ACTIVIDAD 2
SEGURIDAD PROXY

Cristóbal Suárez Abad

SEGURIDAD Y ALTA DISPONIBILIDAD - 2º ASIR

Índice

PARTE 1: Obligar acceso a internet a toda la red desde el servidor proxy..... 2

PARTE 2: HotSpot..... 5

Abre el navegador:..... 8

PARTE 3: Ordenador aislado..... 11

Queremos tener un nuevo ordenador dentro de nuestra red que no pueda conectarse a internet aunque tenga la contraseña configurada en hotspot. Para ello vamos a realizar los siguientes pasos..... 11

Usando GNS3, con un router mikrotik

Usamos el anterior proyecto de GNS3:

CSA_Actividad_01_Tema_06_Seguridad

CONTEXTO:

Trabajáis como administradores de red de una academia. La dirección ha detectado que los estudiantes descargan archivos pesados y entran en sitios no deseados, saturando el ancho de banda. Se os pide implementar un sistema donde:

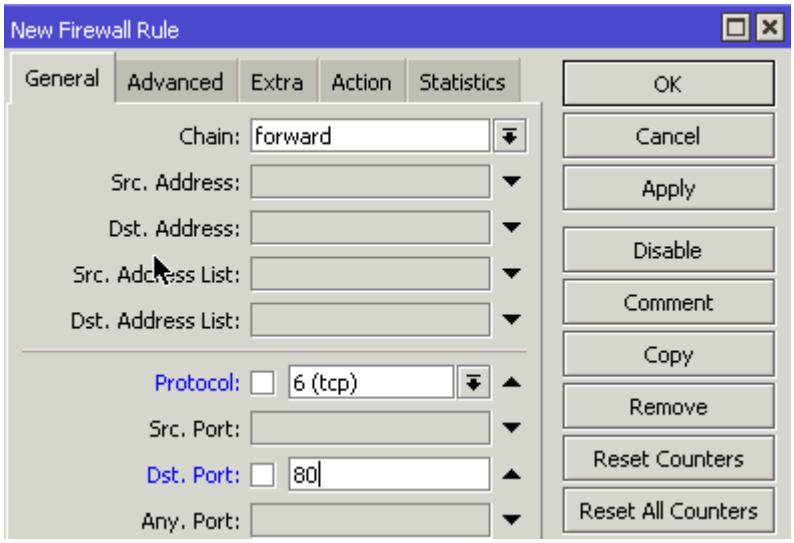
1. Nadie pueda "saltarse" el control de la empresa (Uso obligatorio de Proxy).
2. Cada usuario sea responsable de su navegación (Autenticación Hotspot).
3. Un equipo específico (el PC del aula de exámenes con IP fija) tiene prohibido el acceso total a la web para evitar trampas.

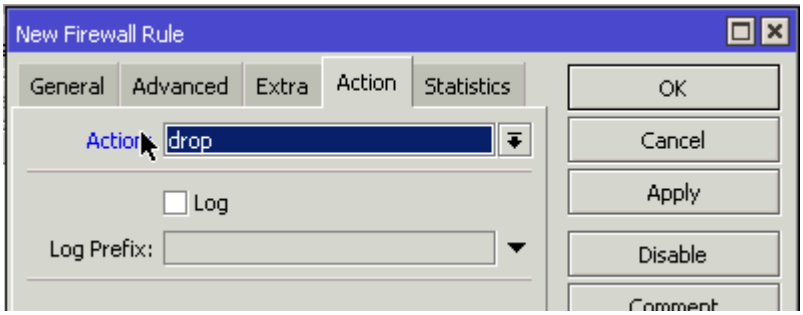
PARTE 1: Obligar acceso a internet a toda la red desde el servidor proxy

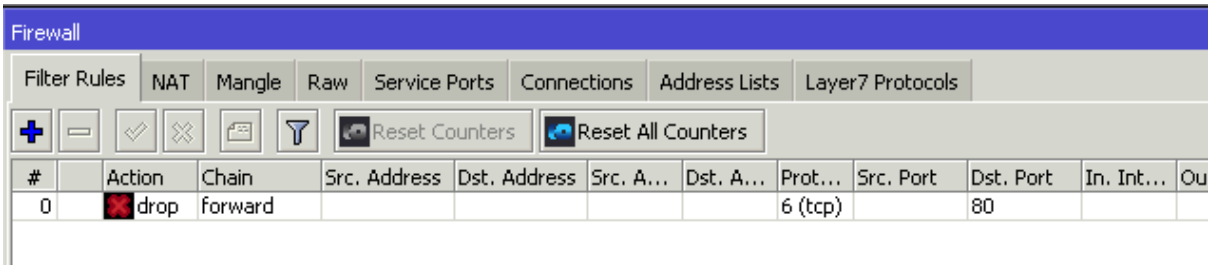
Queremos bloquear el acceso directo a internet en toda la red. Para ello añadir las siguientes reglas de bloqueo en el firewall:

