绕道

Nart Villeneuve 作

最后更新时间:5, 16, 2005

网络内容过滤.....7
网页绕道技术.....8
考量需求与能力.....8
网上数据库绕道.....9
公共网上数据库绕道服务.....10
网上数据库绕道软件.....10
网上数据库绕道的安全顾虑.....11
代理服务器.....12
代理服务器软件.....13
公用代理服务器.....13
定址开放代理服务器.....13
开放代理服务器：特殊连接埠.....14
代理服务器的安全顾虑.....14
加密信道.....14
匿名通讯系统.....15
结语.....16

网络内容过滤

网络内容过滤技术即是对可接收网络内容的控制。虽然此方式曾被用在个人层级—让父母限制孩子访问不适宜的网站—现在过滤、封锁技术已被广泛运用于各单位与国家层级：许多机关单位，包括学校、图书馆、公司社团都开始运用此技术，国家层级机关亦渐如此。某些特别的网站被完全封锁，无人能进入，且极少对此行为负责。

网站内容过滤主要是封锁上黑名单的网站，又往往与关键词封锁合并施行。在过滤软件中输入某些主题清单与网页地址加以封锁，软件可只过滤特定主题、种类。当网民想进入某网页时，过滤软件就会自行对照输入数据库的清单并封锁上了名单的网站。若再配合上关键词过滤，过滤软件还会检查每一网页〔其讨论主题、网页地址及内容〕并自动封锁出现敏感字眼的网页传输。

有两种过滤网页方法：最高标准封锁与最低线封锁。网页过滤不只是常封错网站，而且它无法全面封锁所有的访问路径。但主要是封锁列入禁止名单上的网站，尽管有许多开放〔主要针对色情网站〕、商业网站及国家及网站是保密的。商业类别名单及网站地址是专属于制造商的智能财，而非共享资源。尽管有些网页过滤软件制造商有线上网站查询可供一般人使用，但封锁名单总是列为机密，无法监看与分析

在一些国家会在商业网站的过滤软件上附加想封锁的网站。封锁的网站通常包括政治反对党、新闻媒体、人权组织、国际新闻组织和批评政府的言论。大多数国家针对的是以本国语言书写的网页内容，但如对英文网站及公众交流讨论网站的封锁，如：网上日志及论坛，也日益增多。

网页绕道技术

许多不同方式的网络绕道技术即是为突破国家控管下的网络过滤及内容限制，让网民能跨越封锁系统。不同的战略研发出让个人或私人团体网站确保自身安全并反制或避过网络监控、检查。这类工具称为「网页绕道技术」 大致而言，网页绕道技术是指：依循在一网络被封锁的国家之使用者指令选择路径，以未被封锁的中介代为传输网页以避过封锁。电脑便能取得检索者要求的信息并回传。有时，绕道技术是专门为反制某一特定过滤软件或某一国家的封锁情况而设计的。但在大部分情况下，网民多半可采用已有的技术突破封锁，而无需考虑这技术是否专为此情况而设计。

有些绕道技术是私人公司研发出来的，另一些则是由网络黑客或积极份子所设计。这些技术含括极简单到复杂如网络通讯协议的程序。所以有不同层级程序可选，是为顾及使用者不同的需要，衡量对特殊软件操作技术的能力是否充足，再依此选择合适的绕道程序。

有两种使用绕道技巧的人：一是服务提供者；一是纯粹使用者。绕道程序被提供者安装于一台在未受监控地区的电脑上，为受网络监管地区的网民提供上线路径服务。一个成功的绕道服务评断指针在能符合提供者与使用者双方的需要。

本篇文章主要是为想使用绕道技术者写的，说明可采用的方式与如何选择符合需求的最佳方式。这取决于个人的需求与操作能力—不只是使用者，还包括提供绕道者—衡量安全性与软件的实用性。如果选对适合使用者的绕道技术，其有效性、安全性及稳定性是可以兼顾的。

考量需求与能力

绕道技术往往因使用者的差异而有各种不同的资源与不同专业技术等级。适用于某一情况的方法不见得就能合适其它情况。因此，当选择设定绕道技术时，提供服务者与使用者需要考量下列问题：

- 预期将会有多少用户〔指提供服务者与使用者〕，网络传输速度多少？
- 绕道用户站点及上网后会做什么？
- 运用此技术要具备多少专业知识〔提供服务者与使用者要同时考量〕？
- 远程用户能否信任这跨国的联网方式？
- 若网民被查获使用绕道技术，将会受何等惩处？
- 远程用户了解使用绕道技术的潜在风险吗？

用户数及网络传输速度

提供绕道服务者必须先预测将会有多少使用者，其需求与网络传输速度必须取得平衡。远程用户也必须考量：绕道技术会让上网速度变慢，所以要先估计所使用的网速多少。公共代理服务器的爱用者亦须想到：未受网络监管国家的人们也会使用自己所用的绕道路径。例如：绕道路径可能被用来下载一整部电影，这将会占去许多空间。因此，你可能会想限制使用者人数或传输总流量。不同的绕道技术能符合用户需要的某些或全部条件。

所在站点及用途

依远程使用者从何处上线、会用绕道传送什么，而有不同的绕道技术选择。例如：使用者若从公用电脑或网吧连上网，那里的电脑将不可能允许安装任何软件，只能采取线上数据库的方式绕道。另一些用户就可能会使用通过浏览器以外的其它方式，如：电子邮箱〔SMTP〕及文件传输〔FTP〕，并想在自己电脑上安装软件以改变原有的设定。当然，这就需要使用者有较充足的技术知识。

须具备的专业知识层级

对专业知识越了解〔此方式使用者越少〕，就能选择运用更多的绕道方式。当使用绕道时，安装、激活程序会需要变更或增加设置，对于电脑一窍不通的门外汉较容易受限。掌握专业知识对绕道提供者与远程用户同等重要。不正确的使用绕道将可能使用户面临原可避免的风险。

对联网方式的信任程度

如果远程用户认识并信任自己在国外的朋友，即可使用多种绕道。如果用户对提供绕道者没有充分信心，那么，他们就只限于使用一般大众皆能进入的系统。如果这是人人都可进入的系统，也就容易遭到封锁。远程用户和绕道提供者能建立互信的话，提供者便能依据用户个人特别需要设计绕道功能，并有效保护其隐私、避开侦查。若想使用一成功、长久且稳定的绕道系统，最重要的是，能与身处非网络封锁地的系统提供者建立互信。

预期会受到的惩罚

最重要的是了解被查到使用绕道后将面临的惩罚；后果的严重性会影响绕道系统的选择。如果对合法范围使用限定宽松，预期受到的惩罚不重，用户便能在众多安全保障较低的绕道方式中做选择。若大环境气氛紧张，就要选择隐密性及安全度较高的绕道方式。有时甚至可以合法的面貌为掩护或故意打迷糊仗。

安全风险

在网络遭封锁过滤的国家里，被鼓励使用绕道的用户，往往也被告知可能存在的安全风险；当然，使用者及所采行的绕道技术还有被侦测、封锁并加以控制的可能。使用者必须留心潜在的风险与被反制的可能，必须正确安装、使用绕道，将这些风险减到最低。

网上数据库绕道

网上数据库绕道是一种特殊网页，让用户可键入网页地址，由此数据库搜寻网页内容并传送给用户。用户与访问的网站间没有直接联系，透过网上数据库绕道代理，让用户可浏览被封锁的网站。网上数据库绕道亦能自动重新改写连结，将网页内容回传，用户便能持续以此途径访问网站。使用网上数据库绕道的用户不需安装新软件，也不必变更自己浏览器的设定。他们只需先访问绕道用网页，在其上输入自己接下来想访问的网页地址，按下「提交」〔submit〕键〔各网上数据库的呈现方式或许多少有点不同，但基本功能是相同的〕。使用者不须具备专门技术便可操作，且没有连结地点的限制。

优点:

□网上数据库绕道系统容易使用，不需加装任何软件。
□公共网上数据库绕道服务可让无法在未遭封锁地建立绕道的用户任意上线使用。
□私人网上数据库绕道系统可依个人需求建立特殊绕道方式，这也比较容易避过政府监察。

缺点:
□网上数据库绕道系统往往不容易登入网页(HTTP)或进入加密系统(SSL)。需要鉴别身分的网络服务〔如网上数据库提供的 email〕可能无法完整运作。
□因为公共网上数据库绕道服务广为人知，所以非常可能已遭到封锁。大部分的服务已经被商业用过滤软件封杀。
□私人网上数据库绕道系统，需要使用者在未遭网络封锁地有联系人。最理想的状态是：两地有办法透过不易遭监视的通讯方法取得联系。

公共网上数据库绕道服务

这些是开放公众使用的网上数据库绕道软件。无论是由个人、组织或公司提供绕道服务，都必须安装绕道软件而后设定为人人皆可进入的网页。公共网上数据库绕道服务有很多种，最常见的免费服务中，有些选项，如可选择加密登入，需要额外付费。有些服务是公司提供的，有些则是志愿者自行提供。

```
http://www.anonymizer.com/
http://www.unipeak.com/
http://www.anonymouse.ws/
http://www.proxyweb.net/
http://www.guardster.com/
http://www.webwarper.net/
http://www.proxify.com/
http://www.the-cloak.com/
```

可预见的是，这种服务的网站地址总是广为传播，大部分网络过滤器早已将它们列入封锁名单，当然，那些网络受政府管制的国家就更不用说了。如果这些服务网站遭封锁，就无法连结、使用。并且，多数公共网上数据库绕道在传输过程中皆无经过加密，任何使用者传输的信息均能被提供绕道服务者截取。

公共网上数据库绕道最适合在低安全风险的地区使用，不需要和非封锁地的提供者有互信关系，提供短时间或自由直接的绕道服务给不需传输敏感信息的使用者。

网上数据库绕道软件

安装网上数据库绕道软件需要一定水平的专门技术与硬件支持〔网络服务器与足够的传输速度〕。鉴于公共绕道及匿名服务不仅用户，连监控网络者亦知晓〔而且大部分还被过滤软件列入封锁名单〕，使用私人网上数据库绕道，地址只有提供者及使用者双方知道。相对于公共绕道，私人绕道被查觉与封锁的机率较低。

私人绕道服务可依据用户特殊需求量身打造，最常见的就是依用户需要更改连接端口

号码，如此，网络传输服务便经过加密。加密方式连接(SSL)是一种网上安全传输信息的协议。受加密保护的网站地址是以“HTTPS”开头，代替一般的“HTTP”。

当使用 SSL，它会在网络服务器里生成一个无关的网页，为绕道系统制造出一随机的路径与名称，以此掩护绕道。虽然如网络供货商等中介者有可能会侦测到用户使用的服务器，但他们无法知道用户连结网络的路径，因为这是经过加密的。例如：用户连结“https://example.com/secretcircumventor/”，中介者将可能察觉用户连结的是 example.com，但他们无法知道用户访问的网页是绕道服务。如果绕道服务系统又在 example.com 上生成一个无关的网页，如此一来，无论再怎么侦测，绕道系统也不会被发现。

CGIProxy:运作方式相当于 HTTP 或 FTP 代理服务器.
http://www.jmarshall.com/tools/cgiproxy/
Peacefire's Circumventor:自动安装程序，对于非专业人员而言，安装较容易.
http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
pHproxy:试验版网上数据库绕道.
http://ice.citizenlab.org/projects/phproxy/
Psiphon: SSL 网络服务，内建网上数据库绕道.
http://Soon to be released

对用户而言，私人网上数据库绕道连结加密系统最能稳定使用绕道服务传输信息；最好的情况是能与未受网络间控地的提供服务者若能建立互信关系，而该提供者又具备充分专业技术与足够的空间设置、维护网上数据库绕道。对单纯的信息传输而言，这将是最灵活、弹性的绕道，且最不易被发觉、封锁。

网上数据库绕道的安全顾虑

必需要注意的是，绕道系统不一定有匿名功能。虽然使用者的身分是被隐藏的，访问网站也是透过网上数据库绕道，但如果使用者和网上数据库间的联机传输的是普通网页模式(HTTP)，就如大部分的传输服务，特别是免费的，很容易被中介者〔如网络供货商(ISP)〕截取、解析。因此，虽然成功绕过封锁，但政府当局还是能追踪到用户使用绕道。甚至，还能侦测出用户透过绕道访问的网页内容与网站地址。

网上数据库在普通网页模式〔未经加密处理〕运作，有时会使用模糊网页地址的方式来反制关键词过滤。例如，使用一个简单的技术—ROT-13，会将最常用的字以英文前十三个字母替代。原网址：http://ice.citizenlab.org becomes 会变成 uggc://vpr.pvgvmrayno.bet/。网页地址经过编码，因此，关键词过滤技术无法侦破被访问的网页地址。尽管绕道成功，连结的内容还是容易被发觉。

使用 cookies 或 scripts 也有风险。许多网上数据库绕道会移除 cookies 及 scripts，但许多网站，如：e.g. web mail sites 会要求使用 cookies 及 scripts 浏览,当进入这些接口时一定要留心。另一个附带风险是：当使用某些服务时需要登入或键入密码时，绕道系统会通过普通网页连结，而后再从加密服务下载信息。绕道服务要从加密方式连接服务取得信

息就要通过加密过的方式传输，但在回传信息给用户的同时，就会通过普通网页传输，此时，这些敏感信息传输就可能被打断。

有些安全问题可以使用网上数据库代理服务器，并将连结经过加密。有些网上数据库代理服务器可支持网络加密连结 SSL (HTTPS)，将用户与网上数据库间传输的信息加密。在此情况下，网络供货商等中介者只会知道用户使用绕道，但无法查出访问的网页内容。如果使用者身处安全风险高的国家，强烈建议确定自己使用了具信息加密方式连接功能的网上数据库绕道。

虽然远程使用者连结网上数据库绕道时可能有安全保障，但所有经过网上数据库绕道传输的信息都能被网上数据库绕道服务的提供者截取。最后，对安全的顾虑在：绕道系统会保留传输纪录。政府当局可由绕道使用者或提供者的地址进入他们的登录档案。

即便是使用加密连结的网上数据库绕道，还有其它用户必须留意的安全顾虑。首先，使用加密会导致使用绕道的行为更为显眼；使用加密在某些地方不一定是合法的。其次，当局的网络过滤可能会侦测出哪些是最常经由绕道访问的网站，甚至是使用加密连结的网站亦会遭受 HTTPS fingerprinting 及 Man-In-The-Middle (MITM)的攻击。但是，动态网或绕道技术若附加随机误导功能，让网页内容另外加上不相干的图像，这可使遭攻击的风险减轻。如果在有 SSL 保证时，用户被要求同时使用 “fingerprint”或安全签署协议，可以手动操作方式测验这个保证是否真能避开 MITM 的攻击。[1]

代理服务器

代理服务器相当于是个中介服务器，连结用户〔网络浏览器〕及网络服务器；扮演着介于用户与服务器间的缓冲区，可支持多种信息传输，如：网页传输(HTTP)、文件传输(FTP)、加密传输(SSL)等。代理服务器广为个人、单位或国家使用，以达到安全、匿名、高速存取及过滤等不同目的。欲使用代理服务器，用户必须将其网络浏览器的 IP 地址或用户名改为代理服务器及更改连接埠。尽管技术十分简单，可是在公用电脑上，如：图书馆、网吧、工作单位，就无法更改浏览器设定。

优点:
□许多软件套装可选择从透明代理服务器传输到网页传输(HTTP)，并可设置非常用连接埠。
□有大量的公共代理服务器可供使用。

缺点:
□许多代理服务器无法预设加密，因此，用户与代理服务器间的传输不甚安全。
□用户必须改换浏览器设定，如果网络供货商要求所有信息都必须经由他们的代理服务器传输，就很可能无法使用开放代理服务器。
□浏览及使用公共代理服务器可能是违法的，因此用户可能完全无法使用代理服务器。

[1]更多关于潜在攻击以反制绕道系统的材料，见 Bennett Haselton’s “List of possible weaknesses in systems to circumvent Internet censorship”.可上网查询: http://peacefire.org/circumventor/list-of-possible-weaknesses.html 及 Paul Baranowski’s response at: http://www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

代理服务器软件

代理服务器的软件可经由网络封锁地之外、能信得过的网络传输安装，需要一定水平的专业技术。软件安装时需要再有足够传输频宽的环境下，并该配置加密技术。这对于身处于办公室或小型机构的用户而言，是最有用的绕道办法。当用户在网络封锁地设置代理服务器为中介浏览器后，便可不受阻碍地上网。尽管不是每个服务都是秘密性质的，私人代理服务器还是比网上数据库代理服务更好，因为有些网上数据库，如电邮网站，要求认证及使用 cookies。 代理服务亦可依照用户个人需求及网络封锁地的特殊情况配置。

Squid 免费代理服务器软件，具 Stunnel 安全保障. http://www.squid-cache.org/ http://www.stunnel.org/ http://ice.citizenlab.org/projects/aardvark/ Privoxy 具备过滤功能的代理服务器，能保护隐私. http://www.privoxy.org/ Secure Shell (SSH)具备 socks 功能的代理服务器($ ssh -D port secure.host.com) http://www.openssh.com/ HTTPport/HTTPhost 能绕过封锁的 HTTP 代理服务器.

具加密功能的私人代理服务器可提供团体或个人一个永久、稳定的绕道，并有可靠的境外连结及充足的技术、频宽以安装、维护代理服务器。

公用代理服务器

开放式代理服务器是有意地或在某些方面开放给远程电脑以连结网络。电脑的连接端口对外开放，如同代理、中介，连结分散在远程地址的各用户，提供户联网架构所需的普遍、基本功能。然而，不为人知的是：如果开放式代理服务器被设定为公共服务性质，或者，这些服务器没好好配置而不经意地成为公用代理，那么——
警告：依据美国地方法律规定，使用开放代理服务器可能被视为「未经授权认可的访问」，开放代理服务器用户可能会遭受刑事处分。因此，我们不建议使用开放式代理服务器。

定址开放代理服务器

许多网站提供开放代理服务器的清单，然而，这并非代理服务器都能运作的保证。许多在这清单上的代理服务器早已不对公众开放了。甚至，这些信息没什么质量的保证，特别是那些关于匿名层级与全球寻址的服务是不精确的。使用这些服务时请注意风险。

开放代理服务器网址清单:

http://www.samair.ru/proxy/ http://www.antiproxy.com/ http://tools.rosinstrument.com/proxy/ http://www.multiproxy.org/ http://www.publicproxyservers.com/

软件:代理服务器的工具/当地的代理服务器

http://proxytools.sourceforge.net/

开放代理服务器：特殊连接埠

有些国家级的网络封锁也会封锁一般的代理服务器连结端口。所谓「埠」指的是一个由特殊协议使用的连结点；不同的网络服务有其个别的连接端口号码传输信息。一些连接端口号码是由互联网地址指派机构(IANA)所指派的，例如：port 80 是接收 HTTP 传输。当由浏览器进入网站时，服务器就在 port 80 上运作连结网络。代理服务器也有自己的连接端口，为指定的默认值。因此，许多过滤技术就是让我们无法连结这些连接埠。所以，成功的绕道有赖于使用在非常用连接端口上运作的代理服务器，以避开过滤。

http://www.web.freerk.com/proxylist.htm

代理服务器的安全顾虑

代理服务器的设置特别重要，但光靠设置代理服务器还是无法有安全保障与匿名功能。如果不使用加密代理服务器，两者之间传输的信息就可能被截取，用以判别用户身分和查询此信息的电脑 IP 地址。所有用户与代理服务器间的传输如果都是普通网页，那么就更容易被上游的政府过滤器所截取。任何通过代理服务器传输的信息，也都能被服务器持有者截取。
因此不建议搜寻并使用公共代理服务器。开放式代理服务器通常都很好用，尽管能成功避过网络封锁，但无法保证传输的安全性。

如果是用网上数据库代理服务器，也会面临同样的安全顾虑。虽然合并使用加密代理服务器，有害的 scripts 和 cookies 还是会传输到用户电脑，且无法避免 MITM 及 HTTPS fingerprinting 的攻击。必须要注意的是，使用 socks 代理〔这是一特殊代理服务器，除了依班网页传输外，还能处理其它类型传输〕时，有些浏览器会泄漏敏感信息。当访问一网站时，域名会被转译为一串 IP 地址，有些转译动作是在浏览器上，不会直接经过代理。在此情况下，网站 IP 封锁会由在本国的域名服务系统执行过滤[2]。

使用开放、公共代理服务器不是个好办法，只能使用于低安全顾虑的地区，为无须传输敏感信息者，提供短时间、自由直接的匿名服务。

加密信道

[2]更多关于 Tor 的讯息，请见以下网站: http://tor.eff.org/cvs/tor/doc/CLIENTS

加密信道亦称为转寄，使用户在不安全、非加密传输状态下，寄送一个内含的加密协议。在遭封锁地区的用户可下载一软件，便能打开一条加密信道通往非封锁地的电脑。所有在用户电脑上的服务都能继续运作，但现在是透过加密的信道转寄到非经封锁的电脑，回复是透明的。有好几种加密信道产品。用户如果和非封锁地区有联系，便可设置一条私人加密信道服务；如果没有，可以购买商业加密信道服务，通常是每月签约。

使用免费加密信道服务，用户要注意的是，这些服务里常包含些小广告，如果想看这些广告就必须透过 HTTP 普通网页传输。如此，这就可能遭到拦截，随后即能判别用户在使用加密信道服务。有些加密信道服务是透过 SOCKS 代理的，这也可能会泄漏用户访问的域名。

http://www.http-tunnel.com/
http://www.hopster.com/
http://www.htthost.com/

优点:
□加密信道提供加密网络传输服务。
□加密信道不只能保障网络传输，还能保障代理服务器的安全协议。
□对和非网络封锁地没有联系的用户，可选购商业加密信道服务。

缺点:
□商业加密信道服务常广为人知，许多都已遭到过滤。
□加密信道无法用于公用电脑如网吧或图书馆，因为用户将无法在其上设置软件。
□使用加密信道比其它绕道方式需要更高层次专业技术。

加密信道适用于具备专业技术的使用者，提供比单纯网络传输更安全〔但非匿名〕的绕道服务，且不经由公共地址传输。商业加密信道对身处受网络监控国且与非监空地没有信任联系的用户，是非常好的服务。

匿名通讯系统

绕道技术和匿名通讯系统类似，之间常有些关联，但往往又依不同情况选择使用。匿名系统偏重于保密用户隐私，用户的身分是被屏蔽的，讯息提供者无法查知。此外，更先进的系统会通过多种路由，保障用户的身分被匿名通讯系统确实被屏蔽。除在互联网上重新取得信息，这些匿名系统能让用户匿名发表意见。绕道系统的重点未必放在匿名上，着重的是以绕过对用户的网络限制来保障通讯安全及连结。

许多案例中，匿名通讯服务是种网络绕道手段。匿名通讯服务的好处是，随时都有好几个互联网系统可供连结，如此便可享受匿名通讯的好处—绕过遭禁的内容。这种软件必须安装在使用者的系统中，有的会需要安装者具备一定水平的专业技术。匿名通讯的方式有很多，其中最普遍的一些技术变得越来越易于操作使用、使用越来越频繁。

使用匿名通讯系统作为绕道的限制是：使用者的电脑必须能安装所需软件。若是从公共端点，如：图书馆、网吧上网的用户就可能无法使用此系统。此外，软件可能会使连结速度变慢，情形视运作不同匿名系统而定。但最常与连结速度减慢有关的是，网络过滤技术是否封锁了这些匿名通讯系统的连结途径。

匿名通讯系统不一定会为面临严厉封锁地区设计绕道功能。当使用国家层级或网络供货商层级的通讯，用户想办法要绕过封锁时，可能发现匿名通讯系统遭到封锁。如果匿名通讯系统使用静态连接端口执行绕道，网络过滤软件便能轻易侦测并拒绝与特定连接埠连结。越来越多政府当局〔以及更进步的封锁技术〕的过滤软件能过滤出匿名通讯系统、阻断用户连结；此外，为对抗以同级或公共站点连结的系统，政府封锁系统只需阻挡用户进入主机，即能切断连结。政府的封锁系统甚至可试图运转一个属于他们的匿名通讯站点来监视想连结的用户。最终，在这些上网受限的地区，连结这些著名的反封锁网站系统都是受监控的，使用者可能会引起当局的注意[3]。

优点:
□匿名通讯系统可同时提供安全及匿名的服务。
□一般来说，匿名通讯系统能保障多项代理服务器协议，不只是对网页传输。
□匿名通讯系统会持续与用户保持联系及改良系统，并持续发展更好的辅助技术。

缺点:
□匿名通讯系统不是专门为绕道而设计的，他们广为人知，因此也容易被过滤封锁。
□匿名通讯系统不能在公共电脑上使用，如网吧或图书馆，因为使用者无法安装软件。
□相对于其它绕道方式，使用匿名通讯系统者，可能需要有较高水平的专业技术。

Tor 是一种虚拟信道可增进个人或群组在使用互联网时的隐私与安全性。它同时也能发展出新的内建隐私保障的通讯工具。Tor 提供一个操作平台，让机构或个人透过网络共享信息，无损于保障隐私。
http://tor.eff.org/
JAP 可让用户以匿名方式在网上浏览。用户以绕道方式取代直接连结网络服务，以加密并透过多个中介方式连结，所以也称为 mixes。
http://anon.inf.tu-dresden.de/index_en.html
Freenet 是种免费软件，能让用户发表意见或收取信息而无需担心被监控。以分散网络的方式让发信息及收取者都是匿名。
http://freenet.sourceforge.net/

匿名通讯系统的用户最好是有一定技术水平者，比一般网页传输需要设置更多得软件，如绕道及匿名服务，且不能通过公共地址进入连结。

结语

使用绕道服务前必须慎重考虑，详细分析自己的特殊需要、能运用的资源及使用者的安全顾虑。有许多可运用的技术提供给想绕过网络封锁的用户，但使用这些技术以建立安全、稳定的绕道服务有赖于许多要素，包括：使用者的专业技术水平、潜在的安全风险及能否与被监视国以外的用户取的联系、获得帮助。甚至，政府可能采取某些相应措施封锁特殊的绕道技术。

成功、稳定的绕道的关键为具备可信度与效益。绕道系统是针对用户的特殊情况或迅速修改以配合用户。这些绕道系统必须是安全、可装配且往往是秘密的。绕道提供者与使用者与间的互信要建立在对使用者身处的特殊法律、政治环境上，使用者在此环境中操作并面对使用绕道系统的限制。绕道提供者与使用者都需了解：互联网封锁过滤技术是如

[3]同 18 页注

何执行的，以及将使用的绕道技术。在完全掌握相关信息的情况下，才能选择要使用何种方法。

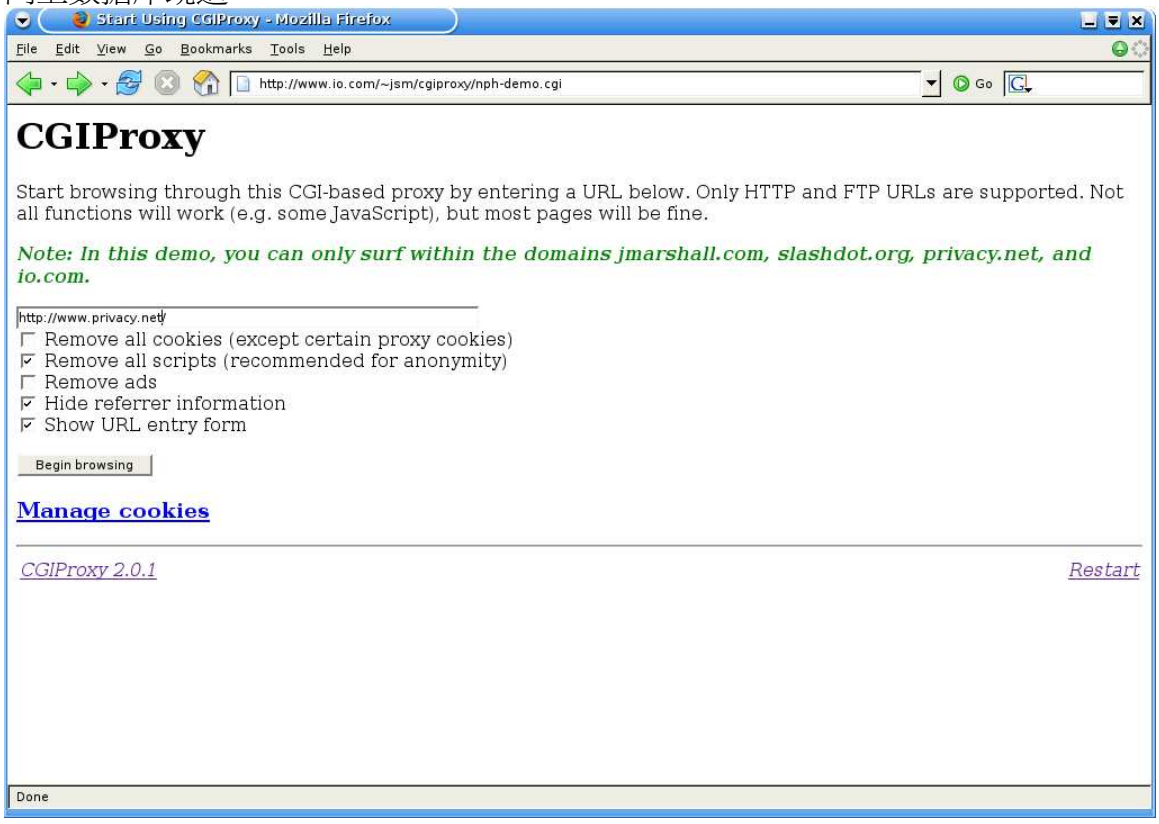
作者简介

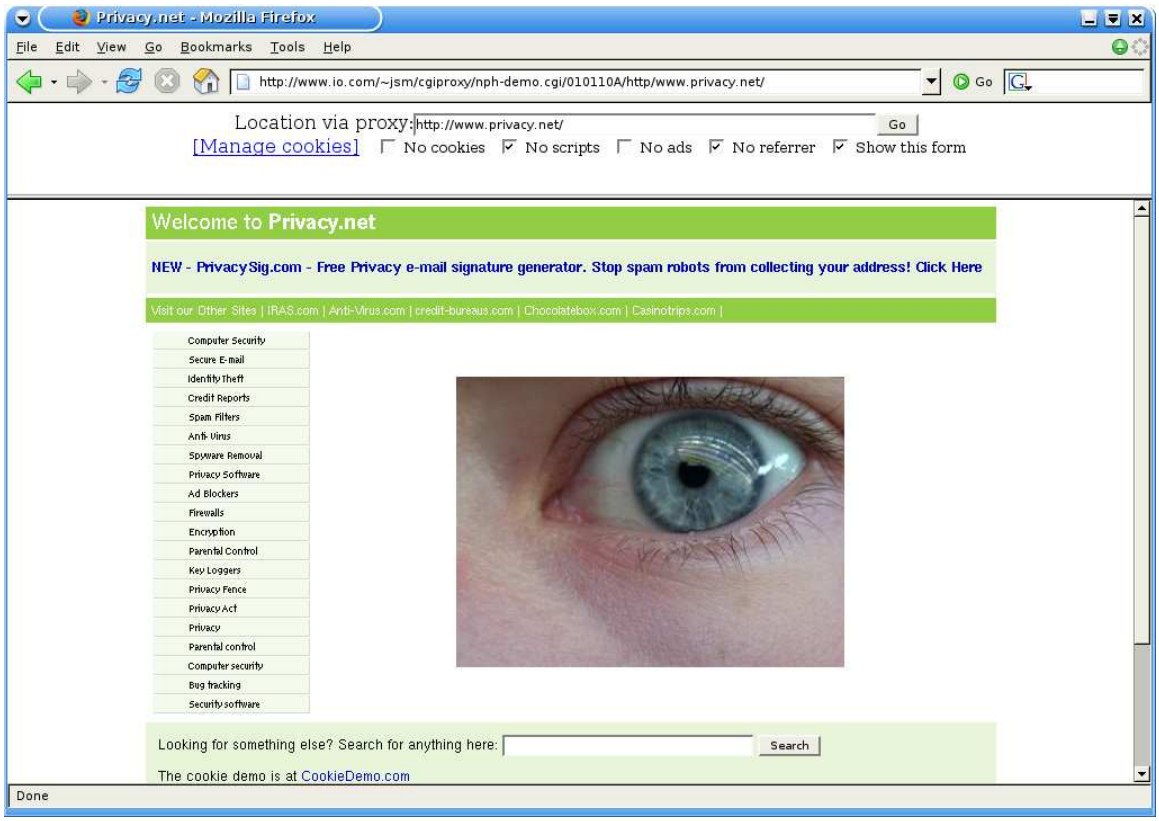
Nart Villeneuve 是 Citizen Lab 研究室的主任，这是个跨学科科技中心，隶属多伦多大学国际研究的 Munk 中心。作者同时亦从事件开发、研究，最近与 OpenNet Initiative (ONI，开放网)，研究各国对互联网内容封锁、监控的实施情况。同时亦曾对现有的绕道技术进行研究与评估，并也曾发展过绕道技术。除研究互联网监控外，还对网络黑客、网际恐怖活动及互联网安全性等主题有所研究。作者最近刚完成在多伦多大学的和平与冲突研究学程。

前言

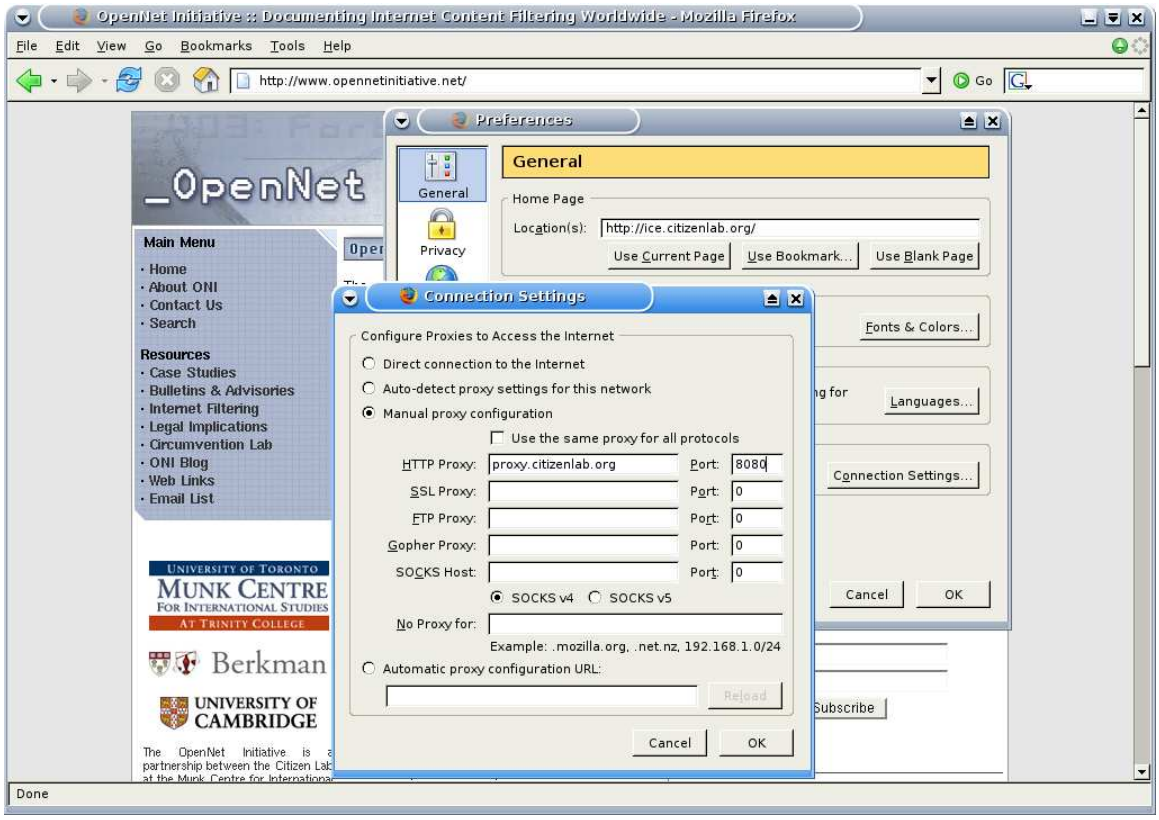
Michelle Levesque, Derek Bambauer 及 Bennett Haselton.

网上数据库绕道

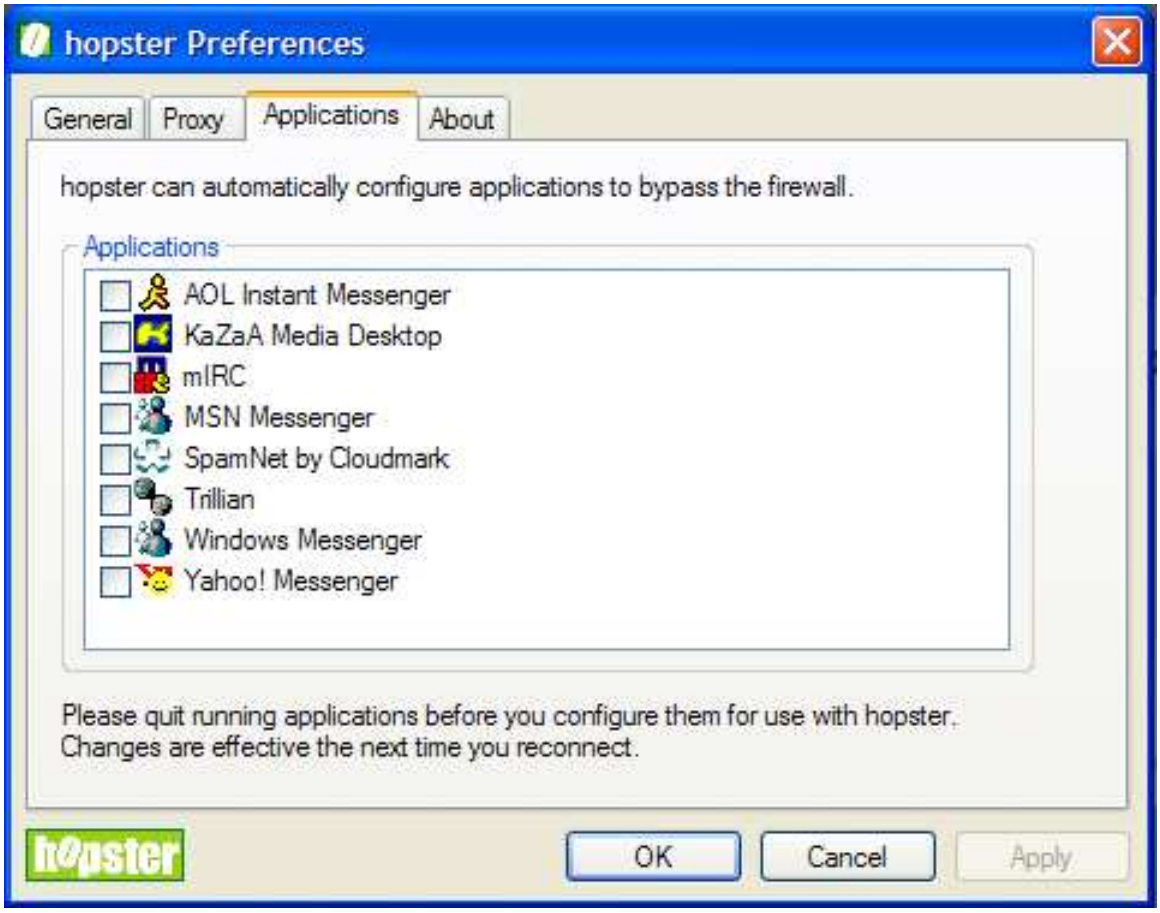




代理服务器/浏览器设定



加密信道软件


hopster Preferences
General
Proxy
Applications
About
hopster can automatically configure applications to bypass the firewall.
Applications
AOL Instant Messenger
KaZaA Media Desktop
mIRC
MSN Messenger
SpamNet by Cloudmark
Trillian
Windows Messenger
Yahoo! Messenger
Please quit running applications before you configure them for use with hopster.
Changes are effective the next time you reconnect.
hopster
OK
Cancel
Apply

匿名通讯系统


JAP
JAP
Anonymity & Privacy
00.04.017
Server:
Dresden-Dresden
Details
Anonymity
User:
1608
Traffic:
low
fair
high
Anonymity
Anonymity
On
Off
Own anonymized Data:
0 Byte
Activity:
Forwarder:
On
Activity:
Help
Config
Exit