Tor 项目扩展应用

Mod233

July 4, 2018

Abstract

对于 Tor 的研究在大四上持续了半学期，可以说收获颇丰。Tor 作为匿名网络的鼻祖，是我为我未来工作生活，提供匿名安全的有效工具。这里我会就 Tor 配置、Tor 爬虫、Tor 木马等方面展开。

Contents

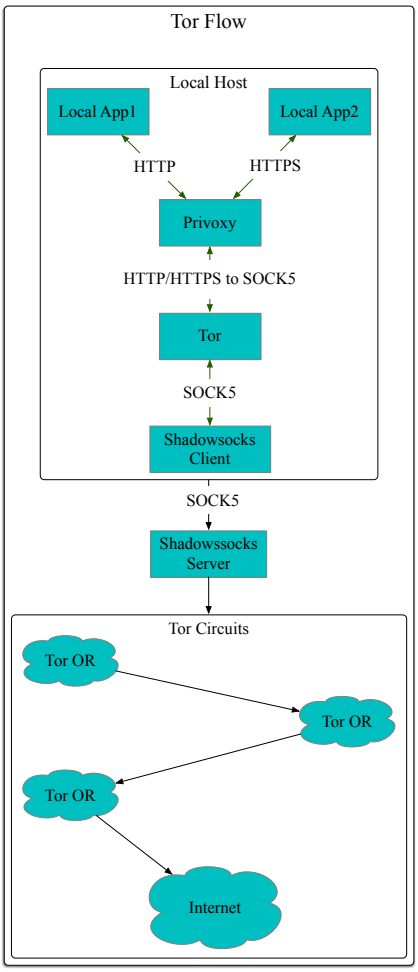
1 Tor 配置

Tor 环境配置，可以使用简单的 Tor 浏览器，或者 CLI 命令行界面。我这里主要以 CLI 展开，因为主要是为了后面章节导入爬虫、木马等等流量做

铺垫。

如果不使用 Tor 浏览器，整个流程的配置，相对复杂。因为大陆会屏蔽 Tor 的流量，在 Tor Browser 中集成了 meek-amazon 和 meek-azure 来绕过检测。但随着技术的慢慢进步，meek 作为跳板肯定不是长久之计，所以这里介绍结合 Shadowsocks、Tor、Privoxy 来实现匿名服务的系统。

基本网络拓扑如下:

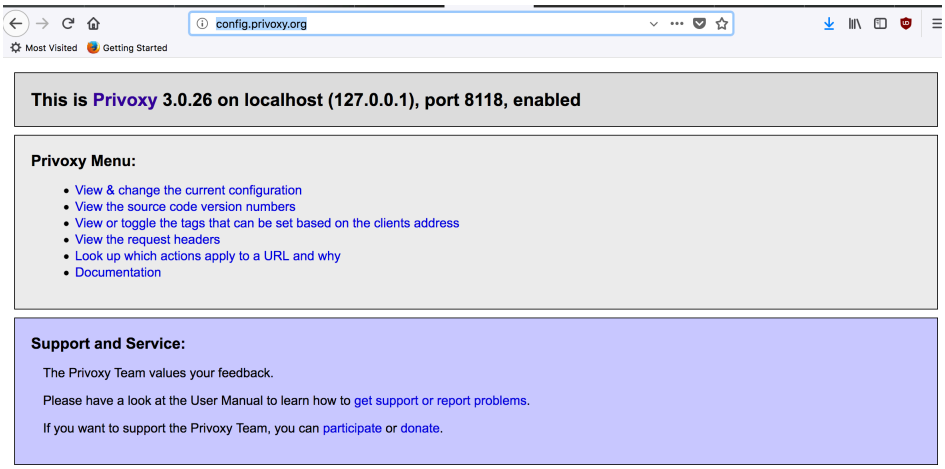


从拓扑中，可以看出，主要是 Privoxy 实现 HTTP/HTTPS 到 SOCK5 的转换，然后又 Tor 封装一层后，交给 Shadowsocks Client，然后由 Shadowsocks Client 将数据包传给处于境外端口的 Shadowsocks Server，这个 Server 节点能访问 Tor 的节点 IP 并且不会被拦截，流量就成功接入了 Tor 网络中。下面逐个介绍 Privoxy,Tor,Shadowsocks 的环境配置情况。

首先是 Privoxy：

```
  ~ brew install privoxy
  ~ cd /usr/local/etc/privoxy
  privoxy ls
config            default.filter   templates        user.
   action
default.action    match-all.action trust            user.
   filter
  privoxy cat config
...SNIP...
listen-address  127.0.0.1:8118
forward-socks5 / 127.0.0.1:9050
forward-socks5t / 127.0.0.1:9050     #socks5-tor
forward-socks   / 127.0.0.1:9050
...SNIP...
  privoxy sudo /Applications/Privoxy/startPrivoxy.sh
  privoxy sudo /Applications/Privoxy/stopPrivoxy.sh
```

