

experiencia con el hotspot del mikrotik



[1]

creado: Lun, 12/07/2010 - 10:50 — [eloi.rebes](#) [1] actualizado: 11/08/2015 - 6:04am

Bien, en este manual agrupo los pasos para montar un hotspot muy útil en un mikrotik. Yo fui el apuntador y en Sebas quien iba configurando. Este hotspot se encuentra en el Far de SantSebastià de Llafranc de Palafrugell. Situado a 1km de la playa, donde no puede ser utilizado desde cerca del mar, pero si desde el mirador del Far. Ofreciendo acceso a internet durante 1h y con un caudal de 256K por usuario, con una media de unos 10 usuarios en las primeras semanas del verano del 2010.

Los requisitos para poder realizarlo:

-Supernodo con mikrotik.

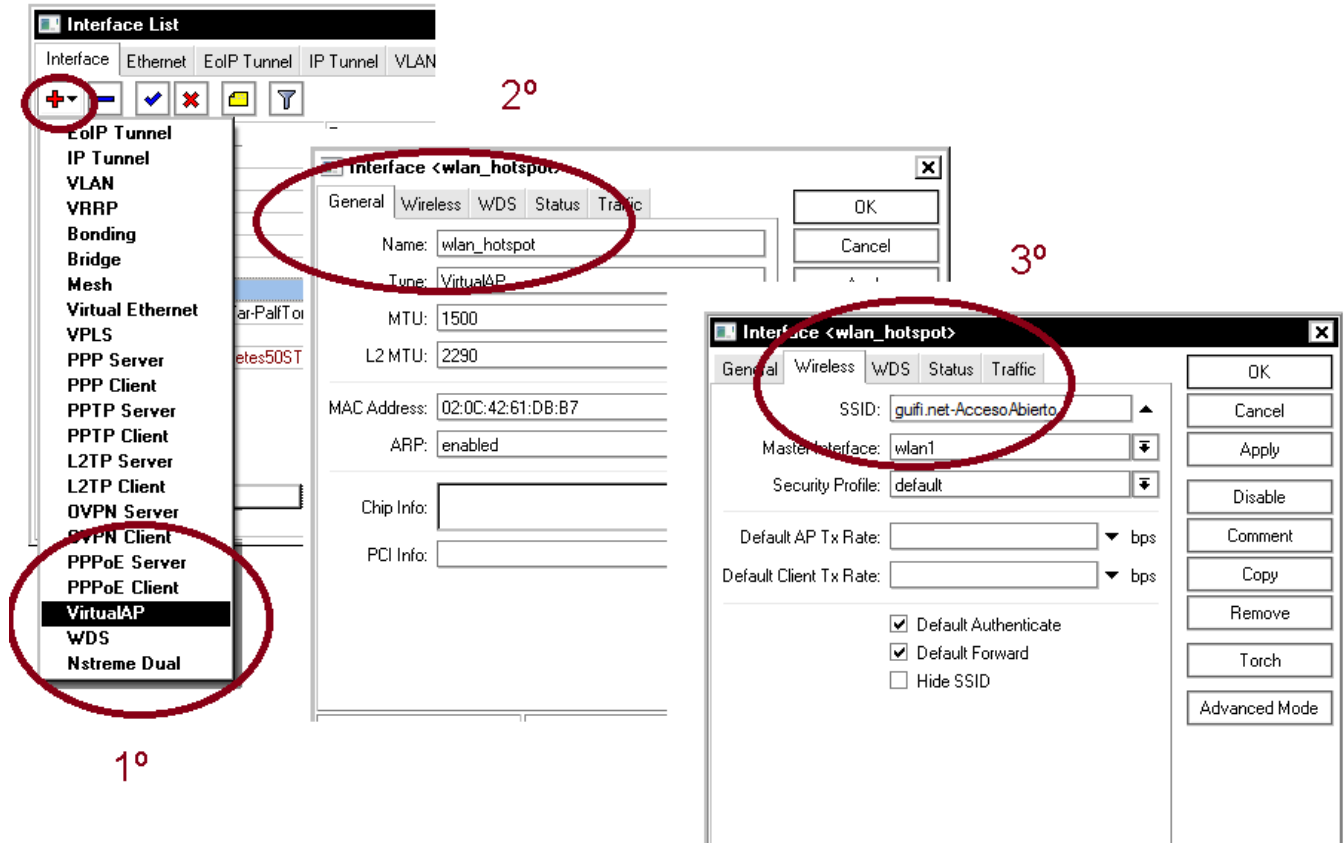
-AP sectorial donde se creará el hotspot. No se recomienda antenas omnidireccionales, al conectar un portatil disminuye el rendimiento de la antena. (nota: si fueran 2 APs, se recomienda crear un bridge entre los 'bridge' de los dos APs, porque si no los usuarios tendrian 2 hotspots con 2h al dia. Información de como hacerlo... al punto 13).

-Un servidor donde este un proxy federado. (transparente no, que no permite el protocolo https, el puerto 443, y es necesario para ver el correo, conectarse a las redes sociales, etc)

