Circumvention Quick Start

Published : 2011-04-29
License : GPLv2+

Table of Contents

QUICK START GUIDE

Introduction

On 10 December 1948, the adoption by the General Assembly of the Universal Declaration of Human Rights launched a new era. Lebanese scholar Charles Habib Malik described it to the assembled delegates as follows:

> *Every member of the United Nations has solemnly pledged itself to achieve respect for and observance of human rights. But, precisely what these rights are we were never told before, either in the Charter or in any other national instrument. This is the first time the principles of human rights and fundamental freedoms are spelled out authoritatively and in precise detail.* ***I now know what my government pledged itself to promote, achieve, and observe. ... I can agitate against my government, and if she does not fulfill her pledge, I shall have and feel the moral support of the entire world.***

One of the fundamental rights the Universal Declaration described, in Article 19, was the right to freedom of speech:

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and* ***to seek, receive, and impart information and ideas through any media and regardless of frontiers.***

When those words were written sixty years ago, no one imagined how the global phenomenon of the Internet would expand people's ability to "seek, receive and impart information", not only across borders but at amazing speeds and in forms that can be copied, edited, manipulated, recombined and shared with small or large audiences in ways fundamentally different than the communications media available in 1948.

More information in more places than ever imagined

The unbelievable growth in the past several years of what is on the Internet and where it is available has the effect of making an unimaginably vast portion of human knowledge and activity suddenly present in unexpected places: a hospital in a remote mountain village, your 12-year-old's bedroom, the conference room where you are showing your closest colleagues the new product design that will put you ahead of the competition, your grandmother's house.

In all of these places, the possibility of connecting to the world opens up many wonderful opportunities for improving people's lives. When you contract a rare disease on vacation, the remote village hospital may save your life by sending your test results to a medical specialist in the capital, or even in another country; your 12-year-old can research her school project or make friends with kids in other countries; you can present your new product design simultaneously to top managers in offices around the world, who can help you improve it; your grandmother can send you her special apple pie recipe by e-mail in time for you to bake it for dessert tonight.

But the Internet does not contain only relevant and helpful educational information, friendship and apple pie. Like the world itself, it is vast, complex and often scary. It is just as available to people who are malicious, greedy, unscrupulous, dishonest or merely rude as it is to you and your 12-year-old child and your grandmother.

Not everyone wants to let the whole world in

With all of the best and worst of human nature reflected on the Internet and certain kinds of deception and harassment made much easier by the technology, it should not surprise anyone that the growth of the Internet has been paralleled by attempts to control how people use it. There are many different motivations for these attempts. The goals include:

- Protecting children from material perceived as inappropriate, or limiting their contact with people who may harm them.

- Reducing the barrage of unwanted commercial offers by e-mail or on the Web.
- Controlling the size of the flow of data any one user is able to access at one time.
- Preventing employees from sharing information that is viewed as the property of their employer, or from using their work time or an employer's technical resources for personal activities.
- Restricting access to materials or online activities that are banned or regulated in a specific jurisdiction (for example a country or an organization like a school) such as explicit sexual or violent materials, drugs or alcohol, gambling and prostitution, and information about religious, political or other groups or ideas that are deemed to be dangerous.

Some of these concerns involve allowing people to control *their own* experience of the Internet (for instance, letting people use spam-filtering tools to prevent spam from being delivered to their own e-mail accounts), but others involve restricting how *other people* can use the Internet and what those *other people* can and can't access. The latter case causes significant conflicts and disagreements when the people whose access is restricted don't agree that the blocking is appropriate or in their interest.

Who is filtering or blocking the Internet?

The kinds of people and institutions who try to restrict the Internet use of specific people are as varied as their goals. They include parents, schools, commercial companies, operators of Internet cafés or Internet Service Providers (ISPs), and governments at different levels.

