nftables bloqueo por país o zona

Para eso necesitamos clonar el repositorio de Geoip que se puede localizar aquí

Luego podemos ver las opciones usando el comando:

```
./nft_geoip --help
```

El script necesita dos archivos .csv.

Un csv de datos de país (location.csv), su ruta se puede especificar con la opción --file-location
Un csv de datos geoip (dbip.csv), su ruta se puede especificar con la opción --file-address

location.csv

El script se envía con este archivo. Un .csv modificado que contiene los datos del país necesarios para generar los mapas.

dbip.csv

Este .csv no se envía y es necesario recuperarlo antes de utilizar el script. Existe la opción --download para hacerlo.

Generando los mapas geoip

Para generar las asignaciones en el directorio actual (suponiendo que no tenga el archivo dbip.csv)

```
./nft_geoip.py --file-location location.csv --download
```

Esto nos descargará los siguientes archivos

```
rwxr-xr-x 2 root root 4,0K ene  4 19:38 .
drwxr-xr-x 5 root root 4,0K ene  4 19:38 ..
-rw-r--r-- 1 root root  22M ene  4 19:38 dbip.csv
-rw-r--r-- 1 root root  956 ene  4 19:38 geoip-def-africa.nft
-rw-r--r-- 1 root root 8,3K ene  4 19:38 geoip-def-all.nft
-rw-r--r-- 1 root root  902 ene  4 19:38 geoip-def-americas.nft
```

```
-rw-r--r-- 1 root root   15 ene  4 19:38 geoip-def-antarctica.nft
-rw-r--r-- 1 root root  808 ene  4 19:38 geoip-def-asia.nft
-rw-r--r-- 1 root root  810 ene  4 19:38 geoip-def-europe.nft
-rw-r--r-- 1 root root  461 ene  4 19:38 geoip-def-oceania.nft
-rw-r--r-- 1 root root 8,8M ene  4 19:38 geoip-ipv4.nft
-rw-r--r-- 1 root root  16M ene  4 19:38 geoip-ipv6.nft
```

geoip-def-all.nft

Contiene todas las definiciones. También contiene un mapa entre las marcas de país y su marca de continente correspondiente.

geoip-def-{continente}.nft
Subconjunto de definiciones para países de un continente determinado. Para ser utilizado como marcas.

geoip-ipv4.nft
Que contiene el mapa entre rangos ipv4 y sus datos geoip. @geoip4

geoip-ipv6.nft
Que contiene el mapa entre rangos ipv6 y sus datos geoip. @geoip6

Ejemplo permitir sólo IP de España por https

```
table inet filter {

        include "/etc/nftables/geoip-def-all.nft"
        include "/etc/nftables/geoip-ipv4.nft"
        include "/etc/nftables/geoip-ipv6.nft"

        chain output {
                type filter hook output priority filter; policy accept;
        }

        chain input {
                type filter hook input priority filter; policy accept;
                meta mark set ip saddr map @geoip4
                meta mark set ip6 saddr map @geoip6
                meta mark $ES tcp dport 443 accept
```

```
                tcp dport 443 drop
        }
}
```

Revision #1
Created 19 October 2023 05:54:05 by Admin
Updated 19 October 2023 06:06:17 by Admin