选择:

1. 是屏蔽掉这个请求吗?
2. 是让这个请求和其后的数据流量都经过某一个代理吗?
3. 是啥都不干假装没看见这个请求直接放行吗?

以上三种就是Postern可以帮你做到的, 但前提是你得通过合适的规则来告诉Postern该如何做. 比如, 某些APP发出的广告流量, 你想屏蔽掉, 就得用规则告诉Postern. 又比如, 对某些地址的访问, 你想通过代理走, 也得用规则告诉Postern.
所以总的来说, 规则这个东西在Postern里面扮演了核心的角色, Postern完全依据规则来管理你设备上的数据流量.

1.2 规则怎么配

Postern能够识别导入的一种格式是目前网上比较流行的surge的配置文件格式, 所以这一节就拿这种配置文件为例说明.

首先是地址的匹配方式: Postern看到通往某个地址的数据时, 就要拿这个地址和规则去比对, 看看到底有没有命中的规则, 这条规则又指定了什么动作. 这就牵涉到地址匹配的问题. 一般来说, 一个地址有两层, 一个是IP地址, 一个是域名. 比如要访问www.google.com, 这是一个域名, 浏览器还得解析这个域名成IP地址. 这个域名和IP地址, 共同构成了这个地址的含义, 它们都代表www.google.com这个服务器的地址. 相应地, 在地址匹配的时候, 就有两类匹配方式:

按照域名来匹配, 又细分:

1. 匹配域名关键字 (DOMAIN-KEYWORD)
   只要域名的某一个字段(**注意: 必须是一个完整的字段**)匹配了关键字就能命中规则
   例: DOMAIN-KEYWORD,google,REJECT
   类似于www.google.com, www.google.com.cn 都能命中这条规则; 但www.googleusercontent.com无法命中.

2. 匹配域名后缀 (DOMAIN-SUFFIX)
   顾名思义, 域名的后缀部分能对上就命中规则
   例: DOMAIN-SUFFIX,google.com,Proxy
   www.google.com, mail.google.com 能命中这条规则, 但www.google.com.hk无法命中

3. 匹配精确域名 (DOMAIN)
   域名完全对上了才能命中规则
   例: DOMAIN, www.google.com,Proxy
   只有对www.google.com的访问才能命中该规则, mail.google.com, www.google.com.cn统统无法命中

按照IP地址来匹配, 又细分:

1. 匹配国家IP
   按照IP地址的国家所属来匹配
   例: GEOIP,CN,DIRECT
   那么你访问中国的网站比如网易的那些数据就会命中这条规则
   值得一提: Postern的GEOIP数据库包含了全球236个国家和地区的IP-国家对应信息. 所以你可以在规则中以二位字母代码的方式指定几乎任意一个国家. 详细的国家代码列表见后面的附录.

2. 匹配CIDR　IP
   按照IP子网段来匹配
   例: IP-CIDR,192.168.0.0/16,DIRECT
   那么192.168.1.10, 192.168.100.1均会命中这条规则

你们肯定已经注意到, 上面例子规则都被逗号分成了三段, 第一段是匹配方式, 如上所述. 第二段是匹配的内容, 第三段就是现在要讲的, 规则命中后Postern所采取的行为, 一共有五种:

1. **直连** – 对命中规则的数据请求, 不加任何处理直接转发到目的地址
2. **通过代理连接** – 对命中规则的这些请求, 使其通过代理
3. **屏蔽** – 对命中规则的这些请求全部拒绝, 丢弃
4. **智能选择** – 对命中规则的请求, 先采取直连的方式, 如果直连失败则尝试走代理
5. **代理组** – 代理组是一组不同动作的组合, 用户可以在"配置代理组"中动态选择使用哪一种动作

对于"通过代理连接"和"智能选择"两种而言, 需要同时指定一个代理服务器.
从配置文件的写法而言, 规则的第三段指定了动作, 有三种写法:

1. **REJECT** – 代表屏蔽
2. **DIRECT**- 代表直连
3. 其他　– Postern会从配置文件的[Proxy]或是[Proxy Group]节段中寻找同名的代理或是代理组. 找到如果是代理, 则动作为通过代理连接; 找到的如果是代理组, 动作即为代理组.

1.3 规则的顺序性

配过路由表的人应该都明白规则顺序的重要性: 目标地址常常可以命中不止一条规则, 这种情况下, 处在较前位置的那条规则被使用, 而不是后面的规则. 例子:

```
[Rule]
DOMAIN-KEYWORD,google,DIRECT
DOMAIN-SUFFIX,google.com,REJECT
DOMAIN,www.google.com,Proxy
```

这个时候浏览器发起了对www.google.com的连接, 对于这个地址, 上面这三条规则都是命中的, 这个时候Postern会怎么办? 它会选择第一条规则, 即采取直连的方式对待这次访问.