- Bloquear HTTP directo para toda la red local

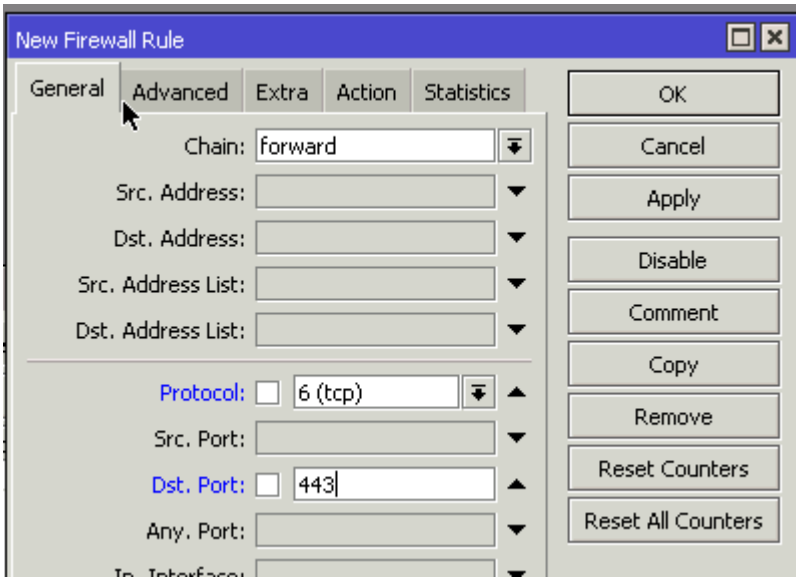
Desde el router Mikrotik, **IP → Firewall → Filter Rules:**

