



:: [portada](#) :: [Conocimiento Libre](#) ::

16-11-2004

Como evitar la censura en Internet

Freerk

Freerk<freerk@gmx.net> (escribe en Inglés, Aleman or Español), last updated 2003-08-19

traducido por daexmaIE . Este artículo es una traducción del [original en Inglés](#) que su autor irá completando y actualizando con el tiempo.

Se ha pretendido que permanezca lo más fiel posible a la versión original.

[Introducción](#)

- [1.1 Acerca de la censura en Internet](#)
- [1.2 ¿Por qué escribo esto?](#)
- [1.3 ¿Dónde puedo conseguir este artículo?](#)

[2. Puntos débiles](#)

[3. Diferentes modos de censura](#)

- [3.1 Bloquear URL's usando el servidor DNS](#)
- [3.2 Uso obligado de un servidor proxy / proxy transparente](#)
- [3.3 Filtrar palabras](#)
- [3.4 Bloqueando puertos](#)
- [3.5 Software en el PC cliente \(protección para la navegación de menores, e.t.c.\)](#)
 - [3.5.1 NetNanny](#)
 - [3.5.2 CyberSitter](#)
 - [3.5.3 AOL Parental Control](#)
 - [3.5.4 CyberPatrol](#)
 - [3.5.5. SurfWatch / SurfControl](#)
- [3.6 Software en el servidor \(dentro de la red.\)](#)
 - [3.6.1 Bess/N2H2](#)
 - [3.6.2 DansGuardian](#)
 - [3.6.3 WebSense](#)
 - [3.6.4 WebWasher](#)
 - [3.6.5 SmartFilter](#)
 - [3.6.6 squidGuard](#)
- [3.7 Lista blanca](#)
- [3.8 Bloqueando IP's en el router](#)



4. Diferentes maneras de pasar la censura.

- [4.1 Usando un ISP diferente](#)
- [4.2 Usando un servidor DNS que no use la censura](#)
- [4.3 Usando un servidor proxy que no use la censura](#)
 - [4.3.1 Proxy standard](#)
 - [4.3.2 Proxy que usan puertos no comunes](#)
 - [4.3.3 Socks proxy](#)
 - [4.3.4 Montar nuestro propio servidor proxy](#)
 - [4.3.5 Proxys especiales / tunnel tools](#)
 - [4.3.5.1 JAP](#)
 - [4.3.5.2 Httpport](#)
 - [4.3.5.3 Localproxy](#)
 - [4.3.5.4 HttpTunnel](#)
- [4.3.6 Wingates](#)
- [4.4 Usando un shell](#)
- [4.5 Usando un proxy web](#)
 - [4.5.1 Proxys web standard](#)
 - [4.5.2 Proxys web con URL's cifradas](#)
 - [4.5.3 Proxys web bajo conexión segura \(SSL\)](#)
 - [4.5.4 Traductores, warpers, e.t.c que pueden ser usados como proxy](#)
- [4.6 Obtener las páginas web mediante E-mail](#)
- [4.7 Usando esteganografía](#)
 - [4.7.1 Camera/Shy](#)
- [4.8 Usando un proxy especial como si de un programa P2P se tratase](#)
 - [4.8.1 Peek a Booty](#)
 - [4.8.2 Freenet](#)
 - [4.8.3 MojoNation](#)
 - [4.8.4 TriangleBoy](#)
 - [4.8.5 Six/Four](#)
 - [4.8.6 Freenet China](#)
 - [4.8.7 Entropy](#)
- [4.9 Servicios especiales](#)
 - [4.9.1 Usenet](#)
 - [4.9.2 Games](#)
 - [4.9.3 FTP](#)
 - [4.9.4 Instant Messenger](#)
 - [4.9.4.1 ICQ](#)
 - [4.9.4.2 MSN Messenger](#)
 - [4.9.4.3 AIM](#)
 - [4.9.4.4 Yahoo Messenger](#)
 - [4.9.5 Programas para compartir archivos](#)



[5. Cómo publicar la información](#)

[6. Apéndice](#)

- [6.1 Enlaces](#)
- [6.1.1 Otros tutoriales para evitar la cesura](#)
- [6.1.2 Otros sitios relacionados con la censura en Internet](#)
- [6.1.3 Dónde conseguir proxys](#)

[volver arriba](#) 1. Introducción

- 1.1 Acerca de la censura en Internet

En los últimos 10 años Internet a crecido mucho y rápido. Es un entresijo de miles de pequeñas redes todas unidas entre sí. Millones de ordenadores están conectados y esto es así básicamente sin control ni propiedad de ningún gobierno o compañía. No hay leyes, cualquiera puede poner su página web online, a la cual podrá acceder cualquier persona en el mundo sentada enfrente de un ordenador conectado a Internet. Creo que esto puede y, de hecho, cambiará el mundo que conocemos hoy.

Pero hay muchos gobiernos que piensan que este acceso ilimitado a la información es peligroso para sus ciudadanos. Estos son por ejemplo China, Arabia Saudí, Australia, Bahrain, Cuba, Jordania, Túnez, Burma, Singapur, Uzbekistan, Yemen, Kuwait, Vietnam, Siria, Irán, Emiratos Árabes Unidos y partes de África y Alemania. Este rango va desde desde un simple bloqueo DNS de solo 2 sitios web nazis en parte de Alemania, hasta una oficina gubernamental con 30.000 empleados trabajando exclusivamente en bloquear miles de sitios web, servicios y puertos en China.

Debido a que los métodos de bloqueo son diferentes, también lo son los métodos para evitarlos. Intentaré mostrar cómo acceder a los sitios web de Amnistía Internacional, BBC, Google y otros sitios bloqueados en tu país. Este artículo está hecho en un HTML básico para que pueda ser visualizado incluso con un viejo ordenador. Por favor, comparte esta información, enlaza el sitio, cópialo, crea un espejo, imprímelo (no se ha "escondido" ningún enlace por lo que ninguno se perderá si lo imprimes) y enséñalo a tus amigos y familiares.

- 1.2 ¿Por qué escribo esto?

Bien, yo vivo en Alemania, la cual no es muy famosa por su censura, pero el gobierno local de un Estado Aleman (NRW) intenta introducir la censura bloqueando 2 sitio nazis norteamericanos. No es que me guste esa gente, pero en mi opinión ningún gobierno ni administrador de sistemas tiene el derecho a elegir a que información puede tener acceso una persona, ¿qué sitio será el siguiente?, ¿quién decide que sitios serán bloqueados?. Además, mi instituto bloquea algunos sitios, lo cual hizo interesarme en el tema.



