



Your Freedom

Guía del Usuario

Una introducción gradual y Guía de Referencia para Your Freedom

<https://www.your-freedom.net/>

Version 3.0

Release Date: 2013-06-26

Todas las marcas comerciales mencionadas en esta guía son propiedad de sus respectivos dueños y son solo usadas como referencia ocasional.

La versión más actualizada de esta guía está disponible en nuestro sitio, <https://www.yourfreedom.net/> , en la sección de Documentación. Si encuentra problemas o no puede encontrar en esta versión la información que necesita, por favor verifique si existe una versión más reciente.

Esta guía es © Copyright 2006 - 2013 de resolution Reichert Network Solutions GmbH, Saarbrücken, Alemania. Todos los derechos reservados. Usted puede redistribuir ésta guía tanto en forma electrónica como en papel siempre que la distribuya como un todo y no parcialmente, se abstenga de modificar su contenido y la referencia a su origen se mantenga intacta. Por favor hágale saber a los eventuales destinatarios que esta puede no ser la última versión del documento, pudiéndose encontrar ésta en nuestro sitio.

Introducción

¿Cuál es su libertad?

¿Qué no es?

¿Qué puedo usar?

¿Cómo funciona?

¿Es seguro? Es anónimo? ¿Se compromete mi seguridad? ¿Puedo coger un virus?

¿Cuánto cuesta?

Es su libertad "spyware" o "adware"

¿Cuántos servidores tiene? ¿Son todos iguales?

Obtener introducción

proceso de registro

de instalación del software de que se conecta

cliente por primera vez

en una PC

en un dispositivo Android

aplicaciones Configurar

automáticamente

manualmente

configuración Manual

El diálogo de configuración de su libertad

Iniciar y detener la conexión

Cada usuario sólo puede iniciar sesión en el una

elección de los servidores

ubicación en estos Servidor

Protocolos de

relés CGI

[Conexión de aplicaciones y juegos](#)

[Introducción](#)

[Utilizando "socksifiers"](#)

[Windows](#)

[Linux y otros derivados de Unix](#)

[de Mac OS X](#)

[soporteOpenVPN](#)

[Introducción](#)

[Requisitos](#)

[Las tareas de configuración](#)

[configurar las aplicaciones](#)

[Solución de problemas](#)

[Uso de la libertad sin cliente de aplicaciones](#)

[PPTP](#)

[Generalidades](#)

[Es PPTP segura](#)

[¿Cómo configurar PPTP cuentas:???](#)

[¿Qué pasa si no funciona](#)

[Compartir los de conexión PPTP](#)

[servidores DNS](#)

[más de una conexión PPTP predefinido](#)

[Tipos de actualizaciones basadas en el tiempo y vales](#)

[FreeFreedom \(uso gratuito\)](#)

[Actualizaciones y vales](#)

[vales](#)

[de prueba unidades](#)

[Advanced Topics](#)

[Puerto Delanteros](#)

[Local port forwards](#)

[SIP reenvía](#)

[puerto del servidor reenvía](#)

[ConexiónSharing](#)

[retransmisión](#)

[Con OpenVPN y el ICS para conectar otros PC, Playstation, Xbox, etc](#)

[Will tethering en el trabajo de Android con su libertad?](#)

[IPv6](#)

[Afinarmodo CGI](#)

[Apéndices](#)

[Apéndice A](#)

[Resolución de problemas](#)

[¿Por qué que mi app / juego no funciona? Si realiza](#)

[#una prueba de velocidad #](#)

[Creación de un "vertedero"archivo utilizando](#)

[Escritorio](#)

[Android](#)

[un sniffer de paquetes #](#)

[Actualización de ladel cliente](#)

[información País](#)

[Paísplanes específicos](#)

[disponibilidad del servidor al país](#)

[Tweaks](#)

[El archivo de configuración del cliente de la Libertad su #](#)

[¿Dónde está mi hogar directorio?](#)

[opciones de configuración](#)

Introducción

¿Qué es Your Freedom?

Your Freedom es una aplicación que te permite navegar libremente cuando tu acceso a Internet está siendo restringido. Incluso si te encuentras en un lugar donde la conectividad a Internet es mediante un punto de acceso público y no tienes credenciales para acceder. Aun cuando las técnicas que usa para burlar estas restricciones son bastante complejas, Your Freedom no resulta difícil de usar.

Your Freedom consiste en Servicio de Conectividad que permite sortear restricciones impuestas sobre el uso de Internet ya sea por parte de administradores de red, proveedores o el hecho de vivir en algún país determinado. También brinda cierto nivel de anonimato además de mantener en privado lo que haces mientras navegas.

El funcionamiento de Your Freedom se basa en convertir a la PC en un **Proxy Web** y/o **SOCKS**. Éste permite a las aplicaciones conectarse a servidores en Internet sorteando Proxys o firewalls que se interpongan. En vez de conectarse directamente, las aplicaciones tramitarán sus conexiones a través de Your Freedom. En su lugar, el cliente Your Freedom se conecta a algún servidor Your Freedom a través de un **protocolo de conexión** que no esté restringido en tu entorno de red. Esta es además una forma transparente que no requiere configurar ninguna aplicación, y sobre dispositivos **Android**, Your Freedom trabajará sin ninguna configuración adicional.

Your Freedom tunnels trata todo el tráfico a través de un túnel que pasa de largo firewalls, proxys Web, DNS servers y cosas por el estilo. Suena complicado y en verdad lo es, pero la buena noticia es que ¡no tienes que ocuparte personalmente de los detalles! Your Freedom se encarga.

¿Qué no es?

Your Freedom no es una red privada virtual (VPN). No brinda ninguna conexión a red privada alguna, solo a Internet. Algunos lo llaman un software VPN pero el es realmente una solución de conectividad.

Your Freedom **tampoco es una solución de firewall**, su objeto es más bien burlarlos, no ser uno de ellos. Tampoco hará tu PC más segura, pero ese no es un asunto del que debemos preocuparnos, siempre hay gente trabajando en la tarea de velar por tu seguridad.

Your Freedom **no es un anonimizador perfecto**. Este servicio brinda cierto nivel de anonimato escondiendo tu IP; desde el punto de vista del servicio al que queremos acceder, la petición tiene la apariencia de haberse originado desde uno de los servidores de Your Freedom. Your Freedom sin embargo, no puede protegerte de tus propios errores o de las fallas en los protocolos de las aplicaciones que usamos. Serás anónimo a menos

que cometas errores.

Your Freedom **no acelerará tu conexión a internet**. No proveerá compresión de datos y no mejorará la velocidad de tu conexión a internet en manera alguna. De hecho, hay cierto procesamiento adicional requerido para realizar el túnel que hará la conexión más lenta.

¿De qué nos sirve Your Freedom?

Podemos usar Your Freedom para librarnos de:

- **Restricciones de protocolos**

Si no podemos usar ciertas aplicaciones o servicios porque éstas no pueden conectarse a Internet por la vía usual, YF puede ayudarnos. Por ejemplo, si nuestro juego en línea preferido no trabaja en nuestra red porque alguien decidió que no podíamos jugarlo, lo podremos hacer a través de Your Freedom. Entre los juegos que funcionan bien con Your Freedom están WOW, EVE, Counterstrike y muchos más.

Si se nos está vedado usar protocolos P2P porque alguien piensa que es ilegal. La mayoría de los clientes P2P trabajan bien con YF, y podemos incluso conseguir un puerto servidor, que nos dará un "id alto".

- **Censuradores**

Si no podemos visitar ciertas páginas Web. YF Convierte nuestra PC en un Proxy Web sin restricciones que nos da acceso a todas las páginas Web accesibles, o a acceder transparentemente a Internet.

- **Restricciones temporales**

Se han reportado casos de algunos que han logrado librarse de las restricciones de tiempo. En la mayoría de éstos casos las conexiones establecidas se respetan y no se desconectan a la fuerza una vez terminado el plazo de tiempo. Es por eso que Your Freedom permite hacer ese tipo de cosas, porque establece una conexión que no termina hasta que el cliente Your Freedom se haya desconectado (si no ocurre nada fortuito).

- **Restricciones de Acceso**

Si tu conexión a Internet (mediante un punto de acceso o una instalación similar) pero no necesitas una identificación que no tienes, nosotros probablemente seamos capaces de conseguirte total conexión.

¿Cómo funciona?

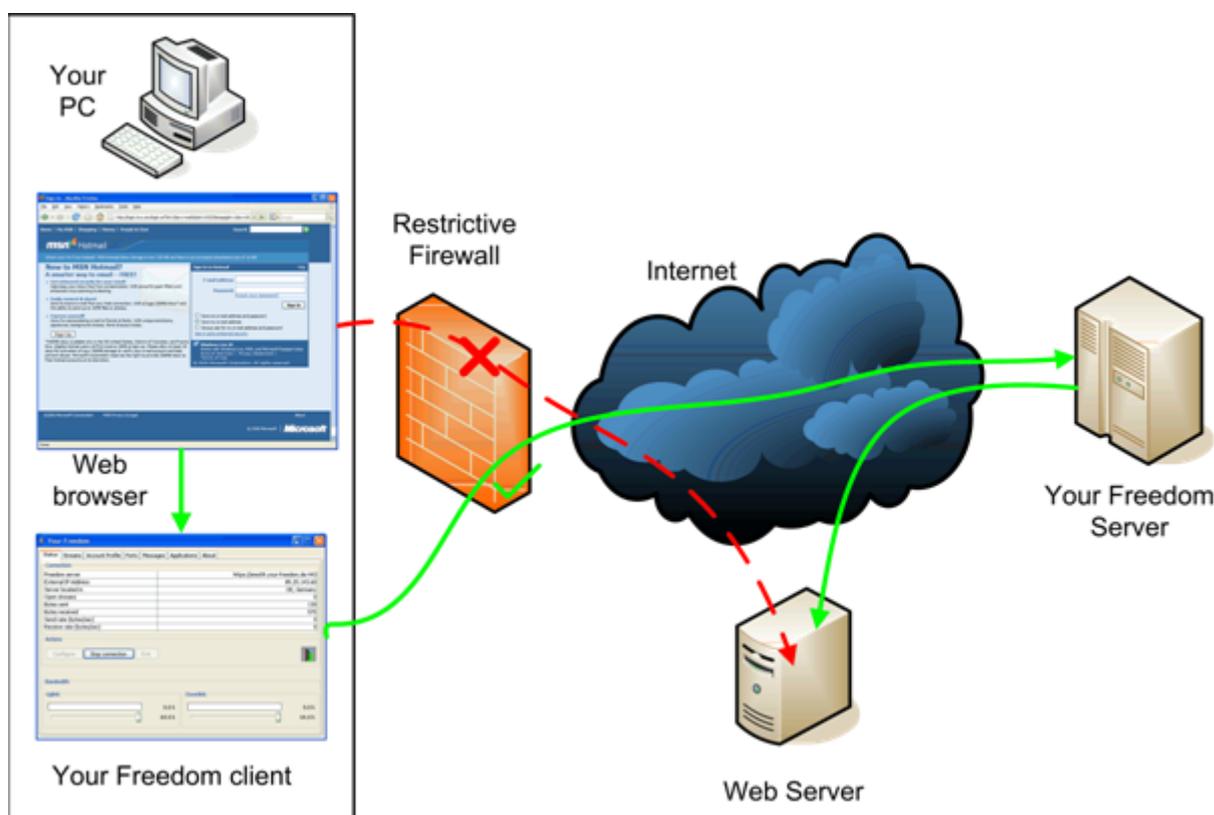
Ejecutamos el cliente Your Freedom en nuestra PC. El cliente es un programa escrito en Java y debe funcionar en cualquier sistema operativo sin necesidad de privilegios de administración. También es posible descargar un instalador para los que no tengan Java instalado, en cuyo caso si necesita privilegios de administración.

Si usas Android, solo instala nuestra aplicación Your Freedom, y ejecútala.

El cliente Your Freedom se conecta a un servidor Your Freedom a través de alguno de los protocolos de conexión disponibles. En la mayoría de los casos se trata de una conexión

HTTP o HTTPS a través de un Proxy Web o una conexión FTP. En muchos lugares puede también usarse UDP o ICMP ECHO. Casi todo el mundo dondequiera puede usar el modo DNS.

En la siguiente figura se ilustra el esquema: la caja a la izquierda es nuestro ordenador. Supongamos que un firewall con restricciones nos impide acceder a hotmail.com. Si queremos leer nuestro correo desde donde estamos solo tenemos que ejecutar el cliente Your Freedom y hacerlo conectar a uno de los servidores Your Freedom, seguido configuramos el navegador para que use nuestra PC como Proxy. Desde este momento podremos conectarnos libremente a hotmail.com usando el cliente Your Freedom el cual tramitará las peticiones HTTP a través de los servidores de Your Freedom, los que finalmente se conectarán a hotmail.com. Las respuestas desde el servidor Hotmail tomarán el mismo camino pero en sentido inverso.



Este es solo un escenario simple más ilustra que el cliente y el servidor Your Freedom actúan como pasos intermedios en la conexión de las aplicaciones.

¿Es seguro? ¿Es anónimo? ¿Compromete mi seguridad? ¿Corro riesgo de infectarme?

Conectarse a Internet via Your Freedom es menos peligroso que hacerlo a través de una conexión de acceso telefónico. Mientras no configures ningún redireccionamiento de puerto de servidor, nadie podrá conectarse a tu PC por esa vía. Cuando se descarga algún ejecutable de Internet (ya sea intencionalmente o no), existe un cierto grado de riesgo, el

mismo que existe cuando te conectas por algún otro medio a Internet y descargas datos desde ahí. Sin embargo, es posible que en tu empresa o en donde quiera que estemos, se apliquen mecanismos de protección sofisticados que Your Freedom no brinda (Ej. chequeo de virus en las descargas desde servidores de Internet). En estos casos es en verdad menos seguro. Pero tomemos en cuenta que es menos seguro precisamente porque permite hacer cosas que de otro modo no se podrían. La protección más segura de los peligros de Internet es estar totalmente desconectado. Estaríamos seguros, pero solos.

Your Freedom no es un anonimizador perfecto, solo permite ocultar nuestra IP, a menos que la aplicación lo comunique por el protocolo que ésta usa. Los administradores de los servicios que accedes no podrán ver de donde te conectas, en su lugar verán la dirección IP del servidor Your Freedom. No se tomarán medidas adicionales para asegurar nuestro anonimato, no se eliminan cookies, tampoco se "limpiarán" los encabezamientos de las peticiones que envían los navegadores.

Para una mayor privacidad, el servicio ofrece **niveles elevados de cifrados** usando el estándar de cifrado AES, que usa llave pública/privada, y fuertes llaves de sesión. Para mayor información puede consultar nuestra página Web en <https://www.your-freedom.net/?id=encryption> (necesita estar logueado). A menos que deshabilite explícitamente el cifrado, usted estará a salvo de intrusos.

Respecto a los virus: no hay ningún mecanismo de protección contra virus incorporados en los contenidos que accedemos y por tanto, no se ofrece protección contra virus. Por favor instale un software antivirus en su PC o móvil; deberá encargarse de esta tarea.

¿Cuánto cuesta?

Un servicio elemental (FreeFreedom) se proporciona gratuitamente. Se limita en el ancho de banda y el número de conexiones simultáneas, además se limita el tiempo de conexión (aunque podemos volver a conectarnos inmediatamente). Diariamente el tiempo de uso es limitado a 2 horas, y semanalmente el tiempo de uso es limitado a 5 horas. Algunos de nuestros servidores no están disponibles para usuarios FreeFreedom. Si esto es suficiente para usted, puede ser hacer uso del mismo.

Se ofrecen actualizaciones que eliminan toda restricción de tiempo de uso, que incrementan o eliminan la restricción de ancho de banda y que permiten más conexiones simultáneas, y además se ofrecen puertos de servidor que nos permiten aceptar conexiones entrantes desde Internet hacia nuestra PC o hacia otra PC en la misma red, si lo desea. Las actualizaciones están disponibles por un mes, tres meses, seis meses o doce meses, y vienen en tres diferentes niveles: BasicFreedom, EnhancedFreedom, y TotalFreedom. Como alternativa a las actualizaciones por tiempo, existen los carnets vouchers. Los vouchers pueden ser usados para mejorar temporalmente las prestaciones del perfil de Your Freedom sin tener que pagar por un mes completo y malgastar partes de éste. Para más detalles ver capítulo 4 esta guía.

¿Es Your Freedom “Spyware” o “AdWare”?

Your Freedom no contiene ningún código para espiar o causar molestia alguna (excepto la restricción del servicio FreeFreedom, que está ahí, por supuesto, para convencernos de los beneficios de comprar una actualización). No se publica el código fuente porque mucho del código está también incluido en el servidor y no se quiere exponer. También, esa sería una forma de ayudar innecesariamente a aquellos que desarrollan aplicaciones para bloquear Your Freedom.

Para la privacidad de nuestros clientes los servidores Your Freedom no registran nada excepto aquello legalmente y técnicamente necesario – y permitido por la ley. De hecho, la conexión a los servidores no guardan registro alguno que no sea de interés exclusivo de los desarrolladores y operadores (Estos solo contienen elementos como cargas realizadas en el servidor y excepciones ocurridas en las operaciones) todos los registros con información de nuestros clientes están guardados a salvo en un servidor en Alemania. No obstante nosotros cooperaríamos con las autoridades en Alemania hasta el grado requerido para protegernos de que se emprendan acciones legales contra nosotros. Esto puede significar que tengamos que revelar datos de tu cuenta y detalles de pago así como la IP desde donde te conectas si así lo requiriesen las autoridades.

Nosotros no registramos lo que nuestros clientes acceden en internet. *Las regulaciones de telecomunicaciones alemanas ni siquiera permiten esto.* Si registramos el hecho de que se haya accedido a nuestro servicio desde tu dirección (si pudiésemos! En modo DNS, normalmente no podemos), 16 bits más bajos de la dirección IP (no toda la dirección IP, solamente los 2 últimos números) y datos estadísticos acerca del uso para contabilidad y aseguramiento. Ésta información se almacena como regla general por solo unos días y nunca por mas de 4 semanas. Esta información no se utiliza en manera alguna excepto para análisis estadístico, depuración, contabilidad y para combatir violaciones de los términos de uso, y en los casos en que las autoridades en Alemania lo requieran. Nosotros nunca proporcionaremos ningún dato a entidades privadas o regímenes opresores.

Existe una consola de control en los servidores que les permite a los técnicos explorar la actividad de los servidores. Muy útil para detectar posibles problemas técnicos que estén experimentando los usuarios.

Puedes estar diciendo “Otros me ofrecen el mismo servicio y no llevan registro de todo”, Bien, ellos o son ingenuos o están mintiendo. Nuestros competidores también necesitan protegerse contra maltratos, y solamente pueden hacerlo si tienen tus datos. Nosotros decidimos ser honestos contigo.

¿Cuántos servidores hay en total? ¿Se comportan igual todos los servidores?

Este punto está sujeto con frecuencia a cambios. En el momento en que se escribe esta guía tenemos 23 servidores online distribuidos en 9 países. Todos brindan el servicio de una navegación básica y chateo, solo algunos rechazarán conexiones P2P (específicamente, los que están localizados en Norteamérica) de acuerdo a nuestras

políticas de privacidad. Algunos pueden manejar más tráfico que otros. Hay una página de estadísticas disponibles en <https://www.your-freedom.net/?id=servers> . Los servidores que no están en el grupo "P2P" no están capacitados para permitir aplicaciones P2P, los servidores que no están en el grupo "volume" no son adecuados para permitir transferencias de fichero grandes, etc. (la clasificación es bastante intuitiva).

Todos podemos usar los servidores en el grupo "Free", los otros son reservados para clientes Premium. En este momento todos los servidores están en este grupo, pero esto puede cambiar. Algunos servidores no están disponibles para aquellos usuarios que se tratan de conectar desde ciertos países, o solo están disponibles para usuarios que se conectan desde ciertos países. El cliente Your Freedom notificará al usuario en cada caso con un mensaje "Authentication not valid for your contry of residence". Si esto sucede, deberemos tratar de conectarnos a otro servidor. Solamente hacemos esto para protegernos.ej.: no siempre, si podemos evitarlo.

En la página de estadísticas se muestra la carga del servidor. Mientras mayor el número más cargado está. Una carga por debajo de los 40000 es considerada baja, cargas superiores a los 125000 se consideran altas, números altos indican un servicio sobrecargado. En esa página se utiliza un esquema de semáforos para indicar el estado de los servidores. Una luz "verde" indica que el servidor está bien y que puede aceptar conexiones. Una luz "amarilla" indicaría que el servidor está en buen estado pero está algo sobrecargado y probablemente el servicio a través de él no sea el mejor (en la práctica el servicio suele ser igual de bueno). Una luz roja indica que el servidor está fuera de servicio.

Primeros pasos

¿Cómo suscribirse?

Lo primero que tenemos que hacer para usar el servicio es **suscribirnos al mismo en el sitio Web**. Visítenos en <https://www.your-freedom.net/> y cree una cuenta allí. Existe un vínculo en la parte roja del banner debajo del formulario de entrada de nombre de usuario y contraseña.

En la página de suscripción, escogeremos un nombre de usuario (preferiblemente uno que sepamos que no esté en uso) y una contraseña. Es conveniente que ésta última sea relativamente larga, por nuestra propia protección. Tanto el nombre de usuario como la contraseña pueden contener letras mayúsculas o minúsculas, dígitos, guiones y guiones bajos; otros caracteres pueden también servir pero no es una buena idea probar. El único campo requerido es la dirección de correo (los demás no son obligatorios), no debe completarse con tonterías si no se quiere dar la información. Muchos de estos campos están aún ahí probablemente porque no se han tomado el trabajo de quitarlos, si no desea llenarlos los puede dejar en vacíos. Usted siempre podrá hacerlo en otro momento.

Una vez que se haya completado todo, se debe dar clic en el botón “Create account”. Se requerirá que confirmemos la información que introdujimos antes dando clic en “Create account now”. Si existe algún error en su información, aparecerá un mensaje en rojo indicándole el campo incorrecto, corríjalo e intente nuevamente.

A los pocos minutos recibiremos un correo donde estarán presentes los datos de la suscripción y un vínculo de activación. Si la dirección está protegida con medidas anti-spam deberán ser flexibilizadas para que puedan llegar los correos desde your-freedom.net. Activaremos la cuenta dando clic en el vínculo (o abriéndolo en un navegador). Si no se ha recibido ningún mensaje o no se puede culminar el proceso de suscripción por cualquier otro motivo entonces se deberá enviar el nombre de usuario en un correo a soporte@your-freedom.net, pidiendo que se le active la cuenta y de paso relatando con detalles lo sucedido. Indíquenos el usuario escogido por usted, pero no su password.

En caso de **no poder accederse a la página Web porque esté bloqueada** estaríamos en un caso del tipo del problema del huevo y la gallina. En este caso podría procederse a conectarse al sitio a través del cliente your-freedom con el usuario “unregistered” y contraseña “unregistered”. Ésta cuentasólo dará acceso a la página Web de Your Freedom. Otra alternativa sería mandar un correo al soporte técnico, solicitando crear una cuenta. La dirección es soporte@your-freedom.net, se deberán incluir todos los datos de la cuenta y la explicación del problema para suscribirse (será preferible que el nombre de usuario y la contraseña solo contengan letras, dígitos y guiones bajos). Si queremos recibir el cliente una instalación del cliente YF por email solo debemos escribir un correo en blanco a get@your-freedom.net; enseguida se nos enviará un correo con instrucciones sobre como proceder. Si después de todo no se puede conseguir una versión del cliente podemos escribir una carta por correo y se nos enviará un CD.

Instalando el software cliente

Una vez que dispongamos de una cuenta ésta puede usarse para registrarse en el sitio. Esto dará acceso a la sección de descargas. Existen muchas maneras de ejecutar el cliente Your Freedom y por consiguiente existe más de una versión para descargar:

- **Instalador para Windows**

Para instalar esta versión necesitamos de una instalación apropiada del entorno de ejecución de java (JRE)[2] y tener los privilegios suficientes para instalar software en nuestra PC. La descarga se lleva aproximadamente 1Mb. Si por alguna razón no estuviésemos habilitados para descargar ejecutables también puede accederse bajo la extensión .txt. Una vez descargado en su PC, renombre el fichero a extensión .exe y listo.

- **Instalador completo para windows**

Ésta versión viene empaquetada con su propio JRE, por tanto no tiene prerequisites. Cualquier usuario de Windows debe poder ejecutar esta versión, siempre que tenga derechos a instalar software en su ordenador. Ésta descarga es algo voluminosa (14 Mb). Si por alguna razón no estuviésemos habilitados para descargar ejecutables también puede accederse bajo la extensión .txt. La ventaja de esta versión es que está compilada a código nativo y probablemente necesite menos recursos.

Ambas versiones se instalan ejecutando el fichero .exe. Solo han de seguirse las instrucciones del instalador y estará listo en par de minutos. Si vamos a instalar una versión más nueva **debemos antes desinstalar la anterior**. Una vez que el cliente esté instalado vayamos directo a la sección 2.3.

Para aquellos que no pueden instalar software en sus PCs o que no son usuarios de Windows está la versión **archivo de Java**. Solo es necesario descargar el fichero ZIP y extraer su contenido en una carpeta donde existan derechos de escritura (también puede ser una memoria flash o un CD). Seguido ejecutamos el intérprete de java con fichero freedom.jar. En Windows suele ser suficiente con hacer doble clic encima del jar, pero puede que se necesite abrir una ventana de comandos, cambiar la carpeta actual con "cd" hasta la carpeta donde yace el contenido del zip y ejecutar "java -jar freedom.jar". En sistemas tipo Unix, normalmente se puede usar "java -jar freedom.jar", "kaffe -jar freedom.jar" o algo similar. Los usuarios de Unix normalmente están familiarizados.

De modo general, la versión archivo de Java del cliente YF deberá ejecutarse en toda computadora con un JRE apropiado y suficiente memoria.

También ofrecemos un instalador para **Mac OSX**. Aún cuando las ediciones de Mac OSX traen empaquetado un JRE, hay versiones como Leopard que vienen con la versión 1.5 que ya no es soportada, por lo que puede ser necesario instalar JRE 6 o 7. Instrucciones adicionales para Mac OSX y otros sistemas operativos pueden consultarse en la sección de documentación en nuestro sitio web.



El cliente YF solo funciona con Java 6 y no Java 5. Leopard no viene con Java 6 pero éste se puede descargar desde <http://developer.apple.com/java/download/> (descargar “Java for Mac OS X 10.x Update (o lo que sea)”). Una vez instalado, Java 5 sigue siendo el predeterminado. El instalador que proveemos debe ser capaz de asegurar que la versión correcta sea tomada; si ésta no funciona deberemos cambiar la versión predeterminada: Abrimos el Finder, vamos a Aplicaciones, Utilidades, Java, “Java Preferences”. Movemos “Java SE 6” al tope de la lista.

- **Android APK**

La aplicación Android solamente puede ser ejecutada **sobre Android 4.0 o dispositivos con versiones superiores** a esta. Versiones anteriores de Android no son soportadas, no importa si su móvil es nuevo o no. Esto se debe a que versiones anteriores no incluyen la necesaria implementación de la API VPN. Si no está seguro de su versión de Android, consulte la opción de configuración, vaya a “Sobre el Móvil” y verifique ahí la “versión de Android”. Si esta es 1.x, 2.x o 3.x, entonces la aplicación Your Freedom no podrá ser ejecutada en su móvil. Puede consultar con su fabricante la actualización de su versión. Le sugerimos que también consulte <http://www.cyanogenmod.org/>.

Recomendamos que configure su dispositivo para **permitir la instalación de aplicaciones desde fuentes externas**; esto le permitirá descargar e instalar la aplicación desde nuestro sitio y recibir las actualizaciones correspondientes. Consulte la opción de configuración, vaya a la sección de Seguridad, en la sección de “Administración de Dispositivos” y marque “Fuentes Desconocidas”. Esto no pone en riesgo su dispositivo. Ahora puede descargar el fichero Your Freedom APK u obtenerlo mediante su correo electrónico (escribanos a get@your-freedom.net e indique como asunto “Android”). Haga click en la aplicación y siga el procedimiento de instalación.

También puede realizar la búsqueda de la aplicación “Your Freedom” en Google Play. Esto le ofrece beneficios adicionales como poder configurar las descargas automáticas de las actualizaciones.

