

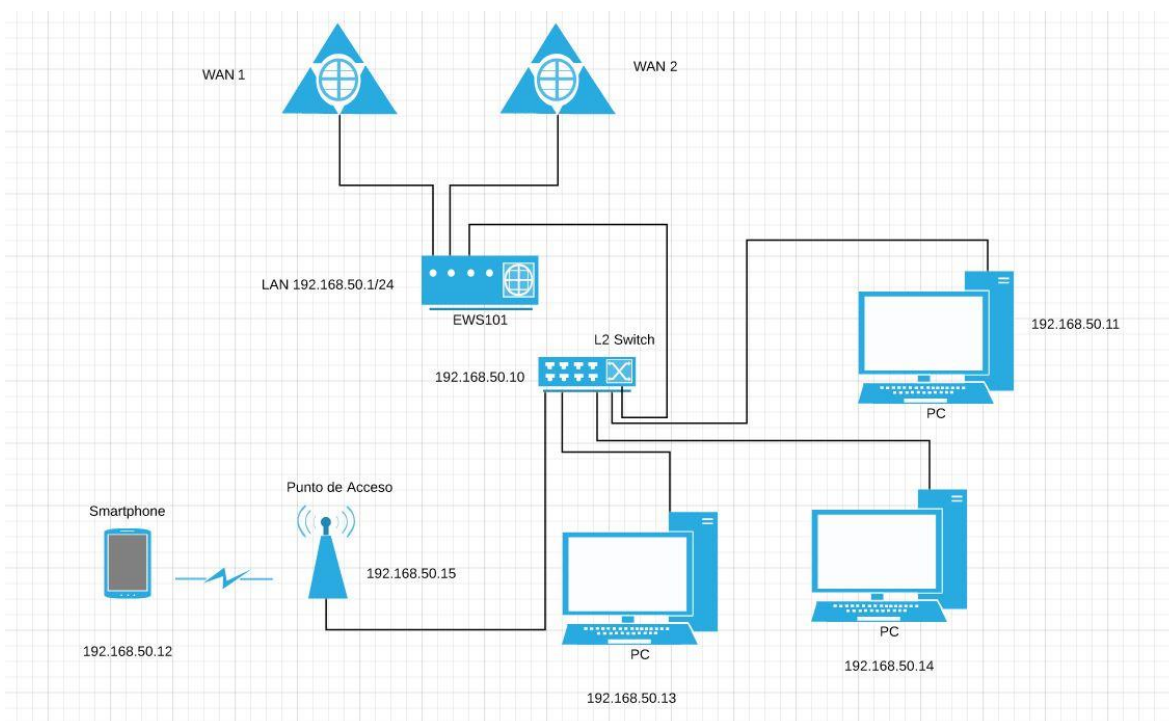


Configuración bloqueo de contenido con DNS WifiCloud con HotSpot Edgecore

(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

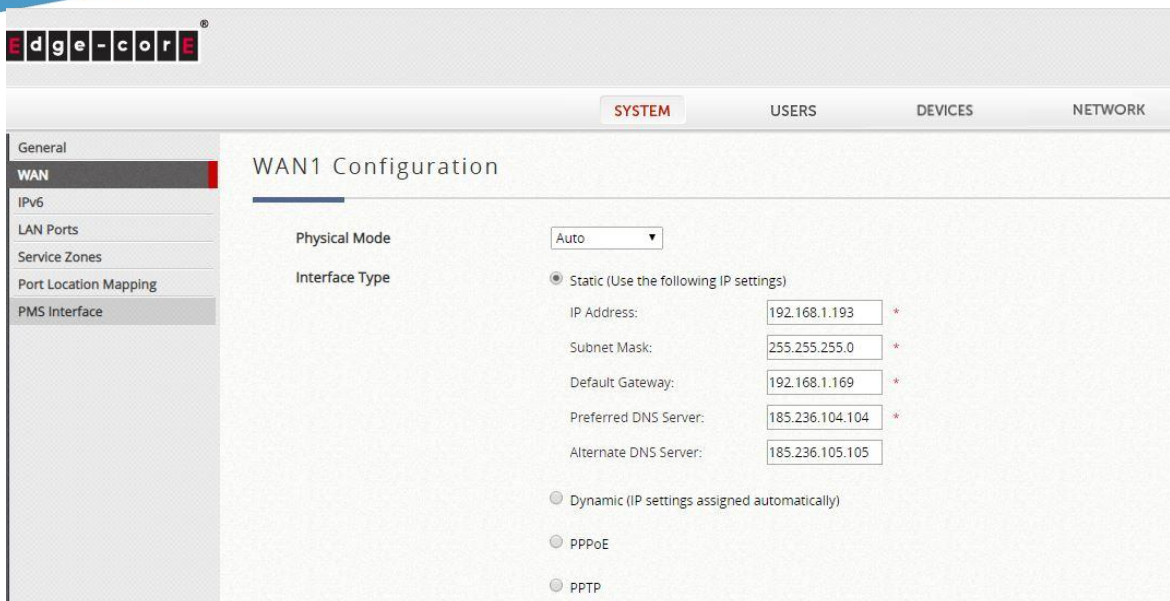
Para esta guía, utilizaremos la misma topología de red que en otras ocasiones. No entraremos en detalles de la configuración de los HotSpot EdgeCore, ya que éste tema, lo hemos tratado en el manual del equipo publicado en la web.



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 **"preferred DNS server"** y **"alternative DNS server"**.

