

Anonimato En Red

Ante todo, hay que tener claro que **el anonimato 100%** fiable en internet, **no existe**. Aún así, con diversos programas puedes “camuflarte” en un porcentaje bastante elevado.

Indice

- **Vpn**
 - [VPNs que aceptan pagos anónimos](#)
 - [VPNs de pago](#)
 - [VPNs gratuitas](#)
- **Servidores DNS libres**
 - [¿Qué son?](#)
 - [Cambiar DNS en WinXP](#)
 - [Cambiar DNS en Windows Vista o Win7](#)
 - [Cambiar DNS en GNU/Linux](#)
 - [Securizar DNS](#)
 - [Lista de servidores DNS libres](#)
- **Tor**
 - [¿Cómo funciona?](#)
 - [Instalación en Windows](#)
 - [Instalación en Debian/Ubuntu](#)
 - [Debilidades de la red Tor](#)
- **i2p**
 - [¿Qué es?](#)
 - [Como acceder a IRC a través de i2p](#)
 - [Iniciando i2p en Linux](#)
- **FoxyProxy**
 - [¿Qué es?](#)
 - [¿Qué es un proxy?](#)
 - [Instalación](#)
 - [Utilización](#)
 - [Otra información de interés](#)
- **JonDonym**
 - [¿Qué es?](#)
 - [Configuración y uso](#)
- **Freenet**
 - [¿Qué es?](#)
 - [Configuración en Linux](#)
 - [Descarga](#)

VPN

VPN o Redes Privadas Virtuales (wiki: en.wikipedia.org/wiki/Virtual_private_n...). “El mejor método” para navegar de forma anónima y casi el más fácil de configurar sería un VPN de PAGO. Hay versiones gratuitas de VPNs, pero no son recomendables, ya que podrían dar información de tu acceso a Internet a compañías

de publicidad y lo más probable es que estén más dispuestos a renunciar a proteger tu información en cualquier situación legal delicada. Las instrucciones para instalar y/o configurar tu VPN suelen ser facilitadas por los propios proveedores del servicio.

VPNs que aceptan pagos anónimos (ukash, cashu, paysafecar, BitCoin etc...)

- www.101sec.net (Recomendada por #opspain)
- www.bwprivacy.to
- www.yourprivatevpn.com
- www.ivacy.com
- www.microvpn.com (solo IPs de EEUU)
- www.ovpn.to
- www.change-mon-ip.com
- www.cinipac.com
- www.airvpn.org
- mullvad.net/en/bitcoin.php

Lista de VPNs de pago

- www.swissvpn.net
- www.Linkideo.com
- www.perfect-privacy.com
- www.ipredator.se
- www.anonine.se
- www.vpntunnel.se
- www.relakks.com
- www.steganos.com

Lista de VPN gratuitas

- www.openvpn.net
- www.packetix.net/en
- www.proxpn.com
- www.cyberghostvpn.com
- www.bestukvpn.com
- www.securitykiss.com (Tráfico limitado)
- www.projectloki.com
- www.freesslvpn.net
- www.raptorvpn.com
- www.hotspotshield.com
- www.usaip.eu/en/free_vpn.php (Desconexiones forzadas cada 7 minutos)
- www.expatshield.com
- www.your-freedom.net Similar a una VPN
- www.gpass1.com/gpass Similar a una VPN y proxy web online
- bb.s6n.org/viewtopic.php?id=81 (1 Gb de tráfico al mes)
- www.torvpn.com
- www.hostizze.com

Servidores DNS libres

¿Qué son?

Un DNS o Servidor de Nombre de Dominio, a grandes rasgos, es aquel que traduce las direcciones que escribimos en nuestro navegador para acceder a las webs en direcciones IP. Cada ISP (proveedor de

Internet) tiene servidores DNS propios y existen en total 13 servidores raíces de DNS que son la última instancia a buscar para encontrar la dirección del servidor DNS autorizado para la zona de más alto nivel del dominio buscado.

Adicionalmente ciertos servicios proveen una protección ante sitios de phishing y resolución automática de direcciones mal escritas.

Cambiar DNS en WinXP

Acceder a Menú Inicio → Panel de Control → Conexiones de Redes → Botón derecho sobre la conexión (posiblemente se llame Conexión de Área Local) → Propiedades → Doble Click sobre el elemento de Protocolo Internet (TCP/IP) → Seleccionar “Usar las siguientes direcciones de servidor DNS” → Y configuramos las DNS en los 2 campos que nos deja, en el primero la DNS principal y en el segundo una DNS alternativa.

Cambiar DNS en Windows Vista o Win7

Cambiar los servidores DNS que tiene configurado en Windows Vista/7 es muy sencillo. Hacemos click en inicio → Panel de control → en la categoría Redes e Internet hacemos clic sobre Ver el estado y tareas de red → Clic en Conexión de área local (o el nombre que tenga nuestra conexión a Internet) → En la ventana de Estado de Conexión de área local clic en Propiedades → Seleccionamos Protocolo de Internet versión 4 (TCP/IPv4) y clic en el botón de Propiedades → Tenemos que marcar la casilla Usar las siguientes direcciones de servidor DNS y en Servidor DNS preferido y Servidor DNS alternativo escribimos las direcciones del servidor DNS → Aceptar y botón Cerrar para activar los nuevos servidores DNS.

Cambiar DNS en GNU/Linux

Para cambiar las DNS, debemos abrir un terminal y editar el archivo resolv.conf:

```
vim /etc/resolv.conf
```

El archivo contiene lo siguiente:

```
search local
nameserver
nameserver
```

Donde dice “nameserver” ahí debemos colocar las dns. En otras palabras:

```
nameserver tu_dns_primaria
nameserver tu_dns_secundaria
```

Por ejemplo:

```
search local
nameserver 80.150.31.200
nameserver 80.150.31.150
```

Guardamos los cambios y listo.

Securizar DNS

DNSEncrypt

Esta herramienta cifra el tráfico DNS, de nuestro ordenador al servidor DNS. Esto sirve para evitar ataques Man-In-The-Middle, que te espíen, DNS poisoning y que el ISP bloquee páginas web.

Para Windows hay GUI, por lo que solo explicaré la instalación en Debian/Ubuntu.

Antes que nada, debemos instalar un paquete llamado `libsodium` de la que DNSEncrypt depende. Descargamos la última versión del paquete, en este caso la versión 0.4.5 de la página siguiente:

download.libsodium.org/libsodium/releases

Una vez descargado solo tenemos que descomprimirlo, compilarlo y ejecutarlo:

```
tar -xvzf libsodium-0.4.5.tar.gz
cd libsodium-0.4.5
./configure
make && make check && make installcheck && make install
```

Ahora podemos proceder a instalar la herramienta en cuestión. Lo primero será descargar el comprimido tar.bz2 de la página dnscrypt.org/dnscrypt-proxy/downloads Para descomprimirlo usaremos el siguiente comando, siendo * la versión que tengamos:

```
bunzip2 -cd dnscrypt-proxy-*.tar.bz2 | tar xvf -
```

Una vez descomprimido entramos en el directorio mediante el comando:

```
cd dnscrypt-proxy-*
```

Ahora ya solo queda compilarlo y instalarlo. El parámetro -j2 indica que usemos dos núcleos de la CPU, podemos poner el número que queramos, cuanto más alto más rápido irá:

```
./configure && make -j2
make install
```

El proxy se instalará en /usr/local/sbin/dnscrypt-proxy por defecto.

Su uso es el siguiente.

```
dnscrypt-proxy --daemonize --resolver-address=113.20.6.2:443 --provider-name=2.dnscrypt-cert.cloudns.com.au --provider-key=1971:7C1A:C55
```

DNSEncrypt usa por defecto DNS de openDNS, pero yo he escogido el de arriba por que no loguean IPs ni guardan las búsquedas que se realizan. Si queremos usar los DNS por defecto sólo hay que poner

```
dnscrypt-proxy --daemonize.
```

—resolver-address=**IP:puerto**= La IP y puerto del DNS que escojamos.

—provider-name=**nombre**= El nombre del DNS que escojamos.

—provider-key**llave**= La clave del servidor.

Una vez establecido el proxy, ahora tenemos que empezar a usarlo. Para hacerlo sólo tenemos que poner en el DNS que usamos la ip 127.0.0.1.

Y ya sólo queda hacer que se establezca de nuevo cada vez que reiniciamos. Podemos hacerlo copiando el comando que hemos puesto arriba a /etc/rc.local.

Lista de servidores DNS libres

- Swiss Privacy Foundation
 - 62.141.58.13 (HTTPS-DNS/DNSEC)
 - 87.118.104.203 (DNSEC)
 - 87.118.109.2
- Telecomix Censorship-proof DNS
 - 91.191.136.152
- OpenNIC
 - Lista servidores con distintas características, ver tabla:
www.opennicproject.org/configure-your-dns
- OpenDNS:
 - 208.67.222.222
 - 208.67.220.220
- DNS Advantage:
 - 156.154.70.1
 - 156.154.71.1
- CloudNS
 - Requiere DNSEncrypt. Acepta DNSSEC, Namecoin y Tor.

- o Dirección: 113.20.6.2 o gc2tzw6lbmeagrp3.onion
 - Puerto:443
 - Nombre del proveedor: 2.dnscrypt-cert.cloudns.com.au
 - Llave DNSCrypt:
1971:7C1A:C550:6C09:F09B:ACB1:1AF7:C349:6425:2676:247F:B738:1C5A:243A:C1CC:89F4
- o Dirección: 113.20.8.17 o l65q62lf7wnfme7m.onion
 - Puerto:443
 - Nombre del proveedor: 2.dnscrypt-cert-2.cloudns.com.au
 - Llave DNSCrypt:
67A4:323E:581F:79B9:BC54:825F:54FE:1025:8B4F:37EB:0D07:0BCE:4010:6195:D94F:E330

TOR

Tor (The Onion Router) es una implementación libre de un sistema de encaminamiento llamado onion routing que permite a sus usuarios comunicarse en Internet de manera anónima.

Web del proyecto: www.torproject.org

¿Cómo funciona?

Al conectar a internet a través de la red tor, la información enviada es cifrada y viaja por diversos servidores ocultando la ip de origen. Al llegar a su destino la información es descifrada y enviada, de manera que no hay manera de saber quien envió la información.

Instalación en Windows

1. Descarga Tor Browser Bundle [aquí](#)
2. Haz doble click en el .exe y elige un directorio donde descomprimirlo
3. Se creará una carpeta llamada "Tor Browser" con todos los componentes necesarios
4. Entra en "Tor Browser" y haz click en el icono "Start Tor Browser".
5. Se abrirá el panel de control y seguidamente el navegador Firefox mostrará la confirmación de que Tor está funcionando correctamente

Todo esto te servirá para navegar con Firefox a través de TOR, pero no para otros programas (p.e. mensajería instantánea, o ssh). Para ello tendrás que "torificar", es decir, redirigir el tráfico de cada programa a la red Tor.

Instalación en Debian/Ubuntu

Sigue estas [instrucciones](#) detalladamente para instalar TOR en Debian o Ubuntu. No te fies de ninguna otra instalación, configuración o modificación de Tor. A grandes rasgos lo que tienes que hacer es lo siguiente (hazlo siguiendo las instrucciones de torproject.org):

1. Instala Tor habilitando las fuentes (apt-sources) de Ubuntu/Debian específicas para Tor
2. Instala y configura Polipo o Privoxy (te permite redirigir cierto tráfico, p.e. del navegador, por un puerto específico)
3. Instala la extensión de Firefox Torbutton [aquí](#)
4. Comprueba que Tor funciona entrando a la web check.torproject.org

Todo esto te servirá para navegar con Firefox a través de TOR, pero no para otros programas (p.e. mensajería instantánea, o ssh). Para ello tendrás que "torificar", es decir, redirigir el tráfico de cada programa a la red Tor.

Debilidades de la red tor

La función principal de tor es asegurar el anonimato del usuario, pero existen ciertas debilidades de la red

que podrían explotarse para rastrear al usuario.

Un propietario de un servidor de salida podría ver la información que es enviada ya que ahí es donde se descifra, aunque no sería posible saber el origen de la información si que podría conocerse su contenido. Muchas veces se envían cookies que pueden comprometer en anonimato del usuario, y que podrían interceptarse en un servidor de salida.

Ejemplo: hal.inria.fr/inria-00574178/en

Por eso se recomienda cifrar la información enviada (con SSL por ejemplo), desactivar las cookies y los plugins java en el navegador.

I2P

¿Que es?

I2P es una red anónima, que ofrece a las aplicaciones que requieren de protección de identidad una simple capa para la comunicación segura. Todos los datos son cifrados varias veces y la red misma es tanto distribuida como dinámica - sin parte ninguna en la que haya que confiar. I2P esta formada por una serie de nodos(routers) con una serie de encaminadores virtuales(tuneles)

Estos routers se comunican entre si a través de protocolos de red(TCP,UDP,etc..) pasando varios mensajes.Las aplicaciones cliente tienen su propio identificador de cifrado(Destino) que les permite enviar y recibir estos mensajes Estos clientes pueden conectarse a cualquier router y autorizar la asignación temporal de unos túneles que se utilizará para enviar y recibir mensajes a través de la red. I2P tiene su propia base de datos de la red interna usando un algoritmo modificado de Kademlia para la distribución de rutas e información de contacto de forma segura.

Todos los datos son cifrados varias veces y la red misma es tanto distribuida como dinámica - sin parte ninguna en la que haya que confiar, I2P se basa en que los datos se encaminan a través de otros nodos, mezclándose con los flujos de datos de otros usuarios y de esta manera dificultando el rastreo de las diversas comunicaciones y prácticamente imposibilitando que se sepa el origen o el destino de ellos. En este proceso todos los datos están cifrados desde el router proveniente hasta él del destinatario.

La red I2P es una red que esta totalmente separada de la internet normal, por lo tanto I2P tiene sus propias paginas web llamadas eppsites para acceder a ellas hay que estar en la red i2p no son accesibles desde la internet.

¿Como acceder a IRC-P2P?

Hay varios servidores IRC en la redes I2P, entre ellos (irc.postman.i2p,irc.freshcoffee.i2p) Para conectar a I2P solo necesitamos un software y tener java jre 1.5 o superior

- Instalable windows mirror.i2p2.de/i2pinstall_0.8.8.exe
- Instalable (Debian Ubuntu): Buscar paquete I2P en synaptic, apt-get,aptitude.
- Instalable (Otras versiones Linux) mirror.i2p2.d/i2psource_0.8.8.tar.bz2

Bajar instalable y ejecutar los siguientes comandos desde el terminal: tar xjvf i2psource_0.8.8.tar.bz2 ; cd i2p-0.8.8 ; ant pkg

- Instalacion Mac: Despues de bajar el instalable mirror.i2p2.de/i2pinstall_0.8.8.exe.

Ejecutar java -jar i2pinstall_0.8.8.exe desde el terminal.

Iniciando I2P

En todos los sistemas indicados para arrancar I2P solo hay que arrancar la aplicación grafica, pero en sistemas linux si instalas el paquete de la distribucion tendras que arrancarlo desde el terminal puesto que

no tiene aplicacion grafica.

```
/usr/local/i2p/i2prouter start
```

Una vez iniciado I2P solo teneis que que acceder atraves del navegador a la aplicación web desde tu navegador localmente.

localhost:7657

Desde aquí tenemos el panel de control de la configuracion I2P es una configuracion compleja es mejor no tocarla si no sabemos lo que hacemos, para ver si los tuneles de aplicación estan arrancados o si hay problemas poder arrancarlos debemos de acceder a el enlace que indica tunnels

localhost:7657/i2ptunnel

Si queremos conectar a IRC solo tenemos que indicarle al cliente(xchat,mirc,etc..) que la conexión tiene que ser a localhost(127.0.0.1) y puerto 6668.

```
127.0.0.1/6668
```

FoxyProxy

¿Qué es?

Es un complemento para firefox que te permite configurar y utilizar proxies de una manera muy sencilla y rapida.

¿Qué es un proxy?

Un proxy es un "intermediario". Supongamos que tu quieres entrar en google.es, mandas la peticion al proxy, el proxy accede a google.es y te manda la pagina; todo esto de manera automática una vez que el proxy este activado. De este modo la IP que sale reflejada en google.es es la del proxy y no la tuya. **En el caso concreto de FoxyProxy solo anonimiza la información que pasa por el navegador firefox.**

Instalación

Entramos [aquí](#) y pinchamos en "Seguir a la descarga", una vez en la página de descarga pinchamos en "Añadir a firefox".

Utilización

[Aquí](#) tienes una lista de proxies de bastante calidad y regularmente actualizada.

Primer paso, buscar proxies

Entramos en la web que mencioné antes y configuramos los menus despleables de esta manera:

- Type of proxy: Anonymous
- Latency: Less than 1 sec

Esto hará que nos muestre los proxies anonimos que tengan un tiempo de respuesta menor a un segundo.

Segundo paso, añadir el proxy a foxyproxy

En la lista de proxies que nos muestra la web, a la izquierda de cada proxy, hay un icono de un zorro, pinchamos en ese icono y nos saldra un mensaje emergente en firefox preguntandonos si permitimos que esa web cambie la configuración de firefox, le damos a "Allow" o "Permitir".

Tercer paso, comprobar que el proxy funciona

Nada más darle a permitir se nos abrirá una página, esa página nos dirá cual es la IP que estamos usando actualmente. Lo ideal es mirar esa página antes y después de añadir el proxy. Otra opción es hacer este [test](#).

Otra información de interés

Al instalar el complemento y reiniciar firefox saldrá un icono nuevo de un zorro al lado de la barra de direcciones del navegador. Si el zorro esta naranja pero tachado significa que el proxy está desactivado, si esta azul estático es que el proxy esta activado pero sin trafico y si esta azul y en movimiento significa que esta activado y recibiendo o enviando información.

Para más opciones (desactivar el proxy, añadir filtros, etc...) hacer click derecho en el icono del zorro en vuestro firefox. ¡Explorad las opciones y divertios!

JonDonym

¿Qué es?

JonDo (conocido anteriormente comoJAP) es un cliente VPN escrito en Java que enruta los datos a través de la red de JonDo. Lamentablemente, el hecho de estar basado en Java significa que la aplicación está un tanto inflada. Sin embargo, JonDo tiene una interfaz atractiva y fácil de usar, que compensa el abultado consumo de memoria y que muestra un montón de información visual sobre tu conexión a la red JonDo. El estar basado en Java implica que es verdaderamente multi-plataforma. El servicio gratuito ofrece velocidades de entre 30-50 kbit/s y ancho de banda ilimitado. La opción de pago ofrece muchas más opciones, como mayor velocidad, acceso a todos los puertos y soporte para SOCKS5. El grupo JonDonym suministra un perfil gratuito de navegación para Firefox llamadoJonDoFox. Está preconfigurado para colocarse en anonimato alto y destacan sus muchos extras, como No-Script, CS Lite y AdBlock Plus.

Configuración y Uso

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

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

Una vez que se haya completado, JonDo nos pide que comprobemos la configuración. En el panel de control, cambiamos el valor de Anonymity a Off y luego intentamos abrir un sitio web con el navegador que acabamos de configurar. Si JonDo nos muestra una advertencia y tenemos que seleccionar "Yes" para ver el sitio Web, todo ha sido configurado correctamente y podemos seleccionar "The warning is shown. Websurfing is possible after confirmation". Si alguna otra descripción aplica para nuestro caso, la seleccionamos y el asistente de instalación nos dará más información sobre cómo resolver el problema.

Ahora el segundo paso para asegurar una configuración adecuada: Cambiamos el valor Anonymity a "On" en el panel de control y abrimos un sitio Web al azar con el navegador que hemos configurado. Si se carga el sitio Web, todo está bien y podemos hacer clic en "Connection established, websurfing is fine" Si alguna otra descripción aplica para nuestro caso, la seleccionamos y el asistente de instalación nos dará más información sobre cómo resolver el problema.

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

Si los servidores estándares JonDo ya están bloqueados en nuestro país, debemos probar la opción de anti -

censura. Hacemos clic en “Config” en el panel de control y seleccionamos la pestaña Network. Hacemos clic en “Connect to other JAP/JonDo users in order to reach the anonymization service”. Leemos la advertencia y confirmamos haciendo clic en “Yes”.

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

Podemos descargar la herramienta JonDoFox en la dirección anonymous-proxy-servers.net/en/jondofox...

Freenet

¿Qué es?

Freenet es software libre el cual te permite compartir archivos anónimamente, navegar y publicar “freesites” (sitios web accesible solamente mediante Freenet) y discutir en foros, sin temor de censura. Freenet es descentralizada para hacerla menos vulnerable a ataques, y si es usada en modo “darknet”, dónde los usuarios conectan solamente con sus, es muy difícil de detectar.

Las comunicaciones por los nodos Freenet están cifradas y son dirigidas a través de otros nodos para hacer extremadamente difícil de determinar quién está solicitando la información y cual es su contenido.

Los usuarios contribuyen a la red proporcionando ancho de banda y una porción de su disco rígido (llamado el “almacén de datos”) para almacenar archivos. Los archivos son automáticamente mantenidos o borrados dependiendo de cuán populares son, con los menos populares siendo descartados para hacer lugar para contenidos nuevos o más populares. Los archivos están cifrados, así generalmente el usuario no puede descubrir fácilmente qué hay en su almacén de datos, y no puede ser responsable de ellos. Foros, Sitios web y funcionalidades de búsqueda, son todas construidas sobre este almacén de datos.

Configuración en Linux

Es necesario tener instalada la máquina virtual de Java, se recomienda como mínimo la versión 6.0 del JDK.

Descargar el software que realizará los pasos de instalación, para ello ir a freenet.googlecode.com/files/new_instal... una vez descargado, ejecutar el fichero JAR.

```
>java -jar new_installer_offline_1405.jar
```

Con esto se abrirá un asistente en el que se debe seleccionar el lenguaje de instalación, la ruta donde se deben ubicar los ficheros de instalación y finalmente si se desean crear iconos en el menú de inicio.

NOTA: No se debe intentar ejecutar el instalador como usuario ROOT ya que el script de inicio tiene un filtro para evitar que se utilice dicho usuario para iniciar el proceso con sus privilegios.

Una vez ingresados todos los campos anteriores, el asistente stand-alone se cerrará y posteriormente se abrirá un asistente en el navegador por defecto del usuario, apuntando a 127.0.0.1:8888/wizard en dicho asistente se solicitará en primera instancia el nivel de seguridad que se quiere utilizar para la instalación, habiendo 3 niveles **LOW, HIGH y CUSTOM**.

En el caso de que se seleccione LOW, se asume que el uso de FreeNet es permitido en el país donde se encuentra ejecutándose y deja el nodo abierto a que cualquier participante en la red de FreeNet pueda contactar y establecer conexiones. HIGH indica que nadie puede realizar conexiones a este nodo a excepción de los “Friends”, esto permite crear una “Darknet” tal como se ha explicado en líneas anteriores, CUSTOM indica un control más fino permitiendo al usuario definir sus propias políticas de relacionadas con la privacidad. Se aconseja seleccionar la opción CUSTOM.

Una vez seleccionado el modo de instalación, la primera interfaz advierte que se debe utilizar un navegador distinto del que se utiliza habitualmente para utilizar FreeNet, esta recomendación ya se ha indicado anteriormente con I2P y TOR, aquí vuelve a cobrar sentido, ya que un sitio web en internet podría atacar a un usuario buscando en el historial del navegador y revelando de esta forma, FreeSites a los que ha

accedido un usuario en la red FreeNet y atentar contra su anonimato y privacidad.

En los siguientes pasos del asistente se debe seleccionar la opción de habilitar la interfaz UPnP, seleccionar si se desea actualizar FreeNet automáticamente cuando exista una nueva versión y definir si se desea conectar solamente con amigos o permitir también extraños, con sus correspondientes ventajas y desventajas.

En caso de seleccionar la opción de solo amigos se puede seleccionar el nivel de protección contra extraños ALTO o MAXIMO, en el caso de seleccionar la opción de Conectarse con extraños se pueden seleccionar los niveles de protección MEDIO o BAJO.

NOTA: Posiblemente para un primer uso de FreeNet sea prudente utilizar el perfil de conexión con extraños para poder explorar la red y sus servicios sin problemas, dado que para poder utilizar el perfil de conectarse solo con amigos y crear un DarkNet es necesario tener como mínimo a 5 participantes.

Posteriormente se debe seleccionar el tipo de seguridad física del ordenador, de los niveles que aparecen en este paso del asistente se recomienda utilizar un nivel ALTO o MAXIMO.

El siguiente paso del asistente solicita el tamaño que tendrá el "Data Store" de este nodo, entre más espacio se dedique, más se beneficia la red de FreeNet y será más óptimo el funcionamiento de este nodo.

El siguiente paso se relaciona con el ancho de banda que se desea dedicar para FreeNet, se recomienda aproximadamente la mitad sobre el límite que establece el ISP del usuario.

Una vez completados estos pasos, se puede apreciar en el navegador la interfaz principal de FProxy, con todas las opciones que se encuentran disponibles en la instancia de FreeNet recién instalada. En concreto en dicha interfaz se encuentran las siguientes opciones:

Browsing: Permite interactuar con la red de FreeNet realizando búsquedas de FreeSites publicados por otros usuarios, subir un FreeSite a la red y ver directorios de sitios web en FreeNet.

FileSharing: Como su nombre lo indica permite compartir archivos en la red de FreeNet

Friends: Permite ver los amigos que se encuentran agregados al nodo y adicionar nuevos.

Discussion: Para utilizar el foro de FreeNet y participar en las discusiones relacionadas con la red.

Status: Avisos sobre eventos relacionados con el Nodo.

Configuration: Permite modificar opciones de configuración básicas y avanzadas en el nodo

Key Utils: Utilidades disponibles en el nodo para el tratamiento de claves.

CREACIÓN DELSERVICIOFREENET

Ahora, se recomienda establecer FreeNet como servicio, los siguientes pasos se han seguido utilizando Debian Squeeze, no obstante sirven del mismo modo para cualquier otra distribución basada en Debian.

Se recomienda crear un usuario con el comando "adduser" no obstante puede utilizarse el mismo que se ha utilizado para instalar FreeNet. Establecer los permisos adecuados al directorio de instalación de FreeNet

```
>chown -R adastra /opt/Freenet/
```

Crear los enlaces simbólicos y posteriormente adicionarlos al script de inicio.

```
>ln -s /opt/Freenet/run.sh /etc/init.d/freenet>update-rc.d freenet defaults
```

Posteriormente es necesario editar el script de arranque de FreeNet run.sh que se encuentra ubicado en el directorio de instalación. El objetivo es simplemente arrancar el servicio con el usuario anteriormente creado, para ello se debe editar la siguiente línea

```
RUN_AS_USER=
```

Y cambiarla por esto (evidentemente, especificar el usuario correcto):

RUN_AS_USER=adastra

Posteriormente es posible iniciar FreeNet como cualquier servicio en Debian ubicado en /etc/init.d del siguiente modo

>/etc/init.d/freenet stop>/etc/init.d/freenet start>/etc/init.d/freenet restart

Descarga

- freenetproject.org/download.html

Fuentes

- wiki.hacktivistas.net/index.php?title=T...
- wiki.hacktivistas.net/index.php?title=Manual_anticensura:_Tor
- www.teayudo.es/cambiar-los-servidores-d...
- www.elgrupoinformatico.com/cambiar-dns-...
- ericlinux.blogspot.com/2008/02/cambiar-...