- 1.3 Cómo puedo conseguir este artículo

Como estás leyendo esto, puede que lo hayas encontrado por cualquier sitio. Puedes obtener la versión mas reciente desde:

European mirror: <http://www.zensur.freerk.com/> - (Lambdanet - Erfurt, Germany)

American mirror: <http://nocensor.opennetinitiative.net/> - (University of Toronto, ON, Canada)

Asian/Pacific mirror: <http://tokyo.cool.ne.jp/cship/> (Infoseek - Tokyo, Japan)

SSL mirror: <https://secure.sslpowered.com/bpass/> (Netfirms, Toronto, ON, Canada)

Dynamic IP mirror: <http://maybe-yours.dyndns.org/> (please [email](#) me)

eMail autoresponder: index.htm@zensur.freerk.com (solo tienes que enviar un e-mail vacío, y automáticamente recibirás el original de este artículo en HTML plano.)

[volver arriba](#) 2. Puntos débiles

TU debes decidir si saltarte la censura en Internet o no, yo solo te mostraré como pero no puedo aceptar ninguna responsabilidad por ello. En muchos países podrías ir a la cárcel si te cogen, en muchas compañías serías despedido y en algunas escuelas expulsado.

Por supuesto los censores no solo bloquean el tráfico de Internet, también lo observan (en países / compañías con una pequeña población en Internet) e intentan averiguar quién y cómo está saltándose su cortafuegos. Una manera fácil de averiguar esto, es simplemente buscando algún indicador en los logfiles.

-

Justo después de que la conexión ha Internet es establecida, el usuario es conectado a un servidor único y permanece conectado a él durante todo el tiempo que esté conectado.

-

Qué hace un usuario después de obtener un mensaje de "acceso denegado" de su censor (abrir un sitio especial, usar el chat, conectarse a un servidor especial).

¡Intenta no ser cogido de esta manera!.



Mas información: <http://www.peacefire.org/circumventor/list-of-possible-weaknesses.html>
<http://peek-a-bouty.org/pbhtml/downloads/ResponseToLopwistcic.htm>

[volver arriba](#) 3. Diferentes modos de censura

Hay diferentes soluciones para censurar el tráfico en Internet, a veces se combinan 2 o más. Por favor escríbeme a freerk@gmx.net con los métodos que son usados en tu país, qué ISP estás usando y la manera que usas para evitarlo, sería de mucha utilidad para otros usuarios.

- 3.1 Bloquear URL's usando el servidor DNS

Esto por ejemplo es usado por algunos proveedores alemanes. Es un método fácil y barato de censura y lo mismo es aplicable a cómo evitarlo. Primero explicaré qué es un Domain Name System (Servidor de Nombres de Dominio). Cada ordenador en Internet tiene un identificador único, similar a un número de teléfono, esto es, 4 números del 0 al 255 separados por un punto. Por ejemplo, 62.141.48.209 es la dirección IP para www.freerk.com. Como recordar esta clase de números es muy difícil, se inventó el DNS, este servicio asocia una URL con su dirección IP. Si tecleas www.freerk.com en tu navegador, la petición será enviada a un servidor DNS, este te es asignado automáticamente por tu ISP cuando te conectas a Internet. Muchas de las direcciones ya estarán en su caché, y el servidor DNS devolverá la dirección IP asociada a la URL, si la caché del servidor DNS no contiene la información referente a la URL que has solicitado, buscará en los 13 servidores principales (comunes para todo el mundo), en los cuales están almacenadas todas las direcciones. Si el servidor DNS de tu proveedor está censurando, simplemente no te enviará la dirección IP, no te enviará nada o te enviará a una dirección con un mensaje de "lo siento...";

- 3.2 Uso obligado de un servidor proxy / proxy transparente

Debes especificar un servidor proxy en la configuración de tu navegador para poder conectarte a Internet. A veces un ISP usa un proxy transparente, con lo cual no puedes saber fácilmente si existe un proxy o no. Cualquier petición que envías o recibes desde Internet pasa primero por este servidor y después es redireccionada a ti (bueno, o no...)

- 3.3 Filtrar palabras

Esto significa que todo el tráfico de Internet pasa por el servidor del censor, el cual escanea el contenido en busca de "malas palabras". Este tipo de filtrado es usado en escuelas, bibliotecas y compañías, si el sitio contiene malas palabras es bloqueado. La persona que ofrece la información bloqueada puede prevenir la censura "escondiendo" el contenido dentro de imágenes; para el usuario prácticamente no hay diferencia, pero es muy difícil para un programa de ordenador "leer" el texto contenido en una imagen. Tampoco el tráfico cifrado SSL (URL's que comienzan por <https://...>) puede ser escaneado fácilmente. Puedes comprobar que palabras serán bloqueadas en tu conexión en <http://www.zensur.freerk.com/kword/>, allí podrás introducir las palabras que quieras comprobar, luego pincha en "send", y si recibes el mensaje "You entered *****" todo está correcto, pero si obtienes un mensaje de error, es que esa palabra está siendo bloqueada.

- 3.4 Bloqueando puertos

Los puertos son como puertas para un servicio especial para un servidor o PC, van desde 0 a 65535;



los puertos comunes son del 0 al 1024, estos son los "well known ports". Puedes obtener la lista oficial desde <http://www.iana.org/assignments/port-numbers>. Si un censor bloquea un puerto, todo el tráfico dirigido a ese puerto se rechazará y será inútil para ti. Muchos censores bloquean los puertos 80, 1080, 3128 y 8080, porque son los puertos más usados por los proxy's. Como todos los proxy's comunes serán inútiles para ti, deberás encontrar proxys que escuchen en puertos no comunes y estos son difíciles de encontrar.

Puedes comprobar qué puertos están bloqueados en tu conexión simplemente abriendo un consola y escribiendo telnet login.icq.com 80 y pulsando "intro" (el número es el puerto que quieres comprobar); si recibes algún símbolo extraño como respuesta, está correcto, si recibes un "timeout" o algo similar, ese puerto está bloqueado. Aquí están los puertos más importantes para nosotros:

- 20+21 - FTP (file transfer)
- 22 - SSH (secure remote access)
- 23 - telnet (remote access) and also Wingates (special kind of proxies)
- 25 - SMTP (enviar email)
- 53 - DNS (resolves an URL to an IP)
- 80 - HTTP (normal web browsing) y tambien un proxy
- 110 - POP3 (recibir email)
- 443 - SSL (secure HTTPS connections)
- 1080 - Socks proxy
- 3128 - Squid proxy
- 8000 - Junkbuster proxy
- 8080 - un proxy

- 3.5 Software en el PC cliente (protección para la navegación de menores, e.t.c)

Normalmente los programas encargados de censurar son implementados en los servidores por el ISP o por el gobierno, pero en algunos colegios, hogares y en algunas compañías, el software es instalado en cada PC.

