CIRCUMVENTION TOOLS

Published : 2011-03-10

1. 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.

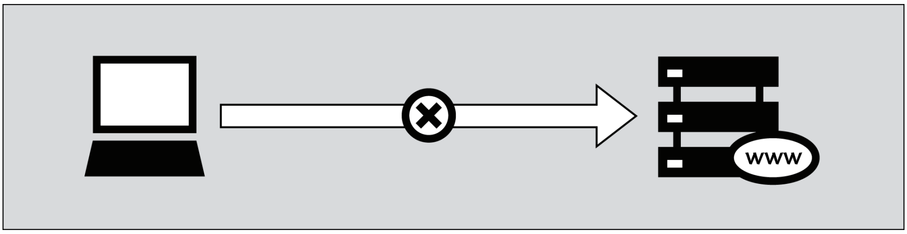
At all levels of possible filtering, from individual to national, the technical difficulties of blocking precisely what is viewed as undesirable may have unexpected and often ridiculous consequences. "Family-friendly" filters meant to block sexual materials prevent access to useful health information.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

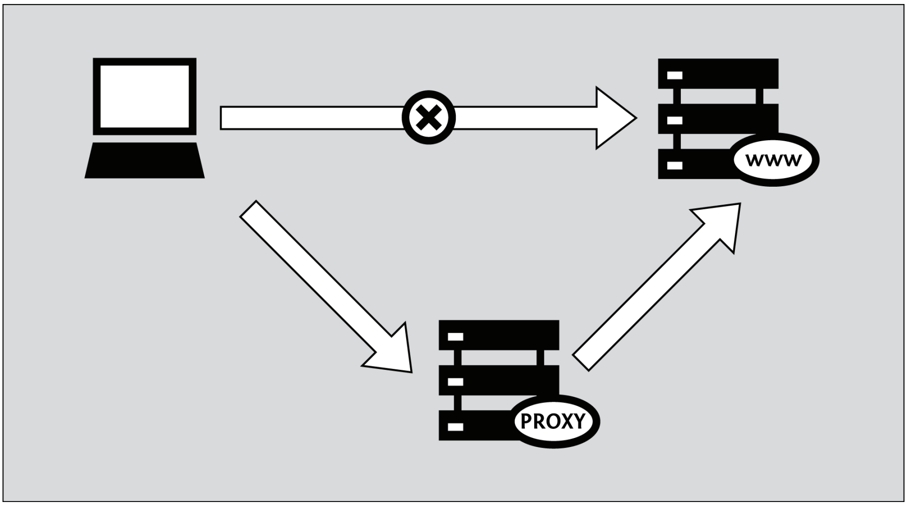
WHAT METHODS EXIST TO BYPASS FILTERING?

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.

2. ABOUT THIS MANUAL

This manual, 'Bypassing Internet Censorship', provides an introduction to the topic and explains some of the software and methods most often used for circumventing censorship. There is some information on avoiding surveillance and other means of detection while bypassing censorship, however this is a large topic in itself so we have only addressed it where it coincides directly with issues of circumvention.

A full discussion of techniques for maintaining anonymity and preventing detection of content or activities is beyond the scope of this book.

HOW AND BY WHOM THIS BOOK WAS WRITTEN

The first version of this manual featured content that had been largely written at a Book Sprint that took place in November 2008 in the beautiful hills of Upper New York State in the USA. Eight people worked together over an intensive five-day period to produce the book.

The updated version of this manual that you are currently reading was compiled in the context of a second Book Sprint held near Berlin, Germany, in early 2011. This time, 11 people worked together over an intensive five-day period.

This book is a living document of course and is available online for free, where you can also edit it and improve it.

In addition to the material written during the two Book Sprints, material has been contributed from previous publications. These include contributions from:

- Ronald Deibert
- Ethan Zuckerman
- Roger Dingledine
- Nart Villeneuve
- Steven Murdoch
- Ross Anderson
- Freerk Ohling
- Frontline Defenders
- Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey from The Berkman Center for Internet & Society at Harvard University

These writers kindly agreed to let us use their material within a GPL licensed environment.

This manual has been written within FLOSS Manuals. To improve this manual follow these steps:

1. REGISTER

Register at FLOSS Manuals:
http://booki.flossmanuals.net/

2. CONTRIBUTE!

Select the manual (http://booki.flossmanuals.net/bypassing-censorship/edit/) and a chapter to work on.

If you need to ask us questions about how to contribute then join the chat room listed below and ask us! We look forward to your contribution!

For more information on using FLOSS Manuals you may also wish to read our manual:
http://en.flossmanuals.net/FLOSSManuals

3. CHAT

It's a good idea to talk with us so we can co-ordinate all contributions. We have a chat room for this using Internet Relay Chat (IRC). If you know how to use IRC you can connect to the following:
server: irc.freenode.net
channel: #booksprint

If you do not know how to use IRC then visit the following web based chat software in your browser:
http://irc.flossmanuals.net/

Information about how to use this web-based chat software is here:
http://en.flossmanuals.net/FLOSSManuals/IRC

4. MAILING LIST

For discussing all things about FLOSS Manuals join our mailing list:
http://lists.flossmanuals.net/listinfo.cgi/discuss-flossmanuals.net

QUICK START
3. Quickstart

3. 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 café 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.

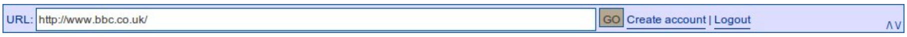
Some tools use more than one intermediary computer in order to hide the fact that you are visiting blocked services. This also hides your activities from the tool provider, which can be important for anonymity. A tool may have a clever way of learning about alternative proxies it may connect to in case 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



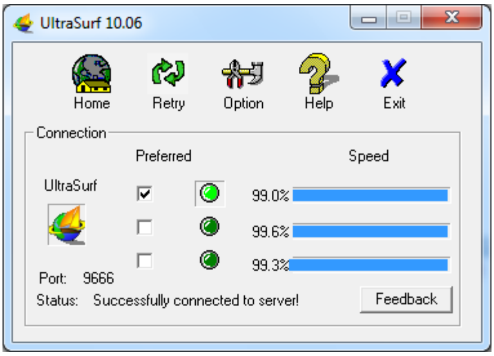
URL: http://www.bbc.co.uk/

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 café) without installation.



☑ ● 99.0%
□ ● 99.6%
□ ● 99.3%

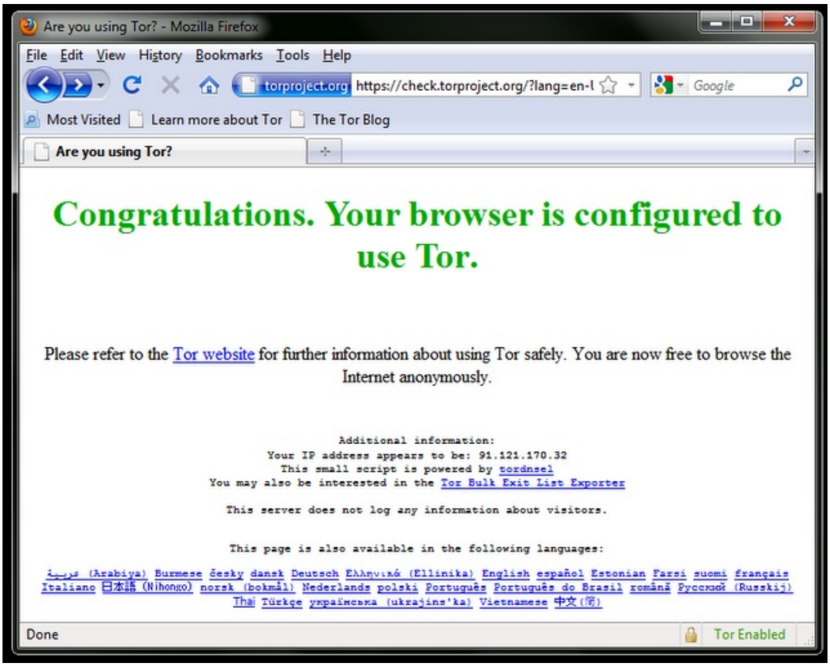
Port: 9666
Status: Successfully connected to server!

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 café. 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.



Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
torproject.org https://check.torproject.org/?lang=en-l
Google
Most Visited
Learn more about Tor
The Tor Blog
Are you using Tor?
Done
Tor Enabled

Congratulations. Your browser is configured to use Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

```
Additional information:
Your IP address appears to be: 91.121.170.32
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

This page is also available in the following languages:
```

عربية (Arabiya) Burmese česky dansk Deutsch Ελληνικά (Ellinika) English español Estonian Farsi suomi français Italiano 日本語 (Nihongo) norsk (bokmål) Nederlands polski Português Português do Brasil română Русский (Russkij) Thai Türkçe українська (ukrajins'ka) Vietnamese 中文(简)

CHANNEL ALL YOUR INTERNET TRAFFIC THROUGH A SECURE TUNNEL

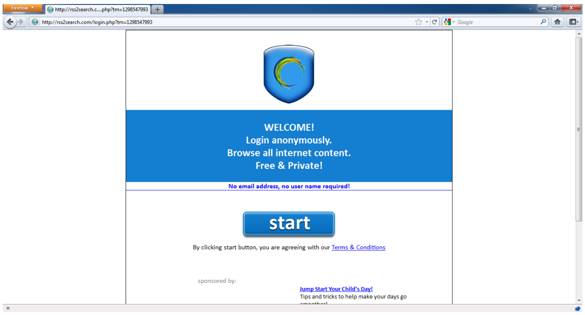
If you want to access Internet services other than the Web, such as e-mail through an e-mail client like Outlook or Thunderbird, one easy and secure way is to use a virtual private network (VPN). A VPN will encrypt and tunnel all Internet traffic between yourself and another computer, so not only will 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.

Hotspot Shield

An easy way to get started with VPNs is to use Hotspot Shield. Hotspot Shield is a free (but commercial) VPN solution available for the Microsoft Windows and Mac OS X operating systems.

To install Hotspot Shield you must download the software from https://www.hotspotshield.com. The file size is about 6MB, so on a slow dial-up connection the download might take 25 minutes or more. To install, double-click the downloaded file and follow the steps presented by the installation wizard.

Once the installation is complete, start Hotspot Shield from the "Hotspot Shield Launch" icon on your desktop or via "Programs > Hotspot Shield". A browser window will open with a status page showing different stages of the connection attempt such as "Authenticating" and "Assigning IP address". Once connected, Hotspot Shield will redirect you to a welcome page. Click on "start" to begin surfing.



Firefox
http://rss2search.c....php?tm=1298547993
http://rss2search.com/login.php?tm=1298547993
Google
start

WELCOME!
Login anonymously.
Browse all internet content.
Free & Private!

No email address, no user name required!

By clicking start button, you are agreeing with our Terms & Conditions

sponsored by:

Jump Start Your Child's Day!
Tips and tricks to help make your days go smoother!

To stop Hotspot Shield, right click on the traybar icon and select "Disconnect/OFF".

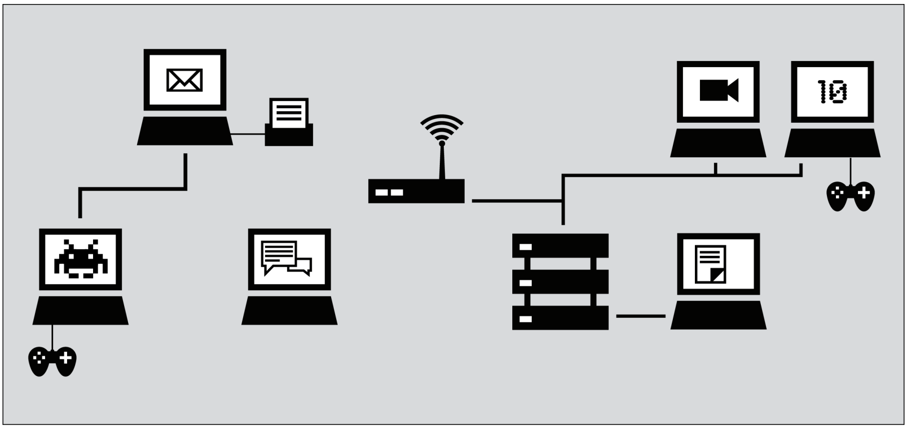
BACKGROUND
4. How the Net Works
5. Censorship and the Net
6. Circumvention and Safety

4. HOW THE NET WORKS

Imagine a group of individuals who decide to share information on their computers by connecting them, and by sending information between these computers. Their efforts result in a set of devices able to communicate with each other via a computer network. Of course, the network can be even more valuable and useful if it is connected to other networks and hence to other computers and network users. This simple desire to connect and share information electronically is manifested today in the global Internet. As the Internet has grown rapidly, the complexity of its interconnections has also increased, and the Internet is literally built up from the interconnection of a tremendous number of networks.

The fundamental task of the Internet can be described as facilitating the journey of digital information from its origin to its destination, using a suitable path and an appropriate mode of transportation.

Local computer networks, called Local Area Networks, or LANs, physically connect a number of computers and other devices at the same physical location to one another. They can also connect to other networks via devices called routers that manage the information flow between networks. Computers in a LAN can communicate with each other directly for purposes like sharing files and printers, or playing multi-player networked video games. A LAN could be useful even if it were not connected to the outside world, but it clearly becomes more useful when it is.



The Internet today is a decentralized world-wide network of such local computer networks, as well as larger networks such as university and corporate networks, and the networks of hosting providers.

The organizations that arrange these interconnections between networks are called Internet Service Providers or ISPs. An ISP's responsibility is to deliver data to the appropriate place, usually by forwarding the data to another router (called "the next hop") closer to the data's final destination. Often, the next hop actually belongs to a different ISP.

In order to do this, the ISP may purchase its own Internet access from a larger ISP, such as a national provider. (Some countries have only a single national-level provider, perhaps government-operated or government-affiliated, while others have several, which might be competing private telecommunications firms.) National providers may similarly receive their connections from one of the multinational companies that maintain and operate the servers and connections that are often mentioned as the *backbone* of the Internet.

The backbone is made up of major network equipment installations and global connections between them via fiber-optic cables and satellites. These connections enable communications between Internet users in different countries and continents. National and international providers connect to this backbone through routers sometimes known as gateways, which are connections that allow disparate networks to communicate with each other. These gateways, just like other routers, may be a point at which Internet traffic is monitored or controlled.

BUILDING THE INTERNET

The creators of the Internet generally believed that there is only one Internet, that it is global, and that it should allow any two computers anywhere in the world to communicate directly with one another, assuming the owners of both computers want this to happen.

In a 1996 memo, Brian Carpenter, then chairman of the Internet Architecture Board, wrote:

```
in very general terms, the [Internet engineering] community believes
that the goal is connectivity ... [the] growth of the network seems
to show that connectivity is its own reward, and is more valuable than
any individual application.
```

There is still a major community of Internet pioneers and early adopters who champion the ideals of worldwide interconnectivity, open standards, and free access to information, although these ideals often come into conflict with political and business interests and thus don't always directly influence the day-to-day operating practices and policies of individual parts of the Internet.

The originators of the Internet also created and continue to create standards aimed to make it easier for others to also create their own networks, and to join them to each other. Understanding Internet standards helps make clear how the Internet works and how network sites and services become accessible – or inaccessible.

STANDARDS FOR CONNECTING DEVICES

Most LANs today are built with wired Ethernet or with wireless Ethernet (802.11 or Wi-Fi) technology. All of the interconnections (of LANs and other devices) that make up the Internet use common technical standards, or Internet **protocols**, to let computers find and communicate with to one another. Often, the interconnections use privately-owned equipment and facilities, and are operated on a for-profit basis. In some jurisdictions, Internet connections are extensively regulated by law. In others, there is little or no regulation.

The most basic standard that unites all of the devices on the global Internet is called the Internet Protocol (IP).

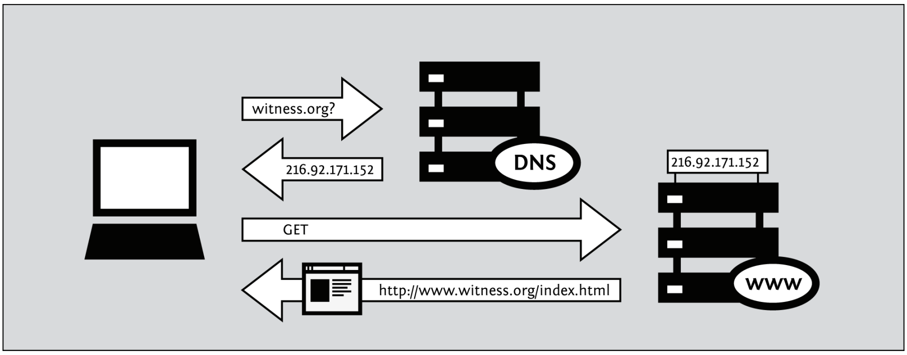
STANDARDS FOR IDENTIFYING DEVICES ON THE NETWORK

When your computer connects to the Internet, it is normally assigned a numeric IP address. Like a postal address, the IP address uniquely identifies a single computer on the Internet. Unlike the postal address, however, an IP address (particularly for a personal computing device) is not necessarily permanently associated with a specific computer. So, when your computer disconnects from the Internet and reconnects at a later time, it may receive a different (unique) IP address. The IP protocol version currently in predominant use is IPv4. In the IPv4 protocol, an IP address is written as four numbers in the range 0-255, separated by dots (e.g. 207.123.209.9).

DOMAIN NAMES AND IP ADDRESSES

All Internet servers, such as those which host Web sites, also have IP addresses. For example, the IP address of www.witness.org is 216.92.171.152. Since remembering IP addresses is cumbersome and IP addresses might change over time, specific systems are in place to make it easier for you to reach your destination on the Internet. This system is the Domain Name System (DNS), where a set of computers are dedicated to serving your computer with the IP addresses associated with the human-memorable "names".

For example, to access the Witness Web site you would type in the www.witness.org address, also known as a domain name, instead of 216.92.171.152. Your computer then sends a message with this name to a DNS server. After the DNS server translates the domain name into an IP address, it shares that information with your computer. This system makes Web browsing and other Internet applications more human-friendly for humans, and computer-friendly for computers.



Mathematically speaking, IPv4 allows for a pool of about 4.2 billion different computers to be connected to the Internet. There is also technology that lets multiple computers share a single IP address. Despite this, the pool of available addresses was more or less exhausted at the beginning of 2011. As a result, the IPv6 protocol has been devised, with a much larger repository of possible unique addresses. IPv6 addresses are much longer, and even harder to remember, than traditional IPv4 addresses. An example of an IPv6 address is:

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

Although as of 2011 less than 1% of the Internet uses the IPv6 protocol, this will probably change dramatically in the near future.

PROTOCOLS FOR SENDING INFORMATION THROUGH THE NETWORK

The information you exchange as you use the Internet could take many forms:

- an e-mail to your cousin
- a picture or video of an event
- a database of contact information
- a file containing a set of instructions
- a document containing a report on a sensitive topic
- a computer program that teaches a skill.

There is a wide variety of Internet software to accommodate proper handling of the various forms of information according to specific protocols, such as:

- e-mail via Simple Mail Transport Protocol (SMTP)
- instant messaging via Extensible Messaging and Presence Protocol (XMPP)
- file sharing via File Transfer Protocol (FTP),
- peer-to-peer file sharing via BitTorrent protocol
- Usenet news via Network News Transfer Protocol (NNTP)
- a combination of protocols: voice communication using Voice Over Internet Protocol (VoIP), Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP)

THE WEB

Although many people use the terms "the Internet" and "the Web" interchangeably, actually the Web refers to just one way of communicating using the Internet. When you access the Web, you do so using software called a Web browser, such as Mozilla Firefox, Google Chrome, Opera, or Microsoft Internet Explorer. The protocol that the Web operates on is called the Hyper-Text Transfer Protocol or HTTP. You might also have heard of HTTPS, which is the secure version of HTTP that uses Transport Layer Security (TLS) encryption to protect your communications.

FOLLOWING YOUR INFORMATION ON THE INTERNET - THE JOURNEY

Let's follow the example of visiting a Web site from your home computer.

Connecting to the Internet

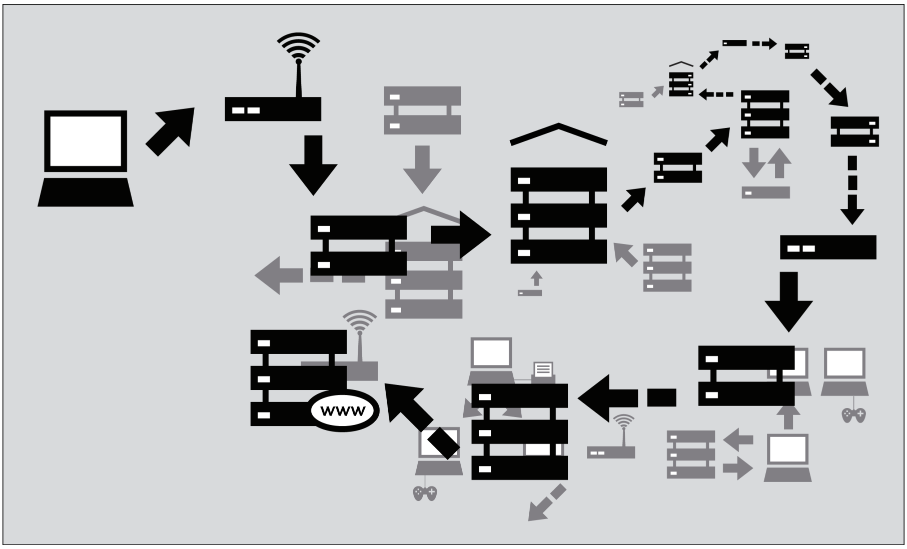
To connect your computer to the Internet, you may need some extra equipment, such as a modem or a router, to first connect to your ISP's network. Usually, end-user computers or home networks are connected with ISPs via one of several technologies:

- telephone modem ("dial-up"), sending Internet data over telephone lines in the form of a telephone call
- DSL, a more efficient and higher-speed way to send data over telephone lines over short distances
- cable modem (or "cable Internet"), sending Internet data over a cable television company's coaxial cable
- fiber-optic cables, particularly in densely-populated areas of developed countries
- wide-area fixed wireless links, particularly in rural areas
- data service over the mobile phone network.

Browse to the Web site

1. You type in https://security.ngoinabox.org/. The computer sends the domain name "security.ngoinabox.org" to a selected DNS server, which returns a message containing the IP address for the Tactical Tech Security in a Box Web server (currently, 64.150.181.101).
2. The browser then sends a request for a connection to that IP address.
3. The request goes through a series of routers, each one forwarding a copy of the request to a router closer to the destination, until it reaches a router that finds the specific computer needed.
4. This computer sends information back to you, allowing your browser to send the full URL and receive the data to display the page.

The message from the Web site to you travels through other devices (computers or routers). Each such device along a path can be referred to as a "hop"; the number of hops is the number of computers or routers your message comes in contact with along its way and is often between 5 and 30.



WHY THIS MATTERS

Normally all of these complex processes are hidden and you don't need to understand them in order to find the information you need. However, when people or organizations attempting to limit your access to information interfere with the operation of the system, your ability to use the Internet may be restricted. In that case, understanding just what they have done to interfere with your access can become extremely relevant.

Consider firewalls, which are devices that intentionally prevent certain kinds of communication between one computer and another. Firewalls help a network owner enforce policies about what kinds of communication and use of a network are allowed. Initially, the use of firewalls was conceived as a computer security measure, because they can help repel electronic attacks against inadvertently misconfigured and vulnerable computers. But firewalls have come to be used for a much wider range of purposes and for enforcing policies far beyond the purview of computer security, including content controls.

Another example is DNS servers, which were described as helping provide IP addresses corresponding to requested domain names. However, in some cases, these servers can be used as censoring mechanisms by preventing the proper IP address from being returned, and effectively blocking access to the requested information from that domain.

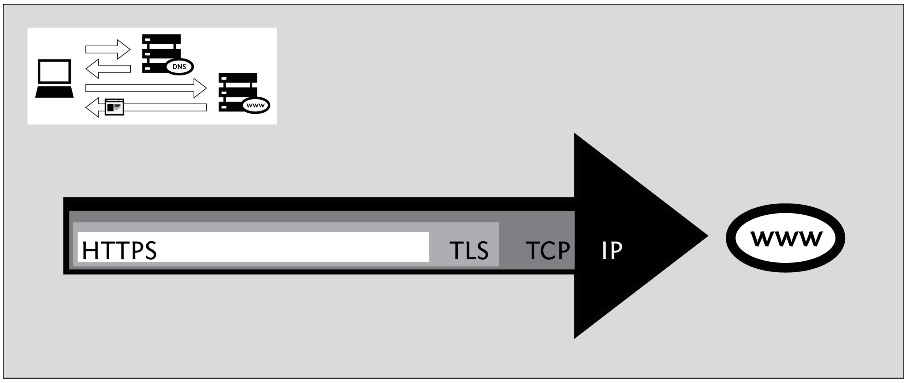
Censorship can occur at different points in the Internet infrastructure, covering whole networks, domains or subdomains, individual protocols, or specific content identified by filtering software. The best method to avoid censorship will depend on the specific censorship technique used. Understanding these differences will help you to choose appropriate measures for you to use the Internet effectively and safely.

PORTS AND PROTOCOLS

In order to share data and resources, computers need to agree on conventions about how to format and communicate information. These conventions, which we call **protocols**, are sometimes compared to the grammar of human languages. The Internet is based on a series of such protocols.

The layered networking model

Internet protocols rely on other protocols. For example, when you use a Web browser to access a Web site, the browser relies on the HTTP or HTTPS protocol to communicate with the Web server. This communication, in turn, relies on other protocols. Suppose we are using HTTPS for a particular Web site to ensure that we access it securely.



In the above example, the HTTPS protocol relies on the **TLS** protocol to perform encryption of the communications so that they are private and unmodified as they travel across the network. The TLS protocol, in turn, relies on the **TCP** protocol to ensure that information is not accidentally lost or corrupted in transmission. Finally, TCP relies on the IP protocol to ensure that data is delivered to the intended destination.

While using the encrypted HTTPS protocol, your computer still uses the unencrypted DNS protocol for retrieving an IP address for the domain name. The DNS protocol uses the **UDP** protocol to mark the request for proper routing to a DNS server, and UDP relies on IP for actual transmission of data to the intended destination.

Because of this hierarchical protocol relationship, we often refer to network protocols as existing in a set of layers. A protocol at each layer is responsible for a particular aspect of the communications functionality.

Using Ports

Computers connect to each other via the TCP protocol mentioned above and stay connected for a period of time to allow higher-level protocols to carry out their tasks. TCP uses a concept of numbered **ports** to manage these connections and distinguish connections from one another. The use of numbered ports also allows the computer to decide which particular software should handle a specific request or piece of data. (UDP also uses port numbers for this purpose.)

The **IANA** (Internet Assigned Names Authority) assigns port numbers for various higher-level protocols used by application services. A few common examples of the standard assigned port numbers are:

- 20 and 21 - FTP (file transfer)
- 22 - SSH (secure shell remote access)
- 23 - Telnet (insecure remote access)
- 25 - SMTP (send e-mail)
- 53 - DNS (resolves a computer's name to an IP address)
- 80 - HTTP (normal Web browsing; also sometimes used for a proxy)
- 110 - POP3 (receive e-mail)
- 143 - IMAP (send/receive e-mail)
- 443 - HTTPS (secure Web connections)
- 993 - secure IMAP
- 995 - secure POP3
- 1080 - SOCKS proxy
- 1194 - OpenVPN
- 3128 - Squid proxy
- 8080 - Standard HTTP-style proxy

Using these particular numbers is not generally a technical requirement of the protocols; in fact, any sort of data could be sent over any port (and using non standard ports can be a useful circumvention technique). However, these assignments are used by default, for convenience. For example, your Web browser knows that if you access a Web site without specifying any port number, it should automatically try using port 80. Other kinds of software have similar defaults so that you can normally use Internet services without knowing or remembering the port numbers associated with the services you use.

Cryptography

Cryptography is a form of technical defense against surveillance that uses sophisticated mathematical techniques to scramble communications, making them unintelligible to an eavesdropper. Cryptography can also prevent a network operator from modifying communications, or at least make such modifications detectable. It usually works like a tunnel from the software you are using, such as a Web browser, to the other end of the connection, such as a Web server.

Modern cryptography is thought to be extremely difficult to defeat by technical means; widely available cryptographic software can give users very powerful privacy protection against eavesdropping. On the other hand, encryption can be circumvented by several means, including targeted **malware**, or in general through **key-management** and **key-exchange** problems, when users cannot or do not follow the procedures necessary to use cryptography securely. For example, cryptographic applications usually need a way to verify the identity of the person or computer at the other end of a network connection; otherwise, the communication could be vulnerable to a **man-in-the-middle attack** where an eavesdropper impersonates one's communication partner in order to intercept supposedly private communications. This identity verification is handled in different ways by different software, but skipping or bypassing the verification step can increase one's vulnerability to surveillance.

Another surveillance technique is **traffic analysis**, where facts *about* a communication are used to infer something about its content, origin, destination, or meaning even if an eavesdropper is unable to understand the *contents* of the communication. Traffic analysis can be a very powerful technique and is very difficult to defend against; it is of particular concern for anonymity systems, where traffic analysis techniques might help identify an anonymous party. Advanced anonymity systems like Tor contain some measures intended to reduce the effectiveness of traffic analysis, but might still be vulnerable to it depending on the capabilities of the eavesdropper.

5. CENSORSHIP AND THE NET

Understanding how the Internet is controlled in practice can help to relate the sources of Internet censorship to the possible threats. Internet controls and censorship can be wide-ranging. A national government might not only block access to content, but also monitor what information people in its country are accessing, and might penalize users for Internet-related activities that the government deems unacceptable. Governments may both define what to block and carry out the blocking, or they may create legislation, regulations, or extra-legal incentives to compel the staff of nominally independent companies to carry out blocking and surveillance.

WHO CONTROLS THE INTERNET?

The full story of Internet governance is complicated, political and still being actively disputed. Governments often have the authority and resources to implement their preferred schemes of Internet monitoring and control, whether Internet infrastructure is owned and operated by governments themselves or by private telecommunications companies. So a government that wants to block access to information can often readily exercise direct or indirect control over points where that information is produced, or where it enters or exits the country.

Governments also have extensive legal authority to spy on citizens, and many go behind what the law allows, using *extra-legal* methods to monitor or restrict Internet use and reshape it according to their own rules.

GOVERNMENT INVOLVEMENT

The Internet was developed by U.S. government-sponsored research during the 1970s. It gradually spread to academic use, then to business and public use. Today, a global community is working to maintain the standards and agreements that attempt to achieve world-wide open connectivity and interoperability without any geographical distinction.

However, governments are not compelled to implement Internet infrastructure in accordance with these goals or related recommendations about Internet architecture. Some governments design their national telecommunications systems to have single "*choke points*" where they can control their whole country's access to specific sites and services, and in some cases prevent access to their section of the Internet from outside.

Other governments have passed laws or adopted informal controls to regulate the behavior of private ISPs, sometimes compelling them to participate in surveillance or blocking or removing access to particular materials.

Some of the Internet's facilities and coordinating functions are managed by governments or by corporations under government charter. There is no international Internet governance that operates entirely independently. Governments treat the ability to control Internet and telecommunications infrastructure as matters of national sovereignty, and many have asserted the right to forbid or block access to certain kinds of content and services deemed offensive or dangerous.

WHY WOULD GOVERNMENTS CONTROL THE NET?

Many governments have a problem with the fact that there is only one global Internet with technically no geographic or political borders. For the end-user, it makes (apart from a delay of a few milliseconds) no difference if a Web site is hosted in the same country or on the other side of the world – a reality often delightful for Internet users and deeply alarming for states. Internet censorship, inspired by hopes of re-imposing geography and geographic distinctions, can occur for many reasons.

Adapting a classification from the Open Net Initiative (http://opennet.net), we can describe some of these reasons as:

- **Political reasons**
  Governments want to censor views and opinions contrary to the respective country's policies including topics such as human rights and religions.
- **Social reasons**
  Governments want to censor Web pages related to pornography, gambling, alcohol, drugs and other subjects that might seem offensive for the population.
- **National security reasons**
  Governments want to block content related to dissident movements, and anything threatening national security.

In order to ensure that information controls are effective, governments may also filter tools that enable people to bypass Internet censorship.

In the extreme case, governments can refuse to provide Internet service to the public, as in North Korea, or can cut off the Internet throughout their territory during periods of public protest, as happened briefly in Nepal in 2005, and in Egypt and Libya in 2011.

Control can be aimed at both access providers and content providers.

- Governments can submit access providers to strict control, in order to regulate and shape Internet traffic, and enable surveillance and monitoring upon Internet users within the country. This is also a means to block global content that has been made available from abroad. For example, the Pakistani government asked local ISPs to block access to Facebook in May 2010 in order to block access to caricatures of the Prophet Muhammad that had been made available on the social networking site, as they had no control over the content provider Facebook.

- Governments can request content providers, such as in-country Web site editors, Webmasters or search engines to forbid and block access to certain kinds of content and services deemed offensive or dangerous. For example, local Google subsidiaries have been requested to remove controversial content in a couple of countries (such as in China, before March 2010, when it redirected search engine activities towards Google Hong Kong).

AM I BEING BLOCKED OR FILTERED?

In general, it can be difficult to determine whether someone is preventing you from accessing a Web site or from sending information to others. When you try to access a blocked site, you may see a conventional error message or nothing at all. The behavior may make it look like the site is inaccessible for technical reasons. The government or the ISP may deny the fact that censorship is in place and even blame the (foreign) Web site.

Some organizations, most notably the OpenNet Initiative, are using software to test Internet access in various countries and to understand how access may be compromised by different parties. In some cases, this is a difficult or even dangerous task, depending on the authorities concerned.

In some countries, there is no doubt about government blocking of parts of the Internet. In Saudi Arabia, for example, attempting to access sexually explicit material results in a noticeable message from the government explaining that the site is blocked, and why.

In countries that block without notification, one of the most common signs of censorship is that a large number of sites with related content are apparently inaccessible for technical reasons or seem to be out of order (for example, "Page Not Found" errors, or connections timing out often). Another potential indication is that search engines appear to return useless results or nothing at all about certain topics.

Filtering or blocking is also done by entities other than governments. Parents may filter the information that reaches their children. Many organizations, from schools to businesses, restrict Internet access in order to prevent users from having unmonitored communications, using company time or hardware for personal reasons, infringing copyrights, or using excessive networking resources.

Many governments have the resources and legal ability to control large portions of a country's network infrastructure. If the government is your adversary, keep in mind that the entire communications infrastructure from the Internet to mobile and landline phones can be monitored.

GEOGRAPHIC CONTEXT

Users in different places may have widely varying experiences of Internet content controls.

- In some places, your government may be legally constrained from filtering or decide not to filter content. You may be monitored by your ISP so the information can be sold to advertisers. The government may have required ISPs to install monitoring (but not blocking) capabilities in their networks. The government may make a formal request for your browsing history and chat logs, or may store information for later use. It will try not to attract attention as it does this. You face threats from non-government actors, such as computer criminals who attack Web sites or steal personal financial information.
- In some places, ISPs may use technical means to block some sites or services, but the government doesn't currently appear to track or retaliate against attempts to access them, or appear to operate a coordinated Internet content control strategy.
- In some places, you may have access to local services that are a fair match for foreign services. These services are patrolled by your ISP or government agents. You may be free to post sensitive content, but it will be removed. If this happens too often, however, the penalties may become more severe. Restrictions may only become obvious during politically charged events.
- In some places, your government may filter most foreign websites, especially news. It exercises tight control over ISPs to block content and keep track of people creating content. If you use a social networking platform, efforts will be made to infiltrate it. The government may encourage your neighbors to spy on you.

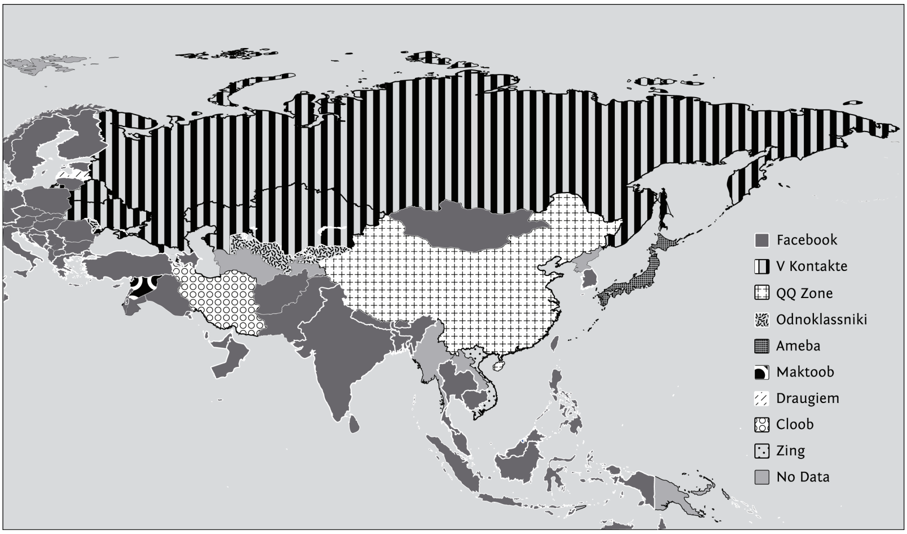
PERSONAL CONTEXT

Governments have a range of motivations for monitoring or restricting different kinds of people's online activity.

- Activists: you may want to improve your government or are seeking a new one. Perhaps you want to reform a particular segment of society or work for the rights of minority groups. You may want to expose environmental issues, labor abuses, fraud, or corruption at your place of work. Your government and employers are going to be unhappy about this no matter the time of year, but they may put more effort into monitoring you if they suspect that there will be protests in the streets soon.
- Bloggers: you may want to write about everyday life, but some people are silenced because of ethnicity or gender. Regardless of what you have to say you're not supposed to be saying it. You may be in a country with mostly unrestricted users, but your opinions are not popular in your community. You might prefer anonymity or need it to connect with a support group.
- Journalists: you may have some of the same concerns as activists and bloggers. Organized crime, corruption, and government brutality are dangerous subjects to cover. You may need to protect yourself and any activists who become sources of information.
- Readers: you may not be politically active, but so much content is censored that you need circumvention software to get to entertainment, science, and industry periodicals. You may want to read a Web comic or browse the news about other countries. Your government may ignore this until it has some other reason to monitor you.

The most commonly blocked Internet resource used to be sexually explicit material; today, it is social networking platforms. The growing international popularity of social networking sites has turned millions of Internet users around the world into potential victims of censorship.

Some social networking sites are popular at a global level, such as Facebook, MySpace or LinkedIn, while others have a large number of users in a given country or region: QQ (Qzone) in China, Cloob in Iran, vKontakte in Russia, Hi5 in Peru and Colombia, Odnoklassniki in CIS countries, Orkut in India and Brazil, Zing in Vietnam, Maktoob in Syria, Ameba and Mixi in Japan, Bebo in the UK, and others.



HOW CENSORSHIP WORKS

[This is adapted in part from *Access Denied*, Chapter 3, by Steven J. Murdoch and Ross Anderson.]

The techniques described in this chapter are some of the methods employed by censors that try to prevent Internet users from accessing particular content or services. Network operators can filter or manipulate Internet traffic at any point in a network, using a wide variety of technologies, with varying levels of accuracy and customization. Typically, these maneuvers involve using software to look at what users are attempting to do and to interfere selectively with activities that the operator considers forbidden by policy. A filter could be created and applied by a national government or by a national or local ISP, or even by the operator of a local network; or software-based filters could be installed directly onto individual computers.

The goals of deploying a filtering mechanism vary depending on the motivations of the organization deploying them. They may be to make a particular Web site (or individual Web page) inaccessible to those who wish to view it, to make it unreliable, or to deter users from even attempting to access it in the first place. The choice of mechanism will also depend upon the capability of the organization that requests the filtering – what access and influence they have, the people against whom they can enforce their wishes, and how much they are willing to spend. Other considerations include the number of acceptable errors, whether the filtering should be overt or covert, and how reliable it is (both against casual users and those who wish to bypass it).

We will describe several techniques by which particular content can be blocked once the list of resources to be blocked is established. Building this list is a considerable challenge and a common weakness in deployed systems. Not only does the huge number of Web sites make building a comprehensive list of prohibited content difficult, but as content moves and Web sites change their IP addresses, keeping this list up-to-date requires a lot of effort. Moreover, if the operator of a site wishes to interfere with the blocking, the site could be moved more rapidly than it would be otherwise.

We first describe technical measures used against end users, and then briefly discuss measures used against publishers and hosting providers, as well as non-technical intimidation.

Please note that the list of methods is not exhaustive, and more than one of these tactics might be applied in a particular case.

TECHNICAL MEASURES AGAINST END-USERS

On modern communications networks like the Internet, censorship and surveillance (the monitoring of people's communications or activities) are intimately connected in practice.

Most ISPs in the world monitor some aspects of their users' communications for accounting purposes and to combat abuse such as spam. ISPs often record user account names together with IP addresses. Unless users employ privacy-enhancing technologies to prevent it, it is technically possible for an ISP to record *all* the information that flows over its cables, including the exact contents of users' communications.

This surveillance is also a prerequisite for technically-based network censorship. An ISP trying to censor communications that its users want to send has to be able to read those communications in order to determine which ones violate its policies. Hence a core approach to reducing Internet censorship is hiding the detailed content of communications from ISPs, both in individual cases and by encouraging widespread use of pro-privacy technologies that hinder surveillance.

This means that technical counter-measures to network censorship often rely on using obfuscation or encryption wherever possible in order to make it impossible for the ISP to see exactly what content has been transferred.

This section discusses some of the specific ways that censors block content and access by technical means.

URL filtering

One way for countries and other entities to block access to information on the Web is to prevent access based on the **URL** – either the entire URL or some part of it. Internet censors often want to block specific **domain names** in their entirety, because they object to the content of those domains. One of the easiest ways to block Web sites is by blocking the complete domain name. Sometimes, authorities are more selective, blocking only certain **subdomains** in a particular domain, while leaving the rest of the domain accessible. This is the case for Vietnam, where the government blocks specific sections of a Web site (such as the Vietnamese-language versions of the BBC and Radio Free Asia) but rarely censors content written in English.

Censors, for example, might filter only the subdomain news.bbc.co.uk, while leaving bbc.co.uk and www.bbc.co.uk unfiltered. Similarly, they might want to filter out pages containing specific types of content while allowing access to the rest of the domain hosting those pages. One filtering approach is to look for a directory name, such as "worldservice" to block only the BBC foreign-language news service at bbc.co.uk/worldservice, without blocking the BBC's English-language Web site as a whole. Censors can sometimes even block specific pages based on page names, or search terms in queries, that suggest offensive or undesired content.

URL filtering can be performed locally, through the use of special software installed in the computer that you are using. For example, computers in an Internet café may all be running filtering software that prevents certain sites from being accessed.

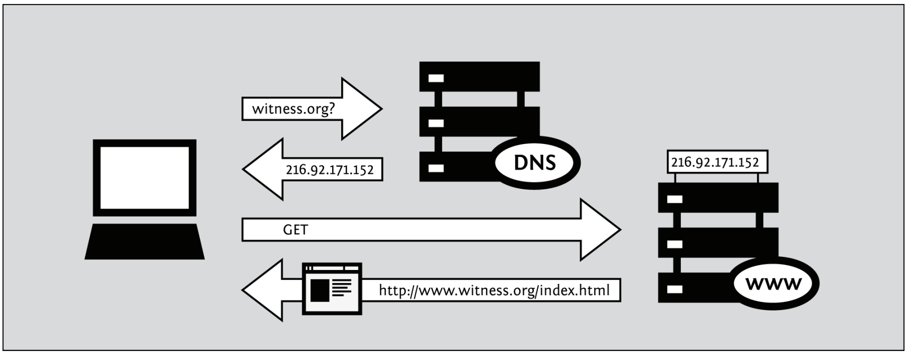
URL filtering can also be performed at a central point in the network, such as a **proxy server**. A network can be configured not to allow users to connect directly to Web sites but instead to force (or just encourage) all users to access those sites via a proxy server.

Proxy servers are used to relay requests, as well as temporarily storing web pages they retrieve in a cache and delivering them to multiple users. This reduces the need for an ISP to frequently retrieve a popularly requested page, thus saving on resources and improving delivery time.

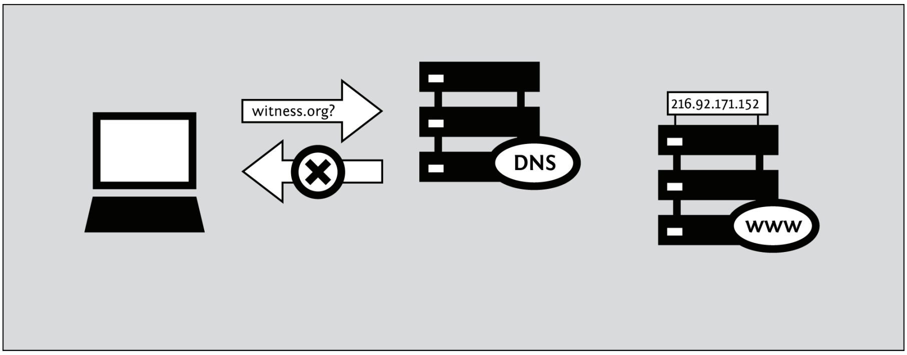
However, as well as improving performance, an HTTP proxy can also block Web sites. The proxy decides whether requests for Web pages should be permitted, and if so, sends the request to the Web server hosting the requested content. Since the full content of the request is available, individual Web pages can be filtered, based on both page names and the actual content of the page. If a page is blocked, the proxy server could return an accurate explanation of the reason why, or pretend that the page didn't exist or produced an error.

DNS filtering and spoofing

When you enter a URL in a Web browser, the first thing the Web browser does is to ask a **DNS (Domain Name System)** server, at a known numeric address, to look up the domain name referenced in the URL and supply the corresponding IP address.



If the DNS server is configured to block access, it consults a **blacklist** of banned domain names. When a browser requests the IP address for one of these domain names, the DNS server gives a wrong answer or no answer at all.



When the DNS server gives a meaningless answer or no answer, the requesting computer fails to learn the correct IP address for the service it wanted to contact. Without the correct IP address, the requesting computer cannot continue, and it displays an error message. Since the browser does not learn the Web site's correct IP address, it is not able to contact the site to request a page. The result is that all of the services under a particular domain name, such as all of the pages on a particular Web server, are unavailable. In this case, deliberate blocking may wrongly appear as a technical problem or random failure.

Similarly, a censor could force a DNS entry to point to an incorrect IP address, thus redirecting Internet users to incorrect Web sites. This technique is called **DNS spoofing**, and censors can use it to hijack the identity of a particular server and display forged Web sites or reroute the users' traffic to unauthorized servers that could intercept their data. (In some networks, the wrong answer would lead to a different Web server that clearly explains the nature of the blocking that has occurred. This technique is used by censors who don't mind admitting that they are engaged in censorship and who don't want users to be confused about what has taken place.)

IP filtering

When data is sent over the Internet, it is grouped into small units, called **packets**. A packet contains both the data being sent and information about how to send the packet, such as the IP addresses of the computer it came from and the one it should go to. **Routers** are computers that relay packets on their way from a sender to a receiver, determining where they go next. If censors wants to prevent users from accessing specific servers, they can configure routers that they control to **drop** (ignore and fail to transmit) data destined for IP addresses on a blacklist or to return an error message for them. Filtering based solely on IP addresses blocks *all* services provided by a particular server, such as both Web sites and e-mail servers. Since only the IP address is inspected, multiple **domain names** that share the same IP address are also blocked, even if only one was originally meant to be prohibited.

Keyword filtering

IP address filtering can only block communication on the basis of where packets are going to or coming from, not what they contain. This can be a problem for the censor if it is impossible to establish the full list of IP addresses containing prohibited content, or if an IP address contains enough non-prohibited content to make it seem unjustifiable to totally block all communication with it. There is a finer-grained control possible: the content of packets can be inspected for banned keywords. As network routers do not normally examine the entire packet contents, extra equipment may be needed; the process of examining packet contents is often called **deep packet inspection**.

A communication identified as containing forbidden content may be disrupted by blocking the packets directly or by forging a message to both of the communicating parties advising them that the other party has terminated the conversation. Equipment that performs all of these censoring functions and others is readily available on the market.

Alternatively, the censor can use a forced HTTP proxy, as described earlier.

Traffic shaping

Traffic shaping is a technique utilized by network managers to make a network run smoothly by prioritizing some kinds of packets and delaying other kinds of packets that meet certain criteria. Traffic shaping is somewhat similar to controlling vehicle traffic on a street. In general, all vehicles (packets) have the same priority, but some vehicles are temporarily delayed by traffic controllers or stop lights to avoid traffic jams at certain points. At the same time, some vehicles (fire trucks, ambulances) may need to reach their destination faster, and therefore they are given priority by delaying other vehicles. Similar logic is applicable to Internet packets that need low **latency** for optimal performance (such as **voice over IP, VoIP**).

Traffic shaping can also be used by governments or other entities to delay packets with specific information. If censors want to restrict access to certain services, they can easily identify packets related to these services and increase their latency by setting their priority low. This could give users the misleading impression that a site is inherently slow or unreliable, or it could simply make the disfavored site unpleasant to use relative to other sites. This technique is sometimes used against peer-to-peer file-sharing networks, such as **BitTorrent**, by ISPs that disfavor file sharing.

Port blocking

Blacklisting individual port numbers restricts access to individual services on a server, such as Web or e-mail. Common services on the Internet have characteristic port numbers. The relationships between services and port numbers are assigned by IANA, but they are not mandatory. These assignments allow routers to make a guess as to the service being accessed. Thus, to block just the Web traffic to a site, a censor might block only port 80, because that is the port typically used for Web access.

Access to ports may be controlled by the network administrator of the organization that hosts the computer you're using – whether a private company or an Internet café, by the ISP that is providing Internet access, or by someone else such as a government censor who has access to the connections that are available to the ISP. Ports may also be blocked for reasons other than pure content censorship – to reduce spam, or to discourage disfavored network uses such as peer-to-peer file sharing, instant messaging, or network gaming.

If a port is blocked, all traffic on this port becomes inaccessible to you. Censors often block the ports 1080, 3128, and 8080 because these are the most common proxy ports. If this is the case, you won't be able to directly use any proxies that require use of those ports; you'll have to use a different circumvention technique or else find or arrange for the creation of proxies that are listening on an uncommon port.

For example, in one university, only the ports 22 (SSH), 110 (POP3), 143 (IMAP), 993 (secure IMAP), 995 (secure POP3) and 5190 (ICQ instant messaging) may be open for external connections, forcing users to use circumvention technology or access services on nonstandard ports if they want to use other Internet services.

Internet shutdown

Shutting down Internet connectivity is an example of extreme censorship perpetrated by governments in response to sensitive political and social events. However, complete network disruption (i.e. from both domestic and international networks) requires intense work, since it is necessary to shut down not only the protocols that connect the country to the international network but also the protocols that connect ISPs with one another and with users. Countries have shut down Internet access completely (Nepal in 2005, Burma in 2007 and Egypt and Libya in 2011) as a means to quell political unrest. These shutdowns lasted from a few hours to several weeks, though some people managed to connect through dial-up to an ISP abroad or by using mobile connections or satellite links.

Breaking international connections, therefore, does not necessarily destroy connectivity among domestic ISPs or communication among various users of a single ISP. It would take further steps to completely isolate users from an internal network. For this reason, it is harder to disrupt local interconnectivity in countries with several ISPs.

ATTACKS ON PUBLISHERS

Censors can also try to suppress content and services at their source by attacking the publishers' ability to publish or host information. This can be accomplished in several ways.

Legal restrictions

Sometimes, legal authorities can induce service operators themselves to perform or cooperate with censorship. Some blog hosts or e-mail providers, for example, may decide to perform keyword filtering within their own servers – perhaps because governments told them to. (In this case, there's little hope that any sort of "circumvention" will counteract these services' censorship; we generally conceive of circumvention as an effort to reach desired network services somewhere else, such as in a different country or jurisdiction.)

Denial of service

Where the organization deploying the filtering does not have the authority (or access to the network infrastructure) to add conventional blocking mechanisms, Web sites can be made inaccessible by overloading the server or network connection. This technique, known as a Denial-of-Service (DoS) attack, could be mounted by one computer with a very fast network connection; more commonly, a large number of computers are taken over and used to mount a distributed DoS (**DDoS**).

Domain deregistration

As mentioned earlier, the first stage of a Web request is to contact the local DNS server to find the IP address of the desired location. Storing all domain names in existence would be unfeasible, so instead so-called "recursive resolvers" store pointers to other DNS servers that are more likely to know the answer. These servers will direct the recursive resolver to further DNS servers until one, the "authoritative" server, can return the answer.

The domain name system is organized hierarchically, with country domains such as ".uk" and ".de" at the top, along with the nongeographic top-level domains such as ".org" and ".com". The servers responsible for these domains delegate responsibility for subdomains, such as example.com, to other DNS servers, directing requests for these domains there. Thus, if the DNS server for a top-level domain deregisters a domain name, recursive resolvers will be unable to discover the IP address and so make the site inaccessible.

Country-specific top-level domains are usually operated by the government of the country in question, or by an organization appointed by it. So if a site is registered under the domain of a country that prohibits the hosted content, it runs the risk of being deregistered.

Server takedown

Servers hosting content must be physically located somewhere, as must the administrators who operate them. If these locations are under the legal or extra-legal control of someone who objects to the content hosted, the server can be disconnected or the operators can be required to disable it.

INTIMIDATION OF USERS

Censors may also try to deter users from even attempting to access banned material in various ways.

Surveillance

The above mechanisms inhibit the access to banned material, but are both crude and possible to circumvent. Another approach, which may be applied in parallel to filtering, is to monitor which Web sites are being visited. If prohibited content is accessed (or attempted to be accessed) then legal (or extra-legal) measures could be deployed as punishment.

If this fact is widely publicized, it could discourage others from attempting to access banned content, even if the technical measures for preventing access are inadequate by themselves. In some places, censors try to create an impression that their agents are everywhere and that everyone is constantly being watched – whether or not this really is the case.

Social Techniques

Social mechanisms are often used to discourage users from accessing inappropriate content. For example, families may place the PC in the living room where the screen is visible to all present, rather than somewhere more private, as a low-key way of discouraging children from accessing unsuitable sites. A library may situate PCs so that their screens are all visible from the librarian's desk. An Internet café may have a CCTV surveillance camera. There might be a local law requiring such cameras, and also requiring that users register with government-issued photo ID.

Stealing and destroying communications equipment

In some places, censors have the ability to prohibit some kinds of communications technology entirely. In that case, they may conspicuously confiscate or seek out and destroy prohibited communications equipment in order to send the message that its use will not be tolerated.

6. CIRCUMVENTION AND SAFETY

The type of security you need depends on your activities and their consequences. There are some security measures that everyone should practice whether they feel threatened or not. Some ways to be cautious online require more effort, but are necessary because of severe restrictions on Internet access. You may be facing threats from technology that is being researched and deployed rapidly, old technology, use of human intelligence instead, or a combination of all three. All of these factors may change often.

SOME SECURITY BEST-PRACTICES

There are steps that everyone with a computer should take to keep it secure. This may involve protecting information about your network of activists or it could be your credit card number, but some of the tools you need are the same.

Beware of programs that promise perfect security: online safety is a combination of good software *and* human behavior. Knowing what should be kept offline, who to trust, and other security questions cannot be answered by technology alone. Look for programs that list risks on their Web sites or have been peer reviewed.

Keep your operating system up-to-date: the developers of operating systems provide updates that you should install from time to time. These may be automatic or you may have to request them by entering a command or adjusting your system settings. Some of these updates make your computer more efficient and easier to use, and others fix security holes. Attackers learn about these security holes rapidly, sometimes even before they're fixed, so fixing them promptly is crucial.

If you're still using Microsoft Windows, use anti-virus software and keep it updated. Malware is software written in order to steal information or to use your computer for other purposes. Viruses and malware can gain access to your system, make changes and hide themselves. They could be sent to you in an e-mail, be on a Web page you visit, or be part of a file that does not appear to be suspicious. Anti-virus software providers constantly research emerging threats and add them to lists of things that your computer will block. In order to allow the software to recognize new threats, you must install updates as they are released.

Use good passwords: no password selection system can guard against being threatened with violence, but you can improve your security by making it harder to guess. Use combinations of letters, punctuation, and numbers. Combine lower and upper case letters. Do not use birthdates, telephone numbers, or words that can be guessed by going through public information about you.

Use Free and Open Source Software (FOSS). Open source software is made available both as a working product and as a work in progress to users and software engineers. This offers several security advantages over closed source, for-profit software that may only be available in your country through illegal channels due to export restrictions or expense. You may not be able to download official updates for pirated software. With Open Source software there is no need to search through several suspicious sites for a copy free of spyware and security glitches. Any legitimate copy will be free and is available from the creators. If security flaws emerge, they can be spotted by volunteers or interested users. A community of software engineers will then work on a solution, often very quickly.

Use software that separates who you are from where you are. Every computer connected to the Internet has an IP address. An IP address can be used to find your physical location as easily as typing it into a public "whois" site. Proxies, VPNs and Tor route your traffic through one to three computers around the world. If you are going through only one server, be aware that just like an ISP, the proxy provider can see all of your traffic. You may trust the proxy provider more than your ISP, but the same warnings apply to any single source of connectivity. See the sections that cover proxies, Tor, and VPNs for more on risks.

Use live CDs and bootable USB drives. If you are using a public computer or another computer on which you do not want to leave data, use a version of Linux that you can run from portable media. A Live CD or bootable USB drive can be plugged into a computer and used without installing anything.

Use "portable" programs: there are also portable versions of circumvention software that can be run under Windows from a USB drive.

Keep yourself updated: the effort put into finding you may change. The technology that works one day may stop working or be insecure the next day. Even if you don't need it now, know where to find information. If the software providers you use have ways to get support, make sure you know about them before their Web sites are blocked.

SAFER ACCESS TO SOCIAL NETWORKING SITES

In the context of closed societies and repressive countries, monitoring becomes a major threat for users of social networking sites, especially if they use the service to coordinate civil society activity or engage in online activism or citizen journalism.

One central issue with social networking platforms is the amount of private data that you share about yourself, your activities and your contacts, and who has access to it. As the technology evolves and social networking platforms are more and more accessed through smart phones, the disclosure of the locations of the users of a social networking platform at any given moment is also becoming a significant menace.

In that context, some precautions become even more crucial; for example, you should:

- edit your default privacy settings in the social networking platform
- know precisely what information you are sharing with whom
- make sure that you understand the default geolocation settings, and edit them if needed
- only accept into your network people who you really know and trust
- only accept into your network people who will be savvy enough to also protect the private information that you share with them, or train them to do so
- be aware that even the most savvy people in your network might give up information if they are threatened by your adversary, so consider limiting who has access to which information
- be aware that accessing your social networking platform via a circumvention tool will *not* automatically protect you from most of the threats to your privacy.

Read more in this article from Privacy Rights Clearinghouse: "Social Networking Privacy: How to be Safe, Secure and Social": http://www.privacyrights.org/social-networking-privacy/#general-tips

How can you access your social networking platform when it is filtered?

As described below, using HTTPS to access Web sites is important. If your social networking platform allows HTTPS access, you should use it exclusively, and, if possible, make it the default. For example, on Facebook, you can edit Account Settings > Account Security > Secure Browsing (https) to make HTTPS the default way to connect to your Facebook account. In some places, using HTTPS may also allow you to access to an otherwise blocked service; for example, http://twitter.com/ has been blocked in Burma while https://twitter.com/ remained accessible.

If you want to protect your anonymity and privacy while circumventing the filtering imposed on your social networking service, an SSH tunnel or VPN will give you stronger privacy guarantees than a Web proxy, including against the risk of revealing your IP address. Even using an anonymity network like Tor can be insufficient because social networking platforms make it so easy to reveal identifying information and expose details about your contacts and social relationships.

SAFER USE OF SHARED COMPUTERS

A significant proportion of the world's population, especially in developing countries, does not have personal access to the Internet at their homes. This can be because of the costs of having private Internet connection at their homes, the lack of personal computer equipment, or problems in the telecommunication or electrical network infrastructures.

For this portion of the population the only existing, convenient or affordable mean to access the Internet is to use places where the computers are shared with several different individuals. This includes Internet cafés, Telecenters, work stations, schools or libraries.

Potential advantages of shared computers

There are advantages to accessing the Internet on shared computers:

- You may receive technical advice and assistance from other users or facility staff on how to circumvent filtering.
- Circumvention tools may already be installed and pre-configured.
- Other users may share uncensored information with you through alternative, offline means.
- If you aren't a regular user of a particular computing facility, you didn't provide identity documents to the facility's operator, and you don't sign in online using your real name or account information, it would be hard for anyone to track you down personally based on your online activity.

General risks of shared computers

The fact that you access the Internet in a public space does not make it anonymous or safe for you. It is quite often the very opposite. Some of the main threats are:

- The owner of the computer, or even a person who used the computer before you, could easily program the computer to spy on everything you do, including recording all of your passwords. The computer can also be programmed to circumvent or nullify the protections of any privacy and security software you use on it.
- In some countries, such as Burma and Cuba, Internet café clients are required to show their ID or passport before using the service. This ID information can be stored and filed together with the clients' Web browsing history.
- Any data you leave on the computer you have used may be logged (browsing history, cookies, downloaded files, etc).
- Software or hardware keyloggers installed in the client's computer may record every keystroke during your session, including your passwords, even before this information is sent over the Internet. In Vietnam, an apparently innocuous virtual keyboard for typing Vietnamese characters was being used by the government to monitor user activity at Internet cafés and other public access spots.
- Your screen activity may be recorded by special software that takes screenshots at frequent intervals, monitored through CCTV cameras, or simply observed by a person (e.g. the Internet café manager) looking over your shoulder.

Shared computers and censorship

Besides the surveillance, users of shared computers are often offered access to a limited Internet and have to face additional hurdles to use their favorite circumvention solution:

- In some countries, such as Burma, Internet café owners have to display posters about banned Web content and are responsible for the enforcement censorship law inside their business.
- Extra filtering might be implemented by Internet café managers (client side control and filtering), to complement filtering implemented at the ISP or national level.
- Users might be pushed by the environmental restrictions to avoid visiting specific Web sites for fear of punishment, thus enforcing self-censorship.
- Computers are often configured so that users are prevented from installing any software, including circumvention tools, or connecting any kind of devices to the USB port (such as USB flash drives). In Cuba, authorities have begun deploying a controlling software for Internet cafés named AvilaLink that prevents users from installing or executing specific software or running applications from a USB flash drive.
- Users may be prevented from using any other browser but Internet Explorer, to prevent the use of privacy or circumvention Add-ons or settings for browsers such as Mozilla Firefox or Google Chrome.

Best practices for security and circumvention

Depending on the environment in which you use your shared computer, you can try the following:

- Identify the surveillance measures implemented based on the list mentioned above (CCTV, human surveillance, keyloggers, etc.) and behave accordingly.

- Run portable circumvention software from a USB flash drive.
- Use an operating system on which you have control through the use of a Live CD.
- Change Internet cafés often if you fear recurring surveillance, or stick to one where you trust it is safe to connect.
- Take your own laptop to the Internet café and use it instead of the public computers.

CONFIDENTIALITY AND HTTPS

Some filtered networks use mainly (or exclusively) keyword filtering, rather than blocking particular sites. For example, networks might block any communication mentioning keywords that are considered politically, religiously, or culturally sensitive. This blocking can be overt or disguised as a technical error. For example, some networks make it look like a technical error occurred whenever you search for something that the network operator thinks you shouldn't be looking for. This way, users are less likely to blame the problem on censorship.

If the content of Internet communications is unencrypted, it will be visible to ISPs' network equipment such as routers and firewalls, where keyword-based monitoring and censorship can be implemented. Hiding the content of communications with encryption makes the task of censorship much more difficult, because network equipment can no longer distinguish the communications that contain forbidden keywords from those that don't.

Using encryption to keep communications confidential also prevents network equipment from logging communications in order to analyze them and target individuals after the fact for what they read or write.

What is HTTPS?

HTTPS is the secure version of the HTTP protocol used to access Web sites. It provides a security upgrade for accessing Web sites by using encryption to stop eavesdropping and tampering with the contents of your communications. Using HTTPS to access a site can prevent network operators from knowing which part of the site you're using or what information you sent to and received from the site. HTTPS support is already included in every popular Web browser, so you don't need to install or add any software in order to use HTTPS.

Usually, if a site is available through HTTPS, you can access the site's secure version by entering its address (URL) beginning with **https://** instead of **http://**. You can also tell if you are using the secure version of a site by looking at the address displayed in your Web browser's navigation bar, and seeing whether it begins with **https://**.

Not every Web site has an HTTPS version. Indeed, perhaps less than 10% of sites do – though the sites with HTTPS versions include several of the largest and most popular sites. A Web site is only available through HTTPS if the Web site operator deliberately configures its HTTPS version. Internet security experts have been urging Web site operators to do this routinely, and the number of sites with HTTPS support has been growing steadily.

If you try to access a site through HTTPS and receive an error, this doesn't always mean that your network is blocking access to the site. It might mean that the site is simply not available in HTTPS (to anyone). However, certain kinds of error messages are more likely to show that someone is actively blocking or tampering with the connection, especially if you know that a site is supposed to be available through HTTPS.

Examples of sites that offer HTTPS

Here are a few examples of popular sites that offer HTTPS. In some cases, the use of HTTPS is optional on these sites, not mandatory, so you have to explicitly choose the secure version of the site in order to get the benefits of HTTPS.

Site name	Insecure (HTTP) version	Secure (HTTPS) version
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/

For example, if you make a Google search from https://encrypted.google.com/ instead of http://www.google.com/, your network operator will not be able to see what terms you searched for, and therefore it can't block Google from answering "inappropriate" searches. (However, the network operator could decide to block encrypted.google.com in its entirety.) Similarly, if you use Twitter through https://twitter.com/ instead of http://twitter.com/, the network operator can't see which tweets you are reading, what tags you are searching for, what you post there, or which account you log into. (However, the network operator could decide to block all access to twitter.com using HTTPS.)

HTTPS and SSL

HTTPS makes use of an Internet security protocol called TLS (Transport Layer Security) or SSL (Secure Sockets Layer). You may hear people refer to a site "using SSL" or being "an SSL site". In the context of a Web site, this means that the site is available through HTTPS.

Using HTTPS in addition to circumvention technology

Even circumvention technologies that use encryption are not a substitute for using HTTPS, because the purpose for which encryption is used is different.

For many kinds of circumvention technology, including VPNs, proxies, and Tor, it is still possible and appropriate to use HTTPS addresses when accessing a blocked site through the circumvention technology. This provides greater privacy and prevents the circumvention provider itself from observing or recording what you do. This could be important even if you're confident that the circumvention provider is friendly to you, because the circumvention provider (or the network that the circumvention provider uses) could be broken into or pressured to provide information about you.

Some circumvention technology developers like Tor strongly urge users to always use HTTPS, to make sure that circumvention providers themselves can't spy on users. You can read more about this issue at https://blog.torproject.org/blog/plaintext-over-tor-still-plaintext. It's good to get in the habit of using HTTPS whenever possible, even when using some other method for circumvention.

Tips for using HTTPS

If you like to **bookmark** sites that you access frequently so that you don't have to type in the full site address, remember to bookmark the secure version of each site instead of the insecure version.

In Firefox, you can install the HTTPS Everywhere extension to turn on HTTPS automatically whenever you visit a site that's known to offer HTTPS. It is available from https://www.eff.org/https-everywhere/.

Risks when not using HTTPS

When you don't use HTTPS, a network operator such as your ISP or a national firewall operator, can record everything you do – including the contents of the specific pages that you access. They can use this information to block particular pages or to create records that might be used against you later on. They can also modify the contents of Web pages to delete certain information or to add malicious software to spy on you or infect your computer. In many cases, other users of the same network can also do these things even if they aren't officially the network operator.

In 2010, some of these problems were dramatized by a program called Firesheep, which makes it extremely easy for users on a network to take over other users' social networking site accounts. Firesheep works because, at the time it was created, these social networking sites were not commonly using HTTPS, or were using it in a limited way to protect only some portions of their sites. This demonstration created a lot of attention in international media, and also led more sites to require the use of HTTPS or to offer HTTPS access as an option. It also allowed technically unskilled people to abuse others by breaking into their accounts.

In January 2011, during a period of political unrest in Tunisia, the Tunisian government began tampering with users' connections to Facebook in a way that allowed the government to steal users' passwords. This was done by modifying the Facebook login page and invisibly adding software that sent a copy of the user's Facebook password to the authorities. Such modifications are technically straightforward to perform and could be done by any network operator at any time. As far as we know, Tunisian Facebook users who were using HTTPS were totally protected from this attack.

