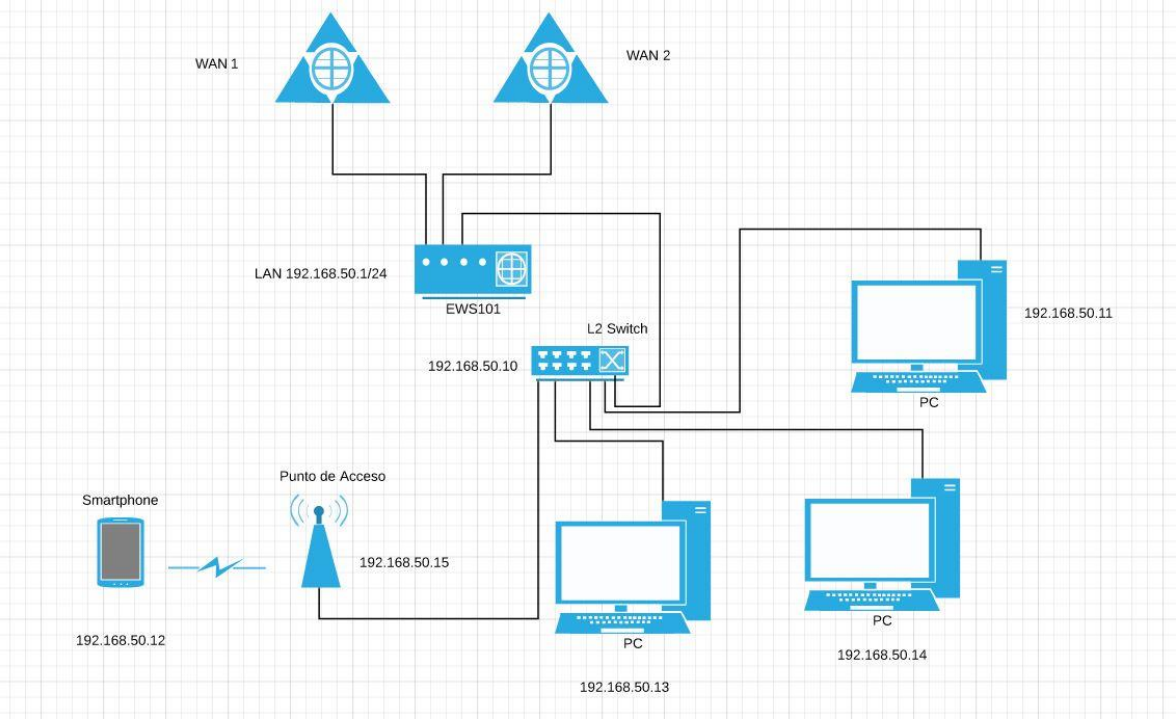
Configuración bloqueo de contenido con DNS WifiCloud con HotSpot Edgecore

