CIRCUMVENTION TOOLS

Published : 2011-06-22
License : None

1. INTRODUCCIÓN

El 10 de Diciembre de 1948, la Asamblea General de las Naciones Unidas inició una nueva era con el lanzamiento de la Declaración Universal de los Derechos Humanos. El estudiante libanés Charles Habib Malik lo describe a los delegados reunidos así:

> *Cada miembro de las Naciones Unidas se ha comprometido solemnemente a respetar y acatar los derechos humanos. Pero, concretamente nunca hemos sido instruidos en cuáles son estos derechos, ni siquiera en los estatutos o en otro instrumento nacional. Esta es la primera vez que los derechos humanos y las libertades fundamentales son escritos correctamente con autoridad y en detalle.* ***Ahora se qué mi gobierno se comprometió a promover, acatar, y consumar... Puedo protestar contra mi gobierno, y si este no cumple su compromiso, tendré y sentiré el apoyo moral del mundo entero.***

Uno de los derechos fundamentales descritos en la Declaración Universal de los Derechos Humanos, en el Artículo 19, fue el derecho a la libertad de expresión:

> *Todo el mundo tiene el derecho a la libertad de opinión y expresión; este derecho incluye la libertad de sostener opiniones sin interferencia y* ***buscar, recibir y compartir ideas e información a través de los medios de comunicación, con independencia de las fronteras.***

Cuando aquellas palabras fueron escritas setenta años atrás, nadie imaginó cómo el fenómeno global de Internet expandiría la habilidad de "buscar, recibir e compartir información", no solo atravesando las fronteras y los límites sino a velocidades asombrosas y que pueden ser copiadas, editadas, manipuladas, recombinadas y compartidas con audiencias pequeñas y grandes y en formas diferentes a los medios de comunicación disponibles en 1948.

MÁS INFORMACIÓN EN LUGARES JAMÁS IMAGINADOS

En los últimos años el increíble crecimiento de la información que hay en Internet y su disponibilidad ha tenido el efecto de hacer accesible en los lugares más insospechados gran parte del quehacer y del conocimiento humano: el hospital en una aldea remota, el cuarto de nuestra hija de 12 años, la sala de conferencia donde mostramos a nuestros colegas un nuevo diseño de producto que nos pondrá a la cabecera de la competencia, la casa de la abuela.

En todos esos lugares, la posibilidad de conectarse con el mundo abre muchas oportunidades fabulosas que mejoran la vida de las personas. Cuando contraemos una enfermedad rara en vacaciones, el hospital de la aldea remota puede salvarnos la vida enviando los resultados de los exámenes médicos a un médico especialista en la capital, o incluso a otro país; nuestra hija de 12 años puede hacer su proyecto de investigación o hacer amigos en otros países; podemos presentar el nuevo diseño del producto simultáneamente a los mejores directores en sus oficinas alrededor del mundo, los que pueden ayudarnos a mejorarlo; la abuela puede enviarnos su receta especial de pastel de manzana por correo electrónico en tiempo para hornearlo para el postre.

Pero Internet no solo sirve para acceder a información relevante y educativa, amistades y recetas de pastel de manzanas. Como el mundo en sí mismo, es vasto, complejo y muchas veces temible. Está disponible a personas maliciosas, ambiciosas, inescrupulosas, deshonestas o rudas así como está disponible para nosotros, nuestra hija de 12 años y nuestra abuela.

HAY QUIENES NO QUIEREN INCLUIRNOS A TODOS

Con todo lo mejor y lo peor de la naturaleza humana reflejada en Internet y la facilidad con que ciertos tipos de engaños y hostigamientos pueden ser hechos gracias a la tecnología, no debería sorprender a nadie que el crecimiento de Internet ha sido paralelo a los intentos de controlar cómo las personas lo usan. Existen diferentes motivaciones para controlar el uso de Internet. Las principales incluyen:

- Proteger a los niños del material inapropiado, o limitar el contacto con personas que puedan dañarlos.
- Reducir el bombardeo de ofertas comerciales por correo electrónico o en la Web.
- Controlar el tamaño del flujo de datos que cualquier usuario es capaz de acceder en un momento determinado.
- Evitar que los empleados compartan información que sea propiedad del empresario, o que usen el tiempo de trabajo o los recursos técnicos del empresario en actividades personales.
- Restringir el acceso a materiales o actividades en línea que son prohibidas o reguladas en una jurisdicción específica (que puede ser un país o una organización como la escuela), como son los materiales sexuales explícitos o violentos, drogas o alcohol, apuestas y prostitución, e información acerca de grupos religiosos o políticos, o ideas que se estiman peligrosas.

Algunas de estas preocupaciones solo implican permitir que las personas controlen su propia experiencia de Internet (por ejemplo, dejar que las personas usen herramientas de filtrado de spam para prevenir que el spam sea enviado a sus propias cuentas de correo), pero otras restringen cómo otras personas usan Internet y que pueden o no acceder. El último caso causa conflictos significativos y desacuerdos cuando las personas a las que se les ha restringido el acceso no están de acuerdo con que el bloqueo sea apropiado.

¿QUIÉN ESTÁ FILTRANDO O BLOQUEANDO INTERNET?

Los tipos de personas e instituciones que están tratando de restringir el uso de Internet a personas específicas varían según sus objetivos. Entre estas personas se incluyen padres, escuelas, compañías comerciales, operadores de Cibercafés o Proveedores de Servicios de Internet, y gobiernos a diferentes niveles.

El otro extremo del espectro del control de Internet es cuando un gobierno nacional intenta restringir el acceso en Internet a categorías completas de información o a compartir información libremente con el resto del mundo. Investigaciones realizadas por OpenNet Initiative (http://opennet.net) documentan las diferentes formas en que los países filtran y bloquean el acceso a Internet de sus ciudadanos. Estos países con políticas de filtrado penetrantes han hecho una rutina del bloqueo a las organizaciones de los derechos humanos, noticias, blogs, y servicios Web que desafían su estado actual existente o se estiman amenazadores o indeseables. Otros bloquean el acceso a categorías simples de contenido en Internet, o de forma intermitente a sitios específicos o servicios de red que coinciden con eventos estratégicos, como elecciones o demostraciones públicas. Incluso los países que generalmente protegen con fuerza la libertad de expresión algunas veces tratan de limitar o monitorear el uso de Internet suprimiendo la pornografía, los llamados “discursos de odio”, el terrorismo y otras actividades criminales, o la infracción de las leyes de derecho de autor.

EL FILTRAJE CONDUCE AL MONITOREO

Cualquiera de estos grupos oficiales o privados puede usar varias técnicas para monitorear las actividades en Internet de las personas que le conciernen y asegurarse de que las restricciones están funcionando. Esto va desde los padres mirando por encima del hombro de sus hijos o buscando los sitios que se han accedido desde sus computadoras, hasta las compañías que monitorean los correos de sus empleados o las agencias de cumplimiento de la ley demandando información desde los Proveedores de Internet o incluso apoderándose de nuestra computadora en la casa buscando evidencia de que hemos estado ocupados en actividades “indeseables”.

¿CUANDO SE PRODUCE LA CENSURA?

Dependiendo de quién esté restringiendo el acceso a Internet y/o monitoreando su uso, y la perspectiva de la persona cuyo acceso ha sido restringido, cualquiera de estos objetivos y métodos para alcanzarlos pueden ser vistos como legítimo y necesario o como algo inaceptable y una violación de los derechos humanos. Un adolescente cuya escuela bloquea en Internet su juego favorito o su sitio social MySpace por ejemplo, siente su libertad personal limitada tanto como aquellos a los que el gobierno les impide leer un periódico de la oposición política.

¿QUIÉN ESTÁ BLOQUEANDO MI ACCESO A INTERNET EXACTAMENTE?

La persona que restringe el acceso a Internet en cualquier computadora y desde cualquier país depende de quien tenga el control de partes específicas de la infraestructura técnica. Este control se puede basar en establecer relaciones legales o requerimientos o en el poder gubernamental o de otros cuerpos para presionar a aquellos que tienen el control legal sobre la infraestructura técnica para dar cumplimiento a la solicitud de bloqueo, filtrado o recolección de información. Muchas partes de la infraestructura internacional que soportan Internet están bajo el control de gobiernos o agencias de control gubernamentales, los cuales pueden hacer valer el control de acuerdo o no con las leyes locales.

El filtrado o bloqueo de partes de Internet puede ser pesado o ligero, muy claro o invisible. Algunos países admiten abiertamente el bloqueo y publican sus criterios al respecto, y sustituyen los sitios bloqueados con mensajes explicativos. Otros países no tienen estándares definidos claramente y algunas veces confían en el entendimiento informal y en la incertidumbre de presionar a los proveedores de Internet para que filtren el contenido. En otros países, el filtrado viene disfrazado con fallas técnicas y los gobiernos no se responsabilizan abiertamente cuando el bloqueo es deliberado. Distintos operadores de redes, incluso en el mismo país y sujetos a las mismas regulaciones, pueden ejecutar el filtrado con diferentes niveles de precaución o ignorancia técnica.

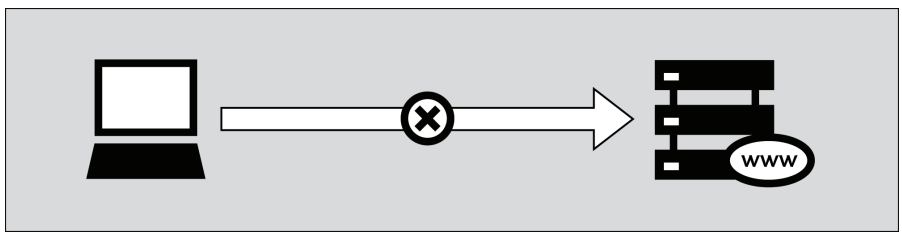
En todos los niveles de posibles filtrados, desde individuales hasta nacionales, las dificultades técnicas de bloquear exactamente lo que es visto como indeseable puede traer consecuencias inesperadas y casi ridículas. Los llamados filtros "Familiares" que pretenden bloquear los materiales sexuales impiden el acceso a información sobre la salud de gran utilidad. El bloqueo de spam puede filtrar correspondencia de negocio importante. Así mismo el bloqueo a sitios específicos de noticias puede eliminar investigaciones educacionales valiosas.

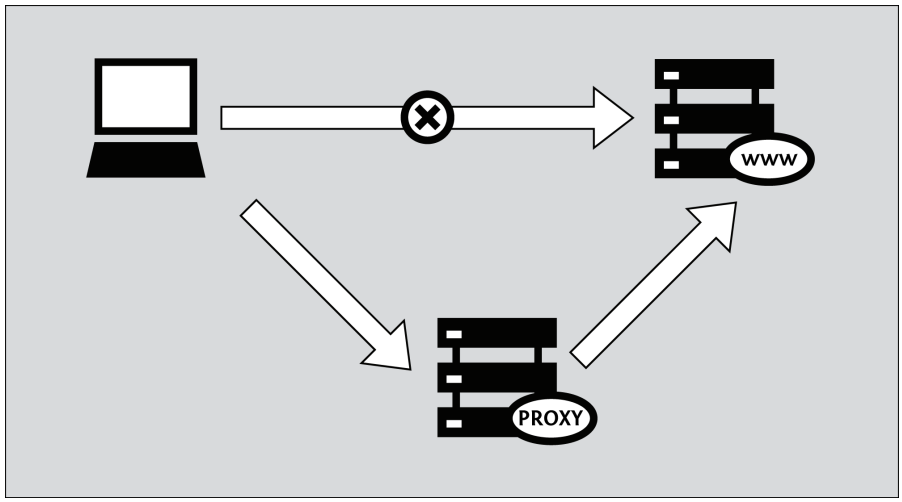
¿QUÉ MÉTODOS EXISTEN PARA EVADIR EL FILTRADO?

Como muchos individuos, corporaciones y gobiernos ven en Internet una fuente de información peligrosa que debe ser controlada, hay muchos individuos y grupos que trabajan muy duro para garantizar que Internet, y la información ahí presente esté libremente disponible para todo el que la desee. Estas personas tienen tantas y diferentes motivaciones como los que buscan controlar Internet. Sin embargo, para alguien cuyo acceso a Internet ha sido restringido y que desea hacer algo con respecto a eso, no es importante si las herramientas fueron desarrolladas por alguien que quería chatear con su novia, escribir un manifiesto político o enviar un spam.

Hay una gran energía, desde entes comerciales, hasta grupos no lucrativos y voluntarios, todos devotos a crear herramientas y técnicas para sortear la censura de Internet. A esto se le llama métodos de **evasión de censura** y van desde simples soluciones, comunicaciones protegidas, hasta programas complejos. De cualquier forma, estos métodos, funcionan aproximadamente de la misma forma. Instruyen al navegador Web para que tome una desviación a través de una computadora intermediaria, llamada **proxy** que:

- está localizado en algún lugar que no está sujeto a la censura de Internet.
- no ha sido bloqueado en nuestra localización.
- sabe cómo buscar y devolver el contenido a usuarios como nosotros.





¿CUÁLES SON LOS RIESGOS DE USAR LAS HERRAMIENTAS DE EVASIÓN?

Solo la persona que espera sobrepasar las restricciones de su acceso a Internet, puede decidir si hay riesgos significativos implicados en la información que desea acceder. Y solo esa persona puede decidir los beneficios que sobrepasan los riesgos. Puede que no haya una ley que prohíba específicamente la información que deseamos o el acceso a ella. Por otra parte, la falta de sanciones legales no significa que se esté poniendo en riesgo otras consecuencias, tales como hostigamiento o la pérdida del empleo.

Los siguientes capítulos describen cómo funciona Internet, las varias formas de censura, y explican un número de herramientas y técnicas que pueden ayudar a sortear las barreras a la libertad de expresión. El tema general de la privacidad y seguridad digital es considerada durante todo el libro, que empieza recorriendo lo básico y después algunos tópicos avanzados antes de cerrar con una breve sección dedicada a los administradores de red y especialistas de la computación que desean ayudar a otros a evadir la censura de Internet.

2. ACERCA DE ESTE MANUAL

El manual 'Evadiendo la Censura de Internet' provee una introducción al tópico y explica algunos de los programas y métodos más usados frecuentemente para evadir la censura. También se trata brevemente cómo evitar la supervisión y otros medios de detección mientras se traspasa la censura, sin embargo este es un tópico bastante grande, así que solo hemos tocado los temas que coinciden directamente con la evasión de la censura.

Una discusión completa de técnicas para el mantenimiento del anonimato y la prevención de la detección del contenido o actividades que realizamos está más allá del alcance de este libro.

¿CÓMO Y POR QUIÉN FUE ESCRITO ESTE LIBRO?

La primera versión de este manual fue escrita en un maratón de escritura en Noviembre de 2008 en las bellas montañas de Upper New York State en los Estados Unidos. Ocho personas trabajaron unidas intensamente en un periodo de cinco días para producir el libro.

La versión actualizada de este manual fue compilada en el contexto de un segundo maratón cerca de Berlín, Alemania, a principios del 2011. Esta vez, 11 personas trabajaron juntas por un periodo de cinco días.

Este libro es por supuesto un documento vivo y está gratis en Internet, donde también podemos editarlo y mejorarlo.

Además del material escrito durante los dos maratones, existen contribuciones de publicaciones anteriores. Esto incluye contribuciones de:

- 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

Estos escritores amablemente acordaron dejarnos usar sus materiales con una licencia GPL.

Este manual ha sido escrito con FLOSS Manuals. Para mejorar el manual sigamos estos pasos:

1. REGISTRARSE

Regístrese en FLOSS Manuals:
http://booki.flossmanuals.net/

2. ¡APORTAR!

Seleccionamos el manual (http://booki.flossmanuals.net/bypassing-censorship/edit/) y el capítulo deseado.

Si necesitamos hacer preguntas acerca de cómo contribuir podemos unirnos a la sala de chat listada debajo. Todos nuestros aportes serán bienvenidos.

Para más información sobre el uso de los manuales podemos leer el manual:
http://en.flossmanuals.net/FLOSSManuals

3. CHAT

Resulta una buena idea contactar con el equipo técnico y nos ayudarán a coordinar las contribuciones. Para ello está la sala de chat que utiliza IRC (Internet Relay Chat). Si sabemos cómo usar IRC podemos conectarnos al siguiente:
server: irc.freenode.net
channel: #booksprint

Si no sabemos usar IRC podemos visitar el chat basado en web desde el navegador:
http://irc.flossmanuals.net/

La información de cómo usar este programa de chat basado en web está aquí:
http://en.flossmanuals.net/FLOSSManuals/IRC

4. LISTA DE CORREOS

Para discutir cualquier cosa sobre el Manual Floss podemos unirnos a la lista:
http://lists.flossmanuals.net/listinfo.cgi/discuss-flossmanuals.net

INTRODUCCIÓN RÁPIDA
3. INTRODUCCIÓN RAPIDA

3. INTRODUCCIÓN RAPIDA

Internet es censurado cuando personas o grupos que controlan la red impiden acceder a los usuarios de Internet a algún contenido o servicio en particular.La censura de Internet adopta muchas formas. Por ejemplo, los gobiernos pueden bloquear servicios de correo electrónico regulares con el objetivo de obligar a los ciudadanos a usar el correo electrónico establecido por el gobierno que puede ser fácilmente monitoreado, filtrado o apagado. Algunos padres pueden controlar el acceso de sus hijos. Una universidad puede impedir a sus estudiantes el acceso a Facebook desde la biblioteca. Un dueño de un Cibercafé puede bloquear la transferencia de ficheros punto a punto. Gobiernos autoritarios pueden censurar reportes de abusos de los derechos humanos o de la última elección robada. Las personas tienen una amplia variedad de puntos de vista acerca de la legitimidad o ilegitimidad de estas formas.

EVASIÓN DE LA CENSURA

Evadir la censura es el acto de sortear o burlar las prohibiciones que rigen el acceso a Internet. Hay muchas formas de hacer esto, pero casi todas las herramientas de evasión funcionan aproximadamente de la misma forma. Hacen que nuestro navegador Web tome un desvío a través de una computadora intermediaria, llamada proxy, que:

- está localizado en algún lugar que no está sujeto a la censura de Internet
- no ha sido bloqueado en nuestra localización
- sabe cómo buscar y devolver el contenido a usuarios como nosotros.

SEGURIDAD Y ANONIMATO

Es preciso tener en mente que ninguna herramienta es la solución perfecta para nuestra situación. Diferentes herramientas ofrecen varios grados de seguridad, pero la tecnología no puede eliminar los riesgos físicos que aceptamos cuando nos oponemos a las personas que tienen el poder. Este libro contiene varios capítulos que explican cómo funciona Internet lo que es muy importante para entender cómo estar más seguros cuando evadimos la censura.

HAY MUCHAS VARIACIONES

Algunas herramientas solo trabajan con el navegador Web, mientras otras pueden ser usadas por varios programas a la vez. Estos programas necesitan ser configurados para enviar el tráfico a Internet a través de un proxy. Con un poco de paciencia extra, podemos hacer todo esto sin necesidad de instalar ningún software en la máquina. Es bueno notar que las herramientas que buscan páginas Web pueden mostrar el sitio de forma incorrecta.

Algunas herramientas usan más de un intermediario con el objetivo de ocultar el hecho de que estamos visitando servicios bloqueados. Esto también oculta nuestras actividades del proveedor de la herramienta, lo que puede ser importante para el anonimato. Una herramienta puede tener una forma inteligente de aprender sobre proxis alternativos, y puede conectarse a ellos en caso de que el que estemos usando haya sido censurado. Idealmente, el tráfico creado por estas peticiones, ya sean búsquedas o envíos, es encriptado con el objetivo de protegernos de los entrometidos.

Pero la selección de la herramienta adecuada para una situación particular no es la decisión más importante que tomaremos cuando accedamos o produzcamos contenido frente a la censura de Internet. Aunque es difícil proporcionar un consejo concreto en estas cosas, es muy importante que nos dediquemos a evaluar:

- Cómo, cuándo y dónde pretendemos usar estas herramientas
- Quién puede querer impedir que hagamos las cosas que permiten hacer las herramientas
- Qué tan fuerte esas organizaciones e individuos se oponen a su uso
- Qué recursos tienen a su disposición para alcanzar su meta deseada, incluyendo la violencia

ACCEDIENDO A LOS SITIOS WEB MÁS BLOQUEADOS SIN PROGRAMAS EXTRAS

La herramienta de evasión de censura de Internet básica es un proxy Web. Mientras existen muchas razones por las cuales esta no sea la solución óptima, para propósitos de sorteo de censura básicos este puede ser un buen comienzo. Asumiendo que aún no ha sido bloqueado desde nuestra localidad, visita la siguiente dirección: http://sesaweenglishforum.net

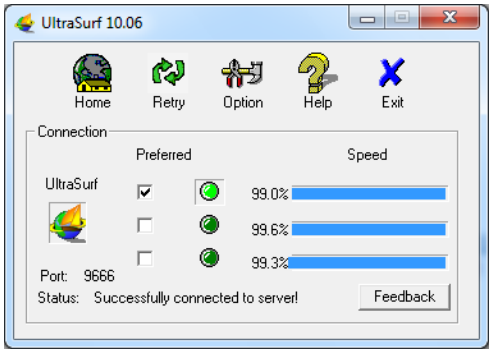
Aceptamos las Condiciones del Servicio e introducimos en la barra de URL la dirección del sitio bloqueado que queremos visitar:

Presionamos Enter o hacemos click en GO, y si navegamos satisfactoriamente al sitio solicitado entonces funciona. Si el enlace de arriba no funciona, debemos buscar un método de sorteo de censura alternativo. Los capítulos Proxy Web y Psiphon de este libro ofrecen algunas recomendaciones sobre cómo encontrar un proxy web y muchos consejos sobre si nos conviene usarlo o no una vez que decidamos hacerlo.

Si necesitamos acceso a todo un sitio como Facebook, podemos usar una herramienta instalable como Ultrasurf en lugar de un proxy Web. Si deseamos o requerimos una solución que pase por una prueba rigurosa de seguridad y que nos ayude a mantener en el anonimato sin necesidad de saber quien administra el servicio podemos usar Tor. Si necesitamos acceder a recursos no-web filtrados, como plataformas de mensajería instantánea o servidores de correo filtrado (del tipo que usan programas como Mozilla Thunderbird o Microsoft Outlook), podemos intentar con HotSpot Shield o algún otro servicio OpenVPN. Todas estas herramientas, que tienen su propio capítulo en este libro, son brevemente descritas debajo.

ACCEDIENDO A TODOS LOS SITIOS WEB BLOQUEADOS Y PLATAFORMAS

Ultrasurf es una herramienta proxy gratis para el sistema operativo Windows que puede ser descargado en http://www.ultrareach.com/, http://www.ultrareach.net/ o http://www.wujie.net/. El fichero descargable zip se extrae con un clic derecho y seleccionando “Extraer todo...”. El fichero resultante .exe puede ser inicializado directamente (incluso desde una memoria extraíble USB en un Cibercafé) sin instalación.

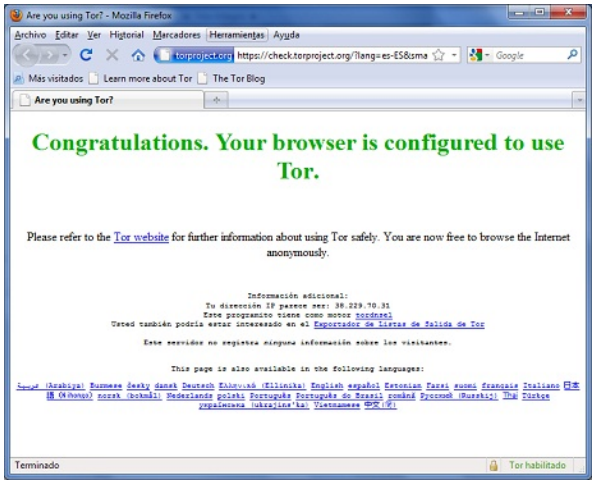


Ultrasurf se conecta automáticamente y lanza una nueva instancia del Internet Explorer que puede ser usado para abrir sitios bloqueados.

EVADIENDO LOS FILTROS Y MANTENIENDO EL ANONIMATO EN LA RED

Tor es una red de servidores proxy sofisticada. Es un programa de código abierto gratis desarrollado principalmente para permitir navegación Web anónima, pero es además una herramienta de sorteo de censura genial. El Tor Browser Bundle para Windows, Mac OS X o GNU/Linux puede descargarse desde: https://www.torproject.org/download/download.html.en. Si el sitio Web torproject.org está bloqueado, podemos intentar descargarlo escribiendo en el motor de búsqueda favorito “tor mirror” o enviando un correo electrónico a gettor@torproject.org con la palabra "help" en el cuerpo del mensaje.

Cuando hacemos clic en el fichero descargable, el se extrae en el lugar que seleccionamos. Esto puede ser también en una memoria extraíble USB en un Cibercafé. Podemos iniciar Tor haciendo clic en “Start Tor Browser” (debemos asegurarnos de cerrar cualquier instancia de Tor o Firefox que se esté ejecutando). Después de unos segundos, Tor inicia automáticamente una versión especial del navegador Web Firefox con una página de prueba. Si vemos el mensaje verde “Congratulations. Your browser is configured to use Tor ” entonces podemos usar esa ventana para abrir sitios Web bloqueados.



ENVIANDO TODO EL TRÁFICO DE INTENRNET A TRAVÉS DE UN TÚNEL SEGURO

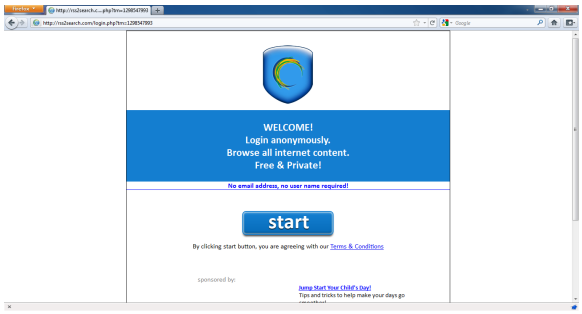
Si deseamos acceder a otros servicios de Internet, por ejemplo a un cliente de correo electrónico como Outlook o Thunderbird, una forma fácil y segura es usar una red privada virtual (VPN). Una VPN cifra y envía todo el tráfico de Internet entre nuestra computadora y otra computadora, así que no solo hará que todo el tráfico de Internet parezca similar ante una “escucha” sino que el cifrado hará ilegible el tráfico del túnel a cualquiera que esté escuchando en el camino. Mientras estamos conectados a una VPN el ISP no verá nuestro contenido, pero podrá ver que nos estamos conectando a una VPN. Como muchas compañías internacionales usan la tecnología VPN para conectar de forma segura sus oficinas remotas, es poco probable bloquear está tecnología completamente.

Hotspot Shield

Una forma fácil de empezar con VPN es usando Hotspot Shield. Hotspot Shield es una solución VPN gratis (pero es comercial) disponible para los sistemas operativos Windows y Mac OS X.

Para instalar Hotspot Shield debemos descargar el programa desde https://www.hotspotshield.com. El tamaño es de 6MB, así que en una conexión dial-up lenta tomará para descargarlo 25 minutos o más. Para instalarlo, hacemos doble clic en el fichero descargado y seguimos los pasos del asistente de instalación.

Una vez que la instalación esté completa, iniciamos Hotspot Shield desde el ícono en el escritorio o por la vía “Programas > Hotspot Shield”. Una ventana de navegación se abre con una página de estado que muestra varias etapas de conexión como "Authenticating" y "Assigning IP address". Una vez que nos conectemos, Hotspot Shield nos redirecciona a la página de bienvenida. Clic en “Start” para comenzar a navegar.



Para parar Hotspot Shield, clic derecho en el icono de la barra de tareas y seleccionamos "Disconnect/OFF".

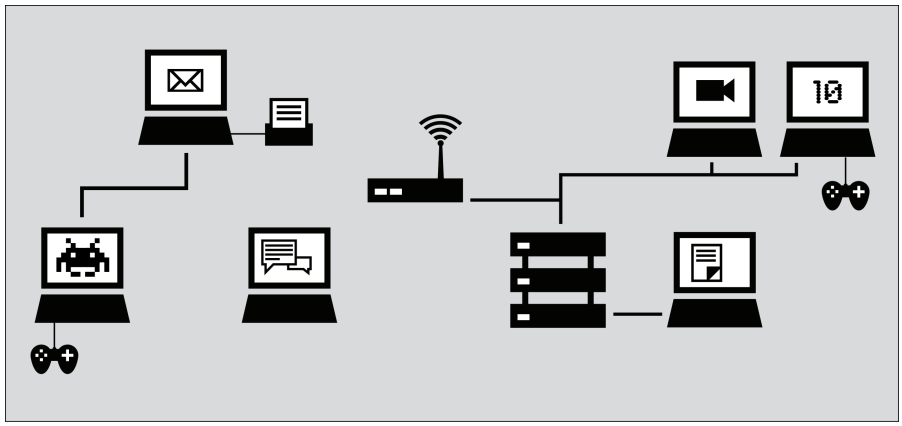
FUNDAMENTOS
4. CÓMO FUNCIONA LA RED
5. LA CENSURA Y LA RED
6. EVASIÓN Y SEGURIDAD

4. CÓMO FUNCIONA LA RED

Imaginemos un grupo de individuos que deciden compartir información en sus computadoras conectándolas y enviando información entre estas. Sus esfuerzos darán como resultado un grupo de dispositivos conectados a través de una red de computadoras. Por supuesto, la red puede ser aún más útil si puede conectarse a otras redes y por tanto a otras computadoras y otros usuarios de red. Este deseo simple de conectarse y compartir información electrónica se pone de manifiesto hoy en el Internet global. Como Internet crece rápidamente, la complejidad de sus interconexiones también aumenta, e Internet se construye literalmente desde las interacciones de un gran número de redes.

La tarea fundamental de Internet se puede decir que es facilitar el viaje de la información digital desde el origen hasta su destino, usando el camino adecuado y el modo apropiado de transportación.

Las redes de computadoras locales, llamadas Local Area Networks, o LANs, físicamente conectan un número de computadoras y otros dispositivos en una misma ubicación física. Estas pueden también conectarse a otras redes a través de unos dispositivos llamados routers que pueden gestionar el flujo de información entre redes. Las computadoras de una LAN pueden comunicarse entre sí directamente para compartir ficheros e impresoras, o para jugar video juegos en red. Una LAN puede ser útil incluso aunque no esté conectada con el mundo exterior, pero claramente es más útil cuando lo está.



Hoy Internet es una red amplia y descentralizada formada por esas redes locales de computadoras, y por otras grandes redes como las redes universitarias, las corporativas, y las redes de proveedores de alojamiento.

Las organizaciones que tramitan estas interconexiones entre redes se llaman Proveedores de Servicio a Internet (o ISP por sus siglas en inglés, Internet Service Provider). Una de las responsabilidades de los ISP es entregar datos al lugar apropiado, usualmente reenviando los datos a un enrutador (llamado "salto próximo") más cercano al destino final de los datos. A menudo, el "salto próximo" pertenece a un ISP diferente.

Con el objetivo de hacer esto, el ISP puede contratar su propio acceso a Internet a un ISP más grande, algo como un proveedor nacional. (Algunos países tienen un solo nivel de proveedor nacional, quizás operado por el gobierno o afiliados al mismo, mientras otros tienen varios, que pueden ser firmas de telecomunicaciones privadas.) De forma similar los proveedores nacionales pueden recibir sus conexiones de una compañía multinacional que mantiene y opera los servidores y conexiones que a menudo se nombran *backbone*(columna vertebral) de Internet.

El backbone está formado por instalaciones de equipamiento mayor de redes y comunicaciones globales a través de cables de fibra óptica y satélites. Estas conexiones permiten las comunicaciones entre usuarios de Internet en diferentes países y continentes. Los proveedores nacionales e internacionales se conectan a este backbone a través de enrutadores conocidos como gateways o puertas de enlace, que son conexiones que permiten a las redes comunicarse entre sí. Estas puertas de enlace, como otros enrutadores, pueden constituir un punto estratégico para monitorear y controlar el tráfico de Internet.

CONSTRUYENDO INTERNET

Los creadores de Internet creían de forma general que Internet es uno solo, que es global, y que se debería permitir comunicar dos computadoras en cualquier lugar del mundo una directamente con la otra, asumiendo que los usuarios de dichas computadoras desearan hacerlo.

En una nota en 1996, Brian Carpenter, el presidente de Internet Architecture Board, escribió:

```
en términos muy generales, la Comunidad(de ingenieros de Internet) cree que la meta es la
conectividad… (el) crecimiento de la red parece mostrar que la conectividad es su propia
recompensa, y es más valiosa que cualquier aplicación individual.
```

Existe aún una gran comunidad de pioneros de la Internet que abogan por los ideales de una inter-conectividad en todo el mundo, estándares abiertos, y acceso gratis a la información, sin embargo estas ideas muchas veces entran en conflicto con intereses políticos y de negocio y por tanto no siempre influyen las políticas y prácticas de partes individuales de Internet.

También, los creadores de Internet crearon y continúan creando estándares que persiguen facilitar a otros la creación de sus propias redes de forma más fácil, y unirlas con las demás. Entender los estándares de Internet ayuda a esclarecer cómo funciona Internet y cómo los sitios y servicios se hacen accesibles – o inaccesibles.

ESTÁNDARES PARA CONECTAR DISPOSITIVOS

La mayoría de las LANs, hoy día, se construyen con tecnología Ethernet o Ethernet inalámbrico (802.11 o Wi-Fi). Todas las interconexiones (de LANs y otros dispositivos) que forman Internet usan estándares técnicos comunes, o protocolos de Internet, para permitir a las computadoras encontrar y comunicarse con otras. A menudo, las interconexiones usan facilidades y equipamiento privado, y son operadas con fines de lucro. En algunas jurisdicciones, las conexiones a Internet son ampliamente reguladas por la ley. En otras, las regulaciones son escasas o simplemente no hay.

El estándar básico que unifica todos los dispositivos del Internet Global se llama Protocolo de Internet (IP por las siglas en inglés de Internet Protocol).

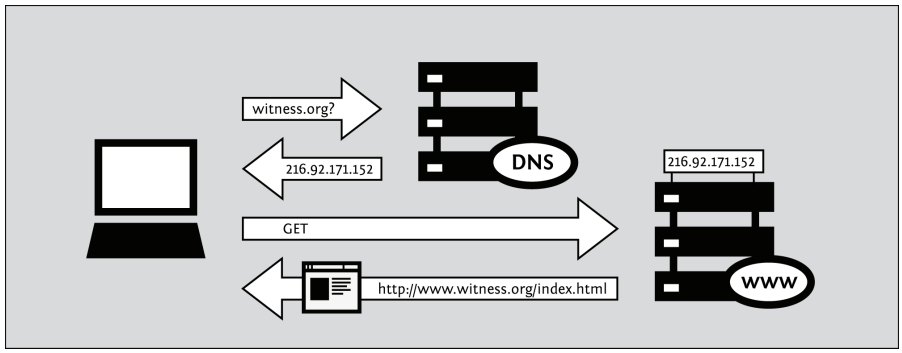
ESTÁNDARES PARA IDENTIFICAR DISPOSITIVOS EN LA RED

Cuando nuestra computadora se conecta a Internet, se le asigna una dirección numérica IP. Como una dirección postal, la dirección IP identifica únicamente una computadora en Internet. Sin embargo, a diferencia de la dirección postal, una dirección IP (particularmente en una computadora personal) no está permanentemente asociada a una computadora específica. Por eso, cuando nuestra computadora se desconecta de Internet y se reconecta más tarde, puede recibir una dirección IP (única) y diferente. La versión del protocolo IP que predomina actualmente es IPv4. En el protocolo IPv4, una dirección IP se escribe con cuatro números en el rango de 0-255, separados por puntos. (por ejemplo, 207.123.209.9).

NOMBRES DE DOMINIO Y DIRECCIONES IP

Todos los servidores de Internet, como esos que hospedan sitios Web, también tienen direcciones IP. Por ejemplo, la dirección IP de www.witness.org es 216.92.171.152. Como recordar las direcciones IP es incómodo y pueden cambiar en el tiempo, hay sistemas específicos que hacen posible que sea más fácil alcanzar el destino deseado en Internet. Este sistema es el Sistema de Nombres de Dominio (DNS por sus siglas en inglés, Domain Names System), donde un grupo de computadoras se dedican a entregar a nuestra computadora una dirección IP asociada con "nombres" más fáciles de recordar humanamente.

Por ejemplo, para acceder al sitio web Witness solo tenemos que escribir www.witness.org, conocido también como nombre de dominio, en lugar de escribir 216.92.171.152. La computadora envía un mensaje con este nombre al servidor DNS. Después que el DNS traduce el nombre de dominio en una dirección IP, comparte esta información con nuestra computadora. Este sistema hace aplicaciones de navegación Web y de Internet más amigables a los usuarios, y más amigables también a nivel de computadoras.



Matemáticamente hablando, IPv4 permite que un gran grupo de 4.2 billones de computadoras se conecten a Internet. También existen tecnologías que permiten que múltiples computadoras compartan una dirección IP. A pesar de esto, las direcciones disponibles estuvieron más o menos agotadas a principios del 2011. Como resultado se ha ideado IPv6, con un repositorio de direcciones únicas mucho mayor. Las direcciones IPv6 son mucho más largas, y más difíciles de aprender, que las direcciones tradicionales IPv4. Un ejemplo de una dirección IPv6 es:

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

Aunque todavía en el 2011 menos de un 1% de los usuarios de Internet usan el protocolo IPv6, se espera que esto cambie de forma dramática en un futuro cercano.

PROTOCOLOS PARA ENVIAR INFORMACIÓN A TRAVÉS DE LA RED

La información que trasmitimos cuando usamos Internet puede tomar varias formas:

- Un correo electrónico a un primo
- Una foto o video durante un evento
- Una base de datos con información de contacto
- Un fichero que contiene un conjunto de instrucciones
- Un documento con un reporte de un tema sensible
- Un programa de computadora que enseña una habilidad

Hay una gran variedad de programas de Internet para acomodar el manejo de varias formas de información de acuerdo a protocolos específicos, tales como:

- Correo electrónico por la vía Simple Mail Transport Protocol (SMTP)
- Mensajería instantánea vía Extensible Messaging y Presence Protocol (XMPP)
- Ficheros compartidos vía File Transfer Protocol (FTP)
- Ficheros compartidos punto a punto vía BitTorrent
- Usenet news via Network News Transfer Protocol (NNTP)
- Una combinación de protocolos: comunicación de voz usando Voice Over Internet Protocol (VoIP), Session Initiation Protocol (SIP) y Real-time Transport Protocol (RTP)

LA WEB

Aunque muchas personas usan los términos “Internet” y “la Web” indistintamente, la Web en realidad, se refiere a solo una forma de comunicación usando Internet. Cuando accedemos la Web, lo hacemos a través de un navegador Web, como Mozilla Firefox, Google Chrome, Opera o Microsoft Internet Explorer. El protocolo que opera la web se llama Hyper-Text Transfer Protocol o HTTP. Seguro hemos oído hablar de HTTPS, que es una versión segura de HTTP que usa el cifrado Transport Layer Security (TLS) para proteger las comunicaciones.

SIGUIENDO NUESTRA INFORMACIÓN EN INTERNET - EL VIAJE

Vamos a seguir los pasos del ejemplo que consiste en visitar un sitio Web desde nuestra computadora.

Conectándose a Internet

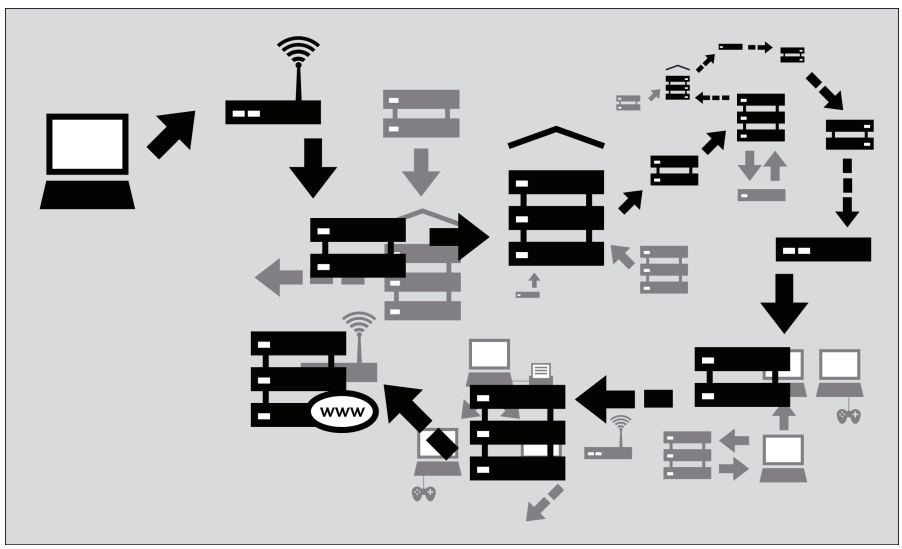
Para conectar la computadora a Internet, necesitamos algún equipamiento extra, quizás un modem o un enrutador, para conectarnos primeramente a un ISP de red. Usualmente, los usuarios finales de redes en casa están conectados con ISP por varias tecnologías:

- Modem y teléfono ("dial-up"), enviando los datos a Internet a través de líneas telefónicas en forma de llamadas telefónicas.
- DSL, una forma más eficiente y de mayor velocidad para enviar datos a través de líneas telefónicas a distancias cortas.
- Cable modem (o "Internet por cable"), enviando datos a Internet por un cable coaxial de una compañía de televisión por cable
- Cables de fibra óptica, particularmente en áreas densamente pobladas de países desarrollados
- Enlaces inalámbricos fijos de amplia cobertura, particularmente en áreas rurales
- Servicios de datos por redes de telefonía móvil

Navegando en la Web

1. Escribimos https://security.ngoinabox.org/. La computadora envía el nombre de dominio "security.ngoinabox.org" al servidor DNS seleccionado, este devuelve un mensaje que contiene la dirección IP para la "Tactical Tech Security" en un servidor web(actualmente, 64.150.181.101).
2. El navegador envía una petición para una conexión a esa dirección IP.
3. La petición viaja a través de una serie de enrutadores, cada uno reenviando una copia de la petición a un enrutador más cercano al destino, hasta que alcanza el enrutador que encuentra la computadora específica que se necesita.
4. Esta computadora envía la información de regreso a nosotros, permitiendo al navegador Web enviar la URL completa y recibir los datos a mostrar en la página.

El mensaje desde el sitio Web hasta nosotros viaja a través de otros dispositivos (computadoras o enrutadores). Cada uno de esos dispositivos se pueden llamar "hop" (salto); el número de saltos es el número de computadoras y enrutadores que el mensaje debe contactar durante el camino y casi siempre está entre 5 y 30.



¿POR QUÉ ES IMPORTANTE?

Normalmente todos estos procesos complejos están ocultos y no necesitamos entenderlos mientras estamos navegando por internet. Sin embargo, cuando las personas u organizaciones que intentan limitarnos el acceso a internet interfieren con la operación del sistema, se restringen nuestras posibilidades de utilizar Internet. En ese caso, entender lo que han hecho para bloquearnos el acceso puede ser muy relevante.

Consideremos los cortafuegos, dispositivos que intencionalmente impiden ciertos tipos de comunicación entre computadoras. Los cortafuegos ayudan a un administrador de red a forzar políticas sobre los distintos tipos de comunicación y el uso de la red. Inicialmente, el uso de estos cortafuegos fue concebido como medida de seguridad, porque ellos pueden ayudar a repeler ataques electrónicos contra computadoras vulnerables y mal configuradas. Pero los cortafuegos se están utilizando para un rango amplio de propósitos y para forzar políticas más allá de la seguridad de la computadora, incluyendo el control de contenidos.

Otro ejemplo son los servidores DNS, que fueron descritos como proveedores de direcciones IP correspondientes a los nombres de dominio solicitados. Sin embargo, en algunos casos, estos servidores pueden usarse como mecanismos de censura cuando impiden que retorne la dirección IP adecuada, y de esa forma bloquean el acceso a la información solicitada.

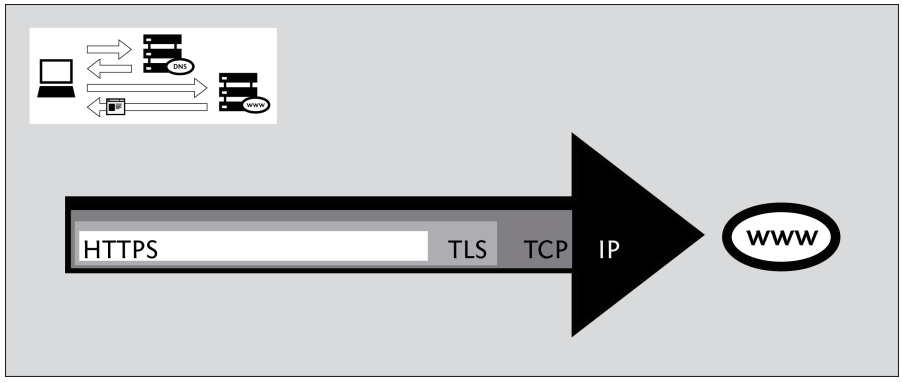
La censura puede ocurrir en varios puntos en la infraestructura de Internet, cubre redes enteras, dominios o subdominios, protocolos individuales, o contenido específico identificado por programas de filtrado. El mejor método para evitar la censura dependerá de la técnica de censura específica usada. Entender estas diferencias nos ayudaré a tomar las mejores medidas para usar Internet eficazmente y de forma segura.

PUERTOS Y PROTOCOLOS

Con el objetivo de compartir datos y recursos, las computadoras necesitan tener convenios acerca del formato y la comunicación de la información. Estos convenios, que nosotros llamamos protocolos, son algunas veces comparados con la gramática de los idiomas. Internet está basado en esos protocolos.

El modelo de red por capas

Los protocolos de Internet dependen de otros protocolos. Por ejemplo, cuando usamos un navegador Web para acceder un sitio Web, el navegador depende del protocolo HTTP o HTTPS para comunicarse con el servidor Web. Esta comunicación, a su vez, depende de otros protocolos. Supongamos que estamos usando HTTPS para un sitio Web en particular para asegurarnos que accedemos a él de forma segura.



En el ejemplo anterior, el protocolo HTPPS depende del protocolo **TSL** para realizar el cifrado de las comunicaciones para que sean privadas y no se puedan modificar durante su viaje a través de la red. El protocolo **TSL**, a su vez, depende del protocolo TCP para asegurarse que la información no se pierda accidentalmente o se corrompa durante la transmisión. Finalmente, TCP depende del protocolo IP para asegurarse de que los datos son entregados en el destino esperado.

Mientras usa el protocolo HTTPS, nuestra computadora aún usa el protocolo DNS sin cifrado para devolver una dirección IP para el nombre de dominio. El protocolo DNS usa el protocolo **UDP** para hacer que la solicitud sea dirigida hacia el servidor DNS apropiado, y UDP depende de IP para la transmisión de datos al destino esperado.

Debido a esta relación jerárquica entre protocolos, frecuentemente nos referimos a los protocolos de red como definidos en capas. Cada protocolo en su capa es responsable de un aspecto particular del funcionamiento de las comunicaciones.

Usando Puertos

Las computadoras se conectan entre sí por la vía del protocolo TCP mencionado anteriormente y se mantienen conectadas por un periodo de tiempo para que los protocolos de más alto nivel puedan realizar sus tareas. TCP usa puertos enumerados para gestionar estas conexiones y distinguir las conexiones entre sí. El uso de puertos enumerados también permite decidir cual programa en particular puede manejar una petición específica o una parte de un dato. (UDP también usa los puertos enumerados para estos propósitos.)

La **IANA** (por sus siglas en inglés, Internet Assigned Names Authority) asigna los números a los puertos para varios protocolos de alto nivel usados por servicios de aplicaciones. Algunos ejemplos comunes de números de puertos asignados son:

- 20 and 21 - FTP (transferencia de ficheros)
- 22 - SSH (secure shell remote access)
- 23 - Telnet (acceso remoto inseguro)
- 25 - SMTP (envío de correo electrónico)
- 53 - DNS (resuelve el nombre de la computadora a partir de una dirección IP)
- 80 - HTTP (navegación Web normal; también se usa a veces para un proxy)
- 110 - POP3 (recibo de correo electrónico)
- 143 - IMAP (envío/recibo de correo electrónico)
- 443 - HTTPS (conexiones Web seguras)
- 993 –IMAP seguro
- 995 - POP3 seguro
- 1080 - SOCKS proxy
- 1194 - OpenVPN
- 3128 - Squid proxy
- 8080 - Standard HTTP-style proxy

Usar estos números particulares no es generalmente un requerimiento técnico de estos protocolos; de hecho, cualquier tipo de dato puede ser enviado por cualquier puerto (y usar puertos no estándares puede ser una técnica de sorteo de censura muy útil). Sin embargo, estas asignaciones se usan por defecto, por conveniencia. Por ejemplo, nuestro navegador Web conoce que si accedemos a un sitio Web sin especificar ningún número de puerto, entonces debe intentar usar el puerto 80. Otros programas tienen otros puertos por defecto de manera que podemos usar Internet sin conocer o recordar el número de los puertos de los servicios que usamos.

Criptografía

La criptografía una forma de defensa técnica contra la vigilancia usando técnicas matemáticas sofisticadas para confundir las comunicaciones, haciéndolas ininteligibles a los ojos de un tercero. La criptografía puede impedir también a un operador de redes modificar las comunicaciones, o al menos hacer estas modificaciones detectables. Usualmente funciona como un túnel desde el programa que usamos hasta el extremo de la otra conexión, por ejemplo entre un navegador Web y un servidor Web.

La criptografía moderna es un concepto extremadamente difícil de derrotar por medios técnicos; un amplio número de programas de criptografía disponibles pueden brindarnos protección suficiente contra curiosos. Por otra parte, el cifrado puede ser saboteado por varios medios, incluyendo software dañino, o en general a través de problemas de administración de llaves e intercambio de llaves, principalmente cuando los usuarios no pueden o siguen los procedimientos necesarios para usar la criptografía de forma segura. Por ejemplo, las aplicaciones criptográficas usualmente necesitan una forma de verificar la identidad de la persona o computadora en el otro extremo de la conexión; de lo contrario, la comunicación puede ser vulnerable a un ataque "man-in–the-middle"(intermediario o interceptor, literalmente "hombre en el medio") donde un curioso se hace pasar por uno de los extremos de la comunicación para interceptar comunicaciones supuestamente privadas. Esta verificación de identidad es manejada por diferentes programas de diferentes formas, pero saltarse el paso de verificación puede incrementar la vulnerabilidad a la vigilancia.

Otra técnica de vigilancia es el **análisis de tráfico**, donde el dato acerca de una comunicación es usada para inferir algo acerca del contenido, origen, destino, o significado de la comunicación incluso si un curioso es incapaz de entender el contenido de la comunicación. El análisis de tráfico puede ser una técnica muy poderosa y contra la que es muy difícil defenderse; es un asunto concerniente de los sistemas de anonimato, donde las técnicas de análisis de tráfico pueden ayudar a identificar la parte anónima. Los sistemas de anonimato avanzados como Tor contienen algunos medios que pretenden reducir la efectividad del análisis del tráfico, pero puede ser aún vulnerable dependiendo de las habilidades del curioso.

5. LA CENSURA Y LA RED

Entender cómo se controla Internet en la práctica puede ayudar a relacionar las fuentes de la censura de Internet y sus posibles amenazas. El control y la censura de Internet pueden abarcar un amplio rango.
Un gobierno nacional puede no solo bloquear el acceso al contenido, sino también monitorear la información que acceden las persona de ese país, y puede penalizar a los usuarios relacionados con actividades que considera inaceptables. Los gobiernos pueden definir qué cosas bloquear y llevar a cabo el bloqueo, o pueden crear legislaciones, regulaciones, o incentivos extra-legales para obligar al personal de compañías independientes a llevar a cabo el bloqueo y la vigilancia.

¿QUIÉN CONTROLA INTERNET?

La historia completa del gobierno de Internet es complicada, política y todavía es disputada activamente. Los gobiernos muchas veces tienen la autoridad y los recursos para implementar sus esquemas preferidos de control y monitoreo de Internet, sin importar si la infraestructura de Internet está operada y subordinada por los propios gobiernos o por una compañía privada de telecomunicaciones. Un gobierno que desea bloquear el acceso a la información puede ejercer control directo o indirecto sobre puntos donde se produce la información, o donde entra y sale del país.

Los gobiernos tienen autoridad legal extensiva para espiar a sus ciudadanos, y muchos también van más allá de lo que permite la ley, usando métodos extrajudiciales para monitorear o restringir el uso de Internet.

IMPLICACIÓN DEL GOBIERNO

Internet fue desarrollado a partir de una investigación patrocinada por el gobierno de Estados Unidos durante 1970. Ésta se fue extendiendo gradualmente al uso académico, y después al uso público y los negocios. Hoy, existe una comunidad global de personas trabajando para mantener los estándares y acuerdos que intentan lograr una conectividad y interoperabilidad abierta a nivel mundial.

Sin embargo, los gobiernos no están obligados a implementar la infraestructura de Internet en concordancia con estos objetivos o recomendaciones relacionadas acerca de la arquitectura de Internet. Algunos gobiernos pueden diseñar sus sistemas de telecomunicaciones nacionales para tener "choke points" (puntos de sofoco), lugares donde pueden controlar el acceso del país entero a sitios y servicios específicos, y en algunos casos prevenir el acceso de su sección de Internet desde afuera.

Otros gobiernos han sobrepasado la ley o adoptado controles informales para regular el comportamiento de los proveedores de servicios de Internet privados, algunas veces obligándolos a participar en la vigilancia y supervisión, bloquear o eliminar el acceso a materiales particulares.

Algunas de las facilidades de Internet y funciones de coordinación son manejadas por gobiernos o por corporaciones bajo estatutos de gobiernos. No existe una autoridad internacional de Internet que opere completamente independiente de los gobiernos nacionales. Los gobiernos tratan la habilidad de controlar Internet y la infraestructura de las telecomunicaciones como un problema de soberanía nacional, y muchos han sostenido el derecho de prohibir o bloquear el acceso a ciertos tipos de contenidos y servicios estimados como ofensivos o peligrosos.

¿QUÉ HACE QUE LOS GOBIERNOS QUIERAN CONTROLAR LA RED?

Muchos gobiernos tienen problemas con el hecho de que solo hay un Internet Global técnicamente sin bordes geográficos o políticos. Para el usuario final (excepto por una demora de unos pocos milisegundos) no hay diferencia si un sitio web está hospedado en el propio país o al otro lado del mundo – una realidad muchas veces encantadora para los usuarios de Internet y alarmante para los estados.

La censura en Internet, inspirada por la esperanza de re-imponer las distinciones geográficas puede ocurrir por muchas razones.

- **Razones políticas**.
  Gobiernos que quieren censurar puntos de vista y opiniones contrarias a las políticas de dicho gobierno incluyendo temas como derechos humanos y religiones.
- **Razones sociales**.
  Gobiernos que desean censurar páginas web relacionadas con pornografía, juegos, alcohol, drogas, y otros asuntos que pueden ser ofensivos a la población.
- **Razones de seguridad nacional**.
  Gobiernos que desean bloquear contenido relacionado con movimientos disidentes, y cualquier cosa que amenace la seguridad nacional.

Con el propósito de asegurarse de que el control de la información es efectivo, los gobiernos pueden filtrar las herramientas que permiten a las personas sortear la censura a Internet.

En el caso extremo, los gobiernos pueden negarse a proporcionar servicio de Internet al público, como en Corea del Norte, o pueden cortar Internet durante periodos de protesta pública, como sucedió en Nepal en 2005, y en Egipto y Libia en 2011.

Este control puede estar dirigido tanto a los proveedores de acceso como a los proveedores de contenido.

- Los gobiernos pueden someter a los proveedores de acceso a un control estricto, con el objetivo de regular el tráfico de Internet, y permitir la vigilancia y el monitoreo sobre los usuarios de Internet. Esto también es una medida para bloquear el contenido global que está disponible desde el extranjero. Por ejemplo, el gobierno Pakistaní pidió a los ISPs que bloquearan el acceso a Facebook en Mayo de 2010 con el objetivo de bloquear el acceso a caricaturas del Profeta Mahoma que estaban disponibles en esta red social, pues no tenían el control sobre el proveedor de Facebook.

- Los gobiernos pueden solicitar a los proveedores de contenido, como editores de sitios Web, administradores de red, o motores de búsqueda que prohíban y bloqueen el acceso a ciertos tipos de contenido y servicios, considerados ofensivos o peligrosos. Por ejemplo, a las filiales de Google locales en algunos países se les han solicitado eliminar contenido controversial (como en China, antes de Marzo de 2010, cuando se redirigían las actividades de búsqueda hacia Google Hong Kong).

¿ESTOY BLOQUEADO O FILTRADO?

En general, determinar si alguien impide acceder a un sitio determinado o enviar información a otros puede ser difícil. Cuando tratamos de acceder a un sitio bloqueado, podemos ver un mensaje de error convencional o no ver nada. El comportamiento puede parecer que el sitio es inaccesible por razones técnicas. El gobierno o el ISP pueden negar que haya censura e incluso culpar al sitio Web (extranjero).

Algunas organizaciones, la más notable OpenNet Initiative (http://opennet.net), están usando programas para probar el acceso a Internet en varios países y entender cómo se ve comprometido el acceso por diferentes partes. En algunos casos, es una tarea difícil o incluso peligrosa, dependiendo de las autoridades concernientes.

En algunos países, no hay dudas acerca del bloqueo por el gobierno de partes de Internet. En Arabia Saudita, intentar acceder pornografía resulta en un mensaje del gobierno explicando que el sitio está bloqueado, y por qué.

En los países que bloquean sin una notificación, una de las señales más comunes de censura es que un gran número de sitios con el contenido relacionado está inaccesible por un largo período de tiempo (por ejemplo, errores "Page Not Found", o conexiones con tiempo de espera agotado). Otro es que los motores de búsqueda retornan resultados inútiles o nada acerca de ciertos tópicos.

El filtrado o el bloqueo se hace también por otras organizaciones que no son los gobiernos. Los padres pueden filtrar la información que llega a sus hijos. Muchas organizaciones, desde escuelas, compañías comerciales, restringen el acceso a Internet con el propósito de prohibir a los usuarios tener comunicaciones no monitorizadas, usar el tiempo de la compañía o el hardware para propósitos personales, infringir los derechos de autor, o usar recursos de red excesivos.

Muchos gobiernos tienen los recursos y las habilidades legales de controlar gran parte de la infraestructura del país. Si el gobierno es tu adversario, es necesario tener en cuenta que toda la infraestructura de comunicaciones desde Internet hasta las tecnologías de telefonía fija y móvil puede estar monitoreada.

CONTEXTO GEOGRÁFICO

Usuarios de diferentes lugares pueden tener variadas experiencias del control del acceso a Internet.

- En algunos lugares, el gobierno puede estar legalmente limitado a lo que pueden filtrar o no. Podríamos estar monitoreados por nuestro ISP si éste buscara vender nuestra información a compañías publicitarias. El gobierno pudiera haber pedido a nuestro ISP que instale en la red herramientas de monitoreo (no de bloqueo). El gobierno pudiera hacer una petición formal de nuestro historial de navegación y de los registros de chat, o pudiera almacenar información para usarla más tarde. Trataría de no llamar la atención mientras hace esto encubiertamente. Enfrentamos las amenazas de criminales cibernéticos que atacan los sitios Web o roban información financiera personal.

- En algunos lugares, los ISP pueden usar medios técnicos para bloquear sitios o servicios, pero el gobierno parece estar persiguiendo los intentos de acceder a éstos.

- En algunos lugares, podemos tener que acceder a servicios locales que son una copia de algún servicio extranjero. Estos servicios son patrullados por los ISP o por agentes de gobierno. Podríamos tener la posibilidad de postear información sensible, pero ésta sería eliminada posteriormente. Si esto sucede muy a menudo, las penalidades pueden ser más severas. Las restricciones solo se pueden hacer obvias durante un evento de carga política.

- En algunos lugares, nuestro gobierno puede filtrar la mayoría de los sitios Web extranjeros, especialmente noticias. Puede ejercer un control estricto sobre el ISP para bloquear el contenido y mantener rastreada a las personas que crean contenido. Si usamos una plataforma de red social, se harán esfuerzos para infiltrarla. Pudiera alentar a nuestros vecinos para espiarnos.

CONTEXTO PERSONAL

Los gobiernos tienen un rango de motivaciones para monitorear o restringir diferentes tipos de actividad en línea.

- Activistas: que quizás quieran mejorar su gobierno o estás buscando uno nuevo; reformar un segmento en particular de la sociedad o trabajar por los derechos de una minoría; exponer cuestiones del ambiente, abusos de trabajo, fraude, o corrupción en puestos de trabajo. El gobierno y empleadores pueden no estar de acuerdo con esto y pueden realizar acciones para monitorear la Internet si creen que habrán manifestaciones.

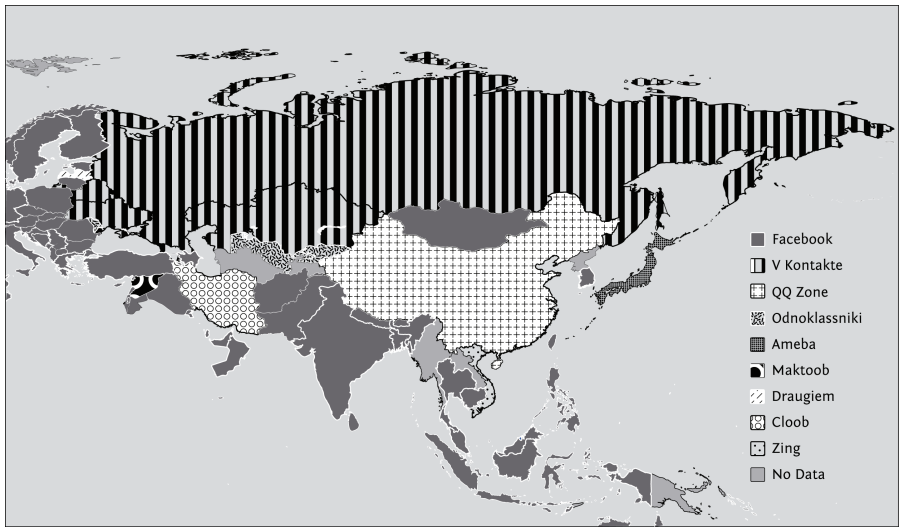
- Blogueros: personas que quizás quieran escribir sobre la vida cotidiana, pero están silenciadas debido a su origen étnico, o simplemente no se supone que opinen con independencia de cual sea su opinión. Puede que estén en un país donde la mayoría de los usuarios no son restringidos, pero sus opiniones no son populares en su comunidad. Puede que prefieran el anonimato o necesite conectarte con un grupo de soporte.

- Periodistas: pueden tener las mismas inquietudes de los activistas y blogueros. Hacer reportajes sobre el crimen organizado, la corrupción y la brutalidad del gobierno suele ser peligroso. Necesitan protección y proteger a cualquier activista que sea fuente de información.

- Lectores: puede que no sea políticamente activo, pero hay tanto contenido censurado que necesita una herramienta de evasión para alcanzar los periódicos de entretenimiento, ciencia e industria. Puede que quiera leer una Web cómica o navegar en las noticias de otros países. El gobierno puede ignorar esto hasta que tenga otra razón para monitorearlos.

El recurso de Internet más bloqueado solían ser los sitios de material sexual explícito; hoy son las plataformas de red social. El aumento de la popularidad de estos sitios ha convertido a millones de usuarios de Internet en víctimas potenciales de la censura.

Algunos sitios de red social son populares a nivel mundial, como Facebook, MySpace o LinkedIn, mientras otros tienen un gran número de usuarios en un país o región determinado: QQ (Qzone) en China, Cloob en Irán, vKontakte en Rusia, Hi5 en Perú y Colombia, Odnoklassniki en los países CIS, Orkut en India y Brazil, Zing en Vietnam, Maktoob en Syria, Ameba y Mixi en Japan, Bebo en UK, y otros.



¿CÓMO FUNCIONA LA CENSURA?

[Esto es adaptado en parte de Access Denied, Capítulo 3, de Steven J. Murdoch and Ross Anderson.]

El filtrado de Internet consiste en una serie de técnicas que los censuradores utilizan para tratar de impedir que los usuarios accedan a contenidos o servicios determinados. Los operadores de redes pueden filtrar o manipular el tráfico de Internet en cualquier punto de una red, usando una amplia variedad de tecnologías, con niveles variables de exactitud y personalización. Generalmente, el filtrado implica el uso de programas para revisar qué están tratando de hacer los usuarios e interferir selectivamente con actividades que los operadores consideran van en contra de sus políticas. Un filtro puede ser creado y aplicado por un gobierno nacional o por un proveedor nacional o local o incluso por un operador de una red local; o pueden ser filtros basados en software que es instalado directamente en las computadoras individuales.

Los objetivos de desplegar un mecanismo de filtrado varían dependiendo de las motivaciones de las organizaciones interesadas en hacerlo. Puede ser el de hacer un sitio Web particular (o una página Web individual) inaccesible a aquellos que la visiten, hacerlo ilegible, o determinar incluso los usuarios que intentan acceder éstos recursos. La selección de un mecanismo también dependerá de la capacidad de la organización que solicita el filtrado – el acceso e influencia que tenga, las personas contra las que se enfrenta, y lo que piensa gastar en este proceso. Otras consideraciones incluyen el número de errores aceptables, si el filtrado debe ser encubierto o no, y cuan inexpugnable es (tanto para usuarios casuales para aquellos dispuestos a evadirlo).

A continuación se describirán varias técnicas a partir de las cuales se pueden bloquear algunos contenidos una vez que la lista de recursos a bloquear esté determinada. Construir esta lista es un reto considerable y una debilidad común en los sistemas desarrollados. No solo la enorme cantidad de sitios Web a bloquear representa una dificultad, sino que los sitios al estar en constante movimiento y cambiar de dirección IP, hacen que mantener esta lista actualizada requiera un esfuerzo aún mayor. Más aún, si un operador de un sitio desea interferir con el bloqueo, el sitio se moverá más rápido que cualquier otro.

Primero se describirá los medios técnicos que se usan contra los usuarios, y después brevemente se discutirá los medios usados contra los publicadores y proveedores de hospedaje, así como intimidación no-técnica.

Es necesario notar que la lista de métodos no es exhaustiva, y más de una de estas tácticas deben ser aplicadas en casos particulares.

MEDIOS TÉCNICOS CONTRA LOS INTERNAUTAS

En redes de comunicaciones modernas como Internet, la censura y la vigilancia (el monitoreo de las actividades y comunicaciones de las personas) están íntimamente conectadas en la práctica.

La mayoría de los ISP en el mundo monitorean algunos aspectos de las comunicaciones de sus usuarios para propósitos contables y para combatir abusos como el envío de SPAM. Los ISP usualmente guardan los nombres de cuenta de los usuarios junto a la dirección IP. A menos que los usuarios empleen tecnologías de mejora de privacidad para evitar esto, es técnicamente posible para un ISP almacenar toda la información que fluye por sus cables, incluyendo el contenido exacto de las comunicaciones de los usuarios.

Esta vigilancia es también un prerrequisito para llevar a cabo una censura técnica en la red. Un ISP que intenta censurar las comunicaciones que sus usuarios desean enviar necesita ser capaz de leer estas comunicaciones para poder determinar quien viola sus políticas. Por lo tanto, un acercamiento a reducir la censura de Internet es ocultar de los ISP el contenido de las comunicaciones, y reforzar el uso de tecnologías que mejoran la privacidad y obstaculizan la supervisión.

Estos medios contra la censura muchas veces dependen de la ofuscación o el cifrado para dificultar al ISP el acceso al contenido exacto que fue transmitido.

Esta sección discute algunos de las formas específicas que utilizan los censuradores para bloquear el acceso a partir de medios técnicos.

Filtrado por URL

Un criterio para bloquear el acceso a información en la Web por parte de muchos países y otras entidades consiste basarse en la URL – puede ser la **URL** entera o parte de ella. Los censuradores de Internet casi siempre desean bloquear **dominios** Web específicos en su totalidad, por el contenido de esos dominios. Pueden bloquear dominios por el nombre o el número IP. Algunas veces, las autoridades son más selectivas, bloquean solo ciertos **subdominios** en un dominio en particular, mientras dejan el resto accesible. Este es el caso de Vietnam, donde el gobierno bloquea secciones específicas de un sitio web (como las versiones en lenguaje vietnamita de BBC y Radio Free Asia).

Los censuradores, por ejemplo, pueden querer filtrar solo el subdominio news.bbc.co.uk, mientras se deja bbc.co.uk y www.bbc.co.uk sin filtrar. De forma similar, pudieran querer filtrar páginas que contengan tipos específicos de contenido mientras se deja acceso al resto del dominio que las hospeda. Un enfoque para el filtrado es bloquear solo un directorio como por ejemplo "worldservice" para bloquear solo el servicio de noticias en idioma extranjero de la bbc en bbc.co.uk/worldservice, sin necesidad de bloquear el sitio en inglés de la BBC en su totalidad. Los censuradores pueden a veces incluso bloquear páginas específicas basadas en el nombre de la página o en términos de búsquedas que sugieran contenido no deseado o ofensivo.

El filtrado de URL se puede llevar a cabo localmente, a través del uso de algún software especial instalado en la computadora que usamos. Por ejemplo, las computadoras de un Cibercafé pueden ejecutar un programa de filtrado que impide el acceso ciertos sitios.

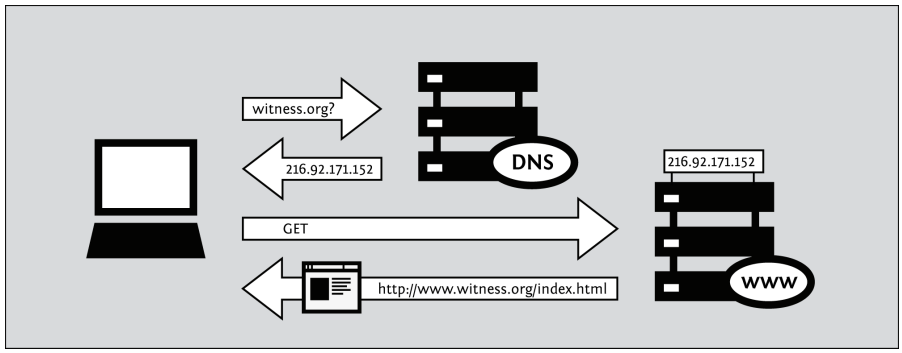
El filtrado de URL puede llevarse a cabo en un punto central de la red, como en un **servidor proxy**. Una red puede configurarse para que no permita a sus usuarios conectarse directamente a los sitios web sino forzarlos a acceder a los sitios por la vía de un servidor proxy.

Los servidores proxis se usan para retransmitir una solicitud, así como páginas web almacenadas en su caché y entregarlas a múltiples usuarios. Esto reduce la necesidad del ISP de tramitar peticiones a páginas populares, y por tanto aprovecha los recursos y mejora el tiempo de entrega.

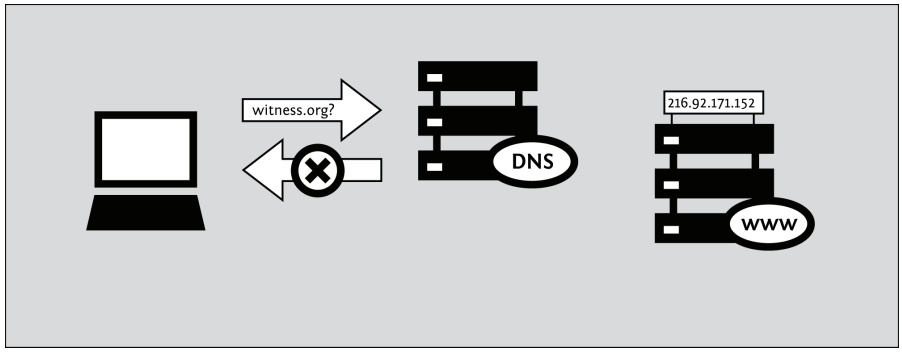
Sin embargo, así como para mejorar el rendimiento, un proxy HTTP puede usarse también para bloquear sitios web. El proxy decide si las peticiones deben ser permitidas. Aunque el contenido completo de la petición esté disponible, las páginas Web individuales pueden ser filtradas, basadas en el nombre de la página y el contenido actual de la página. Si una página es bloqueada, el servidor proxy puede devolver una explicación del por qué, o pretender que la página no existe y mostrar un error.

Filtrado y falsificación de DNS

Cuando entramos un nombre de dominio en un navegador Web, la primera cosa que hace el navegador es preguntar a un servidor **DNS (Domain Name System)** en una dirección numérica conocida, la dirección IP correspondiente.



Si el DNS está configurado para bloquear el acceso, consulta una **lista negra** de nombres de dominios prohibidos. Cuando un navegador solicita una dirección IP por uno de estos nombres de dominios, el servidor DNS da una respuesta incorrecta o no responde nada.



Cuando el servidor DNS da una respuesta sin sentido o simplemente no responde, la computadora que hace la solicitud no aprende la dirección IP del servicio que desea contactar. Sin la dirección IP correcta, la computadora solicitante no puede continuar, y muestra un mensaje de error. Como el navegador no encuentra la dirección IP correcta, no es capaz de contactar al sitio para solicitar la página. El resultado es que todos los servicios bajo un nombre de dominio particular, ejemplo todas las páginas de un servidor Web determinado, no estarán disponibles. En este caso, el bloqueo puede aparecer erróneamente como un problema técnico o una falla aleatoria.

Similarmente, un censurador puede forzar una entrada para direccionar a una IP incorrecta, y así redirigir a los usuarios a sitios Web incorrectos. Esta técnica es llamada falsificación de DNS(DNS spoofing), y los censuradores pueden usarla para piratear la identidad de un servidor particular y mostrar sitios web ficticios o dirigir el tráfico de los usuarios a servidores sin autorización que pueden interceptar los datos. (En algunas redes, la respuesta incorrecta guiará a un servidor web diferente que explica la razón del bloqueo que ha ocurrido. Esta técnica es usada por los censuradores que no les importa admitir que ellos censuran el tráfico y que no quieren confundir a los usuarios respecto a lo que está sucediendo.)