1.4 UI界面上规则怎么配

规则不仅可以从配置文件导入, 还可以从用户界面中直接配置. 比如你导入了一个配置文件, 然后发现哪边要修改, 这个时候你不需要重新修改文件再次导入, Postern允许你直接在用户界面中修改.

添加规则

左侧菜单中点选"配置规则", 进入上图页面, 点选"添加规则", 如下图:

在”匹配类型”里, 选择你希望的匹配方式, 前面说过, 按照域名和IP地址分类, 一共有五种不同的匹配方式:

在”动作”里, 选择规则命中后你希望Postern采取什么行为, 前面同样说过,有五种:

如上, 如果你选的是”通过代理连接”, “智能选择”, 则需要选择一个代理:

如果你选”代理组”, 则同样需要选择一个代理组. 不赘述.
在目标地址一栏里, 填写你需要匹配的目标, 以分号隔开(**注意必须是英文输入法的分号**):

上图, 最后的规则效果是, 以google.com, twitter.com后缀的域名, 统统通过代理192.168.1.1:1080来访问. 等同于配置文件的:

```
[Proxy]
Proxy2 = https, 192.168.1.1, 1080, username, password

[Rule]
DOMAIN-SUFFIX,google.com,Proxy
DOMAIN-SUFFIX,twitter.com,Proxy
```

编辑/删除规则

这个比较简单, 点选相应的规则, 即可编辑, 如同上述. 点击删除按钮, 即可删除.

插入规则

这件事情比较重要, **值得再强调一遍, Postern的规则是由顺序性的, 先前的规则如果被命中, 则优先选择先前的规则. 所以规则有前后之分.**

在某条规则上长按, 会跳出上图的菜单, 选择”在此前新建规则”, 则在长按的规则前会插入一条新规则.选择”在此后新建规则”, 则在后面插入一条规则. 按”删除”亦可删除当前规则.

2. 代理

刚说过规则的配置需要用到代理, 那么代理怎么配置呢? 很简单, 同样先以配置文件的格式为例:

```
[Proxy]
Proxy = shadowsocks,11.22.33.44,1080,aes-256-cfb,password
Proxy2 = ssh, 22.33.44.55, 22, username, password
```

所有的代理信息以[Proxy]起头, 等号左边的是代理的名字, 规则中用到的就是这些名字. **要注意的是这些名字必须由字母,数字和下划线构成, 类似surge配置中的emoji表情和汉字不能写到代理名字里**; 右边是代理服务器的详细信息, 同样以逗号分隔成几段, 分别需要填写的是:

1. **代理类型**
目前支持的类型有
Shadowsocks
SSH
SOCKS5
HTTP CONNECT隧道

GFW.PRESS (某网友的自制协议)

2. 代理服务器地址

比如上面的11.22.33.44, 代表你的代理服务器IP地址是11.22.33.44; 这个字段也可以是域名

3. 代理服务器端口

有地址就得有端口

4. 用户名/Shadowsocks加密类型

5. 密码

再看看在用户界面下如何配置代理, 左侧菜单点选"配置代理":

出现此界面, 点击已有的代理, 可以进入代理配置页面; 点击"添加代理", 则可以添加一个新的代理服务器:

无论是添加新代理, 还是修改已有的代理, 都是在上图页面中修改服务器地址, 端口, 类型, 帐号和密码等. 对于shadowsocks代理, 还需要指定一个加密方式.

Postern支持主流的代理服务器类型:

3. 代理组

代理组存在的意义在于: 你不用修改规则, 就能够快速的修改规则中的访问方法. 这么说不具体, 举个例子, 你回家用WIFI和在外用4G想用不同的代理方案, 你的规则又特别的多, 比如有10条规则里都选了走代理, 这个时候, 回家了你得把10条规则里的代理一个个改成代理服务器A, 出了门又得一条条规则改成代理服务器B. 你不胜其烦, 于是代理组这个东西就可以起作用了: 你把这10条规则都设成代理组, 于是回家了你到"配置代理组"中把代理组改成代理A, 就等于一下子改了10条规则. 出门了也是一样. 方便你的操作.

```
[Proxy]
Proxy_WIFI= SSH,11.22.33.44,22,username,password
Proxy_4G=Shadowsocks,22.33.44.55, 8888, aes-256-cfb,password

[Proxy Group]
ProxyG = select, Proxy_WIFI, Proxy_4G

[Rule]
DOMAIN,www.google.com,ProxyG
```

在此配置之下, Postern界面的”配置代理组”中会有一项关于ProxyG的配置项, 在其中选择Proxy_WIFI, 则对www.google.com的访问使用名字Proxy_WIFI代理, 选择Proxy_4G则使用名字为Proxy_4G 的代理.

需要注意的是, Proxy_WIFI 和 Proxy_4G 必须在[Proxy]先定义好.