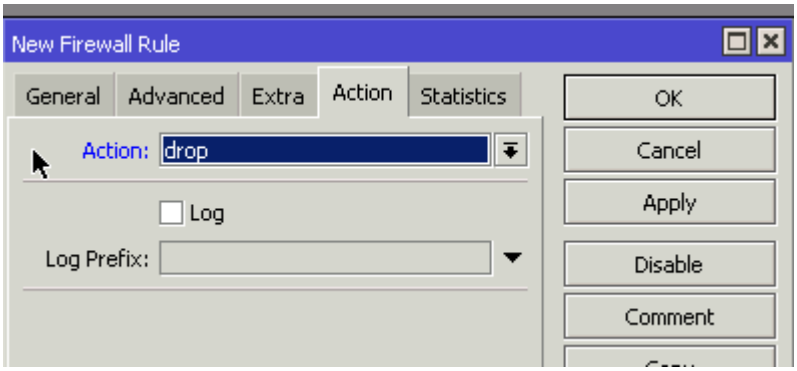


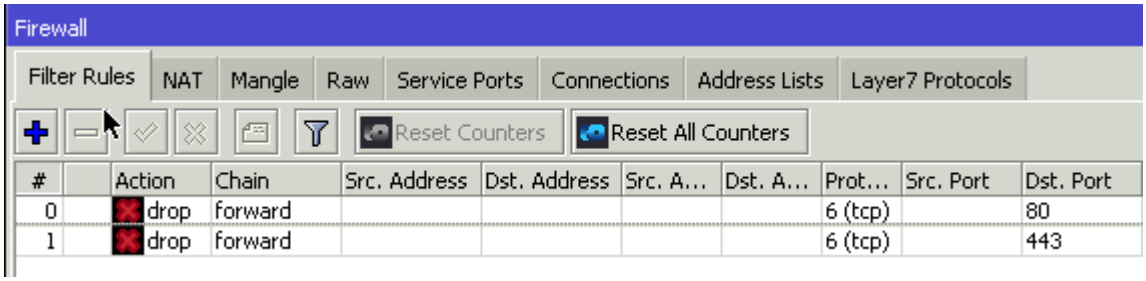




- Bloquear HTTPS directo para toda la red local





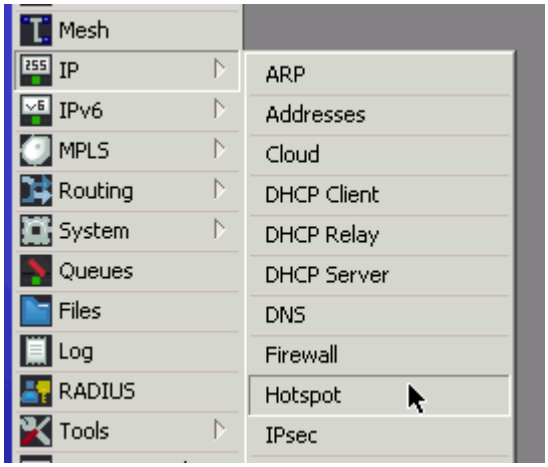

Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Action Chain Src. Address Dst. Address Src. A... Dst. A... Prot... Src. Port Dst. Port
0 drop forward 6 (tcp) 80
1 drop forward 6 (tcp) 443

PARTE 2: HotSpot

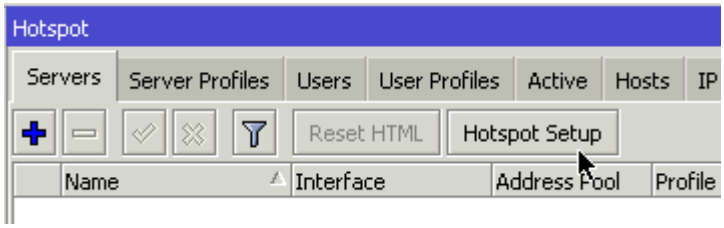
Damos seguridad al Proxy mediante HotSpot.

La forma más fácil es usar el asistente, que configura automáticamente el DHCP, el DNS y las reglas de Firewall necesarias.

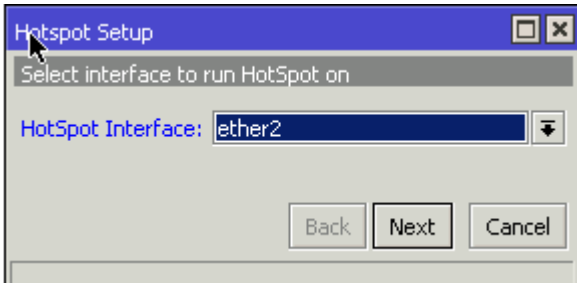
1. **Abre Mikrotik** y ve a `IP` -> `Hotspot`.



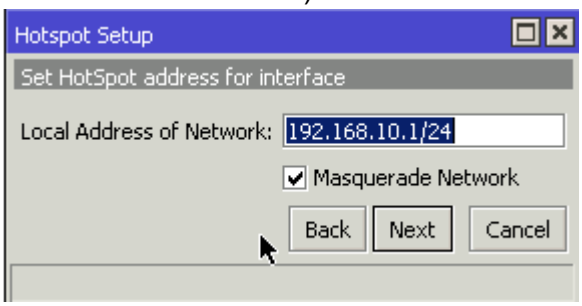
2. En la pestaña `Servers`, haz clic en el botón **Hotspot Setup**.



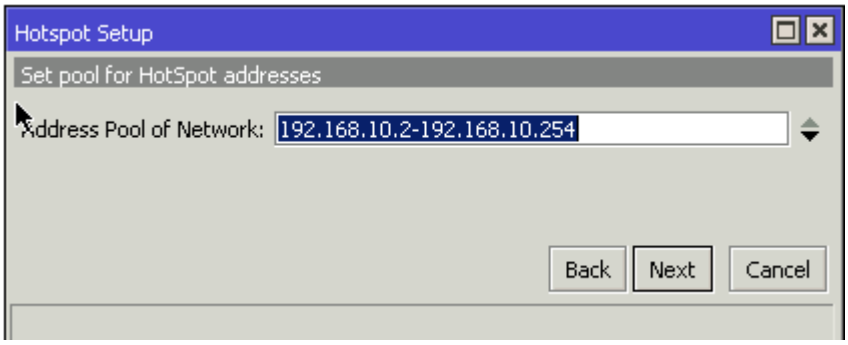
3. **Sigue los pasos del asistente:**
    - **Hotspot Interface:** Elige la interfaz donde está conectado tu `webterm` (ej. `ether2`).



