DNSCRYPT IN THE NIGHT

Fanta

14/03/16

Índice

1. Introducción

Cifrar las peticiones DNS es un paso más. Cifrar las peticiones DNS solamente supone eso, que cada vez que busquemos duckduckgo.com la petición para saber en que IP anda ese dominio no se realize en plano.

Web del proyecto: https://dnscrypt.org/

En este articulillo veremos como podemos montar un server dnscrypt y tambien el cliente.

2. Instalación de dependencias

En debian 8 podemos instalar las dependencias así:

```
# apt-get update
# apt-get install git autoconf libsodium-dev libevent-dev dnsutils gcc bind9
ntpdate
```

Una vez tengamos las dependencias instaladas vamos a crear un par de directorios:

```
$ mkdir dnscrypt
$ cd dnscrypt
$ mkdir dnscrypt-server dnscrypt-client keys-and-certs
```

3. Compilar servidor dnscrypt

Necesitamos una maquina donde instalar dnscrypt server. En esa maquina compilaremos la última versión de dnscrypt server.

La versión estable de dnscrypt server es la 0.2.0 a fecha de hoy 2 de noviembre del 2015.

Este es el repositorio git: https://github.com/Cofyc/dnscrypt-wrapper

El proceso para compilarlo e instalarlo en el sistema es este:

```
$ cd dnscrypt-server
$ git clone https://github.com/Cofyc/dnscrypt-wrapper
$ make configure
$ ./configure
$ make
# make install
```

Ya tenemos instalado dnscrypt server en la maquina que queremos que haga de servidor. Esto no quiere decir que funcione. Simplemente esta el programa.

4. Compilar cliente dnscrypt

El cliente se llama dnscrypt-proxy y podemos instalarlo también en la maquina servidor para hacer pruebas.

Lo ideal es que dnscrypt-proxy lo instalemos en los ordenadores que queramos se conecten al servidor dnscrypt.

Esto ya lo explicaremos luego. Ahora lo importante es saber como compilar dnscryp-proxy (el cliente).

La versión estable del cliente dnscrypt es la 1.6.0 a fecha de hoy 2 de noviembre del 2015.

Podemos bajar esta versión desde aquí: http://download.dnscrypt.org/dnscrypt-proxy/dnscrypt-

proxy-1.6.0.tar.gz

```
$ cd ..
$ cd dnscrypt-client
$ wget http://download.dnscrypt.org/dnscrypt-proxy/dnscrypt-proxy-1.6.0.tar.gz
$ tar xfvz dnscrypt-proxy-1.6.0.tar.gz
$ rm -rf dnscrypt-proxy-1.6.0.tar.gz
$ mv dnscrypt-proxy-1.6.0/* .
$ rm -rf dnscrypt-proxy-1.6.0
$ ./configure
$ make
# make install
```

Ya tenemos compilado dnscryp cliente (el proxy) e instalado en el sistema.

5. Comprobar las versiones

Ahora es el momento de comprobar las versiones tanto del servidor (dnscrypt-wrapper) como del cliente (dnscrypt-proxy).

Esto se puede realizar de forma sencilla desde la línea de comandos como root así para ver **la versión del server**:

```
# dnscrypt-wrapper --version
```

Tendriamos que ver algo así como esto: *dnscrypt-wrapper 0.2-14.g2cf8ecf*

Y para ver **la versión del cliente** así:

```
# dnscrypt-proxy --version
```

Saldrá algo así como esto: *dnscrypt-proxy 1.6.0*

6. Generación de claves y certificados

Generamos el par de llaves de proveedor:

```
# cd ..
# cd keys-and-certs
# dnscrypt-wrapper --gen-provider-keypair
```

Esto generará 2 archivos: *public.key* y *secret.key*.

Nos mostrará un ejemplo de lo que han de usar los clientes que utilicen nuestro servicio.

Nos mostrará también el fingerpint, no obstante también podemos sacarlo así cuando queramos:

```
# dnscrypt-wrapper --show-provider-publickey-fingerprint
```

Ese chorro se lo pasaremos a quienes quieran conectar o lo publicaremos en algún lado para que la gente conozca la huella del server.

Ya tenemos las llaves de proveedor. Ahora vamos a crear llaves de tiempo limitado para cifrar las peticiones DNS.

Generaremos una llave y un certificado que podrán ser actualizados cuando nos de la real gana sin requerir al cliente o a los clientes cambiar su configuración/ones.

Esto lo generaremos así:

```
# dnscrypt-wrapper --gen-crypt-keypair --crypt-secretkey-file=1.key
```

Tendremos un archivo llamado 1.key

Ahora vamos a generar el certificado:

```
# dnscrypt-wrapper --gen-cert-file --crypt-secretkey-file=1.key --provider-cert-file=1.cert
```

Nos guardará un archivo llamado 1.cert

Haciendo un ls tendríamos que ver 4 archivos:

- 1.cert
- 1.key
- public.key
- secret.key

7. Iniciar servidor

Ahora viene la parte bonita. Vamos a iniciar el servidor indicando un servidor dns en *–resolver-address* como por ejemplo 8.8.8.8 (cuidado que es de google. Para probar esta bien, pero mejor buscar otros).

Un ejemplo de como iniciarlo que hemos de adaptar a nuestras condiciones es este:

```
# dnscrypt-wrapper -VVV --resolver-address=8.8.8.8:53 --listen-address=127.0.0.2:443 --provider-name=2.dnscrypt-cert.bash-street-boys-and-girls.com --crypt-secretkey-file=1.key --provider-cert-file=1.cert
```

Es importante poner en *–provider-name* 2.dnscrypt-cert. y luego por ejemplo tu dominio. En el caso del ejemplo queda así: 2.dnscrypt-cert.bash-street-boys-and-girls.com

8. Comprobar que el servidor resuelve

Lo primero es ver que la hora esta sincronizada. Es importante para que no tengamos problemas con el certificado.

En debian podemos usar *dpkg-reconfigure tzdata* y por ejemplo *ntpdate -u 1.europe.pool.ntp.org* para sincronizar la hora.

Como tenemos en el server tambien dnscrypt-proxy vamos a probar a montar el proxy así por ejemplo:

```
# dnscrypt-proxy --local-address=127.0.0.2:53 --resolver-address=127.0.0.2:443 --provider-name=2.dnscrypt-cert.bash-street-boys-and-girls.com --provider-key=B67F:1944:2110:E41F:542C:CB37:5D01:5A83:E793:2B91:45AA:5DE8:7E23:3317:1855:BC53
```

Esto es buena cosa. Ahora con dig probaremos a ver si nos resuelve:

```
# dig -p 53 elbinario.net @127.0.0.2
```

Si nos resuelve es que todo va bien :). Si tienes problemas revisa la hora del sistema, revisa que le metes la fingerprint (huella) adecuada ya que es fácil meter la que no es. Recuerda añadir en /etc/resolv.conf nameserver 127.0.0.2

Para probar eso esta bien pero finalmente si quisiéramos ofrecerlo hacia el exterior tendríamos que poner dnscrypt-wrapper con algo como esto (modifica lo que tengas que modificar para que se adapte a tu configuración):

```
# dnscrypt-wrapper -VVV --resolver-address=8.8.8.8:53 --listen-
address=37.228.134.139:443 --provider-name=2.dnscrypt-cert.bash-street-boys-
and-girls.com --crypt-secretkey-file=1.key --provider-cert-file=1.cert
```

9. Conectarse desde un equipo cliente al servidor

Tenemos que compilar en nuestra maquina dnscrypt-proxy tal y como hemos indicado en el apartado Compilar cliente dnscrypt. Una vez compilado e instalado en el sistema tendremos que ejecutar en una terminal esto:

```
# dnscrypt-proxy --local-address=127.0.0.2:53 --resolver-
address=37.228.134.139:443 --provider-name=2.dnscrypt-cert.bash-street-boys-
and-girls.com --provider-
key=B67F:1944:2110:E41F:542C:CB37:5D01:5A83:E793:2B91:45AA:5DE8:7E23:3317:1855:
BC53
```

Para probar que resuelve podemos hacerlo así:

```
# dig -p 53 elbinario.net @127.0.0.2
```

Finalmente en /etc/resolv.conf pondremos nameserver 127.0.0.2 y tendría que resolver pasando por el dnscrypt.

10. Lista de proveedores de servicio dnscryp

Aquí pueden verse: https://github.com/jedisct1/dnscrypt-proxy/blob/master/dnscrypt-resolvers.csv#L2