ESNI:«Encrypted Server Name Indication»

SNI permite que un servidor web que aloja varios dominios el entregar el certificado digital correcto a fin de lograr una conexión segura (HTTPS). Bajo HTTPS todo viaja de forma cifrada **excepto el SNI**, con tal propósito fue creado el protocolo **ESNI.**

Actualizado el sábado 6 de marzo de 2021.

Mozilla Firefox

> Mozilla Firefox dejó de ofrecer ESNI desde la versión 85
>
> https://www.ghacks.net/2021/02/24/the-case-of-the-missing-esni-support-in-firefox-85/

Por mucho nuestro navegador web favorito es Mozilla Firefox, a pesar de todos sus detractores. Desde 2018 este navegador ofrece soporte para ESNI pero ¿Qué motivó tal cambio? Desde hace mucho tiempo (15 años a la fecha) se tiene como «excepción consciente» de esa debilidad, la cual permite a muchos proveedores de internet tanto el rastreo de nuestro historial de navegación como también la censura o bloqueo a ciertos dominios o direcciones IP.

La gota que derramó el vaso fue la voluntad de la empresa **Cloudflare** (la cual alberga una muy gran cantidad -demasiados, digo yo- de sitios web, así como sus respectivos CDN) de apoyar esta tecnología, así como el apoyo de los DNS seguros de varias maneras (esto último da para una entrada aparte completa).

Una explicación en detalle del asunto, en idioma inglés, podremos leerlo en la página web de la *Electronic Frontier Foundation*, en esta entrada explicaremos como habilitarlo para Firefox.

La versión última de Mozilla Firefox que soportó ESNI fue la versión 84. Para GNU/Linux existen muchísimos repositorios históricos, sin embargo para Microsoft Windows puede ser tedioso buscar esta versión. Ofrecemos estos enlaces directos (en idioma inglés) del CDN de la Fundación Mozilla, en 32 y 65 bits respectivamente:

```
https://download-installer.cdn.mozilla.net/pub/firefox/releases/84.0.1/win32/en-US/Firefox%20Setup%2084.0.1.exe

https://download-installer.cdn.mozilla.net/pub/firefox/releases/84.0.1/win64/en-US/Firefox%20Setup%2084.0.1.exe
```

Configuración de Mozilla Firefox

Para este nuestro navegador preferido lo debemos configurar de la siguiente manera:

DNS over HTTPS (DoH) protocol

Este protocolo permitirá que hagamos nuestras consultas sin que nadie en el medio que de manera involuntaria *o de manera aviesa* conozca y sepa de nuestros movimientos.

Para ello debemos escribir en la barra de direcciones:

```
about:config
```

Aceptamos la responsabilidad de que sabemos lo que estamos haciendo y buscamos la siguiente clave:

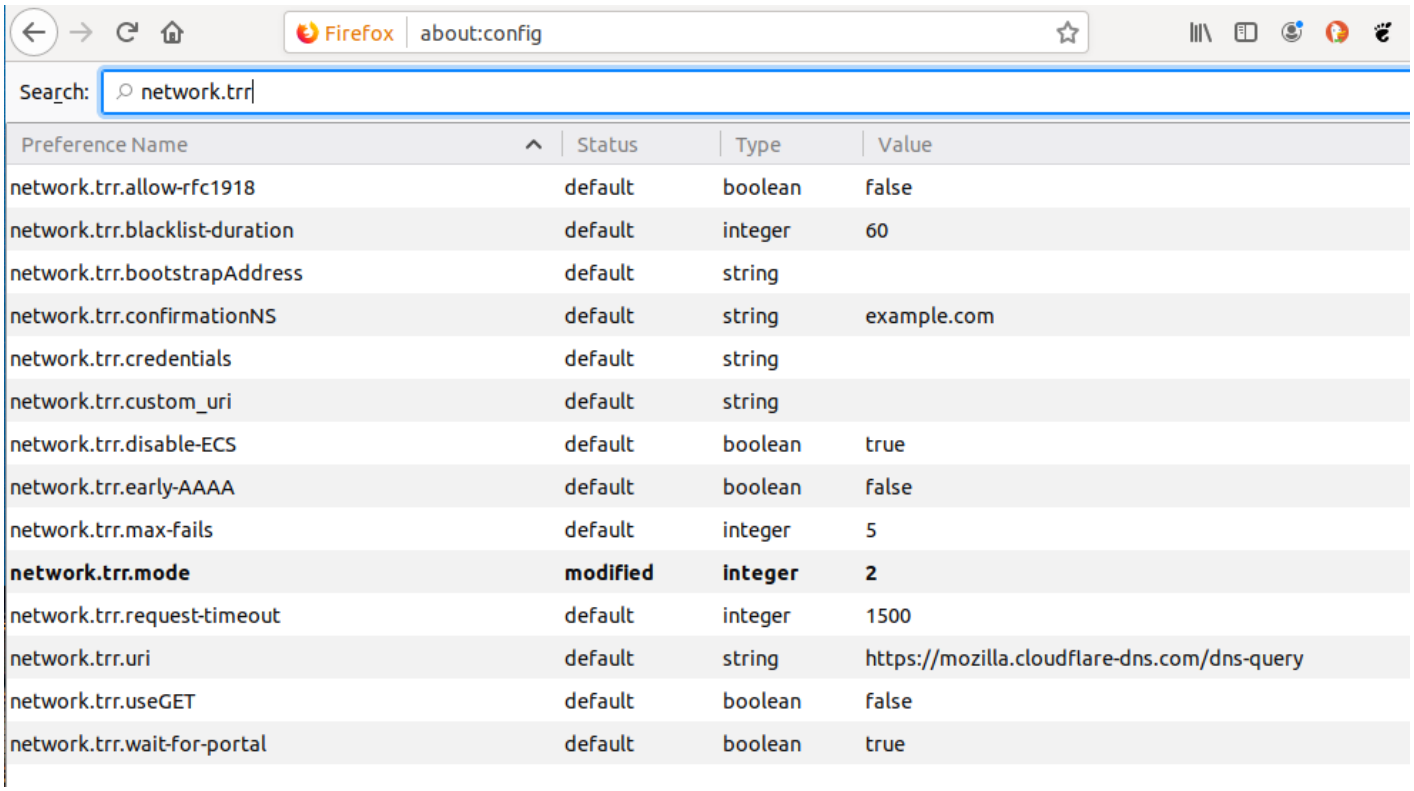
```
network.trr
```

Aparecerán varias opciones pero la que primero nos interesa es la siguiente (cambiaremos su valor a 2):

```
network.trr.mode = 2
```

Esto intentará usar de manera predeterminada el DoH pero hace una excepción para los sitios que necesiten conectarse como portales cautivos.

Debemos notar que Firefox trae su propia dirección DoH y cuando queramos lo podremos cambiar a voluntad, miremos las otras claves en la siguiente imagen:



Preference Name	Status	Type	Value
network.trr.allow-rfc1918	default	boolean	false
network.trr.blacklist-duration	default	integer	60
network.trr.bootstrapAddress	default	string	
network.trr.confirmationNS	default	string	example.com
network.trr.credentials	default	string	
network.trr.custom_uri	default	string	
network.trr.disable-ECS	default	boolean	true
network.trr.early-AAAA	default	boolean	false
network.trr.max-fails	default	integer	5
network.trr.mode	**modified**	**integer**	**2**
network.trr.request-timeout	default	integer	1500
network.trr.uri	default	string	https://mozilla.cloudflare-dns.com/dns-query
network.trr.useGET	default	boolean	false
network.trr.wait-for-portal	default	boolean	true

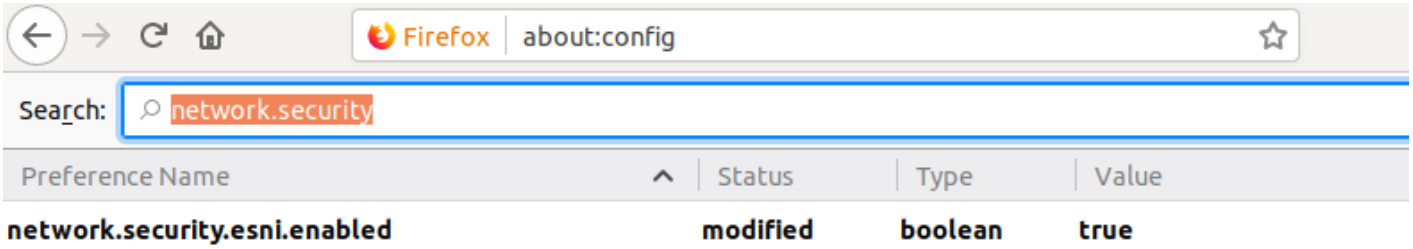
about:config (búsqueda de la palabra clave network.trr)

Configurando ESNI

Lo siguiente será buscar la siguiente palabra clave:

`network.security.esni.enabled`

Y cambiar su valor a **verdadero *(true)***, seleccionando con el ratón y haciendo doble clic o presionando la tecla Intro.



about:config (palabra clave network.security)

Verificando DoH

Actualizado el sábado 7 de septiembre de 2019

Una manera de ver en tiempo real si los sitios web que estamos navegando, en la barra de direcciones metemos:

```
about:networking#dns
```

Marcamos la opción de refrescar cada tres segundos y navegamos de manera normal:

Configurando DNS

Configurar el ESNI fue de lo más sencillo: ahora que estamos entusiasmados y entusiasmadas pueden continuar con el cambio de DNS en nuestro anterior artículo (recomendamos a Cloudflare: 1.1.1.1 y 1.0.0.1).

¿Qué más nos hace falta?

¡Eso sería todo para Mozilla Firefox! ***¿Cómo lo comprobamos?*** Por ahora Cloudflare tiene una página especialmente dedicada para ello:

https://www.cloudflare.com/ssl/encrypted-sni/

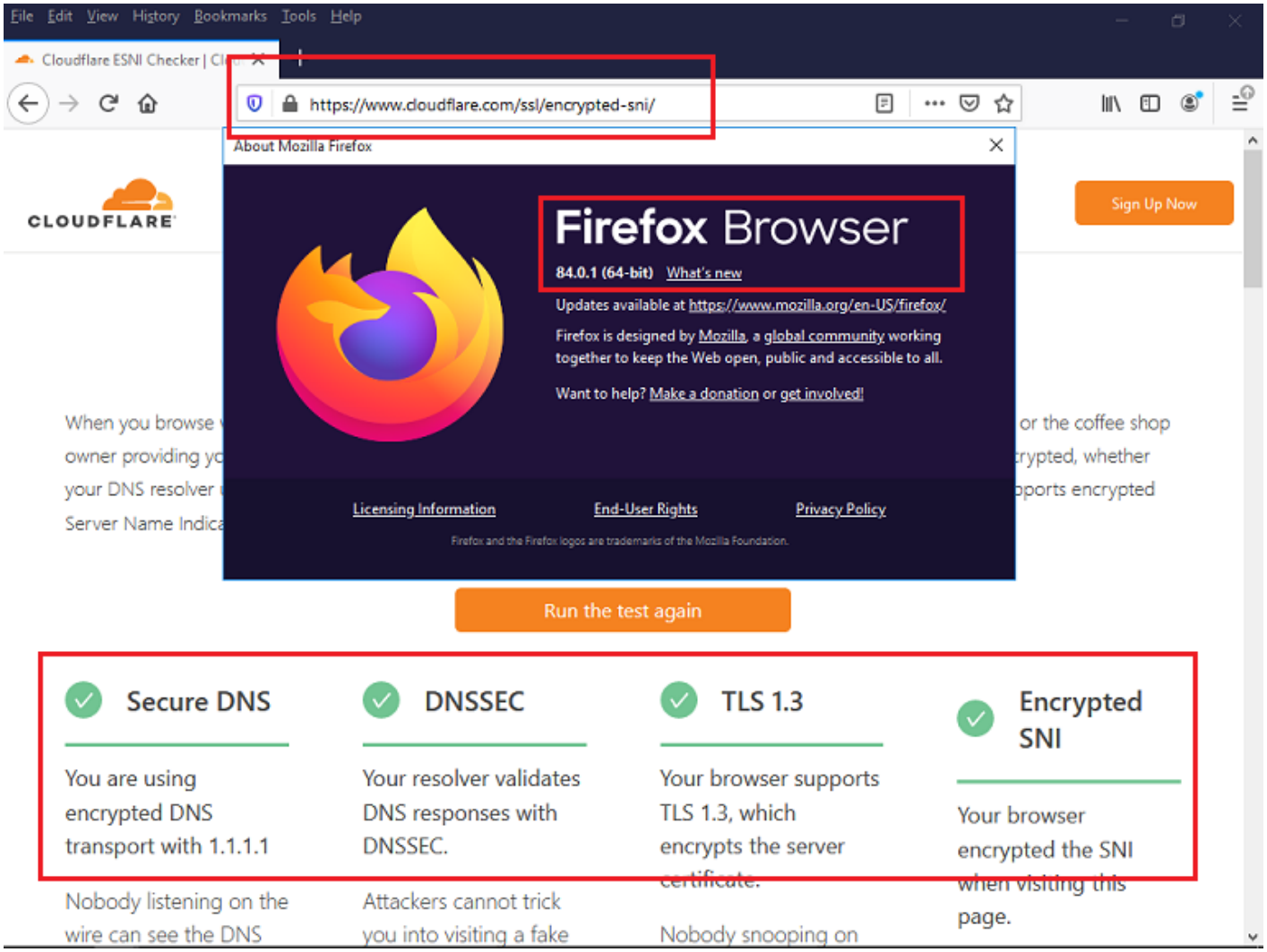
Actualizado el domingo 21 de julio de 2019

Recogemos la inquietud del Licenciado Bracci Roa por medio de su cuenta en Twitter @lubrio acerca del bloqueo por parte de CANTV de ciertas páginas web de contenido político, **dedicamos entonces este humilde trabajo acerca de la privacidad en Internet para dar cumplimiento a nuestra ideología: ¡la libertad se basa en NO tener amo alguno!**

https://twitter.com/ks7000/status/1147111208316735490

Actualizado el sábado 6 de marzo de 2021.

Hemos comprobado que la versión 84, la última disponible que apoya el ESNI funciona apropiadamente según la configuración que hemos descrito:



Mozilla Firefox 84 ESNI

https://twitter.com/ks7000/status/1368191756341231617

Fuentes consultadas

En idioma castellano

- «Indicador del nombre del servidor» en Wikipedia.
- «Firefox cifrará todas consultas web habilitando DNS sobre HTTPS» por David Naranjo en Ubunlog.

En idioma inglés

- «Improving DNS Privacy in Firefox» by Patrick McManus.
- «Encrypted SNI Comes to Firefox Nightly» by Eric Rescorla.
- «Encrypt it or lose it: how encrypted SNI works» by Alessandro Ghedini.
- «ESNI: A Privacy-Protecting Upgrade to HTTPS» by Seth Schoen.
- «Improving DNS Privacy in Firefox» by Patrick McManus.
- «What's next in making Encrypted DNS-over-HTTPS the Default» by Selena Deckelmann.
- «Trusted Recursive Resolver» at Mozilla Wiki (thanks to Daniel Stenberg!).

Enlaces relacionados

En idioma castellano

En idioma inglés

- «Centralised DoH is bad for privacy, in 2019 and beyond» blog PowerDNS.