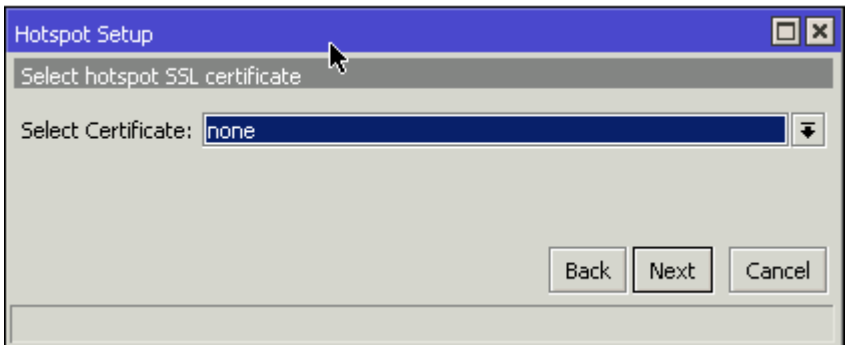
- **Local Address of Network:** Déjalo como está (normalmente la IP del MikroTik).



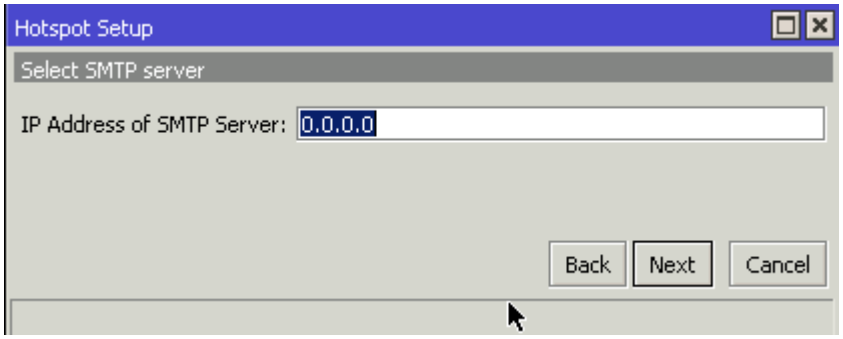
- **Address Pool:** El rango de IPs que dará a los clientes.



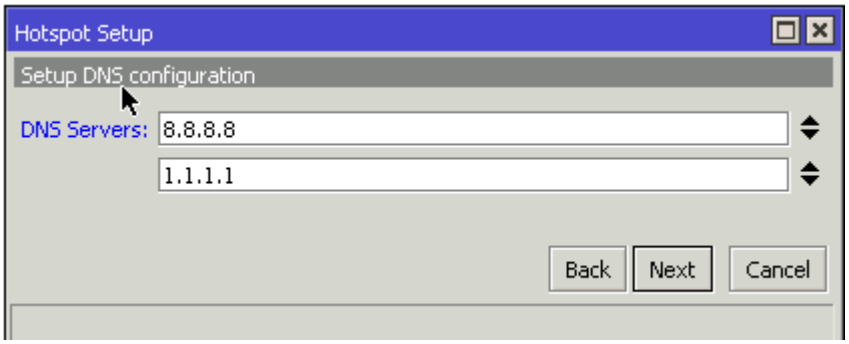
- **Select Certificate:** Pon `none`.



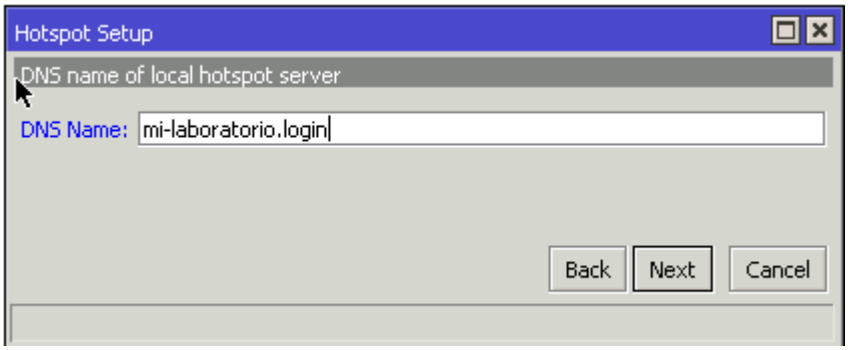
- **IP Address of SMTP Server:** `0.0.0.0`.