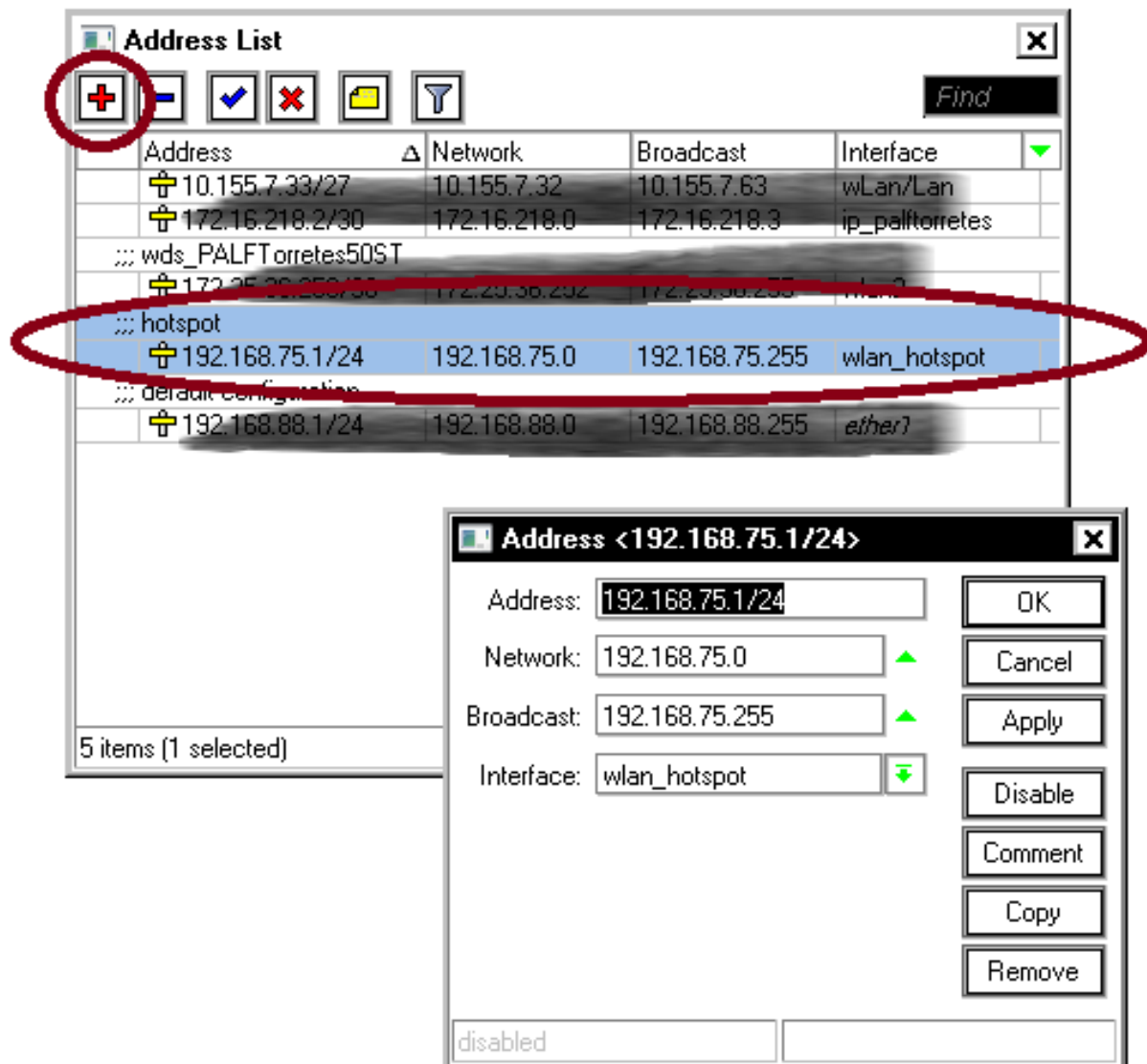
-En este caso hemos utilizado un servidor en Debian, para crear un túnel para el https. Hemos de crear un túnel porque la conexión segura (https) no puede ser redirigida.

Proceso:

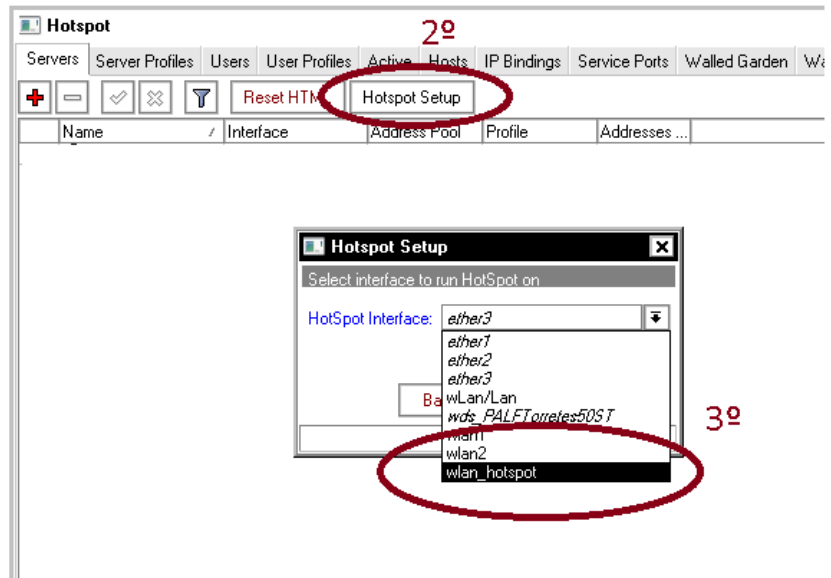
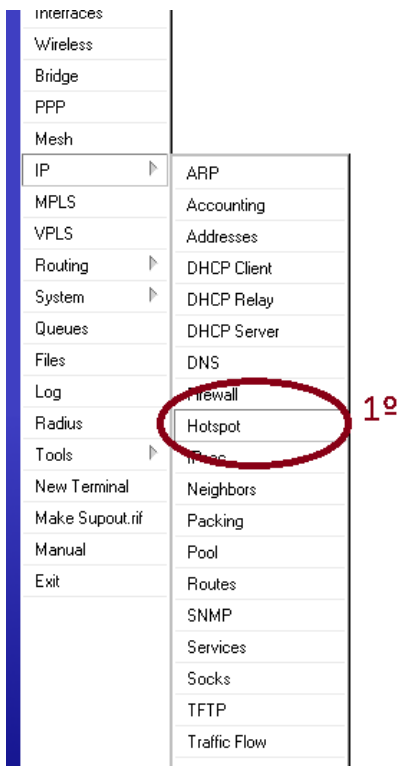
1º- Creamos la nueva antena virtual: Interfaces > Añadir > VirtualAP, y la asociamos a la antena donde queremos ofrecer cobertura del hotspot.



2º- Creamos un nuevo rango de IPs para los usuarios del hotspot... por ejemplo 192.168.75.1/24



3º- Ya podemos comenzar con el asistente del hotspot: indicar el virtualAP creada, y él solito ya nos indicara los valores necesarios siguientes... eso si, comprobamos que correspondan.



nota: vereis que os ha generado reglas al firewall, para poder funcionar correctamente

4º- El asistente crea los datos necesarios, pero hace falta modificar algunos valores:

The screenshot shows the Mikrotik WinBox DHCP Server configuration interface. At the top, there are tabs for 'DHCP', 'Networks', 'Leases', 'Options', and 'Alerts'. Below these are buttons for '+', '-', checkmark, 'x', and a filter icon, followed by 'DHCP Config' and 'DHCP Setup' buttons.

Name	Interface	Relay	Lease Time	Address Pool	Add
dhcp-wlan/Lan	wlan/Lan		3d 00:00:00	dhcp-wlan/L...	no
dhcp1	wlan_hotspo		1d 00:00:00	hs-pool-12	no

The configuration dialog for 'dhcp1' is open, showing the following fields:

- Name: dhcp1
- Interface: wlan_hotspot
- Relay: (empty)
- Lease Time: 1d 00:00:00 (circled in red)
- Address Pool: hs-pool-12
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: after 2s delay
- Bootp Support
- Add ARP For Leases
- Always Broadcast
- Use RADIUS

Buttons on the right side of the dialog include OK, Cancel, Apply, Disable, Copy, and Remove. At the bottom left of the main window, it says '2 items (1 selected)'.

modificamos el valor de guardar la ip a 1 día, al dhcp que ha creado el asistente del hotspot, para coincidir la ip reservada con la mac registrada al hotspot.

Hotspot Servers

Name	Interface	Address Pool	Profile	Addresses ...
hotspot1	wlan_hotspot	hs-pool-12	hsprof1	1

Hotspot Server <hotspot1>

Name: hotspot1
 Interface: wlan_hotspot
 Address Pool: hs-pool-12
 Profile: hsprof1
 Idle Timeout: 00:05:00
 Keepalive Timeout:
 Addresses Per MAC: 1
 IP of DNS Name: 0.0.0.0
 Proxy Status: running

Hotspot Server Profiles

Name	DNS Name	HTML Directory	Rate Limit (rx/tx)
hsprof1	hotspot	hotspot	

Hotspot Server Profile <hsprof1>

Name: hsprof1
 Hotspot Address: 192.168.75.1
 DNS Name:
 HTML Directory: hotspot
 Rate Limit (rx/tx):
 HTTP Proxy: 10.x.x.x
 HTTP Proxy Port: 3128
 SMTP Server:
 Status: disabled

Hotspot Server Profile <hsprof1>

General Login RADIUS

MAC HTTP CHAP Cookie
 HTTP PAP HTTPS Trial

MAC Auth. Password:
 HTTP Cookie Lifetime: 3d 00:00:00
 SSL Certificate: none
 Split User Domain
 Trial Uptime Limit: 01:00:00
 Trial Uptime Reset: 1d 00:00:00
 Trial User Profile: default

a *HTTP Proxy* poneis un proxy a utilizar, también su puerto

donde pone *Trial Uptime Limit: 01:00:00* quiere decir que permitiremos 1h de acceso, si quereis 30min pondremos 00:30:00

a *Trial Uptime Reset* es el valor a coincidir con la ip guardada del servidor dhcp (comentado 3 imagenes atras)

The screenshot shows the Mikrotik Hotspot configuration interface. At the top, there are tabs for 'Server Profiles', 'Users', 'User Profiles', 'Active', 'Hosts', 'IP Bindings', 'Service Ports', 'Walled Garden', and 'Walled Garder'. Below these are icons for adding, deleting, and filtering. A table lists the user profiles, with the 'default' profile selected and circled in red. The table has columns for Name, Session Time..., Idle Timeout, Shared U..., and Rate Limit (rx/tx). The 'default' profile has a Name of 'default', Session Time of 'none', Idle Timeout of 'none', Shared U... of '100', and Rate Limit (rx/tx) of '256K/256K'. Below the table, it says '1 item (1 selected)'. A dialog box titled 'Hotspot User Profile <default>' is open, showing the configuration for the selected profile. The dialog has tabs for 'General', 'Advertise', and 'Scripts'. The 'General' tab is active, showing fields for Name (default), Address Pool (none), Session Timeout, Idle Timeout (none), Keepalive Timeout (00:02:00), Status Autorefresh (00:01:00), Shared Users (100), Rate Limit (rx/tx) (256K/256K), Address List, Incoming Filter, Outgoing Filter, Incoming Packet Mark, Outgoing Packet Mark, Open Status Page (HTTP login), and a checked 'Transparent Proxy' checkbox. The 'Shared Users' and 'Rate Limit (rx/tx)' fields are circled in red. The 'Open Status Page' field is also circled in red. The dialog has buttons for OK, Cancel, Apply, Copy, and Remove.

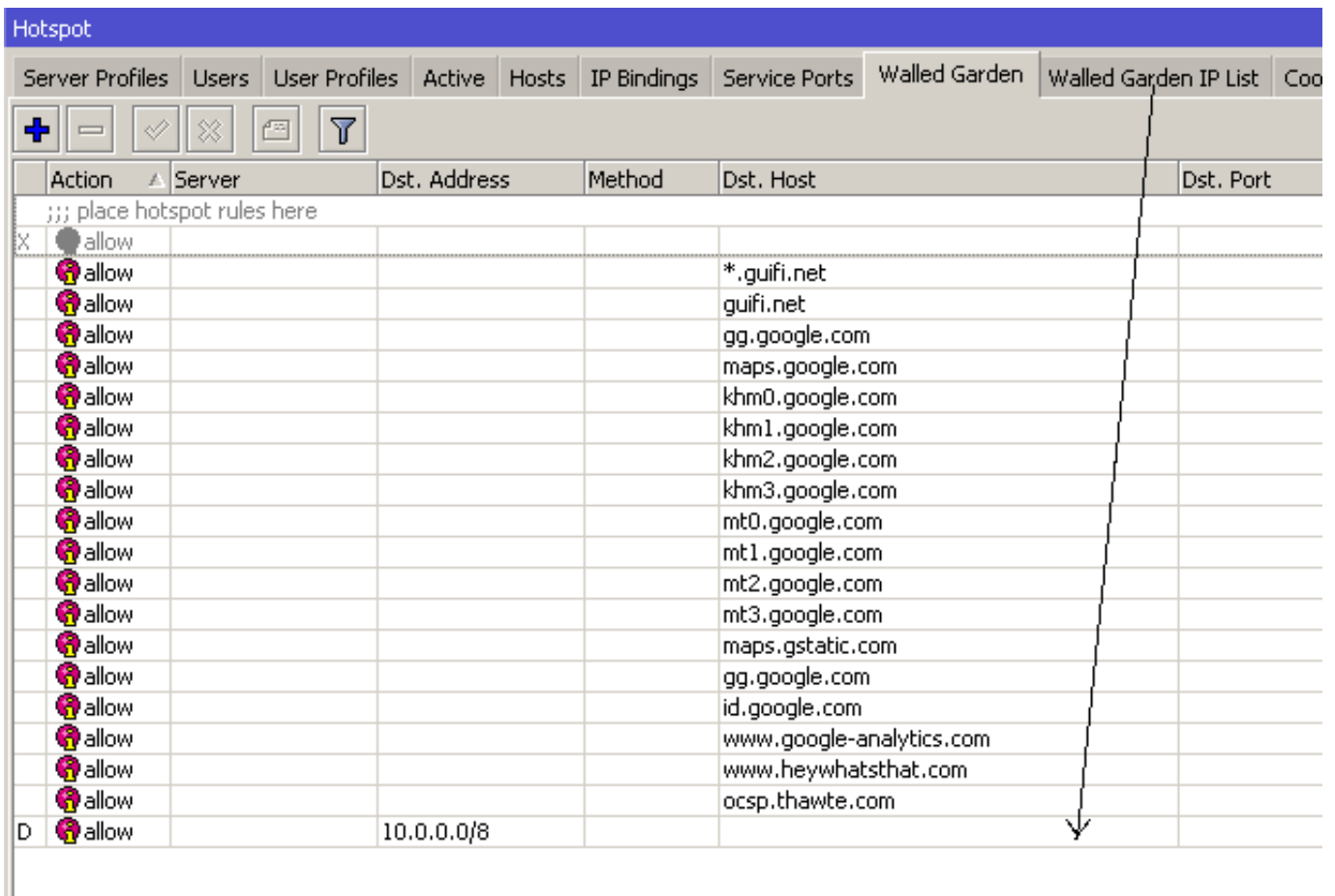
Share Users son los usuarios simultáneos, y *Rate Límit* el caudal por usuario, si quereis poner 1 mega por usuario seria 1M/1M

