如何突破网络审查

Published : 2011-10-28

Table of Contents

INTRODUCTION

简介

1948年12月10日，《世界人权宣言》的通过开启了一个新的时代。黎巴嫩学者查理斯·哈比卜·马利克向参会代表做了如下描述：

> 联合国的每个会员均已庄严承诺实现对人权的尊重和遵守。但是，无论是在《宪章》里还是在其他任何国际条约中，这些权利究竟明确地是哪些我们之前却从未讲过。这是人权和基本自由的原则第一次权威性地和精确细致地被阐述出来。现在我知道了我的政府承诺促进、实现和遵守的是什么。……我可以鼓动反对我的政府，并且如果她不履行她的承诺，我将得到和感受到整个世界的精神支持。

《世界人权宣言》在第19条所述的基本权利之一就是言论自由的权利：

> 每个人都有见解和表达自由的权利；这个权利包括坚持主张不受干涉及通过任一媒介且无论国界寻求、接受和传递信息和观点的自由。

当这些话六十年前被写入时，没人想象到全球互联网现象将怎样扩大人们“寻求、接受和传递信息”的能力，不仅跨越了边界，而且以惊人的速度和可复制、编辑、处理、重组的形式，通过与1948年可用的传播媒介根本不同的方式与或大或小的观众共享。

比想象中更多的信息在更多的地方

互联网上的东西及其适用的地方在过去几年中难以置信的增长产生了这样的效果，使得人类知识和活动中难以想象的庞大部分突然出现在了意想不到的地方：一个偏僻小山村里的医院、你12岁孩子的卧室、你向你最亲密的同事展示将使你超越竞争对手的新产品设计的会议室、你祖母的房子。

在所有这些地方，与世界连接的可能性开辟了许多改善人们生活的极好机会。当你在度假时得了一种罕见的疾病，偏僻山村的医院可通过将你的检测结果发给首都甚至另一个国家的医疗专家来挽救你的生命；你12岁的孩子可以研究她的学校项目或与其他国家的孩子交朋友；你可以同时向分布全世界的办事处的高层管理者展示你的新产品设计，他们可以帮助你改进它；你的祖母可以通过电子邮件及时发送给你她特殊的苹果派食谱，以便你今晚烤它做餐后甜点。

但是，互联网并不只包含相关和有用的教育信息、友谊和苹果派。就像世界本身一样，它庞大、复杂，且经常吓人。它对恶意、贪婪、不择手段、不诚实或仅粗鲁的人可用就像对你和你12岁的孩子及你的祖母一样。

并不是每个人都想让整个世界加入

随着互联网上反映出的人性所有的最好面和最坏面，以及某些种类的欺诈和骚扰通过技术更容易实施，任何人都不会感到惊讶互联网在增长的同时伴随着控制人们如何使用它的努力。这些努力有很多不同的动机。目标包括：

- 保护孩子远离被认为不适当的资料，或者限制他们与可能伤害他们的人接触。
- 减少通过电子邮件或在网上的不必要的商业邀请的泛滥。
- 控制任一使用者在同一时间能访问的数据流的大小。
- 防止雇员分享被认为是其雇主财产的信息，或者防止其为个人活动利用其工作时间或雇主的技术资源。
- 限制对在特定管辖区内（如一个国家或一个类似学校的组织）禁止或规管的资料或在线活动的访问，如明显的色情或暴力资料、药物或酒精、赌博和卖淫，以及被认为是危险的有关宗教、政治或者其他团体或观点的信息。

其中一些关注点包括允许人们控制他们自己的互联网行为（如让人们使用垃圾邮件过滤工具阻止垃圾邮件被投递到他们自己的电子邮件账户），但另一些关注点则包括限制他人能怎样使用互联网以及他们能和不能访问什么。当访问被限的人不同意这种封锁是合适的或符合他们利益的时，后一种情况导致了重大的冲突和分歧。

谁在过滤或封锁互联网？

尝试限制特定人使用互联网的人士和机构的种类就如同其目的一样多样。他们包括父母、学校、商业公司、网吧经营者或互联网服务提供商（ISPs），以及各级政府。

互联网控制的极端情形是当一个国家的政府尝试限制其所有国民使用互联网访问所有种类的信息或与外部世界自由共享信息的活动。网络公开倡议（http://opennet.net）的研究已列明了国家对其公民上网过滤和封锁的许多方式。这包括实行无孔不入的过滤政策的国家，其被发现定期封锁对挑战现状或者被视为有威胁的或不良的人权组织、新闻、博客和网络服务的访问。其他国家封锁对某一种互联网内容的访问，或者间歇性地封锁特定的网站或网络服务以配合战略事件，比如选举或公共示威。即使一般对言论自由有力保护的国家有时也尝试限制或监控与抑制色情、所谓仇恨言论、恐怖主义和其他犯罪活动、泄露军事或外交通信、违反著作权法有关的互联网使用。

过滤导致监控

任一这些官方或民间团体也可能使用各种技术监控他们关心的人的互联网活动，从而确保他们限制的尝试是有效的。这个范围从父母透过孩子的肩膀或查看孩子电脑上访问了什么网站，到公司监控雇员的电子邮件，到法律执行机构从互联网服务提供商处要求信息或者甚而查封你家中的电脑以寻找你参与了“不良”活动的证据。

何时审查？

根据谁限制对互联网的访问和/或监控其使用，以及访问被限的人的判断，几乎任一这些目标和任一用来实现其的方法都可能被视为是合法必要的或是不可接受的审查和对基本人权的侵犯。一个十几岁的男孩，他的学校封锁其访问他最喜欢的网络游戏或像Facebook类的社交网站，他感觉他的个人自由被削减了，丝毫不亚于其政府阻止其阅读有关政治反对派的网络报纸的那些人。

到底是谁封锁了我对互联网的访问？

谁能在任何给定的国家内在任何给定的电脑上限制访问取决于谁有能力控制技术基础设施的特定部分。这种控制可能基于合法建立的关系或要求，或者基于政府或其他机构的能力，从而迫使合法控制技术基础设施的主体依从封锁、过滤或收集信息的要求。国际互联网基础设施的许多部分是由政府或政府控制的机构控制的，他们可能按照或不按照当地的法律主张控制。

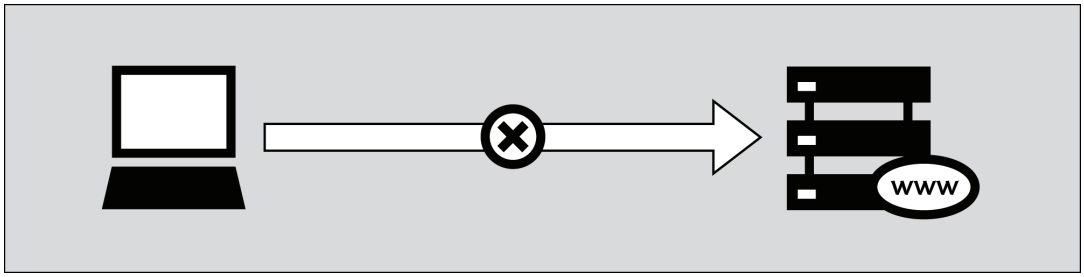
过滤或封锁部分互联网可能出重手或者很轻，可能明确规定或者几乎看不见。一些国家公开承认封锁并发布封锁标准，同时将被封锁的网站代之以说明信息。其他国家没有明确的标准，有时依靠非正式的理解和不确定地迫使互联网服务提供商进行过滤。在一些地方，过滤被伪装成技术故障，且当封锁是故意时政府并不公开承担责任或确认。即使是在同一国家并遵守相同法规的不同网络运营商也可能会因为谨慎、技术无知或商业竞争而采用完全不同的方式执行过滤。

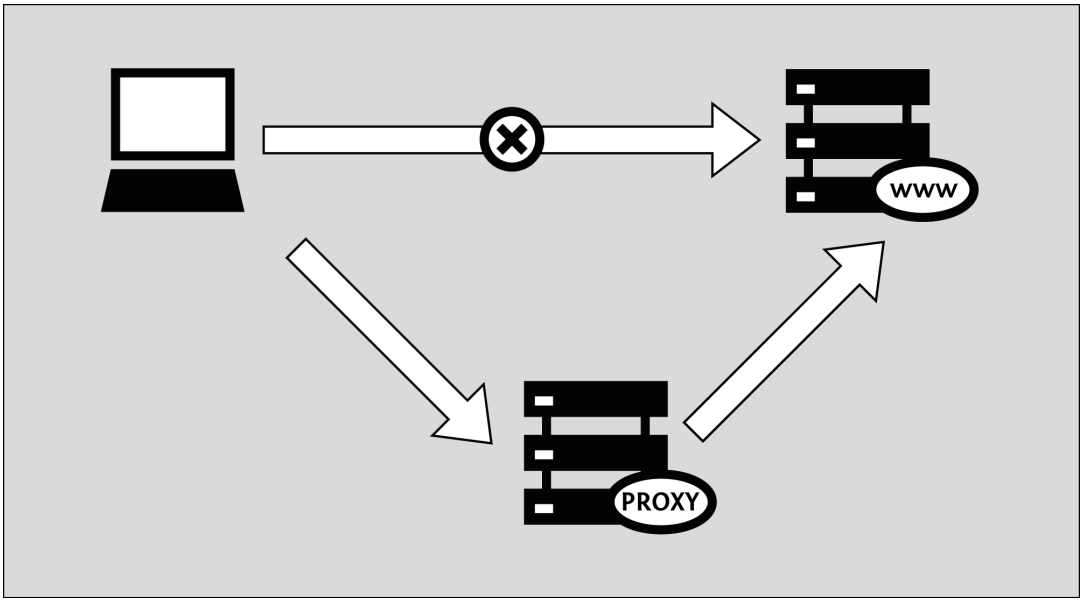
在从个人到国家各级可能的过滤中，封锁恰被认为不良的访问的技术困难可能有意想不到的且往往是可笑的结果。意在封锁色情资料的“家庭友善”过滤阻止了对有用健康信息的访问。封锁垃圾邮件的尝试可能过滤掉重要的商业信函。封锁对特定新闻网站访问的尝试同样可能切断教育资源。

存在哪些方法绕过过滤？

就如同一些个人、企业和政府将互联网视为危险信息的来源之一而必须受到控制一样，许多个人和团体正努力确保互联网及其上的信息能被每个需要它的人自由使用。这些人像寻求控制互联网的那些人一样有许多不同的动机。然而，对那些互联网访问被限制和想要做一些事情的人来说，这些工具是否由一些想要和女朋友聊天、写一份政治宣言或发送垃圾邮件的人开发可能并不重要。有来自商业、非营利和志愿者团体的大量资源致力于开发工具和技术绕过互联网审查，产生了大量绕过互联网过滤的方法。总的来说，这些被称为绕行方法，且其范围能从简单的解决方法、保护途径到复杂的计算机程序。然而，它们几乎都以大致相同的方式工作。它们指示你的网络浏览器通过一个被称为代理的中介计算机进行迂回，其：

- 被设置在不受互联网审查的某处
- 并未封锁你的位置
- 知道如何为像你一样的用户获取和回馈内容





什么是使用绕行工具的风险？

只有你，想绕过你的网络访问限制的人，能决定访问你想要的信息是否有重大风险，也只有你能觉得受益是否超过风险。可能没有法律明确地禁止你想要的信息或者访问它这一行为。另一方面，缺乏法律制裁并不意味你没有冒着其他后果的风险，如骚扰、失去工作或者更坏的结果。

下面的章节讨论互联网是如何工作的，描述了各种形式的网络审查，并详细说明大量可以帮助你绕开这些言论自由障碍物的工具和技术。关于数字隐私和安全的首要问题的思考贯穿全书，从基本开始，然后在结束前，为那些想帮助他人绕过网络审查的网站管理员和电脑专家用一个简短的章节，讨论一些复杂的话题。

关于这本指南

《绕过网络审查》这本指南介绍了这一话题，并解释了一些用来绕过网络审查的最常用的软件和方法。还有关于在绕开审查时避免监视和其它探测手段的信息，然而它本身是一个广博的主题，所以我们仅在它直接与审查问题

全面讨论保持匿名和防止探测内容或活动已超出本书的范畴。

这本书是如何写就的以及谁是作者

这本指南的第一版刊载的内容主要在2008年11月Book Sprint写就。八个人在密集的五天内紧锣密鼓共同工作创造本书。

你正在阅读的这本指南的更新版编辑于2011年初期在德国举行的第二届

Book Sprint。这一次，有十一人在密集的五天内紧锣密鼓共同工作。

这本书是"活"的课程文档，在网络上免费，你也可以编辑和改进它。

除了在两届Book Sprint写就的材料外，还有材料来源于早先的出版物。包括来自于下列人士的稿件：

- Ronald Deibert
- Ethan Zuckerman
- Roger Dingledine
- Nart Villeneuve
- Steven Murdoch
- Ross Anderson
- Freerk Ohling
- Frontline Defenders
- 哈佛大学Berkman互联网和社会中心的Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, 以及John Palfrey

这些作者友善地同意我们在GPL授权协议环境下使用这些材料。

这本指南已在FLOSS Manuals上写就。按照下列步骤改进这本指南：

1.注册

在FLOSS Manuals上注册：http://booki.flossmanuals.net/

2.撰稿！

选择这本指南（http://en.flossmanuals.net/bypassing-censorship/ch002_about-this-manual/edit）和其中一章进行撰稿。

如果你需要就如何撰稿向我们提问，加入下面所列的聊天室并向我们提问！

我们期待你的撰稿！

欲知更多关于使用FLOSS Manuals的信息，你可能也希望阅读我们的指南：

http://booki.flossmanuals.net/

3.聊天

与我们交谈是个好主意，这样我们能够协调所有的撰稿。我们有一个使用IRC的聊天室。如果你知道怎样使用 IRC，你可以连接下列的：

server: irc.freenode.net
channel: #booksprint

如果你不知道怎么使用IRC，在你的浏览器访问下列基于网页的聊天软件：

http://irc.flossmanuals.net/

关于如何使用这些基于网页的聊天软件的信息在这：

http://en.flossmanuals.net/FLOSSManuals/IRC

4.邮件列表

讨论所有关于FLOSS Manuals的事宜，加入我们的邮件列表：
http://lists.flossmanuals.net/listinfo.cgi/discuss-flossmanuals.net

QUICK START

快速入门

当人们或团体控制互联网阻止网民访问特定内容或服务时，互联网是被审查的。

网络审查有多种形式。例如，政府可能封锁普通的电子邮件服务，试图迫使公民使用政府的电子邮件，它易于被监视、过滤或者关闭。父母可以控制他们的未成年的孩子访问的内容。大学可能阻止学生在图书馆访问Facebook。网吧的所有者可能封锁点对点文件分享服务。独裁政府可能审查关于侵犯人权或上次被盗的选举的报道。对这些审查形式的合法或非法，人们有广泛不同的观点。

绕行

绕行是绕过互联网审查的活动。有很多种方法可以做到，但是几乎所有的绕行工具几乎以同样的方式工作。他们命令你的浏览器通过一个中介电脑绕道而行，被叫做代理（proxy），它:

- 位于没有互联网审查的地方
- 没有被你所在地封锁
- 知道如何为你这样的用户获取和返回内容。

安全和匿名

记住没有工具对你的情况是完美的解决方案。不同种类的工具提供不同程度的安全性，但是技术不能消除你反对当权者所承担的身体危险。这本书有几章解释互联网是如何工作的，它对理解在绕行审查时如何更安全是重要的。

存在很多不同

有些工具只能在你所用的浏览器使用，而其他的可能立刻就可在数个程序使用。这些程序可能需要配置通过代理发送网络流量。有一点额外的耐心，你不用在你电脑上安装任何软件就可以做所有这些。注意你的获取网页的工具可能不能准确地显示网页。

一些工具为了隐瞒你正在访问被封锁的服务的事实，使用超过一台中介电脑。这也可以对工具的提供者隐藏你的活动，这对匿名非常重要。一个工具可能有聪明的方法知道可以连接的替代代理，如果你正在使用的自身被审查。理想地，为保护它免受窥探，请求、获取和发送所产生的流量被加密。对于面对互联网审查访问或者制作内容来说，就你特定的处境选择正确的工具几乎肯定不是你将要做的最重要的决定。尽管关于这些事提供具体的建议困难，花点时间思考下背景是重要的，比如：

- 你打算怎样、什么时候和在哪使用这些工具
- 谁可能想阻止你做这些工具可以让你做的事
- 这些组织和个体反对这些使用有多强烈
- 他们掌握什么资源用来帮助他们实现自己想要的结果，直至暴力。

访问大多数被封锁的网站不使用另外的软件

最基本的绕行工具是网页代理。虽然它不是你最理想的解决方案有众多理由，就非常基本的绕行目的而言，它经常是一个好的起点。假设它还没有在你的所在地被封锁，访问以下网址：
http://sesaweenglishforum.net

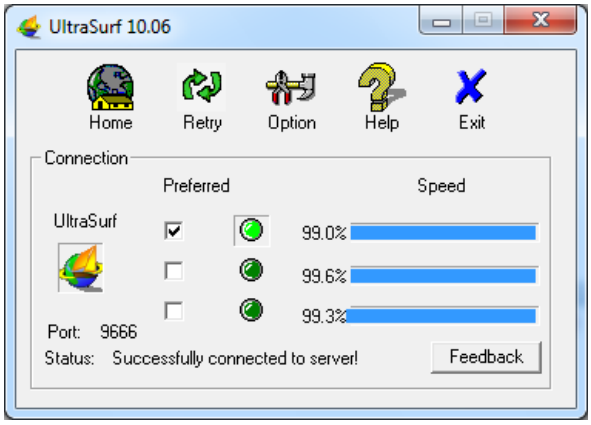
接受服务条款，在蓝色的地址栏输入你想访问的被封锁网站的地址：

按回车（Enter）或点击GO, 如果成功导航到请求的网站，那么它是可行的。如果上面的连接不起作用，你需要寻找一个替代绕行方法。这本书的网页代理（Web proxy）和赛风（Psiphon） 章节提供一些寻找网页代理的建议和大量关于一旦你使用它你应不应该愿意使用它的决定。

如果你需要访问特别复杂的网站Facebook的全部功能，你可能需要使用一个简单的、可安装的工具如Ultrasurf ，而不是网页代理。如果你想要或者需要一个解决方案，它通过严格安全测试且能帮助你保持匿名，不需要你知道谁真正管理服务自身，你应该使用Tor。如果你需要访问被过滤的网络资源而不仅仅是网站，如被封锁的即时通信平台或者被过滤的邮件服务器（被Mozilla Thunderbird 或者Microsoft Outlook等程序使用），你可以尝试HotSpot Shield 或者其他的OpenVPN 服务。所有的这些工具，在这本书的后面有自己的章节，简要描述如下。

访问所有被封锁的网站和平台

Ultrasurf 是一个适合Windows操作系统的免费的代理工具，可以从 http://www.ultrareach.com/, http://www.ultrareach.net/ 或者http://www.wujie.net/下载。下载的压缩文件需要解压，右击并选择“全部解压”（ "Extract All..."）。得到的.exe文件可以不需要安装直接启动（即使在网吧用USB闪盘）

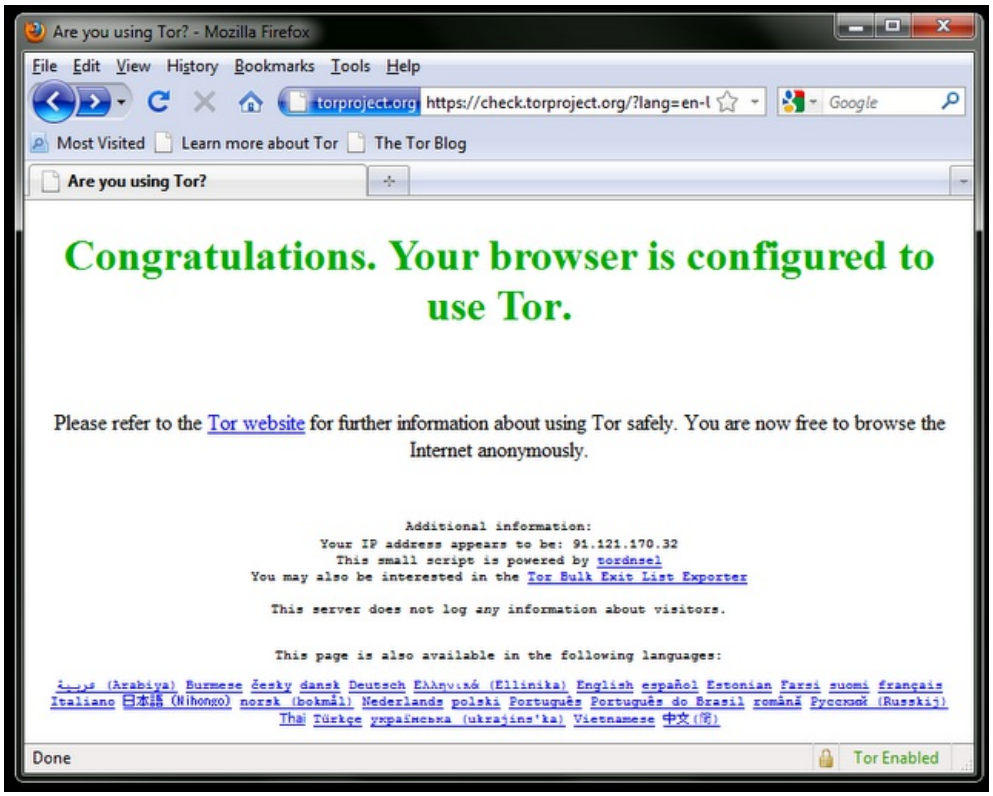


Ultrasurf自动连接，将启动一个新的Internet Explorer浏览器窗口，你可以使用它打开被封锁的网站。

绕开过滤器和在网上保持匿名

Tor是一个复杂的代理服务器网络。它是免费的开源软件，主要是用来允许匿名网络浏览，但它也是一个很好的审查绕行工具。支持Windows、Mac OS X 或者GNU/Linux 的 Tor 浏览器组件可以在https://www.torproject.org/download/download.html.en上下载。如果torproject.org网站被封锁，你可以通过在喜欢的搜索引擎搜索"tor mirror"，或者在邮件的正文写有“"help"，发送一封电子邮件到gettor@torproject.org，找到其他的下载地址。

当你点击下载文件，它将解压到你选择保存的位置。也可以是USB闪盘，你可以在网吧使用。你然后可以点击“启动Tor浏览器”（"Start Tor Browser"），启动Tor（确保你已关掉已经在运行的Tor或Firefox）。几秒钟后，Tor自动启动一个特别版本的Firefox浏览器，打开一个测试网站。如果你看到绿色的信息”恭喜你”(“Congratulations”)。你的浏览器已经配置好使用Tor。你然后可以使用这个窗口打开被封锁的网站。



使用一个安全的隧道传输所有网络流量

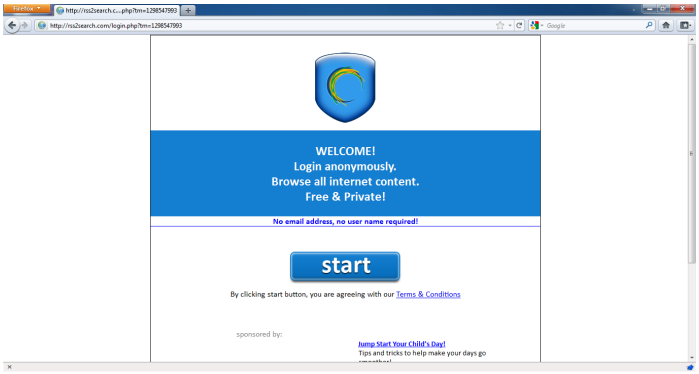
如果你想使用网站之外的互联网服务，如通过电子邮件客户端如Outlook或Thunderbird使用电子邮件，一个容易又安全的方法就是使用虚拟专用网络（virtual private network (VPN)）。VPN将在你自己和其他的电脑间加密传输所有的网络流量，所以不仅可以使你所有的不同种类的流量看起来和窃听者一样，而且加密使得它对所有沿途的人来说不可读取。当连接上VPN，你的互联网服务提供商看不到你的内容，但是它能看到你正在连接VPN。因为许多跨国公司使用VPN技术安全连接它们的远程办公室，VPN技术不可能总体上被封锁。

Hotspot Shield

一个简单的开始使用VPNs的方法是使用Hotspot Shield 。Hotspot Shield 是一个可以在Microsoft Windows 和Mac OS X操作系统使用的免费的（但是是商业的）VPN解决方案。

安装Hotspot Shield前你须从https://www.hotspotshield.com下载软件。文件6MB大，所以使用慢的拨号上网连接下载可能需要花费25分钟或更多时间。 安装，请双击下载好的文件，按照安装向导提示的步骤安装。

一旦安装完成后，从桌面上的"Hotspot Shield Launch"图标或通过"程序（Programs ）› Hotspot Shield"启动Hotspot Shield。一个窗口将打开，是一个显示不同连接尝试阶段如“正在验证”（"Authenticating"）和“正在分配IP地址”（"Assigning IP address"）的状态页面。连接好后，Hotspot Shield把你转到欢迎页面。点击“启动“（"start" ）开始冲浪。



退出Hotspot Shield, 右击图标，选择"Disconnect/OFF"。

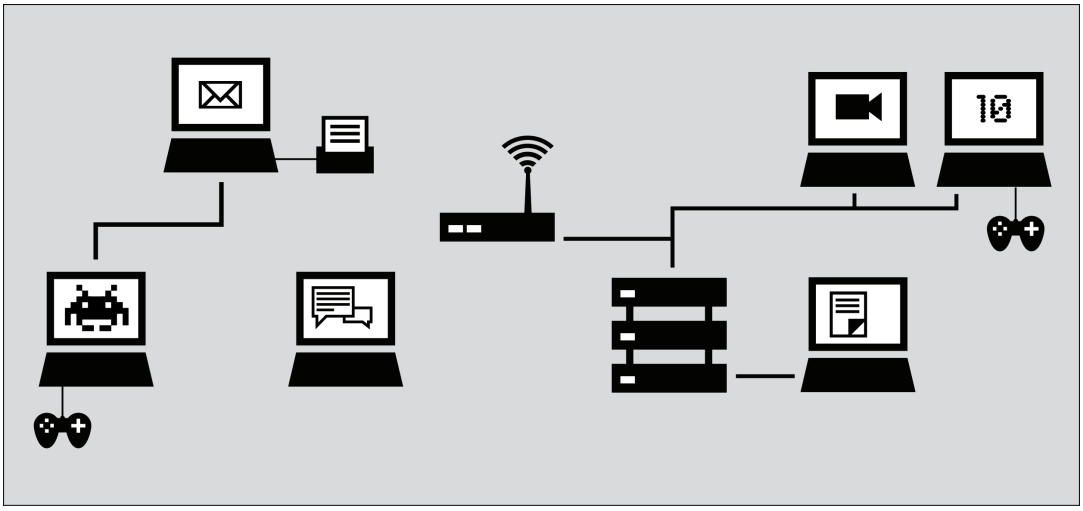
BACKGROUND

互联网如何工作

想象一下，一组人决定要通过连接其电脑和在这些电脑间发送信息来共享其电脑上的信息。他们努力的结果是一组能通过计算机网络相互连接的设备。当然，如果该网络能与其他网络，从而与其他计算机和网络用户相连接，那么它将更有价值和用处。这种电子化连接和共享信息的简单愿望现今在全球互联网上实现了。随着互联网的迅速发展，其互联的复杂性也已增加，且互联网已真正从大量网络的互联中建立起来了。

互联网的基本任务可以描述为便利数字信息使用一个合适的路径和一种适当的传输模式从其来源到目的地的传输。

本地的计算机网络，被称为本地局域网或LANs，将同一物理位置的许多计算机和其他设备与彼此物理连接起来。他们还可以通过被称为路由器的设备与其他网络相连接，而路由器管理着网络间的信息流。一个局域网中的电脑可以出于类似分享文件和打印机或玩多玩家网络视频游戏的目的而直接相互连接。即使不与外部世界相连接，局域网也是十分有用的，但当它与外部世界相连接时，其显然会变得更加有用。



今天的互联网是一个由这种本地计算机网络与诸如大学和企业网络的大型网络以及虚拟主机服务提供商网络组成的分散的全球性网络。

安排网络之间这些相互联系的组织被称为互联网服务提供商或ISPs。一个互联网服务提供商的职责是将数据传送到适当的位置，往往是通过转发数据到另一个更靠近数据最终目的地的路由器（被称为“下一跳”）。通常情况下，下一跳实际上属于不同的互联网服务提供商。

为了做到这一点，互联网服务提供商可能从一个如国家级提供商般的更大的互联网服务提供商处购买其自己的互联网通路。（某些国家只有一个单独的国家级提供商，可能是政府经营的或政府下属的，而其他国家则有很多，可能是竞争性的私营电信公司。）国家级提供商同样可能收到其来自跨国公司之一的连接，这些跨国公司管理和操作常被称为主干网的服务器和连接。

主干网由主要网络设备安装及它们之间通过光缆和卫星的全球连接组成。这些连接使不同国家和大洲的互联网用户之间的通讯成为可能。通过路由器与该主干网连接的国家和国际提供商有时被称为网关，其是允许不同网络与彼此沟通的连线。这些网关，就像其他路由器一样，可能是互联网活动被监测或控制的一点。

建设互联网

互联网的创造者普遍认为只有一个互联网，其是全球性的，且在假设计算机的主人想要发生时，其应允许世界上任何地方的任何两台计算机与彼此直接联系。

在1996年的一份备忘录中，后来成为互联网架构委员会主席的布莱恩·卡彭特写道：

一般而言，“互联网工程”团体认为目标是连接。……网络的增长似乎表明连接本身就是一种奖赏，且其比任何个人应用都要更有价值。

仍有大批的互联网先驱和早期采用者拥护全球互联互通、开放标准和自由访问信息的理想，虽然这些理想常与政治和商业利益相冲突，而并不常直接影响日常的经营活动和互联网各个部分的政策。

互联网的创始人们也创造了并继续创造旨在使他人也更容易地创造其自己的网络和加入彼此的标准。了解互联网标准可帮助弄清互联网是如何工作的，以及网络站点和服务是如何变成可访问或不可访问的。

连接设备的标准

如今，大多数局域网通过有线以太网或无线以太网（802.11或Wi-Fi）技术建立。所有这些组成互联网使用共同技术标准或互联网协议的互联（局域网和其他设备）使计算机找到彼此并与彼此交流。通常情况下，该互联使用私人所有的设备和设施，且在以营利为目的的基础上运作。在某些管辖区，互联网连接由法律广泛规定。在其他国家或地区，则很少或没有规定。

统一全球互联网上所有设备的最基本的标准被称为互联网协议（IP）。

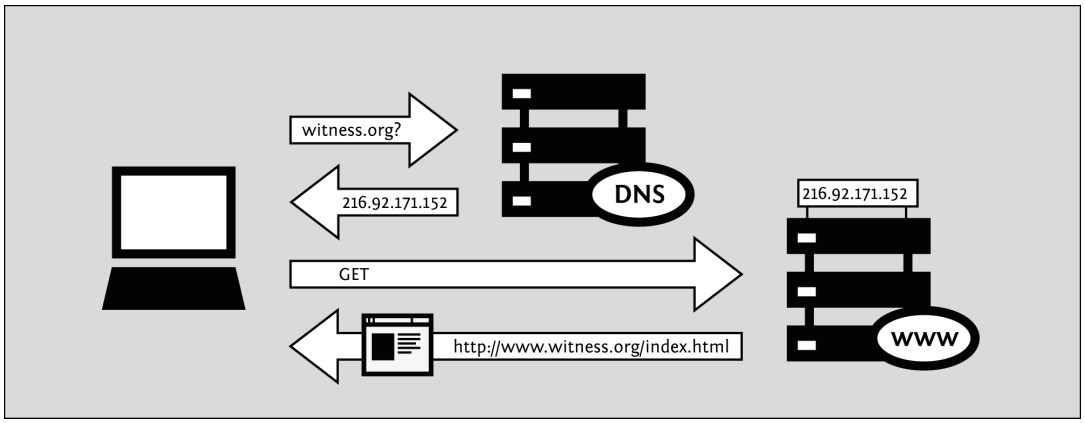
识别网络设备的标准

当你的电脑连接到互联网时，它通常会被分配给一个数字IP地址。就像一个邮政地址般，该IP地址唯一标识互联网上单一的一台计算机。然而，又不像邮政地址，一个IP地址（尤其是个人电脑设备）并不一定永久与一台特定的计算机相关联。因此，当你的电脑从互联网上断开并在稍后时间重新连接，其可能收到一个不同的（但唯一的）IP地址。目前普遍使用的IP协议版本是IPV4。在IPV4协议中，一个IP地址以用点分隔的0–255范围内的四个数字写出（如207.123.209.9）。

域名和IP地址

所有的互联网服务器，如那些主机网站的服务器，也拥有IP地址。例如，www.witness.org的IP地址是216.92.171.152。由于记忆IP地址是繁琐的，且IP地址可能随着时间而改变，特定的系统在适当的地方以使你能更容易地在互联网上达到你的目的地。这个系统就是域名系统（DNS），在此，一组计算机专用于为你的电脑提供已与人类难忘的“名字”相关的IP地址的服务。

例如，想要访问证人网站，你可以键入www.witness.org地址，即一个域名，从而代替216.92.171.152。然后，你的电脑向一个DNS服务器发送有该名称的信息。当该DNS服务器将该域名转换成IP地址后，其与你的计算机分享该信息。该系统使网页浏览和其他互联网应用对人来说更人性化，对计算机来说更有利于计算机。



从数学上讲，IPV4允许一批大约4.2亿不同的计算机连接到互联网。同样也有技术使多台计算机共享一个IP地址。尽管这样，可用地址池或多或少在2011年初将被耗尽。因此，IPV6协议已被制定，其有一个更大的可能唯一地址的资源库。IPV6地址比传统的IPV4地址更长，且更难记忆。IPV6地址的一个例子是：

2001:0db8:85a3:0000:0000:8a2e:0370:7334。

虽然2011年少于1%的互联网用户使用IPV6协议，但这种情况在不久的将来可能会发生巨大的变化。

通过网络发送信息的协议

你使用互联网交换的信息可以有多种形式：

- 发送给你表亲的电子邮件
- 一个事件的图片或视频
- 联系方式的资料库
- 包含一组指令的档案
- 包含一份关于敏感话题报告的文件
- 教一门技能的计算机程序。

有各种各样的互联网软件根据特定协议去配合妥善处理各种形式的信息，比如：

• 通过简单邮件传输协议（SMTP）的电子邮件

• 通过可扩展消息在线协议（XMPP）的即时消息

• 通过文件传输协议（FTP）的文件共享

• 通过比特流（BitTorrent）协议的点对点文件共享

• 通过网络新闻传输协议（NNTP）的网络新闻组

• 协议的结合：使用互联网语音协议（VoIP）的语音通讯，会话发起协议（SIP）和实时传输协议（RTP）

网页

虽然很多人互换着使用术语“互联网”和“网页”，但实际上网页仅指使用互联网交流的一种方式。当你访问网页时，你使用一种被称为网页浏览器的软件，比如火狐、谷歌浏览器、Opera或者微软IE浏览器。网页运行其上的协议被称为超文本传输协议或HTTP。你可能还听说过HTTPS，其是HTTP的安全版，使用传输层安全（TLS）加密以保护你的通讯。

追随你在互联网上的信息——旅行

让我们追随从你的家庭电脑访问一个网站这一例子。

连接互联网

要将你的电脑连接到互联网，你可能需要一些额外的设备以首先连接到你的互联网服务提供商的网络，比如一个调制解调器或一个路由器。通常情况下，最终用户的计算机或家庭网络通过下列几种技术之一与互联网服务提供商相连接。

• 电话调制解调器（“拨号”），以打电话的形式通过电话线发送互联网数据

• 数字用户线路（DSL），一种更有效和高速的在短距离间通过电话线发送数据的方式

• 电缆调制解调器（或“有线互联网”），通过有线电视公司的同轴电缆发送互联网数据

• 光纤电缆，尤其是在发达国家人口密集的地区

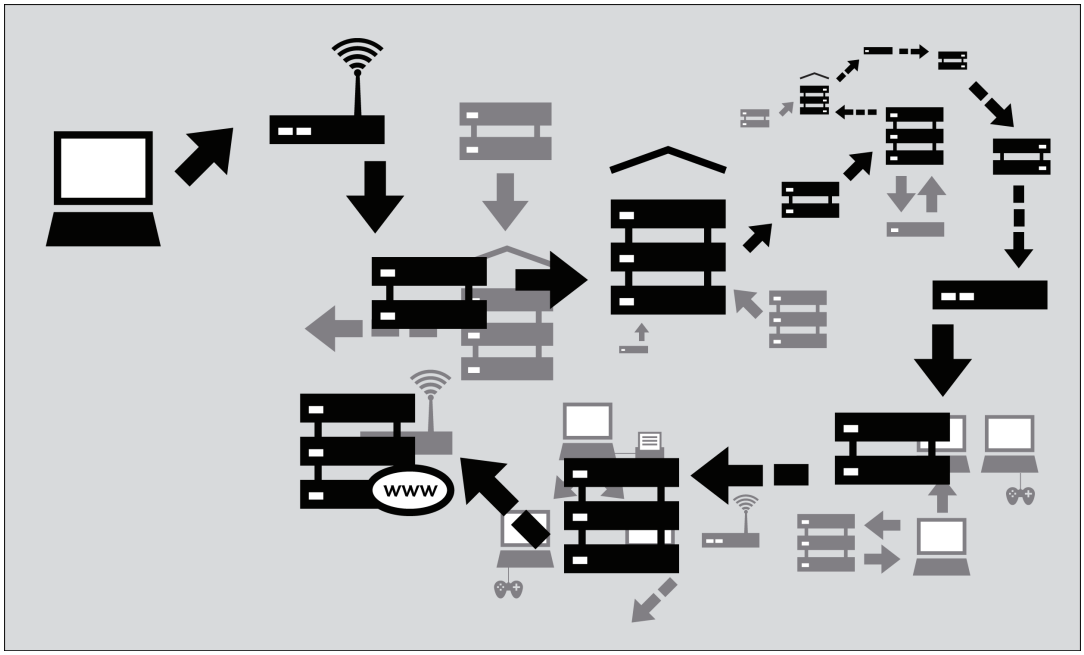
• 广域固定无线链路，尤其是在农村地区

• 通过移动电话网络的数据服务

浏览网站

1. 你输入https://security.ngoinabox.org/。计算机将域名“security.ngoinabox.org”发送给一个指定的域名服务器，其会返回一个包含提供给盒网络服务器（目前是64.150.181.101）中战略技术安全的IP地址的信息。
2. 然后，浏览器发送一个与该IP地址相连接的请求。
3. 该请求经过一系列的路由器，每一个都将请求的副本转发到更接近目的地的路由器，直到其到达找到所需特定计算机的路由器。
4. 该计算机将信息发回给你，允许你的浏览器发送完整的统一资源定位符（URL）和接收数据，从而显示页面。

从网站发给你的信息穿越了其他设备（计算机或路由器）。沿路径的每一个这样的设备可以被称为一“跃点”；跃点数即你的信息沿其路径接触的计算机或路由器的数量，且往往在5到30之间。



为什么这很重要

通常情况下所有这些复杂过程都是被隐藏的，且你为了找到你所需的信息并不需要了解这些。然而，当有人或组织试图干扰系统运作限制你对信息的访问时，你使用互联网的能力可能受到限制。在这种情况下，了解他们做了什么以干扰你的访问可以变得极其有意义。

想一想防火墙，其是有意阻止一台计算机和另一台之间某些种类交流的设备。防火墙帮助网络所有者执行有关何种网络交流和使用被允许的政策。最初，防火墙的使用被视为一种计算机安全措施，因为其可以帮助击退针对无意错误配置和易受感染计算机的电子攻击。但是，防火墙已被用于更广泛的目的和执行远超出计算机安全范围的政策，包括对内容的控制。

另一个例子是域名服务器，其曾被描述为帮助提供对应被请求域名的IP地址。然而，在某些情况下，这些服务器可以被作为审查机制，阻止特定的IP地址被返回，同时有效封锁对来自该域的被请求信息的访问。

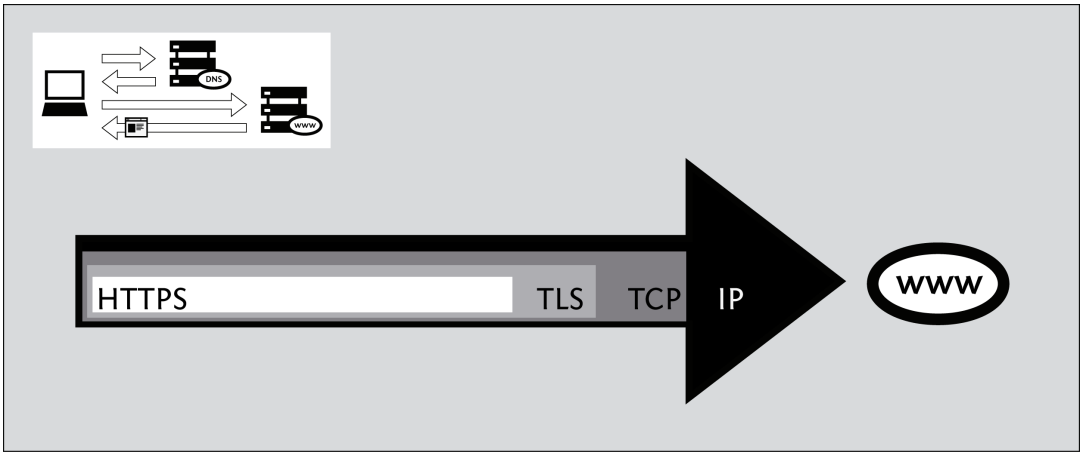
审查可以发生在互联网基础设施中的不同点，覆盖整个网络、域或子域、个别协议或者由过滤软件确定的特定内容。避开审查的最好方法取决于使用的特定审查技术。了解这些不同将有助于你为自己选择适当的措施以有效和安全地使用互联网。

端口和协议

为了共享数据和资源，计算机需要同意有关如何格式化和交流信息的约定。这些我们称为协议的约定有时被比作是人类语言的语法。互联网正基于一系列这种协议。

分层网络模型

互联网协议依赖于其他协议。例如，当你使用一个网络浏览器访问一个网站时，该浏览器依赖于HTTP或HTTPS协议以同网络服务器相交流。这种交流转而也依赖于其他协议。试想，我们为一个特定网站使用HTTPS，从而确保我们安全地访问它。



在上述例子中，HTTPS协议依赖于传输层安全（**TLS**）协议以加密通讯，从而使其穿过网络时是不公开的和未修改的。转而，传输层安全（TLS）协议依赖于传输控制协议（**TCP**）以确保信息在传输中不会意外丢失或损坏。最后，传输控制协议（TCP）依靠IP协议以确保数据被传递到预定的目的地。

当使用加密的HTTPS协议时，你的电脑仍然使用未加密的域名服务器（DNS）协议，从而为域名检索IP地址。域名服务器（DNS）协议使用用户数据协议（**UDP**）标记正确路由到域名服务器的请求，且用户数据协议（UDP）依靠IP实际传输数据到预定的目的地。

由于这种分层协议关系，我们经常把网络协议称作存在于一组层中。每一层的协议负责通讯功能的某一特定方面。

使用端口

计算机通过以上提到的传输控制协议（TCP）相互连接并在一段时间内保持连接以允许更高级别的协议执行其任务。传输控制协议（TCP）使用编号端口的概念来管理这些连接并区分不同的连接。编号端口的使用也允许计算机决定哪个特定软件应处理某特定请求或数据块。（用户数据协议也为此使用端口编号。）

IANA（因特网名称指定机构）为各种被应用服务使用的高级别协议分配端口编号。几个常见的标准分配端口编号的例子如下：

- 20和21-FTP（文件传输）
- 22-SSH（安全壳远程访问）
- 23-Telnet（不安全远程访问）
- 25-SMTP（发送电子邮件）
- 53-DNS（解析计算机名称到一个IP地址）
- 80-HTTP （正常网页浏览；有时也用作代理）
- 110-POP3 （接收电子邮件）
- 143-IMAP （发送/接收电子邮件）
- 443-HTTPS （安全网络连接）
- 993-安全IMAP
- 995-POP3
- 1080-SOCKS代理
- 1194-OpenVPN
- 3128-Squid代理
- 8080-标准HTTP式代理

使用这些特殊编号并不通常是那些协议的技术要求；事实上，任何类型的数据可以通过任何端口发送（并且使用非标准化端口可以成为一种有用的绕行技术）。然而，这些分配为方便起见在默认情况下使用。例如，你的网络浏览器知道，如果你未指定任何端口号访问一个网站时，它应自动尝

试使用端口80。其他种类的软件也有类似的默认值，因此你可以正常使用互联网服务，而不用知道或记住与你使用的服务相关的端口编号。

加密

加密是一种针对监视的技术性防御，它利用高深的数学技术对数据重新编码，使窃听者无法理解这种通信。加密还能够防止网络监管者对通信进行修改，或者至少可探测到这种修改。它通常工作起来就像一个隧道，从你正在使用的软件，如一个网络浏览器，到其他的连接终端，如网络服务器。

对于利用现代密码学的加密通信，想要通过技术方式破解是极度困难的；大量可用的加密软件为防止窃听提供了强大的隐私保护措施。但另一方面，如果用户无法或没有按照相应的流程进行加密，一些方式能够绕过加密，其中包括目标式恶意软件，或者通过密钥管理或密钥交换。例如，加密程序通常需要一种方法来确认网络连接另一端的用户或计算机身份，否则，通信将易受到中间人攻击，窃听者冒充某人的通信对象，以此截获私密通信数据。对于这种身份验证，不同的软件采用了不同的方式，但忽略或跳过这个验证步骤将使用户的加密通信对于监视变得更加脆弱。

另一种监视技术是通信分析，它利用对通信进行分析，推测通信的内容、来源、目的地或意义，即使窃听者无法理解通信的内容。通信分析是一种非常强大的技术，并且对其进行防御也非常困难。通信分析有助于确认匿名方的身份，对于匿名系统，这种技术尤其需要留意。类似 Tor 之类的先进的匿名系统采用了一些方法，可以降低通信分析的效率，但可能仍然易受攻击，这取决于窃听者的能力。

审查和网络

解互联网在实践中是如何被控制的可以帮助将互联网审查的来源与可能的威胁联系起来。互联网控制和审查可以很广泛。一个国家的政府可能不仅封锁对内容的访问，还可能会监控其国家内的人们正访问什么信息，且可能因为政府认为不可接受的互联网相关活动而惩罚用户。各国政府可能同时定义对什么封锁和实施封锁，或者他们可能制定法律法规或额外的法律激励从而促使名义上独立的公司的员工去实施拦截和监视。

谁控制着网络？

互联网治理的完整版故事是复杂的、政治性的，且仍饱受争议。政府经常拥有权力和资源去实现他们互联网监测和控制的首选方案，无论互联网基础设施是由政府自己或私营电信公司拥有和经营。因此，一个想要封锁信息访问的政府往往能够容易地对该信息产生或出入该国的信息点进行直接或间接的控制。

政府同时拥有广泛的法定权力监视其公民，且很多比法律允许的更进一步，其会使用额外的法律手段监视或限制互联网使用并按照其自己的规则去重塑它。

政府的参与

互联网是由美国政府资助的研究在20世纪70年代开发的。它逐渐扩展到学术用途，然后到商业和公共使用。今天，一个全球共同体正努力维持那些标准和协议，其旨在实现全世界范围内公开的连接性和互操作性而没有任何地域的区别。

然而，政府并没有被强求按照这些目标或有关互联网架构的相关建议来构建互联网基础设施。一些政府设计本国的电信系统有单一的“咽喉要道”，在此其能够控制整个国家对特定网站和服务的访问，且在某些情况下能阻止外界对其互联网部分的访问。

其他政府则通过法律或采用非正式的控制规制私人互联网服务提供商的行为，有时迫使他们参与监视、封锁或删除对特殊资料的访问。

一些互联网设施和协调功能是由政府或政府特许的企业管理的。没有一个国际互联网治理是完全独立运作的。政府将控制互联网和电信基础设施的活动作为国家主权的事项，且很多声称有权禁止或封锁对被认为攻击性的或危险的特种内容和服务的访问。

政府为什么要控制网络？

许多政府对这样一个事实存在问题，即只有一个技术上没有地理或政治边界的全球互联网。对最终用户来说，（除了几毫秒的延迟）一个网站是办在同一个国家还是世界的另一边并没有区别，但办在世界另一边的事实常让互联网用户愉快却深深地让国家恐慌。受到重新设置地理和地域差别希望的激励，互联网审查可以因为很多原因发生。

从网络公开倡议（http://opennet.net）选取一个分类，我们可以介绍其中一些原因如下：

- 政治原因
  政府想要审查与各自国家的政策相反的观点和意见，包括如人权和宗教类的主题。
- 社会原因
  政府想要审查与色情、赌博、酗酒、药物和其他可能看起来冒犯人的主题有关的网页。
- 国家安全原因
  政府想要封锁与反对运动有关的内容，以及任何危害国家安全的事情。

为了确保信息控制是有效的，政府可能也过滤能使人们绕过网络审查的工具。在极端情况下，政府可以拒绝向公众提供互联网服务，就像在朝鲜一样，或者其也能在公众抗议期间在其领土内切断互联网，就如同2005年在尼泊尔及2011年在埃及和利比亚短暂发生的那样。

控制可以同时针对接入服务提供商和内容提供商。

> 政府可以对接入服务提供商实施严格的控制，从而规制和塑造互联网活动，并能监测和监控该国的互联网用户。这也是一种封锁从国外流入的全球内容的手段。例如，巴基斯坦政府2010年5月要求当地互联网服务提供商封锁对Facebook的访问，从而封锁对在该社交网站上可用的先知穆罕默德讽刺画的访问，因为他们并不能控制内容提供商Facebook。
>
> 政府可以要求内容提供商，比如国内的网站编辑、网站管理员或搜索引擎，禁止和封锁对被认为攻击性的或危险的特种内容和服务的访问。例如，本地的谷歌子公司在多国（如2010年3月前在中国，此后其重定向搜索引擎活动指向谷歌香港）被要求删除有争议的内容。

我被封锁或过滤了吗？

一般来说，很难确定是否有人阻止你访问一个网站或向他人发送信息。当你尝试访问一个被封锁的网站时，你可能看到一个常规错误信息或什么也没有。该行为可能会使其看起来像该网站是因技术原因而无法访问。政府或互联网服务提供商可能否认此处有审查的事实，甚至会责备该（国外）网站。

一些组织，最引人注目的是网络公开倡议，使用软件测试不同国家的网络访问，从而了解访问可能如何被不同各方损害。在某些情况下，这是一个困难甚至危险的任务，其取决于有关当局。

在一些国家，政府毫无疑问封锁了部分互联网。例如，在沙特阿拉伯，访问露骨色情资料的尝试会得到一个来自政府的明显的信息，解释该网站被封锁了以及为什么被封锁。

在不告知封锁的国家里，审查最常见的标志之一是很多有相关内容的网站表面上因技术原因而无法访问或者看起来发生了故障（比如，“网页未找到”的错误，或者连接经常超时）。另一个潜在迹象是搜索引擎对特定主题出现反馈无用的结果或什么也没有。

过滤或封锁也可能由实体而不是政府实施。父母可能过滤影响他们孩子的信息。许多组织，从学校到企业，限制互联网访问以阻止用户从事不受监控的通讯、为个人原因使用上班时间或公司硬件、侵犯著作权或者使用过多的网络资源。

很多政府拥有资源和法定权力去控制一个国家网络基础设施的大部分。如果政府是你的对手的话，请记住，从互联网到移动和固定电话的整个通信基础设施都能被监控。

地理环境

不同地方的用户可能有各种不同的互联网内容管制经验。

- 在一些地方，你的政府可能被法律约束过滤或者决定不过滤内容。你可能被你的互联网服务提供商监控，那么这些信息可以被出售给广告商。政府可能要求互联网服务提供商在其网络上安装监控（但不是封锁）功能。政府可对你的浏览器历史记录和聊天记录提出正式的请求，或者可储存信息以供日后使用。当其这样做时，其将试着不吸引注意力。你面临着来自非政府行为者的威胁，比如攻击网站或窃取个人财务信息的计算机犯罪分子。
- 在一些地方，互联网服务提供商可能使用技术方法封锁某些网站或服务，但政府目前不会跟踪或打击报复访问其的尝试，也没有实施一个协调性的网络内容控制策略。
- 在一些地方，你可以访问能公平匹配外国服务的本地服务。这些服务由你的互联网服务提供商或政府工作人员巡视。你可以自由地发布敏感内容，但其将被删除。如果这种情况发生过于频繁，那么处罚可能会变得更加严重。限制可能只有在充满政治色彩的事件中才变得明显。
- 在一些地方，你的政府可能过滤大部分的外国网站，特别是新闻网站。其对互联网服务提供商实施严格控制，并跟踪人们创建内容。如果你使用一个社交网络平台，其会努力渗透它。政府可能怂恿你的邻居暗中监视你。

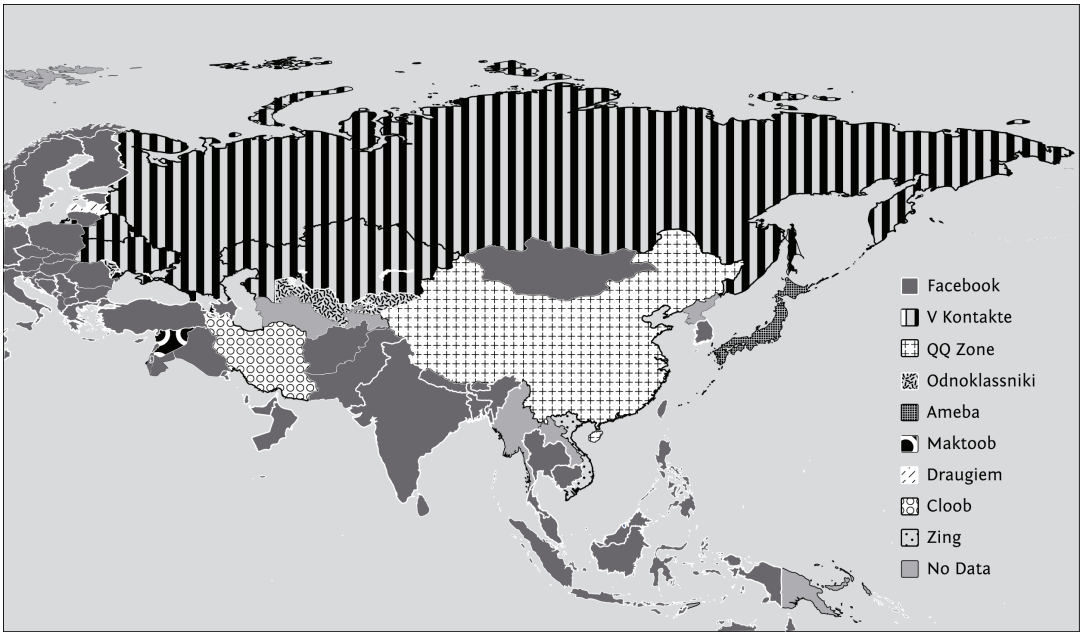
个人环境

政府有一系列动机监控或限制不同人的网上活动。

- 活动家：你可能想要改进你的政府或正寻求一个新的。也许你想要改革社会的某特定部分或为少数群体的权利而奋斗。你可能想要曝光你工作地方的环境问题、虐待劳工、欺诈或贪污。你的政府和雇主在任何时候都将对此感到不满，但如果他们怀疑街头很快会有抗议活动，那么他们可能将更多的精力放在监视你上。
- 博客：你可能想要写日常生活，但有些人却因为种族或性别而被禁言。不管你有什么要说你都不应该说。你可能处在一个大多是不受限制的用户的国家，但你的观点在你的社区却不受欢迎。你可能更喜欢匿名或者需要连接到一个支持团队。
- 记者：你可能有一些同活动家和博客主一样的关注点。有组织犯罪、腐败和政府暴行是危险的报道主题。你可能需要保护自己和成为消息来源的任何活动家。
- 读者：你可能不积极参与政治，但如此多的内容被审查，故你需要绕行软件以访问娱乐、科学和行业期刊。你可能想要阅读一个网络漫画或浏览关于其他国家的新闻。你的政府可能会忽略这个直到它有一些其他原因去监控你。

过去最常见被封锁的互联网资源是露骨的色情资料；如今，则是社交网络平台。社交网站在国际上的日益流行使得世界上数以百万计的互联网用户变为潜在的审查受害者。

一些社交网站在全球范围内流行，如Facebook、MySpace或LinkedIn，而另一些网站则在特定的国家或地区拥有大量的用户：中国的QQ（Qzone）、伊朗的Cloob、俄罗斯的vKontakte、秘鲁和哥伦比亚的Hi5、独联体国家的Odnoklassniki、印度和巴西的Orkut、越南的Zing、叙利亚的Maktoob、日本的Ameba和Mixi、英国的Bebo及其他。



审查如何工作

[以下部分改编自斯蒂芬·J. 默多克和罗斯·安德森所著的《访问被拒》第三章。]

在该章中所描述的技术是审查员采用的一些用来试以阻止互联网用户访问特定内容或服务的方法。网络运营商能够使用各种各样的技术在不同程度的准确度和定制化上过滤或操纵网络中任何一点的互联网活动。通常情况下，这些活动包括使用软件监视用户正尝试做什么和选择性地干预运营商认为被政策禁止的活动。过滤可以由一国政府或者一个国家或地方的互联网服务提供商甚至是一个本地网络的运营商创建或实施；或者基于软件的过滤可以被直接安装到个人电脑上。

根据部署组织的动机，部署过滤机制的目标也有变化。他们可能是为了使想要查看某特定网站（或个人网页）的人无法访问，或者使其不可靠，或者甚至为阻止用户尝试首先去访问它。机制的选择同样基于请求过滤的组织的能力，即他们有什么通路和影响、他们能强制执行其意愿的人群，以及他们愿意花费多少。其他的考虑因素包括可接受错误的数量、过滤是否应公开或隐蔽、以及其可靠性如何（同时针对普通用户和想要绕过它的用户）。

我们将介绍几种技术，一旦要封锁的资源列表被创建，则通过其可以对特定内容进行封锁。创建这个列表是一个相当大的挑战，且是部署系统中的共同弱点。不仅网站的庞大数量使得创建一份全面的禁止内容列表困难，而且内容是移动的，网站会改变其IP地址，故保持这份列表的更新需要很多努力。此外，如果一个网站的运营者想要对封锁进行干扰，那么该网站能比其不想干扰更迅速地移动。

我们首先介绍对最终用户使用的技术措施，然后简要讨论对出版商和虚拟主机服务提供商使用的措施，以及非技术性胁迫。

请注意该方法列表并不详尽，且在特定情况下一种以上的这些策略可能被使用。

针对最终用户的技术措施

在像互联网般的现代通信网络中，审查和监测（监控人们的通讯或活动）在实践中紧密相连。

世界上大多数的互联网服务提供商为会计目的和打击类似垃圾邮件的滥用而监控其用户通讯的某些方面。互联网服务提供商经常一起记录用户账户名和IP地址。除非用户使用隐私增强软件加以阻止，否则从技术上，一个互联网服务提供商可以记录所有通过其电缆的信息，包括用户通讯的确切内容。

该监控亦是以技术为基础的网络审查的前提。一个尝试审查其用户想要发送的通讯的互联网服务提供商能够读取那些通讯，从而确定哪些违反了其政策。因此，减少互联网审查的核心方法是向互联网服务提供商隐藏通讯的详细内容，不管是在私人事务中还是推广阻碍监测的亲隐私技术的使用时。

这意味着针对网络审查的反技术措施往往依赖于尽可能随地使用模糊处理或加密，从而使互联网服务提供商不能确切看到已传输的内容是什么。

本节讨论审查员运用技术手段封锁内容和访问的一些具体方式。

网址过滤

禁止访问网址（整个网址或部分网址）是国家和其它机构屏蔽网络信息的方法之一。网络审查者通常会完全屏蔽某些网站域名，因为他们反对这些域名所包含的内容。屏蔽整个网址是是最简单的屏蔽网站的方法之一。有时，当局会更有选择性地屏蔽某个域名的子域名，其它子域名仍可访问。越南就是这样，政府屏蔽网站的特定部分（如BBC和自由亚洲电台的越南语版），但很少审查用英文写的内容。

比如，审查者可能过滤掉子域名news.bbc.co.uk，而不会过滤bbc.co.uk 和www.bbc.co.uk。同样，他们还会过滤掉某些内容，而该域名的其它网页内容仍可以访问。方法之一就是查找目录名，比如通过“worldservice”来屏蔽bbc.co.uk/worldservice下的外语新闻，英语网站内容则不受影响。他们甚至可以根据网页名称屏蔽某些网页，以及屏蔽搜索问题中涉嫌攻击或非法内容的关键词。

网址过滤可以在本地实现，通过使用安装在你正在使用的电脑上的特殊软件。例如，网吧的电脑可能都运行过滤软件，阻止访问某些网站。

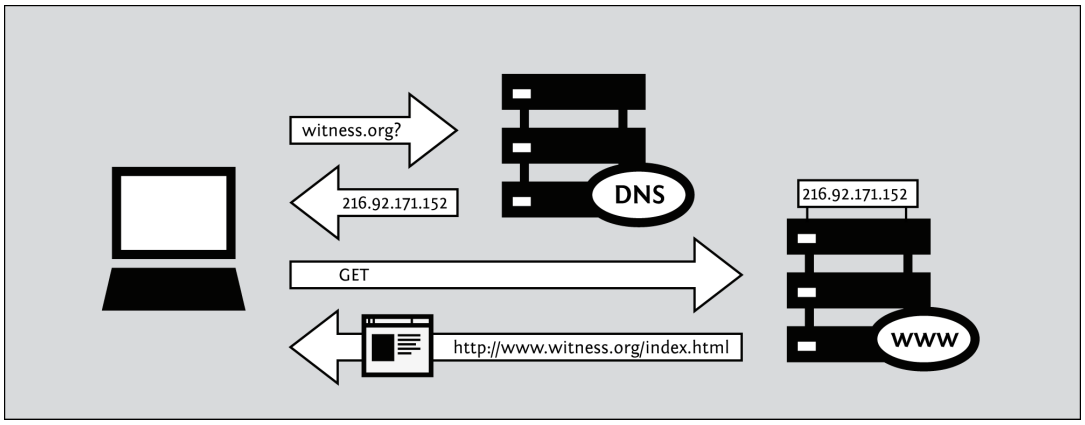
网址过滤也可以在网络的中间点实施，如代理服务器。网络可以被设置为不允许用户直接访问网站，强制（或者只是鼓励）所有的用户通过代理服务器访问这些网站。

代理服务器被用来传送请求，和在缓存里临时储存它们获取的网页，并向多个用户传送它们。对互联网服务提供商来说，这减少频繁获取一个经常被请求的页面的需要，因此可以节约资源和改进传送时间。

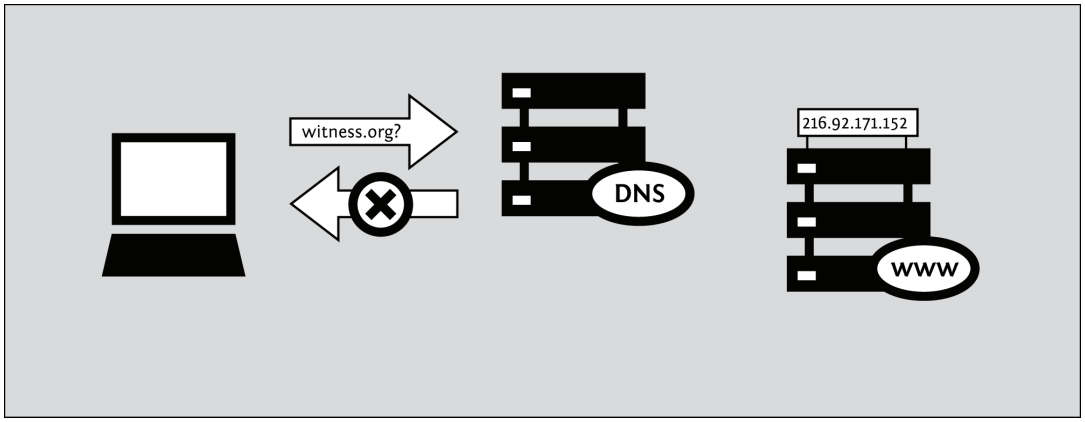
然而，除了改善性能以外，HTTP代理也可以屏蔽网站。代理决定网页请求是否被允许，如果是这样的话，向托管被请求内容的网络服务器发送请求。因为请求的全部内容可供使用，网页可能被过滤，基于网页名和网页的真实内容。如果网页被过滤，代理服务器可能返回一个正确的原因的解释，或者假装这个网页不存在或者产生一个错误。

DNS过滤和DNS欺骗

当你在浏览器中输入一个域名后，浏览器首先会向一台 DNS服务器发出请求（对应于一个已知的数字地址），查找域名，并提供相应的IP地址。



如果DNS服务器被设定为屏蔽访问，它将询问非法域名黑名单。如果浏览器向黑名单中的域名对应的IP地址发出请求 ，DNS服务器就会给出错误应答，或者根本没有反应。



如果DNS服务器给予一个无意义的应答或者没有应答，发送请求的电脑不能知道它想联系的服务的正确的IP地址。没有正确的IP地址，发出请求的计算机就无法继续，进而显示错误信息。既然浏览器无法得到网站IP地址，它也无法向网站发出页面请求，结果该域名下的所有服务，如该域名下的所有网页都会被屏蔽。在这种情况下，故意的过滤可能错误地作为技术问题或者偶然故障。

同样地，审查员可能强制一个DNS项目指向错误的IP地址，因此将网民重定向到错误的网站。这种技术叫做DNS欺骗，审查员可以用它来劫持某个服务器的身份，显示伪造的网站，或者更改用户流量路线到可以拦截他们的数据的未经授权的服务器。（在一些网络，错误的应答可能有不同的网络服务器，这清楚地说明发生的过滤的性质。不担心承认他们从事审查的审查员和那些不想让用户对发生的事感到困扰的人使用这一技术。）

IP 过滤

当数据通过互联网发送时，会被划分为数据组 （packets）。一个数据组包括发送数据以及和发送方式相关的信息，比如发送数据计算机的IP地址，以及目标IP地址。路由器是数据组从发送者到接受者之间所经过的计算机，其作用是确定信息走向。如果审查者希望阻止用户访问路由器，他们可以设置路由器，令其“放弃 ”（忽视和不能传送）发往黑名单IP地址的数据，或者返回错误信息。单纯基于IP地址的过滤会屏蔽某个服务器提供的所有服务，比如网站服务器和电子邮件服务器。既然只依靠IP地址屏蔽内容，即使本来只打算禁止一个，与其共享同一IP地址的多个域名也会同时被封。

关键词过滤

IP地址过滤只能用于根据数据包来源或去处的通信封锁，而不适用于数据包内容封锁。对于包含违禁内容的 IP 地址，如果无法制作一份完整的列表，或者某些 IP 地址包括足够多的非违禁内容，如果封锁与其相关的所有通信，这看起来并不合理，因此，对于审查者来说，网址过滤存在一些问题。如果让更为精细的控制成为可能，需要检查数据包内容是否包含违禁关键字。由于路由器通常并不检查数据包内容，而只是查看数据包头部，因此需要额外的设备，检查数据包内容的过程通常被称为深度包检测（**Deep Packet Inspection**）。

一个被确认包含违禁内容的通信，可通过直接封锁数据包使通信中断，或者向通信的双方发送信息，请求中断会话。实施这些审查和其他功能的设备已在市场上提供。

作为替代方案，可以使用下述的 HTTP 代理过滤方式。

流量整形

流量整形是网络管理者用来让一些网络顺利运行的技术，通过优先某种数据包，延迟其他种类符合一定标准的数据包。流量整形有点类似在街上控制车辆流量。总的来说，所有的车辆（数据包）有同样的优先次序，但是有些车辆被交通管理员或者红绿灯临时阻挡，以避免在某个地方交通堵塞。同时，一些车辆（消防车，救护车）可能需要更快地到达它们的目的地，因此通过阻挡其他车辆，给予他们被给予优先权。对为实现最佳性能需要低延时的网络数据包可以适用相同的逻辑（如**voice over IP**，**VoIP**）。

流量整形也可以被政府或者其他机构用来延迟有特定内容的数据包。如果审查员想限制访问某些服务，他们可以轻松地识别与这些服务相关的数据包，并通过设置它们的优先级为低，增加延迟。这可能给予用户容易误解的印象，这个网站本来就速度慢或者不可靠，或者它可以简单地使不受欢迎的网站相对其他网站来说不愉快地被使用。这项技术被不赞成文件分享的互联网服务提供商用来对付点对点文件分享网络，如**BitTorrent**。

端口封锁

把单个端口编号列入黑名单会限制访问服务器上的某个服务，比如网络或电子邮件。网络上的普通服务都有典型的端口编号。服务和端口编号之间的关系由网络分配号码机构（IANA） 分配，但是它们不是强制性的。 这些分配指令允许路由器对受访服务进行推测。因而，为了屏蔽访问某个网站的网络流量，审查者可以只屏蔽80端口，因为该端口通常提供网络接入服务。

用户所在的机构，无论是私人企业还是网吧，其网络管理员都可以控制端口的访问，此外，提供互联网连接的 ISP（网络服务提供商）或某些能够访问 ISP 所用连接的组织，如政府审查机构，也可以控制端口访问。除审查之外，还有许多原因可能导致端口被封锁——减少垃圾邮件，阻止使用不受欢迎的网络使用如点对点文件分享、即时通信或者网络游戏。

如果端口被封锁，对于用户，所有使用该端口传输的信息都是不可访问。审查通常会封锁端口 1080、3128 和 8080，因为这些是最常用的代理端口。如果用户面临的正是这种情况，你不能直接使用任何需要使用这些端口的代理，你将不得不使用一个不同的绕行技术，否则找到或者安排创建使用非常用端口的代理。

例如，在某个大学，对于外部连接，可能只能使用端口 22（SSH）、110（POP3）、143（IMAP）、993（加密式 IMAP）、995（加密式 POP3）和 5190（ICQ 即时通讯）。如果用户想使用其他的网络服务，这迫使用户使用绕行工具或者用非常用端口访问服务。

关闭互联网

关闭互联网连接是政府为应对敏感的政治和社会事件实施极端审查的一个例子。然而，完全的网络中断（如，国内和国际互联网）需要高强度的工作，因为必须关闭连接国际网络的协议和互联网服务提供商之间互相连接并和用户相连接的协议。有些国家完全关闭网络连接（2005年的尼泊尔，2007年的缅甸和2011年的埃及和利比亚）将它作为平息政治动荡的方法。关闭从持续数小时到几星期，尽管有些人试图通过拨号连接国外的互联网服务提供商或者使用移动网络或者卫星连接。

中断国际连接并不必然破坏国内的互联网服务提供商之间的连接或者单个互联网服务提供商的不同用户间的交流。将用户与内网完全隔离还需采取进一步措施。因此，中断有多个互联网服务提供商的国家的本地网络连接更难。

攻击出版人

审查员也可以通过侵害出版人的出版或者托管信息的能力，从源头上禁止发布内容和服务，这有多种实现方法。

法律限制

有时,执法者能诱导服务运营商自己履行或配合审查。例如，一些博客主机或电子邮件服务提供商,可能决定在自己的服务器上执行关键字过滤，也许是因为政府告诉他们该这么做。(在这种情况下,期待任何形式的“规避行为”将抵消这些服务的审查, 这几乎没有希望；我们通常设想将规避行为作为一种获得在别的地方的想要的网络服务的努力,如在一个不同的国家,或不同的管辖区域。)

Denial of Service（拒绝服务）

如果部署过滤的组织没有权利（或无法访问网络基础设备）实施常规的封锁，可通过令服务器或网络连接过载的方式使网站服务访问。这种技术，称为 DoS（拒绝服务）攻击，可通过一台具有快速网络连接能力的计算机进行实施；更为常用的是，利用数量更多的计算机实施分布式 DoS（DDoS）攻击。

域名注销

在前文中，我们已经提到，网页请求的第一阶段是联系本地 DNS 服务器，查找目标网址的 IP 地址。保存所有已存在的域名是不可行的，因此使用一种名为递归解析器来存储指向其他 DNS 服务器的指针，而这些 DNS 服务器更可能提供所需的答案。递归解析器将遍历每个 DNS 服务器，直到发现能够返回请求答案的“可信的”服务器。

域名系统是按照等级方式进行组织的，最上层为域名中的国家域，如“.uk”和“.de”，以及非地理位置的顶级域名如“.org”和“.com”。负责这类域名的服务器将子域名（如 example.com）的解析授权给其他 DNS 服务器，而后者对这些域名的请求进行解析。因此，如果负责等级域名的 DNS 服务器将某个域名注销，递归解析器将无法找到 IP 地址，并为用户提供该网站的访问服务。

国家类的顶级域名通常由相应国家的政府或由其指定的机构进行管理。因此，如果网站使用某个国家的域名，而对于这个国家，该网站提供的内容违禁，那么它将面临域名被注销的危险。

关闭服务器

为内容提供主机服务的服务器必须存放在某个地点，以便管理员进行管理。对于这些服务器的存放地点，如果反对这些网站内容的人员具有法律或非法律的控制权，那么他们可以断掉这些服务器的连接或要求管理员关掉它。

威胁用户

审查员同样可以以各种不同的方式阻止用户访问被禁止的材料。

监视

上述对违禁内容的封锁机制使用的是未成熟的技术，并且存在规避的可能。还有一种方式，可能与过滤同时使用，即对访问的网站进行监视。如果用户访问（或试图访问）违禁内容，那么将采取实施法律（或非法律）措施进行惩罚。

如果真相已在很多网站公布，它将阻止人们试图访问这些被禁内容，即使那些封锁的技术本身并不能真正能够防止人们获得这些信息。在一些地方,审查员试图制造一种到处都是他们的情报人员以及每个人都不断地被监视的印象,不论是否真的是这样。

社会化技术

社会化技术通常用于阻碍用户访问不当内容。例如，在一个家庭里，将个人电脑放在起居室而不是有更多隐私的房间，这样所有人都可以看到电脑显示器；阻碍孩子访问不当网站，这是一种低调而隐蔽的方式。在图书馆中，对电脑进行精心的摆放，以使图书馆官员在办公桌处就可以清楚地看到电脑屏幕。网吧安装闭路电视监控（CCTV）摄像头。当地法律可能要求安装这种摄像头，并且还要求提供用户提供政府颁发的带有照片的身份证。

偷窃和破坏通讯器材

在一些地方,审查人员有能力完全禁止某些种类的通信技术。在这种情况下,他们可以公然没收或搜寻并摧毁被禁止的通信设备，以发送一个信息，就是它的使用将不被允许。

绕行和安全

你需要的安全种类取决于你的活动及其后果。有一些安全措施每个人都应实施而无论其是否感到威胁。一些在网上要谨慎的方法需要更多的努力，但因为网络访问的严厉控制而十分必要。你可能面临来自正被研究和迅速部署的技术、老技术、替代人类智能的使用或者上述三者的结合的威胁。所有这些因素可能常常改变。

一些安全的最佳做法

有些步骤每个有计算机的人都应实施以保证其安全。这可能包括保护有关你网络活动家的信息或其可能是你的信用卡号码，但是，你需要的一些工具是相同的。

谨防承诺完美安全的程序：网络安全是一个良好软件和人类行为的结合。要知道什么应保持脱机、该相信谁以及其他安全问题不能仅靠技术回答。寻找在其网站上列明风险或已被优先审核的程序。

保持你的操作系统更新：操作系统的开发人员提供了你应时常安装的更新。这些可能是自动的，或者你可能需要输入指令或调整你的系统设置请求这些更新。一些这种更新使你的计算机更有效且更容易使用，而另一些则修复安全漏洞。攻击者能迅速了解这些安全漏洞，有时甚至早于其被修复，所以及时修复它们至关重要。

如果你仍在使用微软的Windows，那么请使用防病毒软件并保持其更新。恶意软件是为窃取信息或为其他目的使用你的计算机而编写的软件。病毒和恶意软件能够访问你的系统，进行修改并隐藏其自身。它们可以在一封电子邮件中发送给你，可以在你访问的网页上，或者作为看起来不可疑的文件的一部分。防病毒软件供应商不断研究新出现的威胁并将其添加到你的计算机将封锁的事物列表。为了使软件能识别新的威胁，你必须在更新被发布时及时安装更新。

使用好的密码：没有一个密码选择系统可以防范暴力威胁，但你可以通过使其更难猜测从而提高你的安全性。使用字母、标点和数字的组合。结合小写和大写字母。不要使用通过查阅有关你的公共信息能猜到的生日、电话号码或单词。

保持你自己更新：投入到发现你的努力可能改变。在某天起作用的技术可能在第二天就停止工作或不安全。即使你现在不需要它，你也要知道去哪里寻找信息。如果你使用的软件供应商有方法获得支持，那么在他们的网站被封之前，请确保你了解他们。

使用自由和开源软件（FOSS）。开源软件可同时用作一个可行的产品和一个针对用户和软件工程师的半成品。其比因为出口限制或费用而仅能通过非法渠道在你的国家可用的封闭源代码、以营利为目的的软件有许多安全优势。你可能无法下载盗版软件的官方更新。使用开源软件则没有必要搜索许多可疑网站以寻找免费的间谍软件和安全毛刺副本。任何合法复制都将是自由的，且可从开发者处获得。如果出现安全漏洞，其将被志愿者或有兴趣的用户发现。然后，一批软件工程师将从事解决方案，这通常是很快的。

使用分离你是谁和你在哪的软件。每个连接到互联网的计算机有一个IP地址。IP地址可被用作寻找你的物理位置，就像将其输入到一个公共“域名注册”网站一样简单。代理服务器、虚拟专用网络（VPNs）和Tor通过世界各地一到三台计算机路由你的访问。如果你只通过一个服务器，那么请注意，就像一个互联网服务提供商一样，代理提供商可以看到你所有的访问。你可能比你的互联网服务提供商更相信该代理提供商，但同样的警告适用于任何单一来源的连接。注意覆盖代理、Tor和虚拟专用网络（VPNs）的部分有更多的风险。

使用自生系统CD和可引导USB驱动器。如果你正使用一台你并不想留下数据的公共计算机或其他计算机，你可以使用Linux的一个版本，从而你能从便携式媒体运行。自生系统CD或可引导USB驱动器可插入计算机且无需安装任何东西而使用。

使用“便携式”程序：也有便携式版本的绕行软件，其可从一个USB驱动器在Windows下运行。

更安全地访问社交网站

在封闭社会和专制国家的背景下，监测成为对社交网站用户的主要威胁，特别是如果他们使用该服务协调民间社会活动或者从事网上维权行动或公民新闻时。

社交网络平台的一个核心问题是你共享有关你自己、你的活动和联系人等私人资料的数量，以及谁有权访问这些内容。随着技术的发展，社交网络平台越来越多地通过智能手机访问，社交网络平台用户位置在任何特定时刻的披露也正成为一个重大威胁。

在这种情况下，一些预防措施变得更加重要；例如，你应当：

- 编辑你在社交网络平台的默认隐私设置
- 准确地知道你和谁共享什么信息
- 确保你了解默认地理位置设置，并在需要时对其进行编辑
- 只接受你真正了解和信任的人进入你的网络
- 只接受有足够悟性也要保护你与之共享的私人信息的人进入你的网络，或者训练他们这样做。

• 必须注意，即使是你网络中最懂行的人，其也可能在被你的对手威胁时交出信息，所以要考虑限制谁有权访问哪些信息。

• 必须注意，通过绕行工具访问你的社交网络平台并不会自动保护你远离对你隐私的大部分威胁。

你可以在隐私权交流中心的这篇文章中读到更多："社交网络隐私：如何保证安全、可靠和社交"：http://www.privacyrights.org/social-networking-privacy/#general-tips

当你的社交网络平台被过滤时，你如何访问它？

如下所述，使用HTTPS访问网站是很重要的。如果你的社交网络平台允许HTTPS访问，那么你应完全使用它，并且如果可能的话，你可以将其设为默认。例如，在Facebook上，你可以编辑帐户设置>帐户安全>安全浏览（https）以使HTTPS作为连接到你的Facebook帐户的默认方式。在某些地方，使用HTTPS也可能允许你访问一个被封锁的服务；例如，在缅甸，http://twitter.com/已被封锁而https://twitter.com/仍然可访问。

如果你想要在绕行强加于你的社交网络服务上的过滤的同时保护你的匿名和隐私，那么，SSH隧道或VPN将比网站代理给你更强的隐私保证，包括针对揭示你的IP地址的风险。即使使用像Tor的匿名网络也不够，因为社交网络平台使得揭示识别信息和公开有关你的联系人和社会关系的详细信息变得十分容易。

更安全地使用共用计算机

世界人口的相当大比例，特别是在发展中国家，并不能在其家里个人上网。这可能是因为在其家里拥有私人网络连接的成本、个人计算机设备的缺乏，或者是电信或电力网络基础设施中的问题。

对这部分人口来说，现存唯一地、方便地或实惠地访问互联网的方法即是使用与许多不同的人共用计算机的地方。这包括网吧、电信中心、工作场所、学校或图书馆等。

共用计算机的潜在优势

在共用计算机上访问互联网有如下优势：

• 你可能从其他用户或设备工作人员处获得关于如何绕行过滤的技术建议和帮助。

• 绕行工具可能已安装和预配置。

• 其他用户可通过替代、离线手段与你共享未经审查的信息。

• 如果你不是一台特定计算机设备的经常用户，你没有向该设备经营者提供身份证明文件，且你没有使用你的真实姓名或帐户信息在网上注册，那么，对任何人来说都将很难单独根据你的网上活动跟踪你。

共用计算机的一般风险

事实上，你在公共场所访问互联网并没有使其对你来说匿名或安全。它往往适得其反。一些主要的威胁是：

- 计算机的所有者，或者甚至是在你之前使用该计算机的人，可以容易地将该计算机编程以暗中监视你所做的一切，包括记录你所有的密码。该计算机也可以被编程以绕行或废止你在其上使用的任何隐私和安全软件的保护。
- 在某些国家，比如缅甸和古巴，网吧顾客在使用该服务前被要求出示其身份证或护照。该身份证信息可以被储存并和该顾客的网页浏览历史一并提交。
- 你留在你使用过的计算机上的任何数据都可能被记录（浏览历史、信息记录、下载的文件等）。
- 安装在顾客计算机中的软件或硬件键盘记录器可能记录下你会话期间的每个按键，包括你的密码，甚至早于该信息通过互联网被发送。在越南，一个显然无害的输入越南字符的虚拟键盘正被政府用于监控网吧和其他公共接入点的用户活动。
- 你的屏幕活动可能被频繁截图的特殊软件记录、通过闭路电视摄像机监控，或者只是由一个偷看你的人（例如网吧管理员）观察。

共用计算机和审查

除了监视，共用计算机用户往往只能访问有限的互联网，且必须面对额外的障碍以使用其喜爱的绕行解决方案：

• 在某些国家，比如缅甸，网吧所有者必须展示有关被禁止网络内容的海报，并有责任在其业务内执行审查法律。

• 网吧管理员可能实施额外的过滤（客户端控制和过滤），从而补充在互联网服务提供商或者国家级实施的过滤。

• 用户可能为环境限制所迫出于对惩罚的恐惧而避免访问特定的网站，因此会执行自我审查。

• 计算机经常被设置以阻止用户安装任何软件，包括绕行工具或连接任何一种设备到USB端口（比如USB闪存驱动器）。在古巴，当局已开始为网吧部署一种名为AvilaLink的控制软件，其可以阻止用户安装或执行特定软件或者从一个USB闪存驱动器运行应用程序。

• 用户可能被阻止使用除Internet Explorer,以外的任何其他浏览器，从而阻止针对类似Mozilla Firefox或Google Chrome浏览器的隐私或绕行附件或设置的使用。

出于安全和绕行的最佳做法

- 根据你使用共用计算机的环境，你可以尝试以下做法：
- 根据上面提到的名单（闭路电视、人工监控、键盘记录等）确定实施的监控措施并采取相应的行动。
- 从一个USB闪存驱动器运行便携式绕行软件。
- 使用一个你通过自生系统CD的使用能控制的操作系统。
- 如果你害怕经常性监控就经常更换网吧，或者坚持在一个你相信其是安全连接的网吧。
- 带你自己的笔记本电脑去网吧并代替公共计算机而使用它。

保密和HTTPS

某些过滤网络主要（或完全）使用关键词过滤，而不是封锁特定的网站。例如，网络可能封锁任何提及被认为政治、宗教或文化敏感的关键词的交流。这种封锁可以是公开的，或者假扮成一个技术性错误。例如，无论你何时搜索网络运营商认为你不应查找的东西，某些网络会使其看起来像一个技术性错误。这样，用户不太可能将问题归咎于审查。

如果互联网通讯的内容未加密，则其对互联网服务提供商的类似路由器和防火墙的网络设备是可见的，在此，可以实施基于关键词的监控和审查。隐藏和加密通讯的内容使得审查任务更加困难，因为网络设备再也不能区分包含被禁关键词和那些未包含的通讯了。

使用加密保密通讯也可以防止网络设备记录通讯以对其进行分析和在分析其读或写了什么的事实后将个体作为目标。

HTTPS 是什么?

