TOR安装教程-MacOS Mojave

MacOS系统安装tor教程。

ShadowsocksX-NG-R8安装

Tor安装

- Tor原理：

  Tor每发出一次请求经过Tor网络的3个节点。

  其中有2种服务器角色：中继服务器和目录服务器。中继服务器：负责数据包的转发；目录服务器：保存中继服务器的信息(ip地址，公钥等)。

  Tor客户端先与目录服务器通信获得全球活跃中继节点信息，然后再随机选择三个节点（hop）组成circuit （电路），用户流量跳跃这三个节点（hop）之后最终到达目标网站服务器。

  Tor客户端与目标服务器的通信分为两个部分：建立通信链路和在通信链路上发送数据包。

  一、建立通信链路的过程：

  1. 客户端与目录服务器建立链接，并从目录服务器中选取一个时延最低的服务器作为第一个中继服务器/OR1；
  2. 客户端向OR1发送一个请求建链请求，OR1验证完客户端的合法性后生成一对密钥（公钥pubkey_OR1_Client、私钥prikey_OR1_Client）,然后将公钥pubkey_OR1_Client发回给客户端（至此，客户端成功的建立了其与OR1的通信链路）；
  3. 客户端又从目录服务器中选择一个时延最低的中继服务器OR2，并向OR1发送一个数据包：使用pubkey_OR1_Client加密OR2的地址；
  4. OR1收到数据包后使用prikey_OR1_Client解开数据包，发现是一个让其自身与另外一个服务器OR2建立链接的请求，那么OR1重复步骤2与OR2建立链接，并将OR2返回的OR1与OR2链路的公钥pubkey_OR1_OR2返回给客户端；
  5. 客户端重复步骤3、4，建立OR2与OR3之间的通信链路，并接收到OR2与OR3之间链路的公钥pubkey_OR2_OR3；
  6. 至此，客户端与3个中继服务器之间的链路/circuit已经成功建立，客户端拥有3把公钥：pubkey_Client_OR1、pubkey_OR1_OR2、pubkey_OR2_OR3。

  二、发送数据包：

  1. 客户端将要发送的数据（data）经过3层加密包裹：*第一层：使用pubkey_OR2_OR3加密data：pubkey_OR2_OR3(data)；*第二层：使用pubkey_OR1_OR2加密第一层加密后的数据：pubkey_OR1_OR2(pubkey_OR2_OR3(data))；*第三层：使用pubkey_Client_OR1加密第二层机密后的数据：pubkey_Client_OR1(pubkey_OR1_OR2(pubkey_OR2_OR3(data)))；
  2. OR1收到客户端发来的数据后使用其与Client链路的私钥prikey_Client_OR1解开数据包，发现数据包是发往OR2的，那么OR1就将解开后的数据包发送给OR2；
  3. OR2收到OR1发来的数据包重复OR1的步骤：将接收的数据包解开发往OR3；
  4. OR3收到数据包后，使用prikey_OR2_OR3解开数据包，这个时候的数据包是客户端要发往目的服务器的真实数据包data。此时，OR3就将data路由给目标服务器。
- Tor安装：

```
brew install tor
```

配置：

```
cd /usr/local/etc/tor
cp torrc.sample torrc

vim torrc
```

在文件末尾添加：Socks5Proxy 127.0.0.1:1086

```
tor --hash-password mypassword # 生成密码
```

生成结果类似于：

```
HashedControlPassword
16:F52F93044E39564D60E66BB2C3A680D3DE1F1DD4477F4F7CC761ECCC56
```

在文件末尾添加：

```
ControlPort 9051
HashedControlPassword
16:F52F93044E39564D60E66BB2C3A680D3DE1F1DD4477F4F7CC761ECCC56
CookieAuthentication 1
```

运行tor：

```
tor
```

终端输出类似于：

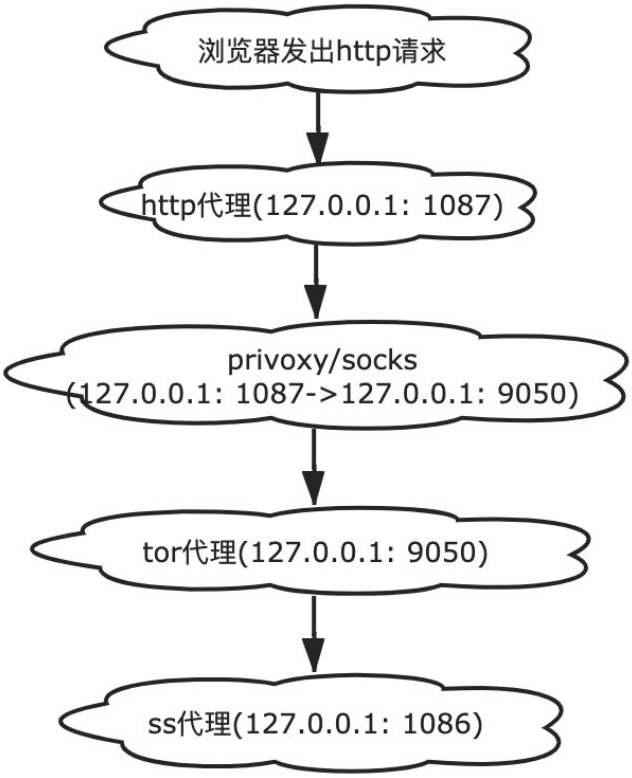
```
Apr 02 19:39:58.961 [notice] Tor 0.3.5.8 running on Darwin with Libevent
2.1.8-stable, OpenSSL 1.0.2r, Zlib 1.2.11, Liblzma N/A, and Libzstd N/A.
Apr 02 19:39:58.961 [notice] Tor can't help you if you use it wrong! Learn
how to be safe at https://www.torproject.org/download/download#warning
Apr 02 19:39:58.961 [notice] Read configuration file
"/usr/local/etc/tor/torrc".
Apr 02 19:39:58.969 [notice] Opening Socks listener on 127.0.0.1:9050
Apr 02 19:39:58.970 [notice] Opened Socks listener on 127.0.0.1:9050
Apr 02 19:39:58.970 [notice] Opening Control listener on 127.0.0.1:9051
Apr 02 19:39:58.970 [notice] Opened Control listener on 127.0.0.1:9051
```

浏览器配置（chrome）：

在[SwitchyOmega]的[options]中设置代理：SOCKS5，127.0.0.1，9050。

输入https://check.torproject.org/?lang=zh_CN测试是否连接到Tor网络。

ss代理原理：


浏览器发出http请求
http代理(127.0.0.1: 1087)
privoxy/socks
(127.0.0.1: 1087->127.0.0.1: 9050)
tor代理(127.0.0.1: 9050)
ss代理(127.0.0.1: 1086)