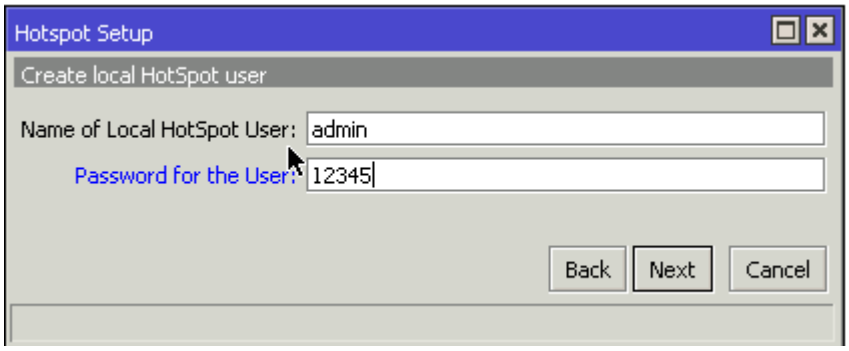
- **DNS Servers:** Puedes usar los de Google (`8.8.8.8`).



- **DNS Name:** Inventa un nombre (ej. `mi-laboratorio.login`). **Este paso es importante** para que el navegador sepa a dónde ir.



- **User/Password:** Crea el primer usuario (ej. `admin` / `1234`).



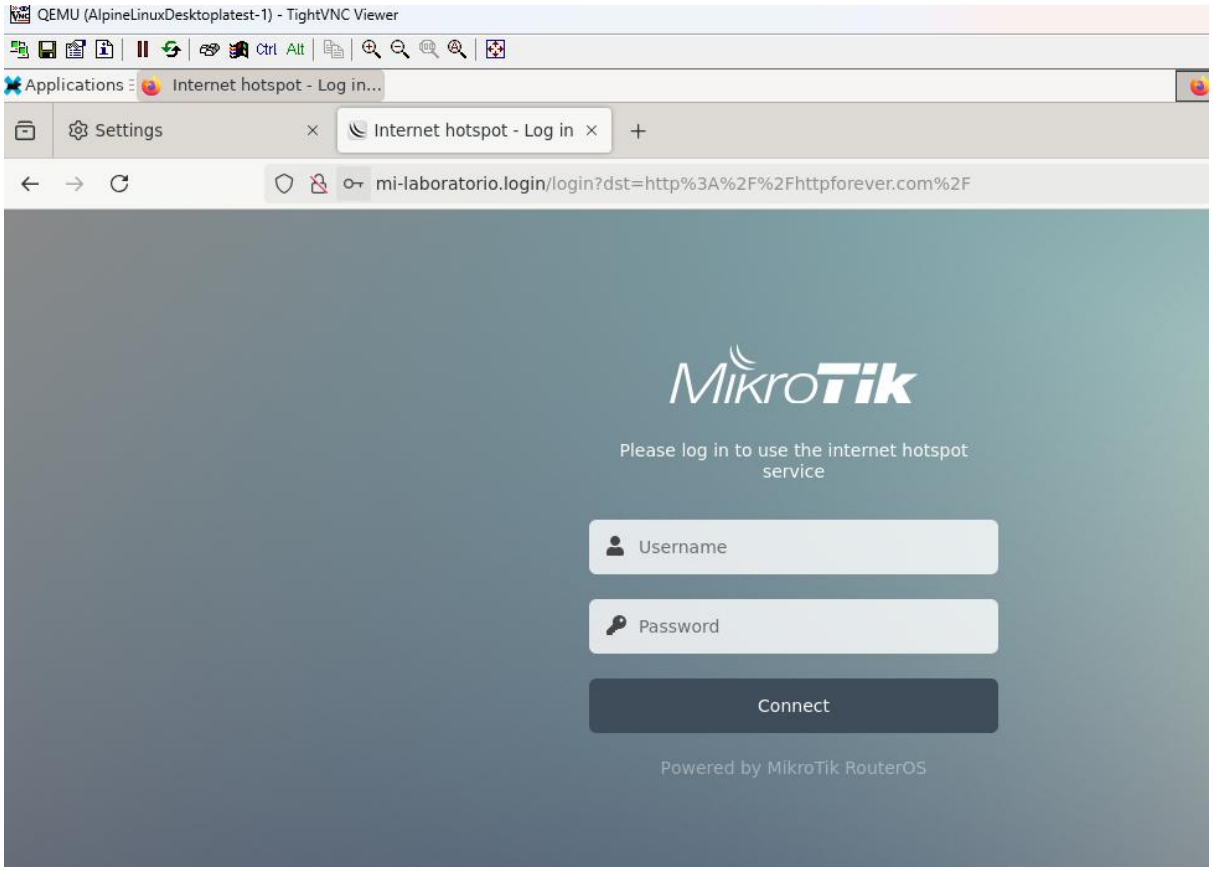
Una vez que le das a OK, te echa fuera de WineBox y no puedes acceder desde los clientes de dentro del proyecto. Esto se debe a que bloquea todo lo que sea HTTP y HTTPS. A partir de ahora seguiremos usando el Mikrotik desde fuera del proyecto.