Más información:: <http://www.peacefire.org/>
<http://www.cexx.org/censware.htm>
<http://www.epinions.com/cmsw-Kids-Topics-2>
http://www.securiteam.com/securityreviews/Web_blocking_software_can_be_easily_bypassed.html

- 3.5.1 NetNanny

Más información:: <http://www.netnanny.com/index.html>
http://peacefire.org/censorware/Net_Nanny/

- 3.5.2 CyberSitter

Más información:: <http://www.cybersitter.com/>
<http://www.spectacle.org/alert/peace.html>



<http://www.peacefire.org/censorware/CYBERSitter/>

- 3.5.3 AOL Parental Control

Más información:: <http://www.aol.com/info/parentcontrol.html>

- 3.5.4 CyberPatrol

Más información:: <http://www.cyberpatrol.com/>
http://www.peacefire.org/censorware/Cyber_Patrol/

- 3.5.5. SurfControl

Más información:: <http://www.surfcontrol.com/>
<http://peacefire.org/censorware/SurfWatch/>

- 3.6 Software en el servidor (dentro de la red)

Son programas mayormente instalados en servidores de escuelas, bibliotecas, compañías o países con una pequeña población en Internet.

- 3.6.1 Bess/N2H2

Bess es un filtro proxy frecuentemente usado en escuelas, universidades y compañías, que puede ser fácilmente pasado mediante el uso de [proxys web](#).

Más información: http://www.n2h2.com/products/bess_home.php
<http://www.peacefire.org/censorware/BESS/>

- 3.6.2 DansGuardian

Es filtro web de Código Abierto, gratuito para uso no comercial y muy extendido en escuelas, universidades y bibliotecas. Trabaja como un proxy filtrando tanto URL's como palabras (y también con PICS-Srandard). Frecuentemente es usado en máquinas IPCop, sin embargo esto no es del agrado de su autor.

Más información:<http://dansguardian.org/>

- 3.6.3 WebSense



Más información: <http://www.websense.com/>
<http://www.peacefire.org/censorware/WebSENSE/>

- 3.6.4 WebWasher

Más información: <http://www.webwasher.com/>

- 3.6.5 SmartFilter

Más información: <http://www.securecomputing.com/index.cfm?skey=85>
<http://www.peacefire.org/censorware/SmartFilter/>

- 3.6.6 squidGuard

Más información: <http://www.squidguard.org/>

- 3.6.7 new_new

- 3.7 Lista blanca

Muchos filtros en Internet se basan en una "lista negra", lo cual significa que el acceso a todos los sitios está permitido excepto algunos sitios en especial (bueno, a veces hay muchas excepciones...). Una "lista blanca" trabaja de manera opuesta, el acceso a todos los sitios está bloqueado excepto para algunos especiales. Para un ISP normal esto es casi imposible de ofrecer ya que Internet no tendría ningún valor, la lista blanca es usada en terminales de acceso gratuito que están esponsorizados por alguna compañía, la cual, por ejemplo, permite a los usuarios libre acceso a sus sitios de comercio electrónico. Este tipo de filtro es el mas difícil de evitar.

Hace un tiempo, hubo un ISP alemán que ofrecía conexión completamente gratuita a través de un número de teléfono, una vez conectabas solo podías navegar por amazon.de y alrededor de otros 10 sitios de comercio electrónico, pero también podías conectar con los demás clientes del ISP, por ello alguien con tarifa plana conectado a ambos, su ISP normal y al número gratuito instaló un proxy para que todos los usuarios de la línea gratuita pudieran usar ese proxy para conectar con otros sitios.

- 3.8 Bloqueando IP's en el router



[volver arriba](#) 4. Diferentes maneras de pasar la censura

Desde el momento en que no puedas acceder directamente a un servidor bloqueado, deberás enviar tu petición a un servidor no bloqueado que redirija el tráfico al sitio real que quieres visitar. Hay varios tipos de "puertas traseras";

- 4.1 Usando un ISP diferente

Tan fácil como suena, simplemente cambia de Proveedor de Acceso a Internet (ISP, Internet Service Provider), pero la censura funciona en todo el país, por lo que una posibilidad es intentarlo con un ISP fuera del país. Es algo muy caro, pero de esta manera tendrás un acceso normal a Internet y no tendrás que preocuparte de cerca de saltarte filtros, este podría ser un proveedor de acceso telefónico en un país vecino o aún mejor un acceso a Internet vía satélite de 2-vías como <http://www.europeonline.com/>, http://registrierung.tiscali.de/produkte/1400_satellit.php, <http://www.gilat.de/>, <http://www.hns.com/>, <http://www.vsatnet.com/>, <http://www.starband.com/>, <http://www.wildblue.com/>, <http://www.skycasters.com/>, <http://www.directduo.com/>, <http://www.orbitsat.com/>, <http://www.ottawaonline.com/> y más, sólo busca en cualquier buscador por "2-way internet via satellite [tu país o país vecino]";

- 4.2 Usar un servidor DNS que no use censura

Normalmente usarás el servidor DNS de tu ISP para resolver los nombre de dominio, como www.freerk.com a 62.141.48.209, internamente sólo esa dirección IP es usada para enviar y recibir datos en Internet; si tu servidor DNS usa censura, simplemente cambia a otro. En Windows haz clic con el botón derecho del ratón en el Panel de Control sobre el icono de Conexiones de Red... y selecciona propiedades de protocolo TCP/IP. En Linux deberás editar el archivo `/etc/resolv.conf`, usa el servidor que esté mas cerca de tu localización. Si quieres instalar tu propio servidor DNS puedes usar Bind <http://www.isc.org/products/BIND/>. La lista de los 13 servidores DNS principales está aquí <ftp://ftp.rs.internic.net/domain/named.root>; sería bueno añadir los servidores DNS principales alternativos localizados en Europa desde ORSN <ftp://ftp.orsn.org/orsn/orsn.hint>.