(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

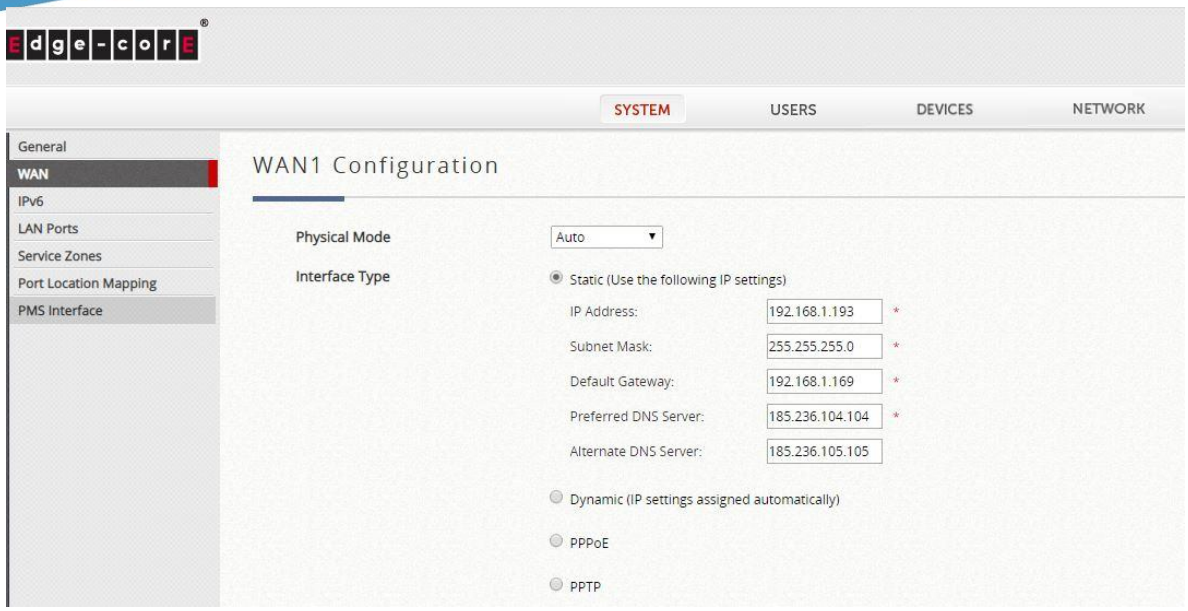
Para esta guía, utilizaremos la misma topología de red que en otras ocasiones. No entraremos en detalles de la configuración de los HotSpot EdgeCore, ya que éste tema, lo hemos tratado en el manual del equipo publicado en la web.



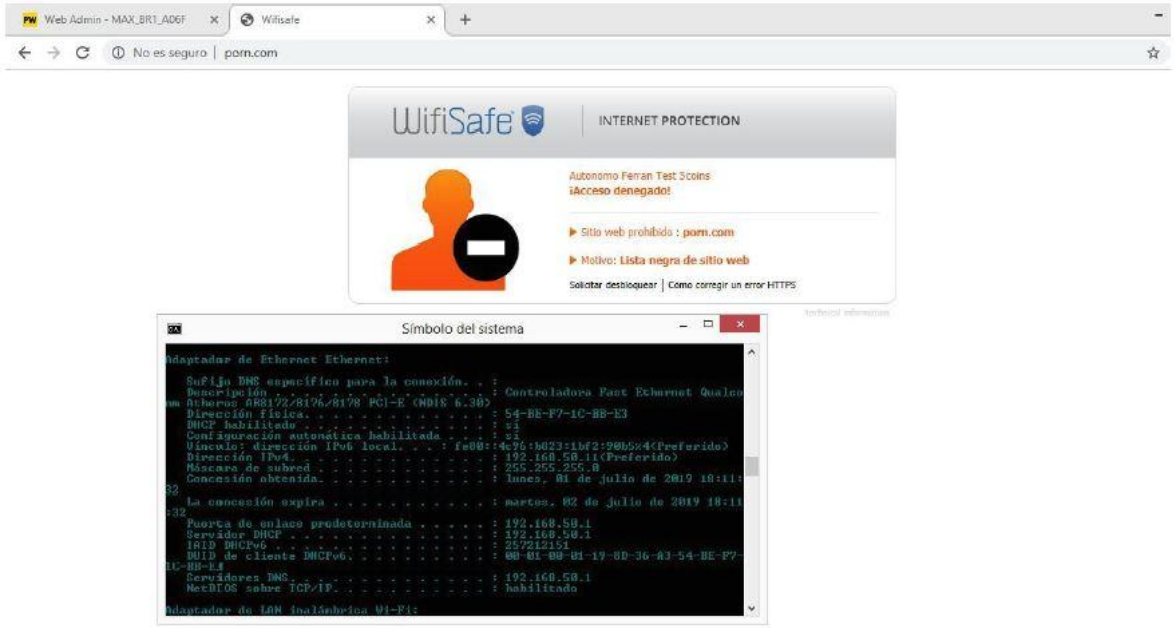
El primer paso, es configurar las DNS de WifiCloud en la WAN del equipo.

Para ello, accedemos a "**System→ WAN**". Seleccionamos la opción: "**Use the following ip settings**" e introducimos las DNS de WifiCloud en los campos "**preffered DNS server**" y "**alternative DNS server**".

Quedando la configuración de la siguiente forma:



Una vez configurado las DNS de WifiCloud en la WAN del equipo, el filtro de contenido ya estaría listo para su uso, y veríamos en siguiente mensaje al entrar en una web bloqueada:



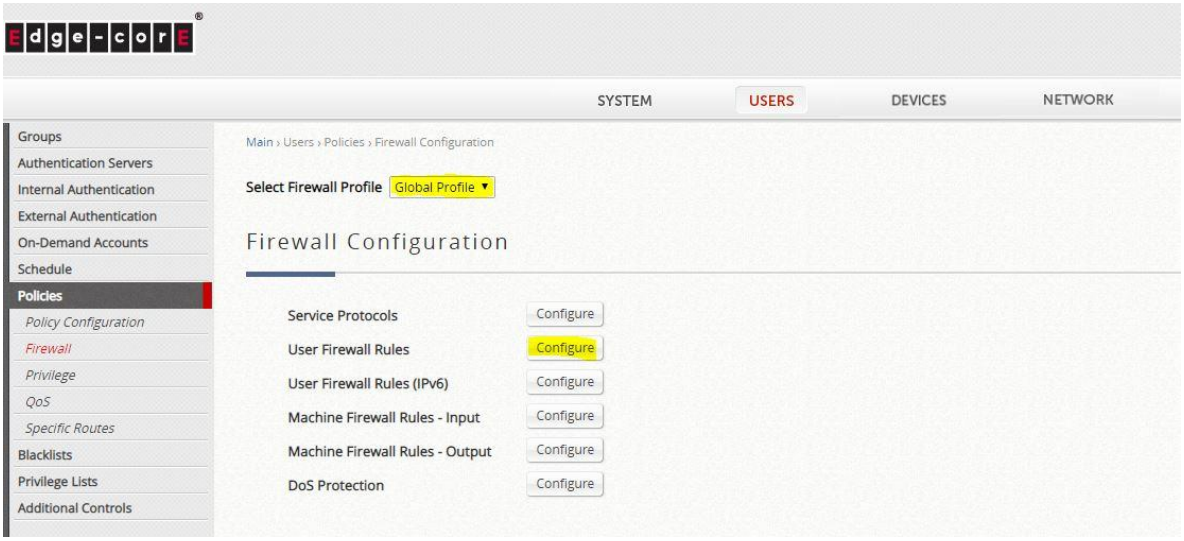
Ahora pasaremos a crear una regla de firewall para prevenir que el usuario cambie manualmente las DNS del equipo y salte el filtro de contenido.

Hay dos formas de crear las reglas de firewall en el equipo, o bien la creamos por grupos y solo aplicará las reglas al usuario bajo la política asociada a este grupo, o podemos crear en el perfil global. En este caso, aplicaría la regla a todos los usuarios del equipo.

En este guía, haremos la regla para el perfil global.

Accedemos a "**Users→ Policies→ Firewall**".

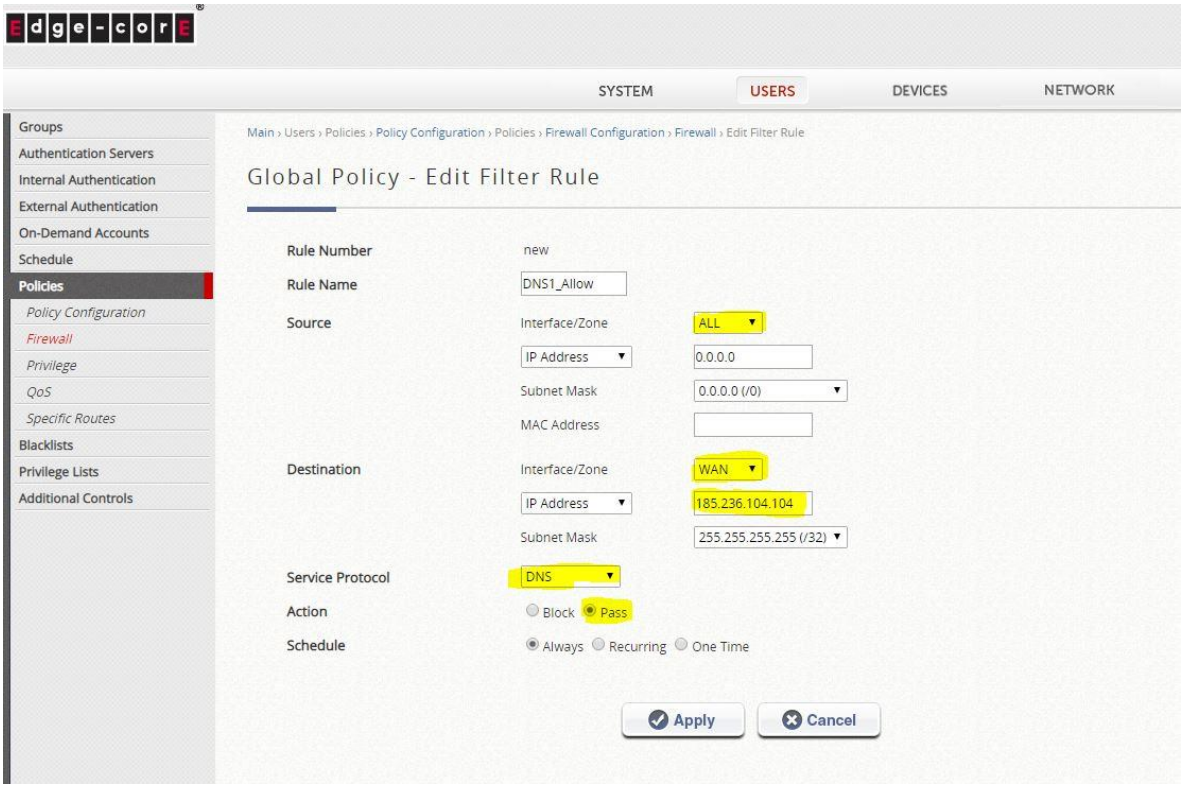
1. En el menú "**Select Firewall Profile**" seleccione "**Global Profile**" y luego, entramos en el menú "**User Firewall Rules**" y hacemos clic en "**Edit**" para crear la regla.



Dentro del menú "**User Firewall Rules**" creamos la regla de la siguiente forma:

Rule Name: Definimos un nombre para la regla
Source: All / **Interface**: IP address (Para aplicarlo a todas las zonas)
Destination: WAN / **Interface**: IP Address = 185.236.104.104 / **Subnet Mask**: 255.255.255.255
Service Protocol: DNS
Acction: Pass

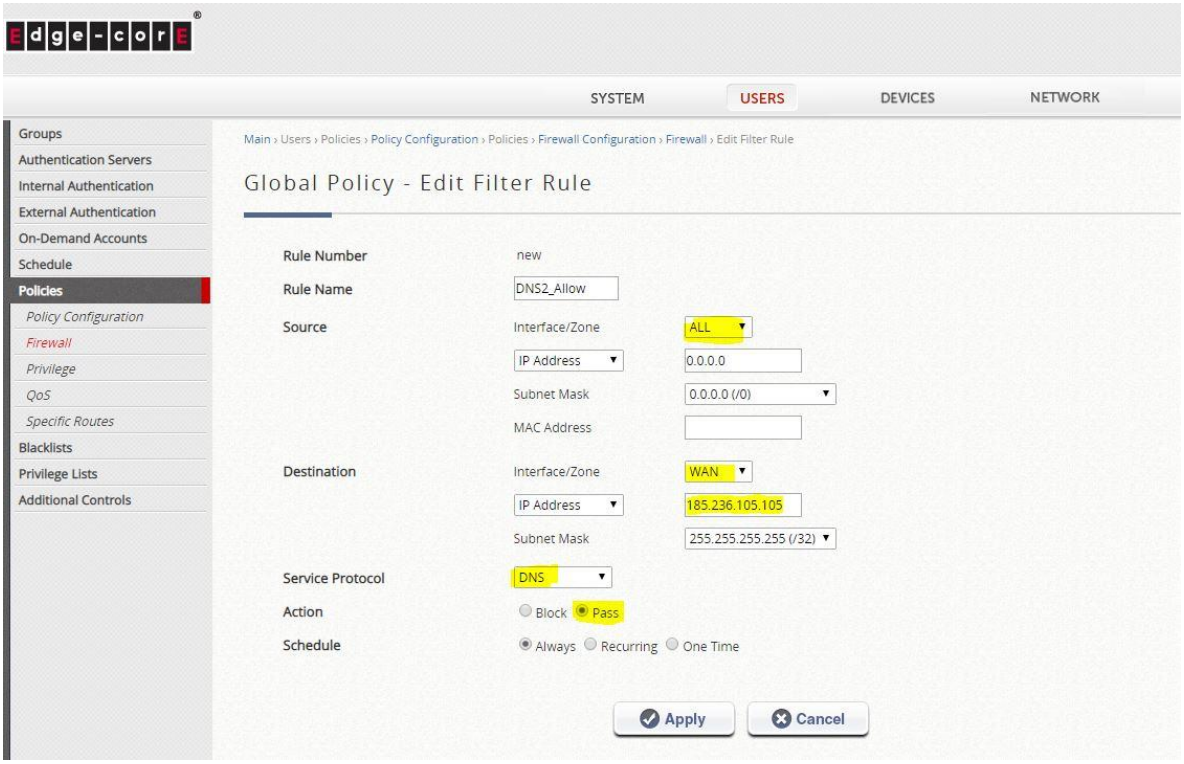
Quedando la regla de la siguiente manera:



Ahora crearemos una regla exactamente igual, pero para la DNS alternativa de WifiCloud.

Rule Name: Definimos un nombre para la regla
Source: All / **Interface**: IP address (Para aplicarlo a todas las zonas)
Destination: WAN / **Interface**: IP Address = 185.236.105.105 / **Subnet Mask**: 255.255.255.255
Service Protocol: DNS
Acction: Pass

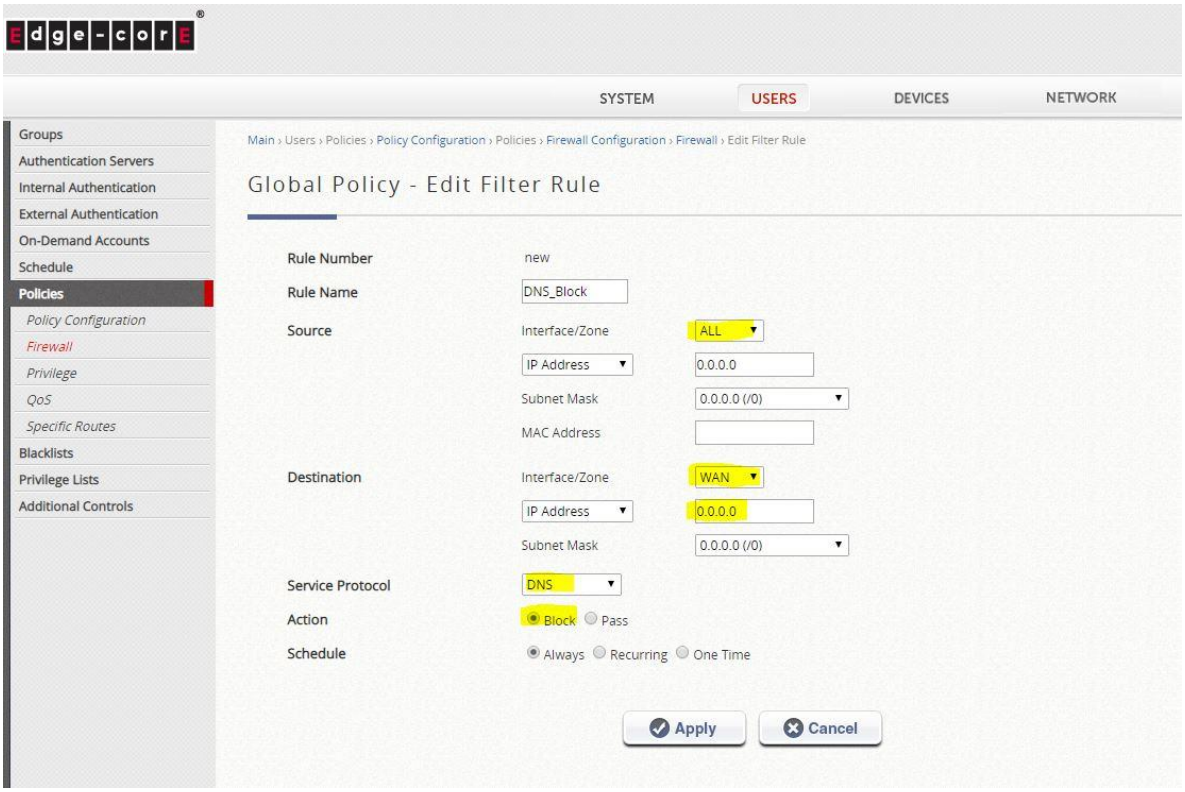
Quedando la regla de la siguiente manera:



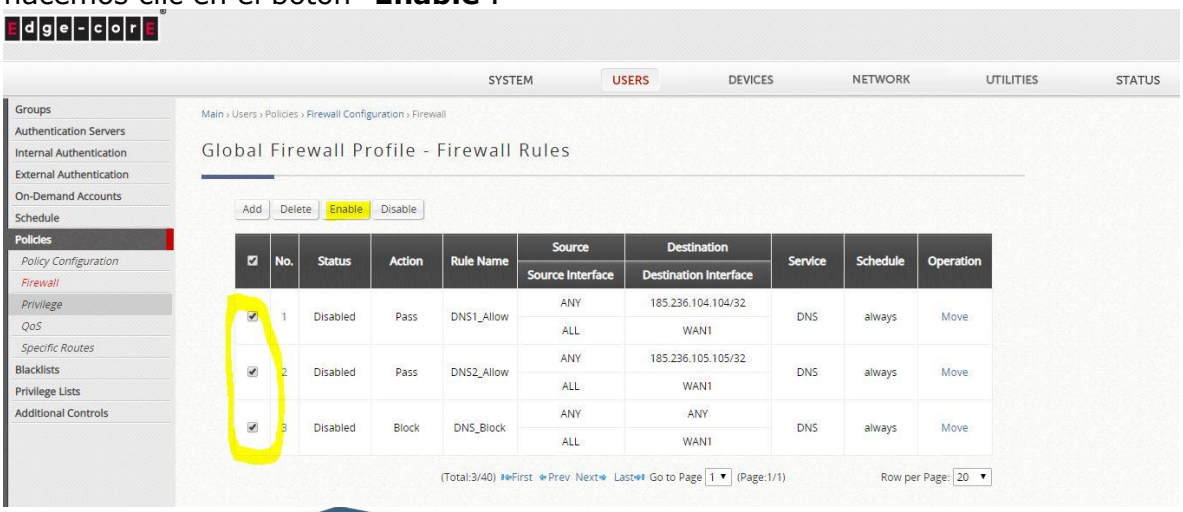
Y por último, creamos la regla para bloquear el tráfico en el puerto 53, que no tenga como destino las DNS de WifiCloud.

Rule Name: Definimos un nombre para la regla
Source: All / **Interface**: IP address (Para aplicarlo a todas las zonas)
Destination: WAN / **Interface**: IP Address = 0.0.0.0 / **Subnet Mask**: 0.0.0.0
Service Protocol: DNS
Acction: Block

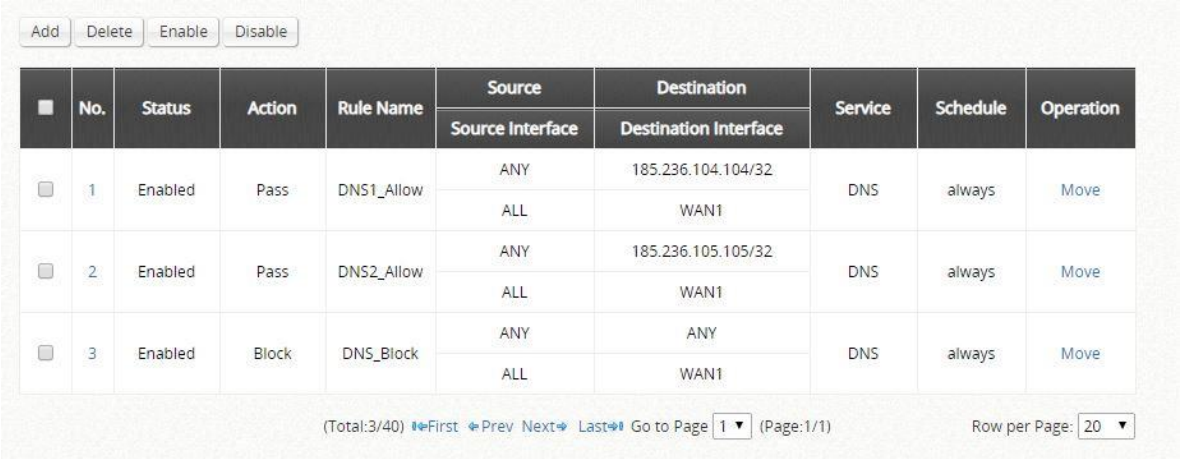
La regla creada seria quedaría de la siguiente forma:



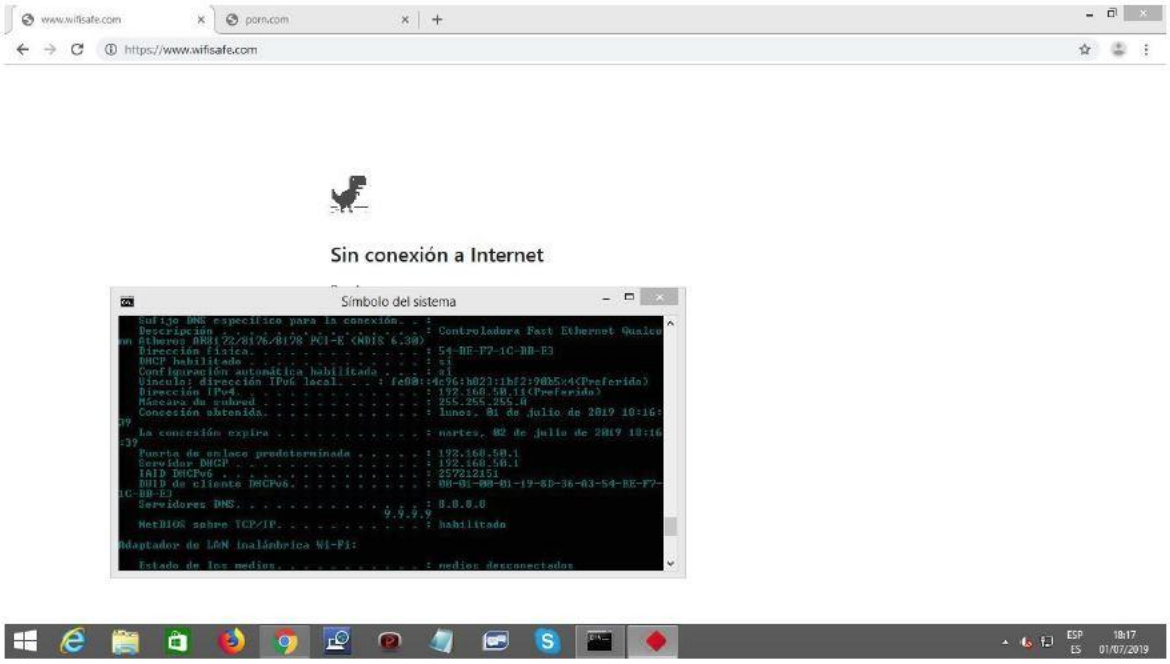
Y por último, nos quedaría activar las reglas, ya que por defecto, son creadas desactivadas. Para activarla, seleccionamos las 3 reglas que hemos creado y hacemos clic en el botón "**Enable**".



Una vez activadas, aparecerá como "**Enable**" en "**Status**".



Ahora, si un usuario cambia las DNS de su equipo, no tendrá acceso a Internet.



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

Contacto: soporte@wifisafe.com