Risks when using HTTPS

When it's available, using HTTPS is almost always safer than using HTTP. Even if something goes wrong, it shouldn't make your communications any easier to spy on or filter. So it makes sense to try to use HTTPS where you can (but be aware that, in principle, using encryption could be restricted by law in some countries). However, there are some ways that HTTPS might not provide complete protection.

Certificate warnings

Sometimes, when you try to access a web site over HTTPS, your Web browser will show you a warning message describing a problem with the site's **digital certificate**. The certificate is used to ensure the security of the connection. *These warning messages exist to protect you against attacks; please don't ignore them.* If you ignore or bypass certificate warnings, you may still be able to use a site but limit the ability of the HTTPS technology to protect your communications. In that case, your access to the site could become no more secure than an ordinary HTTP connection.

If you encounter a certificate warning, you should report it by e-mail to the Webmaster of the site you were trying to access, to encourage the site to fix the problem.

If you're using an HTTPS site set up by an individual, such as some kinds of Web proxies, you might receive an certificate error because the certificate is **self-signed**, meaning that there is no basis given for your browser to determine whether or not the communication is being intercepted. For some such sites, you might have no alternative but to accept the self-signed certificate if you want to use the site. However, you could try to confirm via another channel, like e-mail or instant messaging, that the certificate is the one you should expect, or see whether it looks the same when using a different Internet connection from a different computer.

Mixed content

A single Web page is usually made up of many different elements, which can come from different places and be transferred separately from one another. Sometimes a site will use HTTPS for some of the elements of a Web page but use insecure HTTP for the others. For example, a site might allow only HTTP for accessing certain images. As of February 2011, Wikipedia's secure site has this problem; although the text of Wikipedia pages can be loaded using HTTPS, all of the images are loaded using HTTP, and so particular images can be identified and blocked, or used to determine which Wikipedia page is a user is reading.

Redirection to insecure HTTP version of a site

Some sites use HTTPS in a limited way and will force users back to using insecure HTTP access even after the user initially used HTTPS access. For example, some sites use HTTPS for login pages, where users enter their account information, but then HTTP for other pages after the user has logged in. This kind of configuration leaves users vulnerable to surveillance. You should be aware that, if you get sent back to an insecure page during the course of using a site, you no longer have the protections of HTTPS.

Networks and firewalls blocking HTTPS

Because of the way HTTPS hinders monitoring and blocking, some networks will completely block HTTPS access to particular Web sites, or even block the use of HTTPS altogether. In that case, you may be limited to using insecure access to those sites while on those networks. You might find that you're unable to access a site because of blocking of HTTPS. If you use HTTPS Everywhere or certain similar software, you may not be able to use some sites at all because this software does not permit an insecure connection.

If your network blocks HTTPS, you should assume that the network operator can see and record all of your Web browsing activities on the network. In that case, you may want to explore other circumvention techniques, particularly those that provide other forms of encryption, such as VPNs and SSH proxies.

Using HTTPS from an insecure computer

HTTPS only protects the contents of your communications while they travel over the Internet. It doesn't protect your computer or the contents of your screen or hard drive. If the computer you use is shared or otherwise insecure, it could contain monitoring or spying software, or censorship software that records or blocks sensitive keywords. In that case, the protection offered by HTTPS could be less relevant, since monitoring and censorship could happen within your computer itself, instead of at a network firewall.

Vulnerability of HTTPS certificate system

There are problems with the certificate authority system, also called **public-key infrastructure** (PKI) used to authenticate HTTPS connections. This could mean that a sophisticated attacker could trick your browser into not displaying a warning during an attack, if the attacker has the right kind of resources. It has not yet been clearly documented that this is taking place anywhere. This is not a reason to avoid using HTTPS, since even in the worst case, the HTTPS connection would be no less secure than an HTTP connection.

BASIC TECHNIQUES
7. Simple Tricks
8. Get Creative
9. Web Proxies
10. Psiphon
11. SabzProxy

7. SIMPLE TRICKS

There are a number of techniques to get past Internet filtering. If your aim is simply to reach pages or services on the Internet that are blocked from your location, and you are not concerned whether other people can detect and monitor your circumvention, these techniques may be all you need:

- HTTPS
- using alternative domain names or URLs to reach blocked content
- using third-party Web sites to reach blocked content
- using e-mail gateways to retrieve blocked Web pages over e-mail.

USING HTTPS

HTTPS is the secure version of the HTTP protocol used to access Web sites.

In certain countries, and if the site you want to see has enabled HTTPS, just entering its address (URL) beginning with **https://** instead of **http://** may allow you to access the site, even when the http:// URL is blocked.

For instance http://twitter.com/ has been blocked in Burma, whereas https://twitter.com/ has been accessible.

Before trying any other circumvention tool or technique, try adding an s after http in the URL of your target site, if the http:// URL has been blocked. If this works, not only you will access the target site, but the traffic between you and the site will also be encrypted.

For extra details on this technique, read the chapters "Confidentiality and HTTPS" and "HTTPS Everywhere".

USING ALTERNATE DOMAIN NAMES OR URLS

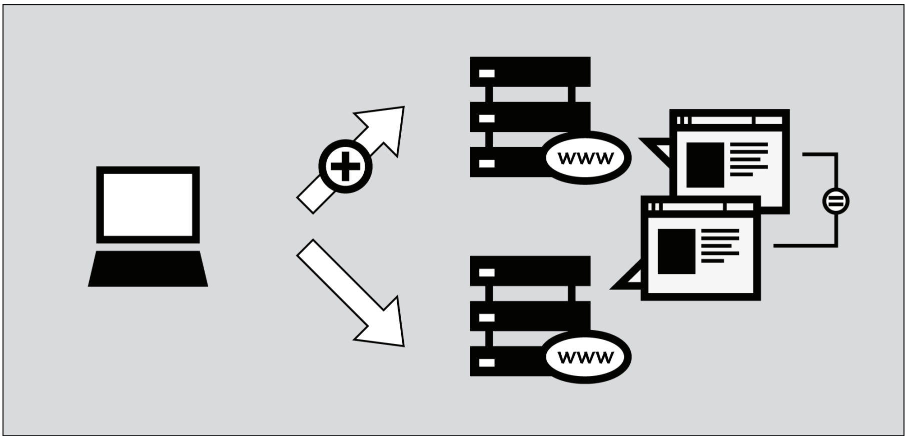
One of the most common ways to censor a Web site is to block access to its domain name, for example, "news.bbc.co.uk". However, sites are often accessible at other domain names, such as "newsrss.bbc.co.uk". If one domain name is blocked, try to find out if the content is available at another domain.

You could also try to access special versions that some Web sites create for **smartphones**. These are often the same URL with the addition of "m" or "mobile" at the beginning, for example:

- 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.com

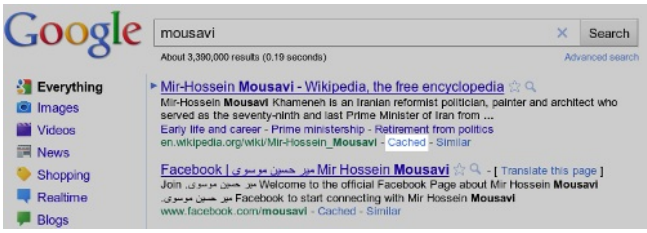
USING THIRD-PARTY SITES

There are a number of different ways you can reach the content on a Web page by going through a third-party web site rather than directly to the source Web site.



Cached Pages

Many search engines keep copies of Web pages they have previously indexed, called **cached** pages. When searching for a Web site, look for a small link labeled "cached" next to your search results. Since you are retrieving a copy of the blocked page from the search engine's servers, and not from the blocked Web site itself, you may be able to access the blocked content. However, some countries have targeted caching services for blocking as well.



About 3,390,000 results (0.19 seconds)

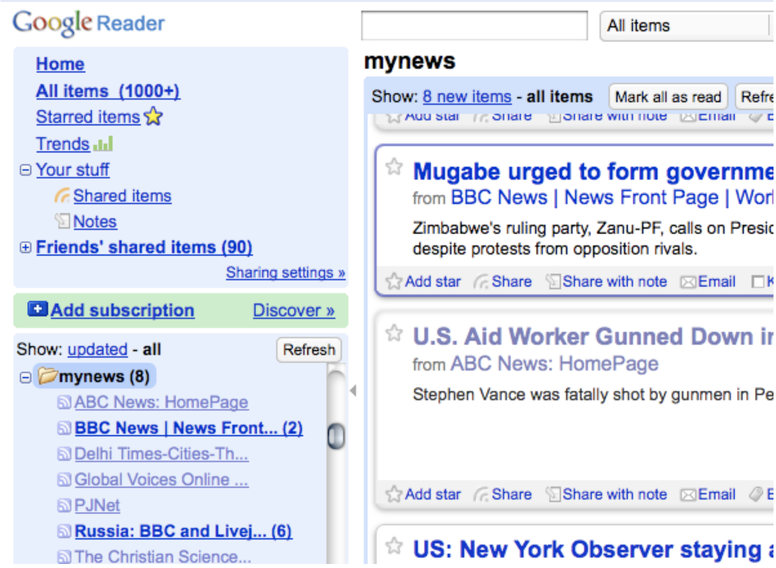
Mir-Hossein **Mousavi** - Wikipedia, the free encyclopedia
Mir-Hossein **Mousavi** Khameneh is an Iranian reformist politician, painter and architect who served as the seventy-ninth and last Prime Minister of Iran from ...
Early life and career - Prime ministership - Retirement from politics
en.wikipedia.org/wiki/Mir-Hossein_**Mousavi** - Cached - Similar

Facebook | میر حسین موسوی Mir Hossein **Mousavi** - [Translate this page]
Join .میر حسین موسوی Welcome to the official Facebook Page about Mir Hossein **Mousavi**
.میر حسین موسوی Facebook to start connecting with Mir Hossein **Mousavi**
www.facebook.com/**mousavi** - Cached - Similar

RSS Aggregators

RSS aggregators are Web sites that allow you to subscribe to and read **RSS feeds**, which are streams of news or other information put out by sites you have chosen. (RSS stands for "Really Simple Syndication"; for more on how to use it, see http://rssexplained.blogspot.com.) An RSS aggregator connects to Web sites, downloads the feeds that you have selected, and displays them. Since it is the aggregator connecting to the Web sites, and not you, you may be able to access sites that would otherwise be blocked. This technique works only for Web sites that publish RSS feeds of their content, of course, and therefore is most useful for blogs and news sites. There are a lot of free, online RSS aggregators available. Some of the most popular ones include Google Reader (http://reader.google.com), Bloglines (http://www.bloglines.com) or Friendfeed (http://friendfeed.com)

Below is an example of Google Reader displaying the news:



Mugabe urged to form governme
from BBC News | News Front Page | Worl
Zimbabwe's ruling party, Zanu-PF, calls on Presic
despite protests from opposition rivals.

U.S. Aid Worker Gunned Down ir
from ABC News: HomePage
Stephen Vance was fatally shot by gunmen in Pe

US: New York Observer staying a

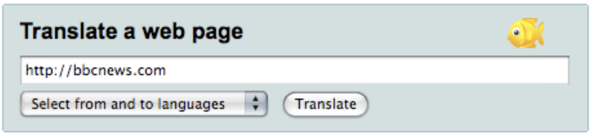
Translators

There are many language translation services available on the Internet, often provided by search engines. If you access a Web site through a translation service, the translation service is accessing the blocked site, not you. This allows you to read the blocked content translated into a number of different languages.

You can use the translation service to bypass blocking, even if you don't actually need to translate the text. You do this by choosing translation from a language that does not appear on the original Web site back to the original language. For example, to use a translation service to view an English-language Web site, choose translation from Chinese to English. The translation service translates only the Chinese sections (there are none), and leaves the English sections (which is the whole Web page) untranslated.

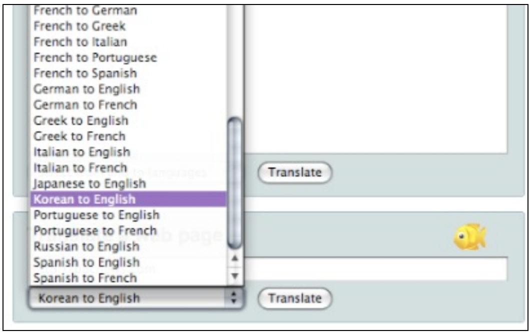
Popular translation services include http://babelfish.yahoo.com and http://translate.google.com.

The example below illustrates the three steps necessary to view a page in Babelfish. First, enter the URL of the Web site you wish to visit:



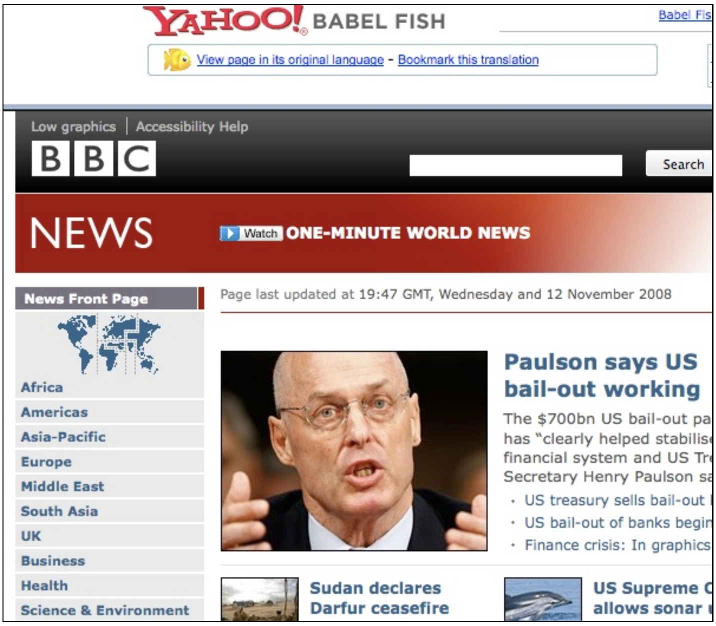
http://bbcnews.com

Next, choose the language you wish to read the Web site in. In this example, we tell Babelfish to translate from Korean to English. Since there is no Korean text, the page will remain untranslated.



Korean to English

When you have chosen the language, click "Translate" and the page displays.



Page last updated at 19:47 GMT, Wednesday and 12 November 2008

Paulson says US bail-out working

The $700bn US bail-out pa has "clearly helped stabilis financial system and US Tr Secretary Henry Paulson sa

- US treasury sells bail-out
- US bail-out of banks begin
- Finance crisis: In graphics

Sudan declares Darfur ceasefire

US Supreme C allows sonar

Of course this requires that the translator site itself is accessible, which is not always the case because some blocking authorities are aware of the potential use of translators for circumvention.

For instance http://translate.google.com is not accessible in Saudi Arabia, according to http://www.herdict.org.

Low-Bandwidth Filters

Low-bandwidth filters are Web services designed to make browsing the Web easier in places where connection speeds are slow. They remove or reduce images, remove advertisements, and otherwise compress the Web site to make it use less data, so that it downloads faster.

But, as with translation and aggregation services, you can also use low-bandwidth filters to bypass simple Web site blocking by fetching Web sites from their servers rather than from your computer. One useful low-bandwidth filter is at http://loband.org.

Web archive

The archive.org cache (the Wayback Engine - http://www.archive.org/web/web.php) allows users to see archived versions of web pages of the past. Millions of Web sites and their associated data (images, source code, documents, etc.) are saved in a gigantic database.

Not all Web sites are available, however, because many Web site owners choose to exclude their sites; also snapshots usually take at a long time to be added.

USING E-MAIL SERVICES

E-mail and Web mail services can be used to share documents with groups of friends or colleagues, and even to browse the Web.

Accessing Web pages through e-mail

Similar to low-bandwidth filters, there are services intended for people with slow or unreliable Internet connections that let you request a Web page via e-mail. The service sends a reply e-mail that includes the requested Web page either in the body of the message or as an attachment. These services can be quite cumbersome to use, since they require you to send a separate request for one or more Web pages, and then wait for the reply, but, in certain situations, they can be very effective at reaching blocked Web pages, especially if you use them from a secure Web mail service.

Web2mail

One such service is **web2mail.com**. To use it, send an e-mail message to www@web2mail.com with the Web address (URL) of the Web page you want in the subject line. You can also perform simple Web searches by typing searches into the subject line. For example you can search for censorship circumvention tools by typing "search censorship circumvention tools" in the subject line of an e-mail message and sending it to www@web2mail.com.

EmailTheWeb

Another service of the same kind is EmailTheWeb, http://www.emailtheweb.com, that allows you to e-mail any Web page to anyone, including to yourself. To send the Web page by e-mail you will need to register on the site or to use your Gmail account. The free service allows you to send up to 25 pages per day.

You can find more information and support on this topic on the ACCMAIL mailing list. To subscribe, send an e-mail with "SUBSCRIBE ACCMAIL" in the body to listserv@listserv.aol.com.

RSS to e-mail

Some platforms offer a similar Web to e-mail service, but with a focus on RSS feeds rather simple Web pages; they include:

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

FoE

(Feed over Email) is another interesting project of the same kind, created by Sho Sing Ho from the Broadcasting Board of Governors. At the time of writing this, FoE is still under development. The progress of FoE can be followed here: http://code.google.com/p/foe-project.

Sabznameh

If you are interested in accessing filtered news in Persian from inside Iran, Sabznameh is an option that you should consider. Sabznameh is a robust and scalable "feeds over e-mail" newsletter platform that allows independent news consumers to access censored and blocked content via e-mail.

The simplest way to access Sabznameh is to send a blank e-mail (with empty subject and body) to help@sabznameh.com. This way you can register even if you can't access the Web site http://sabznameh.com. You will receive a reply by e-mail that will guide you through the steps to register to one or more of the publications available.

Using Web mail to share documents

If you are trying to share documents online, but want to control who can see them, you can keep them in a private space where they are visible only to those with the correct password. A simple way to share documents among a small group of friends or colleagues is to use a single Web mail account with an online e-mail provider, such as Gmail (https://mail.google.com), and to share the user name and password with those who need to access the documents. Since most Web mail providers are free, it is easy to switch to a new account at intervals, making it harder for anyone outside the group to keep track of what you are doing. A list of free online e-mail providers is located at www.emailaddresses.com/email_web.htm.

ADVANTAGES AND RISKS

These simple techniques are quick and easy to use; you can try them with minimal effort. Many of them will work at least some of the time in many situations. However, they are also easy to detect and block. Since most of them do not encrypt or otherwise hide your communications, they are also vulnerable to keyword-based blocking and monitoring.

8. GET CREATIVE

If your Internet Service Provider (ISP) censors access to certain Web sites or services, you can use the tools described in the other chapters of this book, or you can think about creative ways to access unfettered information. Here are some examples.

USE ALTERNATIVE ISPS

Sometimes filtering regulations are not applied uniformly and consistently by all ISPs. Big providers with large numbers of subscribers, as well as state-owned telecommunications companies, may be subject to more scrutiny and more extensive law enforcement than small Internet start-ups. In 2002 the German government passed a law regulating the Internet that was applicable to ISPs based in only one of its states. Users therefore were able to circumvent these regulations by subscribing to a nationwide ISP with offices in other regions of the country. Similarly, a German regulation imposed in 2010 that would affect only ISPs with over 10,000 subscribers (in order to prevent a leak of the blacklist) was easily overcome by subscribing to small, local ISPs. During the 2011 Egyptian revolution, there has been speculation that Noor DSL was the last ISP to comply with the Internet shutdown order because of its relatively small market participation (8%) and the prominence of its customers, such as the Egyptian stock exchange, the National Bank of Egypt and Coca-Cola.

Alternative ISPs can also be found abroad, and some companies even waive the subscription fee for users who live in a country where there is severe political unrest. During the revolts of 2011 in Libya and Egypt, several citizens were able to publicize the political and social situations in their respective countries by hooking up their dial-up modems to ISPs abroad, or by using alternative communications methods, such as satellite, packet radio, and unfiltered connectivity provided by multinational companies or embassies.

MOBILE NETWORKS

Mobile networks are increasingly popular means of disseminating and accessing uncensored information, partly because of their high penetration rates in countries where the costs of owning a computer or a private Internet connection are prohibitive. Because many mobile carriers are not ISPs, their networks may not be affected by regulations in exactly the same way. However, these networks are usually easier to monitor and are frequently subject to extensive surveillance.

Activists in several countries have used their phones and free, open-source software such as FrontlineSMS (http://www.frontlinesms.com) to manage short message service (SMS) campaigns and bridge SMS technology with microblogging services, such as Twitter. A computer running FrontlineSMS and connected to the Internet can serve as a platform for others to post information to the Internet through their cell (mobile) phones.

Mobile networks can also be used with alternative devices. Amazon's Kindle 3G e-book reader, for example, comes with free international mobile roaming, which allows free access to Wikipedia through the mobile network in more than 100 countries.

DON'T USE THE INTERNET

Sometimes access to the Internet is completely restricted, and activists are forced to use alternative means to distribute and access uncensored information. In 1989, well before the Internet was widespread, some students from the University of Michigan purchased a fax machine to send daily summaries of international media to universities, government entities, hospitals, and major businesses in China to provide an alternative to the government's reports about the events at Tiananmen Square.

If your access to the Internet is restricted, consider the possibility of conducting peer-to-peer exchanges through alternative means. IrDA (Infrared) and Bluetooth are available in most modern mobile phones and can be used to transfer data over short distances. Other projects, such as "The Pirate Box" (http://wiki.daviddarts.com/PirateBox), use Wi-Fi and free, open source software to create mobile file-sharing devices. In countries with low Internet penetration, such as Cuba, USB flash drives have garnered widespread use by people who want to distribute uncensored information. Other technologies that were used by activists during the 2011 political unrest in Libya and Egypt include fax, speak2tweet (a platform launched by Google and Twitter that enables landline users to tweet via voicemail) and SMS.

USE EITHER VERY OLD OR VERY NEW TECHNOLOGY

Sometimes a censor's filtering and monitoring techniques are only applied to current standard Internet protocols and services, so consider using very old or very recent technology that may not be blocked or monitored. Before the advent of instant messaging (IM) software (Windows Live Messenger, AIM, etc.) group communication was performed using Internet Relay Chat (IRC), a protocol that allows real-time Internet text messaging. Although less popular than its successors, IRC still exists and is still widely used by a big community of Internet users. A bulletin board system (BBS) is a computer running software that allows users to connect, upload and download software as well as other data, read news, and exchange messages with other users. Originally users would call a telephone number using their modems to access these systems, but by the early 1990s some bulletin board systems also allowed access over Internet interactive text protocols, such as Telnet and, later, SSH.

In this regard, new technologies enjoy many of the the same benefits as old technologies, as they are used by limited numbers of users and therefore are less subject to censorship. The new Internet protocol IPv6, for example, is already deployed over some ISPs in some countries, and usually it is not filtered.

ALTERNATIVE USES FOR WEB SERVICES

Many Internet users whose connections are censored have started using Web services in ways different than those for which they were initially designed. For example, users have employed the chat capabilities of some video games to discuss sensitive matters that would otherwise be detected in common chat rooms. Another technique is to share a single e-mail account and save the conversation in the "Drafts" folder to avoid sending any e-mails over the Internet.

Online backup services such as Dropbox.com and Spideroak.com have been used by activists to distribute and share documents, as well as other kinds of data.

Services that are intended for translation, caching, or formatting have been used as simple proxies to bypass Internet censorship. Prominent examples are Google Translator, Google Cache, and Archive.org. However, there are many creative applications, such as Browsershots.org (takes screenshots of Web sites), PDFMyURL.com (creates a PDF from a Web site), URL2PNG.com (creates a PNG image from a URL), and InstantPaper.com (creates easy-to-read documents for e-book readers, such as Nook and Kindle).

ANY COMMUNICATION CHANNEL COULD BE A CIRCUMVENTION CHANNEL

If you have any kind of communication channel with a co-operative person or computer outside of the censorship you're experiencing, you should be able to turn it into a means of circumventing censorship. As mentioned above, people have already used video game chat to bypass censorship because censors often didn't think to monitor or censor it or to block access to popular video games. In games that allow players to create sophisticated in-world objects, people have discussed the idea of creating in-world computers, TV screens, or other devices that players could use to get uncensored access to blocked resources.

People have also suggested the idea of disguising information within social networking site profiles. For example, one person could put the address of a Web site he wanted to access in a disguised form inside his social networking site profile. A friend with uncensored access would then create an image of the contents of that site as a graphics file and post that in a different profile. This process could be automated by software so that it happens quickly and automatically, rather than requiring human beings to do the work.

With the help of computer programming, even a channel that simply allows a small amount of numeric or textual information to flow back and forth can be converted into a communications channel for a Web proxy. (When a channel hides the existence of some kind of communications entirely, it's called a **covert channel**.) For example, programmers have created IP-over-DNS or HTTP-over-DNS proxy applications to circumvent firewalls using the Domain Name System (DNS). An example is the iodine software at http://code.kryo.se/iodine. You can also read documentation for similar software at http://en.cship.org/wiki/DNS_tunnel and http://www.dnstunnel.de. With these applications, a request to access something is disguised as a request to look up the addresses of a large number of unrelated sites. The content of the information requested is then disguised as the content of the replies to these requests. Many firewalls are not configured to block this kind of communication, because the DNS system was never intended to be used to carry end-user communications rather than basic directory information about sites' locations.

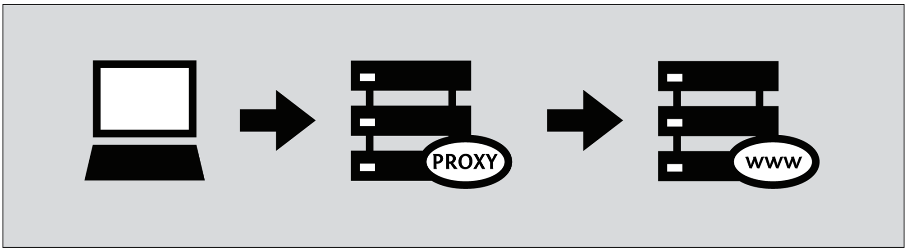
Many clever applications that use covert channels for circumvention are possible, and this is an area of ongoing research and discussion. To be useful, these require a dedicated server elsewhere, and the software at both ends must be set up by technically sophisticated users.

9. WEB PROXIES

A proxy allows you to retrieve a Web site or other Internet resource even when direct access to that resource is blocked from your location. There are many different kinds of proxies, including:

- Web proxies, which only require that you know the proxy Web site's address. A Web proxy URL may look like http://www.example.com/cgi-bin/nph-proxy.cgi.
- HTTP proxies, which require that you or a piece of software modify your browser settings. HTTP proxies only work for Web content. You may get the information about a HTTP proxy in the format "proxy.example.com:3128" or "192.168.0.1:8080".
- SOCKS proxies, which also require that you or a piece of software modify your browser settings. SOCKS proxies work for many different Internet applications, including e-mail and instant messaging tools. The SOCKS proxy information looks just like HTTP proxy information.

A Web proxy is like a browser embedded inside a Web page, and typically features a small form where you can submit the URL of the Web site that you want to access. The proxy then shows you the page, without requiring that you connect to it directly.

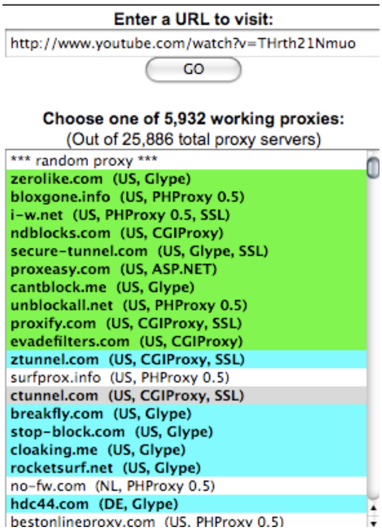


When using a Web proxy, you do not have to install software or change settings on your computer, which means that you can use a Web proxy from any computer, including those at Internet cafés. Simply enter the URL of the Web proxy into your browser, enter the destination URL you wish to visit into the Web proxy, and press Enter or click the submit button.

Once you are viewing a page through a Web proxy, you should be able to use your browser's forward and back buttons, click on links and submit forms without losing your proxied connection to the filtered site. This is because your proxy has rewritten all of the links on that page so that they now tell your browser to request the destination resources through the proxy. Given the complexity of today's Web sites, however, this can be a difficult task. As a result, you might find that some pages, links or forms "break out" of the proxied connection. Typically, when this happens, the Web proxy's URL form will disappear from your browser window.

HOW CAN I FIND A WEB PROXY?

You can find Web proxy URLs at sites such as http://www.proxy.org, by signing up for a mailing list such as the one at http://www.peacefire.org/circumventor, by following a country-specific twitter feed, or simply by searching for "free Web proxy" in a search engine. Proxy.org lists thousands of free Web proxies:



Enter a URL to visit:

http://www.youtube.com/watch?v=THrth21Nmuo

GO

Choose one of 5,932 working proxies:
(Out of 25,886 total proxy servers)

*** random proxy ***
zerolike.com (US, Glype)
bloxgone.info (US, PHProxy 0.5)
i-w.net (US, PHProxy 0.5, SSL)
ndblocks.com (US, CGIProxy)
secure-tunnel.com (US, Glype, SSL)
proxeasy.com (US, ASP.NET)
cantblock.me (US, Glype)
unblockall.net (US, PHProxy 0.5)
proxify.com (US, CGIProxy, SSL)
evadefilters.com (US, CGIProxy)
ztunnel.com (US, CGIProxy, SSL)
surfprox.info (US, PHProxy 0.5)
ctunnel.com (US, CGIProxy, SSL)
breakfly.com (US, Glype)
stop-block.com (US, Glype)
cloaking.me (US, Glype)
rocketsurf.net (US, Glype)
no-fw.com (NL, PHProxy 0.5)
hdc44.com (DE, Glype)
bestonlineproxy.com (US, PHProxy 0.5)

Examples of Web proxy platforms include CGIProxy, PHProxy, Zelune, Glype, Psiphon, and Picidae. As mentioned above, these are not tools that you install on your own computer. They are server software that someone else must install on a computer that is connected to the Internet in a location that is not subject to filtering. All of these platforms provide the same basic functionality, but they look different and may have different strengths and weaknesses. Some are better at certain things, such as streaming videos or displaying complex Web sites accurately.

Some Web proxies are private. These are usually accessible only to a small group of users known to the individual running the proxy or to customers who pay for the service. Private Web proxies have certain advantages. Specifically, they may be:

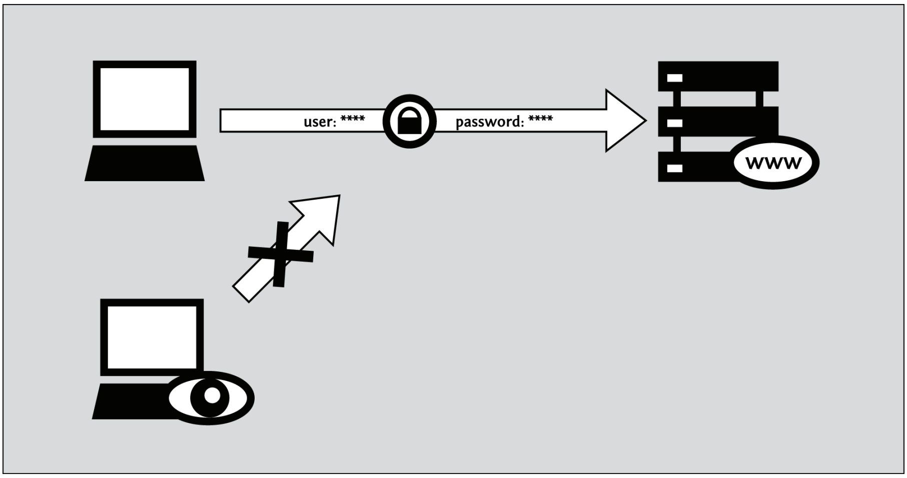
- more likely to remain undiscovered and therefore accessible
- less congested and therefore faster
- more trustworthy, assuming they are encrypted (see below) and run by someone you know.

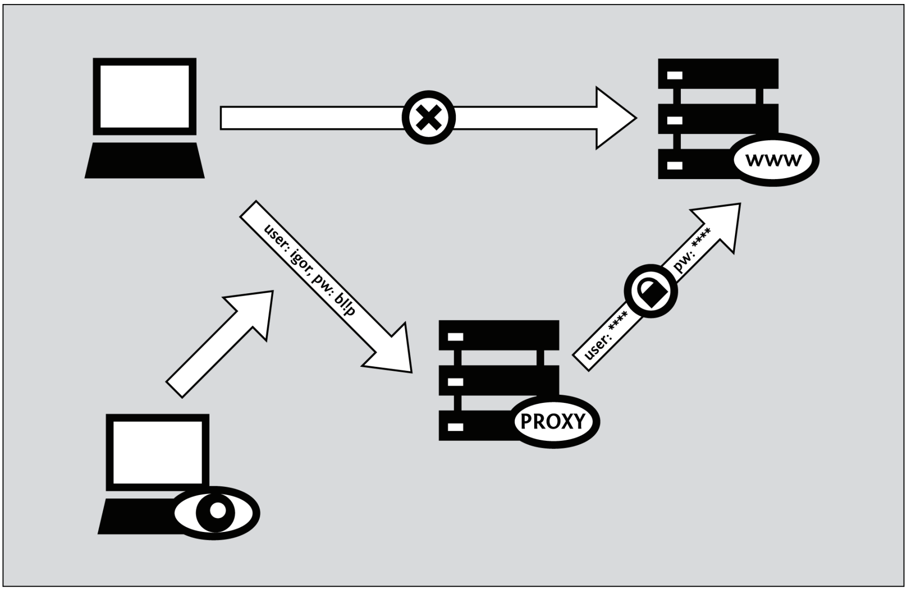
Access may be restricted by requiring users to log in with a username and password or simply by preventing the proxy URL from appearing in public directories such as those described above.

Web proxies are easy to use, but they have major disadvantages relative to other circumvention tools. As a result, people often use them as a temporary way to obtain and learn how to use more advanced tools, which must often be downloaded from Web sites that are themselves filtered. Similarly, access to a Web proxy can be useful when attempting to fix or replace another tool that has stopped working.

COMPATIBILITY ISSUES WITH WEB PROXIES

Web proxies only work for Web traffic, so they can not be used for other Internet services such as e-mail or instant messaging. Many are also incompatible with complex Web sites like Facebook, streaming multimedia content on sites such as YouTube, and encrypted sites that are accessed through HTTPS. This latter restriction means that many Web proxies will be unable to help you reach filtered sites that require a login, such as Web-based e-mail services. Worse yet, some Web proxies cannot themselves be accessed through HTTPS. If you use such a proxy to log in to a destination site that is normally secure, you may be putting your sensitive information, including your password, at risk.





Security issues like this are discussed in more detail below.

With the notable exception of the HTTPS concerns described above, most Web proxy compatibility issues can be resolved by using the "mobile" or "basic HTML" version of the destination Web site, provided one is available. Unfortunately, relatively few sites offer this kind of simplified interface, and even fewer do so in a way that exposes all of the site's functionality. If a Web site does provide a mobile version, its URL will frequently begin with an "m" instead of "www." Examples include https://m.facebook.com, http://m.gmail.com, and https://m.youtube.com. You can sometimes find a link for the mobile or basic HTML version of a Web site among the small links toward the bottom of the site's main page.

SECURITY RISKS WITH WEB PROXIES

You should be aware of some of the risks associated with the use of Web proxies, particularly those operated by individuals or organizations you do not know. If you use a Web proxy simply to read a public Web site such as www.bbc.co.uk, your only real concerns are that:

- someone might learn that you are viewing a censored news source
- someone might learn which proxy you rely on to do so.

Furthermore, if your Web proxy is working properly, and if you access it through HTTPS, the former information should only be available to the administrator of the proxy itself. However, if you rely on an insecure HTTP connection or if your proxy malfunctions (or is poorly designed) this information will be revealed to anyone who might be monitoring your Internet connection. In fact, unencrypted Web proxies do not work at all in some countries, because they cannot circumvent filters that rely on keywords, rather than URLs or IP addresses, to block content.

For some users, the risks above are not a major concern. However, they may become quite serious if you intend to use a Web proxy to access certain types of online resources, such as:

- sites that require you to log in with a password
- sites through which you intend to access sensitive information
- sites through which you intend to create or share content
- online commerce or Web banking sites
- sites that support HTTPS encryption themselves.

In such cases, you should avoid using insecure or untrusted Web proxies. In fact, you might want to avoid using a Web proxy altogether. While there is no guarantee that a more "advanced" tool will be more secure, the challenges that installable circumvention software must address in order to keep your traffic private are generally less complex than those faced by Web proxy software.

Obfuscation is not encryption

Some Web proxies, most notably those that lack support for HTTPS, use simple encoding schemes to circumvent poorly-configured domain name and keyword filters. One such scheme, called ROT-13, replaces each character with whatever lies 13 places ahead of it in the standard Latin alphabet. (See http://www.rot13.com to try it out for yourself.) Using ROT-13, the URL http://www.bbc.co.uk becomes uggc://jjj.oop.pb.hx, which would make it unrecognizable to a very basic keyword filter. Proxy designers have found this trick useful even in countries where keyword filtering is not present, because Web proxies often include the target URL inside the actual URL that your browser sends to the proxy every time you click on a link or submit a new address. In other words, when using a proxy, your browser might request http://www.proxy.org/get?site=http://www.bbc.co.uk instead of just http://www.bbc.co.uk, but a domain name filter written to catch the latter would catch the former just as readily. http://www.proxy.org/get?site=uggc://jjj.oop.pb.hx, on the other hand, might slip through the filter. Unfortunately, character encoding schemes are not very reliable. After all, there is nothing to prevent a censor from adding "jjj.oop.pb.hx" to the blacklist along with "www.bbc.co.uk." (Or, better yet, she could add "uggc://" to the list, which would block all use of the proxy.)

The important thing to remember about character encoding is that it does not protect your anonymity from third party observers, who can still track the list of sites that you visit. And, even if it is applied to the full text of the pages you view and content you submit (rather than just to URLs), it still can not provide confidentiality. If these things matter to you, restrict your use of Web proxies to those that support HTTPS.

Don't forget, the proxy administrator can see everything.

The advice above emphasizes the importance of HTTPS, both on the censored target site and on the proxy itself, when using a Web proxy to create or obtain sensitive information. However, it is important to note that even when you access a secure site through a secure proxy, you are still putting a great deal of faith in whoever administers your Web proxy, as that individual or organization can read all of the traffic that you send or receive. This includes any passwords that you might have to submit in order to access the destination Web site.

Even the more advanced circumvention tools, which tend to require that you install software on your computer, must rely on some kind of intermediary proxy in order to circumvent Web filters. However, all reputable tools of this kind are implemented in such a way as to protect the content of HTTPS Web traffic even from the circumvention services themselves. Unfortunately, this is not possible for Web proxies, which must rely more heavily on good old-fashioned trust. And trust is a complicated function, that depends not only on a service administrator's willingness to protect your interests, but also on her logging and record-keeping policies, her technical competency, and the legal and regulatory environment in which she operates.

ANONYMITY RISKS WITH WEB PROXIES

Tools designed to circumvent filtering do not necessarily provide anonymity, even those that might include words like "anonymizer" in their names! In general, anonymity is a much more elusive security property than basic confidentiality (preventing eavesdroppers from viewing the information that you exchange with a Web site). And, as discussed above, even to ensure basic confidentiality through a Web proxy requires, at the very least, that you:

- use an HTTPS Web proxy
- connect through that proxy to an HTTPS destination Web site
- trust the proxy administrator's intentions, policies, software and technical competence
- heed any browser warnings, as discussed in the HTTPS chapter of this book.

All of these conditions are also prerequisites for any degree of anonymity. If a third party can read the content of your traffic, he can easily connect your IP address with the list of specific Web sites that you visit. This is true even if, for example, you log in to those sites or post messages on them using a pseudonym. (Of course, the opposite is true, as well. Even a perfectly secure proxy cannot protect your identity if you sign your name to a public post on the destination Web site!)

Advertising, viruses and malware

Some of the people who set up Web proxies do it to make money. They may do this simply and openly by selling advertisements on each proxied page, as in the example below.

Or, a malicious proxy administrator might try to infect his users' computers with malware. These so-called "drive-by-downloads" can hijack your computer for spamming or other commercial or even illegal purposes.

The most important thing you can do to protect yourself against viruses and other malware is to keep all of your software – especially your operating system and your anti-virus scanner – updated. You can also block ads by using the AdBlockPlus extension (http://www.adblockplus.org) and some malicious content by using the NoScript extension (http://noscript.net). Both of these extensions are for the Firefox Web browser. You can find more information on avoiding the risks described above on the StopBadware Web site (http://www.stopbadware.org).

Cookies and scripts

There are also risks associated with the use of **cookies** and **embedded scripts**. Many Web proxies can be configured to remove cookies and scripts, but many sites (for example, social networking sites like Facebook and media streaming sites like YouTube) require them to work properly. Web sites and advertisers can use these mechanisms to track you, even when you use proxies, and to produce evidence that, for example, the person who did one thing openly is the same person who did another thing anonymously. Some cookies may be saved on your computer even after you restart it, so it might be a good idea to allow only selective use of cookies. In Firefox, for example, you can instruct the browser to accept cookies only "Until I close Firefox". (Similarly, you can instruct your browser to erase your browsing history when you close it.) Generally speaking, however, Web proxies are extremely limited in their ability to protect your identity from the Web sites that you access through them. If this is your goal, then you will have to be very careful how you configure your browser and proxy settings, and you might want to use a more advanced circumvention tool.

Helping others

If you are in a country with unrestricted Internet access and you are willing to help others get around censorship, you can install a Web proxy script on your own Web site (or even on your home computer), as discussed in the Helping Others section of this book.

10. PSIPHON

Psiphon is an open-source Web proxy platform that has changed quite a bit over the past few years. It differs from other proxy software (such as CGIProxy and Glype) in various ways, depending on how it is configured on the server. In general, Psiphon:

- is accessible through HTTPS
- supports access to HTTPS destination sites
- offers improved (though far from perfect) compatibility with a few complex Web sites, including YouTube
- may or may not require you to log in with a username and password
- allows you to register an e-mail address to receive new proxy URLs from the administrator in the event that your proxy is blocked
- allows you to invite others to use your proxy (assuming it is configured to require a password).

The current version of the Psiphon server software runs only on Linux, and is much more difficult to install and administer than most other proxies. It is designed primarily to facilitate the operation of a large scale, blocking-resistant circumvention service for those who lack the ability to install and use more advanced tools.

THE HISTORY OF PSIPHON

Psiphon 1, the original version of the Web proxy platform, was designed to run on Windows, and allowed a non-expert computer user in a country that does not filter the Internet to provide basic circumvention services to specific individuals from countries that do. It was easy to install, easy to use and featured partial support for HTTPS, which made it more secure than many of the alternatives. It also required users to log in, which helped prevent congestion and reduced the likelihood that these small Web proxies, called nodes, would be targeted for blocking. Psiphon 1 is no longer maintained or supported by the organization that developed it.

Psiphon 2 was completely rewritten, with an eye toward performance, security, compatibility and scalability in the context of a centralized service model. These goals have been met with varying degrees of success. Initially, a Psiphon 2 user was required to log in to a particular private node with a username and password. Psiphon, Inc. gave a few early users from each region additional privileges that allowed them to invite others to access their proxies. Early Psiphon 2 proxies also required users to ignore "invalid certificate" browser warnings because, while they were accessible through HTTPS, their administrators were unable or unwilling to purchase signed SSL certificates. All Psiphon private nodes deployed by the company itself now have signed certificates and should not trigger browser warnings. Obviously, this might not hold true for third-party installations of the Psiphon software. Finally, all Psiphon users now earn the right to send a limited number of invitations.

Psiphon 2 open nodes, which were implemented somewhat later, can be used without logging in. An open node automatically loads a particular homepage, and presents itself in a particular language, but can then be used to browse elsewhere while evading online censorship. Open nodes include a link through which a user can create an account and, optionally, register an e-mail address. Doing so allows the proxy administrators to send a new URL to users whose nodes are blocked from within their country. In general, open nodes are expected to be blocked and replaced much more quickly than private nodes. As with new private nodes, all Psiphon open nodes are secured using HTTPS, and those operated by Psiphon, Inc. identify themselves using valid, signed certificates.

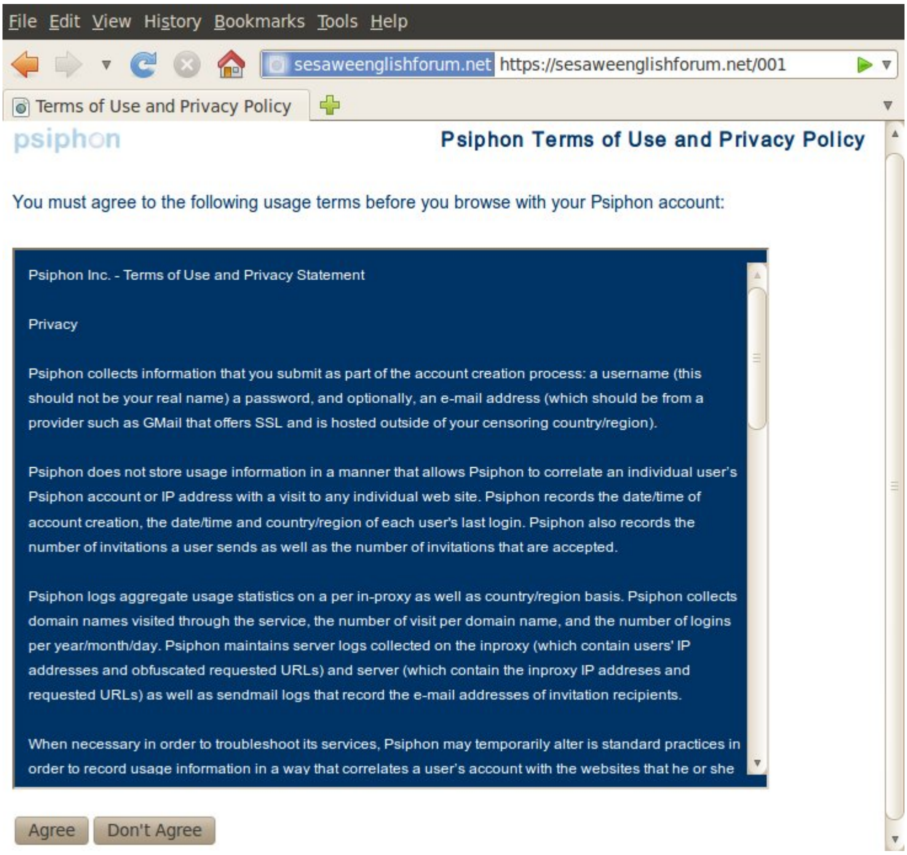
HOW CAN I GET ACCESS TO A PSIPHON NODE?

To limit and monitor the blocking of its proxies, Psiphon, Inc. has no centralized way to distribute open nodes (which it sometimes refers to as right2know nodes). One English language open node, dedicated to the Sesawe circumvention support forum, is available at http://sesaweenglishforum.net. Other open nodes are distributed privately (through mailing lists, twitter feeds, radio broadcasts, etc.) by the various content producers that make up Psiphon's client base.

Psiphon private nodes work differently. Even if it were possible to print an invitation link in this book, it would be ill-advised, as the whole point of maintaining a private node is to limit its growth and preserve some resemblance to a social network of trust among its members. After all, a single invitation sent to a single 'informer' could be enough to get a node's IP address added to a national blacklist. Worse yet, if that invitation were accepted, the informant would also receive any replacement proxy URLs sent out by the system's administrators. If you do receive an invitation, it will include a link similar to the following, https://privatenode.info/w.php?p=A9EE04A3, which will allow you to create an account and register an e-mail address. To do so, follow the instructions under "Create an account", below. After creating your account, you no longer need to use the invitation link. Instead, you will log in through a somewhat easier-to-remember URL such as https://privatenode.info/harpo.

USING A PSIPHON OPEN NODE

The first time you connect to an open Psiphon proxy, you will see the "Psiphon Terms of Use and Privacy Policy." Please read the terms carefully, as they contain important security advice as well as information about how the proxy administrator claims to handle your data. In order to use the proxy, you must click Agree.


File Edit View History Bookmarks Tools Help
sesaweenglishforum.net https://sesaweenglishforum.net/001
Terms of Use and Privacy Policy
psiphon
Psiphon Terms of Use and Privacy Policy

You must agree to the following usage terms before you browse with your Psiphon account:

Psiphon Inc. - Terms of Use and Privacy Statement

Privacy

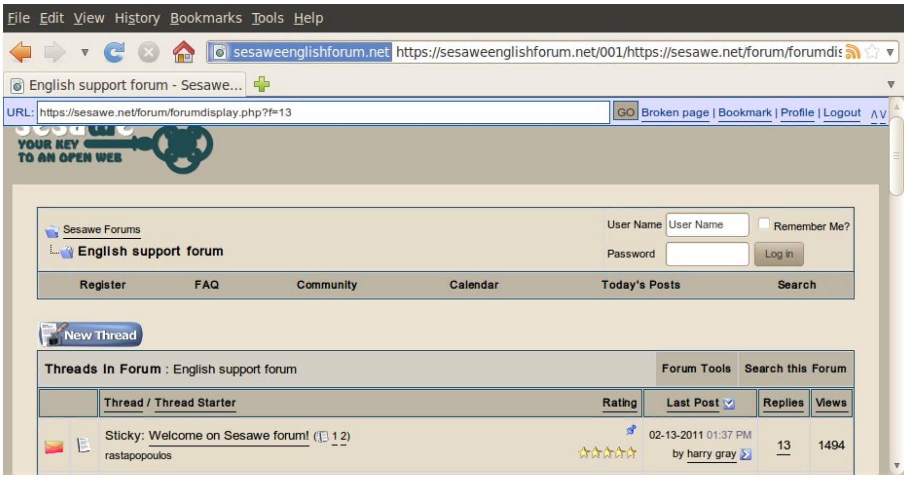
Psiphon collects information that you submit as part of the account creation process: a username (this should not be your real name) a password, and optionally, an e-mail address (which should be from a provider such as GMail that offers SSL and is hosted outside of your censoring country/region).

Psiphon does not store usage information in a manner that allows Psiphon to correlate an individual user's Psiphon account or IP address with a visit to any individual web site. Psiphon records the date/time of account creation, the date/time and country/region of each user's last login. Psiphon also records the number of invitations a user sends as well as the number of invitations that are accepted.

Psiphon logs aggregate usage statistics on a per in-proxy as well as country/region basis. Psiphon collects domain names visited through the service, the number of visit per domain name, and the number of logins per year/month/day. Psiphon maintains server logs collected on the inproxy (which contain users' IP addresses and obfuscated requested URLs) and server (which contain the inproxy IP addreses and requested URLs) as well as sendmail logs that record the e-mail addresses of invitation recipients.

When necessary in order to troubleshoot its services, Psiphon may temporarily alter is standard practices in order to record usage information in a way that correlates a user's account with the websites that he or she

After you accept the Terms of Use, Psiphon will load the default home page associated with that node, as shown below. You can follow the links displayed on this page, which will automatically request content through the proxy, or you can visit other Web sites using the blue URL bar (called the Bluebar in Psiphon lingo) at the top of your browser window.


File Edit View History Bookmarks Tools Help
sesaweenglishforum.net https://sesaweenglishforum.net/001/https://sesawe.net/forum/forumdis
English support forum - Sesawe...
GO Broken page | Bookmark | Profile | Logout
YOUR KEY TO AN OPEN WEB
New Thread

URL: https://sesawe.net/forum/forumdisplay.php?f=13

Sesawe Forums
English support forum

User Name: User Name ☐ Remember Me?
Password: Log in

Register | FAQ | Community | Calendar | Today's Posts | Search

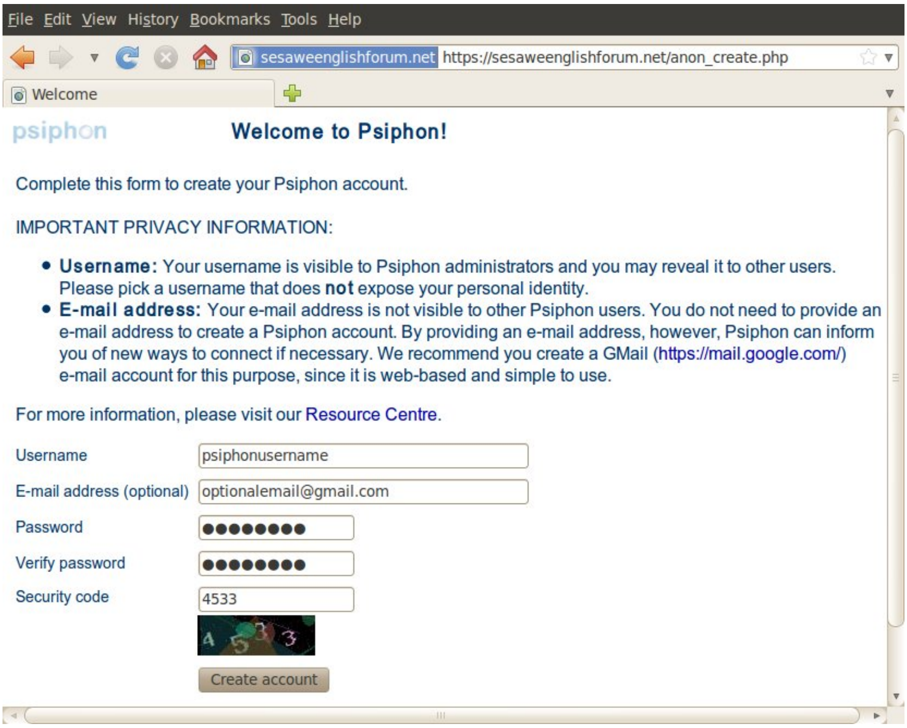
Threads in Forum : English support forum — Forum Tools | Search this Forum

Thread / Thread Starter	Rating	Last Post	Replies	Views
Sticky: Welcome on Sesawe forum! (1 2) rastapopoulos	☆☆☆☆☆	02-13-2011 01:37 PM by harry gray	13	1494

CREATING AN ACCOUNT

As long as you remember or bookmark the URL of an unblocked open node, you can use it to access filtered Web sites. Creating an account allows you to modify certain preferences, including the proxy's language and default home page. It also allows you to register an e-mail address so that the node's administrator can e-mail you a new proxy URL if this one gets blocked. To do so, click on the "Create account" link in the Bluebar.

If you receive an invitation to a Psiphon private node, the steps require to create your account are identical to those described below.


File Edit View History Bookmarks Tools Help
sesaweenglishforum.net https://sesaweenglishforum.net/anon_create.php
Welcome
psiphon
Create account

Welcome to Psiphon!

Complete this form to create your Psiphon account.

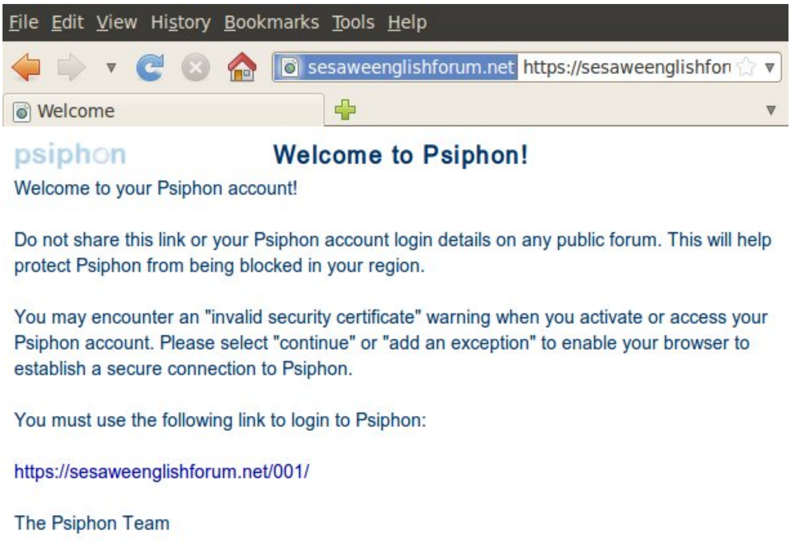
IMPORTANT PRIVACY INFORMATION:

- **Username:** Your username is visible to Psiphon administrators and you may reveal it to other users. Please pick a username that does **not** expose your personal identity.
- **E-mail address:** Your e-mail address is not visible to other Psiphon users. You do not need to provide an e-mail address to create a Psiphon account. By providing an e-mail address, however, Psiphon can inform you of new ways to connect if necessary. We recommend you create a GMail (https://mail.google.com/) e-mail account for this purpose, since it is web-based and simple to use.

For more information, please visit our Resource Centre.

Username	psiphonusername
E-mail address (optional)	optionalemail@gmail.com
Password	●●●●●●●●
Verify password	●●●●●●●●
Security code	4533

When filling out the registration form, you might want to choose a username that is not connected to your real identity through e-mail services, social networking sites, or other such platforms. The same applies to your e-mail address, if you choose to register one. Most other users of your proxy are prevented from seeing your username or your e-mail address, but both items are stored in a database somewhere and are visible to Psiphon administrators. If you choose to register an e-mail address, it is recommended that you select one that allows you to access your e-mail through an HTTPS connection. Free e-mail providers that support HTTPS include https://mail.google.com, https://www.hushmail.com, and https://mail.riseup.net. To prevent the automated registration of Psiphon accounts, you must read the number displayed on the Security code image and enter it in the last field. When you are done, click "Create account".


File Edit View History Bookmarks Tools Help
sesaweenglishforum.net https://sesaweenglishforu
Welcome
psiphon

Welcome to Psiphon!

Welcome to your Psiphon account!

Do not share this link or your Psiphon account login details on any public forum. This will help protect Psiphon from being blocked in your region.

You may encounter an "invalid security certificate" warning when you activate or access your Psiphon account. Please select "continue" or "add an exception" to enable your browser to establish a secure connection to Psiphon.

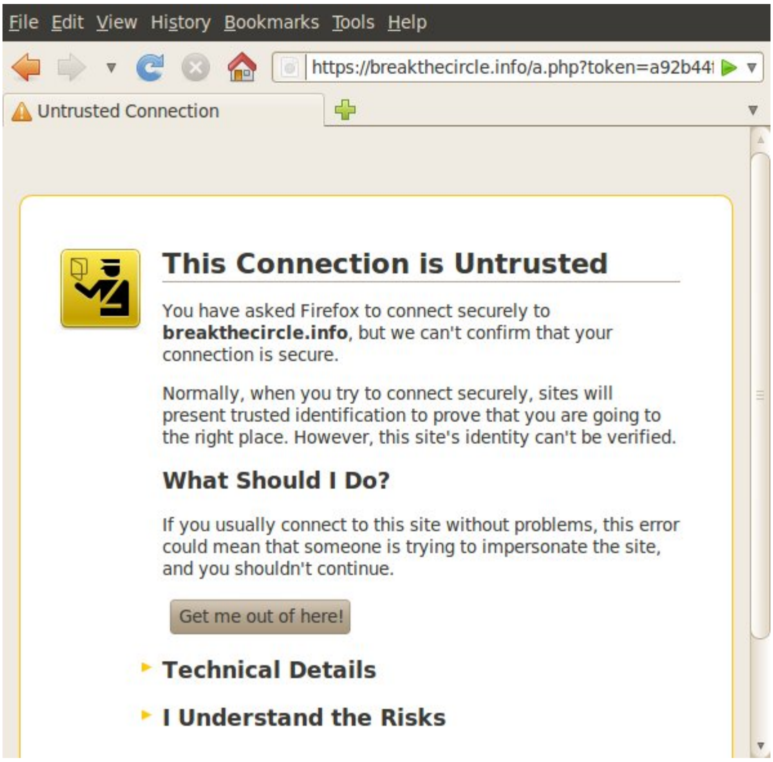
You must use the following link to login to Psiphon:

https://sesaweenglishforum.net/001/

The Psiphon Team

You should see a message confirming the successful creation of your account. From now on please use the URL displayed on this page to log in to your Psiphon node. Note that it includes an HTTPS prefix and a short suffix ("/001" in the image above). You might want to print out this welcome page or bookmark the linked URL (but be careful not to bookmark the welcome page itself, by accident). Or course, you will also need the username and password that you chose in the steps above.

This welcome page might also provide some advice, as shown above, about "invalid security certificate" warnings and the need to accept them in order to use Psiphon. In fact, these instructions are outdated, and you should no longer follow them. If, when connecting to a Psiphon proxy, you see warnings such as those displayed below, you should pay attention to them. If that happens, you might want to close your browser and contact info@psiphon.ca or english@sesawe.net for additional advice.


File Edit View History Bookmarks Tools Help
https://breakthecircle.info/a.php?token=a92b44
Untrusted Connection
Get me out of here!

This Connection is Untrusted

You have asked Firefox to connect securely to **breakthecircle.info**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

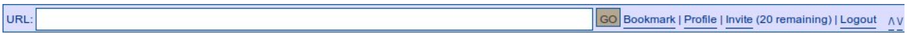
▸ Technical Details

▸ I Understand the Risks

INVITING OTHERS

If you use an account to log in to your Psiphon proxy, you will eventually gain the ability to invite others. In order to help prevent blocking, you will collect invite tokens slowly, and there is a limit to the number that you can have at any one time. Obviously, if your proxy is an open node, you can simply send the proxy URL to others. However, after a blocking event, if you receive a follow-up "migration" message at your registered e-mail address, you might find that your account has been moved to a private node. You should never share the URL of a private node, except through Psiphon's built-in invitation mechanism.

Once you have collected one or more invitations, you will see an link on your Bluebar that says something like Invite (1 remaining), as shown below.



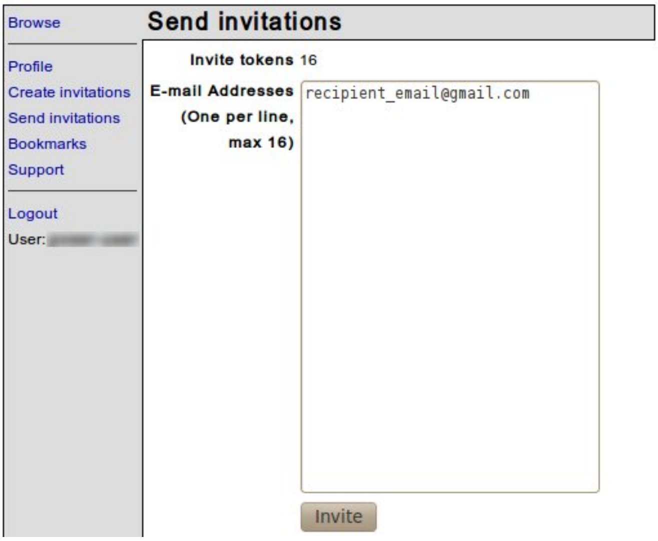
There are two ways to invite others to use your Psiphon proxy:

- The Send invitations method automatically sends invitation links to one or more recipients. The invitation messages will come from Psiphon, not from your own account.
- The Create invitations method generates one or more invitation links for you to distribute through other channels.

If you click on the Bluebar link, you will be taken to the Send invitations screen. In order to create an invitation link without e-mailing it, you must click on the Profile link first, then "Create invitations".

Send invitations

Click "Invite" on your Bluebar or Send invitations on the Profile screen. Enter an e-mail address for each person to whom you want to send an invitation, one address per line, and then click "Invite".



User: [redacted]

Send invitations

Invite tokens 16

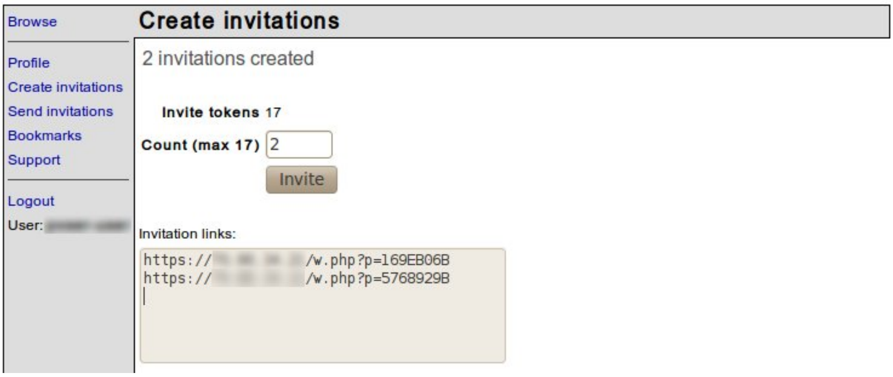
E-mail Addresses (One per line, max 16) recipient_email@gmail.com

You will see a message telling you that one or more messages have been queued, which means that Psiphon will e-mail out your invitation links within the next few minutes.

Remember that you should only invite people you know to private nodes.

Create invitations

Click "Create invitations" in the Profile screen. Select the number of invitation links to create and click "Invite".



User: [redacted]

Create invitations

2 invitations created

Invite tokens 17

Count (max 17) 2

Invitation links:

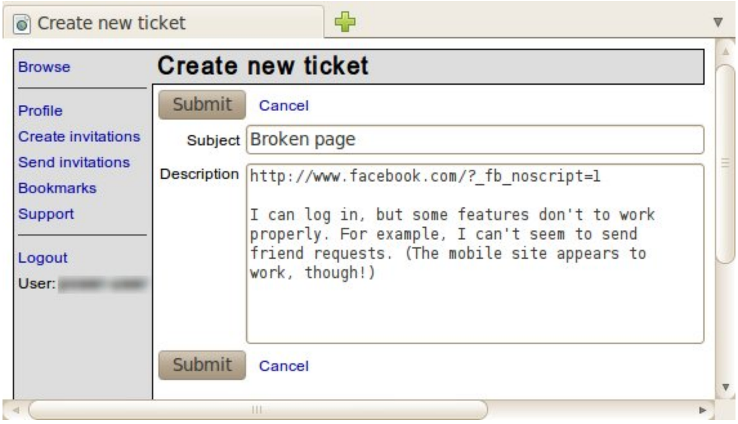
```
https://[redacted]/w.php?p=169EB06B
https://[redacted]/w.php?p=5768929B
```

You may distribute these invitation links through whatever channels are available to you, but:

- each invitation can be used only once
- for private nodes, do not display the links publicly, to avoid exposing the proxy URL
- for private nodes, you should only invite people you know.

REPORTING A BROKEN WEB SITE

Some Web sites that rely on embedded scripts and complex Web technology like Flash and AJAX may not display properly through Psiphon. In order to improve Psiphon's compatibility with such Web sites, the developers need to know which sites are problematic. If you find such a site, you can report it easily by clicking the Broken Page link on the Bluebar. If you provide a brief explanation of the problem in the Description field, it will allow the Psiphon development team to reproduce the error and help them find a solution. When you have finished, click "Submit" and your message will be sent to the developers.