[Proxy Group]另外一点特性是允许REJECT和 DIRECT, 即代理组的选项不一定都是代理,也可以是”直连”或是”屏蔽”, 你需要做的是在[Proxy]节段中定义伪代理。下面是一个例子：

```
[Proxy]
Pseudo_REJECT = REJECT
Pseudo_DIRECT = DIRECT
MyProxy = https,1.2.3.4,443,username,password

[Proxy Group]
ProxyG = select, Pseudo_REJECT, Pseudo_DIRECT, MyProxy

[Rule]
DOMAIN,www.google.com,ProxyG
```

对于这个例子来说， 名为ProxyG的代理组最后的三个选项分别是：屏蔽, 直连和代理MyProxy. 那么在”配置代理组”页面中, 点击相应的代理组后, 你可以选择当前使用哪个动作来应对那些命中该代理组的规则:

值得注意的是,配置文件[Proxy Group]的写法, 每一个代理组的定义, 必须以”select”加一个逗号开头. 你觉得这个很莫名也办法, 这是为了最大限度和surge的配置文件保持兼容.

4. 导入配置

手动在用户界面里面把代理, 规则和代理组这些东西填进去是很麻烦的事情, 尤其是你的规则特别多的情况下. 所以才有了前面的那些文本配置 – 你在电脑上写好了直接往手机里一导入, 方便许多.
点选”导入代理/规则”:

你可以把你的配置文件放到手机/PAD上, 点选”导入本地设备文件”, 然后找到你的文件. 也可以填入你的配置文件URL位置, 然后点击”从URL导入”.
关于代理, 代理组和规则三种东西在规则中的写法, 前面都已经介绍过了. 现在自己写一个试试把. 或者你特别懒, 实在懒得自己写, 可以关注这个地址:
https://github.com/postern-overwal/postern-stuff
会不定期更新一些懒人配置文件, 你可以直接从这里导入. 但需要注意你导入后还得自己修改一下代理服务器信息.

5. GEOIP 支持的IP国家代号

根据国家分段IP来进行规则配置, 可以帮你实现一些有趣实用的功能. 比如Shadowsocks APP根据国内外分流量, 就可以用下面这个规则很容易的实现:

```
[Proxy]
Proxy=Shadowsocks,22.33.44.55, 8888, aes-256-cfb,password

[Rule]
GEOIP,CN,DIRECT
FINAL,Proxy
```

该规则的意义是: 对于CN, 即中国区的IP访问, 使用直连的方式; 其余的IP地址统统采用代理连接方式.
另一个例子是你很富有, 在全世界各地拥有好几个代理服务器, 于是你可以把这些不同地区的代理服务器作为访问这些地区地址的入口:

```
[Proxy]
HK_Proxy=Shadowsocks,22.33.44.55, 8888,aes-256-cfb,password
US_Proxy=SSH,1.2.3.4,22,username,password
JP_Proxy=HTTPS,2.3.4.5,1080,username,password
GB_Proxy=SOCKS5,5.6.7.8,10080,username,password

[Rules]
GEOIP,HK,HK_Proxy
GEOIP,US,US_Proxy
GEOIP,JP,JP_Proxy
GEOIP,GB,GB_Proxy
```

注意: 使用GEOIP依赖于你的DNS服务器. 如果DNS服务器返回不正确的IP, 则规则可能会失灵, 超出你的意料之外.
前面说过目前Postern支持236个国家代号的GEOIP信息. 下面是一个列表, 至于二字母代表哪些国家, 请自行到此查阅: https://zh.wikipedia.org/wiki/ISO_3166-1 , 不再一一列举.

```
ZA EG ZW LR KE GH NG TZ
MU ZM MG AO NA CI SD CM
MW GA ML BJ TD BW LY CV
RW CG UG MZ GM LS MA DZ
GN CD SZ BF SO SL NE CF
TG SS BI GQ SC SN MR DJ
RE TN YT ST GW KM ET ER
AU CN JP TH IN MY KR SG
TW HK PH VN NZ BD PK ID
NP PG TK KH MO MV AF NC
FJ MN WF MM LA LK BN AE
NR NL GU VU BT WS FM PF
TL TO GB MP TR US NU SB
KI PW NF BS BZ VG CA MH
FR IR SE AS KP NO TV IO
CK KY PR BB VC JM BM DE
TC VI DM AG PM MF GD AI
MQ GP CZ FI CH IT BE BL
LC KN MS ES LU AT IL IE
DO MX AR TT CO VE BO BR
CR CL UY PY CW HN PA SV
SX PE EC GY GT NI BQ AW
```

HT CU GF SR EU RU KZ PT
GR SA DK SY UA CY IQ RO
LB GE AZ PS LT OM RS IS
HU BG SI MD MK EE LI HR
PL BA LV JO KG IM AM YE
BY GI SK MT QA AL JE SM
KW ME TJ UZ BH GL VA FO
GG MC AD TM