HTTPS是用于访问网站的HTTP协议的安全版。它通过使用加密断绝对你的通讯内容的窃听和篡改从而为访问网站提供安全升级。使用HTTPS访问网站可以防止网站运营商知道你正使用网站的哪一部分或你向该网站发送和从该网站收到了哪些信息。HTTPS支持已被包含在每个流行的网络浏览器，因此你不需要安装或添加任何软件以使用HTTPS。

通常情况下，如果一个网站通过HTTPS是可用的，那么你可以通过输入其以**https://**开头而不是以**http://**开头的地址（URL）访问该网站的安全版本。如果你正在使用一个网站的安全版本，你同样可以通过查看显示在你的网络浏览器导航栏中的地址和看它是否以**https://**开头来判别。

并不是每一个网站都有HTTPS版本。实际上，虽然有HTTPS版本的网站包括一些最大和最流行的网站，但也许不到10%的网站有HTTPS版本。一个网站只有在该网站经营者有意配置其HTTPS版本时才能通过HTTPS可用。互联网安全专家已敦促网站经营者经常做到这一点，且支持HTTPS网站的数量已稳步增长。

如果你尝试通过HTTPS访问一个网站但收到一个错误，这并不总是意味着你的网络正阻止访问该网站。它可能仅意味着该网站在HTTPS中不可用（对任何人）。不过，某些种类的错误信息更可能表明有人正积极封锁或干预连接，特别是在你知道该网站通过HTTPS应该是可用的时。

提供HTTPS网站的例子

这里是一些提供HTTPS的热门网站的例子。在某些情况下，在这些网站使用HTTPS是可选的，而不是强制的，因此你必须明确选择该网站的安全版本以获得HTTPS的好处。

网站名称	非安全 **(HTTP)** 版本	安全 **(HTTPS)** 版本
Facebook	http://www.facebook.com/	https://www.facebook.com/
Gmail	http://mail.google.com/	https://mail.google.com/
Google Search	http://www.google.com/	https://encrypted.google.com/
Twitter	http://twitter.com/	https://twitter.com/
Wikipedia	http://en.wikipedia.org/	https://secure.wikimedia.org/wikipedia/en/wiki/
Windows Live Mail (MSN Hotmail)	http://mail.live.com/ http://www.hotmail.com/	https://mail.live.com/

例如，如果你是从https://encrypted.google.com/而不是http://www.google.com/进行谷歌搜索，那么你的网络运营商将不能看到你搜索的条件是什么，因此，其不能阻止谷歌回答“不适当”的搜索。（然而，网络运营商可以决定全面封锁encrypted.google.com。）同样地，如果你通过https://twitter.com/而不是http://twitter.com/使用Twitter，那么网络运营商不能看到你正在阅读哪个消息、你正在搜寻什么标签、你在那发布了什么或者你登录了哪个帐户。（然而，网络运营商可以决定封锁所有使用HTTPS对twitter.com的访问。）

HTTPS 和 SSL

HTTPS使用一种被称为TLS（传输层安全）或SSL（安全套接层）的互联网安全协议。你可能听说过人们提到一个网站“使用SSL”或是“一个SSL网站”。在网站的语境中，这意味着该网站通过HTTPS可用。

在绕行技术外使用HTTPS

即使是使用加密的绕行技术也不能代替使用HTTPS，因为使用何种加密的目的是不同的。

对许多种绕行技术来说，包括VPNs、代理和Tor，在通过绕行技术访问一个被封网站时，使用HTTPS地址仍是可能和适当的。其提供了更大的隐私，并阻止绕行提供者本身观察或记录你在做什么。即使你有信心绕行提供者对你是友善的，这也十分重要，因为绕行提供者（或是绕行提供者所使用的网络）可能被侵入或被迫提供有关你的信息。

一些像Tor一样的绕行技术开发者强烈呼吁用户始终使用HTTPS，从而确保绕行提供者本身不能暗中监视用户。你可以在https://blog.torproject.org/blog/plaintext-over-tor-still-plaintext阅读到有关这一问题的更多信息。养成尽可能使用HTTPS的习惯是很好的，即使正使用一些其他绕行方法。

使用HTTPS的秘诀

如果你喜欢把你经常访问的网站加入书签以使你不必输入完整的网站地址，那么请记住书签每个网站的安全版本而不是非安全版本。

在Firefox中，你可以安装HTTPS Everywhere扩展，从而在每当你访问已知提供HTTPS的网站时以自动打开HTTPS。它可从https://www.eff.org/https-everywhere/获得。

不使用HTTPS时的风险

当你不使用HTTPS时，网络运营商，如你的互联网服务提供商或国家级防火墙运营商，可以记录你做的每一件事情，包括你访问的特定网页的内容。他们可以使用该信息封锁特定网页或创建以后可能被用于对付你的记录。他们也可以修改网页的内容从而删除某些信息或者添加恶意软件以暗中监视你或感染你的电脑。在许多情况下，同一网络的其他用户也可能做这些事情，即使他们并不是正式的网络运营商。

在2010年，一些这种问题将被一种被称为Firesheep的程序改写，其使得网络上的用户能极其容易地接管其他用户的社交网站帐户。Firesheep能够起作用是因为，当其被开发出来时，这些社交网站并没有普遍使用HTTPS，或者以有限的方式使用它去仅仅保护其网站的某些部分。这个范例在国际媒体引起了很多关注，也导致更多的网站要求使用HTTPS或者提供HTTPS访问作为一种选择。其同样允许技术不熟练的人通过侵入他人帐户侮辱他人。

2011年1月，在突尼斯政治动乱期间，突尼斯政府开始以允许政府窃取用户密码的方式干预用户连接到Facebook。这是通过修改Facebook登录页面和悄悄地添加发送用户Facebook密码副本给当局的软件做到的。这种修改在技术上能直接执行，且能被任何网络运营商在任何时候实施。据我们所知，突尼斯使用HTTPS的Facebook用户完全被保护免受该攻击。

使用HTTPS时的风险

当可用时，使用HTTPS几乎总是比使用HTTP更安全。即使有时出错，其也不会使你的通讯更容易被暗中监视或过滤。所以，尝试在你可以的地方使用HTTPS是很有意义的（但是请注意，原则上，使用加密在某些国家可以受到法律的限制）。然而，有一些方式HTTPS可能无法提供完整的保护。

证书警告

有时，当你尝试通过HTTPS访问一个网站时，你的网络浏览器将显示给你一条警告信息，描述该网站数字证书的问题。该证书是用来确保连接安全的。这些警告信息存在以保护你免受攻击；请不要忽略它们。如果你忽略或绕过证书警告，你可能仍能使用网站但限制了HTTPS技术保护你的通讯的能力。在这种情况下，你对该网站的访问可能变得不比一个普通的HTTP连接更安全。

如果你遇到一个证书警告，那么你应当通过电子邮件将其报告给你尝试访问网站的网站管理员，从而激励网站去解决该问题。

如果你使用一个私人设置的HTTPS网站，像某些种类的网络代理，你可能会收到一个证书错误，因为该证书是自签名的，其意味着你的浏览器未被授权确定通讯是否正被拦截。对某些这种网站来说，你可能别无选择，如果你想使用该网站你只能接受该自签名的证书。然而，你可以尝试通过其他渠道，比如电子邮件或即时消息，确认该证书是你期望的那个或者看看当从不同电脑使用不同互联网连接时其是否看起来一样。

混合内容

一个单一的网页通常由许多不同的元素组成，其可以来自不同的地方，也可以彼此分开转移。有时，一个网站会使用HTTPS于网页的某些元素而使用不安全的HTTP于其他元素。例如，一个网站可能只允许HTTP访问某些图像。在2011年2月，维基百科的安全网站出现了这个问题；虽然维基百科页面的文本可以使用HTTPS载入，但所有的图像都使用HTTP载入，因此，特定的图像可以被识别和封锁，或者用于确定用户正在阅读维基百科的哪个页面。

重定向到网站的HTTP不安全版本

某些网站仅以有限的方式使用HTTPS，且即使在用户已初始使用HTTPS访问后亦迫使用户重返使用不安全的HTTP访问。例如，某些网站使用HTTPS于用户输入其帐户信息的登录页面，但在用户登录后则使用HTTP于其他页面。这种配置使得用户容易受到监视。你应当注意，如果你在使用一个网站的过程中被发回到一个不安全页面，那么你将不再享有HTTPS的保护。

封锁HTTPS的网络和防火墙

由于HTTPS阻碍监控和封锁，有些网络完全封锁对特定网站的HTTPS访问，或者甚至整个封锁HTTPS的使用。在这种情况下，你可能被限于在那些网络上对那些网站使用不安全访问。你可能发现你由于HTTPS的封锁而无法访问一个网站。如果你使用HTTPS Everywhere或某些类似软件，那么你可能完全无法使用某些网站，因为该软件不允许不安全的连接。

如果你的网络封锁HTTPS，你应假设网络运营商可以看到和记录你所有在网上的网络浏览器活动。在这种情况下，你可能想要探寻其他绕行技术，尤其是那些提供其他形式加密的技术，比如VPNs和SSH代理。

在一个不安全计算机使用HTTPS

HTTPS仅保护当你的通讯在互联网上环游时其的内容。它并不保护你的计算机或者你的屏幕或硬盘驱动器的内容。如果你使用的计算机是共用的或在其他方面不安全，其可能包含监控或间谍软件或者审查软件，从而记录或封锁敏感关键词。在这种情况下，HTTPS提供的保护可能不是那么相关，因为监控和审查可能发生在你的计算机自身内部而不是网络防火墙上。

HTTPS证书系统的脆弱性

HTTSP证书系统也存在另一个问题--也被称为公共密钥基础结构（**PKI**）的用来验证HTTPS连接的证书权威系统存在问题。这意味着如果攻击者拥有正确的资源，那么一个富有经验的攻击者可以欺骗你的浏览器在攻击期间不显示警告。这在任何地方都在发生但尚未被明确记载。不过这不是避开使用HTTPS的理由，因为即使在最坏的情况下，HTTPS连接都将不会比HTTP连接更不安全。

BASIC TECHNIQUES

简单技巧

有一些技术可以绕开互联网过滤。如果你的目的仅仅是访问在本地被屏蔽的网页或服务，而不担心是否有人会发现并监视你的规避行为， 以下这些技巧就足够了：

- HTTPS
- 通过替代域名
  （或域名服务器）访问被屏蔽内容。
- 通过第三方网站访问被屏蔽内容。
- 通过电子邮件网关使用电子邮件获得被屏蔽网页。

使用 HTTPS

HTTPS是用于访问网站的HTTP协议的安全版本。

在某些国家,如果你想访问的网站启用了HTTPS,输入它的地址(URL)只需用https://代替http://，就可以允许你访问网站,甚至当http:// URL被封锁了。

例如http://twitter.com/在缅甸被封锁 ,而https://twitter.com/可以访问。

如果http://网址已被封锁，在尝试其他绕行工具或技术前,试着在你想访问的网站的网址http后加一个。如果这方法可行,不仅你可以访问目标网站，而且你和网站间的流量也会被加密。

了解更多关于这个技术的细节，阅读“保密和HTTPS”和“HTTPS Everywhere”这两章。

使用替代域名或者网址

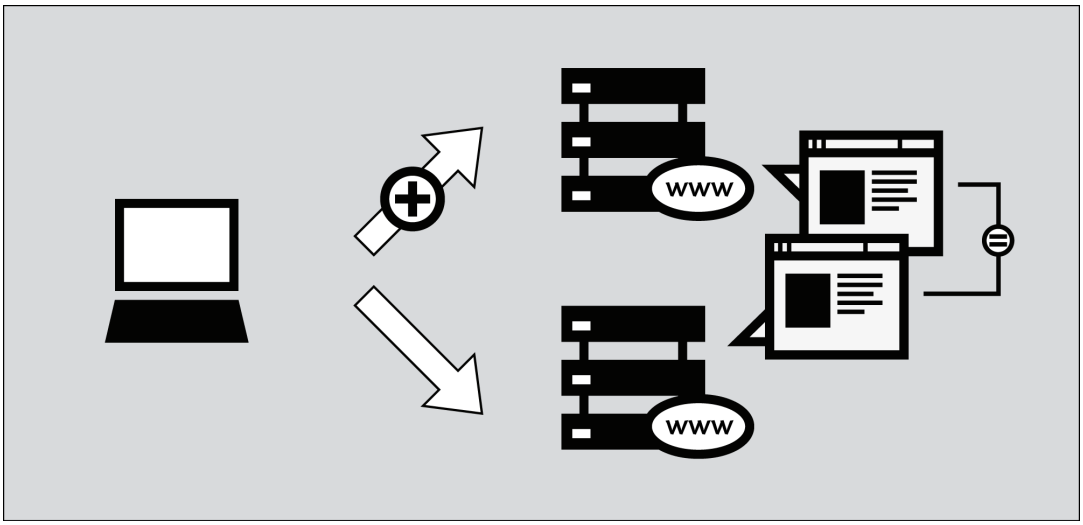
审查一个网站的最常用办法就是屏蔽其域名，比如，“news.bbc.co.uk”。但是，通常通过其它域名也可以访问同一网站，比如“newsrss.bbc.co.uk”。如果一个域名被屏蔽了，你可以试试能否通过其它域名访问该网站。

你也可以尝尝访问一些网站为创造智能手机制作的特殊版本。通常是一样的URL在开始的地方加上“m”或者“mobile”,例如：

- http://m.google.com/mail (Gmail)
- http://mobile.twitter.com
- http://m.facebook.com or http://touch.facebook.com
- http://m.flickr.com
- http://m.spiegel.de
- http://m.hushmail.c

通过第三方网站

有几种不同的方法可以让你通过第三方网站访问网页内容，而不用直接访问原网站。



缓存网页

很多搜索引擎都留有收录网页的备份，被叫做缓存网页。在搜索一个网站时，你可以在搜索结果旁边看到一个标有“缓存（cached）”的链接。因为你是从搜索引擎的服务器中检索被屏蔽网页，而不是从被屏蔽网站上，所以你也许能够访问被屏蔽内容。但是，有些国家也把缓存服务作为屏蔽的对象。

RSS 聚合器

RSS聚合器（RSS aggregators）是可以允许你订阅并阅读RSS 推送文件（feeds）的网站。所谓RSS推送文件就是你订阅的网站发布的新闻信息流及其它信息（RSS是“超简单聚合 【Really Simple Syndication】”的缩写；想了解更多使用信息，请参考http://rssexplained.blogspot.com/）。RSS聚合器会连接其它网站，下载你订阅的推送文件，然后展示给你。既然是聚合器访问其它网站，而不是你，你或许可以访问本该被屏蔽的网站。当然，该方法只适用于那些发布RSS推送文件的网站，因而对博客和新闻网站来说最有用。免费的在线RSS聚合器有很多。其中最著名的包括Google阅读器（http://reader.google.com)），Bloglines (http://www.bloglines.com)，或者Friendfeed（http://friendfeed.com）。

以下是Google阅读器显示新闻内容的示例：

翻译器

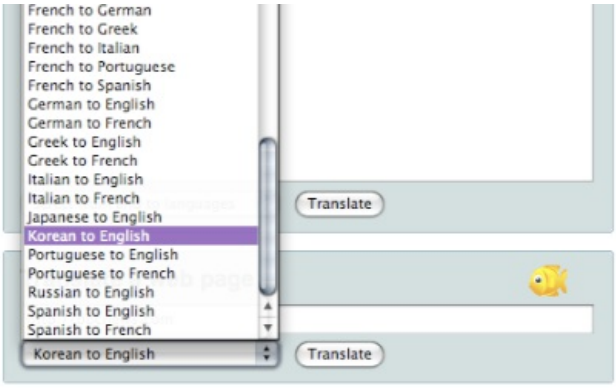
网上有很多语言翻译服务，通常由搜索引擎提供。如果你通过翻译服务访问一个网站，访问被屏蔽网站的是该翻译网站，而不是你。这样你就可以看到翻译成其它语言的被屏蔽内容。

即便你不想翻译文字内容，你也可以通过翻译服务绕开屏蔽。为此，你需要选择一种原网站上没有的语言，然后翻译成原网站语言。比如，为了使用翻译服务访问一个英文网站，你可以选择从中文到英文的翻译服务。该翻译服务只翻译中文部分（英文网站没有中文），英文部分不变（也就是整个网页）。

流行的翻译服务包括 http://babelfish.yahoo.com/ 以及http://translate.google.com/等。

以下这个例子演示了使用Babelfish浏览网页的三个必要步骤。首先输入你想访问的网址链接：

接着，选择你希望在该网站上看到的语言。在本例中，我们让Babelfish把韩语翻译成英语。既然没有韩语文字，页面将保持不变。



选好语言之后，点击“翻译”就会出现希望访问的页面。

当然这需要翻译器本身可以被访问，可并不总是这样，因为有些屏蔽当局意识到这些翻译器可能被用来绕行。

例如根据http://www.herdict.org，http://translate.google.com在沙特阿拉伯已被封锁。

窄带过滤器

窄带过滤器（**Low-bandwidth filters**）是一种网络服务，其目的是让你在网速比较慢的地方更容易地浏览网页。它们会删除或减少图片，去掉广告，压缩网站使其使用更少的数据 ，所以下载更快。

但是，和翻译和聚合服务一样，你可以通过窄带过滤器绕开网站屏蔽，从这些过滤服务网站读取数据，而不是从你的计算机上 。http://loband.org/ 是一个有用的窄带过滤服务网站。

网页存档

archive.org的缓存的(Wayback Engine - http://www.archive.org/web/web.php)允许用户看到存档的过去的网页的各种版本。数以百万计的的网站和相关数据(图像、源代码、文件等等)都保存在一个庞大的数据库。

然而，不是所有的网站都是可利用的，因为许多网站的主人选择不包括他们的网站，同时添加快照通常需要很长的事件。

通过电子邮件服务

电子邮件和网络邮件可以用来和朋友及同事分享文档，甚至可以用来浏览网页。

通过电子邮件访问网页

和窄带过滤服务一样，这些服务适用于网速低或网络不安全的用户，允许用户通过电子邮件发出网页请求。服务网站会回复一封邮件，在邮件正文或者在附件中会包含所请求的页面。这些网站需要你为一个或多个网页发送独立的请求，然后等待邮件回复，因而非常难用。但是在某些情况下，尤其是当你通过安全的网页邮件服务访问这些网站时，它们在访问被屏蔽网站时效率很高。

Web2mail

web2mail.com就是这样一个服务。在使用时，发送邮件到www@web2mail.com，并在标题栏输入你想访问的网页地址。你还可以通过在标题栏输入搜索关键词进行简单的网页搜索。比如，你可以在邮件标题栏输入“搜索审查绕行工具”，然后把邮件发送到www@web2mail.com，就可以搜索审查绕行工具。

EmailTheWeb

EmailTheWeb是另一个同类服务，http://www.emailtheweb.com,它允许你用电子邮件发送任何网页给任何人,包括你自己。通过电子邮件发送网页，你需要在网站上注册，或者使用你的Gmail帐户。免费服务最多允许你每天发送25页。

你可以在ACCMAIL邮件列表中找到更多与该话题相关的信息和支持。
向listserv@listserv.aol.com发送一封正文含有“SUBSCRIBE ACCMAIL”字样的邮件，你就可以订阅该列表。

RSS 转换成电子邮件

某些平台上提供一种类似发送网页到电子邮件的服务,但它以RSS种子为重点，而不是简单的网页；包括：

- https://www.feedmyinbox.com
- http://www.myrssalerts.com
- http://www.feedmailer.net
- http://blogtrottr.com

FoE

从电邮订阅（Feed Over Email）是另一个有趣的同类项目，由美国联邦广播理事会的Sho Sing Ho创建。在写这本书的时候，从电邮订阅（Feed Over Email）仍处于开发阶段。可以在http://code.google.com/p/foe-project上跟进了解从电邮订阅（Feed Over Email）。

Sabznameh

如果你在伊朗有兴趣阅读波斯语的被过滤的新闻。Sabznameh是一个你应该考虑的选项。Sabznameh是一个耐用的和可扩展的“电邮订阅”通讯平台,让独立的新闻读者通过电子邮件访问被审查的和被封锁的内容。

最简单的获得Sabznameh的方法是发送一封空白的电子邮件（主题和内容为空）到help@sabznameh.com。使用这种方法你可以注册，即便你不能访问该网站http://sabznameh.com。你将收到一个回复电子邮件，将引导你完成在现有的一个或多个出版物注册的步骤。

通过网页邮件分享文档

如果你想在线分享文档，但希望控制浏览权限，你可以把它们放在一个私人空间，只有输入正确的密码才可以访问。有一个简单办法可以让你跟好友和同事分享文档，那就是使用网络电子邮件提供商提供的网络邮件账户，比如Gmail(https://mail.google.com/)，然后跟你的好友和同事共享用户名和密码。由于大部分网络邮件服务都是免费的，你可以不时切换到新账户，让其他任何人都无法知道你们在做什么 。你可以在这里找到一个免费网络邮件提供商列表：www.emailaddresses.com/email_web.htm。

优点和风险

这些简单技巧快捷易用；不用费事就可以使用。很多方法在很多数情况下（至少在某些时候）都可以发挥作用。但是，它们很容易被发现和屏蔽。由于它们不会对你的信息进行加密或隐藏，很容易遭到关键词屏蔽和监视。

创新

如果你的互联网服务提供商封锁一些网站或服务，你可以使用其他章节介绍的工具，或者你可以思考创造性的途径访问不受限制的信息。下面是一些例子。

使用替代 ISPs

有时候所有的互联网服务提供商并不统一和一致适用过滤规则。大的提供商有大量的用户，和国有电信公司一样，比小型互联网企业可能受到更多监视和更多执法。2002年德国政府通过了一部管理互联网的法律，仅适用于它的一个州的互联网服务提供商。用户因此可以通过订购办公室在本国其他地区的全国性的互联网服务提供商的服务，规避这一管制。同样地，2010年实施的一部德国规章可能只影响有超过10，000用户的互联网服务提供商（为了泄漏黑名单），通过订购小型的、当地的互联网服务提供商的服务容易规避。2011年埃及革命期间，有猜测认为Noor DSL是最后一个执行关闭网络命令的互联网互联网服务提供商，因为它相对较小的市场份额（8%）和它的那些著名客户，如埃及证券交易所、埃及国家银

替代互联网服务提供商也可找海外的，一些公司甚至为那些住在剧烈政治动荡国家的用户免除订购费用。在2011年利比亚和埃及革命期间，个别公民能在他们各自国家公布政治和社会形势，是通过国外的互联网服务商拨号上网，或使用其他的通讯方法，如卫星、无线分组和跨国公司或大使馆提供的未过滤的连接。

移动网络

移动网络逐渐地成为流行的传播和访问未收审查信息的方法，原因之一是它们在拥有一台电脑或私人网络连接的成本国过高的国家有高的普及率。因为许多移动运营商并不是网络服务提供商，它们的网络不同样的受规章的影响。然而，它们

一些国家的活动家已使用他们的手机和免费的开源软件如FrontlineSMS (http://www.frontlinesms.com)管理短信（short message service (SMS)）活动， 并将短信技术和Twitter等微博服务结合起来。运行FrontlineSMS的已连接上网的电脑可以作为一个供他人通过他们的手机发布信息到网上的平台。

其他的设备也可使用移动网络。例如，Amazon的Kindle 3G电子书阅读器附带国际漫游，在超过100个国家可以通过移动网络自由访问维基百科。

不使用互联网

有时访问互联网完全受限，活动家不得不使用其他方法传播和获得未受审查的信息。1989年，互联网普及前，，一些密歇根大学的学生购买传真机向中国的大学、政府部门、医院和主要企业发送每天的国际媒体摘要，提供政府对天安门

如果你连接互联网受限，可以考虑通过其他方法进行点对点交流的可能性。IrDA (Infrared) 和Bluetooth装在大多数手机里，可以用来在短距离传输数据。其他项目，如"The Pirate Box" (http://wiki.daviddarts.com/PirateBox)，使用Wi-Fi和免费开源软件开发手机文件分享设备。在互联网普及率低的国家，如古巴，USB闪存驱动器被那些想传播未受审查信息的人广泛使用。在2011年利比亚和埃及政治动乱期间，活动家使用的其他技术包括传
真、speak2tweet（Google和Twitter推出的平台，可以是固定电话用户通过语音邮件（voicemail）发布tweet）和短信。

使用很旧或很新的技术

有时过滤和监视技术只针对当前的标准互联网协议和服务，所以可以考虑使用很旧或很新的技术，可能没被封锁或监视。及时通信（instant messaging (IM)）软件(Windows Live Messenger, AIM, 等等)出现前，使用互联网中继聊天（Internet Relay Chat (IRC)）进行团体沟通，它是一个允许实时互联网文本信息的协议。尽管不如它的后继者流行，互联网中继聊天（IRC）仍然存在，并被大量互联网用户广泛使用。电子公告板系统（bulletin board system）一个电脑运行软件，允许用户联系，上传和下载软件及其他数据，阅读新闻，和与其他用户交流信息。最初用户可以拨号使用调制解调器访问这些系统，到了1990年初期，有些电子公告板系统（bulletin board system）也允许使用互联网交互文本协议访问，如Telnet以及后来的SSH。

就这一点而言，新的技术有和旧的技术同样的好处，因为它们被有限的用户使用，因此较少被审查。例如，新的互联网协议IPv6已经被一些国家的互联网服务提供商部署，通常它没有被过滤。

网络服务的其他用途

许多网络被审查的用户使用网络服务的方式与它们最初被设计的不同。例如，网民使用视频游戏的聊天功能讨论敏感事项，在普通的聊天室聊会被发现。另一项技术是分享一个电子邮件帐号，保存会话到草稿箱文件夹，以避免在网络上发送

在线备份服务如Dropbox.com 和 Spideroak.com已被活动家用来传播和分享文件和其他数据。

原用来翻译、缓存或格式化的服务已被用作简单的代理来绕过网络审查。著名的例子有Google翻译, Google 缓存, 和 Archive.org。有其他的创造性应用, 如 Browsershots.org (给网站截图), PDFMyURL.com (给网站创制PDF版), URL2PNG.com (将网址的内容转换成PNG图片), 和 InstantPaper.com (为Nook 和Kindle等电子书阅读器创建易读的文档)。

任何通信通道都可以是绕行通道

如果你有任何形式的和合作人或者未受审查的电脑的通信通道,你应该能把它变成一种绕行的方法。如上所述,人们已用视频游戏聊天来绕过审查，因为审查者经常不会想到去监视或者审查它或者封锁流行的视频游戏。在允许玩家创建复杂的在线物体的游戏中,人们讨论创建在线电脑、电视机屏幕或其他设备,玩家可以使用他们不受审查访问被封锁的资源。。

人们也建议使用社交网络网站的个人资料隐藏信息。例如，一个人可以把他想访问的网站地址隐藏在他的社交网络网站的个人资料里。他未受网络审查的朋友将这个网站的内容保存为图形文件，然后发到另一个个人资料上。这个过程可以通过软件实现自动实现，所以它快速而且自动,而不需要人来做这项工作。

借助计算机编程,即使一个只是允许少量的数字或文本信息来回流动的通道，可以转换成一个作为网页代理的通信通道。(当一个通道, 完全掩盖了某种形式的通信存在时,它被称为隐蔽通道。)例如，程序员们创造了IP-over-DNS或HTTP-over-DNS代理应用程序使用DNS来绕过防火墙。一个例子是http://code.kryo.se/iodine上的iodine软件。你还可以在http://en.cship.org/wiki/DNS_tunnel和http://www.dnstunnel.de上阅读类似的软件的文档。 使用这些应用程序,一个访问某个网站的请求被伪装成查询众多不习关的网站地址的请求。请求的信息的内容然后被伪装成回复这些请求的内容。许多防火墙没有被配置用来阻止此类沟通,因为DNS系统从来不会被特意用来供终端用户进行通信，而是被用来运载关于网站地址的基本目录信息。

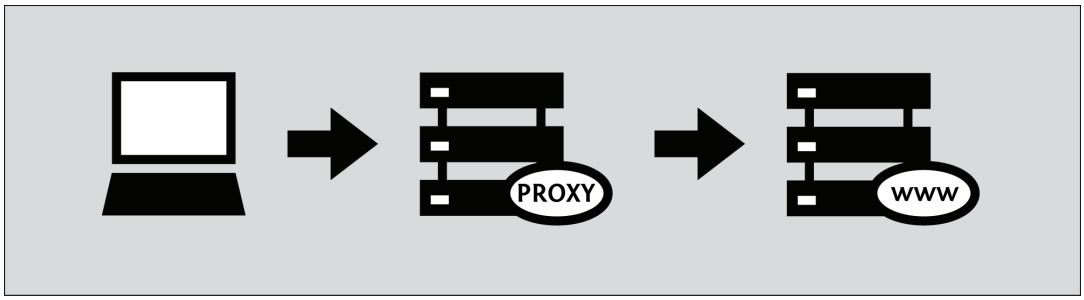
许多聪明的使用隐蔽通道来绕行的应用程序是可能的,而且这是正在进行研究和探讨的领域。为了使它有用，这些需要一个专用服务器在其他地方,两端的软件必须由精通技术的用户来设置。

网页代理

代理可以让你访问一个网站或其他互联网资源，即便在你所在地不能直接访问这个资源。有许多不同种类的代理,包括：

- 网页代理，这只需要你知道代理网站的地址。一个网页代理的网址可能看起来像http://www.example.com/cgi-bin/nph-proxy.cgi
- HTTP代理，需要你或者软件修改你的浏览器设置。HTTP代理只可以使用网页内容。你可以得到一个HTTP代理的信息，这样的格式："proxy.example.com:3128"或"192.168.0.1:8080"。
- SOKS代理,需要你或软件修改你的浏览器设置。SOKS代理可以使用许多不同的网络应用程序,包括电子邮件和即时通信工具。SOCKS代理信息看起来就像是HTTP代理信息。

网页代理就像一个嵌入你网页的浏览器。通常，网页代理都有一个地址栏，你可以在地址栏里提交想要访问的网址。然后网页代理就会显示你要的页面，但是不会让你和被请求网站之间建立直接联系。

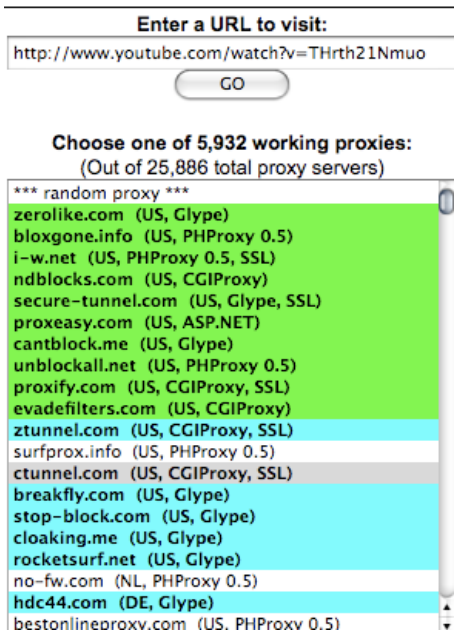


在使用网页代理时，你不需要安装软件或改变计算机设置。这意味着你可以在任何电脑上使用网页代理，包括网吧的电脑。在浏览器输入网页代理的网址 ，然后在网页代理输入你想要访问的网址，接着按回车键（Enter）或者点击"提交（submit）"按钮。

一旦你通过网页代理浏览网页,你应该能够使用你的浏览器的前进或者返回按钮,点击链接和提交地址栏，你还在用代理连接到过滤网站。这是因为你的代理人已经改写了页面上的所有的链接,所以它们现在告诉你的浏览器通过代理请求目的地资源。然而，考虑到今天的网站的复杂性,这可能是一个艰巨的任务。因此,你可能会发现一些网页,链接或者表格 "突破"了代理连接。通常,当这一切发生的时候,网络代理的URL表单将消失在你的浏览器窗口。

我怎么找到网页代理？

你可以在http://www.proxy.org这样的网站找到网页代理的网址，你可以通过加入邮件列表，如http://www.peacefire.org/circumventor，或者通过订阅一个具体国家的twitter种子（feed），或者在搜索引擎搜索"免费网页代理"（"free Web proxy"）。 Proxy.org有数以千计的免费网页代理。



免费网页代理平台包括 **CGIProxy**， **PHProxy**，**Zelune**，**Glype**，**Psiphon** 和**Picidae**。如上所述，这些都不需要你在电脑上安装。他们是服务器软件,别人必须安装在电脑上，这台电脑在不受过滤的地位连接上网。所有的这些平台提供相同的基本功能,但是他们看起来不同,可能会有不同的优点和缺点。有些可能某些方面更好，如准确地播放视频或者显示复杂网站。

有些网页代理是私人的。只有代理提供者的联系人才知道这些代理，使用者人数有限。私人网络代理有一定的优势。具体地来说,它们可能是:

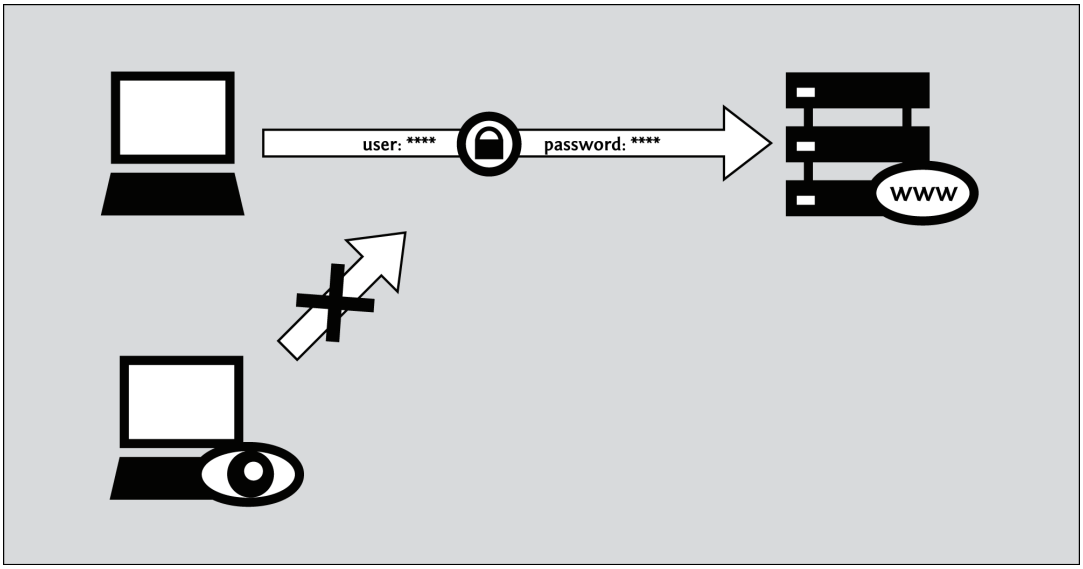
- 更有可能不被发现，因此可以访问
- 不容易拥挤,因此速度更快
- 更值得信赖,假设他们是经过加密的(见下文)和由你认识的人运行。

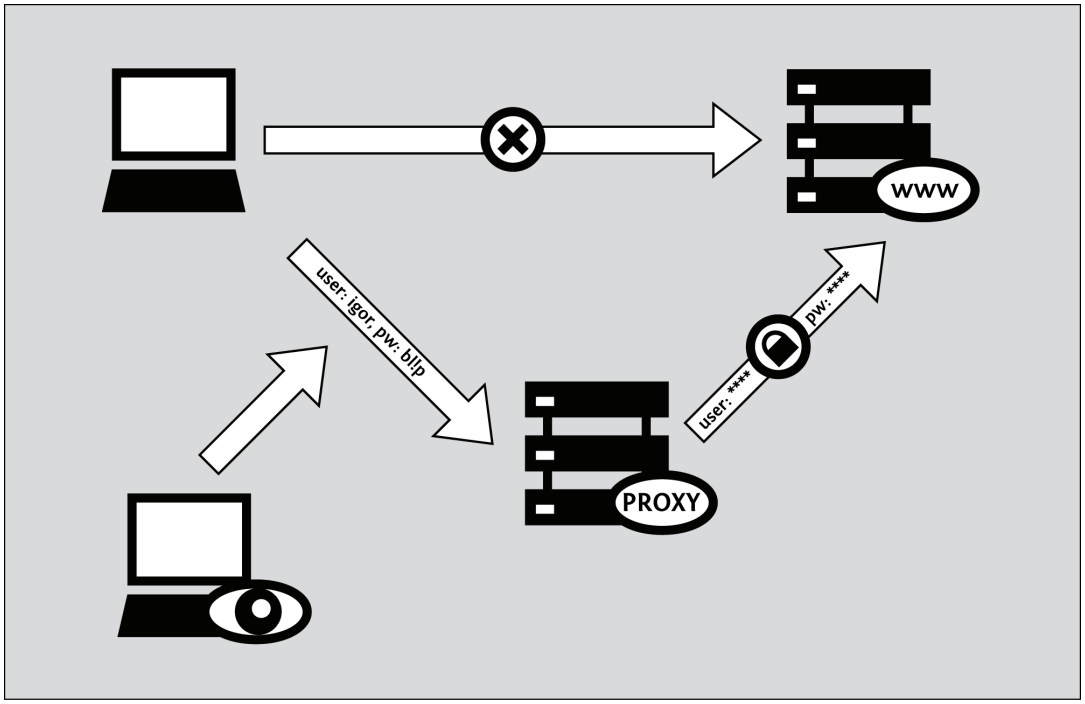
访问也会受到限制,要求用户用用户名和密码登录,或只是防止代理网址出现在如之前所述的公开目录上。

网络代理是易于使用,但他们比其他绕行工具有较多缺点。结果,人们经常使用它们作为一个临时的方法，用来获得和学习如何使用更先进的工具，这些常常需要从本身已被过滤的网站上下载。同样,当试图修复或替换已经不能用的另一个工具时，使用一个网页代理可以是有用的。

网页代理兼容性问题

网页代理只对网页通信起作用，所以他们不能被用来使用其他互联网服务,如电子邮件或即时通信。许多网页代理和复杂的网站如Facebook，流媒体网站如Youtube和通过HTTPS访问的加密网站不兼容。后面的这一限制意味着许多网页代理将无法帮助你访问需要登录的过滤网站,如基于网页的电子邮件服务。更糟的是,有些网页代理它们自身不能通过HTTPS访问。如果你使用这样一个代理登录通常安全的目标网站,你敏感的信息，包括你的密码,可能处于危险之中。





像这样的安全问题下面将进行更详细的讨论。

以上描述的HTTPS问题的显著例外，大多数网站的兼容性问题,是可以通过使用目标网站的“移动”或“基本的HTML”版本解决,假如有一个是可用的。不幸的是,相对较少的网站提供这种简化的界面,甚至更少有网站展示网站的所有功能。如果网站提供了一种移动版本,它的网址经常用“m”开头而不是“www”。例子包括：https://m.facebook.com，http://m.gmail.com，和https://m.youtube.com。 有时你能找到一个移动版或者基本的HTML版本的链接,在到网站的首页的底部的小的链接中。

使用网页代理的风险

你应该意识到使用网页代理存在着一些风险，尤其当你使用网页代理是由那些你不甚了解的组织和人员所维护时，这种风险会很大，如果你使用代理来浏览www.bbc.co.uk这样的公共站点时，你唯一的真正问题是：

- 有人可能会知道你正在浏览被审查的新闻来源
- 有人可能知道你做这些事依赖哪一种代理。

此外,如果你的网页代理运作正常,如果你访问它通过HTTPS,前者的信息只有代理的管理员知道。然而，如果你依赖一个不安全的HTTP连接故障或你的代理不起作用（或者设计糟糕），这条信息将被可能监视你网络连接的人看到。事实上,未加密的网页代理在一些国家根本不起作用,因为他们不能绕过使用关键词而不是网址或IP地址过滤的过滤器。

对于某些用户来说,上述的风险并不是一个主要问题。然而, 如果你想用一个网页代理访问特定类型的网上资源，它们可能变得相当严重，如：

- 要求你用密码登录的网站
- 你打算通过它访问敏感信息的网站
- 你打算通过它创作和分享内容的网站
- 电子商务或网络银行网站
- 自身支持HTTPS加密的网站。

在这种情况下，你应该避免使用不安全的或不可信赖的网页代理。事实上，你完全可以网页代理。不能保证一个更“高级”的工具将更加可靠,为保持你的通信隐私，可安装的绕行软件必须面对的挑战通常没有网页代理软件面对的复杂。

但是如果你使用代理来进行私人通信或者登录网页邮箱，网上银行，和网上购物这类应用时，别人可能会盗取并滥用你的个人信息，其中包括个人密码。尤其当你使用的这些服务本身未对信息加密，或者你使用的代理阻不准你对信息的加密，这种可能性会更大。

混淆不是加密

有些网页代理，尤其是那些缺乏支持HTTPS的网页代理,使用简单的编码方案，以绕开糟糕设置的域名和关键字过滤。其中的一个方案，被称作ROT-13，在拉丁字母里用在字母前13位的其他字母替代它（你可以访问http://www.rot13.com/自己尝试一下。）。当用ROT-13规则转换后，http://www.bbc.co.uk网址就变成了uggc://jjj.oop.pb.hx，它可以让关键词过滤器无法识别。代理设计者觉得这个技巧，即使在没有关键词过滤的国家。因为网页代理通常把目标网址包含在每次你点击一个链接或提交一个新的地址你的浏览器向代理发送的实际网址里。换句话说,当你使用一个代理,您的浏览器可能请求http://www.proxy.org/get?site=http:/ / www.bbc.co.uk，而不是用来对付后者的域名过滤器可能乐于对付前者。http://www.proxy.org/get?site=uggc:/ / jjj.oop.pb.hx，另一方面，就可能通过过滤器。不幸的是,字符编码方案并不十分可靠。毕竟,没什么可防止审查员增加“jjj.oop.pb.hx”到它的黑名单，和,www.bbc.co.uk一起。 (或者，更好的是，她可以添加“uggc://”到黑名单，将阻挡所有代理的使用。)

要记住的重要一点是字符编码它不能保护你的匿名性，第三方观察者仍然可以跟踪你访问的网站列表。以及，即使它可以应用到你浏览的网页的全文和你提交的全文（而不仅仅是网址），它还能不能提供机密保护。如果这些事情对你来说重要，限制你使用网页代理访问支持HTTPS的网站。

别忘了,代理的管理员可以看到所有事情。

上述建议强调了,在被审查的目标网站和代理自身上 ,当使用一个网页代理创建或获取敏感信息时，HTTPS的重要性。然而,值得注意的是,即使当你访问一个安全站点通过安全代理,你仍然坚信管理代理的任何人，这些个人或组织能读取你发送或接收的所有的通信。这包括你为了访问目标网站可能需要提交的密码。

即便更加先进的绕行工具,通常会要求你在你的计算机上安装软件,为了绕过网络过滤器必须依靠某种中介代理。然而,所有这个种类的著名工具都以这样的方式实施，为保护HTTPS网页的内容，流量甚至来源于绕行服务自身。不幸的是,这对网页代理来说是不可能的，它必须更多地依赖旧式的信任。信任是一个复杂的功能，不仅取决于服务的管理员意愿保护你的利益,也取决于她的日志和记录保存政策、她的技术能力和她经营的法律和监管环境。

网页代理的匿名风险

用来规避过滤的工具不一定提供匿名性,甚至包括那些在它们的名字里面可能包括“匿名””这样的词的工具。一般来说，匿名性是一个比基本保密更加难以捉摸的安全属性（防止窃听者查看你与网站交换的信息)。如上所述,甚至通过网页代理所要求的基本保密性确保保密，你:

- 使用HTTPS网页代理
- 通过代理连接到一个HTTPS目的网站
- 信任代理管理员的意图，政策，软件和技术能力
- 注意,任何浏览器的警告，如本书HTTPS章所讨论的。

所有的这些条件也是任何程度匿名性的先决条件。如果第三方可以阅读你通信的内容，他可以很容易将您的IP地址和你访问的网站的详细清单联系起来。这是真的，即便，例如，你用假名登录这些网站或张贴消息。(当然，相反的才是对的。你在目标网站用你的名字署名在你的帖子上，甚至一个完美的安全代理也无法保护你的身份！)

广告，病毒以及恶意软件

一些人架设网页代理是为了赚钱。他们可以网页上公开出售每个代理页面的广告，如下面的例子。或者，一些不良的代理运营者会使用恶意软件来感染用户的计算机。这类所谓的“路过时下载”（ "drive-by-downloads"）会劫持你的计算机来发送垃圾邮件和商业广告，甚至用于其他非法目的。

而确保你计算机免受病毒和其他恶意软件的侵害的一个重要方法就是保持软件的更新（尤其是你的操作系统和杀毒软件）。你也可以使用火狐浏览器的广告屏蔽扩展AdBlockPlus(http://adblockplus.org)来屏蔽广告，以及使用Noscipt扩展(http://noscript.net/)来屏蔽恶意的内容。这两款扩展都是Firefox浏览器扩展。要想了解更多避免上述风险的信息，用户可以访问StopBadware(http://www.stopbadware.org/)网站。

Cookies 和脚本

Cookie和脚本的使用也有风险。用户可以禁止掉许多站点的Cookie和脚本，但是其他许多站点（比如像Facebook这类的社交站点和Youtube这类的流媒体网站）也需要使用Cookie和脚本。网站和广告商使用这些机制跟踪你，即便你使用代理，以及提供证据，例如公开做某事的人是匿名做另一件事的人。即便你重启后，有些Cookie也会保存在计算机中，所以一个可能好的办法是有选择的使用Cookie。例如，在火狐浏览器中，你可以告诉浏览器在浏览器关闭之后自动清除Cookie。（同样的，你也可以告诉浏览器在关闭之后自动清除你的浏览记录）然而,一般来说，网页代理有着极其有限的能力来保护你的身份不被你通过它们访问的网站跟踪。如果这是你的目标，你就必须非常小心你是如何配置你的浏览器和代理设置的，你可能想要使用一种更先进的绕行工具。

帮助别人

如果你在一个可以没有限制网络访问的国家，你愿意帮助别人逃避审查，如本书帮助别人部分所讨论的，你可以在自己的网站安装在一个网页代理脚本 (甚至在你家用电脑上)。

赛风（Psiphon）

Psiphon是一个开源的网页代理平台, 过去几年改变了不少。它各种方式不同于其他代理软件（如CGIProxy和Glype）,取决于它是如何在服务器上配置它。一般来说，Psiphon:

- 通过HTTPS访问
- 支持访问HTTPS目标网站
- 改进与一些复杂网站的兼容(虽然远非完美)，包括Youtube
- 可能或可能不要求用用户名和密码登录
- 允许你用电子邮件地址注册，当你的代理被屏蔽时，从管理员那收到新的代理网址
- 允许你邀请他们使用你的代理（假设它被设置为要求密码）

当前版本的Psiphon服务器软件运行只能在Linux上运行，比大多数其他代理更难安装和管理。它主要是为了促进一个大范围的、抗封锁的绕行服务的运行，它针对那些没有能力安装和使用更先进的工具的人。

Psiphon的历史

Psiphon 1，这个网页代理平台的原版，设计用来在Windows上运行，允许在没有屏蔽互联网的国家的非专业的电脑用户向屏蔽互联网国家的具体个人提供基本的绕行服务。它安装容易，使用方便，部分支HTTPS，使得它比许多其他的服务更安全。它也需要用户登录，有利于防止拥堵和减少这些被叫做节点的小网页代理被作为屏蔽对象的可能性。Psiphon 1不再被开发它的组织维护和支持。

Psiphon 2完全重写，着眼于在集中服务模式下的性能、安全、兼容性和可扩展性体现在一个集中式服务模型。这些目标已经得到不同程度的实现。最初，一个Psiphon 2用户必须用户名和口令登录到一个特定的私人节点。Psiphon公司给了一些来自各个地区的早期的用户额外的特权，让他们能够邀请其他人访问其代理。早期的Psiphon 2代理也需要用户忽略“无效证书”的浏览器警告，因为当他们可以通过HTTPS访问，它们的管理人员不能或者不愿意购买SSL证书。所有公司部署的Psiphon私人节点本身现在已签署证书，应该不会引发浏览器的警告。很明显，对第三方安装的Psiphon软件来说可能不是这样。最后，所有的Psiphon用户现在获得发送有限数量邀请的权利。

后来实施的Psiphon 2开放节点，不用登录就可以使用。开放的节点自动载入一个特定主页，自身显示特定的语言，但当逃避网络审查时可以用来浏览其他网页。开放的节点包含一个连接，通过它用户能创建一个帐户，可以选择注册一个电子邮件地址。这样做，可以让代理管理员向所在国节点被屏蔽的用户发送一个新的网址。一般来说，开放节点比私人节点更容易被屏蔽，取代也更快。与新的私人节点一样，所有的Psiphon开放节点使用HTTPS来保证安全，Psiphon公司运行的那些节点确定自己使用有效的和签署的证书。

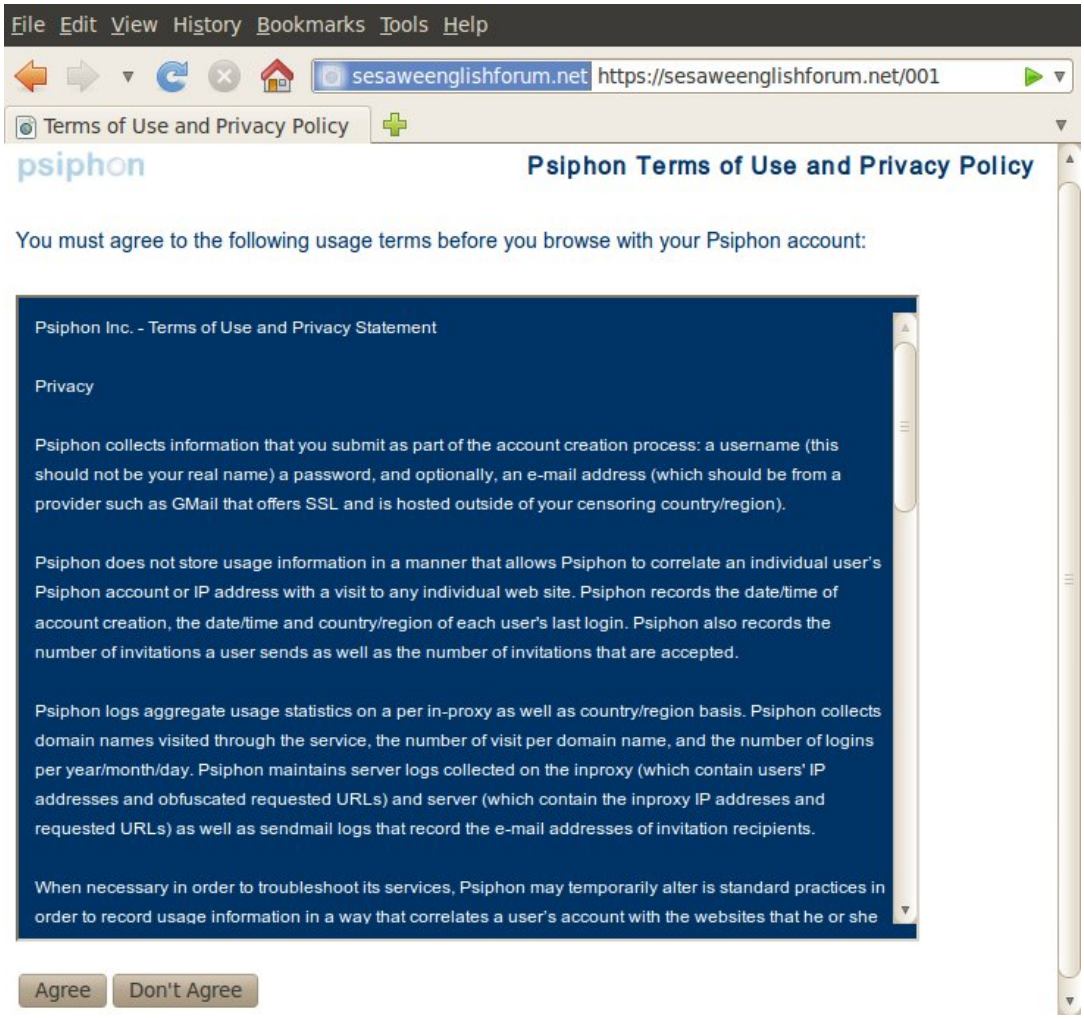
我怎样才能访问一个Psiphon节点？

为限制和监控它的代理被过滤，Psiphon公司没有集中的方式来发布公开节点(有时被称作right2know节点)。一个Sesawe绕行支持论坛专用的英语开放节点, 可在http://sesaweenglishforum.net找到。 另外的开放节点由组成Psiphon客户基础的不同的内容制作人私下传播(通过邮件列表，twitter种子，广播等)。

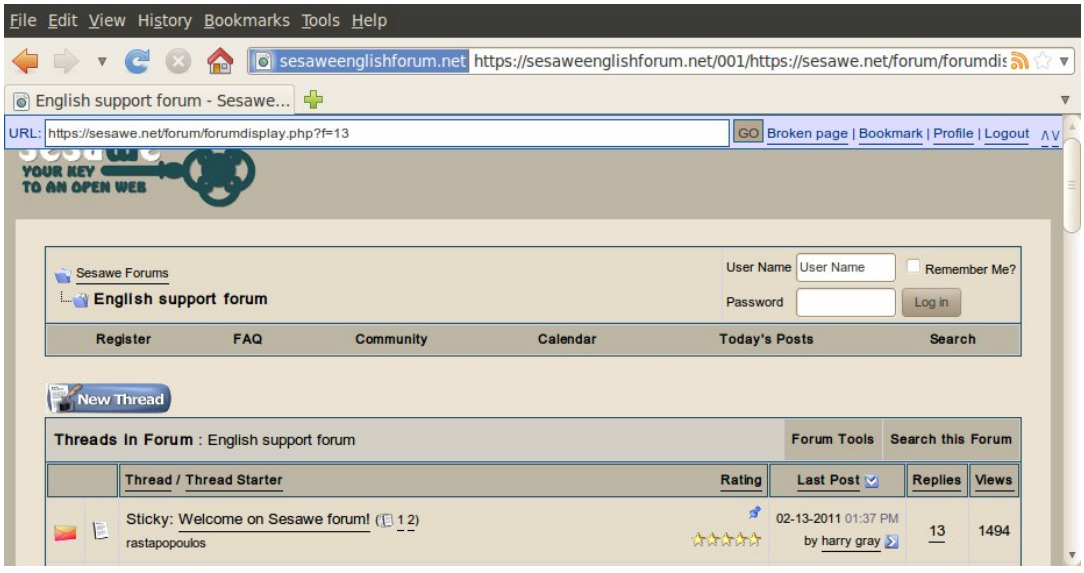
Psiphon私人节点则不一样。即使在这本书上刊载一个邀请链接是可能的，但这是不明智的,因为维护一个私人的节点最重要的一点是是限制其发展和保持一种类似与社会网络成员之间的信任。毕竟，一个发送到单个告密者邀请就可能足以让一个节点的IP地址被加到一个国家的黑名单里。更糟的是，如果邀请被接受，告密者也可以收到系统管理员发送的替代代理地址。如果你接收到了一个邀请，它将包括一个类似于下面链接的链接，https://privatenode.info/w.php?p=A9EE04A3，它将允许你创建一个帐户和注册一个电子邮件地址。跟着下面的“创建一个帐户”的指示去做。创建帐户后，就不再需要使用邀请链接。相反，你将通过一个有点容易记住的网址如https://privatenode.info/harpo登录。

使用Psiphon开放节点

你首次连接一个开放Psiphon代理，你将可以看到“Psiphon使用条款和隐私政策”。请仔细阅读服务条款，因为它们包含重要的安全建议和关于代理的管理员声称如何处理你的数据的信息。为使用这些代理，你必须点击同意（Agree）。



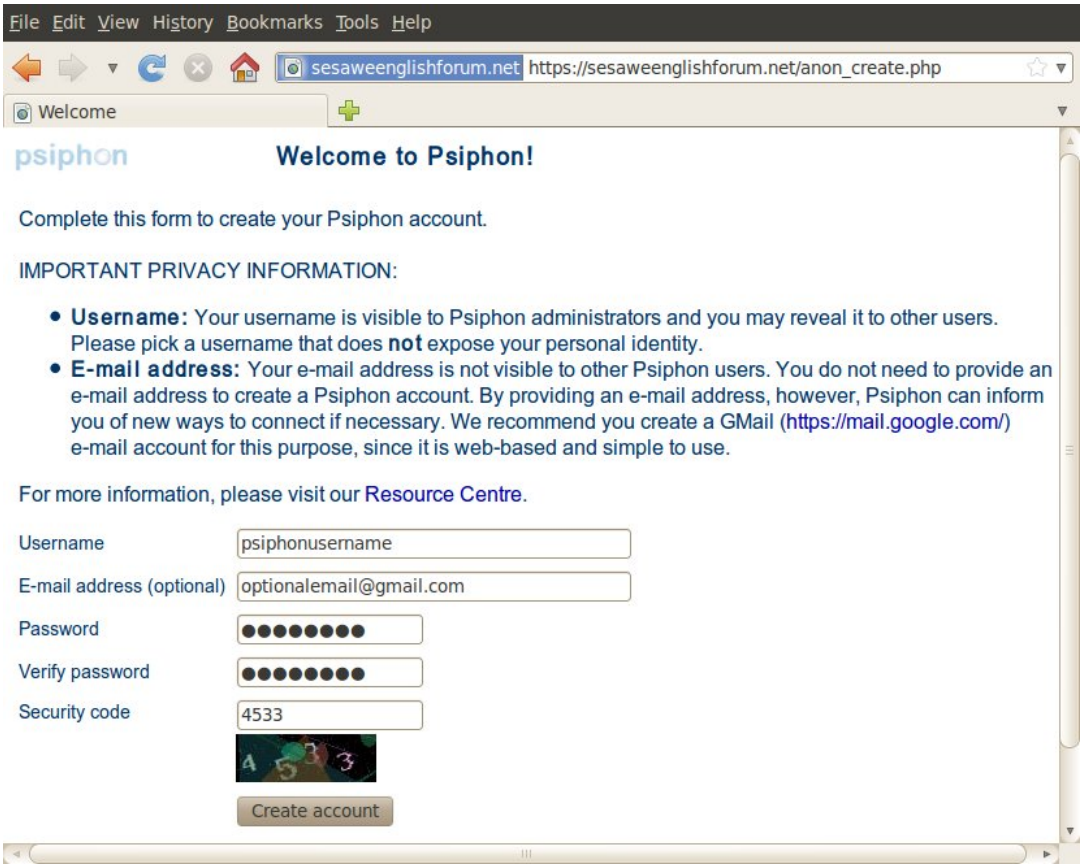
你接受使用条款后，Psiphon将会载入下面显示的一个和节点有关的默认的主页。你可以你可以点击显示在这个页面的链接，将会自动通过代理请求内容，或者你可以通过使用你浏览器窗口顶部的蓝色的地址栏（在Psiphon术语里被叫做Bluebar）访问别的网站。



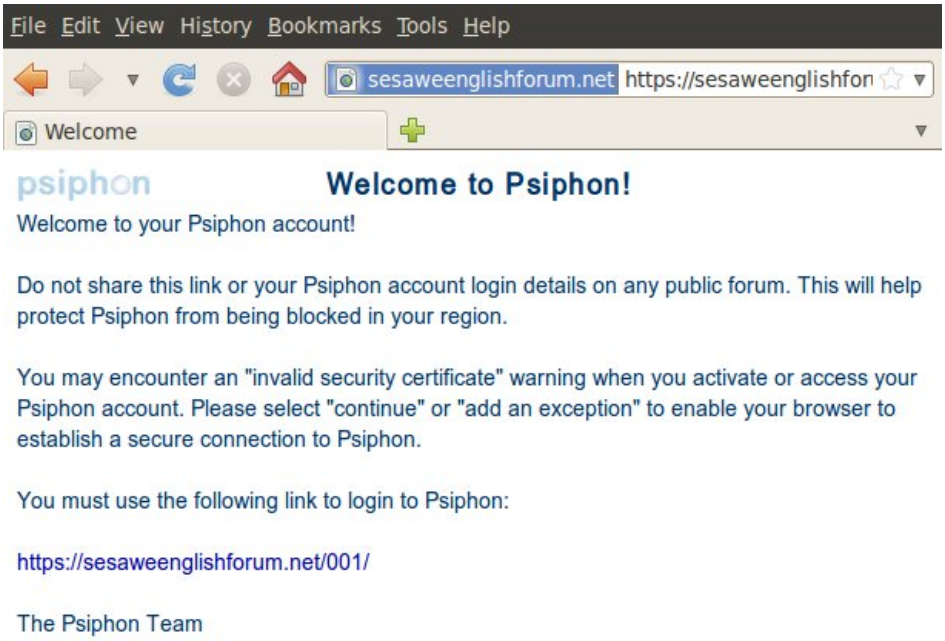
创建一个帐号

只要你还记得一个没有被屏蔽的的开放节点的网址或者将它加为书签，你可以使用它来访问被过滤的网站。创建一个帐户，允许你修改某些偏好，包括代理的语言和默认主页。它还允许您注册一个电子邮箱地址，这样，如果被过滤，节点的管理员可以发送一个新的代理网址的电子邮件给你，。要做到这一点，点击Bluebar 上的“创建帐户”链接。

如果您收到一个Psiphon私人节点的邀请，创建你的帐户所需的步骤和下面所述是相同的。

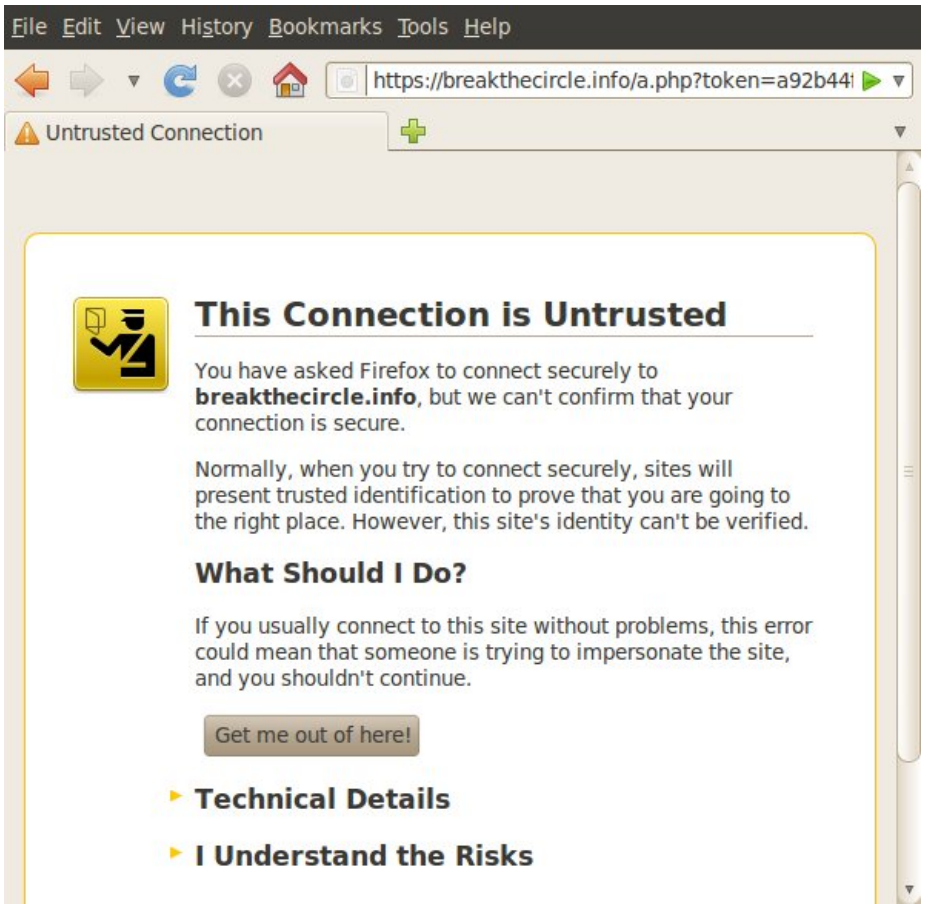


填写注册表时，你可能想选择一个不能通过电子邮件服务，社交网络网站，或其他类似平台与你的真实身份联系上的用户名。这同样适用于你的电子地址，如果你选择注册一个。大多数你的代理的其他用户无法看到您的用户名或你的电子邮件地址，但是它们都存储在数据库中的某处，网页代理的管理员可以见到。如果你选择注册一个电子邮件地址，建议你选择一个能够让你通过HTTPS连接访问电子邮件的服务。支持HTTP的免费电子邮件服务提供商包括https://mail.google.com，https://www.hushmail.com和https://mail.riseup.net。为了防止自动注册的Psiphon帐户，你必须看下安全代码图像上显示的号码，并在最后一个空格输入。当你完成后，点击“创建帐户”（"Create account"）。



你应该看到一条消息，确认你的帐户创建成功。从现在开始，请使用此页上显示的网址登录到你的Psiphon节点。请注意，它包括一个HTTPS的前缀和一个短后缀（在上面的图片“/ 001”）。你可能想打印出这个欢迎页面或将链接的网址加为书签（但要小心，不要无意中将欢迎页面本身加为书签）。当然，你也需要你在上述步骤中选择的用户名和密码。

这个欢迎页面，也可能会提供一些如上图所示的建议，关于“无效的安全证书”警告，和为使用Psiphon需要接受它们。事实上，这些说明是过时的，你不应该再遵循它们。如果连接到一个Psiphon代理时，你会看到如下面所显示的警告，你应该注意他们。如果出现这种情况，您可能需要关闭浏览器和联系info@psiphon.ca或者english@sesawe.net获得其他建议。



psiphon_right2know_sslerror_ie

邀请他人

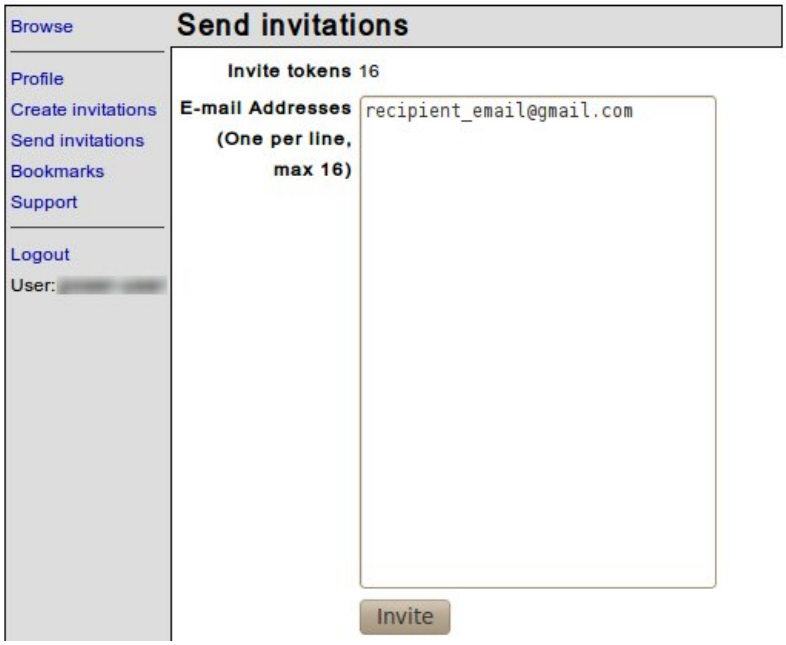
如果你使用的帐户登录到你的Psiphon代理，你最终会获得邀请他人的能力。为了帮助防止屏蔽，你会收集邀请许可将会比较缓慢，任何时间你可以获得的邀请数目都有限。显然，如果你的代理是一个开放的节点，你可以简单地发送代理网址给他人。然而，被屏蔽后，如果你在你注册的电子邮箱收到后续的“迁移”消息，你可能会发现，你的帐户已被转移到一个私人的节点。你不应该和他人共享私人节点的网址，除了通过Psiphon内置的邀请机制。

一旦你收集到一个或多个邀请，你会在Bluebar上看到一个链接，显示邀请（余下1个），如下图所示。

邀请其他人使用您的Psiphon代理有两种方式：

- 发送邀请的方法自动发送邀请链接到一个或多个收件人。邀请消息将来自Psiphon，而不是从你自己的帐户。
- 创建邀请方法生成一个或多个邀请链接，你可通过其他渠道分发。

如果你点击Bluebar链接，你将被带到发送邀请页面上。为了创造一个不需要用电子邮件发送的邀请链接，你必须首先单击“简档”（“profile”）链接，然后再“创建邀请”。



你将会看到一个提示告诉你一条或更多的信息已经进入排序阶段，这意味着在未来的几分钟内Psiphon会将你的邀请通过电子邮件发送给你。

请记住，你应该只邀请你信任的人使用私人节点。

创建邀请

单击“简档”（“profile”）页面的“创建邀请”（"Create invitations"）。选择创建的邀请链接的数量，然后点击“邀请”（"Invite"）。

您可以分发这些邀请链接，通过你可以使用的任何渠道，但是：

- 每个邀请只可以使用一次
- 不公开显示私人节点的链接，以避免暴露代理网址
- 你应该只邀请你认识的人使用私人节点。

报告不能访问的网站

使用Psiphon可能不能正常显示某些依赖嵌入的脚本和复杂的网络技术如Flash和AJAX的网站。为了提高Psiphon与此类网站的兼容性，我们的开发人员需要知道哪些网站不能正常浏览。如果您发现了此类网站，可以通过点击Bluebar上的“不能访问的页面（Broken Page）”链接，将它们报告给我们。如果你在“描述（Description）”一栏中提供对问题的简单的解释，它可以让开发人员更容易地锁定并解决问题。当完成后，点击“提交（Submit）”，您的反馈就会发送给开发人员。


Create new ticket
Browse
Profile
Create invitations
Send invitations
Bookmarks
Support
Logout
User:
Create new ticket
Submit
Cancel
Subject
Broken page
Description
http://www.facebook.com/?_fb_noscript=1
I can log in, but some features don't to work properly. For example, I can't seem to send friend requests. (The mobile site appears to work, though!)
Submit
Cancel

SabzProxy

SabzProxy（波斯语的意思是“绿色代理”）是一个免费的分布式网页代理，是由Sabznameh.com团队提出来的。它是基于PHProxy遗留代码（自2007年以来就没有维护）。如需了解网页代理的概念的其他详细信息，请参阅前面的章节。

和PHProxy相比，SabzProxy主要的改进是它的网址编码。这使得SabzProxy更难以被检测（PHProxy有一个预知足迹，这意味着现在它在一些国家被过滤，包括伊朗在内）。只有深度包检测可检测并阻止SabzProxy服务器。

SabzProxy的语言是波斯语，但在任何语言环境都能实现全部功能。不同国家的许多人都使用它来建立自己的公共网页代理。

一般信息

Supported operating system	
Localization	Persian
Web site	http://www.sabzproxy.com
Support	E-mail: sabzproxy@gmail.com

我如何访问 SabzProxy

SabzProxy是一个分布式的网页代理。这意味着，既没有中心的SabzProxy代理，也没有一个商业实体，来创造和传播它。相反，它依赖于它的社区和用户创建自己的代理，并与他们的网络分享这些。你可以通过各种论坛或网络访问它，当你有机会访问时，欢迎你与你的朋友分享。

Sesawe绕行支持论坛运营一个专用的代理，在http://kahkeshan-e-sabz.info/home（您可以用用户名flossmanuals，密码flossmanuals登录）。

如果你拥有一个网络主机空间，并有兴趣创建和与你的朋友和家人分享您的SabzProxy代理，请参阅本书的帮助他人部分安装SabzProxy这一章。

它是如何工作的？

下面是一个例子，说明如何SabzProxy是如何工作的。

1. 在你正在使用的浏览器中输入SabzProxy代理的地址。

2. SabzProxy页面上的网页地址框中，输入你想要访问的被审查的网站地址。例如，http://www.bbc.co.uk/persian。你可以保留默认的选项。

单击Go或Enter。

网站在浏览器的窗口显示。

你可以看到SabzProxy绿色的地址栏在浏览器窗口里，和地址栏下方的BBC波斯语网站。

继续浏览，你或者：

- 点击当前页面的任何链接。网页代理将自动检索被链接的网页。
- 在页面顶部的地址框中输入新的网址。

高级选项

通常你可以使用默认选项浏览网页。但您也可以设置以下几个高级选项：

- 在每个页面中都采用迷你URL/ **فرم آدرس**

如果您想在任何一个通过代理打开的页面上保留一个地址栏，以便输入新的网址而不用再返回到Sabzproxy的主页输入，你可以使用这个选项。如果您的屏幕比较小，最好把这个选项关闭，以便有更多的空间显示页面。

- 禁用客户端脚本（如JavaScript）/ **حذف اسکریپت ها**

如果你想从网页删除动态技术脚本，你可以使用这个选项。有时，JavaScript可以造成不必要的问题，因为它也可以用来显示在线广告，甚至跟踪你的身份。浏览复杂的网站（如网络邮件服务，或社交网络平台）的移动/轻的版本也是一种使用SabzProxy时避免JavaScript问题的替代方法。

- 允许保存cookie/ **قبول کردن کوکی ها**

cookie是由你的浏览器自动保存的小型文本文件。在一些需要认证的网站上它是必需的，但也可能用来跟踪你的身份。打开这个选项之后，每个cookie都会被保存较长一段时间。如果您想在进程结束后就删除它们，就关闭这个选项并选择“仅在该线程运行 时保存cookie”（详见下文）。

- 显示页面图片/ **نمایش عکسها**

如果您的网速较慢，可以关闭这个选项，这样页面将更轻，从而加快页面加载速度。

- 显示实际引用来源/ **نمایش مسیرها**

浏览器会默认发送你链入的链接。浏览器会自动在日志中记录结果页面的链接并加以分析。为了达到更好的匿名性，你可以关闭这个选项。

- 去除页面中的元信息标签（meta information tags）/ حذف تگ هاي متا

许多网站上保存的元信息标签可以被计算机程序自动取用。这些信息可能包括作者姓名、网站内容描述或者搜索引擎关键词。过滤技术可以在这些标签上运行。你可以打开这个选项来防止关键字过滤发现这些元信息。

- 去除页面标题/ **حذف عنوان صفحات**

如果打开这个选项，Sabzproxy会删除显示在浏览器顶部标题栏上的页面标题。这个技巧很有用，比如隐藏你正在访问的页面名称，当你最小化浏览器窗口时，你不想周围的人看到它。

- 仅在该线程运行时保存cookie/ **كوكي ها موقت**

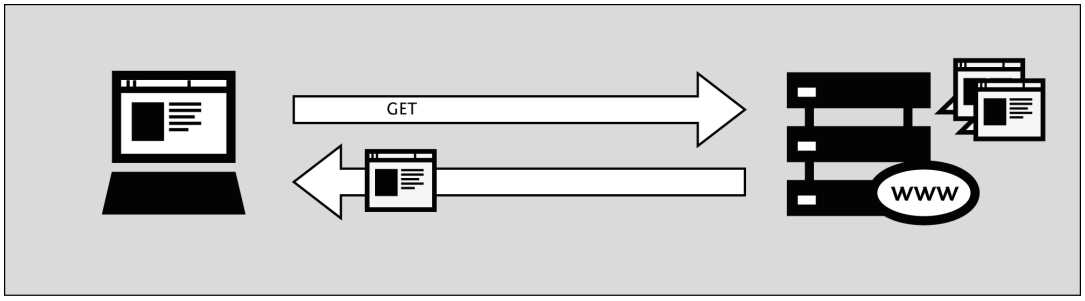
该选项与“允许保存cookie”类似。打开该选项后，一旦你通过退出浏览器关闭Sabzproxy进程，则保存在电脑中的cookie也会被删除。

FIREFOX AND ITS ADD-ONS

介绍火狐（Firefox）

我们猜想除非你已经知道网络浏览器是什么，否则你不会阅读这一章。然而，如果你不知道，浏览器是你用来在网上访问和浏览网站的软件。

在之前的一章里，我们解释了互联网是一个庞大的计算机网络，都相互连接。一部分计算机是“网络服务器”——网站在其上的计算机。如果你想使用电脑或移动设备访问这些网站，你需要一种冲浪和显示它们的方法。这就是浏览器的用途。



Firefox是最流行的浏览器之一，是一款由 Mozilla基金会2003年研发的免费、开源的网页浏览器。Firefox可运行于所有的主要操作系统（Windows, MacOS 和Linux）。它至少被翻译成75种语言。最重要的是，它完全免费。

从那里得到 Firefox

如果你想安装Firefox，你可以在这找到安装文件：https://www.mozilla.com/en-US/firefox/

当你访问这个网站，将会自动出现适合你操作系统(Windows/Mac/Linux)的安装文件。欲知更多关于在这些操作系统安装Firefox方法的信息，请阅读FLOSS Manuals Firefox指南：http://en.flossmanuals.net/firefox

什么是 Firefox 附加组件（add-on）?