Create new ticket

User: [redacted]

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!)
```

11. SABZPROXY

SabzProxy ("*green proxy*" in Persian) is a free distributed Web proxy proposed by the Sabznameh.com team. It is based on the legacy code of PHProxy (which has not being maintained since 2007). For additional detail about the Web proxies concept, please refer to the previous chapter.

The main improvement in SabzProxy, compared to PHProxy, is URL encoding. This makes SabzProxy harder to detect (PHProxy has a predictive footprint that means it is now blocked in several countries, including Iran). Only deep-packet inspection would allow SabzProxy servers to be detected and blocked.

SabzProxy is localized in Persian but is fully functional in any language. Many people in various countries have used it to set up their own public Web proxy.

GENERAL INFORMATION

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

HOW DO I ACCESS SABZPROXY?

SabzProxy is a distributed Web proxy. This means that there are neither central SabzProxy instances, nor a commercial entity designed to create and diffuse them. Rather, it relies on its community and users to create their own instances, and to share these to their network. You can access instances through various forums, or networks, and when you have access you are welcome to share it with your friends.

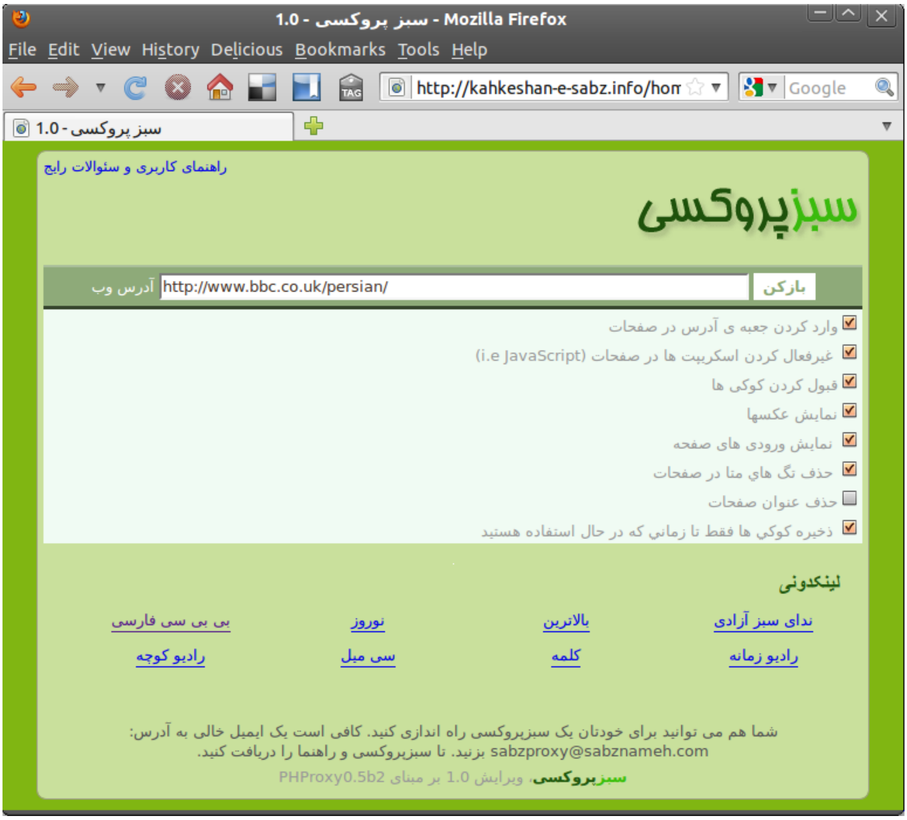
One dedicated instance is run by the Sesawe circumvention support forum, and it is available at http://kahkeshan-e-sabz.info/home (you can log in with the username *flossmanuals*, and password *flossmanuals*).

If you own a Web hosting space and are interested in creating and sharing your SabzProxy instance with your friends and family, please refer to the *Installing SabzProxy* chapter in the *Helping Others* section of this book.

HOW DOES IT WORK?

Here's an example that illustrates how SabzProxy works.

1. Enter the address of the SabzProxy instance you are using in your browser.
2. In the Web Address box on the SabzProxy page, enter the address of the censored Web site you want to visit. For example, http://www.bbc.co.uk/persian. You can keep the default options.
3. Click Go or Enter.


1.0 - سبز پروکسی - Mozilla Firefox
File Edit View History Delicious Bookmarks Tools Help
http://kahkeshan-e-sabz.info/hom
Google
1.0 - سبز پروکسی
سبزپروکسی
بازکن

راهنمای کاربری و سئوالات رایج

آدرس وب http://www.bbc.co.uk/persian/

☑ وارد کردن جعبه ی آدرس در صفحات

☑ غیرفعال کردن اسکریپت ها در صفحات (i.e JavaScript)

☑ قبول کردن کوکی ها

☑ نمایش عکسها

☑ نمایش ورودی های صفحه

☑ حذف تگ هاي متا در صفحات

□ حذف عنوان صفحات

☑ ذخیره کوکی ها فقط تا زمانی که در حال استفاده هستید

لینکدونی

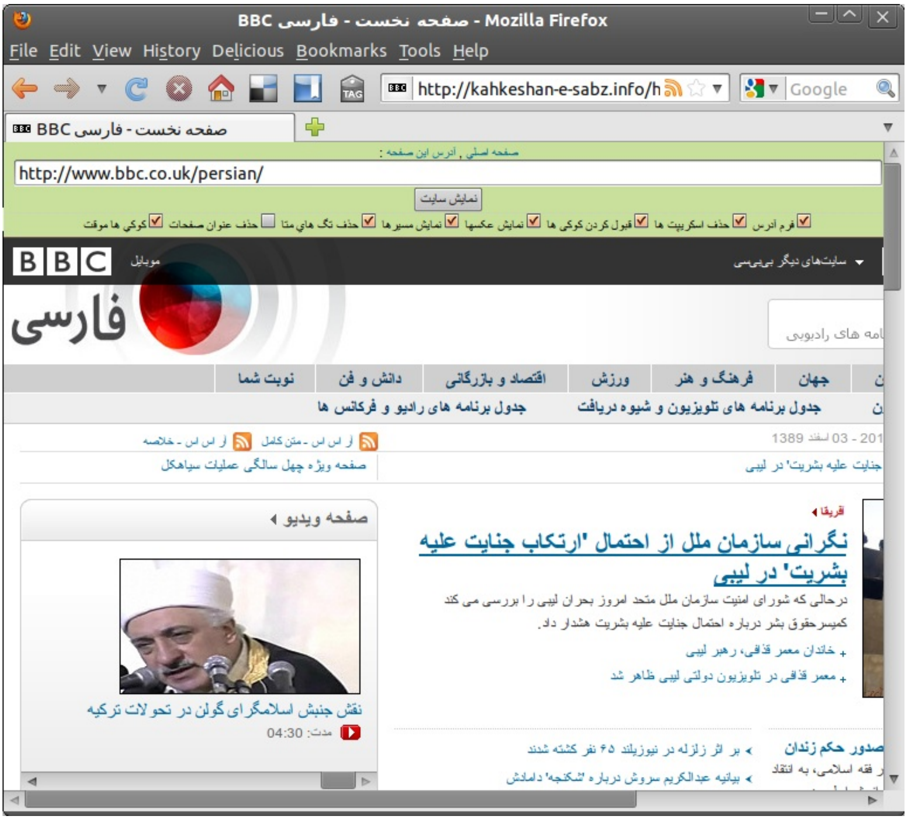
ندای سبز آزادی | بالاترین | نوروز | بی بی سی فارسی

رادیو زمانه | کلمه | سی میل | رادیو کوچه

شما هم می توانید برای خودتان یک سبزپروکسی راه اندازی کنید. کافی است یک ایمیل خالی به آدرس:
sabzproxy@sabznameh.com بزنید. تا سبزپروکسی و راهنما را دریافت کنید.

سبزپروکسی، ویرایش 1.0 بر مبنای PHProxy0.5b2

The Web site is displayed in the browser window.



صفحه اصلي , آدرس اين صفحه :

http://www.bbc.co.uk/persian/

☑ فرم آدرس ☑ حذف اسکريپت ها ☑ قبول کردن کوکی ها ☑ نمايش عکسها ☑ نمايش مسير ها ☑ حذف تگ هاي متا □ حذف عنوان صفحات ☑ کوکي ها موقت

201 - 03 اسفند 1389

جنایت علیه بشریت' در لیبی | صفحه ویژه چهل سالگی عملیات سیاهکل

افریقا

نگرانی سازمان ملل از احتمال 'ارتکاب جنایت علیه بشریت' در لیبی

درحالی که شورای امنیت سازمان ملل متحد امروز بحران لیبی را بررسی می کند کمیسرحقوق بشر درباره احتمال جنایت علیه بشریت هشدار داد.

+ خاندان معمر قذافی، رهبر لیبی

+ معمر قذافی در تلویزیون دولتی لیبی ظاهر شد

نقش جنبش اسلامگرای گولن در تحولات ترکیه

› بر اثر زلزله در نیوزیلند ۶۵ نفر کشته شدند

› بیانیه عبدالکریم سروش درباره 'شکنجه' داماش

صدور حکم زندان

ر فقه اسلامی، به انتقاد

You can see the SabzProxy green bar within the browser window, and the BBC Farsi Web site below the bar.

To continue browsing, you can either:

- Click any link from the current page. The Web proxy will automatically retrieve linked pages.
- Enter a new URL in the Address box at the top of the page.

ADVANCED OPTIONS

Usually, you can keep the default options to browse. However you can choose between several advanced options:

- **Include mini URL-form on every page / فرم آدرس**
  Check this option if you want to have a form on the proxified Web sites so that you can enter new URLs without going back to the start page of SabzProxy. You may want to deselect this option if you have a small screen, so you have more space for the target Web page.

- **Remove client-side scripting (i.e., JavaScript) / حذف اسکریپت ها**
  Check this option if you want to remove dynamic technology scripting from Web pages. Sometimes JavaScript can cause unwanted issues, as it is also used to display online ads or even to track your identity. Browsing mobile/light versions of complex Web sites (like Web mail services, or social networking platforms) is also an alternative to avoid Javascript issues while using SabzProxy.

- **Allow cookies to be stored / قبول کردن کوکی ها**
  Cookies are small pieces of text files which are often automatically stored by your Web browser. They are required for Web sites which need authentication but can also be used to track your identity. With this option turned on, every cookie is stored for a long time. If you want to allow cookies for this session only, deselect this option and select "Store cookies for this session only" (see below).

- **Show images on browsed pages / نمایش عکسها**
  If you are on a slow Internet connection, you may want deselect this option so the pages will be lighter, hence faster to load.

- **Show actual referring Web site / نمایش مسیرها**
  By default, your browser sends every Web site the URL you are coming from, where you have clicked on a link. These URLs are stored in the Web site log files and are analysed automatically. For increased privacy, you can deselect this option.

- **Strip meta information tags from pages / حذف تگ هاي متا**
  Meta tags are additional information stored in many Web sites to be used automatically by computer programs. Such information may include the name of the author, description of the site content or keywords for search engines. Filtering techniques could be run on these tags. You may leave this option checked to avoid presenting this information to keyword filters.

- **Strip page title / حذف عنوان صفحات**
  With this option turned on, SabzProxy removes the page title of the Web site, which you normally see in the title bar on top of your Web browser. This can be useful, for example to hide the name of the Web site you are visiting if you don't want surrounding people to see this when you minimize your browser.

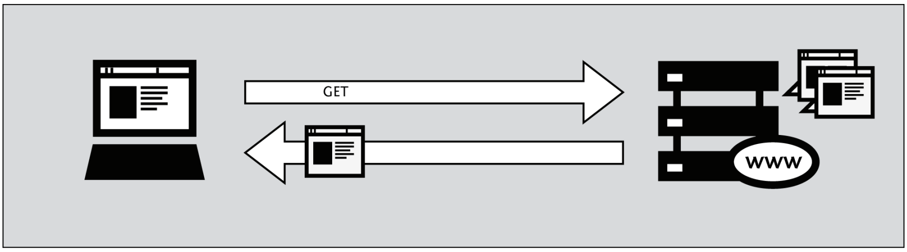
- **Store cookies for this session only / کوکي ها موقت**
  Similar to the "Allow cookies to be stored" option; with this option turned on, cookies are only stored until you close your SabzProxy session by exiting your Web browser.

FIREFOX AND ITS ADD-ONS

12. INTRODUCTION TO FIREFOX

Our guess is that you wouldn't be reading this chapter unless you already knew what a Web browser was. However, if you don't know, a browser is the software you use to visit and view Web sites on the Internet.

In an earlier chapter, we explained that the Internet is a giant network of computers, all connected to each other. Some of the computers are "Web servers" – computers that have Web sites on them. If you want to visit these sites from your computer or a mobile device, you need a way to surf around and display them. That's what a browser does.



One of the most popular browsers is Firefox, a free, open source Web browser created by the Mozilla foundation in 2003. Firefox runs on all the major operating systems – Windows, MacOS and Linux – and it has been translated into more than 75 languages. Best of all, It's completely free of charge.

WHERE TO GET FIREFOX

If you want to install Firefox you can find the installation files here: https://www.mozilla.com/en-US/firefox/

When you visit this site you will be presented automatically with the correct installation file for your operating system (Windows/Mac/Linux). For more information on how to install Firefox on each of these operating systems, please see the FLOSS Manuals Firefox manual: http://en.flossmanuals.net/firefox

WHAT IS A FIREFOX ADD-ON?

When you first download and install Firefox, it can handle basic browser tasks immediately. You can also add extra capabilities or change the way Firefox behaves by installing *add-ons*, small additions that extend Firefox's power. There are several kinds of add-ons:

- extensions that provide additional functionality to the browser
- themes that change Firefox's appearance
- plugins that help Firefox handle things it normally can't process (for instance Flash movies, Java applications, and so on).

The variety of add-ons available is enormous. You can add dictionaries for different languages, track the weather in other countries, get suggestions for Web sites that are similar to the one you are currently viewing, and much more.

Firefox keeps a list of current add-ons on its site (https://addons.mozilla.org/firefox), or you can browse them by category at https://addons.mozilla.org/firefox/browse.

Before you install any add-on, keep in mind that it can read a lot of information from your browser so it is very important to choose add-ons from trusted sources. Otherwise, an add-on you install might share information about you without your knowing, keep a record or the sites you have visited, or even harm your computer.

We recommend that you never install an add-on for Firefox unless it is available from the Firefox add-on pages. You should also never install Firefox unless you get the installation files from a trusted source. It is important to note that using Firefox on someone else's computer or in an Internet café increases your potential vulnerability.

In the next three chapters, we will look at some add-ons that are particularly relevant for dealing with Internet censorship.

13. NOSCRIPT AND ADBLOCK

While no tool can protect you completely against all threats to your online privacy and security, the Firefox extensions described in this chapter can significantly reduce your exposure to the most common ones, and increase your chances of remaining anonymous.

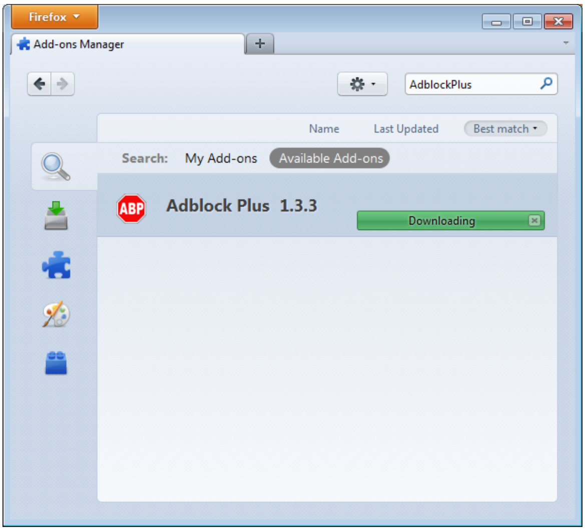
ADBLOCK PLUS

Adblock Plus (http://www.adblockplus.org) scans Web pages for advertisements and other content that may try to track you, and then blocks it. To keep current with the latest threats, AdBlock Plus relies on blacklists maintained by volunteers.

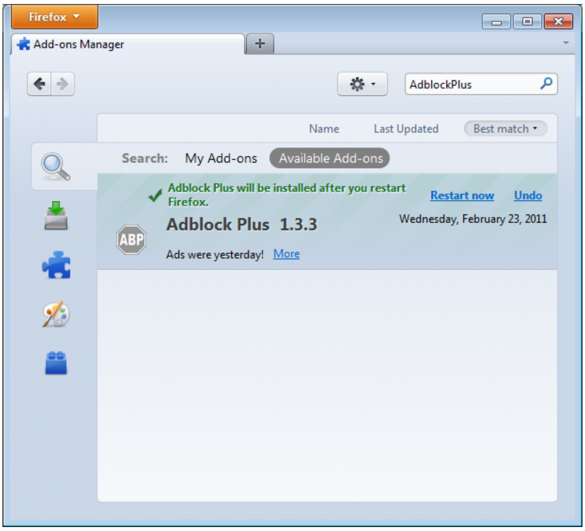
Getting started with AdBlock Plus

Once you have Firefox installed:

1. Download the latest version of AdBlock Plus from http://adblockplus.org/en/installation#release or search for the plugin with Firefox's Add-ons Manager ("Firefox" > "Add-ons").
2. Confirm that your want AdBlock Plus by clicking "Install Now".



3. After AdBlock Plus has been installed, Firefox will ask to restart.



Adblock Plus will be installed after you restart Firefox.

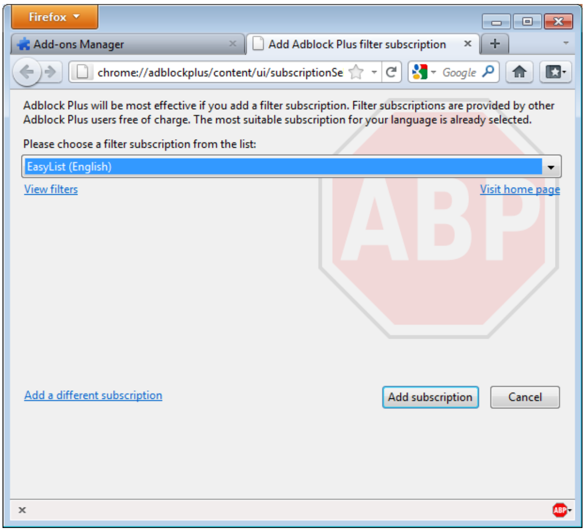
Adblock Plus 1.3.3

Wednesday, February 23, 2011

Ads were yesterday!

Choosing a filter subscription

Adblock Plus by itself doesn't do anything. It can see each element that a Web site attempts to load, but it doesn't know which ones should be blocked. This is what AdBlock's filters are for. After restarting Firefox, you will be asked to choose a filter subscription (free).



Firefox
Add-ons Manager
Add Adblock Plus filter subscription
chrome://adblockplus/content/ui/subscriptionSe
Google

Adblock Plus will be most effective if you add a filter subscription. Filter subscriptions are provided by other Adblock Plus users free of charge. The most suitable subscription for your language is already selected.

Please choose a filter subscription from the list:

EasyList (English)

View filters
Visit home page
Add a different subscription
Add subscription
Cancel

Which filter subscription should you choose? Adblock Plus offers a few in its dropdown menu and you may wish to learn about the strengths of each. A good filter to start protecting your privacy is EasyList (also available at http://easylist.adblockplus.org/en).

As tempting as it may seem, don't add as many subscriptions as you can get, since some may overlap, resulting in unexpected outcomes. EasyList (mainly targeted at English-language sites) works well with other EasyList extensions (such as region-specific lists like RuAdList or thematic lists like EasyPrivacy). But it collides with Fanboy's List (another list with main focus on English-language sites).

You can always change your filter subscriptions at any time within preferences (press Ctrl+Shift+E). Once you've made your changes, click OK.

Creating personalized filters

AdBlock Plus also lets you create your own filters, if you are so inclined. To add a filter, start with Adblock Plus preferences (Ctrl+Shift+E) and click on "Add Filter" at the bottom left corner of the window. Personalized filters may not replace the benefits of well-maintained blacklists like EasyList, but they're very useful for blocking specific content that isn't covered in the public lists. For example, if you wanted to prevent interaction with Facebook from other Web sites, you could add the following filter:

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

The first part (||facebook.*) will initially block everything coming from Facebook's domain. The second part ($domain=~facebook.com|~127.0.0.1) is an exception that tells the filter to allow Facebook requests only when you are in Facebook or if the Facebook requests come from 127.0.0.1 (your own computer) in order to keep certain features of Facebook working.

A guide on how to create your own Adblock Plus filters can be found at http://adblockplus.org/en/filters.

Enabling and disabling AdBlock Plus for specific elements or Web sites

You can see the elements identified by AdBlock Plus by clicking on the ABP icon in your browser (usually next to the search bar) and selecting "Open blockable items", or by pressing Ctrl+Shit+V. A window at the bottom of your browser will let you enable or disable each element on a case-by-case basis. Alternatively, you can disable AdBlock Plus for a specific domain or page by clicking on the ABP icon and ticking the option "Disable on [domain name]" or "Disable on this page only".

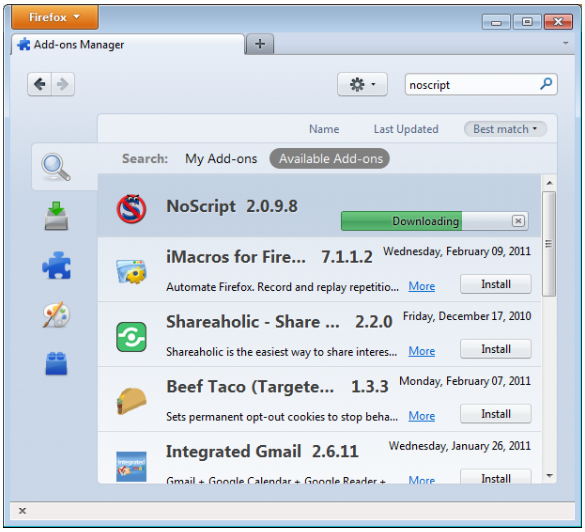
NOSCRIPT

The NoScript extension takes browser protection further by globally blocking all JavaScript, Java and other executable content that could load from a Web site and run on your computer. To tell NoScript to ignore specific sites, you need to add them to a whitelist. This may sound tedious, but NoScript does a good job in protecting Internet users from several threats such as cross-site scripting (when attackers place malicious code from one site in another site) and clickjacking (when clicking on an innocuous object on a page reveals confidential information or allows the attacker to take control of your computer). To get NoScript, visit http://addons.mozilla.org or http://noscript.net/getit.

The same method by which NoScript protects you can alter the appearance and functionality of good Web pages, too. Luckily, you can adjust how NoScript treats individual pages or Web sites manually – it is up to you to find the right balance between convenience and security.

Getting started with NoScript

1. Go to the NoScript download section at http://noscript.net/getit. Click on the green "INSTALL" button.
2. Confirm that you want NoScript by clicking "Install Now".



NoScript 2.0.9.8

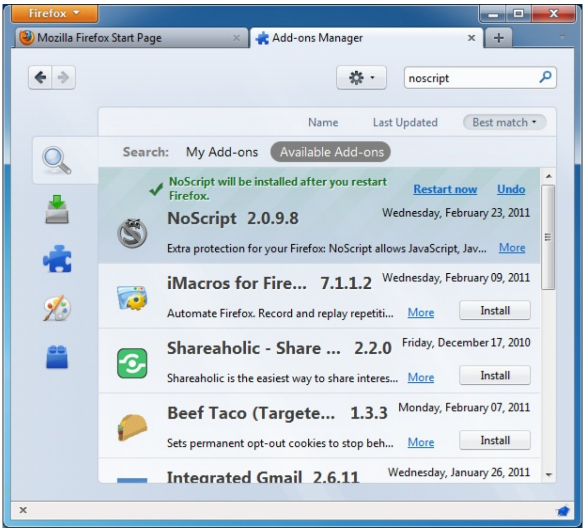
iMacros for Fire... 7.1.1.2 Wednesday, February 09, 2011
Automate Firefox. Record and replay repetitio...

Shareaholic - Share ... 2.2.0 Friday, December 17, 2010
Shareaholic is the easiest way to share interes...

Beef Taco (Targete... 1.3.3 Monday, February 07, 2011
Sets permanent opt-out cookies to stop beha...

Integrated Gmail 2.6.11 Wednesday, January 26, 2011
Gmail + Google Calendar + Google Reader + ...

3. Restart your browser when asked.



NoScript will be installed after you restart Firefox.

NoScript 2.0.9.8 Wednesday, February 23, 2011
Extra protection for your Firefox: NoScript allows JavaScript, Jav...

iMacros for Fire... 7.1.1.2 Wednesday, February 09, 2011
Automate Firefox. Record and replay repetiti...

Shareaholic - Share ... 2.2.0 Friday, December 17, 2010
Shareaholic is the easiest way to share interes...

Beef Taco (Targete... 1.3.3 Monday, February 07, 2011
Sets permanent opt-out cookies to stop beh...

Integrated Gmail 2.6.11 Wednesday, January 26, 2011

NoScript notifications and adding Web sites to your whitelist

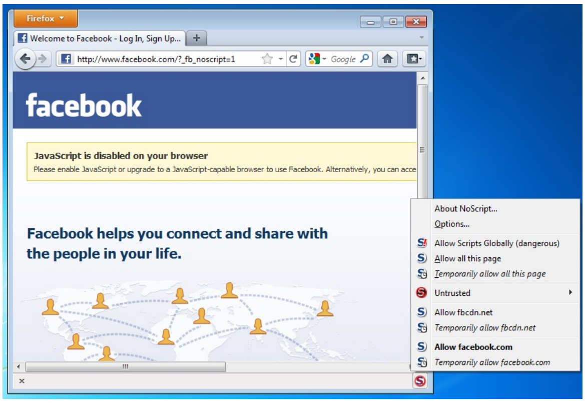
Once restarted, your browser will have a NoScript icon at the bottom right corner, where the status bar is, indicating what level of permission the current Web site has to execute content on your PC.

- Full protection: scripts are blocked for the current site and its subframes. Even if some of the script sources imported by the page are in your whitelist, code won't run (the hosting documents are not enabled).
- Very restricted: the main site is still forbidden, but some pieces (such as frames) are allowed. In this case, some code may be running, but the page is unlikely to work correctly because its main script source is still blocked.
- Limited permissions: scripts are allowed for the main document, but other active elements, or script sources imported by the page, are not allowed. This happens when there are multiple frames on a page or script elements that link to code hosted on other platforms.
- Mostly trusted: all the script sources for the page are allowed, but some embedded content (such as frames) are blocked.
- Selective protection: scripts are allowed for some URLs. All the others are marked as untrusted.
- All scripts are allowed for the current site.
- Scripts are allowed globally, however content marked as untrusted will not be loaded.

To add a site that you trust to your whitelist, click on the NoScript icon and select:

- "Allow [domain name]" to allow all scripts that are hosted under a specific domain name, or
- "Allow all this page" to allow complete script execution - including third party scripts that may be hosted elsewhere, but are imported by the main Web site.

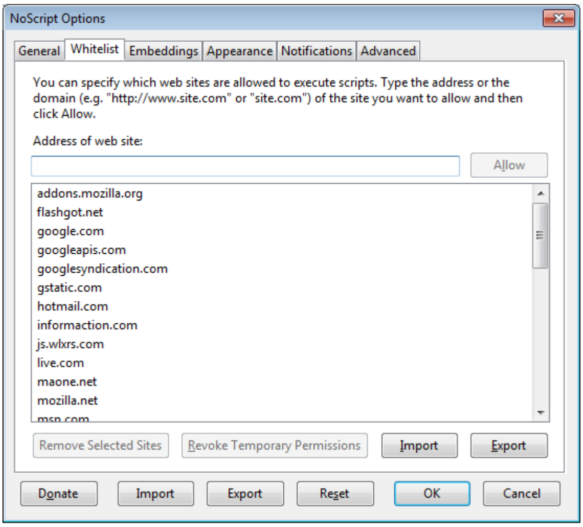
(You can also use the "Temporarily allow" options to allow content loading only for the current browsing session. This is useful for people who intend to visit a site just once, and who want to keep their whitelist at a manageable size.)


Firefox
Welcome to Facebook - Log In, Sign Up...
http://www.facebook.com/?_fb_noscript=1
Google
facebook
About NoScript...
Options...
Allow Scripts Globally (dangerous)
Allow all this page
Temporarily allow all this page
Untrusted
Allow fbcdn.net
Temporarily allow fbcdn.net
Allow facebook.com
Temporarily allow facebook.com

JavaScript is disabled on your browser
Please enable JavaScript or upgrade to a JavaScript-capable browser to use Facebook. Alternatively, you can acce

Facebook helps you connect and share with the people in your life.

Alternatively, you can add domain names directly to the whitelist by clicking on the NoScript button, selecting Options and then clicking on the Whitelist tab.



You can specify which web sites are allowed to execute scripts. Type the address or the domain (e.g. "http://www.site.com" or "site.com") of the site you want to allow and then click Allow.

Address of web site:

addons.mozilla.org
flashgot.net
google.com
googleapis.com
googlesyndication.com
gstatic.com
hotmail.com
informaction.com
js.wlxrs.com
live.com
maone.net
mozilla.net
msn.com

Marking content as untrusted

If you want to permanently prevent scripts from loading on a particular Web site, you can mark it as untrusted: just click the NoScript icon, open the "Untrusted" menu and select "Mark [domain name] as Untrusted". NoScript will remember your choice, even if the "Allow Scripts Globally" option is enabled.

14. HTTPS EVERYWHERE

HTTPS Everywhere is a Firefox add-on produced as a collaboration between The Tor Project (https://www.torproject.org) and the Electronic Frontier Foundation (https://eff.org/). It encrypts your communications with a number of major Web sites, including Google, Wikipedia, and popular social networking platforms such as Facebook and Twitter.

Many sites on the Web offer some support for encryption over HTTPS, but make it difficult to use. For instance, they may connect you to HTTP by default, even when HTTPS is available. Or they may fill encrypted pages with links that go back to the unencrypted site. This way, data (such as usernames and passwords) sent to and received by these Web sites are transferred as plain text and are easy to read by third parties.

The HTTPS Everywhere extension fixes these problems by rewriting all requests to these sites to HTTPS. (Although the extension is called "HTTPS Everywhere", it only activates HTTPS on a particular list of sites and can only use HTTPS on sites that have chosen to support it. It cannot make your connection to a site secure if that site does not offer HTTPS as an option.)

Please note that some of those sites still include a lot of content, such as images or icons, from third party domains that is not available over HTTPS. As always, if the browser's lock icon is broken or carries an exclamation mark, you may remain vulnerable to some adversaries that use active attacks or traffic analysis. However, the effort required to monitor your browsing should still be usefully increased.

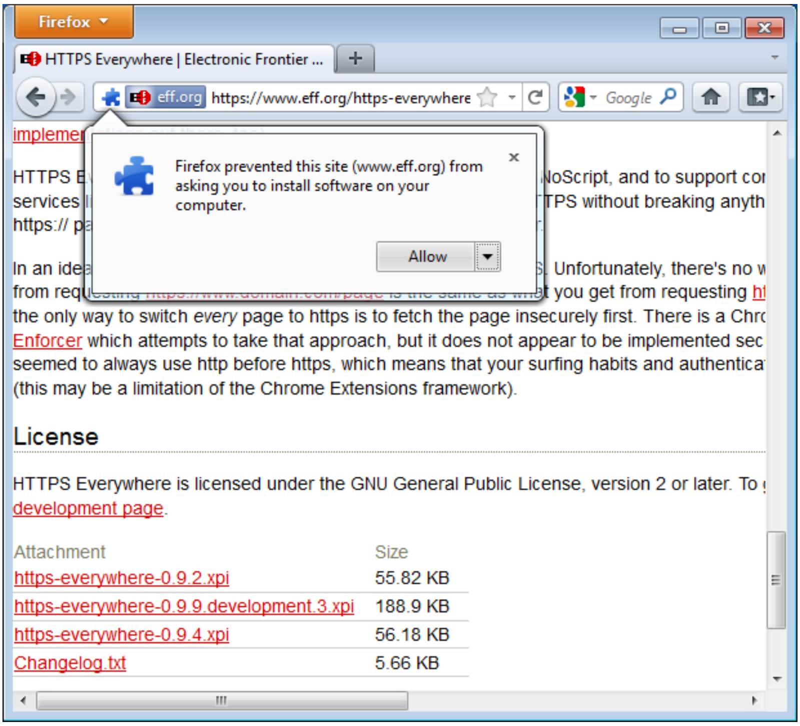
Some Web sites (such as Gmail) provide HTTPS support automatically, but using HTTPS Everywhere will also protect you from SSL-stripping attacks, in which an attacker hides the HTTPS version of the site from your computer if you initially try to access the HTTP version.

Additional information can be found at: https://www.eff.org/https-everywhere.

INSTALLATION

First, download the HTTPS Everywhere extension from the official Web site: https://www.eff.org/https-everywhere.

Select the newest release. In the example below, version 0.9.4 of HTTPS Everywhere was used. (A newer version may be available now.)



Firefox
HTTPS Everywhere | Electronic Frontier ...
eff.org
https://www.eff.org/https-everywhere
Google
Allow

Firefox prevented this site (www.eff.org) from asking you to install software on your computer.

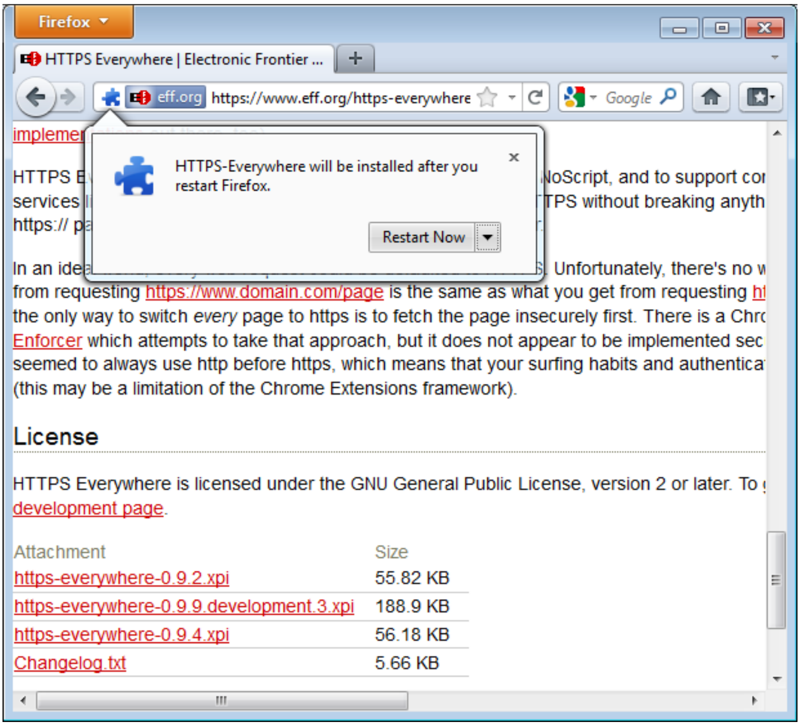
the only way to switch *every* page to https is to fetch the page insecurely first. There is a Chro
Enforcer which attempts to take that approach, but it does not appear to be implemented sec
seemed to always use http before https, which means that your surfing habits and authentica
(this may be a limitation of the Chrome Extensions framework).

License

HTTPS Everywhere is licensed under the GNU General Public License, version 2 or later. To
development page.

Attachment	Size
https-everywhere-0.9.2.xpi	55.82 KB
https-everywhere-0.9.9.development.3.xpi	188.9 KB
https-everywhere-0.9.4.xpi	56.18 KB
Changelog.txt	5.66 KB

Click on "Allow". You will then have to restart Firefox by clicking on the "Restart Now" button. HTTPS Everywhere is now installed.


Firefox
HTTPS Everywhere | Electronic Frontier ...
eff.org
https://www.eff.org/https-everywhere
Google
Restart Now

HTTPS-Everywhere will be installed after you restart Firefox.

implemer

HTTPS E NoScript, and to support co
services TPS without breaking anyth
https:// pa

In an idea Unfortunately, there's no w
from requesting https://www.domain.com/page is the same as what you get from requesting ht
the only way to switch *every* page to https is to fetch the page insecurely first. There is a Chro
Enforcer which attempts to take that approach, but it does not appear to be implemented sec
seemed to always use http before https, which means that your surfing habits and authentica
(this may be a limitation of the Chrome Extensions framework).

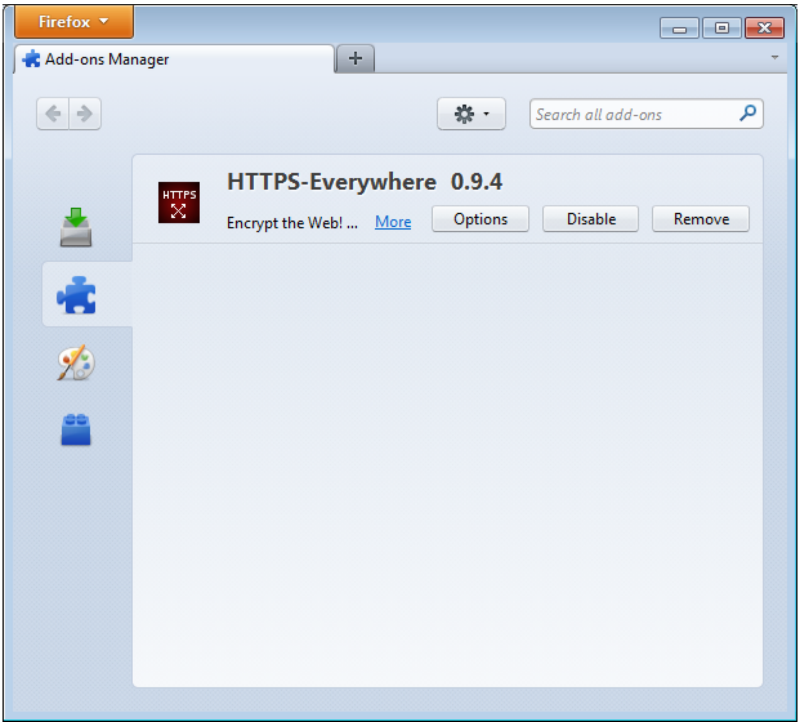
License

HTTPS Everywhere is licensed under the GNU General Public License, version 2 or later. To
development page.

Attachment	Size
https-everywhere-0.9.2.xpi	55.82 KB
https-everywhere-0.9.9.development.3.xpi	188.9 KB
https-everywhere-0.9.4.xpi	56.18 KB
Changelog.txt	5.66 KB

CONFIGURATION

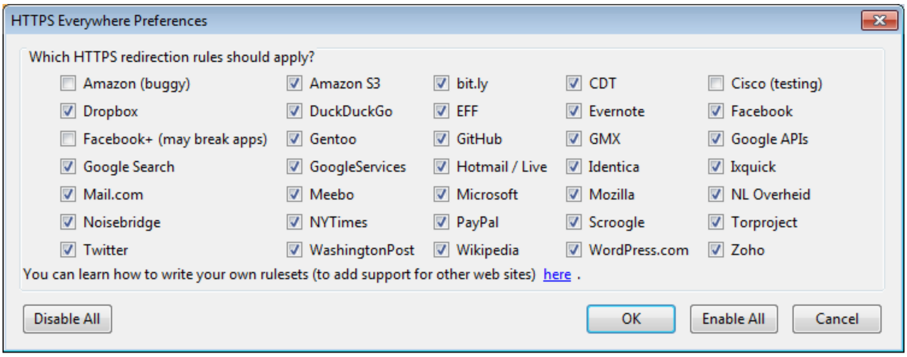
To access the HTTPS Everywhere settings panel in Firefox 4 (Linux), click on the Firefox menu at the top left on your screen and then select Add-ons Manager. (Note that in different versions of Firefox and different operating systems, the Add-ons Manager may be located in different places in the interface.)



HTTPS-Everywhere 0.9.4

Encrypt the Web! ...

Click on the Options button.



HTTPS Everywhere Preferences

Which HTTPS redirection rules should apply?

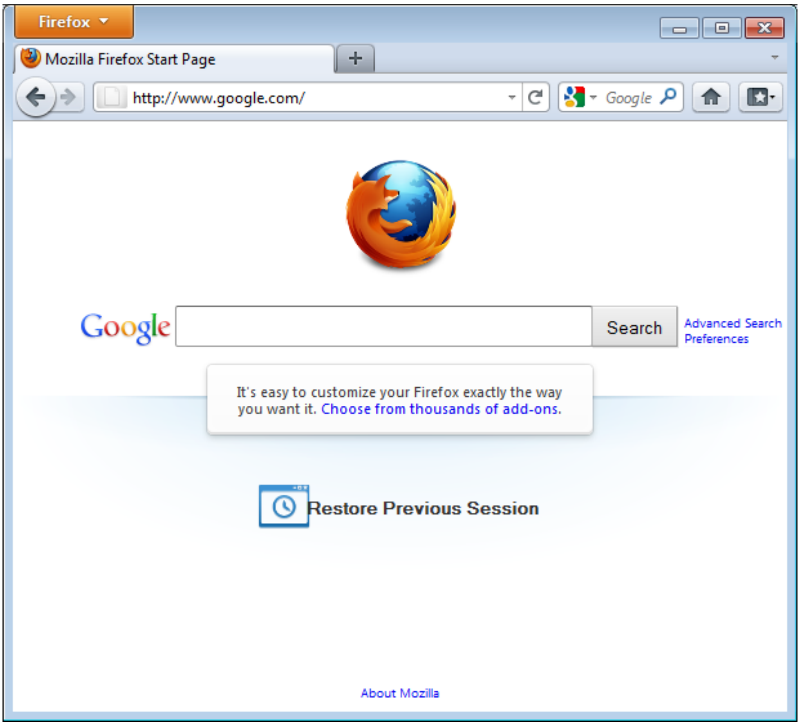
☐ Amazon (buggy)	☑ Amazon S3	☑ bit.ly	☑ CDT	☐ Cisco (testing)
☑ Dropbox	☑ DuckDuckGo	☑ EFF	☑ Evernote	☑ Facebook
☐ Facebook+ (may break apps)	☑ Gentoo	☑ GitHub	☑ GMX	☑ Google APIs
☑ Google Search	☑ GoogleServices	☑ Hotmail / Live	☑ Identica	☑ Ixquick
☑ Mail.com	☑ Meebo	☑ Microsoft	☑ Mozilla	☑ NL Overheid
☑ Noisebridge	☑ NYTimes	☑ PayPal	☑ Scroogle	☑ Torproject
☑ Twitter	☑ WashingtonPost	☑ Wikipedia	☑ WordPress.com	☑ Zoho

You can learn how to write your own rulesets (to add support for other web sites) here .

A list of all supported Web sites where HTTPS redirection rules should be applied will be displayed. If you have problems with a specific redirection rule, you can uncheck it here. In that case, HTTPS Everywhere will no longer modify your connections to that specific site.

USAGE

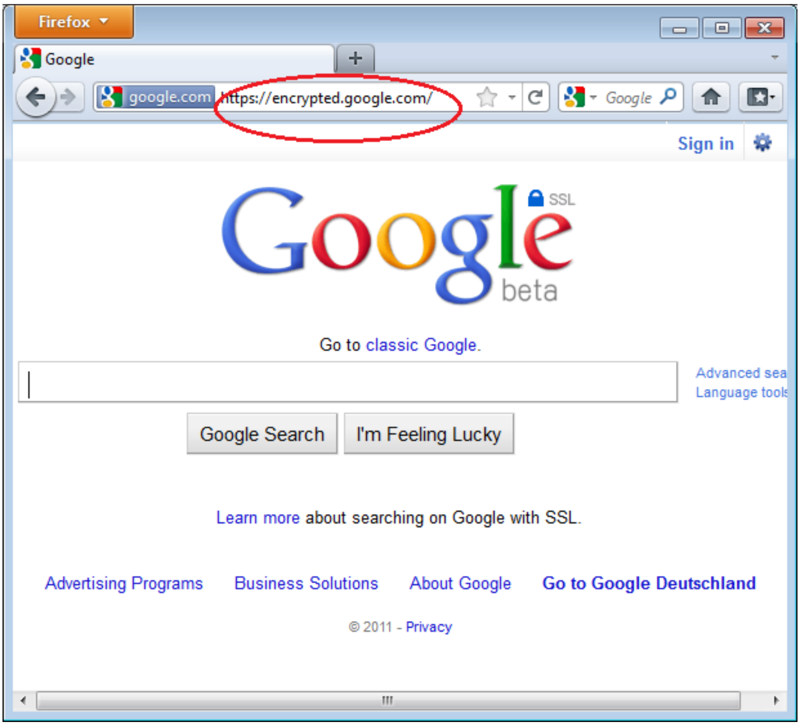
Once enabled and configured, HTTPS Everywhere is very easy and transparent to use. Type an insecure HTTP URL (for example, http://www.google.com).



http://www.google.com/

Firefox
Mozilla Firefox Start Page
Google
Google
Search
Advanced Search
Preferences
It's easy to customize your Firefox exactly the way you want it. Choose from thousands of add-ons.
Restore Previous Session
About Mozilla

Press Enter. You will be automatically redirected to the secure HTTPS encrypted Web site (in this example: https://encrypted.google.com). No other action is needed.



Go to classic Google.

Learn more about searching on Google with SSL.

If networks block HTTPS

Your network operator may decide to block the secure versions of Web sites in order to increase its ability to spy on what you do. In such cases, HTTPS Everywhere could prevent you from using these sites because it forces your browser to use only the secure version of these sites, never the insecure version. (For example, we heard about an airport Wi-Fi network where all HTTP connections were permitted, but not HTTPS connections. Perhaps the Wi-Fi operators were interested in watching what users did. At that airport, users with HTTPS Everywhere were not able to use certain Web sites unless they temporarily disabled HTTPS Everywhere.)

In this scenario, you might choose to use HTTPS Everywhere together with a circumvention technology such as Tor or a VPN in order to bypass the network's blocking of secure access to Web sites.

Adding support for additional sites in HTTPS Everywhere

You can add your own rules to the HTTPS Everywhere add-on for your favorite Web sites. You can find out how to do that at: https://www.eff.org/https-everywhere/rulesets. The benefit of adding rules is that they teach HTTPS Everywhere how to ensure that your access to these sites is secure. But remember: HTTPS Everywhere does *not* allow you to access sites securely unless the site operators have already chosen to make their sites available through HTTPS. If a site does not support HTTPS, there is no benefit to adding a ruleset for it.

If you are managing a Web site and have made an HTTPS version of the site available, a good practice would be to submit your Web site to the official HTTPS Everywhere release.

15. PROXY SETTINGS AND FOXYPROXY

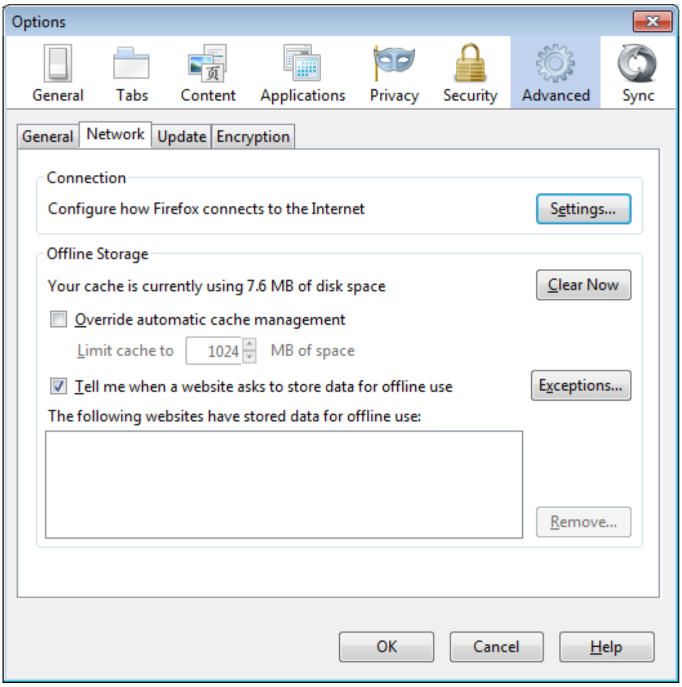
A proxy server allows you to reach a Web site or other Internet location even when direct access is blocked in your country or by your ISP. There are many different kinds of proxies, including:

- Web proxies, which only require that you know the proxy Web site's address. A Web proxy URL may look like http://www.example.com/cgi-bin/nph-proxy.cgi
- HTTP proxies, which require that you modify your Browser settings. HTTP proxies only work for Web content. You may get the information about a HTTP proxy in the format "proxy.example.com:3128" or "192.168.0.1:8080".
- SOCKS proxies, which also require that you modify your Browser settings. SOCKS proxies work for many different Internet applications, including e-mail and instant messaging tools. The SOCKS proxy information looks just like HTTP proxy information.

You can use a Web proxy directly without any configuration by typing in the URL. The HTTP and SOCKS proxies, however, have to be configured in your Web browser.

DEFAULT FIREFOX PROXY CONFIGURATION

In Firefox 4 (Linux), you enter the configuration screen by clicking on the Firefox menu at the top left on your screen and then selecting Options. In the pop-up window, select the icon labeled Advanced and then choose the Network tab. You should see this window:



Connection

Configure how Firefox connects to the Internet

Offline Storage

Your cache is currently using 7.6 MB of disk space

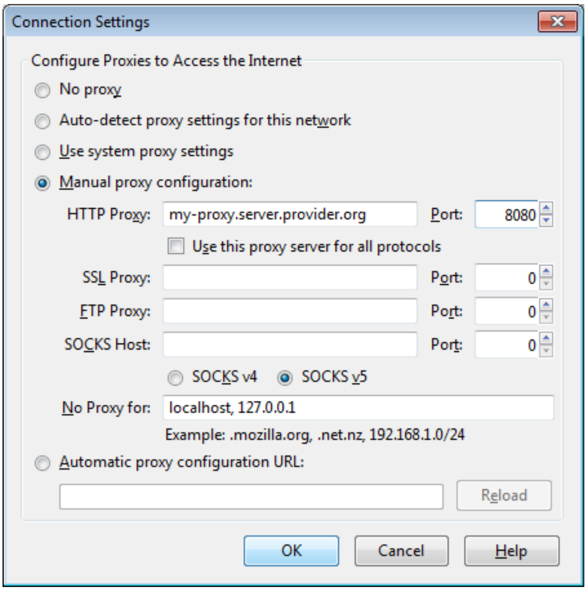
□ Override automatic cache management

Limit cache to 1024 MB of space

☑ Tell me when a website asks to store data for offline use

The following websites have stored data for offline use:

Select Settings, click on "Manual proxy configuration" and enter the information of the proxy server you want to use. Please remember that HTTP proxies and SOCKS proxies work differently and have to be entered in the corresponding fields. If there is a colon (:) in your proxy information, that is the separator between the proxy address and the port number. Your screen should look like this:



Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: my-proxy.server.provider.org Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

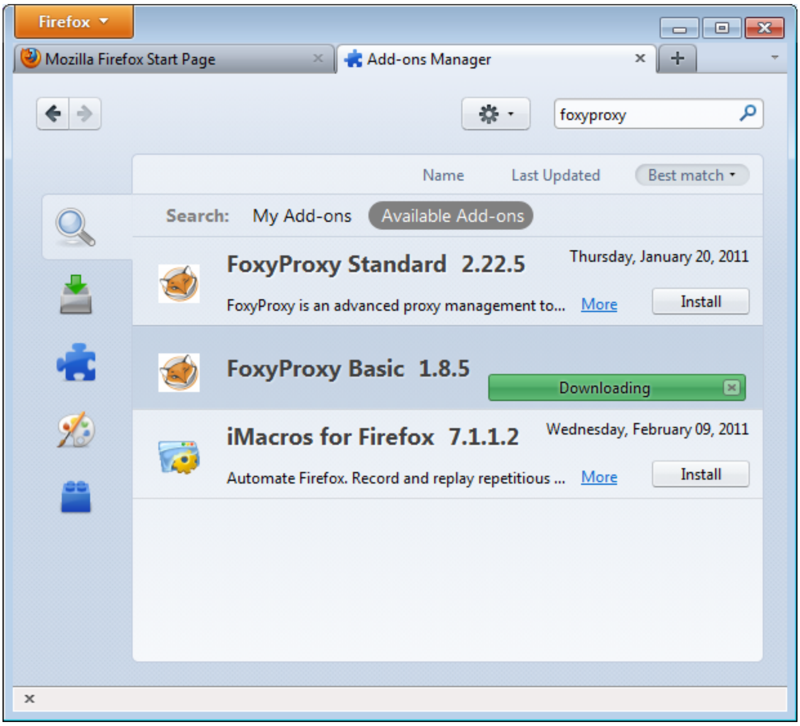
After you click OK, your configuration will be saved and your Web browser will automatically connect through that proxy on all future connections. If you get an error message such as, "The proxy server is refusing connections" or "Unable to find the proxy server", there is a problem with your proxy configuration. In that case, repeat the steps above and select "No proxy" in the last screen to deactivate the proxy.

FOXYPROXY

FoxyProxy is a freeware add-on for the Firefox Web browser which makes it easy to manage many different proxy servers and change between them. For details about FoxyProxy, visit http://getfoxyproxy.org/.

Installation

In Firefox 4 (Linux), click on the Firefox menu at the top left on your screen and then select Add-ons. In the pop-up window, type the name of the add-on you want to install (in this case "FoxyProxy") in the search box on the top right and click Enter. In the search results, you will see two different versions of FoxyProxy: Standard and Basic. For a full comparison of the two free editions, visit http://getfoxyproxy.org/downloads.html#editions, but the Basic edition is sufficient for basic circumvention needs. After deciding which edition you want, click Install.

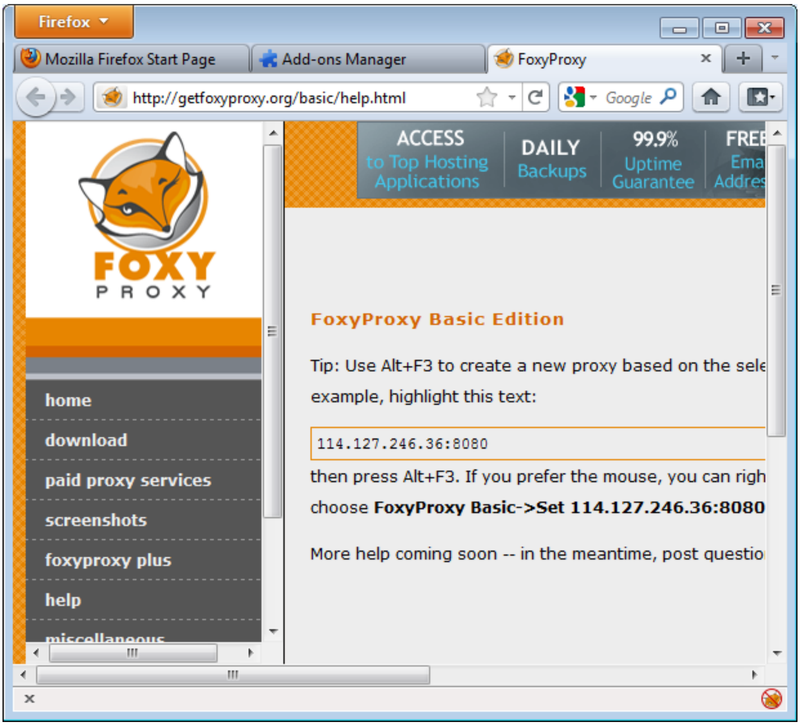


FoxyProxy Standard 2.22.5 — Thursday, January 20, 2011
FoxyProxy is an advanced proxy management to...

FoxyProxy Basic 1.8.5

iMacros for Firefox 7.1.1.2 — Wednesday, February 09, 2011
Automate Firefox. Record and replay repetitious ...

After installation, Firefox should restart and open the Help site of FoxyProxy. You should see the FoxyProxy icon at the bottom right.



FoxyProxy Basic Edition

Tip: Use Alt+F3 to create a new proxy based on the sele
example, highlight this text:

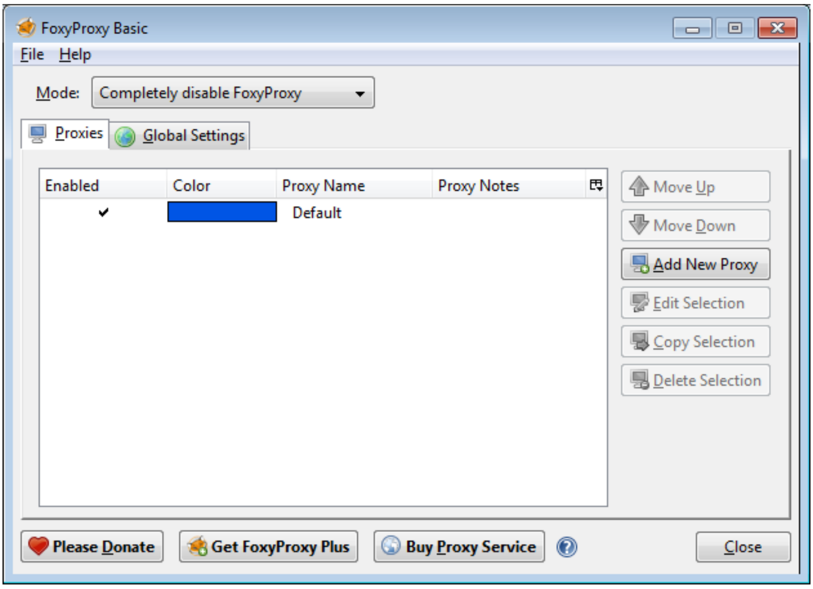
114.127.246.36:8080

then press Alt+F3. If you prefer the mouse, you can righ
choose **FoxyProxy Basic->Set 114.127.246.36:8080**

More help coming soon -- in the meantime, post questio

Configuration

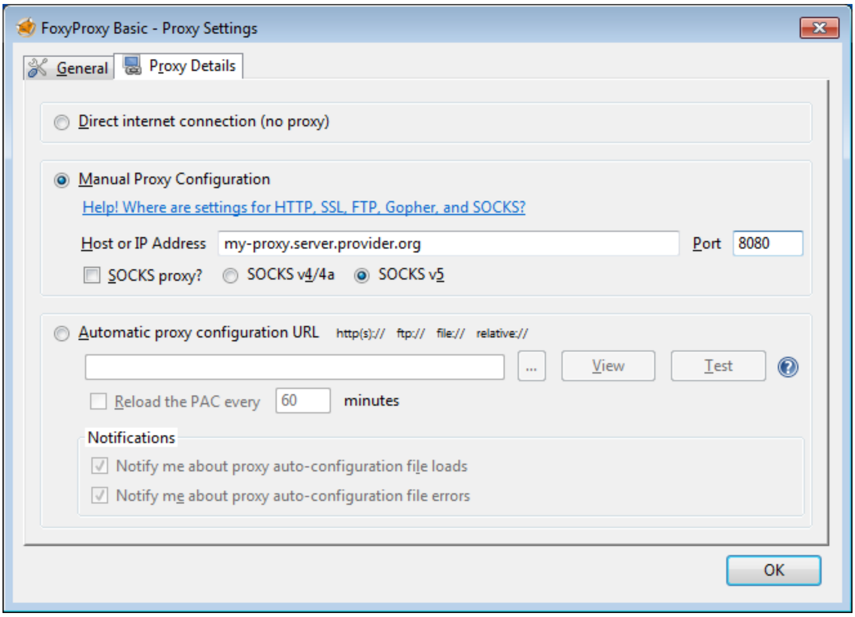
For FoxyProxy to do its job, it needs to know what proxy settings to use. Open the configuration window by clicking the icon at the bottom right of the Firefox window. The configuration window looks like this:



Mode: Completely disable FoxyProxy

Enabled	Color	Proxy Name	Proxy Notes
✓	🟦	Default	

Click on "Add New Proxy". In the following window, enter the proxy details in a similar way to the default Firefox proxy configuration:


FoxyProxy Basic - Proxy Settings
General
Proxy Details
Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?
http(s)://
ftp://
file://
relative://
...
View
Test
OK

○ Direct internet connection (no proxy)

● Manual Proxy Configuration

Host or IP Address: my-proxy.server.provider.org Port: 8080

□ SOCKS proxy? ○ SOCKS v4/4a ● SOCKS v5

○ Automatic proxy configuration URL

□ Reload the PAC every 60 minutes

Notifications

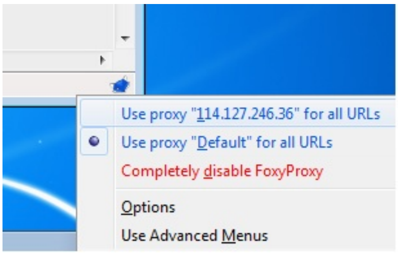
☑ Notify me about proxy auto-configuration file loads

☑ Notify me about proxy auto-configuration file errors

Select "Manual Proxy Configuration", enter the host or IP address and the port of your proxy in the appropriate fields. Check "SOCKS proxy?" if applicable, then click OK. You can add more proxies by repeating the steps above.

Usage

You can switch among your proxies (or choose not to use a proxy) by right-clicking on the fox icon on the bottom right of your Firefox window:


Use proxy "114.127.246.36" for all URLs
● Use proxy "Default" for all URLs
Completely disable FoxyProxy
Options
Use Advanced Menus

To select a proxy server, simply left-click on the proxy you want to use.

TOOLS

16. INTRODUCTION

The basic idea of circumventing Internet censorship is to route the requests over a third server which is not blocked and is connected to the Internet through a non filtered connection. This chapter explains some of the tools which make it possible to use such a server in order to defeat Internet blocking, filtering, and monitoring. The choice of which tool might best accomplish your objectives should be based on an initial assessment on the type of content you want to access, your available resources, and the risks of doing so.

Tools to defeat Internet blocking, filtering and monitoring are designed to deal with different obstacles and threats. They may facilitate:

- **Circumventing censorship**: enabling you to read or author content, send or receive information, or communicate with particular people, sites or services by bypassing attempts to prevent you from doing so. Similar to the operation of the Google cache or an RSS aggregator which can be used to access a blocked Web site indirectly.
- **Preventing eavesdropping**: keeping communications private, so that nobody can see or hear the content of what you're communicating (even if they might still be able to see with whom you're communicating). Tools that try to circumvent censorship without also preventing eavesdropping may remain vulnerable to censorship by keyword filters that block all communications containing certain prohibited words. For example, various forms of encryption, such as HTTPS or SSH, make the information unreadable to anyone other than the sender and receiver. An eavesdropper will see which user is connecting to which Web server, but from the content he can only see a string of characters that looks like nonsense.
- **Remaining anonymous**: the ability to communicate so that no one can connect you to the information or people you are connecting with – neither the operator of your Internet connection nor the sites or people with whom you're communicating. Many proxy servers and proxy tools don't offer perfect, or *any*, anonymity: the proxy operator is able to observe the traffic going into and out of the proxy and easily determine who is sending it, when they're sending it, and how often they're sending it; a malicious observer on either side of the connection is able to gather the same information. Tools like Tor are designed to make it difficult for attackers to gather this kind of information about users by limiting the amount of information any node in the network can have about the user's identity or location.
- **Concealing what you are doing**: disguising the communications you send so that someone spying on you will not be able to tell that you are trying to circumvent censorship. For example, steganography, the hiding of text messages within an ordinary image file, may conceal that you are using a circumvention tool at all. Using a network with many kinds of users means that an adversary can not tell what you are doing because of your choice of software. This is especially good when others are using the same system to get to uncontroversial content.

Some tools protect your communications in only one of these ways. For example, many proxies can circumvent censorship but don't prevent eavesdropping. It's important to understand that you may need a combination of tools to achieve your goal.

Each kind of protection is relevant to different people in different situations. When you choose tools that bypass Internet censorship, you should keep in mind what kind of protection you need and whether the particular set of tools you're using can provide that sort of protection. For example, what will happen if someone detects that you are attempting to circumvent a censorship system? Is accessing your main concern, or do you need to remain anonymous while doing so?

Sometimes, one tool can be used to defeat censorship and protect anonymity, but the steps for each are different. For instance, Tor software is commonly used for both purposes, but Tor users who are most concerned with one or the other will use Tor differently. For anonymity reasons, it is important that you use the Web browser bundled with Tor, since it has been modified to prevent leaking of your real identity.

AN IMPORTANT WARNING

Most circumvention tools can be detected with sufficient effort by network operators or government agencies, since the traffic they generate may show distinctive patterns. This is certainly true for circumvention methods that don't use encryption, but it can also be true for methods that do. It's very difficult to keep secret the fact that you're using technology to circumvent filtering, especially if you use a fairly popular technique or continue using the same service or method for a long period of time. Also, there are ways to discover your behavior that do not rely on technology: in-person observation, surveillance, or many other forms of traditional human information-gathering.

We cannot provide specific advice on threat analysis or the choice of tools to meet the threats. The risks are different in each situation and country, and change frequently. You should always expect that those attempting to restrict communications or activities will continue to improve their methods.

If you are doing something that may put you at risk in the location where you are, you should make your own judgments about your security and (if possible) consult experts.

- Most often, you will have to rely on a service provided by a stranger. Be aware that they may have access to information about where you are coming from, the sites you are visiting and even the passwords you enter on unencrypted Web sites. Even if you know and trust the person running a single-hop proxy or VPN, they may be hacked or forced to compromise your information.
- Remember that the promises of anonymity and security made by different systems may not be accurate. Look for independent confirmation. Open source tools can be evaluated by tech-savvy friends. Security flaws in open source tools can be discovered and fixed by volunteers. It is difficult to do the same with proprietary software.
- Achieving anonymity or security may require you to be disciplined and carefully obey certain security procedures and practices. Ignoring security procedures may dramatically reduce the security protections you receive. It is dangerous to think that it is possible to have a "one click solution" for anonymity or security. For instance, routing your traffic through a proxy or through Tor is not enough. Be sure to use encryption, keep your computer safe and avoid leaking your identity in the content you post.
- Be aware that people (or governments) may set up honeypots – fake Web sites and proxies that pretend to offer secure communication or censorship circumvention but actually capture the communications from unwitting users.
- Sometimes even "Policeware" may be installed on users' computers – either remotely or directly – that acts like malware, monitoring all activities on the computer even when it is not connected to the Internet and undermining most other preventive security measures.
- Pay attention to non-technical threats. What happens if someone steals your computer or mobile phone or that of your best friend? What if an Internet café staff member looks over your shoulder or points a camera to your screen or keyboard? What happens if someone sits down at a computer in a café somewhere where your friend has forgotten to log out and sends you a message pretending to be from her? What if someone in your social network is arrested and forced to give up passwords?
- If there are laws or regulations that restrict or prohibit the materials you are accessing or the activities you are undertaking, be aware of the possible consequences.

To learn more about digital security and privacy, read:

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

17. FREEGATE

Freegate is a proxy tool for Windows users that was initially developed by DIT-INC to bypass Internet censorship in China and Iran.

GENERAL INFORMATION

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

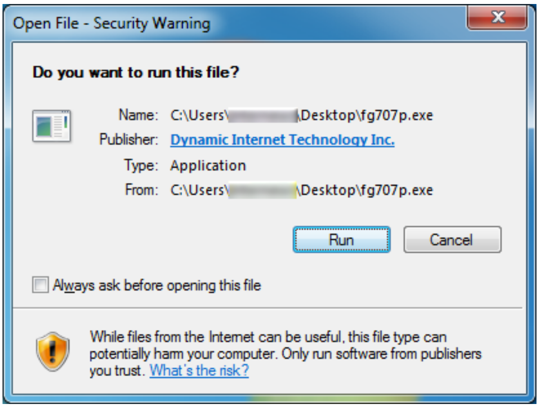
HOW TO GET FREEGATE

You can download the software for free at http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/Freegate.shtml.

You will get a file with the extension .zip, which you have to extract first. Right-click on the downloaded file and select "Extract All", then click on the button "Extract". The resulting file is about 1.5 MB. The name of the executable file may look like a short series of letters and numbers (e.g. "fg707p.exe").

INSTALLATION

When you run the application for the first time, you may see a Security Warning. You can accept this Security Warning by unchecking the box "Always ask before opening this file" and clicking Run.



Open File - Security Warning

Do you want to run this file?

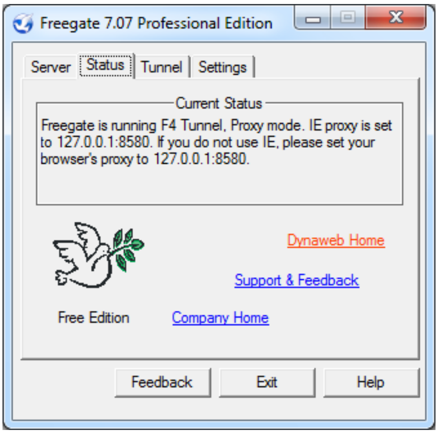
Name: C:\Users\[redacted]\Desktop\fg707p.exe
Publisher: Dynamic Internet Technology Inc.
Type: Application
From: C:\Users\[redacted]\Desktop\fg707p.exe

□ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

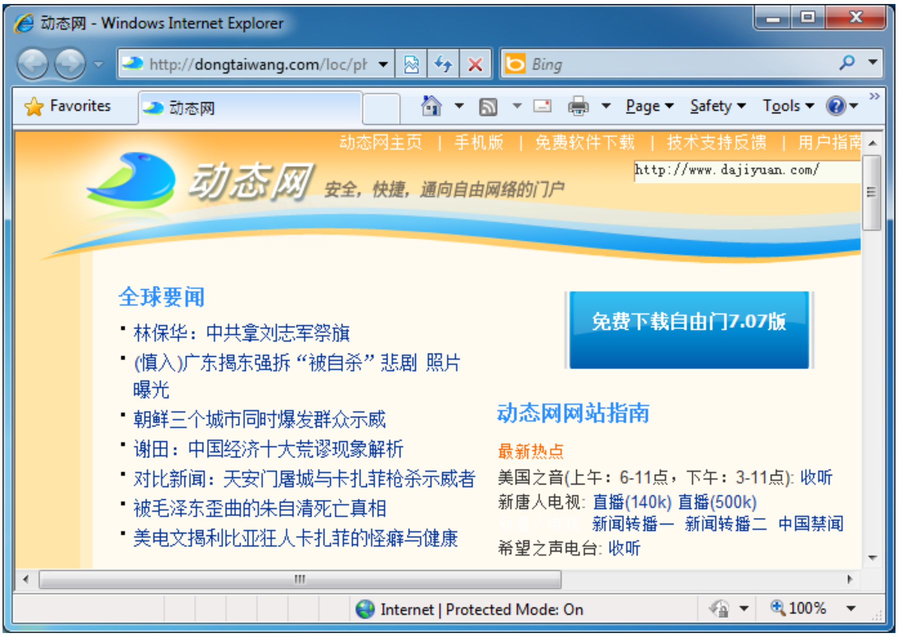
RUNNING FREEGATE

Now the application should start and connect automatically to a server.



Freegate is running F4 Tunnel, Proxy mode. IE proxy is set to 127.0.0.1:8580. If you do not use IE, please set your browser's proxy to 127.0.0.1:8580.

When the secure tunnel has started successfully, you will see the Freegate status Window and a new instance of the Internet Explorer will open automatically with the URL "http://dongtaiwang.com/loc/phome.php?v7.07&l=409" loaded, depending on your version and language. This is the confirmation that you are using Freegate correctly through an encrypted tunnel.


动态网 - Windows Internet Explorer
http://dongtaiwang.com/loc/pł
Bing
Favorites
动态网
Page
Safety
Tools
动态网主页 | 手机版 | 免费软件下载 | 技术支持反馈 | 用户指南
http://www.dajiyuan.com/
动态网
安全，快捷，通向自由网络的门户
免费下载自由门7.07版
Internet | Protected Mode: On
100%

全球要闻

- 林保华：中共拿刘志军祭旗
- (慎入)广东揭东强拆“被自杀”悲剧 照片曝光
- 朝鲜三个城市同时爆发群众示威
- 谢田：中国经济十大荒谬现象解析
- 对比新闻：天安门屠城与卡扎菲枪杀示威者
- 被毛泽东歪曲的朱自清死亡真相
- 美电文揭利比亚狂人卡扎菲的怪癖与健康

动态网网站指南

最新热点

美国之音(上午：6-11点，下午：3-11点): 收听
新唐人电视: 直播(140k) 直播(500k)
新闻转播一 新闻转播二 中国禁闻
希望之声电台: 收听

If all has gone well, you can start browsing normally using the automatically-opened Internet Explorer window to get around Internet censorship.

If you want to use another application with Freegate (for example the Firefox Web browser or the Pidgin instant messaging client), you will have to configure them to use Freegate as a proxy server. The IP is 127.0.0.1, and the port is 8580.

Under the Settings tab in Freegate, you can choose your interface language from English, Traditional Chinese, Simplified Chinese, Farsi and Spanish. Under Status, you can track your upload/download traffic through the Freegate network. The Server tab allows you to pick from several severs, one of which may be faster than your current connection.

18. SIMURGH

Simurgh (which means "phoenix" in Persian) is a lightweight stand-alone proxy software and service. This means that it can be run without any prior installation or administrator rights on the computer. You can copy it to your USB flash drive and use it on a shared computer (in an Internet café, for example).

GENERAL INFORMATION

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

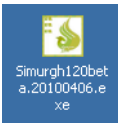
DOWNLOADING SIMURGH

To use the Simurgh service, download the tool for free from https://simurghesabz.net/.

It is available for any version of Microsoft Windows. The size of the file is less than 1MB, so it can be downloaded even on a slow Internet connection in a reasonable time.

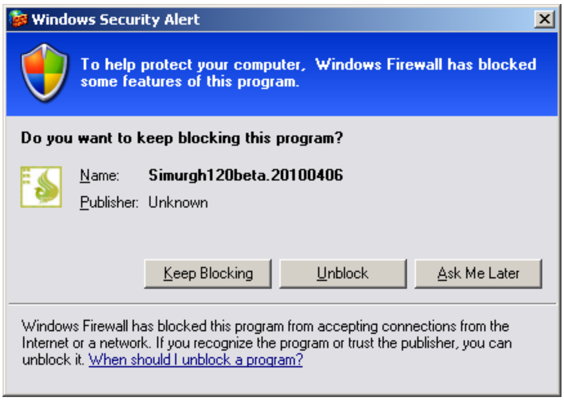
USING SIMURGH

To start Simurgh, click on the file you have downloaded. By default, files downloaded with Microsoft Internet Explorer are located on your Desktop and files downloaded with Mozilla Firefox are located in "My Documents" and then "Downloads".



Note that when you run Simurgh for the first time, you may encounter a Windows Security Alert which asks if you want to keep blocking Simurgh. Since Simurgh has to communicate with the Internet in order to work it is very important that you select "Unblock" or "Allow Access" (depending on your version of Microsoft Windows).

You may see this warning pop-up:



To help protect your computer, Windows Firewall has blocked some features of this program.

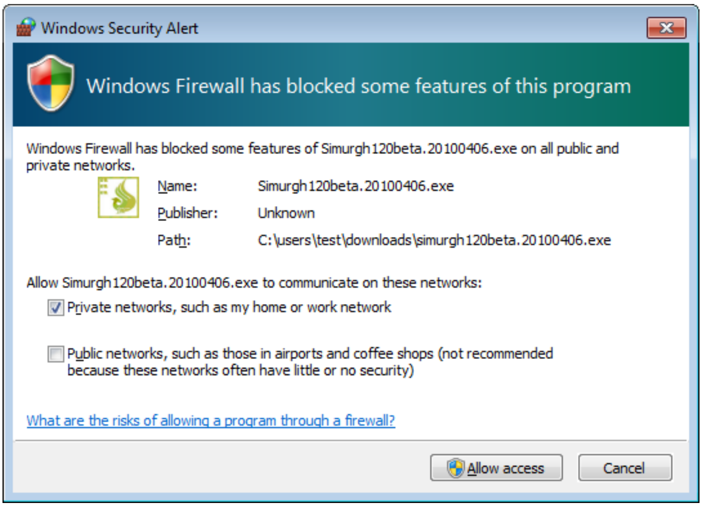
Do you want to keep blocking this program?

Name: Simurgh120beta.20100406

Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

or this one:



Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of Simurgh120beta.20100406.exe on all public and private networks.

Name: Simurgh120beta.20100406.exe

Publisher: Unknown

Path: C:\users\test\downloads\simurgh120beta.20100406.exe

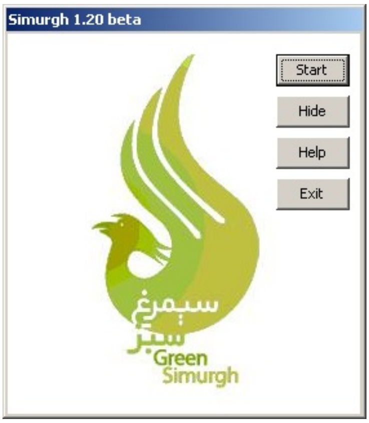
Allow Simurgh120beta.20100406.exe to communicate on these networks:

☑ Private networks, such as my home or work network

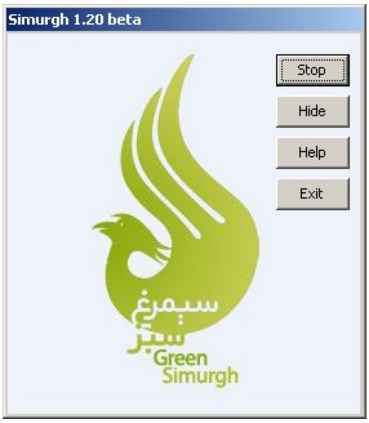
☐ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

After you have successfully started Simurgh, click on Start to create a secure connection.

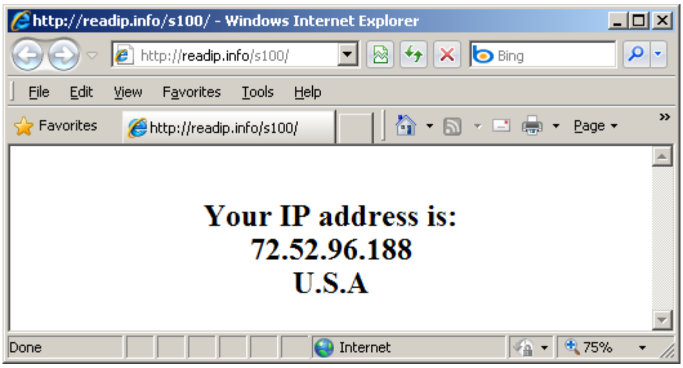


When the Start button changed to a Stop button, Simurgh has successfully connected to its servers.



Make sure you are connected to the Simurgh server

Now a new window of your Internet Explorer browser will open with a test page. If you see your connection originating from another country, such as U.S.A., this confirms that Simurgh has successfully changed the settings of your browser and you are automatically surfing over the secure Simurgh connection.



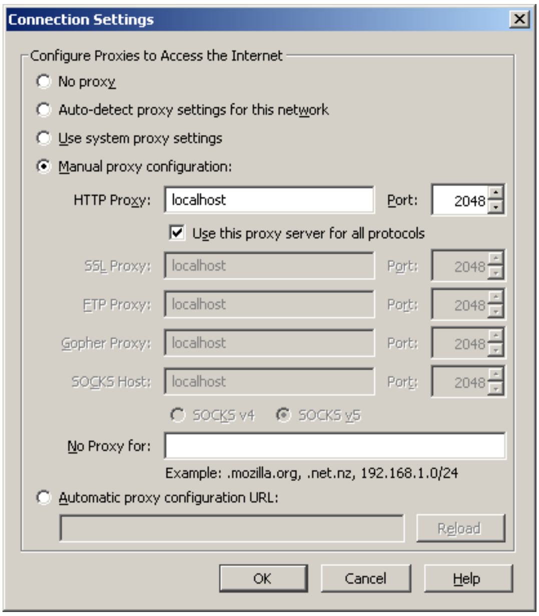
Your IP address is:
72.52.96.188
U.S.A

You can also use the website http://www.geoiptool.com to check where your connection appears to be from. If the websites shows your location very far away (in another country such as the USA), you are using the secure Simurgh connection.

USING SIMURGH WITH MOZILLA FIREFOX

In order to use another web browser like Mozilla Firefox, you need to configure it to use the HTTP proxy "localhost" with the port 2048.

In Firefox, you can find the proxy settings via Tools > Options > Network > Settings.
In the "Connection settings" window choose "Manual proxy configuration" and enter "localhost" (without the quotemarks) as the HTTP proxy and the port 2048, as shown in the screenshot below. To accept the new settings, click OK.



○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration:

HTTP Proxy: localhost Port: 2048

☑ Use this proxy server for all protocols

SSL Proxy: localhost Port: 2048

FTP Proxy: localhost Port: 2048

Gopher Proxy: localhost Port: 2048

SOCKS Host: localhost Port: 2048

○ SOCKS v4 ● SOCKS v5

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

19. ULTRASURF

UltraSurf, from developer UltraReach Internet Corp, is a proxy tool designed to help Chinese Internet users to get around their censorship. It may work for users in other countries as well.

GENERAL INFORMATION

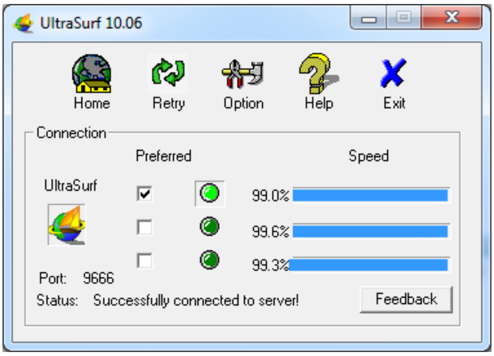
Supported operating system	⊞
Localization	English
Web site	http://www.ultrareach.com
Support	FAQ: http://www.ultrareach.com/usercenter_en.htm

HOW TO GET ULTRASURF

You can download the free software (for Windows only), at http://www.ultrareach.com or http://www.ultrareach.net/ or http://www.wujie.net (the latter page is in Chinese, but the download is still easy to find and in English).

INSTALLING AND USING ULTRASURF

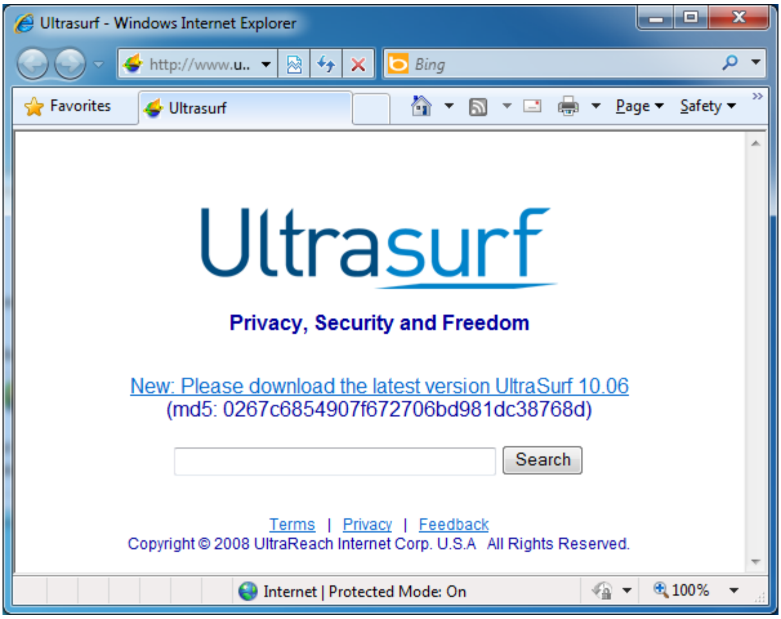
Once you have downloaded the file, named something like "u1006.zip" (depending on the version number), extract it by right-clicking the file and selecting "Extract All". Double-click the new "u1006" icon to start the application.



☑ ● 99.0%
□ ● 99.6%
□ ● 99.3%

Port: 9666
Status: Successfully connected to server!

UltraSurf will automatically open Internet Explorer and display the UltraSurf search page http://www.ultrareach.com/search.htm. You can now start browsing using the instance of Internet Explorer that UltraSurf has launched.


Ultrasurf - Windows Internet Explorer
http://www.u..
Bing
Favorites
Ultrasurf
Page
Safety
Ultrasurf
Search
Terms | Privacy | Feedback
Internet | Protected Mode: On
100%

Privacy, Security and Freedom

New: Please download the latest version UltraSurf 10.06
(md5: 0267c6854907f672706bd981dc38768d)

Copyright © 2008 UltraReach Internet Corp. U.S.A All Rights Reserved.

If you want to use another application with UltraSurf (for example the Firefox Web browser or the Pidgin instant messaging client), you need to configure them to use the UltraSurf client as a proxy server: the IP is 127.0.0.1 (your PC, also known as "localhost") and the port is 9666.

You can open the UltraSurf User Guide by clicking Help in the UltraSurf main window.

Info on Chinese UltraSurf (wujie): http://www.internetfreedom.org/UltraSurf

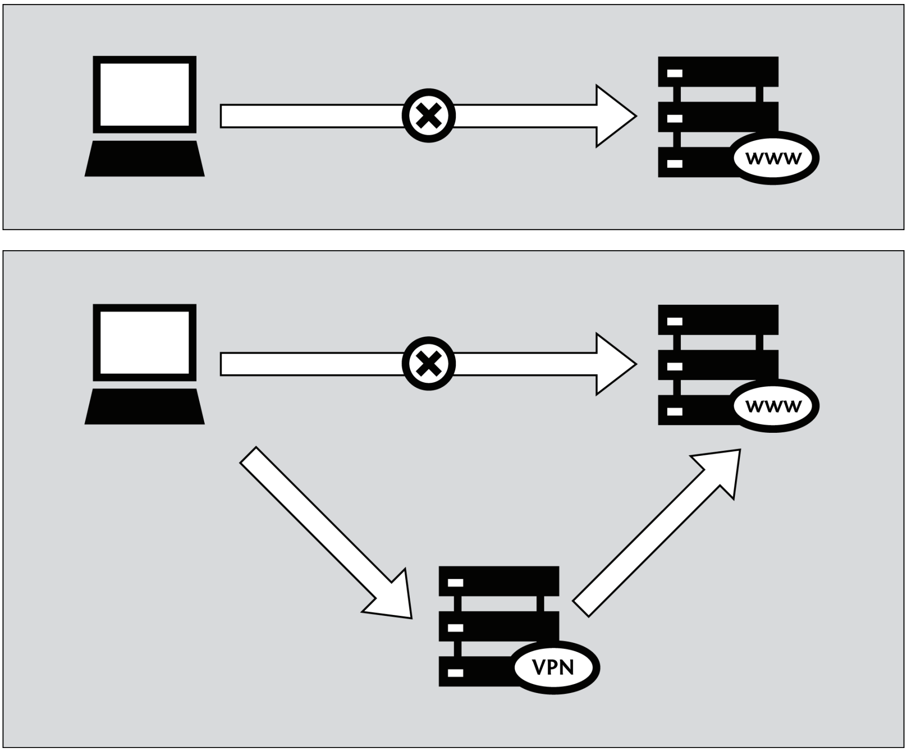
Chinese user guide: http://www.wujie.net/userguide.htm

20. VPN SERVICES

A **VPN (virtual private network)** encrypts and tunnels all Internet traffic between yourself and another computer. This computer might belong to a commercial VPN service, your organization, or a trusted contact.

Because VPN services tunnel all Internet traffic, they can be used for e-mail, instant messaging, **Voice over IP** (VoIP) and any other Internet service in addition to Web browsing, making everything that travels through the tunnel unreadable to anyone along the way.

If the tunnel ends outside the area where the Internet is being restricted, this can be an effective method of **circumvention**, since the filtering entity/server sees only encrypted data, and has no way of knowing what data is passing through the tunnel. It has the additional effect of making all your different kinds of traffic look similar to an eavesdropper.



Since many international companies use VPN technology to allow employees who need access to sensitive financial or other information to access the companies' computer systems from home or other remote locations over the Internet, VPN technology is less likely to be blocked than the technologies used only for circumvention purposes.

It is important to note that the data is only encrypted as far as the end of the tunnel, and then travels unencrypted to its final destination. If, for example, you set up a tunnel to a commercial VPN provider, and then request the Web page http://news.bbc.co.uk through the tunnel, the data will be encrypted from your computer to the VPN provider's computer at the other end, but from there it will be unencrypted to the servers run by the BBC, just like normal Internet traffic. This means that the VPN provider, the BBC and anyone with control over a system between these two servers, will, in theory, be able to see what data you sent or have requested.

USING VPN SERVICES

VPN services might or might not require installation of client-side software (many rely on existing VPN support in Windows, Mac OS or GNU/Linux and so need no extra client software).

Using a VPN service requires you to trust the owners of the service, but provides a simple and convenient method of bypassing Internet filtering, for free or for a monthly fee generally between 5 and 10 US dollars, depending on the service. Free services are often either ad-supported, or limit the bandwidth and/or the maximum traffic allowed over a given period.

Popular free VPN services:

- Hotspot Shield, https://hotspotshield.com
  According to a 2010 report from the Berkman Center, Hotspot Shield is overwhelmingly the most popular VPN service. For more details on how to get and use Hotspot Shield, read the "Hotspot Shield" chapter of this manual.

- UltraVPN, http://www.ultravpn.fr
- FreeVPN, http://www.thefreevpn.com
- CyberGhost, http://cyberghostvpn.com
- Air VPN, https://airvpn.org
- Vpnod, http://www.vpnod.com
- VpnSteel, http://www.vpnsteel.com
- Loki Network Project, http://www.projectloki.com
- ItsHidden, http://itshidden.com

Examples of paid VPN services include Anonymizer, GhostSurf, XeroBank, HotSpotVPN, WiTopia, VPN Swiss, Steganos, Hamachi LogMeIn, Relakks, Skydur, iPig, *iVPN.net*, FindNot, Dold, UnblockVPN and SecureIX.

You can find a list of free and paid VPN providers, with their monthly fee and technical characteristics at http://en.cship.org/wiki/VPN.

VPN STANDARDS AND ENCRYPTION

There are a number of different standards for setting up VPN networks, including **IPSec**, **SSL/TLS** and **PPTP**, that vary in terms of complexity, the level of security they provide, and which operating systems they are available for. Naturally, there are also many different implementations of each standard within software that have various other features.

- While PPTP is known to use weaker encryption than either IPSec or SSL/TLS, it may still be useful for bypassing Internet blocking, and the client software is conveniently built into most versions of Microsoft Windows.
- SSL/TLS-based VPN systems are relatively simple to configure, and provide a solid level of security.
- IPSec runs at the Internet level, responsible for packet transfer in the Internet architecture, while the others run at the Application level. This makes IPsec more flexible, as it can be used for protecting all the higher level protocols, but also difficult to set up.

SET UP YOUR OWN VPN SERVICE

As an alternative to paying for commercial VPN services, users with contacts in unrestricted locations may have these contacts download and install software that sets up a private VPN service. This requires a much higher level of technical knowledge, but it will be free. Also the private nature of such a setup means it is less likely to be blocked than a commercial service that has been available for a long time. One of the most widely used free and open source programs available for setting up this kind of private VPN is OpenVPN (http://openvpn.net), which can be installed on Linux, MacOS, Windows and many other operating systems.

To understand how to set up an OpenVPN system, read the "Using OpenVPN" chapter in this manual.

ADVANTAGES

A VPN provides encrypted transfer of your data, so it is one of the safest ways to bypass Internet censorship. Once configured, it is easy and transparent to use.

VPNs are best suited for technically capable users who require secure circumvention services for more than just web traffic and who access the Internet from their own computer where they can install additional software. VPNs are an excellent resource for users in censored locations who do not have trusted contacts in non-filtered locations. VPN technology is a common business application that is not likely to be blocked.

DISADVANTAGES AND RISKS

Some commercial VPNs (especially the free ones) are publicly known and may be filtered. They normally cannot be used in public access locations where users cannot install software, such as Internet cafés or libraries. Use of VPNs may require a higher level of technical expertise than other circumvention methods.

A network operator can detect that a VPN is being used and determine who the VPN provider is. The network operator should not be able to view the communications sent over the VPN unless the VPN is set up incorrectly.

The VPN operator (much like a proxy operator) can see what you're doing unless you use some additional encryption for your communications, like HTTPS for Web traffic; without additional encryption, you have to trust the VPN or tunnel operator not to abuse this access.

21. VPN ON UBUNTU

If you use Ubuntu as your operating system, you can connect to a VPN by using the built-in NetworkManager feature and the free OpenVPN client.

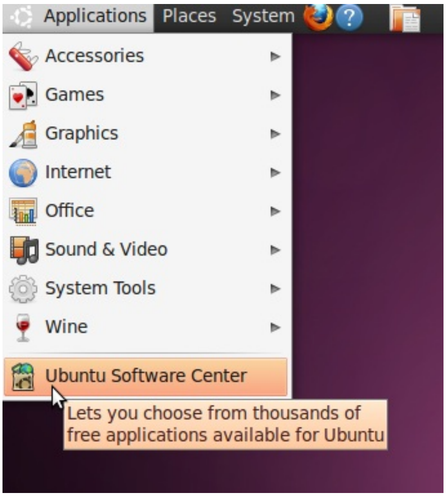
OpenVPN allows you to connect to VPN networks using a variety of authentication methods. For our example, we'll learn how to connect to a VPN server using AirVPN, a free VPN service. The configuration process for OpenVPN on Ubuntu is the same, regardless of which VPN service you use.

Installing OpenVPN for NetworkManager

NetworkManager, a network utility that will let you open or close your VPN connection, is included with Ubuntu by default – you can find it in the notification area of your screen, right next to your system clock.

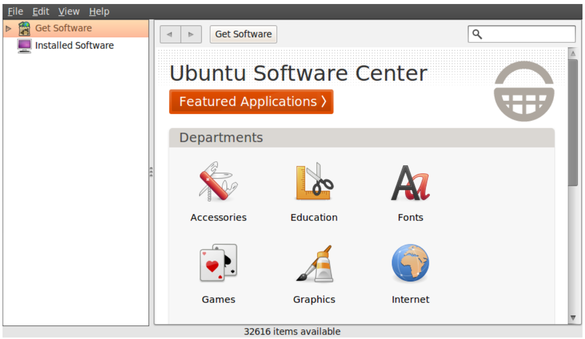
Next, find an OpenVPN extension that will work with NetworkManager, from the Ubuntu Software Center.

1. Open the Ubuntu Software Center from the Applications menu located at the top left of your screen



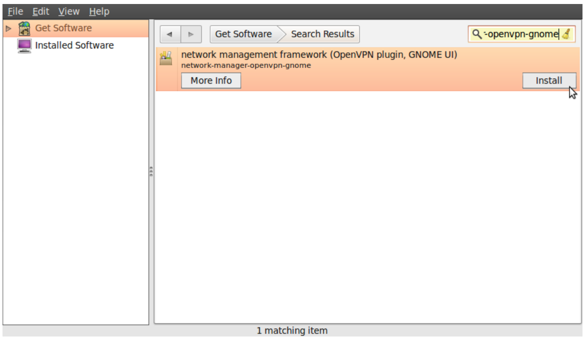
Lets you choose from thousands of free applications available for Ubuntu

2. The Ubuntu Software Center lets you search, install and remove software on your computer. Click on the search box at the top right of the window.



32616 items available

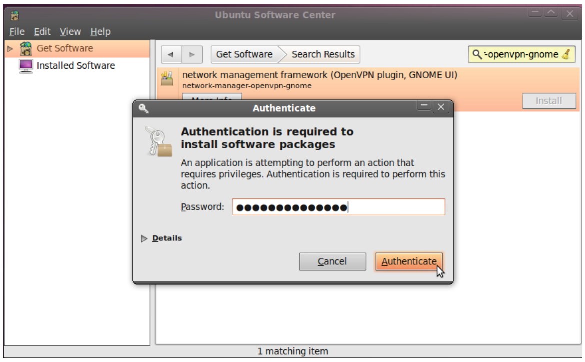
3. In the search box, type in "network-manager-openvpn-gnome" (the extension for NetworkManager that will enable OpenVPN). This package includes all the files you need to establish a VPN connection successfully, including the OpenVPN client. Click on Install.



network management framework (OpenVPN plugin, GNOME UI)
network-manager-openvpn-gnome

1 matching item

4. Ubuntu may ask you for additional permissions to install the program. If that is the case, type in your password and click Authenticate. Once the package is installed, you can close the Software Center window.



network management framework (OpenVPN plugin, GNOME UI)
network-manager-openvpn-gnome

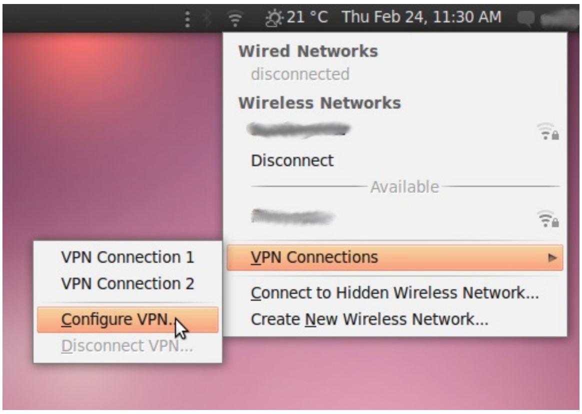
Authenticate

Authentication is required to install software packages

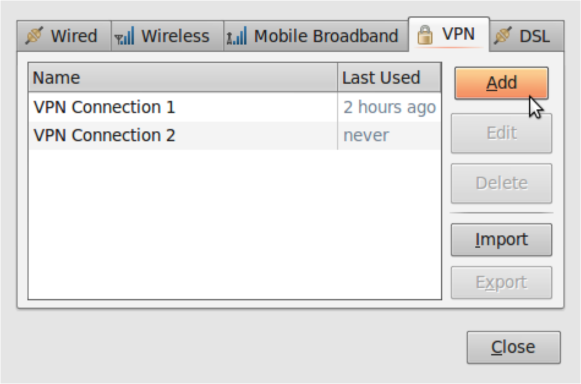
An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password: ●●●●●●●●●●●●●●

5. To check if the OpenVPN client is correctly installed, click on the NetworkManager (the icon at the left of your system clock) and select VPN Connections > Configure VPN.

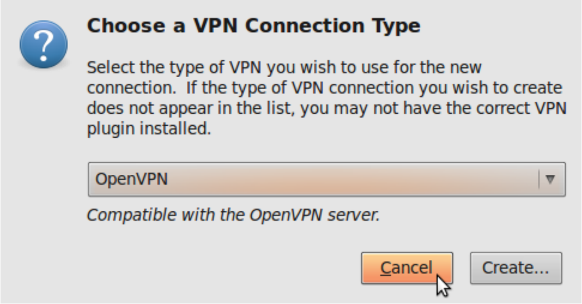


6. Click Add under the VPN tab.



Name	Last Used
VPN Connection 1	2 hours ago
VPN Connection 2	never

7. If you see an OpenVPN option this means that you have installed the OpenVPN client in Ubuntu correctly. Click on cancel and close the NetworkManager.


Choose a VPN Connection Type

Select the type of VPN you wish to use for the new connection. If the type of VPN connection you wish to create does not appear in the list, you may not have the correct VPN plugin installed.

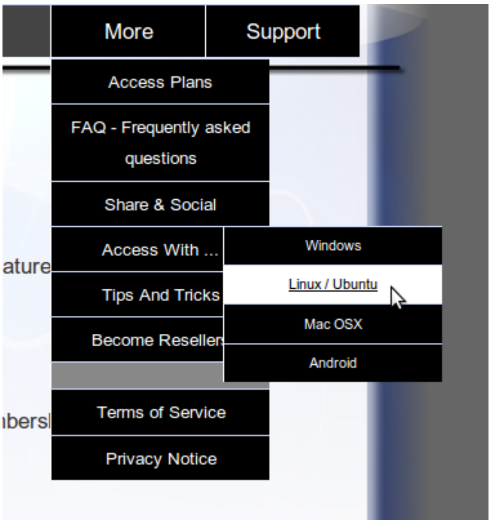
OpenVPN

Compatible with the OpenVPN server.

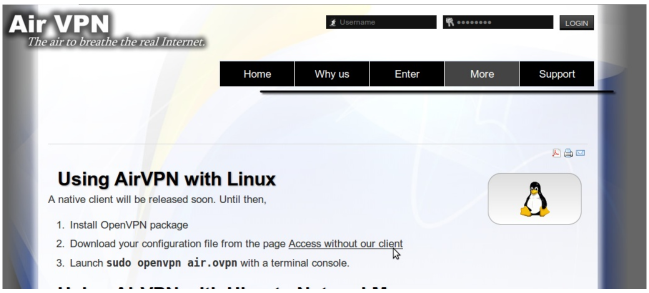
Registering an AirVPN account

AirVPN (http://www.airvpn.org) is a free service, but you will need to register at their Web site to download the configuration files for your VPN connection.

1. Go to https://airvpn.org/?option=com_user&view=register and register for a free account. Make sure you pick a strong password, as this will also be the password for your VPN access. (For tips on strong passwords, see the chapter on "Threats and Threat Assessment" in this book.)
2. On AirVPN's site navigation menu, select More > Access with... > Linux/Ubuntu.



3. Click on "Access without our client". You will be prompted for the same username and password you used when you registered.

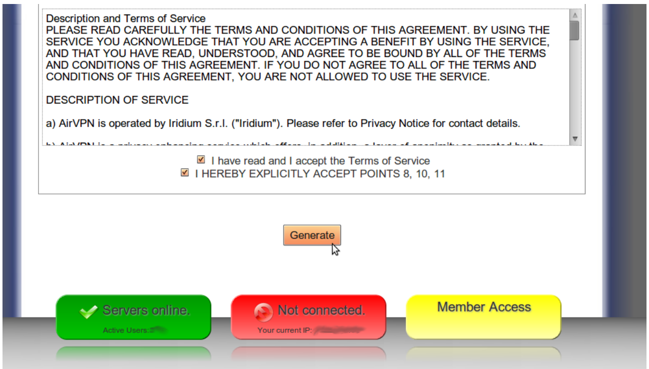


Using AirVPN with Linux

A native client will be released soon. Until then,

1. Install OpenVPN package
2. Download your configuration file from the page Access without our client
3. Launch **sudo openvpn air.ovpn** with a terminal console.

4. Select the VPN Mode you would like to configure in NetworkManager (for our example we used "Free - TCP - 53") and leave the rest of the options as they are. Make sure you have checked the Terms of Service agreement at the bottom of the page, and then click Generate.



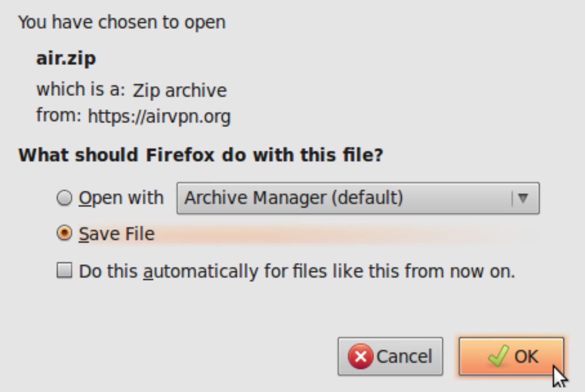
Description and Terms of Service
PLEASE READ CAREFULLY THE TERMS AND CONDITIONS OF THIS AGREEMENT. BY USING THE SERVICE YOU ACKNOWLEDGE THAT YOU ARE ACCEPTING A BENEFIT BY USING THE SERVICE, AND THAT YOU HAVE READ, UNDERSTOOD, AND AGREE TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU ARE NOT ALLOWED TO USE THE SERVICE.

DESCRIPTION OF SERVICE

a) AirVPN is operated by Iridium S.r.l. ("Iridium"). Please refer to Privacy Notice for contact details.

☑ I have read and I accept the Terms of Service
☑ I HEREBY EXPLICITLY ACCEPT POINTS 8, 10, 11

5. A pop-up window will let you know that the file air.zip is ready for downloading. This contains the configuration files and credentials you need to connect to the VPN. Click OK.



You have chosen to open

air.zip

which is a: Zip archive
from: https://airvpn.org

What should Firefox do with this file?

○ Open with Archive Manager (default)

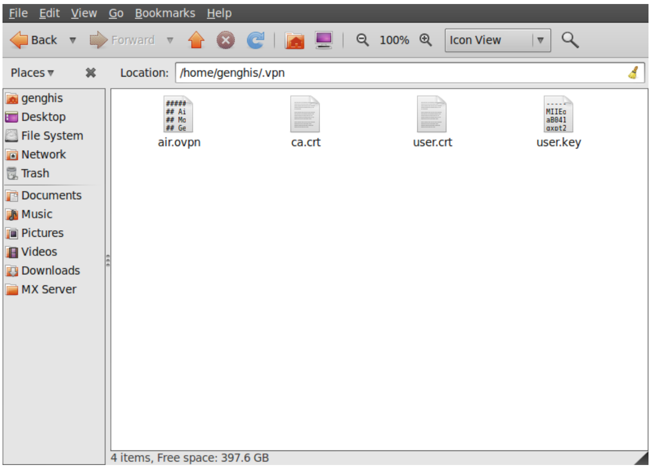
● Save File

□ Do this automatically for files like this from now on.

Configuring AirVPN on NetworkManager

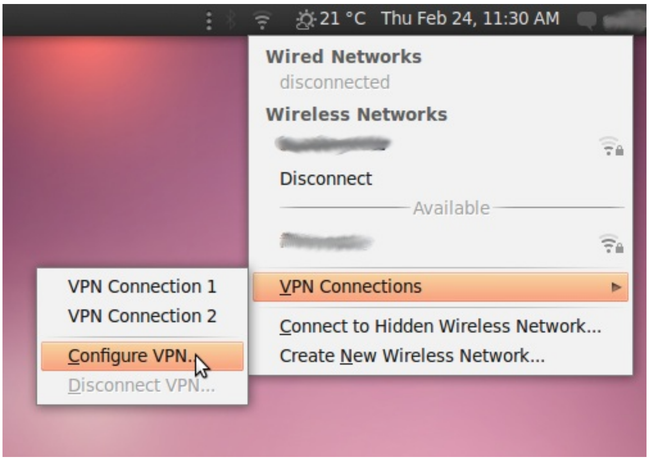
Now that you have your configuration files and credentials, you can configure NetworkManager to connect to the AirVPN service.

1. Unzip the file you have downloaded to a folder on your hard drive (e.g.: "/home/[yourusername]/.vpn"). You should now have four files. The file "air.ovpn" is the configuration file that you need to import into NetworkManager.

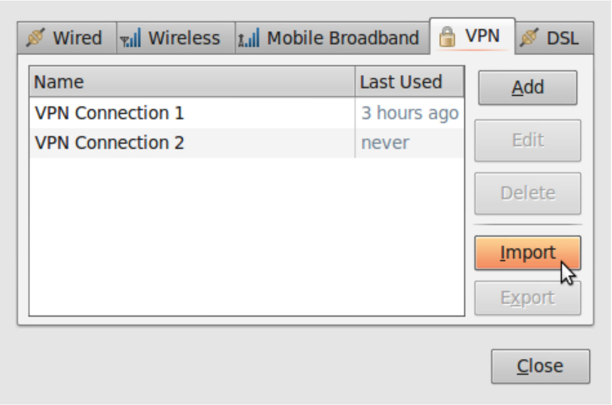


Location: /home/genghis/.vpn

2. To import the configuration file, open NetworkManager and go to VPN Connections > Configure VPN.

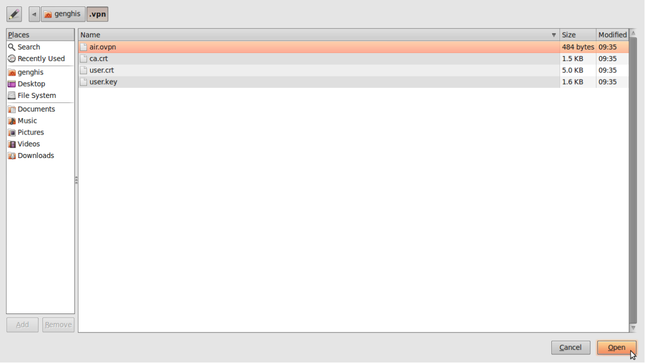


3. Under the VPN tab, click Import.



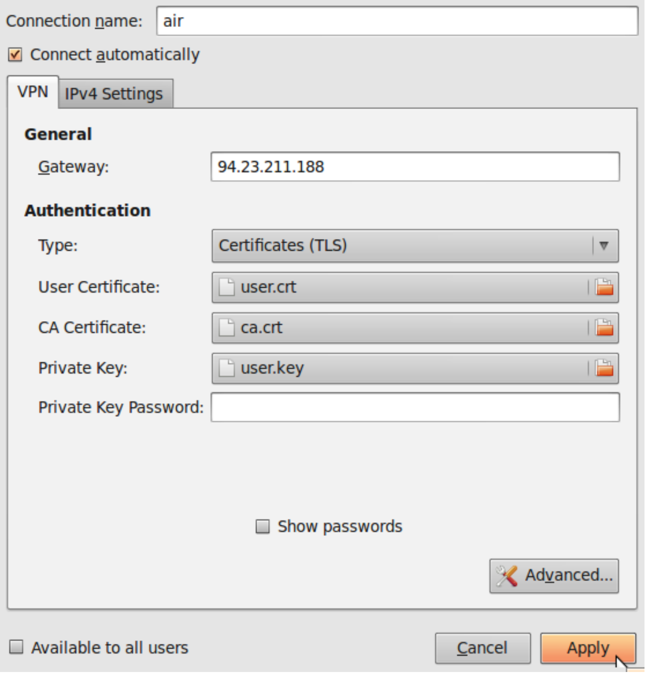
Name	Last Used
VPN Connection 1	3 hours ago
VPN Connection 2	never

4. Locate the file air.ovpn that you have just unzipped. Click Open.



Name	Size	Modified
air.ovpn	484 bytes	09:35
ca.crt	1.5 KB	09:35
user.crt	5.0 KB	09:35
user.key	1.6 KB	09:35

5. A new window will open. Leave everything as it is and click Apply.



Connection name: air

☑ Connect automatically

General

Gateway: 94.23.211.188

Authentication

Type: Certificates (TLS)

User Certificate: user.crt

CA Certificate: ca.crt

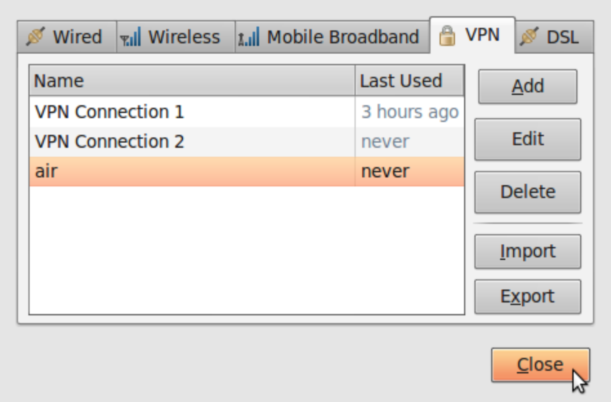
Private Key: user.key

Private Key Password:

☐ Show passwords

☐ Available to all users

6. Congratulations! Your VPN connection is ready to be used and should appear on the list of connections under the VPN tab. You can now close NetworkManager.

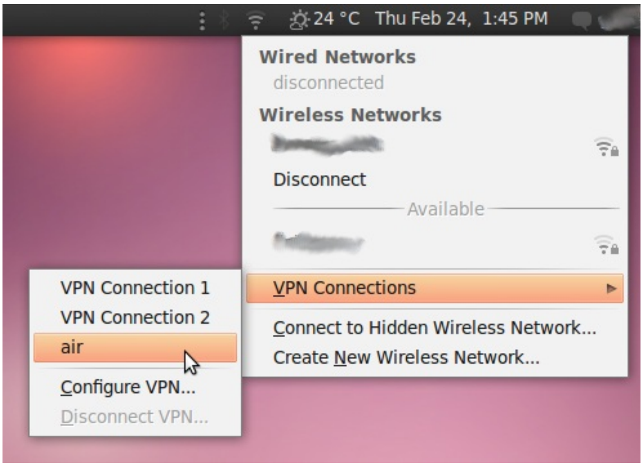


Name	Last Used
VPN Connection 1	3 hours ago
VPN Connection 2	never
air	never

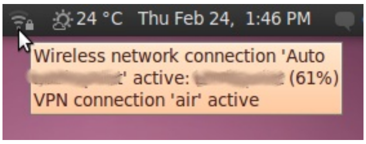
Using your new VPN connection

Now that you configured NetworkManager to connect to a VPN service using the OpenVPN client, you can use your new VPN connection to circumvent Internet censorship. To get started, follow these steps:

1. In the NetworkManager menu, select your new connection from VPN Connections.

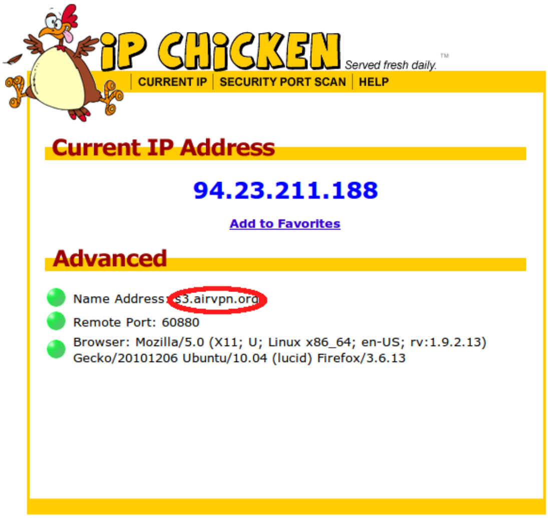


2. Wait for the VPN connection to be established. When connected, a small padlock should appear right next to your NetworkManager icon, indicating that you are now using a secure connection. Move your cursor over the icon to confirm that the VPN connection is active.



Wireless network connection 'Auto [redacted]' active: [redacted] (61%)
VPN connection 'air' active

3. You can also check the status of your connection by visiting http://www.ipchicken.com. This free IP-checker should confirm that you are using a airvpn.org server.



Current IP Address

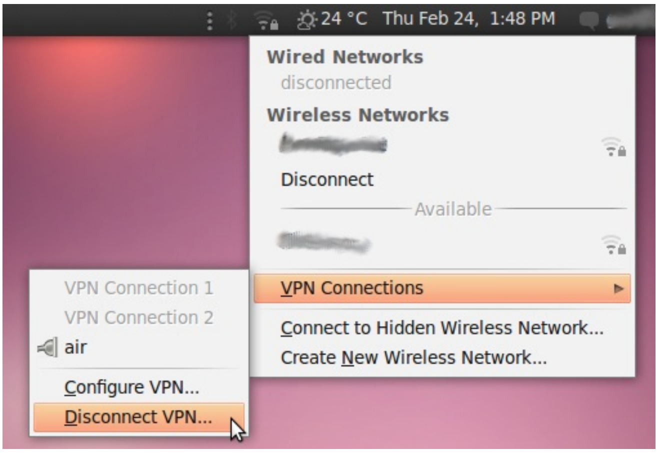
94.23.211.188

Add to Favorites

Advanced

- Name Address: s3.airvpn.org
- Remote Port: 60880
- Browser: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.13) Gecko/20101206 Ubuntu/10.04 (lucid) Firefox/3.6.13

4. To disconnect from your VPN, select VPN Connections > Disconnect VPN in the NetworkManager menu. You are now using your normal (filtered) connection again.


24 °C Thu Feb 24, 1:48 PM
[redacted]
Wired Networks
disconnected
Wireless Networks
[redacted]
Disconnect
Available
[redacted]
VPN Connections
Connect to Hidden Wireless Network...
Create New Wireless Network...
VPN Connection 1
VPN Connection 2
air
Configure VPN...
Disconnect VPN...

22. HOTSPOT SHIELD

Hotspot Shield is a free (but commercial) VPN solution available for Microsoft Windows and Mac OS, which can be used to access the uncensored Internet through a secure tunnel (over your normal, censored Internet connection).

Hotspot Shield encrypts all your communications, so your censor's surveillance software can't see what sites you're accessing.

GENERAL INFORMATION

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

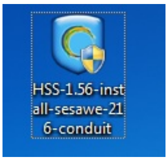
HOW TO GET HOTSPOT SHIELD

Download the software from https://www.hotspotshield.com. The file size is about 6MB, so on a slow dial-up connection this can take up to 25 minutes or more. If the download is blocked from where you are trying to access it, write to hss-sesawe@anchorfree.com and include at least one of these words in the subject line of your e-mail: "hss", "sesawe", "hotspot" or "shield". You will receive the installer as an e-mail attachment in your inbox.

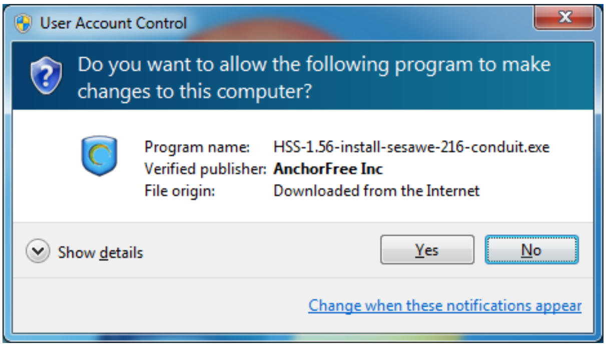
Important: if you are using Firefox with the NoScript extension enabled, you may experience some issues when trying to use Hotspot Shield. Make sure that all URLs that Hotspot Shield connects to are whitelisted, or that you temporarily allow scripts globally while using this service.

Installing Hotspot Shield

1. After a successful download, locate the downloaded file on your computer and start the installation by double clicking the icon



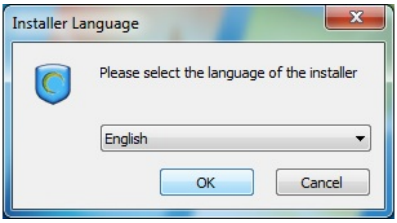
2. Windows may ask you for permission to install the software. Click Yes.


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: HSS-1.56-install-sesawe-216-conduit.exe
Verified publisher: **AnchorFree Inc**
File origin: Downloaded from the Internet

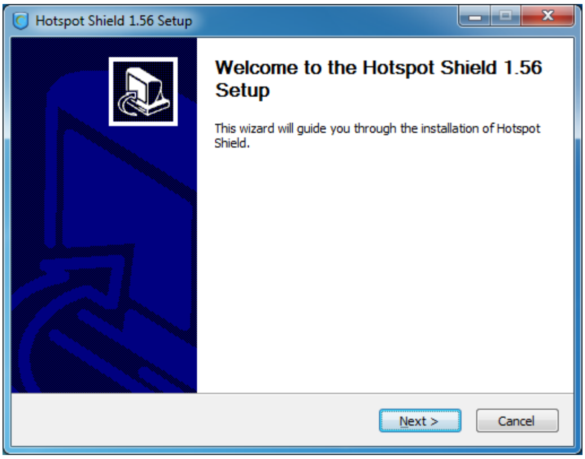
3. Select your preferred installation language from the dropdown menu.


Installer Language

Please select the language of the installer

English

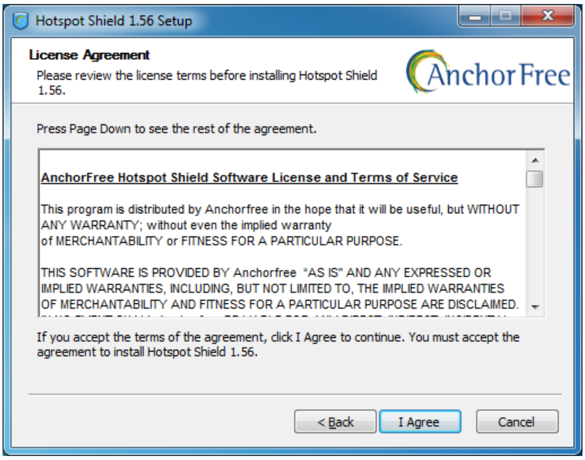
4. After you select the language, you will see a welcome screen. Click Next.


Hotspot Shield 1.56 Setup

Welcome to the Hotspot Shield 1.56 Setup

This wizard will guide you through the installation of Hotspot Shield.

5. Accept the license agreement by clicking on "I Agree".



License Agreement

Please review the license terms before installing Hotspot Shield 1.56.

Press Page Down to see the rest of the agreement.

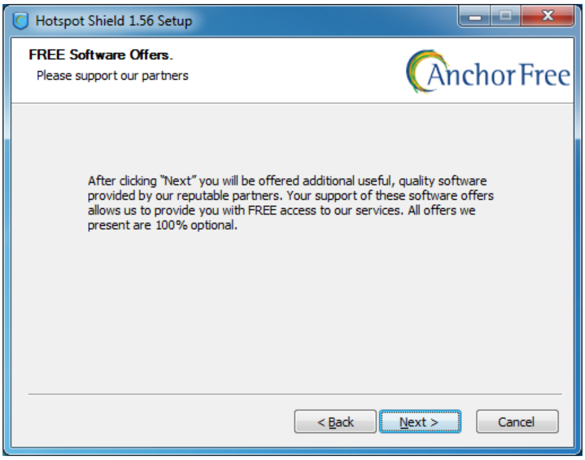
AnchorFree Hotspot Shield Software License and Terms of Service

This program is distributed by Anchorfree in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

THIS SOFTWARE IS PROVIDED BY Anchorfree "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Hotspot Shield 1.56.

6. You will see a window informing you about additional software which can be installed optionally. Click Next.

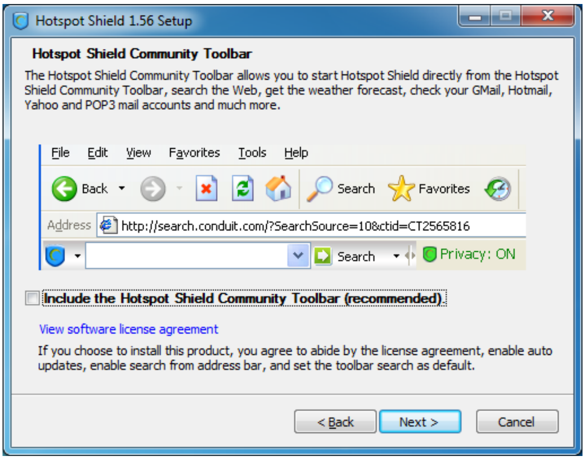


FREE Software Offers.

Please support our partners

After clicking "Next" you will be offered additional useful, quality software provided by our reputable partners. Your support of these software offers allows us to provide you with FREE access to our services. All offers we present are 100% optional.

7. On the next screen you can uncheck the option to install the optional Hotspot Shield Community Toolbar. This feature is not needed to run Hotspot Shield.



Hotspot Shield Community Toolbar

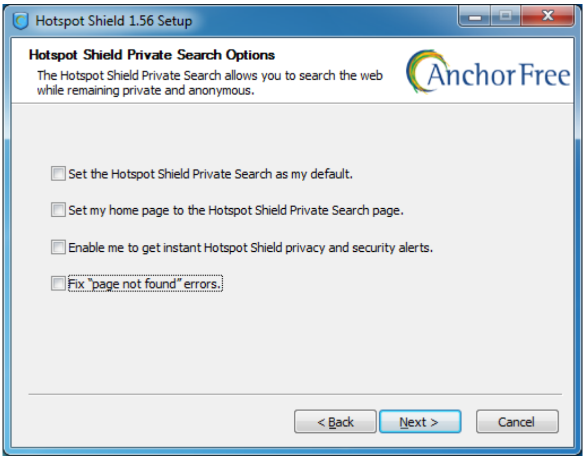
The Hotspot Shield Community Toolbar allows you to start Hotspot Shield directly from the Hotspot Shield Community Toolbar, search the Web, get the weather forecast, check your GMail, Hotmail, Yahoo and POP3 mail accounts and much more.

Address: http://search.conduit.com/?SearchSource=10&ctid=CT2565816

☐ **Include the Hotspot Shield Community Toolbar (recommended)**

If you choose to install this product, you agree to abide by the license agreement, enable auto updates, enable search from address bar, and set the toolbar search as default.

8. Additional options will be presented at the next screen. All these features are optional, and you don't need any of them enabled to run Hotspot Shield.



Hotspot Shield 1.56 Setup

Hotspot Shield Private Search Options

The Hotspot Shield Private Search allows you to search the web while remaining private and anonymous.

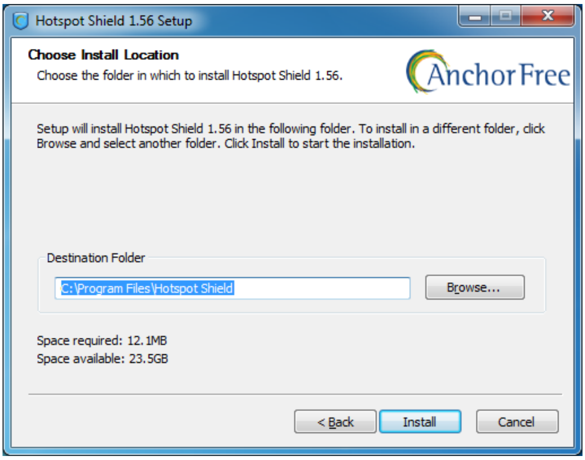
□ Set the Hotspot Shield Private Search as my default.

□ Set my home page to the Hotspot Shield Private Search page.

□ Enable me to get instant Hotspot Shield privacy and security alerts.

□ Fix "page not found" errors.

9. Select the location on your hard drive where you want Hotspot Shield to be installed. In most cases you can leave the default values and proceed by clicking Install.



Hotspot Shield 1.56 Setup

Choose Install Location

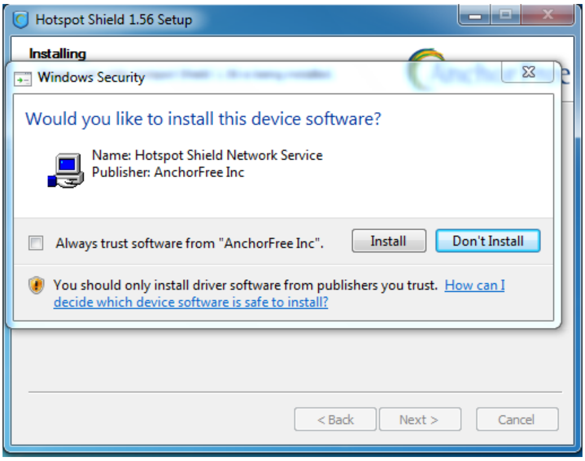
Choose the folder in which to install Hotspot Shield 1.56.

Setup will install Hotspot Shield 1.56 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\Hotspot Shield

Space required: 12.1MB
Space available: 23.5GB

10. Windows may request additional permissions several times to install different components of Hotspot Shield. You can safely proceed by clicking Install every time.



Hotspot Shield 1.56 Setup

Installing

Windows Security

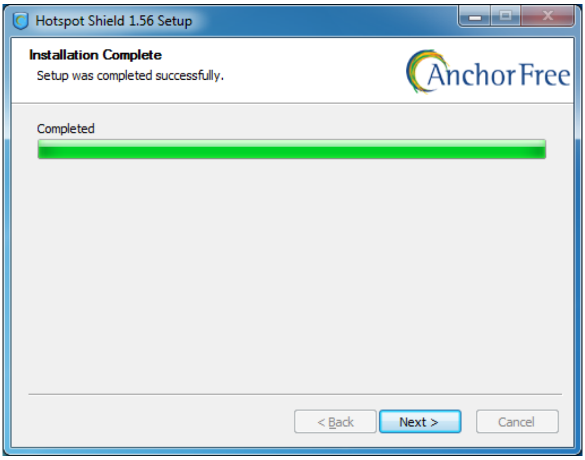
Would you like to install this device software?

Name: Hotspot Shield Network Service
Publisher: AnchorFree Inc

□ Always trust software from "AnchorFree Inc".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

11. When the installation is completed, click Next.

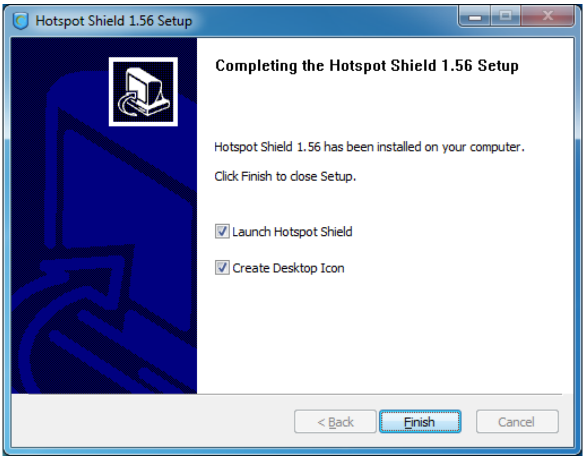


Installation Complete

Setup was completed successfully.

Completed

12. Finally, you can launch Hotspot Shield immediately after installation and you can create an icon for your desktop. Choose your preferences and click Finish.



Completing the Hotspot Shield 1.56 Setup

Hotspot Shield 1.56 has been installed on your computer.

Click Finish to close Setup.

☑ Launch Hotspot Shield

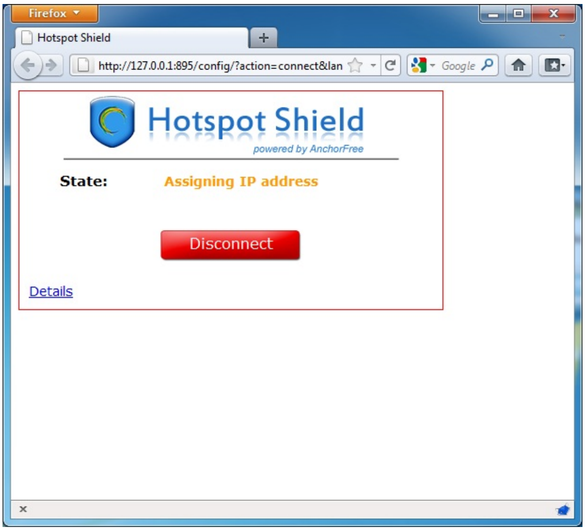
☑ Create Desktop Icon

Hotspot Shield is now installed on your computer.

Connecting to the Hotspot Shield service

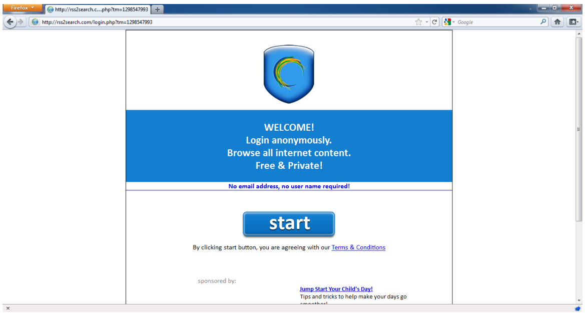
1. Click on the Hotspot Shield Launch icon on your desktop or from the menu Programs > Hotspot Shield.

2. Once you launch Hotspot Shield, a browser window will open with a status page showing different stages of the connection attempt, such as "Authenticating" and "Assigning IP address".



State: Assigning IP address

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


Firefox
http://rss2search.c....php?tm=1298547993
http://rss2search.com/login.php?tm=1298547993
Google

WELCOME!
Login anonymously.
Browse all internet content.
Free & Private!

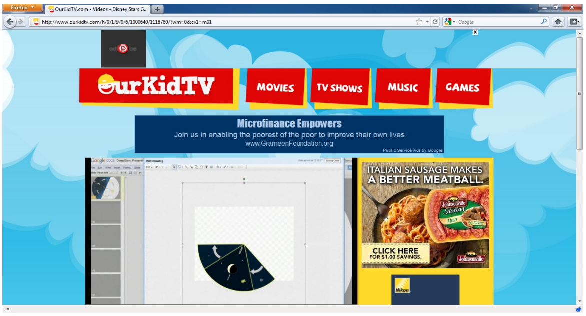
No email address, no user name required!

By clicking start button, you are agreeing with our Terms & Conditions

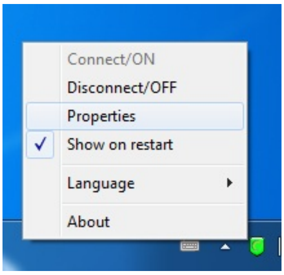
sponsored by:

Jump Start Your Child's Day!
Tips and tricks to help make your days go

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).

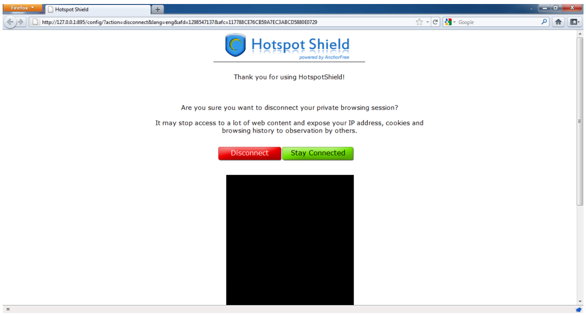

Firefox
OurKidTV.com - Videos - Disney Stars G...
http://www.ourkidtv.com/h/0/1/9/0/6/1000640/1118780/?wm=0&cv1=m01
Google
OurKidTV
MOVIES
TV SHOWS
MUSIC
GAMES
Microfinance Empowers
Join us in enabling the poorest of the poor to improve their own lives
www.GrameenFoundation.org
Public Service Ads by Google
ITALIAN SAUSAGE MAKES A BETTER MEATBALL.
CLICK HERE FOR $1.00 SAVINGS.
Johnsonville
Nikon

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



Disconnecting from the Hotspot Shield service

1. To disconnect from the Hotspot Shield service right click on the system tray icon (see image above) and select Disconnect/OFF.
2. Hotspot Shield will ask you to confirm this action. Click Disconnect.



http://127.0.0.1:895/config/?action=disconnect&lang=eng&afd=1298547137&afc=117788CE76CB59A7EC3ABCD5880E0729

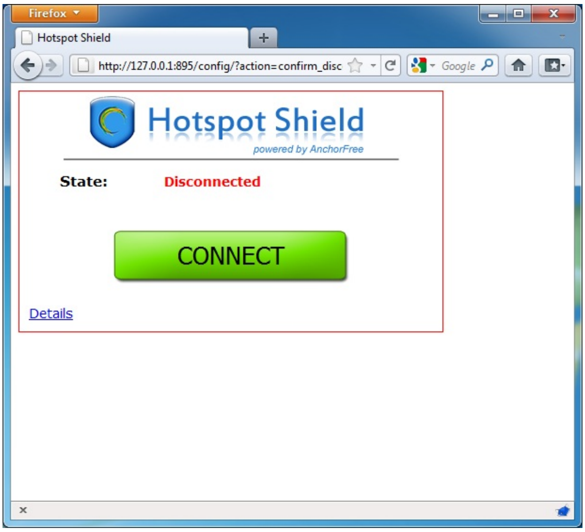
Thank you for using HotspotShield!

Are you sure you want to disconnect your private browsing session?

It may stop access to a lot of web content and expose your IP address, cookies and browsing history to observation by others.

[redacted]

3. A status window will appear confirming you are now disconnected and surfing on your normal (filtered) connection. Click on the "CONNECT" button to resume circumvention.



http://127.0.0.1:895/config/?action=confirm_disc

State: Disconnected

23. ALKASIR

Alkasir is an innovative server/client tool facilitating the tracking, analysis, and circumvention of Web site censorship (filtering). Alkasir is mainly used in the Middle East region but can be used globally.

It utilizes a dedicated client software and is powered by proxy servers. Its innovative feature is to keep the list of blocked sites up-to-date by getting semi-automatic updates, and allows reporting of newly blocked sites through its globally-distributed user community.

GENERAL INFORMATION

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

HOW DOES ALKASIR WORK?

Alkasir has implemented two innovative and complementary new features. It is designed as a Web browser (based on Mozilla Firefox) with an embedded pre-configured HTTP proxy, and a self-learning blocked URLs database.

Bypassing Internet censorship

The innovation is that Alkasir only relies on its blocked URLs database and built-in proxy to reach blocked URLs. Non-blocked URLs are accessed directly, without proxy requests. Using HTTP proxy only when it is really needed optimizes bandwidth usage and allows non-blocked Web pages to be accessed more quickly (since directly-accessed Web pages load quicker).

Keeping the blocked URLs database up-to-date

Any time a user suspects that a URL is blocked, he can report it via the software interface. Alkasir checks the report thoroughly, then asks that country's moderator (a human person) to approve that addition to the database (to keep the database relevant and to prevent undesirable content, such as porn, from entering it).

A single "blocked content unit" (a Web site that is blocked in a certain country) is often dependent on more than one URL. When Alkasir detects a blocked URL in a certain country, it checks all the URLs referenced on that page to determine whether any of them are also blocked. Thus, Alkasir builds its blocked content database through a simple, primitive, one-level spidering methodology.

Finally, if an Alkasir user fails to load an URL with a direct request (i.e. not through the proxy), the client notes this and automatically checks to see whether it is a new (not yet in the database) blocked URL or not, and if it is, adds it automatically.

The database is available at the following address: https://alkasir.com/map.

To summarise, Alkasir's blocked URLs database is continuously fed by all Alkasir users (using human submissions or automatic reports) and the Alkasir browser relies on this database to optimize the global tool's reactivity by redirecting only blocked URLs requests through the proxy.

HOW DO I GET ALKASIR?

You can download Alkasir directly from the website or receive it by e-mail.

Download Alkasir via the website

You can download Alkasir from the official website, https://alkasir.com.

Depending on the operating system and programs you have, you will choose one of the following versions:

- If you have Windows Vista or Windows 7 and have Mozilla Firefox installed, you only need the "Alkasir Installation package" (which requires installation, size: 3 MB).
- If this is not the case, you need to download the "Alkasir Complete Installation package" (which also requires installation, size: 41.04 MB)

If you are not able or do not want to install Alkasir permanently on the computer you are using (e.g. a shared computer in an Internet café or library), you can download any of the two USB versions of Alkasir:

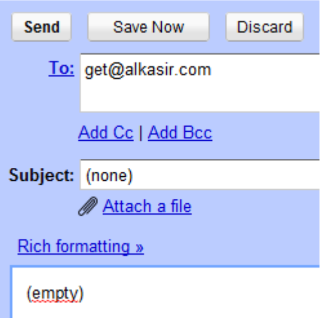
- Alkasir USB package without Mozilla (does not need installation – portable – but needs Mozilla Firefox; size: 4MB)
- Alkasir USB package with Mozilla browser (does not need installation – portable; size: 12MB)

Please note that both versions require the .Net Framework to be installed, which is pre-installed on all Windows Vista and Windows 7 operating systems.

Optionally, you can register an account to receive regular updates and news from Alkasir by e-mail. Updates are released on a regular basis, so you should be sure to get the latest version from the official website.

Receive Alkasir by e-mail

If the Alkasir website blocked in your country, you can get the installation file from an e-mail autoresponder. Simply send a blank email to the address get@alkasir.com to request the installation file as an attachment.



To: get@alkasir.com

Subject: (none)

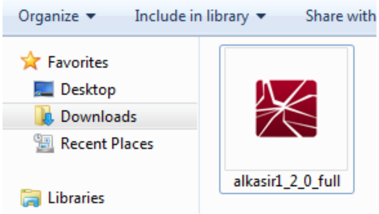
(empty)

You will receive an e-mail with the software attached and instructions on how to install Alkasir on your computer.

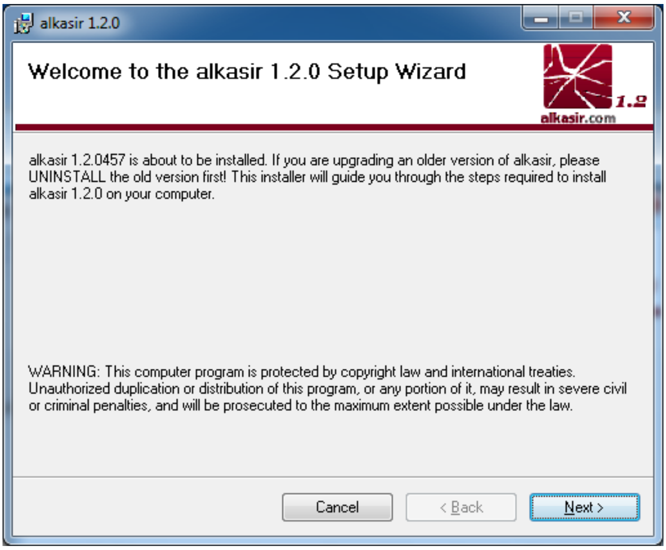
If you don't receive the software after a few minutes, you may need to add get@alkasir.com to your contacts whitelist so the e-mail is not considered as spam.

INSTALLATION

Once you have downloaded the installation file, double-click on the software icon.



You may get a security warning. Click Run or Accept.

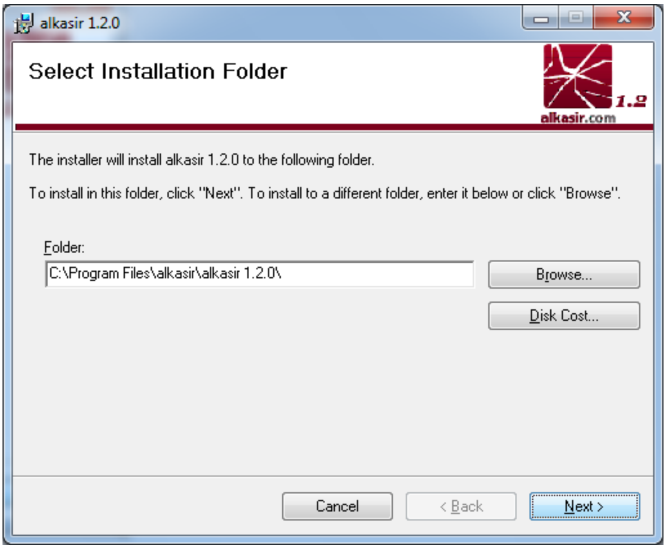


Welcome to the alkasir 1.2.0 Setup Wizard

alkasir 1.2.0457 is about to be installed. If you are upgrading an older version of alkasir, please UNINSTALL the old version first! This installer will guide you through the steps required to install alkasir 1.2.0 on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Follow the Alkasir installation wizard by clicking the Next button.



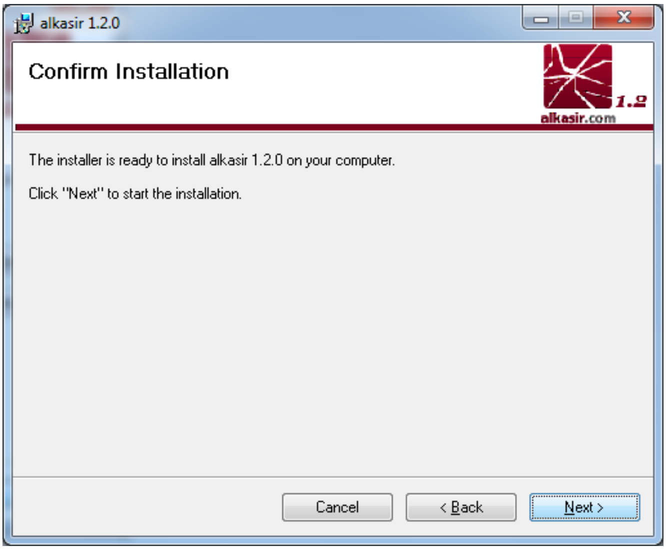
Select Installation Folder

The installer will install alkasir 1.2.0 to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\alkasir\alkasir 1.2.0\

You can change the installation folder (but this is not recommended).

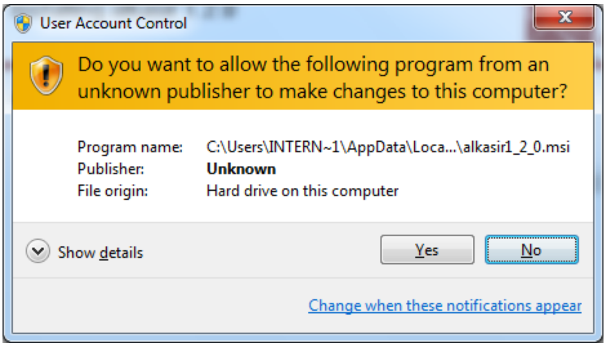


Confirm Installation

The installer is ready to install alkasir 1.2.0 on your computer.

Click "Next" to start the installation.

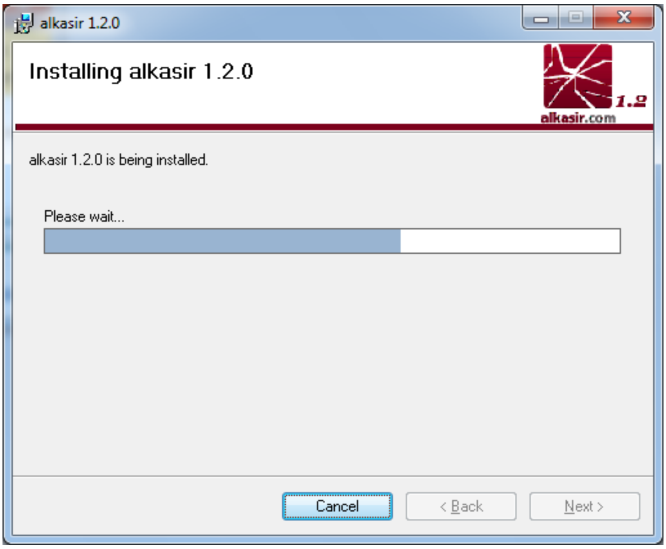
When ready, click Next.



Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: C:\Users\INTERN~1\AppData\Loca...\alkasir1_2_0.msi
Publisher: **Unknown**
File origin: Hard drive on this computer

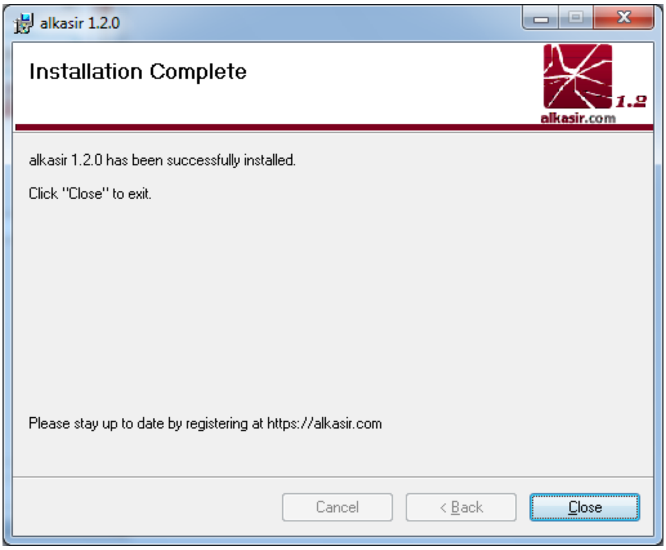
Validate the security warning shown above by clicking Yes.



Installing alkasir 1.2.0

alkasir 1.2.0 is being installed.

Please wait...



alkasir 1.2.0 has been successfully installed.

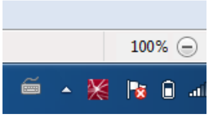
Click "Close" to exit.

Please stay up to date by registering at https://alkasir.com

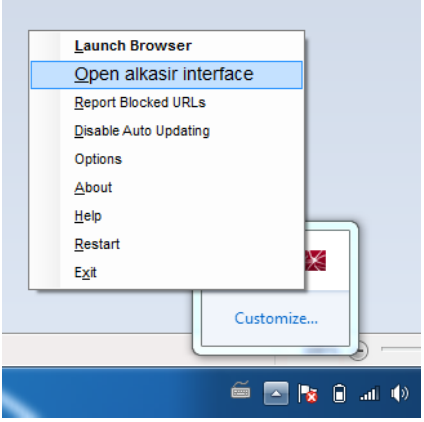
When the installation is finished, click Close.

HOW DO I USE ALKASIR?

Alkasir should start by default whenever Windows is started. Ensure that the software is running by checking that the Alkasir icon is displayed in your system task bar, near the clock.



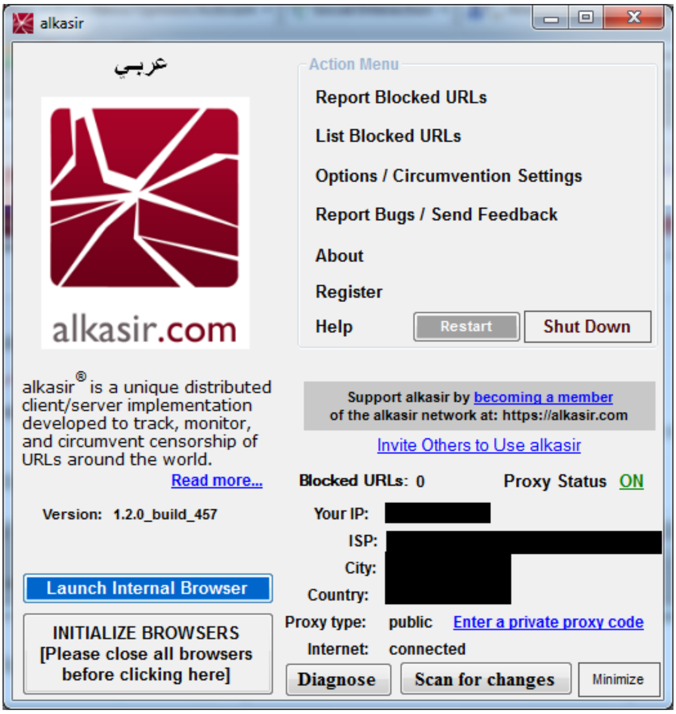
Right clicking the icon reveals the configuration menu.



- Launch Browser
- Open Alkasir interface
- Report blocked URLs

The main Alkasir interface gathers all the features from the software. You can do the following:

- start, shut down and restart the software
- launch the Alkasir browser
- register or login on https://alkasir.com
- get updates for your installed version of Alkasir.



alkasir® is a unique distributed client/server implementation developed to track, monitor, and circumvent censorship of URLs around the world.

Version: 1.2.0_build_457

Support alkasir by becoming a member of the alkasir network at: https://alkasir.com

Blocked URLs: 0 Proxy Status ON

Your IP: [redacted]

ISP: [redacted]

City: [redacted]

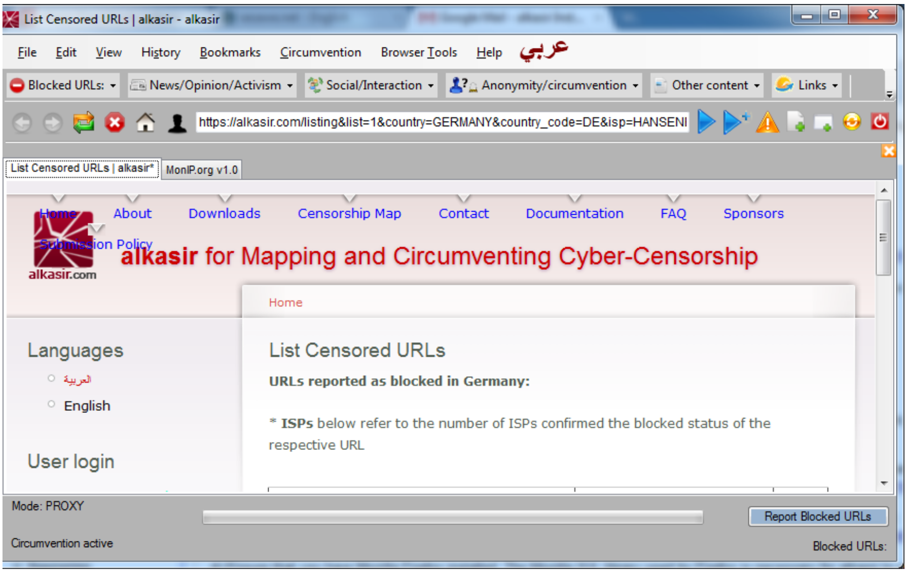
Country: [redacted]

Proxy type: public

Internet: connected

INITIALIZE BROWSERS [Please close all browsers before clicking here]

First, let's launch the Alkasir browser.


List Censored URLs | alkasir - alkasir
File Edit View History Bookmarks Circumvention Browser Tools Help عربي
Blocked URLs: News/Opinion/Activism Social/Interaction Anonymity/circumvention Other content Links
List Censored URLs | alkasir*
MonIP.org v1.0
Home About Downloads Censorship Map Contact Documentation FAQ Sponsors
Submission Policy
alkasir.com
Languages
العربية
English
User login
Report Blocked URLs

https://alkasir.com/listing&list=1&country=GERMANY&country_code=DE&isp=HANSENI

alkasir for Mapping and Circumventing Cyber-Censorship

Home

List Censored URLs

URLs reported as blocked in Germany:

* ISPs below refer to the number of ISPs confirmed the blocked status of the respective URL

Mode: PROXY

Circumvention active

Blocked URLs:

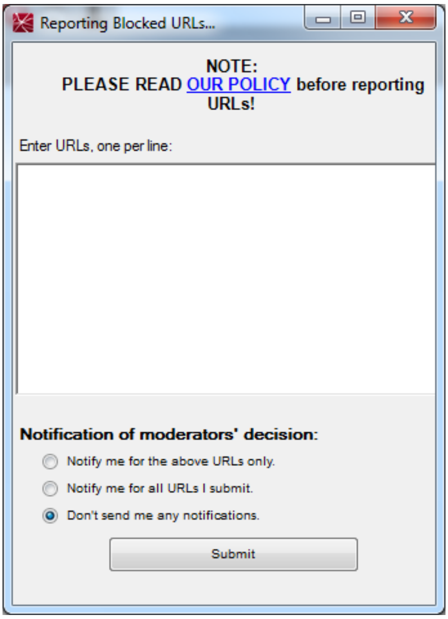
The browser's graphical user interface is very similar to Mozilla Firefox as it is based on the same technical framework. Note some specific features:

- a button for complete Arabic localization
- the "Report Blocked URLs" button, to use when you are trying to reach a website that appears to be blocked. This button is displayed near the address bar and the status bar.
- an Alkasir icon to go to the main interface.

You can also find other menus to integrate your Alkasir browser with your Alkasir account.

It is possible to enable or disable the automatic updates for the software, the proxy list and blocked sites database.

If you are arrive at an error page that could indicate a blocked website (such as an Access Denied or Connection Timeout error), you can submit this URL to the Alkasir database by clicking the Report Blocked URL button. You can choose to be notified of the moderator's decision about whether to enter this URL into the database or not (this decision is based on the tool's policy).



Reporting Blocked URLs...

NOTE:
PLEASE READ OUR POLICY before reporting URLs!

Enter URLs, one per line:

Notification of moderators' decision:

○ Notify me for the above URLs only.
○ Notify me for all URLs I submit.
● Don't send me any notifications.

FURTHER INFORMATION

Visit https://alkasir.com for:

- a comprehensive documentation for the software: https://alkasir.com/help
- a list of Frequently Asked Questions: https://alkasir.com/faq

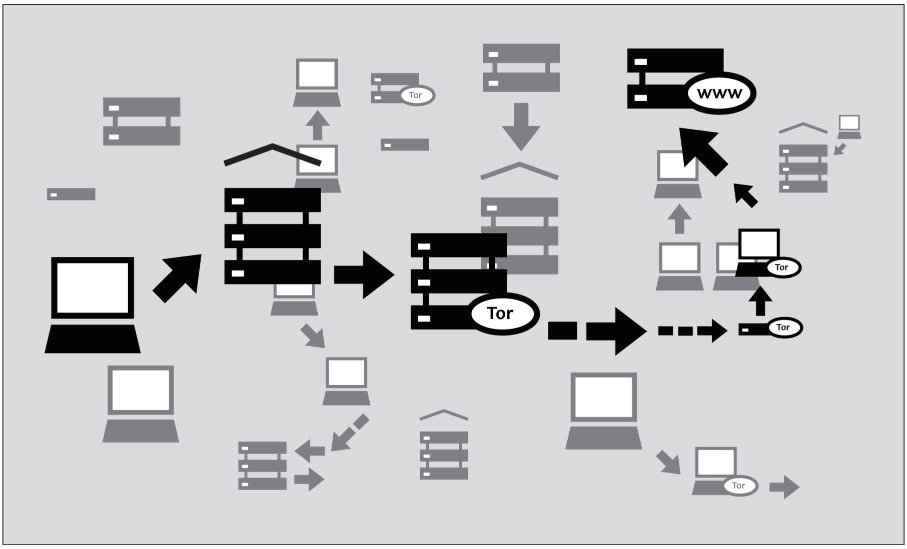
24. TOR : THE ONION ROUTER

Tor (The Onion Router) is a very sophisticated network of proxy servers.

GENERAL INFORMATION

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

When you use Tor to access a Web site, your communications are randomly routed through a network of independent, volunteer proxies. All the traffic between Tor servers (or relays) is encrypted, and each of the relays knows only the IP address of two other machines – the one immediately previous to it and the one immediately after it in the chain.



The goal of this is *unlinkability*. Tor makes it very difficult for:

- your ISP or any other local observer to know what your target Web site is or what information you are sending
- the target Web site to know who you are (at least, to know your IP address)
- any of the independent relays to know who you are and where you go either by directly having your IP address or by being able to correlate browsing habits by consistently observing your traffic.

WHAT DO I NEED TO USE THE TOR NETWORK?

To connect to the Internet through the Tor network and use it for **anonymity, privacy,** and **circumvention**, you need to install the Tor client software on your computer. It is also possible to run a portable version of the program from a USB flash drive or other external device.

Tor is compatible with most versions of Windows, Mac OS X, and GNU/Linux.

WITH WHAT SOFTWARE IS TOR COMPATIBLE?

Tor uses a SOCKS proxy interface to connect to applications, so any application that supports SOCKS (versions 4, 4a and 5) can have its traffic anonymized with Tor, including:

- most Web browsers
- many instant messaging and IRC clients
- SSH clients
- e-mail clients.

If you installed Tor from the Vidalia Bundle, Tor Browser Bundle or Tor IM Browser Bundle, Tor will have also configured an HTTP application proxy as a front-end to the Tor network. This will allow some applications that do not support SOCKS to work with Tor.

If you are mostly interested in using Tor for Web surfing and chatting, you may find it easiest to use the Tor Browser Bundle or the Tor IM Browser Bundle which will provide you with ready-to-use pre-configured solutions. The Tor Browser Bundle also includes Torbutton, which improves privacy protection when using Tor with a Web browser. Both versions of Tor can be downloaded at https://www.torproject.org/projects/torbrowser.

ADVANTAGES AND RISKS

Tor can be a very effective tool for circumvention and protecting your identity. Tor's encryption hides the contents of your communications from your local network operator, and conceals whom you are communicating with or what Web sites you're viewing. When used properly, it provides significantly stronger anonymity protection than a single proxy.

But:

- Tor is vulnerable to blocking. Most Tor nodes are listed in a public directory, so it is easy for network operators to access the list and add the IP addresses of **nodes** to a filter. (One way of attempting to get around this kind of blocking is to use one of several **Tor bridges**, which are Tor entry nodes not publicly listed, specifically to avoid blocking.)
- Some programs you might use with Tor have problems that can compromise anonymity. The Tor Browser Bundle comes with a version of Firefox with Torbutton installed. Torbutton disables some plugins and changes your browser fingerprint so it looks like any other Torbutton user. Tor will not protect you if you do not configure your appplications to run through Tor. Some plugins and scripts ignore local proxy settings and can reveal your IP address.
- If you're not using additional encryption to protect your communications, your data will be unencrypted once it reaches the last Tor node in the chain (called an **exit node**). This means that your data will be potentially visible to the owner of the last Tor node and to the ISP between that node and your destination Web site.

The developers of Tor have thought a lot about these and other risks and offer three warnings:

1. Tor does not protect you if you do not *use it correctly*. Read the list of warnings here: https://www.torproject.org/download/download.html.en#warning and then make sure to follow the instructions for your platform carefully: https://www.torproject.org/documentation.html.en#RunningTor
2. Even if you configure and use Tor correctly, there are still *potential attacks* that could compromise Tor's ability to protect you: https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#Whatattacksremainagainstonionrouting
3. *No anonymity system is perfect* these days, and Tor is no exception: you should not rely solely on the current Tor network if you really need strong anonymity.

USING TOR BROWSER BUNDLE

The Tor Browser Bundle lets you use Tor on Windows, OS X, or GNU/Linux without requiring you to configure a Web browser. Even better, it's also a portable application that can be run from a USB flash drive, allowing you to carry it to any computer without installing it on each computer's hard drive.

DOWNLOADING TOR BROWSER BUNDLE

You can download the Tor Browser Bundle from the torproject.org Web site, either as a single file or a "split" version that is multiple files. If your Internet connection is slow and unreliable, the split version may work better than trying to download one very large file.

If the torproject.org Web site is filtered from where you are, type "tor mirrors" in your favorite Web search engine; the results will probably include some alternative addresses to download the Tor Browser Bundle.

Get Tor through e-mail: send an e-mail to gettor@torproject.org with "help" in the message body, and you will receive instructions on how to have the autoresponder bot send you the Tor software.

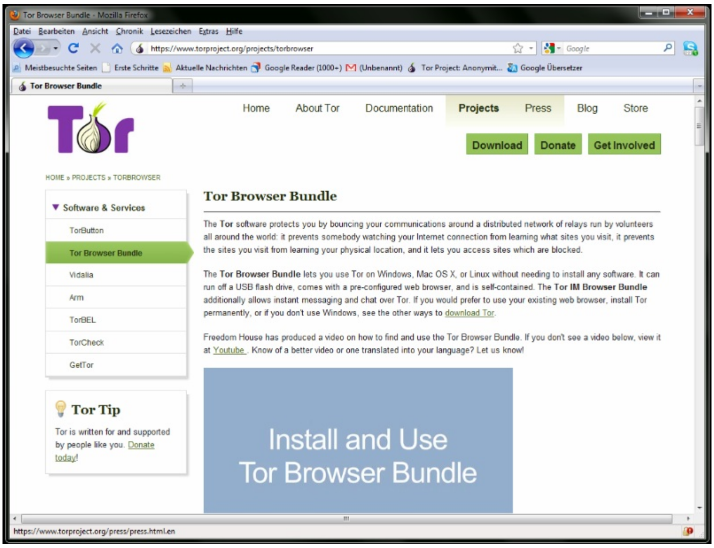
Caution: When you download the Tor Browser Bundle (plain or split versions), you should check the signatures of the files, especially if you are downloading the files from a mirror site. This step ensures that the files have not been tampered with. To learn more about signature files and how to check them, read https://www.torproject.org/docs/verifying-signatures.

You can download the GnuPG software that you will need to check the signature here: http://www.gnupg.org/download/index.en.html#auto-ref-2.

The instructions below refer to installing Tor Browser on Microsoft Windows. If you are using a different operating system, refer to the Tor Web site for download links and instructions.

Installing from a single file

1. In your Web browser, enter the download URL for Tor Browser: https://www.torproject.org/projects/torbrowser


Tor Browser Bundle - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://www.torproject.org/projects/torbrowser
Meistbesuchte Seiten Erste Schritte Aktuelle Nachrichten Google Reader (1000+) (Unbenannt) Tor Project: Anonymit... Google Übersetzer
Tor Browser Bundle
Home About Tor Documentation Projects Press Blog Store
Download Donate Get Involved
HOME » PROJECTS » TORBROWSER
Software & Services
TorButton
Tor Browser Bundle
Vidalia
Arm
TorBEL
TorCheck
GetTor
Install and Use
Tor Browser Bundle
https://www.torproject.org/press/press.html.en

Tor Browser Bundle

The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

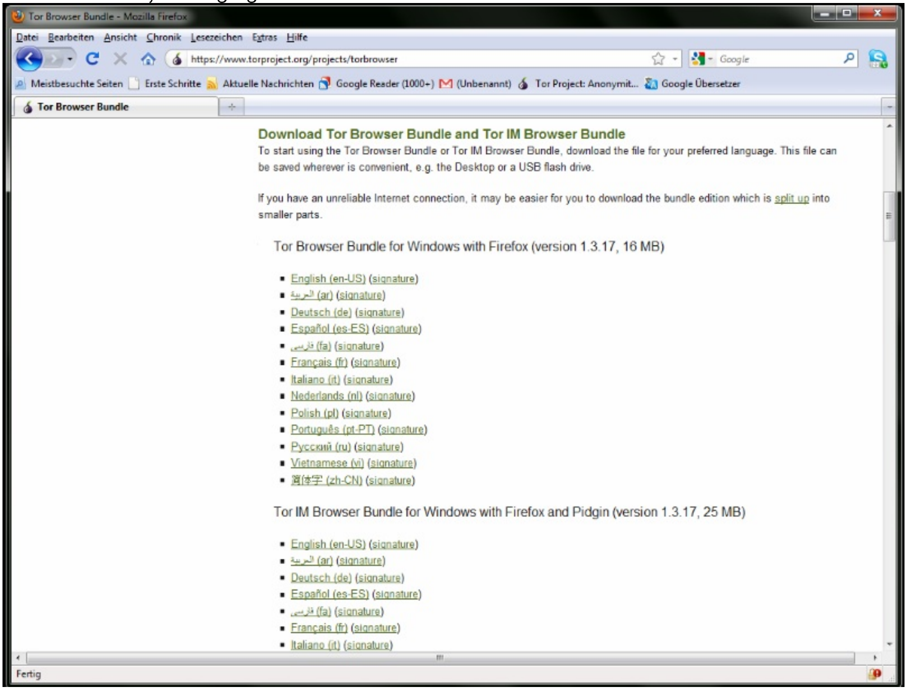
The **Tor Browser Bundle** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser, and is self-contained. The **Tor IM Browser Bundle** additionally allows instant messaging and chat over Tor. If you would prefer to use your existing web browser, install Tor permanently, or if you don't use Windows, see the other ways to download Tor.

Freedom House has produced a video on how to find and use the Tor Browser Bundle. If you don't see a video below, view it at Youtube . Know of a better video or one translated into your language? Let us know!

Tor Tip

Tor is written for and supported by people like you. Donate today!

2. Click the link for your language to download the installation file.


Tor Browser Bundle - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://www.torproject.org/projects/torbrowser
Meistbesuchte Seiten Erste Schritte Aktuelle Nachrichten Google Reader (1000+) (Unbenannt) Tor Project: Anonymit... Google Übersetzer
Tor Browser Bundle
Fertig

Download Tor Browser Bundle and Tor IM Browser Bundle

To start using the Tor Browser Bundle or Tor IM Browser Bundle, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

If you have an unreliable Internet connection, it may be easier for you to download the bundle edition which is split up into smaller parts.

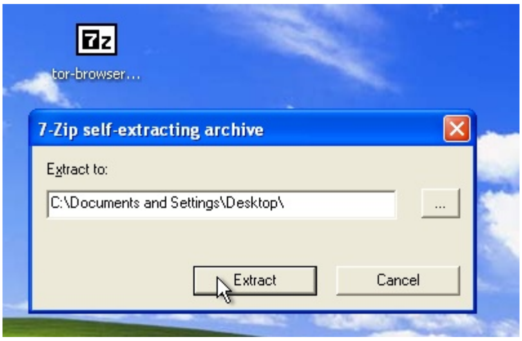
Tor Browser Bundle for Windows with Firefox (version 1.3.17, 16 MB)

- English (en-US) (signature)
- العربية (ar) (signature)
- Deutsch (de) (signature)
- Español (es-ES) (signature)
- فارسی (fa) (signature)
- Français (fr) (signature)
- Italiano (it) (signature)
- Nederlands (nl) (signature)
- Polish (pl) (signature)
- Português (pt-PT) (signature)
- Русский (ru) (signature)
- Vietnamese (vi) (signature)
- 简体字 (zh-CN) (signature)

Tor IM Browser Bundle for Windows with Firefox and Pidgin (version 1.3.17, 25 MB)

- English (en-US) (signature)
- العربية (ar) (signature)
- Deutsch (de) (signature)
- Español (es-ES) (signature)
- فارسی (fa) (signature)
- Français (fr) (signature)
- Italiano (it) (signature)

3. Double-click the .exe file that you have now downloaded. A "7-Zip self-extracting archive" window appears.



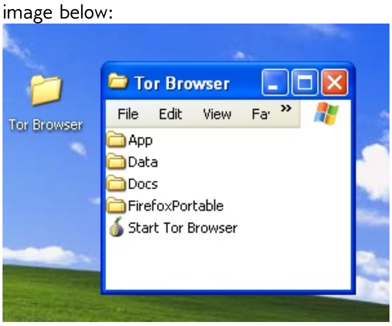
Extract to:

C:\Documents and Settings\Desktop\

1. Choose a folder into which you want to extract the files and click Extract.

   Note: you can choose to extract the files directly onto a USB flash drive if you want to use Tor Browser on different computers (for instance on public computers in Internet cafés).

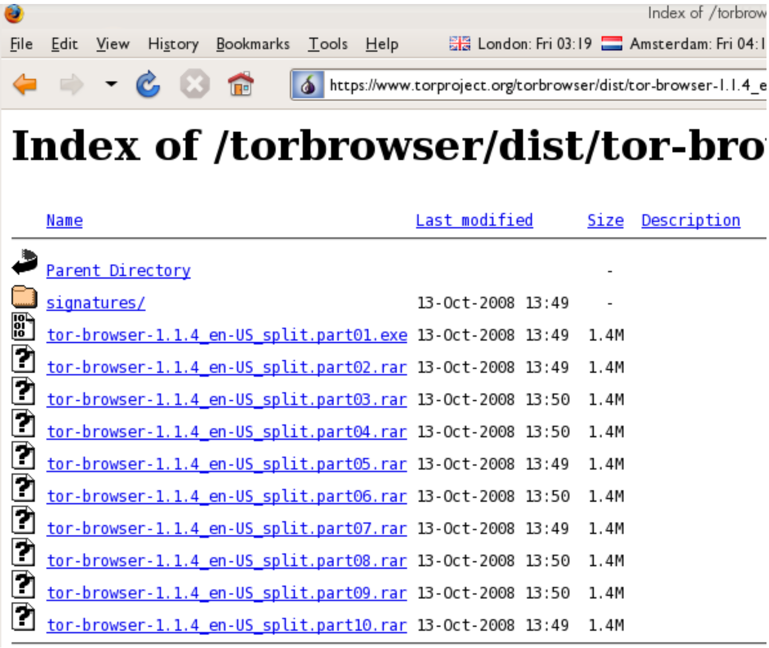
2. When the extraction is completed, open the folder and check that the contents match the image below:



   To clean up, delete the .exe file you originally downloaded.

Installing from split files

1. In your Web browser, enter the URL for the split version of the Tor Browser Bundle (https://www.torproject.org/projects/torbrowser-split.html.en), then click the link for your language to get to a page that looks like the one for English below:

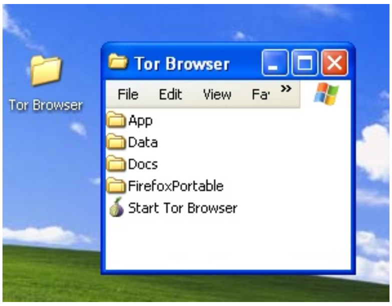


Index of /torbrowser/dist/tor-bro

Name	Last modified	Size	Description
Parent Directory		-	
signatures/	13-Oct-2008 13:49	-	
tor-browser-1.1.4_en-US_split.part01.exe	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part02.rar	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part03.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part04.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part05.rar	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part06.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part07.rar	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part08.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part09.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part10.rar	13-Oct-2008 13:49	1.4M	

2. Click each file to download it (one ending in .exe and nine others ending in .rar), one after the other, and save them all in one folder on your hard drive.
3. Double-click the first part (the file whose name ends in .exe). This runs a program to gather all the parts together.

   "Split installer for Tor Browser Bundle" src="static/CircumventionTools-InstallingTor-tor_winrar_2-en.png" height="384" width="562">
4. Choose a folder where you want to install the files, and click Install. The program displays progress messages while it's running, and then quits.
5. When the extraction is completed, open the folder and check that the contents match the image below:



6. To clean up, delete all the files you originally downloaded.

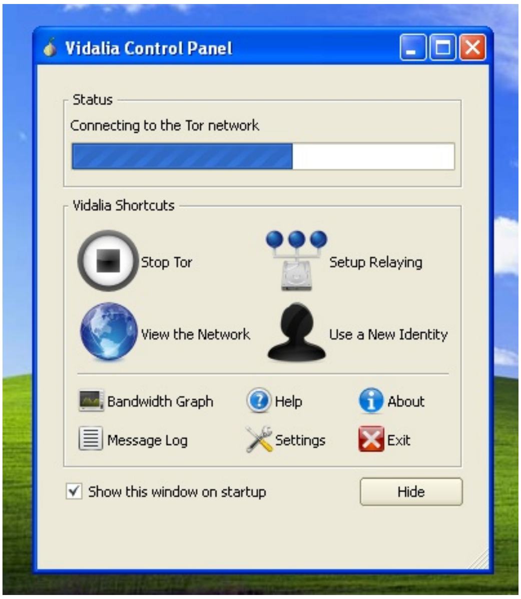
USING TOR BROWSER

Before you start:

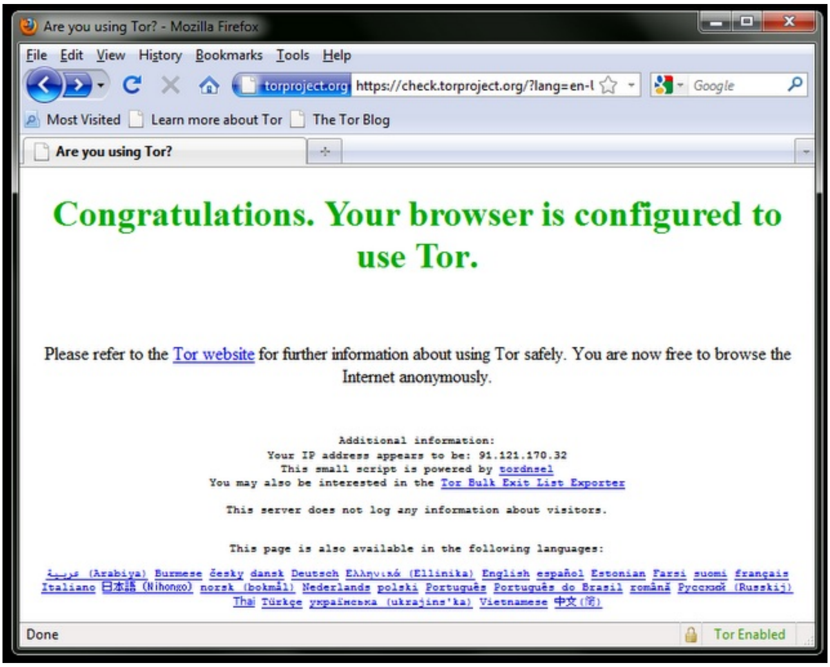
- Close Tor. If Tor is already installed on your computer, make sure it is not currently running.

Launch the Tor Browser:

In the Tor Browser folder, double-click Start Tor Browser. The Tor control panel (Vidalia) opens and Tor starts to connect to the Tor network.

- 

When a connection is established, Firefox automatically connects to the TorCheck page and then confirms that your browser is configured to use Tor. This may take some time, depending on the quality of your Internet connection.



Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
torproject.org https://check.torproject.org/?lang=en-l
Google
Most Visited
Learn more about Tor
The Tor Blog
Are you using Tor?

Congratulations. Your browser is configured to use Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

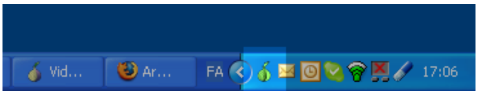
```
Additional information:
Your IP address appears to be: 91.121.170.32
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

This page is also available in the following languages:

عربية (Arabiya) Burmese česky dansk Deutsch Ελληνικά (Ellinika) English español Estonian Farsi suomi français
Italiano 日本語 (Nihongo) norsk (bokmål) Nederlands polski Português Português do Brasil română Русский (Russkij)
Thai Türkçe українська (ukrajins'ka) Vietnamese 中文(简)
```

If you are connected to the Tor network, a green onion icon appears in the system tray on the lower-right-hand corner of your screen:

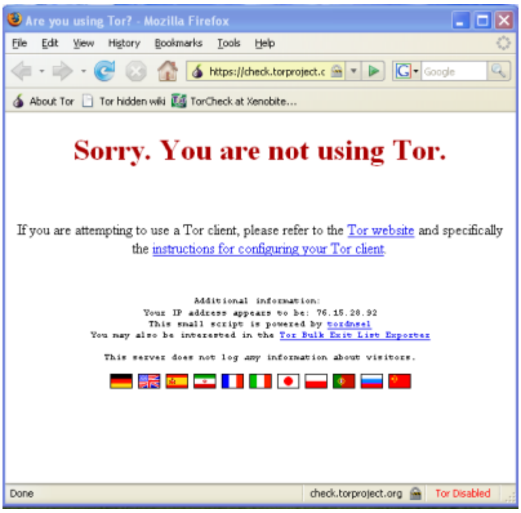


BROWSING THE WEB USING TOR BROWSER

Try viewing a few Web sites, and see if they are working. The sites are likely to load more slowly than usual because your connection is being routed through several relays.

IF THIS DOES NOT WORK

If the onion in the Vidalia Control Panel never turns green or if Firefox opened, but displayed a page saying "Sorry. You are not using Tor", as in the image below, then you are not using Tor.


Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://check.torproject.c
Google
About Tor
Tor hidden wiki
TorCheck at Xenobite...

Sorry. You are not using Tor.

If you are attempting to use a Tor client, please refer to the Tor website and specifically the instructions for configuring your Tor client.

Additional information:
Your IP address appears to be: 76.15.28.92
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

If you see this message, close Firefox and Tor Browser and then repeat the steps above. You can perform this check to ensure that you are using Tor at any time by going to https://check.torproject.org/.

If Tor Browser doesn't work after two or three tries, Tor may be partly blocked by your ISP and you should try using the **bridge** feature of Tor – see the section below on "Using Tor with Bridges".

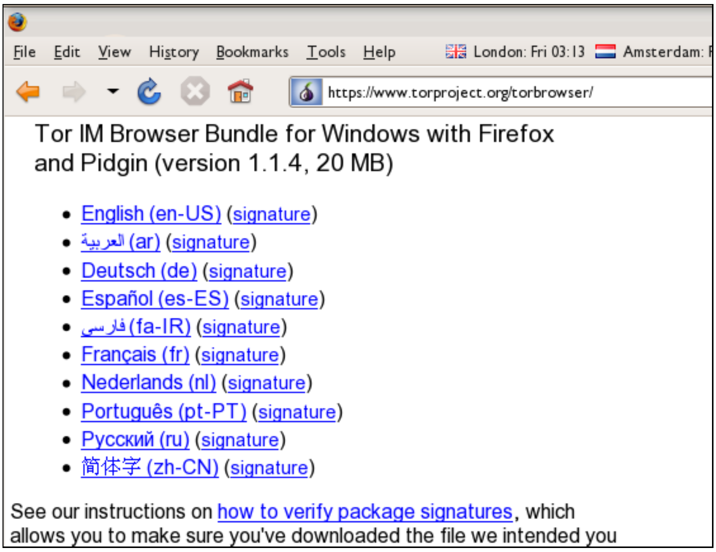
USING TOR IM BROWSER BUNDLE

The Tor IM Browser Bundle is similar to the Tor Browser Bundle, but includes access to the Pidgin multi-protocol instant messaging client, so you can chat encrypted over your favourite instant messenger protocol such as ICQ, MSN Messenger, Yahoo! Messenger or QQ which may be filtered.

You can learn more about Pidgin here: http://www.pidgin.im/

DOWNLOAD TOR IM BROWSER BUNDLE

You can download the Tor IM Browser Bundle directly from the Tor Web site at https://www.torproject.org/projects/torbrowser

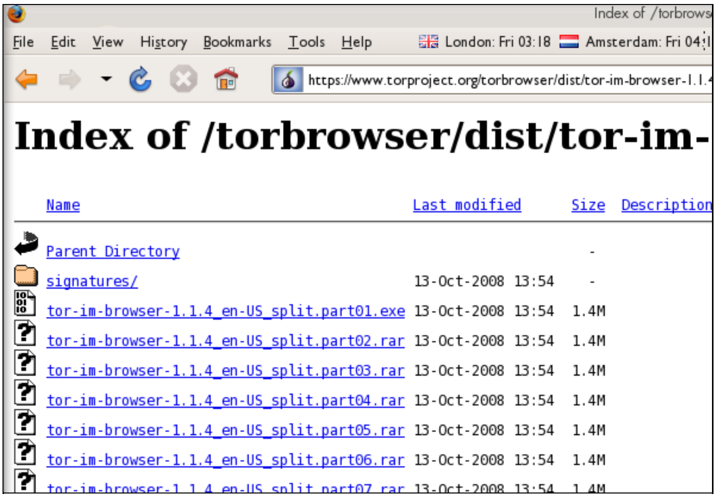

File Edit View History Bookmarks Tools Help
London: Fri 03:13 Amsterdam: F
https://www.torproject.org/torbrowser/

Tor IM Browser Bundle for Windows with Firefox and Pidgin (version 1.1.4, 20 MB)

- English (en-US) (signature)
- العربية (ar) (signature)
- Deutsch (de) (signature)
- Español (es-ES) (signature)
- فارسی (fa-IR) (signature)
- Français (fr) (signature)
- Nederlands (nl) (signature)
- Português (pt-PT) (signature)
- Русский (ru) (signature)
- 简体字 (zh-CN) (signature)

See our instructions on how to verify package signatures, which allows you to make sure you've downloaded the file we intended you

If your Internet connection is slow or unreliable, you can also get a split up version on the torproject.org Web site at https://www.torproject.org/projects/torbrowser-split.html.en.


Index of /torbrows
File Edit View History Bookmarks Tools Help
London: Fri 03:18 Amsterdam: Fri 04:
https://www.torproject.org/torbrowser/dist/tor-im-browser-1.1.4

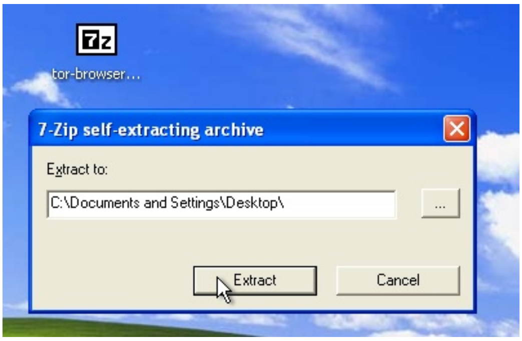
Index of /torbrowser/dist/tor-im-

Name	Last modified	Size	Description
Parent Directory		-	
signatures/	13-Oct-2008 13:54	-	
tor-im-browser-1.1.4_en-US_split.part01.exe	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part02.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part03.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part04.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part05.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part06.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part07.rar	13-Oct-2008 13:54	1.4M	

AUTO-EXTRACT THE ARCHIVE

To get started, double-click the .exe file you have downloaded.

You should see the window below:



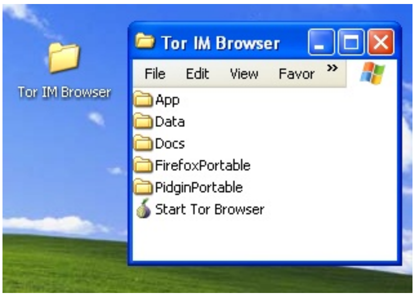
Extract to:

C:\Documents and Settings\Desktop\

- Choose a folder into which you want to extract the files. If you are not sure leave the default value untouched. Then click Extract.

Note: you can choose to extract the files directly onto a USB flash drive if you want to use Tor Browser on different computers (for instance on public computers in Internet cafés).

- When the extraction is completed, open the newly-created folder and check that it looks like the image below (note the PidginPortable folder):



- You can now safely delete the .exe file you originally downloaded (or the several .rar and .exe files if you used the split version).

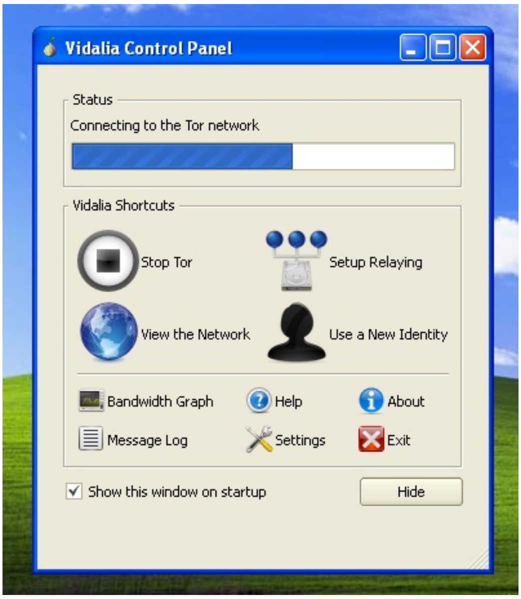
USING TOR IM BROWSER BUNDLE

Before you start:

- Close Firefox. If the Firefox browser is installed on your computer, make sure it is not currently running.
- Close Tor. If Tor is already installed on your computer, make sure it is not currently running.

Launch Tor IM Browser:

- In the Tor Browser folder, double-click Start Tor Browser. The Tor control panel (Vidalia) opens and Tor connects to the Tor network.

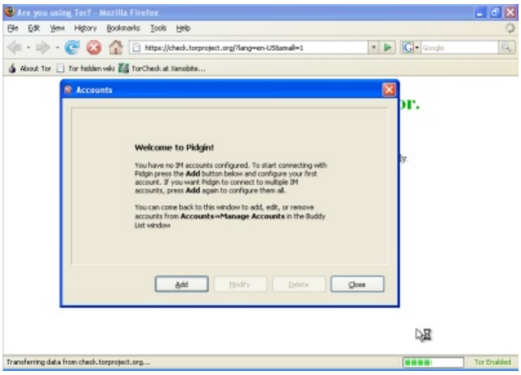

Vidalia Control Panel

Status

Connecting to the Tor network

When a connection is established:

- A Firefox browser window pops up and connects to the TorCheck page, which should show a green onion that confirms you that your browser is configured to use Tor.
- A Pidgin assistant window (below) pops up inviting you to set up your IM account on Pidgin.

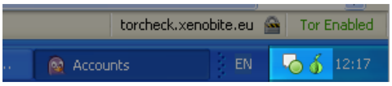

Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://check.torproject.org/?lang=en-US&small=1
Google
About Tor
Tor hidden wiki
TorCheck at Xenobite...
Accounts
Add
Modify
Delete
Close
Transferring data from check.torproject.org...
Tor Enabled

Welcome to Pidgin!

You have no IM accounts configured. To start connecting with Pidgin press the **Add** button below and configure your first account. If you want Pidgin to connect to multiple IM accounts, press **Add** again to configure them all.

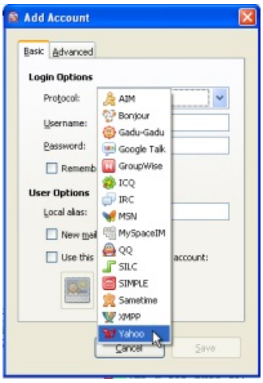
You can come back to this window to add, edit, or remove accounts from **Accounts→Manage Accounts** in the Buddy List window

You will also see the Tor icon (a green onion if you are connected) and a Pidgin icon appear in the system tray on the lower right corner of your screen:



SET UP YOUR IM ACCOUNT IN PIDGIN

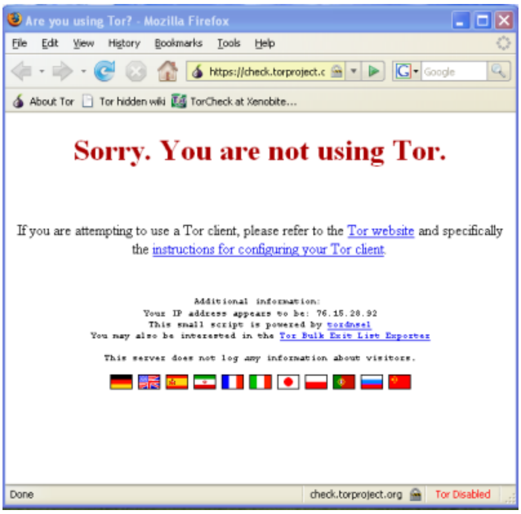
You can set up your IM account in the Pidgin window. Pidgin is compatible with most major IM services (AIM, MSN, Yahoo!, Google Talk, Jabber, XMPP, ICQ and others):



To learn more on how you can use Pidgin, read:

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

IF THIS DOES NOT WORK


Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://check.torproject.c
Google
About Tor
Tor hidden wiki
TorCheck at Xenobite...
Done
check.torproject.org
Tor Disabled

Sorry. You are not using Tor.

If you are attempting to use a Tor client, please refer to the Tor website and specifically the instructions for configuring your Tor client.

```
Additional information:
Your IP address appears to be: 76.15.28.92
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.
```

If the onion in the Vidalia Control Panel doesn't turn green or if Firefox opens, but displays a page saying "Sorry. You are not using Tor", then you should:

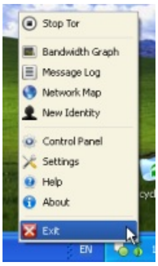
- Exit Vidalia and Pidgin (see below for details).
- Relaunch Tor IM Browser following the steps above ("Using Tor IM Browser Bundle").

If Tor Browser still doesn't work after two or three tries, Tor may be partly blocked by your ISP. Refer to the "Using Tor with Bridges" section below to use the bridge feature of Tor.

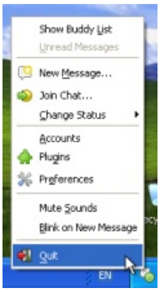
EXIT TOR IM BROWSER

To exit the Tor IM Browser you need to:

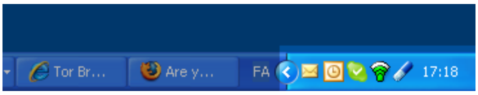
- Exit Vidalia by right-clicking on the onion icon in your tray bar and choosing Exit in the Vidalia contextual menu.



- Exit Pidgin by right-clicking on the Pidgin icon in your tray bar and choosing Quit in the Pidgin contextual menu.



When the Vidalia onion icon and the Pidgin icon have disappeared from the Windows system tray in the lower-right-hand corner of your screen, Tor IM Browser is closed.



USING TOR WITH BRIDGES

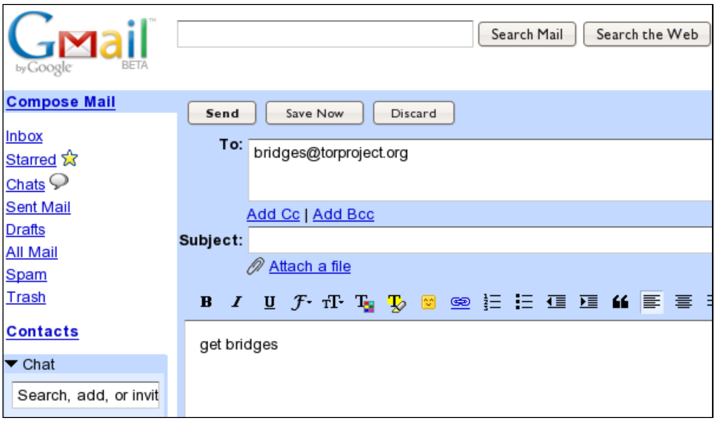
If you suspect your access to the Tor network is being blocked, you may want to use the **bridge** feature of Tor. The bridge feature was created specifically to help people use Tor from places where access to the Tor network is blocked. You must already have successfully downloaded and installed the Tor software to use a bridge.

WHAT IS A BRIDGE?

Bridge relays (or *bridges* for short) are Tor relays that aren't listed in the main public Tor directory. This is a deliberate measure to stop these relays from being blocked. Even if your ISP is filtering connections to all the publicly known Tor relays, it may not be able to block all the bridges.

WHERE DO I FIND BRIDGES?

To use a bridge, you need to locate one and add its information in your network settings. A simple way to get a few bridges is by simply accessing https://bridges.torproject.org/ with your Web browser. If that Web site is blocked or you need more bridges, send an e-mail from a Gmail account to bridges@torproject.org with "get bridges" (without the quotemarks) in the body of the message.

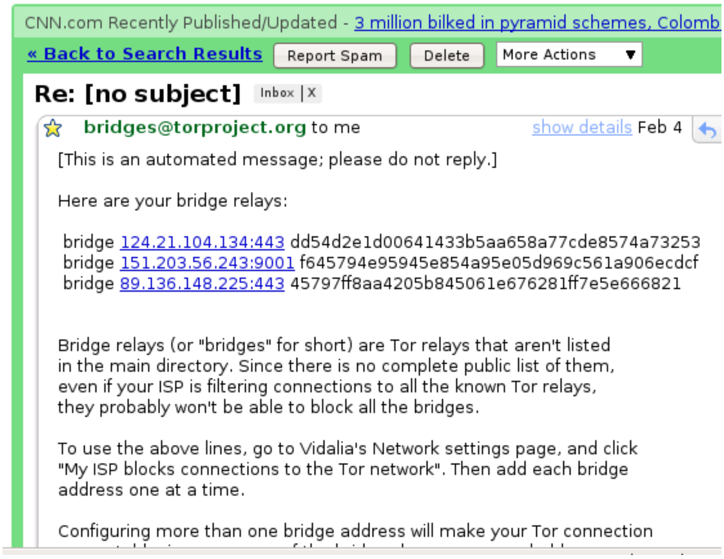


To: bridges@torproject.org

Subject:

get bridges

Almost instantly, you will receive a reply that includes information about a few bridges:


CNN.com Recently Published/Updated - 3 million bilked in pyramid schemes, Colomb
« Back to Search Results
Report Spam
Delete
More Actions
Inbox | X
show details

Re: [no subject]

bridges@torproject.org to me Feb 4

[This is an automated message; please do not reply.]

Here are your bridge relays:

```
bridge 124.21.104.134:443 dd54d2e1d00641433b5aa658a77cde8574a73253
bridge 151.203.56.243:9001 f645794e95945e854a95e05d969c561a906ecdcf
bridge 89.136.148.225:443 45797ff8aa4205b845061e676281ff7e5e666821
```

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

To use the above lines, go to Vidalia's Network settings page, and click "My ISP blocks connections to the Tor network". Then add each bridge address one at a time.

Configuring more than one bridge address will make your Tor connection

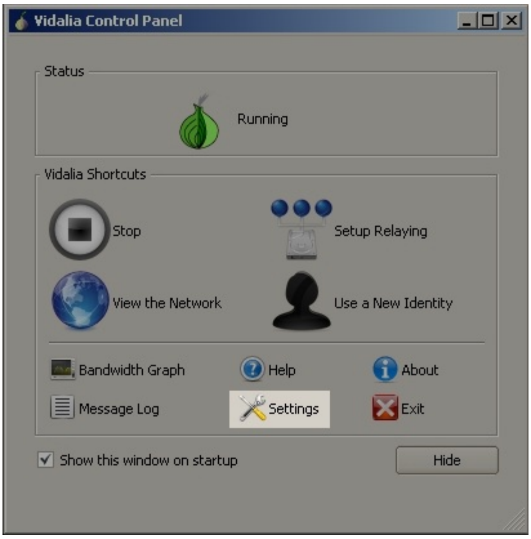
Important Notes:

1. You *must* use a Gmail account to send the request. If torproject.org accepted requests from other mail accounts, an attacker could easily create a lot of email addresses and quickly learn about all the bridges. If you do not have a Gmail account already, creating one takes only a few minutes.
2. If you are on a slow Internet connection you can use the URL https://mail.google.com/mail/h/ for a direct access to the basic HTML version of Gmail.

TURN ON BRIDGING AND ENTER BRIDGE INFORMATION

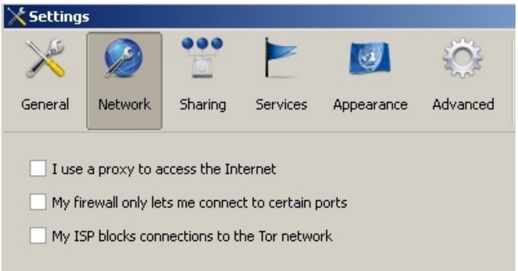
After you get addresses for some bridge relays, you must configure Tor with whatever bridge address you intend to use:

1. Open the Tor control panel (Vidalia).



☑ Show this window on startup

2. Click Settings. A Settings window opens.

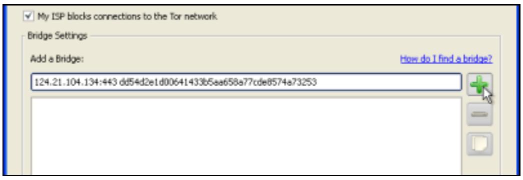


☐ I use a proxy to access the Internet

☐ My firewall only lets me connect to certain ports

☐ My ISP blocks connections to the Tor network

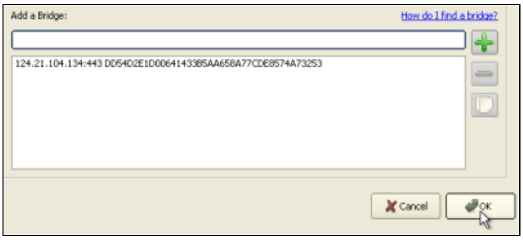
3. Click Network.
4. Select "My Firewall only lets me connect to certain ports" and "My ISP blocks connections to the Tor network".
5. Enter the bridge URL information you received by e-mail in the "Add a Bridge" field.
6. Click the green + on the right side of the "Add a Bridge" field. The URL is added to the box below.



☑ My ISP blocks connections to the Tor network

Add a Bridge: 124.21.104.134:443 dd54d2e1d00641433b5aa658a77cde8574a73253

7. Click OK at the bottom of the window to validate your new settings.



Add a Bridge:

124.21.104.134:443 DD54D2E1D00641433B5AA658A77CDE8574A73253

8. In the Tor control panel, stop and restart Tor to use your new settings.

Note:

Add as many bridge addresses as you can. Additional bridges increase reliability. One bridge is enough to reach the Tor network, however if you have only one bridge and it gets blocked or stops operating, you will be cut off from the Tor network until you add new bridges.

To add more bridges in your network settings, repeat the steps above with the information on the additional bridges that you got from the bridges@torproject.org e-mail message.

25. JONDO

JonDo started as a German university project called Java Anon Proxy (JAP) and has become a robust anonymity tool that, like Tor, sends traffic through several independent servers.

Unlike Tor, however, the JonDo network mixes servers run by volunteers with others maintained by a parent company. The arrangement gives users a choice of speeds: 30-50 kBit/s (about the speed of an analog modem connection) for free, >600 kBit/s for a fee. For a more detailed comparison and price list, see: https://anonymous-proxy-servers.net/en/payment.html.

GENERAL INFORMATION

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?

INSTALLATION

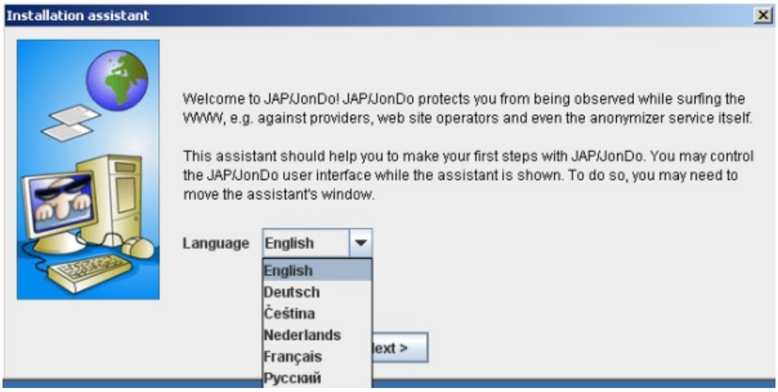
To use the JonDo network, called JonDonym, you'll need to download the JonDo client for your operating system from https://www.jondos.de/en/download. Versions are available for Linux (about 9 MB), Mac OS X (about 17 MB) and Windows (about 35 MB).

Once you have download the client, install it as you would any software for your platform. You may be asked if you wish to install it on your PC or if you wish to create a portable version. For our example, we will assume you are installing JonDo on a PC.

Windows users also may be invited to install the JonDoFox web browser, discussed below.

CONFIGURATION AND USAGE

When you first start JonDo, you can choose the language you want displayed.



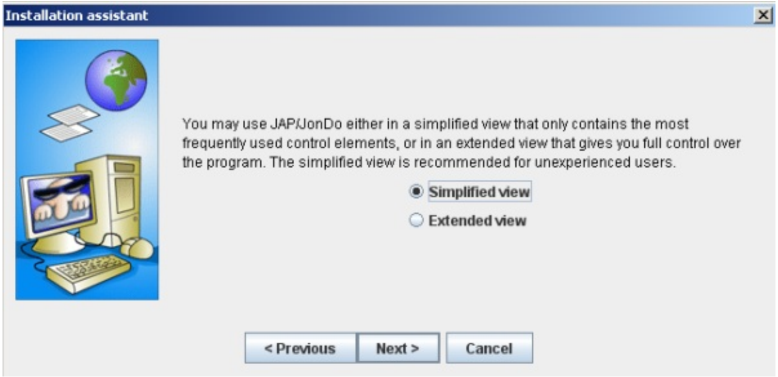
Installation assistant

Welcome to JAP/JonDo! JAP/JonDo protects you from being observed while surfing the WWW, e.g. against providers, web site operators and even the anonymizer service itself.

This assistant should help you to make your first steps with JAP/JonDo. You may control the JAP/JonDo user interface while the assistant is shown. To do so, you may need to move the assistant's window.

Language: English

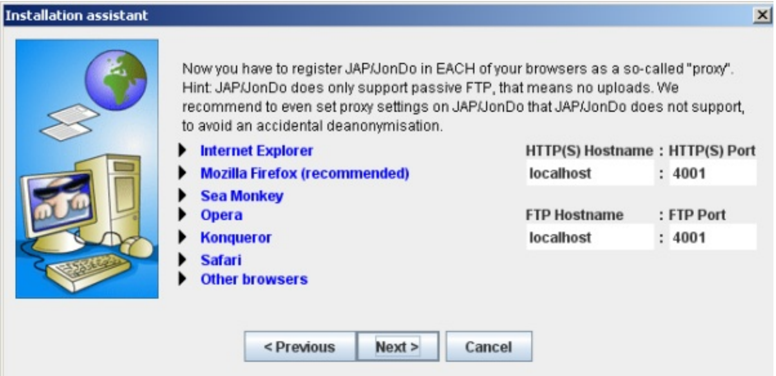
Next, you can choose the level of detail you wish to see when using the service. Inexperienced users should choose "Simplified view".



You may use JAP/JonDo either in a simplified view that only contains the most frequently used control elements, or in an extended view that gives you full control over the program. The simplified view is recommended for unexperienced users.

● Simplified view
○ Extended view

On the next screen, the Installation assistant asks you to choose the Web browser that you want to use the JonDo proxy tool. Click on the name of your browser, and follow the instructions.



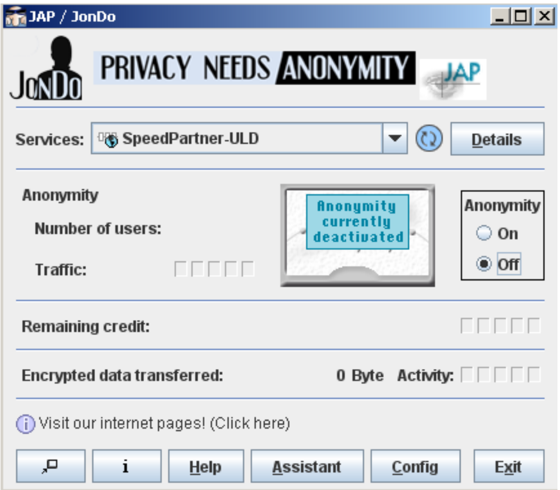
Now you have to register JAP/JonDo in EACH of your browsers as a so-called "proxy". Hint: JAP/JonDo does only support passive FTP, that means no uploads. We recommend to even set proxy settings on JAP/JonDo that JAP/JonDo does not support, to avoid an accidental deanonymisation.

- Internet Explorer
- Mozilla Firefox (recommended)
- Sea Monkey
- Opera
- Konqueror
- Safari
- Other browsers

HTTP(S) Hostname : HTTP(S) Port
localhost : 4001

FTP Hostname : FTP Port
localhost : 4001

Once that is completed, JonDo asks you to test your configuration. In the control panel, switch anonymity to Off and then try opening a Web site with the browser you have just configured.



Services: SpeedPartner-ULD

Anonymity
Number of users:
Traffic:

Anonymity currently deactivated

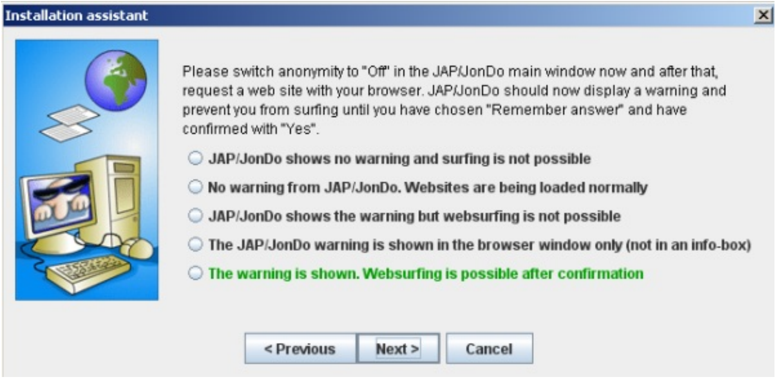
Anonymity
○ On
● Off

Remaining credit:

Encrypted data transferred: 0 Byte Activity:

Visit our internet pages! (Click here)

If JonDo shows you a warning and you have to choose "Yes" to view the Web site, everything is configured properly and you can select "The warning is shown. Websurfing is possible after confirmation". If any other description applies to you, choose it and the Installation assistant will give you more information on how to solve the problem.



Please switch anonymity to "Off" in the JAP/JonDo main window now and after that, request a web site with your browser. JAP/JonDo should now display a warning and prevent you from surfing until you have chosen "Remember answer" and have confirmed with "Yes".

○ JAP/JonDo shows no warning and surfing is not possible

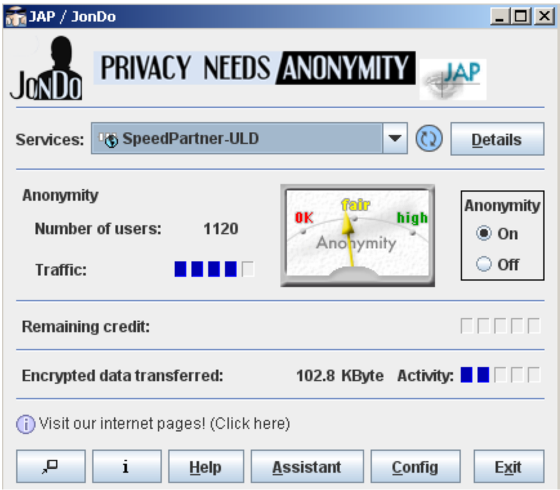
○ No warning from JAP/JonDo. Websites are being loaded normally

○ JAP/JonDo shows the warning but websurfing is not possible

○ The JAP/JonDo warning is shown in the browser window only (not in an info-box)

○ The warning is shown. Websurfing is possible after confirmation

Now take the second step to insure a proper configuration: Switch anonymity to "On" in the control panel and open a random Web site with the browser you have configured.



Services: SpeedPartner-ULD

Anonymity

Number of users: 1120

Traffic:

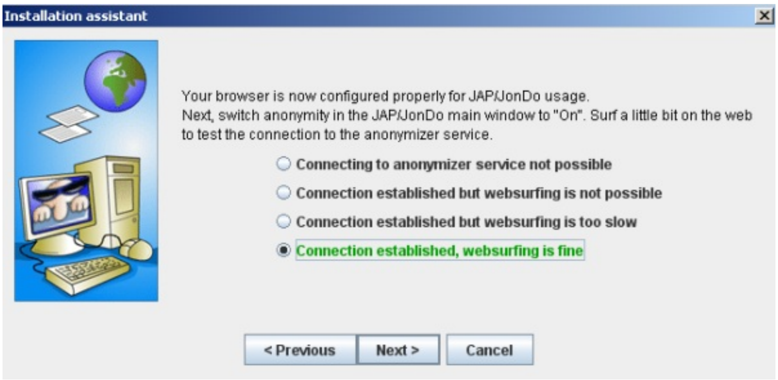
Anonymity ● On ○ Off

Remaining credit:

Encrypted data transferred: 102.8 KByte Activity:

Visit our internet pages! (Click here)

If the Web site loads, everything is fine and you can click "Connection established, websurfing is fine". If another description applies to you choose that one and the Installation assistant will help you solve the problem.



Your browser is now configured properly for JAP/JonDo usage.
Next, switch anonymity in the JAP/JonDo main window to "On". Surf a little bit on the web to test the connection to the anonymizer service.

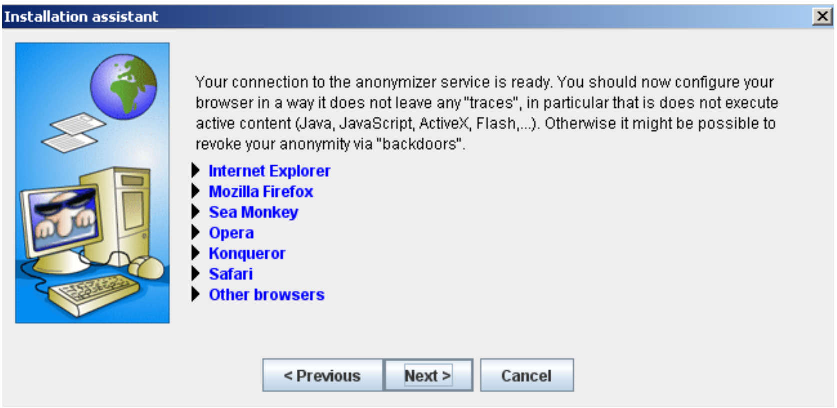
○ Connecting to anonymizer service not possible

○ Connection established but websurfing is not possible

○ Connection established but websurfing is too slow

● Connection established, websurfing is fine

We're almost done. You have successfully configured your browser to connect through the JonDo network. Now, you should also configure your browser so that it doesn't accidentally leak any information. Click on the name of your browser to start the process.

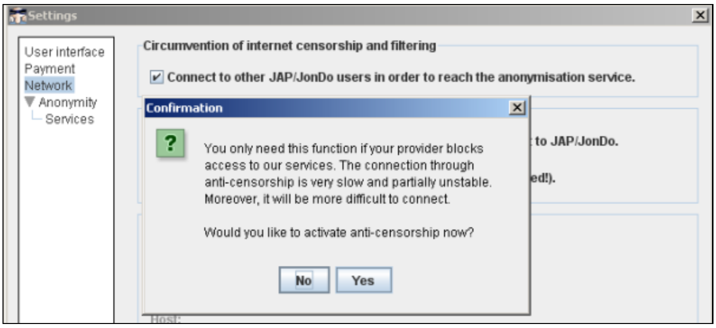


Installation assistant

Your connection to the anonymizer service is ready. You should now configure your browser in a way it does not leave any "traces", in particular that is does not execute active content (Java, JavaScript, ActiveX, Flash,...). Otherwise it might be possible to revoke your anonymity via "backdoors".

- Internet Explorer
- Mozilla Firefox
- Sea Monkey
- Opera
- Konqueror
- Safari
- Other browsers

If the standard JonDo servers are already blocked in your country, you should try the anti-censorship option. Click "Config" in the control panel and select the Network tab. Click on "Connect to other JAP/JonDo users in order to reach the anonymization service". Read the warning and confirm by clicking "Yes".



Settings

Circumvention of internet censorship and filtering

☑ Connect to other JAP/JonDo users in order to reach the anonymisation service.

Confirmation

You only need this function if your provider blocks access to our services. The connection through anti-censorship is very slow and partially unstable. Moreover, it will be more difficult to connect.

Would you like to activate anti-censorship now?

To make sure you configured your browser correctly, you can point it to http://what-is-my-ip-address.anonymous-proxy-servers.net which will tell you if there is any problem.

JONDOFOX

For additional security, the JonDoNym team offers a modified Firefox Web browser called JonDoFox. Similar to the Tor browser bundle, it prevents leaking additional information while using the anonymization tool.

You can download the tool at https://anonymous-proxy-servers.net/en/jondofox.html.

26. YOUR-FREEDOM

Your-Freedom is a commercial proxy tool that also offers a free (though slower) service.

The software is available for Microsoft Windows, Linux and Mac OS and connects you to a network of about 30 servers across ten countries. Your-Freedom also offers advanced services like OpenVPN and SOCKS, making it a relatively sophisticated tool to bypass Internet censorship.

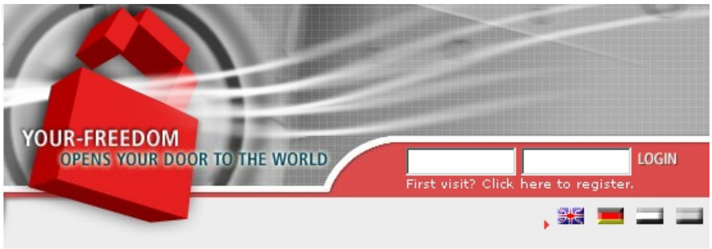
GENERAL INFORMATION

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

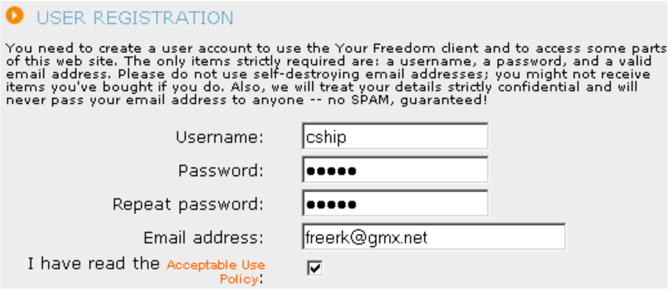
PREPARING THE USE OF YOUR-FREEDOM

First, download the tool for free from https://www.your-freedom.net/index.php?id=downloads. If you already have Java installed, you can download the small version which is about 2 MB. To check whether Java is installed, visit http://www.java.com/en/download/testjava.jsp. If you don't have Java installed, download the full installer, which is about 12 MB. All files are also available from http://mediafire.com/yourfreedom.

If you live in a country where the government censors access to the Internet, Your-Freedom may work for you with the Sesawe account (username: sesawe, password: sesawe). If that doesn't work you have to register for a account. To get started, register a free account on the Web site https://www.your-freedom.net/index.php?id=170&L=0.


YOUR-FREEDOM
OPENS YOUR DOOR TO THE WORLD
LOGIN
First visit? Click here to register.

Click the "First visit? Click here to register" link below the two login fields.



USER REGISTRATION

You need to create a user account to use the Your Freedom client and to access some parts of this web site. The only items strictly required are: a username, a password, and a valid email address. Please do not use self-destroying email addresses; you might not receive items you've bought if you do. Also, we will treat your details strictly confidential and will never pass your email address to anyone -- no SPAM, guaranteed!

Username: cship

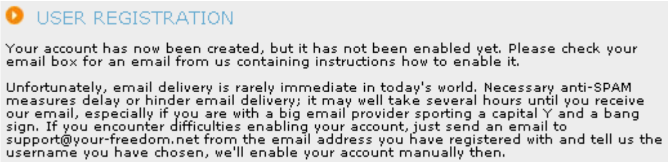
Password: ●●●●●

Repeat password: ●●●●●

Email address: freerk@gmx.net

I have read the Acceptable Use Policy: ☑

On the next page, enter the required information. Only a username, password, and e-mail address are needed. Other information is optional.

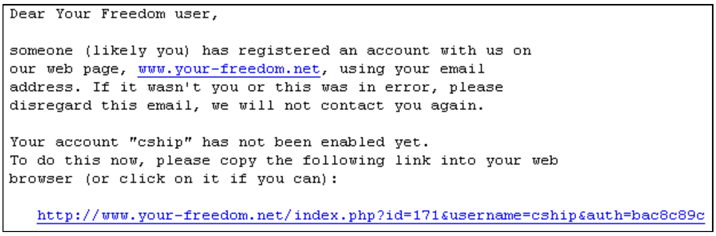


USER REGISTRATION

Your account has now been created, but it has not been enabled yet. Please check your email box for an email from us containing instructions how to enable it.

Unfortunately, email delivery is rarely immediate in today's world. Necessary anti-SPAM measures delay or hinder email delivery; it may well take several hours until you receive our email, especially if you are with a big email provider sporting a capital Y and a bang sign. If you encounter difficulties enabling your account, just send an email to support@your-freedom.net from the email address you have registered with and tell us the username you have chosen, we'll enable your account manually then.

You'll see a message that your registration is almost complete and within a few seconds, you should receive an e-mail at the address you provided.



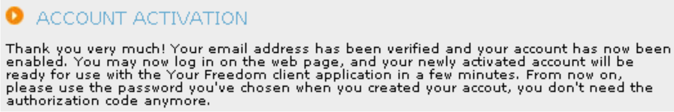
```
Dear Your Freedom user,

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
```

Click the second link (the longer one) to confirm your registration.



ACCOUNT ACTIVATION

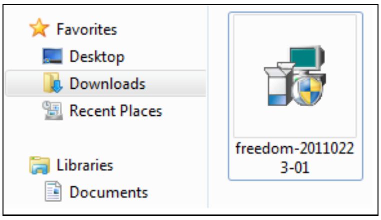
Thank you very much! Your email address has been verified and your account has now been enabled. You may now log in on the web page, and your newly activated account will be ready for use with the Your Freedom client application in a few minutes. From now on, please use the password you've chosen when you created your accout, you don't need the authorization code anymore.

When you see the "Thank you" screen, your account has been activated.

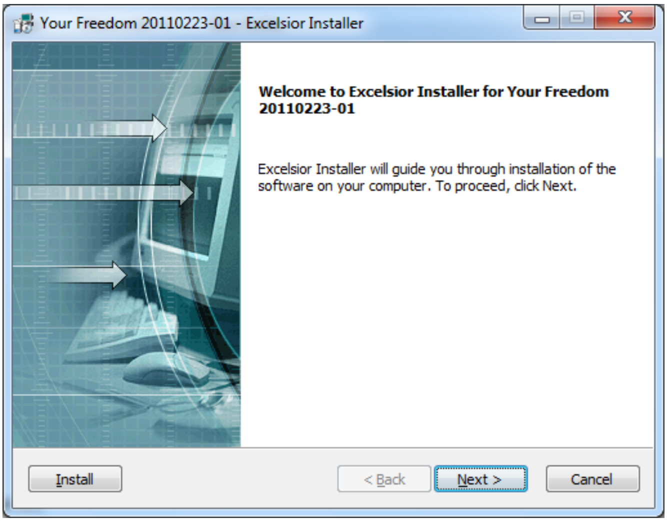
INSTALLATION

The following instructions and screenshots have been captured under Windows, but all the steps and settings are very similar for other operating systems.

Now you are ready to install Your-Freedom.



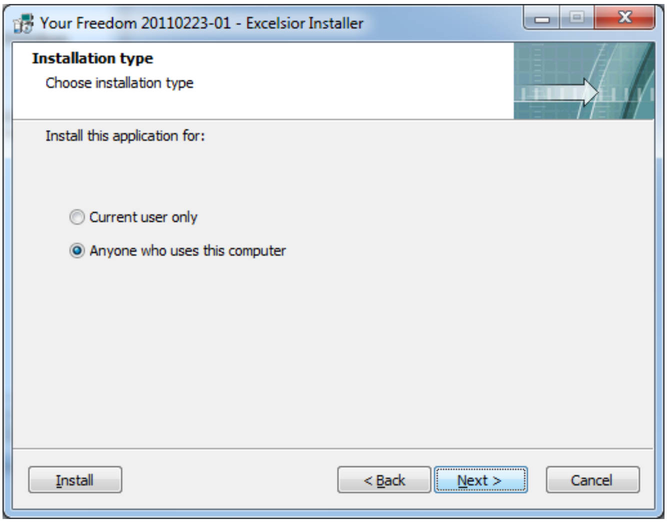
Click on the downloaded file. The file name may vary as new versions are released on a regular basis.



Welcome to Excelsior Installer for Your Freedom 20110223-01

Excelsior Installer will guide you through installation of the software on your computer. To proceed, click Next.

Click Next in the first screen.



Your Freedom 20110223-01 - Excelsior Installer

Installation type

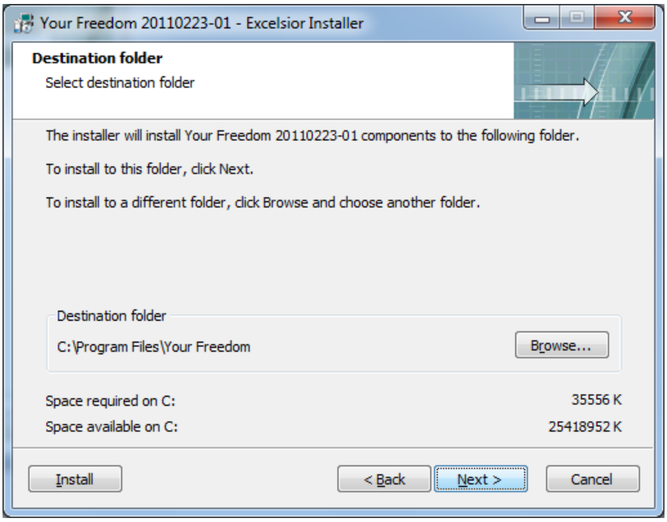
Choose installation type

Install this application for:

○ Current user only

● Anyone who uses this computer

In the next screen you can choose if the program should be usable only for your account only or for all users of your computer (common). Then click Next.



Your Freedom 20110223-01 - Excelsior Installer

Destination folder

Select destination folder

The installer will install Your Freedom 20110223-01 components to the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and choose another folder.

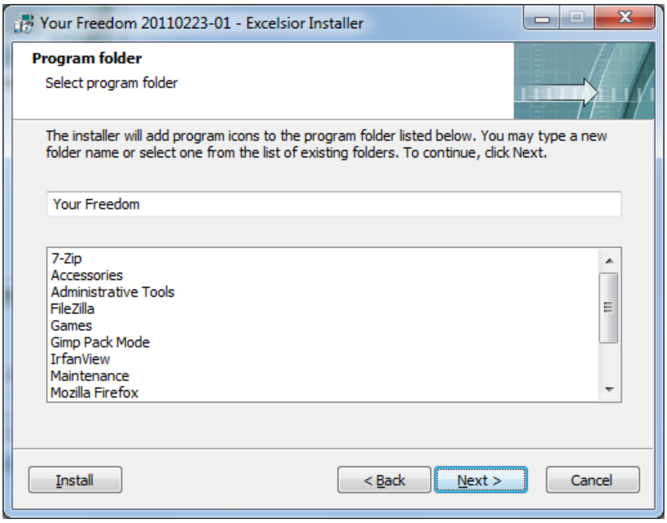
Destination folder

C:\Program Files\Your Freedom

Space required on C: 35556 K

Space available on C: 25418952 K

Choose the directory for installing Your-Freedom. Most users should accept the default selection. Click Next.



Program folder

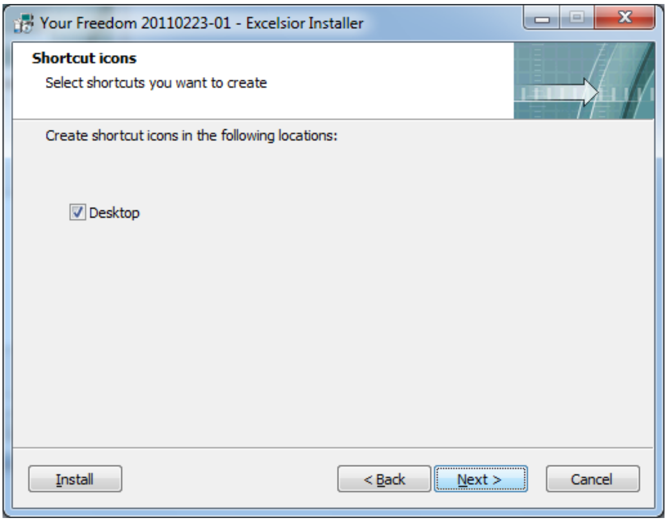
Select program folder

The installer will add program icons to the program folder listed below. You may type a new folder name or select one from the list of existing folders. To continue, click Next.

Your Freedom

7-Zip
Accessories
Administrative Tools
FileZilla
Games
Gimp Pack Mode
IrfanView
Maintenance
Mozilla Firefox

On the next screen of the installer you can alter the name which will be used in the program folder. You can leave the default untouched and click Next.



Shortcut icons

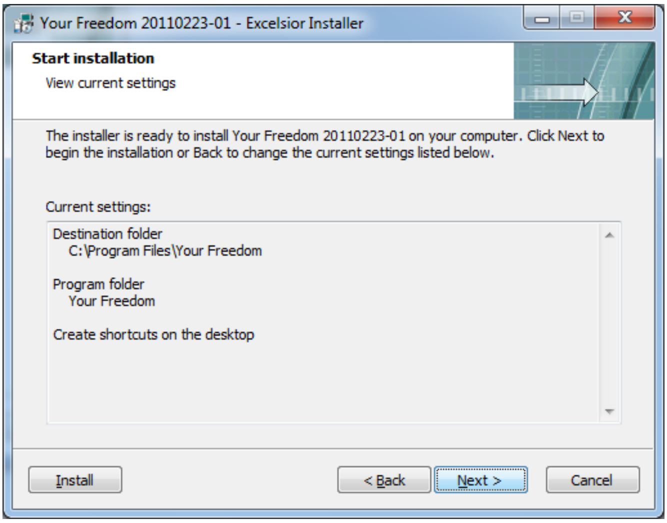
Select shortcuts you want to create

Create shortcut icons in the following locations:

☑ Desktop

Choose whether you want to create an icon on the desktop. Click Next again.

Here you can see a summary of the decisions you made. Confirm them by clicking Next, or go back if anything needs changing.


Your Freedom 20110223-01 - Excelsior Installer

Start installation

View current settings

The installer is ready to install Your Freedom 20110223-01 on your computer. Click Next to begin the installation or Back to change the current settings listed below.

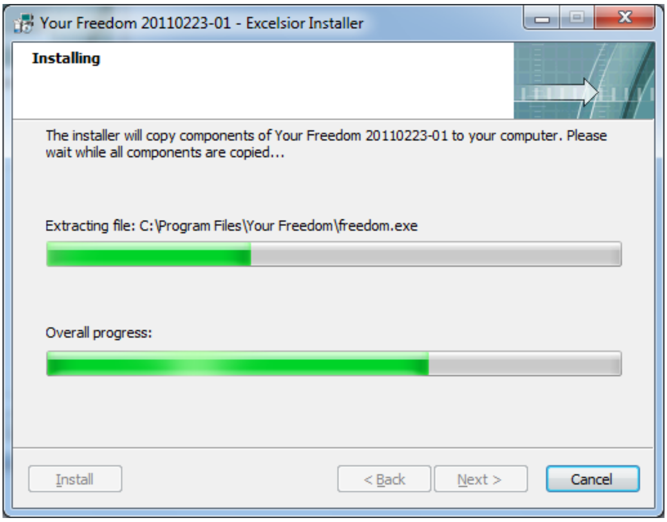
Current settings:

Destination folder
  C:\Program Files\Your Freedom

Program folder
  Your Freedom

Create shortcuts on the desktop

Now the installation takes place. This may take a few minutes, depending on your PC.

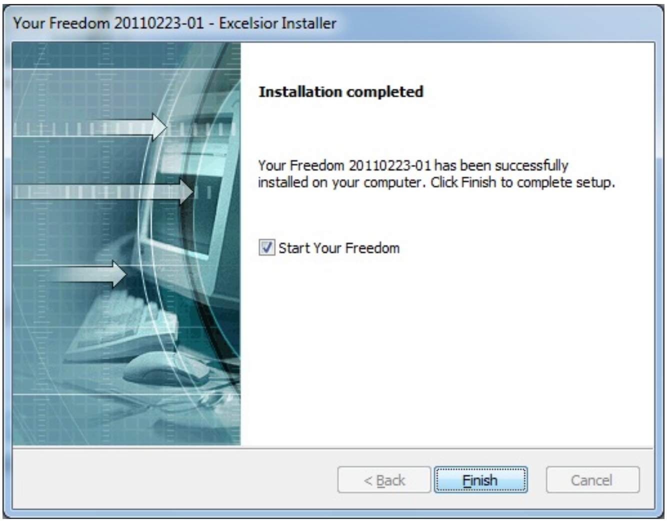

Your Freedom 20110223-01 - Excelsior Installer

Installing

The installer will copy components of Your Freedom 20110223-01 to your computer. Please wait while all components are copied...

Extracting file: C:\Program Files\Your Freedom\freedom.exe

Overall progress:


Your Freedom 20110223-01 - Excelsior Installer

Installation completed

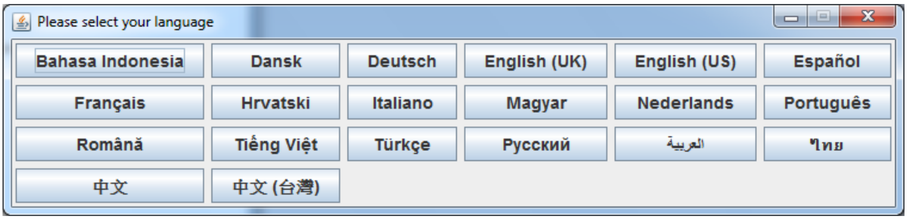
Your Freedom 20110223-01 has been successfully installed on your computer. Click Finish to complete setup.

☑ Start Your Freedom

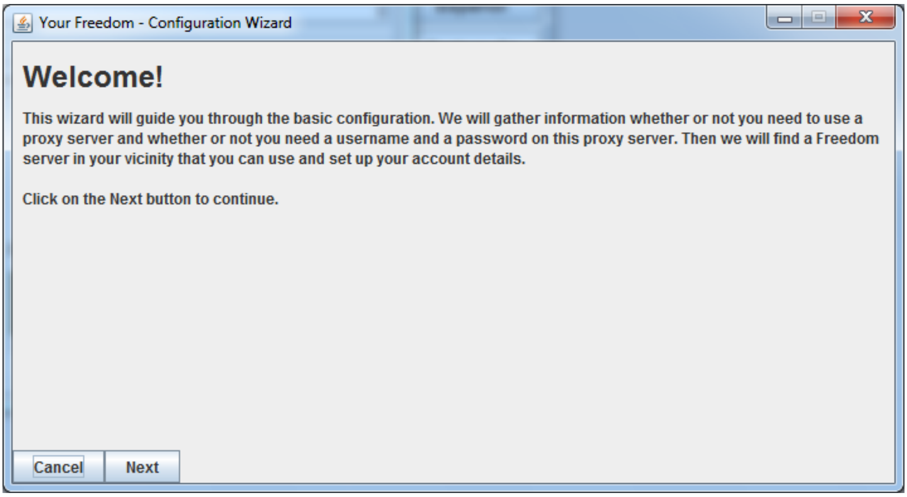
Finally the installation is ready. Quit the installation program by clicking Finish.

Your-Freedom will start automatically. When you later want to start it manually click on the Your-Freedom icon (the door) on your desktop.

When you first start Your-Freedom you need to configure it.



The first step is to choose your language. Click on the language you want. You will be able to change the settings later.

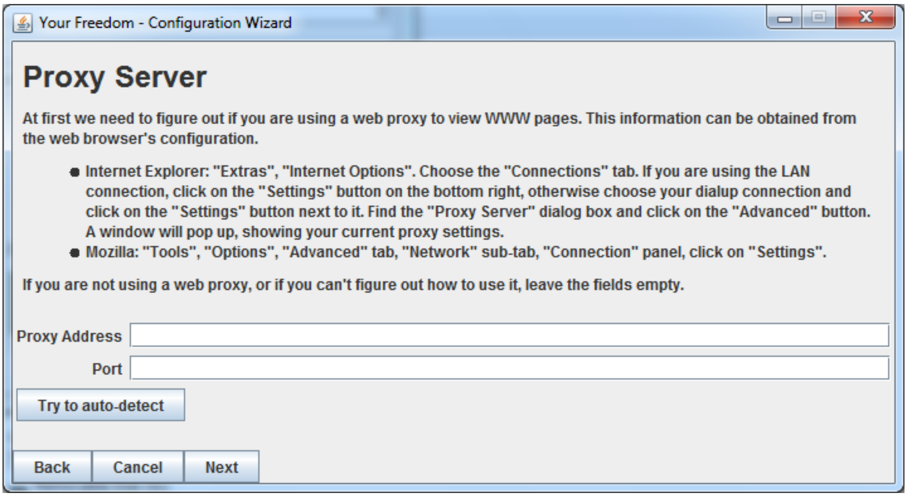


Welcome!

This wizard will guide you through the basic configuration. We will gather information whether or not you need to use a proxy server and whether or not you need a username and a password on this proxy server. Then we will find a Freedom server in your vicinity that you can use and set up your account details.

Click on the Next button to continue.

Right after the first start you will see the configuration wizard. Click Next.



Proxy Server

At first we need to figure out if you are using a web proxy to view WWW pages. This information can be obtained from the web browser's configuration.

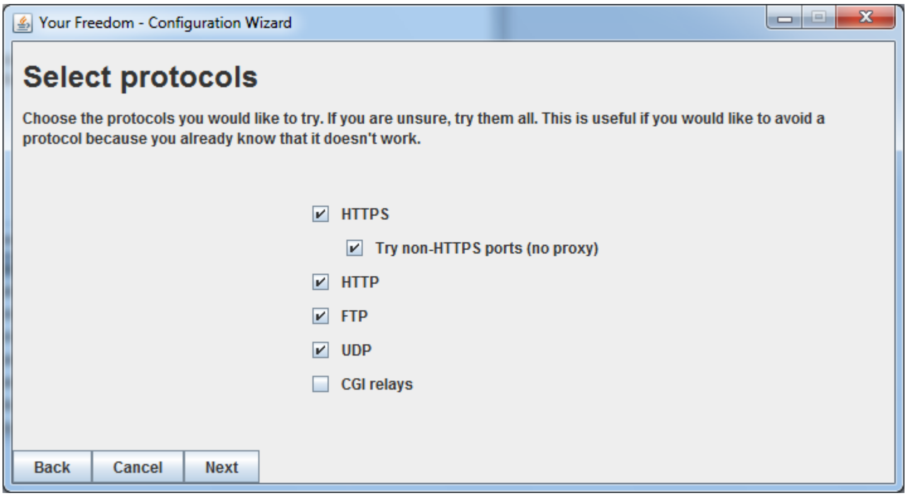
- Internet Explorer: "Extras", "Internet Options". Choose the "Connections" tab. If you are using the LAN connection, click on the "Settings" button on the bottom right, otherwise choose your dialup connection and click on the "Settings" button next to it. Find the "Proxy Server" dialog box and click on the "Advanced" button. A window will pop up, showing your current proxy settings.
- Mozilla: "Tools", "Options", "Advanced" tab, "Network" sub-tab, "Connection" panel, click on "Settings".

If you are not using a web proxy, or if you can't figure out how to use it, leave the fields empty.

Proxy Address

Port

In the Proxy Server dialog the program will auto-detect the information of a proxy server you can use. Click Next.

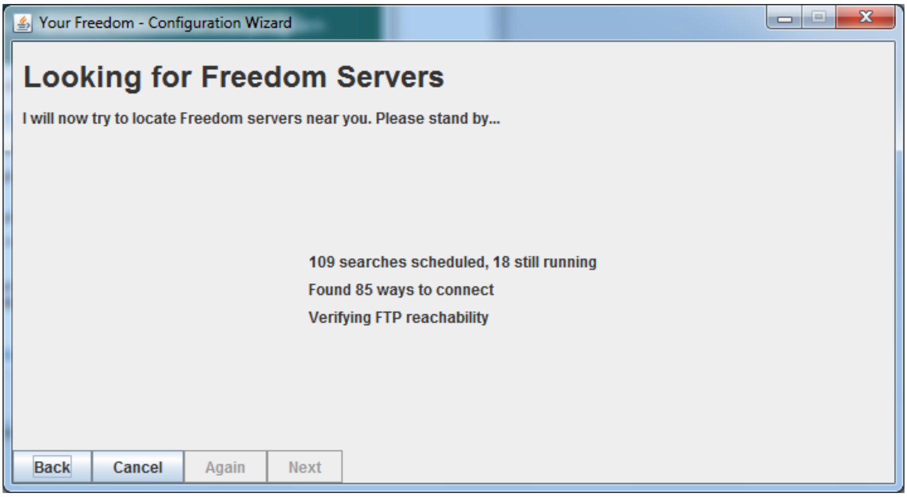


Select protocols

Choose the protocols you would like to try. If you are unsure, try them all. This is useful if you would like to avoid a protocol because you already know that it doesn't work.

☑ HTTPS
☑ Try non-HTTPS ports (no proxy)
☑ HTTP
☑ FTP
☑ UDP
□ CGI relays

In the Select Protocols dialog you should keep the default values and proceed by clicking Next.



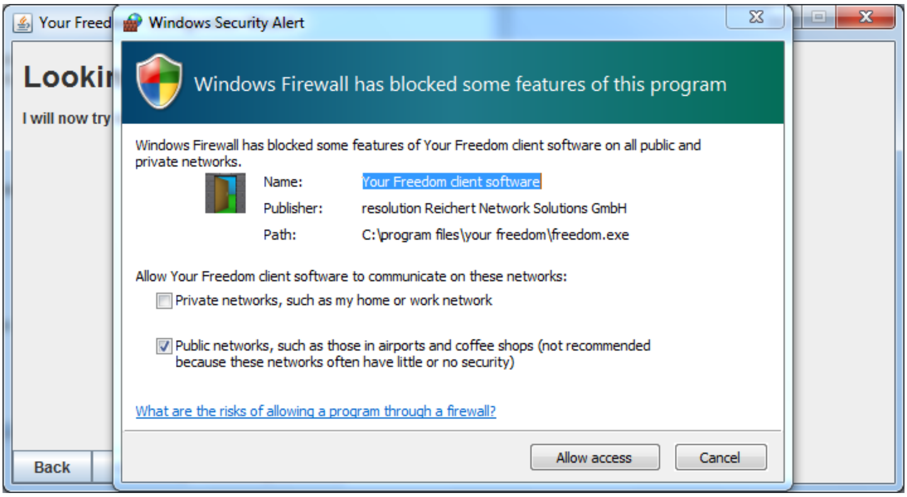
Looking for Freedom Servers

I will now try to locate Freedom servers near you. Please stand by...

109 searches scheduled, 18 still running
Found 85 ways to connect
Verifying FTP reachability

Now the Your-Freedom configuration wizard will make several tests to find available servers and check your type of connection and filtering. This may take some minutes.

You may get an warning from your firewall (here, for example the one from Windows 7). You can allow access to Your-Freedom.



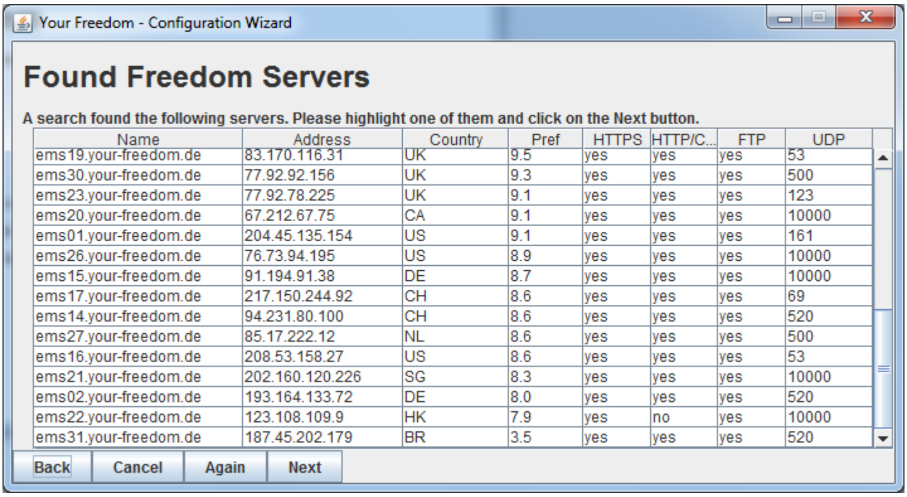
Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of Your Freedom client software on all public and private networks.

Name: Your Freedom client software
Publisher: resolution Reichert Network Solutions GmbH
Path: C:\program files\your freedom\freedom.exe

Allow Your Freedom client software to communicate on these networks:
□ Private networks, such as my home or work network
☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

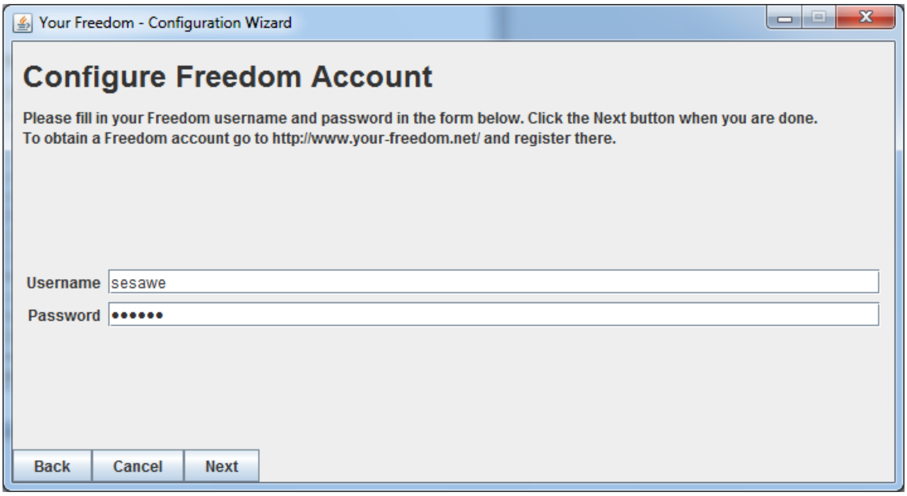


Found Freedom Servers

A search found the following servers. Please highlight one of them and click on the Next button.

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

When the wizard is ready you see the Found Freedom Servers screen where you can choose one server and click Next again.



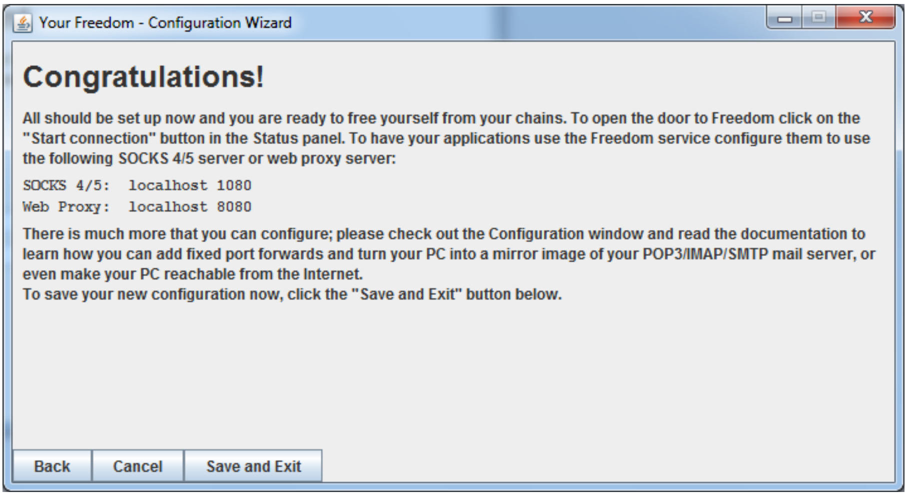
Configure Freedom Account

Please fill in your Freedom username and password in the form below. Click the Next button when you are done.
To obtain a Freedom account go to http://www.your-freedom.net/ and register there.

Username sesawe
Password ••••••

Now enter your previously created account information. If you don't have one, you can get a free access by sending a request to the email address: english@sesawe.net

Click Next.



Congratulations!

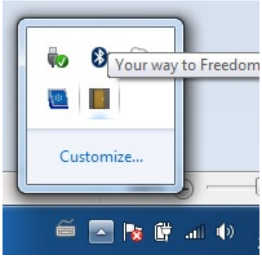
All should be set up now and you are ready to free yourself from your chains. To open the door to Freedom click on the "Start connection" button in the Status panel. To have your applications use the Freedom service configure them to use the following SOCKS 4/5 server or web proxy server:

```
SOCKS 4/5:  localhost 1080
Web Proxy:  localhost 8080
```

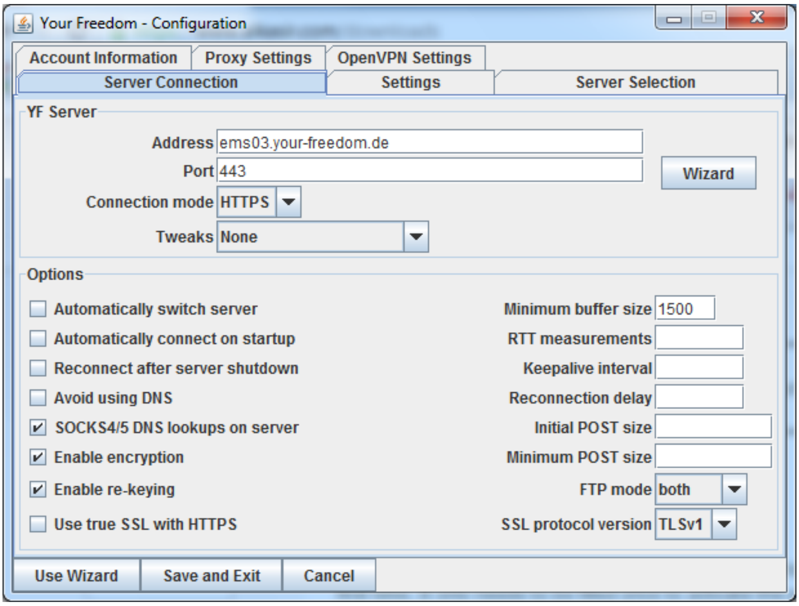
There is much more that you can configure; please check out the Configuration window and read the documentation to learn how you can add fixed port forwards and turn your PC into a mirror image of your POP3/IMAP/SMTP mail server, or even make your PC reachable from the Internet.
To save your new configuration now, click the "Save and Exit" button below.

When you see the "Congratulations!" screen, the configuration wizard is ready. Click on Save and Exit.

Your-Freedom is now running on your computer, and you can see an icon in your task bar.



For additional security and better ways to bypass filters you should tweak the options by clicking on Configure in the main Your-Freedom window and selecting the options shown in the screenshot below. Then click Save and Exit.



YF Server

Address ems03.your-freedom.de

Port 443

Connection mode HTTPS

Tweaks None

Options

- □ Automatically switch server
- □ Automatically connect on startup
- □ Reconnect after server shutdown
- □ Avoid using DNS
- ☑ SOCKS4/5 DNS lookups on server
- ☑ Enable encryption
- ☑ Enable re-keying
- □ Use true SSL with HTTPS

Minimum buffer size 1500

RTT measurements

Keepalive interval

Reconnection delay

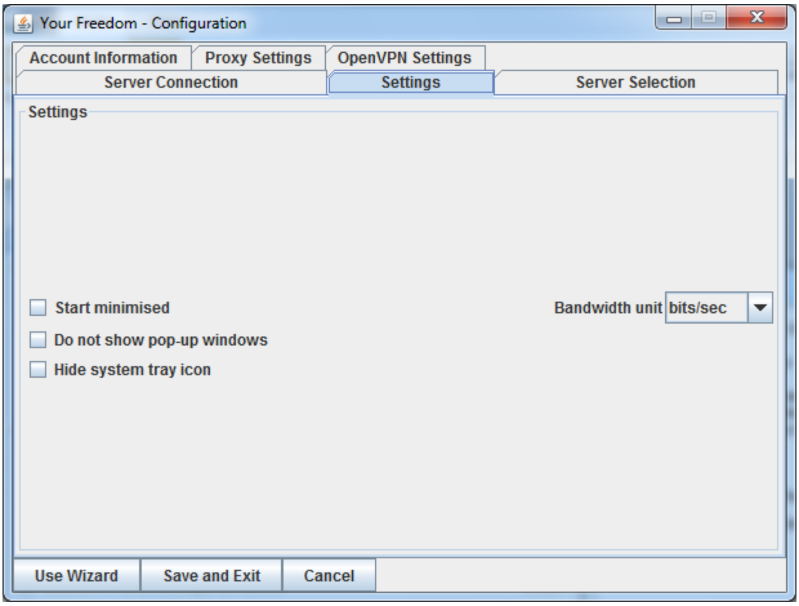
Initial POST size

Minimum POST size

FTP mode both

SSL protocol version TLSv1

Now Your-Freedom is connected to a server and provides a local proxy that you can use with your preferred software such as Internet Explorer or Firefox. To automatically configure them, click on the Application tab in the main Your-Freedom window, select which software you want to use and click OK. Your-Freedom will automatically configure that software so that it connects over the encrypted Your-Freedom tunnel to the Internet.



Settings

☐ Start minimised

☐ Do not show pop-up windows

☐ Hide system tray icon

Bandwidth unit bits/sec

To make sure you are using Your-Freedom correctly go to the https://www.your-freedom.net Web site and check the Your Footprint section on the left. If the country detected is not where you are, you are successfully using the encrypted Your-Freedom tunnel to access the Internet.

ADVANCED TECHNIQUES
27. Domains and DNS
28. HTTP Proxies
29. The Command Line
30. OpenVPN
31. SSH Tunnelling
32. SOCKS Proxies

27. DOMAINS AND DNS

If you have identified, suspect or were told that the main censorship technique on your network is based on DNS filtering and spoofing, you should consider these techniques.

USING ALTERNATIVE DOMAIN SERVERS OR NAMES

Simply speaking, a DNS server translates a human-friendly Internet address such as google.com into the IP address, such as 72.14.207.19, that identifies the specific server or servers on the Internet associated with that name. This service is most often accessed through DNS servers maintained by your Internet Service Provider (**ISP**). Simple DNS blocking is implemented by giving an incorrect or invalid response to a DNS request, in order to prevent users from locating the servers they're looking for. This method is very easy to implement on the censor side, so it is widely used. Keep in mind that often there are several censorship methods are combined, so DNS blocking may not be the only problem.

You can potentially bypass this type of blocking in two ways: by changing your computer's DNS settings to use alternative DNS servers, or by editing your hosts file.

ALTERNATIVE DNS SERVERS

You can bypass the DNS servers of your local ISP, using third-party servers to let your computer find the addresses of domains that may be blocked by the ISP's DNS servers. There are a number of free, internationally available DNS services that you can try. OpenDNS (https://www.opendns.com) provides one such service and also maintains guides on how to change the DNS server that your computer uses (https://www.opendns.com/smb/start/computer). There is also an updated list of available DNS servers from around the world at http://www.dnsserverlist.org.

Here is a list of publicly-available DNS services, via the Internet Censorship Wiki at http://en.cship.org/wiki/DNS. (Some of these services may themselves block a limited number of sites; consult the providers' sites to learn more about their policies.)

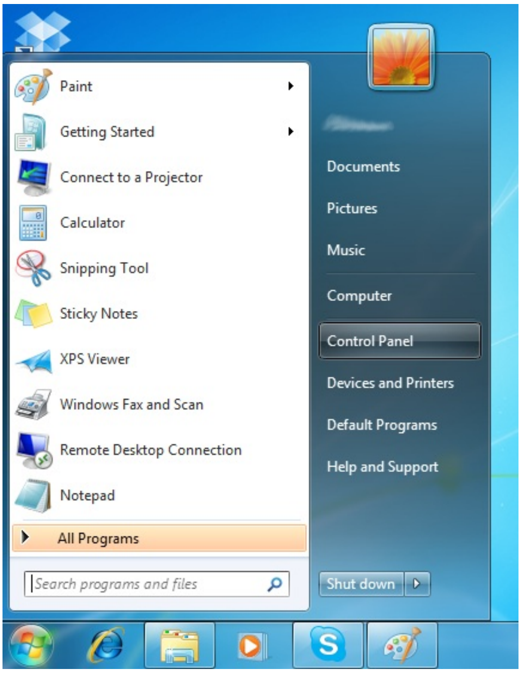
Publicly-available DNS servers

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

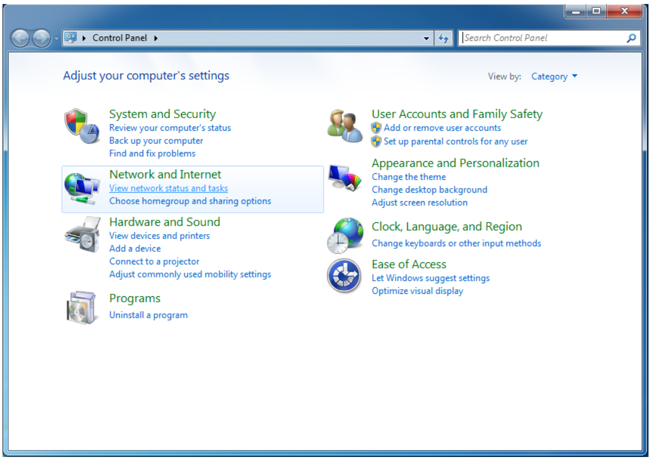
Once you've chosen a DNS server to use, you need to enter your selection into your operating system's DNS settings.

Change your DNS settings in Windows

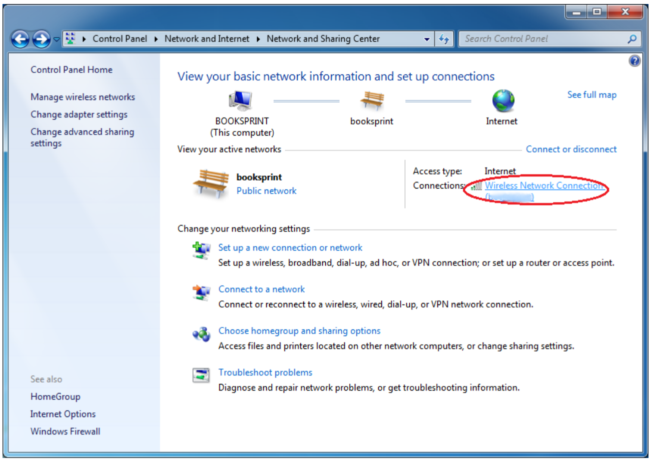
1. Open your control panel under the Start menu.



2. Under Network and Internet, click on "View network status and stats".


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Connect to a projector
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

3. Click on your wireless connection at the right side of the window.



View your basic network information and set up connections

View your active networks

booksprint
Public network

Access type: Internet
Connections: Wireless Network Connection
([redacted])

Change your networking settings

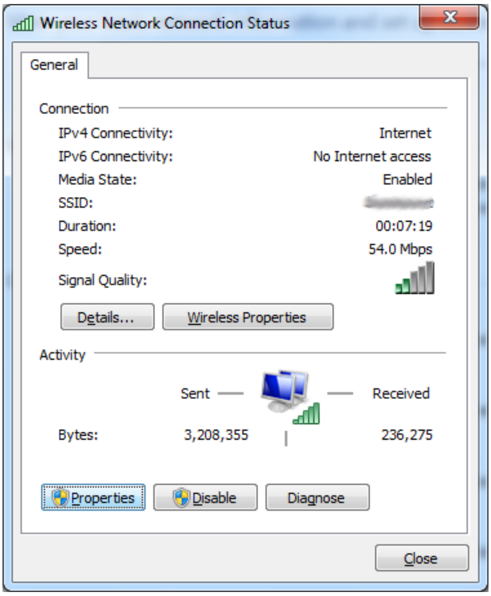
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

4. The Wireless Network Connection Status window will open. Click on Properties.



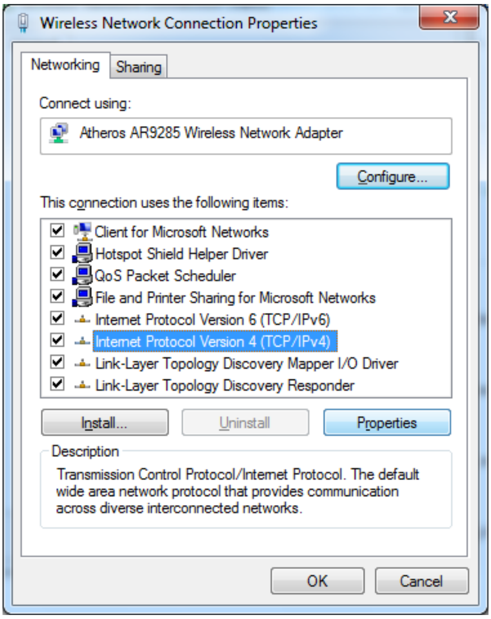
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
SSID:	[redacted]
Duration:	00:07:19
Speed:	54.0 Mbps
Signal Quality:	

Activity

	Sent	Received
Bytes:	3,208,355	236,275

5. In the Wireless Network Connection Properties window select Internet Protocol Version 4 (TCP/IPv4), and click on Properties.



Connect using:

Atheros AR9285 Wireless Network Adapter

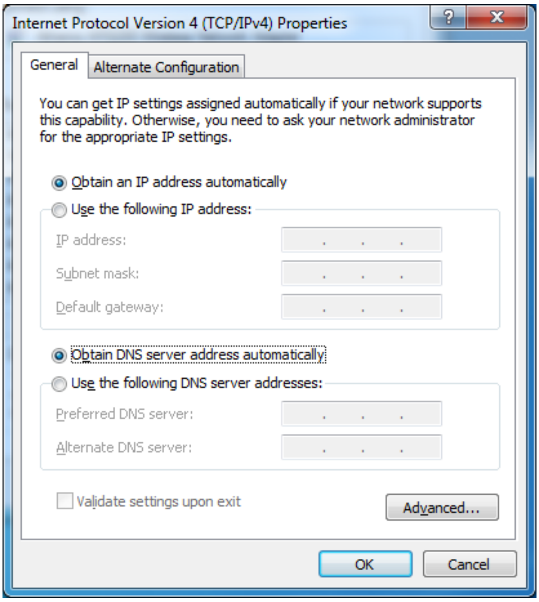
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Hotspot Shield Helper Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6. You should now be in the Internet Protocol Version 4 (TCP/IPv4) Properties window, where you are going to specify your alternate DNS address (for example: Google Public DNS)



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

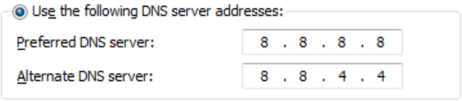
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

7. At the bottom of the window, click on "Use the following DNS server addresses" and complete the fields with your preferred and alternate DNS server IP information. When you are done, click OK. By default the first DNS server will be used. The alternate DNS server can be from another company.



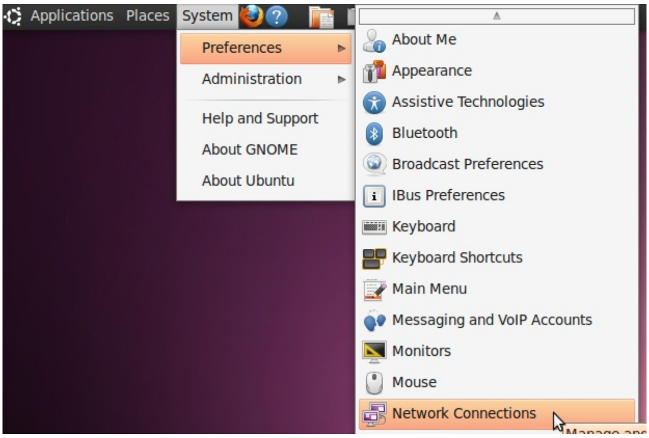
● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

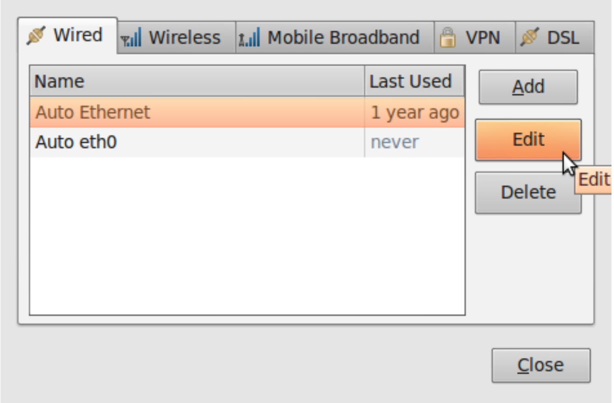
Alternate DNS server: 8 . 8 . 4 . 4

Change your DNS settings in Ubuntu

1. In the System menu go to Preferences > Network Connections.

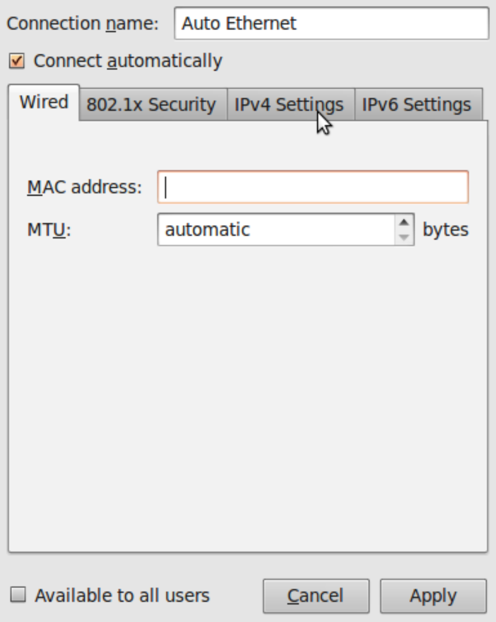


2. Select the connection for which you want to configure Google Public DNS. If you want to change the settings for an Ethernet connection (cable), select the Wired tab, then select your network interface in the list. If you want to change the settings for a wireless connection instead, select the Wireless tab, then select the appropriate wireless network.



Name	Last Used
Auto Ethernet	1 year ago
Auto eth0	never

3. Click Edit, and in the window that appears, select the IPv4 Settings tab



Connection name: Auto Ethernet

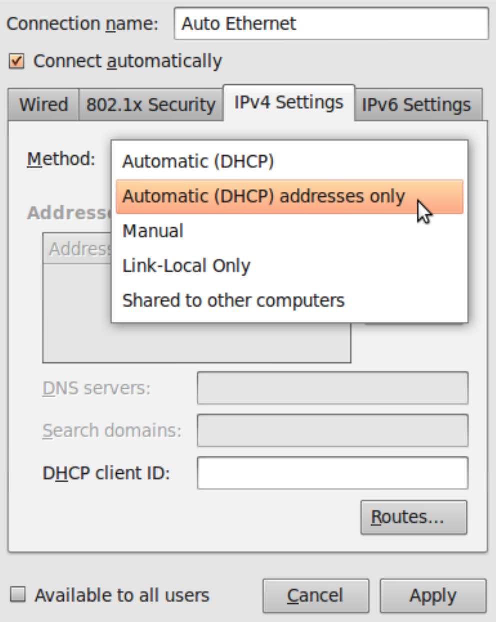
☑ Connect automatically

MAC address:

MTU: automatic bytes

☐ Available to all users

4. If the selected method is Automatic (DHCP), open the dropdown menu and select "Automatic (DHCP) addresses only" instead. If the method is set to something else, do not change it.



Connection name: Auto Ethernet

☑ Connect automatically

Method: Automatic (DHCP) addresses only

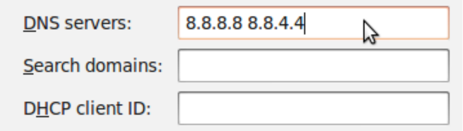
DNS servers:

Search domains:

DHCP client ID:

☐ Available to all users

5. In the DNS servers field, enter your alternate DNS IP information, separated by a space. For example, if you want to add Google DNS write: 8.8.8.8 8.8.4.4

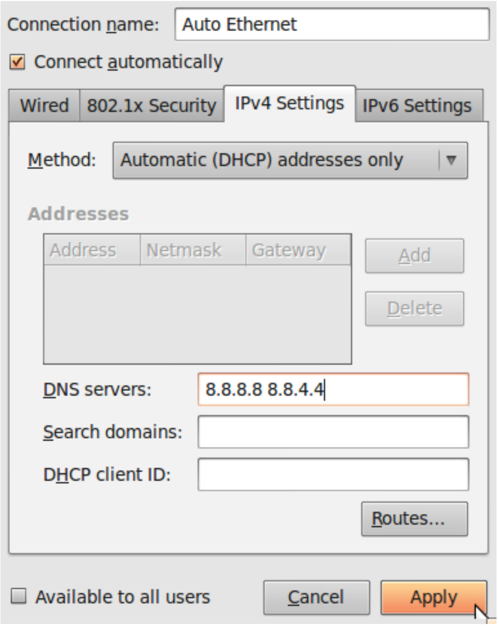


DNS servers: 8.8.8.8 8.8.4.4

Search domains:

DHCP client ID:

6. Click Apply to save the changes. If you are prompted for a password or confirmation, type the password or confirm that you want to make the changes.



Connection name: Auto Ethernet

☑ Connect automatically

Method: Automatic (DHCP) addresses only

DNS servers: 8.8.8.8 8.8.4.4

□ Available to all users

7. Repeat steps 1-6 for every network connection you want to modify.

EDIT YOUR HOSTS FILE

If you know the IP address of one particular web site or other Internet service that is blocked by your ISP's DNS servers, you can list this site in your own computer's hosts file, which is a local list of name-to-IP address equivalents that your computer will use before checking external DNS servers. The hosts file is a text file with an extremely simple format; its contents look like:

```
208.80.152.134 secure.wikimedia.org
```

where each line contains an IP address, then a space, and then a name. You can add any number of sites to your hosts file (but note that if you use the wrong address for a site, it could prevent you from accessing that site by name until you fix it or remove it from the list).

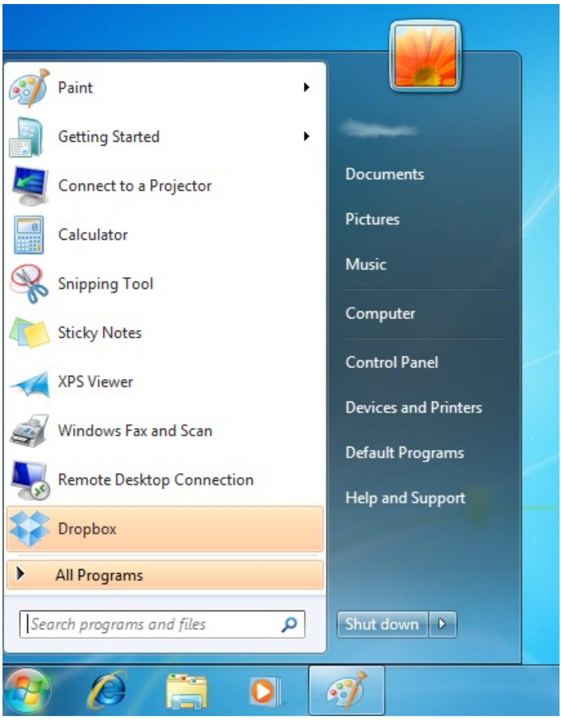
If you can't find a site's IP address because of your ISP's DNS blocking, there are hundreds of services that will help you do an uncensored DNS lookup. For example, you could use any of the tools at http://www.dnsstuff.com/tools.

You could also consider using the tools at http://www.traceroute.org, which are sophisticated network diagnostic tools provided by various ISPs. They were originally intended for diagnosing accidental network outages rather than intentional censorship, but they can be useful for diagnosing censorship too. These tools also include the ability to look up the IP address of a particular server.

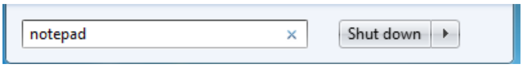
Edit your hosts file in Windows Vista / 7

You will need to use a simple text editor, such as Notepad, to edit your hosts file. In Windows Vista and 7, your hosts file is usually located at C:\Windows\system32\drivers\etc\hosts.

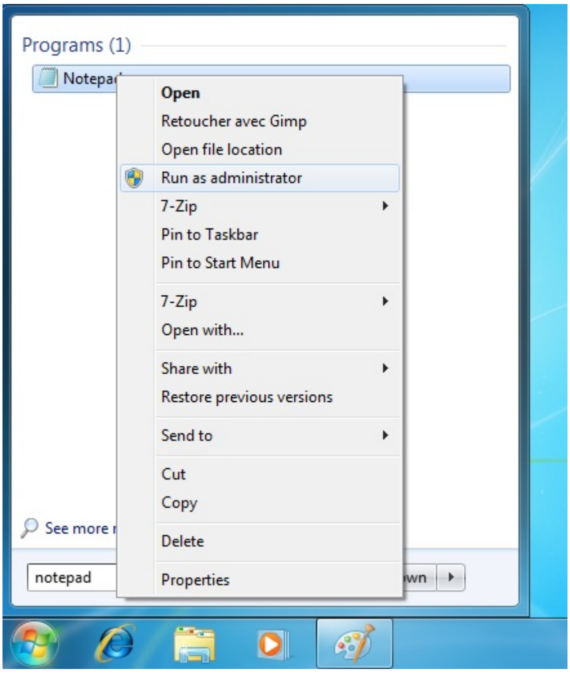
1. Click on the Start button.



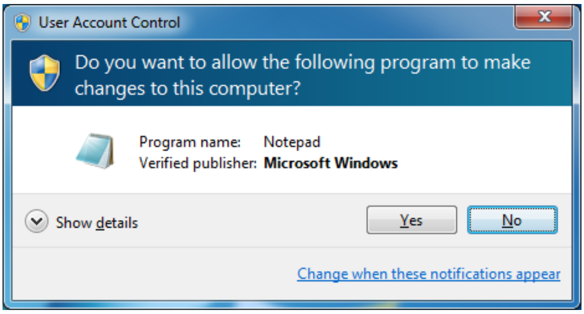
2. Type "notepad" at the search box.


notepad

3. Once you found the program, right-click on it and select "Run as administrator"


notepad

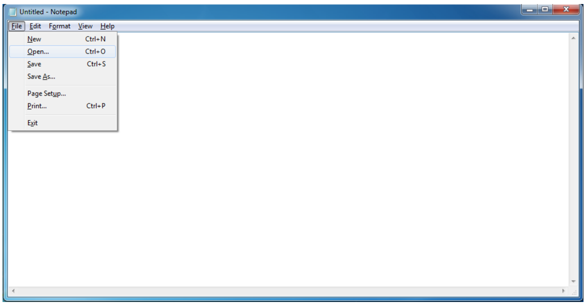
4. Windows will ask for your permission to make changes to files. Click Yes.


User Account Control

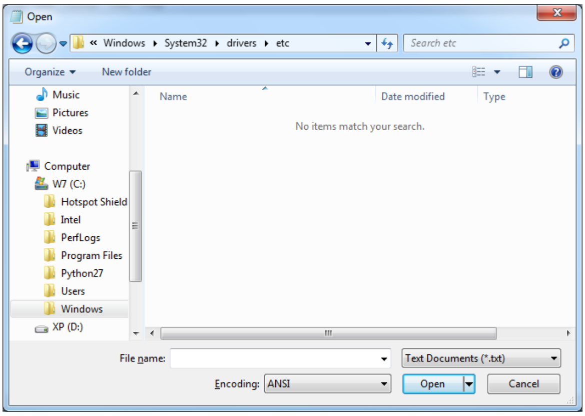
Do you want to allow the following program to make changes to this computer?

Program name: Notepad
Verified publisher: **Microsoft Windows**

5. Under the File menu, select Open.



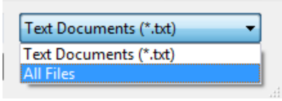
6. Browse to C:\Windows\System32\Drivers\etc\. You may notice that the folder seems initially empty.


« Windows ▸ System32 ▸ drivers ▸ etc

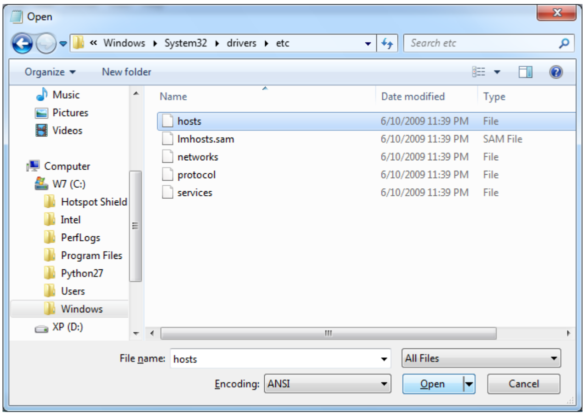
No items match your search.

File name:
Text Documents (*.txt)
Encoding: ANSI

7. At the bottom right of the open dialog, select All Files.



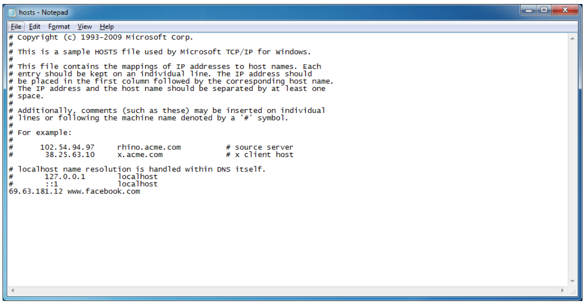
8. Select the file "hosts" and click Open.



Name	Date modified	Type
hosts	6/10/2009 11:39 PM	File
lmhosts.sam	6/10/2009 11:39 PM	SAM File
networks	6/10/2009 11:39 PM	File
protocol	6/10/2009 11:39 PM	File
services	6/10/2009 11:39 PM	File

File name: hosts
All Files
Encoding: ANSI

9. Add for example the line "69.63.181.12 www.facebook.com" at the end of the file and save it by pressing Ctrl+S or by selecting File > Save from the menu.



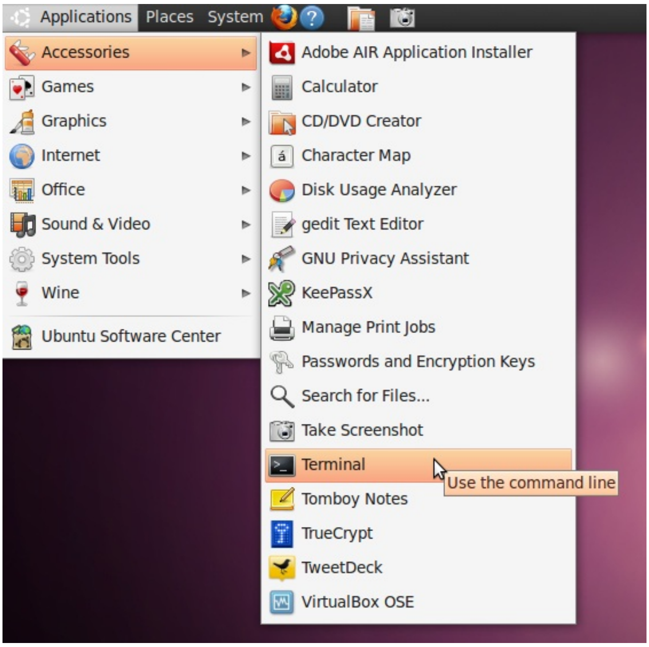
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
69.63.181.12 www.facebook.com
```

Edit your hosts file in Ubuntu

In Ubuntu, your hosts file is located in /etc/hosts. To edit it, you will need to have some knowledge of the command line. Please refer to the chapter "The Command Line" in this book for a brief tutorial on this feature.

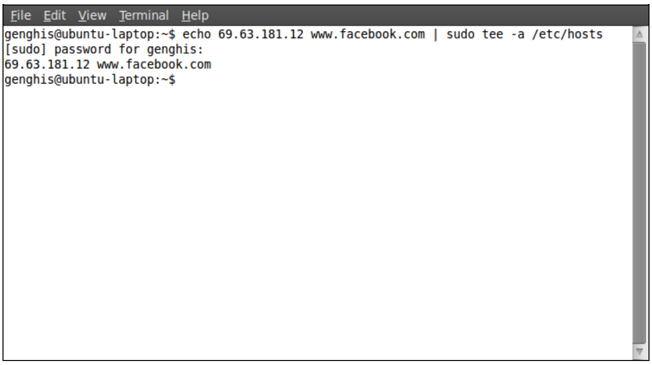
1. Open the terminal by going to Accessories > Terminal under your Applications menu.



2. Use the following command line to automatically add a line to your hosts file:

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

3. You may be prompted for your password in order to modify the file. Once authorized, the command will append "69.63.181.12 www.facebook.com" to the the last line of the hosts file.

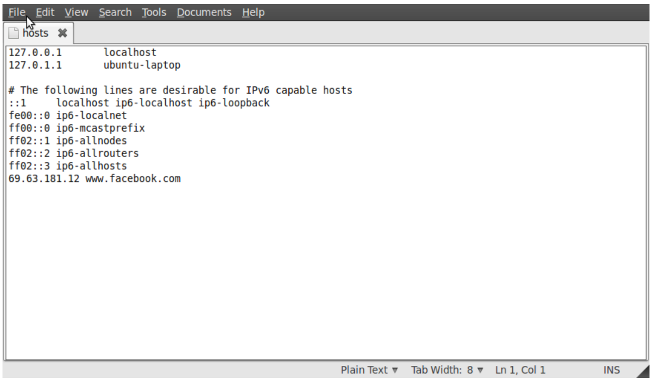


```
genghis@ubuntu-laptop:~$ echo 69.63.181.12 www.facebook.com | sudo tee -a /etc/hosts
[sudo] password for genghis:
69.63.181.12 www.facebook.com
genghis@ubuntu-laptop:~$
```

4. Optional: if you feel more comfortable working in a graphical interface, open the terminal and use the following command line to launch a text editor:

   sudo gedit /etc/hosts

5. You may be prompted for your password in order to modify the file. Once the window has opened, simply add the line "69.63.181.12 www.facebook.com" at the end of the file, and save it by pressing Ctrl+S or selecting File > Save from the menu.



```
127.0.0.1       localhost
127.0.1.1       ubuntu-laptop

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
69.63.181.12 www.facebook.com
```

28. HTTP PROXIES

Software called an *application proxy* enables one computer on the Internet to process requests from another computer. The most common kinds of application proxies are **HTTP** proxies, which handle requests for Web sites, and **SOCKS** proxies, which handle connection requests from a wide variety of applications. In this chapter we will look at HTTP proxies and how they work.

GOOD PROXIES AND BAD PROXIES

Application proxies can be used by **network operators** to censor the Internet or to monitor and control what users do. However, application proxies are also a tool for users to get around censorship and other network restrictions.

Proxies that restrict access

A network operator may force users to access the Internet (or at least Web pages) only through a certain proxy. The network operator can program this proxy to keep records of what users access and also to deny access to certain sites or services (IP blocking or port blocking). In this case, the network operator may use a *firewall* to block connections that do not go through the restrictive proxy. This configuration is sometimes called a *forced proxy*, because users are required to use it.

Proxies for circumvention

However, an application proxy can also be helpful for circumventing restrictions. If you can communicate with a computer in an unrestricted location that is running an application proxy, you can benefit from its unrestricted connectivity. Sometimes a proxy is available for the public to use; in that case, it's called an *open proxy*. Many open proxies are blocked in Internet-restricting countries if the people administering the network restrictions know about them.

WHERE TO FIND AN APPLICATION PROXY

There are many Web sites with lists of open application proxies. An overview of such sites is available at http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists.

Please note that many open application proxies only exist for a few hours, so it is important to get a proxy from a list which was very recently updated.

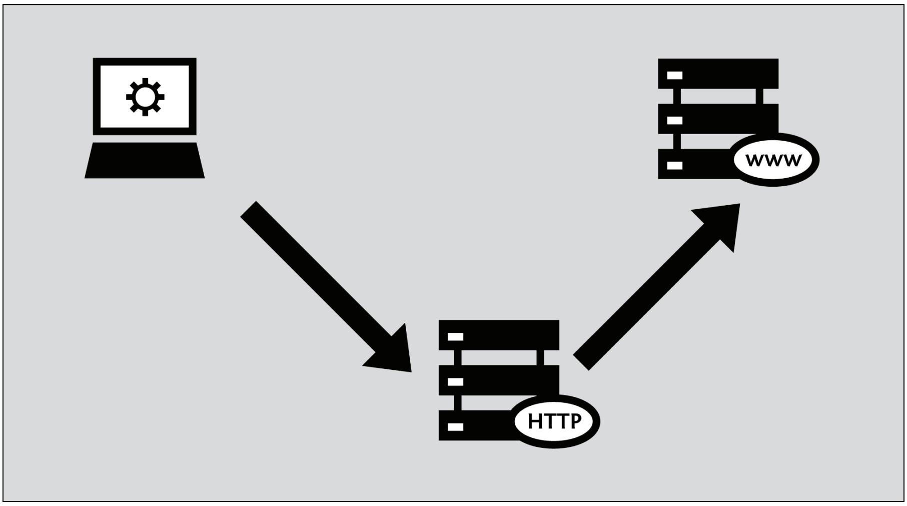
HTTP PROXY SETTINGS

To use an application proxy, you must configure the proxy settings for your operating system or within individual applications. Once you have selected a proxy in an application's proxy settings, the application tries to use that proxy for all of its Internet access.

Be sure you make note of the original settings so that you can restore them. If the proxy becomes unavailable or unreachable for some reason, the software that is set to use it generally stops working. In that case, you may need to reset to the original settings.

On Mac OS X and some Linux systems, these settings can be configured in the operating system, and will automatically be applied to applications such as the web browser or instant messaging applications. On Windows and some Linux systems, there is no central place to configure proxy settings, and each application must be configured locally. Bear in mind that, even if the proxy settings are configured centrally, there is no guarantee that applications will support these settings, so it is always a good idea to check the settings of each individual application.

Typically only Web browsers can directly use an HTTP proxy.



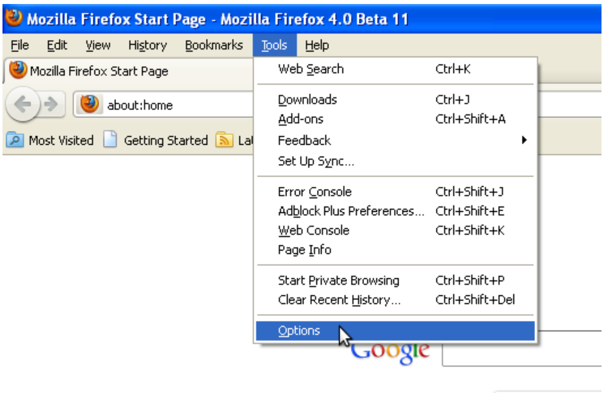
The steps below describe how to configure Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and the free and open source instant messaging client Pidgin to use a proxy. If you use Firefox for Web browsing, it may be simpler to use the FoxyProxy software; it is an alternative to the steps below. If you use Tor, it is safest to use the TorButton software (which is provided as part of the Tor Bundle download) to configure your browser to use Tor.

While e-mail clients such as Microsoft Outlook and Mozilla Thunderbird can also be configured to use HTTP proxies, actual e-mail traffic when sending and fetching e-mail uses other protocols such as POP3, IMAP and SMTP; this traffic will not pass through the HTTP proxy.

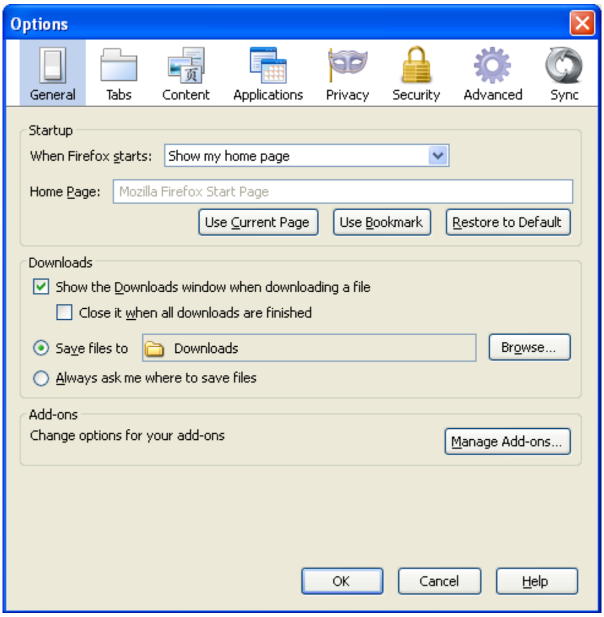
Mozilla Firefox

To configure Firefox to use an HTTP proxy:

1. Select Tools > Options:


Mozilla Firefox Start Page - Mozilla Firefox 4.0 Beta 11
File Edit View History Bookmarks Tools Help
Mozilla Firefox Start Page
about:home
Most Visited Getting Started Lat
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons Ctrl+Shift+A
Feedback
Set Up Sync...
Error Console Ctrl+Shift+J
Adblock Plus Preferences... Ctrl+Shift+E
Web Console Ctrl+Shift+K
Page Info
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Options
Google

2. The Options window appears:


Options
General Tabs Content Applications Privacy Security Advanced Sync
Use Current Page Use Bookmark Restore to Default
Browse...
Manage Add-ons...
OK Cancel Help

Startup

When Firefox starts: Show my home page

Home Page: Mozilla Firefox Start Page

Downloads

☑ Show the Downloads window when downloading a file

□ Close it when all downloads are finished

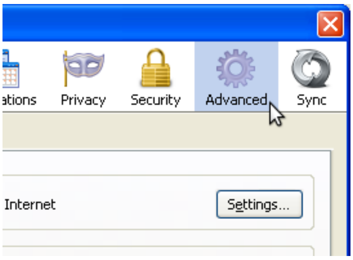
● Save files to Downloads

○ Always ask me where to save files

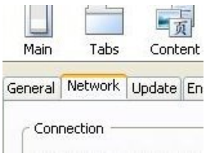
Add-ons

Change options for your add-ons

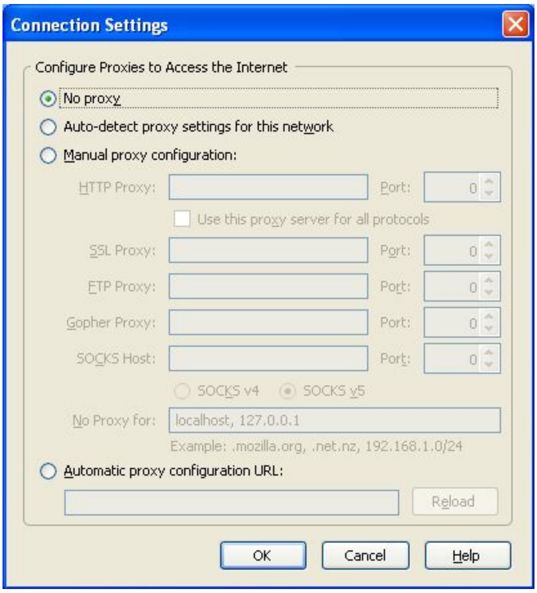
3. In the toolbar at the top of the window, click Advanced:



4. Click the Network tab:



5. Click Settings. Firefox displays the Connection Settings window:


Connection Settings

Configure Proxies to Access the Internet

● No proxy

○ Auto-detect proxy settings for this network

○ Manual proxy configuration:

HTTP Proxy: Port: 0

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

SOCKS Host: Port: 0

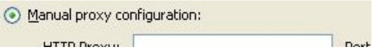
○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

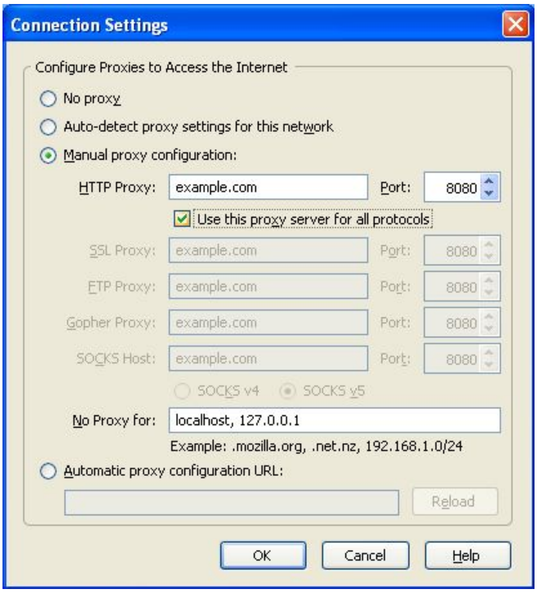
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

6. Select "Manual proxy configuration". The fields below that option become available.


● Manual proxy configuration:

7. Enter the HTTP proxy address and port number, and then click OK.


Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy: example.com Port: 8080

☑ Use this proxy server for all protocols

SSL Proxy: example.com Port: 8080

FTP Proxy: example.com Port: 8080

Gopher Proxy: example.com Port: 8080

SOCKS Host: example.com Port: 8080

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

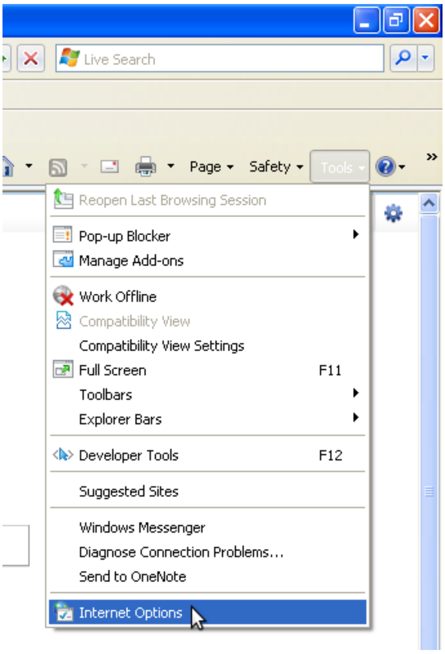
If you click "Use this proxy server for all protocols", Firefox will attempt to send HTTPS (secure HTTP) and FTP traffic through the proxy. This may not work if you are using a public application proxy, since many of these do not support HTTPS and FTP traffic. If, on the other hand your HTTPS and/or FTP traffic is being blocked, you can try to find a public application proxy with HTTPS and/or FTP support, and use the "Use this proxy server for all protocols" setting in Firefox.

Now Firefox is configured to use an HTTP proxy.

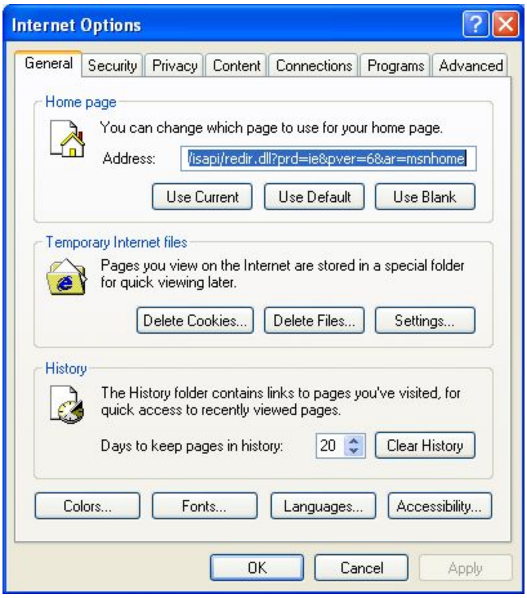
Microsoft Internet Explorer

To configure Internet Explorer to use an HTTP proxy:

1. Select Tools > Internet Options:



2. Internet Explorer displays the Internet Options window:



You can change which page to use for your home page.

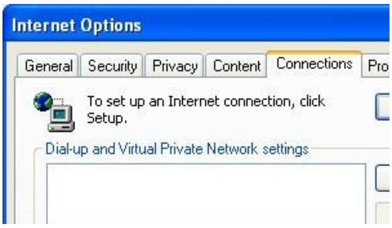
Address: /isapi/redir.dll?prd=ie&pver=6&ar=msnhome

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

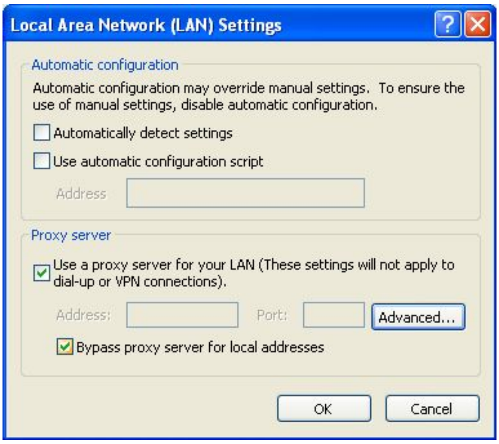
Days to keep pages in history: 20

3. Click the Connections tab.



To set up an Internet connection, click Setup.

4. Click LAN Settings. The Local Area Network (LAN) Settings window appears.



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

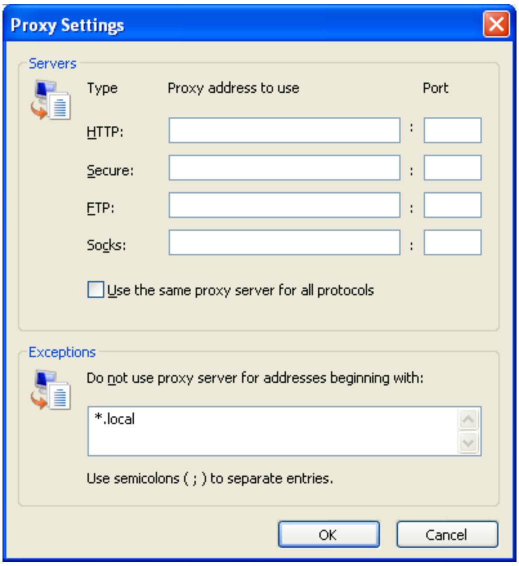
Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☑ Bypass proxy server for local addresses

5. Select "Use a proxy server for your LAN".
6. Click Advanced. The Proxy Settings window appears.



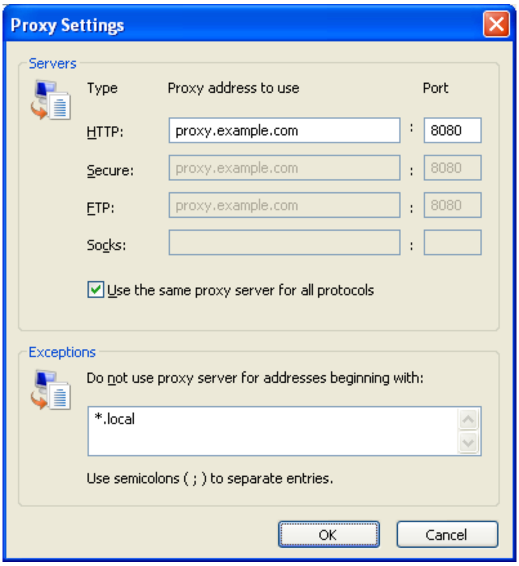
☐ Use the same proxy server for all protocols

Do not use proxy server for addresses beginning with:

*.local

Use semicolons (;) to separate entries.

7. Enter the proxy address and port number in the first row of fields.
8. If you click "Use the same proxy server for all protocols", Internet Explorer will attempt to send HTTPS (secure HTTP) and FTP traffic through the proxy. This may not work if you are using a public application proxy, since many of these do not support HTTPS and FTP traffic. If, on the other hand your HTTPS and/or FTP traffic is being blocked, you can try to find a public application proxy with HTTPS and/or FTP support, and use the "Use this proxy server for all protocols" setting in Internet Explorer.



HTTP: proxy.example.com : 8080

Secure: proxy.example.com : 8080

FTP: proxy.example.com : 8080

Socks: :

☑ Use the same proxy server for all protocols

Do not use proxy server for addresses beginning with:

*.local

Use semicolons (;) to separate entries.

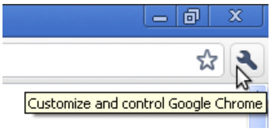
Now Internet Explorer is configured to use an HTTP proxy.

Google Chrome

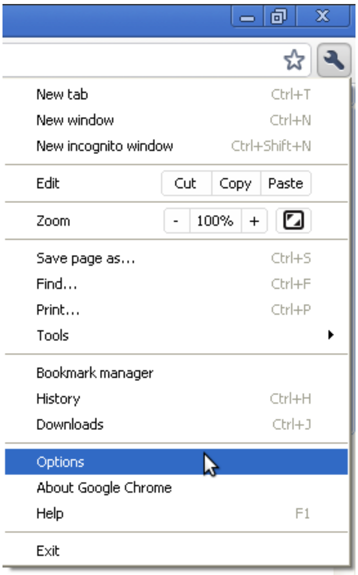
Google Chrome uses the same connection and proxy settings as the Windows operating system. Changing these settings affects Google Chrome as well as Internet Explorer and other Windows programs. If you configured your HTTP proxy through Internet Explorer then you don't need to take this steps to configure Chrome.

Follow these steps to configure your HTTP proxy:

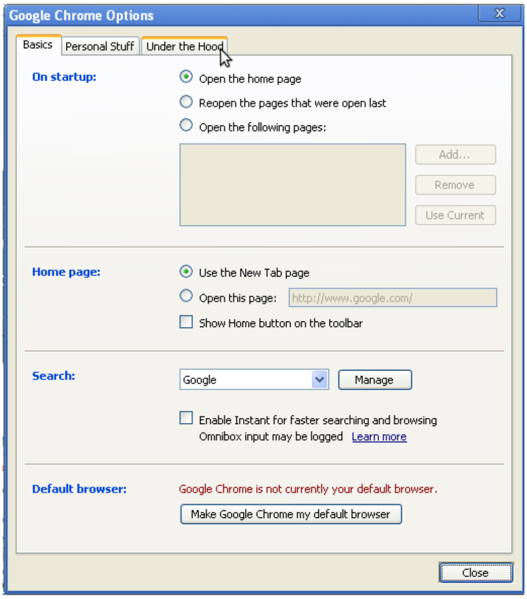
1. Click on the "Customize and control Google Chrome" menu (the little wrench next to the URL address bar):



2. Click on Options:



3. In the Google Chrome Options window, select the Under the Hood tab:



On startup:
● Open the home page
○ Reopen the pages that were open last
○ Open the following pages:

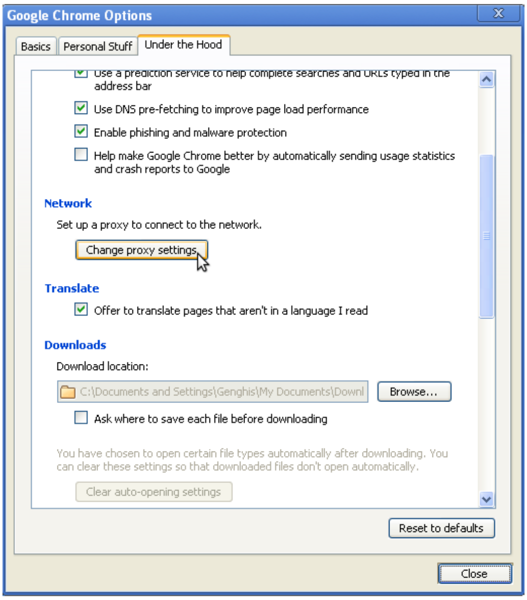
Home page:
● Use the New Tab page
○ Open this page: http://www.google.com/
□ Show Home button on the toolbar

Search: Google

□ Enable Instant for faster searching and browsing
Omnibox input may be logged Learn more

Default browser: Google Chrome is not currently your default browser.

4. In the Network section, click the "Change proxy settings" button:



☑ Use a prediction service to help complete searches and URLs typed in the address bar

☑ Use DNS pre-fetching to improve page load performance

☑ Enable phishing and malware protection

☐ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google

Network

Set up a proxy to connect to the network.

Translate

☑ Offer to translate pages that aren't in a language I read

Downloads

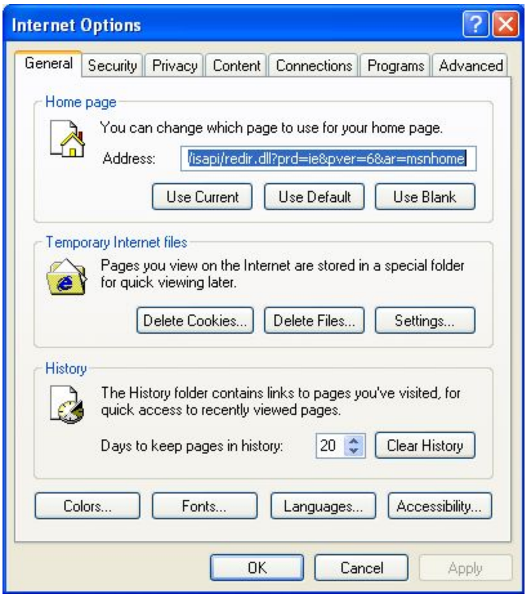
Download location:

C:\Documents and Settings\Genghis\My Documents\Downl

☐ Ask where to save each file before downloading

You have chosen to open certain file types automatically after downloading. You can clear these settings so that downloaded files don't open automatically.

5. The Internet Options window will open. Follow steps 2-8 from "How to configure the HTTP Proxy under Internet Explorer" (above) to finish setting up your HTTP proxy.



Home page

You can change which page to use for your home page.

Address: /isapi/redir.dll?prd=ie&pver=6&ar=msnhome

Temporary Internet files

Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

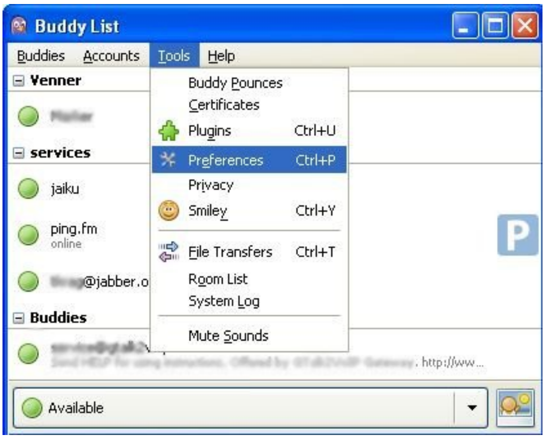
Days to keep pages in history: 20

Chrome is now configured to use HTTP proxy.

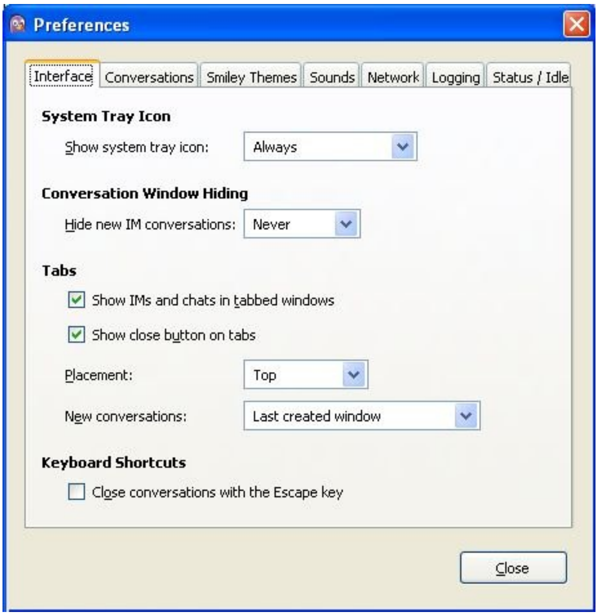
Pidgin instant messaging client

Some Internet applications other than Web browsers can also use a HTTP proxy to connect to the Internet, potentially bypassing blocking. Here is an example with the instant messaging software Pidgin.

1. Select Tools > Preferences:



Pidgin displays the Preferences window:



System Tray Icon

Show system tray icon: Always

Conversation Window Hiding

Hide new IM conversations: Never

Tabs

☑ Show IMs and chats in tabbed windows

☑ Show close button on tabs

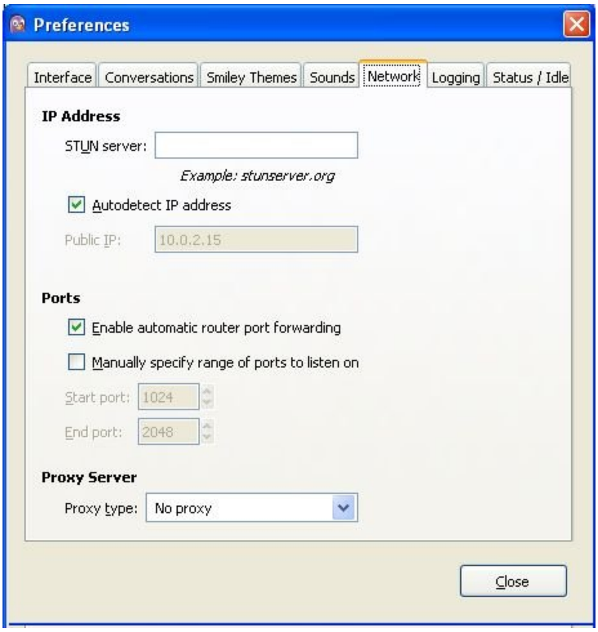
Placement: Top

New conversations: Last created window

Keyboard Shortcuts

☐ Close conversations with the Escape key

2. Click the Network tab:



IP Address

STUN server:

Example: stunserver.org

☑ Autodetect IP address

Public IP: 10.0.2.15

Ports

☑ Enable automatic router port forwarding

□ Manually specify range of ports to listen on

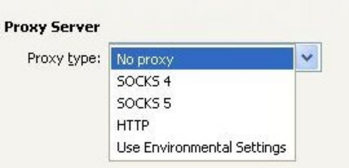
Start port: 1024

End port: 2048

Proxy Server

Proxy type: No proxy

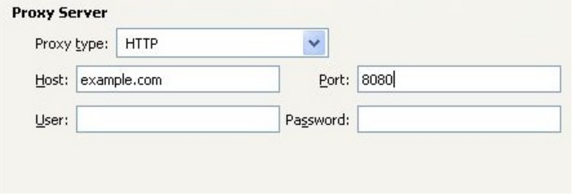
3. For Proxy type, select HTTP. Additional fields appear under that option.



Proxy Server

Proxy type: No proxy

4. Enter the Host address and port number of your HTTP proxy.



Proxy Server

Proxy type: HTTP

Host: example.com

Port: 8080

User:

Password:

5. Click Close.

Pidgin is now configured to use the HTTP proxy.

When you're done with the proxy

When you are done using a proxy, particularly on a shared computer, return the settings you've changed to their previous values. Otherwise, those applications will continue to try to use the proxy. This could be a problem if you don't want people to know that you were using the proxy or if you were using a local proxy provided by a particular circumvention application that isn't running all the time.

29. THE COMMAND LINE

Modern computing is highly interactive, and using the command line is just another form of interaction. Most people use the computer through its desktop or graphical interface, interacting at a rapid pace. They click on an object, drag and drop it, double-click another to open it, alter it, and so on.

Although interactions happen so fast you don't think about it, each click or keystroke is a command to the computer, which it reacts to. Using the command line is the same thing, but more deliberate. You type a command and press the Return or Enter key. For instance, in my terminal I type:

```
date
```

And the computer replies with:

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

That's pretty computerish. In later chapters we'll explain how to request the date and time in a more congenial format. We'll also explain how working in different countries and with different languages changes the output. The idea for now is that you've just had an interaction.

THE COMMAND LINE CAN DO MUCH BETTER

The *date* command, as seen so far, compares poorly with the alternative of glancing at a calendar or clock. The main problem is not the unappetizing appearance of the output, mentioned already, but the inability to do anything of value with the output. For instance, if I'm looking at the date in order to insert it into a document I'm writing or update an event on my online calendar, I have to do some retyping. The command line can do much better than this.

After you learn basic commands and some useful ways to save yourself time, you'll find out more in this book about feeding the output of commands into other commands, automating activities, and saving commands for later use.

WHAT DO WE MEAN BY A COMMAND?

At the beginning of this chapter we used the word *command* very generally to refer to any way of telling the computer what to do. But in the context of this book, a command has a very specific meaning. It's a file on your computer that can be executed, or in some cases an action that is built into the shell program. Except for the *built-in commands*, the computer runs each command by finding the file that bears its name and executing that file. We'll give you more details as they become useful.

WAYS TO ENTER COMMANDS

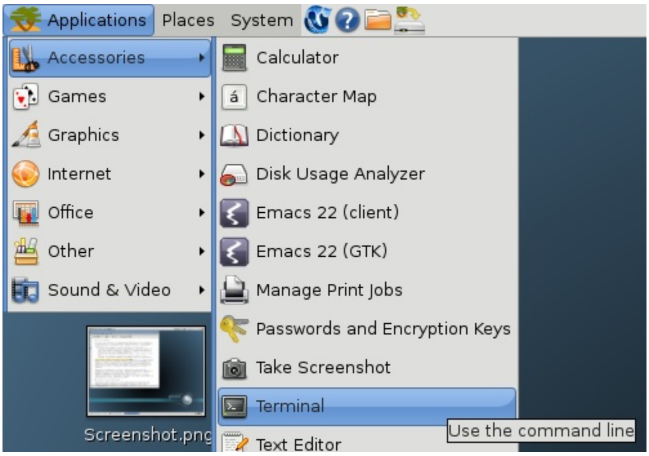
To follow along on this book, you need to open a command-line interpreter or **command-line interface** (called a **shell** or terminal in GNU/Linux) on your computer. Pre-graphical computer screens presented people with this interpreter as soon as they logged in. Nowadays almost everybody except professional system administrators uses a graphical interface, although the pre-graphical one is still easier and quicker to use for many purposes. So we'll show you how to pull up a shell.

FINDING A TERMINAL

You can get a terminal interface from the desktop, but it may be easier to leave the desktop and use the original text-only terminal. To do that, use the < ctrl + alt + F1 > key combination. You get a nearly blank screen with an invitation to log in. Give it your username and password. You can go to other terminals with < alt + F2 > and so on, and set up sessions with different (or the same) users for whatever tasks you want to do. At any time, switch from one to another by using the < alt + F# > keystroke for the one you want. One of these, probably F7 or F8, will get you back to the desktop. In text terminals you can use the mouse (assuming your system has gpm running) to select a word, line or range of lines. You can then paste that text somewhere else in that or any other terminal.

GNU/Linux distributions come with different graphical user interfaces (GUI) offering different aesthetics and semantic metaphors. Those running on top of the operating system are known as *desktop environments*. GNOME, KDE and Xfce are among the most widely used. Virtually every desktop environment provides a program that mimics the old text-only terminals that computers used to offer as interfaces. On your desktop, try looking through the menus of applications for a program called Terminal. Often it's on a menu named something such as Accessories, which is not really appropriate because once you read this book you'll be spending a lot of time in the terminal every day.

In GNOME you select Applications > Accessories > Terminal.



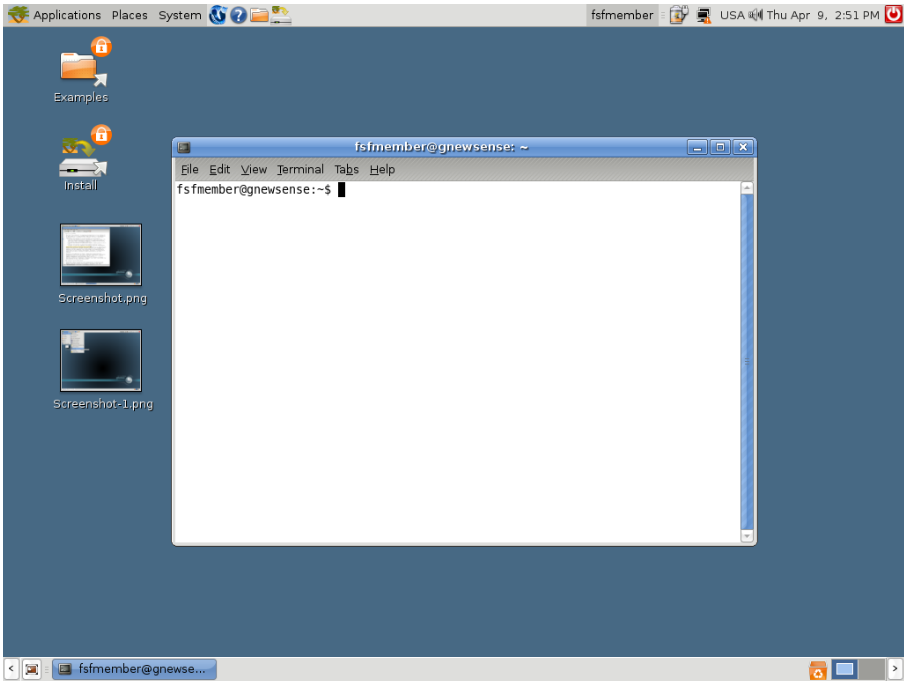
In KDE, select K Menu -> System -> Terminal.

In Xfce, select Xfce Menu -> System -> Terminal.

Wherever it's located, you can almost certainly find a terminal program.

When you run the terminal program, it just shows a blank window; there's not much in the way of help. You're expected to know what to do – and we'll show you.

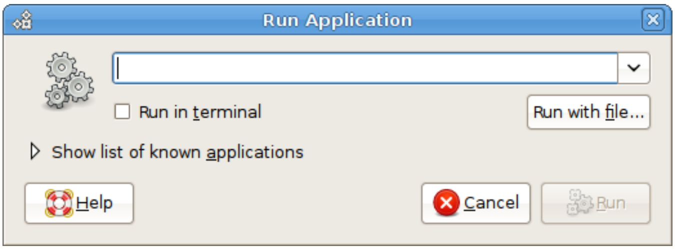
The following figure shows the Terminal window opened on the desktop in GNOME.



```
fsfmember@gnewsense:~$
```

RUNNING AN INDIVIDUAL COMMAND

Many graphical interfaces also provide a small dialog box called something like "Run command". It presents a small text area where you can type in a command and press the Return or Enter key.



To invoke this dialog box, try typing the < alt + F2 > key combination, or searching through the menus of applications. You can use this box as a shortcut to quickly start up a terminal program, as long as you know the name of a terminal program installed on your computer. If you are working on an unfamiliar computer and don't know the name of the default terminal program, try typing `xterm` to start up a no-frills terminal program (no fancy menus allowing choice of color themes or fonts). If you desperately need these fancy menus,

- in GNOME the default terminal program should be `gnome-terminal`
- in KDE it should be `konsole`
- in Xfce try `Terminal` or version specific terminal names, for example in Xfce 4 you should find `xfce4-terminal`.

HOW WE SHOW COMMANDS AND OUTPUT IN THIS CHAPTER

There's a common convention in books about the command line. When you start up a terminal, you see a little message indicating that the terminal is ready to accept your command. This message is called a *prompt*, and it may be as simple as:

```
$
```

After you type your command and press the Return or Enter key, the terminal displays the command's output (if there is any) followed by another prompt. So my earlier interaction would be shown in the book like this:

```
$ date
Thu Mar 12 17:15:09 EDT 2009
$
```

You have to know how to interpret examples like the preceding one. All you type here is *date*. Then press the Return key. The word *date* in the example is printed in bold to indicate that it's something you type. The rest is output on the terminal.

30. OPENVPN

OpenVPN is a well-respected, free, open source Virtual Private Network (**VPN**) solution. It works on most versions of Windows (Windows Vista support is expected soon), Mac OS X and Linux. OpenVPN is **SSL**-based, which means it uses the same type of **encryption** that is used when visiting secure Web sites where the URL starts with https.

GENERAL INFORMATION

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 is not suitable for temporary use in Internet cafés or elsewhere on shared computers where you can't install additional software.

For a more general presentation of VPNs and ready-to-use VPN services, read the "VPN Services" chapter in this manual.

In an OpenVPN system, there is one computer set up as a server (in an unrestricted location), and one or more clients. The server must be set up to be accessible from the Internet, not blocked by a firewall and with a *publicly routable IP address* (in some places, the person establishing the server may have to request this from their ISP). Each client connects to the server and creates a VPN **tunnel** through which traffic from the client can pass.

There are commercial OpenVPN providers such as WiTopia (http://witopia.net/personalmore.html) where you can purchase access to an OpenVPN server for a fee of about 5-10 US dollars a month. These providers will also help you install and configure OpenVPN on your computer. A list of such commercial providers is available at http://en.cship.org/wiki/VPN.

OpenVPN also can be used by a trusted contact in an unfiltered location, providing an OpenVPN server to one or more clients and passing their traffic to his/her computer before continuing on to the Internet. Setting this up correctly is somewhat complicated, however.

TIPS FOR SETTING UP OPENVPN

To setup your own OpenVPN server and client, follow the documentation provided by OpenVPN (http://openvpn.net/index.php/documentation/howto.html). If you want to use OpenVPN to visit blocked Web sites, the following notes are important:

Client

There is a graphical user interface (GUI) available for Windows which will make it easy to start and stop OpenVPN as required, and also enables you to configure OpenVPN to use an HTTP proxy to get onto the Internet. To download the GUI go to http://openvpn.se.

To configure OpenVPN to use a proxy server in Linux or Mac OS X, read the relevant section on the Web site (http://openvpn.net/index.php/documentation/howto.html#http).

Server

- When choosing between routing and bridging, there is no additional advantage in configuring bridging when your clients just want to use it to bypass Internet censorship. Choose routing.
- Pay special attention to the section of the guide that explains how to ensure that all traffic from the client is passed through the server. Without this configuration the system will not help you to visit blocked Web pages (http://openvpn.net/index.php/documentation/howto.html#redirect).
- If the client computer is behind a very restrictive firewall, and the default OpenVPN port is blocked, it is possible to change the port that OpenVPN uses. One option is to use port 443, which is normally used for secure websites (**HTTPS**), and to switch to **TCP** protocol instead of **UDP**. In this configuration, it is difficult for firewall operators to differentiate between OpenVPN traffic and normal secure Web traffic. To do this, near the top of the configuration files on both the client and server, replace "proto udp" with "proto tcp" and "port 1194" with "port 443".

ADVANTAGES AND RISKS

Once it is set up and configured correctly, OpenVPN can provide an effective way to bypass Internet filters. Since all traffic is encrypted between the client and the server, and can pass through a single port, it is very difficult to distinguish from any other secure Web traffic, such as data going to an online shopping site or other encrypted services.

OpenVPN can be used for all Internet traffic, including Web traffic, e-mail, instant messaging and **VoIP**.

OpenVPN also provides a degree of protection against surveillance, as long as you can trust the owner of the OpenVPN server, and you have followed the instructions in the OpenVPN documentation on how to handle the certificates and keys used. Remember that traffic is only encrypted as far as the OpenVPN server, after which it passes unencrypted onto the Internet.

The primary disadvantage of OpenVPN is the difficulty of installation and configuration. It also requires access to a server in an unrestricted location. OpenVPN also does not reliably provide anonymity.

31. SSH TUNNELLING

SSH, the Secure Shell, is a standard protocol that encrypts communications between your computer and a server. The encryption prevents these communications from being viewed or modified by network operators. SSH can be used for a wide variety of secure communications applications, where secure log-in to a server and secure file transfers (scp or SFTP) are the most common.

SSH is especially useful for censorship circumvention because it can provide encrypted tunnels and work as a generic proxy client. Censors may be reluctant to block SSH entirely because it is used for many purposes other than circumventing censorship; for example, it is used by system administrators to administer their servers over the Internet.

Using SSH requires an account on a server machine, generally a Unix or Linux server. For censorship circumvention, this server needs to have unrestricted Internet access and, ideally, is operated by a trusted contact. Some companies also sell accounts on their servers, and many Web hosting plans provide SSH access. There is a list of shell account providers at: http://www.google.com/Top/Computers/Internet/Access_Providers/Unix_Shell_Providers which sell accounts for about 2-10 US dollars a month.

An SSH program called OpenSSH is already installed on most Unix, Linux, and Mac OS computers as a command-line program run from a terminal as "ssh". For Windows, you can also get a free SSH implementation called PuTTY.

All recent versions of SSH support creating a **SOCKS** proxy that allows a Web browser and a wide variety of other software to use the encrypted SSH connection to communicate with the unfiltered Internet. In this example, we will describe only this use of SSH. The steps below will set up a SOCKS proxy on local port 1080 of your computer.

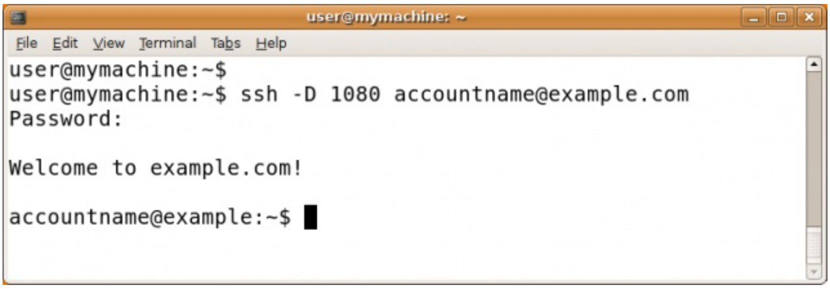
LINUX/UNIX AND MACOS COMMAND LINE (WITH OPENSSH)

OpenSSH is available from http://www.openssh.com/, but it comes pre-installed on Linux/Unix and Mac OS computers.

The ssh command you'll run contains a local port number (typically 1080), a server name, and a username (account name). It looks like this:

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

For example:



```
user@mymachine:~$
user@mymachine:~$ ssh -D 1080 accountname@example.com
Password:

Welcome to example.com!

accountname@example:~$
```

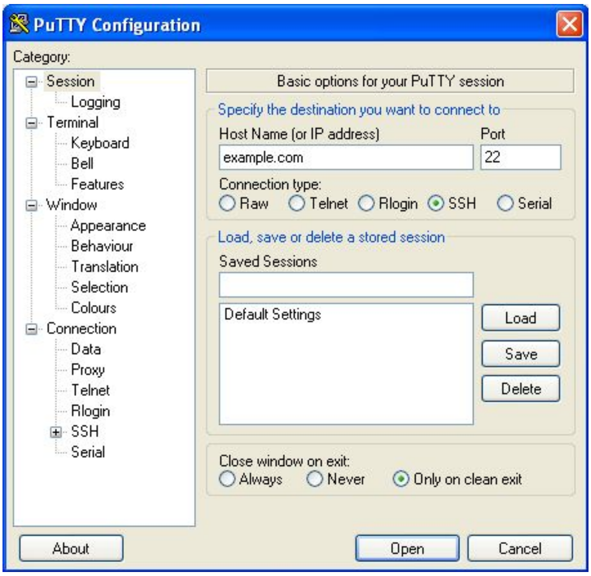
You'll be prompted for your password and then you'll be logged into the server. With the use of the -D option, a local SOCKS proxy will be created and will exist as long as you're connected to the server. Important: you should now verify the host key and configure your applications, otherwise you are not using the tunnel you have created!

WINDOWS GRAPHICAL USER INTERFACE (WITH PUTTY)

PuTTY is available from : http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

You can save the putty.exe program on your hard drive for future use, or run it directly from the Web site (often, this is possible on a shared or public-access computer, such as a computer in a library or Internet café).

When you start PuTTY, a session configuration dialog appears. First enter the host name (address) of the SSH server you are going to connect to (here, example.com). If you only know the IP address or if DNS blocking is preventing you from using the host name, you can use the IP address instead. If you will perform these steps frequently, you can create a PuTTY profile that saves these options as well as the options described below so they will be used every time.



Host Name (or IP address): example.com

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

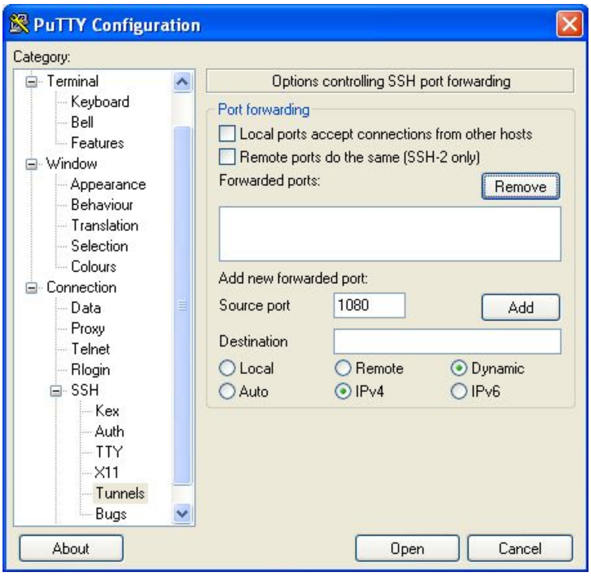
Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Next, in the Category list, select Connection > SSH > Tunnels.

Enter 1080 for the Source port, and check the Dynamic and IPv4 boxes.



□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH-2 only)

Forwarded ports:

Add new forwarded port:

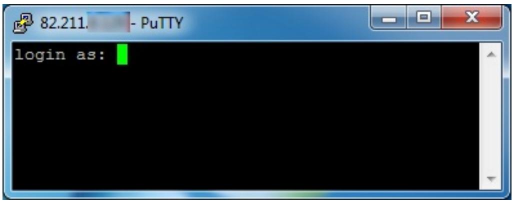
Source port: 1080

Destination:

○ Local ○ Remote ● Dynamic

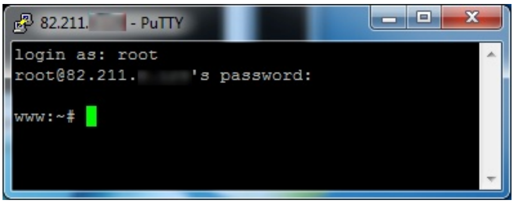
○ Auto ● IPv4 ○ IPv6

Now click Add, and then Open. A connection is established to the server, and a new window opens, prompting you for your username and password.



```
login as:
```

Enter this information and you will be logged into the server and receive a command line prompt from the server. The SOCKS proxy is then established. Important: you should now verify the host key and configure your applications, otherwise you are not using the tunnel you have created.



```
login as: root
root@82.211.[redacted]'s password:

www:~# 
```

HOST KEY VERIFICATION

The first time you connect to a server, you should be prompted to confirm the *host key fingerprint* for that server. The host key fingerprint is a long sequence of letters and numbers (hexadecimal) like 57:ff:c9:60:10:17:67:bc:5c:00:85:37:20:95:36:dd that securely identifies a particular server. Checking the host key fingerprint is a security measure to confirm that you are communicating with the server you think you are, and that the encrypted connection cannot be intercepted.

SSH does not provide a means of verifying this automatically. To get the benefit of this security mechanism, you should try to check the value of the host key fingerprint with the administrator of the server you're using, or ask a trusted contact to try connecting to the same server to see if they see the same fingerprint.

Verifying host key fingerprints is important for ensuring that SSH protects the privacy of your communications against eavesdropping, but it isn't necessary if you only want to circumvent censorship and don't care if network operators can see the contents of your communications.

CONFIGURING APPLICATIONS TO USE THE PROXY

The proxy created by the steps above should work until you close the SSH program. However, if your connection to the server is interrupted, you will need to repeat the same steps to reactivate the proxy.

Once the proxy is up and running, you need to configure software applications to use it. Using the steps above, the proxy will be a SOCKS proxy located on *localhost*, port 1080 (also known as 127.0.0.1, port 1080). You should try to ensure that your applications are configured in a way that prevents **DNS leaks**, which could make SSH less effective both for privacy protection and censorship circumvention.

MORE OPTIONS

So far, all these commands display a command line on the remote machine from which you can then execute whatever commands that machine provides to you. Sometimes you may want to execute a single command on a remote machine, returning afterward to the command line on your local machine. This can be achieved by placing the command to be executed by the remote machine in single quotes.

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

`Sometimes` what you need is to execute time consuming commands on a remote machine, but you aren't sure to have sufficient time during your current `ssh` session. If you close the remote connection before a command execution has been completed, that command will be aborted. To avoid losing your work, you may start via `ssh` a remote `screen` session and then detach it and reconnect to it whenever you want. To detach a remote `screen` session, simply close the `ssh` connection: a detached `screen` session will remain running on the remote machine.

`ssh` offers many other options, which are described on the manual page. You can also set up your favorite systems to allow you to log in or run commands without specifying your password each time. The setup is complicated but can save you a lot of typing; try doing some Web searches for "ssh-keygen", "ssh-add", and "authorized_keys".

SCP: FILE COPYING

The SSH protocol extends beyond the basic `ssh` command. A particularly useful command based on the SSH protocol is `scp`, the secure copy command. The following example copies a file from the current directory on your local machine to the directory */home/me/stuff* on a remote machine.

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

Be warned that the command will overwrite any file that's already present with the name */home/me/stuff/myprog.py*. (Or you'll get an error message if there's a file of that name and you don't have the privilege to overwrite it.) If */home/me* is your home directory, the target directory can be abbreviated.

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

You can just as easily copy in the other direction: from the remote machine to your local one.

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

The file on the remote machine is *interview.txt* in the *docs* subdirectory of your home directory. The file will be copied to *yesterday-interview.txt* in the home directory of your local system

`scp` can be used to copy a file from one remote machine to another.

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

To recursively copy all of the files and subdirectories in a directory, use the `-r` option.

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

See the `scp` man page for more options.

RSYNC: AUTOMATED BULK TRANSFERS AND BACKUPS

`rsync` is a very useful command that keeps a remote directory in sync with a local directory. We mention it here because it's a useful command-line way to do networking, like `ssh`, and because the SSH protocol is recommended as the underlying transmission for `rsync`.

The following is a simple and useful example. It copies files from your local */home/myname/docs* directory to a directory named *backup/* in your home directory on the system *quantum.example.edu*. `rsync` actually minimizes the amount of copying necessary through various sophisticated checks.

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

The `-e` option to `ssh` uses the SSH protocol underneath for transmission, as recommended. The `-a` option (which stands for "archive") copies everything within the specified directory. If you want to delete the files on the local system as they're copied, include a `--delete` option. See the `rsync` manual page for more details about `rsync`.

MAKING LIFE EASIER WHEN YOU USE SSH OFTEN

If you use SSH to connect to a lot of different servers, you will often make mistakes by mistyping usernames or even host names (imagine trying to remember 20 different username/host combinations). Thankfully, SSH offers a simple method to manage session information through a configuration file.

The configuration file is hidden in your home directory under the directory *.ssh* (the full path would be something like */home/jsmith/.ssh/config* – if this file does not exist you can create it). Use your favorite editor to open this file and specify hosts like this:

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

You can set up multiple hosts like this in your configuration file, and after you have saved it, connect to the host you called "dev" by running the following command:

```
$ ssh dev
```

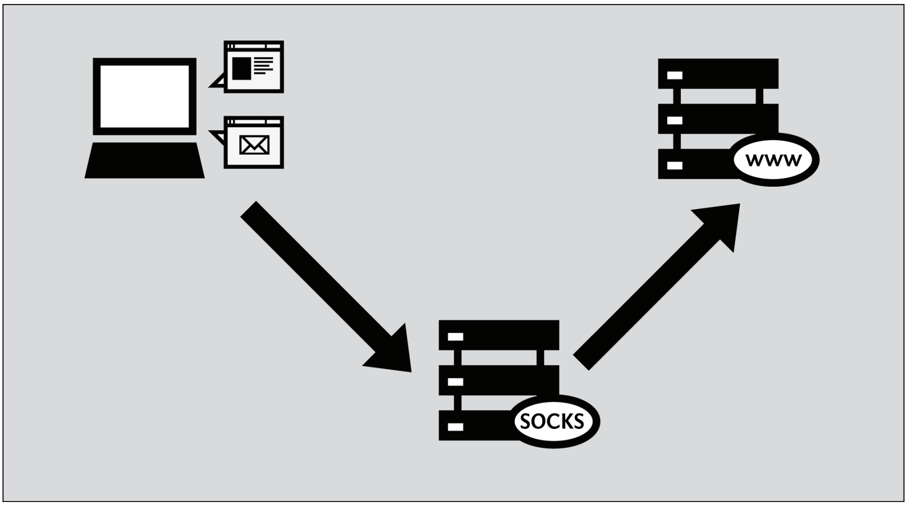
Remember, the more often you use these commands the more time you save.

32. SOCKS PROXIES

SOCKS is an Internet **protocol** which presents a special kind of **proxy server**. The default port for SOCKS proxies is 1080, but they may also be available on other ports. The practical difference to normal HTTP proxies is that SOCKS proxies work not only for Web browsing, but also for other applications like video games, file transfer or instant messenger clients. Similar to a VPN, they work as a secure tunnel.

Common SOCKS versions include 4, 4a and 5. The version 4 always needs the IP address to create a connection, so the DNS resolution still has to take place on the client. This make it useless for many circumvention needs. Version 4a usually uses hostnames. Version 5 includes newer techniques such as authentication, **UDP** and IPv6, but it often uses IP addresses, so it might also not be the perfect solution. See also the section "DNS leaks" at the end of this chapter.

A variety of software can take advantage of a SOCKS proxy to bypass filters or other restrictions not only Web browsers, but also other Internet software like instant messaging and e-mail applications.



Although public SOCKS proxies do exist, in many cases SOCKS proxies will run locally on your computer, and will be provided by a software application. Because SOCKS tunnels are so flexible, some censorship circumvention software creates a *local proxy* running on your own computer (which is usually referred to by the name *localhost* or the IP address 127.0.0.1). This local proxy is a way to let applications such as a Web browser take advantage of the circumvention software. Tools that can work in this way include Tor, Your-Freedom and SSH tunnels set up with PuTTY.

Local proxy enthusiast T-shirt (get it?)

In order to use an application proxy for circumventing censorship, you must tell software on your computer that you want to use that proxy when communicating with other systems on the Internet.

Some Internet applications don't ordinarily work with a proxy because their developers didn't create them with proxy support. However, many of these applications can be made to work with a SOCKS proxy using *socksifier* software. Some examples of such software include:

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

CONFIGURING YOUR APPLICATIONS

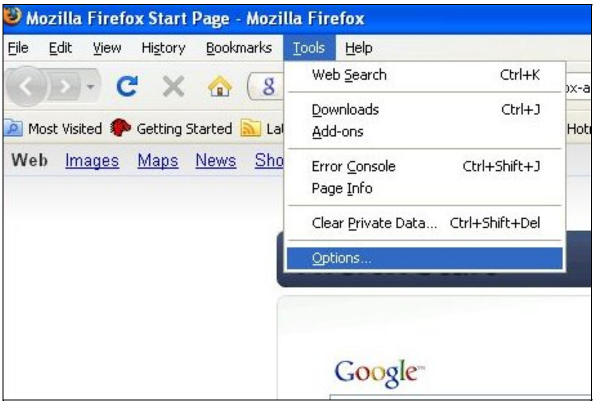
In most cases configuring applications to use a SOCKS proxy is done in much the same way as configuring them to use HTTP proxies. Applications that support SOCKS proxies will have a separate entry in the menu or configuration dialog where HTTP proxies are configured which let you configure a SOCKS proxy. Some applications will ask you to choose between SOCKS 4 and SOCKS 5 proxy settings; in most cases SOCKS 5 is the better option, although some SOCKS proxies may only work with SOCKS 4.

Some applications, such as Mozilla Firefox, will allow you to configure both an HTTP proxy and a SOCKS proxy at the same time. In this case, normal web-browsing will happen through the HTTP proxy, and Firefox may use the SOCKS proxy for other traffic such as streaming video.

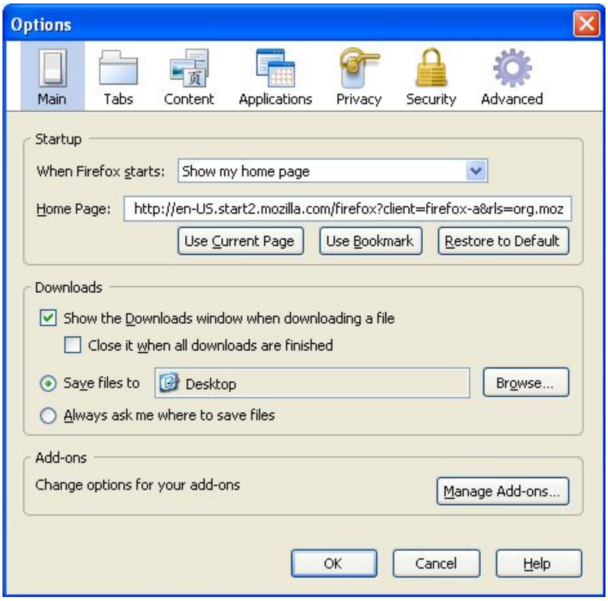
Mozilla Firefox

To configure Mozilla Firefox to use a SOCKS proxy:

1. Select Tools > Options:



2. The Options window appears:



Startup

When Firefox starts: Show my home page

Home Page: http://en-US.start2.mozilla.com/firefox?client=firefox-a&rls=org.moz

Downloads

☑ Show the Downloads window when downloading a file

□ Close it when all downloads are finished

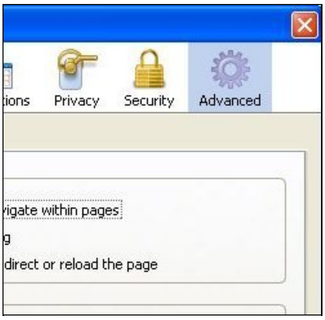
● Save files to Desktop

○ Always ask me where to save files

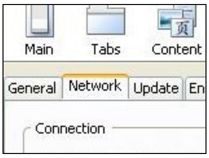
Add-ons

Change options for your add-ons

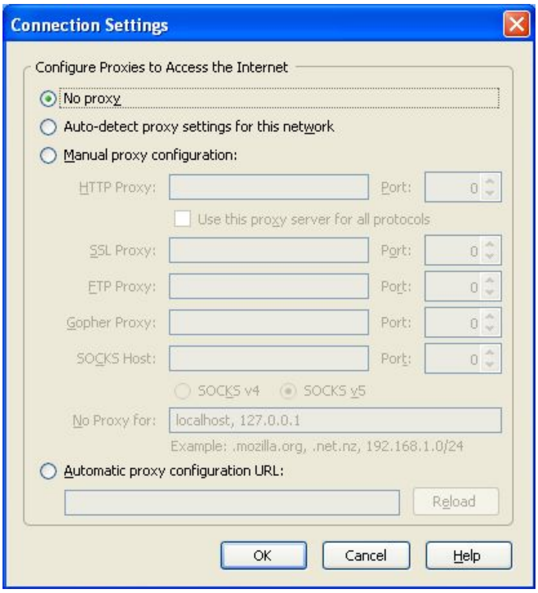
3. In the toolbar at the top of the window, click Advanced:



4. Click the Network tab:



5. Click Settings. The Connection Settings window opens:



Connection Settings

Configure Proxies to Access the Internet

● No proxy
○ Auto-detect proxy settings for this network
○ Manual proxy configuration:

HTTP Proxy: Port: 0

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

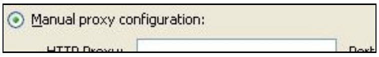
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

Reload

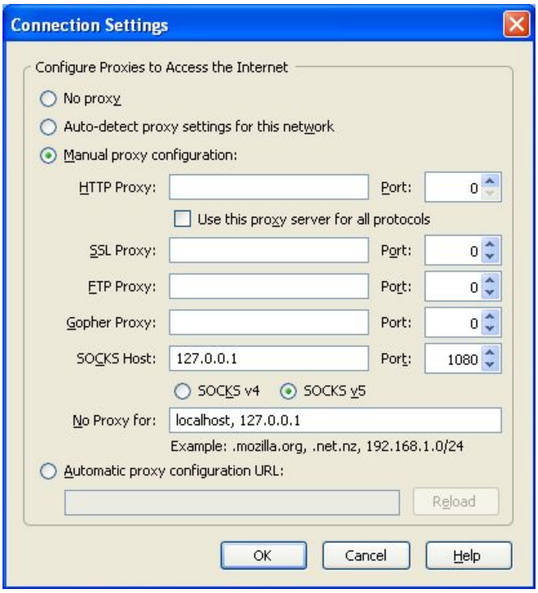
OK Cancel Help

6. Select "Manual proxy configuration". The fields below that option become available.



● Manual proxy configuration:

7. Enter the SOCKS proxy address and port number, choose SOCKS v5, then click OK.



Connection Settings

Configure Proxies to Access the Internet

○ No proxy
○ Auto-detect proxy settings for this network
● Manual proxy configuration:

HTTP Proxy: Port: 0

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

SOCKS Host: 127.0.0.1 Port: 1080

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

Reload

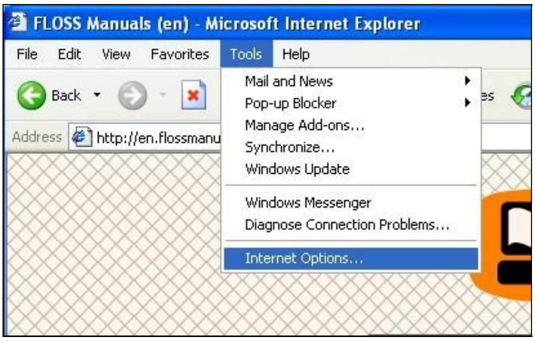
OK Cancel Help

Now Firefox is configured to use a SOCKS proxy.

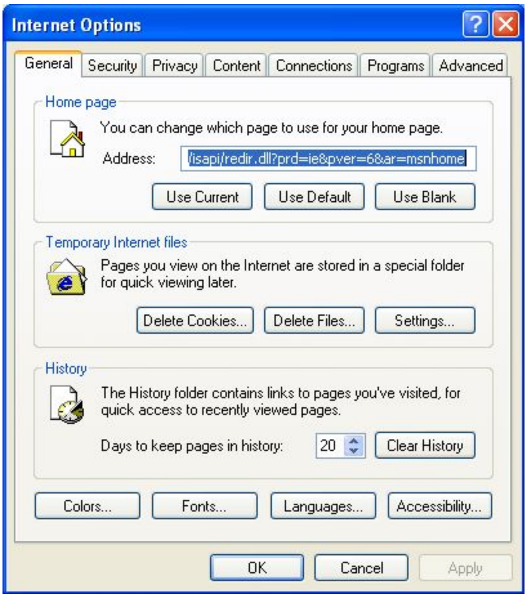
Microsoft Internet Explorer

To configure Internet Explorer to use a SOCKS proxy:

1. Select Tools > Internet Options:



2. Internet Explorer displays the Internet Options window:



You can change which page to use for your home page.

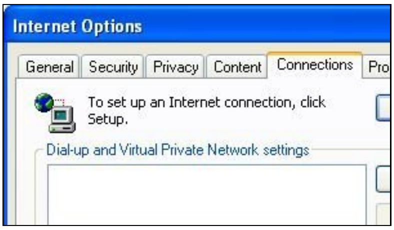
Address: /isapi/redir.dll?prd=ie&pver=6&ar=msnhome

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

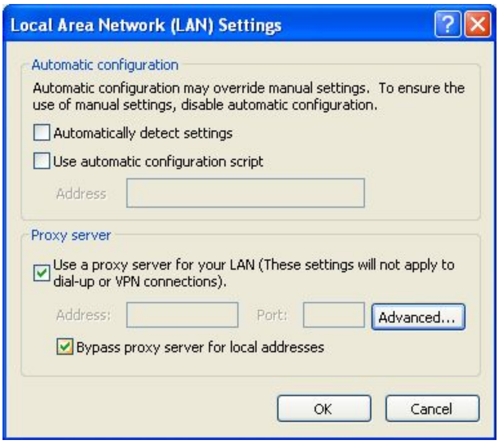
Days to keep pages in history: 20

3. Click the Connections tab:



To set up an Internet connection, click Setup.

4. Click LAN Settings. Internet Explorer displays the Local Area Network (LAN) Settings window:



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

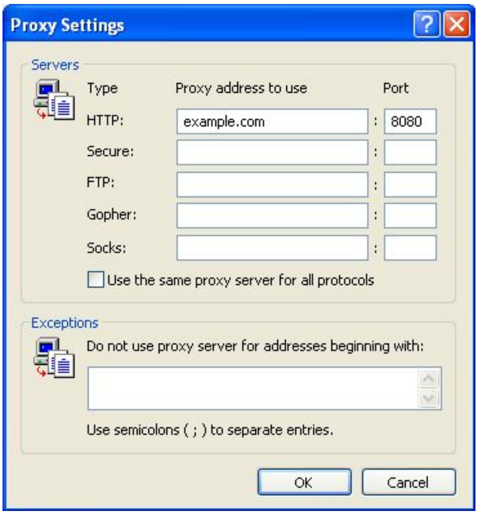
Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☑ Bypass proxy server for local addresses

5. Select "Use a proxy server for your LAN" and click Advanced.
   Internet Explorer displays the Proxy Settings window:



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	example.com	8080
Secure:		
FTP:		
Gopher:		
Socks:		

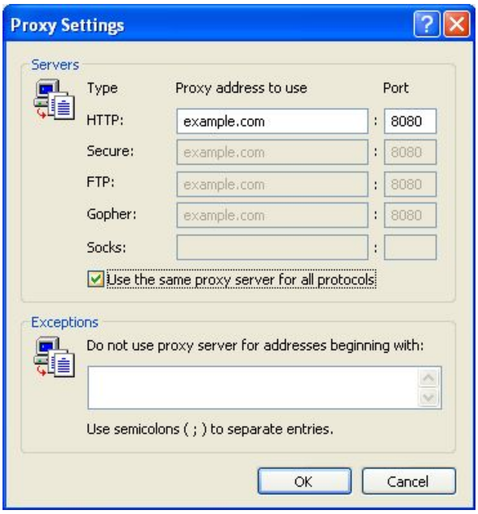
□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

6. Clear "Use the same proxy server for all protocols" if it is selected:



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	example.com	8080
Secure:	example.com	8080
FTP:	example.com	8080
Gopher:	example.com	8080
Socks:		

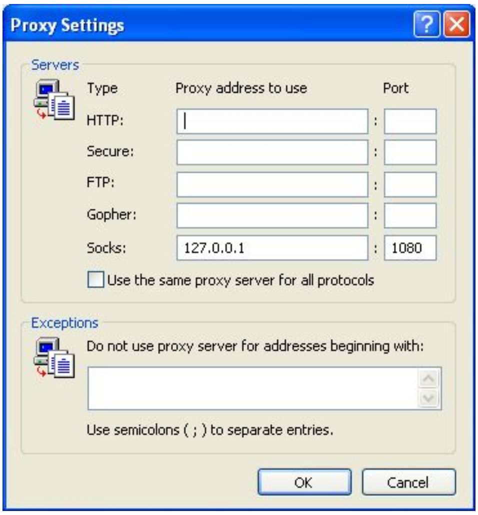
☑ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

7. Enter the proxy address to use and port number in the Socks row and click OK:



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:		
Secure:		
FTP:		
Gopher:		
Socks:	127.0.0.1	1080

□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

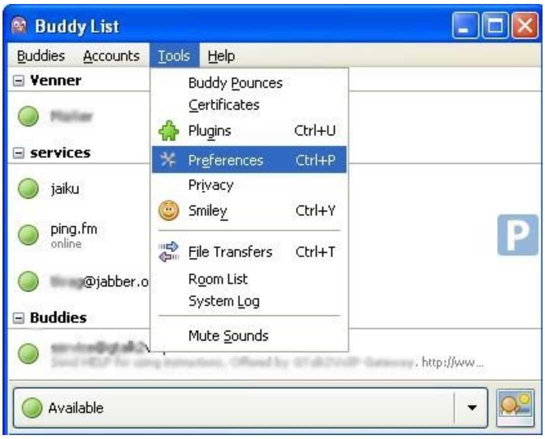
Use semicolons (;) to separate entries.

Now Internet Explorer is configured to use a SOCKS proxy.

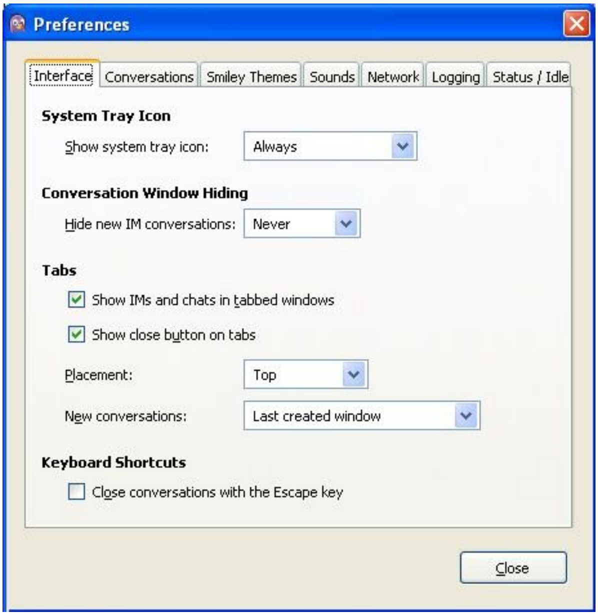
Configuring a SOCKS proxy for other applications

Many Internet applications other than Web browsers can use a SOCKS proxy to connect to the Internet, potentially bypassing blocking. Here is an example with the instant messaging software Pidgin. This is a typical example, but the exact sequence of steps to configure some other application to use a SOCKS proxy would be slightly different.

1. Select Tools > Preferences:



2. Pidgin displays the Preferences window:



System Tray Icon

Show system tray icon: Always

Conversation Window Hiding

Hide new IM conversations: Never

Tabs

☑ Show IMs and chats in tabbed windows

☑ Show close button on tabs

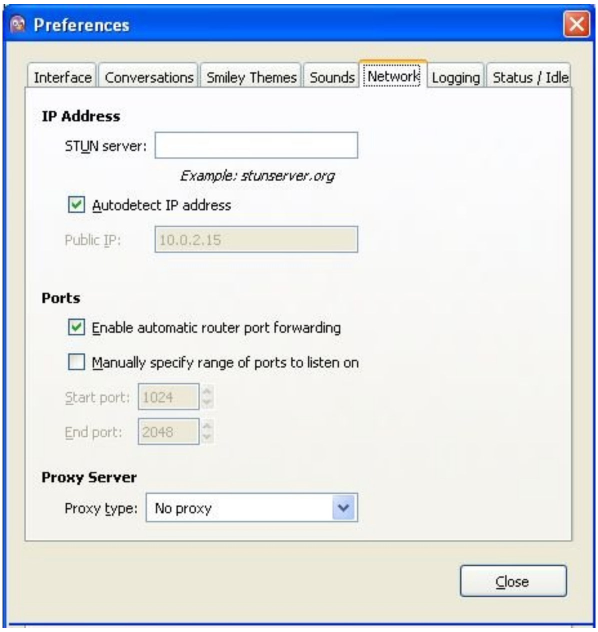
Placement: Top

New conversations: Last created window

Keyboard Shortcuts

□ Close conversations with the Escape key

3. Click the Network tab:



IP Address

STUN server:

Example: stunserver.org

☑ Autodetect IP address

Public IP: 10.0.2.15

Ports

☑ Enable automatic router port forwarding

□ Manually specify range of ports to listen on

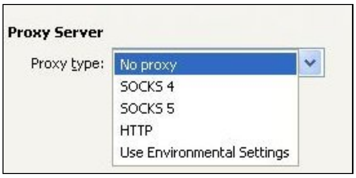
Start port: 1024

End port: 2048

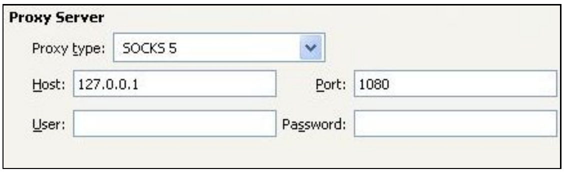
Proxy Server

Proxy type: No proxy

4. For Proxy type, select SOCKS 5. Additional fields appear under that option.



5. Enter the host address and port number of your SOCKS proxy:


Proxy Server

Proxy type: SOCKS 5

Host: 127.0.0.1

Port: 1080

User:

Password:

6. Click Close.

Pidgin is now configured to use a SOCKS proxy.

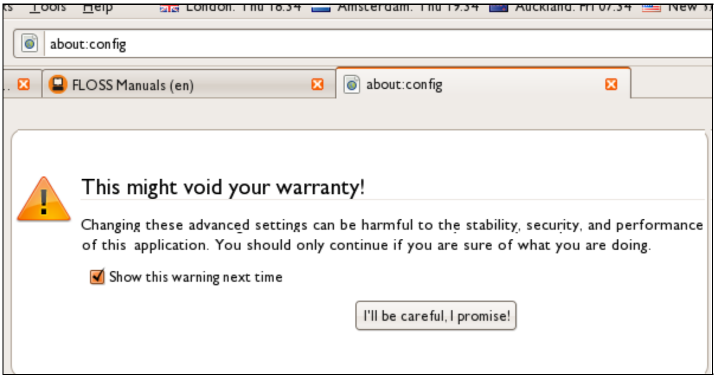
When you're done with the proxy

When you are done using a proxy, particularly on a shared computer, return the settings you've changed to their previous values. Otherwise, those applications will continue to try to use the proxy. This could be a problem if you don't want people to know that you were using the proxy or if you were using a local proxy provided by a particular circumvention application that isn't running all the time.

DNS LEAKS

One important problem with SOCKS proxies is that some applications that support the use of SOCKS proxies may not use the proxy for all their network communications. The most common problem is that Domain Name System (DNS) requests may be made without going through the proxy. This **DNS leak** can be a privacy problem and can also leave you vulnerable to DNS blocking, which a proxy could otherwise have circumvented. Whether an application is vulnerable to DNS leaks may vary from version to version. Mozilla Firefox is currently vulnerable to DNS leaks in its default configuration, but you can avoid these by making a permanent configuration change to prevent DNS leaks:

1. In the Firefox address bar, enter `about:config` as if it were a URL (you may see a warning about changing advanced settings):

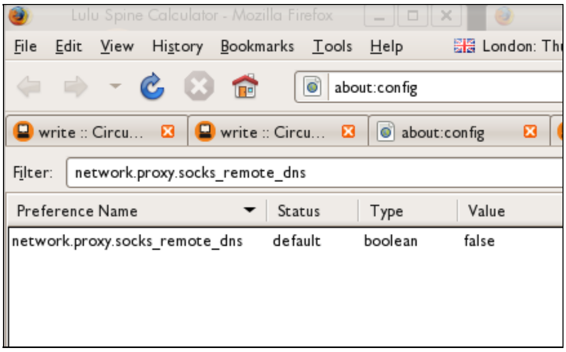


This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

2. If necessary, click "I'll be careful, I promise!" to confirm that you want to modify your browser settings. The browser displays a list of configuration settings information.
3. In the Filter field, enter `network.proxy.socks_remote_dns`. Only that setting is displayed:


Lulu Spine Calculator - Mozilla Firefox
File Edit View History Bookmarks Tools Help
London: Th
about:config
write :: Circu...
write :: Circu...
about:config

Filter: network.proxy.socks_remote_dns

Preference Name	Status	Type	Value
network.proxy.socks_remote_dns	default	boolean	false

4. If this setting has the value *false*, double-click it to change its value to *true*.

Firefox is now configured to avoid DNS leaks. Once the value is displayed as *true*, this setting is automatically saved permanently.

There is no documented way to prevent DNS leaks within Microsoft Internet Explorer, without using an external program.

At the time of this writing there are no known DNS leaks in Pidgin when configured to use a SOCKS 5 proxy.

HELPING OTHERS

33. RESEARCHING AND DOCUMENTING CENSORSHIP

In many countries, it is no secret that government censorship of the Internet exists. The scope and methods of censorship have been documented for example in the books *Access Denied: The Practice and Policy of Global Internet Filtering* and *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, both edited by Ronald Delbert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (http://opennet.net/accessdenied and http://www.access-controlled.net).

When a popular site is widely blocked, that fact tends to become widely known within the country. However, some governments (including some rather active censors) officially deny the existence of censorship or try to disguise it as random technical errors. If you're subject to censorship, you can use your situation to help others (including the international academic and activist community that studies censorship) understand it and potentially publicize it.

Of course, you need to be cautious about this; governments that deny their network censorship practice may not appreciate your participation in efforts to expose them.

RESEARCH CENSORSHIP KNOWLEDGE DATABASES

Some censorship knowledge databases have been made public in the last couple of years. Some of them are crowd-sourced but they are all validated by field experts. They are being constantly updated to keep information and blocked sites lists as accurate as possible. Some databases are available at the following URLs:

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

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

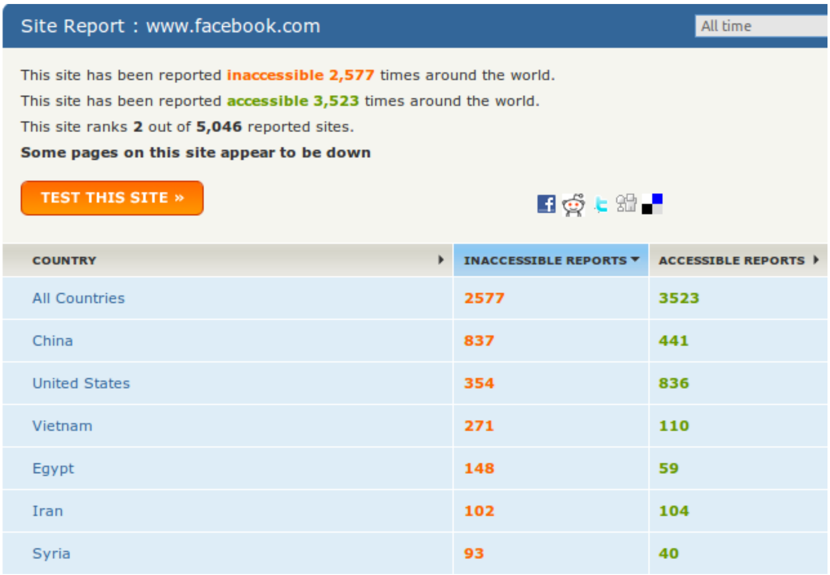
On a more macro-geographic level, OpenNet Initiative and Reporters without Borders release a "State of Internet" for every country on a regular basis. You can access them online:

- *OpenNet Initiative* research report: http://opennet.net/research
- *Reporters Without Borders* Internet Enemies: http://www.rsf.org/ennemis.html

REPORTING BLOCKED SITES USING HERDICT

Herdict (https://www.herdict.org) is a Web site which aggregates reports of inaccessible sites. It's run by researchers at the Berkman Center For Internet and Society at Harvard University in the United States who study how the Internet is being censored.

The data in Herdict isn't perfect – for example, many users can't distinguish a site that is not available because of a technical glitch or because they mistyped the address from actual censorship – but the data is collected from all over the world and is constantly updated.



Site Report : www.facebook.com

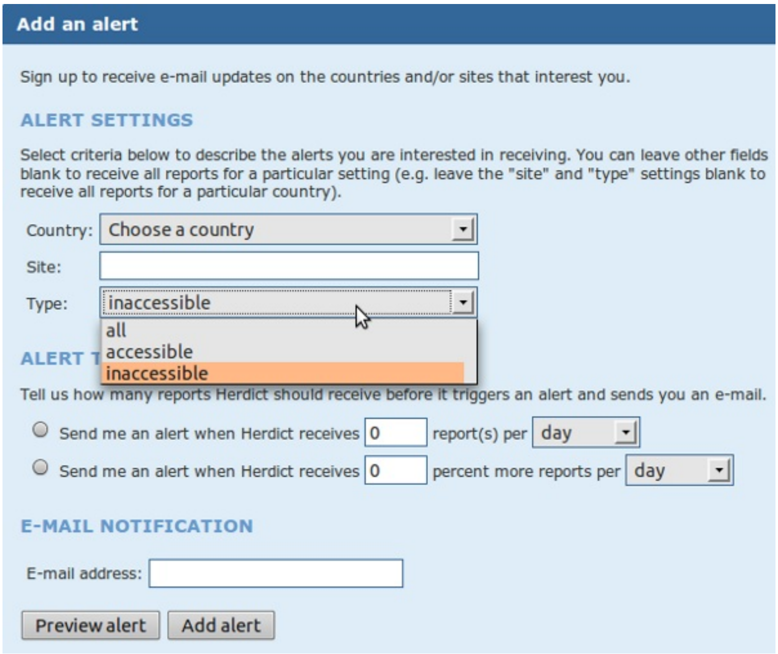
All time

This site has been reported **inaccessible 2,577** times around the world.
This site has been reported **accessible 3,523** times around the world.
This site ranks **2** out of **5,046** reported sites.
Some pages on this site appear to be down

COUNTRY	INACCESSIBLE REPORTS	ACCESSIBLE REPORTS
All Countries	2577	3523
China	837	441
United States	354	836
Vietnam	271	110
Egypt	148	59
Iran	102	104
Syria	93	40

Above is an overview of the Facebook report.

You can help these researchers by submitting your own reports to Herdict through their web site. It is free, easy to use and you don't even have to register. You can also register to get updates on future block notifications about a website.



Add an alert

Sign up to receive e-mail updates on the countries and/or sites that interest you.

ALERT SETTINGS

Select criteria below to describe the alerts you are interested in receiving. You can leave other fields blank to receive all reports for a particular setting (e.g. leave the "site" and "type" settings blank to receive all reports for a particular country).

Country: Choose a country

Site:

Type: inaccessible

ALERT T

Tell us how many reports Herdict should receive before it triggers an alert and sends you an e-mail.

○ Send me an alert when Herdict receives 0 report(s) per day

○ Send me an alert when Herdict receives 0 percent more reports per day

E-MAIL NOTIFICATION

E-mail address:

Herdict also offers add-ons for the Firefox and Internet Explorer Web browsers to make it easier to report whether particular Web sites are blocked or not as you browse the web.

REPORTING BLOCKED SITES USING ALKASIR

Alkasir is a censorship circumvention tool with a build in research part which allows its users to report a blocked Web site with a simple click on the "Report Blocked URLs" button. Alkasir maintains a relevant list of blocked sites per country and may automatically check other related URLs for availability. By using the report feature you can easily contribute to this research.

You can find more details about how to use the tool in the chapter "Using Alkasir".

ENABLING REMOTE ACCESS FOR OTHERS

You can also help censorship research by giving researchers remote access to your computer so that they can use it to carry out their own tests. You should only do this if you trust the researchers in question with the kind of access you're offering them, since they may get full control over your computer and everything they do on your machine will look like your own actions to your ISP or government.

For GNU/Linux operating systems a *shell account* is the best option; you can find help in setting this up at http://ubuntuforums.org and other sites.

For Windows operating systems the build-in *remote desktop* feature should be used. You can find instructions for this at http://www.howtogeek.com/howto/windows-vista/turn-on-remote-desktop-in-windows-vista. You may also have to change *port forwarding* settings on the router box you use to connect to the Internet; this is explained on http://portforward.com.

Another solution for remote access is the free tool TeamViewer (http://www.teamviewer.com) which is available for all operating systems.

COMPARING NOTES

The basic technique for documenting network censorship is to try to access a huge number of network resources, such as a long list of URLs, from various places on the Internet and then compare the results. Did some of the URLs fail to load in one place but not in another? Are these differences ongoing and systematic? If you have a reliable circumvention technology such as a VPN, you can do some of these experiments by yourself, by comparing how the net looks with and without circumvention. For example, in the United States, this was the method used to document how ISPs were disrupting the use of peer-to-peer filesharing software.

These comparisons can be done with automated software or by hand.

PACKET SNIFFING

If you become familiar with the technical details of how Internet protocols work, a packet sniffer like Wireshark (http://www.wireshark.com/) will let you record the actual network packets that your computer transmits and receives.

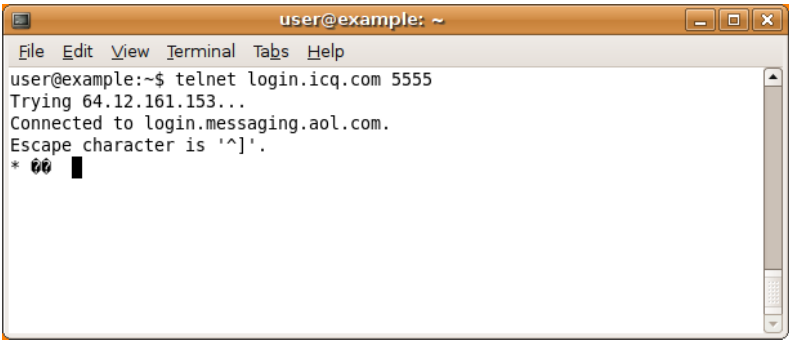
34. DEALING WITH PORT BLOCKING

Network firewalls can be used to block all communications that are directed to a particular port number. This can be used to try to prevent the use of a particular **protocol** or kind of network software. To try to circumvent these restrictions, ISPs and users could arrange access to services at non standard port numbers. This allows software to circumvent simple port blocking.

Many software applications can easily be made to use non standard port numbers. URLs for web pages have a particularly convenient way of doing this right inside the URL. For example, the URL *http://www.example.com:8000/foo/* would tell a web browser to make an HTTP request to example.com on port 8000, rather than the default http port 80. Of course, this will only work if the web server software on www.example.com is already expecting requests on port 8000.

TESTING FOR PORT BLOCKING

You can test which ports (if any) are blocked on your connection using Telnet. Just open a command line, type "telnet login.icq.com 5555" or "telnet login.oscar.aol.com 5555" and press Enter. The number is the port you want to test. If you get some strange symbols in return, the connection succeeded.



```
user@example:~$ telnet login.icq.com 5555
Trying 64.12.161.153...
Connected to login.messaging.aol.com.
Escape character is '^]'.
* ��  █
```

If, on the other hand, the computer reports that the connection failed, timed out, or was interrupted, disconnected, or reset, that port is probably being blocked. (Keep in mind that some ports could be blocked only in conjunction with certain IP addresses.)

35. INSTALLING WEB PROXIES

If you have access to a Web server in a country which is not censoring access to the Internet, you can install a **Web proxy**, which is a small software written in the programming languages PHP, Perl, Python or ASP. Installation of Web-based circumvention software requires some technical expertise and resources (a compatible Web hosting and sufficient bandwidth).

If you want to install your own Web proxy, you need one of the following:

- a Web hosting space with PHP support (which can be purchased for a few US dollars a year from hosting companies such as https://www.dreamhost.com or http://www.hostgator.com, or provided by your school or university)
- a virtual (VPS) or dedicated server (which are more expensive and more complicated to use)
- a PC connected to a broadband connection (with a publicly routable IP address).

PUBLIC AND PRIVATE WEB PROXIES

Public Web proxies are available to anyone able to search them, on search engines such as Google for example. Public Web proxies and anonymity services may be found by users and those authorities implementing filtering, so they are more vulnerable to blacklisting.

The locations of Private Web proxies are only known to the intended users. Therefore, private Web proxies are best suited for users who require stable circumvention services for Web traffic and have trusted contacts in non-filtered locations with sufficient technical skills and available bandwidth to set up and maintain the Web proxy. The chances of private Web proxies being detected and blocked are lower than those of public circumvention services. This is also the most flexible circumvention option available for simple Web traffic and is less likely to be discovered and blocked than a public Web proxy, particularly if it is used with SSL encryption.

FEATURES OF WEB PROXIES

Web proxies can be set up with some level of customization tailored to the specific needs of the end user. Common customizations would include changing the port number that the Web server runs on and implementing encryption such as SSL. Since some blacklists may block keywords associated with popular proxy software, changing items like the default URL, the name of the script, or elements of the user interface can also reduce the risk of automated detection and blocking of the proxy. It is possible to protect the use of the Web proxy by enabling .htaccess with a username and a password.

When using SSL, it's also useful to create an innocuous Web page at the root of the Web server and conceal the Web proxy with a random path and file name. Although intermediaries may be able to determine the server you are connecting to, they will not be able to determine the requested path because that part of the request is encrypted. For example, if a user connects to https://example.com/secretproxy/, an intermediary will be able to determine that the user connected to example.com but they will not know that the user requested the Web proxy. If the Web proxy operator places an innocuous page at example.com, then the Web proxy is less likely to be discovered by monitoring network transmissions. A valid SSL certificate which is trusted in all popular Web browsers is available for free at https://www.startcom.org/.

There are several free open source Web proxies available on the Internet. The main differences are the programming languages they are written in, since not every Web server supports every programming language. The other big difference is the compatibility of the script with modern Web sites with technologies like AJAX (used by GMail or Facebook) or streaming Flash video (used by YouTube).

Popular free Web proxy programs include:

- CGIProxy (http://www.jmarshall.com/tools/cgiproxy): a CGI script written in the Perl programming language that acts as both an HTTP and an FTP proxy.
- Peacefire's Circumventor (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html): an automated installer program that makes it much easier for non-technical users to install and configure CGIProxy on a Windows machine.
- SabzProxy (http://sabzproxy.com): both an HTTP and an FTP proxy. It is based on the legacy code of PHProxy written in PHP with new features, such as random encoding of the URL, to make it harder to block.

- Glype Proxy (http://www.glype.com): another free-to-use, web-based proxy script, also written in PHP.

The sites of these Web proxies provide instructions on how to set them up. Basically, this involves downloading the script, extracting it on the local hard disk, uploading the script via FTP or SCP to your Web server, setting permissions and testing the script. The following example is for the installation of SabzProxy, but the steps are similar for other Web proxies.

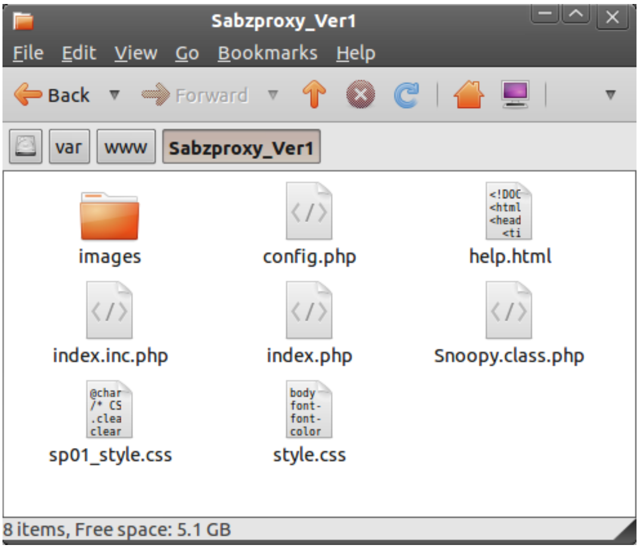
INSTALLING SABZPROXY

SabzProxy is only available in Persian, but the GUI is simple and is still easy to understand.

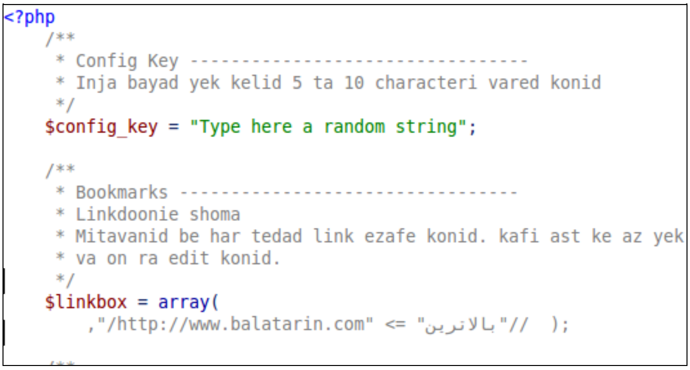
These instructions describe the most common case: using FTP to transfer SabzProxy to a Web space account that already supports PHP. For this technique, you will also need an FTP client program such as FileZilla (http://filezilla-project.org).

Although this method is the most common, it isn't applicable to every situation (for example if you're setting up your own server through the comand line), but the steps should be similar.

1. The first step is to download the SabzProxy archive file from http://www.sabzproxy.com.
2. Next, extract the contents of the .zip file by clicking with the right mouse button on the file and choosing Extract All.



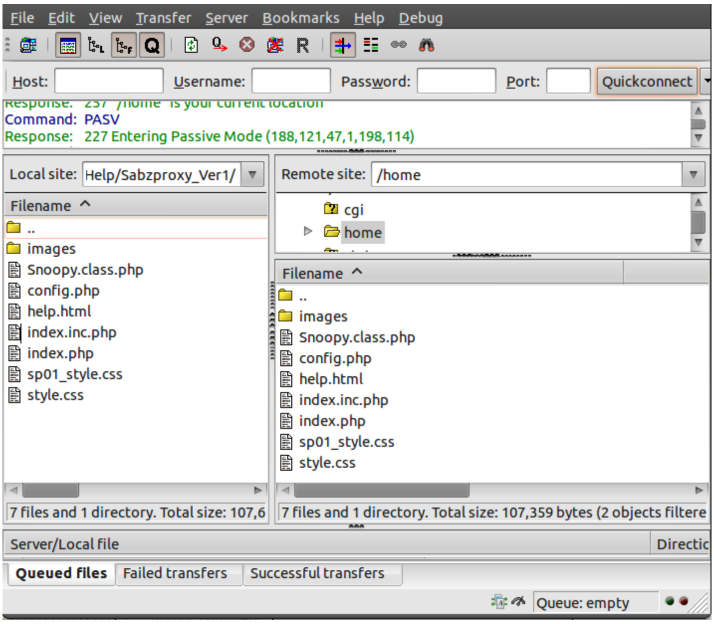
3. Open the config.php file with a basic text editor (e.g. Notepad for Windows, Gedit or Nano for Linux systems, Texteditor for MacOS)
4. Edit line 8, starting with *$config_key*. Type a random string between "". This string will be used to randomize the URL encoding, so make it as random as possible.



```
<?php
    /**
     * Config Key --------------------------------
     * Inja bayad yek kelid 5 ta 10 characteri vared konid
     */
    $config_key = "Type here a random string";

    /**
     * Bookmarks --------------------------------
     * Linkdoonie shoma
     * Mitavanid be har tedad link ezafe konid. kafi ast ke az yek
     * va on ra edit konid.
     */
    $linkbox = array(
        ,"/http://www.balatarin.com" <= "بالاترین"//  );
```

5. You can also configure a couple of options, such as the welcoming text and links.
6. Open FileZilla, enter the server (host), username and password of your Web space and click on Quickconnect (or similar if you are using a different FTP client).
7. The left part of the FTP client window represents your local PC, so you can locate the SabzProxy files that you have just extracted here.



```
Response:  257 "/home" is your current location
Command:   PASV
Response:  227 Entering Passive Mode (188,121,47,1,198,114)
```

Local site: Help/Sabzproxy_Ver1/

```
..
images
Snoopy.class.php
config.php
help.html
index.inc.php
index.php
sp01_style.css
style.css
```

7 files and 1 directory. Total size: 107,6

Remote site: /home

```
cgi
home
```

```
..
images
Snoopy.class.php
config.php
help.html
index.inc.php
index.php
sp01_style.css
style.css
```

7 files and 1 directory. Total size: 107,359 bytes (2 objects filtere

8. Drag-and-drop the files from the left part of the FTP client window to the right part, which represents the remote FTP server (your Web space).
9. You can now access SabzProxy by browsing to the domain of your Web space and the directory to which you uploaded PHProxy. (In this example http://kahkeshan-e-sabz.info/home.)

If this doesn't work, your server account may not support PHP, or support for PHP may be disabled or may require additional steps. Please refer to the documentation for your account or the Web server software in use. You can also look for an appropriate support forum or ask your web server operator for additional help.

36. SETTING UP A TOR RELAY

If you live in an area with little or no Internet censorship, you may want to run a Tor *relay* or a **Tor bridge** relay to help other Tor users access an uncensored Internet.

The Tor network relies on volunteers to donate bandwidth. The more people run relays, the faster and more secure the Tor network will be. To help people using Tor bypass Internet censorship, set up a bridge relay rather than an ordinary relay.

Bridge relays (or *bridges* for short) are Tor relays that are not listed in the main (and public) Tor directory. Even if an ISP is filtering connections to all the known Tor relays, it probably will not be able to block all the bridges.

RISKS OF OPERATING A TOR NODE (TOR RELAY)

A *Tor node* is a kind of public proxy, so running one can have the general risks of running a proxy mentioned in the "Risks of Operating a Proxy" chapter of this manual. However, a Tor node is typically set up in one of two ways: as an **exit node** or as a **middleman node** (sometimes called a *non-exit node*). A middleman node forwards encrypted traffic only to other Tor nodes, and does not allow anonymous users to communicate directly with sites outside of the Tor network. Running either kind of node is helpful to the Tor network as a whole. Running an exit node is particularly helpful because exit nodes are comparatively scarce. Running a middleman node is comparatively less risky because the middleman node is unlikely to draw the kinds of complaints that a public proxy might, since the IP address of a middleman node will never appear on log files.

Since a bridge is not an exit node, you are unlikely to receive complaints about the use of a bridge node by others.

Even though it is unlikely to draw specific complaints, operating a middleman or bridge node may cause your ISP to object for more general reasons. For example, the ISP may disapprove of the Tor network or may forbid subscribers from operating any sort of public service. You can find more best practices on how to safety run a Tor exit node on https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment.

WHAT DO I NEED TO RUN A RELAY OR A BRIDGE RELAY?

There are only a few prerequisites for running a Tor relay:

- Your Internet connection needs to have a bandwidth of at least 20 kilobytes/second in both directions (and it needs to be OK for your connection to be constantly in use when your computer is on).
- You need an Internet connection with an IP address that is publicly routable.
- If your computer is behind a **network address translation (NAT)** firewall and doesn't have access to its public (or external) IP address, you'll need to set up a *port forwarding* rule on your router. You can do this via the Tor Universal Plug and Play facility, or manually, by following the instructions in your router manual or at portforward.com (http://portforward.com/english/applications/port_forwarding/HTTPS/HTTPSindex.htm).

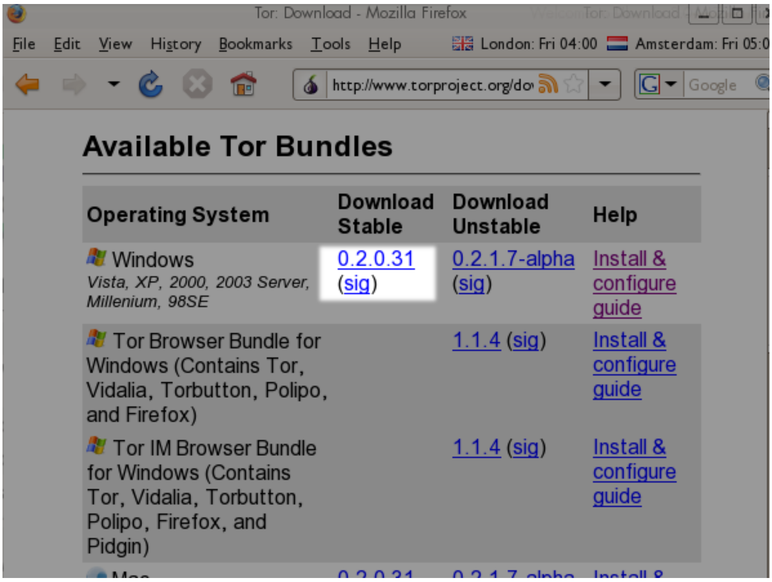
What is *not* required:

- Your computer does not have to be always on and online (the Tor directory will figure out when it is).
- You do not need to have a static IP address.

DOWNLOADING TOR

To download Tor, go to the https://www.torproject.org/ Web site and click Download in the navigation menu.

On the Available Tor Bundles page, select the stable version that fits your operating system.



Available Tor Bundles

Operating System	Download Stable	Download Unstable	Help
Windows *Vista, XP, 2000, 2003 Server, Millenium, 98SE*	0.2.0.31 (sig)	0.2.1.7-alpha (sig)	Install & configure guide
Tor Browser Bundle for Windows (Contains Tor, Vidalia, Torbutton, Polipo, and Firefox)		1.1.4 (sig)	Install & configure guide
Tor IM Browser Bundle for Windows (Contains Tor, Vidalia, Torbutton, Polipo, Firefox, and Pidgin)		1.1.4 (sig)	Install & configure guide
Mac	0.2.0.31	0.2.1.7-alpha	Install &

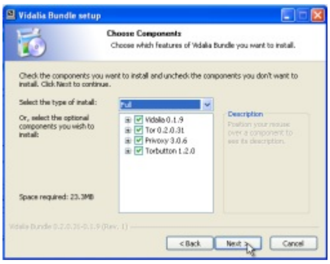
INSTALLING TOR ON GNU/LINUX

You can find detailed instructions on how to set up a Tor relay or bridge on https://www.torproject.org/docs/tor-doc-relay.html.en.

INSTALLING TOR ON MICROSOFT WINDOWS

Launch the installer and click Next when asked.

If you are using Firefox, install all the components proposed in the dialog shown below:



Choose which features of Vidalia Bundle you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Full

Or, select the optional components you wish to install:

- ☑ Vidalia 0.1.9
- ☑ Tor 0.2.0.31
- ☑ Privoxy 3.0.6
- ☑ Torbutton 1.2.0

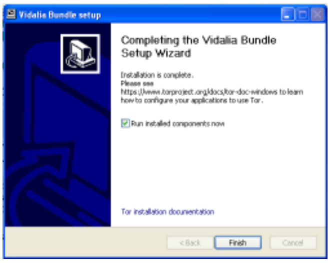
Position your mouse over a component to see its description.

Space required: 23.3MB

Vidalia Bundle 0.2.0.31-0.1.9 (Rev. 1)

If you do not have Firefox installed, deselect Torbutton (you will have the option to install Firefox and Torbutton afterwards).

When the installation is completed, launch Tor by clicking Finish with the "Run installed components now" box selected, as in the dialog shown below:



Completing the Vidalia Bundle Setup Wizard

Installation is complete.
Please see https://www.torproject.org/docs/tor-doc-windows to learn how to configure your applications to use Tor.

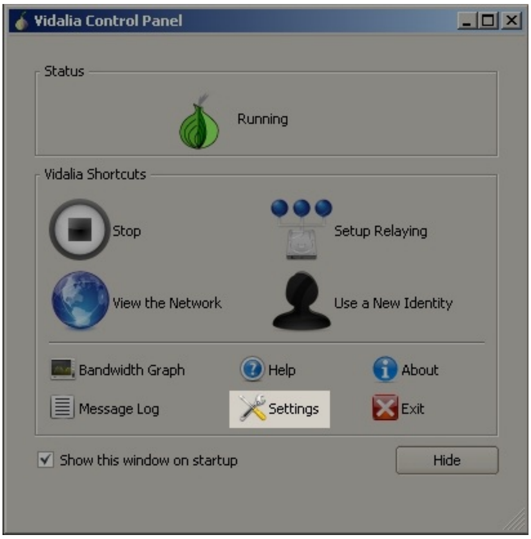
☑ Run installed components now

Tor installation documentation

CONFIGURING TOR TO BE A BRIDGE

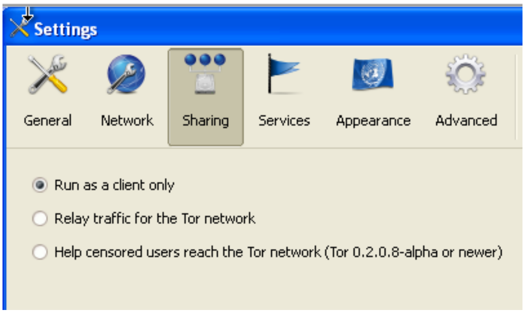
To activate your bridge:

1. Open the Vidalia control panel.
2. In the Vidalia control panel, click Settings:



☑ Show this window on startup

3. In the Settings window, click Sharing:

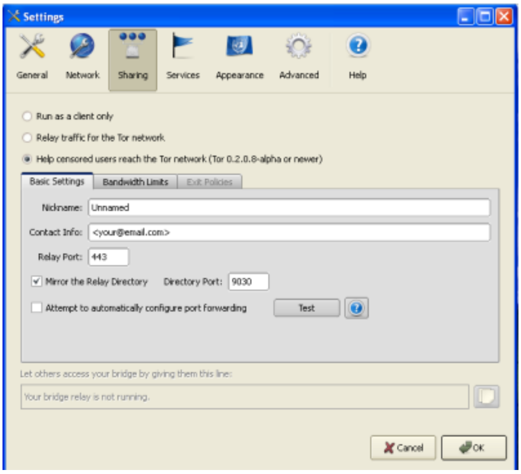


● Run as a client only

○ Relay traffic for the Tor network

○ Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)

4. To create the bridge, click "Help censored users reach the Tor network":



○ 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)

Nickname: Unnamed

Contact Info: <your@email.com>

Relay Port: 443

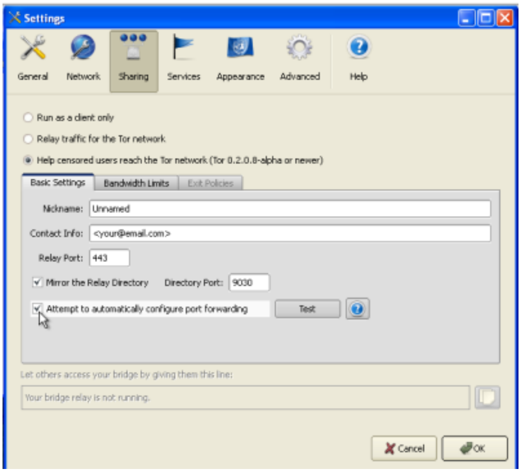
☑ Mirror the Relay Directory Directory Port: 9030

□ Attempt to automatically configure port forwarding

Let others access your bridge by giving them this line:

Your bridge relay is not running.

5. If you are using a NAT IP address on a local network, you will need to create a *port forwarding* rule in your router. You can ask Tor to try to configure port forwarding for you. To do so, click "Attempt to automatically configure port forwarding":

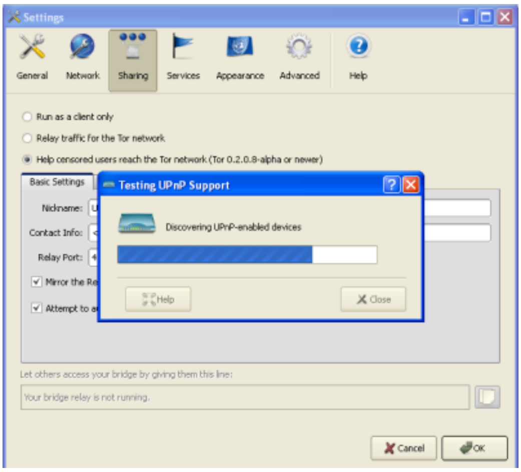


○ Run as a client only
○ Relay traffic for the Tor network
● Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)

Nickname: Unnamed
Contact Info: <your@email.com>
Relay Port: 443
☑ Mirror the Relay Directory Directory Port: 9030
☑ Attempt to automatically configure port forwarding

Let others access your bridge by giving them this line:
Your bridge relay is not running.

6. Click Test to see if Tor has correctly created a setting for port forwarding in the router:



○ 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)

Discovering UPnP-enabled devices

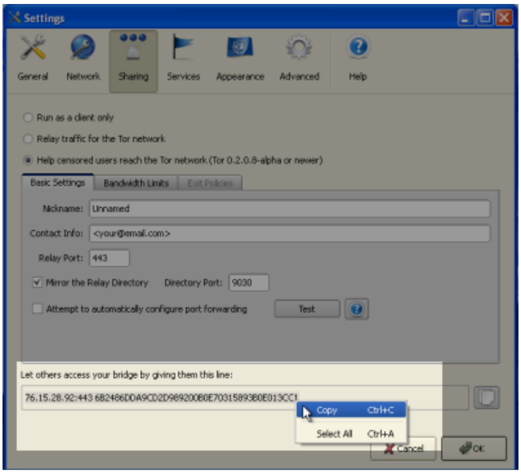
Let others access your bridge by giving them this line:
Your bridge relay is not running.

If Tor could not configure port forwarding, please read the Tor FAQ entry on this topic: https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#ServerForFirewalledClients

Congratulations. If all has gone well, your bridge is up and running. Your bridge information will be added to the hidden bridge directory and made available to users who request it.

SHARING YOUR BRIDGE WITH FRIENDS

If you specifically established your bridge to help a friend access the Tor network, you can copy the information at the bottom of the Settings window and send it to her:



○ 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)

Nickname: Unnamed

Contact Info: <your@email.com>

Relay Port: 443

☑ Mirror the Relay Directory Directory Port: 9030

□ Attempt to automatically configure port forwarding

Let others access your bridge by giving them this line:

76.15.28.92:443 6B2486DDA9CD2D989200B0E70315893B0E013CC1

37. RISKS OF OPERATING A PROXY

When you run a **Web proxy** or *application proxy* on your computer to help others, requests and connections forwarded through that proxy will appear to originate from your computer. Your computer is acting on behalf of other Internet users, so their activity could be attributed to you, as if you had done it yourself. So if someone uses the proxy to send or receive material that a third party objects to, you could receive complaints that assume that you are responsible and may ask you to stop that activity. In some cases, activities using your proxy could attract legal action or the attention of law enforcement agencies in your own or another country.

In some countries, proxy operators have received legal complaints, and, in some cases, law enforcement agents have even seized computers that were functioning as proxies. This could happen for several reasons:

- Someone may (incorrectly) assume that the operator of the proxy computer was personally involved in activity passing through the proxy.
- Someone may assert that the operator of the proxy has a legal duty to stop certain uses, even if the uses are being made by third parties.
- Someone may hope to examine the proxy to find evidence (e.g. logfiles) of who was responsible for some activity.

If you think this could be a risk for your proxy in your area, it may be safer to operate the proxy on a dedicated computer in a data center. That way it won't attract attention to your home Internet connection.

National laws may vary in the way and extent they protect proxy operators from liability. For details about your situation, you should consult a lawyer or qualified legal expert in your jurisdiction.

RISKS OF OPERATING A PUBLIC PROXY

Internet service providers may complain about your operation of a proxy, especially if they receive complaints about abuse of the proxy. Some **ISP**s may assert that running a public proxy violates their terms of service, or that they simply do not wish to permit users to run public proxies. These ISPs may disconnect you or threaten to disconnect you in the future.

A public proxy may be used by many people all over the world and may use huge amounts of bandwidth and traffic, so when using ISPs that charge on a non-flat-rate tariff, one should take precautions to avoid a large traffic bill at the end of the month.

RISKS OF OPERATING A PRIVATE PROXY

These risks still exist if you operate a proxy for your own benefit or for the use of a small number of individuals, but operating a non-public proxy is much less risky than operating a public proxy.

If the user of your non-public proxy is detected and monitored, whoever is doing the monitoring may realize or speculate that there is a connection between you and the user and that you are trying to help that person circumvent filtering.

Although your own ISP is much more likely to object to your running a public proxy than a private proxy, some ISPs may have such comprehensive anti-proxy policies that they object even to the operation of a private proxy on their networks.

DATA RETENTION LAWS MIGHT REGULATE PROXY OPERATION

In some countries, **data retention laws** or similar laws meant to restrict anonymity might be interpreted to regulate the operation of proxy services. For more information about data retention, see https://secure.wikimedia.org/wikipedia/en/wiki/Telecommunications_data_retention.

38. BEST PRACTICES FOR WEBMASTERS

Running a Web site, exposed to a wide audience or not, is not always easy. It is important to think about your personal safety as well as the safety of the visitors. Often, Webmasters are surprised when their Web sites are unexpectedly blocked in a certain country. If a large number of visitors are unable to access the site, the site operator may also face economic problems. Losing your Web site content or server, or having to set up a new server can also be disturbing and frustrating.

This chapter intends to gather a checklist of good practices and advice to have in mind when running your Web site.

PROTECT YOUR WEBSITE

- Always **schedule automated backups** (files and database) on at least one another physical machine. Be sure to know how to restore it.
- **Monitor your traffic** to learn something about the countries your visitors come from. You can use geo location databases to make a guess about which country an IP address is located in. If you notice a major drop in traffic from a specific country, your Web site may have been blocked. You can share this with geographical blocked Web sites databases, like Herdict (https://www.herdict.org/web).
- **Secure your Web site**, especially if you use a CMS (Content Management System). Always install the latest stable updates to fix security flaws.
- **Secure your Web server software** with high level security settings (you can find plenty of online resources about how to secure Linux Web servers).
- Register (or transfer) your domain name to **another DNS provider** which is not your hosting provider. In case of attack on your current provider, you will be able to easily point your domain name to a new hosting provider.
- You may also want to create a **mirror server** running as a standby to which you can switch easily. Learn how to switch your DNS entries to the mirror server.
- Consider **hosting your website in a foreign country**, where the content is less controversial and clearly legally protected. This may imply only a small additional delay in page load time (usually a few milliseconds) for your visitors and may save you a lot of trouble if you are located in a country where you web site's content is considered very controversial.
- **Test and optimize your website** with the main circumvention tools your visitors are likely to use. Check and fix any broken pages or features. Ideally, make your website usable to visitors without JavaScript or plugins, since these may be unavailable or broken when people are using proxies.
- **Avoid using FTP** to upload your files. FTP sends your password over the Internet unencrypted, making it easy for eavesdroppers to steal your login credentials. Consider using SFTP (File Transfer Protocol over SSH), SCP, or secure WebDAV (over HTTPS) instead.
- **Use alternative ports** to access your back-end. Hackers usually run automatic scans on standard ports to detect vulnerabilities. Consider changing your ports to non-standard values (such as SSH) to minimize the risks of these attacks.
- **Protect your server against brute-force attacks** by installing a tool such as DenyHosts on your server (http://denyhosts.sourceforge.net) to protect your server by blacklisting IPs that attempt unsuccessful logins more than a certain amount of times.

PROTECT YOURSELF

Here are some tips to prevent potential personal harm, if staying anonymous as a webmaster is important for you.

- Use an anonymous e-mail address and name which is never associated with your real identity.
- If you own a dedicated domain name, you can record dummy entries in the **WHOIS** public database by using a service often called "WHOIS proxy", "WHOIS protect" or "domain privacy".
- Use a service like Tor to stay anonymous when updating your Web site.

PROTECT YOUR VISITORS

Apart from protecting your Web site and yourself, it is also important to protect the visitors from potential third party monitoring, especially if they submit content to your website.

- **Deploy HTTPS** so your users can access your site over an encrypted connection, to make it more difficult to look automatically at the content which is being transferred and to assure your identity. Ensure that your HTTPS configuration covers your entire site and that you use other best practices for HTTPS configuration. You can find information on how to deploy it correctly on *https://www.eff.org/pages/how-deploy-https-correctly and also try the automated tests at https://www.ssllabs.com/ for many technical parameters.*
- **Minimize retained data** in your logs. Avoid saving IP addresses or any personal data related to your visitors longer than necessary.

- **Encrypt critical user data** such as passwords, for example using salted hashes.
- External services like **Google Analytics** or other third-party content like ad networks are difficult to control. Avoid them.
- Create a **light and secure version** of your Web site, without any Flash or Javascript embedded code, compliant with Tor and low-bandwidth connections.

EDUCATE YOUR VISITORS

- **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.

SHARE CIRCUMVENTION TOOLS WITH YOUR VISITORS

- **Host Web proxy instances** (such as SabzProxy or Glype Proxy). Share them with your visitors, by email, through your social networks.
- **Send out psiphon invitations** if you have an account on a private node
- **Install other kinds of Web and application proxies** if you own a dedicated server and share it.
- **Link** to this manual or relevant circumvention tools from your website.

MULTIPLY CHANNELS OF DISTRIBUTION

Webmasters can and should take different actions in order to spread their content as much as possible, to prevent being shut down or blocked.

- **Set up a newsletter**, and send regular updates of new content by e-mail. You will still be able to reach users when they are not able to visit your Web site anymore.
- **Set up a RSS feed** and make sure it contains full articles and not only excerpts (snippets). This way your content can be parsed very easily by third party websites and applications such as Google Reader, which can be used to read your content where direct access is blocked.
- **Share your content on popular social networking platforms**, such as Facebook or Twitter, which may be hard to block.
- **Spread the content** as much as possible. Make your content available for download. Wikipedia, for example distributes its entire content freely as a database dump which can used to easily create new mirror Web sites with the same content elsewhere.
- Consider **publishing your articles under an open license** (like GPL or Creative Commons) which allows everyone to reuse your content and create mirrors.
- Mirror your files on free **sharehosting services** like Rapidshare.com or Megaupload.com and **peer-to-peer** filesharing software like Bittorrent.
- Configure your Web server to also serve content on **different ports** than the standard ports 80 (*http*) and 443 (*https*).
- **Offer an API** (application programming interface) which allows others to access your content automatically via third-party software such as Twitter or Wikipedia does.

REDUCE YOUR PAGE LOAD TIME

Reducing your page load time not only will save you some bandwidth and money, but will also help your visitors coming from developing countries to access your information better. A good list of best practices for speeding up your website can be found at http://developer.yahoo.com/performance/rules.html and https://code.google.com/speed/page-speed/.

- **Adopt a minimalist style**. Consider keeping images to a minimum, and use CSS to style your layout. A good introduction to CSS can be found at http://www.w3schools.com/css/css_intro.asp.
- **Optimize your images**. Use programs like OptiPNG (http://optipng.sourceforge.net/) to make your pictures load faster by optimizing them for the Web. Also, never scale images with HTML if you don't need to (i.e. if you need a 60x60 image then resize it directly, rather than using HTML).
- **Reduce Java, JavaScript, Flash** and other content that runs in the client's computer to a minimum. Remember that some Internet cafés disable this kind of content for security reasons. Make sure that the information you want to convey is displayed in pure HTML.
- **Use external files for your CSS and JavaScript**. If you have a certain CSS style or JavaScript that is recurrent in your Web site, consider saving it in a separate file and calling it in the header of your Web page. This will allow your client's browser to cache the files, and they will not have to download all this content each time they visit a Web page on your site.
- **Minify your code**. Remove any unnecessary break lines and spaces. Some tools that do this automatically can be found at http://javascriptcompressor.com
- **Reduce the number of server requests to a minimum**. If you have a dynamic Web site but the content doesn't change really frequently, you may want to install some cache extensions that will provide your users with a static version of your content, thus significantly reducing the number of requests to your database.

APPENDICES

39. 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 NY Times 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

40. TEN THINGS

by Roger Dingledine, project leader for The Tor Project

As more countries crack down on Internet use, people around the world are turning to anti-censorship software that lets them reach blocked websites. Many types of software, also known as **circumvention** tools, have been created to answer the threat to freedom online. These tools provide different features and levels of security, and it's important for users to understand the trade-offs.

This article lays out ten features you should consider when evaluating a circumvention tool. The goal isn't to advocate for any specific tool, but to point out what kind of tools are useful for different situations. I've chosen the order of features based on ease of presentation; so you shouldn't conclude the first feature is the most critical.

Internet-based circumvention software consists of two components: a *relaying* component and a *discovery* component. The relaying component is what establishes a connection to some server or **proxy**, handles **encryption**, and sends traffic back and forth. The discovery component is the step before that the process of finding one or more reachable addresses.

Some tools have a simple relaying component. For example, if you're using an open proxy, the process of using the proxy is straightforward: you configure your web browser or other application to use the proxy. The big challenge for open proxy users is finding an open proxy that's reliable and fast. On the other hand, some tools have much more sophisticated relaying components, made up of multiple proxies, multiple layers of encryption, and so on.

One caveat to start out: I'm an inventor and developer of a tool called Tor that is used both for privacy and for circumvention. While my bias for more secure tools like Tor shows through here based on which features I've picked (meaning I raise issues that highlight Tor's strengths and that some other tool developers may not care about), I have also tried to include features that other tool developers consider important.

1. Has a diverse set of users

One of the simplest questions you can ask when looking at a circumvention tool is who else uses it. A wide variety of users means that if somebody finds out you are using the software, they can't conclude much about why you're using it. A privacy tool like Tor has many different classes of users around the world (ranging from ordinary people and human rights activists to corporations, law enforcement, and militaries) so the fact that you have Tor installed doesn't give people much additional information about who you are or what sorts of sites you might visit. On the other hand, imagine a group of Iranian bloggers using a circumvention tool created just for them. If anybody discovers that one of them is using it, they can easily guess why.

Beyond technical features that make a given tool useful to a few people in one country or people all over the world, marketing plays a big role in which users show up. A lot of tools spread through word of mouth, so if the first few users are in Vietnam and they find it useful, the next users will tend to be from Vietnam too. Whether a tool is translated into some languages but not others can also direct (or hamper) which users it will attract.

2. Works in your country

The next question to consider is whether the tool operator artificially restricts which countries can use it. For several years, the commercial Anonymizer.com made its service free to people in Iran. Thus connections coming from Anonymizer's servers were either paying customers (mostly in America) or people in Iran trying to get around their country's filters.

For more recent examples,
Your-Freedom restricts free usage to a few countries such as Burma, while at times systems like Freegate and UltraSurf outright block connections from all but the few countries that they care to serve (China and, in the case of Ultrasurf recently, Iran). On the one hand, this strategy makes sense in terms of limiting the bandwidth costs. But on the other hand, if you're in Saudi Arabia and need a circumvention tool, some otherwise useful tools are not an option for you.

3. Has a sustainable network and software development strategy

If you're going to invest the time to figure out how to use a given tool, you want to make sure it's going to be around for a while. There are several ways that different tools ensure their long-term existence. The main three approaches are the use of volunteers, making a profit, and getting funds from sponsors.

Networks like Tor rely on volunteers to provide the relays that make up the network. Thousands of people around the world have computers with good network connections and want to help make the world a better place. By joining them into one big network, Tor ensures that the network is independent from the organization writing the software; so the network will be around down the road even if The Tor Project as an entity ceases to exist. Psiphon takes the second approach: collecting money for service. They reason that if they can create a profitable company, then that company will be able to fund the network on an ongoing basis. The third approach is to rely on sponsors to pay for the bandwidth costs. The Java Anon Proxy or JAP project relied on government grants to fund its bandwidth; now that the grant has finished they're investigating the for-profit approach. Ultrareach and Freegate use the sponsor model to good effect, though they are constantly hunting for more sponsors to keep their network operational.

After asking about the long-term survival of the network, the next question to ask is about sustainability of the software itself. The same three approaches apply here, but the examples change. While Tor's network is operated by volunteers, Tor relies on sponsors (governments and NGOs) to fund new features and software maintenance. Ultrareach and Freegate, on the other hand, are in a more sustainable position with respect to software updates: they have a team of individuals around the world, mostly volunteers, devoted to making sure the tools are one step ahead of censors.

Each of the three approaches can work, but understanding the approach a tool uses can help you predict what problems it might encounter in the future.

4. Has an open design

The first step to transparency and reusability of the tool's software and design is to distribute the software (not just the client-side software, but also the server-side software) under an open source license. Open source licenses mean that you can examine the software to see how it really operates, and you have the right to modify the program. Even if not every user takes advantage of this opportunity (many people just want to use the tool as-is), providing the option makes it much more likely that the tool will remain safe and useful. Otherwise, you are forced to trust that a small number of developers have thought of and addressed every possible problem.

Just having an open source licence is not enough. Trustworthy circumvention tools need to provide clear, complete documentation for other security experts not just about how it's built but what features and goals its developers aimed for. Do they intend for it to provide privacy? What kind and against what attackers? In what way does it use encryption? Do they intend for it to stand up to attacks from censors? What kind of attacks do they expect to resist and why will their tool resist them? Without seeing the source code *and* knowing what the developers meant for it to do, it's harder to decide whether there are security problems in the tool, or to evaluate whether it will reach its goals.

In the field of cryptography, Kerckhoffs' principle explains that you should design your system so the amount you need to keep secret is as small and well-understood as possible. That's why crypto algorithms have keys (the secret part) and the rest can be explained in public to anybody. Historically, any crypto design that has a lot of secret parts has turned out to be less safe than its designers thought. Similarly, in the case of secret designs for circumvention tools, the only groups examining the tool are its original developers and its attackers; other developers and users who could help to make it better and more sustainable are left out.

Ideas from one project could be reusable beyond that project's lifetime. Too many circumvention tools keep their designs secret, hoping that government censors will have a harder time figuring out how the system works, but the result is that few projects can learn from other projects and the field of circumvention development as a whole moves forward too slowly.

5. Has a decentralized architecture

Another feature to look for in a circumvention tool is whether its network is centralized or decentralized. A centralized tool puts all of its users' requests through one or a few servers that the tool operator controls. A decentralized design like Tor or JAP sends the traffic through multiple different locations, so there is no single location or entity that gets to watch what websites each user is accessing.

Another way to look at this division is based on whether the *trust* is centralized or decentralized. If you have to put all your trust in one entity, then the best you can hope for is "privacy by policy" meaning they have all your data and they promise not to look at it, lose it, or sell it. The alternative is what the Ontario Privacy Commissioner calls "privacy by design" meaning the design of the system itself ensures that users get their privacy. The openness of the design in turn lets everybody evaluate the level of privacy provided.

This concern isn't just theoretical. In early 2009 Hal Roberts from the Berkman Center ran across a FAQ entry for a circumvention tool that offered to sell its users' clicklogs. I later talked to a different circumvention tool provider who explained that they had all the logs of every request ever made through their system "because you never know when you might want them."

I've left out the names of the tools here because the point is not that some tool providers may have shared user data; the point is that any tool with a centralized trust architecture *could* share user data, and its users have no way to tell whether it's happening. Worse, even if the tool provider means well, the fact that all the data flows through one location creates an attractive target for other attackers to come snooping.

Many of these tools see circumvention and user privacy as totally unrelated goals. This separation isn't necessarily bad, as long as you know what you're getting into for example, we hear from many people in censoring countries that just reading a news website isn't going to get you locked up. But as we've been learning in many other contexts over the past few years, large databases of personal information tend to end up more public than we'd like.

6. Keeps you safe from websites too

Privacy isn't only about whether the tool operator can log your requests. It's also about whether the websites you visit can recognize or track you. Remember the case of Yahoo turning over information about one of its Chinese webmail users? What if a blog aggregator wants to find out who's posting to a blog, or who added the latest comment, or what other websites a particular blogger reads? Using a safer tool to reach the website means the website won't have as much to hand over.

Some circumvention tools are safer than others. At one extreme are open proxies. They often pass along the address of the client with their web request, so it's easy for the website to learn exactly where the request is coming from. At the other extreme are tools like Tor that include client-side browser extensions to hide your browser version, language preference, browser window size, time zone, and so on; segregate cookies, history, and cache; and prevent plugins like Flash from leaking information about you.

This level of application-level protection comes at a cost though: some websites don't work correctly. As more websites move to the latest "web 2.0" fads, they require more and more invasive features with respect to browser behavior. The safest answer is to disable the dangerous behaviors but if somebody in Turkey is trying to reach YouTube and Tor disables his Flash plugin to keep him safe, his videos won't work.

No tools have solved this trade-off well yet. Psiphon manually evaluates each website, and programs its central proxy to rewrite each page. Mostly they do this rewriting not for privacy but to make sure all links on the page lead back to their proxy service, but the result is that if they haven't manually vetted your destination site yet, it probably won't work for you. As an example, they seem to be in a constant battle to keep up with Facebook's changing front page. Tor currently disables some content that is probably safe in practice, because we haven't figured out a good interface to let the user decide in an informed way. Still other tools just let through any active content, meaning it's trivial to unmask their users.

7. Doesn't promise to magically encrypt the entire Internet

I should draw a distinction here between encryption and privacy. Most circumvention tools (all but the really simple ones like open proxies) encrypt the traffic between the user and the circumvention provider. They need this encryption to avoid the keyword filtering done by such censors as China's firewall. But none of the tools can encrypt the traffic between the provider and the destination websites if a destination website doesn't support encryption; there's no magic way to make the traffic encrypted.

The ideal answer would be for everybody to use https (also known as SSL) when accessing websites, and for all websites to support https connections. When used correctly, https provides encryption between your web browser and the website. This "end-to-end" encryption means nobody on the network (not your ISP, not the backbone Internet providers, and not your circumvention provider) can listen in on the contents of your communication. But for a wide variety of reasons, pervasive encryption hasn't taken off. If the destination website doesn't support encryption, the best you can do is 1) not send identifying or sensitive information, such as a real name in a blog post or a password you don't want other people to learn, and then 2) use a circumvention tool that doesn't have any trust bottlenecks that allow somebody to link you to your destinations despite the precautions in step 1.

Alas, things get messy when you can't avoid sending sensitive info. Some people have expressed concern over Tor's volunteer-run network design, reasoning that at least with the centralized designs you know who runs the infrastructure. But in practice it's going to be strangers reading your traffic either way. The trade-off is between volunteer strangers who don't know it's you (meaning they can't target you), or dedicated strangers who get to see your entire traffic profile (and link you to it). Anybody who promises "100% security" is selling something.

8. Provides consistently good latency and throughput

The next feature you might look for in a circumvention tool is speed. Some tools tend to be consistently fast, some consistently slow, and some provide wildly unpredictable performance. Speed is based on many factors, including how many users the system has, what the users are doing, how much capacity there is, and whether the load is spread evenly over the network.

The centralized-trust designs have two advantages here. First, they can see all their users and what they're doing, meaning they have a head start at spreading them out evenly and at discouraging behaviors that tax the system. Second, they can buy more capacity as needed, so the more they pay the faster the tool is. The distributed-trust designs on the other hand have a harder time tracking their users, and if they rely on volunteers to provide capacity, then getting more volunteers is a more complex process than just paying for more bandwidth.

The flip side of the performance question is flexibility. Many systems ensure good speed by limiting what their users can do. While Psiphon prevents you from reaching sites that they haven't manually vetted, Ultrareach and Freegate actually actively censor which destination websites you're allowed to reach so they can keep their bandwidth costs down. Tor, by contrast, lets you access any protocol and destination, meaning for example you can instant message through it too; but the downside is that the network is often overwhelmed by users doing bulk transfer.

9. Makes it easy to get the software and updates

Once a circumvention tool becomes well-known, its website is going to get blocked. If it's impossible to get a copy of the tool itself, who cares how good it is? The best answer here is to not require any specialized client software. Psiphon, for example, relies on a normal web browser, so it doesn't matter if the censors block their website. Another approach is a tiny program like Ultrareach or Freegate that you can instant message to your friends. Option three is Tor's Browser Bundle: it comes with all the software you need preconfigured, but since it includes large programs like Firefox it's harder to pass around online. In that case distribution tends to be done through social networks and USB sticks, or using our e-mail autoresponder that lets you download Tor via Gmail.

Then you need to consider the trade-offs that come with each approach. First, which operating systems are supported? Psiphon does well here too by not requiring any extra client software. Ultrareach and Freegate are so specialized that they only work on Windows, whereas Tor and its accompanying software can run pretty much everywhere. Next, consider that client-side software can automatically handle failover from one proxy to the next, so you don't need to manually type in a new address if your current address disappears or gets blocked.

Last, does the tool have a track record for responding to blocking? For example, UltraSurf and Freegate have a history of releasing quick updates when the current version of their tool stops working. They have a lot of experience at this particular cat-and-mouse game, so it's reasonable to assume they're ready for the next round. Along these lines, Tor prepared for its eventual blocking by streamlining its network communications to look more like encrypted web browsing, and introducing unpublished "bridge relays" that are harder for an attacker to find and block than Tor's public relays. Tor tries to separate software updates from proxy address updates. If the bridge relay you're using gets blocked, you can stick with the same software and just configure it to use a new bridge address. Our bridge design was put to the test in China in September of 2009, and tens of thousands of users seamlessly moved from the public relays to bridges.

10. Doesn't promote itself as a circumvention tool

Many circumvention tools launch with a huge media splash. The media loves this approach, and they end up with front page articles like "American hackers declare war on China!" But while this attention helps attract support (volunteers, profit, sponsors), the publicity also attracts the attention of the censors.

Censors generally block two categories of tools: 1) the ones that are working really well, meaning they have hundreds of thousands of users, and 2) the ones that make a lot of noise. In many cases censorship is less about blocking all sensitive content and more about creating an atmosphere of repression so people end up self-censoring. Articles in the press threaten the censors' *appearance* of control, so they are forced to respond.

The lesson here is that we can control the pace of the arms race. Counterintuitively, even if a tool has many users, as long as nobody talks about it much it tends not to get blocked. But if nobody talks about it, how do users learn about it? One way out of the paradox is to spread through word of mouth and social networks rather than the more traditional media. Another approach is to position the tool in a different context; for example, we present Tor primarily as a privacy and civil liberties tool rather than a circumvention tool. Alas, this balancing act is tough to maintain in the face of increasing popularity.

Conclusion

This article explains some of the issues you should consider when evaluating the strengths and weaknesses of circumvention tools. I've intentionally avoided drawing up a table of different tools and scoring them on each category. No doubt somebody will do that eventually and sum up how many checkmarks each tool gets, but the point here is not to find the "best" tool. Having a diversity of circumvention tools in wide use increases robustness for all the tools, since censors have to tackle every strategy at once.

Last, we should keep in mind that technology won't solve the whole problem. After all, firewalls are *socially* very successful in these countries. As long as many people in censored countries are saying "I'm so glad my government keeps me safe on the Internet," the social challenges are at least as important. But at the same time, there are people in all of these countries who want to learn and spread information online, and a strong technical solution remains a critical piece of the puzzle.

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.

Originally prepared for the March 2010 "Index on Censorship", then adapted for the July 2010 "China Rights Forum" (Chinese translation). Last updated 25 May 2010.

41. FURTHER RESOURCES

Bypassing Internet censorship is a big topic, with dozens of tools and services available. There are also lots of things to consider if you want your **circumvention** activities to be harder to detect or to **block** in the future, if you want to achieve anonymity in your Internet use, or if you want to help other people circumvent censorship. Here are some recommended resources for further study about related matters. (Some of these resources may be unavailable or blocked in some places.)

MANUALS AND GUIDES

Circumventing Internet censorship

- 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/

Computer security advice for activists

- 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

Studies on Internet censorship

- 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

ORGANIZATIONS THAT WORK ON DOCUMENTING, FIGHTING OR CIRCUMVENTING INTERNET RESTRICTIONS

- 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)

OPEN WEB PROXIES AND APPLICATION PROXIES

- 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

CIRCUMVENTION SOLUTIONS AND SERVICE OPERATORS

- 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/

A list of commercial VPN providers

- http://en.cship.org/wiki/VPN

Socksification software (to make non-proxy aware software work with a SOCKS proxy)

- 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

42. LICENSE

AUTHORS

All chapters © the contributors unless otherwise noted below.

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
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
© Freerk Ohling 2010
Modifications:
Roberto Rastapopoulos 2010
Zorrino Zorrinno 2010

USING TOR BROWSER BUNDLE
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING TOR IM BROWSER BUNDLE
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008, 2009
Alice Miller 2008
Freerk Ohling 2008
Sahal Ansari 2008
Sam Tennyson 2008

Tom Boyle 2008
Tomas Krag 2008

HTTP PROXIES
© adam hyde 2008
Modifications:
Alice Miller 2008
Freerk Ohling 2008, 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

USING A WEB PROXY
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

WHAT IS CIRCUMVENTION
© Ronald Deibert 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Sam Tennyson 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008

WHAT IS VPN?
© 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

WHO CONTROLS THE NET
© adam hyde 2008
Modifications:
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tomas Krag 2008

FLOSS MANUALS

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