Accediendo por vez primera

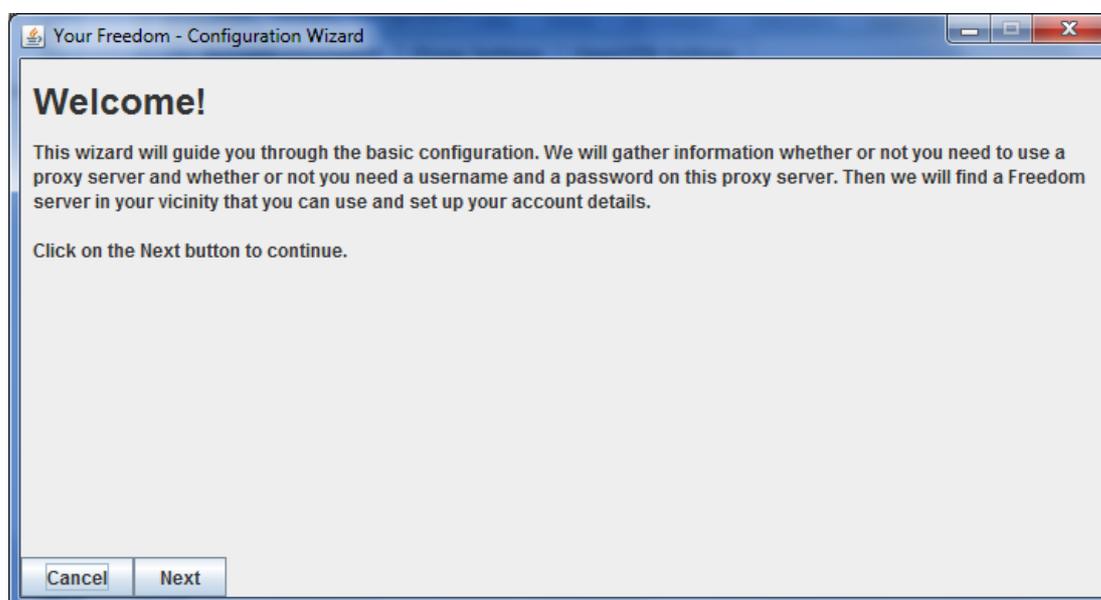
Desde una PC

Cuando se inicia el cliente YF por vez primera, éste preguntará por el idioma por defecto. El idioma que escojamos será el de la interfaz de usuario. Ésta configuración se puede restablecer más tarde.

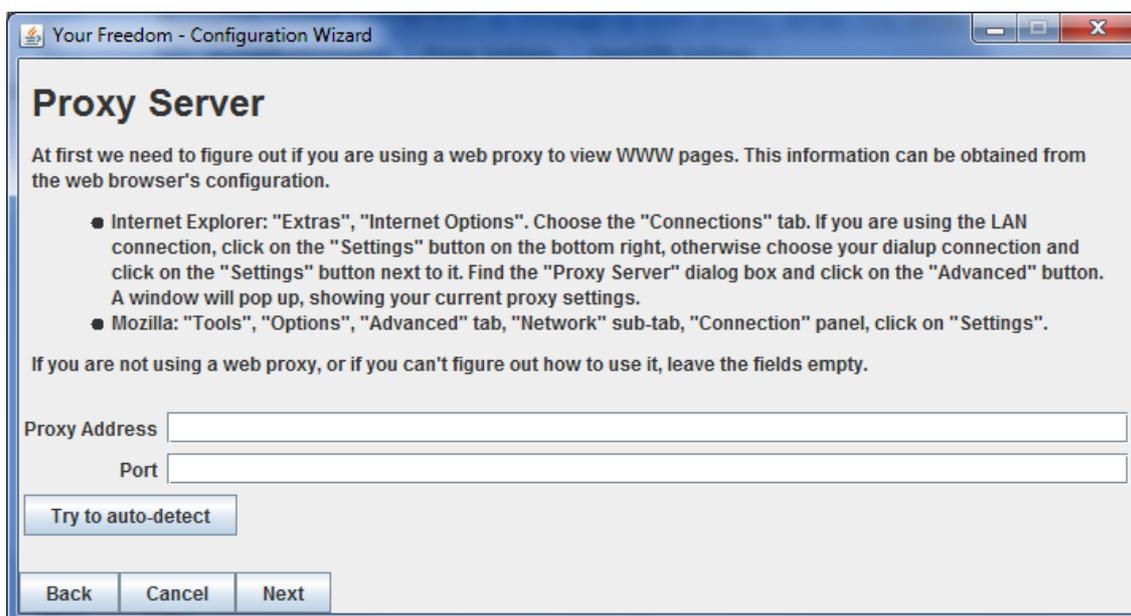


Después de escojamos el idioma de nuestra preferencia se mostrará un “Asistente”. No es obligatorio pero ante la duda recomendamos usarlo. La configuración manual puede ser requerida en escenarios donde la conexión es difícil, véanse los capítulos 2.5 página 27 para más detalles.

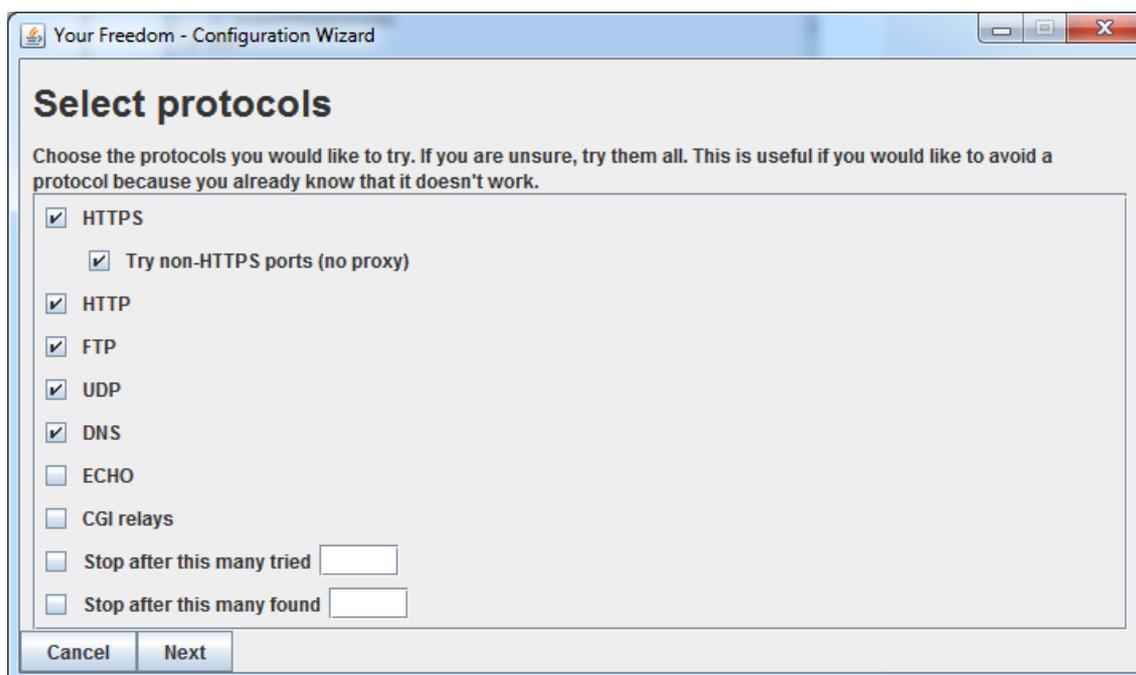
Cuando se abra el asistente veremos una pantalla de bienvenida:



Procedemos haciendo clic en el botón “Siguiente”. Nos encontraremos:



Si la conexión es a través de un proxy, éntrense los detalles aquí. Si no estamos seguros demos clic en “Siguiente” por ahora.

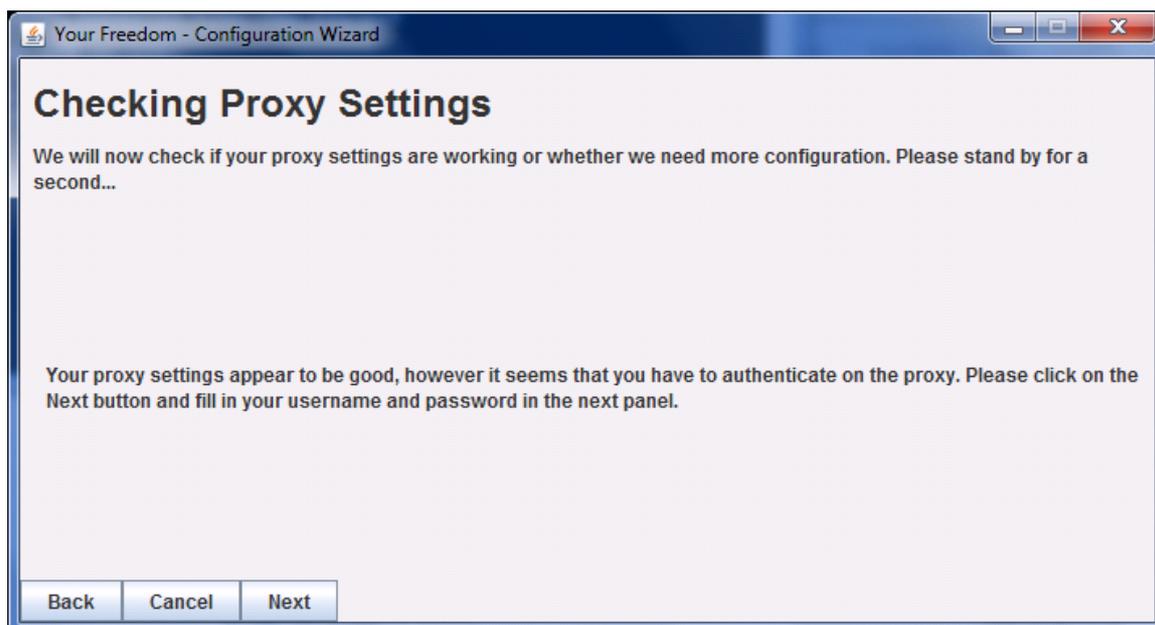


Encontraremos una ventana pidiéndonos que seleccionemos los protocolos a usar para efectuar la conexión a los servidores YF. Los protocolos seleccionados afectarán el modo en que el asistente chequeará la conexión con los servidores. En dependencia de la plataforma y si están ejecutando Your Freedom como administrador, es posible que algunos modos de conexión no se encuentren disponibles. (Este es un requisito para el modo ECHO). Si no estamos seguros dejémos la selección por defecto y damos clic en “Siguiente”:

Si todo lo que percibimos es una lista vacía como ésta:

tendremos que averiguar cuál es la configuración del proxy web (o quizás configurar todo manualmente, como en el caso que quisiéramos usar un proxy FTP).

Si en cambio obtenemos esto,

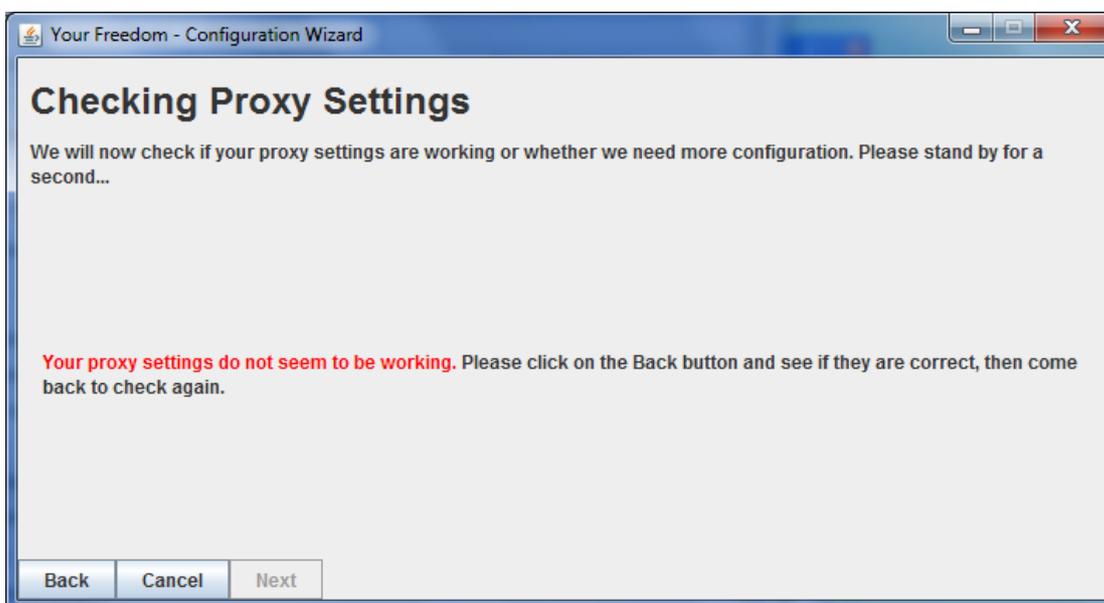


Entonces los detalles del proxy son correctos pero necesitamos las credenciales para autenticarnos. Démos clic en "Siguiente"...

The screenshot shows a window titled "Your Freedom - Configuration Wizard". The main heading is "Proxy Server Authentication". Below the heading, the text reads: "Your proxy server requires you to authenticate by supplying a username and a password. Please enter these values in the fields below. If you have no idea what to supply there, try your Windows domain username and password, and if that does not work, fill in your windows domain as well or try to prepend it to the username with a backslash. If all fails, ask a knowledgeable person around you." Below this text, it says: "When done, click on Next to check." There are three input fields: "Proxy Username", "Proxy Password", and "Proxy Domain". At the bottom of the window, there are three buttons: "Back", "Cancel", and "Next".

E introducimos las credenciales de autenticación correctas. En muchos casos éstas coincidirán con nuestras credenciales del dominio de Windows (y puede ser necesario que pongámos el dominio también). Intentémoslo hasta que funcione, démos clic en "Siguiente" para intentarlo.

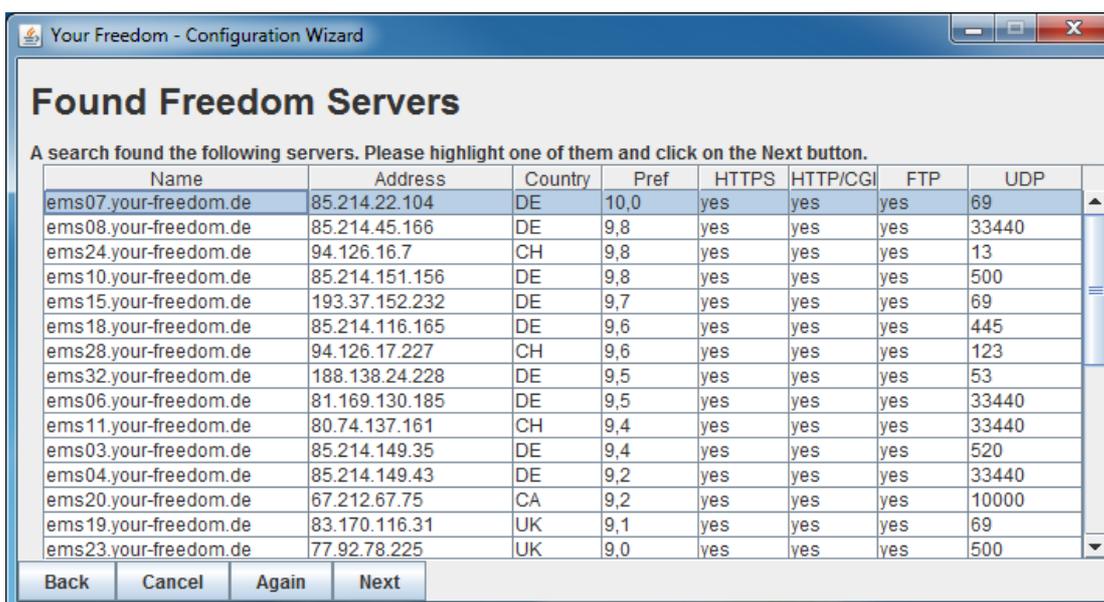
Si nos encontramos con esta página:



es que no hemos introducido correctamente las configuraciones de proxy. Demos clic en “Atrás” y modifiquemos el hostname/dirección IP y/o el puerto. Muchos proxis utilizan los puertos 80, 3128 u 8080. Se puede tomar como referencia la configuración de nuestro navegador.

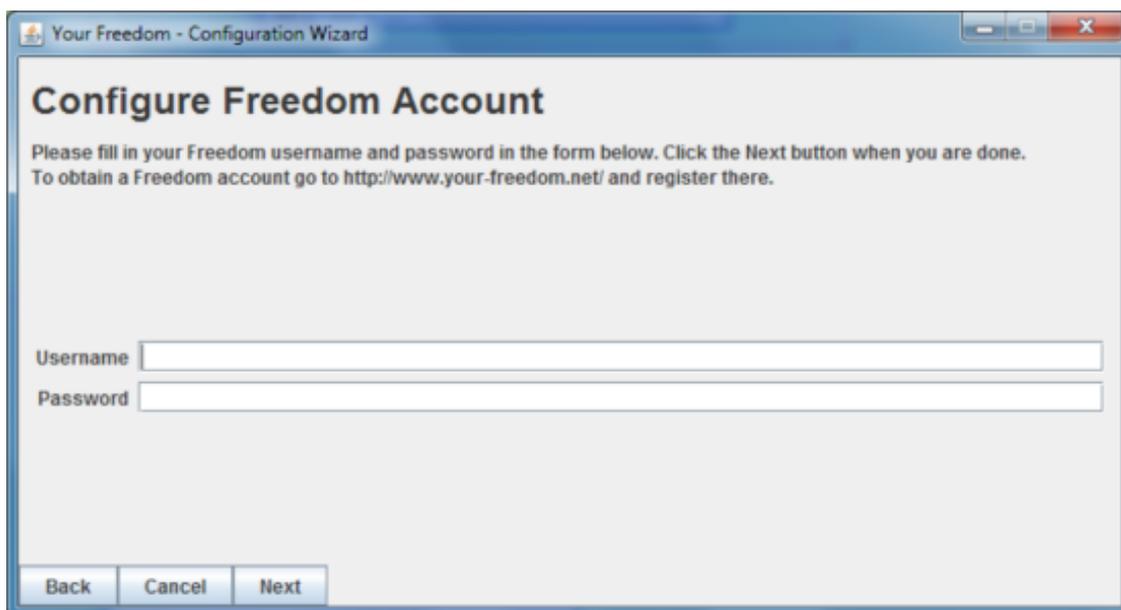
Si notamos que el wizard ha completado los detalles del proxy automáticamente es porque el cliente Your Freedom está preparado para importarlas automáticamente del registro de Windows.

Si no logramos hacerlo funcionar deberemos preguntarle a alguien cercano ducho en detalles técnicos). Si vemos algo como esto significa que funcionó:



Es importante que veamos algún “Si” en algunas de las columnas HTTP, HTTPS FTP o UDP. Un “Si” significa que el cliente ha sido capaz de usar este protocolo para conectarnos al servidor usando los puertos por defecto. Un número significa que fue capaz de

conectarse pero utilizando un puerto diferente y un “no” significa que el protocolo no pudo ser usado para establecer una conexión con el servidor. Los resultados están ordenados por preferencia (un número entre 0 y 10), indicando cuando apropiado resulta el servidor según nuestros requerimientos. Escojámos un servidor y demos clic en “Next”.



Your Freedom - Configuration Wizard

Configure Freedom Account

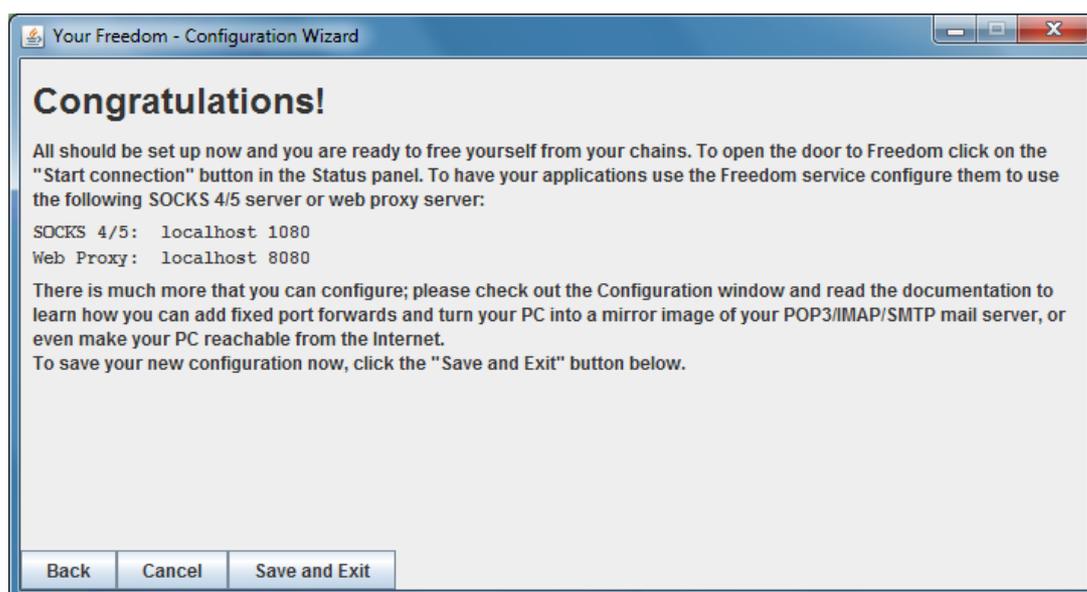
Please fill in your Freedom username and password in the form below. Click the Next button when you are done. To obtain a Freedom account go to <http://www.your-freedom.net/> and register there.

Username

Password

Back Cancel Next

En esta página introduciremos nuestras credenciales para conectarnos a Your Freedom. Demos clic en “Proximo”.



Your Freedom - Configuration Wizard

Congratulations!

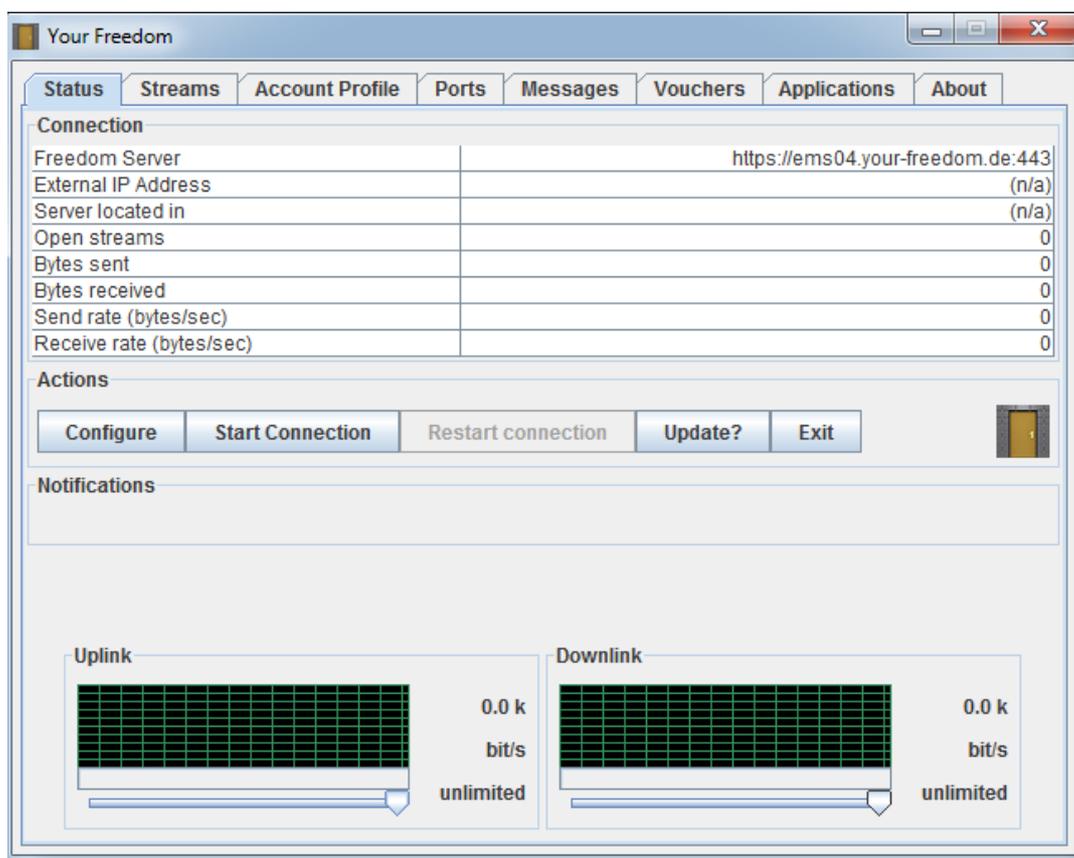
All should be set up now and you are ready to free yourself from your chains. To open the door to Freedom click on the "Start connection" button in the Status panel. To have your applications use the Freedom service configure them to use the following SOCKS 4/5 server or web proxy server:

SOCKS 4/5: localhost 1080
Web Proxy: localhost 8080

There is much more that you can configure; please check out the Configuration window and read the documentation to learn how you can add fixed port forwards and turn your PC into a mirror image of your POP3/IMAP/SMTP mail server, or even make your PC reachable from the Internet. To save your new configuration now, click the "Save and Exit" button below.

Back Cancel Save and Exit

Hemos terminado. Optemos por “Salvar y salir”. La ventana del cliente Your Freedom se verá así:



Es de señalar que el cliente no conoce ningún dato sobre el servidor ni sobre el perfil del usuario Your Freedom antes de conectarse al servidor, por eso es que algunos de los valores están en cero o simplemente vacíos: (incluyendo en ancho de banda- éste no es ilimitado a menos que hayamos comprado un paquete).

Presionemos “Conectar” y veremos algo así en unos pocos segundos:

The screenshot shows the 'Your Freedom' application window with the following details:

Connection	
Freedom Server	https://ems04.your-freedom.de:443
External IP Address	81.169.154.27
Server located in	DE, Germany
Open streams	0
Bytes sent	570
Bytes received	599
Send rate (bytes/sec)	0
Receive rate (bytes/sec)	0

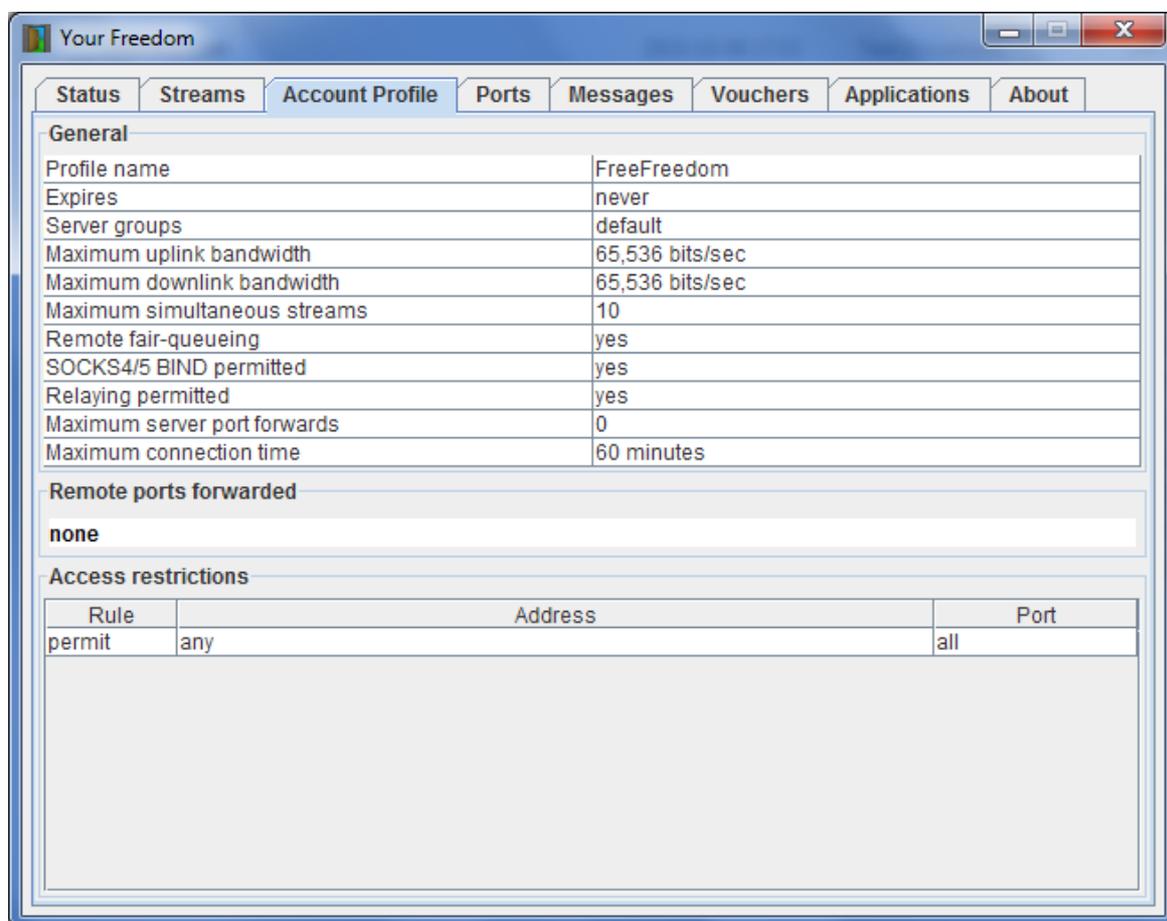
Actions: Configure, Stop connection, Restart connection, Update?, Exit

Notifications:

Uplink: 0.0 k bit/s, unlimited

Downlink: 0.0 k bit/s, unlimited

Nótese que se encuentran detallados los datos de nuestro perfil y que bajo el letrero de ancho de banda se lee “64.0k”. Es más o menos la velocidad de una conexión ISDN, un poco más rápido que un MODEM de alta velocidad. Seguido demos clic en Demos clic en “Perfil de Cuenta”:



Éste panel contiene los detalles de nuestra cuenta. Sin un paquete no podremos acceder a los servidores especiales (solo los servidores por defecto), nuestro ancho de banda es limitado y nuestro máximo número de conexiones simultáneas es más bien limitado, tampoco podremos servir de Proxy para otros. Nuestra conexión con el servidor será terminada después de 60 minutos (pero podremos reconectarnos cuando esto pase). No hay puertos de servidor asignados. Pero al menos no hay restricciones de acceso, podremos acceder a todo cuanto hay en Internet.

Si estamos usando el protocolo HTTP para conectarnos y nuestra conexión no parece trabajar bien del todo, se deberá intentar con el modo POST o CGI(ver configuración manual capítulo2.5página27).

Bien, es tiempo de configurar nuestras aplicaciones. Haremos referencia al capítulo 2.4 página19 para aprender como hacer esto. Una vez que hayamos configurado al menos un navegador para que use Your Freedom habremos logrado el principal objetivo: somos libres de acceder a la Web.



Si la versión del cliente YF que estamos usando está muy desactualizada, podremos chocar con el mensaje *client [is] too old*. Esto significa que debemos actualizar nuestra versión del cliente YF porque la nuestra ya no está soportada. El modo recomendado es descargar la última versión, desinstalar la versión anterior e instalar la nueva.

Sobre dispositivos Android

Seleccione el icono que se muestra a la derecha, e inicie la aplicación de Your Freedom. Verá un banner de bienvenida similar al que se muestra a la derecha con una breve explicación de los elementos más importantes. Repase todas las instrucciones (recomendamos que lea hasta el final) y haga click en “OK” o “Use Asistente”.

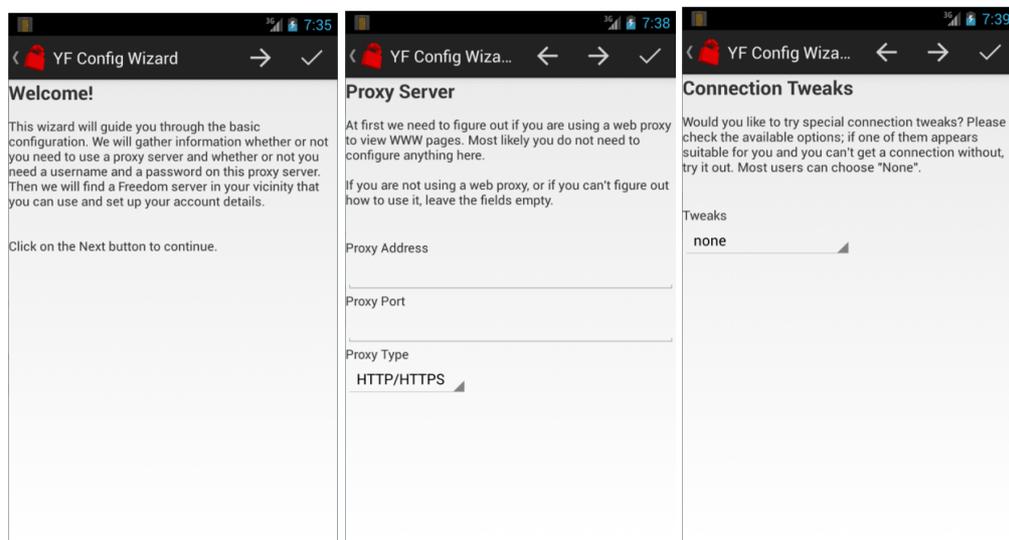


Sugerimos que elija “Use wizard”. (Si presionó “OK”, haga click en el botón Configuración en la esquina superior derecha y elija “Exit” para comenzar nuevamente). En este punto la aplicación le guiará a través de los pasos iniciales de instalación. Cuando haya completado la información solicitada, pase al próximo paso haciendo click la flecha que indica la derecha siguiente. Siempre podrá regresar al paso previo haciendo uso de la flecha a la izquierda que indica el paso anterior. Si la configuración a sido completada, puede hacer click en la marca de OK.

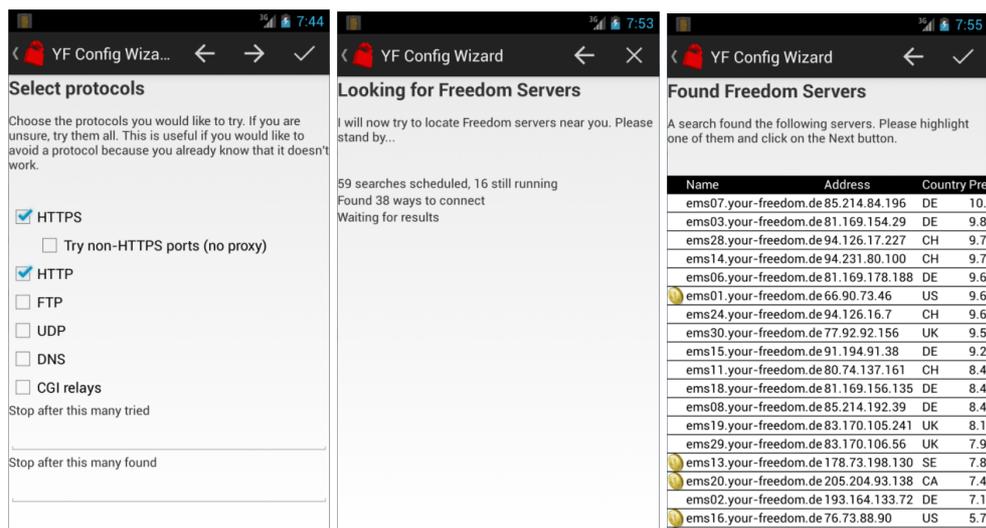


Si usted necesita configurar un servidor proxy, escriba la dirección ip o el nombre del DNS y su puerto, y si es un proxy SOCKS seleccione el tipo correspondiente. La aplicación le indicará si necesita o no credenciales de autenticación, en tal caso, deberá indicarlos.

Tenemos algunos “Tweak” útiles para algunos países y/o redes. Si usted se encuentra entre ellos, seleccione la mejor opción en la próxima página. Siempre podrá regresar a esta página de configuración para hacer uso de esta opción



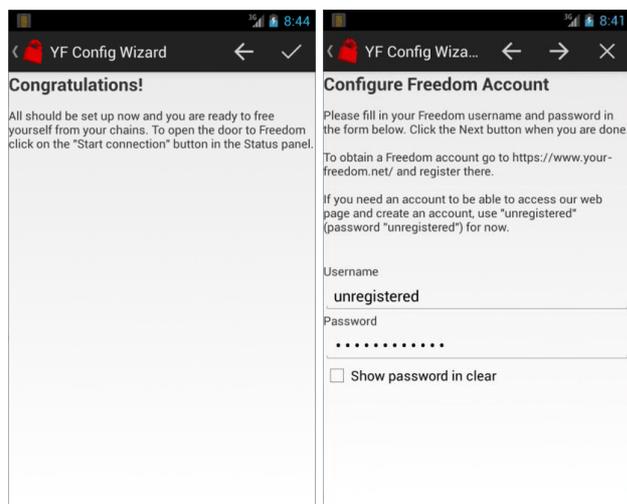
La siguiente página muestra una lista de los modelos de conexión disponibles y le permite seleccionar uno de ellos. Le sugerimos que indique HTTPS, HTTP y DNS. Normalmente, mientras más opciones indique, más tiempo le tomará, pero la posibilidad de conexión será mucho mayor. Si está satisfecho con los resultados parciales, habilite los campos en la parte inferior para detener la búsqueda. Una vez indicadas las opciones de conexión, haga click en la flecha derecha para comenzar la búsqueda. Una vez completada la misma podrá ver una lista de los servidores Your Freedom disponibles. Estos son ordenados por “preferencia”, con un número entre 0 y 10 que es calculado según la configuración de tu servidor. Los servidores que tengan el símbolo de una moneda, estarán disponibles para clientes premium solamente, mientras el resto podrá ser usados por cualquiera.



Indique el valor de más alto registro, y haga click en la flecha derecha

En la última pantalla, ingrese su usuario y contraseña (si posee alguno). Puede usar la configuración por defecto de usuario “unregistered” y contraseña “unregistered” si no posee ninguna cuenta aún. Esta última será necesaria si desea hacer uso de las ofertas de

BasicFreedom, EnhancedFreedom o TotalFreedom.



Una vez realizada esta última configuración, puede hacer click en la opción de OK.

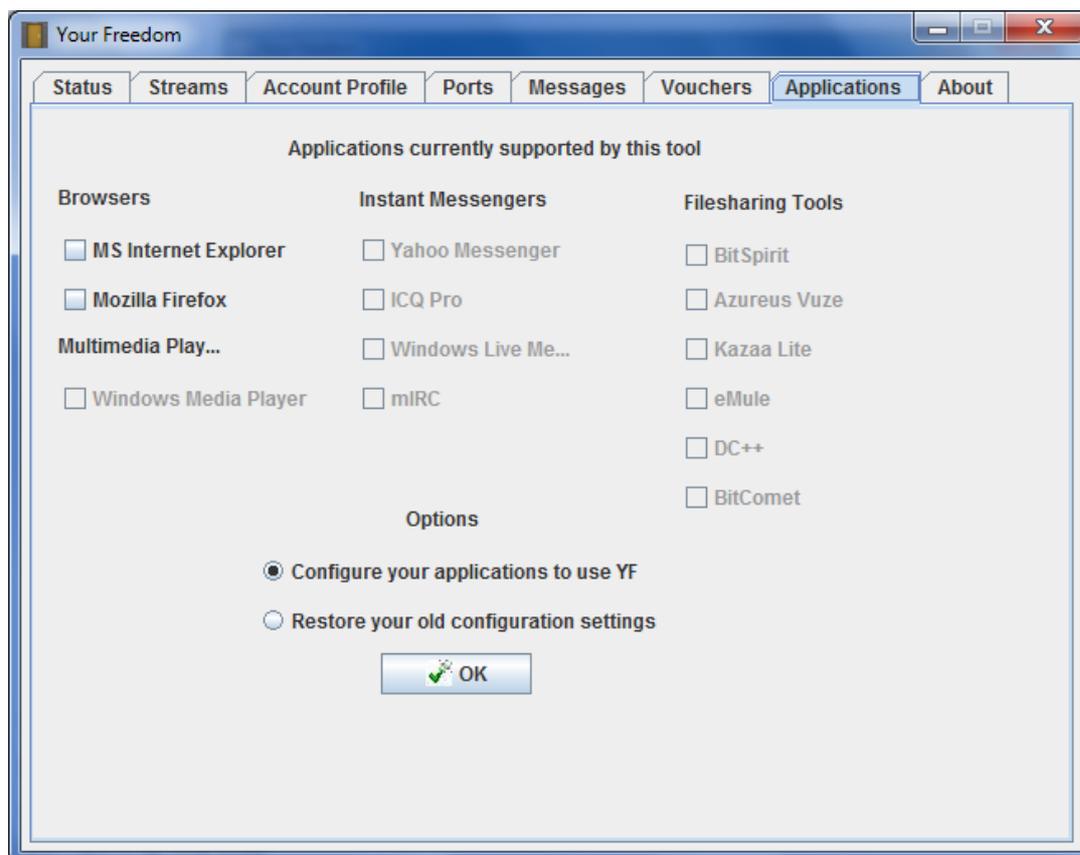
Sobre Android, no es necesario configurar ninguna aplicación, así que puede pasar por alto la próxima sección.

Configurar aplicaciones

Automáticamente

Nosotros recomendamos la configuración manual. Ésta característica está aquí sólo para su uso si así lo estima conveniente.

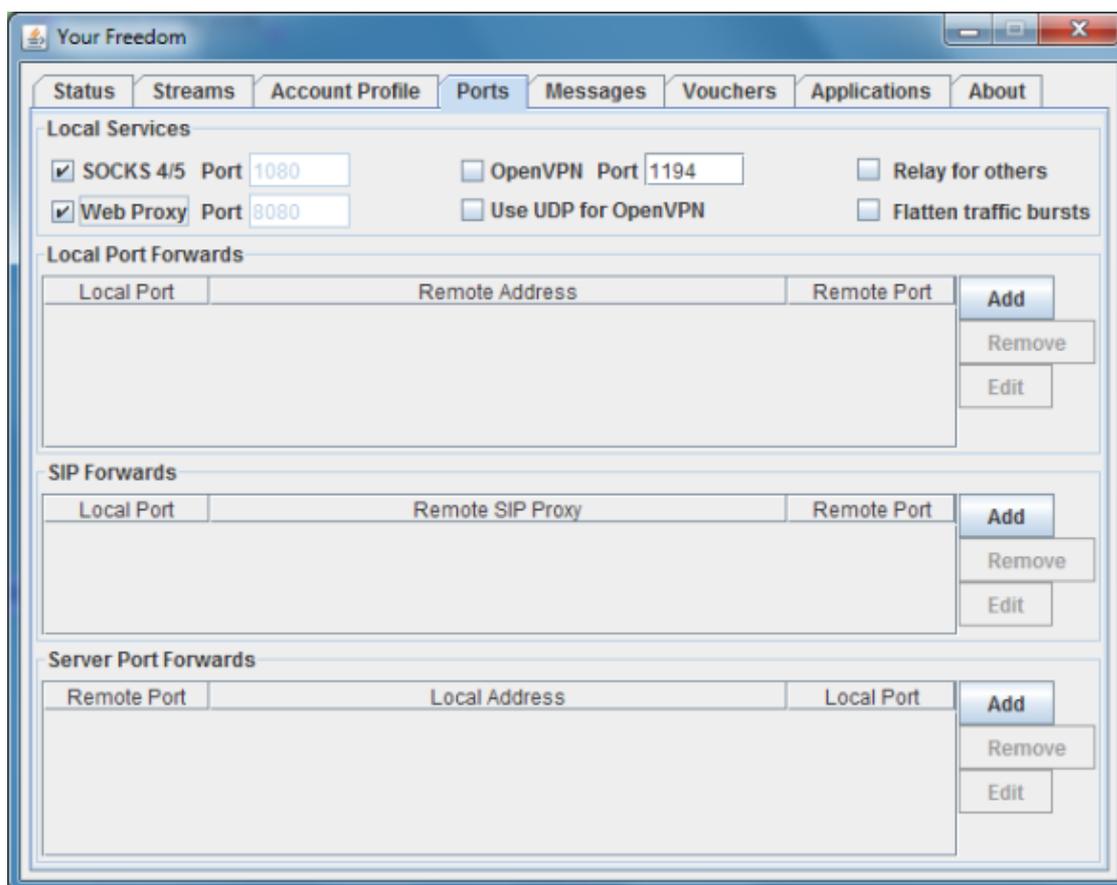
Los usuarios de Windows solo necesitan dar clic en la pestaña “Aplicaciones” y verán algo como esto:



Ésta es una lista de aplicaciones que pueden ser configuradas directamente por el cliente Your Freedom. Las que estén instaladas tendrán cajas marcables, las demás estarán deshabilitadas. Marquemos las que se quieran configurar y demos clic en "OK". Si todo sale bien veremos una confirmación.

Si todo sale bien demos clic en “OK”. Para restaurar las configuraciones anteriores escojamos Restaurar, seguido marquemos las configuraciones de las aplicaciones que queremos restaurar y demos clic en “OK”. Nótese que las aplicaciones que se han configurado para utilizar Your Freedom solo trabajaran correctamente si está establecida la conexión con el servidor. ¡No debemos olvidar restaurar todas las configuraciones antes de desinstalar el cliente Your Freedom!

Para configurar manualmente las aplicaciones antes debemos echarle un vistazo a la pestaña “Puertos”:



En esta pestaña vemos que nuestro ordenador está funcionando como un proxy SOCKS4/5 por el puerto 1080 y como uno Web por el 8080. Para cambiar esos valores solo deberemos desmarcar la casilla, cambiar el valor y volver a marcarla (esto puede hacerse en caliente). Lo que está debajo será explicado en el capítulo 5 pues que son temas más complejos.

Si por alguna razón no podemos configurar alguna aplicación desde el cliente Your Freedom, deberemos hacerlo manualmente configurándose para usar el proxy Web localhost por el puerto 8080 o SOCKS por el 1080 (si tenemos la oportunidad, debemos usar SOCKS versión 5). Es bueno leer la documentación de las aplicaciones antes de configurarles el Proxy (o simplemente preguntarle a alguien que sepa, en la sección de FAQ/Documentación del sitio Web <https://www.your-freedom.net/?id=faq> , están publicados algunos ejemplos).

El soporte OpenVPN no está habilitado por defecto – para más información ir al capítulo 3.3 página 35.

Manualmente

Por problemas de espacio no es posible detallar TODAS las configuraciones de las aplicaciones que pueden conectarse usando Your Freedom. Existen básicamente 4 formas de configuración.

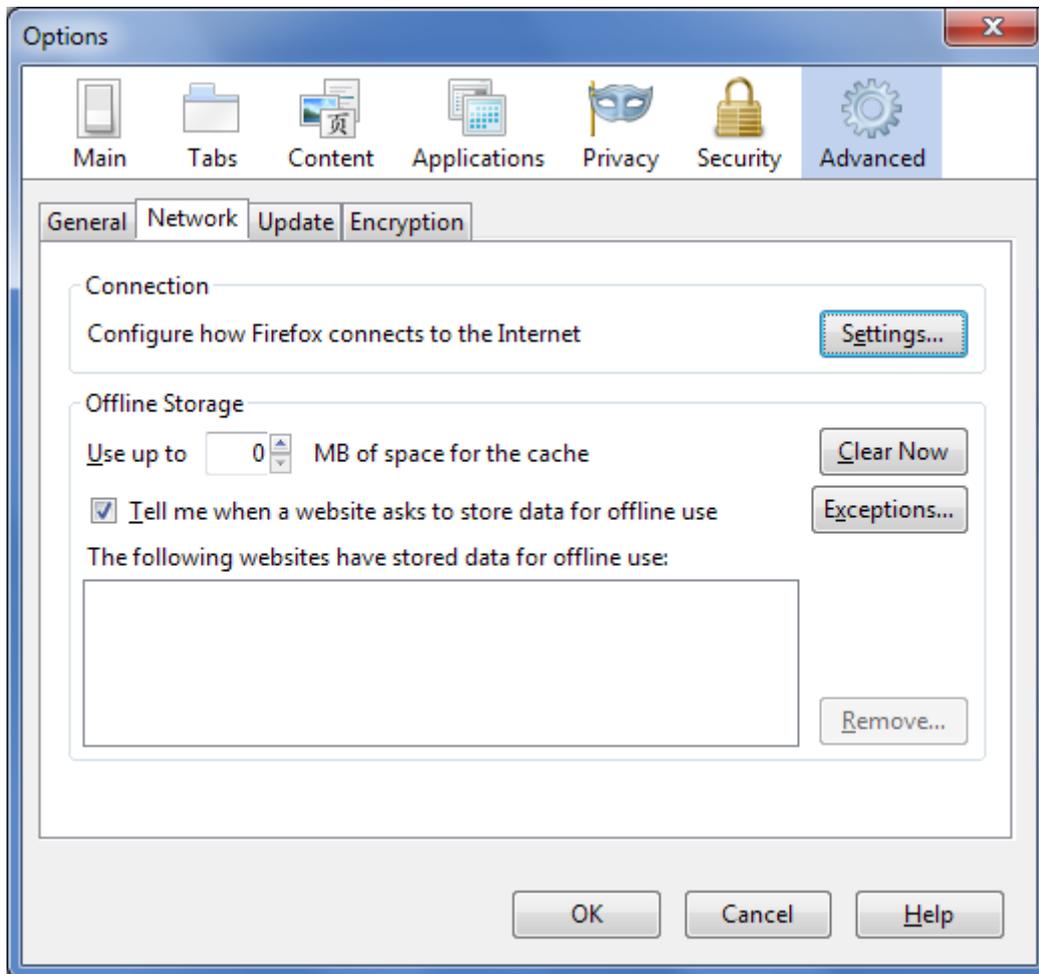
- 1) Configurando las aplicaciones que soporten el uso de un proxy Web para que

utilicen localhost o 127.0.0.1 por el puerto 8080 como tal.

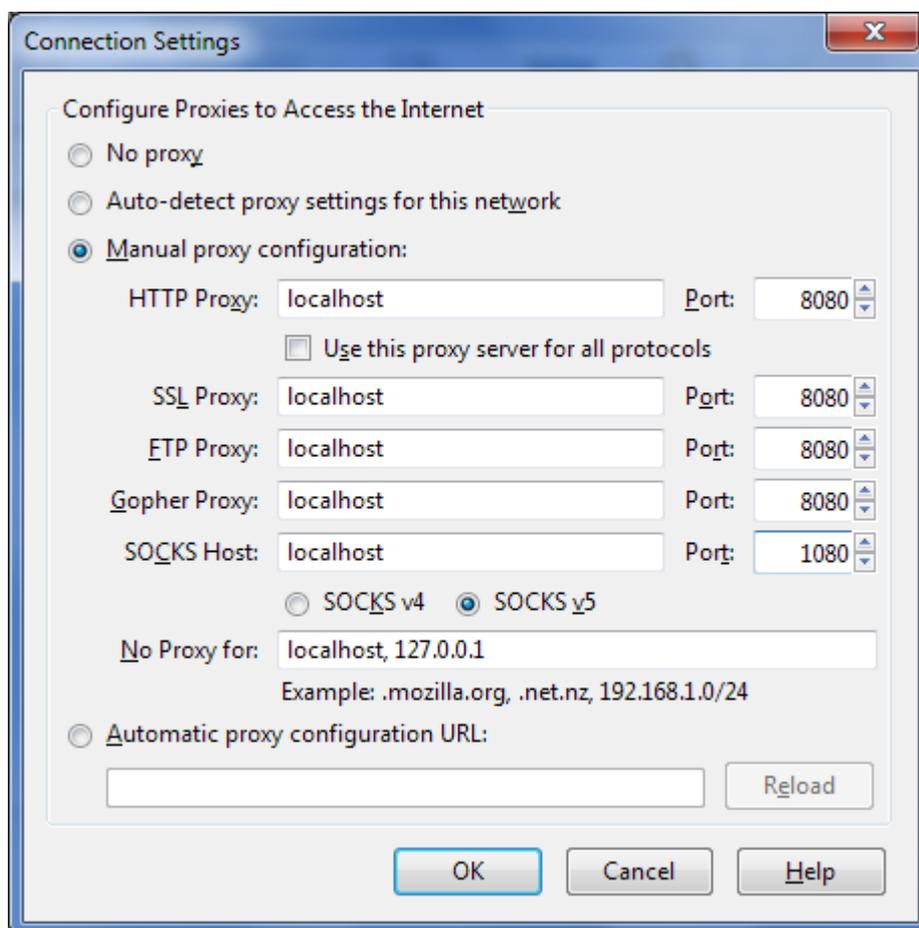
- 2) Similarmente las aplicaciones que soportan el uso de proxis SOCKS deberán ser configuradas para que usen la dirección localhost o 127.0.0.1 por el puerto 1080. Esta opción es preferible ante la variante de usar un proxy Web. No obstante, ambas deben funcionar igual de bien. Probemos con SOCKS5, si no resulta probemos con SOCKS 4. Algunas aplicaciones tienen problemas con las implementaciones de SOCKS.
- 3) Usar una aplicación que permita “socksificar” a otras. Muchas aplicaciones no están diseñadas para trabajar en ciertos entornos de red y no previenen la posibilidad de ser configuradas para usar proxis. Muchas de ellas trabajan bien con Your Freedom si se las ejecuta desde dentro de un “socksificador”. Un socksificador es una aplicación que trueca la DLL “winsock” por otra especialmente modificada y diseñada para tramitar todas las peticiones de red a través de un Proxy SOCKS, en este caso el cliente Your Freedom. Ejemplos de dichas aplicaciones son Sockscap (de 32 bit solamente!), ProxyCap y FreeCap. Éstas son abordadas en el capítulo 3.2 página 34. Usar un socksificador puede ser una opción si no podemos/sabemos como configurar nuestra aplicación o simplemente no tenemos permisos de administración. Es de señalar que es a veces difícil sobrescribir configuraciones de Proxy existentes por esta vía.
- 4) Usando redireccionamiento de puertos salientes y entrantes: Si nuestra aplicación solo necesita acceder a un servidor particular a través de una conexión TCP por un puerto específico quizás sea más conveniente crear un espejo de este puerto en nuestra PC y hacemos acceder a esa aplicación a ese puerto local. De igual forma se puede crear un espejo de algún puerto del ordenador en alguno de los servidores de Your Freedom, y hacerlo así accesible a otros en Internet. Éste tema se detalla en el capítulo 5.1 página42.

Configurando Mozilla Firefox

Todos los navegadores pueden usar proxis Web por tanto la opción1) debe servir. Seleccionemos “Herramientas” > “Opciones” > “Avanzado”, al hacer click en la pestaña “Red”, vemos lo siguiente:



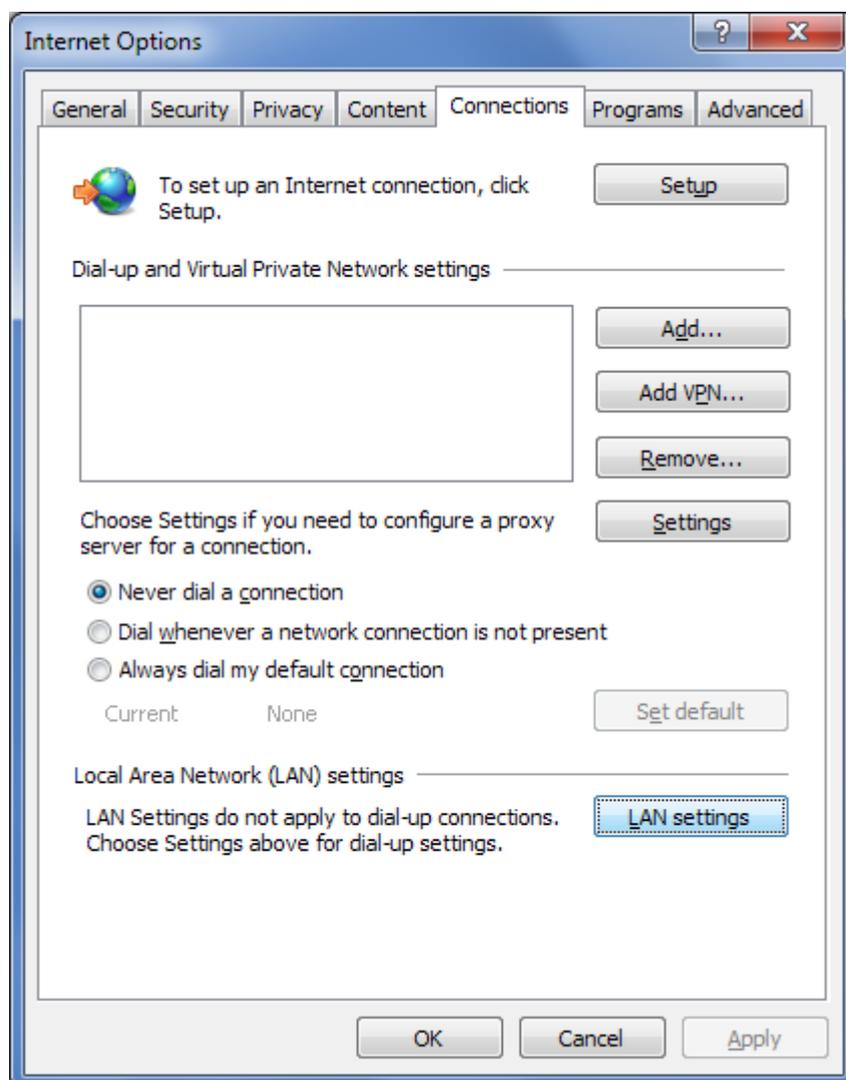
Hacemos clic en “Configuración”.



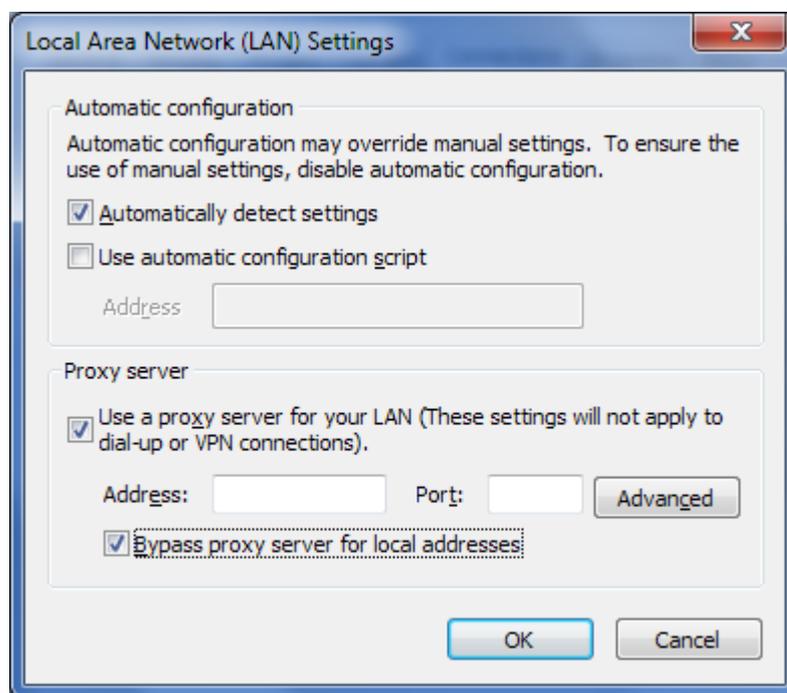
Complétese los valores como se muestra en la figura (se recomienda tomar nota de los valores originales para que así pueda ser más fácil recuperar la configuración inicial), hacer clic en ambas ventanas. Firefox estará ahora usando la configuración de Your Freedom.

Configurando Internet Explorer.

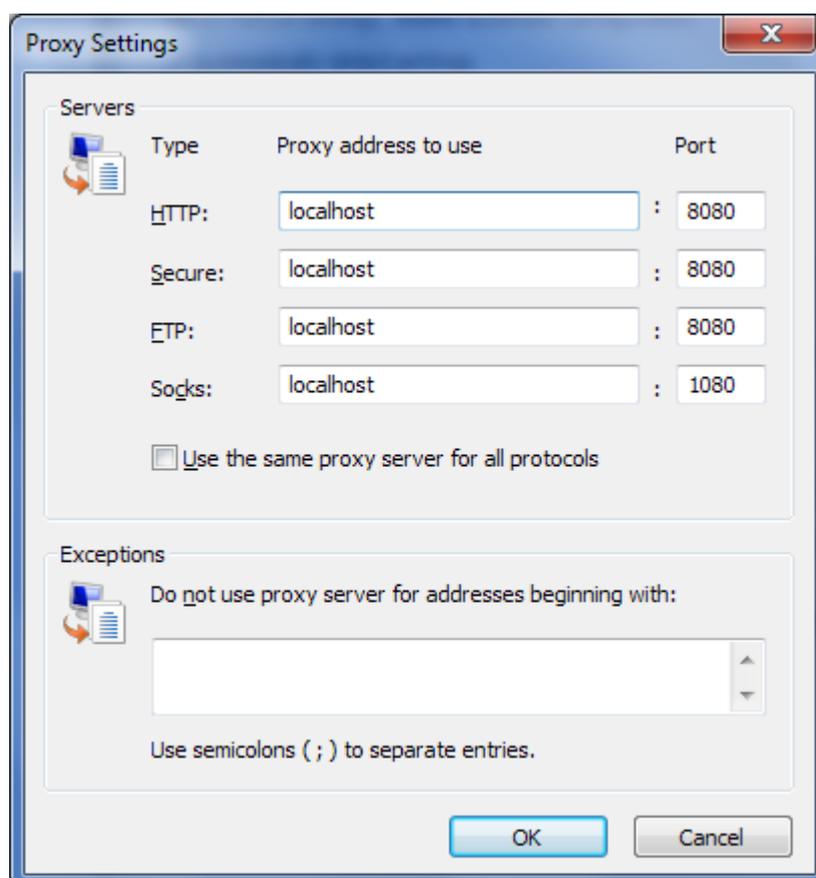
Como todos los navegadores Internet Explorer soporta proxis directamente. Y lo que es más, su configuración es compartida por muchas otras aplicaciones. Al seleccionar “Herramientas”, “Opciones de Internet” y hacer clic en la pestaña “Conexiones” veremos algo así:



Si se está usando una conexión LAN hacer clic en “Configuración LAN”, o en caso de no ser así, seleccionar la conexión que se usa para conectarse a Internet y hacer clic en configuración. Una ventana similar a esta se abrirá:



Márquese las casillas “Usar servidor Proxy” e “ignorar servidor Proxy para direcciones locales”. Dar clic en “Avanzadas” y otra ventana emergerá:



Complétense los valores que se muestran arriba. Hacer clic en “OK” en todas las ventanas, Internet Explorer ahora estará usando Your Freedom (y por tanto solo funciona

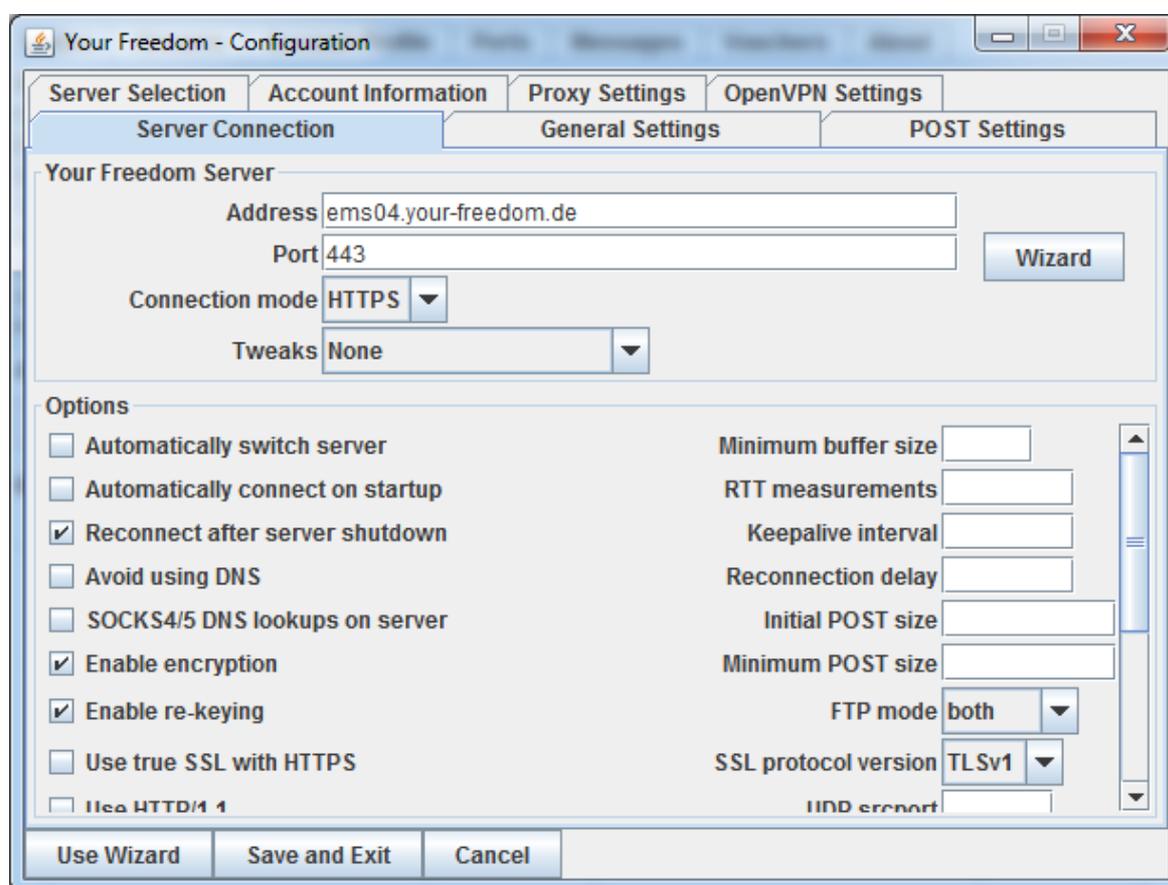
cuando estemos conectados a través de él). Se recomienda tomar nota de los valores originales para que así pueda ser más fácil recuperar la configuración inicial.

Configuraciones avanzadas

La mayoría de las opciones pueden ser trabajadas usando el dialogo “Configurar” disponible desde la pestaña “Estado”, hay sin embargo un grupo de ellas solo disponibles a través del fichero de configuración. No es recomendable trabajar el fichero de configuración sin supervisión a menos que se sepa lo que se está haciendo :-)

La ventana de configuración de Your Freedom

Ir a la pestaña “Estado” del cliente Your Freedom y hacer clic en “Configurar”. Se abrirá una ventana dediálogo como esta:

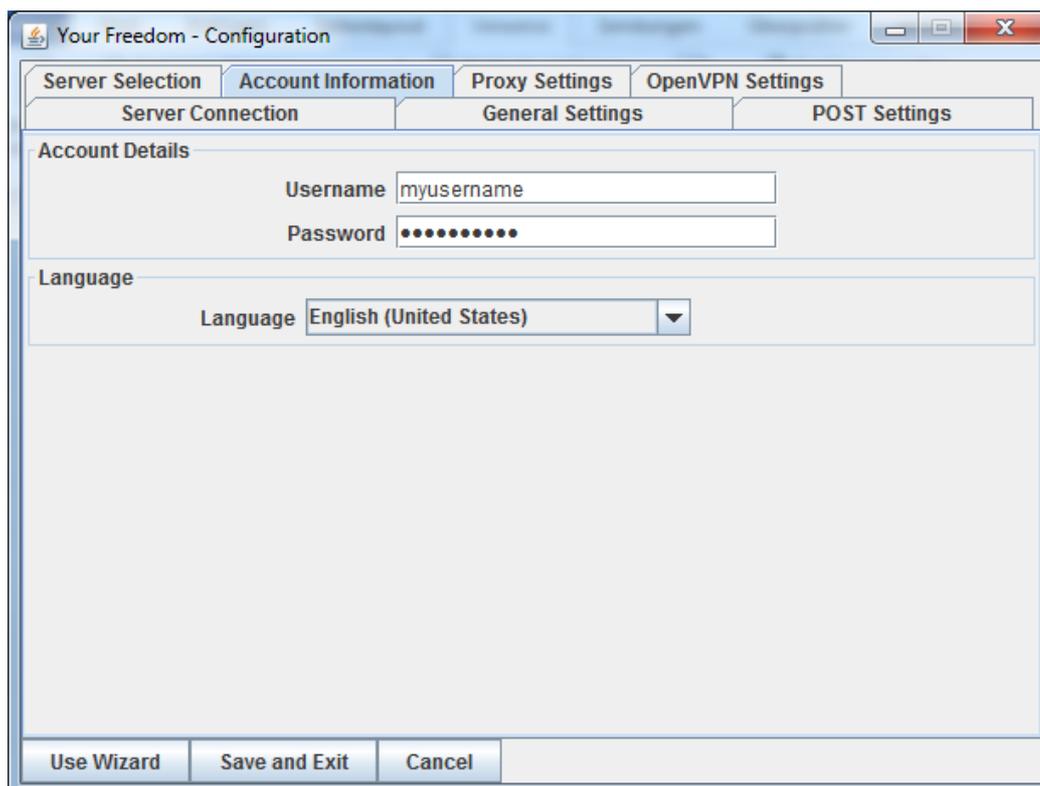


En la pestaña “Conexión con el servidor” configurar el nombre del servidor Your Freedom o su dirección IP (muchos nombres o IPs pueden ser separados por punto y coma ¡sin dejar espacios adicionales!) Seleccionamos el protocolo de conexión del menú desplegable y aparecerá automáticamente el puerto por defecto. Pueden usarse el asistente para las opciones de conexión y dejar que el cliente escoja la mejor forma (Pero realice la configuración de las opciones del proxy si usted necesita usar un proxy).

También pueden seleccionarse las opciones de conexión. Para la mayoría de los usuarios la configuración por defecto funcionará sin problemas. Y quizás sea conveniente marcar también “Evitar usar DNS” si se quiere conectar al servidor de Your Freedom por su

dirección IP y no se quiere preguntar al DNS local. No es aconsejable que se habilite la opción “Cambiar automáticamente de Servidor”, es posible que la misma no este disonible en futuras versiones.

Si se hace clic en la pestaña “Información de cuenta” se verá lo siguiente:



The screenshot shows the 'Your Freedom - Configuration' window. The 'Account Information' tab is selected, and the 'General Settings' sub-tab is active. The 'Account Details' section includes a 'Username' field containing 'myusername' and a 'Password' field with masked characters. The 'Language' section has a dropdown menu set to 'English (United States)'. At the bottom of the window are three buttons: 'Use Wizard', 'Save and Exit', and 'Cancel'.

Complete la información de cuenta de Your Freedom: usuario y contraseña, y escoja un idioma diferente si se desea. Muchos textos y mensajes están disponibles en otros idiomas y quizás sean más fáciles de entender si se cambian. Es de señalar que se necesita reiniciar el cliente para hacer efectivo los cambios:

Hay muchas opciones que pueden configurarse aquí. Quizás sea conveniente usar el asistente para configurar un Proxy Web pero no es obligatorio hacerlo, no hay mucha diferencia, salvo que de usarse el asistente el cliente Your Freedom verificará si las configuraciones son correctas. Si se conocen los detalles solo se necesita completarlos. Seguramente se necesitará configurar la dirección (nombre del servidor e IP) y el puerto. Si el servidor Proxy necesita autenticación hará falta el usuario y la contraseña y si es un proxy con autenticación por NTLM se hará falta saber el nombre de dominio (en estos casos el trío usuario, contraseña y dominio suelen coincidir con nuestras credenciales de Windows).

Si queremos usar conexión FTP y no tenemos acceso directo por este protocolo a los servidores de Your Freedom quizás se necesite especificar un Proxy FTP presente en la red (si la herramienta de línea de comando ftp funciona perfectamente significa que no es necesario configurar nada). El puerto probablemente sea el 21, se necesitará también el nombre de servidor o la dirección IP - se puede preguntar, usar FTP suele ser algo perfectamente legal y legítimo, nadie sospechará.

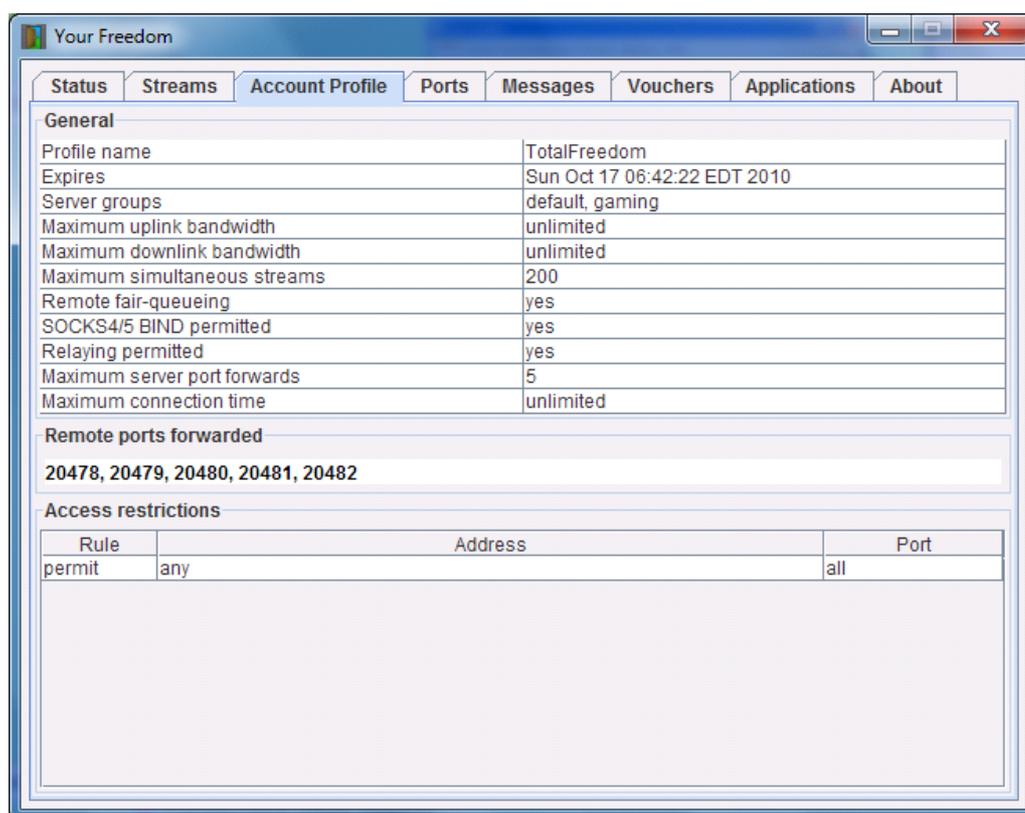
Los escenarios de conexión más comunes están cubiertos también por el asistente disponible desde el botón en la parte inferior - es el mismo que se ejecuta cuando se inicia el cliente por primera vez y se describe en detalle en el capítulo 2.3 página12.

Cuando hayamos terminado procederemos a dar clic en “Salvar y Salir” para salvar los cambios o “Cancelar” para abortar los.

Después de haber configurado el cliente estaremos en condiciones de conectarnos desde la pestaña “Estado”. El indicador de conexión (la puerta) deberá abrirse, un signo de interrogación deberá aparecer mientras el cliente y el servidor negocian y desaparecerá

después de algunos segundos. Si no desaparece es que la configuración de conexión no es correcta. Si revisamos la pestaña “Mensajes” probablemente encontremos alguna pista sobre el error. Si al final no se puede hacer funcionar la conexión, véase el Anexo A para más información sobre cómo comunicarse con el equipo de soporte.

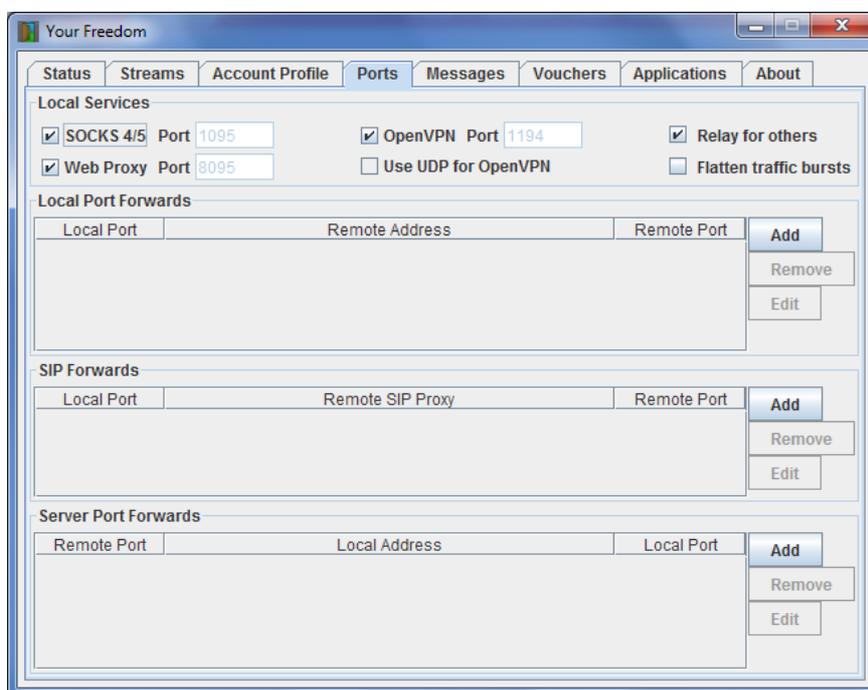
Una vez conectados verifiquemos el perfil de la cuenta accediendo a la pestaña “Account Profile”:



La mayor parte de las cosas aquí mostradas se explican por si solas, excepto quizás “Grupos” o “Redireccionar puertos remotos”.

El elemento “Grupos de servidores” indicará los grupos de servidores a los cuales se podrá tener acceso. Si hay múltiples grupos permitidos serán separados por coma. Todos tendremos “default” en el grupo de servidores de nuestro perfil, lo que significa que nos podemos conectar a cualquier servidor Your Freedom en el grupo “default” (en el momento que se escribe esta guía, todos los servidores están en este grupo, pero esto puede cambiar). Algunas cuentas tienen grupos de servidores adicionales en su perfil, dependiendo de los paquetes comprados.

Si nuestro perfil tiene algún puerto asignado, se mostrarán en la línea “Redireccionar puertos remotos”. Estos son puertos de servidor que podrán ser redireccionados a nuestro ordenador cuando se haya establecido la conexión.



Todas las opciones se pueden cambiar mientras la conexión esté activa y serán efectivos de inmediato. Si queremos modificar los puertos locales en los cuales el ordenador funge como Proxy Web o SOCKS es necesario desmarcar el servicio primero, cambiar el valor y volverlo a activar. Si queremos que el ordenador tramite peticiones originadas desde otros ordenadores es preciso marcar la casilla “Retransmisión para otros” Esto solo será posible si el perfil de la cuenta lo permite (verificar antes en “Permitir retransmisión para otros” en la pestaña “Información de cuenta”)

Iniciando y terminando la conexión

Cada usuario solo puede autenticarse una sola vez

En efecto, una cuenta no puede estar conectada desde dos lugares al mismo tiempo. Si uno quiere usar la misma cuenta desde otra computadora la primera sesión terminará. Esto significa que siempre podremos de iniciar sesión en casa aunque hayamos dejado accidentalmente nuestra cuenta conectada en nuestra oficina, la cual se desconectará.

Escogiendo el servidor correcto

Posición del servidor

Deberemos conectarnos a un servidor Your Freedom que esté cerca de donde nos estamos conectando o cerca del servicio al que queremos acceder. El esquema es el de un triángulo, los vértices son la PC, el servicio de Internet que queremos acceder y el servidor Your Freedom. Mientras más se asemeje estetriángulo a una línea recta entre nosotros y el servicio de Internet más rápido será usar Your Freedom.

Tomemos por ejemplo. Si estamos situados en Europa y el servicio que queremos usar está también situado en Europa(digamos que estamos jugando en línea) un servidor en estados unidos no sería lo más conveniente. Las leyes de la física hacen que la

información no pueda viajar más rápido que la luz y agregar 20.000 kilómetros de cables y fibra óptica entre nosotros y el servicio solo traerá latencias.

Una buena idea usar un servidor Your Freedom cercano a nosotros. ¿Por qué? Porque normalmente nosotros usaremos más de un servicio en la Internet y es imposible encontrar un servidor Your Freedom que esté topológicamente cerca de todos ellos, en cambio es posible encontrar el servidor Your Freedom que esté más cerca de nosotros. Por otro lado, hay aplicaciones que no se afectan por la latencia (como por ejemplo las transferencias de ficheros), en estos casos la localización del servidor es secundaria.

Cuando iniciemos sesión el cliente YF nos dirá donde está ubicado el servidor al que nos conectamos. Desdichadamente no tenemos muchos servidores fuera de Europa porque sencillamente porque:

- a) No son rentables: Los servidores dedicados sin límite de tráfico son inmensamente caros en la mayoría de los lugares fuera de Europa.
- b) Los proveedores imponen condiciones muy prohibitivas sobre lo que con el Server se puede hacer y lo que no - El equipo de Your Freedom ha empeñado gran parte de su tiempo explicando sin mucho éxito a los proveedores americanos que la esencia de dar el servicio no es ilegal.

Si alguien conoce de algún proveedor de servidores asequible siéntase libre de contactar con Your Freedom, ellos atienden. Es válido señalar que los servidores de Your Freedom generan entre 1 y 8 terabytes de tráfico mensual, necesitan al menos 2 GB de RAM, un buen CPU y deberá tener instalado Debian Linux. Si esto es menos de 100 US dollars por mes, sería genial.J

Protocolos

No todos los servidores de Your Freedom permiten todos los protocolos . Algunos proveedores (para ser precisos los americanos) imponen restricciones de protocolo y de vez en cuando se les antoja que han encontrado algo y lo que es peor, no escuchan razones. Por tanto si no queremos que nos cierren nuestros servidores tenemos que bloquear ciertos protocolos.

Por tanto, si estamos teniendo problemas con nuestra aplicación, echémosle un vistazo a la pestaña de mensajes del cliente Your Freedom. Si aparece un mensaje acerca de un protocolo no permitido entonces tendremos que usar un servidor diferente.

De manera general, debemos usar servidores europeos siempre que nos preocupen las restricciones de protocolos.

Hay una restricción que se aplica a todos los servidores: no está permitido conectarse por SMTP a servidores remotos, es más, todas las conexiones SMTP son redirigidas a un servidor central donde se hacen chequeos antivirus y se verifica que no sea SPAM. Esto solo es relevante si la aplicación de correo que usamos debe conectarse a un relay específico, normalmente no constituye un problema(pero pudiera significar que desearía deshabilitar el cifrado a nivel de transporte). Además existen vastos mecanismos de protección incluidos dentro de los servidores para hacerle la vida difícil a los "spammers". Afortunadamente los usuarios normales no notaremos ninguna diferencia.

Relays CGI

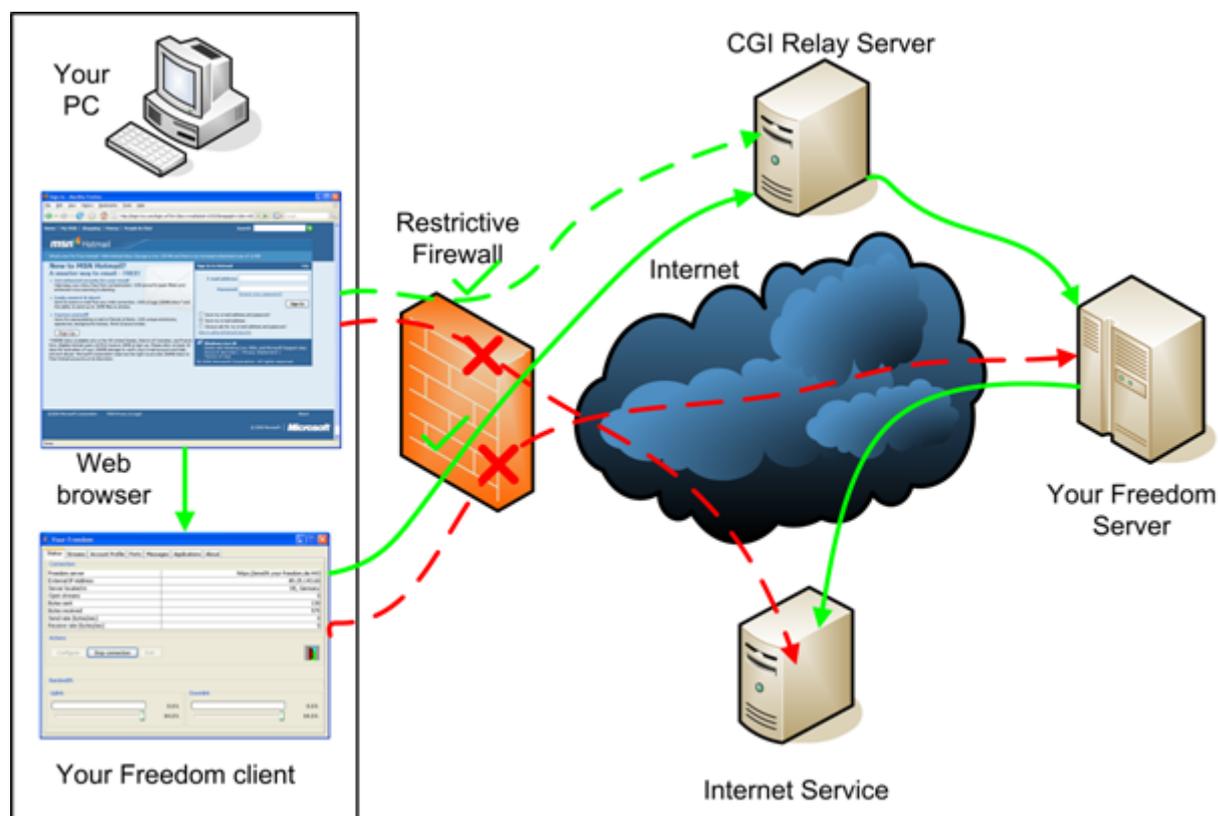
El método de conexión CGI es tan estándar que no solo engaña a los proxies, también permite que usemos un script que sirva de puente entre los usuarios y el servidor real de Your Freedom. Ese script es una página PHP que podemos colgar en cualquier servidor. Si bien es simple bloquear todos los servidores Your Freedom a medida que aparecen (porque además no podemos tener nuevos servidores todos los días), es bastante difícil bloquear miles de urls que no tienen nada en común.

Es bastante por qué alguien necesitaría usar un “relay CGI”: por necesidad. No existe otra razón porque obviamente este método no es tan rápido e interactivo como los otros métodos de conexión. Pero cuando estamos desesperados y no queda otra vía de conectarse es mejor que nada. ¿Pero por qué razón alguien querría poner el script en su servidor si todo lo que van a obtener es más tráfico adicional?

Es simple. Este es un proyecto gratificante. Your Freedom piensa recompensar a las personas que instalen relays CGI en función del tráfico total que éste genere. Cada vez que se use un servidor relay, se acumularán puntos que pueden ser usado en las compras de nuestro sitio web. Si desea conocer más sobre relay, puede consultar <https://www.your-freedom.net/?id=cgirelays> para más detalles. Ha de tenerse en cuenta que tal relay pudiera generar mucho tráfico mensual (del orden de los cientos de GB).

¿Cómo usamos dicho relay CGI? Necesitamos saber la url. Tal dirección no es una url con todo incluido - solo se necesita el nombre del servidor y el uri. Por ejemplo, si el script está situado en la url <http://algun.servidor.com/alguna-carpeta/script.php>, en el cliente pondríamos solo `algun.servidor.com/alguna-carpeta/script.php`. Esto en lugar del nombre del servidor Your Freedom. Escogeríamos CGI como el modelo de conexión y deshabilitaríamos la selección automática de servidores.

A continuación se esquematiza el concepto de este modelo de conexión.



¿Cómo encontrar la url del relay? Eso es otro tema completamente. Your Freedom no publica esta lista ni debemos hacerlo nosotros para que no terminen en listas negras. El cliente Your Freedom si conoce como encontrar el relay.

Para más información sobre como instalar el script este se encuentra en https://www.your-freedom.net/ems-dist/enduring_freedom.php-RENAME . Se necesita escoger cual servidor Your Freedom vamos a usar. El nombre no deberá levantar sospechas. Después tendremos que probarlo (usar el navegador - debemos ver un texto largo con mucha cáscara - eso significa que todo está bien). Si funciona debemos registrarlo en el sitio Web de Your Freedom (<https://www.your-freedom.net/?id=cgirelays> , inicie sesión primero para asegurarse de que recibio el saldo!). El sistema analizará si funciona, se agregará a la base de datos y los clientes podrán encontrarlo (toma su tiempo, no esperamos que los clientes lo usen de inmediato).

También tenemos la posibilidad de instalar relays para nuestro propio consumo, no necesitamos registrarlo y podemos publicar la url. Solo si queremos registrarlo nos abstendremos de publicarlo.

Conectando juegos y otras aplicaciones

Nota: Este capítulo solamente aplica para la versión desktop de YF, no para la aplicación Android. Sobre Android, no es necesario configurar nada para hacer funcionar otras aplicaciones con YourFreedom.

Introducción

Además de los navegadores, otras aplicaciones pueden sacar provecho de Your Freedom y conectarse a Internet. Desde clientes de escritorio remoto, chat y mensajeros instantáneos como GTalk, Pandion o Yahoo Messenger, tecnologías P2P como BitTorrent hasta los juegos más exigentes pueden ser configurados para conectarse a través de Your Freedom.

Este capítulo aborda conceptos necesarios para hacer funcionar cualquier aplicación en general.



Para técnicas más específicas como redireccionamientos de puertos locales ver el capítulo 5.1

Usando “socksificadores”

Hay una forma de usar aplicaciones que no soportan el uso de Proxis Web o SOCKS. Como el cliente Your Freedom es un servidor SOCKS completamente funcional solo necesitamos “socksificar” nuestra aplicación. Hay muchas maneras de hacer esto y todas ellas usan una funcionalidad llamada precarga de librería de enlace dinámico.

Para no reinventar la rueda los programadores crearon librerías que se enlazan dinámicamente a la aplicación en tiempo de ejecución. Cualquier sistema operativo ya sea Windows, Linux, MacOS, etc. viene con este tipo de librerías y una de ellas ofrece funciones de red. La primera vez que alguna de estas funciones es llamada por la aplicación la librería es cargada automáticamente, pero solo si no ha sido cargada ya en el contexto de la aplicación. El truco está en asegurarse de que una librería igual pero truqueada se haya cargado antes de que la aplicación es inicie. Esta librería se encargaría de tramitar todas las funciones de red a través de un Proxy SOCKS.

Windows

Existen muchas herramientas “socksificadoras” en el mercado:

WideCap

WideCap es un socksificador libre que se integra con el “stack” de red del sistema y no basa su funcionamiento en la carga previa de ninguna librería como lo hacen otros socksificadores. Es ideal para muchos juegos y aplicaciones que no pueden ser usados con socksificadores como SocksCap. Sabemos que funciona bien para juegos basados en

Steam. Puede encontrarlo en <http://www.widecap.ru/eng/>.

SocksCap

Esta es una herramienta para uso no comercial(y ya no estará disponible comercialmente). Tendremos que buscarlo en google “sc32r240.exe” para descargarlo.

FreeCap

FreeCap, como lo sugiere su nombre es freeware. Está disponible para descargar desde la página del proyecto en <http://www.freecap.ru/eng/>. Existe documentación adicional ahí pero su uso con Your Freedom es bastante simple. Lo mejor que tiene es que es gratuito y fácil de usar y su funcionamiento suele ser suficiente para cualquier aplicación.

ProxyCap

Un producto comercial. Para más información remitirse a <http://proxylabs.netwu.com/>.

Proxifier

Proxifier es una pieza de software muy ingeniosa. Se puede probar por 31 días, la licencia cuesta USD 40. Además también está disponible para Mac OSX. Puede chequear en el sitio web de Proxifier en <http://www.proxifier.com/>.

HummingbirdSocks

La suite Hummingbird contiene un socksifier. Se puede descargar desde el sitio principal de Hummingbird <http://connectivity.opentext.com/>.

Linux y derivados de Unix

Dante

Dante es el estándar de-facto en el mundo Unix/Linux. Es gratuito. Está disponible para descarga desde <http://www.inet.no/dante/>. Muchas distribuciones de Linux tienen un paquete “dante-client”. Una vez instalado tendremos que editar /etc/dante.conf para redirigir el tráfico correctamente a nuestro cliente Your Freedom y después usar el script “socksify” para ejecutar nuestras aplicaciones.

Tsocks

Tsocks es otra herramienta del mundo Unix/Linux, y es también gratis. Se puede descargar desde Sourceforge. Existe una versión para Mac OSX.

Mac OS X

Proxifier

Proxifier está también disponible para MacOSX.

Tsocks

Veaselas instrucciones sobre socks en MacOSX en <http://forums.macosxhints.com/archive/index.php/t-55338.html>.

Soporte OpenVPN

Introducción

Existe otro modo de hacer que nuestras aplicaciones se conecten a Internet a través de Your Freedom sin necesidad alguna de configurarlas. Esto está bien probado y ha demostrado ser casi infalible frente a sus contrapartes los “socksificadores”. En teoría, cualquier aplicación que funcione detrás de una DSL o conexión por cable debiera trabajar bien usando el modo OpenVPN.

Requisitos

Es necesario cumplir con un par de requisitos para poder usar OpenVPN con Your Freedom:

Privilegios administrativos

No hay forma de escapar de esto: para instalar OpenVPN se necesitan privilegios de administración (en los sistemas Unix deberemos ser capaces de instalar los binarios de OpenVPN). Normalmente en una PC de empresa con autenticación por dominio no se gozan de tales privilegios.

En Windows Vista necesitamos ejecutar explícitamente el cliente Your Freedom con privilegios de administración. Hay una forma conveniente de hacer esto de una buena vez: damos clic derecho en el acceso directo del menú inicio >>“Propiedades”>>“Compatibilidad” y después marcamos la casilla “Ejecutar como administrador”. Esto servirá siempre que usemos este mismo acceso directo para ejecutar el cliente Your Freedom.

Se necesita tener OpenVPN instalado

OpenVPN es libre y su código es abierto (se aceptan donaciones). Se puede descargar en <http://openvpn.net/download.html> . Para los usuarios de Windows hay un instalador, otros necesitarán compilar los fuentes de OpenVPN - es también posible que venga con la distribución del sistema operativo. De cualquier manera si abrimos una consola de comandos, tecleamos openvpn y sale algo es que está instalado. OpenVPN necesita instalar una interfaz túnel de red en la PC, su nombre en Windows es TAP-WIN32, en Linux sería tun0.

Para los usuarios de Windows Vista, Windows 7 o superior, es recomendado configurar el ejecutable de openvpn.exe para que se ejecute con privilegios. Para esto debemos ir a "C:\Program Files\OpenVPN\bin\", damos click derecho en el ejecutable de openvpn, seleccionamos “Propiedades”, “Compatibilidad”, y marcamos la casilla “Ejecutar como Administrador”. Esto asegurará que el proceso de openvpn se ejecute con los privilegios necesarios.

Antes de hacer uso de OpenVPN debemos asegurarnos de tener nuestra PC protegida y limpia de virus, gusanos o troyanos. Debemos asegurarnos que no sea parte de una bot-net. Si la PC está infectada nuestros servidores bloquearán su



acceso y deshabilitarán la cuenta para proteger nuestros sistemas. Si no se dispone de alguna suite de seguridad apropiada instalada en la PC ábrase Internet Explorer y visítese la página <http://onecare.live.com/site/en-US/default.htm>

Es aconsejable que repitamos esto de vez en cuando para nuestra propia protección. Considere instalar alguna herramienta de protección como Microsoft Security Essentials, Avira Antivir o avast.

No se necesita ningún paquete Your Freedom. FreeFreedom es suficiente.

El soporte OpenVPN ya está disponible para todos los usuarios. A pesar de que el otro extremo del túnel consume más recursos el equipo Your Freedom decidió ponerlo a disposición de toda la comunidad. Aunque en realidad 64k no son suficientes para disfrutarlo a plenitud.

Tareas de configuración

Tener conocimiento del entorno de red

Si se está detrás de un firewall y se quiere tener acceso a servidores que tienen dirección IP de Internet pero que no son accesibles desde Internet se necesita hacer una exclusión de ruta.

El 99% de los usuarios no necesitan configurar exclusiones. Además, todos los rangos de IPs no pertenecientes a Internet son excluidos automáticamente (esto abarca 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Las rutas ya presentes en nuestra red también son excluidas también.

Para el resto de los casos, debemos agregar una línea `openvpn_exclude` por IPo red como se describe en el Anexo C, e.g.

```
openvpn_exclude 1.2.3.4
openvpn_exclude 2.3.0.0 255.255.0.0
```

Your Freedom es lo suficientemente inteligente para excluir todas las direcciones IP que son necesarias para mantener la conexión al servidor de Your Freedom.

Activar la casilla OpenVPN

Vayamos al panel de puertos y activemos la casilla OpenVPN. Dejemos el número de puerto como está, a menos que haya razones para usar un puerto diferente.

Iniciemos la conexión Your Freedom.

La configuración de la conexión luce como siempre, solo que a los 10 segundos después la puerta abre un poco más. :-) El registro de mensajes deberá advertirnos cuando esto suceda también. Si viéramos la tabla de ruteo (en Windows, abrimos una consola y tecleamos "route print", los usuarios de Unix escribimos "netstat -rn" o "route -n"); se deberán ver una gran cantidad de rutas todas rumbo a la dirección 169.254.xxx.yyy. Estas rutas cubren todo el espacio de direcciones de Internet menos las exclusiones configuradas con anterioridad. No se puede reemplazar la ruta por defecto de la PC, eso ocasionaría que se cortara la comunicación con la red local y el cliente Your Freedom

quedaría desconectado.

¿Retransmisión para otros?

Pero a menos que nuestra PC enmascare a las demás, cada una de las otras necesitará su propia sesión OpenVPN. Cuando se inicia la conexión el cliente Your Freedom crea unos cuantos ficheros de configuración en nuestra carpeta “home”(ver Anexo C para más información sobre su localización). Estos ficheros comienzan con “client” o “server”; cópiense a las otras PC en alguna carpeta, edítense el fichero “client.ovpn” y reempácese 127.0.0.1 con el IP de la PC donde está corriendo la sesión Your Freedom. Cada PC necesita tener instalado OpenVPN.



Existe otra técnica más genérica para compartir la conexión Your Freedom con equipamiento vario como un Xbox o una Playstation e incluso otras PCs. Ver capítulo 5.2.2 en la página 44..

¿Interfieren el cortafuegos de Window?

No debe haber inconveniente en usarlo. Pero no hay tampoco razón para hacerlo, el firewall solo cortaría las conexiones entrantes(o sea, no podríamos hacer relay para otros). Usarlo en caso de que sospechemos que nuestras aplicaciones abren conexiones clandestinamente pero si algo no funciona debemos probar sin él.

Configurar las aplicaciones

Lo mejor de OpenVPN es que ¡no hay que configurar nada! No se necesita configurar ni Proxy ni usar socksificadores. Solo asegurarnos de que las aplicaciones no están usando ningún Proxy y listo.

Es de señalar que la PC no es visible desde Internet a través del túnel OpenVPN, aplicaciones que dependan de esto no funcionarán bien. Si la página Web del fabricante menciona algo sobre puertos que han de ser abiertos entonces es probable que no funcione. Aunque es válido señalar que es posible combinar OpenVPN con redireccionamientos de puerto de servidor. Ver capítulo 5.1.3 página 43 para más detalles sobre el tema.

Diagnóstico de problemas

El túnel OpenVPN no se inicia correctamente

Chequese el registro de mensajes, ahí podrá estar la causa reflejada. Si no, se deberá enviar un fichero “dump” en un correo a soporte@your-freedom.net(ver Anexo A: “creando un fichero dump”) – o verifíquelo usted mismo.

Debemos verificar que no haya ya otro proceso OpenVPN ejecutándose cuando se cierre la conexión Your Freedom. En Windows debemos presionar Ctrl+Alt+Del ordenar las tareas y buscar “openvpn”. Terminar el proceso antes de reiniciar la conexión Your Freedom. Esto puede pasar si se cierra el cliente Your Freedom de forma inusual antes de éste que tenga oportunidad de cerrar OpenVPN.

El túnel OpenVPN se abre, pero la conexión Your Freedom falla

De alguna manera el túnel cortó la comunicación con el servidor Your Freedom. Debemos mandar un fichero “dump” a soporte técnico.

¿Qué son las direcciones 169.254.xxx.yyy?

Representa una red clase B reservada para comunicaciones de emergencia en un medio de broadcast como Ethernet. Cada computadora escoge un IP al azar y chequea si está en uso.

Nadie usa este tipo de red para nada, solo Windows lo hace en ausencia de un servidor DHCP o una configuración estática. La red no está enrutada hacia Internet y nadie la usa de forma privada, por eso fue escogida para éste fin. Es muy poco probable que cause un conflicto de direcciones en algún lugar.

El otro extremo del túnel OpenVPN está siempre en 169.254.0.1; si se desea chequear cuanta demora de paquetes se introduce por Your Freedom solo necesitamos hacer ping a esta dirección.

Nuestra PC siempre recibirá una dirección impar en una subred /30 en este rango y enrutará todo a la contraparte par en esta subred.

Usando Your Freedom sin la aplicación cliente

PPTP

Información General

La forma habitual de usar nuestros servicios es mediante la aplicación cliente de Your Freedom. Esta permite hacer cosas que normalmente no pudieran hacerse con un software VPN. Pero hay ocasiones (y lugares) donde necesitamos asegurarnos de que nos conectamos sin interferencia de ningún intruso, o simplemente por enmascarar la ubicación y localización que realmente tenemos.

Los servidores de conectividad Your Freedom ahora aceptan conexiones PPTP VPN. PPTP es un protocolo de tunnel BPN desarrollado por Microsoft y algunas compañías más no tan reconocidas en el ámbito de desarrollar buenos protocolos. Sin embargo, tiene una ventaja: esta soportado en cada pc, en cada smartphone, estos entienden PPTP sin necesidad de ningún software adicional. Contrariamente a los protocolos bien-diseñados como son OpenVPN, PPTP usa una combinación de TCP para el control de conexión y GRE en la encapsulación de frames PPP para transportar datos. Si consideramos que

necesitamos usar MSCHAPv2 y MPPE-128 para la autenticación y el cifrado, al procurarnos un mínimo de protección puede que nos encontremos en problemas. Ya no es necesario preocuparse por detalles engorrosos, nosotros nos ocupamos!.

Cuando usar PPTP? Aquí mostramos algunos ejemplos:

- Cuando accedemos a un punto de acceso inalámbrico sin cifrado, si usando PPTP nos aseguramos de que nadie pueda ver lo que hacemos.
- Si vivimos en un país A y queremos hacer ver a algún servicio de internet que provenimos realmente de algún país B (genial si deseamos ver transmisiones de TV no disponibles para nuestro país!).
- Si nos encontramos en un entorno censurado, de bajo rigor (muchas de las cosas de que no funcionan aparecen como fallos técnicos).
- Si nuestro proveedor penaliza algún servicio que usamos, usando PPTP podemos hacer que funcione adecuadamente (por ejemplo: en ocasiones YouTube es lento porque nuestro proveedor local *quiere* que sea lento) .

Claro, el cliente YF puede ayudarnos en cada una de estas situaciones.

Independientemente del servicio que usted reciba (FreeFreedom, BasicFreedom, EnhancedFreedom, TotalFreedom), todos usan la misma aplicación cliente de YF. Los vouchers pueden ser enviados a través de nuestra página web. Usted puede usar su cuenta tanto con el cliente como con PPTP, pero no tanto en ambas al mismo tiempo. Usted usará una dirección IP compartida sólo con el cliente de YF.

Es PPTP seguro?

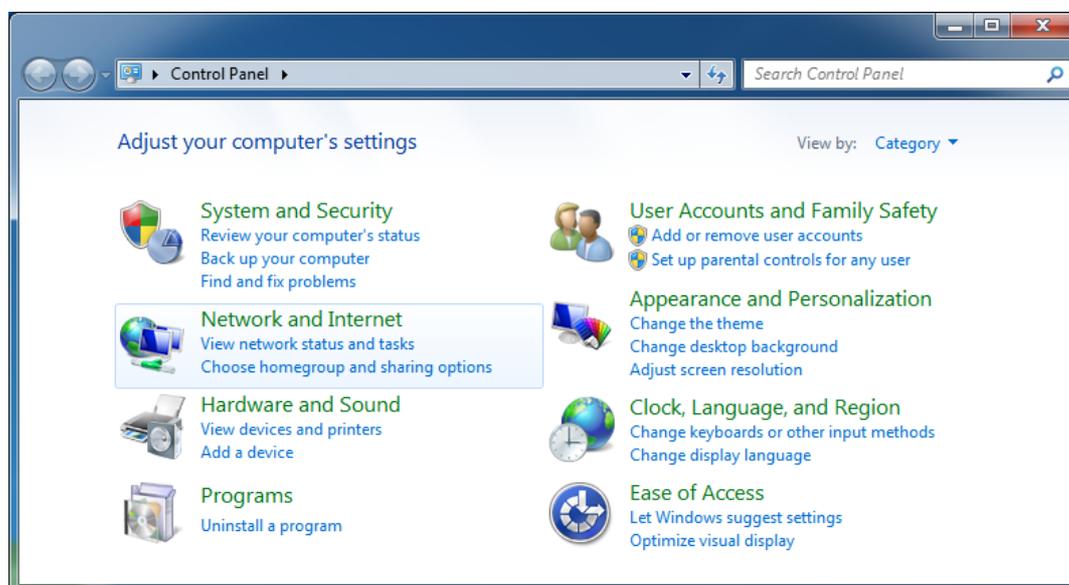
El cliente de YF usa un fuerte cifrado y protege su privacidad mejor que PPTP. Aún, PPTP es aproximadamente tan fuerte como usar HTTPS para acceder a los servidores web. Usa RC4 con una llave maestra de 128 bits y genera las claves de sesiones con bastante frecuencia. Su mayor debilidad es que depende de que la contraseña sea suficientemente fuerte.

Usted podría haber leído acerca de los ataques en contra de MSCHAPv2. Esto no es nuevo. MSCHAPv2 y MPPE ambos dependen de la reserva de un hash MD4 de su contraseña. Si alguien puede obtener este hash de MD4, no solamente lo impresionaría sino también que puede descifrar los datos almacenados. Nuestro consejo es que use contraseñas suficientemente fuertes. Si lo hace, PPTP usando MSCHAPv2 y MPPE es relativamente seguro.

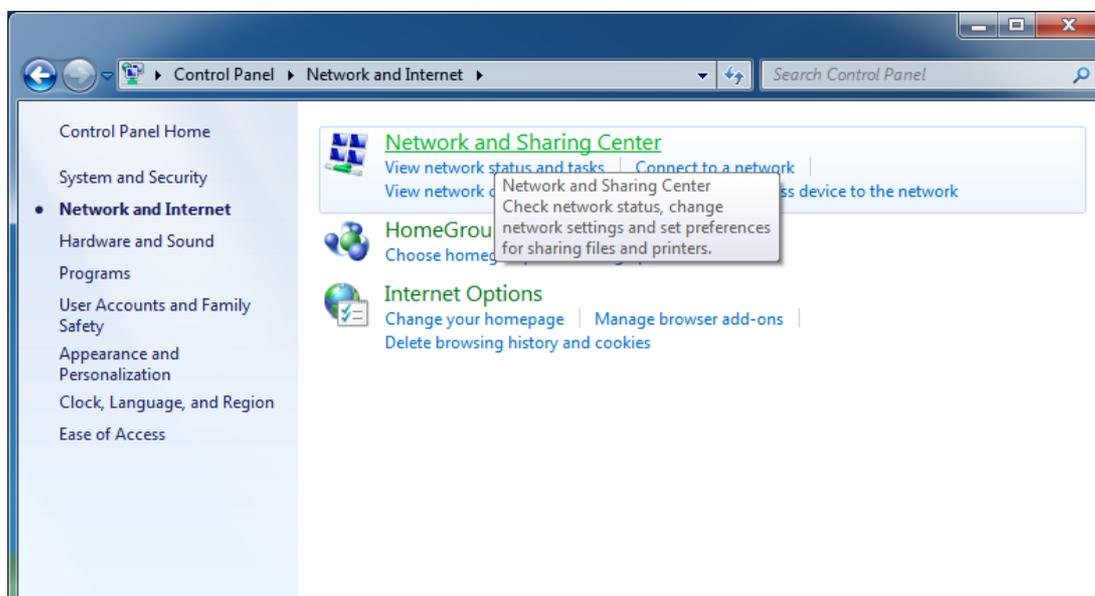
Cómo configurar PPTP?

Explicaremos aquí cómo hacerlo sobre Windows 7. Usted encontrará información sobre cómo hacerlo para su sistema si busca google; no hay nada especial en nuestro servicio de PPTP.

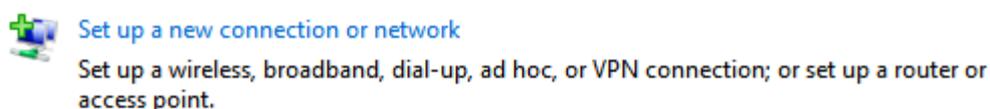
Primero, haga click en el botón de Windows abajo en la esquina izquierda de la pantalla, y seleccione el "Panel de control". Parecerá esto:



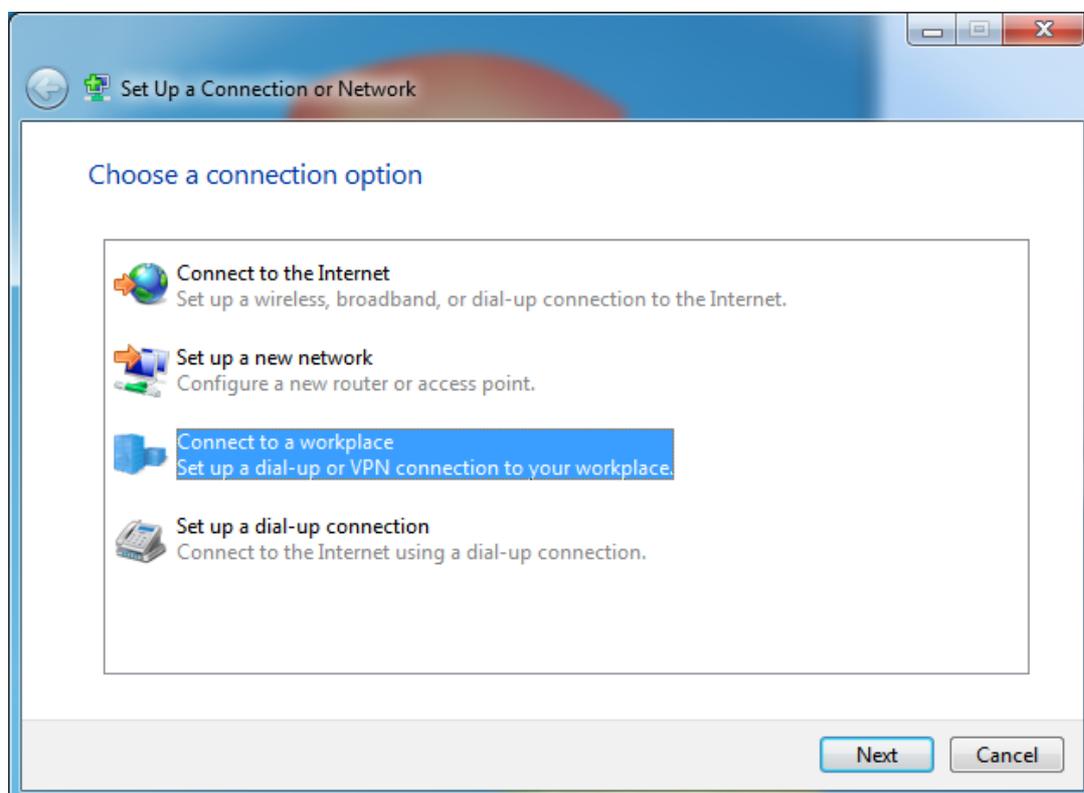
Seleccione "Network and Internet":



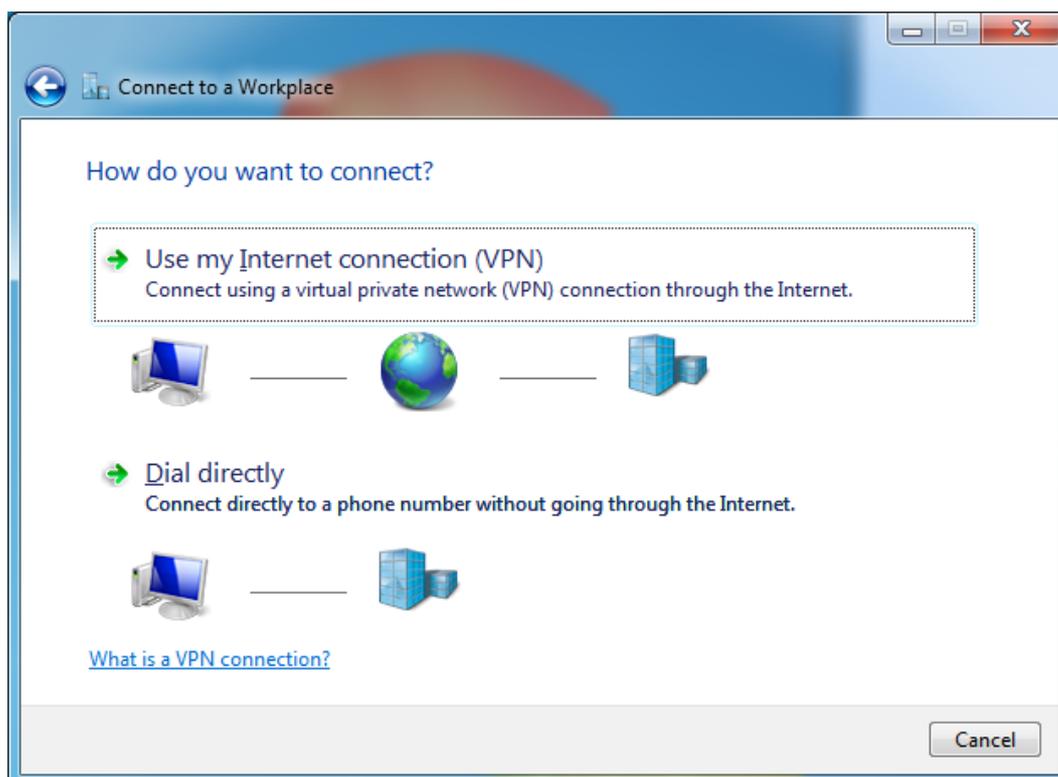
Click en "Network and Sharing Center". En la red y comparta el panel central, haga click en "Set up a new connection or network", que se muestra tal como se indica a continuación:



Seleccione "Connect to a workplace", incluso si le puede sonar obvio el procedimiento (y trate de pasar detalles por alto), haga click en el botón Next:



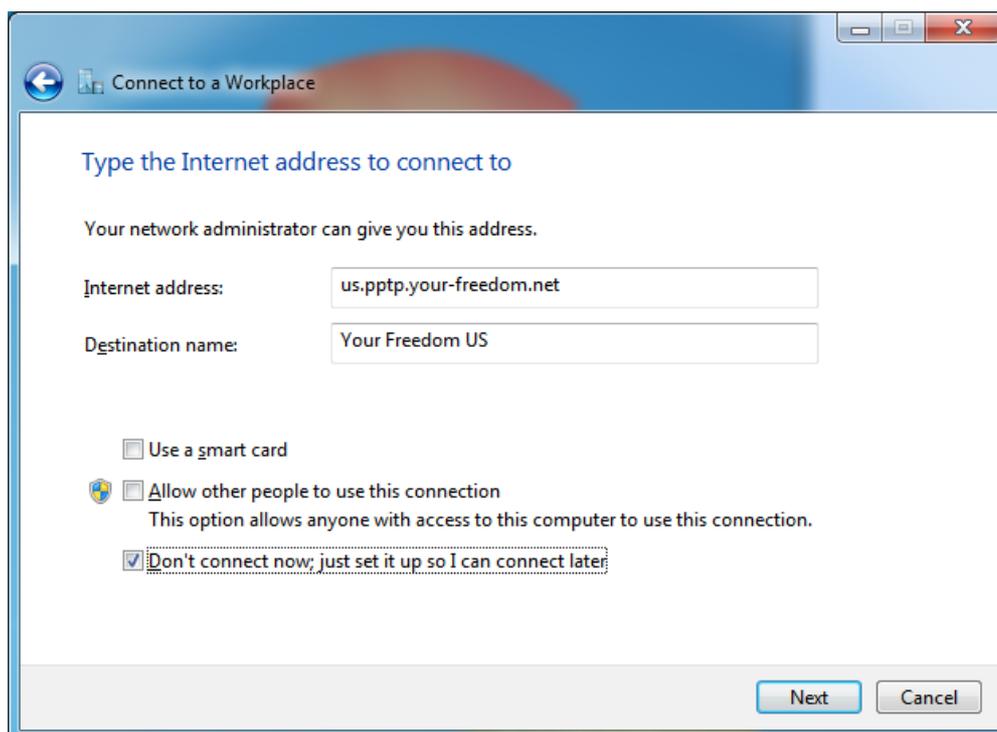
Ahora selecciones "Use my Internet connection (VPN)", esto es lo que estamos tratando de hacer, instale la nueva conexión a través de su conexión a internet existente:



En el paso siguiente, ingrese una dirección de internet a la que se desea conectar. Llene en el servidor PPTP de su elección. Si conoce la dirección IP o el nombre del servidor puede usarlo , pero sugerimos que usted use los nombres genéricos por país que

proporcionamos. En este ejemplo, queremos un servidor de los EE.UU., pero pudo haber sido "de" para Alemania o también "uk" para el Reino Unido. Usted puede usar "EmsXX.your - freedom.de" tanto en la aplicación cliente de YF , o una dirección IP. El "Nombre de destino" o como usted quiera llamarlo, no tiene significado técnico.

Marque " Don't connect now" –necesitamos modificarr algunos parámetros antes de que la conexión esté lista definitivamente.Haga click en Next.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

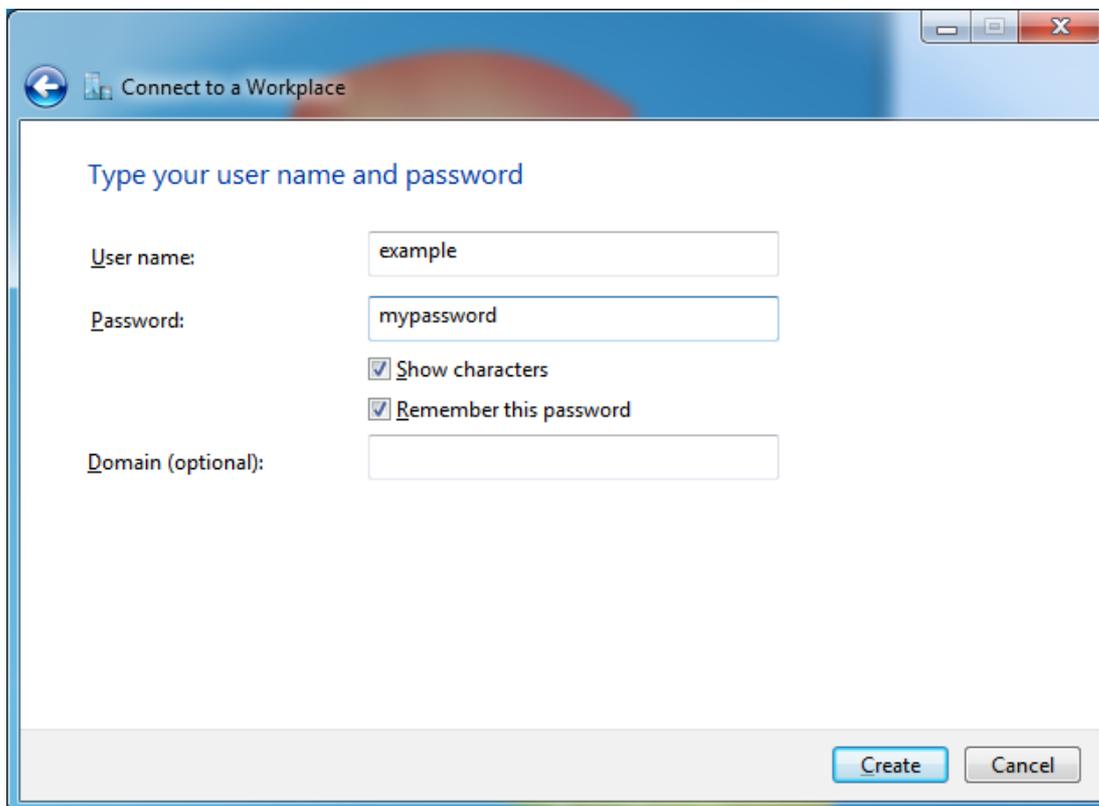
Use a smart card

Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

Next Cancel

En el próximo paso, indique su usuario y contraseña de Your Freedom. Si usted quiere, seleccione "show characters" y "Remember password" (seguro si ésta es su computadora y el acceso está restringido). No la incluya en ningún dominio.Haga click en "Create".



Connect to a Workplace

Type your user name and password

User name:

Password:

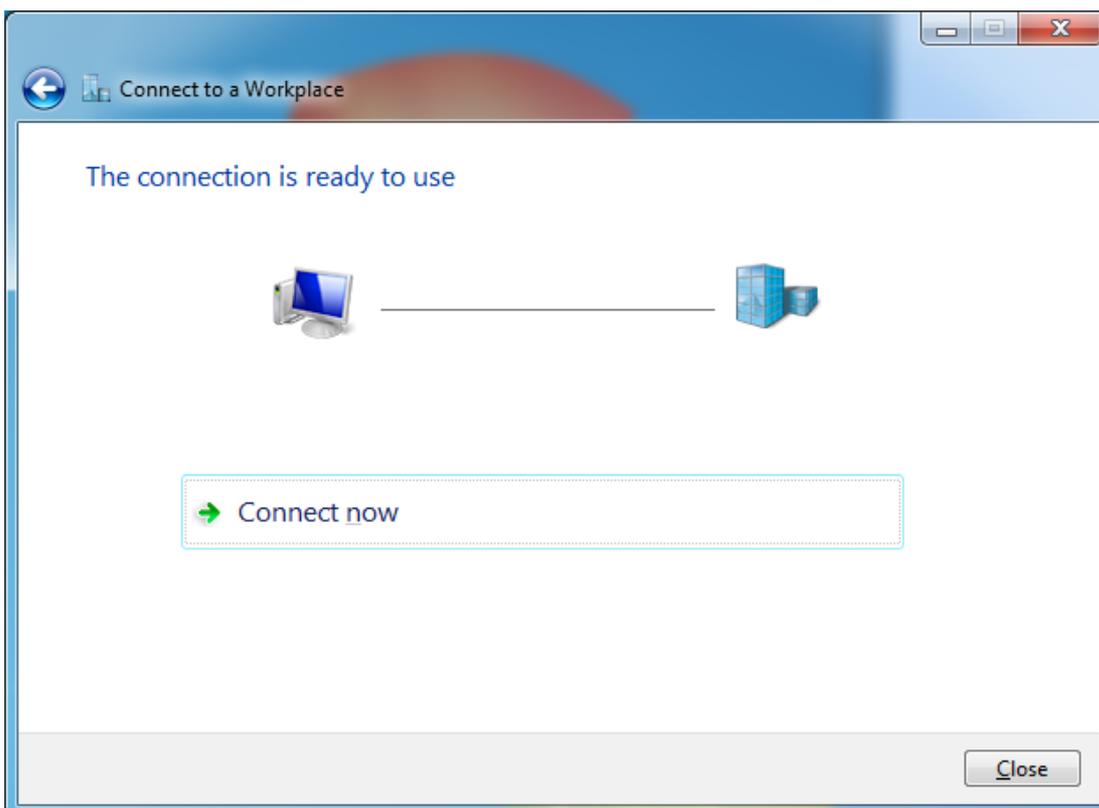
Show characters

Remember this password

Domain (optional):

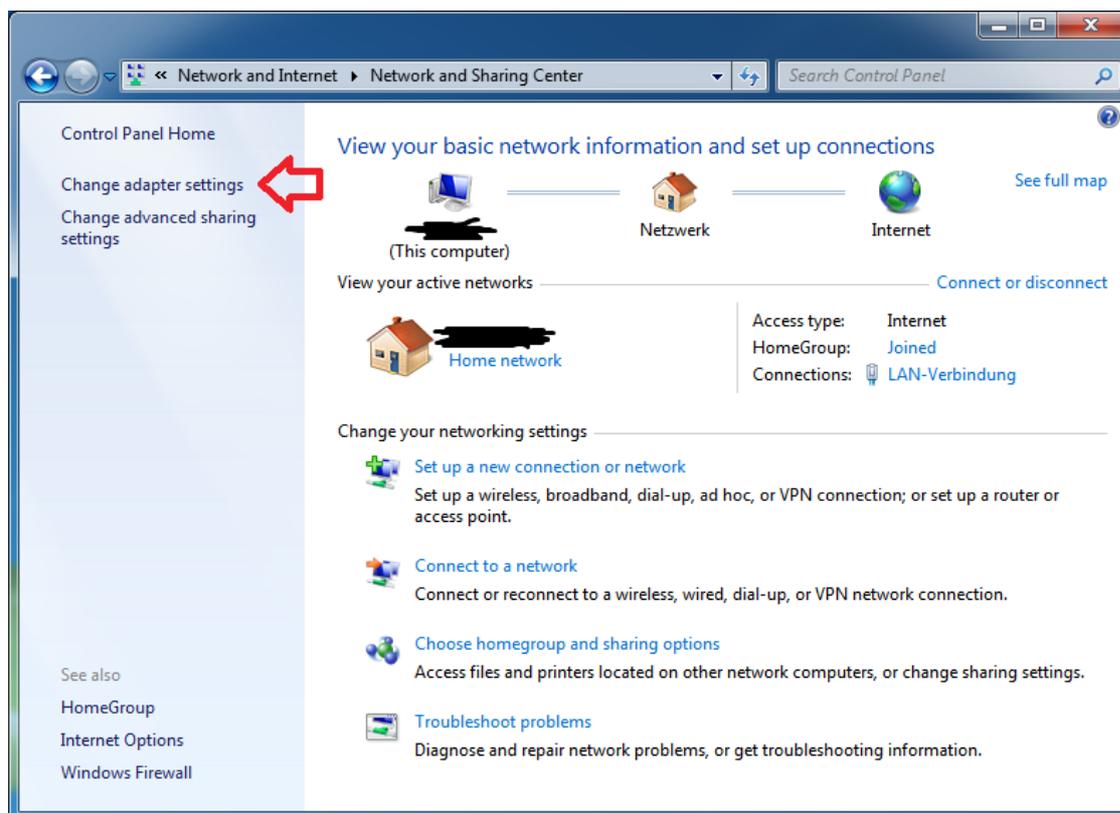
Create Cancel

Windows le indicará que la conexión está lista para usarse, pero no es así. Es por ello que debemos hacer click en el botón de Cerrar.

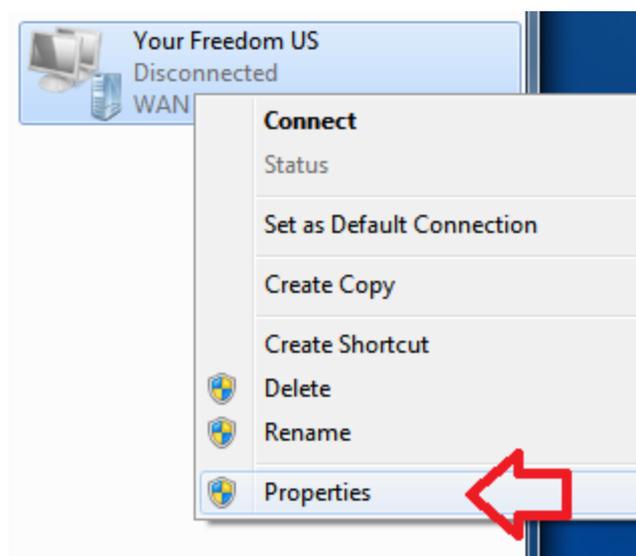


En el "Network and Sharing Center" que todavía debe estar en su pantalla (si no, haga click

en los botón de Windows, " Control Panel ", " Network and Sharing Center " para acceder nuevamente), haga click en " Change adapter settings " a la izquierda:

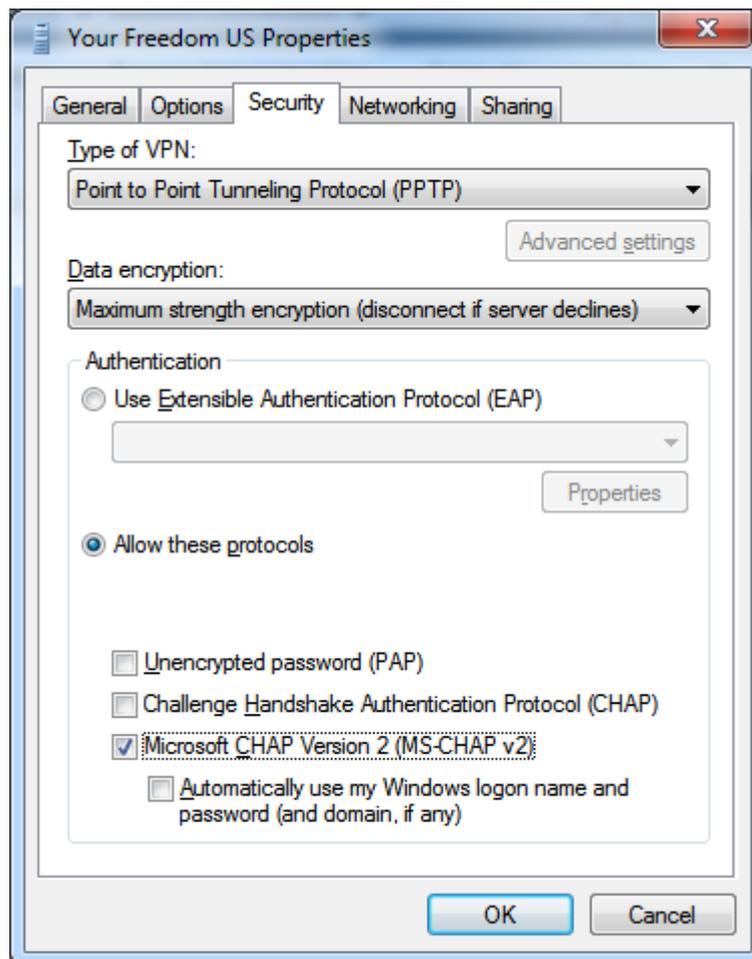


Esto mostrará los adaptadores de red, tanto físicos como virtuales. El adaptador de nueva creación "min puerto WAN" deberá estar entre ellos (se afirman que es un adaptador tipo IKEv2, y es por eso que tenemos que modificarlo). Haga clic derecho sobre él y seleccione "Propiedades":

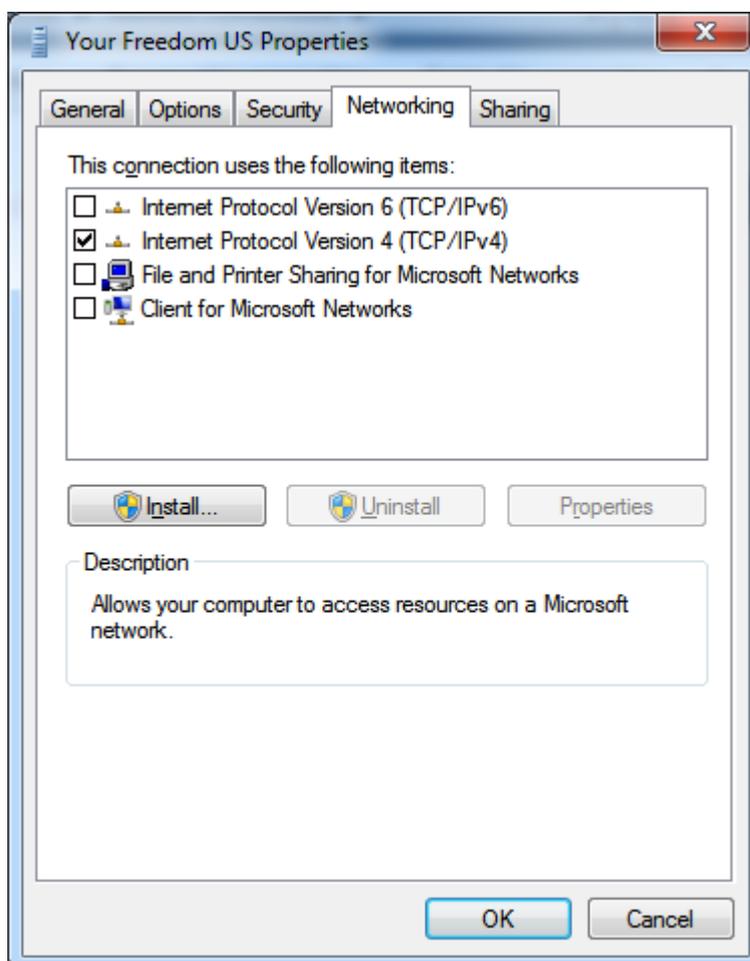


Haga click en la pestaña "Security", cambie las configuraciones por defecto. El tipo del VPN debe ser "PPTP", y usted debe indicar el cifrado de los datos a la máxima fortaleza de encriptación (aunque nuestro servidor se encargara de ello de todos modos). Desmarque la opción "Challenge Handshake Authentication Protocol" y deje marcado " Microsoft CHAP

Version 2" –Necesitamos usar MS - CHAPv2 en lugar de CHAP porque esto es un requisito esencial para la encriptación de datos de MPPE. La pestaña de debe verse de la siguiente manera:

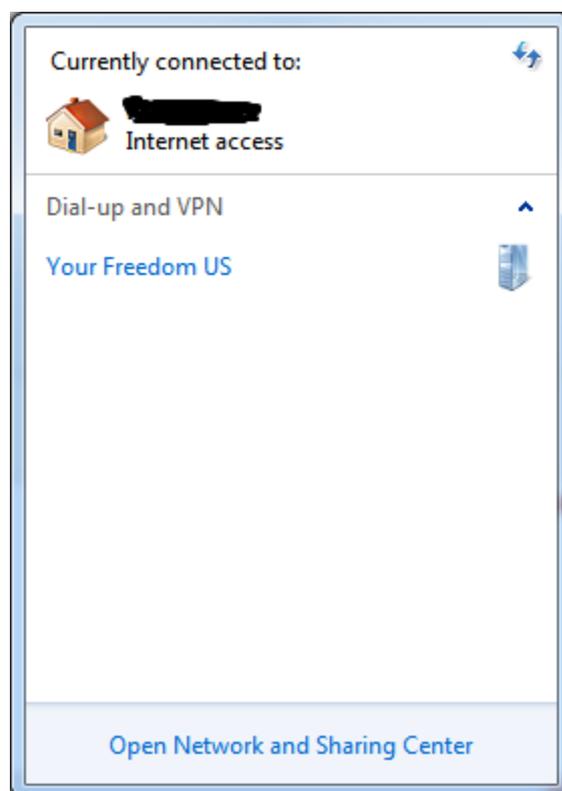


Haga click en la pestaña " Networking" y desmarque todo excepto IPv4 (Esto hará la conexión de VPN menos "Ruidosa", economiza el ancho de banda y acelera ligeramente la configuración de conexión). No puede usar IPv6 hasta este momento porque nuestros servidores no lo respaldan aún:



Haga click "OK".

Ya las configuraciones estan listas. Hay varias maneras de acceder a la conexión. La que funciona para todos es esta: haga click en el botón de Windows, luego " Control Panel", " Network and Sharing Cente", y " Connect to a network". (o si hay un icono de conexión de red en su barra de tareas puede hacer clic en él). Este saca la lista de las conexiones disponibles:



Seleccione la que desee,y haga click en "connect":



Indique su contraseña nuevamente si usted no la salvó durante el proceso de configuración, haga click "Connect", y listo! Aparecerán algunos mensajes de estado, y una vez dejen de mostrarse usted deberá estar conectado. Puede verificar esto en su lista de conexión (ver de arriba) - le indicará que usted ahora está conectado mediante Your

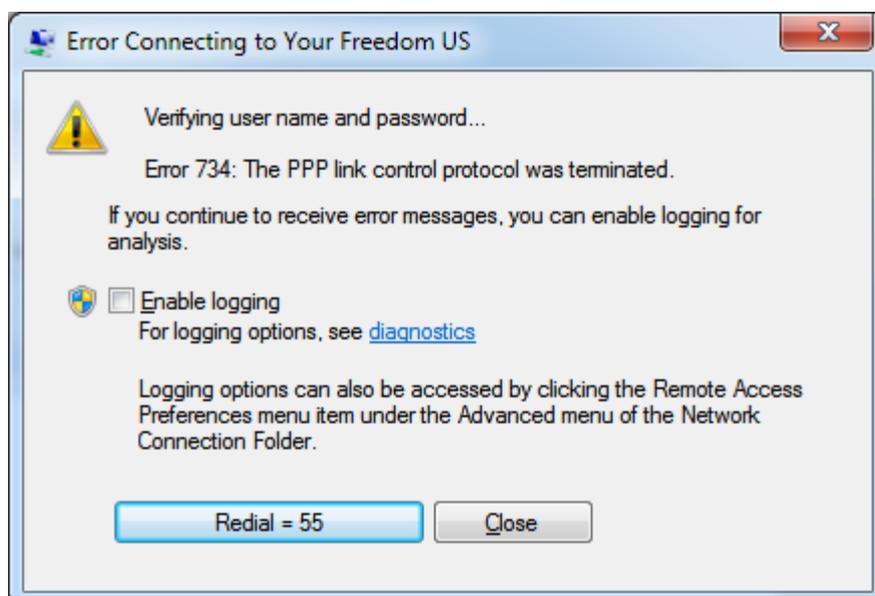
Freedom. Para desconectarse, haga click en la conexión correspondiente en la lista de conexiones y elija "Disconnect".

En este momento, una ventana pop-up le pedirá que indique una " network location" para la nueva conexión. Recomendamos que usted elija "public network" para que evitar riesgos de seguridad innecesarios:



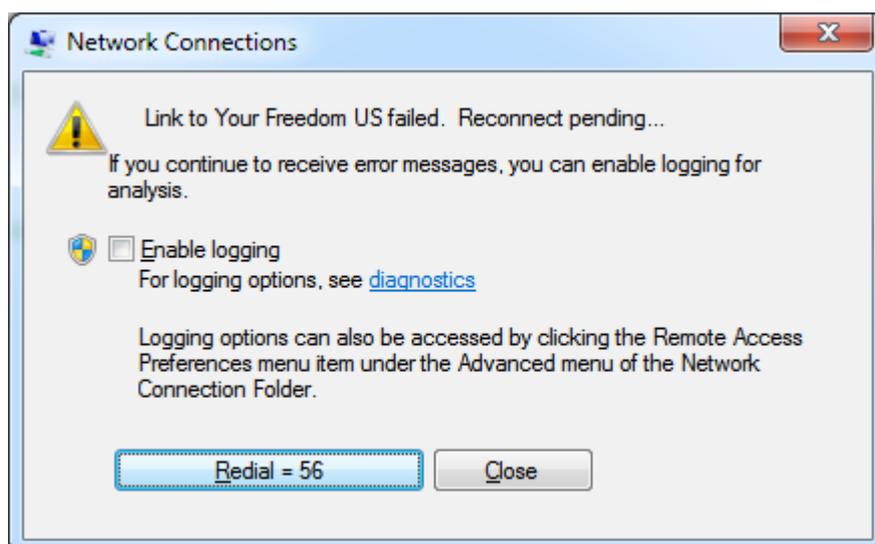
Qué pasa si no funciona?

Recibió este mensaje durante la configuración de la conexión?



Esto indica que nuestro servidor ha negado su inicio de sesión, posiblemente porque nombre de usuario y/o contraseña no eran correctos, o su cuenta ha sido deshabilitada, o usted (como un usuario FreeFreedom) está tratando de acceder a una cuenta premium, o existe algún problema con nuestro servidor. Desafortunadamente no podemos decirlo cuál de éstos es la causa. Si el problema persiste y usted está seguro de que su nombre de usuario y contraseña son correctos, intente loguearse a nuestra página web y vea si su cuenta ha sido desactivada. Si no, verifique si usted está accediendo al tipo de cuenta correcto.

Si ve este mensaje durante la conexión:



Quiere decir que nuestro servidor lo está rechazando muy probablemente. Si usa FreeFreedom podría estar excedida de tiempo, o su cuenta desactivada. Intente reconectarse. Si funciona, era muy probablemente algún problema técnico (un timeout o cualquier otra cosa). Si los problemas persisten, anote todos los detalles pertinentes e indique al soporte técnico sobre ello.

Compartiendo la conexión PPTP

Usted puede usar la funcionalidad de Windows de compartir la conexión a Internet. Puede encontrarlas en las propiedades del adaptador virtual de red (ver de arriba). Por favor note

que usted no puede compartir su conexión con otras computadoras que se encuentran en la misma red que usted usa para correr el tunel PPTP. Un ejemplo sería alguien en un laboratorio de computadoras conectado mediante Ethernet - usted no puede compartir la conexión con otras PCs en el mismo Ethernet. Para compartir la conexión, las otras computadoras tienen que estar conectadas con una interfaz de Ethernet diferente a la que usted no usa.

Servidores DNS

A menos que usted lo configure explícitamente, la conexión de PPTP negociará el uso de los servidores de DNS de Google. Google no sabrá quiénes es usted, solamente verá la dirección IP address de nuestro servidor.

Más que una conexión PPTP predeterminada?

Usted puede configurar tantas conexiones como usted quiere, pero no es recomendable utilizar más que una a la vez. Por ejemplo, usted podría definir conexiones diferentes para países diferentes. Sólo siga el procedimiento indicado arriba para crear más conexiones. Para eliminarlas otra vez, abra el panel de adaptador y elimine el adaptador (Es aquí donde usted puede renombrar una conexión existente también).

Si se está preguntando si usted y su amigo pueden usar una misma cuenta al mismo tiempo, la respuesta es no. Sus cuentas de Your Freedom solo funcionan generalmente para una persona a la vez. Si una segunda conexión es establecida, la conexión previamente iniciada es finalizada. Si usted está en el mismo lugar, usted puede compartir la conexión como se explicó de arriba. .

Tipos de Cuentas:Actualizaciones basadas en tiempo y vouchers

FreeFreedom (uso gratuito)

Your Freedom ofrece un servicio básico gratis. Es lo suficientemente bueno como para introducirnos y familiarizarnos con Your Freedom y probar si nuestra aplicación funcionará bien. Esto puede ser suficiente para algunos.

Hay algunas restricciones en el perfil de FreeFreedom. Primero que todo, el ancho de banda es muy bajo (aproximadamente igual que el que brindan otros competidores solo que Your Freedom lo ofrece gratis). En segundo lugar el número de flujos concurrentes es bajo(pero suficiente para chatear, navegar la web, etc.). En tercer lugar, hay un límite de tiempo de conexión – solo se podrá estar conectado 5 horas en cualquier intervalo de 7 días, 2 horas en intervalos de 24h y además, cada hora que pase el cliente YF se desconectará automáticamente y tendremos que conectarnos otra vez.

Actualizaciones y vouchers

Si usted quiere tener más ancho de banda, más conexiones simultáneas, u otra característica adicional, o simplemente si usted quiere proporcionar ayuda a Your Freedom por sus esfuerzos para brindar acceso a Internet sin restricción a otros, considere comprar un paquete. La tabla de abajo detalla todos los paquetes disponibles, sus características y precios.(En Euros)

	Gratis	Basic	mejoradas	total
de ancho de banda	de 64 Kbit / s	256 Kbit / s	4 Mbit / s	ilimitadas
Streams simultáneos	15	50	100	200
Proxy Web	✓	✓	✓	✓
Socks Proxy	✓✓✓	✓		
OpenVPN modo	✓✓✓	✓		
PPTP modo	✓✓✓	✓		
SOCKS5 modo	✓✓✓	✓		
cifrado Enlace	✓✓✓	✓		
conexión HTTP	✓✓✓	✓		
HTTPS conexión	✓✓✓	✓		
conexión CGI	✓✓✓	✓		
conexión FTP	✓✓✓	✓		
conexión UDP	✓✓✓	✓		

conexión DNS	✓✓✓	✓		
conexión ECHO	✓✓✓	✓		
retransmisión permitida	✓✓✓	✓		
Tiempo de conexión	6 horas	ilimitado	ilimitado	ilimitado de
puertos del servidor	✗✗	✗		✓(5)
Paquete de 1 mes	gratis	€ 4,00	€ 10,00	€ 19,99
3 meses paquete	gratis	€ 10,00	€ 28,00	€ 57,99
6 meses paquete	gratis	€ 17,00	€ 50,00	€ 109,99
paquete de 12 meses	libre	€ 30,00	€ 95,00	€ 199,99

Para comprar paquetes, debe visitar la página Web <https://www.your-freedom.net/> , regístrese, y de clic en la etiqueta “Precios”. Hay una calculadora que nos ayuda convertir precios en Euros a nuestra moneda circulante o al menos a alguna conocida. En el momento en que se escribe esta guía, 1€ corresponde aproximadamente a 1.30 dólares estadounidenses.

Sobre Android, visite la tienda de aplicaciones. Podrá comprar una cuenta premium de la misma forma que puede comprar aplicaciones.

Cuando se compra un paquete, en pocos minutos nuestro perfil de cuenta se actualiza (se recibirá un mensaje cuando eso suceda). Sin embargo algunos métodos de pago se demoran más que otros en completarse. Es conveniente visitar la página de “Precios” en <https://www.your-freedom.net/> para conocer los detalles pues estos pueden cambiar(debemos registrarnos antes para verlo todo). Los paquetes recién comprados son activados en el instante, otros paquetes que no hayan expirado aún son suspendidos. Podemos usar los botones con flechas en la página de precios para reordenar nuestros paquetes en cualquier momento y decidir cuales de ellos estarán actualmente activos y cuales suspendidos.



Valore comprar un paquete si usted usa Your Freedom regularmente, incluso si FreeFreedom es suficiente para usted. Los servidores no crecen en árboles y al equipo de soporte y a los desarrolladores les agradecerá recibir un cheque ocasionalmente.

Vouchers o cupones

Los códigos vouchers son secuencias de caracteres que podemos llenar en un formulario en el sitio Web o directamente en el cliente YF para crear paquetes. Podemos recibir un código voucher de parte del equipo Your Freedom como parte de alguna promoción o en compensación por problemas de servicios, o como expresión de gratitud por alguna ayuda prestada. Podemos comprar vouchers en varias denominaciones como carnés de vouchers. Los vouchers son válidos por un año a partir del día de su adquisición.

Nuestros carnés de vouchers pueden ser usados temporalmente para mejorar nuestra cuenta Your Freedom con un paquete sin tener que pagar por un mes entero y no usar parte de él. También los carnés de vouchers son transferibles (significa que no están relacionados a cuenta alguna) y pueden ser cobrados en diferentes momentos.

El código de los Voucher puede ser adicionado en el panel de voucher en la aplicación de YF. Escriba el código y haga click en "Add". Puede importar todo el carnet de voucher en un intento si usted usa la "Etiqueta" que le hemos enviado por correo electrónico en lugar de los códigos individuales del voucher. Si usted no tiene nuestro correo electrónico de confirmación a mano, sólo entre a nuestro sitio web y visite el sección de CUENTA. Es seguro añadir vouchers o carnets en algunas instalaciones de YF, incluso con cuentas diferentes, pero usted puede usar cada código del voucher solamente una vez. Haga clic en "Actualizar" para verificar automáticamente qué códigos han sido usado, y "limpiar" para retirar todas claves usadas de la lista.

Para usar un código de voucher en particular, haga click en "send sel". Sobre Android, si usted selecciona alguna categorías de códigos, el primer código de voucher sin usarse en esta categoría será enviado.

Si, por cualquier razón, usted no puede registrar códigos de voucher en la aplicación de YourFreedom, usted puede hacerlo a través del sitio web.

Por favor vea la sección de preguntas frecuentes de Voucher en nuestro sitio web para más detalles.

Test drives

Si estamos considerando comprar un paquete pero no estamos seguros si será lo que esperamos podemos probar gratis antes. Después de registrarnos <https://www.your-freedom.net/>, navegamos hacia "Precios", y hacemos clic en "Try before you buy" que se encuentra a la izquierda. Todos podemos probar, pero solo nos es permitido probar con cuentas de nueva creación y que no hayan probado extensivamente con anterioridad. También, rechazan pruebas desde cuentas que hayan estado involucradas en cancelaciones de pagos.

Sin embargo, el equipo de soporte puede ayudar en caso de que se necesiten pruebas adicionales; solo envíe un correo a soporte@your-freedom.net.

Durante la prueba recibiremos todos los beneficios del paquete seleccionado, y lo que es más, podremos cambiar de un paquete a otro para poder probarlos todos. Solo necesitamos visitar la página "Try before you buy" para modificar o terminar las pruebas.

Con los paquetes comprados, tomará unos minutos para que la actualización se propague a todos los servidores. Debe reiniciarse la conexión o incluso el cliente Your Freedom para ver las diferencias.

Con las últimas versiones de la aplicación YF(desktop), usted puede activar "test drivers" desde el panel "Perfil de la Cuenta" o en la tienda de aplicaciones (para Android).

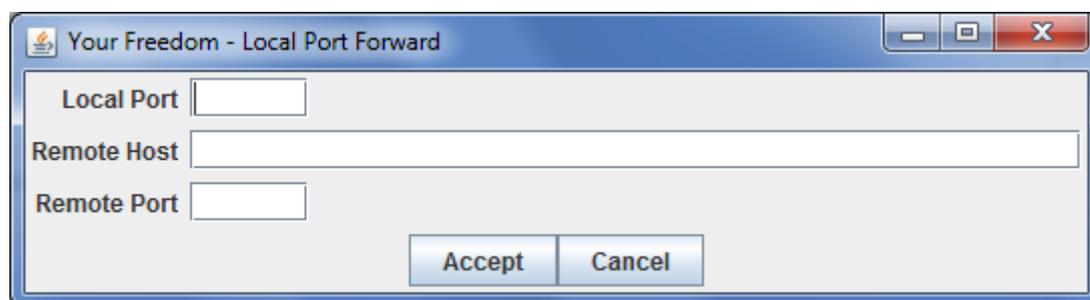
Temas Avanzados

Redireccionamiento de puertos

Por favor tenga en cuenta que este capítulo solamente aplica a la versión de aplicación desktop de YF, no para su aplicación Android.

Redireccionamiento de puertos locales

Otra vía de permitir que una aplicación se conecte a un servicio en la Internet a través de Your Freedom es hacer en nuestra PC un espejo de un puerto existente en Internet. Supongamos que hay un servidor en Internet con una cierta dirección IP y está escuchando por conexiones SSH. Queremos conectarnos a ese servidor pero nuestro cliente SSH no permite que se le configure un Proxy SOCKS. En este caso simplemente configuraremos un redireccionamiento de puerto local similar al siguiente.



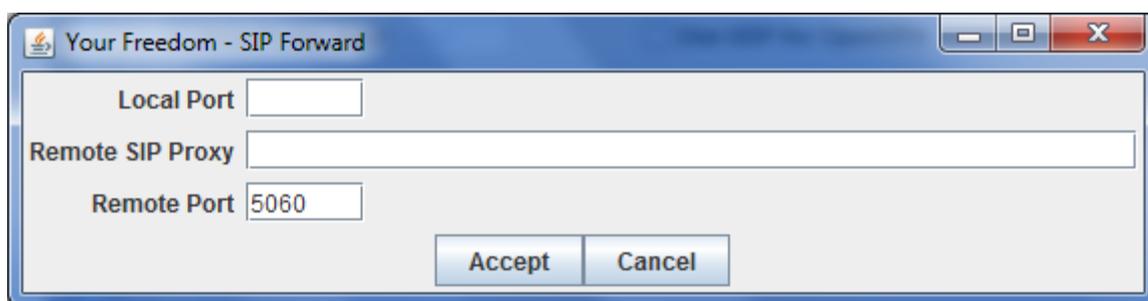
Ahora en vez de conectarnos por SSH a "some.host.somewhere" por el puerto 22 simplemente le ordenamos al cliente SSH que se conecte a localhost por el puerto 2222. Your Freedom se encargará de hacer el puente. Es válido señalar que si el servidor remoto no es alcanzable el cliente SSH se comportará como si la conexión se hubiera establecido pero más temprano que tarde dará un error.

Esto es solo un ejemplo de como usar esta funcionalidad. En general si una aplicación necesita conectarse a un servidor determinado por un puerto un redireccionamiento de puerto local constituye una buena opción.

Redireccionamientos SIP

En efecto, se pueden usar teléfonos SIP con Your Freedom. Hemos escuchado que el audio solo trabaja en una dirección pero una vez que determinemos la causa de esto lo corregiremos. Esto está aún en una fase beta avanzada, y puede no funcionar del todo. En cualquier caso, el modo OpenVPN probablemente sirva.

Supongamos que estamos usando un servidor SIP llamado "sip.sipgate.de" por el puerto 5060 (el puerto oficial de SIP). Si se configura un redireccionamiento de puerto SIP como este:



...el ordenador será desde ese momento un espejo del servidor SIP. Desde ese momento el teléfono SIP se configuraría para apuntar hacia el servidor “localhost”. Es recomendable deshabilitar STUN ya que no tendría sentido en este contexto (solo haría las cosas más lentas)

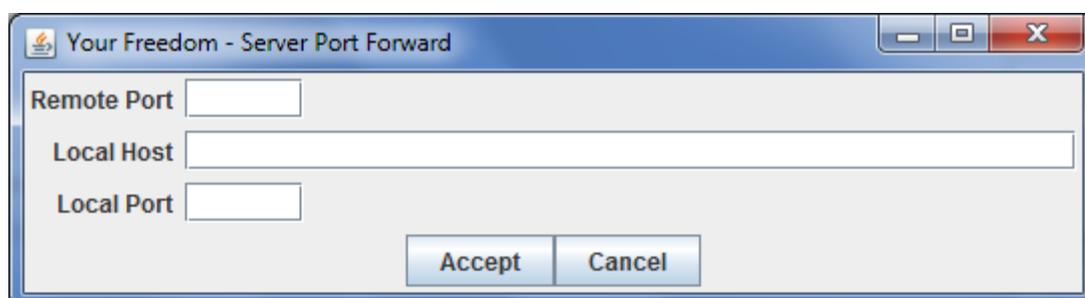
Los redireccionamientos SIP son una tarea compleja, en la cual el cliente no solo tiene que redireccionar todas las peticiones sino que también tiene que dinámicamente establecer redireccionamientos UDP para todas las sesiones de audio y video. No lo hemos probado con muchos proveedores SIP o teléfonos, así que probablemente no funcione bien en todos los casos. Cualquier retroalimentación de parte de los usuarios será bienvenida.



Los redireccionamientos SIP solo funcionan con UDP, no TCP. Casi todos los clientes y servidores usan UDP. Además, tengase en cuenta que usar un teléfono SIP consume cierta cantidad de ancho de banda (dependiendo de los Codecs que se usen); el perfil FreeFreedom probablemente no sea lo suficientemente rápido para soportar redireccionamientos SIP (la voz se entrecortará).

Redireccionamiento de puertos del servidor (RPS)

Si se desea hacer que el ordenador sea visible desde Internet utilizar redireccionamiento de puertos de servidor puede ser la opción. Antes verifíquese la pestaña “Información de Cuenta” después de establecer la conexión, si se logra ver entre comillas “Redireccionar puertos remotos” significaría que el perfil de cuenta está habilitado para utilizar este servicio (se puede configurar de todas formas pero si el perfil no lo permite no funcionará). Es importante entender que solo se puede redireccionar puertos de servidor que estén asignados al perfil. Los redireccionamientos se configurarían de esta forma:



No es absolutamente necesario asignar los mismos números para “puerto remoto” y “puerto local”, pero hemos encontrado casos de aplicaciones que ocasionan problemas porque anuncian otro puerto hacia la red diferente al que están realmente usando para escuchar. Por ejemplo, los clientes de BitTorrent usualmente pueden anunciar IP externas

diferentes y puertos, pero 99% de los rastreadores simplemente ignorarán esto. Así que por favor use el mismo puerto en ambos extremos (configurando las aplicaciones acorde a este escenario).

Los puertos son asignados de manera secuencial; no se asignan puertos especiales a petición del usuario.

Usos más comunes de un RPS:

- Hacer nuestra PC accesible desde internet, ej. rdesktop, VNC, SSH
- Obtener una ID alta en eMule
- Acelerar las descargas BitTorrent.



Actualmente solo los usuarios de paquetes TotalFreedom pueden acceder a este tipo de redireccionamiento

Compartir nuestra conexión con otros

Retransmisión

Si nuestro perfil soporta “Retransmisión para otros” y hemos activado la funcionalidad, otras personas en nuestra red local podrán configurar sus navegadores para conectarse a internet usando nuestro cliente Your Freedom a manera de proxy de la misma forma que nosotros lo hacemos. Todo lo que deben hacer es especificar la dirección IP de nuestra computadora y el puerto 8080 (o el valor que hayamos configurado en la casilla Proxy Web), o 1080 (proxy socks) en sus aplicaciones dondequiera que se requieran los datos de un proxy.

El uso más común es compartir nuestra conexión con compañeros de cuarto o colegas en nuestra oficina.

Usando OPENVPN y ICS para conectar otras PCs, Playstations, Xbox, etc.

Si quisiéramos conectar nuestras PCs, Playstations, teléfonos VoIP, o alguna otra cosa a Internet a través de Your Freedom, todo lo que necesitamos es una segunda interfaz de red. Asegurémonos que no está siendo usada para nada más. Necesitamos conectar nuestra PC/Playstation/etc. a esta interfaz de red, lo mismo directamente (con un cable cruzado) o a través de un pequeño bug/switch. No debemos usar el mismo cable de red o hub que nuestra otra interfaz (menos la que provee VLANs). Otra cosa que debemos tener en cuenta es que nuestra otra Interfaz de red no use una red 192.168.0.0/24 – si así fuese, debemos reconfigurar nuestra DSL o router para que utilice otra red diferente.

Abramos al menú Inicio -> Panel de Control -> Conexiones de Red. Seleccionemos la interfaz de red local que no estamos utilizando (probablemente se llame “Local Area

Network 2” o algo similar). Después busquemos la interfaz de red TAP32 que viene con OpenVPN. Damos clic derecho encima y escogamos “Propiedades” -> “Avanzado” y seleccionemos “Permitir a otros usuarios de esta red conectarse a través de ésta conexión a internet” y escogamos la interfaz de red que conecta a nuestra otra PC/Playstation/etc. Damos clic en “Aceptar” y cerramos la ventana de Network Connections.

Eso es todo. Ahora podremos conectarnos a internet desde nuestra otra PC/Playstation siempre que tengamos nuestra conexión a Your Freedom con OpenVPN activado.

Enlazando el funcionamiento de Android con Your Freedom

Esta funcionalidad desafortunadamente no es posible. Existen varias razones para ello. Primero que todo la API VPN de Android no soporta la configuración de direcciones sobre tuneles de interfaces. En segundo lugar es que el enlace no soporta una pasarela por defecto a tu PC cuando la conexión VPN se active. Estamos seguros que esto se debe a medidas de seguridad.

Por su puesto que puede tener la aplicación de Your Freedom en su PC y correr esta version de la aplicación Android, siempre y cuando use la conectividad de su móvil para conectarse.

IPV6

El cliente Your Freedom puede usar IPv6 para conectarse a los servidores YF. Las direcciones IPv6 pueden alcanzarse a través de SOCKS5 y la facilidad de redireccionamiento de puerto local, pero no a través de OpenVPN o proxy web. Tengase en cuenta también que no todos nuestros servidores soportan IPv6.

Si estamos teniendo problemas conectándonos o meramente encontrando servidores de Your Freedom es una buena idea intentar habilitar IPv6 en nuestra PC (si es que no está ya habilitada). También, habilitaremos todo tipo de mecanismo de túnel, nunca se sabe – uno de ellos puede funcionar desde donde estamos.

En Windows Vista y Windows 7, tanto IPv6 como Teredo están habilitados por defecto, pero a menos que nuestra PC tenga una IP global estos mecanismos no van a funcionar. Para hacerlos funcionar, damos clic en “Inicio” y después teclémos “cmd” pero no presionemos “Enter”. Esperemos que “cmd.exe” aparezca, demosle clic derecho y escogamos “Ejecutar como Administrador”. Cuando la consola abra teclémos

```
netsh interface ipv6 show teredo
```

Si "status" es "offline" introduzcamos:

```
netsh interface ipv6 set teredo enterpriseclient
```

Esperemos un rato y chequeemos el estado otra vez:

```
netsh interface ipv6 show teredo
```

Deberá salir que “status” es “qualified” o “dormant”. Cuando termine demos “exit”.

Con Windows XP SP1/SP2, Teredo viene incluido pero no está instalado por defecto. Podemos fácilmente arreglar eso abriendo una ventana de comandos (damos clic en “Inicio” -> “Ejecutar” y teclémos cmd). Una vez abierta la consola teclémos “netsh

interfaceipv6 install", y después procedemos como describimos arriba (o simplemente tocamos "netsh interface ipv6 set teredo enterpriseclient").

A menos que alguien filtre Teredo esto debe darle a tu computadora conectividad plena por IPv6. El cliente notará automáticamente esto e intentará acceder a los servidores por IPv6.

Ajustando el modo CGI

De modo general, el modo de conexión CGI es el más lento de todos los modos de conexión posibles. Esto se debe a la forma en que éste modo trabaja; se necesita de una acumulación de datos antes de enviarlos hacia el otro lado. Pero siempre se pueden ajustar algunos parámetros y hacer que esto funcione más rápido.

En primer lugar, localicemos el fichero de configuración ".ems.cfg". Este fichero puede ser editado con cualquier editor de textos, por ejemplo el Notepad. Asegurémonos que el cliente Your Freedom no esté ejecutándose mientras editamos este fichero o nuestros cambios pueden perderse.

Hay cuatro valores que controlan el comportamiento del modo CGI. No recomendamos cambiar ninguno de estos parámetros excepto quizás "cgi_uplink_maxdelay". Aquí están los parámetros y sus valores por defecto:

- `cgi_uplink_maxdelay`. 500 milisegundos por defecto. El cliente acumulará datos como máximo por este tiempo hasta que se inicie una o hasta que se inicie una nueva conexión ascendente, sin importar la cantidad de datos que se hayan acumulado. Quizás se pueda poner esto a un valor menos, quizás 200 milisegundos.
- `cgi_uplink_urgentdelay`. Puesto a 20 milisegundos por defecto. El cliente Your Freedom usará este valor en lugar del valor anterior cuando tenga marcos que entregar que se consideren urgentes, por ejemplo "ACKs".
- `cgi_uplink_threshold`. Por defecto a 3. Si esta cantidad de marcos (marco es la unidad de datos de YF) están listos para entregar, se creará una conexión ascendente inmediatamente. Establecer este valor a 1 deshabilitará la acumulación de datos y hará que la conexión actúe de manera más inmediata, pero creará también mucho tráfico adicional. Si la cantidad de conexiones establecidas no es importante se puede poner este valor a 1 y no preocuparnos por el resto.
- `cgi_uplink_mindelay`. Por defecto a 1 milisegundo. Esta es la mínima cantidad de tiempo entre dos conexiones ascendentes. Este valor nunca debiera ser 0 y en la mayoría de los casos no debiera ser necesario incrementarlo, pero si nuestra conexión se interrumpe cuando los intentos de conexión se acumulan, fíjese a un valor superior.
- `cgi_downlink_connect_timeout`

Todos estos valores normalmente no aparecen en el fichero de configuración y no son configurables a través del front-end. Solo debemos agregar líneas al fichero(no importa donde) que contengan el nombre de la llave, un espacio y un valor numérico(omitir las unidades).

El desempeño óptimo probablemente se logre estableciendo el `cgi_uplink_threshold` a 1

ycgi_uplink_mindelay a quizás 20. Intentémoslo, no se puede romper nada, si no funciona, simplemente quitémos la línea.

Anexo

Diagnóstico de errores

El cliente Your Freedom viene con una serie de provisiones para el diagnóstico de errores. Hay un registro de mensajes que se pueden acceder por la pestaña “Mensajes” (se pueden salvar a un fichero) pero solo pueden ayudar en situaciones ordinarias. Para un mayor nivel de detalle se necesita ejecutar el cliente Your Freedom en modo “dump”. Usar un analizador de paquetes puede ser útil para las personas más duchas.

¿Por qué no funciona mi aplicación?

No hay una respuesta absoluta para este tipo de pregunta. Lo primero que debemos chequear es el panel de flujo de nuestro cliente Your Freedom. ¿Se registra actividad de flujo después que se inicia la aplicación y antes de que ésta reporte error al conectarse? Si no, entonces no está configurada correctamente. Chequeemos si las propiedades del Proxy en la aplicación están correctas – si se está ejecutando la aplicación en la misma PC que el cliente Your Freedom, pondremos “localhost” o “127.0.0.1” en la dirección del Proxy, y 1080 (SOCKS) o 8080 (web/http/https) en el puerto del Proxy. Si la aplicación está corriendo en otra PC debemos asegurarnos de tener habilitada la retransmisión para otros (en la pestaña de Puertos) y si está permitida por el perfil (pestaña Cuenta), y que se ha usado como la dirección de Proxy la dirección local LAN de la PC donde el cliente Your Freedom se está ejecutando.

Verificaremos el panel de mensajes en el cliente Your Freedom – si vemos mensajes de protocolos bloqueados entonces necesitamos otro servidor de Your Freedom, el que está usando ahora no soporta el protocolo que necesitamos.

Siempre es bueno echarle un vistazo a la documentación online. Sabemos que no es perfecta y que la página introductoria no es muy atrayente pero hay muchas mas cosas ahí de lo que parece. <https://www.your-freedom.net/4/>

Otro plan podría ser darle un vistazo a los foros de usuarios. Quizás alguien más haya tenido el mismo problema antes. Los foros pueden encontrarse en: <https://www.your-freedom.net/2/> .

Realizando una prueba de velocidad

Una prueba de velocidad es una manera muy directa de saber cuanto tráfico por unidad de tiempo puede ser manejado por nuestra conexión Your Freedom. Para esto deberá generarse tráfico de aplicación suficiente para saturar los vínculos ascendente y descendente. Para esto podremos usar una aplicación que genere suficiente ancho de banda o simplemente usar el generador de tráfico embebido de Your Freedom. Para poder usarlo, iniciemos el cliente y creemos un redireccionamiento de puerto local desde un puerto (por ejemplo 1234) a un host virtual llamado “speedtest” por el puerto 0. Entonces abrimos una consola de comando(en Windows vayamos a “Inicio” -> “Run” y ejecutemos “cmd”). En esta consola escribámos “telnet localhost 1234” (o el puerto que sea) – la prueba comenzará y se extenderá por 1 minuto usando el enlace a la mayor velocidad posible. Durante la prueba de ancho de banda, todas las restricciones de ancho de banda

vigentes se seguirán aplicando. No se reportarán usos del enlace que superen aquellos límites impuestos por nuestro perfil o por la velocidad que nuestros cursores de ancho de banda indican (en la pestaña principal), pero las lecturas de ancho de banda deberán ser muy cercanas al lo que tienen marcado los cursores de ancho de banda. Si no fuese así, entonces hay alguna otra limitación en la conexión que usamos agena a Your Freedom. Tratemos de ajustar el cursor de enlace ascendente un poco por debajo de la velocidad que marcó la prueba, esto puede mejorar la velocidad de conexión en la dirección contraria. Esta característica de generación de tráfico tiene como objetivo ser utilizada para diagnóstico de errores, no debe ser usada con mucha frecuencia. La mejor justificación para efectuar una prueba de velocidad es que el equipo de soporte así nos lo pida. Para los mejores resultados de prueba, usted debe realizar pruebas de velocidad múltiples en paralelo. Una actividad de flujo individual no podrá saturar una conexión rápida.

Creando un fichero “dump”

Desktop

Dependiendo de como se inicie el cliente Your Freedom, hay varias formas de iniciar el modo “dump”. Todas estas formas tienen en común que usan la opción de línea de comandos, pero puede estar oculta por el entorno de escritorio. La versión de instalador de Windows se puede ejecutar en el modo “dump” desde el menú de inicio; ellos crean un fichero llamado “dump.log” en el escritorio(en el caso de los sistemas Unix, este se creará en el directorio “home”). Si estamos ejecutando el cliente desde la línea de comandos, usaremos la opción `-dump=somefile` para activar el modo “dump”. Se notará que merma el rendimiento ligeramente cuando se activa este modo, y el fichero “dump” irá creciendo con el tiempo.

Normalmente, el cliente no guardará ningún paquete de datos real. Denecesitare tal cliente especial el equipo técnico de Your Freedom se encargará de dar uno especial para la ocasión.

Lo que aparece en el fichero “dump” no es difícil de interpretar para el ojo entrenado, probablemente muchas de las cosas ahí presentes tengan sentido para nosotros, otras solo tendrán sentido para los desarrolladores o el equipo de soporte técnico.

Por otra parte, los ficheros “dump” pueden llegar a ser verdaderamente grandes, si vamos a enviarlos por correo debemos comprimirlos. Como son ficheros texto sutasaa de compresión es alta, y se tornan muy pequeños. No es recomendable usar algoritmos de compresión propietarios, ha de usarse preferiblemente ZIP o Gz o cualquier formato archivo comprimido.

Si tenemos problemas con la conexión, será de gran ayuda ejecutar el asistente (Wizard) en el modo “dump” también.

Android

Acceda a la configuración del menú,haga click en "Configuración General". Seleccione la opción "enable dump mode", recomendamos que marque también "Compresión usando gzip"; le ahorrará al paso adicional de comprimir el archivo dump. No seleccione "Extensivo" a menos le indiquemos. Su archivo dump aparecerá en la tarjeta de SD en un directorio called "Your Freedom Dumps". Es posible que necesitará una aplicación como

"ES Explorador de Archivo" (Altamente recomendada!) para hacérselo llegar por correo electrónico, o acceder a él conectando su teléfono o tablet a su PC.

Usando un analizador de paquetes(sniffer)

Esto es depuración cruda y es solo para los audaces. Pueden existir situaciones donde el equipo de soporte nos pregunte si podemos usar un sniffer para localizar los problemas en nuestra conexión o aplicación. El equipo de Your Freedom recomienda usar Wireshark (disponible en www.wireshark.org o www.ethereal.org – Ethereal es el nombre histórico de Wireshark). En la mayoría de los casos debemos ejecutar Wireshark en la misma PC que el cliente Your Freedom, y debemos capturar en la interfase que conecta el cliente YF con el servidor YF o en la interfase que conecta otras PCs con la PC del cliente de YF, dependiendo de la naturaleza del problema. Iniciar la captura de paquetes, entonces procederemos a recrear el problema y después detener la captura. La salvamos a un fichero y la enviamos (comprimida).

Actualizando el cliente

Es altamente recomendable que actualice su instalación de vez en cuando para asegurar las correcciones de bugs realizadas e incorpore las últimas características.

El proceso de actualizar la instalación de la aplicación YF es muy fácil, tanto en Windows como en Android: solo tiene que hacer uso de la funcionalidad actualizar, y seguir las instrucciones. Si por alguna razón, usted necesita actualizar manualmente, sugerimos que se siga este procedimiento para actualizar la instalación (eso es para Windows, pero en cualquier otro sistema el procedimiento es similar – descargar, desinstalar, e instalar):

1. Verificar si hay nuevas versiones publicadas en <https://www.your-freedom.net/index.php?id=downloads>(comparemos la versión con la que aparece en la pestaña "About").
2. Descarguese la nueva versión si hay alguna. Es conveniente que guardemos una copia de la instalación anterior hasta que estemos seguros que la nueva versión trabaja adecuadamente, por si tenemos que regresar a la versión anterior).
3. Una vez descargada la nueva versión debemos desconectarnos y cerrar el cliente YF.
4. Desinstalar la versión actual por medio de "Inicio"-> "Programas"-> "Your Freedom"-> "Desinstalar" o a través del "Panel de Control". Si bien suele ser seguro instalar nuevas versiones sobre versiones anteriores esto puede fallar cuando se usan instaladores diferentes. Además, no hay razón para no desinstalar, ya que las configuraciones se preservan.
5. Instalar la nueva versión descargara ejecutando el fichero del instalador y siguiendo las instrucciones en la pantalla.

Si se detecta que la nueva versión deja de hacer algo que la anterior hacía bien envíenos un correo a soporte@your-freedom.net(incluyendo ambas versiones y el tipo de instalador, NSI – el más pequeño – o JET – el más grande).

Los números de versiones generadas en los clientes siguen el siguiente patrón:

AAAAMMDD-Serial

AAAA = Año

MM = Mes

DD = Día

Serie = consecutivo dentro del día.

Ejemplo: 20101108-02, sería la segunda versión liberada el 8 de noviembre del 2010.



Sobre Android, las actualizaciones son automáticas mediante Google Play (recomendamos que habilite actualizaciones automáticas en Google Play). Si prefiere usar nuestra funcionalidad de repositorio de actualizaciones, puede encontrarla en la opción de configuración del menú.

Temas relacionados con el país de origen

Planes específicos para países.

Your Freedom tiene planes especiales creados para aquellos que se conectan desde ciertos países en los que el acceso a Internet está restringido. Omitimos la lista de dichos países aquí, más información puede ser encontrada en nuestro sitio web.

En dichos países el paquete FreeFreedom se comporta de manera diferente. Según el lugar desde el que nos conectemos, el paquete FreeFreedom puede exhibir variaciones las cuotas de tiempo y el ancho de banda. Como regla general el límite de tiempo de conexión pasa de 2h por día a ilimitado. Estos límites se activan en el momento en que un usuario se conecta desde un país afectado. El resultado más usual es que los usuarios pueden mantenerse conectados por el tiempo que lo estimen conveniente.

Destacar que es a veces técnicamente imposible determinar si una conexión viene o no de un país que se encuentra en nuestra lista, sobre todo si usa modo de conexión de DNS.

Disponibilidad de los servidores por países

Varios de nuestros servidores no están disponibles para usuarios de todos los lugares todo el tiempo. Limitamos el acceso de algunos servidores en función de su situación geográficamente estratégica, así evitar su sobrecarga desde otros lugares cuando realmente pueden usar otros servidores .

Otra razón es la auto-protección, como impedir que ese servidor sea abusado por spammers. La mayor parte del SPAM viene del mismo país. La experiencia nos ha enseñado que no hay necesidad de permitir que usuarios recién registrados se conecten y abusen de estos servidores y pongan en vilo de esta manera la relación con nuestros proveedores.

Existen sin embargo servidores para todo el mundo sin importar el país desde el que se accedan. Para información actualizada sobre el tema visite nuestro sitio web o escribanos un correo al equipo de soporte.



Algunos servidores pueden denegar la conexión desde ciertos países como una medida de protección contra abusos. Cuando a un usuario se le deniega la conexión por causa de alguna política aplicada al país desde el que se está conectando el cliente YF puede emitir un mensaje “Autenticación no válida para su país de residencia”. Inténtelo con otro servidor.

Tweaks

“Tweaks” es básicamente una serie de reglas y código específicamente creado en el cliente YF para conectarse en algunos entornos de red donde la conexión es más difícil. La mayor parte de la gente no necesita esto y se puede dejar deshabilitado. De hecho, si uno está pudiendo conectarse bien, los Tweaks no harán ninguna falta.

Los nombres de los Tweaks son bastante explícitos. Éstos han sido agregados después que hemos descubierto como hacer que el cliente YF se conecte en ciertas condiciones de red (normalmente muy bien representadas en ciertos países) donde las técnicas normales no parecen funcionar.

El fichero de configuración de Your Freedom

El cliente Your Freedom almacena todas sus configuraciones en el directorio home en un archivo llamado `.ems.cfg`.

Si queremos copiar el fichero y editarlo, asegurémonos que el cliente Your Freedom no está ejecutándose. El fichero está en texto plano, por lo que es fácil su edición en los editores de texto ordinarios. (por ejemplo, pico o bien sistemas Unix, o Notepad en Windows).

¿Dónde está el directorio home?

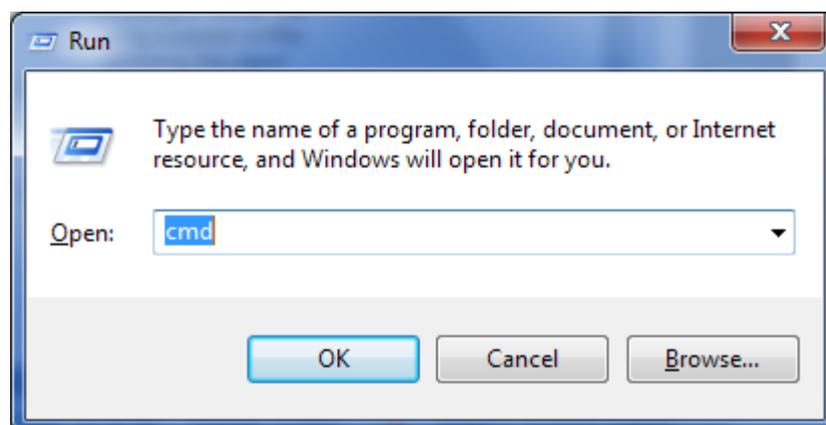
Los usuarios de Unix normalmente saben donde está, ya que están ahí todo el tiempo. En la mayoría de los casos hay un directorio llamado `/home` conteniendo un subdirectorio para cada usuario. El fichero de configuración tiene nombre `".ems.cfg"` aunque quizás no se muestre porque es un fichero "oculto" (empieza con un punto). Si queremos verlo debemos ejecutar `"ls -a"`.

Con Windows Vista y Windows 7, abrir un Explorador e ir a `"C:\Users"`. Ahí encontraremos un directorio para cada usuario, el nombre del directorio debe coincidir con tu nombre de usuario. Éste directorio es tu carpeta o “directorio home”. En entornos Windows, la variable `%HOMEPATH%` apunta a ésta carpeta. Ahí encontrará un directorio llamado `"AppData"` (si no tiene deshabilitado que no se muestren los ficheros del sistema como se indica en on

<http://www.techrepublic.com/blog/window-on-windows/quick-tip-reveal-hidden-system-files-in-windows-explorer/2467>), dentro de "Local", dentro de "Your Freedom" se encuentra el fichero de configuración ".ems.cfg" .

En versiones de Windows más antiguas, la carpeta "home" está situada en "C:\Documents and Settings", y dentro se encontrarán las carpetas con los nombres de los usuarios.

Un recurso nemotécnico para encontrar rápidamente la carpeta "home" pudiera ser ejecutar "cmd" desde la ventanilla "Ejecutar" (después de tocar Windows + R).



Nos encontraríamos frente a una terminal negra con un cursor parpadeante. El texto a la izquierda es el camino a tu carpeta home.

```
C:\Users\ myusername>_
```

Opciones de configuración

¡Atención! Algunas de las opciones listadas a continuación están marcadas como “ocultas”, lo que significa que no son accesibles a través de la ventana “Configuración”, solo usando un editor de texto. Estas opciones son para aquellos que saben lo que están haciendo. Si existen dudas debe consultarse primero el soporte técnico.

Es importante notar que todas las opciones son en minúsculas. Existen opciones que solo pueden aparecer una vez en un fichero de configuración (marcadas como “simple”), otras pueden aparecer más de una vez (tipo “multi”). Las opciones que aceptan un solo argumento tratarán a todo lo que sucede al primer espacio después de su nombre como parte de ese argumento, préstese atención al final de cada línea y evítese los espacios innecesarios. Se pueden usar comentarios también (líneas que empiezan con un “#”) pero éstos desaparecerán la próxima vez que el cliente salve la configuración.

Lo que sigue es la lista en orden alfabético!

Opción	Descripción	Tipo	Argumentos
aes	Activa o desactiva la fuerte encriptación (AES)	booleano opcional	"true" (valor predeterminado) o "false"
autoscroll_messages	ventana de Scroll mensaje automáticamente cuando aparecen nuevos mensajes	booleanos opcionales	"verdadero" o "falso" (por defecto)

avoid_dns	Use la dirección IP del servidor, no el nombre de host (si se conoce)	booleano opcional	"true" o "false" (por defecto)
bandwidth_unit	unidad de visualización para anchos de banda	entera opcional	"bit / s"(predeterminado) o "Bytes / s "(EXACTLY!)
barf	informaCrash	múltiples base64 FYI	Contiene base64 informes de errores codificados aún no ha enviado a nosotros. Estos informes no contienen datos de carácter personal.
bw_downlink	deseado enlace descendente (el servidor al cliente) de ancho de banda en bits por segundo (ajuste deslizante)	enteros opcionales	bits por segundo. 0 means "ilimitado".
bw_uplink	deseado enlace ascendente (el cliente al servidor) de ancho de banda en bits por segundo (ajuste deslizante)	enteros opcionales	bits por segundo. 0 means "ilimitado".
cgi_downlink_connect_timeout	tiempo de espera de conexión de enlace descendente en modo CGI, en milisegundos	enteros ocultos	predeterminados para connect_timeout
cgi_downlink_reconnect_delay	descendente temporización de reconexión en modo CGI, en milisegundos	enteros oculta	por defecto 500 ms
cgi_uplink_maxdelay [†]	Plazo máximo antes de tramas en cola desencadenan un conexión	entero escondida	Después de este tiempo, la cola se vacía por mucho los datos se va a enviar (en su caso). predeterminado para 500 ms
cgi_uplink_mindelay [†]	Retardo mínimo para que se active una nueva conexión	entero escondido	el retardo mínimo entre dos descargas de colas (POST). to 1ms defecto.
cgi_uplink_threshold	Número de tramas en cola que causan mindelay a utilizar en lugar de maydelay	única oculta	0 para desactivar, o cualquier número (bajo). El valor predeterminado es 3 [†]
cgi_uplink_urgentdelay [†]	Plazo máximo para datos urgentes.	entero oculto	El retardo máximo si los datos urgentes está en la cola (por ejemplo pequeño

			cuerpo que pertenece a una corriente que no ha enviado datos por un tiempo --- interactividad -.) por defecto es 20msocultos.
connect_on_startup	Fuego de la conexión cuando el cliente se pone en marcha	booleano opcional	"true" o "false"(por
connect_timeout	tiempo de espera de conexión general(defecto), en milisegundos	enteros	predeterminados a 10.000 ms.
debuglevel	Turnde depuración en la consola de Java (no el panel de mensajes!)	entero escondido	Cuanto menor sea, más detallado. predeterminado es "999". Probablemente no hace mucho más en estos días.
dns_domain	dominio para utilizar en DNS mode	string opcional	Usted no debe configurar manualmente esta opción, utilice el panel de configuración en su lugar.
dns_max_tx_interval	retraso máximo entre el envío de dos consultas en el modo de DNS, en milisegundos	entero opcional	por defecto 1000 ms.
dns_min_tx_interval	retardo mínimo entre el envío de dos consultas en el modo de DNS, en milisegundos	número entero opcional:.	predeterminado 1/500 de dns_max_tx_interval
dns_no_direct_connection	Evite directamente enviar consultas al servidor YF en modo DNS, forzar el uso de una configuración del servidor de nombres	booleano opcional	"true" o "false" (por defecto)
dns_rep_interval	RepitaUNREPLIED consultas en modo absoluto después esto muchos milisegundos	entero opcional	5 veces dns_max_tx_interval
dns_tx_adaption_factor	velocidad Adaptación en el modo de DNS	flotar opcional	entre 1,1 y 5,0, por defecto 1.5. Los valores más altos son más agresivos.

dont_show_popups	Evite a aparecer ventanas de notificación en la pantalla	booleano opcional	"true" o "false" (por defecto).
echo_max_tx_interval	máximaintervalo entre dos peticiones de eco ICMP en modoECHO	entero opcional	1.000 msdefecto
echo_min_tx_interval	Intervalo mínimoentre dos peticiones de eco ICMP en el modo ECHO	entero opcional de	predeterminado1/200, de echo_max_tx_interval
echo_tx_adaption_factor	velocidad de adaptación en el modo ECHO	flotar opcional	entre 1,1 y 5,0, por defecto 1.5. Los valores más altos son más agresivos
echo_max_payload_size	Tamaño máximo de carga útil en el modo ECHO	entero opcional	predeterminado1464 (el valor máximo)
cifrado	Activar cifrado de conexión	booleano opcional	"true" o "false" (por defecto). Tenga en cuenta que el asistente se convierte esto en el usted. Sólo debe activar el cifrado de la depuración!
file_extip	Escribir IP externa del servidor a un archivo cuando se conecte	cadena opcional	Esto le permite utilizar IP externa del servidor en scripts
flatten_bursts	Reduzca la velocidad de transmisión de tramas en los períodos ráfagas de obtener un patrón de tráfico más suave	booleano opcional	"true" o "false" (por defecto). Establecer si nota conexión cuelga en ráfagas.
follow_server_recommendations	permitir que el cliente siga las recomendaciones del servidor para utilizar otro servidor	booleano opcional	"true" o "false" (por defecto). DEPRECATED.
fool_pix	Prueba un truco que puede engañar a versiones antiguas PixOS a pasarWebSense	booleano oculto	"true" o "false" (por defecto) Sólo encenderá si usted sabe que su relación está pasando por un antiguo servidor de seguridad PIX usando WebSense y no se puede conectar,. puede funcionar con este juego en "true".
found_servers	Base64 registros codificados de los servidores que se encuentran en la última	devarios base64	No se metan con ella a menos que sepa lo que

	búsqueda servidores	opcional	está haciendo.
ftp_mode	datos de conexión de configuración estilo para usar en el modo FTP.	string opcional	"ambos" (por defecto), "normal" o "pasiva". "normal" hará que el servidor YF para iniciar la conexión de datos (esto es lo que hace normalmente FTP) ", tanto" utilizará lo que funcione
ftpproxy	Utilice un no- Proxy FTP transparente con laprotocolo de conexión FTP	cadena de opcional	Dejar el nombre de host del proxy FTP o la dirección IP. Suprimir cuando no se necesita una(<i>muy probable</i>).
ftpproxyport	usar un proxy FTP no transparente con la conexión FTP protocolo	entero opcional	Ponga en el puerto de control del proxy FTP (normalmente 21). Suprimir cuando no es necesario un proxy FTP(<i>muy probable</i>) ..
cabecera	cabeceras adicionales al enviar peticiones al proxy web	múltiples string opcionales	Si necesita encabezados adicionales o desea anular cosas como "User-Agent", hazlo aquí, por ejemplo: "encabezados User-Agent: NoneOfYourBusiness 1.0"
hide_tray_icon	En Windows, no muestran un icono de la bandeja	booleano opcional	"true" o "false" (por defecto)
http_flush	Cerrar y volver a abrir la conexión HTTP enlace ascendente a intervalos	enteros opcional	Tiempo en milisegundos. Si usted necesita esto, utilice el protocolo de conexión CGI en su lugar. Esto no está actualizado.
http_postfix	En el modo HTTP, añada esto después de un? de laURL	cadena oculta	se puede utilizar para elaborar especial URL
https_ssl	de conexión Wrapen "modo HTTPS" en SSL (TLS).	booleano opcional	ayuda con los filtros exigentes que llevan a cabo el protocolo de detección
idle_kill	conexión muertas cuando está inactivo para esta cantidad de	entero	Esta es obsoleto y no funciona como se

	milisegundos	opcional	esperaba más, don ' t lo utilizan.
initial_post_size	Al hacer un POST HTTP, utilice este tamaño inicial	entero oculta	por defecto es 10000000 o 10 Megabytes. El cliente disminuye este por un factor 0,8 hasta que el proxy web lo acepta o no se alcanza minimum_post_size. Si sabe de su representante límites ponen aquí, se ahorra el tiempo de conexión.
keepalive_interval	Enviar un marco keepalive toda esta cantidad de milisegundos	entero opcional	predeterminadoes 20000 ms. detección de fallos de conexión es de 2,5 veces.
level_messages	Mostrar sólo los mensajes por encima de este nivel en los mensajes del panel	entero opcional	0 es "debug ", 7 es de " emergencia ". predeterminado es 1 " informativo ".
locale	Sus preferidos " lenguaje (2 letras ISO, minúsculas, opcionalmente seguido de un guión bajo y un código de 2 letras ISO del país en mayúsculas)locale	de cadena opcionales	predeterminadosa"en . "Sólo unos pocos son los idiomas disponibles, consulte el cuadro de diálogo Configuración.
location_x	Coordenadas de la ventana de su libertad en la pantalla de	entero opcional	0 es la esquina superior izquierda, los valores más altos son másderecho
location_y	Coordenadas de la ventana de su libertad en lapantalla	entera opcional	0 es la esquina superior izquierda, los valores más altos están más abajo en
minimum_post_size	mínimo HTTP POST tamaño	entero oculta	por defecto es 20000 o 20Kilobytes. Sólo bajo si usted sabe que su poder se niegan puestos de arriba 20kand que realmente tenga que hacerlo.
min_buffersize	tamaño de búfer mínimo para los flujos.	entero opcional	El valor predeterminado es 1500. Trate de aumentar esto si usted quiere lograr anchos de banda de

			transmisión individuales de más de varios megabits por segundo. máxima es de 8192.
openvpn	OpenVPN puerto	entero que opcional	por defecto es 1194, sólo cambiará si usted necesita este puerto para otra cosa.
openvpn_exclude	IPs y las redes que se excluirán de enrutamiento a través del túnel OpenVPN	múltiple cadena opcional	para cada IP o de red (dirección IP, un espacio opcional y máscara de red), que no debe ser encaminado a través del túnel OpenVPN, añada una línea alconfig.
openvpn_nat_interface	listado de interfaces que desee modificar el trazado de la conexión OpenVPN usando Network Address Translation	múltiples cadenas opcionales	Útil sólo en Windows. Le permite conectar tu Play Station o Xbox o de otros equipos para una segunda interfaz LAN y utiliza la conexión OpenVPN YF.
openvpn_option	OpenVPN adicionales opciones	múltiples cadenas ocultas	Pass estas opciones adicionales como si fueran líneas en el archivo de configuración de OpenVPN.
openvpn_path	Configurar la ruta completa del OpenVPN ejecutable	string opcional de	uso esto si el ejecutable OpenVPN no está en el ejecutable camino
openvpn_tap_sleep	Set opción "tap-sleep" en OpenVPN a este valor	entero opcional	predeterminados de 2 segundos. relevante sólo en Windows.
openvpn_route_delay	Set opción "route-delay" en OpenVPN a este valor	entero oculto	defecto de 2 segundos (segundo parámetro es siempre 30). relevante sólo en Windows.
openvpn_route_method	Configurar OpenVPN ruta método de	cadena oculta	por defecto es "exe". Consulte la

			documentación de OpenVPN para más opciones. relevante sólo en Windows.
openvpn_ip_method	Configurar OpenVPN "ip-win32" método de	cadena oculta	por defecto es "dinámico". Consulte la documentación de OpenVPN para más opciones. relevante sólo en Windows .
openvpn_tmp	directorio temporal que se utilizará para los archivos de configuración de OpenVPN y certificados de	cadena oculta	por defecto es la carpeta "home", o un subdirectorio debajo. Configurar una ruta absoluta aquí.
openvpn_udp	Haga túnel OpenVPN a través de UDP en lugar de reenviar reenvío TCP en YF	booleano opcional	UDP uso en lugar de reenvío TCP para la conexión del túnel OpenVPN si "true".
contraseña	su sude contraseña La libertad	cadena requiere	la contraseña de su libertad, o una forma ofuscada de ella
portaccept	Reenvía un puerto del servidor a un local de puertos	múltiples serie opcional	puerto de servidor acogida local locales de puerto
portforward	Delantero un puerto local a una distancia puertos	de varios serie opcional	local, puerto remoto host remoto puerto
post_avg_uplink_dur	post Vista duración media de enlace ascendente, en milisegundos	entero opcional	En el modo POST, cuánto tiempo should una transferencia de enlace ascendente toma en promedio (en milisegundos) ¿influye en la longitud máxima POST. defecto es 500 ms.
post_err_holdoff	POSTE modo de tiempo de retención de error, en milisegundos	entero opcional	En el modo POST, esperar esta cantidad de milisegundos en una condición de error antes de volver a intentarlo.

post_max_connectio ns	número máximo de conexiones simultáneas en modo POST.	entero opcional	Algunas personas podrían tener que reducir esto a uno. Es seguro utilizar los números más grandes, pero en algún momento se incrementará por encima. Incumplimiento (2) es bueno para la mayoría de la gente.
post_min_holdoff	Tiempo de espera antes de nueva conexión se realiza. (milisegundos	enteros opcionale s	..)predeterminadosa 5000
post_min_post_size	tamaño mínimo de una petición POST	entero opcional	Nunca bajar el tamaño máximo de la POST debajo de este límite Podría morir de hambre el camino ascendente (por defecto:.. 3000)
post_min_queue	mimum tamaño de la cola para la transmisión rápida en modo POST.	entero opcional	Número de tramas en cola que desencadenan una nueva conexión después de un tiempo mínimo de sólo holdoff (por defecto: 3)
post_typ_holdoff	tiempo de retención típico en modo POST, en milisegundos	enteroque opcional	esperar tanto tiempo para más cuadros antes de activar una conexión (por defecto: 500 ms)
de protocolo	El protocolo de conexión para utilizar	string requiere	Uno de: "http", "https", "aislado", "mensaje", "ftp", "udp", "dns", "eco"
de proxy	El proxy puerto	entero opcional	Haga que su PC de un proxy web, proporcionando el número de puerto. Se establece en 0 o quitar para apagarla. defecto es 8080.
proxyauth	Fuerza un método de	string	Unade "ninguna

	autenticación en particular en proxy web.	opción	ninguna ore" (por defecto), "básico o ninguno ", " NTLM o ninguno ", " Resumen o nada ". Por defecto se usa lo que se ofrece por el proxy y prefieren métodos más seguros frente a los métodos menos seguros.
proxydomain	su dominio para la autenticación de proxy web, si es necesario (sólo proxies NTLM)	string opcional	Un nombre de dominio de Windows, si lo necesita para autenticar en el servidor proxy web.
ProxyHost	El proxy web host o dirección IP a través del cual hacer un túnel cuando se utiliza "http", "https" o"cgi".	cadena opcional	un nombre de host o dirección IP. Dejar en blanco o eliminar si no necesita utilizar un proxy.
ProxyPass	su contraseña para autenticarse en lade proxy web	cadena opcional de	una contraseña, si se requiere autenticación.
proxyport	puerto del proxy web.	entero opcional	un número de puerto. Set to0 o eliminar si usted no necesita utilizar un proxy web.
ProxyType	Utilice el tipo de representación no estándar para los modos de conexión basadas en TCP (HTTPS, HTTP POST, CGI)	cadena opcional	Al usar modos de conexión basadas en TCP y un "proxy web" está configurado, asuma que es de este tipo. Puede ser "HTTP / HTTPS" (por defecto), "SOCKSv4" o "SOCKSv5".
proxyuser	Tu nombre de usuario para autenticarse en lade proxy web	cadena opcional	un nombre de usuario, si se necesita autenticación.
rcport	"control remoto"puerto	entero escondido	utilizar un puerto TCP particular para singularización (es decir, asegurarse de que la fiebre amarilla se ejecuta una sola vez). El valor predeterminado es 62799, obligado a

			127.253.19.87.
reconnect_after_shut down	Si el servidor se apaga, intente volver a conectar automáticamente después de un tiempo	booleano opcional	"true" (por defecto) o"false"
reconnect_delay	Si una reconexión es necesario, esperar esta cantidad de milisegundos antes de un intento	entero opcional	por defecto es 5000 milisegundos.
redirect_dns	no resuelven los nombres de host local al usar SOCKS	booleano opcional)	"true" o "false" (por defecto . Use esto si su servidor de nombres local no puede resolver nombres de Internet (o si no <i>quieres</i> que)
rekey	clave de cifrado Cambiar frecuencia	booleano opcional	"true" o "false" (por defecto). El asistente ajústelo a "true", y hay normalmente ninguna razón por la que usted quiere ponerlo en "false" a menos que sospeche que hay un error en el código clave de negociación y se pierde la conexión. Recomendamos que establezca este valor a "true".
relay	Permitir que otros compartir su YF sesión	booleano opcional	Seta "true" o "false" (o quitar). Tenga en cuenta que esto sólo funciona si su perfil lo permite también.
rtt_interval	Medida tiempo de ida y vuelta cada esta cantidad de milisegundos	entero opcional	0 para desactivar (es decir, sólo miden una vez después de 10 segundos)
server_connection_pr otocol	Set preferencia protocolo de túnel (influye en la resolución de nombres DNS sólo)	entero opcional	0: lo que funciona 4: IPv4 sólo 6: IPv6 sólo 46: prefiera IPv4 64: prefiera IPv6
server_criterion	Definir criterios por los que se puede seleccionar automáticamente los servidores	múltiple cadena opcional	de nombre del criterio número entre 0 (negado) y 10 (requerido), por defecto

			es 5 (no me importa)
sipforward	Espejoun gatewayremota SIP	múltiples string opcionales	puerto local SIP gatewayaddr SIP gatewaypuerto de
sip_fixup_audiostream	Fix dirección en el destino IP flujo UDP para SIP audio	booleano opcional	Pruebe esto si los flujos de audio SIP son sólo unidireccionales
medias	Los CALCETINES puerto	entero opcional	Haga que su PC un proxy SOCKS suministrando el número de puerto. Eliminar o el valor 0 para girar calcetines.
sslproto	Si se configura https_ssl, definir SSL / TLS versión del protocolo de usar	cadena opcional	"any" (por defecto), "SSLv2" o "TLSv1"
start_minimized	Inicio en la bandeja del sistema (sólo Windows)	solo opcional	"true" o "false" (por defecto)
stopafter_found	Durante la búsqueda de servidores , deja de búsqueda después de haber encontrado esta cantidad de servidores.	entero opcional	0 probar hasta que se conozcan formas hay más potenciales
stopafter_tried	Durante la búsqueda de servidores, detenga después de haber hecho esto muchas tentativas.	entero opcional	0 a tratar hasta que no se conocen maneras más potencial
tunnelhost	El servidor de su libertad de usar	cadena requiere	un nombre de host, una dirección IP, las direcciones IP múltiples separados por coma, o una URL relay CGI. En el modo de DNS, servidores DNS (separados por comas) se puede añadir con punto y coma para un nombre de host (no es una IP). En el modo HTTP / POST, puede contener un nombre de host y un URI.
tunnelport	El Your Freedom puerto del servidor	entero requiere	un número de puerto
ajustes	Utilice esta "ajustar ajuste"	cadena opcional	Nombre de ajuste pellizcar (utilice la

			ventana de configuración, no se ajusta manualmente), o sacar ninguna
udp_newsrcportevery	Utilice un nuevo puerto UDP de origen (el modo UDP / DNS) todos los paquetes de este número	entero opcional	Valor puede ser tan bajo como 1, pero esto va a afectar al rendimiento. Utilice con cuidado. defecto es 0 (no change)
udp_newsrcporttime	Use a new UDP source port (UDP/DNS mode) every this many milliseconds	integer optional	Port changes if this many milliseconds have passed since the last change. Default is 0 (don't change based on time)
udp_srcport	Use a particular UDP source port (UDP/DNS mode)	integer optional	0 or remove to use an ephemeral port
use_http11	Use HTTP/1.1 instead of HTTP/1.0 in requests	boolean optional	If your proxy is acting stupid, try if this fixes the problem. Can either be "true" or "false" (default)
useragent	Send this "user agent" header in requests	string optional	Used to fake a particular browser.
Your YF username	stringrequired	Your Your Freedom username	
vm_code	Voucher code information	multiple string optional	Information about known voucher codes
vpn	Use new-style VPN mode	boolean hidden	Experimental, not yet effective
webproxy	Port for new-style web proxy implementation	integer hidden	Experimental: use new-style web proxy implementation for your applications