本文整理自官方文档：[《Surge 官方中文指引：理解 Surge 原理 - 章节 4 转发，代理和规则系统》](https://links.jianshu.com/go?to=https://manual.nssurge.com/book/understanding-surge/cn/%23%E8%BD%AC%E5%8F%91%E4%BB%A3%E7%90%86%E5%92%8C%E8%A7%84%E5%88%99%E7%B3%BB%E7%BB%9F" \t "https://www.jianshu.com/p/_blank)

本文旨在介绍清楚概念，所以只描述常用只要功能，更多细节请参考官方文档

### **一、出站模式**

被 Surge 拦截的请求在处理完毕后将被转发。

如果 Surge 的出站模式设置为****直接连接****，那么该请求将被****直接发往目标服务器****；

如果出站模式设置为****全局代理****，那么将****转发给指定的代理服务器****；

当出站模式设置被设置为****规则判定****时，将****根据配置的规则决定转发策略****。

### **二、规则-策略系统概述**

规则系统中有两个基本概念：****策略****和****规则****

1、策略：描述了 Surge 进行转发的方式，有三种类别：

* 内置策略：DIRECT、REJECT、REJECT-TINYGIF、REJECT-DROP
* 代理策略：每个策略对应一个代理服务
* 策略组：根据一定的规则从子策略中选择一个最终策略。

2、规则：规则由四个部分组成：类型、条件、策略和参数。当条件满足时，该规则匹配，使用该规则指定的策略。

### **三、策略**

#### **1、内置策略**

内置策略由 Surge 提供，不随配置而变化：

* DIRECT：将该请求直接发往目标服务器
* REJECT：拒绝该请求，当连接类型为 HTTP 时，会返回一个错误页面。（该行为可被 show-error-page-for-reject 参数控制）
* REJECT-TINYGIF：拒绝该请求，当连接类型为 HTTP 时，返回一个 1px 的 GIF 图片响应。若为其他类型连接则直接断开。该策略主要用于 Web 广告屏蔽。
* REJECT-DROP：拒绝该请求，与 REJECT 不同的是，该策略将静默抛弃请求。因为部分程序有着十分暴力的重试逻辑，连接失败后会立刻进行重试，导致请求风暴。

由于操作系统对用户空间程序（user-space program）的 socket 并没有提供抛弃的操作，Surge 静默抛弃的实现方式是将该 socket 闲置一段时间后再关闭。

同时，如果发往某主机名的请求短时间内大量触发 REJECT/REJECT-TINYGIF 策略（当前版本的阈值为 30 秒内 10 次），为了避免产生大量资源浪费，Surge 将自动升级策略为 REJECT-DROP 策略。

#### **2、代理策略**

代理策略由用户自己定义，每个策略描述了一个代理服务，当使用该策略时即为通过该代理服务转发请求。

一个简单的代理策略定义行如下：

ProxyA = http, 11.22.33.44, 8080, username=user, password=pass

其中，ProxyA 为策略名，供规则和策略组所使用。第一个参数为代理协议类型，目前 Surge 支持的代理协议类型有：

* HTTP
* HTTPS
* SOCKS5
* SOCKS5-TLS
* Shadowsocks
* Snell
* VMess
* Trojan

另外还有两个特殊类型：

* external
* direct

第二个参数为代理服务器主机名，第三个参数为代理服务器端口号，后续为 key=value 的参数表，根据协议类型不同需要提供不同的参数。

##### **2.1、direct 类型（仅限 Surge Mac）**

这是一个特别的类型，严格来说并不是一个代理，用于强制使用某一个网卡进行请求。

PolicyName = direct, interface=en2, allow-other-interface=false

##### **2.2、external 类型（仅限 Surge Mac）**

external 类型策略可以让 Surge 与其他代理客户端（如：SSR、Brook）更方便的协同工作。

该功能****目前只能通过直接编辑配置****实现，策略定义行为：

External = external, exec = “/usr/local/bin/local”, args = “-c”, args = “/usr/local/etc/config.json”, local-port = 1080, addresses = 11.22.33.44

其中 args 和 addresses 参数为选填，其他必填。args 和 addresses 字段可以反复使用进行追加。

当使用到该策略时 Surge 会进行以下工作：

（1）使用 exec 和 args 参数启动该外部程序，之后向 SOCKS5 127.0.0.1:[local-port] 转发请求。

（2）如果外部进程被终止，当再次使用该策略时会自动进行重启。

（3）Surge 会在启动增强模式时自动将 addresses 参数中的地址排除在 VIF 路由表外。（请在该字段填写使用的代理服务器 IP 地址）

（4）当由 Surge 启动的外部进程的请求被 Surge VIF 处理时，永远使用 DIRECT 策略。（为了应对像 obfs-local 这样的插件请求问题，外部进程的子进程也会被同样处理）

（5）Surge 退出时会自动关闭所有外部进程，增强模式关闭时会自动清理加入的路由表。

上述 3 和 4 的功能是有重叠的，请尽量使用 addresses 声明使用到的地址以排除 TUN 处理，这样可以减少系统开销，4 的功能是一重额外保护。

##### **2.3、策略组**

* select 策略组：通过 UI 菜单选择一个策略。
* url-test 策略组：选择延迟最低的策略。
* fallback 策略组：选择可用的策略中，最靠前的策略。
* ssid 策略组：根据当前的 Wi-Fi SSID 选择一个策略。
* load-balance 策略组：随机使用一个子策略，可选进行可用性检查。

### **四、规则**

* 域名规则
* IP 地址规则
* HTTP 相关规则
* 其他规则
* 规则集

RULE-SET 规则集可以将****多个子规则****放在****一个单独的文件中****，便于分享和复用。但是规则集中的规则****不可以指定策略****，整个规则集指向一个同一个策略。

另外 Surge 自带了 SYSTEM 和 LAN 两个规则集，规则集包含的具体子规则会随 Surge 更新而有所调整。注意 LAN 规则集会触发 DNS 解析。

* 逻辑规则

可通过 AND，OR，NOT 运算对所有规则类型进行组合使用。如

AND,((PROCESS-NAME,Google Chrome),(PROTOCOL,UDP)),REJECT

可以拦截 Chrome 发出的 UDP 数据包。

（完）