Servidores DNS no censurados:

dns2.de.net - 194.246.96.49 (Frankfurt, Germany)
sunic.sunet.se - 192.36.125.2 (Stockholm, Sweden)
master.ns.dns.be - 193.109.126.140 (Leuven, Belgium)
merapi.switch.ch - 130.59.211.10 (Zurich, Switzerland)
prades.cesca.es - 192.94.163.152 (Barcelona, Spain)
michael.vatican.va - 212.77.0.2 (Vatican City, Italy)
dns.inria.fr - 193.51.208.13 (Nice, France)
ns0.ja.net - 128.86.1.20 (London, UK)
nic.aix.gr - 195.130.89.210 (Athens, Greece)
ns.ati.tn - 193.95.66.10 (Tunis, Tunisia)
ns1.relcom.ru - 193.125.152.3 (Moscow, Russia)
trantor.umd.edu - 128.8.10.14 (College Park, MD, USA)
ns1.berkeley.edu - 128.32.136.9 (Berkeley, CA, USA)
merle.cira.ca - 64.26.149.98 (Ottawa, Canada)
ns2.dns.br - 200.19.119.99 (Sao Paulo, Brasil)
ns2.gisc.cl - 200.10.237.14 (Santiago, Chile)



ns.uvg.edu.gt - 168.234.68.2 (Guatemala, Guatemala)
ns1.retina.ar - 200.10.202.3 (Buenos Aires, Argentina)
ns.unam.mx - 132.248.253.1 (Mexico City, Mexico)
ns.wide.ad.jp - 203.178.136.63 (Osaka, Japan)
ns.twnic.net - 192.83.166.11 (Taipei, Taiwan)
ns3.dns.net.nz - 203.97.8.250 (Wellington, New Zealand)
box2.aunic.net - 203.202.150.20 (Melbourne, Australia)

También es posible actuar como servidor DNS manualmente por uno mismo, simplemente usa el servicio ping o traceroute en una máquina no censurada para obtener la IP del servidor deseado, luego usa esa IP en lugar de la URL en tu navegador. Siempre obtendrás una IP, pero acceder a un sitio web vía IP no funciona siempre, porque muchos alojamientos web, alojan 500 o más sitios en un solo servidor con una sola IP, pero funcionará con los grandes sitios.

<http://195.193.168.164/> - Rotterdam, Netherlands (JAVA VISUALROUTE)

<http://www.vs1.ffs-server.de:8000/> - Darmstadt, Germany (JAVA VISUALROUTE)

<http://202.85.153.198:8080/> - Hong Kong (JAVA VISUALROUTE)

<https://www.velia.net/tools/traceroute.php> - Hanau, Germany (HTTPS encrypted)

<http://www.traceroute-gateways.com/> - About 1000 public ping/traceroute gateways sorted by country

<http://www.traceroute.org/> - Another list with public ping/traceroute services sorted by country

- 4.3 Usar un servidor proxy que no use censura

Puedes intercalar un servidor proxy entre tu conexión a Internet y el sitio que deseas visitar. Lo que hacemos es enviar la petición a ese servidor proxy, el cual solicitará la página y nos la enviará,. Normalmente este tipo de servidores guardan las páginas solicitadas en su caché, por lo que la próxima vez que solicitemos la misma página nos la servirá directamente desde su caché, lo cual resulta mas rápido y barato. Para los ojos de nuestro ISP/Gobierno sólo estamos conectados al proxy, no pueden ver fácilmente que estamos conectados a un "mal sitio", pero a veces los puertos proxy comunes (80, 1080, 3128 y 8080) están bloqueados. En ese caso debemos usar



aquellos que escuchan en puertos no comunes.

- 4.3.1 Standard proxy

Puedes encontrar proxys comunes fácilmente en Internet, casi todos los proveedores ofrecen uno a sus clientes. Aquí tienes algunos en el formato ampliamente usado de `"hostname:port"`. Estos proxys son mayoritariamente no anónimos.

www-proxy.t-online.de:80 (Bonn, Germany)
cair.res.in:80 (Bangalore, India)
esjv.com.hk:80 (Hong Kong)
mail.unisol.com.ar:80 (Argentina)
souththornlieps.wa.edu.au:3128 (Perth, Australia)
proxy.olimpo.com.br:8080 (Rio de Janeiro, Brasil)
203.77.236.3:8080 (Jakarta, Indonesia)

- 4.3.2 Proxys que usan puertos no comunes

Debido al hecho de que muchos censores bloquean el acceso a los puertos proxy comunes, para evitar este bloqueo debemos usar proxys que escuchan en puertos no comunes, por ejemplo 8000 para Junkbuster proxy o 6588 para AnalogX proxy. Puedes obtener una lista de este tipo de proxys actualizada semanalmente en <http://www.zensur.freerk.com/list.txt> o vía e-mail de respuesta automática en list.txt@zensur.freerk.com.

- 4.3.3 Socks proxy

Más información: <http://www.ufasoft.com/socks/>
<http://proxylabs.netwu.com/proxycap/>

- 4.3.4 Instalar nuestro propio servidor proxy

Más información: <http://www.qcd.org/sengoku/stone/>
<http://www.junkbusters.com/ijb.html>
<http://www.boutell.com/rinetd/>

- 4.3.5 Proxys especiales / tunnel tools

- 4.3.5.1 JAP

JAP es una herramienta de anonimato gratuita y de código abierto, creada por un universitario alemán. El programa envía nuestro tráfico cifrado a través de diferentes servidores llamados `"mixes"`, por lo que nadie, ni siquiera el propietario de uno de los mixes, puede conocer quién está accediendo a que sitio. Esta también es una de las mejores maneras de evitar la



censura. Para descargar el programa y obtener información, así como instrucciones para su instalación: http://anon.inf.tu-dresden.de/index_en.html. El Infoservice escucha en el puerto 6543, el Dresden-ULD mix en el puerto 26544, el Dresden-Dresden mix en el puerto 6544 y el Dresden-Luebeck en el puerto 9544.

- 4.3.5.2 Httpport

<http://www.htthost.com/>

- 4.3.5.3 Localproxy

<http://proxytools.sourceforge.net/>

- 4.3.5.4 HttpTunnel

<http://www.http-tunnel.com/>

<http://www.nocrew.org/software/httpunnel.html>

- 4.3.6 Wingates

Más información: <http://www.deerfield.com/products/wingate/>

-
- 4.4 Usando un Shell

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

http://directory.google.com/Top/Computers/Internet/Access_Providers/Unix_Shell_Providers/

<http://www.panix.com/shell.html>

<http://www.shellux.net/>

- 4.5 Usando un proxy web

Los proxys web son CGI-scripts a los que conectamos con nuestro navegador y después desde allí abriremos las diferentes URL's a las que queramos acceder, para nuestro cortafuegos solo estamos conectados al servidor del CGI-script. Las direcciones del punto 4.5.4 no son realmente proxys, si no que son traductores, chequeadores-HTML o archivos web, pero podemos usarlos también como proxys. Los proxy web son una buena manera de evitar rápida y limpiamente la censura, ya que no hay que configurar nada, pero son un poco lentos y no funcionan con todas las páginas web. Solo los proxys que funcionan bajo conexión segura pueden ser usados para evitar el filtro por palabras, pero el resto son perfectos para evitar los filtros por URL/IP. Puedes usarlos en tu colegio, biblioteca o compañía, donde no tengas los privilegios para instalar o cambiar algo en el ordenador. Los enlaces apuntan a google.de porque el sitio es pequeño, útil, siempre funciona y no contiene la extensión ".com"; de los archivos DOS que son filtrados por algunos proxys.

