

Hola, hoy os vamos a comentar en esta entrada como montar vuestro propio cliente DNSEncrypt, que nos servirá para *anonimizar* los datos de resolución de dominio que van por nuestra conexión, esto pondrá un poco más difícil la parametrización que hacen los gobiernos y grandes corporaciones con nuestra información.

¿Qué es DNSEncrypt?

DNSEncrypt crea un túnel cifrado entre el servidor y el cliente, y resuelve las peticiones DNS que realiza. Evita la suplantación de identidad y utiliza firmas criptográficas para verificar que las respuestas se originan en el sistema y que no hayan sido manipuladas.

Es una especificación abierta, con implementación libre, y que no está afiliada a ninguna empresa u organización.

Usar DNSEncrypt

Necesitamos tener instalado el programa `dnscrypt-proxy` para conectar a un servidor.

```
$ apt install dnscrypt-proxy
```

Configuramos el programa para que escuche en el puerto 53 de localhost (127.0.0.1) y se conecte al servidor DNSEncrypt de *HatThieves*.

```
listen_addresses = ['127.0.0.1:53']  
server_names = ['hatthieves', 'hatthieves6']
```

```
[static.'hatthieves']  
  stamp =  
'sdns://AQUAAAAAAAAAETgyLjIyMy4zLjEzNT01NDQzICIJ3we16VXeoGdYSn0d3QY  
m2h5ZQCUmjS_GNx-J0ELOHTIuZG5zY3J5cHQyY2VydC5oYXR0aGlldmVzLmVz '  
[static.'hatthieves6']  
  stamp =  
'sdns://AQUAAAAAAAAAAHFsyMDAx0mJhMDox0DAw0jgwZTA60jFd0jU0NDMgIgnfB7X  
pVd6gZ1hKc53dBibaHl1AJSaNL8Y3H4k4Qs4dMi5kbnNjcnlwdC1jZXJ0LmhhdHRoaW  
V2ZXMuZXM'
```

Una vez conectado podremos configurar nuestro sistema para que utilice el puerto local.

```
$ echo 'nameserver 127.0.0.1' > /etc/resolv.conf
```

Y todas las peticiones del sistema pasarán a través de nuestro servidor que resuelve directamente a los servidores raíz de internet, usamos DNSSEC y no guardamos registros como puede verse en nuestra instancia. También se pueden usar los servidores públicos oficiales.

Un saludo, estad seguros y nos vemos en la próxima entrada.