Filtrado IP

Cuando se envía algún dato por Internet, es dividido en segmentos e introducidos en paquetes. Un paquete contiene el dato enviado y la información de a donde enviarlo, concretamente la dirección IP de la computadora de la que viene el mensaje y a la que debe ir. Los **enrutadores** son computadoras por las que atraviesan paquetes en su ruta desde el remitente hasta el receptor, para determinar a donde ir en cada paso. Si los censuradores quieren prohibir a los usuarios el acceso a servidores específicos, pudieran configurar los enrutadores que ellos controlan para **descartar** los paquetes destinados a determinadas direcciones IP en una lista negra o retornar un mensaje de error. El filtrado basado en direcciones IP bloquea todos los servicios proporcionados desde esa dirección, tales como sitios Web y servidores de correo. Como solo la dirección IP es controlada, muchos **nombres de dominios** que comparten la misma dirección IP serán bloqueados también aún si esta no fuese la intención original.

Filtrado de palabras clave

El filtrado de IP solo puede bloquear la comunicación basándose en a dónde van los paquetes o de donde vienen, y no en cuanto a sus contenidos. Esto puede ser un problema para el censurador si le fuese imposible establecer la lista completa de direcciones IP con contenido prohibido, o si una dirección IP contiene suficiente contenido no-prohibido que haga injustificable el bloqueo total de todas las comunicaciones. Hay un control incluso más fino: consiste en inspeccionar los paquetes a partir de palabras claves. Como normalmente los enrutadores no examinan el contenido de los paquetes, se necesita un equipo extra; el proceso de examinar el contenido de los paquetes a menudo se llama **inspección profunda de paquetes**.

Una comunicación que se haya identificado como portadora de contenido prohibido puede ser interrumpida bloqueando los paquetes directamente o enviando un mensaje a ambas partes de la comunicación avisando que la otra parte ha terminado la conversación. El equipamiento que lleva a cabo estas funciones de censura está disponible en el mercado.

Alternativamente, el censor puede usar un proxy HTTP, como se mencionó anteriormente.

Acondicionamiento del tráfico

El acondicionamiento del tráfico es una técnica utilizada por los administradores de red para hacer que el tráfico sobre ésta fluya suavemente priorizando algunos paquetes y demorando otros que encajan con algún criterio. Ésta preparación del tráfico es parecida al hecho de controlar el tráfico de los vehículos en una avenida. En general, todos los vehículos (paquetes) tienen la misma prioridad, pero algunos vehículos son demorados por los controladores de tráfico o por las luces que evitan atascos en ciertos puntos. Al mismo tiempo, algunos vehículos (camiones de bomberos, ambulancias) necesitan alcanzar su destino más rápido, y por lo tanto ellos son priorizados al demorar otros vehículos. Una lógica similar es aplicable a los paquetes de Internet que necesitan una **latencia** baja para un rendimiento óptimo (como **voz sobre IP, VoIP**).

El acondicionamiento del tráfico puede ser usado además por gobiernos u otras entidades para demorar paquetes con información específica. Si los censuradores quieren restringir el acceso a ciertos servicios, ellos pueden fácilmente identificar paquetes relacionados con estos servicios e incrementar su latencia haciendo que su prioridad sea baja. Esto puede dar la impresión engañosa a los usuarios de que un sitio es inherentemente lento, o puede desfavorecer el acceso al sitio con respecto a otros. Esta técnica es algunas veces aplicada contra las redes de archivos compartidos punto-a-punto, como **BitTorrent**, por los ISP que no están a favor de la compartición de archivos.

Bloqueo de puertos

Poner en lista negra números de puertos individuales restringe el acceso a servicios individuales en un servidor, como el Web o el de correo electrónico. Los servicios más estándares en Internet tienen números de puertos característicos. La relación entre servicios y números de puertos son asignados por IANA, pero no son obligatorios. Estas asignaciones permiten a los enrutadores suponer el servicio que ha sido accedido. Así, para bloquear solo el tráfico web de un sitio Web, un censurador puede bloquear el puerto 80 solamente, porque ese es el puerto que típicamente se usa para el acceso web.

El acceso a los puertos puede ser controlado por el administrador de red de la organización donde se encuentra nuestra computadora- así sea una compañía privada o un cibercafé, o por el proveedor de acceso a Internet, o por cualquier otro como un censurador de gobierno que tiene acceso a las conexiones disponibles al ISP. A veces el bloqueo de puertos se hace por otras razones que no tienen que ver con la censura- para reducir el SPAM, o para desalentar a usuarios que comparten ficheros punto-a-punto, mensajería instantánea, o juegos en línea.

Si un Puerto es bloqueado, todo el tráfico que pasa por ese puerto se hace inaccesible. Los censuradores a menudo bloquean los puertos 1080, 3128, y 8080 porque estos son los puertos de proxy más comunes, necesitaremos usar una técnica de evasión diferente o encontrar un proxy que escuche por un puerto no común.

Por ejemplo, en una Universidad, solo los puertos 22 (SSH), 110 (POP3), 143 (IMAP), 993 (IMAP seguro), 995 (POP3 seguro) and 5190 (ICQ mensajería instantánea) pueden estar abiertos para conexiones externas, forzando a los usuarios a usar tecnología de evasión o acceder servicios o puertos no estándares si desean usar otro servicio de Internet.

Cierre de Internet

El cierre de la conectividad a Internet es un ejemplo de extrema censura perpetrado por gobiernos en respuesta a eventos sensibles ya sean políticos o sociales. Sin embargo, la interrupción de toda la red (o sea, de ambas redes la doméstica y la internacional) requiere un trabajo intenso, ya que es necesario apagar no solo los protocolos que conectan a los países con la red internacional sino también hay que cerrar los protocolos que conectan los ISP con otros y con los usuarios. Hay países que han cerrado completamente el acceso a Internet (Nepal en 2005, Myanmar en 2007 y Egipto y Libia en 2011) para reprimir los disturbios políticos. Estos cierres de Internet pueden durar desde horas hasta semanas, aunque algunas personas se las agencian para conectarse por vía dial-up a un ISP extranjero o usando su conexión móvil o enlaces satelitales.

Romper las conexiones internacionales, por lo tanto, no necesariamente destruye la conectividad de ISP domésticos o la comunicación entre varios usuarios de un ISP individual. Tomaría algunos pasos para aislar completamente a los usuarios de una red interna. Por esta razón, es más difícil interrumpir la conectividad doméstica en países con varios ISP.

ATAQUES A EDITORES

Los censuradores pueden también intentar suprimir contenido y servicios en sus fuentes atacando la habilidad de los editores de publicar información. Esto se puede lograr de varias formas.

Restricciones legales

Algunas veces, autoridades legales pueden persuadir a los operadores de servicio para que cooperen con la censura. Algunos proveedores de correo electrónico o blogs, por ejemplo, pueden decidir realizar el filtrado de palabras claves con sus propios servidores – quizás porque el gobierno les dice que lo hagan. (En este caso, no hay mucha esperanza de que algún tipo de "evasión" neutralice la censura, generalmente se considera la "evasión" como un esfuerzo por alcanzar el servicio de red deseado en algún lugar, ya sea en diferentes países o jurisdicciones).

Denegación de Servicio

En los lugares en los que las organizaciones no tienen la autoridad (o acceso a la infraestructura de red) para adicionar mecanismos de bloqueo convencionales, los sitios Web pueden hacerse inaccesibles recargando el servidor o las conexiones de redes. Esta técnica, conocida por ataque de Denegación de Servicio (DoS por sus siglas en inglés), puede montarse por una computadora con una conexión a Internet muy rápida; más comúnmente, un gran número de computadoras son tomadas y usadas para montar un ataque DoS distribuido (**DDoS**).

Borrado de dominio

Como se mencionó anteriormente, la primera etapa de una solicitud Web es contactar el servidor DNS local para encontrar la dirección IP del servicio deseado. Almacenar todos los nombres de dominio que existen en la actualidad sería poco factible, en su lugar los llamados tramitadores recursivos almacenan punteros a otros servidores DNS los que pueden saber con más probabilidad la respuesta. Estos servidores dirigirán al tramitador recursivo hacia otros servidores DNS hasta uno, el servidor "autoritario", que es entonces el que retorna una respuesta.

El sistema de nombres de dominio está organizado jerárquicamente, con dominios de países tales como ".uk" y ".de" en el tope, junto a dominios no geográficos como ".org" y ".com". Los servidores responsables de estos dominios delegan responsabilidad por subdominios, como example.com, a otros servidores DNS, dirigiendo solicitudes para estos dominios. Así, si el servidor DNS de un dominio de nivel máximo des registra un nombre de dominio, los solucionadores recursivos serán incapaces de descubrir la dirección IP y así hacer el sitio inaccesible.

Los dominios de nivel máximo específicos de países son usualmente operados por el gobierno de país en cuestión, o por organizaciones destinadas para hacerlo. Así que si un sitio se registra bajo el dominio de un país que prohíbe el contenido hospedado, corre el riesgo que su dominio sea borrado.

Desmontaje de servidores

Los servidores que hospedan contenido deben estar ubicados físicamente en algún lugar, así como el operador que los opera. Si estos lugares están bajo control legal o extra-legal de alguien que está en contra del contenido hospedado, el servidor puede ser desconectado o el operador puede requerir deshabilitarlo.

INTIMIDACIÓN DE USUARIOS

Los censuradores pueden incluso tratar de determinar los usuarios que intentan acceder a materiales determinados en varias formas.

Vigilancia

Los mecanismos anteriores inhiben el acceso al material prohibido, pero son crudos y posibles de evadir. Otra aproximación, que se puede aplicar en paralelo al filtrado, es monitorear cual sitio Web ha sido visitado. Si el contenido prohibido es accedido (o se intenta accederlo) entonces se pueden llevar a cabo castigos legales (o extra legales).

Si este hecho es ampliamente difundido, puede desmotivar a otros a que accedan al contenido prohibido, incluso si las medidas técnicas para prevenir el acceso son inadecuadas por sí mismas. En algunos lugares, los censuradores tratan de crear la impresión de que sus agentes están en todas partes y que todo el mundo está siendo vigilado – aunque no sea realmente el caso.

Técnicas Sociales

Los mecanismos sociales son usados frecuentemente para acceder contenidos inapropiados. Por ejemplo, las familias pueden ubicar la PC en la sala donde la pantalla está visible a todos los presentes, en lugar de hacerlo en un lugar más privado, esta forma simple evita que los niños accedan sitios inapropiados. En bibliotecas o cuartos de estudios se pueden ubicar las PCs de modo que sus pantallas se vean visibles desde el escritorio del bibliotecario. Un CyberCafé puede tener una cámara de vigilancia CCTV (Circuito Cerrado de Televisión). Puede ser que exista una ley local que exija el uso de cámaras, y que exija también que los usuarios se registren con una identificación de foto pública de gobierno.

Robando y destruyendo equipamiento de comunicaciones

En algunos lugares, los censuradores tienen la capacidad de prohibir algunos tipos de tecnologías de comunicaciones completas. En este caso, ellos deberán eliminar obviamente y destruir el equipamiento de comunicación y mandar así el mensaje de que su uso no será tolerado.

6. EVASIÓN Y SEGURIDAD

El tipo de seguridad que necesitamos depende de nuestras actividades y sus consecuencias. Hay algunas medidas de seguridad que todos debiéramos practicar aunque no nos sintamos amenazados. Algunas formas de ser cautelosos en línea requieren más esfuerzo, pero son necesarias debido a severas restricciones al acceso a Internet. Podemos estar amenazados por tecnología que se esté investigando y poniendo en práctica rápidamente, vieja tecnología, uso de inteligencia humana, o la combinación de las tres. Todos estos factores pueden cambiar a menudo.

ALGUNAS BUENAS PRÁCTICAS DE SEGURIDAD

Hay algunos pasos que todo el mundo debiera dar para mantener su computadora segura. Esto va desde proteger la información de nuestra red de activistas hasta el número de nuestra tarjeta de crédito, pero en todos estos casos las herramientas pueden ser las mismas.

Debemos tener cuidado de los programas que prometen una seguridad perfecta: la seguridad en línea es la combinación de un buen programa y de un buen comportamiento humano. La tecnología por sí sola no nos ayuda a saber lo que debemos mantener offline, en quien confiar, y otras preguntas de seguridad. Por eso debemos buscar programas que tengan listadas sus debilidades conocidas en el sitio de sus autores o programas que sean revisados o validados por terceros.

Es necesario mantener nuestro sistema operativo actualizado: los desarrolladores de sistemas operativos brindan actualizaciones que debemos instalar de cuando en cuando. Esto se puede hacer de forma automática o podemos solicitarla entrando un comando o ajustando la configuración del sistema. Algunas de estas actualizaciones hacen nuestras computadoras más eficientes y facilitan su uso, y otras reparan huecos de seguridad. Los atacantes aprenden sobre los huecos de seguridad de forma rápida, algunas veces incluso antes de que sean reparados, así que repararlos a tiempo es crucial.

Si aún usamos Microsoft Windows, debemos usar un antivirus y mantenerlo actualizado. Se denota por **malware** a los programas desarrollados con el propósito de robar información o para usar nuestra computadora para otros propósitos.
Los virus y el **malware** en general pueden ganar acceso en nuestro sistema, hacer cambios y ocultarse. Estos pueden llegar a nosotros a través del correo electrónico, o estar simplemente en alguna página Web que visitemos, o ser parte de un fichero que no parezca sospechoso. Los proveedores de programas antivirus constantemente investigan las amenazas emergentes y las adicionan en la lista de cosas que nuestra computadora debe bloquear. Con el objetivo de permitir que el programa reconozca nuevas amenazas debemos instalar las actualizaciones en la medida que son publicadas.

Es necesario el uso de buenas contraseñas: todos los sitemas de contraseña son vulnerables, pero podemos mejorar nuestra seguridad haciendo más difícil de adivinar nuestras contraseñas. Es necesario usar combinación de letras, signos de puntuación y números. Combinar letras mayúsculas y minúsculas. No usar números de cumpleaños, o palabras que puedan ser adivinadas a través de información pública acerca de nosotros.

Es aconsejable también usar programas de código abierto, (FOSS por sus siglas en inglés, Free and Open Source Software). Los programas de código abierto están disponibles como productos terminados o productos en desarrollo para usuarios e ingenieros de software. Esto ofrece algunas ventajas en cuanto a seguridad, frente a los programas de código cerrado que solo están disponibles en los países a través de canales ilegales debido a restricciones de exportación o costo. Quizás no podamos descargar actualizaciones oficiales para software pirateado. Con los programas de código abierto no hay necesidad de buscar a través de sitios de dudosa procedencia una copia libre de spyware y de problemas técnicos. Cualquier copia legítima será gratis y será provista por sus creadores. Si emergen defectos en la seguridad, serán reparados por voluntarios y usuarios interesados. Una comunidad de ingenieros trabajarán en la solución, rápidamente.

También es bueno usar programas que separen "quienes somos" del "donde estamos". Toda computadora conectada a Internet tiene una dirección IP. Una dirección IP puede ser usada para encontrar nuestra ubicación física tecleando dicha dirección en algún sitio "whois". Los proxis, **VPN** y Tor enrutan nuestro tráfico a través de una a tres computadoras alrededor del mundo. Si vamos a pasar por un solo servidor, debemos tener en cuenta que al igual que un ISP, el operador del proxy puede ver todo nuestro tráfico. Puede que confiemos mas en el operador del proxy que en el ISP, pero las mismas advertencias se aplican para cualquier fuente individual de conectividad. Ver las secciones que abarcan proxis, Tor, y VPN para más detalles sobre sus riesgos.

Otro elemento de importancia es usar CDs y memorias USB booteables. Si usamos una computadora de uso público o cualquier otra en la que no queramos dejar datos, es aconsejable usar una versión de Linux que podamos ejecutar desde una memoria USB. Los CD y memorias USB booteables se pueden usar sin necesidad de instalar nada.

Es bueno también usar programas "portables": hay versiones portables de programas de evasión que se pueden ejecutar en Windows desde una memoria USB.

Por último es necesario mantenernos informados. La tecnología que funciona hoy puede mañana dejar de hacerlo o ser insegura. Incluso aunque no la necesitemos ahora, debemos saber dónde encontrar la información. Si los proveedores de programa que usamos tienen forma de brindar soporte, debemos asegurarnos de cómo contactarlos antes que los sitios sean bloqueados.

ACCEDIENDO A REDES SOCIALES DE FORMA MÁS SEGURA

En el contexto de las sociedades cerradas y los países autoritarios, el monitoreo se convierte en la mayor amenaza para los usuarios de redes sociales, especialmente si usan el servicio para coordinar actividades sociales y civiles o conectarse con el activismo en línea o el periodismo nacional.

Un tema central con la plataforma de red social es la cantidad de datos privados que compartimos sobre nosotros mismos, nuestras actividades y nuestros contactos, y quienes tienen acceso a esto. Como la tecnología evoluciona y las plataformas de red social son más accedidas a través de teléfonos sofisticados, la revelación de las ubicaciones de los usuarios de una plataforma de red social en cualquier momento se convierte en una amenaza significativa.

En este contexto, algunas precauciones son cruciales; por ejemplo debemos:

- revisar nuestra configuración de privacidad
- saber precisamente que información compartimos y con quién
- asegurarnos de que entendemos la configuración de posicionamiento geográfico, y editarla si es necesario
- solo aceptar en nuestra red personas en las que realmente confiemos
- solo aceptar en nuestra red personas que protegerán nuestra información privada
- tener en cuenta que incluso las personas más confidentes pueden dar información nuestra si se sienten amenazadas por nuestro adversario, así que es necesario limitar quién accede a qué información
- tener en cuenta que acceder a una plataforma de red social por la vía de una herramienta de evasión no nos protegerá automáticamente de las amenazas a nuestra privacidad

Una lectura recomendada es este artículo de Privacy Rights Clearinghouse: "Social Networking Privacy: How to be Safe, Secure and Social": http://www.privacyrights.org/social-networking-privacy/#general-tips

¿Cómo podemos acceder a nuestra plataforma de red social cuando está filtrada?

Como se describió antes, usar HTTPS para acceder a sitios Web es importante. Si nuestra plataforma de red social permite accesos HTTPS, debemos usarlo exclusivamente y si es posible, hacerlo por defecto. Por ejemplo, en Facebook, podemos editar nuestra configuración de cuenta: Account Settings > Account Security > Secure Browsing (https) para lograr que HTTPS sea la vía de conexión por defecto en nuestra cuenta. En algunos lugares, usar HTTPS nos permite acceder a algunos servicios bloqueados; por ejemplo, http://twitter.com/ ha sido bloqueado en Burma mientras https://twitter.com/ permanece accesible.

Si deseamos proteger nuestro anonimato y privacidad mientras usamos una herramienta de evasión un túnel SSH o VPN nos pueden garantizar una mayor privacidad que un proxy web, incluso ante el riesgo de revelar nuestra dirección IP. Incluso usando una red anónima como Tor puede ser insuficiente porque las plataformas de red social hacen que sea muy fácil revelar la

información de identificación y exponer detalles de nuestros contactos y relaciones sociales.

USO MÁS SEGURO DE COMPUTADORAS DE USO COMPARTIDO

Una proporción significativa de la población mundial, especialmente en países desarrollados, no tienen acceso personal a Internet desde su casa. Esto puede ser debido a los costos de tener Internet privado en las casas, la falta de equipamiento de computadoras personales, o problemas en las infraestructuras de redes eléctricas y de telecomunicaciones.

Para esta parte de la población el único medio razonable para acceder a Internet es usar lugares donde las computadoras se comparten entre individuos diferentes. Esto incluye cibercafés, Telecentros, estaciones de trabajo, escuelas o bibliotecas.

Ventajas potenciales de computadoras compartidas

Hay ventajas al acceder a Internet en computadoras compartidas:

- Podemos recibir consejos o asistencia técnica de otros usuarios o personal capacitado en cómo evadir el filtrado.
- Las herramientas de evasión pueden estar instaladas y pre-configuradas.
- Los usuarios pueden compartir información no censurada a través de medios sin conexión.
- Si no somos usuarios regulares de un local de navegación en particular, no tenemos que ofrecer documentos identificativos al operador de dichas habilidades y no tenemos que registrarnos usando nuestro nombre real o información de cuenta, será más difícil rastrearnos basándose en nuestra actividad en línea.

Riesgos generales de las computadoras compartidas

El hecho de que accedamos a Internet desde un espacio público no lo hace anónimo o más seguro para nosotros. Es muy posible que sea todo lo contrario. Algunas de las principales amenazas son:

- El dueño de la computadora, o incluso la persona que la usó antes de nosotros, puede fácilmente programar la computadora para que espíe lo que hacemos, incluyendo que puede guardar todas nuestras contraseñas. La computadora también puede ser programada para evadir y anular cualquier protección de privacidad o software de seguridad que usemos.
- En algunos países como Burma y Cuba, los clientes de cibercafés tienen que mostrar su carnet de identidad o número de pasaporte antes de usar un servicio. Esta identificación puede ser almacenada junto al historial de navegación Web.
- Cualquier información que dejemos en la computadora puede ser registrada (historial de navegación, cookies, ficheros descargados, etc.).
- Pueden estar instalados programas que guarden cada golpe de teclado durante nuestra sesión. Incluyendo nuestras contraseñas, incluso antes que esta información sea enviada a Internet. En Vietnam, un teclado aparentemente inocente para teclear caracteres vietnamitas fue usado para monitorear las actividades en los cibercafés y en otros lugares de acceso público.
- La actividad de nuestro monitor puede ser guardada por un programa que toma instantáneas de pantalla en intervalos regulares, monitoreados a través de cámaras CCTV, o simplemente observados por una persona (por ejemplo, el administrador de un cibercafé) sobre nuestro hombro.

Computadoras compartidas y censura

Además de la vigilancia, los usuarios de computadoras compartidas a menudo tienen acceso limitado a Internet y tienen que enfrentar obstáculos adicionales para usar su herramienta de evasión favorita:

- En algunos países, como Burma, los dueños de los cibercafés tienen que mostrar la lista de contenidos Web censurados y son responsables por el cumplimiento de la ley de censura forzada en sus negocios.
- Un filtraje extra puede ser implementado por los administradores de los cibercafés (control y filtrado del lado del cliente), para complementar el filtrado implementado en el ISP o a nivel nacional.
- Los usuarios pueden ser forzados por las restricciones del entorno a evitar la visita de sitios Web específicos por miedo al castigo, reforzando así la autocensura.
- Las computadoras muchas veces son configuradas para que los usuarios no puedan instalar ningún programa, incluyendo las herramientas de evasión, o para que no puedan conectar ningún tipo de dispositivo al puerto USB (como memorias externas por USB). En Cuba, las autoridades han comenzado a desarrollar un programa de control para los cibercafés llamado AvilaLink que no permite a los usuarios instalar o ejecutar herramientas específicas desde una memoria externa USB.
- Los usuarios pueden ser obligados a usar solo el navegador Internet Explorer, para evitar el uso de privacidad o de complementos de evasión para navegadores como en Mozilla Firefox o Google Chrome.

Mejores prácticas para seguridad y evasión

Dependiendo del entorno en el cual compartimos una computadora, podemos intentar hacer lo siguiente:

- Identificar los medios de vigilancia implementados basados en la lista anterior (CCTV, vigilancia humana, keyloggers, etc) y comportarse consecuentemente.

- Ejecutar programas de evasión desde memorias externas USB.
- Usar un sistema operativo en el que tengamos control a través del uso de un LiveCD.
- Cambiar de cibercafé a menudo cuando tememos a la vigilancia recurrente, o visitar el que sepamos que es confiable y seguro para conectarnos.
- Usar nuestra propia laptop en los cibercafés en lugar de las computadoras públicas.

CONFIDENCIALIDAD Y HTTPS

Algunas redes filtradas usan principalmente (o exclusivamente) el filtrado de palabras claves, en lugar del filtrado de sitios web particulares. Por ejemplo, alguna red pudiera bloquear toda comunicación que contenga una palabra clave consideradas sensible desde el punto de vista político, religioso o cultural. Este tipo de bloqueo puede ser obvio o puede estar enmascarado tras un error técnico. Por ejemplo, algunas redes pueden hacer que aparezca un error técnico cuando se hace la búsqueda de algo que el operador de red piense que no debemos ver. De esta forma, los usuarios son menos propensos a responsabilizar de este problema a la censura.

Si el contenido de las comunicaciones de Internet no está cifrado, estará expuesto durante todo el trayecto de red del ISP, es decir enrutadores y firewalls, donde puede estar implementado el monitoreo basado en palabras clave. Ocultar el contenido de las comunicaciones cifrándolas hace que la censura sea mucho más difícil, porque el equipamiento de red no puede distinguir la comunicación que contiene las palabras claves prohibidas del resto.

Usar el cifrado de datos para mantener las comunicaciones confidenciales también evitan que el equipamiento de red pueda guardar los datos para analizarlos más tarde y etiquetar de forma individual lo que leemos o escribimos.

¿Qué es HTTPS?

HTTPS es la versión segura del protocolo HTTP usado para acceder a sitios web. Brinda una seguridad avanzada para acceder a los sitios web usando cifrado y así impedir que la comunicación esté expuesta a terceros. Usar HTTPS para acceder a un sitio puede evitar que los operadores de redes sepan que parte del sitio estamos usando o que información enviamos o recibimos desde el sitio. El soporte para HTTPS está incluido en los navegadores Web más populares, así que no necesitamos instalar o adicionar ningún programa para usarlo.

Usualmente, si un sitio está disponible a través de HTTPS, podemos acceder a la versión segura del sitio tecleando su dirección comenzando con **https://** en lugar de **http://**. También podemos decir que estamos usando una versión segura de un sitio si la dirección mostrada en la barra de navegación de nuestro navegador comienza con **https://**.

No todos los sitios Web tienen una versión HTTPS. En realidad, quizás menos del 10% lo tienen –aunque los sitios más populares generalmente si lo soportan. Un sitio Web puede estar solo disponible a través de HTTPS si el operador de dicho sitio así lo dispone. Los expertos en seguridad de Internet han estado aconsejando con regularidad a los operadores de sitios a hacer esto, por lo que el número de sitios con HTTPS ha aumentado gradualmente.

Si tratamos de acceder a un sitio a través de HTTPS y recibimos un error, no siempre quiere decir que la red esté bloqueando el acceso a este sitio. Puede significar que este sitio no está disponible en HTTPS (para nadie). Sin embargo, ciertos tipos de mensajes de error muestran que alguien está bloqueando la conexión, especialmente si sabemos que ese sitio se supone debe estar disponible a través de HTTPS.

Ejemplos de sitios que ofrecen HTTPS

Aquí hay algunos ejemplos de sitios populares que ofrecen HTTPS. En algunos casos, el uso de HTTPS es opcional en estos sitios, y no obligatorio, así que debemos explícitamente seleccionar la versión segura para poder obtener los beneficios de HTTPS.

Nombre de sitio	Versión insegura (HTTP)	Versión segura (HTTPS)
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/

Por ejemplo, si hacemos una búsqueda desde https://encrypted.google.com/ en lugar de hacerlo desde http://www.google.com/, nuestro operador de red no será capaz de ver a partir de que términos se realice la búsqueda, y por tanto no puede bloquear Google de responder búsquedas "inapropiadas". (Sin embargo, el operador de red puede decidir bloquear encrypted.google.com totalmente). Similarmente, si usamos Twitter a través de https://twitter.com/ en lugar de http://twitter.com/, el operador de red no puede ver cuales tweets estamos leyendo, que etiquetas buscamos, cuales posteamos, o a qué cuenta nos registramos. (Sin embargo, el operador de red puede decidir bloquear el acceso a twitter.com usando HTTPS.)

HTTPS y SSL

HTTPS hace uso de un protocolo de seguridad de Internet llamado TLS (Transport Layer Security) o SSL (Secure Sockets Layer). Puede que hayamos escuchado referirse a un sitio como que usa SSL o que es un sitio SSL. En el contexto de un sitio Web, esto significa que el sitio está disponible a través de HTTPS.

Usando HTTPS además de nuestra tecnología de evasión

Incluso las tecnologías de evasión de censura que usan cifrado no son un sustituto de HTTPS, porque el propósito para el que se usa cada cifrado es diferente.

Para muchos tipos de tecnologías de evasión de censura, incluyendo VPN, proxis, y Tor, aún es posible y apropiado usar direcciones HTTPS cuando accedemos a un sitio bloqueado a través de la tecnología de evasión. Esto proporciona una gran privacidad y evita que el proveedor de tecnología de evasión guarde u observe lo que hacemos. Esto es importante incluso si confiamos en el proveedor de tecnología de evasión, (o la red que brinda dicha posibilidad) porque este puede ser forzado a dar información nuestra.

Algunos desarrolladores de tecnología de evasión como Tor aconsejan usar siempre HTTPS, para asegurarnos que los proveedores de evasión no puedan espiarnos. Podemos leer más de este tema en https://blog.torproject.org/blog/plaintext-over-tor-still-plaintext. Es bueno tener el hábito de usar HTTPS siempre que sea posible, aún cuando usemos algún otro método de evasión de censura.

Consejos para usar HTTPS

Si nos gusta marcar los sitios que accedemos frecuentemente de manera que no tengamos que teclear la dirección del sitio complete, es bueno marcar la versión segura de cada sitio en lugar de la insegura.

En Firefox, podemos instalar la extensión HTTPS Everywhere para llevar a cualquier sitio que visitemos a HTTPS automáticamente. Esto está disponible en https://www.eff.org/https-everywhere/.

Riesgos de no usar HTTPS

Cuando no usamos HTTPS, un operador de red como nuestro ISP o un operador de firewall nacional puede registrar todo lo que hacemos – incluyendo el contenido específico de las páginas que accedemos. Ellos pueden usar esta información para bloquear páginas particulares para crear registros que puedan ser usados en nuestra contra. Pueden también modificar el contenido de ciertas páginas o adicionar programas maliciosos para espiarnos o infectar nuestras computadoras. En muchos casos, otros usuarios de la misma red pueden también hacer esto aunque no sean los operadores oficiales.

En 2010, algunos de estos problemas fueron dramatizados por un programa llamado Firesheep, que hacía extremadamente fácil para los usuarios de una red tomar las cuentas de sitios de red social de otros usuarios. Firesheep funcionó porque, en el momento de ser creado, estas redes sociales no usaban HTTPS comúnmente, o lo usaban de forma limitada para proteger solo partes de sus sitios. Esta demostración llamó mucho la atención de los medios y provocó que varios sitios hicieran del HTTPS un requisito o al menos lo ofrecieran como una opción.También permitió que usuarios con pocas habilidades abusaran de otros usuarios tomando sus cuentas.

En Enero de 2011, durante un periodo de conflicto político en Túnez, el gobierno Tunecino comenzó a supervisar las conexiones de usuarios a Facebook de manera que el gobierno podía robar las contraseñas de usuarios. Esto se hizo modificando la página de registrarse a Facebook y adicionando un programa invisible que enviaba una copia de las contraseñas a las autoridades. Estas modificaciones son muy fáciles técnicamente y pueden ser hechas por cualquier operador en cualquier momento. Hasta donde se conoce, los usuarios tunecinos de Facebook que usaban HTTPS se mantuvieron a salvo de este ataque.

Riesgos de usar HTTPS

Cuando está disponible, usar HTTPS es siempre más seguro que usar HTTP. Incluso si algo va mal, no será fácil espiar nuestras comunicaciones. Por tanto es inteligente usar HTTPS siempre que podamos (pero debemos tener cuidado, en principio, usar cifrado puede estar regulado por ley en algunos países). Sin embargo, hay algunas formas en que HTTPS no brinda una protección completa.

Advertencias de seguridad de certificados

Algunas veces, cuando intentamos acceder a un sitio web sobre HTTPS, nuestro navegador web nos nuestra un mensaje de aviso describiendo un problema con el **certificado digital** del sitio. El certificado se usa para asegurar la seguridad de la conexión. Estos mensajes de avisos existen para protegernos contra los ataques, no debemos ignorarlos. Si ignoramos o sobrepasamos el aviso de certificado, podemos aún ser capaces de usar el sitio pero limitamos las ventajas de la tecnología HTTPS para salvaguardar nuestras comunicaciones. En ese caso, nuestro acceso al sitio puede no ser más seguro que hacerlo por HTTP.

Si encontramos un aviso de seguridad de certificado, debemos reportarlo por correo electrónico al administrador de la Web del sitio que estamos tratando de acceder, para animar al sitio a reparar el problema.

Si estamos usando un sitio HTTPS individual, como algunos tipos de proxis Web, podemos recibir un error de certificado porque el certificado es **auto-firmado**, lo que significa que no hay bases para que nuestro navegador determine si la comunicación está siendo interceptada. Para estos sitios, podemos no tener otra alternativa que aceptar el certificado **auto-firmado**. Sin embargo, podemos intentar confirmarlo por otra vía, como por correo electrónico o mensajería instantánea y chequear que es el que esperábamos, o ver si se ve igual usando una conexión de Internet diferente desde una computadora diferente.

Contenido mixto

Una página Web simple usualmente está hecha de muchos y diferentes elementos, que pueden venir de diferentes lugares y ser transferidos separadamente desde otro. Algunas veces un sitio usará HTTPS para algunos elementos de una página Web pero para otros usará HTTP inseguro. Por ejemplo, un sitio puede permitir solo http para acceder ciertas imágenes. Por ejemplo, en Febrero de 2011, el sitio seguro de Wikipedia presentaba este problema; aunque el texto de Wikipedia se podía cargar usando HTTPS, todas las imágenes se cargan usando http, de esta forma algunas imágenes pueden ser identificadas y bloqueadas, o usadas para determinar que páginas de Wikipedia el usuario está leyendo.

Redirección a la versión insegura HTTP de un sitio

Algunos sitios usan HTTPS de forma limitada y obligan a los usuarios a volver al HTTP inseguro incluso después que el usuario inicialmente usara el acceso HTTPS. Por ejemplo, algunos sitios usan HTTPS en las páginas de autenticación, pero en cuanto los usuarios entran su información de cuenta, vuelven a usar HTTP para el resto de las páginas. Este tipo de configuración deja a los usuarios vulnerables a la vigilancia. Debemos tener cuidado con esto, si nos vemos redirigidos a una página insegura mientras usamos un sitio, estaremos sin la protección de HTTPS.

Redes y firewalls bloqueando HTTPS

Por la forma en que HTTPS impide el monitoreo y bloqueo, algunas redes bloquean completamente el acceso por HTTPS de sitios particulares, o incluso bloquean el uso de HTTPS completamente. En este caso, estaremos limitados a usar accesos inseguros a esos sitios mientras estamos en esas redes. Podemos estar inhabilitados de acceder a un sitio porque nos ha sido bloqueado HTTPS. Si usamos HTTPS Eveywhere o algún programa similar, puede que no podamos usar algunos sitios porque este software no permite conexiones inseguras.

Si nuestra red bloquea HTTPS, podemos asumir que el operador de red puede ver y grabar todas nuestras actividades de navegación Web en la red. En este caso, quizás queramos explorar otras técnicas de evasión de censura, particularmente aquellas que brindan otras formas de cifrado, como proxis VPN y SSH.

Usando HTTPS desde una computadora insegura

HTTPS solo protege el contenido de nuestras comunicaciones mientras estas viajan por Internet. No protege nuestro ordenador, o nuestra pantalla o disco duro. Si el ordenador que usamos es compartido o inseguro de alguna otra forma, puede contener programas de monitoreo o espionaje, programas de censura que graban o bloquean palabras claves sensibles. En este caso, la protección que ofrece HTTPS puede ser menos que relevante, pues el monitoreo y la censura pueden suceder en nuestra propia computadora.

Vulnerabilidad del sistema de certificado de HTTPS

Existen problemas con el sistema de autoridad de certificación, llamado también **infraestructura de llave pública** (PKI por sus siglas en inglés) que se usa para autenticar conexiones HTTPS. Esto puede significar que un atacante sofisticado puede engañar nuestro navegador para que no muestre un aviso durante un ataque, si el atacante tiene el tipo de recurso indicado. Esto no es una razón para dejar de usar HTTPS, pues incluso en el peor de los casos, la conexión HTTPS no será más insegura que una conexión HTTP.

TECNICAS BASICAS
7. TRUCOS SIMPLES
8. SEAMOS CREATIVOS
9. PROXIS WEB
10. Psiphon

7. TRUCOS SIMPLES

Hay un número de técnicas para sortear el filtrado en Internet. Si nuestra meta es alcanzar páginas o servicios en Internet que están bloqueados desde nuestra localización, y no queremos que otras personas detecten y monitoreen nuestra evasión, estas técnicas pueden ser lo que necesitamos:

- Usando nombres de dominios alternativos para alcanzar contenido bloqueado.
- Usando sitios de terceros para alcanzar contenido bloqueado.
- Usando puertas de enlace de correo para recuperar páginas web bloqueadas a través del correo.
- Usando HTTPS

HTTPS es una versión segura del protocolo HTTP usado para acceder a sitios Web.

En algunos países, y si el sitio que deseamos ver tiene habilitado HTTPS, solo entrando su dirección (URL) empezando con **https://** en lugar de **http://** puede permitirnos acceder al sitio incluso aunque la URL http:// esté bloqueada.

Por ejemplo, http://twitter.com/ fue bloqueado en Burma, mientras https://twitter.com/ estuvo accesible.

Antes de utilizar otra herramienta de evasión de censura, tratemos de adicionar una 's' después de 'http' en la URL de nuestro sitio, si la URL http:// ha sido bloqueada. Si esto funciona, no solo tendremos acceso al sitio, sino que el tráfico entre nosotros y el sitio estará cifrado.

Para otros detalles en esta técnica, leamos los capítulos “Confidencialidad y HTTPS” y “HTTPS Everywhere”.

USANDO NOMBRES DE DOMINIO ALTERNATIVOS O URLS

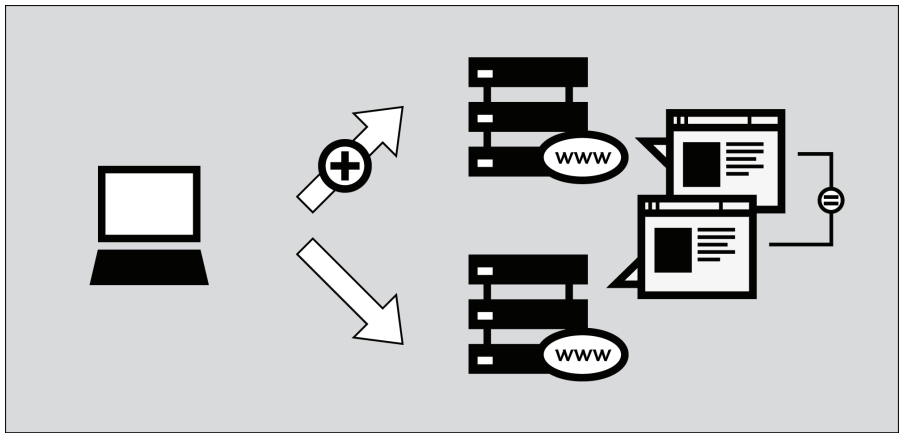
Una de las formas más comunes de censurar un sitio Web es bloquear el acceso al nombre de dominio, por ejemplo, “news.bbc.co.uk”. Sin embargo, casi siempre los sitios son accesibles en otros nombres de dominios, como “newsrss.bbc.co.uk”. Si un nombre de dominio está bloqueado, tratemos de ver si el contenido está disponible en otro dominio.

Podemos intentar acceder algunas versiones que crean algunos sitios para **smartphones**. Estos generalmente tienen la misma URL adicionando una “m” o “mobile” al comienzo, por ejemplo:

- 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

USANDO SITIOS DE TERCEROS

Existen diferentes maneras de acceder el contenido de una página sin hacerlo directamente sino a través del sitio de un tercero.



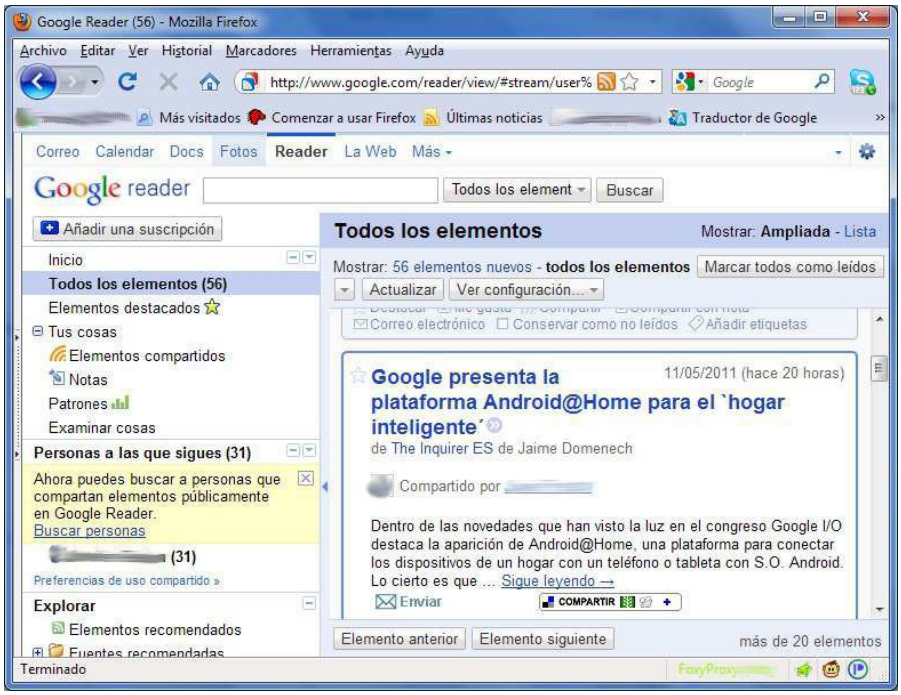
Páginas en Caché

Muchos motores de búsqueda mantienen copias de páginas Web que han indexado previamente, llamadas "en caché". Cuando investigamos por un sitio Web, buscamos un enlace pequeño etiquetado "en caché" próximo a los resultados de búsqueda. Como estamos recuperando una copia de la página bloqueada desde el servidor del motor de búsqueda, y no del sitio Web bloqueado en sí mismo, podemos ser capaces de ver el contenido bloqueado.
Sin embargo, algunos países han bloqueado algunos servicios de caché también.

Agregadores RSS

Los **Agregadores RSS** son sitios Web que nos permiten suscribirnos y leer **suplementos RSS**, que son flujos de noticias u otra información publicados por los sitios que hayamos seleccionado. (RSS: Really Simple Syndication, para más informaión sobre cómo usarlo, veamos http://rssexplained.blogspot.com/.) Un agregador RSS se conecta a sitios Web, descarga los suplementos que seleccionó, y los muestra. Como el RSS es el que se conecta al sitio y no nosotros, podemos acceder sitios bloqueados. Esta técnica solo funciona para sitios que publican suplementos RSS de su contenido, por supuesto, y en consecuencia es más útil para blogs y sitios de noticias. Existen una gran cantidad de agregadores RSS gratis en línea y disponibles. Algunos de los más populares incluyen Google Reader (http://reader.google.com) y Bloglines (http://www.bloglines.com).

Debajo hay un ejemplo de Google Reader mostrando las noticias:



Traductores

Hay muchos servicios de traducción disponibles en Internet, casi siempre proporcionados por motores de búsqueda. Si accedemos a través de un servicio de traducción, el servicio de traducción es el que está accediendo y no nosotros. Esto permite leer el contenido bloqueado traducido en diferentes lenguajes.

Podemos usar el servicio de traducción para evadir el bloqueo, incluso aunque no necesitemos traducir el texto. Esto se hace seleccionando traducción desde un lenguaje que no aparezca en el sitio Web original al lenguaje original. Por ejemplo, para usar el servicio de traducción para ver un sitio Web en inglés, seleccione traducción de Chino a Inglés. El servicio de traducción traduce solo la sección China (no hay ninguna), y deja la sección en Inglés (que es la página web completa) sin traducir.

Algunos servicios de traducción populares son: http://babelfish.yahoo.com y http://translate.google.com.

El ejemplo de abajo ilustra los tres pasos necesarios para ver la página en Babelfish. Primero, entre la URL del sitio que desea visitar:

A continuación, seleccionamos el lenguaje en el que deseamos leer el sitio. En este ejemplo, le decimos a Babelfish que traduzca desde el Coreano al Inglés. Como no hay texto en Coreano, la página se mantendrá sin traducir.

<span id="><span id="> border-style: solid;" alt="babelfish2" src="static/CircumventionTools-SimpleTricks-babelfish2-en.png" height="252" width="406">

Cuando hayamos seleccionado el lenguaje, clic “Traducir” y la página se muestra.

Por supuesto esto requiere que el traductor sea accesible, lo que no siempre es el caso porque algunas autoridades conocen el uso potencial que se le puede dar a un traductor para la evasión de censura.

Por ejemplo, http://translate.google.com no está accesible en Arabia Saudita, de acuerdo con http://www.herdict.org.

Filtros de bajo ancho de banda

Los filtros de bajo ancho de banda son servicios web diseñados para hacer la navegación más fácil en lugares donde la velocidad de la conexión es lenta. Estos eliminan o reducen las imágenes, eliminan los mensajes publicitarios, y en ocasiones comprimen el sitio Web para que usen menos datos, y descarguen rápido.

Igual que en el caso de los servicios traducción y agregadores, podemos usar el los filtros de ancho de banda bajo, sortear bloqueos simples accediendo a los contenidos bloqueados desde sus servidores en lugar de hacerlo directamente desde nuestro ordenador. Uno de los filtros de ancho de banda bajos más útil está en http://loband.org/.

Archivo Web

La caché archive.org (the Wayback Engine - http://www.archive.org/web/web.php) permite a los usuarios ver versiones de páginas web archivadas en el pasado. Millones de sitios Web y la información asociada a ellos (imágenes, código fuente, documentos, etc) son salvados en una base de datos gigante.

No todos los sitios Web son salvados, aún, porque muchos dueños de sitios Web no quieren incluir los suyos, también los snapshots usualmente toman un mayor tiempo para ser adicionados.

USANDO SERVICIOS DE CORREO ELECTRÓNICO

Los servicios de correo electrónico y correo Web se pueden usar para compartir documentos con grupos de amigos o colegas, e incluso para navegar en la Web.

Accediendo a páginas web a través del correo electrónico

De manera similar a los filtros de ancho de banda bajos, hay servicios pensados para personas con conexiones lentas o poco fiables que te permiten solicitar una página web vía correo electrónico. El servicio envía un mensaje de respuesta que incluye la página web ya sea en el cuerpo del mensaje o en un adjunto. Estos servicios pueden resultar un poco engorrosos de usar, puesto que requieren enviar una solicitud separada para una o más páginas web, y esperar por la respuesta, pero en ciertas situaciones, pueden ser muy efectivos para alcanzar páginas web bloqueadas, especialmente si los usamos desde un servicio de correo web seguro.

Web2mail

Un servicio similar se puede encontrar en **web2mail.com**. Para usarlo, solo hace falta enviar un correo a www@web2mail.com con la dirección Web (URL) de la página web que se desea consultar. También se pueden hacer búsquedas simples en la línea del asunto. Por ejemplo, podemos buscar por herramientas de evasión de censura escribiendo "search circumvention tools" en el asunto de un mensaje de correo y enviarlo a www@web2mail.com.

EmailTheWeb

Otro servicio similar es EmailTheWeb, http://www.emailtheweb.com, que permite enviar por correo electrónico una página cualquiera a cualquier persona, incluyéndonos a nosotros mismos. Para enviar la página web por correo electrónico necesitamos registrarnos en el sitio o usar nuestra cuenta Gmail. El servicio gratis permite enviar 25 páginas por día.

Podemos encontrar más información y soporte en este tema en la lista ACCMAIL. Para suscribirnos, enviamos un correo electrónico con el texto "SUBSCRIBE ACCMAIL" en el cuerpo del mensaje a la dirección listserv@listserv.aol.com.

RSS al correo electrónico

Algunas plataformas ofrecen servicios web similares, pero enfocándose en los suplementos RSS en lugar de simples páginas web; entre ellos:

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

FoE

(Feed over Email) es otro proyecto interesante del mismo tipo, creado por Sho Sing Ho desde el Broadcasting Board of Governors. En el momento de confección de este manual, FoE está aún en fase de desarrollo. El progreso de FoE se puede seguir aquí: http://code.google.com/p/foe-project.

Sabznameh

Para los interesados en acceder a noticias filtradas en Persa desde el interior de Iran, Sabznameh es una opción que debemos considerar. Sabznameh es una plataforma de noticias robusta y escalable que permite a los consumidores de noticias independientes acceder a contenido bloqueado por la vía del correo electrónico.

La forma más simple de acceder a Sabznameh es enviando un correo electrónico en blanco (con el asunto y cuerpo del mensaje en blanco) a help@sabznameh.com. Recibiremos un correo de respuesta que nos guiará a través de los pasos para registrarnos a una o más publicaciones disponibles.

Usando correo Web para compartir documentos

Si queremos compartir documentos en línea, pero queremos controlar quien puede verlos, podemos mantenerlos en un espacio privado donde sean visibles solo a aquellos con la contraseña correcta. Una forma simple de compartir documentos entre un pequeño grupo de amigos o colegas es usar una cuenta de correo Web con un proveedor en línea, como Gmail (https://mail.google.com), y compartir el usuario y la contraseña con esos que necesitan el acceso a los documentos. Como la mayoría de los proveedores de correo Web son gratis, es muy fácil cambiar de cuenta por intervalos de tiempo, haciendo más difícil para alguien fuera de grupo mantener la trayectoria de lo que hacemos. Una lista de proveedores de correo electrónico gratis se localiza aquí www.emailaddresses.com/email_web.htm.

VENTAJAS Y RIESGOS

Estas técnicas simples son rápidas y fáciles de usar, podemos probarlas con esfuerzos mínimos. Muchas de ellas trabajarán al menos parte del tiempo en muchas situaciones. Sin embargo, son también muy fáciles de detectar y bloquear. Como no cifran ni ocultan la comunicación son vulnerables al bloqueo y monitoreo basado en palabras claves.

8. SEAMOS CREATIVOS

Si nuestro proveedor de servicio de Internet (ISP) censura el acceso a ciertos sitios Web o servicios, podemos usar las herramientas descritas en otros capítulos de este libro, o podemos pensar en formas creativas para acceder a la información bloqueada. Aquí hay algunos ejemplos.

USANDO ISPS ALTERNATIVOS

Algunas veces las regulaciones de filtrado no se aplican uniformemente en todos los ISPs. Los proveedores que tienen un gran número de suscriptores, como las compañías de telecomunicaciones dirigidas por estados pueden estar sujetas a leyes de escrutinio reforzadas. En el 2002 el gobierno alemán promulgó una ley de regulación de Internet que solo era aplicable a solo los ISP de un estado específico. Como resultado los usuarios fueron capaces de evadir estas regulaciones suscribiéndose a un ISP nacional con oficinas en otras regiones del país. Similarmente, una regulación alemana impuesta en 2010 que solo afectaría ISPs con más de 10,000 suscriptores (con el objetivo de prevenir la fuga de listas negras) fue fácilmente evadida suscribiéndose a ISPs locales. Durante la revolución egipcia de 2011, han existido especulaciones sobre Noor DSL que dicen que fue el último en obedecer con el cierre de Internet por su pequeña porción de mercado (8%) y la prominencia de sus clientes, como la bolsa Egipcia, el Banco Nacional de Egipto y Coca-Cola.

ISPs alternativos se pueden encontrar fuera del país, y algunas compañías incluso llegan a no cobrarles a aquellos usuarios que viven en países donde hay conflictos políticos severos. Durante los revuelos de 2011 en Libia y Egipto, varios ciudadanos fueron capaces de publicar la situación política y social en sus respectivos países conectando sus módems a ISPs fuera del país, usando métodos de comunicación alternativos, como satélites, packet radio, y conectividad no filtrada brindada por compañías multinacionales o embajadas.

REDES MÓVILES

Las redes móviles son medios de acceso a información sin censurar cuya popularidad ha ido en ascenso, en parte por las altas tasas en países donde el costo de una computadora o una red privada son prohibitivos. Como muchas líneas no son ISPs, sus redes no están afectadas de la misma forma que el resto. Sin embargo, estas redes son usualmente más fáciles de monitorear y son frecuentemente tema de vigilancia extendida.

Activistas de varios países han usado sus teléfonos, y sus programas gratis y de código abierto como FrontlineSMS (http://www.frontlinesms.com) para hacer campañas de servicios de mensajes pequeños (SMS) y establecer un puente entre la tecnología SMS con los servicios de microblogging, como Twitter. Una computadora ejecutando FrontlineSMS y conectada a Internet puede servir como plataforma para otros que postean información a Internet a través de sus teléfonos celulares.

Las redes móviles pueden ser usadas también con dispositivos alternativos. El libro electrónico Amazon's Kindle 3G, por ejemplo, viene con línea móvil internacional, lo que permite acceso gratis a Wikipedia a través de las redes móviles en más de 100 países.

NO USAR INTERNET

Algunas veces el acceso a Internet está completamente restringido, y los activistas están obligados a usar medios alternativos para acceder y distribuir la información sin censurar. En 1989, antes que Internet estuviera tan extendida; algunos estudiantes de la Universidad de Michigan compraron una máquina de fax para enviar resúmenes diarios a universidades internacionales, entidades gubernamentales, hospitales, y negocios en China y proporcionar así reportes alternativos al gobierno sobre los eventos en Tiananmen Square.

Si nuestro acceso está restringido, podemos considerar la posibilidad de hacer intercambios punto – a – punto a través de medios alternativos. IrDA (Infrared) y Bluetooth están disponibles en la mayoría de los teléfonos modernos móviles y pueden ser usados para transferir datos sobre distancias cortas. Otros proyectos, como "The Pirate Box" (http://wiki.daviddarts.com/PirateBox), usan Wi-FI y programas de código abierto gratis para crear dispositivos móviles de ficheros compartidos. En países con baja difusión de Internet, como Cuba, las memorias externas USB tienen un amplio uso por personas que desean distribuir información sin restricciones. Otras tecnologías que fueron usadas por activistas durante el conflicto de Libia y Egipto en el 2011 incluyen fax, speak2tweet (una plataforma lanzada por Google y Twitter que habilitan a los usuarios a hacer tweets vía voicemail) y SMS.

USAR O BIEN TECNOLOGÍA MUY NUEVA O MUY VIEJA

Algunas veces el filtrado de un censurador y las técnicas de monitoreo son solo aplicadas a protocolos y servicios de Internet estándares, de modo que considerar el uso de tecnología antigua o muy moderna que no haya sido bloqueada o monitoreada puede ser una buena estrategia. Antes de la llegada de la mensajería instantánea (IM) los programas (Windows Live Messenger, AIM, etc.) se desarrollaron usando Internet Relay Chat (IRC), un protocolo que permite mensajería de texto en tiempo real. Aunque es menos popular que sus sucesores, IRC aún existe y es usado ampliamente por una gran comunidad de usuarios de Internet. Un Sistema de Tablón de Anuncios (BBS por las siglas en inglés de Bulletin Board System) consiste en una computadora que ejecuta un programa que permite a los usuarios conectarse, cargar y descargar programas así como otros tipos de datos, leer noticias, e intercambiar mensajes con otros usuarios. Originalmente los usuarios llamarán a un número de teléfono usando sus módems para acceder a estos sistemas, pero a inicios de los 90 algunos sistemas de tablón de anuncios también permitían acceso sobre protocolos interactivos como telnet y más tarde SSH.

En este punto, las tecnologías más recientes disfrutan muchos de los mismos beneficios que las viejas tecnologías, pues estas son usadas por un número limitado de usuarios y por tanto menos propensas a ser censuradas. El nuevo protocolo de Internet IPv6, por ejemplo, actualmente se está usando en algunos ISP de algunos países y usualmente no está filtrado.

USOS ALTERNATIVOS PARA SERVICIOS WEB

Muchos usuarios de Internet cuyas conexiones están censuradas han comenzado a usar los servicios Web de formas diferentes a las que originalmente fueron concebidos. Por ejemplo, los usuarios emplearon las capacidades del chat de algunos juegos de video para discutir asuntos que pudieran ser detectados en salas de chat comunes. Otra técnica es compartir una cuenta de correo electrónico y salvar la conversación en la carpeta de “Drafts” para evitar enviar correos por Internet.

Servicios de restaura online como Dropbox.com y Spideroak.com se han usado por activistas para distribuir y compartir documentos, así como otros tipos de datos.

Servicios que se supone sean para traducción, caché, o formato se han usado como simples proxis para sortear la censura de Internet. Los ejemplos más populares son Google Translator, Google Cache, y Archive.org. Sin embargo, hay muchas aplicaciones creativas, como Browsershots.org (toma screenshots de sitios Web), PDFMyURL.com (crea un PDF de un sitio Web), URL2PNG.com (crea una imagen PNG de una URL), y InstantPaper.com (crea documentos de fácil lectura para lectores e-libros como Nook y Kindle).

CUALQUIER CANAL DE COMUNICACIÓN PUEDE AYUDARNOS A EVADIR LA CENSURA

Si tenemos cualquier tipo de canal de comunicación con un cooperante o con una computadora fuera del radio de censura en el que estamos, podemos convertir esto en un medio de evadir la censura. Como se mencionó anteriormente, las personas usaron los chats de los juegos de video para sobrepasar la censura porque los censuradores generalmente no piensan en monitorear o censurar o bloquear el acceso a juegos de video populares. En los juegos donde se permite a jugadores crear sofisticados objetos in-world, las personas han discutido la idea de crear computadoras in-world, pantallas de TV, u otros dispositivos que los jugadores pueden usar para obtener acceso a recursos bloqueados.

Algunas personas han sugerido la idea de disfrazar la información en los perfiles de sitios de red social. Por ejemplo, una persona puede poner la dirección de un sitio Web que quiere acceder en un formulario dentro del perfil del sitio de red social. Un amigo con acceso sin censurar puede crear una imagen de los contenidos de ese sitio en forma de fichero gráfico y postearlo en un perfil diferente. Este proceso puede ser automatizado por un programa para que ocurra rápidamente y automáticamente, en lugar de requerir del trabajo humano para que funcione.

Con la ayuda de la programación, incluso un canal que simplemente permita un flujo de una pequeña cantidad de información numérica o textual puede convertirse en un canal de comunicaciones para un proxy Web. (Cuando un canal oculta la existencia de algún tipo de comunicación completamente, se le llama **canal encubierto**.) Por ejemplo, algunos programadores han creado aplicaciones proxy IP-sobre-DNS o HTTP-sobre-DNS para evadir los firewalls usando el DNS.
Un ejemplo es el programa iodine en http://code.kryo.se/iodine. Podemos encontrar documentación similar para un programa similar en http://en.cship.org/wiki/DNS_tunnel y en http://www.dnstunnel.de. Con estas aplicaciones, una solicitud para acceder a algo es disfrazada como una solicitud de búsqueda de direcciones de sitios que no están relacionados. El contenido de la información es disfrazado como el contenido de las respuestas de estas solicitudes. Muchos firewalls no son configurados para bloquear este tipo de comunicación, porque el sistema DNS nunca fue creado con el propósito de transportar información de peso.

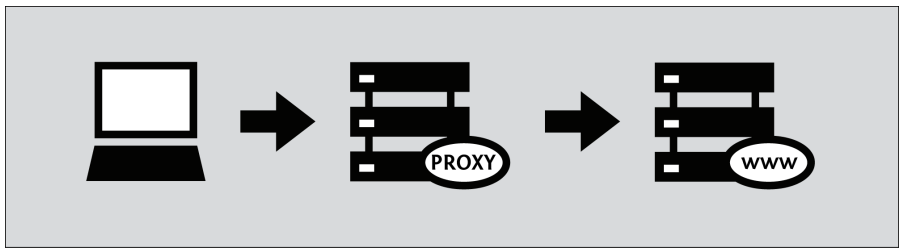
Existe potencial para que aplicaciones inteligentes usen canales secretos para evadir la censura, y está es un área de investigación y discusión constante. No obstante, para que éstas técnicas sean útiles, siempre se requiere de un servidor dedicado a estos propósitos en algún lugar, y el programa en ambos finales debe ser configurado por usuarios sofisticados técnicamente.

9. PROXIS WEB

Un proxy Web permite recuperar un sitio Web incluso cuando el acceso directo a ese sitio está bloqueado en nuestra locación. Existen muchos tipos diferentes de proxis, incluyendo:

- Proxis Web, que solo requieren que sepamos la dirección del sitio de proxy Web. Una URL de un proxy Web puede ser como esta http://www.example.com/cgi-bin/nph-proxy.cgi.
- Los proxis HTTP, requieren que configuremos nuestro navegador. Los proxis HTTP solo funcionan para contenido Web. Podemos obtener la información acerca de un proxy HTTP en el formato "proxy.example.com:3128" or "192.168.0.1:8080".
- Los proxis SOCKS, también requieren que cambiemos la configuración de nuestros navegadores. Los proxis SOCKS trabajan para diferentes aplicaciones de Internet, incluyendo correo electrónico y herramientas para mensajería instantánea.

Un proxy Web es como un navegador embebido dentro de una página Web, y típicamente poseen un formulario pequeño donde podemos entrar la URL del sitio Web que queremos acceder. El proxy entonces nos muestra la página, sin tener que conectarnos a ella directamente.

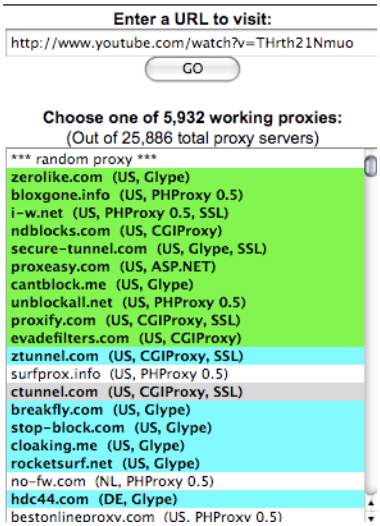


Cuando usamos un proxy Web, no necesitamos instalar ningún programa o cambiar alguna configuración en la computadora, lo que significa que podemos usar un proxy Web desde cualquier computadora, incluyendo las de los cibercafés. Simplemente entramos la URL del proxy Web en nuestro navegador, entramos la URL destino que queremos visitar y presionamos Enter o hacemos clic en el botón Submit.

Una vez que veamos una página a través del proxy Web, debemos ser capaces de usar los botones Atrás y Adelante del navegador, hacer clic en los enlaces y en los formularios sin perder la conexión con el proxy al sitio filtrado. Esto es porque nuestro proxy ha reescrito todos los enlaces en esa página para que estas le digan a nuestro navegador que solicite los recursos a través del proxy. Dada la complejidad de los sitios Web actuales, por otra parte, esto puede ser una tarea difícil. Como resultado, podemos encontrar que algunas páginas, enlaces o formularios pierden la conexión al proxy. Típicamente, cuando esto sucede, la URL del proxy Web desaparecerá de la ventana del navegador.

¿CÓMO PUEDO ENCONTRAR UN PROXY WEB?

Podemos encontrar una lista de proxis Web en sitios como: http://www.proxy.org/, uniéndonos a la lista de discusión en http://www.peacefire.org/circumventor/, o solo haciendo una búsqueda con las palabras claves “free Web proxy” desde cualquier motor de búsqueda. Proxy.org lista miles de proxis Web gratis.



Ejemplos de proxys Web gratis incluyen CGIProxy, PHProxy y Zelune, Glype, Psiphon, y Picidae. Como se mencionó anteriormente, estas no son herramientas para instalar en la computadora. Son programas de servidor que alguien debe instalar en una computadora que está conectada a Internet y que no está sujeta al filtrado. Todas estas plataformas poseen la misma funcionalidad básicamente, pero lucen diferentes y pueden tener diferentes fortalezas y debilidades. Algunas son mejores en ciertas cosas, como reproducción de videos o sitios web complejos.

Algunos proxis Web son privados. Estos usualmente son accesibles solo por un pequeño grupo de usuarios conocido por la persona que ejecuta el proxy o por los clientes que pagan por el servicio. Los proxis web privados tienen ciertas ventajas. Específicamente, ellos pueden ser:

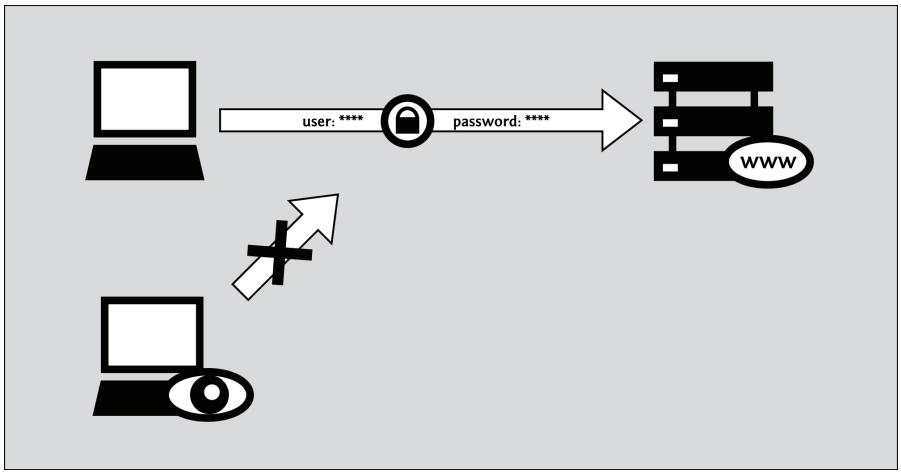
- Más propensos a mantenerse ocultos y por ello accesibles.
- Menos congestionados y por tanto más rápidos.
- Más confiables, asumiendo que están cifrados (ver debajo) y ejecutados por alguien que conozcamos.

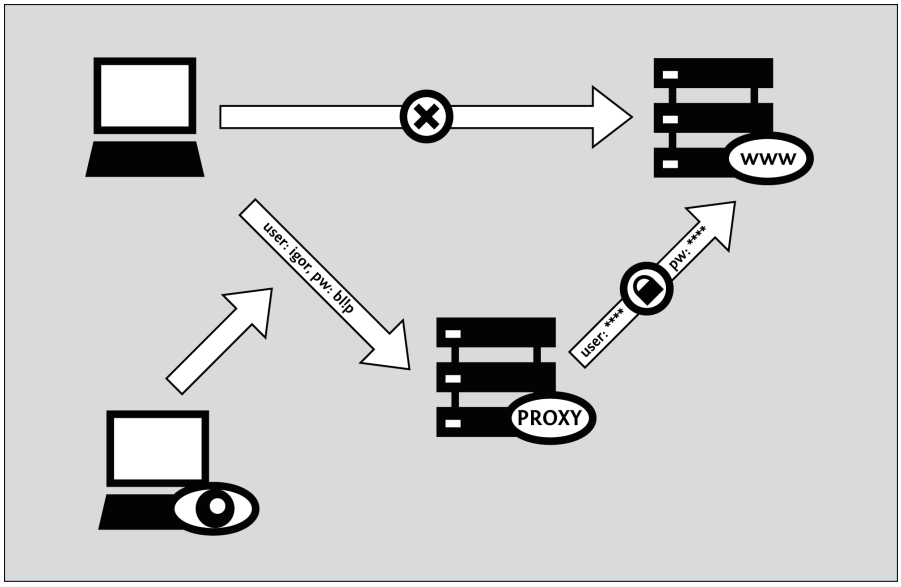
El acceso pudiera ser restringido si se les pide a los usuarios registrarse con un nombre de usuario y una contraseña o simplemente evitando que la URL de proxy aparezca en directorios públicos como esos que se describen arriba.

Los proxis Web son fáciles de usar, pero tienen mayores desventajas que otras herramientas de evasión. Como resultado, las personas a menudo lo usan de forma temporal para obtener y aprender más herramientas avanzadas, que muchas veces deben ser descargadas desde sitios Web que son filtrados. Similarmente, el proxy Web puede ser útil cuando intentamos arreglar o reemplazar otra herramienta que ha dejado de funcionar.

CUESTIONES DE COMPATIBILIDAD CON LOS PROXIS WEB

Los proxis Web solo funcionan para tráfico Web, por lo que no se pueden usar para otros servicios de Internet como correo electrónico o mensajería instantánea. Muchos también son incompatibles con sitios Web complejos como Facebook, reproducción de multimedia en sitios como YouTube, y sitios encriptados que son accedidos a través de HTTPS. Esta última restricción significa que muchos proxis Web no podrán ayudarnos a alcanzar los sitios filtrados que requieran entrar un nombre de usuario, como los servicios de correo electrónico sobre Web. Peor aún, algunos proxis Web no pueden ellos mismos ser accedidos a través de HTTPS. Así que si usamos un proxy como el caso anterior para registrarnos en un sitio que normalmente es seguro, podemos estar poniendo información nuestra, incluyendo contraseñas en riesgo.





Las cuestiones de seguridad como estas se discutirán en detalle más adelante.

Con la notable omisión de HTTPS descrito anteriormente, la mayoría de las cuestiones de compatibilidad de los proxis Web pueden ser resueltas usando el "móvil" o la versión "HTML básico" del sitio Web destino, si existiese alguna. Desgraciadamente, unos pocos sitios ofrecen este tipo de interfaz simplificada, e incluso menos hacen eso de forma que expongan todas las funcionalidades del sitio. Si un sitio Web proporciona una versión móvil, su URL frecuentemente comienza con una "m" en lugar de "www". Algunos ejemplos incluyen: https://m.facebook.com, http://m.gmail.com, y https://m.youtube.com. Nosotros podemos encontrar algunas veces algún link para la versión móvil o HTML básico de un sitio Web entre los enlaces pequeños de la página principal del sitio.

RIESGOS DE SEGURIDAD CON PROXIS WEB

Debemos tener cuidado con algunos riesgos asociados con el uso de proxis Web, particularmente aquellos que son operados por individuos u organizaciones que no conocemos. Si usamos un proxy Web simplemente para leer un sitio Web público como www.bbc.co.uk, nuestras únicas preocupaciones son:

- Alguien puede saber que estamos viendo fuentes de noticias censuradas
- Alguien puede saber cual proxy usamos para esto

Es más, si nuestro proxy web funciona correctamente, y accedemos a través de HTTPS, la información previa solo estará disponible al administrador del proxy. Sin embargo, si descansamos en una conexión HTTP insegura o si nuestro proxy funciona mal (o está mal diseñado) esta información se revelará a cualquiera que pueda estar monitoreando nuestra

conexión a Internet. De hecho, los proxis Web sin cifrado no funcionan en algunos países, porque no pueden evadir los filtros de palabras claves.

Para algunos usuarios, los riesgos anteriores no son una preocupación. Sin embargo, las cosas pueden tornarse más serias si intentamos usar un proxy Web para acceder ciertos tipos de recursos en línea, como:

- Sitios que requieren registrarse con una contraseña
- Sitios a través de los cuales intentamos acceder información sensible
- Sitios a través de los cuales intentamos crear o compartir contenido
- Comercios en línea o sitios Web de bancos
- Sitios que soportan HTTPS ellos mismos

En estos casos, debemos evitar usar proxis Web inseguros. De hecho, debemos evitar totalmente el uso de proxis Web. Mientras no haya garantía de que una herramienta más avanzada sea más segura, el desafío que deben enfrentar los programas de evasión para mantener nuestro tráfico privado es generalmente menos complejo que los proxis Web.

Ofuscación no es encripción

Algunos proxis Web, principalmente aquellos que requieren de soporte para HTTPS, usan simplemente esquemas de codificación para evadir sistemas de nombres de dominio y filtrados de palabras clave pobremente configurados. Uno de esos esquemas llamados ROT-13, sustituye cada carácter con aquel que se encuentra 13 lugares después en el alfabeto latino estándar. (Ver http://www.rot13.com). Usando ROT-13, la URL http://www.bbc.co.uk se convierte en uggc://jjj.oop.pb.hx, que sería irreconocible para los filtros de palabras claves bien simples. Los diseñadores de proxy han encontrado este truco muy útil incluso en países donde el filtrado de palabras clave no está presente, porque los proxis Web muchas veces incluyen la URL marcada dentro de la actual URL que nuestro navegador envía al proxy cada vez que hacemos clic en algún enlace o entramos una nueva dirección. En otras palabras, cuando usamos un proxy, nuestro navegador puede solicitar http://www.proxy.org/get?site=http://www.bbc.co.uk en lugar de solo http://www.bbc.co.uk, de modo que un filtro de nombre de dominio escrito para bloquear esta última dirección también bloqueará el del proxy Web. Si usamos ROT-13 entonces se vería http://www.proxy.org/get?site=uggc://jjj.oop.pb.hx, por lo que burlaríamos el filtro. Desafortunadamente, los esquemas de codificación de caracteres no son muy consistentes. Después de todo, nada puede impedir que un censurador adicione "jjj.oop.pb.hx" a la lista negra junto a www.bbc.co.uk.. (O incluso mejor, puede adicionar "uggc://" a la lista, lo que bloquearía totalmente el uso del proxy web).

Lo más importante que debemos recordar sobre la codificación de caracteres es que no nos protege de ser observados por terceros, quienes pueden aún grabar la lista de los sitios que visitamos. Incluso si se aplica a todo el texto de la página que vemos y al contenido de lo que entramos (en lugar de solo las URL), aún así no brindará confidencialidad. Si estas cosas nos preocupan, debemos restringir nuestro uso solo a aquellos proxis web que soportan HTTPS.

Es importante no olvidar que aún así el administrador del proxy podrá siempre ver todo lo que hacemos.

El consejo anterior enfatiza la importancia de HTTPS, en ambos lugares, en el sitio y en el proxy, cuando usamos un proxy Web para crear u obtener información sensible. Sin embargo, es importante notar que incluso cuando accedemos un sitio seguro a través de un proxy Web, estamos poniendo nuestra confianza en el administrador del proxy Web, y esta persona u organización puede leer todo el tráfico que enviamos o recibimos. Esto incluye cualquier contraseña que pongamos para acceder al sitio destino.

Incluso las herramientas de evasión más avanzadas, que necesitan instalarse, descansan en algún tipo de proxy intermediario para evadir los filtros Web. Sin embargo, todas las herramientas respetables de este tipo son implementadas de manera que protejan el contenido del trafico web HTTPS de manera que ni los propios administradores de los servicios de evasión puedan auditar el tráfico. Desafortunadamente, esto no es posible para los proxis web, los cuales descansan en la confianza que sus usuarios puedan tener. Y la confianza es una función complicada que depende no solo en la motivación del administrador del servicio para proteger nuestros intereses, sino también en sus políticas de mantención de registros, su competencia técnica, y el entorno legal en el que opera.

