DNS

Evitar la censura mediante el bloqueo de los DNS

Una práctica que se ha utilizado en varias situaciones es la censura por parte de los gobiernos mediante el bloqueo de los DNS. Esto se ha registrado en la primavera Árabe y en Venezuela, solo por citar dos ejemplos.

Existen varios DNS "abiertos" disponibles para evitar la censura que un gobierno puede hacer bloqueando este servicio. Los más conocidos son el de google, 8.8.8.8 (anycast), OpenDNS https://www.opennic.org (Cisco) y los que mantiene OpenNicProyect, https://www.opennic.org

Se propone brindar una alternativa más robusta, que permita seleccionar de manera automática un DNS "Libre" y "Seguro", como los de OpenNicProyect (es decir, que no corresponda a una empresa, como el caso google y OpenDNS que puedan registrar las consultas).

La idea es registrar un DNS en una dirección anycast y permitir agregar servidores que quieran "sumarse" al proyecto, siguiendo el modelo del F root server , https://www.isc.org/f-root

Estos DNS que se "integren" al proyecto deberan ser de instituciones con amplia trayectoria en la defenza de las libertades de los usuarios, lo que garantizará su correcto funcionamiento y que no esté registrando ninguna actividad de los usuarios.

Recientemente NIC Argentina y RIU implementaron una red anycast

Se muestra el gráfico del desarrollo

Para mostrar como los ISPs bloquean ciertos dominios, muestro que Arnet no permite resolver el dominio de Bahía Pirata, https://thepiratebay.org

```
newen ~  dig thepiratebay.org

; <<>> DiG 9.10.3-P4-Debian <<>> thepiratebay.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 15123
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

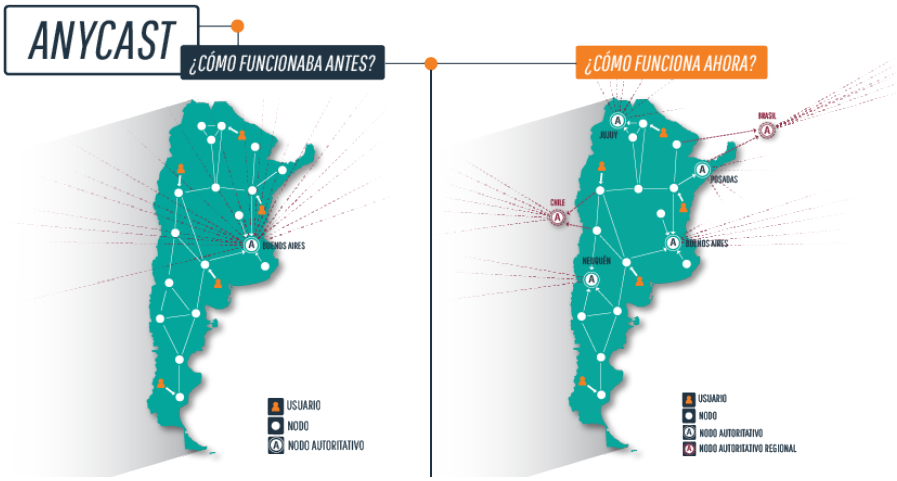

Figure 1: red anycast

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;thepiratebay.org.      IN   A

;; Query time: 39 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sun Oct 29 21:53:32 -03 2017
;; MSG SIZE  rcvd: 45
```

Breve resumen del modo de trabajo

El usuario final (o una app) solo va a definir una única dirección de DNS. Como lo que está haciendo es configurar un poll de servidores. en el supuesto caso de una censura, el mismo protocolo anycast es el encargado de seleccionar otro servidor. Es importante, para que el sistema tenga una verdadera utilidad, realizar las acciones de promoción necesarias con el objetivo de aumentar la cantidad de servidores (instituciones que confíen y apoyen la idea).

Ampliar la red Tor en el país.

Para mejorar la infraestructura de la red Tor en el país se propone la instalación de nodos de salida Tor en los distintos NAPs de CABASE.

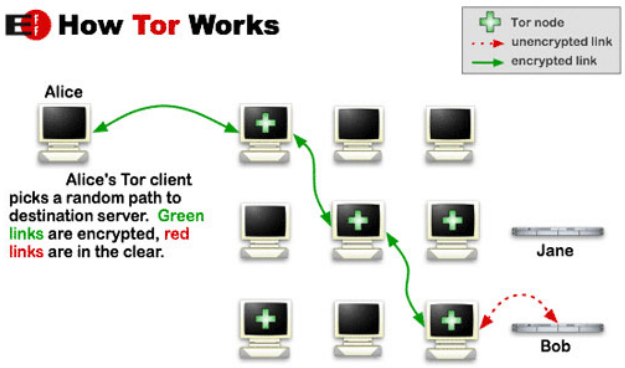

Figure 2: Tor

Recientemente un activista de los derechos de la sociedad civil ha sufrido graves problemas con la justicia Argentina debido a la instalación y configuración de un nodo de salida a la red Tor en su domicilio, con idea de fortalecer la infraestructura de la red Tor en el país. Con este antecedentes, se propone la instalación de nodos de salida de la red Tor en los NAPs de CABASE.

Ref

¿Cómo funciona la red Anycast de Argentina?

Google DNS: Figuring out which DNS Cluster you are using

TOR Exit Nodes en la justicia Argentina

documento en formato pdf