Your Freedom

Guía del Usuario

Una introducción gradual y Guía de Referencia para Your Freedom

http://www.your-freedom.net/

Version 2.1

Release Date: 2011-01-17

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, http://www.your-freedom.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.

1 Introducción

1.1 ¿Qué es Your Freedom?

Your Freedom es una aplicación que te permite navegar libremente cuando tu acceso a Internet esta siendo restringido. Aun cuando las técnicas que usa para burlar estas restricciones son harto 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.

Su funcionamiento 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. Your Freedom trata todo el tráfico a través de un **túnel** que pasa de largo firewalls, proxis Web 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.

1.2 Qué no es

Your Freedom **no es una red privada virtual (VPN)**. No brinda ninguna conexión a red privada alguna, solo a Internet.

Your Freedom tampoco es una **solución integral 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 debamos 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.

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.

1.3 ¿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[1]. La mayoría de los clientes P2P trabajan bien con YF, y podemos incluso conseguir un puerto servidor, que nos dará un "id alto".

- **Listas negras**
  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 desde 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).

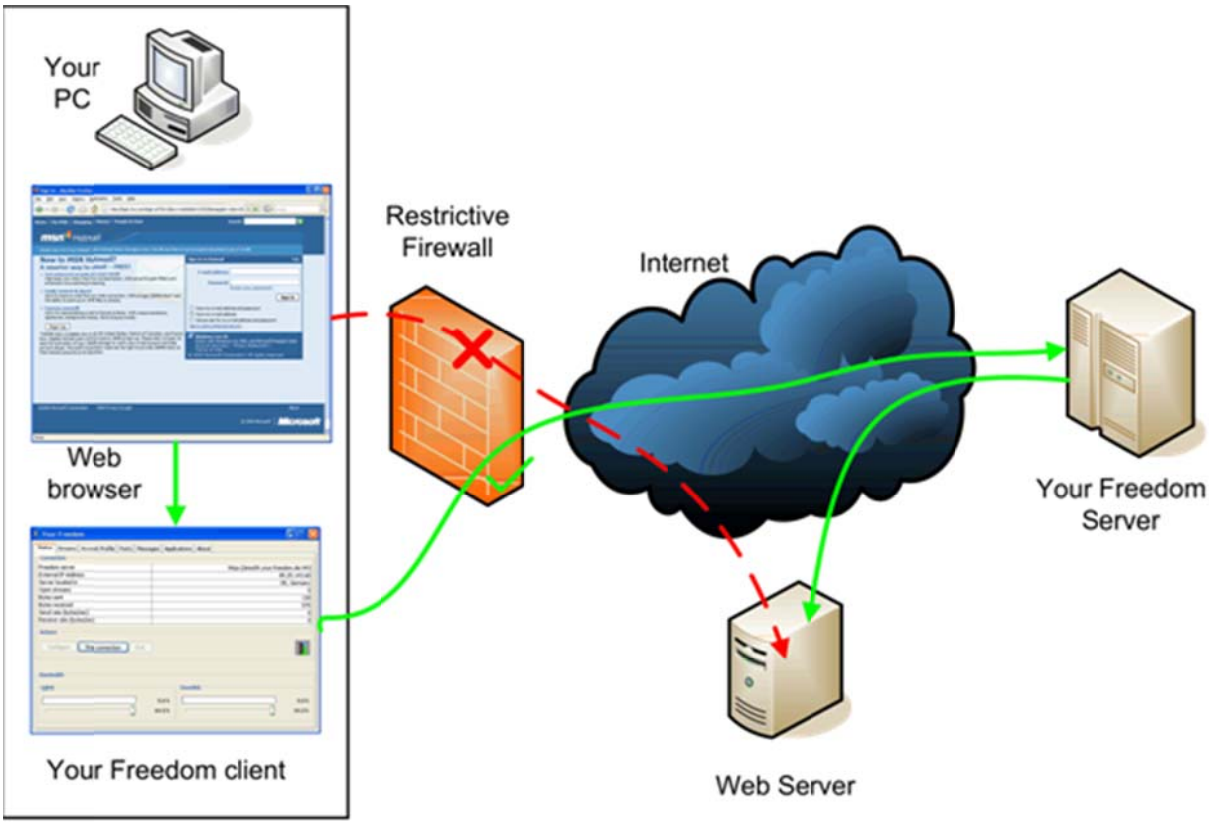
1.4 ¿Cómo funciona?

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.

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. En la mayoría de los casos todo lo que necesitamos es poner la dirección de un Proxy Web o FTP (y posiblemente las credenciales de autenticación); en este punto el cliente tratará de conectarse.

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 configurarmos 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 hotmail.com. Las respuestas desde el servidor Hotmail tomarán el mismo camino pero en sentido inverso.

[1]El protocolo por supuesto, no es ilegal, por ende no tiene sentido bloquearlo. Las acciones de los usuarios pueden ser ilegales sin embargo.– Your-Freedom no se responsabiliza por las acciones de los usuarios.



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

1.5 ¿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 via. 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 de cifrados comparables a los de una WIFI WEP-128. No podemos usar cifrados más robustos en un servicio de la escala de Your Freedom; de hacerlo las CPUs sufrirían de sobrecarga. Sin embargo habilitar cifrado y re-

keying garantiza un nivel que solo agencias especializadas podrían tener la determinación de romper.

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[2].Nuestro antivirus deberá encargarse de esta tarea.

1.6 ¿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).

Se ofrecen paquetes de actualización que reducen 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. Los paquetes están disponibles como actualizaciones por un mes, tres meses, seis meses o doce meses, y vienen en tres diferentes niveles: BasicFreedom, EnhancedFreedom, y TotalFreedom. Como alternativa a los paquetes completos existen los vouchers. Los vouchers pueden ser usados para mejorar temporalmente las prestaciones del perfil de Your Freedom con un paquete sin tener que pagar por un mes completo y malgastar partes de éste. Para mas detalles ver capítulo 4.2.1.

1.7 ¿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 un paquete). 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, los servidores no guardan registro alguno que no sea de interés exclusivo de los desarrolladores y todos los registros con información de nuestros clientes están guardados a salvo en un servidor en Alemania. No obstante nosotros cooperaríamos con las autoridades 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 asi como la IP desde donde te conectas si asi lo requiriesen las autoridades.

Nosotros no registramos lo que nuestros clientes acceden en internet. Las regulaciones alemanas ni siquiera permiten esto. Si registramos el hecho de que se haya accedido a nuestro servicio desde tu dirección, 16 bits más bajos de la dirección IP 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

[2]Esto no es completamente cierto. El correo saliente que es enviado por YF es analizado. Hacemos esto para evitar que nuestros servidores aparezcan en lista negra, lo que impediría a nuestros usuarios enviar correos en un futuro. Esto no es para proteger al usuario, es para proteger a otros y a YF de el uso indebido.

combatir violaciones de los términos de uso, y en los casos en que las autoridades lo requieran.

Además, 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.

1.8 ¿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 31 distribuidos en 9 paises. Todos brindan el servicio de una navegación básica y chateo, solo algunos rechazarán conexiones P2P (específicamente, los que están localizados en Norteamérica). Algunos pueden manejar más tráfico que otros. Hay una página de estadísticas disponibles en http:///www.your-freedom.net/142/. 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 “default”. 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.

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. 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

2 Primeros pasos

2.1 ¿Cómo suscribirse?

Lo primero que tenemos que hacer para usar el servicio es suscribirnos al mismo en el sitio Web: http://www.your-freedom.net/. Debemos crearnos 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.

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”.

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.

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 cuenta solo 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.

2.2 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 (en realidad no se necesita estar registrado para poder descargar el cliente). 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) [3] 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.
- **Instalador completo para windows**
  Ésta versión viene empaquetada con su propio JRE, por tanto no tiene prerrequisitos. 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 versions 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.

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. Instrucciones adicionales para Mac OSX 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 10.5 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.

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

[3] Es requerido que tengamos una versión Java Runtime Environment compatible con Java 1.6 or superior. En caso de duda visitese http://java.oracle.com/, démos clic en “Java SE” en la seción “Descargas”, y descárgese e instálese “JRE” o “JDK”. Oracle da estas descargas gratis pero siempre ha de revisarse los términos de la licencia.

2.2.1 Usuarios de países que censuran Internet

YF está en colaboración con Sesawe, una ONG dedicada a educar y colaborar con personas de todos los países para burlar la censura de internet.

Se ha creado en your-freedom la cuenta “sesawe” (password “sesawe”) con características especiales y la pusimos a disposición exclusiva de aquellas personas que viven en aquellos países que sesawe considera aplican restricciones a internet con mayor rigor.

Existe una versión SESAWE del cliente YF en forma de Windows Installer, Windows Full Installer o aplicación Mac OSX. Puede ser descargada lo mismo de www.your-freedom.net/sesawe/ o por correo enviando un correo en blanco a get@your-freedom.net con asunto "sesawe".

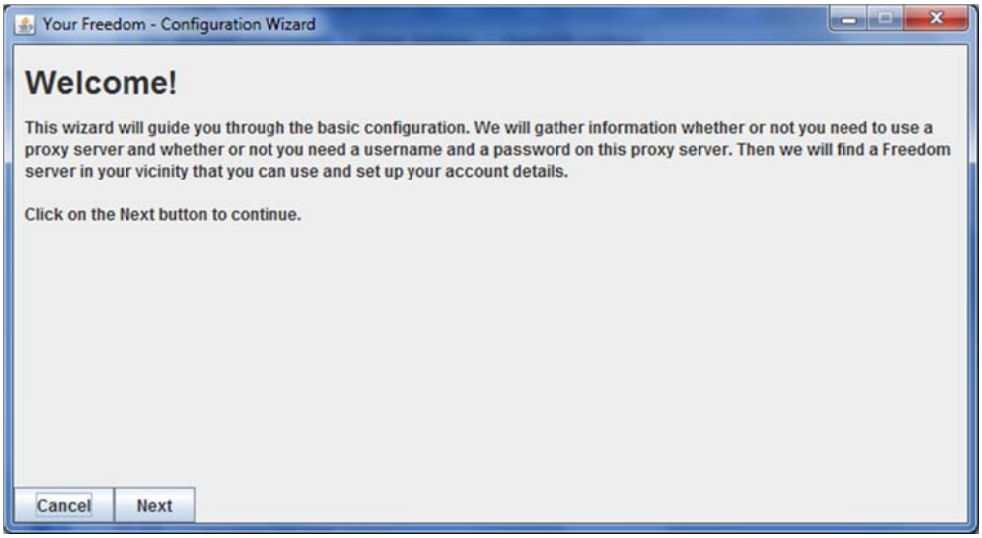
Tanto cuenta “sesawe” como la preconfiguración Sesawe del cliente YF solo funcionarán desde aquellos países auspiciados por el proyecto Sesawe. Si ésta cuenta se usa desde otro país el cliente YF emitirá el mensaje “AUTHENTICATION NOT VALID FOR YOUR COUNTRY OF RESIDENCE”

2.3 Accediendo por vez primera

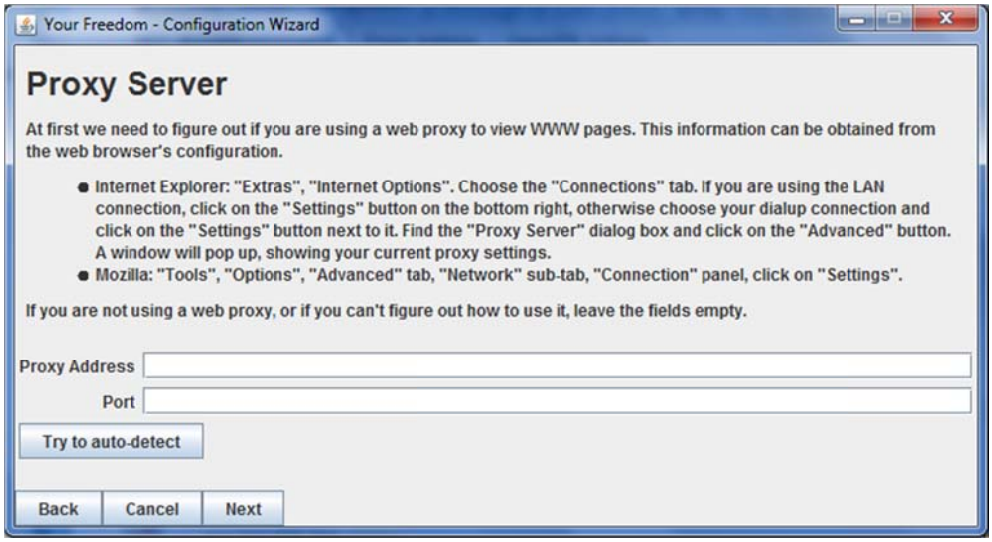
Cuando se inicia el cliente YF por vez primera, éste preguntará por el idioma por defecto. El idioma que escojamos será el de la interfaz de usuario. Ésta configuración se puede restablecer mas tarde.

Después que 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 mas detalles.

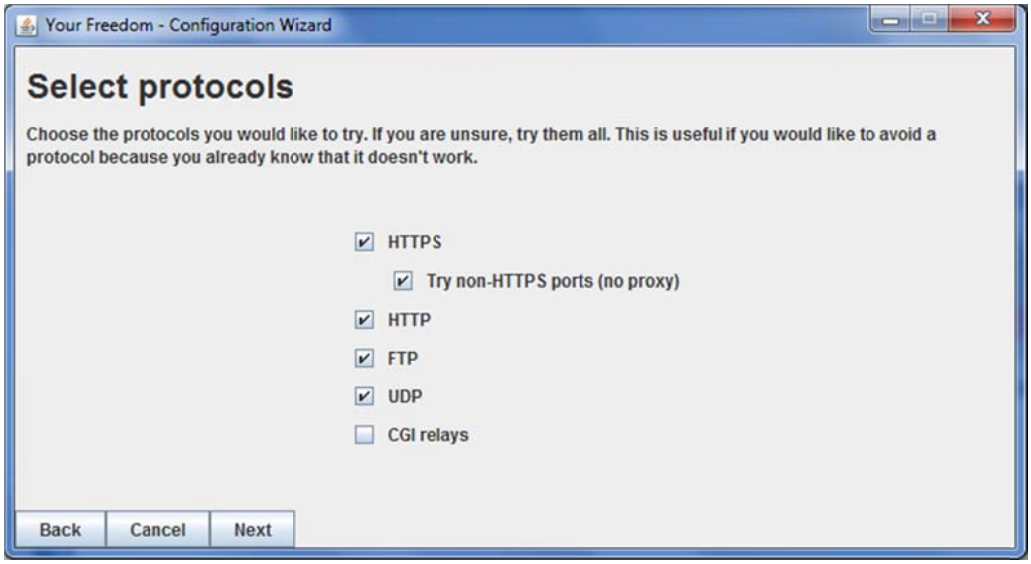
Cuando se abra el asistente veremos una pantalla de bienvenida:



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

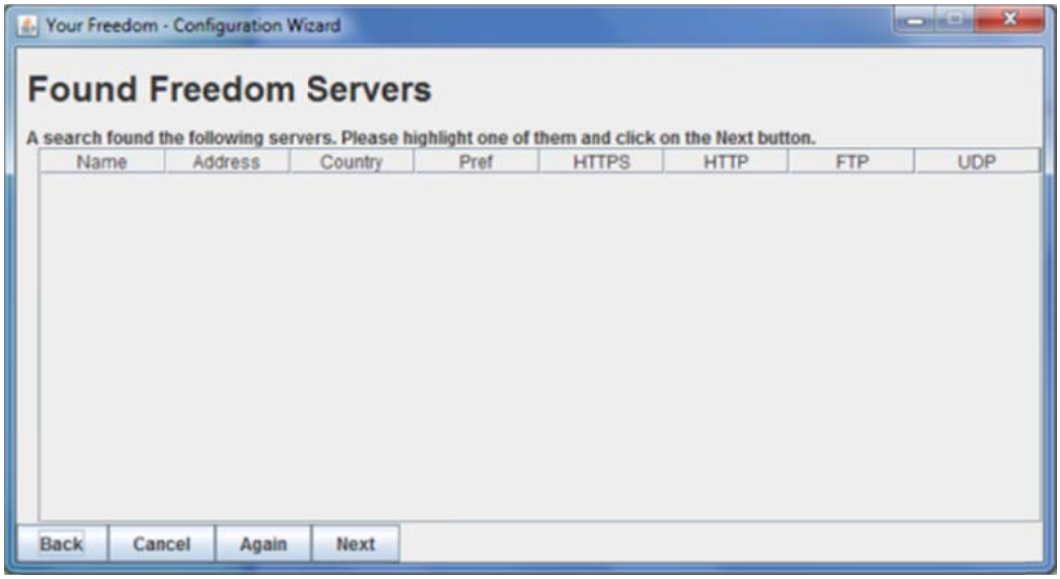


Si la conexión es a través de un proxy, éntrense los detalles aquí. Si no estamos seguros démos clic en “Siguiente” por ahora.



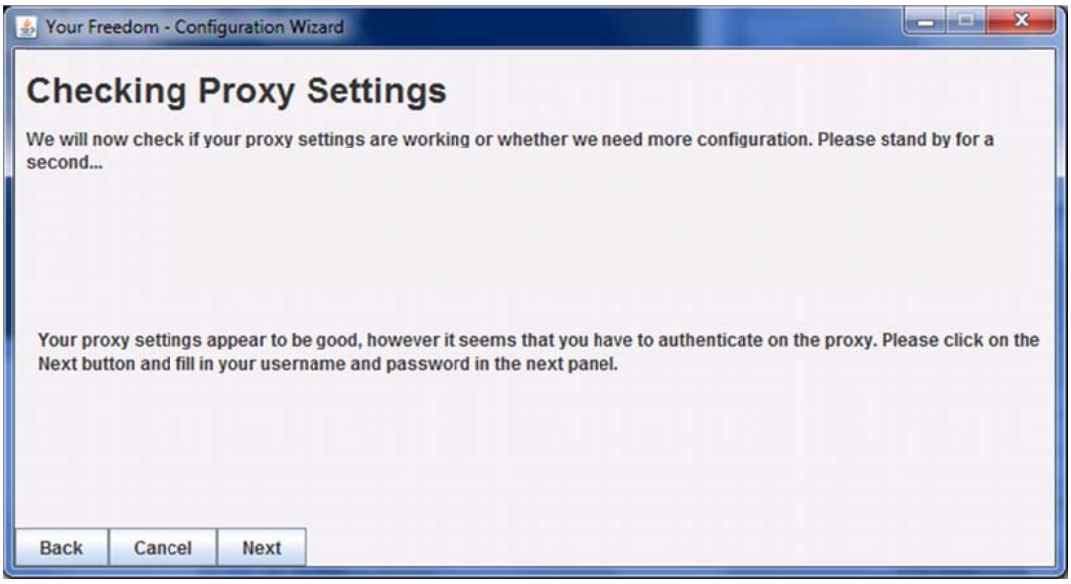
Encontraremos una ventana pidiéndonos que seleccionemos los protocolos a usar para efectuar la conexión a los servidores YF. Los protocolos seleccionados afectarán el modo en que el asistente chequeará la conexión con los servidores. Si no estamos seguros dejémos la selección por defecto y démos clic en “Siguiente”:

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

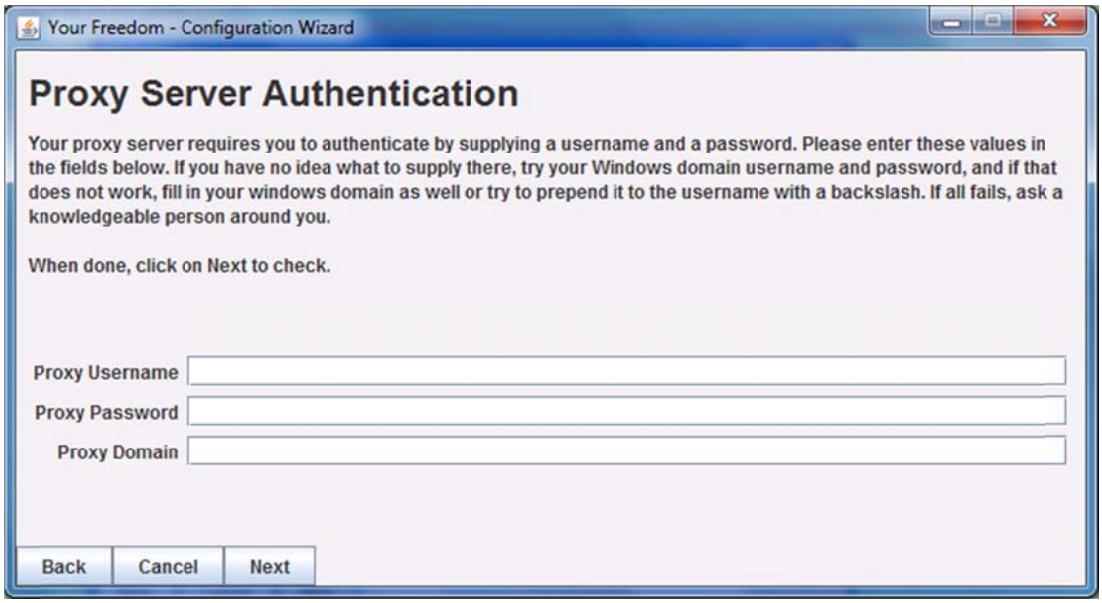


tendremos que averiguar cuál es la configuración del proxy web (o quizás configurar todo manualmente, como en el caso que quisiseramos usar un proxy FTP).

Si en cambio obtenemos esto,

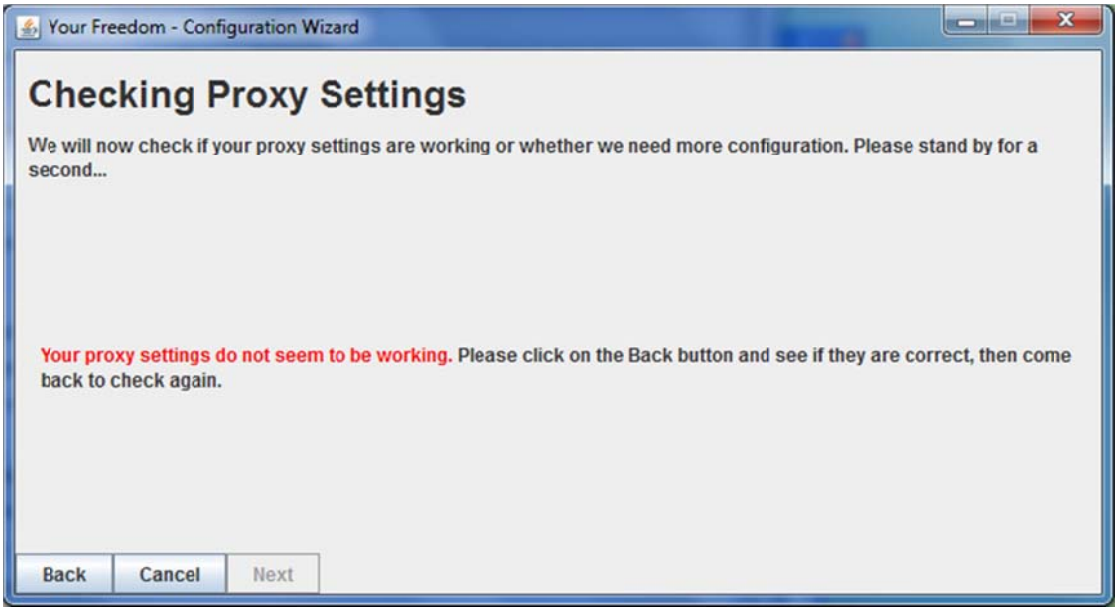


Entonces los detalles del proxy son correctos pero necesitamos las credenciales para autenticarnos. Démos clic en “Siguiente”…



E introduzcamos 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.

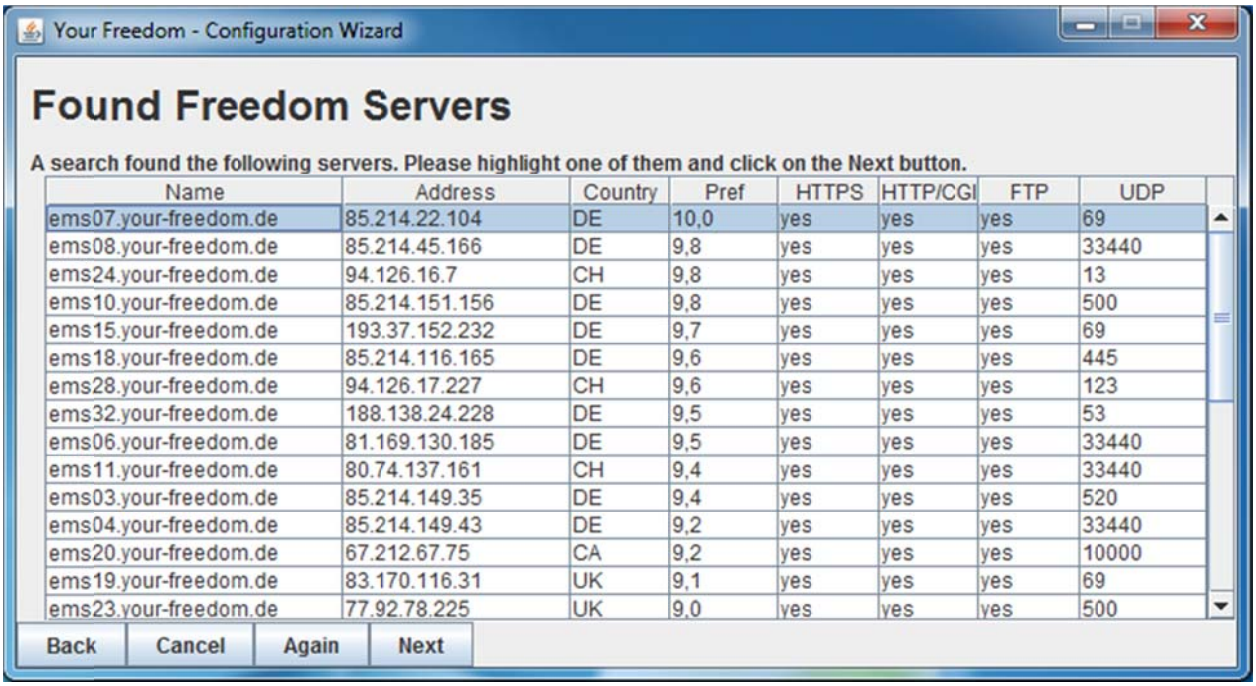
Si nos encontramos con esta página:



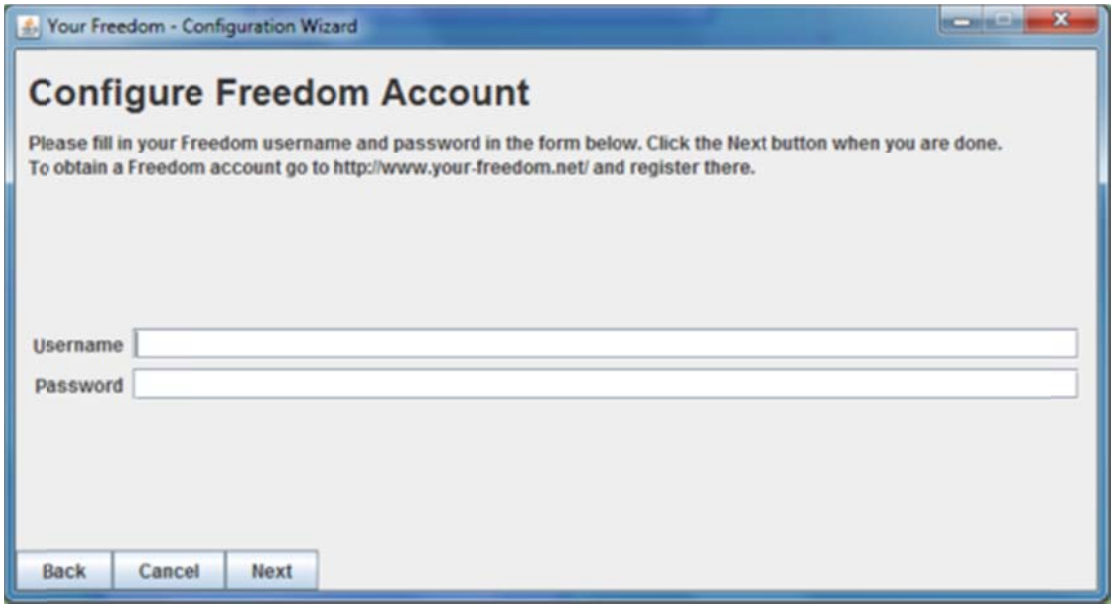
es que no hemos introducido correctamente las configuraciones de proxy. Demos clic en “Atrás” y modifiquemos el hostname/dirección IP y/o el puerto. Muchos proxis utilizan los puertos 80, 3128 u 8080. Se puede tomar como referencia la configuración de nuestro navegador.

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:

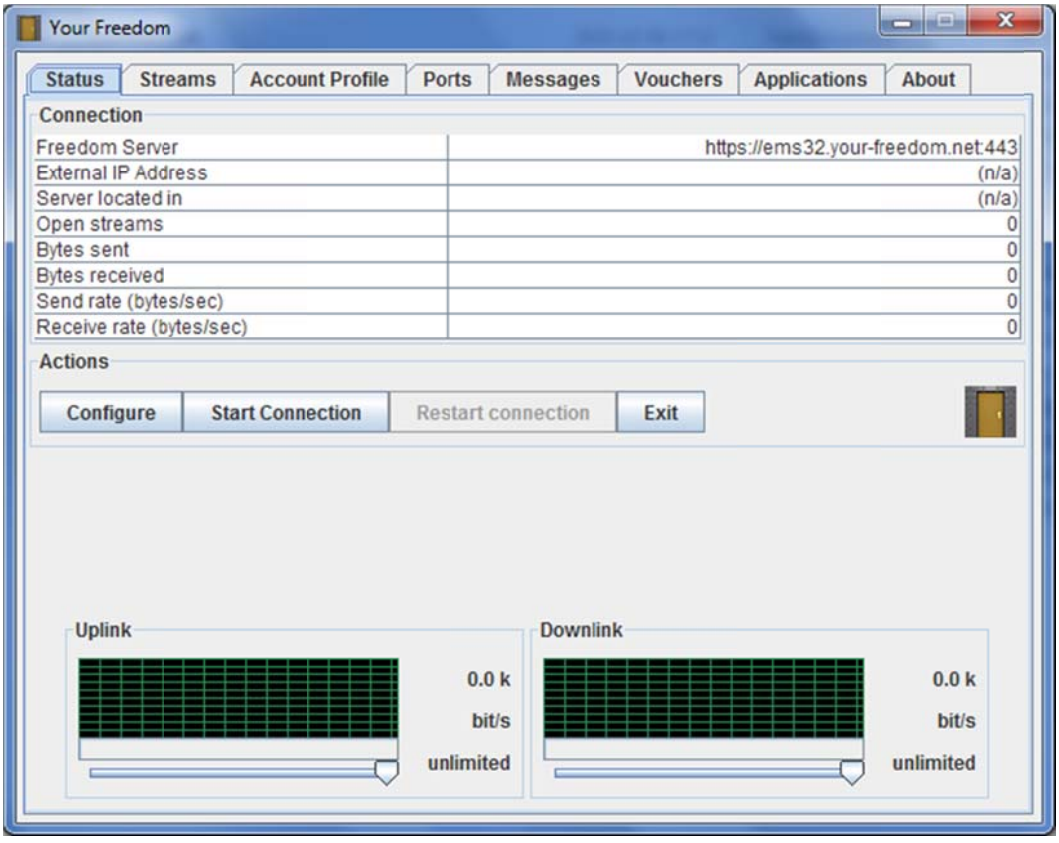


Es importante que veamos algún “Si” en algunas de las columnas HTTP, HTTPS FTP o UDP. Un “Si” significa que el cliente ha sido capaz de usar este protocolo para conectarnos al servidor usando los puertos por defecto. Un número significa que fue capaz de conectarse pero utilizando un puerto diferente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



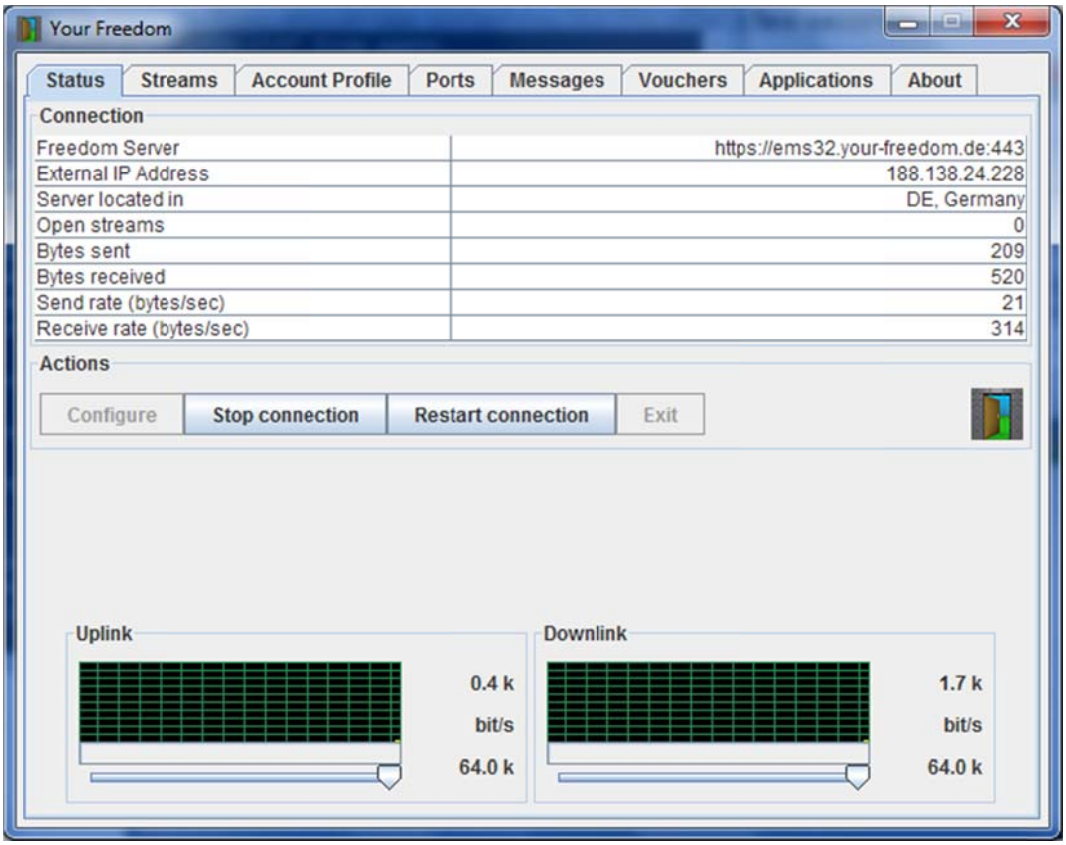
En esta página introduciremos nuestras credenciales para conectarnos a Your Freedom. Démos clic en “Proximo”.

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

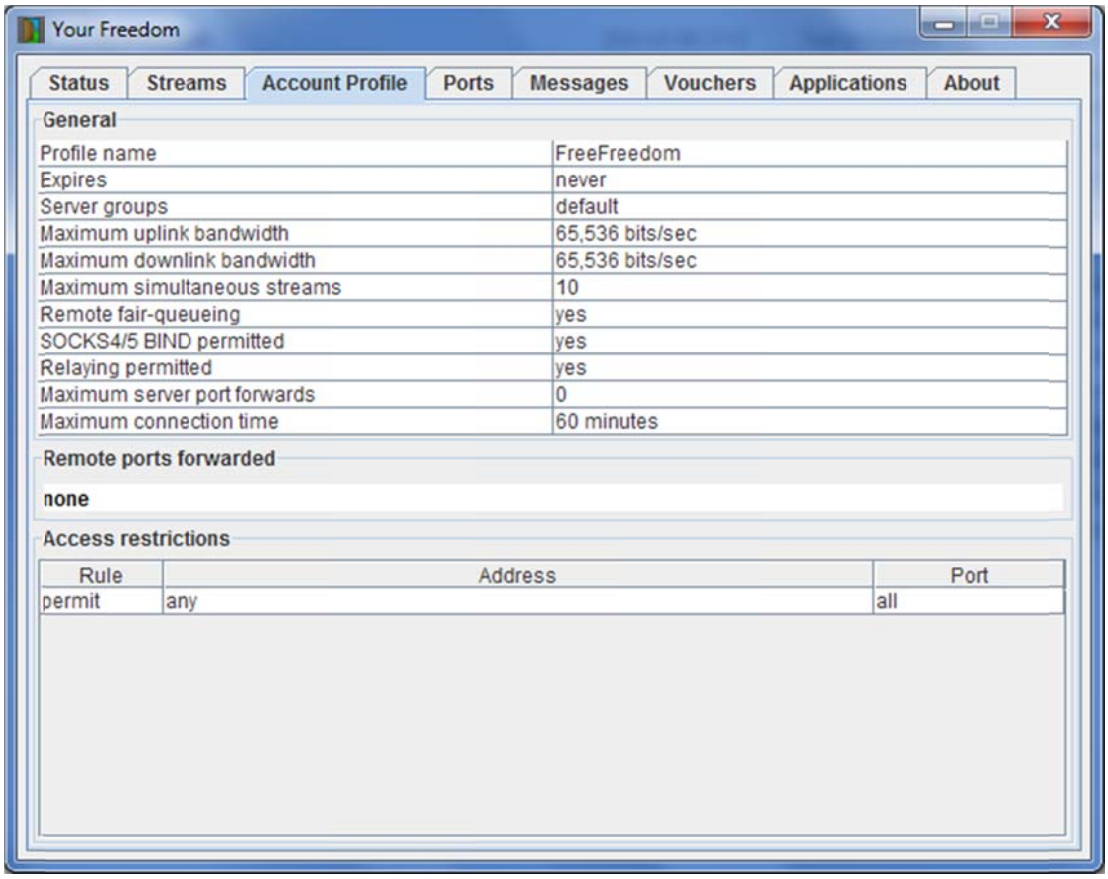


Es de señalar que el cliente no conoce ningún dato sobre el servidor ni sobre el perfil del usuario Your Freedom antes de conectarse al servidor, por eso es que algunos de los valores están en cero o simplemente vacíos: (incluyendo en ancho de banda- éste no es ilimitado a menos que hayamos comprado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

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



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 démos 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[4].

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 capítulo 2.5 página 27).

Bien, es tiempo de configurar nuestras aplicaciones. Haremos referencia al capítulo 2.4 página 20 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.

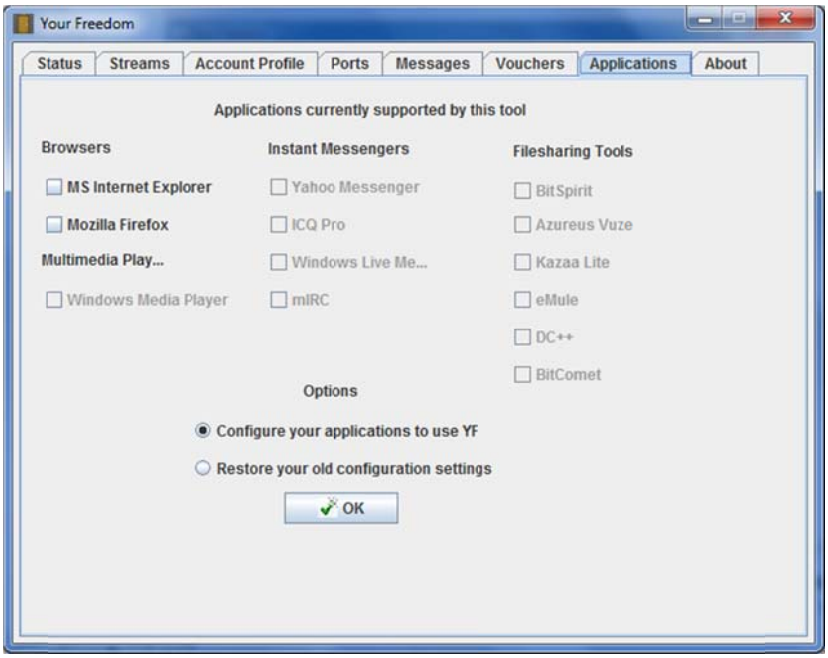
[4]Hay un grupo de restricciones de hecho, pero no se echan a ver. Solo están ahí para proteger los servidores del abuso, no estorban.

2.4 Configurar aplicaciones

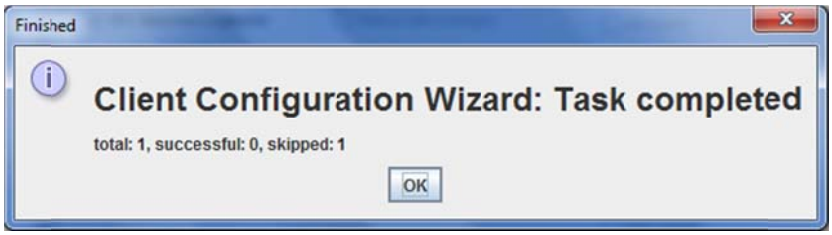
2.4.1 Automáticamente

Nosotros recomendamos la configuración manual. Ésta característica está aquí solo para facilitar la tarea.

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

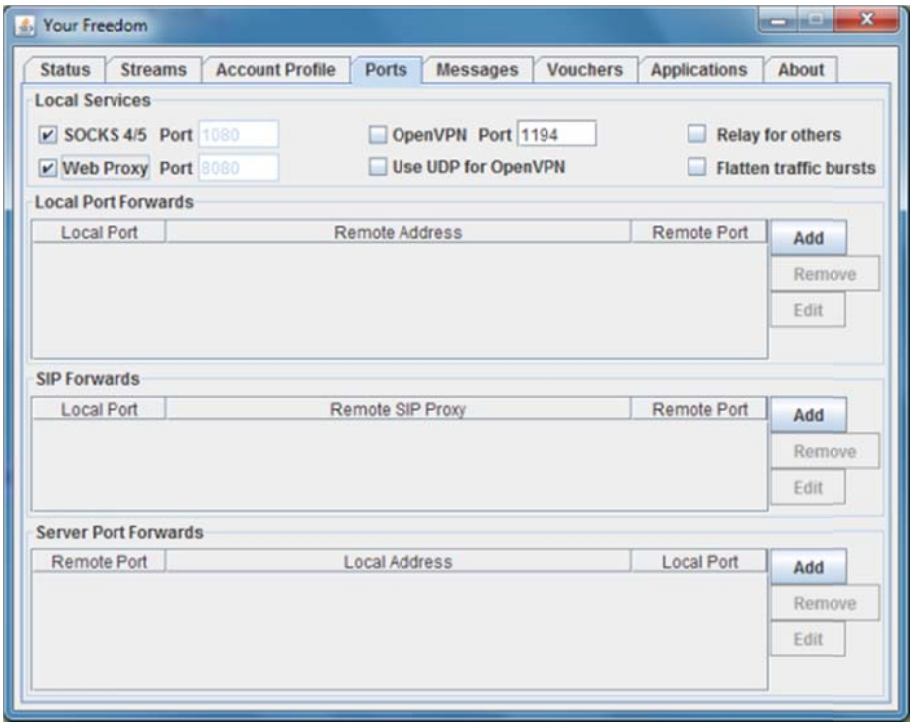


Ésta es una lista de aplicaciones que pueden ser configuradas directamente por el cliente Your Freedom. Las que estén instaladas tendrán cajas marcables, las demás estarán deshabilitadas. Marquemos las que se quieran configurar y demos clic en "OK". Si todo sale bien veremos una confirmación.



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 fungiendo 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 configurándolas 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 http://www.your-freedom.net/, están publicados algunos ejemplos.

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

2.4.2 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.

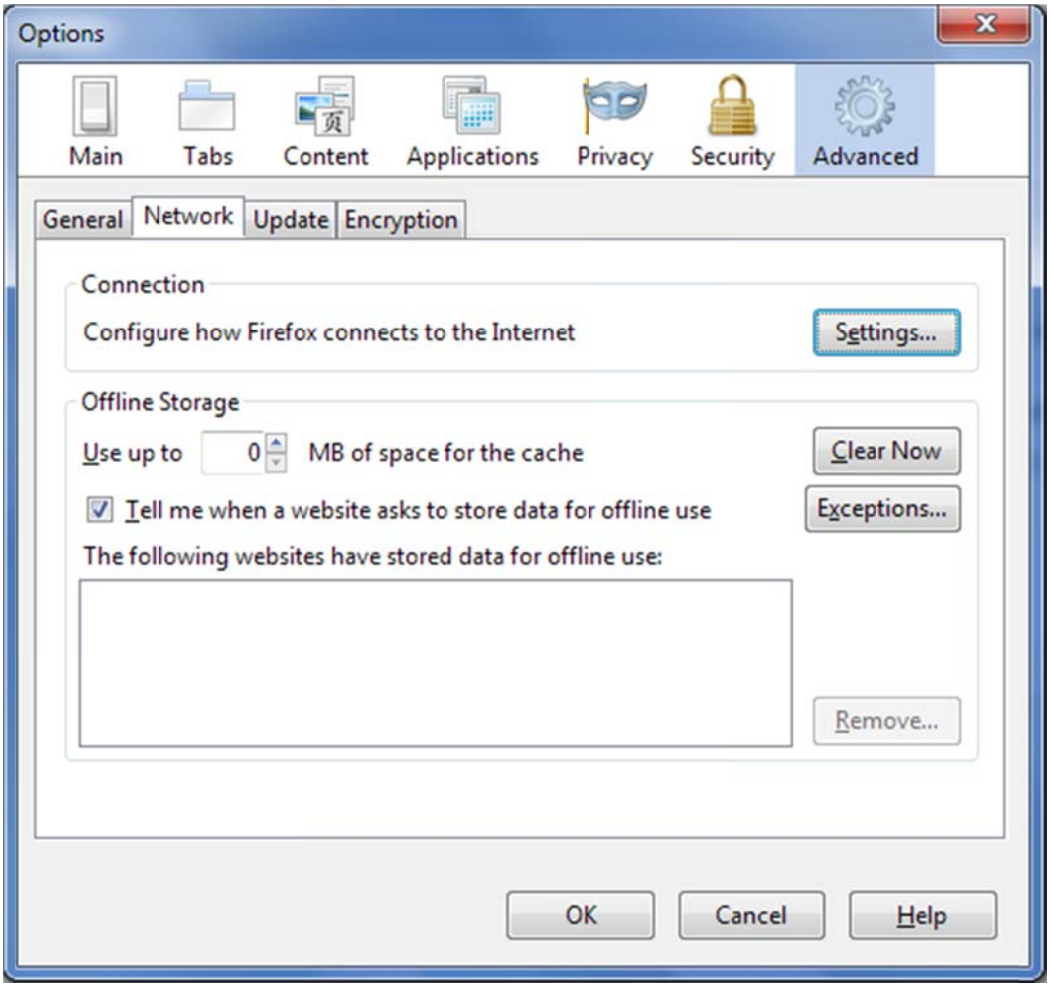
3) Usar una aplicación que permita “socksificar” a otras. Muchas aplicaciones no están diseñadas para trabajar en ciertos entornos de red y no preveen la posibilidad de ser configuradas para usar proxis. Muchas de ellas trabajan bien con Your Freedom si se las ejecuta desde dentro de un “socksificador”. 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, 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[5]. Éste tema se detalla en el capítulo 5.1 página 42.

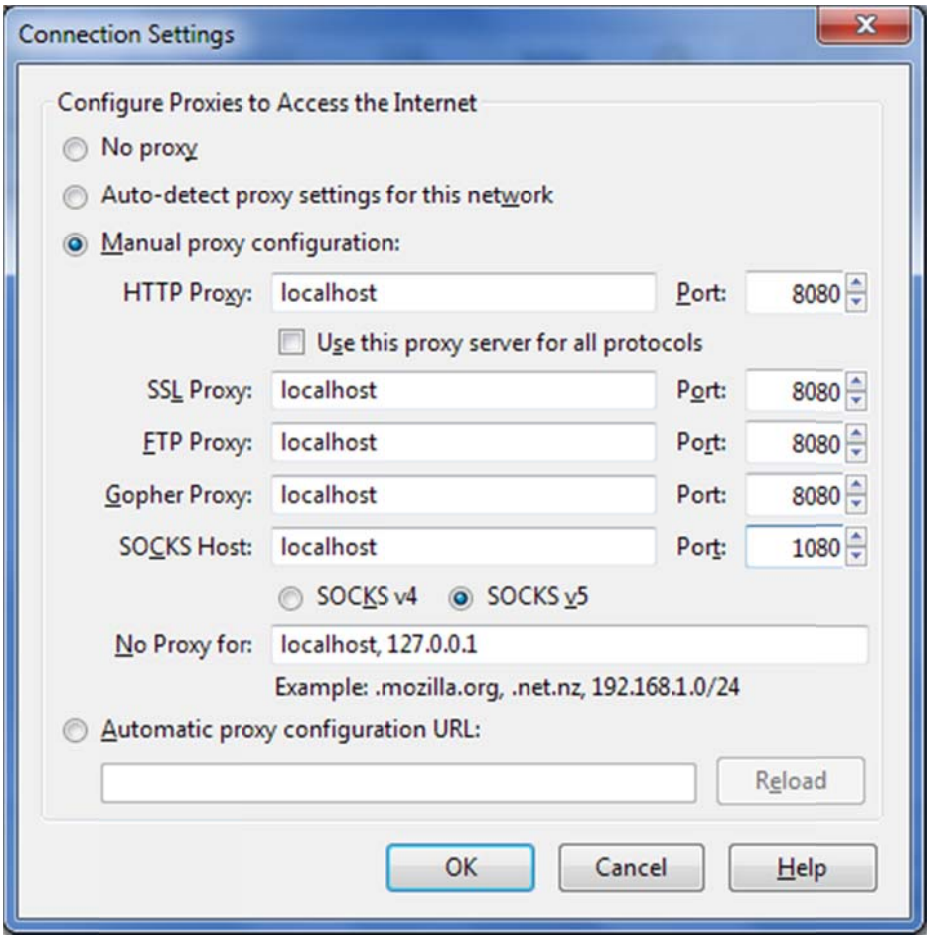
[5]Es necesario tener una cuenta cuyo perfil permita redireccionamientos de puertos de servidor. En la actualidad solo los poseedores de cuentas TotalFreedom pueden redireccionar puertos de servidor a sus PCs locales.

Configurando Mozilla Firefox

Todos los navegadores pueden usar proxis Web por tanto la opción 1) debe servir. Seleccionemos “Herramientas” > “Opciones” > “Avanzado”, al hacer click en la pestaña “Red”, vemos lo siguiente:



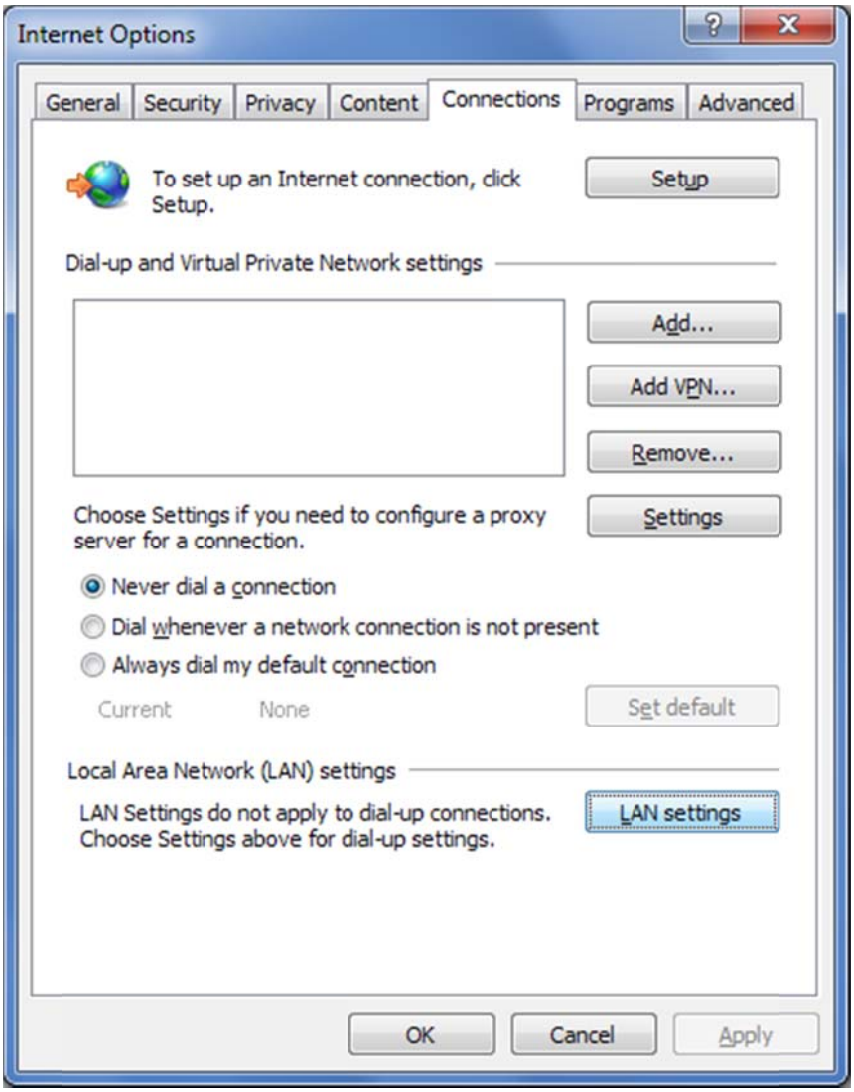
Hacemos clic en “Configuración”.



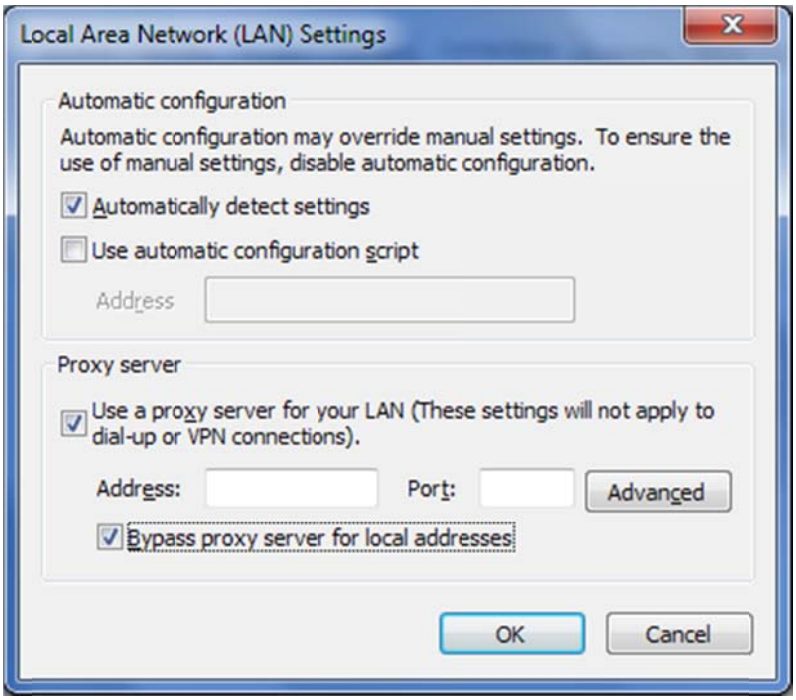
Complétese los valores como se muestra en la figura (se recomienda tomar nota de los valores originales para que así pueda ser más fácil recuperar la configuración inicial), hacer clic en ambas ventanas. Firefox estará ahora usando la configuración de Your Freedom.

Configurando Internet Explorer.

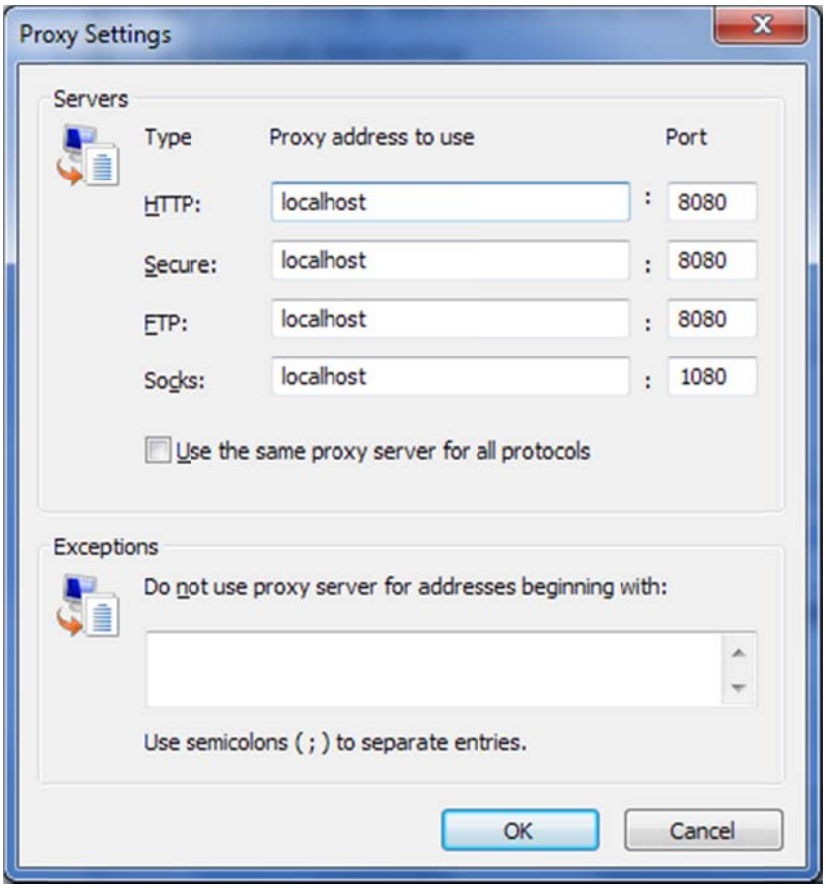
Como todos los navegadores Internet Explorer soporta proxis directamente. Y lo que es más, su configuración es compartida por muchas otras aplicaciones. Al seleccionar “Herramientas”, “Opciones de Internet” y hacer clic en la pestaña “Conexiones” veremos algo así:



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

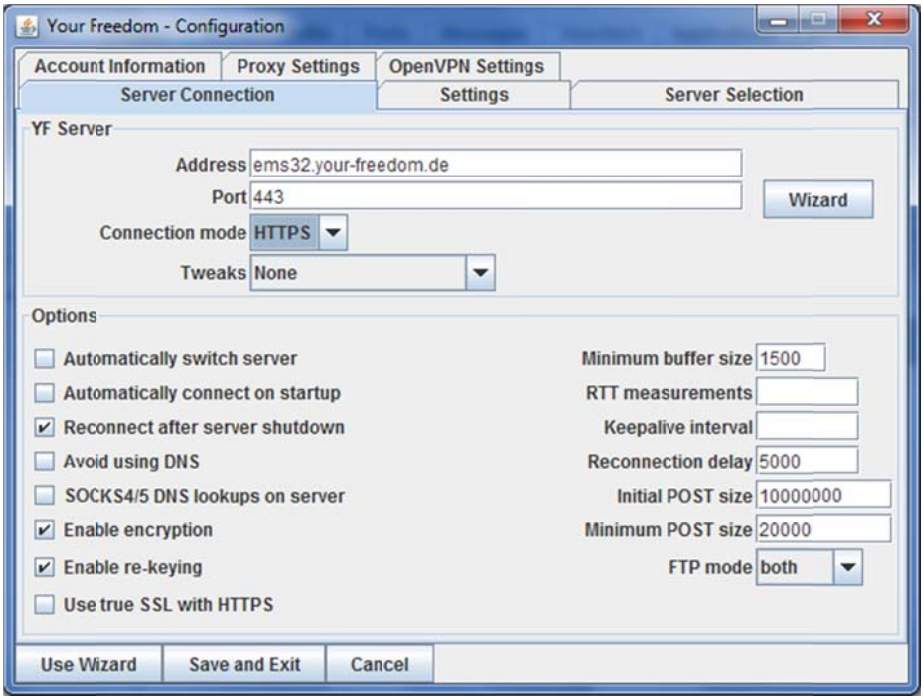
estemos conectados a través de él). Se recomienda tomar nota de los valores originales para que así pueda ser más fácil recuperar la configuración inicial.

2.5 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 aconsejable trabajar el fichero de configuración sin supervisión a menos que se sepa lo que se está haciendo :-)

2.5.1 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 de dialogo como esta:

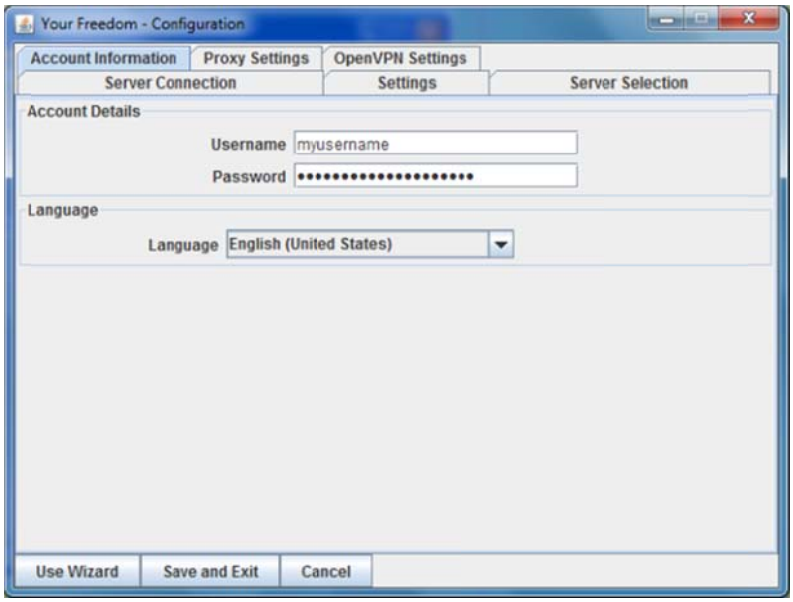


En la pestaña “Conexión con el servidor” configurar el nombre del servidor Your Freedom o su dirección IP (muchos nombres o IPs pueden ser separados por punto y coma ¡sin dejar espacios adicionales!) Seleccionemos el protocolo de conexión del menú desplegable y aparecerá automáticamente el puerto por defecto. Puede usarse el asistente para las opciones de conexión y dejar que el cliente escoja la mejor forma (debemos estar seguros que la configuración proxy del cliente es correcta).

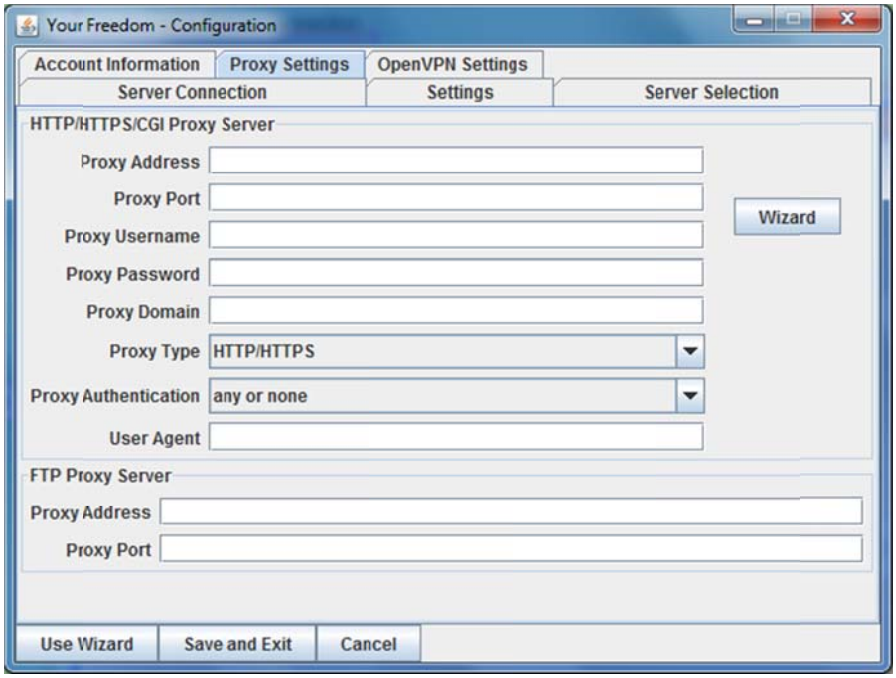
También pueden seleccionarse las opciones de conexión. Para la mayoría de los usuarios las últimas tres opciones deberán estar activadas. Y quizás sea conveniente marcar también “Evitar usar DNS” si se quiere conectar al servidor de Your Freedom por su dirección IP y no se quiere preguntar al DNS local. En este punto no es necesariamente aconsejable que se habilite la opción “Seleccionar automáticamente el mejor servidor” a menos que se sepa que se pueden usar todos los servidores. Estamos trabajando para mejorar esto, y de hecho gran parte está ya implementada.

La opción “Iniciar minimizado” está solo disponible para usuarios Windows. Cuando se inicie el cliente si ésta está activa, solo aparecerá un icono en la bandeja del sistema. Quizás sea conveniente activar “Conectar automáticamente al iniciar” y quizás combinarlo con el menú

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



Complétese la información de cuenta de Your Freedom: usuario y contraseña, y escójase 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).

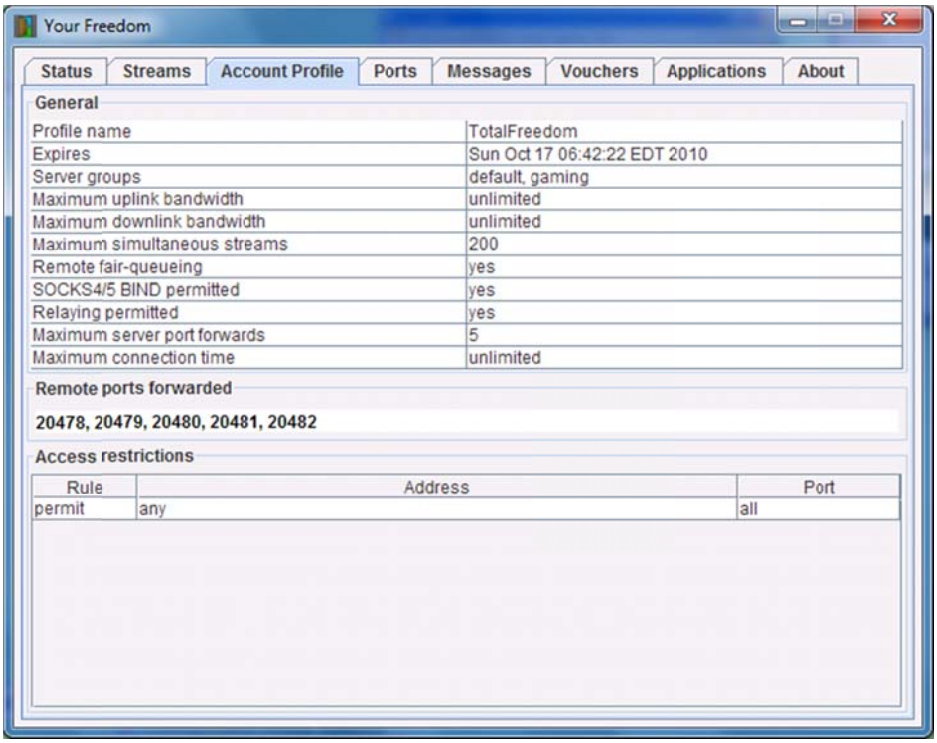
Si queremos usar conexión FTP y no tenemos acceso directo por este protocolo a los servidores de Your Freedom quizás se necesite especificar un Proxy FTP presente en la red (si la herramienta de línea de comando ftp funciona perfectamente significa que no es necesario configurar nada). El puerto probablemente 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 página 12.

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

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 como comunicarse con el equipo de soporte.

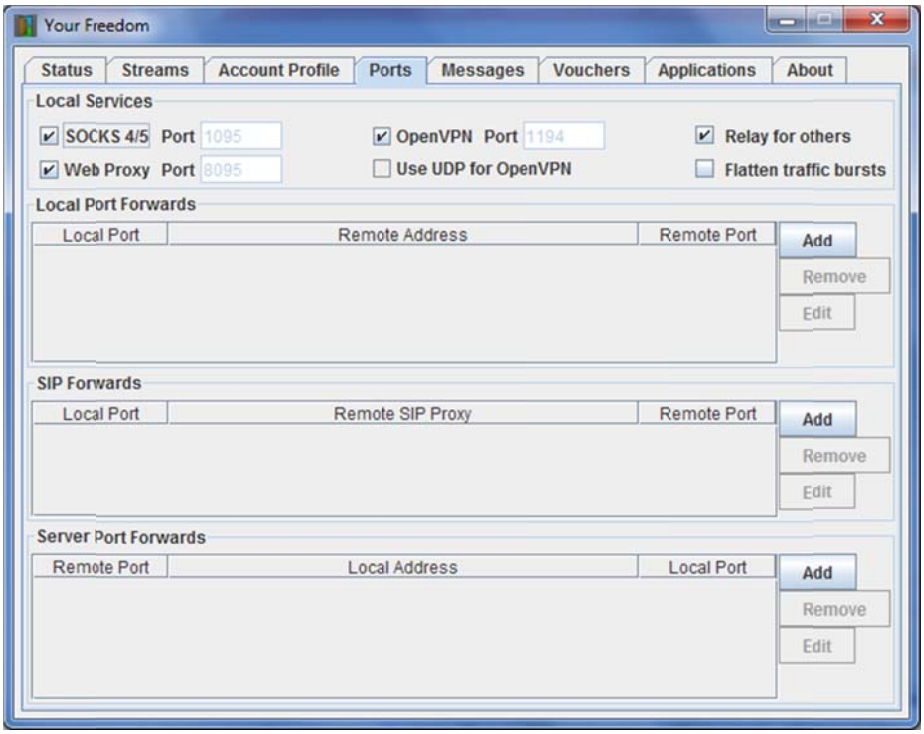
Una vez conectados verifiquemos el perfil de la cuenta accediendo a la pestaña “Account Profile”:



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”)

2.6 Iniciando y terminando la conexión

2.6.1 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 auque hayamos dejado accidentalmente nuestra cuenta conectada en nuestra oficina, la cual se desconectará.

Existe un bug en el modo de conexión FTP que puede ser disparado si cerramos la conexión y la reabrimos inmediatamente. Recibiremos un mensaje de error que dice que nuestra sesión

está duplicada. Si esto sucede deberán esperarse unos minutos antes de volver a conectarse o cerrar el cliente y abrirlo de nuevo[6].

2.7 Escogiendo el servidor correcto

2.7.1 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 triangulo, los vértices son la PC, el servicio de Internet que queremos acceder y el servidor Your Freedom. Mientras más se asemeje este triangulo 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[7] 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 valido señalar que los servidores de Your Freedom generan entre 2 y 8 terabytes de tráfico mensual, necesitan al menos 1GB de RAM, un buen CPU y deberá tener instalado Debian Linux.

2.7.2 Protocolos

No todos los servidores de Your Freedom permiten todos los protocolos[8] . 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.

[6]Éste es un bug archiconocido de Your-Freedom. Aún estamos buscando la forma de resolverlo.
[7] Esto puede no ser enteramente correcto, pero lo es para Internet.
[8]Todos los servidores permiten todos los modelos de conexion; esto no se refiere a como uno se conecta a un servidor de Your-Freedom sino que es lo que se puede hacer a través de la connexion.

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. 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.

2.7.3 Relays CGI

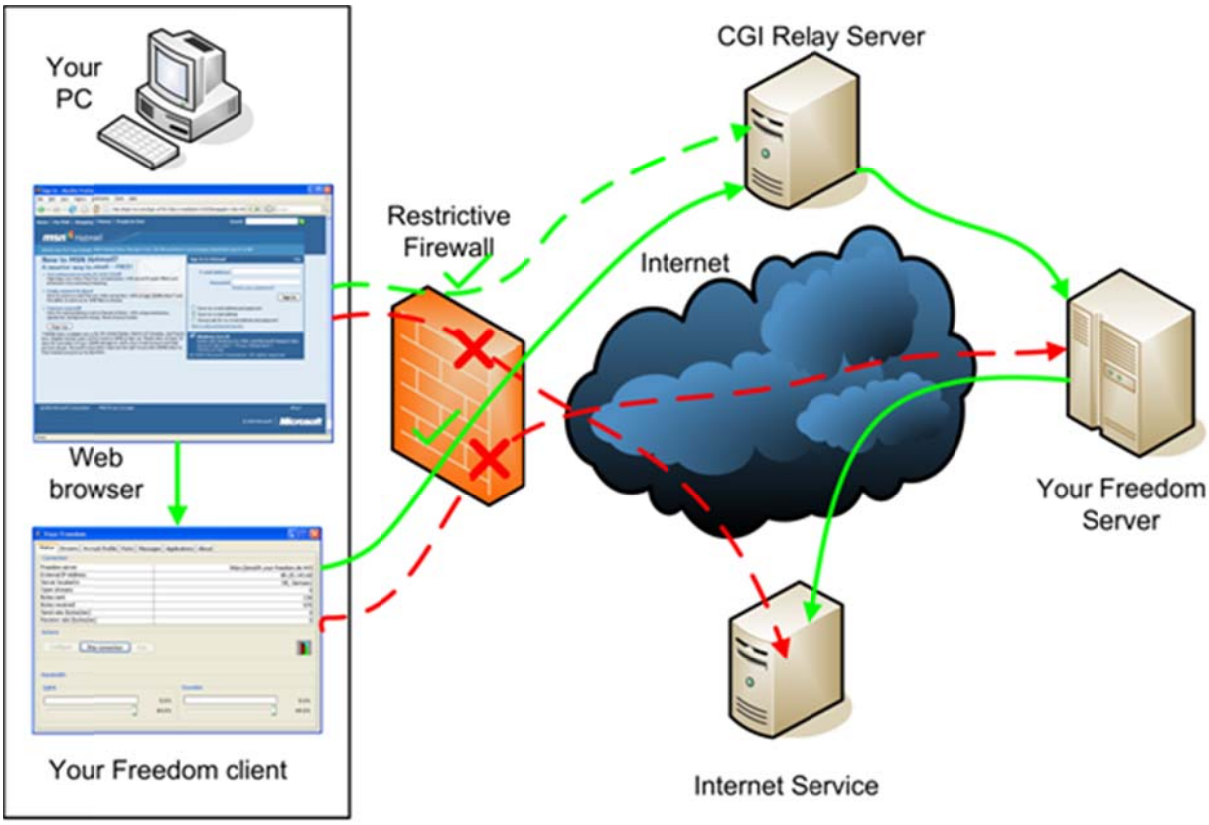
El método de conexión CGI es tan estándar que no solo engaña a los proxis, también permite que usemos un script que sirva de puente entre los usuarios y el servidor real de Your Freedom. Ese script es una página PHP que podemos colgar en cualquier servidor. Si bien es simple bloquear todos los servidores 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?

Your Freedom piensa recompensar a las personas que instalen relays CGI en función del tráfico total que éste genere. 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 ésta 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 http://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 (http://www.your-freedom.net/156/). El sistema analizará si funciona, se agregará a la base de datos y los clientes podrán encontrarlo (toma su tiempo, no esperemos 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.

3 Conectando juegos y otras aplicaciones

3.1 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 **Fehler! Verweisquelle konnte nicht gefunden werden.** Redireccionamiento de puertos página 42

3.2 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.

3.2.1 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.

SocksCap

Esta es una herramienta para uso no comercial. La locación exacta de la descarga no está disponible. Tendrémos que buscarlo en google 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 dias, la licencia cuesta USD 40. Además también está disponible para Mac OSX.

HummingbirdSocks

La suite Hummingbird contiene un socksifier. Se puede descargar desde el sitio principal de Hummingbird.

3.2.2 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 trafico 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.

3.2.3 Mac OS X

Proxifier

Proxifier está también disponible para MacOSX.

Tsocks

Vease las instrucciones sobre socks en MacOSX en http://forums.macosxhints.com/archive/index.php/t-55338.html.

3.3 Soporte OpenVPN

3.3.1 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.

3.3.2 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 nuesetra 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. Considerese 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.

3.3.3 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 randos 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 IP o 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.

¿Retrasmisión 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 mas información sobre su localización). Estos ficheros comienzan con “client” o “server”; cópiense a las otras PC en alguna carpeta, edítese 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.

3.3.4 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 valido 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.

3.3.5 Diagnóstico de problemas

El túnel OpenVPN no se inicia correctamente

Chequéese 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.

4 Planes, paquetes y vouchers

4.1 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 15 horas en cualquier intervalo de 7 dias, 6 horas en intervalos de 24h y además, cada hora que pase el cliente YF se desconectará automáticamente y tendremos que conectarnos otra vez.

4.2 Paquetes 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.

	Free	Basic	Enhanced	Total
Ancho de banda	64 Kbit/s	256 Kbit/s	4 Mbit/s	unlimited
Conexiones simultaneas	10	50	100	200
Proxy Web	✓	✓	✓	✓
Proxy Socks	✓	✓	✓	✓
Cifrado	✓	✓	✓	✓
Conexión HTTP	✓	✓	✓	✓
Conexión HTTPS	✓	✓	✓	✓
Conexión CGI	✓	✓	✓	✓
Conexión FTP	✓	✓	✓	✓
Conexión UDP	✓	✓	✓	✓
Retransmisión para otros	✓	✓	✓	✓
Tiempo de conexión	6 hours	unlimited	unlimited	unlimited
Puertos de servidor	✗	✗	✗	✓ (5)

1 mes	Free	€ 4.00	€ 10.00	€ 19.99
3 meses	Free	€ 10.00	€ 28.00	€ 57.99
6 meses	Free	€ 17.00	€ 50.00	€ 109.99
12 meses	Free	€ 30.00	€ 95.00	€ 199.99

Para comprar paquetes, debemos visitar la página Web www.your-freedom.net, registrarnos, 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 1.25 dólares estadounidenses.

Cuando compramos 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 http://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[9].

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 agradará recibir un cheque ocasionalmente.

4.2.1 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.

4.3 Test drives

Si estamos considerando comprar un paquete pero no estamos seguros si será lo que esperamos podemos probar gratis antes. Después de registrarnos 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 que tengan más de 3 días de creadas y que no hayan probado extensivamente con anterioridad.

[9] Si, esto puede ser usada para evitar que expire un paquete más caro.

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.

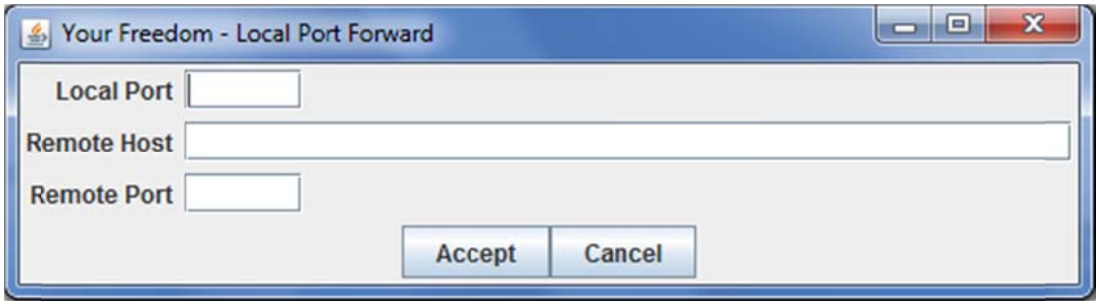
Con los paquetes comprados, tomará unos minutos para que la actualización se propague a todos los servidores. Debe reiniciarse la conexión o incluso el cliente Your Freedom para ver las diferencias.

5 Temas Avanzados

5.1 Redireccionamiento de puertos

5.1.1 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 configuraríamos un redireccionamiento de puerto local similar al siguiente.



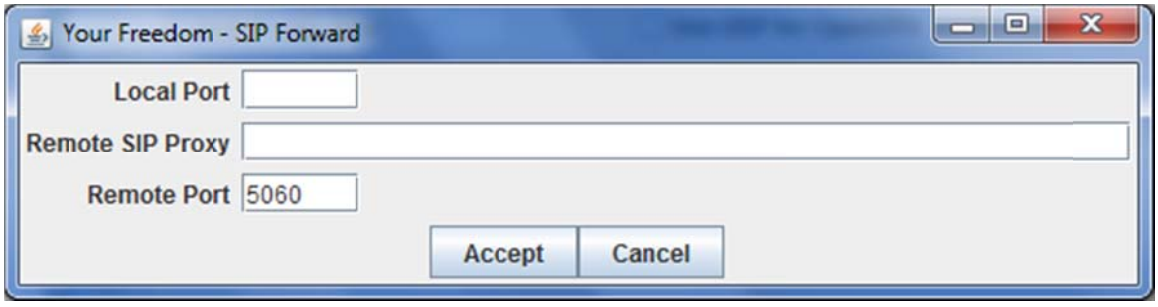
Ahora en vez de conectarnos por SSH a “some.host.somewhere” por el puerto 22 simplemente le ordenaríamos al cliente SSH que se conecte a localhost por el puerto 2222. Your Freedom se encargará de hacer el puente. Es válido señalar que si el servidor remoto no es alcanzable el cliente SSH se comportará 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.

5.1.2 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

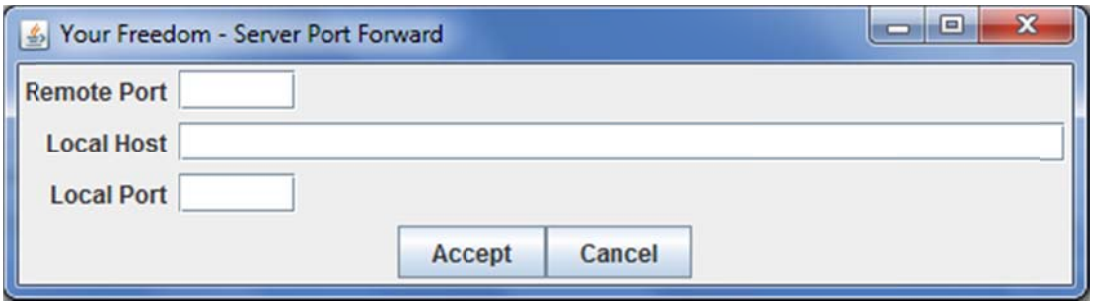
deshabilitar STUN ya que no tendría sentido en este contexto (solo haría las cosas más lentas)

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, asi 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).

5.1.3 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 esta servicio (se puede configurar de todas formas pero si el perfil no lo permite no funcionara). 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 TOTAL pueden acceder a este tipo de redireccionamiento

5.2 Compartir nuestra conexión con otros

5.2.1 Retrasmisión

Si nuestro perfil soporta “Retrasmisión 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 mas común es compartir nuestra conexión con compañeros de cuarto o colegas en nuestra oficina.

5.2.2 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. Otra cosa que debemos tener en cuenta es que nuestra otra Interfaz de red no use una red 192.168.0.0/24 – si asi 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. Demos clic derecho encima y escojamos “Propiedades” -> “Avanzado” y seleccionemos “Permitir a otros usuarios de esta red conectarse a través de ésta conexión a internet” y escojamos la interfaz de red que conecta a nuestra otra PC/Playstation/etc. Demos clic en “Aceptar” y cerremos 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.

5.3 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, demos clic en “Inicio” y después tecléemos “cmd” pero no presionemos “Enter”. Esperemos que “cmd.exe” aparezca, demosle clic derecho y escojamos “Ejecutar como Administrador”. Cuando la consola abra tecléemos

```
netsh interface ipv6 show teredo
```

Si "status" es "offline" introduzcamos:

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

Esperemos un rato y chequéemos 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 tecleamos cmd). Una vez abierta la consola tecleamos “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.

5.4 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 trafico 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 y cgi_uplink_mindelay a quizás 20. Intentémoslo, no se puede romper nada, si no funciona, simplemente quitémos la línea.

Anexos

Anexo A. 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 situationes 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 mas 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 “locahost” 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. http://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: http://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, iniciémos 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 ejecutémos “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

* En el momento en que se escribe este manual, la retrasmisión para otros es permitida a todos los usuarios.

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.

Creando un fichero “dump”

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. De necesitarse 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 su taza 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.

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

El cliente Your Freedom no tiene provisiones para actualizarse automáticamente. La actualización es manual y debe hacerse con cierta frecuencia. Mantener nuestra instalación de Your Freedom actualizada es crucial especialmente cuando dependemos de la habilidad de Your Freedom para conectarnos.

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 envíese 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 = Dia

Serie = consecutivo dentro del dia.

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

Anexo B. 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 encotrada 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 6h por dia a imilitado. 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.

Otro tipo de plan específico para algunos países viene de la colaboración con Sesawe. Para más información remitirse al capítulo 2.2.1 en la página 12.

Disponibilidad de los servidores por países

Reservar el uso de algunos servidores situados en algunos puntos geográficamente estratégicos es una razón para limitar el acceso a estos servidores desde otros lugares. Este es el caso de algunos servidores situados en Asia y Sudamerica, a los que los usuarios conectados desde países cercanos tienen prioridad por encima usuarios conectados desde otras latitudes.

La otra razón es 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 visitese nuestro sitio web o escríbase 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”. Inténtese con otro servidor.

Tweaks

Esta es una característica que se adicionó en la versión 20100204-01. Consiste en 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 explíticos. 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.

Anexo C. 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 vi en sistemas Unix, o Notepad en Windows).

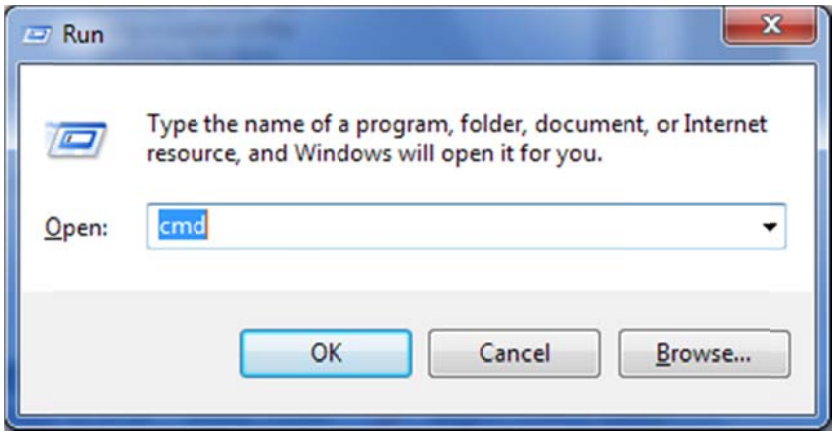
¿Donde está el directorio home?

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 y 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\pedro>_
```

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. Éstas 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 evítense 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!

Option	Description	Type	Arguments
autoscroll_messages	Desplazar para hacer visible lo nuevo en la ventana de mensajes	simple opcional	“true”/ “false”(por defecto)
avoid_dns	No usar el nombre si se conoce el IP del servidor	simple opcional	“true” / “false”(por defecto)
bw_downlink	Ancho de banda del enlace descendente	simple opcional	Bits por segundo. 0 para “ilimitado”.
bw_uplink	Ancho de banda del enlace ascendente	simple opcional	Bits por segundo. 0 para “ilimitado”.
connect_on_startup	Iniciar conexión apenas se ejecute el cliente	simple opcional	“true” / “false”(por defecto)
debuglevel	Habilita mensajes de depuración en la consola Java(no en la consola de mensajes)	simple invisible	Mientras más bajo más detallado. Por defecto es 999.
dont_show_popups	No mostrar ventanas emergentes	simple opcional	“true” /“false” (por defecto).
encryption	Activa el cifrado de la conexión	simple opcional	“true” / “false” (por defecto). El wizard lo activa por defecto. No es recomendable dejarlo desactivado.
file_extip	Registra la IP externa del servidor en el fichero de configuración.	simple opcional	Esto permite usar la IP externa del servidor en scripts
follow_server_recommendations	Indica al cliente que siga las recomendaciones de otros servidores.	simple opcional	“true” / “false” (por defecto).

fool_pix	Prueba un recurso en versiones vieja de PixOS para burlar WebSense	simple invisible	“true” / “false”.Solo habilitaremos esto si sabemos que nuestro cortafuegos PIX usa WebSense y no podemos conectarnos a través de él.
ftpproxy	Si se está usando el protocolo FTP se usará un proxy FTP no transparente	simple opcional	Completaremos el nombre/IP del Proxy para FTP. Quitar de no necesitarse.
ftpproxyport	Si se está usando el protocolo FTP se usará un proxy FTP no transparente	simple opcional	El parámetro es el nombre/IP del Proxy para FTP. Quitar de no necesitarse.
headers	Cuando se hace la petición al Proxy se Incluyen encabezamientos adicionales	multi opcional	Si necesitamos encabezamientos adicionales o queremos redefinir cosas como ‘User Agent’, este es el lugar. Por ejemplo:”headers User Agent: DontCare 1.0”
http_flush	Cierra y reabre el enlace ascendente de la conexión HTTP a intervalos regulares.	simple opcional	Tiempo en milisegundos. Si necesitásemos hacer esto deberemos usar el modo de conexión CGI.
idle_kill	Terminar conexiones que hayan estado ociosas por este tiempo.	simple opcional	obsoleto
initial_post_size	Usar este tamaño inicial al hacer una petición POST	simple invisible	Por defecto es 10000000(10Mb). El cliente irá reduciendo el tamaño hasta que el Proxy Web acepte el valor o caiga por debajo de minimum_post_size. De establecerse en el límite aceptable por el Proxy ahorraría tiempo de conexión.

level_messages	Solo los mensajes que estén por encima de este nivel serán mostrados	simple opcional	0 es “depuración”, 7 es “emergencia”. 1 “informativo”.
language	Idioma de la interfaz(2 letras minúsculas ISO)	simple opcional	Por defecto es “en” Solo están disponibles un número reducido de idiomas
location_x	Coordenada X de la ventana Your Freedom en la pantalla.	simple opcional	0 es el lado izquierdo, valores más grandes están más a la derecha
location_y	Coordenada Y de la ventana Your Freedom en la pantalla.	simple opcional	0 es el tope, valores más grandes están más abajo
minimum_post_size	Tamaño mínimo de la petición POST	simple invisible	Por defecto es 20000(20Kb). Solo reducir si se sabe que el Proxy rechazará peticiones “posts posts” por encima de los 20K.
openvpn	Puerto OpenVPN	simple opcional	Su valor por defecto es 1194, cambiar solo si se necesita este puerto para alguna otra cosa.
openvpn_exclude	Redes y rangos de IPs que deberán ser excluidos de ser enrutados a través de OpenVPN.	múltiple invisible	Adicionar una línea para cada dirección IP o de red (dirección IP con una máscara) que no deba ser enrutada a través del canal OpenVPN.
password	Contraseña de cuenta de Your Freedom	Simple requerido	One: your Your Freedom password
portaccept	Redireccionar un Puerto de servidor	Multiple opcional	server port local host local port
portforward	Redireccionar un Puerto local a un Puerto remoto	Multiple opcional	local port remote host remote port

protocol	El protocolo de conexión a usar	Simple requerido	Solo son válidos los siguientes valores: “http”, “https”, “cgi”, “ftp”, “udp”.
proxy	El puerto del proxy	Simple opcional	Si está presente y es distinto de cero el ordenador fungirá como Proxy Web por el puerto especificado.
proxydomain	El dominio del Proxy si acaso se requiere(Proxy NTLM solamente)	Simple opcional	Un nombre de dominio de Windows para autenticarse en el Proxy Web.
proxyhost	El nombre/IP del servidor Proxy a través del cual Your Freedom crea el túnel.	Simple opcional	Nombre o IP del Servidor Proxy. Dejar en blanco si no se necesita Proxy.
proxyport	El puerto del Proxy Web	Simple opcional	El puerto del servidor Proxy. Poner en 0 o quitar si no se necesita proxy.
proxypass	La contraseña para autenticarse en el Proxy	Simple opcional	Password del proxy.
proxyuser	Nombre de usuario para autenticarse en el Proxy Web.	simple opcional	Un nombre de usuario en caso de necesitarse autenticación
redirect_dns	No resolver nombres de dominio localmente cuando se esté usando SOCKS	Simple opcional	”true”/”false”. Usar si no queremos que el servidor de nombres local resuelva los nombres.
rekey	Cambiar llave de cifrado frecuentemente	Simple opcional	“true”/“false”. El asistente establecerá el valor de esta propiedad en “true”, este es el valor recomendado.
relay	Permite que otros usuarios usen la misma sesión Your Freedom.	simple opcional	”true”/”false”. Esta opcion solo funciona si nuestro perfil lo permite.

server_criterion	Definir criterios para selección automática de servidores	multi opcional	nombre del criterio número entre 0(rechazado) y 10(requerido), por defecto es 5(no tomar en cuenta)
sipforward	Simula ser una puerta SIP remota	multiple opcional	puerto local dirección SIP remota puerto SIP remoto
socks	El puerto SOCKS	simple opcional	Si está presente el ordenador fungirá como un Proxy SOCKS por el puerto especificado.
start_minimized	Empezar minimizado y en la bandeja del sistema	simple opcional	“true” /“false”
tunnelhost	El servidor your-freedom a usar	simple requerido	Uno o varios nombres de dominio/direcciones IP/urls de relays CGI. Múltiples direcciones separadas por punto y coma
tunnelport	El Puerto del servidor Your Freedom	simple requerido	Un puerto
use_http11	Usar HTTP/1.1 en lugar de HTTP/1.0 cuando se hacen peticiones al Proxy	simple invisible	”true”/”false” Si el Proxy está actuando de forma inesperada conmutar el valor.
username	El nombre de usuario de Your Freedom	simple requerido	El nombre de usuario de Your Freedom.
cgi_uplink_maxdelay†	Delay máximo antes de enviar la cola de paquetes ascendentes pendientes.	simple invisible	Después de este tiempo la cola es vaciada sin importar lo pequeña que sea la cantidad de paquetes a enviar.
cgi_uplink_mindelay†	Numero de paquetes que disparan la descarga de la cola	simple invisible	El tiempo de espera mínimo entre dos vaciados de la cola. (Peticiones POST). En su defecto 1ms.

cgi_uplink_urgentdelay[†]	Demora máxima para los datos urgentes	simple invisible	El tiempo máximo de demora si hay datos urgentes que enviar en la cola (ej. Pequeños marcos pertenecientes a una conexión que no ha enviado paquetes recientemente - -- interactividad! --). Por defecto 20ms.
cgi_uplink_threshold[†]	Número de marcos que disparan un vaciado.	simple invisible	El número de paquetes que causan que cgi_uplink_mindelay sea utilizado en lugar de cgi_uplink_maxdelay (0 para deshabilidar), en otras palabras: si ésta cantidad de frames están en espera, vaciar inmediatamente. Por defecto en 3[††]
post_min_holdoff	Tiempo a esperar antes de abrir nuevas conexiones.(milisegundos)	simple	Por defecto en 5000.
post_max_connections:	Número máximo de conexiones concurrentes.	simple	Algunos tendrán que reducir esto a 1. Aunque es posible usar valores superiores, en algún punto comenzará a afectarse el performance. El valor por defecto (2) es suficientemente bueno para la mayoría de los casos.
post_min_post_size	Tamaño mínimo del request del POST.	simple	Nunca establecer el tamaño máximo del post por debajo de éste límite. Esto pudiera significar un bloqueo del enlace ascendente. (Por defecto: 3000)

[†]Todos estos valores solo se aplican al enlace ascendente del modo CGI. Si hay un marco keepalive en cola se usa mindelay – valores fuera del rango mindelay maxdelay no serán usados --

Las opcoines cgi_? Fueron agregadas específicamente para permitir que los usuarios ajustaran el mecanismo de cgi relays. Por ejemplo, si los POSTs frecuentes en gran número no fueran deseable, los usuarios pudieran establecer maxdelay=3000, mindelay=1000, urgentdelay=500 y threshold=0. Los POSTs serían menos aunque mayores y el impacto sería menor aunque no insignificante.