首次下载和安装Firefox时，它能直接处理基本的浏览器任务。通过安装附加组件（*add-ons*），能增强Firefox能力的小附件，你也可以增加额外的性能或者改变Firefox的活动。这里有几种附加组件（*add-ons*）：

- 给浏览器提供额外功能的扩展
- 改变Firefox外观的主题
- 帮助Firefox处理其通常不能处理的事情（如闪客电影， Java应用程序等等）的插件

可用的附加组件（*add-ons*）的种类巨多。你可以安装不同语言的字典，跟踪其他国家的天气情况，获得类似你正在浏览的网站的建议，等等。

Firefox在其网站(https://addons.mozilla.org/firefox)上有现有的附加组件（*add-ons*）的清单，或者你可以在https://addons.mozilla.org/firefox/browse上按种类浏览它们。

在安装任何附加组件（*add-on*）前，切记它能从你的浏览器读取大量的信息，所以从可靠的来源选择附加组件（*add-ons*）非常重要。要不然，你安装的附加组件（*add-on*）可能偷偷分享你的信息，记录你访问过你网站，甚至伤害你的计算机。

我们推荐你决不为Firefox安装附加组件（*add-on*），除非它可以从Firefox的附加组件（*add-on*）页面获得。你也不应该安装Firefox，除非你能从可靠的来源获得安装文件。请注意在他人的电脑或在网吧使用Firefox增加了潜在的脆弱性，这一点很重要。

接下来的三章，我们将了解与用来对付网络审查尤为相关的附加组件（*add-ons*）。

Noscript 和 Adblock

虽然没有任何工具可以完全保护你，防范所有对你的网络隐私和安全的威胁，这章所介绍的Firefox扩展能够显著减少你遇到你最常见的威胁，增加你保持匿名的可能性。

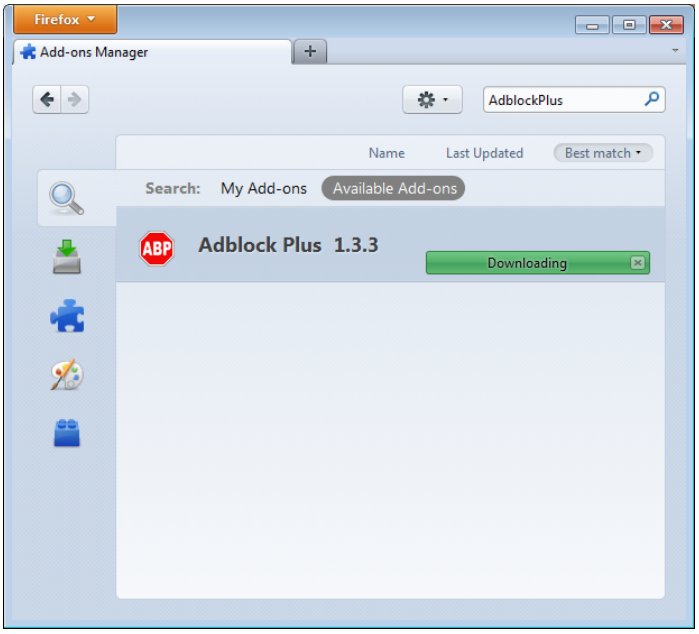
AdBlock Plus

Adblock Plus(http://www.adblockplus.org)扫描网页，发现广告和其他试图跟踪你的内容，然后阻挡它们。Adblock Plus依赖志愿者维护的黑名单，以保持与最新的威胁同步。

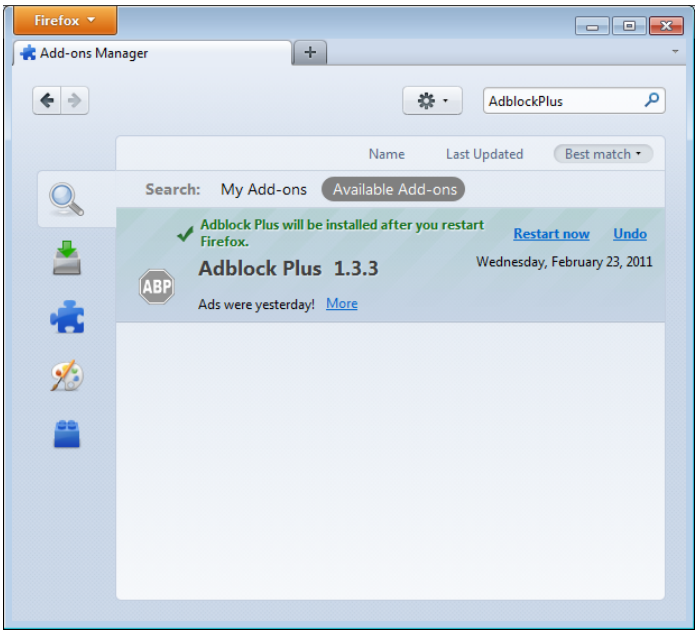
开始使用 AdBlock Plus

有了安装好的Firefox后:

1. 从http://adblockplus.org/en/installation#release，下载AdBlock Plus 的最新版本，或用附加组件管理器（Add-ons Manager）("Firefox" > "Add-ons").搜索这个插件。
2. 点击“现在安装”（ "Install Now"），确认你需要AdBlock Plus。

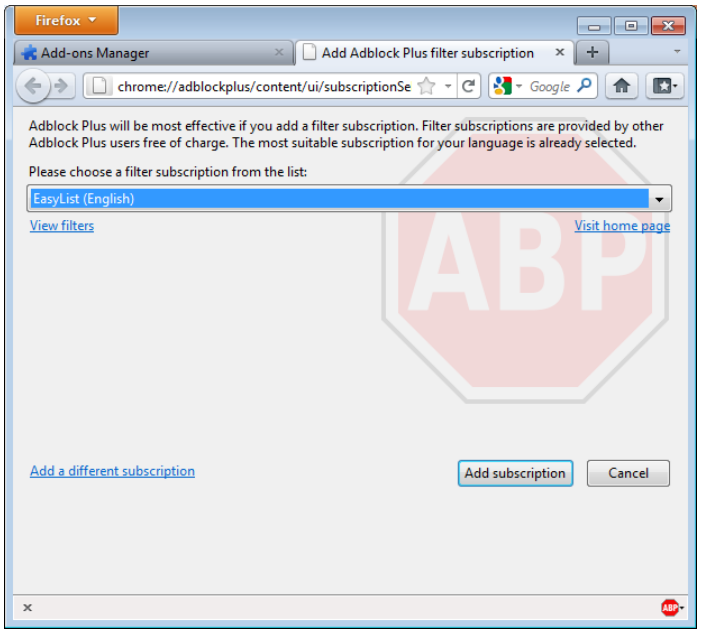


3. AdBlock Plus安装好后，Firefox要求重新启动。



选择过滤规则

Adblock Plus 自身不能做什么。它可以看到网站企图加载的每一个成分，但是它不知道该过滤哪些。这正是Adblock过滤规则所要解决的。重启Firefox后，你将被要求选择一个过滤规则订阅（免费）。



你应该选择哪一个过滤规则订阅呢？Adblock Plus在下拉菜单提供了一些，你也许希望了解每一个的优点。EasyList就是一个好的保护隐私的过滤规则。（它也在http://easylist.adblockplus.org/en上面）

尽管看起来很诱人，但不要把你能得到的过滤规则订阅都添加上。因为有些可能重叠，从而导致意想不到的结果。EasyList（主要针对英文网站）能与其他EasyList扩展一起工作（如RuAdList等特定区域列表，EasyPrivacy等主题列表）。但是它与Fanboy的列表（另一个主要针对英文网站的列表）相冲突。

你可以在首选项（preferences）里随时更改你的过滤订阅(按 Ctrl+Shift+E)。更改后，点击OK。

创建个性化的过滤规则

如果你有兴趣的话，AdBlock Plus允许你创建自己的过滤规则。添加过滤从Adblock Plus首选项（preferences）开始（按Ctrl+Shift+E），点击窗口左下角的“添加过滤规则”（"Add Filter"）。个性化的过滤规则不能取代维护好的黑名单如EasyList，但它们对阻挡公共列表上没有的特定内容非常有用。例如，如果你想阻止来自其他网站和Facebook进行互动，你应该添加下列的过滤规则：

```
||facebook.*$domain=~facebook.com|~127.0.0.1
```

第一部分（|| FACEBOOK.*）首先屏蔽一切来自Facebook的域名的访问。第二部分（$域=～facebook.com |～127.0.0.1）是一个例外，那就是告诉过滤规则为了使Facebook的某些功能保持运转，只有当你在Facebook上或从127.0.0.1（您自己的电脑）访问时允许Facebook的请求。

关于如何创建自己的Adblock Plus过滤规则的指南，可以在http://adblockplus.org/en/filters上找到。

为特定元素或网站启用和禁用 AdBlock Plus

你可以点击你浏览器上的ABP工具栏图标（通常挨着搜索栏），选择"打开可过滤项目"（"Open blockable items"），或按 Ctrl+Shift+V，看到AdBlock Plus识别的各种元素。你浏览器底部的窗口可以让你逐一启用和禁用每一个元素。或者，你可以点击ABP工具栏图标，勾选“对域名禁用”（"Disable on [domain name]"）或“只对这个网页禁用”（"Disable on this page only"），在某个特定域名或网页禁用 Adblock Plus。

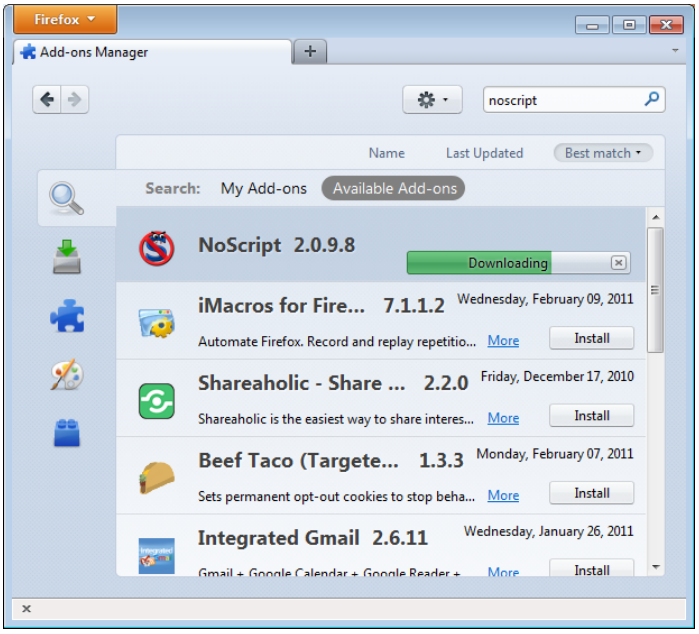
NoScript

NoScript全面禁止所有的JavaScript、Java插件和其他网站载入在你电脑上运行的可执行内容，进一步保护浏览器的安全。告诉NoScript忽略一些特定的网站，你需要把它们加入白名单。这听起来可能乏味，但在NoScript保护网民免受跨站脚本（攻击者将恶意代码从一个网站植入另一网站）和点击劫持（点击一个页面的无害目标时暴露保密信息，或者允许攻击者控制你的电脑）之类的威胁方面做得很好。访问http://addons.mozilla.org 或http://noscript.net/getit,得到NoScript.

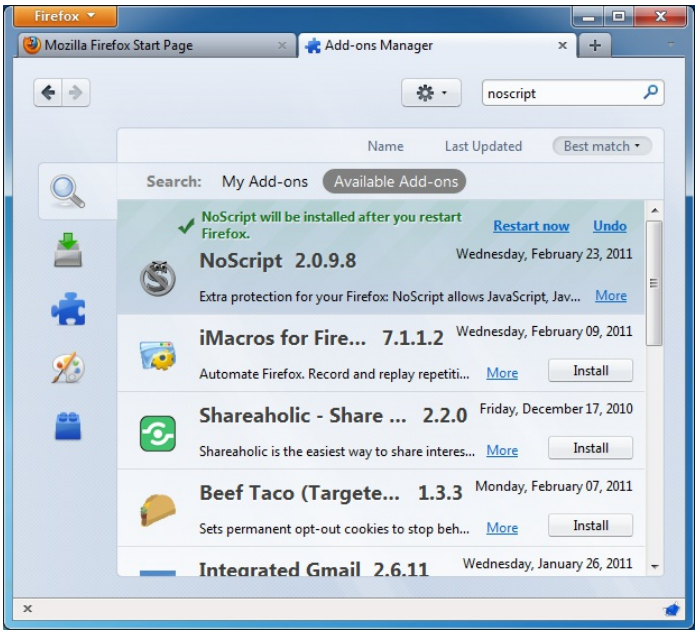
NoScript
保护你的方法也可能改变好的网页的外观和功能。幸运的是，你可以手动调整NoScript对每个网页和网站的处理方式，由你来找到方便和安全之间合理的平衡点。

开始使用 NoScript

1. 访问NoScript的下载部分： http://noscript.net/getit.。点击绿色的“安装 ”（"INSTALL" ）按钮。
2. 点击“现在安装” ，确认你需要NoScript。



3. 要求重启时重启Firefox。



NoScript 通知和添加网站到白名单

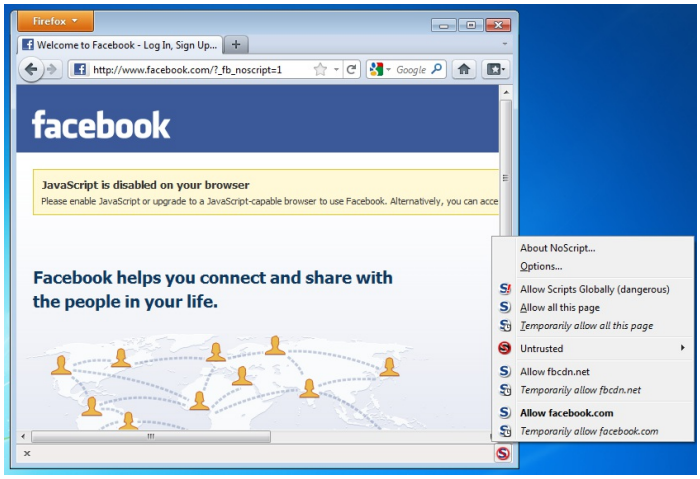
重启后，NoScript的图标将会出现在你浏览器的右下角，就是状态栏所在的位置，显示当前的网站在你的电脑上执行内容的权限。

- 完全保护：禁止当前网站和其subframe的脚本。即使有些脚本由你白名单上的网页导入，代码将不会被运行（托管文件不会被启用）。
- 严重受限：主要站点仍然被禁止，但有些部分（如框架）被允许。这种情况下，部分代码可以运行，因为主要脚本有被禁止，这个页面不可能正常运转。
- 有限允许：允许主要文件的脚本，但其他活性元素或网页导入的脚本不会被允许。一个页面上有多种框架或者链接存储在其他平台的代码的脚本成分时发生。
- 最受信任： 允许网页上的所有脚本，但是部分嵌入内容被禁止（如框架）。
- 选择性保护：允许部分网址上的脚本，其他的标记为不信任。
- 允许当前网站上的所有脚本。
- 全局允许脚本，，但标记为不信任的内容将不会被载入。

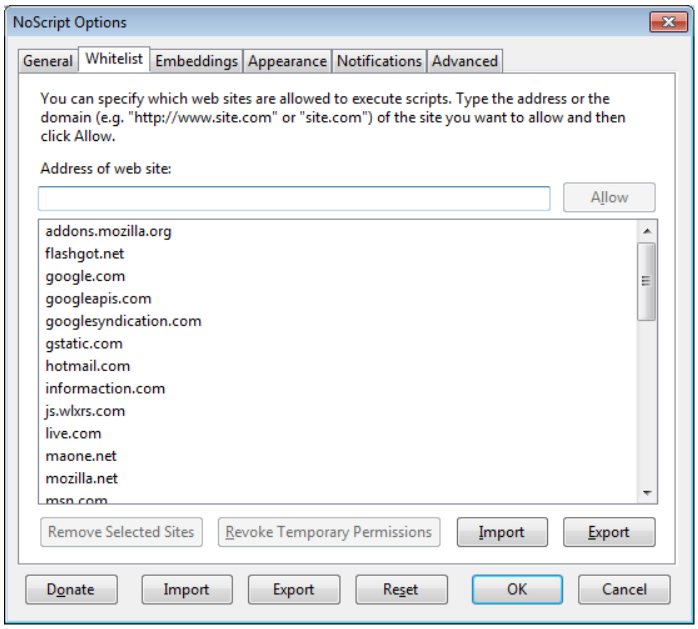
添加一个你信任的站点到白名单，点击NoScript按钮选择：

- “允许域名”（"Allow [domain name]"）允许一个特定域名上的所有脚本，或者
- “允许本页面所有对象”（"Allow all this page"） 完全允许脚本运行，包括来自其他地方，但从主要网站载入的第三方脚本。

（你也可以使用“临时允许”（ "Temporarily allow"）选项只允许当前会话的内容载入。对只想就一次访问该网站以及想让白名单在可控水平上的人有用。）



或者，你可以点击NoScript按钮，直接添加域名到白名单，选择选项（Options），然后点击白名单（Whitelist）选项卡。



标记内容为不可信的

如果你想永久地禁止脚本加载某一网站，你可以标记它为不可信任的：点击NoScript图标，打开“不信任的”（ "Untrusted"）彩电，选择“标记【域名】为不可信的”。 NoScript会记住你的选择，即使启用“全局允许脚本” （"Allow Scripts Globally"）。

HTTPS （超文本传输安全协议） Everywhere

HTTPS Everywhere是 Tor 项目(https://www.torproject.org)和 EFF（Electronic Frontier Foundation）(https://eff.org/)合作开发的 Firefox 附加组件（add-on）。它加密你与若干重要网站之间的通讯，包括Google，Wikipedia，和流行社交网络平台如Facebook和 Twitter。

很多网站有限的支持通过HTTPS加密，但使用不方便。例如，默认用未加密的HTTP，即便可以使用HTTPS。或者在加密网页中嵌入大量非加密链接。

这样，这些网站发送和收到的数据（如用户名和密码）以纯文本的方式传送，容易被第三方看到。

HTTPS Everywhere通过重新要求这些网站使用HTTPS，来修复这些问题。（尽管这个扩展叫做"HTTPS Everywhere"，它只能激活个别网站使用HTTPS，只能使那些以选择支持它的网站使用HTTPS。如果这个网站没有提供HTTPS，它并不能使你安全的连接上这个网站。）

请注意有些网站包括来自不支持HTTPS的其他网站上的图片或者图标等大量内容。一如既往，如果浏览器的锁定图标是损坏的或带有一个感叹号，你可能仍然容易受到一些敌人主动攻击或流量分析。但是，监控你浏览情况所需要投入的努力仍有效增加。

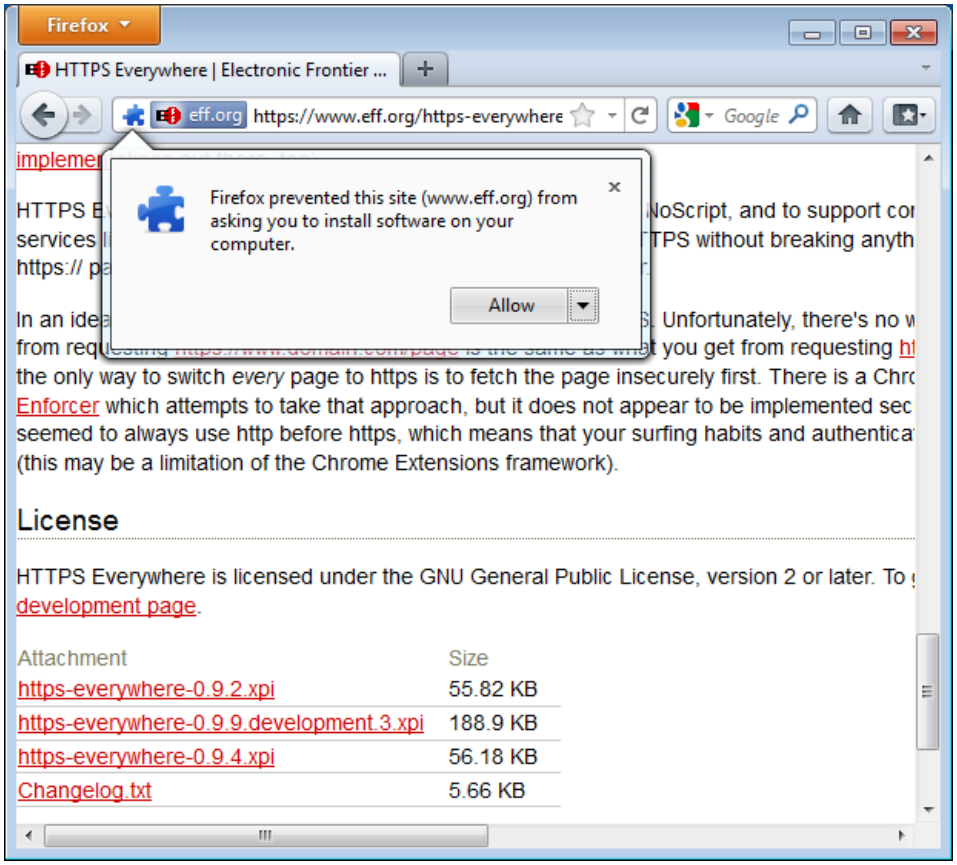
有些网站（如Gmail）自动提供HTTPS支持，但是用HTTPS Everywhere仍将保护你免受SSL-stripping攻击，如果最初你试图访问HTTP版本，攻击者从你的电脑隐藏这个网站的HTTPS版本。

更多详情请访问： https://www.eff.org/https-everywhere.

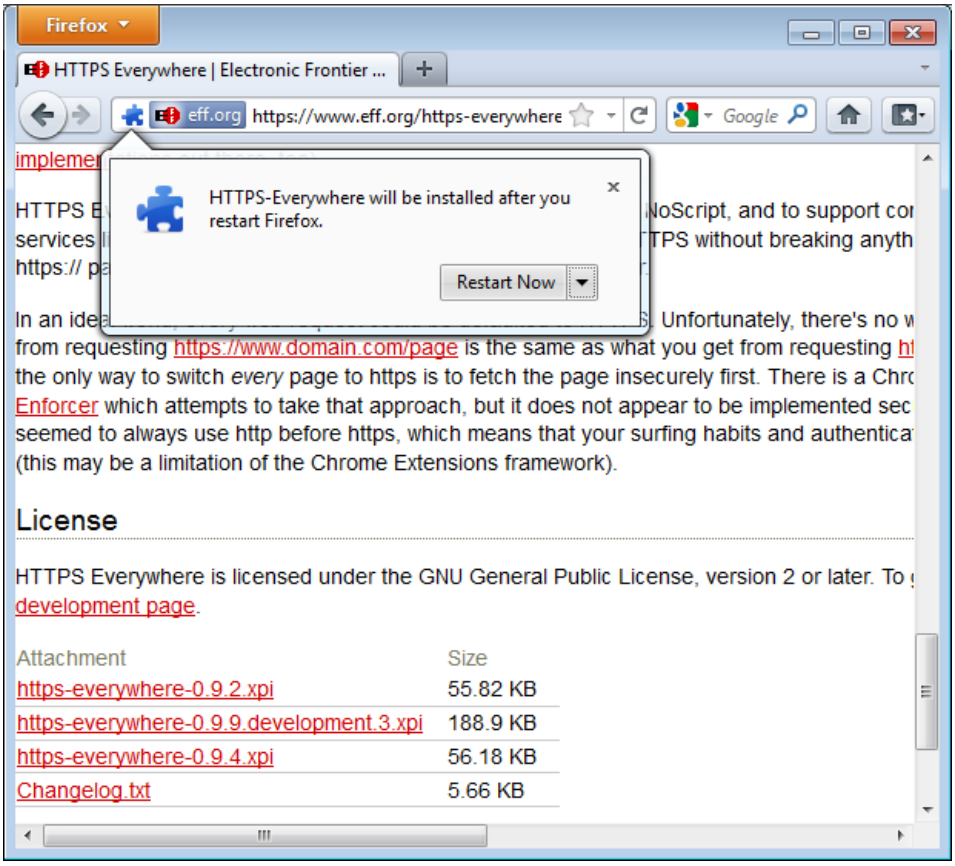
安装

首先，在官方网站下载HTTPS Everythere：https://www.eff.org/https-everywhere.

选择最新版本 （newest release）。在下面这个例子中，我们使用了HTTPS Everywhere 的 0.9.4 版本。 （一个更新的版本可能已经发布）

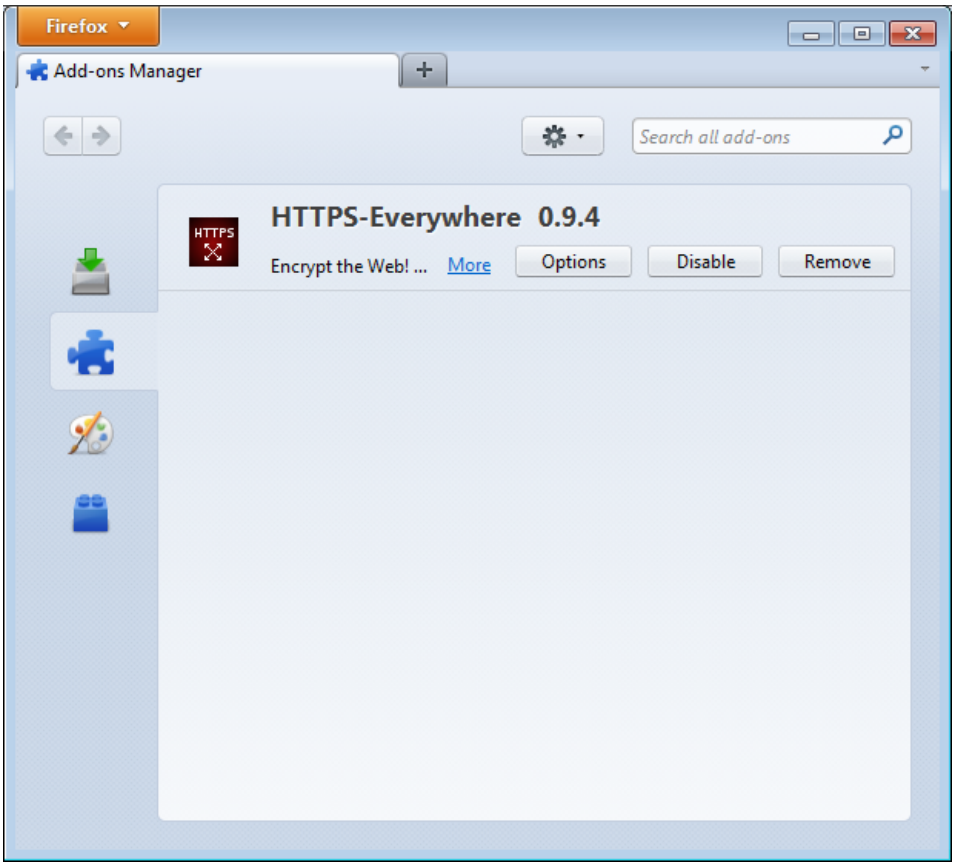


点击“允许”（ "Allow"）。然后你需要点击“现在重启”（ "Restart Now"）按钮重启Firefox。现在HTTPS Everywhere已被安装好。

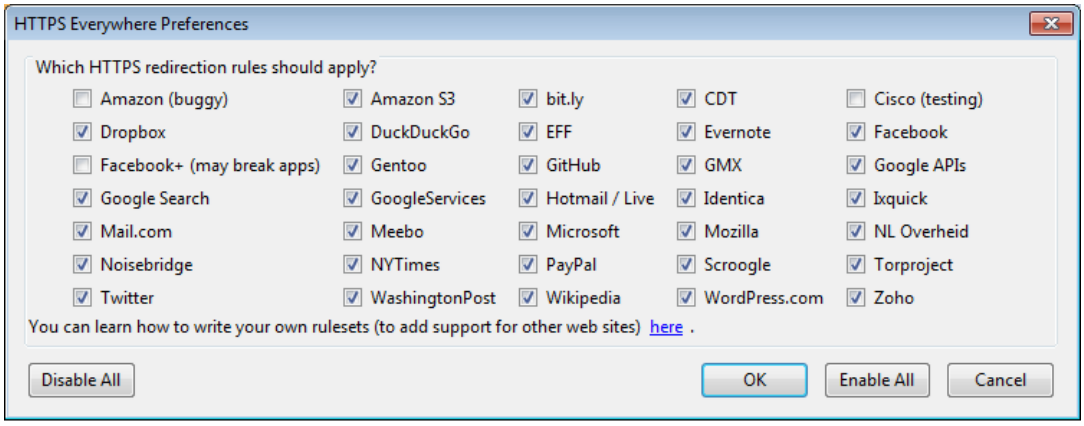


配置

点击屏幕的左上方的Firefox菜单，然后选择附加组件管理器 （Add-ons Manager），在Firefox 4 (Linux)里进入HTTPS Everywhere的设置面板（settings panel）。（注意不同版本的Firefox和不同的操作系统，附加组件管理器



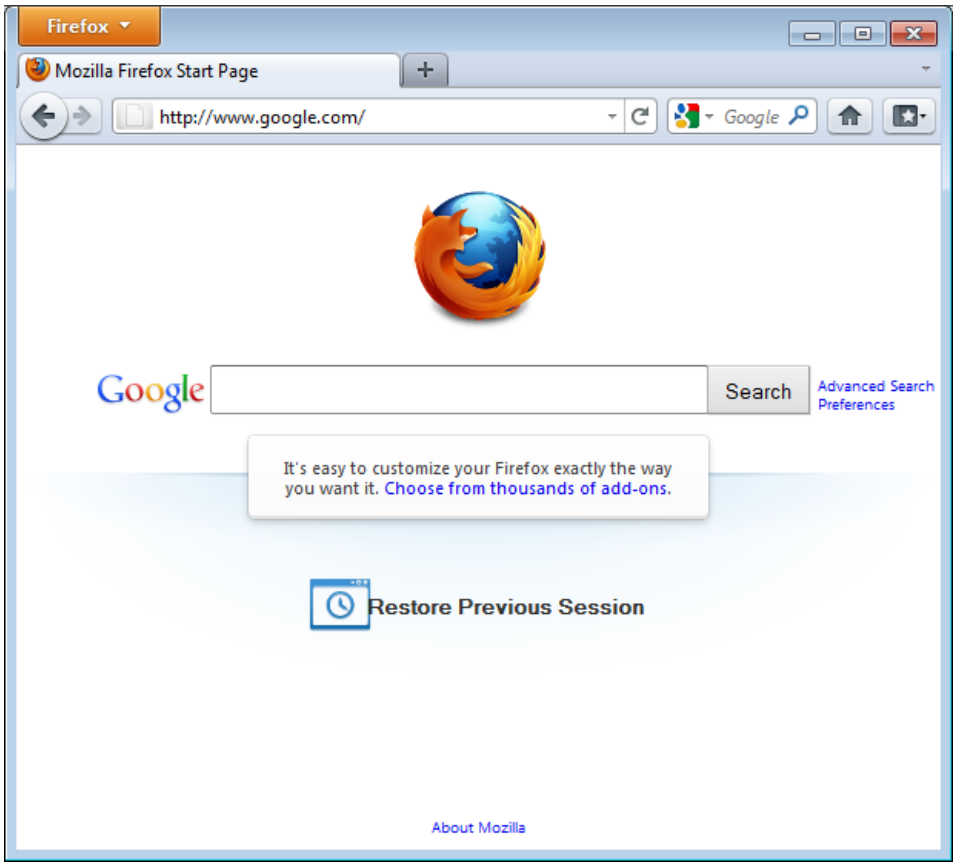
点击选项（Options）按钮。



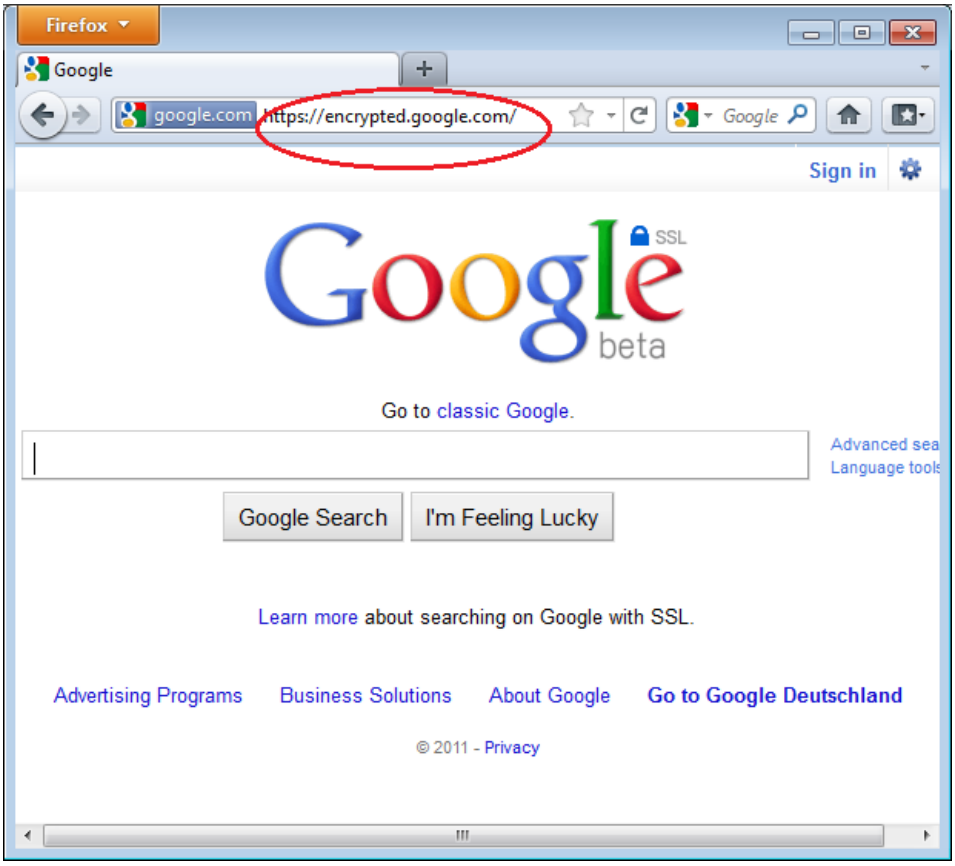
HTTPS重定向规则应适用的所有支持的Web站点的列表将显示出来。如果你有一个特定的重定向规则问题，你可以在这取消它。在这种情况下，HTTPS Everywhere不再修改你与那些特定的站点的连接。

使用

启用和配置好后，HTTPS Everywhere使用非常简单和易懂 。输入一个不安全的HTTP网址（如：http://www.google.com）。



按回车（Enter）。你将被自动重定向到安全的HTTPS加密网站(如: https://encrypted.google.com)。不需要要做别的什么。



如果网络屏蔽 HTTPS

你的网络运营商为增强其侦察你活动的能力，它可能屏蔽网站的安全版本。在这种情况下，HTTPS Everywhere可能阻止你使用这些网站，因为它强制你的浏览器只使用这些网站的安全版本，决不用不安全的版本。（例如，我们听说一个机场的Wi-Fi网络允许所有的HTTP连接，不允许HTTPS连接。可能Wi-Fi的经营商对用户的行为感兴趣，在那个机场，用户使用HTTPS Everywhere不能使用某些网站，除非它们临时禁用HTTPS Everywhere。）

在这种情况下，为了绕开网络对网站安全连接的过滤，你可以选择结合绕行技术如Tor或VPN使用HTTPS Everywhere。

在HTTPS Everywhere 新增对其他网站的支持

你可以在HTTPS Everywhere 附加组件（add-on）为自己喜欢的网站增加自己的规则。你可以在这找到方法：https://www.eff.org/https-everywhere/rulesets。增加规则的好处是它们能告诉HTTPS Everywhere如何确保你访问这些网站是安全的。但请记住：除非网站的经营者已经选择让它们的网站使用HTTPS，HTTPS Everywhere不能让你安全访问网站。如果网站不支持HTTPS，为它添加规则没有益处。

代理设置和 FoxyProxy

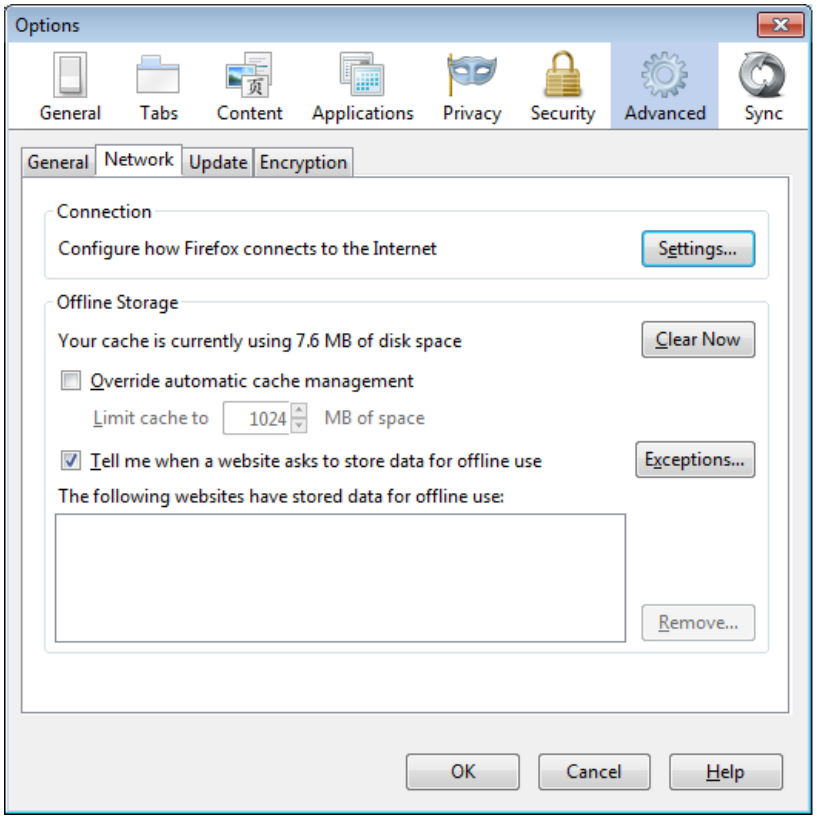
代理服务器可以让你访问一个网站或其他互联网资源，即便当直接访问已被你的国家或你的互联网服务提供商过滤。有许多不同种类的代理,包括：

- 网页代理，这只需要你知道代理网站的地址。一个网页代理的网址可能看起来像http://www.example.com/cgi-bin/nph-proxy.cgi。
- HTTP代理，需要你或者软件修改你的浏览器设置。HTTP代理只可以使用网页内容。你可以得到一个HTTP代理的信息，这样的格式："proxy.example.com:3128"或"192.168.0.1:8080"。
- SOKS代理,需要你或软件修改你的浏览器设置。SOKS代理可以使用许多不同的网络应用程序,包括电子邮件和即时通信工具。SOCKS代理信息看起来就像是HTTP代理信息。

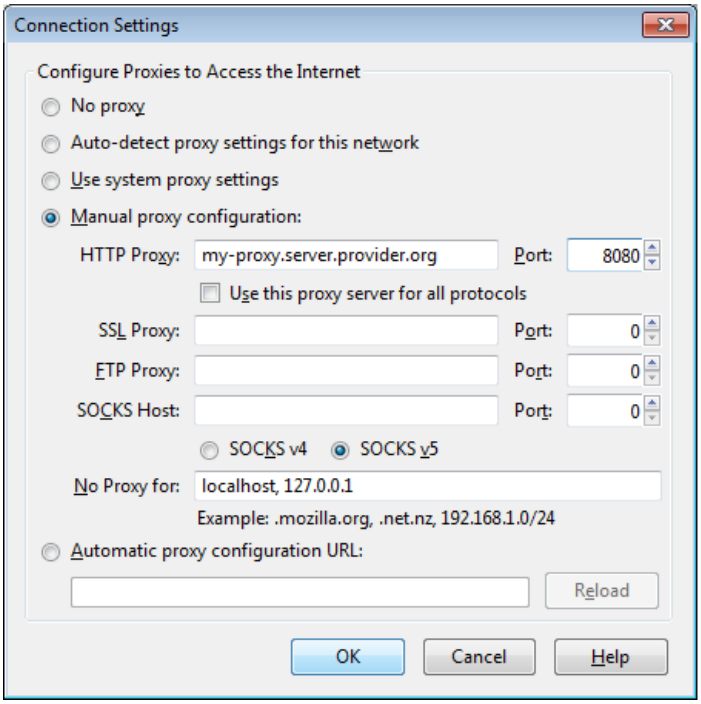
你使用网页代理无需任何配置，直接输入网址。然而，HTTP和SOCKS代理，需要在浏览器上配置。

默认火狐代理配置

在Firefox4（Linux）上，你点击你屏幕左上方的Firefox菜单，进入配置界面，然后选择选项（Options）。在弹出窗口中，选择标有高级（Advanced）的图标，然后选择"网络"（Network）选项卡。你应该看到这个窗口：



选择"设置"（Settings），单击"手动配置代理"，并输入你要使用的代理服务器信息。请记住，HTTP代理和SOCKS代理的工作方式不同，必须在相应的字段输入。如果有一个冒号（：），在您的代理信息，是代理地址和端口号之间的分隔符。你的屏幕上看起来应该像这样：



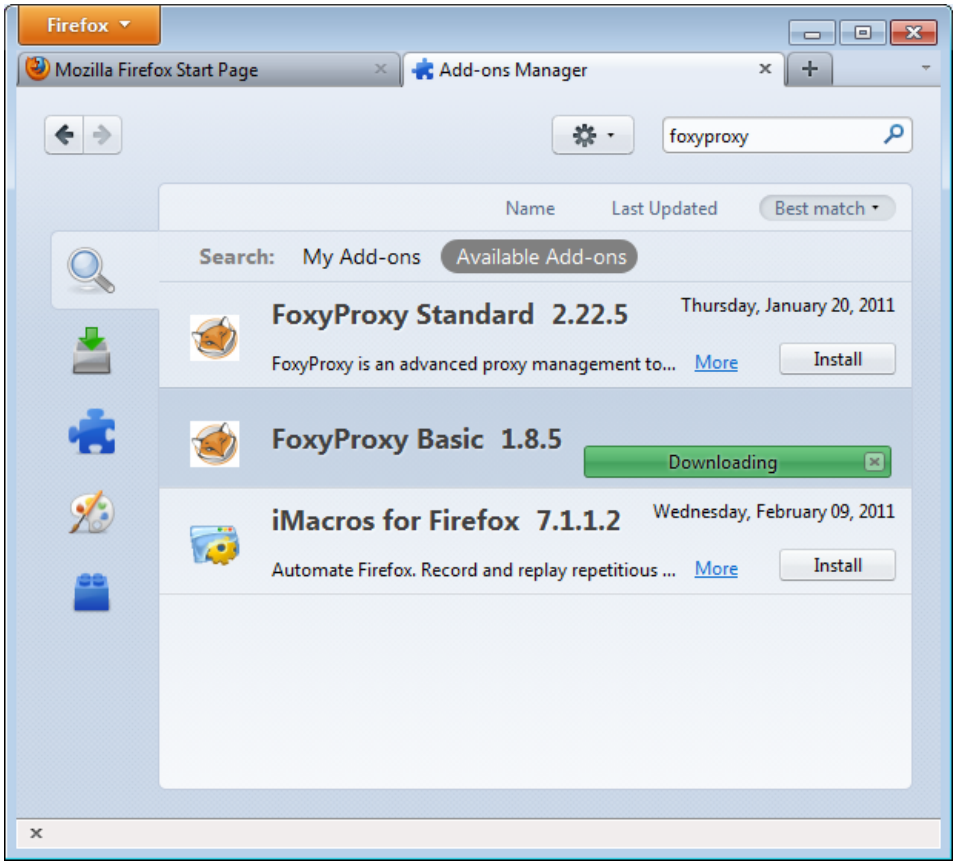
单击OK后，你的配置将被保存，你的浏览器未来的所有连接将自动通过代理连接。如果你得到一个错误信息，如“代理服务器拒绝连接”或“无法找到该代理服务器”，这个问题与你的代理配置有关。在这种情况下，重复上述步骤，并在最后一个屏幕选择“无代理”停用代理。

FoxyProxy

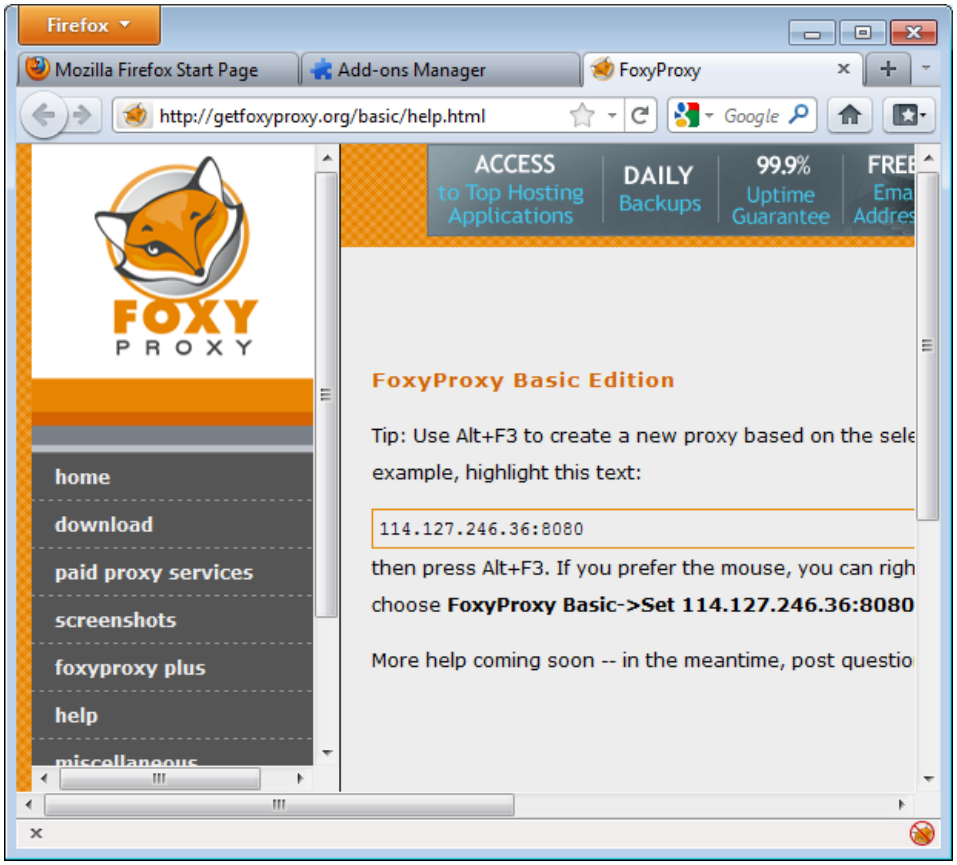
FoxyProxy是一个免费Firefox浏览器附加组件，这使得它易于管理许多不同的代理服务器，并互相切换。有关FoxyProxy的详细信息，请访问http://getfoxyproxy.org/。

安装

在Firefox4（Linux）里，在屏幕上的左上角点击Firefox菜单，然后选择附加组件。在弹出窗口中，在右上角的搜索框输入你想安装的附件组件的名称（在这种情况下是“FoxyProxy”），并单击Enter。在搜索结果中，你会看到两个不同版本的FoxyProxy：标准和基本。全面的比较两个免费版本，请访问http://getfoxyproxy.org/downloads.html#editions，但基本版已经能满足基本的绕行需要。决定你想要哪个版本后，单击“安装”。

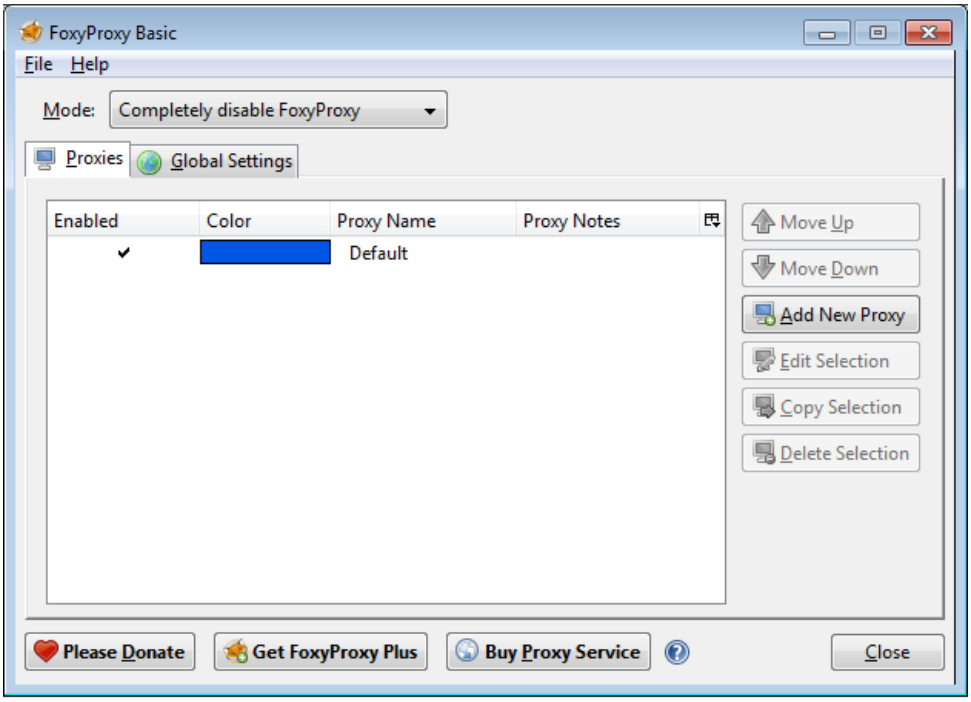


安装后，Firefox应该已重新启动，打开FoxyProxy的帮助网站。你应该看到在右下角看到FoxyProxy图标。

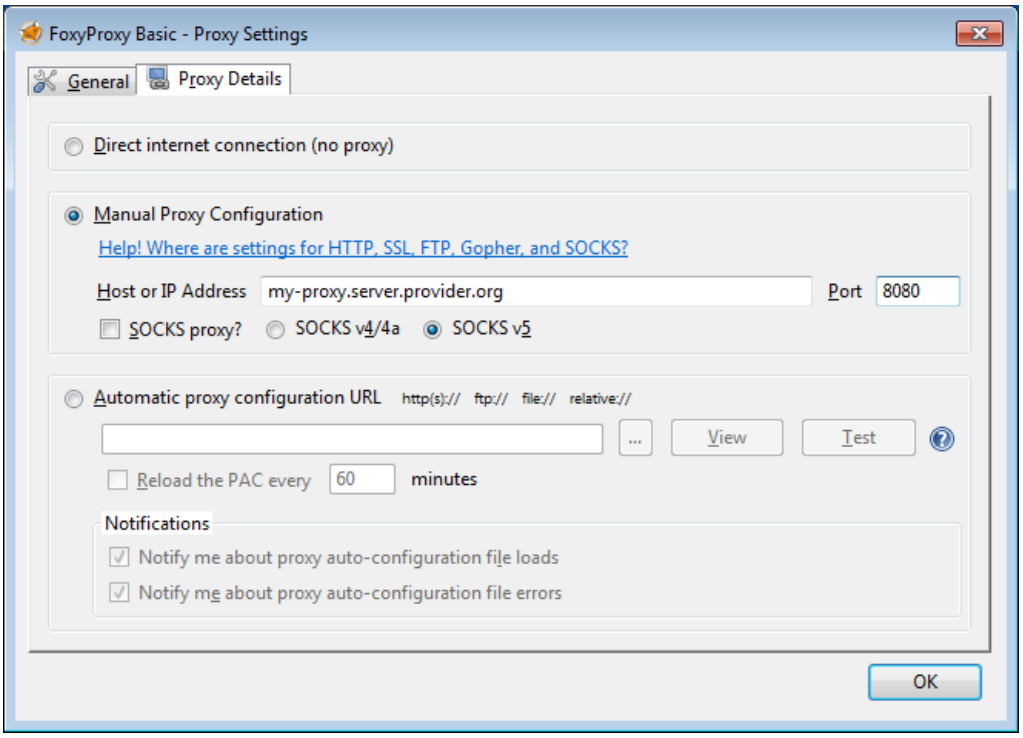


配置

为使FoxyProxy完成其工作，它需要知道使用什么代理设置。点击Firefox窗口的右下角图标，打开配置窗口。配置窗口看起来像这样：



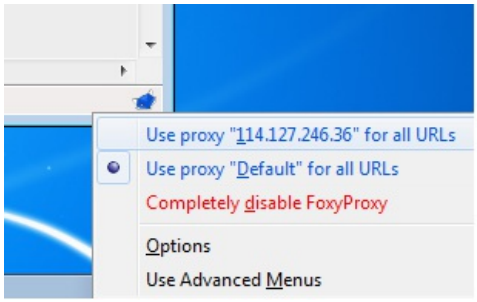
点击“添加新代理”。在下面的窗口，以Firefox的默认代理配置相类似的方式输入代理细节：



选择“手动配置代理”，在相应的输入框输入主机或IP地址和你的代理的端口。如果适用的话，检查“SOCKS代理？”，然后单击OK。重复上述步骤，你可以添加更多的代理。

使用

右击Firefox窗口的右下角的狐狸图标，可以切换你的代理（或选择不使用代理）：



要选择一个代理服务器，只需左击你要使用的代理。

TOOLS

简介

绕行互联网审查的基本思路是通过未被封锁和经非过滤连接连接到互联网的第三方服务器路由请求。本章介绍了一些使用这种服务器的工具以阻止互联网封锁、过滤和监控。选择哪种能最好实现你的目标的工具应根据你要访问内容类型的初步评估、你可用的资源和这样做的风险。

为了应对不同的障碍和威胁，人们开发了用来阻止互联网封锁、过滤和监控的工具。他们有助于：

- 绕开审查： 使你能阅读或创作内容、收发消息，以及通过绕开阻止你这么做的努力与特定的用户、网站或服务进行交流。比如通过Google缓存或RSS阅读器间接访问一个被封网站。
- 阻止窃听：保持交流的私密性，从而没人可以看到或听到你的沟通内容（但是，他们可能知道你在和谁交流）。有的工具能够绕开审查，但无法阻止窃听，仍有可能受到关键词过滤，其封锁所有含有特定被禁止词语的交流。比如，各种形式的加密技术，如HTTPS或SSH，只允许发件人和收件人读取信息。窃听者能看到哪个用户正和哪个网络服务器连接，但从内容上其只能看到一个看起来无关紧要的字符串。
- 保持匿名：没人能通过信息或者跟你交流的人识别你的交流能力-无论是你连接网络的运营商还是网站以及跟你交流的人都无法认出你是谁。许多代理服务器和代理工具都不提供完美的或任何匿名服务：代理运营商能够观察进出代理的流量以及其发送的频率；连接任一端的恶意观察者能够收集到相同的信息。像Tor一样的工具被用于通过限制网络中任一节点可以包含的关于用户身份或位置信息的数量使攻击者很难收集到关于用户的这类信息。
- 隐藏用户活动：掩饰你发出的交流信息，让间谍无法知道你在绕开审查制度 。比如，信息隐藏技术（steganography）可以把文本消息隐藏在一个普通图片文件里，根本看不出你在使用绕行工具。使用有各种不同用户的网络意味着对手因为你选择的软件而无法知道你正在做什么。当其他人使用相同的系统访问有争议的内容时，这样做特别好。

  有的工具只能通过一种方式保护你的交流信息。比如，很多代理可以绕开审查，但无法阻止窃听。你可能需要多种工具来绕过审查，明白这一点很重要。

在不同情况下每种保护措施都和不同的人群有关。当你选择工具绕过网络审查时，你应该记住自己需要哪种保护，以及你所采用的工具能否提供这种保护。比如，如果有人发现你试图绕过审查系统会怎么样？你这样做时是否要访问你的主要内容或者你是否需要继续匿名。

有时，一个工具可以同时做到绕开审查和匿名保护，但是所涉及的步骤各不相同。比如，Tor软件通常可以用来达到这两个目的，但是Tor用户关心的侧重点不同，使用Tor的方法也不同。出于匿名的目的，使用捆绑了Tor的网络浏览器很重要，因为它已被修改为阻止泄露你的真实身份。

重要警告

经过足够努力，网络运营商和政府机构可以发现大多数绕行工具，因为这些工具产生的流量具有特定性。这一点对于不使用加密技术的绕行方法来说肯定适用，但是也可能适用于采用加密技术的方法。如果你通过技术绕开过滤，很难不被发现，尤其是如果你使用非常流行的技术，或者长期使用同一种服务或方法。此外，也有一些方法不需要技术就可以发现你的活动：亲自观察、监测以及很多其他传统的手工信息收集方法。

我们无法就威胁分析及处理威胁的工具提供具体建议。情况和国家不同，风险也不一样，而且风险也在不断变化。你应该明白那些试图限制你的交流和活动的人会不断改进自己的手段。

如果你做的事情会让你在所在地区遇到风险，你应该自己判断安全状况，并且（如果可能）向专家咨询：

- 大多数情况下，你必须依靠陌生人提供的服务。请注意，他们可能对有关你从哪来、你正访问的网站甚至是你在未加密网站输入的密码等信息有访问权限。即使你认识且相信运行单跳代理或VPN的人，他们也可能被入侵或被强迫提供你的信息。
- 请记住，不同系统做出的匿名和安全承诺可能并不准确。你需要独立证实。开源工具可以由技术娴熟的朋友评估。开源工具中的安全漏洞可以被志愿者发现并解决。专有软件却很难做到一样。
- 实现匿名或安全可能要求你遵守纪律并认真遵守一定的安全程序和做法。忽视安全程序可能极大地减少你获得的安全保护。认为有你匿名或安全的“一键解决办法”是很危险的。例如，通过代理或Tor路由你的连接是不够的。请务必使用加密，维护你的计算机安全，避免在你发布的内容中泄露你的身份。
- 请注意，他人（或政府）可能会设置诱捕系统（honeypots），这些虚假网站会假装提供安全交流或审查绕行，但实际上会从不知情用户身上收集信息。
- 有时，甚至连像恶意软件般活动的“Policeware”也可能会被或远程或直接地安装到用户的计算机上，其会监控计算机上的所有活动，即使在计算机未连接到互联网时也一样，而且其还会破坏大部分其他预防性安全措施。
- 请注意非技术威胁。如果有人偷了你的或你的好友的计算机或者手机，会有什么后果？如果网吧工作人员偷看或将摄像头指向你的屏幕或键盘怎么办？如果有人在你朋友忘记登出帐户的网吧计算机旁坐下并假装成她给你发送信息，会有什么后果？如果你社交网络中有人被捕或被迫交出密码怎么办？

- 如果法律和法规限制或禁止你正在访问的内容或者你正在从事的活动，一定要小心可能发生的后果。

若想了解更多数字安全和隐私知识，请阅读：

http://www.frontlinedefenders.org/manual/en/esecman/intro.html
http://security.ngoinabox.org/html/en/index.html

自由门（Freegate）

自由门是为Windows用户使用的代理工具，最初由DIT- INC开发，可以绕过中国和伊朗的网络审查。

一般信息

Supported operating system	
Localization	English, Chinese, Persian, Spanish
Web site	http://www.dit-inc.us/freegate
Support	Forum: http://www.dit-inc.us/support

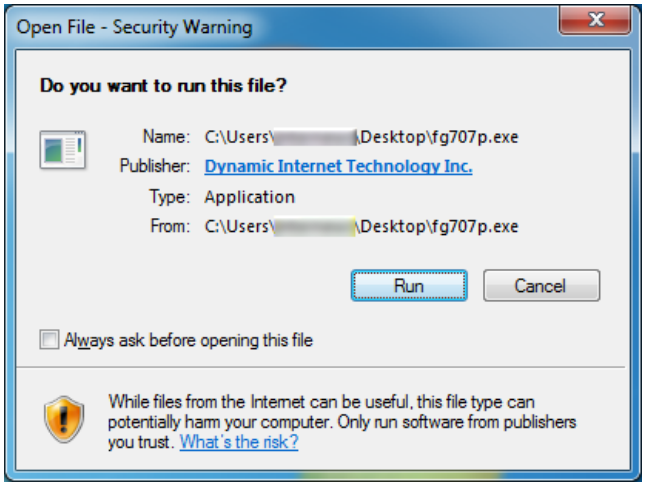
如何获得自由门

您可以在http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/Freegate.shtml上免费下载这个软件。

你会得到一个后缀名.zip的文件，你必须先解压。右击下载的文件，并选择“全部解压”，然后点击“加压”按钮。生成的文件大约1.5 MB。可执行文件的名称可能看起来像一系列字母和数字（如“fg707p.exe”）。

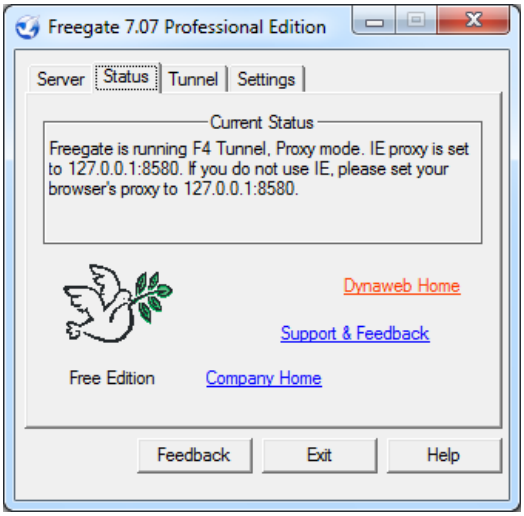
安装

当你第一次运行这个应用程序，你可能会看到一个安全警告。您可以接受此安全警告，通过取消选中复选框“打开此文件前总是询问”，单击“运行”。



运行自由门

现在，应用程序已启动，并自动连接到服务器。



安全通道已成功启动时，你会看到自由门的状态窗口，将自动打开一个新的Internet Explorer，加载网址为http://dongtaiwang.com/loc/phome.php?v7.07&l=409的页面，这取决于你的版本和语言。这是确认你正在的通过一个加密的通道正确地使用自由门。

如果一切顺利，你就可以开始使用自动打开的Internet Explorer窗口正常地浏览，绕过互联网审查。

如果你想使用自由门运行另一个应用程序（如Firefox浏览器或Pidgin即时通信客户端），你将不得不对它们进行配置它们使用自由门作为一个代理服务器。 IP是127.0.0.1，端口是8580。

在自由门设置选项卡下，你可以从英文、繁体中文、简体中文，波斯文和西班牙文中选择界面语言。在状态下，你可以跟踪你通过自由门网络的上传/下载的流量。 服务器选项卡允许你从几个服务器中挑选，其中有一个可能会快于当前连接。

Simurgh

Simurgh（波斯语中意指凤凰）是一个轻量级的独立的代理软件和服务。就是说不需要事先安装什么或者拥有对电脑的管理权限。你可以复制它到你的USB闪盘在合用的电脑上使用（如在网吧）。

一般信息

Supported operating system	
Localization	English
Web site	https://simurghesabz.net
Support	E-mail: info@simurghesabz.net

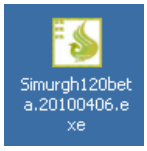
下载 Simurgh

欲使用Simurgh的服务， 从https://simurghesabz.net/免费下载工具。

可以在Microsoft Windows的所有版本上使用。文件小于1MB，所以即便是在网速慢的情况下仍能在在合理的时间内下载完。

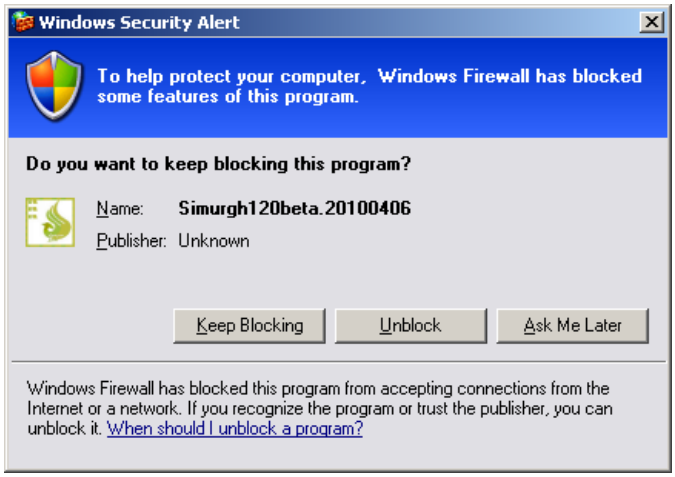
使用 Simurgh

点击已下载好的文件启动Simurgh。使用Microsoft Internet Explorer下载的文件默认保存在你的桌面，使用Mozilla Firefox下载的文件默认保存在“我的文件”的"Downloads"里。

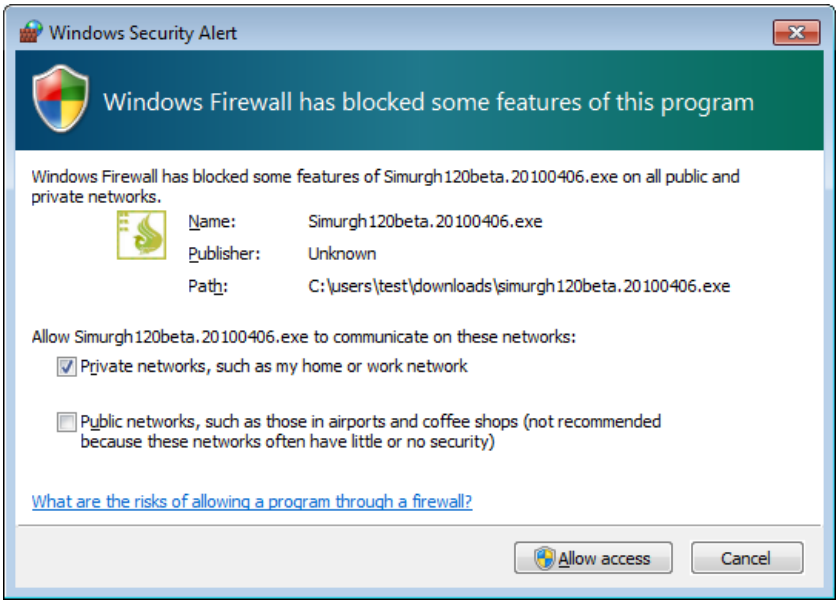


注意：当你第一次使用Simurgh，你可能会遇到Windows安全警告，询问你是否阻止Simurgh。因为Simurgh需要联网，为使它能使用，选择“解除组织”或者“允许访问”（取决于你Microsoft Windows的版本）很重要。

你可能见到这个警告窗口：



或这个：

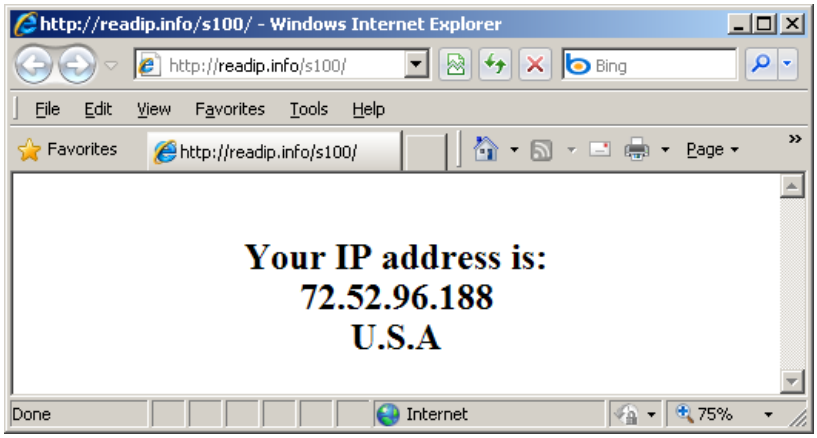


成功启动Simurgh后, 点击开始（Start）建立安全连接。

当开始（Start）按钮变成结束（Stop）按钮后，Simurgh已成功连接上其服务器。

确保你已连接上Simurgh的服务器

现在你Internet Explorer浏览器将会打开一个测试页面的新窗口。如果你看到你的连接来自其他国家，如美国，这证实Simurgh已成功改变你浏览器的设置，你自动地正在安全的Simurgh连接上冲浪。

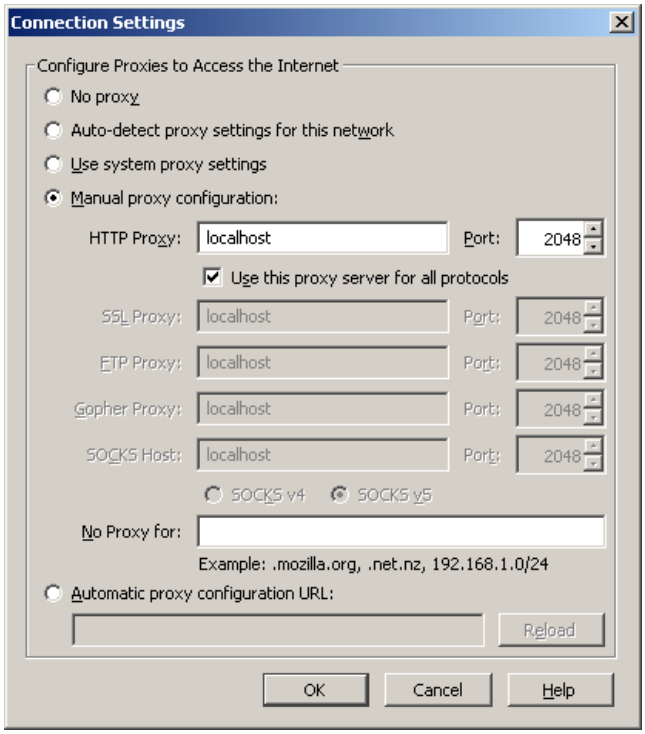


你也能使用http://www.geoiptool.com 这个网站来检查你的连接来自何处.。如果网站显示你的位置非常遥远（在其他国家，如美国），你正在使用you 安全的Simurgh连接。

在Mozilla Firefox （火狐）使用Simurgh

为使用其他的浏览器如Mozilla Firefox，你需要配置它，使用HTTP代理“localhost”，端口为2048.

在Firefox中，你可以找到代理设置通过工具（Tools）› 选项（Options）› 网络（Network）› 设置（Settings）。
如下面的截图所示在“连接设置”（"Connection settings"）窗口选择“手工代理配置” "Manual proxy configuration" ，输入 "localhost" (没有引号) 作为HTTP 代理，端口为2048。点击 OK，接受新的设置。



无界浏览

无界浏览是极景网络公司开发的一款代理工具，旨在帮助中国网民绕过他们的审查。它可以为其他国家的用户工作。

一般信息

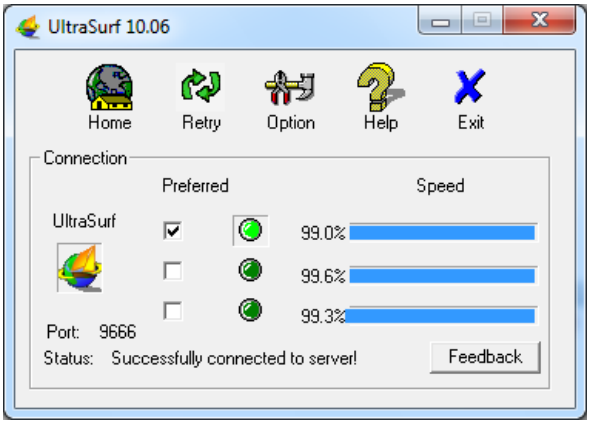
Supported operating system	
Localization	English
Web site	http://www.ultrareach.com
Support	FAQ: http://www.ultrareach.com/usercenter_en.htm

怎样得到无界浏览

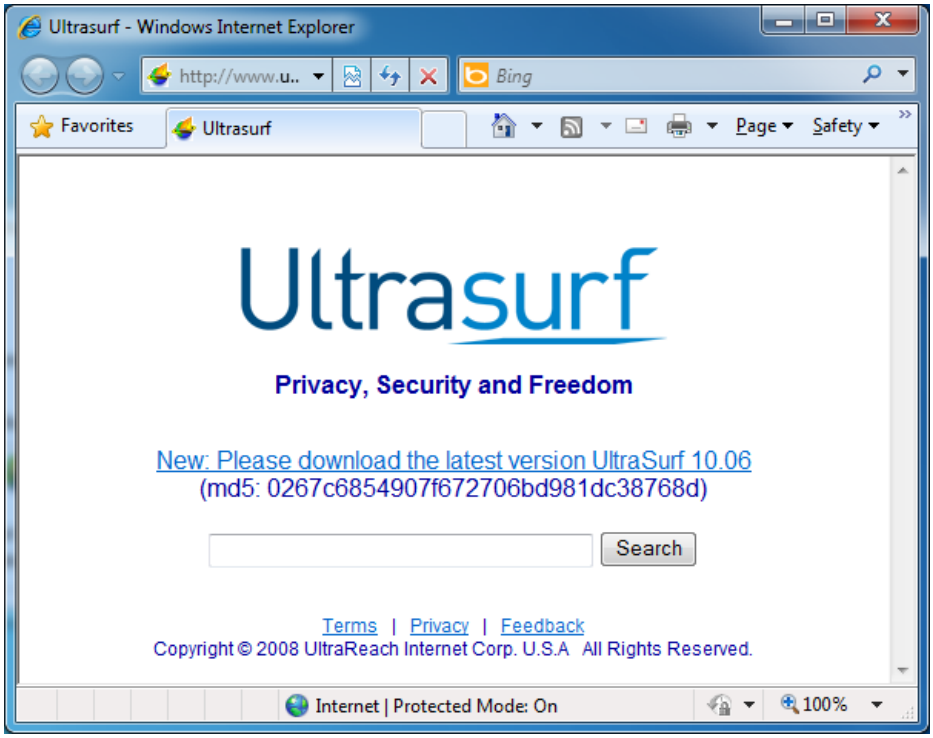
你可以从http://www.ultrareach.com，http://www.ultrareach.net/或者http://www.wujie.net (后面的网页是中文的，但是仍然容易下载，下载是英文的)。

安装和使用无界浏览

一旦你已经下载好命名类似“u1006.zip”（根据版本号）的文件，通过右键点击该文件，并选择“全部解压”，将它解压。双击新的“u1006”图标来启动该应用程序。



无界浏览将自动打开Internet Explorer并显示无界浏览的搜索页面http://www.ultrareach.com/search.htm。你现在就可以使用无界打开的Internet Explorer开始浏览。



如果你想用无界浏览使用另一个应用程序（例如Firefox浏览器或Pidgin即时通信客户端），你需要对它们进行配置，使用无界浏览的客服端作为代理服务器：IP是127.0.0.1（你的电脑，也被称为“localhost”），端口是9666。

您可以通过点击无界浏览主窗口中的“帮助”，打开无界浏览用户指南。

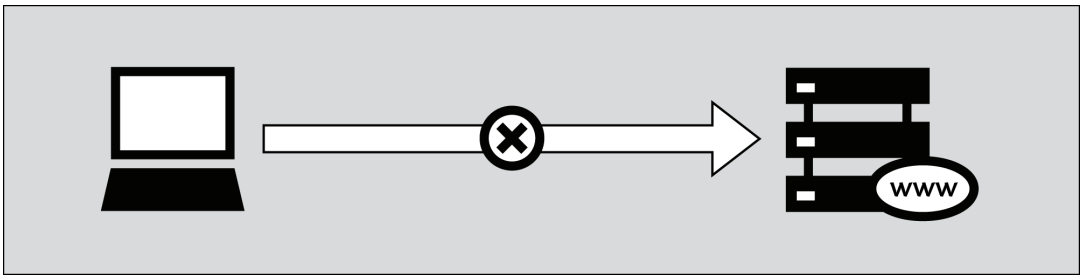
中文无界浏览信息(wujie)：http://www.internetfreedom.org/UltraSurf：
中文用户指南：http://www.wujie.net/userguide.htm

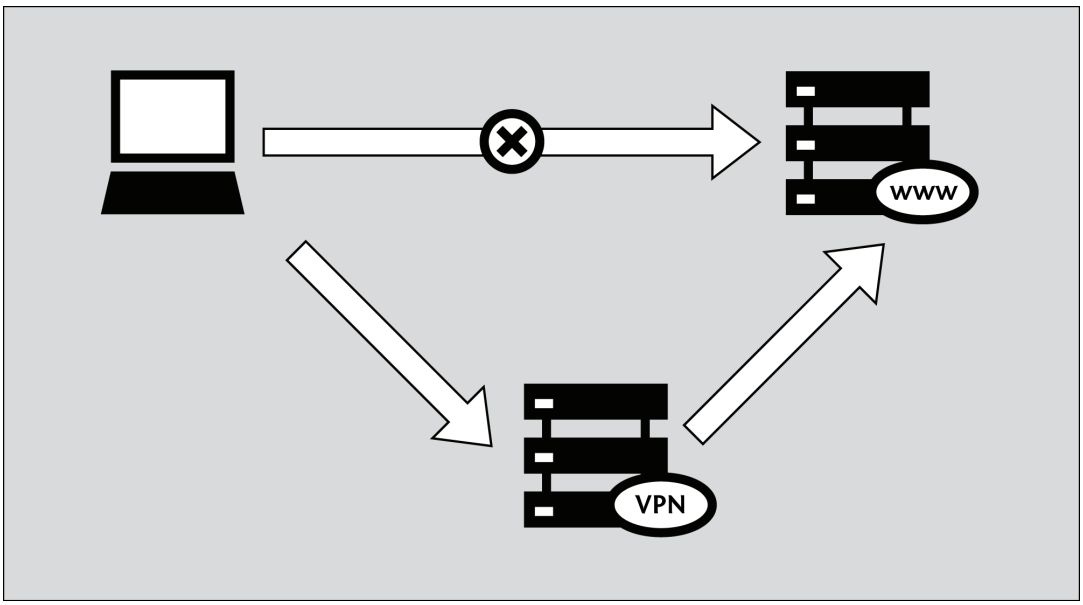
VPN 服务

VPN（虚拟专用网络）加密你与其他计算机之间的所有互联网连接并为其建立隧道。该计算机可能属于一个商业化虚拟专用网络服务、你的机构或你信任的联系人。

由于虚拟专用网络服务为所有的互联网连接建隧道，故其可被用于电子邮件、即时消息、语音IP电话（VoIP）及其他任何添加到网络浏览器的互联网服务，从而使沿途的任何人都不能阅读通过该隧道环游的一切。

如果该隧道终止于互联网被限制的区域之外，那么其可以一种有效的绕行方法，因为过滤主体/服务器只能看到加密的数据却没有办法知道哪些数据正穿过隧道。其还有一个附加效果就是使你所有不同种类的连接对窃听者来说看起来都差不多。





由于许多跨国公司使用VPN技术允许其需要访问敏感财务或其他信息的雇员通过互联网从家里或其他远程地点访问公司的计算机系统，VPN技术比起只用于绕行目的的技术来更不大可能被封锁。

重要的是，要注意数据只加密到隧道的尽头，然后未加密传输到其最终目的地。例如，如果你设置一条隧道到一个商业化虚拟专用网络提供商，然后请求网页http://news.bbc.co.uk通过该隧道，数据从你的计算机到另一端虚拟专用网络提供商的计算机将被加密，但从该处起，它将未加密到BBC运行的服务器，就像正常互联网连接一样。这意味着，理论上，该虚拟专用网络提供商、BBC和任何控制这两个服务器之间系统的人都可以看到你发送或请求了什么数据。

使用虚拟专用网络服务

虚拟专用网络服务不一定要求客户端软件的安装（许多依赖于Windows,、Mac OS或GNU/Linux中已有的虚拟专用网络支持，因此不需要额外的客户端软件）。

使用虚拟专用网络服务要求你相信该服务的所有者，其提供了一种简单便利的绕开互联网过滤的方法，它可以是免费的或收取一般在5到10美元之间的月租费，具体数额取决于该服务。免费服务往往或者是靠广告支持，或者是限制带宽和/或在特定时期内允许的最大流量。

流行的免费虚拟专用网络服务有：

• 热点保护盾，https://hotspotshield.com

根据一份2010年来自伯克曼中心的报告，热点保护盾很大程度上是最流行性的虚拟专用网络服务。如需关于如何获取和使用热点保护盾的更多详细信息，请查阅本手册的“热点保护盾”章。

• UltraVPN, http://www.ultravpn.fr

• FreeVPN, http://www.thefreevpn.com

• CyberGhost, http://cyberghostvpn.com

• Air VPN, https://airvpn.org

Air VPN通过请求为活动家提供不限制带宽或流量且没有广告的免费帐户。

• Vpnod, http://www.vpnod.com

• VpnSteel, http://www.vpnsteel.com

• Loki Network Project, http://www.projectloki.com

• ItsHidden, http://itshidden.com

付费虚拟专用网络服务的例子包括Anonymizer、GhostSurf、XeroBank、HotSpotVPN、WiTopia、VPN Swiss、Steganos、Hamachi LogMeIn、Relakks、Skydur、iPig、iVPN.net、FindNot、Dold、UnblockVPN和SecureIX。

你可以在http://en.cship.org/wiki/VPN找到一份免费和付费虚拟专用网络提供商的列表，上有他们的月租费和技术功能。

虚拟专用网络标准和加密

对于虚拟专用网络的设置，有许多不同的标准，其中包括网络协议安全（IPSec），安全套接协议层/传输层安全（SSL/TLS）以及传输层安全（PPTP），这些标准在复杂程度，提供的安全等级，以及适用的操作系统方面有所不同。而且不同功能的软件对这些标准的实现也有许多不同方式。

• 我们知道与网络协议安全和安全套接协议层/传输层安全相比，传输层安全的保密性相对要弱一些，它也许可以绕过互联网封锁，而且微软Windows操作系统的多数版本都内置有传输层安全客户端软件。

• 基于安全套接协议层/传输层安全的虚拟专用网络系统设置上相对简单，而且也提供了可靠的安全等级

• 网络协议安全（IPSec）是在网络层运行的，在互联网的架构里面，它负责数据包的传输，而其他协议都是运行在应用层的。这使得网络协议安全标准更具灵活性，因为它可以用来保护所有更高层的协议，但也难以设置。

设置你自己的虚拟专用网络服务

作为商业化付费虚拟专用网络服务的替代品，用户如果在那些网络不受限的国家有联系人，其可以让这些联系人下载并安装用于架设私人虚拟专用网络服务的软件。这需要有用户比较好的技术知识，但是这种虚拟专用网络将会是免费。这类私人架设的虚拟专用网络跟那些商业化的虚拟专用网络相比被封锁的可能性更小。其中一个常用来架设此类私人虚拟专用网络的免费开源程序就是OpenVPN(http://openvpn.net/)，该程序可以在Linux，MacOS，Windows以及其他许多操作系统中安装。

要了解如何设置一个OpenVPN系统，请参阅本手册的“使用OpenVPN”章。

优点

虚拟专用网络提供商加密你的数据传输，因此它是绕开互联网审查的最安全方式之一。一旦配置好，使用起来很方便易懂。

虚拟专用网络最适合有技术能力也有需求的用户使用，这些用户不仅仅要求为网络连接提供安全的绕行服务，他们也希望能在自己的计算机上安装一些额外的软件，然后通过自己的计算机访问互联网。如果用户所处地区的互联网遭到审查，而且用户在其他互联网未遭过滤的地区找不到值得信赖的人，那么虚拟专用网络是一个不错的选择。虚拟专用网络是一种常见的商务应用，不太可能被封锁。

缺点和风险

一些知名的商业化虚拟专用网络（特别是那些免费的）可能已经被过滤了。在网吧和图书馆这类无法安装软件的公共上网场所，用户通常无法使用这些服务。虚拟专用网络的使用可能比其他绕行方法需要更高级别的专业技术知识。

网络运营商可以检测到虚拟专用网络正被使用，而且也可以判断虚拟专用网络的提供商是谁。但是，除非虚拟专用网络设置不正确，网络运营商是无法查看通过虚拟专用网络发送的通讯的。

除非你为你的通讯使用一些额外的加密，比如针对网络连接的HTTPS，虚拟专用网络运营商（更像一个代理运营商）可以看到你正在做什么；没有额外的加密，你必须相信虚拟专用网络或隧道运营商不会滥用这个权限。

在 Ubuntu 上使用VPN

如果你使用Ubuntu作为你的操作系统，你可以使用内置的NetworkManager和免费OpenVPN 客户端连接VPN。

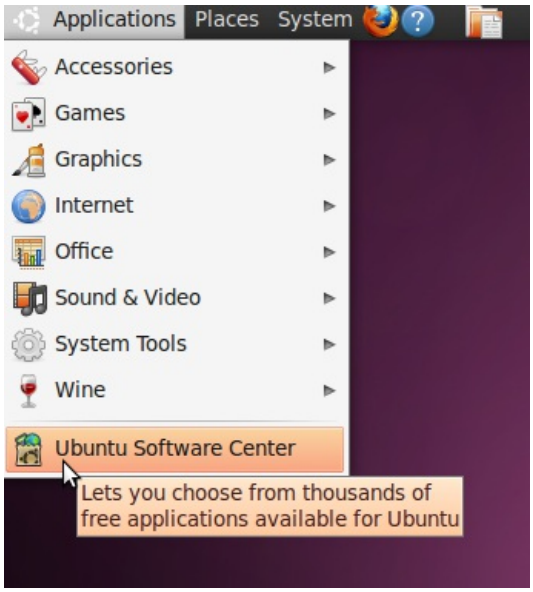
OpenVPN允许你使用多种验证方法连接VPN网络。举个例子，我们将知道怎样使用免费的VPN服务AirVPN连接VPN服务器。不管你使用哪款VPN服务，在Ubuntu上使用OpenVPN配置过程是一样的。

为 NetworkManager 安装OpenVPN

网络实用工具NetworkManager可以让你你打开或者关闭VPN连接，默认安装在Ubuntu内，你可以在你屏幕的通知区域找到它，挨着系统时钟。

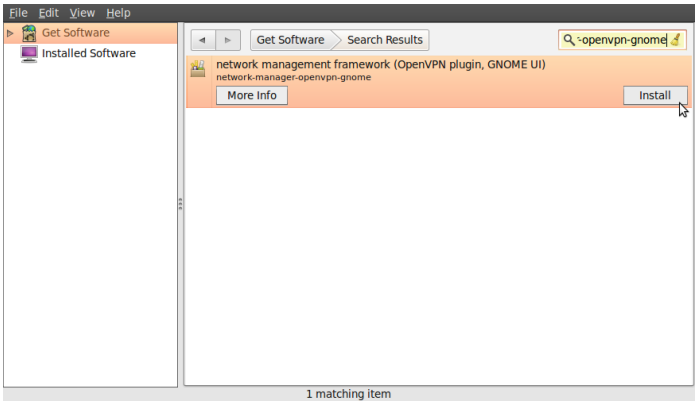
下一步，从Ubuntu软件中心（Ubuntu Software Center）找到可以与NetworkManager一起工作的OpenVPN扩展。

1. 在屏幕左上方应用程序菜单（Applications menu）打开Ubuntu软件中心（Ubuntu Software Center）

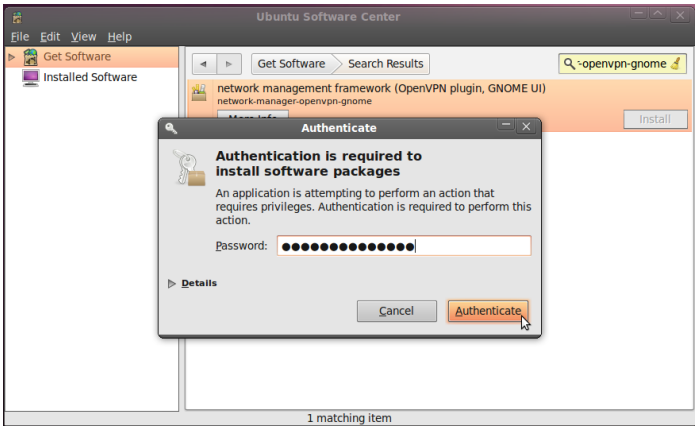


2. Ubuntu软件中心（Ubuntu Software Center）可以让你搜索、安装和卸载软件。点击窗口右上方的搜索框。

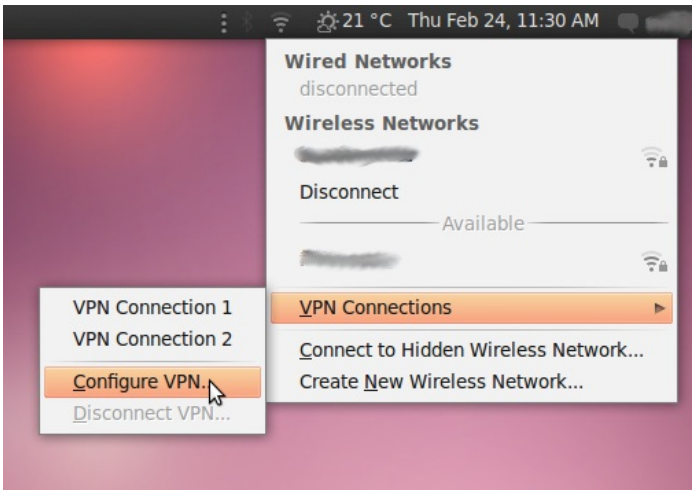
3. 在搜索框输入"network-manager-openvpn-gnome"（可以启动OpenVPN的NetworkManager扩展）。程序包包含了你需要成功建立VPN连接的所有文件，包括OpenVPN客户端。点击安装（Install）。



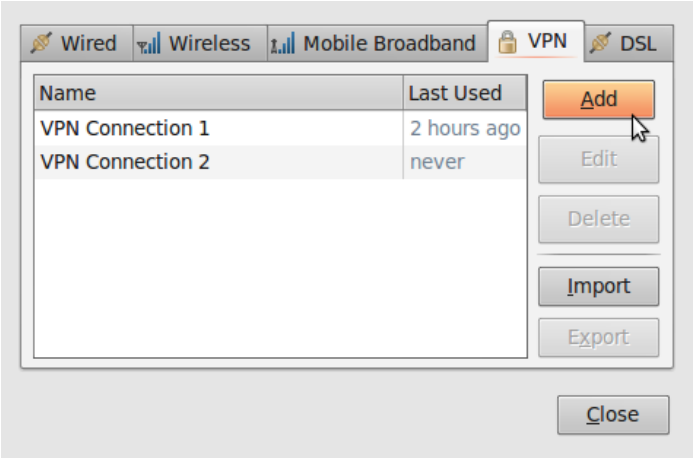
4. Ubuntu可能提示你需要安装软件的额外权限。如果这样的话，输入你的密码点击验证（Authenticate）。程序包安装好后，你可以关闭Ubuntu软件中心（Ubuntu Software Center）。



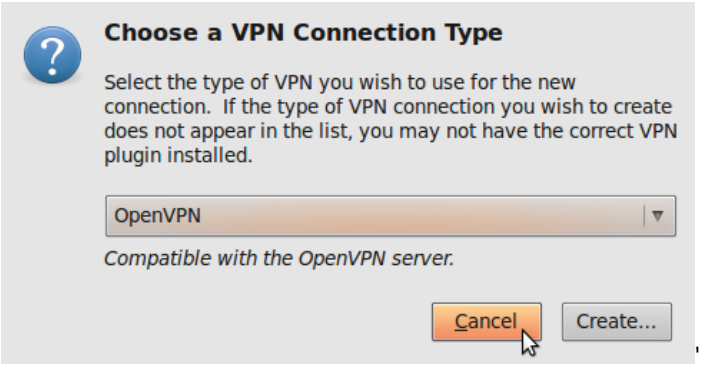
5. 检查OpenVPN是否已正确安装，点击NetworkManager（图标在系统时钟的左边），选择VPN连接（VPN Connections）> 设置VPN （Configure VPN）。



6. 在VPN选项卡上点击添加（Add）。



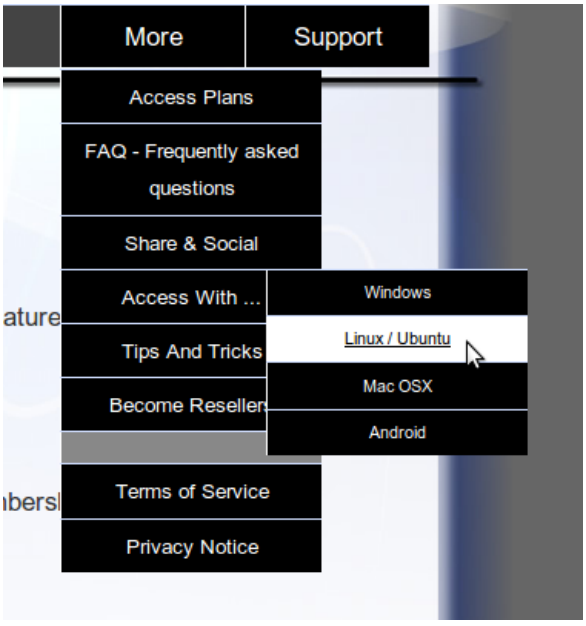
7. 如果你能看到OpenVPN选项，这意味着你已成功在Ubuntu上安装OpenVPN客户端。点击取消（cancel），关闭NetworkManager。



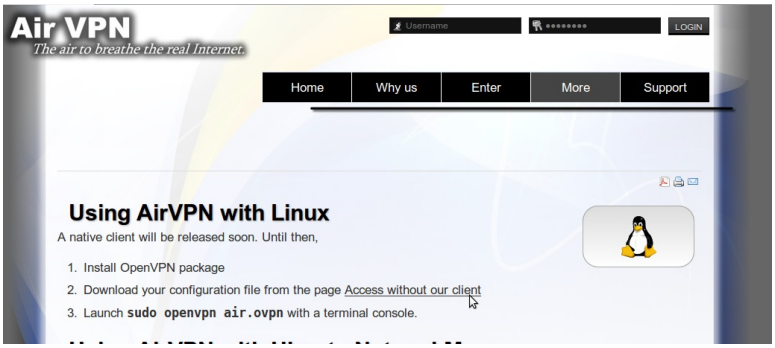
注册一个AirVPN帐号

AirVPN(http://www.airvpn.org)是一款免费服务，但是你需要在它们网站上注册，为你的VPN连接下载配置文件。

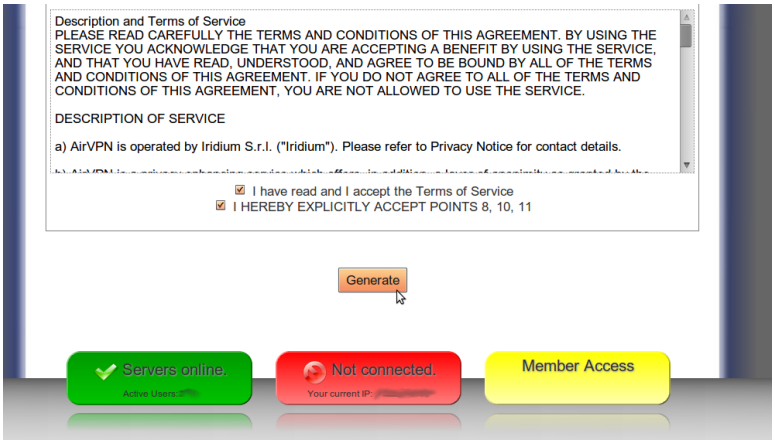
1. 访问https://airvpn.org/?option=com_user&view=register，注册一个免费帐号。确保你选择了一个强密码，因为它将是你使用VPN的密码。（阅读本书“威胁和威胁评估”这一章获得强密码的贴士。）
2. 在AirVPN 的网站导航菜单，选择More > Access with... > Linux/Ubuntu。



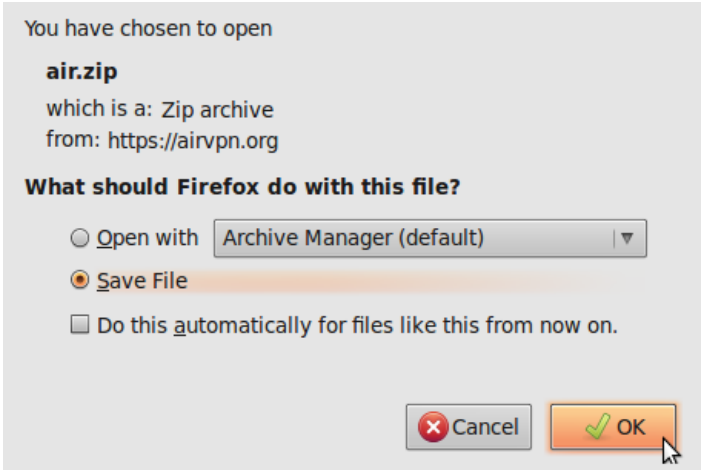
1. 点击"Access without our client"，将会被要求输入你注册时使用的用户名和密码。



2. 选择你想在NetworkManager设置的VPN模式（那我们来说，我们使用"Free - TCP - 53"）其他选项为默认。确保你已检查页面底部的服务条款合同，然后点击生成（Generate）。



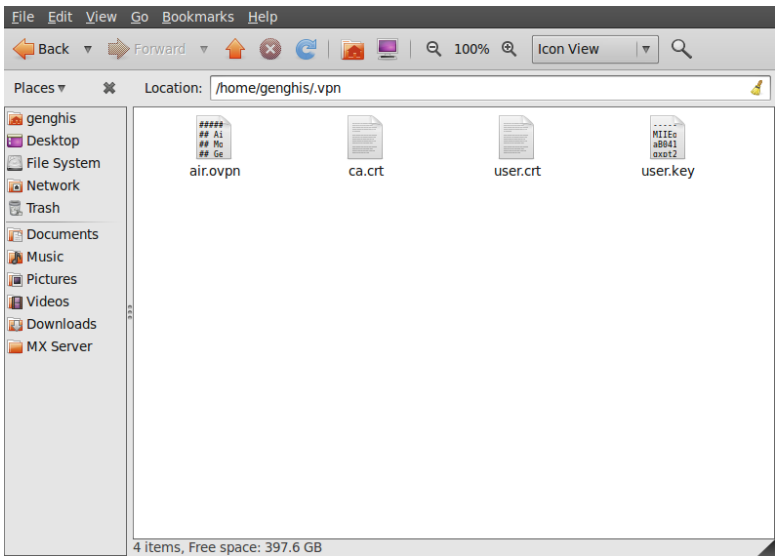
3. 一个弹出窗口告诉你air.zip文件已可以下载。它包含配置文件和你连接VPN所需的证书，点击OK。



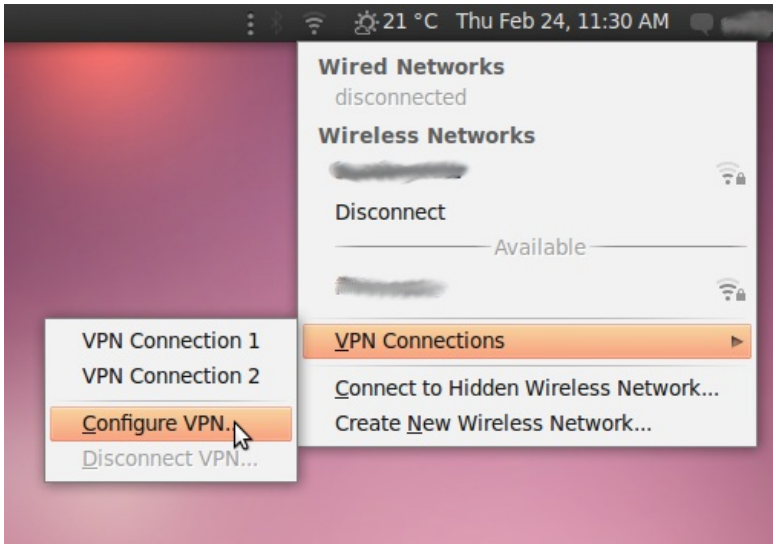
在NetworkManager配置AirVPN

现在你有配置文件和证书，你可以配置NetworkManager连接AirVPN服务。

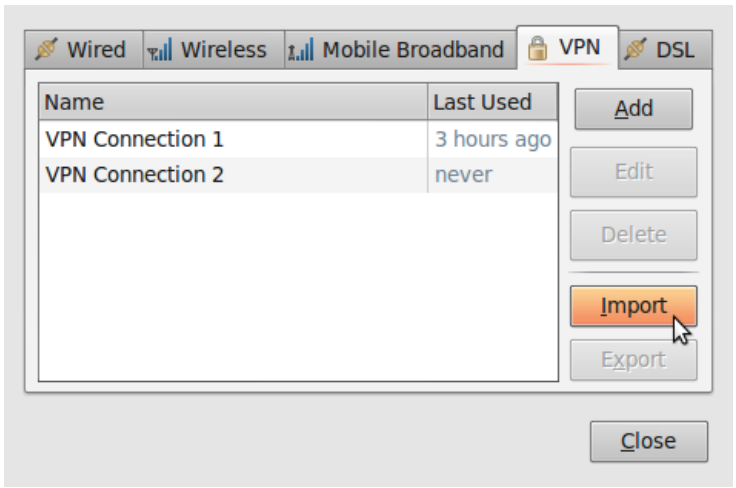
1. 解压你下载的文件到你硬盘的一个文件夹（如"/home/[yourusername]/.vpn"）。你现在应该有四个文件。"air.ovpn"文件是你需要导入NetworkManager的配置文件。



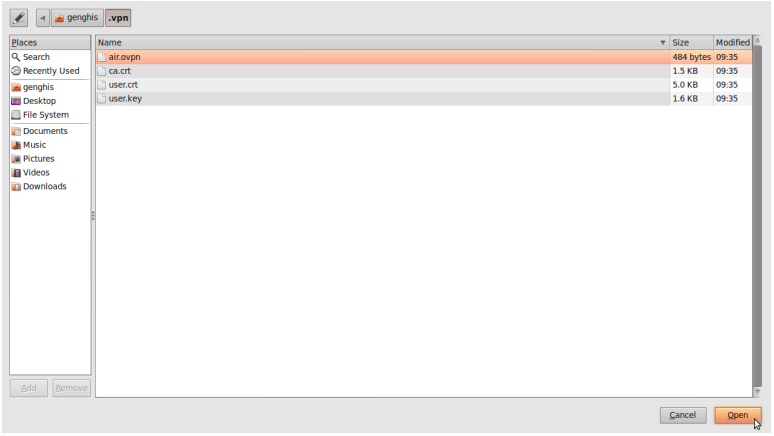
2. 打开NetworkManager，前往VPN 连接（VPN Connections ）> 配置VPN （Configure VPN），导入配置文件



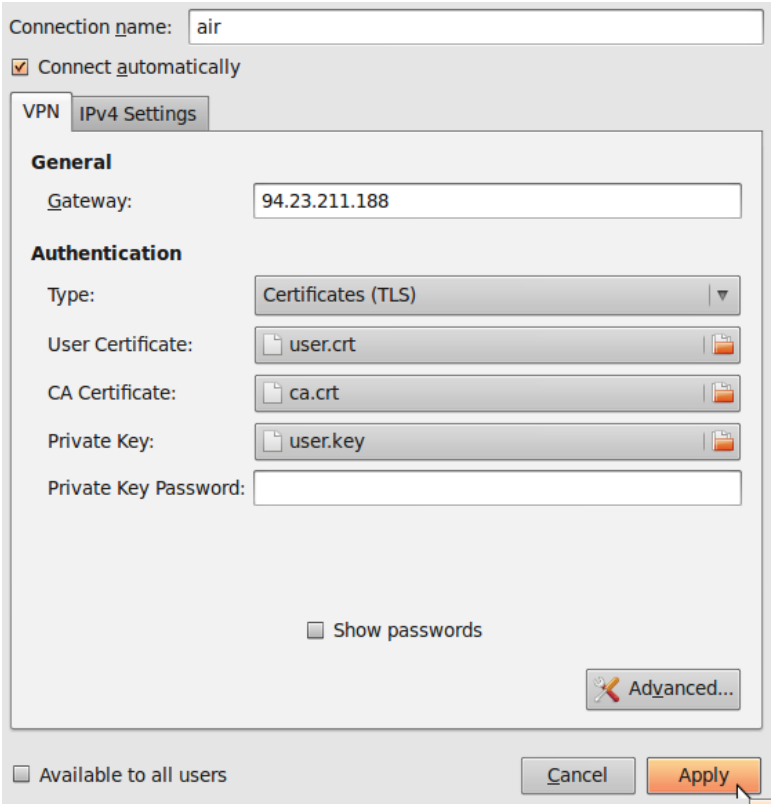
3. 在VPN选项卡，点击导入（Import）。



4. 找到你刚解压的air.ovpn，点击打开（Open）。



5. 一个新的窗口将被打开。保持默认，点击应用（Apply）。

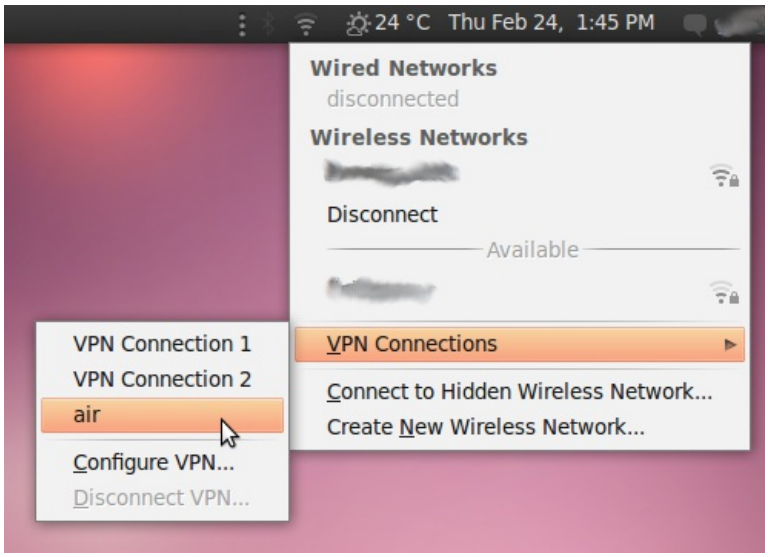


6. 恭喜你！你的VPN连接已可使用，出现在VPN选项卡的连接列表中。现在你可以关闭NetworkManager。

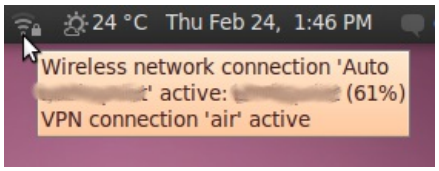
使用你新的VPN连接

现在你配置NetworkManager使用VPN客户端连接VPN服务，你可以使用新的VPN连接绕开网络审查。按照下面的步骤开始：

1. 在NetworkManager菜单，从VPN 连接中选择新的连接。

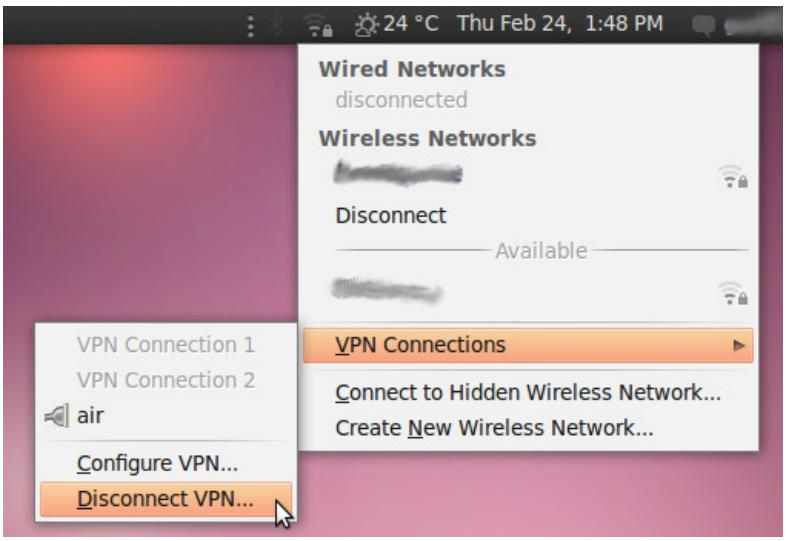


2. 等待VPN连接建立。当连接时，一个小挂锁的图标将会紧挨在NetworkManager图标的右边，显示你正在使用一个安全的连接。把光标移到图标上，确认VPN连接已连上。



3. 你也可以访问http://www.ipchicken.com.，检查连接的现状。这个免费的IP查询工具确认你正在使用airvpn.org的一个服务器。

4. 在NetworkManager菜单选择VPN 连接（VPN Connections ）>断开VPN （Disconnect VPN），断开你的VPN。你现在又在使用你的正常连接（被过滤）。



热点保护盾

热点保护盾（Hotspot Shield）是一个免费（但商业的）适用于微软Windows和Mac OS的虚拟专用网络（VPN）解决方案，其可被用于通过一个安全隧道（在你的正常被审查互联网连接之上）访问网络。

热点保护盾加密你所有的通讯，所以你的审查者的监视软件不能看到你正访问什么网站。

一般信息

Supported operating system	
Localization	English
Web site	https://www.hotspotshield.com
Support	FAQ: https://www.anchorfree.com/support/hotspot-shield.html E-mail: support@anchorfree.com

如何获得热点保护盾

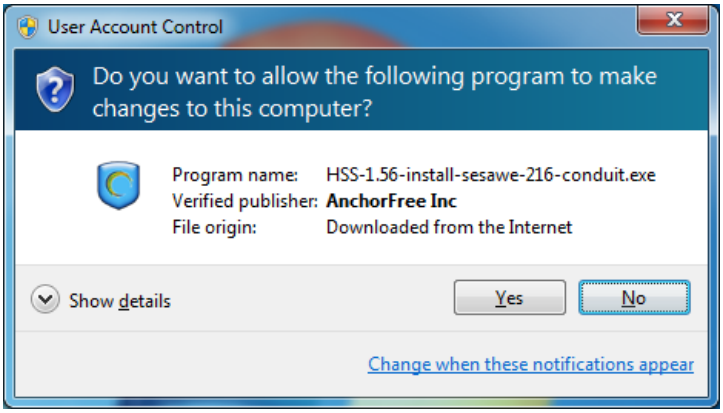
从https://www.hotspotshield.com下载软件。文件大小大约是6兆，因此通过缓慢的拨号连接下载可能需要长达25分钟或更多。如果该下载在你尝试访问的地方被封锁，那么写邮件给hss-sesawe@anchorfree.com，并且在你的电子邮件的主题行中至少包括以下字之一：“hss”、“sesawe”、“hotspot”或“shield”。你将在你的收件箱收到作为电子邮件附件的安装程序。

注意事项：如果你使用的是启用NoScript扩展的Firefox，那么当你尝试使用热点保护盾时可能会遇到一些问题。请确保热点保护盾连接的所有URL都是白名单，或者当你使用该服务时你暂时允许全球脚本。

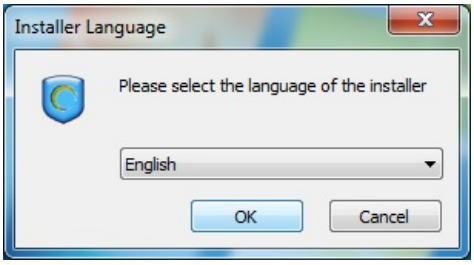
安装热点保护盾

1. 在成功下载后，查找你计算机上下载好的文件，并双击图标以开始安装

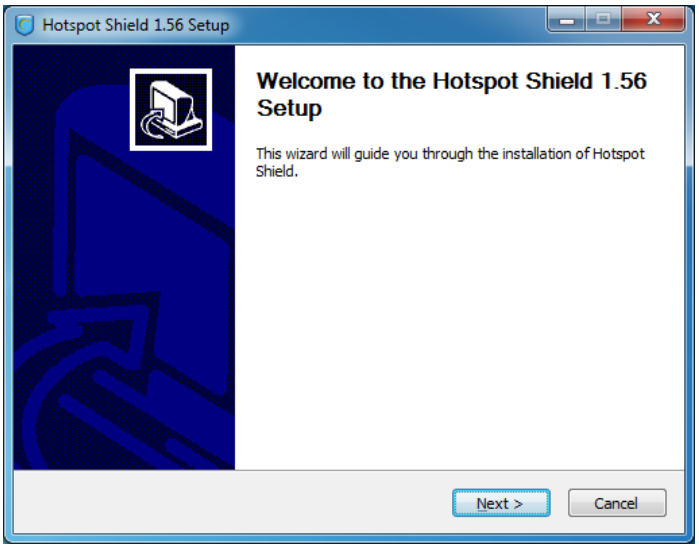
2. Windows可能询问你安装该软件的许可。点击是。



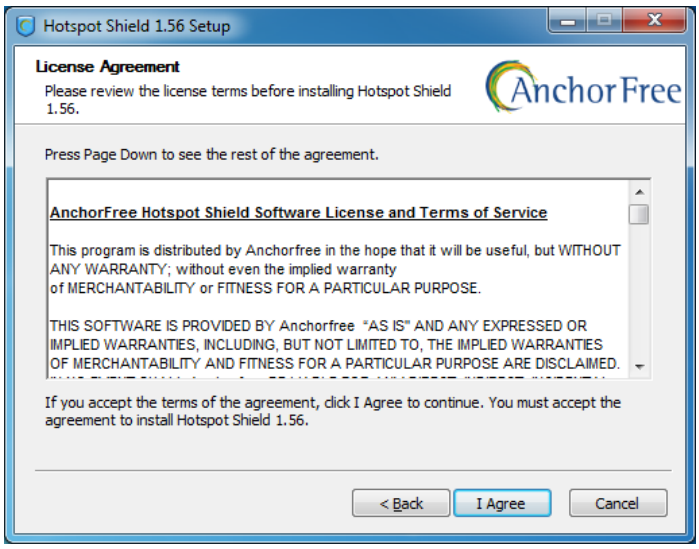
3. 从下拉菜单中选择你喜欢的安装语言。



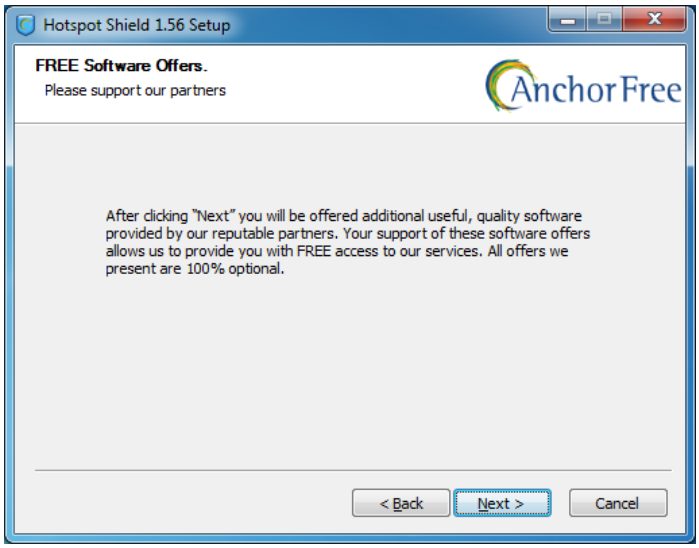
4. 在你选择好语言后，你将看到一个欢迎界面。点击下一步。



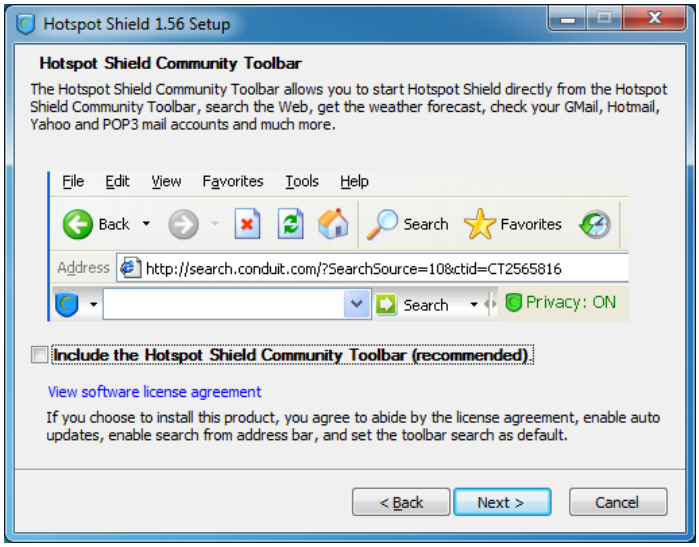
5. 通过点击“我同意” （I agree）接受许可协议。



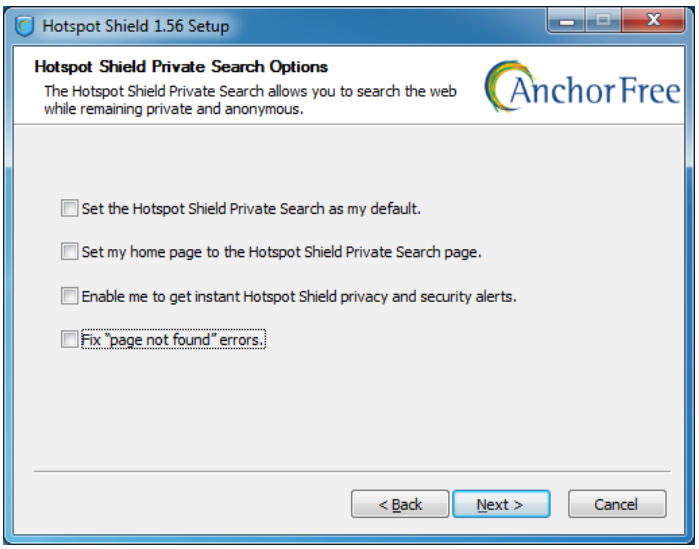
6. 你将看到一个窗口，通知你可以选择安装的附加软件。点击下一步。



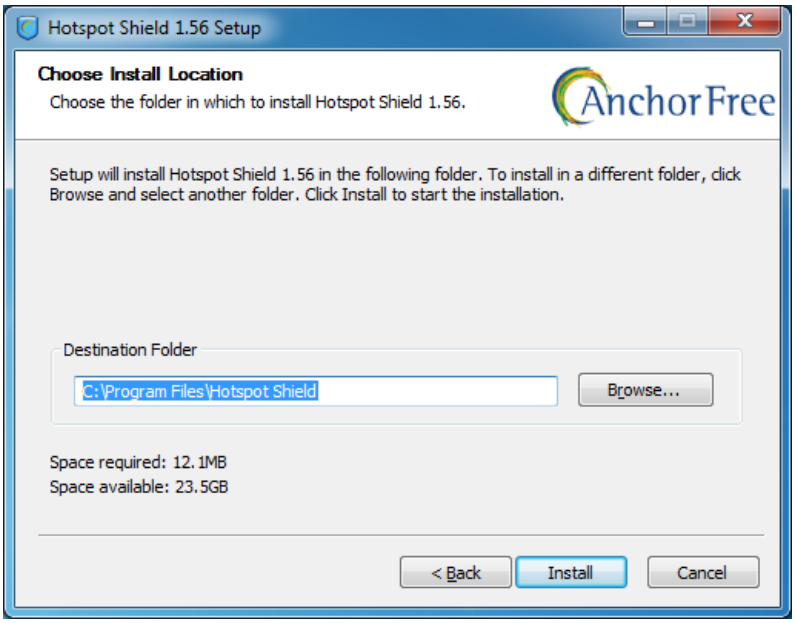
7. 在下一个界面，你可以去掉安装热点保护盾社区工具栏的选项。运行热点保护盾并不必需该产品。



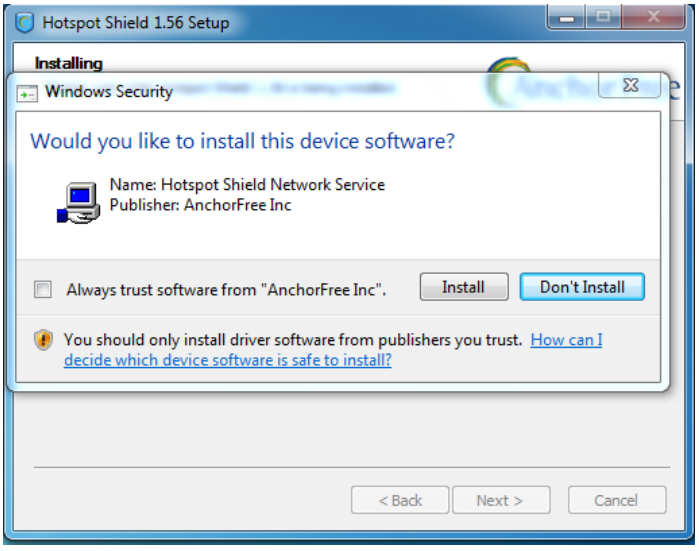
8. 附件选项将在下一个界面出现。所有这些产品都是可选的，且你并不必需它们中的任何一个以运行热点保护盾。



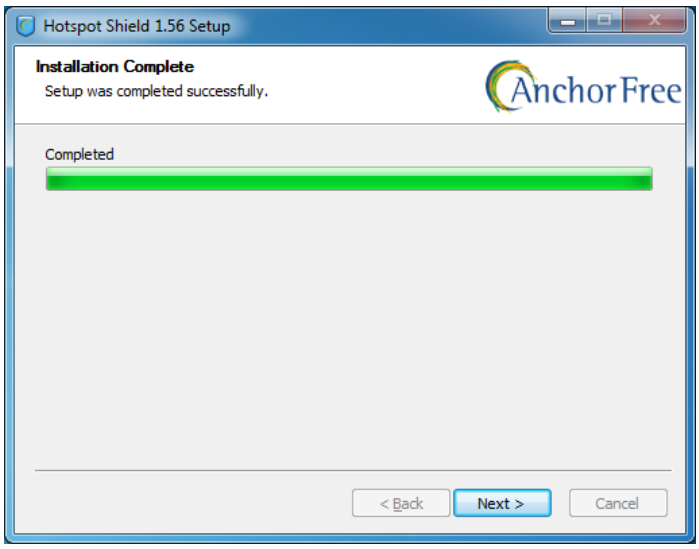
9. 选择你想要安装热点保护盾硬盘位置。在大多数情况下，你可以保留默认路径，继续点击安装。



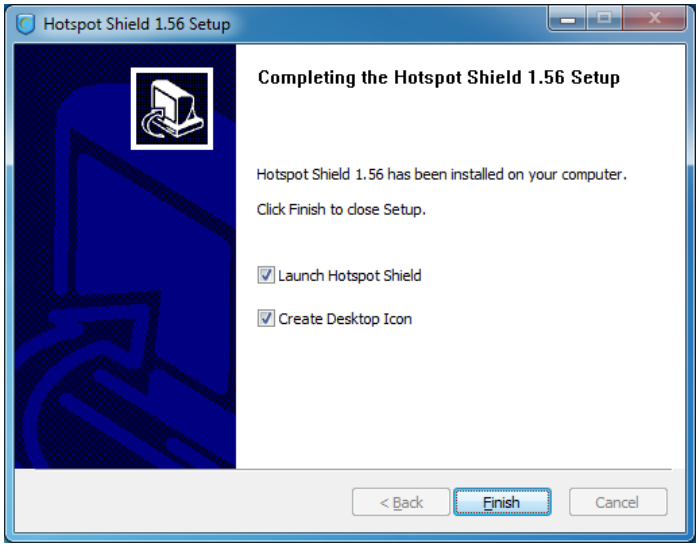
10. Windows可能不断请求额外许可安装热点保护盾的不同组件。你每次都可以放心地继续点击安装。



11. 当安装完成后，点击下一步。



12. 最后，你可以在安装后立即启动热点保护盾和在你的桌面上创建一个图标。选择你喜欢的并点击完成。

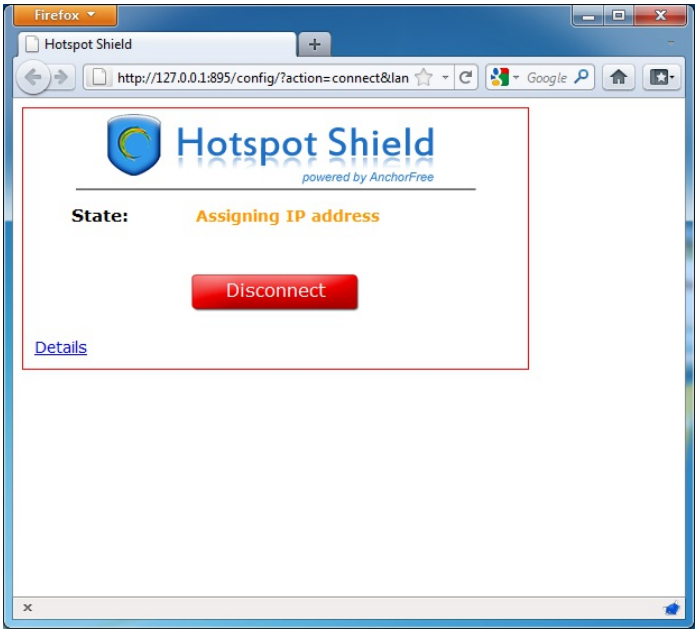


现在，热点保护盾已安装到你的电脑上。

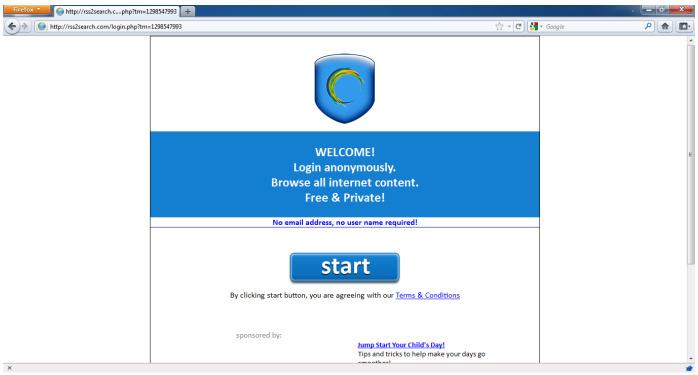
连接到热点保护盾服务

1. 点击你桌面上或目录程序中的热点保护盾图标> Hotspot Shield。

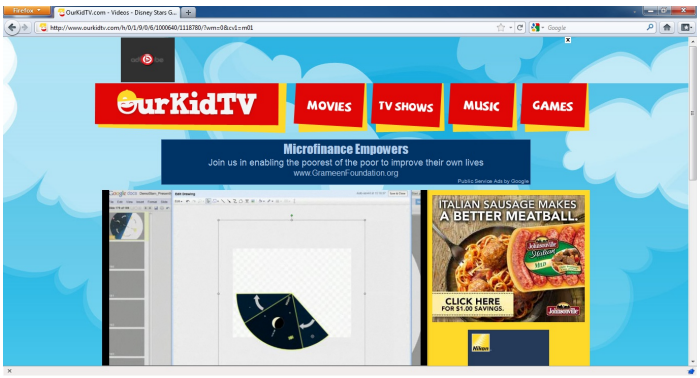
2. 一旦你启动热点保护盾，浏览器窗口将打开一个状态页面显示连接尝试的不同阶段，如“认证”和“分配IP地址”。



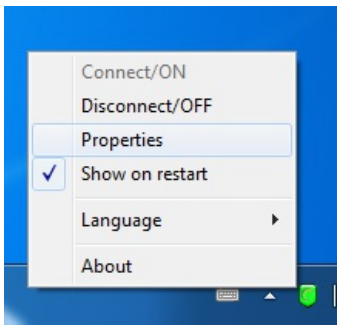
3. Once connected, Hotspot Shield will redirect you to a welcome page. Click Start to begin surfing.



4. Please note that after you click Start, Hotspot Shield may redirect you to an advertisement page such as the one displayed below. You can close this tab and start surfing the Web as usual. You can check that you are connected to the Hotspot Shield service by looking at the green Hotspot Shield icon in your system tray (next to the clock).

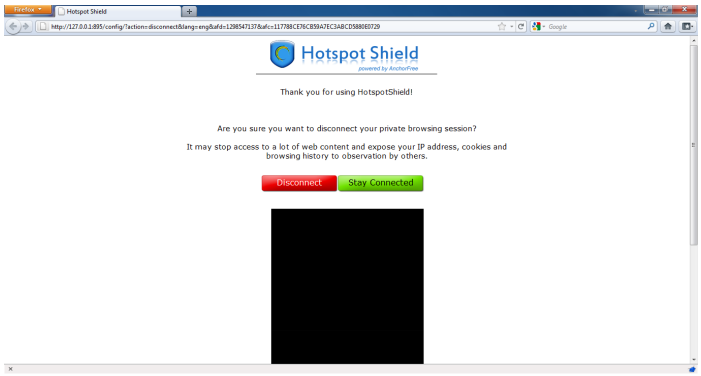


5. To check your connection status, simply right click on the Hotspot Shield system tray icon and select Properties.

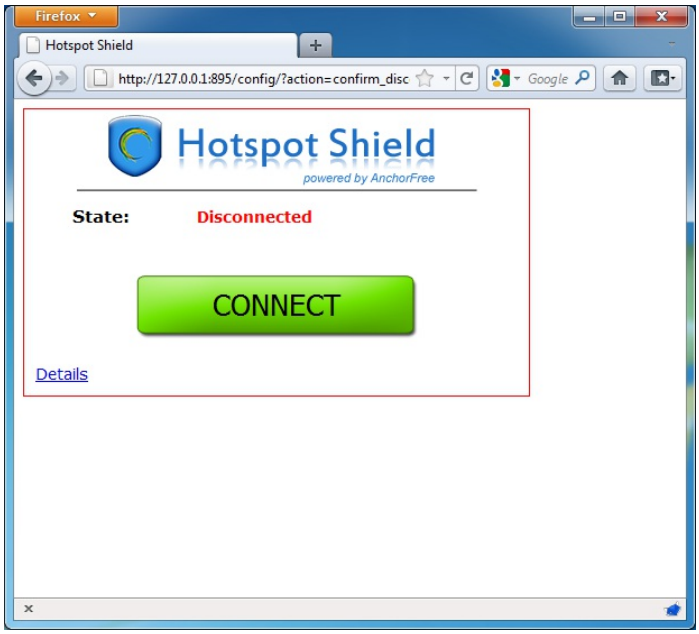


断开热点保护盾服务

1. 要断开热点保护盾服务，只要右击系统托盘图标（见上图）并选择断开/关闭。
2. 热点保护盾将询问你以确认该动作。点击断开。



3. 一个状态窗口将出现，确认你现已断开并在你正常的（被过滤的）连接上网上冲浪。点击“连接”按钮继续绕行。



Alkasir

Alkasir是一款创新的服务器/客服端工具促进对网站审查（过滤）进行跟踪、分析和绕行。Alkasir主要在中东地区使用，但是在全球都可使用。

它利用一个专用的客服端软件和使用代理服务器。通过半自动更新，允许全球用户社区报道新近被屏蔽的网站，以保持被屏蔽的网站列表是最新的，是其创新点。

一般信息

Supported operating system	
Localization	English and Arabic
Web site	https://alkasir.com
Help	https://alkasir.com/help
FAQ	https://alkasir.com/faq
Contact	https://alkasir.com/contact

Alkasir 是如何工作的?

Alkasir已实施两个创新性和互补性的新功能。它被设计成一个嵌入式的预配置的HTTP代理网络浏览器（基于Mozilla Firefox），和一个可以自己添加被过滤的网址的数据库。

绕过网络审查

Alkasir的创新只依靠其被屏蔽网址数据库，并内置了代理来访问被屏蔽的网址。没有被屏蔽的网址可以直接访问，无需通过代理。只有当它真正需要优化带宽的使用情况，并允许更迅速地访问没有被过滤的网页时（因为直接访问的网页加载更快），才使用HTTP代理。

保持被过滤网址数据库更新

任何时候当用户怀疑网址被屏蔽，他可以通过软件界面报告。 Alkasir彻底检查这个报告，然后要求该国的版主（一个人）批准添加到数据库，除了数据库（保持数据库的相关性，并防止不良内容被加入，如色情）。

一个“被屏蔽的内容单位”（一个在某一个国家被屏蔽的网站）往往依赖于多个网址。 Alkasir检测在某一个国家被屏蔽的网址时，它会检查该网页上的所有来源网址，以确定他们是否也封锁。因此，Alkasir通过一个简单的、原始的和一级蜘蛛爬行方法建立被屏蔽的内容数据库。

最后，如果Alkasir用户直接请求（即不通过代理）加载一个网址失败，客户端注意到这一点，自动检查，看它是否是一个新的（尚未在数据库中）被屏蔽的网址，如果是的话，则自动将其添加。

数据库在https://alkasir.com/map上。

总之，Alkasir的被屏蔽网址数据库连续不断地从用户那获得信息（通过人工提交或自动报告），Alkasir浏览器依赖这个数据库通过仅重定向那些经由代理的被屏蔽网址请求，来优化这个全球工具的反应。

怎样得到 Alkasir?

你可以直接从网站上下载或者通过邮件接收。

从网站下载 Alkasir

你可以从官网上下载Alkasir， https://alkasir.com。

取决于你的操作系统和你的程序，你可以从下列版本选择一个：

- 如果你使用Windows Vista 或者Windows 7，并已安装好Mozilla Firefox，你只需要“Alkasir安装包”（需要安装，3MB）。
- 如果不是上述情况，你需要下载“Alkasir完整安装包”（也需要安装，41.04MB）。

如果你无法安装或不想在电脑上永久地安装Alkasir（比如公用电脑，网吧，或者图书馆的电脑），你可以选择下载2个USB版本的Alkasir中的一个：

- 不包含Mozilla的 Alkasir USB 包 (无需安装--便携--但需要用火狐打开；大小：4MB)

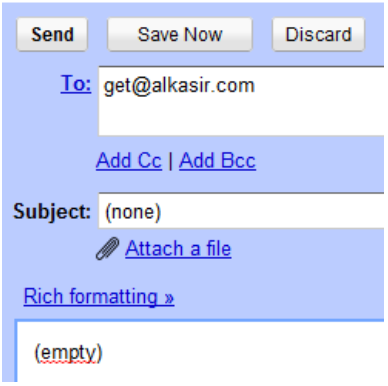
- 包含Mozilla 浏览器（火狐）的 Alkasir USB 包 (无需安装--便携；大小：12MB)

请注意两种版本都需要安装Net Framework，在Windows Vista和 Windows 7操作系统里已预先安装。

你可以注册一个帐号，通过邮件从Alkasir收到定期更新和新闻。更新定期发布，所以，你应该能肯定的从官方网站获取最新版本。

通过邮件接收 Alkasir

如果Alkasir网站在你的国家被屏蔽，你可以通过电子邮件自动回复得到安装文件。只需要发送一封空白邮件到get@alkasir.com索取作为附件的安装文件。

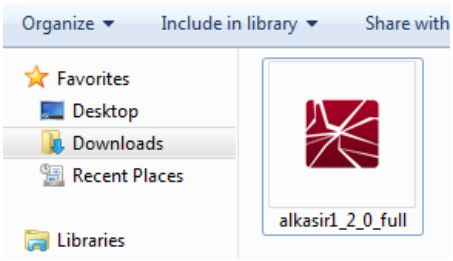


你将收到一封邮件，软件在附件中，还有关于如何在你电脑上安装Alkasir的说明。

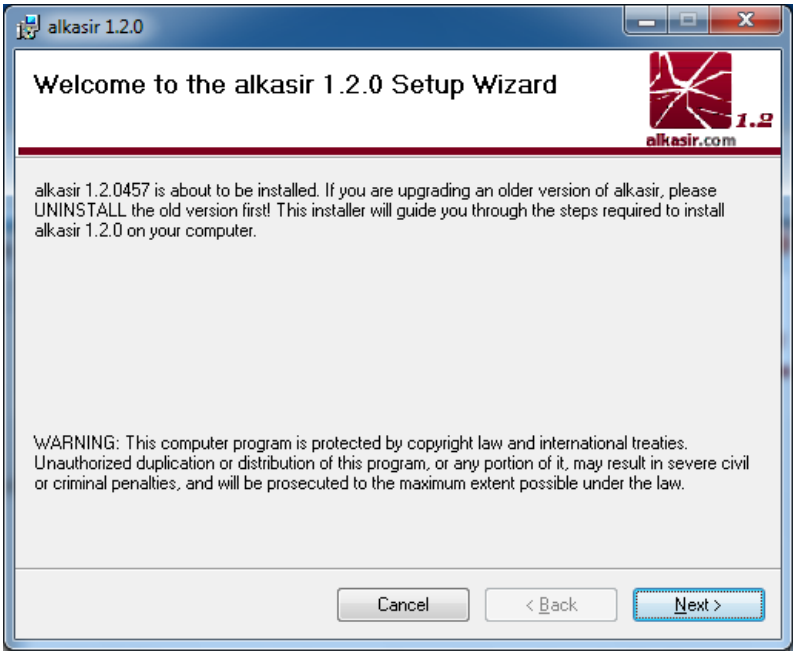
如果几分钟以后你还没收到软件，你可能需要添加get@alkasir.com到你的联系人白名单上，这样的话邮件不会被认为是垃圾邮件。

安装

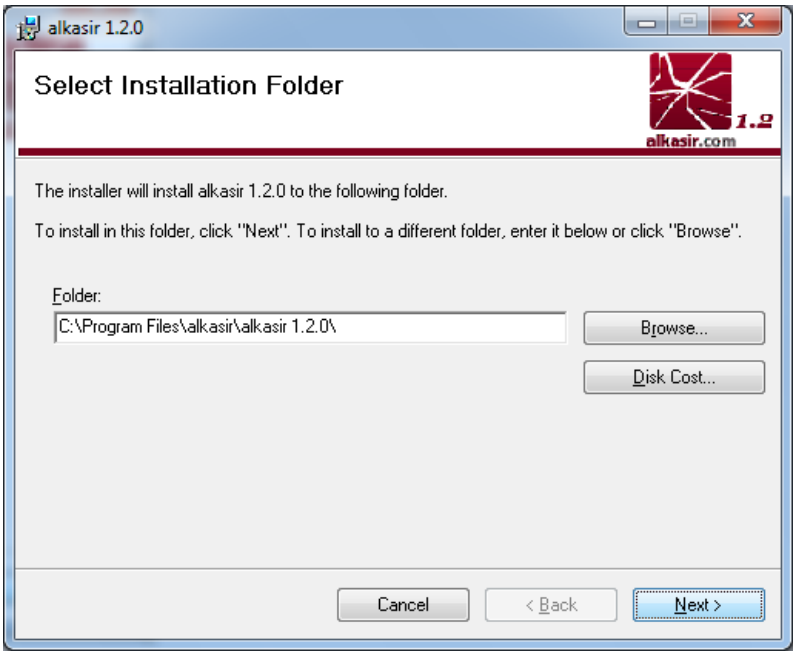
下载好安装文件后，双击软件图标。



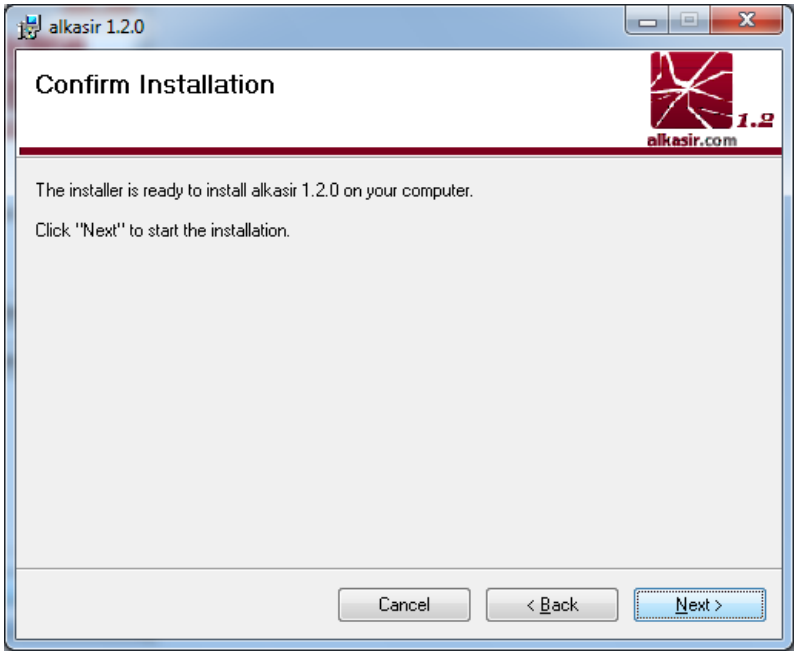
你可能会遇到安全警告。点击运行（Run）或者接受（Accept）。



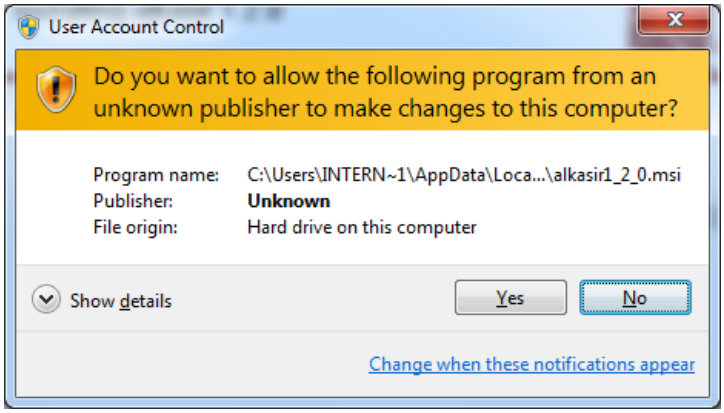
按照Alkasir安装向导，点击下一步（Next）按钮。



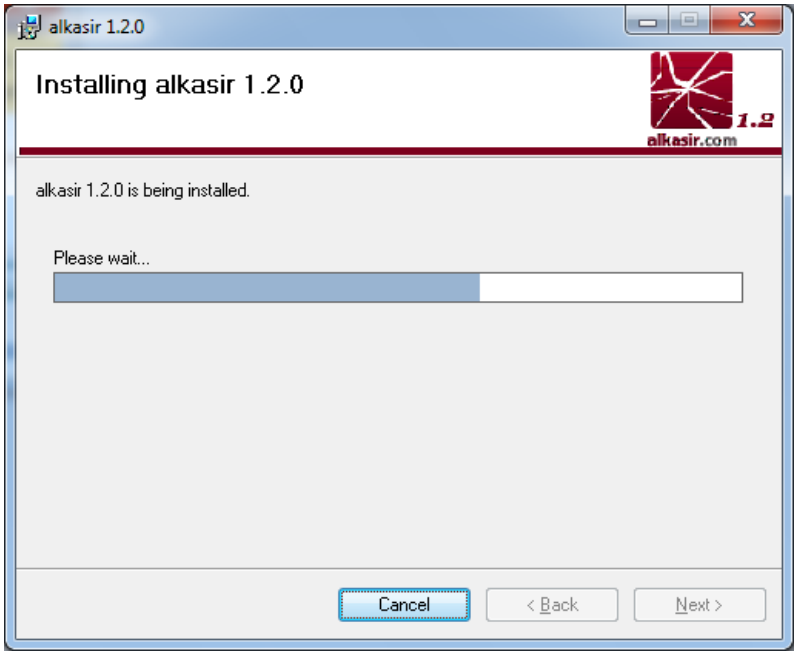
你可以更改安装文件夹（但不建议这样做）。

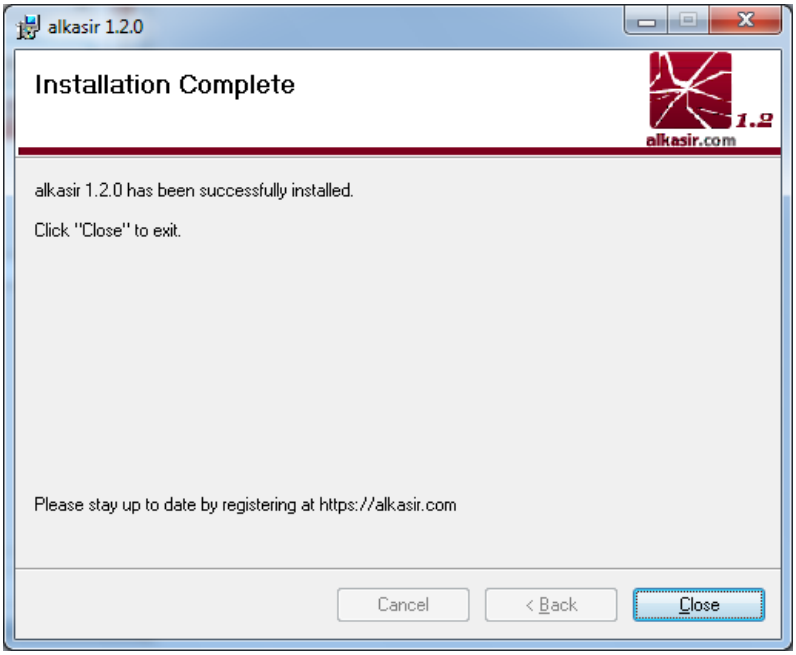


准备好时，点击下一步（Next）。



验证上图所示的安全警告，点击是（Yes）。

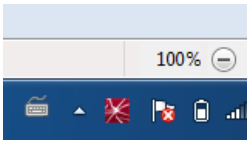




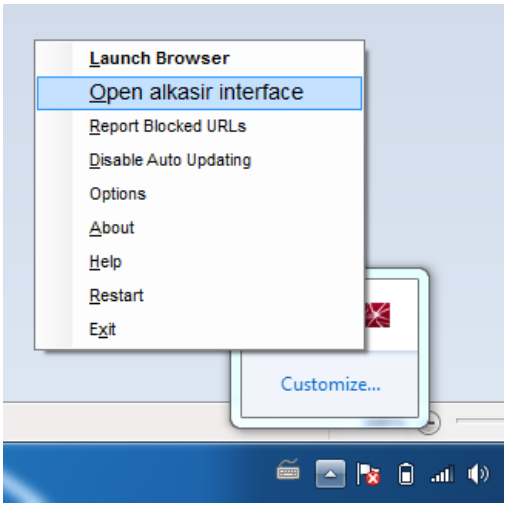
安装完成后，点击关闭（Close）。

怎样使用 Alkasir?

