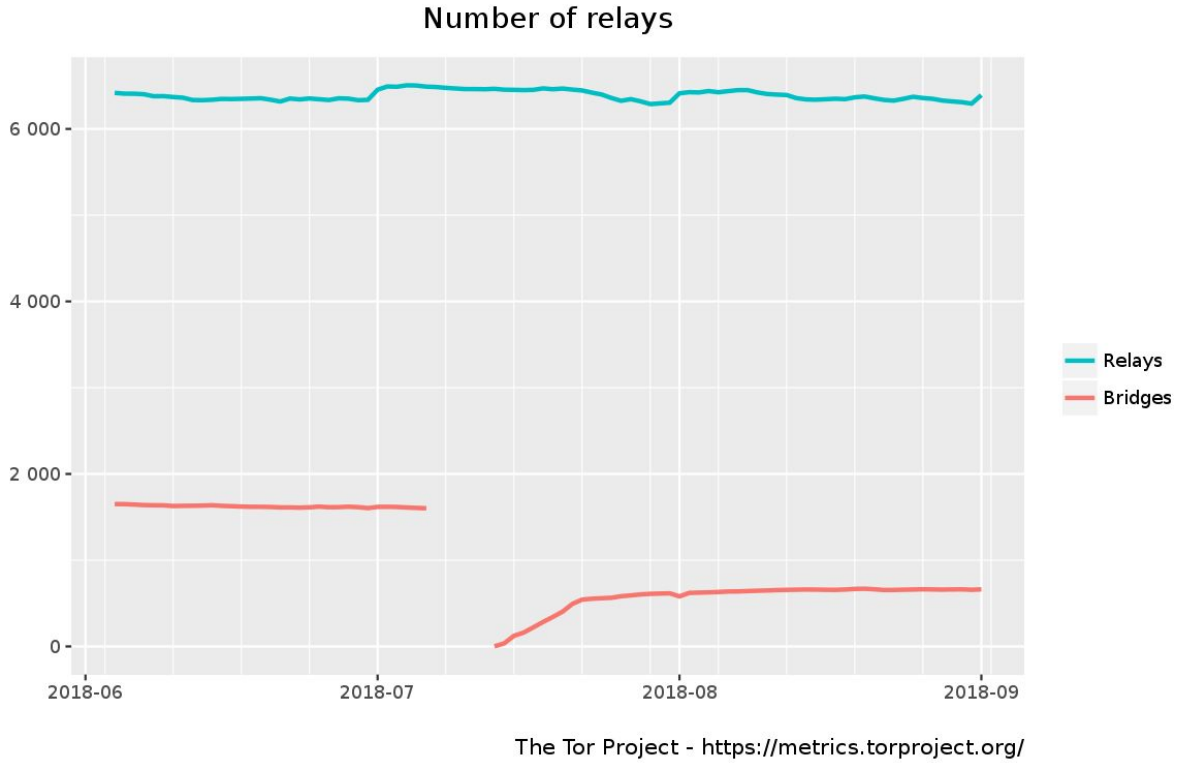
TOR

The Onion Router

¿Qué es TOR?

- “Circuit-based low-latency anonymous communication service” (Paper oficial).
- La red Tor está compuesta por un grupo de **servidores voluntarios** que permite a las personas mejorar su **privacidad** y **seguridad** en internet.
- Usuarios de Tor usan esta red a través de una serie de túneles virtuales, en vez de hacer una conexión directa.

Cantidad de voluntarios



¿Por qué necesitaría Tor?

- Porque protege contra el “**traffic analysis**”.
- Permite saber quién está hablando con quién.
- Otros pueden saber tus hábitos e intereses.
- Incluso podría saber qué mensaje estás enviando analizando el source, destination, size, timing, etc. del **header**.

The anonymous Internet

Daily Tor users per 100,000 Internet users

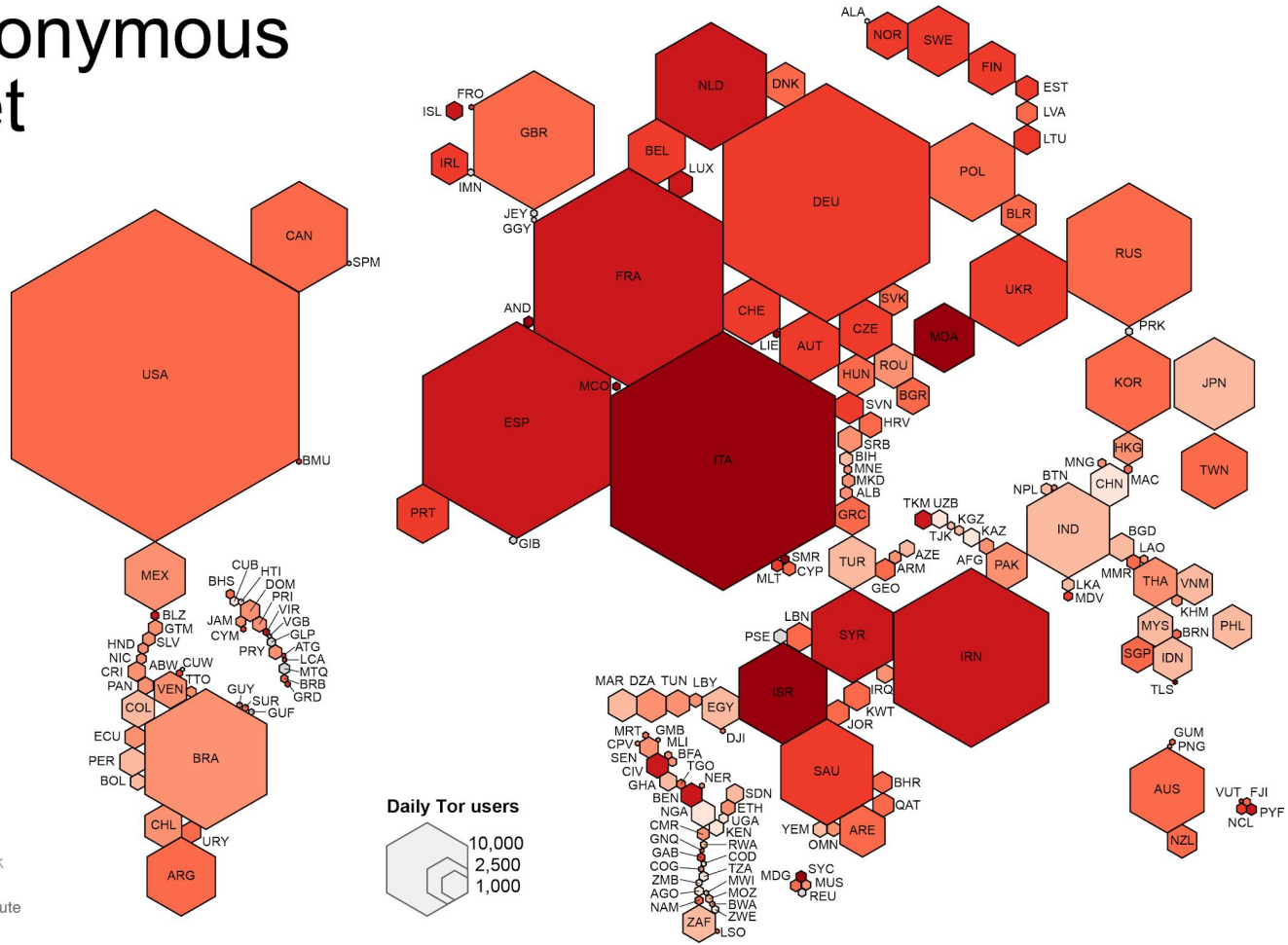
- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

oiioiioii
oiioiioii
oiioiioii
Oxford Internet Institute
University of Oxford

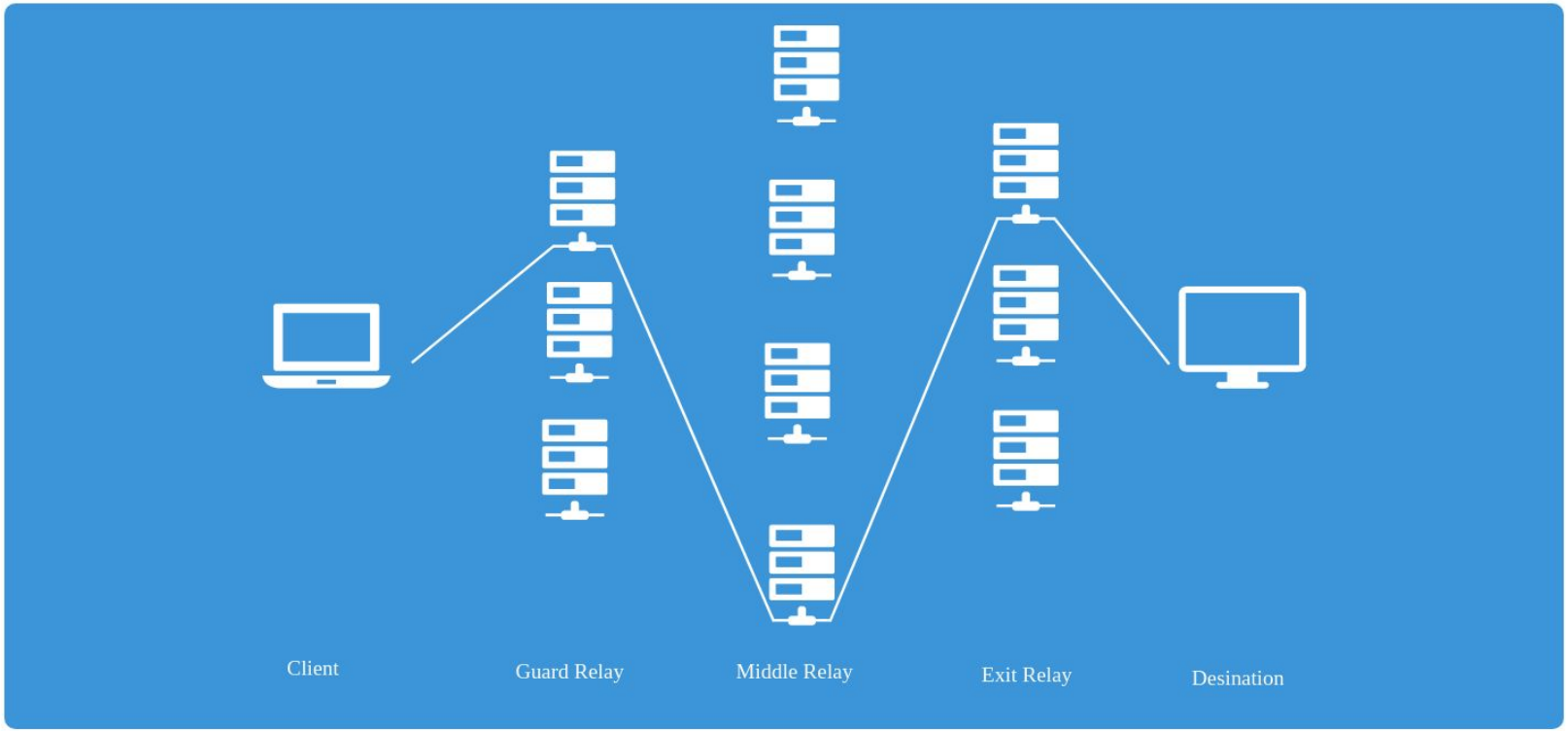


¿Cómo puedo acceder a la red Tor?

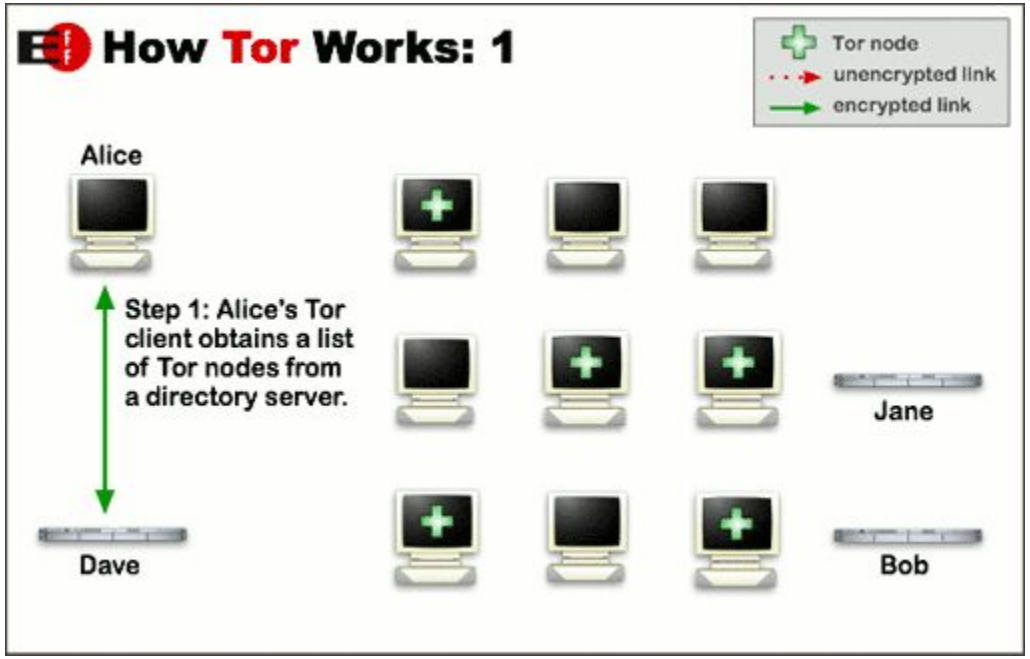
- Tor Browser.
- Versión modificada de Mozilla Firefox ESR.
- NoScript.
- HTTPS Everywhere.

¿Qué pasa cuando entro a una página a través de Tor Browser?

Funcionamiento

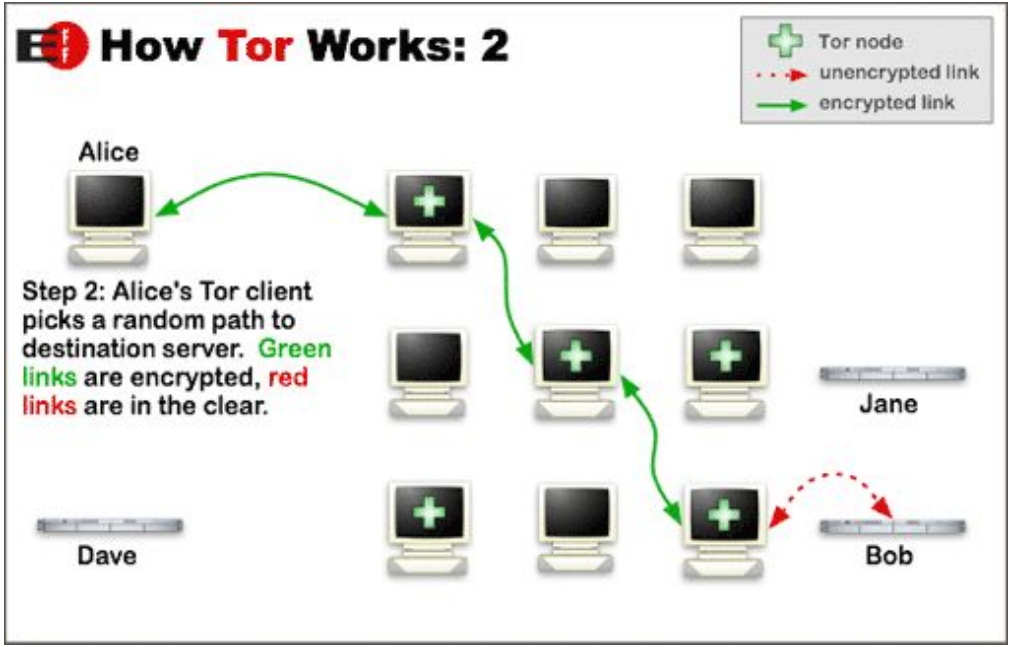


Funcionamiento

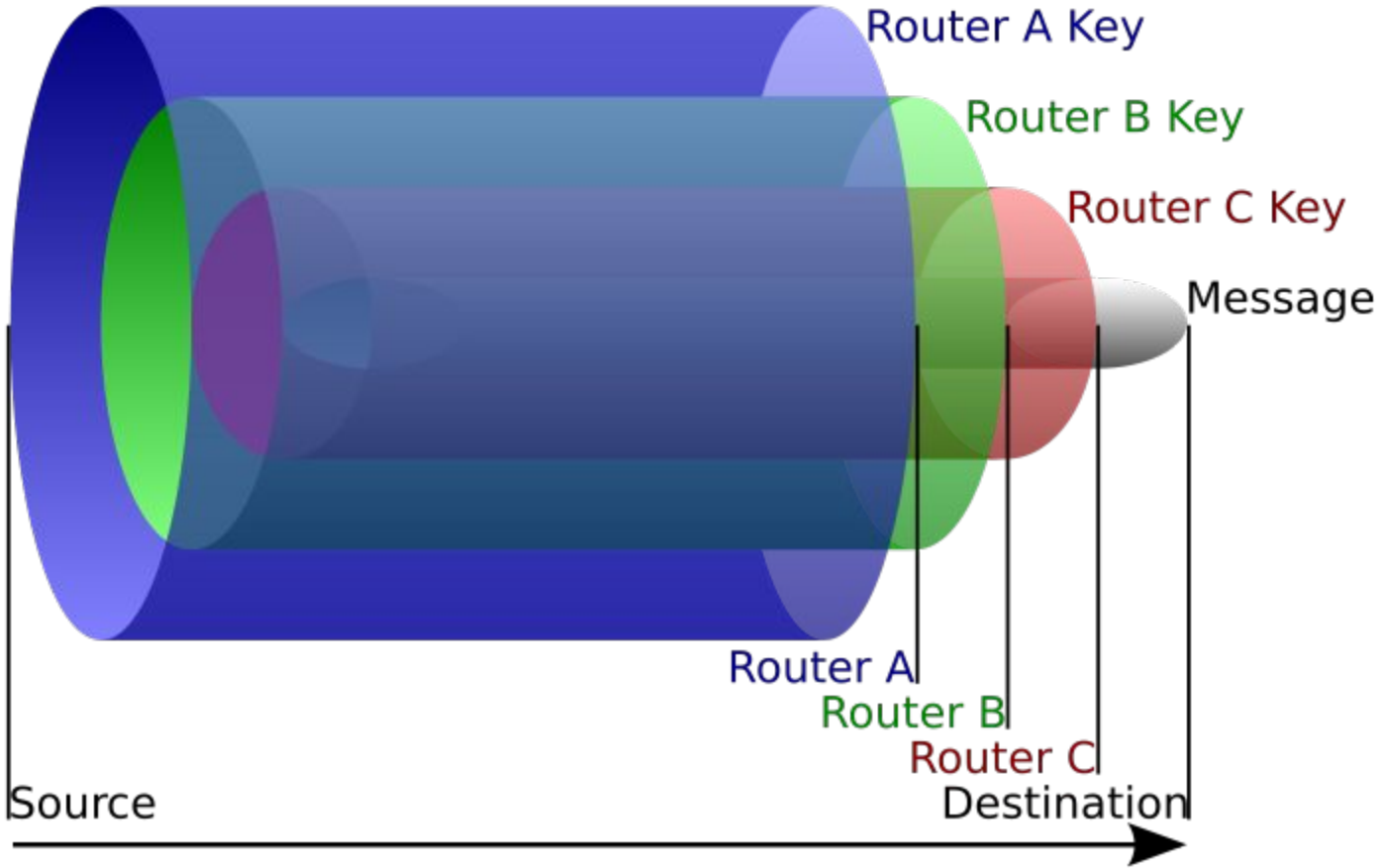


Fuente: https://www.torproject.org/about/overview.html.en

Funcionamiento

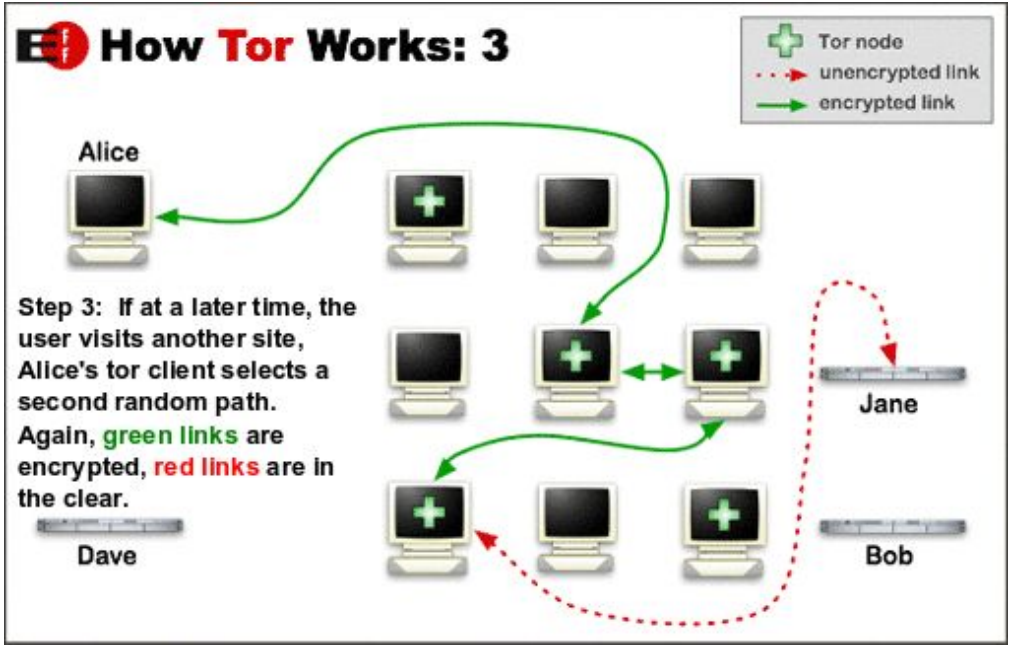


Fuente: https://www.torproject.org/about/overview.html.en



Fuente: http://openxarxes.com/tor-raspberry-pi-3-onion-pi/

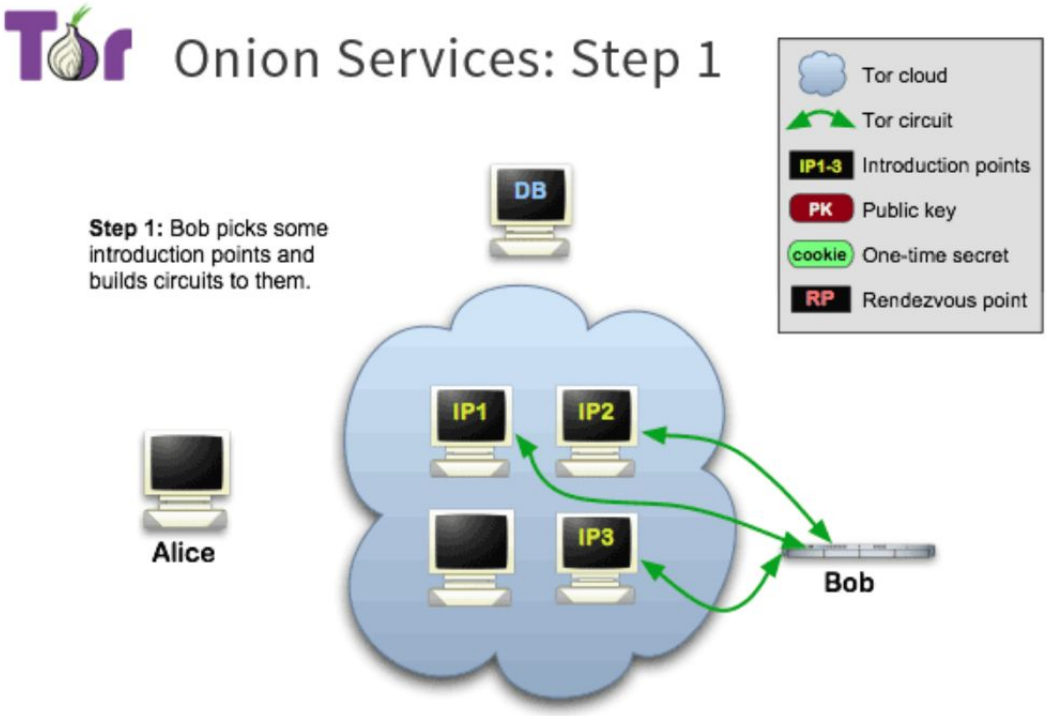
Funcionamiento



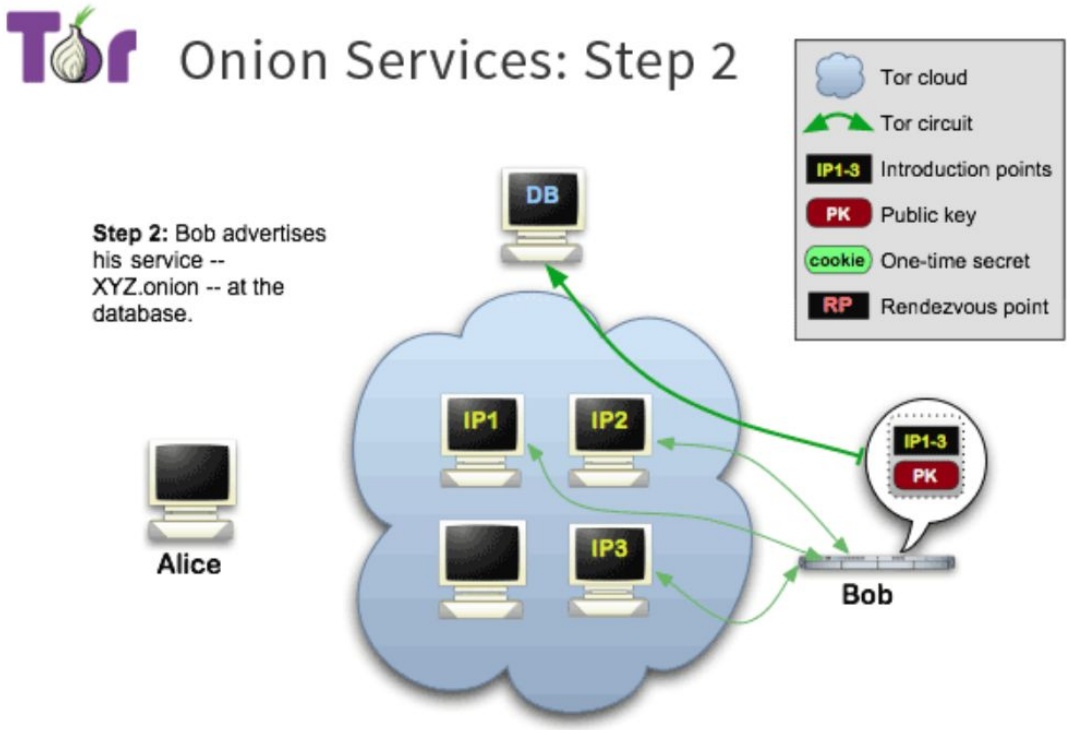
Fuente: https://www.torproject.org/about/overview.html.en

¿Cómo lo hace Tor para que un servidor pueda ofrecer un servicio sin revelar su IP?

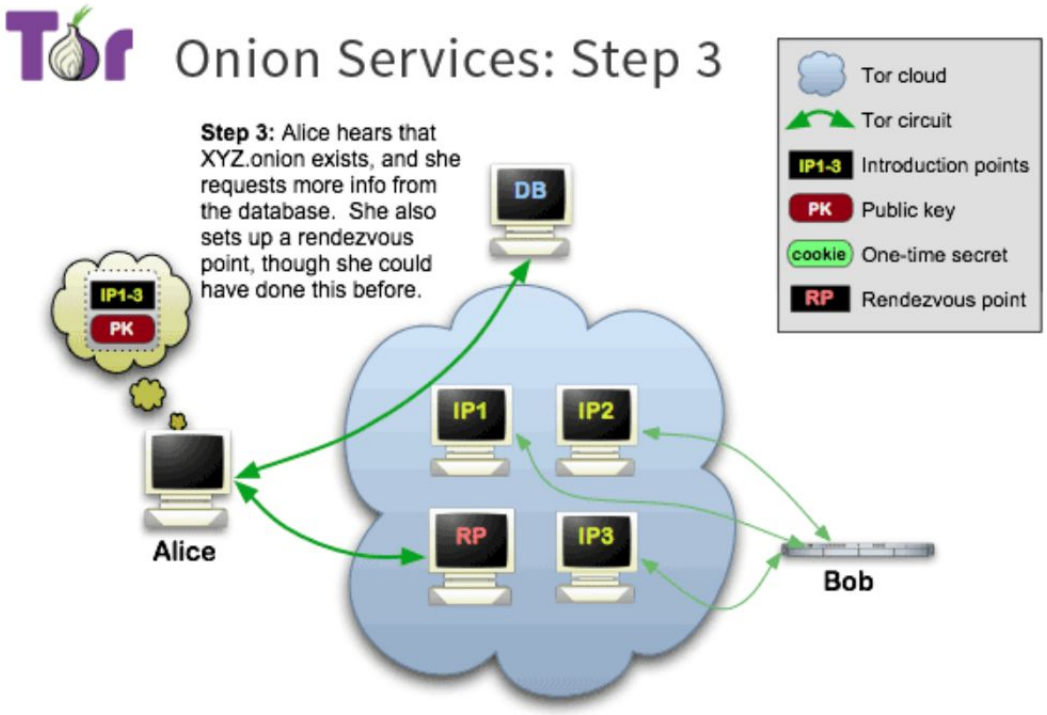
Funcionamiento



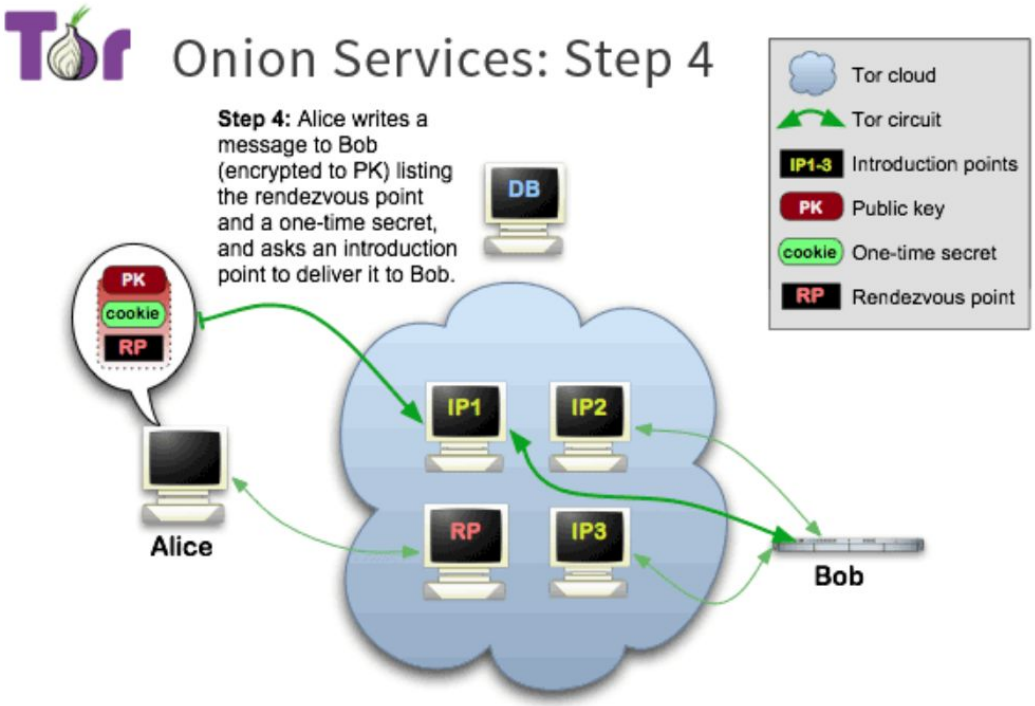
Funcionamiento



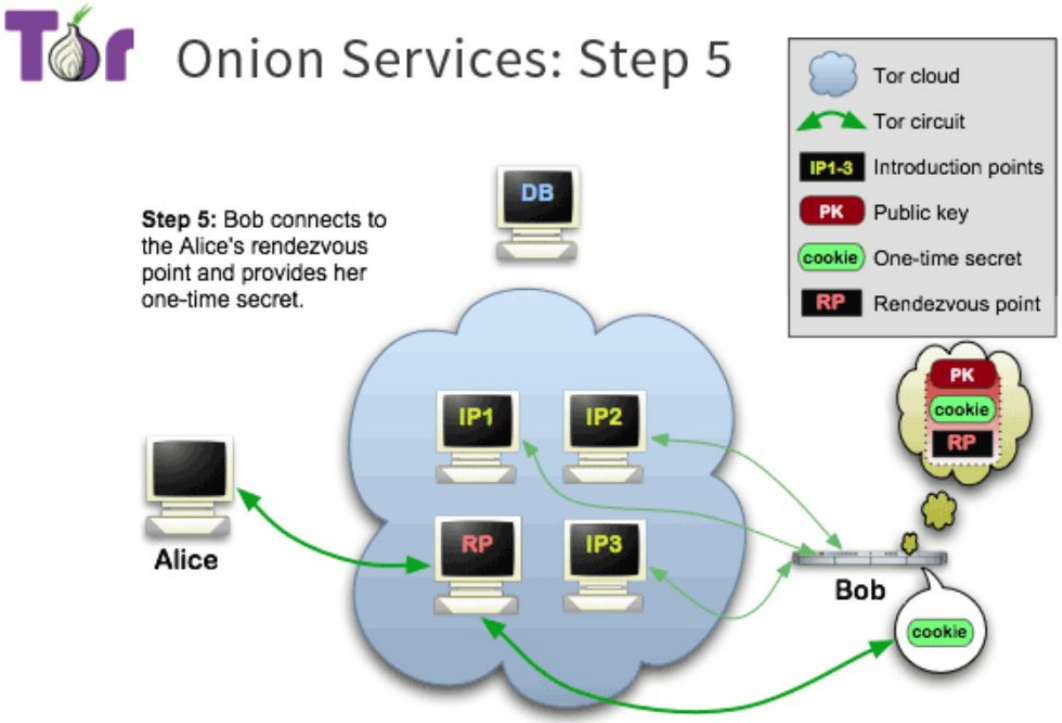
Funcionamiento



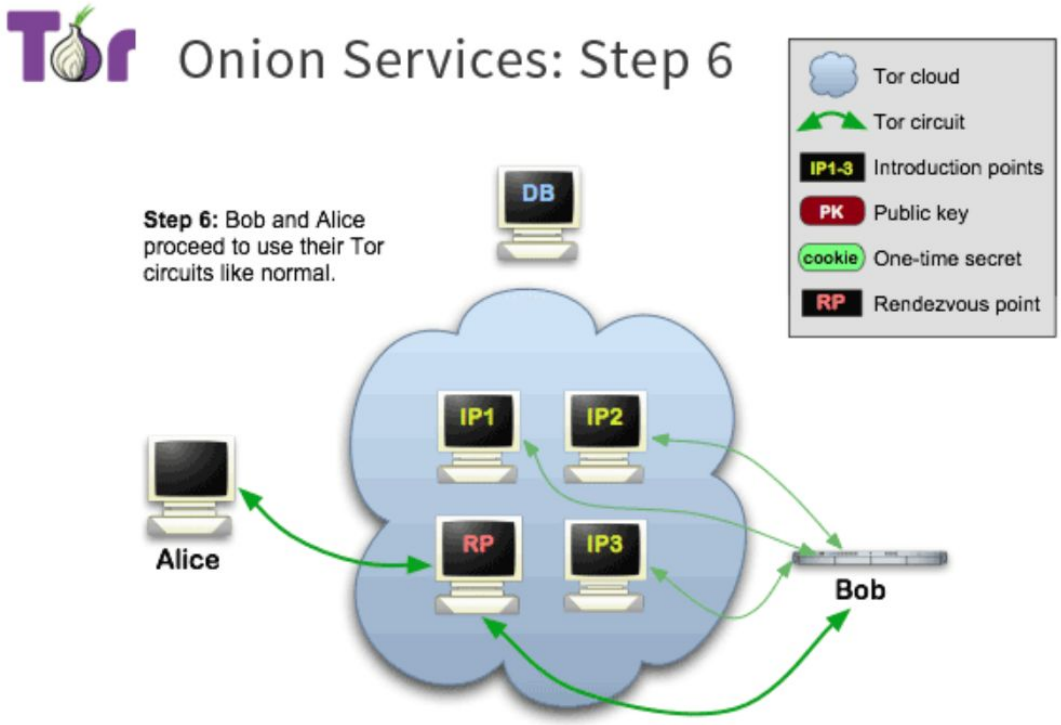
Funcionamiento



Funcionamiento



Funcionamiento



Bloqueo de relays y tráfico

- **ISP’s bloquean Guard Nodes.**

  Bridges relays son relays de Tor que no están en las listas públicas de relays.

- **ISP’s podrían detectar tráfico de Tor** a través de instrumentos especiales que vigilan el tráfico en la red.

  Pluggable transports transforman el tráfico de Tor entre el cliente y el bridge en uno que parezca normal (protocolo).

Algunas vulnerabilidades

- **DoS non-observed nodes**: un observador, que solo puede ver ciertos nodos de la red Tor, aumenta el tráfico de aquellos nodos que no puede ver para apagarlos y reducir su confiabilidad.
- **Run a hostile OR:** si un adversario tiene varios nodos comprometidos y logra que el directorio de nodos los considere confiables, un circuito podría elegir uno de esos nodos como entrada y otro como salida.
- **End-to-end timing/size correlation.**

Referencias

- https://www.torproject.org/about/overview.html.en
- https://jordan-wright.com/blog/2015/02/28/how-tor-works-part-one/
- https://www.torproject.org/docs/onion-services
- https://en.wikipedia.org/wiki/Tor_(anonymity_network)#Implementations
- https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf (paper original)