The extreme end of the spectrum of Internet control is when a national government attempts to restrict the ability of its entire population to use the Internet to access whole categories of information or to share information freely with the outside world. Research by the OpenNet Initiative (http://opennet.net) has documented the many ways that countries filter and block Internet access for their citizens. These include countries with pervasive filtering policies, who have been found to routinely block access to human rights organizations, news, blogs, and Web services that challenge the *status quo* or are deemed threatening or undesirable. Others block access to single categories of Internet content, or intermittently to specific websites or network services to coincide with strategic events, such as elections or public demonstrations. Even countries with generally strong protections for free speech sometimes try to limit or monitor Internet use in connection with suppressing pornography, so-called "hate speech", terrorism and other criminal activities, leaked military or diplomatic communications, or the infringement of copyright laws.

Filtering leads to monitoring

Any of these official or private groups may also use various techniques to monitor the Internet activity of people they are concerned about, to make sure that their attempts at restriction are working. This ranges from parents looking over their child's shoulder or looking at what sites were visited on the child's computer, to companies monitoring employees' e-mail, to law enforcement agencies demanding information from ISPs or even seizing the computer in your home looking for evidence that you have engaged in "undesirable" activities.

When is it censorship?

Depending on who is restricting access to the Internet and/or monitoring its use, and the perspective of the person whose access is being restricted, nearly any of these goals and any of the methods used to achieve them may be seen as legitimate and necessary or as unacceptable censorship and a violation of fundamental human rights. A teenage boy whose school blocks access to his favorite online games or to social networking sites such as Facebook feels his personal freedom to be abridged just as much as someone whose government prevents him from reading an online newspaper about the political opposition.

Who exactly is blocking my access to the Internet?

Who is able to restrict access to the Internet on any given computer in any given country depends on who has the ability to control specific parts of the technical infrastructure. This control may be based on legally established relationships or requirements, or on the ability of governmental or other bodies to pressure those who have legal control over the technical infrastructure to comply with requests to block, filter or collect information. Many parts of the international infrastructure that supports the Internet are under the control of governments or government-controlled agencies, any of which may assert control, in accordance with local law or not.

Filtering or blocking of parts of the Internet may be heavy-handed or very light, clearly defined or nearly invisible. Some countries openly admit to blocking and publish blocking criteria, as well as replacing blocked sites with explanatory messages. Other countries have no clear standards and sometimes rely on informal understandings and uncertainty to pressure ISPs to filter. In some places, filtering comes disguised as technical failures and governments don't openly take responsibility or confirm when blocking is deliberate. Different network operators even in the same country and subject to the same regulations may execute filtering in quite different ways out of caution, technical ignorance, or commercial competition.

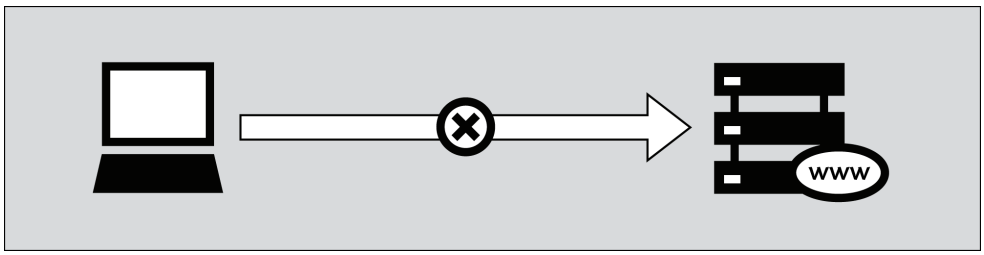
At all levels of possible filtering, from individual to national, the technical difficulties of blocking precisely what is viewed as undesirable may have unexpected and often ridiculous consequences. "Family-friendly" filters meant to block sexual materials prevent access to useful health information. Attempts to block spam may filter out important business correspondence. Attempts to block access to specific news sites may also cut off educational resources.