每当Windows启动，Alkasir就默认启动。检查Alkasir的图标出现在你的系统任务栏，在时钟（clock）的附近，确保软件正在运行。



右击图标显示的配置菜单。

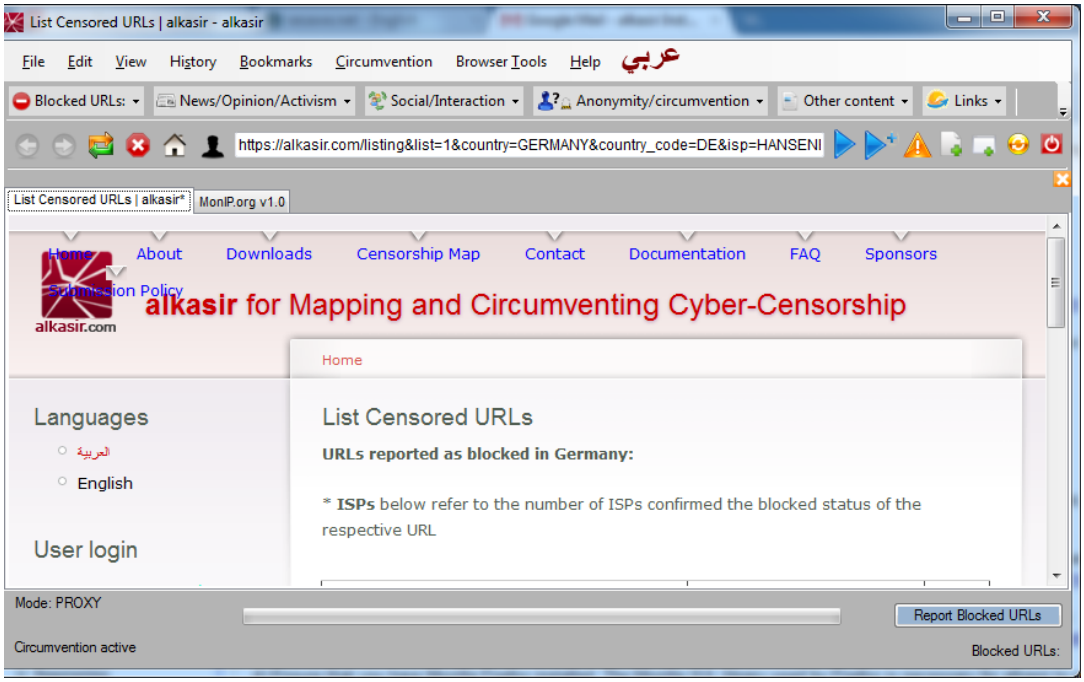


- 启动浏览器（Launch Browser）
- 打开Alkasir界面（Open Alkasir interface）
- 报告被屏蔽的网址（Report blocked URLs）

Alkasir的主界面集中了这个软件的所用功能。你可以：

- 启动，关闭和重启软件
- 启动Alkasir浏览器
- 在https://alkasir.com上注册或登录
- 获得已安装Alkasir版本的更新。

首先，启动Alkasir浏览器。



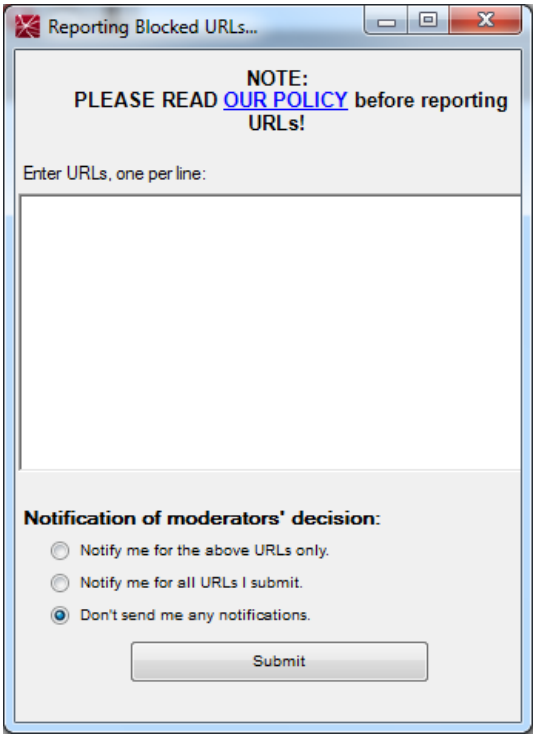
因为基于同样的技术架构，浏览器的图形用户界面和Mozilla Firefox非常相似。注意下列若干特有的功能：

- 一个完全阿拉伯语的按钮
- 报告被屏蔽网址的按钮，当你正在试图访问一个被屏蔽的网站是使用。这个按钮挨着地址栏（address bar）和状态栏（status bar）。
- 去主页面的Alkasir按钮。

你也可以找到其他菜单，整合你的Alkasir浏览器和Alkasir帐号。

可以启用或禁止软件、代理列表和被屏蔽网站数据库的自动更新。

如果你遇到可能表明一个被屏蔽的网站的一个错误页面（如拒绝访问或连接超时错误），你可以点击报告被屏蔽网址按钮提交网址到Alkasir数据库。你可以选择得到协调员决定是否将该网址加入数据库的通知（这一决定基于工具的政策）。



更多信息

访问https://alkasir.com：

- 这个软件的全面文档：https://alkasir.com/help
- 一些常见问题：:https://alkasir.com/faq

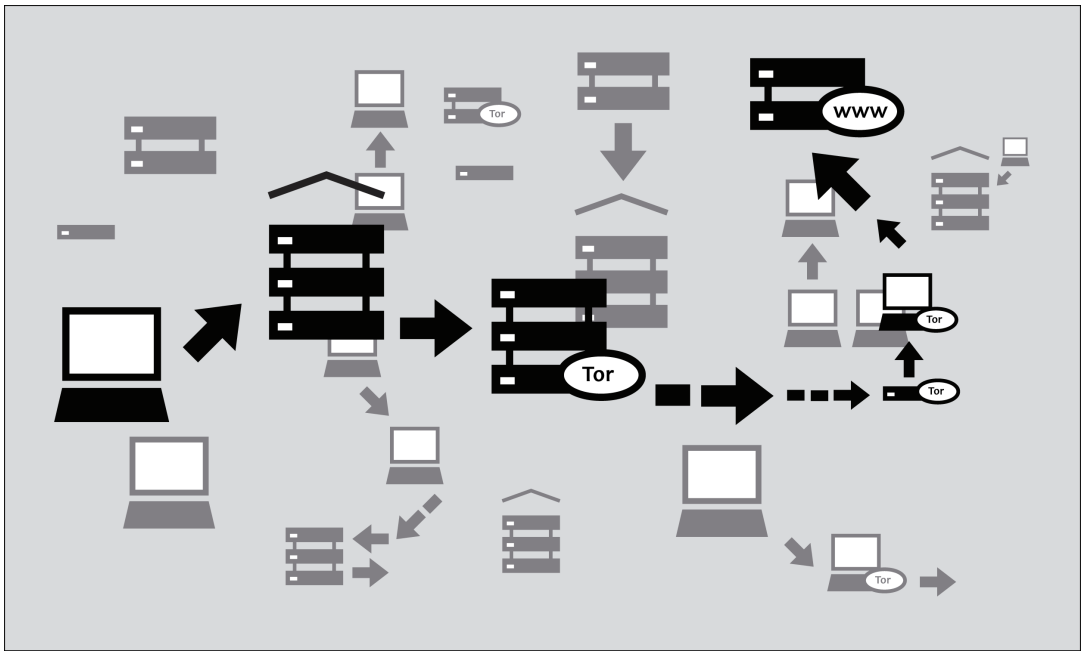
Tor：洋葱路由器

Tor（洋葱路由器）是一个非常高级的代理服务器网络。

一般信息

Supported operating system	
Localization	13 languages
Web site	https://www.torproject.org
Support	Mailinglist: https://lists.torproject.org/cgi-bin/mailman/listinfo/tor-talk FAQ: https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ IRC: #tor on irc.oftc.net

使用 Tor 访问网站时，用户的通信可通过由独立的、自愿的代理组成的网络随机转发。所有 Tor 服务器（或中继器）之间的通信都是经过加密的，并且每个中继器只知道其他两个相邻中继器的 IP 地址：通信传输链中位于它之前和之后的两个中继器。



这样做的目标是不可链接性。Tor使以下意图很难得逞：

• 互联网服务提供商或任何其他本地观察者获悉用户目标网站或用户发送的信息

• 目标网站获悉用户是谁（至少获悉用户的 IP 地址）

• 任何无关的中继器或者通过直接获取IP地址或者通过不断观察流量对浏览习惯进行相关从而获悉用户是谁以及用户数据的目的地

Tor与哪些软件兼容？

想要使用Tor网络连接互联网，或者想要使用它来保护匿名、隐私和绕行，用户需要在计算机上安装Tor客户端软件。也可以使用存储棒或其他外部设备运行该程序的可移动版本。

Tor可以兼容Windows、Mac OS X和GUN/Linux操作系统的大多数版本。

With what software is Tor compatible?

Tor使用SOCKS代理接口连接应用程序，因此所有支持SOCKS（4、4a和5版本）的应用程序都可以匿名地使用Tor，其中包括：

• 大多数的网络浏览器

• 许多即时通讯和 IRC 客户端

• SSH 客户端

• 电子邮件客户端

如果你从Vidalia Bundle、Tor Browser Bundle或Tor IM Browser Bundle安装Tor，其中绑定的Tor工具已将某个HTTP应用代理设置为Tor网路的前端（frontend）。通过这种方式，某些不支持SOCKS的应用程序也可以使用 Tor。

如果用户最感兴趣的是使用 Tor 来进行网页浏览和聊天，那么使用Tor Browser Bundle或Tor IM Browser Bundle 是最简单的选择，因为它们已进行预先设置，可以直接使用。Tor browser bundle中还包含Torbutton，使用Tor进行网页浏览时，该工具可以提供隐私的安全性。这两种版本的Tor工具可以从下面的网站下载：https://www.torproject.org/projects/torbrowser。

优势与风险

对于规避封锁和保护用户隐私，Tor是一个非常高效的工具。用户的通信内容经过Tor工具的加密处理，当地网络运营商无法获悉相关信息，并且这种加密还可以隐藏用户的通信对象以及用户查看了什么网站。比起单个代理，正确地使用这种工具，用户可以取得更为强大的隐私保护。

但是：

- 对于封锁，Tor很容易受到影响。大多数的Tor节点已在公共目录中列出，所以网络运营商能够很容易地获取该列表，然后将节点的IP地址添加到黑名单中进行过滤。（有一种方式可以绕开这种封锁，使用**Tor bridges**，它是那些未公开列出的节点，专门用于规避封锁。）
- 某些使用Tor的程序存在一些问题，会降低隐私的安全性。Tor Browser Bundle配备安装了Torbutton的Firefox版本。Torbutton禁用一些插件并改变你的浏览器痕迹，使其看起来像任何其他Torbutton用户。如果你没有配置你的应用通过Tor运行，Tor将无法保护你。一些插件和脚本会忽略本地代理设置，可以显示你的IP地址。
- 如果用户没有使用额外的加密对通信进行保护，那么在通信链的最后节点（称为出口节点：**exit node**）处，用户的数据将是非加密的。这意味着，对于最后Tor节点的所有者以及该节点与目标网站之间的互联网服务提供商来说，用户数据是可见的。

Tor 开发者一直很关注这个漏洞和其他一些潜在的风险，并提出三点警告：

1. 如果用户没有正确地使用Tor，它将不能为用户提供保护。打开下面的链接，阅读其中的警告信息： https://www.torproject.org/download/download.html.en#warning，然后查看下面的网页，确保按照其中指示对用户平台进行设置：https://www.torproject.org/documentation.html.en#RunningTor。
2. 即使用户正确地设置和使用 Tor，仍然存在潜在的攻击，能够降低 Tor 的用户保护能力：https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#Whatattacksremainagainstonionrouting。
3. 目前，没有哪个匿名系统是完美无缺的，Tor也不例外：如果真的需要强大的匿名保护，用户不应只依靠当前的Tor网络。

使用Tor浏览器套件

在Windows、OS X或GNU/Linux上使用 Tor 浏览器套件，用户无需再对网页浏览器进行配置。更为方便的是，该程序是便携式的，可以从 USB 闪存驱动器直接运行，对于任何计算机来说，用户无需在硬盘上安装就可以直接使用该程序。

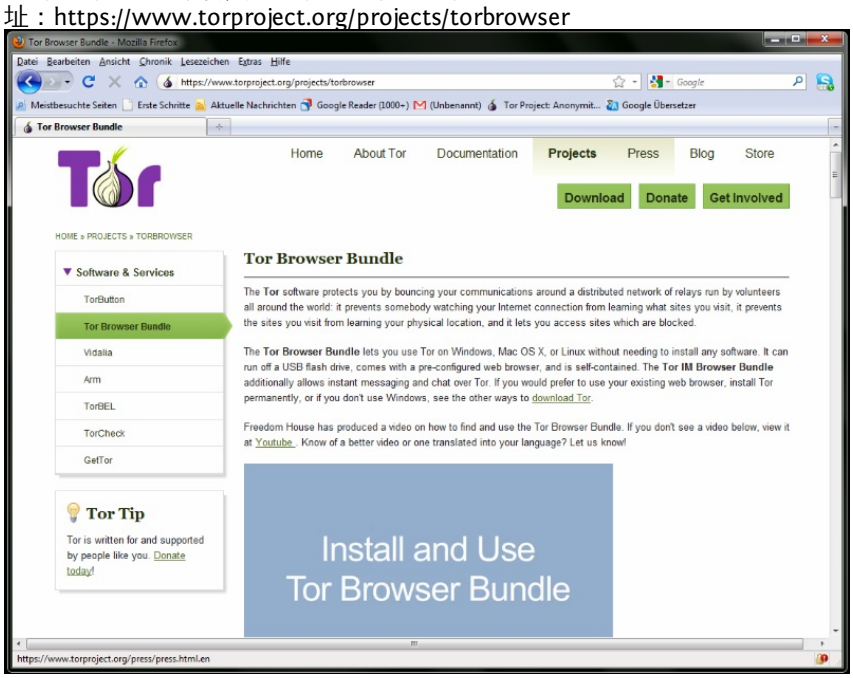
下载Tor浏览器套件

用户可以从torproject.org网站下载Tor浏览器套件，有两种格式，一种是单个文件，一种是多个文件的“分割”版。如果用户的互联网连接速度比较慢或者不稳定，最好下载分割版而不是一个较大的文件。
如果torproject.org网站在用户所在地被过滤，可在常用的网页搜索引擎中输入“tor mirrors”（即搜索tor镜像）：在搜索结果中将显示一些替代地址，用于下载Tor浏览器套件。
通过电子邮件获得**Tor**：以“帮助”为邮件主题向gettor@torproject.org发送一封电子邮件，你将收到关于如何使自动应答机器人发送给你Tor软件的说明。
注意：下载Tor Bundle（普通格式或分割版）时，用户应该检查文件签名，尤其是对于从镜像网站下载。这个检查步骤用于确保软件文件没有被篡改。有关签名文件的更多信息以及如何进行检查，请查阅：https://www.torproject.org/docs/verifying-signatures。
用户可以从下面的网址下载 GnuPG 软件，检查签名时需要使用该软件：http://www.gnupg.org/download/index.en.html#auto-ref-2。

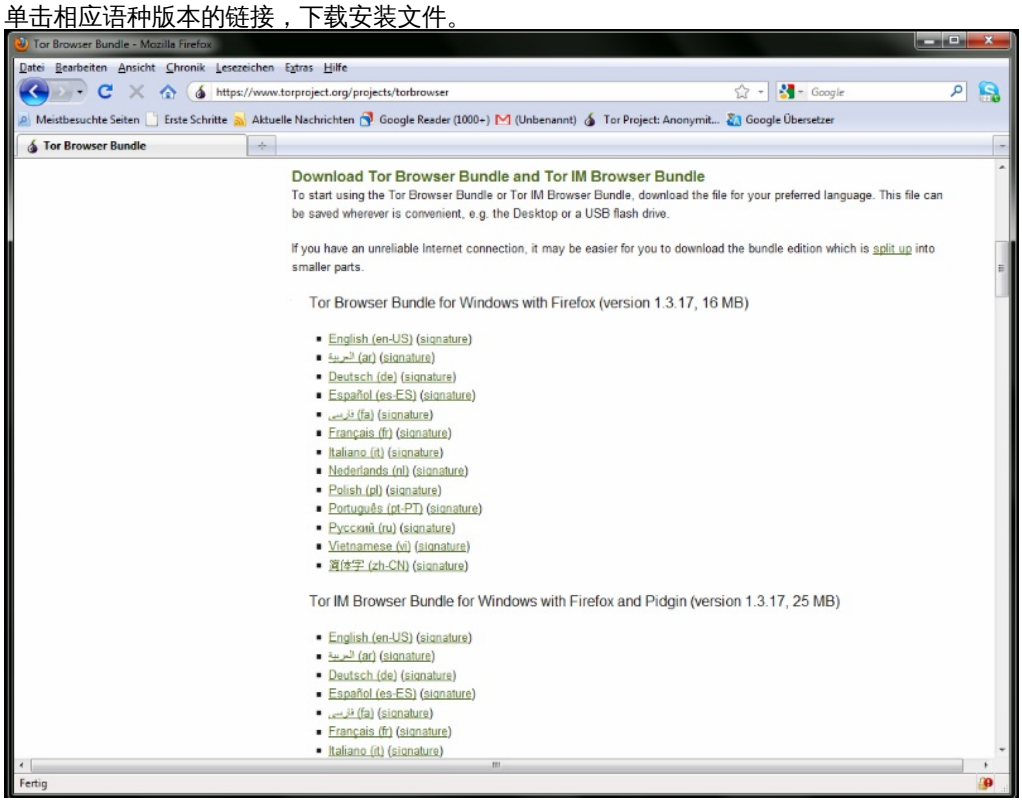
在Microsoft Windows系统下安装Tor浏览器，请查阅下面的安装指南。如果用户使用不同的操作系统，请查阅Tor网站的下载链接和相关指南。

从单个文件安装

1. 在网络浏览器中，输入Tor浏览器的下载网址：https://www.torproject.org/projects/torbrowser



2. 单击相应语种版本的链接，下载安装文件。



3. 下载完成之后，双击.exe文件。弹出“7-Zip self-extracting archive”（7-Zip文档自解压）窗口。

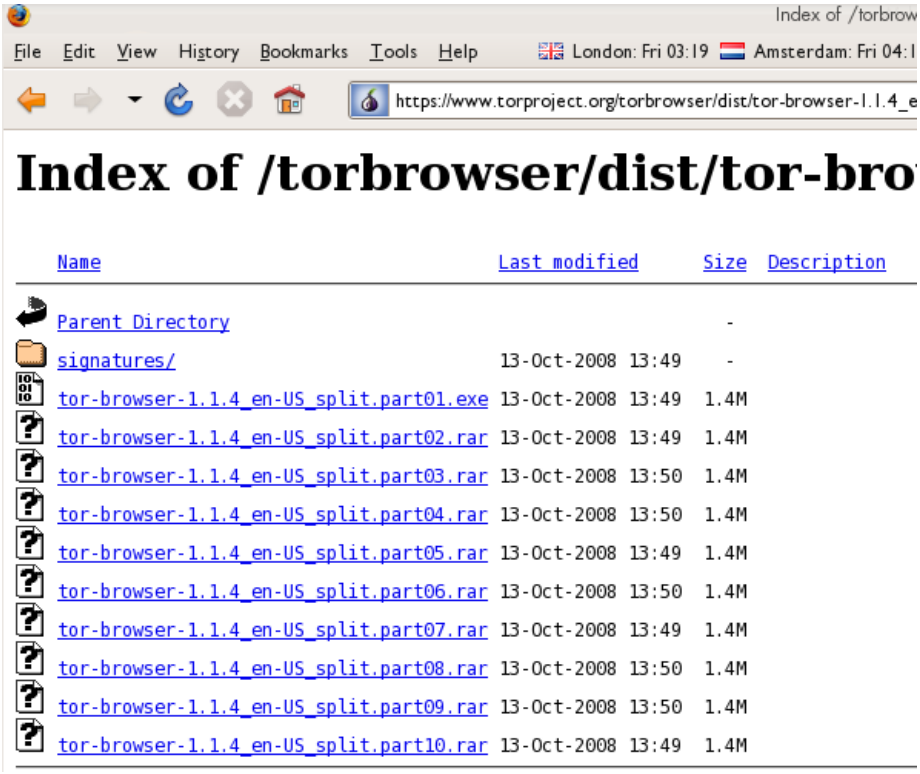
1. 为解压文件选择一个文件夹，然后单击“Extract”（解压）。
   注：如果用户想要在不同的计算机（比如在网吧的电脑）上使用该软件，可选择将文件直接解压至USB闪存驱动器。

   解压完成之后，打开相应的文件夹，查看文件夹下的内容是否与下图相同：

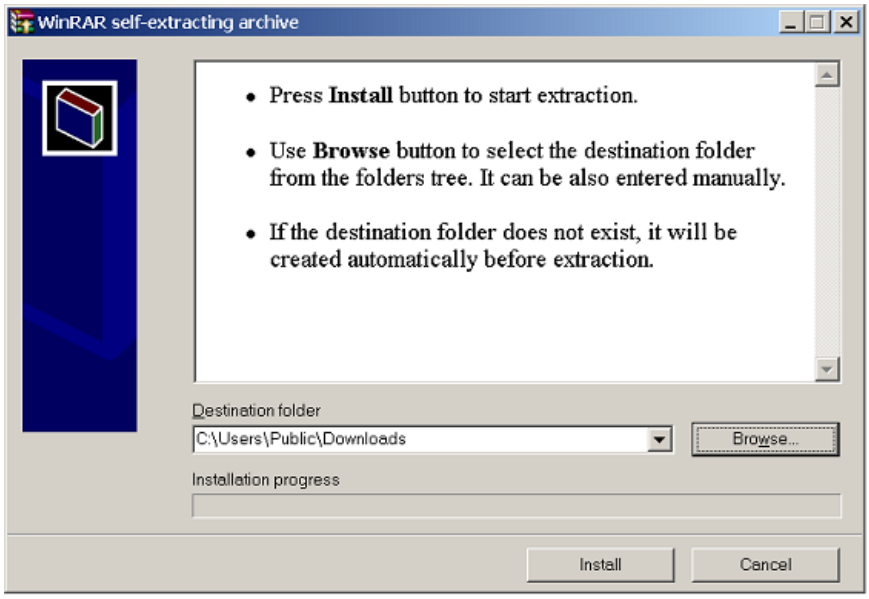
   如果不再需要下载文件，可将最初下载的.exe文件删除。

从多个分割文件安装

1. 在网络浏览器中，输入Tor浏览器套件分割版的下载网址（https://www.torproject.org/projects/torbrowser-split.html.en），然后单击相应语言版本的链接，打开一个页面，下图为英文版网页：



2. 单击每个文件链接进行下载（一个文件的后缀名为“.exe”，其他九个文件为“.rar”），将所有文件都保持在用户硬盘的同一文件夹中。
3. 双击后缀名为“.exe”的第一个文件。 然后将运行一个程序，将该程序的所有文件组合起来。



4. 选择安装文件夹，然后单击“Install”（安装）。上图中解压程序将显示进度信息，然后自动关闭。
5. 解压完成之后，打开相应的文件夹，查看文件夹下的内容是否与下图相同：

6. 如果不再需要下载文件，可将它们都删除。

使用Tor浏览器

在开始之前：

- 关闭Tor。如果用户计算机已安装Tor，请确保当前它没有运行。

启动Tor浏览器：

Tor starting

在“Tor Browser”文件夹中，双击“Start Tor Browser”文件。Tor控制面板（Vidalia）将打开，并且Tor开始连接Tor网络。

连接建立完成之后，Firefox将自动打开TorCheck页面，然后确认用户的浏览器是否已配置使用Tor。这可能需要一些时间，取决于用户的互联网连接状况。

如果已连接到 Tor 网络，在计算机屏幕的右下角的系统托盘中显示绿色的洋葱图片：

使用Tor浏览器浏览网页

试着查看一些网站，检查是否能够打开网页。由于使用了Tor，用户的连接将通过多个中继进行转发，所以打开网页的速度为比较慢。

如果Tor无法正常工作

如果 Vidalia 控制面板中的洋葱图标没有变为绿色，或者Firefox已启动，但显示一个“Sorry. You are not using Tor”（抱歉，Tor未正常运行）的页面，如下图所示，那么表示用户并没有使用Tor。

如果看到该信息，请关闭Firefox和Tor浏览器，然后重复上述步骤。你可以随时通过访问https://check.torproject.org/进行该检查以确保你使用了Tor。

如果Tor浏览器在两三次尝试后仍不起作用，Tor可能被你的互联网服务提供商部分封锁，你应尝试使用Tor的**bridge**功能。参见以下“通过网桥使用Tor”部分。

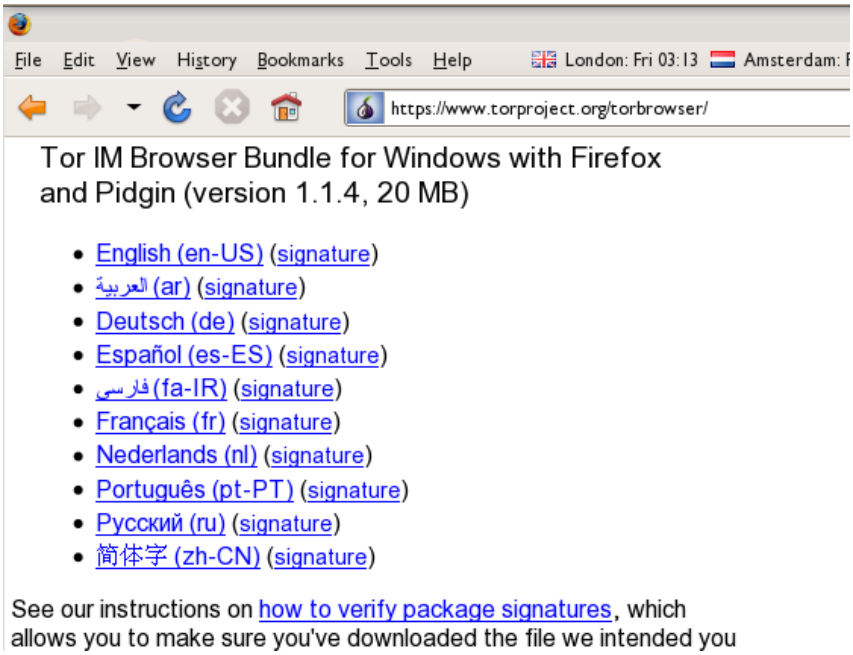
使用 Tor IM 浏览器套件

Tor IM 浏览器套件和 Tor 浏览器套件类似，但利用前者，用户可以使用一个多协议的即时通讯客户端：Pidgin；该客户端可以对常用的可能被过滤的即时通讯协议如 ICQ, MSN Messenger、Yahoo! Messenger或QQ进行加密。

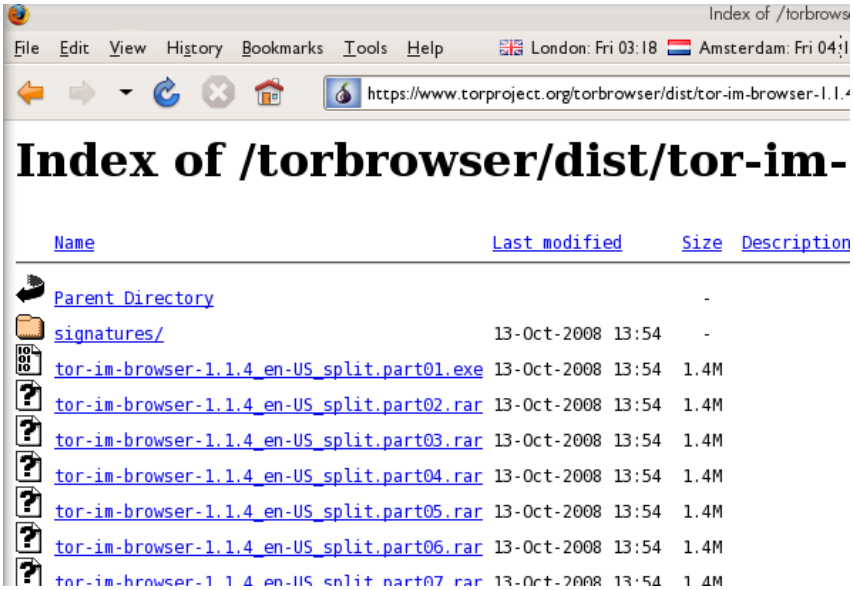
有关Pidgin更多信息，请查阅：http://www.pidgin.im/

下载 Tor IM 浏览器套件

你可以直接从Tor网站（https://www.torproject.org/torbrowser/）下载 Tor IM 浏览器套件。



如果用户的互联网连接数速度较慢或不够稳定，可以从 torproject.org 网站的 https://www.torproject.org/torbrowser/split.html 页面下载分割版。



自动解压文档

首先，双击刚刚下载的 .EXE 文件。
用户可以看到如下窗口：

- 为解压文件选择一个文件夹。如果不确定保存在何处，可使用缺省设置。然后单击“Extract”（解压）按钮。
  注：如果用户想要在不同的计算机（比如在网吧的电脑）上使用该软件，可选择将文件加压至 USB 闪盘。

- 解压完成之后，打开新创建的解压文件夹，然后检查内容，下图为“PidginPortable”文件下的内容：

- 解压之后，用户就可以安全地删除下载的“.exe”文件或分割版的所有“.rar”和“.exe”文件。

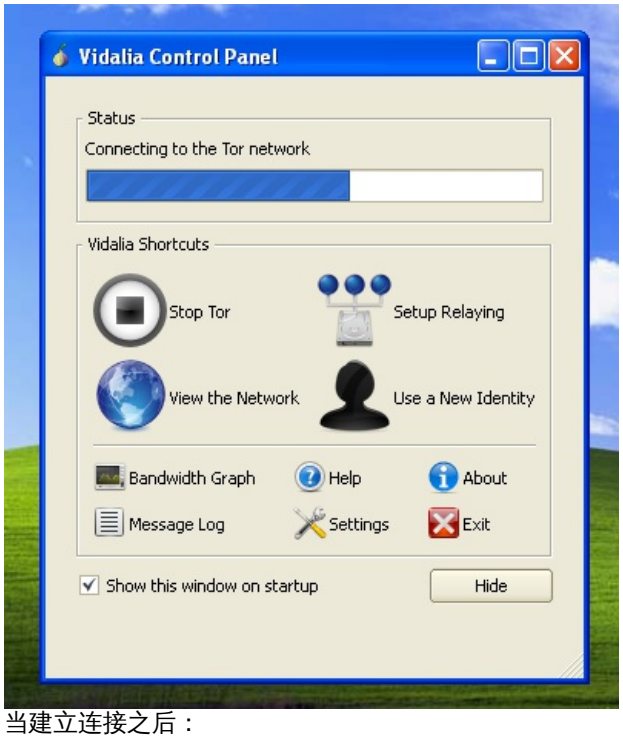
使用 Tor IM 浏览器套件

在开始之前：

- 关闭 Firefox 浏览器。如果用户计算机已安装 Firefox，请确保当前该浏览器没有运行。
- 关闭 Tor。如果用户计算机已安装 Tor，请确保当前它没有运行。

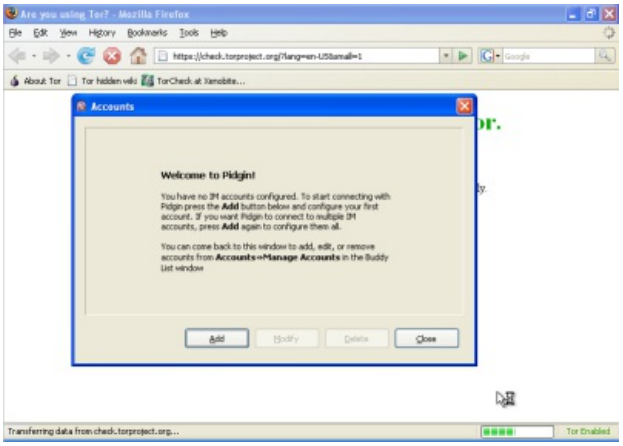
启动 Tor IM 浏览器：

- 在“Tor Browser”文件夹中，双击“Start Tor Browser文件。”Tor 控制面板（Vidalia）将打开，并且 Tor 开始连接 Tor 网络。

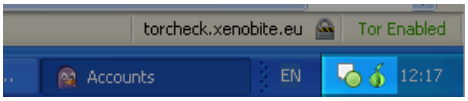


当建立连接之后：

- 将打开 Firefox 浏览器并访问 TorCheck 页面，该页面显示如果显示绿色图标，表示已经连接到 Tor 网络。
- 弹出 Pidgin 帐号窗口（如下图所示），邀请用户在 Pidgin 上设置 IM 帐号。



此外，在屏幕的右下角的系统托盘中，用户还可以看到 Tor 图标（绿色表示已连接到 Tor 网络）和 Pidgin 图标：



在 Pidgin 中设置 IM 帐号

用户可以在 Pidgin 窗口中添加 IM 帐号。Pidgin 可以兼容大多数的 IM 服务（AIM、MSN、Yahoo!、Google Talk、Jabber、XMPP、QQ 和 ICQ 等等）。

有关 Pidgin 使用方法的更多信息，请查阅：

http://developer.pidgin.im/wiki/Using%20Pidgin#GSoCMentoring.Evaluations

如果 Tor 无法正常工作

如果 Vidalia 控制面板中的洋葱图标没有变为绿色，或者 Firefox 已启动，但显示一个“Sorry. You are not using Tor”（抱歉,Tor 未正常运行）的页面，那么用户应：

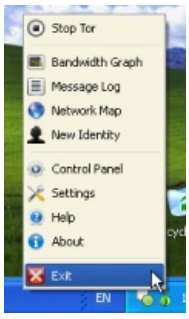
- 退出 Vidalia 和 Pidgin（详情见下文）。
- 按照上文“使用 Tor IM 浏览器套件”中描述的步骤，重新启动 Tor IM 浏览器。

经过几次尝试之后，Tor 浏览器仍然无法正常运行，可能是因为 Tor 被用户的 ISP 封锁。请参考本手册的“通过 Bridge（网桥）的使用 Tor”章节，然后使用 Tor 的 bridge 功能，再次尝试运行 Tor。

关闭 Tor IM 浏览器

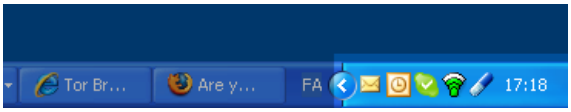
想要关闭 Tor IM 浏览器，用户需要：

- 在系统托盘中，右键单击洋葱图标，然后在弹出的 Vidalia 菜单中选择“Exit”，关闭 Vidalia。



- 在系统托盘中，右键单击洋葱图标，然后在弹出的 Vidalia 菜单中选择“Exit”，关闭 Pidgin。

屏幕右下角系统托盘中的 Vidalia 洋葱图标和 Pidgin 图标消失之后，也就关闭了 Tor IM 浏览器。



通过 Bridge（网桥）使用 Tor

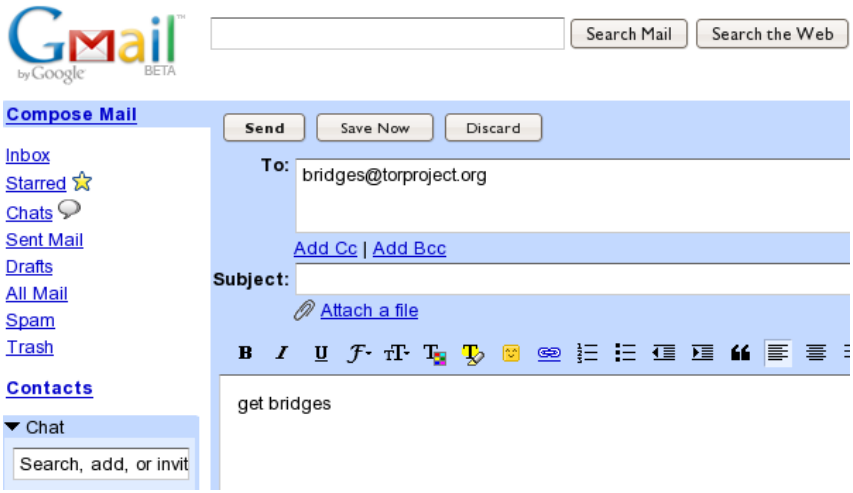
如果你怀疑Tor网络被封锁，你可以使用Tor的网桥功能。网桥这一功能专门为帮助Tor网络被封锁的用户使用 Tor。在使用网桥功能之前，用户必须已下载并安装Tor软件。

什么是网桥？

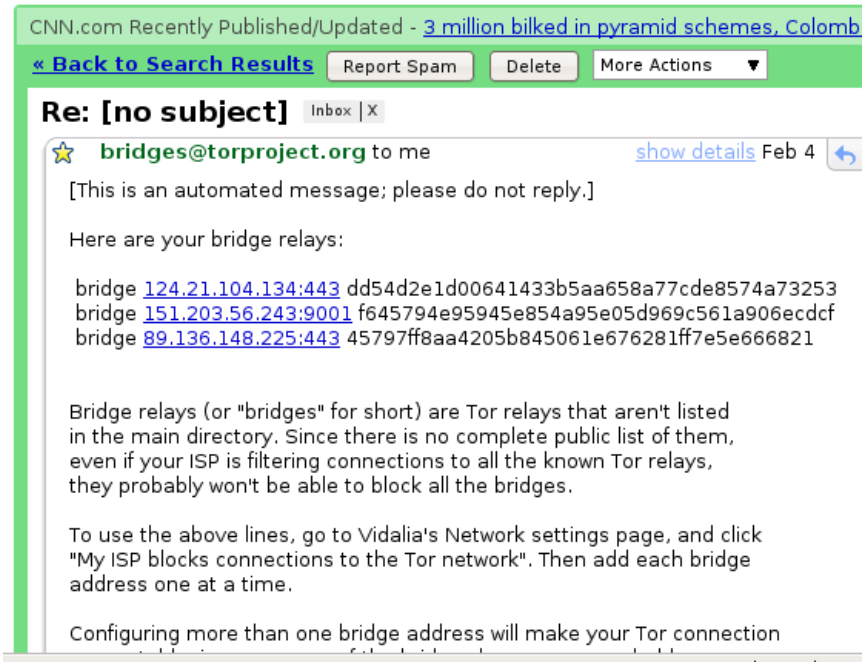
网桥中继（Bridge relay，简写为 bridge）是指那些没有在主要的公共Tor 目录中列出的Tor中继。这样做，是专门为了防止这些中继被封锁。即使用户的 ISP将所有公共所知的Tor中继封锁过滤掉，它也不可能封锁所有网桥。

在哪里可找到网桥？

为了使用网桥,用户需要知道一个桥中继地址，并将相关信息添加到用户的网络设置中。一件简单的获得网桥的方法是访问https://bridges.torproject.org/。如果这个页面被过滤，或者你需要更多的网桥，从Gmail帐号发送一封电子邮件至 bridges@torproject.org，在邮件主题中写“get bridges”（没有引号）。



很快，用户就可以收到一份邮件回复，其中包含了一些桥中继的信息。



重要注释：

1. 用户必须使用 Gmail 帐号发送请求。如果 torproject.org 接受其他邮件帐号的请求，那么攻击者可以很容易创建大量电子邮件地址，并快速获得所有桥中继信息。如果用户没有 Gmail 帐号，只需几分钟时间就可以申请一个。
2. 如果用户的互联网连接速度较慢，可以使用网址 https://mail.google.com/mail/h/，直接访问Gmail简单的HTML版本。

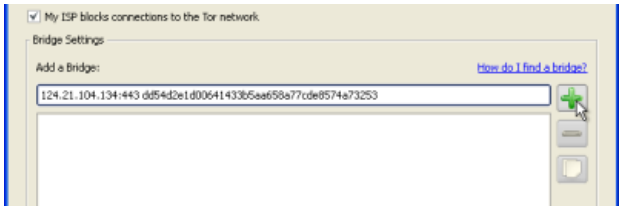
启动网桥并输入网桥信息

用户获得一些网桥的地址之后，必须使用用户想要使用的网桥地址对 Tor 进行配置。

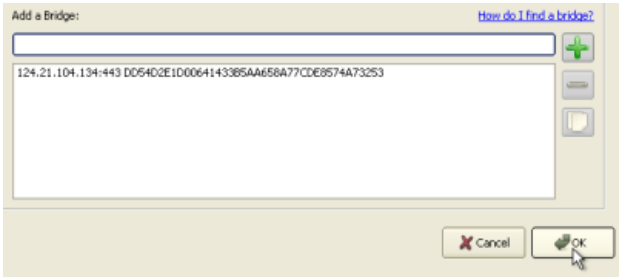
1. 打开 Tor 控制面板（Vidalia）。

单击“Settings”（设置）。弹出“Settings”窗口。

3. 单击“Network”（网络）。
4. 选中“My Firewall only lets me connect to certain ports”（防火墙仅允许连接某些端口）和“My ISP blocks Connections to the Tor network”（ISP 封锁了 Tor 网络的连接）。
5. 在“Add a Bridge”（添加网桥）字段中，输入回复邮件中的桥地址信息。
6. 单击位于该字段右边的绿色“+”号。该地址将添加到下面的文本框内，如下图所示：



7. 单击窗口底部的“OK”按钮，启动新的设置。



8. 在 Tor 控制面板中，停止并重启 Tor，就可以使用新的设置了。

注：

添加尽可能多的网桥地址。更多的网桥可增加可用性。要连接Tor网络，一个网桥已足够，然而，如果用户只使用了一个网桥，而它被封锁或停止运行时，用户的Tor网络连接将被切断，直到用户添加新的网桥。

想要在网络设置中添加更多网桥，用户只需重复上述步骤，添加更多网桥信息，这些信息可通过来自 bridges@torproject.org 的电子邮件获取。

JonDo

JonDo开始于一个被称为Java匿名代理（JAP）的德国大学项目，且已成为一款像Tor的强大匿名工具，其可以通过数个不同的独立服务器发送网页流量。

然而，并不像Tor，JonDo网络融合了由志愿者与母公司维持的其他主体运行的服务器。这种安排给了用户一个速度选择：免费的30-50KBit/s还是收费的>600 kBit/s。如需更详细的比较和价格清单，请参阅：https://anonymous-proxy-servers.net/en/payment.html。

一般信息

Supported operating system	
Localization	English, German, Czech, Dutch, French and Russian
Web site	https://www.jondos.de
Support	Forum: https://anonymous-proxy-servers.net/forum Wiki: https://anonymous-proxy-servers.net/wiki Contact form: https://anonymous-proxy-servers.net/bin/contact.pl?

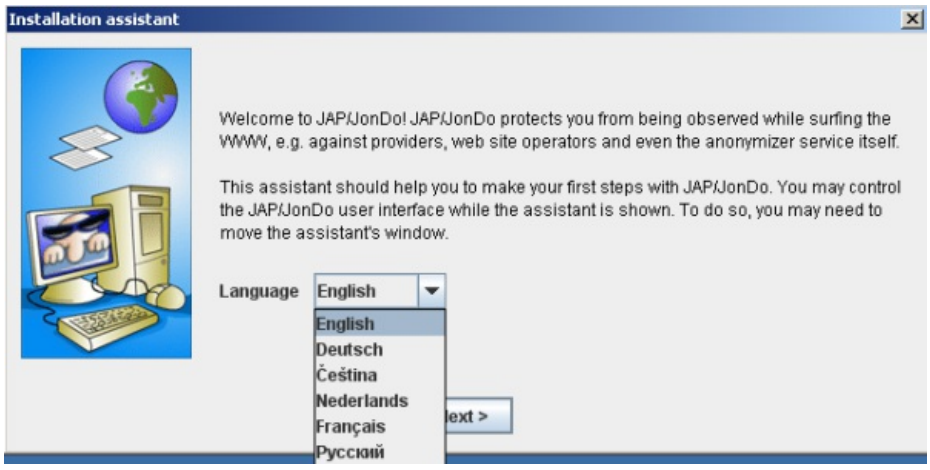
安装

要使用被称为JonDonym的JonDo网络，你需要从https://www.jondos.de/en/download为你的操作系统下载JonDo客户端。版本适用于Linux（大约9兆）、Mac OS X（大约17兆）和Windows（大约35兆）。
一旦你下载了客户端，就像安装其他软件到你的平台一样安装它。你可能会被询问是想安装它到你的个人电脑还是想创建一个便携版本。在我们的例子中，我们假定你安装JonDo到个人电脑。

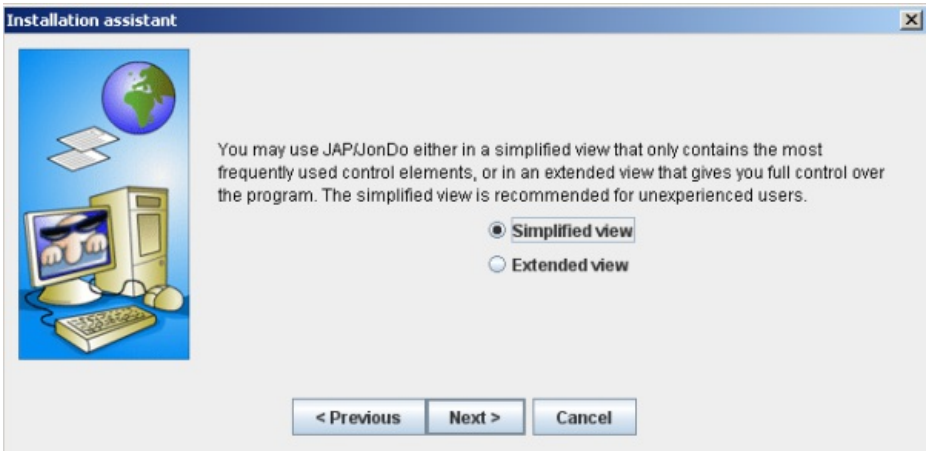
Windows用户还可能被邀请安装JonDoFox网络浏览器，这将在下面讨论。

配置和使用

当你第一次启动JonDo，你可以选择你想要显示的语言。

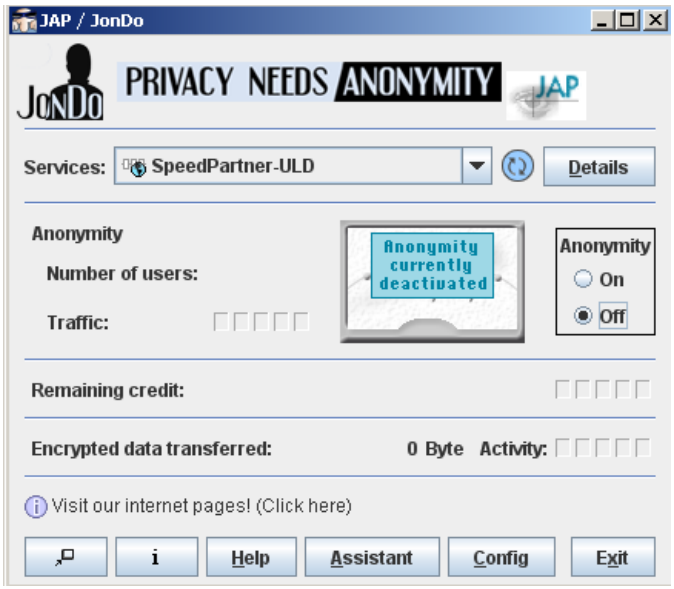


接下来，你可以选择使用该服务时你想看到的详细信息级别。没有经验的用户应选择“简化视图”。

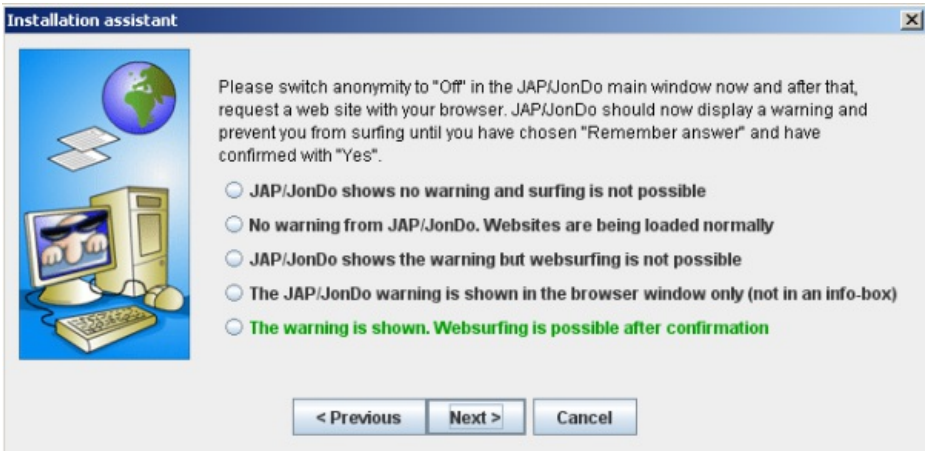


在下一个界面，安装助手会询问你选择你想要使用JonDo代理工具的网络浏览器。点击你的浏览器名称，并遵照说明操作。

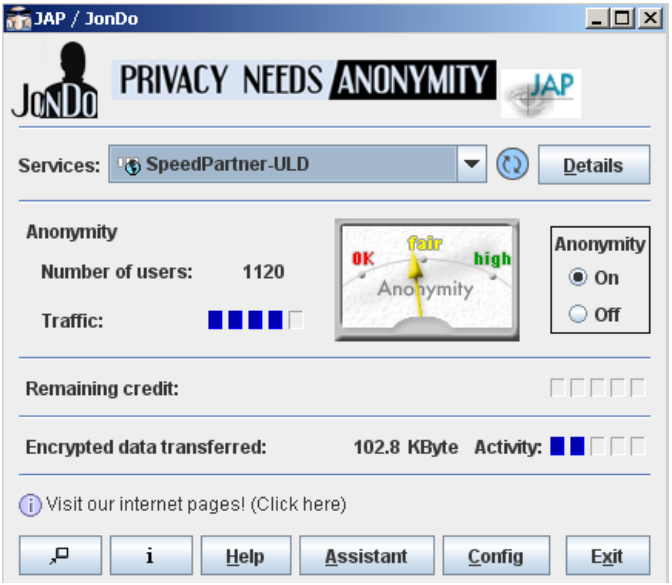
一旦这些完成，JonDo会询问你检测你的配置。在控制面板中，转换匿名到关闭，然后尝试用你刚配置好的浏览器打开一个网站。



如果JonDo显示了一个警告，且你必须选择“是”以查看该网站，那么一切都已正确配置，你可以选择“警告已显示。配置后可网上冲浪”。如果你看到任何其他描述，选择它，安装助手将给你更多关于如何解决该问题的信息。

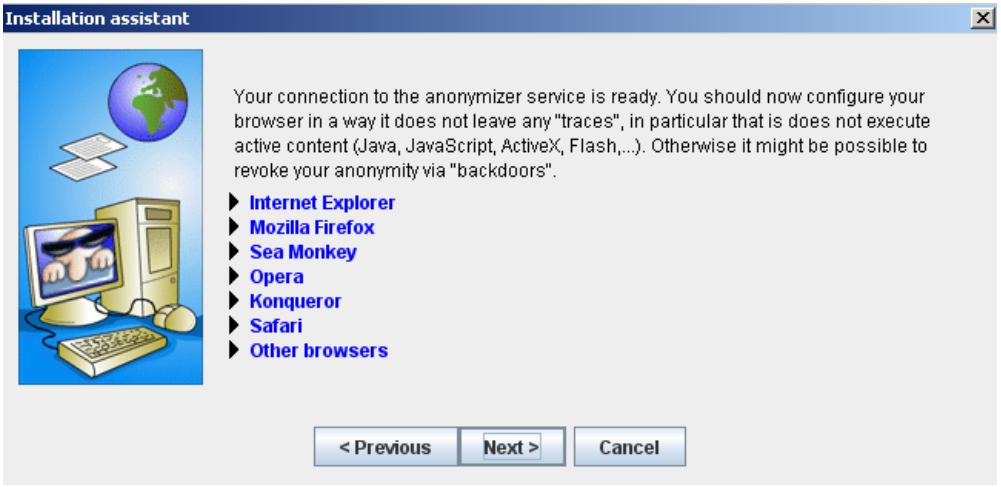


现在，采取第二步以确保正确配置：在控制面板中转换匿名到“开”，用你已配置的浏览器打开一个随机网站。

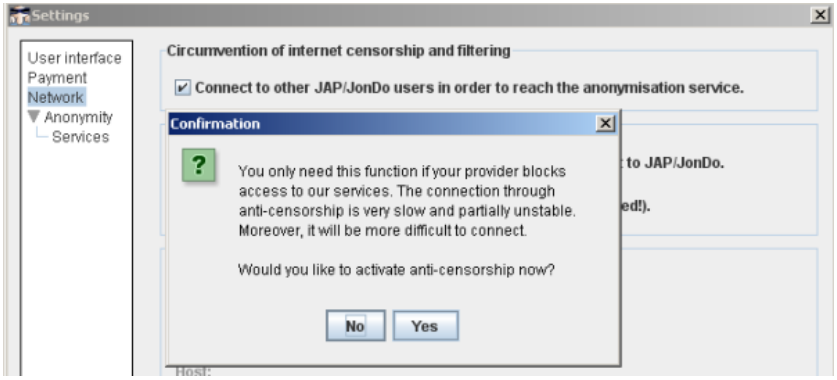


如果该网站载入，那么一切都很好，你可以点击“连接已建立，网上冲浪很好”。如果你看到其他描述，选择它，安装助手将帮助你解决该问题。

我们已差不多完成了。你已成功配置你的浏览器通过JonDo网络连接。现在，你还应配置你的浏览器以使其不会意外泄露任何信息。点击你的浏览器的名称以启动下列进程。



如果JonDo的标准服务器在你的国家已被封锁，你应尝试反审查选项。在控制面板中点击“配置”，选择网络选项卡。点击“连接到其他JAP/JonDo用户以到达匿名服务”。阅读警告并通过点击“是”确认。



要确认你正确配置了你的浏览器，你可以将其指向http://what-is-my-ip-address.anonymous-proxy-servers.net，它将告诉你是否有任何问题。

JonDoFox

为了更安全，JonDoNym团队提供了一个被称为JonDoFox的修改过的Firefox（火狐）网络浏览器。类似Tor浏览器套件，其阻止在使用匿名工具时泄露多余的信息。

你可以在 https://anonymous-proxy-servers.net/en/jondofox.html 下载该工具。

Your-Freedom

Your-Freedom是一款商业化的代理工具，其也提供免费（虽然较慢）的服务。

该软件可用于Windows,Linux和Mac OS操作系统，并将你连接到一个由大约遍布10个国家的30台服务器组成的网络。Your-Freedom也提供类似OpenVPN和SOCKS的先进服务，使其成为一个相对复杂的绕过互联网审查的工具。

一般信息

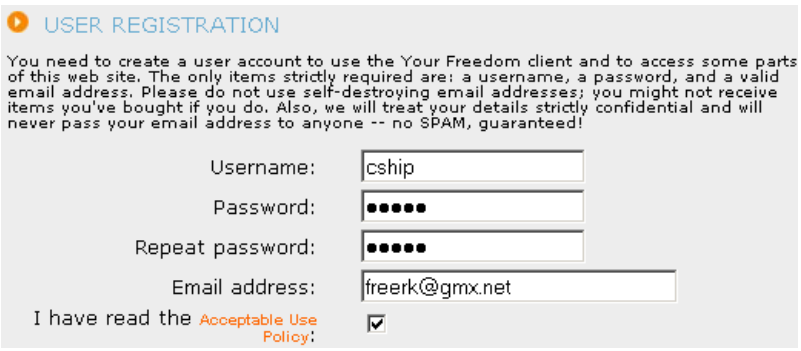
Supported operating system	
Localization	20 languages
Web site	https://www.your-freedom.net
Support	Forum: https://www.your-freedom.net/index.php?id=2 User guide: https://www.your-freedom.net/ems-dist/Your%20Freedom%20User%20Guide.pdf

准备使用 Your-Freedom

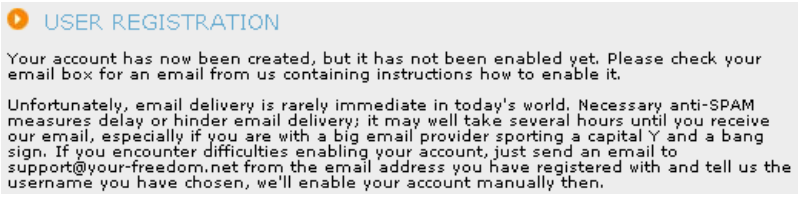
首先，从https://www.your-freedom.net/index.php?id=downloads下载自由工具。如果你已经安装了Java，你可以下载大约2兆的小版本。要检查是否已安装Java，登录http://www.java.com/en/download/testjava.jsp。如果你未安装Java，则下载大约12兆的完整版安装程序。所有文件同样可以从http://mediafire.com/yourfreedom获得。

如果你生活在一个政府审查互联网访问的国家，Your-Freedom可能用Sesawe帐户为你工作（用户名：sesawe，密码：sesawe）。如果这不起作用，那么你必须注册一个帐户。为了启动，请在网站https://www.your-freedom.net/index.php?id=170&L=0注册一个免费帐户。

点击两个登录框下的“首次访问？点击这里注册”链接。



在下一页，输入被要求的信息。只有用户名、密码和电子邮箱地址是必须的。其他信息是可选的。



你将看到一个提示你的注册差不多完成的信息，并且在几秒内，你会在你提供的地址收到一封电子邮件。

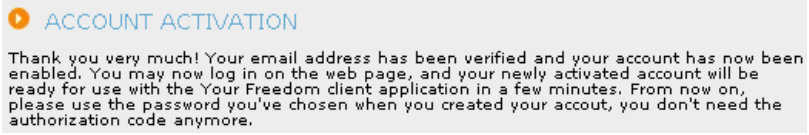
```
Dear Your Freedom user,

someone (likely you) has registered an account with us on
our web page, www.your-freedom.net, using your email
address. If it wasn't you or this was in error, please
disregard this email, we will not contact you again.

Your account "cship" has not been enabled yet.
To do this now, please copy the following link into your web
browser (or click on it if you can):

    http://www.your-freedom.net/index.php?id=171&username=cship&auth=bac8c89c
```

点击第二个链接（更长的那个）以确认你的注册。

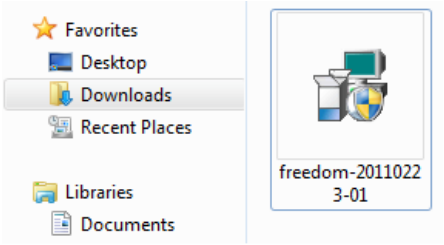


当你看到“谢谢你”界面时，你的帐户被激活了。

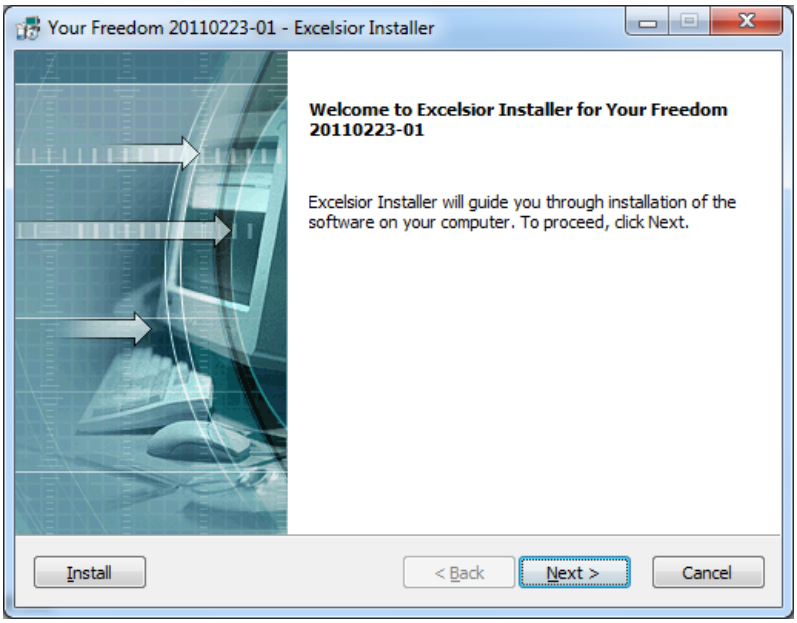
安装

以下说明和截图是在Windows下被抓取的，但所有步骤和设置对其他操作系统来说都是非常相似的。

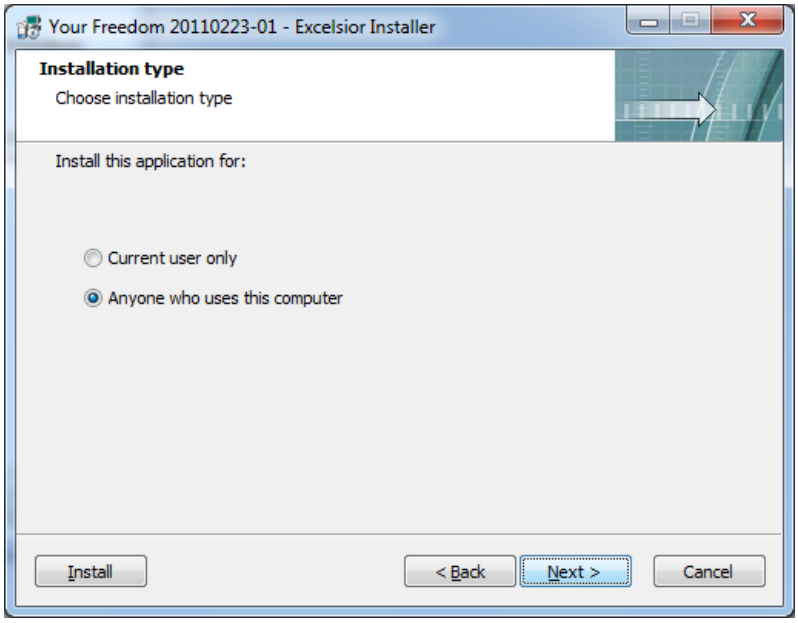
现在，准备安装Your-Freedom。



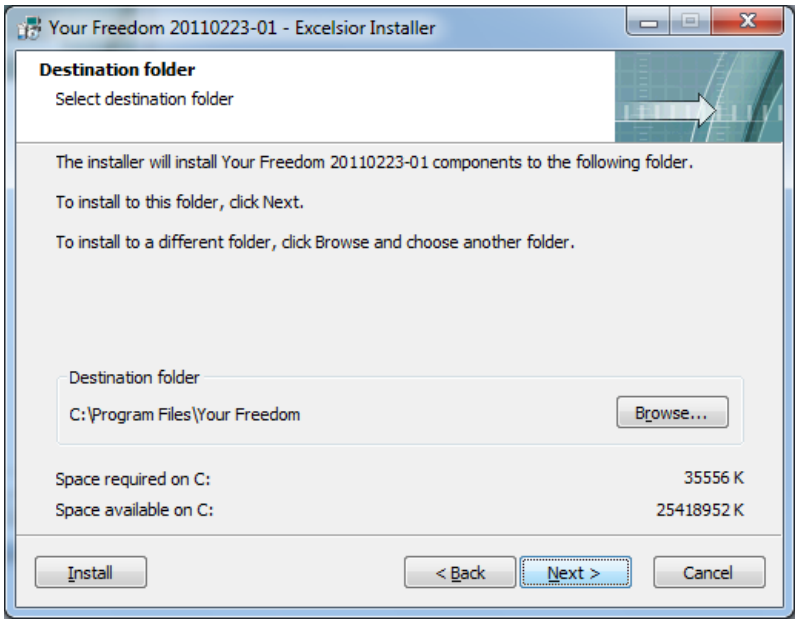
点击下载好的文件。文件名可能因为新版本的定期发布而有所不同。



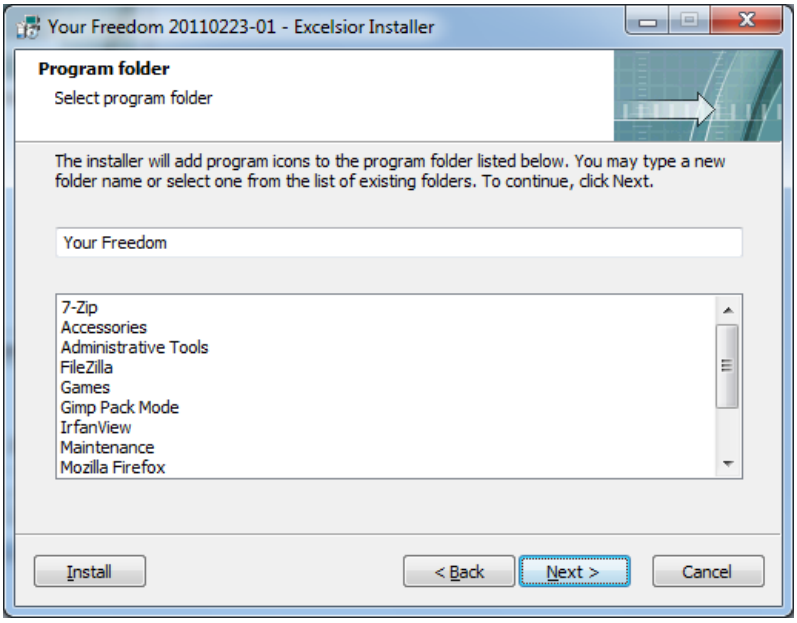
在第一个界面点击下一步。



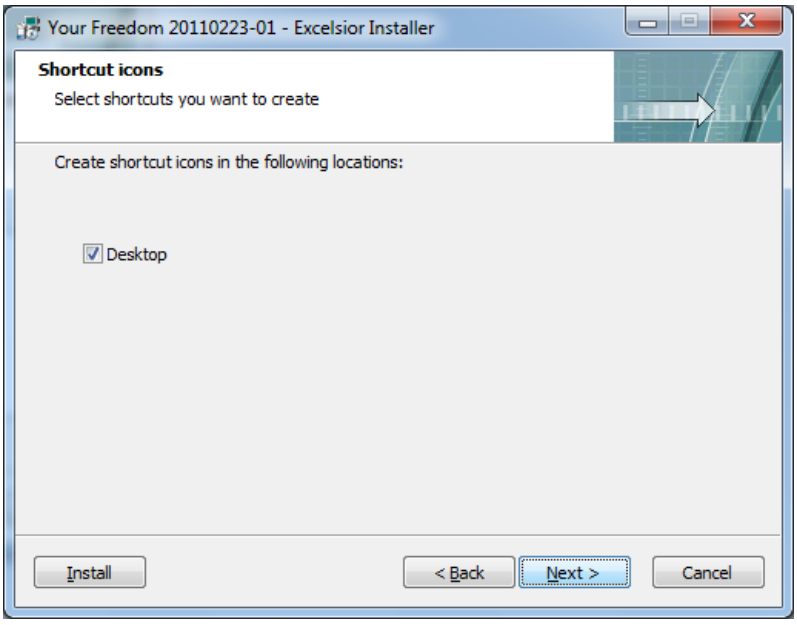
在下一个界面你可以选择该程序是只对你的帐户还是对你计算机的所有用户（共同）有用。然后点击下一步。



选择安装Your-Freedom的目录。大多数用户应接受默认选择。点击下一步。

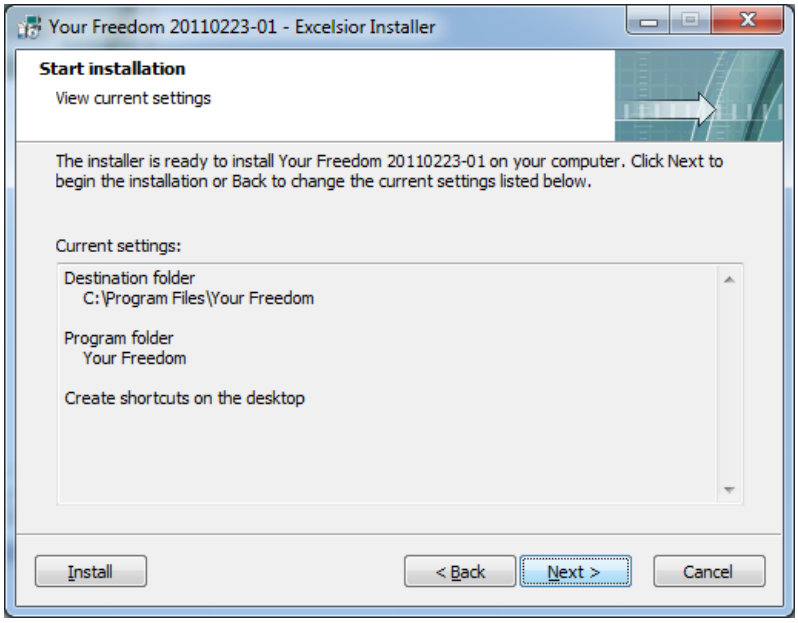


在安装程序的下一个界面，你可以改变在程序文件夹中使用的名称。你可以保留默认值不变并点击下一步。

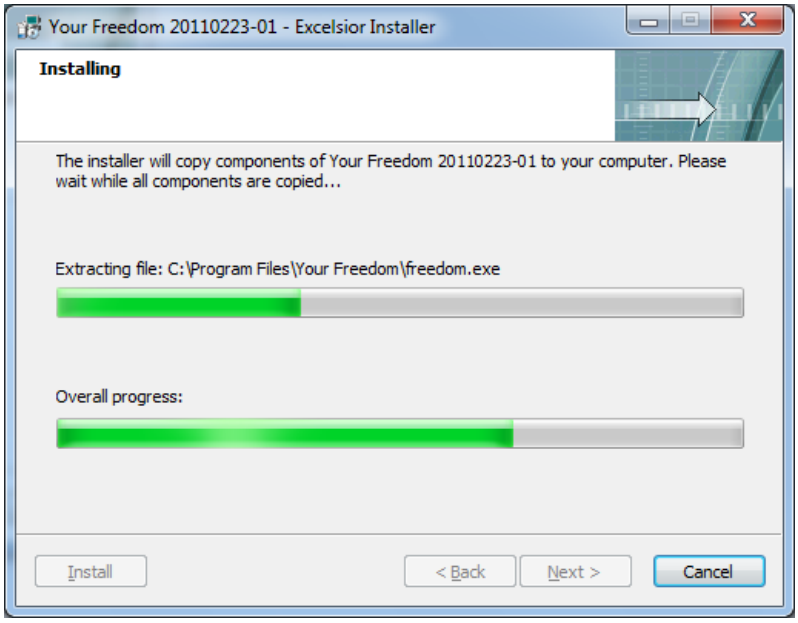


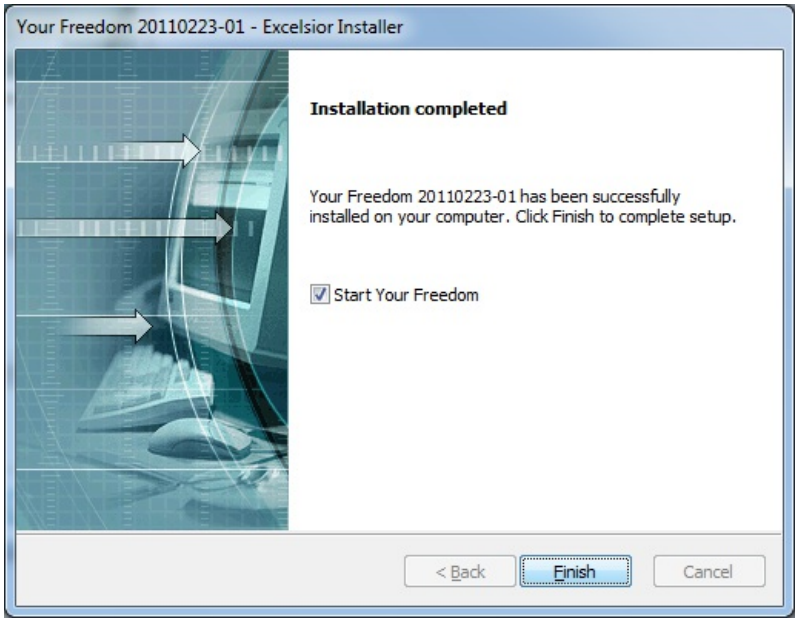
选择你是否想在桌面上创建一个图标。再次点击下一步。

在这里你可以看到你之前设置的汇总。确认后点击下一步，或者如果需要修改，点击返回。



现在，安装开始了。这可能需要几分钟，具体时间取决于你的电脑性能。





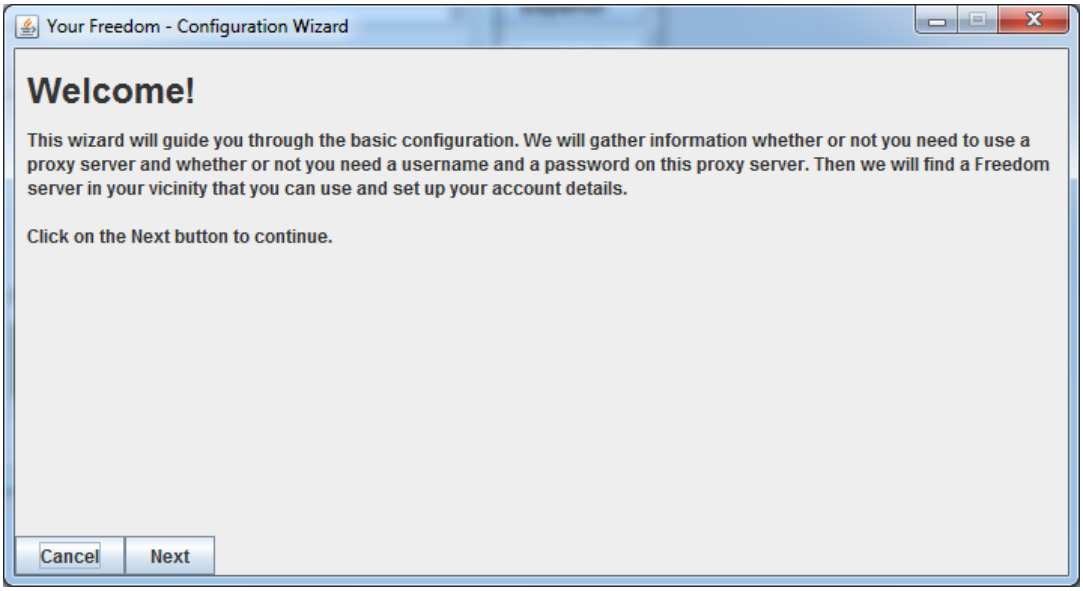
最后，安装完成。点击完成退出安装程序。

设置

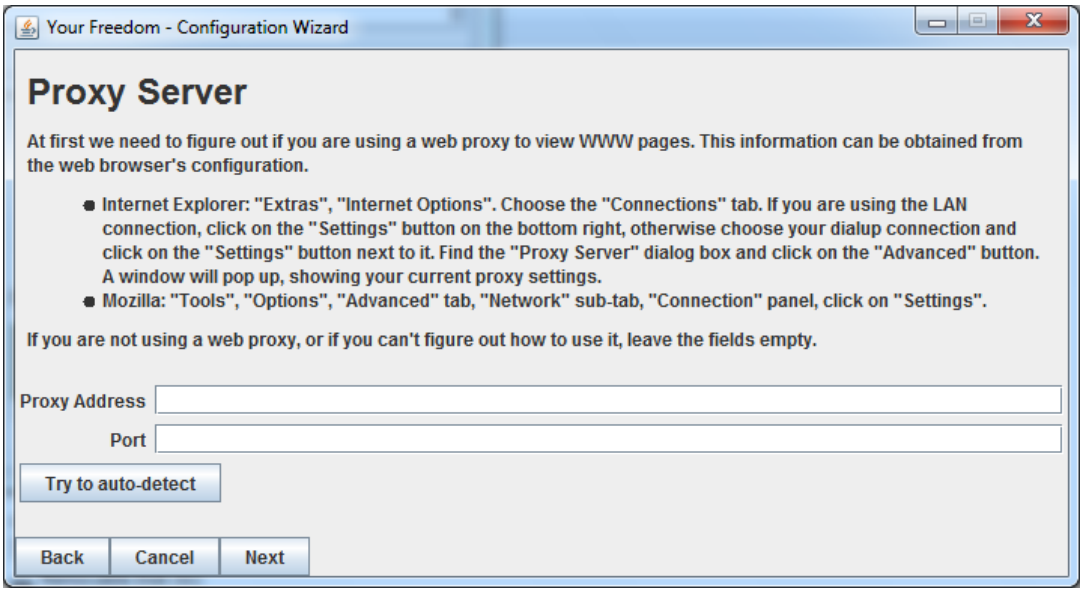
Your-Freedom会自动启动。如果你以后想人工启动它，点击你桌面的Your-Freedom图标（那个门）。

当你第一次启动Your-Freedom时，你需要配置它。

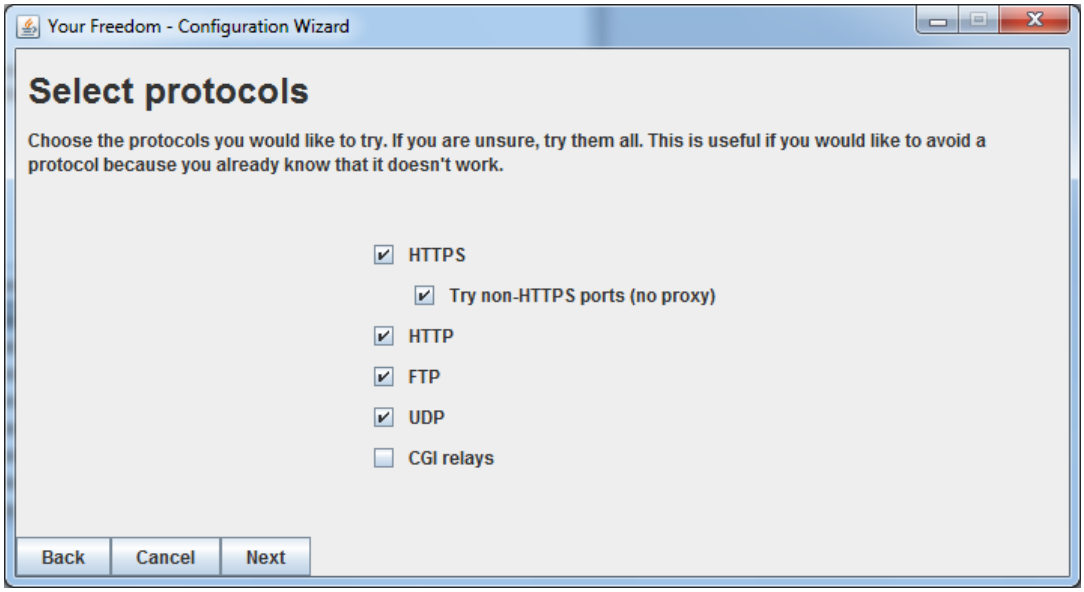
第一步是选择你的语言。点击你想要的语言。你以后也能改变这些设置。



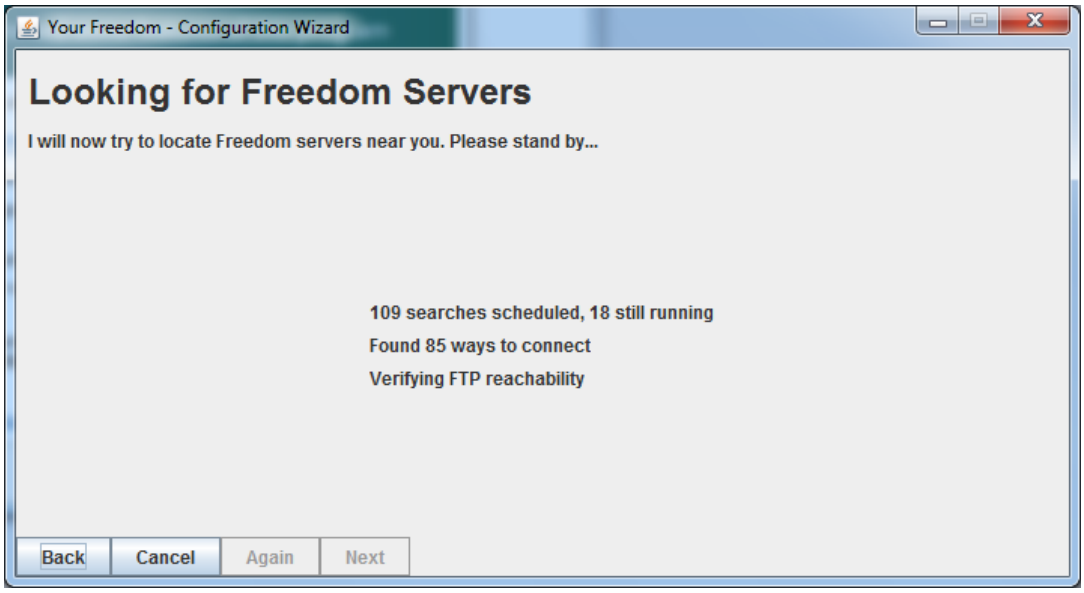
第一次启动完成后，你会看到一个配置向导。点击下一步。



在代理服务对话框中，程序将自动检测你可以使用的代理服务器的信息。点击下一步。

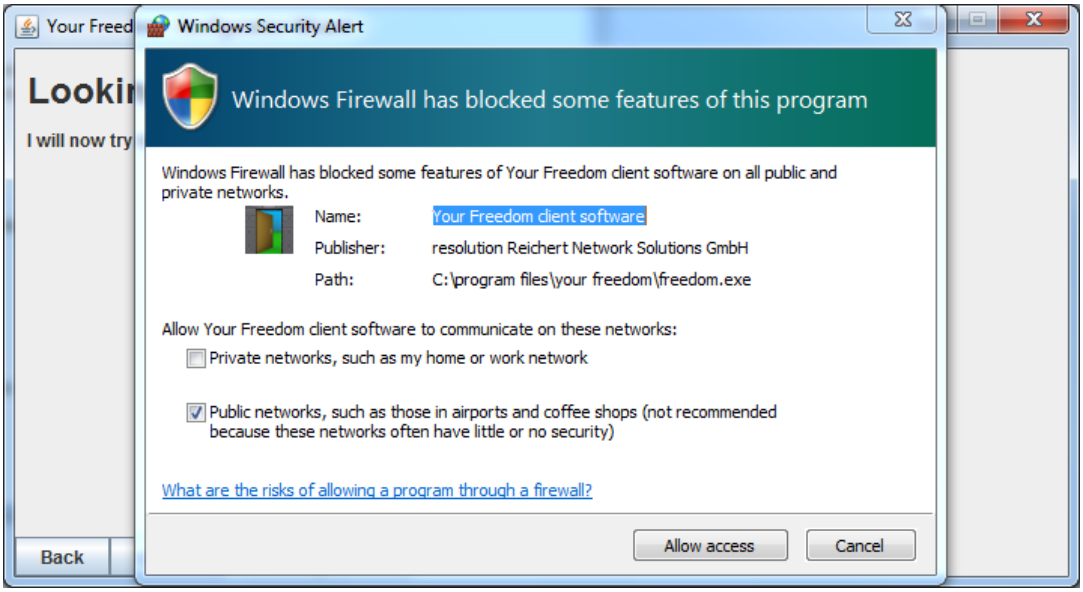


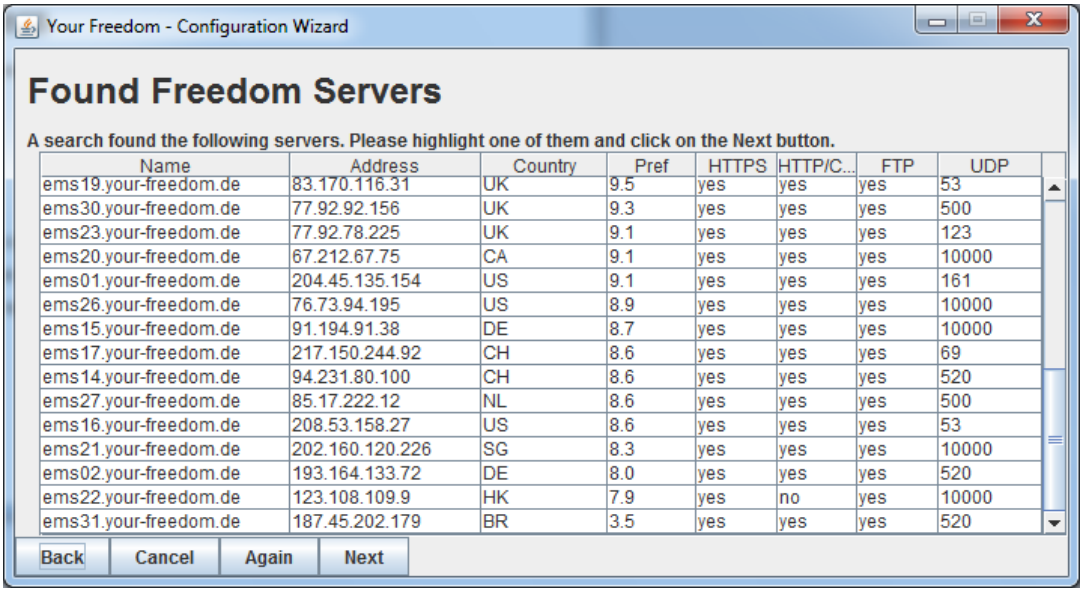
在选择协议对话框中，你应保持默认值并继续点击下一步。



接下来，Your-Freedom配置向导将做一些监测来搜寻可用的服务器，并检查你的连接和过滤的类型。这可能会花上一点时间。

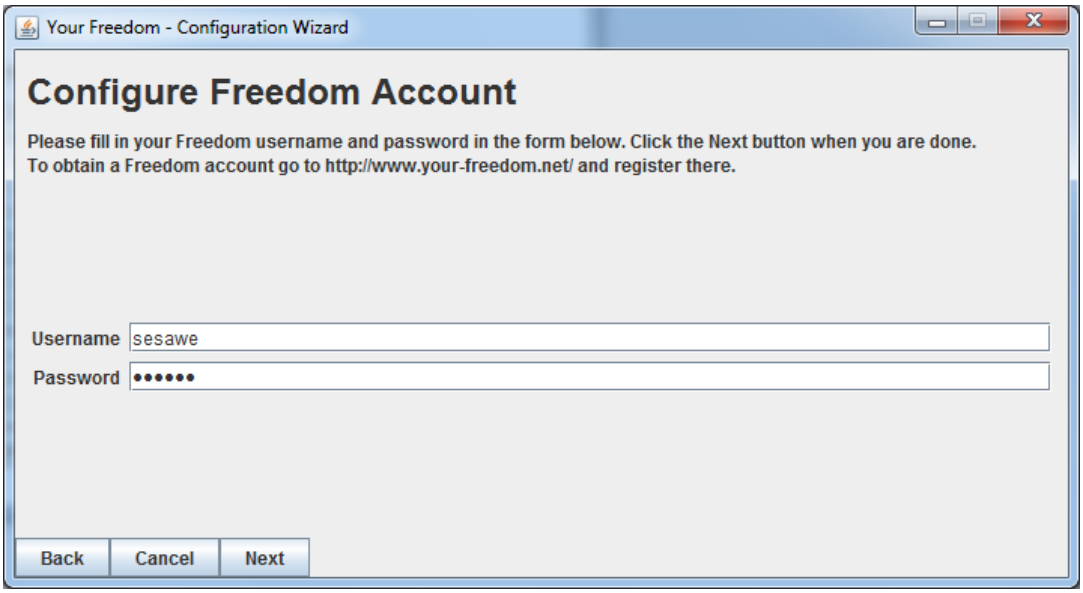
你可能从你的防火墙得到一个警告（这里例如来自Windows 7的一个警告）。你可以允许访问Your-Freedom。





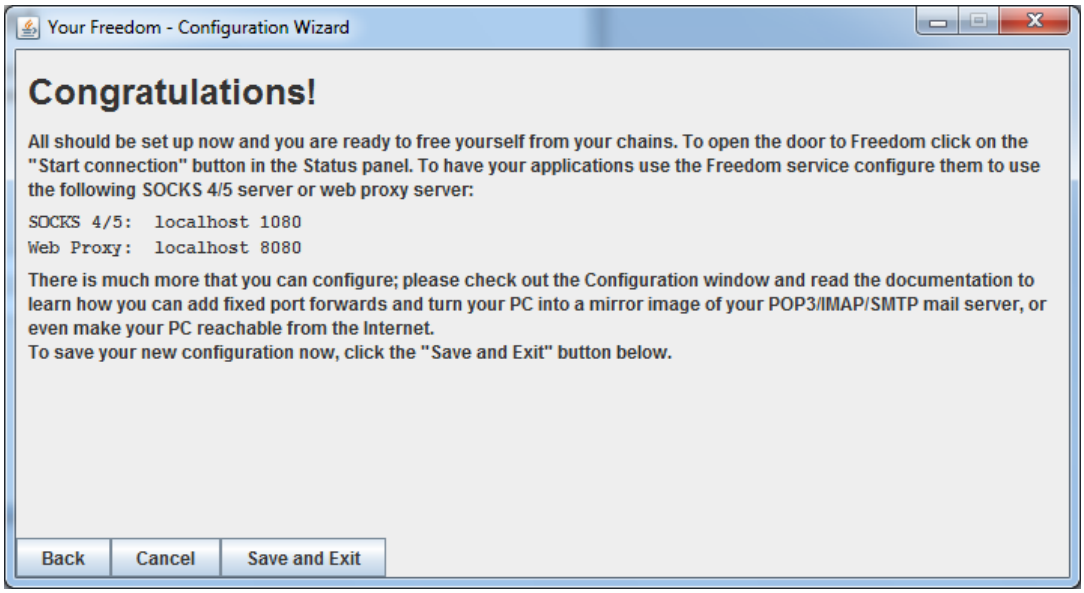
Name	Address	Country	Pref	HTTPS	HTTP/C...	FTP	UDP
ems19.your-freedom.de	83.170.116.31	UK	9.5	yes	yes	yes	53
ems30.your-freedom.de	77.92.92.156	UK	9.3	yes	yes	yes	500
ems23.your-freedom.de	77.92.78.225	UK	9.1	yes	yes	yes	123
ems20.your-freedom.de	67.212.67.75	CA	9.1	yes	yes	yes	10000
ems01.your-freedom.de	204.45.135.154	US	9.1	yes	yes	yes	161
ems26.your-freedom.de	76.73.94.195	US	8.9	yes	yes	yes	10000
ems15.your-freedom.de	91.194.91.38	DE	8.7	yes	yes	yes	10000
ems17.your-freedom.de	217.150.244.92	CH	8.6	yes	yes	yes	69
ems14.your-freedom.de	94.231.80.100	CH	8.6	yes	yes	yes	520
ems27.your-freedom.de	85.17.222.12	NL	8.6	yes	yes	yes	500
ems16.your-freedom.de	208.53.158.27	US	8.6	yes	yes	yes	53
ems21.your-freedom.de	202.160.120.226	SG	8.3	yes	yes	yes	10000
ems02.your-freedom.de	193.164.133.72	DE	8.0	yes	yes	yes	520
ems22.your-freedom.de	123.108.109.9	HK	7.9	yes	no	yes	10000
ems31.your-freedom.de	187.45.202.179	BR	3.5	yes	yes	yes	520

当向导完成后，你会看到发现的自由服务器界面，在此你可以选择一个服务器并再次点击下一步。



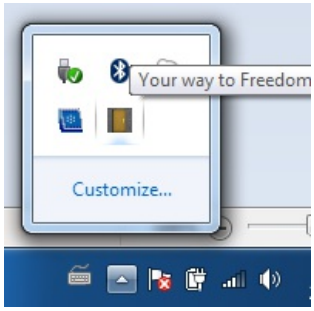
接着输入你先前创建的帐户信息。如果你没有，你可以通过向以下电子邮箱地址发送请求而获得免费访问：english@sesawe.net。

点击下一步。

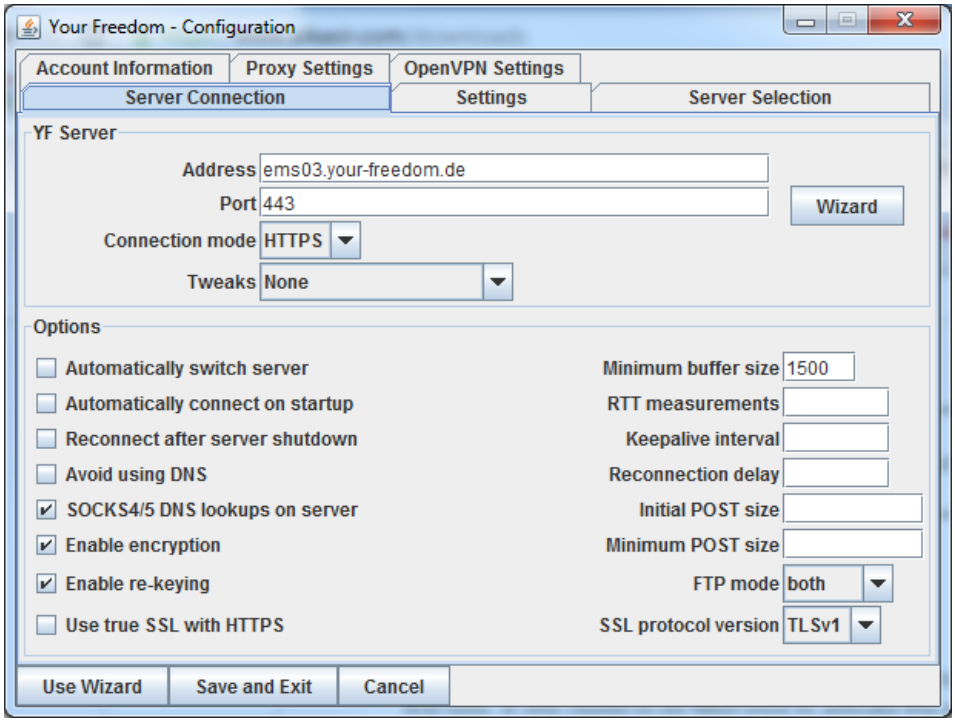


当你看到“恭喜”界面时，说明配置向导已经完成。点击保存并退出。

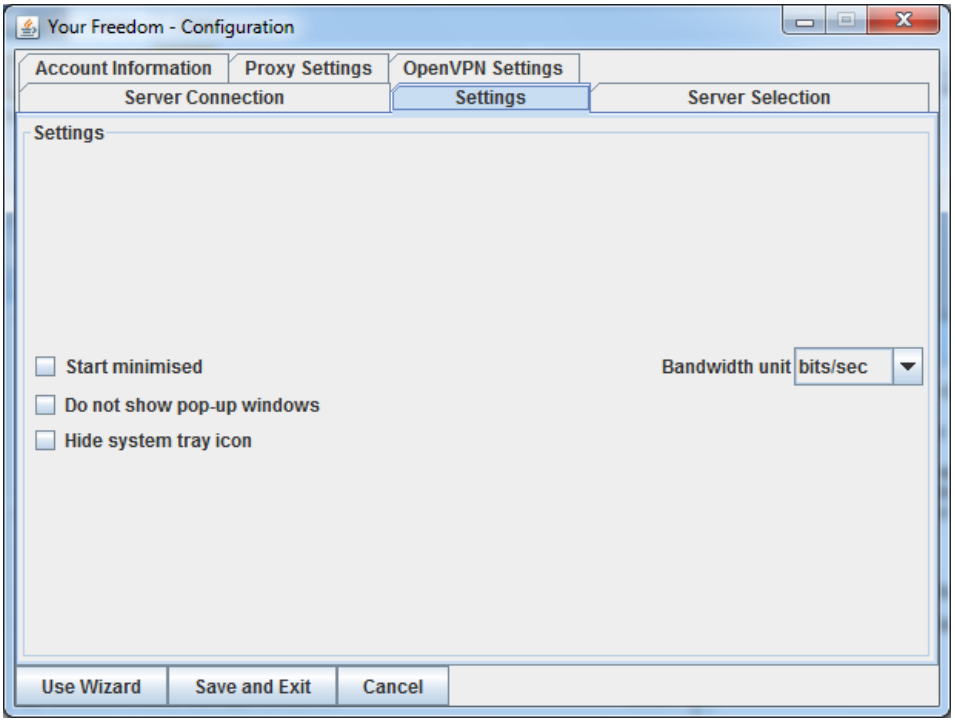
现在，Your-Freedom运行在你的计算机上，并且你可以在你的任务栏里看到一个图标。



为了更多安全性和更好地绕开过滤，你应在Your-Freedom主窗口中点击配置并选择以下截图中显示的选项从而调整选项。完成后点击保存并退出。



现在，Your-Freedom已经连接到了服务器，并且提供了一个你可以在你喜欢的类似Internet Explorer或Firefox软件中使用的本地代理。如果想自动对其进行配置，点击Your-Freedom主窗口中的应用程序标签，选择你想用的软件并点击确定。Your-Freedom将自动配置该软件，以使其通过加密的Your-Freedom链路连接到互联网。



如果想确认你正确使用了Your-Freedom，你可以访问网站https://www.your-freedom.net，并检查左边的你的踪迹栏目。如果检测到的不是你所在的国家，那么说明你正成功地使用加密的Your-Freedom链路访问互联网。

ADVANCED TECHNIQUES

域名和域名解析系统（DNS）

如果你确认、怀疑或被告知你网络上主要的审查技术基于DNS过滤和欺骗，你应该考虑这些技术。

使用其他的域服务器或域名

简单地说，DNS服务器将人性化的网络地址如google.com转换成IP地址，如72.14.207.19，它确认与域名相关联的网络上特定的服务器。这一服务通常通过你的互联网服务提供商维护的DNS服务器进行。简单的DNS封锁通过错误的或无效的回应DNS请求来实施，防止用户找到他们所需的服务器。对审查这一方来说这个方法很容易被实施，所以它广为使用。记住通常集中审查方法结合使用，所以DNS封锁可能不是唯一的问题。

使用这两种方法，你有可能绕过这个封锁：更改你电脑的DNS设置，使用其他的DNS服务器，或者编辑你的hosts文件。

使用其他的DNS服务器

你可以使用第三方服务器，绕开你本地的互联网服务提供商的DNS服务器,让你的电脑找到域名地址，它们可能被互联网服务提供商的DNS服务器封锁。有大量的免费、国际范围内可用的DNS服务器可使用。OpenDNS (https://www.opendns.com) 提供一个这样的服务，并有如何更改你电脑使用的DNS服务器的指南(https://www.opendns.com/smb/start/computer)。这里还有一个更新的全球可使用的DNS服务器列表： http://www.dnsserverlist.org。

这是一份公开提供的DSN服务器清单，转自网络审查维基（Internet Censorship Wiki），地址：http://en.cship.org/wiki/DNS。（部分服务自身可能封锁有限数量的网站，查阅提供商的网站进一步了解它们的政策）

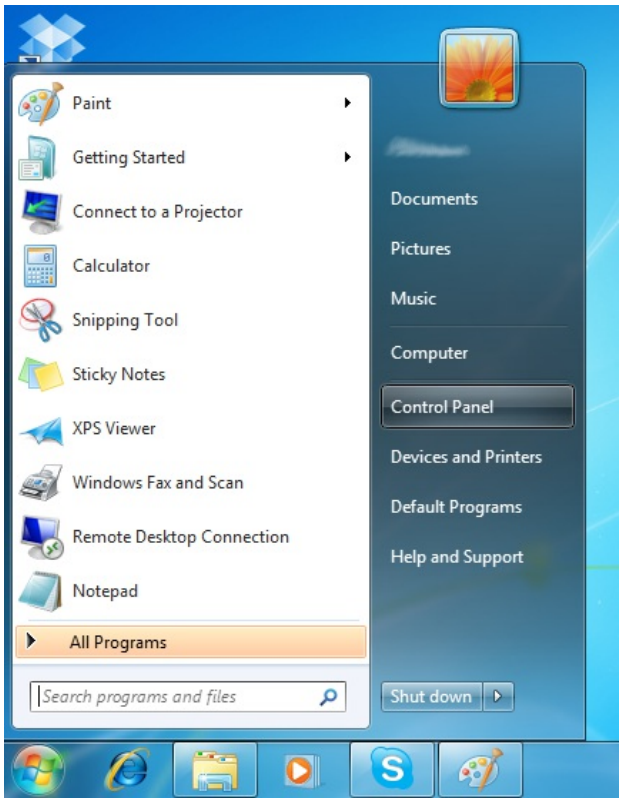
Publicly-available DNS servers

Address	**Provider**
8.8.8.8	Google
8.8.4.4	Google
208.67.222.222	OpenDNS
208.67.220.220	OpenDNS
216.146.35.35	DynDNS
216.146.36.36	DynDNS
74.50.55.161	Visizone
74.50.55.162	Visizone
198.153.192.1	NortonDNS
198.153.194.1	NortonDNS
156.154.70.1	DNS Advantage
156.154.71.1	DNS Advantage
205.210.42.205	DNSResolvers
64.68.200.200	DNSResolvers
4.2.2.2	Level 3
141.1.1.1	Cable & Wireless

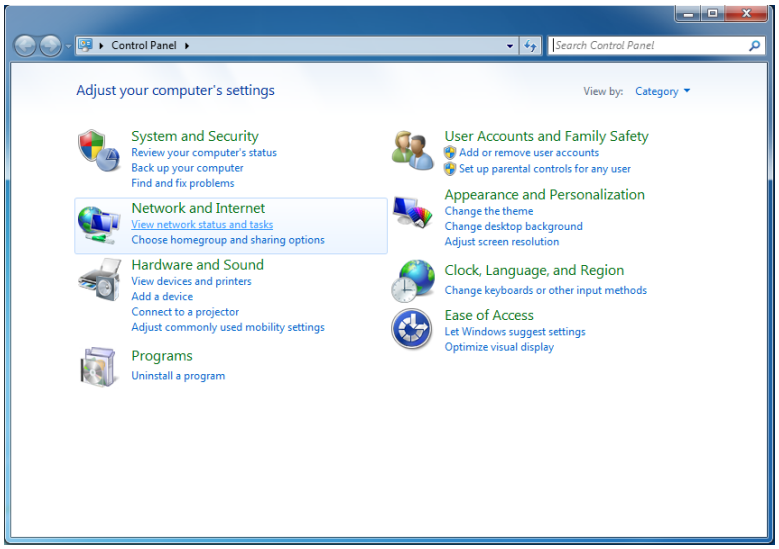
选择好DNS服务器后，你需要在你的操作系统的DNS设置里输入你的选择。

在Windows更改你的DNS设置

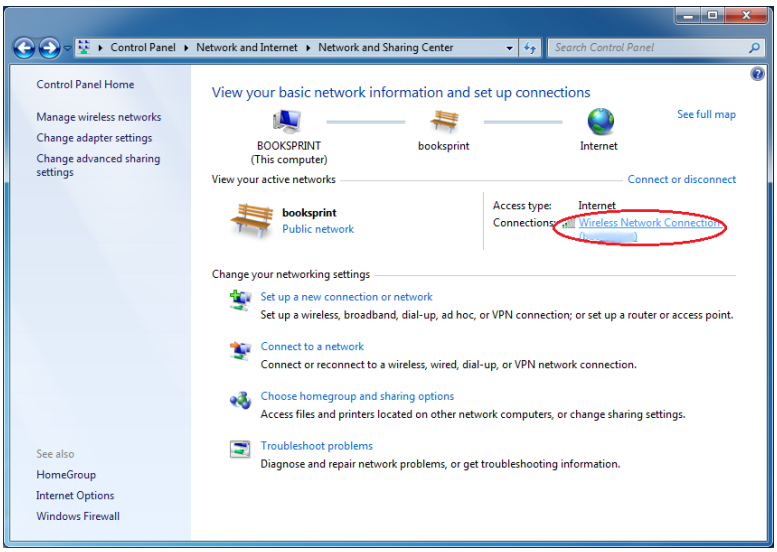
1. 在开始菜单（Start menu）打开你的控制面板（control panel）。



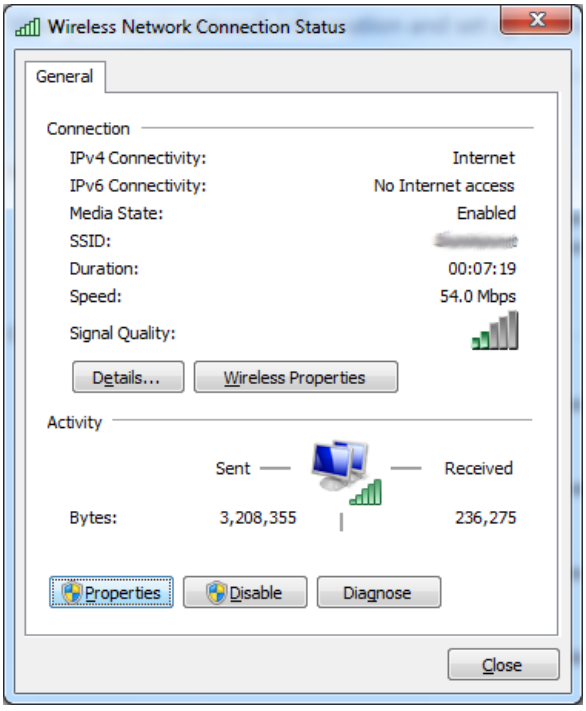
2. 在网络和Internet连接，，点击“查看网络状态和任务”（ "View network status and tasks"）。



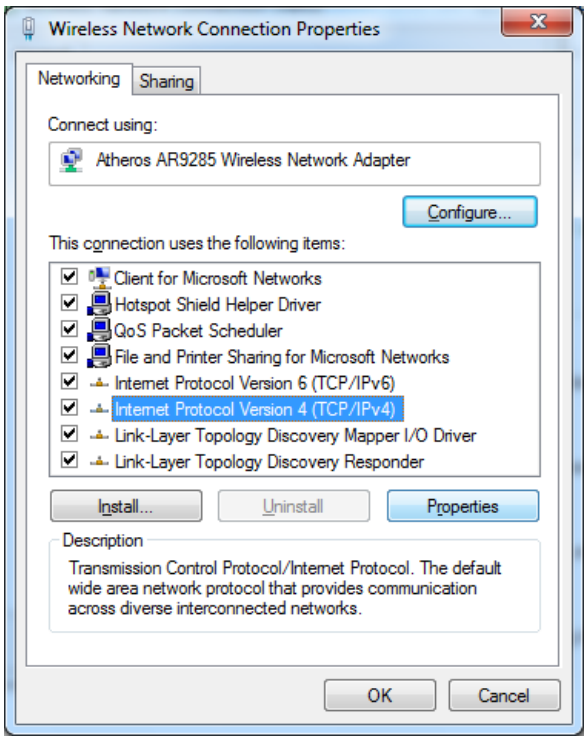
3. 在窗口的右边点击你的无线网络连接。



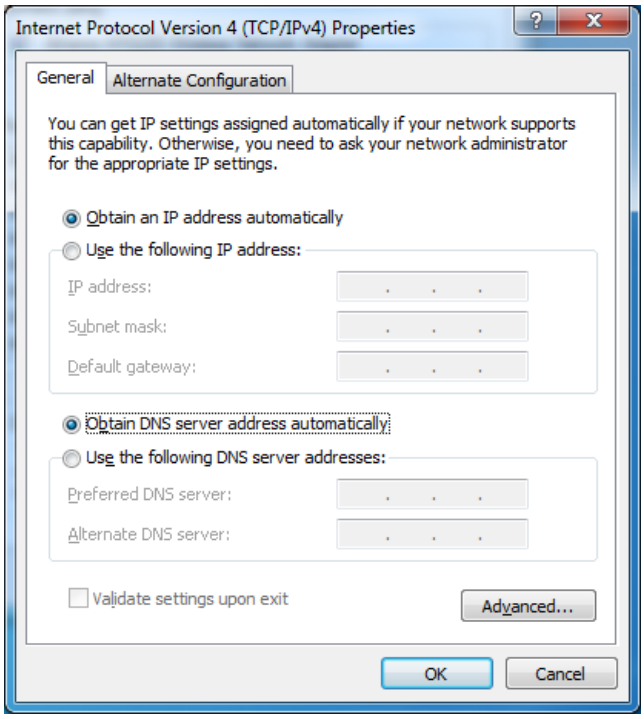
4. 无线网络连接（Wireless Network Connection ）状态窗口将会被打开.。点击属性（Properties）。



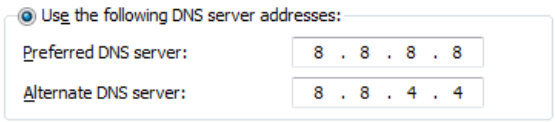
5. 在无线网络连接（Wireless Network Connection ）属性（Properties）窗口选择 Internet Protocol 版本4 (TCP/IPv4)，再点击属性（Properties）。



6. 你现在应该在Internet Protocol 版本 4 (TCP/IPv4) 属性（Properties ）窗口，在这你将指定你的替代DNS地址（例如，Google Public DNS)。



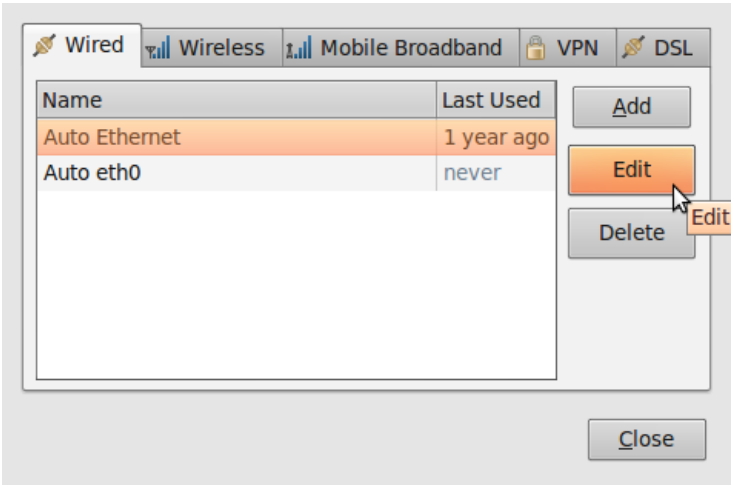
7. 在窗口的底部，点击“使用下面的DNS服务器地址（ "Use the following DNS server addresses" ），用你偏爱的DNS服务器IP信息填写输入框。完成后，，点击OK。默认情况下，将使用第一个DNS服务器。备选DNS服务器可以来自另一公司。



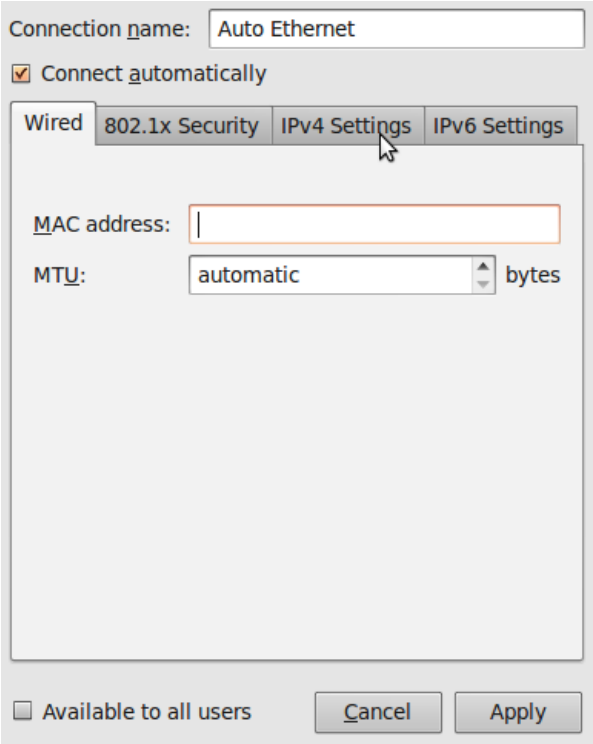
在Ubuntu更改你的DNS设置

1. 在系统菜单到首选项（Preferences）› 网络连接（Network Connections）。

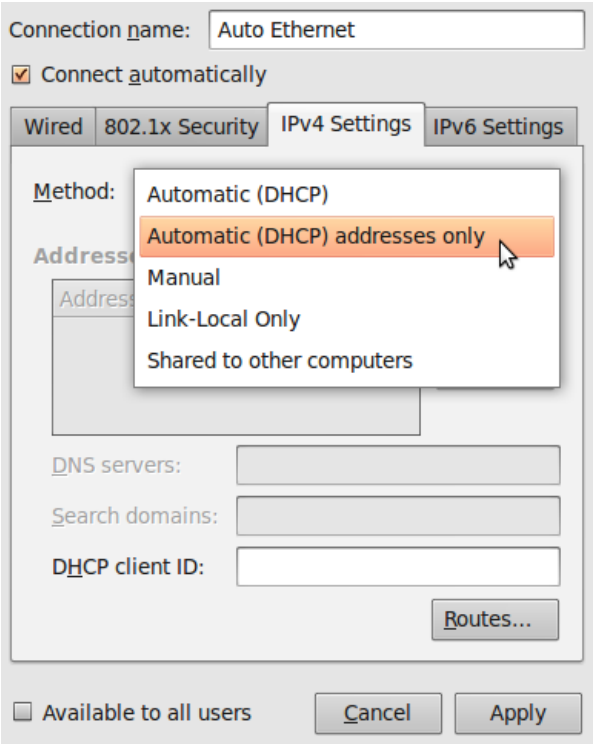
2. 选择连接，你想为它配置Google Public DNS 。如果你想更改Ethernet 连接（有线）的设置，选择有线（Wired）选项卡，然后在列表中选择你的网络界面。如果你想为无线连接更改设置，选择无线（wireless）选项卡，然后选择合适的无线网络。



3. 点击编辑（Edit），在出现的窗口里，选择IPv4 设置选项卡。

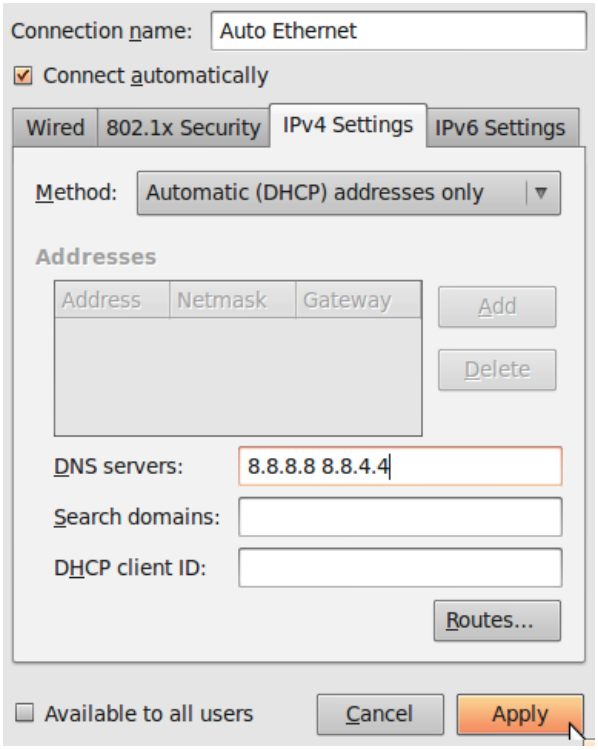


4. 如果选择的方法是Automatic (DHCP)，打开下拉菜单（dropdown menu），选择"Automatic (DHCP) addresses only"更换。如果是其他方法，不需要更改。



5. 在DNS服务器输入框，输入你的替代DNS IP 信息，以一个空格隔开。例如，如果你想添加Google DNS，输入8.8.8.8 8.8.4.4

6. 点击应用（Apply）保存更改。如果提示输入密码或确认，输入密码或确认你想更改。



7. 对你想更改的每个网络连接，重复步骤 1-6。

编辑 hosts文件

如果你知道被你的网络服务提供商的DNS服务器封锁的网站或网络服务的IP地址，你可以把这个网站添加到你的Hosts文件里，它是一个本地的name-to-IP地址列表，在使用外面的DNS服务器前，你的电脑将使用它。Hosts文件是文本文件，格式非常简单，它的内容类似:

208.80.152.134 secure.wikimedia.org

每一行包括一个IP地址, 然后一个空格,再一个域名。你可以添加任何数量的网站到你的hosts文件（但请注意如果你使用错误的地址，它可能会阻碍你通过地址访问你这个网站，直到你修正它，或者把它从列表中移除）。

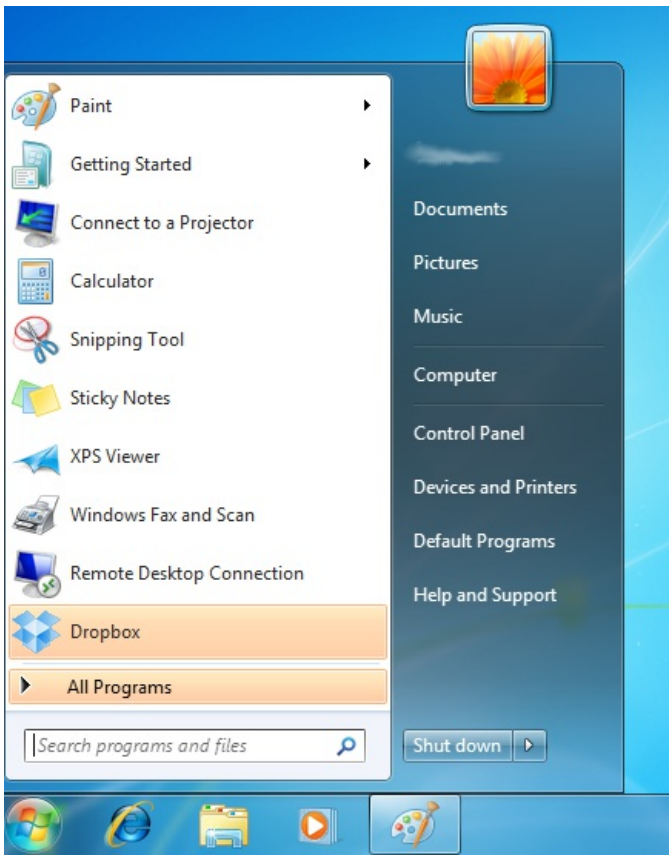
如果你因为你的网络服务提供商的DNS封锁，找不到网站的IP地址，有许许多多的服务可以帮助你进行一次未受审查的DNS查询。例如，你可以使用http://www.dnsstuff.com/tools上的任意一款工具。

你也可以考虑使用http://www.traceroute.org上的工具，它是不同的网络服务提供商提供的高级网络诊断工具。起初用来诊断意外的网络中断而不是故意的审查，但是它也可以用来诊断审查。这些工具也包含查找服务器IP地址的功能。

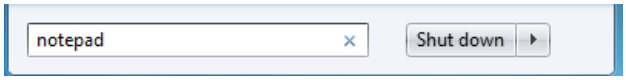
在Windows Vista / 7编辑hosts文件

你需要一个简单的文本编辑器, 如Notepad, 用来编辑你的hosts文件。在Windows Vista 和Windows 7, 你的hosts文件通常位于C:\Windows\system32\drivers\etc\hosts。

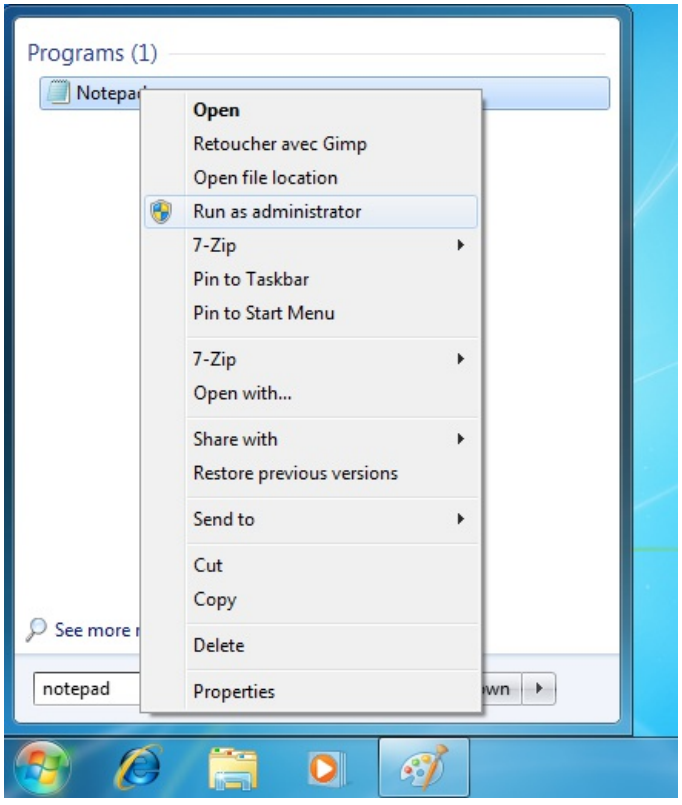
1. 点击开始（Start）按钮。



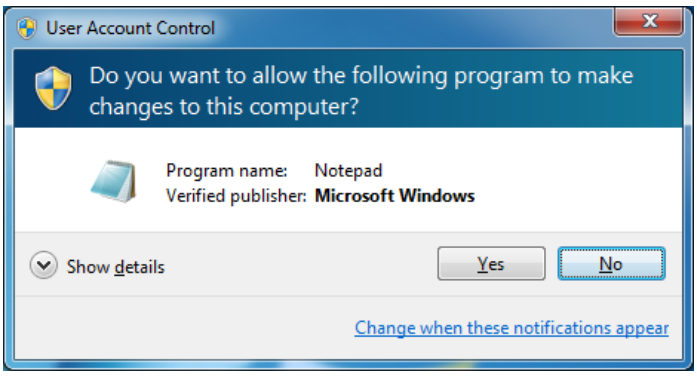
2. 在搜索框（search box）输入 "notepad" 。



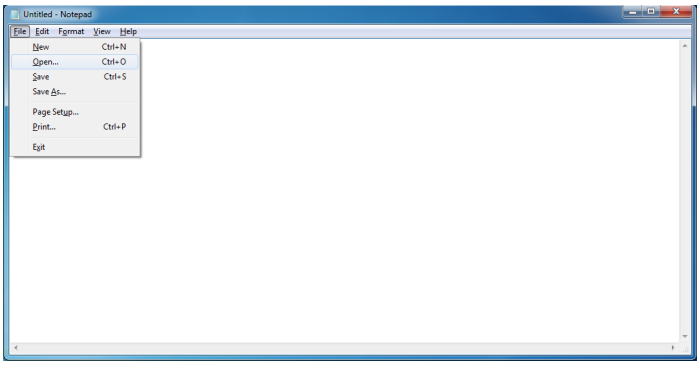
3. 找到这个程序后，右击它并选择“用管理员身份运行“（"Run as administrator"）。



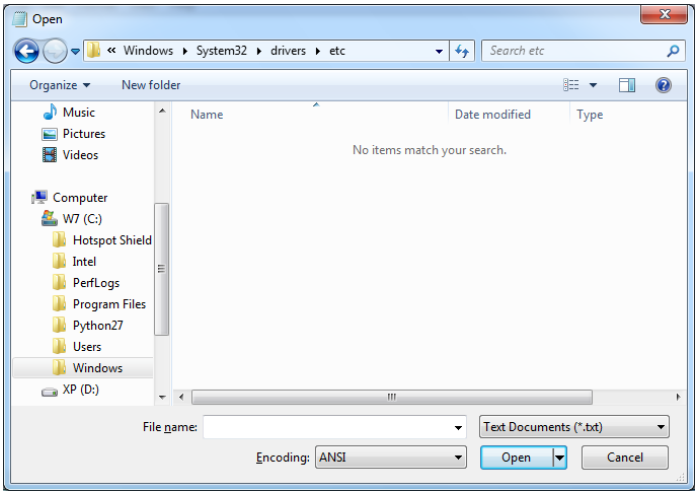
4. Windows 将征求你同意更改这些文件。点击Yes。



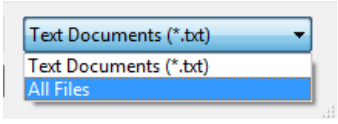
5. 在文件（File）菜单，选择打开（Open）。



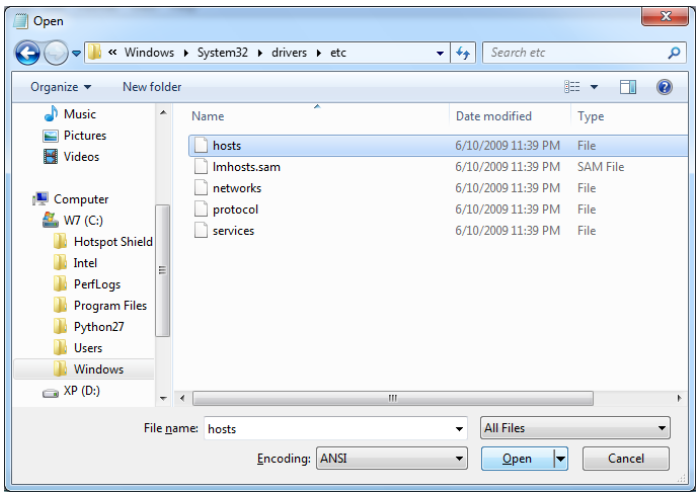
6. 浏览 C:\Windows\System32\Drivers\etc\.。你可能注意到文件夹最初似乎是空的。



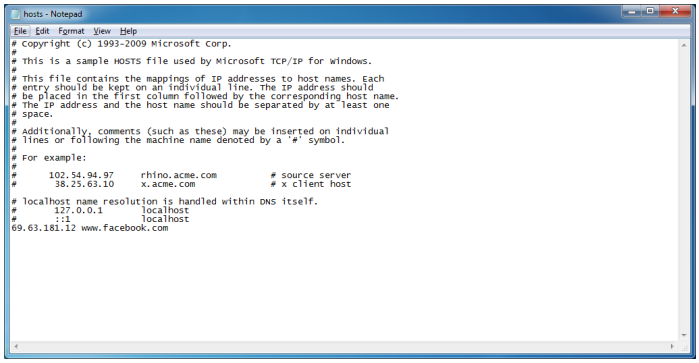
7. 在打开对话框（open dialog）的右下方，选择所有文件（All Files）。



8. 选择以 "hosts"命名的文件，点击打开（Open）。



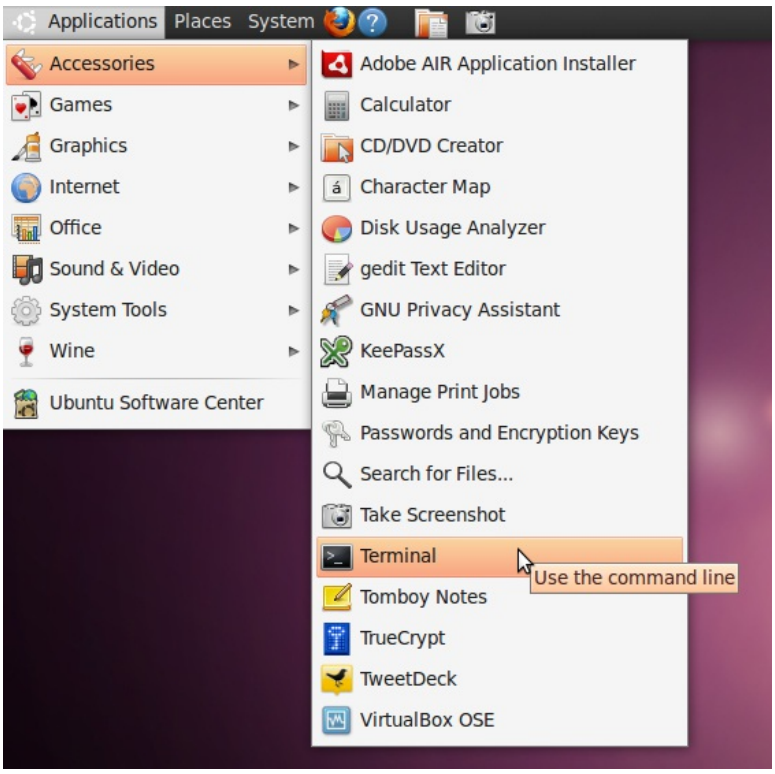
9. 举例，在文件的末尾添加一行 "69.63.181.12 www.facebook.com" ， 按Ctrl+S 或选择文件（ File ）› 保存（Save from the menu.）保存它。



在Ubuntu编辑你的hosts文件

在Ubuntu, 你的hosts文件位于located in /etc/hosts。编辑它，你需要了解命令行的知识。 请参考这本书“命令行“这一章，作为这个功能的简单介绍。

1. 在你的应用程序菜单（Applications menu）附件（Accessories）› 终端（Terminal ），打开终端（terminal）。



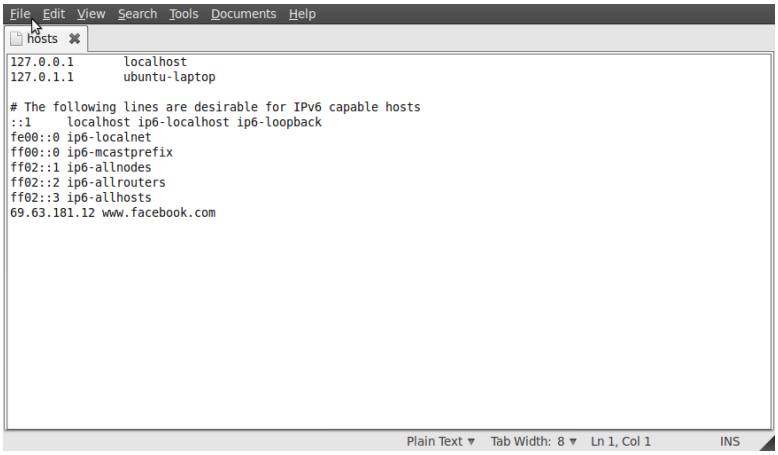
2. 使用下面的命令行自动添加一行到你的hosts文件：

   echo 69.63.181.12 www.facebook.com | sudo tee -a /etc/hosts

3. 为修改文件，你可能被提示输入密码。一经认定, 命令将添加"69.63.181.12 www.facebook.com" 到hosts文件的最后一行。

4. 可选项：如果你觉得用图形界面更舒服，打开终端（Terminal ），使用下面的命令行启动文本编辑器：sudo gedit /etc/hosts

5. 为修改文件，你可能被提示输入密码。窗口打开后，仅需添加一行 "69.63.181.12 www.facebook.com" 到文件的最后部分，按 Ctrl+S 或选择文件（File）> 保存（Save from the menu）保存它。



HTTP 代理

称为应用代理的软件可使互联网中的一台计算机处理来自其他计算机的请求。最常见的应用代理有**HTTP**代理和**SOCKS**代理，前者处理网站请求，后者处理来自多种应用程序的请求。在本章节中，我们将介绍 HTTP 代理以及其工作原理。

代理的好与坏

网络运营商可使用应用代理对互联网进行审查或者监控用户的所作所为。但是，应用代理还可为用户用于规避审查以及其他网络限制。

限制访问的代理

网络运营商可能要求用户只通过某个代理访问互联网（或网页）。网络运营商可编写程序，利用这种代理记录用户访问的内容，并且还可以拒绝用户对某些网站或服务的访问（IP 封锁或端口封锁）。在这种情况下，网络运营商可以使用防火墙来封锁未通过限制性代理的连接。这种配置有时称为强制性代理，因为用户被要求必须使用它。

用于规避封锁的代理

应用代理同时还可以帮助用户规避封锁的限制。如果用户可以与位于非限制区域的应用代理计算机建立连接，那么就可以利用这种代理的非限制连接来突破封锁。有时，某个代理对公众开放，则成为公共代理。在互联网受限的国家，网络封锁的管理人员如果获悉这些公共代理，将会封锁这些代理。

在何处可找到应用代理

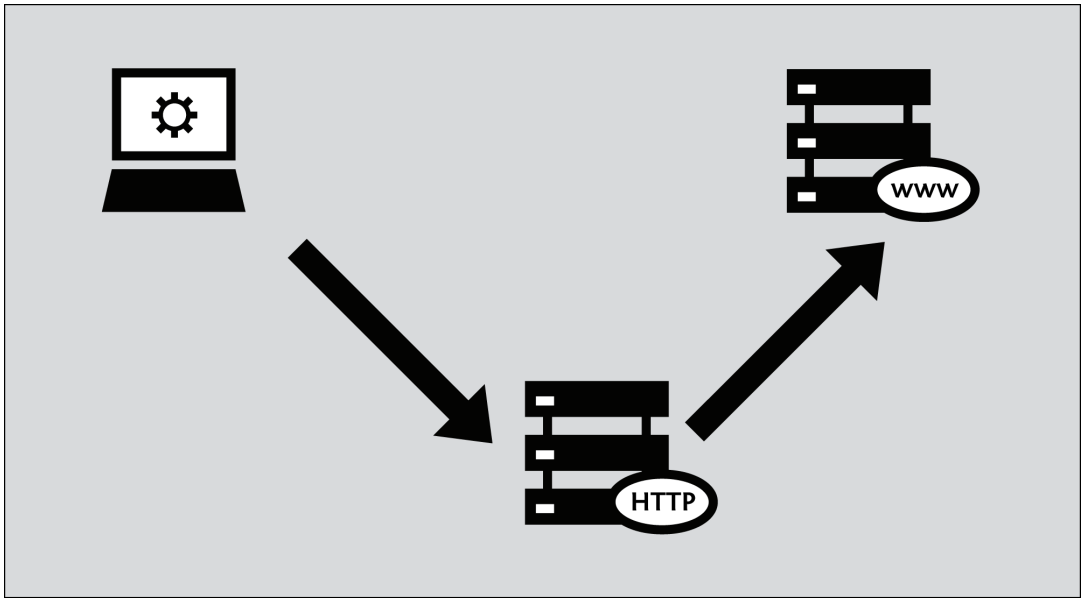
许多网站提供公共的应用代理列表。这类网站的综合列表可查看以下链接：http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists。
请注意，许多公共应用代理仅存在几个小时，所以代理列表能够及时更新是很重要的。

HTTP 代理设置

为了使用应用代理，用户必须对用户所用的操作系统或在单独的应用程序中，对代理的配置选项进行相应的设置。用户在应用程序的代理配置中选择代理之后，这个应用程序的所有互联网连接都将使用选中的代理。
请确保已对初始设置进行备份，以便恢复。如果由于某些原因代理不可用或无法访问，使用它的软件通常会停止运行。对于这种情况，用户需要进行重置，恢复为初始设置。

对于 Mac OS X 和某些 Linux 系统，可在操作系统中进行代理设置，并自动应用于应用程序如网页浏览器或即时通讯程序。对于 Windows 和某些 Linux 系统，没有控制程序可以进行代理设置，并且必须对每个应用程序进行单独配置。请注意，即使对代理进行中心设置，并不保证应用程序支持这些设置，因此，最好对每个应用程序进行单独检查。

通常只有网页浏览器可以直接使用 HTTP 代理。



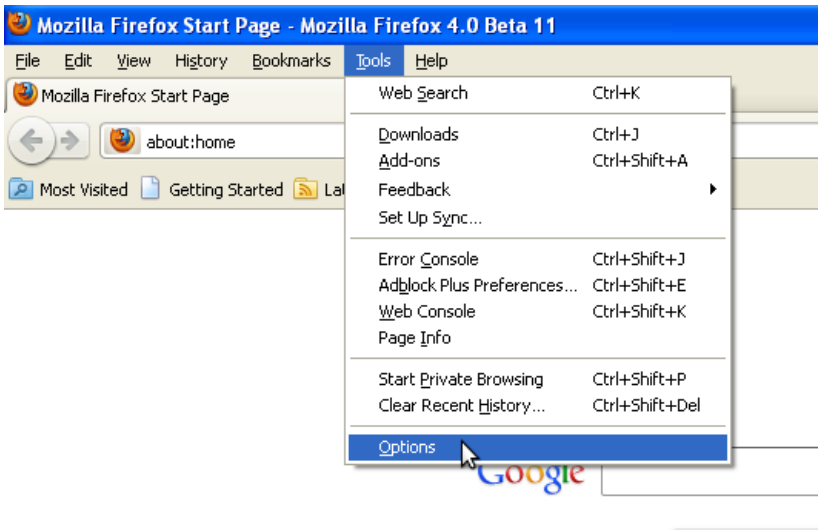
以下步骤描述了在Microsoft IE、Mozilla Firefox、Google Chrome和免费开源即时通讯客户端 Pidgin 中如何设置，以便使用代理。如果用户使用Firefox进行网页浏览，使用FoxyProxy软件更为简单；使用它可以省去以下描述的步骤。如果用户使用 Tor 工具，那么使用 TorButton 软件（Tor Bundle 下载包中的一部分）对使用 Tor 的浏览器进行设置是最安全的方式。

虽然电子邮件客户端，如Microsoft Outlook和Mozilla Thunderbird也可以设置为使用HTTP代理，收发邮件时，实际的邮件通信使用其他协议如POP3、IMAP和SMTP；并且这些数据流将不会通过HTTP代理。

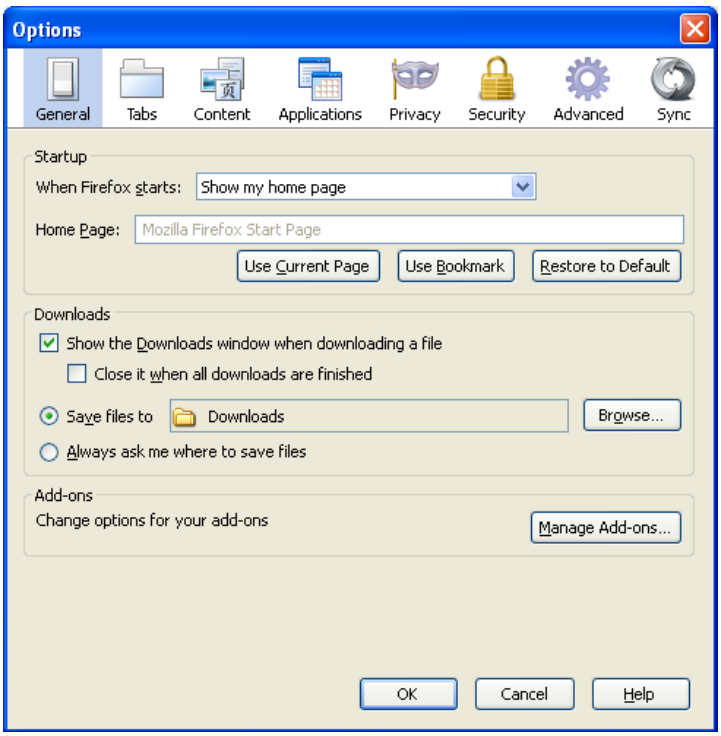
Mozilla Firefox

对 Firefox 使用 HTTP 代理进行设置：

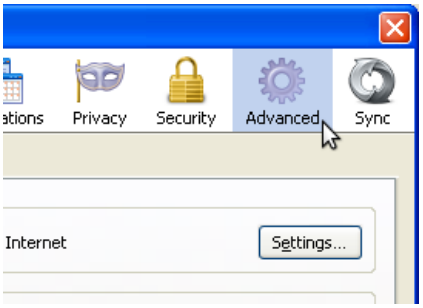
1. 在“工具”菜单中，单击“选项”：



2. 选项窗口出现：

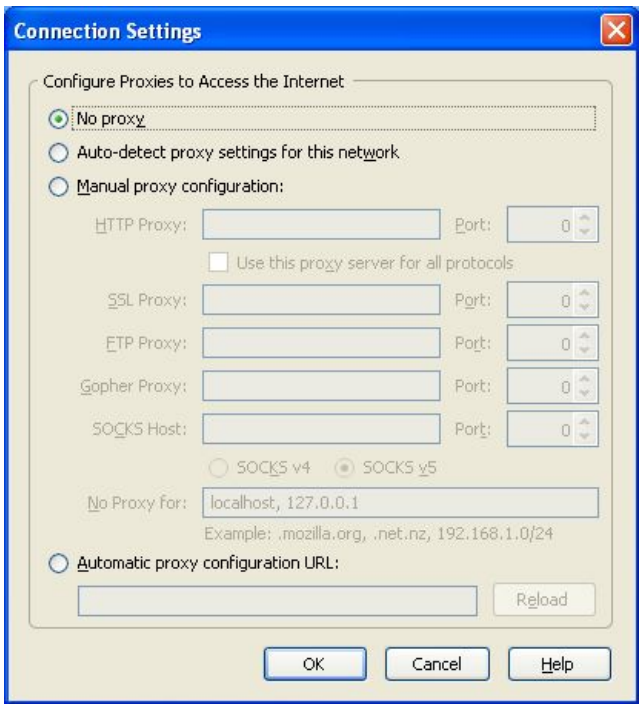


3. . 在窗口顶部工具栏中，单击“高级”：



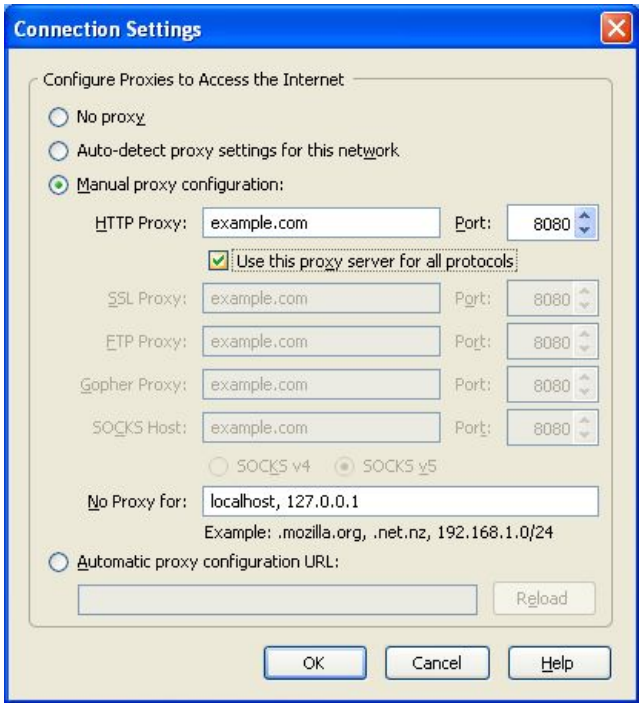
4. 单击“网络”标签：

5. 单击“设置”。Firefox 将显示“连接设置”窗口：



6. 选择“手动配置代理”。该选项下的字段将激活。

7. 输入“HTTP 代理”地址和“端口”编号，然后点击“确定”。



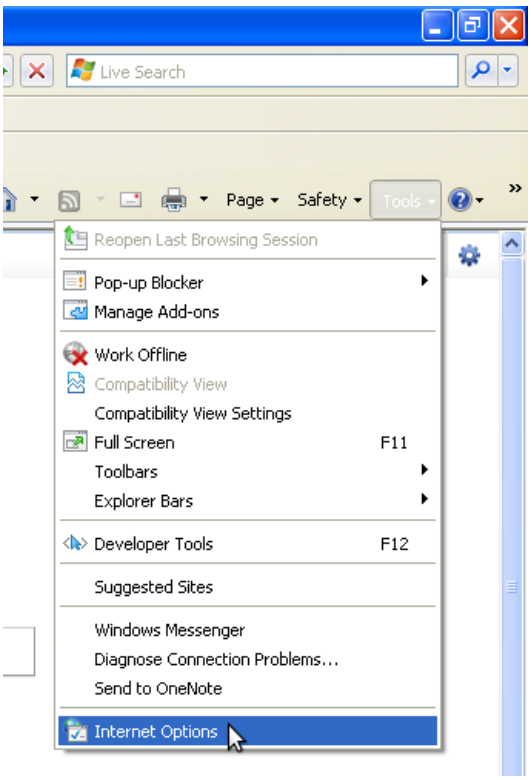
如果用户选中“为所有协议使用该服务器代理”，Firefox将通过代理发送HTTPS（加密式 HTTP）和FTP通信。如果用户使用的是公共应用代理，该选项可能不起作用，因为很多公共代理不支持HTTPS和FTP通信。但另一方面，如果用户的HTTPS和/或FTP通行被封锁，用户可以使用支持HTTPS和/或FTP的公共应用代理，并在Firefox中选中“为所有协议使用该服务器代理”。

现在，Firefox已经设置为可以使用HTTP代理了。

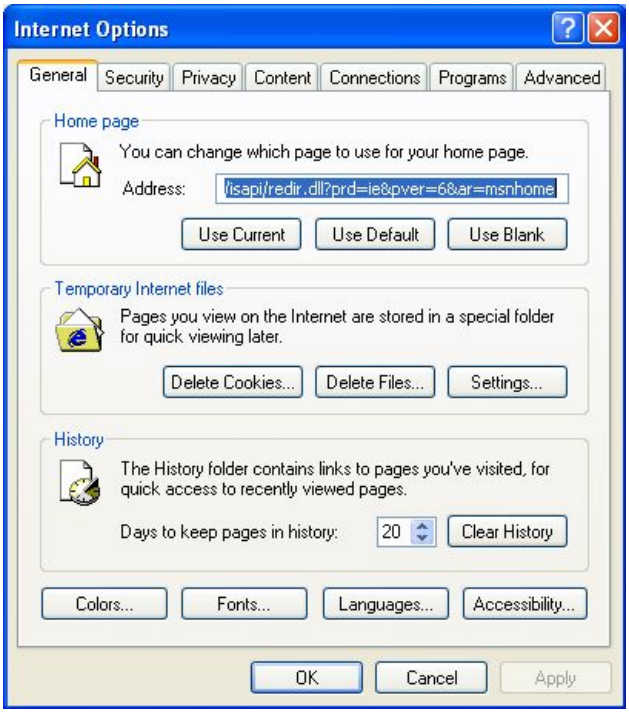
Microsoft IE 浏览器

对IE浏览器使用HTTP代理进行设置：

1. 在“工具”菜单中，单击“互联网选项”：

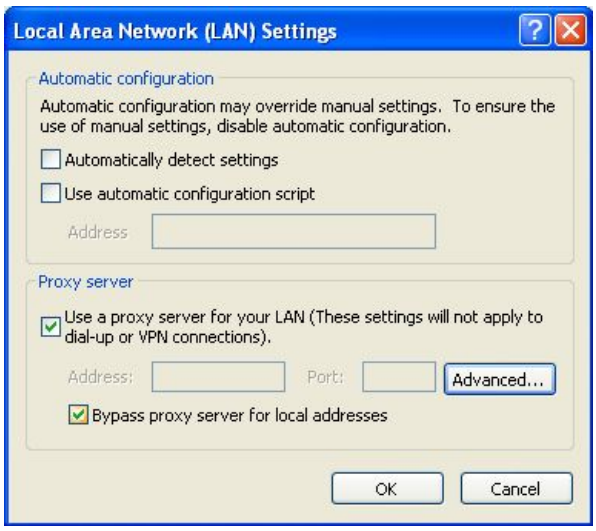


2. IE 浏览器显示“Internet 选项”窗口：

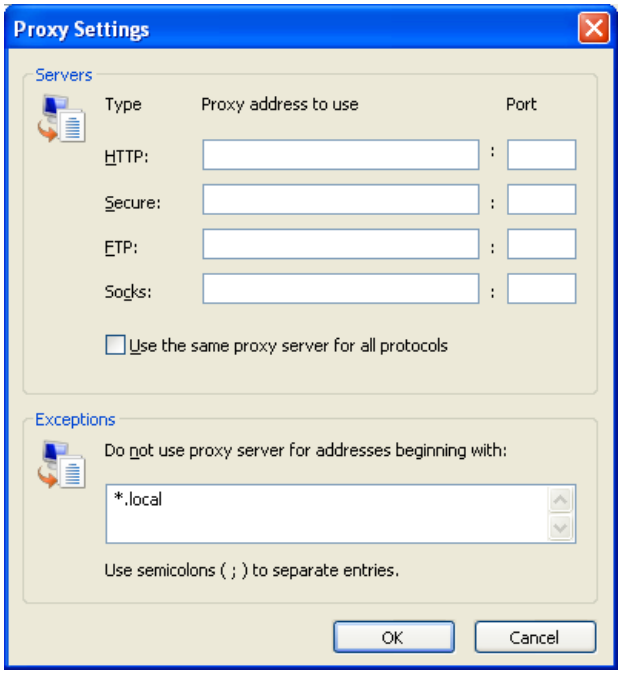


3. 单击“连接”标签：

4. 单击“局域网设置”。弹出的“局域网（LAN）设置”窗口如下图所示：

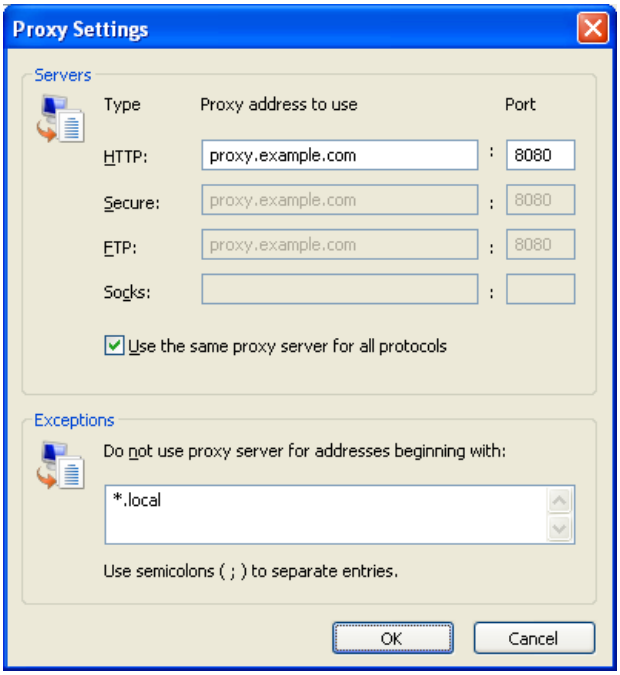


5. 选中“为LAN使用代理服务器”。
6. 单击“高级”。弹出的“代理服务器设置”窗口如下图所示：



7. 在第一行文本框中输入“代理服务器地址”和“端口”编号。

8. 如果用户选中“为所有协议使用相同服务器代理”，Internet Explorer将通过代理发送HTTPS（加密式 HTTP）和FTP通信。如果用户使用的是公共应用代理，该选项可能不起作用，因为很多公共代理不支持HTTPS和FTP通信。但另一方面，如果用户的HTTPS和/或FTP通行被封锁，用户可以使用支持HTTPS和/或FTP的公共应用代理，并在Internet Explorer中选中“为所有协议使用该服务器代理”。



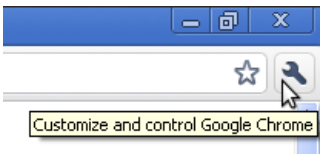
现在，IE 浏览器已经设置为可以使用 HTTP 代理了。

Google Chrome

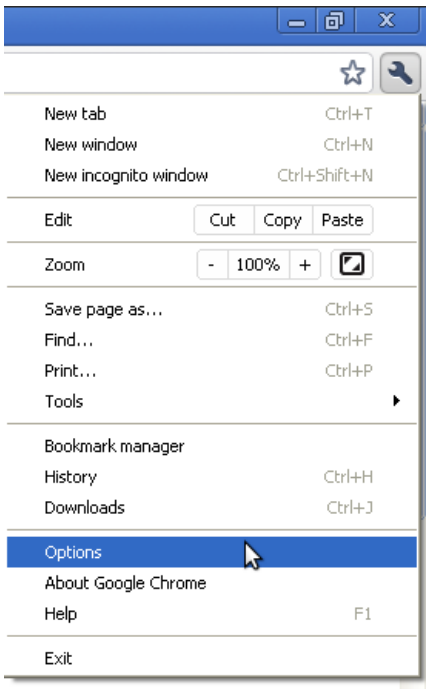
Google Chrome和Windows操作系统使用相同的连接和代理设置。改变这些设置影响Google Chrome、 Internet Explorer和其他Windows程序。如果你通过Internet Explorer配置HTTP代理，那么你接着不需要采取以下步骤配置Chrome。

遵照以下步骤配置你的HTTP代理：

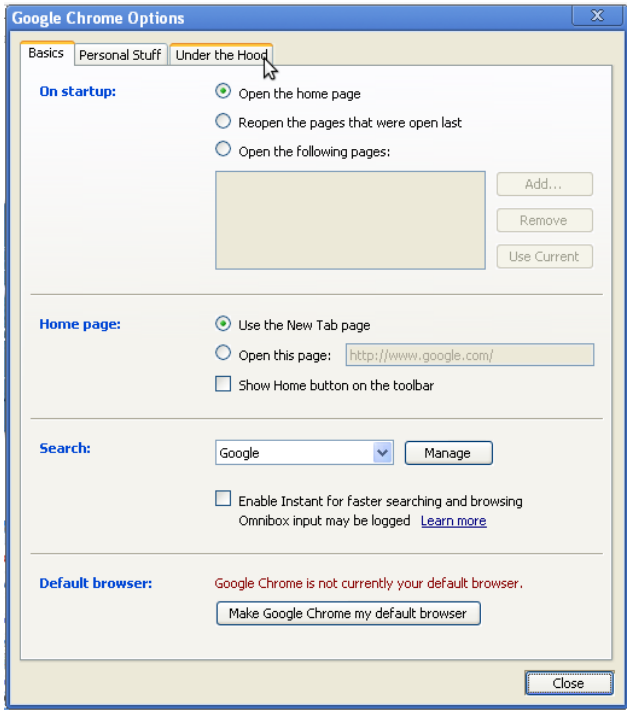
1. 点击“定制和控制Google Chrome”目录（URL地址栏旁边的小扳手）：



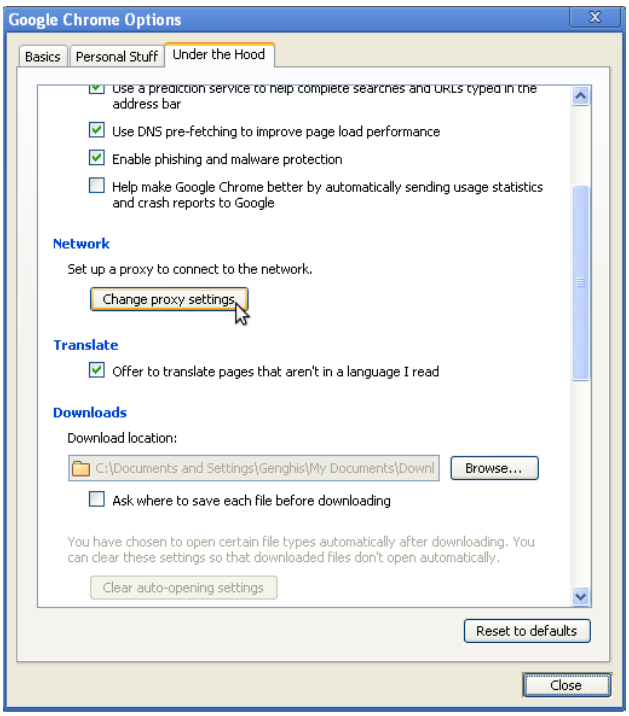
2. 点击“选项”：



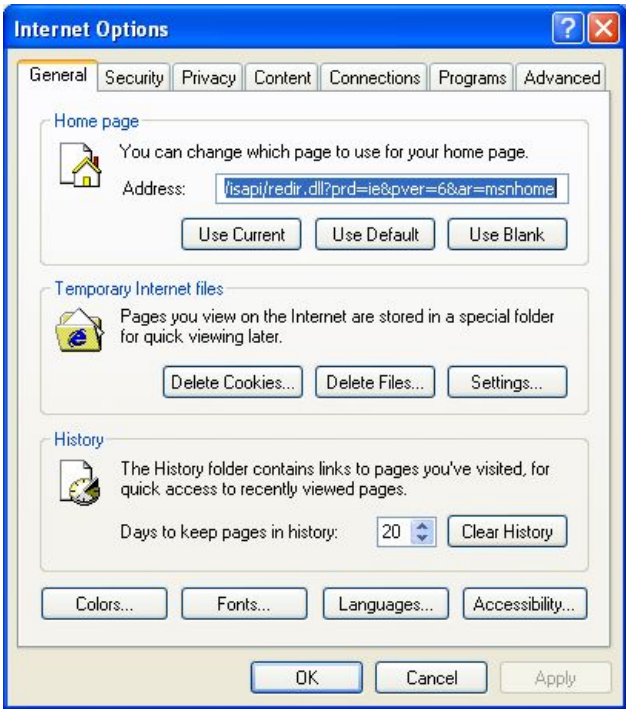
3. 在Google Chrome选项窗口中，选择高级选项标签：



4. 在网络部分点击“改变代理设置”按钮：



5. 互联网选项窗口将打开，根据（以上）“如何在Internet Explorer下配置HTTP代理”中的第2-8步完成HTTP代理设置。



现在，Chrome已经设置为可以使用 HTTP 代理了。

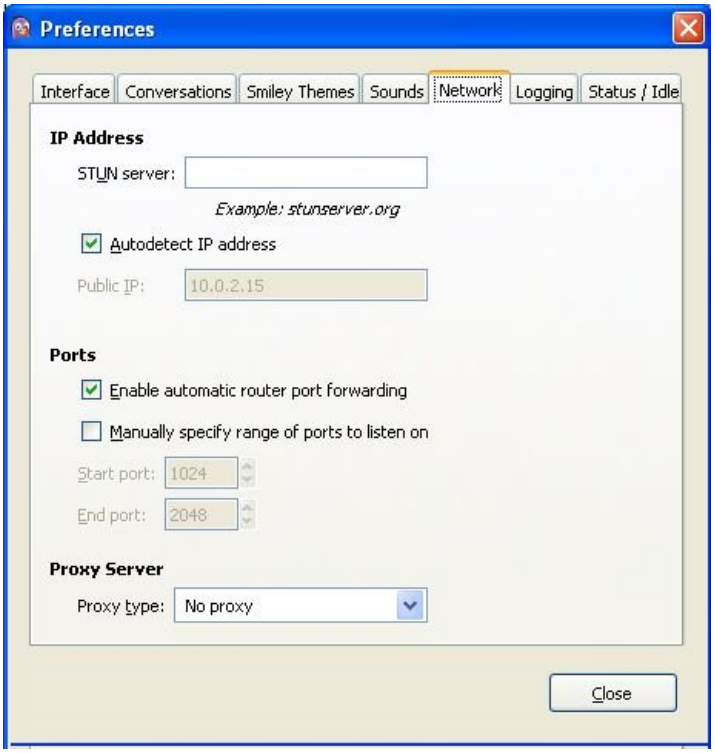
Pidgin 即时通讯客户端

网页浏览器之外的某些互联网应用程序也可以使用HTTP代理进行互联网连接，从而可以绕开封锁。下面以即时通讯软件Pidgin为例，对使用HTTP代理进行配置。

1. 在“工具（Tools）”菜单上，单击“预置（Preferences）”：

2. 单击“网络（Network）”标签，弹出如下图所示窗口：

3. 单击“网络（Network）”标签，弹出如下图所示窗口：



4. 在代理类型（Proxy type）下拉列表中选择“HTTP”。在该选项下方将显示相关的输入框。

5. 输入 HTTP 代理的“主机”地址和“端口”编号。

6. 单击“关闭”。

现在，Pidgin已经设置为可以使用HTTP代理了。

使用代理之后

在使用代理之后，尤其对于公用计算机，用户应将各项设置恢复为初始值。否则，这些应用程序将继续使用代理。如果用户不想其他人知道自己使用了代理或者所用的由特定绕行程序提供的本地代理并不是一直都在运行，不恢复初始值可能会造成一些问题。

命令行

在继续本书剩下的部分之前，了解命令行是这样工作的是有用的。如果你不熟悉命令行，下面的内容用来帮助你迅速获得基本知识。

基础

虽然电脑上的互动发生得如此之快以至于你来不及想，每一次点击或者击键是一次给电脑的命令，它对此作出反应。使用命令行是同样的事，但它更deliberate 。你输入一个命令，按Return或Enter键。例如，在我的终端，我输入：

```
date
```

电脑回复：

```
Fri Feb 25 14:28:09 CET 2011
```

这个很电脑化。在以后的章节里我们将说明如何用一种更合适的格式请求日期和时间。我们也将说明在不同的国家工作和用不同的语言是如何改变输出的。现在的想法是你已有了一次互动。

命令行可以做得更好

日期（*date*）命令， 就现在所见而言, 没有看一下日历或者时钟好。主要问题并不是让人反胃的输出的外观，我们已提及，而是不能使用输入做有价值的所有事。例如，如果我正在找日期，为了将它插入一个我正在写的文档或在我的网络日程表上更新一个活动，我不得不重新输入。命令行可以比这个做得更好。

如果你知道基本的命令和一些节省时间的有用方法，你将在这本书找到更到关于将命令的输出输送到其他命令，自动操作活动，和保存命令供以后使用的方法。

我们所将的命令指什么？

在本章的开头我们大量使用命令一词，指的是告诉电脑做什么的任何方法。但是在这本书的语境里，命令有非常特定的含义。它是你电脑上的文件，可以被执行，或者在某些情况下是整合到shell程序的活动。除了内置的命令之外，电脑通过找到有其名字的文件和执行这个文件运行每个命令。当它们变得有用时，我们将告诉你更多的细节。

输入命令的方法

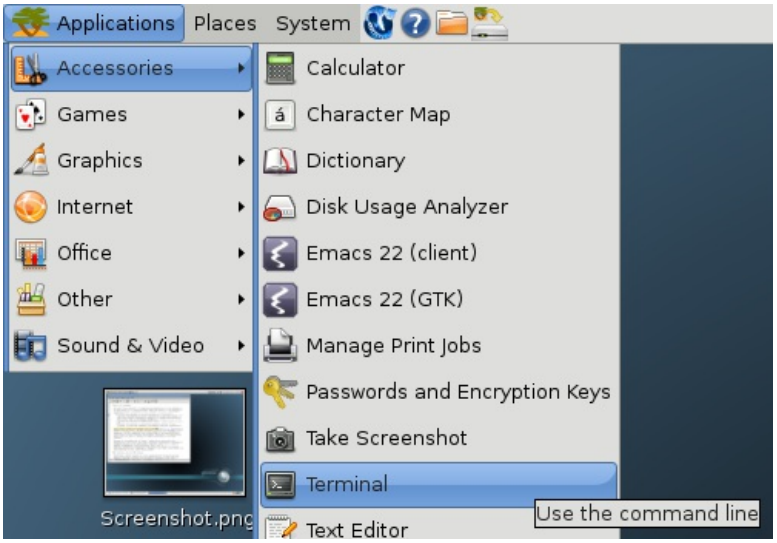
为跟上这本书，你需要在你的电脑打开一个命令行解释器（command-line interpreter）或者命令行界面（**command-line interface**）(在GNU/Linux叫**shell**或者终端（terminal）。只要一登录，非图形电脑屏幕就呈现它的解释器。现在几乎所有的人除了专业的系统管理员外都使用图形界面，尽管对许多种用途的使用来说非图形界面仍然更容易和快捷。所以我们将告诉你如何来做。

找到终端

你可以从桌面打开终端的界面，但使用最初的纯文本终端可能更容易。要做到这一点，使用< ctrl + alt + F1 >组合键。你打开一个几乎空白的屏幕邀请你登录。输入你的名字和密码。你可以使用其他的终端使用< alt + F2 >组合键，如此等等，不管你想完成什么任务，创建会话使用不同（或者相同）的用户。在任何时候，可以使用< alt + F# >击键从一个切换到你想要的另一个。其中，可能是F7或者F8，将让你回到桌面。在文本终端，你可以使用的鼠标（如果你的系统Gpm (通用鼠标守护进程)正在运行）选择一个命令、命令行和多行命令。你然后可以粘贴文本到在这个终端或其他终端的别的地方。

GNU/Linux发行版包含不同的图形用户界面提供不同的美感和语义隐喻。那些运行在操作系统上的被称为桌面环境（*desktop environments*）。GNOME、KDE 和Xfce使用最广泛。事实上，每一个桌面环境（*desktop environments*）提供一个模仿旧的过去常常用来作界面的纯文本终端的程序。在你的桌面上，试着在应用程序菜单找到一个叫做终端（Terminal）的程序。通常它在被叫做附件（Accessories）等的菜单上，它并不是很恰当，因为一旦你阅读这本书，你每天将花费大量的时间在终端上。

在GNOME上选择应用程序（Applications ）> 附件（Accessories）> 终端（Terminal）。



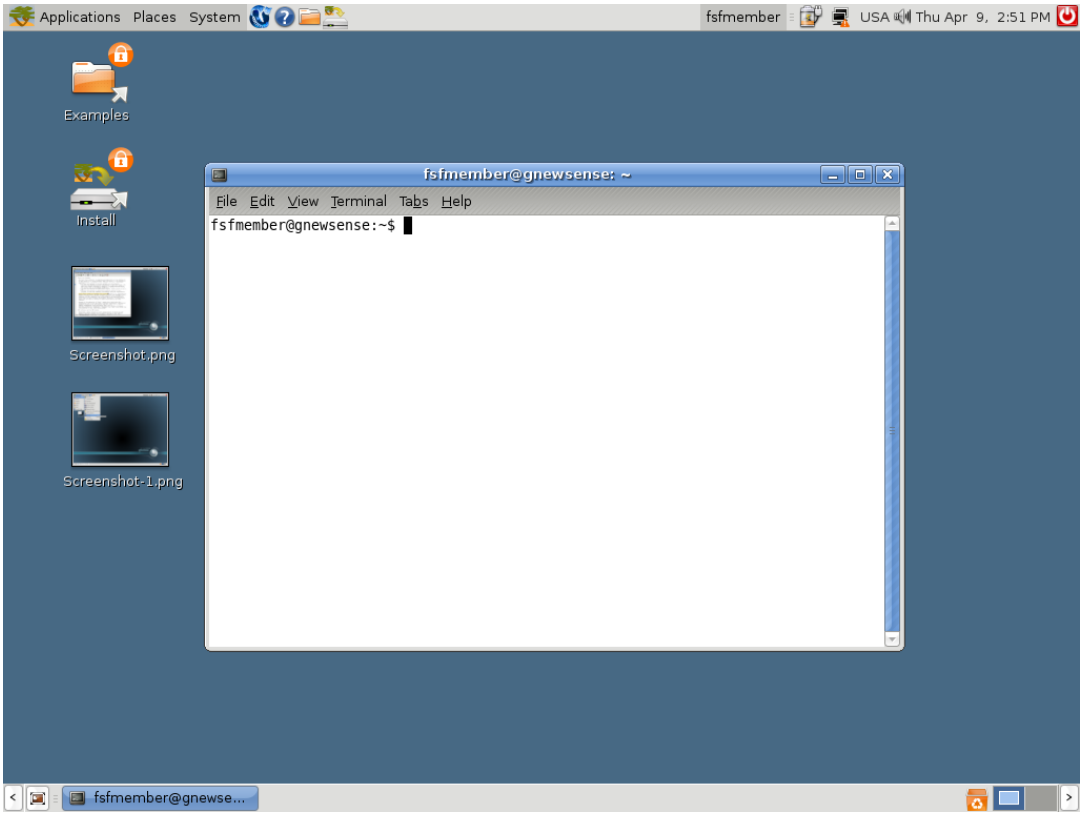
在KDE上,选择 K Menu -> System -> Terminal。

在Xfce上, 选择 Xfce Menu -> System -> Terminal。

不管它在哪个位置，你几乎必定能找到终端程序。

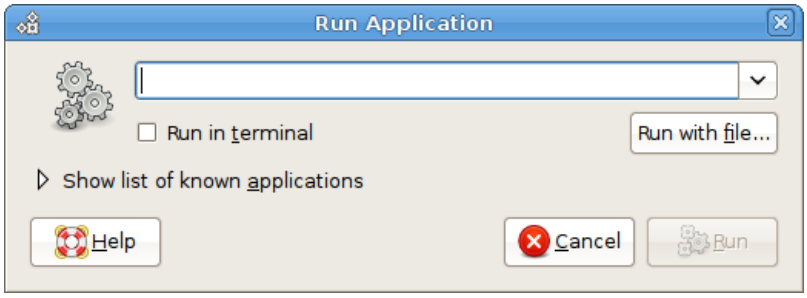
当你运行终端程序，只会打开一个空白窗口；找不到多少帮助。你应该知道怎么做，我们将教你。

下图显示在GNOME桌面打开的终端（Terminal）窗口。



运行单个命令

许多图形界面也提供小的对话窗口，被叫做“运行命令”（"Run command"）等。 它显示一个小的文本框，你可以在那输入命令，按回车键（Return or Enter key）。



可以按< alt + F2 >组合键，或通过应用程序菜单搜索，调用这个对话窗口。你可以使用这个窗口作为快速启动终端程序的捷径，只要你知道安装在你电脑上的终端程序的名字。如果你使用一台不熟悉的电脑，不知道默认的终端程序的名字，输入`xterm`启动一个基本的终端程序（没有允许选择颜色主题或字体的花哨的菜单）。如果你极度地需要这些花哨的菜单，

- 在GNOME默认的终端程序应该是`gnome-terminal`
- 在KDE应该是 `konsole`
- 在 Xfce试下 `Terminal` 或特定版本的终端名字，如Xfce 4，你应该找 `xfce4-terminal`。

开放虚拟专用网络（OpenVPN)

开放虚拟专用网络（OpenVPN）是一种广受好评的免费开源虚拟专用网络（VPN）解决方案。该软件支持大部分Windows(即将支持 Windows Vista)操作系统，Mac OS X以及Linux系统。OpenVPN是一款基于SSL的软件，也就是说，它使用的加密技术跟访问以https开头的安全网站所使用的技术是一样的。

一般信息

Supported operating system	
Localization	English, German, Italian, French and Spanish
Web site	https://openvpn.net/index.php/open-source.html
Support	Forum: https://forums.openvpn.net

OpenVPN不适合在网吧，或其它共享计算机上临时使用，因为你无法安装其它软件。

更加详细了解VPN和随时可用的VPN服务，阅读本指南中的“VPN服务”这一章。

一个OpenVPN系统包含一台充当服务器（在未屏蔽地区）的计算机，以及一个或多个客户端。该服务器必须可以通过网络访问 ，不能被防火墙屏蔽，并且要有一个可以公开路由的IP地址 （在某些地方，搭建服务器的用户必须向其网络服务提供商发出申请 ）。每个客户端连接到服务器，并且创建一个VPN“隧道”，这样客户端网络流量就可以通过。

商业OpenVPN提供商有很多，比如WiTopia (http://witopia.net /personalmore.html)，每月支付5-10美元的费用，你就可以访问他们的OpenVPN服务器。这些提供商还会帮助你在计算机上安装设置OpenVPN。从这里可以找到类似的商业OpenVPN提供商列表：http://en.cship.org/wiki/VPN。

OpenVPN可以被一个在未过滤地区的可信任的联系人用来，向一个或多个客户端提供OpenVPN服务器，把客户网络流量转移到自己的计算机上，然后再转移到网上。但是正确安装OpenVPN有点复杂。

安装 OpenVPN 的建议

你可以按照OpenVPN提供的文档安装自己的OpenVPN服务器和客户端。如果你想通过OpenVPN访问被屏蔽网站，以下事项对你非常重要：

客户端

Windows用户可以使用一个图形用户界面（GUI），根据需要启动和停止OpenVPN ，并且你可以通过配置OpenVPN使用HTTP代理上网。GUI下载地址：http://openvpn.se。

如果你在Linux或Mac OS X下通过设置OpenVPN使用代理服务器，可以阅读以下相关内容：(http://openvpn.net/index.php/documentation/howto.html#http).

服务器

- 在选择采用路由（routing）还是桥接（bridging）时，如果你的客户端只想通过服务器绕开网络审查，配置桥接没有什么额外好处，选择路由就行。
- 指南中有些地方介绍了如何确保所有客户端流量都经过服务器，需要特别注意。没有该配置，系统无法帮助你访问被屏蔽网页。(http://openvpn.net/index.php/documentation/howto.html#redirect)
- 如果客户端计算机位于非常强大的防火墙之后，并且默认OpenVPN端口已经被屏蔽，你可能需要改变OpenVPN端口。选择之一就是使用 443端口，该端口通常用于访问安全网站（HTTPS），并且用用户数据电文协议（UDP）取代传输控制协议（TCP）。经过这样的设置，防火墙就很难区 分OpenVPN流量和普通安全网络流量了。为此，在客户端和服务器配置文件的靠近上方处，把“proto udp”换成“proto tcp”，把“1194端口”换成“443端口”。

优势与风险

一经正确安装和配置，OpenVPN可以非常有效地绕开网络过滤器。由于所有流量都已经在客户端和服务器之间进行加密，并且从单一端口通过，很难将其与其它安全网站的流量区分开来，比如访问在线购物网站或其它加密服务的网络流量。
OpenVPN可用于所有网站流量，其中包括网页流量，电子邮件，即时通讯，以及IP语音电话流量。只要你信得过OpenVPN服务器提供者，并且根据OpenVPN文档说明正确安装相关证书和密钥，OpenVPN还可以提供一定程度的反监视保护。记住，流量只是在OpenVPN服务器这里经过加密，在此之后，流量就会在未经加密的情况下传输到网上了。

OpenVPN主要的缺点就是安装和配置比较复杂，并且需要访问未屏蔽地区的服务器。此外，OpenVPN无法提供可靠的匿名代理服务。

SSH隧道加密技术

SSH，即安全外壳（Secure Shell），是一种标准协议，可对你的计算机和服务器之间的通信内容进行加密。该加密技术可以防止通信内容被网络运营商查看或修改。SSH可广泛应用于安全通信应用，最常见的就是安全登录服务器，以及安全文件转移（安全复制协议，SCP或安全文件传输协议，SFTP）。

SSH尤其适用于绕开网络审查，因为它可以提供加密隧道，充当一个通用代理客户端。审查者不能完全屏蔽SSH，因为它不仅仅用来绕开网络审查；比如系统管理员也会使用SSH通过网络管理服务器。

使用SSH时需要一个服务器上的账户，通常使用Unix或Linux服务器。为了绕开审查，该服务器需要能自由访问网络，并且提供者最好是信得过的人。有些公司也销售服务器账户，并且很多网络虚拟主机服务可以提供SSH访问。你可以在这里找到一个外壳账户提供商名单：http://www.google.com/Top/Computers/Internet/Access_Providers/Unix_Shell_Providers/，每个账户每月收费2-10美元。

大部分Unix，Linux，和Mac OS计算机上已经预装了一个叫做OpenSSH的SSH程序，作为一个命令行程序，从终端计算机上输入“ssh”就可以运行。Windows用户也可以使用一个叫做PuTTY的免费SSH工具。

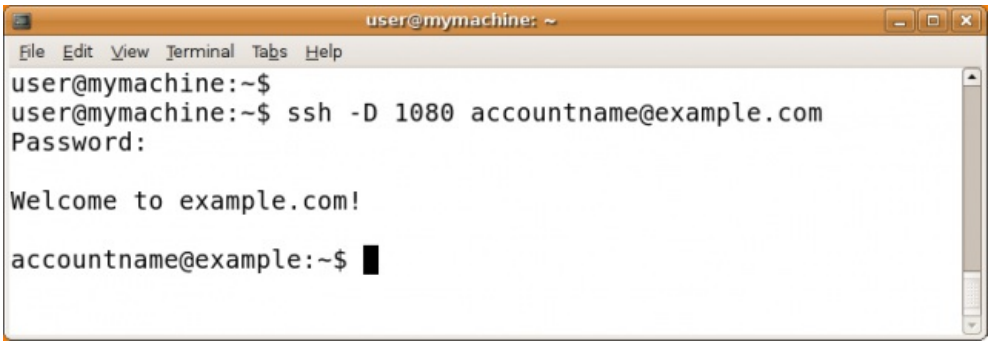
所有新版SSH都支持创建防火墙安全会话转换协议（SOCKS）代理，允许网页浏览器和很多其它软件通过加密SSH链接使用未经屏蔽的网络。在本例中，我们仅讨论SSH的这种应用。下列步骤将在计算机的本地1080端口上设置一个SOCKS代理。

Linux/Unix 以及 MacOS 命令行 (以 OpenSSH 为例)

你可以从http://www.openssh.com/得到OpenSSH，但一般Linux/Unix和Mac OS计算机上会预装该程序。
你将运行的ssh命令包括一个本地端口号（典型的是1080），一个服务器名称和一个用户名（帐户名）。如下所示：

```
ssh -D localportnumber accountname@servername
```

例如：

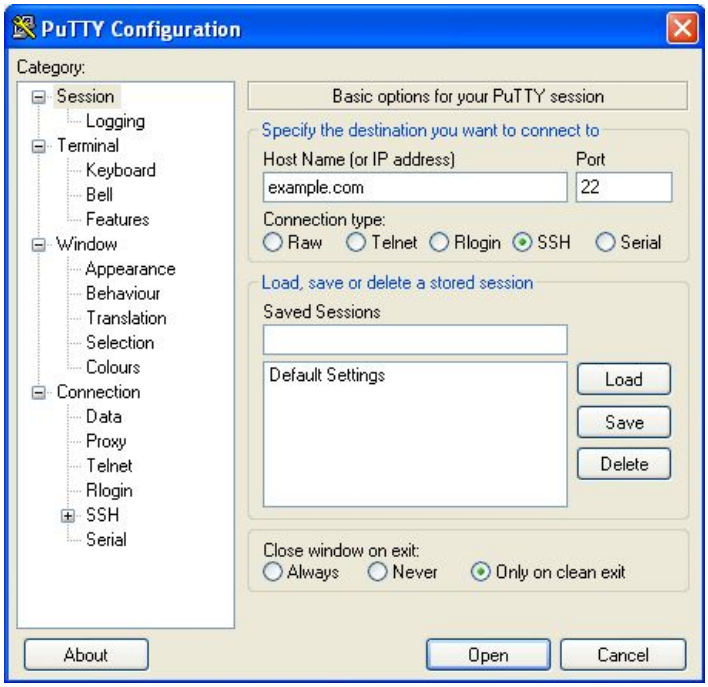


然后会提示你输入密码，接着你就可以登录到服务器。通过使用-D选项，你可以建立一个本地SOCKS代理，只要你的计算机连接在服务器上，该代理就不会消失。注意：现在你可以验证主机密钥并配置你的程序了，否则你将不能使用你创建的隧道！

Windows图形用户界面（以PuTTY为例）

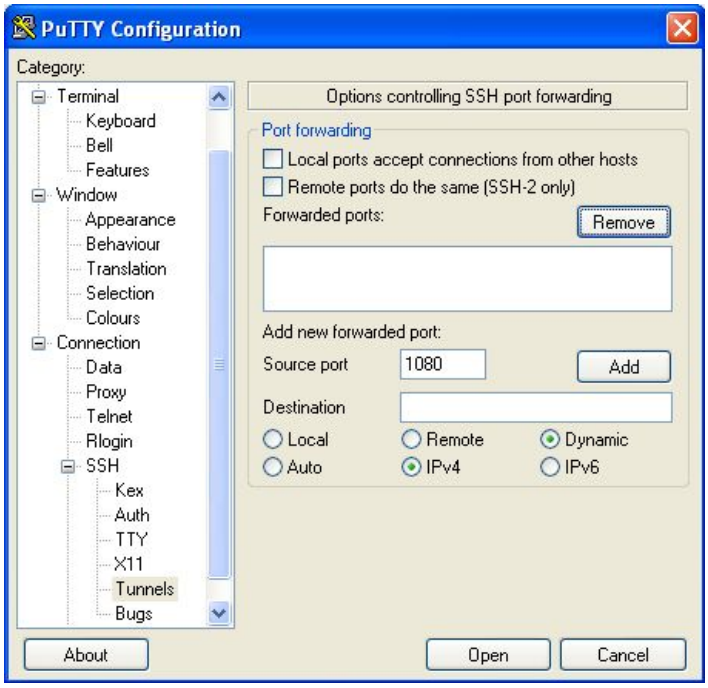
你可以从http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html下载到PuTTY。你可以把putty.exe程序保存到你的硬盘上，以备将来使用，或者你也可以直接从网站上运行该程序（通常，你可以在共用或公共的计算机上实现，比如图书馆或者网吧里的计算机）。

启动PuTTY后，你可以看到一个配置对话框。首先，你要输入打算连接的SSH服务器的主机名（地址）（这里比如example.com）。如果你只知道IP地址，或者DNS屏蔽让你无法使用主机名，你可以用IP地址代替。如果你需要经常进行此操作，你可以创建一个PuTTY档案，这样就可以保存这些选项及后续选项以便将来使用。



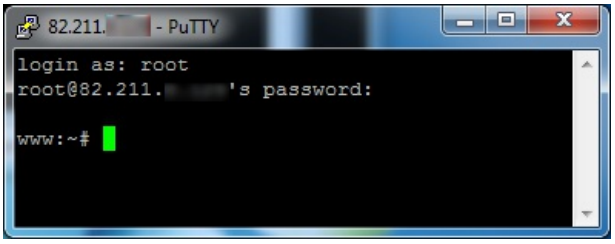
接下来，在目录（Category）列表选择连接（Connection）--> SSH，然后选择隧道（Tunnels）。

在源端口（Source port）后输入1080，然后选中“动态（Dynamic）”和“Ipv4”选项框。



现在点击添加（Add）按钮，接着点击“打开（Open）“按钮。之后会建立一个到服务器的连接，然后会弹出一个窗口，提示你输入用户名（username）和密码（password）。

输入这些信息后你就可以登录到服务器，然后会收到一条来自服务器的命令行提示。这样就建立了SOCKS代理。注意：现在你可以验证主机密钥并配置你的程序了，否则你将不能使用你创建的隧道！



主机密钥验证

当你第一次连接到服务器时，会提示你确认该服务器的主机密钥指纹（host key fingerprint）。主机密钥指纹是一长串可以安全识别特定服务器的字母和数字（十六进制），比如：57:ff:c9:60:10:17:67:bc:5c:00:85:37:20:95:36:dd。检查主机密钥指纹是一项安全措施，可以确保你是在和你认为你连接的服务器进行通信，并且加密后的连接无法破解。

SSH并不提供自动验证方法。为了享用该安全机制带来的好处，你应该和服务器提供者一起核对主机密钥指纹，或者让一个信得过的人连接同一台服务器，看其是否可以看到同样的指纹。

如果你想确保让SSH保护你的通信内容不被窃听，验证主机密钥指纹就很有必要；但如果你只想绕开审查，而不在乎网络运营商时候可以看到你的通信内容，则没有必要验证指纹。

配置程序，使用代理

只要你不关闭SSH程序，通过以上步骤建立的代理会一直有效。但如果你的网络连接被中断了，你需要重复上面的步骤，重新激活代理。

启动并运行代理之后，你需要设置软件以使用代理。通过以上步骤，你得到的是一个位于本地主机（localhost）的SOCKS代理，端口为1080（也即127.0.0.1，端口1080）。你应该确保软件设置可以阻止**DNS**泄漏，否则SSH的隐私保护和审查绕行效果可能会受到影响。

更多选项

到目前为止，所有这些命令都显示在远程计算机上，接着你可以从该远程计算机执行其提供给你的任何命令。有时你可能想要在远程计算机上只执行一个命令，随后返回你的本地计算机上的命令行。这可以通过将要在远程计算机上执行的命令放在单引号中实现。

```
$ ssh remoteusername@othermachine.domain.org 'mkdir /home/myname/newdir'
```

有时，你需要在远程计算机上执行耗时命令，但你不能确保你当前的ssh会话有足够的时间。如果你在命令执行完成前关闭远程连接，那么该命令将被中止。为了防止你的任务丢失，你可以通过ssh启动一个远程窗口会话，然后断开它，并在你想的任何时候重连它。要断开一个远程窗口会话，只要关闭ssh连接即可：断开的窗口会话将仍运行于远程计算机上。

ssh提供了许多其他选项。你也可以设置你最喜爱的系统允许不用每次输入你的密码就可以登录或运行命令。该设置是复杂的，但可以节省你很多的输入工作；尝试对“ssh-keygen”、“ssh-add”和“authorized_keys”做一些网络搜索。

scp: file copying

SSH协议超出了基本ssh命令。一种基于SSH协议的特别有用的命令是scp，即安全复制命令。下面的例子从你本地计算机上的当前目录复制一个文件到远程计算机上的目录*/home/me/stuff*。

```
$ scp myprog.py me@othermachine.domain.org:/home/me/stuff
```

请注意，该命令将覆盖已存在于*name /home/me/stuff/myprog.py*的任何文件。（或者当已有该名称的文件且你无权重写它时，你将得到一个错误信息。）如果*/home/me*是你的主目录，那么目标目录可以被缩写。

```
$ scp myprog.py me@othermachine.domain.org:stuff
```

在另一个方向，你也可以如此简单地复制：从远程计算机到你的本地计算机。

```
$ scp me@othermachine.domain.org:docs/interview.txt yesterday-interview.txt
```

远程计算机上的文件是你主目录的docs子目录中的interview.txt。这个文件将被复制到你本地系统主目录中的yesterday-interview.txt。

scp可被用于从一个远程计算机向另一个远程计算机复制文件。

```
$ scp user1@host1:file1 user2@host2:otherdir
```

要循环复制一个目录中的所有文件和子目录，可以使用-r选项。

```
$ scp -r user1@host1:dir1 user2@host2:dir2
```

查看scp手册页以获得更多选项。

rsync: 自动批量传输和备份

rsync是一个非常有用的命令，其可以使远程目录和本地目录保持同步。我们在此提到它是因为其像ssh一样是进行网络活动的有用的命令行形式，同时也因为SSH协议被推荐为rsync的底层传输。以下是一个简单而有用的例子。其从你的本地/home/myname/docs目录向system quantum.example.edu上你的主目录中名为backup/的目录复制文件。实际上，rsync减少了通过各种复杂检查必须的复制量。

```
$ rsync -e ssh -a /home/myname/docs me@quantum.example.edu:backup/
```

指向ssh的-e选项使用被推荐的底层传输SSH协议。-a选项（代表“存档”）复制指定目录内的一切东西。如果你想在本地系统上的文件被复制后将其删除，那么要包含一个--删除选项。

经常使用SSH使你的生活更容易

如果你使用SSH连接到许多不同的服务器，你经常会出现误输用户名或者甚至是主机名的错误（试想要尝试记住20个不同的用户名/主机的组合）。值得庆幸的是，SSH提供了一种简单的方法来通过一个配置文件管理会话信息。

该配置文件隐藏在.ssh目录（完整路径可能类似/home/jsmith/.ssh/config-如果该文件不存在，你可以创建它）下你的主目录中。使用你最喜爱的编辑器打开这个文件，并像这样指定主机：

```
Host dev
HostName example.com
User fc
```

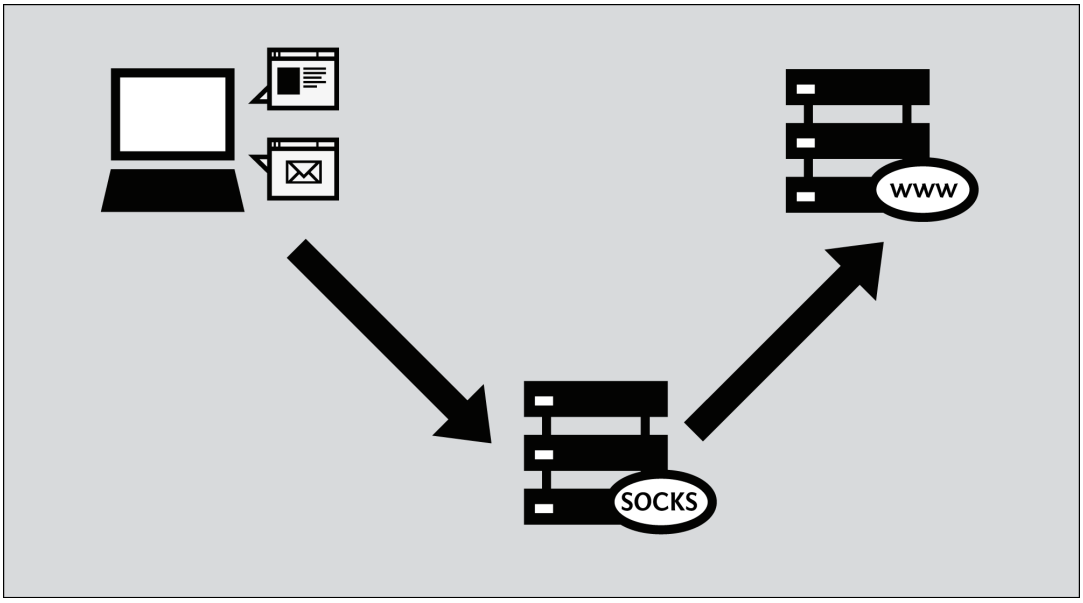
你可以像这样在你的配置文件里设置多个主机，在保存以后，通过运行以下命令连接到你成为“dev”的主机。

```
$ ssh dev
```

请记住，你经常使用这些命令越多，你节省的时间也就越多。

SOCKS 代理

SOCKS是一种互联网协议，它显示了一种特殊的代理服务器。 SOCKS代理的默认端口是1080，但它们也可能在其他端口上。与普通的HTTP代理的实际区别是，SOCKS代理不仅可以用来网络浏Web浏览，但也可为其他应用程序使用，如视频游戏、文件传输或即时通信客户端。和VPN类似，它们作为一个安全的隧道。
普通的SOCKS版本包括4，4A及5。第4版创建一个连接总是需要IP地址，所以DNS解析仍然在客户端上进行。这使得它不能满足很多绕行需要。4A版通常使用主机名。第5版包括身份验证、UDP和IPv6等新技术，但它通常使用IP地址，所以它也可能不是完美的解决方案。另见本章末尾的“DNS泄漏”部分。
各种软件可以利用SOCKS代理来绕过过滤器或其他限制，不仅仅是浏览器，还包括即时通信和电子邮件应用程序等其他互联网软件。



尽管确实存在公共SOCKS代理，但大部分SOCKS代理运行在你的本地计算机上，并且由软件程序提供。因为SOCKS隧道非常灵活，一些审查绕行软件可以在你的计算机上创建一个本地代理（通常可以通过账户名localhost或者IP地址127.0.0.1访问）。这个本地代理可以让网页浏览器等软件使用绕行软件。这类工具包括Tor，Your-Freedom，以及通过PuTTY安装的ssh隧道。

本地代理爱好者T恤（明白了？）

为了使用应用代理绕开审查，在和其它网络通信时，你必须让本地计算机上的软件知道你想使用代理。

有些网络软件通常不支持代理，因为软件开发者没有提供代理支持。但很多软件可以通过“SOCKS化（socksifier）”软件支持SOCKS代理，这些软件的一些例子包括：

- tsocks (http://tsocks.sourceforge.net/)支持Unix/Linux
- WideCap (http://www.widecap.com/)支持Windows
- ProxyCap (http://www.proxycap.com/)支持Windows

配置应用软件

在大多数情况下，通过设置软件使用SOCKS代理的方法和使用HTTP代理的方法差不多。软件如果支持SOCKS代理，在它的菜单或者选项对话框里设置HTTP代理的地方通常会有一个单独的部分让你设置SOCKS代理。有些软件会让你选择SOCKS 4或SOCKS 5代理设置，一般选择SOCKS 5更好，但有的SOCKS代理只支持SOCKS 4.

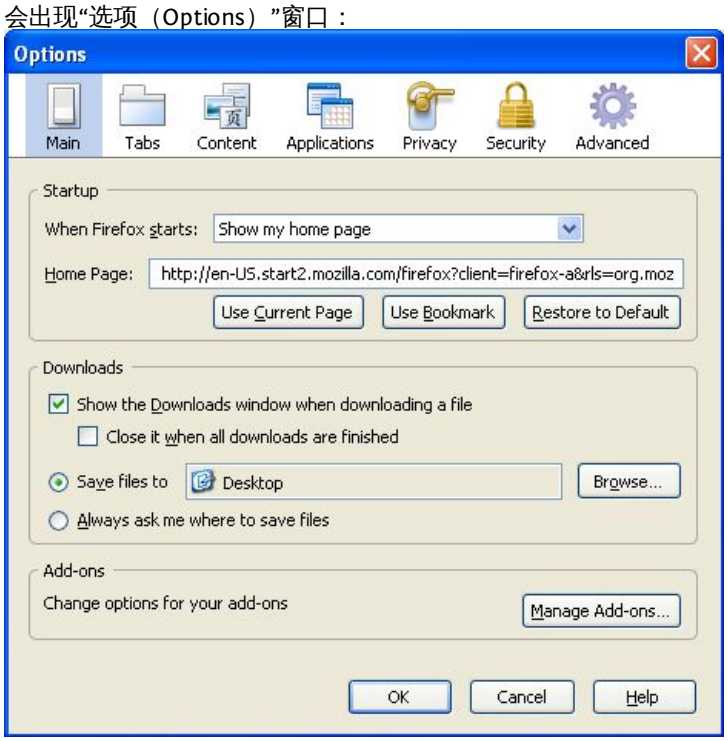
有些软件，如火狐（Firefox）允许用户同时设置HTTP和SOCKS代理。这种情况下，你就可以在正常网页浏览时使用HTTP代理，当访问视频播放等内容使用SOCKS代理。

Mozilla Firefox

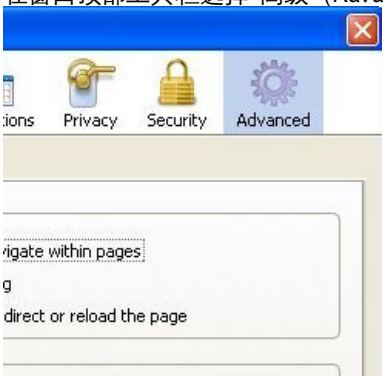
配置Mozilla Firefox使用SOCKS代理：

1. 选择“工具（Tools）”菜单，点击“选项（Options）”：

2. 会出现“选项（Options）”窗口：

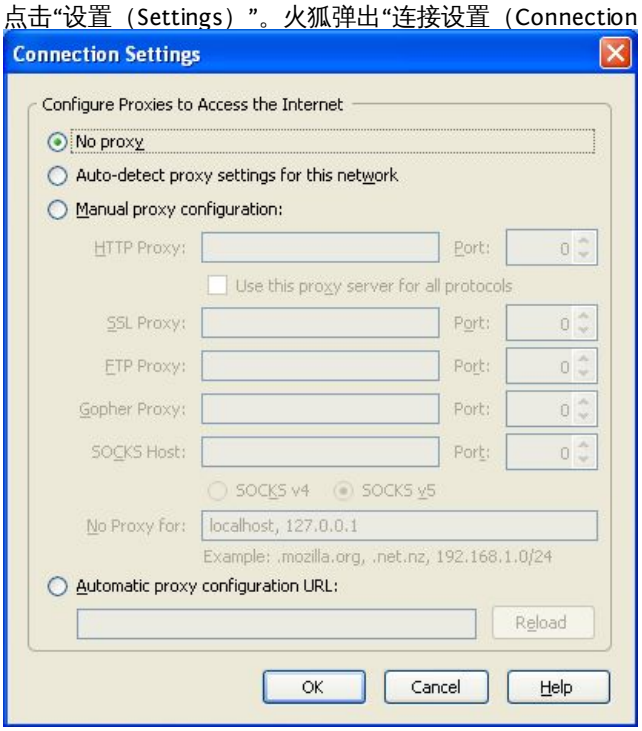


3. 在窗口顶部工具栏选择“高级（Advanced）”：

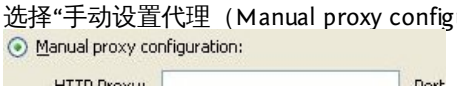


4. 点击“网络（Network）”选项卡：

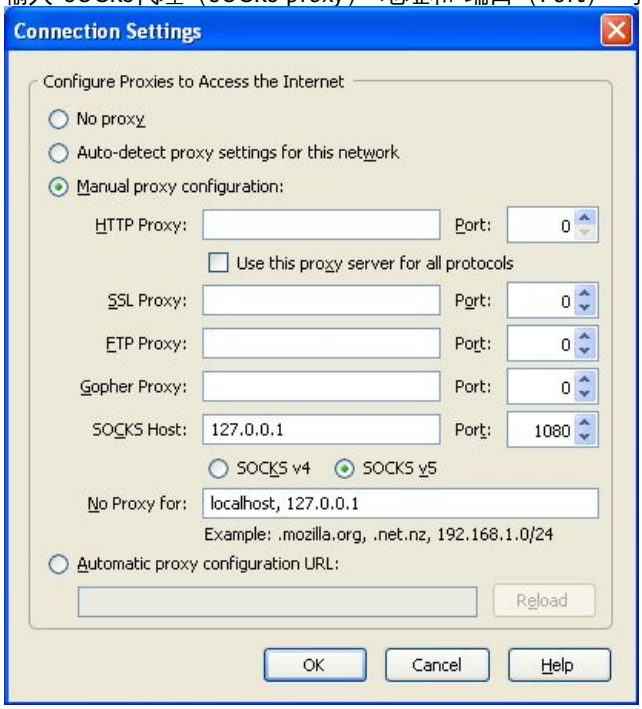
5. 点击“设置（Settings）”。火狐弹出“连接设置（Connection Settings）”窗口：



6. 选择“手动设置代理（Manual proxy configuration）”，然后其下的选项就可以更改了。



7. 输入“SOCKS代理（SOCKS proxy）”地址和“端口（Port）”号，选择“SOCKS v5”然后点击“OK”。



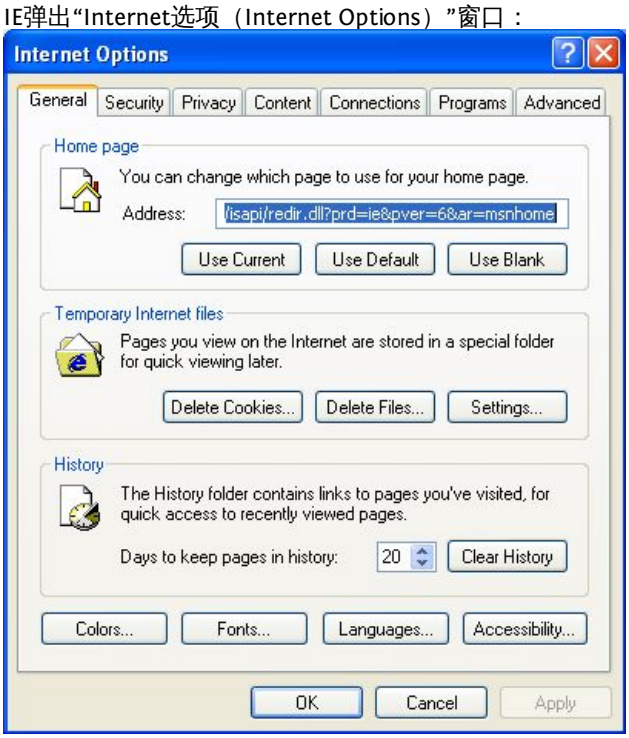
现在火狐就可以使用SOCKS代理了。

微软IE浏览器

通过以下步骤让IE浏览器使用SOCKS代理：

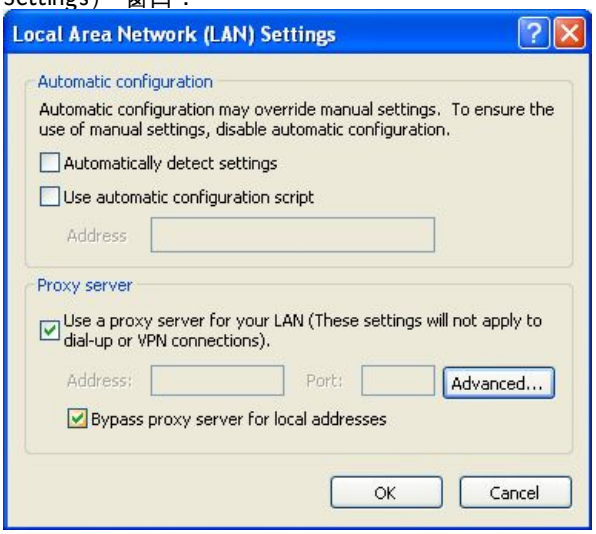
1. 在“工具（Tools）”菜单选择“Internet选项（Internet Options）”：

2. IE弹出“Internet选项（Internet Options）”窗口：

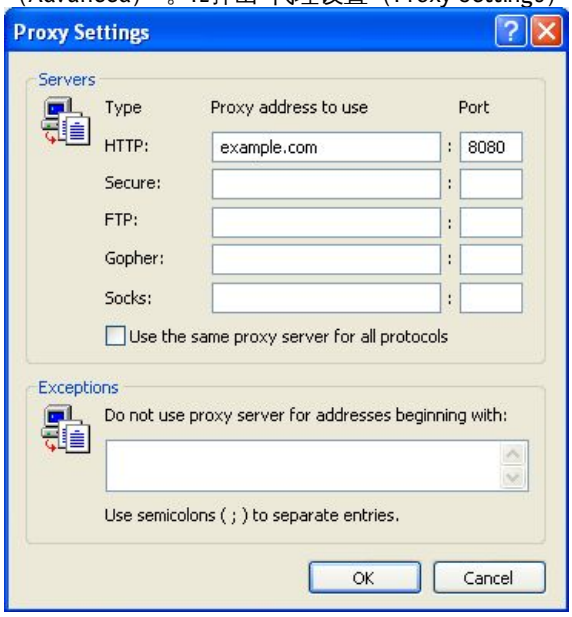


3. 单击“连接（Connections）”选项卡：

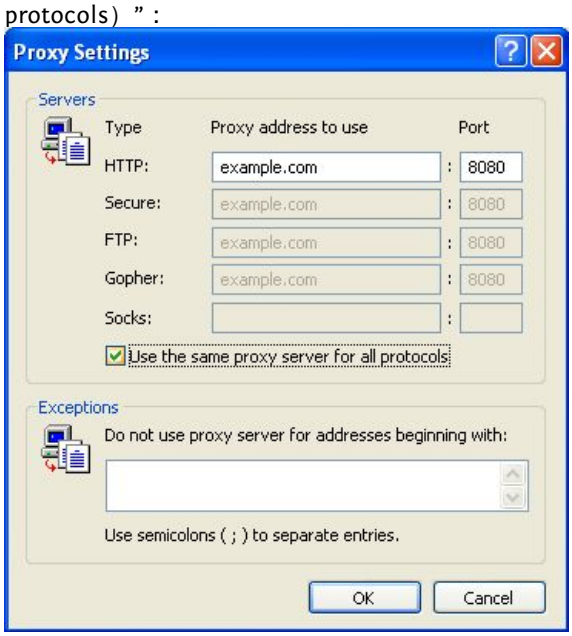
4. 单击“LAN设置（LAN Settings）”，IE会弹出“局域网设置（Local Area Network （LAN）Settings）”窗口：



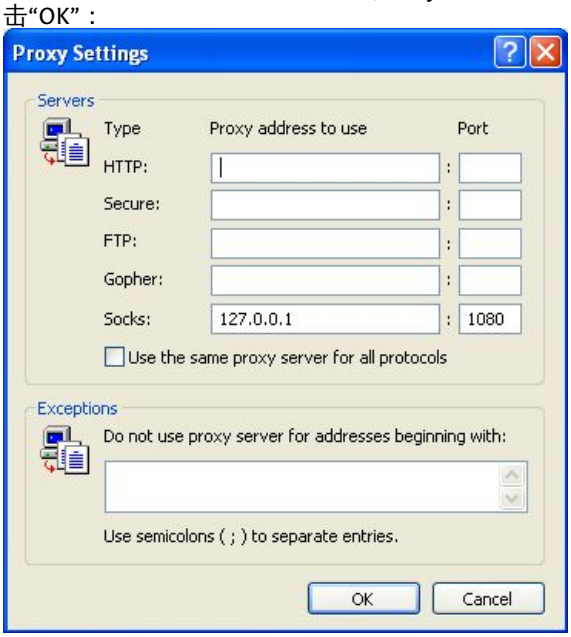
5. 选择“为LAN使用代理服务器（Use a proxy server for your LAN）”然后点击“高级（Advanced）”。IE弹出“代理设置（Proxy Settings）”窗口：



6. 确保没有选中“为所有协议使用同一代理服务器（Use the same proxy server for all protocols）”：



7. 在SOCKS行输入“使用的代理地址（Proxy address to use）”和“端口（Port）”号，然后点击“OK”：



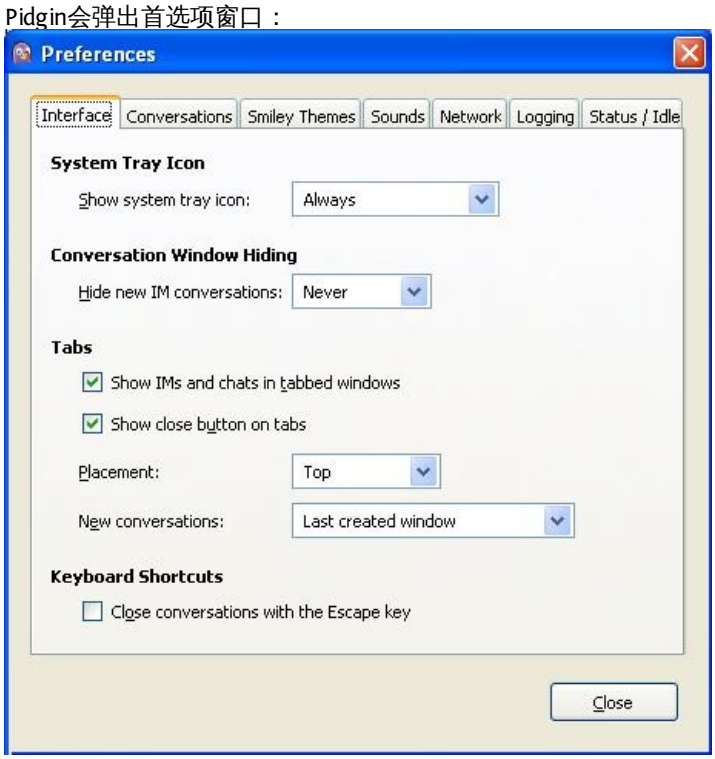
现在IE就可以使用SOCKS代理了。

为其他程序设置 SOCKS 代理

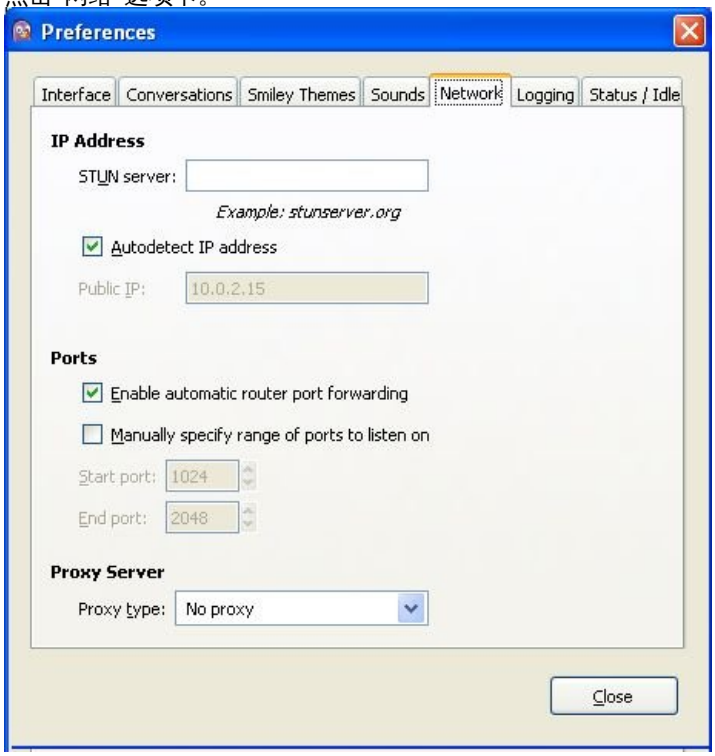
除浏览器之外的很多网络程序也可以通过SOCKS代理连接到网络，绕开网络屏蔽。以下设置的即时通讯软件Pidgin就是一个典型的例子，但是设置其它软件使用SOCKS代理的具体步骤可能略有不同。

1. 在“工具（Tools）”菜单单击“首选项（Preferences）”：

2. Pidgin会弹出首选项窗口：



3. 点击“网络”选项卡。



4. 在“代理类型（Proxy type）”里选择“SOCKS 5”，然后会出现更多选项。

5. 输入你想使用的SOCKS代理的“主机（Host）”和“端口（Port）”号。

6. 点击“关闭（Close）”。

这样Pidgin就可以使用SOCKS代理了。

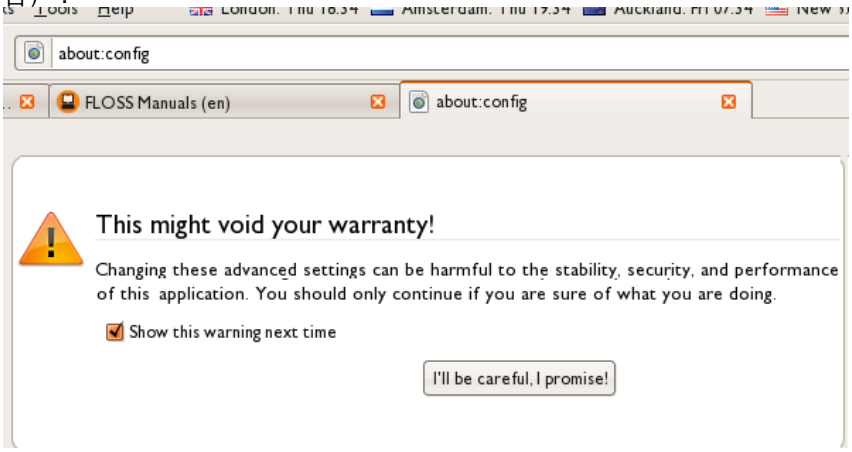
用完代理之后

在你用完代理之后，尤其是在共享计算机上，一定要把修改过的设置恢复到默认状态。不然，这些程序将继续尝试使用代理。如果你不想让别人知道你用过代理，或者提供本地代理的绕行程序没有同时运行，这会带来麻烦。

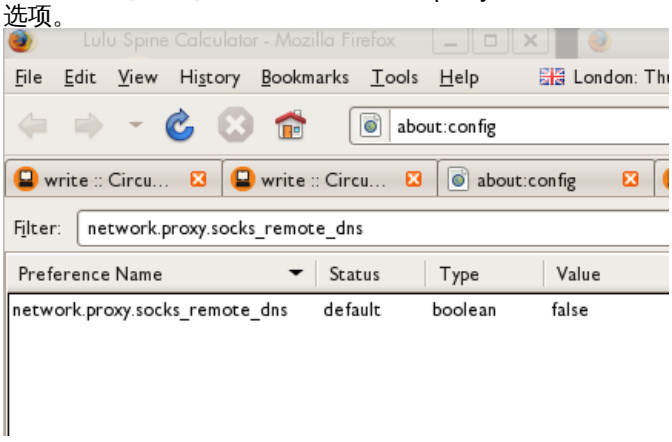
DNS 泄漏

使用SOCKS代理会存在一个严重的问题，即有些支持SOCKS代理的程序不会一直通过代理进行网络通信。最常见的就是域名系统（DNS）请求可能不通过代理发出。这种DNS泄漏会造成隐私问题，并可能导致你试图利用代理绕过的DNS被屏蔽。软件是否存在DNS泄漏问题视版本不同而不同。Mozilla Firefox当前的默认设置存在DNS泄漏问题，但是你可以通过永久设置更改阻止DNS泄漏，避免DNS泄漏的发生：

1. 像输入网址一样在火狐地址栏输入“about:config”（你可能会看到一个关于改变高级设置的警告）：



2. 如有必要，点击“我会小心，我保证！（I'll be careful, I promise!）”来确认你想修改浏览器设置。浏览器会显示一个配置设置信息列表。
3. 在“过滤器（Filter）”一栏输入“network.proxy.socks_remote_dns”。这里只会出现这一个设置选项。



4. 如果该设置的值为假（false），双击改变为“真（true）”。

现在火狐就可以阻止DNS泄漏了。一旦该值显示为真（true），火狐就会自动永久保存该设置。

如果不使用外部程序，目前还无法阻止微软IE浏览器内的DNS泄漏问题。

在本文撰写时，使用SOCKS 5代理的Pidgin软件还没有发生过DNS泄漏的情况。

HELPING OTHERS

研究和记录审查

在许多国家，存在政府审查互联网不是秘密。审查的范围和方法已被记录，如这些书：*Access Denied: The Practice and Policy of Global Internet Filtering* 和*Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace，都由*Ronald Delbert, John Palfrey, Rafal Rohozinski和 Jonathan Zittrain编辑(网址：http://opennet.net/accessdenied 和http://www.access-controlled.net)。

当一个流行的网站被广泛地封锁，这一事实易于被为这个国家所广泛了解。然而，有些国家（包括相当活跃的审查国家）官方否认存在审查，或者伪装成随机的技术错误。如果你遭受审查，你可以用你的情况帮助他人（包括研究审查的国际学者和活动家团体）了解审查并可能公布它。

当然，你需要小心：否认网络审查实践的国家可能并不欣赏你参与揭发他们的活动。

研究审查知识数据库

一些审查知识数据库最近几年已被公开。它们中有些是众包的（crowd-sourced），但它们都被这个领域的专家验证。它们不断更新以保持信息和被封锁网站的列表尽可能准确。部分数据库网址如下：

- *Herdict Web*: https://www.herdict.org

  Alkasir Map: https://www.alkasir.com/map

  在一个更大的地理范围， OpenNet Initiative 和 Reporters without Borders定期对每个国家发布“网络状态”的报告 。

- *OpenNet Initiative* 研究报告: http://opennet.net/research
- *Reporters Without Borders（无国界记者）* 网络敌人: http://www.rsf.org/ennemis.html

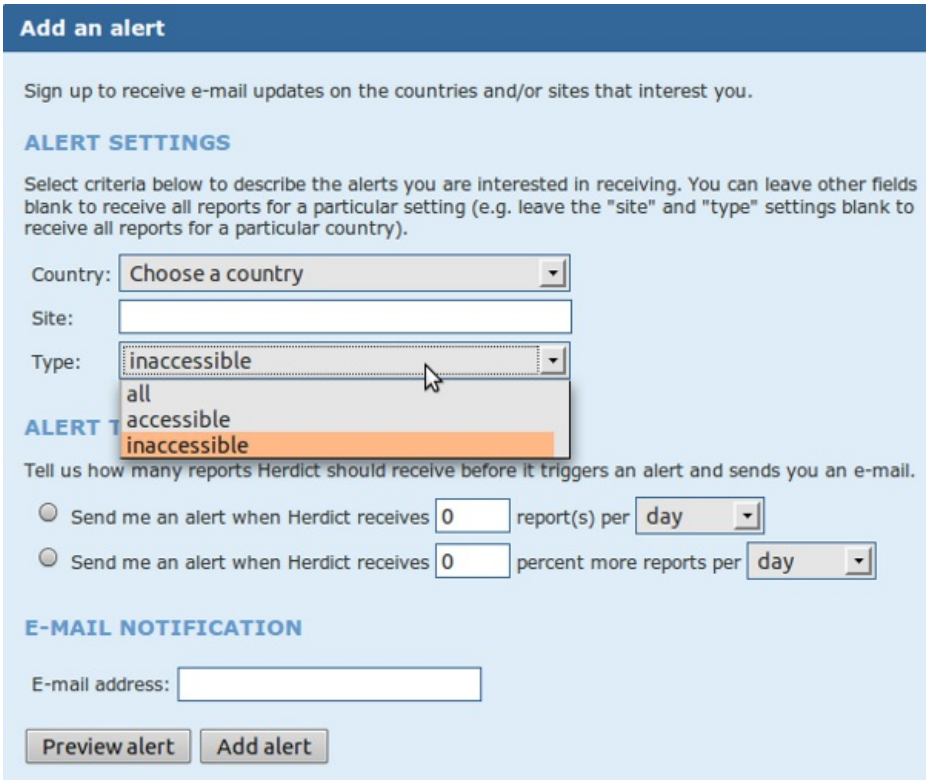
使用Herdict被告被封锁网站

Herdict (https://www.herdict.org)是一个聚合无法进入的网站报告的网站。它由美国哈佛大学Bekman互联网和社会研究中心的研究人员运营，他们研究互联网是如何被审查的。

Herdict的数据并不完美，例如许多用户并不能区分一个网站因为技术故障或者输错地址不可以使用和真正的审查，但数据在世界范围内收集并经常更新。

上图是Facebook报告的概貌。

你可以通过他们的网站提交你自己的报告给Herdic，帮助这些研究人员。它是免费的，容易使用，你甚至不需要注册。你也可以注册以获得一个网站将来封锁通知的消息。



Herdict也提供Firefox 和Internet Explorer浏览器的附加组件，使得报告你浏览时网站是否被封锁变得更简单。

使用Alkasir报告被封锁网站

Alkasir是一款审查绕行工具，允许用户轻轻点击“报告被封锁的地址” "Report Blocked URLs" 按钮，报告被封锁的网站。 Alkasir有一个相关的每个国家被封锁网站列表，可以自动检查其他网址的可用性。通过使用报告功能，你可以轻松地对这一研究做出贡献。

你可以在“使用Alkasir”这一章了解更多关于如何使用这个工具的内容。

允许他人远程访问

你可以通过允许研究人员远程访问你的电脑，使用它进行他们自己的测试，帮助审查研究。你只有在你信任研究人员和你提供给他们访问的性质的情况下才这样做，因为他们可以完全控制你的电脑，对你的互联网服务提供商和政府来说，他们在你电脑上做的任何事看起来跟你做的一样。

对GNU/Linux操作系统，一个*shell帐号是最好的选择* ，你可以在http://ubuntuforums.org和其他网站上找到安装帮助。

对Windows操作系统， 内置的远程桌面（*remote desktop* ）功能应该被使用。你可以在http://www.howtogeek.com/howto/windows-vista/turn-on-remote-desktop-in-windows-vista上找到说明。你可能也需要在你连接互联网用的路由器盒改变端口转发（*port forwarding）设置*，这有解释： http://portforward.com。

远程访问的另一个解决方案是免费工具TeamViewer (http://www.teamviewer.com)， 所有操作系统都可以使用它。

对比记录

记录网络审查的基本技术是尝试访问大量的网络资源，如一长串网址，从不同的地方访问，然后对比结果。是否有些网站在一些地方加载失败而在其他地方则不是？ 这些差别是持续的和系统的吗？如果你有可靠的绕行技术如VPN，你自己可以进行一些实验，对比有绕行工具和没有绕行工具网络是怎样的。例如，在美国这是用来记录互联网服务提供商是如和中断点对点文件分享软件使用的方法。

对比可以用自动操作的软件或手工进行。

数据包嗅探

如果你熟悉互联网协议是如果工作的技术细节，数据包嗅探工具如Wireshark (http://www.wireshark.com/) 可以让你记录你电脑目前传输和接受的网络数据包。

应对端口封锁

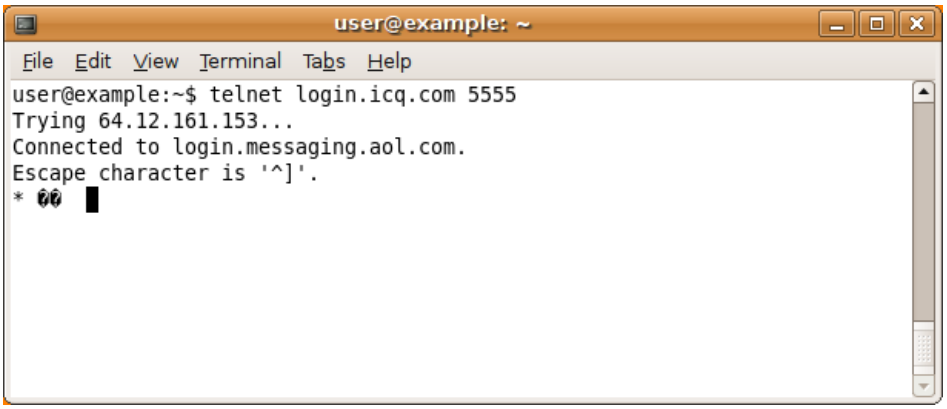
网络防火墙可以用来封锁指向一个特定端口（port）上的所有的通信。

这个用来阻止使用一个特定端口或某种网络软件。为绕开这一网络限制，互联网服务提供商和用户可以用非标准的端口访问服务。这允许软件绕开简单的端口封锁。

许多软件应用可以轻松使用非标准端口号。网页的网址有一个特别方便的方法，就在网址里进行。例如，网址*http://www.example.com:8000/foo/*可以告诉浏览器在端口8000向example.com进行一个 HTTP请求，而不是默认的http 端口 80。当然，这只有在www.example.com上网站服务器软件已经期待端口8000上的请求才可以。

测试端口屏蔽

你可以利用 Telnet 来测试你连接中的哪些端口被封锁。只需打开命令行，键入“telnet login.icq.com 5555”或“telnet login.oscar.aol.com 5555”，然后按下 Enter（回车键）。其中的数字是想要测试的端口。如果返回一些奇怪的字符，说明连接成功。



相反，如果计算机立即报告连接失败、超时或中断、断开或重置，那么说明该端口很可能已被封锁。（请注意，某些端口可能只对于某些特定 IP 地址是封锁的。）

安装网页代理

如果你在一个不审查互联网访问的国家有访问网络服务器的权限，你可以安装一个网页代理，其是以PHP、Perl、Python或ASP程序语言编写的小软件。基于网页的绕行软件的安装需要一些专业技术知识和资源（一个兼容的网络主机和足够的带宽）。

如果你想要安装你自己的网页代理，你需要以下之一：

• 一个有PHP支持的网络主机空间（其可以年费从类似https://www.dreamhost.com或http://www.hostgator.com的主机公司购买，或者由你的学校或大学提供）

• 一个虚拟的（VPS）或专用的服务器（这更昂贵且使用起来更复杂）

• 一台连接到宽带连接的个人电脑（有一个公共路由IP地址）

公共和私人网页代理

公共网页代理对每个想搜索其的人都可用，例如在像谷歌一样的搜索引擎上。公共网页代理和匿名服务可能被用户和那些实施过滤的当局发现，因此，他们更容易被列入黑名单。

私人网页代理的位置只有目标用户知道。因此，私人网页代理最适合需要稳定网络连接绕行服务及有值得信任的、拥有足够的技术能力与可用带宽设置和维护网页代理的联系人在未过滤地点的用户。私人网页代理被发现和封锁的几率低于那些公共绕行服务。其也是仅对网络连接可用的最灵活的绕行选择，且比公共网页代理更不容易被发现和封锁，特别是当它使用SSL加密时。

网页代理的功能

网页代理可以根据终端用户的具体需要而进行不同程度的定制。通常定制内容包括更换服务器运行端口或者使用SSL加密。由于一些黑名单中会包括一些和常用代理软件相关的关键词，所以通过改变默认URL、脚本名称或者用户界面元素，也可以降低代理服务被自动探测和封禁的风险。通过使用用户名和密码启用.htaccess可用保护网页代理的使用。

当使用SSL加密时，也可以在服务器的根目录下建立一个伪装页面，然后用随机路径和文件名把网页代理掩饰起来。虽然监控者可以发现你使用的服务器，但却不会发现代理路径，因为它是经过加密的。例如，如果一位用户链接到https://example.com/secretproxy/，监控者会发现该用户打开的是example.com，但却不会知道他实际上打开的是网页代理。如果网页代理运营商在example.com上放了一个伪装页面，那么通过监控网络传输就不太可能发现这个网页代理。一个在所有流行的网络浏览器中被信任的有效SSL证书可用在https://www.startcom.org/免费获取。

在互联网上有很多免费的开源网页代理。他们主要的不同在于其编写的程序语言，因为并不是每个网络服务器都支持每种程序语言。另一个较大的不同是使用像AJAX（被Gmail或Facebook使用）或Flash视频流（被YouTube使用）技术的现代网站脚本的兼容性。

常用的网页代理程序包括：

• CGIProxy (http://www.jmarshall.com/tools/cgiproxy)：一个以Perl程序语言编写的可以提供HTTP和FTP代理的CGI脚本。

• Peacefire's Circumventor (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html)：一个自动安装的程序，可以让没有技术背景的用户在Windows平台上方便地安装和调试CGIProxy。

• SabzProxy (http://sabzproxy.com)：一个HTTP和FTP代理。其基于以PHP编写的PHProxy的程式码，有一些新的功能，比如随机编码URL，使其更难封锁。

• Glype Proxy (http://www.glype.com)：另一个免费使用、基于网络的代理脚本，同样以PHP编写。

这些网页代理的网站提供有关如何安装它们的说明。基本上，这包括下载脚本、在本地硬盘提取、通过FTP或SCP上传脚本到你的网络服务器、设置权限和检测脚本。以下是安装SabzProxy的例子，不过对其他网页代理来说步骤是类似的。

Installing SabzProxy

SabzProxy只波斯语的界面可用，但GUI更简单且容易理解

这些说明描述了最常见的情况：使用FTP传输SabzProxy到一个已支持PHP的网络空间帐户。使用该技术，你同样需要一个像FileZilla （http://filezilla-project.org）的FTP客户端。

虽然这种方法最常见，但并不适用于每种情况（例如当你通过命令行设置你自己的服务器时），不过，这些步骤应该是类似的。

1. 第一步是从http://www.sabzproxy.com下载SabzProxy压缩文件。
2. 接下来，通过鼠标右键点击该.zip文件和选择提取所有以提取其内容。

3. 用基础文本编辑器打开config.php文件（例如，Windows中的Notepad、Linux系统中的Gedit或Nano、MacOS中的Texteditor）。
4. 编辑第8行，以*$config_key*开头。在“”“”之间输入一个随机字符串。该字符串将被用于随机化URL编码，因此使其尽可能地随机。

5. 你也可以配置一些选项，比如欢迎文本和链接。
6. 打开FileZilla，输入你网络空间的（主）服务器、用户名和密码，点击快速连接（或者类似的，如果你正是用一个不同的FTP客户端）。
7. FTP客户端窗口的左部代表你的本地个人电脑，因此你可以找到你刚提取在这里的SabzProxy文件。

8. 将文件从FTP客户端窗口的左部拖放到右部，右部代表远程FTP服务（你的网络空间）。
9. 现在，你可以通过浏览你的网络空间域和你上传PHProxy的目录访问SabzProxy。（如在http://kahkeshan-e-sabz.info/home的例子中。）如这不起作用，那么你的服务器帐户可能不支持PHP，或者PHP支持可能已失效或需要额外的步骤。请参考你的帐户文件或者使用的网络服务器软件。你也可以找一个合适的技术支持论坛或向你的网络服务器运营商询问更多的帮助。

运行代理的风险

当你在电脑上提供在线代理服务或使用代理软件时，通过代理发出的请求和连接就会显示发自你的电脑。你的计算机代表其他互联网用户，因此，他们的活动被认为是你做的，好像你自己做了这件事。如果有人使用代理发送或接受第三方所反对的资料， 你可能会被投诉、要求承担责任并停止这种行为。在一些情况下，使用代理还会带来法律问题，或者引起你所在国家或其他国家执法机关的注意。

一些国家的代理提供商曾经收到过法律投诉，而且在有些案子中，执法机关甚至还没收了提供代理服务的电脑。造成这种情况的原因可能有以下几个：

- 有人误以为代理服务提供者亲自参与了通过代理进行的活动。
- 有人可能认为代理服务提供者在法律上有义务制止某些代理使用行为。
- 有人可能希望检查代理服务（比如查找代理服务运行日志）以获取某人进行过某种活动的证据。

如果你认为在你所在地区提供代理服务会有风险，最好把代理服务放在数据中心的一台专用电脑上。这样，不会吸引别人注意你的家庭互联网连接。

不通国家向代理提供者提供的法律保护方式和程度可能会有所不同。如想知道你所在国的具体规定，你可以咨询律师或所在国法律专家。

运行公共代理的风险

网络服务提供商（ISP）也可能会因为你提供代理服务而投诉你，特别是当他们收到代理被滥用的申诉时。一些ISP会声称运行公共代理违反了他们的服务条款，或者他们干脆不想让用户运行公共代理。这些ISP可能会断开你的网络，或者威胁会在将来断开你的网络。

一个公共代理可能被世界各地的许多人使用，可能使用大量的带宽和流量，所以在使用非固定收费的互联网服务提供商时，应采取预防措施，以避免在月末支付很多的流量费用。

运行私人代理的风险

如果为了你个人或一小部分人的需要而运行非公共的代理，虽然也会有一定风险，但其风险要比运行公共代理小许多。

如果你建立的非公共代理被发现并监控，监控者就会意识到或推断出你正在通过连接帮助用户避开网络过滤。

与公共代理相比，你所在地的ISP对私人代理不太排斥，但一些ISP会的反代理政策非常全面，甚至不允许你利用他们的网络提供私人代理服务。

数据保留法律可能会管制代理服务

在某些国家，用来限制匿名使用的数据保留法律或相似法律，也可能适用于管制代理服务。如想了解更多关于数据保留的信息，请参阅https://secure.wikimedia.org/wikipedia/en/wiki/Telecommunications_data_retention.

网站管理员的最佳做法

运营一个网站，无论是否有广大的读者，不总是容易。考虑自己的安全和访问者的安全是重要的。当网站出人意料地在某个国家被封锁，网站管理员常常感到惊奇。如果大量的访问者不能访问网站，网站的经营者可能也会遇到经济问题。失去网站的内容或者服务器，或者不得不架设新的服务器，也是件令人不安和沮丧的事。

这一章试图收集一个运营网站需要记住的好的做法和建议的清单。

保护你的网站

- 一直定期在至少一台其他的物理计算机上自动备份（文件和数据库）。确保你知道怎么还原它。
- 监控你的流量了解你的访问者来自哪些国家。你可以使用地理位置数据库猜测一个**IP**地址来自哪个国家。如果你注意到来自某个国家的流量有较多的下降，你的网站可能被屏蔽了。你可以在区域被封锁网站数据库如Herdict (https://www.herdict.org/web)上分享。
- 保护你的网站，尤其你使用CMS (Content Management System)时。总是按照最新的稳定更新修复安全漏洞。
- 进行高度安全性设置，保护你的网络服务器软件（你可以找到大量的关于如何保护Linux网络服务器的网络资源）
- 注册（或转移）你的域名到其他的**DNS**提供商，它不是你的空间服务商。如果你现在的提供商遭到攻击，你可以轻松地将你的域名指向新的空间服务商。
- 你也可以创建一个镜像服务器，作为一个你可以轻松转换的备用品。学会怎样将你的DNS服务转换到镜像服务器。
- 考虑你的网站托管到国外，在那内容较少受到争议并清晰地受到法律保护。这意味着你的访问者加载网页所花的时间有一点延时（通常几毫秒），如果在你所在的国家你的网站的内容被认为非常有争议，你可以避免很多麻烦。
- 使用你的访问者可能使用的主要的绕行工具测试和优化你的网站。检查和修复任何无法显示的页面或者功能。理想地，让那些没有JavaScript 或插件的访问者可以使用你的网站，因为当人们使用代理时这些可能不能被使用。
- 避免使用**FTP** 上传你的文件。FTP在网上发送你的密码没有加密，使得窃听者容易窃取你的登录信息。考虑用SFTP (File Transfer Protocol over SSH), SCP, 或者 secure WebDAV (over HTTPS) 替代。
- 使用其他的端口进入你的后台。黑客经常自动扫描标准的端口发现漏洞。考虑将你的端口改成非标准的（如**SSH**），将受攻击的风险最小化。
- 通过在服务器安装DenyHosts（(http://denyhosts.sourceforge.net)）之类的工具保护你的服务器，将超过一定时间登录失败的IP地址列入黑名单，保护你的服务器免受暴力攻击。

保护你自己

如果作为网站管理员保持匿名对你来说重要的话，这些技巧可以帮助你防止可能的人身伤害。

- 使用匿名的跟你真实身份无关的电子邮件地址和名字。
- 如果你有一个专用的域名，你可以在**WHOIS** 公开数据库通过使用叫做"WHOIS proxy", "WHOIS protect" 或"domain privacy"的服务输入假的信息。
- 更新网站时使用Tor等服务保持匿名。

保护你的访问者

除了保护网站和你自己，保护访问者免受可能的第三方监视也重要，尤其他们向你的网站提交内容。

- 配置HTTPS，这样你的用户可以使用加密连接访问你的网站，自动查看正在传送的内容和弄清楚你的身份将变得更难。确保你HTTPS配置覆盖你整个网站和使用其他配置HTTPS的最佳做法。你可以在https://www.eff.org/pages/how-deploy-https-correctly 上找到如何正确配置它的信息。你也可以在https://www.ssllabs.com/上就很多技术参数进行自动测试。
- 尽可能在日志中减少保存的数据。没有必要，不要保存IP地址或者其他与你访问者有关的个人人数据。
- 加密关键的用户数据如密码，例如使用salted hashes。
- 外部的服务如Google Analytics或者其他第三方内容如广告网络难以控制。避免使用它们。

- 为你的网站创建一个轻的和安全的版本，没有Flash或者 Javascript 嵌入代码，和Tor以及低带宽的网络连接相容。

教育你的访问者

- **Teach your users** how to use circumvention tools, and be able to improve their online security.
- **Make a digital safety checklist** available so your visitors can be sure they are not being monitored or attacked.
- 教你的用户使用绕行工具和改进他们的网络安全。
- 制作一个数字安全清单，你的访问者可以确保他们没有被监视或攻击。

向你的访问者分享绕行工具

- 托管网页代理
(如SabzProxy 或 Glype Proxy).。通过邮件或者你的社交网络向你的访问者分享它们。
- 如果你在私人节点有一个帐号，向他们
发送赛风（**psiphon**）邀请。
- 如果你有一个装用的服务器，
安装其他种类的网页代理和应用代理，并分享它。
- 在你的网站
连接这本指南或者相关的绕行工具。

增加发行渠道

网站管理员可以而且应该为尽可能地传播他们的内容而采取不同的措施防止被关闭或者被封锁。

- 创建一份简讯（**newsletter**），通过邮件发送新内容的定期更新。当你的读者不再能访问你的网站时，你仍然能联络他们。
- 创建**RSS**种子，确保它包含全文而不是摘要（片段）。这样你的内容可以轻易地被第三方网站和应用如**Google Reader**解析，在不能直接访问的地方它们可以用来阅读你的内容。
- 在流行的社交网络平台分享你的内容，如Facebook 或者Twitter ，它们难以被封锁。
- 尽可能传播你的内容。让你的内容可以被下载。例如，维基百科将它的全部内容作为数据库转储发送，可以轻松地用来在别处创建有着同样内容的新的镜像网站。
- 考虑采用开放授权协议（如**GPL** 或者**Creative Commons**）发表你的文章，它允许每个人重新使用你的内容和创建镜像。
- 在文件分享托管服务如Rapidshare.com或者Megaupload.com上，以及点对点文件分享软件如Bittorrent上备份你的文件。
- 配置你的网络服务器让它也能服务在其他端口的内容，而不仅仅是标准端口80 (*http*) 和443 (*https*)。
- 提供一个应用程序界面（**API** (application programming interface)），如 Twitter 或者 维基百科（Wikipedia）所做的，可以允许他人通过第三方软件自动访问你的内容。

减少你的页面加载时间

减少你的页面加载时间不仅可以节省你的带宽和金钱，也可以帮助来自发展中国际的访问者更好地访问你的信息。一个好的加快你网站的最佳做法的列表可以在 http://developer.yahoo.com/performance/rules.html和 https://code.google.com/speed/page-speed/找到。

- 采用简约风格。 考虑将图片最小化，使用CSS设计你的布局。一个好的关于CSS的介绍可以在http://www.w3schools.com/css/css_intro.asp.找到。
- 优化你的图片。使用OptiPNG (http://optipng.sourceforge.net/)之类的程序优化它们，让你的图片加载速度更快。另外，如果你不需要，不要使用HTML改变图片的大小（例如，你需要一个60x60的图片，直接调整它的大小，而不是使用HTML）。

- 尽量减少**Java**、**JavaScript**、**Flash**和其他可在客户电脑运行的内容。记住有些网吧处于安全考虑不支持这种内容。务必让你想传递的信息以纯**HTML**格式显示。
- 为你的**CSS**和**JavaScript** 使用外部文件。如果你使用某种**CSS**样式或JavaScript，它们一再在你网站上出现，可以考虑保存为单独的文件，并在网页的页眉调用它。这将允许你的客户的浏览器把文件存储于硬盘，每次他们访问你网站的网页时，他们将不需要下载所有的内容。
- 缩减你的代码。去掉不需要的不起作用的行和空格。有些工具可以自动做这些，可以在http://javascriptcompressor.com上找到。
- 尽可能减少服务器请求。如果你有一个动态的网站，但是内容改变不频繁，你可能需要安装一个缓存扩展，它可以向你的用户提供你的内容的静态版本，因此明显的减少请求你数据库的数量。

设置一个 Tor 中继

如果你生活在一个没有/几乎没有网络审查的地区，你只需要运行简单的Tor*中继*或者Tor网桥中继，就可以帮助其他Tor用户避开审查访问互联网。

Tor网络靠的是志愿者贡献带宽，所以运行中继的人越多，Tor网络的速度也会越快、访问也就越安全。如果想帮助其他使用Tor的人绕过网络审查，就建立一个网桥中继，而不要建立普通中继。

*网桥中继（Bridge relays）*指的是那些没有列入主力（公开）Tor目录中的Tor中继。即便网络服务提供商会过滤所有已知的Tor中继，也不可能把所有网桥中继封禁掉。

运行Tor节点（Tor中继）的风险

一个Tor节点是一种公共代理，所以运行一个可能会有本指南“运行代理的风险”一章中提到运行一个代理的一般风险。但是典型的Tor节点有两种类型：出口节点（exit node）和中间人节点（middleman node），也叫做非出口节点（non-exit node）。中间人节点只把经过加密的通信传递给其他节点，并不允许匿名用户与Tor网络之外的站点直接通信。运行这两种节点对整个Tor网络来说都有帮助，运行出口节点尤其有用，因为它相对数量较少。运行中间人节点相对风险较低，它不会作为公共代理被投诉，因为中间人节点的IP地址永远不会被写入运行日 志。

因为网桥不是出口节点（exit node），你不会因为他人使用网桥节点而被投诉。

尽管运行中间人节点和网桥节点并不会招致投诉，但它们会让您的ISP有更多理由反对你提供代理。例如，ISP可能会反对你使用Tor网络，或者禁止用户运行任何类型的公共服务。 你可以在https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment上找到如何安全运行一个Tor出口节点（exit node）的最佳做法。

运行Tor中继或者网桥中继需要我做什么？

运行一个Tor中继只需满足以下几个条件：

- 你的互联网连接的上下行带宽至少为20KB/S（而且在你电脑开机期间都要保证稳定的连接）。
- 你的互联网连接必须拥有一个可以路由传送的公网IP地址。
- 如果你的电脑处于网络地址转换（NAT）防火墙内，没有公网IP地址，你必须在路由器上设定端口映射规则。你可以借助Tor的通用即插即用设备完成这一步骤，也可以通过查看你的路由器使用说明，或者根据portforward.com（http://portforward.com/english/applications/port_forwarding/HTTPS/HTTPSindex.htm）上的说明手动设置它。

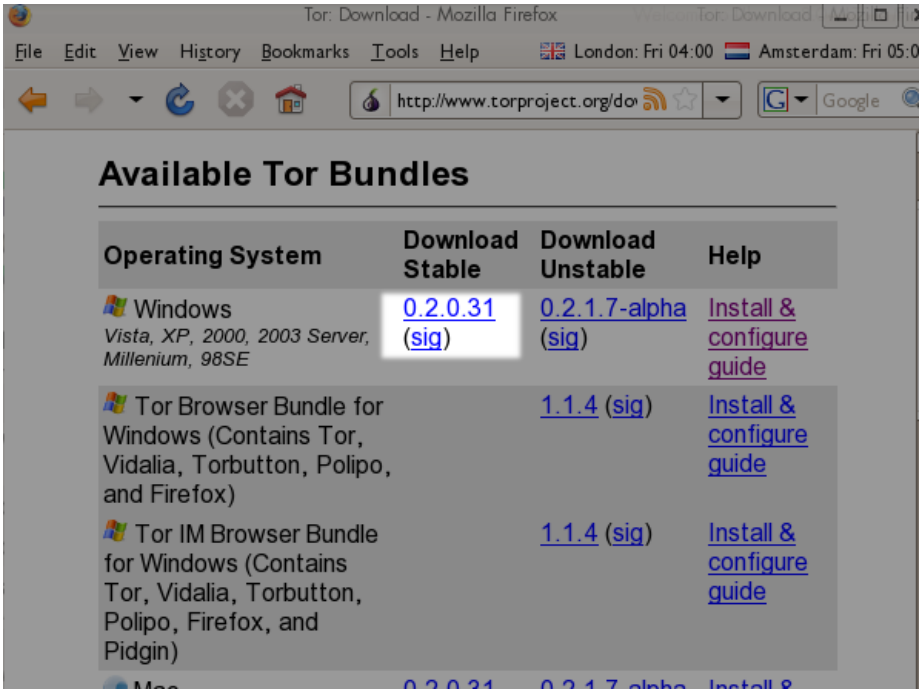
非必需条件有：

- 你的电脑不必一直开机联网（Tor目录会在开机并联网的时候设置好一切）。
- 你不必拥有一个静态IP地址。

下载 Tor

你可以到http://www.torproject.org/点击导航栏中的“下载（Download）”得到Tor。

在“可用的Tor套件（Available Tor Bundles）”页面，选择适合你操作系统的稳定版本。



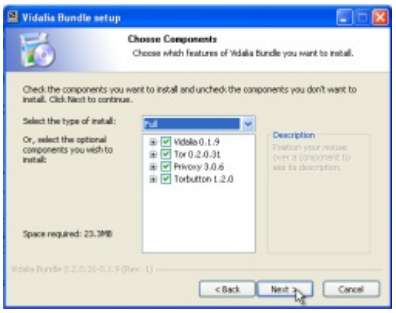
在GNU / Linux上安装Tor

你可以在https://www.torproject.org/docs/tor-doc-relay.html.en上找到关于如何运行一个Tor中继或网桥的详细说明。

在Microsoft Windows上安装Tor

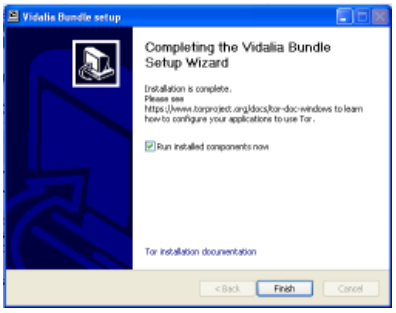
打开安装程序并一路点击“下一步（Next）”。

如果你使用的是火狐浏览器，则需安装下图对话框中所列出的所有组件：



如果你没有安装火狐，则要取消选择“Torbutton”（随后你将会看到安装火狐和Torbutton的选项）。

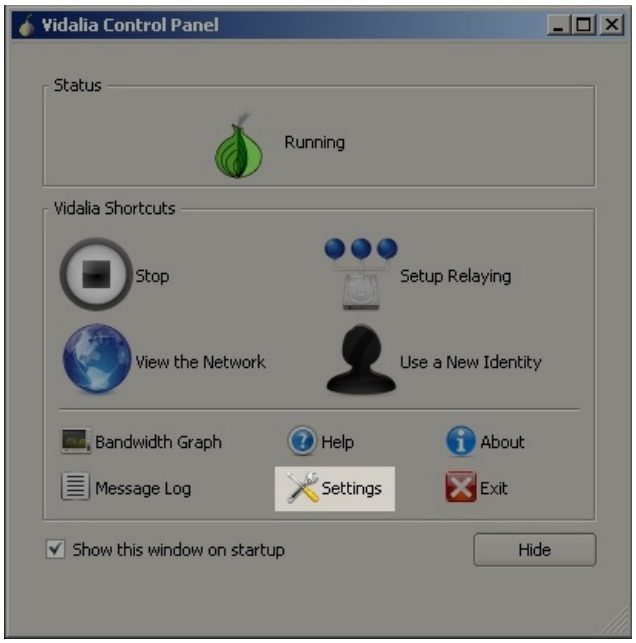
当安装完成后，选中如下图所示的“现在运行安装好的组件（Run installed components now）”，点击“完成（Finish）”按钮：



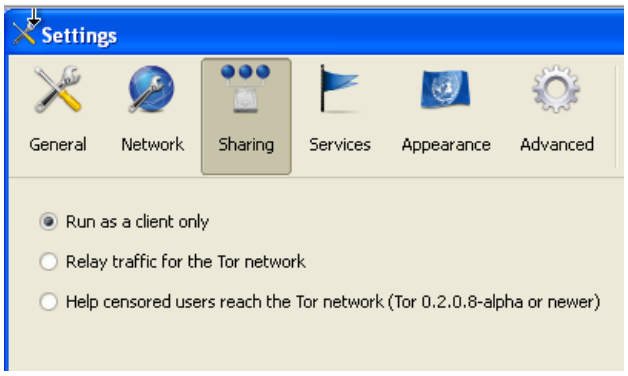
设置 Tor 网桥

执行以下操作来打开你的网桥：

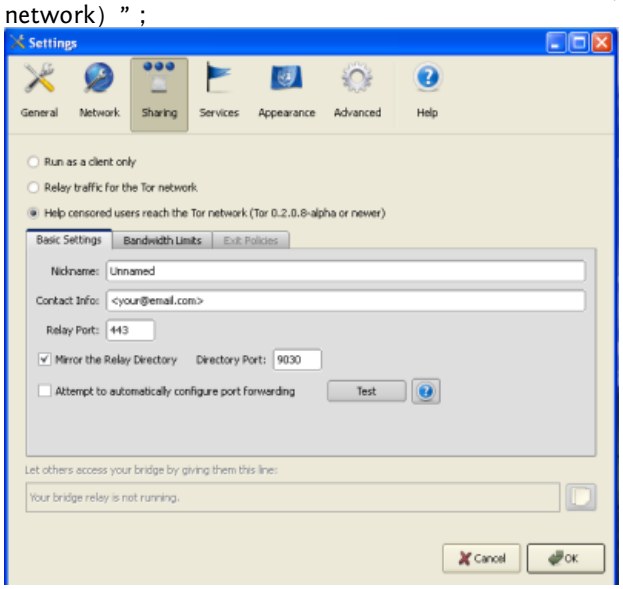
- 打开Vidalia控制面板；
- 点击控制面板中的“设置（Settings）”：



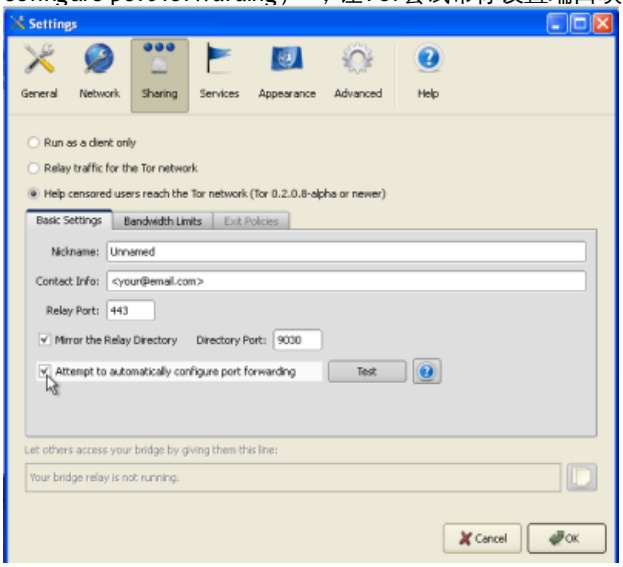
2. 在“设置”窗口中，点击“分享（Sharing）”；



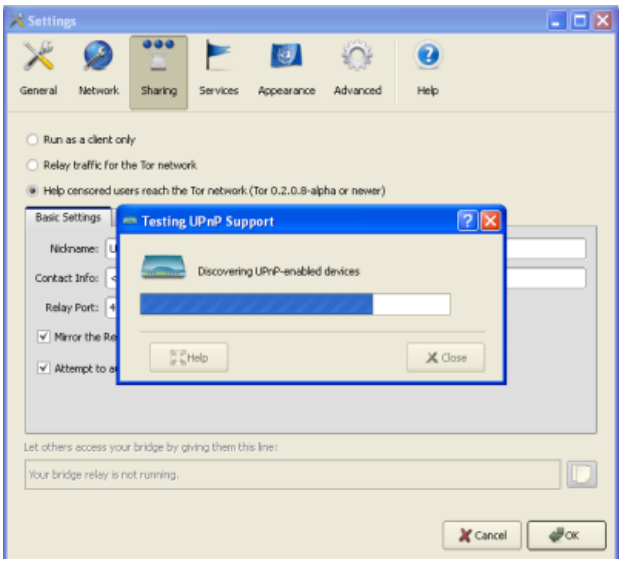
3. 要创建网桥，点击“帮助有网络审查的用户使用Tor网络（Help censored users reach the Tor network）”；



4. 如果你的本地网络使用的是网络地址转换后的IP地址（NAT IP address），则需要在路由器中创建端口映射规则。你可以通过点击“尝试自动设置端口映射（Attempt to automatically configure port forwarding）”，让Tor尝试帮你设置端口映射；



5. 点击“测试（Test）”来检测Tor是否在路由器上正确地创建了端口映射；

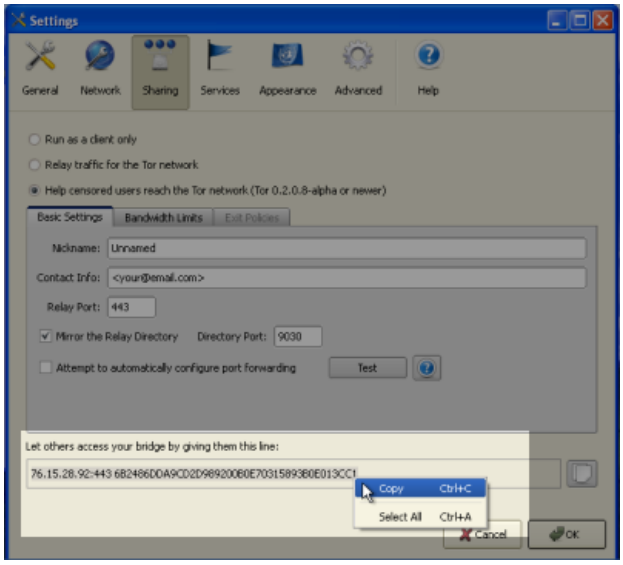


如果Tor不能自动设置端口映射，请参阅Tor FAQ中关于此问题的解决方法：https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#ServerForFirewalledClients

恭喜！如果一切正常的话，你的网桥已经建立并能正常运行了。你的网桥信息将被加入到隐藏的网桥目录，并供其他发送了请求的用户使用。

与朋友分享你的网桥

如果你建立网桥是为了能让你的朋友使用Tor网络，你可以把设置窗口下方的信息拷贝下来，发送给他/她。


Settings
General
Network
Sharing
Services
Appearance
Advanced
Help
Run as a client only
Relay traffic for the Tor network
Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)
Basic Settings
Bandwidth Limits
Exit Policies
Nickname: Unnamed
Contact Info: <your@email.com>
Relay Port: 443
Mirror the Relay Directory
Directory Port: 9030
Attempt to automatically configure port forwarding
Test
Let others access your bridge by giving them this line:
76.15.28.92:443 6B2486DDA9CD2D98920060E70315893B0E013CC1
Copy Ctrl+C
Select All Ctrl+A
Cancel
OK

APPENDICES

Glossary

Much of this content is based on http://en.cship.org/wiki/Special:Allpages

aggregator

An aggregator is a service that gathers syndicated information from one or many sites and makes it available at a different address. Sometimes called an RSS aggregator, a feed aggregator, a feed reader, or a news reader. (Not to be confused with a **Usenet** News reader.)

anonymity

(Not be confused with privacy, pseudonymity, security, or confidentiality.)

Anonymity on the Internet is the ability to use services without leaving clues to one's identity. The level of protection depends on the anonymity techniques used and the extent of monitoring. The strongest techniques in use to protect anonymity involve creating a chain of communication using a random process to select some of the links, in which each link has access to only partial information about the process. The first knows the user's IP address but not the content, destination, or purpose of the communication, because the message contents and destination information are encrypted. The last knows the identity of the site being contacted, but not the source of the session. One or more steps in between prevents the first and last links from sharing their partial knowledge in order to connect the user and the target site.

anonymous remailer

An anonymous remailer is a service that accepts e-mail messages containing instructions for delivery, and sends them out without revealing their sources. Since the remailer has access to the user's address, the content of the message, and the destination of the message, remailers should be used as part of a chain of *multiple* remailers so that no one remailer knows all this information.

ASP (application service provider)

An ASP is an organization that offers software services over the Internet, allowing the software to be upgraded and maintained centrally.

backbone

A backbone is one of the high-bandwidth communications links that tie together networks in different countries and organizations around the world to form the Internet.

badware

See **malware**.

bandwidth

The bandwidth of a connection is the maximum rate of data transfer on that connection, limited by its capacity and the capabilities of the computers at both ends of the connection.

bash (Bourne-again shell)

The bash shell is a command-line interface for Linux/Unix operating systems, based on the Bourne shell.

BitTorrent

BitTorrent is a **peer-to-peer** file-sharing **protocol** invented by Bram Cohen in 2001. It allows individuals to cheaply and effectively distribute large files, such as CD images, video, or music files.

blacklist

A blacklist is a list of forbidden persons or things. In Internet censorship, lists of forbidden Web sites may be used as blacklists; **censorware** may allow access to all sites except for those specifically listed on its blacklist. An alternative to a blacklist is a **whitelist**, or a list of permitted things. A whitelist system blocks access to all sites except for those specifically listed on the whitelist. This is a less common approach to Internet censorship. It is possible to combine both approaches, using string matching or other conditional techniques on **URL**s that do not match either list.

bluebar

The blue **URL** bar (called the Bluebar in Psiphon lingo) is the form at the top of your Psiphon node browser window, which allows you to access blocked site by typing its URL inside.

See also **Psiphon node**

block

To block is to prevent access to an Internet resource, using any number of methods.

bookmark

A bookmark is a placeholder within software that contains a reference to an external resource. In a browser, a bookmark is a reference to a Web page – by choosing the bookmark you can quickly load the Web site without needing to type in the full **URL**.

bridge

See **Tor bridge**.

brute-force attack

A brute force attack consists of trying every possible code, combination, or password until you find the right one. These are some of the most trivial hacking attacks.

cache

A cache is a part of an information-processing system used to store recently used or frequently used data to speed up repeated access to it. A Web cache holds copies of Web page files.

censor

To censor is to prevent publication or retrieval of information, or take action, legal or otherwise, against publishers and readers.

censorware

Censorware is software used to **filter** or **block** access to the Internet. This term is most often used to refer to Internet filtering or blocking software installed on the client machine (the PC which is used to access the Internet). Most such client-side censorware is used for parental control purposes.

Sometimes the term censorware is also used to refer to software used for the same purpose installed on a network server or **router**.

CGI (Common Gateway Interface)

CGI is a common standard used to let programs on a Web server run as Web applications. Many Web-based proxies use CGI and thus are also called "CGI proxies". (One popular CGI proxy application written by James Marshall using the Perl programming language is called CGIProxy.)

chat

Chat, also called **instant messaging**, is a common method of communication among two or more people in which each line typed by a participant in a session is echoed to all of the others. There are numerous chat protocols, including those created by specific companies (AOL, Yahoo!, Microsoft, Google, and others) and publicly defined protocols. Some chat client software uses only one of these protocols, while others use a range of popular protocols.

circumvention
Circumvention is publishing or accessing content in spite of attempts at censorship.

Common Gateway Interface
See CGI.

command-line interface
A method of controlling the execution of software using commands entered on a keyboard, such as a Unix shell or the Windows command line.

cookie
A cookie is a text string sent by a Web server to the user's browser to store on the user's computer, containing information needed to maintain continuity in sessions across multiple Web pages, or across multiple sessions. Some Web sites cannot be used without accepting and storing a cookie. Some people consider this an invasion of privacy or a security risk.

country code top-level domain (ccTLD)
Each country has a two-letter country code, and a TLD (**top-level domain**) based on it, such as .ca for Canada; this domain is called a country code top-level domain. Each such ccTLD has a DNS server that lists all second-level domains within the TLD. The Internet root servers point to all TLDs, and cache frequently-used information on lower-level domains.

DARPA (Defense Advanced Projects Research Agency)
DARPA is the successor to ARPA, which funded the Internet and its predecessor, the ARPAnet.

decryption
Decryption is recovering plain text or other messages from encrypted data with the use of a key.

See also **encryption**.

domain
A domain can be a **Top-Level Domain** (TLD) or secondary domain on the Internet.

See also **Top-Level Domain**, **country code Top-Level Domain** and **secondary domain**.

DNS (Domain Name System)
The Domain Name System (DNS) converts domain names, made up of easy-to-remember combinations of letters, to IP addresses, which are hard-to-remember strings of numbers. Every computer on the Internet has a unique address (a little bit like an area code+telephone number).

DNS leak
A DNS leak occurs when a computer configured to use a **proxy** for its Internet connection nonetheless makes DNS queries without using the proxy, thus exposing the user's attempts to connect with blocked sites. Some Web browsers have configuration options to force the use of the proxy.

DNS server
A DNS server, or name server, is a server that provides the look-up function of the Domain Name System. It does this either by accessing an existing cached record of the IP address of a specific **domain**, or by sending a request for information to another name server.

DNS tunnel
A DNS tunnel is a way to **tunnel** almost everything over DNS/Nameservers.

Because you "abuse" the DNS system for an unintended purpose, it only allows a very slow connection of about 3 kb/s which is even less than the speed of an analog modem. That is not enough for YouTube or **file sharing**, but should be sufficient for instant messengers like ICQ or MSN Messenger and also for plain text e-mail.

On the connection you want to use a DNS tunnel, you only need port 53 to be open; therefore it even works on many commercial Wi-Fi providers without the need to pay.

The main problem is that there are no public modified nameservers that you can use. You have to set up your own. You need a server with a permanent connection to the Internet running Linux. There you can install the free software OzymanDNS and in combination with SSH and a proxy like Squid you can use the tunnel. More Information on this on http://www.dnstunnel.de.

eavesdropping

Eavesdropping is listening to voice traffic or reading or filtering data traffic on a telephone line or digital data connection, usually to detect or prevent illegal or unwanted activities or to control or monitor what people are talking about.

e-mail

E-mail, short for electronic mail, is a method to send and receive messages over the Internet. It is possible to use a Web mail service or to send e-mails with the SMTP protocol and receive them with the POP3 protocol by using an e-mail client such as Outlook Express or Thunderbird. It is comparatively rare for a government to block e-mail, but e-mail surveillance is common. If e-mail is not encrypted, it could be read easily by a network operator or government.

embedded script

An embedded script is a piece of software code.

encryption

Encryption is any method for recoding and scrambling data or transforming it mathematically to make it unreadable to a third party who doesn't know the secret key to decrypt it. It is possible to encrypt data on your local hard drive using software like TrueCrypt (http://www.truecrypt.org) or to encrypt Internet traffic with **SSL** or SSH.

See also **decryption**.

exit node

An exit node is a Tor node that forwards data outside the Tor network.

See also **middleman node**.

file sharing

File sharing refers to any computer system where multiple people can use the same information, but often refers to making music, films or other materials available to others free of charge over the Internet.

file spreading engine

A file spreading engine is a Web site a publisher can use to get around censorship. A user only has to upload a file to publish once and the file spreading engine uploads that file to some set of sharehosting services (like Rapidshare or Megaupload).

filter

To filter is to search in various ways for specific data patterns to **block** or permit communications.

Firefox

Firefox is the most popular free and open source Web browser, developed by the Mozilla Foundation.

forum

On a Web site, a forum is a place for discussion, where users can post messages and comment on previously posted messages. It is distinguished from a mailing list or a **Usenet** newsgroup by the persistence of the pages containing the message threads. Newsgroup and mailing list archives, in contrast, typically display messages one per page, with navigation pages listing only the headers of the messages in a thread.

frame

A frame is a portion of a Web page with its own separate **URL**. For example, frames are frequently used to place a static menu next to a scrolling text window.

FTP (File Transfer Protocol)

The FTP **protocol** is used for file transfers. Many people use it mostly for downloads; it can also be used to upload Web pages and scripts to some Web servers. It normally uses ports 20 and 21, which are sometimes blocked. Some FTP servers listen to an uncommon port, which can evade port-based blocking.

A popular free and open source FTP client for Windows and Mac OS is FileZilla. There are also some Web-based FTP clients that you can use with a normal Web browser like Firefox.

gateway

A gateway is a **node** connecting two networks on the Internet. An important example is a national gateway that requires all incoming or outgoing traffic to go through it.

honeypot

A honeypot is a site that pretends to offer a service in order to entice potential users to use it, and to capture information about them or their activities.

hop

A hop is a link in a chain of **packet** transfers from one computer to another, or any computer along the route. The number of hops between computers can give a rough measure of the delay (**latency**) in communications between them. Each individual hop is also an entity that has the ability to eavesdrop on, block, or tamper with communications.

HTTP (Hypertext Transfer Protocol)

HTTP is the fundamental **protocol** of the World Wide Web, providing methods for requesting and serving Web pages, querying and generating answers to queries, and accessing a wide range of services.

HTTPS (Secure HTTP)

Secure HTTP is a **protocol** for secure communication using **encrypted** HTTP messages. Messages between client and server are encrypted in both directions, using keys generated when the connection is requested and exchanged securely. Source and destination IP addresses are in the headers of every **packet**, so HTTPS cannot hide the fact of the communication, just the contents of the data transmitted and received.

IANA (Internet Assigned Numbers Authority)

IANA is the organization responsible for technical work in managing the infrastructure of the Internet, including assigning blocks of IP addresses for **top-level domains** and licensing domain registrars for ccTLDs and for the generic TLDs, running the root name servers of the Internet, and other duties.

ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN is a corporation created by the US Department of Commerce to manage the highest levels of the Internet. Its technical work is performed by IANA.

Instant Messaging (IM)

Instant messaging is either certain proprietary forms of chat using proprietary protocols, or chat in general. Common instant messaging clients include MSN Messenger, ICQ, AIM or Yahoo! Messenger.

intermediary

See **man in the middle**.

Internet

The Internet is a network of networks interconnected using TCP/IP and other communication **protocols**.

IP (Internet Protocol) Address

An IP address is a number identifying a particular computer on the Internet. In the previous version 4 of the Internet Protocol an IP address consisted of four bytes (32 bits), often represented as four integers in the range 0-255 separated by dots, such as 74.54.30.85. In IPv6, which the Net is currently switching to, an IP address is four times longer, and consists of 16 bytes (128 bits). It can be written as 8 groups of 4 hex digits separated by colons, such as `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

IRC (Internet relay chat)

IRC is a more than 20-year-old Internet **protocol** used for real-time text conversations (chat or **instant messaging**). There exist several IRC networks -- the largest have more than 50 000 users.

ISP (Internet Service Provider)

An ISP (Internet service provider) is a business or organization that provides access to the Internet for its customers.

JavaScript

JavaScript is a scripting language, commonly used in Web pages to provide interactive functions.

keyword filter

A keyword filter scans all Internet traffic going through a server for forbidden words or terms to **block**.

latency

Latency is a measure of time delay experienced in a system, here in a computer network. It is measured by the time between the *start* of **packet** *transmission* to the *start* of packet *reception*, between one network end (e.g. you) to the other end (e.g. the Web server). One very powerful way of Web filtering is maintaining a very high latency, which makes lots of **circumvention** tools very difficult to use.

log file

A log file is a file that records a sequence of messages from a software process, which can be an application or a component of the operating system. For example, Web servers or proxies may keep log files containing records about which IP addresses used these services when and what pages were accessed.

low-bandwidth filter

A low-bandwidth filter is a Web service that removes extraneous elements such as advertising and images from a Web page and otherwise compresses it, making page download much quicker.

malware

Malware is a general term for malicious software, including viruses, that may be installed or executed without your knowledge. Malware may take control of your computer for purposes such as sending spam. (Malware is also sometimes called badware.)

man in the middle

A man in the middle or man-in-the-middle is a person or computer capturing traffic on a communication channel, especially to selectively change or **block** content in a way that undermines cryptographic security. Generally the man-in-the-middle attack involves impersonating a Web site, service, or individual in order to record or alter communications. Governments can run man-in-the-middle attacks at country **gateways** where all traffic entering or leaving the country must pass.

middleman node

A middleman node is a **Tor node** that is not an **exit node**. Running a middleman node can be safer than running an exit node because a middleman node will not show up in third parties' log files. (A middleman node is sometimes called a non-exit node.)

monitor

To monitor is to check a data stream continuously for unwanted activity.

network address translation (NAT)

NAT is a **router** function for hiding an address space by remapping. All traffic going out from the router then uses the router's IP address, and the router knows how to route incoming traffic to the requestor. NAT is frequently implemented by firewalls. Because incoming connections are normally forbidden by NAT, NAT makes it difficult to offer a service to the general public, such as a Web site or public proxy. On a network where NAT is in use, offering such a service requires some kind of firewall configuration or NAT traversal method.

network operator

A network operator is a person or organization who runs or controls a network and thus is in a position to **monitor**, **block**, or alter communications passing through that network.

node

A node is an active device on a network. A **router** is an example of a node. In the Psiphon and Tor networks, a server is referred to as a node.

non-exit node

See **middleman node**.

obfuscation

Obfuscation means obscuring text using easily-understood and easily-reversed transformation techniques that will withstand casual inspection but not cryptanalysis, or making minor changes in text strings to prevent simple matches. **Web proxies** often use obfuscation to hide certain names and addresses from simple text filters that might be fooled by the obfuscation. As another example, any **domain** name can optionally contain a final dot, as in "somewhere.com.", but some filters might search only for "somewhere.com" (without the final dot).

open node

An open node is a specific **Psiphon node** which can be used without logging in. It automatically loads a particular homepage, and presents itself in a particular language, but can then be used to browse elsewhere.

See also **Psiphon node**.

packet

A packet is a data structure defined by a communication **protocol** to contain specific information in specific forms, together with arbitrary data to be communicated from one point to another. Messages are broken into pieces that will fit in a packet for transmission, and reassembled at the other end of the link.

peer-to-peer

A peer-to-peer (or P2P) network is a computer network between equal peers. Unlike client-server networks there is no central server and so the traffic is distributed only among the clients.This technology is mostly applied to **file sharing** programs like **BitTorrent**, eMule and Gnutella. But also the very old **Usenet** technology or the **VoIP** program Skype can be categorized as peer-to-peer systems.

See also **file sharing**.

PHP

PHP is a scripting language designed to create dynamic Web sites and web applications. It is installed on a Web server. For example, the popular **Web proxy** PHProxy uses this technology.

plain text

Plain text is unformatted text consisting of a sequence of character codes, as in ASCII plain text or Unicode plain text.

plaintext

Plaintext is unencrypted text, or decrypted text.

See also **encryption**, **SSL**, **SSH**.

privacy

Protection of personal privacy means preventing disclosure of personal information without the permission of the person concerned. In the context of **circumvention**, it means preventing observers from finding out that a person has sought or received information that has been **blocked** or is illegal in the country where that person is at the time.

POP3

Post Office Protocol version 3 is used to receive mail from a server, by default on port 110 with an e-mail program such as Outlook Express or Thunderbird.

port

A hardware port on a computer is a physical connector for a specific purpose, using a particular hardware **protocol**. Examples are a VGA display port or a USB connector.

Software ports also connect computers and other devices over networks using various protocols, but they exist in software only as numbers. Ports are somewhat like numbered doors into different rooms, each for a special service on a server or PC. They are identified by numbers from 0 to 65535.

protocol

A formal definition of a method of communication, and the form of data to be transmitted to accomplish it. Also, the purpose of such a method of communication. For example, Internet Protocol (IP) for transmitting data **packets** on the Internet, or Hypertext Transfer Protocol for interactions on the World Wide Web.

proxy server

A proxy server is a server, a computer system or an application program which acts as a **gateway** between a client and a Web server. A client connects to the proxy server to request a Web page from a different server. Then the proxy server accesses the resource by connecting to the specified server, and returns the information to the requesting site. Proxy servers can serve many different purposes, including restricting Web access or helping users route around obstacles.

Psiphon node

A Psiphon node is a secured **web proxy** designed to evade Internet censorship. It is developed by Psiphon inc. Psiphon nodes can be open or private.

private node

A private node is a **Psiphon node** working with authentication, which means that you have to register before you can use it. Once registered, you will be able to send invitations to your friends and relatives to use this specific node.

See also **Psiphon node**.

publicly routable IP address

Publicly routable IP addresses (sometimes called public IP addresses) are those reachable in the normal way on the Internet, through a chain of **routers**. Some IP addresses are private, such as the 192.168.x.x block, and many are unassigned.

regular expression

A regular expression (also called a regexp or RE) is a text pattern that specifies a set of text strings in a particular regular expression implementation such as the UNIX grep utility. A text string "matches" a regular expression if the string conforms to the pattern, as defined by the regular expression syntax. In each RE syntax, some characters have special meanings, to allow one pattern to match multiple other strings. For example, the regular expression `lo+se` matches `lose`, `loose`, and `looose`.

remailer

An anonymous remailer is a service which allows users to send **e-mails** anonymously. The remailer receives messages via e-mail and forwards them to their intended recipient after removing information that would identify the original sender. Some also provide an anonymous return address that can be used to reply to the original sender without disclosing her identity. Well-known Remailer services include Cypherpunk, Mixmaster and Nym.

router

A router is a computer that determines the route for forwarding **packets**. It uses address information in the packet header and cached information on the server to match address numbers with hardware connections.

root name server

A root name server or root server is any of thirteen server clusters run by **IANA** to direct traffic to all of the **TLD**s, as the core of the **DNS** system.

RSS (Real Simple Syndication)

RSS is a method and protocol for allowing Internet users to subscribe to content from a Web page, and receive updates as soon as they are posted.

scheme

On the Web, a scheme is a mapping from a name to a **protocol**. Thus the HTTP scheme maps **URL**s that begin with HTTP: to the Hypertext Transfer Protocol. The protocol determines the interpretation of the rest of the URL, so that http://www.example.com/dir/content.html identifies a Web site and a specific file in a specific directory, and mailto:user@somewhere.com is an **e-mail** address of a specific person or group at a specific **domain**.

shell

A UNIX **shell** is the traditional **command line** user interface for the UNIX/Linux operating systems. The most common shells are sh and **bash**.

SOCKS

A **SOCKS** proxy is a special kind of **proxy server**. In the ISO/OSI model it operates between the application layer and the transport layer. The standard **port** for SOCKS proxies is 1080, but they can also run on different ports. Many programs support a connection through a SOCKS proxy. If not you can install a SOCKS client like FreeCap, ProxyCap or SocksCap which can force programs to run through the Socks proxy using dynamic port forwarding. It is also possible to use **SSH** tools such as OpenSSH as a SOCKS proxy server.

screenlogger

A screenlogger is software able to record everything your computer displays on the screen. The main feature of a screenlogger is to capture the screen and log it into files to view at any time in the future. Screen loggers can be used as powerful **monitoring** tool. You should be aware of any screen logger running on any computer you are using, anytime.

script

A script is a program, usually written in an interpreted, non-compiled language such as JavaScript, Java, or a command interpreter language such as bash. Many Web pages include scripts to manage user interaction with a Web page, so that the server does not have to send a new page for each change.

smartphone

A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary feature phone, such as Web access, ability to run elaborated operating systems and run built-in applications.

spam

Spam is messages that overwhelm a communications channel used by people, most notably commercial advertising sent to large numbers of individuals or discussion groups. Most spam advertises products or services that are illegal in one or more ways, almost always including fraud. Content **filtering** of **e-mail** to **block** spam, with the permission of the recipient, is almost universally approved of.

SSH (Secure Shell)

SSH or Secure Shell is a network protocol that allows **encrypted** communication between computers. It was invented as a successor of the unencrypted Telnet **protocol** and is also used to access a **shell** on a remote server.

The standard SSH **port** is 22. It can be used to bypass Internet censorship with port forwarding or it can be used to **tunnel** other programs like VNC.

SSL (Secure Sockets Layer)

SSL (or Secure Sockets Layer), is one of several cryptographic standards used to make Internet transactions secure. It is was used as the basis for the creation of the related Transport Layer Security (**TLS**). You can easily see if you are using **SSL**/TLS by looking at the **URL** in your Browser (like Firefox or Internet Explorer): If it starts with https instead of http, your connection is **encrypted**.

steganography

Steganography, from the Greek for *hidden writing*, refers to a variety of methods of sending hidden messages where not only the content of the message is hidden but the very fact that something covert is being sent is also concealed. Usually this is done by concealing something within something else, like a picture or a text about something innocent or completely unrelated. Unlike cryptography, where it is clear that a secret message is being transmitted, steganography does not attract attention to the fact that someone is trying to conceal or **encrypt** a message.

subdomain

A subdomain is part of a larger **domain**. If for example "wikipedia.org" is the domain for the Wikipedia, "en.wikipedia.org" is the subdomain for the English version of the Wikipedia.

threat analysis

A security threat analysis is properly a detailed, formal study of all known ways of attacking the security of servers or **protocols**, or of methods for using them for a particular purpose such as **circumvention**. Threats can be technical, such as code-breaking or exploiting software bugs, or social, such as stealing passwords or bribing someone who has special knowledge. Few companies or individuals have the knowledge and skill to do a comprehensive threat analysis, but everybody involved in circumvention has to make some estimate of the issues.

Top-Level Domain (TLD)

In Internet names, the TLD is the last component of the **domain** name. There are several generic TLDs, most notably .com, .org, .edu, .net, .gov, .mil, .int, and one two-letter country code (**ccTLD**) for each country in the system, such as .ca for Canada. The European Union also has the two-letter code .eu.

TLS (Transport Layer Security)

TLS or Transport Layer Security is a cryptographic standard based on **SSL**, used to make Internet transactions secure.

TCP/IP (Transmission Control Protocol over Internet Protocol)

TCP and IP are the fundamental **protocols** of the Internet, handling **packet** transmission and routing. There are a few alternative protocols that are used at this level of Internet structure, such as **UDP**.

Tor bridge

A bridge is a middleman Tor **node** that is not listed in the main public Tor directory, and so is possibly useful in countries where the public relays are **blocked**. Unlike the case of **exit nodes**, IP addresses of bridge nodes never appear in server log files and never pass through monitoring nodes in a way that can be connected with **circumvention**.

traffic analysis

Traffic analysis is statistical analysis of **encrypted** communications. In some circumstances traffic analysis can reveal information about the people communicating and the information being communicated.

tunnel

A tunnel is an alternate route from one computer to another, usually including a **protocol** that specifies **encryption** of messages.

UDP (User Datagram Packet)

UDP is an alternate **protocol** used with IP. Most Internet services can be accessed using either **TCP** or UDP, but there are some that are defined to use only one of these alternatives. UDP is especially useful for real-time multimedia applications like Internet phone calls (**VoIP**).

URL (Uniform Resource Locator)

The URL (Uniform Resource Locator) is the address of a Web site. For example, the URL for the World News section of the NYTimes is http://www.nytimes.com/pages/world/index.html. Many censoring systems can **block** a single URL. Sometimes an easy way to bypass the block is to obscure the URL. It is for example possible to add a dot after the site name, so the URL http://en.cship.org/wiki/URL becomes http://en.cship.org./wiki/URL. If you are lucky with this little trick you can access blocked Web sites.

Usenet

Usenet is a more than 20-year-old discussion forum system accessed using the NNTP **protocol**. The messages are not stored on one server but on many servers which distribute their content constantly. Because of that it is impossible to censor Usenet as a whole, however *access* to Usenet can and is often **blocked**, and any particular server is likely to carry only a subset of locally-acceptable Usenet newsgroups. Google archives the entire available history of Usenet messages for searching.

VoIP (Voice over Internet Protocol)

VoIP refers to any of several **protocols** for real-time two-way voice communication on the Internet, which is usually much less expensive than calling over telephone company voice networks. It is not subject to the kinds of wiretapping practiced on telephone networks, but can be monitored using digital technology. Many companies produce software and equipment to **eavesdrop** on VoIP calls; securely **encrypted** VoIP technologies have only recently begun to emerge.

VPN (virtual private network)

A VPN (virtual private network) is a private communication network used by many companies and organizations to connect securely over a public network. Usually on the Internet it is **encrypted** and so nobody except the endpoints of the communication can look at the data traffic. There are various standards like IPSec, **SSL**, **TLS** or PPTP. The use of a VPN provider is a very fast secure and convenient method to bypass Internet censorship with little risks but it generally costs money every month.

whitelist

A whitelist is a list of sites specifically authorized for a particular form of communication. Filtering traffic can be done either by a whitelist (**block** everything but the sites on the list), a **blacklist** (allow everything but the sites on the list), a combination of the two, or by other policies based on specific rules and conditions.

World Wide Web (WWW)

The World Wide Web is the network of hyperlinked **domains** and content pages accessible using the Hypertext Transfer Protocol and its numerous extensions. The World Wide Web is the most famous part of the Internet.

Webmail

Webmail is **e-mail** service through a Web site. The service sends and receives mail messages for users in the usual way, but provides a Web interface for reading and managing messages, as an alternative to running a mail client such as Outlook Express or Thunderbird on the user's computer. For example a popular and free webmail service is https://mail.google.com/

Web proxy

A Web proxy is a script running on a Web server which acts as a **proxy**/**gateway**. Users can access such a Web proxy with their normal Web browser (like Firefox) and enter any **URL** in the form located on that Web site. Then the Web proxy program on the server receives that Web content and displays it to the user. This way the **ISP** only sees a connection to the server with the Web proxy since there is no direct connection.

WHOIS

WHOIS (who is) is the aptly named Internet function that allows one to query remote WHOIS databases for **domain** registration information. By performing a simple WHOIS search you can discover when and by whom a domain was registered, contact information, and more.

A WHOIS search can also reveal the name or network mapped to a numerical IP address

评估互联网翻墙工具应考虑的十大问题

*罗杰• 丁高戴恩，Tor项目负责人 （*译者注：本文翻译转自《中国人权论坛》）

当越来越多国家对使用互联网进行镇压时，世界各地的人们正转而寻找反审查软件，以使他们能够进入被屏蔽的网站。这类软件也被称为翻墙工具，是为了应付对网络自由的威胁才被创造出来的。这些工具拥有不同特点，具有不同程度的安全性能。对用户来说，了解使用这些软件的优缺点十分重要。

本文提出十个在你评估一种翻墙工具时应该考虑的问题。我们的目的并不是为了推崇某一种软件，而是为了告诉你在不同情况下什么样的工具更有用。提出这些问题的顺序先后主要根据叙述的需要；所以，并不是首先提到的问题就是最重要的。

用於互联网的翻墙软件，包含两个组件：中继组件和发现组件。中继组件建立与主机或代理服务器的联系，进行加密处理和传输数据；发现组件要做的则是在此之前的步骤–寻找一个或多个可访问地址的过程。

有些工具只有一个简单的中继组件。比如，假定你正在使用一个开放代理服务器，使用过程是很直接的：设置你的网络浏览器或其他软件，以使用代理服务器。对使用开放代理服务器的人来说一个较大的挑战是找到一个可靠、快速的开放代理服务器。另外，有些工具有非常复杂的中继组件，由多个代理服务器、多层加密组成，等等。

首先要告知的是：我是Tor第二代「洋葱路由」软件的发明人和开发者。Tor主要用於保护隐私和翻墙。虽然根据我所选择的问题在这里显示了我对像 Tor这样的更安全的工具的偏爱（即我提出的问题突显了Tor的优点；而这些问题是其他的工具开发者可能并不在意的），但我也试图将其他软件开发者认为重要的问题包括在内。

一、用户多元化

当你评判一个翻墙工具时你会问的一个最简单问题就是：还有谁在用它？使用者的多元性意味着如果有人发现你正使用这一软件，他们将无法确定你用它的原因。安装了一个像Tor这样的保护隐私的工具––在全世界有许多不同阶层的使用者（从普通民众和人权活跃人士，到企业、执法部门和军方）––这个事实并不会让别人获得更多有关你是谁或你可能会访问哪些网站的信息。另一方面，设想一下一组伊朗博客使用只为他们设计的翻墙工具，那么当任何人发现他们中有人使用这一软件时，就很容易猜出使用它的目的。

除了技术上的特点，也就是使某种工具在一个国家对一些人很有用，或对世界上所有人都有用之外，市场营销扮演着一个重要角色。许多工具是通过口耳相传普及的，如果第一批用户在越南，他们发现这个工具好用，那么下一批用户很可能仍在越南。一种工具被翻译成某种语言或没有被翻译成某种语言，也会对其可能吸引的用户起引导或阻碍作用。

二、本地适用

下一个需要考虑的问题是这一工具是否人为地限制了在哪些国家可以使用它。几年来，商业性网站Anonymizer.com在伊朗一直是免费使用的。所以该网站准予连接的要么是付费的消费者（大部分在美国），要么是在伊朗的为了规避政府审查的使用者。

最近的例子是Your Freedom只允许像缅甸这样一小部分国家免费使用，像「自由门」和「无界浏览」这样的系统也只在少数他们愿意提供服务的国家（中国，无界浏览则在伊朗）提供免费连接，在其他国家则完全不行。一方面从宽带成本的角度考虑，这一策略是有道理的；但另一方面，如果你在沙特阿拉伯，需要翻墙工具，一些有用的工具可能就不在你可选择的範围之内。

三、可持续性网络和软件开发

如果你准备花时间弄清楚怎样使用某种工具，你想确定的是这种工具是不是会存在一段时间。这里有三种可以确定不同的工具能否长期存在的方法：利用志愿者、能否赢利、从赞助商获得资金。

像Tor这样的网络是依靠志愿者提供中继才形成网络的。全世界数千位有良好网络连接的志愿者，他们想帮助世界变得更美好。通过把他们连接成一个巨大的网络，Tor确保了这个网络独立於编写这软件的公司，因此即便Tor这个项目作为一个实体已经消失，这个网络仍将继续存在。「赛风」（Psiphon）走的是第二条路：收服务费。他们的理由是，如果他们可以使公司赢利，那么公司将有能力在此基础上建立一个网络。第三条路是依靠赞助者来付带宽费。Java 匿名代理（Java Anon Proxy）或是JAP项目依靠政府拨款资助其宽带；现在政府拨款已经停止，他们正在了解收费赢利的办法。「极境网络」（Ultrareach）和「自由门」（Freegate）采用的「赞助者」模式效果不错，不过他们一直在寻找更多赞助者以使他们的网络可以继续操作下去。

在解答了一个网络怎样才能长期生存下去的问题之后，接下来的问题就是软件本身的可持续性。上面说到的三种方法同样适用於此，但是例子不同。虽然Tor的网络是由志愿者来操作的，但是Tor作为软件本身靠的是赞助者（政府和非政府组织）来资助软件的新功能和软件的维护。而「极境网络」和「自由门」，在软件更新方面的可持续性更强：他们在世界各地有一支团队，大部分是志愿者，确保他们的工具永远比政府的审查走前一步。

这三种方法各有优点，但是加深理解某种工具采用的方法，可以帮助你预测未来你可能会碰到什么样的问题。

四、开放式设计

要做到工具软件及其设计透明并有可复用性，首先必须根据开源许可（不仅是客户方面的软件，而且还有服务器方面的软件）来发布软件。开源许可，即使用者可对软件进行检验，看它如何操作，并且有权对应用程式加以修改。虽然并非人人都得益於这样的机会（许多人只想使用工具现有的功能），但实际上有的使用者可以使之更加安全和有用。没有这一选择，你等於被迫相信少数软件开发者已经考虑到并解决了所有可能发生的问题。

仅仅拥有开源许可是不够的。可靠的翻墙工具需要提供其他安全专家可资使用的清楚完整的文件——不仅有关其如何设计，而且有关其特点，以及开发者所要实现的目标。他们准备提供隐私保护吗？他们准备应对攻击性的审查吗？他们准备抵抗什么样的攻击？为什么他们的工具能够抵抗这样的攻击？如果看不到源代码和了解开发者的目的，就很难决定这一工具是否存在安全问题，或是很难评估其能否达到其目标。

在密码学领域里，科克豪福斯（Kerckhoffs）原则要检验的是你所设计的系统应该使你要保密的範围尽可能小和容易理解。这就是为什么在加密算法中有密钥（其秘密部分），而其馀部分则可对任何人公开解释。历史上，任何加密设计如果其中的秘密部分过多，最后的结果一定比设计者设想的更不安全。相似情况也适用於翻墙工具的秘密设计，唯一能对该软件进行检验的人是该软件的开发者和伤害它的攻击者，其他有助於使它更好更可持续的开发者和使用者却都被排除在外了。

设计某一项目的想法可以被重复使用从而超出这一项目本身的寿命。有太多的翻墙工具对自己的设计加以保密，希望政府审查时难以发现其系统如何运作，但这样做的结果是各种项目之间无法相互学习，翻墙工具的发展领域作为一个整体进展缓慢。

五、分布式结构

对翻墙工具另一个需要了解的特点是它的网络是集中式的还是分布式的。集中式的工具将其使用者的发出的所有要求通过一个或几个工具操作者控制的主机来回答。而一个分布式的设计，如Tor或JAP，则通过多个不同地点传输数据。因此，就不存在可以看到每个使用者正进入哪个网站的单一地点或统一体。

另一观察这种区别的角度基於你的信任是集中式的还是分布式的。如果你将所有信任全部放在一个实体上，那么你能期望的最好情况就是「以政策保护隐私」——即，他们虽然拥有你的所有数据，但他们保证不去看，也不会丢失或转卖你的数据。另一个方式就是安大略保护隐私委员会所呼吁的「以设计保护隐私」——即系统设计本身确保使用者的隐私得到保护。这种设计的开放性让每个人评估设计所提供的对隐私的保护程度。

这一关切并非仅为假设。2009年初，伯克曼中心的哈尔•罗伯兹在一个翻墙工具网站的常见问答中发现这一工具在推销其用户「点击记录」（clicklogs）。后来，我跟另一翻墙工具提供商聊天，他说，他们拥有所有对其系统提出的使用要求记录，「因为你永远不知道什么时候你可能会需要他们。」

我在这里隐去了这些工具的名称，因为重要的不是这些工具提供商可能使用了用户的资料，而是任何以集中化信任架构为基础建立起来的工具都能够使用其用户的资料，而这是用户无法知道的事情。糟糕的是，即使工具提供商并无恶意，但实际上所有数据通过一个地方，便使这个地方成了攻击者前来窥探的具吸引力的目标。

许多这类工具把翻墙与保护用户隐私看作完全互不相连的两个目的。这种分离并不一定是坏事，只要你知道你正处於怎样的境况。比如，在对信息进行审查的国家中，我们从许多人那里听说，仅仅到一个新闻网上阅读并不会被盯上。但是，正如我们在过去几年里从各方面所了解到的，巨大的个人信息数据库最终往往比我们希望的更公开。

六、上网安全

隐私问题不仅仅涉及你使用的工具是否能记录你的使用请求，而且还涉及你访问的网站会不会认识或跟踪你。还记得雅虎交出其一位中国客户信息的事吗？如果一个博客聚合要找出谁正在某个博客上贴文、谁贴了最新评论，或某一位博客到其它网站阅读了什么，那将会怎么样？使用安全的工具上网意味着网站没有多少信息可以交出去。

一些翻墙工具比另一些更安全，其根本原因在於代理服务器。代理服务器常常将客户地址跟着他们的网络使用请求一起发送出去，因此网站很容易确切地了解使用请求是从哪里来的。从另一个角度来讲，像Tor这样的工具使用客户端浏览器延伸来隐藏你的浏览器版本、语言偏好、浏览器视窗尺寸、时区等等，来隔离你的「小甜点」（Cookies）、过往历史和缓冲，从而可以预防像「快闪」（Flash）这样的插件洩漏你的信息。

但是使用应用程序级的保护是有代价的：一些网站不能正确工作。当更多网站发展到最新「互联网2.0」版本时，这些网站要求浏览器的功能有更大的入侵性。如果要达到最安全的目的，就要解除那些会带来危险的功能。但如果某人在土耳其试图登录YouTube，而Tor为了安全，关闭了他的插件（Flash），那么他的视频就工作不了了。

没有哪个工具可以既安全又好用。赛风（Psiphon）在它的集中化代理服务器上手工评估每个网站和应用程式，改写每一篇网页。他们的改写主要并不是为了保护隐私而是为了确保网页上的所有连接能被导回其代理服务器，但结果是，如果他们没有查到你的目标网站，它可能就不能帮助你了。比如，因为 Facebook首页一直不断变化，赛风为了跟上它也必须跟着不断变化。Tor目前将一些内容关闭了，这些内容也许在实践中是安全的，之所以这样做是因为我们还没有设计出一个好的界面，可以让用户在充分掌握信息的情况下做出决定。其它工具则还是让任何内容通过，他们不太在乎客户被暴露。

七、不承诺能为整个互联网加密

我应该在加密和隐私之间做一区分。大部分翻墙工具将用户与翻墙工具提供商之间的网络数据加密，但像代理服务器这样非常简单的服务器则不加密。翻墙工具需要加密以规避像中国的防火墙这样的审查机制设置的关键字过滤。但是，如果目标网站不支持加密的话，没有一种工具可以对工具提供商和目标网站之间的网络数据加密。因此，不存在一种神奇的办法可以为网络数据加密。

对每个人来说，理想的答案是使用安全超文本传输协议（HTTPS）上网；对每个网站来说，最好都支持安全超文本传输协议的连接。只要你正确使用，安全超文本传输协议会在你的浏览器和网站间提供加密。这种终端对终端的加密意味着网络上无人（并非指你的互联网服务供应商，互联网主干供应商和翻墙工具提供商）能获得你的通讯内容。但是由於种种原因，扩大加密还没有被完全接受。如果你的目标网站不支持加密，那么最好的办法是：第一，不要发送可辨识或敏感的信息，如在博客帖子上署真名，或你不希望别人知道的密码；第二，使用无任何信任瓶颈的翻墙工具。所谓有信任瓶颈的翻墙工具就是，尽管在你已经做到了第一点的情况下，还是会让别人将你和你造访的目标网站联系在一起的工具。

另外，当你必须传送敏感信息时安全问题就变得更为复杂。有人对Tor使用志愿者操作的这种网络设计表示关切，理由是如果使用集中式设计你至少知道谁在操作基础设施。但实际上不管采取哪种方式都是陌生人在读你的数据，不同点不过是陌生的志愿者还是陌生的专注於你的人。前者不知道你是谁（他们不会以你为目标），后者的目的就是要获得你的全部流量资料（及你与它的关系）。任何人承诺绝对安全其实都是在花言巧语地推销东西。

八、快

对於一个翻墙工具下一个你要注意的问题是速度。有些工具总是很快，有些则总是很慢，有些完全无法预测其表现。速度受制於很多因素，包括该系统有多少人使用、用户在做什么、有多大的电脑资源，以及负荷是否均匀地分布在网络上。

「集中化信任设计」有两个优点。第一，他们能看到所有用户以及他们正在做什么，即，他们可以事先将资源均匀分布，并可减少增加系统负担的行为。第二，在需要的时侯可以购买更多电脑资源。因此，他们付出越多他们的工具速度就越快。而分布式信任设计就不那么容易跟踪他们的用户。如果他们依靠志愿者提供的资源，那么，相对於集中式付更多宽带费可使速度加快，分布式使用志愿者越多其过程就越复杂速度也就越慢。

工具的性能问题的另一面是灵活性问题。许多系统通过限制其用户功能来确保速度。虽然「赛风」（Psiphon）限制用户造访他们还未经手工检查的网站，但「极境网络」（Ultrareach）和「自由门」（Freegate）实际上已主动对允许用户造访的网站设限。这样他们才能控制他们的宽带费用。相比之下，Tor能够让用户进入任何协议（protocol）和目标网站，即，比如，你也可以发送即时信息；但缺点是网络常常因用户的批量传输而不胜负荷。

九、软件和更新易获得

当某种翻墙工具一出名，其网站就会被屏蔽。如果无从获得这一工具，工具再好又有何用。在这里最好的解决办法是不要使用任何专门的客户软件。这样就不必从工具网站上下载软件。比如「赛风」，只靠一般的浏览器，就不在乎网站可能被封，因为使用者不需要下载软件。另一种办法是使用微型应用程式，如「极境网络」或「自由门」，你可以用实时消息的方式将链接传送给朋友。Tor的浏览器套件也是一个选择：套件包括所有已经配置好的所需要的软件。但是，由於它包含了大型应用程式，如火狐（Firefox），因此不容易在网上传递。而通过社会网络、闪存硬盘，或使用电子邮件自动应答系统，则可得以分发。电子邮件自动应答允许你通过谷歌的G-mail来下载Tor。

然后，你需要考虑每一种方法的特点。首先，什么样的操作系统是它可支持的？「赛风」不需要任何额外的客户软件就可以很好工作；「极境网络」和「自由门」都很特别，只能在微软视窗环境中工作；Tor及其软件基本上可以在任何环境中操作。其次，要考虑客户软件可自动处理从一个代理服务器转到另一个的失效备援，所以，如果你目前的地址消失了或被封了，你不必用手工记下新的地址。

最后，你使用的工具是否有跟踪记录功能来对付屏蔽？比如「无界浏览」和「自由门」都曾有当现有版本的工具停止工作时立刻发布更新版本的历史。他们在这种「猫捉老鼠」的游戏中积累了丰富的经验，因此，有理由相信他们已经为下一轮变故做好了准备。在Tor这方面，也已经为最终可能被屏蔽做好了准备，那就是将其网络通信更精简，看上去更像加密的网页浏览， 并介绍了还未出版的网桥中继（bridge relays）。对黑客来说网桥中继比公共中继（public relays）更难被发现和被屏蔽。Tor试图将软件更新跟代理服务器地址更新这两者区别开——如果你使用的网桥中继被屏蔽了，你可以继续使用同一个软件，只要改变一下配置以使用新的网桥地址。我们的网桥设计2009年9月在中国进行了测试，数万用户顺畅地从使用公共中继转移到使用网桥中继。

十、不把自己作为翻墙工具推销

许多翻墙工具通过大量媒体高调推出。媒体当然喜欢这样的做法，他们常常以《美国黑客对中国宣战！》为首页通栏标题。但这种亮相虽有助於吸引支持（志愿者、利润、赞助商），但大肆宣传也吸引了审查者的注意。审查机构通常屏蔽两类翻墙工具：一类是好用的工具，即拥有数十万用户的工具；一类是名气很响的工具。一般来说，审查制度屏蔽所有敏感内容的情况很少，更多的情况是制造一种打压的气氛，从而使人们进行自我约束。媒体上的文章对当局的控制能力造成威胁，他们被迫做出回应。

这里要表明的是我们能够控制武器竞赛的速度。尽管某种工具拥有许多用户，但只要无人谈论它，一般来说就不会被屏蔽。但是如果无人谈论它，用户又从何知道它？走出这一悖论的方法之一是通过口耳相传和社会网络，而不是通过传统的媒体宣传来传播。另一方法是将工具置於一个不同的背景中——比如，我们主要将 Tor展现为一个保护隐私和公民自由的工具，而不是翻墙工具。但是，一个工具在名声日益增长时要维持这种平衡是很难的。

结语

本文解释了一些你在评估翻墙工具的优缺点时应该考虑的问题。我故意没有将不同的工具做成图表及在不同的分类中对他们进行评分。毫无疑问，有人最终会这样做，并概括出每种工具被打上多少个钩。但是现在的问题并不是要找出「最佳」工具。各种各样的翻墙工具被广泛使用，增加了所有这类工具的力量，因为审查者必须同时去对付每一个策略。

最后，我们应该记住，技术不能解决所有的问题。防火墙毕竟在许多国家都成功地发挥了作用。只要在审查制度下仍有很多人说「我很高兴政府使我感到互联网是安全的」，那么就说明社会方面的挑战至少还是非常严重的。但与此同时，在所有这些国家仍然有人希望通过互联网学习和传播信息，那么一个强大的技术解决方案就仍是至关紧要的一环。

Roger Dingledine is project leader for The Tor Project, a US non-profit working on anonymity research and development for such diverse organizations as the US Navy, the Electronic Frontier Foundation, and Voice of America. In addition to all the hats he wears for Tor, Roger organizes academic conferences on anonymity, speaks at a wide variety of industry and hacker conferences, and also does tutorials on anonymity for national and foreign law enforcement.

更多资源

绕过网络审查是一个广博的话题，有很多可用的工具和服务。如果你想你的绕行行为更加难以被发现或者将来被封锁，如果你想你的网络使用实现匿名，或者如果你想帮助他人绕过审查，你也有许多的事情需要考虑。下面是一些推荐的资源供进一步学习相关事项。（这些资源的一部分在一些地方可能已经不可使用或者已被封锁）

手册和指南

绕过网络审查

- Reporters Without Borders, *Handbook for Bloggers and Cyber-Dissidents,* http://www.rsf.org/article.php3?id_article=26187
- The Internet Censorship Wiki, http://en.cship.org/wiki/

给活动家的计算机安全建议

- NGO-in-a-Box, a collection of free portable applications, https://security.ngoinabox.org
- Digital Security and Privacy for Human Rights Defenders, https://www.frontlinedefenders.org/esecman
- Surveillance Self-Defense International, https://www.eff.org/wp/surveillance-self-defense-international

对网络审查的研究

- Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008), ISBN 0-262-54196-3 http://www.opennet.net/accessdenied/
- Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), ISBN 0-262-51435-4 http://www.access-controlled.net
- Hal Roberts, Ethan Zuckerman, Jillian York, Rob Faris, John Palfrey, *2010 Circumvention Tool Usage Report* (Berkman Center for Internet & Society) http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage
- More resources on Internet censorship: http://bailiwick.lib.uiowa.edu/journalism/mediaLaw/cyber_censors.html

从事记录，斗争或绕开网络限制的组织

- Citizen Lab (http://www.citizenlab.org)
- Committee to Protect Bloggers (http://www.committeetoprotectbloggers.org)
- Committee to Project Journalists (https://www.cpj.org)
- Berkman Center for Internet and Society (http://cyber.law.harvard.edu)
- Electronic Frontier Foundation (https://www.eff.org)
- FrontLine (https://www.frontlinedefenders.org)
- Global Internet Freedom Consortium (http://www.internetfreedom.org)
- The Herdict (https://www.herdict.org/web)
- OpenNet Initiative (http://opennet.net)
- Peacefire (http://www.peacefire.org)
- Reporters Sans Frontières/Reporters Without Borders (http://www.rsf.org)
- Sesawe (https://sesawe.net)
- Tactical Tech Collective (https://www.tacticaltech.org)

公开的网页代理和应用程序代理

- Proxy.org, a list of thousands of open Web Proxies: http://www.proxy.org
- Peacefire, a mailing list which sends out new web proxies: http://www.peacefire.org/circumventor/,
- Application proxies:
    - http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists/
    - http://www.publicproxyservers.com

绕行解决方案和服务提供商

- Access Flickr!: https://addons.mozilla.org/en-US/firefox/addon/4286
- Alkasir: https://www.alkasir.com/
- CECID: http://cecid.labyrinthdata.net.au/
- Circumventor CGIProxy: http://peacefire.org/circumventor/
- Codeen: http://codeen.cs.princeton.edu/
- Coral: http://www.coralcdn.org/
- CProxy: http://www.cproxy.com/
- Dynaweb FreeGate: http://www.dit-inc.us/freegate
- FirePhoenix: http://firephoenix.edoors.com/
- FoxyProxy: http://foxyproxy.mozdev.org/
- Glype: http://www.glype.com/
- GPass: http://gpass1.com/gpass/
- GProxy: http://gpass1.com/gproxy.php
- Gtunnel: http://gardennetworks.org/products
- Guardster: http://www.guardster.com/
- Hamachi LogMeIn: https://secure.logmein.com/products/hamachi/vpn.asp
- hopster: http://www.hopster.com/
- HotSpotVPN: http://hotspotvpn.com/
- HTTPS Everywhere: https://www.eff.org/https-everywhere
- httpTunnel: http://www.http-tunnel.com/
- JAP / JonDo: http://www.jondos.de/en
- Megaproxy: http://www.megaproxy.com/
- OpenVPN: http://www.openvpn.net/
- PHProxy: http://sourceforge.net/projects/poxy/
- Picidae: http://www.picidae.net/
- Proxify: http://proxify.com/
- psiphon: http://www.psiphon.ca/
- PublicVPN: http://www.publicvpn.com/
- SabzProxy: http://www.sabzproxy.com/
- Simurgh: https://simurghesabz.net/
- SmartHide: http://www.smarthide.com/
- Tor: https://www.torproject.org/
- TrafficCompressor: http://www.tcompressor.ru/
- UltraReach UltraSurf: http://www.ultrareach.com/
- Your-Freedom: http://www.your-freedom.net/

商业VPN提供商列表

- http://en.cship.org/wiki/VPN

Socksification软件 (让非代理软件使用SOCKS代理)

- tsocks: http://tsocks.sourceforge.net/
- WideCap: http://www.widecap.com/
- ProxyCap: http://www.proxycap.com/
- FreeCap: http://www.freecap.ru/eng/
- Proxifier: http://www.proxifier.com/
- SocksCap: http://soft.softoogle.com/ap/sockscap-download-5157.shtml

License

Authors

INTRODUCTION

Modifications:
gravy - A Ravi Oli 2011
Mokurai - Edward Mokurai Cherlin 2011
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
poser - Poser 2011
lalala - laleh 2011

ABOUT THIS MANUAL

Modifications:
Zorrino - Zorrino Hermanos 2011
booki - adam or aco 2011

QUICKSTART

Modifications:
booki - adam or aco 2011
erinn - Erinn Clark 2011
puffin - Karen Reilly 2011
freerk - Freerk Ohling 2011
Zorrino - Zorrino Hermanos 2011
helen - helen varley jamieson 2011
poser - Poser 2011
schoen - Seth Schoen 2011

HOW THE NET WORKS

Modifications:
booki - adam or aco 2011
gravy - A Ravi Oli 2011
lalala - laleh 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

CENSORSHIP AND THE NET

Modifications:
gravy - A Ravi Oli 2011
booki - adam or aco 2011
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

CIRCUMVENTION AND SAFETY

Modifications:
gravy - A Ravi Oli 2011
booki - adam or aco 2011
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011

INTRODUCTION

Modifications:
booki - adam or aco 2010

ABOUT THIS MANUAL

Modifications:
booki - adam or aco 2010

SIMPLE TRICKS

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
poser - Poser 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

GET CREATIVE

Modifications:
freerk - Freerk Ohling 2011
DavidElwell - David Elwell 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

WEB PROXIES

Modifications:
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
lalala - laleh 2011
poser - Poser 2011
booki - adam or aco 2011

WHAT IS CIRCUMVENTION

Modifications:
booki - adam or aco 2010

PSIPHON

Modifications:
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
helen - helen varley jamieson 2011
poser - Poser 2011
booki - adam or aco 2011

AM I BEING CENSORED?

Modifications:
booki - adam or aco 2010

DETECTION AND ANONYMITY

Modifications:
booki - adam or aco 2010

SABZPROXY

Modifications:
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

HOW THE NET WORKS

Modifications:
booki - adam or aco 2010

INTRODUCTION TO FIREFOX

Modifications:
SamTennyson - Samuel L. Tennyson 2011
booki - adam or aco 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
freerk - Freerk Ohling 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

WHO CONTROLS THE NET

Modifications:
booki - adam or aco 2010

FILTERING TECHNIQUES

Modifications:
booki - adam or aco 2010

ADBLOCK PLUS AND NOSCRIPT

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
scherezade - Genghis Kahn 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

HTTPS EVERYWHERE

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011

SIMPLE TRICKS

Modifications:
booki - adam or aco 2010

PROXY SETTINGS AND FOXYPROXY

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

USING A WEB PROXY

Modifications:

INTRODUCTION

Modifications:
gravy - A Ravi Oli 2011
freerk - Freerk Ohling 2011
erinn - Erinn Clark 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
poser - Poser 2011

USING PHProxy

Modifications:

FREEGATE

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

USING PSIPHON

Modifications:

USING PSIPHON2

Modifications:

SIMURGH

Modifications:
booki - adam or aco 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
freerk - Freerk Ohling 2011

ULTRASURF

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

USING PSIPHON2 OPEN NODES

Modifications:

VPN SERVICES

Modifications:
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011
lalala - laleh 2011
booki - adam or aco 2011

RISKS

Modifications:

VPN ON UBUNTU

Modifications:
SamTennyson - Samuel L. Tennyson 2011
booki - adam or aco 2011

scherezade - Genghis Kahn 2011
freerk - Freerk Ohling 2011

HOTSPOT SHIELD

Modifications:
booki - adam or aco 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

ADVANCED BACKGROUND

Modifications:

HTTP PROXIES

Modifications:

ALKASIR

Modifications:
booki - adam or aco 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

TOR: THE ONION ROUTER

Modifications:
freerk - Freerk Ohling 2011
erinn - Erinn Clark 2011
puffin - Karen Reilly 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
helen - helen varley jamieson 2011
lalala - laleh 2011

INSTALLING SWITCH PROXY

Modifications:

USING SWITCH PROXY

Modifications:

JONDO

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

YOUR-FREEDOM

Modifications:
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

TOR: THE ONION ROUTER

Modifications:

USING TOR BROWSER BUNDLE

Modifications:

DOMAINS AND DNS

Modifications:
gravy - A Ravi Oli 2011
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

USING TOR IM BROWSER BUNDLE

Modifications:
SahalAnsari - Sahal Ansari 2010

HTTP PROXIES

Modifications:
booki - adam or aco 2011
lalala - laleh 2011
scherezade - Genghis Kahn 2011
helen - helen varley jamieson 2011

USING TOR WITH BRIDGES

Modifications:

THE COMMAND LINE

Modifications:
booki - adam or aco 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

USING JON DO

Modifications:

OPENVPN

Modifications:
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

SSH TUNNELLING

Modifications:
freerk - Freerk Ohling 2011
booki - adam or aco 2011

WHAT IS VPN?

Modifications:

OPENVPN

Modifications:

SOCKS PROXIES

Modifications:
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011

lalala - laleh 2011
booki - adam or aco 2011

SSH TUNNELLING

Modifications:

RESEARCHING AND DOCUMENTING CENSORSHIP

Modifications:
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

SOCKS PROXIES

Modifications:

DEALING WITH PORT BLOCKING

Modifications:
booki - adam or aco 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

INSTALLING WEB PROXIES

Modifications:
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

INSTALLING WEB PROXIES

Modifications:

SETTING UP A TOR RELAY

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

INSTALLING PHProxy

Modifications:

RISKS OF OPERATING A PROXY

Modifications:
freerk - Freerk Ohling 2011
schoen - Seth Schoen 2011

INSTALLING PSIPHON

Modifications:

SETTING UP A TOR RELAY

Modifications:

BEST PRACTICES FOR WEBMASTERS

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011

schoen - Seth Schoen 2011

RISKS OF OPERATING A PROXY

Modifications:

GLOSSARY

Modifications:
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Mokurai - Edward Mokurai Cherlin 2011

TEN THINGS

Modifications:
Zorrino - Zorrino Hermanos 2011
booki - adam or aco 2011
puffin - Karen Reilly 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

FURTHER RESOURCES

Modifications:

FURTHER RESOURCES

Modifications:
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

GLOSSARY

Modifications:

CREDITS

Modifications:
booki - adam or aco 2011

CREDITS

Modifications:

The below is information for pre-2011 content

Authors

ABOUT THIS MANUAL
© adam hyde 2008
Modifications:
Austin Martin 2009
Edward Cherlin 2008
Janet Swisher 2008
Tom Boyle 2008
Zorrino Zorrinno 2009

ADVANCED BACKGROUND
© Steven Murdoch And Ross Anderson 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008

Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

DETECTION AND ANONYMITY
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

RISKS
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Austin Martin 2009
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

SOCKS PROXIES
© Seth Schoen 2008
Modifications:
adam hyde 2008
Freerk Ohling 2008, 2009
Tom Boyle 2008

USING SWITCH PROXY
© adam hyde 2008, 2009
Modifications:
Alice Miller 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

CREDITS
© adam hyde 2006, 2007, 2008
Modifications:
Edward Cherlin 2008

FILTERING TECHNIQUES
© Edward Cherlin 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Janet Swisher 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

FURTHER RESOURCES
© adam hyde 2008
Modifications:
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Zorrino Zorrinno 2008, 2009

GLOSSARY
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

AM I BEING CENSORED?
© adam hyde 2008
Modifications:
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

HOW THE NET WORKS
© Frontline Defenders 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

INSTALLING WEB PROXIES
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

INSTALLING PHProxy
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

INSTALLING PSIPHON
© Freek Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

INSTALLING SWITCH PROXY
© adam hyde 2008
Modifications:
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

INTRODUCTION
© Alice Miller 2006, 2008
Modifications:
adam hyde 2008, 2009
Ariel Viera 2009
Austin Martin 2009
Edward Cherlin 2008
Janet Swisher 2008
Seth Schoen 2008
Tom Boyle 2008

RISKS OF OPERATING A PROXY
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Tom Boyle 2008

SSH TUNNELLING
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008, 2009
Sam Tennyson 2008
TWikiGuest 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

SETTING UP A TOR RELAY
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

SIMPLE TRICKS
© Ronald Deibert 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

TOR: THE ONION ROUTER
© Zorrino Zorrinno 2008
Modifications:

adam hyde 2008
Alice Miller 2008
Ben Weissmann 2009
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING TOR WITH BRIDGES
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING JON DO
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

OPENVPN
© Tomas Krag 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008

USING PHProxy
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

USING PSIPHON
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Austin Martin 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

USING PSIPHON2
© Freerk Ohling 2009
Modifications:
adam hyde 2010
Austin Martin 2009
Zorrino Zorrinno 2009

USING PSIPHON2 OPEN NODES

USING TOR BROWSER BUNDLE

USING TOR IM BROWSER BUNDLE

HTTP PROXIES

USING A WEB PROXY

WHAT IS CIRCUMVENTION

WHAT IS VPN?

Free manuals for free software

General Public License

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> **b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete

machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Made with Booki

Visit http://software.booki.cc