

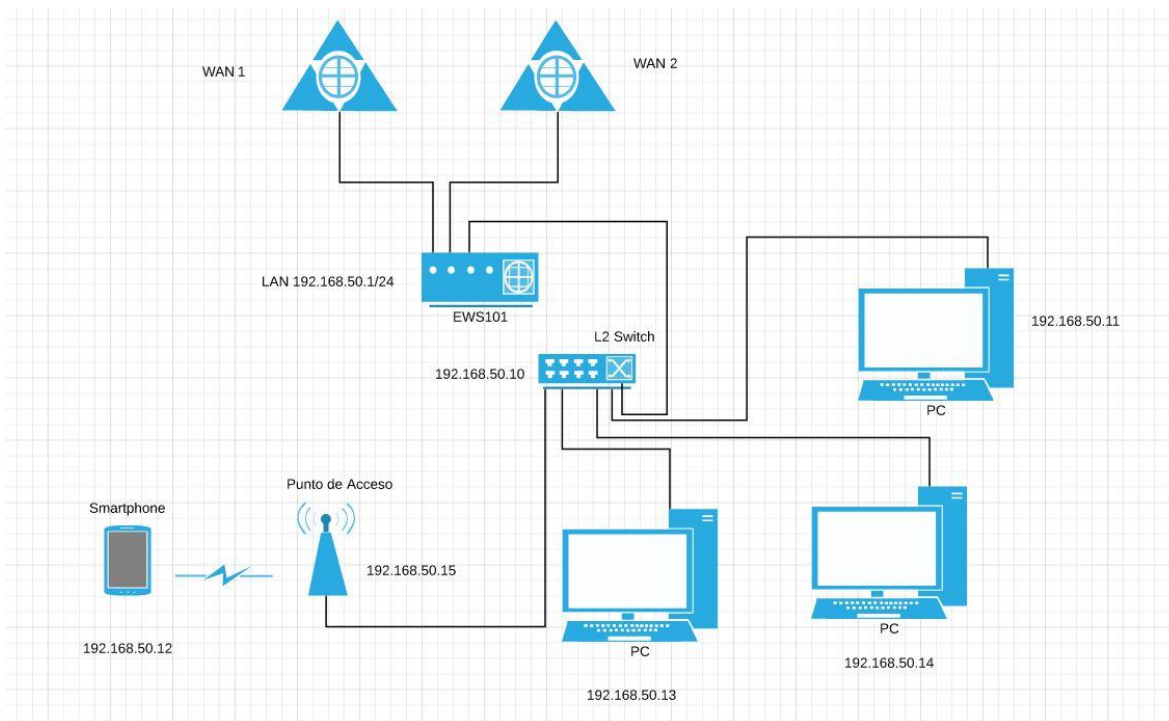


WifiCloud con Peplink Bloquear DNS públicas que no sean de WifiCloud

(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:

PEPWAVE Dashboard **Network** Advanced AP System Status Apply Change

LAN

- Network Settings
- Port Settings
- Captive Portal

WAN

[Logout](#)

Connection Details x

WAN Status

IP Address	192.168.1.219
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.169
Uptime	10 minutes

WAN Connection Settings

WAN Connection Name	WAN Default
Connection Method	Static IP
Routing Mode	<input checked="" type="radio"/> NAT
IP Address	192.168.1.38
Subnet Mask	255.255.255.0 (/24)
Default Gateway	192.168.1.169
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: 185.236.104.104 DNS Server 2: 185.236.105.105
IP Passthrough	<input type="checkbox"/>
Independent from Backup WANs	<input type="checkbox"/>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Reply to ICMP PING	<input checked="" type="radio"/> Yes <input type="radio"/> No
Upload Bandwidth	100 Mbps
Download Bandwidth	100 Mbps

Physical Interface Settings

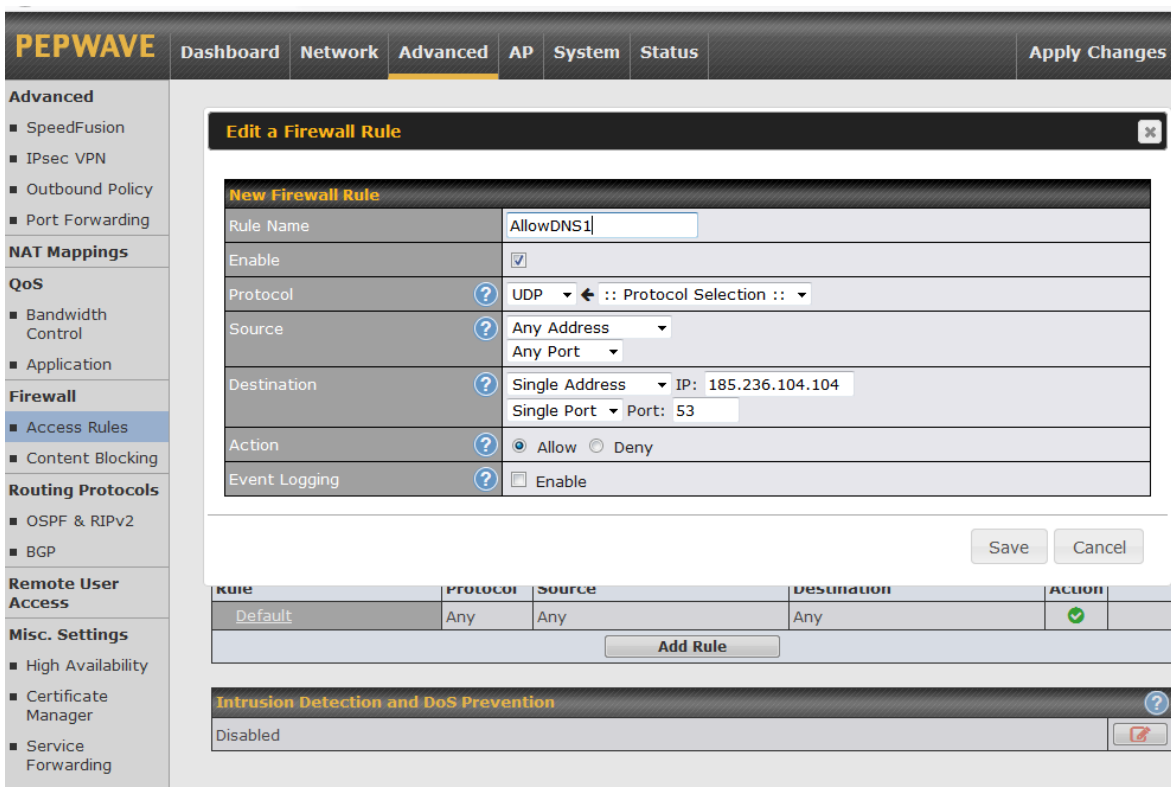
Port Speed	Auto
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: 1440 Default
MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom Value: <input type="text"/>
MAC Address Clone	00 : 1A : DD : ED : 06 : C1 Default

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:



The screenshot shows the PEPWAVE management interface. The 'Advanced' tab is selected, and the 'Firewall' section is active. A 'New Firewall Rule' dialog is open, showing the following configuration:

- Rule Name:** AllowDNS1
- Enable:**
- Protocol:** UDP
- Source:** Any Address, Any Port
- Destination:** Single Address, IP: 185.236.104.104, Single Port, Port: 53
- Action:** Allow
- Event Logging:** Enable

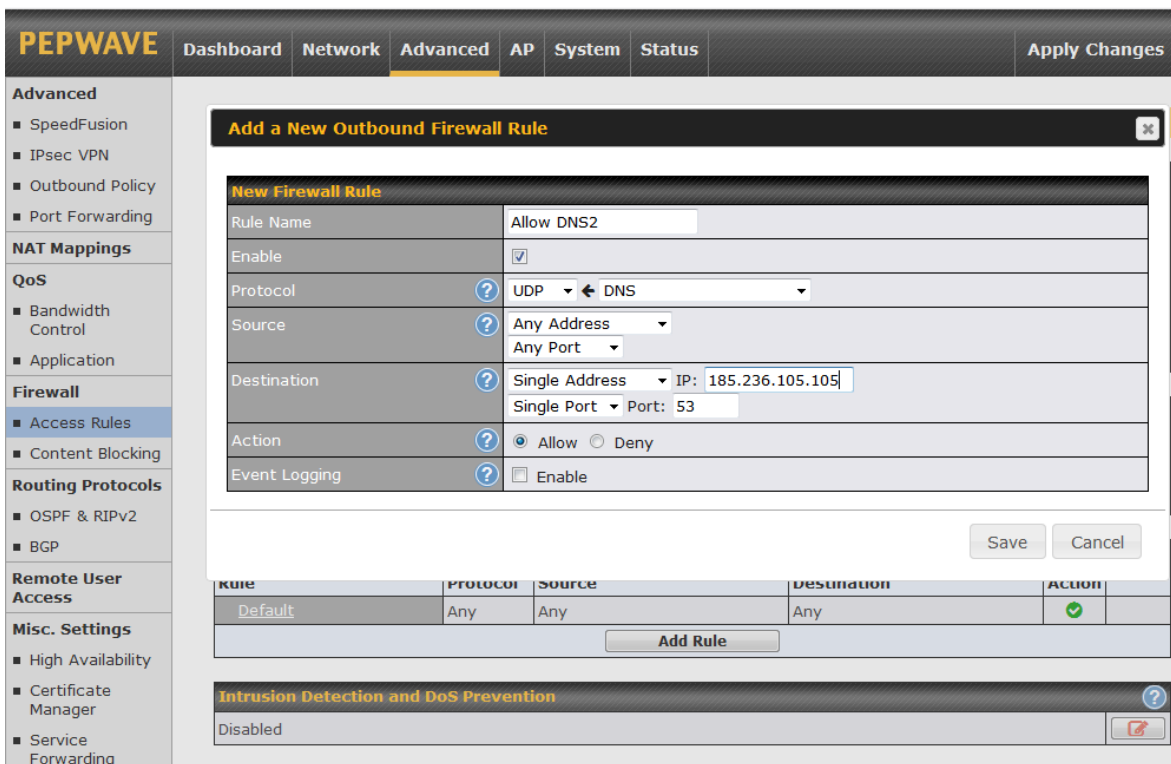
Below the dialog, a table shows the current firewall rules:

Rule	Protocol	Source	Destination	Action
Default	Any	Any	Any	✓

An 'Add Rule' button is visible below the table. At the bottom of the interface, the 'Intrusion Detection and DoS Prevention' section is shown as 'Disabled'.

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:



PEPWAVE Dashboard Network **Advanced** AP System Status Apply Changes

Advanced

- SpeedFusion
- IPsec VPN
- Outbound Policy
- Port Forwarding

NAT Mappings

QoS

- Bandwidth Control
- Application

Firewall

- Access Rules**
- Content Blocking

Routing Protocols

- OSPF & RIPv2
- BGP

Remote User Access

Misc. Settings

- High Availability
- Certificate Manager
- Service Forwarding

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	Allow DNS2
Enable	<input checked="" type="checkbox"/>
Protocol	UDP ← DNS
Source	Any Address Any Port
Destination	Single Address IP: 185.236.105.105 Single Port Port: 53
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

Save Cancel

Rule	Protocol	Source	Destination	Action
Default	Any	Any	Any	✔

Add Rule

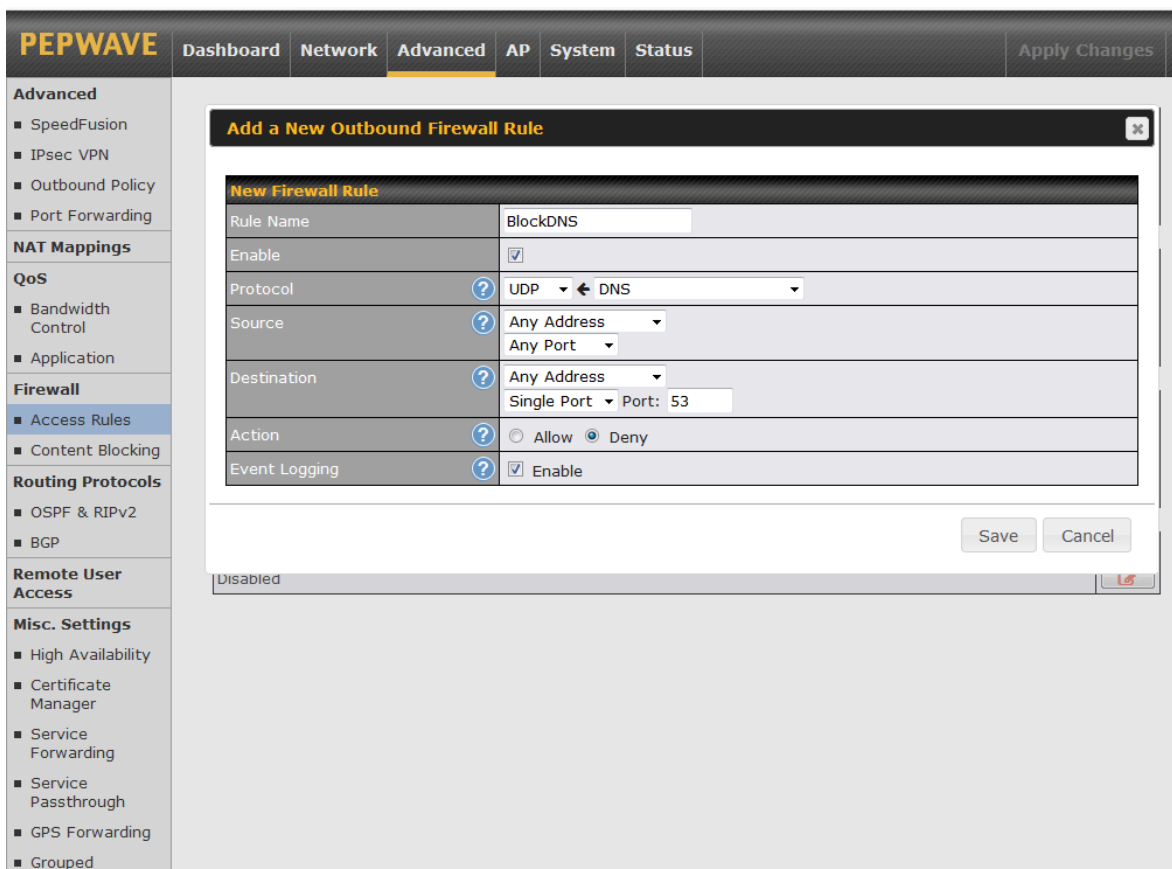
Intrusion Detection and DoS Prevention ?

Disabled ?

Y por último, crearemos una regla, para bloquear el tráfico 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:



The screenshot shows the PEPWAVE web interface with the 'Advanced' tab selected. The left sidebar contains a navigation menu with categories like 'Advanced', 'NAT Mappings', 'QoS', 'Firewall', 'Routing Protocols', 'Remote User Access', and 'Misc. Settings'. The 'Firewall' section is expanded, showing 'Access Rules' as the active sub-section. The main content area displays a form titled 'Add a New Outbound Firewall Rule' for a rule named 'BlockDNS'. The form fields are as follows:

New Firewall Rule	
Rule Name	BlockDNS
Enable	<input checked="" type="checkbox"/>
Protocol	UDP ← DNS
Source	Any Address Any Port
Destination	Any Address Single Port Port: 53
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

At the bottom right of the form are 'Save' and 'Cancel' buttons. Below the form, a status bar indicates 'Disabled'.

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

PEPWAVE Dashboard Network Advanced AP System **Status** Apply Changes

Status

- Device
- Active Sessions
- Client List
- OSPF & RIPv2
- BGP
- Event Log**
- WAN Quality
- Usage Reports
 - Real-Time
 - Hourly
 - Daily
 - Monthly

Logout

Device Event Log

Device Event Log Auto Refresh

Jul 01 17:16:35	Firewall: Denied CONN=lan MAC=[REDACTED] DST=8.8.8.8 LEN=68 TOS=0x00 PREC=0x00 TTL=127 ID=1306 PROTO=UDP SPT=61661 DPT=53 LEN=48 MARK=0x2
Jul 01 17:16:35	Firewall: Denied CONN=lan MAC=[REDACTED] DST=8.8.8.8 LEN=59 TOS=0x00 PREC=0x00 TTL=127 ID=1305 PROTO=UDP SPT=52084 DPT=53 LEN=39 MARK=0x2
Jul 01 17:16:35	Firewall: Denied CONN=lan MAC=[REDACTED] DST=8.8.8.8 LEN=66 TOS=0x00 PREC=0x00 TTL=127 ID=1304 PROTO=UDP SPT=60745 DPT=53 LEN=46 MARK=0x2
Jul 01 17:16:35	Firewall: Denied CONN=lan MAC=[REDACTED] DST=8.8.8.8 LEN=69 TOS=0x00 PREC=0x00 TTL=127 ID=1303 PROTO=UDP SPT=58025 DPT=53 LEN=49 MARK=0x2
Jul 01 17:16:35	Firewall: Denied CONN=lan MAC=[REDACTED] DST=8.8.8.8 LEN=62 TOS=0x00 PREC=0x00 TTL=127 ID=1302 PROTO=UDP SPT=56628 DPT=53 LEN=42 MARK=0x2
Jul 01 17:09:55	System: Changes applied
Jul 01 17:09:17	Admin: admin (192.168.1.4) login successful
Jul 01 17:08:57	WAN: WAN connected (192.168.1.38)
Jul 01 17:08:49	WAN: WAN disconnected
Jul 01 17:08:49	WAN: WAN changes applied
Jul 01 17:02:34	Admin: admin (192.168.1.4) login successful
Jul 01 17:02:13	System: Changes applied
Jul 01 17:01:22	Admin: admin (192.168.50.11) login successful
Jul 01 16:57:48	System: Time synchronization successful

Clear 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:

PEPWAVE Dashboard Network **Advanced** AP System Status Apply Changes

Advanced

- SpeedFusion
- IPsec VPN
- Outbound Policy
- Port Forwarding

NAT Mappings

QoS

- Bandwidth Control
- Application

Firewall

- Access Rules
- Content Blocking

Routing Protocols

- OSPF & RIPV2
- BGP

Remote User Access

Misc. Settings

- High Availability
- Certificate Manager
- Service Forwarding
- Service Passthrough

Outbound Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
AllowDNS1	UDP	Any	185.236.104.104 53	✓	✗
Allow_DNS2	UDP	Any	185.236.105.105 53	✓	✗
BlockDNS	UDP	Any	Any 53	⊘	✗
Default	Any	Any	Any	✓	


Inbound Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	WAN	Source	Destination	Action	
Default	Any	Any	Any	Any	✓	

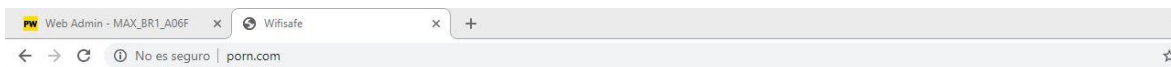
Internal Network Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
Default	Any	Any	Any	✓	

Intrusion Detection and DoS Prevention

Disabled 

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:



WifiSafe  INTERNET PROTECTION

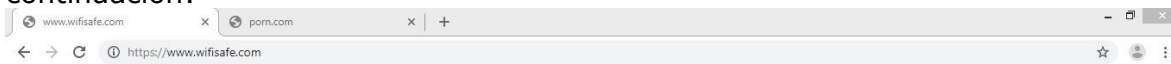
Autonomo Ferran Test Scoins
¡Acceso denegado!

► Sitio web prohibido: **porn.com**
► Motivo: **Lista negra de sitio web**

Solicitar desbloquear | [Cómo corregir un error HTTPS](#)

```
Símbolo del sistema
Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . :
  Descripción . . . . . : Controladora Fast Ethernet Qualco
  Athers 08172/0176/0178 PCI-E <NDIS 6.30> . . . . . :
  Dirección física. . . . . : 54-BE-F7-1C-BB-E3
  DHCP habilitado . . . . . : 1
  Configuración automática habilitada . . . . . : 1
  Vínculo dirección IPv6 local. . . . . : fe80::4c96:b823:1bf2:90b5a4<Preferido>
  Dirección IPv4. . . . . : 192.168.50.11<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Concesión obtenida. . . . . : lunes, 01 de julio de 2019 18:11:
  La concesión expira . . . . . : martes, 02 de julio de 2019 18:11:
  Puerta de enlace predeterminada . . . . . : 192.168.50.1
  Servidor DHCP . . . . . : 192.168.50.1
  IRID DHCPv6 . . . . . : 257212151
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-8D-36-A3-54-BE-F7-
  1C-BB-E3
  Servidores DNS. . . . . : 192.168.50.1
  NetBIOS sobre TCP/IP. . . . . : habilitado
Adaptador de LAN inalámbrica Wi-Fi:
  Estado de los medios. . . . . : medios desconectados
```

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



Sin conexión a Internet

```
Símbolo del sistema
Sufijo DNS específico para la conexión. . . :
  Descripción . . . . . : Controladora Fast Ethernet Qualco
  Athers 08172/0176/0178 PCI-E <NDIS 6.30> . . . . . :
  Dirección física. . . . . : 54-BE-F7-1C-BB-E3
  DHCP habilitado . . . . . : 1
  Configuración automática habilitada . . . . . : 1
  Vínculo dirección IPv6 local. . . . . : fe80::4c96:b823:1bf2:90b5a4<Preferido>
  Dirección IPv4. . . . . : 192.168.50.11<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Concesión obtenida. . . . . : lunes, 01 de julio de 2019 18:16:
  La concesión expira . . . . . : martes, 02 de julio de 2019 18:16:
  Puerta de enlace predeterminada . . . . . : 192.168.50.1
  Servidor DHCP . . . . . : 192.168.50.1
  IRID DHCPv6 . . . . . : 257212151
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-8D-36-A3-54-BE-F7-
  1C-BB-E3
  Servidores DNS. . . . . : 8.8.8.8
  NetBIOS sobre TCP/IP. . . . . : 9.9.9.9 habilitado
Adaptador de LAN inalámbrica Wi-Fi:
  Estado de los medios. . . . . : medios desconectados
```



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

Contacto: soporte@wifisafe.com