Quedando la configuración de la siguiente forma:



Edge-core

SYSTEM USERS DEVICES NETWORK

General
WAN
IPv6
LAN Ports
Service Zones
Port Location Mapping
PMS Interface

WAN1 Configuration

Physical Mode: Auto

Interface Type: ☒ Static (Use the following IP settings)

IP Address: 192.168.1.193 *

Subnet Mask: 255.255.255.0 *

Default Gateway: 192.168.1.169 *

Preferred DNS Server: 185.236.104.104 *

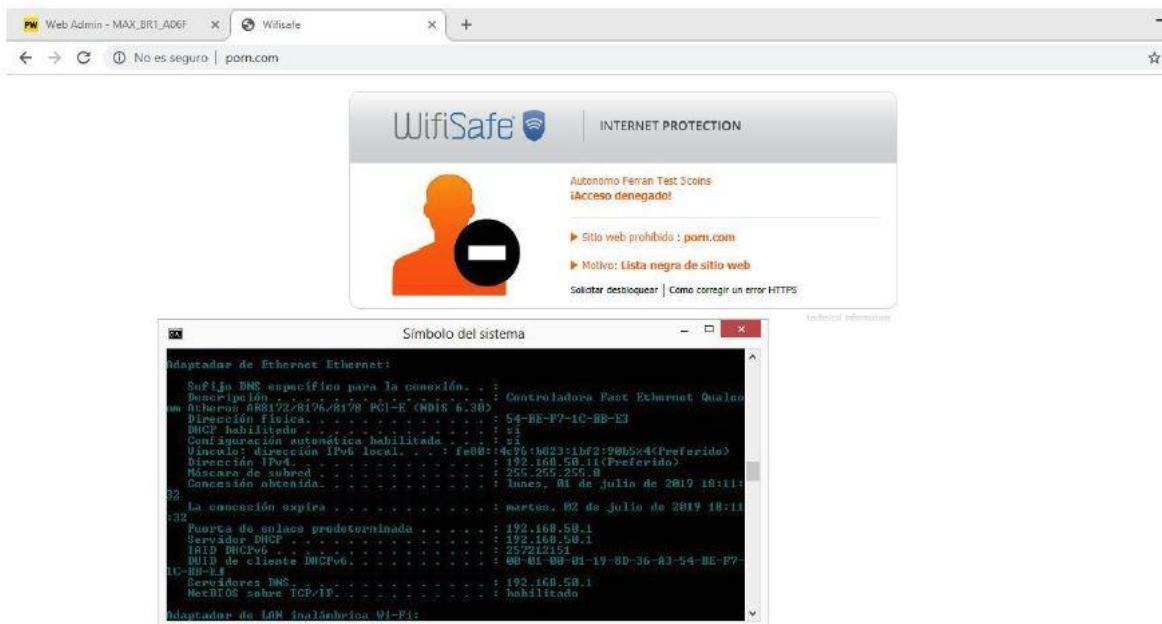
Alternate DNS Server: 185.236.105.105

☐ Dynamic (IP settings assigned automatically)

☐ PPPoE

☐ PPTP

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:



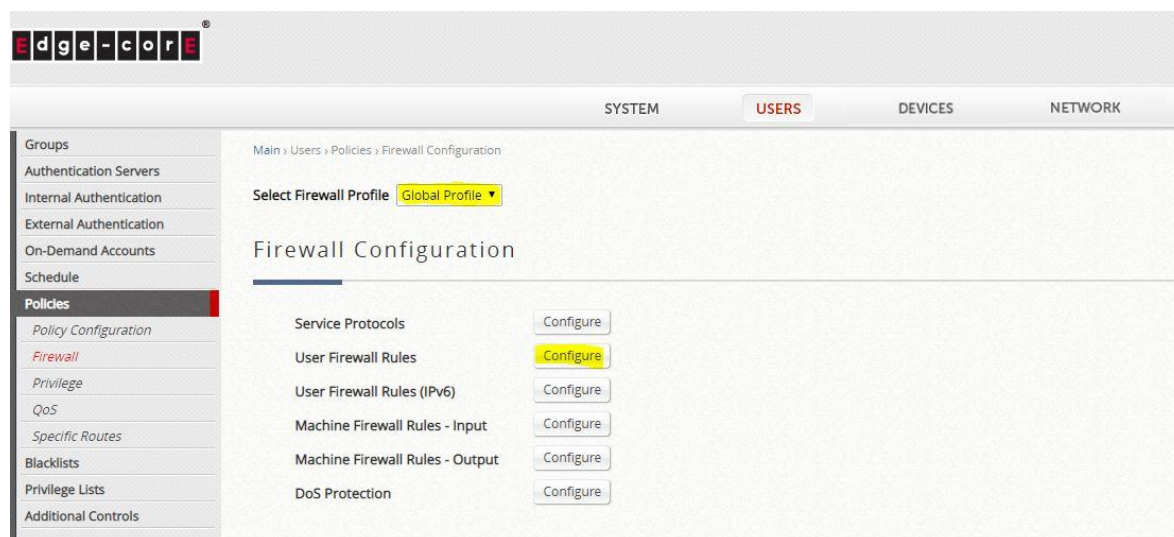
Ahora pasaremos a crear una regla de firewall para prevenir que el usuario cambie manualmente las DNS del equipo y salte el filtro de contenido.

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)

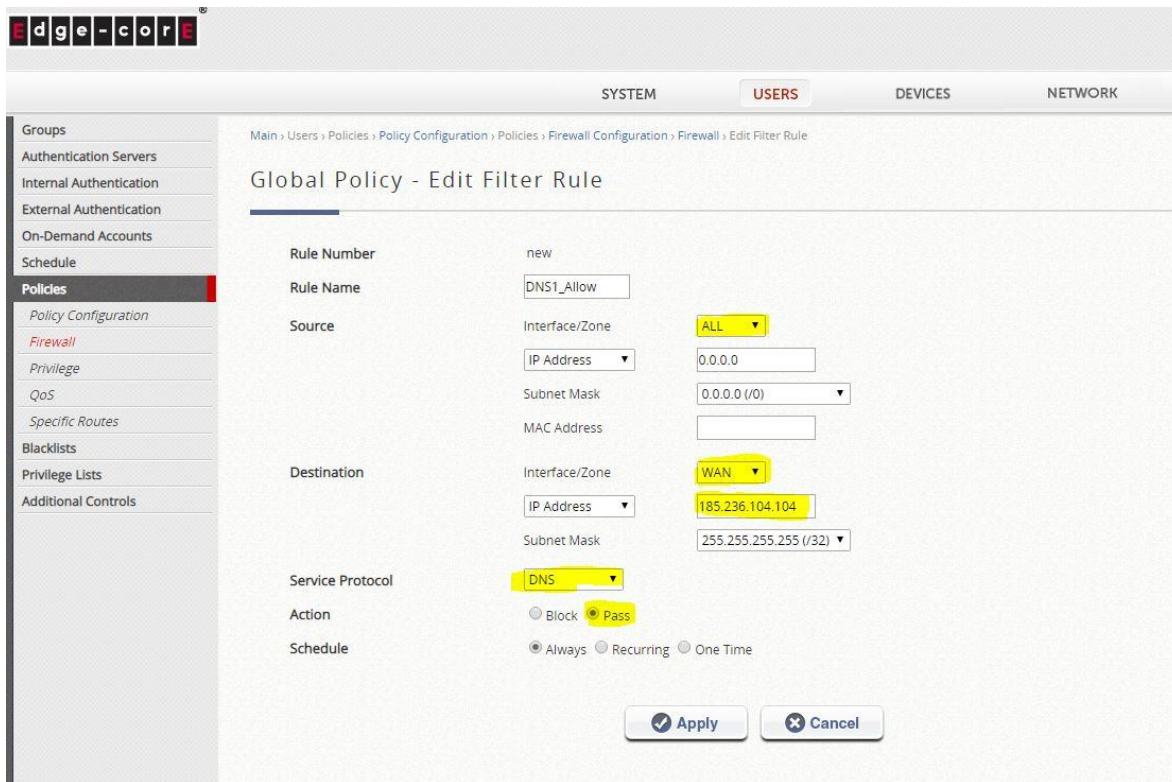
Destination: WAN / **Interface:** IP Address = 185.236.104.104 / **Subnet**

Mask: 255.255.255.255

Service Protocol: DNS

Action: Pass

Quedando la regla de la siguiente manera:



Edge-core

SYSTEM USERS DEVICES NETWORK

Main > Users > Policies > Policy Configuration > Policies > Firewall Configuration > Firewall > Edit Filter Rule

Global Policy - Edit Filter Rule

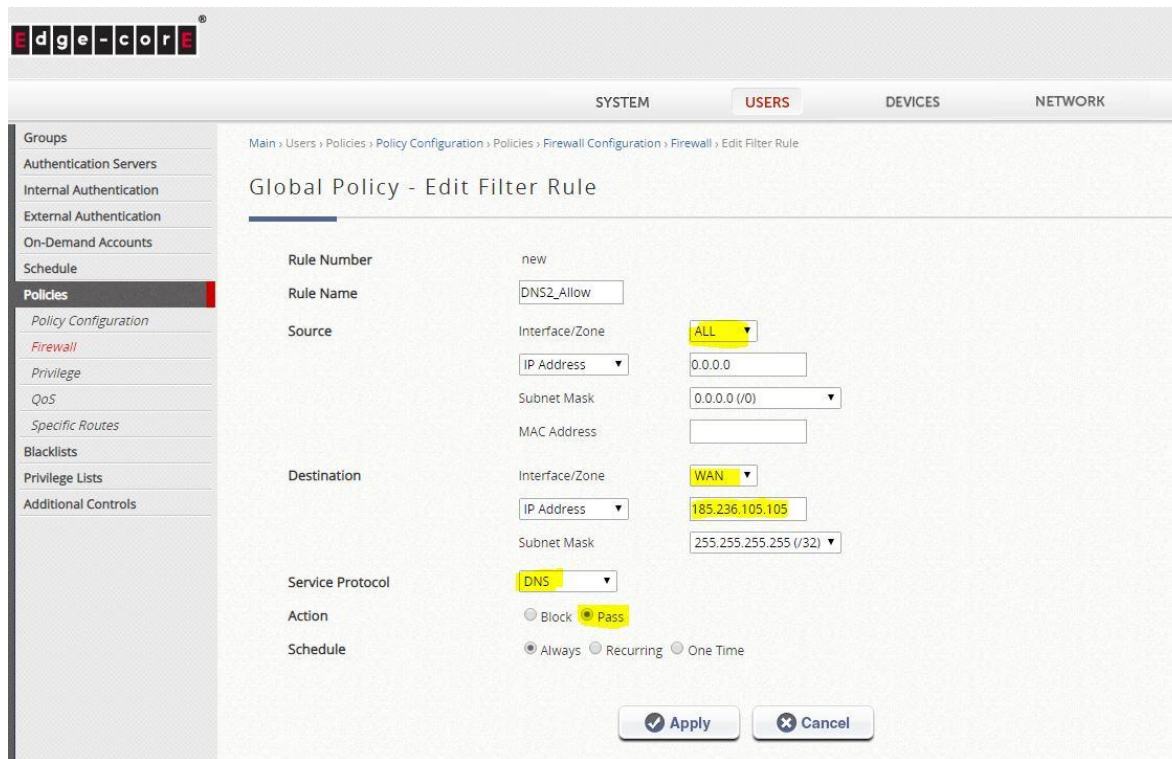
Rule Number	new		
Rule Name	DNS1_Allow		
Source	Interface/Zone	ALL	
	IP Address	0.0.0.0	
	Subnet Mask	0.0.0.0 (/0)	
	MAC Address		
Destination	Interface/Zone	WAN	
	IP Address	185.236.104.104	
	Subnet Mask	255.255.255.255 (/32)	
Service Protocol	DNS		
Action	☐ Block ☒ Pass		
Schedule	☒ Always ☐ Recurring ☐ One Time		

Apply Cancel

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
Action: Pass

Quedando la regla de la siguiente manera:



The screenshot shows the Edge-Core firewall configuration interface. The left sidebar contains a menu with options like Groups, Authentication Servers, Internal Authentication, External Authentication, On-Demand Accounts, Schedule, Policies, Policy Configuration, Firewall, Privilege, QoS, Specific Routes, Blacklists, Privilege Lists, and Additional Controls. The main area is titled 'Global Policy - Edit Filter Rule' and contains the following fields:

- Rule Number:** new
- Rule Name:** DNS2_Allow
- Source:**
 - Interface/Zone: ALL
 - IP Address: 0.0.0.0
 - Subnet Mask: 0.0.0.0 (/0)
 - MAC Address: (empty)
- Destination:**
 - Interface/Zone: WAN
 - IP Address: 185.236.105.105
 - Subnet Mask: 255.255.255.255 (/32)
- Service Protocol:** DNS
- Action:** Block (radio button), Pass (radio button, selected)
- Schedule:** Always (radio button, selected), Recurring (radio button), One Time (radio button)

At the bottom right, there are 'Apply' and 'Cancel' buttons.

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

Action: Block

La regla creada seria quedaría de la siguiente forma:



SYSTEM
USERS
DEVICES
NETWORK

Groups
Authentication Servers
Internal Authentication
External Authentication
On-Demand Accounts
Schedule
Policies
Policy Configuration
Firewall
Privilege
QoS
Specific Routes
Blacklists
Privilege Lists
Additional Controls

Main > Users > Policies > Policy Configuration > Policies > Firewall Configuration > Firewall > Edit Filter Rule

Global Policy - Edit Filter Rule

Rule Number

new

Rule Name

DNS_Block

Source

Interface/Zone

ALL

IP Address

0.0.0.0

Subnet Mask

0.0.0.0 (/0)

MAC Address

Destination

Interface/Zone

WAN

IP Address

0.0.0.0

Subnet Mask

0.0.0.0 (/0)

Service Protocol

DNS

Action

☒ Block
☐ Pass

Schedule

☒ Always
☐ Recurring
☐ One Time

Apply

Cancel

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"**.



SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS

Groups
Authentication Servers
Internal Authentication
External Authentication
On-Demand Accounts
Schedule
Policies
Policy Configuration
Firewall
Privilege
QoS
Specific Routes
Blacklists
Privilege Lists
Additional Controls

Main > Users > Policies > Firewall Configuration > Firewall

Global Firewall Profile - Firewall Rules

Add
Delete
Enable
Disable

☒	No.	Status	Action	Rule Name	Source Source Interface	Destination Destination Interface	Service	Schedule	Operation
☒	1	Disabled	Pass	DNS1_Allow	ANY	185.236.104.104/32	DNS	always	Move
☒	2	Disabled	Pass	DNS2_Allow	ANY	185.236.105.105/32	DNS	always	Move
☒	3	Disabled	Block	DNS_Block	ANY	ANY	DNS	always	Move

(Total:3/40)
First
Prev
Next
Last
Go to Page 1 (Page:1/1)
Row per Page: 20

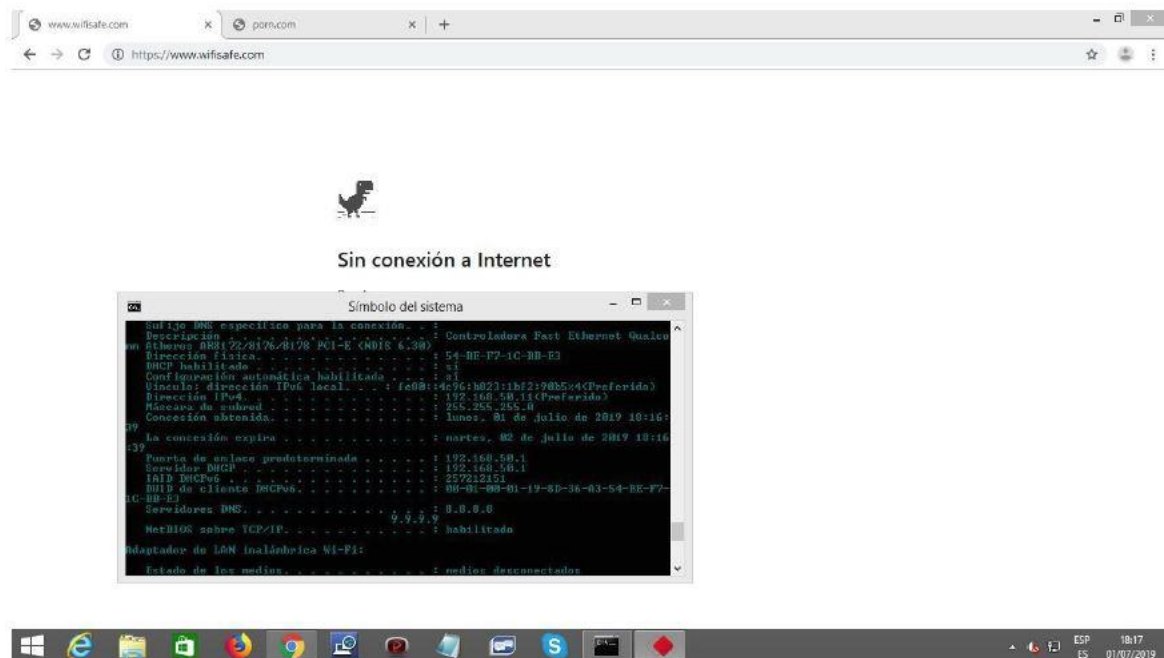
Una vez activadas, aparecerá como **"Enable"** en **"Status"**.

Add Delete Enable Disable

■	No.	Status	Action	Rule Name	Source	Destination	Service	Schedule	Operation
					Source Interface	Destination Interface			
☐	1	Enabled	Pass	DNS1_Allow	ANY	185.236.104.104/32	DNS	always	Move
					ALL	WAN1			
☐	2	Enabled	Pass	DNS2_Allow	ANY	185.236.105.105/32	DNS	always	Move
					ALL	WAN1			
☐	3	Enabled	Block	DNS_Block	ANY	ANY	DNS	always	Move
					ALL	WAN1			

(Total:3/40) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 20

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