Si posees un sitio web que admita CGI, puedes descargar el CGIProxy de James Marshall e instalarlo en ese espacio web (hay un instalador que lo hace todo por tí <http://install.xav.com/>). Para



encontrar nuevos proxys que funciones solo tienes que buscar por "nph-proxy.cgi", "nph-proxy.pl", "Start Using CGIProxy", "Start browsing through this CGI-based proxy" o algo similar en Google, Altavista, Yahoo o otro buscador.

- 4.5.1 Proxys web standard (mayormente CGIProxies: <http://www.jmarshall.com/tools/cgiproxy/>)

<http://anon.free.anonymizer.com/http://www.google.de/>
<http://invis.free.anonymizer.com/http://www.google.de/>
http://anonymouse.ws/cgi-bin/anon-www_de.cgi/http://www.google.de/ (Advertisement)
<http://www.sendfakemail.com/anonbrowser/> (Without images)
<http://203.26.19.30/proxy/proxy.pl/000000A/http/www.google.de/> (Whitout images)
<http://www.mdsme.de/cgi-bin/nph-spinnerproxy.cgi/111111A/http/www.google.de/>
<http://www.marzie.com/webtools/proxybuster/browse.asp?url=http://www.google.de/>
(Advertisement)
<http://203.26.19.30/proxy/nph-proxy.pl/111110A/http/www.google.de/>
<http://www.tku.ac.jp/~99e1330/cgi-bin/nph-proxy.cgi/111/http/www.google.de/>
<http://www.delorie.com/web/purify.cgi?purity=html40l&url=http%3A%2F%2Fwww.google.de>
(Advertisement)
<http://proxy.drkangel.com/nph-index.cgi/111110A/http/www.google.de/>
<http://www.perseus.tufts.edu/cgi-bin/nph-filter/000010AA/http/www.google.de/>
<http://www.anonymization.net/1/1/A/http://www.google.de/>
<http://www.wgbh.org:81/cgi-bin/nph-algs.cgi/011111A/http/www.google.de/>
<http://www.jetropolis.com/cgi-bin/nph-proxy.cgi/000000A/http/www.google.de/>
<http://digitalizedzone.com/cgiproxy/nph-proxy.pl/111110A/http/www.google.de/>
<http://unfeomateo.com/cgiproxy/nph-proxy.pl/000100A/http/www.google.de/>
<http://www.linuxdistributions.com/cgi-bin/nph-proxy.cgi/000111A/http/www.google.de/>
<http://ym2400z.virtualave.net/cgi-bin/cgiproxy131/nph-proxy.cgi/000/http/www.google.de/>
<http://glass.ipe.tsukuba.ac.jp/~s011304/cgi/nph-proxy.cgi/000010A/http/www.google.de/>
<http://www.anonsurf.de/cgi-bin/nph-asurf.cgi/000100A/http/www.google.de/>
<http://www.valkaryn.net/proxy/nph-proxy.cgi/000010A/http/www.google.de/> (Advertisement)
<http://www.rahty.com/nph-proxy.cgi/00010/http/www.google.de/>
<http://www.boyscorp.com/prx/nph-proxy.cgi/000/http/www.google.de/>
<http://www.thinksquad.com/cgi-bin/nph-proxy.cgi/000110A/http/www.google.de/>
<http://www.hostsite.org/proxy/nph-proxy.pl/000000A/http/www.google.de/>
<http://free2.surffreedom.com/nph-free.cgi/000000A/http/www.google.de/>
<http://birthdays.hisham.cc/nph-proxy.cgi/000010A/http/www.google.de/>
<http://www.triumphpc.com/cgi-bin/nph-proxy.cgi/000010A/http/www.google.de/>

- 4.5.2 Proxys web con URL's cifradas

<http://www.proxyone.com/cgi-bin/nph-prxone.cgi/111111A/687474702f7777772e676f6f676c652e64652f> (Without images)

<http://proxy.guardster.com/cgi-bin/nph-proxy.cgi/111101A/687474702f7777772e676f6f676c652e64652f> (Advertisement)

<http://proxify.com/nph-proxy.cgi/000010A/687474702f7777772e676f6f676c652e64652f>
(Advertisement)

<http://www.team777.com/cgi-bin/ey3/nph-proxy.cgi/000010A/687474702f7777772e676f6f676c652e64652f>



- 4.5.3 Proxys web bajo conexión segura SSL-connection
se pueden encontrar muchos SSL-webproxies aquí: <http://qingxin.mine.nu/ssl.asp>

<https://www.anonsurf.de/cgi-bin/nph-asurf.cgi/000100A/http/www.google.de/>
<https://dtw.ods.org/cgi-bin/nph-proxyb.cgi/000000A/http/www.google.de/>
<https://nav.ebutechnologies.com/securing/free-anon.cgi/542/http://www.google.de/>
<https://ym2400z.virtualave.net/cgi-bin/cgiproxy131/nph-proxy.cgi/100/http/www.google.de/>
https://vip.megaproxy.com/go/_mp_framed?http://www.google.de/ (Advertisment)
<https://proxify.com/nph-proxy.cgi/000010A/687474702f7777772e676f6676c652e64652f>
(Advertisment)
<https://www.perseus.tufts.edu/cgi-bin/nph-filter/000010AA/http/www.google.de/> (Without images)
<https://www.eopledaily.com/dmirror/http/www.google.de/>
<https://nhuanet.com/cgi-bin/nph-proxyb.cgi/000000A/http/www.google.de/>
<https://dtaiwang.ftphost.net/cgi-bin/nph-proxyb.cgi/000000A/http/www.google.de/>
<https://www.eopledaily.com/cgi-bin/nph-proxyb.cgi/000000A/http/www.google.de/>
<https://www.amduus.com/cgi-bin/nph-proxy.cgi/000010A/http/www.google.de/>
<https://ym2400z.virtualave.net/cgi-bin/cgiproxy131/nph-proxy.cgi/000/http/www.google.de/>