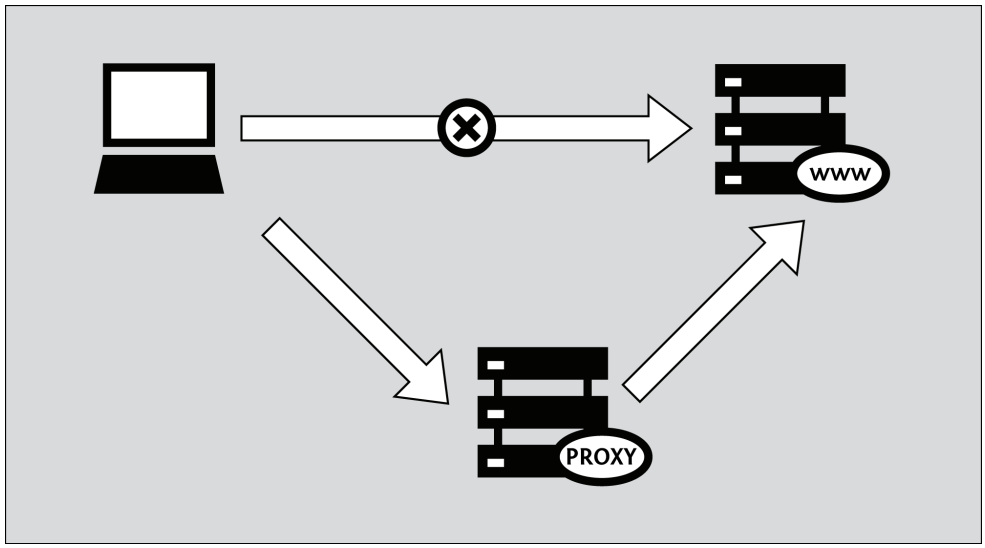
What methods exist to bypass filtering?

Just as many individuals, corporations and governments see the Internet as a source of dangerous information that must be controlled, there are many individuals and groups who are working hard to ensure that the Internet, and the information on it, is freely available to everyone who wants it. These people have as many different motivations as those seeking to control the Internet. However, for someone whose Internet access is restricted and who wants to do something about it, it may not matter whether the tools were developed by someone who wanted to chat with a girlfriend, write a political manifesto, or send spam.

There is a vast amount of energy, from commercial, non-profit and volunteer groups, devoted to creating tools and techniques to bypass Internet censorship, resulting in a number of methods to bypass Internet filters. Collectively, these are called **circumvention** methods, and can range from simple work-arounds, protected pathways, to complex computer programs. However, they nearly all work in approximately the same manner. They instruct your Web browser to take a detour through an intermediary computer, called a **proxy**, that:

- is located somewhere that is not subject to Internet censorship
- has not been blocked from your location
- knows how to fetch and return content for users like you.





What are the risks of using circumvention tools?

Only you, the person who hopes to bypass restrictions on your Internet access, can decide whether there are significant risks involved in accessing the information you want; and only you can decide whether the benefits outweigh the risks. There may be no law specifically banning the information you want or the act of accessing it. On the other hand, the lack of legal sanctions does not mean you are not risking other consequences, such as harassment, losing your job, or worse.

The following chapters discuss how the Internet works, describe various forms of online censorship, and elaborate on a number of tools and techniques that might help you circumvent these barriers to free expression. The overarching issue of digital privacy and security is considered throughout the book, which begins by covering the basics, then addresses a few advanced topics before closing with a brief section intended for webmasters and computer specialists who want to help others bypass Internet censorship.

Quickstart

The Internet is censored when the people or groups controlling a network prevent Internet users from accessing particular content or services.

Internet censorship takes many forms. For example, governments may block regular e-mail services in order to compel citizens to use government e-mail that can be easily monitored, filtered, or shut down. Parents can control the content their minor children access. A university may prevent students from accessing Facebook from the library. An Internet caf owner can block peer-to-peer file sharing. Authoritarian governments may censor reports on human rights abuses or the last stolen election. People have widely varying views about the legitimacy or illegitimacy of these forms.

Circumvention

Circumvention is the act of bypassing Internet censorship. There are many ways to do this, but nearly all circumvention tools work in approximately the same manner. They instruct your Web browser to take a detour through an intermediary computer, called a proxy, that:

- is located somewhere that is not subject to Internet censorship
- has not been blocked from your location
- knows how to fetch and return content for users like you.

Security and anonymity

Keep in mind that no tool is a perfect solution for your situation. Different tools offer varying degrees of security, but technology cannot eliminate the physical risks you take by opposing people in power. This book contains several chapters explaining how the Internet works which is important for understanding how to be safer while circumventing censorship.

There are many variations

Some tools only work with your Web browser, while others might be applied to several programs at once. These programs might need to be configured to send Internet traffic through a proxy. With a little extra patience, you can do all of this without installing any software on your computer. Note that tools that fetch Web pages for you may not display the site correctly.

Some tools use more than one intermediary computer in order to hide the fact that you are visiting blocked services. This also hides your activities from the tool provider, which can be important for anonymity. A tool may have a clever way of learning about alternative proxies it may connect to in case the one you are using gets censored itself. Ideally, the traffic created by all of this requesting, fetching and sending is encrypted in order to protect it from prying eyes.

But choosing the right tool for your particular situation is almost certainly *not* the most important decision you will make when it comes to accessing or producing content in the face of Internet censorship. Though it is difficult to provide concrete advice on such things, it is crucial to spend your time thinking about context, such as:

- how, when, and where you intend to use these tools
- who might want to prevent you from doing the things the tools allow you to do
- how strongly those organizations and individuals oppose this usage
- what resources they have at their disposal to help them achieve their desired outcome, up to and including violence.

Access most blocked Web sites without extra software

The most basic type of circumvention tool is a Web proxy. While there are many reasons why it might not be the optimal solution for you, for very basic circumvention purposes it is often a good place to start. Assuming it has not yet been blocked from your location, visit the following URL: http://sesaweenglishforum.net

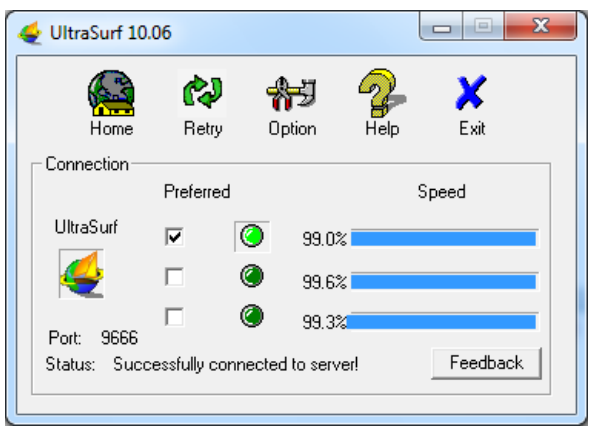
Accept the Terms of Use, and enter the URL of the blocked site you wish to visit into the blue URL bar:

Press Enter or click GO, and if it successfully navigates to the requested website then it is working. If the link above does not work, you will have to find an alternative circumvention method. The Web proxy and Psiphon chapters of this book offer a little advice about finding a Web proxy and a lot of advice about deciding whether or not you should be willing to use it once you do.

If you need access to the full feature set of a particularly complex Web site such as Facebook you might want to use a simple, installable tool like Ultrasurf instead of a Web proxy. If you desire or require a solution that has been through rigorous security testing and that can help you remain anonymous without requiring that you know who actually administers the service itself, you should use Tor. If you need access to filtered Internet resources other than just Web sites, such as blocked instant messaging platforms or filtered email servers (the kind used by programs like Mozilla Thunderbird or Microsoft Outlook), you might try HotSpot Shield or some other OpenVPN service. All of these tools, which have their own chapter later in the book, are briefly described below.

Access all blocked Web sites and platforms

Ultrasurf is a free proxy tool for the Windows operating system which can be downloaded at http://www.ultrareach.com/, http://www.ultrareach.net/ or http://www.wujie.net/. The downloaded zip file has to be extracted with a right click and selecting "Extract All...". The resulting .exe file can be started directly (even from a USB flash drive in an Internet caf) without installation.

