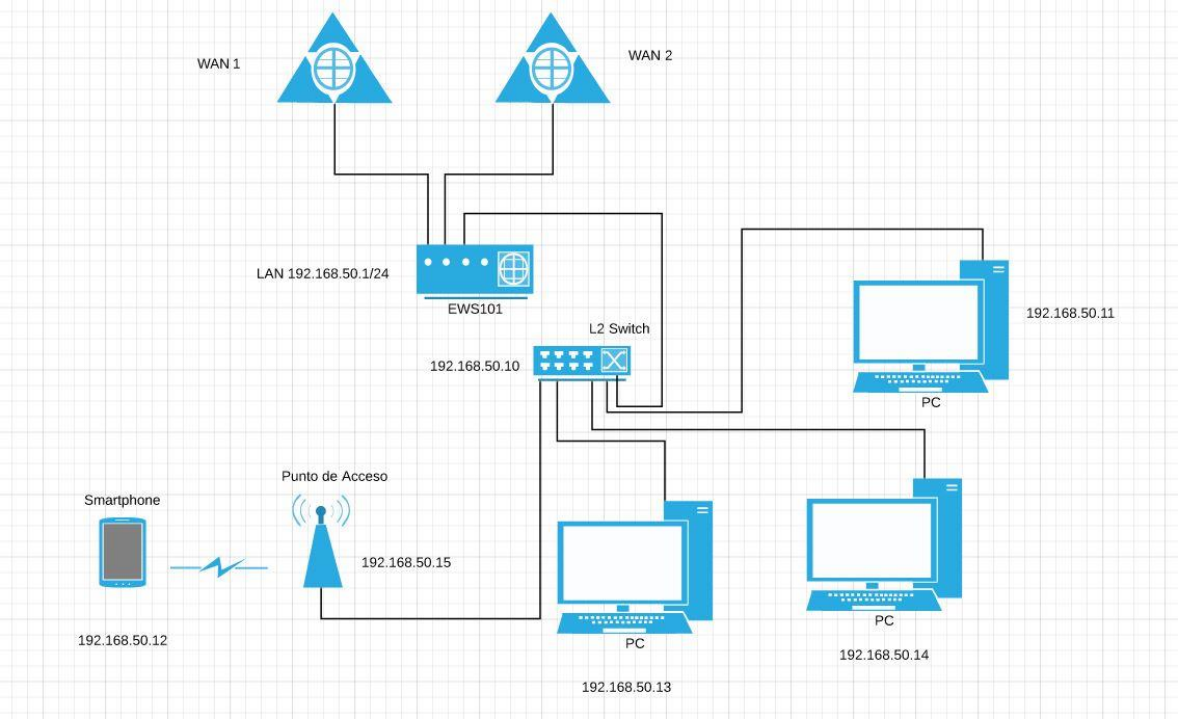
WifiCloud con Peplink Bloquear DNS públicas que no sean de WifiCloud

(2019)

En esta guía rápida, explicaremos como evitar que el usuario se salte el filtrado de contenido de WifiCloud cambiando las DNS's de su equipo por una DNS pública como 8.8.8.8 o 8.8.4.4

Para esta guía, utilizaremos la siguiente topología de red.

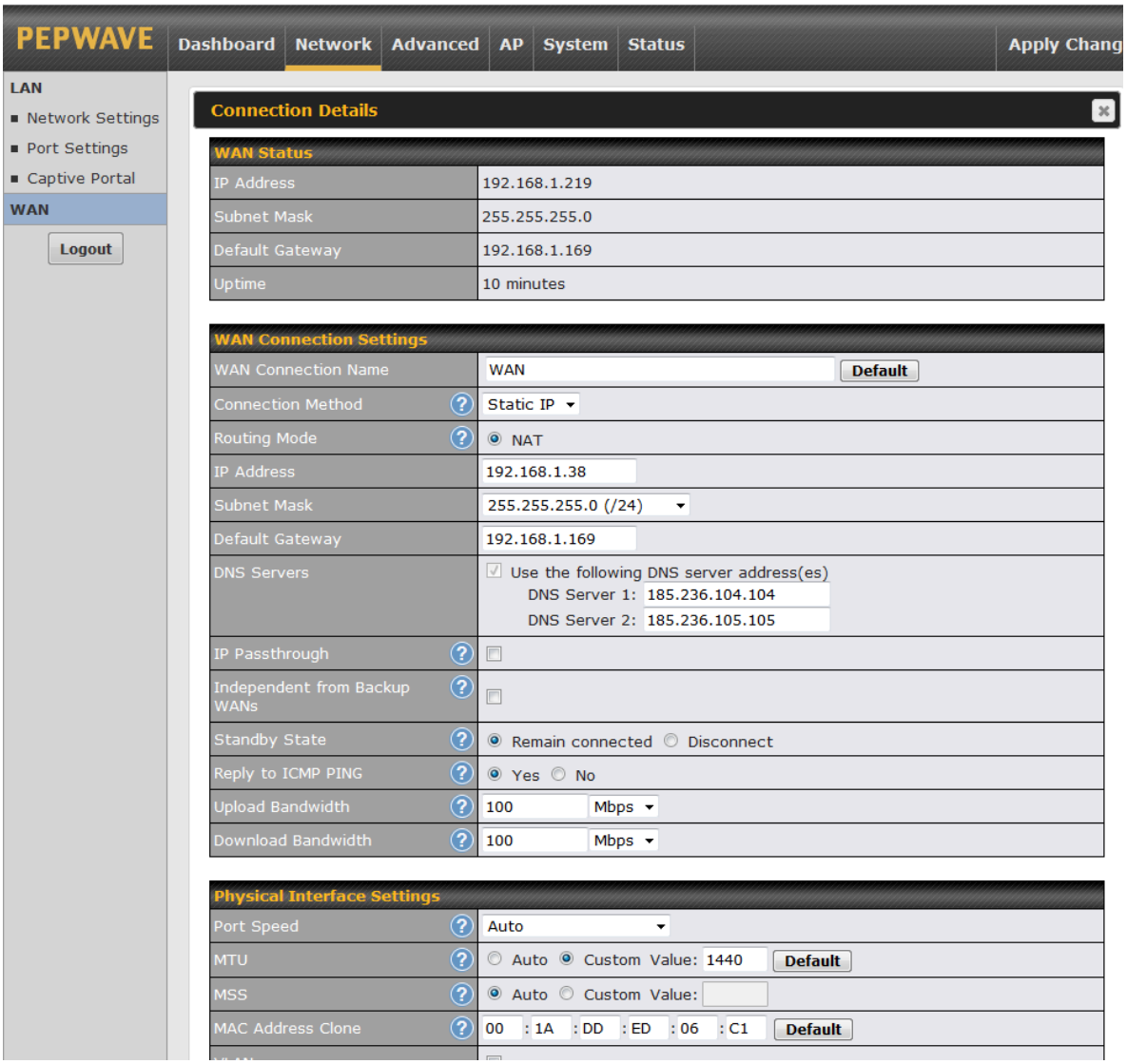


El primer paso, es configurar las DNS's de WifiCloud en nuestro Balance One Core.

Para ello, accedemos al "**Dashboard**" del equipo y hacemos clic sobre el botón "**Details**" sobre la conexión WAN que queremos utilizar, y en el apartado "**DNS Server**" marcamos la casilla de "Use the following DNS serve Address(es)" e introducimos las DNS de WifiCloud.

DNS Server 1: 185.236.104.104
DNS Server 2: 185.236.105.105

Quedando la configuración de la siguiente manera:

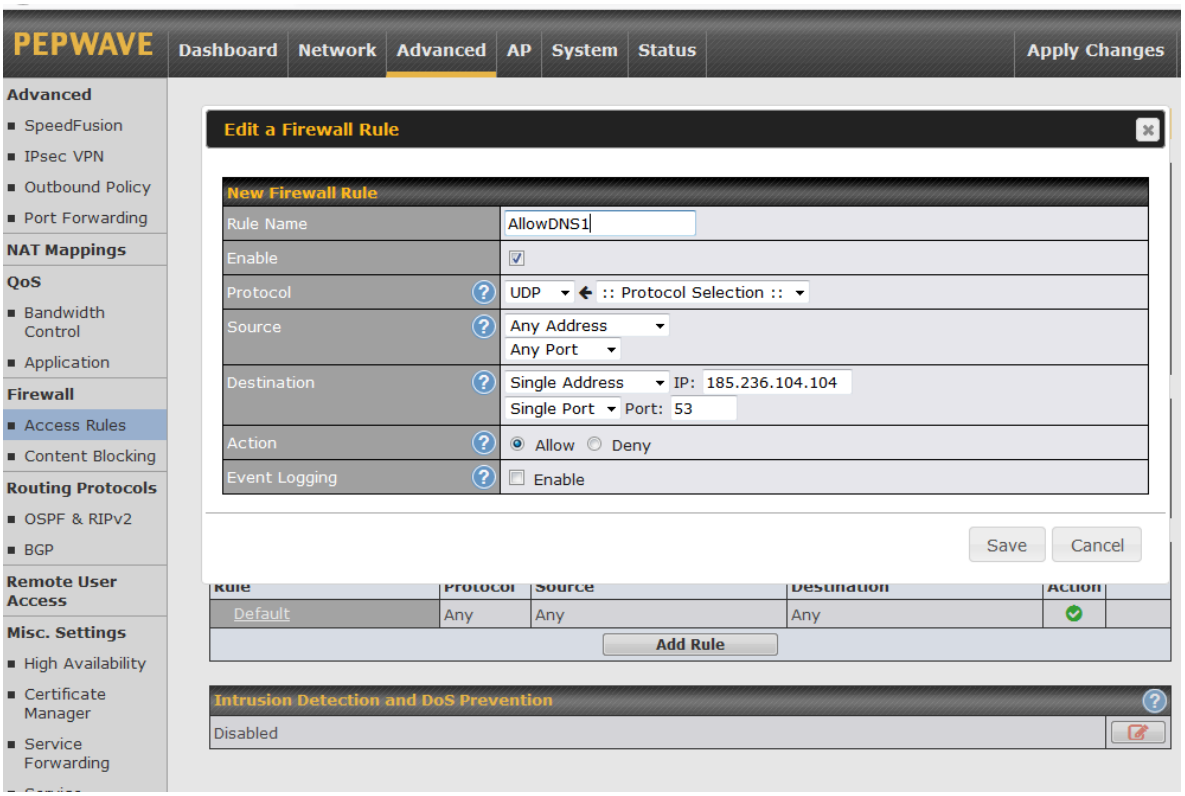


Una vez configuradas las DNS en la WAN, procederemos a crear las reglas de firewall para prevenir los cambios de DNS por parte del usuario. De esta forma, si el usuario cambia las DNS de su equipo, no tendrá acceso a internet.

Para realizar esta configuración, accedemos a "**Advanced → Firewall→ Access Rules**".

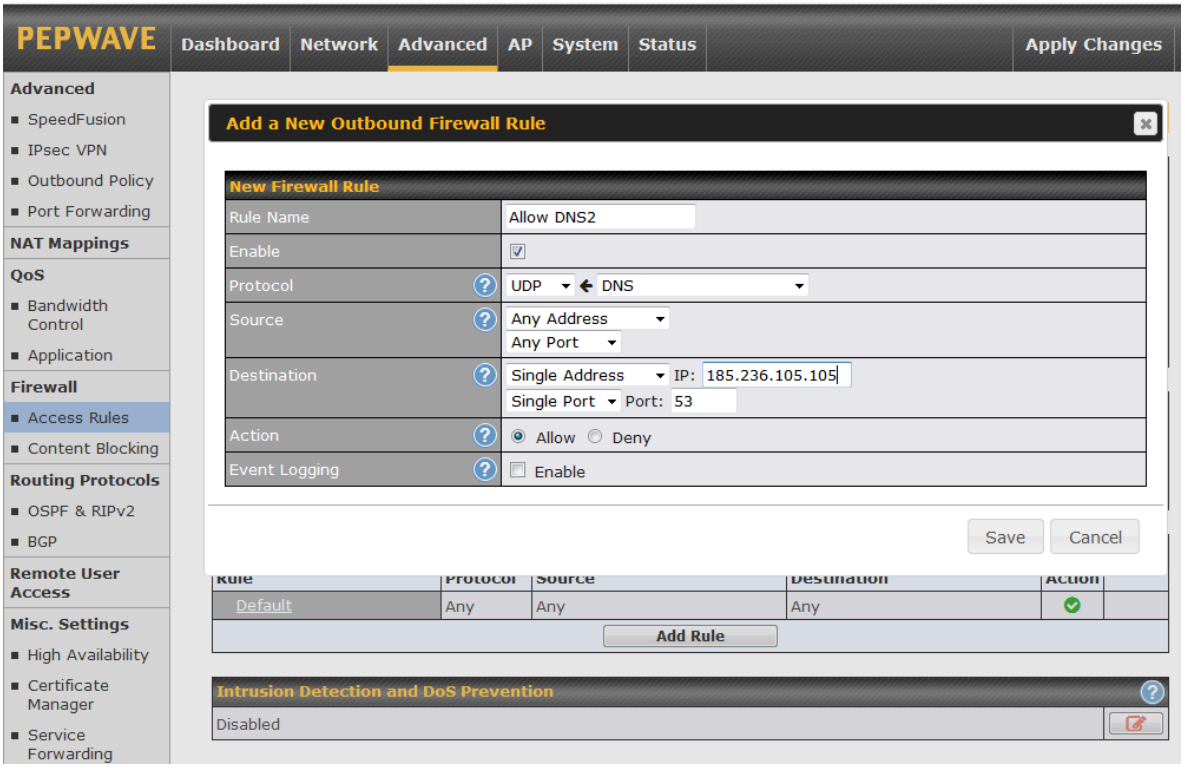
Crearemos la primera regla para permitir el tráfico USD por el puerto 53 hacia la DNS primera de WifiCloud. (185.236.104.104)

La regla quedaría de la siguiente manera:



Luego, creamos otra regla para permitir el tráfico por el puerto 53 hacia la segunda DNS de WifiCloud (185.236.105.105)

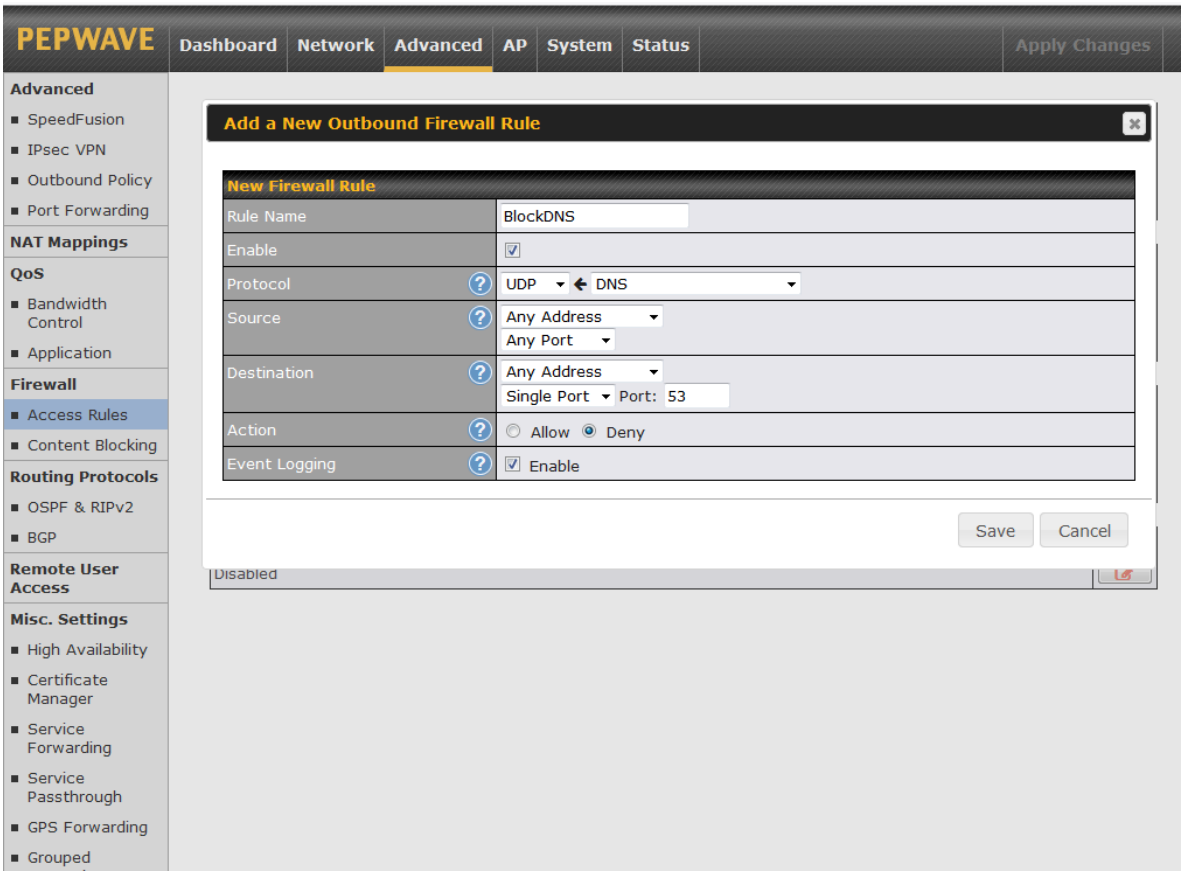
La regla quedaría de la siguiente manera:



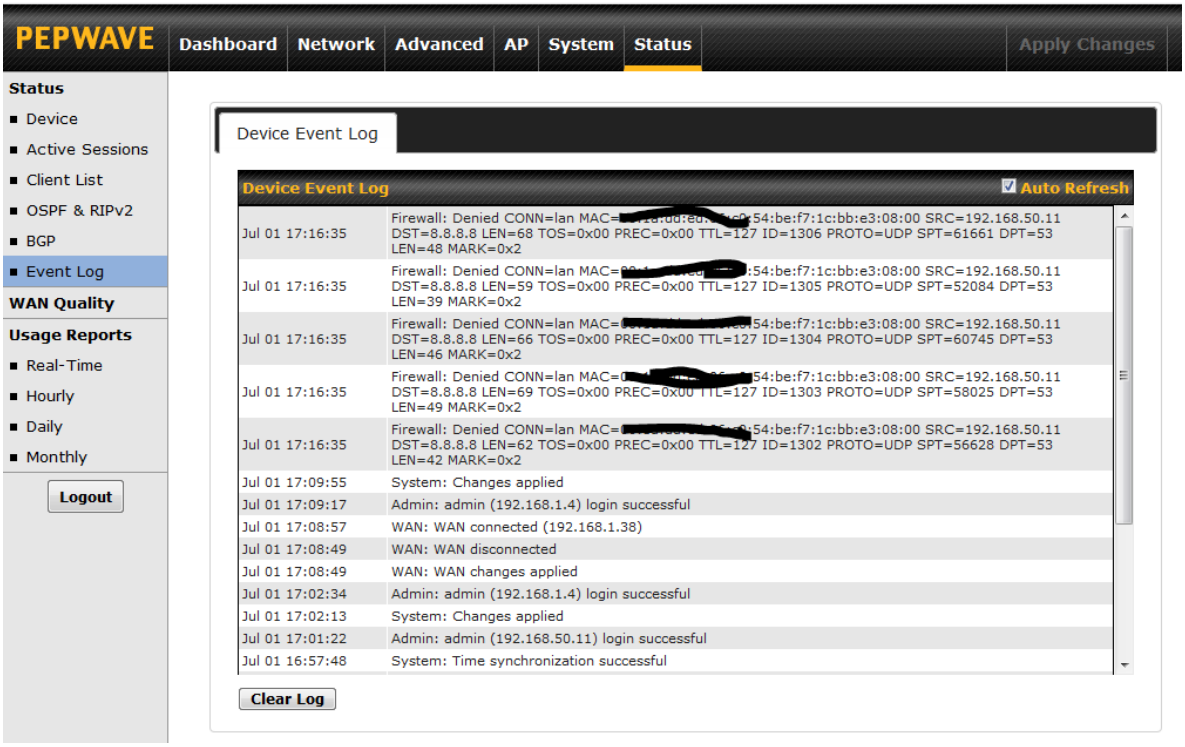
Y por último, crearemos una regla, para bloquear el trafico UDP en el puerto 53 para todo lo demás. De esta forma, si el cliente cambia la DNS del equipo, no saldrá a Internet.

En esta regla, también activaremos la opción de "**event logging**" de esta forma, podremos ver si algún usuario ha cambiado sus DNS por otra que no sea las de WifiCloud.

La regla creada quedaría de la siguiente manera:



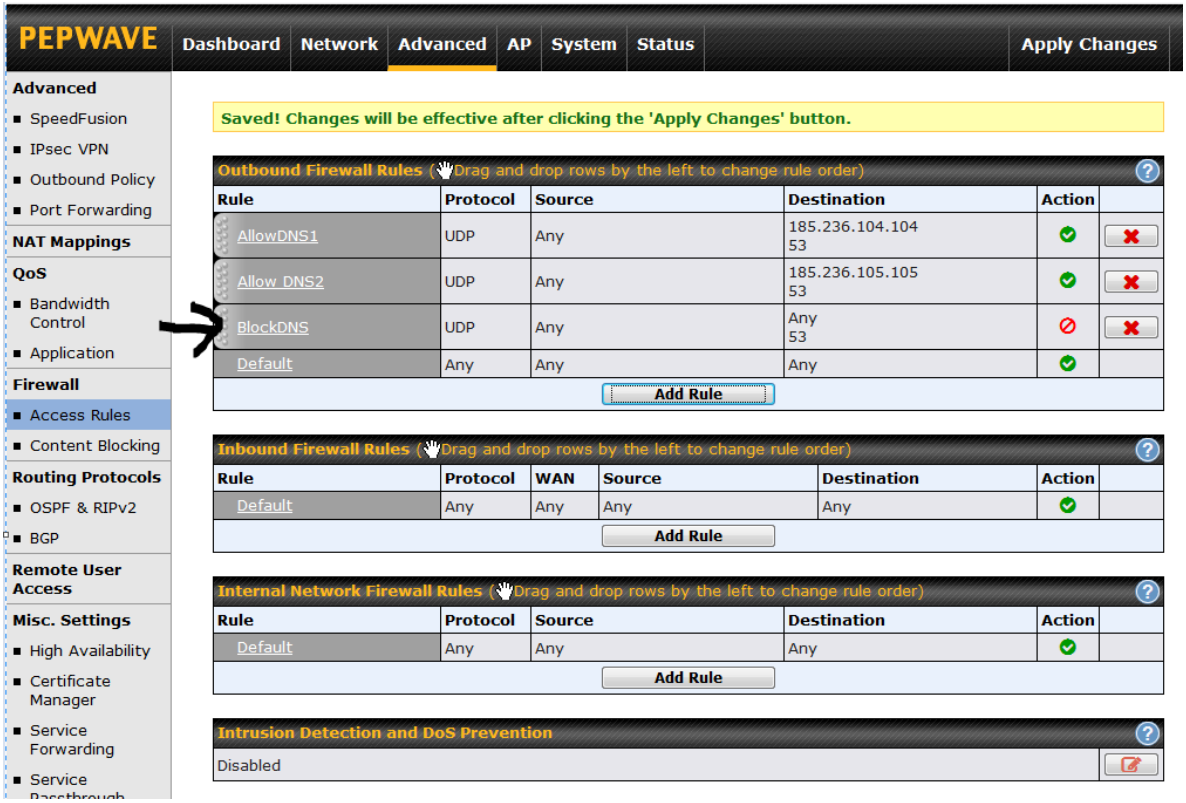
Si un usuario ha incumplido esta regla, lo podremos ver en el log.



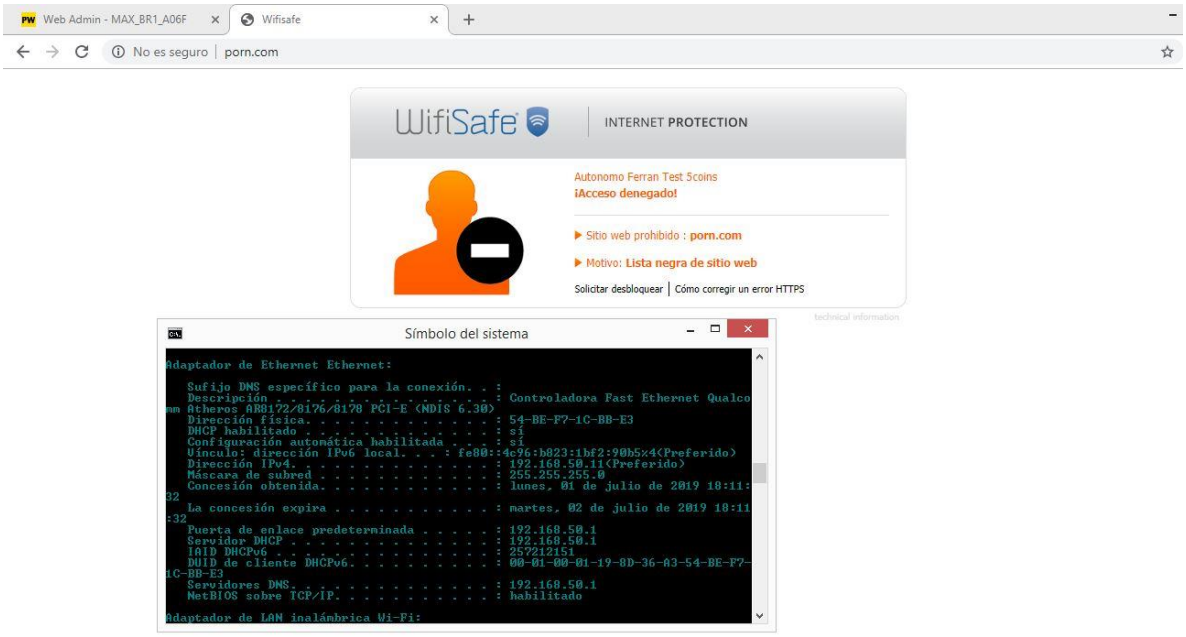
Cabe destacar que las reglas de firewall funcionan de forma secuencial, por lo tanto, hay que ordenar las reglas que hemos creado, ya que al consultarlas, el equipo utilizará la primera regla que coincida con la política que hemos creado, e ignorará las demás reglas…

Debemos asegurarnos que las reglas para permitir y el tráfico sobre las DNS se encuentran en primero, y segundo lugar en la lista.

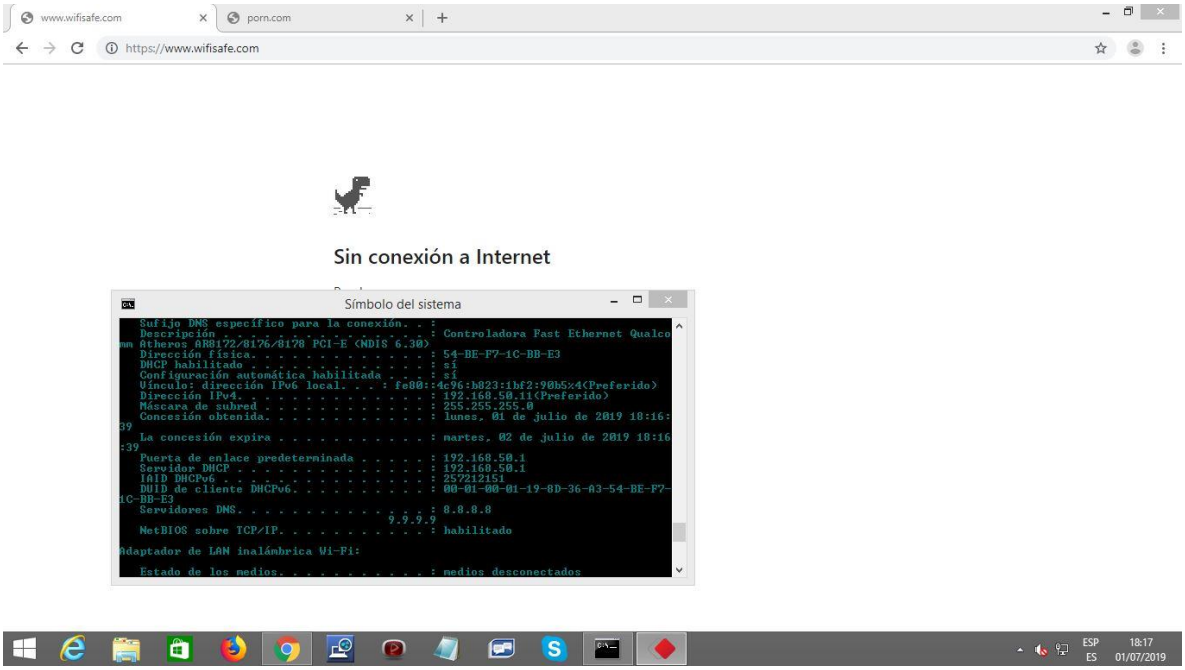
De la siguiente forma:



Como podremos ver en la siguiente captura, si un usuario, con las DNS de WifiCLOUD intenta acceder a una web bloqueada, saldrá el siguiente mensaje:



En caso de cambio de DNS, el usuario no saldría a Internet, como podremos ver a continuación:



Más información y otros artículos/manuales en
Blog de WifiSafe (https://www.wifisafe.com/blog/categoria/soporte)

Contacto: soporte@wifisafe.com