- 4.5.4 Traductores, warper, e.t.c que pueden ser usados como proxy

<http://www.dejavu.org/> (Browser Emulator)
<http://crit.org/http://www.google.de/>
<http://paranormal.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.google.de>
<http://bobby.cast.org/bobby/bobbyServlet?URL=http://www.google.de> (Websitechecker)
<http://www.vischeck.com/vischeck/vischeckURL.php> (Websitechecker)
<http://spireproject.com/cgi-bin/footnote.pl?form=2&page=http://www.google.de> (Footnote?)
<http://cyber.law.harvard.edu/cite/annotate.cgi?view=http://www.google.de> (kind of a footnote)
http://webwarper.net/ww/~GZ/www.google.de/?* (Warper)
<http://babelfish.altavista.com/> (Translator)
<http://www.freetranslation.com/web.htm> (Translator)
<http://translation.langenberg.com/> (Translator)
<http://www.systransoft.com/> (Translator)
<http://www.translate.ru/srvurl.asp?lang=de> (Translator)
<http://translator.abacho.de/> (Translator)
<http://www.t-mail.com/cgi-bin/tsail> (Translator)
http://www.google.com/language_tools?hl=de (Translator)
<http://tarjim.ajeeb.com/ajeeb/default.asp?lang=1> (Translator)

<http://www.sdlintl.com/enterprise-systems/enterprise-translation-server/ets-demo/ets-demo-web-translation.htm> (Translator)
<http://rinkworks.com/dialect/> (Fun-Translator)
<http://www.brunching.com/drugslanger.html> (Fun-Translator)

<http://www.pornolize.com/cgi-bin/pornolize2/pornolize2.cgi?lang=en&url=http%3A%2F%2Fwww.google.de&submit=submit> (Fun-Translator)
<http://unimut.fsk.uni-heidelberg.de/schwob.html> (Fun-Translator)
<http://www.google.com/.de/.fr/> (the Google Cache)
http://web.archive.org/web/*/http://www.google.de (Archive of the Internet since 1996)
<http://www.marzie.com/webtools/proxybuster/> (get files)
<http://alltooflat.com/geeky/elgoog/> (a Google fun mirror mirror)
<http://www.guhgel.de/> (another Google fun mirror)
<http://www.assoziations-blaster.de/www.something.de/>
<http://mirror.sytes.org/> (a fun mirror mirror *gg*)
<http://proxy.citizenlab.org/google/> (a Google mirror)



<http://hispeed.rogers.com/search/google.jsp> (a Google mirror)
<http://www.gogole.com/> (a Google mirror)
<http://google.icq.com/search/> (a Google mirror)
<http://www.zensur.freerk.com/google/> (a mirror for the Google mirror...)
<http://www.google-watch.org/cgi-bin/proxy.htm> (another Google and Alltheweb mirror)
<http://www.aigeeek.com/txt2html/txt2html-url.cgi?url=http%3A%2F%2Fwww.google.de> (html2text)
<http://gritechnologies.com/tools/diagnostic.go?www.google.de/> (see as a search engine)
<http://www.accu.org/cgi-bin/accu/access/access?Au=http%3A%2F%2Fwww.google.de> (a gateway/browser emulator)

- 4.6 Obtener las páginas web vía e-mail

Mucho tiempo atrás, cuando las conexiones de Internet eran lentas y el "www" acababa de ser inventado, mucha gente tenía como único acceso a Internet el uso del correo electrónico, este es el origen de los programas "Agora" y "www4email". Alguno de estos robots de correo electrónico están disponibles todavía y podemos usarlos para saltar la censura. La mejor manera sería suscribirse a un proveedor gratuito de correo que permitiese las conexiones SSL, (como <https://www.fastmail.fm/>, <https://www.ziplip.com/>, <https://www.hushmail.com/>, <https://www.safe-mail.net/>, <https://www.mail2world.com/>, <https://webmail.co.za/>, <https://www.webmails.com/> etc.) y usar el correo con las direcciones de abajo; he puesto el campo donde debemos introducir la URL entre corchetes, funciona perfectamente para texto, pero hay grandes problemas con imágenes e incluso DHTML, Javascript, Java, Flash, etc. También otros servicios a demás del www son accesibles vía e-mail, puedes ver un buen tutorial sobre el tema en <ftp://rtfm.mit.edu/pub/usenet/news.answers/internet-services/access-via-email>. Este servicio también está disponible vía web <http://www.web2mail.com/>.

Se ha vuelto a usar google.de por la misma razón antes comentada. El programa www4mail (<http://www.www4mail.org/>) es más reciente que el programa Agora. Un correo con tan solo "help" en el asunto, te devolverá un tutorial de cómo usar el servicio correctamente.

agora@kamakura.mss.co.jp
[BODY] send <http://www.google.de>

agora@dna.affrc.go.jp
[BODY] send <http://www.google.de>

page@grabpage.org
[SUBJECT] url: <http://www.google.de>
info: <http://www.grabpage.org/>

frames@pagegetter.com
[BODY] <http://www.google.de>
info: <http://www.pagegetter.com/>



web@pagegetter.com

[BODY] <http://www.google.de>

info: <http://www.pagegetter.com/>

webgate@vancouver-webpages.com

[BODY] get <http://www.google.de>

info: <http://vancouver-webpages.com/webgate/>

webgate@vancouver-webpages.com

[BODY] mail <http://www.google.de>

info: <http://vancouver-webpages.com/webgate/>

www4mail@wm.ictp.trieste.it

[BODY] <http://www.google.de>

info: <http://www.ictp.trieste.it/~www4mail/>

www4mail@access.bellanet.org

[BODY] <http://www.google.de>

info: <http://www.bellanet.org/email.html>

www4mail@kabissa.org

[BODY] <http://www.google.de>

info: <http://www.kabissa.org/members/www4mail/>

www4mail@ftp.uni-stuttgart.de

[BODY] <http://www.google.de>

www4mail@collaborium.org

[BODY] <http://www.google.de>

info: <http://www.collaborium.org/~www4mail/>

binky@junoaccmail.org

[BODY] url <http://www.google.de>

info: <http://boas.anthro.mnsu.edu/>

iliad@prime.jsc.nasa.gov

[SUBJECT] GET URL

[BODY] url:<http://www.google.de>



info: <http://prime.jsc.nasa.gov/iliad/>

Google Search via eMail:

google@capeclear.com

[Subject] search keywords

info: <http://www.capeclear.com/google/>

Más información: <http://www.cix.co.uk/~net-services/mrcool/>

<ftp://rtfm.mit.edu/pub/usenet/news.answers/internet-services/access-via-email>

- 4.7 Uso de esteganografía

Hide content inside of images.

Más información: <http://www.wikipedia.org/wiki/Steganography>

- 4.7.1 Camera/Shy

Camera/Shy is the only steganographic tool that automatically scans for and delivers decrypted content straight from the Web. It is a stand-alone, Internet Explorer-based browser that leaves no trace on the user's system and has enhanced security.

Camera/Shy is an application that enables stealth communications, such software can be useful in countries where Email communications are regularly monitored and censored, such as happens in China.

Más información:

<http://hacktivismo.com/news/modules.php?name=Content&pa=showpage&pid=12/>

<http://sourceforge.net/projects/camerashy/>

- 4.8 Usar un proxy especial como un programa P2P

Hay diferentes proyectos de programas P2P para pasar la censura, trabajan como Napster, Kazaa, eDonkey, etc, lo cual significa que tenemos que descargar e instalar una pequeña herramienta que



contiene la parte del servidor o cliente del programa.

- 4.8.1 Peek a Booty

The goal of the Peekabooty Project is to create a product that can bypass the nationwide censorship of the World Wide Web practiced by many countries.

Peekabooty uses a complicated communications system to allow users to share information while revealing little about their identity. When a node receives a request for a web page it randomly decides whether to pass this on or access the page itself. It also only knows the address of its nearest partner. This makes it difficult to determine who requested what information and is designed to protect users from anyone trying to infiltrate the system from inside.

Más información: <http://www.peek-a-booty.org/>

- 4.8.2 Freenet

Freenet es el más antiguo y extendido programa para evitar la censura, por ello mucha gente lo usa y continúa funcionando bastante bien desde hace muchos años. No hay acceso posible a Internet a través del cliente Freenet, sólo podemos ver / bajar cosas desde la *"free net"*. El programa se instala como proxy local que escucha en el puerto 8888 y puede acceder a enlaces como <http://localhost:8888/SSK@fjfkHAbxdwMyTMFgtZjCp2ge-AYPAqM/sites/fwhh/index.html>, lo cual parece una URL normal, donde *"localhost:8888"* conecta con el proxy local que está instalado en nuestra máquina y el resto es algo como un nombre de archivo cifrado. Es imposible determinar quién ha puesto alguna información en la red o quien se la está bajando.

Más información: <http://freenetproject.org/>
<http://www.freenet-china.org/>

- 4.8.3 MojoNation

Más información: <http://www.mojonation.net/>

- 4.8.4 TriangleBoy

Safeweb, a company that received funding from In-Q-Tel, the CIA's venture fund, released software called *"Triangle Boy"*. The software is a peer-to-peer application that volunteers download onto their PC's. A User that has been denied access to any website by a censor can use the Triangle Boy software to circumvent the censorship. Currently the Triangle Boy software only provides access to the Voice of America, because this service is blocked by the Chinese government.

Más información: http://www.safeweb.com/tboy_service.html



- 4.8.5 Six/Four

Más información: <http://www.hacktivismo.com/>

- 4.8.6 Entropy

Más información: <http://entropy.stop1984.com/>

- 4.9 Servicios especiales

Otros servicios que el www.

- 4.9.1 Usenet

El puerto 119, habitual para los servidores de noticias, está normalmente bloqueado por lo que deberemos acceder a usenet por un puerto diferente. Si lo que quieres es leer de vez en cuando algún grupo de noticias común puedes visitarlo fácilmente vía algún servidor de noticias web como <http://groups.google.com/> o <http://news.spaceports.com/>. Muchas compañías ofrecen sus servicios por un puerto no standard, simplemente pregúntales antes de suscribirte. Si lo que necesitas es acceder a un servidor de noticias con tu cliente de noticias, deberás suscribirte a una de esas compañías que ofrecen acceso a su servidor de noticias en un puerto no común:

<http://www.giganews.com/> - (puertos 23 y 80 funcionan)

<http://www.easynews.com/> - (usa su servidor de noticias web o prueba 'proxy.news.easynews.com' con los puertos 21, 22, 23, 25, 53, 80, 110, 443 o 8080)

<http://www.newscene.com/> - (prueba 'proxy.newscene.com' con los puertos 20, 21, 22, 23, 25, 53, 80, 81, 110, 443 o 8080)

<http://www.supernews.com/> - (puedes acceder a su servidor de noticias a través del puerto que quieras)

Nota: todo el tráfico viaja sin cifrar, por lo que podrás acceder al servidor de noticias, pero el censor puede monitorear todo tu tráfico fácilmente, sería mas seguro usar un puerto SSH.



thanks to 'sshproxy' from the nocensorship mailinglist

- 4.9.2 Juegos

- 4.9.3 FTP

<http://inebria.com/phpftp/>
<http://www.angehrn.com/index.php?cat=28>
<http://www2ftp.de/>
<http://webftp.host.sk/>

- 4.9.4 Mensajería instantánea

La mensajería instantánea es algo popular, solo tienes que descargar el software y registrar tu nick; una vez estás conectado a la red puedes ejecutar el programa y conectar con sus servidores, desde ese momento estás marcado como "online" y todos los contactos que conocen tu nick y usan ese mismo programa pueden ver que estás conectado y chatear contigo. Las cuatro grandes compañías tienen su propio software cliente, que contiene publicidad, spyware y no son compatibles con otros protocolos de mensajería instantánea. Mi recomendación es que descargues Miranda, un programa de código abierto de pequeño tamaño sin más "añadidos" que además no necesita instalación y funciona correctamente con todos los protocolos de mensajería instantánea, incluso al mismo tiempo. <http://miranda-im.org/>

- 4.9.4.1 ICQ

ICQ es el más veterano y usado dentro de la mensajería instantánea, del cual existen muchos diferentes clientes. Todos ellos normalmente conectan por login.icq.com:5190 vía TCP en ambas direcciones, pero el servidor acepta conexiones en todos los puertos, la versión Java puede ser ejecutada desde aquí <http://go.icq.com/>, con esto conectarás normalmente por iht-d01.icq.com(205.188.213.0) por el puerto común http (80), desde "Settings" puedes escoger un puerto diferente.

- 4.9.4.2 MSN Messenger

messenger.hotmail.com:1863. Hasta ahora no hay un sitio oficial web desde el que usar este cliente por lo que deberás probar desde diferentes compañías, debes de darles tu password, por lo que deberás de confiar en ellos. Puedes contactar con Microsoft y pedir que ponga en funcionamiento un cliente web. <http://www.mister-i.com/i-mode/messenger.jsp> (i-mode después de tres días hay que pagar), <http://kickme.to/msnmessenger2go> (todavía en construcción), <http://www.messengeradictos.com/index.php?accion=messengeronline> (en español, requiere activeX), <http://odigo.org/features/express.html> (el cliente odigo funciona online correctamente), <http://messenger.lycos.co.uk/messenger/index.jsp> (funciona con MSN y Yahoo).

- 4.9.4.3 AIM



login.oscar.aol.com:5190 Acepta conexiones en todos los puertos y existen 2 clientes web oficiales, el antiguo QuickBuddy: <http://toc.oscar.aol.com/> y el nuevo AIM Express: <http://toc.oscar.aol.com/aimexpress/index.html>.

- 4.9.4.6 Yahoo Messenger

cs.yahoo.com:5050 o cs.yahoo.co.jp:5050. Se puede acceder online vía <http://messenger.yahoo.com/>.

- 4.9.5 Programas para compartir archivos

Gnutella (decentralized) - BearShare, Gnucleus, LimeWire, new Morpheus

FastTrack (commercial, with Server) - KaZaA, KaZaA Lite, Grokster, old Morpheus

eDonkey2000 (lots of servers, uses mainly port 4662) - eDonkey2000, Overnet, eMule

OpenNap (lots of servers) - FileNavigator, WinMX, Rapigator, TekNap, audioGnome, XNap

[volver arriba](#) 5. Cómo publicar la información

Una cosa es acceder a una información que está censurada, pero otro desafío es publicar nuestra propia información para que no pueda ser fácilmente censurada. Aquí tienes mis ideas de como evitar a la censura:

- Publicar en muchos espejos. Especialmente IP's dinámicas redireccionadas desde dyndns.org es útil. Coloca tus páginas en tantos sitios que el censor no pueda llegar a bloquear todos los servidores.
- Usa one-time-addresses. Son enlaces/URL's sólo válidos durante una visita o una hora. Frecuentemente utilizado para descargas de pago.
- Esconde el contenido "peligroso". Por ejemplo, guarda el texto como imágenes, el usuario no lo notará, pero será difícil para los rastreadores del censor leer el contenido.
- Cuelga tu página en un servidor seguro en otro país. Por ejemplo con <http://www.havenco.com/> el cual está localizado en Sealand, un pequeño país independiente en una isla al norte del Mar de Inglaterra.
- Cifra el contenido. Usa .htaccess y/o SSL para tus sitios web así como AES, Twofish or Rijndael para los archivos.
- Ofrece tus datos en los programas P2p. Programas para compartir archivos, como Kazaa o eDonkey son muy difíciles de censurar (sólo hay que observar los problemas de las compañías de música)
- Envía contenidos vía e-mail. Crea una repuesta automática desde la cual todo el mundo con una cuenta de correo puede recibir tu contenido.
- Martus. Es un servicio de boletín cifrado para postear y ver información. <http://www.martus.org/>



Más información: <http://www.wired.com/news/technology/0,1282,5778,00.html>

[volver arriba](#) 6. Apéndice

- 6.1 Enlaces

- 6.1.1 Otros tutoriales para evitar la censura

<http://galileo.spaceports.com/~simeon/censorship-evasion.html>

<http://www.angelfire.com/my/6waynes/>

<http://www.ijs.co.nz/proxies.htm>

<http://sethf.com/anticensorware/>

- 6.1.2 Otros sitios sobre la censura en Internet

<http://cyber.law.harvard.edu/filtering/>

<http://www.opennetinitiative.net/oni/ice/>

<http://peacefire.org/circumventor/>

<http://www.free-market.net/directorybytopic/censorship/>

<http://www.stop1984.info/>

<http://www.cmis.csiro.au/projects+sectors/blocking.pdf>

<http://www.topology.org/net/censor.html>

Mailinglist: <http://lists.efa.org.au/mailman/listinfo/stop-censorship> - (Discussions about censorship in Australia, english)

Mailinglist: <http://www.freelists.org/webpage/nocensorship> - (How to beat censorship and proxies. Very good!)

<http://www.vicnet.net.au/community/issues/censorship/>

http://ch.dmoz.org/Society/Issues/Human_Rights_and_Liberties/Free_Speech/The_Censorship_Debate/Internet_Censorship/

http://ch.dmoz.org/Computers/Software/Internet/Servers/Proxy/Filtering/Getting_Around_Filters/

<http://ch.dmoz.org/Computers/Software/Internet/Servers/Proxy/Filtering/Censorware/>

<http://ch.dmoz.org/Computers/Software/Internet/Clients/Filtering/>

http://ch.dmoz.org/Reference/Libraries/Library_and_Information_Science/Intellectual_Freedom/Filtering_Software/

- 6.1.3 Dónde obtener proxys

<http://tools.rosinstrument.com/proxy/>

<http://www.samair.ru/proxy/>

<http://www.atomintersoft.com/products/alive-proxy/proxy-list/>

<http://www.steganos.com/software/anonproxylist.sia>

<http://www.zensur.freerk.com/list.txt>

Via autoresponder from list.txt@zensur.freerk.com

<http://www.proxyblind.org/phpBB2/> (Very good!)

<http://www.samair.ru/f/> (Very good!)

<http://www.freeproxy.ru/download/lists/goodproxy.txt>



[volver arriba](#) Cosas por hacer:

Voice-over-IP

Bildung von Untergrund-(Inter)Netzen in Deutschland (GAMEnet etc.) <http://www.personaltelco.net/>
WLAN
dIRC (ChaosComputerCongress 1997) und Abwandlungen

<http://www.guardianet.net/>

<http://www.w3.org/PICS/>

<http://www.peacefire.org/bypass/Proxy/akamai.html>

web-2-phone: <http://www.teletrust.info/>, <http://www.ecommercetimes.com/perl/story/3380.html>

ssh as a redirection server
rinetd as a redirection server
junkbuster
http-gw
VPNs
stone as both a redirector and a proxy
running a Perl proxy

often used non standard ports: 20, 21, 22, 23, 24, 25, 81, 82, 83, 84, 443, 1128, 2000, 5000, 6000, 6588, 7070, 8000, 8001, 8002, 8003, 8040, 8081, 8082, 8084, 8090, 8888, 8965, 9080, 9081, 10080, 22788

<http://www.arbornet.org/projects.html>
telnet m-net.arbornet.org

<http://www.cyberspace.org/>
telnet cyberspace.org

<http://www.ductape.net/>



telnet ductape.net

<http://sdf.lonestar.org/>
telnet sdf.lonestar.org

<http://www.nyx.net/>
telnet nyx.nyx.net

<http://www.suburbia.com.au/>
telnet suburbia.com.au (SSH)
telnet suburbia.com.au 2323 (telnet)

http://www.saunalahti.fi/~aekman/taboom/free_shell.html
<http://www.freebelt.com/freesHELLs.html>
<http://www.geocities.com/SiliconValley/Way/2183/freeuspl.html>
<http://www.leftfoot.com/free-shell.html>

faxabruf

web.de answering machine0049-1212-552489659

softhome.net: free email with smtp server mail.softhome.net:2500 and mail.softhome.net:25000

url hiding with ascii, hex, oktal e.t.c codes.

This link is for bad machines only, uninteresting for humans: