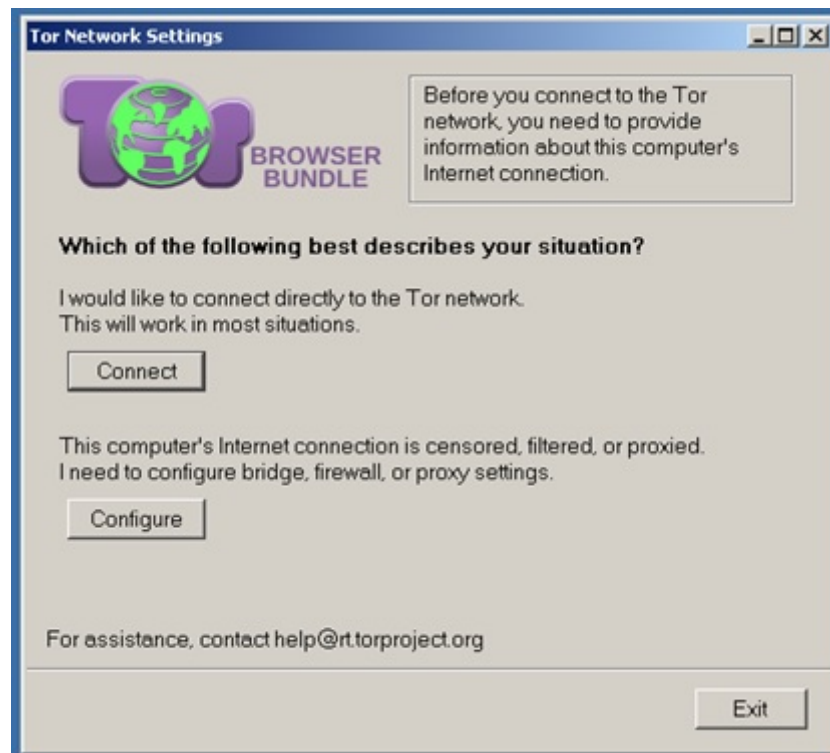


Cuando utilizas Internet gran parte de la información que recibes y transmites es registrada. Incluso si utilizas un navegador en modo privado o cifras tu información, es posible conocer lo que realizas en la red.

En este sentido, la navegación anónima es útil para evitar el seguimiento de sitios web que buscan conocer tus hábitos y preferencias, utilizar servicios que han sido restringidos en tu país o mantener el anonimato en comunicaciones que resulten sensibles. Combinado con otras conductas, es posible evitar que tu información sea registrada por terceros.

Un servicio que permite anonimizar tus actividades es Tor (The Onion Router), un software libre que junto con una red de computadoras voluntarias oculta tu dirección IP (número que identifica tu máquina en la red) y asigna otra de cualquier parte del mundo. A pesar de que la información no es un secreto, tampoco es asunto de otras personas.

En este post explicamos cómo utilizar la herramienta en un sistema Windows. Para comenzar, descarga Tor (preferentemente del sitio oficial). La manera más sencilla de comenzar es con el navegador preconfigurado, a través del paquete Tor Browser Bundle. La instalación crea una carpeta que incluye la aplicación Start Tor Browser, la cual debes ejecutar. Cuentas con dos opciones: conectarte de manera directa a la red de Tor o configurar la aplicación en el caso de que exista alguna restricción en tu red.



La primera opción (*Connect*) ejecuta el navegador, a partir de lo cual ya puedes comenzar a navegar de forma anónima en la red.



De manera aleatoria se asigna una dirección IP a tu conexión, que geográficamente se encuentra en otro lugar. Este cambio permite ocultar tu ubicación física, para verificarlo puedes hacer uso de los servicios que te permiten conocer la dirección IP con la que navegas.

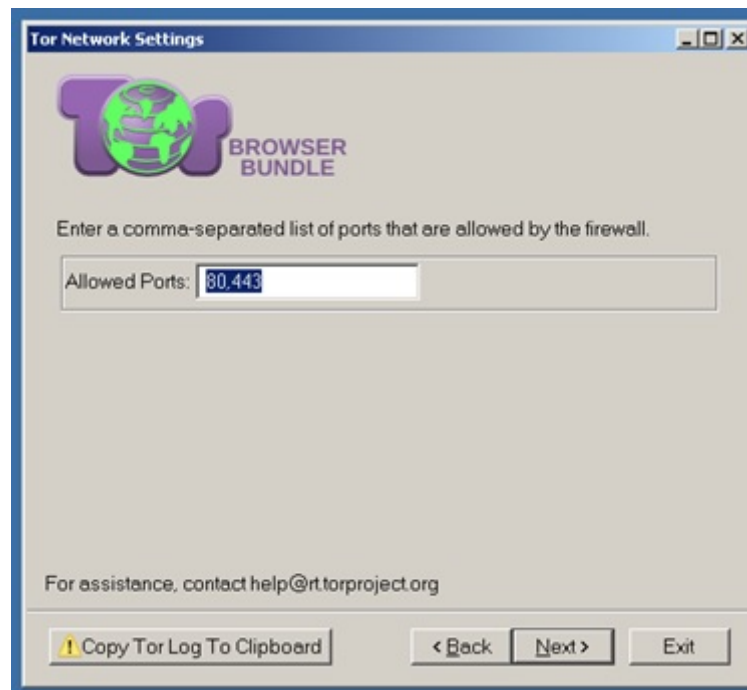
Con la segunda opción (*Configure*), puedes configurar la herramienta para tres casos: si utilizas un *proxy*, si estás protegido por un *firewall* o si el Proveedor de Servicios de Internet (ISP por sus siglas en inglés) bloquea las conexiones de Tor.

Para el primer caso se debe proporcionar el tipo de *proxy*, dirección IP y puerto. Si es requerido por el servidor, debes introducir el nombre de usuario y la

contraseña.



En el segundo caso, si la navegación que realizas está protegida por un *firewall* (de red o *host*), es necesario indicar los puertos permitidos para los servicios *web*.



Para el tercer caso, puedes configurar *bridges* si algún ISP bloquea las conexiones de Tor para tener el control sobre las comunicaciones.

¿Pero qué es un *bridge*? Para funcionar, Tor hace uso de una red de computadoras a través de las cuales redirecciona el tráfico antes de mostrar la dirección IP modificada. Dicho tráfico debe pasar por al menos tres computadoras (o nodos) previo a su destino.

El ISP puede bloquear los nodos que son conocidos, por esta razón, la configuración del *bridge* consiste en incluir un nodo que no es conocido públicamente y por lo tanto no puede ser bloqueado:



Con esta guía básica podrás comenzar a navegar de manera anónima en Internet. Si deseas conocer más, en publicaciones posteriores mostraremos configuraciones avanzadas de Tor.

¿Entonces además de TOR disponemos de otras alternativas para la navegación privada? Tajantemente si, existen otras distribuciones en forma de sistema operativo independiente que hacen lo mismo que TOR que solo es un programa, entre ellas podemos destacar Tails y Liberte como las más destacadas, pero existen además otras distribuciones linux de anonimizaje como Mythbuntu y Elive.