SORTEANDO LA CENSURA DE INTERNET

Published : 21 Apr 2010
ISBN :

TABLE OF CONTENTS

INTRODUCCION

1. INTRODUCCION
2. ACERCA DE ESTE MANUAL

1. INTRODUCCIÓN

El 10 de Diciembre de 1948, la Asamblea General inició una nueva era con el lanzamiento de la Declaración Universal de los Derechos Humanos. El intelectual libanés Charles Habiz 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 cuales 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 sé a qué se comprometió mi gobierno a promover, acatar, y consumar...; Puedo agitar contra mi gobierno, y si este no cumple su compromiso, yo tendré y sentiré el soporte 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 e impartir información e ideas a través de los medios de comunicación e independientemente de las fronteras.*

Cuando aquellas palabras fueron escritas sesenta años atrás, nadie imaginó cómo el fenómeno global de Internet expandiría la habilidad de "buscar, recibir e impartir información", no solo atravesando las fronteras y los límites sino a velocidades asombrosas y en formas 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 QUE LO NUNCA IMAGINADO

El increible crecimiento que lo que está en internet ha tenido en los ultimos años tiene el efecto de hacer que una inimaginable vasta porcion del conocimiento humano se haga presente en lugares inesperados: el hospital en una aldea remota, el cuarto de tu hija de 12 años, la sala de conferencia donde muestras a tus colegas un nuevo diseño de producto que te pondrá a la cabecera de la competencia, la casa de tu abuela.

En todos esos lugares, la posibilidad de conectarse con el mundo abre muchas oportunidades fabulosas que mejoran la vida de las personas. Cuando contraes una enfermedad rara en vacaciones, el hospital de la aldea remota puede salvar tu vida enviando los resultados de tus exámenes médicos a un médico especialista en la capital, o incluso a otro país; tu hija de 12 años

puede hacer su proyecto de investigación o hacer amigos en otros países; tú puedes presentar el nuevo diseño del producto simultáneamente a los mejores directores en sus oficinas alrededor del mundo, los que pueden ayudarte a mejorarlo; tu abuela puede enviarte su receta especial de torta de manzana por correo electrónico en tiempo para hornearlo para el postre.

Pero Internet no solo contiene información relevante y educacional, amistad y tortas de manzanas. Como el mundo en sí mismo, es vasto, complejo y muchas veces aterrador. Está disponible a personas maliciosas, ambiciosas, inescrupulosas, deshonestas o grosero así como está disponible para ti, tu hija de 12 años y tu abuela.

NO TODOS QUIEREN DEJARNOS ENTRAR

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 SON:

- 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 lo puede ser una escuela -- 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 contemplan 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 Cybercafés o Proveedores de Servicios de Internet, y gobiernos a diferentes niveles.

El colmo del control de Internet es cuando un gobierno nacional intenta restringir a toda la población la capacidad de usar Internet para acceder 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 invasivas 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 discursos de odio, el terrorismo y otras actividades criminales, o la infracción de las leyes de derecho de autor.

FILTRAR CONLLEVA A MONITOREAR

Cualquiera de estos grupos oficiales o privados puede usar varias técnicas para monitorear las actividades en Internet de las personas que le conciernen para asegurarse 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 hasta las agencias de cumplimiento de la ley demandando información desde los Proveedores de Internet o incluso apoderándose de tu computadora en tu casa buscando evidencia de que has estado ocupado en actividades "indeseables".

¿CUÁNDO SE PRODUCE LA CENSURA?

En dependencia de quien 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 o métodos puede ser visto como legítimo y necesario o 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 la habilidad gubernamental o de otros cuerpos para presionar a quellos 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 pueden 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 algunos 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.

Filtros "familiares" creados para filtrar contenido sexual pueden accidentalmente bloquear el acceso a información médica útil. 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 SORTEAR EL FILTRADO?

Como muchos individuos, corporaciones y gobiernos ven Internet como 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 en él 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 volcada a crear herramientas y técnicas para sobrepasar la censura de Internet por parte de grupos comerciales, no lucrativos y voluntarios. Algunas técnicas no requieren programas especiales, solo un conocimiento sobre donde buscar la información. Muchos programadores han desarrollado una variedad de herramientas dirigidas a diferentes

tipos de filtros y bloqueos. Estas herramientas frecuentemente nombradas "herramientas de evasión" ayudan a los usuarios de Internet a acceder información que de otra forma no podrían ver.

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

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

2. ACERCA DE ESTE MANUAL

El manual 'Sorteando la Censura de Internet' provee una introducción al tópico y explica algunos de los programas y métodos más usados frecuentemente para evadir la censura. Hay alguna información para evitar la supervisión y otros medios de detección mientras se sortea 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 está más allá de lo que abarca este libro.

Este manual fue escrito en colaboración con la coalición Sesawe.

¿QUÉ ES SESAWE?

Sesawe es un consorcio internacional que trabaja para apoyar el acceso libre a Internet. Aquí se incluyen tanto desarrolladores como organizaciones e individuos que comparten el ideal de un Internet abierto. Ellos incluyen además centros de investigación académicos, grupos de expertos, organizaciones sin fines de lucro que trabajan en grupos de defensa y publicación, así como docenas de individuos que comparten los mismos objetivos. Sesawe no es una organización, es un lugar de reunión para compartir información y recursos relacionados. Las organizaciones asociadas son financiadas y manipuladas independientemente, y responsables por sus actividades.

Visite el sitio web en https://www.sesawe.net

AUTORES

Este manual tiene contenido que fue escrito en un Book Sprint. The Book Sprint se organizó en las bellas colinas de Alturas del Estado de Nueva York en los Estados Unidos. Ocho personas trabajaron juntas durante un periodo intensivo de cinco dias para producir este libro. Este es un documento actual y por supuesto está disponible gratis en internet, desde donde todos podemos mejorarlo.

Además del material escrito en el Book Sprint, se ha contribuido con material de publicaciones anteriores. Estos incluyen contribuciones de:

- Ronald Deibert
- Ethan Zuckerman
- Nart Villeneuve

- Steven Murdoch
- Ross Anderson
- Freerk Ohling
- Frontline Defenders

Estos autores acordaron dejarnos usar su material en el entorno de la licencia GPL.

Este manual fue escrito desde FLOSS Manuals. Para mejorar este manual por favor siga estos pasos.

1. Registro

Resgístrese en Manuales Floss:

http://en.flossmanuals.net/register

2. ¡Contribuye!

Seleccione el manual (http://en.flossmanuals.net/bin/view/CircumventionTools) y el capítulo deseado.

Si necesita hacer preguntas acerca de cómo constribuir únase a la sala de chat listada debajo y pregunte por nosotros. Esperamos por tu contribución.

Para más información sobre el uso de los manuales puede leer nuestro manual:

http://en.flossmanuals.net/FLOSSManuals

3. Chat

Resulta una buena idea contactar con nosotros y le ayudaremos a coordinar las contribuciones. Para ello está la sala de chat que utiliza IRC (Internet Relay Chat). Si sabe cómo usar IRC puede conectarse al siguiente:

server:irc.freenode.net channel: #booksprint

Si no sabe usar IRC visite el chat basado en web desde su 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. Listas de Envío

Para discutir cualquier cosa sobre el Manual Floss únase a nuestra lista:

http://lists.flossmanuals.net/listinfo.cgi/discuss-flossmanuals.net

Author : *AboutThisManual*

Modifications:

Ariel Viera 2009
Austin Martin 2009
Edward Cherlin 2008
Janet Swisher 2008
Tom Boyle 2008
Zorrino Zorrinno 2009

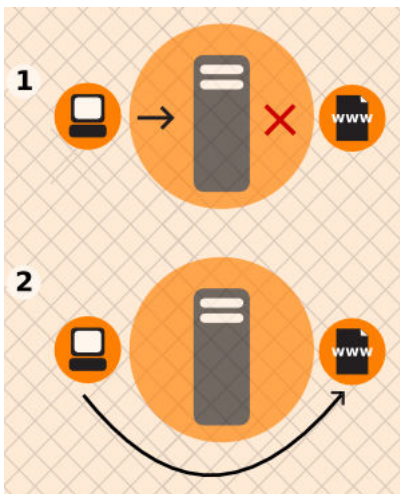
Produced in FLOSS Manuals

BASES

3. SORTEANDO EL FILTRADO
4. ESTOY SIENDO BLOQUEADO?
5. DETECCION Y ANONIMATO
6. COMO FUNCIONA INTERNET?
7. QUIEN CONTROLA LA RED?
8. TECNICAS DE FILTRADO

3. SORTEANDO EL FILTRADO DE INTERNET.

Existen algunos métodos para evadir filtros de Internet, incluyendo herramientas de software y rutas protegidas. A ese conjunto, se le llama métodos de evasión y van desde simples rodeos hasta programas complejos de computación. Por ejemplo, a veces es posible acceder a un sitio web prohibido abriendo una copia que esté en caché en un motor de búsqueda, en lugar de accederla directamente.



PROVEEDORES DE EVASIÓN

Los proveedores de evasión son individuos u organizaciones que brindan métodos para evitar los filtros en Internet. Ellos pueden ser organizaciones comerciales que ofrecen servicios de evasión por un pago o individuos u organizaciones que ofrecen servicios de evasión gratis. Los proveedores de evasión frecuentemente instalan programas en una computadora que se encuentra en una locación no bloqueada y realizan conexiones a esta computadora desde aquellas que acceden a Internet desde una locación bloqueda.

USUARIOS DE EVASIÓN

Los usuarios de evasión son individuos u organizaciones que sortean los filtros de Internet usando tecnologías de evasión y usualmente incluyen a personas que desean acceder o enviar información desde locaciones restringidas. Por ejemplo, muchos usuarios de Internet quieren proteger sus identidades o actividades mas allá de un deseo personal de privacidad. Puede ser que ellos deseen evitar repercusiones de las autoridades que restringen el acceso a Internet -- ya sea un padre en desacuerdo, un empleador, un titular de derechos de autor, un agente de la ley o un censor gubernamental.

Autores : *WhatIsCircumvention*
© Ronald Deibert 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Sam Tennyson 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008

Produced in FLOSS Manuals

4. ¿ESTOY SIENDO BLOQUEADO O FILTRADO?

En muchos países, no es secreto que existe la censura del gobierno en Internet, como se documenta en el libro: *Access Denied: The Practice and Policy of Global Internet Filtering*, editado por Ronald Delbert, John Palfrey, Rafal Rohozinski, y Jonathan Zittrain (http://opennet.net/accessdenied). Cuando un sitio popular es ampliamente bloqueado, ese hecho se convierte en algo conocido en el país.

Pero, en general, determinar si alguien impide acceder a un sitio determinado o enviar información a otros puede ser difícil. Cuando tratas de acceder a un sitio bloqueado, puedes ver un mensaje de error convencional o no ver nada... el comportamiento puede hacer creer que el sitio es inaccesible por razones técnicas.

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 del 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 contenido relacionado está inaccesible por un largo período de tiempo, excepto quizás cuando ellos toman medidas en contra como moverse a un nuevo dominio. Otro es que los motores de búsqueda retornan resultados inútiles o nada acerca de ciertos tópicos. Estos pueden estar relacionados con pornografía, apuestas, drogas (incluyendo alcohol) u otra actividad ilegal o movimientos políticos o religiosos que se estiman peligrosos (por ejemplo, sitios neo-nazi bloqueados en Alemania).

Filtrar o bloquear se hace también por una variedad de razones que tienen un poco que ver con la política. Los padres pueden filtrar la información que llega a sus hijos. Muchas organizaciones, desde escuelas, compañías comerciales, ejército de EU, 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.

Autores : *HowDoIKnow*

Modifications:

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

Produced in FLOSS Manuals

5. DETECCIÓN Y ANONIMATO

Las herramientas para vencer el bloqueo y monitoreo de Internet son diseñadas para tratar con diferentes obstáculos y amenazas. Estas herramientas pueden mejorar el acceso a la información y la comunicación entre personas, así como mitigar los riesgos asociados con el acceso. Las diferentes herramientas pueden facilitarnos:

- **Evadir la censura**: Leyendo o creando documentos u otras formas de contenido, enviando y recibiendo información, o comunicando con personas en particular, sitios o servicios mientras evadimos los intentos de impedirnoslo. 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 ver o escuchar el contenido de lo que estamos comunicando. (No obstante, ellos pueden ser capaces de 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 encripción, tales como https o SSH, hacen que la información sea indecifrable para todo el mundo excepto el remitente y el receptor de la misma.
- **Mantener el anonimato**: La habilidad de comunicar de forma que nadie pueda vincularnos a la información o personas con las que estamos conectado -- ni siquiera el operador de nuestra conexión de Internet ni los sitios de las personas con las que nos comunicamos. Por ejemplo, "relays" de correo electronico anónimos y algunos servicios de proxy, tales como Tor (donde se toman ciertas precauciones de anonimato) proveen este servicio.
- **Ocultar lo que hacemos**: Disfrazando las comunicaciones que enviamos de forma que alguien que nos pueda estar espiando no pueda decirnos que estamos tratando de evitar la censura. Por ejemplo, la esteganografía, que consiste en ocultar un mensaje de texto en una imagen, puede ocultar que estamos usando una herramienta de evasión.

Algunas herramientas protegen la comunicación en solo una de estas formas. Por ejemplo, muchos proxies pueden evadir la censura pero no previenen la escucha secreta -- ellos nos permiten ver un sitio bloqueado pero no evitan que alguien monitoree lo que estamos leyendo. Es importante comprendamos que quizás sea necesaria una combinación de herramientas para lograr nuestros objetivos.

Cada tipo de protección es relevante para cada persona en cada situación. Cuando seleccionamos herramientas que evitan la censura de Internet, debemos tener en cuenta qué tipo

de protección necesitamos y qué grupo de herramientas nos pueden facilitar protección. Por ejemplo. ¿Qué sucederá si alguien detecta que intentamos evadir un sistema de censura? ¿Es realmente importante ocultar lo que leemos y escribimos, o solo 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 comunmente 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 POR LOS OPERADORES O AGENCIAS DE GOBIERNO, YA QUE GENERAN TRÁFICO CON PATRONES DISTINTIVOS. ESTO ES SEGURO PARA LOS MÉTODOS DE EVASIÓN QUE NO USAN CODIFICACIÓN, PERO PUEDE SUCEDER TAMBIÉN CON LOS QUE USAN CODIFICACIÓN. RESULTA DIFÍCIL MANTENER EN SECRETO EL HECHO DE QUE SE ESTÁ USANDO UNA HERRAMIENTA DE EVASIÓN DE FILTRADO, 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.

El Manual FLOSS no brinda un consejo específico sobre el análisis de amenazas o la selección de la herramienta para determinar las amenazas. Los riesgos son diferentes en cada situación, y cambian frecuentemente. Podemos confiar que todos esos intentos de restringir las comunicaciones contribuirán al mejoramiento de los métodos de evasión.

Si estás haciendo algo que pueda ponerte en riesgo en el lugar donde estás, deberás hacer tus propias valoraciones acerca de la seguridad y (si es posible) consultar expertos:

- Si seleccionamos un método que requiere que confiemos en un extraño, debemos hacer lo posible para garantizar la confiabilidad de esa persona.
- Recordemos que las promesas de anonimato y seguridad de muchos sistemas pueden ser poco precisas. Debemos buscar siempre una confirmación independiente.
- Conseguir el anonimato y la seguridad puede requerir de disciplina y cumplir ciertas prácticas y procedimientos de seguridad. Si ignoras los procedimientos de seguridad se puede reducir dramáticamente la protección de seguridad que recibes.
- Seamos consciente de que las personas (o gobiernos) pueden ofrecer señuelos -- falsos sitios Web que pretenden ofrecer comunicación segura pero en realidad capturan la comunicación de usuarios involuntarios.

- Pongámos atención a las amenazas no técnicas. ¿Qué sucede si alguien roba nuestra computadora o teléfono móvil o los de un amigo? ¿Si en un CyberCafé los empleados miran por sobre el hombro? ¿Qué sucede si alguien se sienta en la computadora de un café donde una amiga olvidó cerrar la sesión y envía un mensaje pretendiendo ser ella?
- Si hay leyes o regulaciones que restringen o prohíben el material que estás accediendo o las actividades que estás acometiendo, debes ser consciente de las consecuencias.

Para saber más sobre seguridad y privacidad digital, lee:
http://www.frontlinedefenders.org/manual/en/esecman/intro.html y
http://security.ngoinabox.org/html/en/index.html

Autores : *BeingAnonymous*

Modifications:
adam hyde 2008
Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Produced in FLOSS Manuals

6. CÓMO FUNCIONA INTERNET

INTERNET ES UNA RED A NIVEL MUNDIAL DE REDES DE COMPUTADORAS. AUNQUE MUCHAS PERSONAS USEN EL TÉRMINO "INTERNET" Y "LA WEB" DE FORMA INTERMITENTE, INTERNET ES LA CONEXIÓN FÍSICA DE REDES DE COMPUTADORAS EN CONJUNTO CON CIERTOS MÉTODOS DE COMUNICACIÓN. LA WEB ES UNA DE LAS MUCHAS MANERAS DE COMUNICARSE USANDO INTERNET. TAMBIÉN SE PUEDE USAR PARA **correo electrónico, compartir ficheros, grupos de discusión**, y **chat**.

CONECTÁNDOSE A INTERNET

La forma más fácil de usar la Web es a menudo buscar un Cyber Café local o telecentro con acceso Web. Si necesitamos conectar nuestra computadora a Internet, típicamente abrimos una cuenta con un **proveedor de servicio de Internet** (ISP). Quizás necesitemos un equipamiento extra, como un modem o un **router**, para posibilitar la conexión con el proveedor de Internet.

El ISP a su vez puede adquirir su acceso a Internet de un proveedor nacional (a menos que sea una dependencia de un proveedor nacional). Similarmente los proveedores nacionales pueden recibir su conexión de una compañía multinacional que mantienen y operan sus servicios y conexiones llamados **backbone** (columna vertebral) de Internet. El *backbone* está hecho de instalaciones de servidores mejoradas en puntos críticos, y las conexiones globales entre ellos son de vía fibra óptica y satelital. Estas conexiones posibilitan la comunicación entre los usuarios de Internet en diferentes países y continentes. Los proveedores nacionales e internacionales se conectan al *backbone* a través de **routers** especiales conocidos como **gateways** (puerta de enlace), que son conexiones que permiten comunicar una red con otra. Los *gateways* como otros *routers*, pueden ser puntos por los cuales se monitorea y controla el tráfico.

Cuando nos conectamos a Internet, se le asigna una dirección IP, que puede ser escrita con cuatro números en el rango de 0-255, separados por puntos. Como una dirección postal, identifica de forma inequívoca una computadora en Internet. Dependiendo del Proveedor de Servicios de Internet, se pueden asignar varias direcciones IP en diferentes momentos que nos conectamos a ellos. Todos los sitios Web y Servidores Web también tienen una dirección IP. Por ejemplo, la dirección IP de www.frontlinedefenders.org es 217.173.101.253.

VISITANDO UN SITIO WEB

Cuando queremos visitar un sitio Web, normalmente escribimos el "nombre" del sitio Web en el navegador y no la dirección IP. Por ejemplo, para acceder al sitio Web Frontline se escribirá http://www.frontlinedefenders.org en lugar de 217.173.101.253. El nombre del sitio Web es también llamado **dominio** o **nombre de dominio**.

Después que escribe el nombre del dominio en el navegador, la computadora envía un mensaje con este nombre al Sistema de Nombres de Dominio (DNS). Este sistema consiste en computadoras dedicadas en Internet a traducir nombres en direcciones IP. Esto significa que solo necesitamos recordar el nombre del sitio Web en lugar de recordar una cadena compleja de números. Después que el servidor DNS traduce el nombre del dominio en una dirección IP, comparte esa información con nuestra computadora.

Nuestra computadora puede tratar de conectarse a un sitio Web usando la dirección IP. Para ello debe encontrarse el camino desde tu computadora hasta el destino. Este camino puede viajar por países, océanos y el espacio; puede estar a miles de millas de lejanía y pasar a través de numerosas computadoras. ¿Cómo sabe por qué vía ir, cuando hay miles de millones de sitios Web diferentes? La tarea de direccionar nuestro mensaje al sitio Web (y retornarlo) la ejecutan los enrutadores, y el proceso es conocido como **enrutamiento**.

Para nuestros propósitos, vale la pena aclarar que a los enrutadores se les puede administrar algunas instrucciones simples para configurar su comportamiento y puede usarse como herramienta de censura.

Ejemplo de lo que sucede cuando encontramos una página Web:

1. Escribimos http://globalvoicesonline.org/. La computadora envía el nombre de dominio a un servidor DNS seleccionado (usando su dirección numérica), el cual responde con la dirección IP del sitio Web Global Voices.
2. El navegador envía entonces una petición a esa dirección IP.
3. La petición va a través de una serie de enrutadores hasta que alcanza el enrutador que encuentra la computadora que se necesita.
4. Esta computadora envía la información de regreso a nosotros, permitiendo al navegador enviar la URL completa y recibir los datos para mostrar la página.

Se le llama hop (salto) a toda conexión entre computadoras o enrutadores por las que atraviesa un mensaje. El número de hops es el número de computadoras y enrutadores que el mensaje contacta por el camino. Debajo hay un ejemplo de camino tomado por una computadora para llegar a: www.globalvoicesonline.org. Esta petición pasa a través de al menos 14 conexiones de computadoras (hops) antes de alcanzar su destino.

```
traceroute to globalvoicesonline.org (72.249.186.50), 64 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  2.425 ms  0.673 ms  0.637 ms
 2  192.168.15.1 (192.168.15.1)  3.824 ms  1.068 ms  1.139 ms
 3  10.92.32.1 (10.92.32.1)  10.712 ms  9.581 ms  98.359 ms
 4  gig-5-3-lbrtnymtn-rtr1.hvc.rr.com (24.164.160.173)  10.720 ms  10.774 ms  11.147 ms
 5  pos-3-1-nycmnya-rtr1.nyc.rr.com (24.164.160.78)  12.533 ms  12.042 ms  11.206 ms
 6  tenge-0-3-0-nwrknjmd-rtr.nyc.rr.com (24.29.97.6)  12.456 ms  13.922 ms  13.821 ms
 7  ae-4-0.cr0.nyc30.tbone.rr.com (66.109.6.78)  15.844 ms  22.984 ms  14.024 ms
 8  ae-1-0.pr0.nyc20.tbone.rr.com (66.109.6.163)  14.605 ms  14.592 ms  43.455 ms
 9  207.88.182.73.ptr.us.xo.net (207.88.182.73)  14.707 ms  14.437 ms  22.936 ms
10  te-4-0-0.rar3.nyc-ny.us.xo.net (207.88.12.26)  24.168 ms  16.683 ms  16.947 ms
11  207.88.14.9.ptr.us.xo.net (207.88.14.9)  45.446 ms  45.360 ms  46.136 ms
12  207.88.14.10.ptr.us.xo.net (207.88.14.10)  70.949 ms  69.782 ms  70.112 ms
13  207.88.185.38.ptr.us.xo.net (207.88.185.38)  70.162 ms  73.824 ms  73.137 ms
14  switch19.rimuhosting.com (65.99.204.18)  70.630 ms  70.344 ms  70.264 ms
15  server1.globalvoicesonline.org (72.249.186.50)  72.347 ms  72.747 ms  74.179 ms
Destination reached!
```

Siendo usuarios de Internet, debemos saber que todos estos procesos complejos están normalmente ocultos y no hace falta entenderlos para acceder a la información. Sin embargo, cuando personas u organizaciones intentan limitar el acceso a la información interfieren con la operación del sistema, la habilidad de usar Internet puede ser restringida.

POR QUÉ ES IMPORTANTE

La censura puede ocurrir en diferentes puntos de la infraestructura de Internet, cubriendo dominios o subdominios completos, protocolos individuales, o contenido específico identificado por el programa de filtrado. El mejor método para evitar la censura dependerá de la técnica de censura usada. Por eso se necesita entender esas diferencias para usar las medidas apropiadas y así poder usar Internet de forma efectiva y segura.

Autores : *HowTheNetWorks*

Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Produced in FLOSS Manuals

7. ¿QUIÉN CONTROLA LA RED?

LA HISTORIA COMPLETA DEL CONTROL DE INTERNET ES COMPLICADA, POLÍTICA Y TODAVÍA ES DISPUTADA ACTIVAMENTE. ESTE TEXTO TIENE LA INTENCIÓN DE PROVEER DE DETALLES SUFICIENTES PARA AYUDAR A ENTENDER COMO CIERTOS ASPECTOS DEL SISTEMA AFECTAN PARTICULARMENTE MÉTODOS DE RESTRICCIÓN DE ACCESOS. EL PUNTO CLAVE ES QUE, EN ALGUNOS PAÍSES, TODAS LAS INFRAESTRUCTURAS DE INTERNET PERTENECEN Y SON OPERADAS POR GOBIERNOS Y GRANDES COMPAÑÍAS DE TELÉFONO REGULADAS. UN GOBIERNO QUE DESEA BLOQUEAR EL ACCESO A LA INFORMACIÓN PUEDE EJERCER CONTROL DIRECTO O INDIRECTO SOBRE PUNTOS DONDE SE PRODUCE LA INFORMACIÓN, O POR DONDE

ENTRA Y SALE DEL PAÍS. LOS GOBIERNOS TIENEN AUTORIDAD LEGAL EXTENSIVA

PARA ESPIAR EN CIUDADES, Y MUCHOS TAMBIÉN VAN MÁS ALLÁ DE LO QUE PERMITE

LA LEY, USANDO MÉTODOS EXTRA LEGALES 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. Este 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 e 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. Ellos pueden, y algunos lo hacen, 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 o bloqueando o eliminando 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.

¿POR QUÉ ESTO ES IMPORTANTE?

Es importante entender la autoridad sobre Internet para entender la fuente de la censura de Internet y las posibles amenazas. Un gobierno nacional puede no solo bloquear el acceso al contenido, sino que puede monitorear a que información pueden acceder las personas en su país, y puede penalizar usuarios por el uso de actividades relacionadas con Internet que el gobierno estima inaceptables. Los gobiernos pueden hacer ambas cosas, definir que bloquear o llevar a cabo el bloqueo, o puede crear legislaciones, regulaciones, o fuerzas extra legales para obligar a los empleados de las compañías independientes a bloquear y supervisar. Por eso, dependiendo de la situación de un usuario, los intentos de evadir la censura pueden tener consecuencias dañinas en el mundo real. Cuando la seguridad del usuario está implicada, entender como Internet es (o no es) controlado es crítico.

Autores : *WhooControlsTheNet*

Modifications:

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tomas Krag 2008

Produced in FLOSS Manuals

8. TÉCNICAS DE FILTRADO

El filtrado de Internet consiste en una serie de técnicas que los censores usan para tratar de impedir que los usuarios accedan a contenidos o servicios particulares. Los operadores de redes pueden filtrar en cualquier punto de una red, usando una amplia variedad de tecnologías, con niveles variables de exactitud y personalización. Típicamente, el filtrado implica el uso de programas para observar qué están haciendo los usuarios e interferir selectivamente con actividades que los operadores consideran violatorias. Un filtro puede ser creado y aplicado por un gobierno nacional o por un proveedor nacional o local.

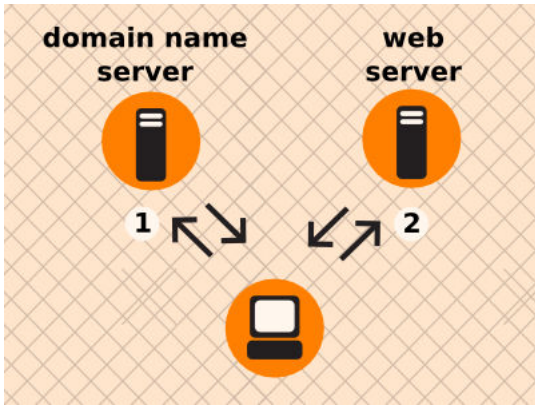
Existen cuatro tipos comunes de filtrado que debe tener en cuenta:

FILTRADO URL

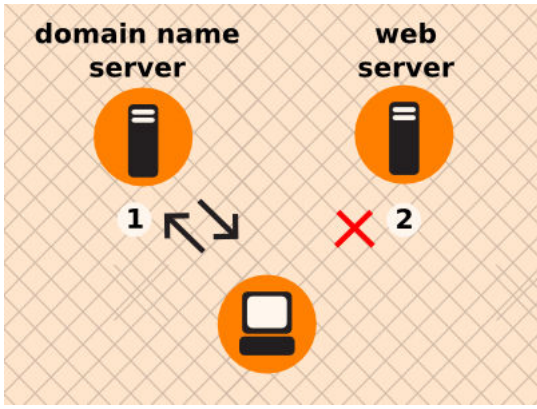
Una de las formas de bloquear el acceso a información en la Web de muchos países y otras entidades es impedir el acceso basado en la URL -- puede ser la URL entera o parte de ella. Los censuradores de Internet casi siempre desean bloquear dominios Web específicos en su totalidad, por el contenido de 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. Por ejemplo, ellos quizás filtran solo el subdominio news.bbc.co.uk, mientras dejan sin bloquear bbc.co.uk y www.bbc.co.uk. Similarmente, ellos pueden querer filtrar tipos de contenido específicos, incluso si ellos permiten el acceso al resto del dominio. Otra de las formas es buscar un nombre de directorio, como "worldservice" para bloquear las noticias en idiomas extranjeros de BBC en bbc.co.uk/worldservice, sin afectar el sitio Web en Inglés. Ellos pueden incluso, bloquear páginas específicas basadas en nombres de páginas, o términos de búsqueda, que sugieren contenido ofensivo o indeseado.

FILTRADO DNS

Cuando las personas usan Internet para comunicarse, generalmente usan nombres de dominio tales como "algunsitioweb.com" en lugar de números de direcciones IP, particularmente para navegar en la Web. Sin embargo, cuando las computadoras se comunican por Internet, necesitan una dirección numérica para navegar. Cuando entras un nombre de dominio en un navegador Web, la primera cosa que hace el navegador es preguntar a un servidor DNS (Domain Name System), por una dirección numérica conocida, para buscar el nombre de dominio y suministrar la correspondiente dirección IP.



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.



Sin la dirección IP, la solicitud de la computadora no puede continuar, y muestra un mensaje de error. Puesto que el navegador no toma la dirección IP del sitio Web, no es capaz de contactar el sitio para pedir la página. El resultado es bloquear todas las páginas bajo un nombre de dominio.

Las alternativas para evadir los filtrados de DNS son:

- Acceder al contenido del sitio deseado desde otro sitio con un nombre de dominio diferente.
- Preguntar por la dirección a un servidor DNS diferente. Esto se puede hacer para un dominio sencillo o permanentemente usando un servidor DNS libre o corriendo tu propio servidor DNS.
- Buscando la dirección numérica publicada en algún lugar.
- Enviar la consulta a través de un sitio diferente que no esté bloqueado. Por ejemplo: un proxy web o el caché de un motor de búsqueda.

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 cómo enviarlo, como 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, ellos pueden configurar los enrutadores que ellos controlan para dejar caer los datos destinados a una dirección IP en una lista negra o retornar un mensaje de error. El filtrado basado solamente en direcciones IP bloquea todos los servicios proporcionados por un servidor particular, 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 son bloquedas también, solo si uno está prohibido.

Para evadir el filtrado por IP, es posible acceder al contenido deseado en otra parte, o enrutar las peticiones a través de sitios no sujetos al bloqueo.

BLOQUEO DE PUERTOS

Los puertos son como puertas enumeradas en un edificio, cada una guía a una habitación o suite. En una computadora, los puertos también están enumerados: los números de los puertos estándares más conocidos van desde 0 a 1024, pero otros van más allá de 65535. Cada puerto enumerado ofrece un servicio específico (por ejemplo. Acceso Web o correo electrónico) en un servidor o en una PC. Cuando una computadora solicita acceso a un tipo especial de servicio en otra computadora, especifica un número de puerto para la petición. La computadora que provee el servicio "escucha" por las peticiones que usan un número de puerto particular.

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. Servicios comunes 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 método más directo para evadir el bloqueo de puertos es usar puertos no estándares para proveer servicios estándares. Los usuarios deben tener algunos conocimientos de sistema para tomar ventajas de esto, para configurar navegadores Web o clientes de correo para usar puertos no estándares. Otros métodos de acceder el contenido incluye acceder el mismo servicio o similar en otros servidores contribuyentes, o accediendo a los servidores a través de locaciones no bloqueadas.

¿POR QUÉ ES IMPORTANTE?

Estas técnicas de censura dependen del trabajo de diferentes partes de la estructura de Internet descrita anteriormente. Debes tener algunos conocimientos de cuál de ellas aplica a tu situación. Si deseas crear un servidor desbloqueado fuera del lugar que está haciendo el bloqueo, necesitarás más información detallada.

PRIMERAS TECNICAS

9. TRUCOS SIMPLES
10. QUE ES UN PROXY WEB?
11. USO DE PHProxy
12. USO DE PSIPHON
13. USO DE PSIPHON2
14. RIESGOS

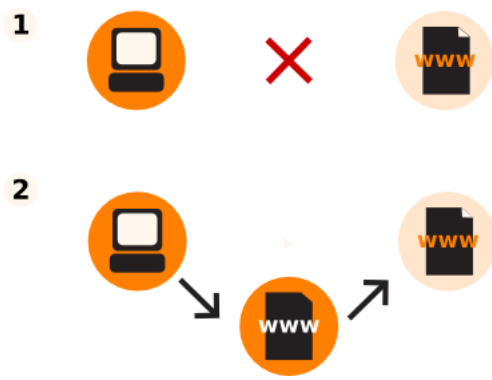
9. TRUCOS SIMPLES

Hay un número de técnicas para pasar el filtrado en Internet. Si tu meta es alcanzar páginas o servicios en Internet que están bloqueados desde tu locación, y no estás preocupado por si otras personas detectan y monitorean tu evasión, estas técnicas pueden ser lo que necesitas:

- Usando sitios de terceros para alcanzar contenido bloqueado.
- Usando nombres de dominios alternativos (o servidores de nombres de dominios) para alcanzar contenido bloqueado.
- Usar correo electrónico para recuperar páginas web bloqueadas a través del correo.

USANDO SITIOS DE TERCEROS

Hay diferentes formas por las que puedes acceder al contenido de una página Web yendo a través de un sitio de un tercero sin ir directamente al sitio web original.



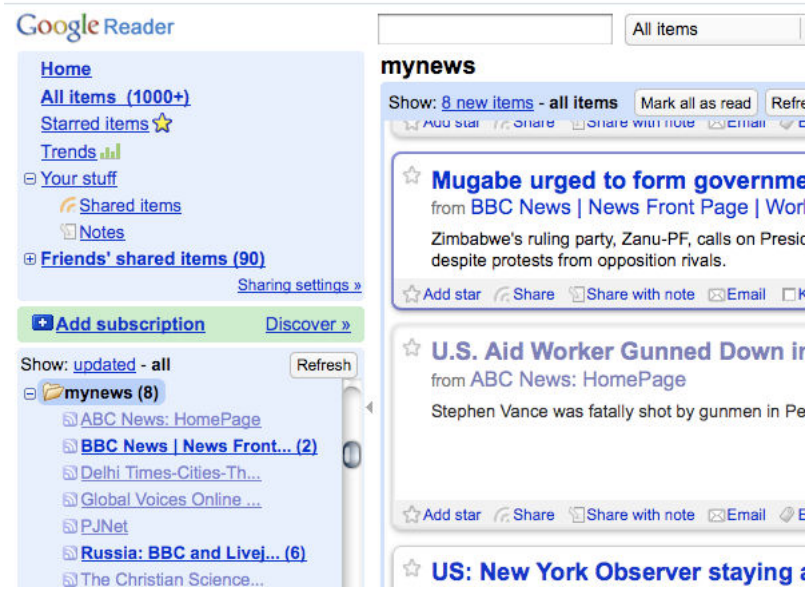
Páginas Caché

Muchos motores de búsqueda mantienen copias de páginas Web que han indexado previamente, llamadas páginas caché. Podemos acceder a un sitio Web siguiendo un pequeño enlace etiquetado "en caché" próximo a cada resultado 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, podremos de ver el contenido bloqueado. Sin embargo, en algunos paises los servicios de caché también están bloqueados.

Agregadores RSS

Los Agregadores RSS son sitios Web que te permiten suscribirte y leer *RSS feeds*, los cuales son flujos de noticias u otra información expuestos por el sitio seleccionado. (RSS: Really Simple Syndication, para más información sobre cómo usarlo, vea http://rssexplained.blogspot.com/.) Un agregador RSS se conecta a sitios Web, descarga los feeds que seleccionó, y los muestra. Como el RSS es el que se conecta al sitio y no nosotros, podemos acceder al sitio bloqueado. Esta técnica solo funciona para sitios que publican RSS feeds en 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 de lenguajes disponibles en Internet, casi siempre proporcionados por motores de búsqueda. Si accedes a través de un servicio de traducción, el servicio de traducción está accediendo y no nosotros. Esto permite leer el contenido bloqueado traducido en diferentes lenguajes.

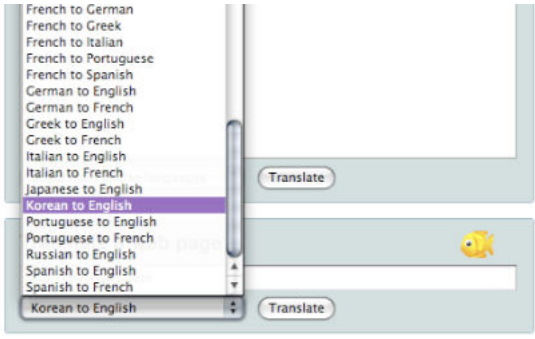
Puedes usar el servicio de traducción para evadir el bloqueo, incluso aunque no se quiera traducir el texto. Esto se hace seleccionando traducción desde un lenguaje que no aparezca en el sitio Web original al lenguaje original. Por ejemplo, para usar el servicio de traducción para ver un sitio Web en inglés, seleccionemos traducción de Chino a Inglés. El servicio de traducción traduce solo la sección China (no hay ninguna), y deja la sección en Inglés (que és 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, seleccionemos el lenguaje en el que deseas 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.



Cuando hayas seleccionado el lenguaje, clic "Traducir" y la página se muestra.

Filtros de ancho de banda bajo

Los filtros de ancho de banda bajo son servicios web diseñados para navegar más fácil en lugares donde la velocidad de la conexión es lenta. Estos eliminan o reducen las imágenes, eliminan los mensajes publicitarios, y otros comprimen el sitio Web para que usen menos datos, y descarguen rápido. Pero, al igual que en los servicios de las traducciones y agregaciones, pueden usarse el para sobrepasar evitar el bloqueo obteniendo el sitio web desde su servidor en lugar de hacerlo desde los servidores originales. Uno de los filtros de ancho de banda bajo más útil está en http://loband.org/.

USANDO SERVIDORES DE NOMBRE ALTERNATIVOS

En pocas palabras, un servidor DNS traduce una dirección Web como google.com en una dirección IP que identifica a un servidor específico con esa página en Internet, como 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.

Puedes evadir este tipo de bloqueo con estas técnicas:

Nombres de Dominios Alternativos

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, trata de ver si el contenido está disponible en otro dominio.

Servidores DNS Alternativos

Una extension de esta técnica es traspasar el Servidor de Nombres de Dominios de tu ISP local usando servidores de terceros para alcanzar dominios que pueden estar bloqueados por los servidores de ISP. Hay un número de servidores DNS gratis disponibles internacionalmente con los que puedes intentar. OpenDNS[7] (https://www.opendns.com) provee este servicio y además tiene las guías de cómo cambiar el servidor DNS que usa tu computadora (https://www.opendns.com/smb/start/computer/). Existe también una lista de servidores DNS disponibles alrededor del mundo en http://www.dnsserverlist.org/.

USANDO SERVICIOS DE CORREO ELECTRÓNICO

El correo electrónico y los servicios de correo vía Web pueden usarse 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 bajo, 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 adjuntado. 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 usas desde un servicio de correo web seguro.

Un servicio como este se puede encontrar en pagegetter.com. Para usarlo, envía un correo, incluyendo una o más URLs en el asunto o el cuerpo del mensaje, a la dirección web@pagegetter.com. Automáticamente recibirás la página solicitada completa con gráficos incluídos.

Las páginas web con **marcos** se enviarán en múltiples correos, porque muchos clientes de correo no pueden mostrar marcos. (Los marcos son formas de mostrar múltiples páginas en una pantalla sencilla.) Pero si tu cliente de correo soporta marcos (por ejemplo, Outlook Express) puedes recibir todos los cuadros en un mensaje sencillo. En este caso, envía el correo electrónico a frames@pagegetter.com.

Para recibir una versión de solo texto de la página solicitada, escribe a text@pagegetter.com. Esto es especialmente útil para Asistentes Personales Digitales (PADs), teléfonos celulares, y sistemas de correo electrónico de solo texto. Puedes también enviar un mensaje a HTML@pagegetter.com para recibir la página HTML completa sin gráficos. Un servicio similar se puede encontrar en web2mail.com. Para usarlo, envía un mensaje de correo a www@web2mail.com con la dirección Web (URL) de la página Web que deseas en la línea asunto. También puedes ejecutar búsquedas Web simples tecleando "search" en la línea asunto. Por ejemplo, puedes buscar por herramientas de evasión de censura escribiendo "search herramientas de evasión de censura" en el asunto de un mensaje de correo y enviarlo a www@web2mail.com.

Puedes encontrar más información y soporte sobre este tema en las listas de envío. Para suscribirte, envía un correo electrónico con "SUBSCRIBE ACCMAIL" en el cuerpo a listserv@listserv.aol.com.

Usando correo Web para compartir documentos

Si quieremos compartir documentos en línea, y controlar quien puede accederlos, podemos mantenerlos en un espacio privado donde estén visibles para aquellos que tengan la contraseña correcta. Una forma simple de compartir documentos entre pequeños grupos de amigos o colegas es usando una cuenta de correo Web con un proveedor en línea, como Gmail (https://mail.google.com/), y compartir el usuario y la contraseña con aquellos que necesitan acceder a estos documentos. Puesto que la mayoría de los proveedores de correo son gratis, es fácil cambiar a una nueva cuenta por intervalos, haciendo más difícil para cualquiera fuera del grupo estar al tanto de lo que están haciendo. Una lista de proveedores de correo gratis está localizada en www.emailaddresses.com/email_web.htm.

VENTAJAS Y RIESGOS

Estas técnicas simples son rápidas y fáciles de usar, puedes 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 u ocultan nuestra comunicación, son vulnerables al bloqueo y monitoreo basado en palabras claves.

Autores : *SimpleTricks*
© Ronald Deibert 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008

10. ¿QUÉ ES UN PROXY WEB?

Un proxy Web permite alcanzar un sitio Web incluso cuando el acceso a ese sitio este bloqueado en nuestra locación. Típicamente, un proxy Web presenta un formulario donde podemos entrar la URL del sitio que queremos ver. El proxy entonces nos muestra la página, pero no ocurre una conexión directa entre nosotros y el sitio Web solicitado.

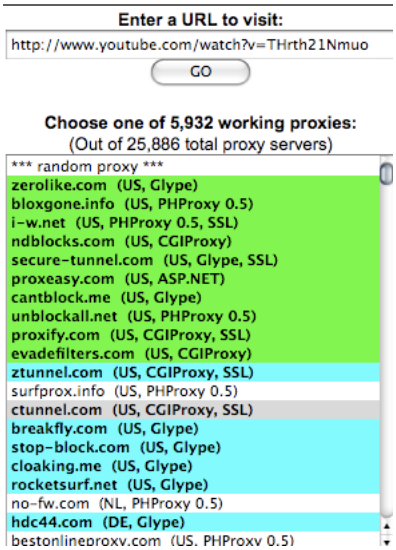
Cuando se usa un proxy Web, no tienes que instalar un software o cambiar las características y propiedades de tu computadora. En cambio, irás a la URL del proxy Web, entrarás la URL que quieres visitar, y clic en el botón "submit" (o el equivalente). Un proxy Web puede ser usado desde cualquier computadora, incluyendo las de los Cyber cafés.

Ejemplos de proxys Web gratis incluyen **CGIProxy**, **PHProxy** y **Zelune**. Todos ellos brindan la misma funcionalidad básica, pero algunos son mejores brindando ciertas funciones como el acceso a videos. Estos y otros programas proxy web, como **Glype**, **Psiphon**, **Picidae** y **bblocked**, son programas que pueden ejecutarse en diferentes computadoras.

Puedes encontrar una lista de proxies Web en sitios como: http://www.proxy.org/, uniéndote a la lista de discusión en http://www.peacefire.org/circumventor/, o solo haciendo una búsqueda con las palabras claves "free web proxys" desde cualquier motor de búsqueda.

(Si estás en un país con acceso a Internet ilimitado y deseas ayudar a otros que se encuentran bajo censura, puedes instalar un script de proxy Web en tu sitio Web o en tu PC.)

Proxy.org lista, literalmente, miles de proxys Web gratis:



VENTAJAS Y RIESGOS

Los proxies Web son fáciles de usar -- no necesitamos instalar ningún software, podemos usar un proxy Web público incluso si no tenemos un contacto confiable en un sitio no filtrado. Los proxies web privados pueden personalizarse para encontrar necesidades específicas de los usuarios y son menos propensos a ser bloqueados o descubiertos por las autoridades que filtran la información.

Pero los proxies Web tienen desventajas potenciales. Muchas veces permiten solo tráfico Web (HTTP), así que no pueden usarse para otros servicios como correo electrónico o mensajería instantánea. Muchos no pueden usar multimedia (como YouTube[7]) o usarlos con encripción (SSL). Los servicios Web que requieren autenticación (tales como el correo electrónico) pueden no funcionar completamente a través de los proxies Web o pueden hacerte vulnerable pues las contraseñas u otra información pueden ser monitoreadas o robadas.

Los proxies Web pueden ser bloqueados o interceptados. Las direcciones de los proxies Web públicos generalmente son bien conocidas y por tanto se puede bloquear el acceso a ellos. Los proxies Web privados requieren que los usuarios tengan un contacto en un lugar no filtrado. Las comunicaciones sin encriptar con los proxies Web pueden ser interceptadas por los operadores de red, a través del filtrado de palabras claves se puede trabajar contra los proxies Web sin encripción.

Los usuarios de los proxies Web deben tener en cuenta que los operadores de sus proxies Web pueden leer sus comunicaciones y registrar la dirección IP desde la cual se utilizó el proxy Web. Si esa información te puede poner en riesgo, debes considerar cuidadosamente la selección de un proxy.

Autores : *WhatIsAWebProxy*
© Nart Villeneuve 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Produced in FLOSS Manuals

11. USANDO PHPROXY

PHProxy es un proxy Web gratis que provee acceso a sitios Web que pudieran estar bloqueados.

PHProxy está hecho en lenguaje PHP, originalmente por alguien que se hacía llamar Abdullah Arif, quien dejó de trabajar en el proyecto en el año 2007. No obstante, se mantiene funcional y útil y muchas personas lo usan para levantar su propio proxy Web público.

¿DÓNDE PODEMOS ACCEDER A PHPROXY?

Puedes encontrar un servicio PHProxy público buscando "PHProxy" en cualquier motor de búsqueda, pero alguien que conozcas que tenga un espacio en un servidor Web con acceso a Internet sin restricciones puede poner a funcionar un servicio PHProxy personalizado para ti.

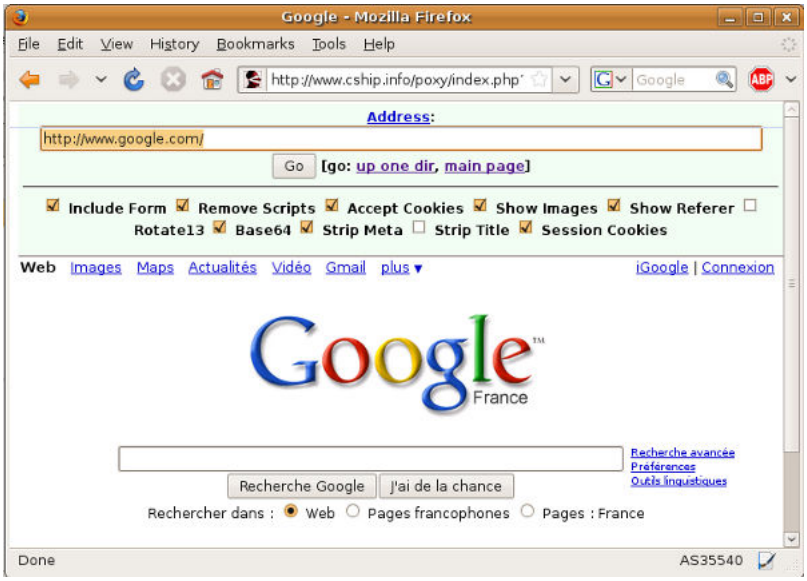
(Con solo disponer de espacio en un servidor Web con acceso a Internet sin restricciones, podemos poner a funcionar un servicio PHProxy nosotros mismos para que lo usen personas con acceso restringido. Para hacer esto, puedes descargar un script PHProxy en http://sourceforge.net/projects/poxy/.)

¿CÓMO FUNCIONA ESTO?

Aquí hay un ejemplo que ilustra cómo funciona un PHProxy:

1. Entremos la dirección de un servicio PHProxy, por ejemplo http://www.cship.info/poxy/, en nuestro navegador Web.
2. En la caja "Web Address" en la página PHProxy, entremos la dirección del sitio Web que deseamos visitar, por ejemplo, http://www.google.com. Dejemos el resto de las opciones por defecto.
3. Demos clic en "Go" o presionemos Enter.

El sitio Web que quieremos visitar se muestra en la ventana del navegador.



Para continuar navegando, tenemos las siguientes opciones:

- Clic en cualquier enlace. El proxy Web es automáticamente usado para recuperar la página enlazada.
- Entre una nueva URL en la caja "Address" al inicio de la página.

OPCIONES AVANZADAS

Usualmente, pueden mantenerse las opciones por defecto para navegar. Sin embargo podemos seleccionar algunas opciones avanzadas:

- **Incluir mini forma-URL en cada página:** Esta opción permite tener una forma en el sitio Web proxificado de manera que podamos entrar nuevas URLs sin regresar a la página de inicio del PHProxy. Si disponemos de una pantalla pequeña quizás sea mejor desmarcar esta opción para que tener más espacio para la página Web destino.
- **Eliminar scripts del lado del cliente (por ejemplo, JavaScript[?]):** JavaScript[?] es una tecnología requerida por algunos sitios Web modernos (como los servicios de correo Web). Algunas veces puede no desearse JavaScript[?] porque también se usa para enviar mensajes publicitarios o incluso para descubrir nuestra identidad.
- **Permitir el almacenamiento de cookies:** Las cookies son pequeños ficheros de texto con un ID de usuario distintivo que son almacenadas en el navegador automáticamente. Se requieren en algunos sitios que necesitan autenticación pero pueden usarse para rastrear nuestra identidad. Con esta opción activada cada cookie es almacenada por un tiempo largo. Si deseamos permitir las cookies para esta sesión solamente, desmarquemos esta opción y seleccionemos "Store cookies for this session only" (vea más abajo).
- **Mostrar imágenes en las páginas navegadas:** Si tenemos una conexión de Internet lenta, podemos desmarcar esta opción para que el sitio Web cargue más rápido.
- **Muestra el sitio Web real referente:** Por defecto el navegador envía a cada sitio web la URL de la que venimos. Por ejemplo, si buscamos en Google "Internet censorship wiki" la página de resultados será http://www.google.com/search?q=internet+censorship+wiki. Cuando hacemos clic en el enlace http://en.cship.org/wiki/ desde los resultados el sitio web tomará el enlace de Google para almacenarlo en los logfiles y analizado automáticamente. Para lograr un mejor anonimato podemos deseleccionar esta opción. Algunos sitios Web pueden no funcionar si esta opción está deseleccionada.
- **Usar codificación ROT13/base64:** Esta opción cambiará la forma en que se transmite la URL del sitio que deseamos visitar. Por ejemplo, la URL http://en.cship.org/wiki/ será uggc://ra.pfuvc.bet/jvxv/ en ROT13 y aHR0cDovL2VuLmNzaGlwLm9yZy93aWtpL01haW5fUGFnZQ en base 64. Ambas técnicas de codificación son bien conocidas, por lo que no pueden considerarse para nada como técnicas de cifrado. Aún así, pueden usarse para confundir filtrados de palabras claves simples. Si usa encripción SSL (la URL de PHProxy comienza con https) esta codificación será redundante, ya que la conexión está encriptada correctamente y oculta de los filtros.
- **Eliminar etiquetas de meta información de las páginas:** 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. Debemos seleccionar esta opción para evitar presentar esta información a los filtros de palabras clave.
- **Eliminar título de página:** Con esta opción activada, PHProxy elimina el título de la página del sitio Web, el cual normalmente se ve en la barra de titulo de tu navegador. Esto puede ser útil, por ejemplo, para ocultar el nombre del sitio Web que estás visitando cuando

minimicemos el navegador.

- **Almacenar cookies para esta sesión solamente:** Similar a la opción "Allow cookies to be stored". Con esta opción activa, los cookies solo se almacenarán hasta que cierremos la sesión PHProxy.

Autores : *UsingPHProxy*
© Freerk Ohling 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

Produced in FLOSS Manuals

12. USANDO PSIPHON

Psiphon es un **proxy Web** diseñado para usarse entre personas que tienen una relación confiable, privada y preestablecida (como lo pueden ser amigos y familiares). Una persona en un sitio sin restricciones provee de un **servicio proxy** psiphon a alguien que conoce en un sitio con acceso limitado. Este sin la intención de ser un servicio de proxy público, abierto.

Si deseamos usar psiphon para traspasar las restricciones de Internet, debemos encontrar a alguien en un lugar sin restricciones de acceso a Internet que desee proveernos de un nodo psiphon. Hay un fórum oficial de psiphon en http://psiphon.civisec.org/forum/ donde los usuarios psiphon comparten información acerca de nodos psiphon disponibles. Podríamos encontrar una persona confiable a través de este fórum, debemos tener en cuenta que esa persona que tiene el nodo psiphon que usaremos tendrá acceso a toda nuestra actividad en Internet, incluyendo contraseñas y datos privados.

(Si tienes un servidor o un espacio Web en una locación sin restricciones de Internet, puedes instalar psiphon para que otras personas lo usen. Visite http://psiphon.ca/download.php para más información.)

CONECTÁNDONOS A UN PROXY PSIPHON

Cuando has establecido contacto con el dueño de un nodo psiphon, esa persona nos enviará una información que debe ser algo así:

URL: https://86.103.195.150:443/cship/

Username: cship

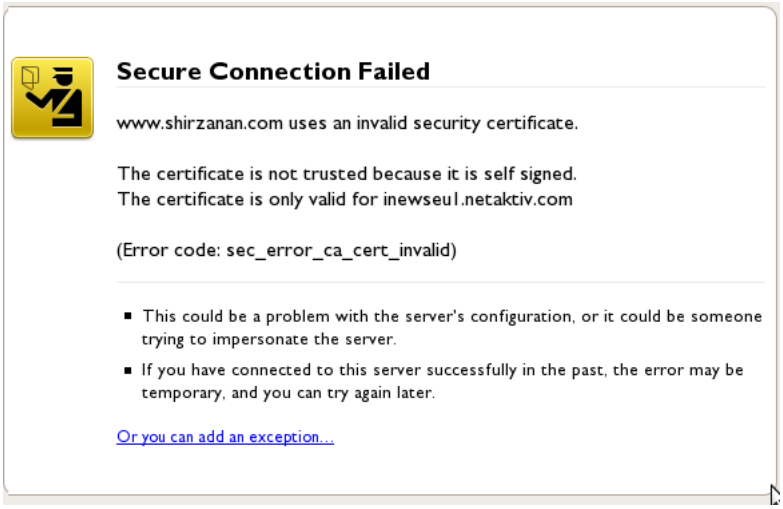
Password: cship

Para usar el proxy psiphon, entramos la URL que recibimos en el navegador Web y nos registramos con la información de cuenta apropiada.

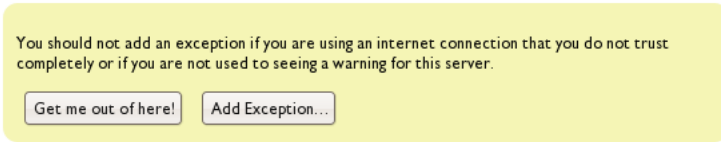
ADICIONANDO UNA EXCEPCIÓN SSL

La primera vez que nos conectamos a una URL psiphon, el navegador Web debe mostrar un mensaje de error acerca de un certificado SSL no válido, como se muestra debajo. Esto sucede porque se está usando una conexión SSL (indicada por "https:" en la URL), y normalmente las conexiones SSL son seguras si para ellas se usan certificados SSL oficiales. Los certificados SSL oficiales cuestan dinero, por eso no debemos suponer que todos los nodos psiphon tienen uno instalado (hasta ahora, la mayoría de los nodos psiphon no los tiene). Ignorar este mensaje error *puede significar un riesgo a tu privacidad* ya que un operador de redes listo pudiera descifrar nuestro tráfico haciéndose pasar por el servidor psiphon. Si se está más preocupado por el acceso y no por la privacidad, ignorar este error puede ser apropiado.

Si seleccionamos proceder, podemos adicionar una regla de excepción en tu navegador para no tener que ver la advertencia cada vez que nos conectemos. En este ejemplo, la excepción es adicionada al navegador de Firefox:



- Hacer clic en el enlace "Or you can add an exception" en el pie de página. El navegador muestra más información y botones.



- Clic en "Add Exception". El navegador abre una caja de diálogo, con la URL que entraste originalmente en la barra Location:
- Clic "Get Certificate". Más información aparece en la caja de diálogo.

- Clic "Confirm Security Exception."

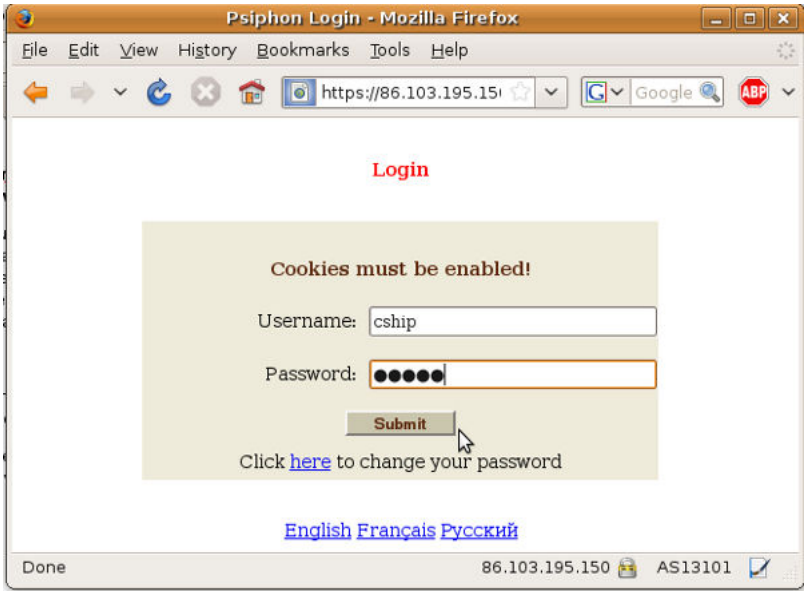
Si estás preocupado por la privacidad

Adicionar una excepción de seguridad o ignorar el aviso de seguridad descrito anteriormente, representa un riesgo a la privacidad ya que es posible para un espía listo que controle componentes claves de nuestra red engañarnos fingiendo ser un servidor psiphon. La severidad de este riesgo depende en la probabilidad de que alguien intercepte nuestra comunicación. En algunos entornos, ignorar los avisos de seguridad puede significar un riesgo substancial. (Si la primera conexión no fue interferida, las conexiones subsecuentes serán seguras porque Firefox recuerda la identidad del sitio con el que te comunicaste.) Si estás más preocupado por la evasión y no por la privacidad, esta inquietud puede ser irrelevante para ti.

Si estás preocupado específicamente con la privacidad, hay formas más seguras de verificar la identidad de un sitio antes de adicionar una excepción de seguridad. Una forma que puede funcionar con Firefox es usar el software Perspectives de la Universidad Carnegie Mellon (http://www.cs.cmu.edu/~perspectives/). Perspectives confirma que un sitio psiphon, u otro sitio Web sin un certificado oficial de seguridad, aparece igual para ti que para otros servidores.

INICIAR SESIÓN EN EL PROXY

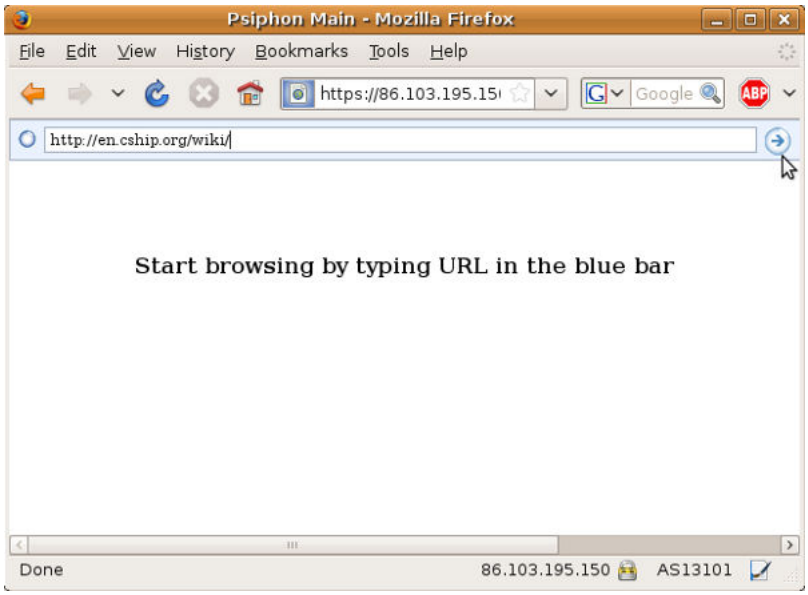
Al mostrarse la página de registro, entramos el nombre de usuario y la contraseña que obtuvimos del contacto (en este ejemplo ambos son "cship"). Debemos asegurarnos que la URL comienza con "https", solo así sabremos que usamos un nodo psiphon bajo una conexión segura.



NAVEGANDO A TRAVÉS DEL PROXY

Después de registrarnos, se verá la página de inicio de psiphon.

Entramos la URL del sitio Web que se quiere visitar (en este ejemplo, http://en.cship.org/wiki/), en la caja que está en el tope de la página (bajo la dirección del navegador en sí)



Damos clic en el botón con la flecha o presionémos la tecla Retorno. El navegador mostrará el sitio Web cuya dirección entramos, y la caja de dirección de psiphon en el tope.

Para continuar navegando puedes hacer cualquiera de estas cosas:

- Clic en cualquier enlace. El proxy Web automáticamente se usa para recuperar la página enlazada.
- Entre una nueva URL en la caja de dirección psiphon en el tope de la página (no la caja de dirección del navegador).

Debemos tener en cuenta que el dueño del nodo psiphon puede monitorear y anotar cada sitio Web y cada contraseña que entramos. De hecho, psiphon normalmente muestra al operador una lista de las URLs visitadas. Es por esto que es importantente que contactemos a alguien confiable.

Autores : *UsingPsiphon*
© Freerk Ohling 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Austin Martin 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

Produced in FLOSS Manuals

13. USO DE PSIPHON 2

Psiphon2 es un tipo especial de proxy web que trabaja a diferencia de otros (como el CGIProxy o PHProxy) con autenticación. Para usar psiphon2 necesitas la URL (dirección) y una cuenta (nombre de usuario y contraseña). Esto hace el uso un poco más difícil, pero adiciona mucha seguridad.

CÓMO OBTENER UNA CUENTA PSIPHON2

Para prevenir y monitorear el bloqueo de un nodo psiphon2 se trabaja con un "web of trust", así que necesitamos una invitación de un usuario que tenga una cuenta psiphon2.

Usar un enlace de invitación para registrarse

Una vez que tengamos un enlace de una invitación como: https://85.31.189.76/w.php?p=384BC accedemos a ese sitio con nuestro navegador favorito (por ejemplo Firefox o Internet Explorer).

Aceptar el mensaje de error SSL

Cuando accedemos al sitio web por primera vez veremos un mensaje de error a causa del certificado SSL no válido. Los certificados SSL se usan para garantizar la identidad de un servidor. Un certificado SSL firmado por las autoridades de Certificaciones cuesta mucho dinero, así que será muy caro comprar un certificado para cada nodo psiphon2. No obstante la conexión es completamente encriptada y puedes confirmar con seguridad el mensaje de error.

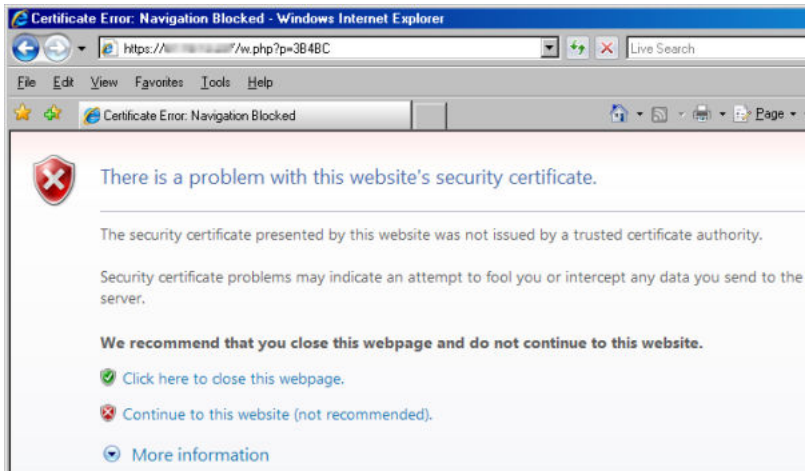
SSL-Error con Internet Explorer 6

Si usas Internet Explorer 6, el mensaje de error se verá así:

Confirmemos el mensaje con un clic en "Yes".

SSL-Error con Internet Explorer 7

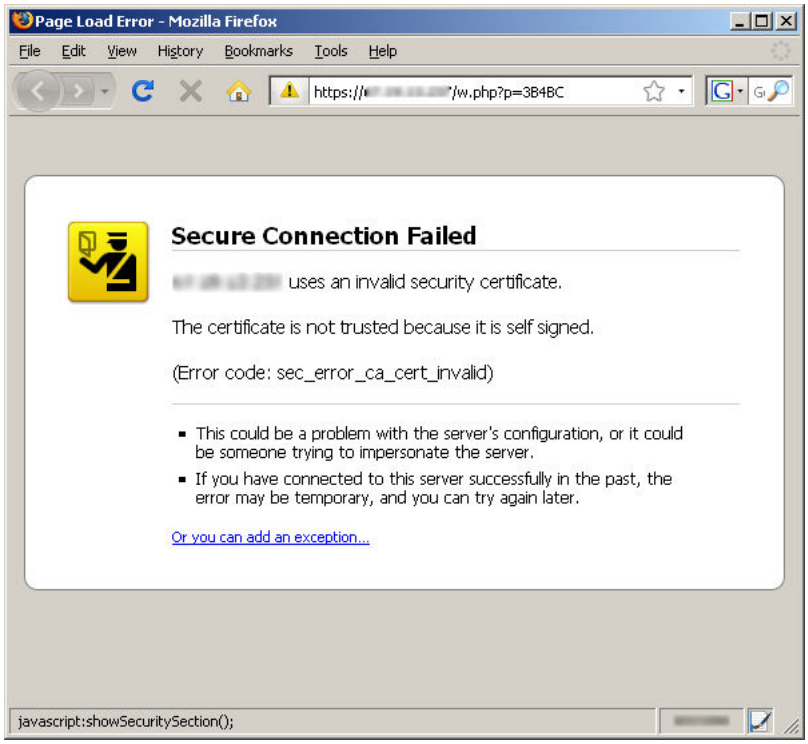
Si usa Internet Explorer 7, el mensaje de error se verá así:



Confirmemos esto con un clic en "Continue to this website (not recommended)."

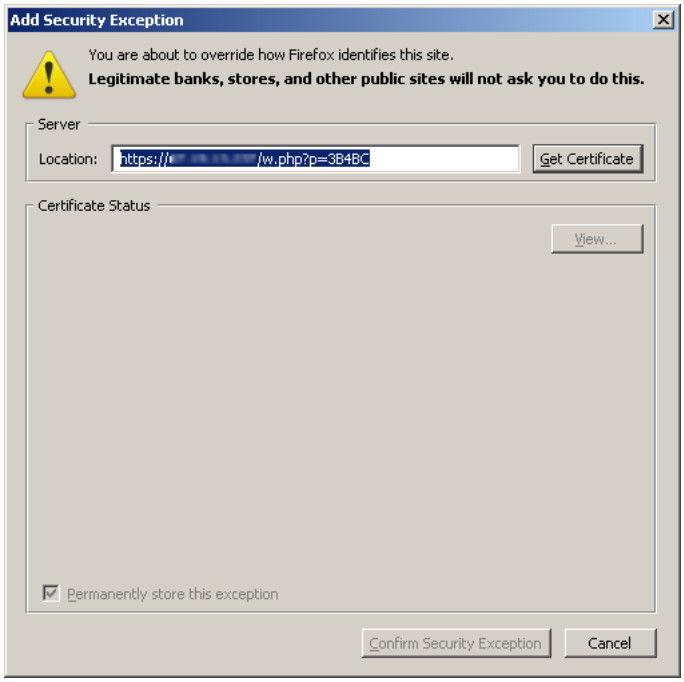
SSL-Error con Firefox 3

Si usamos el navegador Firefox3 es un poco más complicado:

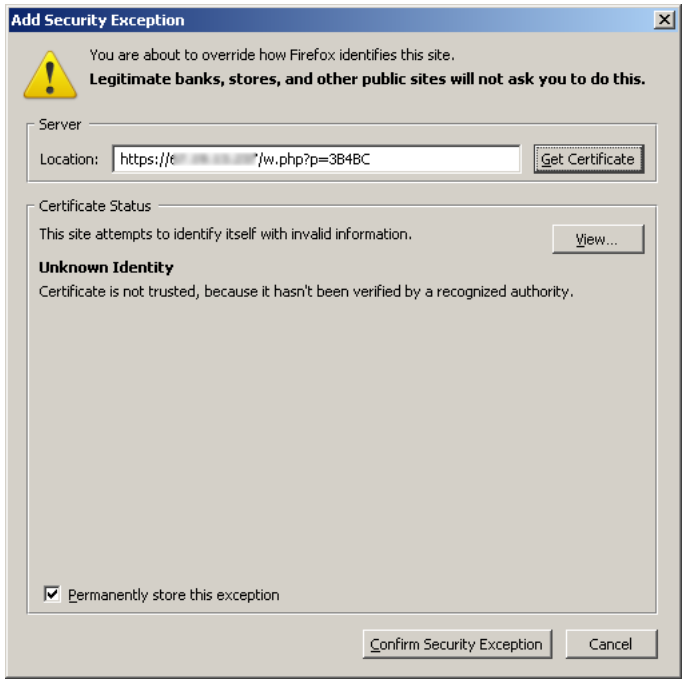


Primero clic en "Or you can add an exception..."

Después clic en "Add Exception..."



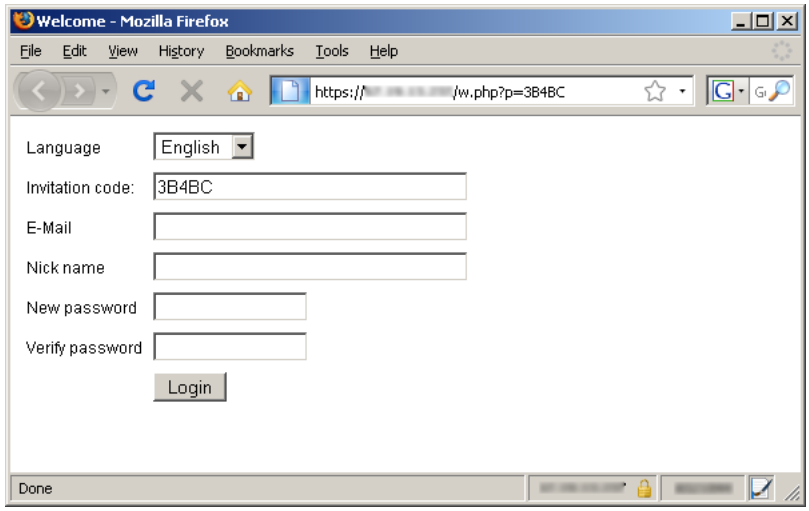
Seguidamente en "Get Certificate"



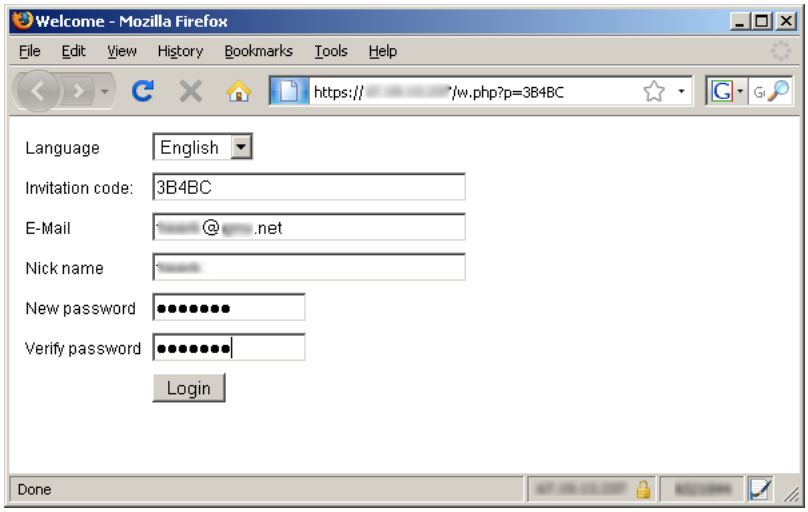
Y finalmente "Confirm Security Exception".

Crear nuestra propia cuenta

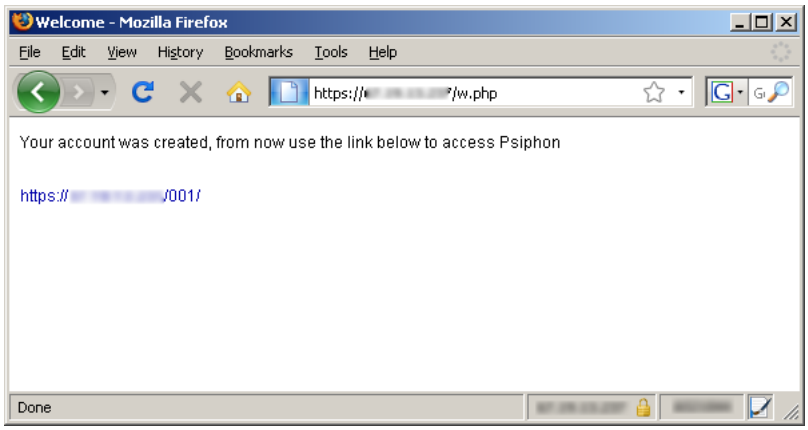
Una vez que hayamos confirmado el aviso de seguridad veremos un formulario simple de registro:



Seleccionamos un idioma, dejamos el código de Invitación como está y entramos la dirección de correo, un nick y una contraseña (dos veces la misma). La dirección de correo electrónico se usará para enviarnos un nodo psiphon nuevo cuando este esté bloqueado. Nunca se enviará spam a esa dirección. La dirección de correo electrónico y la contraseña que seleccionemos se registrará obligatoriamente en el nodo psiphon más tarde, así que tendremos que recordarlos.

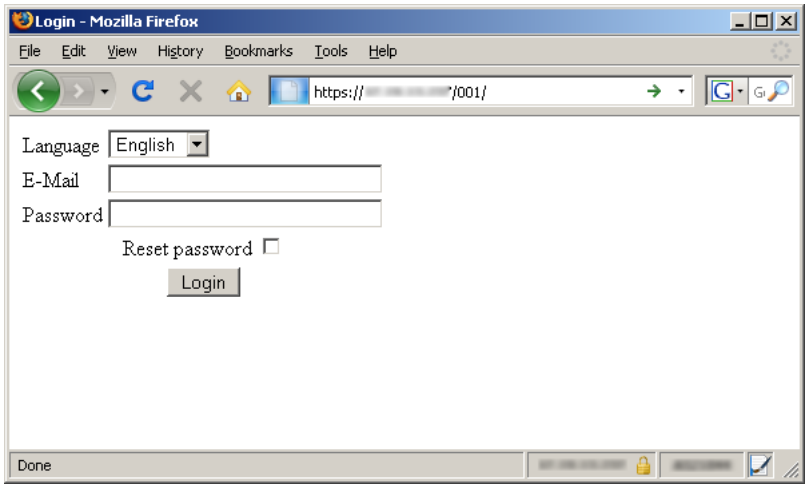


Después de un clic en "Login" verá un mensaje confirmando la creación exitosa de la cuenta:

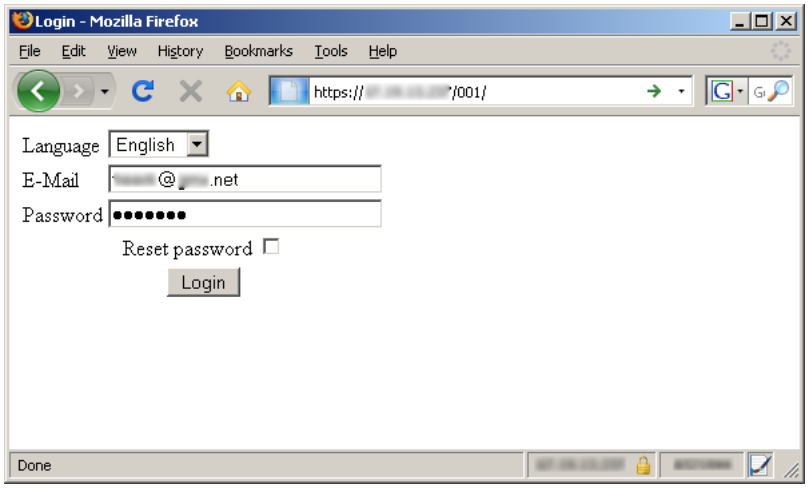


USANDO EL NODO PSIPHON2

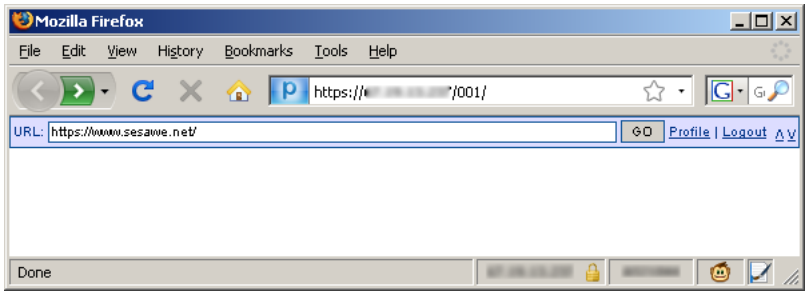
Para usar el nodo psiphon2 no volveremos a necesitar el enlace de la invitación, solo necesitamos recordar el vínculo que aparece al final del registro, por ejemplo "https://85.31.189.76/001/". Accedemos a esa URL con el navegador (por ejemplo Internet Explorer o Firefox)



Ahora introducimos la dirección de correo y la contraseña que se usó para registar la cuenta psiphon2. También se puede seleccionar otro idioma:



Después de registrarse se verá una página en blanco con una forma pequeña en la parte superior. Entramos el sitio que queremos visitar en ese formulario, ej. "https://www.sesawe.net/" y damos clic en "GO".



Ahora el sitio Web que deseamos visitar se cargará y se puede continuar navegando en Internet libremente. Todos los enlaces en el sitio serán reescritos automáticamente para que se accedan a través del nodo psiphon2.

INVITANDO A OTROS

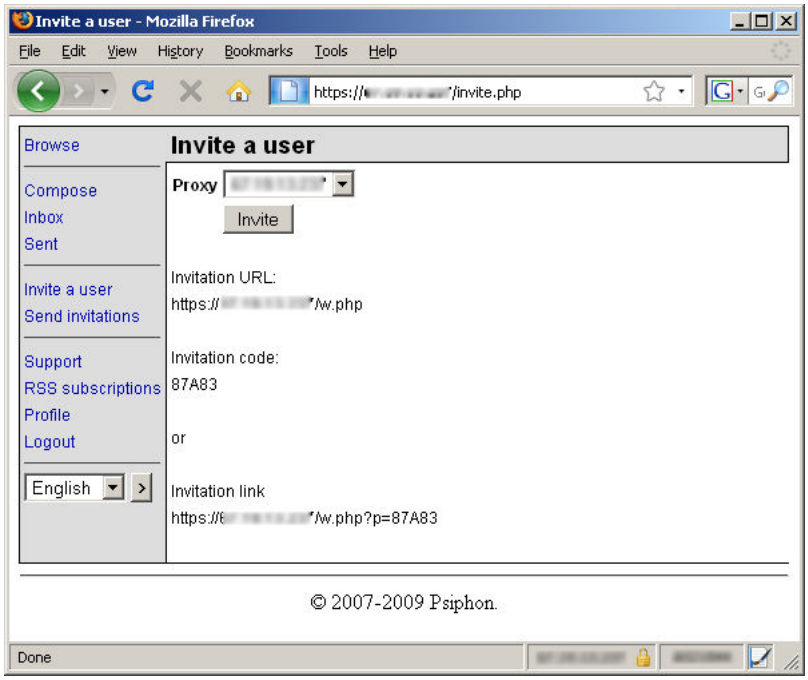
También podemos ayudar a amigos o familiares a acceder a los sitios libremente con psiphon2.

Para poder invitar a otras personas debes ser un "Power user". Para obtener este status, preguntemosle a quién nos invitó si nos puede conceder ese derecho. Podemos ver si tienemos una cuenta de "Power user" buscando en el Perfil (Iniciamos sesión en psiphon2 y clic en "Profile"). Si vemos el enlace "Invite a user" y "Send invitations" en el menú de la izquierda significa que somos un "Power user".

Hay dos formas de invitar a otras personas:

Invitar un usuario

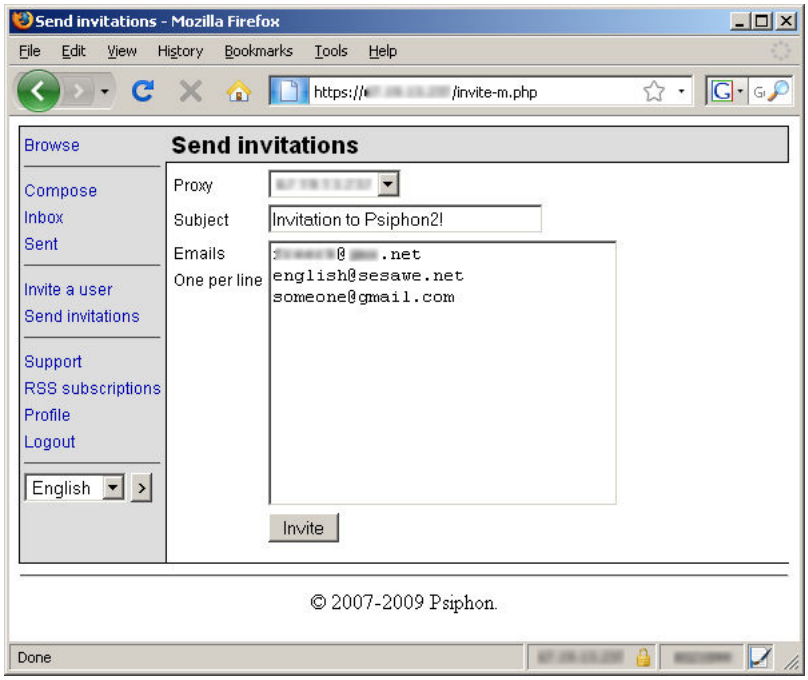
Clic en "Invite a user" en la página de perfil psiphon2 para generar un código de invitación o enlace de una invitación que podemos enviar por ejemplo por correo electrónico, mensajería instantánea o teléfono. Primero, selecciona un nodo psiphon2 por el cual quieres enviar la invitación. Es muy probable que tengamos un solo nodo en el menú, así que dejamos la opción por defecto. Después de hacer clic en "Invite" veremos un enlace de invitación nuevo generado que podemos enviar a amigos. Si tienen problemas para usarlo pueden intentar con "Invitation URL" y el "Invitation Code" manualmente.



Enviar invitaciones

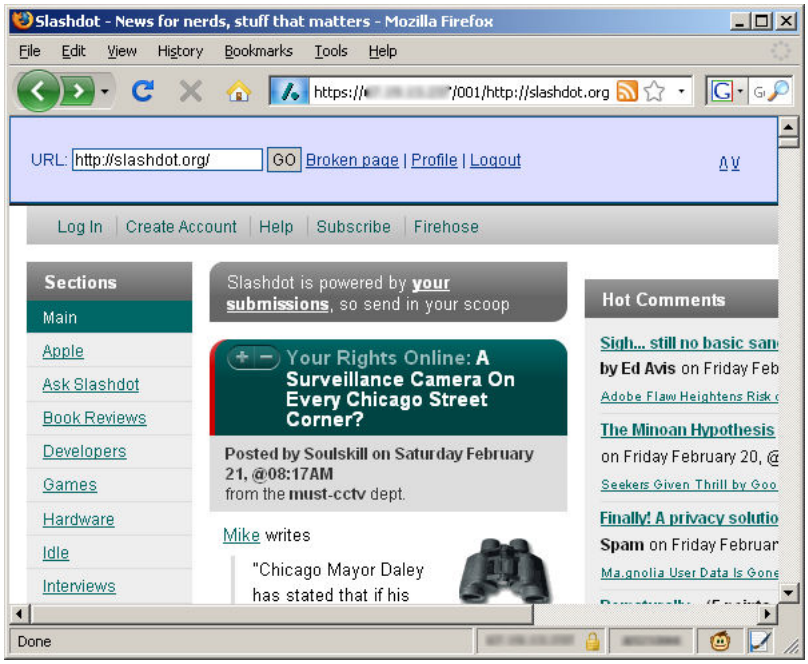
Clic en "Send invitations" en el perfil psiphon2 para enviar uno o más enlaces de invitación automáticamente a través del nodo psiphon2. Las ventajas de este método es que nos mantenemos anónimos, el receptor de la invitación por correo no sabe quien se la envió.

Primero, seleccionamos el nodo psiphon2 desde el cual deseamos enviar la invitación. Es muy probable que tengamos un solo nodo en el menú, así que dejamos la opción por defecto. Esto puede ser muy parecido a "Invitation to psiphon2" u otra frase no directamente relacionada, por ejemplo "Viva el Rey!!". Entrese la dirección de correo electrónico a la que se desee enviar la invitación. Puedes entrar una solo dirección de correo o muchas, una por línea. Después de un clic en "Invite" se verá el mensaje "1 invitations queued" lo que significa que el nodo enviará el correo en los próximos minutos.

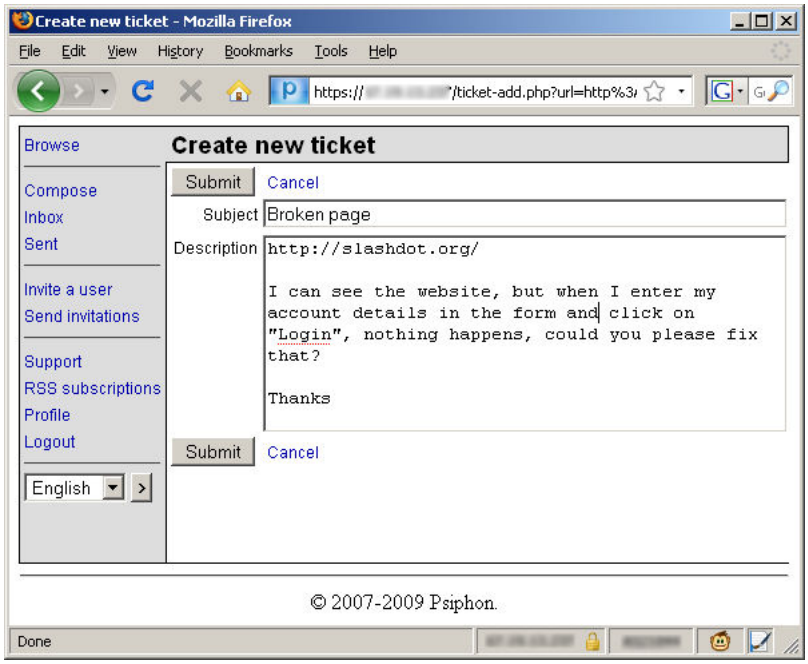


REPORTAR UN SITIO BLOQUEADO

Puede que algunos sitios que usan tecnologías complicadas como Video streaming o AJAX no trabajen en psiphon2. Para mejorar esto nuestros desarrolladores necesitan saber qué sitios no funcionan. Si encontrásemos un sitio así reportémoslo haciendo clic en el enlace "Broken Page" cerca del botón "GO" en la parte superior de la forma:



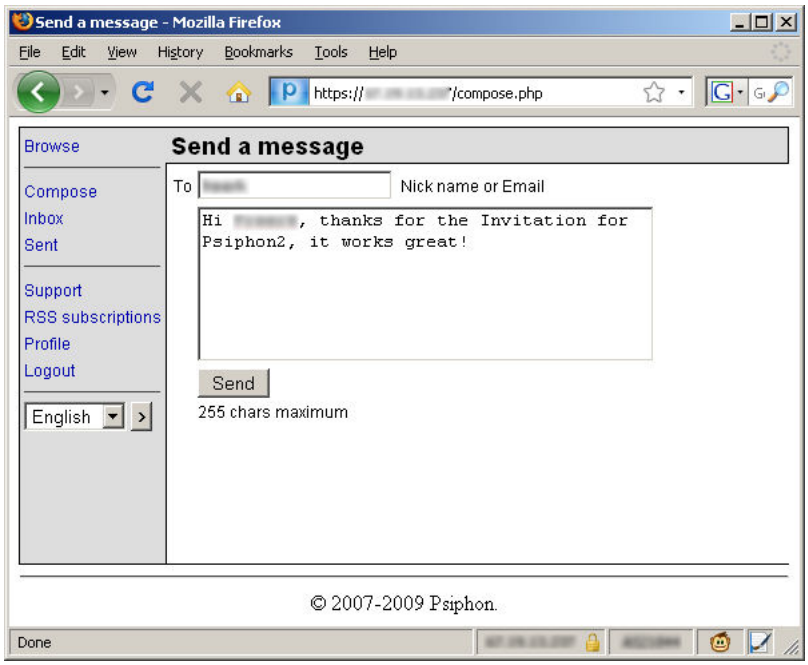
En el siguiente sitio web podemos entrar información adicional en el campo "Description" para hacer más fácil para los desarrolladores reproducir el error y repararlo. Con un clic en "Submit" enviaremos un mensaje a los desarrolladores



USAR PSIMAIL

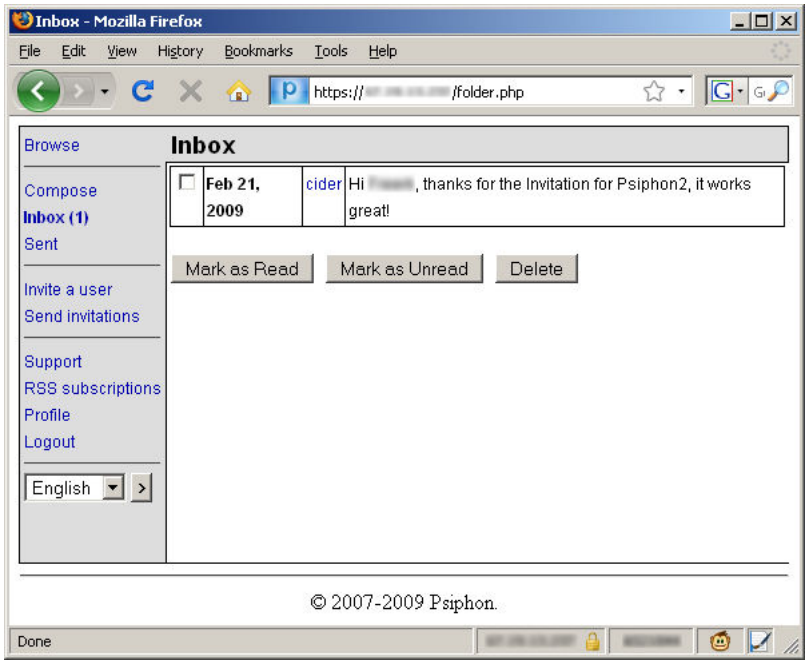
Enviar mensajes

Con psiphon2 es posible enviar mensajes internos a otros usuarios psiphon2. Para escribir un mensaje entremos en su perfil psiphon2 y demos clic en "Compose". Primero hay que entrar el Nick del usuario al que desea enviar el mensaje. Podemos además entrar la dirección de correo que el otro usuario usó al registrarse en psiphon2. Nótese que no es posible enviar mensajes a direcciones de correo normales que no estén registradas en psiphon2. Escríbase el mensaje en el textbox y demos clic en "Send". Se recibirá un mensaje que dice "Message was sent".



Leer Mensajes

Para ver si se recibió algún mensaje nuevo entraremos en nuestro perfil psiphon2. Si "Inbox(1)" está en negrita en el menú de la izquierda, tenemos un mensaje nuevo. El número entre paréntesis representa la cantidad de mensajes nuevos. Después de un clic en el enlace podemos leer los mensajes:



Puedes seleccionar uno o más mensajes y seleccionar una de las posibles opciones: "Mark as Read", "Mark as Unread" o "Delete".

MÁS RECURSOS

Psiphon2 FAQ en sesawe.net: https://www.sesawe.net/Psiphon-FAQ.html

Autores : *UsingPsiphon2*
© Freerk Ohling 2009
Modifications:

Ariel Viera 2009
Austin Martin 2009
Zorrino Zorrinno 2009

Produced in FLOSS Manuals

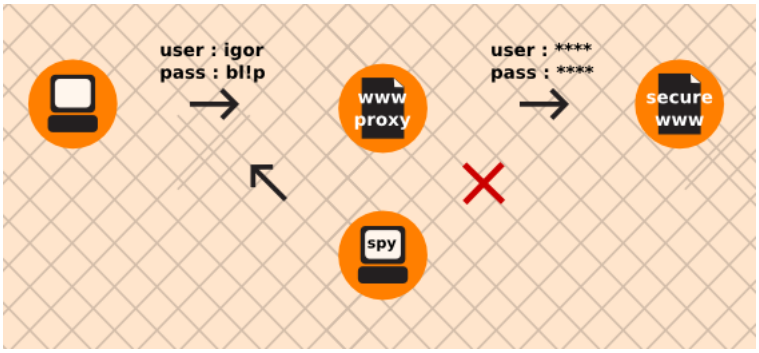
14. RIESGOS DEL PROXY WEB

Han de tenerse en cuenta algunos riesgos asociados con el uso de los **proxies Web**, especialmente aquellos que mantienen personas u organizaciones que no conocemos. Si usamos un proxy para ver sitios Web públicos como npr.org, el único riesgo es que alguien sabrá que estabamos leyendo las noticias de ahí (y usando un proxy para leer). Sin embargo, si usamos un proxy para enviar comunicaciones privadas o para acceder aplicaciones como correo Web, bancos y compras en línea, existe el riesgo de que otras personas puedan acceder y abusar de esa información, incluyendo nuestras contraseñas privadas, especialmente si esos servicios no usan cifrado o si el proxy impide usarlo.

FALTA DE PRIVACIDAD

Los sistemas de evasión de filtrado o bloqueado no necesariamente ofrecen el anonimato (incluso aquellos que incluyen palabras como "anonymizer"en sus nombres). Si el enlace entre el proxy Web y nosotros está sin cifrar (**HTTP** en lugar de **HTTPS**), tal y como pasa con muchos servicios de proxy Web gratis, el operador del proxy o un intermediario como un **Proveedor de Servicios de Internet** (ISP) puede interceptar y analizar el contenido. En ese caso, aunque la evasión puede resultar satisfactoria, los operadores de redes pueden rastrear el hecho de que hayamos usado un proxy Web y pueden determinar el contenido y los sitios Web que hemos visitado.

Un proxy Web que no cifra su conexión algunas veces usa otros métodos para evitar el filtrado de Internet. Por ejemplo, una técnica simple se llama ROT-13, en la cual la letra actual de una URL se sustituye por la letra que está 13 caracteres delante de ella en el alfabeto estándar en Latin. (Podemos com probarlo en http://www.rot13.com/). Usando ROT-13, la URL http://ice.citizenlab.org se convierte en uggc://vpr.pvgvmrayno.bet - haciéndolo irreconocible a un filtro de palabras claves. Esto puede ayudar a alcanzar el destino Web deseado, pero tiene sus debilidades: el contenido de la sesión puede ser detectado y tales medidas pueden revertirse fácilmente

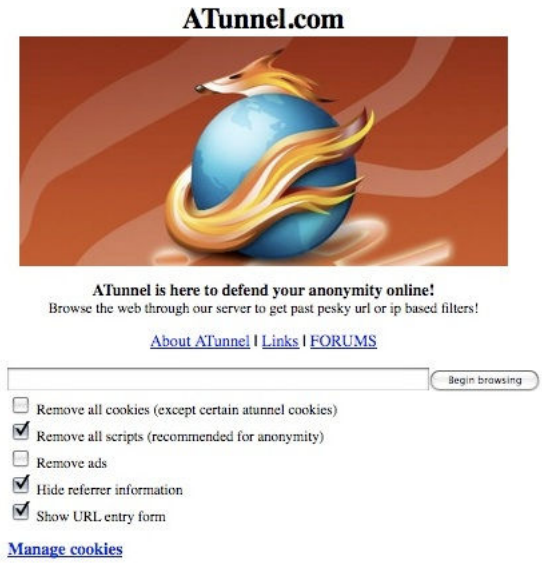


ANUNCIOS PUBLICITARIOS, VIRUS Y MALWARE

Algunas personas que montan proxies Web lo hacen para ganar dinero. Esto se puede hacer simplemente y abiertamente vendiendo anuncios en las páginas. Con alguna mala intención, algunos operadores pueden tratar de infectar las computadoras de aquellos que usan sus proxies con programas maliciosos. Los llamados "drive-by-downloads" pueden secuestrar nuestra computadora para spam u otros propósitos comerciales e incluso ilegales.

Lo más importante que podemos hacer para protegernos contra virus es mantener todos nuestros programas -- incluyendo el sistema operativo -- actualizados y usar un antivirus con la última actualización disponible. Además podemos bloquear los anuncios usando la Extensión AdBlockPlus[7] para el navegador Firefox (http://www.adblockplus.org/). Más información sobre cómo evitar estos riesgos se pueden encontrar en el sitio Web StopBadware[7] (http://www.stopbadware.org/).

El operador de ATunnel.com soporta el servicio gratis vendiendo anuncios. Este es un ejemplo típico de un servidor proxy soportado por anuncios publicitarios.



COOKIES Y SCRIPTS

Existen riesgos relacionados con el uso de las cookies y los scripts. Muchos proxies Web pueden configurarse para eliminar cookies y scripts, pero muchos sitios (por ejemplo, sitios sociales como el MySpace[7]) requieren el uso de cookies y scripts. Debemos tener cuidado al permitir estas opciones, porque las cookies pueden salvarse en nuestra computadora incluso después que la reiniciemos, y puede proveer evidencia de los sitios que has visitado. Una opción es permitir el uso selectivo de Cookies. En Firefox 3, por ejemplo, podemos instruir al navegador para aceptar cookies solo "Hasta que Firefox se cierre". (De manera similar, podemos instruir al navegador para eliminar el historial de navegación cuando lo cerremos.)

Algunos sitios y anunciantes pueden usar estos mecanismos para rastrearnos incluso cuando usamos proxies. Si trataramos de mantenermos anónimos, esto puede ser un problema porque este rastreo puede producir evidencia, por ejemplo, que la persona que hizo una cosa abiertamente es la misma persona que hizo otra cosa de manera anónima.

EL OPERADOR DE PROXY PUEDE VER TODO

Aún cuando la conexión al evasor basado en Web puede ser segura (cifrada), el dueño del proxy tendrá acceso al contenido de tus comunicaciones después de desencriptarla. Una preocupación adicional es los registros (ficheros log) que el proxy puede conservar. Dependiendo de la locación del evasor o de la locación del servidor, las autoridades pueden tener acceso a esos ficheros logs.

TECNICAS AVANZADAS

15. NOCIONES AVANZADAS
16. PROXIES HTTP
17. INSTALANDO SwitchProxy
18. USO DE SwitchProxy
19. TOR - THE ONION ROUTER
20. USO DEL PAQUETE TOR DE NAVEGADOR
21. USO DEL PAQUETE TOR DE MI
22. USO DE TOR CON PUENTES
23. USO DE JON DO

15. NOCIONES AVANZADAS

Pueden existir muchas razones por las que técnicas simples para acceder contenido bloqueado, como el uso de versiones de páginas en caché desde los motores de búsqueda, o un proxy Web simple, son inadecuadas.

En algunos casos, estas técnicas simples no son suficientes para acercarse al bloqueo. En otros, las restricciones pueden afectar los servicios más allá de la simple navegación Web – como puede ser la mensajería instantánea, y el streaming de video o correo electrónico. En ese caso, los proxies Web no resolverán tus problemas.

Pueden existir casos en los que quieras evadir el boqueo de Internet, pero además evitar que las organizaciones que bloquean conozcan las páginas a las que estás accediendo, o evitar que sepan que estás evadiendo el filtrado en primer lugar.

En estos escenarios, hay muchas técnicas más disponibles, y cada una de ellas resuelve un problema diferente y de diferentes maneras. Este capítulo introduce algunos conceptos técnicos clave que te ayudarán a hacer una selección documentada acerca de cuál selección es *aplicable en una situación dada. Cubre además en algún detalle, muchas de las diferentes vías de acceder información que puede estar bloqueada.

PUERTOS Y PROTOCOLOS

Internet está basado en una serie de protocolos, reglas estandarizadas que controlan como se comunican las redes de computadoras. El conjunto principal de protocolos para administrar conexiones y paquetes de mensajes en Internet es TCP/IP (TCP sobre IP). Los protocolos manejan un rango amplio de datos, con programas para fraccionar transmisiones largas en pequeñas, paquetes enumerados para transmitir y reensamblar los segmentos de datos en el paquete final a recibir. La manera más común de especificar cual protocolo usar es direccionar los paquetes a un número de puerto específico. Por ejemplo, HTTP para la Web usa el puerto 80, y POP3 para recibir correo normalmente usa el puerto 110. El bloqueo del tráfico a un puerto en particular en una dirección IP en particular deshabilita el acceso normal a un servicio en ese sitio, mientras deja el resto de los servicios disponibles. La forma más fácil de evadir un puerto bloqueado es proveer el servicio de un puerto no estándar, pero solo lo puede hacer el operador del servicio, y no el usuario.

El modelo de red por capas

Los protocolos de red se describen como un conjunto de capas. Para Internet, la capa más profunda (llamada **Capa de Enlace**) está más cerca del hardware, y la más arriba (llamada **Capa de Aplicación**) está más cerca del usuario. Los protocolos críticos que se encuentran en el medio de estas dos capas son **TCP (Transmission Control Protocol)**, que está en la **capa de Transporte**, y **IP (Internet Protocol)**, que está debajo en la **capa Internet**. A las dos juntas se les refiere como TCP/IP. Uno menos conocido pero también importante es **UDP (User Datagram Protocol)**, el que está al mismo nivel que TCP.

Muchos, pero no todos los servicios brindados sobre TCP están disponibles también sobre UDP, mientras algunos servicios están en UDP solamente.

El nivel tope, llamado **capa de Aplicación**, incluye protocolos como **DNS** (para nombres de dominios), **FTP** (transferencia de ficheros), **HTTP** (Web), **IRC** (chat), **NNTP** (Usenet), **POP3** (recuperación de correo), **SIP** (Voz sobre IP), y **SSH** (comunicaciones encriptadas). **IANA** (Internet Assigned Names Authority) asigna números a los puertos para cada uno de estos servicios de aplicaciones, tales como el puerto 53 para consultas de búsqueda de DNS, 80 para http, y 110 para POP3 (Post Office Protocol 3). Estas asignaciones son por defecto, por conveniencia, y usarlos no son generalmente un requerimiento técnico de los protocolos; de hecho, cualquier tipo de datos puede ser enviado por cualquier puerto. Existen también numerosas asignaciones de puerto por defecto para UDP que opera de la misma forma. En algunos casos, un servicio puede accederse por el mismo puerto usando TCP o UDP. Una excepción es NTP (Network Time Protocol), el cual solo se prevee en UDP. UDP es también comúnmente usado para aplicaciones multimedia en tiempo real tales como Voz sobre IP protocolos (VoIP[?]), algunos de los que no están disponibles sobre TCP.

Los usuarios normalmente no están preocupados por las asignaciones de puertos, las cuales son manejadas automáticamente en los casos por defecto. Sin embargo, el uso de puertos por

defecto no es obligatorio. Por un acuerdo previo entre proveedores de servicios y usuarios, los administradores de sistema pueden levantar los servidores para acceder a servicios estándares en puertos no estándares. Esto permite al programa evadir el bloqueo simple por puertos para prevenir el uso de estos servicios.

Algunos programas pueden configurarse para usar números de puerto no estándares. Las URLs también tienen particularmente una forma estándar conveniente de especificar un número de puerto adentro de una URL. Por ejemplo, la URL http://www.example.com:8000/foo/ hará una solicitud http a example.com en el puerto 8000, en lugar de hacerlo al puerto por defecto 80.

TÉCNICAS DE FILTRADO AVANZADAS

[Adaptado de "Access Denied", Chapter 3, by Steven J. Murdoch and Ross Anderson]

Los objetivos de desplegar un mecanismo de filtrado varía en dependencia de las motivaciones de la organización que los despliega. Ellos pueden hacer un sitio Web en particular (o una página individual) inaccesible para aquellos que quieran verlo, para hacerlo poco confiable, o para impedir a los usuarios que intenten accederlo en primer lugar. La selección del mecanismo dependerá de la capacidad de la organización que solicita el filtrado – donde tienen accesos, las personas contra las que pueden imponer sus deseos, y cuanto tienen la intención de gastar. Otras consideraciones incluyen el número de errores aceptables, si el filtrado debe ser abierto u oculto, y cuan confiable es (ambos contra usuarios casuales y contra aquellos que desean evadir el filtrado).

En esta sección se describe como el contenido particular puede ser bloqueado una vez que la lista de recursos a ser bloqueados está establecida. Construir esta lista es un desafío considerable y una debilidad común de los sistemas desplegados. No solo un gran número de sitios Web hacen la construcción de una lista comprensible de contenido prohibido difícil, sino que como los contenidos se mueven y los sitios Web cambian de dirección IP, mantener esta lista actualizada requiere un gran esfuerzo. Además, si el operador de un sitio desea interferir en el bloqueo, el sitio se moverá más rápido que si el operador no interviniera.

Filtrado de encabezado TCP/IP

Un paquete IP consiste en un encabezado seguido por los datos que carga el paquete (la carga útil). Los routers deben inspeccionar el encabezado del paquete, ya que aquí está la dirección IP destino del paquete. Para prevenir que los ordenadores sean accedidos, los routers pueden ser configurados dejar caer los paquetes destinados a una dirección IP en una lista negra. Sin embargo, cada ordenador puede proveer múltiples servicios, como alojar sitios Web y servidores de correo. El bloqueo basado solamente en la dirección IP hará inaccesibles todos los servicios del ordenador en lista negra.

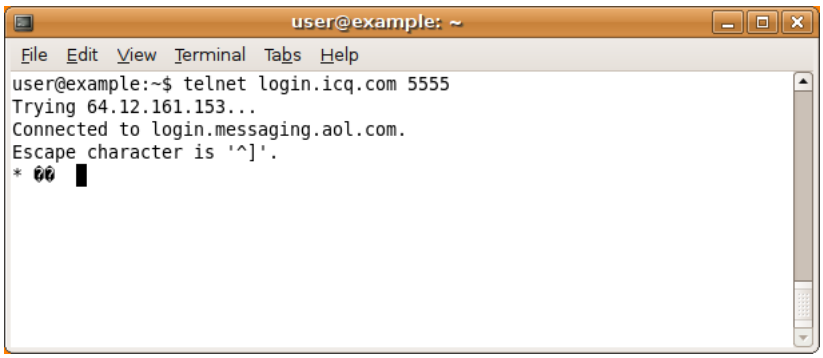
Ligeramente un bloqueo más preciso puede alcanzarse poniendo en lista negra el número de puerto, que está también en el encabezado TCP/IP. Es muy común para muchos sitios web diferentes estar alojados en el mismo número IP, en el mismo número de puerto, 80.

Bloqueo de Puerto

El acceso a puertos puede ser controlado por el administrador de red de la organización que aloja la computadora que usas – ya sea una compañía privada o un Cyber café, por el ISP que provee el acceso a Internet, o por alguien como un censor del gobierno que tiene acceso a las conexiones que están disponibles al ISP. Hay muchas otras razones aparte de la censura por la que pueden ser bloqueados los puertos – para reducir el spam, o para controlar los costos asociados con el uso de ancho de banda alto como compartir ficheros punto a punto.

Si un puerto es bloqueado, todo el tráfico en este puerto se vuelve inaccesible para ti. Los censores frecuentemente bloquean los puertos 1080, 3128, y 8080 porque estos son los puertos de proxy más comunes. Si este es el caso, tienes que encontrar proxies que están escuchando por puertos que no son los comunes. Esto puede ser difícil de encontrar.

Puedes probar cuales puertos son bloqueados en tu conexión usando telnet. Solo abre una ventana de comando (terminal o DOS prompt), escribe "telnet login.icq.com 5555" o "telnet login.oscar.aol.com 5555" y presiona Enter. El número es el puerto que deseas probar. Si recibes algunos símbolos extraños, la conexión tuvo éxito.



Si, por otra parte, la computadora inmediatamente reporta que la conexión falló, se acabó el tiempo, o fue interrupta, desconectada, o reiniciada, ese puerto probablemente está siendo bloqueado. (Ten en cuenta que algunos puertos pueden estar bloqueados en conjunción con ciertas direcciones IP.)

Algunos de los puertos usados más comúnmente son:

- 20 y 21 - FTP (transferencia de ficheros)
- 22 - SSH (acceso remoto seguro)
- 23 - Telnet (acceso remoto inseguro)
- 25 - SMTP (enviar correo electrónico)
- 53 - DNS (asigna un nombre a una dirección IP)
- 80 - HTTP (navegación web normal; algunas veces usado para proxy)
- 110 - POP3 (recibir correo electrónico)
- 143 - IMAP (enviar/recibir correo electrónico)
- 443 - SSL (conexiones HTTPS seguras)

- 993 - IMAP seguro
- 995 - POP3 seguro
- 1080 - SOCKS proxy
- 1194 - OpenVPN[?]
- 3128 - Squid proxy
- 3389 - Remote Desktop
- 8080 – Estilo de proxy estándar http

Por ejemplo, en una universidad, solo los puertos 22 (SSH), 110 (POP3), 143 (IMAP), 993 (IMAP seguro) y 5190 (ICQ mensajería instantánea) pueden estar abiertos para conexiones externas. Esto significa que necesitarás encontrar un servidor proxy o servidor VPN ejecutándose en uno de esos puertos, o convencer a un amigo o contacto fuera de la universidad levantar un servidor en esos puertos. La habilidad de ejecutar servidores en otros puertos diferentes a los en que normalmente se ejecutan hacen las técnicas de evasión posibles en primer lugar.

Filtrado de Contenido TCP/IP

El filtrado de encabezado TCP/IP solo puede bloquear comunicación en la base de a donde van los paquetes y de donde vienen, no de lo que contienen. Esto puede ser un problema para el censor si es imposible establecer la lista completa de direcciones IP que contienen contenido prohibido, o si algunas direcciones IP contienen suficiente contenido no infringido de forma que es injustificable bloquear totalmente toda la comunicación. Hay un control fino posible: el contenido de los paquetes pueden ser inspeccionados por las palabras claves censuradas. Como los routers normalmente no examinan el contenido de los paquetes sino los encabezados, puede que se necesite un equipamiento extra. El hardware típico puede que no sea capaz de reaccionar lo suficientemente rápido para bloquear los paquetes infringidos, so other means to block the information must be used instead. Como los paquetes tienen un tamaño máximo, el contenido completo de la comunicación se fraccionará en múltiples paquetes. Así, mientras los paquetes ofendidos consiguen pasar, la comunicación se puede desestabilizar bloqueando paquetes subsiguientes. Esto se puede lograr bloqueando los paquetes directamente o enviando un mensaje a las dos partes en comunicación solicitando terminar la conversación. Otro efecto del tamaño máximo del paquete es que las palabras claves pueden dividirse en paquetes con límites. Los dispositivos que inspeccionan cada paquete individualmente pueden fallar al identificar palabras claves infringidas. Para que la inspección de paquetes sea completamente efectiva, el flujo debe reensamblarse, lo que adiciona complejidad. Alternativamente, un filtro de proxy HTTP puede usarse, como se describe posteriormente.

Forzar DNS

La mayoría de las comunicaciones de Internet usan nombres de dominio en lugar de direcciones IP, particularmente para la navegación Web. Así, si la etapa de resolución de nombre de dominio puede filtrarse, el acceso a los sitios infringidos puede ser bloqueado. Con esta estrategia, el servidor DNS accedido por los usuarios da una lista de nombres de dominio prohibidos. Cuando una computadora solicita la dirección IP correspondiente para uno de estos nombres de dominio, se da una respuesta errónea o no se da respuesta. Sin la dirección IP, la computadora solicitada no puede continuar y mostrará un mensaje de error.

Note que en la etapa en que se ejecuta el bloqueo, el usuario aún no ha solicitado la página, por lo que todas las páginas bajo un nombre de dominio serán bloqueados.

Filtrado de Proxy HTTP

Una manera alternativa de configurar una red es no permitir que los usuarios se conecten directamente a los sitios Web pero forzar (o solo impulsar) a todos los usuarios a acceder a esos sitios por la vía del servidor proxy. En adición a las solicitudes transmitidas, el servidor proxy puede temporalmente almacenar la página Web en caché. La ventaja de este método es que si un usuario secundario del mismo ISP solicita la misma página, será retornado directamente a la página caché, en lugar de conectarse al servidor Web actual una segunda vez. Desde la perspectiva del usuario esto es mejor pues la página aparece más rápido, pues no tienen que conectarse fuera de su propio ISP. Es mejor para el ISP, pues al conectarse al servidor Web se consume (más caro) ancho de banda, y en lugar de tener que transferir páginas desde un sitio popular cientos de veces, solo tienen que hacerlo una vez.

Sin embargo, así como se mejora el funcionamiento, un proxy HTTP puede también bloquear sitios Web. El proxy decide si las solicitudes de páginas Web deben permitirse, y si es así, envía la solicitud al servidor Web que hospeda el contenido solicitado. Puesto que el contenido completo de la solicitud está disponible, las páginas Web individuales pueden filtrarse, basado en el nombre o el contenido actual de la página.

Híbrido de TCP/IP y proxy http

Como una solicitud interceptada por un proxy HTTP debe ser re ensamblada desde los paquetes originales, decodificarla, y retransmitirla, el hardware requerido para mantener una conexión a Internet rápida es muy caro. So systems exist that provide the versatility of HTTP proxy filtering at a lower cost. Ellos operan construyendo una lista de direcciones IP de sitios con contenido prohibido, pero en lugar de bloquear el flujo de datos de estos servidores, el tráfico es redireccionado a un proxy HTTP transparente. Ahí, la dirección Web completa es inspeccionada y si se refiere a contenido bloqueado, se bloquea, de lo contrario pasa normal.

Denegación de Servicio

Where the organization deploying the filtering does not have the authority (or access to the network infrastructure) to add conventional blocking mechanisms, Web sites can be made inaccessible by overloading the server or network connection. Esta técnica, conocida por ataque de Denegación de Servicio (DoS[?]), puede montarse por una computadora con una conexión a Internet muy rápida; más comúnmente, un gran número de computadoras son tomadas y usadas en montar DoS[?] distribuidos.

Desregistración 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 lugar deseado. Almacenar todos los nombres de dominio que existen en la actualidad sería poco factible, en su lugar los llamados solucionadores recursivos almacenan punteros a otros servidores DNS los que pueden saber con más probabilidad la respuesta. Estos servidores dirigirán el solucionador recursivo a los servidores DNS hasta que uno, el servidor "autoritario", pueda retornar 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 hosteado, corre el riesgo de ser desregistrado.

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 hosteado, el servidor puede ser desconectado o el operador puede requerir deshabilitarlo.

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 si mismas.

Criptografía

La criptografía es – entre las aplicaciones -- una defensa técnica contra la vigilancia que usa técnicas matemáticas sofisticadas para confundir las comunicaciones, haciéndolas ininteligibles a un curioso. La criptografía puede impedir también a un operador de redes modificar las comunicaciones, o al menos hacer estas modificaciones detectables.

La criptografía moderna es un concepto extremadamente difícil de derrotar por medios técnicos; un amplio número de programas de criptografía disponibles pueden brindarles a los usuarios protección y privacidad contra curiosos. Por otra parte, la encripción se puede evadir por varios medios, incluyendo targeted **malware**, o en general a través de problemas de **administración de llaves e intercambio de llaves**, 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" 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, peo puede ser aún vulnerable dependiendo de las habilidades del curioso.

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. Hay un espectro de controles disponibles, que van desde lo que cualquiera puede encontrar sensible hasta lo que cualquiera puede encontrar censurable.

Author : *AdvancedBackground*

Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Freerk Ohling 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

16. ¿QUÉ ES UN PROXY HTTP?

Los programas llamados proxy de aplicaciones permiten a una computadora en Internet procesar solicitudes de otra computadora. Los tipos más comunes de aplicaciones proxys son: los proxys HTTP, los cuales manipulan las solicitudes de sitios Web, los proxies SOCKS, que manejan solicitudes de conexión de una amplia variedad de aplicaciones. En este capítulo veremos los proxies HTTP y como funcionan.

PROXIES BUENOS Y MALOS

Los proxies de aplicaciones pueden ser usados por los operadores de redes para censar Internet o para monitorear y controlar lo que hacen los usuarios. Sin embargo, los proxies de aplicación son también una herramienta para los usuarios que desean evadir la censura y otras restricciones de red.

Proxies que restringen el acceso

Un operador de red puede exigir que los usuarios que acceden Internet (o al menos las páginas Web) solo a través de ciertos proxy. El operador de red puede programar este proxy para que mantenga los registros de los accesos de los usuarios y también deniega el acceso a ciertos sitios o servicios (bloqueo de IP o bloqueo de puertos). En este caso, el operador de redes puede usar un firewall para bloquear las conexiones que no van a través del proxy restrictivo. Esta configuración algunas veces se llama proxy forzado, porque los usuarios son obligados a usarlo.

Proxies para evadir

Sin embargo, un proxy de aplicaciones puede ser también útil para las restricciones de censura. Si puedes comunicarte con una computadora en un lugar sin restricciones que está ejecutando un proxy de aplicaciones, puedes beneficiarte de su conectividad sin restricciones. Algunas veces un proxy está disponible al público para usarse; en este caso, es llamado un proxy abierto. Muchos proxies abiertos son bloqueados en países con restricciones de Internet si las personas que administran las restricciones de redes saben sobre ellos.

DONDE ENCONTRAR UN PROXY DE APLICACIONES

Hay muchos sitios Web con listas de proxies de aplicaciones abiertos. Algunos se pueden encontrar en: http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists/.

Por favor note que muchos de los proxies de aplicación abiertos solo existen unas pocas horas, es por eso es importante seleccionar un proxy de la lista que haya sido actualizado recientemente.

CARACTERÍSTICAS DEL PROXY HTTP

Para usar un proxy de aplicaciones, debe configurar las características del proxy para tu sistema operativo o aplicaciones individuales. Una vez que hayas seleccionado un proxy y lo configures en la aplicación, esta tratará de usar ese proxy para todos los accesos a Internet. Asegúrate de tomar nota de los datos de configuración originales de modo que puedas restaurarlos. Si el proxy se vuelve indisponible o inalcanzable por alguna razón, el programa que lo usa dejará de trabajar. En ese caso, necesita reiniciar la configuración inicial.

En Mac OS X y en algunos sistemas Linux, estas características pueden configurarse en el sistema operativo, y automáticamente se pondrán en las aplicaciones como el navegador web o las aplicaciones de mensajería instantánea. En Windows y algunos sistemas Linux, no hay un lugar central para configurar las características del proxy, y cada aplicación debe ser configurada localmente. 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. Típicamente solo los navegadores Web pueden usar un proxy HTTP directamente.

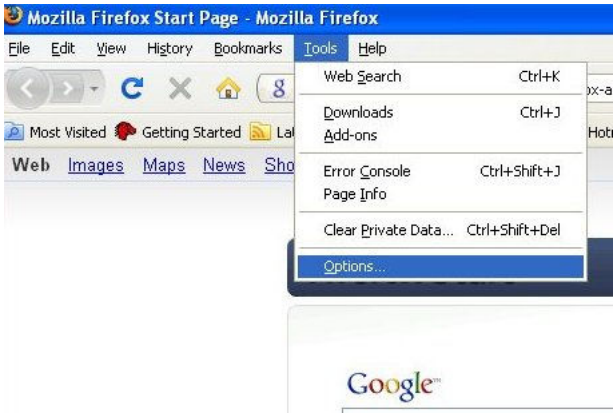
Los pasos a continuación describen como configurar Microsoft Internet Explorer, Mozilla Firefox y el cliente de mensajería instantánea gratis y de código abierto Pidgin para usar un proxy. Si usas Firefox para la navegación Web, será simple usar el programa SwitchProxy[?]; que es una alternativa a los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

Mientras los clientes de correo electrónico como Microsoft Outlook y Mozilla Thunderbird pueden ser también configurados para usar proxies HTTP, el tráfico de correo actual cuando envía correo usa otros protocolos como POP3, IMAP y SMTP, y este tráfico no pasará a través del proxy HTTP.

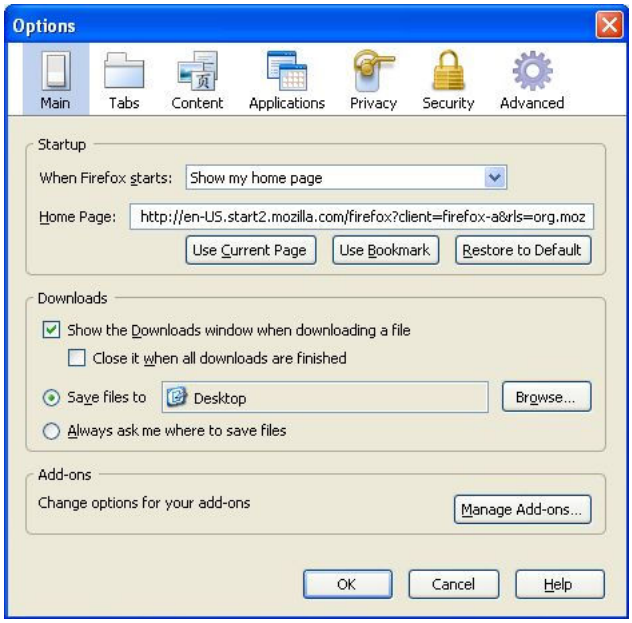
Mozilla Firefox

Configurar Firefox para usar un proxy HTTP:

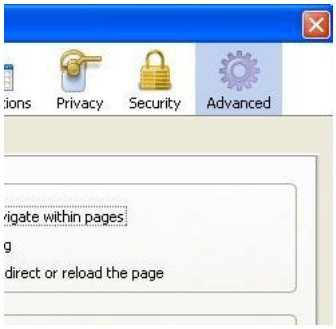
1. En el menú "Herramientas" clic "Opciones":



2. La ventana "Opciones" aparece:

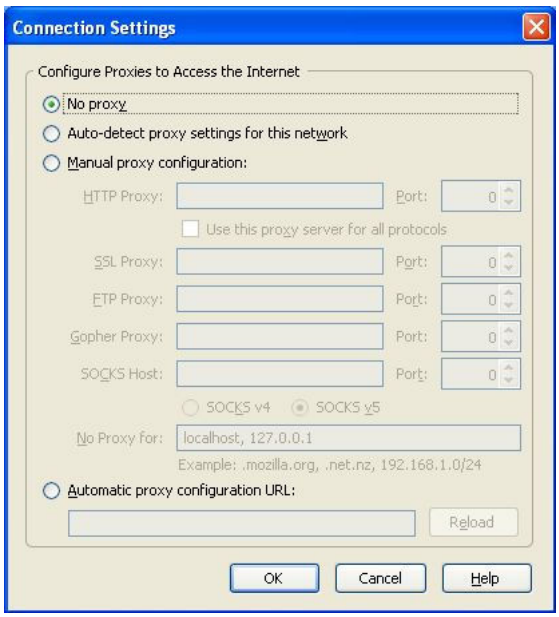


3. En la barra de herramientas en el tope de la ventana, clic "Avanzado":



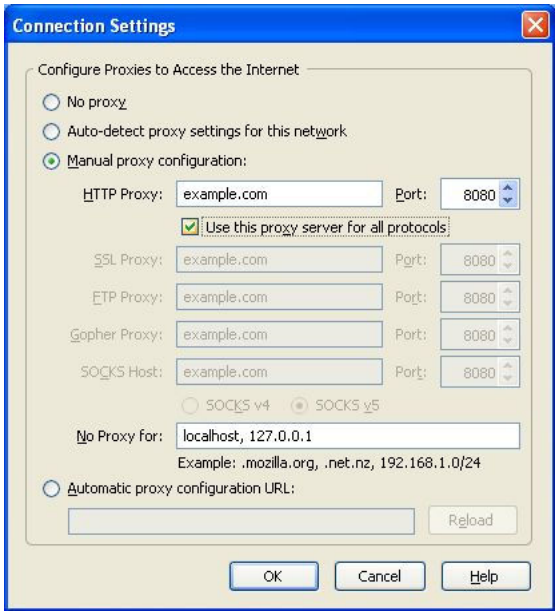
4. Clic el tabulador "Red":

5. Clic en Configuración de conexión:



6. Seleccione "Configuración manual del proxy". Los campos debajo de esta opción se vuelven disponibles.

7. Entre la dirección del "proxy HTTP" y el número del "puerto", y haga clic en "OK".



Si hace 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 estás usando un proxy de aplicaciones público, pues muchos de ellos no soportan HTTPS y FTP. Si, por otra parte tu tráfico HTTPS y/o FTP está siendo bloqueado, puedes intentar un proxy de aplicaciones público con soporte para HTTPS y/o FTP y usar la opción "Usar el mismo proxy para todo&" en Firefox.

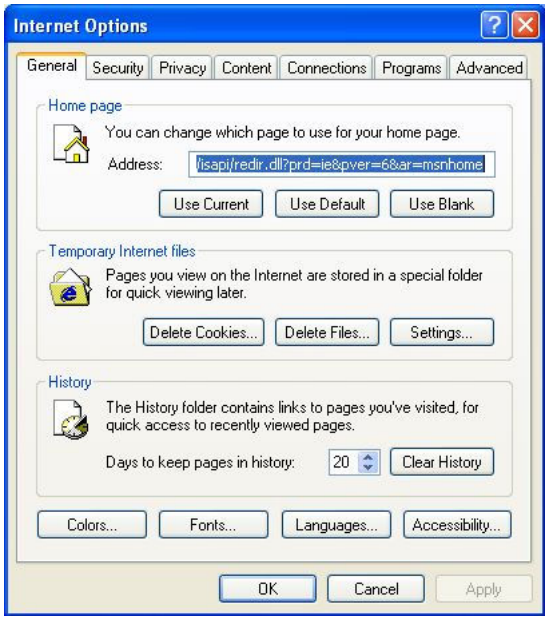
Ahora Firefox está configurado para usar un proxy HTTP.

Microsoft Internet Explorer

Para configurar Internet Explorer para usar un proxy HTTP:

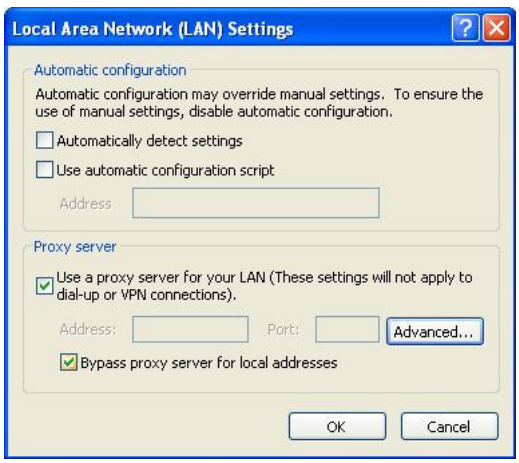
1. En el menú "Herramientas", clic en "Opciones de Internet"

2. Internet Explorer muestra la ventana "Opciones de Internet":

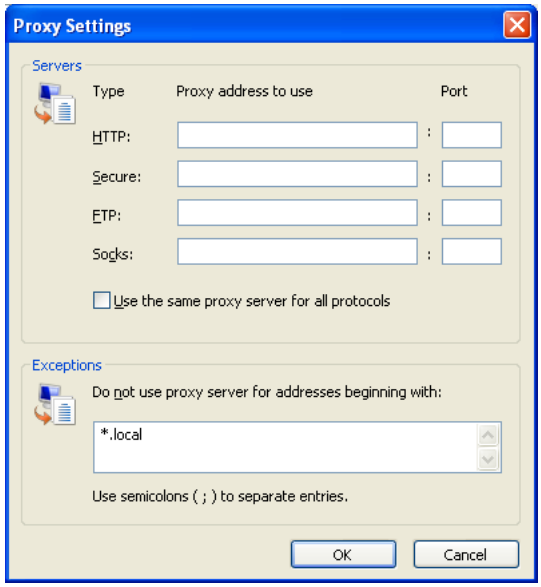


3. Clic en el tabulador "Conexiones":

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



5. Seleccione "Utilizar un servidor proxy para su LAN":
6. Clic en "Avanzado". La configuración de servidores proxy aparece:



7. Entre "Dirección del servidor proxy" y número de "Puerto" en la primera fila de campos.
8. Si hace clic en "Usar el mismo servidor proxy para todos los protocolos", Internet Explorer intentará tráfico enviar tráfico HTTPS (HTTP seguro) y FTP a través del proxy.

Esto puede que no funcione si estás usando un proxy de aplicaciones público, pues muchos de ellos no soportan HTTPS y FTP. Si, por otra parte tu tráfico HTTPS y/o FTP está siendo bloqueado, puedes intentar un proxy de aplicaciones público con soporte para HTTPS y/o FTP y usar la opción "Usar el mismo proxy para todo" en Firefox.

Ahora Internet Explorer está configurado para usar un proxy HTTP.

Cliente de Mensajería Instantánea Pidgin

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

1. En el menú "Tools", clic "Preferences":

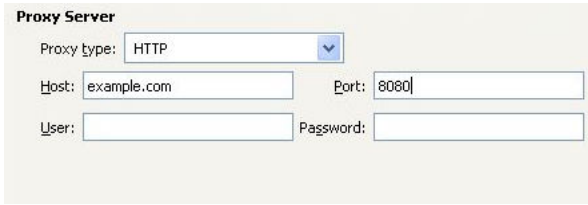
1.

Pidgin muestra la ventana "Preferences":

2. Clic el tabulador "Red" para mostrarlo.

3. En la opción "Proxy type" seleccione "HTTP". Campos adicionales aparecen bajo esa opción.

4. Entre la dirección del "Host" y el número de puerto de tu proxy HTTP.



5. Clic "Close".

Ahora Pidgin está configurado para usar el proxy HTTP.

Cuando termines con el proxy

Cuando terminaste de usar el proxy, particularmente en una computadora compartida, reingresa la configuración que cambiaste a sus valores previos. De lo contrario esas aplicaciones seguirán intentando usar el proxy. Esto puede ser un problema si no quieres que las personas sepan que estabas usando el proxy o si estabas usando un proxy local proporcionado por una aplicación de censura en particular que no está ejecutándose en tiempo real.

Autores : *WhatIsAProxy*

Modifications:
Alice Miller 2008

Ariel Viera 2009
Freerk Ohling 2008, 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Produced in FLOSS Manuals

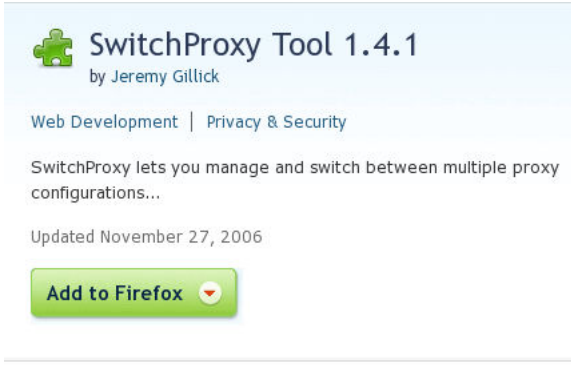
17. INSTALANDO SWITCHPROXY

SwitchProxy puede intercambiar entre múltiples configuraciones de **proxies de aplicaciones** en cualquier computadora usando el navegador Web Firefox. Esto significa que puede fácilmente ejecutarse en **Windows**, **Linux** o **Mac OS X**.

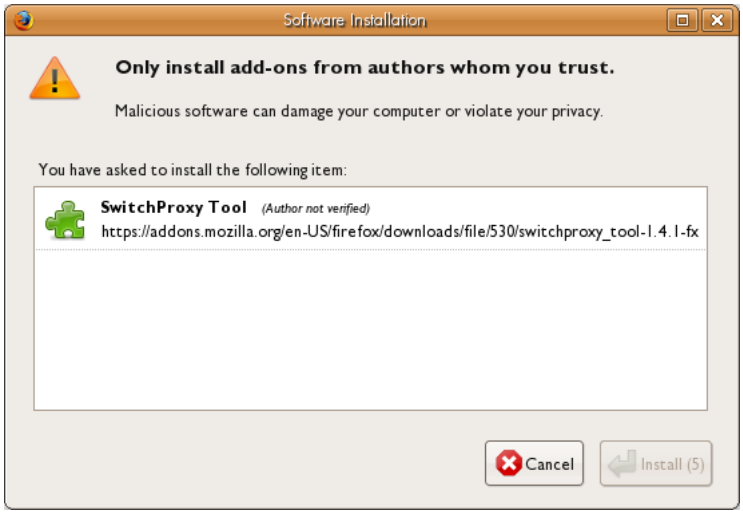
SwithProxy te permite activar y desactivar las conexiones de proxy desde un menú simple. Puede además intercambiar a través de una seriede proxies en un intervalo que especifiques. (El autor de SwitchProxy se refiere a esta característica como soporte para proxies "Anónimos" pero usar esta característica por si sola garantiza tu anonimato.)

Para instalar SwitchProxy:

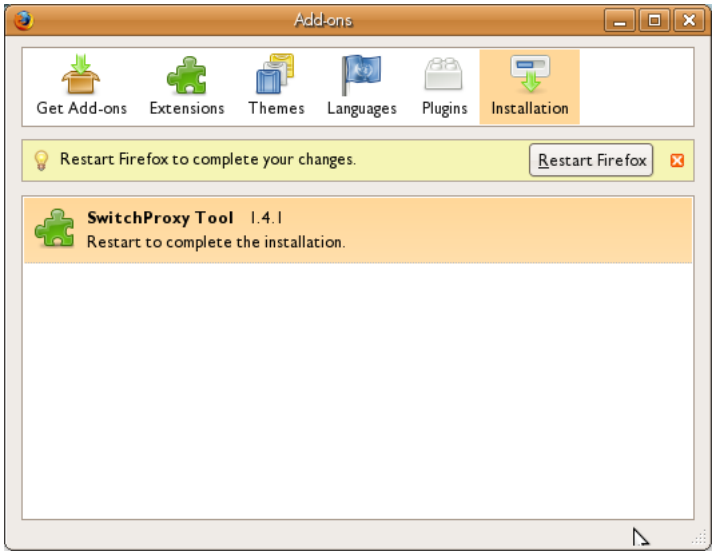
1. Ve a la página Web para adicionar el componente SwitchProxy[7] a FireFox[7]: https://addons.mozilla.org/en-US/firefox/addon/125



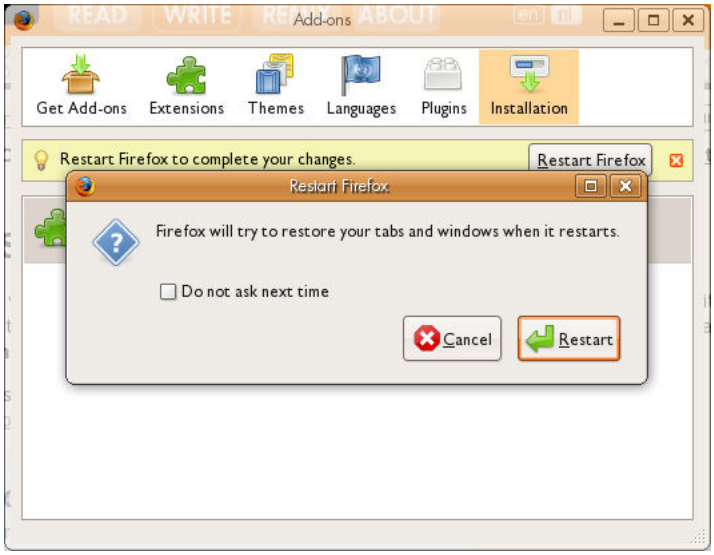
2. Clic "Add to Firefox". El proceso de instalación comienza, y aparece esta ventana:



3. Si haces clic en esta ventana, el botón "Install" (que está inactivo inicialmente) cuenta hacia atrás de 5 a 1. Entonces el botón "Install" se pone activo.
4. Clic "Install". El componente descarga automáticamente y se instala solo. La siguiente ventana aparece:

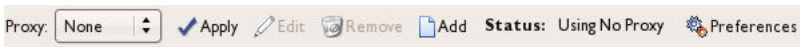


5. Clic "Restart Firefox". Una ventana de confirmación aparece:

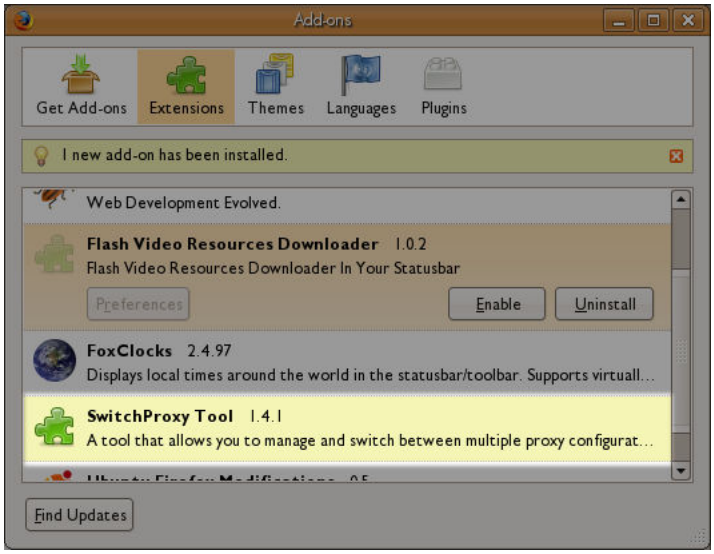


6. Clic "Restart". Firefox se cierra y se vuelve a abrir.

Después que se instala el componente SwitchProxy, la barra de herramientas de Firefox muestra las herramientas para SwitchProxy:



La ventana "Add-ons" de Firefox muestra que switchProxy ha sido instalado:



La lista de componentes puede variar de lo que se ve aquí. Utilice la barra de desplazamiento hasta que vea la herramienta SwitchProxy. Si haces clic en "SwitchProxy", puedes acceder a los controles de Preferencia.

¡Felicitaciones! La herramienta SwitchProxy debe estar instaladad. Ahora es necesario aprender a configurarla y usarla.

Autores : *InstallingSwitchProxy*

Modifications:
Alice Miller 2008

Ariel Viera 2009
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

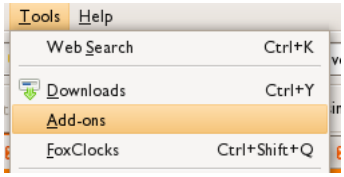
Produced in FLOSS Manuals

18. USANDO SWITCHPROXY

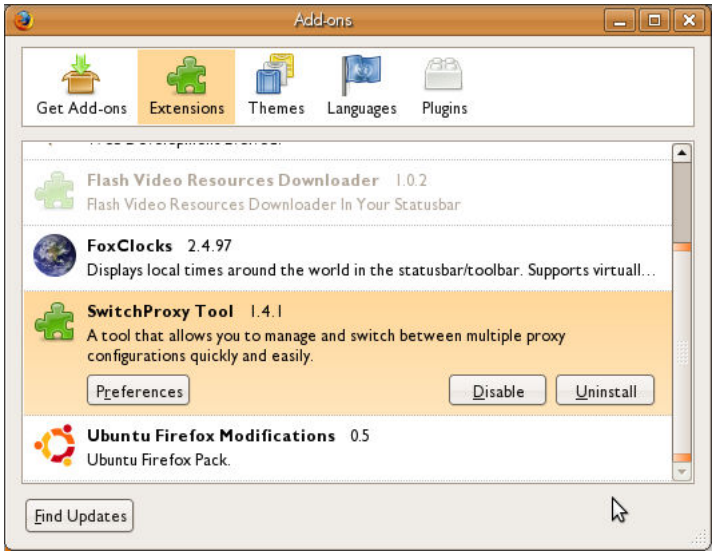
SwitchProxy te permite cambiar la configuración del proxy rápidamente de tu navegador **Firefox**. Puedes hacer esto con el propósito de usar un **proxy público** disponible a cualquiera, un **proxy privado** específico con el que hayas arreglado un acceso, o un **proxy local** proporcionado por una aplicación cliente como SSH. Usualmente, necesitarás tener un proxy de aplicaciones particular o una lista de proxies que deseas usar *antes* de usar SwitchProxy; pues SwitchProxy te ayuda a usar proxies, no a encontrarlos. SwitchProxy también soporta cargar una lista de varios proxies e intercambiarlos frecuentemente.

CONFIGURACIÓN DE SWITCHPROXY

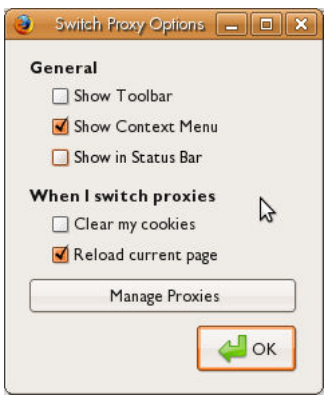
Para onfigurar SwitchProxy, necesitas abrir la ventana de configuración, accedida a través del menú "Herramientas" de Firefox:



Selecciona "Add-ons". Debe verse "SwitchProxy Tool" listada en el menú Add-ons. Clic en el enlace una vez para revelar el botón "Preferences":



Clic en el botón "Preferences" para mostrar el panel y configurar un conjunto simple de preferencias:



Las opciones en la sección **General** están relacionadas con donde se mostrará en el navegador la información de SwitchProxy.

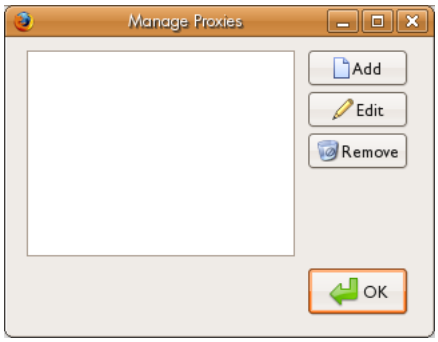
La segunda sección (**When I switch proxies**) es más importante, pues determina el comportamiento de SwitchProxy. Cuando intercambias los proxies, SwitchProxy pueden hacer unas cuantas cosas. Pueden automáticamente limpiar las cookies y puede recargar la página que estbas usando a través del nuevo proxy. Estos comportamientos son controlados por los controles de selección mostrados.

Debes seleccionar "Clear my cookies" cuando recargas un proxy, pues algunos sitios pueden ser capaces de asociar tu dirección IP previa con una cookie. Recargar la página automáticamente cuando cambias un proxy garantizará que no haya comunicación a través del proxy anterior.

Tú manejas el centro de la funcionalidad del SwitchProxy con el último botón, "Manejar Proxy". Si haces clic en este botón puedes adicionar, editar y eliminar proxies.

ADICIONANDO UN PROXY BÁSICO

Vamos a adicionar un proxy a SwitchProxy. Para ello, necesitamos primero seleccionar "Manage Proxies". La ventana "Manage Proxy" aparece:

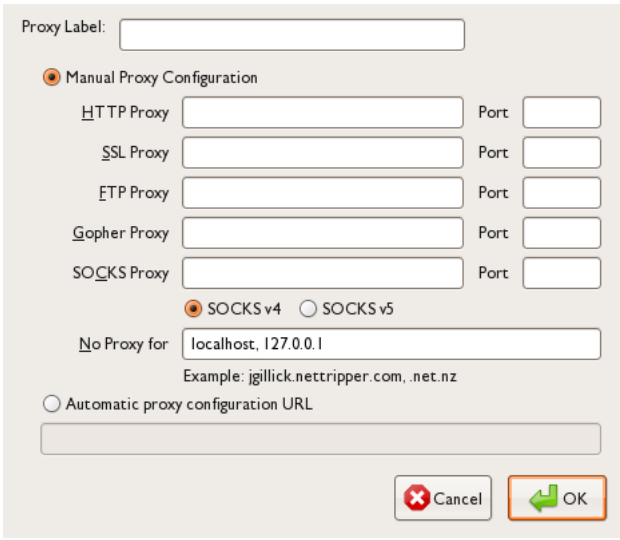


Si tienes otros proxies configurados dentro de SwitchProxy, ellos se mostrarán aquí. Para adicionar un nuevo proxy, clic "Add":

Seleccionando **Standard** te permite levantar un proxy para navegar por la Web, subir ficheros y otras acciones típicas. Esto es útil para acceder servidores que pueden estar bloqueados.

SwitchProxy también ofrece una opción **Anónimo**; sin embargo, esta opción está mal nombrada porque no garantiza anonimato. Simplemente permite el uso de proxies múltiples con intercambio frecuente entre ellos.

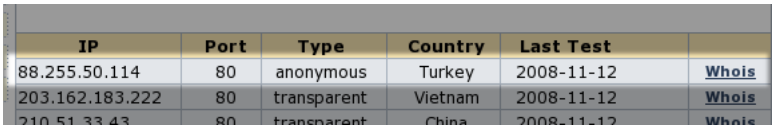
CONFIGURACIÓN DE PROXY ESTÁNDAR



Necesitas conocer las características del proxy que deseas adicionar. Esto puede ser mucha información dependiendo de qué tipo de acceso requieres y de la forma en que el proxy maneja ese tipo de acceso.

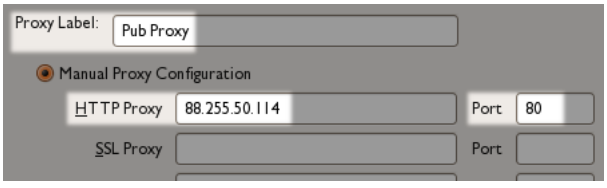
Idealmente, debes conocer las características de los proxies que deseas intentar usar con SwitchProxy. Con el propósito de hacer un ejemplo, buscaremos un proxy público del sitio web "Public Proxy Servers" (http://www.publicproxyservers.com) y lo adicionamos a SwitchProxy[7]. (No tenemos información acerca de quién opera estos proxies, así que realmente no sabemos cuán confiables son.)

Primero, en la página principal de los Servidores Proxy Públicos, seleccionamos "proxy list [1]" desde el panel de navegación de la izquierda (http://www.publicproxyservers.com/page1.html). Vemos una lista:



IP	Port	Type	Country	Last Test	
88.255.50.114	80	anonymous	Turkey	2008-11-12	Whois
203.162.183.222	80	transparent	Vietnam	2008-11-12	Whois
210.51.33.43	80	transparent	China	2008-11-12	Whois

Entramos la información de la IP (en este caso, 88.255.50.114) y el Puerto (en este caso, 80) de la lista en los primeros campos de la ventana de configuración estándar:

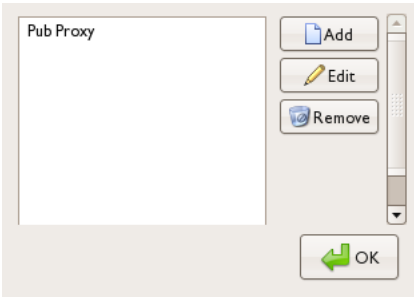


Puedes ponerle una etiqueta a cada proxy (nosotros usamos "Pub Proxy" en el ejemplo). Esto es todo lo que necesitas hacer para levantar este proxy. Si quieres levantar el proxy para otros tipos de acceso (SSL, FTP, Gopher o Socks), necesitarás continuar llenando los detalles en los otros campos. Usualmente el puerto y la IP son los mismos, así que se usará los mismos detalles para cada tipo de acceso requerido.

Nota:

1. Muchos proxies solo ofrecen acceso HTTP (navegación Web). Si deseas usar un proxy para otros tipos de Internet, puedes intentar ver si funciona.
2. Muchos proxies solo funcionan unas pocas horas, así que prepárate para intercambiar los proxies hasta encontrar uno que esté funcionando.
3. La configuración es solo usada por el navegador Firefox que usa el SwitchProxy[?]. Si abres otra ventana o usas otro tipo de aplicación (por ejemplo, un cliente FTP), no tiene acceso a la configuración de SwitchProxy.

Después de entrar los detalles, clic "OK" para salvar la configuración. La ventana "Manage Proxies" aparece de nuevo:



Clic "OK" de nuevo para cerrar esta ventana y salvar el nuevo Proxy a la lista. Es importante notar que estas configuraciones de Proxy no se activan hasta que active el Proxy a través de SwitchProxy.

ADICIONANDO UNA LISTA DE PROXIES PARA ALTERNAR AUTOMÁTICAMENTE

SwitchProxy también te permite crear una lista de proxies y fijar un intervalo para alternar automáticamente entre ellos. Esta opción confusamente hace referencia a configuración de Proxy "Anónima", aunque en realidad, no garantiza el anonimato.

Si decides usar esta característica, puedes fijar la lista de Proxy tú mismo. Esta será un fichero en texto plano con un formato como este:

193.147.162.166:3124 133.1.74.162:3124 130.75.87.83:3124 128.112.139.80:3128
128.112.139.80:3124 72.36.112.74:3124 199.26.254.65:3124

El formato de cada línea es simple.

Dirección IP: Número de puerto

Es importante colocar la coma entre los dos números y no incluir "http://" antes de la dirección IP del Proxy. Cada Proxy debe estar en una línea separada y el fichero debe ser un fichero texto (algunas veces llamados fichero .txt) y no un fichero Word (como Microsoft Word .doc o fichero de OpenOffcie[7] .odt).

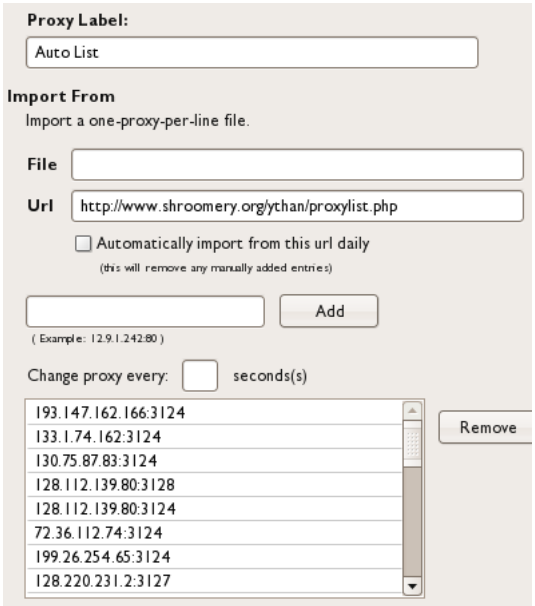
También hay servicios en línea que brindan listas de Proxy compatibles con esta característica. Aunque estos servicios son bloqueados en algunos lugares, puedes encontrar listas de Proxy públicos a través de una búsqueda Web.

Por ejemplo, una búsqueda rápida de "switchproxy anonymous Proxy lists" en Google te dirige a este sitio: http://www.shroomery.org/ythan/proxylist.php. Este servicio, ofrecido por alguien con interés en esta área (aparentemente un amateur, no un servicio comercial) toma una lista de Proxy desde XROXY (http://www.xroxy.com/proxylist.php?type=Anonymous) y formatea la lista de modo que SwitchProxy pueda usarla.

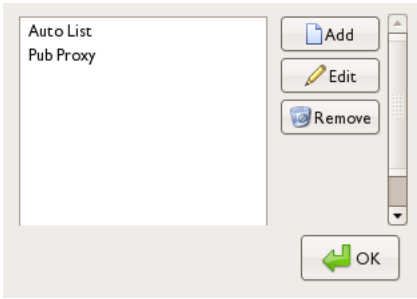
Puedes adicionar cualquiera de estas listas -- una lista creada por ti, o una lista en línea -- a la configuración de SwitchProxy como una lista de proxies "Anónimos". Para hacer esto, selecciona la opción "Anonymous" en lugar de la "Standard".

Clic "Next>>" y la ventana de configuración aparece:

Para usar la lista en línea, simplemente entra la Url de la lista en el campo Url y clic en "Load". Para adicionar una lista que hayas creado clic "Browse" próximo al campo File, selecciona el fichero del disco duro de tu PC y haz clic en "Load". No olvides ponerle un nombre a la lista (o "Label"). Por ejemplo, usando la lista en línea mencionada en el ejemplo anterior este es el resultado después de hacer clic en "Load":

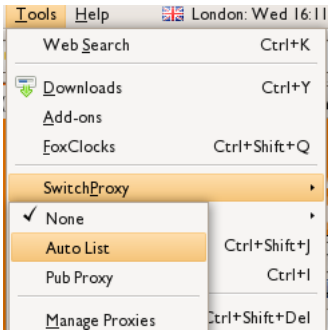


Ahora debes seleccionar el intervalo para circular a través de los proxies. Los intervalos para el intercambio automático en SwitchProxy se representan en segundos, así que si deseas fijar un intervalo de 3 minutos, debes poner "180" en el campo "Change Proxy every []". Después de hacer clic en "OK" la ventana se cierra y SwitchProxy salva la nueva lista de proxies:



USANDO SWITCHPROXY

Para usar los proxies que salvaste , solo haz clic en el menú "Tools" de Firefox:



Selecciona "SwitchProxy" y debes ver una lista de proxies que configuraste. Seleccionando uno de ellos activas el item Proxy. Para no usar Proxy selecciona "None".

DESVENTAJAS Y RIESGOS

Usando un Proxy de aplicación público no garantiza que estarás anónimo. Siempre que uses cualquier Proxy, estás confiando en que el operador del Proxy no revele o abuse de la información que tiene sobre ti o en el modo en el que usas el Proxy.

Tus comunicaciones con el Proxy pueden ser observadas también por el operador de red. Si visitas un sitio Web en diferentes ocasiones usando la misma computadora, por ejemplo, el sitio puede reconocerte como la misma persona usando mecanismos como cookies -- incluso si usas configuraciones de Proxy diferentes para cada visita.

Aunque Tor brinda un Proxy de aplicaciones local, no debes usar SwitchProxy para activar Tor. En su lugar usa Torbutton. Torbutton te protege contra una variedad de riesgos de privacidad potenciales (como DNS leaks) contra los que no te puede proteger SwitchProxy.

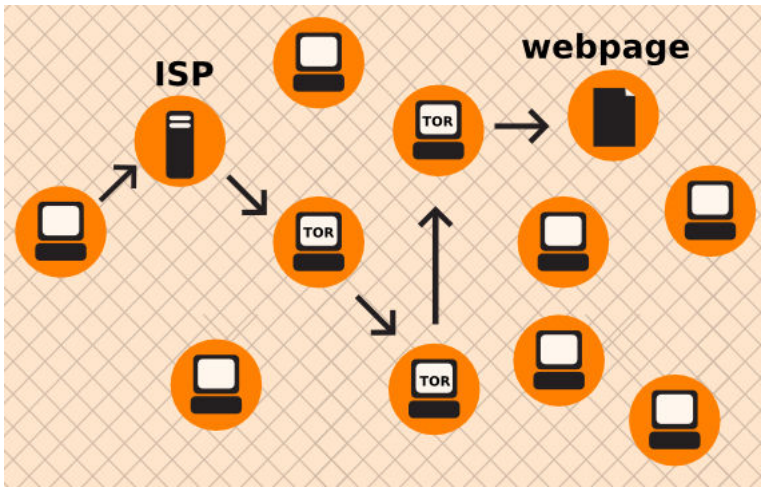
Autores : *ConfiguringSwitchProxy*
© adam hyde 2008, 2009
Modifications:
Alice Miller 2008

Ariel Viera 2009
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

Produced in FLOSS Manuals

19. TOR – THE ONION ROUTER

Tor (por sus siglas en inglés The Onion Router) es una red de servidores proxy muy sofisticada. Cuando usas Tor para acceder un sitio Web, tus comunicaciones son enrutadas aleatoriamente a través de una red de proxies independientes y voluntarios. Todo el tráfico entre los servidores Tor (o transmisores) está encriptado, y cada uno de los transmisores sabe solo la dirección IP de otros dos transmisores – el inmediato anterior y el posterior en la cadena.



Esto es muy difícil para que:

- Tu ISP sepa que es sitio Web estás accediendo o que información estás enviando
- El sitio web sepa quién eres (al menos, saber tu dirección IP)
- Cualquier transmisión independiente sepa quién eres y a dónde vas

¿QUÉ NECESITO PARA USAR LA RED TOR?

Para conectarse a Internet a través de la red Tor y usarla para alcanzar el **anonimato** y la **evasión**, necesitas instalar el cliente Tor en tu computadora. (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?

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) permitan el anonimato usando Tor, incluyendo:

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

Si se instala Tor desde **Tor Bundle, Browser Bundle** o **IM Browser Bundle**, Tor configura también un proxy http como frontend a la red de Tor. Esto permitirá que algunas aplicaciones que no soportan SOCKS trabajen con Tor. Si estas interesado principalmente en 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 usas Tor con un navegador Web. Ambas versiones de Tor pueden descargarse en: http://www.torproject.org/torbrowser/index.html.en.

VENTAJAS Y RIESGOS

Tor puede ser una herramienta efectiva para la evasión y la protección de la identidad. La encripción de Tor oculta el contenido de la comunicación de tu operador de red local, y disimula con quien te estás comunicando o que sitios Web estás viendo. Cuando se usan correctamente, provee protección de anonimato significantemente fuerte que un proxy simpl.

- 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 puedes usar con Tor tienen problemas que pueden comprometer el anonimato.
- Además, si no estás usando encripción adicional para proteger tu comunicación, tus datos serán desencriptados una vez que alcances el último nodo Tor en la cadena (llamada **nodo salida**). Esto significa que tus datos serán potencialmente visibles para el dueño del último nodo Tor y para el ISP entre el nodo y el sitio web destino.
  Los desarrolladores de Tor han pensado mucho acerca de estos y otros riesgos y ofrecen estas advertencias:

1. Tor no ofrece protección si no se usa correctamente. Lea la lista de advertencias aquí: http://www.torproject.org/download.html.en#Warning, y es necesario asegurarse de seguir las instrucciones para cada plataforma con cuidado: http://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://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ#RemainingAttacks
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 necesitas el anonimato.

Autores : *TorTheOnionRouter*
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Ben Weissmann 2009
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

20. USO DEL PAQUETE TOR DE NAVEGADOR

Tor Browser Bundle permite el uso de Tor en Windows sin necesidad de configurar un navegador Web. Incluso mejor, es una aplicación portable que se puede ejecutar desde una memoria flash USB, permitiendo ejecutarlo en cualquier computadora con Windows sin instalarlo en el disco duro de la computadora. Descargando Tor Browser Bundle

Se puede descargar desde el sitio torproject.org, como un fichero simple (13 MB) o una versión "split" (dividida) que consiste en múltiples ficheros de 1.4 MB cada uno. Si su conexión de Internet es lenta y poco confiable, la versión "split" debe ser mejor que tratar de descargar un fichero largo.

Si el sitio Web torproject.org está filtrado, se recomienda buscar en un motor de búsqueda "tor mirrors". Los resultados probablemente incluyan algunas direcciones alternativas para descargar Tor Browser Bundle.

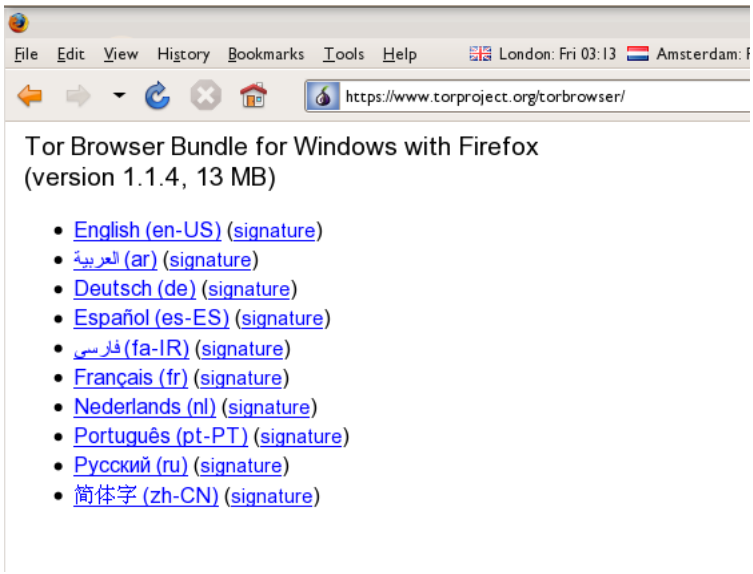
Alerta: Cuando se descarga Tor Bundle (versión plana o dividida en paquetes), se debe chequear las firmas de los ficheros, especialmente si descargas los ficheros desde un sitio espejo. Este paso asegura si los ficheros no han sido interferidos. Para aprender más sobre ficheros de firma y como chequearlos, leer https://wiki.torproject.org/noreply/TheOnionRouter/VerifyingSignatures

(También se puede descargar el programa GnuPG que se necesita para chequear las firmas aquí: http://www.gnupg.org/download/index.en.html#auto-ref-2)

Las instrucciones siguientes instrucciones se refieren a la instalación de Tor Browser en Microsoft Windows. Si se tiene un sistema operativo diferente, en el sitio torproject.org se encuentran los enlaces e instrucciones.

INSTALANDO DESDE UN FICHERO SIMPLE

1. En el navegador Web, entrar la URL para descargar Tor Browser: https://www.torproject.org/torbrowser/index.html.es



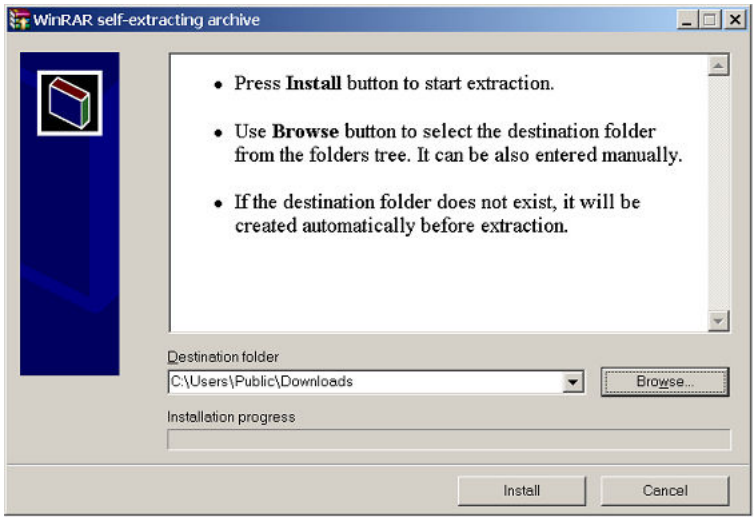
2. Clic en el enlace de tu idioma para descargar el fichero de instalación.
3. Doble-clic en el fichero .EXE que se descargó. Aparece una ventana "7-Zip self-extracting archive".

4. Seleccionar la carpeta donde se desea extraer los ficheros y clic en “Extract”.
   - **Nota**: Se puede extraer los ficheros directamente en una memoria USB si se desea usar Tor Browser en diferentes computadoras (por ejemplo en computadoras públicas en Cyber cafés).
5. Cuando se completa la extracción, chequee que el contenido de la carpeta coincida con la siguiente imagen:

6. Para limpiar todo, elimine el fichero .EXE que originalmente descargó.

INSTALANDO A PARTIR DE FICHEROS DIVIDIDOS

1. En el navegador Web, entrar la URL de la versión "split" de Tor Browser Bundle (https://www.torproject.org/torbrowser/split.html), clic en el enlace de tu idioma para obtener la página:
2. Clic cada fichero para descargarlo (uno termina en ".exe" y otros nueve terminan en ".rar"), uno después de otro, y sálvelos en una carpeta del disco duro.
3. Doble-clic la primera parte (el fichero que termina en ".exe"). Este ejecuta un programa que une todas las partes.



4. Seleccione una carpeta donde se desee instalar los ficheros, y 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, elimine todos los ficheros que descargó originalmente.

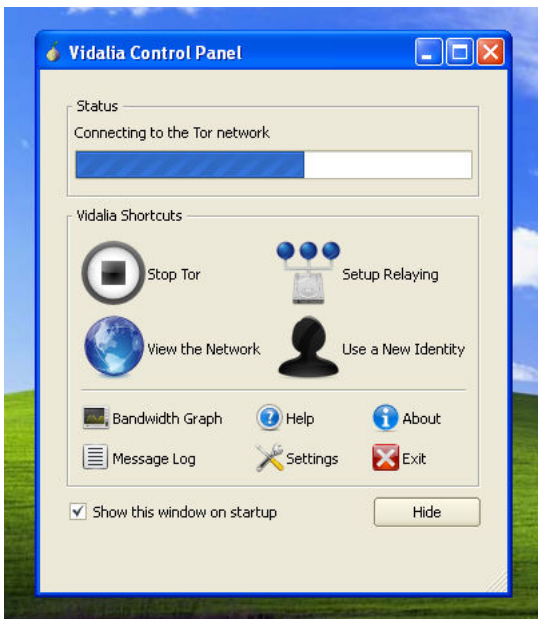
USANDO TOR BROWSER

Antes de comenzar:

- Cierre Firefox. Si Firefox está instalado en la computadora, asegúrese de que no se está ejecutando.
- Cierre Tor. Si Tor está instalado en la computadora, asegúrese de que no se está ejecutando.

Activar 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[7] 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 el System Try en la esquina derecha inferior de la pantalla:

NAVEGANDO EN LA WEB USANDO TOR

Intenta ver algunos sitios Web, y ve como se muestran. Los sitios se cargan más lentos de 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 estás usando Tor.

Si ves este mensaje, cierra Firefox y Tor Browser y repite los pasos anteriores. Se puede chequear esto para asegurarse de que se está usando tor, en cualquier momento haciendo clic en el botón marcador con la etiqueta "TorCheck at Xenobite..." en la barra de tarea de Firefox.

Si Firefox no se activa, otra instancia del navegador puede interferir con el Tor Browser. Para arreglar esto:

1. Abrir la ventana del Task Manager. Esto depende de cómo está configurada la computadora. En la mayoría de los sistemas, haciendo clic derecho en la Barra de Tarea y clic en “Task Manager”.
2. Clic en el tab “Processes”.
3. Buscar un proceso en la lista llamado “firefox.exe”.
4. Si encuentras uno, selecciona la entrada y clic “End Process”.
5. Repetir los pasos anteriores para activar Tor Browser.

Si Tor Browser aún no funciona después de dos o tres intentos, Tor puede estar parciamente bloqueado por tu ISP y debes intentar entonces con la característica de Tor bridge (puente).

ALTERNATIVAS

Hay otros dos proyectos que se empaquetan con Tor y un navegador:

- XeroBank, un paquete de Tor con Firefox (http://xerobank.com/xB_Browser.php)
- OperaTor, un paquete de Tor con Opera (http://archetwist.com/en/opera/operator)

Autores : *UsingTheTorBrowserBundle*

Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

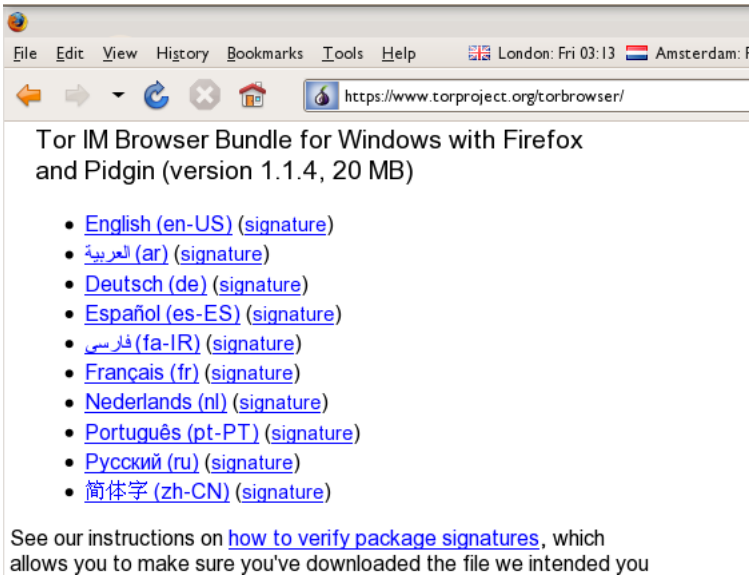
21. USO DEL PAQUETE TOR DE MI

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

Puedes aprender más acerca de Pidgin aquí: http://www.pidgin.im/

DESCARGA TOR IM BROWSER BUNDLE

Puedes descargar el Tor IM Browser Bundle directamente desde el sitio Web Tor (20MB) en https://www.torproject.org/torbrowser/



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

Si el sitio Web torproject.org está filtrado, se recomienda buscar en un motor de búsqueda "tor mirrors". Los resultados probablemente incluyan algunas direcciones alternativas para descargar Tor Browser Bundle.

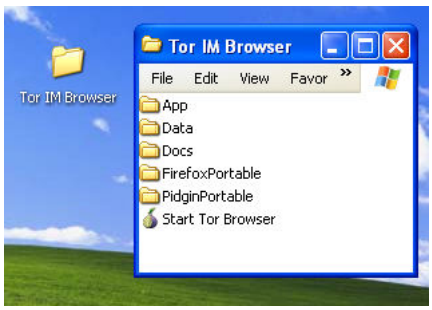
Advertencia: Cuando se descarga Tor Bundle (versión plana o dividida en paquetes), se debe chequear las firmas de los ficheros, especialmente si descargas los ficheros desde un sitio espejo. Este paso asegura si los ficheros no han sido interferidos. Para aprender más sobre ficheros de firma y como chequearlos, leer https://wiki.torproject.org/noreply/TheOnionRouter/VerifyingSignatures

(También se puede descargar el programa GnuPG[7] que se necesita para chequear las firmas aquí: http://www.gnupg.org/download/index.en.html#auto-ref-2)

AUTO-EXTRAER EL ARCHIVO

- Para empezar, doble-clic en el fichero .EXE que descargaste.
  Debes ver la ventana siguiente:

- Selecciona la carpeta en la cual se extraerán los ficheros. Sino estás seguro deja el valor por defecto como está. Clic "Extract".
  Nota: Se puede extraer los ficheros directamente en una memoria USB si se desea usar Tor Browser en diferentes computadoras (por ejemplo en computadoras públicas en Cyber cafés).
- Cuando se completa la extracción, abrir la carpeta recién creada y chequea que se vea como la siguiente imagen (Nota la carpeta "PidginPortable"):



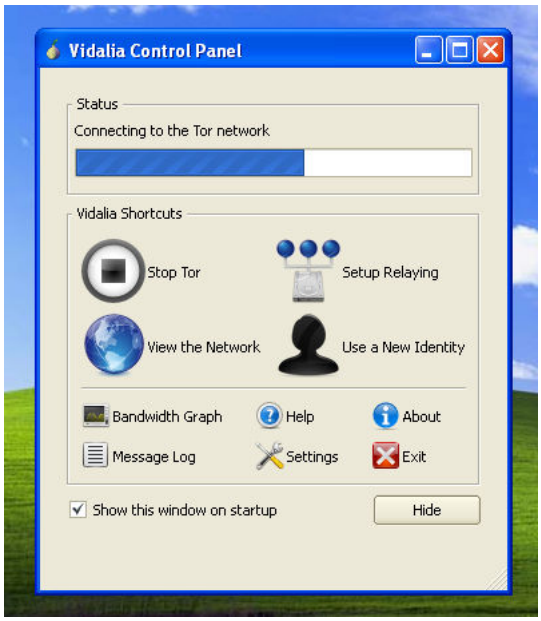
- Puedes borrar el fichero ".exe" que originalmente descargaste (o los distintos ficheros ".rar" y ".exe" si usaste la versión "split").

USANDO TOR IM BROWSER BUNDLE

ANTES DE COMENZAR:

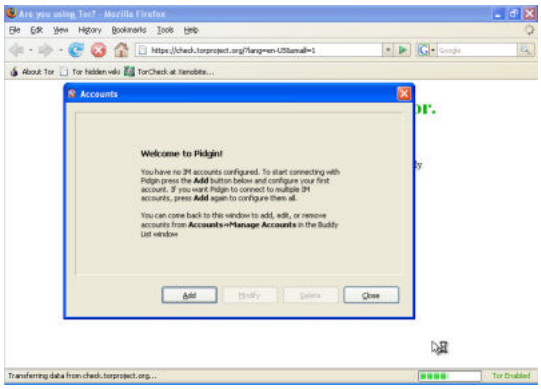
- **Cierra Firefox.** Si Firefox está instalado en la computadora, asegúrate que no esté ejecutándose.

- **Cierra Tor.** Si Tor está instalado en la computadora, asegúrate que no esté ejecutándose. Activa 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.

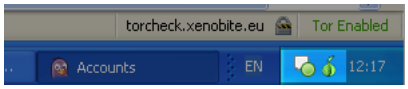


Cuando se establece una conexión:

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

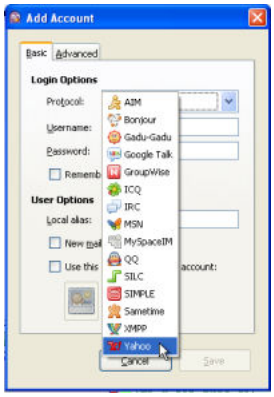


También se verá un ícono de Tor (una cebolla verde si estás conectado) y un ícono Pidgin aparecer en el System Try en la esquina derecha inferior de la pantalla:



CONFIGURANDO LA CUENTA DE IM EN PIDGIN

Puedes levantar tu 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):



Mas información acerca de Pidgin en este enlace:
http://developer.pidgin.im/wiki/Using%20Pidgin#GettingStarted

SI ESTO NO FUNCIONA

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

- **Salir de Vidalia y Pidgin** (vea abajo para más detalle).

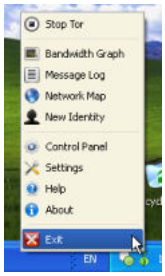
- **Reactive Tor IM Browser** siguiendo los pasos más abajo ("Usando Tor IM Browser Bundle").

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

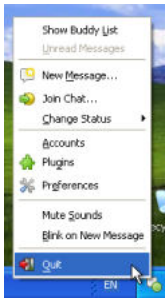
SALIR DE TOR IM BROWSER

Para salir de Tor IM Browser necesitas:

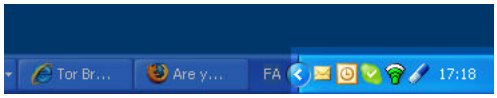
- **Salir de Vidalia** haciendo clic derecho en el ícono de la cebolla del System try y seleccionar "Exit" en el menú contextual de Vidalia.



- **Salir de Pidgin** haciendo clic derecho en el ícono Pidgin en el System Try y seleccione "Quit" en el menú contextual de Pidgin.



Cuando el ícono cebolla de Vidalia y el ícono de Pidgin hayan desaparecido del System Try de Windows en la esquina inferior derecha de la pantalla, Tor IM Browser está cerrado.



Autores : *UsingTorIMBrowserBundle*
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008, 2009

Ariel Viera 2009
Alice Miller 2008
Freerk Ohling 2008
Sahal Ansari 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

22. USANDO TOR CON PUENTES

Si sospechas que el acceso a la red Tor está bloqueado, quizás quieras usar la característica Tor de puente. El puente fue creado específicamente para ayudar a las personas a usar Tor que lo tienen bloqueado. (Debes haber descargado e instalado el programa Tor para usar un puente.)

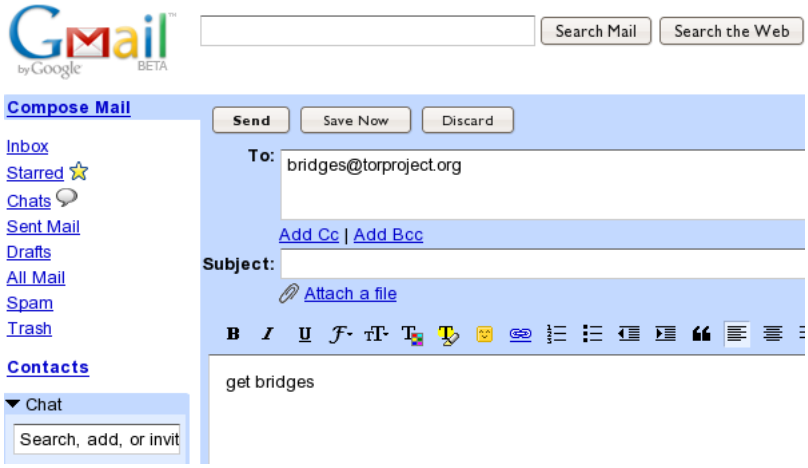
¿QUÉ ES UN PUENTE?

Bridge relays (o "puentes") son transmisores que no están listados en el directorio público de Tor. Esta es una medida deliberada para evitar que estos transmisores sean bloqueados.

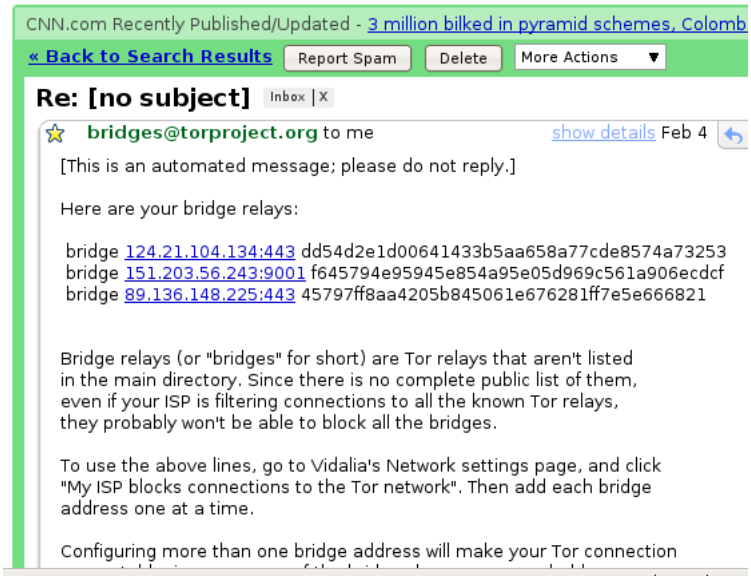
Incluso si tu ISP está filtrando las conexiones a todos los transmisores Tor públicos conocidos, quizás no es capaz de bloquear todos los puentes.

¿DÓNDE ENCUENTRO LOS PUENTES?

Para usar un puente, necesitas localizar uno y adicionar la información en tu configuración de red. Enviar un correo electrónico desde una cuenta **Gmail** a **bridges@torproject.org** con la línea **"get bridges"** en el cuerpo del correo.



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



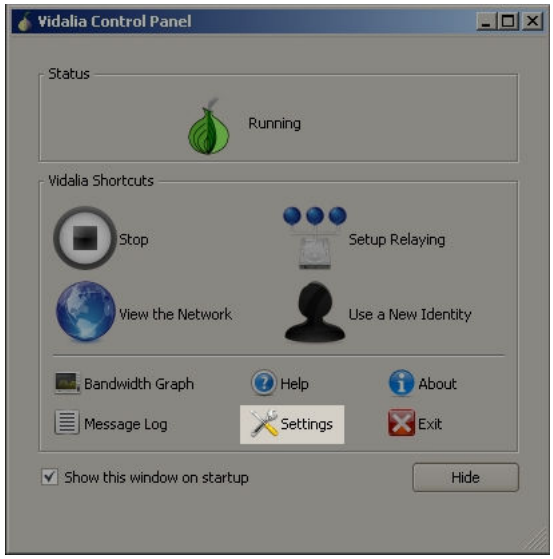
Notas importantes:

1. Debes usar una cuenta Gmail para enviar la petición. Si torproject.org acepta solicitudes desde otras cuentas de correo, un atacante puede fácilmente crear un montón de direcciones y conocer rápidamente todos los puentes. Si aún no tienes cuenta de Gmail, crear una solo toma unos pocos minutos.
2. Generalmente es recomendable usar Gmail con una conexión segura SSL en "https://mail.google.com", en lugar de la URL desencriptada http://mail.google. En la página de configuración de Gmail puedes determinar que HTTPS sea por defecto, en caso de que olvides usar el prefijo https.
3. Si estás en una conexión a Internet lenta puedes usar la URL https://mail.google.com/mail/h/ para un acceso directo a la versión básica HTML de Gmail.

ACTIVAR EL PUENTEO Y ENTRAR LA INFORMACIÓN DE PUENTE

Después de obtener las direcciones de algunos puentes, se debe configurar Tor cualquier dirección de puente que pretendes usar:

1. Abre el panel de control Tor (Vidalia).



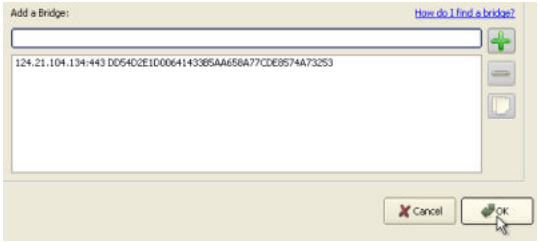
2. Clic “Settings”. Una ventana “Settings” se abre.

3. Clic “Network”.
4. Selecciona "My Firewall only lets me connect to certain ports" y "My ISP blocks Connections to the Tor network".

5. Entra la información de la URL del puente que recibiste por correo en el campo “Add a Bridge”.

6. Clic en “+” verde que aparece en el lado derecho del campo “Add a Bridge”. La URL se adiciona a la caja de abajo.

7. Clic "OK" al pié de la ventana para validar las nuevas configuraciones.



8. In the Tor control panel, stop and restart Tor to use your new settings.

Nota:

Adiciona tantas direcciones de puentes como puedas. Puentes adicionales aumentan la fiabilidad. Un puente es suficiente para alcanzar la red Tor, sin embargo, si solo tienes un puente y este es bloqueado o deja de operar, se cortará tu conexión a la red Tor hasta que adiciones nuevos puentes.

Para adicionar más puentes en la configuración de tu red, repite los pasos anteriores con la información en los puentes adicionales que recibiste del mensaje de correo de bridges@torproject.org.

Autores: *Torusingbridges*
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
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

Produced in FLOSS Manuals

23. ACERCA DE JONDO

JonDo es una herramienta proxy similar a Tor la cual puede usarse para traspasar la censura de Internet. Fue inventada en el año 2000 como un proyecto universitario alemán llamado Java Anon Proxy (JAP) y ahora ofrece servicios comerciales y gratis. Los servidores gratis solo ofrecen la velocidad de un modem analógico mientras que el servicio comercial ofrece altas velocidades a 10 USD por 1 GB de tráfico. El cliente Java se ejecuta en Linux, Mac OS y Windows.
Como Tor, el propósito principal de JonDo es proveer anonimato para los usuarios cuando visitan sitios Web. Como Tor, funciona enviando tráfico a través de varios servidores independientes.

INSTALACIÓN

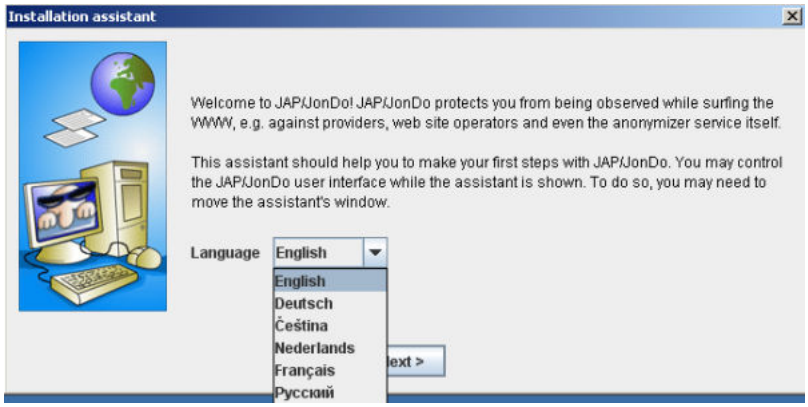
PARA USAR LA RED JonDo necesitamos descargar el cliente JonDo para nuestro sistema operativo desde https://www.jondos.de/en/download. Para Llinux y Mac OS X hay una opción simple de descarga (6 MB).
Para Windows sin embargo, hay tres posibilidades diferentes:

- El instalador de ventana estándar que trae Java incluido (cerca de 15MB)·
- Una versión PortableApps también con Java incluido que puede ejecutarse desde una memoria flash USB para usar en Cyber Cafés o en otras computadoras compartidas (cerca de 20MB)
- De la tres opciones el mínimo necesario para ejecutar JonDo sin el instalador y sin Java: Consiste en los ficheros http://anon.inf.tu-dresden.de/develop/jap.exe, http://anon.inf.tu-dresden.de/develop/japdll.dll y http://anon.inf.tu-dresden.de/jap/JAP.jar (en total cerca de 6MB).

Seleccionemos una descarga en dependencia de nuestra experiencia, propósitos y la velocidad de nuestra conexión a Internet. Para instalar el cliente JonDo solo hay que hacer clic en el fichero descargado y seguir las instrucciones.

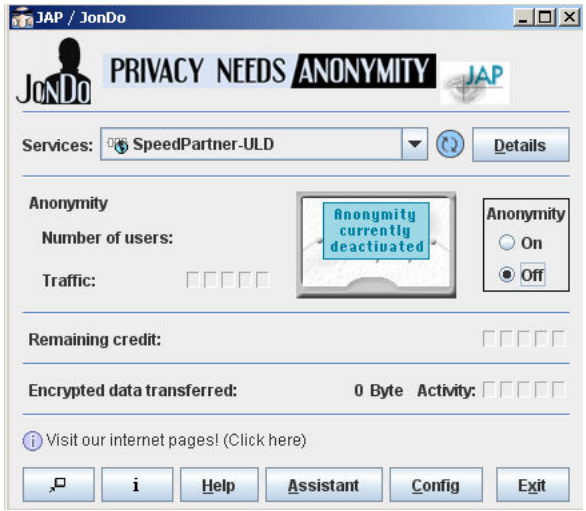
CONFIGURACIÓN Y USO

Cuando iniciamos JonDo aparece una ventana donde puedes seleccionar entre los idiomas Inglés, Alemán, Checo, Holandés, Francés y Ruso.

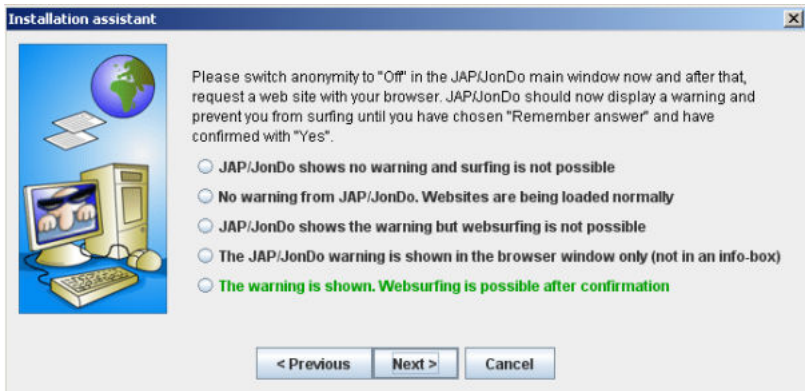


En la próxima pantalla, se nos notificará que tienemos que configurar el navegador Web para usar la herramienta proxy JonDo. Démos clic en el nombre de tu navegador y sigue las instrucciones que recibes.

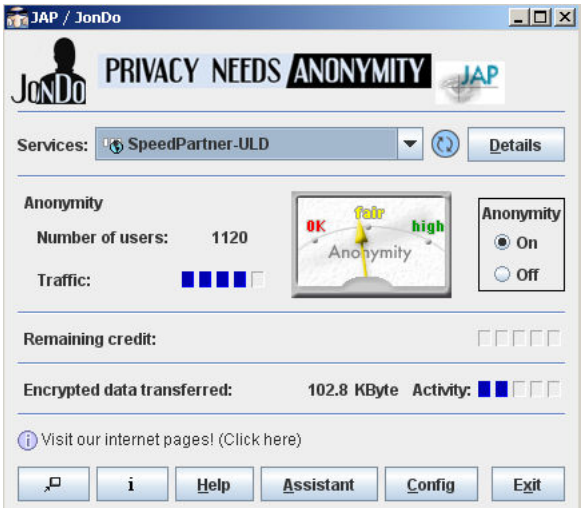
Seguidamente probaremos si el navegador está configurado correctamente. Pongámos "Anonymity" en "Off" en la ventana principal de JonDo y abramos un sitio Web en el navegador que acabamos de configurar.



Si JonDo muestra una advertencia y escogemos "Yes" para ver el sitio todo está configurado correctamente y podemos escoger " *The warning is shown. Websurfing is possible after confirmation* ". Si alguna de las otras descripciones se aplica a nuestro caso, escojámosla y el asistente de instalación nos dará mas información sobre cómo resolver este problema.

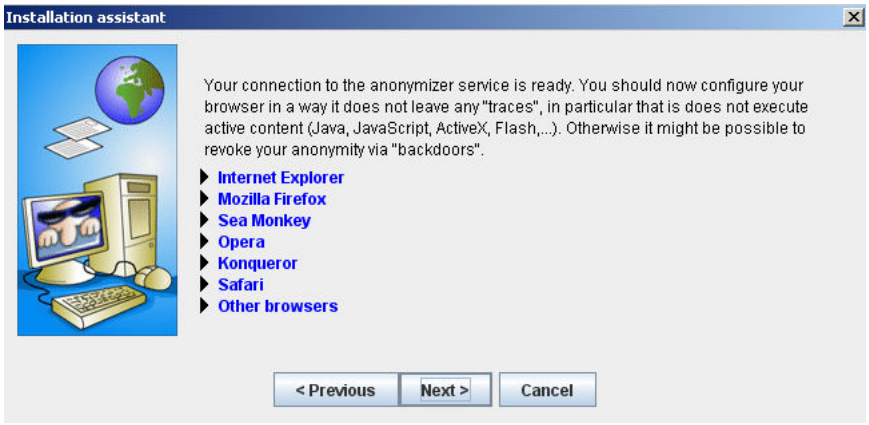


Ahora configuremos JonDo apropiadamente: tornémos "anonymity" a "On" en la ventana principal de JonDo y de abrámos un sitio web aleatorio con el browser que hemos configurado.

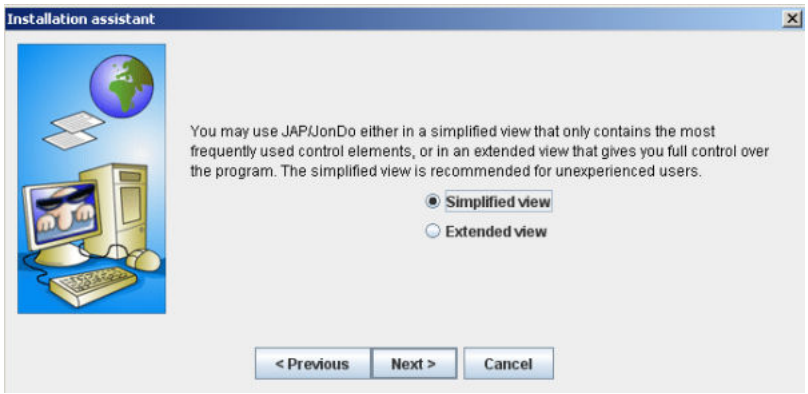


Si el sitio Web carga, todo está bien y podemos hacer clic " *Connection established, websurfing is fine* ". Si otra descripción se aplica la seleccionamos y el asistente de la instalación ayudará a solucionar el problema.

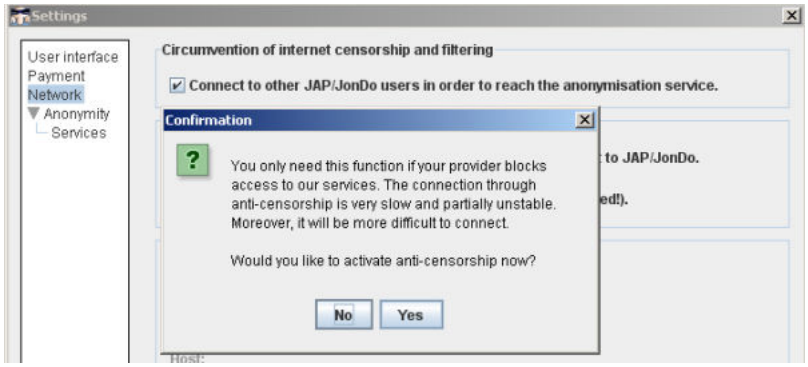
Ahora la configuración está casi completa. Estaremos navegando a través de la red JonDo. Sin embargo, hay que configurar el navegador Web para que no deje escapar ninguna información. Esto es explicado cuando damos clic en el nombre del navegador Web.



Ahora seleccionamos la opción que deseas ver en el cliente JonDo basado en tu experiencia con la computadora. Usuarios inexpertos deben seleccionar "Simplified view".



Si los servidores estándares JonDo están bloqueados en nuestro país, podemos intentar la opción anti-censorship. Demos clic en *"Config"* en la ventana principal de JonDo y seleccionemos el tabulador *"network* ". Ahí demos clic en"Connect to other JAP/JonDo users *in order to reach the anonymization service* ". Después de leer la advertencia confirmemos haciendo clic en *"Yes"*.



Autores : *UsingJonDo*

Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

TUNNELLING

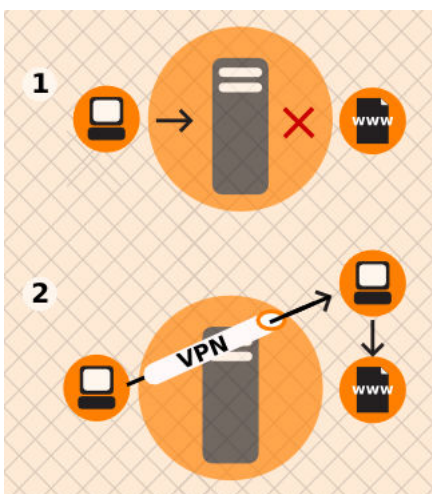
24. QUE ES UNA VPN?
25. OPENVPN
26. TUNELES SSH
27. PROXIS SOCKS

24. ¿QUÉ SON VPN Y TUNNELING?

VPN (virtual private network) y **tunneling** son técnicas que te permiten encriptar los datos de conexiones entre otra computadora y tú. Esta computadora puede pertenecer a tu organización, un contacto confiable o un servicio VPN. Tunneling encapsula un flujo específico de datos con un protocolo encriptado, haciendo que todo lo que pase por el túnel no se pueda leer por nadie a lo largo del camino. Los VPNs son comúnmente usados por corporaciones para permitir a los empleados que necesitan acceder a información financiera sensible para acceder a sistemas de computadoras de la compañía desde su casa o desde una locación remota en Intenet.

Usando un VPN u otro tipo de túnel para encriptar la información puede ser una buena forma de asegurar que no será vista por nadie excepto tú y las personas en quien confías. Tiene el efecto adicional de hacer ver todo el tráfico similar a la vista de un curioso o de un sistema que intenta bloquear tu tráfico. Es poco probable que ésta tecnología sea bloqueada, ya que muchas compañías la utilizan.

Estas técnicas crean un túnel desde tu computadora hacia otra computadora de algún lugar en Internet. Tus datos pueden viajar a través de este túnel y continuar a un destino final en la Web. La integridad y privacidad del tráfico dentro del túnel son protegidas por encripción.



Si el túnel termina fuera del área donde Internet está restringido, este puede ser un modo efectivo de evasión, pues el servidor o la entidad de filtrado ve solo datos encriptados, y no tiene modo de conocer que datos están pasando a través del túnel.

Es importante notar que los datos solo se encriptan hasta el final del túnel, y después viaja desencriptada hasta su destino final. Si, por ejemplo, si levantamos un túnel a un proveedor VPN, y después solicitamos la página Web news.bbc.co.uk a través de un túnel, los datos viajarán cifrados desde nuestra computadora a la computadora de nuestro proveedor de VPN, pero a partir de ahí viajarán desencriptados hasta los servidores de la BBC, como el tráfico normal de Internet. Esto significa que el proveedor de VPN, la BBC y cualquiera con control sobre un sistema entre estos dos servidores, en teoría, serán capaces de ver la información que solicitamos.

TUNNELING

La diferencia principal entre una conexión VPN y un túnel es que un sistema VPN está configurado de forma que encripta toda la información desde tu computadora hasta Internet, mientras un túnel solo encripta tráfico desde aplicaciones específicas, incluso basado en números de puerto que usan o requiriendo que especifiques qué túnel usar para cada aplicación. A diferencia de un VPN, los túneles requieren que cada aplicación, como un navegador Web, cliente de correo electrónico o programa de Mensajería Instantánea que necesita usar el túnel encriptado, configure individualmente un túnel. Significativamente, no todas las aplicaciones son capaces de pasar a través de tipos comunes de túneles. Muchos sistemas VoIP (Voices over IP), por ejemplo, usan el protocolo UDP, el cual no se soporta en muchos sistemas de túnel comunes. Además, algunas aplicaciones comunes tales como el navegador web Opera no tienen incorporado el soporte para proxies SOCKS que es el tipo más común de software de túnel. En este caso debes usar una aplicación extra como FreeCap para Windows (http://www.freecap.ru/eng/) o tsocks para Linux (http://tsocks.sourceforge.net/).

Una vez que el túnel está establecido y las aplicaciones han sido configuradas, estas se ejecutarán a través de túnel encriptado a la computadora con el software de túnel, quien reenvía tu petición y responde de forma transparente. Los usuarios con contactos en un país no filtrado pueden levantar un servicio de túnel mientras aquellos sin contactos pueden adquirir servicios comerciales de túnel, usualmente con suscripción mensual por 5 USD el mes (usualmente requieren una tarjeta de crédito).

Varios servicios gratis de túnel están disponibles. Cuando se usa servicios de túnel los usuarios deben notar que a menudo se incluyen avisos. Las solicitudes de avisos publicitarios algunas veces se transmiten a través de solicitudes HTTP en texto plano sin encriptar, y pueden ser interceptadas por cualquier intermediario que puede entonces determinar que el usuario está usando un servicio de túnel. Además, muchos servicios de túnel confían en el uso de proxies SOCKS los que pueden dejar escapar el nombre de dominio de las solicitudes. Algunos sistemas de túnel comerciales que brindan un servicio gratis (lento) son:

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

VPN

A diferencia de los túneles, los sistemas VPN transportan todos las datos sobre redes encriptadas, incluyendo VoIP (Voice over IP) y comunicaciones desde aplicaciones sin soporte incorporado para SOCKS. Una vez que se levanta el VPN son más fáciles que los túneles, pero son más complicados de configurar que la mayoría de las aplicaciones.

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 para cada estándar con software que tiene varias otras características.

- Mientras PPTP es conocida por usar encripción 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. Las aplicaciones no necesitan ser diseñadas para usar IPSec, mientras que SSL/TLS u otras funciones de capas superiores de protocolo deben ser incorporadas a una aplicación.

Los VPN son frecuentemente usados por compañías y organizaciones como canales de comunicación privados para conectarse de forma segura sobre Internet. Por su popularidad hay muchos proveedores de servicios VPN, los que permiten adquirir acceso a servicios VPN por un pago. Usar un servicio como este requiere que confíes en los dueños del servicio, pero proveen un método simple y conveniente de sobrepasar el filtrado de Internet por un pago mensual de 5 a 10 USD. Hay una lista de proveedores VPN disponibles en: http://en.cship.org/wiki/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.

VENTAJAS

Las aplicaciones de túnel y VPN brindan transferencia de datos encriptada. Ellos generalmente tienen la habilidad asegurar muchas funciones de proxy, no solo tráfico web. Así que es la forma más segura de evadir la censura de Internet. Una vez que se configuran son muy fáciles de usar.

Las aplicaciones de túnel y VPN son más convenientes 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 de negocio común que no tiende a ser bloqueada.

Algunos, no todos los servicios comerciales de túnel y VPN hacen publicidad de su anonimato, los que levantan servicios que no se pueden alcanzar. Esta protección de anonimato bastante efectiva si el operador de túnel o VPN comercial es confiable.

DESVENTAJAS Y RIESGOS

Servicios comerciales de túnel y 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 quien 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 estás haciendo a menos que uses alguna encripción adicional para tus comunicaciones; cuando no usas encripción adicional, debes confiar en que el operador de VPN o túnel no abusará del acceso a tus comunicaciones.

Autores : *WhatIsVPN*
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008

Ariel Viera 2009
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

25. USANDO 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 encripción que se usa cuando se visita un sitio Web seguro cuando la URL empieza con https.

OpenVPN no es apropiado para uso temporal en Cyber cafés o en cualquier lugar con computadoras compartidas donde no puedes instalar ningún programa.

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 firewall 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 puedes adquirir acceso a un servidor OpenVPN por un pago de 5 a 10 USD por mes. Estos proveedores te ayudarán a instalar y configurar OpenVPN en tu computadora. Una lista de estos proveedores comerciales están disponibles 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.

INFORMACIONES PARA CONFIGURAR UN OPENVPN

Para configurar un servidor OpenVPN y un cliente sigue la documentación que brinda OpenVPN (http://openvpn.net/index.php/documentation/howto.html). Si deseas 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 parar openVPN cuando se requiera, y también te permite configurar OpenVPN para usar un proxy HTTP para entrar a Internet. Para descargar la GUI vaya a: http://openvpn.se/.

Para configurar OpenVPN para usar un servidor proxy en Linux o Mac OS X, lee la sección relativa a ello en el sitio Web: (http://openvpn.net/index.php/documentation/howto.html#http).

Server

- Cuando tengas que elegir entre enrutar o puentear, no hay ventaja adicional en configurar puente cuando tus clientes solo desean usarlo para evadir la censura de Internet. Selecciona enrutar.
- Presta 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 te ayudará a visitar páginas bloqueadas. (http://openvpn.net/index.php/documentation/howto.html#redirect).
- Si la computadora del cliente está detrás de un firewall 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 de firewall 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, reemplaza “proto udp” con “proto tcp” y “puerto 1194” con “puerto 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.

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 usados. Hay que recordar que el tráfico solo está encriptado hasta el servidor OpenVPN, a partir de él pasa desencriptado 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.

Produced in FLOSS Manuals

26. SSH TUNNELING

SSH (Secure Shell), es un protocolo estándar que encripta las comunicaciones entre la computadora y el servidor. La encripción 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 encriptados y trabajar como un cliente Proxy genérico. Los censores 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.

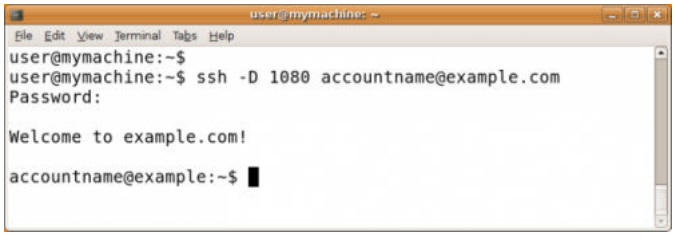
Usar SSH requiere de una cuenta en un servidor, generalmente un servidor Linux o Unix. Para evadir la censura este servidor necesita tener acceso sin restricciones a Internet e, idealmente ser operado por un contacto confiable. Algunas compañías también venden cuentas en sus servidores, y muchos sitios de hosting 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 vende 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 encriptadas para conectarse con Internet sin restricciones. En este ejemplo, solo describiremos este uso de SSH. Los pasos a continuación configuran un Proxy SOCKS en un puerto local 1080 en la computadora usando una cuenta shell llamada accountname@example.com.

LÍNEA DE COMANDO DE LINUX/UNIX Y MAC OS (CON OPENSSH)

OpenSSH está disponible en http://www.openssh.com/, pero viene pre instalado en Linux/Unix y Mac OS. Se necesita una cuenta shell en un servidor con conexiones a Internet sin restricciones.



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:

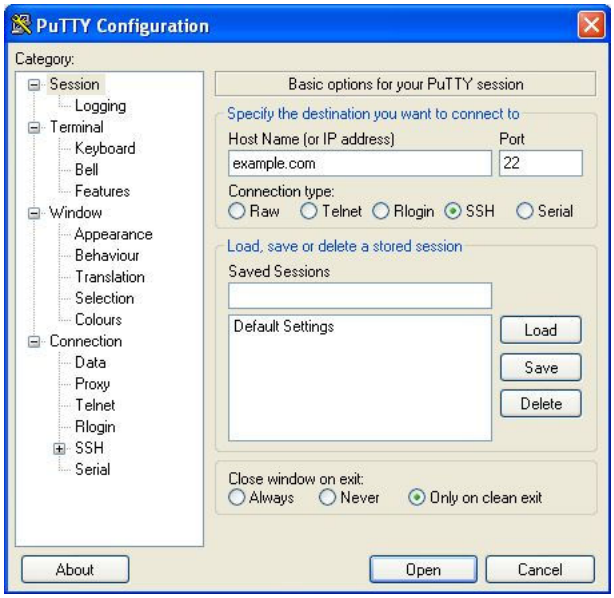
ssh -D puertolocal nombredecuenta@nombredeservidor

Se pedirá la contraseña y se entrará en el servidor. Con el uso de la opción –D, se creará un Proxy SOCKS que existirá mientras se esté conectado al servidor. Después de verifica la llave del host y se configuran las aplicaciones.

INTERFAZ DE USUARIO GRÁFICA PARA WINDOWS (CON PUTTY)

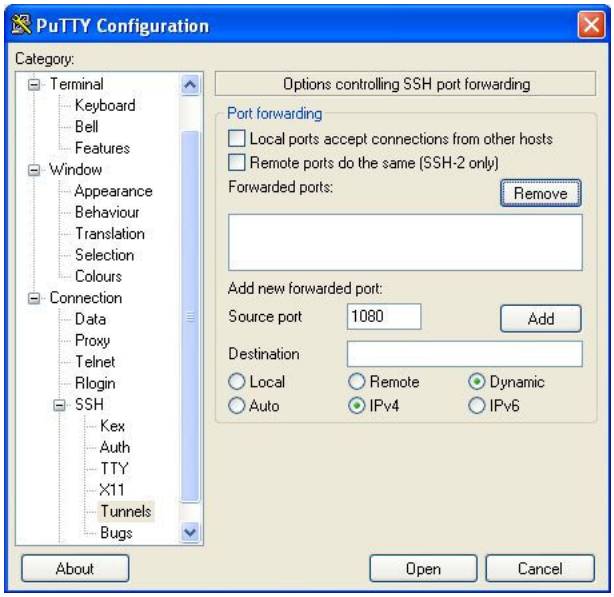
PuTTY está disponible en: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html. Podemos salvar el programa putty.exe en el disco duro para usos futuros, o ejecutarlo directamente desde el sitio Web (a menudo, esto es posible en una computadora compartida o con acceso público como las de las librerías o Cyber cafés).

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.

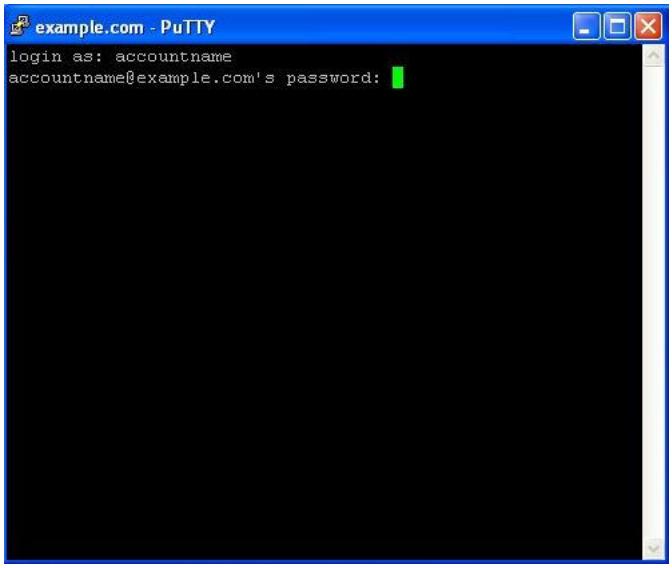


Después en la lista, Category, seleccionamos Connection, después SSH, y después Tunnels.

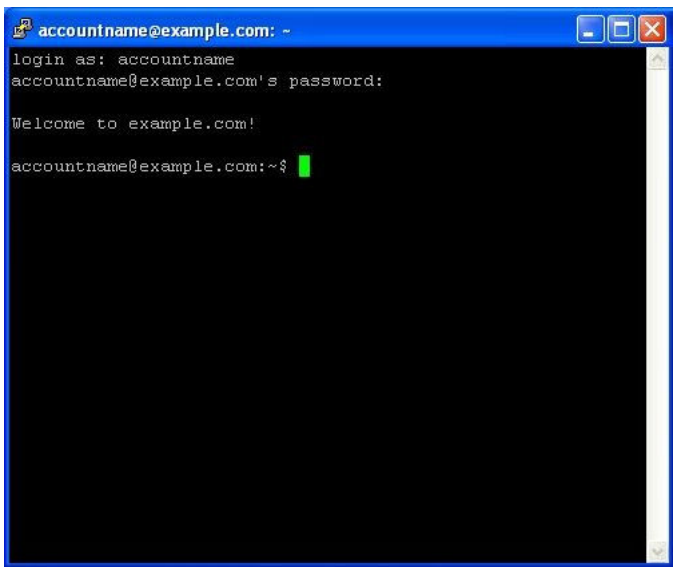
Entramos 1080 como Source port, y seleccionamos las cajas "Dynamic" y "IPv4".



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 ususario y la contraseña.



Entramos la información y accederemos al servidor recibiendo una ventana de línea de comando del servidor. Entonces queda establecido el Proxy SOCKS.



VERIFICACIÓN DE LLAVE DE HOST

La primera vez que nos conectamos a un servidor, debemos confirmar la firma digital llave de ese servidor. La firma digital llave es una secuencia larga de letras y números (hexadecimales) como 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 llave es una medida de seguridad que permite confirmar que estamos comunicando con el servidor que pensamos, y que la conexión encriptada no puede ser interceptada. (SSH no brinda un medio de verificar esto automáticamente. Para obtener el beneficio de este mecanismo, debemos 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 algunos, 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.

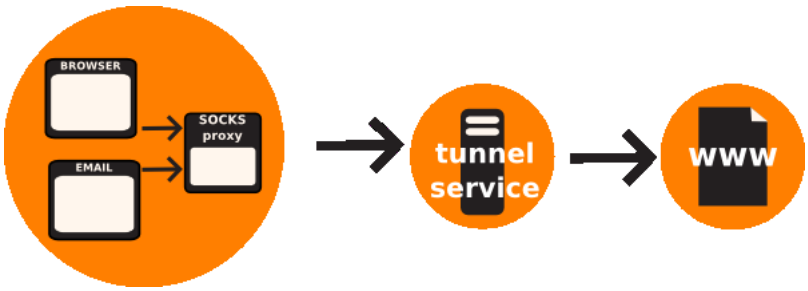
CONFIGURANDO APLICACIONES PARA USAR EL PROXY

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.

27. USANDO PROXIES SOCKS

Una variedad de proxies pueden aprovechar las ventajas de un Proxy SOCKS para evador el filtrado u otras restricciones – no solo los navegadores Web, sino otras aplicaciones como las de mensajería instantánea y de correo electrónico.



Podemos pensar en los proxies SOCKS como una versión de proxies HTTP más avanzados, que permiten diferentes tipos de tráfico Internet desde diferentes protocolos que se envían a través de un túnel y de esa forma traspasan el bloqueo.

Aunque los proxies SOCKS públicos existen, en muchos casos se ejecutarán en la computadora de forma local, y será facilitado 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 proia 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 aprovechen las ventajas del programa de evasión. Algunas herramientas que trabajan de esta forma incluyen a Tor, Your-Freedom y túneles SSH configurados con PuTTY.

Local proxy enthusiast T-shirt(get it?)

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

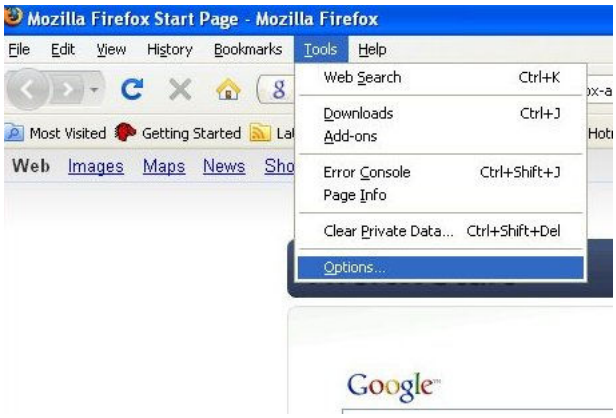
CONFIGURANDO LAS APLICACIONES

En la mayoría de los casos en los que se configuran proxies SOCKS se hace muy parecido a los proxies HTTP. Las aplicaciones que tienen soporte para proxies SOCKS tienen una entrada separada en el menú o diálogo de configuración donde se configuran los proxies HTTP para configurar proxies 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 proxies solo trabajan con SOCKS 4. Algunas aplicaciones, como Mozilla Firefox permiten configurar ambos tipos de proxies 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.

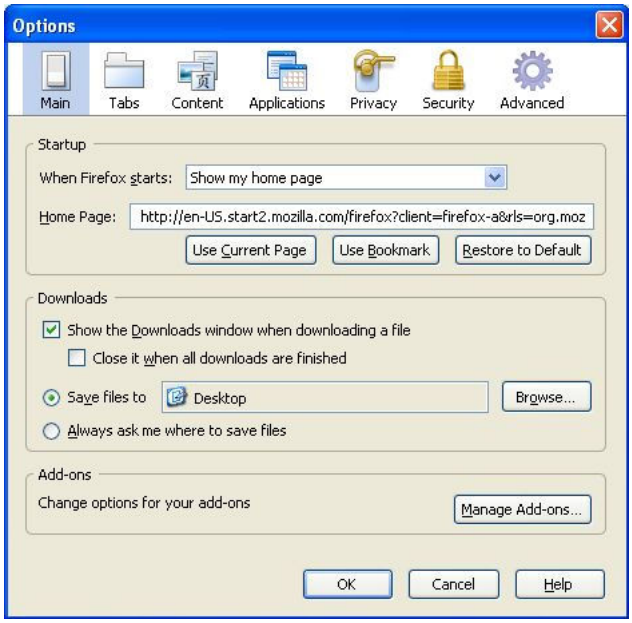
Mozilla Firefox

Entre en la configuración como se muestra en la siguiente imagen y clic en "OK".

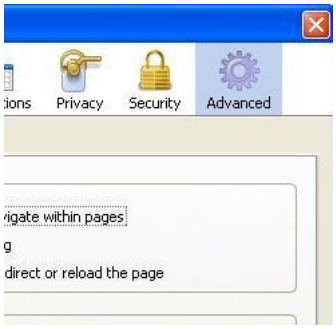
1. En el menu "Herramientas", clic "Opciones":



2. La ventana "Opciones" aparece:

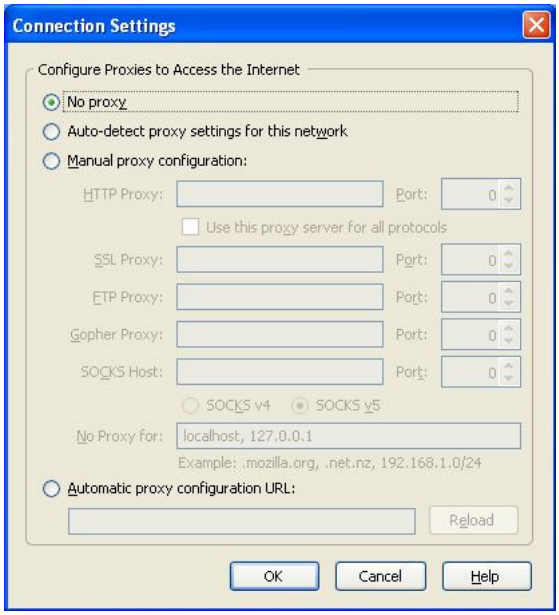


3. En la barra de herramientas en el tope de la ventana, clic "Avanzado":



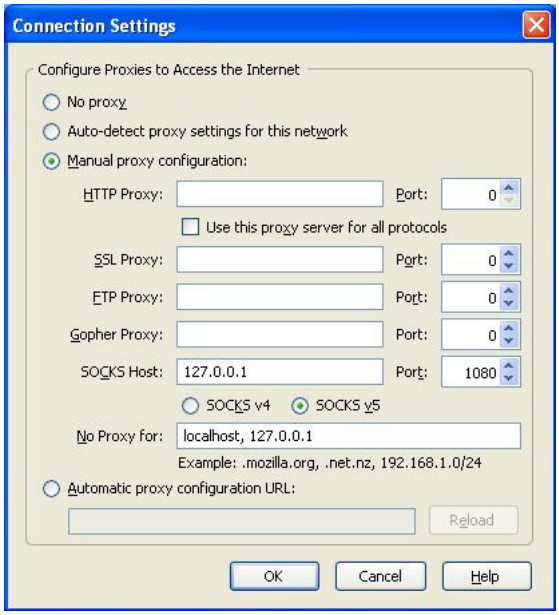
4. Clic el tabulador “Red”:

5. Clic "Configuración". Firefox muestra la ventana "Configuración de Conexión":



6. Seleccione "Configuración manual del proxy". Los campos de debajo de esa opción ahora están disponibles.

7. Entre la dirección del Proxy SOCKS y número de puerto, seleccione "SOCKS v5" y clic en "OK".



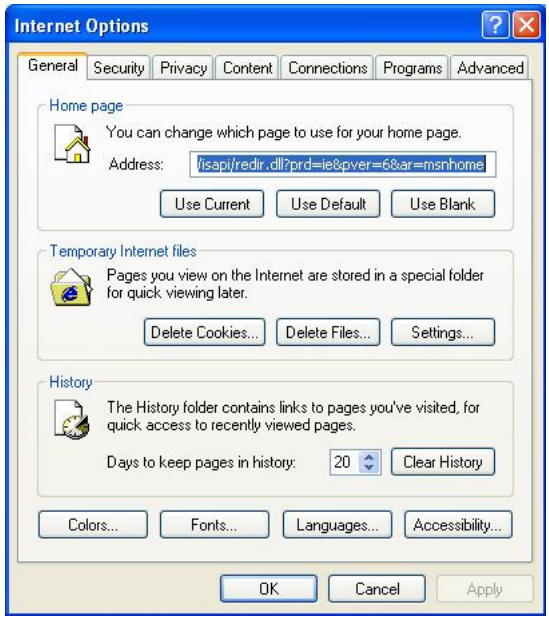
Ahora Firefox está configurado para usar un proxy SOCKS.

Microsoft Internet Explorer

Para configurar Internet Explorer para que use un proxy SOCKS:

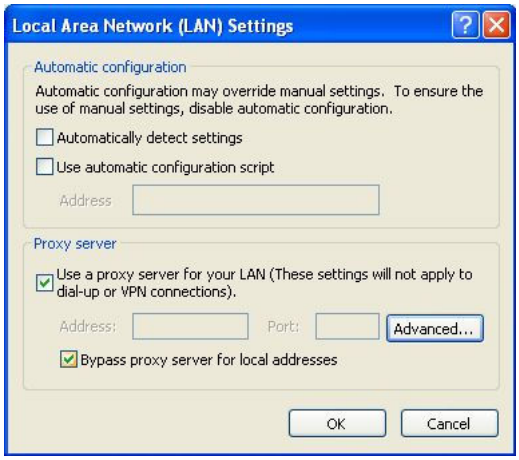
1. En el menu “Herramientas”, clic "Opciones de Internet":

2. Internet Explorer muestra la ventana "Opciones de Internet":

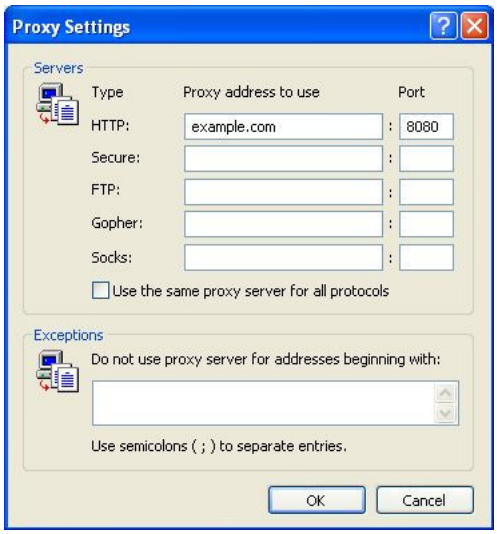


3. Clic el tabulador “Conexiones”:

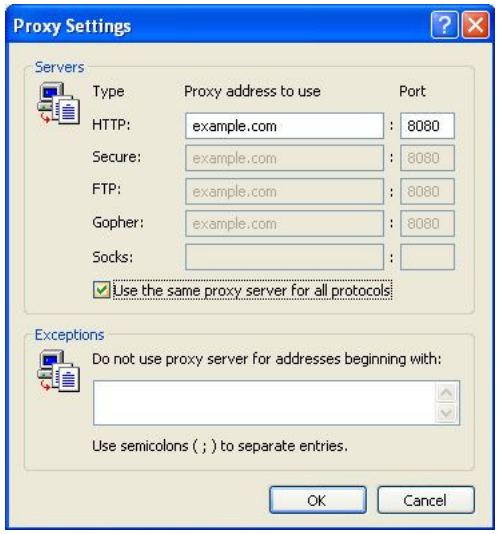
4. Clic "Configuración LAN". Internet Explorer muestra la ventana "Configuración de Red de área local (LAN) ":



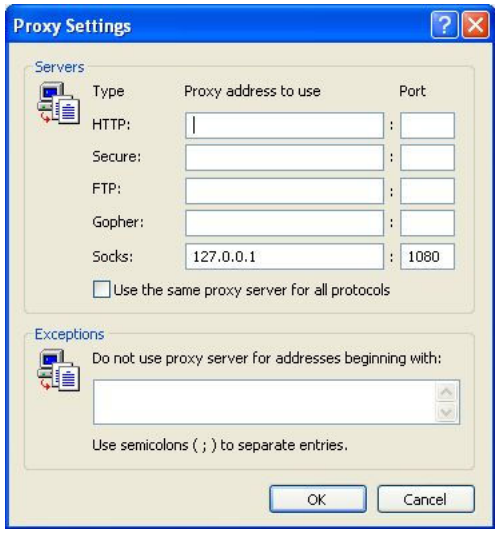
5. Seleccione "Usar un servidor proxy para tu LAN" y clic en "Avanzado". Internet Explorer muestra la ventana de "Configuración de Proxy".



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 “Tools”, clic “Preferences”.

2. Pidgin muestra la ventana Preferentes.

3. Clic en el tabulador “Network” para mostrarlo.

4. En “Proxy type”, seleccione “SOCKS 5”. Aparecen campos adicionales debajo de esta opción.

5. Entre la dirección de “Host” y el número de “Port” de su Proxy SOCKS.

6. Clic “Close”.

Pidgin está ahora configurado para usar un Proxy SOCKS.

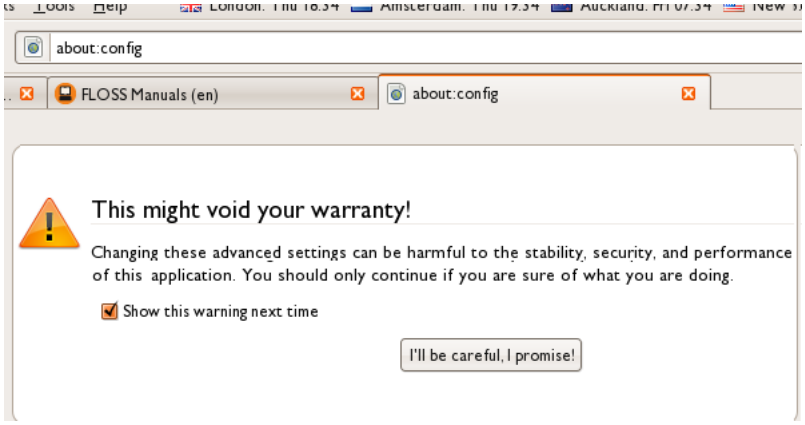
Cuando hayamos terminado con el Proxy

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 ejecunatdo todo el tiempo.

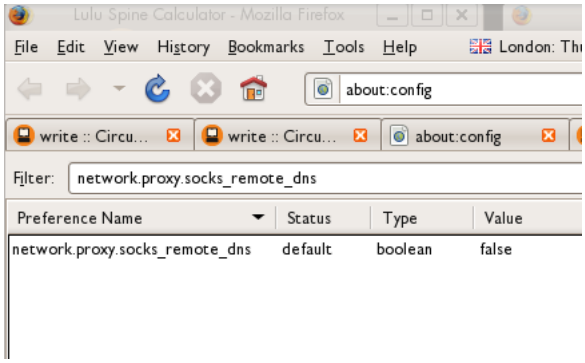
FUGA DE DNS

Un problema importante con proxies SOCKS es que algunas aplicaciones que soportan el uso de proxies 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, which a proxy could otherwise have circumvented. Si una aplicación es 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, entre about:config como si fuera una URL (Debe verse un aviso acerca del cambio en las configuraciones avanzadas):



2. Si es necesario, clic “I’ll be careful, I promise!” para confirmar que se desea cambiar la configuración del navegador. El navegador muestra una lista de configuraciones.
3. En el campo “Filter”, entre network.proxy.socks_remote_dns. Solo esa configuración se muestra.



Si está 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 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.

Autores : *ConfiguringSocksProxies*

Modifications:
adam hyde 2008

Ariel Viera 2009
Freerk Ohling 2008, 2009
Tom Boyle 2008

Produced in FLOSS Manuals

AYUDAR A LOS DEMAS

28. INSTALANDO WEB PROXIES
29. INSTALANDO PHProxy
30. INSTALANDO PSIPHON
31. INSTALANDO UN REPETIDOR TOR
32. RIESGOS DE OPERAR UN PROXY

28. INSTALANDO UN PROXY WEB

La instalación de un programa de evasión basado en Web requiere alguna experiencia técnica así como recursos (un servidor web compatible y suficiente ancho de banda). Hay dos categorías de proxies Web: privados y públicos. Con un proxy Web privado, la ubicación solo es conocida por los usuarios planificados; los proxies Web públicos están disponibles a cualquiera capaz de localizarlos. Los proxies Web públicos y los servicios de anonimato pueden ser conocidos por ambos tipos de usuarios y por aquellos que implementan los filtros, así que son más vulnerables a las listas negras. Las probabilidades de que los proxies Web privados sean detectados y bloqueados son más bajas que los proxies de servicios de evasión públicos.

Los proxies Web privados pueden configurarse con algún nivel de personalización teniendo en cuenta las necesidades del usuario final. Algunas personalizaciones incluyen cambiar el número de puerto por el que se ejecuta el servidor Web e implementar la encripción como es el caso de SSL. Como algunas listas negras pueden bloquear palabras clave asociadas a un proxy popular, cambiar los datos como la URL por defecto, el nombre del script, o elementos de la interfaz de usuario pueden reducir el riesgo de detección automatizada y bloqueo del proxy.

Cuando usamos SSL, es útil crear una página Web inofensiva en la raíz del servidor Web y disfrazar el proxy Web con una ruta y nombre de fichero aleatorios. Aunque los intermediarios pueden ser capaces de determinar el servidor al que te estás conectando, no podrán determinar la dirección solicitada porque la parte de la solicitud estará encriptada. Por ejemplo, si un usuario se conecta a https://example.com/secretproxy/, un intermediario solo será capaz de determinar que el usuario se estará conectando a example.com pero pero no sabrán la solicitud que se ha hecho al proxy Web. (Si el operador del proxy Web coloca una página inocua en example.com entonces el proxy Web es menos propenso a ser descubierto por transmisiones de redes monitorizadas.)

Aquí hay algunos programas proxy Web populares:

- CGIProxy: Un script CGI que actúa como HTTP y como FTP. http://www.jmarshall.com/tools/cgiproxy
- Evasor de Peacefire: Un programa de instalación automático que facilita la instalación y configuración de CGIProxy para usuarios con poca experiencia técnica en una computadora con Windows. http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
- Psiphon: Un programa de instalación automático que facilita la instalación y configuración de PHProxy para usuarios con poca experiencia técnica en una computadora con Windows. http://psiphon.civisec.org/

Los proxies Web privados son más convenientes para usuarios que requieren servicios de evasión estables para tráfico Web y tienen contactos confiables en localidades no filtradas con habilidades técnicas suficientes y ancho de banda disponible para configurar y mantener un proxy Web. Esta es además la forma de evasión más flexible que está disponible para el tráfico Web y que es menos propensa a descubrirse y bloquearse a diferencia del proxy Web público, particularmente si es usado con encripción SSL.

Autores : *InstallingAWebProxy*
© Nart Villeneuve 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

29. INSTALANDO PHPROXY

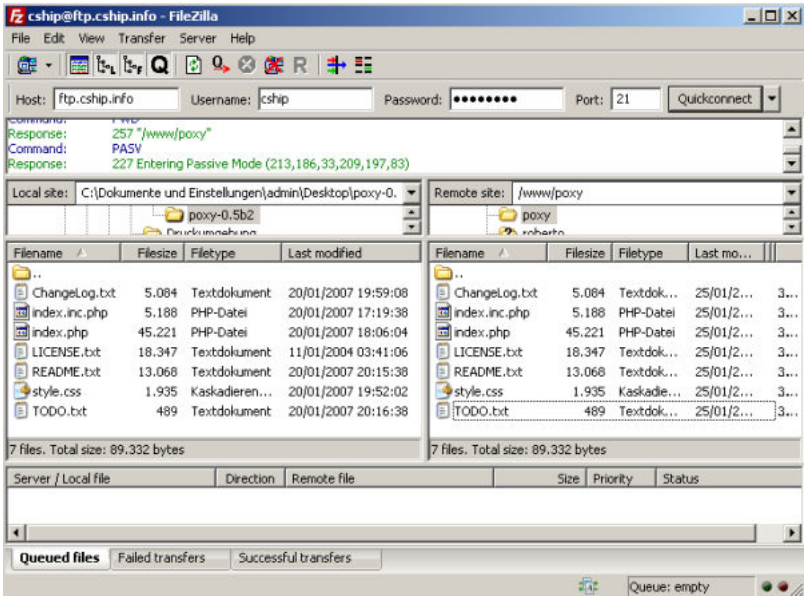
Instalar PHProxy requiere espacio en un servidor Web en una conexión a Internet sin restricciones con soporte para PHP. Pudiera ser:

- Espacio Web rentado (que puede adquirirse por unos pocos USD al año desde compañías de hosting como http://www.dreamhost.com/)
- Un servidor virtual/dedicado (que son más caros y más complicados de usar)
- Una computadora conectada a una conexión DSL/cable (con una dirección IP enrutable pública)
- Una computadora en una universidad con conexión de banda ancha, o una cuenta en un servidor universitario (si la universidad no prohíbe su uso).

Estas instrucciones describen el caso más común: usar FTP para transferir PHProxy a una cuenta en un especio Web que soporta PHP. Para esta técnica, necesitarás un programa cliente FTP como FileZilla (http://filezilla-project.org/).

Aunque este método es el más común, no es aplicable a cada situación. Por ejemplo, si estamos configurando nuestro propio servidor, si el servidor no soporta FTP o si estamos familiarizados con la interfaz de línea de comando, debemos usar un método diferente.

- Primero, descargamos el script PHProxy desde http://sourceforge.net/projects/poxy/. El script solo tiene 25 kilobytes, así que es considerablemente menor que la mayoría de los sitios Web.
- Después, extraemos el contenido del fichero .ZIP haciendo clic derecho en el fichero y seleccionando “Extraer aquí”.
- Iniciamos el cliente FTP, entramos el servidor, nombre de usuario y contraseña que obtuviste de tu proveedor de espacio Web y clic en “Quickconnect”.
- La parte derecha de la ventana del cliente FTP representa la PC local, así que extraemos los ficheros PHProxy aquí.
- Ahora podemos arrastrar y soltar los ficheros desde la parte izquierda del cliente a la derecha, que representa el servidor FTP remoto (nuestro espacio Web)



- Ahora podemos acceder a PHProxy yendo al dominio del espacio Web y al directorio del cual descargamos el PHProxy. (En este ejemplo http://www.cship.info/poxy/.)

Si esto no funciona, la cuenta de servidor puede que no soporte PHP, o puede que esté deshabilitado el soporte para PHP o puede requerir pasos adicionales. Se recomienda consultar la documentación de la cuenta el programa de servidor Web en uso. Podemos además buscar fórums de soporte apropiados o pedir ayuda al operador del servidor web.

Autores : *InstallingPHProxy*
© Freerk Ohling 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

30. INSTALANDO PSIPHON

Para crear una instalación de psiphon necesitamos una computadora con una conexión a Internet sin restricciones que ejecute Windows. Puede que necesitemos además configurar una regla de reenvío de puerto para reenviar el puerto 443 a la computadora Windows. Cómo hacer esto se explica en el manual de router o en http://portforward.com/english/applications/port_forwarding/HTTPS/HTTPSindex.htm.

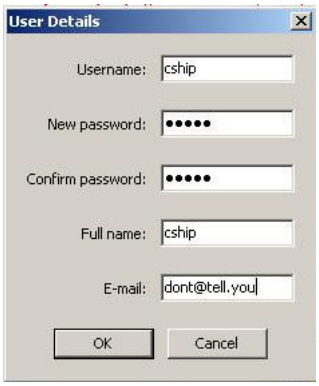
Para comenzar, hay que descargar el script desde http://www.psiphon.ca/download.php (cerca de 2MB).

Doble-clic en el fichero de instalación (que termina en .msi), clic "Next" y selecciona el directorio donde se instalará psiphon. Si no estamos seguros, lo mejor es dejar la carpeta por defecto y clic en "Next".

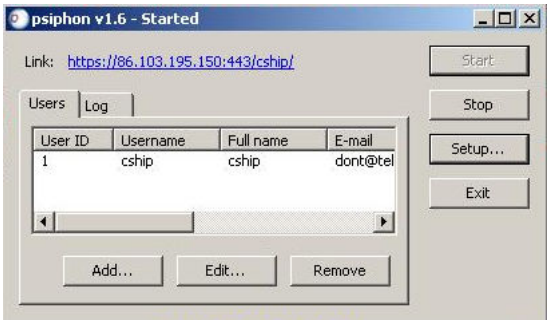
Para iniciar el programa, doble-clic el ícono "psiphon" en el escritorio. Cuando hacemos esto por primera vez, puede que aparezca el aviso de firewall. Si es así, selecciona "Unblock".

Ahora hay que configurar un nodo psiphon. Primero seleccionamos un nombre para el nodo psiphon, por ejemplo "cship". Este nombre será parte de la URL que usaremos o nuestros socios para acceder al nodo.

Para permitir que nuevos usuarios usen el nodo psiphon, hay que crear una cuenta para ellos. Para hacer esto, clic "Add" y entramos los detalles requeridos.



Iniciamos el nodo psiphon haciendo clic en "Start".



Autores : *InstallingPsiphon I*
© Freek Ohling 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008

Produced in FLOSS Manuals

31. CONFIGURANDO UN REPETIDOR TOR(TOR RELAY)

Si estamos en un lugar con poca o ninguna censura de Internet, quizás deseemos ejecutar un simple transmisor Tor o un **transmisor de puente** Tor para ayudar a otros usuarios Tor a acceder a Internet sin censura.

La red Tor confía en voluntarios que donen ancho de banda. Mientras más personas ejecuten los transmisores, más segura y rápida será la red Tor. Para ayudar a las personas a usar Tor para evadir la censura de Internet, configuremos mejor un transmisor de puente que un transmisor ordinario.

Los **transmisores de puentes** (o **puentes** para abreviar) son transmisores Tor que no están listados en el directorio principal de Tor. Incluso si un ISP está filtrando conexiones a todos los transmisores Tor conocidos, probablemente no sea capaz de bloquear todos los puentes.

¿QUÉ NECESITAMOS PARA EJECUTAR UN TRANSMISOR O UN TRANSMISOR DE PUENTE?

Hay solo unos pocos prerrequisitos para ejecutar un transmisor Tor:

- La conexión a Internet necesita un ancho de banda de al menos 20 kilobytes/segundo en ambas direcciones (and it needs to be OK for your connection to be constantly in use when your computer is on)
- Una conexión a Internet con una dirección IP que sea públicamente enrutable.
- Si nuestra computadora está detrás de un firewall NAT (network address translation) y no tiene acceso a su dirección IP pública (o externa), necesitamos configurar una regla de reenvío de puerto en el router. Esto puede hacerse a través de la facilidad de Tor Universal Plug and Play, o manualmente, siguiendo las instrucciones en el manual de router o en portfoward.com (http://portforward.com/english/applications/port_forwarding/HTTPS/HTTPSindex.htm). No se requiere:

- La computadora no tiene que estar siempre encendida y en línea (el directorio Tor sabrá cuando lo está).
- No se necesita una dirección IP estática.

DESCARGANDO TOR

Para descargar Tor, vamos al sitio Web http://www.torproject.org/download.html.es y clic "Descarga" en el menú de navegación. En la página "Available Tor Bundles", selecciona la versión que encaja con tu sistema operativo.

INSTALANDO TOR

Activa el instalador y clic en "Siguiente" cuando pregunte.

Si usamos Firefox, instalamos todos los componentes propuestos en el diálogo que se muestra más abajo:

Si no tenemos Firefox instalado, deseleccionamos "Torbutton" (la opción de instalar Firefox y Torbutton aparecerá después).

Cuando la instalación esté completa, activamos Tor haciendo clic en "Finish" con la caja "Run installed components now" seleccionada, como se muestra en el siguiente diálogo:

CONFIGURANDO TOR PARA QUE SEA UN PUENTE

Para activar el puente:

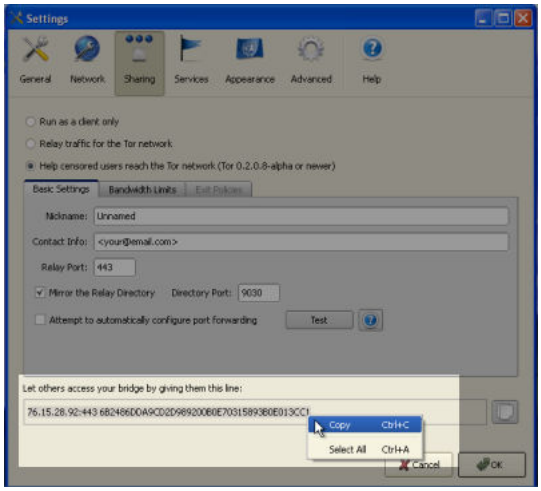
- Abrir el panel de control Vidalia.
- En el panel de control Vidalia, clic "Settings".
- En la ventana "Settings", clic "Sharing":
- Para crear el puente, clic "Help censored users reach the Tor network".
- Si estamos usando una dirección IP NAT en una red local, necesitamos crear una regla de reenvío de de puerto en el router. Se puede pedir a Tor que intente configurar el reenvío de puerto. Para hacer esto, clic "Attempt to automatically configure port forwarding".
- Clic "Test" para ver si Tor creó correctamente una entrada de reenvío de puerto en el router.
- Si Tor no puede configurar el reenvío de puerto, es necesario leer las FAQ relacionadas con el tema en:

https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ#ServerForFirewalledClients

Felicitaciones. Si todo ha ido bien, el puente se está ejecutando. La información de puente se adicionará al directorio de puentes ocultos y lo hacen disponibles a los usuarios que lo solicitan.

COMPARTIENDO EL PUERTO CON AMIGOS

Si establecemos un puente específicamente para ayudar a un amigo a acceder a la red Tor, podemos copiar la información al pie de la ventana de configuración y enviársela.



Autores : *SettingUpaTorRelay*
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Produced in FLOSS Manuals

32. RIESGOS DE OPERAR UN PROXY

Cuando mantenemos un proxy Web o de aplicaciones en nuestra computadora, las solicitudes y conexiones reenviadas a través del proxy aparecerán como originadas desde la misma. Si alguien usara el proxy para enviar o recibir material objetado por un tercero, pudiéramos recibir quejas que asumen que somos responsables y se nos podría exijir que parásemos la actividad. En algunos casos, las actividades en el proxy pueden atraer acciones legales o la atención de agencias de cumplimiento de la ley en nuestro país o en algún otro.

En algunos países, los operadores de proxy han recibido quejas legales y en algunos casos, las agencias de cumplimiento de la ley han confiscado computadoras que funcionaban como proxies. Esto puede pasar por diferentes razones:

- Alguien puede asumir que el operador de proxy estaba personalmente involucrado en la actividad que atraviesa el proxy.
- Alguien puede sostener que el operador del proxy tiene obligación legal de para ciertos usos.
- Alguien tiene la esperanza de examinar el proxy para encontrar evidencia (logfiles) de quien tiene la responsabilidad de alguna actividad.

Si esto puede significar un riesgo en nuestra área puede ser más seguro operar el proxy en una computadora dedicada en un centro de datos. Las leyes nacionales pueden variar en el camino y pueden llegar a liberar a un operador de proxy de responsabilidad legal. Para mas detalles sobre la situación en particular de cada cual, es recomendable consultar un abogado o un experto legal calificado en la jurisdicción en cuestion.

Los proveedores de servicios de Internet pueden también quejarse respecto la operación de un proxy, especialmente si ellos reciben reclamos de abuso de proxy. Algunos **ISP** pueden sostener que que ejecutar un **proxy público** viola sus términos de servicio, o que simplemente no desean permitir que sus usuarios ejecuten proxies públicos. Estos ISP puede desconectar a los usuarios o amenazarlos con desconectarlos en un futuro.

RIESGOS DE OPERAR UN PROXY NO PÚBLICO

Estos riesgos aún existen si operamos un proxy para nuestros propios beneficios o para el uso de un pequeño número de individuos, pero operar un proxy no público es mucho menos riesgoso que operar un proxy público.

Si el usuario de nuestro proxy no público es detectado y monitoreado, cualquiera que esté haciendo la monitorización puede darse cuenta o especular acerca de una conexión entre el usuario y nosotros y que estamos intentando de ayudar a esa persona a evadir el filtrado.

Aunque el ISP probablemente se fije más en los proxies públicos que en los privados, algunos ISP tienen políticas anti-proxy que tienen como objetivo incluso a los proxies privados en sus redes.

RIESGOS DE OPERAR UN NODO TOR (UN RETRANSMISOR TOR)

Un **nodo Tor** es un tipo de proxy público, así que poner a trabajar uno puede implicar los riesgos descritos antes. Sin embargo, un nodo Tor es típicamente configurado de dos formas: como un **nodo de salida** o un **nodo intermedio**. Un nodo intermedio reenvía tráfico encriptado solo a otros nodos Tor, y no permite que usuarios anónimos se comuniquen directamente con sitios fuera de la red Tor. Ejecutar cualquiera de estos tipos de nodos es de gran ayuda para la red Tor. Ejecutar un nodo de salida es particularmente útil porque estos son más escasos. Ejecutar un nodo **intermedio** es comparativamente menos riesgoso porque es poco probable que genere las mismas quejas y reclamos que un proxy público, pues la dirección IP de un nodo middle man nunca aparecerá en los ficheros de log.

Otra configuración de nodo Tor, llamada **puente**, está disponible específicamente para ayudar a otros usuarios a evadir la censura de Internet. Puesto que el puente no es un nodo de salida, no es probable recibir quejas sobre el uso de un nodo puente.

Aún cuando no es probable que se generen quejas específicas, operar un nodo **intermedio** o **puente** puede causar que el ISP objete por razones generales. Por ejemplo, el ISP puede desaprobar la red Tor o prohibir a los suscriptores que operen cualquier tipo de servicio público

LAS LEYES DE RETENCIÓN DE DATOS PUEDEN REGULAR LAS OPERACIONES DE PROXY

En algunos países, las leyes de retención de datos o leyes similares que tienden a restringir el anonimato pueden interpretarse como reguladoras de la operación de los servicios de proxies. Para más información acerca de la retención de datos, leer: http://en.wikipedia.org/wiki/Telecommunications_data_retention.

Autores : *ProxyServerRisks*

Modifications:
adam hyde 2008

Ariel Viera 2009
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008

Sam Tennyson 2008
Tom Boyle 2008

Produced in FLOSS Manuals

ANEXOS

33. RECURSOS
34. GLOSARIO
35. CREDITOS

33. RECURSOS

Evadir la censura de Internet es un tema muy amplio, con decenas de herramientas y servicios disponibles. Hay además muchas cosas que considerar. Si queremos que la actividad de evasión sea más difícil de detectar o bloquear en un futuro, o si queremos usar internet de forma anónima, o ayudar a otras personas a evadir la censura, aquí encontrarás hay algunos recursos recomendados para mejorar el estudio relacionado con la materia. (Algunos de estos recursos están bloqueados en algunos lugares.)

MANUALES Y GUÍAS

Evadiendo la censura de Internet

- Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide, Citizen Lab, http://www.civisec.org/guides/everyones-guides
- Reporters Without Borders, Handbook for Bloggers and Cyber-Dissidents, available at http://www.rsf.org/article.php3?id_article=26187
- The Internet Censorship Wiki: http://en.cship.org/wiki/

Consejos de seguridad para activistas

- NGO-in-a-Box, a collection of free portable applications: http://security.ngoinabox.org/
- Digital Security and Privacy for Human Rights Defenders: http://www.frontlinedefenders.org/manual/en/esecman/

Estudios en 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, available at http://www.opennet.net/accessdenied/
- Otros recursos sobre restricciones de acceso a Internet: http://bailiwick.lib.uiowa.edu/journalism/mediaLaw/cyber_censors.html

ORGANIZACIONES QUE TRABAJAN DOCUMENTANDO, LUCHANDO O EVADIEN RESTRICCIONES DE INTERNET.

- Amnesty International campaign to combat Internet repression (http://irrepressible.info)

- Citizen Lab (http://www.citizenlab.org/) and Civisec Project (http://www.civisec.org/)
- Committee to Protect Bloggers (http://www.committeetoprotectbloggers.org/)
- Berkman Center for Internet and Society (http://cyber.law.harvard.edu/)
- Electronic Frontier Foundation (http://www.eff.org/)
- FrontLine? (http://www.frontlinedefenders.org/)
- Global Internet Freedom Consortium (http://www.internetfreedom.org/)
- The Herdict (http://www.herdict.org/NetworkHealthAbout.jsp?_sourcePage=%2FPCHealthDownload.jsp)
- 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 (http://www.tacticaltech.org/)

PROXIES WEB ABIERTOS Y PROXIES DE APLICACIONES

- Proxy.org, una lista de miles de proxies libres: http://www.proxy.org/
- Subscribirnos en http://www.peacefire.org/circumventor/, una lista de correo que envia una lista de webproxies semanal
- Proxies de aplicaciones:
  - http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_L
  - http://www.publicproxyservers.com/

SOLUCIONES DE EVASIÓN Y OPERADORES DE SERVICIO

- Access Flickr!: https://addons.mozilla.org/en-US/firefox/addon/4286
- Navegación Anonima con Anonimizer: http://www.anonymizer.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/
- Dijjer: http://dijjer.org/
- Dynaweb FreeGate: http://www.dit-inc.us/freegate
- FirePhoenix: http://firephoenix.edoors.com/
- FreeAccess Plus!: https://addons.mozilla.org/en-US/firefox/addon/6139
- 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/
- 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/
- SmartHide: http://www.smarthide.com/
- SwitchProxy Tool: https://addons.mozilla.org/en-US/firefox/addon/125
- Tor: http://torproject.org
- TrafficCompressor: http://www.tcompressor.ru/
- UltraReach UltraSurf: http://www.ultrareach.com/
- VPNBegir: http://www.vpnbegir.com/
- Your-Freedom: http://www.your-freedom.net/
- Zelune: http://www.zelune.net/

Lista de proveedores comerciales de VPN

- http://en.cship.org/wiki/VPN

Programas socksificadores

- 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

Autores : *FurtherResources*

Modifications:

Ariel Viera 2009
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008, 2009

Produced in FLOSS Manuals

34. GLOSARIO

Mucho de este contenido se basa en http://en.cship.org/wiki/Special:Allpages

AGREGADOR

Un agregador es un servicio que recopila información de uno o varios sitios y lo hace disponible en una dirección diferente. A veces llamado un agregador RSS, un agregador de feeds, un lector de feeds, o un lector de noticias. (No debe confundirse con un lector de noticias Usenet).

ANONIMATO

Anonimato en Internet es la capacidad de utilizar los servicios sin dejar pistas sobre su identidad. El nivel de protección depende de las técnicas de anonimato utilizadas y nivel de monitoreo de la red. Las técnicas más fuertes en uso para proteger el anonimato en la red implican la creación de una cadena de comunicación mediante un proceso aleatorio para seleccionar algunos enlaces, en la que cada eslabón sólo tiene acceso a información parcial sobre el proceso. La primera conoce la dirección IP del usuario, pero no el contenido, el destino o finalidad de la comunicación, ya que se cifra el contenido de los mensajes y la información de destino. El último enlace conoce la identidad del sitio que se está visitando, pero no la fuente de la sesión. Uno o más pasos entre estos enlaces impiden que se comparta información parcial entre el primer y el último link.

DESPACHADOR DE CORROS ANONIMOS

Un despachador de correo anónimo es un servicio que acepta mensajes de correo electrónico que contiene instrucciones para la el envió, y los envía sin revelar sus fuentes. Dado que el despachador tiene acceso a la dirección del usuario, el contenido del mensaje, y el destino del mensaje, los despachadores deben ser utilizados como parte de una cadena de reenvíos múltiples de modo que ningún despachador conoce toda la información.

ASP (PROVEEDOR DE SERVICIO DE APLICACIONES)

ASP es una organización que ofrece servicios de software a través de Internet, permitiendo que el software que se actualice y mantenga de forma centralizada.

BACKBONE

Un backbone es una de los enlaces de comunicación de ancho de banda que enlazan las redes en diferentes países y organizaciones de todo el mundo para formar la Internet.

SOFTWARE MALIGNO

Vea Software Maligno.

ANCHO DE BANDA

El ancho de banda de una conexión es la tasa máxima de transferencia de datos en una conexión, limitada por su capacidad y las capacidades de los equipos de ambos extremos de la conexión.

BASH (BASADO EN EL SHELL BOURNE)

El intérprete de comandos bash es una interfaz de línea de comandos para los sistemas operativos Linux y Unix, basado en el shell de Bourne.

BITTORRENT

BitTorrent es un protocolo de compartimiento de ficheros punto a punto inventado por Bram Cohen en 2001. Permite a los individuos de forma barata y eficaz la distribución de archivos grandes, como imágenes de CD, vídeo o archivos de música.

LISTA NEGRA

Una lista negra es una lista de las personas o contenidos prohibidos. En la censura en Internet, listas de sitios Web prohibidos pueden utilizarse como listas negras; los software de censura pueden permitir el acceso a todos los sitios excepto a los específicamente enumerados en su lista negra. Una alternativa a una lista negra es una lista blanca, o una lista de contenidos permitidas. Una sistema de lista blanca bloquea el acceso a todos los sitios excepto en los específicamente enumerados en la lista blanca. Este es un enfoque menos común en la censura de Internet. Es posible combinar ambos métodos, en este caso se utiliza el macheo de cadenas u otras técnicas condicionales sobre las URL que no se adaptan a la lista.

BLOQUEAR

Bloquear es impedir el acceso a un recurso de Internet, utilizando cualquier método.

MARCADOR (BOOKMARK)

Un marcador es un marcador de posición dentro del software, que contiene una referencia a un recurso externo. En un navegador, un marcador es una referencia a una página Web - eligiendo el marcador con el que puede cargar rápidamente el sitio Web sin necesidad de escribir la URL completa.

PUENTE

Ver Puente Tor.

CACHE

La caché es una parte de un sistema de procesamiento de la información utilizada para almacenar los datos recientemente usados o utilizados con frecuencia para acelerar el acceso repetido a la misma. Un caché web almacena copias de los archivos de páginas web.

CENSURAR

Censurar es evitar la publicación o la recuperación de información, o adoptar medidas, legales o de otro tipo, contra los editores y lectores.

SOFWARE DE CENSURA (CENSORWARE)

Un programa de censura "*Censorware*" es el software usado para filtrar o bloquear el acceso a Internet. Este término se utiliza para referirse a la filtración de Internet, o software de bloqueo instalados en la máquina cliente (la PC que se utiliza para acceder a la Internet). La mayoría de los clientes "*censorware*" se utilizan para fines de control parental. A veces el término "programas censura" también se utiliza para referirse al software utilizado para el mismo fin instalado en un servidor de red o router.

CGI (COMMON GATEWAY INTERFACE)

CGI es un standard común utilizado para permitir que los programas en un servidor Web se ejecuten como aplicaciones Web. Muchos de los proxies web utilizan CGI y por lo tanto también se conocen como "proxies CGI". (Una aplicación Proxy CGI muy popular escrita por James Marshall utilizando el lenguaje de programación Perl se llama CGIProxy.)

CHAT

Chat, también llamada de mensajería instantánea, es un método común de comunicación entre dos o más personas en la que cada línea escrita por un participante en una sesión se hace eco a todos los demás. Existen numerosos protocolos de chat, incluidos los creados por empresas especificas (AOL, Yahoo, Microsoft, y otros) y los protocolos definidos públicamente. Algunos programas de chat cliente utilizan sólo uno de estos protocolos, mientras que otros utilizan una serie de protocolos populares.

ELUSION (CIRCUMVENTION)

La elusión es publicar o acceder a los contenidos, a pesar de los intentos de censura. Además, el proceso de evadir vigilancia mientras lo hace.

COMMON GATEWAY INTERFACE

Ver CGI.

INTERFAZ DE LINEA DE COMMANDOS (COMMAND-LINE INTERFACE)

Un método de control de la ejecución de software mediante comandos introducidos en un teclado, como un shell de Unix o la línea de comandos de Windows.

COOKIE

Una cookie es una cadena de texto enviado por un servidor web al navegador del usuario para almacenar en el ordenador del usuario, que contenga la información necesaria para mantener la continuidad en las sesiones a través de múltiples páginas Web, o en varias sesiones. Algunos sitios web no pueden ser utilizados sin aceptar y almacenar una cookie. Algunas personas consideran esto una invasión de la privacidad o un riesgo de seguridad.

CODIGO DE DOMINIO DE PAISES (COUNTRY CODE TOP-LEVEL DOMAIN (CCTLD))

Cada país tiene un código de dos letras, y un TLD basado en él, tales como .ca para Canadá, lo que se llama un dominio superior de código de país. Cada uno de dichos ccTLD tiene un servidor DNS que enumera todos los dominios de segundo nivel en el TLD. Los servidores principales de Internet enumeran a todos los TLDs, y la caché se utiliza con frecuencia sobre los dominios de nivel inferior apara almacenar información.

DARPA (AGENCIA INVESTIGACIÓN AVANZADA DE PROYECTOS DE DEFENSA)

DARPA es la sucesora de ARPA, que financió la Internet y su predecesora, la ARPANET.

DECIFRADO (DESENCRIPTACION)

Descifrar es recuperar el texto u otros mensajes de datos cifrados con el uso de una clave.

Vea tambien Cifrado o encriptación.

DOMINIO

Un dominio puede ser un primer nivel de Dominio (TLD) o un dominio secundario en Internet. Véase también el Dominio de Nivel Superior, código de país de nivel superior del dominio y el dominio secundario.

DNS (SISTEMA DE NOMBRE DE DOMINIO)

El Sistema de Nombre de Dominio (DNS) convierte los nombres de dominio, compuesto por una combinación de caracteres fáciles de recordar a las direcciones IP, secuencias de números difíciles de recordar. Cada ordenador en Internet tiene una dirección única (como un código de área + número de teléfono).

FUGA DE DNS

Una fuga del DNS ocurre cuando un equipo configurado para utilizar un proxy para su conexión a Internet hace consultas DNS sin usar el proxy, permitiendo así a los usuarios para conectarse con sitios bloqueados. Algunos navegadores web tienen opciones de configuración para forzar el uso del proxy.

SERVIDOR DNS

Un servidor DNS o servidor de nombres, es un servidor que proporciona la función de identificación de los nombres de dominio. Para ello, ya sea mediante el acceso a un registro existente en caché de la dirección IP de un dominio específico, o mediante el envío de una solicitud de información a otro servidor de nombres.

TUNEL DNS

Un túnel de DNS es una forma de pasar casi todo a lo largo de los DNS o Servidores de Nombres. Debido a que "abusamos" del sistema de DNS para un fin no deseado, este sólo permite una conexión muy lenta de unos 3 kb/s que es incluso menor que la velocidad de un módem analógico. Eso no es suficiente para servicios como YouTube o filesharing, pero debe ser suficiente para mensajeros instantáneos como ICQ o MSN Messenger y también para los de texto e-mail.

La conexión que desea utilizar un túnel de DNS sólo se necesita el puerto 53 para ser abierta. Así que incluso trabaja en muchos proveedores comerciales Wi-Fi sin necesidad de pagar.

El principal problema es que no existen nombres de servidores públicos modificados que podamos utilizar. Usted tiene que configurar el suyo propio. Usted necesita un servidor con una conexión permanente a Internet que utilice Linux. Luego puede instalar el software libre OzymanDNS y en combinación con SSH y un proxy como Squid puede utilizar el túnel. Más información sobre esto en http://www.dnstunnel.de/

ESPIONAJE

El espionaje es escuchar el tráfico de voz o la lectura o filtrar el tráfico de datos en una línea telefónica o conexión de datos digitales, generalmente para detectar o prevenir actividades ilegales o no deseadas o para controlar o supervisar lo que la gente está hablando.

E-MAIL

E-mail, abreviatura de correo electrónico, es un método para enviar y recibir mensajes a través de Internet. Es posible utilizar un servicio de correo Web o para enviar e-mails con el protocolo SMTP y los que se reciben con el protocolo POP3 usando un cliente de correo electrónico como Outlook Express o Thunderbird. Es relativamente raro que un Gobierno bloquee el correo electrónico, pero el correo electrónico bajo vigilancia es común. Si el correo electrónico no está encriptado, puede ser leído fácilmente por un operador de red o de gobierno.

CIFRADO O ENCRIPTACION

El cifrado es un método de grabación y codificación de datos o su transformación matemática para que sea ilegible para un tercero que no conoce la clave secreta para descifrarlo. Es posible cifrar los datos en su disco duro local usando programas como TrueCrypt (http://www.truecrypt.org/) o para encriptar el tráfico de Internet con SSL o SSH.

Véase también el descifrado.

NODE DE SALIDA

An exit node is a Tor node that forwards data outside the Tor network.

Un nodo de salida Tor es un nodo Tor que envía los datos fuera de la red Tor.

Véase también nodo intermediario.

INTERCAMBIO DE ARCHIVOS (FILE SHARING)

Uso compartido de archivos se refiere a cualquier sistema informático donde las personas pueden usar la misma información, pero a menudo se refiere al intercambio de música, películas u otros materiales disponibles a los demás de forma gratuita a través de Internet.

SISTEMA DE INTERCAMBIO DE ARCHIVOS

Un sistema de intercambio es un sitio web que un editor puede utilizar para burlar la censura. Un usuario sólo tiene que cargar un archivo a publicar y el motor de intercambio de archivos lo presenta a un conjunto de servidores de intercambio (como Rapidshare o Megaupload).

FILTRO

Filtrar es la búsqueda de diversas formas específicas de patrones de datos para bloquear o permitir las comunicaciones.

FIREFOX

Firefox es el más popular navegador web libre y de código abierto, desarrollado por la Fundación Mozilla.

FORO (FORUM)

En un sitio web, un foro es un lugar para el debate, donde los usuarios pueden enviar mensajes y comentarios sobre los mensajes publicados con anterioridad. Se distingue de una lista de correo o de un grupo de noticias Usenet por la persistencia de las páginas que contienen los hilos de mensajes. Los grupos de noticias y archivos de la lista de correo, en cambio, suelen mostrar los mensajes por página, con las páginas de navegación listando sólo los encabezados de los mensajes en un hilo.

FRAME

Un frame es una porción de una página web con su propia URL distinta. Por ejemplo, los frames se utilizan con frecuencia para colocar un menú estático al lado de una ventana de texto con desplazamiento.

FTP (PROTOCOLO DE TRASFERENCIA DE FICHEROS)

El protocolo FTP se utiliza para transferencia de archivos. Muchos usuarios lo utilizan sobre todo para las descargas, además puede ser usado para cargar las páginas Web y scripts para algunos servidores Web. Normalmente se utilizan los puertos 20 y 21, que a veces se bloqueados. Algunos servidores FTP escuchan en un puerto poco frecuente, que permite eludir el bloqueo basado en puertos. Un popular cliente FTP libre y de código abierto para Windows es FileZilla. También hay algunos clientes basados en Web que se pueden utilizar con un navegador Web normal, como Firefox.

PUERTA DE ENLACE (GATEWAY)

Una puerta de enlace (gateway) es un nodo de conexión de dos redes en Internet. Un ejemplo importante es una puerta de enlace nacional que requiere que todo el tráfico entrante o saliente que pase por el.

HONEYPOT

Un honeypot es un sitio que pretende ofrecer un servicio con el fin de atraer a los potenciales usuarios a utilizarlo, y para captar información sobre ellos o sus actividades.

SALTO

Un salto es un enlace en una cadena de transferencias de datos de un ordenador a otro, o de cualquier equipo a lo largo de la ruta. El número de saltos entre los equipos pueden dar una medida aproximada de la demora (latencia) en las comunicaciones entre ellos. Cada salto individual es también una entidad que tiene la capacidad de interceptar, bloquear o manipular las comunicaciones.

HTTP (PROTOCOLO DE TRASFERENCIA DE HIPERTEXTO)

HTTP es el protocolo fundamental de la World Wide Web, que proporciona métodos para solicitar y publicar páginas Web, realizar consultas y generar respuestas a las preguntas, y el acceso a una amplia gama de servicios.

HTTPS (HTTP SEGURO)

HTTP seguro es un protocolo de comunicación segura usando cifrado de mensajes HTTP. Los mensajes entre el cliente y el servidor se cifran en ambas direcciones, usando llaves generadas cuando la conexión se solicita y se intercambia el contenido de forma segura. Las direcciones IP de origen y destino están en las cabeceras de cada paquete, por lo que HTTPS no puede ocultar el hecho de la comunicación, tan sólo el contenido de los datos transmitidos y recibidos.

IANA (AUTORIDAD ASIGNACIÓN DE NÚMEROS DE INTERNET)

IANA es la organización responsable de los trabajos técnicos en la gestión de la infraestructura de la Internet, incluyendo la asignación de bloques de direcciones IP de los dominios de nivel superior y dominios registrados para los ccTLD y de los TLD genéricos. Corriendo los servidores de nombres raíz de Internet, y otras funciones.

ICANN (CORPORACIÓN DE INTERNET PARA NOMBRES Y NÚMEROS ASIGNADOS)

ICANN es una corporación creada por el Departamento de Comercio de EE.UU. para administrar los niveles más altos de la Internet. Su trabajo técnico se lleva a cabo por la IANA.

INSTANT MESSAGING (IM)

La mensajería instantánea (IM) es una forma de chat propietario en el que se emplean protocolos propietarios, o el chat en general. Clientes comunes de mensajeria instantanea incluyen MSN Messenger, ICQ, AIM o Yahoo! Messenger.

INTERMEDIARIO

Ver intermediario o hombre en el medio.

INTERNET

El Internet es una red de redes interconectadas mediante TCP / IP y otros protocolos de comunicación.

IP (PROTOCOLO DE INTERNET) DIRECCIONES

Una dirección IP es un número de cuatro bytes (en la actual versión 4 del protocolo de Internet), la identificación de un equipo determinado en Internet, a menudo representado como cuatro enteros en el rango 0-255 separados por puntos, como 74.54.30.85.

IRC (INTERNET RELAY CHAT)

El IRC es un protocolo de Internet de más de 20 años utilizado para conversaciones de texto en tiempo real (chat). Existen varias redes de IRC - la más grande tiene más de 50 000 usuarios.

ISP (PROVEEDOR DE SERVICIO DE INTERNET)

Un ISP (proveedor de servicios de Internet) es una empresa u organización que proporciona acceso a Internet para sus clientes.

JAVASCRIPT

Javascript es un lenguaje de script, comúnmente utilizado en las páginas web para proporcionar funciones interactivas.

FILTRO DE PALABRAS

Un filtro de palabras clave escanea todo el tráfico de Internet que pasa por un servidor para detectar palabras prohibidas o en condiciones de bloquear.

FICHERO DE REGISTROS

Un archivo de registro es un archivo que registra una secuencia de mensajes de un proceso de software, que puede ser una aplicación o un componente del sistema operativo. Por ejemplo, los servidores web o servidores proxy puede mantener archivos de registro que contienen los registros sobre las direcciones IP utilizadas por estos servicios, cuando y lo que se accedió a las páginas.

FILTRO DE BAJO ANCHO DE BANDA.

Un filtro de ancho de banda es un servicio web que elimina los elementos externos tales como la publicidad y las imágenes de una página Web y los comprime, haciendo la descarga de la página mucho más rápida.

SOFTWARE MALIGNO

Malware is a general term for malicious software, including viruses, that may be installed or executed without your knowledge. Malware may take control of your computer for purposes such as sending spam. (Malware is also sometimes called badware.)

El software maligno (Malware) es un término general para el software malicioso, como virus, que pueden ser instalados o ejecutados sin su conocimiento. El malware puede tomar el control de

su ordenador para fines tales como el envío de spam. (Malware es a veces también llamado software maligno).

HOMBRE EN EL MEDIO

Un hombre en el medio o el "hombre en el medio" es una persona o un equipo de captura de tráfico en un canal de comunicación, especialmente para cambiar selectivamente o bloquear el contenido en una forma que socava la seguridad criptográfica. En general, consiste en hacerse pasar por un sitio Web, servicio o persona a fin de registrar o alterar las comunicaciones. Los gobiernos pueden ejecutar esta función en como puertas del país a todo el tráfico que entre o salga del país.

NODO DE INTERCAMBIO (MIDDLEMAN NODE)

Un nodo es un nodo intermediario Tor que no es un nodo de salida. Ejecutar un nodo de intermediario puede ser más seguro que ejecuta un nodo de salida, porque un nodo de intermediario no aparecerá en los archivos de registro de terceros. (Un nodo intermediario se llama a veces no nodo de salida.)

MONITOREAR

Monitorear es controlar un flujo de datos constante para detectar la actividad no deseada.

TRADUCCIÓN DE DIRECCIÓN DE RED (NAT)

NAT es una función de router para ocultar un espacio de direcciones de reasignación. Todo el tráfico que va desde el router utiliza la dirección IP del router y el router sabe cómo enrutar el tráfico entrante a la solicitante. NAT es frecuentemente aplicado por los cortafuegos (firewalls). Debido a que las conexiones son normalmente prohibidas por NAT, NAT hace difícil ofrecer un servicio al público en general, como un sitio Web o servidor proxy público. En una red NAT, estos servicios requieren algún tipo de configuración del firewall o del método de NAT transversal.

OPERADOR DE LA RED

Un operador de la red es una persona u organización que dirige o controla una red y por lo tanto está en condiciones de supervisar, bloquear o alterar las comunicaciones que pasan por la red.

NODE

Un nodo es un dispositivo activo en una red. Un router es un ejemplo de un nodo. En el psiphon y redes de Tor, un servidor se conoce como un nodo.

NODO DE NO SALIDA

Vea nodo de intercambio.

OFUSCACION

Ofuscación significa ocultar texto que va a recibir una inspecciona casual utilizando técnicas de transformación de fácil entendimiento y conversión, pero no criptoanálisis, o hacer cambios menores en las cadenas de texto para evitar sencillos comparaciones de cadenas. Los Proxies web suelen utilizar la ofuscación para ocultar ciertos nombres y direcciones de los filtros de texto simple que pueden engañar por la ofuscación. Como otro ejemplo, cualquier nombre de dominio, opcionalmente, puede contener un punto final, como en "somewhere.com.", Pero algunos filtros pueden buscar sólo "somewhere.com" (sin el punto final).

PAQUETE

Un paquete es una estructura de datos definidos por un protocolo de comunicaciones que contengan información específica en formas específicas, junto con datos arbitrarios para ser transmitidos a partir de un punto a otro. Los mensajes se dividen en piezas que caben en un paquete para la transmisión, y volverse a montar en el otro extremo del enlace.

PUNTO A PUNTO

Punto a Punto (o P2P) es una red informática entre iguales. A diferencia de las redes cliente-servidor no hay un servidor central por lo que el tráfico se distribuye sólo entre la tecnología clientes. Esta se aplica mayoritariamente a programas para compartir archivos como BitTorrent, eMule y Gnutella. Pero también la tecnología de Usenet o el programa de VoIP Skype puede ser categorizado como "sistema punto a punto".

Véase también el intercambio de archivos.

PHP

PHP es un lenguaje de script diseñado para crear sitios Web dinámicos y aplicaciones web. Se instala en un servidor Web. Por ejemplo, el popular proxy Web "PHProxy" utiliza esta tecnología.

PLAIN TEXT

Texto plano es texto sin formato que consiste en una secuencia de códigos de caracteres, como en texto plano ASCII o texto sin formato Unicode.

PLAINTEXT

Plaintext es texto sin cifrado o no encriptado

Vea además Cifrado, encriptación, SSL, SSH.

PRIVACIDAD

La protección de la intimidad personal (privacidad), es impedir la divulgación de información personal sin el consentimiento de la persona en cuestión. En el contexto de la elusión, que significa la prevención de los observadores de descubrir que una persona haya solicitado o recibido información que se haya bloqueado o es ilegal en el país.

POP3

Post Office Protocol version 3 se utiliza para recibir correo de un servidor, por defecto en el puerto 110 con un programa de correo electrónico como Outlook Express o Thunderbird.

PUERTO

Un puerto de hardware en un ordenador es un conector físico para un propósito específico, utilizando un protocolo de hardware en particular. Ejemplos de ello son un puerto de monitor VGA o un conector USB. Los puertos de software también pueden conectar ordenadores y otros dispositivos a través de redes utilizando diferentes protocolos, pero existen en el software sólo como números. Los puertos son algo así como números en las puertas de las habitaciones diferentes. Ellos se identifican por números del 0 al 65535.

PROTOCOLO

Una definición formal de un método de comunicación, y la forma de datos que se transmitirán para lograrlo. Además, el objetivo de este método de comunicación. Por ejemplo, el Protocolo de Internet (IP) para la transmisión de paquetes de datos en Internet, o Protocolo de transferencia de hipertexto para las interacciones en la World Wide Web.

SERVIDOR PROXY

Un servidor proxy es un servidor, un sistema informático o un programa de aplicación que actúa como una puerta de enlace entre un cliente y un servidor Web. Un cliente se conecta al servidor proxy para solicitar una página Web desde un servidor diferente, entonces, el servidor proxy da acceso al recurso mediante la conexión al servidor especificado, y devuelve la información en la página de la solicitud. Los servidores proxy pueden servir a muchos propósitos, incluyendo la restricción de acceso a la Web o ayudar a los usuarios a vencer obstáculos en la navegación.

DIRECCIONES RUTEABLES IP PUBLICAS.

Las direcciones ruteables IP publicas son direcciones IP (a veces llamadas direcciones IP públicas) que se pueden acceder de la forma habitual en Internet, a través de una cadena de routers. Algunas de las direcciones IP son privadas, tales como 192.168.xx, y muchos están sin asignar.

EXPRESION REGULRAR

Una expresión regular (también llamado regexp o RE) es un modelo de texto que especifica un conjunto de cadenas de texto en la aplicación de una determinada expresión regular como la utilidad grep de Unix. Una cadena de texto "coincide con" una expresión regular si la cadena se ajusta al patrón, según lo definido por la sintaxis de expresión regular. En cada uno de sintaxis RE, algunos caracteres tienen un significado especial, para permitir que un patrón que corresponda con varias cadenas de otros.

DESPACHADOR (REMAILER)

Un repetidor de correo anónimo es un servicio que permite a los usuarios enviar mensajes de correo electrónico de forma anónima. El despachador recibe mensajes a través de correo electrónico y los reenvía a su destinatario después de eliminar información que pudiera identificar al remitente original. Algunos también ofrecen una dirección de remitente anónimo que se puede utilizar para responder al remitente original, sin revelar su identidad. Bien conocidos son los servicios de Remailer cypherpunk, Mixmaster y Nym.

ROUTER

Un router es un ordenador que determina la ruta para el reenvío de paquetes. Utiliza la información de dirección en la cabecera del paquete y la información almacenada en caché en el servidor para que coincida con los números de direcciones con las conexiones de hardware.

SERVIDOR DE NOMBRES DE RAIZ (ROOT NAME SERVER)

Un servidor de nombres raíz o de cualquier servidor raíz es cualquiera de los trece grupos de servidores administrados por IANA para dirigir el tráfico a todos los dominios de nivel superior, como el núcleo del sistema de DNS.

RSS (REAL SIMPLE SYNDICATION)

El RSS es un método y un protocolo para permitir a los usuarios de Internet suscribirse a contenido de una página Web, y recibir las actualizaciones tan pronto como sean publicados.

ESQUEMA (SCHEME)

En la Web, un esquema es una asignación de un nombre a un protocolo. Así, el esquema HTTP mapea la direcciones URL que comienzan con HTTP: al Protocolo de transferencia de hipertexto. El protocolo determina la interpretación del resto de la URL, de modo que http://www.example.com/dir/content.html identifica un sitio web y un archivo específico en un directorio específico, y mailto: user@somewhere.com es una dirección de correo electrónico de una persona o un grupo específico en un dominio específico.

SHELL

Un shell de Unix es la tradicional interfaz de línea de comando de usuario para el sistema 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 este opera entre la capa de aplicación y la capa de transporte. El puerto estándar para servidores proxy SOCKS es 1080, pero también se puede ejecutar en diferentes puertos. Muchos programas soportan conexiones a través de un proxy SOCKS, si no se puede instalar clientes como Socks FreeCap, ProxyCap o SocksCap que pueden forzar a los programas a que se ejecuten a través del proxy Socks mediante el reenvío de puertos dinámicos. También es posible utilizar herramientas SSH como OpenSSH como un servidor proxy SOCKS.

SCRIPT

Un script es un programa, generalmente escrito en un lenguaje interpretado, no compilado como JavaScript, Java, o un intérprete de comandos como el Bash. Muchas páginas web incluyen secuencias de comandos para gestionar la interacción del usuario con una página Web, de modo que el servidor no tiene que enviar una nueva página para cada intercambio.

MENSAJES DE CORREO NO DESEADOS (SPAM)

Los spam (Mensajes de correo no deseado) son mensajes que abruman a un canal de comunicaciones utilizado por los clientes, la mayoría son la publicidad comercial, enviados a un gran número de individuos o grupos de discusión. La mayoría de los spam anuncian productos o servicios que son ilegales en una o más formas, casi siempre incluyendo el fraude. El Filtrado de contenidos de e-mail para bloquear el spam, con el permiso del destinatario, es casi universalmente aprobado.

SSH (SHELL SEGURO)

SSH o Shell seguro es un protocolo de red que permite la comunicación cifrada entre equipos. Se inventó como un sucesor del protocolo Telnet sin cifrar y también se utiliza para acceder a una shell en un servidor remoto.

El puerto SSH estándar es el 22. Puede ser utilizado para eludir la censura en Internet con el reenvío de puertos o puede ser utilizado para otros programas como el túnel de VNC.

SSL (SECURE SOCKETS LAYER)

SSL es uno de varios estándares criptográficos utilizados para hacer transacciones seguras en Internet. Fue utilizado como la base para la creación de las correspondientes Transport Layer Security (TLS). Usted puede ver si usted está usando SSL / TLS mirando en la dirección URL en su navegador (Firefox o Internet Explorer): Si empieza por https en lugar de http, se cifra la conexión.

ESTEGANOGRAFIA

Esteganografía, del griego "escritura oculta", se refiere a una variedad de métodos de envío de mensajes ocultos donde no sólo el contenido del mensaje se oculta sino que tambien se se oculta el hecho mismo de que el enviando es secreto. Normalmente esto se hace mediante la ocultación de algo en otra cosa, como una imagen o un texto sobre algo inocente o completamente independientes. A diferencia de la criptografía, en donde es evidente que un mensaje secreto se transmite, la esteganografía no atrae la atención sobre el hecho de que alguien está tratando de ocultar o encriptar un mensaje.

ANÁLISIS DE LA AMENAZA

A security threat analysis is properly a detailed, formal study of all known ways of attacking the security of servers or protocols, or of methods for using them for a particular purpose such as circumvention. Threats can be technical, such as code-breaking or exploiting software bugs, or social, such as stealing passwords or bribing someone who has special knowledge. Few companies or individuals have the knowledge and skill to do a comprehensive threat analysis, but everybody involved in circumvention has to make some estimate of the issues.

Un análisis de las amenazas de seguridad es propiamente un detallado estudio formal de todas las formas conocidas de atacar la seguridad de los servidores o los protocolos, o de los métodos utilizados para un fin determinado, tales como la elusión. Las amenazas pueden ser de carácter técnico, como el desciframiento de códigos o la explotación de los errores de software, o sociales, como el robo de contraseñas o sobornar a alguien que tiene conocimientos especiales. Pocas compañías o individuos tienen el conocimiento y la habilidad para hacer un análisis de la amenaza global.

DOMINIO A ALTO NIVEL (TLD)

En los nombres de Internet, el TLD es el último componente del nombre de dominio. Hay varios dominios de nivel superior genéricos, sobre todo .com, .org, .edu, .net, .gov, .mil, .int, y un código de dos letras del país (ccTLD) para cada país en el sistema, tales como .ca para Canadá. La Unión Europea también tiene el código de dos letras .eu.

TLS (CAPA DE TRANSPORTE SEGURO)

TLS es un estándar de cifrado basado en SSL, utilizado para hacer transacciones en Internet segura.

TCP/IP (PROTOCOLO DE CONTROL DE TRANSFERENCIA SOBRE INTERNET)

TCP e IP son los protocolos fundamentales de Internet, intervienen en el manejo de la transmisión de paquetes y enrutamiento. Hay pocos protocolos alternativos que se utilizan en este nivel de la estructura de Internet, como UDP.

TOR BRIDGE

A bridge is a middleman Tor node that is not listed in the main public Tor directory, and so is possibly useful in countries where the public relays are blocked. Unlike the case of exit nodes, IP addresses of bridge nodes never appear in server log files and never pass through monitoring nodes in a way that can be connected with circumvention.

Un puente es un nodo intermediario Tor que no aparece en el directorio principal de Tor público, y posiblemente, útil en países donde se bloquean los servicios públicos. A diferencia del caso de los nodos de salida, las direcciones IP de los nodos de la intercambio no aparecen en los archivos de registro del servidor y no pasan a través de los nodos de control de manera que se pueda conectar con la elusión.

ANÁLISIS DE TRÁFICO

El análisis de tráfico es el análisis estadístico de las comunicaciones cifradas. En algunas circunstancias el análisis de tráfico puede revelar información sobre la gente y comunicar la información que se comunica.

TUNNEL

Un túnel es una ruta alterna de un ordenador a otro, que generalmente incluye un protocolo que especifica la codificación de mensajes.

UDP (USER DATAGRAM PACKET)

UDP is an alternate protocol used with IP. Most Internet services can be accessed using either TCP or UDP, but there are some that are defined to use only one of these alternatives. UDP is especially useful for real-time multimedia applications like Internet phone calls (VoIP).

UDP es un protocolo alternativo usado con IP. La mayoría de los servicios de Internet se pueden acceder utilizando TCP o UDP, pero hay algunos que se definen a utilizar sólo una de estas alternativas. UDP es especialmente útil para todas las aplicaciones multimedia en tiempo real, como (VoIP).

URL

La dirección URL (Uniform Resource Locator) es la dirección de un sitio Web. Por ejemplo, la URL de la sección de Noticias Mundial del New York Times es http://www.nytimes.com/pages/world/index.html. Muchos sistemas de censura puede bloquear una URL única. A veces, una manera fácil de eludir el bloqueo es ocultar la dirección URL. Por ejemplo, es posible agregar un punto después del nombre del sitio, así que la URL se convierte en http://en.cship.org/wiki/URL http://en.cship.org./wiki/URL. Si tienes suerte con este pequeño truco puedes tener acceso a sitios Web bloqueados.

USENET

Usenet es un sistema de foros de discusión de más de 20 años que se puede acceder usando el protocolo NNTP. Los mensajes no se almacenan en un servidor sino en muchos servidores que distribuyen sus contenidos constantemente. Debido a que es imposible censurar Usenet como un todo, sin embargo el acceso a Usenet puede y es a menudo bloqueado. Google dispone de los archivos de historia completa de mensajes de Usenet para realizar búsquedas.

VOIP

VoIP se refiere a cualquiera de varios protocolos de comunicación de voz bidireccional en Internet en tiempo real, que es generalmente mucho más barato que llamar a través de las redes telefónicas de la empresa. No está sujeto a los tipos de intervención telefónica practicada en las redes telefónicas, pero puede controlarse utilizando la tecnología digital. Muchas empresas producen software y equipos para espiar las llamadas de VoIP, la codificación de las tecnologías de VoIP sólo recientemente han comenzado a surgir.

VPN

Una VPN (red privada virtual) es una red de comunicación privada utilizada por muchas compañías y organizaciones a conectarse de forma segura en una red pública. Por lo general el acceso a Internet es encriptado y para que nadie, excepto los extremos de la comunicación puede mirar el tráfico de datos. Existen varias normas, como IPSec, SSL, TLS o PPTP. El uso de un proveedor de VPN es un método muy rápido, seguro y conveniente para eludir la censura en Internet, con poco riesgo, pero por lo general, cuesta dinero cada mes.

LISTA BLANCA

Una lista blanca es una lista de sitios autorizados específicamente para una determinada forma de comunicación. El Filtrado de tráfico se puede hacer por una lista blanca (todo bloqueado menos los sitios en la lista), una lista negra (permitir todo, menos los sitios en la lista), una combinación de los dos, o por otras políticas basadas en las normas y condiciones específicas.

WORLD WIDE WEB (WWW)

La WWW es la red de dominios de hipervínculos y páginas de contenido accesible mediante el Protocolo de transferencia de hipertexto y sus numerosas prolongaciones. La WWW es la parte más famosa de Internet.

WEBMAIL

Webmail es el servicio de correo electrónico a través de un sitio Web. El servicio envía y recibe mensajes de correo electrónico para los usuarios de la forma habitual, pero proporciona una interfaz Web para la lectura y la gestión de mensajes, como una alternativa a la ejecución de un cliente de correo como Outlook Express o Thunderbird en el ordenador del usuario. Por ejemplo, un de los servicios de correo web mas popular y gratuito es https://mail.google.com /

WEB PROXY

Un proxy web es un script que se ejecuta en un servidor Web que actúa como un proxy/gateway. Los usuarios pueden acceder a estos proxy web con su navegador web normal (como Firefox) y escribir cualquier URL en el formulario que encontrará en ese sitio Web. Luego, el programa de proxy Web en el servidor recibe el contenido de la Web y lo muestra al usuario. De esta manera el ISP sólo ve una conexión con el servidor proxy Web ya que no hay conexión directa.

35. LICENSE

36. AUTHORS

ACERCA DE ESTE MANUAL
© adam hyde 2009
Modifications:
Ariel Viera 2009
TWikiGuest 2009

NOCIONES AVANZADAS
© adam hyde 2009
Modifications:
Ariel Viera 2009, 2010
Roberto Rastapopoulos 2010
TWikiGuest 2009

DETECCION Y ANONIMATO
© adam hyde 2009
Modifications:
Ariel Viera 2009
TWikiGuest 2009

RIESGOS
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

PROXIS SOCKS
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

USO DE SwitchProxy
© adam hyde 2009
Modifications:

Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

CREDITOS
© adam hyde 2006, 2007

TECNICAS DE FILTRADO
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

RECURSOS
© adam hyde 2009
Modifications:
Ariel Viera 2009
TWikiGuest 2009

GLOSARIO
© adam hyde 2006, 2007
Modifications:
Ariel Viera 2009

¿ESTOY SIENDO BLOQUEADO?
© adam hyde 2009
Modifications:
Ariel Viera 2009
TWikiGuest 2009

¿COMO FUNCIONA INTERNET?
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

INSTALANDO WEB PROXIES
© adam hyde 2009

Modifications:
Ariel Viera 2009
TWikiGuest 2009

INSTALANDO PHProxy
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

INSTALANDO PSIPHON
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

INSTALANDO SwitchProxy
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

INTRODUCCION
© adam hyde 2006, 2009
Modifications:
Ariel Viera 2009
TWikiGuest 2009

RIESGOS DE OPERAR UN PROXY
© adam hyde 2009
Modifications:
Ariel Viera 2009
TWikiGuest 2009

TUNELES SSH
© adam hyde 2009
Modifications:
Ariel Viera 2009

Roberto Rastapopoulos 2010
TWikiGuest 2009

INSTALANDO UN REPETIDOR TOR
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

TRUCOS SIMPLES
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

TOR - THE ONION ROUTER
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

USO DE TOR CON PUENTES
© adam hyde 2009
Modifications:
Ariel Viera 2009
Douglas Bagnall 2010
Roberto Rastapopoulos 2010
TWikiGuest 2009

USO DE JON DO
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

OPENVPN
© adam hyde 2009

Modifications:
Ariel Viera 2009
TWikiGuest 2009

USO DE PHProxy
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

USO DE PSIPHON
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

USO DE PSIPHON2
© adam hyde 2009
Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

USO DEL PAQUETE TOR DE NAVEGADOR
© adam hyde 2009
Modifications:
Ariel Viera 2009, 2010
Roberto Rastapopoulos 2010
TWikiGuest 2009

USO DEL PAQUETE TOR DE MI
© adam hyde 2009
Modifications:
Ariel Viera 2009, 2010
Roberto Rastapopoulos 2010
TWikiGuest 2009

PROXIES HTTP
© adam hyde 2009

Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

QUE ES UN PROXY WEB?

Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

SORTEANDO EL FILTRADO

Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

QUE ES UNA VPN?

Modifications:
Ariel Viera 2009
Roberto Rastapopoulos 2010
TWikiGuest 2009

QUIEN CONTROLA LA RED?

Modifications:
Ariel Viera 2009
TWikiGuest 2009

Free manuals for free software

37. 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