前言：我的互联网自由宣言

至于什么叫做互联网自由，目前尚没有一个流行的定义，不过却有人列出了互联网自由的 5 个基本原则，即自由表达、快速上网、不用翻墙、保护创新以及保障隐私。

作为一个生活在有中国特色的社会主义国家的网民，我 100% 赞成这 5 个原则并且觉得互联网自由是 100% 重要的，因为如果互联网没有自由，那么你就可能因为在网上说了一句话而被劳教，所在地区霎时间长时间断网，不翻墙就无法访问 Facebook、Twitter、YouTube 以及其他多个资本主义的网站，自己的网站会因为某篇文章而导致服务器被封号，甚至连下载 A 片都会被警察破门而入，类似的荒唐事不胜枚举。

听起来很恐怖，是吧？但是上面提到的事都曾活生生地出现在中国互联网上，而如果中国互联网没有改善，类似的事情将会发生在你我身上 —— 而且已经发生在我的身上。2009 年，精品博客发表了一篇叫做《操 GFW 10 大简易招式》的文章，几个月之后，网站的服务器因为这篇文章被封号；后来，我把博客的服务器搬到国外，继续介绍翻墙工具和方法，结果导致整个博客被墙，至今没有解封。

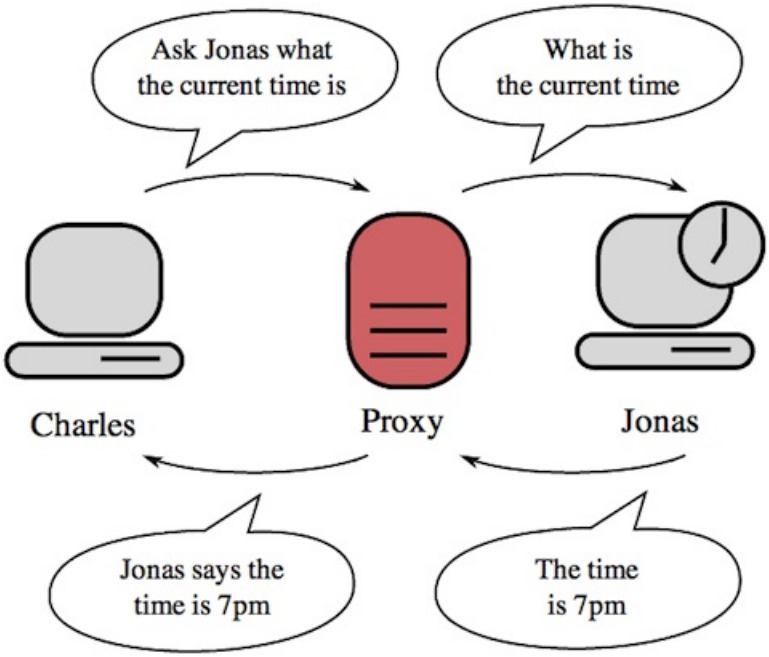
如果没有墙，那我也就没有必要翻墙，更没有必要去折腾翻墙工具，可惜没有如果，所以我就只好翻墙，不断地尝试各种翻墙工具，并且用中文分享到精品博客以及用英文分享到 Free Nuts 博客。

到目前为止，我已经测试并介绍了 100 个免费翻墙工具，其中包括 VPN、Proxy、SSH、等等，当然，随着时间的推移，这些工具里面有些已经不能翻墙了，不过值得庆幸的是，一直都会有新的翻墙工具出现，而我也将继续测试并介绍它们，直到互联网不再有墙。

第一章：100 个免费在线代理

在众多翻墙工具里面，在线代理（web proxy）是最简单的了，只要打开浏览器就可以用，不需要安装任何软件，也不要做任何设置。

在线代理也是所有的免费翻墙工具里面最多的，其中比较强大的有以下 100 个：



1. 007007007.eu
2. 1234abcd.net
3. 123proxy.eu
4. 1987proxy.eu
5. 2fastproxy.tk
6. Aaaproxy.eu
7. Anonboard.cz
8. Anonymouscitizens.info
9. Apenglish.info
10. Apliterature.info
11. Auto-aufladen.de
12. Avoidfiltering.com
13. Awesomeproxy.eu
14. Best-free-proxy.eu
15. Bestproxyes.eu
16. Boersen-insider.de
17. C-proxy.eu
18. Cloakpoint.com
19. Devilproxy.eu
20. Dxyh.com
21. Doobit.info
22. Enproxy.eu
23. Filtersneak.com
24. Free007proxy.eu
25. Free-web-proxy.de
26. Freeunlocker.com
27. Fubrus.com
28. Futureproxy.eu
29. G09.info

30. Goodproxy.eu
31. Hideproxy.eu
32. Hideweb.org
33. Homeproxy.net
34. Icthero.com
35. Ipcamouflage.com
36. Ipchanging.com
37. Isityet.net
38. Itsmyzone.info
39. Iwebproxy.net
40. K12history.net
41. Kixmax.com
42. Lolproxy.eu
43. Lopana.com
44. Longbuluo.info
45. Loveyd.info
46. Luispro.com
47. Ltunnel.net
48. Mancos.de
49. Maptao.info
50. Microxy.com
51. Meut.info
52. Netbypassthree.info
53. Netsneak.com
54. Olympicproxy.net
55. Ondrej.me
56. P-proxy.eu
57. Pazou.info
58. Polysolve.com
59. Pproxy.eu
60. Profeast.info
61. Proxay.co.uk
62. Proxeh.com
63. Proxy-free.org
64. Proxy000.eu
65. Proxy007.eu
66. Proxy4.eaak.tk
67. Proxy4you.eu
68. Proxybutton.com
69. Proxyforfree.eu
70. Proxydot.com
71. Proxydot.eu
72. Proxydot.info
73. Proxydot.org
74. Proxyn.se
75. Proxytools.info
76. Q-tunnel.com
77. Rockvideo.cz
78. Safeforwork.net
79. Secure-street.com
80. Securewebproxy.net
81. Sleekseed.com
82. Snowcz.eu
83. Spem.at
84. Surfnewip.com
85. Surfinweb.tk
86. T-tunnel.net
87. Tblocker.info
88. Tellmenot.org
89. Usawebproxy.net

90. Unblock-internet.ws
91. Unblock-websense.com
92. Ultraproxy.eu
93. Usfreeproxy.com
94. Usproxyserver.info
95. Vtunnel.tv
96. Vvwa.com
97. Websurf.in
98. Workproxy.net
99. Yellowproxy.net
100. Yourinternetproxy.info

要使用以上任意一个在线代理，只需要点击它的链接，接着输入被墙网站的 URL 或者域名，然后按下“输入”键或者点击输入框后面的“Go”、“Surf”、“Browse”之类的按钮，你就可以翻墙了。

顺便一提，以上 100 个在线代理网站在这篇文章发表的时候，都是没有被墙的，而且都可以用来观看 YouTube 网站上的视频。

但是在线代理有一个致命的不足，那就是弹窗广告太多——这点非常令人讨厌，所以我一般只用在线代理去访问其他被墙的翻墙工具的网站（例如自由门）或者偶尔匿名浏览某个网站（例如 YouTube）。

第二章:7 大免费客户端代理

虽然都是代理，客户端代理和在线代理的区别是很大很明显的。

下面就从广告、原理、安全性、易用性和适用范围等 5 个角度对客户端代理和在线代理进行比较：

1、广告

在线代理基本上都是挂满了广告的，而客户端代理则没有广告，或者只是宣传自己的网站。

2、原理

在线代理大多数都是通过 Glype 脚本建立的，而客户端代理的脚本则各不相同，并且相对比较复杂。

3、安全

在线代理的域名和 IP 地址如果被封，那么就无法使用了，而客户端代理通常有多个服务器，不容易被封。

4、易用性

在线代理只需要打开它的网页就可以用，而客户端代理则还需要下载、安装、或者甚至加以设置（例如配置浏览器代理地址）之后才能够使用。

5、适用范围

在线代理几乎都只适用于个人电脑浏览器，对手机和平板电脑的浏览器并不友好。虽然客户端代理有些也仅仅适用于个人电脑，有些则同时也为手机和平板电脑提供不同的版本。

尽管存在不同，但是不管是客户端还是在线版，能够翻墙的代理都是好代理。另外，由于客户端代理的网站几乎全部都被墙了，所以，我们可以通过一些没有被墙的在线代理去访问客户端代理的网站并下载它们。

7 大免费客户端代理

在众多的免费客户端代理里面，以下 7 个是最好的也就最耐用的：

1、**自由门**

2、**无界**

3、**Tor**

4、**GappProxy**

5、**Goagent**

6、**Hyk-proxy**

7、**Snova 6**

第一节：自由门

作为一个免费的代理软件，自由门以简单易用和不断更新而备受欢迎。

基本上，只要能够下载到自由门，你就可以翻墙了，具体步骤如下：

一、下载自由门

由于动态网被墙，所以需要先使用手上的 VPN、SSH、代理或者其他任意的翻墙工具访问该网站的免费软件下载页面，然后选择自己喜欢的版本下载。

目前，自由门有三个版本，即专页版、专家版和限制版，每个版本在界面或默认允许访问的网站上有所不一样，但用法是几乎一样的。以下就以最受欢迎的专业版为例，介绍如何使用自由门翻墙。

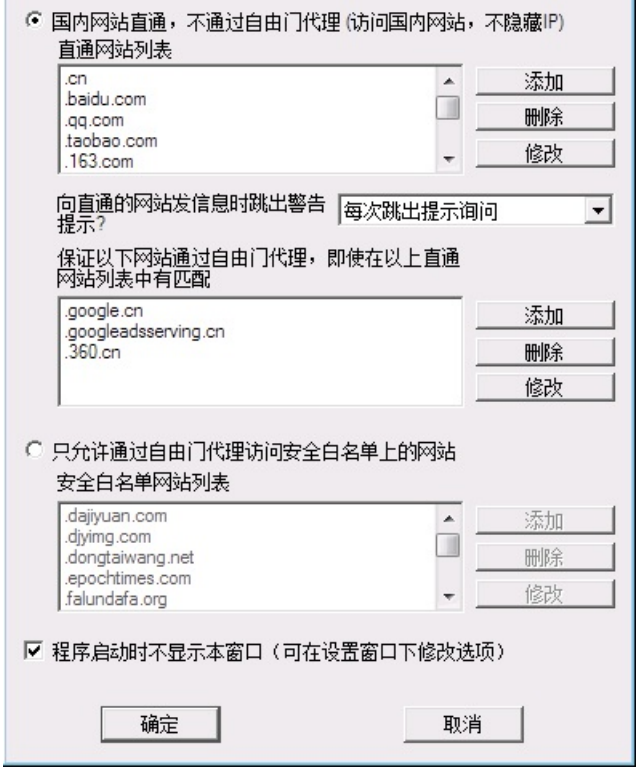
二、启用自由门

下载完了之后，双击自由门应用程序，然后一直点击所有弹窗的左边第一个按钮就可以了，以下是 Win 7 系统下的弹窗：

1. 运行

Windows 应该为自由门开绿灯才对，弄个安全警告就妨碍自由了。

2、代理控制

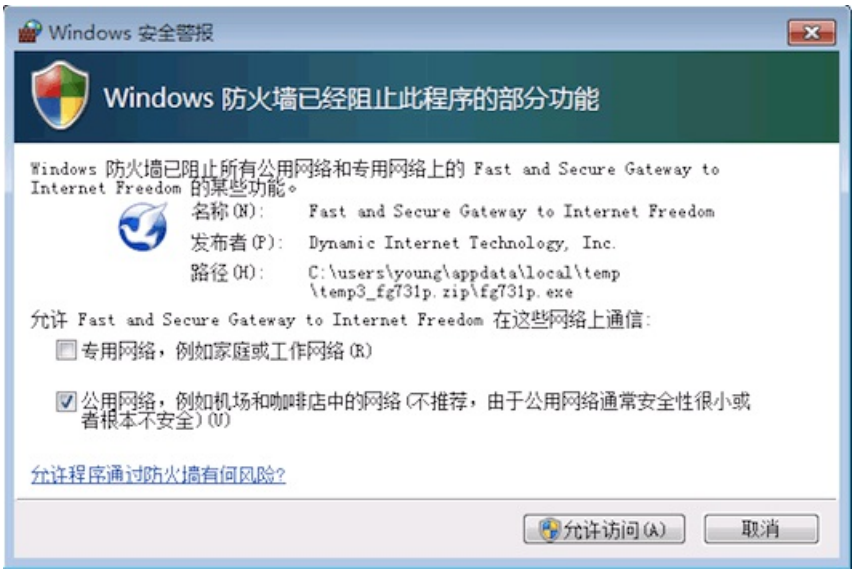


自由门对国内不用翻墙的那些网站是非常不友好的，要么不能访问，要么可以访问但是只能看到部分内容，所以，之前要访问国内网站，就需要先退出自由门，但是现在不用了，因为你可以把这些网站直接拉进黑名单。

除此之外，你也可以只允许自由门访问某些个国外网站，只要把它们拉进白名单就好了。

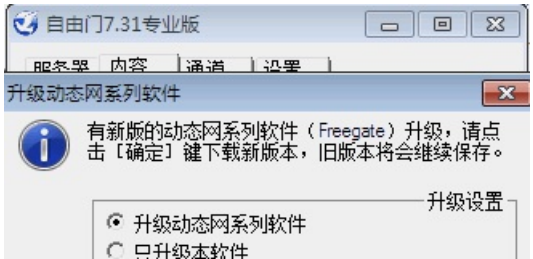
由于国外网站大都被墙，而默认情况下百度、QQ、淘宝等网站已经被拉进了黑名单，所以，直接点击“确定”按钮就可以了。

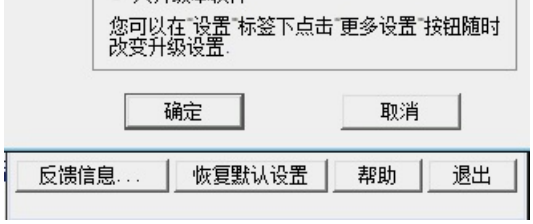
3、防火墙



只有允许自由门访问才能通向自由。

4、软件升级



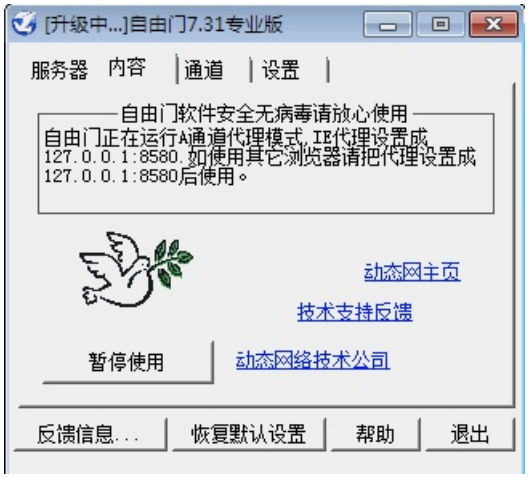


自由门有自动升级的功能，除了正在运行的版本，还可以升级动网通，你可以选择只升级自由门或者全部升级。

5、下载升级软件

如果允许自动升级，那么就需要设置一个下载目录，你可以使用自由门默认的路径，或者另外指定一个。

6、连接翻墙

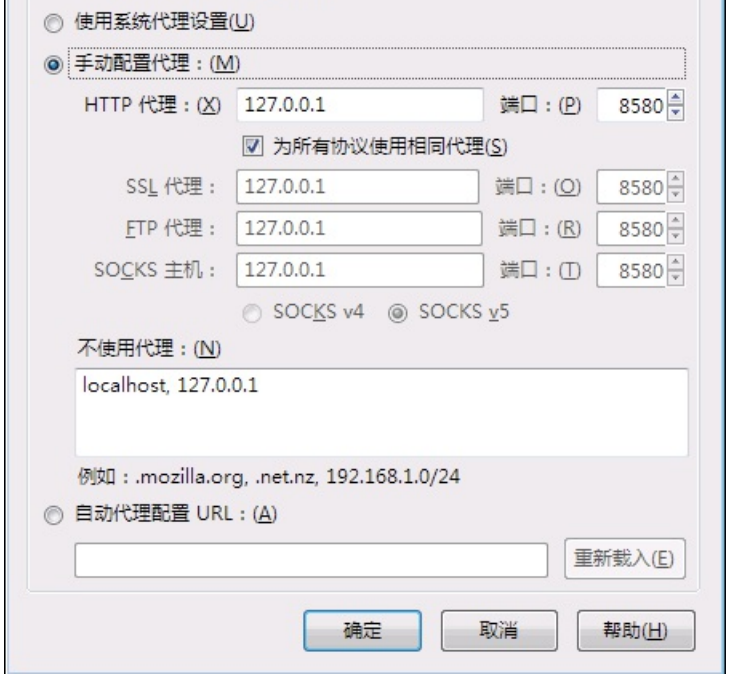


如果连接成功，你就可以通过自由门翻墙了。

三、设置浏览器

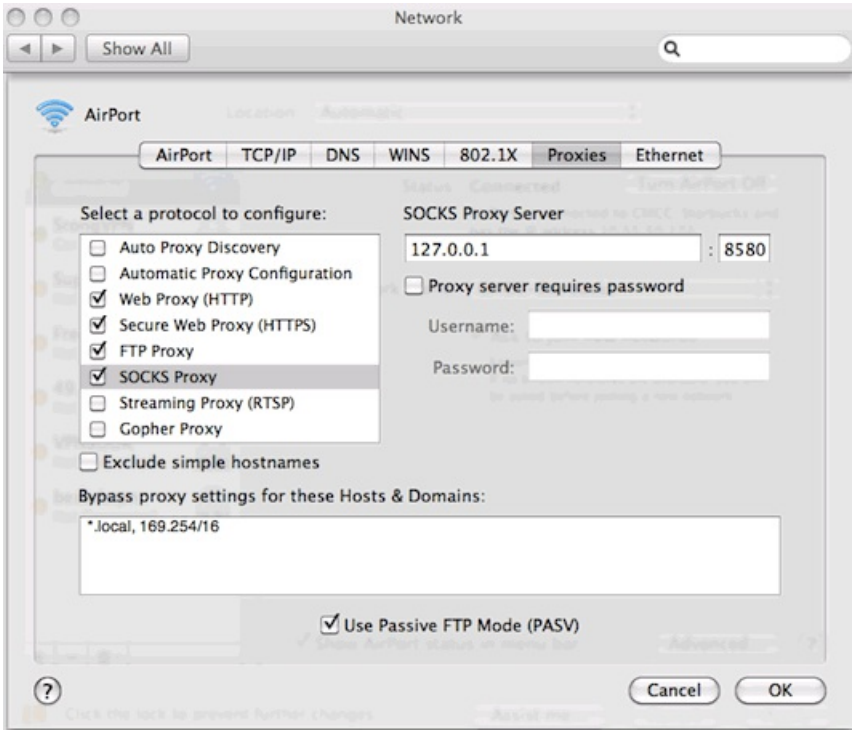
如果你使用的是 IE 浏览器，自由门连接成功之后就可以直接翻墙了；而如果你使用的是 Chrome、Firefox、Safari 或者其他浏览器，则还需要把浏览器的代理设置为“127.0.0.1：8580”。

以 Firefox 为例，你可以通过“选项 –> 高级 –> 网络”找到“配置 Firefox 如何连接至因特网”一栏，接着点击旁边的“设置”按钮，其次勾选“手动配置代理”，再在 HTTP 代理一栏填入“127.0.0.1”，端口填“8580”，如下图所示：



然后勾选“为所有协议使用相同代理”，点击“确定”按钮之后，你就可以在 Firefox 浏览器上使用自由门翻墙了。

Opera 的代理设置界面跟 Firefox 的几乎一样，而 Chrome 和 Safari 的代理设置界面如下：



上图有多个代理选项，我们只需要填 HTTP、HTTPS、FTP 和 SOCKS 这 4 项就可以了。

以上的自由门使用方法是针对 Windows 系统的，而对于 Mac 和 Linux 系统，你可以参考动态网的常见问题页面。

另外，除了电脑版本，自由门还有手机版本，其中包括安卓手机版，Java 手机版和 WM 手机版。

第二节：无界

无界，全称是无界浏览，不是浏览器，而是一个可以在浏览器上翻墙的类似于自由门的工具。

虽然自由门已经很简单，但是无界更加简单，没有黑白名单的干扰，具体使用步骤如下：

1、下载无界

由于无界浏览网站被墙，所以需要先通过手上的 VPN、SSH、代理或者其他任意的翻墙工具访问该网站的下载页面，然后下载最新的版本。

每个版本又分压缩版和执行版，而所谓的压缩版，就是压缩了的执行版。

2、运行无界

如果下载的是执行版，直接打开下载文件就可以了，如果下载的是压缩版，解压之后再打开里面的 exe 文件就可以了。

虽然无界还有经典模式——即通过无界在线代理翻墙、无界分享——把用无界上网的电脑变成代理服务器以及多种链接方式—— U、T、P，但是这些功能没有神马好玩的，基本上只是摆设。

3、设置浏览器代理

如果你使用的是 IE 浏览器，无界连接成功之后就可以直接翻墙了；而如果你使用的是 Chrome、Firefox、Safari 或者其他浏览器，则还需要把浏览器的代理设置为“127.0.0.1：9666”。

以 Firefox 为例，你可以通过“选项 –> 高级 –> 网络”找到“配置 Firefox 如何连接至因特网”一栏，接着点击旁边的“设置”按钮，其次勾选“手动配置代理”，再把每一栏的代理设置为“127.0.0.1”＋端口“9666”，如下图所示：

其他浏览器的代理设置大同小异，可参考上图 Firefox 的。

相比自由门，无界的一个好处是没有黑白名单，也就是说你可以通过它访问国内外的网站；而一个不好的地方是不能自动更新。

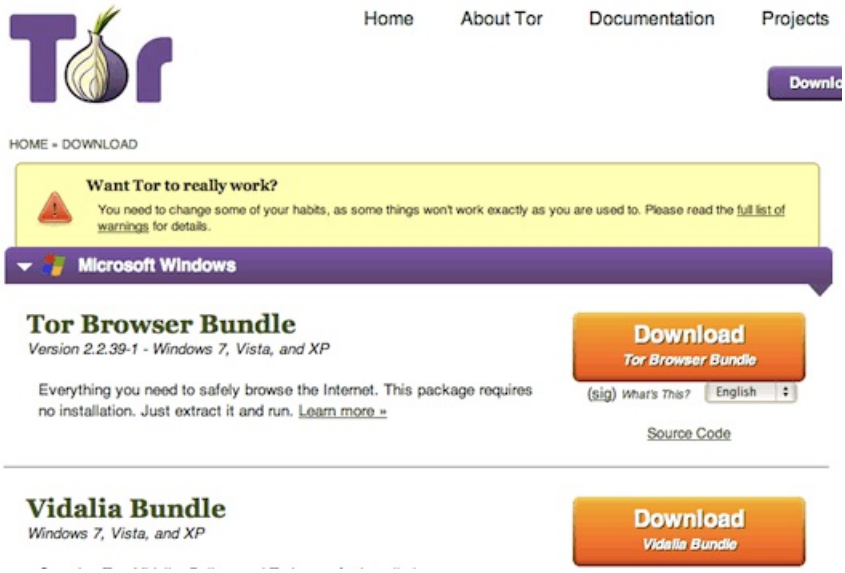
第三节：Tor

其实，我有点想把“如何戴 Tor 翻墙”改成“如何戴套翻墙”的，因为“Tor”和“套”音近，而且都有安全的功效。

但是为了准确，最后还是算了。

废话少说，以下是戴 Tor 翻墙的 4 个步骤：

1、下载 Tor

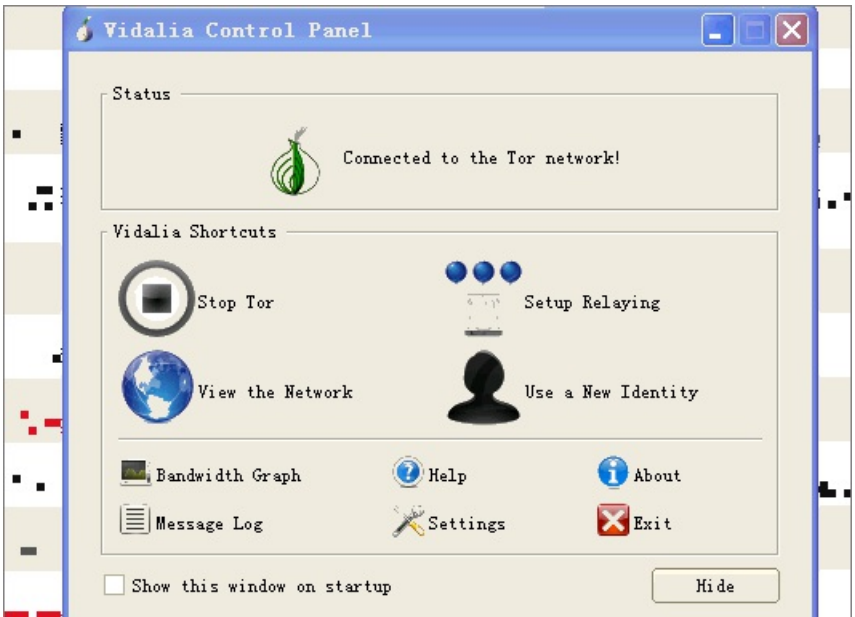


目前，Tor 支持 Windows、Mac、Linux／BSD／Unix、Android 以及 Nokia Maemo/N900 等电脑或者手机系统，每个系统有一个或者多个版本，你可以在下载页面选择自己喜欢的版本下载。

本文主要介绍适用于 Windows 和 Mac 的两个基本的最常用的版本，其中一个是自带浏览器的 Tor Browser Bundle，另外一个是不带浏览器的 Vidalia Bundle，如果选择前者，那么你就只能在 Tor 浏览器（基于 Firefox）上翻墙，而如果选择后者，那就可以在 Firefox、Chrome、Safari 等其他浏览器上翻墙。

另外，Tor Browser Bundle 在下载之前可以选择浏览器界面语言，而不管是哪个版本，其 Vidalia 控制面板的界面语言随时都可以改成法文、意大利文、日文、等等

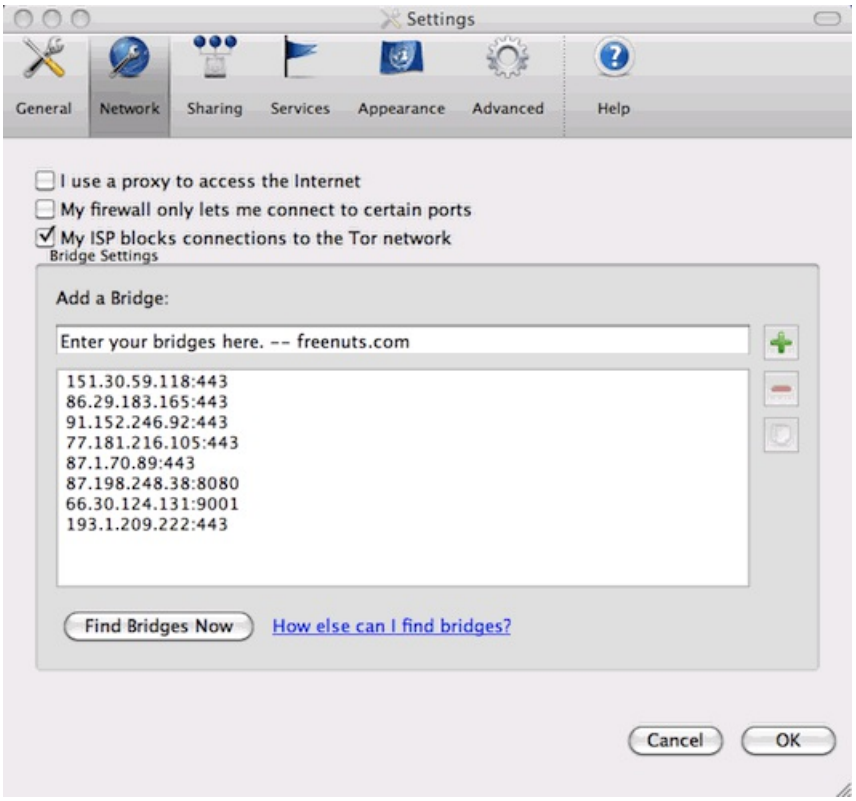
2、运行 Tor



不管是哪个版本，下载之后解压或者安装之后就可以直接运行了。

其中 Tor Browser Bundle 运行 Start Tor Browser（Windows）或者 TorBrowser (Mac)，而 Vidalia Bundle 运行 Vidalia，如果能够看到一个绿色的洋葱头，那就表明 Tor 成功运行。

3、添加网桥



如果洋葱头没有变绿，那就表明当前 Tor 所用的网络已经被墙，最常用的解决方法是添加网桥（Bridge）。具体方法是在 Vidalia 控制面板的“网络”设置页面，勾选“我的 ISP 阻挡了对 Tor 网络的连接”，然后添加“117.199.213.96:443”这样的网桥。

那么，如何获取 Tor 网桥？主要有以下两种方法：

a、网页法

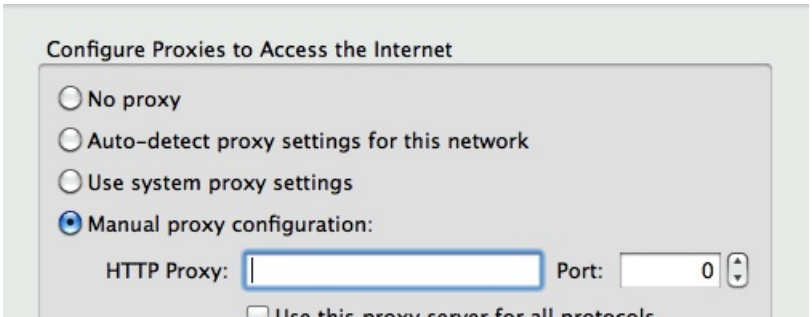
访问 Tor 官方的网桥页面，该页面会提供两三个网桥。

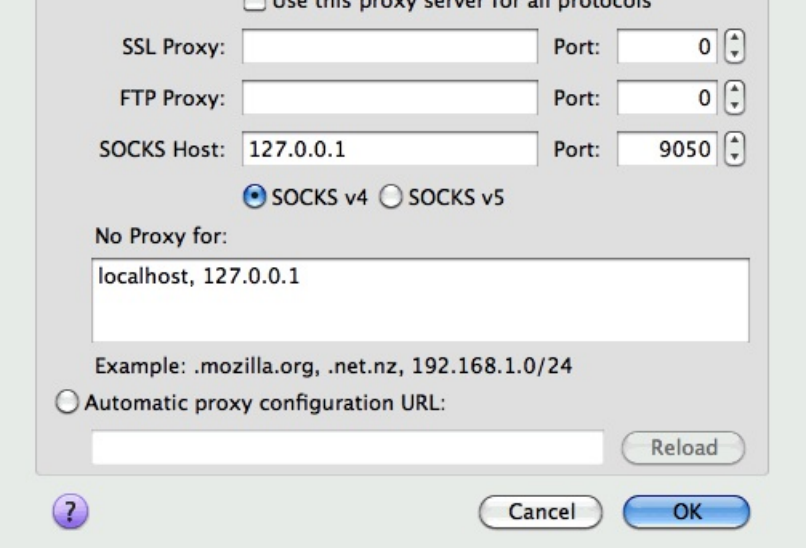
b、邮件法

通过 Gmail 邮箱发送“get bridges”信息到“bridges@torproject.org”，很快就会获得三个网桥。

另外，旧版的 Vidalia 控制面板还提供“立刻搜索网桥”功能（如上图所示），但是新版的已经没有该功能了。还有，之前 Yahoo 邮箱也可以申请网桥，现在不行了，只能用 Gmail 邮箱申请。

4、配置浏览器代理





只要洋葱头变绿，**你就可以戴** Tor **翻墙了。**

对 Tor Browser Bundle **来**讲，**可以直接并且只能够通过它自**带**的**浏览**器翻墙；而**对 Vidalia Bundle **来**讲，则**需要先把**浏览**器的** SOCKS v4 **代理**设**置**为“127.0.0.1：9050”。

以 Firefox 为**例**，**你可以通**过“选项 –> **高**级 –> **网**络”**找到**“**配置** Firefox **如何**连**接至因特网**”**一**栏，**接着点**击**旁**边**的**“设**置**”**按**钮，**其次勾**选“**手**动**配置代理**”，**再在** SOCKS **代理一**栏**填入**“127.0.0.1”，**端口填**“9050”，**并且要**选择 **SOCKS v4**，**因**为 SOCKS v5 连**接不上。**

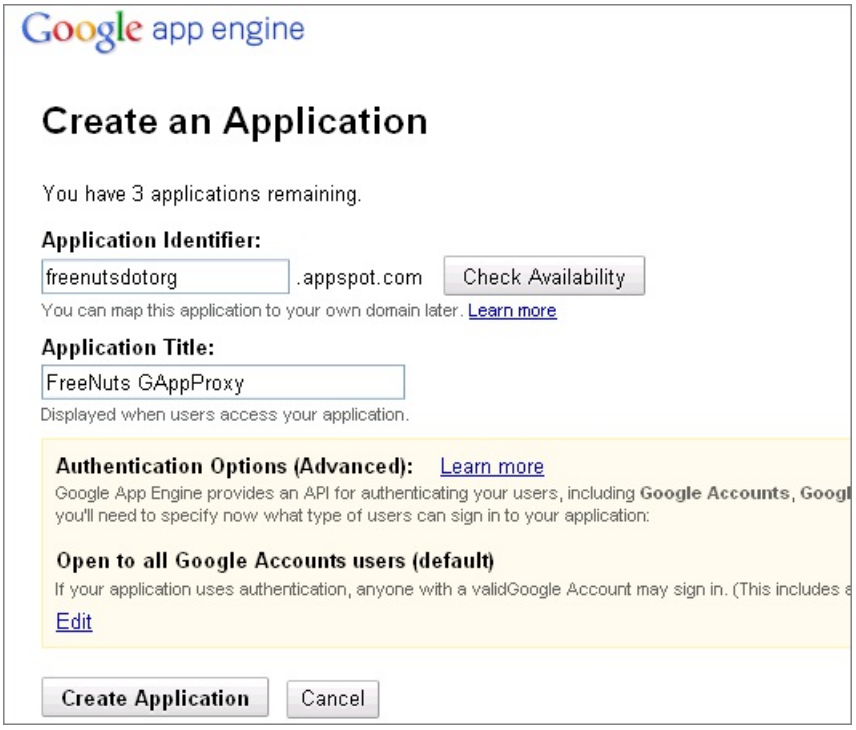
在上面介绍**的** Tor Browser Bundle **和** Vidalia Bundle 这**两个** Tor **版本之中**，**前者是最易用最安全的**，**唯一的缺点就是你只能使用它自**带**的**浏览**器翻**墙。

第四节：GappProxy

GAppProxy 自从 2010 年升级到 2.0.0 版本之后就没有再更新过，而且对 https 的支持不是很好，所以成了鸡肋。

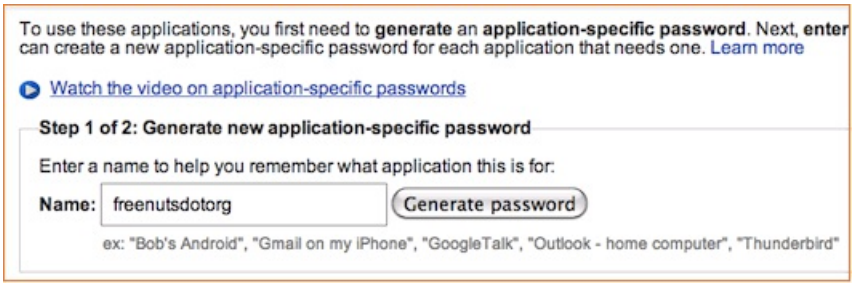
但是肚子饿的时候，鸡肋也能成为佳肴，何况现在 GAppProxy 仍然可以翻墙，所以，有备无患，以下是具体的 7 个安装和使用步骤：

1、创建一个 GAE 应用程序



登录 Google App Engine，创建一个新的应用程序（Application），并记住程序名称（ID）。

2、生成一个应用专用密码



如果 Gmail 帐户启用了两步验证，上传 GAppProxy 服务端到 GAE 时需要一个专用密码（Application-specific password），具体方法是打开 Google 帐户的安全性（Security）页面，接着点击“向应用和网站授权”（Authorizing applications and sites）旁边的“修改”（Edit）按钮，然后输入任意一个名称并点击“生成密码”（Generate password）按钮就可以了。

如果没有启用两步验证，那就可以忽略这个步骤。

3、下载 GAppProxy

在 GAppProxy 下载页面，根据不同的电脑操作系统下载不同的版本。

3.1 下载 Windows 版本

如果要在 Windows 上部署和使用 GAppProxy，则需要下载以下两个压缩文件：

- uploader-2.0.0-win.zip
- localproxy-2.0.0-win.zip

下载并解压之后，将得到以下两个文件夹：

- uploader-2.0.0-win
- localproxy-2.0.0-win

3.2 Mac／Linux 版本

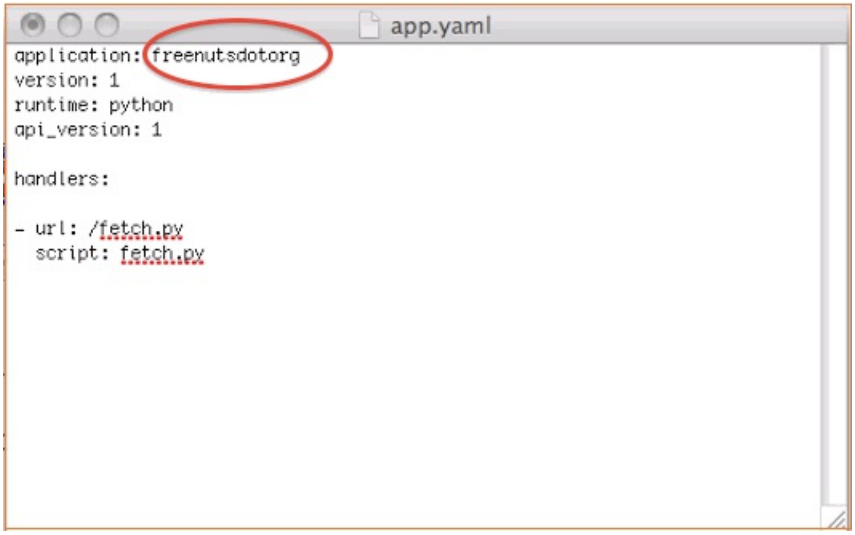
而如果要在 Mac／Linux 上部署和使用 GAppProxy，则需要下载以下两个压缩文件：

- fetchserver-2.0.0.zip
- localproxy-2.0.0.tar.gz

下载并解压之后，将得到以下两个文件夹：

- fetchserver-2.0.0
- localproxy-2.0.0

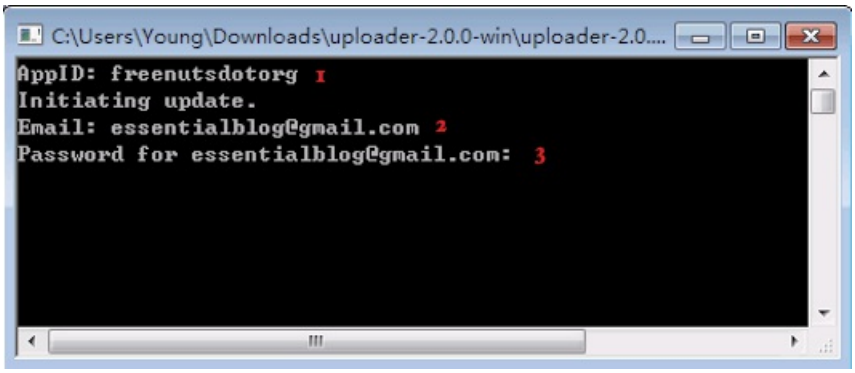
4、修改 app.yaml 文件



在 Windows 系统上，app.yaml 文件位于 “uploader-2.0.0-win” 目录里面的 “fetchserver” 文件夹里面；而在 Mac/Linux 系统上，app.yaml 文件位于 “fetchserver-2.0.0” 文件夹里面，找到并打开该文件之后，只要把里面的 “your_application_name” 替换为你的 GAE 应用程序名称就可以了。

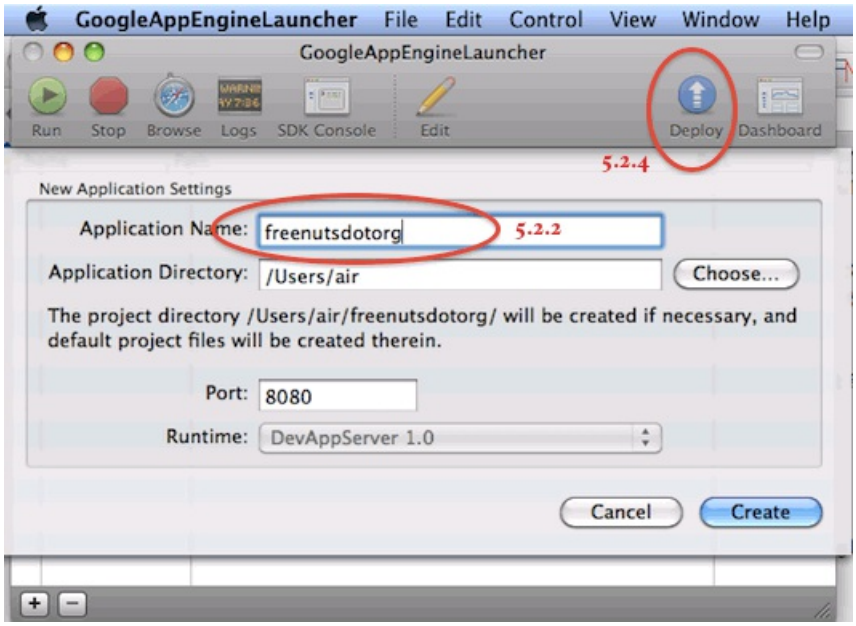
5、部署 GAppProxy 服务器

5.1 如何在 Windows 上部署 GAppProxy 服务器



打开 “uploader-2.0.0-win” **文件夹，双击里面的** “uploader.exe” **文件，在** AppID **提示后输入第一步创建的应用程序名称，然后分别按提示输入自己的** gmail **用户名和密码就可以了。**

5.2 如何在 Mac/Linux 上部署 GAppProxy 服务器



在 Mac/Linux **上部署** GAppProxy **服务器需要借助一个第三方上传工具，具体方法如下**:

5.2.1 下载

下载 Mac **或者** Linux **版本的** Google App Engine SDK for Python**，然后安装。**

5.2.2 添加

运行 GoogleAppEngineLauncher**，点击其顶部文件**(File)**菜单下的** “**新应用程序**”(New Application)**，接着在** “Application Name” **一栏输入** GAE **应用程序名称，而** “Application Directory” **一栏可以使用默认的，也可以指定任意一个路径。**

5.2.3 移动

将 fetchserver **文件夹里面的** “app.yaml” **和** “fetch.py” **两个文件复制粘贴到** “Application Diretory” **对应的文件夹里面。**

5.2.4 上传

回到 GoogleAppEngineLauncher **界面，点击** Deploy **按钮，输入邮箱地址和密码，然后就可以上传** GAppProxy **服务端到** GAE **了。**

5.3 测试 GAppProxy 服务器

在浏览器中输入以下地址：

http://APP_ID.appspot.com/fetch.py

注意将其中的 APP_ID 换成你的 GAE 应用程序名称，如果能看到以下界面：

那就说明 GAppProxy 服务器部署成功，如果看不到，则可以把 http 改成 https 再试一次；如果还看不到，那就可以使用其他翻墙工具再试一次，如果仍然看不到，那就需要重新部署。

6、运行客户端

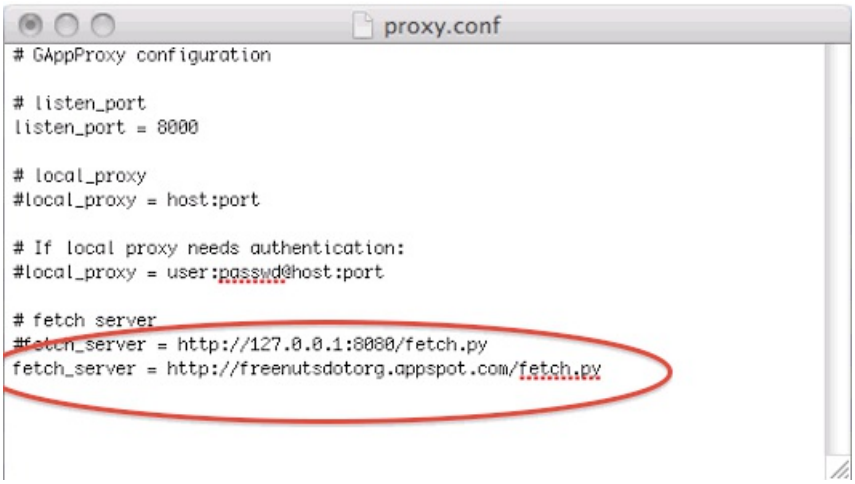
在 GAE 上部署了 GAppProxy 服务端之后，就可以在自己的电脑上运行其客户端了。

6.1 如何在 Windows 上运行 GAppProxy 客户端

Windows 版的有一个执行程序，可以直接点击运行，不过运行之前需要先修改 proxy.conf 文件。

6.1.1 修改 proxy.conf 文件

打开 localproxy-2.0.0-win 目录下的 proxy.conf 文件，把最后一行的 your-fetch-server 改成你的应用程序名称，再删除该行开头的“#”，如下图所示：



然后保存文件。

6.1.2 运行 GAppProxy 客户端

双击同一目录下的 proxy.exe 文件，开始运行 GAppProxy 客户端。

6.2 如何在 Mac/Linux 上运行 GAppProxy 客户端

在 Mac/Linux 上，则需要借助终端应用程序（Terminal）才能运行，并且同样需要先修改 proxy.conf 文件。

6.2.1 修改 proxy.conf 文件

和在 Windows 上的修改一样，只不过 proxy.conf 文件位于 localproxy-2.0.0 目录下。

6.2.2 运行 GAppProxy 客户端

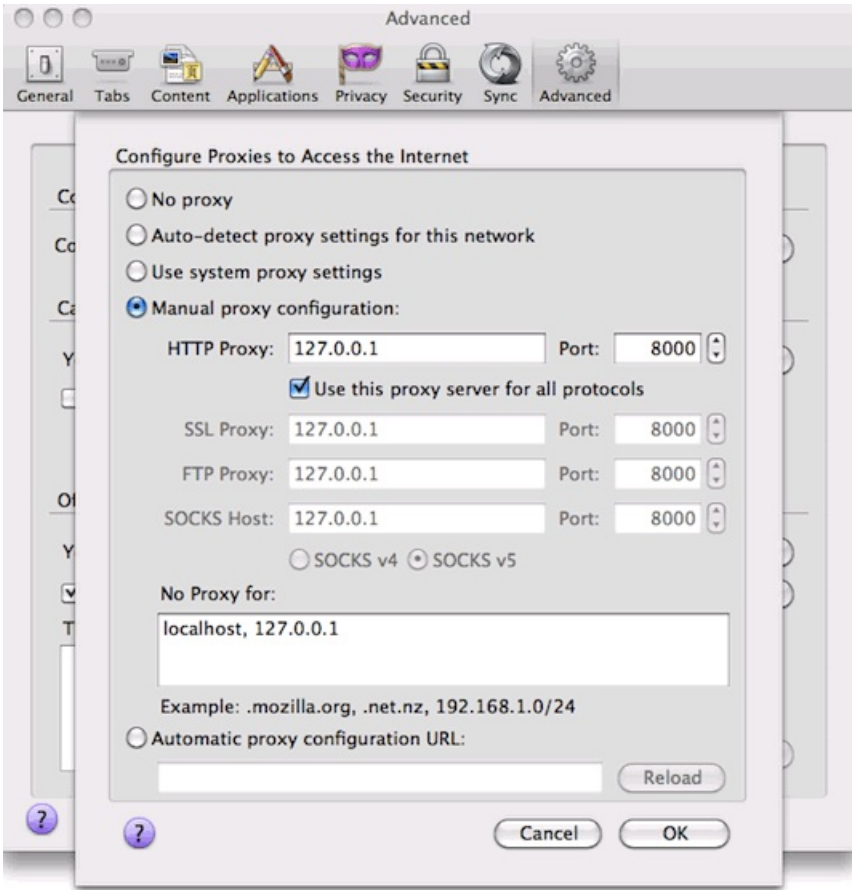
打开终端应用程序，输入以下一行代码：

python xxx/localproxy-2.0.0/proxy.py

注意把 “xxx” 改成 localproxy-2.0.0 文件夹的所有上级目录路径，或者更简单一点，直接把 “proxy.py” 文件拖到 “python” 命令后面。

7、配置浏览器代理

GAppProxy 客户端成功运行之后，打开浏览器，在网络设置里面将代理的服务器 IP 地址设为 127.0.0.1，并且端口为 8000，如下图所示：



由于 GAppProxy 只支持标准 80 端口的 HTTP 协议和 443 端口的 HTTPS 协议，其他端口均不支持，所以，SOCKS 和 FTP 的代理地址可以留空。

备注：

假设你的 GAE 应用程序名称是 “freenutsdotorg”，如果以下链接不可以访问：

http://freenutsdotorg.appspot.com／

但是把 http 改成 https 之后却可以访问，那么你就需要把 proxy.conf 文件里面的 fetch_server 链接改成带 https 的，例如：

fetch-server = https://freenutsdotorg.appspot.com/fetch.py

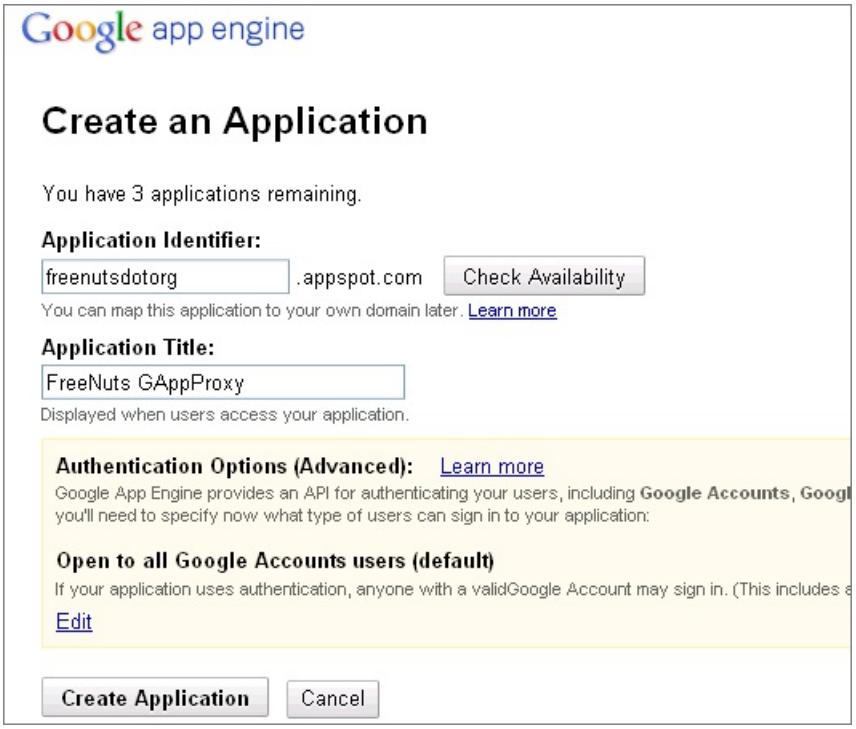
而如果把 http 改成 https 之后还不可以访问，那 GAppProxy 就翻不了墙了，因为你的 GAE 应用程序已经被墙，此时，你可以重新创建一个 GAE 应用程序试试。

第五节：Goagent

类似 GAppProxy 和 Hyk-proxy，Goagent 也是一款 GAE 代理软件。

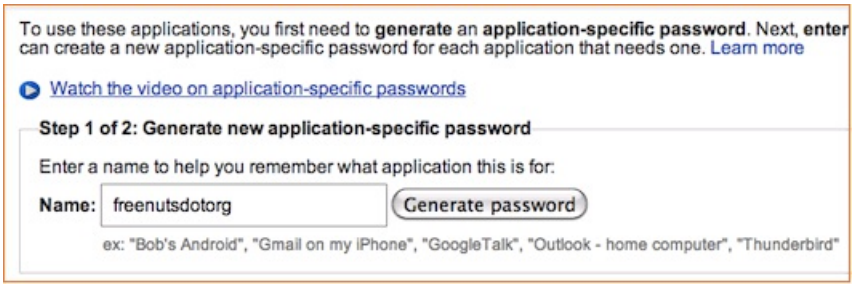
关于如何使用 Goagent，你可以参考其官方网站的简易教程，或者可以参考以下更加通俗易懂的 7 个步骤：

1. 创建一个 GAE 应用程序



和 Hyk-proxy 一样，Goagent 也支持同时连接多个服务器，所以，你可以创建一个或者多个 GAE 应用程序，或者使用旧的应用程序，但是所有应用程序的“存储计划”(Storage Scheme)都必须为“高复制”(High Replication)。

2. 生成一个应用专用密码



如果 Gmail 帐户启用了两步验证，上传 Goagent 服务端到 GAE 时需要一个专用密码(Application-specific password)，具体方法是打开 Google 帐户的安全性(Security)页面，接着点击“向应用和网站授权”(Authorizing applications and sites)旁边的“修改”(Edit)按钮，然后输入任意一个名称并点击“生成密码”(Generate password)按钮就可以了。

如果没有启用两步验证，那就可以忽略这个步骤。

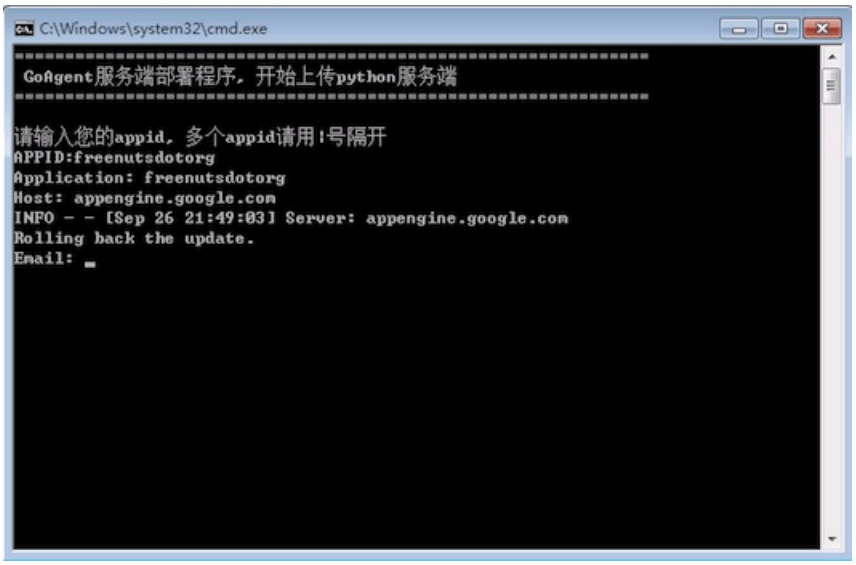
3. 下载 Goagent

如上图所示，点击主页上的下载链接下载 Goagent 压缩文件，解压之后，将会得到 “local” 和 “server” 这两个文件夹。

4. 上传 Goagent 服务端

打开 “server” 文件夹，然后通过以下其中一个方法将 Goagent 的服务端上传到 GAE:

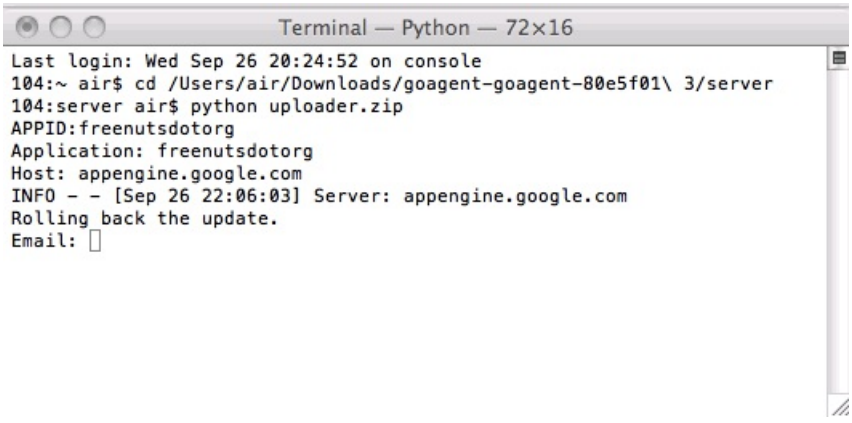
4.1 在 Windows 上如何上传 Goagent 服务端



在 Windows 系统上，打开 “uploader.bat” 文件，输入第一步创建的 GAE 应用程序名称 (ID)、Gmail 地址和(应用专用)密码，然后就可以开始上传了。

如果要同时将 Goagent 服务端上传到多个 GAE 应用程序，每个程序之间可以用 “|” 号隔开。

4.2 在 Mac 上如何上传 Goagent 服务端



在 Mac OS X 系统上，你可以打开终端应用程序 (Terminal)，然后输入以下一行命令:

cd server-文件夹的绝对路径

例如：

cd /Users/air/Downloads/goagent-goagent-80e5f01\ 3/server

你也可以直接把 “server” 文件夹拖到 “cd” 命令后面。

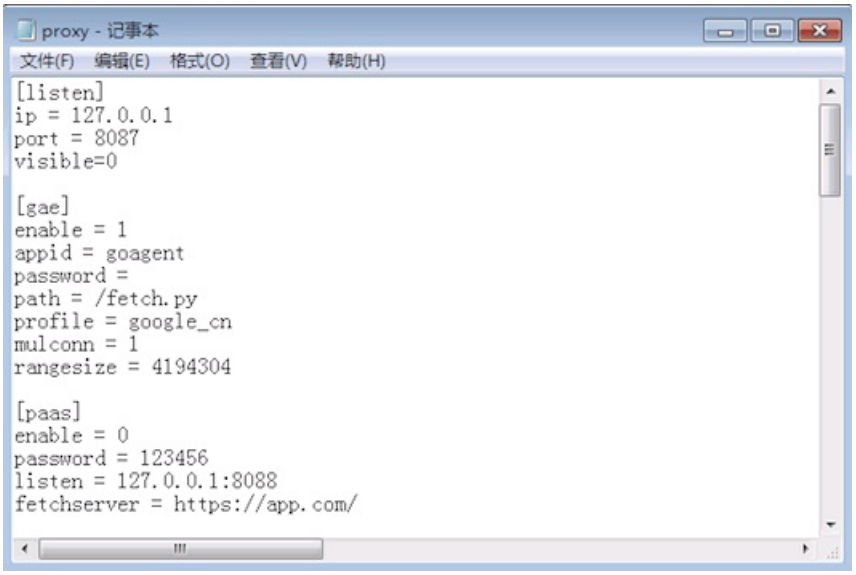
完了之后，输入以下一行命令：

python uploader.zip

回车之后，你就可以输入 GAE 应用程序名称、Gmail 邮箱地址和（应用专用）密码，并开始上传 Goagent 服务端。

顺便一提，不要省略第一行命令而直接把 “uploader.zip” 拖到 “python” 命令后面，否则可能会上传失败，原因不明。

5. 修改 proxy.ini 文件



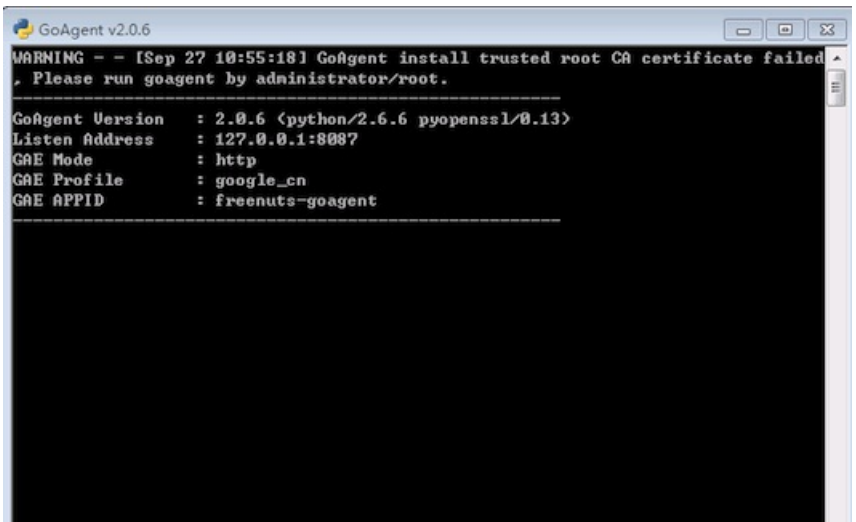
上传成功之后，打开 “local” 文件夹里面的 “proxy.ini” 文件，然后把 “appid” 的 “goagent” 改为你的 GAE 应用程序名称。

另外，你也可以把 “profile” 的值 “google_cn” 改成 “google_hk”，以便通过 https加密链接使用 Goagent 服务。

6. 运行 Goagent 客户端

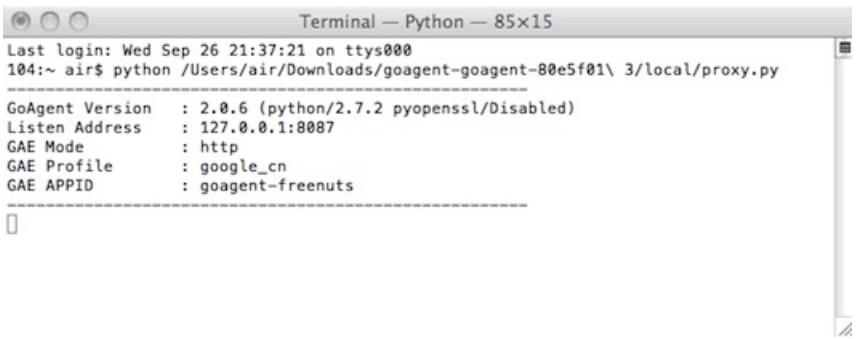
保存 “proxy.ini” 文件之后，你就可以运行 Goagent 客户端了。

6.1 如何在 Windows 上 运行Goagent 客户端



在 Windows 系统上，你可以通过双击 “local” 文件夹里面的 “Goagent.exe” 启动 Goagent。

6.2 如何在 Mac 上运行 Goagent 客户端



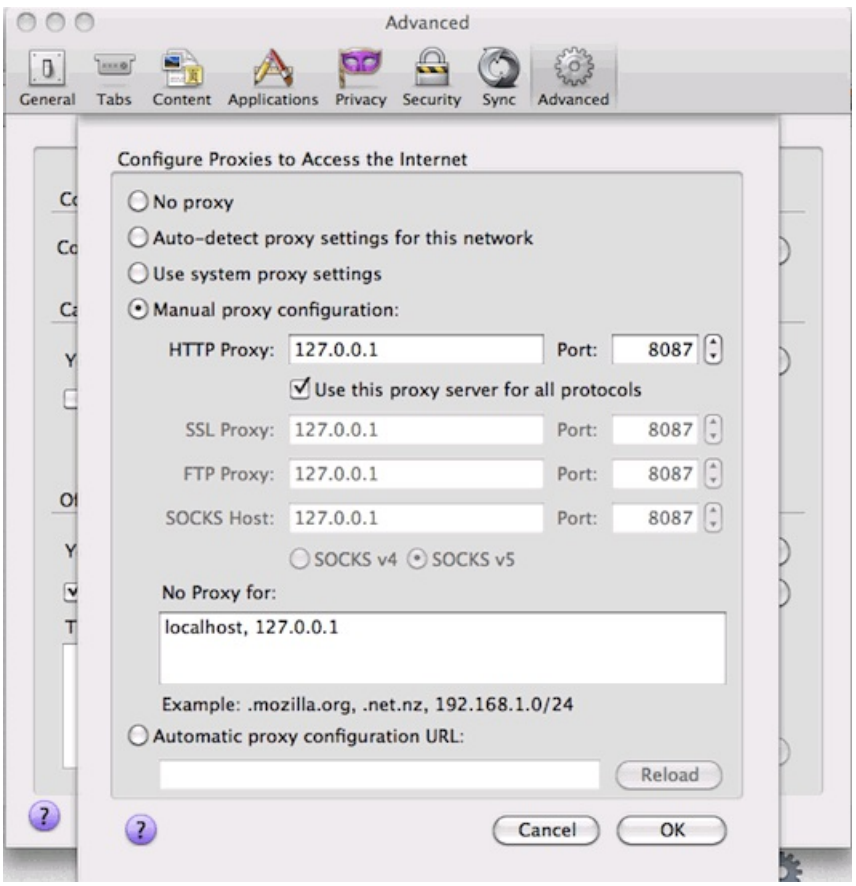
在 Mac OS X 系统上，你可以打开终端应用程序，然后输入以下一行命令：

python proxy.py-文件的绝对路径

这次，你可以直接把 “local” 文件夹里面的 “proxy.py” 文件拖到 “python” 命令的后面。

7. 配置浏览器代理

Goagent 客户端成功连接之后，你可以打开浏览器，在网络设置里面将代理的服务器 IP 地址设为 127.0.0.1，并且端口为 8087，如下图所示：



上图的界面是 Firefox 的，IE、Chrome、Safari 或者其他浏览器的代理配置界面将有所不同。

浏览器代理配置完之后，你就可以通过 Goagent 翻墙了。

和 GAppProxy 以及 Hyk-proxy 一样，Goagent 对 HTTPS 的支持不是很好，虽然你可以双击 “local” 文件夹里面的 “CA.crt” 文件导入证书，但是，导入证书之后，2.0.6 版本在 Safari 上可以正常通过 HTTPS 链接访问 Facebook 和 Twitter，但是在 Chrome 和 Firefox 浏览器上却不行，而最新

的 2.0.11 版本在 Chrome 上可以通过 HTTPS 链接访问 Facebook，但是打不开 Twitter，而在 Safari 和 Firefox 上可以打开，但是却无法正常显示。

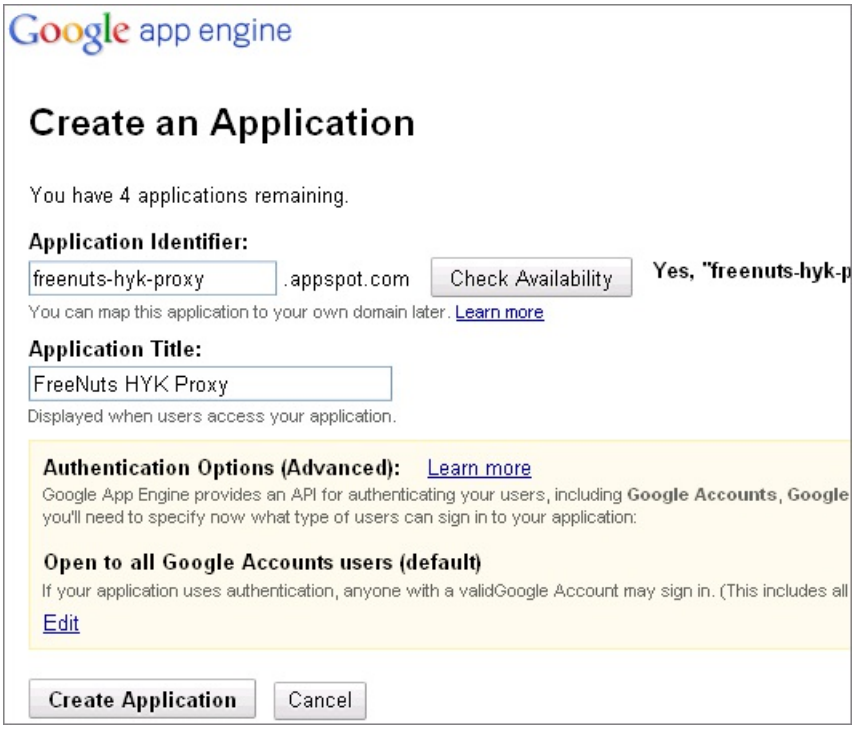
另外，除了 Windows 和 Mac OS X 之外，Goagent 的 GAE 代理服务还适用于 Linux、Android、iOS、webOS、OpenWRT 和 Maemo 等操作系统。

第六节：Hyk-proxy

和 GAppProxy 一样，Hyk-proxy 这个 GAE 代理也不再更新，但是仍然可以翻墙。

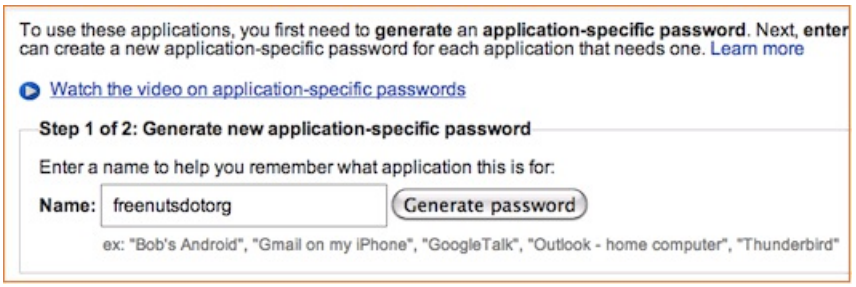
那么如何通过 Hyk-proxy 翻墙呢？你可以参考其官方网站的介绍，或者参考以下更加通俗易懂的 8 个步骤：

1. 创建 GAE 应用程序



和 Goagent 一样，Hyk-proxy 也支持同时连接多个服务器，所以，你可以登录 GAE 帐户创建一个或者多个应用程序。

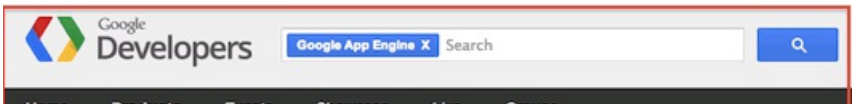
2. 生成一个应用专用密码

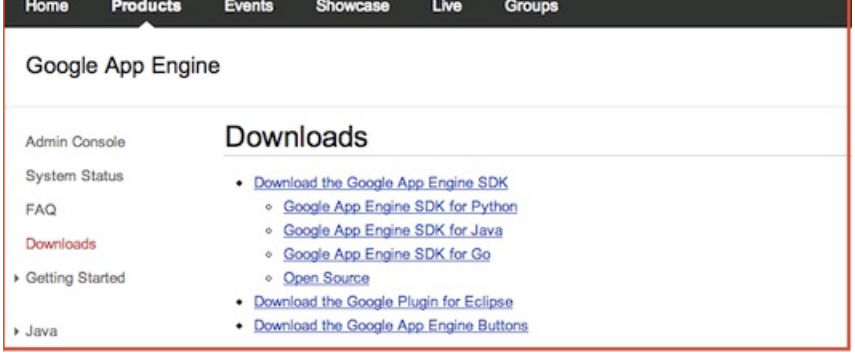


如果 Gmail 帐户启用了两步验证，上传 Hyk-proxy 服务端到 GAE 时需要一个专用密码（Application-specific password），具体方法是打开 Google 帐户的安全性（Security）页面，接着点击“向应用和网站授权”（Authorizing applications and sites）旁边的“修改”（Edit）按钮，然后输入任意一个名称并点击“生成密码”（Generate password）按钮就可以了。

如果没有启用两步验证，那就可以忽略这个步骤。

3. 下载 Java 和 Google App Engine SDK for Java





从官方网站下载 Java，然后安装；从 Google Code 下载 Google App Engine SDK for Java，然后解压。

另外，如果你用的是 Mac OS X 系统，那么只要下载 Google App Engine SDK for Java 就可以了，因为该系统已经预装了 Java。

4. 下载 Hyk-proxy

Hyk-proxy 的下载页面有 4 个文件可供下载，你可以只下载其中的 “hyk-proxy-0.9.4.1.zip” 和 “hyk-proxy-gae-server-0.9.4.1.zip” 这两个。

另外，在 Windows 系统上，你也可以下载 “hyk-proxy-install_0.9.4.1.exe” 而不需要下载 “hyk-proxy-0.9.4.1.zip”。而 “hyk-proxy-android-0.9.4beta.apk” 这个文件是用于 Android 系统上的。

下载完成之后，解压。

5. 部署任务

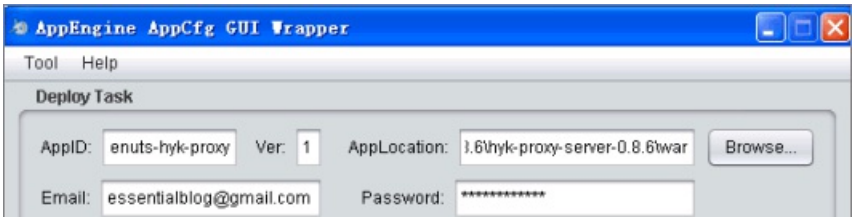
部署任务 (deploy task) 是指上传 Hyk-proxy 服务端到你的 GAE 应用程序。

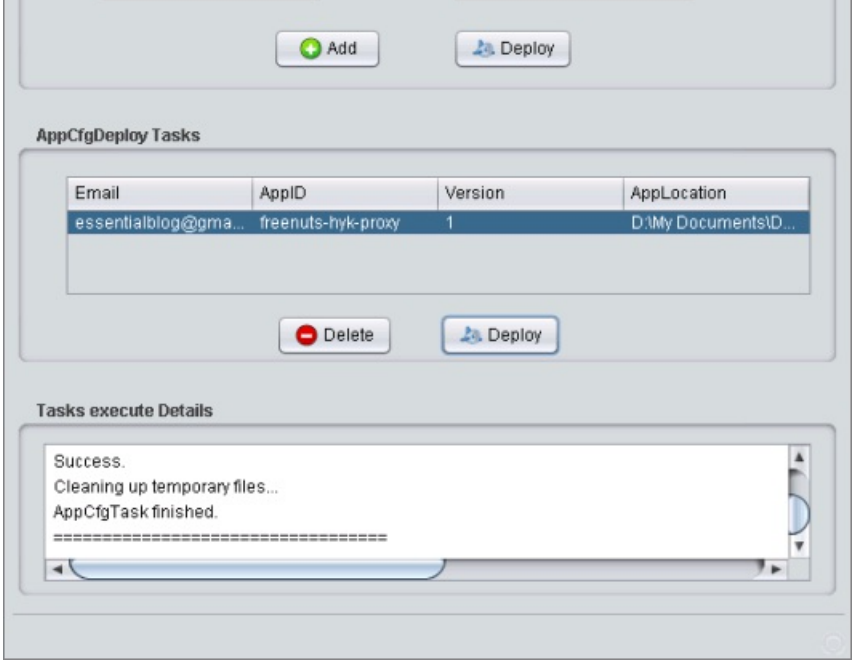
在 Windows 系统上，你可以运行 “hyk-proxy-gae-server-0.9.4.1” 文件夹里面的 “install.bat” 文件；而在 Mac/Linux 上，你可以打开终端服务程序 (Terminal)，然后输入以下一行命令：

```
sh /the-path-to/install.sh
```

你也可以直接把 “install.sh” 文件拖到 “sh” 后面。

然后，你就可以看到一个 “AppEngine AppCfg GUI Wrapper” 窗口，如下图所示：





在该窗口上，确定 “Google App Engine SDK for Java” 解压后的文件夹的路径之后，你可以输入 GAE 应用程序的名称（ID），选择 “hyk-proxy-gae-server-0.9.4.1” 文件夹作为 AppLocation，接着输入 Gmail 邮箱地址和（应用专用）密码，然后就可以点击 “Deploy” 按钮上传 Hyk-proxy 服务端了。

备注：

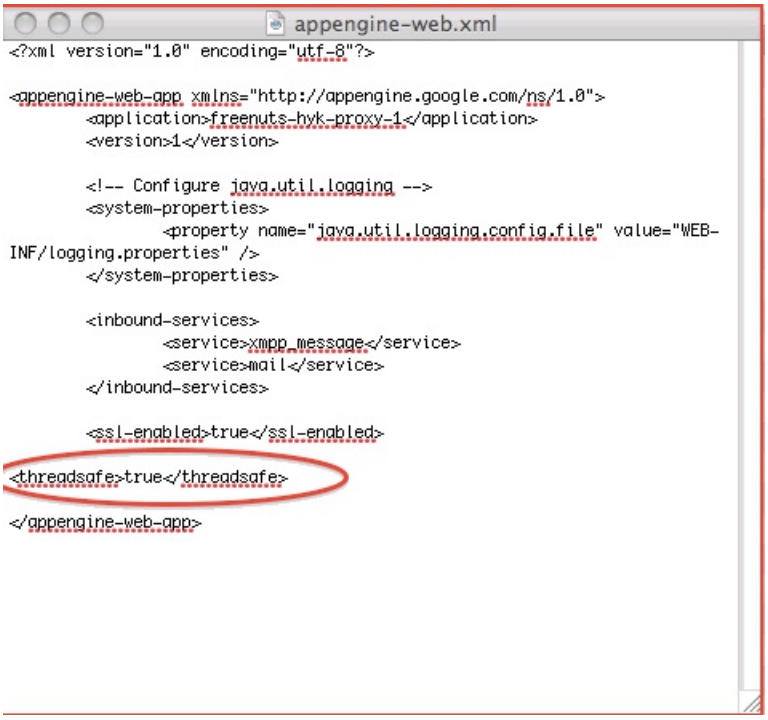
如果部署任务的时候出现以下的错误提示：

Bad configuration: appengine-web.xml does not contain a <threadsafe> element.

那么，你就可以在 “appengine-web.xml” 文件里面添加以下一行代码：

<threadsafe>true</threadsafe>

如下图所示：



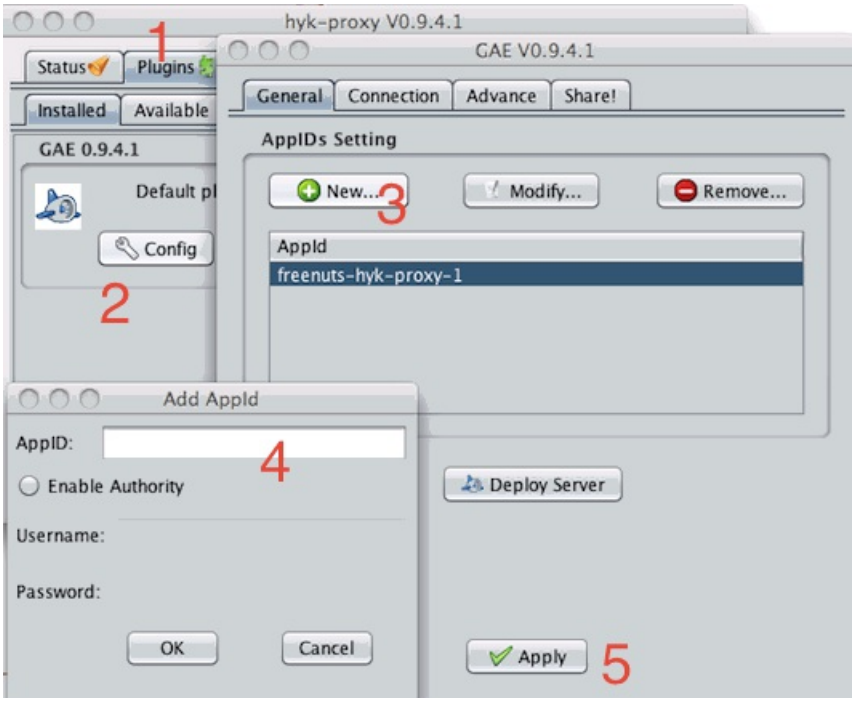
6. 添加 GAE 应用程序到 Hyk-proxy 客户端

在 Windows 上，你可以双击 “bin” 文件夹里面的 “startgui.bat”，或者运行 “Start hyk-proxy (GUI)” 应用程序（如果你下载并安装了前面提到的 “hyk-proxy-install_0.9.4.1.exe” 文件的话）；而在 Mac/Linux 上，你可以打开终端应用程序，并输入以下一行命令：

```
sh /the-path-to/startgui.sh
```

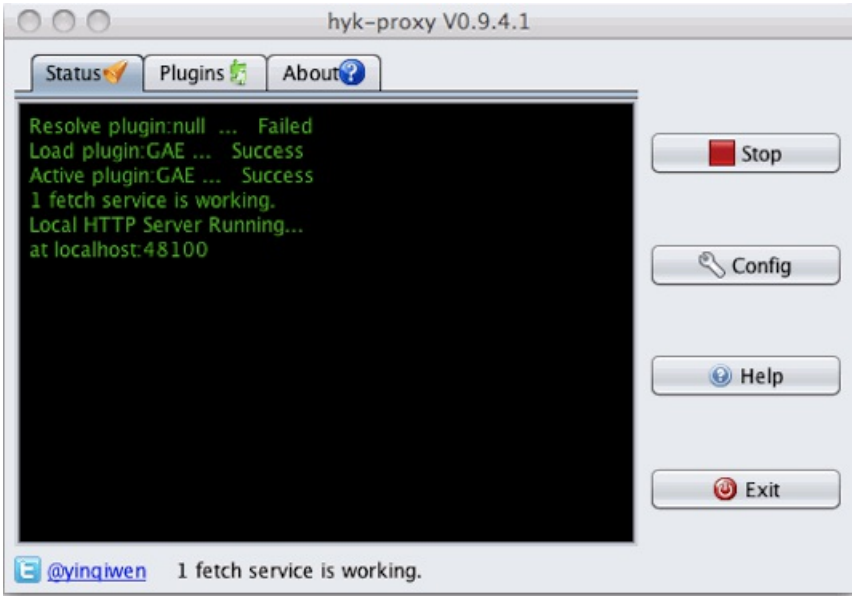
当然，你也可以直接把 “hyk-proxy-0.9.4.1” 文件夹里面的 “startgui.sh” 文件拖到 “sh” 后面。

然后，你就可以打开 Hyk-proxy 客户端，点击 “Plugins” 标签 “GAE 0.9.4.1” 下面的 “Config” 按钮，再点击新窗口里面的 “New” 按钮，然后输入你的 GAE 应用程序名称，如下图所示：



完了之后，点击 “Apply” 按钮就可以了。你可以输入多个 GAE 应用程序名称，但每次只能输入和部署一个。

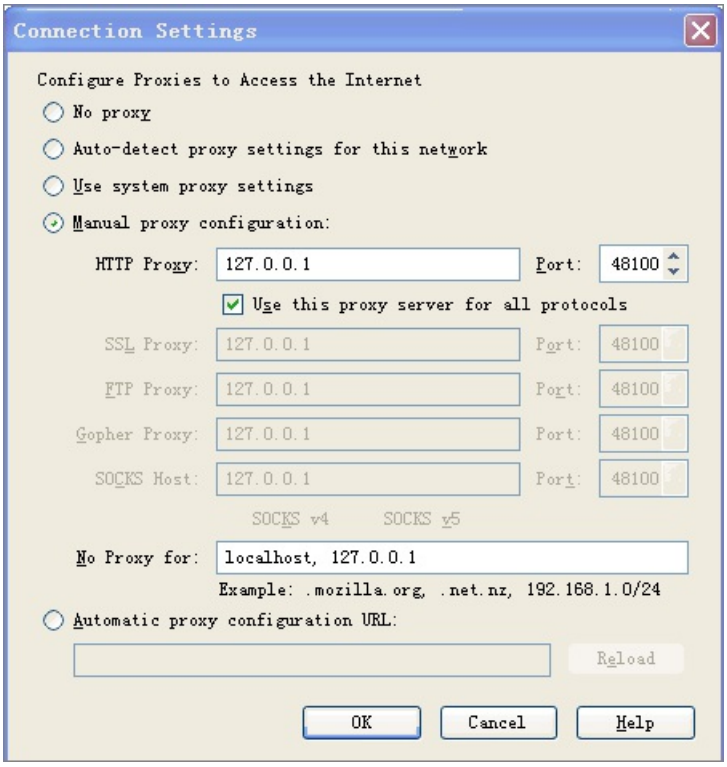
7. 启用 Hyk-proxy



应用程序添加成功之后，点击 “Start” 按钮就可以运行 Hyk-proxy 服务了。

8. 配置浏览器代理

Hyk-proxy 客户端成功连接之后，你可以打开浏览器，在网络设置里面将代理的服务器 IP 地址设为 127.0.0.1，并且端口为 48100，如下图所示：



上图的界面是 Firefox **的，**IE、Chrome、Safari **或者其他浏览器的代理配置界面将有所不同。**

浏览**器代理配置完之后，你就可以通过** Goagent **翻墙了。**

额外收获：

如果你的 GAE **应用程序名称被墙，那么你可以通过** XMPP **的方式连接** Hyk-proxy **服务器。**

具体方法是，在前面提到的添加应用程序的窗口的“Connection**”标签页，选择** XMPP **作为连接方式，然后添加你的** XMPP **帐号(例如** GTalk)。

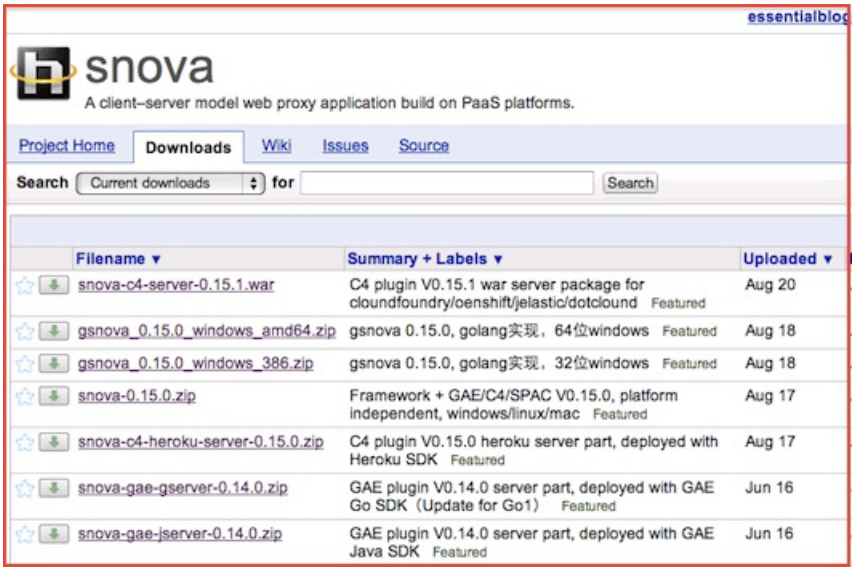
除此之外，你还可以通过 HTTPS **或者代理的方式连接** Hyk-proxy **服务器，但是它们都没有** XMPP **那么快。**

第七节：Snova

在 GAppProxy、Goagent, Hyk-proxy 以及 Snova 这四个流行的 GAE 代理之中，Snova 是最好的，因为它完美地支持 HTTPS。

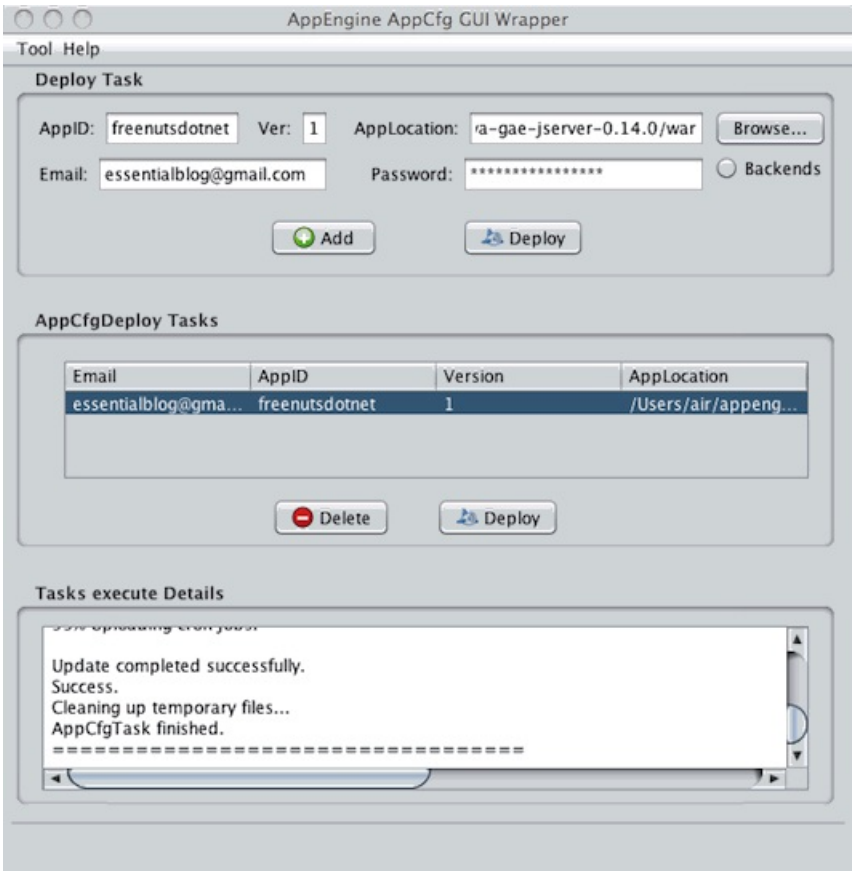
除此之外，它还可以通过以下 6 种不同的方法连接翻墙：

1. 直接法



默认情况下，Snova 可以自动连接其他用户共享的 GAE 应用程序，所以，你可以下载 Snova 客户端后直接启动。

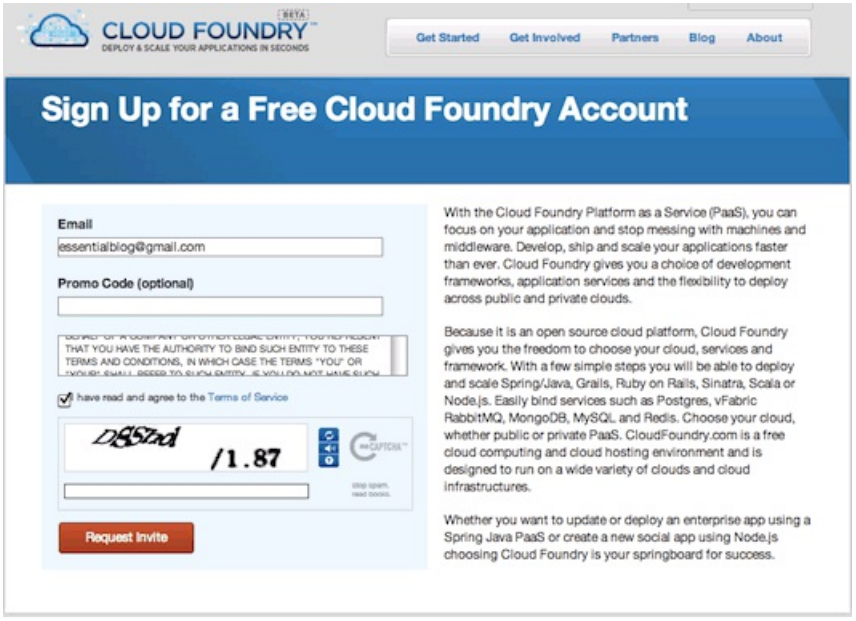
2. GAE 法



除了使用别人共享的 GAE 应用程序，你也可以创建自己的，接着把 Snova 的服务端部署到该应用程序，然后再运行 Snova 客户端。

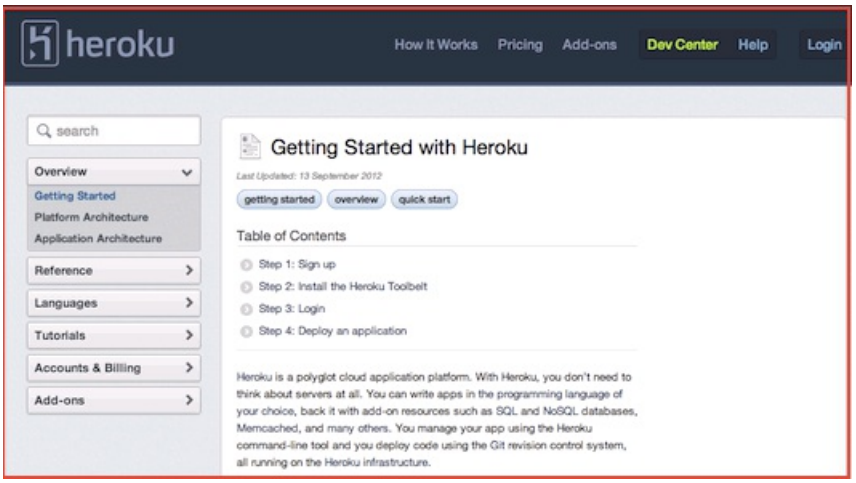
由于 GAE 本身的限制，以上两种方法只能正常访问 HTTP 链接，而如果要正常访问 HTTPS 链接，那你就还需要添加或者单单使用以下一种或者多种的通过其他 PaaS 平台搭建 Snova C4 插件的方法：

3. Cloud Foundry 法



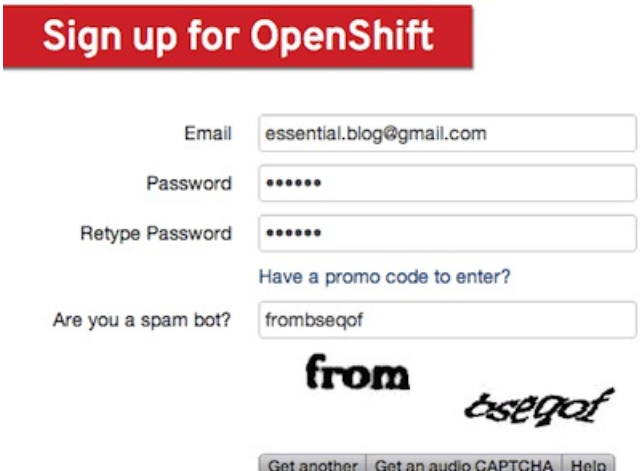
Cloud Foundry 免费提供 4 核 CUP、2G 硬盘、512M 内存的服务器给你安装 C4 插件，并且没有流量限制 —— 至少它没有说有。

4. Heroku 法



Heroku 的免费流量是 2TB/month，足够翻遍所有被墙的网站了。

5. OpenShift 法



OpenShift 可以免费创建最多 3 个应用程序，每个应用程序将配备 1G 空间和 512 内存。

6. Jelastic 法

通过 Jelastic，你可以选择在 Servint、Dogado、Rusonyx 或者其他服务器上搭建 C4 插件，并且可以直接在其网站上部署，而不需要输入任何的命令。

对于 C4 插件，你需要在 Heroku 上使用 “snova-c4-heroku-server-xxx.zip” 文件，而在其他三个 PaaS 平台上使用 “snova-c4-server-xxx.zip” 文件。

以上 6 种方法里面，除了第一种和第二种不可以同时使用之外，任意 n 种都可以同时或者单独使用，并且每一种都可以添加多个应用程序。

一、Hyk-Proxy 和 Snova 的最简单使用方法

不管是 Hyk-proxy、Goagent、Snova 还是其他的 GAE 代理，通常都需要先创建一个 GAE 应用程序才能够使用。

但是这对某些人来讲并非一件容易的事，而伊朗用户甚至不能注册 GAE 帐号。

为了避免 GAE 和其他复杂的步骤，Hyk-proxy 和 Snova 这两个代理允许你直接通过以下的方法直接使用其他用户共享的 GAE 应用程序连接：

1. Hyk-proxy 最简单的使用方法

在 Hyk-proxy 的下载(Downloads)页面，你可以下载 “hyk-proxy-0.9.4.1.zip” 或者 “hyk-proxy-install_0.9.4.1.exe”（仅适用于 Windows），然后解压或者安装就可以在 Windows 和 Mac 系统上使用该代理翻墙了。

1.1 在 Windows 上的使用方法

在 Windows 上，你可以双击 “hyk-proxy-0.9.4.1” 文件夹 “bin” 目录里面的 “startgui.bat” 文件 —— 如果你下载并解压缩了 “hyk-proxy-0.9.4.1.zip” 的话；或者运行 “Start hyk-proxy (GUI)” 程序 —— 如果你下载并安装了 “hyk-proxy-install_0.9.4.1.exe” 的话。

1.2 在 Mac 上的使用方法

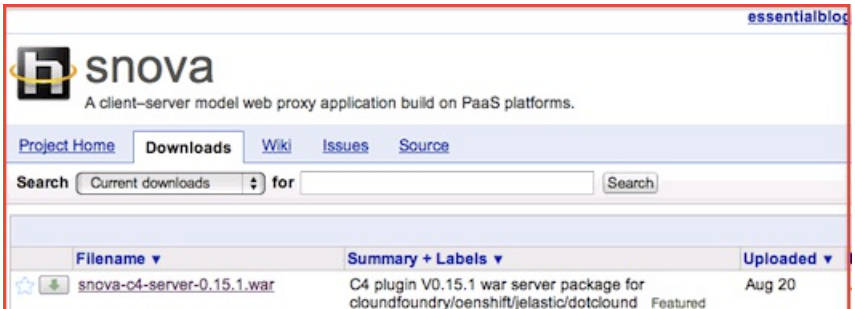
在 Mac 上，你可以打开终端应用程序并输入以下一行命令：

```
sh /the-path-to/startgui.sh
```

记得把 “the-path-to” 替换成 “startgui.sh” 文件的绝对路径。或者你也可以直接把 “hyk-proxy-0.9.4.1” 文件夹里面的 “startgui.sh” 文件拖到 “sh” 后面。

不管使用以上哪一种方法，你都可以打开 Hyk-proxy 客户端并点击 “Start” 按钮，如果连接成功，那么你就可以通过 Hyk-proxy 翻墙了。

2. Snova 最简单的使用方法



gsnova_0.15.0_windows_amd64.zip	gsnova 0.15.0, golang实现，64位windows Featured	Aug 18
gsnova_0.15.0_windows_386.zip	gsnova 0.15.0, golang实现，32位windows Featured	Aug 18
snova-0.15.0.zip	Framework + GAE/C4/SPAC V0.15.0, platform independent, windows/linux/mac Featured	Aug 17
snova-c4-heroku-server-0.15.0.zip	C4 plugin V0.15.0 heroku server part, deployed with Heroku SDK Featured	Aug 17
snova-gae-gserver-0.14.0.zip	GAE plugin V0.14.0 server part, deployed with GAE Go SDK（Update for Go1） Featured	Jun 16
snova-gae-jserver-0.14.0.zip	GAE plugin V0.14.0 server part, deployed with GAE Java SDK Featured	Jun 16

和前面提到的 Hyk-proxy 的使用方法几乎一样。

在 Snova 的下载（Downloads）页面，你只需要下载并解压 “snova-xxx.zip” 文件就可以在 Windows 和 Mac 系统上使用它的代理服务了。

2.1 在 Windows 上的使用方法

在 Windows 上，你可以双击 “snova-xxx” 文件夹 “bin” 目录里面的 “startgui.bat” 文件。

2.2 在 Mac 上的使用方法

在 Mac 上，你可以打开终端应用程序并输入以下一行命令：

```
sh /the-path-to/startgui.sh
```

记得把 “the-path-to” 替换成 “startgui.sh” 文件的绝对路径。或者你也可以直接把 “snova-xxx” 文件夹里面的 “startgui.sh” 文件拖到 “sh” 后面。

不管使用以上哪一种方法，你都可以打开 Snova 客户端并点击 “Start” 按钮，如果连接成功，那么你就可以通过 Snova 翻墙了。

顺便一提，上面所提到的方法并不适用于 GAppProxy 和 Goagent，因为前者的 GAE 应用程序 “fetchserver1” 的流量配额已经用完，而后者并不提供默认的 GAE 应用程序。

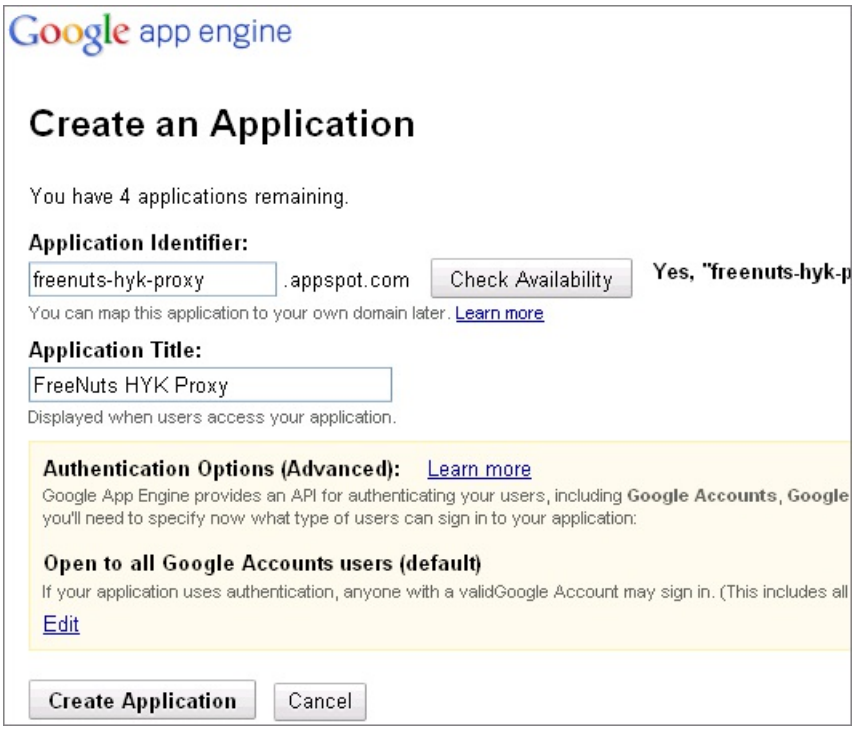
二、如何在 GAE 上安装和使用 Snova 代理

如前面提到的，Hyk-proxy 已经停止更新，因为它的作者开发了一个新的替代产品 — Snova。

类似于 Hyk-proxy，Snova 也是一个基于 GAE 的免费网页代理，但是同时也支持 CloudFoundry、Heroku、OpenShift 和其他 PaaS (Platform as a service，平台即服务) 平台，从而能够正常地访问 HTTPS 加密网页。

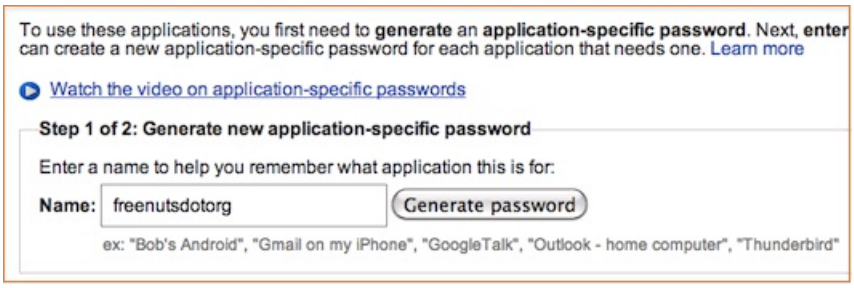
下面将介绍如何在 GAE 上安装和使用 Snova 代理，具体操作步骤和 Hyk-proxy 的差不多：

1. 创建 GAE 应用程序



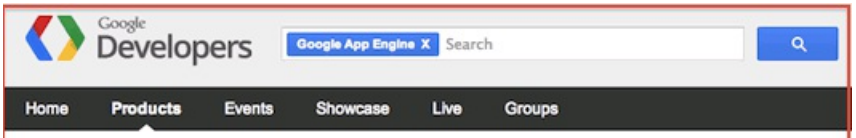
和 Hyk-proxy 一样，Snova 也支持同时连接多个服务器，所以，你可以登录 GAE 帐户创建一个或者多个应用程序。

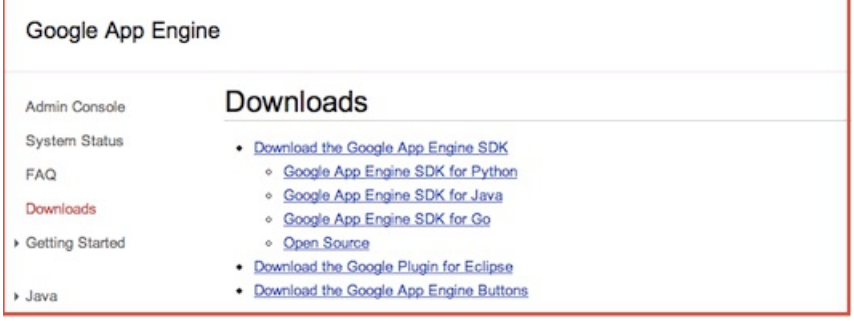
2. 生成一个应用专用密码



具体方法可参考前一篇文章，而如果你的 Gmail 没有启用两步验证，那就可以忽略这个步骤。

3. 下载 Java 和 Google App Engine SDK for Java

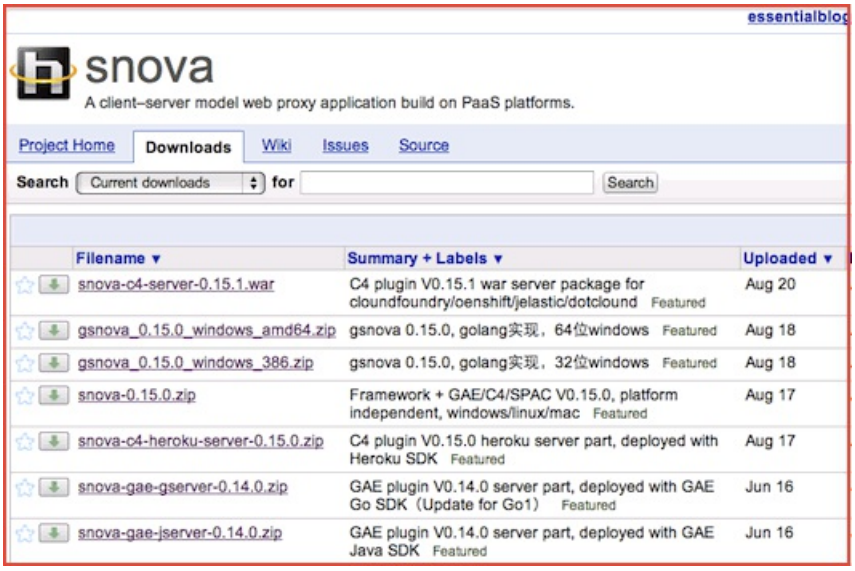




和 Hyk-proxy 一样，Mac OS X 系统只要下载 Google App Engine SDK for Java 就可以了。

另外，由于 Snova 同时还支持 Go 语言，所以你也可以不用下载这两个文件，而取而代之下载 Go 和 Google App Engine SDK for Go。

4. 下载 Snova



下载页面(Downloads)有 7 个文件，你可以只下载 “snova-xxx.zip” 和 “snova-gae-jserver-xx.zip” (针对 Java 语言)。

下载完成之后，解压缩。

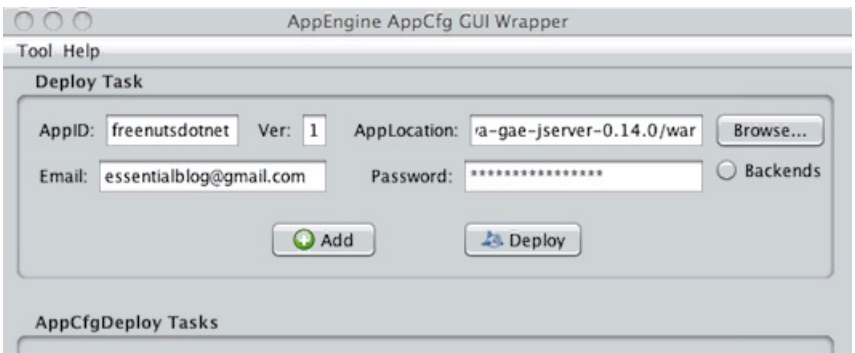
5. 部署服务器

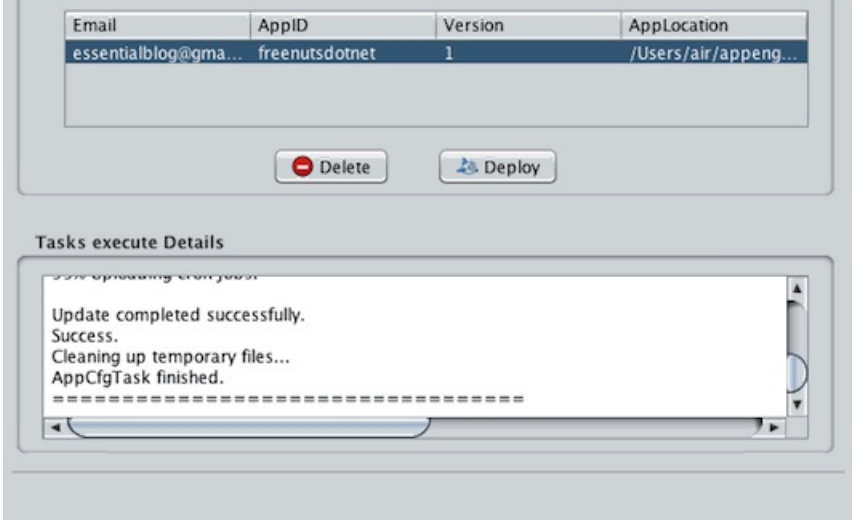
类似 Hyk-proxy，在 Windows 系统上，你可以直接运行 “snova-gae-jserver-xx” 文件夹里的 “install.bat” 文件，而在 Mac 上，你可以打开终端应用程序并输入以下命令：

```
sh /the-path-to/install.sh
```

或者你可以直接把 “snova-gae-jserver-xx” 文件夹里的 “install.bat” 文件拖到 “sh” 命令后面。

完了之后，你就可以看到一个类似以下的 “AppEngine AppCfg GUI Wrapper” 窗口：





在该窗口上，确定 “Google App Engine SDK for Java” 解压后的文件夹的路径之后，你可以输入 GAE 应用程序的名称，选择 “snova-gae-jserver-xx” 文件夹作为 AppLocation，接着输入 Gmail 邮箱地址和(应用专用)密码，然后就可以点击 “Deploy” 按钮上传 Snova 服务端了。

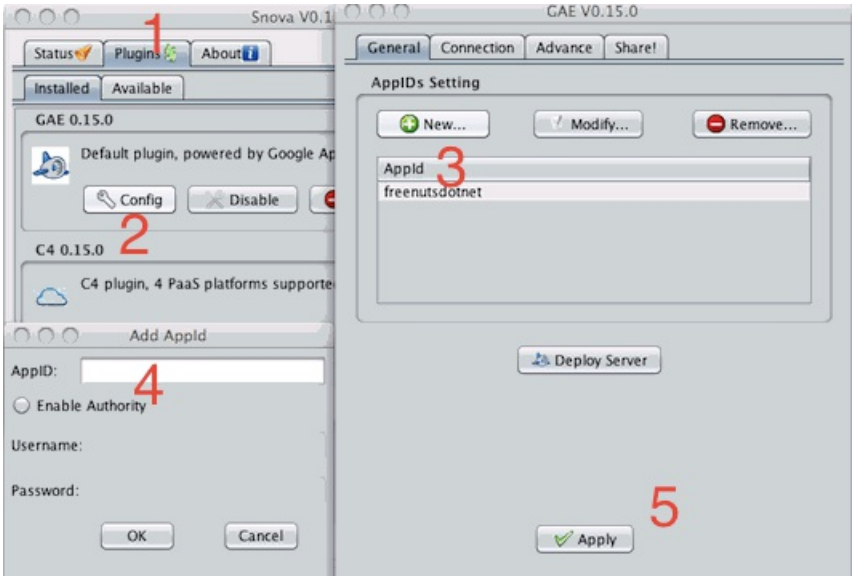
6. 添加 GAE 应用程序到 Snova 客户端

在 Windows 上，你可以双击 “bin” 文件夹里面的 “startgui.bat” 文件; 而在 Mac 上，你可以打开终端应用程序，并输入以下一行命令:

```
sh /the-path-to/startgui.sh
```

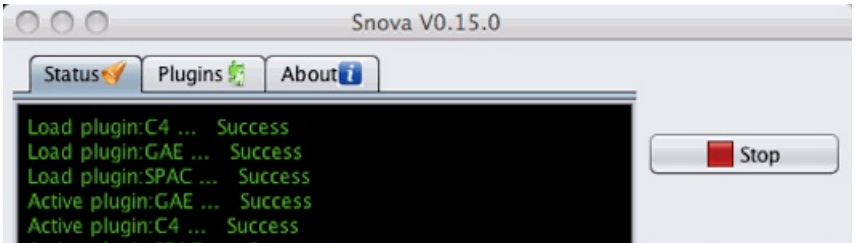
当然，你也可以直接把 “snova-xxx” 文件夹里面的 “startgui.sh” 文件拖到 “sh” 后面。

然后，你就可以打开 Snova 客户端，点击 “Plugins” 标签 “GAE xxx” 插件下面的 “Config” 按钮，再点击新窗口里面的 “New” 按钮，然后输入你的 GAE 应用程序名称，如下图所示:



完了之后，点击 “Apply” 按钮就可以了。你可以输入多个 GAE 应用程序名称，但每次只能输入和部署一个。

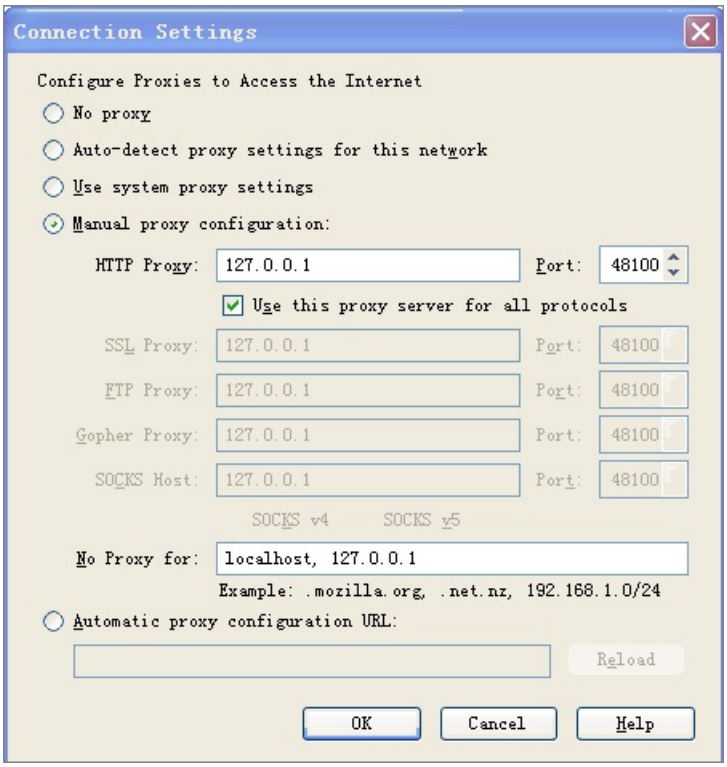
7. 启用 Snova



应用程序添加成功之后，点击 “Start” 按钮就可以运行 Snova 服务了。

8. 配置浏览器代理

和 Hyk-proxy 一样，当 Snova 服务连接成功之后，你也需要打开浏览器，并在网络设置里面将代理的服务器 IP 地址设为 127.0.0.1，端口为 48100，如下图所示：



上图的界面是 Firefox 的，IE、Chrome、Safari 或者其他浏览器的代理配置界面将有所不同。

浏览器代理配置完之后，你就可以通过 Snova 翻墙了。

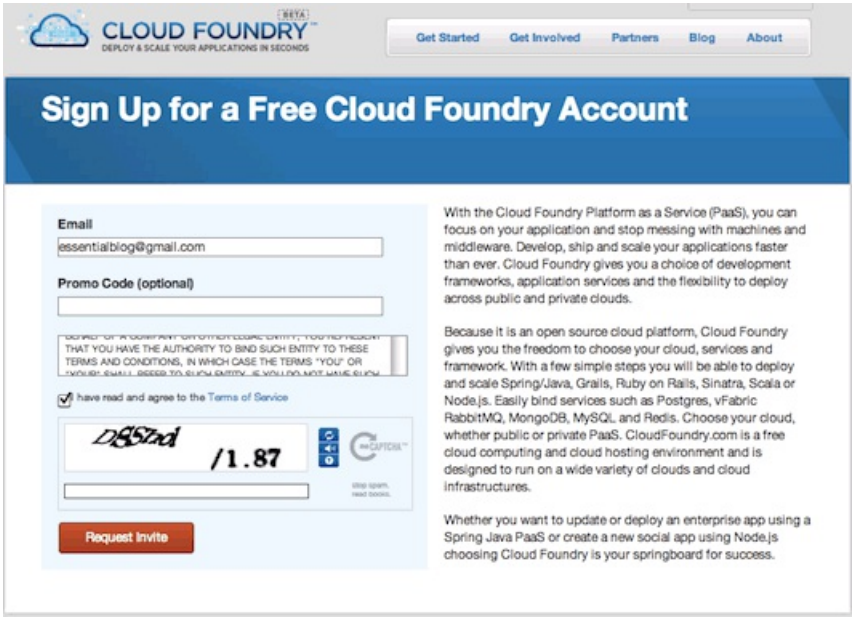
但是，和 Hyk-proxy 一样，这个时候的 Snova 还不可以正常访问 HTTPS 加密链接，除非添加 CloudFoundry、Heroku、OpenShift 和／或其他 PaaS 平台的 Snova 服务端作为插件。

三、如何在 Cloud Foundry 上安装和使用 Snova 代理

如之前所说，Snova 光靠 GAE 是不能正常访问使用 HTTPS 加密链接的被墙网站的，还需要添加 Cloud Foundry、Heroku、OpenShift 和／或其他 PaaS 平台的 Snova 服务端作为插件。

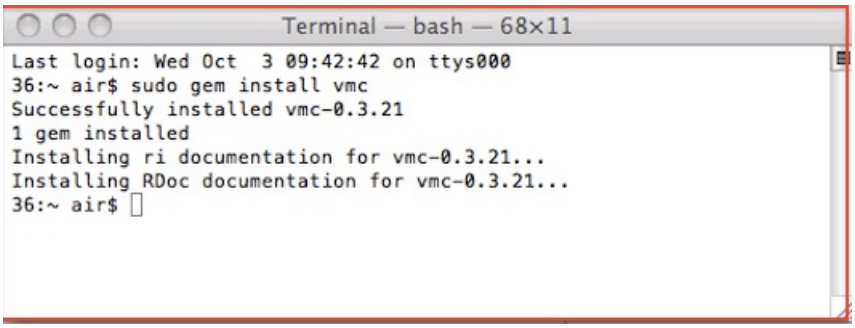
下面将介绍如何在 Cloud Foundry 上安装和使用 Snova 代理：

1. 创建一个 Cloud Foundry 帐号



在 Cloud Foundry 注册页面，输入你的邮箱地址就可以申请帐号了，帐号的用户名和密码很快就会发到你的邮箱。

2. 安装 vmc



基于 Ruby 和 RubyGems 这两个程序，vmc 是部署 Snova 到 Cloud Foundry 的必须命令。

关于在 Windows、Ubuntu、Debian 或者其他系统的安装方法，可以参考官方网站的教程，下面将介绍如何在 Mac 系统上安装 vmc。

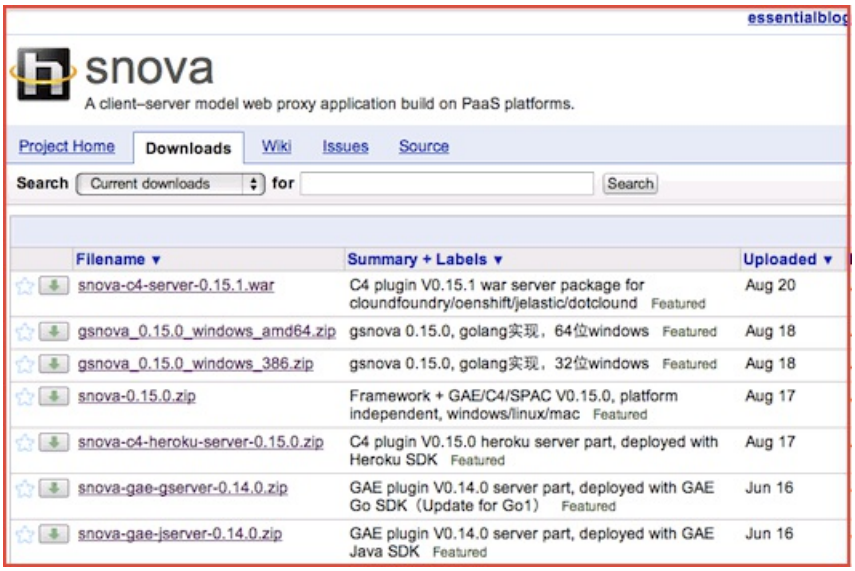
首先，打开终端应用程序，并输入以下一行命令：

```
sudo gem install vmc
```

如果需要的话，输入电脑密码，然后就可以安装 vmc 了。

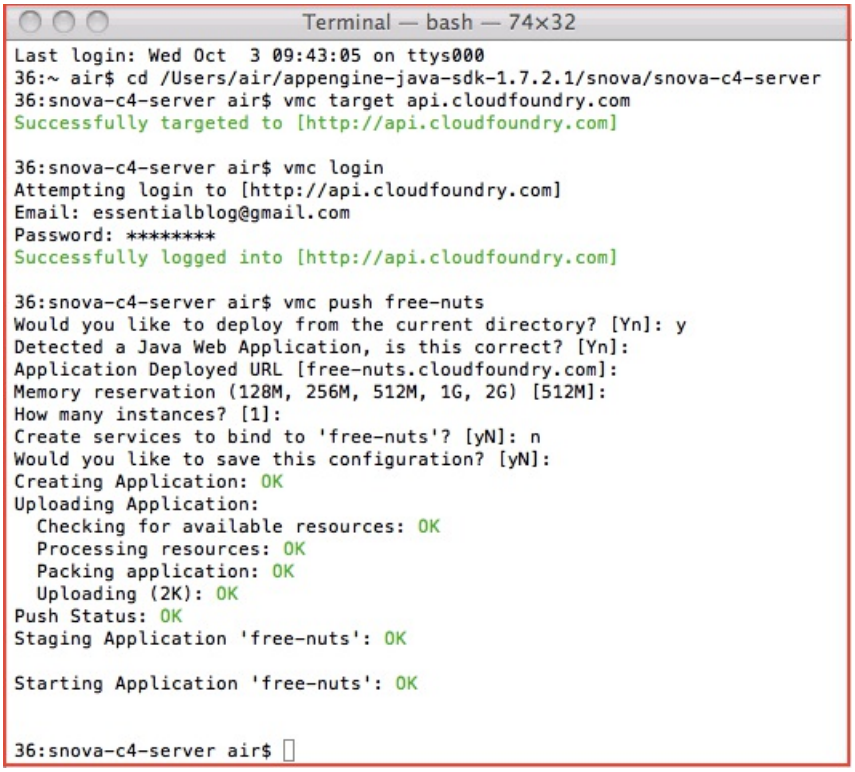
顺便一提，安装过程需要时间，并且需要等到有东西安装完成之后才能显示结果。

3. 下载 snova-c4-server-xxx.war



在 Snova 的下载（Downloads）页面，下载 “snova-c4-server-xxx.war” 文件并把它放到一个新的空文件夹，例如下一个步骤将会用到的 “snova-c4-server”。

4. 部署 Snova c4 服务端到 Cloud Foundry



在终端应用程序上，输入以下一行命令：

cd /the-parth-to/snova-c4-server

你也可以直接把 “snova-c4-server” 文件夹直接拖到 “cd” 命令后面。

然后，一行一行地逐一按照提示输入以下命令：

- vmc target api.cloudfoundry.com
- vmc login (输入你的 Cloud Foundry 用户名和密码)
- vmc push free-nuts (把 free-nuts 替换为你喜欢的任意名字作为 Cloud Foundry 新应用程序)
- Would you like to deploy from the current directory? [Yn]: (输入 y)

- Detected a Java Web Application, is this correct? [Yn]: (输入 y)
- Application Deployed URL [free-nuts.cloudfoundry.com]: (回车)
- Memory reservation (128M, 256M, 512M, 1G, 2G) [512M]: (回车)
- How many instances? [1]: (回车)
- Create services to bind to 'free-nuts'? [yN]: (输入 n)
- Would you like to save this configuration? [yN]: (输入 y)

如果所有结果都显示 OK，那么你就可以打开以下链接的网页：

free-nuts.cloudfoundry.com

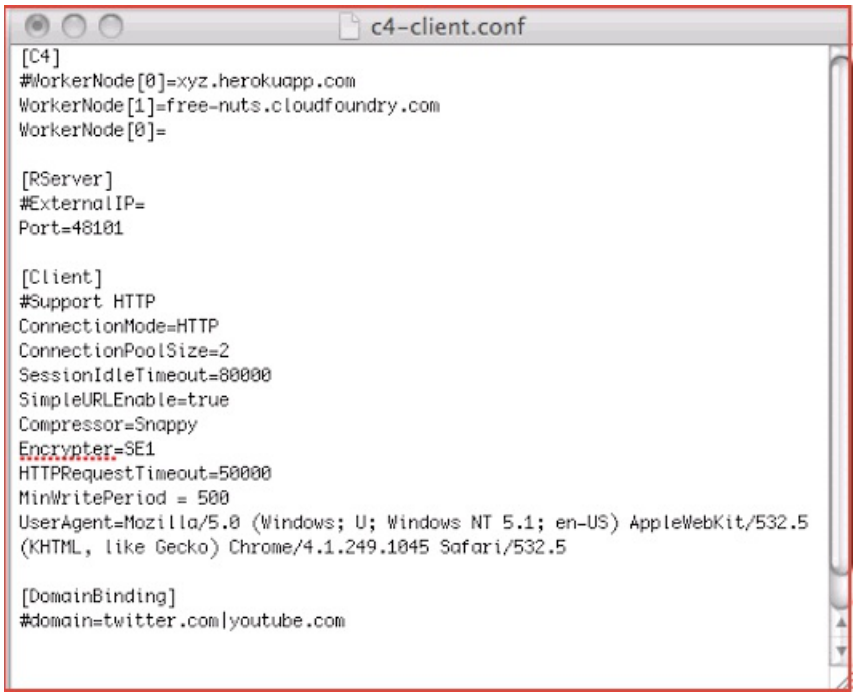
如果能够看到以下的信息：

Welcom to snova-c4 server xxx!

（其中的 Welcom 应该是 Welcome。）

那么就表明 Snova c4 服务端成功部署到 Cloud Foundry 了。

5. 部署 Snova c4 客户端



通过以下路径找到并打开 “c4-client.conf” 文件：

.../snova-xxx/plugins/c4/conf/c4-client.conf

然后删除 “WorkerNode [1]” 前面的 “#” 号并把后面的 “xyz” 改成你在第 4 个步骤创建的 Cloud Foundry 应用程序名称（例如 free-nuts）。

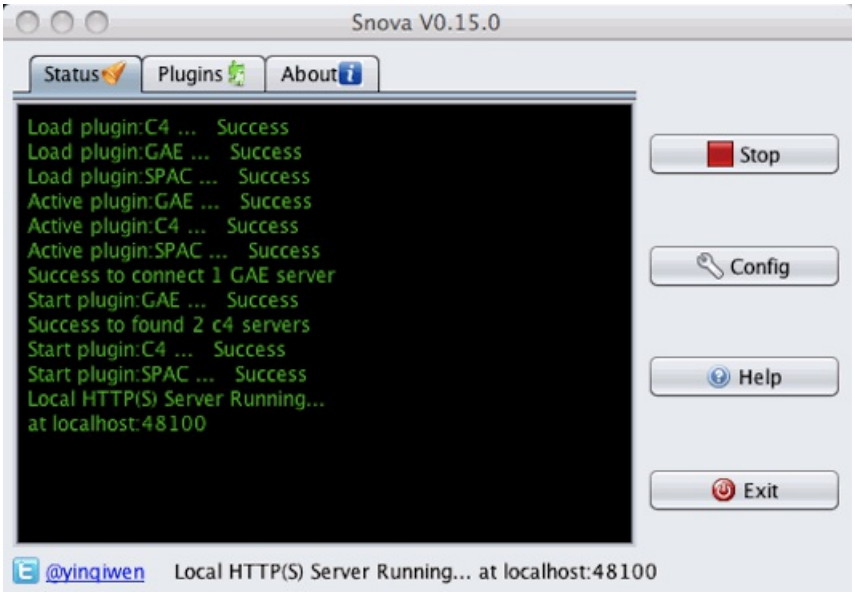
6. 修改 snova.conf 文件

通过以下路径找到并打开 “snova.conf” 文件：

.../snova-xxx/conf/snova.conf

然后把 “ProxyService” 的值从 “GAE” 改成 “C4” 并保存。

7. 启用 Snova 客户端



完了之后，启用 Snova 客户端，如果能够看到以下一行信息：

Start plugin:C4 … Success

那么恭喜你，你可以通过 Snova 访问任意被墙的网站，不管是使用 HTTP 链接的，还是 HTTPS 链接的。

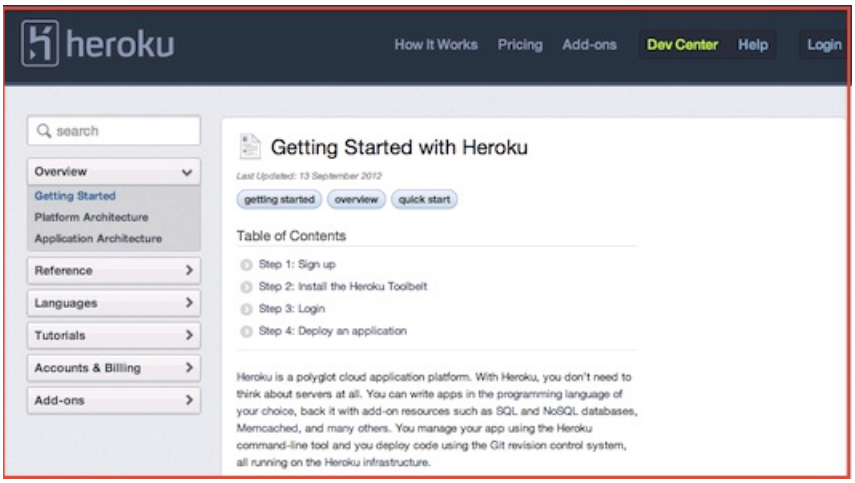
四、如何在 Heroku 上安装和使用 Snova 代理

Snova 虽然可以直接在 GAE 上运行，但是只有运行在 Cloud Foundry、Heroku、OpenShift 和／或其他 PaaS 平台上才能够正常访问 HTTPS 链接页面。

上一篇文章介绍了 Cloud Foundry，这篇文章将介绍 Heroku。

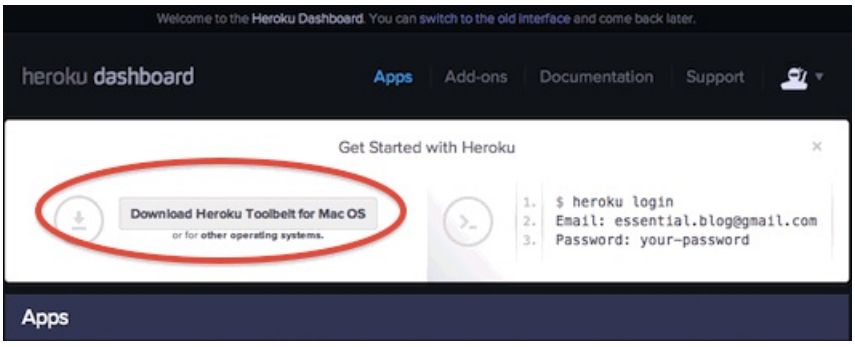
由于都是 PaaS 平台，Heroku 的安装和使用方法和 Cloud Foundry 的差不多，具体步骤如下：

1. 创建一个 Heroku 帐号



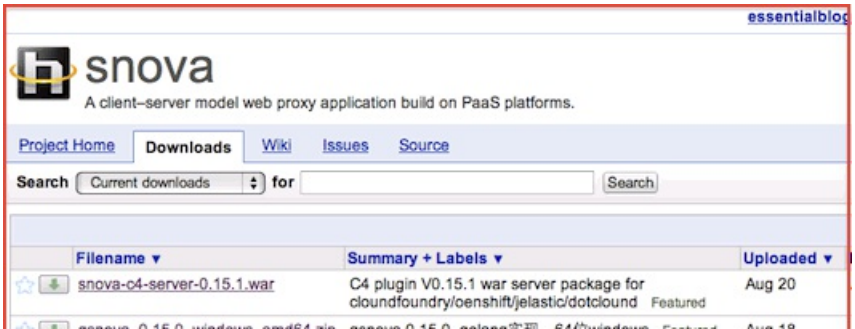
在 这个 Heroku 页面，输入你的邮箱地址并注册一个帐号。

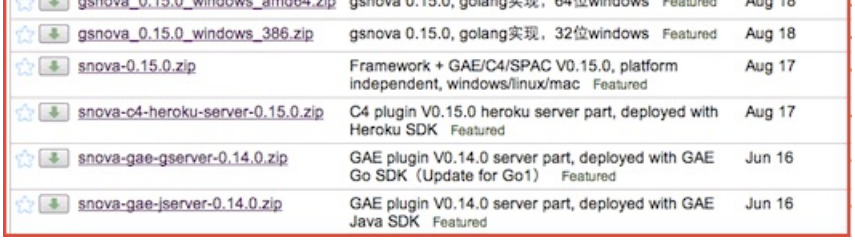
2. 安装 Heroku Toolbelt



注册成功之后，你会收到一封邮件，点击里面的那个长长的链接，然后在打开的页面下载 Heroku Toolbelt 软件并安装。

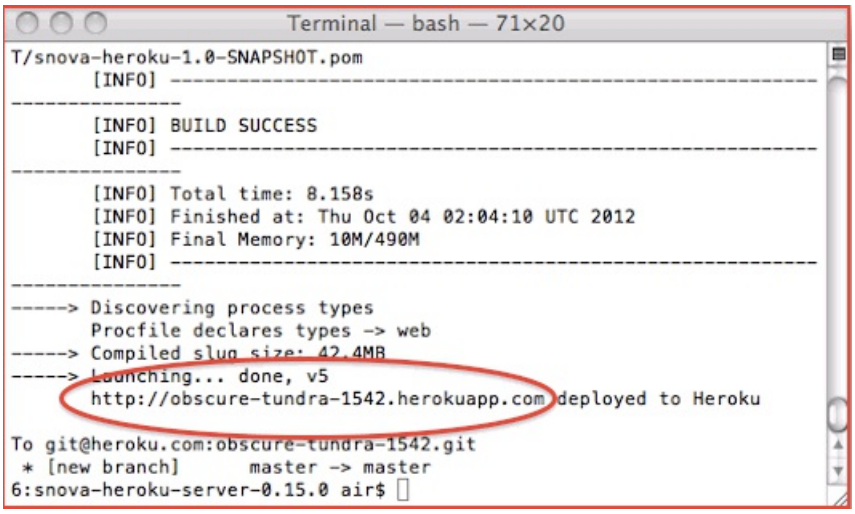
3. 下载 snova-c4-heroku-server-xxx.zip





在 Snova **的**下载（Downloads）页**面，下**载 “snova-c4-heroku-server-xxx.zip” **文件并解**压缩。

4. 部署 Snova c4 服务端到 Heroku



打开 Mac **上的**终**端**应**用程序或者** Windows **上的命令提示符，并**输**入以下一行命令**：

cd /the-parth-to/snova-c4-heroku-server-xxx

你也可以直接把 “snova-c4-heroku-server-xxx” **文件**夹**拖到** “cd” **命令后面。**

然后，一行一行地逐一输**入以下命令**：

- heroku login (**回**车**后需要**输**入你的** Heroku 帐**号和密**码)
- git init
- git add .
- git commit -m "init"
- heroku create --stack cedar
- git push heroku master
  在显**示**结**果的最后，你会**发现**一行**类**似以下的**链**接**：

  http://obscure-tundra-1542.herokuapp.com/

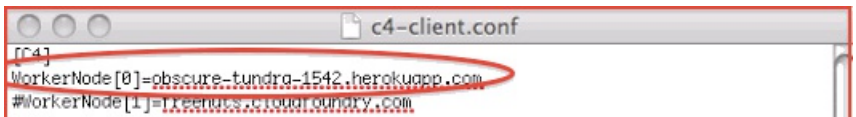
  打开该链**接**页**面，如果能看到以下一行文字**：

  Welcom to snova-c4 server xxx!

  （**其中的** Welcom 应该**是** Welcome。）

  那么就表明 Snova c4 **服**务**端成功部署到** Heroku **了。**

5. 配置 Snova c4 客户端



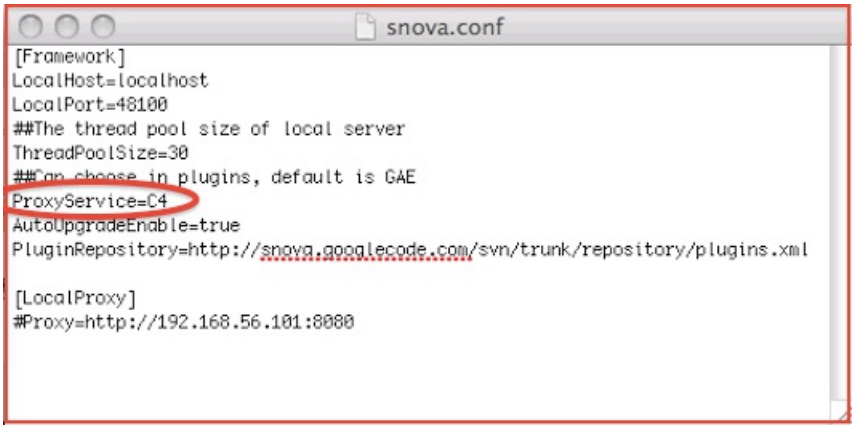
```
#WorkerNode[0]=

[RServer]
#ExternalIP=
Port=48101

[Client]
#Support HTTP
ConnectionMode=HTTP
ConnectionPoolSize=2
SessionIdleTimeout=80000
SimpleURLEnable=true
Compressor=Snappy
Encrypter=SE1
HTTPRequestTimeout=50000
MinWritePeriod = 500
UserAgent=Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5
(KHTML, like Gecko) Chrome/4.1.249.1045 Safari/532.5

[DomainBinding]
#domain=twitter.com|youtube.com
```

通过以下路径找到并打开 “c4-client.conf” 文件：

.../snova-xxx/plugins/c4/conf/c4-client.conf

然后删除第一行 “WorkerNode [0]” 前面的 “#” 号并把后面的 “xyz” 改成你在第 4 个步骤得到的 Heroku 子域名（例如 “obscure-tundra-1542”）。

6. 修改 snova.conf



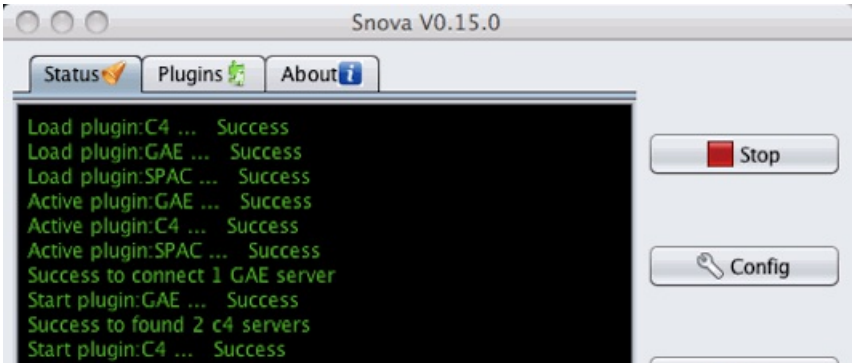
通过以下路径找到并打开 “snova.conf” 文件：

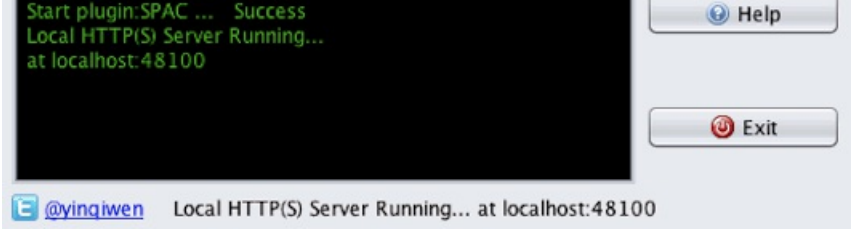
.../snova-xxx/conf/snova.conf

然后把 “ProxyService” 的值从 “GAE” 改成 “C4” 并保存。

如果该文件之前已经修改过，那就可以忽略这个步骤。

7. 启用 Snova 客户端





完了之后，启用 Snova **客户端，如果能够看到以下一行信息**:

Start plugin:C4 … Success

那么恭喜你，你可以通过 Snova **访问任意被墙的网站，不管是使用** HTTP **链接的，还是** HTTPS **链接的。**

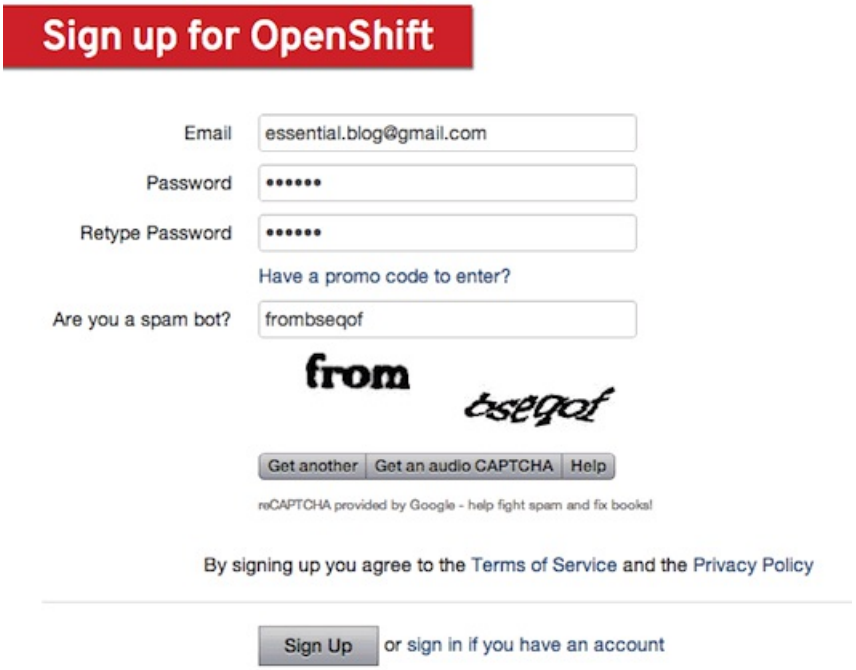
五、如何在 OpenShift 安装和使用 Snova 代理

关于 Snova 代理的安装和使用方法，其官方网站都有介绍，你如果能够看明白，就可以忽略这篇文章。

但是，讲到如何部署 C4 插件到 OpenShift，官方的介绍就有点问题了，例如，“rhc-create-domain” 这样的命令将会无效，“jbossas-7.0” 应该是 “jbossas-7”，“git commit –m” 应该是 “git commit -a -m”，等等。

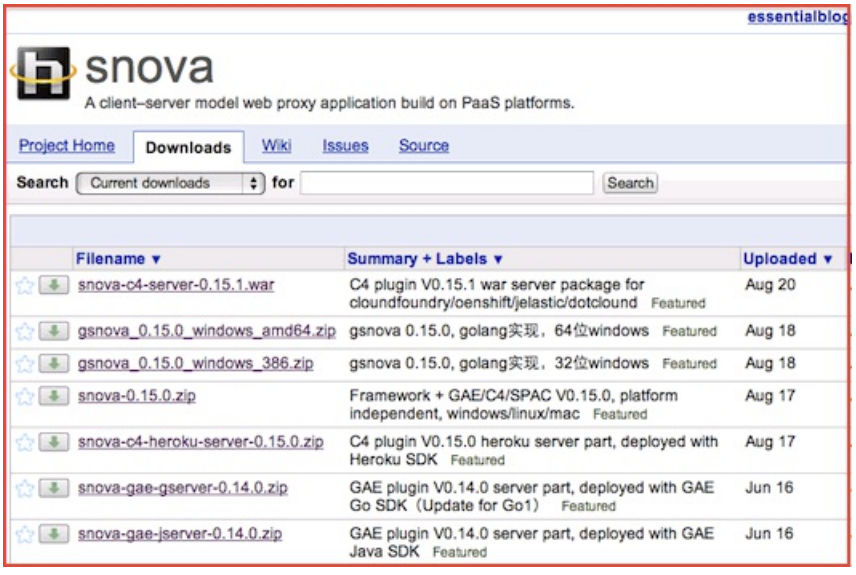
下面将根据个人的实际操作，详细介绍如何在 OpenShift 安装和使用 Snova 代理。

1. 创建一个 OpenShift 帐号



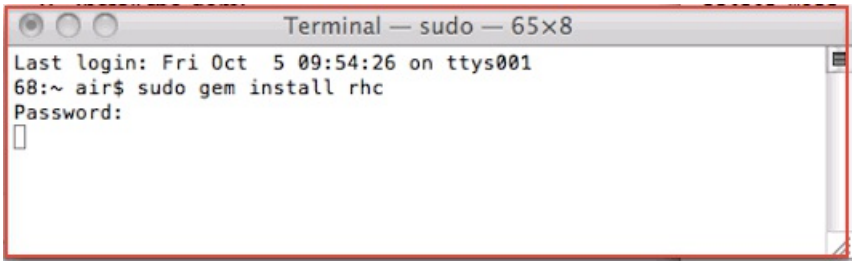
在 OpenShift 的注册页面，输入你的邮箱地址、任意密码和 CAPTCHA 验证码创建一个免费帐户。

2. 下载 snova-c4-server-xxx.war 文件



在 Snova 的下载(Downloads)页面，下载 “snova-c4-server-xxx.war” 文件并把它放到一个新的空文件夹，例如下面步骤将会用到的 “openshift”。

3. 安装 rhc



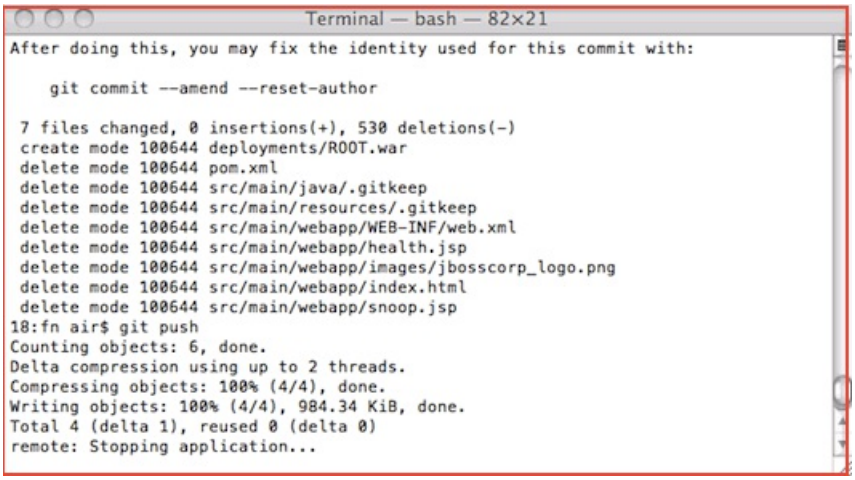
Rhc 是部署 C4 插件到 OpenShift 的必须命令。

在 Mac 系统上，你可以直接在终端应用程序上输入以下一行命令：

sudo gem install rhc

在 Windows 和 Linux 上，你可以参考 OpenShift 网站的官方安装教程。

4. 部署 Snova c4 插件到 OpenShift



打开终端应用程序或者命令提示符，输入以下一行命令进入 “openshift” 文件夹：

cd /the-parth-to/openshift

或者直接把 “openshift” 文件夹拖到 “cd” 后面。

然后，一行一行地逐一输入以下命令：

命令 1：

rhc domain create -n freenutsdot -l xxx@gmail.com -p 123456

(该命令将会创建一个二级域名 “freenutsdot.rhcloud.com”。记得把 “freenutsdot” 改成你喜欢的名字，把 “xxx@gmail.com” 改成你注册的邮箱地址，并把 “123456” 改成你的 OpenShift 帐户密码。)

命令 2：

rhc app create -a fn -t jbossas-7 -p 123456

(该命令将创建一个应用程序，它的名称将会和前面所创建的域名一起构成应用程序的 OpenShift 域名（例如 fn-freenutsdot.rhcloud.com）。记得把 “fn” 改成你喜欢的应用程序名称，把 “123456” 改成你的 OpenShift 帐户密码，然后你就可以在当前文件夹（例如 “openshift”）看到一个和该应用程序同名的文件夹（例如 “fn”）。

命令 3:

cd fn

(该**命令将允**许**你在前面所**创**建的**应**用程序文件**夹**里面**执**行下面的命令。)

命令 4:

mv ../snova-c4-server-xxx.war deployments/ROOT.war

(该**命令将把** “snova-c4-server-xxx.war” **文件移到** “fn” **文件**夹**的** “deployments” **目**录**里面并且重命名**为 “ROOT.war”。)

命令 5:

git rm -r src pom.xml

(该**命令将**删**除** “src” **文件**夹**和** “pom.xml” **文件**。)

命令 6:

git init

(该**命令将初始化** “fn” **文件**夹。)

命令 7:

git add .

(该**命令将添加** “ROOT.war” **文件**。)

命令 8:

git commit -a -m "haha"

(该**命令将确**认**和**显**示前面所做的修改。你可以把其中的** “haha” **替**换**成任意字符**。)

命令 9:

git push

(该**命令将会把** “ROOT.war” **部署到你的** OpenShift **应用程序**。)

如果结**果没有**显**示**错误，**那么**，**你就可以**访问**以下**链**接的**页**面**:

http://fn-freenutsdot.rhcloud.com/

记**得把上面的** “fn-freenutsdot” **改成你的**应**用程序的** OpenShift **域名**。

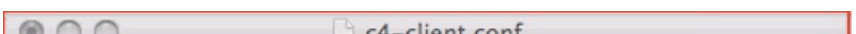
如果页**面**显**示以下内容**:

Welcom to snova-c4 server xxx!

（**其中的** Welcom 应该**是** Welcome。）

那么就表明 Snova c4 **插件成功部署到** OpenShift **了**。

5. 部署 Snova c4 客户端



```
[C4]
#WorkerNode[0]=xyz.herokuapp.com
#WorkerNode[1]=xyz.cloudfoundry.com
WorkerNode[0]=fn-freenutsdot.rhcloud.com

[RServer]
#ExternalIP=
Port=48101

[Client]
#Support HTTP
ConnectionMode=HTTP
ConnectionPoolSize=2
SessionIdleTimeout=80000
SimpleURLEnable=true
Compressor=Snappy
Encrypter=SE1
HTTPRequestTimeout=50000
MinWritePeriod = 500
UserAgent=Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5
(KHTML, like Gecko) Chrome/4.1.249.1045 Safari/532.5

[DomainBinding]
#domain=twitter.com|youtube.com
```

假设你之前已经在 GAE **上部署过** Snova，**那么你就可以通过以下路径找到并打开** “c4-client.conf” **文件**：

.../snova-xxx/plugins/c4/conf/c4-client.conf

在最后那个 “WorkerNode [0]” **一行**，**输入你的** OpenShift **应用程序域名** (**例如** “fn-freenutsdot.rhcloud.com”) **。**

由于 Snova **支持同时使用多个** C4 **插件**，**所以**，**在同一个** “c4-client.conf” **文件里面**，**你还可以添加** Cloud Foundry **和／或** Heroku **应用程序的域名**，**只要** “WorkerNode” **后面中括号里面的数字互不相同就可以了。**

6. 修改 snova.conf 文件

snova.conf

```
[Framework]
LocalHost=localhost
LocalPort=48100
##The thread pool size of local server
ThreadPoolSize=30
##Can choose in plugins, default is GAE
ProxyService=C4
AutoUpgradeEnable=true
PluginRepository=http://snova.googlecode.com/svn/trunk/repository/plugins.xml

[LocalProxy]
#Proxy=http://192.168.56.101:8080
```

通过以下路径找到并打开 “snova.conf” **文件**：

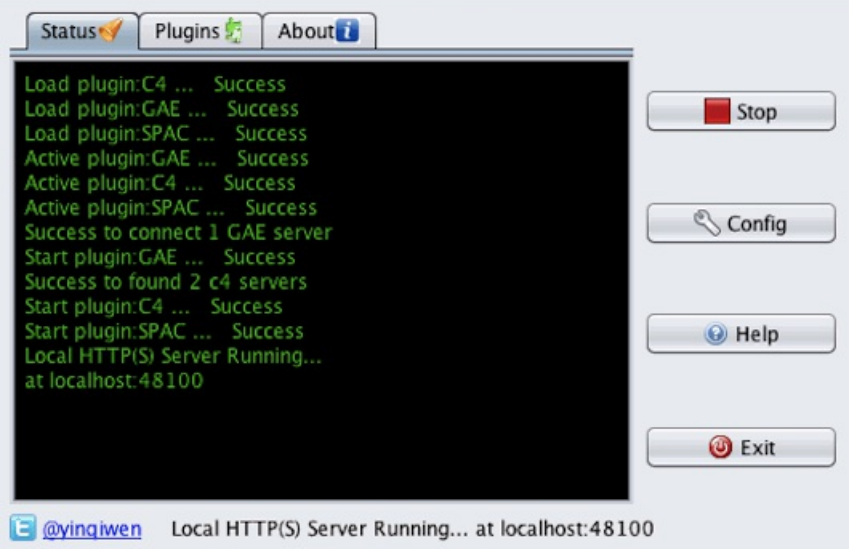
.../snova-xxx/conf/snova.conf

然后把 “ProxyService” **的值从** “GAE” **改成** “C4” **并保存。**

如果该文件之前已经修改过，**那就可以忽略这个步骤。**

7. 启用 Snova 客户端

Snova V0.15.0



完了之后，启用 Snova **客户端，如果能**够**看到以下一行信息**：

Start plugin:C4 … Success

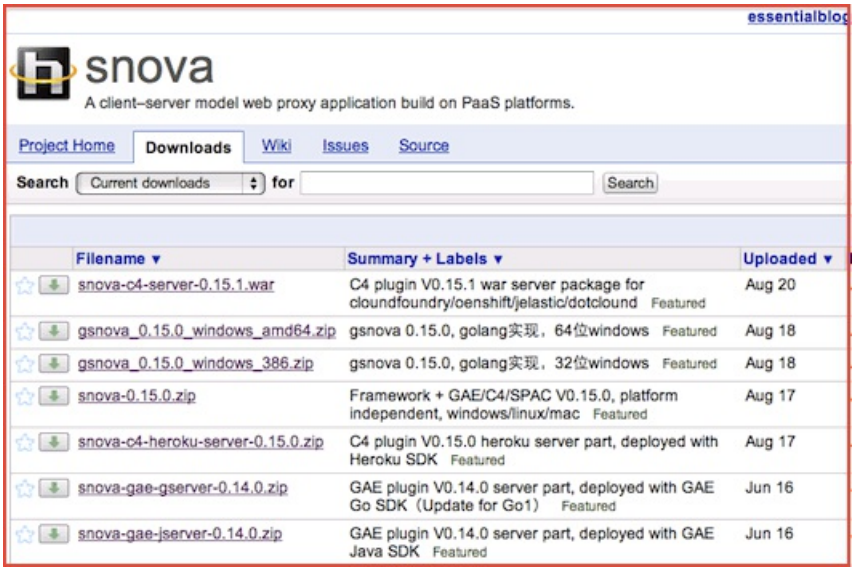
那么恭喜你，你可以通过 Snova 访问**任意被**墙**的网站，不管是使用** HTTP 链**接的**，还**是** HTTPS 链**接的。**

六、如何在 Jelastic 上安装和使用 Snova 代理

如前面提到的，你可以在 Cloud Foundry、Heroku、OpenShift 以及／或者 Jelastic 平台上安装 Snova C4 插件，然后通过它访问任意被墙的网站。

在这四个 PaaS 平台中，Jelastic 是最容易安装 C4 插件的，因为你不需要输入任何的命令行，具体步骤如下：

1. 下载 snova-c4-server-xxx.war 文件

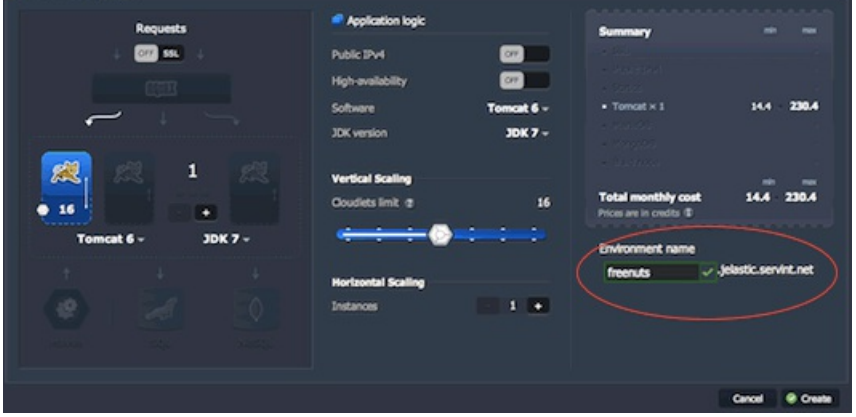


在 Snova 的下载(Downloads)页面，下载 “snova-c4-server-xxx.war” 文件，如果之前已经下载了，就可以忽略这个步骤。

2. 创建一个 Jelastic 帐户

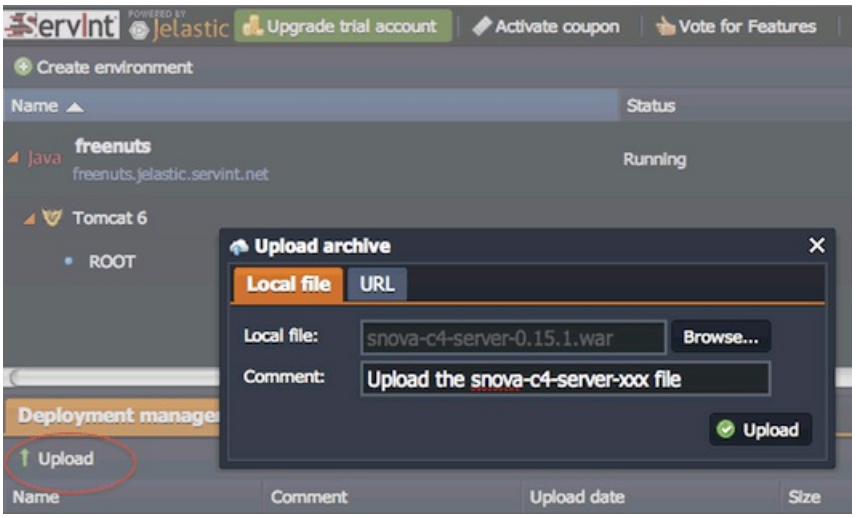
在 Jelastic 首页，输入你的邮箱地址并注册一个帐号，帐号用户名(即你的邮箱地址)和密码将会发到你的邮箱。

3. 创建一个 Jelastic 应用程序域名



登录之后，你可以看到一个“环境的拓扑结构”（Environment topology）窗口，在该窗口上的“环境名字”（Environment name）一栏，你可以输入任意名字（例如“freenuts”），该名字将会构成用来运行 C4 插件的 Jelastic 应用程序域名（例如“freenuts.jelastic.servint.net”），然后点击创建（Create）按钮。

4. 上传 snova-c4-server-xxx.war 文件



域名创建之后，点击当前窗口的“上传”（Upload）按钮，浏览并上传前面下载到的“snova-c4-server-xxx.war”文件。

顺便一提，在上传窗口的“评论”（Comment）一栏，你可以输入任意信息。

5. 部署 Snova c4 插件到 Jelastic

把光标移到上传文件“snova-c4-server-xxx.war”的名字上面，你将会看到旁边有一个黄色的图标，点击该图标，你可以看到前面第 3 步所创建的

环境名字（例如 “freenuts”），点击该名字，你会看到一个弹窗，点击弹窗上面的 “部署” 按钮，你就可以把 C4 插件安装到 Jelastic 上了。

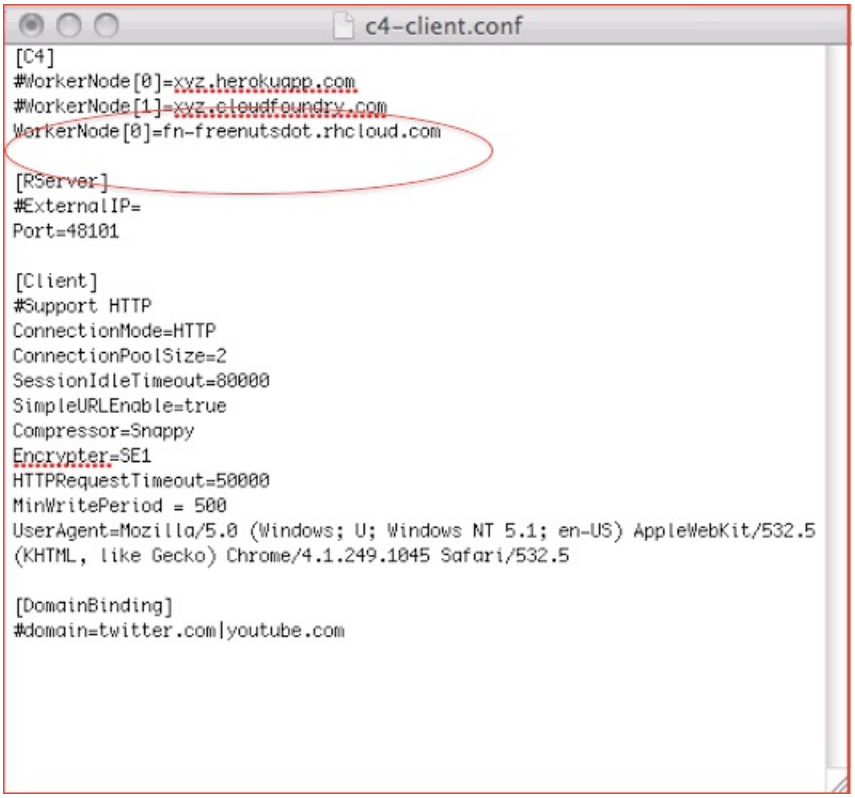
然后，访问你的 Jelastic 应用程序域名（例如 “freenuts.jelastic.servint.net”）页面，如果能看到以下内容：

Welcom to snova-c4 server xxx!

（其中的 Welcom 应该是 Welcome。）

那么就表明安装成功。

6. 配置 Snova c4 客户端



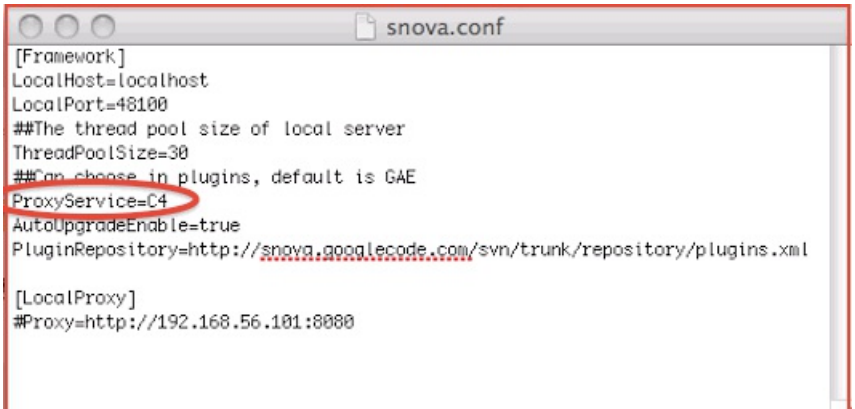
假设你之前已经在 GAE 上部署过 Snova，那么你就可以通过以下路径找到并打开 “c4-client.conf” 文件：

…/snova-xxx/plugins/c4/conf/c4-client.conf

在最后那个 “WorkerNode [0]” 一行，输入你的 Jelastic 应用程序域名（例如 “freenuts.jelastic.servint.net”）并保存。

由于 Snova 支持同时使用多个 C4 插件，所以，在同一个 “c4-client.conf” 文件里面，你还可以添加 Cloud Foundry、Heroku 和／或 OpenShift 应用程序的域名，只要 “WorkerNode” 后面中括号里面的数字互不相同就可以了。

7. 修改 snova.conf 文件



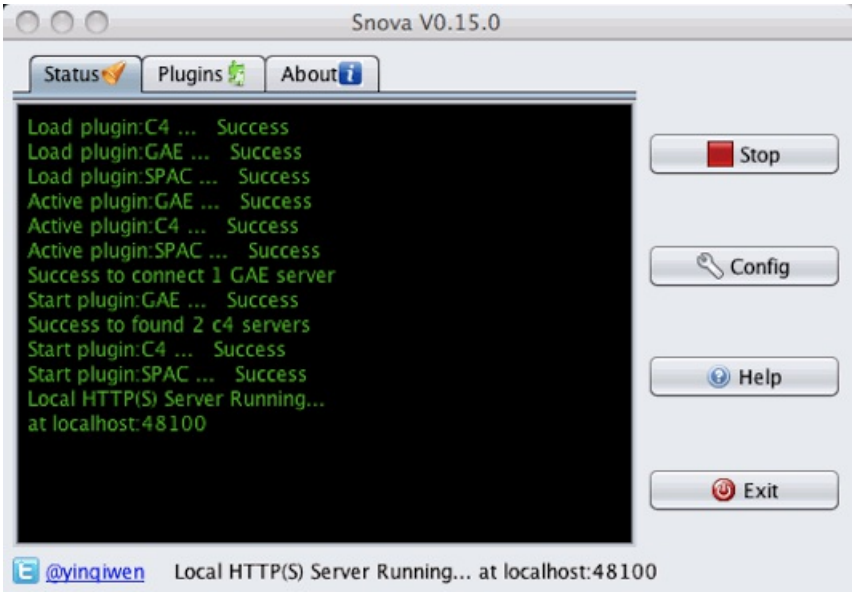
通过以下路径找到并打开 “snova.conf” 文件：

…/snova-xxx/conf/snova.conf

然后把 “ProxyService” 的值从 “GAE” 改成 “C4” 并保存。

如果该文件之前已经修改过，那就可以忽略这个步骤。

8. 启用 Snova 客户端



完了之后，启用 Snova 客户端，如果能够看到以下一行信息：

Start plugin:C4 … Success

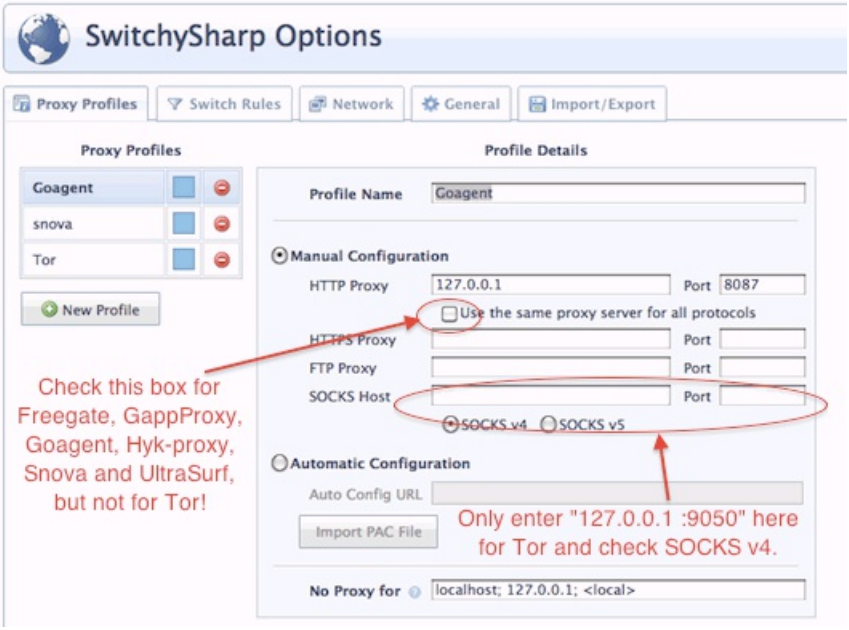
那么恭喜你，你可以通过 Snova 访问任意被墙的网站，不管是使用 HTTP 链接的，还是 HTTPS 链接的。

第八节：可自动配置浏览器代理的两个免费扩展

无论是自由门、Tor、Snova 或者其他任意的客户端代理或者 SSH 代理，使用之前需要先为浏览器的网络连接配置代理。

虽然大家的代理 IP 地址都是 127.0.0.1，但是端口（Port）通常互不相同，比如自由门的是 8580，Tor 的是 9050，Snova 的是 48100，等等，与其手动一个一个地配置和不断地更换端口，不如通过下面这两个免费扩展自动配置：

1. SwitchySharp



SwitchySharp（或者 Proxy SwitchySharp）是一个 Chrome 扩展。

安装之后，你会看到一个新的 SwitchySharp Options 标签页，在该标签页上，你可以输入代理的名字作为 Profile Name，然后输入其代理地址和端口。

对于自由门、无界、GappProxy、Goagent、Hyk-proxy 和 Snova，你可以在 HTTP Proxy 一栏输入 127.0.0.1 和对应的端口，并勾选 “Use the same proxy server for all protocols” 选项；而对于 Tor 和 SSH 代理，你只需要在 SOCKS Hosts (SOCKS v4) 一栏输入 IP 地址 127.0.0.1 以及端口 9050 或 7070 就可以了。

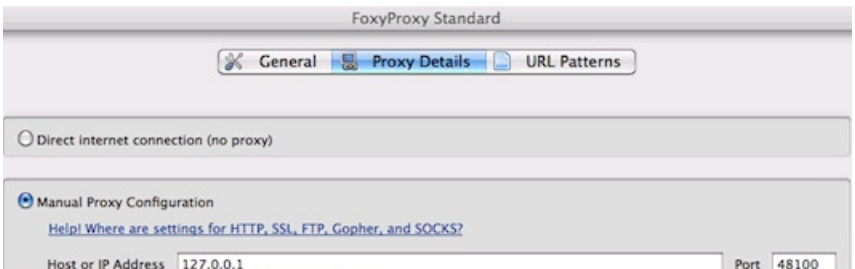
点击侧边栏上的 “New Profile” 按钮可以添加另外一个代理。

完了之后，点击 “Save” 按钮，然后你就可以点击 Chrome 浏览器工具栏上的 SwitchySharp 图标，并选择一个代理翻墙。

额外收获：

Proxy Switchy 也是一款非常类似于 SwitchySharp 的免费 Chrome 扩张，只是没有那么受欢迎。

2. FoxyProxy Standard



FoxyProxy Standard 是一款 Firefox 扩展。

安装之后，你可以分别在浏览器的导航栏和扩展工具栏上看到该扩展图标，点击该图标，然后再点击 “Add New Proxy” 按钮就可以开始添加代理了。

对于自由门、无界、GappProxy、Goagent、Hyk-proxy 和 Snova，你只需要在当前 “Proxy Details” 标签页的 “Host or IP Address” 一栏输入 127.0.0.1 和对应的端口；而对于 Tor 和 SSH 代理，你还需要勾选 “SOCKS proxy?” 和 “SOCKS v4/4a” 这两个选项。

为了方便记住以上代理配置所对应的软件，你可以在 “General” 标签页的 “Proxy Name” 一栏输入软件名称。

完了之后，点击 “OK” 按钮，然后你会看到一个弹窗以及下面的提示：

You didn't enter and enable any whitelisted (inclusive) URL patterns. This means the proxy won't be used unless FoxyProxy is set to "Use Proxy tor for all URLs". Continue anyway?

这个提示是说，你没有设置黑白名单，所以，该代理启用的时候将会用于所有的网页，你可以不需要理它，直接点击 “OK” 按钮，然后就可以在 “Select Mode” 选择该代理翻墙。

额外收获

如果要找替代品，AutoProxy 将是一个非常好的选择。

以上两个扩展里面，不管使用哪一个，你都可以设置一些规则（即黑白名单），只允许某些网页通过代理访问，或者只允许某些网页不通过代理访问，这样做的一个好处是，FoxyProxy Standard 不会再问你是否继续（Continue anyway?）了。

第三章：免费 VPN

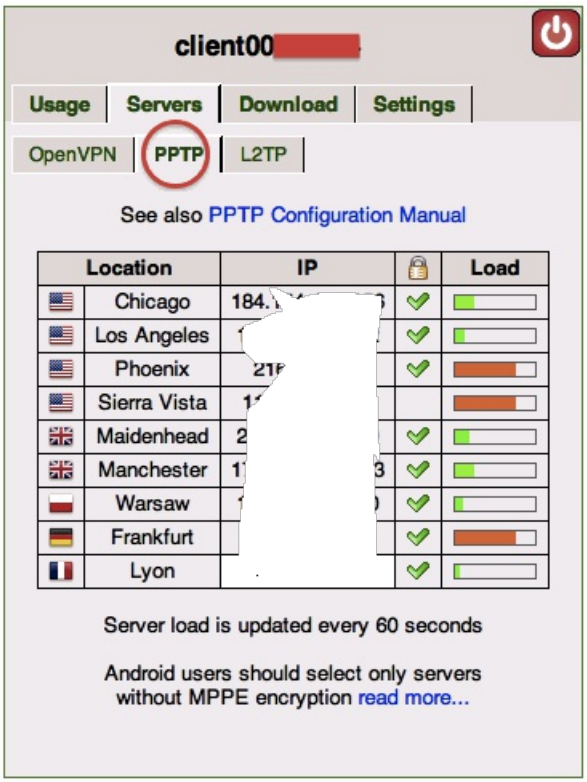
VPN（Virtual Private Network，虚拟私人网络），主要有 PPTP、L2TP 和 OpenVPN 这三种类型，而免费的基本上都是 PPTP 类的和 OpenVPN 类的。

第一节：10 款免费的 PPTP VPN

作为一种常见的 VPN 协议，PPTP (Point-to-Point Tunneling Protocol，点对点隧道协议) 的搭建非常简单。

但是搭建该协议所需要的服务器，不管是虚拟专用服务器、独立服务器、还是云服务器，其价格却不便宜，所以，很少有人愿意提供免费的 VPN 服务，不过庆幸的是，我们仍然有以下 10 款免费的 PPTP VPN 可以用：

1. SecurityKISS



在 SecurityKISS 网站的任意一个下载页面，你只要输入邮箱地址就可以通过邮件获得 2 个 PPTP/L2TP VPN 帐号，其中一个是美国的，另外一个是英国的。

除此之外，你还可以通过邮件里面提到的用户 ID 和密码登录 SecurityKISS 网站，并获得更多的来自美国、英国、法国等地区的服务器 IP 地址。而除了 PPTP 和 L2TP 之外，SecurikyKISS 还提供适用于 Windows、Mac 和 Linux 系统的 OpenVPN 服务。

顺便一提，不管你使用哪种或者多少个 VPN 服务，每天的免费流量最多 300M。

2. Super Free VPN

打开 Super Free VPN 网站，你就可以看到它所提供的免费 PPTP VPN 的帐号，其中服务器和用户名是固定的，而密码则可长达 8 个小时才更新

一次。

顺便一提，由于该网站已经被墙，你或许需要将它的服务器 “superfreevpn.com” 改为以下对应的 IP 地址：

69.60.121.29

3. JustFreeVPN

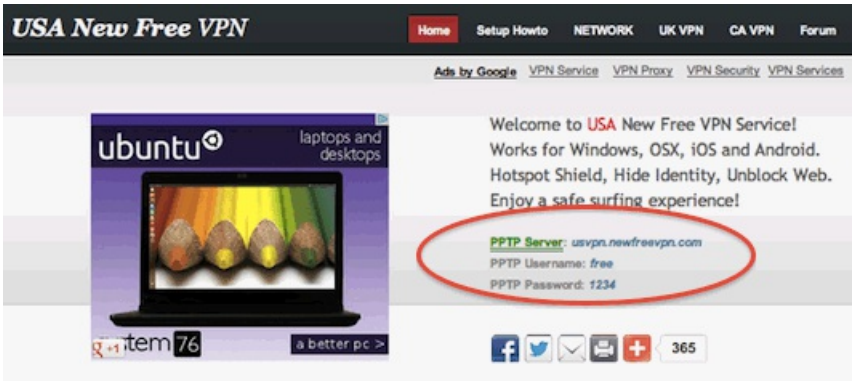
一打开 JustFreeVPN 网站，你就可以看到 3 个免费的 PPTP VPN 帐号，其中一个是美国的、一个是英国的、还有一个是加拿大的。

不同的帐号，服务器不同，用户名都是 “justfreevpn”，密码不同并且不定期更新。

4. UFreeVPN

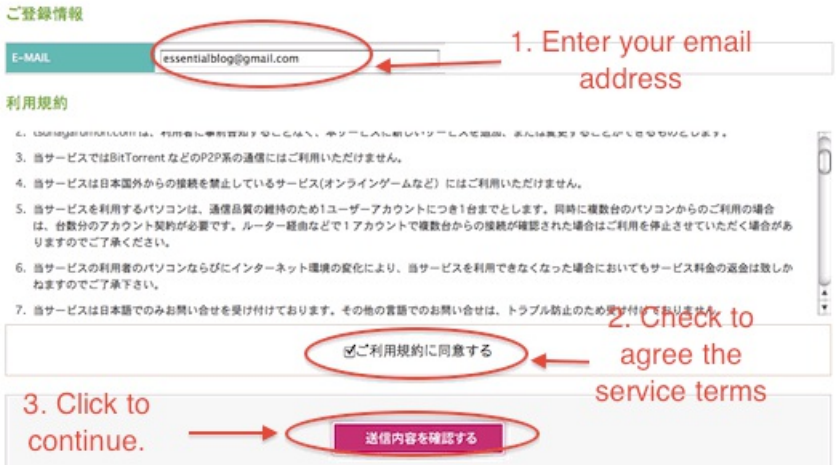
UFreeVPN 网站同样提供一个美国的、一个英国和一个加拿大的免费 PPTP VPN 帐号，其中每个帐号的服务器不同，用户名和密码相同并且都是固定不变的，所以不需要经常更换密码。

5. NewFreeVPN



在 NewFreeVPN 网站三个不同的网页上，你可以发现三个不同的免费 PPTP VPN 帐号，其中一个是美国的、一个是英国的、还有一个是加拿大的，每个帐号的服务器不同，但是用户名都是 “free”，而密码都是 “1234”。

6. Tsunagarumon



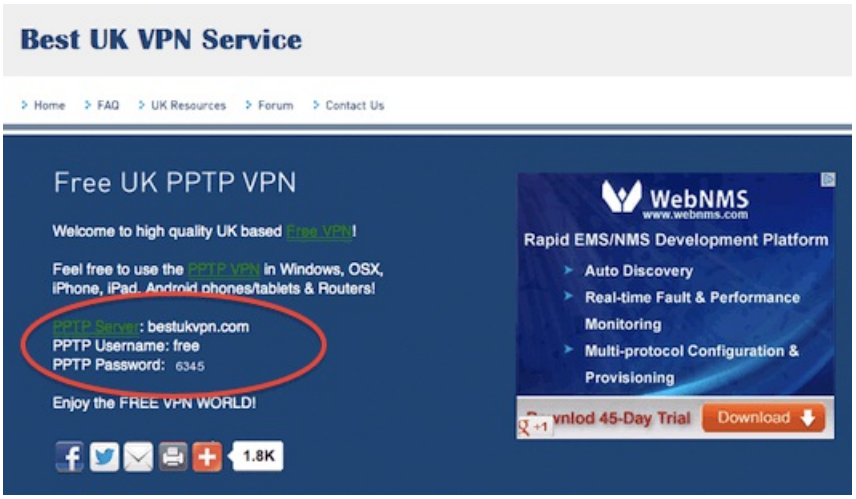
Tsunagarumon 网站是日文的，并且需要注册，但是过程却很简单。你只需要在它的申请页面，输入邮件地址，选择同意服务条款，点击红色按钮，再次确认邮件地址，如果准确无误，点击下一个红色按钮。

完了之后，进入你的收件箱，打开来自 Tsunagarumon 的邮件，并点击里面的链接，然后你就可以收到免费的 PPTP VPN 帐号信息了。

7. FreeCanadaVPN

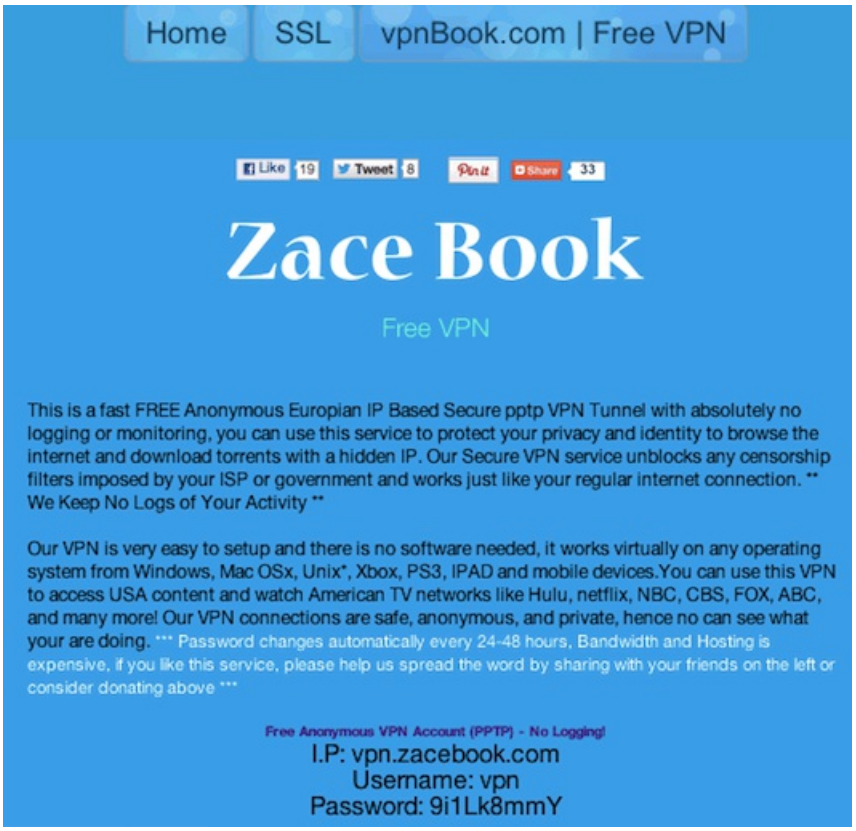
FreeCanadaVPN 是一个免费的加拿大 VPN，服务器是 “freecanadavpn.com”，用户名是 “free”，密码则不定期更新于页面的右上角。

8. BestUKVPN



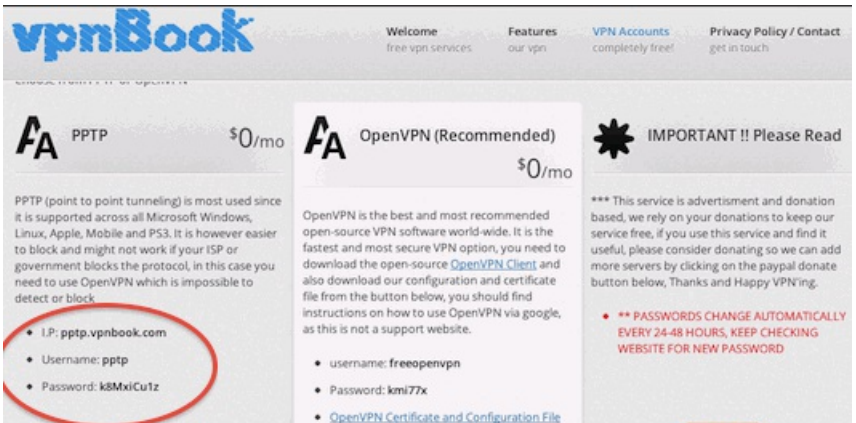
顾名思义，BestUKVPN 是一个英国的 VPN，其中服务器是 “bestukvpn.com”，用户名是 “free”，密码则不定期更新。

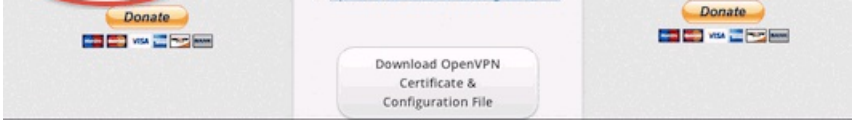
9. [Zace Book]



Zace Book 是一款罗马尼亚的免费 VPN，其服务器是 “vpn.zacebook.com”，用户名是 “VPN”，密码一两天更新一次。

10. [VPN Book]





VPN Book 同样是罗马尼亚的，其服务器是 “pptp.vpnbook.com”，用户名是 “pptp”，密码一两天更新一次。

除了 PPTP，VPN Book 还提供免费的 OpenVPN 服务。

以上 10 款免费的 PPTP VPN 服务里面，SecurityKISS 是最好的，可惜有流量限制，所以，还是那句话，多一个 VPN，翻墙就多一份保障。

额外收获：

如同文章里面提到的 “Super Free VPN” 那样，如果其他某个 PPTP VPN 的服务器域名被墙，你可以将它们改为对应的 IP 地址。

第二节：如何设置 PPTP VPN

有了免费的 PPTP VPN 帐号之后，如何通过它在电脑、手机或者平板电脑上翻墙呢？

由于一个有效的 PPTP VPN 帐号只需要以下三个数据：

- 1、服务器（主机名或者 IP 地址），
- 2、用户名，
- 3、密码。

所以，设置 PPTP VPN 的关键一步就是找到输入以上数据的地方，该地方会因电子设备、操作系统、新旧版本的不同而不同，其中 Windows、Mac、iOS 和 Android 系统常见或者最新版本的如下：

1、Windows XP

网络连接 — 创建一个新的连接 — 连接到我的工作场所的网络 — 虚拟专用网络连接

2、Windows Vista

开始 — 连接到 — 设置连接或网络 — 连接到工作区 —使用我的 Internet 连接(VPN)

3、Windows 7

网络和共享中心 — 设置新的连接或网络 — 连接到工作区

4、Mac OS X

系统设置 — 网络 — 创建新服务(＋)

需要特别注意的是，在 Mac OS X 系统上添加了 VPN 之后，一定要点击“高级”按钮，并勾选“使用VPN连接发送所有流量”。

5、iPhone

设置 — VPN — 添加 VPN 配置

6、Android

设置 — 无线和网络 — 虚拟专用网络设置 — 添加虚拟专用网

以上的路径可能会因为对应的设备的版本不同而有点不一样，但是大同小异，只要能找到“VPN”或者“虚拟专用网络”这样的字眼并把 PPTP VPN 的帐号信息输进出就行了。

关于更详细的、更多电子设备的、更多系统版本的 PPTP VPN 设置教程，你可以参考 StrongVPN（英文），或者 vpnonly.us ／ 3qvpn.info（中文）。

备注：

1、大多数的 PPTP VPN 的服务器都只是提供主机名，如果该域名被墙，你可以尝试把它改成对应的 IP 地址。

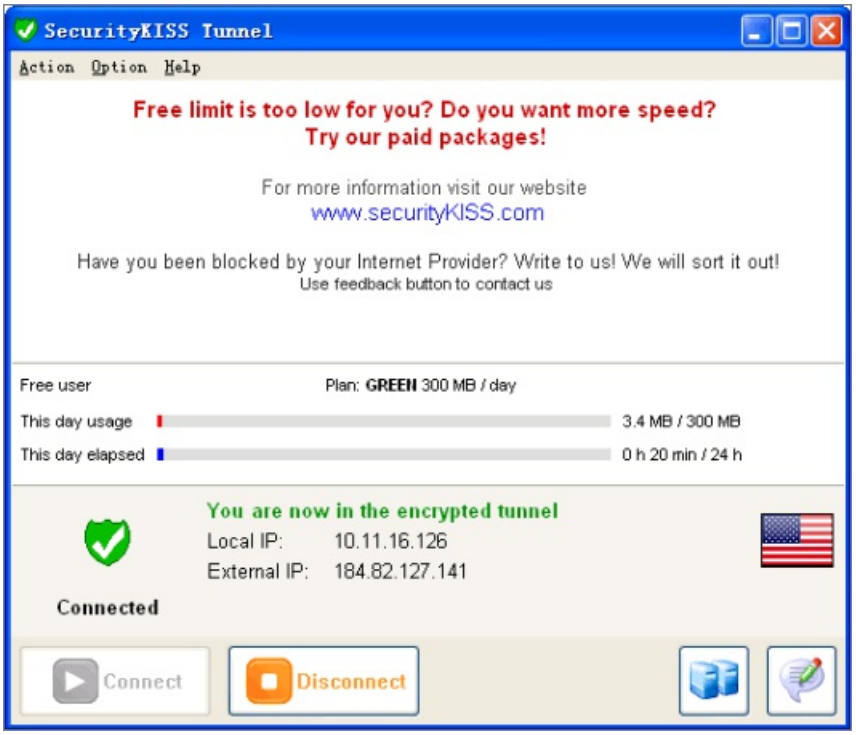
2、L2TP VPN 的设置和 PPTP VPN 的设置基本一样，只是需要多输入一个“共享密钥”（Shared Secret）。

第三节:6 款免费的 VPN 客户端

与 PPTP VPN 明显不同的是，VPN 客户端(基本上都是基于 OpenVPN 的)需要下载安装才能够使用。

以下是 6 款最强大的免费 VPN 客户端:

1. SecurityKiss



如之前所述，SecurityKiss 提供免费的 PPTP/L2TP VPN 帐号，但是要注册才能获取。

除此之外，它还提供适用于 Windows、Mac 和 Linux 系统的 OpenVPN 服务，这些服务不需要注册，直接下载并安装就可以用了，并且有多个不同的服务器可供选择。

顺便一提，不管你使用哪种或者多少个 VPN 服务，每天的免费流量最多 300M。

2. ProXPN

ProXPN 提供适用于 Windows 和 Mac OS 的 VPN 客户端，下载安装并注册一个免费帐号之后就可以用，没有流量和时间限制，不过访问网站之前会先出现一个 ProXPN 的升级页面，而且只有一个服务器。

除此之外，proXPN 也提供适用于 iOS 和 Android 系统的 PPTP VPN，但不是免费的。

3. Private Tunnel

Private Tunnel 是一款由 OpenVPN 官方推出的适用于 Windows 和 Mac 系统的 OpenVPN 服务，有免费的，也有付费的，其中免费的流量为 100 MB，付费的流量根据价格的不同而不同。

注册一个帐号，下载并安装 OpenVPN Connect 软件，从 San Jose, CA、London 和 Zurich 三个服务器里选择一个就可以连接了。

4. Hotspot Shield

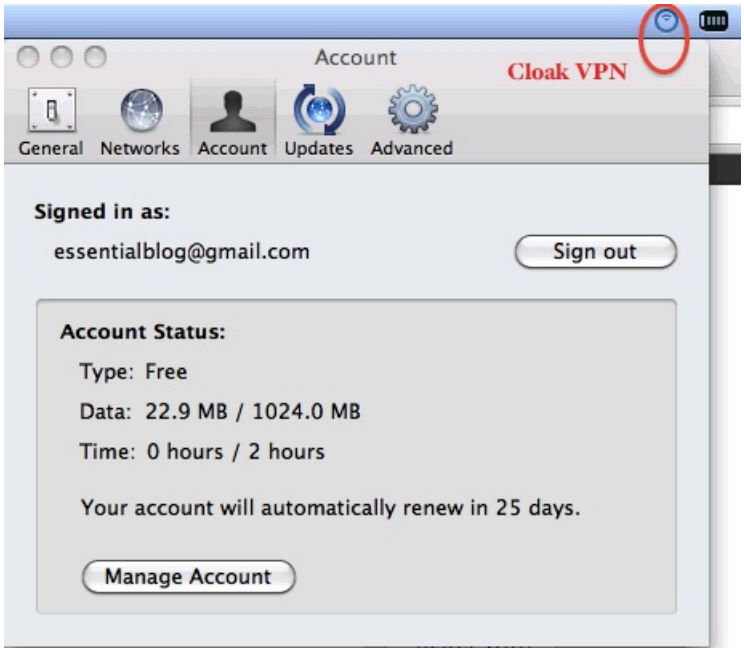
Hotspot Shield 提供 Windows、Mac 以及 Android 版本的免费 VPN 软件，并且支持英文、法文、中文等多种语言。下载安装之后就可以直接使用了，不需要注册，但是通过它访问的每个页面顶部会有广告。

另外，Hotspot Shield 还有 iOS 版本的，不过只有 7 天的免费使用期限。

5. ExpatShield

类似于 Hotspot Shield，ExpatShield 也提供免费的无流量限制的带广告的 VPN 客户端，并且也支持多种语言，但是只适用于 Windows 系统。

6. Cloak VPN



Cloak VPN 可用于 Mac、iPhone 和 iPad。

注册之后，下载电子设备对应的版本并安装就可以直接连接了，免费用户每个月有 1G 的流量和 2 个小时的连接时间。

在以上 6 款免费的 VPN 客户端里面，SecurityKiss 无疑是最好的，但是有时候难免也翻不了墙，所以，还是那句话，多多益善，有备无患。

第四节：如何创建自己的 VPN

如果你有一台虚拟专用服务器（Virtual Private Server，简称 VPS）、独立主机（Dedicated Server）或者云服务器（Cloud Computing），那么就可以自动动手创建 PPTP、L2TP 和 OpenVPN 类型的 VPN。

一、如何创建 PPTP VPN

想搭建自己的 VPN 吗？这篇文章将介绍如何在 VPS（Virtual Private Server，虚拟专用服务器）上快速搭建 PPTP 模式的 VPN。

以下的操作步骤是基于 Mac OS X 系统的终端（Terminal）工具，对 Linux 系统来讲，操作步骤几乎一样，而对 Windows 系统来讲，则须要事先安装一个叫Putty 的工具。

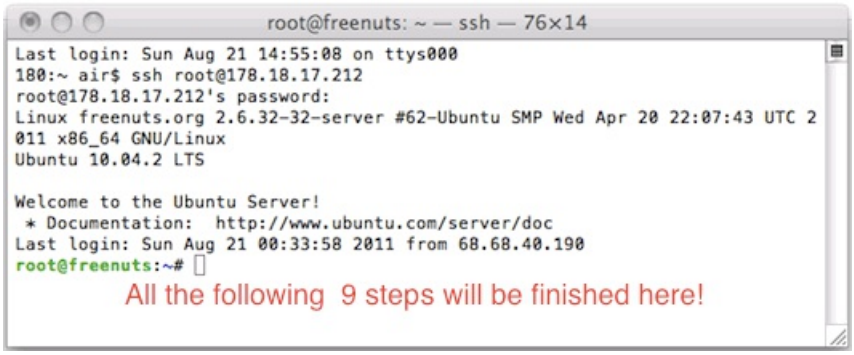
1、购买 VPS

首先，你要拥有一个 Xen（不是 OpenVZ）类型的 VPS，并选择安装 Ubuntu 系统。

顺便提一下，在购买 VPS 的时候，你需要输入一个域名，如果只是为了搭建 VPN，那么这个域名可以随便写，因为它不是必需的。

备注：

VPS 大都不便宜（通常至少每个月要 5 美元），你可以 Google 一下并选择适合的。



2、连接 VPS

打开终端应用程序，并输入以下命令：

ssh root@xxx.xxx.xxx.xxx

记住将 "xxx.xxx.xxx.xxx" 换成 VPS 的 IP 地址，例如 "178.18.17.212"。

按回车后，你将会看到以下问题：

Are you sure you want to continue connecting (yes/no)?

输入 "yes"，回车，输入 VPS 密码，再回车就可以登录 VPS 了。

备注1：

如果你重装系统，那么将会在连接的时候遇到以下错误提示：

Host key verification failed.

这个时候，你需要先输入以下命令：

ssh-keygen -R xxx.xxx.xxx.xxx

记得将 "xxx.xxx.xxx.xxx" 换成你 VPS 的 IP 地址。

备注2：

文章中的所有命令都可以通过复制粘贴的方式输入到终端应用程序。

3、安装 PPTPD

输入以下命令：

apt-get install pptpd

回车后你将会看到以下问题：

Do you want to continue [Y/n]?

输入 "Y"，然后回车。

4、编辑 VPN 接口的 IP 地址

输入以下命令：

nano /etc/pptpd.conf

回车并利用向下键找到以下两行：

#localip 192.168.0.1
#remoteip 192.168.0.234-238,192.168.0.245

将光标分别移到以上两个 "#" 之后，然后按删除键移除它们。

同时按下 "Control" 和 "X" 键，接着按下 "Y" 键，然后回车保存所做的更改。

备注：

除了 "Nano" 命令，你也可以使用 "Vi" 命令，不过后者稍微复杂一点。

5、修改 DNS 地址

输入以下命令：

nano /etc/ppp/pptpd-options

回车并找到以下两行内容：

#ms-dns 10.0.0.1
#ms-dns 10.0.0.2

将以上内容改成：

ms-dns 8.8.8.8
ms-dns 8.8.4.4

(小技巧：你也可以将以上内容复制粘贴到要修改内容的下面。)

改好之后，同时按 "Control" 和 "X" 键，再按 "Y" 键，然后回车保存所做的修改。

备注：

以上所用的 DNS 地址是 Google 的，你也可以换成 OpenDNS 的，即 208.67.222.222 和 208.67.220.220。

6、添加 VPN 帐号

输入以下命令：

nano /etc/ppp/chap-secrets

回车并输入以下内容：

username pptpd password *

例如：

freenuts pptpd 123456 *

备注：

你需要按 Tab 键来创建不同数值之间的空格。

7、IPv4 地址转发

输入以下命令：

nano /etc/sysctl.conf

回车并找到以下一行内容：

#net.ipv4.ip_forward=1

将光标移到 "#" 号后面并按 "Delete" 键移除它。

同时按下 "Control" 和 "X" 键，接着按下 "Y" 键，然后回车保持所做的修改。

8、使转发生效

输入以下命令使得上一个步骤所做的转发得以生效：

sysctl -p

如果一切正常，回车后你将会只看到以下内容：

net.ipv4.ip_forward = 1

9、搭桥

输入以下内容：

iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

然后回车。

10、重启 PPTPD

输入以下命令：

```
/etc/init.d/pptpd restart
```

回车之后，你就可以利用之前所创建的用户名和密码连接 VPS 上的 VPN 翻墙了。

备注：

我无法在 Mac Air OS X 10.6 系统上使用 PPTP 类的 VPN，据说是因为电信封了 PPTP 接口，又据说是该系统本身的问题。

二、如何创建 L2TP VPN

如之前所说，PPTP 类的 VPN 可以在 iPhone 手机上使用，但是不能在 Mac OS X 电脑系统上使用，于是，我需要使用 L2TP/IPSec (L2TP over IPSec，即在 IPSec 上搭建 L2TP) 类的 VPN。

这篇文章将介绍如何在 VPS (Xen)上搭建 L2TP/IPSec 类的 VPN，而你只需要一个 VPS 和一台可以上网的电脑。和 PPTP 的一样，L2TP/IPSec 的操作步骤也是基于 Mac 电脑的终端应用程序，对 Linux 系统来讲，步骤几乎是一模一样的，而对 Windows 用户来讲，则需要先安装一个叫 Putty 的软件。

顺便提一下，Xen VPS 的 Ubuntu 系统最好使用 11.04 版本的，因为其他较低的版本(例如 10.04)很可能不行。

I、连接 VPS

打开终端应用程序并输入以下命令：

```
ssh root@xxx.xxx.xxx.xxx
```

记得将 "xxx.xxx.xxx.xxx" 替换成 VPS 的 IP 地址，例如 "178.18.17.30"，然后回车就可以了。

P.S.:

如果在连接的过程中遇到问题，可以参考之前的 PPTP 教程。

II、安装 OpenSwan

虽然你可以通过输入 "aptitude install openswan" 命令直接安装 OpenSwan，但根据我分别在两个不同的 VPS 上测试的结果，这种方法已经无效，所以，最好还是直接从 OpenSwan 官方网站下载再安装，具体方法如下：

1、输入以下命令：

```
aptitude install build-essential
```

回车，输入 "y"，再回车。

2、输入以下命令：

```
aptitude install libgmp3-dev gawk flex bison
```

回车，输入 "y"，再回车。

3、输入以下命令：

wget http://www.openswan.org/download/openswan-2.6.35.tar.gz

回车。

4、输入以下命令：

tar xzvf openswan-2.6.35.tar.gz

回车。

5、输入以下命令：

cd openswan-2.6.35

回车。

6、输入以下命令：

make programs

回车。

7、输入以下命令：

make install

回车。到此，OpenSwan 就安装成功了。

备注：

a、2.6.35 是目前最新的版本，将来你可以访问 OpenSwan 官方网站看看有没有更新的版本，如有，不妨尝试一下。

b、文章中的所有命令都可以直接复制粘贴到终端应用程序。

III、编辑 IPSec

OpenSwan 是用来建 IPSec 的，而 IPSec 是用来建 L2TP 的。

1、输入以下命令：

vi /etc/ipsec.conf

回车，输入 "dG" 删除所有内容，按 "i" 键，然后复制并粘贴以下内容：

version 2.0 config setup nat_traversal=yes
virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12,%v4:25.0.0.0/8,%v6:fd00::/8,%v6:fe80::/10 oe=off
protostack=netkey conn %default forceencaps=yes conn L2TP-PSK-NAT rightsubnet=vhost:%priv also=L2TP-PSK-noNAT
conn L2TP-PSK-noNAT authby=secret pfs=no auto=add keyingtries=3 rekey=no ikelifetime=8h keylife=1h type=transport
left=YOUR.VPS.IP.ADDRESS leftprotoport=17/1701 right=%any rightprotoport=17/%any
记得将 YOUR.VPS.IP.ADDRESS 替换成自己 VPS 的 IP 地址，例如 178.18.17.30。替换方法如下：

按下"ESC" 键退出插入模式，将光标移到 "Y" 字母上，接着按下 "i" 键，输入 IP 地址，再按一下 "ESC" 键，并将光标移到 "YOUR.VPS.IP.ADDRESS" 上，然后按下 "x" 键把它们全部删除。或者你可以先把内容粘贴到记事本之类的编辑器上并修改好之后再复制粘贴到终端应用程序。

完了之后，输入 ":wq" 并回车保存所做的修改。

备注：

在 Vi 编辑模式下，你需要按 "i" 才能插入内容，完了之后，要按 "ESC" 退出插入模式和保存。

2、输入以下命令：

vi /etc/ipsec.secrets

回车，按 "i" 键并输入以下内容：

YOUR.VPS.IP.ADDRESS %any: PSK "YourSharedSecret"

例如：

178.18.17.30 %any: PSK "123456abcdef"

（小技巧：你需要按 Tab 键创建不同数值之间的空格。）

按 "ESC" 键，输入 ":wq"，再回车保存。

3、一行一行地输入以下命令：

```
for each in /proc/sys/net/ipv4/conf/*
do
echo 0 > $each/accept_redirects
echo 0 > $each/send_redirects
done
```

每一行都要回车。

4、输入以下命令：

service ipsec restart

回车。

备注：

输入 "ipsec verify"，回车，如果一切正确，你将会看到如下图所示的结果：

如果不是，则需要重新检查之前的操作步骤，特别是 "ipsec.conf" 的内容。

Ⅳ、安装 L2TP

基于 IPSec **的** L2TP **就是** VPN **了。**

1、输入以下命令：

cd ..

回车**以便**进**入** VPS **根目**录。

2、输入以下命令：

aptitude install xl2tpd

回车，**输入** "y"，**再回**车。

3、输入以下命令：

vi /etc/xl2tpd/xl2tpd.conf

回车，**输入** "dG" **删除所有的内容，按下** "i" **键，然后粘**贴**以下内容**：

```
[global]
; listen-addr = 192.168.1.98

[lns default]
ip range = 10.1.1.2-10.1.1.255
local ip = 10.1.1.1
require chap = yes
refuse pap = yes
require authentication = yes
name = LinuxVPNserver
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes
```

按下 "ESC" **键，输入** ":wq"，**并回**车**保存。**

Ⅴ、创建 xl2tpd

这**里假**设**你的** VPS **已**经**支持** PPP，**如果没有，先**输**入** "aptitude install ppp" **命令安装** PPP**。**

1、输入以下命令：

vi /etc/ppp/options.xl2tpd

回车，**按下** "i" **键，然后粘**贴**以下内容**：

```
require-mschap-v2
ms-dns 8.8.8.8
ms-dns 8.8.4.4
asyncmap 0
auth
crtscts
lock
hide-password
modem
debug
name l2tpd
```

proxyarp
lcp-echo-interval 30
lcp-echo-failure 4

按下 "ESC" 键，**输入** ":wq"，**并回车保存。**

备注：

你可以将 8.8.8.8 **和** 8.8.4.4 **替换成** 208.67.222.222 **和** 208.67.220.220**。**

2、输入以下命令：

vi /etc/ppp/chap-secrets

回车，按下 "i" 键，**并输入如下内容：**

username l2tpd password *

例如：

freenuts l2tpd 123456 *

记**得用** "tab" 键**输入空格，用** ":wq" **保存文件。**

3、输入以下命令：

service xl2tpd restart

回车。

VI、IP 转发

这**个步骤将使你的** VPN **连接整个互联网。**

1、输入以下命令：

vi /etc/sysctl.conf

回车，找到 "#net.ipv4.ip_forward=1" **这一行，接着按** "x" **键删除** "#" **号，然后输入** ":wq" **保存。**

2、使转发生效：

sysctl -p

回车，如果一切正常，你将会只看到以下结果：

net.ipv4.ip_forward = 1

3、输入以下命令：

iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -o eth0 -j MASQUERADE

回车之后，你就可以连接自己的 L2TP/IPSec VPN **翻墙了，但是如果你重启** VPS **的话，就需要重新执行一次** iptables **命令，并重启** ipsec，**为了避免这些，你只需要输入以下命令：**

vi /etc/rc.local

并在 "exit 0" **这一行之前粘贴以下内容就可以了：**

```
for each in /proc/sys/net/ipv4/conf/*
do
echo 0 > $each/accept_redirects
echo 0 > $each/send_redirects
done
iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -o eth0 -j MASQUERADE
/etc/init.d/ipsec restart
```

完了之后，你就可以尽情地享用自己搭建的 L2TP/IPSec VPN **了。**

三、如何创建 OpenVPN

虽然都是 VPN，但 PPTP 和 L2TP/IPSec 主要适用于 Xen，而 OpenVPN 则既可以在 Xen 也可以在 OpenVZ 类型的 VPS 上搭建，只不过你需要安装一个客户端才能使用。

这篇文章将介绍如何仅通过 10 个步骤就可以成功搭建 OpenVPN 的方法，而你需要的仅是一个 VPS 和一台可以上网的电脑。和 PPTP 以及 L2TP/IPSec 的一样，以下 OpenVPN 的搭建教程也是基于 Xen VPS 的 Ubuntu 系统以及 Mac 电脑自带的终端应用程序，对 Linux 来讲，操作步骤几乎一模一样，但是对 Windows 来讲，你就需要事先安装 Putty 软件。

I、连接 VPS

打开终端应用程序并输入以下命令：

ssh root@xxx.xxx.xxx.xxx

记得把“xxx.xxx.xxx.xxx”替换成你 VPS 的 IP 地址，例如“178.18.17.142″。

小技巧：关于如何连接的更多信息，可以参考 PPTP 的搭建教程。

II、安装 OpenVPN

输入以下命令：

apt-get install openvpn

回车，输入 "y"，再回车。

III、移动 easy-rsa 文件夹

输入以下命令：

cp -R /usr/share/doc/openvpn/examples/easy-rsa /etc/openvpn

回车完成将 easy-rsa 文件夹复制到 OpenVPN 根目录的操作。

IV、生成加密文件

一行一行地输入以下命令，每行都要回车，在出现 "yes/no" 问题的地方输入 "yes" 再回车：

cd /etc/openvpn/easy-rsa/2.0

. ./vars

./clean-all

./build-ca

./build-key-server server

./build-key client

./build-dh

小技巧：你可以将 "client" **改成任意的名字，但是下面的步骤也要跟着改。**

V、应用 iptables 规则

这**个步骤将使你的** OpenVPN **连接到互联网**：

1、转发 IP

输入以下命令：

vi /etc/sysctl.conf

回车，找到 "#net.ipv4.ip_forward=1" **这一行，按** "x" **键删除那个** "#" **号，然后输入** ":wq" **保存。**

2、使转发生效

输入以下命令：

sysctl -p

如果一切正常，你将只会看到以下结果：

net.ipv4.ip_forward=1

3、创建 iptables 规则

输入以下命令：

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j SNAT --to 178.18.17.142

记**得将** "178.18.17.142" **改为你的** VPS **的** IP **地址。**

小技巧：如果是 OpenVZ **类型的** VPS，**则需要将** "etho" **替换成** "veneto"。

VI、创建 VPS 上的 OpenVPN 配置文件

输入以下命令：

vi /etc/openvpn/server.conf

回车，按下 "i" **键，然后粘贴以下内容**：

```
port 1194
proto udp
dev tun
ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt
cert /etc/openvpn/easy-rsa/2.0/keys/server.crt
key /etc/openvpn/easy-rsa/2.0/keys/server.key
dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
client-to-client
duplicate-cn
keepalive 10 120
comp-lzo
```

```
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
log /var/log/openvpn.log
verb 3
```

按下 "esc" 键**退出插入模式**，**输入** ":wq" **保存文件。**

小技巧：**你也可以将** 8.8.8.8 **和** 8.8.4.4 **分**别**替**换**成** 208.67.222.222 **和** 208.67.220.220。

VII、启动 OpenVPN

输入以下命令：

```
# /etc/init.d/openvpn start
```

回车。

VIII、创建电脑上的 OpenVPN 配置文件

输入以下命令：

```
vi /etc/openvpn/easy-rsa/2.0/keys/client.conf
```

回车，**按下** "i" 键，**并粘**贴**以下内容**：

```
client
dev tun
proto udp
remote 178.18.17.142 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
comp-lzo
verb 3
redirect-gateway
script-security 2
```

记**得将** "178.18.17.142" 换**成你** VPS **的** IP **地址。**

完了之后，**按下** "esc" 键**退出插入模式**，**输入** ":wq" **保存。**

IX、重启

为**了避免** VPS **重启后重新**设**置一遍** iptables 规则，**你可以**输**入以下命令**：

```
vi /etc/rc.local
```

回车，**按下** "i" 键，**并将以下内容粘**贴**到** "exit 0" 这**一行的上面**：

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j SNAT --to 178.18.17.142
```

openvpn /etc/openvpn/server.conf

记得将“178.18.17.142”替换成你 VPS 的 IP 地址，完了之后，按下 "esc" 键退出插入模式，然后输入 ":wq" 保存。

小技巧：以上的命令是针对 Xen 类型的 VPS，如果是 OpenVZ 类型的，则需要将 "etho" 替换成 "veneto"。

X、将配置文件下载到电脑里

电脑上需要有以下四个 OpenVPN 的配置文件：

- client.conf
- ca.crt
- client.crt
- client.key

要下载以上文件，你可以使用 Fetch (Mac)、WinSCP (Windows) 或者其他 SFTP 软件，也可以直接在 Mac 的终端上使用以下 SSH 命令：

1、进入文件所在的目录

输入以下命令：

```
cd /etc/openvpn/easy-rsa/2.0/keys/
```

回车。

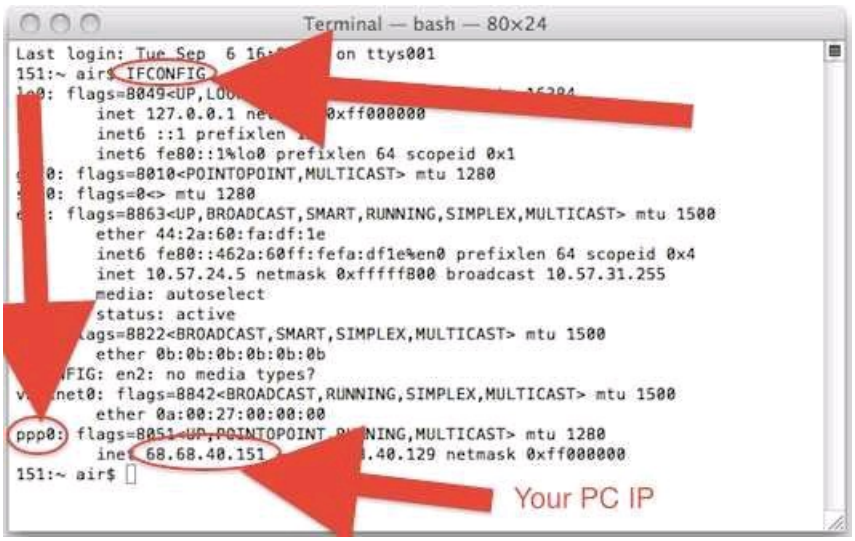
2、下载文件

输入以下命令：

```
scp ca.crt client.crt client.key client.conf air@68.68.40.151:
```

记得将 "air" 换成你电脑的用户名，将 "68.68.40.151" 换成你本地的 IP —— 这个你可以通过以下方法获得：

首先，打开一个新的终端窗口，接着输入 "ifconfig"，回车，如果结果包含一行 "pppo" 的类似如下的内容：



那么第一个 inet 值就是你本地的 IP，如果没有 "pppo" 这一行，那么你就不能通过以上的 SCP 命令直接从 VPS 上下载文件。

完了之后，回车，输入 "yes"，如果电脑有设置密码，则接着输入电脑密码，然后那 4 个文件就会被下载到该用户名的根目录。

3、移动下载文件

完了之后，找到下载的文件并复制粘贴到电脑上 OpenVPN 的 Configurations 文件夹，然后，你的 OpenVPN 就可以翻墙了。

第四章：免费 SSH 代理

SSH（Secure Shell，安全外壳协议）是一种加密渠道，本身并不能翻墙，需要结合代理服务器才能够翻墙。

所以，SSH 代理可以看作是加密了的代理，比较安全。

第一节、5 个免费的 SSH 代理

由于免费的 SSH 代理大都会在半个、一个、四个或者其他短时间内更换一次密码，所以如果你有虚拟专用服务器、独立服务器、或者云服务器，那么你就创建自己的 SSH 代理，具体方法可以参考下一节。

如果没有，或者觉得麻烦，那么你也可以凑合着使用以下 5 个免费的 SSH 代理：

1. Alidage

在 Alidage 首页，点击“猛击这里，探索真理”按钮，输入电子邮箱地址，按下“Enter”键，然后你就可以通过邮件获得免费的 SSH 代理帐号。

该帐号的密码将每个小时更新一次，而每次你都需要重新输入邮箱地址申请新的密码。

2. Onlybird

Onlybird 网站提供两个不同的 SSH 代理帐号，而只要点击上面的链接你就可以看到帐号信息。

顺便一提，该 SSH 帐号的密码将每 4 个小时更新一次，另外，它的服务器端口是 9999，而不是常见的 22。

3. BlueSSH

访问 BlueSSH 网站的“免费 SSH”页面，你就可以看到一个免费的 SSH 代理帐号。

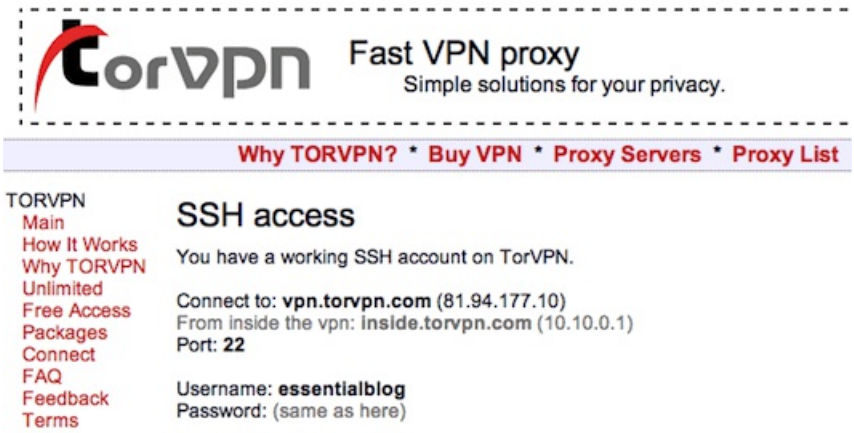
该帐号的服务器端口是 80 或者 443，密码每半个小时更新一次。

4. Usassh

Usassh 提供 2 个不同的免费 SSH 代理帐号，但是端口为 22 的已经不可以用。

而端口为 80 或者 443 的那个将会在整点的时候更新密码。

5. Tor VPN



在 Tor VPN 网站上，你可以注册一个试用(Trial)帐号，并获得有效期为一个月的有 1 GB 流量的免费 SSH 代理帐号。

除了 SSH 代理，该网站还提供免费的 OpenVPN 服务。

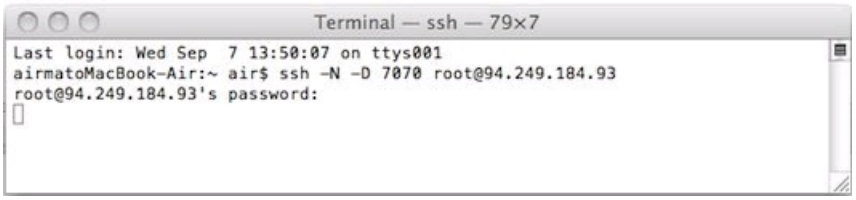
在以上 5 个提供免费 SSH 代理的网站里面，前面 4 个都是中文的，而最后一个是英文的，可惜它已经被墙。

第二节、如何把 VPS 作为 SSH 代理翻墙

VPS 不仅可以用来搭建 PPTP、L2TP/IPSec 和 OpenVPN，而且还可以直接作为 SSH 代理翻墙。

以下将介绍一个如何把 VPS 作为 SSH 代理翻墙的简易方法：

I、连接 VPS



如之前所说，对 Windows 来讲，你可以安装一个 SSH 客户端（例如 Tunnelier），对 Mac 来讲，你也可以安装一个 SSH 客户端（例如 Issh），但更简单的方法是直接在终端应用程序上通过以下命令连接：

```
ssh -N -D 7070 root@94.249.184.93
```

记得将 "94.249.184.93" 替换成你 VPS 的 IP 地址，按下 "Return" 键，输入 VPS 登录密码，如果正确，回车后你将看不到任何新的内容。

顺便说一下，不管你的 VPS 事先是否已经安装了 VPN，你都可以把 VPS 作为 SSH 代理，这不会影响 VPN 的使用。

技巧：

尽管以上是最简单的连接方法，但是只能供你一个人使用——除非你想把自己的 VPS 帐户和别人分享。而如果要和别人分享同一个 SSH 代理，你可以通过以下 4 个步骤新建一个受限的 VPS 用户：

1、登录 VPS

在终端应用程序上输入以下命令：

```
SSH root@94.249.184.93
```

记得将 "94.249.184.93" 替换成你 VPS 的 IP 地址。

2、创建一个用户组

输入以下命令：

```
groupadd internetfreedom
```

你可以将 "internetfreedom" 替换成任意名字。

3、创建受限用户

输入以下命令：

```
useradd -d /home/freenutsdotcom -m -g internetfreedom -s /bin/false freenutsdotcom
```

以上命令将会在 "internetfreedom" 创建一个新的 SSH 用户 "freenutsdotcom"，该用户只能使用 SSH 代理，不能登录你的 VPS 帐户。

4、为新用户设置密码

输入以下命令：

passwd freenutsdotcom

然后，为该用户设置任意密码 (例如 "123456")。

完了之后，你就可以把该用户名和密码分享给朋友，他们也就可以通过以下命令使用你的 SSH 代理：

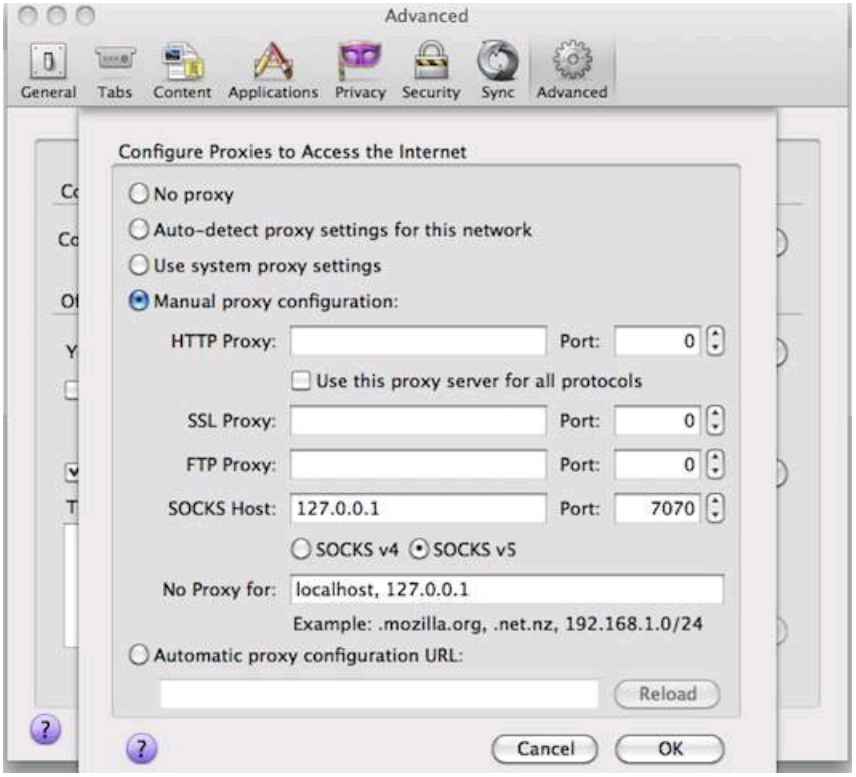
ssh -N -D 7070 freenutsdotcom@94.249.184.93

记得把 "freenutsdotcom" 替换成你新建的用户名，把 "94.249.184.93" 替换成你 VPS 的 IP 地址。

II、配置浏览器代理

连接上 VPS 之后，你需要在浏览器的网络设置里面将 Socks 代理的服务器 IP 地址设为 127.0.0.1，并且端口为 7070。其中 Firefox 和 Chrome 浏览器的设置分别如下：

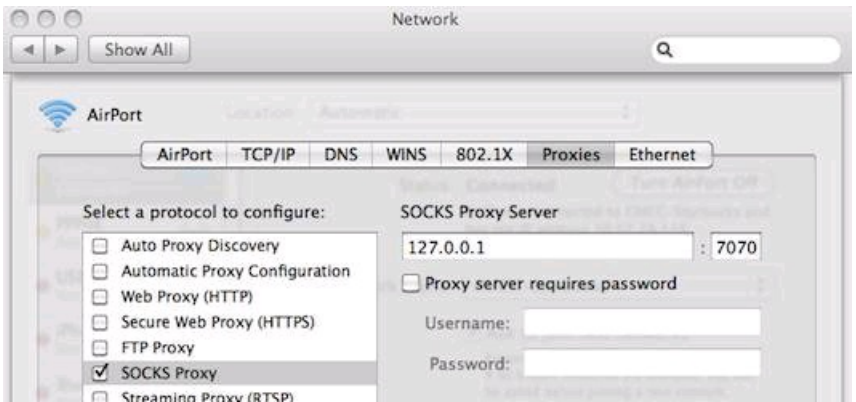
1、Firefox

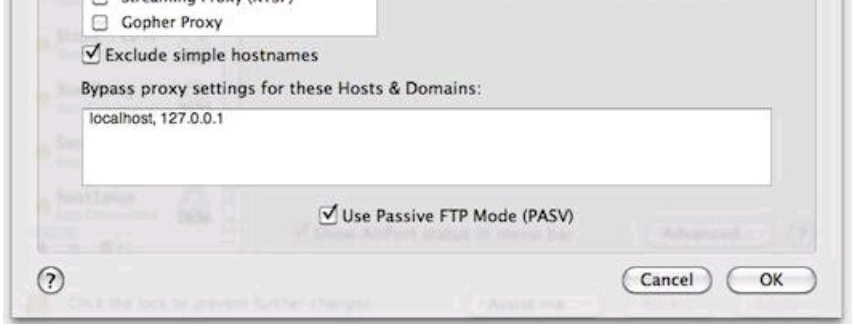


以上的设置界面你可以在 Firefox 浏览器上通过以下路径找到：

Preference –> Advanced –> Network –> Settings

2、Chrome





以上的设**置界面你可以在** Chrome 浏览**器上通**过**以下路径找到**:

Preference –> Under the Hood –> Network –> Change Proxy Settings

顺**便一提**, HTTP、SSL、FTP **以及其他代理服**务**器的** IP **地址一律留空或者不要打勾。**

第三节、如何连接 SSH 代理

有了 SSH 代理（不管是免费的还是付费的）之后，怎样通过它翻墙呢？

Windows 用户可以下载 Putty 或者 Bitvise SSH Client (Tunnelier)，而 Mac 用户则可以使用终端应用程序或者下载 SSH Tunnel Manager 或者 iSSH-improved 。

一、如何通过终端应用程序连接 SSH 代理翻墙

当有了一个 SSH 代理帐号之后，不管是购买的、免费的，还是自建的，如何通过它翻墙呢？

在 Mac OS X 系统上，我们可以直接通过自带的终端应用程序（Terminal）连接 SSH 代理翻墙，而不需要安装任意的第三方应用软件，具体步骤如下：

1. 获取 SSH 代理帐号信息

一个有效的 SSH 代理帐号需要包括以下 4 种信息：

- 服务器（Server）：例如 “s4.alidage.org”；
- 用户名（Username）：例如 “guest”；
- 密码（Password）：例如 “guest29080212737358”；
- 端口（Port）：例如 “22”（这个是默认端口）。

以上例子所用的数据都是来自我的一个阿里大哥 (Alidage.org) 免费 SSH 代理帐号。

2. 连接 SSH 代理

打开终端应用程序，输入以下一行命令：

SSH -N -D 7070 用户名@服务器

例如：

SSH -N -D 7070 guest@s4.alidage.org

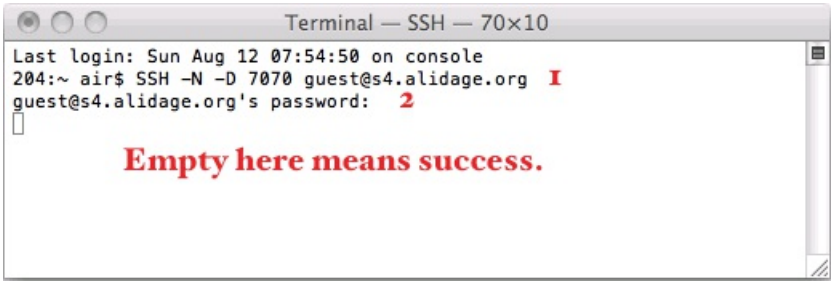
以上的命令是针对 22 端口的，如果 SSH 代理的服务器端口不是 22，而是 80 或者其他数字，那么你还需要在命令里面添加 “-p 端口”，即使用以下一行命令：

SSH -N -p 端口 -D 7070 用户名@服务器

例如：

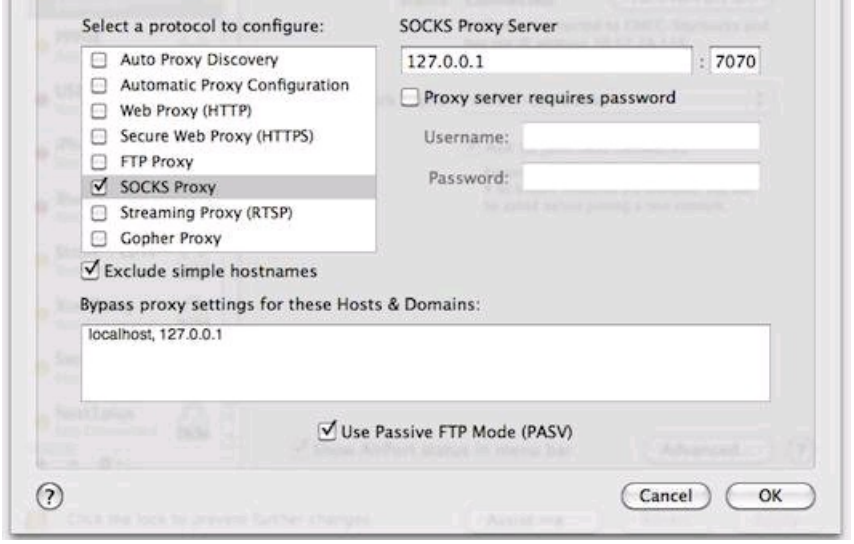
SSH -N -p 80 -D 7070 guest@s4.alidage.org

如果服务器没有宕机或者被墙，那么回车之后就可以输入该 SSH 代理的帐号密码，如果密码正确，再次回车后你将看不到任何新的内容，如下图所示：



3. 设置 Socks 代理

连接成功之后，打开浏览器，在网络设置里面将 Socks 代理的服务器 IP 地址设为 127.0.0.1，并且端口为 7070，如下图所示：



上图的设置页面是针对 Chrome 的，并且适用于 Safari，而对于 Firefox、IE、Opera 或者其他浏览器，它们的设置也是一样的，关键是找到设置页面。

完了之后，你可以通过该浏览器使用 SSH 代理翻墙了。

二、如何通过 SSH Tunnel Manager 连接 SSH 代理翻墙

在 Mac OS X 系统上，我们可以直接通过终端应用程序连接 SSH 代理，而不需要安装任何的第三方应用软件。

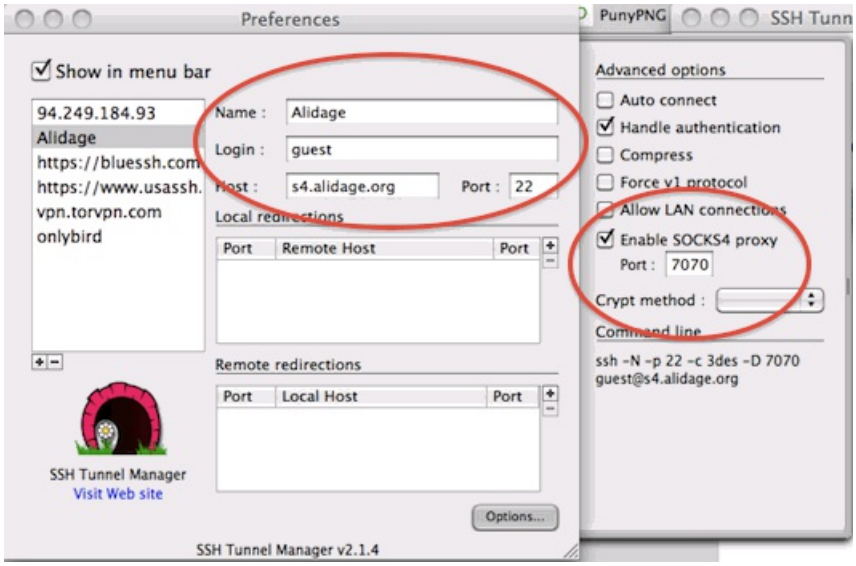
由于每次连接都需要输入一行命令，当要在多个不同的 SSH 代理帐号之间转换时，这种方法就有点麻烦了。

而要避免这种麻烦，可以安装免费的 “SSH Tunnel Manager” 软件。

安装完成之后，运行该软件，点击 Dock 栏上该软件的图标，接着点击弹出窗口上的 “Configuration” 按钮，再点击新窗口上的 “＋” 添加你的 SSH 代理帐号资料，其中以下四项是必填的：

- Name：指 SSH 代理的名称，可以任意填，例如 “alidage”；
- Login：指用户名，例如 “guest”；
- Hosts：指服务器地址，例如 “s4.alidage.org”；
- Port：指服务端口，例如 “22”（默认端口）。
  以上例子所用的数据都是来自我的一个阿里大哥 (Alidage.org) 免费 SSH 代理帐号，你需要将它们改成你的 SSH 代理帐号的实际数据。

  然后，点击 “Options” 按钮，接着选择 “Enable SOCKS4 proxy”，并输入 “7070” 作为服务端口（port），如下图所示：



完了之后，关闭上图所示窗口，在前一个含有 “Configuration” 按钮的窗口上双击该 SSH 代理的名称，接着输入帐号密码，然后就可以连接了。

顺便一提，默认情况下，电脑最顶部的菜单栏上也会有一个 SSH Tunnel Manager 图标，你也可以点击该图标，然后选择要连接的 SSH 代理。

连接成功之后，打开浏览器，在网络设置里面将 Socks 代理的服务器 IP 地址设为 127.0.0.1，并且端口为 7070，和通过终端应用程序连接之后需要做的是一样的。

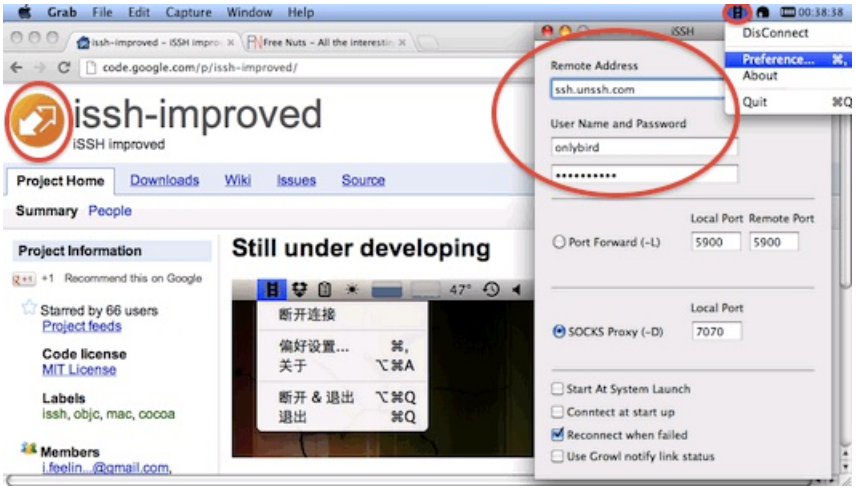
三、如何通过 iSSH-improved 链接 SSH 代理翻墙

不管是通过 SSH Tunnel Manager 还是终端应用程序，每次连接 SSH 代理的时候都需要输入密码。

而如果要避免这种麻烦，则可以使用 iSSH-improved，该免费软件同样可以在 Mac 系统上连接 SSH 代理翻墙，并且不需要每次连接都输入密码，下面是具体的使用方法：

当下载了 “iSSH_alpha1.app.zip” 文件并解压之后，你可以看到一个 “iSSH” 执行文件，双击该文件就可以启用 iSSH-improved 应用程序了。

程序开启之后，点击电脑屏幕最顶部的菜单栏上的该程序图标，并选择下拉菜单里面的 “Preference” (偏好设置)，然后你就可以添加 SSH 代理帐号了，如下图所示：



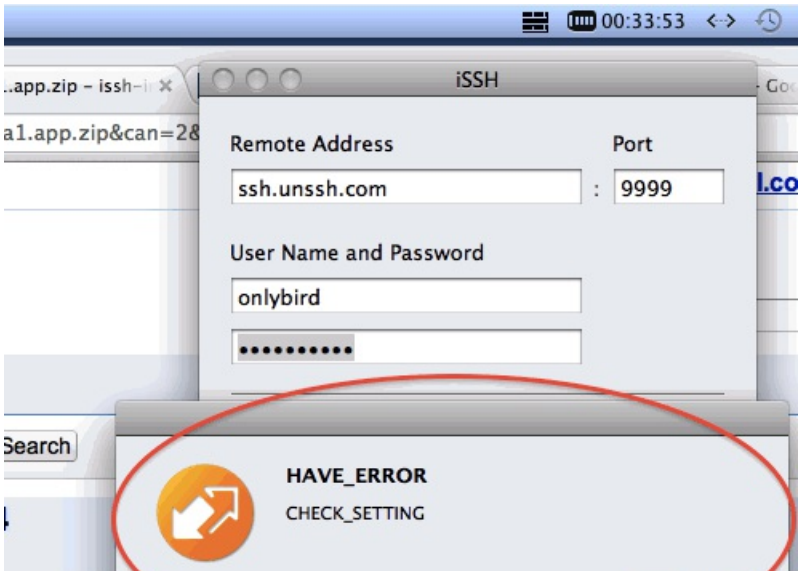
默认情况下，你只需要输入 SSH 代理帐号的以下 4 项内容：

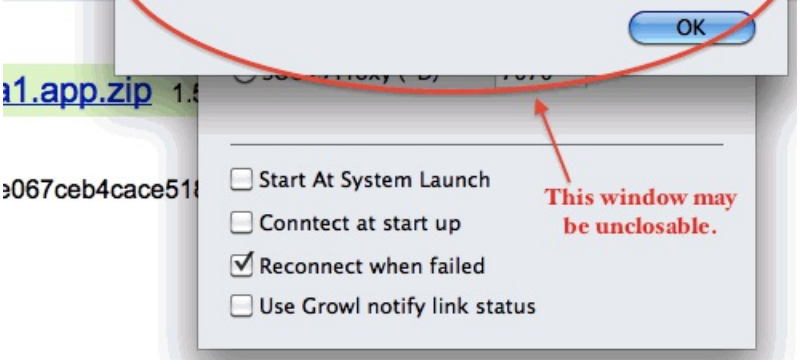
- Remote Address：服务器地址，例如 “ssh.unssh.com”；
- Port：服务端口，例如 “9999”；
- Username：用户名，例如 “onlybird”；
- Password：密码，该用户名对应的密码。
  以上例子所用的数据都来自 Onlybird 的一个免费帐号，你需要改为你自己的 SSH 代理帐号的数据。

  帐号资料添加完了之后，你就可以点击该程序图标下拉菜单里面的 “Connect” (连接) 选项连接你的 SSH 代理。

  另外，你也可以设置当电脑启动的时候自动运行 iSSH-improved，以及／或者当该程序运行的时候自动连接 SSH 代理。

  不过，当连接失败的时候，iSSH-improved 就会自动连接 —— 就算你取消了该功能，并且会出现一个错误提示的弹窗，如下图所示：





以上的弹窗将会一直出现，就算你关闭它，它也会立即重新出现，直到连接成功或者电脑重新启动。

虽然这样的弹窗非常令人讨厌，但是 iSSH-improved 毕竟可以自动连接 SSH 代理，当然，如果要管理多个帐号，那还是 SSH Tunnel Manager 比较方便。

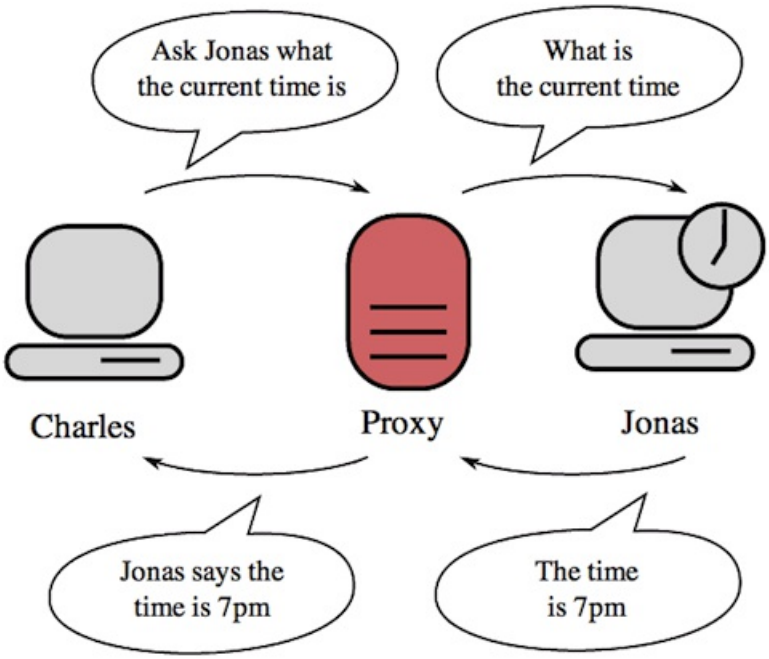
第五章：Proxy、SSH 和 VPN 的区别

虽然翻墙工具有成百上千个，但是如果把它们分类，绝大部分都是 Proxy、SSH 和 VPN 这三类。

那么，Proxy、SSH 和 VPN 之间有什么区别呢？谁的安全性最高呢？

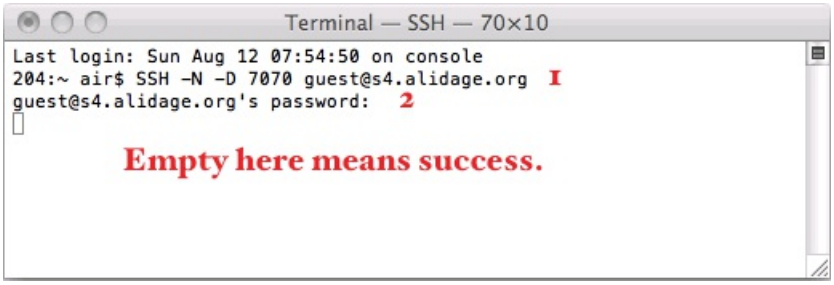
如果把传输的信息看作一个包裹，那么我们就可以用三个简单的比喻来做比较。

1、Proxy



Proxy (代理)，可以看作是一个快递员，负责将你的包裹送达收件人。

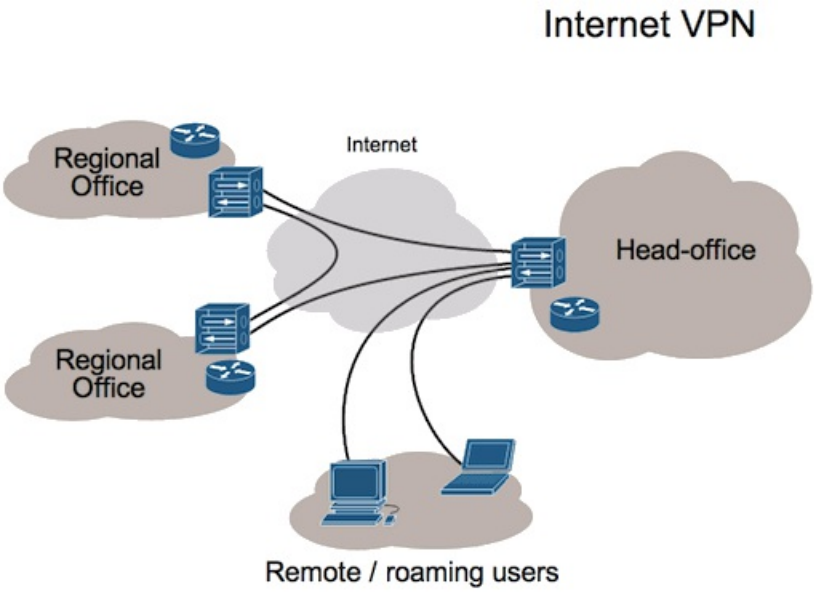
2、SSH



SSH (Secure Shell, 安全外壳协议)是一种加密渠道，本身并不能翻墙，需要结合代理服务器才能够翻墙。所以，我们通常所说的用来翻墙的 SSH，都是指 SSH 代理。

也就是说，SSH 代理 = 代理 + SSH，可以看作是加密了的代理，就好比把包裹装在保险箱里面再交给快递员。

3、VPN



图片来源: http://en.wikipedia.org/wiki/Virtual_private_network

而使用 VPN(Virtual Private Network，虚拟私人网络)，就好比不通过快递员，你亲自把包裹交给收件人所在公司的前台，再由前台转交给收件人。

从以上三个比喻可以看出，VPN 的安全性要高于 SSH、而 SSH 又高于 Proxy，因为相对来讲，包裹中途被拦截的几率要比目的地的高，特别是当大家都是在同一个服务器上搭建的时候，但是大多数情况下，这三类翻墙工具都是不在同一个服务器上的，所以安全性也是相对的。

另外，Proxy 和 SSH 的作用是局部的，只适用于你指定的应用程序(例如浏览器)，而 VPN 的作用是全局的，适用于你的整台设备，不管是浏览器、邮件客户端、iTunes 或者其他任何的连接到互联网的应用程序。

还有，通过 Proxy 和 SSH 翻墙的时候，需要设置网络的代理地址，而 VPN 则不需要。

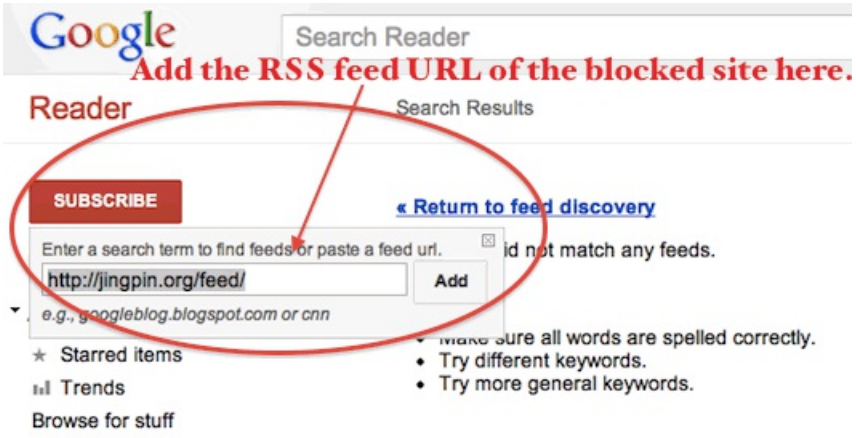
第六章：如何通过 Google Reader 翻墙

如果翻墙只是为了查看某个博客（例如精品博客）的最新文章，那么，除了通过VPN、SSH、Proxy 等工具直接访问该博客之外，你还可以通过 Google Reader（谷歌阅读器）订阅该博客的 RSS feed。

当然，前提条件是 Google Reader 没有被墙。下面将介绍通过 Google Reader 翻墙的两个简易步骤：

1、订阅被墙网站的 RSS feed

如果某个被墙的网站提供 RSS feed，那么你就可以将它直接添加到 Google Reader 上，如下图所示：

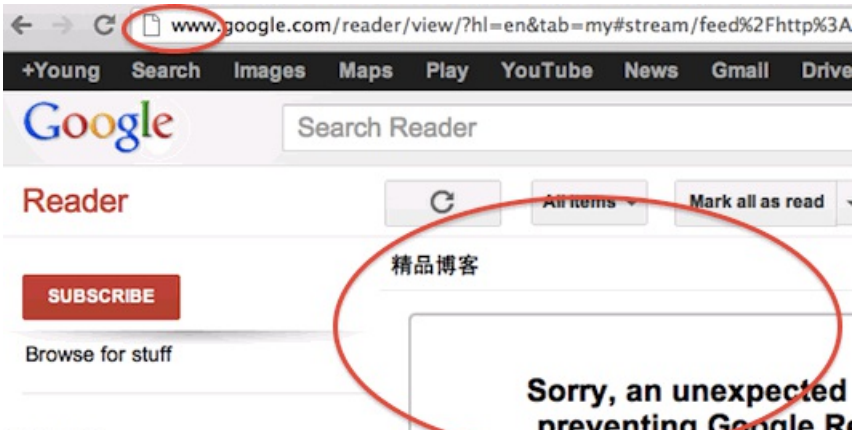


如果该网站没有提供 RSS feed，那么，你可以先访问 Page2RSS 网站，输入被墙网站的网址（URL），从而为该网站生成一个 RSS feed，如下图所示：

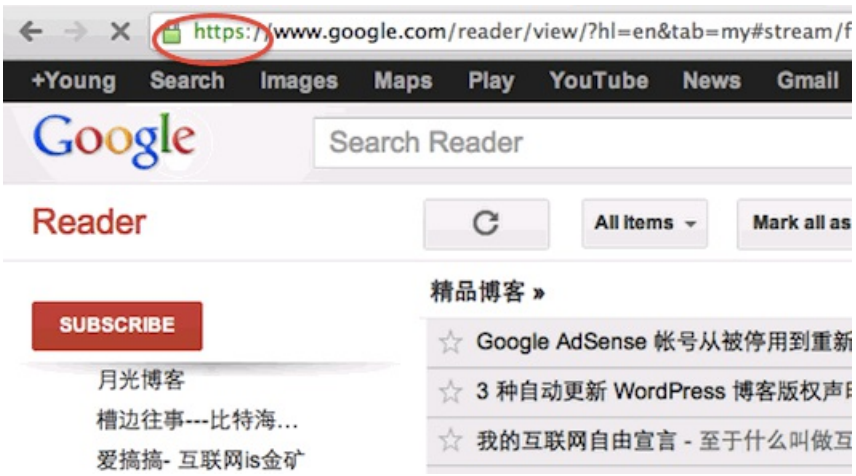
完了之后，复制所生成的 RSS feed 的链接（URL）并粘贴订阅到 Google Reader。

2、使用安全浏览模式

默认情况下，如果某个网站被墙，那么它的 RSS feed 在 Google Reader 里面也是被墙的，如下图所示：



而要解决这个问题，方法很简单，你只要在 Google Reader 页面地址栏链接的开头添加 “https://” 就可以了，如下图所示：



而如果浏览器上的 Google Reader 页面地址栏链接没有隐藏 “http”，那么你只要把 “http” 改成 “https” 就可以了。

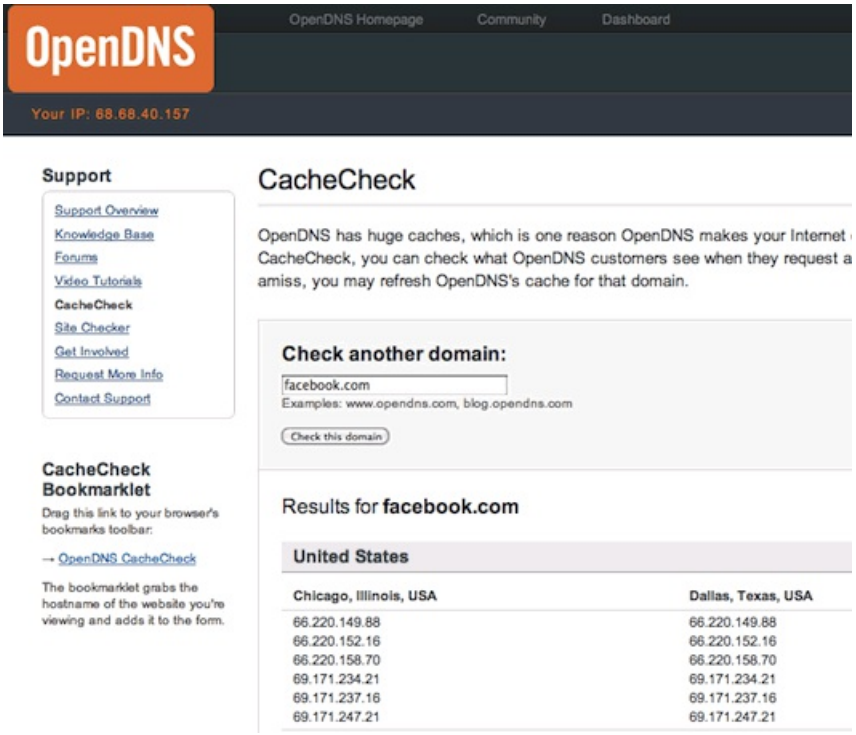
很简单，是吧？不过，通过 Google Reader 只可以阅读某个被墙网站的 RSS feed，而如果你想在该网站上留言，或者将该网站的文章分享到 Twitter、Facebook、Google+ 等地方，那就还是要通过 VPN、SSH、Proxy 等工具翻墙的。

第七章：如何通过 Hosts 文件翻墙

要操 GFW，你可以使用虚拟专用网络（VPN）、安全外壳协议（SSH）、代理（Proxy）等等多种翻墙工具。

其实，翻墙不一定要使用这些第三方的工具，我们也可以通过修改电脑系统自带的一个叫 Hosts 的文件直接翻墙，具体方法如下：

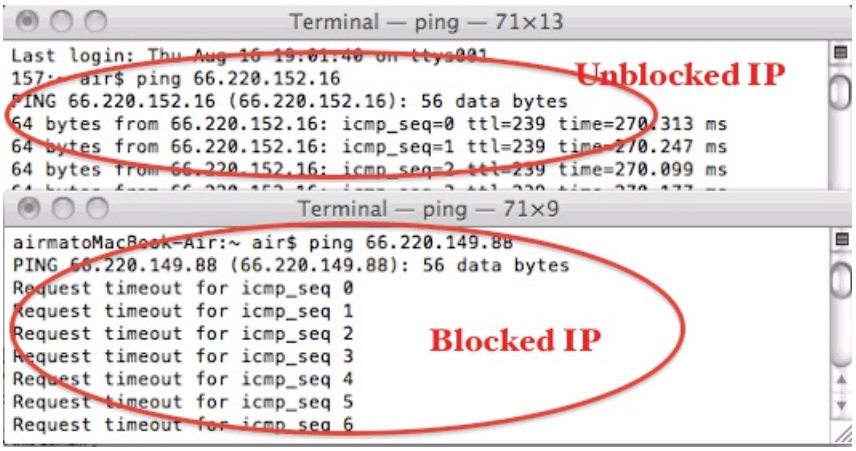
1. 寻找 IP 地址



像 Facebook、Twitter、YouTube 等这些大网站，都有多个不同的 IP 地址，那么如何查看它们的所有 IP 地址呢？

你可以访问 OpenDNS 页面，输入网站的域名（例如 facebook.com），再点击 “Check this domain” 按钮，然后就可以看到该网站世界各地的 IP 地址。

2. 挑选没有被墙的 IP 地址



在某个被墙的网站所有 IP 地址里面，有些或许已经被墙了，那么，如何知道哪些被墙，哪些没有被墙呢？

最简单的方法就是在不翻墙的情况下，Ping 一下它们。在 Windows 系统上，你可以打开命令提示窗（cmd.exe），而在 Mac OS 系统上，你可以打开终端应用程序（Terminal），然后直接输入以下命令：

```
ping 66.220.152.16
```

以上“66.220.152.16”是 Facebook 的一个 IP 地址，你可以将它改成你要 Ping 的实际 IP 地址。

如果显示的结果都是“链接超时”(timeout)，那么该 IP 地址就被墙了，如果不是，那你就可以把它添加到 Hosts 文件。

3. 修改 Hosts 文件

电脑系统自带的 Hosts 文件就好比一个 DNS 系统，所以，我们可以将某个被墙网站的域名指向它其中一个没有被墙的 IP 地址，并突破 GFW 的封锁。

在 Windows 系统上，你可以通过以下路径找到传说中的 Hosts 文件：

C:\WINDOWS\system32\drivers\etc

而在 Mac OS 上，你则可以在终端应用程序上输入以下命令并直接打开 Hosts 文件：

sudo vi /private/etc/hosts

Hosts 文件打开之后，你就可以把被墙网站的没有被墙的 IP 地址以及对应的域名添加到文件的末尾。拿 Facebook 来讲，你可以添加以下两行：

66.220.152.16 facebook.com

66.220.152.16 www.facebook.com

不同的域名对应一个相同或者不相同的 IP，而且该 IP 只对该域名有效。所以，通过以上两行代码，你只能访问 facebook.com 和 www.facebook.com，而如果要访问 Facebook 的其他子域名(例如 developers.facebook.com)，那么就还需要再添加一行含有该域名以及其对应的没有被墙的 IP 地址的代码。

代码添加完之后，保存文件，然后你就可以在不使用任何翻墙工具的情况下访问 Facebook 了，不过需要把网站链接里面的“http”改成“https”，也就是说，你需要通过以下两个链接访问 Facebook 网站：

https://facebook.com

或者

https://www.facebook.com

这种通过修改 Hosts 文件翻墙的方法就好比隔山打牛，不需要借助其他工具。但是，如果某个被墙网站的所有 IP 地址都被墙了，那么这种方法也就无效了，所以，现在要访问 Twitter 网站，就只能使用 VPN、SSH、Proxy 之类的翻墙工具了。

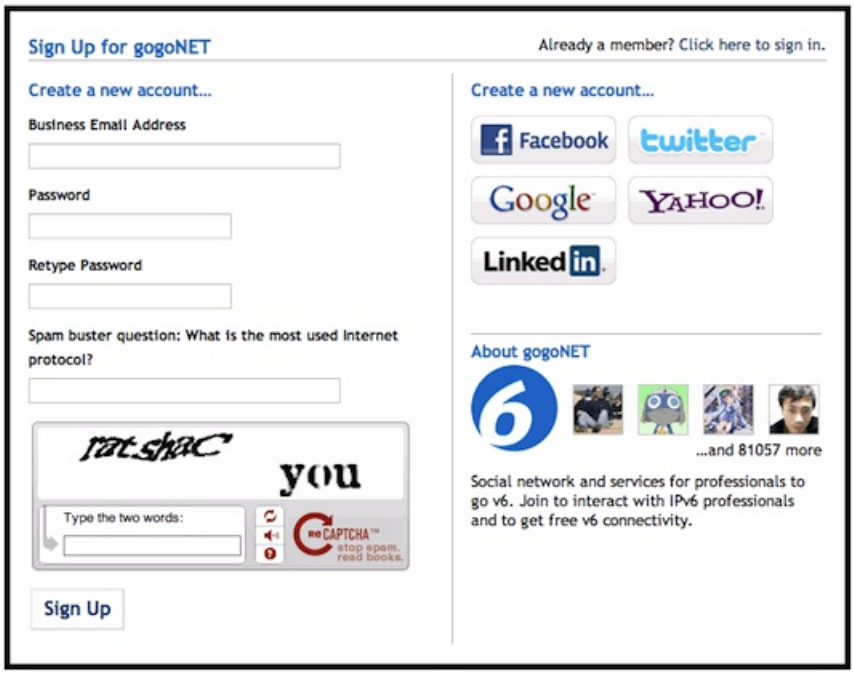
第八章：如何通过 gogoCLIENT 翻墙

IPv4 快不够用了，所以 IPv6 就出现了，于是 Facebook、Google、Twitter 等被墙的网站也都用上了长长的 IP 地址。

对于这些网站，如果你的宽带（例如教育网的）支持 IPv6，那么就可以直接访问；而如果你的宽带和我的一样，不支持 IPv6，那么也可以访问，不过需要借助第三方工具。

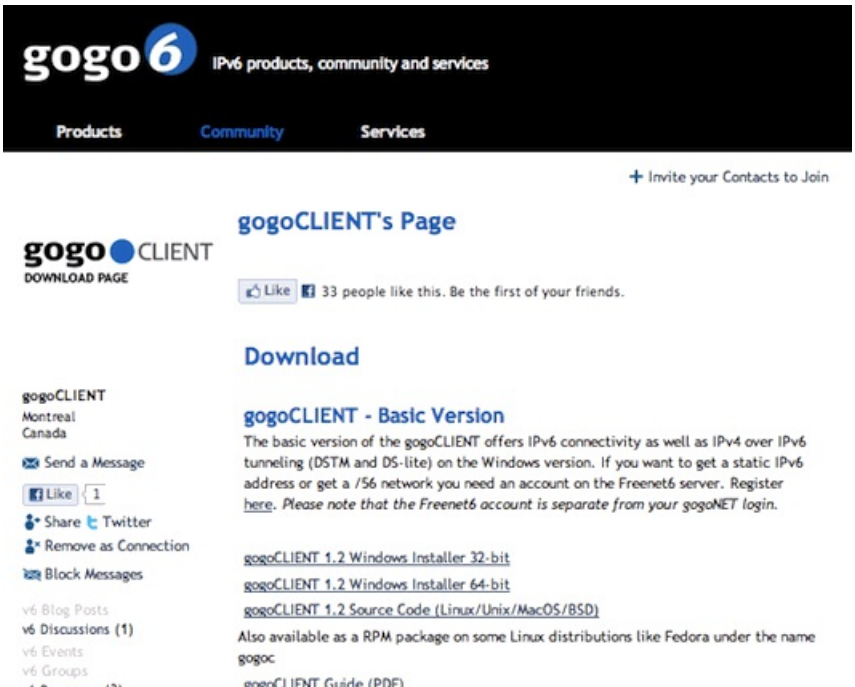
本文将介绍如何通过第三方工具 gogoCLIENT 访问那些有 IPv6 地址的被墙网站，具体步骤如下：

1、注册一个 gogo6 帐户



在 gogoCLIENT 页面，点击 Sign Up 按钮，通过邮箱地址或者 Facebook、Google、Twitter 等创建一个 gogo6 帐户。

2、下载并安装 gogoCLIENT

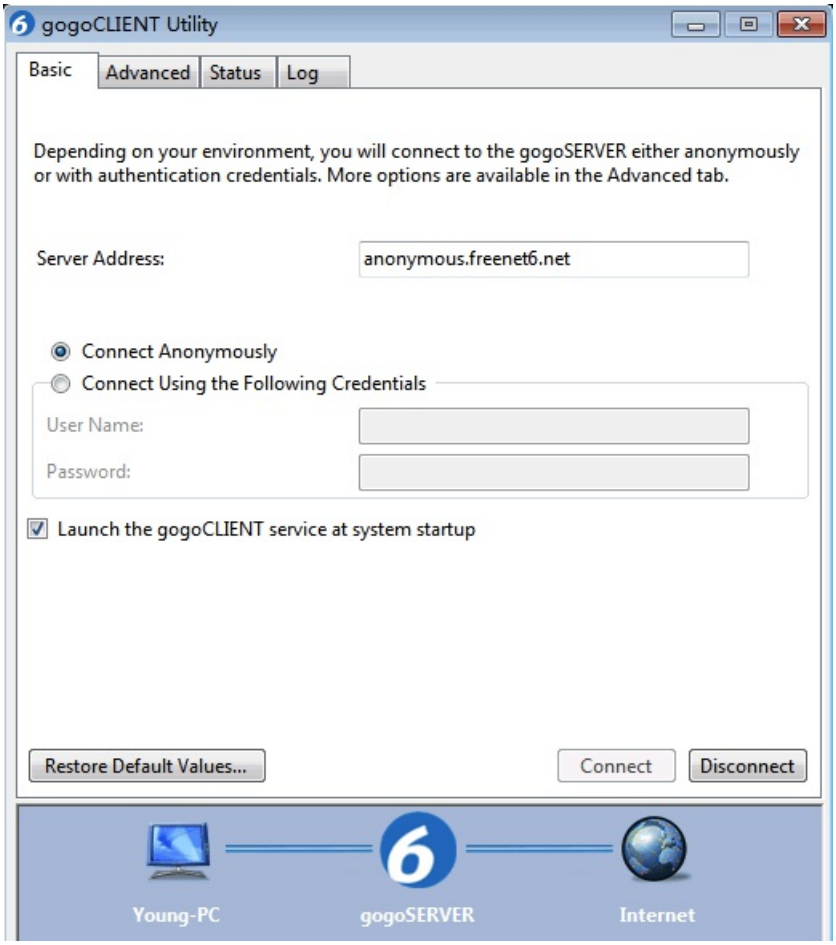


注册成功之后，登录并再次打开前面提到的 gogoCLIENT 页面，选择合适的版本下载。

目前，gogoCLIENT 提供 32 位和 64 位的 Windows 版，并且每个版本又分基本版本（Basic Version）和家庭版本（Home Access Version），其中后者比前者多了一个家庭局域网的功能而已。

另外，gogoCLIENT 还提供适用于 Linux/Unix/MacOS/BSD 系统的基本版，不过是源代码格式，需要使用 MAKE 命令安装，感兴趣的同学可以参考它的 PDF 指南（Guide）。下面只介绍如何在 Windows 系统上通过 gogoCLIENT 翻墙。

3、连接 gogoCIIENT



GogoClient 安装成功之后，运行并点击“Connect”按钮开始连接，如果连接成功，那么你就可以通过以下任意一种方法访问支持 IPv6 的被墙网站了。

3.1 后缀法

在任意支持 IPv6 的网站的网址后面添加以下后缀：

.sixxs.org

例如，要访问 Twitter，就可以直接使用以下链接：

http://twitter.com.sixxs.org

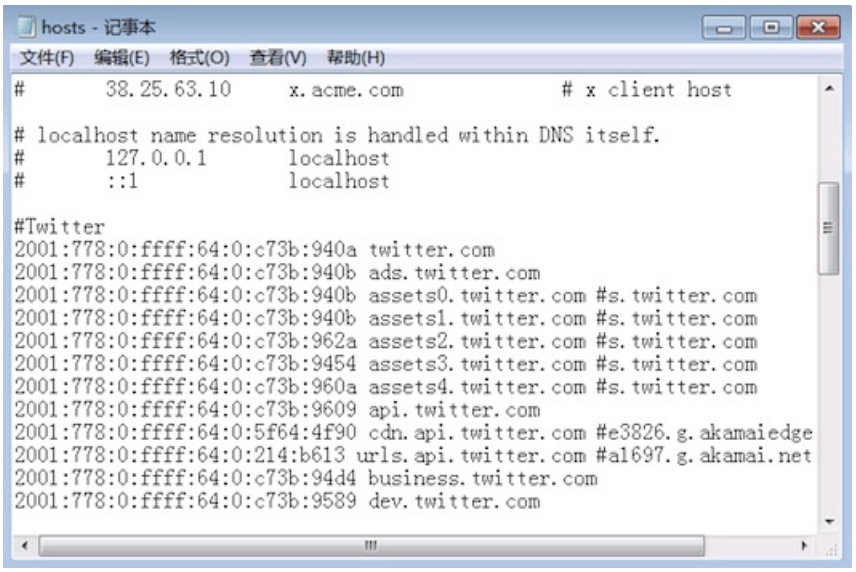
3.2 自动代理法

原来，在浏览器的网络设置里面，只要勾选“自动代理配置”，并输入以下链接就可以了：

http://gfw-proxy.co.cc/proxy.pac

但是以上的链接已经无效，而据我所知，目前还没有其他的自动代理可替代。

3.3 Hosts 法



如之前所说，在 hosts 文件里面添加被墙网站的 IPv4 地址可以翻墙，现在安装了 gogoCLIENT 之后，在 hosts 文件里面添加被墙网站的 IPv6 地址也可以翻墙。

具体方法是，首先通过以下路径找到并打开 hosts 文件：

C:\WINDOWS\system32\drivers\etc

接着，打开这个 Google 文档，并复制里面的 Google、YouTube、Twitter 等任意多个被墙网站的 IPv6 地址和对应的域名，然后粘贴到 hosts 文件并保存就可以了。

对于该 Google 文档没有列出的被墙网站，如果有 IPv6 地址，你也可以把它们添加到 hosts 文件里面。

第九章：如何检测某个网站是否被墙

GFW 要墙某个网站，要么就墙它的 IP，要么就墙它的域名，要么就墙它的敏感词，要么就样样都墙，大有宁可错杀一千，也不放过一个的气概。

在同一时间同一台设备（个人电脑、手机或者平板电脑）同一个浏览器上，如果你可以访问 A 网站，但是却不能访问 B 网站，那么 B 网站要么宕机了，要么就被墙了。

那么，如何检查某个网站是否被墙呢？你可以使用以下 4 种方法：

1. 使用翻墙工具；

2. 直接 Ping；

3. 通过 WebSitePulse；

4. 通过这 10 个免费在线检测工具。

如果某个网站宕机，那就只能等到它恢复正常才能访问了，而如果某个网站被墙了，那么只要使用一个 VPN、SSH、Proxy 等工具就可以直接翻墙访问了。

第一节:通过翻墙工具检测某个网站是否被墙

在这块神奇的大陆上，在没有断网的情况下，在微博可以发信息的时候，如果某个其他网站不能访问，那么该网站要不是宕机了，就是被墙了。

所以，如何检测该网站究竟是宕机了，还是被墙了呢？最简单最可靠的方法莫过于使用一个 VPN、SSH、Proxy 或者其他任意的翻墙工具去访问该网站，如果该网站能够打开，那么，就表示它被墙了，反之，如果不能打开，那么就表明它宕机了。

但是，如果测试的是国内(即 IP 地址是中国大陆的)网站，最好不要使用自由门和无界，因为它们的翻墙服务基本上只是针对国外的(即 IP 地址是国外的)网站。不过，据我所知，国内的网站是没有被墙的，因为它们要么域名被停止解析，要么服务器被封号，不需要 GFW 出马。

第二节：通过 Ping 检测某个网站是否被墙

Ping 是一个用来测试特定主机能否通过 IP 到达的电脑网络工具，不过通常被用作动词。

而如果某个网站不能通过 IP 到达，那么就证明该网站宕机或者被墙了。

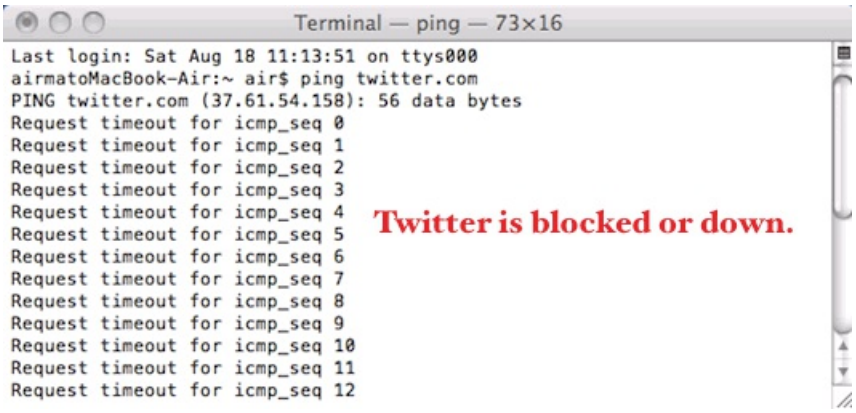
理论上，如果某个网站只有一个 IP，那么不管是 Ping 域名还是 IP，都可以检测它是否被墙，而实际上被墙的网站（例如 Facebook）大都有多个 IP，所以，Ping 域名比较实际方便。

在 Windows 系统上，你可以打开命令提示窗（cmd.exe），而在 Mac OS 系统上，你可以打开终端应用程序（Terminal），然后直接输入以下命令：

```
ping twitter.com
```

你可以将上面的 “twitter.com” 改成你要检测的网站域名。

如果结果显示的都是 “链接超时”（timeout），如下图所示：



那么该网站就大概就被墙了，但是也不一定，因为还有一个可能就是该网站宕机了。

那么如何断定该网站究竟是被墙了还是服务器挂了呢？你可以启用 VPN 再 Ping 一次它的域名，如果结果没有或者几乎没有“链接超时”的错误，那么该网站就是被墙了，而如果结果仍然全部都是“链接超时”的错误，那么该网站就是宕机了。

由于 Ping 只能检测某个网站的 IP 地址是否被墙，所以，如果结果没有没有或者几乎没有“链接超时”的错误，那也只能证明该网站对应的某个 IP 没有被墙，并不能证明它的域名是否被墙。

因此，当你可以成功 Ping 某个网站的域名，但是在浏览器上却无法打开该网站的时候，那就证明该网站被墙了。

第三节：10 个可以在线免费检测某个网站是否被墙的工具

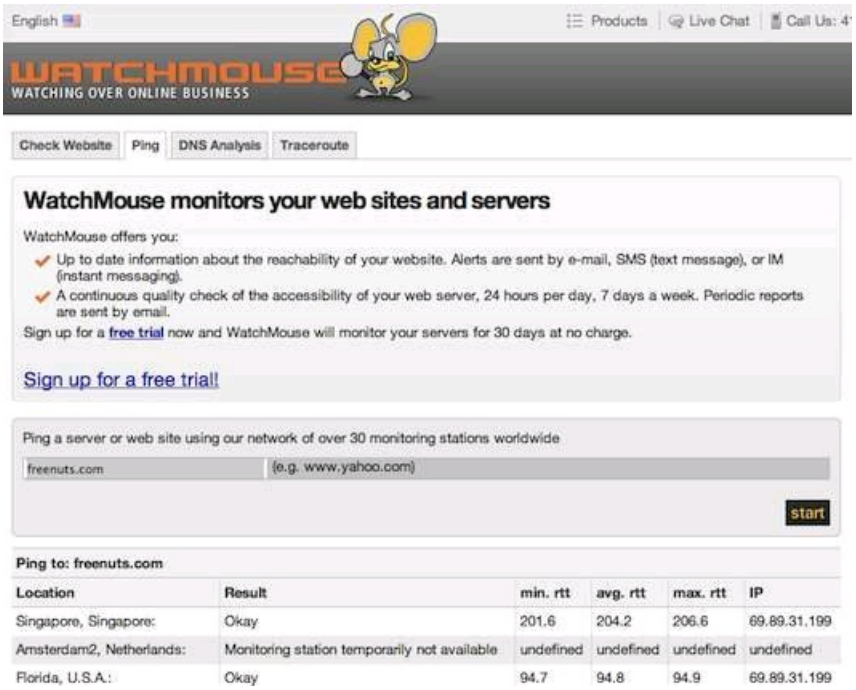
要验证某个网站在你的地区是否被墙，你可以使用翻墙工具、直接 Ping，或者通过 WebSitePulse 网站。

其实，除了 WebSitePulse，我们还可以通过以下 10 个其他第三方免费的在线应用工具直接测试某个网站是否被墙：

1. Just Ping

Just Ping 可以从 50 个不同的地区（包括北京和上海）ping 某个网站，如果所有地区的测试结果都没有 “Okey” 的，那就证明该网站宕机了，而如果只有上海和／或北京地区的测试结果是 “Packets lost (100%)”，那就证明该网站被墙了。

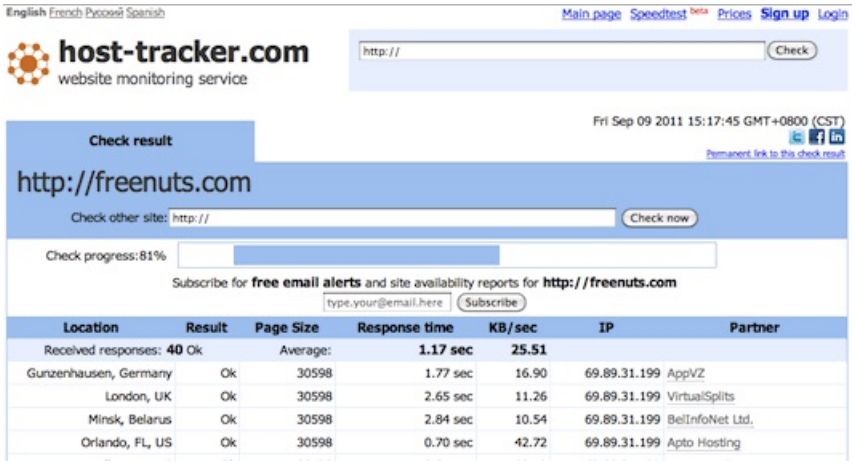
2. Watch Mouse



类似于 Just Ping, Watch Mouse 可以从世界上 30 多个不同的地区（同样包括北京和上海）测试某个网站。

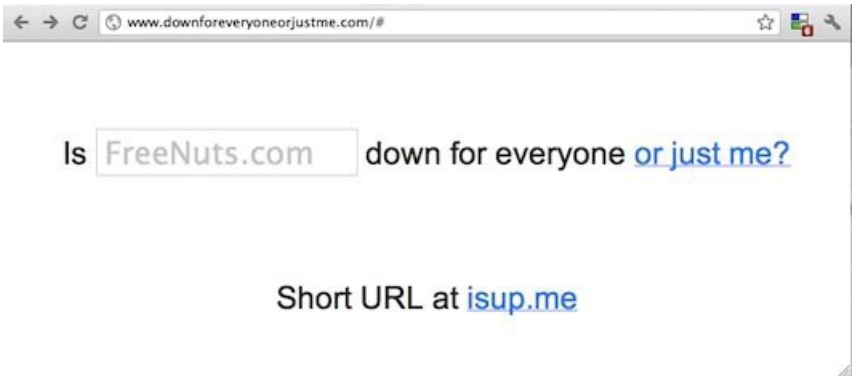
但是此文发表的时候，北京和上海这两个地区的测试服务不可以用。

3. HostTracker



HostTracker 可以从世界 50 多个不同的地区 Ping 某个网站，但是这些地区没有一个是在中国的，不过，如果全部或者绝大部分地区的结果都是“OK”，而你却无法访问该网站的时候，那么也就可以证明该网站被墙了。

4. Down For Everyone Or Just Me



在 Down For Everyone Or Just Me 上，输入要测试网站的域名，回车，如果结果显示网站没有宕机（Up），那么就证明该网站被墙了。

5. IsUp.Me

IsUp.Me 是 Down For Everyone Or Just Me 的另外一个版本，两者的功能是一样的。

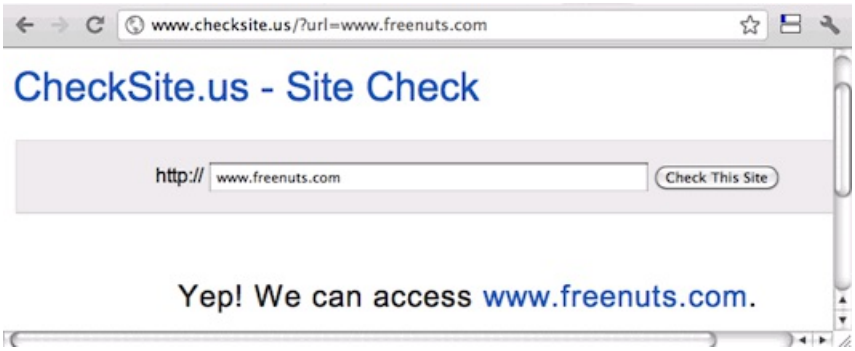
6. Down Or Not

同样，Down Or Not 也是一个可以在线免费检测某个网站是否被墙的工具，但是这篇文章发布的时候，它暂时宕机，因为服务配额（serving quota）不足。

7. Down Or Is It Just Me

Down Or Is It Just Me 也会告诉你某个网站是否只有你访问不了。

8. Checksite.Us



Checksite.Us 会告诉你它是否能够访问你所测试的网站，如果它能够，但是你却不能够，那么就证明该网站被墙了。

9. Up Or Down

Up Or Down 将会显示某个网站是否宕机，如果不是而你却又不能访问，那么就证明该网站被墙了。

10. DOJ.me

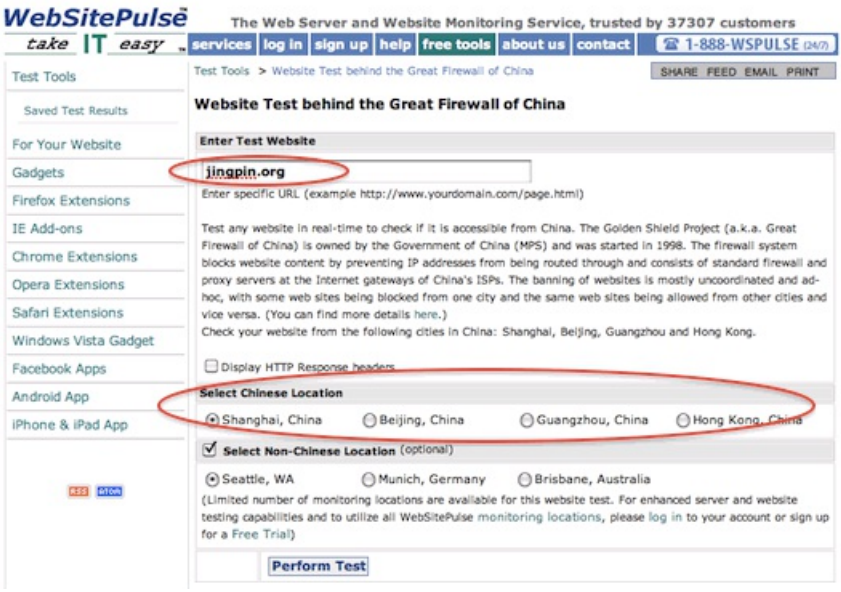
如果 DOJ.me (Down Or Just Me) 告诉你某个网站只有你不能访问，那就证明该网站被墙了。

以上 10 个网站的测试原理都是一样的，从一个或者多个地区 Ping 某个网站，如果成功，但是你却不能访问，那就证明该网站是没有宕机的，只是被墙了罢。

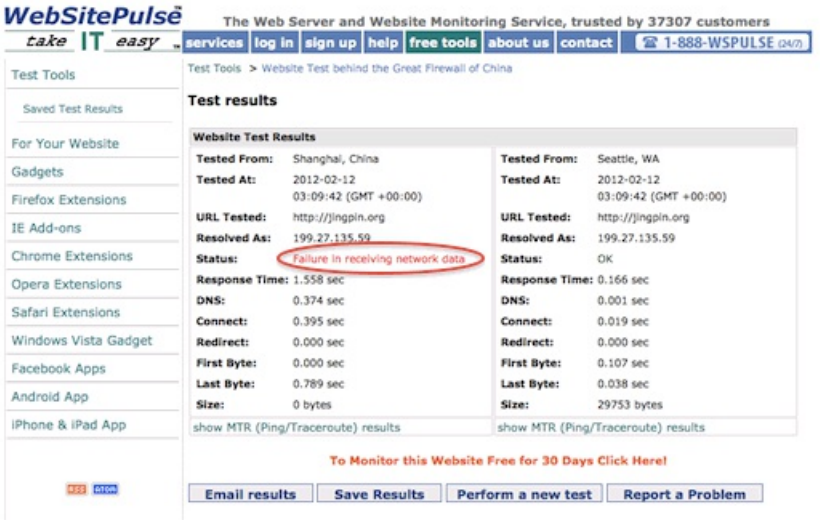
第四节：通过 WebSitePulse 在线免费检测某个网站是否被墙

其实，GFW 还是挺利害的，因为它不仅可以过滤敏感词、封锁域名或者 IP 地址，而且还可以实行区域性的封锁。

而要验证某个网站在你的地区是否被墙，你可以通过翻墙工具或者 Ping 的方法，而如果要验证北京、上海和广州这三个地区，则还可以通过 WebSitePulse 网站所提供的免费工具在线直接测试。



在 WebSitePulse 网站的 GFW 测试页面，输入你要测试的网站域名（例如 jingpin.org），选择上海、北京或者广州作为中国的一个测试地区，再选择美国纽约、德国慕尼黑或者澳大利亚墨尔本作为国外（后者说墙外）的一个地区，接着点击 “Perform Test” 按钮，然后你就可以看到测试结果了，如下图所示：



在测试结果报告上，如果左边中国地区的状态（Status）一栏出现失败（Failed）或者超时（Time out）之类的红色字，而右边国外地区的状态（Status）一栏出现 “OK” 这个绿色的单词，那么，该被测试的网站就被墙了。而如果两边都是绿色，那么该被测试的网站就没有被墙；而如果两边都是红色，那么该被测试的网站就宕机了。

顺便一提，除了上海、北京和广州，WebSitePulse 还可以测试香港地区，但是由于该地区还没有 GFW，所以也就没有网站被墙的事。

第十章:附录

虽然，人有选择翻墙的自由，也有选择不翻墙的自由，甚至可以选择一边翻墙一边坚决拥护 GFW。

但是，生命诚可贵，爱情价更高，若为自由故，两者皆可抛。

而且，如果互联网不自由，言论就不自由，生活也就不自由。

所以，要自由，就翻墙。

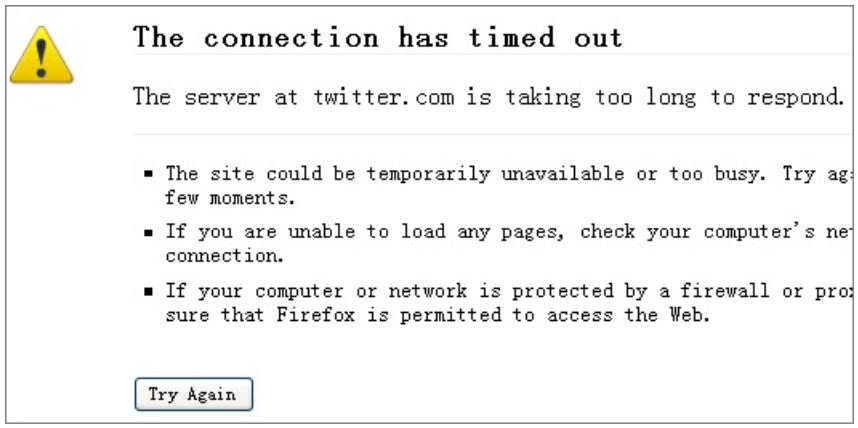
第一节:10 大被墙的国外网站

鬼知道 GFW 到底墙了多少个网站，不管是像 Facebook 这样的大站，还是如精品博客这样的小站，只要服务器在国外，任意网站都有可能被墙，理由自然是莫须有。

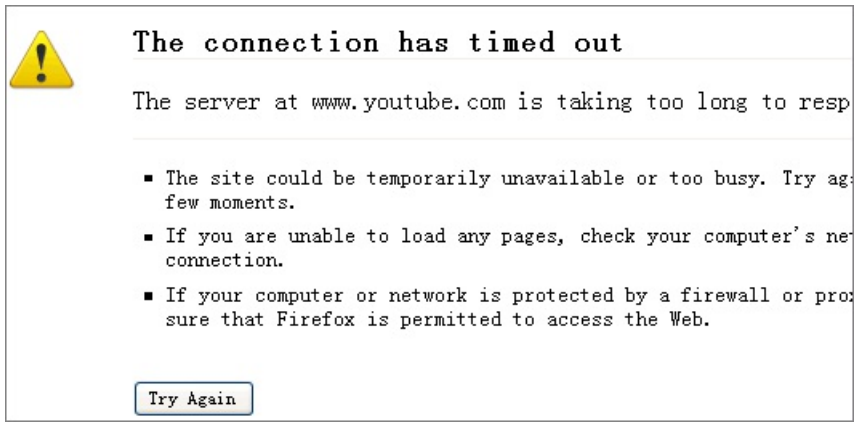
而在众多国外著名的网站里面，大多数都被墙了，例如以下比较流行的 10 个：

1. Facebook

2. Twitter

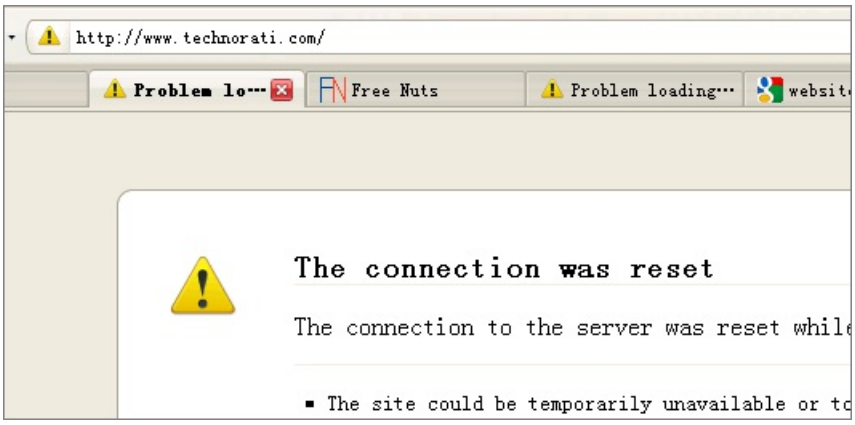


3. YouTube



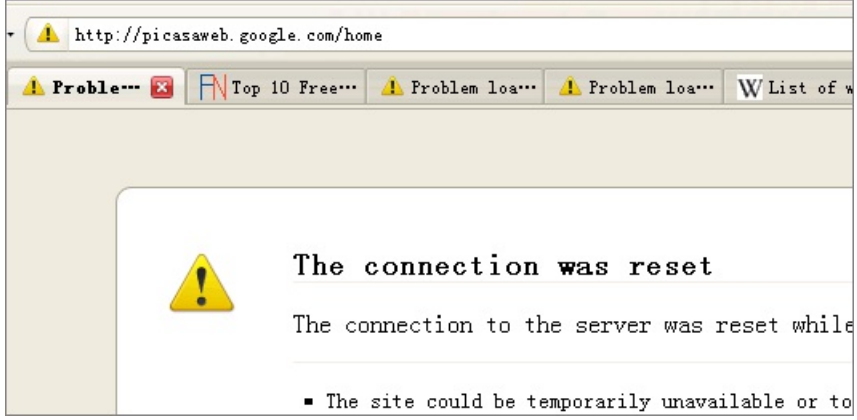
4. Blogger

5. Technorati

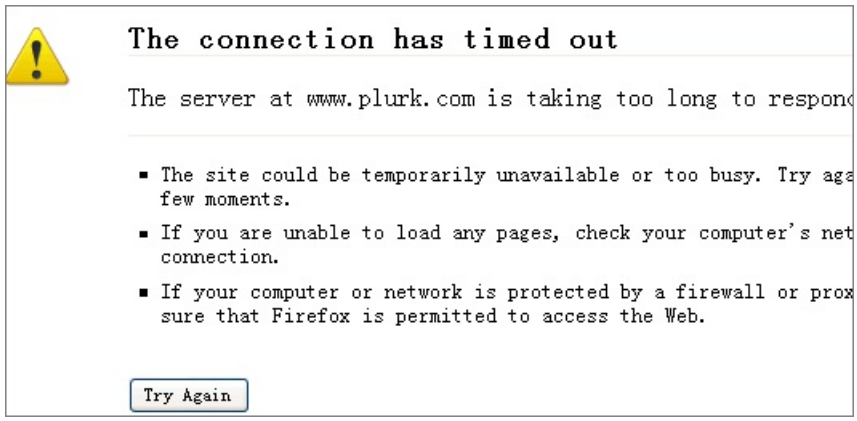


6. Dailymotion

7. Picasa

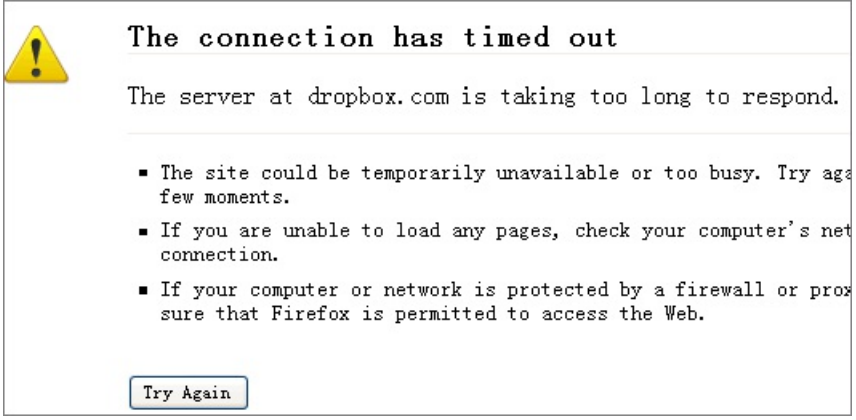


8. Plurk



9. Hellotxt

10. Dropbox



而要访问**以上 10 个被墙的网站，你必**须**翻墙，不管是用** VPN、SSH、Proxy，还**是其他工具。而如果哪一天可以不用翻墙就能**够访问这 10 **个网站，那么中国的互**联网**大概就自由了。**

第二节：哪些国家墙了 Facebook？

Free Nuts 博客曾列举了 Facebook 评论插件的 10 大不足之处，其中一大是该插件有可能无法显示，因为有些国家是禁止访问 Facebook 的。

那么，到底哪些国家墙了 Facebook 呢？根据维基百科的记载，一共有以下 6 个国家：

1、孟加拉

2、中国

3、伊朗

4、巴基斯坦

5、乌兹别克斯坦

6、越南

除了以上六个国家之外，维基百科说叙利亚也和谐了 Facebook，但是根据美国国务卿希拉里·克林顿今年 2 月 15 号在乔治华盛顿大学的演讲，叙利亚在 2 月初已经解除了对 Facebook 的封锁，所以，它不再是以上国家的墙友了。

作为一名墙国的用户，上 Facebook 网站是一件相当痛苦的事，因为你需要通过一些 VPN 服务或者其他的翻墙工具才可以上，而这样会明显拖慢页面的加载速度。虽然也有不少第三方应用工具（例如 IM+），但是用户需要登录 Facebook 对它们进行授权之后才能使用，甚至有些（例如 SocialScope）本身也被墙了，一样需要翻墙才能使用。尽管这样，我还是坚持经常甚至天天登录 Facebook 网站，因为那里和 Twitter 网站一样，可以体验到什么叫做红杏出墙。

希望在不久的将来，以上 6 个国家的互联网越来越自由，到 2012 的时候，这些国家的网民都可以不用翻墙直接登录 Facebook 网站。

第三节：信息是封锁不住的

“历史作为一个过程，本身是没有对错的；历史作为一种学问，应该被公开讨论；历史作为一种财富，应该与世界分享。

封锁信息，就是对历史的不尊重，就是不敢正视现实，就是懦夫的表现。

封锁信息，对下一代是不公平的，侵犯了他们对历史的知情权。

历史不会因为信息封锁而消失，信息是封锁不住的。只有正视过去，才能面对未来。

自愿的事情如果摆到桌上大家讨论，结果肯定是双方都有过错；而不允许讨论，则只能让人觉得你心虚，全是你的错。

老毛时代的不可能在老邓时代变成了可能，老邓时代的不可能在江胡时代还是不可能，但是不代表永远都是不可能，我期待那个可能的时代早点到来。”

以上的内容曾经于2009年6月4日发表过，是抓耳挠腮的作品。为了证明“信息是封锁不住的”，为了证明在互联网上，“除非你不说话，否则你说的每一句话都会被记载”，也为了证明我对“信息封锁”的深恶痛绝，特意把这几句在不情愿的情况下写就的话情愿地再说一遍，并且同时也把曾经删除的“不和谐”作品附上，算是保存历史记录吧。

上面的话你就当我瞎说吧，因为真正让我非操不可的是 GFW 劫持我发财，加上看到国家领导人的儿子手里掌控着几百亿的资产，我心里不平衡，所以就决定大操　GFW。昨天有操过一次，不过觉得不过瘾。于是，在　qingk2、久酷、Fangs 等同学的启发下，我搜索并尝试了十种不同的操 GFW 的招式。

这些招式简单易用，实属居家旅行的必备良方。

操 GFW 第一招——GAppProxy

这招简单易用，速度很快，只要下载 GAppProxy 然后解压并设置HTTP代理为 127.0.0.1:8000 就可以使用了。

下载和使用说明请点击 GAppProxy。

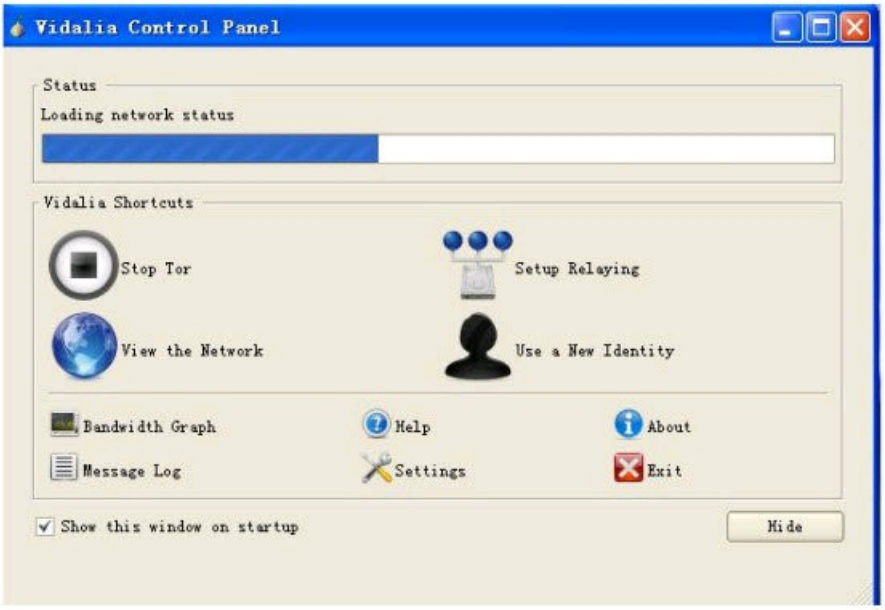
操 GFW 第二招——Go2

只要登录 Go2 网站，输入网址，就可以冲破 GFW 的封锁了。

不过，这招有一个缺点就是原文链接全改了。

操 GFW 第三招——Tor Browser

这招我是从德赛公园那里学来的，不过现在**德赛公园**已经被墙，你可以通过上面第二招进入**德赛公园** Tor Browser 介绍页面，下载 Tor Browser 之后双击那个葱头就可以了：



这招有两个不足的地方：一是软件启动后会自动弹出一个新的 FireFox 界面；二是速度真的很慢，很难达到高潮。

操 GFW 第四招——Hotspot Shield

这招是我昨天操 GFW 所用的，下载安装就可以使用了：

不过这个软件最大的缺点是广告很多很烦人。下载请点击 Hotspot Shield 官方网站。

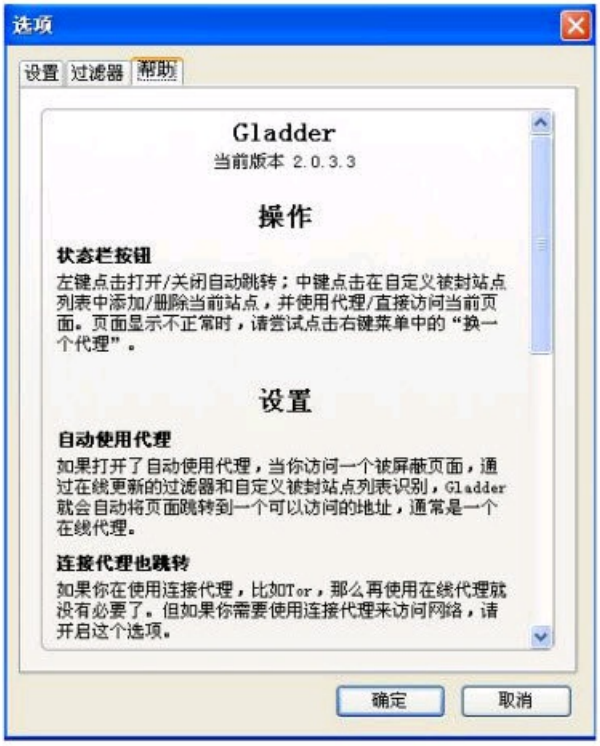
操 GFW 第五招——TOR + FoxyProxy

这是周曙光极力推荐的招式。你可以点击看看周曙光写的《手把手教你使用TOR+FoxyProxy突破GFW》，教程虽然写得很详细，不过我觉得还是有点繁琐，没有 Tor Browser 简单。

当然，你也可以直接点击 TOR + FoxyProxy 分别下载。

操 GFW 第六招——Gladder

此招只能在 FireFox 浏览器上使用，安装后在"查看——工具栏——定制"弹窗找到 gladder 并拖到工具栏，梯子发亮时你就可以翻墙了。



点击 gladder 就可以进入安装页面。

操 GFW 第七招--无界浏览

这招目前只适用于 IE 浏览器，不过速度挺快的。

下载地址：Box.net。下载之后解压再运行 u94.exe 就可以通过 IE 浏览器翻墙了。

操 GFW 第八招--语言工具

这招只要登录 Google 的语言工具页面，然后在"翻译网页"输入 URL，选择目标语言，点击"翻译"就可以翻墙了。

其实，你在"翻译下列文字"输入 URL 再点击"翻译"也是可以的。

操 GFW 第九招--PHProxy

和第二招 Go2 差不多，都是在线代理，登录 PHProxy 网站，输入 URL 就可以翻墙了。

PHProxy 目前没有任何广告。

操 GFW 第十招——psiphon2

根据 sesawe 网站的介绍，“向 english@sesawe.net 发送电子邮件请求，说明 ‘can I have psiphon2 access’ 并告诉我们您所在的国家。您将收到一封电子邮件，其中有 psiphon2 邀请”，我昨天晚上9点多发了邮件，3个多钟后收到了邀请码。

小三的博客对 psiphon2 的使用 做了图解，有兴趣可以看看。

当然，操 GFW 的方法还有很多，可能吧、刀客征途等博客都有介绍，如果你能够在大陆访问 GFW Blog，就说明你会翻墙了。如果你有更多更好的操法，欢迎分享。

0 Comment Tags: GFW, 翻墙

leesum said on March 18th, 2009 at 9:15 am | Edit

招招必杀……我还是习惯用FF+插件，轻松翻墙

Reply

Poshi said on March 18th, 2009 at 9:25 am | Edit

第八招不错呢，以前没有想過。

不過，似乎是不是太直接太敏感了些？現在在風口上。。。

你在上面提到的一個人物，是不是姓鄒的，我聽上一代的人說，以前在中國出關的那些走私販只，都是只要報上某人的名號，都是免查，免稅的呢

Reply

kxboy said on March 18th, 2009 at 9:31 am | Edit

Hotspot Shield 去广告有一个很简单的法子，Firefox可以安装插件User agent swither，然后在 工具-User agent swither-选项中—把Default改成Opera，就可以去掉广告了。

Reply

joojen said on March 18th, 2009 at 9:39 am | Edit

纠正一下，据我实测，无界启用后不只是ie能用，我使用google chrome可以正常使用，firefox装个“无界火狐工具”插件后也能正常使用。

Reply

Darius said on March 18th, 2009 at 9:48 am | Edit

老胡儿子胡海峰控股手上掌握了几百亿的资产的新闻是你在Twitter上发的吗？可有原文出处？young_yang，

Reply

久酷 said on March 18th, 2009 at 10:24 am | Edit

居家必备常用工具^_^

Reply

Young said on March 18th, 2009 at 12:00 pm | Edit

@Darius: 原文信息是 @amolist 同学发在 Twitter 上的，我没有去验证。
@joojen: 谢谢纠正，晚点我会更新一下。
@kxboy: 谢谢你的分享，晚点我玩一下。
@Poshi: 哈哈，操一下 GFW，不会成为政治犯吧？文章中提到的那个人姓胡，不过我没有求证过。

Reply

探客 said on March 18th, 2009 at 12:23 pm | Edit

这些都是躲，操，我操。

Reply

three said on March 18th, 2009 at 12:23 pm | Edit

这个帖子不会被和谐的吧？

Reply

东方博客 said on March 18th, 2009 at 12:35 pm | Edit

估计要被和谐了~

Reply

dhqdx said on March 18th, 2009 at 1:03 pm | Edit

很全啊，博主当心被河蟹

Reply

cooku said on March 18th, 2009 at 3:07 pm | Edit

无界or自由门+firefox+FoxyProxy其实蛮好用的。。。一次设置，终身无忧。。囧。。。

Reply

welee said on March 18th, 2009 at 4:38 pm | Edit

唉~上个网还要那么折腾...辛苦了！

Reply

Young said on March 19th, 2009 at 4:55 am | Edit

@joojen:请问哪里可以下载“无界火狐工具”？我无法从无界下载。
@cooku:请问哪里可以下载“自由门”？

Reply

cooku said on March 19th, 2009 at 9:19 am | Edit

那啥，我一直在小x软件的网址后面加/f/下载xx门 嗯 为避免广告嫌疑，于是我做了屏蔽

Reply

meijindaozei said on March 19th, 2009 at 11:17 am | Edit

@leesum:
FF的翻墙插件是什么，之前装过的，忘了，能够告诉我一下，谢谢

Reply

Young said on March 19th, 2009 at 6:56 pm | Edit

@cooku:谢谢，已经下载了自由门，还认识了一下7z文档。

@meijindaozei:你是指 Gladder 吗？

Reply

yaoguai said on March 19th, 2009 at 11:16 pm | Edit

Hotspot Shield最好用。用kmeleon游览器就没广告出来了。

Reply

Gavin said on March 20th, 2009 at 12:59 pm | Edit

好多不行的，有个轮子网站被转接到人民网了，好笑

Reply

xiao3 said on March 20th, 2009 at 3:02 pm | Edit

我想问问，我的博客feed源地址两天不更新啦！出现如下情况：
CDATA 节未关闭。
行: 33 字符: 25
<![CDATA[

见过你以前似乎也出现过这个情况，能说说这个是怎么回事啊?我的feed源地址是：http://xiao3meng.org/feed/

Reply

原子菌 said on March 20th, 2009 at 8:46 pm | Edit

good thing ,fuck gfw

Reply

Poshi said on March 20th, 2009 at 11:43 pm | Edit

中國有個女學生，已經因為寫博客成為犯人了，所以最好小心

Reply

---

llllll said on March 21st, 2009 at 5:29 pm | Edit

无界 自由门 赛风都用过 学习一下 以后试试别的

Reply

Young said on March 22nd, 2009 at 3:03 am | Edit

@xiao3:你的 Feed 目前正常啊。

@Poshi:谢谢关心，不过该操还是得操。

Reply

深圳SEO said on March 22nd, 2009 at 11:13 pm | Edit

操吧，路过，打酱油去了。

Reply

---

graphis said on March 25th, 2009 at 9:53 pm | Edit

Hotspot Shield 的速度很快
用火狐或ie的话广告很多，
opera。一点广告都没有。

Reply

Payne said on March 26th, 2009 at 10:16 am | Edit

无界是可以用在firefox的，无界＋foxyproxy插件，在foxyproxy设置添加代理，只需添加端口就ok了，个人觉得最好用的

Reply

California said on March 26th, 2009 at 12:47 pm | Edit

什么是GFW？是Going to Foreign Website ??

Reply

Young said on March 26th, 2009 at 7:32 pm | Edit

@Payne:谢谢告知。我现在主要用psiphon2。:-)

@California:GFW 是 the Great Firewall of China 的简写。

Reply

sailor said on March 28th, 2009 at 9:35 am | Edit

operaton这个软件也可以

Reply

Burning said on March 28th, 2009 at 11:51 am | Edit

gappproxy（freedoor）+autoproxy 很不错

Reply

Everest said on March 30th, 2009 at 2:19 pm | Edit

太不和谐了。哈哈，被和谐前，收藏之。

Reply

xman said on April 5th, 2009 at 10:01 pm | Edit

大部分都对我无效，

Reply

i9 said on April 9th, 2009 at 4:58 pm | Edit

今天,是,今天
hss连接后强制升级到1.14
之前并未强制升到1.13
1.14的作用就是:我的电脑再无法连接任何网络包括hss本身
卸载后一切恢复正常
再装,依旧升到1.14然后自动把我电脑墙了
hss当叛徒了么 真的要14么

Reply

LianKK said on April 12th, 2009 at 2:50 pm | Edit

我是自由门和无界老用户了，最近不大上得去。

Reply

听临 said on May 1st, 2009 at 11:41 pm | Edit

翻墙好。。。
谢谢你的工具。不错咱

Reply

DVD said on May 6th, 2009 at 3:00 pm | Edit

SB一个

Reply

mankills said on May 6th, 2009 at 7:51 pm | Edit

肮脏的血液染红了美丽的天安门，世界纯洁了，不洁被消灭，Oh, mybaby，我的神呐.. 掰起点句.咳咳。那啥，为什么我还是操作不了伟大的自由门.自由没有门，囧.....

Reply

AIMILIZZ said on May 9th, 2009 at 9:39 am | Edit

很不错,今天看还是没有被GFW,招招都不错,很实用,非常感谢

Reply

林康 said on May 10th, 2009 at 9:54 am | Edit

我这里有无界浏览的最新版本，还有动态网的最新版本，需要的发邮件就可以了！长期提供！

Reply

推荐两个代理软件 | Wang Chengxi's Blog said on March 18th, 2009 at 5:22 pm | Edit

[...] 在贵国（因为房子、学费等什么都很贵，所以有人叫贵国），一些"低俗"的网站都会被GFW墙掉（"强"在这里是动词，挡住、隔离的意思。什么是GFW？），据说是为了避免我们社会主义的纯洁性遭到侵蚀，当然，这个纯洁性是不是真的纯洁，你自己认为就可以了。那如何访问这些"低俗"的网站呢？这就要学会翻墙了，也可以叫操GFW。操GFW有很多种方法，操GFW十种简易招式介绍的够多的，你可以自己慢慢看，选择自己喜欢的那一种体位。 [...]

一天到晚游泳的鱼 » Blog 存档 » 2009/04/05 Great Fire wall of china said on April 5th, 2009 at 10:08 am | Edit

[...] 互联网知识一：Great Fire wall of china [...]

希望以后我都不用再写这样无聊的文章，有时间还是去谈情说爱好。

第四节：我国 Twitter 上的第一个文字狱

据 Amnesty 网站报道，一个叫程建萍（即王译）的女士因为在推特上说了五个字被以“扰乱社会秩序”的罪名判劳动教养一年，也就是差不多说一个字就要坐牢两个月。

整个事情的经过是这样的：

10 月 17 号，程建萍女士（@wangyi09）锐推她未婚夫华春辉（@wxhch）先生的一条 Twitter 信息，并且在信息前面加上了“愤青们，冲啊！”这么一句话，整条信息如图所示：

就因为上面图片里面的那条信息，华春辉先生被拘留 10 天，程建萍女士被判 1 年的劳动教养，这就是文字狱，也是国内第一个因为在 Twitter 上说话而被逮捕的文字狱，但是这样的文字狱是不是冤案呢？那就要看大家是如何理解“扰乱社会秩序”这个罪名的了。不过这样的文字狱在世界上并不是首例，今年一月份一位年轻的英国男子由于在 Twitter 上扬言要炸飞罗宾汉机场而被逮捕、被炒鱿鱼并被永久禁止进入罗宾汉机场，而这也仅仅是因为一条 Twitter 信息。可见，在 Twitter 上乱说话是会被逮捕的，不管是在国内还是在国外。

回到王译的文字狱，暂且不论判决的结果是否公平，也不管王译所说的是否真心话（我相信那只是一时的气话），那条信息的内容是很危险的，本来砸馆的说法就是滥伤无辜，你鼓动他人砸馆就更糟糕了，所以王译受到的惩罚比华春辉的要重。不妨想想，你如果说你不支持党，那么党可能不理你，因为你只是一个屁民，但是如果你鼓动他人和你一起不支持党，那党就会找你麻烦了，因为它要以儆效尤。当然，也不是说鼓动别人做事不好，关键要看是谁鼓动以及鼓动什么，像昂山素季那种鼓动整个国家的人为自由而奋斗就是英雄的行为，尽管这样的行为也给她带来了牢狱之灾。

另外，我相信王译说“愤青们，冲啊！”的时候只是贪好玩，也没有人因为看到她的那条 Twitter 信息而去砸馆，但法律是无情的——不管它是否公平，也不论你是否知道——除非你爸是李刚。

还有，老大哥想方设法不让屁民上 Twitter，但是又无时无刻不在关注屁民在该网站上说的每一句话，并且随时有可能鸡蛋里挑骨头，制造下一个文字狱。所以，愤青们，请不要乱冲，如果一定要冲，那就请冲啊凉。

第五节：中国茉莉花革命

做梦也没有想到中国的茉莉花革命来得如此之快，就在今天，而且我蜗居的城市广州也有集合地点——人民公园星巴克。

昨天深夜躺在床上看韩寒的新书《1988——我想和这个世界谈谈》，看完的时候发现已经是凌晨 4 点了，打算睡觉，但是睡不着，因为还不知道丁丁哥哥是怎么死的，虽然我猜测是死于 1988 过后的那场运动，但没有证据，因为陆小野都不知道他多少岁。所以又起来重新看一遍，跳过娜娜、10 号、刘茵茵等角色的内容，结果不但找不到证据，而且还增加了两个问题 —— 那个修车的为什么要以及如何攻击化工厂？陆小野是把那制片人的电脑给砸了，抑或只是删除了电脑里面的潜规则视频？

百思不得其解，但是那时已经 6 点了，只好强迫自己睡觉。也不知道有没有睡着，起来的时候已经是中午了，没有什么精神，并且满脑子还是 1988，所以吃过午饭后准备继续睡。不料睡前发现今天下午有个茉莉花革命，于是开始犹豫不决，到底是睡觉呢？还是去革命现场打酱油？

睡觉吧，这么大的事错过了有点可惜，何况去人民公园也只不过 1 个小时。但是去吧，又有点怕，一来前几天刚理了个光头，又没有帽子，怕影响广州市容；二来怕到时侯会被警察当流氓，或者被流氓当警察，白受罪。

一时无法决定，于是就继续在推特上逛，后来发现不少著名的维权人士都被喝茶、被失踪、被在家了，广州有位律师还被打了，人民公园附近有很多警车，等等，但是还没有看到一张现场图片，不像茉莉花革命的前兆，应该不会有血案发生，所以我就晕头晕脑的去了。

刚一出门，就撞见一个头比我还光的大哥，骑着一辆自行车，于是庆幸自己并不孤单；后来在地铁上又看到一个光头的，就觉得多了个志同道合的。在列车上我有开着 SocialScope 并时不时看一下有没有什么革命新闻，看完之后，就抬头看看周围有没有靓女，不过看见靓女之后，仍然无精打彩。

到公园前站的时候，大概两点半，一出站就去星巴克要了一杯中杯的热美式，一来可以提神，二来可以掩饰一下自己的紧张。

在排队等咖啡的时候，我想 Check-in 一下，但是 SocialScope 搜索不到位置，于是作罢并认真环视一下，发现原来里面只有一张没有椅子的空桌子，有靓女帅哥，但没有穿警服的。取咖啡的时候，我拿了一根吸管，但是递咖啡的靓女马上就抢回去了，说热饮是没有吸管的，语气很坚定，也没有“先生”或者“不好意思”这样的客套话。我没有精神搭理她，走到放糖的地方拿了一根吸管，然后就上楼了。

楼上也没有空位置了，于是就往外面走，发现露天的桌子也没有空的了，这个茉莉花革命还真的挤爆了星巴克。不过这个时候我已经看到警察了，站在星巴克外面的广场上，接着看到了警车，除了人行道上等着过马路的之外，没有发现超过 10 个人扎堆的，也没有看到举牌子的，更加没有听到任何人喊口号，或许我来晚了，又或许这就是茉莉花革命。

但是咖啡还没喝完，况且也是第一次来，于是就顺便到旁边的人民公园逛了逛，不逛不知道，一逛吓一跳。里面有警车，并且每走几步就会碰到警察，他们有的一个人，有的两个人，有的三个人，有的多个人，不过除了路边一车打盹的，也没有看见有 10 个警察扎堆的。警察遍布公园的每个角落，广州古城十八门、跳舞广场、鲁迅塑像、..... 甚至上个厕所都会在里面碰到警察。

每次从警察的旁边走过，我都有点担心会被询问，但是结果并没有警察理我，看来我这个穿着黑色风衣黑色运动裤的光头老还不像流氓。也没有发现警察突然叫住其他游客询问，不过倒有听到两个游客问一警察：“这条是什么路？” 然后那个警察说：“公园路。” 除此之外，公园也没有意外，一切都那么和谐。跳舞的还是在跳舞，唱歌的还是在唱歌，打羽毛球的还是在打羽毛球，.....

逛完之后，发现原来整个公园都被警车和警察围住了，附近还有警车在巡逻，在这样的情况下，恐怕恐怖分子都会知难而退，何况不明真相的群众。这时，那杯热美式也已经喝完，又没有艳遇，所以就回去了。回去的路上又碰到一个光头的。

后记：大家翻墙 GFW 倒

众人拾柴火焰高，大家翻墙 GFW 倒。

对此，我是深信不疑的，因为万物都需要经过生死，这是自然规律。

但是 GFW 什么时候倒以及怎么倒，那我就不知道了，不过有一点可以肯定的是，如果大家都翻墙，那么它就会倒得快点。

这里所说的“大家”，是指那些翻墙或者对翻墙感兴趣的人，并不是指所有人。因为毕竟有人是从来不访问 YouTube、Twitter、Facebook 或者其他国外网站的，毕竟有人不知道 GFW 是神马的，毕竟有人甚至连网都不上的。所以，人有选择翻墙的自由，也有选择不翻墙的自由，甚至可以选择一边翻墙一边坚决拥护 GFW。

总之，翻墙的事，不能一厢情愿，需要大家两厢情愿。

只要大家两厢情愿，真爱总是有的，只要大家都想翻墙，方法总是有的。

而翻墙的工具无非就两种，一种是收费的，另外一种是免费的。如果有人跟你讲，收费的比免费的好，不要信，因为一切都是相对的，你不能单单用钱来衡量一样东西的好坏。

所以，免费的也有好的，例如这本书里面提到的 100 多个，其中包括全世界流行的 Proxy、SSH、VPN、等等。

也有人说，不要公开介绍免费的翻墙工具，因为会有被墙的风险，这话说得有点道理，毕竟现在不少翻墙软件（例如自由门、无界、Tor、等等）的网站都被墙了。但是对付 GFW，你不能玩阴的，因为它是阴的，不怕阴，只怕光，正所谓相生相克。

另外，书里面介绍的所有免费翻墙工具都是公开的，要不我就不会知道它们的存在，而介绍它们，只是为了能有多几个翻墙工具可以备用而已，因为没有哪一个翻墙工具是可以保证不会被墙的，如果它们对大家翻墙也有用，那就更好了。

还有，翻墙工具的网站被墙，并不等于这些翻墙工具也无法翻墙了，其实，自由门、无界、Tor 等工具一直被墙，但是也一直更新翻墙。

再说，真的翻墙工具，敢于直面操旦的 GFW，敢于突破不断的封锁，而这样的翻墙工具，大家可以在书里面找到。