RIESGOS DE ANONIMATO CON LOS PROXIS WEB

Las herramientas diseñadas para evadir el filtrado no necesariamente brindan anonimato, incluso aquellas que incluyen palabras como “anonymizer” en sus nombres. En general, el anonimato es una propiedad de la seguridad mucho más amplia que la confidencialidad básica (evitar que vean la información que intercambiamos con un sitio Web). Y como se discutió anteriormente, para asegurarnos la confidencialidad básica a través de un proxy web, debemos al menos:

- Usar un proxy Web HTTPS
- Conectarnos a través de ese proxy a un sitio Web con HTTPS
- Confiar en las intenciones del administrador de proxy, sus políticas, programa y competencia técnica
- Prestar atención a cualquier aviso del navegador, como se discutió en el capítulo de HTTPS de este libro

Todas estas condiciones son prerrequisitos para cualquier grado de anonimato. Si un tercero puede leer el contenido de nuestro tráfico, podrá fácilmente asociar nuestra dirección IP con la lista de los sitios Web que hemos visitado. Esto es verdad incluso si, por ejemplo usamos un pseudónimo para registramos en esos sitios o postear mensajes. (Por supuesto, lo contrario es verdad también. Incluso si un proxy es perfectamente seguro no puede proteger nuestra identidad si ponemos nuestro nombre en un post público de un sitio Web).

Anuncios publicitarios, virus y malware

Algunas personas que levantan proxis Web lo hacen para ganar dinero. A veces lo hacen de forma abierta vendiendo anuncios.

Algunos operadores malintencionados pueden tratar de infectar las computadoras de aquellos que usan sus proxis con troyanos o software malicioso en general. Estos bien llamados "drive-by-downloads" pueden secuestrar nuestra computadora para enviar correos SPAM u otros propósitos comerciales que pueden ser incluso ilegales.

Lo más importante que puedes hacer para protegerte contra virus es mantener todos tus programas – incluyendo el sistema operativo – actualizados y usar un antivirus con la última actualización del momento. Además puedes bloquear los anuncios usando la Extensión AdBlockPlus para el navegador Firefox (http://www.adblockplus.org/). Más información sobre cómo evitar estos riesgos se puede encontrar en el sitio Web StopBadware (http://www.stopbadware.org/).

Cookies y scripts

Existen riesgos para el anonimato relacionados con el uso de las **cookies** y los **scripts**. Muchos proxis Web pueden configurarse para eliminar cookies y scripts, pero muchos sitios (por ejemplo, sitios sociales como el Facebook y sitios de media streaming como YouTube) requieren que estos funcionen correctamente. Los sitios Web y anunciantes publicitarios pueden usar estos mecanismos para rastrearnos, incluso cuando usamos proxis, y para producir evidencia, por ejemplo, de que una persona que hizo una cosa abiertamente es la misma persona que hizo otra cosa de forma anónima. Algunas cookies pueden ser salvadas incluso después de reiniciar la computadora, así que sería buena idea solo selectivamente permitir el uso de cookies. En Firefox 3, por ejemplo, puedes instruir al navegador para aceptar cookies solo “Hasta que se cierre Firefox”. (De manera similar, podemos instruir al navegador para eliminar el historial de navegación cuando se cierre).
Generalmente, sin embargo, los proxis Web son extremadamente limitados en su habilidad de proteger nuestra identidad de los sitios Web que accedemos a través de ellos. Si esta es nuestra meta, debemos tener cuidado en como configuramos nuestro navegador y configuración de proxy, y quizás deseemos usar una herramienta de evasión más avanzada.

Ayudando a otros

Si estamos en un país sin restricciones de acceso a Internet y deseamos ayudar a otras personas a evadir su censura, podemos instalar un script de proxy web en nuestro sitio web (o incluso en nuestra computadora en casa), como se describe en la sección Ayudando a otros de este libro.

10. PSIPHON

Psiphon es una plataforma de proxy Web de código abierto que ha cambiado bastante en los últimos años. Se diferencia de otros programas de proxy (como CGIProxy y Glype) en varias cosas, dependiendo en la forma en la que están configurados en el servidor. En general, Psiphon:

- Está accesible a través de HTTPS
- Soporta acceso a sitios destino con HTTPS
- Ofrece mejor (aunque lejos de la perfección) compatibilidad con sitios web complejos, incluyendo YouTube
- Puede requerir que entremos con un usuario y contraseña.
- Nos permite registrar una cuenta de correo electrónico para recibir nuevas URLs de proxy en caso de que el nuestro sea bloqueado
- Nos permite invitar a otros a usar nuestro proxy (asumiendo que está configurado para requerir de una contraseña).

La versión actual de servidor de Psiphon corre solo sobre Linux, y es mucho más difícil de instalar y administrar que el resto de los proxis. Está diseñado primeramente para facilitar la operación a gran escala, servicios de evasión de bloqueo resistentes para aquellos que tienen la habilidad de instalar y usar herramientas más avanzadas.

LA HISTORIA DE PSIPHON

Psiphon 1, la versión original de la plataforma de proxy Web, fue diseñada para correr en Windows, y permitía a un usuario no experto que no tenía filtrado Internet brindar servicios de evasión básicos a individuos específicos de países bajo censura. Era fácil de instalar, fácil de usar y brindaba soporte parcial para HTTPS, lo que lo hacía más seguro que muchas alternativas. Requería que los usuarios se registraran, lo que ayudaba a prevenir la congestión y reducir la posibilidad de que esos proxis Web pequeños, llamados nodos, fueran objeto de bloqueo. Psiphon 1 desafortunadamente ha sido descontinuado.

Psiphon 2 fue reescrito completamente, enfocándose en la presentación, seguridad, compatibilidad y escalabilidad en el contexto de un modelo de servicio centralizado. Estos objetivos se alcanzaron con varios grados de éxito. Inicialmente, un usuario de Psiphon 2 requería registrarse en un nodo privado particular con un nombre de usuario y contraseña. Psiphon Inc. Les dio a unos pocos usuarios de cada región privilegios adicionales que les permitían invitar a otros a acceder a sus proxis. Al principio los proxis Psiphon 2 también requerían que los usuarios ignoraran los avisos del navegador de "certificado inválido" porque mientras ellos eran accesibles a través de HTTPS, sus administradores no eran capaces o no deseaban comprar certificados SSL. Todos los nodos Psiphon privados desplegados por la compañía ahora tienen certificados firmados y no deben lanzar avisos al navegador. Obviamente, esto puede no ser verdad para instalaciones de terceros. Finalmente, todos los usuarios Psiphon ahora tienen derecho de enviar un número limitado de invitaciones.

Los nodos abiertos de Psiphon 2, que son implementados más tarde, pueden usarse sin registrarse a ellos. Un nodo abierto automáticamente carga una página principal, y se presenta en un idioma en particular, pero pueden usarse para navegar a cualquier parte y evadir la censura. Los nodos abiertos incluyen un enlace a través del cual un usuario puede crear una cuenta y, opcionalmente, registrar una cuenta de correo electrónico. Esto permite que los administradores de proxy envíen nuevas URLs a los usuarios cuyos nodos están bloqueados desde sus países. En general, los nodos abiertos se esperan sean bloqueados más rápido que los privados. Como los nuevos nodos privados, los nodos abiertos son seguros usando HTTPS, y aquellos que son operados por Psiphon Inc, se identifican usando certificados válidos.

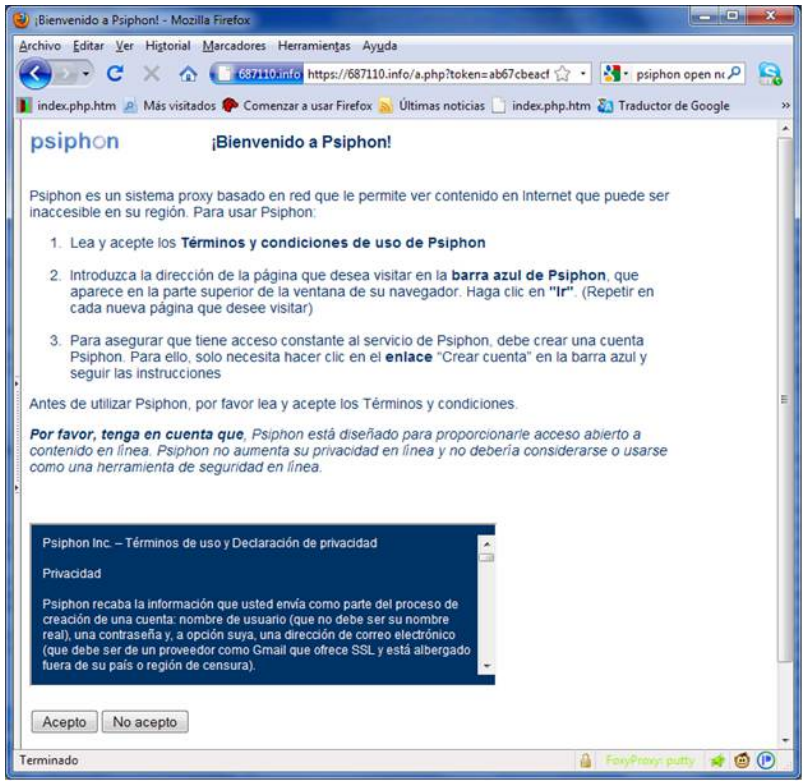
CÓMO PODEMOS OBTENER ACCESO A UN NODO PSIPHON?

Para limitar y monitorear el bloqueo de sus proxis, Psiphon Inc tiene una forma no centralizada de distribuir sus nodos abiertos (a los que a menudo se refieren como nodos right2know). Un nodo abierto en idioma Inglés, dedicado al fórum de soporte de Sesawe, está disponible en http://sesaweenglishforum.net. Otros nodos abiertos están distribuídos de forma privada (a través de listas de correos electrónicos, feeds de twitter, broadcasts de radio, etc.) por los productores de contenido que componen la base de clientes de Psiphon.

Los nodos privados Psiphon funcionan diferentes. Incluso si fuese posible imprimir un enlace de invitación en este libro, no sería recomendable, pues el punto de mantener un nodo privado es limitar su crecimiento y preservar cierta similitud a las redes sociales en cuanto a la confianza entre sus miembros. Después de todo, una simple invitación enviada a un "informante" puede ser suficiente para que la dirección IP del nodo aparezca en la lista negra. Peor aún, si una invitación fuera aceptada, el informante podría recibir y sustituir URL de proxis enviadas por el administrador del sistema. Si recibimos una invitación, esta incluirá un enlace similar al siguiente https://privatenode.info/w.php?p=A9EE04A3, que permite crearnos una cuenta y registrar una dirección de correo electrónico. Para hacer esto, sigamos las instrucciones más abajo en "Crearse una cuenta". Después de crearnos una cuenta, no necesitamos usar más el enlace de la invitación. En su lugar, iremos a través de una URL algo más fácil de recordar como; https://privatenode.info/harpo.

USANDO UN NODO PSIPHON ABIERTO

La primera vez que nos conectamos a un proxy Psiphon abierto, veremos "Psiphon Terminos de Uso y Política Privada." Debemos leer los términos cuidadosamente, pues contiene consejos de seguridad muy importantes así como información acerca de cómo los administradores de los proxis manipulan nuestra información.

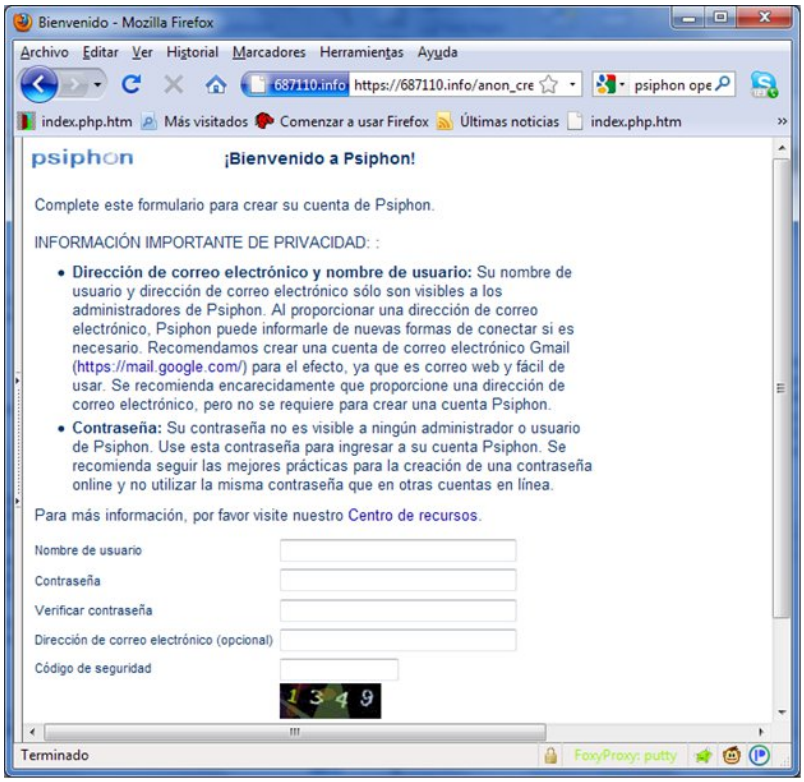


Después de aceptar los Términos de Uso, Psiphon cargará la página principal por defecto asociada con ese nodo, como se muestra a continuación. Podemos seguir los enlaces que se muestran en la página, los que automáticamente solicitan el contenido a través del proxy, o podemos visitar otros sitios Web usando la barra de URL azul (llamada la Bluebar en lenguaje Psiphon) en el tope de la ventana del navegador.

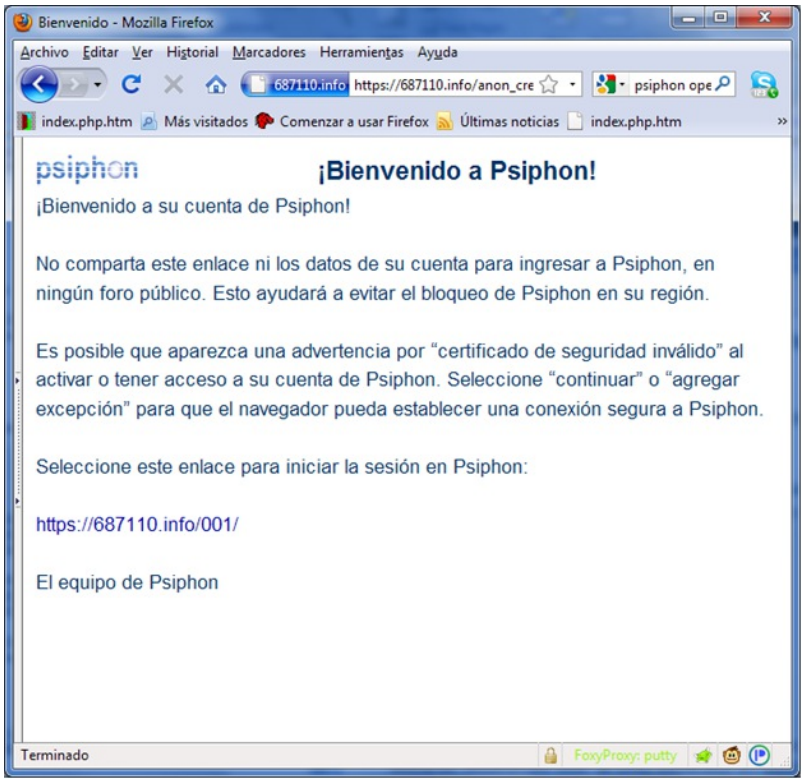
CREANDO UNA CUENTA

Mientras recordemos o marquemos la URL de un nodo abierto desbloqueado, podremos usarlo para acceder a sitios Web filtrados. Crear una cuenta permite modificar algunas preferencias incluyendo el idioma del proxy y la página principal por defecto. Además permite registrar una dirección de correo electrónico para que el administrador del nodo pueda enviar una nueva URL de proxy en caso de que el que se está usando sea bloqueado. Para hacer esto se debe hacer clic en el enlace “Crear cuenta” en la Bluebar.

Si hemos recibido una invitación a un nodo privado de Psiphon, los pasos que se requieren para crearnos una cuenta son los siguientes.

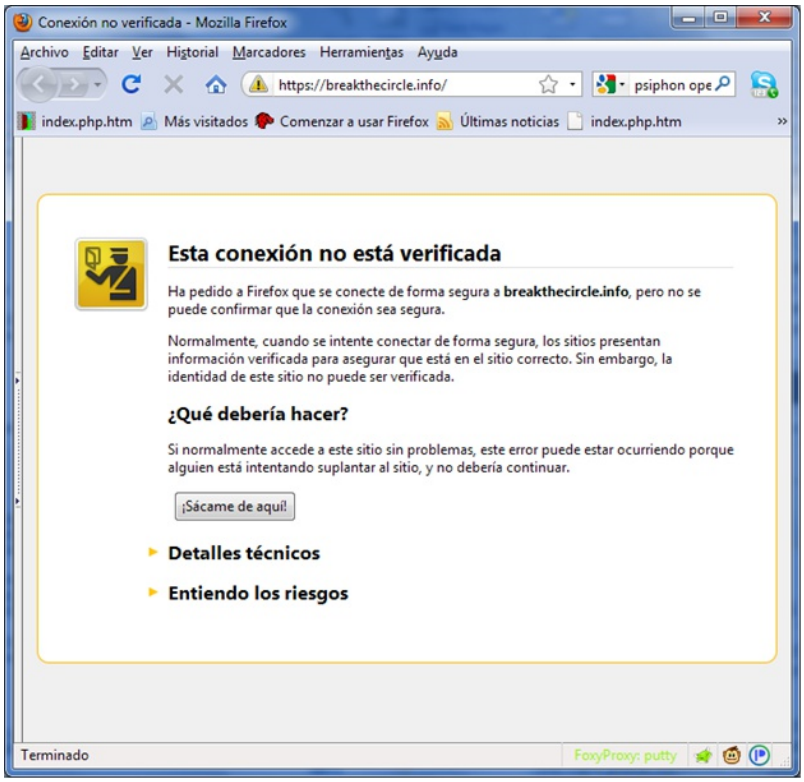


Cuando llenamos el formulario de registro, debemos seleccionar un nombre de usuario que no esté conectado con nuestra identidad real de servicios de correo electrónico, sitios de red social, u otras plataformas como estas. Lo mismo aplica para nuestra dirección de correo electrónico, si seleccionamos registrar alguna. La mayoría del resto de los usuarios no pueden ver nuestro usuario y dirección de correo, pero ambos ítems son almacenados en una base de datos visible a administradores de Psiphon. Si seleccionamos registrar una dirección de correo electrónico, es recomendable que seleccionemos una que nos permita acceder a nuestra cuenta a través de una conexión HTTPS. Algunos de los proveedores que soportan HTTPS incluyen https://mail.google.com, https://www.hushmail.com, y https://mail.riseup.net. Completamos el formulario transcribiendo el número mostrado en la imagen y terminamos hacemos clic en "Crear cuenta".



Debemos ver un mensaje confirmando la creación exitosa de nuestra cuenta. De ahora en adelante deberemos usar la URL mostrada en esta página para registrarnos en nuestro nodo Psiphon. Es de notar que incluye el prefijo HTTPS y un sufijo corto ("/001" en la imagen más arriba). Quizás debamos imprimir la página de bienvenida o marcar la URL de enlace (pero hay que tener cuidado no marcar la página de bienvenida, por accidente). Por supuesto, necesitaremos el usuario y la contraseña que seleccionamos en los pasos anteriores.

Esta página de bienvenida puede brindar también algún consejo, como se muestra arriba, acerca de los avisos "invalid security certificate" y la necesidad de aceptarlos para usar Psiphon. De hecho, estas instrucciones están obsoletas, y no debemos seguirlas. Si cuando nos conectamos a un proxy Psiphon, vimos algún aviso como este que se muestra debajo, debemos prestar atención. Si esto sucede, debemos cerrar el navegador y contactar a info@psiphon.ca o english@sesawe.net para consejos adicionales.



INVITANDO A OTROS

Si usamos una cuenta para registrarnos a nuestro proxy Psiphon, eventualmente ganaremos la habilidad de invitar a otros. Con el propósito de evitar el bloqueo, nos iremos pertrechando de invitaciones hasta alcanzar un límite máximo. Obviamente, si nuestro proxy es un nodo abierto, podemos simplemente enviar la URL del proxy a otros. Sin embargo, después que se produce un evento de bloqueo, si recibimos un mensaje de resumen de "migración" a nuestra dirección de correo de electrónico, podemos significar que nuestra cuenta ha sido movida a un nodo privado. Nunca debemos compartir la URL de un nodo privado, excepto a través del mecanismo de construcción de invitaciones de Psiphon.

Una vez que hayamos coleccionado una o más invitaciones, veremos un enlace en nuestra Bluebar algo como "Invitar (quedan 20)", como se muestra a continuación.

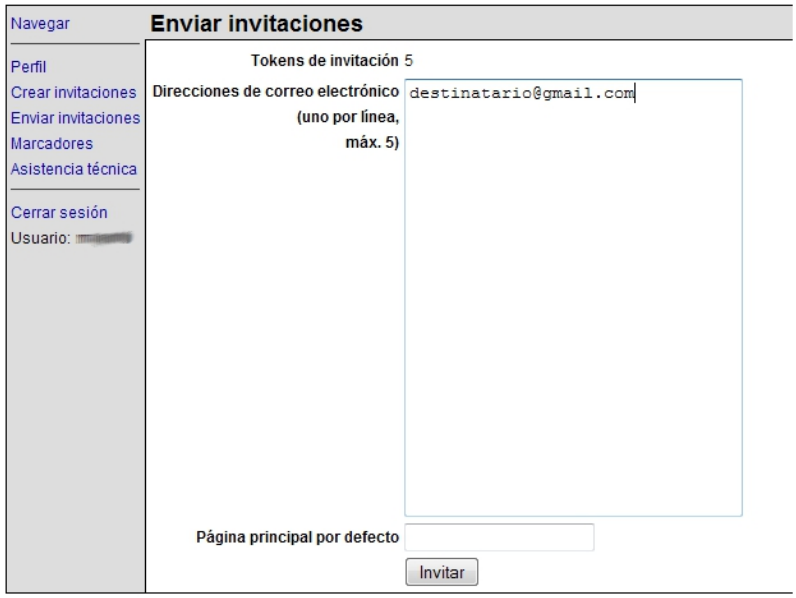
Hay dos formas de invitar a otros a usar nuestro proxy Psiphon:

- El método "Enviar invitaciones" que envía automáticamente enlaces de invitaciones a uno o más destinatarios. Los mensajes de invitación vendrán desde Psiphon, no de nuestra propia cuenta.
- El método de "Crear invitaciones" que genera uno o más enlaces de invitación para nosotros y poder distribuirlos a través de otros canales.

Si hacemos clic en el enlace en la Bluebar, nos llevará a la pantalla Send invitation. Con el propósito de crear un enlace de invitación sin enviarlo por correo electrónico, debemos hacer clic en el enlace Profile primero, y entonces "Crear invitaciones".

Enviar invitaciones

Clic "Invitar" en nuestra Bluebar o Send invitations en la pantalla Profile. Entramos una dirección de correo para cada persona a la que queremos enviar una invitación, una dirección por línea, y entonces clic en "Invitar".



Veremos un mensaje diciendo que hay varios mensajes en cola, lo que significa que Psiphon enviará nuestros enlaces de invitación en los próximos minutos.

Debemos invitar solo a personas que conozcamos.

Crear invitaciones

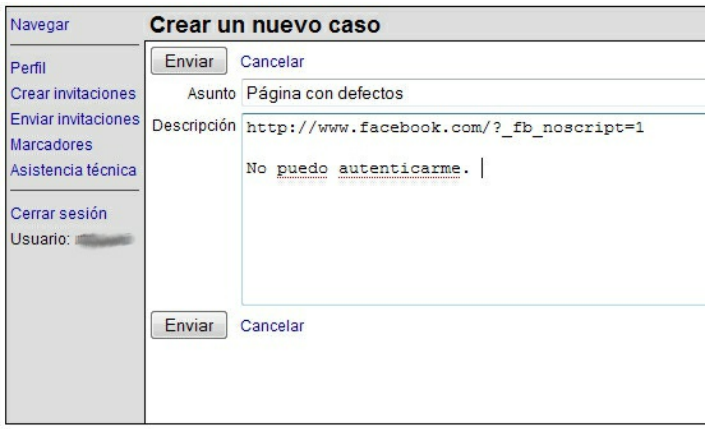
Clic "Crear invitaciones" en la pantalla Profile. Seleccionamos el número de enlaces de invitaciones a crear y hacemos clic en "Invitar".

Podemos distribuir estos enlaces de invitaciones a través de los canales disponibles, pero:

- Cada invitación puede usarse una sola vez
- Para nodos privados, no mostremos los enlaces de publicidad, para evitar exponer las URLs de proxy
- Para nodos privados debemos invitar solo a personas conocidas.

REPORTANDO UN SITIO DAÑADO

Algunos sitios Web que cuentan con scripts embebidos y tecnología compleja como Flash y AJAX puede que no se muestren correctamente a través de Psiphon. Para mejorar la compatibilidad de Psiphon con estos sitios, los desarrolladores necesitan saber qué sitios son problemáticos. Si encontramos un sitio como este, podemos reportarlo fácilmente haciendo clic en el enlace Broken Page en la Bluebar.Si brindamos una breve explicación del problema en el campo Description, permitiremos que el equipo de desarrollo de Psiphon puede reproducir el error y ayudar a encontrar una solución. Cuando terminemos, hacemos clic en “Enviar” y el mensaje será enviado a los desarrolladores.



11. SABZPROXY

SabzProxy ("proxy verde" en Persa) es un proxy web gratis propuesto por el equipo Sabznameh.com. Está basado en el código de legado de PHProxy (al que no se le ha dado mantenimiento desde 2007). Para detalles adicionales acerca del concepto de proxis Web, podemos remitirnos a los capítulos anteriores.

La mejora más significativa en SabzProxy comparada con PHProxy, es la codificación de URL. Esto hace a Sabzproxy más dificil de detectar (Varios países han podido bloquear PHProxy incluido Irán). Solo la inspección a fondo de los paquetes permitiría detectar y bloquear los servidores SabzProxy.

SabzProxy está publicado en persa pero funciona completamente en cualquier idioma. Muchas personas en varios países lo usan para configurar su propio proxy Web público.

INFORMACIÓN GENERAL

Sistemas operativos que soporta	
Localización	Persa
Sitio Web	http://www.sabzproxy.com
Correo electrónico de soporte:	E-mail: sabzproxy@gmail.com

¿CÓMO ACCEDEMOS A SABZPROXY?

SabzProxy es un proxy Web distribuido. Esto significa que no existen ni una instancia central de SabzProxy ni alguna entidad comercial designada a crear y difundirlo. Depende, de su comunidad de usuarios para crear sus propias instancias, y para compartirlas en sus redes. Podemos acceder a estas instancias a través de varios fórums, o redes, y cuando tenemos acceso somos bienvenidos a compartirlo con nuestros amigos.

Una instancia dedicada se ejecuta por el fórum de soporte de Sesawe, y está disponible en http://kahkeshan-e-sabz.info/home (podemos registrarnos con el nombre de usuario flossmanuals y la contraseña flossmanuals).

Si somos dueños de algún espacio Web y estamos interesados en crear y compartir una instancia de SabzProxy con nuestros amigos y familiares, podemos dirigirnos al capítulo Ayudando a otros en la sección Installing SabzProxy de este libro.

¿CÓMO FUNCIONA?

Aquí hay un ejemplo que ilustra cómo funciona SabzProxy.

1. Entramos la dirección de la instancia SabzProxy en nuestro navegador.
2. En la caja de direcciones web de la página SabzProxy, entramos la dirección del sitio censurado que deseamos visitar. Por ejemplo, http://www.bbc.co.uk/persian. Podemos mantener las opciones por defecto.
3. Hacemos clic en Go o Enter.

El sitio Web se muestra en la ventana del navegador.

Podemos ver la barra verde de SabzProxy con la ventana del navegador, y el sitio web BBC Farsi debajo de la barra.

Para continuar navegando, podemos:

- Clic cualquier enlace de la página actual. El proxy Web automáticamente devuelve las páginas enlazadas.
- Entrar una nueva URL en la caja de direcciones en el tope de la página.

OPCIONES AVANZADAS

Para navegar, usualmente las opciones por defecto son suficientes. Sin embargo podemos seleccionar algunas opciones avanzadas:

- **Incluir mini formulario-URL en cada página / فرم آدرس**
  Chequeamos esta opción si deseamos tener un formulario en el sitio Web proxificado para poder entrar nuevas URLs sin tener que ir a la página principal de SabzProxy. O podemos deseleccionar esta opción si tenemos una pantalla pequeña, y necesitamos más especio para ver el sitio seleccionado.

- **Eliminar scripts del lado del cliente (i.e., JavaScript) / حذف اسکریپت ها**
  Chequeamos esta opción si queremos eliminar scripts nuestras páginas Web. Algunas veces JavaScript puede causar cuestiones indeseadas, como cuando es usado para mostrar anuncios publicitarios o incluso para grabar nuestra identidad. Navegar por versiones mobile/light de sitios Web complejos (como servicios de correo Web, o plataformas de red social) es también una alternativa de evitar JavaScript mientras usamos SabzProxy.

- **Permitir almacenar las cookies / قبول کردن کوکی ها**
  Las cookies son pequeños ficheros de texto con un ID de usuario distintivo que son almacenadas en tu navegador automáticamente. Se requieren en algunos sitios que necesitan autenticación pero pueden usarse para rastrear tu identidad. Con esta opción activada cada cookie es almacenada por un tiempo largo. Si queremos permitir las cookies para esta sesión solamente, desmarcamos esta opción y marcamos “Store cookies for this session only” (vea más abajo).

- **Mostrar imágenes en las páginas navegadas / نمایش عکسها**
  Por defecto, nuestro navegador envía a cada sitio Web la URL desde la que venimos, cuando hacemos clic en algún enlace. Estas URLs son almacenadas en los ficheros de logs del sitio Web y son analizados automáticamente. Para mejorar la privacidad, podemos deseleccionar esta opción.

- **Muestra el sitio Web actual referente / نمایش مسیرها**
  Por defecto, nuestro navegador envía a cada sitio Web la URL desde la que venimos, cuando hacemos clic en algún enlace. Estas URLs son almacenadas en los ficheros de logs del sitio Web y son analizados automáticamente. Para mejorar la privacidad, podemos deseleccionar esta opción.

- **Eliminar las etiquetas de meta-información de las páginas / حذف تگ هاي متا**
  Las Meta etiquetas son información adicional almacenada en muchos sitios web para ser usadas automáticamente por programas de computadora. Esta información puede incluir nombre del autor, descripción del contenido del sitio o palabras clave para los motores de búsqueda. Seleccionemos esta opción cuando queremos evitar que sea usada por los filtros de palabras clave para bloquear la navegación.

- **Eliminar título de página / حذف عنوان صفحات**
  Con esta opción activada, SabzProxy elimina el título de la página del sitio Web, el cual normalmente se ve en la barra de titulo del navegador. Esto puede ser útil, por ejemplo, para ocultar el nombre del sitio Web que estamos visitando cuando minimicemos el navegador.

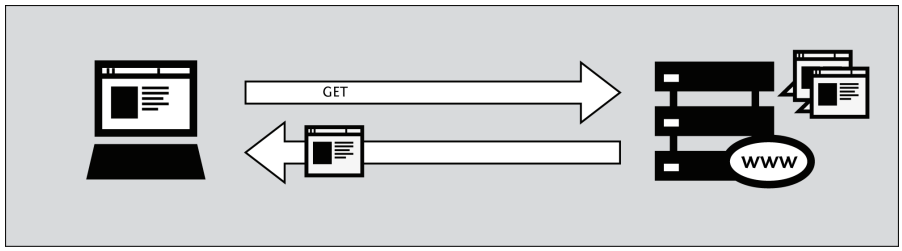
- **Almacenar cookies para esta sesión solamente / کوکي ها موقت**
  Similar a la opción "Allow cookies to be stored". Con esta opción activa, las cookies solo se almacenarán hasta que se cierre la sesión SabzProxy.

FIREFOX Y SUS COMPLEMENTOS
12. Introducción a Firefox
13. Noscript y Adblock
14. HTTPS Everywhere
15. Configuraciones de Proxy y FoxyProxy

12. INTRODUCCIÓN A FIREFOX

Adivinamos que nadie que no sepa que es un navegador Web estaría leyendo este capítulo en primer lugar. De todos modos, por si acaso: un navegador es el programa que se utiliza para visitar y ver sitios Web en Internet.

En capítulos anteriores, se explicó que Internet es una red de computadoras gigante, todas conectadas entre sí. A las computadoras que hospedan sitios web se les llama "servidores web". Si deseamos visitar estos sitios desde nuestra computadora o de un dispositivo móvil, necesitamos una forma de navegar y una forma de mostrarlos. Eso es lo que hace un navegador.



Uno de los navegadores más populares es Firefox, un navegador gratis y de código abierto creado por la fundación Mozilla en el 2003. Firefox corre en la mayoría de los sistemas operativos – Windows, MacOS y Linux - ha sido traducido a más de 75 idiomas. Y lo mejor de todo, es completamente gratuito.

DÓNDE OBTENER FIREFOX

Si deseamos instalar Firefox podemos encontrar los ficheros de instalación aquí:

https://www.mozilla.com/en-US/firefox/

Cuando visitamos este sitio se nos presentará automáticamente el fichero de instalación correcto para nuestro sistema operativo (Windows/Mac/Linux). Para más información en cómo instalar Firefox en cada sistema operativo, leer el manual de Firefox FLOSS Manuals:

http://en.flossmanuals.net/firefox

¿QUÉ ES UN COMPLEMENTO DE FIREFOX?

Cuando instalamos Firefox por primera vez, este puede manejar las tareas de navegación básicas inmediatamente. Pero también podemos adicionarle capacidades extras o cambiar la forma en la que se comporta Firefox instalando complementos, adiciones pequeñas que extienden el poder de Firefox. Hay varios tipos de complementos:

- Extensiones que brindan funcionalidad adicional al navegador
- Temas que cambian la apariencia de Firefox
- Plugins que ayudan a Firefox a manejar cosas que normalmente no puede procesar (por ejemplo, películas Flash, aplicaciones Java).

La variedad de complementos disponibles es enorme. Podemos adicionar diccionarios para diferentes idiomas, ver el clima en otros países, ver sugerencias de sitios Web similares al que estamos viendo y muchos más.

Firefox mantiene una lista de los complementos actuales en su sitio (https://addons.mozilla.org/firefox), o podemos verlos por categoría en https://addons.mozilla.org/firefox/browse.

Antes de instalar cualquier complemento, debemos tener en cuenta que este puede leer mucha información de nuestro navegador, por eso es muy importante seleccionar complementos de fuentes confiables. Si no tenemos cuidado, un complemento instalado puede compartir información acerca de nosotros sin que lo sepamos, pudiera incluso mantener un registro de los sitios que hemos visitado, o incluso hacer daño a nuestras computadoras.

Se recomienda no instalar nunca complementos que no estén disponibles desde el sitio de Firefox. Tampoco debemos instalar nunca Firefox si no lo obtenemos de una fuente confiable.Es importante notar que usar Firefox en la computadora de otra persona o en un cibercafé nos hace aún más vulnerables.

En los próximos tres capítulos, veremos algunos complementos que son particularmente relevantes para la censura de Internet.

13. NOSCRIPT Y ADBLOCK

Aún cuando no existe una herramienta que pueda protegernos completamente contra todas las amenazas a nuestra privacidad y seguridad, las extensiones Firefox descritas en este capítulo pueden reducir significativamente los riesgos, e incrementar nuestras posibilidades de permanecer anónimos.

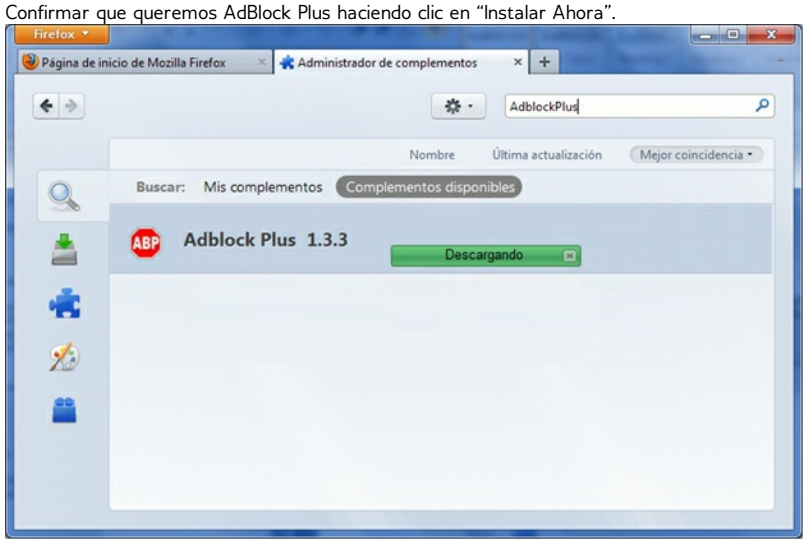
ADBLOCK PLUS

Adblock Plus (http://www.adblockplus.org) busca páginas Web de anuncios y otros contenidos que pueden grabarnos y los bloquea. Para mantenerse actualizados con las últimas amenazas AdBlock Plus tiene una lista negra mantenida por voluntarios.

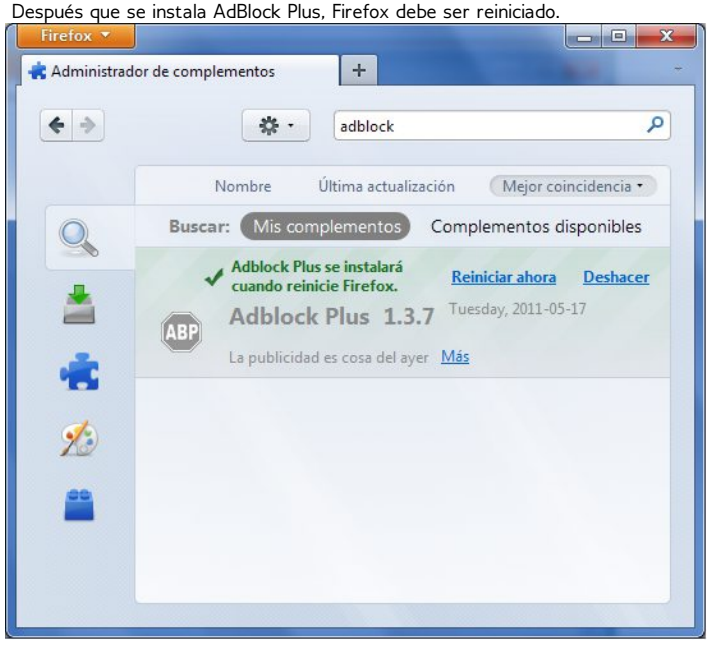
Comenzando con AdBlock Plus

Una vez que tengamos Firefox instalado:

1. Descargamos la última versión de AdBlock Plus desde: http://adblockplus.org/en/installation#release o buscamos el plugin por el administrador de complementos ("Firefox" > "Complementos").
2. Confirmar que queremos AdBlock Plus haciendo clic en “Instalar Ahora”.



3. Después que se instala AdBlock Plus, Firefox debe ser reiniciado.



Seleccionando una suscripción de filtro

Adblock Plus por sí solo no hace nada. Puede ver cada elemento que cada sitio Web intenta cargar, pero no sabe cuál debe ser bloqueado. Esto es lo que hacen los filtros AdBlock. Después de reiniciar Firefox, se nos pedirá seleccionar una suscripción de filtro (gratis).

<span id="> height: 396px;" src="static/ES_13_03.jpg">

¿Qué suscripción de filtro debemos seleccionar? Adblock Plus ofrece unas pocas en su menú desplegable y quizás queramos aprender acerca de la fortaleza de cada una. Un buen filtro para comenzar a a proteger nuestra privacidad es EasyList (también disponible desde http://easylist.adblockplus.org/en).

Aunque pueda verse tentador, no debemos adicionar todas las subscripciones que se nos antojen ya que algunas pueden solaparse, y tener resultados inesperados. EasyList (principalmente enfocado en sitios en idioma Inglés) funciona bien con otras extensiones de EasyList (como listas de regiones específicas como RuAdList o listas temáticas como EasyPrivacy). Pero colisiona con Fanboy's List (otra lista que se enfoca en los sitios en Inglés)

Siempre podemos cambiar nuestras suscripciones de filtros en cualquier momento con sus preferencias (presionando Ctrl+Shift+E). Una vez que hayamos hecho los cambios, hacemos clic en OK.

Creando filtros personalizados

AdBlock Plus también nos permite crear nuestros propios filtros, si queremos. Para adicionar un filtro, empecemos con las preferencias de AdBlock Plus (Ctrl+Shift+E) y hacemos clic en "Add Filter" en la esquina izquierda inferior de la ventana. Los filtros personalizados no reemplazan los beneficios de las listas negras bien mantenidas como EasyList, pero son muy útiles para bloquear contenido específico que no se incluye en las listas públicas.
Por ejemplo, si quisiéramos impedir la interacción de Facebook desde otros sitios Web, podemos adicionar el siguiente filtro:

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

La primera parte (||facebook.*) inicialmente bloqueará todo lo que venga del dominio de facebook. La segunda parte ($domain=~facebook.com|~127.0.0.1) es una excepción que le dice al filtro que permita las solicitudes de facebook solo cuando estemos en facebook o si las solicitudes de Facebook vienen de 127.0.0.1 (nuestra propia computadora) para mantener ciertas características de Facebook funcionando.

Para una guía más rápida sobre cómo crear nuestros propios filtros AdBlock Plus visitese http://adblockplus.org/en/filters.

Habilitando y deshabilitando AdBlock Plus para elementos específicos o sitios Web

Podemos ver los elementos identificados por AdBlock Plus hacienda clic en el icono ABP en  nuestro navegador (usualmente próximo a la página de búsqueda) y seleccionar "Open blockable items", o presionar Ctrl+Shit+V. Una ventana en el medio del navegador nos permitirá habilitar o deshabilitar cada elemento caso por caso. Alternativamente, podemos deshabilitar AdBlock Plus para un dominio específico o página haciendo clic en el icono ABP y seleccionando "Disable on [domain name]" o "Disable on this page only".

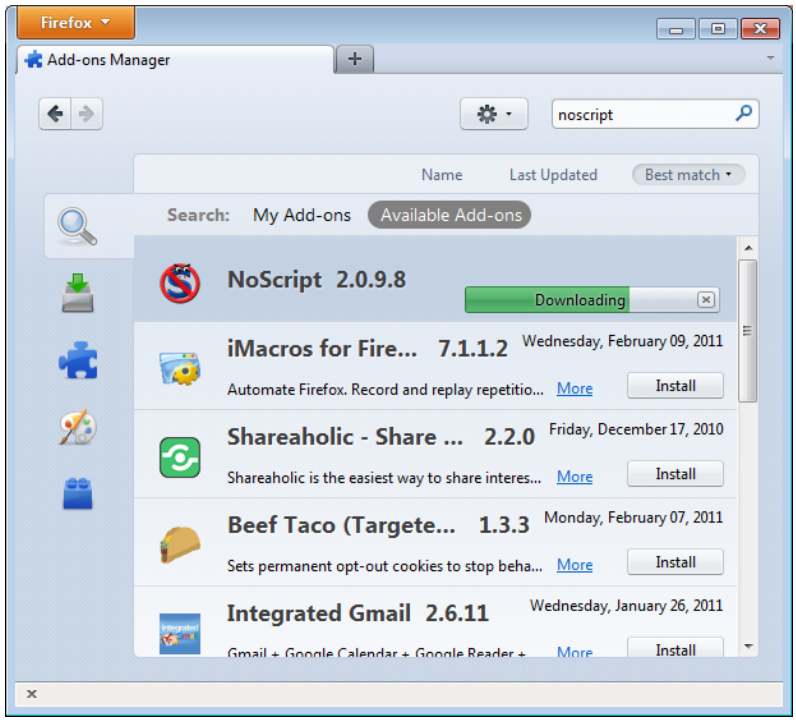
NOSCRIPT

La extension NoScript brinda al navegador protección adicional bloqueando globalmente todo el contenido JavaScript, Java y otros contenidos ejecutables que puedan cargarse de un sitio Web y ejecutarse en nuestra computadora. Para decirle a NoScript que ignore sitios específicos, necesitamos adicionarlos a una lista blanca. Esto puede sonar tedioso, pero NoScript hace un buen trabajo protegiendo a los usuarios de Internet de varias amenazas como cross-site scripting (cuando los atacantes colocan código malicioso de un sitio en otro sitio) y el clickjacking (cuando el hacer click en un objeto inocente en una página puede revelar información sobre nosotros o permitir al atacante a tomar el control de nuestra computadora). Para obtener NoScript, visitemos http://addons.mozilla.org o http://noscript.net/getit.

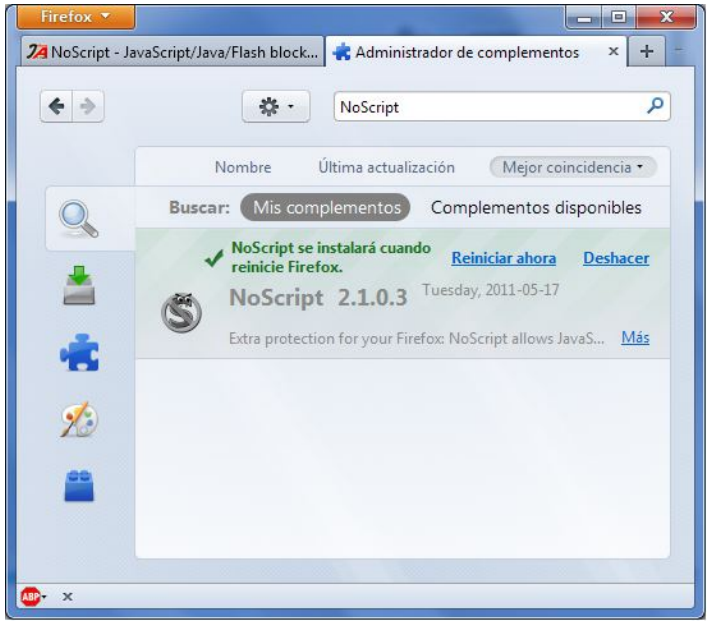
El mismo método por el cual NoScript nos protege puede alterar la apariencia y funcionalidad de las páginas Web, también. Afortunadamente, podemos ajustar cómo NoScript trata a las páginas individualmente o a sitios Web manualmente – depende de nosotros encontrar el justo medio entre la conveniencia y la seguridad.

Comenzando con NoScript

1. Vayamos a la sección de descarga de NoScript en http://noscript.net/getit. Hacemos clic en el botón verde "Instalar".
2. Confirmamos que queremos NoScript haciendo clic en "Instalar ahora".



3. Reiniciamos el navegador cuando lo solicite.



Atendiendo las notificaciones de NoScript y adicionando sitios Web a la lista blanca

Una vez reiniciado, nuestro navegador tendrá un icono en la barra de estado ubicada en la esquina inferior derecha, indicando qué nivel de permiso el sitio Web actual tiene para ejecutar contenido en nuestra PC.

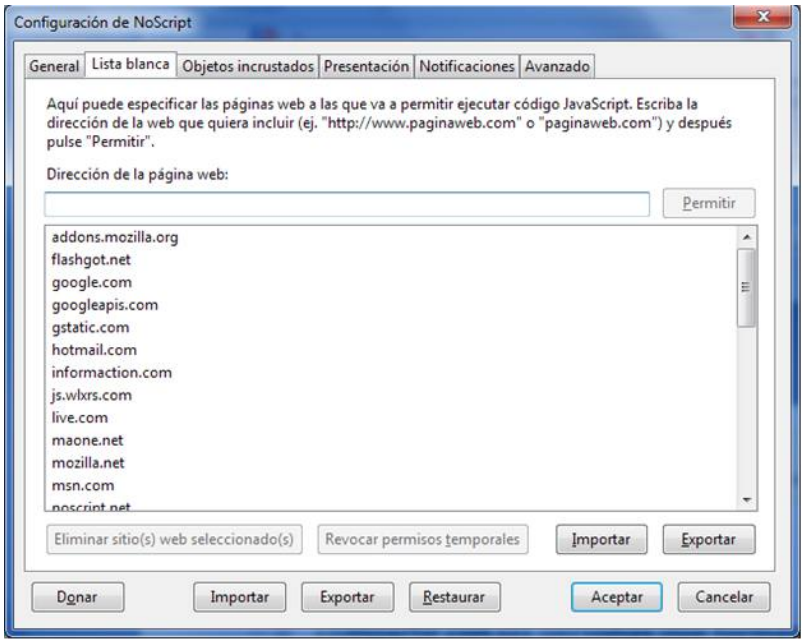
- Protección completa: los scripts son bloqueados para el sitio actual y sus marcos. Incluso si algunas de las Fuentes de scripts importadas por la página están en nuestra lista blanca, el código no se ejecutará (los documentos alojados no están habilitados).
- Muy limitado: el sitio principal es aún prohibido, pero algunas partes (como los marcos) son permitidos. En este caso, algún código puede ejecutarse pero es poco probable que la página funcione correctamente ya que está aún bloqueada la fuente de script principal.
- Permisos limitados: los scripts se permiten para el documento principal, pero otros elementos activos, o scripts importadas por la página de otras fuentes, no serán permitidos. Esto sucede cuando hay múltiples marcos en una página o elementos de scripts que enlazan con código alojados en otras plataformas.
- Mayormente confiable: todas las Fuentes de scripts para la página son permitidos, pero algún contenido embebido (ej. los marcos) serán bloqueados.
- Protección selectiva: los scripts son permitidos para algunas URLs. Los demás son marcados como no confiables.
- Todos los scripts son permitidos por el sitio actual.
- Los scripts son permitidos globalmente, sin embargo el contenido marcado como no confiable no se cargará.

Para adicionar un sitio en el que confiamos a la lista blanca, hacemos en el icono NoScript y seleccionamos:

- "Allow [domain name]" para permitir los scripts que están alojados bajo un nombre de dominio específico, o
- "Allow all this page" para permitir la completa ejecución de scripts – incluyendo los scripts de terceros que pueden estar alojados en cualquier lugar, pero que son importados por la página principal del sitio Web.

(Podemos usar las opciones "Temporarily allow" para permitir que el contenido cargue solo para la sesión actual del navegador. Esto es muy útil par a las personas que visitan un sitio solo una vez, y que quieren mantener la lista blanca de un tamaño manejable).

Alternativamente, podemos adicionar nombres de dominio directamente a la lista blanca haciendo clic en el botón de NoScript, seleccionando Options y haciendo clic en la pestaña Whitelist.



Marcando contenido como “no confiable”

Si deseamos permanentemente impedir que los scripts carguen en un sitio Web en particular, podemos marcarlo como no confiable: solo es necesario hacer clic en el icono NoScript, abrir el menu “Untrusted” y seleccionar "Mark [domain name] as Untrusted". NoScript recordará nuestra selección, incluso aunque la opción "Allow Scripts Globally" esté habilitada.

14. HTTPS EVERYWHERE

HTTPS Everywhere es un complemento de Firefox desarrollado por una colaboración entre The Tor Project (https://www.torproject.org) y Electronic Frontier Foundation (https://eff.org/). Su objetivo es cifrar nuestras comunicaciones con un número de sitios Web, incluyendo Google, Wikipedia y plataformas de red sociales muy populares como Facebook y Twitter.

Muchos sitios en la Web ofrecen algún soporte para cifrado sobre HTTPS, pero se hace difícil utilizarlos. Por ejemplo, ellos pueden conectarnos por defecto a través de HTTP, incluso cuando HTTPS esté disponible. O pueden llenar las páginas cifradas con enlaces que nos llevan de regreso al sitio sin cifrar. De esta forma, los datos (como nombre de usuario y contraseña) enviados y recibidos por estos sitios Web son transferidos en texto plano y pudieran ser vistos por terceros.

La extensión HTTPS Everywhere soluciona estos problemas reescribiendo todas las solicitudes de estos sitios a HTTPS. (Aunque la extensión se llama “HTTPS Everywhere”, solo activa HTTPS en una lista de sitios particular y solo puede usar HTTPS en sitios que lo soporten. No puede hacer que nuestra conexión hacia un sitio que no ofrece HTTPS como una opción sea segura).

Es necesario notar que muchos de estos sitios aún incluyen una gran cantidad de contenido de terceros que no están disponibles sobre HTTPS, como imágenes o iconos. Como siempre, si el icono con forma de candado del navegador está abierto o tiene una marca de exclamación, quiere decir que estamos vulnerables ante algunos adversarios que usan ataques activos o análisis de tráfico. Sin embargo, será mayor el esfuerzo necesario para monitorear nuestro navegador.

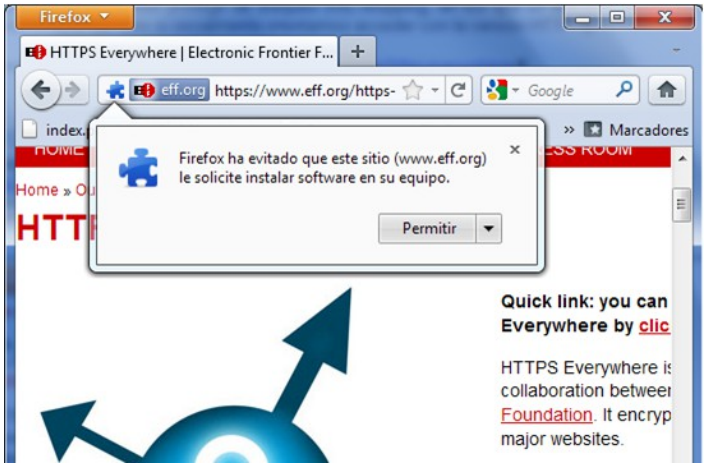
Algunos sitios Web (como Gmail) brindan soporte HTTPS automáticamente, pero usar HTTPS Everywhere también nos protege de ataques SSL-stripping, en los que un atacante oculta la versión HTTPS del sitio si inicialmente intentamos acceder con la versión HTTP.

Sobre el tema podemos profundizar en: https://www.eff.org/https-everywhere.

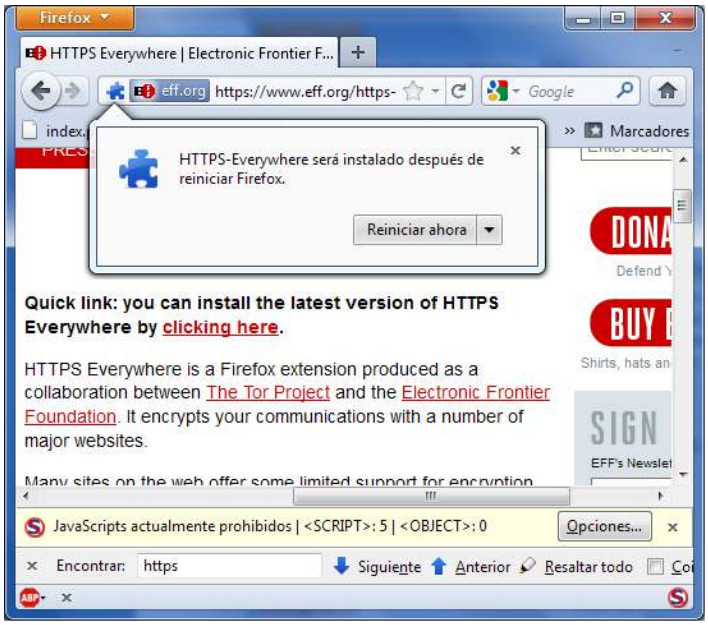
INSTALACIÓN

Primero, descargamos la extension HTTPS Everywhere desde el sitio oficial: https://www.eff.org/https-everywhere.

Seleccionamos la última versión liberada. En el ejemplo a continuación, se usó la versión 0.9.4 de HTTPS Everywhere .(Puede ser que ya haya una versión nueva disponible)

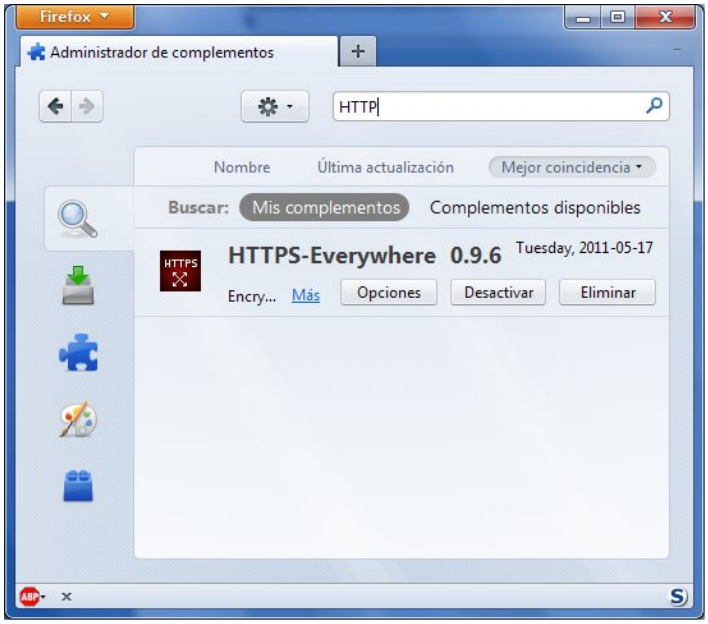


Hacemos clic en “Permitir”. Necesitaremos reiniciar Firefox haciendo clic en el botón "Reiniciar ahora". HTTPS Everywhere estará instalado.

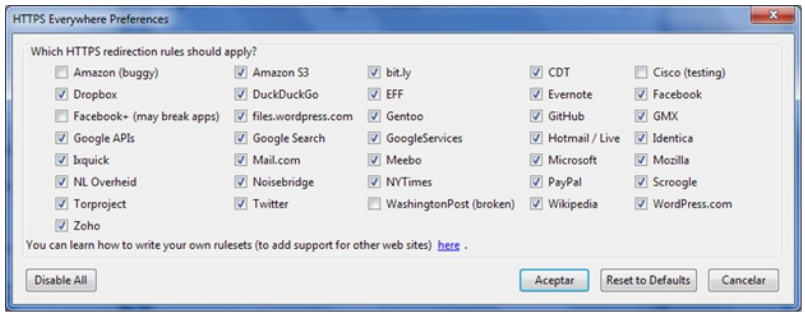


CONFIGURACIÓN

Para acceder al panel de configuración de HTTPS Everywhere en Firefox 4 (Linux), hacemos clic en el menú en la parte superior izquierda de nuestro navegador y seleccionamos Add-ons Manager. (Es bueno notar que la ubicación del Manager de add-ons de Firefox varía según las distintas versiones para sistemas operativos)



Hacemos clic en el botón Options.

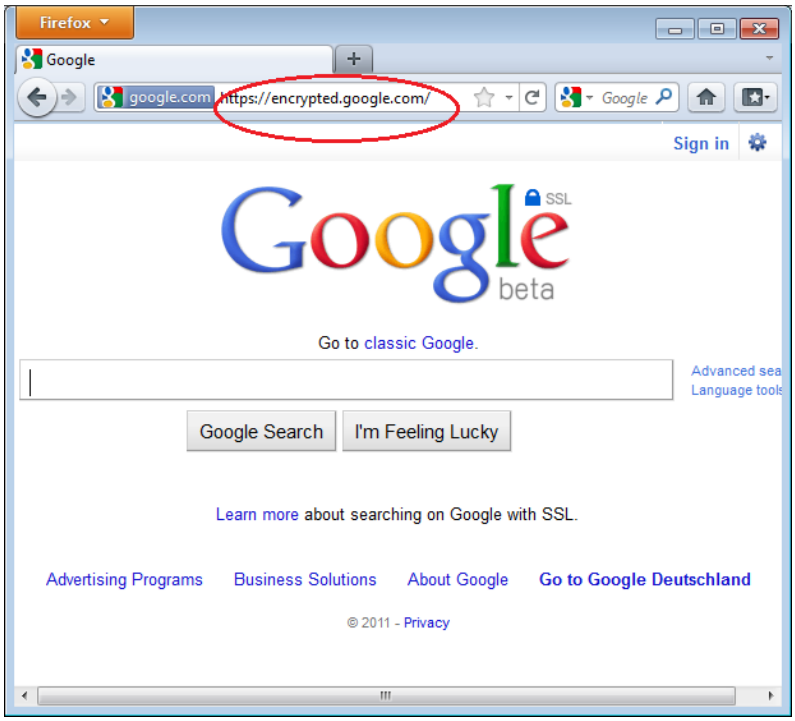


Se mostrará una lista con todos los sitios Web donde se deben aplicar las reglas de redireccionamiento HTTPS. Si tenemos problemas con una regla de redireccionamiento específica, podemos desmarcarla aquí. En este caso, HTTPS Everywhere no intervendrá más en la forma en que nos comunicamos con un sitio específico.

USO

Una vez que esté HTTPS Everywhere habilitado y configurado, es muy fácil y transparente de usar. Escribimos una URL http insegura (por ejemplo, http://www.google.com).

Presionamos Enter. Automáticamente seremos redireccionados al sitio Web encriptado HTTPS (en este ejemplo: https://encrypted.google.com). No es necesaria ninguna otra acción.



Si la red bloquea HTTPS

Nuestro operador de red puede decidir bloquear las versiones seguras de los sitios Web para incrementar su habilidad de espiar lo que hacemos. En esos casos, HTTPS Everywhere puede evitar que usemos estos sitios porque fuerza a nuestro navegador a usar solamente versiones seguras de estos sitios, nuca la versión insegura. (Por ejemplo, se ha oído sobre una red Wi-Fi en un aeropuerto donde todas las conexiones http eran permitidas, pero no las conexiones HTTPS. Quizás los operadores de la WI-FI estaban interesados en ver lo que hacían los usuarios. En el aeropuerto, los usuarios con HTTPS Everywhere no podían navegar en algunos sitios a menos que deshabilitaran temporalmente HTTPS Everywhere).

En este escenario, debemos seleccionar usar HTTPS Everywhere junto a una herramienta de evasión de censura como Tor o una VPN para evadir el bloqueo del acceso seguro a los sitios Web.

Adicionando soporte para sitios adicionales en HTTPS Everywhere

Podemos adicionar nuestras propias reglas al complemento HTTPS Everywhere para nuestros sitios web favoritos. Podemos encontrar como hacer esto en: https://www.eff.org/https-everywhere/rulesets. El beneficio de adicionar reglas es que estas enseñan a HTTPS Everywhere a asegurarse de que el acceso a estos sitios es seguro. Pero es bueno recordar: HTTPS Everywhere no nos permite acceder a los sitios de forma segura a menos que los operadores quieran que los sitios estén disponibles a través de HTTPS. Si un sitio no soporta HTTPS, no hay beneficio de adicionar reglas para él.

Si estamos administrando un sitio Web y tenemos una versión HTTPS disponible, una buena práctica sería enviarle la dirección al equipo de HTTPS Everywhere para que la incluyan en la liberación oficial.

15. CONFIGURACIONES DE PROXY Y FOXYPROXY

Un servidor proxy nos permite alcanzar un sitio Web u otra ubicación de Internet aún cuando no sea posible una conexión directa entre nuestra PC y el ISP. Hay muchos tipos de proxis, incluyendo:

- Proxis Web, los cuales solo requieren que sepamos la dirección del sitio web del proxy. Una URL de proxy Web puede verse como esta: http://www.example.com/cgi-bin/nph-proxy.cgi
- Proxis HTTP, los cuales requieren que modifiquemos las configuraciones del navegador. Los proxis HTTP solo funcionan para contenido Web. Podemos tener la información acerca de un proxy HTTP en el formato "proxy.example.com:3128" o "192.168.0.1:8080".
- Proxis SOCKS, los que requieren también que modifiquemos las configuraciones del navegador. Los proxis SOCKS funcionan para diferentes aplicaciones de Internet, incluyendo correo electrónico y herramientas de mensajería instantánea.

Podemos usar un proxy Web directamente sin ninguna configuración escribiendo en la URL. Los proxis HTTP y SOCKS, sin embargo, necesitan ser configurados en nuestro navegador Web.

CONFIGURACIÓN DE PROXY EN FIREFOX POR DEFECTO

En Firefox 4 (Linux), entramos a la configuración a partir del menú que está en la esquina superior izquierda y seleccionando Opciones. En la ventana que se abre, seleccionamos el icono con la etiqueta Avanzado y seleccionamos la pestaña Red. Debemos ver esta ventana:

Seleccionamos Configuración, hacemos clic en "Configuración manual del proxy" y entramos la información del servidor proxy que vamos a usar. Es bueno recordar que los proxis HTTP y los proxis SOCKS funcionan diferentes y necesitan ser configurados en sus respectivos campos. Si hay un signo de “dos puntos” en la información de nuestro proxy, este indicará la separación entre la dirección del proxy y el número de puerto. Nuestra pantalla debe verse así:

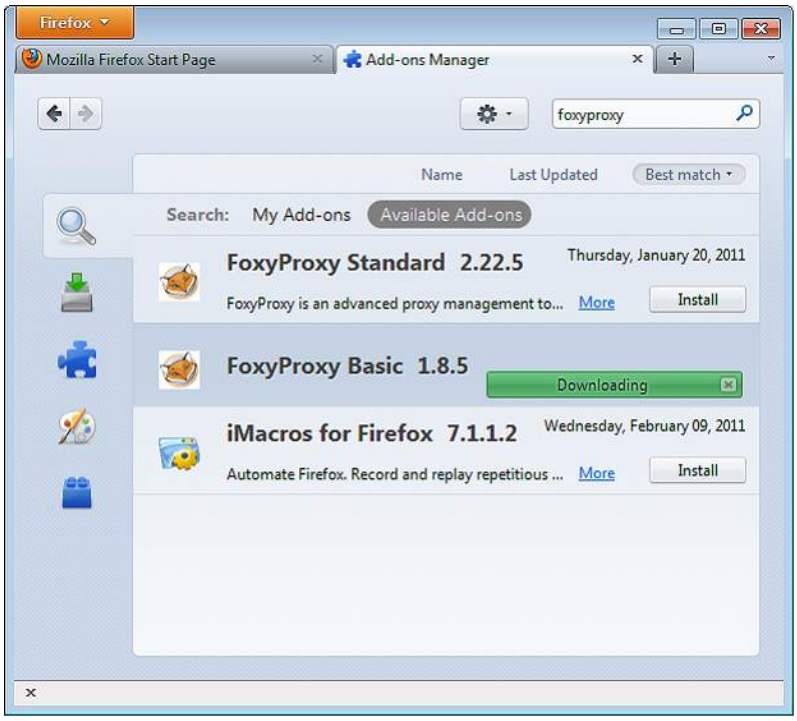
Después de hacer clic en OK, nuestra configuración será salvada y nuestro navegador Web se conectará automáticamente a través de ese proxy en todas las conexiones futuras. Si obtenemos un mensaje de error como, "The proxy server is refusing connections" o "Unable to find the proxy server", es que la configuración del proxy es incorrecta. En este caso, repetimos los pasos anteriores y seleccionamos “No proxy” en la última pantalla para desactivar el proxy.

FOXYPROXY

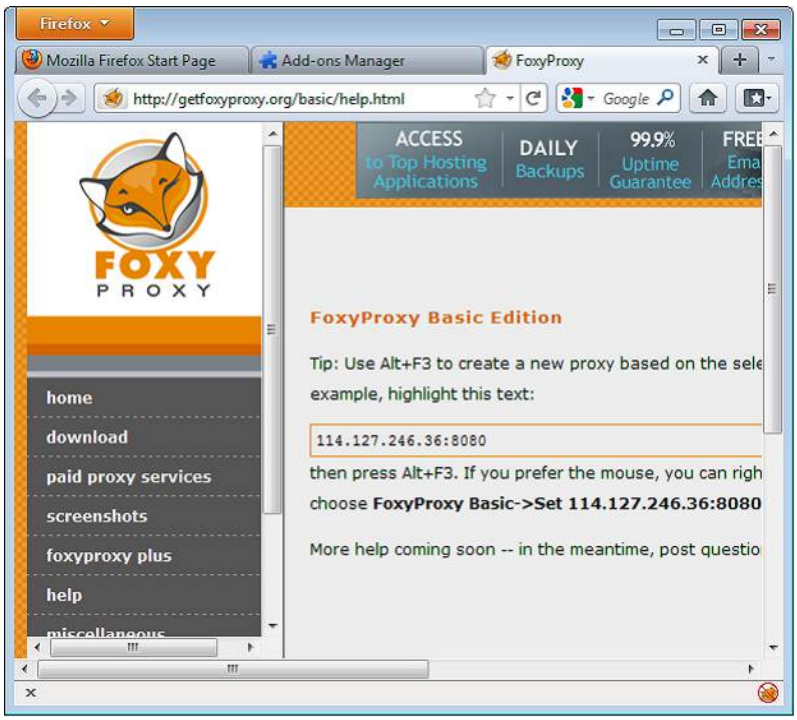
FoxProxy es un complemento de Firefox gratuito que facilita el manejo de diferentes servidores proxy y el intercambio entre ellos. Para detalles sobre FoxProxy, podemos visitar http://getfoxyproxy.org/.

Instalación

En Firefox 4 (Linux), hacemos clic en el menú de la izquierda superior de la pantalla y seleccionamos "Complementos".
En la ventana emergente, entramos el nombre del complemento que queremos instalar (en este caso "FoxyProxy") en la caja de búsqueda en la parte superior derecha y hacemos clic en Enter.
En los resultados de búsqueda, veremos dos versiones diferentes de FoxyProxy: estándar y básica. Para una comparación completa de las dos ediciones podemos visitar http://getfoxyproxy.org/downloads.html#editions, pero la edición básica es suficiente para las necesidades de evasión básicas. Después de decidir qué edición deseamos, hacemos clic en Install.

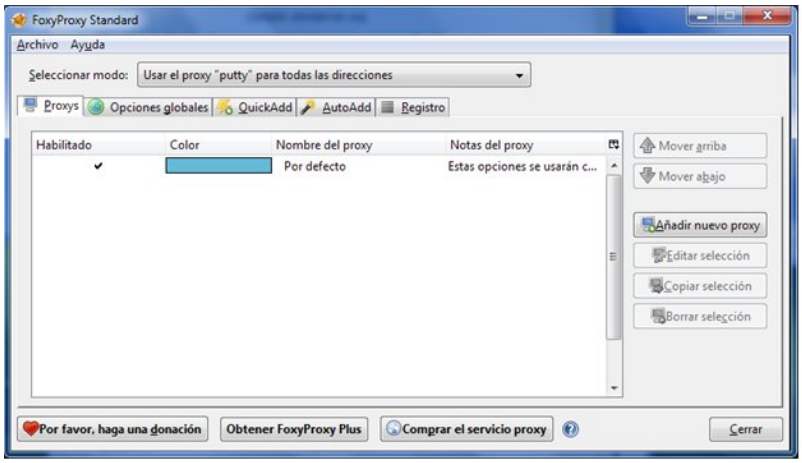


Después de la instalación, Firefox debe reiniciarse y abrir el sitio de Ayuda de FoxyProxy. Veremos el icono de FoxyProxy en la parte inferior derecha.

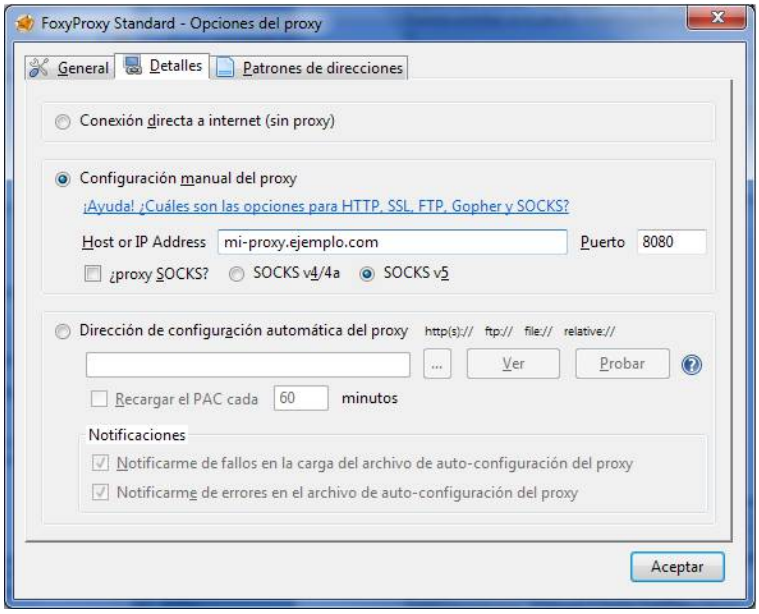


Configuración

Para que FoxyProxy haga su trabajo, necesita saber que configuración de proxy debe usar. Para ello abrimos la ventana de configuración haciendo clic en la parte inferior derecha de la ventana de Firefox. La ventana de configuración se ve así:



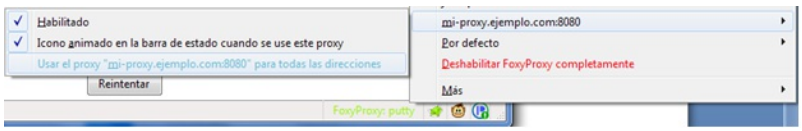
Hacemos clic en "Add New Proxy". En la ventana siguiente, entramos los detalles del proxy de forma similar a cuando configuramos un proxy en Firefox.



Seleccionamos "Manual Proxy Configuration", entramos la dirección IP o el nombre del proxy y el número de puerto en los campos apropiados. Chequeamos "SOCKS proxy?" si aplica, y hacemos clic en OK. Podemos adicionar más proxis repitiendo los pasos anteriores.

Uso

Podemos intercambiar entre nuestros proxis (o seleccionar no usar proxy) haciendo clic derecho en el icono de zorro en la parte inferior derecha de la ventana de Firefox:



Para seleccionar un servidor proxy, simplemente hacemos clic izquierdo en el proxy que deseamos utilizar.

17. Freegate
18. Simurgh
19. UltraSurf
20. Servicios VPN
21. VPN on Ubuntu
22. Hotspot Shield
23. Alkasir
24. Tor : The Onion Router
25. JonDo
26. Your-Freedom

16. INTRODUCCIÓN

El concepto básico de evadir la censura de Internet es enrutar las solicitudes a través de un tercer servidor que no esté bloqueado y que esté conectado a Internet a través de una conexión no censurada. Este capítulo explica algunas de las herramientas que se basan en el uso de dicho tipo de servidores para sortear el bloqueo, filtrado y monitoreo de Internet. La selección de cuál es la mejor herramienta para conseguir nuestros objetivos se basa en una evaluación inicial de acuerdo al tipo de contenido que deseamos acceder, los recursos disponibles, y los riesgos de hacerlo.

Las herramientas para vencer el bloqueo, filtrado y monitoreo de Internet están diseñadas para enfrentarse a diferentes obstáculos y amenazas. Ellas pueden facilitar:

- **Evadir la censura:** Nos permiten leer o escribir documentos u otras formas de contenido, enviar y recibir información, o comunicar con personas en particular, sitios o servicios burlando a la vez los intentos de impedírnoslo. Por ejemplo, leyendo una página desde el cache de Google o un agregador RSS en lugar de hacerlo desde el propio sitio web.
- **Prevenir las escuchas ocultas:** Manteniendo las comunicaciones privadas, para que nadie pueda inspeccionar el contenido de lo que estamos comunicando. (No obstante, siempre se puede ver con quien nos estamos comunicando). Las herramientas que intentan evadir la censura sin tener en cuenta la escucha oculta o secreta pueden ser vulnerables a la censura por los filtros de palabras clave que bloquean todas las comunicaciones que contienen ciertas palabras prohibidas. Por ejemplo, varias formas de cifrado, tales como https o SSH, hacen que la información sea indescifrable salvo para remitente y el receptor de la misma. Un "vigilante" verá qué usuario está accediendo a cada servidor Web, pero del contenido solo verá una cadena de caracteres sin sentido.
- **Mantener el anonimato:** la habilidad de comunicarnos de modo que nadie pueda relacionarnos con la información con la que nos estamos conectando – ni el operador de nuestra conexión a Internet ni los sitios ni personas con las que nos comunicamos. La mayoría de los servicios y herramientas proxy no brindan ofrecen anonimato o simplemente no brindan anonimato alguno: el operador de proxy es capaz de observar el tráfico que entra y sale del proxy y puede determinar fácilmente quien lo envía, cuando, y con qué frecuencia; un observador malicioso en cualquiera de las partes de la conexión es capaz de obtener la misma información. Las herramientas como Tor están diseñadas para dificultar a los atacantes obtener este tipo de información acerca de los usuarios limitando la cantidad de información que cualquier nodo de la red puede tener sobre la identidad del usuario o su ubicación.
- **Ocultar lo que hacemos:** Disfrazando las comunicaciones que enviamos de forma que alguien que nos espíe no pueda probarnos que estamos tratando de evitar la censura. Por ejemplo, la steganography, que consiste en ocultar un mensaje de texto en una imagen, puede ocultar que estamos usando una herramienta de engaño. Usar servicios proxy o redes que sean usadas por muchos tipos de personas diferentes puede servirnos de cobertura para que no se pueda probar que estamos tratando de evadir la censura. Esto es especialmente bueno cuando otros usan el mismo sistema para obtener contenido no sensible.

Algunas herramientas protegen la comunicación en solo una de estas formas. Por ejemplo, muchos proxis pueden evadir la censura pero no previenen la escucha secreta – ellos permiten que veamos un sitio bloqueado pero no evitan que alguien monitoree lo que estamos leyendo. Es importante comprender que quizás se necesite una combinación de herramientas para lograr nuestros objetivos.

Cada tipo de protección es relevante para cada persona en cada situación. Cuando seleccionemos herramientas que evitan la censura de Internet, debemos tener en cuenta qué tipo de protección necesitamos y que grupo de herramientas nos facilitaría dicha protección. Por ejemplo, ¿qué sucedería si alguien detecta que intentamos evadir un sistema de censura? ¿Es realmente importante ocultar lo que leemos y escribimos, o solo queremos lograr el acceso a un servicio o sitio en particular?

Algunas veces, una herramienta puede usarse para vencer la censura y proteger el anonimato, pero los pasos para cada una son diferentes. Por ejemplo, el programa Tor es comúnmente usado para ambos propósitos, pero los usuarios de Tor que están más interesados en uno u otro propósito usarán esta herramienta de forma diferente.

UN AVISO IMPORTANTE

La mayoría de las herramientas de evasión se pueden detectar con suficiente esfuerzo de los operadores o agencias de gobierno, ya que generan tráfico con patrones distintivos. Esto se cumple especialmente para los métodos de evasión que no usan cifrado, pero puede suceder también con los que lo usan. Resulta difícil mantener en secreto el hecho de que se está usando una herramienta de evasión, especialmente si usa una técnica bastante popular o si usa continuamente el mismo método de evasión durante un largo período de tiempo. También hay otras vías de descubrir nuestra conducta que no dependen de la tecnología: la observación en persona, la supervisión o vigilancia, o algún otro modo de recolección de información tradicional.

Los riesgos son diferentes en cada situación, y cambian frecuentemente. Podemos confiar en que todos esos intentos de restringir las comunicaciones contribuirán al mejoramiento de los métodos de evasión.

Si estamos haciendo algo que pueda ponernos en riesgo en el lugar donde estamos, deberemos hacer nuestras propias valoraciones acerca de la seguridad y (si es posible) consultar expertos:

- Muy a menudo, necesitaremos del servicio que provee un extraño. Debemos tener en cuenta que ellos pueden tener acceso a la información que accedemos, los sitios que visitamos e incluso las contraseñas que entramos en aquellos sitios Web sin cifrado. Incluso si conocemos y confiamos en la persona que administra un proxy o VPN, esta puede ser atacada o forzada a comprometer nuestra información.
- Es necesario recordar que las promesas de anonimato y seguridad de muchos sistemas pueden ser poco precisas. Es necesario entonces buscar una confirmación independiente. Las herramientas de código abierto pueden ser evaluadas por amigos entendidos en la materia. Los fallos de seguridad en herramientas de código abierto pueden ser descubiertos y reparados por voluntarios. Es muy difícil hacer lo mismo con programas propietarios.
- Para conseguir el anonimato y la seguridad puede ser preciso cumplir ciertas prácticas y procedimientos de seguridad y hacerlo con disciplina. Ignorar los procedimientos hará vulnerable toda la seguridad que hayamos logrado. Es muy peligroso pensar que existe una solución con un solo clic que garantice el anonimato o la seguridad. Por ejemplo, enrutar nuestro tráfico a través de un proxy o a través de Tor no es suficiente. Tenemos que asegurarnos de usar el cifrado de los datos, mantener nuestra computadora segura y evitar revelar nuestra identidad en el contenido que posteamos.
- Debemos de ser conscientes de que las personas (o gobiernos) pueden ofrecer honeypots (tarros de miel) – falsos sitios Web que pretenden ofrecer comunicación segura pero en realidad capturan la comunicación de usuarios involuntarios.
- Algunas veces incluso "Policeware" pueden ser instalados en las computadoras de los usuarios – ya sea de foma remota o directamente – estos ataques como el malware, monitorean la actividad de la computadora incluso si no está conectada a Internet y socava la mayoría del resto de los medios de seguridad preventivos.
- Debemos prestar atención a las amenazas no técnicas. ¿Qué sucede si alguien roba nuestra computadora o teléfono móvil o los de nuestros amigos? ¿Si en un CyberCafé los empleados miran por sobre nuestro hombro? ¿Qué sucede si alguien se sienta en la computadora de un café donde nuestra amiga olvidó cerrar la sesión y nos envía un mensaje pretendiendo ser ella? Qué si alguien de nuestra red social es arrestado y forzado a dar las contraseñas?
- Si hay leyes o regulaciones que restringen o prohíben el material que estamos accediendo o las actividades que estamos acometiendo, debemos ser consciente de las consecuencias.

Para saber más seguridad y privacidad digital, podemos leer:

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

17. FREEGATE

Freegate es una herramienta proxy para usuarios de Windows que fue desarrollada inicialmente por DIT-INC para sortear la censura de Internet en China e Iran.

INFORMACIÓN GENERAL

Sistemas operativos que soporta	
Localización	English, Chinese, Persian, Spanish
Sitio Web	http://www.dit-inc.us/freegate
Forum de soporte:	http://www.dit-inc.us/support

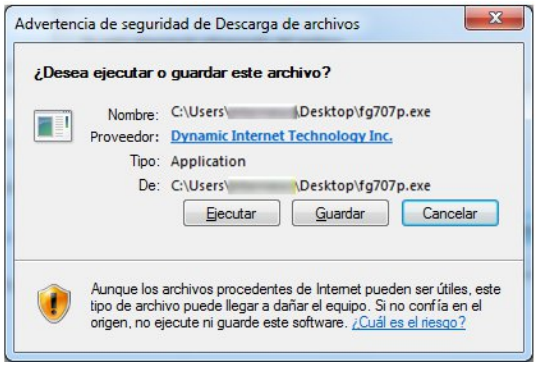
CÓMO OBTENER FREEGATE

Podemos descargar el programa gratis desde http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/Freegate.shtml.

Tendremos un fichero con extensión .zip, que tendremos que extraer primeramente. Hacemos clic derecho en el fichero que descargamos y seleccionamos “Extraer todo”, y hacemos clic en el botón “Extraer”. El fichero resultante tiene cerca de 1.5 MB. El nombre del ejecutable puede verse como una serie corta de letras y números (e.g. “fg707p.exe”).

INSTALACIÓN

Cuando ejecutamos la aplicación por primera vez, podemos ver un Aviso de Seguridad. Podemos aceptar este Aviso de Seguridad desmarcando la caja "Always ask before opening this file" y haciendo clic en Run.



EJECUTANDO FREEGATE

Ahora la aplicación debe comenzar y conectarse automáticamente a un servidor.

Tan pronto como se establezca el canal seguro, veremos la ventana de estado de Freegate y se abrirá una nueva instancia de Internet Explorer con la URL http://dongtaiwang.com/loc/phome.php?v7.07&l=409 cargada, dependiendo de nuestra versión de nuestro idioma. Esta es la confirmación de que estamos usando Freegate correctamente a través de un túnel cifrado.

Si todo va bien, podemos comenzar a navegar usando la ventana de Internet Explorer abierta por Freegate para evadir la censura de Internet.

Si queremos usar otra aplicación con Freegate (por ejemplo el navegador Web Firefox o el cliente de mensajería instantánea Pidgin), tendremos que configurarla para que usen Freegate como servidor proxy. La IP es 127.0.0.1 y el puerto es 8580.

Bajo la pestaña Settings en Freegate, podemos seleccionar nuestro idioma de interfaz que puede ser Inglés, Chino Tradicional, Chino Simplificado, Farsi y Español. Bajo Status, podemos ver nuestro tráfico de carga/descarga a través de la red Freegate. La pestaña Server permite escoger entre varios servidores, los cuales pueden ser más rápidos que nuestra conexión actual.

18. SIMURGH

Simurgh (que significa "phoenix" en Persa) es un programa de proxy y servicio independiente de peso ligero. Esto significa que puede ejecutarse sin instalación previa o derechos de administración en la computadora. Podemos copiarlo a nuestra memoria externa USB y usarlo en una computadora compartida (en un cibercafé por ejemplo).

INFORMACIÓN GENERAL

Sistemas operativos que soporta	
Localización	Inglés
Sitio Web	https://simurghesabz.net
Correo electrónico de soporte	E-mail: info@simurghesabz.net

DESCARGANDO SIMURGH

Para usar el servicio Simurgh, descargar la herramienta gratis desde https://simurghesabz.net/.

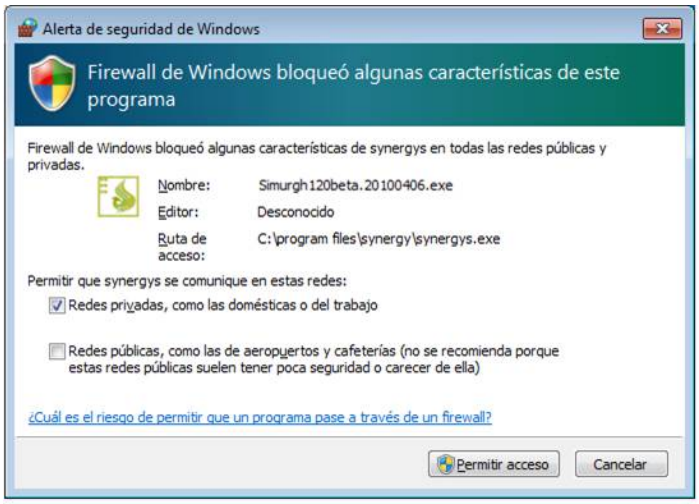
Está disponible para cualquier versión de Microsoft Windows. El tamaño del fichero es menor de 1MB, así que puede ser descargado incluso desde una conexión de Internet lenta en un tiempo razonable.

USANDO SIMURGH

Para iniciar Simurgh, hacemos clic en el fichero que descargamos. Por defecto, los ficheros que se descargan con Microsoft Internet Explorer se guardan en el Escritorio y los descargados con Mozilla Firefox se guardan en "Mis documentos" y "Descargas".

Es necesario notar que cuando ejecutamos Simurgh por primera vez, podemos encontrar una Alerta de Seguridad de Windows que pregunta si queremos mantener bloqueado Simurgh. Como Simurgh necesita comunicarse con Internet es muy importante seleccionar "Desbloquear" o "Permitir Acceso" (dependiendo de nuestra versión de Windows).
Veremos una ventana emergente como esta:

O como esta:



Después que hayamos iniciado Simurgh satisfactoriamente, hacemos clic en Start para crear una conexión segura.

Cuando el botón Start cambia a botón Stop, Simurgh se conectó exitosamente a sus servidores.

Para asegurarnos que estamos conectados al servidor Simurgh

Ahora una nueva ventana de nuestro navegador Internet Explorer se abrirá con una página de prueba. Si nuestra conexión se origina en otro país, como Estados Unidos, esto confirma que Simurgh ha cambiado satisfactoriamente las configuraciones de nuestro navegador y estamos navegando automáticamente sobre una conexión segura Simurgh.

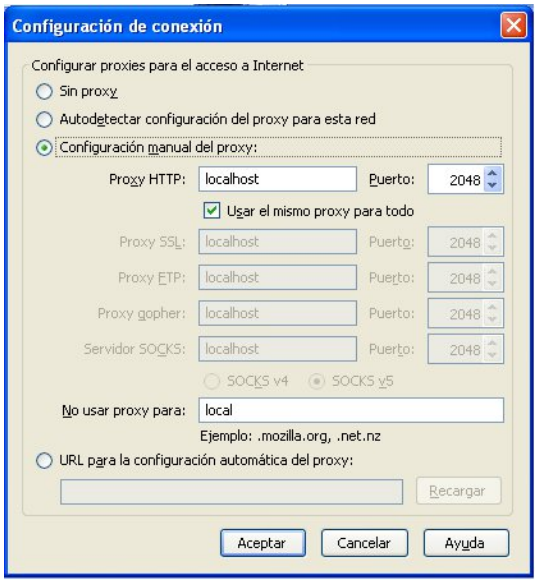
También podemos usar el sitio web http://www.geoiptool.com para chequear de donde viene nuestra conexión. Si el sitio web muestra nuestra ubicación muy lejos de donde estamos (en otro país como en Estados Unidos), quiere decir que estamos usando la conexión segura de Simurgh.

USANDO SIMURGH CON MOZILLA FIREFOX

Para usar otro navegador web como Mozilla Firefox, necesitamos configurarlo para usar el proxy HTTP "localhost" con el puerto 2048.

En Firefox, podemos encontrar las configuraciones de proxy por la vía Herramientas > Opciones > Avanzado > Red > Configuración.

En la ventana "Configuración de conexión" seleccionamos "Configuración manual del proxy" y entramos "locahost" (sin las comillas) como proxy HTTP y en el puerto 2048, como se muestra en la imagen. Para aceptar la nueva configuración, clic en OK.



19. ULTRASURF

UltraSurf, de la compañía de desarrollo UltraReach Internet Corp, es una herramienta de proxy diseñada para ayudar a evadir la censura a los usuarios de Internet Chinos, pero sirve para usuarios de otros países también.

INFORMACIÓN GENERAL

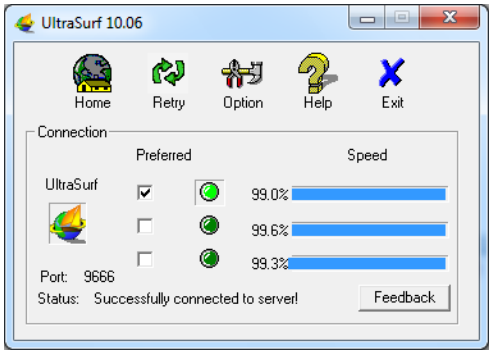
Sistemas operativos que soporta	
Localización	Inglés
Sitio Web	http://www.ultrareach.com
Soporte	FAQ: http://www.ultrareach.com/usercenter_en.htm

CÓMO OBTENER ULTRASURF

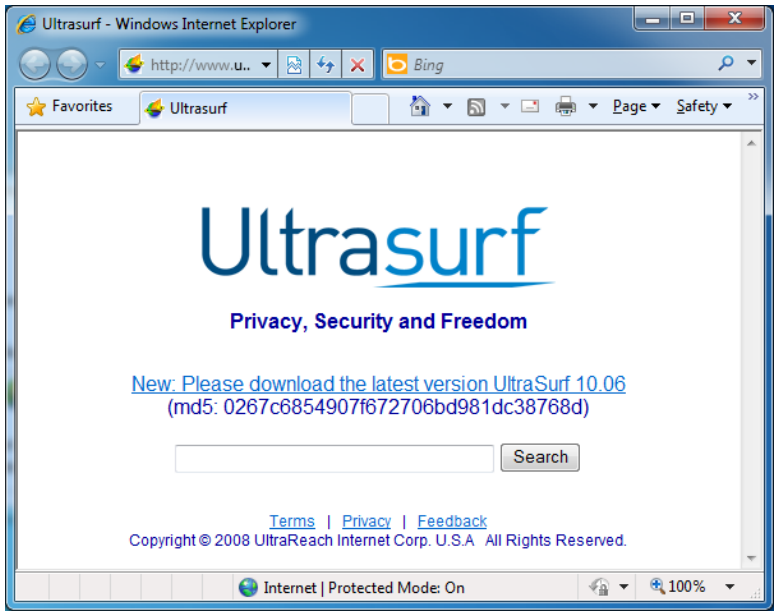
Podemos descargar el software gratis (para Windows solamente) desde http://www.ultrareach.com o http://www.ultrareach.net/ o http://www.wujie.net (La última página está en Chino, pero la descarga es fácil de encontrar y es en Inglés).

INSTALANDO Y USANDO ULTRASURF

Una vez que se termine de descargar el fichero que se verá como "u1006.zip" (dependiendo del número de la versión), extraemos haciendo clic derecho sobre el fichero y seleccionando “Extraer todo”. Hacemos doble clic en el nuevo ícono “u1006” para iniciar la aplicación.



UltraSurf abrirá automáticamente el Internet Explorer y mostrará la página de búsqueda de UltraSurf: http://www.ultrareach.com/search.htm. Ahora podemos comenzar a navegar, usando la instancia de Internet Explorer que UltraSurf activó.



Si deseamos usar otra aplicación con UltaSurf (por ejemplo el navegador Firefox o el cliente de mensajería instantánea Pidgin), necesitamos configurarlos para que usen el cliente UltraSurf como servidor proxy. La IP es 127.0.0.1 (que es nuestra PC, conocida también como "locahost") y el puerto es 9666.

La Guía de Usuario de UltraSurf se puede abrir desde la ventana principal de UltraSurf haciendo clic en "Help".

La información de UltraSurf Chino (wujie) se encuentra en:
http://www.internetfreedom.org/UltraSurf

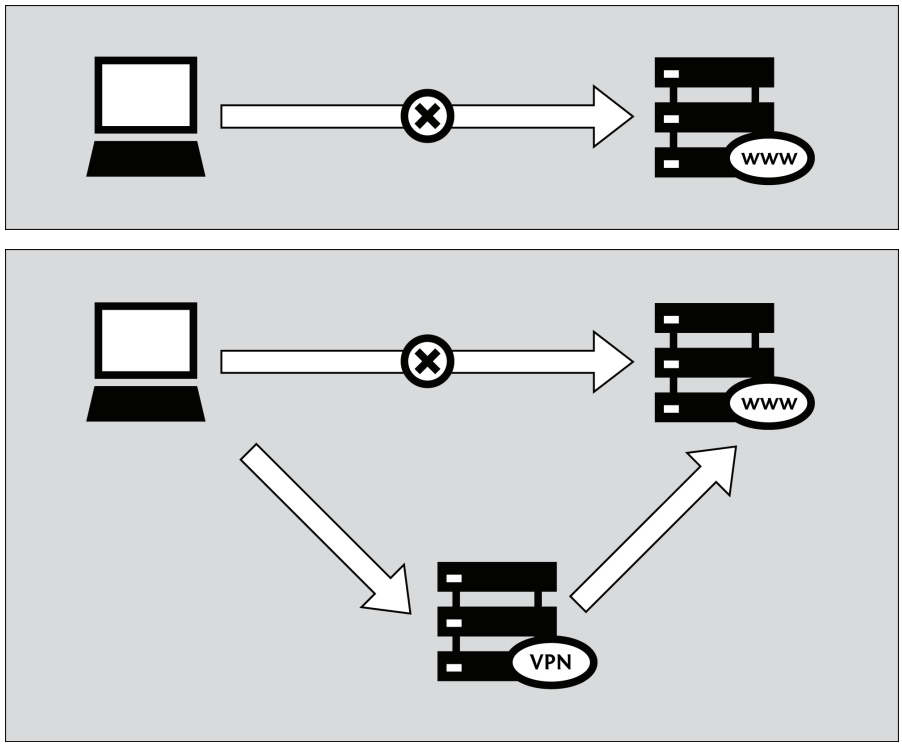
La Guía de usuario china está en: http://www.wujie.net/userguide.htm

20. SERVICIOS VPN

Una **red privada virtual(VPN)** permite cifrar los datos de conexiones entre nosotros y un ordenador en otra localización. Este ordenador puede pertenecer a nuestra organización, un contacto confiable o un servicio VPN.

Como los servicios VPN envían todo el tráfico de Internet a través de un túnel, puede usarse para correo electrónico, mensajería instantánea, **Voz sobre IP** (VoIP) y cualquier otro servicio de Internet en adición a la navegación Web, haciendo que todo lo que viaja a través del túnel sea ilegible para cualquiera que esté observando la comunicación.

Si el túnel termina fuera del área donde Internet está restringido, este puede ser un método efectivo de **evasión**, ya que la entidad/servidor que filtra solo ve datos cifrados, y no tiene forma de saber que datos pasan a través del túnel. Esto tiene el efecto adicional de hacer que todos los tipos diferentes de datos se vean similares ante una "escucha".



Como muchas compañías internacionales usan la tecnología VPN para permitir a los empleados que necesitan acceso a información sensible financiera o de otro tipo de sus compañías desde sus casas u otra ubicación remota sobre Internet, la tecnología VPN es menos propensa a ser bloqueada que las tecnologías usadas para propósitos de evasión de la censura.

Es importante notar que los datos son cifrados solo hasta el final del túnel, y después viaja sin cifrar a su destino final. Si, por ejemplo, configuramos un túnel de un proveedor VPN comercial, y solicitamos la página Web http://news.bbc.co.uk a través del túnel, los datos serán cifrados desde nuestra máquina hasta el proveedor VPN, pero de ahí al servidor que ejecuta la BBC la información viajará sin cifrado, como tráfico normal. Esto significa que el proveedor VPN, la BBC y cualquiera que controle el sistema entre estos dos servidores, podrá en teoría, ser capaz de ver los datos que hemos enviado o solicitado.

USANDO SERVICIOS VPN

Los servicios VPN pueden requerir de instalación o no de un programa del lado del cliente (muchos confían en el soporte VPN que existe en los sistemas Windows, Mac OS or GNU/Linux y no necesitan programas clientes).

Usar un servicio VPN requiere que confiemos en los dueños del servicio, pero brinda método simple y conveniente de evasión del filtrado de Internet, gratis o por un monto mensual entre los 5 y 10 dólares americanos, dependiendo del servicio. Los servicios gratis son a menudo financiados por la publicidad y limitan el ancho de banda y/o el máximo de tráfico permitido sobre un periodo dado.

Algunos servicios VPN gratis más populares son:

- Hotspot Shield, https://hotspotshield.com
  De acuerdo a un reporte hecho en 2010 de Berkman Center, Hotspot Shield es abrumadoramente el servicio VPN más popular. Para más detalle en cómo obtener y usar Hotspot Shield, podemos leer el capítulo "Hotspot Shield" de este 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

Algunos ejemplos de servicios VPN pagados incluyen Anonymizer, GhostSurf, XeroBank, HotSpotVPN, WiTopia, VPN Swiss, Steganos, Hamachi LogMeIn, Relakks, Skydur, iPig, *iVPN.net*, FindNot, Dold, UnblockVPN y SecurelX.

Podemos encontrar una lista de servicios VPN gratis y pagados, con su tarifa mensual y características técnicas en http://en.cship.org/wiki/VPN.

ESTÁNDARES DE VPN STANDARDS Y CIFRADO

Hay un número de estándares diferentes para configurar una red VPN, incluyendo **IPSec**, **SSL/TLS** y **PPTP**, que varían en términos de complejidad, el nivel de seguridad que proveen, y cual sistema operativo está disponible. Naturalmente, hay muchas implementaciones diferentes de cada estándar por diferentes proveedores de solución y por tanto ofrecen diferentes funcionalidades.

- Mientras PPTP es conocida por usar el cifrado más débil incluso que IPSec o SSL/TLS, puede ser útil para traspasar el bloqueo de Internet, y el cliente está convenientemente incorporado en la mayoría de las versiones de Microsoft Windows.
- Los sistemas VPN basados en SSL/TLS son relativamente simples de configurar, y proveen un nivel sólido de seguridad.
- IPSec se ejecuta en el nivel de Internet, responsable de la transferencia de paquetes, en la arquitectura de Internet, mientras los otros se ejecutan en el nivel de aplicación. Esto hace IPSec más flexible, pues puede ser usada para proteger todos los niveles de protocolo superiores, pero también es difícil de configurar.

CONFIGURANDO NUESTRO PROPIO SERVICIO VPN

Como una alternativa de pagar por los servicios de VPN comerciales, los usuarios con contactos en lugares sin restricciones pueden hacer que los contactos descarguen e instalen los programas necesarios para levantar un servicio VPN privado. Esto requiere un conocimiento técnico de un nivel más alto, pero será gratis. Además por la naturaleza privada de esta instalación el servicio tiende a ser menos bloqueado que un servicio comercial que ha estado habilitado por un largo tiempo. Uno de los programas gratis y de código abierto más usado y que está disponible para configurar este tipo de VPN privado es OpenVPN (http://openvpn.net), que puede ser instalado en Linux, MacOS, Windows y muchos otros sistemas operativos.

Para entender cómo configurar un sistema OpenVPN, podemos leer el capítulo "Usando OpenVPN" de este manual.

VENTAJAS

Las VPNs nos aseguran una transferencia cifrada de nuestros datos, de manera que es una de las vías más seguras para evadir la censura de internet. Una vez configuradas, son fáciles y transparentes de usar.

VPN es más conveniente para usuarios capaces que requieren servicios de evasión seguros más allá de solo tráfico web y acceden a Internet desde su propia computadora y pueden instalar programas. Los servicios comerciales de túnel son un excelente recurso para usuarios en lugares con Internet restringido y que no tienen un contacto en quien confiar en sitios sin filtrar. La tecnología VPN es una aplicación muy común para otras tareas y no es probable que sea bloqueada.

DESVENTAJAS Y RIESGOS

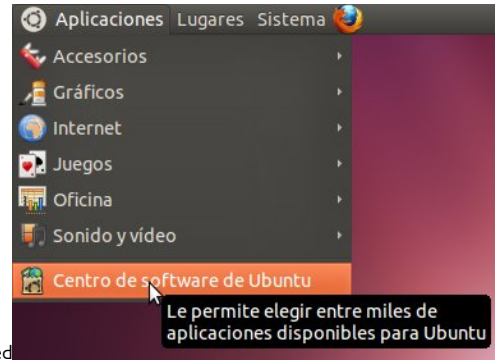
Servicios comerciales de VPN son conocidos públicamente y muchos están filtrados. Ellos normalmente no pueden ser usados por usuarios en lugares de acceso público donde los usuarios no pueden instalar programas, como los Cyber cafés o librerías. El uso de aplicaciones de túnel y especialmente VPN pueden requerir un nivel alto de habilidad técnica que otros métodos de evasión no requieren.

Un operador de red puede detectar que está siendo usado un VPN y determinar quién es el proveedor. El operador de red no debe ser capaz de ver las comunicaciones enviadas sobre VPN a menos que el VPN esté configurado incorrectamente.

El operador de túnel o VPN (algo así como un operador de proxy) puede ver lo que estamos haciendo a menos que usemos algún cifrado adicional para nuestras comunicaciones; cuando no usamos ningún cifrado adicional, debemos confiar en que el operador de VPN o túnel no abusará del acceso a nuestras comunicaciones.

21. VPN ON UBUNTU

Si usamos Ubuntu como sistema operativo, podemos conectarnos a VPN usando la propiedad NetworkManager y el cliente gratis OpenVPN.



OpenVPN permite conectarnos a redes VPN usando una variedad de métodos de autenticación. Por ejemplo, aprenderemos como conectarnos a un servidor VPN usando AirVPN, un servicio VPN gratis. El proceso de configuración para OpenVPN en Ubuntu es el mismo, sin importar el servicio VPN que estemos usando.

Instalando OpenVPN por NetworkManager

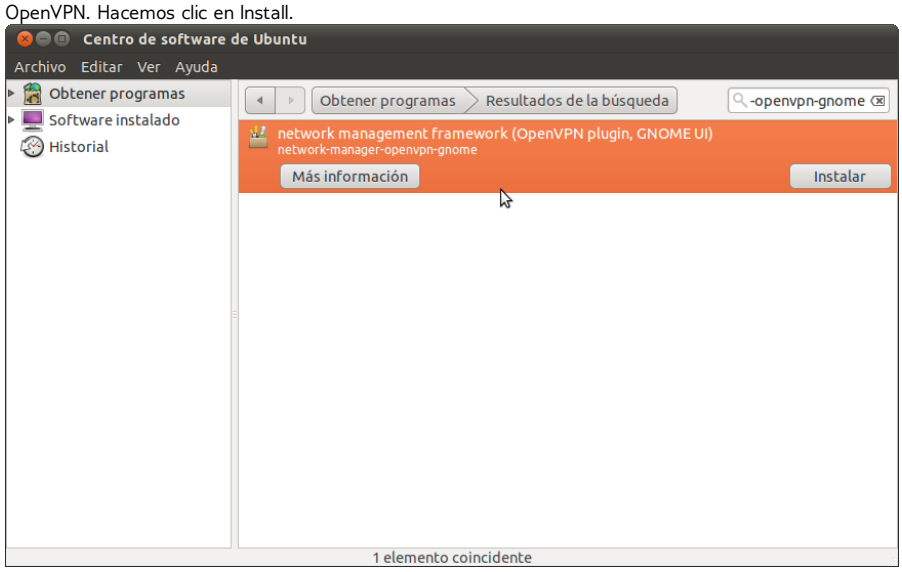
NetworkManager, es la utilidad de red que nos permite abrir o cerrar nuestra conexión VPN, y está incluida con Ubuntu por defecto – la podemos encontrar en el área de notificaciones de nuestra pantalla, cerca del reloj del sistema.

Después, buscamos una extensión de OpenVPN que funcione con NetworkManager, desde Ubuntu Software Center.

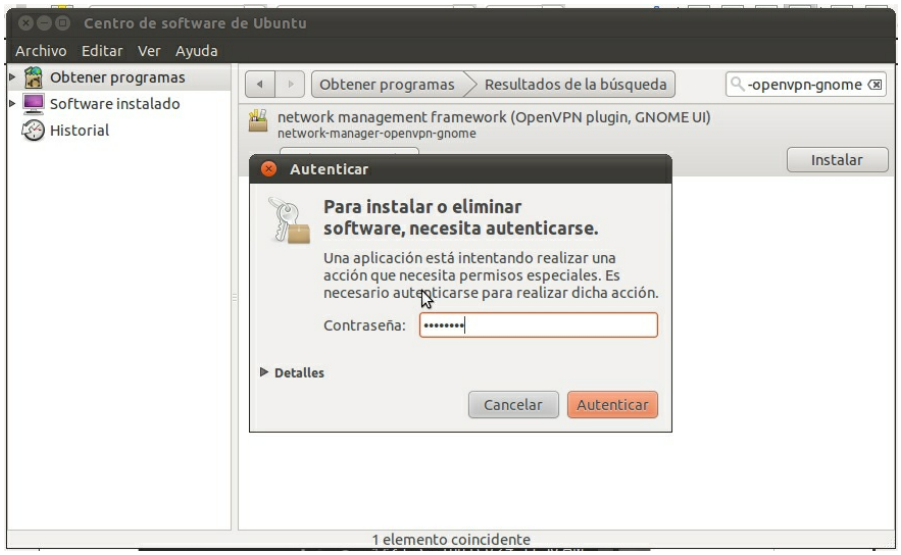
1. Abrimos el Ubuntu Software Center desde el menú de Aplicaciones ubicado en el parte superior izquierda de nuestra pantalla.

2. El Ubuntu Center Software nos permite buscar, instalar y eliminar programas en nuestra computadora. Hacemos clic en la caja de búsqueda en la parte superior derecha de la ventana.

3. En la caja de búsqueda, escribimos "network-manager-openvpn-gnome" (la extensión para NetworkManager que habilitará OpenVPN). Este paquete incluye todos los ficheros que necesitamos para establecer una conexión VPN satisfactoria, incluyendo el cliente OpenVPN. Hacemos clic en Install.

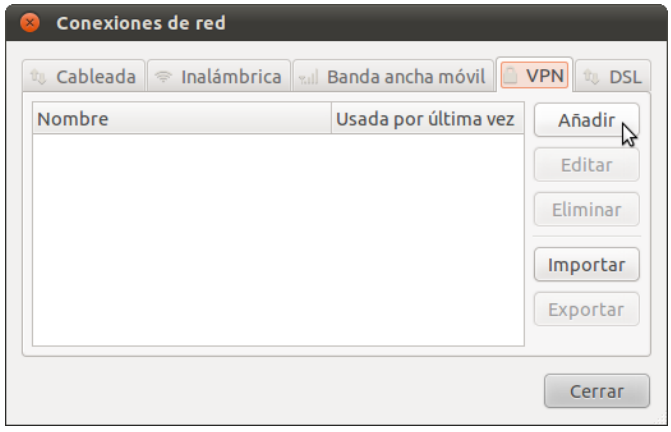


4. Ubuntu puede pedir permisos adicionales para instalar el programa. Si este es el caso, debemos teclear nuestra contraseña y hacer clic en Authenticate. Una vez que el paquete esté instalado, podemos cerrar la ventana del Software Center.



5. Para chequear que el cliente OpenVPN está correctamente instalado, hacemos clic en el NetworkManager (el icono a la izquierda de nuestro reloj de sistema) y seleccionamos VPN Connections > Configure VPN.

6. Hacemos clic en Add bajo la pestaña VPN.

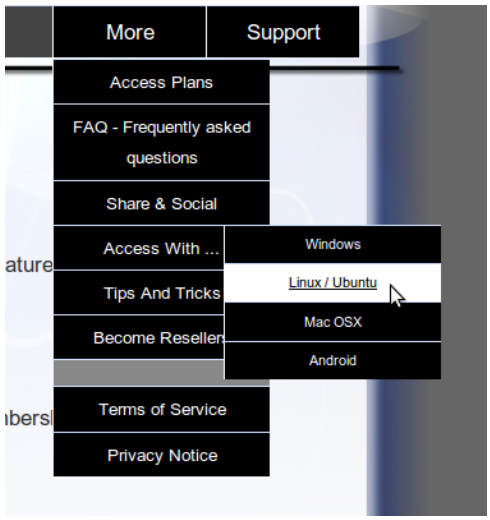


7. Si vemos una opción OpenVPN esto significa que tenemos instalado el cliente OpenVPN en Ubuntu correctamente. Hacemos clic en Cancel y cerramos el NetworkManager.

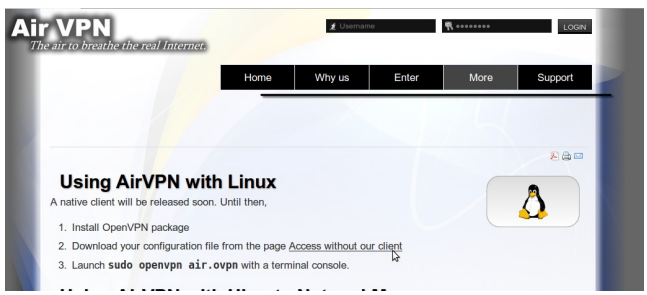
Registrando una cuenta AirVPN

AirVPN (http://www.airvpn.org) es un servicio gratis, pero tenemos que registrarnos en su sitio para poder descargar los ficheros de configuración para nuestra conexión VPN.

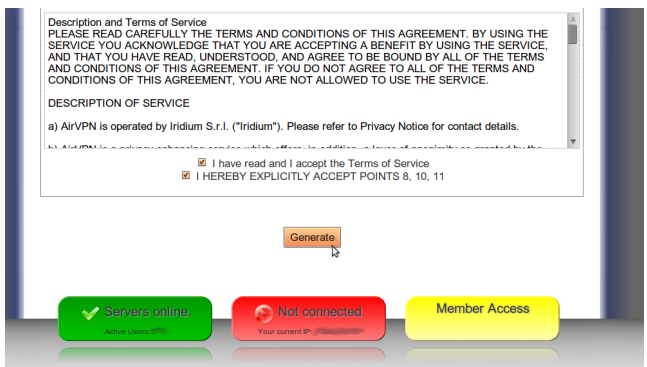
1. Vamos a la página https://airvpn.org/?option=com_user&view=register y nos registramos en una cuenta gratis. Debemos asegurarnos de escoger una contraseña fuerte, pues esa será también nuestra contraseña para el acceso VPN. (para ver algunos consejos sobre contraseñas fuertes, podemos ver el capítulo “Amenazas y evaluación de amenazas” en este libro).
2. En el menú de navegación del sitio de AirVPN, seleccionamos More > Access with... > Linux/Ubuntu.



3. Hacemos clic en “Access without our client”. Se nos pedirá el nombre de usuario y la contraseña que usamos para registrarnos.



4. Seleccionamos el modo VPN que queremos configurar en NetworkManager (para nuestro ejemplo usamos "Free - TCP - 53") y dejamos el resto de las opciones como están. Debemos asegurarnos de chequear el acuerdo de Términos de Servicios al pie de la página, y hacemos clic en Generate.

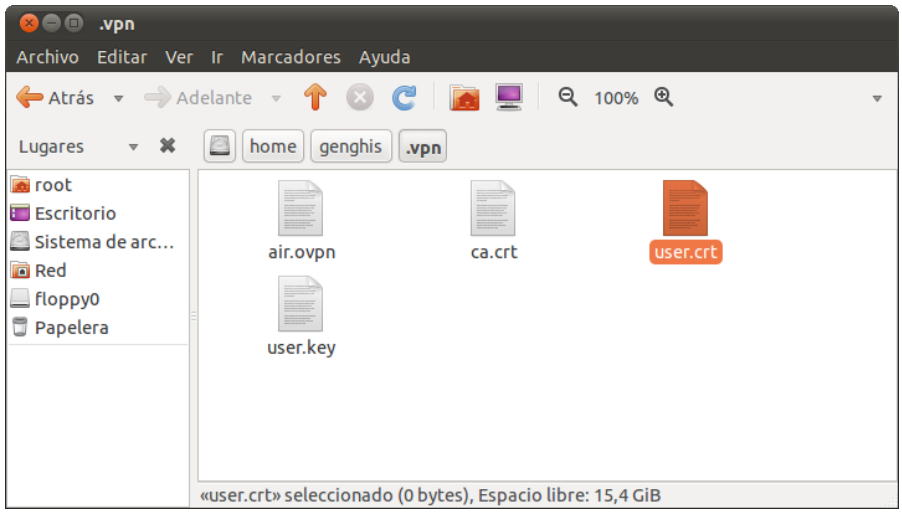


5. Una ventana nos dejará saber que el fichero air.zip está listo para descargarse. Este contiene los ficheros de configuración y las credenciales que necesitamos para conectarnos a VPN. Hacemos clic en OK.

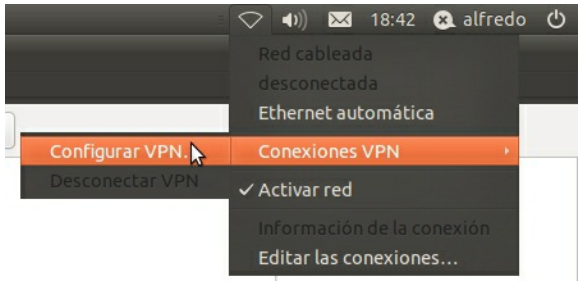
Configurando AirVPN en NetworkManager

Ahora que ya tenemos nuestros ficheros de configuración y nuestras credenciales, podemos configurar NetworkManager para conectarnos al servicio AirVPN.

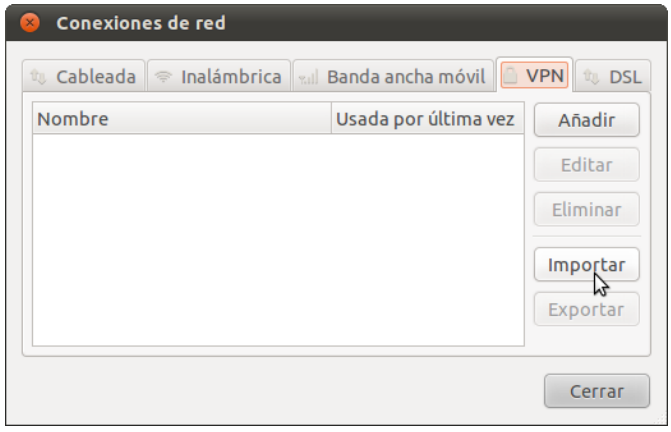
1. Descomprimimos el fichero que descargamos en una carpeta del disco duro (e.g. "/home/[yourusername]/.vpn"). debemos tener cuatro ficheros. El fichero "air.ovpn" es el fichero de configuración que necesitamos importar dentro de NetworkManager.



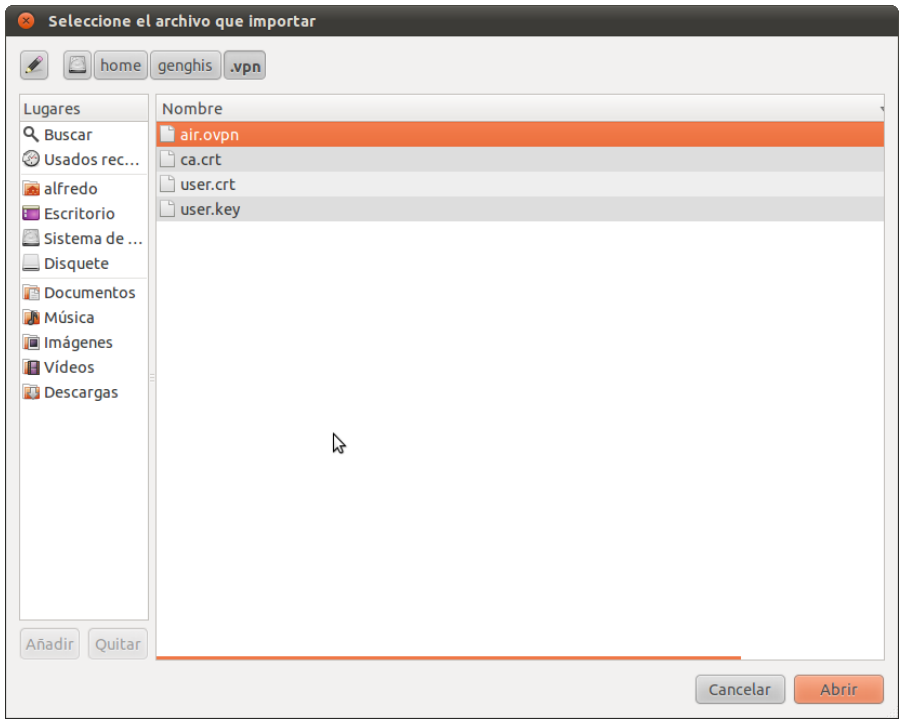
2. Para importar el fichero de configuración, abrimos NetworkManager y vamos a VPN Connections > Configure VPN.



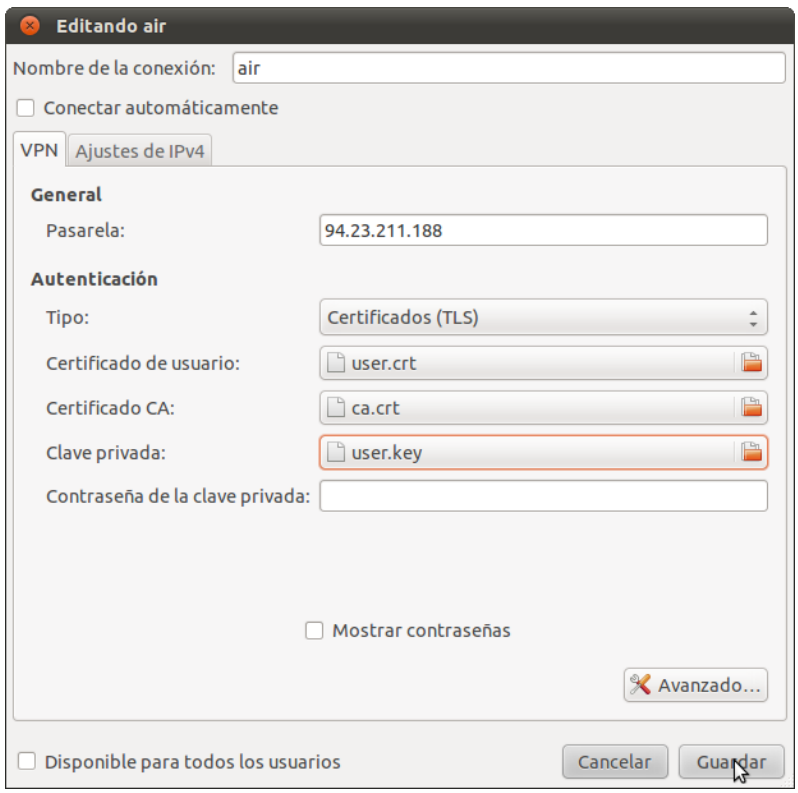
3. Bajo la pestaña VPN, clic en Import.



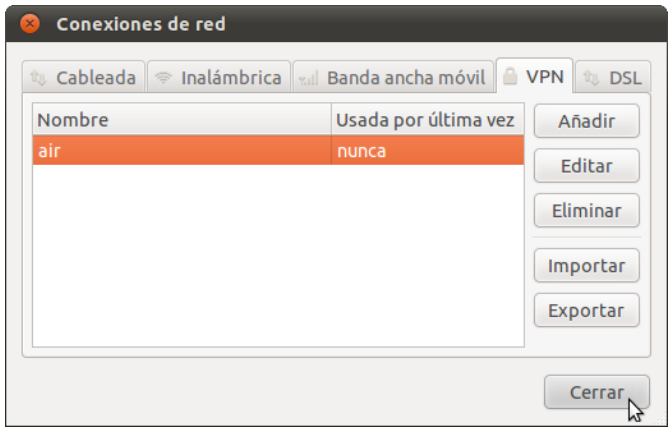
4. Localizamos el fichero air.ovpn que ya des compactamos. Clic en Open.



5. Una nueva ventana se abre. Dejamos todo como está y hacemos clic en Apply.



6. ¡Enhorabuena! Nuestra conexión VPN está lista para usarse y debe aparecer en la lista de conexiones bajo la pestaña VPN. Ahora ya podemos cerrar NetworkManager.

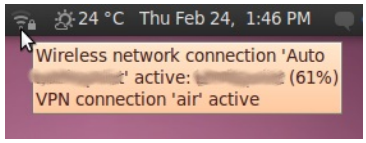


Usando nuestra nueva conexión VPN

Ahora que ya configuramos NetworkManager para conectarnos a un servicio VPN usando el cliente OpenVPN, podemos usar nuestra nueva conexión VPN para evadir la censura de Internet. Para comenzar sigamos estos pasos:

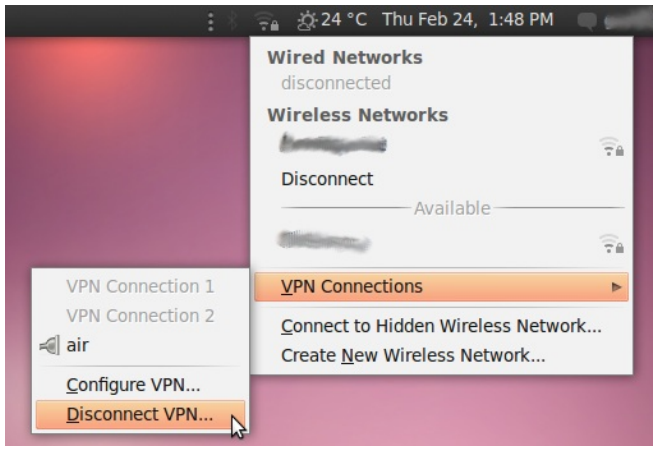
1. En el menú de NetworkManager, seleccionamos nuestra nueva conexión desde VPN Connections.

2. Esperamos que la conexión VPN se establezca. Cuando se conecte, un candado pequeño debe aparecer muy cerca del icono de NetworkManager, indicando que estamos usando ahora una conexión segura. Movemos el cursor sobre el icono para confirmar que la conexión VPN está activa.



3. También podemos chequear el estado de nuestra conexión visitando http://www.ipchicken.com. Este verificador de IP gratis debe confirmarnos que estamos usando un servidor airvpn.org.

4. Para desconectarnos de nuestro VPN, seleccionamos VPN Connections > Disconnect VPN en el menú de NetworkManager. Ahora estaremos usando de nuevo nuestra conexión normal.


24 °C Thu Feb 24, 1:48 PM
Wired Networks
disconnected
Wireless Networks
Disconnect
Available
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 es una solución VPN gratis (pero comercial) disponible para Microsoft Windows y Mac OS, que puede usarse para acceder a contenido sin censurar en Internet a través de un túnel seguro (sobre nuestra conexión a Internet censurada).

Hotspot Shield cifra toda nuestra comunicación, de manera que el software de vigilancia de nuestro censurador no pueda ver qué sitios accedemos.

INFORMACIÓN GENERAL

Sistemas operativos que soporta	
Localización	Inglés
Sitio Web	https://www.hotspotshield.com
Soporte	FAQ: https://www.anchorfree.com/support/hotspot-shield.html E-mail: support@anchorfree.com

CÓMO OBTENER HOTSPOT SHIELD

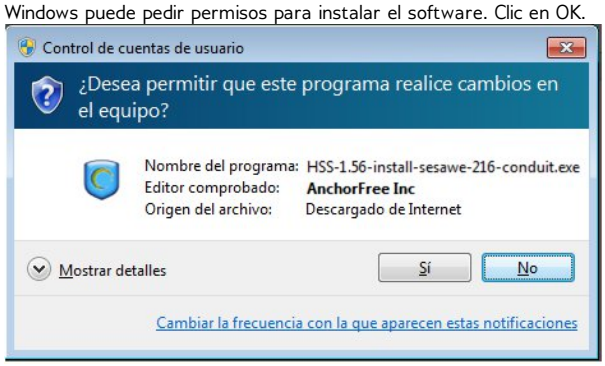
Podemos descargar el programa desde https://www.hotspotshield.com. El tamaño del fichero es cerca de 6 MB, así que en una conexión dial-up lenta demorará 25 minutos o más. Si la descarga está bloqueada donde tratamos de accederla, escribimos a la dirección hss-sesawe@anchorfree.com e incluimos al menos una de estas palabras en el asunto del correo electrónico: "hss", "sesawe", "hotspot" o "shield". Recibiremos el instalador en un adjunto.

Importante: Si estamos usando Firefox con la extensión NoScript habilitada, podemos experimentar algunas cuestiones intentando usar Hotspot Shield. Es bueno asegurarnos de que todas las URLs a las que se conecta Hotspot Shield están en lista blanca, o que temporalmente permitimos los scripts globalmente mientras usamos este servicio.

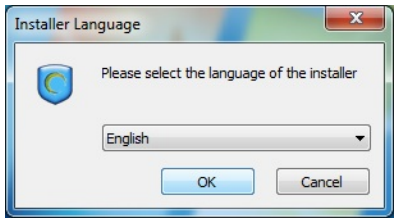
Instalando Hotspot Shield

1. Después de una descarga satisfactoria, localizamos el fichero descargado en nuestra computadora y comenzamos la instalación haciendo doble clic en el ícono.

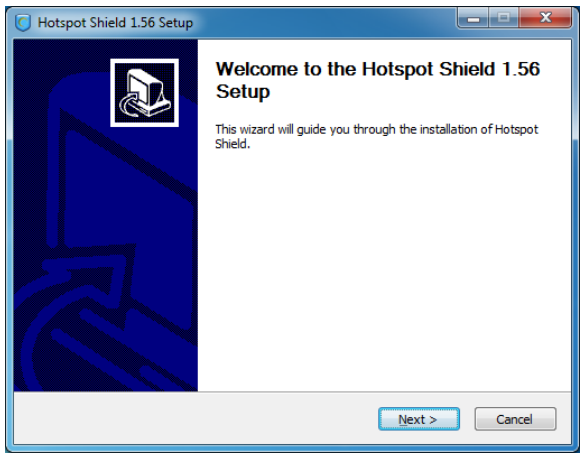
2. Windows puede pedir permisos para instalar el software. Clic en OK.



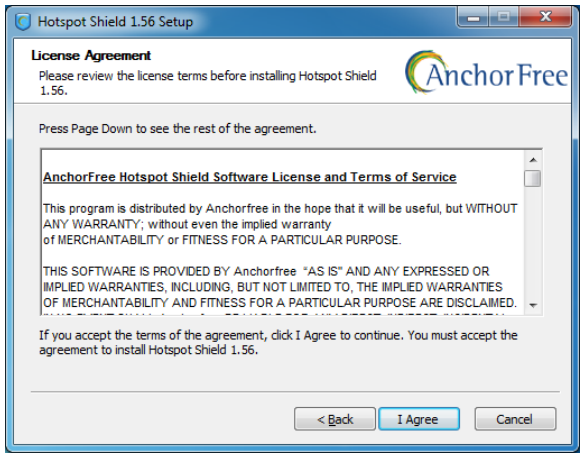
3. Seleccionamos el idioma de preferencia del menú desplegable.



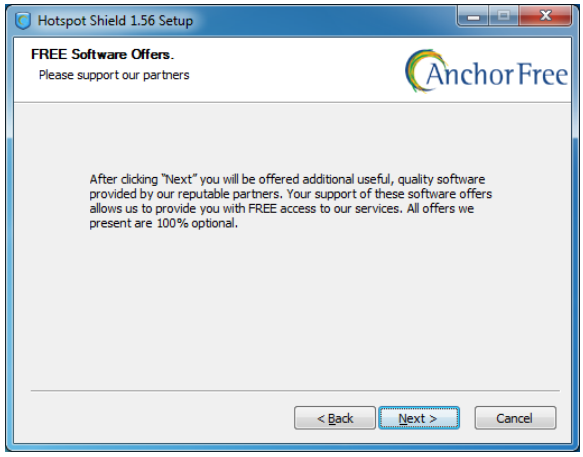
4. Después que seleccionemos el idioma, veremos una página de bienvenida. Clic en Próximo.



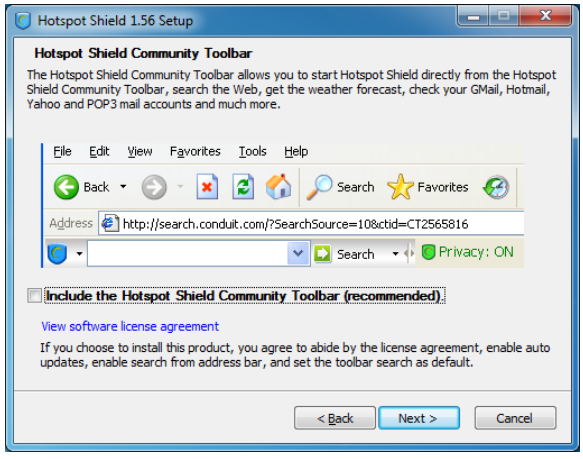
5. Aceptamos el acuerdo de licencia haciendo clic en “Estoy de acuerdo...”.



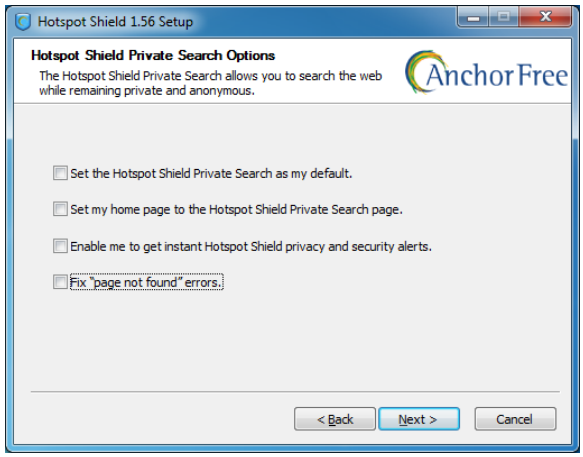
6. Veremos una ventana informando sobre algunos programas adicionales que podemos instalar opcionalmente. Clic en Próximo.



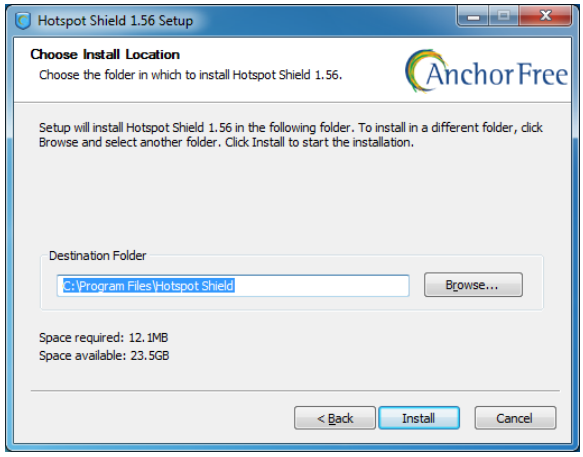
7. En la próxima ventana podemos desmarcar la opción de instalar la Barra Hotspot Shield opcional. Esta característica no es necesaria para ejecutar Hotspot Shield.



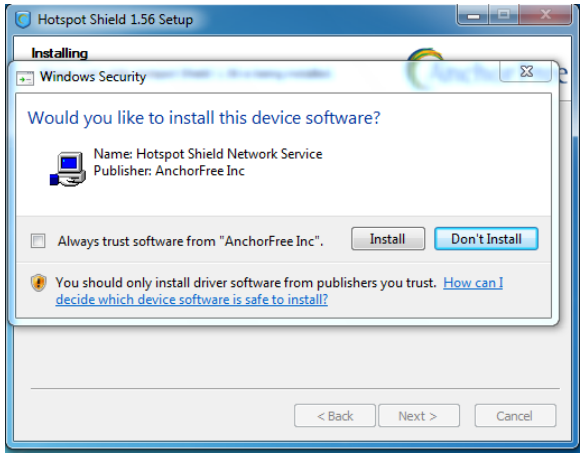
8. Las opciones adicionales se presentarán en la próxima ventana. Todas son opcionales, y no las necesitamos para ejecutar Hotspot Shield.



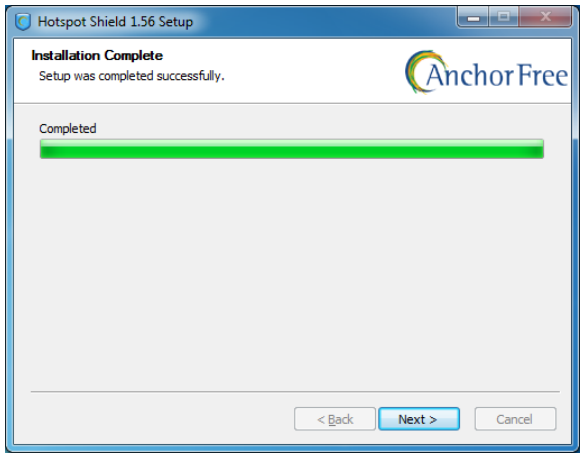
9. Seleccionamos el lugar donde queremos instalar Hotspot Shield. En la mayoría de los casos podemos dejar los valores por defecto y clic en Install.



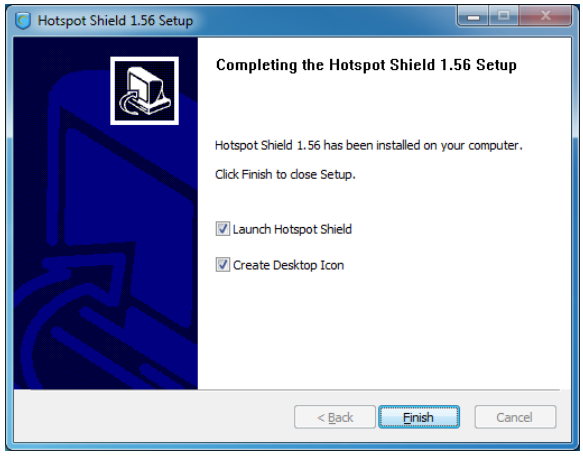
10. Windows puede solicitarnos permisos adicionales varias veces para instalar diferentes componentes de Hotspot Shield. Podemos proceder de seguro haciendo clic en Install todas las veces.



11. Cuando se haya completado la instalación, hacemos clic en Próximo.



12. Finalmente, podemos abrir Hotspot Shield inmediatamente después de la instalación y podemos crear un icono en nuestro escritorio. Seleccionamos nuestras preferencias y hacemos clic en Finish.

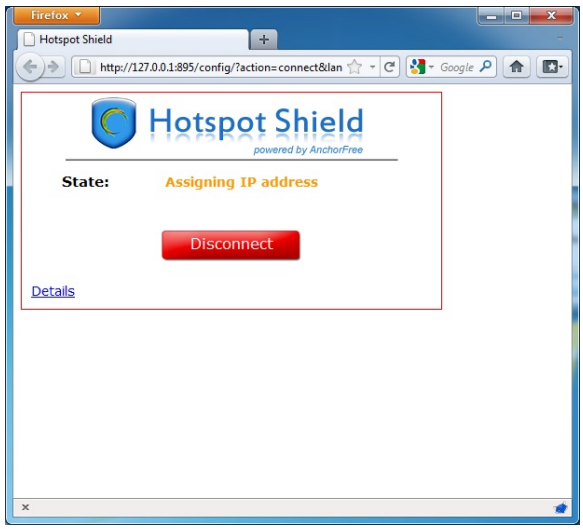


Hotspot Shield está instalado ahora en nuestra computadora.

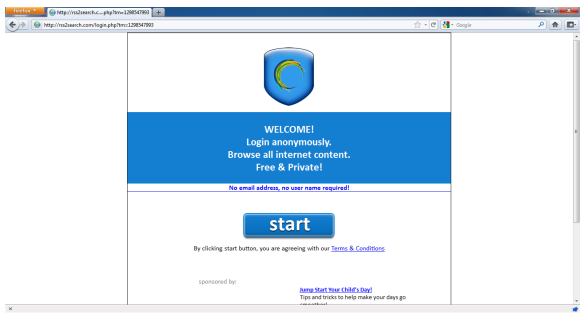
Conectándose al servicio Hotspot Shield

1. Hacemos clic en el icono de Hotspot Shield en el escritorio o en el menú Programas > Hotspot Shield.

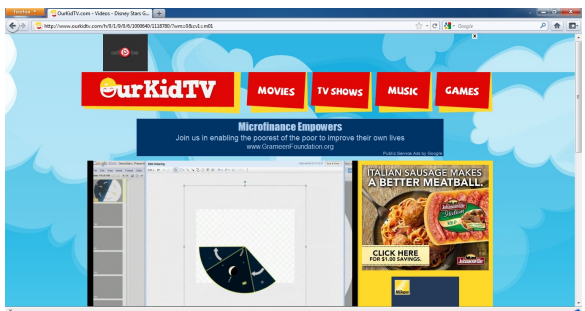
2. Una vez que abrimos Hotspot Shield, una ventana de navegador se abrirá con una página de estado mostrando diferentes estados de intentos de conexión, como "Authenticating" y "Assigning IP address".



3. Una vez conectados, Hotspot Shield nos redireccionará a una página de bienvenida. Hagamos Clic en Start para comenzar a navegar.

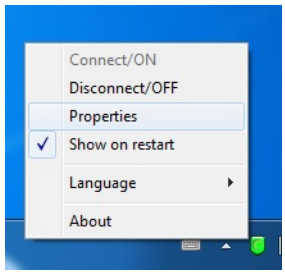


4. Es necesario notar que después que hacemos clic en Start, Hotspot Shield nos puede redireccionar a una página de publicidad como la que se muestra debajo. Podemos cerrar esta pestaña e iniciar la navegación Web como siempre. Podemos chequear que estamos conectados al servicio de Hotspot Shield buscando en el icono de Hotspot Shield que aparece en la barra de sistema (cerca del reloj).



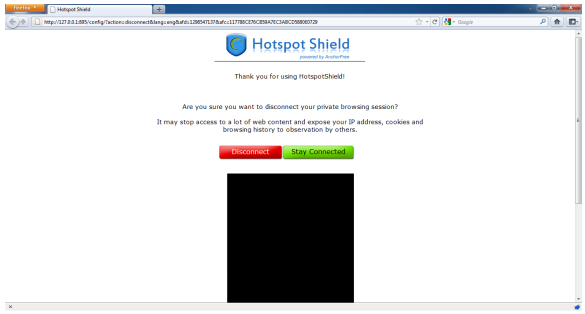
5. Para chequear el estado de nuestra conexión, simplemente hacemos clic derecho en el

icono de Hotspot Shield en la barra de sistema y seleccionamos Propiedades.



Desconectándose del servicio Hotspot Shield

1. Para desconectarnos del servicio Hotspot Shield hacemos clic derecho en el icono de la barra del sistema (vea la imagen anterior) y seleccionamos Disconnect/OFF.
2. Hotspot Shield nos pedirá que confirmemos esta acción. Clic en Disconnect.



3. Una ventana de estado aparecerá confirmando que estamos desconectados y navegando por nuestra conexión (filtrada) normal. Hacemos clic en el botón “CONNECT” para comenzar a evadir la censura.

23. ALKASIR

Alkasir es una herramienta innovadora cliente/servidor que facilita el análisis, y la evasión de la censura de sitios Web (filtrado). Alkasir es mayormente usado en la región del Medio Oriente pero puede ser usada globalmente.

Utiliza un programa cliente dedicado y sustentado por servidores proxis. Su característica innovadora es mantener la lista de sitios bloqueados actualizada haciendo actualizaciones semi-automáticas, y permite reportar nuevos sitios bloqueados a través de la comunidad de usuarios distribuida globalmente.

INFORMACIÓN GENERAL

Sistemas operativos que soporta	
Localización	Inglés y *Árabe*
Sitio Web	https://alkasir.com
Ayuda	https://alkasir.com/help
FAQ	https://alkasir.com/faq
Contacto	https://alkasir.com/contact

¿CÓMO FUNCIONA ALKASIR?

Alkasir ha implementado dos nuevas características innovadoras y complementarias. Se ha diseñado como un navegador Web (basado en Mozilla Firefox) con un proxy HTTP embebido y pre-configurado, y una base de datos de autoaprendizaje con URLs bloqueadas.

Evadiendo la censura de Internet

La innovación es que Alkasir solo depende de su base de datos de URLs bloqueadas y su proxy embebido para alcanzar esas URLs bloqueadas. Las URLs no bloqueadas son accedidas directamente, sin solicitudes de proxy. Usando proxy HTTP solo cuando realmente necesita optimizar el uso del ancho de banda y permite acceder a las páginas Web más rápidamente (pues las páginas Web que se acceden directamente cargan más rápido).

Mantener actualizada la base de datos de URLs

Cuando un usuario sospeche que una URL este bloqueada, puede reportarla a través del programa. Alkasir chequea el reporte minuciosamente, y pregunta al moderador del país (una persona) para que apruebe la adición en la base de datos (para mantener la lista adecuada y evitar que entren contenidos indeseables, como la pornografía).

Una sola “unidad de contenido bloqueado” (un sitio Web bloqueado en un país determinado) a menudo depende de más de una URL. Cuando Alkasir detecta una URL bloqueada en un país determinado, chequea todas las URLs referenciadas en esa página para determinar si alguna de ellas está bloqueada también. Así, Alkasir construye su base de datos de contenido bloqueado a través de una metodología simple, primitiva y de un nivel de rastreo.

Finalmente, el cliente detecta cuando no puede cargar una URL directamente (i.e. no a través del proxy) y automáticamente chequea si es una URL bloqueada nueva (aún no está en la base de datos) y si lo es la adiciona automáticamente.

La base de datos está disponible en la siguiente dirección: https://alkasir.com/map.

Para resumir, la base de datos de URLs bloqueadas de Alkasir es continuamente alimentada por los usuarios Alkasir (usando propuestas humanas o reportes automáticos) y el navegador depende de esta base de datos para optimizar la reactividad de las herramientas globales tramitando solo las solicitudes de URLs bloqueadas a través del proxy.

¿CÓMO OBTENER ALKASIR?

Podemos descargar Alkasir directamente desde el sitio Web o recibirlo por correo electrónico.

Descargar Alkasir por la vía del sitio Web

Podemos descargar Alkasir desde el sitio oficial, https://alkasir.com.

En dependencia del sistema operativo y los programas que tengamos, seleccionamos una de las siguientes versiones:

- Si tenemos Windows Vista o Windows 7 y Mozilla Firefox instalados, solo necesitamos el "Alkasir Installation package" (que requiere instalación, tamaño: 3MB).
- Si este no es el caso, necesitamos descargar el "Alkasir Complete Installation package" (que también requiere instalación, tamaño: 41.04 MB).

Si no podemos o no queremos instalar Alkasir permanentemente en la computadora que usamos (e.g. una computadora compartida en un cibercafé o biblioteca), podemos descargar cualquiera de las dos versiones para USB de Alkasir:

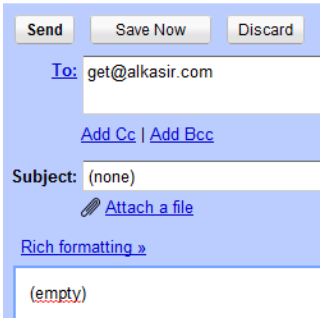
- Alkasir USB package sin Mozilla (no necesita instalación – portable – pero necesita Mozilla Firefox; tamaño: 4 MB)
- Alkasir USB package con Mozilla (no necesita instalación – portable – tamaño: 12 MB)

Es importante tener en cuenta que ambas versiones requieren que .Net Framework esté instalada, que viene pre instalada en los sistemas operativos Windows Vista y Windows 7.

Opcionalmente, podemos registrar una cuenta para recibir actualizaciones regulares y noticias de Alkasir por correo electrónico. Las actualizaciones son liberadas regularmente, así que debemos asegurarnos de tener la última versión del sitio Web oficial.

Recibir Alkasir por correo electrónico

Si el sitio Web de Alkasir está bloqueado en nuestro país, podemos obtener el fichero de instalación en un correo electrónico de respuesta automática. Simplemente enviamos un correo en blanco a la dirección get@alkasir.com solicitando el fichero de instalación en un adjunto.

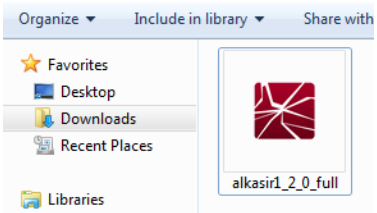


Recibiremos un correo electrónico con el software adjunto y las instrucciones para instalar Alkasir en nuestra computadora.

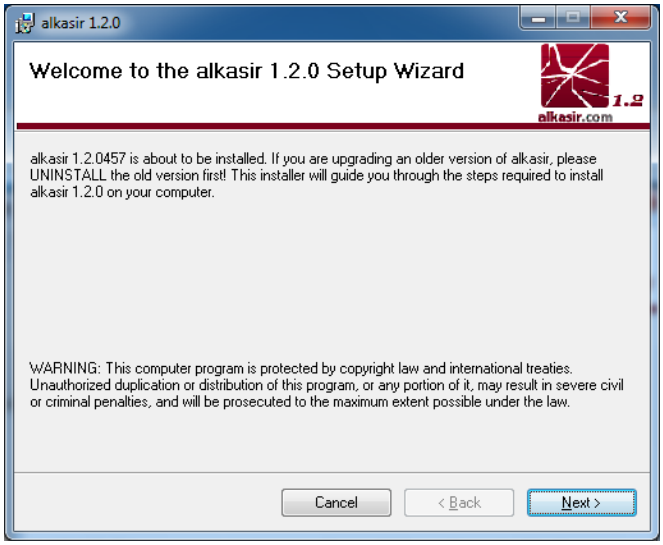
Si no recibimos el programa después de unos minutos, es posible que tengamos que adicionar get@alkasir.com a nuestra lista de contactos para que los correos no se consideren spam.

INSTALACIÓN

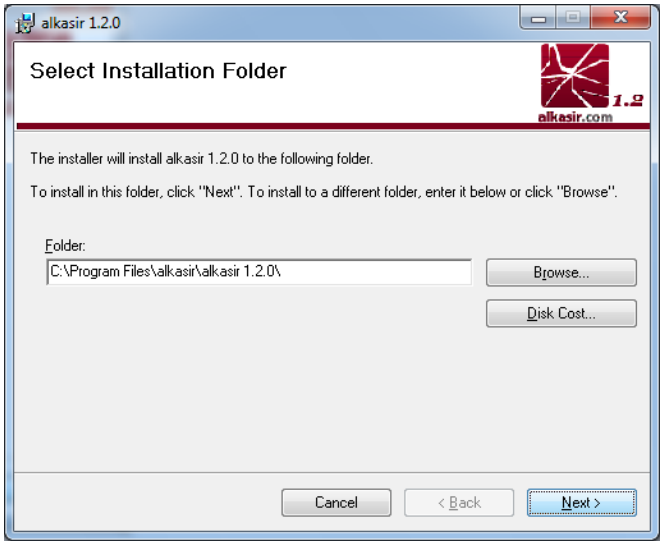
Una vez que descarguemos el fichero de instalación, hacemos doble clic en el ícono.



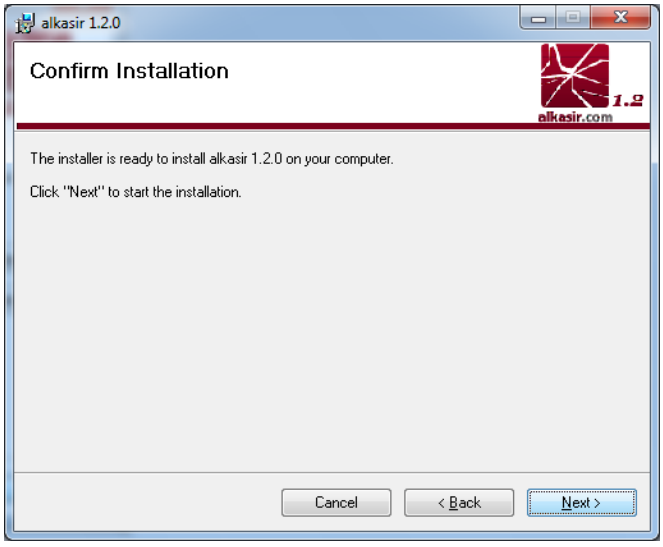
Podemos recibir un aviso de seguridad. Hacemos clic en Run o Accept.



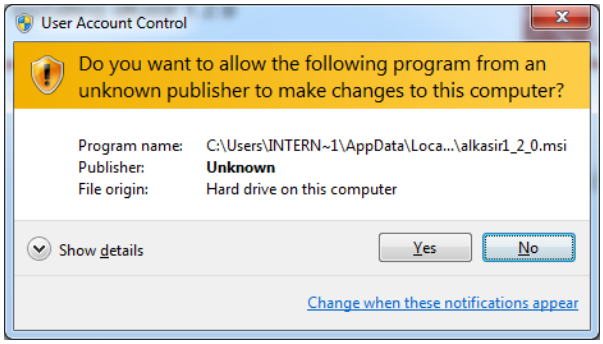
Seguimos el asistente de instalación de Alkasir haciendo clic en el botón Next.



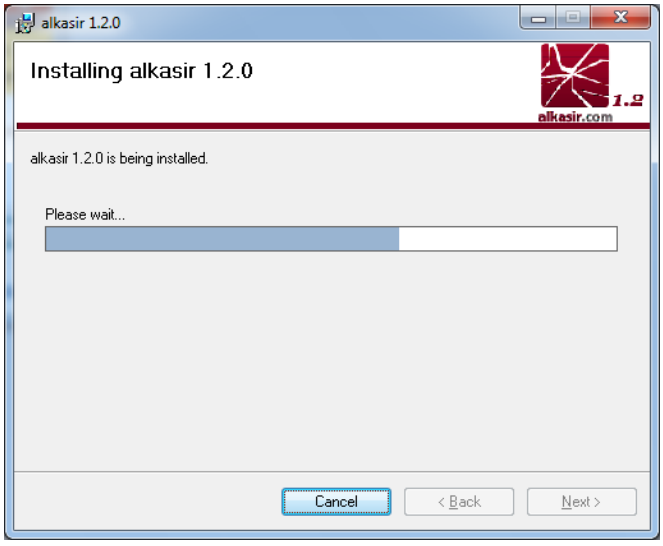
Podemos cambiar la carpeta de instalación (pero no es recomendable).

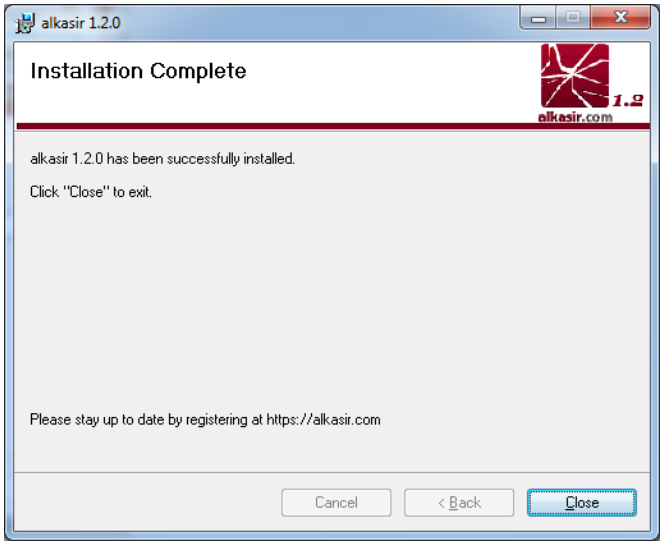


Cuando esté listo, hacemos clic en Next.



Validamos el aviso de seguridad que se muestra más abajo haciendo clic en Yes.

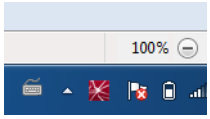




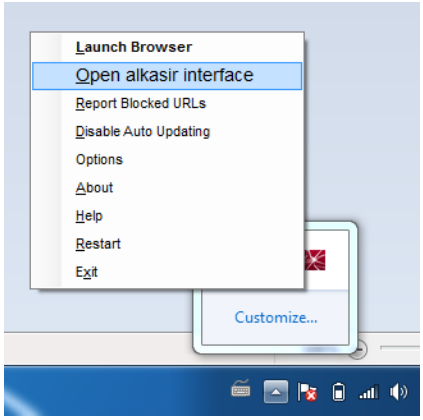
Cuando la instalación haya finalizado, clic en Close.

¿CÓMO USAR ALKASIR?

Alkasir debe iniciarse automáticamente cuando inicia Windows. Para asegurarnos que Alkasir se está ejecutando chequeamos que se muestre el ícono de Alkasir en la barra de sistema, cerca del reloj.



Si hacemos clic derecho sobre el icono veremos el menú de configuración.



- Launch browser (Iniciar el navegador)
- Open alkasir interface (Abrir la interfaz de Alkasir)
- Report bloched URLs (Reportar URLs bloqueadas)

La interfaz principal de Alakasir reúne todas las características del software. Podemos hacer lo siguiente:

- Iniciar, apagar y reiniciar el programa
- Iniciar el navegador de Alkasir
- Registrarnos en https://alkasir.com
- Descargar actualizaciones de nuestra versión de Alkasir.

Primero, iniciemos el navegador Alkasir.

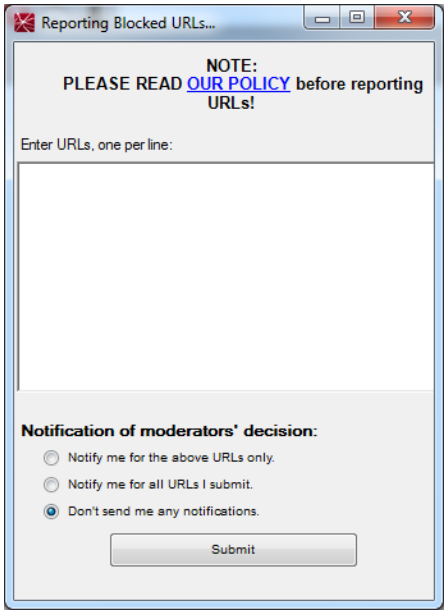
La interfaz de usuario gráfica del navegador es similar a la de Mozilla Firefox pues se basa en la misma plataforma técnica. Notemos algunas características específicas:

- Un botón para localización Árabe completa
- El botón "Report Blocked URLs", para usarlo cuando intentamos alcanzar un sitio Web que parece estar bloqueado. Este botón se muestra cerca de la barra de direcciones y la barra de estado.
- Un icono Alkasir para ir a la interfaz principal.

También podemos encontrar otros menús para integrar nuestro navegador Alkasir con nuestra cuenta Alkasir.

Es posible habilitar o inhabilitar las actualizaciones automáticas para el programa, la lista de proxies y la base de datos de sitios bloqueados.

Si arribamos a una página de error que pueda indicar un sitio Web bloqueado (como un error Acceso Denegado o error Tiempo de Conexión Agotado), podemos entrar esta URL a la base de datos de Alkasir haciendo clic en el botón Report Blocked URL. Podemos seleccionar ser notificados con la decisión del moderador (está decisión está basada en las políticas de la herramienta).



INFORMACIÓN ADICIONAL

Podemos visitar https://alkasir.com para:

- Una documentación completa del software: https://alkasir.com/help
- Una lista de preguntas frecuentes: https://alkasir.com/faq

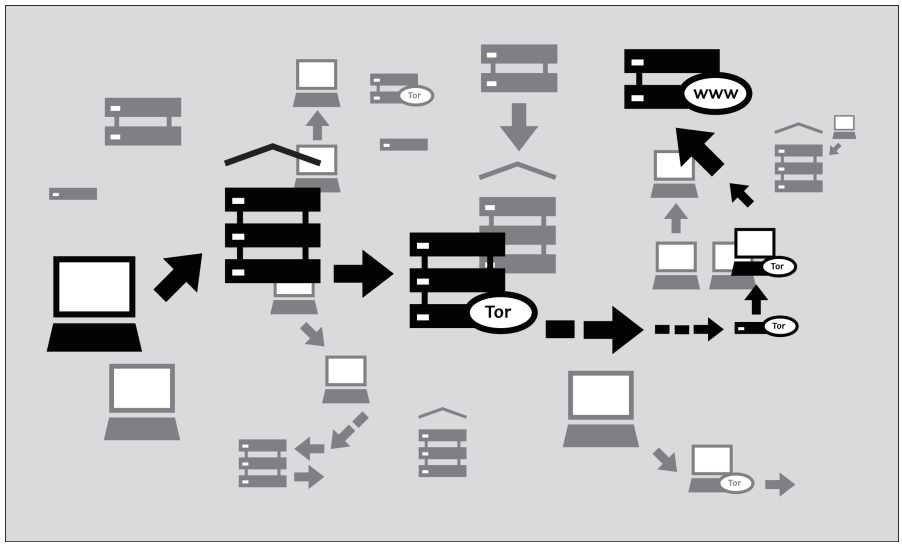
24. TOR : THE ONION ROUTER

Tor (The Onion Router) es una red muy sofisticada de servidores proxis.

INFORMACIÓN GENERAL

Sistemas operativos que soportados	
Localización	13 languages
Sitio Web	https://www.torproject.org
Soporte	Lista de distribución: 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

Cuando usamos Tor para acceder a un sitio Web, nuestras comunicaciones son enrutadas aleatoriamente a través de una red de proxis independientes y voluntarios. Todo el tráfico entre los servidores Tor (o transmisores) viaja cifrado, y cada uno de los transmisores sabe solo la dirección IP de otros dos transmisores – el inmediato anterior y el posterior en la cadena.



El objetivo es hacer difícil que nos rastreen. TOR hace bien difícil que:

- Nuestro ISP sepa qué sitio Web estamos accediendo o que información estamos enviando
- El sitio web sepa quiénes somos (al menos, saber nuestra dirección IP)
- Cualquier repetidor independiente sepa quiénes somos y a dónde vamos ya sea a través de nuestra dirección IP o relacionando nuestros hábitos de navegación observando constantemente nuestro tráfico.

¿QUÉ SE NECESITA PARA USAR LA RED TOR?

Para conectarnos a Internet a través de la red Tor y usarla para navegar anónimamente y evadir la censura, necesitamos instalar el cliente Tor en nuestro ordenador. También es posible ejecutar una versión portable del programa desde una memoria externa u otro dispositivo externo.

Tor es compatible con la mayoría de las versiones de Windows, Mac OS X y GNU/Linux.

¿CON QUÉ PROGRAMAS ES COMPATIBLE?

Tor usa una interfaz de proxy SOCKS para conectarse a las aplicaciones, de modo que todas las aplicaciones que soporten SOCKS (versiones 4, 4ª y 5) pueden tener su tráfico anónimo usando Tor, incluyendo:

- La mayoría de los navegadores
- Muchos clientes de mensajería instantánea e IRC
- Clientes SSH
- Clientes de correo electrónico

Si instalamos Tor desde el Vidalia Bundle, Tor Browser Bundle o Tor IM Browser Bundle, Tor tendrá también una aplicación proxy HTTP configurada como front-end a la red Tor. Esto permite que algunas aplicaciones que no soportan SOCKS funcionen con Tor.
Si queremos principalmente usar Tor para navegar en la web y chatear, puede ser más fácil usar Tor Browser Bundle o el Tor IM Browser Bundle que pueden proveer soluciones pre-configuradas listas para usarse. El paquete browser Tor también incluye Torbutton, que mejora la protección de la privacidad cuando usamos Tor con un navegador Web. Ambas versiones de Tor pueden descargarse desde https://www.torproject.org/projects/torbrowser.

VENTAJAS Y RIESGOS

Tor puede ser una herramienta efectiva para la evasión y la protección de la identidad.La codificación de Tor oculta el contenido de nuestra comunicación de nuestro administrador de red local, y disimula con quien nos comunicamos o qué sitios Web visitamos. Cuando se usa correctamente, brinda una mayor protección de anonimato que un proxy simple.

Pero:

- Tor es vulnerable al bloqueo. La mayoría de los nodos Tor están listados en un directorio público, así que es muy fácil para los operadores de red acceder a la lista y adicionar la dirección IP de nodos para el filtrado. (Una de las formas de evadir este bloqueo es usar uno o varios **puentes Tor**, que son nodos Tor que no están listados públicamente, específicamente para evitar el bloqueo).
- Algunos programas que podemos usar con Tor tienen problemas que pueden comprometer el anonimato. Tor Browser Bundle viene con una versión de Firefox con Torbutton instalado. Torbutton inhabilita algunos plugins y cambia las huellas de nuestro navegador para que se parezca a cualquier otro usuario de Torbutton. Tor no nos protege si no configuramos nuestras aplicaciones para que se ejecuten a través de Tor. Algunos plugins y scripts ignoran las configuraciones de proxis locales y pueden revelar nuestra dirección IP.
- Si no estamos usando cifrado adicional para proteger nuestras comunicaciones, nuestros datos será decodificados una vez que alcancen el último nodo Tor de la cadena (llamado **nodo salida**). Esto significa que nuestros datos serán potencialmente visibles al dueño del último nodo, al ISP entre ese nodo y al sitio Web destino.

Los desarrolladores de Tor han pensado mucho acerca de estos y otros riesgos y hacen estas advertencias:

1. Tor no ofrece protección si no se usa *correctamente*. Lea la lista de advertencias aquí: https://www.torproject.org/download/download.html.en#warning y es necesario asegurarse de seguir las instrucciones para cada plataforma con cuidado: https://www.torproject.org/documentation.html.en#RunningTor
2. Incluso si se configura y se usa Tor correctamente, existen ataques potenciales que pueden comprometer la habilidad de Tor de protección: https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#Whatattacksremainagainstonionrouting
3. *Ningún sistema de anonimato es perfecto en estos días*, y Tor no es la excepción: no se debe confiar solamente en la red Tor si realmente necesitamos el anonimato.

USANDO EL TOR BROWSER BUNDLE

Tor Browser Bundle nos permite usar Tor en Windows, OS X o GNU/Linux sin tener que configurar un navegador Web. Incluso mejor, es además una aplicación portable que se puede ejecutar desde una memoria USB externa, lo que permite llevarlo a cualquier computadora sin instalarlo en cada disco duro.

DESCARGANDO EL TOR BROWSER BUNDLE

Podemos descargar Tor Browser Bundle desde el sitio Web torproject.org, como un fichero simple o versión “en fragmentos” con múltiples ficheros. Si nuestra conexión a Internet es lenta y poco fiable, la versión en partes puede ser mejor que descargar un solo fichero grande.

Si el sitio Web torproject.org está filtrado donde estamos, podemos teclear “tor mirrors” en nuestro motor de búsqueda Web favorito; los resultados probablemente incluirán algunas direcciones alternativas para descargar Tor Browser Bundle.

Obtener Tor a través de correo electrónico: enviamos un correo electrónico a gettor@torproject.org con "help" en el cuerpo del mensaje, y recibiremos las instrucciones de cómo nos pueden enviar Tor.

Precaución: Cuando descargamos Tor Browser Bundle (versiones planas o fragmentadas), debemos chequear las firmas de los ficheros, especialmente si descargamos los ficheros desde un sitio espejo. Este paso nos asegura que los ficheros no hayan sido manipulados. Para saber más sobre ficheros de firma y como chequearlos podemos leer: https://www.torproject.org/docs/verifying-signatures.

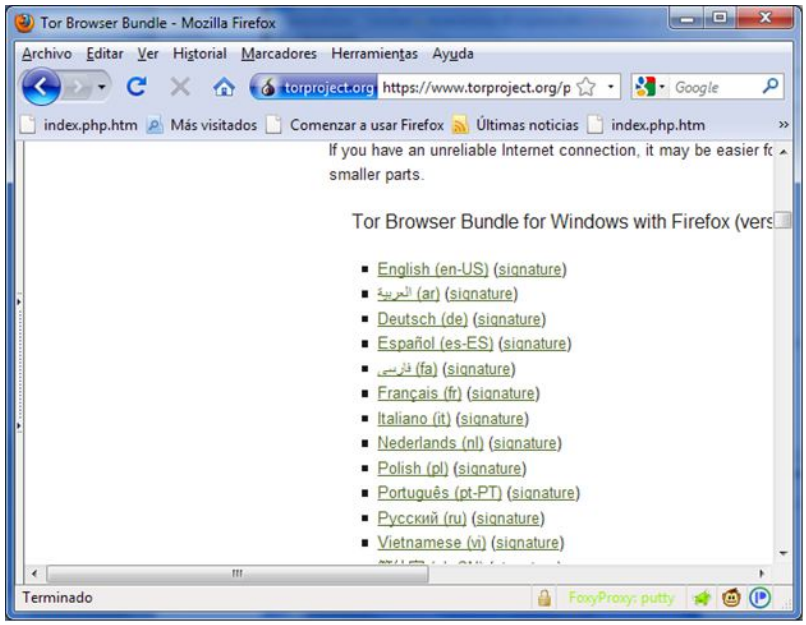
Podemos descargar el programa GnuPG que necesitaremos para chequear la firma aquí: http://www.gnupg.org/download/index.en.html#auto-ref-2.

Las instrucciones más abajo explican la instalación de Tor Browser en Windows. Si usamos un sistema operativo diferente, podemos dirigirnos al sitio Web de Tor para enlaces de descarga e instrucciones.

Instalando desde un solo fichero

1. En nuestro navegador, entramos la URL de descarga para Tor Browser: https://www.torproject.org/projects/torbrowser

2. Hacemos clic en el enlace de nuestro idioma para descargar el fichero de instalación.



3. Doble clic el fichero .exe que hemos descargado. Aparece una ventana "7-Zip self-extracting archive".

1. Seleccionamos la carpeta en la que deseamos extraer los ficheros y hacemos clic en Extract.

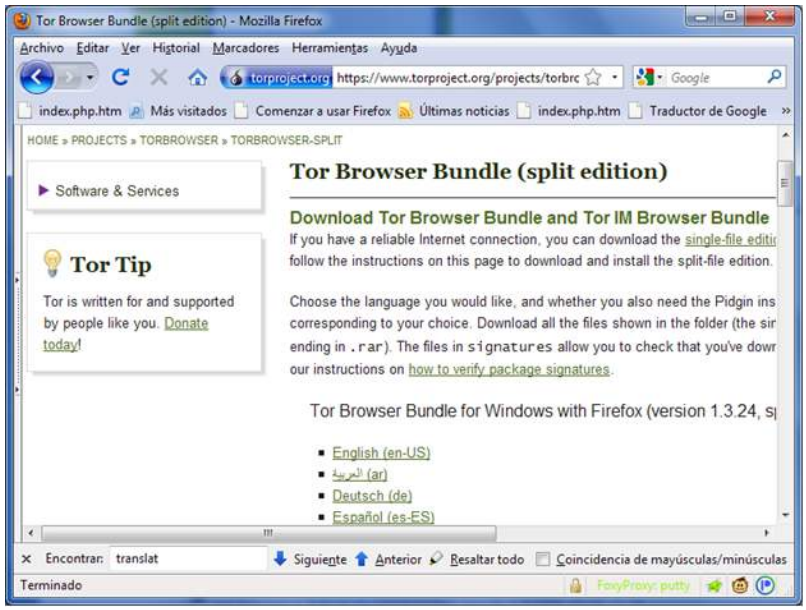
   Nota:podemos escoger extraer los ficheros directamente en una memoria externa USB si queremos usar Tor Browser en diferentes computadoras (por ejemplo en computadoras de cibercafés).

2. Cuando se complete la extracción, abrimos la carpeta y chequeamos que el contenido coincida con la siguiente imagen:

   Para limpiar, eliminamos el fichero .exe que descargamos originalmente.

Instalando desde ficheros fragmentados

1. En nuestro navegador Web, entramos la URL de la versión fragmentada de Tor Browser Bundle (https://www.torproject.org/projects/torbrowser-split.html.en), y hacemos clic en el enlace de nuestro idioma para ir a la página como se muestra a continuación:



2. Hacemos clic en cada fichero que descargamos (uno termina en .exe y otros nueve terminan en .rar), uno tras otro, y los salvamos en una carpeta del disco duro.
3. Hacemos doble-clic en la primera parte (el fichero que termina en ".exe"). Este ejecuta un programa que une todas las partes. "Split installer for Tor Browser Bundle"

"Split installer for Tor Browser Bundle" src="static/CircumventionTools-InstallingTor-tor_winrar_2-en.png" height="384" width="562">

4. Seleccionamos una carpeta donde deseemos instalar los ficheros, y hacemos clic en "Install". El programa muestra mensajes acerca del progreso mientras se ejecuta, y después se cierra.
5. Cuando se completa la extracción, se abre la carpeta para chequear que el contenido coincida con la siguiente imagen:

6. Para limpiar todo, eliminamos todos los ficheros que descargamos originalmente.

USANDO TOR BROWSER

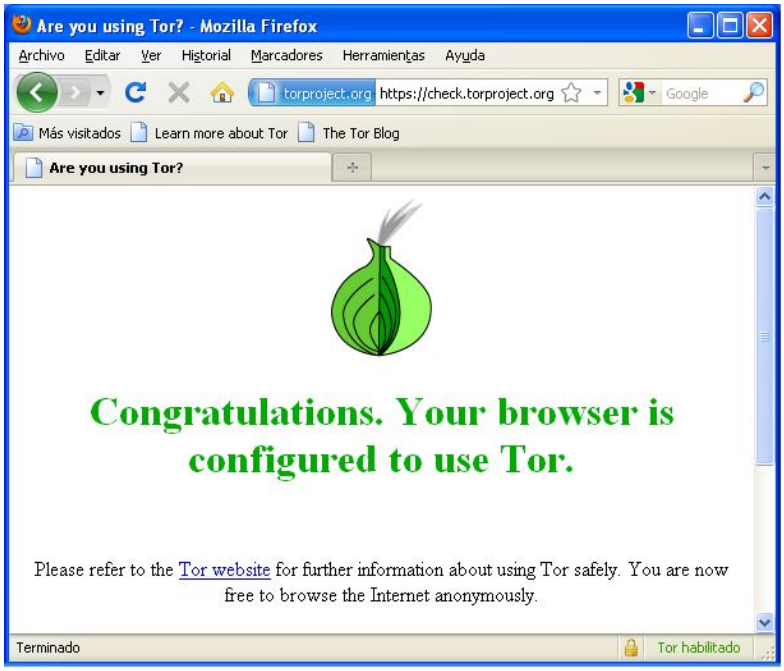
Antes de comenzar:

- Cerramos Tor. Si Tor está instalado en la computadora, debemos asegurarnos de que no se está ejecutando.

Activamos Tor Browser:

En la carpeta "Tor Browser", doble-clic "Start Tor Browser". El panel de control Tor ("Vidalia") se abre y Tor se inicia para conectarse a la red Tor.

Cuando se establece una conexión, Firefox se conecta automáticamente a la página TorCheck y confirma si está conectado a la red Tor. Esto puede tomar algún tiempo, dependiendo de la calidad de la conexión a Internet.



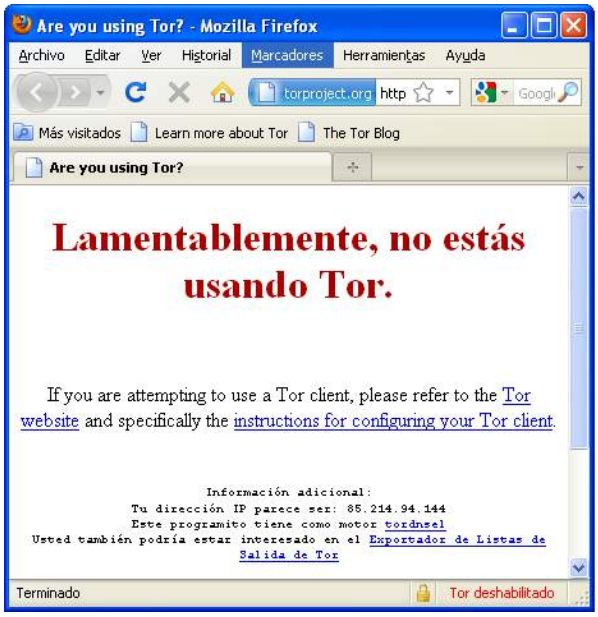
Si está conectado a la red Tor, un ícono de una cebolla verde aparece en la barra del sistema en la esquina derecha inferior de la pantalla:

NAVEGANDO EN LA WEB USANDO TOR BROWSER

Intentemos ver algunos sitios Web, y ver como se muestran. Los sitios se cargan más lentos que lo normal porque la conexión se enruta a través de varios transmisores.

SI ESTO NO FUNCIONA

Si la cebolla en el Panel de Control de Vidalia nunca se vuelve verde o si Firefox se abre, pero muestra una página diciendo "Sorry. You are not using Tor", como en la imagen de abajo, no estamos usando Tor.



Si vemos este mensaje, cerramos Firefox y Tor Browser y repetimos los pasos anteriores. Esto se puede chequear en cualquier momento para asegurarnos de que estamos usando Tor, a través de la página https://check.torproject.org/.

Si Tor Browser no funciona después de dos o tres intentos, Tor puede estar parcialmente bloqueado por nuestro ISP y debemos intentar usar un **puente de Tor** – veamos la sección más adelante "Usando Tor con Puentes".

USANDO TOR IM BROWSER BUNDLE

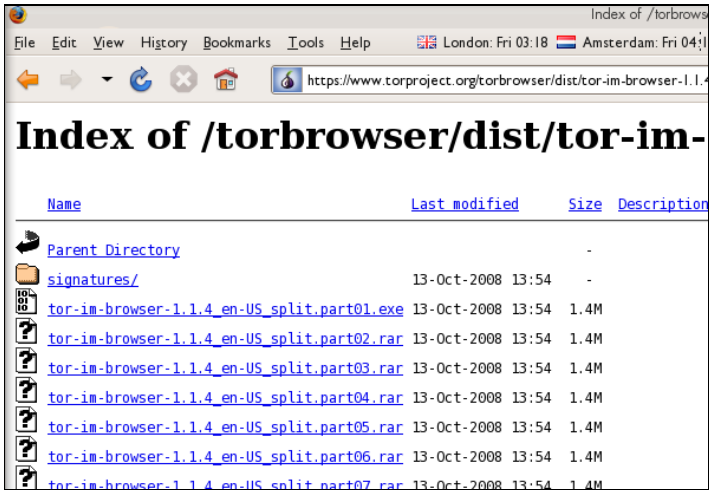
Tor IM Browser Bundle es similar a Tor Browser Bundle, pero ofrece acceso al cliente de mensajería instantánea multi-protocolo Pidgin, así que podremos chatear con encripción sobre nuestro protocolo de mensajería instantánea favorito como ICQ, MSN Messenger, Yahoo! Messenger o QQ los que deben estar filtrados seguramente.

Para aprender más acerca de Pidgin podemos buscar aquí: http://www.pidgin.im/

DESCARGANDO TOR IM BROWSER BUNDLE

Descargamos Tor IM Browser Bundle directamente desde el sitio Web Tor en https://www.torproject.org/projects/torbrowser

Si la conexión a Internet es lenta o poco confiable, podemos obtener una versión "split" (dividida) en el sitio Web torproject.org en https://www.torproject.org/projects/torbrowser-split.html.en.



AUTO-EXTRAER EL ARCHIVO

Para empezar, hacemos doble-clic en el fichero .EXE que descargamos.

Debemos ver la ventana siguiente:

- Seleccionamos la carpeta en la cual se extraerán los ficheros. Si no estamos seguros dejamos el valor por defecto. Hacemos clic en "Extract".

Nota: Se pueden extraer los ficheros directamente en una memoria USB externa si

se desea usar Tor Browser en diferentes computadoras (por ejemplo en computadoras públicas en Cibercafés).

- Cuando se completa la extracción, abrimos la carpeta recién creada y chequeamos que se vea como la siguiente imagen (Notemos la carpeta "PidginPortable"):

- Podemos borrar el fichero ".exe" que originalmente descargamos (o los distintos ficheros ".rar" y ".exe" si usamos la versión "split").

USANDO TOR IM BROWSER BUNDLE

Antes de comenzar:

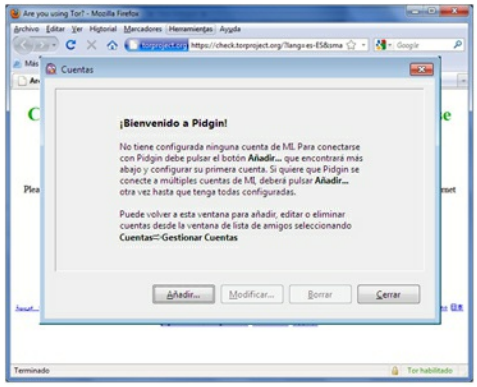
- Cerramos Firefox. Si Firefox está instalado en la computadora, debemos asegurarnos que no esté ejecutándose.
- Cerramos Tor. Si Tor está instalado en la computadora, debemos asegurarnos que no esté ejecutándose.

Activamos Tor IM Browser:

- En la carpeta "Tor Browser", doble clic "Start Tor Browser". El panel de control Tor ("Vidalia") se abre y Tor se conecta a la red Tor.

Cuando se establece una conexión:

- Una ventana de Firefox se dispara y se conecta a la página TorCheck, que debe mostrar una cebolla verde que confirma que estamos conectados con la red Tor.
- Una ventana de asistente de Pidgin (debajo) se dispara invitando a entrar la cuenta de Pidgin.



También se verá un ícono de Tor (una cebolla verde si estás conectado) y un ícono Pidgin aparecer en la barra del sistema en la esquina derecha inferior de la pantalla:

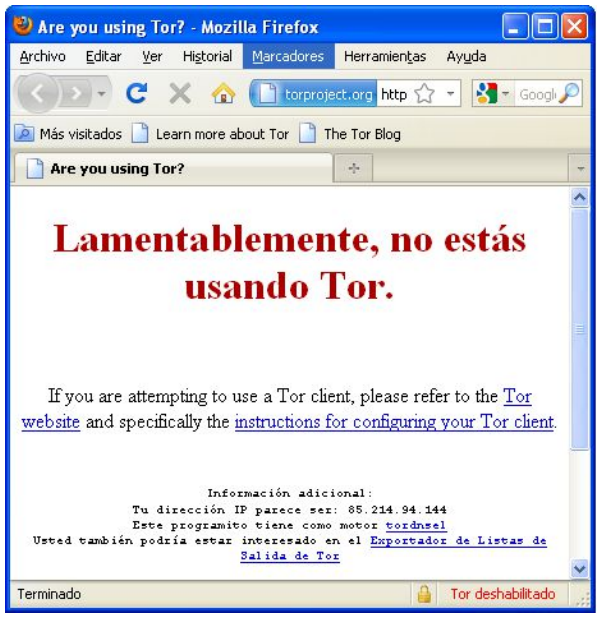
CONFIGURANDO UNA CUENTA ACCOUNT IM EN PIDGIN

Podemos configurar nuestra cuenta IM en la ventana Pidgin. Pidgin es compatible con la mayoría de los servicios IM (AIM, MSN, Yahoo!, Google Talk, Jabber, XMPP, ICQ, y otros):

Para conocer más acerca del uso de Pidgin, podemos leer:

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

SI ESTO NO FUNCIONA



Si la cebolla en el Panel de Control Vidalia no se torna verde o si se abre Firefox, pero muestra una página diciendo "Sorry. You are no using Tor", entonces debemos:

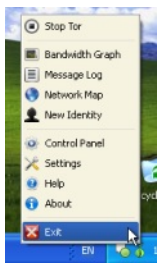
- Salir de Vidalia y Pidgin (veamos más abajo para más detalle).
- Reactivar Tor IM Browser siguiendo los pasos explicados arriba ("Usando Tor IM Browser Bundle").

Si Tor Browser aún no funciona, después de dos o tres intentos, Tor debe estar bloqueado parcialmente por nuestro ISP. Podemos dirigirnos al capítulo "Usando Tor con Puentes" de este manual e intentarlo de nuevo usando la característica puente de Tor.

SALIR DEL TOR IM BROWSER

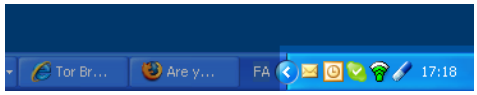
Para salir de Tor IM Browser necesitamos:

- Salir de Vidalia haciendo clic derecho en el ícono de la cebolla de la barra del sistema y seleccionar "Exit" en el menú contextual de Vidalia.



- Salir de Pidgin haciendo clic derecho en el ícono Pidgin en la barra del sistema y seleccionar "Quit" en el menú contextual de Pidgin.

Cuando el ícono cebolla de Vidalia y el ícono de Pidgin hayan desaparecido de la barra del sistema de Windows en la esquina inferior derecha de la pantalla, Tor IM Browser se habrá cerrado.



USANDO TOR CON PUENTES

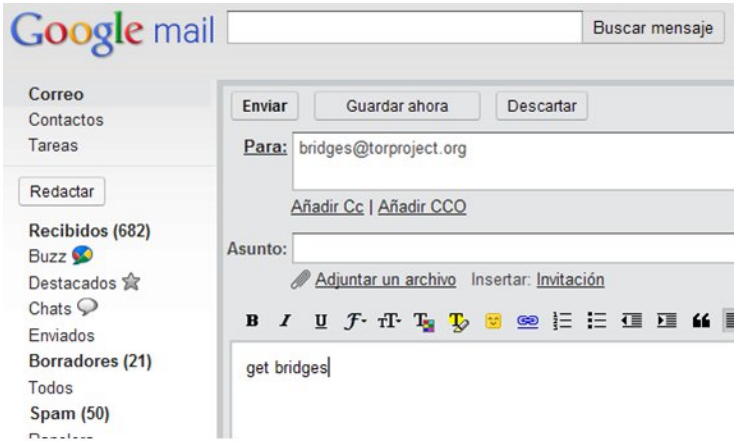
Si sospechamos que el acceso a la red Tor está bloqueado, quizás quisiéramos usar la característica **puente** de Tor. Esta característica fue creada específicamente para ayudar a las personas a usar Tor cuando lo tienen bloqueado. Debemos tener descargado e instalado el programa Tor para usar un puente.

¿QUÉ ES UN PUENTE?

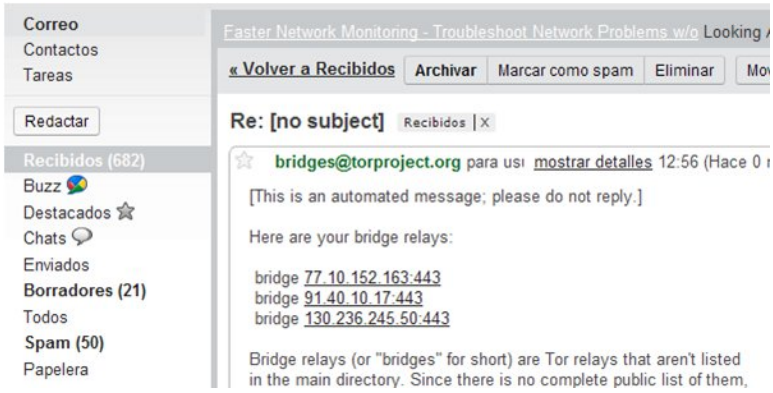
Repetidores puente (o simplemente "puentes") son transmisores que no están listados en el directorio público de Tor. Esta es una medida deliberada para impedir que estos transmisores sean bloqueados.
Incluso si nuestro ISP está filtrando las conexiones a todos los transmisores Tor públicos conocidos, quizás no es capaz de bloquear todos los puentes.

¿DÓNDE ENCONTRAR LOS PUENTES?

Para usar un puente, necesitamos localizar uno y adicionar la información en nuestra configuración de red. Una forma simple de obtener puentes es accediendo a https://bridges.torproject.org/ con nuestro navegador Web. Si ese sitio Web está bloqueado o necesitamos más puentes enviamos un correo electrónico desde una cuenta Gmail a bridges@torproject.org con la línea "get bridges" en el cuerpo del correo, (sin las comillas) en el cuerpo del mensaje.



Casi instantáneamente, recibiremos una respuesta que incluye información acerca de algunos puentes:



Notas Importantes:

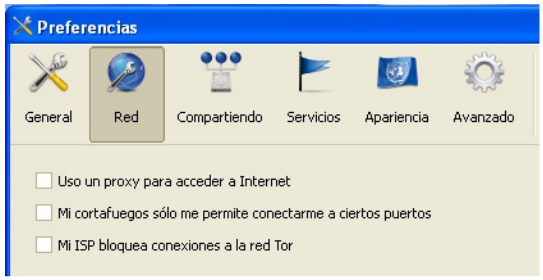
1. Es *necesario* usar una cuenta Gmail para enviar la solicitud. Si torproject.org acepta solicitudes desde otras cuentas de correo, un atacante podría crear fácilmente una gran cantidad de direcciones de correo y rápidamente conocer todo acerca de los puentes. Si no tenemos aún una cuenta Gmail, crear una solo toma unos pocos minutos.
2. Si tenemos una conexión lenta a Internet, podemos usar la dirección https://mail.google.com/mail/h/ para un acceso directo a la versión de vista básica HTML de Gmail.

ACTIVAR "BRIDGING" E INTRODUCIR LOS DETALLES DEL PUENTE

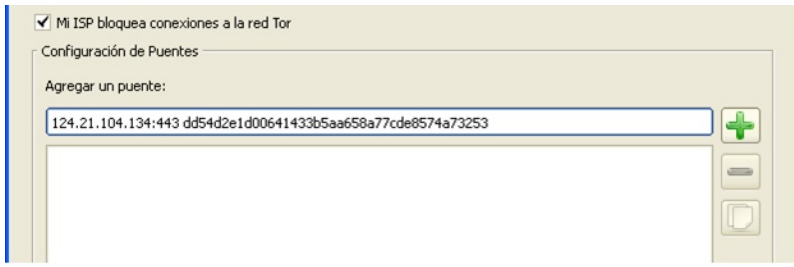
Después de obtener las direcciones para algunos puentes, debemos configurar Tor, para cualquier puente que intentemos usar:

1. Abrir el Panel de Control de Tor (Vidalia).

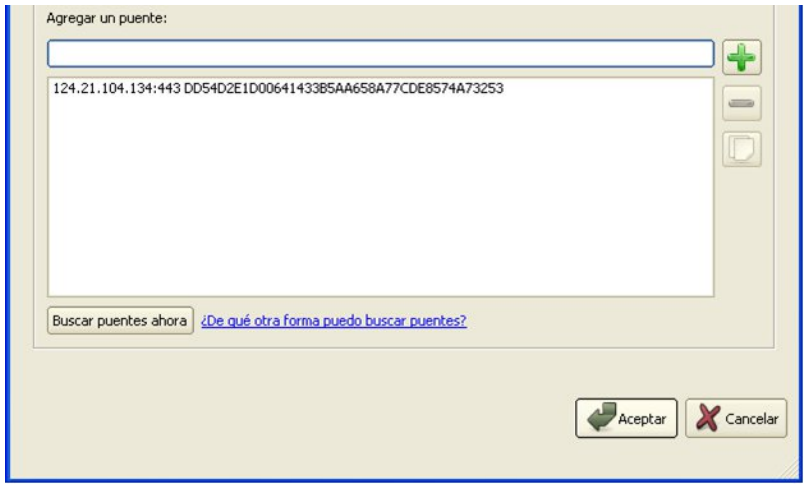
2. Hacemos clic en Preferencias. Se abre una ventana de preferencias.



3. Hacemos clic en Red.
4. Seleccionamos "Mi cortafuegos sólo me permite conectarme a ciertos puertos" y "Mi ISP bloquea conexiones a la red Tor".
5. Introducimos la información de la URL que recibimos por correo en el campo "Agregar un puente".
6. Hacemos clic en el + verde en el lado derecho del campo "Agregar un puente". La dirección URL se agrega al cuadro de abajo.



7. Hacemos clic en Aceptar en la parte inferior de la ventana para validar la nueva configuración.



8. En el panel de control de Tor, detenemos y reiniciamos Tor para usar nuestra nueva configuración.

Nota:

Añadimos tantas direcciones de puentes como podamos. Los puentes adicionales aumentan la fiabilidad. Un puente es suficiente para alcanzar la red Tor, sin embargo, si tenemos sólo un puente y este se bloquea o deja de funcionar, seremos eliminados de la red Tor hasta que agreguemos nuevos puentes.

Para añadir más puentes en nuestra configuración de red, repetimos los pasos anteriores con la información de los puentes adicionales que hemos recibido del mensaje de correo bridges@torproject.org

25. JONDO

JonDo comenzó como un proyecto universitario alemán llamado Java Anon Proxy (JAP) y se ha convertido en una herramienta de anonimato robusta que, como Tor, envía el tráfico a través de varios servidores independientes.

A diferencia de Tor, sin embargo, la red JonDo cuenta con una mezcla servidores operados por voluntarios otros operador por la compañía dueña del proyecto. El acuerdo ofrece a los usuarios una selección de velocidades: de 30-50 kBit/s (alrededor de la velocidad de una conexión de módem analógico) de forma gratuita, y más de 600 kBit/s por una tarifa. Para una descripción más detallada, comparación y lista de precios, podemos consultar: https://anonymous-proxy-servers.net/en/payment.html.

INFORMACIÓN GENERAL

Sistemas operativos soportados	
Localización	English, German, Czech, Dutch, French and Russian
Sitio Web	https://www.jondos.de
Soporte	Forum: https://anonymous-proxy-servers.net/forum Wiki: https://anonymous-proxy-servers.net/wiki Formulario de Contacto: https://anonymous-proxy-servers.net/bin/contact.pl?

INSTALACIÓN

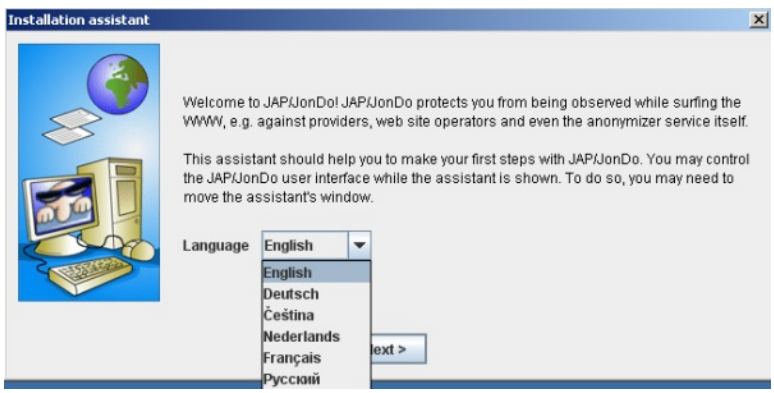
Para utilizar la red JonDo, llamada JonDonym, tendremos que descargar el cliente JonDo para nuestro Sistema operativo desde la página https://www.jondos.de/en/download. Las versiones están disponibles para Linux (alrededor de 9 MB), Mac OS X (unos 17 MB) y Windows (unos 35 MB).

Una vez que hayamos descargado el cliente, lo instalamos como lo haríamos con cualquier software en nuestra plataforma. Nos pueden preguntar si deseamos instalarlo en nuestra PC o si deseamos crear una versión portátil. Por ejemplo, vamos a suponer que estamos instalando JonDo en nuestra PC.

Los usuarios de Windows también podrán ser invitados a instalar el navegador web JonDoFox, que se describe a continuación.

CONFIGURACIÓN Y USO

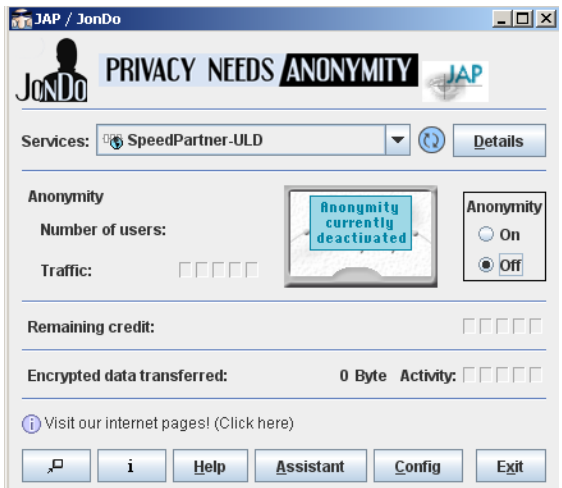
Al iniciar JonDo podemos elegir el idioma que deseamos que nos muestre.



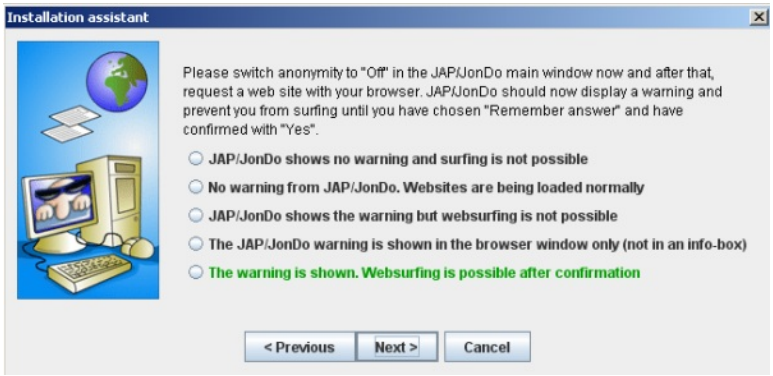
A continuación, podemos elegir el nivel de detalle que deseamos ver al utilizar el servicio. Si somos usuarios inexpertos debemos elegir "Simplified view".

En la siguiente pantalla, el asistente de instalación nos pide que seleccionemos el navegador Web que queremos utilizar con JonDo. Hacemos clic en el nombre de nuestro navegador y seguimos las instrucciones.

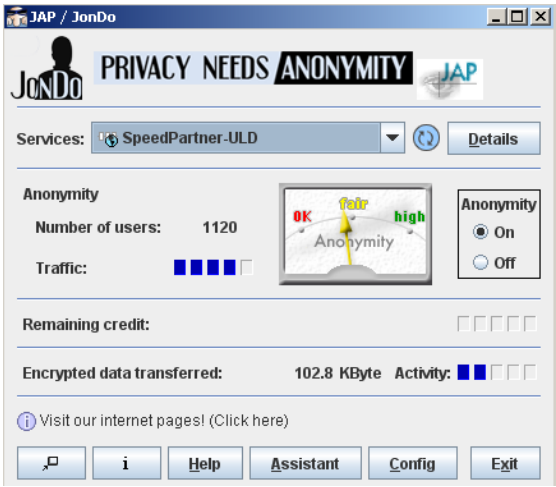
Una vez que se haya completado, JonDo nos pide que comprobemos la configuración. En el panel de control, cambiamos el valor de Anonymity a Off y luego intentamos abrir un sitio web con el navegador que acabamos de configurar.



Si JonDo nos muestra una advertencia y tenemos que seleccionar "Yes" para ver el sitio Web, todo ha sido configurado correctamente y podemos seleccionar "The warning is shown. Websurfing is possible after confirmation". Si alguna otra descripción aplica para nuestro caso, la seleccionamos y el asistente de instalación nos dará más información sobre cómo resolver el problema.

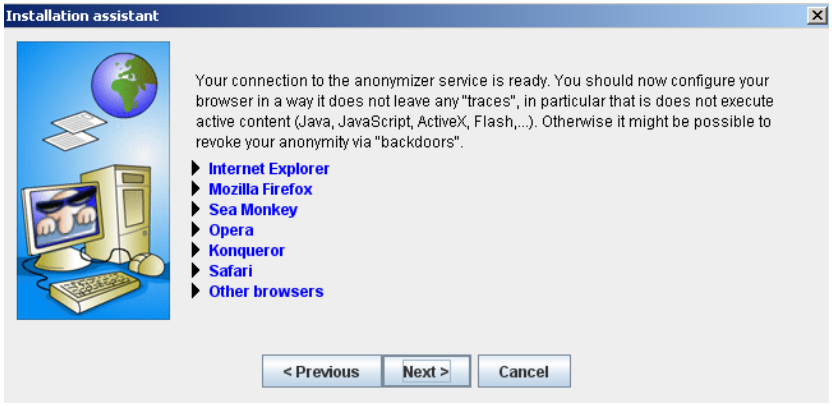


Ahora el segundo paso para asegurar una configuración adecuada: Cambiamos el valor Anonymity a "On" en el panel de control y abrimos un sitio Web al azar con el navegador que hemos configurado.

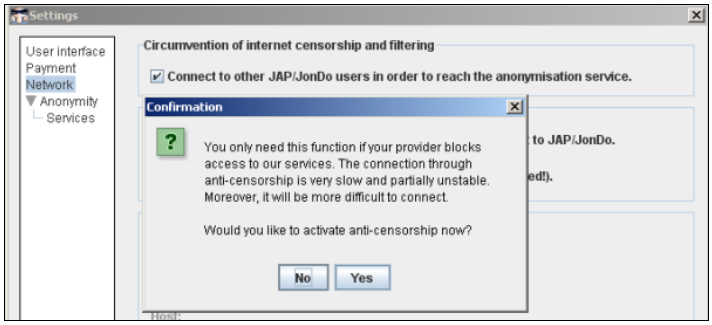


Si se carga el sitio Web, todo está bien y podemos hacer clic en "Connection established, websurfing is fine" Si alguna otra descripción aplica para nuestro caso, la seleccionamos y el asistente de instalación nos dará más información sobre cómo resolver el problema.

Está casi listo. Hemos configurado nuestro navegador para conectarnos a través de la red JonDo. Ahora también debemos configurar nuestro navegador para que no se nos escape accidentalmente ninguna información. Hacemos clic en el nombre de nuestro navegador para iniciar el proceso.



Si los servidores estándares JonDo ya están bloqueados en nuestro país, debemos probar la opción de anti – censura. Hacemos clic en "Config" en el panel de control y seleccionamos la pestaña Network. Hacemos clic en "Connect to other JAP/JonDo users in order to reach the anonymization service". Leemos la advertencia y confirmamos haciendo clic en "Yes".



Para asegurarnos de que el navegador se ha instalado correctamente, podemos entrar a http://what-is-my-ip-address.anonymous-proxy-servers.net que nos dirá si hay algún problema.

JONDOFOX

Para mayor seguridad, el equipo JonDoNym ofrece una versión modificada del navegador web Firefox llamado JonDoFox. Al igual que el paquete del navegador de Tor, impide la fuga de información adicional al utilizar la herramienta de forma anónima.

Podemos descargar la herramienta en la dirección https://anonymous-proxy-servers.net/en/jondofox.html.

26. YOUR-FREEDOM

Your-Freedom es una herramienta proxy comercial que también ofrece un servicio gratuito (aunque más lento).

El software está disponible para Microsoft Windows, Linux and Mac OS y lo conecta a una red de cerca de 30 servidores en diez países. Your-Freedom también ofrece servicios avanzados como OpenVPN y SOCKS, haciéndolo una herramienta relativamente sofisticada para evadir la censura en Internet.

INFORMACIÓN GENERAL

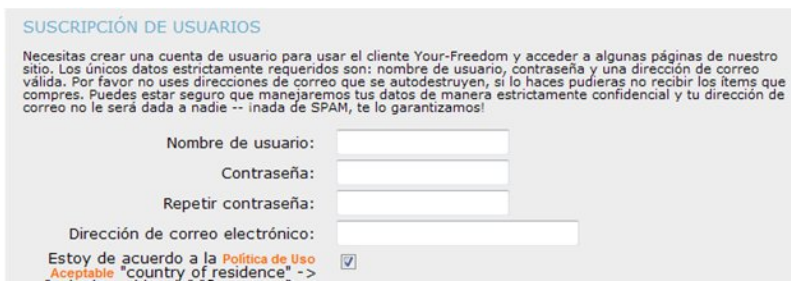
Sistemas operativos que soporta	
Localización	20 languages
Sitio Web	https://www.your-freedom.net
Soporte	Forum: https://www.your-freedom.net/index.php?id=2 Manual: https://www.your-freedom.net/ems-dist/Your%20Freedom%20User%20Guide.pdf

PREPARANDO EL USO DE YOUR-FREEDOM

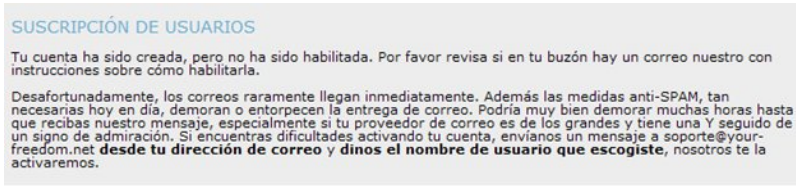
Primeramente, descargamos la herramienta de forma gratuita desde la página https://www.your-freedom.net/index.php?id=downloads. Si ya tenemos Java instalado, podemos descargar la versión pequeña que es de unos 2 MB. Para comprobar si se ha instalado Java, visitamos la página http://www.java.com/en/download/testjava.jsp. Si no tenemos instalado Java, descargamos el instalador completo, que es de aproximadamente 12 MB. Todos los archivos están también disponibles en la página http://mediafire.com/yourfreedom.

Si vivimos en un país en el que el gobierno censura Internet, podemos usar Your-Freedom con la cuenta Sesawe (nombre de usuario: sesawe, contraseña: sesawe). En caso de que no nos funcione tenemos que registrarnos para obtener una cuenta. Para empezar, registramos una cuenta gratuita en el sitio Web https://www.your-freedom.net/index.php?id=170&L=0.

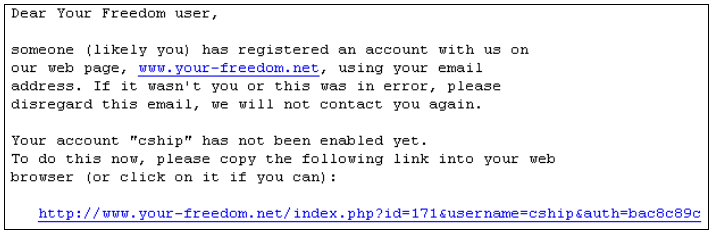
Hacemos clic en la "¿Primera vez que viene? ¡Registrese aquí!" debajo de los dos campos de entrada.



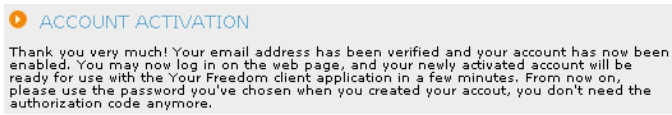
En la siguiente página, introducimos la información necesaria. Es suficiente un nombre de usuario, contraseña y la dirección de correo electrónico. Otra información es opcional.



Veremos un mensaje de que nuestro registro está casi terminado, y en pocos segundos debemos recibir un correo a la dirección que hemos brindado.



Hacemos clic en el segundo enlace (el más largo) para confirmar nuestro registro.



Cuando veamos el mensaje de pantalla "Thank you", nuestra cuenta ha sido activada.

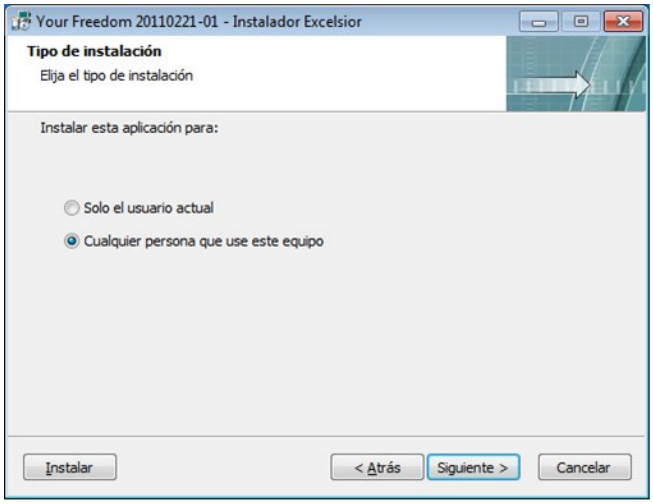
INSTALACIÓN

Las siguientes instrucciones y capturas de pantallas han sido hechas en Windows, pero todos los pasos y la configuración son muy similares para otros sistemas operativos.

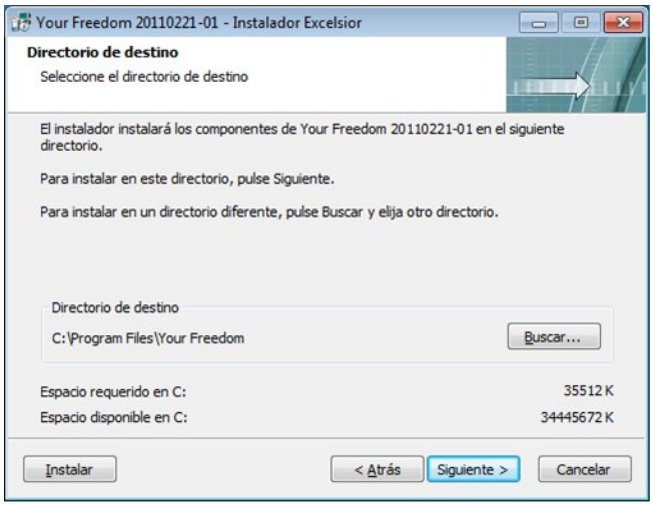
Ahora ya estamos listos para instalar Your-Freedom.

Hacemos clic en el archivo descargado. El nombre del fichero puede variar según las nuevas versiones que se liberan de manera regular.

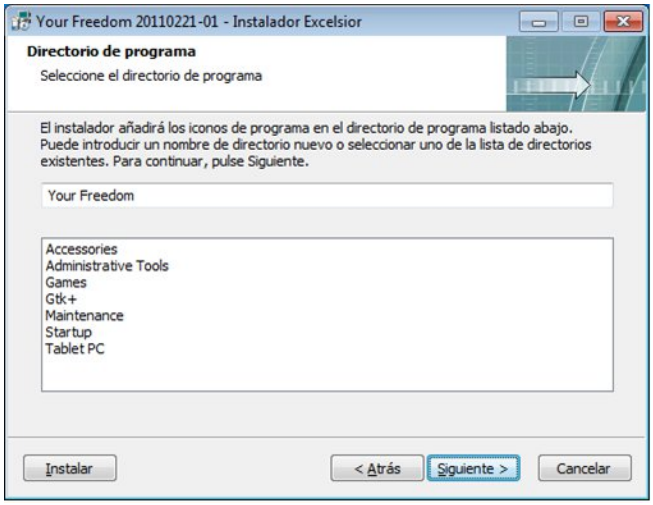
Hacemos clic en Siguiente en la primera pantalla.



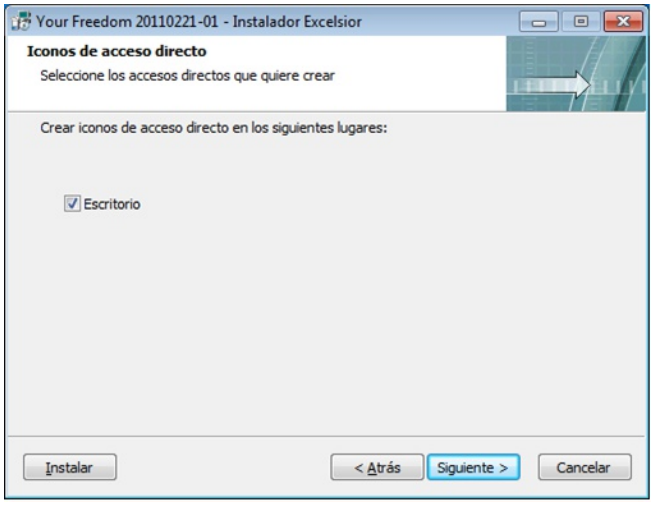
En la siguiente pantalla podemos elegir si el programa será utilizado solo por nosotros o para todos los usuarios de nuestra computadora (común). A continuación, hacemos clic en Siguiente.



Seleccionamos el directorio para la instalación de Your-Freedom. La mayoría de los usuarios pueden usar la selección por defecto.
Hacemos clic en Siguiente.

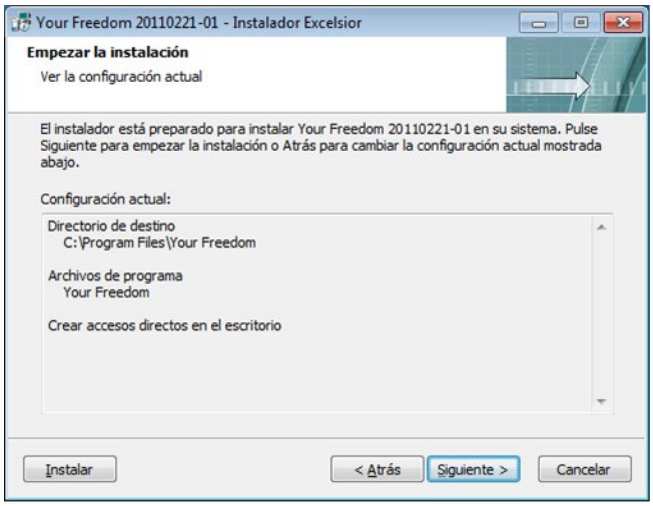


En la próxima pantalla del instalador podemos modificar el nombre que se usará en la carpeta programa. Podemos dejar sin tocar el valor por defecto y hacemos clic en Siguiente.

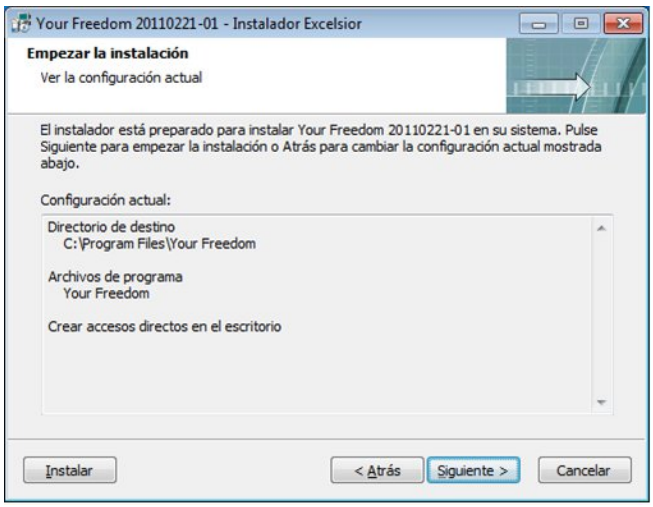


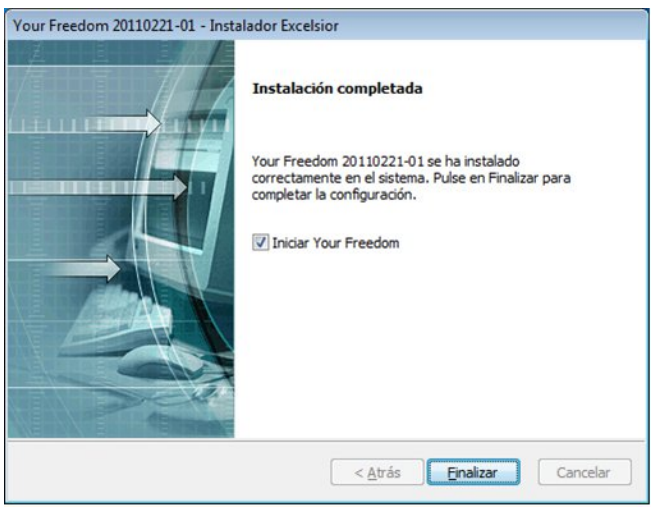
Seleccionamos si deseamos crear un ícono en el escritorio. Hacemos clic en Siguiente nuevamente.

Aquí podemos ver un resumen de las decisiones que tomamos. Confirmamos haciendo clic en Siguiente o volvemos si necesitamos cambiar algo.



Ahora la instalación se lleva a cabo. Este proceso puede tardar unos minutos, dependiendo de nuestro ordenador.





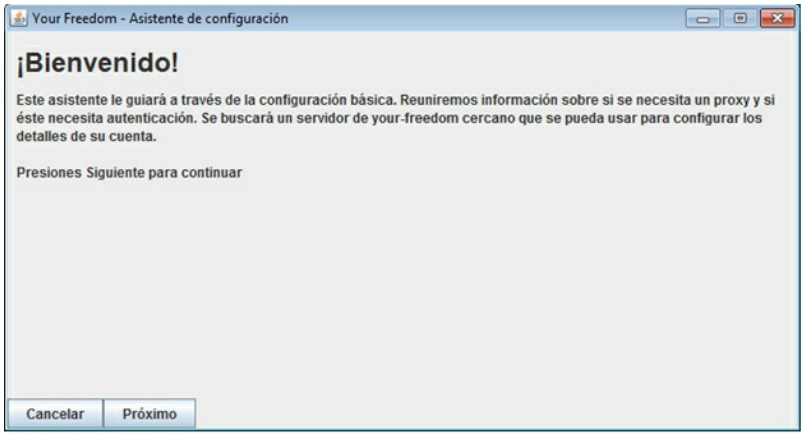
Finalmente la instalación está lista. Cerramos el programa de instalación haciendo clic en Finish.

CONFIGURACIÓN

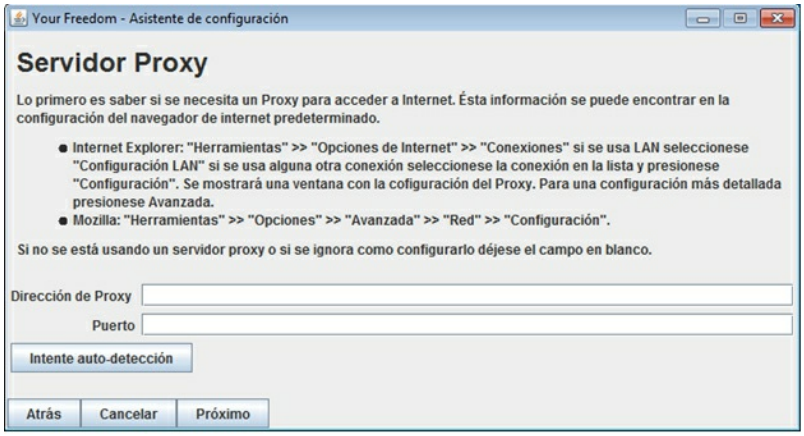
Your-Freedom se iniciará automáticamente. Cuando más adelante deseemos iniciarlo manualmente hacemos clic en el ícono Your-Freedom (la puerta) en nuestro escritorio.

Cuando iniciemos Your-Freedom por primera vez necesitamos configurarlo.

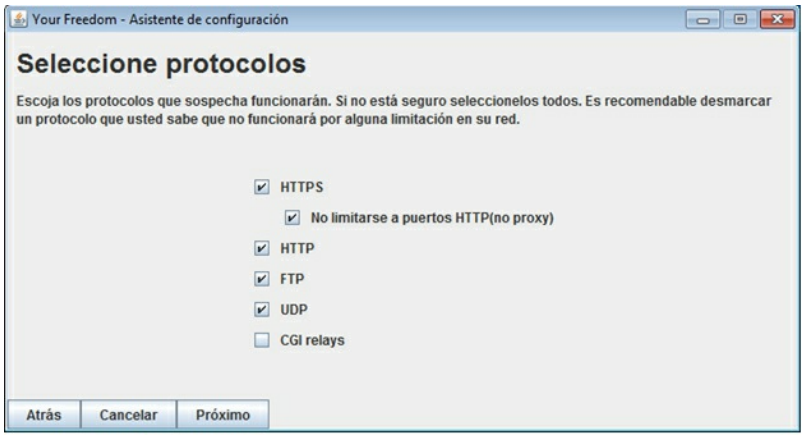
El primer paso es elegir el idioma. Hacemos clic en el idioma que deseemos. Luego tendremos la oportunidad de cambiar la configuración.



Justo después podremos ver el asistente de configuración. Hacemos clic en Proximo



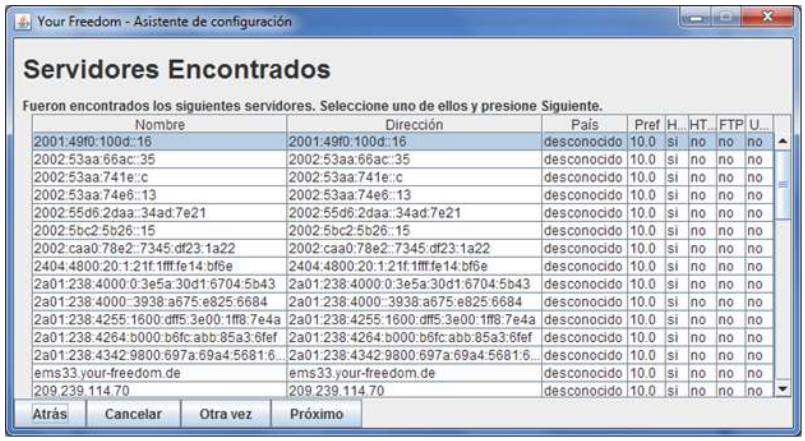
En el cuadro de diálogo del servidor proxy, el programa detectará automáticamente la información del servidor proxy que podemos utilizar. Hacemos clic en Proximo.



En la ventana de diálogo Select Protocol debemos mantener los valores por defecto y continuamos haciendo clic en Proximo.

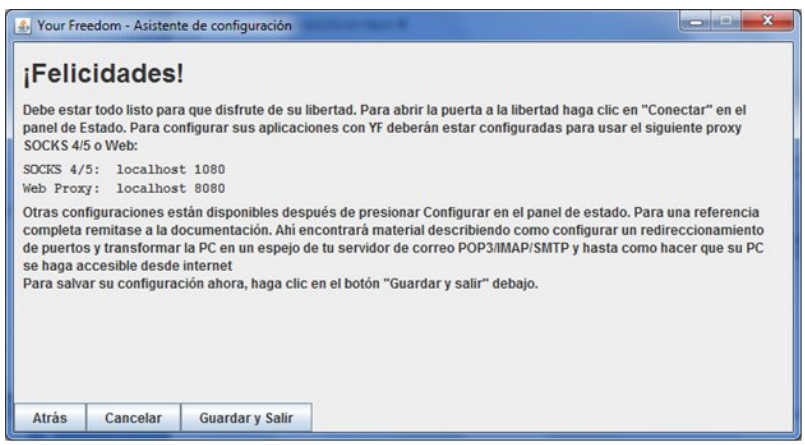
Ahora el asistente de configuración de Your-Freedom hará varias pruebas para encontrar los servidores disponibles y comprobar nuestro tipo de conexión y de filtrado. Esta operación puede tardar algunos minutos.

Podemos recibir una advertencia de nuestro cortafuegos (en este caso, por ejemplo uno de Windows 7). Le indicamos permitir el acceso a Your-Freedom.



Cuando el asistente está listo vemos la pantalla de Servidores Freedom encontrados, donde seleccionamos un servidor y hacemos clic en Proximo.

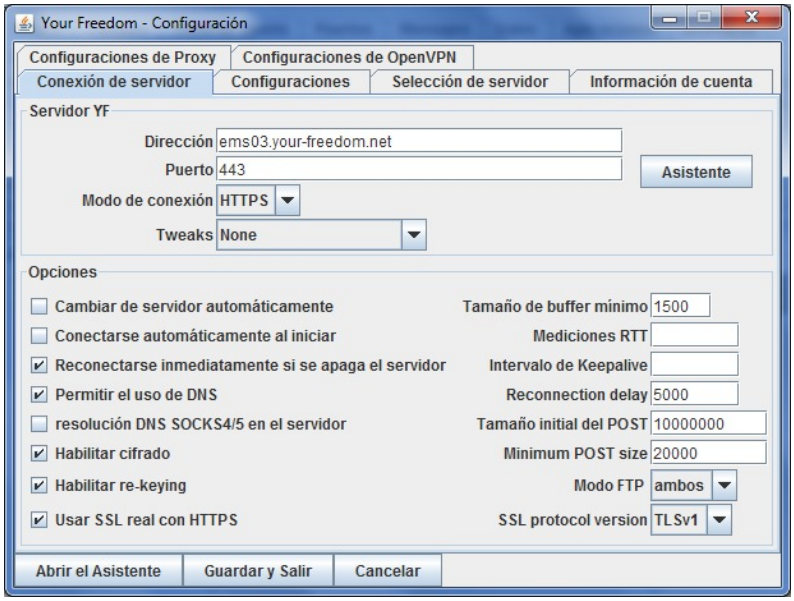
A continuación, introducimos nuestra información de cuenta previamente creada. Si no tenemos una, podemos conseguir libre acceso mediante el envío de una solicitud a la dirección de correo electrónico: spanish@sesawe.net.
Hacemos clic en Next.



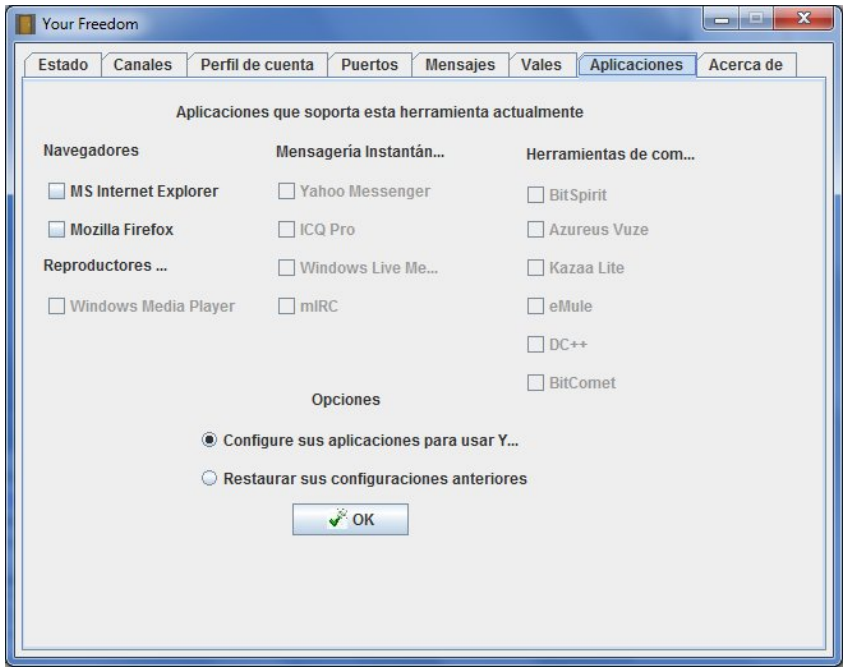
Cuando veamos el mensaje "¡Felicidades!" en la pantalla, el asistente de configuración está listo. Hacemos clic en "Guardar y Salir".

Your-Freedom se está ejecutando ahora en el equipo, y podemos ver un ícono en la barra de tareas.

Para mayor seguridad y mejores formas de evadir los filtros debemos ajustar las opciones haciendo clic en Configurar en la ventana principal de Your-Freedom y seleccionamos las opciones que aparecen en la pantalla de abajo. A continuación hacemos clic en Guardar y Salir.



Ahora Your-Freedom está conectado a un servidor y proporciona un proxy local que podemos utilizar con el software que deseemos, como Internet Explorer o Firefox. Para Configurar automáticamente, hacemos clic en el tabulador Aplicación en la ventana principal de Your-Freedom, seleccionamos el software que deseamos usar y hacemos clic en OK. Your-Freedom configurará automáticamente nuestra aplicación para que se conecte a través de un túnel encriptado de Your-Freedom a Internet.



Para asegurarnos de que estamos usando Your-Freedom correctamente vamos a la página https://www.your-freedom.net y consultamos la sección Your Footprint a la izquierda. Si el país detectado no es el nuestro, estamos utilizando con éxito el túnel cifrado de Your-Freedom para acceder a Internet.

TECNICAS AVANZADAS
27. DOMINIOS Y DNS
28. Proxis HTTP
29. La línea de comando
30. OpenVPN
31. SSH Tunnelling
32. Proxis SOCKS

DOMINOS Y DNS

Si sabemos o sospechamos que la técnica principal de censura en nuestra red se basa en en el filtrado y o la suplantación de identidad de DNS, debemos considerar estas técnicas.

USANDO SERVIDORES DE NOMBRES DE DOMINIO ALTERNATIVOS

En pocas palabras, un servidor DNS traduce una dirección Web ej. google.com en una dirección IP que identifica a un servidor específico con esa página en Internet, ej. 72.14.207.19. Este servicio es casi siempre suministrado por un servidor DNS mantenido por su Proveedor de Servicios de Internet (**ISP**). Un bloqueo simple de DNS es implementado dándole una respuesta incorrecta o no válida a una solicitud de DNS con el fin de evitar que los usuarios localicemos los servidores que estamos buscando. Este método es muy fácil de implementar por parte de la censura, por lo que es ampliamente utilizado. Teniendo en cuenta que a menudo hay varios métodos de censura que se combinan, el bloqueo de DNS no es el único problema.

Podemos evadir este tipo de bloqueo de dos maneras: mediante el cambio de DNS de la configuración de nuestra computadora para utilizar los DNS alternativos o editando nuestro fichero hosts.

SERVIDORES DNS ALTERNATIVOS

Una extensión de esta técnica es prescindir el Servidor de Nombres de Dominios de nuestro ISP local usando servidores de terceros para resolver dominios que pueden estar bloqueados por los servidores de ISP. Hay un número de servidores DNS gratis disponibles internacionalmente con los que se puede intentar. OpenDNS (https://www.opendns.com) provee este servicio y además tiene las guías de cómo cambiar el servidor DNS que usa nuestra computadora (https://www.opendns.com/smb/start/computer). Existe también una lista de servidores DNS disponibles alrededor del mundo en http://www.dnsserverlist.org.

Aquí hay una lista de servicios DNS a disposición del público, en la Wiki Internet Censorship en http://en.cship.org/wiki/DNS. (Algunos de estos servicios pueden bloquear un número limitado de sitios, consultemos los sitios de los proveedores para obtener más información acerca de sus políticas).

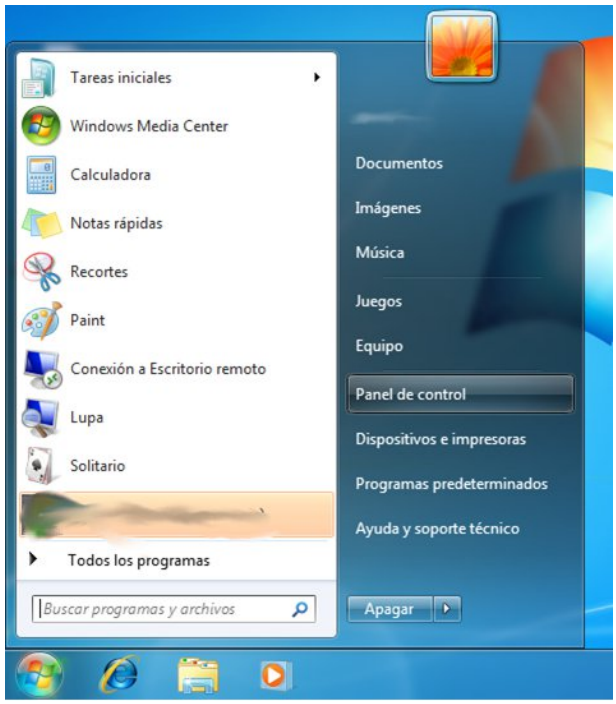
Publicly-available DNS servers

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

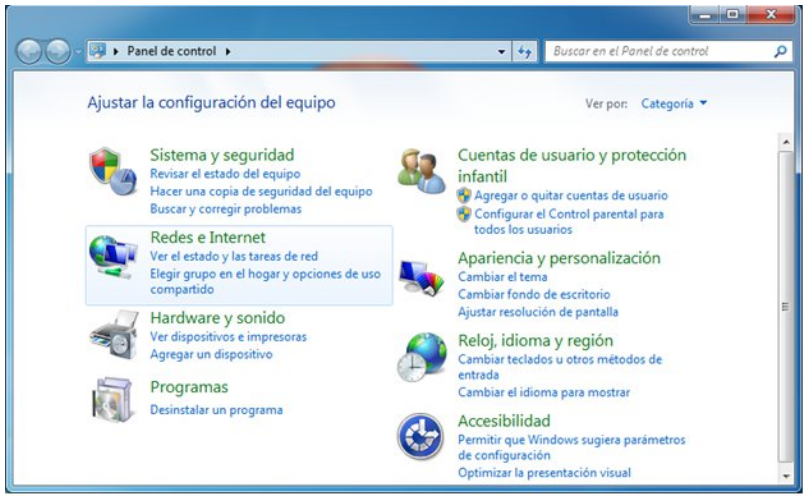
Una vez que seleccionemos el servidor DNS que vamos a usar, necesitaremos introducir nuestra selección en la configuración DNS de nuestro sistema operativo.

Cambiar nuestra configuración DNS en Windows

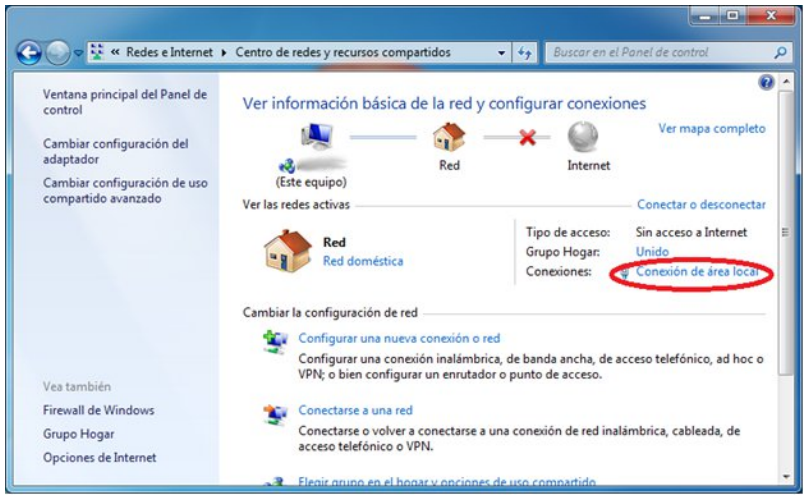
1. Abrimos el panel de control en el menú Inicio.



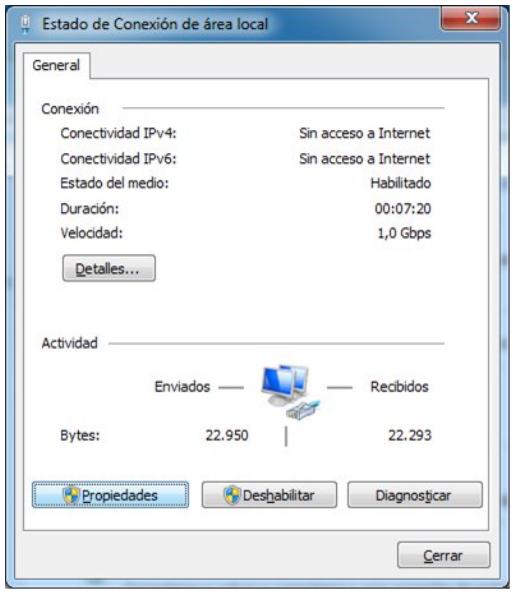
2. Debajo de Redes e Internet, hacemos un clic en "Ver estado de redes y estadísticas".



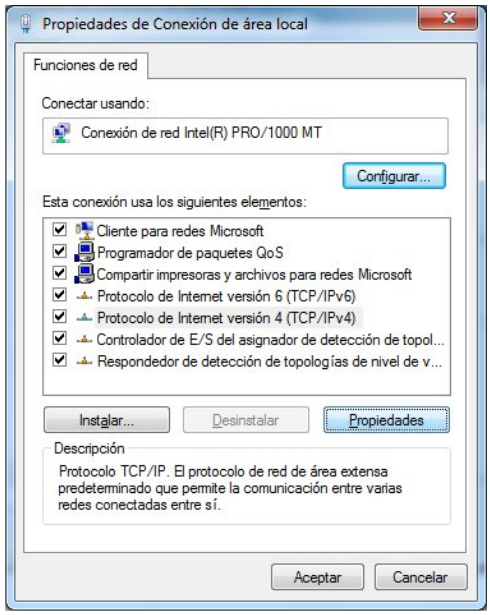
3. Hacemos un clic en Conexión Inalámbrica en el lado derecho de la ventana.



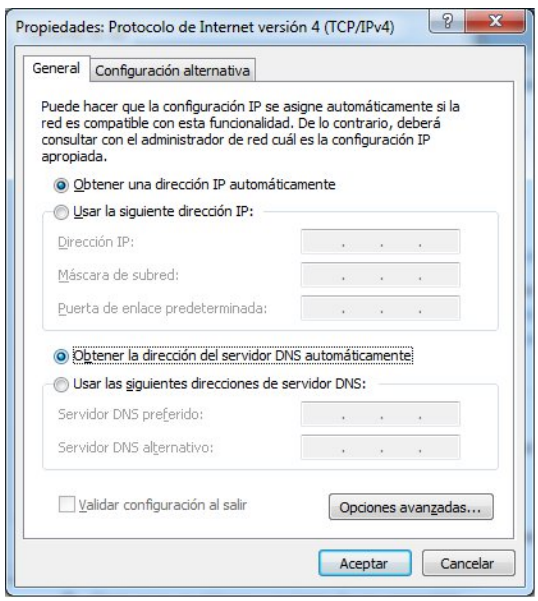
4. Se abrirá la ventana de conexión de red inalámbrica. Hacemos clic en Propiedades.



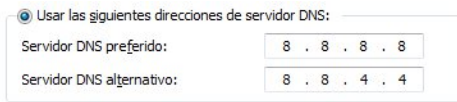
5. En la ventana de Propiedades de conexión de red inalámbrica seleccionamos Internet Protocol Version 4 (TCP/IPv4) y hacemos clic en Propiedades.



6. Ahora deberíamos estar en la ventana de Propiedades de Internet Protocol Version 4 (TCP/IPv4), que es donde vamos a especificar nuestra dirección DNS alternativa (por ejemplo: Google Public DNS)

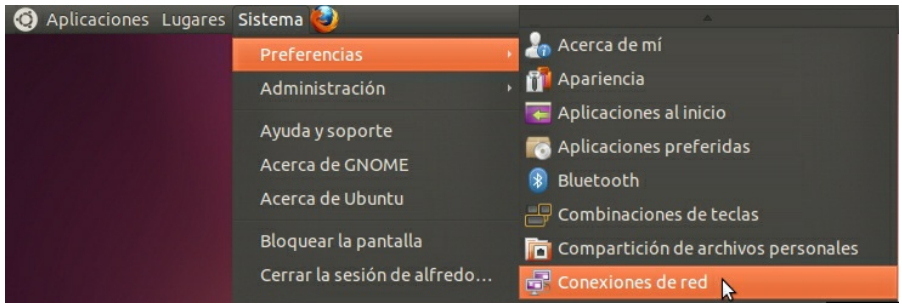


7. En la parte inferior de la ventana, hacemos clic en "Usar las siguientes direcciones de DNS" y completamos los campos con la información de la IP del servidor DNS alternativo. Cuando terminemos hacemos clic en OK. Por defecto, se usa el primer servidor DNS. El servidor DNS alternativo puede ser de otra compañía.

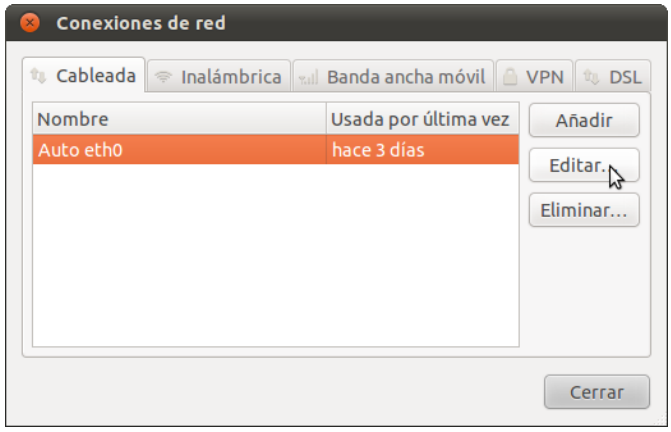


Cambiar nuestra configuración DNS en Ubuntu

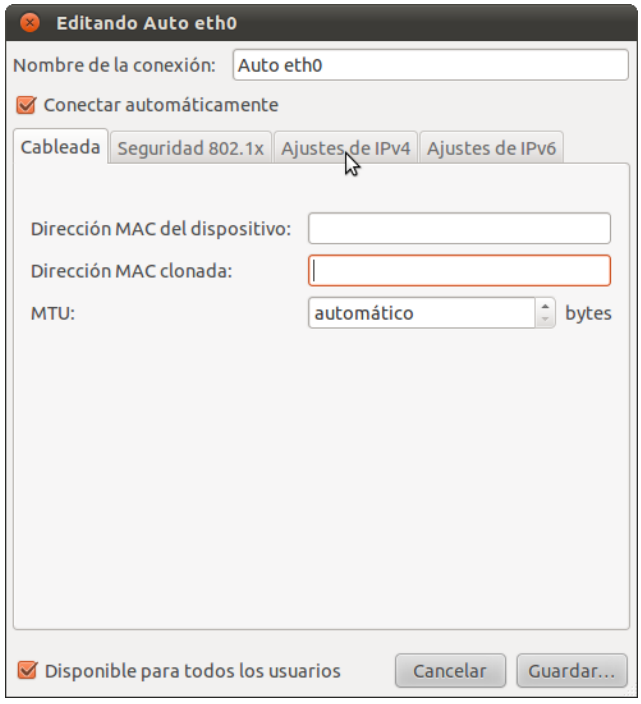
1. En el menú del Sistema vamos a Preferencias > Conexiones de Red.



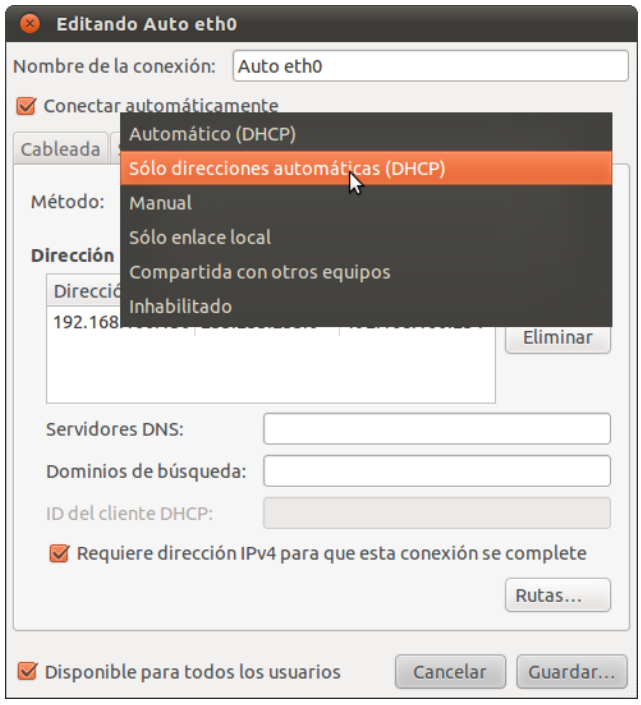
2. Se abre la ventana de configuración de red. Seleccionamos la pestaña adecuada donde se encuentra nuestra conexión a Internet(en este caso es Wired pero puede ser otra). Ahí escogemos nuestra conexión de red y damos clic en Editar.



3. Se abrirá una ventana con propiedades avanzadas de la conexión. Aquí seleccionamos "IPv4".

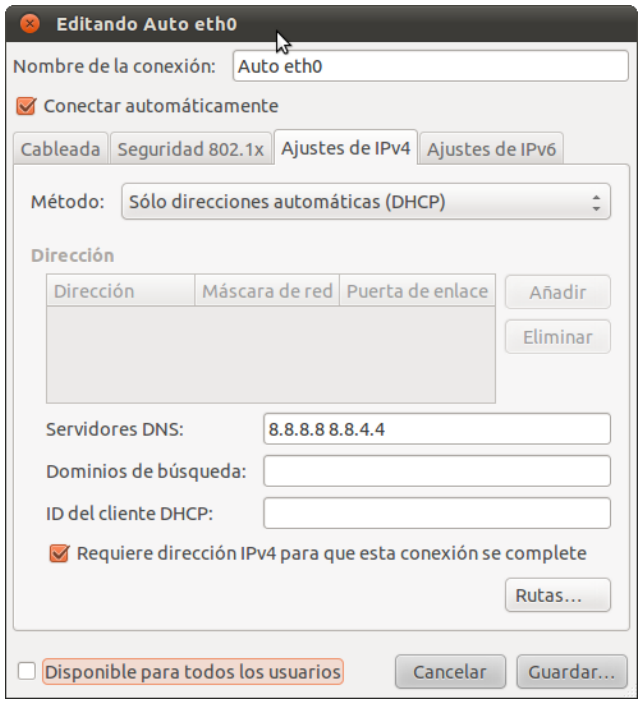


4. Si el método seleccionado es "Automático (DHCP)" desplegamos el menú y escogemos "Automático (DHCP) Solo dirección". Si el método es otro, dejémoslo así.



5. En el campo servidor DNS entremos las direcciones de servidores de DNS alternativos, separadas por espacios. Por ejemplo, si fuesemos a usar los servidores de DNS de google escribíamos "8.8.8.8 8.8.4.4"

6. Damos clic en Aplicar para salvar las configuraciones. Es posible que se nos pregunte por nuestra contraseña y que confirmemos que queremos realizar los cambios.



7. Repetimos los pasos del 1 al 6 para cada conexión que queremos modificar.

EDITAR NUESTRO FICHERO HOSTS

Si conocemos la dirección IP de un sitio Web en particular o de algún otro servicio de Internet que está bloqueado por el proveedor de servidores DNS, podemos hacer un listado de estos sitios en el fichero hosts de nuestro equipo, que es una lista local con los nombres y las direcciones IP correspondientes que nuestra computadora usará antes de consultar los servidores DNS externos. El archivo hosts es un fichero de texto con un formato muy simple; cuyo contenido es equivalente a:

208.80.152.134 secure.wikimedia.org

donde cada línea contiene una dirección IP, un espacio y a continuación un nombre. Podemos añadir cualquier cantidad de sitios a nuestro archivo hosts (pero tengamos en cuenta que si utilizamos la dirección equivocada para un sitio, se podría impedir que tengamos acceso a ese sitio hasta que lo arreglemos o lo eliminemos de la lista).

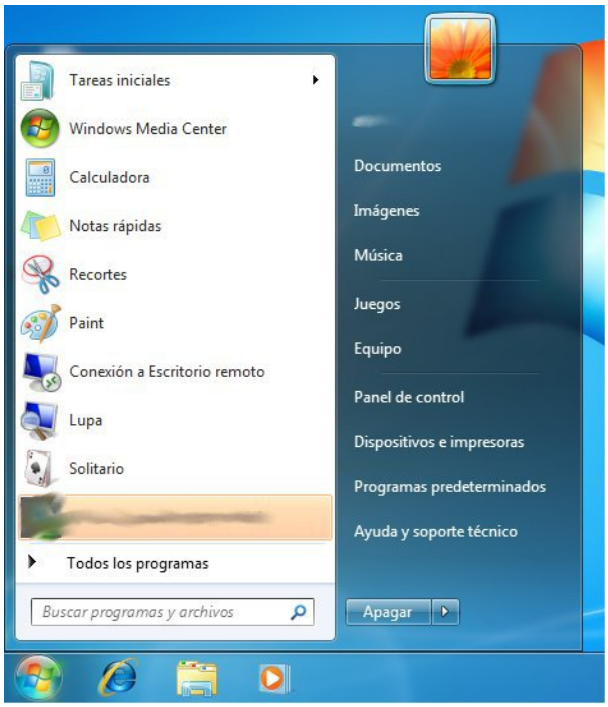
Si no podemos encontrar la dirección IP de un sitio por el bloqueo de DNS de nuestro ISP, hay cientos de servicios que nos ayudarán a realizar una búsqueda de DNS sin censura. Por ejemplo, podemos utilizar cualquiera de las herramientas de http://www.dnsstuff.com/tools.

También podríamos considerar el uso de las herramientas de http://www.traceroute.org, que son sofisticadas herramientas de diagnóstico de red proporcionadas por diferentes proveedores ISPs. Estas estaban destinadas originalmente para el diagnóstico de cortes accidentales de la red más que para la censura, sin embargo puede ser útil para esto también. Estas herramientas también incluyen la posibilidad de buscar la dirección IP de un servidor en particular.

Editar nuestro fichero hosts en Windows Vista / 7

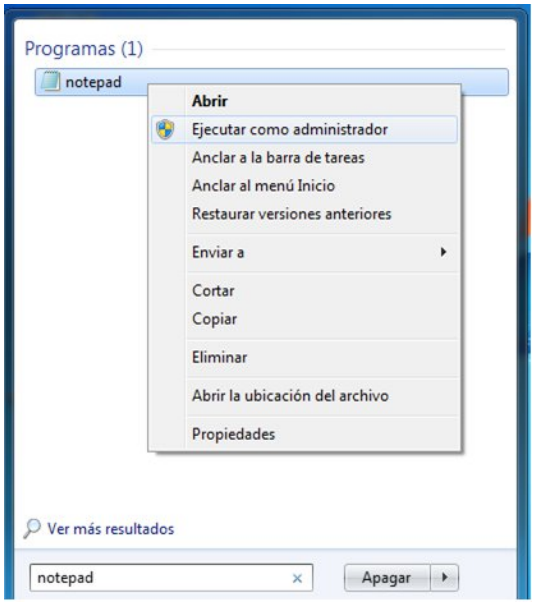
Tendremos que usar siempre un editor de texto, como el Bloc de Notas, para editar el archivo hosts. En WindowsVista y 7, el archivo hosts se encuentra normalmente en C:\Windows\system32\drivers\etc\hosts.

1. Hacemos un clic en el botón Inicio.

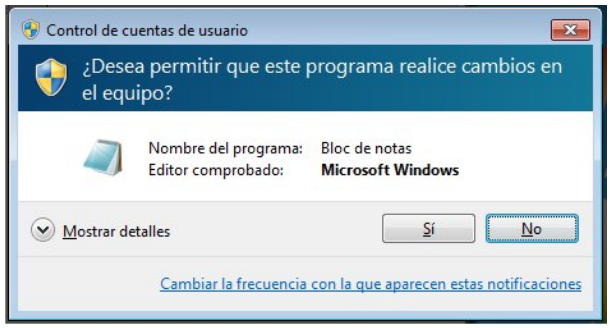


2. Escribimos "notepad" en el cuadro de búsqueda.

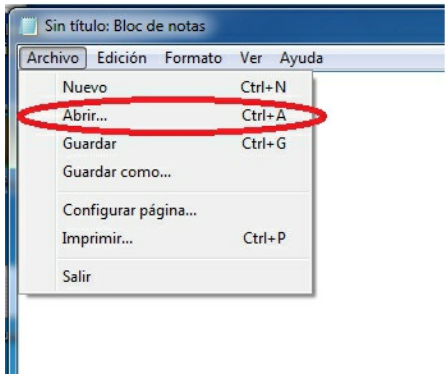
3. Una vez que encontramos el programa, hacemos clic sobre él y seleccionamos "Run as administrator".



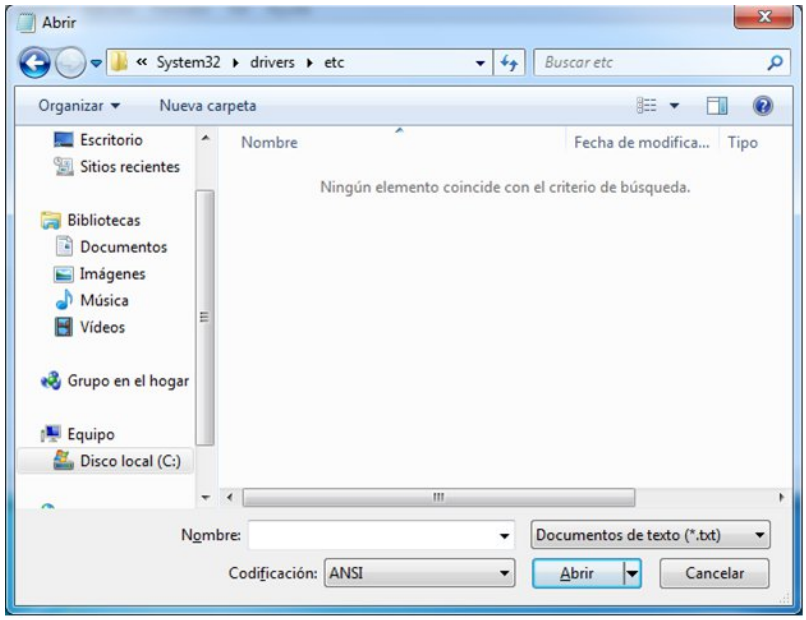
4. Windows nos pedirá permiso para realizar cambios en los archivos. Hacemos clic en Sí.



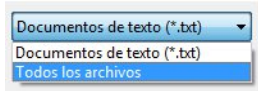
5. En el menú Archivo, seleccionamos Abrir.



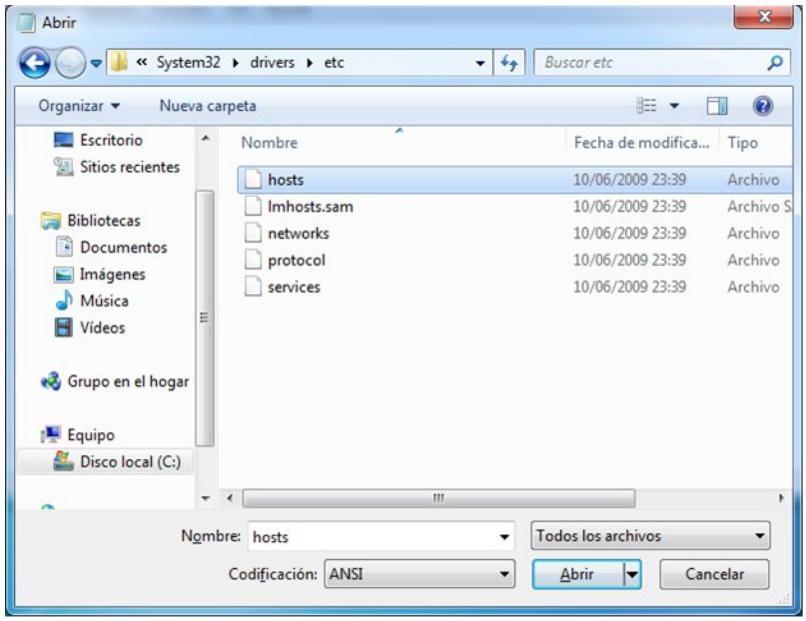
6. Vamos a C:\Windows\System32\Drivers\etc\. Podemos ver que la carpeta aparece inicialmente vacía.



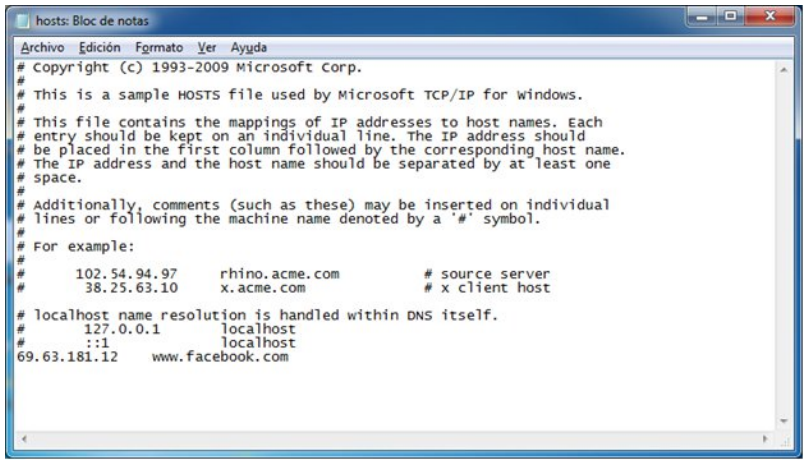
7. En la parte inferior derecha del cuadro de diálogo abierto, seleccionamos Todos.



8. Seleccionamos el archivo "hosts" y hacemos clic en Abrir.



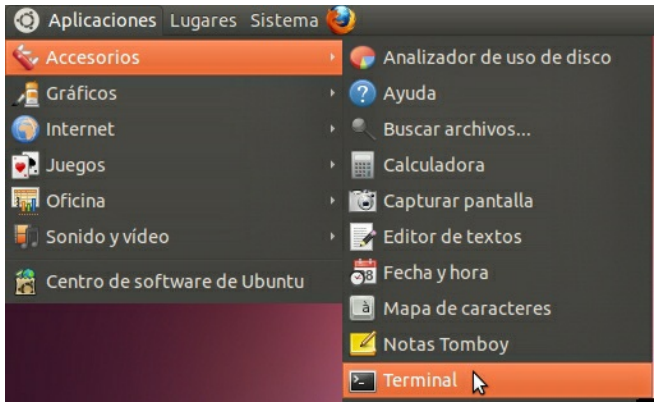
9. Agregamos, por ejemplo, la línea "69.63.181.12 www.facebook.com" al final del archivo, y lo guardamos pulsando Ctrl+S o seleccionando Archivo > Guardar en el menú.



Editar nuestro archivo hots en Ubuntu

En Ubuntu, el archivo hosts se encuentra en /etc/hosts. Para editarlo, tendremos que tener algún conocimiento de la línea de comandos. Es necesario que consultemos el capítulo "La línea de comando " en este libro, para un breve tutorial sobre este tema.

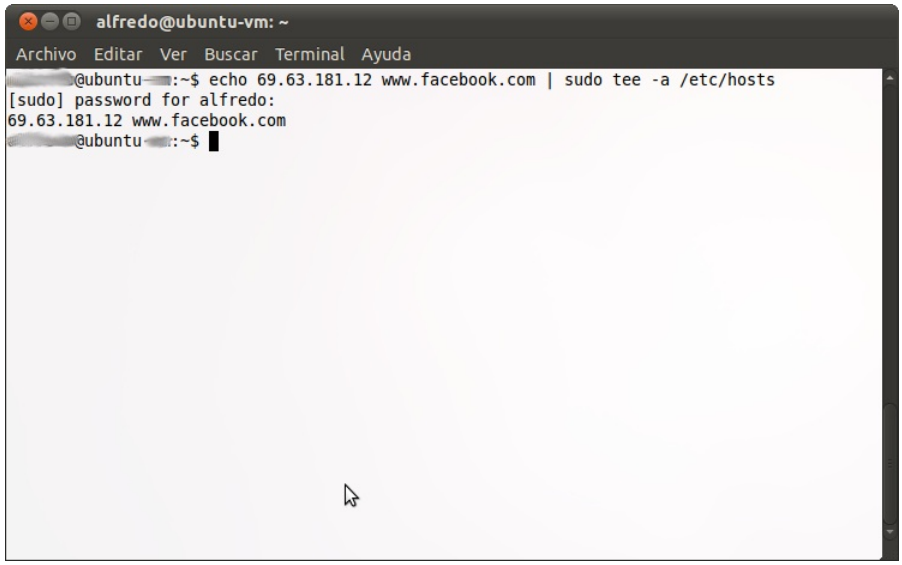
1. Abrimos el terminal, a través de Accessories > Terminal en el menú Applications.



2. Utilizamos la siguiente línea de comando para agregar automáticamente una línea a nuestro archivo hosts:

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

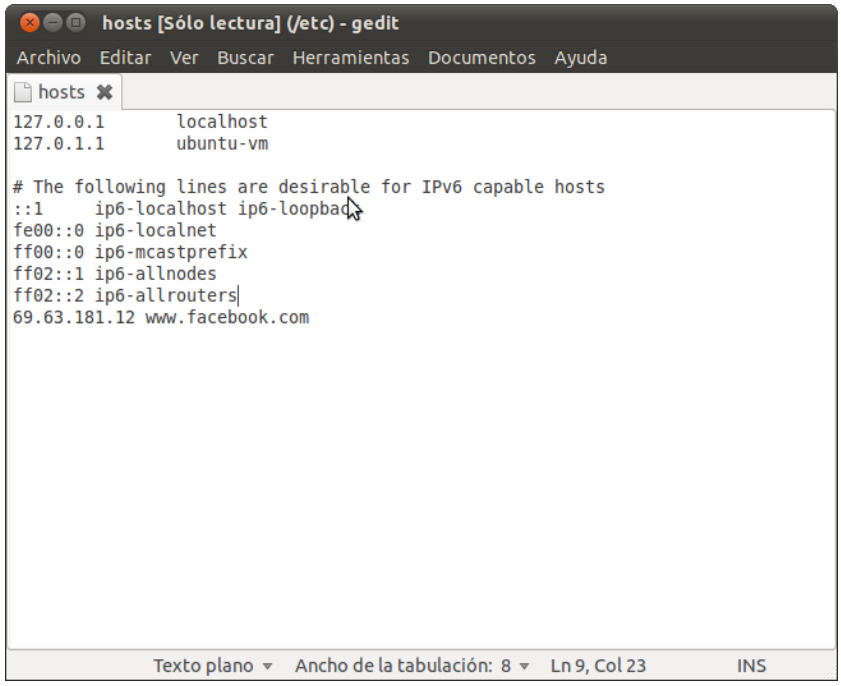
3. Es posible que se nos pida una contraseña para poder modificar el archivo. Una vez autorizados, el comando "69.63.181.12 www.facebook.com" se adicionará a la última línea del archivo hosts.



4. Opcional: Si nos sentimos más cómodos trabajando en una interfaz gráfica, abrimos el terminal y utilizamos la siguiente línea de comandos para iniciar un editor de texto:

   sudo gedit /etc/hosts

5. Es posible que se nos pida una contraseña para poder modificar el archivo. Una vez que la ventana está abierta, solo tenemos que añadir la línea "69.63.181.12 www.facebook.com" al final del archivo, y guardarlo pulsando Ctrl+S o seleccionando File > Save en el menú.


hosts [Sólo lectura] (/etc) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
hosts
127.0.0.1 localhost
127.0.1.1 ubuntu-vm
The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
69.63.181.12 www.facebook.com
Texto plano
Ancho de la tabulación: 8
Ln 9, Col 23
INS

28. PROXIS HTTP

Existen programas, llamados *proxis*, permite a una computadora en Internet procesar las solicitudes que vienen de otro equipo. Los tipos más comunes de proxis son los proxis **HTTP**, que manejan las solicitudes de los sitios Web y los proxis **SOCKS**, que manejan las solicitudes de una amplia variedad de aplicaciones. En este capítulo vamos a ver proxis HTTP y su funcionamiento.

PROXIS BUENOS Y MALOS

Los proxis pueden ser utilizados por los **operadores de red** para censurar Internet y controlar lo que hacen los usuarios. Sin embargo, los proxis son también herramientas para que los usuarios puedan evadir la censura y otras restricciones de red.

Proxis que limitan acceso

Un operador de red puede obligar a los usuarios a acceder a Internet (o por lo menos a las páginas web) sólo a través de un proxy determinado. El operador de red puede programar este proxy para llevar un registro de los usuarios que acceden y también para negar el acceso a determinados sitios o servicios (bloqueo de IP o bloqueo de puertos). En este caso, el operador de red puede utilizar un *cortafuego* para bloquear las conexiones que no pasan a través del proxy restrictivo. Esta configuración es llamada a veces *proxy forzado*, ya que los usuarios se ven obligados a usarlo.

Proxis para la evasión de censura

Sin embargo, un proxy puede ser también útil para evadir las restricciones. Si podemos comunicarnos con una ordenador en un lugar sin restricciones que esté ejecutando un proxy, podremos beneficiarnos de la conectividad sin restricciones. A veces, un proxy está disponible para que el público lo use, en cuyo caso, es llamado proxy abierto. Muchos proxis abiertos están bloqueados en países con Internet restringido si las personas que administran la red conocen sobre ellos.

DÓNDE ENCONTRAR UN PROXY ABIERTO

Hay muchos sitios web con listas de proxis de aplicación abiertos. Una visión general de estos sitios está disponible en http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering_/Hosted_Proxy_Services/Free/Proxy_Lists.

Debemos tener en cuenta que muchos proxis abiertos sólo existen unas pocas horas, por lo que es importante obtener una lista que se haya actualizado recientemente.

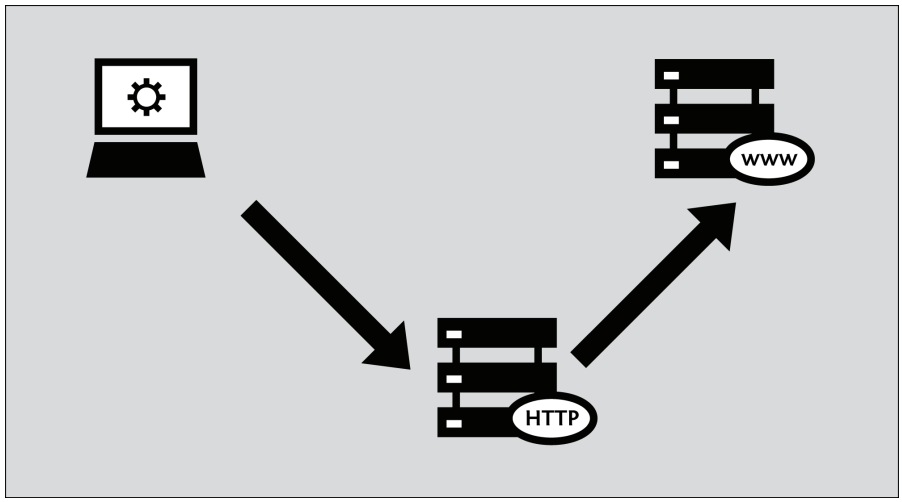
CONFIGURACIÓN DE PROXY HTTP

Para usar un proxy, debemos cambiar la configuración proxy de nuestro sistema operativo o de nuestras aplicaciones individuales. Una vez que hayamos seleccionado un proxy en la configuración de proxy de una aplicación, esta tratará de usar ese proxy para todos los accesos a Internet.

Debemos asegurarnos de tomar nota de los datos de configuración originales para poder restaurarlos. Si el proxy se vuelve indisponible o inalcanzable por alguna razón, el programa que lo usa dejará de trabajar. En ese caso, necesitamos reiniciar la configuración inicial.

En Mac OS X y en algunos sistemas Linux, estas características pueden configurarse en el sistema operativo, y automáticamente se aplicarán en aplicaciones como el navegador web o las aplicaciones de mensajería instantánea. En Windows y otros sistemas Linux, no hay un lugar central para configurar las características del proxy, y cada aplicación debe ser configurada de forma independiente. Es necesario tener en cuenta que aunque el proxy esté configurado centralmente no hay garantía de que las aplicaciones que lo usan soporten estas características de configuración, así que es siempre buena idea seleccionar las características de configuración para cada aplicación individual.

Normalmente los navegadores Web pueden ser configurados para usar proxis HTTP directamente



Los pasos a continuación describen como configurar Microsoft Internet Explorer, Mozilla Firefox, Google Chrome y el cliente de mensajería instantánea gratis y de código abierto Pidgin para usar un proxy. Si usamos Firefox para la navegación Web, será más fácil usar el programa FoxyProxy; que es una alternativa a los pasos que se detallan más abajo. Si usamos Tor, es más seguro usar el programa TorButton (que se ofrece como parte de la descarga de Tor Bundle) para configurar nuestro navegador para que use Tor.

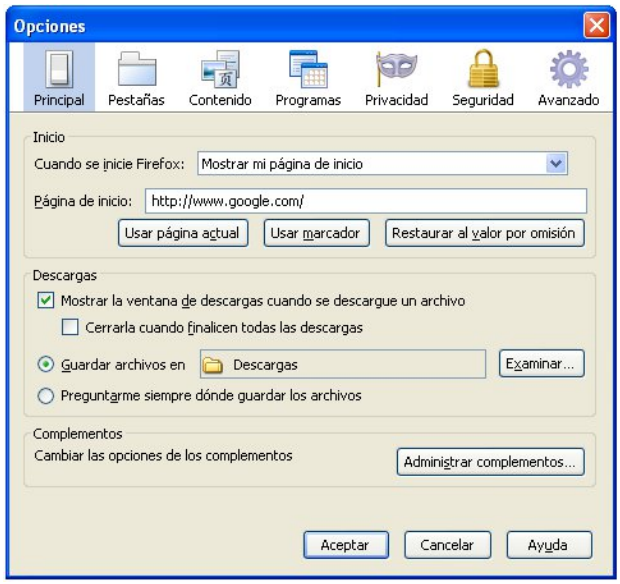
Aunque los clientes de correo electrónico como Microsoft Outlook y Mozilla Thunderbird configurarse para usar proxis HTTP, el tráfico real de correo usa otros protocolos como POP3, IMAP y SMTP, y por tanto no pasa a través de proxis HTTP.

Mozilla Firefox

Configurar Firefox para usar un proxy HTTP:

1. En el menú “Herramientas”, clic “Opciones”:

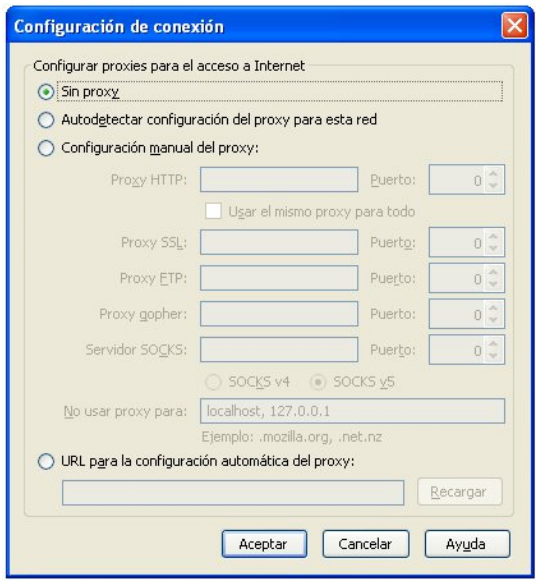
2. La ventana “Opciones” aparece:



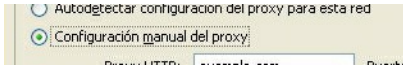
3. En la barra de herramientas en el tope de la ventana, clic “Avanzado”

4. Clic en el tabulador “Red”:

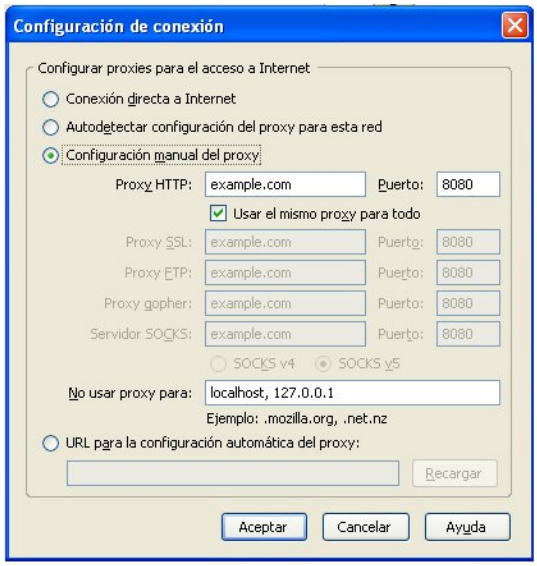
5. Clic en Configuración de conexión. Firefox muestra la ventana de Configuración de conexión:



6. Seleccionamos “Configuración manual del proxy”. Los campos debajo de esta opción se vuelven disponibles.



7. Entramos la dirección del “proxy HTTP” y el número del “puerto”, y hacemos clic en “OK”.



Si hacemos clic en “Usar el mismo proxy para todo”, Firefox intentará enviar tráfico HTTPS (HTTP seguro) y FTP a través del proxy. Esto puede que no funcione si estamos usando un proxy público, pues muchos de ellos no soportan HTTPS y FTP. Si, por otra parte nuestro tráfico HTTPS y/o FTP está siendo bloqueado, podemos intentar un proxy público con soporte para HTTPS y/o FTP y usar la opción “Usar el mismo proxy para todo” en Firefox.

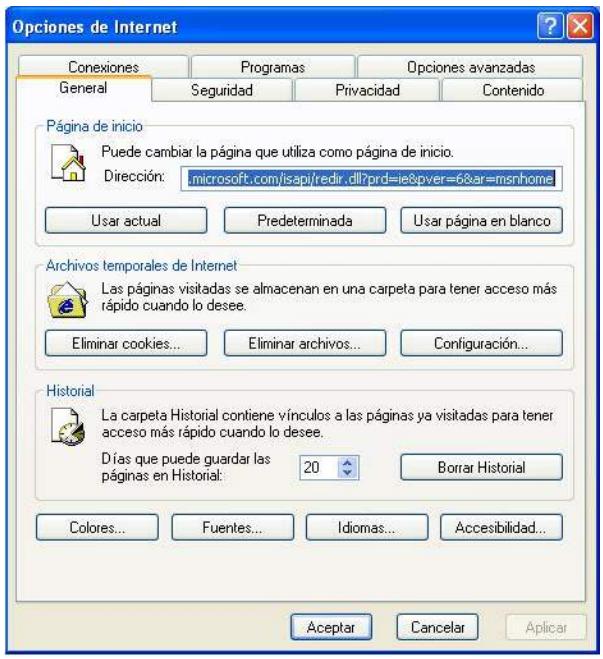
Ahora Firefox está configurado para usar un proxy HTTP.

Microsoft Internet Explorer

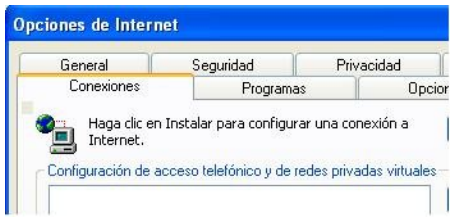
Configurar Internet Explorer para usar un proxy HTTP:

1. En el menú “Herramientas”, clic en “Opciones de Internet”

2. Internet Explorer muestra la ventana “Opciones de Internet”:



3. Clic en el tabulador “Conexiones”:



4. Clic “Configuración de LAN”. La ventana Configuración de red de área local aparece:

5. Seleccionamos “Utilizar un servidor proxy para su LAN”:
6. Clic en “Opciones avanzadas”. La configuración de servidores proxy aparece:

7. Entramos “Dirección del servidor proxy” y número de “Puerto” en la primera fila de campos.
8. Si hacemos clic en “Usar el mismo servidor proxy para todos los protocolos”, Internet Explorer intentará enviar tráfico HTTPS (HTTP seguro) y FTP a través del proxy. Esto puede que no funcione si estamos usando un proxy de aplicaciones público, pues muchos de ellos no soportan HTTPS y FTP. Si, por otra parte nuestro tráfico HTTPS y/o FTP está siendo bloqueado, podemos intentar con un proxy de aplicaciones público con soporte para HTTPS y/o FTP y usar la opción “Usar el mismo proxy para todos los protocolos” en Internet Explorer.

Ahora Internet Explorer está configurado para usar un proxy HTTP.

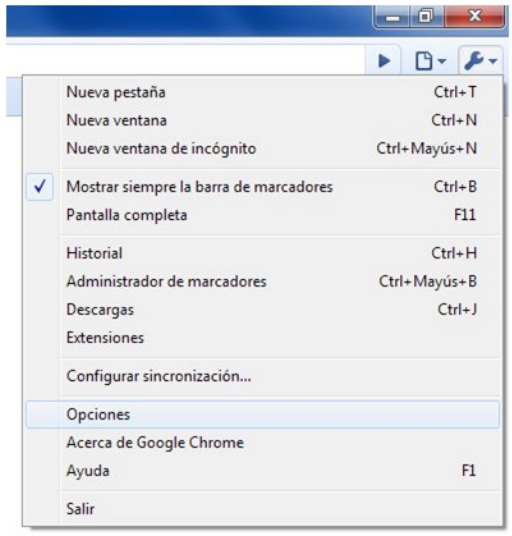
Google Chrome

Si cambiamos esas configuraciones se afecta Google Chrome como Internet Explorer y otros programas de Windows. Si configuramos nuestro proxy HTTP a través de Internet Explorer entonces no necesitamos seguir estos pasos.

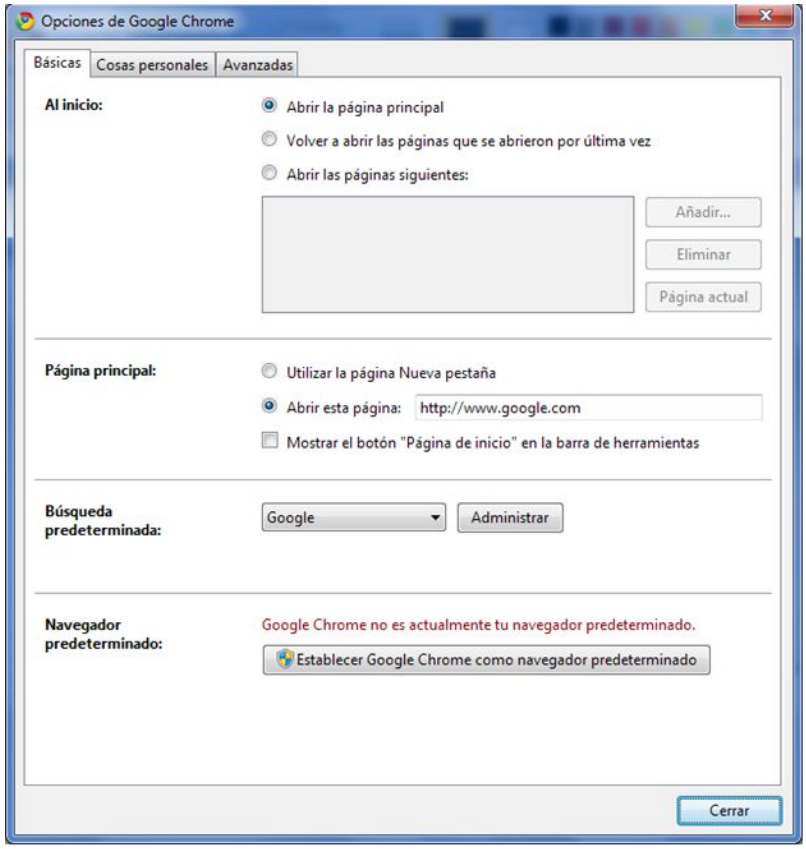
Sigamos estos pasos para configurar nuestro proxy HTTP:

1. Hacemos clic en el menú "Customize and control Google Chrome" (la llave pequeña próxima a la barra de direcciones URL):

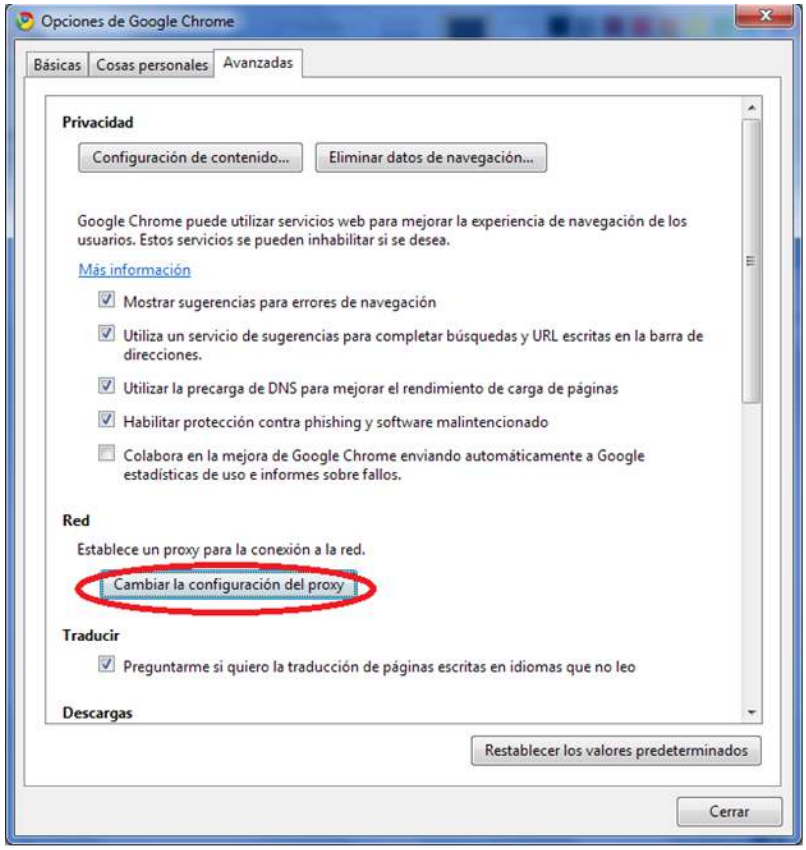
2. Clic en Options.



3. En la ventana Google Chrome Options, seleccionamos la pestaña Under the Hood:



4. En la sección Network, clic en el botón "Change proxy settings":



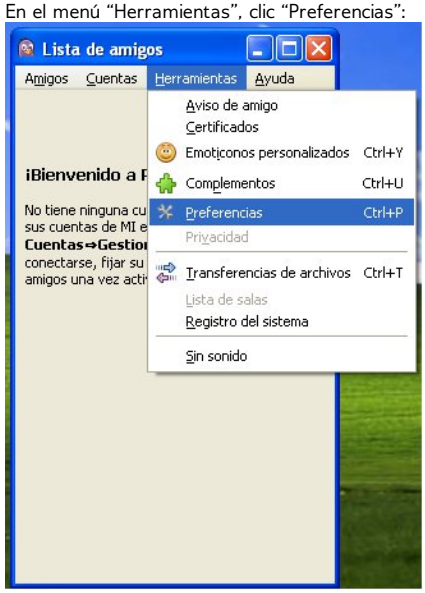
5. Se abrirá la ventana Internet Options. Seguimos los pasos del 2 al 8 de “Cómo configurar un proxy HTTP de Internet Explorer” para terminar de configurar el proxy HTTP.

Chrome está configurado para usar el proxy HTTP.

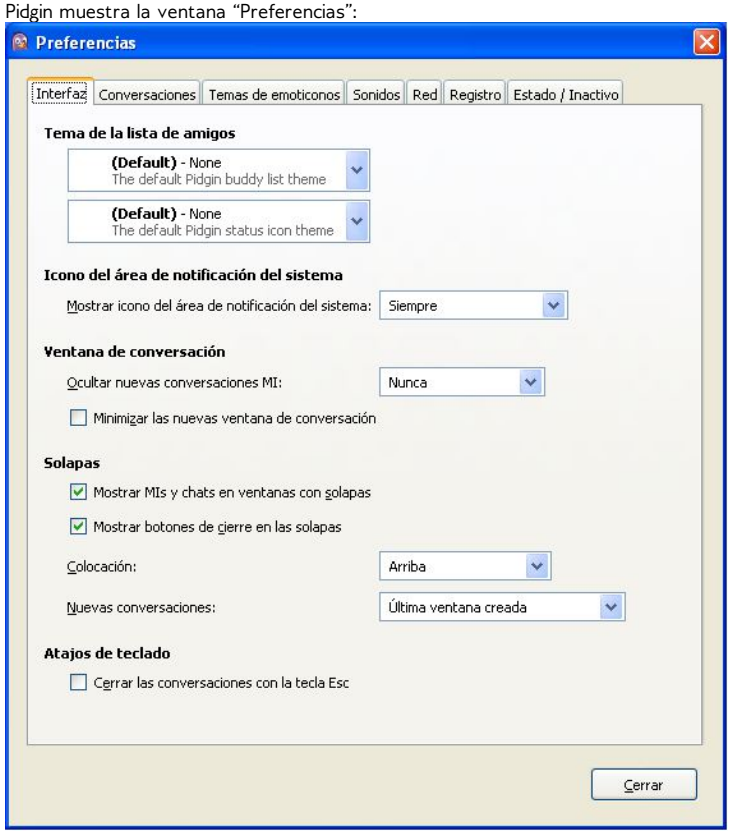
Cliente de mensajería instantánea Pidgin

Algunas aplicaciones que no son navegadores Web pueden también usar un proxy HTTP para conectarse a Internet y potencialmente evadir el bloqueo. Presentamos el ejemplo del programa de mensajería instantánea Pidgin.

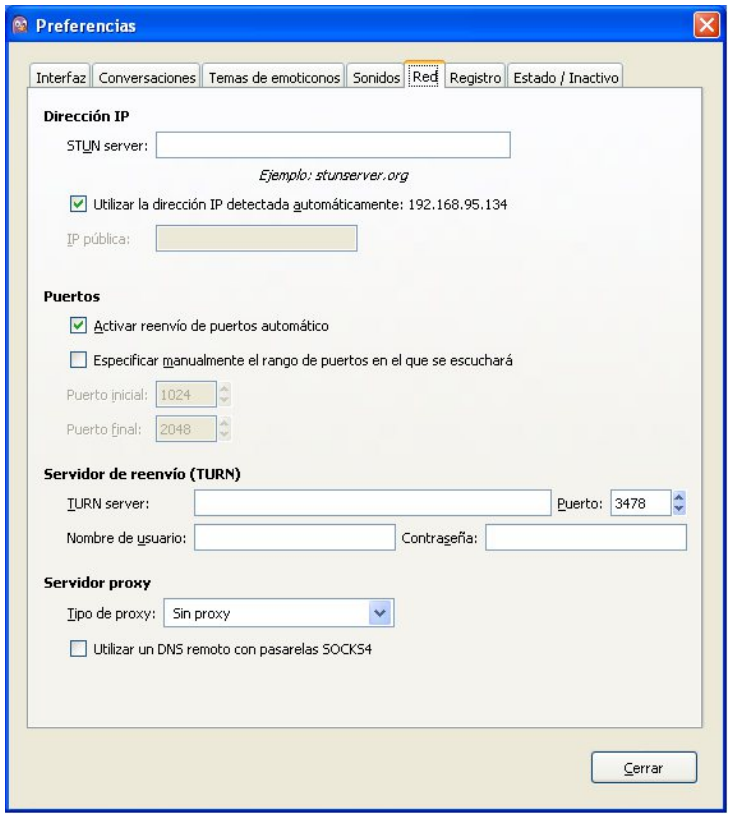
1. En el menú “Herramientas”, clic “Preferencias”:



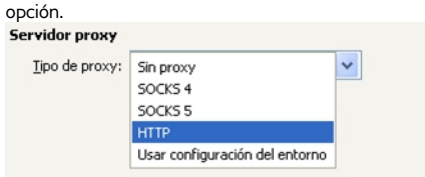
Pidgin muestra la ventana “Preferencias”:



2. Clic en la pestaña “Red”:



3. En la opción “Proxy type” seleccionamos “HTTP”. Aparecen campos adicionales bajo esa opción.



4. Entramos la dirección del “Host”y el número de puerto de nuestro proxy HTTP.

5. Clic “Cerrar”.

Ahora Pidgin está configurado para usar el proxy HTTP.

Cuando terminamos con el proxy

Cuando terminamos de usar el proxy, particularmente en una computadora compartida, reingresamos la configuración que cambiamos a sus valores previos. De lo contrario esas aplicaciones seguirán intentando usar el proxy. Esto puede ser un problema si no queremos que otras personas sepan que estábamos usando ese proxy o si estábamos usando un proxy local proporcionado por una aplicación de evasión de censura en particular que no se está ejecutando todo el tiempo.

29. LA LÍNEA DE COMANDO

Antes de proseguir con el resto de éste libro, sería bueno echarle un vistazo a como funciona la línea de comando. Este capítulo está pensado para que aquellos que no están familiarizados con la línea de comandos se ubiquen rápido.

LO BÁSICO

Aunque éstas interacciones son tan rápidas que no nos detenemos a pensar en ellas, cada clic o golpe de teclado es un comando en la computadora. Usar la línea de comando es la misma cosa, pero más premeditadamente. Escribimos un comando y presionamos Enter. Por ejemplo, en un terminal se escribe:

```
date
```

Y el ordenador responde:

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

Esto último tiene el aspecto de algo bastante avanzado. En capítulos posteriores se explicará como solicitar la fecha y la hora en un formato más amigable. Se explicará también cómo funcionan en diferentes países y como cambia el resultado en diferentes idiomas. La idea por ahora es que hayamos tenido una interacción.

LA LÍNEA DE COMANDO PUEDE HACERLO MUCHO MEJOR

El comando *date*, como se ha visto, se compara con la alternativa de dar una ojeada en el calendario o el reloj. El problema principal no es solo la apariencia de la salida, que ya se mencionó, sino la inhabilidad de hacer algo con el valor de salida. Por ejemplo, si se busca la fecha para insertarla en un documento que se está escribiendo o actualizar un evento de un calendario en línea, habría que reescribirla varias veces. La línea de comando puede hacer algo mejor.

Después que aprendamos los comandos básicos y algunas formas útiles de ahorrar tiempo, encontraremos más en este libro acerca de cómo pasarle las salidas de unos comandos a otros comandos, automatizando actividades, y salvando comandos para su uso posterior.

¿A QUÉ NOS REFERIMOS CUANDO HABLAMOS DE COMANDO?

Al principio de este capítulo se usó la palabra *comando* de forma muy general para hacer referencia a cualquier forma de decirle a una computadora lo que debe hacer. Pero en el contexto de este libro, un comando tiene un significado muy específico. Es un fichero en nuestra computadora que se puede ejecutar, o en algunos casos una acción que se construye en un programa shell. Excepto para los comandos integrados, el ordenador ejecuta cada comando encontrando el programa que lleva su nombre y ejecutándolo. Detallaremos esto en la medida que sea necesario.

FORMAS DE ENTRAR COMANDOS

Para seguir con este libro necesitamos abrir un intérprete de líneas de comando o una **interfaz de línea de comandos** (llamada **shell** o terminal en GNU/Linux) en nuestra computadora. Las pantallas pre-gráficas se presentaban a las personas tan pronto como se registraban en el sistema. Hoy en día casi todo el mundo usa interfaz gráfica excepto los administradores profesionales de sistemas, aunque la pre-gráfica es más fácil y rápida de usar para muchos propósitos. A continuación se mostrará como levantar un shell.

ENCONTRANDO UN TERMINAL

En Linux podemos obtener una interfaz de terminal desde el escritorio, pero sería más fácil dejar el escritorio y usar solo el terminal original de solo texto. Para hacer esto, usamos la combinación de teclas <ctrl + alt + F1>. Tenemos una ventana en blanco con una invitación a registrarnos. Ponemos nuestro nombre de usuario y contraseña. Podemos ir a otros terminales con < alt + F2 > y así, y entrar varias sesiones con diferentes usuarios (o el mismo) para cualquier tarea que queremos llevar a cabo. En cualquier momento, podemos intercambiar de una a otra usando < alt + F# > con el número de la queremos utilizar. Una de esas, probablemente F7 o F8, nos llevará de regreso al escritorio. En los terminales de texto podemos usar el mouse (asumiendo que nuestro sistema tenga gpm ejecutándose) para seleccionar una palabra, línea o rango de líneas. Podemos pegar ese texto en algún lugar en ese terminal o en otro.

Las distribuciones GNU/Linux vienen con interfaces de usuario diferentes (GUI) y ofrecen diferentes metáforas estéticas y semánticas. Aquellas que se ejecutan en el sistema operativo se conocen como *entornos de escritorio*. GNOME, KDE y Xfce son los más usados. Virtualmente cada entorno de escritorio, tiene un programa que imita a los viejos terminales de solo texto que las computadoras solían tener como interfaz. En nuestro escritorio, intentemos buscar en el menú de aplicaciones por un programa llamado Terminal. Casi siempre es en un menú llamado Accesorios, lo que no es realmente apropiado porque después que leamos este manual estaremos mucho tiempo frente a un terminal todos los días.

En GNOME seleccionamos Aplicaciones > Accesorios > Terminal.

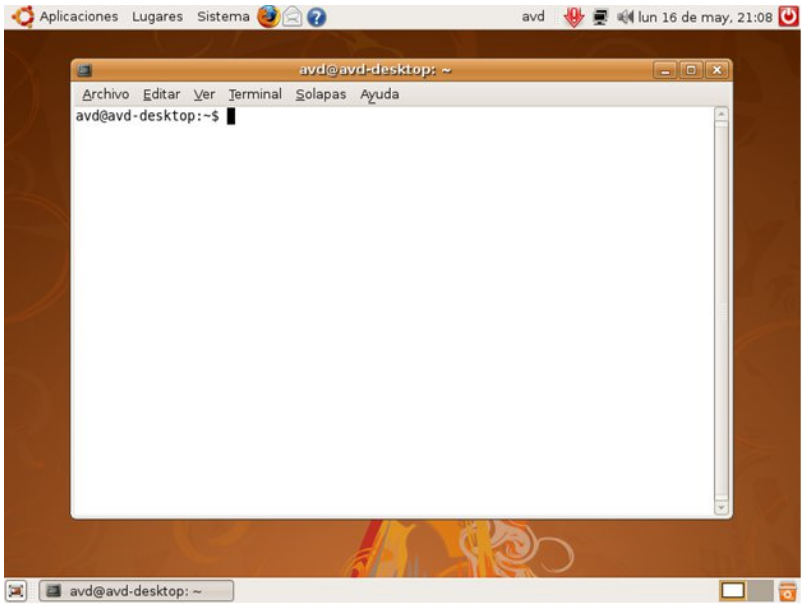
En KDE, seleccionamos K Menu -> Sistema-> Terminal.

En Xfce, seleccionamos Xfce Menu -> Sistema -> Terminal.

Donde quiera que esté ubicado, siempre podemos encontrar un programa terminal.

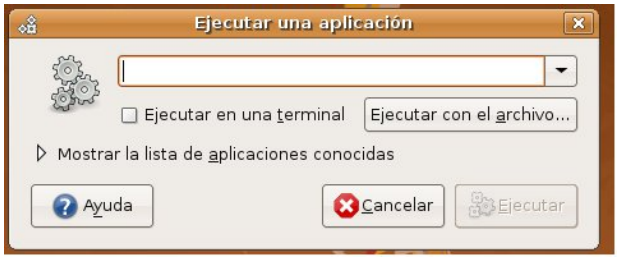
Cuando ejecutemos el terminal, solo muestra una ventana en blanco; no se ve mucha ayuda. Se espera que sepamos qué hacer – y se mostrará a continuación.

Las siguientes imágenes muestran la ventana Terminal abierta en el escritorio en GNOME.



EJECUTANDO UN COMANDO

Muchas interfaces gráficas brindan además una caja de diálogo pequeña llamada algo así como "Run command". Esta presenta un área de texto donde podemos escribir un comando y presionar Enter o retorno.



Para invocar esta caja de diálogo, intentemos teclear la combinación de teclas < alt + F2 >, o buscamos dentro del menú de aplicaciones. Podemos usar esta caja como un acceso directo para iniciar más rápido el programa terminal, siempre y cuando sepamos el nombre del programa terminal instalado en nuestra computadora. Si estamos trabajando en una computadora que no nos resulta familiar y no conocemos el nombre por defecto del programa terminal intentemos entrar `xterm` para iniciar un programa terminal de bajo costo (sin menú sofisticado que permita la opción de colores de fondo y tipos de letras). Si necesitamos desesperadamente estos menús sofisticados,

- en GNOME el programa terminal por defecto debe ser `gnome-terminal`,
- en KDE debe ser `konsole`
- en Xfce podemos intentar con `Terminal` o nombres de versiones específicas, por ejemplo en Xfce 4 debemos encontrar `xfce4-terminal`.

CÓMO MOSTRAMOS LOS COMANDOS Y LAS SALIDAS EN ESTE CAPÍTULO
Existe una convención en los libros acerca de la línea de comandos. Cuando iniciamos un terminal, veremos un pequeño mensaje indicando que el terminal está listo para aceptar nuestro comando. Este mensaje es llamado prompt, y puede ser tan simple como:

```
$
```

Después que entramos el comando y presionamos Enter, el terminal muestra la salida del comando (si hay alguna) seguida de otro prompt. Así que nuestra primera interacción mostrada en el libro sería:

```
$ date
Thu Mar 12 17:15:09 EDT 2009
$
```

Necesitamos saber cómo interpretar los ejemplos como este anterior. Todo lo que debemos escribir aquí es date. Y presionamos la tecla Retorno. La palabra date en el ejemplo se escribe en cursiva para saber que es algo que escribimos. El resto es el resultado del comando.

30. OPENVPN

OpenVPN es una solución de red privada virtual (**VPN**) respetada, gratis y de código abierto. Funciona en la mayoría de las versiones de Windows (el soporte para Windows Vista se espera que llegue pronto), Mac OS X y Linux. OpenVPN está basado en **SSL**, lo que significa que usa el mismo tipo de **cifrado** que se usa cuando se visita un sitio Web seguro cuando la URL empieza con https.

INFORMACIÓN

Sistemas operativos soportados	
Localizaci	English, German, Italian, French and Spanish
Sitio Web	https://openvpn.net/index.php/open-source.html
Soporte	Forum: https://forums.openvpn.net

OpenVPN no es apropiado para uso temporal en Cibercafés o en cualquier lugar con computadoras compartidas donde no podemos instalar algún programa.

Para más información sobre VPNs y servicios VPN listos para usarse, podemos leer "Servicios VPN" en este manual.

En un sistema OpenVPN, hay una computadora configurada como servidor (en un lugar sin restricciones), y uno o más clientes. El servidor debe estar accesible desde Internet, no bloqueado por un cortafuego y con una dirección IP públicamente enrutable (en algunos lugares, la persona que establece el servidor debe solicitarlo a su ISP). Cada cliente se conecta al servidor y crea un "**túnel**" VPN a través del cual puede pasar el tráfico.

Hay proveedores OpenVPN comerciales como WiTopia (http://witopia.net/personalmore.html) donde podemos adquirir acceso a un servidor OpenVPN por un pago de 5 a 10 USD por mes. Estos proveedores nos ayudarán a instalar y configurar OpenVPN en la computadora. Una lista de estos proveedores comerciales está disponible en http://en.cship.org/wiki/VPN.

OpenVPN también puede usarse por un contacto confiable en un lugar sin filtrar, brindando un servidor OpenVPN a uno o más clientes y pasar el tráfico a su computadora antes de continuar en Internet. Sin embargo, configurar esto correctamente es algo complicado.

CONSEJOS PARA CONFIGURAR OPENVPN

Para configurar un servidor OpenVPN y un cliente podemos seguir la documentación que brinda OpenVPN (http://openvpn.net/index.php/documentation/howto.html). Si deseamos usar OpenVPN para visitar sitios Web, las siguientes notas son importantes:

Cliente

Hay una interfaz gráfica de usuario (GUI) disponible para Windows lo que hará más fácil iniciar y detener OpenVPN cuando se requiera, y también permite configurar OpenVPN para usar un proxy HTTP para acceder a Internet. Para descargar la GUI podemos ir a:http://openvpn.se.

Para configurar OpenVPN para usar un servidor proxy en Linux o Mac OS X, podemos leer la sección relativa a ello en el sitio Web:
(http://openvpn.net/index.php/documentation/howto.html#http).

Servidor

- Cuando tengamos que elegir entre enrutar o puentear, no hay ventaja adicional en configurar puentes cuando nuestros clientes solo desean usarlo para evadir la censura de Internet. Seleccionemos enrutar.
- Debemos prestar especial atención a la sección de la guía que explica como asegurarse de que el tráfico del cliente pasa a través del servidor. Sin esta configuración el sistema no nos ayudará a visitar páginas bloqueadas (http://openvpn.net/index.php/documentation/howto.html#redirect).
- Si la computadora del cliente está detrás de un cortafuego muy restrictivo, y el puerto por defecto del OpenVPN está bloqueado, es posible cambiar el puerto de OpenVPN que usa. Una opción es usar el puerto 443, el cual normalmente es usado para sitios web seguros (**HTTPS**), y para cambiar a protocolo **TCP** en lugar de **UDP**. En esta configuración, es difícil para el operador del cortafuego decir la diferencia entre tráfico OpenVPN y tráfico seguro normal Web. Para hacer eso, cerca del tope del fichero de configuración en ambos; el cliente y el servidor, reemplazamos "proto udp" con "proto tcp" y "port 1194" con "port 443".

VENTAJAS Y RIESGOS

Una vez que esté configurado correctamente, OpenVPN puede brindar una forma efectiva de evadir el filtrado en Internet. Puesto que todo el tráfico está encriptado entre el cliente y el servidor, y puede pasar a través de un puerto simple, es muy difícil distinguir este tráfico de otro tráfico Web seguro, como pueden ser datos que viajan a una tienda en línea u otro tipo de servicio encriptado.

OpenVPN puede usarse para todo el tráfico de Internet, incluyendo tráfico Web, correo electrónico, mensajería instantánea y Voz sobre IP (**VoIP**).

OpenVPN además brinda un grado de protección contra la vigilancia o supervisión, en la medida en que se pueda confiar en el dueño del servidor OpenVPN y si se han seguido las instrucciones en la documentación de OpenVPN que explican cómo manejar las llaves y certificados que han de usarse. Hay que recordar que el tráfico solo va codificado hasta el servidor OpenVPN, a partir de él pasa decodificado por Internet.

La desventaja principal de OpenVPN es lo difícil de su instalación y configuración. Además requiere acceso a un servidor en una zona sin restricciones y no brinda anonimato real y fidedigno.

31. SSH TUNNELLING

SSH, (Secure Shell), es un protocolo estándar que cifra las comunicaciones entre el ordenador y el servidor. El cifrado impide que estas comunicaciones sean vistas o modificadas por los operadores de red. SSH puede ser usado por una gran variedad de aplicaciones de comunicaciones seguras, donde lo más común es el acceso seguro a los servidores y la transferencia de ficheros segura (SCP o SFTP).

SSH es especialmente útil para evadir la censura porque puede proveer túneles cifrados y trabajar como un cliente proxy genérico. Los censuradores normalmente no bloquean completamente el SSH porque se usa para muchos propósitos y no solo para evadir la censura; por ejemplo, es usado por los administradores de sistema para administrar sus servidores en Internet.

Usar SSH requiere de una cuenta en un servidor, generalmente un servidor Linux o Unix. Para evadir la censura este servidor necesita tener acceso sin restricciones a Internet e, idealmente ser operado por un contacto confiable. Algunas compañías también venden cuentas en sus servidores, y muchos sitios de hospedaje brindan acceso SSH. Se puede encontrar una lista de proveedores de cuentas en: http://www.google.com/Top/Computers/Internet/Access_Providers/Unix_Shell_Providers que venden cuentas entre los 2 y 10 USD por mes.

Un programa SSH llamado OpenSSH viene instalado en la mayoría de los Unix, Linux y Mac OS y consiste en un programa de líneas de comando ejecutado desde un terminal como “ssh”. Para Windows también se puede obtener una implementación SSH llamada PuTTY.

Todas las versiones recientes que soportan SSH crean un proxy **SOCKS** que permiten que un navegador Web y otras variedades de aplicaciones usen conexiones SSH cifradas para conectarse con Internet sin restricciones. En este ejemplo, solo se describe este uso de SSH. Los pasos a continuación configuran un Proxy SOCKS en un puerto local 1080 en la computadora.

LINEA DE COMANDO EN LINUX/UNIX Y MACOS (CON OPENSSH)

OpenSSH está disponible en http://www.openssh.com/, pero viene pre instalado en Linux/Unix y Mac OS.

El comando ssh que se ejecutará contiene un puerto local (típicamente 1080), un nombre de servidor y un nombre de usuario (nombre de cuenta). El comando sería así:

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

Por ejemplo:

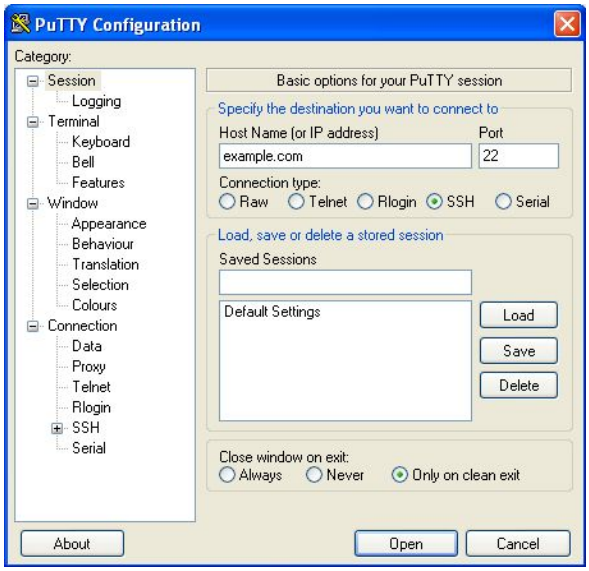
Se nos pedirá la contraseña y se establecerá la conexión con el servidor. Con el uso de la opción –D, se creará un Proxy SOCKS que existirá mientras se esté conectado al servidor. Importante: debemos verificar la llave del host y configurar nuestras aplicaciones, de otra forma no estaremos usando el túnel que creamos.

INTERFAZ DE USUARIO GRÁFICA DE WINDOWS (WITH PUTTY)

PuTTY está disponible en :
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

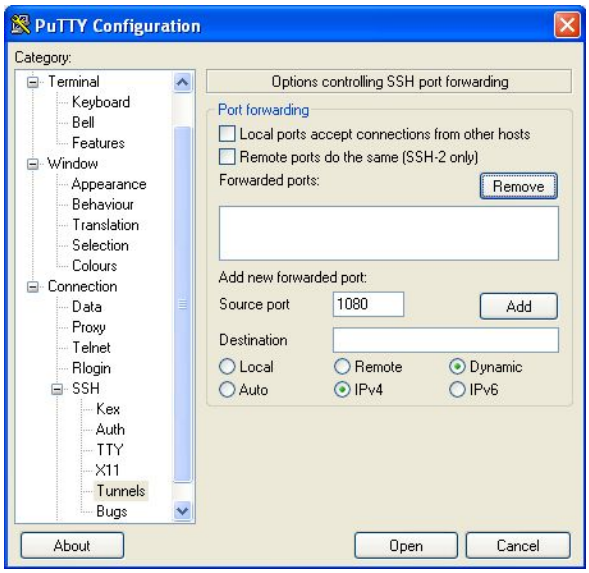
Podemos salvar el programa putty.exe en el disco duro para usos futuros, o ejecutarlo directamente desde el sitio Web (a menudo, esto es posible en una computadora compartida o con acceso público como las de las librerías o Cibercafés).

Cuando iniciamos PuTTY, aparece un diálogo de configuración de sesión. Primero entramos el nombre (dirección) del servidor SSH al que queremos conectarnos (aquí, "ejemplo.com"). Si solo conocemos la dirección IP o si el DNS impide usar el nombre de los servidores, podemos usar la dirección IP. Si ejecutamos estos pasos frecuentemente, podemos crear opcionalmente un perfil PuTTY para salvar estas opciones que se describen anteriormente para usarlas cada vez que se necesiten.

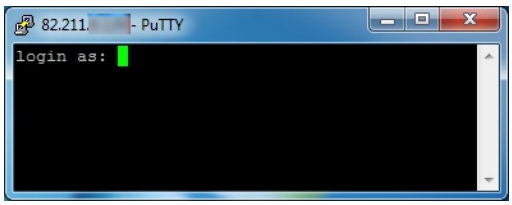


Después en la lista, Category, seleccionamos Connection, después SSH, y después Tunnels.

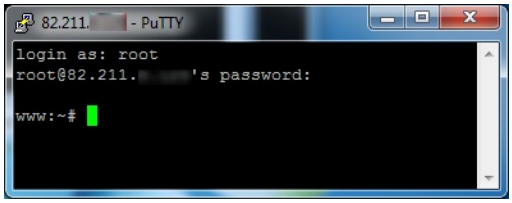
Entramos 1080 en el campo Source port, y seleccionamos las cajas Dynamic e IPv4.



Ahora hacemos clic en el botón Add y después en el botón “Open”. Se establece una conexión con el servidor, y se abre una ventana pidiendo el nombre de usuario y la contraseña.



Entramos esta información y estaremos registrados en el servidor y recibiremos un prompt de una línea de comando desde el servidor. El proxy SOCKS está establecido. Importante: debemos verificar la llave del host y configurar nuestras aplicaciones, de otra forma no estaremos usando el túnel que creamos.



VERIFICACIÓN DE LA LLAVE DE HOST

La primera vez que nos conectamos a un servidor, debemos confirmar la *impresión digital de ese servidor*. La impresión digital es una secuencia larga de letras y números (hexadecimales) ej. 57:ff:c9:60:10:17:67:bc:5c:00:85:37:20:95:36:dd que identifica de forma segura a un servidor en particular. Chequear la impresión digital es una medida de seguridad que permite confirmar que estamos comunicando con el servidor que pensamos, y que la conexión cifrada no está siendo interceptada.

SSH no brinda un medio de verificar esto automáticamente. Para obtener el beneficio de este mecanismo, debemos tratar de chequear el valor de la firma digital del servidor con el administrador del servidor que estamos usando, o pedirle a un contacto de confianza que intente conectarse al mismo servidor para ver si ve la misma firma digital.

Verificar la firma digital es importante para asegurarnos que SSH protege la privacidad de las comunicaciones de la curiosidad de terceros, pero no es necesario si solo deseamos evadir la censura y no nos importa si los operadores de redes pueden ver el contenido de las comunicaciones.

CONFIGURANDO APLICACIONES PARA USAR EL PROXY

El Proxy creado en los pasos anteriores debe trabajar hasta que se cierre el programa SSH. Sin embargo, si se interrumpe la conexión al servidor, se necesitará repetir los mismos pasos para reactivar el Proxy.

Una vez que el Proxy esté ejecutándose, necesitamos configurar las aplicaciones para usarlo. Para ello veremos los pasos a continuación, el Proxy será un Proxy SOCKS localizado en localhost, puerto 1080 (también conocido como 127.0.0.1, puerto 1080). Debemos asegurarnos que las aplicaciones estén configuradas de forma que impida la **fuga de DNS**, lo que puede hacer menos efectivo a SSH en cuanto a protección de privacidad y evasión de censura.

MÁS OPCIONES

Hasta el momento, todos estos comandos muestran una línea de comando en la máquina remota desde la que podemos ejecutar los comandos. Algunas veces podemos querer ejecutar un comando simple en una máquina remota, que se devuelva después a nuestra línea de comandos en la maquina local. Esto se puede lograr poniendo el comando que queremos ejecutar en la máquina remota entre comillas simples.

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

Algunas veces lo que necesitamos es ejecutar comandos que consumen mucho tiempo en una máquina remota, pero no estamos seguros de tener suficiente tiempo durante la sesión actual ssh. Si cerramos la conexión remota antes de que una ejecución de comandos se haya completado, ese comando será abortado. Para evitar perder nuestro trabajo, podemos empezar por la vía ssh una sesión screen remota y separarla y reconectarnos cada vez que queramos. Para separar una sesión remota, simplemente cerramos la conexión ssh: una sesión aparte se mantendrá ejecutándose en la máquina remota.

`ssh` ofrece muchas más opciones, que se describen en la página del manual. Podemos configurar nuestro sistema favorito para permitir registrarnos o ejecutar comandos sin especificar nuestra contraseña todo el tiempo. La instalación es complicada pero puede ahorrarnos bastante interacción con el teclado; intentemos algunas búsquedas web con "ssh-keygen", "ssh-add", y "authorized_keys".

SCP: COPIA DE FICHEROS

El protocolo SSH se extiende más allá del comando ssh. Un comando particularmente útil basado en el protocolo SSH es scp (secure copy command). El siguiente ejemplo copia ficheros del directorio actual de nuestra máquina local al directorio /home/me/stuff en una máquina remota.

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

Debemos tener en cuenta que el comando sobrescribirá cualquier fichero con el mismo nombre /home/me/stuff/myprog.py. (O tendremos un mensaje de error si hay un fichero con el mismo nombre y no tenemos privilegios para sobrescribirlo). Si /home/me es nuestro directorio, el directorio destino puede abreviarse.

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

Podemos fácilmente copiar en la otra dirección: de la máquina remota a la local.

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

El fichero en la máquina remota es *interview.txt* en el subdirectorio docs de nuestro directorio. El fichero será copiado en *yesterday-interview.txt* en nuestro directorio en el sistema local

`scp` puede usarse para copiar un fichero de una máquina remota a otra.

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

Para copiar recursivamente todos los ficheros de un subdirectorio a un directorio, usamos la opción –r.

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

Podemos ver la página man de scp para más opciones.

RSYNC: TRANSFERENCIAS Y COPIAS DE SEGURIDAD AUTOMÁTICAS

`rsync` es un comando muy útil que mantiene un directorio remoto en sincronía con un directorio local. Se menciona aquí porque es una forma muy útil de trabajo en red, como ssh, y porque el protocolo `ssh` es recomendado como transmisión fundamental para `rsync`.

El siguiente es un ejemplo simple y útil. Copia ficheros desde nuestro directorio local `/home/myname/docs` a un directorio llamado `backup/` en nuestro directorio en el sistema quantum.example.edu. Rsync actualmente minimiza la cantidad de copias necesarias a través de varios chequeos sofisticados.

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

La opción –e ssh es para usar el protocol SSH bajo la transmisión, como se recomienda. La opción –a (que significa "archivo") copia cualquier cosa con el directorio especificado. Si deseamos eliminar los ficheros en el sistema local mientras se van copiando, incluimos la opción a –delete. Para más detalles podemos la página del manual acerca de rsync.

HACIÉNDONOS LA VIDA MÁS FÁCIL CUANDO USAMOS SSH CON FRECUENCIA

Si usamos SSH para conectarnos a muchos servidores diferentes, podemos a veces cometer errores escribiendo sus nombres y nuestro nombre de usuario (imaginemos si tenemos que recordar 20 combinaciones nombres de usuario/nombres de servidor). Afortunadamente, SSH ofrece un método simple para manejar la información de sesión a través de un fichero de configuración.

El fichero de configuración está oculto en nuestro directorio bajo el directorio .ssh (el path completo sería algo así */home/jsmith/.ssh/config* – si el fichero no existe podemos crearlo). Usamos nuestro editor favorito para abrir el fichero y especificamos los hosts así:

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

Podemos configurar múltiples hosts en nuestro fichero de configuración, y cuando lo salvemos nos conectamos al host que nombramos "dev" ejecutando el siguiente comando:

```
$ ssh dev
```

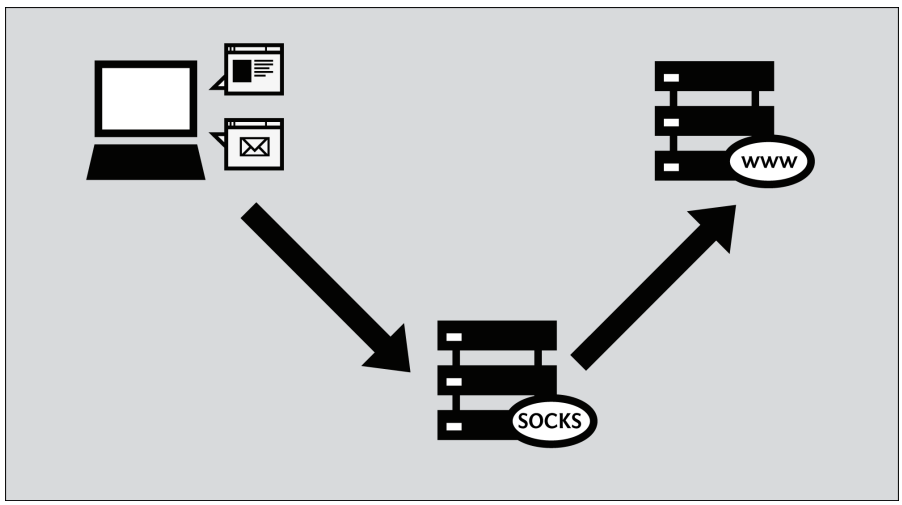
Es necesario recordar, que mientras más usemos estos comandos más tiempo ganamos.

32. PROXIS SOCKS

SOCKS es un **protocolo de Internet** que presenta un tipo de **servidor proxy** especial. El puerto por defecto para SOCKS es el 1080, pero puede estar también disponible en otros puertos. La diferencia funcional con los proxis HTTP es que los proxis SOCKS no solo funcionan para la navegación Web, sino también para otras aplicaciones como juegos de video, transferencia de ficheros o clientes de mensajería instantánea. Similar a un VPN, funciona como un túnel seguro.

Las versiones comunes de SOCKS incluyen la 4, 4ª y 5. La versión 4 siempre necesita la dirección IP para crear la conexión, así que el DNS aún tiene que intervenir en el cliente. Esto hace que no sea útil para muchas necesidades de evasión. La versión 4ª usualmente usa nombres de hosts. La versión 5 incluye nuevas técnicas como autenticación, **UDP** e IPv6, pero casi siempre usa direcciones IP, así que puede que no sea la solución perfecta. Podemos ver también la sección "Fuga de DNS" al final de este capítulo.

Una variedad de proxis puede tomar ventajas de un Proxy SOCKS para evadir el filtrado u otras restricciones – no solo los navegadores Web, sino otras aplicaciones como las de mensajería instantánea y de correo electrónico.



Aunque los proxis SOCKS públicos existen, en la mayoría de los casos se ejecutarán en la computadora de forma local, y serán facilitados por una aplicación. Como los túneles SOCKS son tan flexibles, algunos programas de evasión de censura crean un Proxy local que se ejecuta en nuestra propia computadora (al cual usualmente nos referimos como localhost o la dirección IP 127.0.0.1). Este Proxy local es una forma de permitir que aplicaciones como el navegador Web tomen ventajas del programa de evasión. Algunas herramientas que trabajan de esta forma incluyen a Tor, Your-Freedom y túneles SSH configurados con PuTTY.

Aqui se muestra una camiseta para entusiastas de los proxis locales (similar a "no hay nada como estar en casa").

Con el propósito de usar un Proxy de aplicación para evadir la censura, debemos decirle a nuestros programas de computadora que deseamos comunicarnos con un Proxy cuando nos comuniquemos con otros sistemas en Internet.

Algunas aplicaciones no trabajan con un Proxy porque sus desarrolladores no las crearon con soporte para Proxy. Sin embargo, muchas de estas aplicaciones pueden trabajar con un Proxy SOCKS usando un programa "*socksifier*". Algunos ejemplos de estos programas incluyen:

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

CONFIGURANDO NUESTRAS APLICACIONES

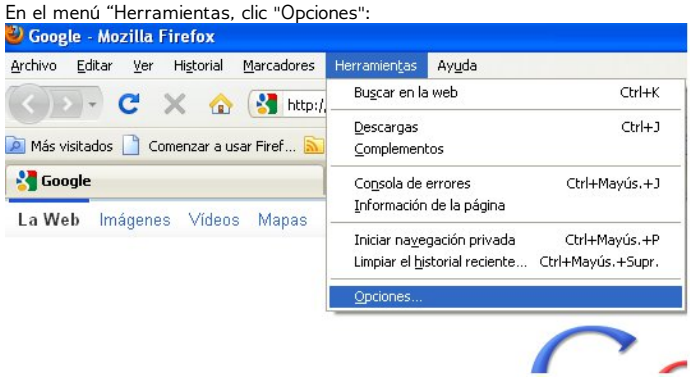
En la mayoría de los casos en los que se configuran proxis SOCKS se hace muy parecido a los proxis HTTP. Las aplicaciones que tienen soporte para proxis SOCKS tienen una entrada separada en el menú o diálogo de configuración donde se configuran los proxis HTTP para configurar proxis SOCKS. Algunas aplicaciones piden seleccionar entre SOCKS 4 y SOCKS 5 y en la mayoría de los casos SOCKS 5 es la mejor opción, aunque algunos proxis solo trabajan con SOCKS 4.

Algunas aplicaciones, como Mozilla Firefox permiten configurar ambos tipos de proxis HTTP y SOCKS al mismo tiempo, el tráfico normal ocurrirá a través del Proxy HTTP, y Firefox utiliza el Proxy SOCKS para otro tráfico como el video streaming.

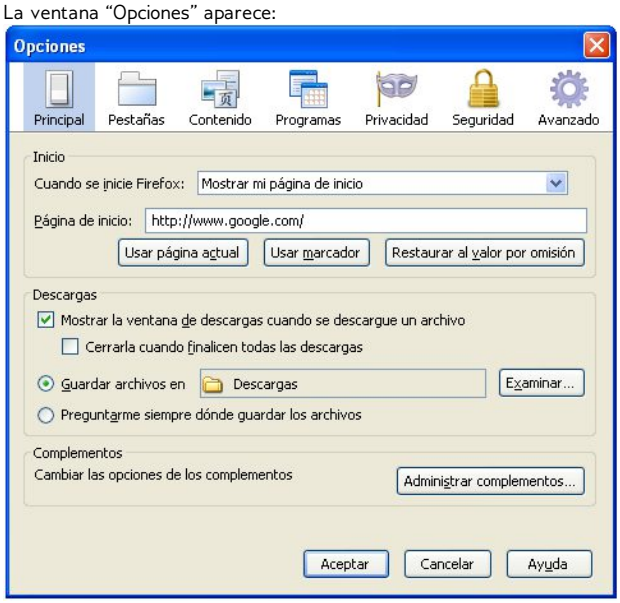
Mozilla Firefox

Entramos en la configuración como se muestra en la siguiente imagen y clic en "OK".

1. En el menú “Herramientas, clic "Opciones":



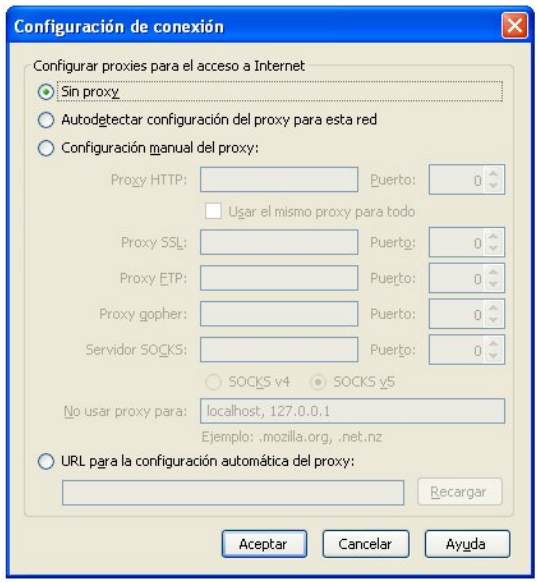
2. La ventana “Opciones” aparece:



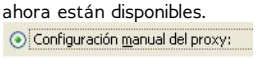
3. En la barra de herramientas en el tope de la ventana, clic "Avanzado":

4. Clic el tabulador “Red”:

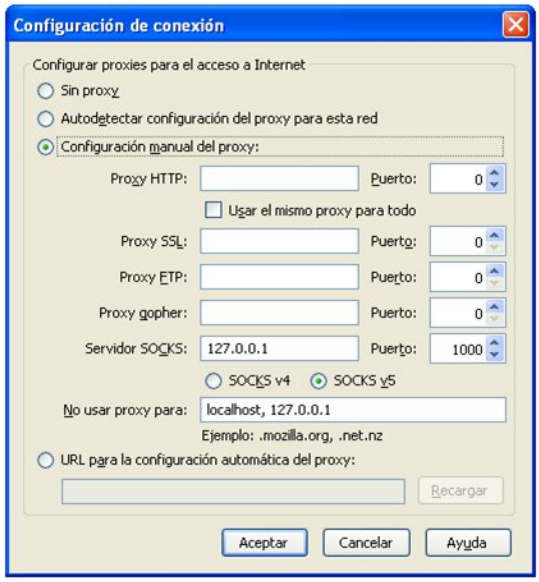
5. Clic "Configuración". Firefox muestra la ventana "Configuración de Conexión":



6. Seleccionamos "Configuración manual del proxy". Los campos de debajo de esa opción ahora están disponibles.



7. Entramos la dirección del Proxy SOCKS y número de puerto, seleccionamos "SOCKS v5" y clic en "OK".

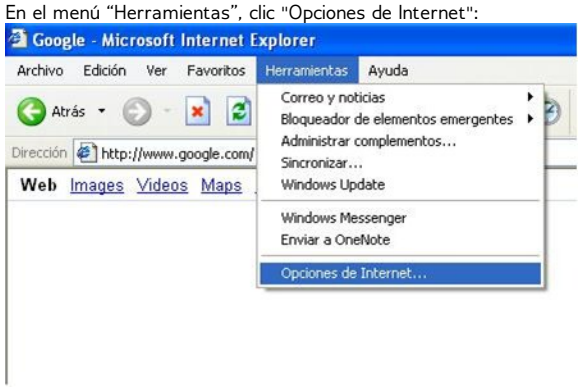


Ahora Firefox está configurado para usar un proxy SOCKS.

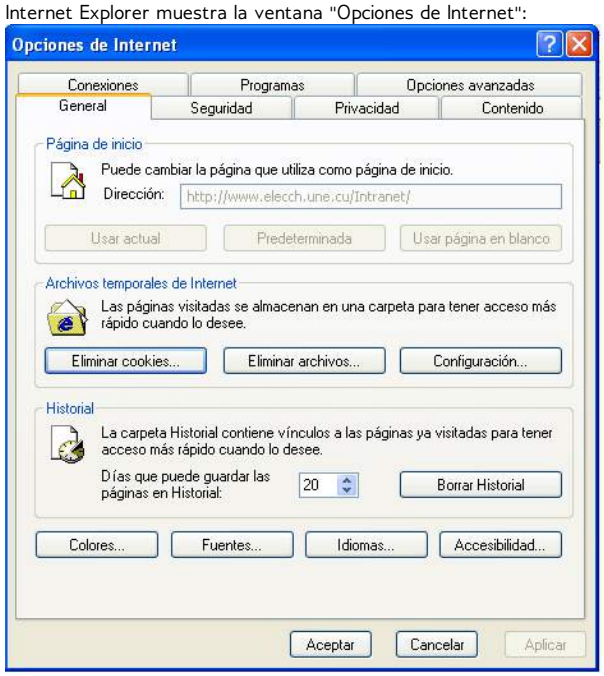
Microsoft Internet Explorer

Para configurar Internet Explorer para que use un proxy SOCKS:

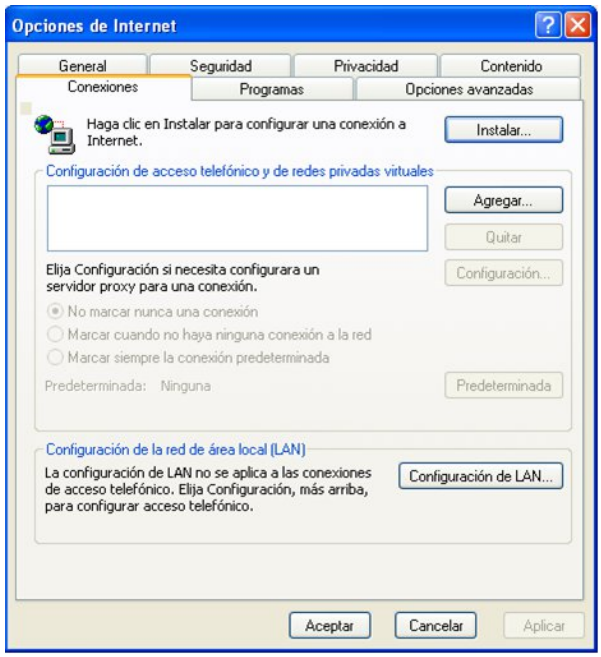
1. En el menú “Herramientas”, clic "Opciones de Internet":



2. Internet Explorer muestra la ventana "Opciones de Internet":



3. Clic en la pestaña “Conexiones”:



4. Clic "Configuración LAN". Internet Explorer muestra la ventana "Configuración de Red de área local (LAN) ":

5. Seleccionamos "Utilizar un servidor proxy para su LAN" y clic en "Opciones avanzadas". Internet Explorer muestra la ventana de "Configuración de Proxy".

6. Desmarcar "Usar el mismo servidor proxy para todos los protocolos " si está seleccionado.

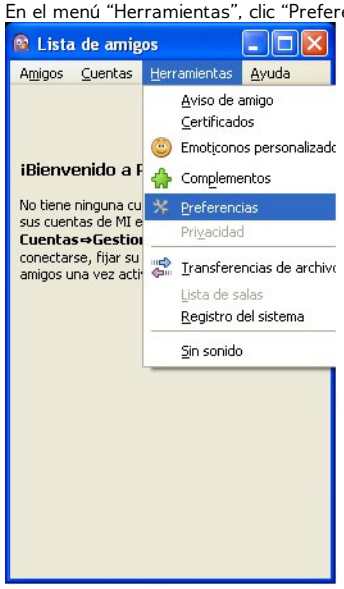
7. Entrar "Dirección proxy" y "Puerto" en la fila "Socks" y clic "OK":

Ahora Internet Explorer está configurado para usar un proxy SOCKS.

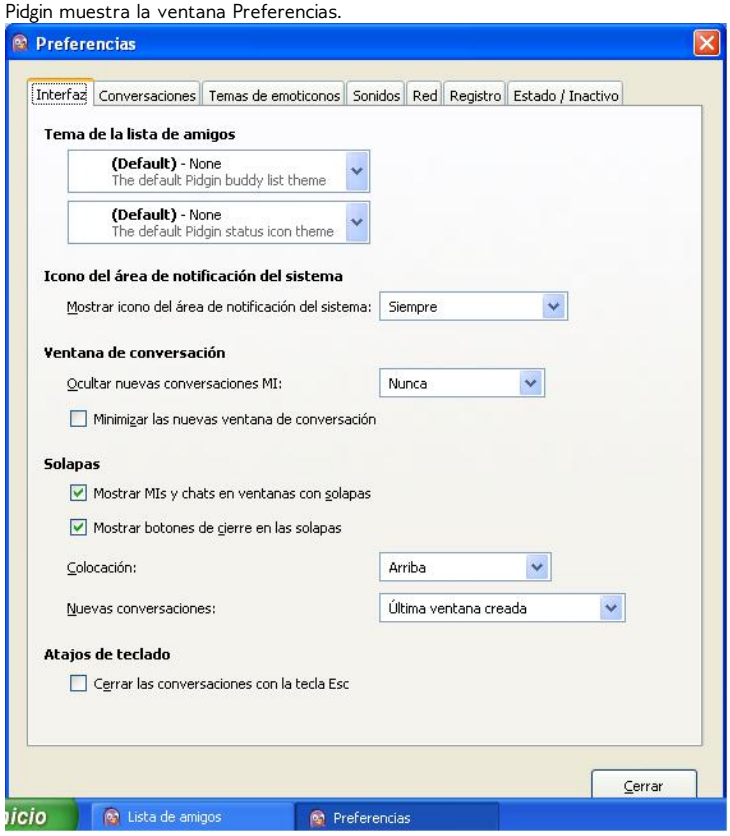
Configurando un proxy SOCKS para otras aplicaciones

Muchas aplicaciones de Internet aparte de los navegadores Web pueden usar un Proxy SOCKS para conectarse a Internet, traspasando de forma potencial el bloqueo y filtrado. Aquí hay un ejemplo con el programa de mensajería instantánea Pidgin. Este es un ejemplo típico, pero la secuencia exacta de pasos para configurar otras aplicaciones para que usen un Proxy SOCKS difiere ligeramente.

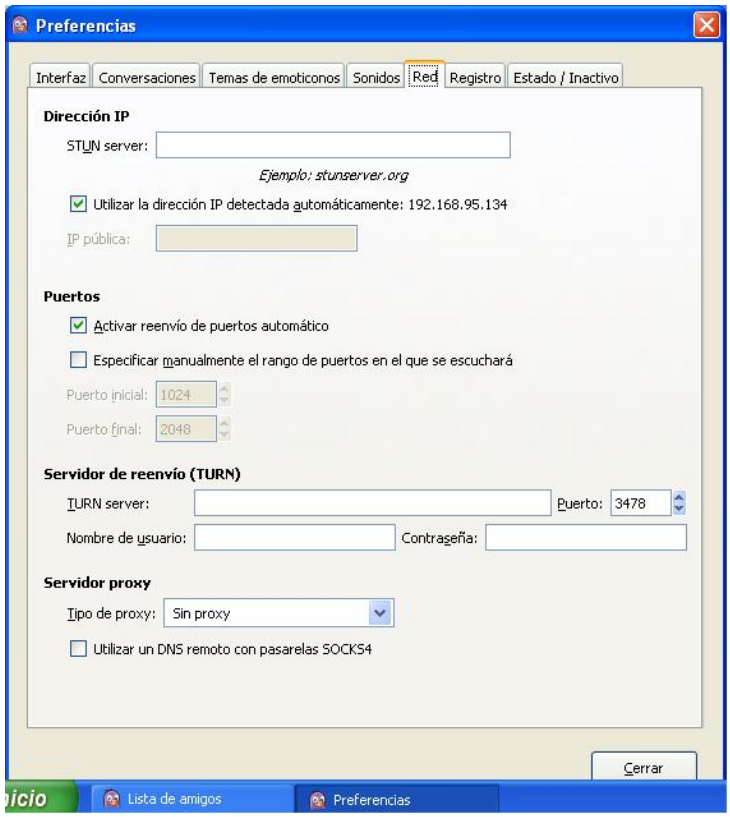
1. En el menú “Herramientas”, clic “Preferencias”.



2. Pidgin muestra la ventana Preferencias.

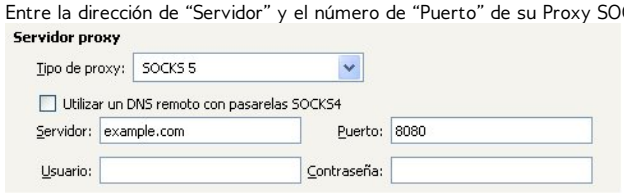


3. Clic en el tabulador “Red” para mostrarlo.



4. En “Tipo de proxy”, seleccionamos “SOCKS 5”. Aparecen campos adicionales debajo de esta opción.

5. Entre la dirección de “Servidor” y el número de “Puerto” de su Proxy SOCKS.



6. Clic “Cerrar”.

Pidgin está ahora configurado para usar un Proxy SOCKS.

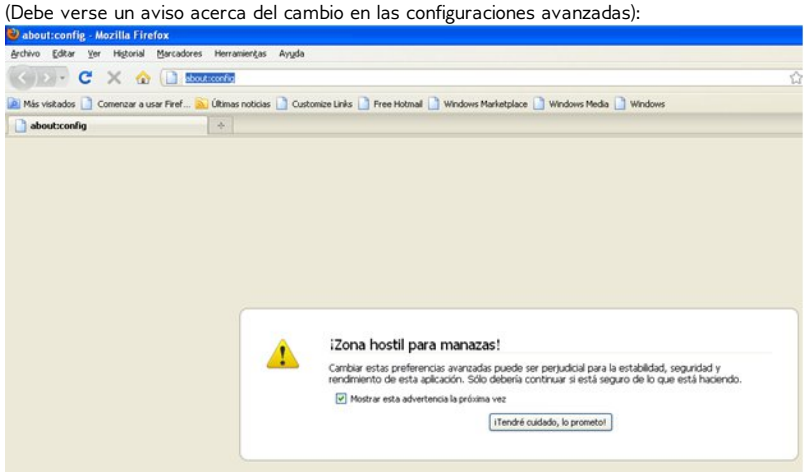
Cuando hayamos terminado con el Proxy

Cuando hayamos terminado con el Proxy, particularmente en una computadora compartida, regresamos la configuración que cambiamos a sus valores previos. De lo contrario, las aplicaciones continuarán intentando usar el Proxy. Esto puede ser un problema si no deseamos que las personas sepan que estuvimos usando un Proxy o si estuvimos usando un Proxy local de una aplicación de evasión que no sé está ejecutando todo el tiempo.

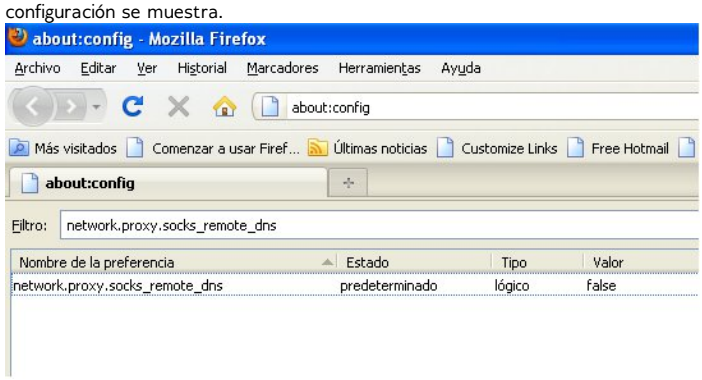
FUGA DE DNS

Un problema importante con los proxis SOCKS es que algunas aplicaciones que soportan el uso de proxis SOCKS puede que no usen el Proxy para todas sus comunicaciones de red. El problema más común es que las solicitudes del Sistema de Nombres de Dominios (DNS) pueden ser hechas sin ir a través del Proxy. Esta **fuga de DNS** puede ser un problema de privacidad y puede dejarnos vulnerables al bloqueo de DNS, al cual un proxy podía por otra parte haber evadido. El hecho de que una aplicación sea vulnerable a la fuga de DNS puede variar de versión a versión. Mozilla Firefox es actualmente vulnerable a la fuga de DNS en su configuración por defecto, pero se puede evitar esto haciendo un cambio de configuración permanente para prevenir la fuga de DNS:

1. En la barra de direcciones de Firefox, entramos `about:config` como si fuera una URL (Debe verse un aviso acerca del cambio en las configuraciones avanzadas):



2. Si es necesario, clic "¡Tendré cuidado, lo prometo!" para confirmar que se desea cambiar la configuración del navegador. El navegador muestra una lista de configuraciones.
3. En el campo "Filtro", entramos `network.proxy.socks_remote_dns`. Solo esa configuración se muestra.



4. Si esta configuración tiene el valor *false*, doble-clic para cambiar el valor a *true*.

Firefox está ahora configurado para evitar la fuga de DNS. Una vez que el valor se muestre como true, esta configuración es automáticamente salvada permanente.

No existe una forma documentada de prevenir la fuga de DNS con Internet Explorer, sin usar un programa externo.

En el momento en que se escribe este manual no hay fugas de DNS conocidas en Pidgin cuando se configura para que use Proxy SOCKS 5.

CÓMO AYUDAR A OTROS
33. Ingestigando y documentando la censura
34. Lidiando con bloqueo de puertos
35. Instalando Proxis Web
36. Instalando un relay Tor
37. Riesgos de operar un proxy
38. Buenas prácticas para Webmasters

33. INGESTIGANDO Y DOCUMENTANDO LA CENSURA

En muchos países, no es un secreto la existencia de la censura de Internet por parte de los gobiernos. El alcance y los métodos de la censura han sido documentados por ejemplo en los libros: Access Denied: The Practice and Policy of Global Internet Filtering y Access Controlled: The Shaping of Power, Rights, y Rule in Cyberspace, ambos editados por Ronald Delbert, John Palfrey, Rafal Rohozinski, y Jonathan Zittrain (http://opennet.net/accessdenied y http://www.access-controlled.net).

Cuando un sitio popular es ampliamente bloqueado, el hecho tiende a conocerse en todo el país. Sin embargo, algunos gobiernos (incluyendo algunos censuradores bastante activos) oficialmente niegan la existencia de la censura o tratan de disfrazarla con errores técnicos aleatorios. Si estamos sujetos a la censura, podemos usar nuestra situación para ayudar a otros (incluyendo la academia internacional y la comunidad de activistas que estudian la censura) a entender y publicarla potencialmente.

Por supuesto, necesitamos ser cuidadosos en esto; los gobiernos que niegan la práctica de la censura de la red pueden no estar contentos con nuestros esfuerzos para desenmascararlos.

EXPLORANDO LAS BASES DE DATOS DE CENSURA

Algunas bases de datos de censura se han hecho públicas en los últimos dos años. Algunas de ellas tienen multitud de orígenes pero todas están validadas por expertos en el campo. Ellas constantemente se están actualizando para mantener la información y los sitios bloqueados tan precisos como sea posible. Algunas bases de datos están disponibles en las siguientes URLs:

- *Herdict Web*: https://www.herdict.org
- *Alkasir Map*: https://www.alkasir.com/map

En un nivel macro-georáfico, OpenNet Initiative and Reporteros sin fronteras libera un "State of Internet" para cada país regularmente. Podemos accederlo en la red:

- *OpenNet Initiative* research report: http://opennet.net/research
- *Reporters Without Borders* Internet Enemies: http://www.rsf.org/ennemis.html

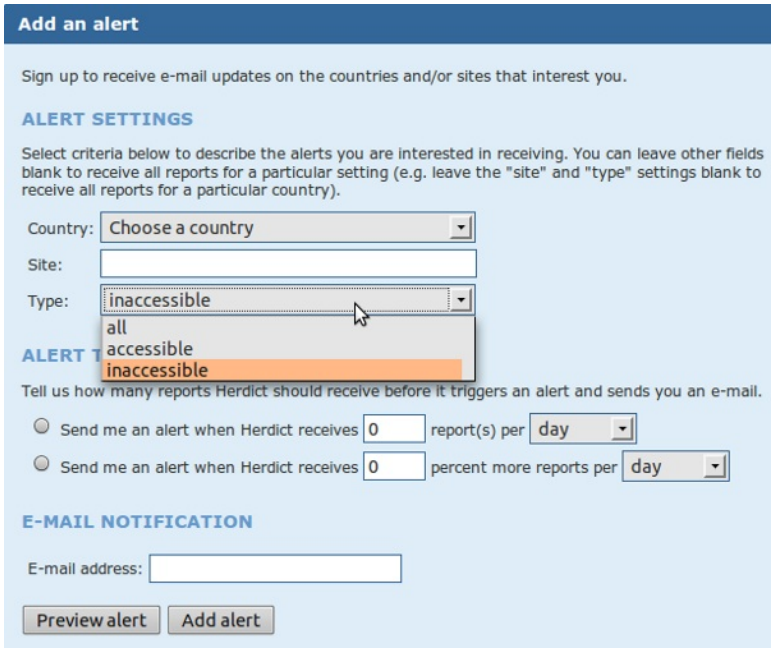
REPORTANDO SITIOS BLOQUEADOS USANDO HERDICT

Herdict (https://www.herdict.org) es un sitio web que agrega reportes de sitios inaccesibles. Se ejecuta por investigadores en Berkman Center For Internet and Society en la Universidad de Harvard en los Estados Unidos quienes estudian cómo se comporta la censura en Internet.

Los datos de Herdict no son perfectos – por ejemplo, muchos usuarios no pueden distinguir entre un sitio que no está disponible por un fallo técnico o porque ellos escribieron mal la dirección de la actual censura – pero la información es recolectada alrededor de todo el mundo y es constantemente actualizada.

Arriba se muestra un reporte sobre Facebook

Nosotros podemos ayudar a estos investigadores entrando nuestros propios reportes a Herdict a través de su sitio web. Es gratis, fácil de usar y no tenemos que registrarnos. También podemos registrarnos para obtener actualizaciones de futuras notificaciones de bloqueo de sitios web.



Herdict también ofrece complementos para los navegadores Firefox e Internet Explorer para hacer más fácil reportar un sitio bloqueado mientras navegamos por la Web.

REPORTANDO SITIOS BLOQUEADOS USANDO ALKASIR

Alkasir es una herramienta de evasión con una parte construida en la investigación que permite a los usuarios reporta un sitio Web bloqueado con un simple botón "Report Blocked URLs". Alkasir mantiene una lista relevante de sitios Web bloqueados por país y puede chequear automáticamente la disponibilidad de otras URLs. Usando la característica de reporte podemos fácilmente contribuir a esta investigación.

Para más detalles nos dirigimos al capítulo “Usando Alkasir”.

HABILITANDO EL ACCESO REMOTO PARA OTROS

Podemos ayudar en la investigación de la censura dando a los investigadores acceso remoto a nuestra computadora para que puedan hacer sus propias pruebas. Esto solo debemos hacerlo si confiamos en los investigadores en cuanto al acceso que les ofrecemos, ya que pueden tomar el control total de nuestra computadora y todo lo que hagan en nuestra máquina se verá como nuestras propias acciones ante el ISP o el gobierno.

Para los sistemas operativos GNU/Linux una cuenta shell es la mejor opción; podemos encontrar ayuda en http://ubuntuforums.org y en otros sitios.

Para sistemas operativos Windows la aplicación escritorio remoto debe usarse. Podemos encontrar instrucciones para esto aquí: http://www.howtogeek.com/howto/windows-vista/turn-on-remote-desktop-in-windows-vista.Quizás también tengamos que cambiar las configuraciones de *port forwarding* en el enrutador que usamos para conectarnos a Internet; esto se explica en http://portforward.com.

Otra solución para acceso remoto es la herramienta gratis TeamViewer (http://www.teamviewer.com) que está disponible para todos los sistemas operativos.

COMPARANDO NOTAS

La técnica básica para documentar la censura de red es intentar acceder a un gran número de recursos de red, como largas listas de URLs, desde varios lugares y después comparar los resultados. Algunas URLs fallaron en cargar en un lugar y en otro no? Son éstas diferencias constantes y sistemáticas? Si tenemos alguna tecnología de evasión confiable como VPN, podemos hacer algunos experimentos nosotros mismos, comparando como se ve la red con y sin evasión. Por ejemplo, en los Estados Unidos, este fue el método usado para documentar como los ISPs interrumpieron los programas de ficheros compartidos punto a punto.

Estas comparaciones se pueden hacer con algún software que automatice la tarea o manualmente.

ANÁLISIS DE PAQUETE

Al familiarizarnos con los detalles técnicos de cómo funcionan los protocolos de Internet, un analizador de paquetes como lo es por ejemplo Wireshark (http://www.wireshark.com/) nos permitirá registrar los paquetes de red concretos que nuestra computadora transmite por la red.

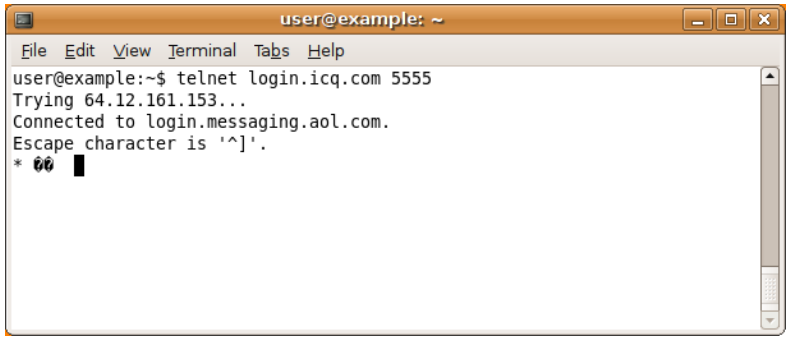
34. LIDIANDO CON BLOQUEO DE PUERTOS

Los cortafuegos pueden ser usados para bloquear las comunicaciones que son dirigidas a un puerto en particular. Esto puede ser usado para impedir el uso de algún protocolo en particular o algún tipo de software de red. Para tratar de evadir estas restricciones, los ISPs y los usuarios pueden preparar accesos a servicios por puertos no-estándares. Esto permite a las aplicaciones evadir una restricción simple como el bloqueo de puertos.

Muchas aplicaciones pueden ser configuradas para usar puertos no estándares. Las URLs para las páginas web tienen un modo particularmente conveniente de hacer esto dentro de las URLs mismas. Por ejemplo, el url *http://www.example.com:8000/foo/* le diría al navegador web que haga una petición http al servidor example.com por el puerto 8000, en lugar del puerto 80. Por supuesto que esto solo funcionará si el servidor web en www.example.com está preparado para recibir peticiones por dicho puerto.

VERIFICAR SI HAY BLOQUEO DE PUERTOS

Usando `telnet` podemos verificar que puertos (si hay alguno) están bloqueados desde donde estamos. Con solo abrir una terminal de comandos y escribir "telnet login.icq.com 5555" o "telnet login.oscar.aol.com 5555" y dar enter. El número es el puerto que queremos verificar. Si obtenemos un número de símbolos extraños entonces quiere decir que se pudo establecer la conexión.



Si, por otra parte, la computadora reporta que la conexión falló, o que fue interrumpida, desconectada o restaurada, ese puerto probablemente esté bloqueado (hay que tomar en cuenta que algunos puertos pueden ser bloqueados solo en conjunto con ciertas direcciones IPs).

35. INSTALANDO PROXIS WEB

Si tuviéramos acceso a un servidor web en un país donde no se está censurando el acceso a Internet, entonces estamos en posición de poder instalar un proxy Web, dicho **proxy web** es un pequeño pedazo de Software que puede estar escrito en PHP, Perl, Python o ASP. La instalación de herramientas de evasión basadas en Web requiere de algunas habilidades técnicas y recursos (un servicio de hospedaje compatible con la tecnología de la aplicación y suficiente ancho de banda).

Si queremos instalar un proxy web necesitamos lo siguiente:

- Un espacio de hospedaje web que soporte PHP(esto puede comprarse por unos pocos dólares al año de compañías como https://www.dreamhost.com o http://www.hostgator.com) o provistos por la escuela o universidad.
- Un VPS(Virtual Private Server) o un servidor dedicado (que son más caros y complicados de usar)
- Una PC conectada a una conexión de banda ancha(con una dirección IP pública accesible desde internet).

PROXIS WEB PÚBLICOS Y PRIVADOS

Los proxis web públicos están disponibles para cualquiera que esté dispuesto a encontrarlos en motores de búsqueda como por ejemplo Google. Los proxis web públicos y otros servicios de anonimato pueden ser encontrados por usuarios y también por las autoridades encargadas de implementar el filtraje web, por tanto son vulnerables a caer en listas negras.

Las ubicaciones de los proxis web privados solo son conocidas por los usuarios interesados. Por tanto, los proxis privados son más adecuados para usuarios que requieran un servicio de evasión estable para tráfico web y que tengan contactos confiables en lugares no filtrados con las habilidades técnicas necesarias y suficiente ancho de banda para soportar un proxy web. Las posibilidades de que un proxy web privado sea bloqueado son menores que las de esos servicios de evasión públicos. Es también la opción de evasión más flexible para tráfico web simple y es menos probable que sea descubierta y bloqueada que un proxy web público, particularmente si es usado con cifrado SSL.

CARACTERÍSTICAS DE UN PROXY WEB

Los proxis web pueden ser puestos en funcionamiento con algún nivel de personalización ajustado a las necesidades específicas de los usuarios finales. Las personalizaciones comunes incluyen cambiar el número del puerto en que el servicio web se está ejecutando e implementar cifrado SSL. Algunas listas negras pueden bloquear algunas palabras claves asociadas a proxis web populares. Cambiar elementos como la URL por defecto o el nombre de algún script, o los elementos de la interfaz de usuario también reducen el riesgo de que el proxy sea detectado automáticamente. También es posible proteger el uso del proxy habilitando .htaccess con nombre de usuario y contraseña.

Cuando usamos SSL es también útil crear una página web inocua en la raíz del servidor y ocultar el proxy web en un camino aleatorio. Aunque los intermediarios podrían determinar a qué servidor nos estamos conectando, no podrían determinar el camino al que va dirigida la petición porque esa parte del la petición va cifrada. Por ejemplo, si un usuario se conecta a https://example.com/secretproxy/ un intermediario solo podría determinar que se conectó a example.com pero no podría ver que el usuario accedió al web proxy. Si el operador del proxy web pone una página inocente en example.com entonces el proxy web es menos probable que sea descubierto a través del monitoreo de transmisiones de red. Un certificado SSL válido que es reconocido en la mayoría de los proxis web está disponible gratuitamente en https://www.startcom.org/.

Existen varios web proxis gratis y de código abierto disponibles en Internet. La mayor diferencia radica en los lenguajes de programación en que están escritos ya que no todos los servidores web soportan todos los lenguajes de programación. La otra gran diferencia es la compatibilidad del programa con los sitios web modernos con tecnologías como AJAX (usado por GMail o Facebook) o flujos de video de Flash (usados por YouTube).

Algunos web proxis populares son

- CGIProxy (http://www.jmarshall.com/tools/cgiproxy): un script CGI escrito en Perl que hace las veces de proxy HTTP o FTP.
- Peacefire's Circumventor (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html): un instalador automático que hace mucho más fácil para usuarios no técnicos instalar y configurar CGIProxy en una máquina Windows.
- SabzProxy (http://sabzproxy.com): al mismo tiempo un proxy HTTP y uno FTP. Está basado en el legado de PHProxy escrito en PHP con nuevas características, tal y como codificación aleatoria de la URL para hacer que sea más dificil de bloquear.

- Glype Proxy (http://www.glype.com): otro proxy web, también escrito en PHP.

Los sitios de estos proxis web proveen instrucciones sobre cómo instalarlos. Básicamente esto involucra descargar los scripts, extraerlos en el disco local, subir el script via FTP o SCP a un servidor Web, establecer los permisos y probar el script. El siguiente ejemplo es para la instalación de SabzProxy, pero los pasos son similares a los de los otros proxis.

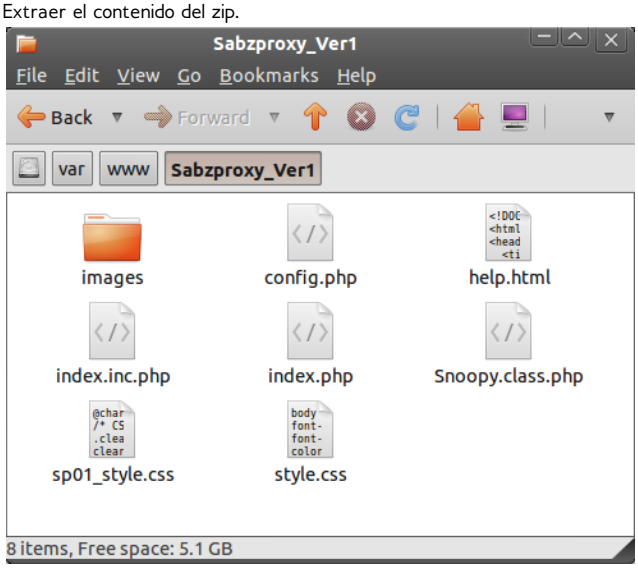
INSTALANDO SABZPROXY

SabzProxy solo está disponible en Persa, pero la interfaz de usuario es muy simple y es fácil de entender.

Estas instrucciones describen los casos más comunes: usar FTP para transferir SabzProxy a un espacio en un servidor Web con soporte para PHP. Para ésta técnica necesitamos un cliente FTP como el FileZilla (http://filezilla-project.org)

Aunque este método es el más común, no es aplicable a todas las situaciones(por ejemplo, si estamos configurando nuestro propio servidor a través de la línea de comando), pero los pasos deben ser similares.

1. El primer paso es descargar el SabzProxy de http://www.sabzproxy.com.
2. Extraer el contenido del zip.

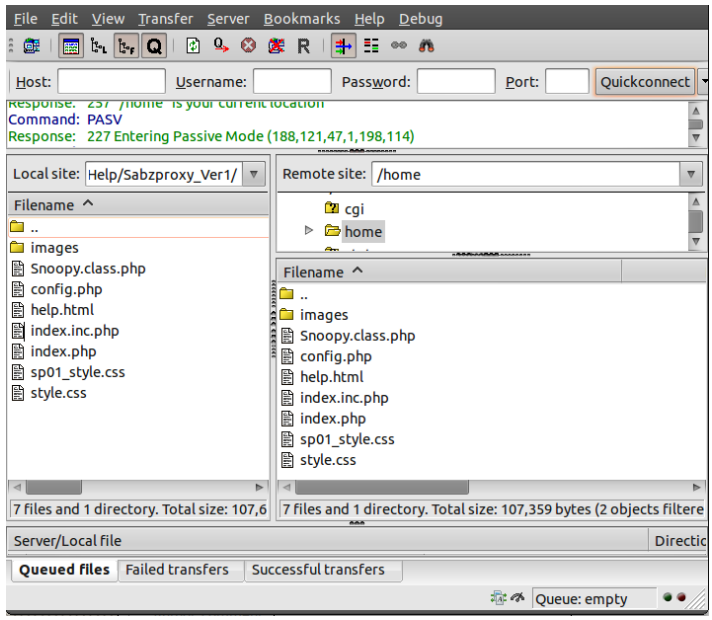


3. Abrir el fichero config.php con un editor de textos cualquiera (e.g. Notepad para Windows, gedit o nano para usuarios de Linux o Texteditor para MacOS).
4. Editar la línea 8, que empieza con *$config_key*. Escribamos una cadena aleatoria entre los "". Esta cadena será usada para hacer la codificación de las URLs aleatorias.

```php
<?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. Podemos también configurar un par de opciones como el texto de bienvenida o algunos vínculos.
6. Abrámos FileZilla, entremos el nombre del servidor(host), nombre de usuario y contraseña del hospedaje web y demos clic en Quickconnect (o opción similar si estamos usando un cliente FTP diferente).
7. La parte izquierda del cliente FTP representa la PC local y podemos ahí localizar los ficheros de SabzProxy que antes descomprimimos.



8. La parte izquierda del cliente FTP representa la PC local y podemos ahí localizar los ficheros de SabzProxy que antes descomprimimos.
9. Ahora podemos acceder a SabzProxy simplemente accediendo al dominio del hospedaje web y del directorio en el que ubicamos PHProxy (en este ejemplo http://kahkeshan-e-sabz.info/home.)

Si esto no funciona entonces es posible que el servidor web no soporte PHP, o que el soporte PHP pueda estar deshabilitado y requiera configuración adicional. Remitámonos a la documentación de nuestra cuenta o del servidor web en uso. Podemos también buscar un fórum de soporte o preguntarle al operador del servidor directamente.

36. INSTALANDO UN RELAY TOR

Si vivimos en un área con poca o ninguna censura de internet, podríamos ayudar a ejecutar un repetidor TOR o un **repetidor puente TOR** para ayudar a otros usuarios TOR acceder a internet sin restricciones.

La red TOR depende de voluntarios para tener ancho de banda. Mientras más personas ejecuten repetidores, más rápida y segura será la conexión TOR. Para ayudar a las personas que usan TOR evadir la censura de internet es preferible poner un repetidor puente que un repetidor ordinario.

Los *repetidores Puente*(Bridge Relays) o "*puentes*" son relays TOR que no están listados en el directorio(público) principal de TOR. Aún cuando un proveedor de internet bloquee el acceso a todos los relays TOR conocidos, es probable que no pueda bloquear todos los puentes.

RIESGOS DE OPERAR UN NODO TOR (TOR RELAY)

Un nodo TOR es un tipo de proxy público de forma que ejecutar uno conlleva los riesgos descritos en el capítulo "Riesgos de operar un Proxy". Sin embargo un nodo TOR puede configurarse de dos maneras, como un **nodo de salida** o como un **nodo intermedio**. Un nodo intermedio solo retransmite el tráfico cifrado a otros nodos TOR, y no permite que los usuarios anónimos se comuniquen directamente con sitios fuera de la red TOR. Operar cualquiera de éstos nodos es útil para la red TOR en su conjunto. Ejecutar un nodo de salida es particularmente útil porque los nodos de salida son particularmente escasos. Ejecutar un nodo intermedio es menos riesgoso porque un nodo intermedio no atrae el tipo que quejas que un proxy público puede acarrear, ya que la dirección IP de un nodo intermedio nunca aparecería en los registros de acceso.

Como un nodo puente no es un nodo de salida es poco probable que recibamos quejas sobre el uso de un nodo puente por otros.

Aún cuando sea improbable que atraigamos ciertas miradas, operar un nodo intermedio o nodo puente puede ocasionar que nuestro proveedor de servicios de internet se oponga por diferentes razones. Por ejemplo, nuestro proveedor puede desaprobar la red TOR o puede desaprobar que suscriptores operen ciertos tipos de servicios públicos. Podemos leer más sobre las mejores prácticas sobre como operar un nodo TOR de salida en https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment.

¿QUÉ NECESITAMOS PARA OPERAR UN RELAY O UN RELAY PUENTE?

Existen solo unos pocos prerrequisitos para ejecutar un relay Tor:

- Nuestra conexión necesita un ancho de banda de por lo menos 20 kilobytes/segundo en ambas direcciones (y necesita estar OK y constantemente en uso cuando encendamos la computadora).
- Necesitamos una conexión con una dirección IP que sea enrutable públicamente.
- Si nuestra computadora se encuentra tras un cortafuego NAT (**network address translation**) y no tiene acceso público o dirección IP pública (o externa), necesitaremos configurar una regla de reenvío de puerto en nuestro enrutador. Podemos hacer esto a través de Tor Universal Plug and Play, o manualmente, siguiendo las instrucciones en el manual del enrutador o en portforward.com (http://portforward.com/english/applications/port_forwarding/HTTPS/HTTPSindex.htm).

Que *no* es necesario:

- Nuestra computadora no tiene que estar siempre en línea (el directorio Tor averiguará cuando esté).
- No necesitamos tener una dirección IP estática.

DESCARGANDO TOR

Para descargar Tor, podemos ir al sitio Web https://www.torproject.org/ y hacernos clic en Download en el menú de navegación.

En la página de los Tor Bundles disponibles, seleccionamos una versión estable que encaje con nuestro sistema operativo.

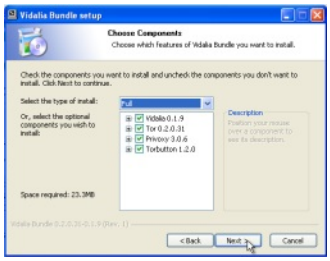
INSTALANDO TOR EN GNU/LINUX

Podemos encontrar instrucciones detalladas de cómo configurar un relay Tor o un puente en https://www.torproject.org/docs/tor-doc-relay.html.en.

INSTALANDO TOR EN MICROSOFT WINDOWS

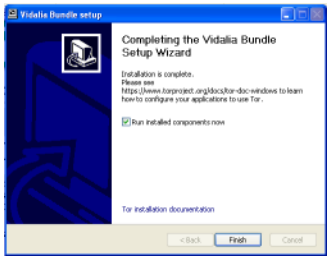
Iniciamos el instalador y hacemos clic en Next cuando nos pregunte.

Si usamos Firefox, instalamos todos los componentes propuestos en el dialogo mostrado abajo:



Si no tenemos Firefox instalado, deseleccionamos Torbutton (tendremos la opción de instalar Firefox y Torbutton después).

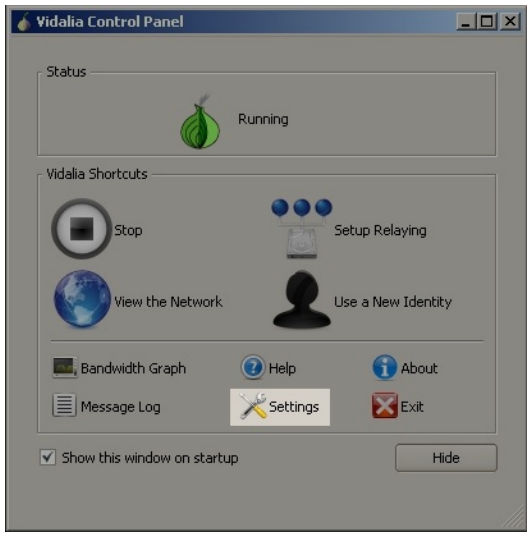
Cuando la instalación se completa, iniciamos Tor haciendo clic en Finish con la caja "Run installed components now" seleccionada, como en el dialogo que se muestra a continuación:



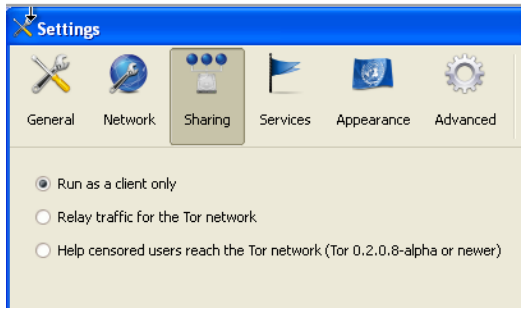
CONFIGURANDO TOR PARA QUE ACTÚE COMO UN PUENTE

Para activar nuestro Puente:

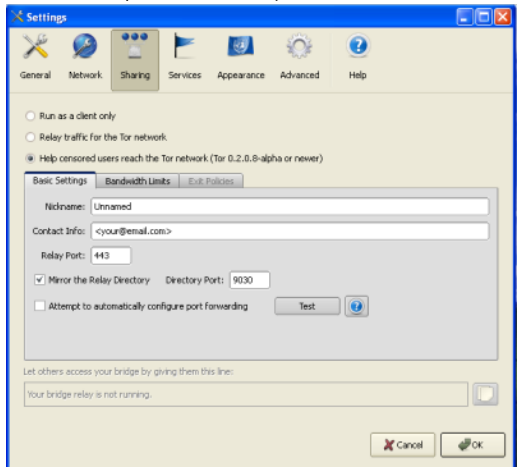
1. Abrimos el panel de control Vidalia.
2. En el panel de control Vidalia, hacemos clic en Prefrencias.



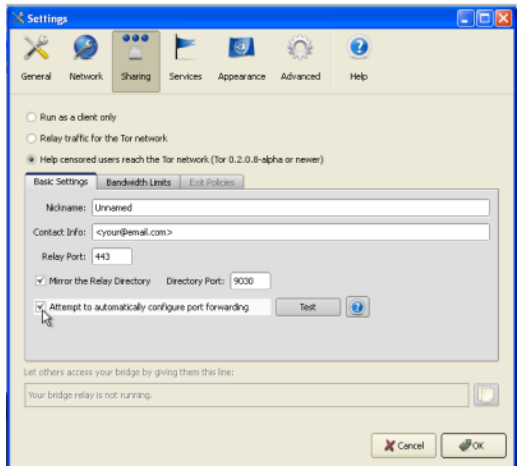
3. En la ventana Preferencias, hacemos clic en Compartiendo.



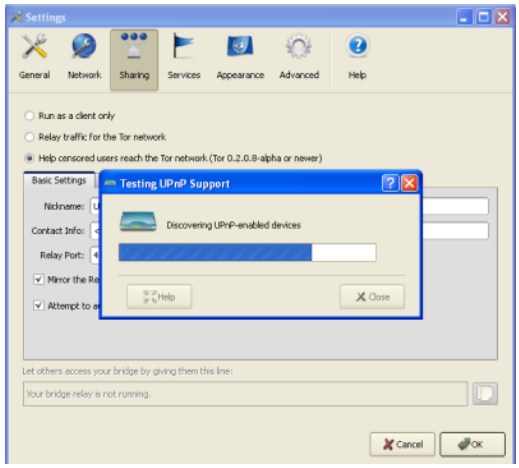
4. Para crear un puente, clic en "Ayude a usuarios censurados a accede a la red Tor":



5. Si estamos usando una dirección IP NAT en una red local, necesitamos crear una regla de *redireccionamiento de puerto* en nuestro enrutador. Podemos pedirle a Tor que configure el reenvío de puerto por nosotros. Para hacer esto, hacemos clic en "Intentar configurar automáticamente el reenvío de puertos":



6. Hacemos clic en Prueba para ver si Tor creó correctamente una configuración para reenvío de puerto en el enrutador:

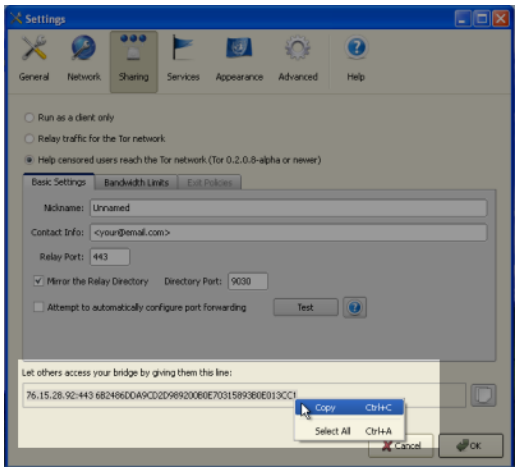


Si Tor no pudo configurar el reenvío de puerto, debemos leer la entrada de Tor FAQ de este tópico: https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#ServerForFirewalledClients

Enhorabuena. Si todo ha ido bien, nuestro Puente se estará ejecutando. La información de Puente será adicionada al directorio oculto de puentes y estará disponible para los usuarios que lo soliciten.

COMPARTIENDO NUESTRO PUENTE CON AMIGOS

Si dispusimos nuestro puente exclusivamente para ayudar a un amigo que accede a la red de Tor, podemos copiar la información al pie de la ventana de Preferencias y enviársela:


Settings
General
Network
Sharing
Services
Appearance
Advanced
Help
Run as a client only
Relay traffic for the Tor network
Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)
Basic Settings
Bandwidth Limits
Exit Policies
Nickname:
Unnamed
Contact Info:
<your@email.com>
Relay Port:
443
Mirror the Relay Directory
Directory Port:
9030
Attempt to automatically configure port forwarding
Test
Let others access your bridge by giving them this line:
Copy Ctrl+C
Select All Ctrl+A
Cancel
OK

37. RIESGOS DE OPERAR UN PROXY

Cuando ejecutamos un **proxy** o **proxy web** en nuestra computadora para ayudar a otros, las solicitudes y las conexiones reenviadas a través de ese proxy aparecerán originadas desde nuestra computadora. Nuestra computadora actúa a favor de otros usuarios de Internet, así que la actividad de ellos se atribuirá a nosotros, como si lo hubiésemos hecho nosotros mismos. Así que si alguien usa el proxy para enviar o recibir material al que un tercero se opone, podemos recibir quejas que asumen que somos responsables y pueden pedirnos que paremos la actividad. En algunos casos, las actividades que usan nuestro proxy pueden atraer acciones legales o la atención de agencias de cumplimiento de la ley en nuestro propio país o en otro.

En algunos países, los operadores de proxy han recibido quejas legales, y, en algunos casos, los agentes de aplicación de la ley han confiscado computadoras que funcionan como proxy. Esto puede suceder por varias razones:

- Alguien puede asumir (incorrectamente) que el operador del proxy estaba personalmente involucrado en las actividades realizadas a través del proxy.
- Alguien puede afirmar que el operador del proxy tiene la obligación de detener ciertos usos, incluso si esos usos son hechos por terceros.
- Alguien puede examinar el proxy para buscar evidencia (ej. registros) de quién fue el responsable de cada actividad.

Si pensamos que esto puede ser un riesgo para nuestro proxy en nuestra área, será más seguro operar el proxy en una computadora dedicada en un centro de datos. De esa forma no llamará la atención de nuestra conexión en casa.

Las leyes nacionales pueden variar en forma y extensión en la que protegen a los operadores de proxy. Para más detalles sobre esta situación, debemos consultar un abogado o un experto legal calificado en nuestra jurisdicción.

RIESGOS DE OPERAR UN PROXY PÚBLICO

Los proveedores de servicio de Internet pueden quejarse de nuestras operaciones de proxy, especialmente si ellos reciben quejas sobre abuso de proxy. Algunos ISPs pueden afirmar que ejecutando un proxy público se violan sus términos de servicio, o que ellos simplemente no desean permitir a los usuarios ejecutar proxis públicos. Estos ISPs pueden desconectarnos o amenazar con desconectarnos en un futuro.

Un proxy público puede ser usado por muchas personas alrededor del mundo y puede usar grandes cantidades de ancho de banda y tráfico, así que cuando usamos ISPs que no aplican una tarifa plana, debemos tomar precauciones para evitar tener que pagar demasiado al final de mes.

RIESGOS DE OPERAR UN PROXY PRIVADO

Estos riesgos aún existen si operamos un proxy para nuestro beneficio o para el uso de un pequeño grupo de individuos, pero operar un proxy no-público es mucho menos riesgoso que operar un proxy público.

Si el usuario de un proxy no público es detectado y monitoreado, quien sea que esté monitoreando piensa o especula que hay una conexión entre nosotros y el usuario y que estamos tratando de ayudar a evadir el filtrado.

Aunque nuestro propio ISP se oponga más a la ejecución de proxis públicos, algunos ISPs pueden tener políticas anti – proxy que se oponen incluso a la operación de proxis privados en su red.

LAS LEYES DE RETENCIÓN DE DATOS PUEDEN REGULAR LAS OPERACIONES DE LOS PROXIS

En algunos países, las **leyes de retención de datos** o leyes similares que son un medio para restringir el anonimato pueden ser interpretadas como reguladoras de la operación de los servicios de proxy. Para más información acerca de la retención de datos veamos https://secure.wikimedia.org/wikipedia/en/wiki/Telecommunications_data_retention.

38. BUENAS PRÁCTICAS PARA WEBMASTERS

Ejecutar un sitio Web, expuesto a una multitud o no, no es siempre fácil. Es importante pensar acerca de nuestra seguridad personal así como en la seguridad de los visitantes. A menudo, los administradores de red se sorprenden cuando sus sitios son bloqueados inesperadamente en cierto país. Si un gran número de visitantes pueden entrar al sitio, el operador del sitio puede enfrentar también problemas económicos.
Perder nuestro sitio Web o servidor, o tener que configurar un nuevo servidor también puede ser preocupante y frustrante.

Este capítulo tiene la intención de reunir una lista de buenas prácticas y consejos a tener en cuenta cuando operamos nuestro propio sitio web.

PROTEGER NUESTRO SITIO WEB

- Siempre **planificar copias de respaldo automáticas** (ficheros y bases de datos) al menos en otra máquina física. Debemos asegurarnos de saber cómo restaurarlos.
- **Monitorear nuestro tráfico** para saber algo acerca de los países de los que provienen nuestros visitantes. Podemos usar bases de datos de geo localización para tener al menos una suposición del país en el que está localizada una dirección IP. Si notamos una caída del tráfico desde un país en específico, nuestro sitio Web debe haber sido bloqueado. Podemos compartir esto con bases de datos de sitios bloqueados, como Herdict (https://www.herdict.org/web).
- **Asegurar nuestro sitio web**, especialmente si usamos un CMS (Content Management System). Es recomendable instalar siempre las últimas actualizaciones del sistema operativo para corregir los fallos de seguridad.
- **Asegurar nuestro software de servidor web** con configuraciones de seguridad de alto nivel (podemos encontrar recursos en línea acerca de cómo asegurar servidores web Linux).
- Registrar (o transferir) nuestro nombre de dominio a **otro proveedor DNS** que no sea nuestro proveedor de hospedaje. En caso de ataque en nuestro proveedor actual, seremos capaces de poner a apuntar fácilmente nuestro nombre de dominio a un nuevo proveedor.
- Evaluar la creación de un **servidor espejo** ejecutándose en estado de espera para poder intercambiarlo fácilmente. Para ello debemos aprender cómo cambiar las entradas de nuestro DNS al servidor espejo.
- Considerar **hospedar nuestro sitio Web en un sitio extranjero**, donde el contenido es menos controversial y legalmente protegido. Esto puede implicar una demora adicional muy pequeña en el tiempo de carga de la página (usualmente unos pocos milisegundos) para nuestros visitantes y puede salvarnos una gran cantidad de problemas si estamos en un país donde el contenido de nuestro sitio web es considerado muy controversial.
- **Probar y optimizar nuestro sitio Web** con las herramientas de evasión principales que nuestros visitantes usan. Debemos chequear y reparar cualquier página o característica dañada. Idealmente, debemos hacer nuestro sitio usable a los visitantes sin JavaScrpit o complementos, ya que estos pueden estar dañados o no disponibles cuando las personas usan proxis.
- **Evitar el uso de FTP** para subir nuestros ficheros. FTP envía nuestra contraseña sobre Internet sin cifrado, haciendo fácil a los atacantes robar nuestras credenciales. Es mejor considerar usar SFTP (File Transfer Protocol sobre SSH), SCP, o WebDAV seguro (sobre HTTPS) en su lugar.
- **Usar puertos alternativos** para acceder a la zona de administración. Los hackers usualmente ejecutan sus búsquedas en puertos estándares para detectar vulnerabilidades. Es bueno considerar cambiar nuestros números de puertos a valores no estándares (como SSH) para minimizar los riesgos de estos ataques.
- **Proteger nuestro servidor de ataques de fuerza bruta** instalando una herramienta como DenyHosts en nuestro servidor (http://denyhosts.sourceforge.net) para proteger nuestro servidor poniendo en lista negra las direcciones IPs de aquellos que intentan registrarse una cierta cantidad de veces insatisfactoriamente.

PROTEGERNOS NOSOTROS MISMOS

Aquí hay algunos consejos para evitar potencialmente el daño personal si el hecho de permanecer anónimos es importante para nosotros.

- Usar una dirección de correo electrónico y un nombre que no esté asociado con nuestra identidad real.
- Si somos dueños de un nombre de dominio, podemos registrar entradas tontas en la base de datos públicas WHOIS usando un servicio llamado "WHOIS proxy", "WHOIS protect" o "domain
privacy".
- Usemos un servicio como Tor para mantenernos anónimos cuando actualicemos nuestro sitio web.

PROTEGIENDO NUESTROS VISITANTES

Aparte de la protección de nuestro sitio Web y de nosotros mismos, también es importante proteger a los visitantes del monitoreo de terceros, especialmente si entran contenido para nuestro sitio web.

- **Usar HTTPS** para que nuestros usuarios puedan acceder a nuestro sitio Web a través de una conexión cifrada, para hacer más difícil la búsqueda automática del contenido que está siendo transferido y asegurar nuestra identidad. Debemos asegurarnos de que la configuración de HTTPS cubre todo el sitio y que usamos otras mejores prácticas para la configuración de HTTPS. Podemos encontrar información sobre cómo implementarlo correctamente en la página *https://www.eff.org/pages/how-deploy-https-correctly y también podemos hacer las pruebas automáticas en https://www.ssllabs.com/ para muchos parámetros técnicos.*
- **Minimizar los datos almacenados en nuestros registros**. Evitemos guardar las direcciones IP u otros datos personales relacionados con nuestros visitantes más de lo necesario.

- **Cifrar los datos del usuario**, como contraseñas, por ejemplo usando funciones de resumen.
- Servicios externos como **Google Analytics** o el contenido de terceros como son las redes de anuncios publicitarios son difíciles de controlar. Evitémoslos.
- Creemos una versión **ligera y segura** de nuestro sitio Web, sin ningún Flash o código Javascript embebido, compatible con Tor y con las conexiones con bajo ancho de banda.

EDUCAR A NUESTROS USUARIOS

- **Enseñemos a nuestros usuarios** cómo utilizar las herramientas de evasión, y seamos capaces de mejorar su propia seguridad en línea.
- Hagamos una **lista de control de seguridad digital** disponible para que los visitantes puedan estar seguros de que no han sido atacados o monitoreados.

COMPARTIR NUESTRAS HERRAMIENTAS DE EVASIÓN CON NUESTROS VISITANTES

- **Hospedar instancias de proxis Web** (como SabzProxy o Proxy Glype). Debemos compartirlo con nuestros visitantes, por correo electrónico, o a través de sus redes sociales.
- **Enviar las invitaciones psiphon** si tenemos una cuenta en un nodo privado
- **Instalamos otros tipos de proxis** si poseemos un servidor dedicado.
- Hagámos **enlaces** a sitios de herramientas de evasión pertinentes.

MULTIPLICAR LOS CANALES DE DISTRIBUCIÓN

Si somos Webmasters podemos y debemos tomar diferentes acciones con el fin de difundir el contenido tanto como sea posible, para evitar el ser bloqueados bloqueados.

- **Establecer un boletín de noticias**, y enviar actualizaciones periódicas de los nuevos contenidos por correo electrónico, que debe de llegar a los usuarios, aún cuando estos no sean capaces de visitar más nuestro sitio Web.
- **Establecer un canal RSS** y debemos asegurarnos de que contiene artículos completos y no sólo fragmentos. De esta manera el contenido puede ser analizado con facilidad por sitios Web y aplicaciones de terceros, como Google Reader, que puede ser usado para leer nuestro contenido, donde el acceso directo es bloqueado.
- **Compartir nuestro contenido en plataformas de redes sociales** populares como Facebook o Twitter, que puede ser difícil de bloquear.
- **Difundir el contenido tanto como sea posible.** Hagamos nuestro contenido disponible para la descarga, Wikipedia,por ejemplo, distribuye todo su contenido libremente como un volcado de la base de datos que se puede utilizar fácilmente para crear una réplica del sitio Web espejo con el mismo contenido, en otros lugares.
- Evaluemos la **publicación de nuestros artículos bajo una licencia libre** (como GPL Creative Wikipedia), que permita que cada uno reutilice su contenido y cree réplicas.
- Repliquemos nuestros archivos en los servidores gratuitos **compartición de ficheros** como Rapidshare.com o Megaupload.com y a través de programas de compartición **peer-to-peer** (ej. BitTorrent).
- Configuremos nuestro servidor Web para servir también contenido en **puertos diferentes** al estándar el puerto estándar 80 (http) y 443 (https).
- **Ofrezcamos un API** (interfaz de programación) que permite a otros accede a nuestro contenido de forma automática a través de software de otros fabricantes, como hacen Twitter o Wikipedia

REDUCIR EL TIEMPO DE CARGA DE LA PÁGINA.

Reducir el tiempo de carga de la página no sólo nos va a ahorrar un poco de ancho de banda y dinero, sino que también va ayudar a nuestros visitantes procedentes de países en desarrollo a acceder mejor a nuestra información. Una buena lista de las mejores prácticas para acelerar nuestro sitio web la podemos encontrar en http://developer.yahoo.com/performance/rules.html y https://code.google.com/speed/page-speed/.

- **Adoptar un estilo minimalista.** Consideremos la posibilidad de mantener las imágenes a un mínimo, y el uso de CSS para el estilo de nuestro diseño. Una buena introducción a CSS la podemos encontrar en http://www.w3schools.com/css/css_intro.asp.
- **Optimicemos nuestras imágenes.** Usemos programas como OptiPNG (http://optipng.sourceforge.net/) para hacer que nuestras imágenes se carguen más rápido mediante la optimización de ellos por la Web. Además, nunca hagamos la escala de imágenes con HTML si no es necesario (es decir, si necesitamos una imagen de 60x60 a continuación, cambiamos el tamaño de él directamente, en lugar de usar HTML).
- **Reduzcamos Java, JavaScript, Flash** y otros contenidos que se ejecutan en el ordenador del cliente a un mínimo. Recordemos que algunos cafés de Internet desactivan este tipo de contenidos por razones de seguridad. Debemos asegurarnos de que la información que deseamos transmitir es la que aparece en HTML puro.
- **Utilizar archivos externos para el CSS y JavaScript**. Si tenemos un cierto estilo CSS o JavaScript quef es recurrente en nuestro sitio Web, consideremos la posibilidad de guardarlo en un archivo separado y llamarlo en el encabezado de nuestra página web. Esto nos permitirá que el navegador de nuestro cliente almacene en caché los archivos,
- **Minimicemos nuestro código.** Eliminemos todos los descansos de líneas y espacios innecesarios. Algunas de las herramientas que lo hacen automáticamente, las podemos encontrar en http://javascriptcompressor.com
- **Reduzcamos el número de peticiones al servidor al mínimo.** Si tenemos un sitio web dinámico pero el contenido no cambia muy a menudo, es posible que deseemos instalar algunas extensiones caché que ofrecen a los usuarios una versión estática de su contenido, por lo tanto reducen significativamente el número de solicitudes de la base de datos.

39. GLOSARIO

La mayoría de estos contenidos se basan en http://en.cship.org/wiki/Special:Allpages

AGREGADOR

Un agregador es un servicio que reúne información asociada a uno o más sitios y la hace disponible desde diferentes direcciones. Muchas veces es llamado agregador RSS, agregador de suplementos, lector de suplementos o lector de noticias.

ANÁLISIS DE TRÁFICO

El análisis de tráfico es un análisis estadístico de las comunicaciones cifradas. En algunas circunstancias el análisis de tráfico puede revelar información acercade las comunicaciones de las personas y de la información que ha sido comunicada.

ANÁLISIS DE AMENAZAS

Un análisis de amenazas de seguridad es un estudio formal y detallado de todas las formas conocidas de atacar la seguridad de servidores o protocolos, o de métodos para usarlos para un propósito en particular como la evasión de la censura. Las amenazas pueden ser técnicas, como ruptura de código, exploiting software bugs, o social, como robar contraseñas o sobornar a alguien que sepa algo en especial. Unas pocas compañías o individuos tienen el conocimiento y la habiliadad de hacer un análisis de amenazas detallado, pero todo el mundo envuelto en el tema de la evasión de censura tiene que hacer un estimado del asunto.

ANONIMATO

(No debe confundirse con privacidad, uso de seudónimos, seguridad, o confidencialidad.)
El anonimato en Internet es la habilidad de usar servicios sin dejar huellas de nuestra identidad. El nivel de protección depende de las técnicas de anonimato que se usan y de la extensión del monitoreo. Las técnicas más fuertes que se usan para proteger el anonimato incluyen la creación de una cadena de comunicación usando un proceso aleatorio para seleccionar algunos enlaces, en la cual cada enlace tiene acceso solo a información parcial de todo el proceso. El primero conoce la dirección IP del usuario pero no el contenido, destino, o propósito de la comunicación pues el contenido del mensaje y la información del destino están cifrados. El último enlace conoce la identidad del sitio que ha sido contactado, pero no la fuente de la sesión. Uno o más enlaces intermedios impiden que el primer y último enlace compartan la información parcial que conocen con el fin de conectar al usuario al sitio destino.

ARCHIVO DE REGISTRO

Un archivo de registro es un archivo que almacena una secuencia de los mensajes del proceso de un programa, que puede ser una aplicación o un componente de un sistema operativo. Por ejemplo, los servidores Web o proxis pueden mantener ficheros log que almacenan datos acerca de las direcciones IP que usaron el servicio, cuando y a que páginas se accedieron.

ASP (APPLICATION SERVICE PROVIDER)

ASP es una organización que ofrece servicios de software sobre Internet, permitiendo que dicho software se actualice y mantenga centralmente.

ATAQUES DE FUERZA BRUTA

Un ataque de fuerza bruta consiste en intentar cada código posible, combinación, o contraseña hasta encontrar la correcta. Estos son los ataques de piratería más triviales.

BACKBONE

Un backbone es un enlace de comunicación de gran ancho de banda que une las redes en diferentes países y organizaciones alrededor del mundo para formar Internet.

BADWARE

Ver malware.

ANCHO DE BANDA

El ancho de banda de una conexión es la cantidad máxima de datos transferida en esa conexión, limitada por su capacidad y las capacidades de los ordenadores en los dos extremos de la conexión.

BASH (BOURNE-AGAIN SHELL)

El shell bash es una interfaz de línea de comando para los sistemas operativos Linux/Unix, basados en el shell Bourne.

BITTORRENT

Es un protocolo para compartir ficheros punto-a-punto inventado por Bram Cohen en el 2001. Permite a los individuos distribuir ficheros grandes como imágenes de discos, videos, o música, de forma fácil y efectiva.

BLUEBAR

La barra de URL azul (llamada Bluebar en el lenguaje de Psiphon) es la forma al tope de la ventana de navegación del nodo Psiphon, que permite acceder a sitios bloqueados escribiendo la URL en ella.
Ver también nodo Psiphon

CACHÉ

Es una parte de un sistema de procesamiento de información que se usa para almacenar datos que han sido usados recientemente o frecuentemente para aumentar la velocidad de acceso a estos. El caché de la Web tiene copias de páginas Web.

CENSURAR

Censurar es impedir la publicación o recuperación de información, o llevar a cabo acciones legales o de otro tipo contra los editores o los lectores.

CENSORWARE

Es un tipo de aplicación informática que se usa para filtrar o bloquear el acceso a Internet. Este término es frecuentemente usado para referirse a los programas de filtrado y bloqueo de Internet que se instalan en la máquina cliente (el ordenador que se usa para acceder a Internet). La mayoría los censorwares instalados del lado del cliente son usados para propósitos de control. Algunas veces el término censorware se usa también para referirse al programa usado el mismo propósito pero instalado en un servidor de red o en router.

CGI (COMMON GATEWAY INTERFACE)

CGI es un estándar común usado para permitir que programas alojados en un servidor Web puedan ser ejecutados como aplicaciones Web. Muchos proxis Web usan CGI y por ello se les conoce como “proxis CGI”. (Un buen ejemplo de esto lo constituye es el CGIProxy escrito en Perl

por James Marshall.)

CHAT

El chat, llamado también mensajería intantánea, es un método de comunicación entre dos o más personas en el cual cada línea escrita por un participante en una sesión se hace eco a todos los demás. Existen muchos protocolos de chat, incluyendo aquellos que han creado compañías específicas (AOL, Yahoo!, Microsoft, Google, y otros) y protocolos definidos públicamente. Algunos programas de clientes chat usan solo uno de estos protocolos, mientras otros usan un rango de protocolos populares.

COOKIE

Una cookie es una cadena de texto que envía un servidor Web al navegador del usuario para almacenarla en el ordenador del usuario, y que contiene la información necesaria para mantener la continuidad de la sesiones a través de múltiples páginas web, o a través de sesiones múltiples. Algunos sitios Web no pueden usarse sin aceptar y almacenar una cookie. Algunas personas consideran esto una invasión de la privacidad o un riesgo de seguridad.

CCTLD (SIGLAS DE COUNTRY CODE TOP LEVEL DOMAIN)

Cada país tiene un código de dos letras, y un TLD (top-level domain) se basa en este, como .ca para Canadá; este dominio es llamado un código de primer nivel de país o en inglés top-level domain. Cada uno de esos ccTLD tiene un servidor DNS que lista todos los dominios de segundo nivel con el TLD. Los servidores raíces de Internet apuntan a todos los TLDs, y cachean la información que se usa frecuentemente en dominios de más bajo nivel.

CORREO ELECTRÓNICO

El correo electrónico es un método para enviar y recibir mensajes en Internet. Es posible usar un servicio de correo Web o enviar correos con el protocolo SMTP o recibirlos con el protocolo POP3 usando un cliente de correo electrónico como el Outlook Express o el Thunderbird. Es raro que un gobierno bloquee el correo electrónico, pero es muy común la inspección de correo electrónico. Si el correo electrónico no está cifrado, puede ser leído fácilmente por un operador de red o el propio gobierno.

COMPARTICIÓN DE ARCHIVOS

La compartición de archivos se refiere a cualquier sistema de computadora donde múltiples personas pueden usar la misma información, casi siempre se refiere a intercambio de música, películas u otros materiales disponibles de forma gratuita.

CIFRADO

El cifrado es cualquier método para recodificar datos y transformarlos matemáticamente para hacerlos ilegibles a un tercero que no sepa la llave secreta para descifrarlo. Es posible cifrar datos en nuestro disco duro local usando un programa como TrueCrypt (http://www.truecrypt.org) o cifrar el tráfico de Internet con SSL o SSH.

DARPA (DEFENSE ADVANCED PROJECTS RESEARCH AGENCY)

DARPA es el succesor de ARPA, que fundó Internet y su predecesor, el ARPAnet.

DOMINIO

Un dominio puede ser un Top-Level Domain (TLD) o un dominio secundario en Internet.

Ver también Top-Level Domain, country code Top-Level Domain y dominio secundario.

DNS (DOMAIN NAME SYSTEM)

El Sistema de Nombres de Dominio (DNS) convierte los nombres de dominios, que se forman con combinaciones de letras fáciles de recordar, en direcciones IP, que son cadenas de números difíciles de recordar. Cada ordenador en Internet tiene una dirección única (parecido a el código de un área + un número de teléfono)

DIRECCIÓN IP (INTERNET PROTOCOL)

Una dirección IP es un número que identifica a una computadora en particular en Internet. En la anterior versión 4 del Protocolo de Internet una dirección IP consiste en cuatro bytes (32 bits), casi siempre representados como cuatro enteros en el rango de 0-255 separados por puntos, como 74.54.30.85. En IPv6, a la cual se está cambiando actualmente, una dirección IP es cuatro veces más larga, y consiste en 16 bytes (128 bits). Se puede escribir en 8 grupos de 4 digitos hexadecimales separados por dos puntos como 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

DIRECCIÓN IP ENRUTABLE PUBLICAMENTE

Las direcciones IP enrutables públicamente (algunas veces llamada dirección IP pública) son aquellas que se pueden alcanzar por la vía normal en Internet, a través de una cadena de routers. Algunas direcciones IP son privadas, como el bloque 192.168.x.x, y muchas están sin asignar.

EXPRESIÓN REGULAR

Una expresión regular (llamada también regeexp o RE) es un patrón de texto que especifica una serie de cadenas de texto en una implementación de expresión regular en particular como la utilidad grep de Unix. Una cadena de texto “concuerda” con una expresión regular si la cadena se ajusta al patrón, como se definió en la sintáxis de expresión regular. En cada sintáxis RE, algunos caracteres tienen significados especiales, para permitir que un patrón concuerde con otras cadenas. Por ejemplo, la expresión regular lo+se concuerda con
lose, loose, y looose.

ENRUTADOR

Un enrutador es una computadora que determina la ruta de los paquetes reenviados. Para ello usa la información de dirección en el encabezamiento del paquete y la información “en caché” del servidor para hacer concordar los números de dirección con las conexiones de hardware.

ESCUCHA

La escucha es precisamente escuchar el tráfico de voz o leer o filtrar tráfico de datos en una línea telefónica o una conexión de datos digital, usualmente para detectar o evitar actividades ilegales o indeseadas o controlar o monitorear lo que las personas conversan.

ESTEGANOGRAFÍA

La esteganografía, del griego para escritura oculta, se refiere a una variedad de métodos de envío de mensajes ocultos donde no solo el contenido del mensaje está oculto sino que el hecho mismo de enviar algo encubierto está oculto también. Usualmente esto se hace ocultando algo con algo más, como una imagen o un texto acerca de algo inocente o completamente diferente y sin relación. A diferencia de la criptografía, donde está claro que se ha transmitido un mensaje secreto, la estaganografía no atrae la atención del hecho de que alguien está tratando de ocultar o cifrar un mensaje.

ESQUEMA

En la Web, un esquema es una correspondencia entre un nombre y un protocolo. Así el esquema HTTP mapea URLs que comienzan con HTTP: al Hypertext Transfer Protocol. El protocolo determina la interpretación del resto de la URL, así que http://www.example.com/dir/content.html identifica un sitio Web y un fichero específico en un directorio específico, y mailto:user@somewhere.com es una dirección de correo electrónico de una persona específica o grupo específico en un dominio específico.

FUGA DE DNS

Una fuga de DNS ocurre cuando un ordenador a pesar de estar configurado para usar un proxy para su conexión a Internet hace consultas DNS sin usar dicho proxy, y así expone los intentos de los usuarios al conectarse a sitios boqueados. Algunos navegadores tienen opciones de configuración para forzar el uso del proxy.

FILTRAR

Filtrar es buscar de varias formas patrones de datos específicos para bloquear o permitir las comunicaciones.

FITRO DE ANCHO DE BANDA BAJO

Un filtro de ancho de banda bajo es un servicio Web que elimina elementos extraños como anuncios publicitarios e imágenes de una página web y los comprime, haciendo que la descarga de la página sea mucho más rápida.

FIREFOX

Firefox es el navegador Web gratis y de código abierto más popular, desarrollado por Mozilla Foundation.

FORUM

En un sitio web, un fórum es un lugar de discusión, donde los usuarios pueden escribir mensajes y comentar mensajes enviados anteriormente. Se distingue por una lista de correo o un grupo de noticias Usenet por la persistencia de las páginas que contienen los encabezados. Los archivos de grupos de noticias y listas de correo, a diferencia, típicamente muestran los mensajes uno por página, con páginas de navegación que listan solo los encabezados de los mensajes en un tema.

FTP (FILE TRANSFER PROTOCOL)

El protocolo FTP se usa para la transferencia de ficheros. Muchas personas lo usan para descargas de ficheros; también puede usarse para subir páginas Web y scripts a algunos servidores Web. Normalmente usa los puertos 20 y 21, que muchas veces están bloqueados. Algunos servidores FTP escuchan por un puerto poco común, lo que permite evadir el bloqueo de puertos.
Un cliente FTP gratis y de código abierto para Windows y Mac muy popular es FileZilla. Existen también clientes FTP web que podemos usar con navegador web como el Firefox.

GATEWAY O PUERTA DE ENLACE

Un Gateway es un nodo que conecta dos redes en Internet. Un ejemplo importante es un Gateway nacional que requiere que todo el tráfico que entra y sale pase a través de él.

HONEYPOT

Un honeypot es un sitio que pretende ofrecer un servicio para atraer a usuarios potenciales y capturar información sobre ellos o sus actividades.

HOP (SALTO)

Un hop es un enlace en una cadena de transferencias de paquetes de una computadora a otra, o cualquier computadora a lo largo del camino. El número de hops entre computadoras puede dar un aproximado de la demora (latencia) en las comunicaciones entre ellas. Cada hop individual es también una entidad que tiene la habilidad de "escuchar", bloquear o manipular las comunicaciones.

HTTP (HYPERTEXT TRANSFER PROTOCOL)

HTTP es el protocolo fundamental del Worl Wide Web, que brinda los métodos para solicitar y servir páginas Web, consultando y generando respuestas a las consultas, y accediendo a un gran rango de servicios.

HTTPS (HTTP SEGURO)

HTTP seguro es un protocol para comunicaciones seguras usando mensajes HTTP cifrados. Los mensajes entre el cliente y el servidor son cifrados en varias direcciones, usando llaves generadas cuando se solicita la conexión. Las direcciones IP origen y destino están en los encabezamientos de cada paquete, así que HTTPS no puede ocultar el hecho de la comunicación, solo el contenido de los datos que se envían y se reciben.

IANA (INTERNET ASSIGNED NUMBERS AUTHORITY)

IANA es la organización responsable del trabajo técnico en la gestión de la infraestructura de Internet, incluyendoasignando bloques de direcciones IP a dominios de primer nivel y concediendo licencias a registradores de dominios para ccTLDs y para TLDs genéricos, ejecutando los servidores de nombre raíz de Internet y otras funciones.

ICANN (INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS)

ICANN es una corporación creada por el Departamento de Comercio de Estados Unidos para dirigir los más altos niveles de Internet. El trabajo técnico es desarrollado por IANA.

INTERFAZ DE LÍNEA DE COMANDO

Es un método de control de ejecución de programas usando comandos que se entran con el teclado, como un shell de Unix o la línea de comandos de Windows.

INTERNET

Internet es una red de redes interconectadas que usan TCP/IP y otros protocolos de comunicación.

IRC (INTERNET RELAY CHAT)

IRC es un protocolo de Internet de más de 20 años usado para conversaciones de texto en

tiempo real (chat o mensajería instantánea). Existen varias redes IRC – la más larga tiene más de 50 000 usuarios.

ISP (INTERNET SERVICE PROVIDER)

Un ISP (Internet service provider) es un negocio u organización que brinda acceso a Internet a sus clientes.

JAVASCRIPT

Javascript es un lenguaje de scripts usado en las páginas Web para ofrecer funciones interactivas.

LATENCIA

La latencia es una medida de la demora de tiempo experimentada en un sistema, en una red de computadoras. Está medida por el tiempo entre el inicio de la transmisión del paquete al inicio de la recepción del paquete, entre un extremo de la conexión (nosotros por ejemplo) y el otro (por ejemplo un servidor Web). Una forma muy poderosa de filtrado Web es mantener una latencia bien alta, lo que hace muy difícil el uso de muchas de las herramientas de evasión de censura.

LISTA BLANCA

Es una lista de sitios específicamente autorizados para una forma de comunicación particular. El filtrado del tráfico puede hacerse a través de una lista blanca (bloquear todo excepto los sitios en la lista blanca), o de una lista negra (permitir todo excepto lo que hay en lista negra), o una combinación de las dos, o a través de otras políticas basada en reglas y condiones específicas.

LISTA NEGRA

Una lista negra es una lista de personas o cosas prohibidas. En la censura a Internet, las listas de sitios Web prohibidos se usan como listas negras; las sistemas automáticos de censura pueden restringir el acceso a aquellos que figuran en las listas negras. Una alternativa a la lista negra es la lista blanca, o una lista de cosas permitidas. Este enfoque es menos común en la censura de Internet. Es posible combinar ambos enfoques, haciendo coincidir las cadenas u otras técnicas condicionales en las URLs que no están en ninguna de las dos listas.

MARCADOR

Un marcador de páginas es un marcador de posiciones que contiene una referencia a un recurso externo. En un navegador, un marcador de páginas es una referencia a una página Web – seleccionando el marcador de páginas podemos cargar rápidamente el sitio Web que necesitamos sin necesidad de teclear la URL completa.

MARCO

Un marco es una parte de una página Web con su URL separada. Por ejemplo, los marcos usualmente son usados para colocar un menú estático próximo a una ventana de texto con desplazamiento.

MALWARE

Malware es un término general para programas maliciosos, incluyendo los virus, que pueden ser instalados o ejecutados sin nuestro conocimiento. El malware puede tomar el control de nuestra computadora entre otras cosas para enviar spam. (Malware algunas veces es llamado badware.)

MAN IN THE MIDDLE

Man – in – the – middle es una persona o computadora que captura el tráfico en un canal de comunicaciones, especificamente para cambiar o bloquear selectivamente de manera que se vulnere el cifrado y la seguridad. Este ataque principalmente comprende la suplantación de la identidad de sitios Web, servicios, o personas individuales con el objetivo de registrar o alterar las comunicaciones. Los gobiernos pueden desplegar ataques man-in-the-middle en las compuertas

de entrada o gateways del pais por donde debe pasar todo el tráfico que entra o sale del pais.

MENSAJERÍA INSTANTÁNEA

La mensajería instantánea puede ser formas propietarias de chat usando protocolos propietarios, o chat en general. Los clientes de mesagería instantánea más comunes incluyen MSN Messener, ICQ, AIM o Yahoo! Messenger.

MONITOREAR

Monitorear es chequear un flujo de datos continuamente en busca de actividades indeseadas.

NODO ABIERTO

Un nodo abierto es un nodo Psiphon específico que puede ser usado sin registrarse. Este automáticamente carga una página de bienvenida particular, y se muestra en un idioma en particular, pero puede usarse para navegar a donde queramos.
Ver también nodo Psiphon.

NODO SALIDA

Un nodo salida es un nodo Tor que reenvía datos fuera de la red Tor.
Ver también nodo intermedio.

NODO INTERMEDIO

Un nodo intermedio es un nodo Tor que no es un nodo salida. Ejecutar un nodo intermedio puede ser más seguro que ejecutar un nodo salida pues el nodo intermedio no se mostrará en los ficheros log de terceros. (Un nodo intermedio es llamado muchas veces un nodo de no-salida.)

NODO

Un nodo es un dispositivo activo en una red. Un router es un ejemplo de un nodo. En las redes de Psiphon y Tor, se refieren a un servidor como un nodo también.

NODO DE NO – SALIDA

Ver nodo intermedio.

NODO PSIPHON

Un nodo Psiphon es un proxy web seguro diseñado para evadir la censura de Internet. Es desarrollado por Psiphon inc. Los nodos Psiphon pueden ser abiertos o privados.

NODO PRIVADO

Un nodo privado es un nodo Psiphon que trabaja con autenticación, lo que siginifica que tenemos que registrarnos antes de usarlo. Una vez registrados, podremos enviar invitaciones a los amigos para este nodo en específico.
Ver también nodo Psiphon.

NETWORK ADDRESS TRANSLATION (NAT)

NAT es una función de router para ocultar un espacio de dirección para remapear. Todo el tráfico que sale del router usa la dirección IP del router y el router sabe como enrutar el tráfico entrante hacia el solicitante. NAT es implemetando muchas veces por los cortafuegos. Como las conexiones entrantes son normalmente prohibidas por NAT, es muy difícil que NAT ofrezca un servicio al público general, como un sitio Web o un proxy público. En una red donde se esa NAT, ofrecer este servicio requiere algún tipo de configuración de cortafuegos o método traversal de NAT.

OPERADOR DE RED

Un operador de red es una persona u organización que ejecuta o controla una red y por ello está en la posición de monitoreo, bloqueo, o alteración de las comunicaciones que pasan a través de la red.

OFUSCACIÓN

Ofuscación significa modificar un texto usando técnicas sencillas y reversibles que resistan la inspección casual(no el criptoanális), o hacer cambios menores en cadenas de texto para evitar simples concordancias. Los proxies Web a menudo usan la ofuscación para ocultar ciertos nombres y direcciones y así burlar los filtros.

PUENTE

Ver puente Tor.

PAQUETE

Un paquete es una estrctura de datos definida por un protocolo de comunicación para contener información específica en formas específicas, junto a datos arbitrariospara comunicarlos de un punto a otro. Los mensajes son divididos en partes que se colocarán en un paquete para la transmisión, y se reensamblan en el otro final del enlace.

PUNTO – A – PUNTO

Una red punto a punto (o P2P) es una red de computadoras entre puntos iguales. A diferencia de las redes cliente – servidor no hay un servidor central y por ello el tráfico es distribuído solo entre los clientes. Esta tecnología se aplica mayormente a los programas de intercambio de ficheros como BitTorrent, eMule y Gnutella. Pero además las viejas tecnologías Usenet o el programa de VoIP Skype pueden ser categorizados como sistemas punto – a –punto.
Ver también intercambio de ficheros.

PHP

PHP es un lenguaje diseñado para crear sitios Web dinámicos y aplicaciones Web. Está instalado en un servidor Web. Por ejemplo, el popular proxy Web PHProxy usa esta tecnología.

PRIVACIDAD

La protección de la privacidad personal significa evitar revelar la información personal sin permiso de la persona en cuestión. En el contexto de la evasión de la censura, significa evitar que los observadores sepan que una persona ha buscado o recibido información que haya sido bloqueada o es ilegal en el país donde se encuentra dicha persona.
POP3

Post Office Protocol versión 3 se usa para recibir correo electrónico desde un servidor, por defecto en el puerto 10 con un programa de correo electrónico como el Outlook Express o Thunderbird.

PUERTO

Un puerto de hardware en una computadora es un conector físico para un propósito específico, que usa un protocolo de hardware particular. Algunos ejemplos son puerto de VGA o un conector USB.
Los puertos de software también conectan computadoras con otros dispositivos sobre las redes usando varios protocolos, pero existen en los software solo como números. Los puertos son como puertas enumeradas en diferentes habitaciones, cada uno para un servicio especial en un servidor o en una computadora. Se identifican con números en el rango de 0 a 65535.

PUENTE TOR

Un puente es un nodo intermedio Tor que no está listado en el directorio público de Tor, y así es útil en países donde los relays públicos están bloqueados. A diferencia del caso de los nodos salida, las direcciones IP de los nodos puentes nunca aparecen en los ficheros de log de los servidores y nunca pasan a través de los nodos de monitoreo de forma que puedan ser conectados con la evasión de censura.

PROTOCOLO

Una definición formal de un método de comunicación, y la forma de los datos a ser transmitidos. Además, el propósito de dicho método de comunicación. Por ejemplo,Internet protocol (IP) para transmitir los paquetes de datos en Internet, o Hipertext Transfer Protocol para las interacciones en la Web.

PROXY WEB

Un proxy Web es un script que se ejecuta en un servidor web y que actua como un proxy/Gateway (o puerta de enlace). Los usarios pueden acceder a un proxy web con sus navegadores (como Firefox) y entrar cualquier URL en la forma localizada en ese sitio web. Entonces el programa del proxy web en el servidor recibe ese contenido web y lo muestra al usuario. De esta forma el ISP solo ve una conexión al servidor con el proxy web ya que no hay conexión directa.

RSS (REAL SIMPLE SYNDICATION)

RSS es un método y protocolo para permitir a los usuarios de Internet suscribirse a un contenido de una página Web, y recibir actualizaciones tan rápido como son liberadas.

SERVIDOR DNS

Un servidor DNS, o servidor de nombres, es un servidor que brinda la función de búsqueda del Sistema de Nombres de Dominio. Esto se hace de dos formas: accediendo a un registro en caché de la dirección IP de un dominio específico, o enviando una solicitud de información a otro servidor de nombres.

SERVIDOR PROXY

Un servidor proxy es un servidor, un sistema de computadora o un programa de aplicaciónque actúa como puerta de enlace entre el cliente y el servidor Web. Un cliente se conecta a un servidor proxy para solicitar una página Web de un servidor diferente. El servidor proxy accede al recurso conectándose al servidor específico, y devuelve la información del sitio solicitado. Los servidores proxis pueden servir para diferentes propósitos, incluyendo restricciones del acceso Web o ayudar a los usuarios a enrutarse a través de los obstáculos.

SERVIDOR DE NOMBRE RAÍZ

Un servidor de nombres raíz o servidor raíz es cualquiera de los trece clusters de servidores ejecutados por IANA para direccionar el tráfico a todos los TLDs, como el núcleo del sistema DNS.

SHELL

Un shell de Unix es la interfaz de usuario de una línea de comandos tradicional para los sistemas operativos UNIX/Linux. Los shells más comunes son sh y bash.

SOCKS

Un proxy SOCKS es un tipo especial de servidor proxy. En el modelo ISO/OSI opera entre las capas de aplicación y transporte. El puerto estándar para los proxis SOCKS es 1080, pero también se pueden ejecutar en diferentes puertos. Muchos programas soportan una conexión a través de un proxy SOCKS. Si no podemos instalar un cliente SOCKS como FreeCap, ProxyCap o SocksCap que puede forzar a los programas a ejecutarse a través del proxy Socks usando reenvío de puertos dinámico. Es posible también usar herramientas SSH como OpenSSH como un servidor proxy SOCKS.

SCRIPT

Un script es un programa, usualmente escrito en un lenguaje interpretado, no – compilado como JavaScript, Java o un lenguaje intérprete de comandos como bash. Muchas páginas Web incluyen scripts para manipular la interacción con una página web, para que el servidor no tenga que enviar una nueva página por cada cambio.

SMARTPHONE

En un teléfono móvil que ofrece habilidades más avanzadas de computación y conectividad que los teléfonos contemporáneos, como acceso Web, la habilidad de ejecutar sistemas operativos elaborados y ejecutar aplicaciones incorporadas.

SPAM

Son mensajes que inundan un canal de comunicaciones usado por las personas, sobretodo los anuncios publicitarios enviados a un gran número de individuos o grupos de discusiones. La mayoría de los productos de anuncios spam o servicios que son ilegales en una o varias formas, casi siempre incluyen el fraude. El filtrado de contenido de correo electrónico para bloquear el spam, con el permiso del receptor, está universalmente aprobado.

SSH (SHELL SEGURO)

SSH o Secure Shell es un protocolo de red que permite comunicaciones cifradas entre las computadoras. Fue inventado como sucesor del protocolo sin cifrar Telnet y es usado también para acceder a un Shell en un servidor remoto.
El puerto estándar para SSH es el 22. Puede usarse para sobrepasar la censura de Internet con el reenvío de puertos o puede usarse para pasar por un túnel otros programas como VNC.

SSL (CAPA DE SOCKETS SEGURA)

SSL (o Secure Sockects Layer), es uno de varios estandares de la criptografía usado para hacer seguras las transacciones de Internet. Se usó como base para la creación de Transport Layer Security (TLS). Podemos fácilmente ver si estamos usando SSL/TSL buscando en la URL de nuestro navegador (como Firefox o Internet explorer): Si comienza con https en lugar de http, nuestra conexión está cifrada.

SUBDOMINIO

Un subdominio es una parte de un dominio más largo. Si por ejemplo “wikipwdia.org” es el dominio para Wikipedia. “en.wokipedia.org” es el subdominio para la versión en Inglés de Wikipedia.

TOP – LEVEL DOMAIN (TLD)

En los nombres de Internet, el TLD es el último componente del nombre de dominio. Hay varios TLDs genéricos, los más notables son .com, .org, .net, .gov, .mil, .int y códigos de dos letras (ccTLD) para cada país en el sistema, como .ca para Canadá. La Unión Europea también tiene un código de dos letras .eu.

TLS (TRANSPORT LAYER SECURITY)

TLS o Transport layer security es un estándar de criptografía basado en SSL, usado para hacer seguras las transacciones de Internet.

TCP/IP (TRANSMISSION CONTROL PROTOCOL OVER INTERNET PROTOCOL)

TCP e IP son los protocolos fundamentals de Internet, manipulan la transmisión de paquetes y los enrutan. Existen otros pocos protocolos alternativos que se usan a este nivel de estructura de Internet como UDP.

TÚNEL

Un túnel es una ruta alternativa de una a otra computadora, usualmente incluyendo un protocolo que especifica el cifrado de los mensajes.

TÚNEL DNS

Un túnel DNS es una forma de hacer pasar casi todo por un túnel basado en el protocolo DNS.

Como “abusamos” del sistema DNS para propósitos indeseados, este solo permite una conexión muy lenta de cerca de 3 kb/s lo que es incluso menos que la velocidad de un módem análogo. Esto no es suficiente para YouTube ni para el intercambio de archivos, pero debe ser suficiente para la mensajería instantánea como ICQ o MSN Messenger y también para correo electrónico de texto plano.
En la conexión donde deseamos usar el túnel DNS, solo necesitamos abrir el puerto 53; por lo tanto funcionará incluso en muchos proveedores Wi-Fi comerciales sin necesidad de pagar.
El problema fundamental es que no existen servidores de nombres públicos modificados que podamos usar. Necesitamos configurar uno nosotros mismos. Necesitamos un servidor con conexión permanente a Internet ejecutando Linux. Ahí podemos instalar el programa gratis OzymanDNS y en combinación con SSH y proxy como squid podemos usar el túnel. Para más información vayamos a: http://www.dnstunnel.de.

TEXTO PLANO

El texto plano es texto sin formato que consiste en una secuencia de códigos de caracteres,

como en texto plano ASSCII o texto plano Unicode.

TEXTO CLARO

El textoplano es texto sin cifrar.
Ver también cifrado, SSL, SSH.

UDP (USER DATAGRAM PACKET)

UDP es un protocolo alternativo usado con IP. La mayoría de los servicios de Internet se pueden acceder usando TCP o UDP, pero hay algunos que están definidos para usar solo una de las dos alternativas. UDP es especialmente útil para aplicaciones multimedia en tiempo real como las llamadas telefónicas (VoIP).

URL (UNIFORM RESOURCE LOCATOR)

La URL es la dirección de un sitio Web. Por ejemplo, la URL para la sección de noticias del Mundo del NY Times es http://www.nytimes.com/pages/world/index.html. Muchos sistemas censores pueden bloquear una simple URL. Algunas veces una forma fácil de evadir el bloqueo es oscurecer la URL. Es posible por ejemplo adicionar un punto después del nombre del sitio, así la URL http://en.cship.org/wiki/URL se convierte en http://en.cship.org./wiki/URL. Si tenemos suerte con este truco en el título podemos acceder sitios Web bloqueados.

USENET

Usenet es un forum de discusión de más de 20 años que se accede usando el protocolo NNTP. Los mensajes no son almacenados en un servidor sino en varios que distribuyen su contenido constantemente. Es por esto que es imposible censurar Usenet completo, sin embargo el acceso a Usenet puede y es casi siempre bloqueado, y cualquier servidor particular solo acepta una subserie de grupos de noticias localmente aceptados. Google archiva toda la historia disponible de mensajes de Usnet para la búsqueda.

VOIP (VOICE OVER INTERNET PROTOCOL)

VoIP se refiere a cualquiera de los varios protocolos para comunicaciones de de voces en dos direcciones en tiempo real en Internet, lo que usualmente es mucho menos caro que llamar a través de redes de voz de compañías telefónicas. It is not subject to the kinds of wiretapping practiced on telephone networks, pero puede ser monitoreado usando tecnología digital. Muchas companies producen softwares y equipamiento para “escuchar” en llamadas VoIP; las tecnologías VoIP cifradas y seguras recientemente han comenzado a surgir.

VPN (VIRTUAL PRIVATE NETWORK)

Una VPN es una red de comunicación privada usada por muchas compañías y organizaciones para conectarse de forma segura sobre una red pública. Usualmente está expuesta de forma cifrada en Internet y así nadie excepto los extremos finales de la comunicación pueden ver todo el tráfico de los datos. Hay varios estándares como IPSec, SSL, TSL o PPTP. El uso de un proveedor VPN es un método convenitnte , seguro y rápido para evadir la censura de Internet con pequeños riesgos pero generalmente cuesta una cantidad de dinero mensual.

WORL WIDE WEB (WWW)

El Worl Wide Web es una red de domiios enlazados y páginas de contenido accesibles usando Hypertext transfer Protocol y sus numerosas extensiones. El Worl Wide Web es la parte más famosa de Internet.

WEBMAIL

El webmail es un servicio de correo electrónico a través de un sitio Web. El servicio envía y recibe mensajes de correo de usuarios en la forma usual, pero brinda una interfaz Web para leer

y manipular los mensajes, como alternativa a ejecutar un cliente de correo electrónico como Outlook express o Thunderbird en la computadora de los usuarios. Por ejemplo un servicio webmail gratos y muy popular es https://mail.google.com/.

WHOIS

WHOIS (quien es) es el nombre apropiado para la función de Internet que permite consultar bases de datos remotas WHOIS para información de registración de dominios. Haciendo una simple búsqueda WHOIS podemos descubrir cuando y por quien fue registrado un dominio, información de contacto, y más.
Una búsqueda WHOIS puede también revelar el nombre o el mapa de red de una dirección numérica IP.

40. DIEZ COSAS

por Roger Dingledine, lider del Proyecto Tor

A medida que más países atacan el uso de Internet, más personas alrededor del mundo se amparan en soluciones de software anticensura que les permita navegar por sitios bloqueados. Muchos tipos de aplicaciones, también conocidas como "**herramientas de evasión**", han sido creadas para responder a las amenazas a la libertad en línea. Estas herramientas proveen diferentes características y niveles de seguridad, es importante para los usuarios entender también cuáles son sus prestaciones.'

Éste artículo expone 10 características que deben tenerse en cuenta cuando se evalúe una herramienta de evasión. El objetivo no es favorecer alguna herramienta específica, sino señalar que tipo de herramienta es más útil según la situación en que estemos. He escogido el orden de estas características basado en la simplicidad de su exposición, no debe implicarse por tanto que las primeras sean más críticas.

Las herramientas de evasión basadas en Internet constan de dos componentes: un componente repetidor(relay) y un componente de *detección*(discovery). El componente repetidor establece la conexión a algún servidor o **proxy**, maneja el **cifrado**, y hace pasar el tráfico en las dos direcciones. El componente tramitador es el paso previo necesario para encontrar esos servidores proxy.

Algunas herramientas tienen un componente de tramitación muy simple. Por ejemplo, si estamos usando un proxy abierto, el proceso de usarlo es muy básico: se configura el navegador web o aplicación para usar el proxy. El gran reto para los usuarios de proxis es encontrar un proxy abierto que sea confiable y rápido. Por otra parte, algunas herramientas tienen componentes de tramitación mucho más sofisticados, hechos por múltiples proxis, múltiples capas de cifrado, y así.

Una advertencia antes de empezar: soy el inventor y desarrollador de una herramienta llamada TOR que es usada tanto para privacidad como para evasión. Aún cuando mi parcialidad hacia herramientas más seguras como TOR se muestra aquí basada en las características que he seleccionado para discutir(hablo de temas que subrayan las fortalezas de TOR y que pueden no tener tanta importancia para otros desarrolladores de herramientas), he intentado seleccionar aquellas características que otros desarrolladores de herramientas consideran importantes.

1. Una base de usuarios heterogénea

Una de las cuestiones más simples que pueden preguntarse cuando se está buscando una herramienta de evasión es quién más la utiliza. La existencia de una gran variedad de usuarios implica que si alguien nos descubre usándola no puede sacar muchas conclusiones acerca del por qué estamos usándola. Una herramienta de privacidad como TOR tiene muchas clases diferentes de usuarios (desde personas ordinarias, activistas pro derechos humanos, corporaciones, fuerzas del orden y hasta militares) por tanto el hecho de que tengamos TOR instalado no da mucha información acerca de quiénes somos o qué tipo de sitios estamos visitando. Por otra parte, imaginemos un grupo de blogueros Iraníes usando una herramienta de evasión creada especialmente para ellos. Si alguien descubre que uno de ellos está usándola, puede fácilmente adivinar por qué.

Más allá de las características técnicas que hacen que una herramienta sea útil para algunas personas en un país o para muchas personas alrededor del mundo, el enfoque de mercado juega un papel muy importante sobre cuales personas serán sus potenciales usuarios.
Muchas herramientas se difunden de mano en mano, de forma que si algunos usuarios están en Vietnam y la encuentran útil, es probable que los próximos usuarios también sean de Vietnam. El hecho de que una herramienta tenga una interfaz traducida a algunos idiomas y no a otros también puede facilitar (o impedir) el uso por parte algunos conjuntos de internautas.

2. Funciona en nuestro país

La próxima cuestión a considerar es si el creador de la herramienta restringe artificialmente desde qué países se puede usar. Por muchos años, el proveedor comercial Anonymizer.com ha hecho que sus servicios estén disponibles gratuitamente en Irán. De esta manera las conexiones salientes de los servidores de Anonymizer podían ser tanto de clientes que pagaban el servicio (mayormente en América) o personas en Irán tratando de escapar de los filtros de su país.

Como ejemplos más recientes,Your-Freedom restringe el uso gratuito a unos pocos países como por ejemplo Burma, mientras que en casos como el de Freegate y Ultrasurf se bloquea totalmente las conexiones desde todos los países exceptuando un grupo de países a los que ellos se preocuparon por proveerles el servicio(China, y recientemente Irán, en el caso de Ultrasurf). Por otra parte, esta estrategia es lógica en términos de limitar los costos de ancho de banda. Pero por otra parte, si estuviésemos en Arabia Saudita y necesitáramos una herramienta de evasión, podríamos carecer de opciones que de otra manera nos serían útiles.

3. Tiene una estrategia de desarrollo de sus redes y su software sostenible

Si fuéramos a invertir tiempo en averiguar cómo usar una herramienta dada, deberíamos estar seguros que ésta estará disponible al menos por un tiempo. Existen varias maneras en que las diferentes herramientas aseguran su existencia a largo plazo. Los principales tres enfoques son el uso de voluntarios, el ánimo de lucro, y la financiación de por parte de patrocinadores.

Las redes como TOR dependen de los voluntarios que proveen de los repetidores que conforman la red. Miles de personas alrededor del mundo tienen computadoras con buenas condiciones de conectividad y además ganas de hacer del mundo un mejor lugar. Al unir esas computadoras en una gran red, TOR asegura que la red se mantenga independiente de la organización que hace la solución informática. Asi que la red seguirá existiendo aún cuando el Proyecto TOR deje de existir como una entidad. Psiphon asume el enfoque de obtener ganancias económicas. Su razón es simple: si pueden mantener una compañía rentable, entonces esa compañía será capaz de mantener funcionando la red de forma sostenible y creciente. El Java Anon Proxy depende de financiación oficial para hacer funcionar su red, ahora que el otorgamiento oficial ha terminado están explorando un esquema de pago. Ultrareach y Freegate usan el modelo de patrocinio con buenos resultados, aunque están constantemente buscando más patrocinadores para mantener su red operativa.

La otra preocupación aparte de la propia sobrevivencia de la red es la cuestión de la sostenibilidad de la solución de software. Los mismos tres enfoques se aplican aquí, pero los ejemplos cambian. Mientras la red TOR está operada por voluntarios, TOR depende de patrocinadores (gobiernos y ONGs) para financiar nuevas funcionalidades y para el mantenimiento del software. Ultrareach y Freegate por otra parte están en una mejor posición con respecto a las actualizaciones del software: tienen un equipo de individuos alrededor del mundo, mayormente voluntarios, devotos a asegurar que la herramienta esté un paso por delante de sus perseguidores.

Cada uno de los tres enfoques puede funcionar, pero entender cual enfoque es el usado por una herramienta puede ayudarnos a predecir que problemas puede enfrentar en un futuro.

4. Tienen un diseño abierto

El primer paso para la transparencia y reusabilidad del diseño y software de la herramienta es distribuir el software (no solamente el cliente, sino también el servidor) bajo una licencia de código abierto. Una de código abierto significa que cualquiera puede examinar el software, verificar de qué forma trabaja internamente, y además se tiene el derecho a modificar el programa. Aún cuando no todos los usuarios saquen ventajas de esta oportunidad (la mayoría de los usuarios solo están interesados en usar la herramienta tal cual la obtuvieron), proveerlos de la opción hace mucho más probable que la herramienta se mantenga funcional y útil con el tiempo. De otra manara estamos forzados a confiar en lo que un grupo de desarrolladores han pensado y a asumir que ellos han pensado en cada problema posible.

Solo proveer de una licencia de código abierto no es suficiente. Las herramientas de evasión confiables necesitan proveer de una clara y completa documentación para que terceras partes expertas en seguridad puedan saber no solo como se construyó sino también qué características y objetivos persiguieron sus desarrolladores. ¿La idearon como herramienta de privacidad? ¿Qué tipo de privacidad y contra qué ataques? ¿En qué modo usan el cifrado? ¿Pretenden que resista los ataques de los censuradores? ¿Qué tipo de ataques esperan que resista y por qué la herramienta los resiste? Sin ver el código fuente y sin saber qué persiguieron sus desarrolladores es más difícil decidir si hay problemas de seguridad en la herramienta, o evaluar si ésta logra sus objetivos.

En el campo de la criptografía, el principio de Kerckhoff explica que uno tiene que diseñar un sistema para que la parte que se mantenga en secreto sea lo más pequeña y comprensible posible. Es por eso que los algoritmos de cifrado usan llaves(la parte secreta) y el resto puede ser explicado en público a cualquiera. Historicamente, un diseño criptográfico que tiene muchas partes secreta ha demostrado ser menos seguro que lo que sus diseñadores pensaron.

Similarmente ocurre en el caso de las herramientas de evasión que no son de código abierto. El único grupo examinando la herramienta son sus desarrolladores originales y los atacantes, el resto de los desarrolladores y usuarios que pudieran ser de ayuda para hacerla mejor y más sostenible son dejados fuera.

Las ideas de un proyecto pueden ser reutilizadas más allá del tiempo de vida de un proyecto. Un número demasiado grande de herramientas de evasión mantienen su diseño en secreto, con la esperanza de que los censuradores de los gobiernos tendrán que pasar más trabajo para determinar cómo el sistema funciona, pero el resultado es que pocos proyectos pueden sacar provecho de otros proyectos y el campo del desarrollo de herramientas de evasión como un todo se evoluciona muy lentamente.

5. Tiene una arquitectura descentralizada

Otra característica a buscar en una herramienta de evasión es que su red esté centralizada o descentralizada. Una herramienta centralizada pone todas las peticiones de sus clientes en uno o unos pocos servidores que el operador de la herramienta controla. Un diseño descentralizado como TOR o JAP envía el tráfico a través de múltiples nodos diferentes de forma que no hay una localización central o entidad que pueda verificar que sitios web un usuario está tratando de acceder.

Otra forma demorar a esta división es basarse en cuando la confianza es centralizada o descentralizada. Si uno tiene que poner toda la confianza en una entidad entonces lo mejor que uno puede esperar es "privacidad por política", que significa que ellos tienen todos nuestros datos y ellos prometen no mirarlos, borrarlos o venderlos.
La alternativa es lo que el Comisionado para la Privacidad de Ontario llama "privacidad por diseño", que significa que el sistema en si mismo asegura que el usuario obtenga su privacidad. La condición abierta del diseño, en cambio, deja a otros evaluar el nivel de privacidad provisto.

Esta preocupación no es solamente teórica. En los inicios de 2009 Hal Roberts del Centro Berkman encontró una entrada en una FAQ de una herramienta de evasión que ofrecía vender los registros de clicks de sus usuarios. En otra ocasión habló con otro proveedor de herramienta de evasión que mantenía todos los registros de la actividad de sus usuarios porque "nadie sabe cuándo nos pueda hacer falta".

He dejado fuera los nombres de las herramientas porque el punto no es que tal o cual proveedor pueda haber compartido nuestros datos, el punto es que cualquier herramienta con una arquitectura centralizada puede compartir nuestros datos, y los usuarios no tenemos garantía alguna de que esto no esté pasando. Peor, aún cuando el proveedor de la herramienta tenga buenas intenciones el hecho de que todos los datos fluyan por un punto central crea un objetivo atractivo para que los atacantes vengan a husmear.

La mayoría de estas herramientas ven evasión y privacidad como objetivos totalmente separados. Esta separación no es necesariamente mala, mientras uno sepa por supuesto en qué se está metiendo. Escuchamos de mucha gente en países donde hay censura que el solo hecho de entrar en un sitio de noticias puede ponerte tras las rejas. Pero tal y como hemos venido viendo en otros contextos a lo largo de muchos años las largas bases de datos con información personal tienden a terminar siendo más publicas de lo que uno desearía.

6. Nos mantiene a salvo también de los sitios web

Cuando de privacidad se trata, no es suficiente con protegernos contra lo que el operador de la herramienta pueda hacer con nuestros registros de navegación, también hay que tomar en cuenta que los sitios web que visitemos pueden reconocernos y rastrearnos. Recordemos el caso de Yahoo dando información sobre uno de sus usuarios de webmail. Qué hay si un operador de blog quiere averiguar quién está posteando en un blog, o quién adicionó el último comentario, o qué otros sitios web un bloguero particular lee. Usando una herramienta más segura para acceder a un sitio implicará que este último no tendrá mucha información qué manejar.

Algunas herramientas de evasión son más seguras que otras. En un extremo están los proxis abiertos, ellos simplemente reenvían la dirección del cliente con su petición web, de manera que es fácil para un sitio web saber de dónde vino la petición exactamente. En el otro extremo están las herramientas como TOR, que incluyen extensiones del lado del cliente para esconder la versión del browser, preferencias de idioma, tamaño de la ventana del browser, zona horaria, y otras; además restringe los cookies, historial de navegación, caché y previene que otros complementos como Flash filtren información acerca de los usuarios.

Este nivel de protecciones de nivel de aplicación tiene un costo: algunos sitios web no trabajan correctamente. Mientras más sitios web evolucionen hacia los modismos del "web 2.0", requerirán más y más características invasivas con respecto al comportamiento de los navegadores. La respuesta más sabia es deshabilitar los comportamientos más peligrosos, pero si alguien en Turquía está tratando de ver un video en YouTube y Tor deshabilita su complemento de Flash para que éste esté a salvo, sus videos no se mostrarán.

Ninguna herramienta ha resuelto este problema bien aún. Psiphon manualmente evalúa cada sitio y programa su proxy central para que reescriba cada página. Esta reconfiguración se hace principalmente no por privacidad, sino para asegurar que los links en la página nos lleven de vuelta a su servicio de proxy, pero el resultado es que ellos no han inspeccionado manualmente el sitio web destino que uno va a consumir, es probable que el mecanismo no funcione. A manera de ejemplo, al parecer ellos están en una batalla constante para mantenerse actualizados de los cambios en la página principal de facebook. Tor actualmente deshabilita algún contenido que es usualmente seguro en la práctica, simplemente porque no hemos encontrado una interfaz de usuario apropiada para dejar que el usuario decida de una manera informativa. Otras herramientas simplemente dejan pasar cualquier contenido activo, significando que es trivial para los sitios web descubrir quiénes son los usuarios.

7. No promete cifrar mágicamente toda la internet

Debo trazar una separación entre cifrado y privacidad. La mayoría de las herramientas de evasión (todas excepto las realmente simples, como los proxis abiertos) cifran el tráfico entre el usuario y el proveedor de evasión. Ellos necesitan el cifrado para evitar la censura basada en palabras claves hechas por ejemplo el gran firewall de China. Pero ninguna de las herramientas cifra el tráfico entre el proveedor y el sitio web final si un sitio web final no soporta cifrado; no existe forma mágica de hacer que el tráfico esté cifrado.

La respuesta ideal sería que todo el mundo usara HTTPS (también conocido como SSL) cuando trataran de acceder a algún sitio web, y para todos los sitios que soporten conexiones HTTPS. Cuando se usa correctamente HTTPS provee una capa de cifrado entre el navegador web. Este cifrado "de extremo a extremo" significa que nadie en la red (ni siquiera nuestro proveedor de servicios de internet, ni los proveedores de evasión, ni nadie) pueden descifrar lo que está pasando entre el navegador y el sitio web accedido. Pero por un numero de razones, la era en que el cifrado sea omnipresente aún no ha llegado. Si el sitio web destino no soporta cifrado, lo mejor que se puede hacer es 1) no mandar información que sensible o que nos identifique tal y como lo son nuestro nombre real en una publicación de un blog o una contraseña que queremos salvaguardar del conocimiento ajeno y 2) usar una herramienta de evasión que no haga pasar tu tráfico por alguna dependencia central pueda potencialmente permitir que alguien nos vincule con el tráfico que estamos generando a pesar del punto haber observado el punto 1.

Desafortunadamente, las cosas se complican cuando uno no puede evitar mandar información sensible. Algunas personas han expresado preocupación acerca de la red de TOR sostenida por esfuerzos voluntarios bajo el razonamiento que al menos con un diseño centralizado uno sabe quién es el que está operando la infraestructura. Pero en la práctica consistirá de extraños leyendo nuestro tráfico en ambos sentidos. La decisión sería entre voluntarios desconocidos que no saben quiénes somos (y por tanto carecen de referencia alguna hacia nosotros) y extraños dedicados que pueden ver y perfilar nuestro tráfico (y vincularlo a nosotros). Cualquiera que prometa "100% seguridad" está vendiéndonos algo.

8. Provee una buena latencia y velocidad

La próxima característica que podríamos mirar en una herramienta de evasión es velocidad. Algunas herramientas tienen a ser estables en su rapidez, otras establemente lentas, y otras proveen de una calidad de servicio impredecible. La velocidad se basa en muchos factores, incluyendo cuantos usuarios tiene el sistema, qué están haciendo los usuarios, cuanta capacidad hay instalada, y si la carga está distribuida equitativamente a través de la red.

El diseño de dependencia-central tiene dos ventajas aquí. Primero, pueden ver todos los usuarios y lo que éstos están haciendo lo que permitiría distribuirlos equitativamente y potencialmente atajar situaciones técnicas que pueda embargar el sistema. En segundo lugar, los proveedores pueden comprar más capacidad en caso que la necesiten, de esta manera mientras más inviertan más rápida será la herramienta. El diseño distribuido por otra parte la tiene más difícil para rastrear a sus usuarios, y si dependen de voluntarios para contar con capacidad, entonces buscar más voluntarios es una tarea más compleja que simplemente pagar por más ancho de banda.

La cara opuesta de la moneda del desempeño es la flexibilidad. Muchos sistemas aseguran una buena velocidad limitando lo que sus usuarios pueden hacer. Mientras que Psiphon nos impide navegar por sitios que ellos no hallan habilitado manualmente, Ultrareach y Freegate en realidad censuran que sitios se pueden acceder usando el servicio para así mantener bajos los costes de ancho de banda. Tor por el contrario nos permite acceder cualquier protocolo o destino, significando por ejemplo que podemos mandar mensajes instantáneos a través de éste, pero la parte negativa es que a veces la red está sobrecargada por usuarios que están haciendo transferencias voluminosas.

9. Es fácil obtener el software y actualizarlo

Una vez que una herramienta de evasión se hace famosa, su sitio web será bloqueado. Si es imposible obtener una copia de la herramienta. ¿A quién le importa cuán buena pueda ser? La mejor respuesta aquí es no requerir ningún cliente especializado. Psiphon por ejemplo solo depende de un browser normal, de esta manera no interesa si el censurador bloquea su sitio web. Otro enfoque es un pequeño programa como Ultrareach o Freegate que uno puede enviar a sus amigos en un mensaje. La tercera opción es el paquete para navegadores de Tor: viene con todo el software necesario que necesitamos pre configurado, pero como incluye programas grandes como Firefox es más difícil compartirlo online. En este caso, la distribución tiende a ser a través de redes sociales y memorias flash o usando nuestro auto-respondedor de emails que nos permite descargar Tor via Gmail.

Cuando uno necesita tomar en cuenta las decisiones que vienen con cada enfoque. El primero, qué sistema operativos están soportados? Psiphon también saca una buena nota aquí, ya que al no requerir de ningún software extra. Ultrareach y Freegate están tan especializados que solo trabajan en Windows, mientras que TOR y su software acompañante pueden ejecutarse prácticamente en cualquier plataforma. Lo próximo es que el cliente pueda automáticamente manejar las fallas de un proxy y cambiar a otro de esta manera no tenemos que escribir manualmente las nuevas direcciones de los proxis si las actuales son bloqueadas o desaparecen.

Por último. ¿Suele la herramienta manejar bien el hecho de ser bloqueada? Por ejemplo, Ultrasurf y Freegate tiene un largo historial de actualizaciones cada vez que las versiones actuales de su software dejan de funcionar por algún motivo. Ellos tienen una vasta experiencia en este campo de manera que es razonable asumir que estarán listos para el próximo round. En medio de todo esto, Tor se ha ido preparando para su eventual bloqueo reformando sus comunicaciones para que luzcan mas como una comunicación web ordinaria y mediante la introducción de "repetidores" que son más difíciles de descubrir por algún atacante y bloquear que los repetidores públicos de TOR. TOR trata de separar las actualizaciones de software de las actualizaciones de las direcciones de los proxis. Si el repetidor que estamos usando es bloqueado podemos quedarnos con el mismo software y simplemente configurarlo para que use nuevos repetidores. El diseño de repetidores fue puesto a prueba en China en septiembre del 2009, y decenas de miles de usuarios se movieron simplemente de los repetidores públicos a los repetidores puentes.

10. No se anuncia a sí misma como una herramienta de evasión

Muchas herramientas de evasión lanzan una gran campaña mediática. A los medios les gusta este enfoque y terminan incluyendo artículos en primera plana con titulares estilo "Hackers Americanos declaran la guerra a China!". Pero mientras esta atención atrae soporte de voluntarios, ganancias y patrocinadores, la publicidad también atrae a los esfuerzos de los censores.

Los censuradores generalmente bloquean dos categorías de herramientas: 1) las que están trabajando realmente bien, lo que significa que tienen cientos de miles de usuarios y 2) las que hacen un gran ruido. En muchos casos la censura es menos acerca de bloquear todo el contenido sensible y más acerca de crear una atmosfera de represión para que las personas terminen censurándose a sí mismas. Artículos en la prensa amenazan retan un poco la apariencia que dan los censuradores de tener la situación bajo control y de esta manera los fuerzan a responder.

La lección aquí es que podemos controlar el paso de la carrera armamentística. Paradójicamente, aún cuando una herramienta tenga muchos usuarios, mientras a nadie se le ocurra hablar mucho de ella, tiende a pasar desapercibida. Pero si nadie habla de ella, ¿cómo los usuarios la llegan a conocer? Una salida de esta paradoja es hacer que se corra la voz de boca en boca y a través de redes sociales en ves de hacerlo por los medios más tradicionales. Otro enfoque es posicionar la herramienta en un contexto diferente; por ejemplo, presentamos TOR primariamente como una herramienta para la privacidad y para las libertades civiles, y no tanto como una herramienta de evasión. Desdichadamente este balance es difícil de mantener de frente a su incrementada popularidad.

Conclusiones

Este artículo explica algunos de los elementos que debemos considerar al evaluar las fortalezas y debilidades de una herramienta de evasión. He evitado intencionalmente trazar tabla comparativa con las diferentes herramientas y hacer marcas en cada categoría. No dudo que alguien haga eso eventualmente y sume cuantas marcas tiene cada herramienta, pero el punto no es encontrar la "mejor" herramienta. Tener una diversidad de herramientas de amplio espectro incrementan la robustez de todas las herramientas ya que los censuradores tienen que lidiar con cada estrategia por separado.

Debemos tener en cuenta que la tecnología no resolverá todo el problema. Después de todo, los cortafuegos son *socialmente* muy efectivos en esos países. Mientras más personas en países censurados estén diciendo "Estoy tan contento de que mi gobierno me mantenga a salvo en Internet" los retos sociales son al menos tan importantes como los técnicos. Pero al mismo tiempo, existen personas en cada uno de esos países que quieren saber y difundir información online, y una solución técnica fuerte es una pieza crítica del rompecabezas.

Roger Dingledine es el líder del Proyecto TOR, una organización norteamericana sin ánimo de lucro que trabaja en investigaciones de anonimato y desarrolla para organizaciones tan diversas como el Ejercito Americano, la Organización Frontera Electrónica, y la Voz de América. Adicionalmente a todos los roles que él funge en TOR, Roger también organiza conferencias académicas sobre anonimato, habla en una amplia variedad de foros de hackers y de la industria, y además da tutoriales de anonimato digital para las autoridades nacionales y foráneas.

41. OTROS MATERIALES

Sortear la censura de Internet es un tema muy amplio. Existen muchas cosas a tomar en cuenta si queremos que nuestras actividades al respecto sean difíciles de detectar o bloquear en un futuro, si queremos lograr anonimato en el uso de Internet, o si queremos ayudar a otras personas a sortear la censura. Aquí se listan algunos materiales adicionales para el que quiera profundizar acerca de materias relacionadas (algunos de estos materiales pueden no estar disponibles o pueden estar bloqueados en algunos lugares).

MANUALES Y GUÍAS

Sortear la Censura de Internet

- Reporteros sin fronteras, *Manual de Blogueros y Ciberdisidentes,* http://www.rsf.org/article.php3?id_article=26187
- La Wiki de la Censura en Internet, http://en.cship.org/wiki/

Recomendaciones de seguridad para activistas

- ONG-en-una-Caja, una colección de aplicaciones portables, https://security.ngoinabox.org
- Seguridad Digital y Privacidad para Defensores de los Derechos Humanos, https://www.frontlinedefenders.org/esecman
- La Internacional para la Autodefensa contra la Vigilancia, https://www.eff.org/wp/surveillance-self-defense-international

Estudios sobre censura de Internet

- 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
- Mas recursos sobre censura de internet http://bailiwick.lib.uiowa.edu/journalism/mediaLaw/cyber_censors.html

ORGANIZACIONES QUE TRABAJAN EN DOCUMENTAR ENFRENTAR O SORTEAR LAS RESTRICCIONES DE ACCESO A INTERNET

- 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)

PROXIS LIBRES Y PROXIS WEB

- Proxy.org, un listado de miles de proxis abiertos: http://www.proxy.org
- Una lista de correo que envía proxis web nuevos: http://www.peacefire.org/circumventor/,
- Proxis:
  - http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists/
  - http://www.publicproxyservers.com

SOLUCIONES DE EVASIÓN Y PROVEEDORES DE SERVICIO

- 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/

Lista de proveedores de VPN comerciales

- http://en.cship.org/wiki/VPN

Software para la socksificación (hacer que un software no preparado para usar proxis funciones con un proxy SOCKS)

- 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

INTRODUCTION

Modifications:
gravy - A Ravi Oli 2011
Mokurai - Edward Mokurai Cherlin 2011
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
poser - Poser 2011
lalala - laleh 2011

ABOUT THIS MANUAL

Modifications:
Zorrino - Zorrino Hermanos 2011
booki - adam or aco 2011

QUICKSTART

Modifications:
booki - adam or aco 2011
erinn - Erinn Clark 2011
puffin - Karen Reilly 2011
freerk - Freerk Ohling 2011
Zorrino - Zorrino Hermanos 2011
helen - helen varley jamieson 2011
poser - Poser 2011
schoen - Seth Schoen 2011

HOW THE NET WORKS

Modifications:
booki - adam or aco 2011
gravy - A Ravi Oli 2011
lalala - laleh 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

CENSORSHIP AND THE NET

Modifications:
gravy - A Ravi Oli 2011
booki - adam or aco 2011

freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

CIRCUMVENTION AND SAFETY

Modifications:
gravy - A Ravi Oli 2011
booki - adam or aco 2011
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011

INTRODUCTION

Modifications:
booki - adam or aco 2010

ABOUT THIS MANUAL

Modifications:
booki - adam or aco 2010

SIMPLE TRICKS

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
poser - Poser 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

GET CREATIVE

Modifications:
freerk - Freerk Ohling 2011
DavidElwell - David Elwell 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

WEB PROXIES

Modifications:
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
lalala - laleh 2011
poser - Poser 2011
booki - adam or aco 2011

WHAT IS CIRCUMVENTION

Modifications:
booki - adam or aco 2010

PSIPHON

Modifications:
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
helen - helen varley jamieson 2011
poser - Poser 2011
booki - adam or aco 2011

AM I BEING CENSORED?

Modifications:
booki - adam or aco 2010

DETECTION AND ANONYMITY

Modifications:
booki - adam or aco 2010

SABZPROXY

Modifications:
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

HOW THE NET WORKS

Modifications:
booki - adam or aco 2010

INTRODUCTION TO FIREFOX

Modifications:
SamTennyson - Samuel L. Tennyson 2011
booki - adam or aco 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
freerk - Freerk Ohling 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

WHO CONTROLS THE NET

Modifications:
booki - adam or aco 2010

FILTERING TECHNIQUES

Modifications:
booki - adam or aco 2010

ADBLOCK PLUS AND NOSCRIPT

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
scherezade - Genghis Kahn 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

HTTPS EVERYWHERE

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011

SIMPLE TRICKS

Modifications:
booki - adam or aco 2010

PROXY SETTINGS AND FOXYPROXY

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

USING A WEB PROXY

Modifications:

INTRODUCTION

Modifications:
gravy - A Ravi Oli 2011
freerk - Freerk Ohling 2011
erinn - Erinn Clark 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
poser - Poser 2011

USING PHProxy

Modifications:

FREEGATE

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

USING PSIPHON

Modifications:

USING PSIPHON2

Modifications:

SIMURGH

Modifications:
booki - adam or aco 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
freerk - Freerk Ohling 2011

ULTRASURF

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

USING PSIPHON2 OPEN NODES

Modifications:

VPN SERVICES

Modifications:
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011

lalala - laleh 2011
booki - adam or aco 2011

RISKS

Modifications:

VPN ON UBUNTU

Modifications:
SamTennyson - Samuel L. Tennyson 2011
booki - adam or aco 2011
scherezade - Genghis Kahn 2011
freerk - Freerk Ohling 2011

HOTSPOT SHIELD

Modifications:
booki - adam or aco 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

ADVANCED BACKGROUND

Modifications:

HTTP PROXIES

Modifications:

ALKASIR

Modifications:
booki - adam or aco 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

TOR: THE ONION ROUTER

Modifications:
freerk - Freerk Ohling 2011
erinn - Erinn Clark 2011
puffin - Karen Reilly 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
helen - helen varley jamieson 2011
lalala - laleh 2011

INSTALLING SWITCH PROXY

Modifications:

USING SWITCH PROXY

Modifications:

JONDO

Modifications:
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011

rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

YOUR-FREEDOM

Modifications:
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

TOR: THE ONION ROUTER

Modifications:

USING TOR BROWSER BUNDLE

Modifications:

DOMAINS AND DNS

Modifications:
gravy - A Ravi Oli 2011
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

USING TOR IM BROWSER BUNDLE

Modifications:
SahalAnsari - Sahal Ansari 2010

HTTP PROXIES

Modifications:
booki - adam or aco 2011
lalala - laleh 2011
scherezade - Genghis Kahn 2011
helen - helen varley jamieson 2011

USING TOR WITH BRIDGES

Modifications:

THE COMMAND LINE

Modifications:
booki - adam or aco 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

USING JON DO

Modifications:

OPENVPN

Modifications:
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

SSH TUNNELLING

Modifications:
freerk - Freerk Ohling 2011
booki - adam or aco 2011

WHAT IS VPN?

Modifications:

OPENVPN

Modifications:

SOCKS PROXIES

Modifications:
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011
lalala - laleh 2011
booki - adam or aco 2011

SSH TUNNELLING

Modifications:

RESEARCHING AND DOCUMENTING CENSORSHIP

Modifications:
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

SOCKS PROXIES

Modifications:

DEALING WITH PORT BLOCKING

Modifications:
booki - adam or aco 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

INSTALLING WEB PROXIES

Modifications:
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

INSTALLING WEB PROXIES

Modifications:

SETTING UP A TOR RELAY

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

INSTALLING PHProxy

Modifications:

RISKS OF OPERATING A PROXY

Modifications:
freerk - Freerk Ohling 2011
schoen - Seth Schoen 2011

INSTALLING PSIPHON

Modifications:

SETTING UP A TOR RELAY

Modifications:

BEST PRACTICES FOR WEBMASTERS

Modifications:
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

RISKS OF OPERATING A PROXY

Modifications:

GLOSSARY

Modifications:
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Mokurai - Edward Mokurai Cherlin 2011

TEN THINGS

Modifications:
Zorrino - Zorrino Hermanos 2011
booki - adam or aco 2011
puffin - Karen Reilly 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

FURTHER RESOURCES

Modifications:

FURTHER RESOURCES

Modifications:
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

GLOSSARY

Modifications:

CREDITS

Modifications:
booki - adam or aco 2011

CREDITS

Modifications:

The below is information for pre-2011 content

AUTHORS

ABOUT THIS MANUAL
© adam hyde 2008
Modifications:
Austin Martin 2009
Edward Cherlin 2008
Janet Swisher 2008
Tom Boyle 2008
Zorrino Zorrinno 2009

ADVANCED BACKGROUND
© Steven Murdoch And Ross Anderson 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

DETECTION AND ANONYMITY
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

RISKS
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Austin Martin 2009
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

SOCKS PROXIES
© Seth Schoen 2008
Modifications:
adam hyde 2008
Freerk Ohling 2008, 2009
Tom Boyle 2008

USING SWITCH PROXY
© adam hyde 2008, 2009
Modifications:
Alice Miller 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

CREDITS
© adam hyde 2006, 2007, 2008
Modifications:
Edward Cherlin 2008

FILTERING TECHNIQUES
© Edward Cherlin 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Janet Swisher 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

FURTHER RESOURCES
© adam hyde 2008
Modifications:
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008, 2009

GLOSSARY
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

AM I BEING CENSORED?
© adam hyde 2008
Modifications:
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

HOW THE NET WORKS
© Frontline Defenders 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

INSTALLING WEB PROXIES
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008

Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

INSTALLING PHProxy
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

INSTALLING PSIPHON
© Freek Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

INSTALLING SWITCH PROXY
© adam hyde 2008
Modifications:
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

INTRODUCTION
© Alice Miller 2006, 2008
Modifications:
adam hyde 2008, 2009
Ariel Viera 2009
Austin Martin 2009
Edward Cherlin 2008
Janet Swisher 2008
Seth Schoen 2008
Tom Boyle 2008

RISKS OF OPERATING A PROXY
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Tom Boyle 2008

SSH TUNNELLING
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008, 2009
Sam Tennyson 2008

TWikiGuest 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

SETTING UP A TOR RELAY
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

SIMPLE TRICKS
© Ronald Deibert 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

TOR: THE ONION ROUTER
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Ben Weissmann 2009
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING TOR WITH BRIDGES
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING JON DO
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

OPENVPN
© Tomas Krag 2008
Modifications:
adam hyde 2008

Alice Miller 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008

USING PHProxy
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

USING PSIPHON
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Austin Martin 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

USING PSIPHON2
© Freerk Ohling 2009
Modifications:
adam hyde 2010
Austin Martin 2009
Zorrino Zorrinno 2009

USING PSIPHON2 OPEN NODES
© 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

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