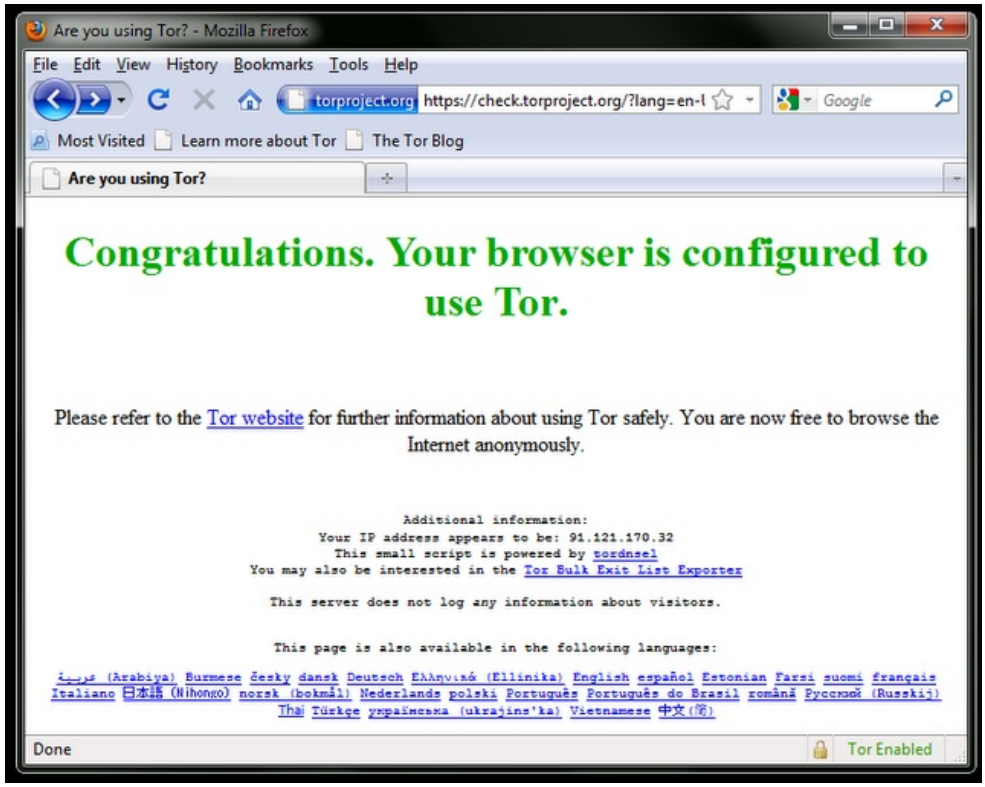


Ultrasurf connects automatically and will launch a new instance of the Internet Explorer Web browser which you can use to open blocked Web sites.

Bypass the filters and stay anonymous on the Web

Tor is a sophisticated network of proxy servers. It is free open source software developed primarily to allow anonymous Web browsing, but it is also a great censorship circumvention tool. The Tor Browser Bundle for Windows, Mac OS X or GNU/Linux can be downloaded from https://www.torproject.org/download/download.html.en. If the torproject.org Web site is blocked for you, you may find other download locations by typing "tor mirror" in your favorite Web search engine or by sending an email to gettor@torproject.org with "help" in the message body.

When you click on the downloaded file, it will extract itself to the location you choose. This may also be a USB flash drive which can be used in an Internet caf. You can then launch Tor by clicking "Start Tor Browser" (make sure you close any Tor or Firefox instances that are already running). After a few seconds, Tor automatically launches a special version of the Firefox Web browser with a test Web site. If you see the green message "Congratulations. Your browser is configured to use Tor." you can then use that window to open blocked Web sites.



Channel all your Internet traffic through a secure tunnel

If you want to access Internet services other than the Web, such as e-mail through an e-mail client like Outlook or Thunderbird, one easy and secure way is to use a virtual private network (VPN). A VPN will encrypt and tunnel all Internet traffic between yourself and another computer, so not only will it make all your various kinds of traffic appear similar to an eavesdropper, but the encryption will make it unreadable to anyone along the way. While connecting with the VPN, your ISP will not see your content, but will be able to see that you are connecting to the VPN. Since many international companies use VPN technology to securely connect their remote offices, VPN technology is unlikely to be blocked as a whole.

Made with Booki

Visit http://software.booki.cc