Privoxy 中，listen-address，指名了监听的 ip 及 port，forward 指明了转发规则。完成了 privoxy 的配置后，可以登陆 *http://config.privoxy.org/*进行测试：



接下来需要下载 Tor 源码，并编译安装，源代码从官网（https://www.torproject.org/download/download.html.en）下载即可，一般类 Unix 系统都会有对用的包管理器提供快速的安装：

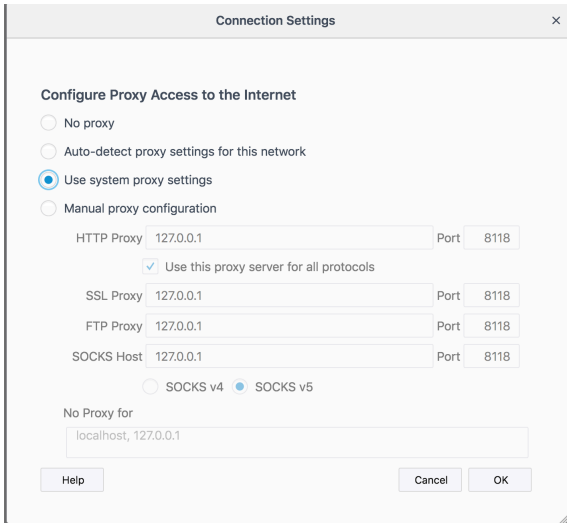
```
  CodeTor—0.3.3.7 brew install tor
...SNIP...
To have launchd start tor now and restart at login:
  brew services start tor
Or, if you don't want/need a background service you can
    just run:
  tor
==> Summary
  /usr/local/Cellar/tor/0.3.3.7: 21 files, 11.2MB
...SNIP...
  ~ cd /usr/local/etc/tor
  tor ls
torrc
  tor cat torrc
...SNIP...
Socks5Proxy 127.0.0.1:1077
SocksPort 9050
ControlPort 9051
  tor —f /usr/local/etc/tor/torrc
```

之后需要到 */usr/local/tor/* 文件夹下，修改配置文件，改成如上的情况即可。之后利用启动即可。

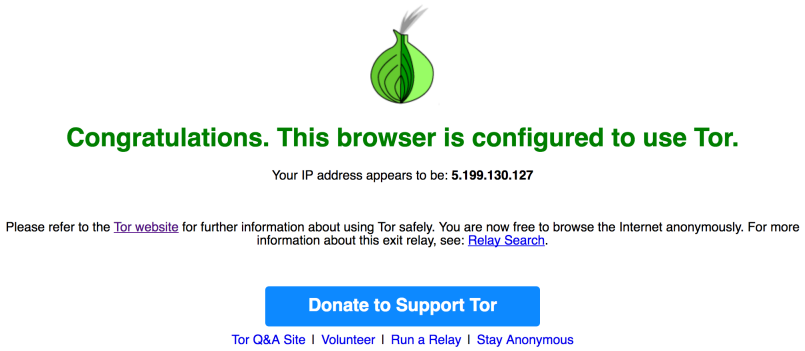
配置 shadowsocks 环境，网上已经有非常多教程了，而且 shadowsocks 在整个系统中相当于流量转发的功能，这里不赘述了。想要测试 shadowssocks 是否成功，可以尝试下面的命令，如果返回 ss-server 的地址，则说明配置成功：

```
  ~ curl ——socks5 127.0.0.1:1077 http://httpbin.org/ip
{"origin":"95.163.200.165"}
```

接下来是浏览器的配置，如果自己是 firefox 浏览器，在浏览器 *preference->setting* 配置对应的代理服务即可：



Tor 提供了一个测试网站，供用户测试流量是否经过了 Tor 网络，登陆 *https://check.torproject.org/* 访问即可：



2 Tor 认证原理

仔细想想，Tor 有很多值得自己推敲的问题。比如为什么 Tor 选择 Socks 协议，为什么 Tor 能够防追踪。

3 Tor 爬虫

Tor 爬虫有两种理解，一种是指利用 Tor 特性中 IP 动态调变的优势，以不同的 IP 动态爬取网页信息，而不会因为单个 IP 频发访问遭到屏蔽；另一种是通过 Tor 进入暗网，爬取暗网中的数据。

4 玩转数学公式

b

5 绘制图表

6 幻灯片演示

7 从错误中救赎

8 Latex 无极限