(tendreis que modificar la web del hotspot indicando el caudal limitado a 1Mbps, en vez de 256Kbps)

5º- Extraigo la lista de las páginas blancas(páginas permitidas siempre), para no tener que introducir una a una. Solo hay de pegar en el terminal. Son las webs donde siempre se podran visitar, incluso con la hora diaria finalizada.

[codigo a pegar al terminal del mikrotik](#) [2] (podeis hacer un "guardar como..." o clicar y se abrirá una ventana nueva)

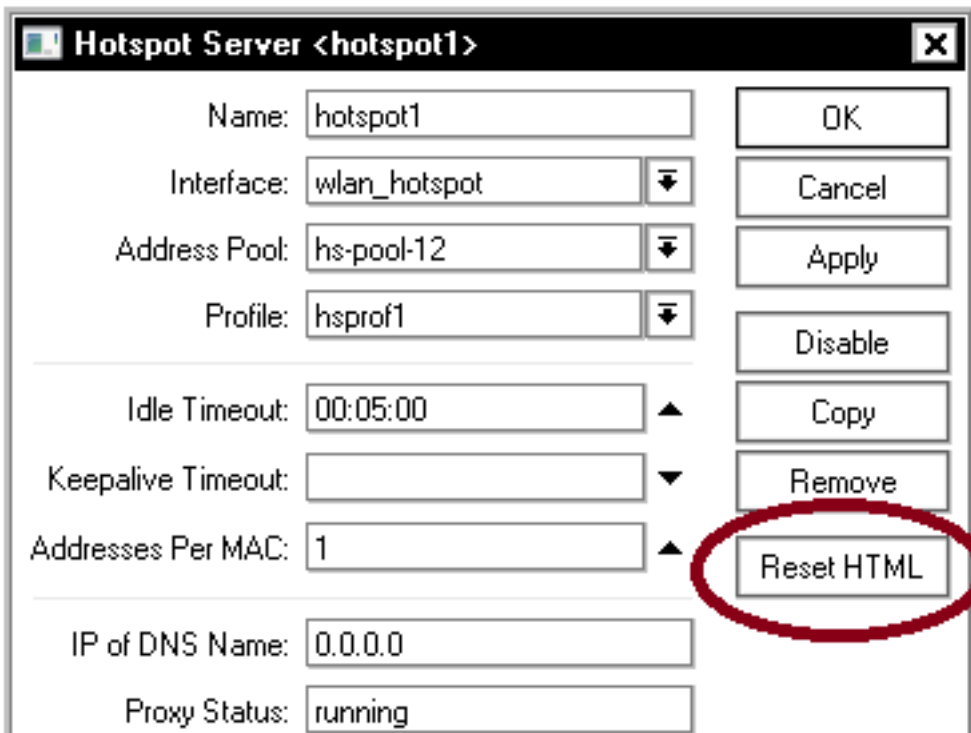
quedará así:



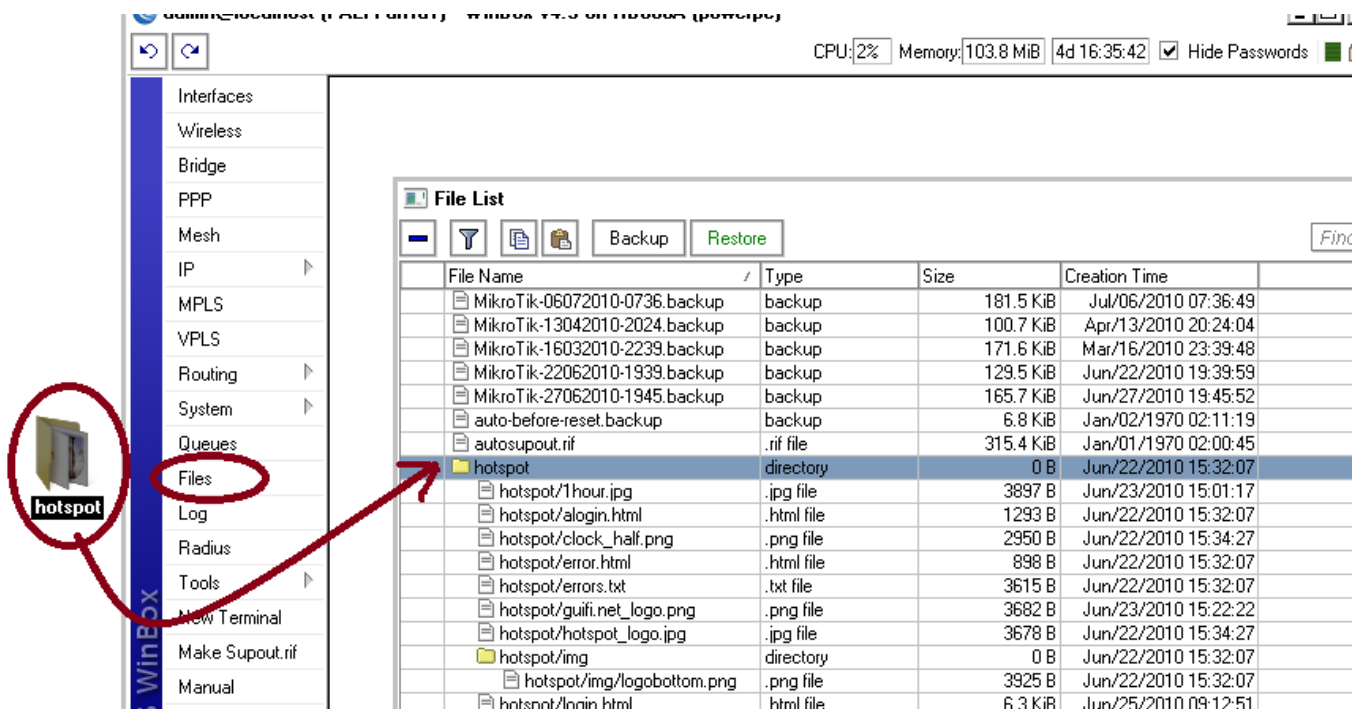
la mayoría de estos enlaces de páginas blancas son de los mapas de google para verlos en la web de guifi, tambien todos los dominios de guifi, y tambien permite acceder a cualquier contenido de la red de guifi (=10.0.0.0/8, que es muy importante para dar acceso a la red de forma separada del sistema hotspot, es decir, que si se acaba el tiempo de conexión directa a Internet siempre tengamos acceso a la red de guifi, ya que por licencia tenemos que garantizar el libre acceso a la red, como así recoge la XOLN [3])

(la última línea de esta lista se crea automáticamente ya que el código lo introduce a Walled Garden IP List)

6º- Importamos los ficheros de la web del hotspot, a la carpeta correspondiente del mikrotik.



nota: si alguien ya habia creado alguna web hotspot y quiere dejarlo de fábrica, clicar sobre "Reset HTML"



[web hotspot \(versión 1h\)](#) [4]

[web hotspot \(versión 30min\)](#) [5]

ponemos una página donde podeis cojer ideas, o dejarla tal com está

(lo más importante són los valores que necesita el mikrotik para validar el usuario, que es el botón de "clicar para comenzar a navegar")

7º- Añadir las IPs del mikrotik y del servidor donde esté el tunel creado a las ACLs del proxy

The screenshot shows two parts of the Mikrotik WinBox interface. The top part, labeled '1º Creació d'ACL', shows the 'Adreces Client ACL' configuration. The 'Nom d'ACL' field is set to 'hotspot'. The 'Des de la IP' field has two entries: '10.mikrotik' and '10.servidor'. The bottom part, labeled '2º Control d'Accés', shows the 'Restriccions de proxy' tab. A table lists various ACLs with their actions. The 'hotspot' entry is circled in red, showing a 'Permet' action.

1º Creació d'ACL

Adreces Client ACL

Nom d'ACL: hotspot

Des de la IP: 10.mikrotik, 10.servidor

Màscara de subxarxa: [empty]

URL d'error: [empty]

Emmagatzema els valors de l'ACL al fitxer: [empty]

Desa | Suprimeix

Torna a la llista d'ACLs | Torna a l'índex

2º Control d'Accés

Listes de control d'accés | Restriccions de proxy | Restriccions ICP | Programes ACL externs | Resi

Afegeix restricció de proxy.

Acció	ACLs
<input type="checkbox"/> Permet	manager localhost
<input type="checkbox"/> Denega	manager
<input type="checkbox"/> Permet	purge localhost
<input type="checkbox"/> Denega	purge
<input type="checkbox"/> Denega	!Safe_ports
<input type="checkbox"/> Denega	CONNECT !SSL_ports
<input type="checkbox"/> Permet	localhost
<input type="checkbox"/> Permet	hotspot
<input type="checkbox"/> Permet	usuaris_authenticats
<input type="checkbox"/> Denega	all

Afegeix restricció de proxy.

Suprimeix les Restriccions Seleccionades

- comprobamos si hay algún problema con las ACLs creadas: > squid -k parse
- reiniciamos el Squid: > /etc/init.d/squid reload

nota: Si utilizamos un proxy federado habrá que crear con el acceso permitido a las IPs del mikrotik y del propio servidor donde estará el otro punto del túnel, o sea el propio proxy.

Hasta aquí hecho el hotspot simple, o básicamente con el protocolo http. Ara montamos un túnel entre el mikrotik y un servidor donde esté un proxy, para redirigir el protocolo seguro https.

8º- Añadir el túnel al fichero de configuración a INTERFACES, para montarlo en arrancar el sistema.

```
up ip tunnel add ip_tunnel_srv mode
  ipip remote 10.x.x.x(mikrotik)
  local 10.x.x.x(servidor)

up ifconfig ip_tunnel_srv
  172.16.218.1 netmask
  255.255.255.252 up
```

```

up iptables -t nat -A POSTROUTING
-s 172.16.218.2 -j MASQUERADE

down iptables -t nat -D POSTROUTING
-s 172.16.218.2 -j MASQUERADE

down ip tunnel del ip_tunnel_srv mode
ipip remote 10.x.x.x(mikrotik) local
10.x.x.x(servidor)
    
```

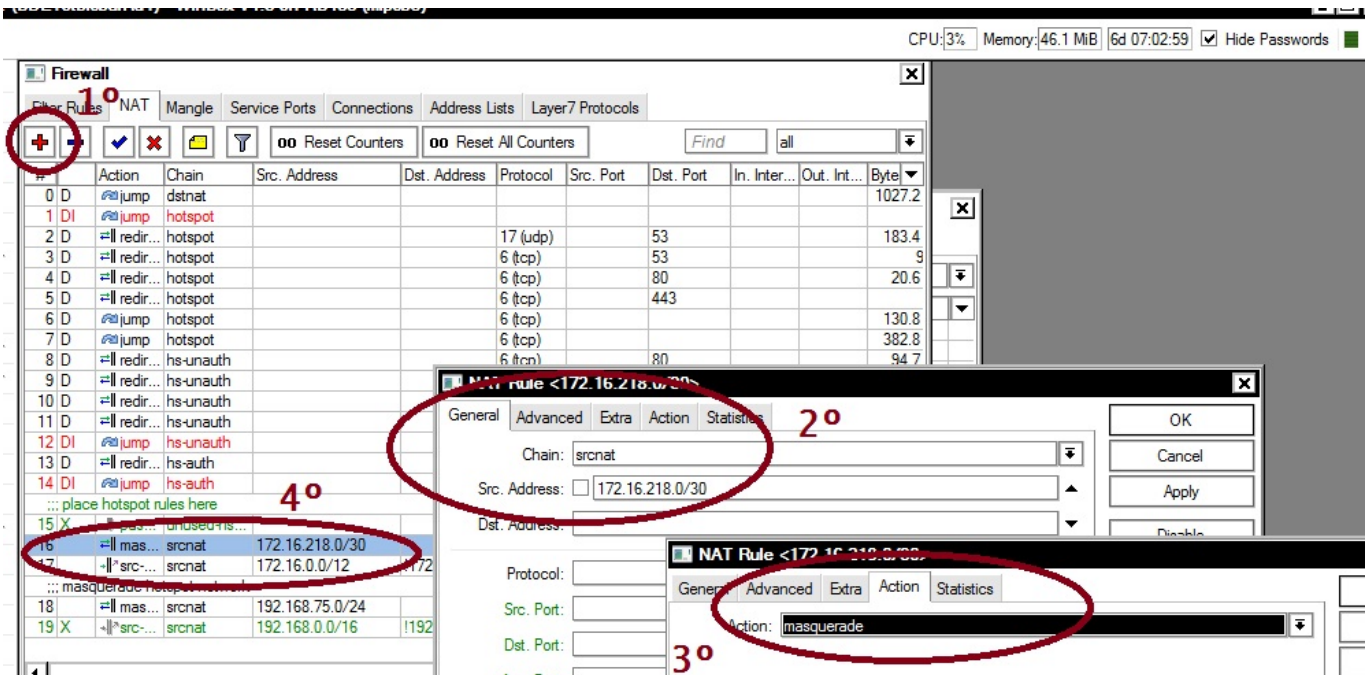
nota: todo lo que está en negreta es lo que hay que cambiar para vuestro caso,

a remote poner la IP del mikrotik y a local la del servidor,

les 172.16.x.1 la ip del del servidor y 172.16.x.2 la ip del mikrotik (se recomiendan dejar tal como estan)

nota: vigilar si teneis 2 tarjetas de red(normalmente es así), la de guifi y la del adsl... va dentro de la de guifi

9º- Añadir otra regla nat al firewall



En el 4º punto muestra la posición de la nueva regla, que tiene que estar por encima de la que introduce el "unsolclick"

10º- Añadir el otro punto del túnel al mikrotik

1º

2º

3º

4º

nota: los valores en rojo, tenéis que poner los vuestros

11º- Marcar los paquetes del protocolo https que salgan del hotspot para redirigirlos a través del túnel creado.

+

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	mark routing	prerouting	192.168.75.0/24		6 (tcp)		443			23.5 MIB	127 828

Mangle Rule <192.168.75.0/24->443>

Chain: prerouting

Src. Address: 192.168.75.0/24

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 443

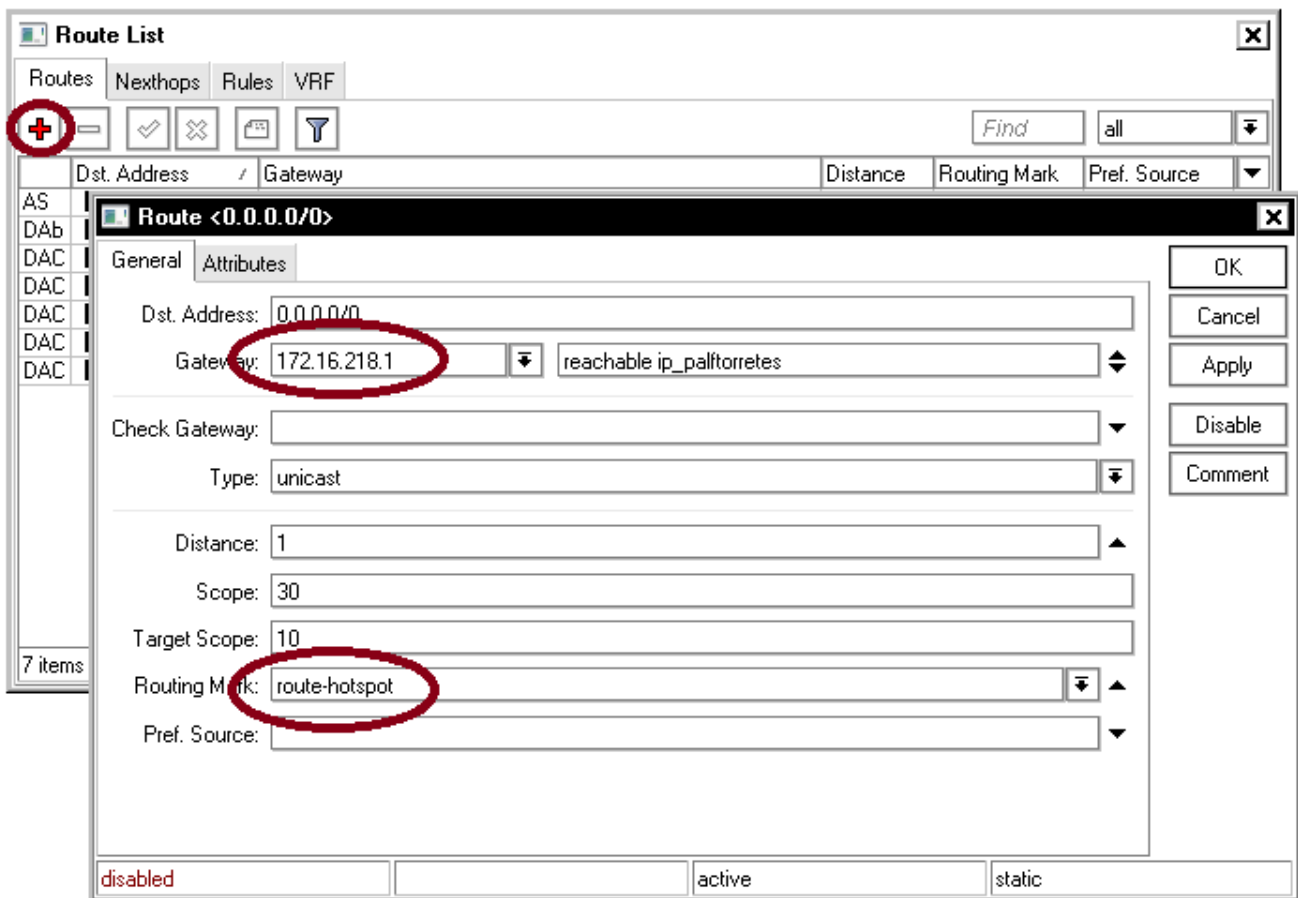
Mangle Rule <192.168.75.0/24->443>

Action: mark routing

New Routing Mark: route-hotspot

Passthrough

a *New Routing Mark* hay que poner un nombre, podeis escogerlo si quereis



12º- Dejar pasar hacia internet los paquetes HTTPS que llegan del mikrotik

Editar el archivo `/etc/sysctl.conf` y descomentar la línea (sacar el símbolo #)

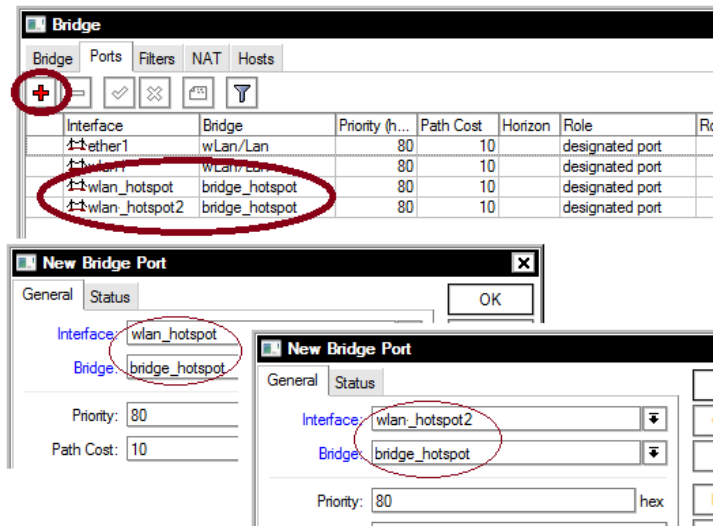
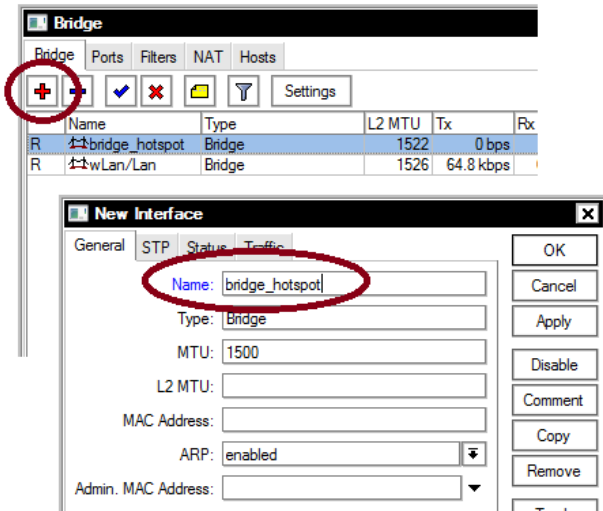
```
#net.ipv4.ip_forward=1
```

13º- (opcional) Crear un bridge con las diferentes antenas posibles sobre donde se harán los hotspots.

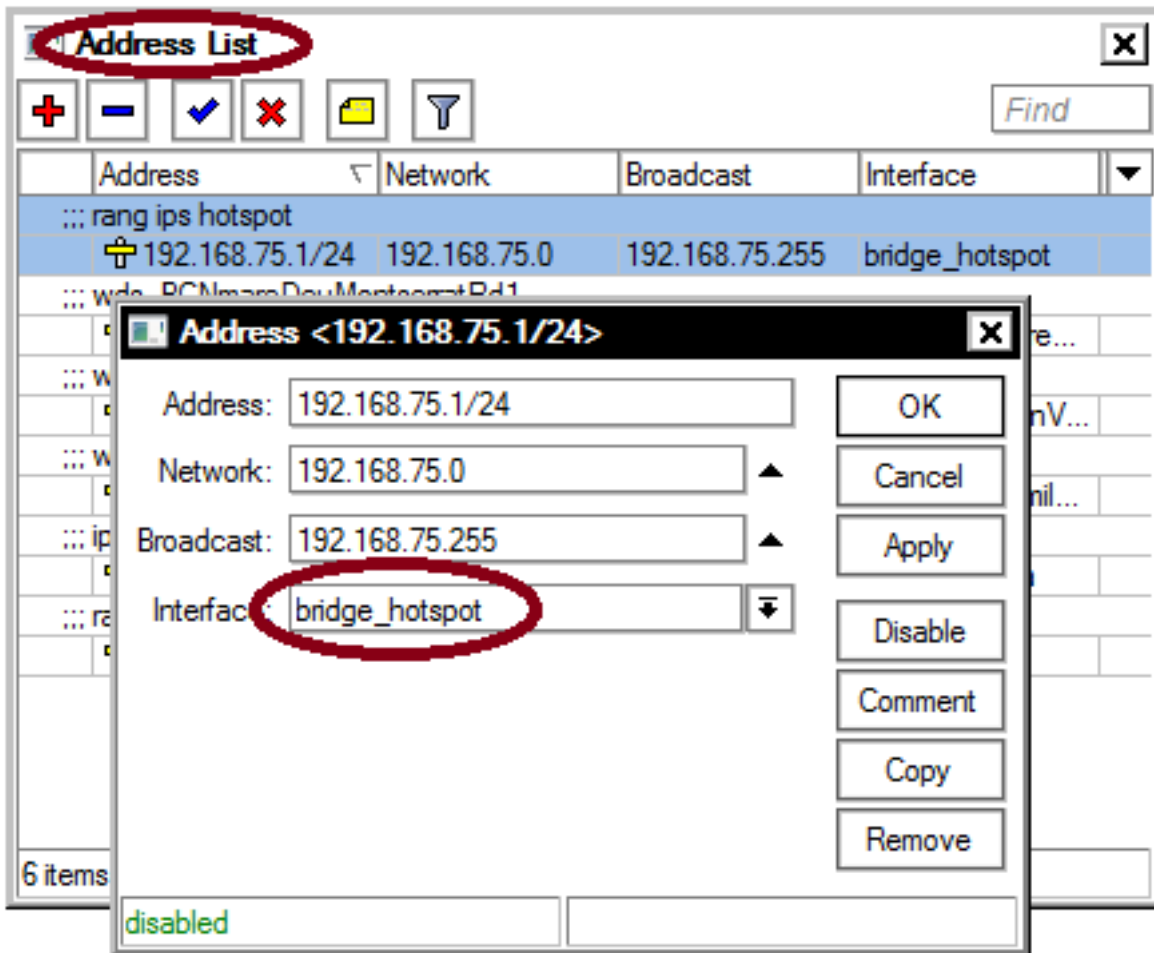
Todo este proceso sirve por si tenemos, una, dos, tres o más antenas que se utilizarán como un hotspot. Solo se tendrá de repetir el primer paso, para cada wlan real. En vez de aplicar ciertos pasos a una sola interfície, lo podemos hacer sobre un bridge. En este bridge podremos añadir las VirtualAPs que queramos.

Interface List						
Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN	VRRP	Bonding
R	bridge_hotspot	Bridge	1522	0 bps	0 bps	
R	ether1	Ethernet	1526	71.0 kbps	9.8 kbps	
	ether2	Ethernet	1522	0 bps	0 bps	
	ether3	Ethernet	1522	0 bps	0 bps	
R	ip_tunnel	IP Tunnel		0 bps	0 bps	
R	wLan/Lan	Bridge	1526	71.0 kbps	8.1 kbps	
R	wlan1	Wireless (Atheros AR5...	2290	1410 bps	0 bps	
::: guifi.net-AccesObert						
	wlan_hotspot	VirtualAP	2290	0 bps	0 bps	
R	wlan2	Wireless (Atheros AR5...	2290	0 bps	0 bps	
::: guifi.net-AccesObert 2						
	wlan_hotspot 2	VirtualAP	2290	0 bps	0 bps	

En este ejemplo tenemos 2 wlans



Este es el pas donde añadimos las VirtualAPs



(nota: quizás modificando los valores del servidor hotspot se os pone estos en rojo (error), desactivar y activar este rango de direcciones como el último paso.)

The screenshot shows the Mikrotik WinBox DHCP Server configuration interface. At the top, the 'DHCP Server' window is open, with tabs for 'DHCP', 'Networks', 'Leases', 'Options', and 'Alerts'. Below the tabs are several icons and buttons: a red plus sign, a blue minus sign, a blue checkmark, a red X, a funnel icon, 'DHCP Config', and 'DHCP Setup'. A table lists two DHCP servers:

Name	Interface	Relay	Lease Time	Address Pool	Ac
dhcp-wLan/Lan	wLan/Lan		1d 00:00:00	dhcp-wLan/L...	nc
dhcp_hotspots	bridge_hotspot		1d 00:00:00	hs-pool-12	nc

Below the table, a configuration dialog for 'DHCP Server <dhcp_hotspots>' is open. The dialog contains the following fields and buttons:

- Name: dhcp_hotspots
- Interface: bridge_hotspot (circled in red)
- Relay: (empty)
- Lease Time: 1d 00:00:00
- Address Pool: hs-pool-12
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: after 2s delay
- Proxy Support

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Copy, and Remove. At the bottom left of the dialog, it says '2 items (1 se'.

Hotspot

Servers Server Profiles Users User Profiles Active Hosts IP Bindings Service Port

+ - ✓ ✗ ⏏ Reset HTML Hotspot Setup

Name	Interface	Address Pool	Profile	Address
hotspot1	bridge_hotspot	hs-pool-12	hsprof1	

Hotspot Server <hotspot 1>

Name: hotspot1

Interface: **bridge_hotspot**

Address Pool: hs-pool-12

Profile: hsprof1

Idle Timeout: 01:00:00 ▲

Keepalive Timeout: ▼

Addresses Per MAC: 1 ▲

IP of DNS Name: 0.0.0.0

Proxy Status: running

OK
Cancel
Apply
Disable
Copy
Remove
Reset HTML

1 item (

LISTOS!!

...resultado:

¿Que es guifi.net?



Es una red de telecomunicaciones, abierta, libre y neutral que se vertebra a partir de un [acuerdo de interconexión entre iguales](#), donde cada participante, al conectarse, extiende la red y obtiene conexión con todos los demás.

guifi.net es de todos sus participantes.
+ información en: guifi.net/es/que_es

HotSpot



Este sistema HotSpot **guifi.net-AccesoAbierto** permite la navegación a Internet con algunas limitaciones:

- 1 hora al día
- Caudal limitado - *256 kbps/user*

Esta dirigido a aquellas personas que necesitan un acceso puntual y temporal a Internet.

Si se desea realizar una conexión más prolongada y libre de limitaciones horarias, es necesario realizar una correcta conexión a la red.

Sigue los pasos descritos en: guifi.net/es/trespasos



Puede acceder a Internet desde el sistema Hotspot haciendo click aquí

Adjunto	Tamaño
hotspot_es_1h_v1.2.zip [6]	51.38 KB
hotspot_es_30min_v1.2.zip [7]	51.38 KB

- [noticias de guifi.net - Castellano](#) [8]
- [Mig](#) [9]
- [Gestors de continguts / Portals](#) [10]

URL de origen: <https://guifi.net/es/hotspot-mikrotik>

Enlaces:

- [1] <https://guifi.net/es/user/8771>
- [2] <http://guifi.net/files/walled-garden-llista.txt>
- [3] <http://guifi.net/es/ProcomunXOLN>
- [4] http://guifi.net/files/hotspot_es_1h_v1.2.zip
- [5] http://guifi.net/files/hotspot_es_30min_v1.2.zip
- [6] https://guifi.net/files/hotspot_es_1h_v1.2.zip
- [7] https://guifi.net/files/hotspot_es_30min_v1.2.zip
- [8] <https://guifi.net/es/taxonomy/term/230>
- [9] <https://guifi.net/es/taxonomy/term/106>

[10] <https://guifi.net/es/taxonomy/term/66>