Abre el navegador:

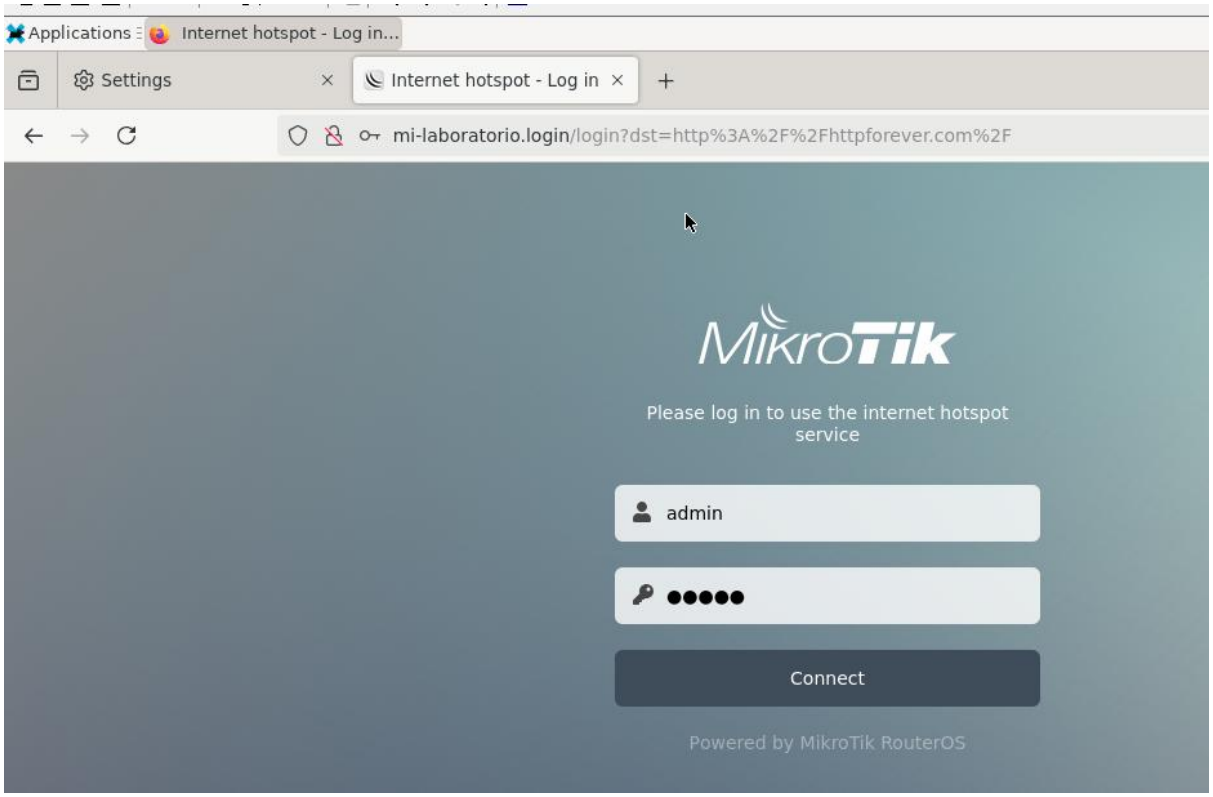
1. Intenta entrar primero en una página web http, ya que no tenemos configurada la seguridad https.

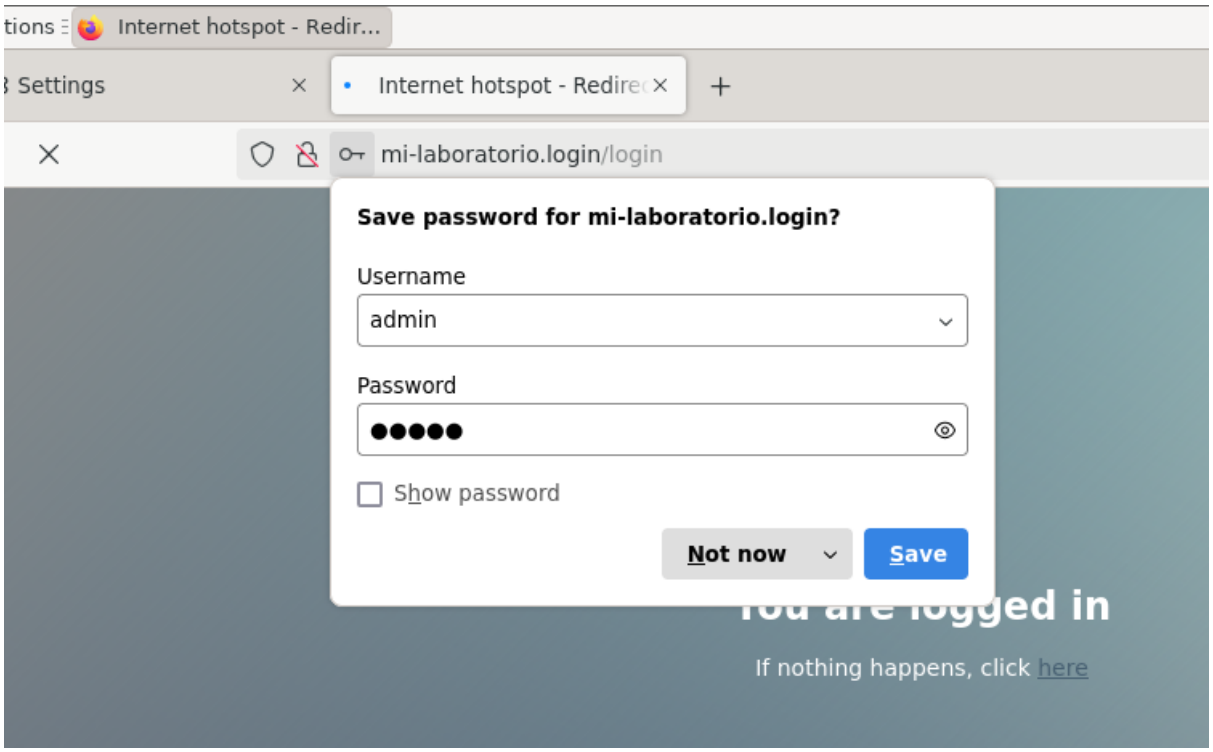
Probamos con http://httpforever.com/

2. El MikroTik dirá: *"¡Alto! No te has logueado"*.
3. Automáticamente te redirigirá a la página de login que acabas de crear.



4. Pones el usuario y, una vez aceptado, ya podrás navegar a través del proxy por todas las pagínas (incluídas https).


Applications
Internet hotspot - Log in...
Settings
Internet hotspot - Log in
mi-laboratorio.login/login?dst=http%3A%2F%2Fhttpforever.com%2F
MikroTik
Please log in to use the internet hotspot service
admin
Connect
Powered by MikroTik RouterOS


Internet hotspot - Redir...
Settings
Internet hotspot - Redire
mi-laboratorio.login/login
Save password for mi-laboratorio.login?
Username
admin
Password
Show password
Not now
Save
If nothing happens, click here

HTTP FOREVER

A reliably insecure connection

Why does this site exist?
This domain started out as my personal 'captive portal buster' but I wanted to publicise it for anyone to use. If you're on a train, in a hotel or bar, on a flight or anywhere that you have to login for WiFi, this site could help you!

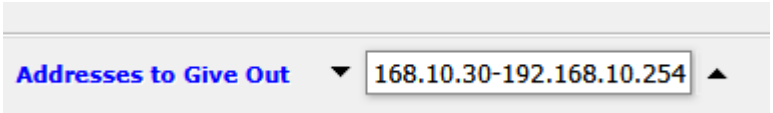
How does it work?
If you connect to a WiFi hotspot whilst out and about, sometimes you have to login or accept Terms and Conditions. To do that

PARTE 3: Ordenador aislado

Queremos tener un nuevo ordenador dentro de nuestra red que no pueda conectarse a internet aunque tenga la contraseña configurada en hotspot. Para ello vamos a realizar los siguientes pasos.

