飞跃手册

Complete Manual of Circumventing the Great Firewall

集体编写

第一版

飞跃手册

GFW是什么篇

禁闻代理-轻量级翻墙工具

禁闻代理简介：
禁闻代理翻墙,轻量级翻墙工具,极速访问绝大多数被墙网站.
最新版下载：
https://github.com/bannedbook/fanqiang/wiki
禁闻代理下载 下载短网址: https://git.io/jwd

禁闻代理使用说明：
禁闻代理提供 2 种翻墙模式，代理模式和直翻模式，默认使用代理模式，如果代理模式链接不畅，可尝试使用直翻模式。推荐使用 Google Chrome 浏览器。下载解压后，双击 jwproxy.exe 启动程序即可实现翻墙浏览了。

支持平台：
禁闻代理中的 jwproxy.exe 为 PC 平台 Windows 程序，支持 Windows XP、Windows 7、Windows 8、Windows 10 等环境。
压缩包中携带的 htm 文件，为 htm 版翻墙工具，只要用支持 js 的浏览器打开即可翻墙，无论任意平台、任意设备只要能打开本地 htm 文件并支持 js 的浏览器都可实现翻墙。

安卓翻墙工具-禁闻浏览器 JWBrowser

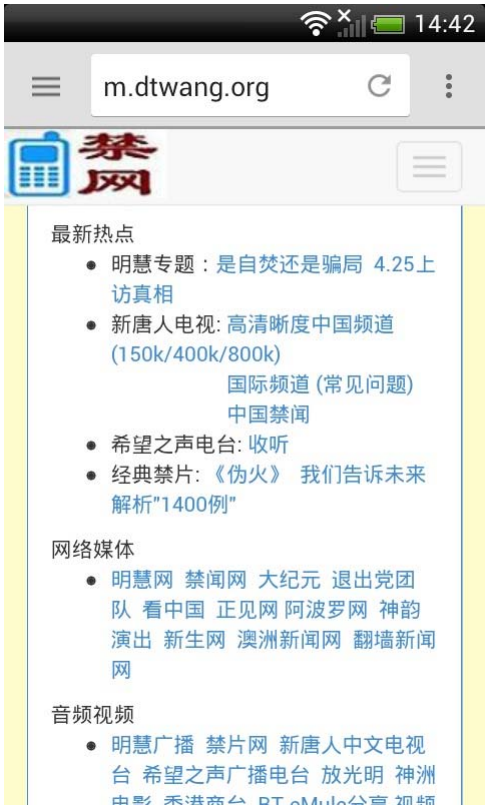
安卓翻墙工具-禁闻浏览器 JWBrowser 简介：
安卓翻墙工具-禁闻浏览器 JWBrowser 翻墙,轻量级翻墙工具,极速访问绝大多数被墙网站.
禁闻浏览器 JWBrowser 由禁闻网出品，宗旨是帮助中国大陆网友自由翻墙上网，获取海外自由世界的信息。

特别提醒：
禁闻浏览器 JWBrowser 不加密网络流量，对安全性要求很高的敏感人士建议慎用或不用。

使用说明：如果代理暂时无法连接，请不要删除应用，我们很快就会更新，也许过一会儿就好用了。

最新版下载：
https://github.com/bannedbook/fanqiang/wiki#androidfq

下载：
禁闻浏览器下载　下载短网址:https://git.io/vzafO 从 Google 安卓市场下载:翻墙



飞跃手册

實戰分析篇

致謝　關於

什么是墙？

在大陆访问某些外国网站时，你是否时不时见到下面的界面？

前言

IE

提示无法显示该页面

Google Chrome

提示 **Web page is not available**

Firefox

提示 **Connection Interrupted** (中文版译为 连接被重置)

这说明：您被“墙”了!!!

墙是中国大陆网络审查及屏障机制（也称防火长城）的简称

> **墙**是中国政府监控和过滤互联网内容的软硬件系统，由服务器和路由器等设备，加上相关的应用程序所构成。由于中国网络审查广泛，中国国内含有“不合适”内容的网站，会受到政府直接的行政干预，被要求自我审查、自我监管，乃至关闭，故防火长城主要作用在于分析和过滤中国境内外网络的资讯互相访问

根据哈佛大学的一项研究，目前至少已有

18,000+个网站在中国大陆被封锁

证据表明，这是中国大陆政府所为

在美国，网络审查仅用于防止侵权内容的传播

在香港，仅屏障对未成年人不利的网站

在中华民国，不做限制，但是自动在限制级网站中加入特殊标签

中国大陆政府不应该对网络审查的事实隐瞒真相

读完本书您将学会翻墙技术

了解互联网审查的内幕

希望您能将掌握的翻墙技术教给更多的人

超級小饅頭序

凡讀本書請先具下列諸信念：

一、當信任何一國之網民，尤其是自稱知識在水平線以上之網民，對其本國以外之網絡，應該略有所知。否則最多只算一有知識的人，不能算一有知識的國民。

二、所謂對其本國已有封鎖略有所知者，尤必附隨一種對其國外開放之溫情與敬意。否則只算知道了一些外國，不得雲對外國民主自由有知識。

三、所謂對其國外開放有一種溫情與敬意者，至少不會對其外國歷史抱一種偏激的虛無主義，即視外國已往歷史為無一點有價值，亦無一處足以使彼滿意。亦至少不會感到現在我們是站在已往歷史最高之頂點，此乃一種淺薄狂妄的進化觀。而將我們當身種種罪惡與弱點，一切諉卸於國外反對勢力。此乃一種似是而非之文化自譴。

四、當信每一國家必待其國民具備上列諸條件者比較漸多，其國家乃再有向前發展之希望。否則其所改進，等於一個被征服國或次殖民地之改進，對其自身國家不發生關係。換言之，此種改進，無異是一種變相的文化征服，乃其文化自身之萎縮與消滅，並非其文化自身之轉變。

士之讀書治學，蓋將以托心志於俗諦之桎梏，真理因得以發揚。思想而不自有，毋寧死耳。斯古今仁聖所同殉之精義，夫豈庸鄙之敢望！推友@multiple1902以一己之力，見其獨立自由之意志。嗚呼！來世不可知者也，先生之著述，或有時而不章；先生之學說，或有時而可商，惟此獨立之精神，自由之思想，曆千萬祀，與天壤而同久，共三光而永光！

超級小饅頭與民國九十九年，閱multiple1902所編《飛躍手冊》，鬥膽攢修錢穆先生及陳寅恪老師之文字，是為作序。敬祝我中華民族獨立之精神，自由之思想在狂風暴雨中，永遠屹立不搖；在淬礪磨練後，更為燦爛奪目！

超級小饅頭 民國99年2月19日 致辭

拥抱自由（自序）

没有深度的思考，其实质等于没有思考。没有深度的发言，其实质等于没有发言。党媒之文章之所以不值一读，因为其文正如其人，不能正确对待不同的意见和观点，而是通过各种下流的手段来贬低对手、提高自己。文章的读者大多有自己的大脑，了解事情的真相后可以自己做出判断。然而他们如此喜欢混淆黑白，以至于相当一部分群众怀疑自己是不是有知道真实情况的自由。

是自己的自由，就不要怀疑。

应该确信无疑，你有上网的自由，也有不上网的自由；你有上这个网的自由，也有上那个网的自由；你有今天上网而明天不上网的自由，也有今天不上网而明天上网的自由。总之，上网的自由一点也不亚于上厕所的自由。如果一天政府说，你不能访问一个既非色情也非成人的网站，没有为什么，就是不能访问，那给我的感觉就像便便之后不给冲水一样荒诞可笑。这种荒唐的事情发生了。不要问我为什么，这是中国呀！你还想不通吗？

我认为安全、无障碍地访问互联网的自由，理所当然地应当被每个人所享有。稍有常识的人都能看出，这与他们素质是不是太低不适合实行民主无关。

2010年，史上最贵的世博会将在中国上海举办，作为东道主，我感到压力很大。一旦外国来宾遭遇了上网障碍，对我国互联网“全世界最自由”的论调产生怀疑，我们可以用这本手册告诉他，那是因为你们智商太低不适合实行翻墙上网制度。

在本书中，还对参与GFW项目研发的单位和个人的名单做了整理，对于重点参与者做了大篇幅的介绍。如果有那么一天，具体的个人应当为他今天的所为承担责任。

由于编写仓促，错漏在所难免。在此向所有支持本书编写的网友致谢！

multiple1902
西元2010年2月20日晚于南京

中国网络封锁和监控简史

文 / 黄健

STEP 1

封锁少数揭露真相的网站

还记得我离开中国的前夜。当时正值某组织遭受全国性的清洗。明明几天前还可以登录的网站，忽然间都无法登陆了，有的页面更为可疑，打开一半时突然出错。和许多人一样，这也是我平生第一次清楚体验GFW的存在。只是当时并不了解它的工作原理，也对之束手无策。

第一次的亲密接触虽然短暂，但却印象深刻。从那时起，中国正式对互联网上的内容开始了审查。这应该是1999年前后。

在这一阶段，被封锁的多为国外网站，这些网站无非是民运人士活动的前沿阵地，对于国内大多数人影响不大。除此之外，这一时期被封闭的还包括Wikipedia、YouTube等智库型的网站。这些网站提供的真实信息使政府感到前所未有的恐慌。

由于当时GFW采取的方法是将主机列入黑名单和对页面进行关键字过滤，所以有很多方法可以绕过。翻墙软件随之开始在国内兴起，当时的方法也主要是基于HTTP代理。但很有意思的是，直到今日，这些翻墙软件居然无一是墙内的中国人自己开发的。

诞生之初的GFW，从一开始起就暴露了行动迟缓的特征。GFW运作无非是发现一个屏蔽一个，这种守株待兔的被动做法使漏网之鱼甚多。也正是由于这一时期的行动迟缓，才会有后面无法逆转的发展。

STEP 2

遏制国内不和谐声音

随着互联网在中国的发展，民主自由的信息“随风潜入夜，润物细无声”地进入了中国普通知识分子的视野。随之而来的是国内BBS、论坛、网站、博客上不和谐的声音逐渐增多。

由于这些“有害”信息都是在中国互联网内部的，所以设置在国境线上的GFW审查设备根本无用武之地，新的方案呼之欲出，其中不乏一些令人啼笑皆非的。网络监控的主战场也从国外转向了国内。

中国网络封锁和监控简史

对于这些越来越多的国内“有害”信息，政府机构采取的主要方式是威胁国内的网民和互联网服务提供商。这段时间颁布了一系列的条例，如实名上网、网站备案，以及规定网站对于用户发言负法律责任，逼迫网站实行自我审查。一时间，许多著名论坛、博客、网站人人自危，关闭和删贴风起云涌。其中不乏一些国际性的著名网站，如谷歌和微软，他们在压力下不得不对中国政府妥协。

同时政府又雇用一些“网络评论员”——五毛——对网络民意进行引导。最诡异的监控方案莫过于2009年5月工信部出台的绿坝预装方案。这一方案一出台便如过街老鼠般遭受各方强烈抨击，最终不了了之。但是这一方案的提出从一个侧面体现了政府对于互联网正面临全面失控，并极力争取以简单粗暴的手段夺回控制权。这一信息使网民信心大增，同时也把这场原本暗中的较量摆上了台面。

这一时期的网络监控对许多人生活造成了影响，也引起了普通人的反感、好奇和关注。网络上一时间怨声载道。同时，由于许多国内关闭的网站被迫流亡海外，一个适得其反的结果是，在这段时间内，翻墙在国内网民间迅速流行开来。

魔高一尺道高一丈。同一时间，一场封锁和反封锁的竞争在翻墙软件和GFW之间展开，双方都不断以升级来抵消对方的升级。但是，GFW始终无法找到终极封锁方案，却始终有翻墙软件可以找到它的破绽，GFW再一次在这场竞赛中面临尴尬境地。

STEP 3

向信息交流平台开战

经过这两个阶段一路伴随中国互联网成长起来的人，由于对于自由获取信息产生了依赖，同时对于传统媒体习惯性的撒谎忍无可忍，翻墙已经成为许多人生活的一部分，更多人也开始加入翻墙的行列。这段时期另一个重要的现象就是许多互联网专业人士加入了翻墙的行列。他们对于翻墙技术的传播和革新起到了重要推动作用。他们借助最新的互联网技术给GFW出了一个接一个的难题。

这段时期又恰逢大事件发生的高峰期。民族事件、历史纪念日、自然灾害、庆典盛会、维权示威、黑恶事件、食品医疗事故等等层出不穷。这些事件的报道和揭露都借助最新的网络技术以不同形式得以实现，直至网络直播形式的出

中国网络封锁和监控简史

现，彻底击毁了传统媒体形成的信息垄断，引起政府的强烈恐慌，同时也促进了网络维权事业的蓬勃发展，为即将到来的更大规模的抗争做好了准备。

大到社交网站，如Facebook，小到微型博客，如Twitter在这一时期纷纷落马。基于P2P技术的资源分享平台，如VeryCD、BTChina也在这一时期沦陷。从2009年后半年开始，传播信息的平台成为了这一轮争斗的主战场。但是很快，政府将会意识到，真正的敌人不是这些平台，而是信息传播本身。

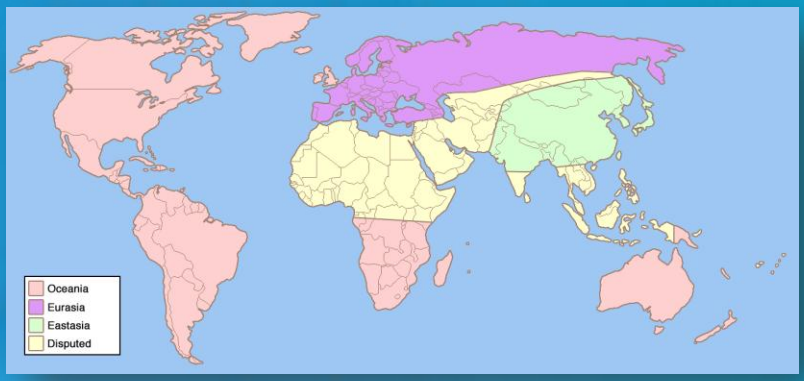
这一阶段将是决定输赢的一步，所以政府一定会不遗余力地最后一搏。在可预见的将来，从文字到图片、从音频到视频，所有形式的传播都无法幸免。更多的网站将被关闭、网络审查设备的更新将会更快、更多的网监和五毛将被雇用。直至监视所有即时通讯、电子邮件、短信；监听所有移动通话，当然也承受更多来自社会的责骂。这虽然无疑将耗尽社会资源，但似乎是唯一的出路，因为这一步如果不能一剑封喉，那么双方心里都很明白，剩下的选择只有缴械投降了。

STEP 4

切断一切信息交流

如果还有第四阶段的话，这一阶段将是短暂的。届时中国将关闭互联网、移动电话网，新疆的局面将会扩散到整个中华大地。和朝鲜一样，中国将回归飞鸽传信的年代。届时大量外资将撤离；股市将崩盘，改革开放活动将顺利落下帷幕。

最近发生的一切，说明历史已经走到了第三阶段的后期。在经历短暂的黑暗之后，光明最终将会到来，互联网的到来加快了这一历史进程。对于他们来说，真希望一切都可以重来。



乔治·奥威尔小说《一九八四》中的世界分为大洋国、欧亚国和东亚国。

“GFW”的前世今生

编者按：根据维基百科介绍，金盾工程，有时被称为“中国国家防火墙”，指的是中华人民共和国公安部对国内互联网的监视和审查机制。本文由匿名投稿并在自由新闻首发。在不改变原意的前提下，编者对本文有删改。

写在前面

标题的GFW之所以加上引号是因为，GFW是局外人起的绰号，它的真实称呼并非如此，但“GFW”也确实如实涵盖了这一在中国一贯隐晦而模糊的概念。

雪中的长城

时间表

●1998年9月22日，公安部部长办公会议通过研究，决定在全国公安机关开展全国公安工作信息化工程——“**金盾工程**”建设。
●1999年4月20日，公安部向国家计委送交**金盾工程**立项报告和金盾工程项目建议书。
●
●1999年6月，**国家计算机网络与信息安全管理中心**成立，局级事业单位。
●

●1999-2000年，在哈尔滨工业大学任教多年的**方滨兴**调任国家计算机网络与信息安全管理中心副总工程师。
●1999年12月23日，国务院发文成立国家信息化工作领导小组，国务院副总理吴邦国任组长。其第一下属机构计算机网络与信息安全管理工作办公室设在已经成立的国家计算机网络与信息安全管理中心，取代计算机网络与信息安全管理部际协调小组，对“公安部、安全部、保密局、商用密码管理办公室以及信息产业部”等部门的网络安全管理进行组织协调。
●2000-2002年，**方滨兴**在国家计算机网络与信息安全管理中心任总工程师、副主任、教授级高级工程师。
●2000年4月20日，公安部成立**金盾工程**领导小组及办公室。
●2000年5月，005工程开始实施。
●2000年8月19日，大纪元时报创刊。
●2000年10月，信息产业部组建计算机网络应急处理协调中心。
●2000年12月28日，第九届全国人民代表大会常务委员会第十九次会议通过《关于维护互联网安全的决定》。
●2001年，**方滨兴**“计算机病毒及其预防技术”获国防科学技术三等奖，排名第一。
●2001年，**方滨兴**获国务院政府特殊津贴、信息产业部“在信息产业部重点工程中做出突出贡献特等奖先进个人”称号，中组部、中宣部、中央政法委、公安部、民政部、人事部等联合授予“先进个人”称号。
●2001年1月19日，**国家计算机网络与信息安全管理中心上海分中心**成立，位于上海市黄浦区中山南路508号6楼。国家计算机网络应急技术处理协调中心上海分中心是工业和信息化部直属的中央财政全额拨款事业单位。
●2001年4月25日，“**金盾工程**”经国务院批准立项。
●2001年7月，计算机网络与信息安全管理工作办公室批准哈尔滨工业大学建立国家计算机信息内容安全重点实验室，胡铭曾、**方滨兴**牵头。
●2001年7月24日，国家计算机网络与信息安全管理中心广州分中心成立，位于广州市越秀区建中路2、4号。

时间表

●2001年8月8日，国家计算机网络与信息安全管理中心组建国家计算机网络应急处理协调中心，缩写CNCERT/CC。
●2001年8月23日，国家信息化领导小组重新组建，中央政治局常委、国务院总理朱镕基任组长。
●2001年11月28日，国家计算机网络与信息安全管理中心上海互联网交换中心成立。提供“互联网交换服务，互联网骨干网华东地区数据交换，数据流量监测与统计，网间通信质量监督，交换中心设备维护与运行，网间互联费用计算，网间互联争议协调”，位于上海市黄浦区中山南路508号。
●2001年11月28日，国家计算机网络与信息安全管理中心广州互联网交换中心成立，位于广州市越秀区建中路204号。
●2001年12月，在北京的国家计算机网络与信息安全管理中心综合楼开始兴建。
●2001年12月17日，国家计算机网络与信息安全管理中心湖北分中心成立。
●2002年，**方滨兴**任中国科学院计算技术研究所客座研究员、博士生导师、信息安全首席科学家。2002-2006年，方滨兴在国家计算机网络与信息安全管理中心任主任、总工程师、教授级高级工程师，升迁后任其名誉主任。
●2002年1月25日，报道称：“国家计算机网络与信息安全管理中心上海互联网交换中心日前开通并投入试运行，中国电信、中国网通、中国联通、中国吉通等4家国家级互联单位首批接入。中国移动互联网的接入正在进行之中，近期可望成为第五家接入单位。”
●2002年2月1日，国家计算机网络与信息安全管理中心新疆分中心成立。
●2002年2月25日，国家计算机网络与信息安全管理中心贵州分中心成立。
●2002年3月20日，多个国家计算机网络与信息安全管理中心省级分中心同时成立。
●2002年9月3日，**Google.com被封锁**，主要手段为**DNS污染**。
●2002年9月12日，Google.com封锁解除，之后**网页快照等功能被封锁**，手段为**TCP会话阻断**。
2002年11月，经费6600万的国家信息安全重大项目“**大范围宽带网络动态阻断系统**”（大范围宽带网络动态处置系统）项目获国防科学技术二等奖。云晓春排名第一，**方滨兴**排名第二。哈尔滨工业大学计算机网络与信息内容安全重点实验室李斌、清华大学计算机系网络技术研究所、清华大学网格计算研究部杨广文有参与。
●2003-2007年，**方滨兴**任信息产业部互联网应急处理协调办公室主任。
●2003年1月31日，经费4.9亿的国家信息安全重大项目“**国家信息安全管理系统**”（005工程）获2002年度国家科技进步一等奖，**方滨兴**排名

时间表

第一，胡铭曾排名第二，清华大学排名第三，哈尔滨工业大学排名第四，云晓春排名第四，北京大学排名第五，郑纬民排名第七，中国科学院计算技术研究所有参与。

●2003年2月，在北京的国家计算机网络与信息安全管理中心综合楼工程竣工。

●2003年7月，国家计算机网络应急处理协调中心更名为国家计算机网络应急技术处理协调中心。

●2003年9月2日，全国“**金盾工程**”会议在北京召开，“金盾工程”全面启动。

●2004年，国家信息安全重大项目“大规模网络特定信息获取系统”，经费7000万，获国家科技进步二等奖。

●2005年，**方滨兴**任国防科学技术大学兼职教授、特聘教授、博士生导师。

●2005年，**方滨兴**被遴选为中国工程院院士。

●2005年，“该系统”已经在北京、上海、广州、长沙建立了互相镜像的4套主系统，之间用万兆网互联。每套系统由8CPU的多节点集群构成，操作系统是红旗Linux，数据库用的是OracleRAC。2005年国家计算机网络与信息安全管理中心（北京）就已经建立了一套384*16节点的集群用于网络内容过滤（005工程）和短信过滤（016工程）。该系统在广州、上海都有镜像，互相以十万兆网链接，可以协同工作，也可以独立接管工作。

●2006年11月16日，“**金盾工程**”一期在北京正式通过国家验收，其为“为中华人民共和国公安部设计，处理中国公安管理的业务，涉外饭店管理，出入境管理，治安管理等的工程”。

●2007年4月6日，国家计算机网络与信息安全管理中心上海分中心机房楼奠基，位于康桥镇杨高南路5788号，投资9047万元，“……是国家发改委批准实施的国家级重大项目，目前全国只有北京和上海建立了分中心，它是全国互联网信息海关，对保障国家信息安全担负着重要作用。”

●2007年7月17日，大量使用中国国内邮件服务商的用户与国外通信出现了**退信**、**丢信**等普遍现象。

●2007年12月，**方滨兴**任北京邮电大学校长。

●2008年1月18日，信息产业部决定免去方滨兴的国家计算机网络与信息安全管理中心名誉主任、信息产业部互联网应急处理协调办公室主任职务，“另有职用”。

●2008年2月29日，**方滨兴**当选第十一届全国人民代表大会安徽省代表。

●2009年8月10日，**方滨兴**在“第一届中国互联网治理与法律论坛”上大力**鼓吹网络实名制**。

从小推特告诉我，翻墙不忘方滨兴>>

机构关系

国家计算机网络与信息安全管理中心（安管中心）是原信产部现工信部的直属部门。

安管中心与国家信息化工作领导小组计算机网络与信息安全管理工作办公室与国家计算机网络应急技术处理协调中心（CNCERT/CC，互联网应急中心）是一个机构几块牌子的关系。比如方滨兴简历中“1999-2000年在国家计算机网络应急技术处理协调中心任副总工”与“计算机网络应急处理协调中心”的成立时间两种说法就有着微妙的矛盾。实际上几个机构的人员基本一致。

安管中心下属互联网交换中心与国家互联网络交换中心是不同的机构。

各安管中心省级分中心一般挂靠当地的通信管理局。

安管中心的主要科研力量来自“哈尔滨工业大学”方滨兴当博导有一批学生的哈工大以及关系良好的中科院计算所，这两个机构是那三个国家信息安全重大项目的主要参与者，之后还在不断吸引人才并为安管中心输送人才和技术。在方滨兴空降北邮之后，往安管中心输血的成分中哈工大的逐渐减少，北邮的逐渐增多。

CNCERT/CC的国内“合作伙伴”有中国互联网协会主办北京光芒在线网络科技有限公司承办的中国互联网用户反垃圾邮件中心，是个没有实权的空壳；国家反计算机入侵及防病毒研究中心、国家计算机病毒应急处理中心，是公安部、科技部麾下；违法和不良信息举报中心是国新办势力范围；国家计算机网络入侵防范中心是中科院研究生院的机构，同样直接支撑CNCERT/CC。 CNCERT/CC的应急支撑单位中民营企业最初领跑者是绿盟，后来绿盟因其台谍案被罢黜，启明星辰取而代之。而安管中心具有一些资质认证、准入审批的行政权力，这可能是民间安全企业趋之若鹜的原因。不过，民营企业并未参与到国家信息安全的核心项目建设中，安管中心许多外围项目交给民企外企做，比如像隔离器之类的访问限制设备外包给启明星辰以作为辅助、备用，或者在与他们在网络安全监测上有所交流。

GFW与金盾没有关系

敏锐的读者从时间表应该已经看出这样的感觉了。实际上，GFW与金盾就是没有关系，两者泾渭分明，有很多区别。

GFW主要是宣传系统的工具，而金盾主要是公安系统的工具。GFW的总支持者是负责宣传工作的李长春，最初的主要需求来自各610办公室；而金盾的总支持者是公安系统的高层人士，主要需求来自公安

GFW与金盾没有关系

部门。GFW主外，作网络海关用；而金盾主内，作侦查取证用。GFW建设时间短，花费少，成效好；而金盾建设时间长，花费巨大（GFW的十倍以上），成效不显著。GFW依附于三个国家级互联网交换中心（不存在省级GFW）分光到自己的交换中心搞入侵防御，再扩散到一些放在ISP那里的路由封IP，位置集中，设备数量少；而金盾则是进驻各大交换中心数据中心，无处不在，数量巨大。GFW的科研实力雄厚，国内研究信息安全的顶尖人才和实验室有不少在为其服务，比如哈工大的信息安全重点实验室、中科院计算所、北邮；而金盾的科研实力较弱，公安系统的公安部第三研究所信息网络安全研发中心、国家反计算机入侵与防病毒研究中心都缺乏科研力量和科研成果，2008年8月成立信息网络安全公安部重点实验室想与哈工大的重点实验室抗衡，还特意邀请方滨兴来实验室学术委员会，不过这个实验室光是电子数据取证的研究方向就没什么前景，而且也没什么研究成果。GFW之父方滨兴没有参与金盾工程，而工程院里在支持金盾工程的是沈昌祥；实际上那个公安部重点实验室的学术委员会名单很是有趣，沈昌祥自然排第一，方滨兴因为最近声名太显赫也不好意思不邀请他，方滨兴可能也有屈尊与公安系统打好关系的用意。

GFW发展和状况

GFW主要使用的硬件来自曙光和华为，没有思科、Juniper，软件大部为自主开发。原因很简单，对国家信息安全基础设施建设，方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中也一直强调“信息安全应该以自主知识产权为主”。而且GFW没有闲钱去养洋老爷，肥水不流外人田。李国杰是工程院信息工程部主任、曙光公司董事长、中科院计算所所长，GFW的大量服务器设备订单都给了曙光。方滨兴还将安管中心所需的大型机大订单给李国杰、国防科大卢锡城、总参56所陈左宁三位院士所在单位各一份。所以GFW为什么那么多曙光的设备，GFW为什么那么多中科院计算所的科研力量，为什么方滨兴成为中科院计算所和国防科大都有显赫的兼职，为什么方滨兴从老家哈尔滨出来打拼短短7年时间就入选工程院卢浮宫？就是因为方滨兴头脑灵活，做事皆大欢喜。

网上有人讽刺GFW夜郎自大，事实上这是盲目乐观，无知者无畏。GFW的技术是世界顶尖的，GFW集中了哈工大、中科院、北邮货真价实的顶尖人才，科研力量也是实打实地雄厚，什么动态轮什么Feed Over Email算什么葱。所有的翻墙方法，只要有人想得到，GFW都有研究并且有反制措施的实验室方案储备。GFW主要是入侵防御系统，检测-攻击两相模型。所有传输层明文的翻墙方案，检测然后立即进行攻击是

GFW发展和状况

向最终用户肯定是透明的，谁也不能阻止GFW也作为最终用户来静态分析其网络层可检测特征。入侵检测然后TCP会话重置攻击算是干净利落的手段了，最不济也能通过人工的方式来查出翻墙方法的网络层特征（仅仅目标IP地址就已经足够）然后进行定点清除。如果是一两个国家的敌人，GFW也能找到集群来算密钥。GFW是难得能有中央财政喂奶的科研项目。那些在哈工大地下室、中科院破楼里的穷研究生即使没有钱也能搞出东西来，现在中央财政喂奶，更是干劲十足了。GFW什么都行，就是P2P没办法，因为匿名性太好了，既不能实时检测出来，也无法通过静态分析找到固定的、或者变化而可跟踪的网络层特征。就这样也能建两个陷阱节点搞点小破坏，而且中科院的242项目“P2P协议分析与测量”一直都没停。什么时候国外开学术会议还是Defcon谁谁发一篇讲Tor安全性的paper，立即拿回来研究一番实现一下，已然紧跟学术技术最前沿了。不过实际上，即使GFW这样一个中国最顶尖的技术项目也摆脱不了山寨的本性，就是做一个东西出来很容易，但是要把东西做细致就不行了。

不过可能有人就疑问，为什么GFW什么都能封但又不真的封呢？我的这个翻墙方法一直还是好好的嘛。其实GFW有它自己的运作方式。GFW从性质上讲是纯粹的科研技术部门，对政治势力来说是一个完全没有主观能动性的工具。GFW内部有很严格权限管理，技术与政治封装隔离得非常彻底。封什么还是解封什么，都是完全由上峰决定，党指挥枪，授权专门人员操作关键词列表，与技术实现者隔离得很彻底，互相都不知道在做什么。所以很多时候一些莫名其妙的封禁比如封freebsd.org封freepascal.org（可能都联想到freetibet.org），或者把跟轮子的GPass八杆子打不着的“package.debian.org/zh-cn/lenny/gpass”列为关键词，都是那些摆弄着IE6的官僚们的颐指气使，技术人员要是知道了都得气死。方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中讲一个立足国情的原则，说：“主要是强调综合平衡安全成本与风险，如果风险不大就没有必要花太大的安全成本来做。在这里面需要强调一点就是确保重点的，如等级保护就是根据信息系统的重要性来定级，从而施加适当强度的保护。”所以对于小众的翻墙方式，GFW按照它的职能发现了也就只能过一下目心里有个底，上峰根本都不知道有这么一种方式所以也根本不会去封、GFW自己也没权限封，或者知道了也懒得再花钱花精力去布置。枪打出头鸟，什么时候都是这样。

方滨兴一个人把GFW崛起过程中的政治势能全部转化为他的动能之后就把GFW扔掉了。现在GFW是平稳期，完全是清水衙门，既没有什么后台，也无法再有什么政治、资金上的利益可以攫取，也无法再搞什么新的大型项目，连IPv6对GFW来说都成了一件麻烦事情。方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中也感慨道：“比如说Web 2.0概念出现后，甚至包括病毒等等这些问题就比较容易扩散，再比如说IPv6出来之后，入侵检测就没有意义了，因为协议都看不懂还

GFW发展和状况

检测什么……”GFW一直就没有地位，一直就是一个没人管的萝莉，国新办、网监、广电、版权、通管局之类的怪蜀黍都压在上面要做这做那。所以方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中也首先强调一个机制，“需要宏观层面，包括主管部门予以支持。”所以，想解封网站，不要去找GFW本体，那没用，要去找GFW的上峰，随便哪个都行。而ISP就根本跟GFW没关系了，都不知道GFW具体搞些什么，起诉ISP完全属于没找到脉门。

不过GFW现在还是运行得很好，工作能力还有很大潜力可挖，唯一害怕的就是DDoS死撞墙。GFW的规模在前面的时间表里也有数字可以估计，而且GFW现在的网站封禁列表也有几十万条之多。网络监控和短信监控也都尽善尽美。不过GFW也没有像机器学习之类的自组织反馈机制来自动生成关键词，因为它本身没有修改关键词的权限，所以这种技术也没必要，况且国内这种技术也是概念吹得多论文发得多实践不成熟。现在GFW和金盾最想要的就是能够从万草从中揪出一小撮毒草的数据挖掘之类的人工智能技术。方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中提到“舆情驾驭核心能力”，“首先要能够发现和获取，然后要有分析和引导的能力”。怎么发现？就靠中科院在研的973课题“文本识别及信息过滤”和863重点项目“大规模网络安全事件监控”这种项目。金盾工程花大钱搞出来，好评反而不如GFW，十一局的干警们脸上无光无法跟老一辈交代啊。公安系统的技术力量跟GFW没法比，不过公安系统有的是钱，先游山玩水吃喝一通，然后把剩下的税金像冲厕所一样随便买个几十万个摄像头几万台刀片几十PB硬盘接到省市级网络中心，把什么东西都记录下来。问题是记下来不能用，只能靠公安干警一页一页地翻Excel。所以说，虽然看起来GFW千疮百孔，金盾深不可测，只是因为公安部门比起GFW来比较有攻击性，看到毒草不是给你一个RST而是给你一张拘留证。反而是GFW大多数时候都把毒草给挡住了，而大多数毒草金盾都是没发现的。

国家信息安全话语范式

在轮子闹事被取缔之后，轮子组织仍然在从四面八方进行各种手段的宣传，而且逐渐依靠上了各种境外背景。境内的宣传活动很快就被公安和国安清理掉了，然而从境外网上而来的大量网络宣传让从未有过网络化经验的中央无所适从、毫无办法、十分着急。这些东西对中央来说都是难以忍受的安全威胁，为这些威胁又发生在网上，自然国家网络安全就被提上了首要议程。适逢信息化大潮，电子政务概念兴起，中央下决心好好应对信息化的问题，于是就成立了国家信息化工作领导小组。我们可以看到，首批组成名单中，安全部门和宣传部门占了大多数席位，

国家信息安全话语范式

而且其第一下属机构就是处理安全问题，第二下属才是处理信息化改革，安全需求之强烈，可见一斑。

正是这个时候，一贯对信息安全充满独到见解的方滨兴被信产部的张春江调入了安管中心练级。方滨兴对信息安全的见解与高层对网络安全的需求不谋而合。一个方滨兴见解的集大成概括，方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中说：“一定要有一个信息安全法，有了这个核心法你才能做一系列的工作。”国家信息安全体系的首要核心就是以信息安全为纲的法律保障体系，通过国家意志——法律来定义何谓“信息安全”。信息安全本来是纯技术、完全中性的词语，通过国家意志的定义，将“煽动…煽动…煽动…煽动…捏造…宣扬…侮辱…损害…其他…”定义为所谓的网络攻击、网络垃圾、网络有害信息、网络安全威胁，却在实现层面完全技术性、中立性地看待安全，丝毫不考虑现实政治问题。这样既在技术上实现完备的封装，也给了用户高可扩展性的安全事件定义界面。对国家安全与技术安全实现充满隐喻的捆绑，对意识形态与信息科学进行牢不可破的焊接，这就是方滨兴带给高层的开拓性思维，这就是方滨兴提出的国家信息安全话语范式。

这个话语范式是如此自然、封装得如此彻底，以至于几乎所有人都没有意识到中国的网络化发展出现了怎样严重的问题。几乎所有网民都没有意识到，给他们带来巨大麻烦和沮丧的GFW竟然是本来应该为网民打黑除恶的国家互联网应急响应中心；几乎所有网民都没有意识到，自己在网上某处的一亩三分地修剪花草对于国家来说竟然是网络安全攻击事件；几乎所有决策者都没有意识到，那个看似立竿见影的防火墙实际上具有怎样强大的副作用、会给互联网发展带来怎样大的伤害；几乎所有决策者都没有意识到，使用GFW这样专业的安全工具来进行网络封锁意味着什么。意识形态面对网络化这样变幻莫测的景色无法忍受，就只能用眼罩封闭住眼睛。在讨论网络化的中文理论文本中，摆到首要位置占据最多篇幅的便是网络安全和网络威胁。国家信息化工作领导小组第一下属机构便是处理安全问题。这样，在网络本身都没有发展起来的时候，就在理论上对网络进行种种限制和控制；在网络仍然自发地成长起来以后，便在文化上对网络进行系统性妖魔化，在地理上对网络中国进行闭关锁国。更严重的是，在根本不了解技术本质和副作用的情况下使用国家信息安全工具，就像一个不懂事的小孩把玩枪械。在维护安全的话语之下，决策者根本不知道使用GFW进行网络封锁就是在自己的网络国土上使用军队进行镇压，切断网线就是在自己的网络国土上种蘑菇。

更悲哀的是，GFW的建设者们大多都没有意识到他们在做的究竟是什么事情，在签订保密协议之后就无意识中投身党国事业滚滚长江东逝水。像云晓春这种跟着方滨兴出来打江山的，方滨兴倒是高飞了，云晓春们就只能鞠躬尽瘁干死技术，在安管中心反而被王秀军、黄澄清之辈后来居上。而当初在哈工大跟着方滨兴的穷研究生们，最后也陆陆续续去了百度之类的公司。GFW面临与曼哈顿工程一样的伦理困局。科学本

是中立的，但科学家却被政治摆弄。技术工作者们只关心也只被允许关心如何实现安全，并不能关心安全的定义到底如何。他们缺乏学术伦理精神，不能实践“对自己工作的一切可能后果进行检验和评估；一旦发现弊端或危险，应改变甚至中断自己的工作；如果不能独自做出抉择，应暂缓或中止相关研究，及时向社会报警”的准则。结果就算他们辛辛苦苦做研究却也不能造福民生，反而被扣上“扼杀中国人权”“纳粹帮凶”的帽子，不可谓不是历史的悲哀。

这种话语范式浸透了社会的方方面面。在这种话语之下，中国有了世界上最强大的防火墙，但中国的网络建设却远远落后于世界先进水平；中国有了世界上最庞大的网瘾治疗产业链，但中国的网络产业却只会山寨技；中国有了世界上最多的网民，但在互联网上却听不见中国的声音。GFW已经实现了人们的自我审查，让人们即使重获自由也无法飞翔，完成了其根本目的。现在即使对GFW的DDoS的技术已经成熟，推倒墙却也变得没有意义，只能让公安系统的金盾得势，更多的网民被捕，最终新墙竖起。这一切都出自意识形态化现代性与网络化后现代性之间巨大断裂，以及“国家信息安全话语”这种致命的讳疾忌医。

结语

一部GFW简史同时也是中国网络化简史。网络化既是技术变革，也是文化变革。网络文化这种“有害成份”无法分而治之，因为网络化的技术变革与文化变革是一体的；后现代的网络文化也无法与现代的意识形态文化进行同化，因为两者分属不同的范式。网络的确是意识形态完全的敌人，因为网络多元化文化要求取消意识形态的中心地位；但意识形态不是网络的敌人，事实上网络没有敌人，因为网络只有解构对象。因此对于执政者来说，意识形态的中心地位与网络化发展趋势两者只能选择其一。实际情况是，执政者选择了前者，而把大刀挥向了Web 2.0。于是网络用它一贯调侃的风格模仿意识形态话语进行了如下讽刺：“我们对你陈旧的政权概念和意识形态烂腌菜毫不感兴趣。你无法理解在人类网络化的历史潮流之前宏大叙事为何而消解，你也无法理解国家和民族概念为何将分崩离析，你无法改变你对互联网的无知。你的政权无法成为我们真正的敌人。”其实，《2009匿名网民宣言》只是过早的预言，赛博朋克式的谜语。

然而，无论中国的互联网受到了怎样的限制和压迫，即便中国网民的眼界已经被成功禁锢，中国的网络还是以它自己的方式适应种种压力顽强地发展。无论有多么强大的GFW或者金盾，即使被关在果壳之中，网络仍然在以意识形态完全不能理解的方式走向后现代蓝海，自成为无限空间之王。

他们，用智慧筑起新的长城

参与GFW研发的单位不完全名单

上海交通大学信息安全学院
南京邮电大学计算机学院信息安全系
哈尔滨工业大学
北京邮电大学
中科院数学所
赛门铁克公司
ServGate
哈尔滨工业大学软件工程有限公司
北京瑞星科技股份有限公司
清华紫光比威网络技术有限公司
Wensense有限公司
安氏互联网安全系统中国有限公司
东软软件股份有限公司
北京港湾网络有限公司
华为技术有限公司
juniper瞻博网络公司
NORTEL北方电讯
思科系统中国网络技术有限公司
总参第五十六研究所
国防科大
哈工大信息安全试验室
中科院计算所
中科院软件所信息安全试验室
国家计算机网络与信息安全管理中心
信息产业部网络安全中心
浙大网新科技股份有限公司
北京天融信公司
阿姆瑞特亚洲网络有限公司
联想网御科技北京有限公司
北京电信通绿信科技有限公司
北京喜安科高科技有限公司
珠海捷朗菱网络科技有限公司
广州星外信息科技有限公司
清华同方知网技术有限公司
北京中教高科信息技术有限公司
卓尔伟业信息技术有限公司
北京网康科技有限公司
中科新业信息科技发展有限公司
汉邦软科集团
上海汉景信息科技有限公司
厦门诚创科技有限公司
厦门泛德科技开发有限公司
珠海同易信息技术有限公司
深圳赛佛莱特科技有限公司
海天软件控股有限公司
厦门翼讯科技有限公司
泉州市南狐软件有限公司
CheckPoint软件技术有限公司
北京冠群金辰软件有限公司
易思同创信息技术北京有限公司
上海鹏越惊虹信息技术发展有限公司
上海百络信息技术有限公司
北京麦纳科技发展有限公司
北京大正语言知识处理科技有限公司
亿阳信通股份有限公司
北京启明星辰信息技术有限公司
东软集团有限公司
北京海信数码科技有限公司
南山之桥微电子有限公司
....

还有很多不一一列举了

multiple1902整理自1984bbs

他们，用智慧筑起新的长城

七一劳动模范

大家好，我是**方滨兴**，国家计算机网络与信息安全管理中心主任。

我是**刘欣然**，北京邮电大学计算机科学与技术学院兼职硕士研究生导师。

我是**齐向东**，雅虎中国副总裁兼3721公司总经理（2005年9月任北京三际无限网络科技有限公司总裁）。

我是**李伍峰**，国务院新闻办网络局局长。

我是**石晓虹**，雅虎中国CTO（2005年9月任北京三际无限网络科技有限公司董事长助理）。

我是**刘正荣**，国务院新闻办公室网络局副局长、中国互联网新闻研究中心主任。

刘欣然

Bio: 1971年2月生，北京邮电大学计算机科学与技术学院兼职硕士研究生导师，高级工程师。刘欣然于1998年6月在哈尔滨工业大学获计算机系统结构专业工学博士学位，毕业论文为“基于Web的计算资源发布研究”。研究方向：网络入侵行为分析与防范、互联网安全事件应急处理、系统安全性评估、互联网攻防对抗等。

2002年4月—2005年3月，刘欣然在海淀园博士后科研工作站北京启明星辰信息技术有限公司分站做博士后。他的研究成果为保障国家网络与信息安全发挥了重要的支撑作用，获得了国家科技进步二等奖和国防科学技术二等奖各一项。

刘欣然先后从事过分布式并行计算、计算机网络、网络与信息安全方面的科研工作，作为主要负责人和参与人参加过国家青年自然科学基金、国家自然科学基金、863、航天部、国防科工委等7个科研项目，目前在研项目为863信息安全组课题“大规模网络应急响应体系及原型系统的研究”。先后在国内外期刊、会议发表论文十余篇。

我们的作品：
搜索引擎安全管理系统

完成人：刘欣然；方滨兴；齐向东；李伍峰；石晓虹；刘正荣；杨臻；丁丽；张鸿；陈斌

单位： 国家计算机网络与信息安全管理中心；北京三际无限网络科技有限公司；国务院新闻办公室互联网新闻研究中心

日期：2005年2月2日

简介：该系统提供了第三方的基于HTTP标准的规范高性能过滤接口，在输入和输出两个环节分三级进行有效的信息过滤；提供了统一管理平台，可以远程进行管理，经单点配置过滤策略即可实现全局同时生效，且策略下发过程可保证对过滤目标的保密要求系统可以采用分布式或集中式的部署结构。系统接入简单，易于部署，适用于绝大多数现有的搜索引擎，可以满足现有国内日查询量的处理要求。**该系统已实际部署一些国内较大的搜索引擎，取得了良好的使用效果。全面推广和部署该系统，将为净化国内互联网空间提供有力保障。**

从小推特告诉我翻墙不忘方滨兴

图为方滨兴院士

从小推特告诉我 翻墙不忘方滨兴

——你是互联网，我是防火墙

方滨兴，男，汉族，1960年生于哈尔滨市，籍贯江西省万年人，中共党员，第十一届全国人大代表。中国工程院院士，北京邮电大学校长，国家信息化专家咨询委员会网络与信息安全专委会副主任，国家应急管理专家组成员，国家计算机网络与信息安全管理中心科技委主任，国家973计划信息安全理论及若干关键技术首席科学家，中国互联网协会副理事长兼网络与信息安全工作委员会主任，中国计算机学会副理事长兼计算机安全专业委员会主任，信息网络与信息安全专家。北京市信息化咨询专业委员会委员,中国国家防火墙（GFW）之父。

出处

方滨兴谈如何加强网络舆情驾驭能力

从小推特告诉我 翻墙不忘方滨兴

我的奋斗

1978-1981年哈尔滨工业大学计算机系77级本科生，获学士学位
1982-1984年在清华大学计算机系81级研究生，获硕士学位
1986-1989年在哈尔滨工业大学计算机系85级在职博士研究生，获博士学位
1990-1993年在国防科学技术大学计算机科学与技术博士后流动站在职研究学习
2003年，在中央党校地厅级干部进修班第41期脱产学习半年
1984-1992年在哈尔滨工业大学计算机系
任助教、讲师、副教授；其间任教研室副主任
1992-1995年在哈尔滨工业大学计算机系任教授；其间任教研室副主任、主任
1995-1999年在哈尔滨工业大学计算机与电气工程学院任教授，
博士生导师；其间任教研室主任，副院长，网络中心主任
1999-2000年在国家计算机网络应急技术处理协调中心任副总工
2000-2002年在国家计算机网络应急技术处理协调中心
任总工程师、副主任、教授级高级工程师
2002-2006年在国家计算机网络应急技术处理协调中心
任主任、总工程师、教授级高级工程师
2003-2007年任信息产业部互联网应急处理协调办公室主任
2005年起被遴选为中国工程院院士
2006年起被信息产业部任命为国家计算机网络与信息安全管理中心名誉主任
2007年12月起任北京邮电大学校长，教授

从小推特告诉我 翻墙不忘方滨兴

学术兼职：

2001年起：哈尔滨工业大学兼职教授，博士生导师
2001年起：中国通信学会常务理事，
会士，通信安全技术委员会主任
2002年起：中科院计算所客座研究员，
博士生导师，信息安全首席科学家
2002年起：中国计算机学会理事，计算机安全专业委员会副主任
2002年起：中国互联网协会常务理事
兼副秘书长、副理事长，网络与信息安全工作委员会主任
2002年起：中国通信标准化协会理事会理事，
网络与信息安全技术委员会（TC8）主席
2004-2006年：计算机科学与技术学报（英文版）信息安全领域编辑
2005年起：国防科学技术大学兼职教授、特聘教授，博士生导师
2005年起：清华大学计算机系兼职教授
2007年起：《通信学报》编辑委员会主任

工作兼职：

2001年起：国家863计划“十五”信息技术领域信息安全主题组
管理专家、信息技术领域专家，“十一五”信息技术领域专家委员会委员
2002年起：国家自然科学基金信息安全重大专项专家组成员，
可信软件重大专项专家组副组长
2003-2005年：国家“十一五”信息安全产业发展规划工作组组长
2003年起：财政部“金财工程”专家咨询委员会委员
2004年起：中国下一代互联网示范工程（CNGI）项目专家委员会委员
2005年起：全国人大信息化系统改造和建设工程专家咨询顾问组成员
2007年起：国家973计划“信息安全理论及若干关键技术”首席科学家

社会兼职：

2002年起：国家信息化专家咨询委员会
第一、二、三届委员，网络与信息安全专业委员会副主任
2002年起：信息产业部通信科学技术委员会常务委员
2003-2005年：国家税务总局信息技术咨询委员会委员
2004年起：国家计算机网络与信息安全管理中心科学技术委员会主任
2004年起：解放军总后勤部信息化专家咨询委员会委员
2005年起：国家信息安全产品认证管理委员会委员
2005年起：中国网络通信集团公司技术委员会委员
2006年起：上海市互联网宣传管理技术咨询专家
2006年起：北京市信息化专家咨询委员会委员
2006年起：国家应急管理专家组成员
2007年起：公安部信息安全特聘专家
2007年起：“新世纪百千万人才工程国家级人选”
评审委员会委员

从小推特告诉我 翻墙不忘方滨兴

科研成果：

1995年“支持存储器无冲突访问的互连开关门阵列芯片的研制”
获部级科学进步二等奖
1995年“多机系统的性能评价的研究”
获部级科学进步二等奖
1996年“支持存储器无冲突访问的互连开关设计理论及方法”
获部级科学进步三等奖
1996年“ABC-90阵列计算机综合模拟器”
获部级科学进步三等奖
2001年“计算机病毒及其预防技术”
获国防科学技术三等奖，排名第一
2002年“信息安全管理系统”
获国家科学技术进步一等奖，排名第一
2002年“大范围宽带网络动态阻断系统”
获国防科学技术二等奖，排名第二
2004年“大规模网络信息获取系统”
获国家科学技术进步二等奖，排名第一
2004年“国家信息安全战略研究”
获国家发展改革委机关优秀成果三等奖
2005年“搜索引擎安全管理系统”
获中国通信学会科学技术二等奖，排名第二
2007年“通信数据安全管理系统”
获国家科学技术进步二等奖，排名第一

奖励与荣誉：

2001年获国务院政府特殊津贴
2001年获中组部、中宣部、中央政法委、公安部、
民政部、人事部等联合授予“先进个人”称号
2001年获信息产业部“在信息产业部重点工程中做出
突出贡献特等奖先进个人”称号
2002年获中组部中宣部、人事部、科技部
联合授予全国“杰出专业技术人才”荣誉称号
2004年获人事部、科学技术部、教育部、
财政部、国家发展和改革委员会、国家自然科学基金委员会、
中国科学技术协会联合授予“新世纪百千万人才工程国家级人选”
2006年获信息产业部“信息产业科技创新先进工作者”
2007年获何梁何利基金科学与技术进步奖

“金盾工程”时间表

编者注：本文是一篇虚拟作品，没有任何真实依据。

文 / 阮一峰

2009年

中国政府宣布境内销售的所有计算机，必须预装绿色上网过滤软件，以便过滤互联网上的不良文字和图像。

2010年

中国政府宣布网站备案制度与“绿色上网”相结合。境内所有没有备案的网站，都会被软件过滤，无法浏览。

2011年

中国政府宣布“网站备案制度”扩展到境外网站。凡是在中国境内可以访问到的境外网站，视同在华开展业务的外国机构进行管理，适用相关的外国机构管理法规。境外网站如果想在华开展业务，必须向中国政府进行备案，得到批准后才能开展业务。

2012年

中国政府宣布启动域名备案，境内所有域名都必须向政府备案。

2013年

中国政府宣布启用域名白名单制度，即只有在“白名单”中的域名，才提供解析服务。境内和境外网站在华一旦备案成功，其域名将自动加入“白名单”。

2014年

中国政府宣布对所有互联网上使用的加密证书进行备案。不管是公钥还是私钥，都必须在政府报备。如果加密通信中，使用了没有报备的密钥，电信公司的网关将自动拦截，阻止其通过。

2015年

中国政府宣布实行电子邮件实名制。凡是需要开通电子邮件的公民和企业，一律凭相应证件到政府指定的电子邮件服务商处申请。如果一封电子邮件的发信域，不在有合格资质的电子邮件服务提供商的列表之中，该封邮件将被自动退回。

2016年

中国政府宣布实行IP地址实名制。那个时候，IPv6已经得到广泛应用，IP地址不再是稀缺资源。根据中国政府的设想，每个公民一出生，就可以分配到一个IP地址，终生保持不变。然后，每个人上网，都必须使用自己的法定地址，不得擅自使用他人的地址。

2017年

中国政府向全世界宣告，“金盾工程”初步完成，中国已经建成了世界上最安全的互联网。（完）

實戰分析篇

本篇中，对当下比较流行的利用动态网系列软件、无界浏览、Gtunnel、Puff、Tor、GAppProxy、SSH等翻墙方法从具体操作到技术原理做了或深或浅的介绍，也对在手机上网时翻墙的方法做了一定的说明。

动态网系列软件、无界浏览、GTunnel和Puff都是轻量级的翻墙工具，使用非常方便，速度也很令人满意。其中前三者都是由法轮功学员义务开发，安全性非常好。Puff的开发者身份难以确定。

洋葱路由软件TOR虽然配置略微复杂，速度较慢，但技术成熟，安全性比较高，在使用网桥的情况下稳定性也不错，跨平台表现优异。希望大家都能抽点时间掌握TOR的使用。

SSH和VPN属于比较高级的翻墙技术，技术原理较为简单，但安全性很高，而速度依赖于选择的服务器。通常SSH和VPN账号需要付费购买，虽然网上偶尔能找到免费的账号，但购买商业账号将能得到更好的服务。

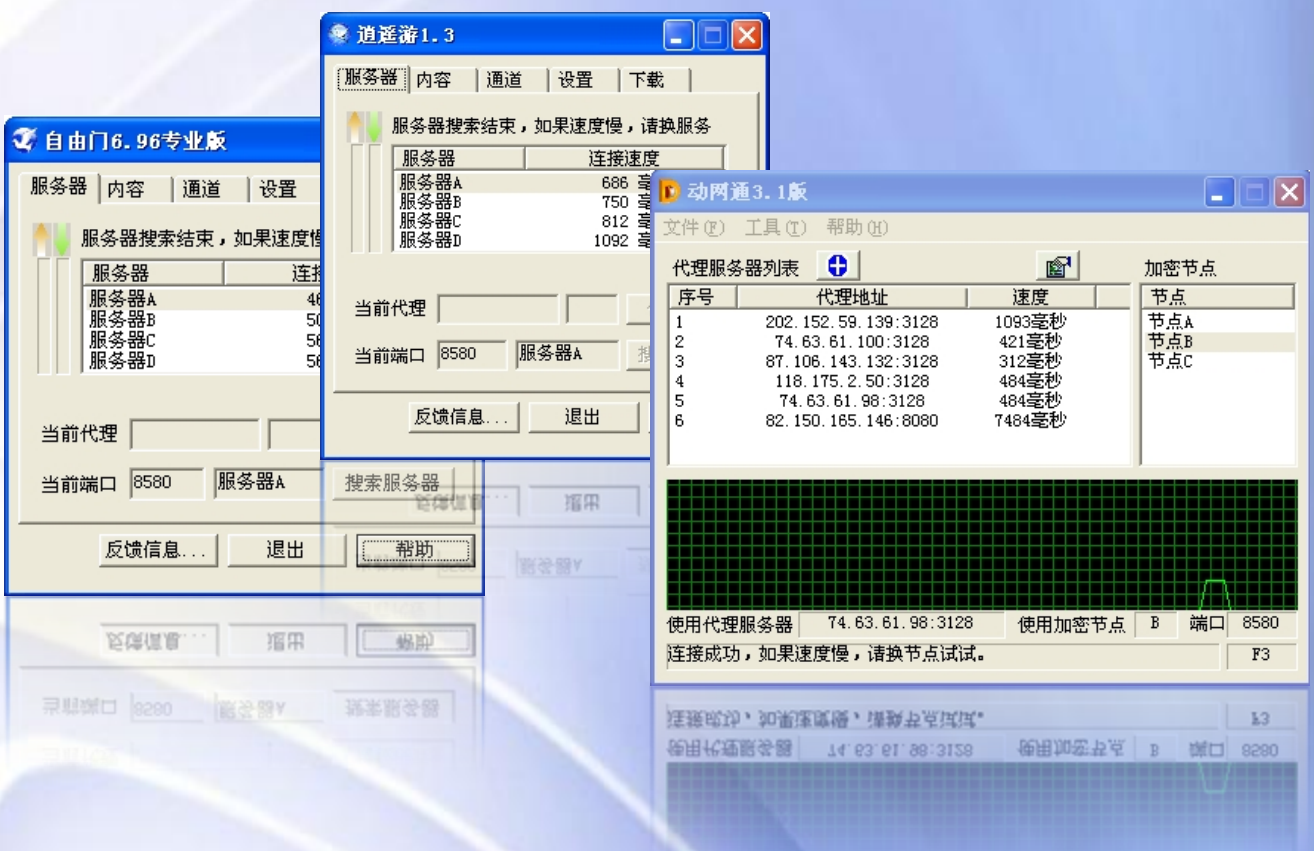
您可以在http://www.chinavpns.com/找到VPN翻墙的技术教程，同时可以购买到VPN账号。与卖家交谈时报出“墙倒众人推”的暗号，首次购买可以享受8折优惠。

使用动态网系列软件翻墙教程

文 / Allen

优缺点总结

优点:
获取方便，操作简单，速度快，可以看YouTube视频



简介

动态网致力于突破网络封锁。自由门(FreeGate)，逍遥游(FreeU)，动网通(DynaPass)均为动态网产品，这些软件通过连接在海外的加密代理服务器，来达到突破网络封锁的目的。

如何获得自由门（逍遥游，动网通）

由于动态网在中国大陆是被封锁的，无法直接访问，因此我们可以通过以下方式获取最新的自由门（逍遥游，动网通）。使用其他代理服务器进入动态网下载。

●电子邮件索取。使用国外信箱如gmail，hotmail等，发送一封空邮件给动态网，大约10分钟就可收到回信，每个邮箱一天只能索取一次。索取自由门fg@dongtaiwang.com，索取逍遥游freeU@dongtaiwang.com

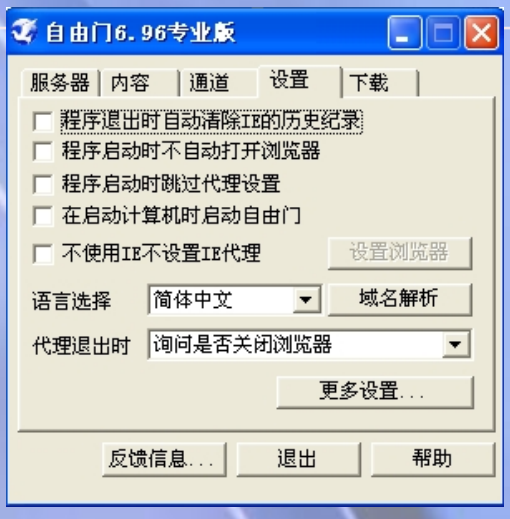
●Gtalk索取。给dtwip001@gmail.com, dtwip002@gmail.com, dtwip003@gmail.com, dtwip004@gmail.com, 或dtwip005@gmail.com随便打几个字，对方会自动回复几个IP。通过这些IP可以进入动态网。

●Skype索取。加“dongtaiwang.com”为好友，对方会自动回复最新的IP，通过这些IP可以进入动态网。

●emule下载。电驴/电骡/迅雷等都支持ed2k协议。统一提供的文件命名格式，比如 GIFC_20091210_Dweb_690p.zip。GIFC为全球互联网自由联盟的缩写，日期为该zip文件的发布日期，dweb为软件类型，690P为该软件版本号。用Emule软件搜索 GIFC 2010等关键字搜索后就可以找到。

使用方法

自由门、逍遥游和动网通使用方法类似，但采用的通道不同。自由门采用F3和F4通道，而逍遥游采用U通道。U/F4通道是针对现行封锁而开发的新技术，通常能解决当前的封锁问题。F3 通道是基于SSL，提供2次代理功能(当局域网规定必须透过特定的代理才能上网时)。由于去年十一封网空前，自由门一度失效，动态网在原来自由门的基础上，又开发了逍遥游与动网通。一般来说，为防止封网，这三个软件都应该准备好，以便在封锁严重的时候交替使用。



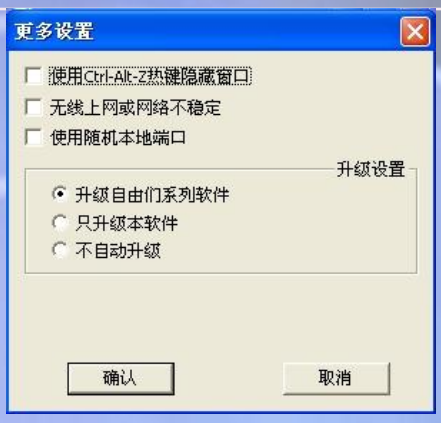
Windows平台

A 自由门

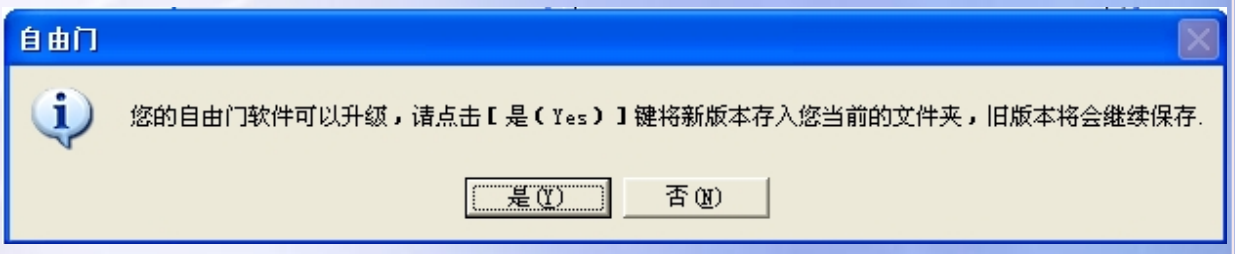
自由门的使用是最简单的，双击自由门图标即可运行。找到服务器后，IE浏览器会自动弹出动态网网页。如果您不想弹出网页，可以进入设置选项卡勾选"程序启动时不自动打开浏览器"。不使用IE浏览器的，可以勾选"不使用IE不设置IE代理"。

点击“域名解析”可以解析域名，查询网站真正的IP。

点击“更多设置”，会打开如右图的窗口，您可以根据具体情况进行选择。值得一提的是"使用随机本地端口"是一个有用的功能，例如在局域网中使用自由门，局域网将8580端口封锁等等。

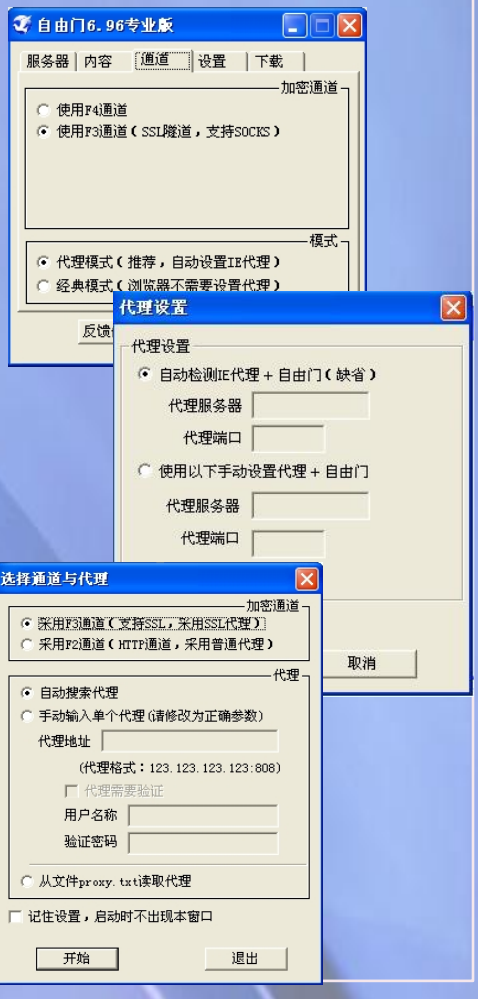


当发现有新版的自由门（逍遥游、动网通）时，会有提醒，您可以设置取消该提醒。当然，最好多准备两个软件，以防万一。



如果您在局域网，必须通过特定的代理才能上网，或者您希望使用二次代理，请使用F3通道。

更换通道需要重新启动自由门。重启后就可以设置代理，如右图。您可以配合MultiProxy等软件使用自由门。当封锁严重时，寻找海外代理并且给自由门进行代理设置是不错的选择，能大大提高连接成功率。



经典模式：IE不会设置代理，只能从动态网页面连接打开新页面。代理模式：代理模式会给IE设置代理。一般使用代理模式，经典模式很少使用。

B 逍遥游

逍遥游与自由门界面一致，并且使用方法相同，但仅提供U通道，并且不能设置二级代理。

C 动网通

动网通与自由门和逍遥游不太相同。动网通采用F3或F2通道，仅有中文版本。无自动启动火狐的功能，必须手动并指定端口。打开后会有如下设置。您可以自动搜索代理，也可以手动输入代理，也可配合MultiProxy等软件使用。当封锁严重时，自己寻找海外代理并且给动网通进行代理设置是不错的选择。

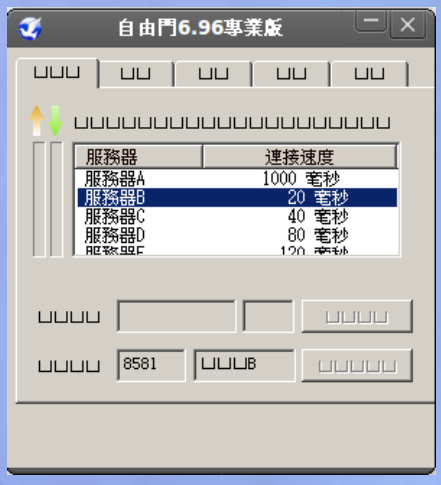
Linux平台

在linux下运行windows软件需要安装wine。wine不是模拟器(Wine Is Not an Emulator)，而是通过调用一系列dll文件来运行windows程序。由于linux发行版众多，安装方法可能有所不同，下面以ubuntu 9.10为例说明。

进入终端，输入命令`sudo apt-get install wine`，按回车输入密码，自动安装。或者进入新立得(Synaptic)搜索"wine",然后标记安装。wine文件较大，请耐心等待几分钟。

安装完成后，右键点击自由门(逍遥游，动网通)，用wine打开，此时自由门仍然不能运行。

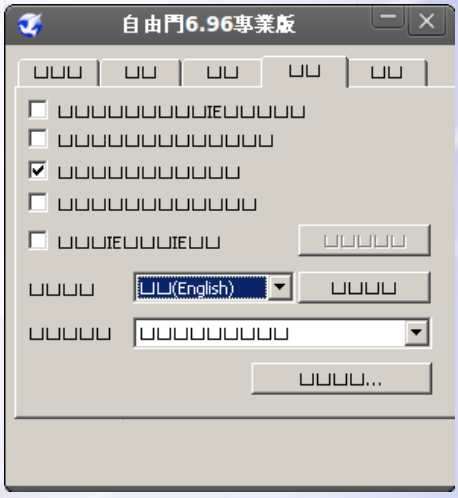
提示缺少mfc42.dll文件。该文件可以在windows系统中获得，路径为C:\windows\System32\mfc42.dll。将该文件拷贝到自由门同一文件夹下，自由门就可以运行了。



linux系统是没有IE浏览器的，而ie4linux并不好用，所以我们点击"否"，运行代理模式，然后将firefox的代理设置为127.0.0.1:8580。

Wine internet explorer自动打开了。用处不大，使用也不方便，可以把它关掉。

在linux下使用windows软件，中文字体经常会出现乱码，这是wine的老毛病了。我们可以把语言设置成英文，然后重新启动自由门。



把语言设置成英文就正常了。

Wine可以在类unix操作系统上运行，如mac、OpenBSD、OpenSolaris等。不同的操作系统安装方法有所不同，详细的安装方法可以在www.winehq.org上找到。您也可以下载源代码，自己编译安装。

逍遥游和动网通的使用方法和自由门是一样的。都需要将mfc42.dll放在同一文件夹下。

常见问题和提示

Q：破网软件下载后不能使用，显示为"不是有效的win32应用程序"
A：软件没有下载完全，请重新下载。
Q：杀毒软件报毒
A：第一，因为破网软件需要“听”服务器的指令，因此常见的防毒软件如果有高敏感异常行为侦测就会把这个动作视为“后门(backdoor)”。第二，国内的杀毒软件将自由门判为病毒。
Q：退出自由门后IE就无法上网了
A：这是由于自由门退出不正常所造成的。请启动自由门，再退出自由门或者手动打开IE取消勾选“代理服务器”设置。
Q：自由门（逍遥游、动网通）运行后后只看到闪了一下就消失了
A：这是破网软件的自我保护措施。新版的动态网系列软件会自动检测用户电脑上是否装有可能盗取破网软件信息的软件存在。如果发现可疑，就会自动退出。请检查电脑上是否安装了不常见的软件，可以这些软件卸载后试试。
Q：自由门（逍遥游、动网通）升级后会在同一文件夹下留下.part文件。
A：出现.part不是坏文件，是更新下载尚未完成时退出破网软件产生的，保留这个.part文件，下次启动后会续传。

使用无界浏览翻墙教程

文 / Allen

优缺点总结

优点:
获取方便，操作简单，速度快

获取无界浏览

1 电邮索取。用国外电子邮箱给wj@wujie.net发一个电子邮件，几分钟内会收到回信，拿到几个有效IP地址，通过这些IP能够访问无界浏览网站，下载无界浏览。

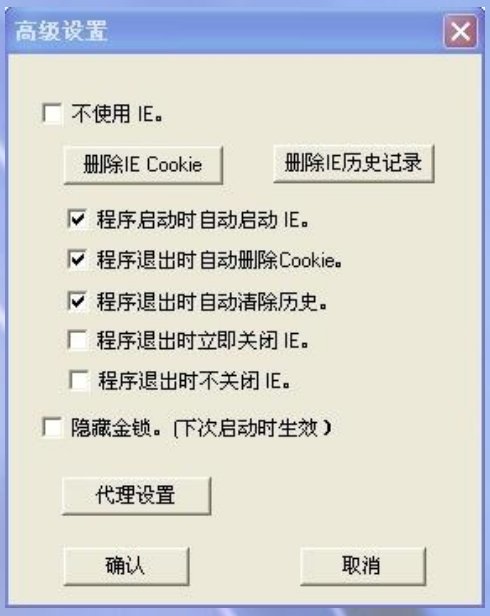
2 SKYPE索取。将"wujie.net"加为好友，个人资料上便会显示无界当前有效网址，给此帐号发任何讯息，便会收到无界说明及软件下载。

3 GTALK索取。给wj2007001@gmail.com，wj2007002@gmail.com，wj2007003@gmail.com，wj2007004@gmail.com，wj2007005@gmail.com，wj2007006@gmail.com发送任意消息，对方会立即回复最新IP。

使用方法

初次使用会弹出设置的窗口。点击"代理设置"可以设置二级代理。

无界浏览的经典模式和自由门的经典模式一样，IE不会设置代理，只能从无界浏览页面连接打开新页面。无界浏览功能比较简单，使用其他浏览器的，请设置代理127.0.0.1:9666。经测试，无界浏览不能通过wine在linux系统中运行。



使用GTunnel翻墙教程

文 / Allen

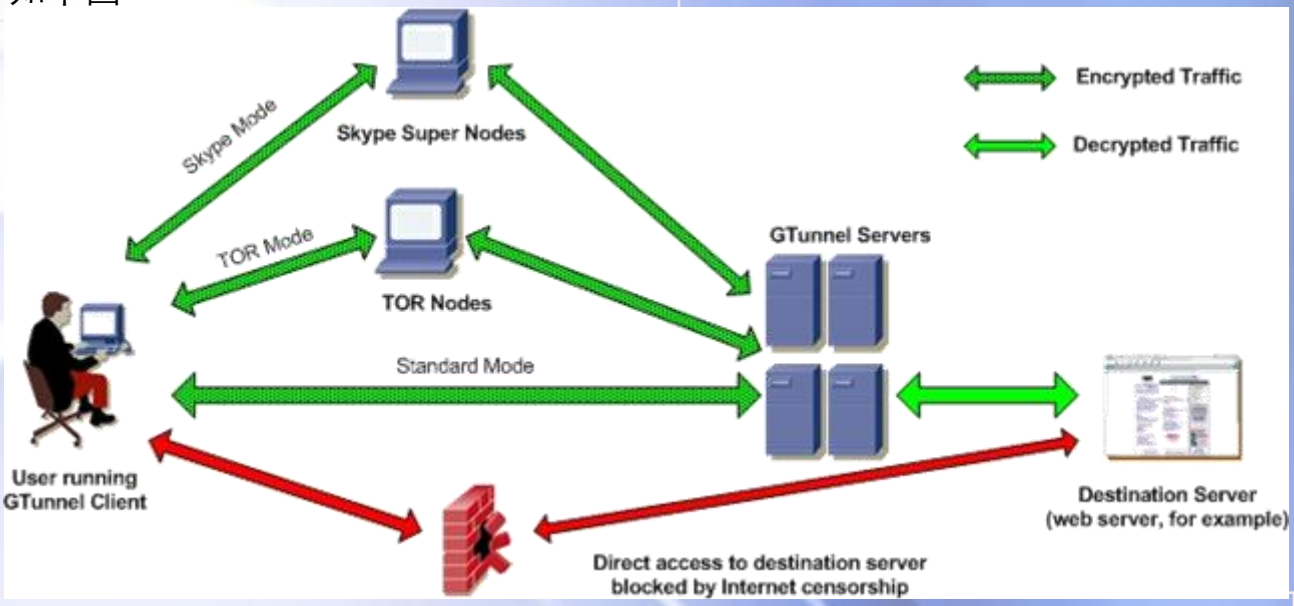
优缺点总结

优点:
拥有多种模式，适用于不同的网络环境（包括教育网）

Gtunnel是一个运行在Windows上的HTTP/SOCKS代理软件。

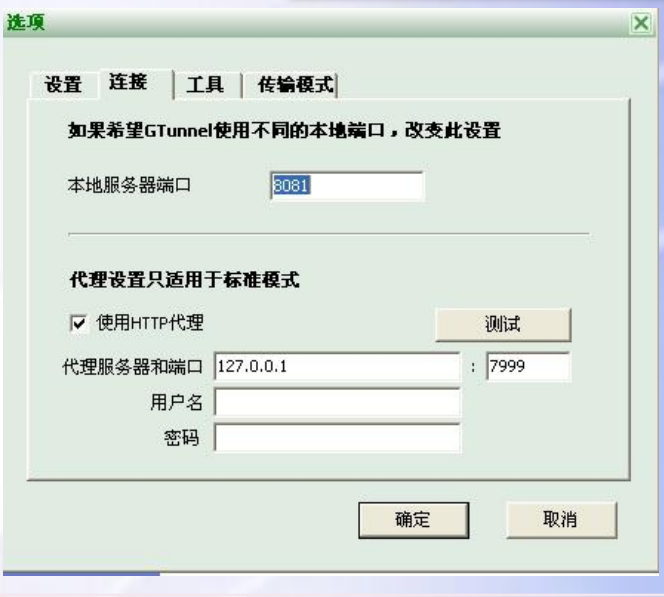
要获取Gtunnel请发电邮到support@gardennetworks.org。

Gtunnel有四种模式，标准模式，GTALK模式，SKYPE模式和TOR模式。GTunnel可以通过wine在linux系统中使用标准模式和GTALK模式。
推荐使用GTALK模式。GTUNNEL原理如下图:



1标准模式。STUNNEL的默认模式，直接连接GTUNNEL服务器，连接成功率不高，可以设置二级代理。

2 GTALK模式。速度快，连接成功率高，在无法访问国外网站的教育网可以使用。进入设置菜单中的传输模式选项卡，填入您的GMAIL邮箱的帐号密码，点击测试，如果测试成功则可使用。原理是通过GOOGLE的服务器连接GTUNNEL服务器，从而突破网络封锁，有了GOOGLE的带宽，速度也有保障。缺点在于，不能下载大文件或长时间看YOUTUBE视频。一旦GOOGLE发现流量异常巨大，会将GOOGLE帐号暂停一段时间，在暂停期间无法使用



GOOGLE的服务，所以为了不影响正常使用，建议单独注册一个GOOGLE帐号用来使用GTUNNEL。

3 SKYPE模式。需要安装SKYPE，您应该下载原版的SKYPE而不是TOM-SKYPE。

使用步骤

一 运行skype程序，要申请一个skype免费帐号，并且用这个帐号登录skype。 当然如果你本来就有skype免费帐号，那就不用申请了，直接登录即可，然后再运行GTunnel。

二 在GTunnel"选项"里，将"工作模式"定为"skype模式"，重启GTunnel使设置生效。

三 这时Skype这个软件会跳出一个提示，提示你有个第三方插件GTunnel.exe想使用Skype，这时，请选择"同意"！。只有选择了同意，GTunnel才能正常运用skype模式。

四 重要提示：有些朋友选择错误了，或者由于一直没有做选择，结果Skype就拒绝GTunnel调用它。这样当然GTunnel的skype模式就不能正常工作了。而且这种拒绝是有记忆性的，以后skype不再有提示，你根本不知道问题出在哪里。那么，这时该怎么办呢?

1 登录进入Skype主窗口。

2 单击"工具"菜单下的"选项"命令，显示"skype选项"窗口。

3 单击"高级"目录下的"高级设置"子目录，窗口右侧显示"高级设置：Skype更新及外部程序"视图。

4 单击"其它程序对Skype的访问"，显示"管理API访问控制"窗口。

5 在列表中选择"GTunnel.exe"，然后单击"更改"，显示另一个视图。

6 单击"允许此程序使用Skype"单选按钮，然后单击"确定"，返回之前的视图。

7 单击"确定"，完成Skype允许花园软件访问的设置。

8 不同版本的SKYPE设置可能有所不同，具体操作见"帮助"。

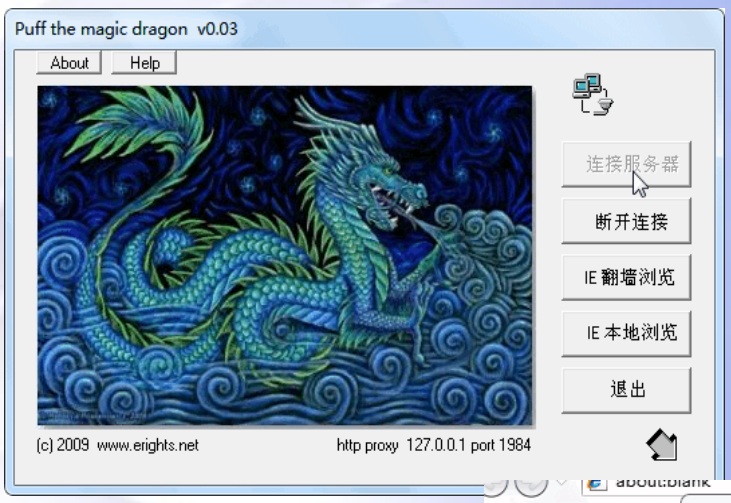
4 tor模式。需要安装TOR并添加网桥，通过TOR连接GTUNNEL服务器，速度较慢。

使用PUFF翻墙操作教程

文 / huxim

优缺点总结

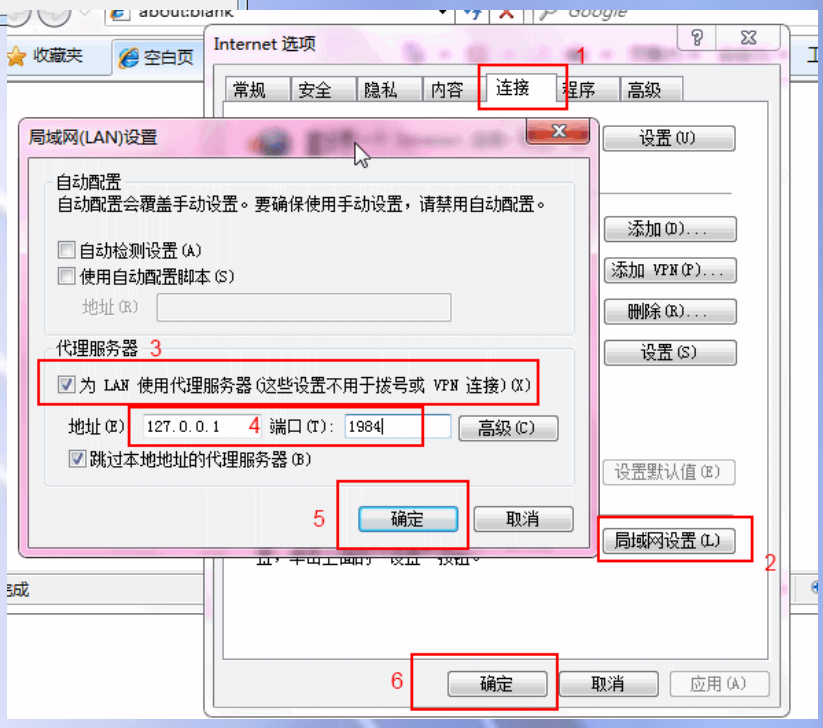
优点:
简单,快速,能看YouTube视频.
缺点:
在敏感时期,GFW会加紧封锁,Puff可能会无法使用



Puff的使用很简单:
安装，启动，连接服务器

然后在浏览器中设置代理服务器，地址为127.0.0.1，端口为1984，类型为HTTP

搞定.访问
http://twitter.com/试试吧



洋葱路由：TOR快速上手教程

文 / huxim

优缺点总结

优点:
- 匿名,意味着更加安全
- 健壮,即使是在GFW最严的时候,Tor依然可用(需手动添加网桥)

缺点:
- 慢速,几乎不能用来看YouTube

推荐使用Tor便携版，下载请猛击我

STEPS

1、直接启动Tor.exe，等待Tor连入网络。（如果是官方原版，需要安装后启动Vidalia.exe）

2、（编者注：2、3、4步骤为获取和添加网桥，非必要）如果你的Tor长时间无法连接，用你的Gmail给bridges@torproject.org 发送一封邮件（记得要用纯文本格式），邮件的标题和正文写上get bridges（注意当中有空格）。稍后你会收到一封邮件，里面有3个bridges（类似201.53.68.143:443格式）。

3、点 设定->网络,将前面收到的bridges添加进去，确定即可。

4、点 停止TOR,再点 启动TOR,确保洋葱头变绿。（如果是官方原版，还需再启动Privoxy.exe）

5、在浏览器中设置代理服务器,地址为127.0.0.1,端口为8118，类型为HTTP，完成!

在Linux系统上使用TOR

文 / Allen

本文以Ubuntu 9.10为例演示Linux系统上使用TOR翻墙的方法。

准备工作：安装libevent1和tsocks。进入终端，输入命令

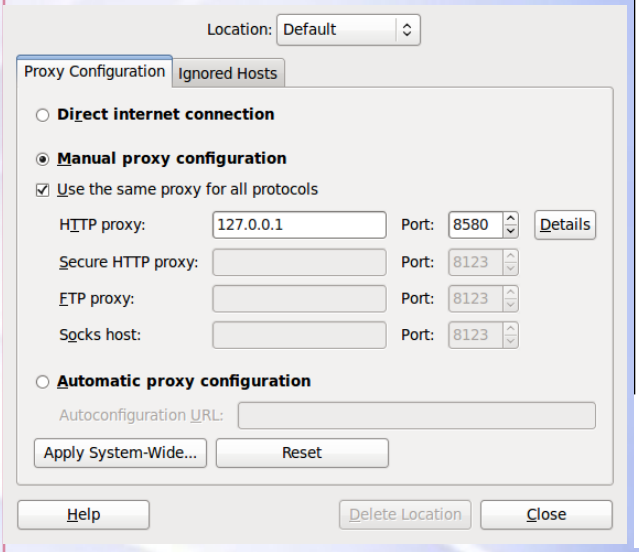
```
sudo apt-get install libevent1 tsocks
```

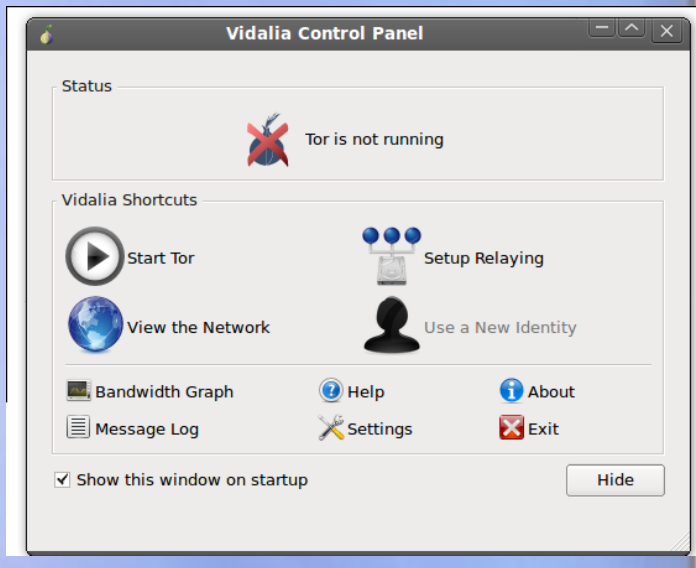
如果已经安装，可以跳过这一步。

安装tor：由于ubuntu官方软件源里的tor版本太老，不适合使用，而torproject.org被封锁,这就给安装带来了一些不便。因此需要给系统设置代理。

点击System-Preferences--Network proxy设置代理

点击Apply system-wide可以给系统设置全局代理。





添加原装Tor软件源（Software Sources）

在/etc/apt/sources.list文件中或者通过System--Administration--Software Sources--Other Software来填加如下原装Tor软件源:

```
deb http://deb.torproject.org/torproject.org karmic main
deb-src http://deb.torproject.org/torproject.org karmic main
```

导入原装Tor的签名键:

```
sudo gpg -keyserver keys.gnupg.net  -recv 886DDD89
sudo gpg -export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 |
sudo apt-key add -
```

在完成以上命令后，更新软件源:

```
sudo apt-get update
```

安装tor

```
sudo apt-get install tor polipo
```

顺便说一下，tor是socks代理，需要使用polipo将socks转换成http。privoxy的功能和polipo是一样的，您也可以选择安装privoxy。

如果您不想使用图形界面，那么安装就到此结束了。接下来应该对tor进行设置，如果您希望像windows一样拥有vidalia图形界面，请跳到B步骤。由于tor和polipo默认开机启动，所以使用比较方便。

接下来应该添加网桥了。使用管理员身份打开/etc/tor/torrc文件，这是tor的配置文件。进入终端，输入命令sudo gedit /etc/tor/torrc

输入格式如下：

```
UseBridges 1
Bridge 76.84.109.179:443
Bridge 80.219.71.234:9876
Bridge 92.224.168.69:443
```

网桥可以自行添加，保存后退出。

下面配置polipo，使用管理员身份打开/etc/polipo/config文件，这是polipo的配置文件。进入终端，输入命令

```
sudo gedit /etc/polipo/config
```

找到如下两行，将前面的#去掉，然后保存退出。

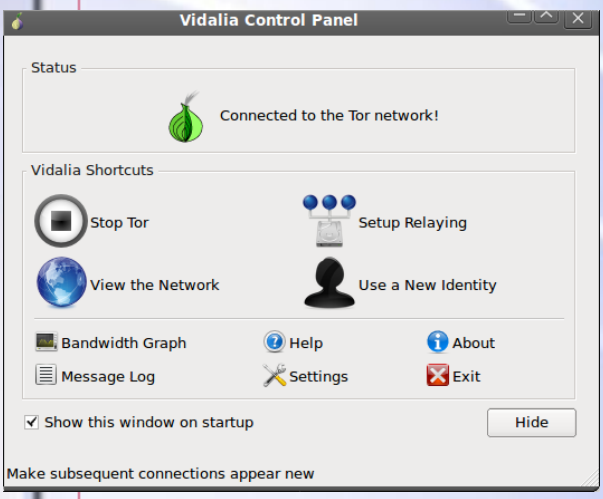
```
# socksParentProxy = "localhost:9050"
# socksProxyType = socks5
```

您需要重新启动polipo使配置生效。输入命令sudo /etc/init.d/polipo restart

polipo的端口是8123，所以将浏览器代理设置为127.0.0.1:8123

安装vidalia，输入命令sudo apt-get install vidalia

由于tor默认随系统启动，所以需要停止tor服务，否则会产生冲突。如上页右图。



Tor装好后/etc/rc2.d目录下多了个启动链接:S20tor，将其改名为K20tor就可以禁止其开机启动。进入终端输入命令：

```
sudo mv /etc/rc2.d/S20tor /etc/ra2.d/K20tor
```

输入命令sudo service tor stop或sudo /etc/init.d/tor stop停止tor服务。

启动vidalia（Applications>Internet>Vidalia）

现在可以和windows一样启动tor了。所有操作和windows下的tor一样。

此时torrc文件的路径为：/home/~/.vidalia/torrc，修改该文件无须启用管理员身份。

附录：torrc常用设置，windows和linux都适用

●网桥

UseBridges 0|1

用来开关网桥，1是使用网桥，0 是不使用网桥。

网桥的格式

Bridge xxx.xxx.xxx.xxx:端口

●排除节点

ExcludeNodes node,node,...

排除较慢节点 ExcludeNodes SlowServer

排除中国，伊朗节点 ExcludeNodes {cn},{ir} {}里面为国家代码

排除IP ExcludeNodes 255.254.0.0/8

Tor使用手册

文 / J.Smith

编者按：由于本文较长，这里不提供全文，请您联网后点击下面的链接在线阅读本文。本文有可能会随本书附带。

随着网络封锁的加重，现在越来越多的网站都需要翻墙才能访问，虽然Tor速度相对较慢，但是作为目前最稳定的翻墙工具，Tor还是应该必备了，可以在其他翻墙工具都无法使用的时候作为一个后备工具，用来获取其他速度较快的翻墙工具.本系列将从简入深详细说明Tor的使用和配置。

http://is.gd/94rNf

目录

Your Freedom使用手册

文 / J.Smith

编者按：由于本文较长，这里不提供全文，请您联网后点击下面的链接在线阅读本文。本文有可能会随本书附带。

Your Freedom免费版提供了128Kbps的上行和下行带宽，而且相当稳定，算是一个满不错的翻墙工具。

http://is.gd/94s9F

目录

教你几招：

1. 请学习使用最普通的HTTP代理和HTTPS代理（有效期短，无法访问DNS被污染的网站）
2. 学习修改本地DNS，试试Google的DNS 8.8.8.8和OpenDNS 208.67.222.222
3. 学习使用Firefox的插件Autoproxy（参考autoproxy.org和http://livessh.spaces.live.com），能突破DNS污染
4. Chrome浏览器的DEV版也可以突破DNS污染
   http://build.chromium.org/buildbot/snapshots/chromium-rel-xp/LATEST
   在地址栏打上这个网址，会出来一个数字，意思就是最近刚刚刷新的版本号。然后把上面那个LATEST换成获得的数字，回车就进入dev的最新的ftp了，右键直接下载就成。有zip包，也有exe安装包。很方便的。

——zjsz007

使用GAppProxy翻墙操作教程

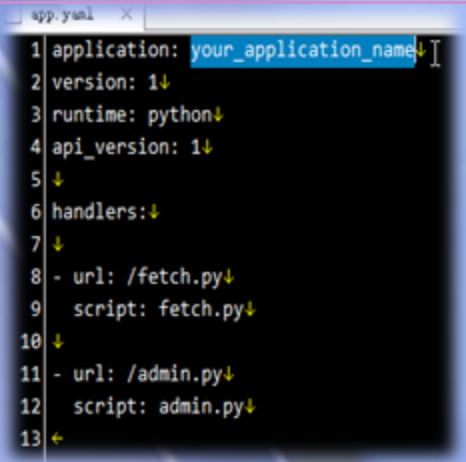
编者按：GAppProxy是运行于Google App Engine上的一个开源的HTTP Proxy软件。

文 / huxim

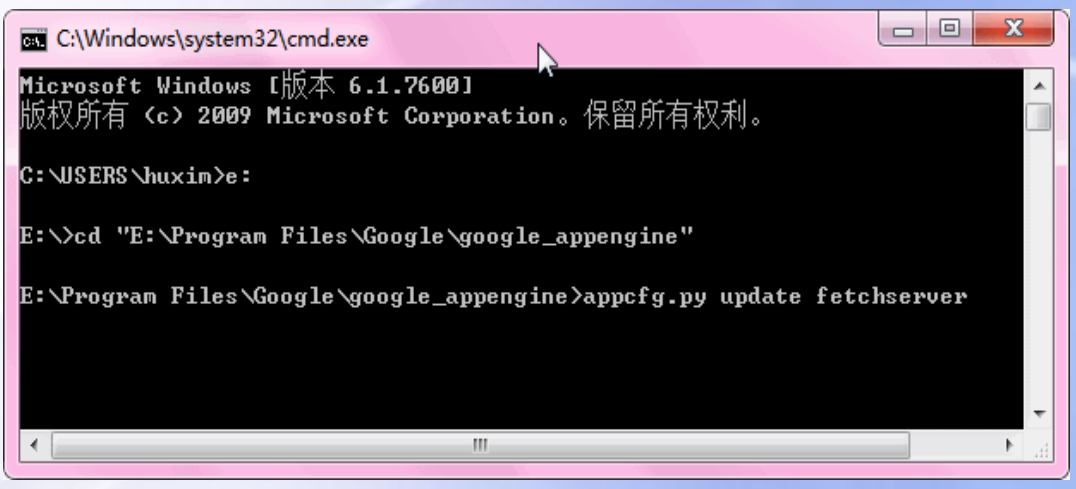
优缺点总结

优点:
●私有性，自己管理，自己使用，而且除非GFW将整个Google App Engine封掉，否则无法阻止我们翻墙.
●快速,使用Google服务器，速度有保障.
缺点:
●仅支持标准80端口的HTTP协议和443端口的HTTPS协议，其他端口均不支持.
●由于Google App Engine限制，对HTTPS链接安全性不高.
●Google App Engine有一系列配额限制，但仅仅用来翻墙足够使用.

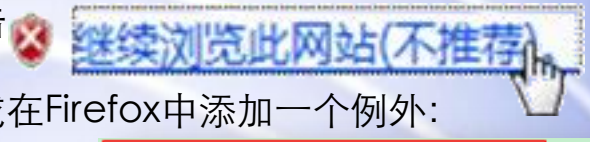
1、注册一个Google账户并申请Google App Engine（申请过程参考）（记下你的App地址,类似*aaa.appspot.com*，后面需要这里的*aaa*）；
2、安装 python-2.6.4.msi；
3.、安装 GoogleAppEngine_1.3.1.msi（假定安装在 *E:\Program Files\Google\google_appengine*）；
4、下载 GAppProxy完整源码并解压；
5、将 完整源码r102 中的 fetchserver 文件夹复制到 GoogleAppEngine SDK 的安装目录中（即上例中的 E:\Program Files\Google\google_appengine ，如果你安装到了别的目录,请作相应变更）；
6、把E:\Program Files\Google\google_appengine\fetchserver 中的app.yaml用记事本打开，将your_application_name 替换为你的Appname（如上例中的aaa,请根据自己的Appname替换），保存退出。



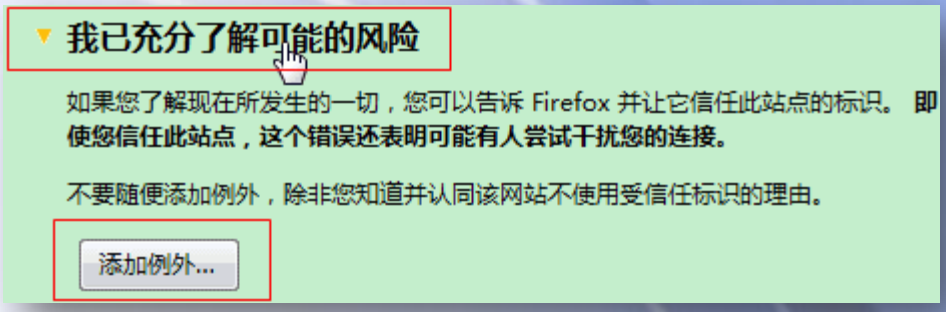
7、点击 开始->运行,输入 “cmd” ， 确定;
8、进入 GoogleAppEngine SDK 的安装目录,并执行:
appcfg.py update fetchserver



然后它会提示你输入google帐户和密码（输密码时不会有反应，不过确实在输入）;
9、等待上传完毕，服务端架设完毕，下面设置本地端;
10、回到 完整源码r102，进入 localproxy 文件夹，将 proxy.conf 用记事本打开，在最后增加一行:
fetch_server = http://aaa.appspot.com/fetch.py
(请根据自己的Appname替换上面的aaa)
保存退出;
11、双击proxy.py，GAppProxy启动!
12、在浏览器中设置代理服务器，地址为127.0.0.1,端口为8000，类型为HTTP。然后访问twitter试试;
13、如果你使用GAppProxy访问HTTPS链接，会出现证书错误，请在IE中点击



或在Firefox中添加一个例外:



SSH翻墙指南

文 / 萧易寒

优缺点总结

优点:
- 速度快;
- 断线自动重连;
- 智能判断网址并切换代理（仅在访问被墙网站是时才走SSH Tunnel）。

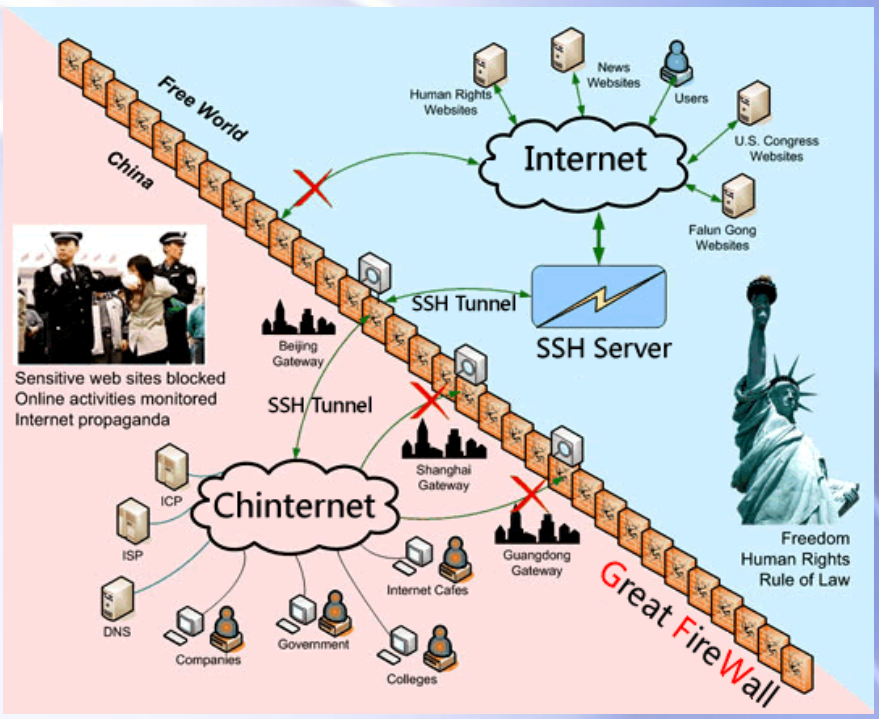
缺点:
- 免费的SSH服务器不好找。

SSH简介

SSH全称Secure Shell，是建立在应用层和传输层基础上的安全协议。

传统的网络服务程序，如FTP、POP和Telnet其本质上都是不安全的；因为它们在网络上用明文传输数据、用户帐号和口令，很容易被监听。

而SSH则是加密的，并且可以取代Telnet和FTP等协议用来远程登录会话。大部分Linux主机都默认提供SSH进行远程管理，在Windows下面则需要额外安装SSH Server，比如F-Secure SSH等软件。



SSH翻墙原理

SSH翻墙的原理是本地与墙外远程服务器建立一个加密的隧道（SSH Tunnel），经过它的数据被加密过，不会被拦截。由墙外的服务器获取想要访问的内容后，再通过这个通道传输回来。

SSH翻墙操作

1、获取SSH帐号

一般有下列三种途径：

- "寻找国外免费的并且提供SSH帐号的虚拟主机。
- "购买单独的SSH代理帐号，价格约为0.1元/天或者几十元/年至1元/天或几十元/月不等。

在http://www.ssher.net购买SSH账号时报出暗号“墙倒众人推”可以获得一段时间试用等优惠。

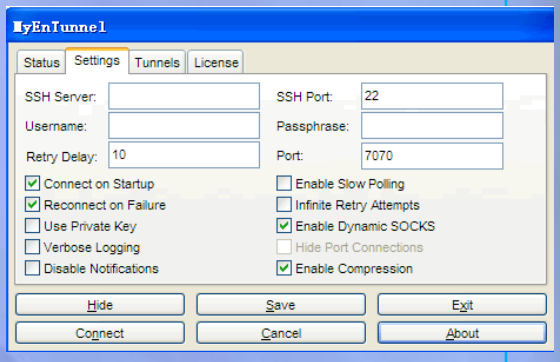
- "购买一个国外的收费空间或者VPS，一年的费用不会超过500元，可以供数十位朋友一起使用SSH，同时还可以建立独立博客，畅所欲言，不用担心文章被国内的BSP删除。几乎所有国外收费的Linux虚拟主机/VPS/独立主机都提供SSH管理帐号，著名的IDC中，除Godaddy外，大部分SSH都支持SSH Tunnel，也就是可以在GFW中穿一个加密隧道，访问被墙网站。

2、安装配置MyEnTunnel软件

下载并安装MyEnTunnel，该软件全名为My Encrypted Tunnel，需要和Putty中的plink.exe配合使用，官方网站：http://nemesis2.qx.net/pages/MyEnTunnel（已被墙）。

点击这里下载MyEnTunnel和PLink的打包版本，在Google中搜索MyEnTunnel也可以找到很多其他下载点。

如图所示：



在MyEnTunnel的Settings页中填入SSH Server的域名或IP，在Username和Passphrase/Password中填入SSH帐号的用户名和密码。

远程的SSH端口默认是22，本地代理端口默认是7070，必须勾选Enable Dynamic SOCKS，可选Enable Compression用以压缩数据、加快速度。

点击Connect，待MyEnTunnel的状态图标变绿，即在本地7070端口和国外SSH Server的22端口之间建立了一条加密的通道。

3、配置浏览器

下载pac脚本文件存至本地硬盘，比如C盘根目录。用户也可以访问https://autoproxy2pac.appspot.com/勾选ssh -D 获取最新的pac文件。

下载的pac文件是一个脚本，可以用文本编辑器打开，通过这个pac脚本：

"当用户访问被墙的网站时，脚本文件自动命令浏览器访问本地的7070端口，也就是走SSH Tunnel，达到翻墙的目的；

“当用户访问国内的网站时，脚本文件自动命令浏览器不通过SSH代理，达到快速访问的目的。

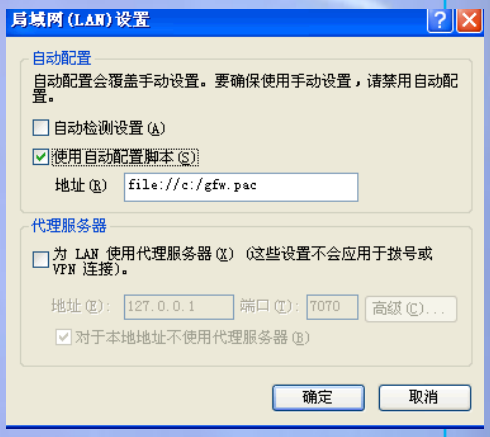
主流的三种浏览器配置如下：

"IE：打开菜单"工具 - Internet选项 - 连接 - 局域网设置"，勾选"使用自动配置脚本"填入 file://c:/gfw.pac（表示自动脚本为gfw.pac，且该文件位于C盘根目录）。

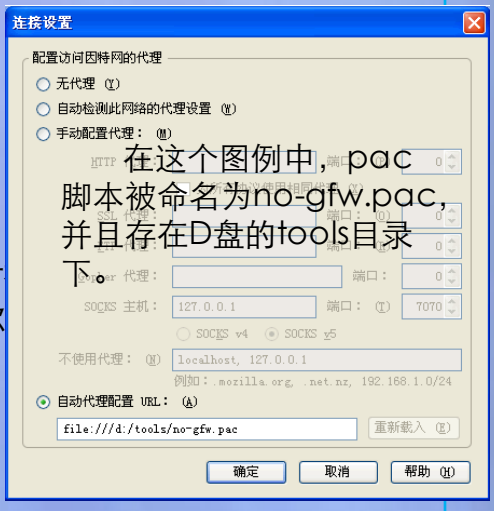
"Chrome：打开菜单"选项 - 高级设置 - 更改代理服务器设置 - 局域网设置"，勾选"使用自动配置脚本"填入 file://c:/gfw.pac。

由于Chrome和IE共享一样的局域网设置，可参考IE的设置图。

“FireFox：打开菜单”工具 - 选项 - 高级 - 网络 - 设置“，勾选”自动代理配置URL“填入 file:///c:/gfw.pac（注意ff使用file:///代表本机地址，ie使用file://）



另外，pac文件也可以存储在网络上，你可以在IE/Chrome/FireFox的脚本地址中填入网络地址，比如 https://www.proxy.com/proxy.pac，建议使用https协议，因为pac文件的内容会被GFW嗅探到，触发关键词而撞墙。



在这个图例中，pac脚本被命名为no-gfw.pac，并且存在D盘的tools目录下。

4、测试是否能成功翻墙

全部关闭浏览器后重新打开，并访问平时www.blogger.com，如果访问正常，恭喜你条隧道，可以自由的访问被屏蔽的网站了。

如果失败，请检测以下常见问题：

"MyEnTunnel是否连接正常

"浏览器中pac脚本的地址是否正确

"不能访问的网站是否出现在pac脚本中（pac脚本的屏蔽网站列表可能不全，可以自行添加网站在pac文件中，详见后续章节或者上 https://autoproxy2pac.appspot.com/ 下载最新的pac脚本）

"域名被DNS污染（FaceBook、Twitter等网站的域名被污染，光使用SSH还是无法访问，必须修改Hosts文件指定正确的IP）

扩展阅读

1、pac文件简介

pac是文本格式的脚本文件，由浏览器自动调用，最简单的格式就是包含一个叫FindProxyForURL的JavaScript函数。

函数定义：

```
function FindProxyForURL( url, host )
```

参数url表示用户浏览地址的URL全路经，如

http://www.google.cn/search?hl=zh-CN&q=64

参数host表示这个URL中的主机名部分，如 www.google.cn

FindProxyForURL函数有三种可能的字符串返回值，

1."DIRECT"，就是直接连接，不通过代理；

2."PROXY proxyaddr:port"，其中proxyaddr和port分别是代理的地址和代理的端口；

3."SOCKS socksaddr:port"，其中socksaddr和port分别是socks代理的地址和端口。

一个自动代理文件可以是多个选择的组合，用分号";"隔开，如：

```
function FindProxyForURL(url,host)
{
if (host == "www.notblocked.com")
return "DIRECT";
else
return "PROXY myproxy:80;SOCKS 127.0.0.1:7070;DIRECT";
}
```

2、扩充pac文件

网上下载的pac文件中，一般类似于如下格式：

```
function FindProxyForURL( url, host )
{
if ( shExpMatch(url, "*blocked-site-a.org*")
|| shExpMatch(url, "*.blocked-site-b.com")
......
|| shExpMatch(url, "*.blocked-site-yyy.com*")
)
return "SOCKS 127.0.0.1:7070";
else
return "DIRECT";
}
```

由于屏蔽网站列表不一定是最新和最全的，用户需要自行扩充，以访问被屏蔽但没有进入代理列表的网站。

假定www.xxx.com被墙，但PAC脚本中没有xxx.com，将xxx.com加入代理列表加密访问的方法如下：

在|| shExpMatch(url, "*.another-free-site.com*")后面新增一行：|| shExpMatch(url, "*.xxx.com*")

保存pac文件，重启浏览器，键入www.xxx.com即可直接访问。

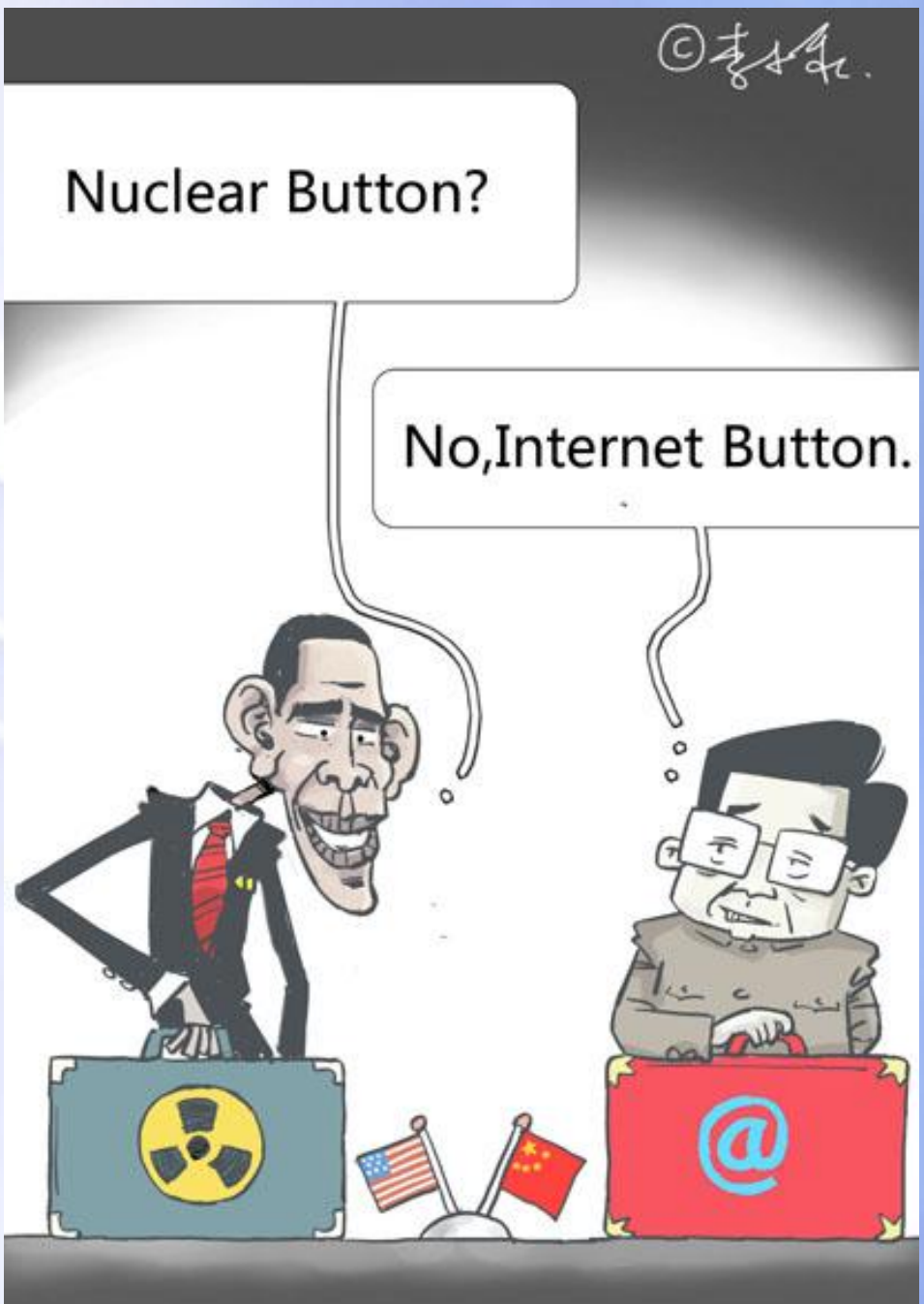
扩充后的pac文件格式如下：

```
function FindProxyForURL( url, host )
{
if ( shExpMatch(url, "*blocked-site-a.org*")
|| shExpMatch(url, "*.blocked-site-b.com")
```

```
......
|| shExpMatch(url,  "*.blocked-site-yyy.com*")
|| shExpMatch(url,  "*.xxx.com*")
)
return "SOCKS 127.0.0.1:7070";
else
return "DIRECT“;
```

参考资料：
JavaScript or JScript Auto-Proxy Example Files
PAC Functions Explained

都是按钮／李小乖



利用IPv6翻墙

文 / 匿名

IPv6翻墙原理

IPv6是什么东西：

IPv6，全称Internet Protocol version 6，是被正式广泛使用的第二版互联网协议。现有标准IPv4只支持大概40亿（232）个网络地址，而IPv6支持2128（约3.4×1038）个。[1]

那么为什么IPv6可以用来翻墙呢？原因在于GFW现在对IPv6束手无策。在GFW开发完成对IPv6的封锁之前，利用IPv6是一种相当稳定、可靠的免费翻墙工具。那么它相比其他众多的翻墙手段（Tor、VPN等），有什么优势和劣势呢？

优势：

1. 一次设置，不需要手动或者靠第三方插件切换。

IPv6翻墙只需要配置好IPv6，在hosts文件中添加好相应信息即可，市面上大部分浏览器，包括IE、Firefox、Chrome、Safari、Opera都支持IPv6。

2. 稳定性更强。利用Teredo和HE Tunnel，可以手动选择服务器地点。

3. 更快的速度。配置基于IPv4的6to4协议本身不提供流量中转，只是一个协议，负责获取IPv6地址，并将IPv6数据包封装在IPv4的UDP数据包中，与提供IPv6连接的服务器建立隧道。相比下VPN技术，需要大宽带的代理服务器支持，转发数据，在代理服务器上造成了不必要的流量和延时，影响速度。

劣势：

1. 仅有部分网站支持IPv6，Google提供了大量IPv6服务，同时网友也利用反向代理技术给许多不支持IPv6的网站提供IPv6。

2. 许多反向代理构造的IPv6网站不支持使用https协议的网站。Twitter则是一个例子。Twitter要求在登录的时候使用https加密防窃听。但是Twitter登录有网友提供了方法。[2]

谁应该考虑使用IPv6翻墙

在配置IPv6之前，请确认你的网络环境，假如符合以下情况，往往IPv6不是最好的选择。

1. 你是在单位、集体内部网络，没有修改防火墙的权利。

2. 你的内网内已经有用户使用IPv6。

如何获取IPv6

途径一：教育网内部分学校已经有原生的IPv6接入。

假如你使用教育网，请查看是否已经接入IPv6，可能你幸运地已经拥有了天然的翻墙环境。

途径二：公网的Windows用户可以使用六飞，需要下载客户端。[3]

途径三：使用HE Tunnel Broker服务获取IPv6。支持Windows、Linux、MacOS X、BSD等众多系统。**强烈推荐有静态公网接入的用户使用[4]，强烈不推荐动态公网和内网用户使用，如3G、(A)DSL、Cable等。**

途径四：使用Teredo协议。支持Windows、Linux、MacOS X、BSD等系统，**支持部分内网和大部分网络环境**，强烈推荐。Teredo有一个局限性，就是一个IPv4公网IP只能有对应一个用户使用，即同一内网内只能有一个人同时使用。

修改hosts文件

在一般情况下，当你在浏览器输入一个URL（网址），浏览器首先会去寻找这个URL中涉及的域名的具体IP地址。浏览器先查阅本地的hosts文件[5]，假如未发现该域名对应的IP地址，则向域名解析服务器发送请求查询，服务器返回具体IP，浏览器再连接此IP。默认情况下，浏览器不会使用IPv6进行连接，所以我们必须在hosts文件中指定域名对应的IP，才可能让浏览器使用IPv6。

hosts文件形式

```
# 井号打头的是注释，没有语言限制
# 又一行注释，不起任何作用
<IP地址（可以是v4或者v6）>  <域名1>  <域名2 域名3...)>
```

例1：

```
2001:4860:c004::68  blogger.com  google.com
```

指定blogger.com和google.com对应的IP地址为2001:4860:c004::68。2001:4860:c004::68属于IPv6。

例2：

```
168.143.162.100   twitter.com
```

指定twitter.com对应的IP地址为168.143.162.100。168.143.162.100属于IPv4。

附录中有详细的IPv6翻墙需要的hosts文件。

注释

[1] 引自Wikipedia中文版，IPv6条目 (http://zh.wikipedia.org/wiki/IPv6)
[2] 参见GFWBlog文章（用IPV6反向代理翻墙），
http://www.chinagfw.org/2010/01/ipv6_19.html
[3] 六飞官方网站，http://www.6fei.com.cn
[4] 内网用户无法使用，动态公网用户可以使用，但是需要经常更新，Linux用户可以尝试ez-ipupdate，将来我可能会写一个Shell脚本负责这个任务，来推广这个途径。
http://wahjava.wordpress.com/2008/09/01/setup-ipv6-tunnels-from-hurricane-electric/
[5] hosts文件具体位置：Windows 2000及以上：
%SystemRoot%\system32\drivers\etc\hosts （默认只读，需要先修改可写权限）
Unix（包括MacOS X、Linux、BSD）上：/etc/hosts （修改需要root权限）

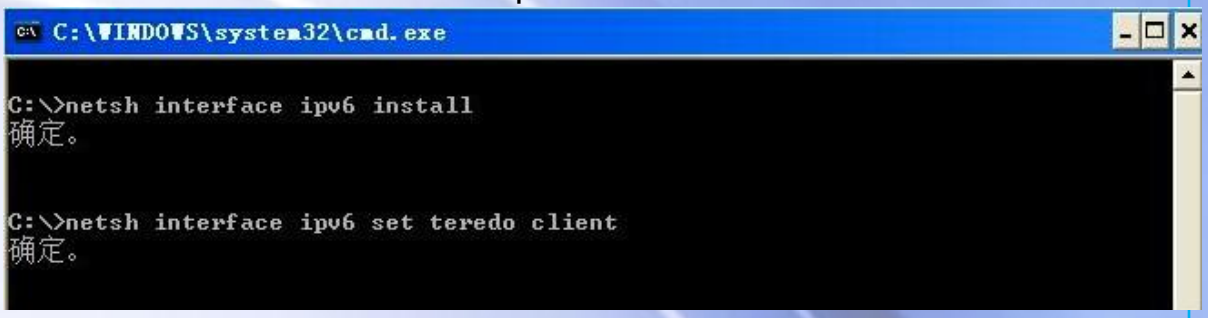
利用Teredo获取IPv6配置

Windows XP SP2&SP3:

官方文档：
http://www.microsoft.com/taiwan/technet/prodtechnol/winxppro/maintain/teredo.mspx （正体中文/台湾）
http://www.microsoft.com/china/technet/prodtechnol/winxppro/maintain/teredo.mspx （简体中文/大陆）

1. 请确保你拥有管理员权限。
2. 点击开始(Start)，点击运行(Run)，在弹出窗口中输入：cmd，回车。
3. 在弹出的命令提示符中，输入：

```
netsh interface ipv6 install
netsh interface ipv6 set teredo client
```



执行以上操作后，应当能够获取IPv6地址。
以上配置完成请看hosts文件配置。

Windows Vista & Windows 7:

Teredo在Windows Vista & Windows 7下已经自动开启。在你的网络适配器的属性内，将自动获取IPv6地址勾上即可。

MacOS X下的配置：

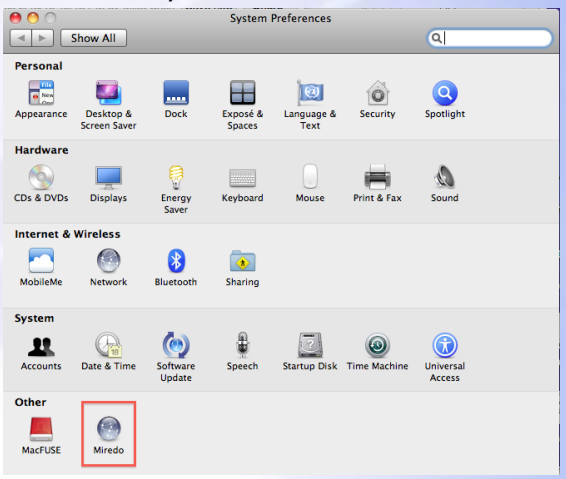
Miredo for OSX目前只支持MacOS X 10.4(Tiger), 10.5(Leopard), 10.6(Snow Leopard 32bit)。

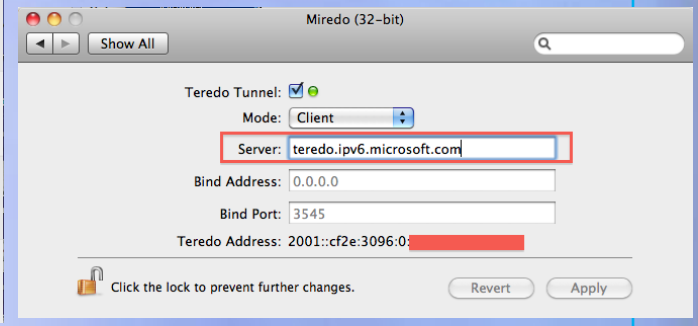
Mac下配置相当简单。这里简单描述。

1. 在官方网站（http://www.deepdarc.com/miredo-osx/）下下载Miredo For OSX。

2. 安装软件。

3. 在System Preferences内，Others一栏内，点击Miredo。





4. 在Server内填入：`teredo.ipv6.microsoft.com`

5. 这时你应该能够看到下方的IPv6地址了。

以上配置完成请看hosts文件配置。

Linux下的配置：

这里以Ubuntu Linux 9.04 (Jaunty) 为例，其他Ubuntu版本和Debian及Debian衍生系列Linux均可以按照此教程配置IPv6。此方法适用于基本所有网络环境，包括外网、内网和防火墙内。

1. 打开终端，进行以后操作。

操作：打开终端。在<应用程序>(Applications)菜单中，进入<附件>(Accessories)子菜单，点击<终端>(Terminal)。

2. 安装Linux下Teredo客户端，名为Miredo。教程使用apt-get快速安装。其他使用RPM包管理的平台同样可以使用yum安装或者编译安装。

操作：输入：`sudo apt-get install miredo`

提示要求输入密码，请输入您的密码。

在确认安装时，输入Y继续。

```
文件(F)  编辑(E)  查看(V)  终端(T)  帮助(H)
ccp@me-laptop:~$ sudo apt-get install miredo
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
将会安装下列额外的软件包：
  libjudydebian1
下列【新】软件包将被安装：
  libjudydebian1 miredo
共升级了 0 个软件包，新安装了 2 个软件包，要卸载 0 个软件包，有 151 个软件未被升级。
需要下载 0B/232kB 的软件包。
解压缩后会消耗掉 627kB 的额外空间。
您希望继续执行吗？[Y/n]Y
选中了曾被取消选择的软件包 libjudydebian1。
(正在读取数据库 ... 系统当前总共安装有 144178 个文件和目录。)
正在解压缩 libjudydebian1 (从 .../libjudydebian1_1.0.5-1_i386.deb) ...
选中了曾被取消选择的软件包 miredo。
正在解压缩 miredo (从 .../miredo_1.1.5-2_i386.deb) ...
正在处理用于 man-db 的触发器...
正在设置 libjudydebian1 (1.0.5-1) ...

正在设置 miredo (1.1.5-2) ...
 * Starting Teredo IPv6 tunneling daemon miredo                    [ OK ]

正在处理用于 libc6 的触发器...
ldconfig deferred processing now taking place
ccp@me-laptop:~$
```

3. 在上个操作中，假如显示如图，说明客户端已经正常安装。

在 Starting Teredo IPv6 tunneling daemon miredo 后，显示有[OK]字样，表示服务已经正常运行，如为Failed，则需要进一步排查原因。

4. 等待10-20秒，miredo 会尝试连接服务器获取IPv6地址。这个过程没有提示。

5. 查看是否已经连接成功。

操作：终端中输入：**ifconfig teredo**

假如返回如图所示，则连接成功：

```
文件(F)  编辑(E)  查看(V)  终端(T)  帮助(H)
ccp@me-laptop:~$ ifconfig teredo
teredo    Link encap:未指定  硬件地址 00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00-00
          inet6 地址：fe80::ffff:ffff:ffff/64 Scope:Link
          inet6 地址：2001:0:53aa:64c:14ea:380d:8884:3680/32 Scope:Global
          UP POINTOPOINT RUNNING NOARP  MTU:1280  跃点数:1
          接收数据包:0 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:3 错误:0 丢弃:0 过载:0 载波:0
          碰撞:0 发送队列长度:500
          接收字节:0 (0.0 B)  发送字节:144 (144.0 B)

ccp@me-laptop:~$
```

假如返回如下图，说明连接失败：

```
文件(F)  编辑(E)  查看(V)  终端(T)  帮助(H)
ccp@me-laptop:~$ ifconfig teredo
teredo    Link encap:未指定  硬件地址 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00
          POINTOPOINT NOARP  MTU:1500  跃点数:1
          接收数据包:0 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:0 错误:0 丢弃:0 过载:0 载波:0
          碰撞:0 发送队列长度:500
          接收字节:0 (0.0 B)  发送字节:0 (0.0 B)

ccp@me-laptop:~$
```

若连接失败需要修改服务器：

操作：1. 在终端中输入：**sudo gedit /etc/miredo/miredo.conf**

2. 修改：

```
# Pick a Teredo server:
#ServerAddress teredo.ipv6.microsoft.com
ServerAddress teredo-debian.remlab.net
```

为：

```
# Pick a Teredo server:
ServerAddress teredo.ipv6.microsoft.com
#ServerAddress teredo-debian.remlab.net
```

3. 保存，终端中执行：**sudo /etc/init.d/miredo restart**

```
文件(F)  编辑(E)  查看(V)  终端(T)  帮助(H)
ccp@me-laptop:~$ sudo /etc/init.d/miredo restart
 * Stopping Teredo IPv6 tunneling daemon miredo
 * Starting Teredo IPv6 tunneling daemon miredo
ccp@me-laptop:~$
```

4. 重新查看是否成功连接

6. 查看连接是否可以正常使用：
操作：终端中输入：`ping6 ipv6.google.com -c5`
返回如图则可以正常使用。

```
文件(F)  编辑(E)  查看(V)  终端(T)  帮助(H)
ccp@me-laptop:~$ ping6 ipv6.google.com -c5
PING ipv6.google.com(www.google.com) 56 data bytes
64 bytes from www.google.com: icmp_seq=1 ttl=58 time=357 ms
64 bytes from www.google.com: icmp_seq=2 ttl=58 time=357 ms
64 bytes from www.google.com: icmp_seq=3 ttl=58 time=356 ms
64 bytes from www.google.com: icmp_seq=4 ttl=58 time=357 ms
64 bytes from www.google.com: icmp_seq=5 ttl=58 time=357 ms

--- ipv6.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 356.816/357.401/357.811/0.758 ms
ccp@me-laptop:~$
```

以上配置完成请看hosts文件配置。

hosts文件配置

Windows:

1. 打开文件夹浏览器。
2. 地址栏中输入：%SystemRoot%\system32\drivers\etc\hosts
3. 假如这是你第一次修改hosts文件：
找到hosts文件，右键，属性。在下方权限处，反选只读，确定并关闭属性窗口。
4. 双击hosts文件，将会使用记事本或其他文本编辑器打开。
5. 修改并保存。

Unix (MacOS X、Linux、BSD)：

1. 打开终端。Linux下可以是konsole、gnome-terminal等，MacOS X下终端位于/Applications/Utilities/Terminal.app
2. 运行：

```
cd /etc
cp hosts hosts.old
sudo <nano/vi/gedit/kate> hosts
```

Unix下hosts文件范例：

```
127.0.0.1 localhost
127.0.1.1 <主机名>

# The following lines are desirable for IPv6 capable
hosts
::1     localhost ip6-localhost ip6-loopback
#fe00::0 ip6-localnet
#ff00::0 ip6-mcastprefix
#ff02::1 ip6-allnodes
#ff02::2 ip6-allrouters
#ff02::3 ip6-allhosts
2001:4860:c004::68 www.google.com
2001:4860:c004::68 www.google.com.tw
2001:4860:c004::68 clients1.google.com
2001:4860:c004::68 ipv6.google.com
2001:4860:c004::68 mail.google.com
2001:4860:c004::68 www.youtube.com
2001:4860:c004::68 gdata.youtube.com
2001:4860:c004::68 upload.youtube.com
2001:4860:c004::68 insight.youtube.com
2001:4860:c004::68 help.youtube.com
2001:4860:c004::68 s.ytimg.com
2001:4860:c004::68 www.blogspot.com
2001:4860:c004::68 www.blogger.com
2001:4860:c004::68 blogspot.com
2001:4860:c004::68 blogger.com
```

hosts文件汇集：

完整的列表可以在这里找到：

http://docs.google.com/Doc?docid=0ARhAbsvps1PlZGZrZG14bnRfNjFkOWNrOWZmcQ&hl=zh_CN

下一页提供了三个常用网站对应的hosts内容。

```
#Twitter
2001:470:83f2::710:1 twitter.com
2001:470:83f2::710:1 www.twitter.com
2001:470:83f2::710:1 m.twitter.com    #Twitter Mobile
2001:470:83f2::710:1 search.twitter.com #Twitter Serach
2001:470:83f2::710:1 integratedsearch.twitter.com
2001:470:83f2::710:1 api.twitter.com
2001:470:83f2::710:1 s.twimg.com     #Twitter Search
2001:470:83f2::710:1 a0.twimg.com
2001:470:83f2::710:1 a1.twimg.com
2001:470:83f2::710:1 a2.twimg.com
2001:470:83f2::710:1 a3.twimg.com
2001:470:83f2::710:1 twitpic.com
2001:470:83f2::710:1 twitgoo.com

#Google Picasa
2001:4860:c004::62 photos.google.com
2001:4860:c004::62 picasa.google.com
2001:4860:c004::62 picasaweb.google.com
2001:4860:c004::62 lh0.ggpht.com
2001:4860:c004::62 lh1.ggpht.com
2001:4860:c004::62 lh2.ggpht.com
2001:4860:c004::62 lh3.ggpht.com
2001:4860:c004::62 lh4.ggpht.com
2001:4860:c004::62 lh5.ggpht.com
2001:4860:c004::62 lh6.ggpht.com
2001:4860:c004::62 lh7.ggpht.com
2001:4860:c004::62 lh8.ggpht.com
2001:4860:c004::62 lh9.ggpht.com

# Google Docs
# Google Docs的https加密版本现在被墙，以下支持https加密
# 同时也可以防止某些敏感文章被墙
2001:4860:c004::64 docs.google.com
2001:4860:c004::64 writely.l.google.com
2001:4860:c004::62 spreadsheet.google.com
2001:4860:c004::62 spreadsheets.google.com
2001:4860:c004::62 spreadsheets.l.google.com
2001:4860:c004::62 writely.google.com
2001:4860:c004::62 writely.l.google.com
2001:4860:c004::62 writely-com.l.google.com
2001:4860:c004::62 writely-china.l.google.com
```

手机翻墙指南

文 / tootoo1993 silsien

被NOKIA广泛使用的Symbian S60V3系统，是一个普遍被国人认可的手机系统。很多手机软件首先出的就是S60V3的版本。虽然这个系统不算很开放，但是在S60V3系统上，翻墙的难度并不是很大。

这里主要讲讲主要Symbian S60V3系统上的翻墙方法。

Opera Mini篇

首先，我说说曾经口碑很好的Opera Mini浏览器的翻墙方法。

大家或许知道，曾经有一个Opera Mini的国际版，可以直接下载，傻瓜化的翻墙，一度让很多有特殊需要的用户很满意。

但是，最近的几个月，我国的网络封锁逐渐加剧，或许是由于政府的压力，Opera Mini国际版的服务器不再向中国IP开放，也就是说要正常连接到Opera Mini国际版的服务器需要一个非中国境内的IP。

这样，"曲线救国"的方法基本明了了。修改Opera Mini的网络连接逻辑，使之连接到一个不限制IP的中转上，即可达到翻墙的效果。

知道了方法，下面看我们要准备什么东西吧。

1、Opera Mini Server Mirror

http://opm-server-mirror.googlecode.com/files/index_2009_11_25.zip

2、Opera Mini 可改服务器版

http://www.multiupload.com/LB9CII4FAL

3、一个服务器在国外并且支持PHP的空间

（抱歉，这个我不能告诉大家如何去找到，否则说出来很快就会被封掉。请大家自行搜索免费空间的申请方法）

下面是步骤。

获得了免费空间，知道了上传的方法之后，解压缩Opera Mini Server Mirror的压缩包，获得了一个叫做"index.php"的文件。我们把它上传到那个免费空间的根目录或者是指定目录（当然最好那个目录没有其他的文件）。

接着在浏览器里访问你的免费空间，如果自动转向至Google，就代表这个空间可用。否则，再试试看另外的空间吧。

之后在手机上安装Opera Mini可改服务器版，服务器地址改成你的免费空间地址，socket地址也依葫芦画瓢填上（前面的"socket://"别改就好）。确认之后，等待初始化，接着可以试试看，是不是可以访问一些以前不能访问的网站了？

当然，这个方法可以在任何能较好支持Java的手机上使用，而且由于服务器是你一人独占的，所以速度应该很快（这个还要看服务器的速度），并且不易被封锁。Enjoy it!

UCWeb篇

请在这里下载作案工具：

http://www.coshim.com/

就拿uc_usa来说，解包后用十六进制编辑器打开主程序，服务器位置可以查找字符串”ucweb.v70.us”获得，也可以直接跳转到0914A0（99187左右）

这个网址最多24个字符，去掉前面http://和结尾:80，还剩14个，所以太长的域名不行替换（不能增加，否则uc打不开）成index.php所在地址，xxxx.com/index.php则是”http://xxxx.com:80″形式，不用加’/’

域名长度只能看人品了，太长的话申请个免费的短域名转发（未测试）

代理文件用index_2009_11_25.zip，靠下方opera地址改成uc.ucweb.com

http://opm-server-mirror.googlecode.com/files/index_2009_11_25.zip

ftp上传用bin模式

解包、打包、签名、空间，不在讨论范围内，自己解决。

版权声明

上网实用安全技术

文 / multiple1902

遵循以下原则，可以使你上网冲浪更安全。

不要使用国产安全软件，如：瑞星，金山，360，江民等。不要使用在中国市场上销售的安全软件，如卡巴斯基。这类软件可能内置后门用于有关部门搜集情报，或导致重要的隐私泄露。可以考虑的替代软件：Avast!，comodo；

经常修复系统漏洞，安装最新补丁；

尽量避免使用QQ、迅雷等软件，以免受到监视。不要使用TOM版Skype。推荐使用Gtalk；

不要使用国内电子邮件服务，如QQ邮箱、网易、雅虎（国际的也别用）、搜狐等。这些邮件服务提供商很可能会在未经允许的情况下出卖你的重要信息，其中雅虎有前科，已将多位异议人士送进监狱；放弃隐私，就是放弃电子邮件服务的底线。推荐使用Gmail；

使用Windows时，从“资源管理器”的目录树（左边）中点开U盘，常见的双击U盘图标和右键|打开都是错误的；

使用高强度的密码，经常更换，经常检查邮箱和账号的安全性；上网时不要使用“记录密码”功能；上网结束后及时清除临时文件；敏感数据删除后多次用垃圾数据覆盖；

使用公用的无线网络时不要访问敏感网站或键入敏感数据，避免被嗅探；私有无线网络尽量配置为WPA-PSK/WPA2-PSK
加密制式（目前最安全）和AES加密算法（目前无人能破解），采用静态地址分配；禁用SSID广播；

不信任CNNIC的加密证书。部分系统默认信任了CNNIC的根证书，这会导致的严重后果是中国当局可以伪造gmail等网站的加密证书，配合成熟的DNS劫持对账户进行钓鱼；请阅读CNNIC，我不信任你！——从“受信任的根证书”里赶走CNNIC；

使用Google.com，避免使用百度等国产搜索引擎查找敏感信息；不要居住在某个没有安全感的国家；移民到法治国家。

墙外优秀网站介绍

文 / freemoren multiple1902

http://www.twitter.com

twitter（非官方中文名称：推特）是最受欢迎的微博客服务。

微博客可以理解为“一句话博客”；使用它随时随地和朋友分享最新信息；可以通过电脑或手机发布。

由于Twitter是消息传播最快速和便捷的通道，它的影响力在2008年美国总统选举、伊朗绿色革命、丹佛飞机脱离跑道事件、印度孟买连环恐怖袭击事件、迈克尔·杰克逊逝世，到中央电视台新台址大火、石首事件、新疆骚乱事件等都能体现出来。在伊朗总统大选事件中，美国政府更罕有地要求Twitter延后原本已经安排好的维修工作至伊朗当地时间的凌晨时分进行，好让网站在白天能继续正常运作。不过此举被外界批评有干涉伊朗内政之嫌，美国国务院则辩称Twitter是伊朗民众在总统大选后的重要联络工具，所以才下达此要求。Twitter则表示此决定是出自其网络服务供应商，而非国务院的强制规定。

twitter不仅仅是一个网站，更是一系列的服务。一项服务很难被完全封锁。除了翻墙浏览twitter官方网站以外，身处中国大陆的用户也可以通过第三方客户端等方法绕过防火墙访问twitter服务。其中，各种网页客户端非常方便电脑和手机端的使用。如Dabr、Rabr、推特中文圈等。

他们也在使用twitter，follow他们，与他们交流：

aiww（艾未未），ranyunfei（冉云飞），williamlong（月光博客），ndzk（南都周刊），engengpu（翟明磊），songshinan（宋石男），zhiyongxu（许志永），cuiweiping（崔卫平），hecaitou（和菜头），wenyunchao（北风），NanZhou（南方周末），fzhenghu（冯正虎），lianyue（连岳），whitehouse（美国白宫），dalailama（达赖喇嘛），kaifulee（李开复），LadyGaga，zuola（周曙光），Stefsunyanzi（孙燕姿），jason5ng32（可能吧阿禅），multiple1902（我）……

Q：为什么不使用国产的新浪围脖、人民微勃？你不爱国！

A：若批评不自由，则赞美无意义。用上面或者下面说话或者不说话都是自由，但通过不许别人说话来说话，这算哪门子事？

目前大陆地区可以使用以下地址访问推特服务（PC和手机均可用）：

http://rabr.in　http://dabr.in　http://acm.buaa.edu.cn/admin/

http://www.youtube.com

YouTube设立在美国，让使用者上载观看及分享影片短片。它是一个可供网友上传、观看及分享影片的网站，至今已经成为同类型网站的翘楚，并造就多位网上名人和激发网上创作。2006年，Google公司合并YouTube。

Youtube由于世界各地网友的分享信息更加丰富，没有国内网站经历的重重审查，用户就更能接触到多样化的信息。中国互联网是开放自由的，但Youtube上有太多伤害未成年人的视频了，于是我国依法将其屏蔽。

根据维基百科介绍，2009年3月29日晚间21时左右YouTube再次被屏蔽。有外国记者向中国外交部再次询问为何再次被封时，发言人秦刚说：“上次记者会我已经回答了这个问题，我在这里再简短重申一下。中国的互联网是充分开放的，同时中国政府也要依法管理网络。至于能看什么，不能看什么，能看的就看，不能看的就别看。”

同年8月6日，《中国国防报》发表文章指责Twitter、Facebook和YouTube是“西方敌对势力”的宣传与颠覆工具，并称“要加快提高网络隔绝、屏蔽、锁定和反击网上攻击的能力”。

YouTube以视频记录的方式证明了发生过的事情，因此被封锁。

http://www.google.com

过去，经常看到有人转载百十来个网站推荐，百十来个购物店铺，或者是国外知名大学课件下载的链接，这些大家一拥而上纷纷传播之后常常什么也没留下，那些东西不会看第二遍，因为过度繁琐并且鱼龙混杂。其实对抗纷杂只有一个利器，那就是Google。如果说，这些资源推荐化繁为简，只推荐一个，那么就是Google，善用Google，从Google如何使用Google开始。

对的，我没弄错。Google.com确实在一定程度上被封锁，比如，大多数对Google.com的访问会被自动跳转到Google.cn，而Google.cn是有内容审查的。强行在Google.com上搜索敏感关键词会导致GFW高潮。

搜索引擎的任务不是查出那些政治正确的内容，而是要找的内容。

Google让人们找到要找的内容，因此被封锁。

通过http://www.google.com/ncr来访问无内容审查的Google。

http://www.gmail.com

防火防盗防中共的GMail

Gmail是Google公司在2004年4月1日发布的一个免费的电子邮件服务。在最初推出时，新用户需要现有用户的电子邮件邀请，但2007年2月7日Google宣布将Gmail的注册完全开放，不再需要现有用户的电子邮件邀请。最初推出时有1GB的储存空间，大大的提高免费信箱容量的标准。

目前Gmail用户已可以享有超过7GB的容量，并且以大约每月10MB的速度在增加。Gmail最令人称道的就是它的使用界面，不但容易使用而且速度很快，此外Gmail也是一个著名的AJAX应用。

Gmail在2009年7月7日正式取消了Beta标志。这意味着Gmail在推出5年多后终于转为正式版本。

2009年6月，Gmail将支持的最大邮件提升到25MB。

支持全程SSL加密安全连接Gmail可以让Web用户在登入和使用GMail的整个连接过程全部为HTTPS协议加密传输。方法为使用https://mail.google.com登入系统即可。要注意如使用http://www.gmail.com登入，则只会在登入时采用安全连接。但是，登入后又可以把http://改为https://安全连接，反之亦可。

界面Gmail运用AJAX，建立了一个良好的用户界面，速度上比起传统的Webmail快上很多。如果浏览器不支持AJAX，Gmail也提供没有AJAX接口的基本接口。

通讯录与邮件管理 提供强大的通讯录管理功能，可以从outlook和Yahoo等电子邮件通讯录以CSV文件导入，以及从通讯录导出形成CSV文件（目前仅英文（美国）语言版本）。并且会根据联系频率显示常用联系人和所有联系人，基于会话管理方式，所有往来于用户与联系人之间的邮件自动集成会话，邮件管理一目了然。

在线聊天2006年2月，Gmail开始了与聊天软件Google Talk的整合。用户可以WEB方式登录Gmail，利用Quick Contacts直接与Google Talk中的好友进行单对单的文字聊天，而不需要安装任何专门的辅助软件。聊天记录（包括Google Talk软件的聊天记录）可以根据用户需求，自动保存在Gmail邮箱中的交谈（Chats）文件夹里。2008年11月，Gmail新增语音和视频聊天功能。

整合Google日历，Docs & Spreadsheets当Gmail发现在邮件内容中出现日期、时间、地点等资料时，它便会在界面的右边显示月历图示，并问你是否想把这事项加进GoogleCalendar之内。Gmail附件中的.doc、.docx、.xls、.xlsx文件可以直接用Google文件打开。

http://docs.google.com

Google 文件（Google Docs）是Google公司开发的一款自由的在线文书处理，电子制表和演示程式。通过它用户能够在线创建和编辑文档，并与其它用户实时协作。2006年10月10日Google将Writely与旗下Google Spreadsheets整合为Google 文件（Google Docs & Spreadsheets），它的第三个组件，演示功能（幻灯片），在引入Tonic Systems所开发的而技术之后于2007年9月17日发布。

用户可以在Google 文件中创建文档、电子表格和演示文件，也可以通过web界面或电子邮件导入到Google 文件中。默认情况下这些文件保存在Google的服务器上，用户也可以将这些文件以多种格式（包括OpenOffice, HTML, PDF, RTF, 文本文件, Word）下载到本地电脑中。正在编辑的文件会被自动保存以防止数据丢失，编辑更新的历史也会被记录在案。为方便组织管理，文件可以存档或加上自定义的标签。

Google 文件支持多用户协同工作，此为Google文件的一大特点。文档可以同时被多个用户共享，开启和编辑。在电子制表中，用户可以设置通过电子邮件提醒任何指定区域的更改。程式支持ISO标准的OpenDocuments格式。支持流行的Office的文件格式，包括.doc，.docx，.xls和.xlsx。而对PDF格式仅zhichi上传和共享。

http://www.facebook.com

Facebook是一个社交网络服务网站。从2006年9月11日起，任何用户输入有效电子邮件地址和自己的年龄段，即可加入。用户可以加好友，发消息，并创建个人页面使朋友了解自己。此外，用户可以选择加入一个或以上网络，例如中学的、公司的、或地区的。网站的名字Facebook来自传统的纸质「花名册」。通常美国的大学和预科学校把这种印有学校社区所有成员的“花名册”发放给新入学或入职的学生和教职员，协助大家认识学校内其他成员。

http://www.wikipedia.org

维基百科

维基百科是一部在线的百科全书。

维基百科是一部内容开放的百科全书，内容开放的材料允许任何第三方不受限制地复制、修改，它方便不同行业的人士寻找知识，而使用者也可以不断增加自己的知识从而充实自己。“维基”的最大意义在于赋予了普通人对知识的定义权和诠释权。而维基的存在使普及事件知识、串联信息变得更加容易。

2004年6月（1989年六四事件15周年）以来维基百科被中国大陆多次封锁。2008年奥运会开始至今，维基百科被有限解禁。部分内容如“中国共产党”、“江泽民”和政治内容如“六四天安门事件”、“法轮功”等内容依然无法访问。

维基百科使人有机会接触到中立的信息，因此被封锁。

http://www.bullogger.com

牛博国际

老罗（罗永浩）主办的博客社区，文章尺度较大且几乎没有内容审查。冉云飞、柴静、韩寒、陈晓卿、连岳、艾未未、崔卫平等在此开博。

其墙内镜像为嫣部落：http://www.bullock.cn，无政治内容。

Google Reader
https://www.google.com/reader

Google阅读器（Google Reader）是Google旗下一个基于网络的聚合器，能在线或者离线阅读Atom和RSS。Google Reader使阅读博客变得简单轻松，一个个写字的人或许为你的生活找到新的敞口。

Itunes U
http://www.apple.com/education/itunes-u/

Itunes U基于苹果公司出品的媒体播放器程序，它是一个强大的分享平台，从演讲到语言课程，从电影到实验课，从有声书到校园游览，Itunes U把教育资源以创新的方式送到学生手中。在这里，可以体会许多欧美大学的课堂，演讲，研讨会，只要你愿意去发掘。当然，很多大学或机构（如TTC）都在网上提供公开课（open course），有的甚至配有讲义及文本，所以只要善于搜索，你依旧可以在互联网世界中重新步入课堂。

gigapedia
http://gigapedia.com/

维基百科也许只能帮你解决入门知识，真正想要深入了解一个事物，书籍是更好的手段。这个网站含有大量电子书的文本分享，特别是英文书。

IMDb
http://www.imdb.com/

互联网电影数据库（Internet Movie Database，简称IMDb）是一个关于电影演员、电影、电视节目、电视艺人、电子游戏和电影制作小组的在线数据库。IMDb开办于1990年10月17日，从1998年开始成为亚马逊公司旗下的网站，在2005年10月17日时，IMDb欢庆了他们15周年的纪念。截至2009年7月4日，IMDb收录了共1,456,511部作品以及3,047,419名人物的资料。IMDB成为众多电影电视爱好者大本营，由于数据样本大，其评分和评论功为普通人提供了有效的“观影指南”。

IMDb不只是电影和电子游戏等的数据库，还提供每日更新的电影电视新闻，以及为不同电影活动比如奥斯卡奖推出特别报道。IMDb的论坛也十分活跃，除每个数据库条目都有留言板之外，还有关于多种多样的主题的各种综合讨论版。IMDb扩展出来的姐妹站IMDbPro为专业人士提供额外的信息，如电影业界人士的联系方式，电影活动日期表等等。

致谢

@Kristy_xiao / 超級小饅頭
@freemoren / FreeMoreNews 自曲新闻 / freemorenews.com
huxim
@silsien / 西瓜君
Allen
@secretaryzhang / 张书记
@ _J_SMITH / J.Smith / twitbrowser.net
@tootoo1993 / tootoo1993 / tootoo1993.blogspot.com
g5v991x
萧易寒
@jiehanzheng / Jiehan Zheng
阮一峰
@ccp0101
@newsinchina / 牧师
@yww1218 / ViviShineR
@eXrld
@gongchen713 / gongchen713
zjsz007

媒体合作

日人民报	http://www.people.com.cn/
新华网	http://www.xinhuanet.com/
真理部	http://www.scio.gov.cn/
举报中心	http://net.china.cn/chinese/index.htm
新闻出版总署	http://www.gapp.gov.cn/
中国扫黄打非网	http://www.shdf.gov.cn/
中国文明网	http://www.wenming.cn/
中华人民共和国文化部	http://www.ccnt.gov.cn/
中国中央电视台	http://www.ccav.com/

关于本书

本书的勘误、补充以及后续更新将会发表在这里：

http://docs.google.com/View?id=dgtbmwd6_934gg99v6g4

如果不出意外，本书将每隔一个月发布一个新版本，加入新的内容，去除过时的和不准确的内容。请关注以上地址。

本书的联系邮箱为

GFWMANUAL@gmail.com

，

意见建议反馈、投稿、商业合作、索取手册、问询皆使用以上地址，我将尽量阅读和回复每一封来信。

本书另有正体中文版本。

战争即和平

自由即奴役

无知即力量

——乔治·奥威尔《一九八四》

关于编者

multiple1902，南京人，在西安就读。大一金牛座男生，毕业于南京师大附中。未婚且单身。

1999年起接触互联网，信息业界资深人士。目前就读于西安交通大学计算机科学与技术专业，研究方向为自然语言处理和信息安全。

邮箱 multiple1902@gmail.com
推特 @multiple1902