- Añade un nuevo web terminal con ip fija (ten en cuenta el rango que asigna el DHCP)
-

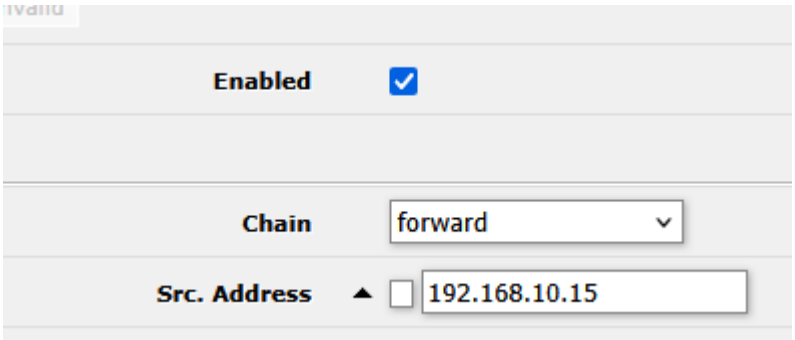
El servidor DHCP de Ethernet2 da IPs desde 192.168.10.31 a 192.168.10.254



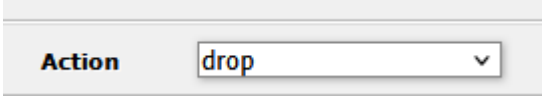

```
# Static config for eth0
auto eth0
iface eth0 inet static
                address 192.168.10.15
                netmask 255.255.255.0
                gateway 192.168.10.1
                up echo nameserver 172.16.200.1 > /etc/resolv.conf

# DHCP config for eth0
```

- Añade las reglas necesarias para que no permita el acceso a este equipo.

Chain: Forward
Source Address: 192.168.10.15



Action: Drop



Le damos a OK. Y lo colocamos en la posición 0, porque las reglas se leen de arriba abajo. De esta manera el router Mikrotik tirará todo lo que salga de este equipo.

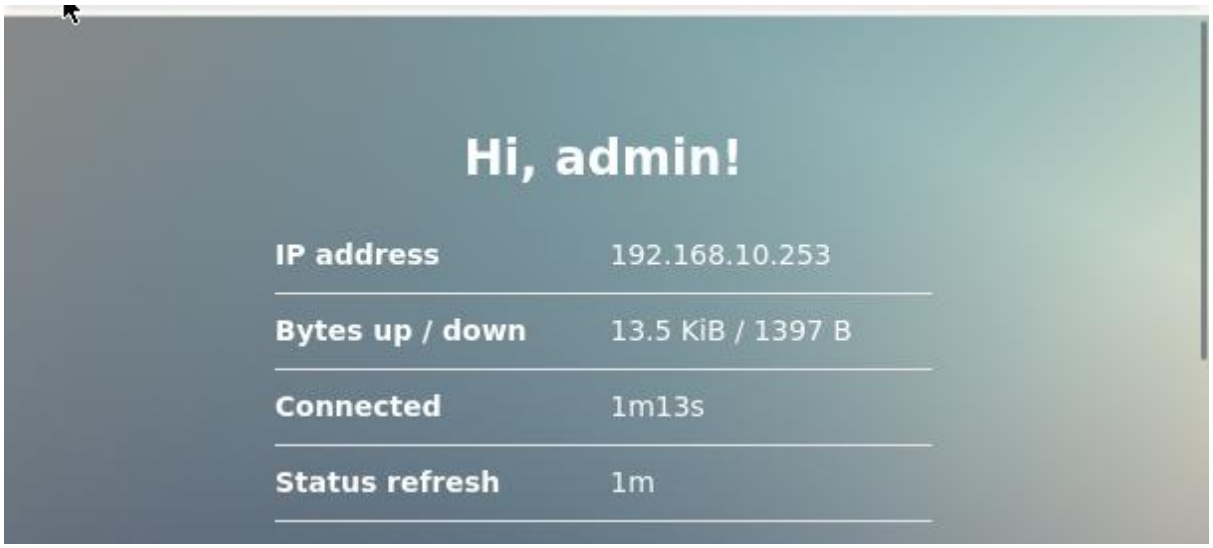
		#	Action	Chain	Src. Address	Dst. Address
- D		0	drop	forward	192.168.10.1	
-	D	1	jump	forward		
-	D	2	jump	forward		

- Comprueba que funciona como se espera.

En Terminal: Se hizo un ping a una dirección de Internet y no se pudo enviar nada.

```
~ $ ping x.uk
PING x.uk (185.249.71.213) 56(84) bytes of data.
^C
--- x.uk ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8286ms

~ $
```

Desde el navegador: nos logeamos



Y se agota (tras un buen rato) el tiempo de intento de conexión: