ACTIVIDAD 1 - INSTALACIÓN PROXY

Cristóbal Suárez Abad

SEGURIDAD Y ALTA DISPONIBILIDAD - 2º ASIR

Índice

Nombre del proyecto en GNS3:
CSA_Actividad_01_Tema_06_Seguridad

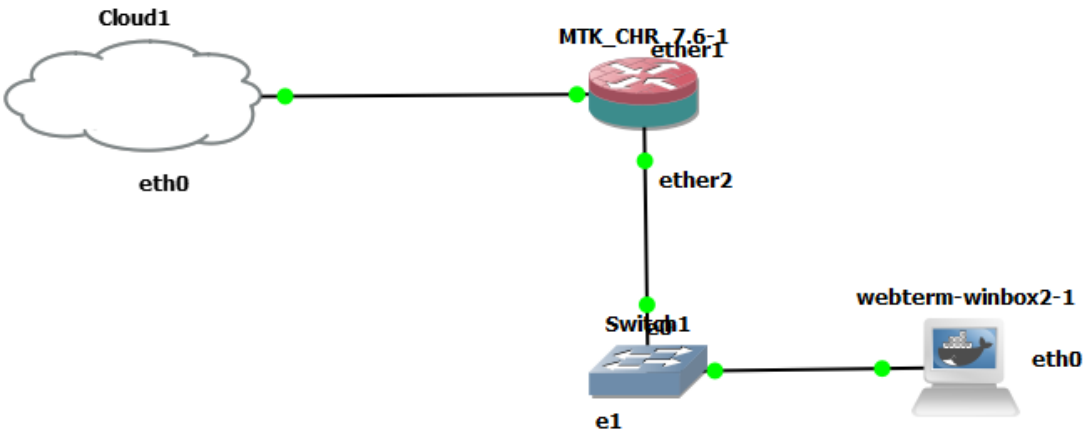
Actividad 1 - Instalación del proxy

1. Contexto y Objetivos

Has sido contratado como administrador de red para el IES Delgado Hernández. La dirección ha detectado que sus alumnos y profesores pierden tiempo en redes sociales y que la conexión es lenta por descargas indebidas. Tu misión es implementar un **Servidor Proxy con MikroTik** para acelerar la navegación y bloquear sitios no autorizados.

2. Topología en GNS3

- **1 x Cloud (NAT):** Para salida a Internet real.
- **1 x MikroTik:** Router y Proxy.
    - `ether1` -> Conectado a Cloud (WAN - DHCP Client).
    - `ether2` -> Conectado al Switch (LAN - IP: 192.168.10.1/24).
- **1 x Ethernet Switch.**
- **1 x Cliente (Webterm o Docker Firefox):**



3. Desarrollo de la Actividad

Fase 1: Despliegue y Conectividad Básica

Objetivo: Que el cliente tenga ping y salida a internet antes de activar el proxy.

1. Configura la IP `192.168.10.1/24` en la interfaz `ether2`.

Desde la propia terminal del router Mikrotik:

ip address/add address=192.168.10.1/24 interface=ether2

```
#   ADDRESS          NETWORK     INTERFACE
0 D 10.255.1.94/21   10.255.0.0  ether1
[admin@MikroTik] > ip address/add address=192.168.10.1/24 interface=ether2
[admin@MikroTik] > ip address/print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#   ADDRESS          NETWORK       INTERFACE
0 D 10.255.1.94/21   10.255.0.0    ether1
1   192.168.10.1/24  192.168.10.0  ether2
```

2. Configura un servidor **DHCP Server** básico en la `ether2` (o configura IP estática en el cliente `Webterm`).

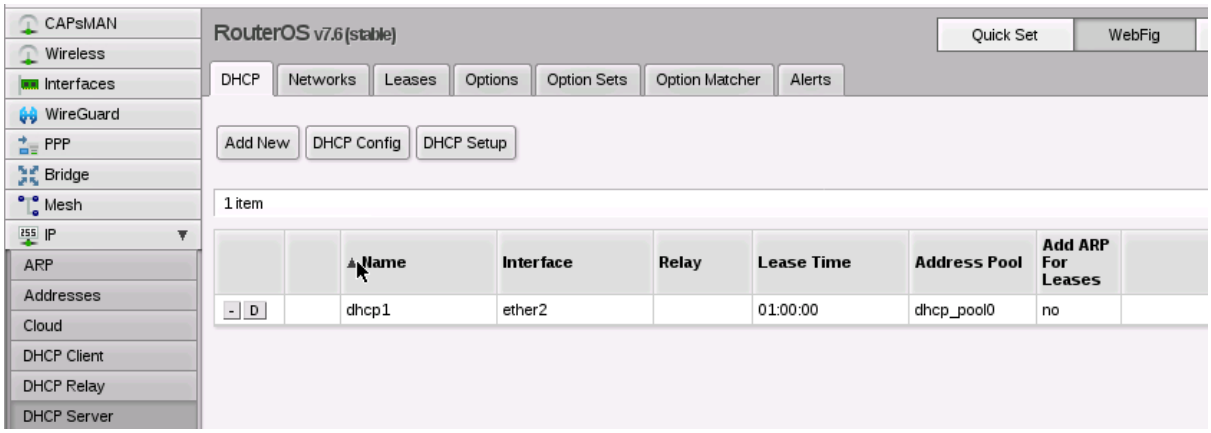
Al equipo cliente se le configura una IP estática.
IMPORTANTE: DNS la del instituto. 172.16.200.1

webterm-winbox2-1 interfaces

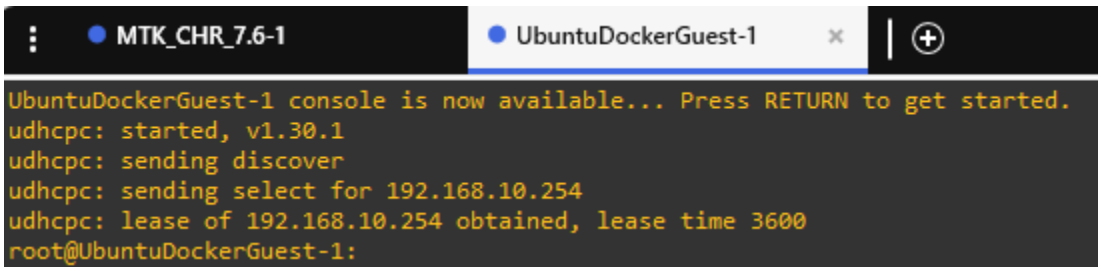
```
#
# This is a sample network config, please uncomment lines to configure the network
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.10.50
        netmask 255.255.255.0
        gateway 192.168.10.1
        up echo nameserver 172.16.200.1 > /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
#       hostname webterm-winbox2-1
```

Ahora podemos acceder al Router Mikrotik y configurarlo desde la plataforma Web.

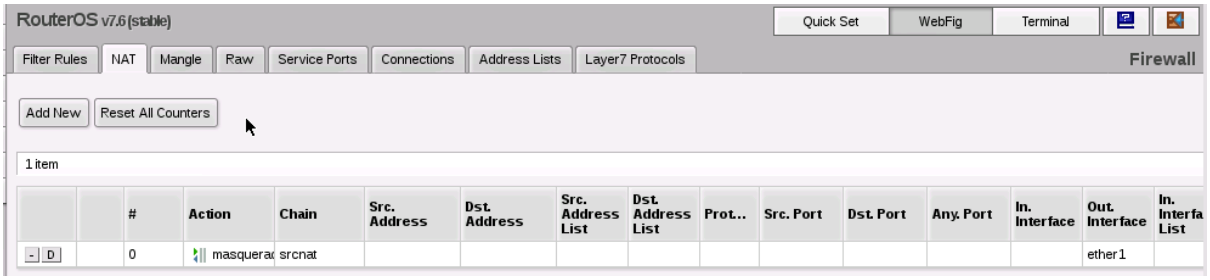
Configuramos el DHCP Server para Ethernet2:



Funciona porque conectamos otro equipo más y adquiere la IP en el arranque (configuramos en el cliente adquisición de IP por DHCP):

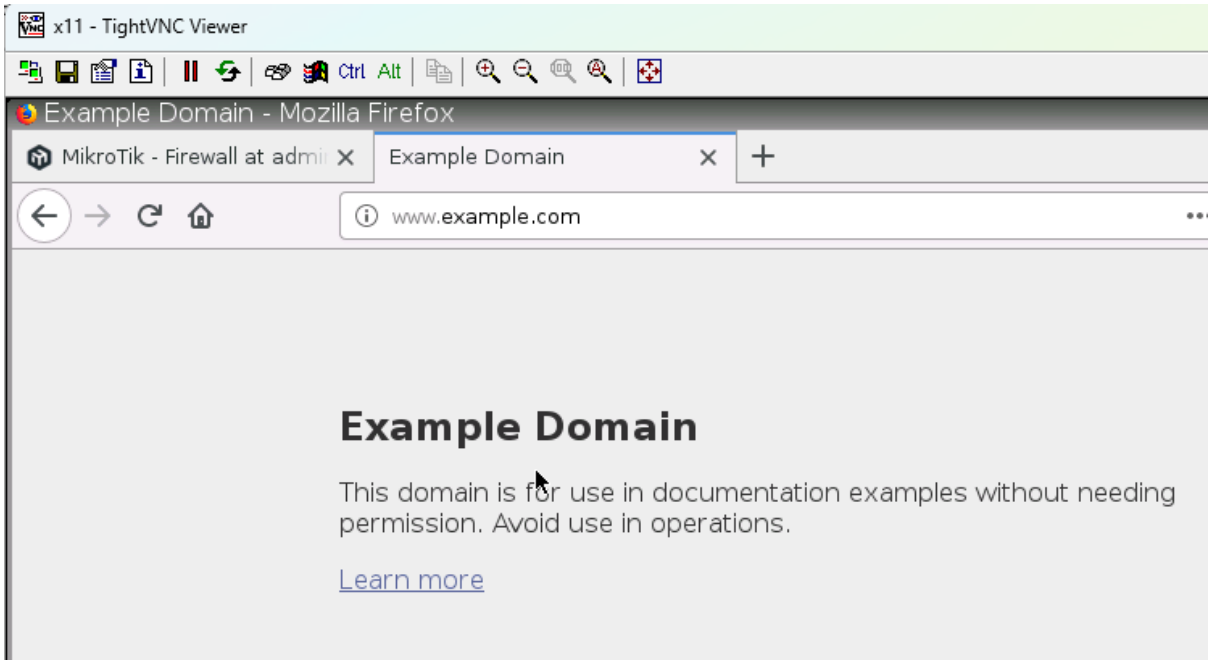


3. Configura una regla de **NAT (Masquerade)** para que el cliente tenga salida a Internet.



Chain: scrnat
Action: Masquerade.
Out. Interface: Ethernet1.

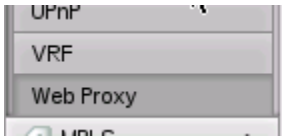
4. Abre el navegador en el cliente y entra en `www.example.com`. Debe cargar.



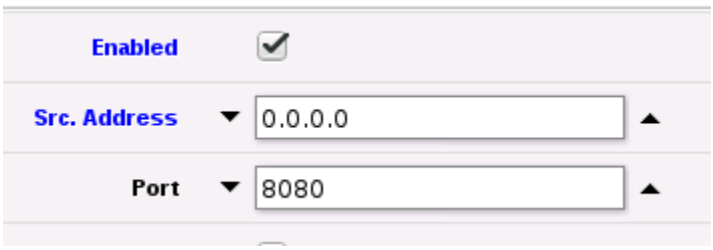
Fase 2: Activación del Proxy Caché

Objetivo: Habilitar el servicio de Proxy Cache y configurar el navegador del cliente.

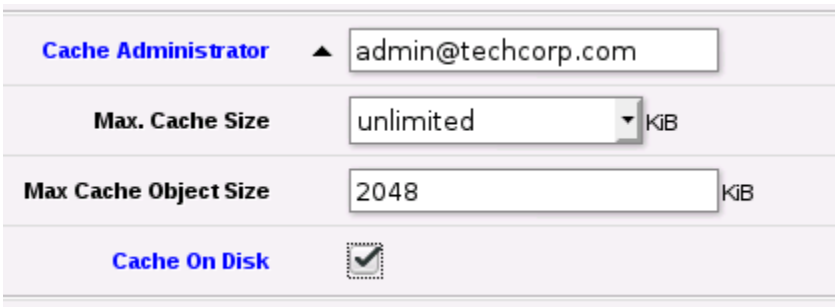
1. Accede al MikroTik.
2. Ve a **IP -> Web Proxy**.



3. Configura lo siguiente:
    - **Enabled:** Marcado (Check).
    - **Src. Address:** 0.0.0.0
    - **Port:** `8080`.



    - **Cache Administrator:** `admin@techcorp.com` (Para personalizar el error).
    - **Max. Cache Size:** `unlimited` (o un valor alto).
    - **Cache on Disk:** Marcado (Check).

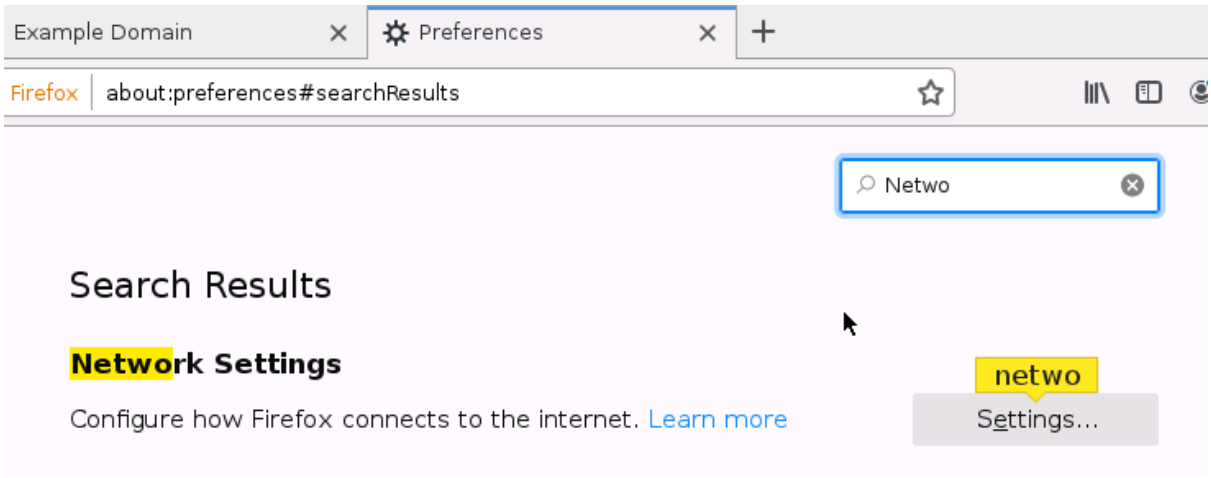


4. Haz clic en **Apply**.

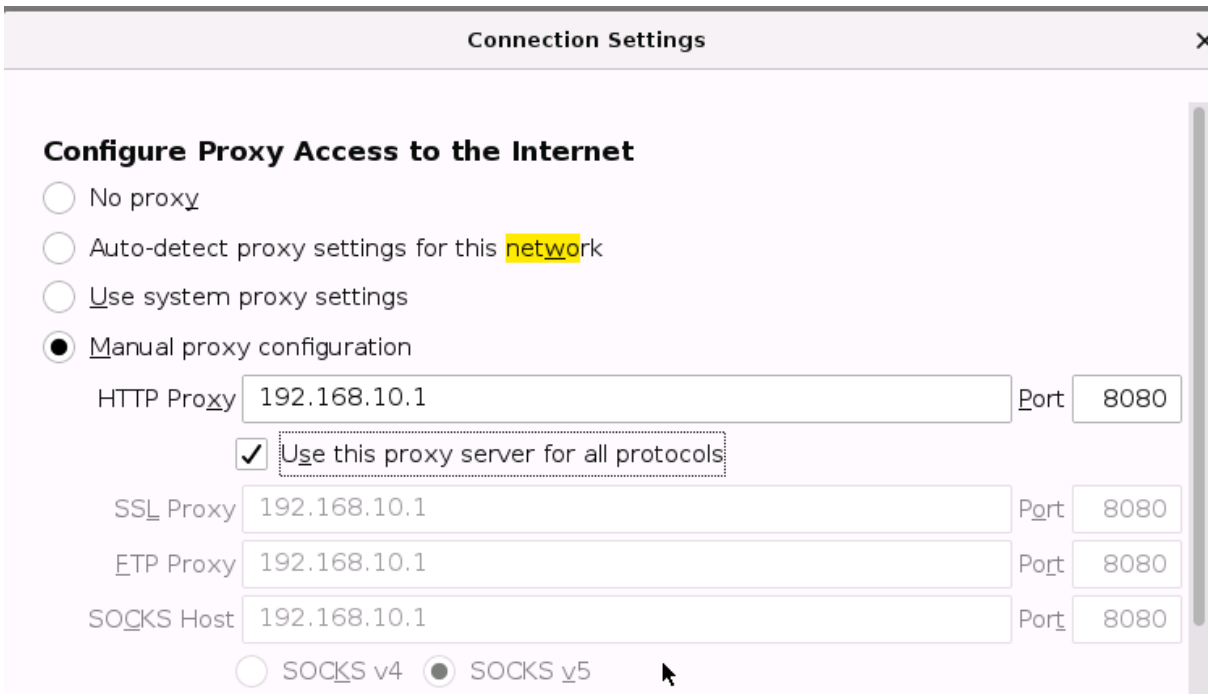
Objetivo: configurar el navegador del cliente.

5. **En el Cliente (Webterm):**

    - Abre Firefox -> Preferencias -> Configuración de Red.



    - Selecciona "Configuración manual del proxy".
    - Proxy HTTP: `192.168.10.1` Puerto: `8080`.
    - Marca "Usar este proxy para todo".



6. **Validación:** Navega por un par de webs (ej. wikipedia.org). Si cargan, el proxy está funcionando.

ATENCIÓN: Antes de nada, reinicia TODO (Router y Cliente).

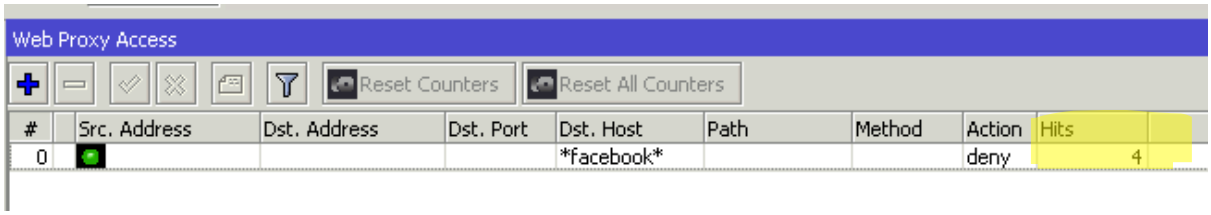
Fase 3: Restricciones de Acceso

Objetivo: Bloquear redes sociales y descargas de ejecutables.

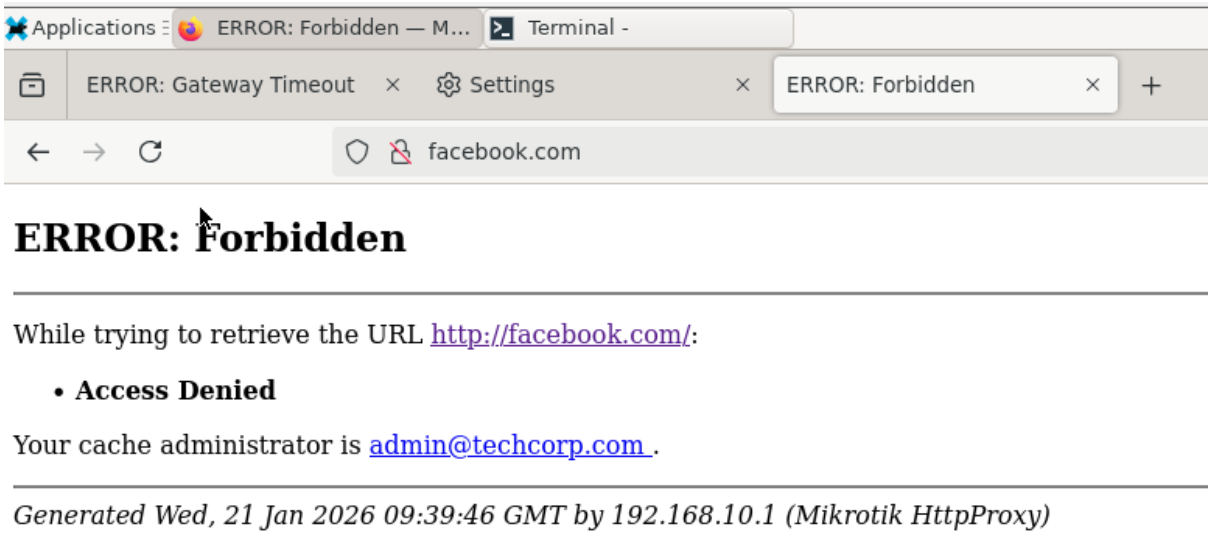
1. En WinBox, ve a **IP -> Web Proxy -> Access**.
2. **Misión A: Bloquear Facebook.**
    - Añade una regla nueva (Símbolo **+**).
    - **Dst. Host:** `*facebook*` (Usa asteriscos como comodines).
    - **Action:** `deny`.

- *Prueba:* Intenta entrar a facebook.com desde el cliente. Deberías ver una página de error generada por MikroTik.

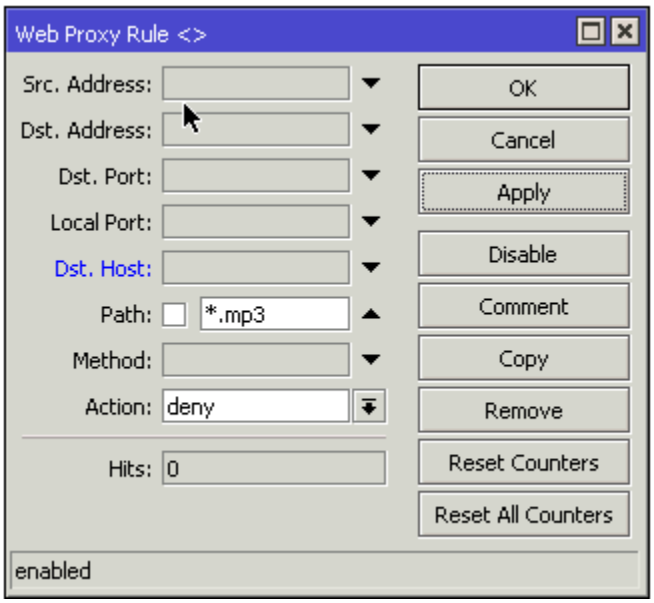
A mí no me sale una página con el Forbidden como al resto de compañeros, sino una de Timeout. Pero me aumenta el conteo:



En el cliente **Alpine** si funciona el **Forbidden**.

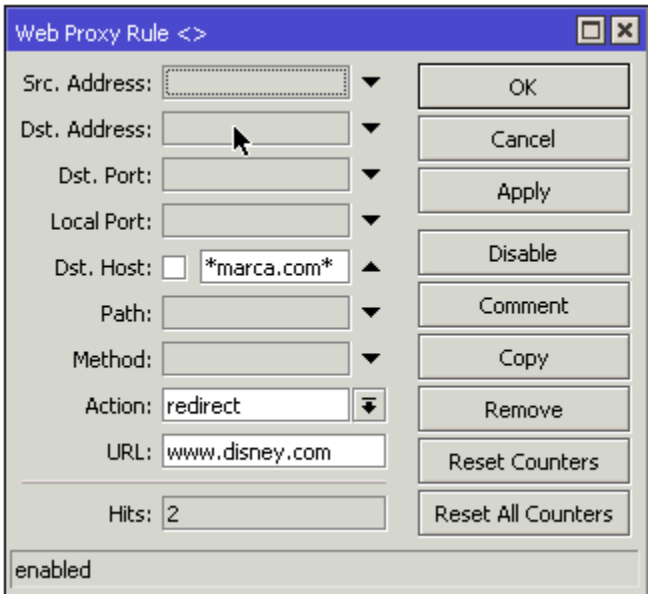


3. **Misión B: Bloquear archivos MP3.**
    - Añade una regla nueva.
    - **Path:** `*.mp3`
    - **Action:** `deny`.

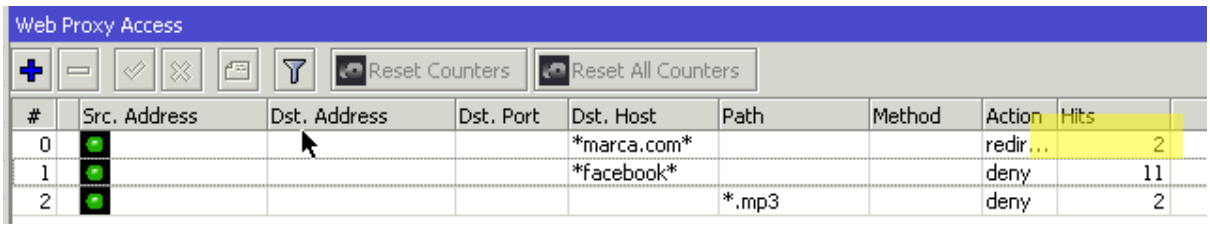


    - *Prueba:* http://prueba.com/prueba.mp3 Debe fallar

4. **Misión C: Redirección (Broma del Admin).**
    - Añade una regla para bloquear `*marca.com*`.
    - **Action:** `deny`.
    - **Redirect to:** `www.disney.com`
    - *Prueba:* Al entrar en Marca, debe llevarte a Disney.



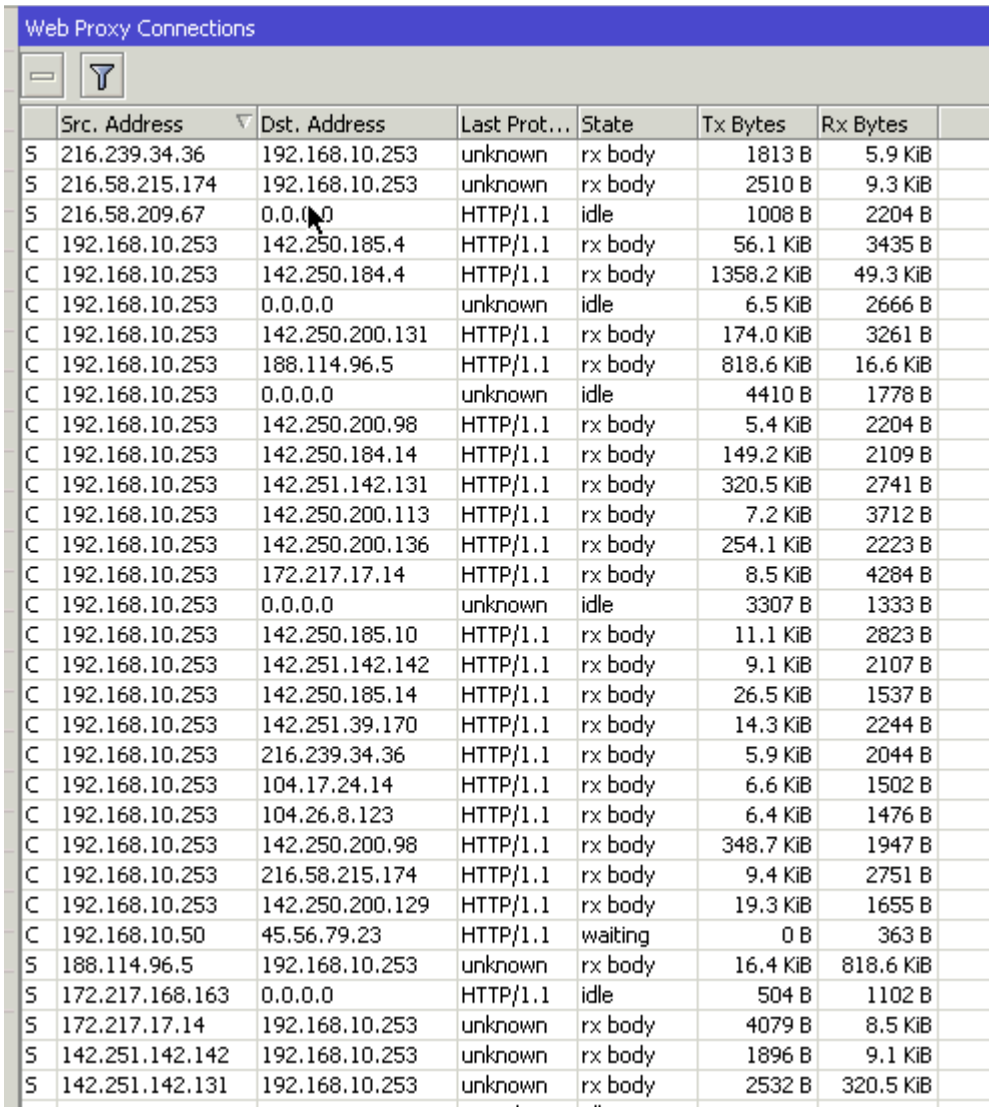
Es difícil de mostrar a pantallazos, pero se ve el conteo como sube.



Fase 4: Monitorización Gráfica

Objetivo: Ver "quién hace qué" en tiempo real usando las herramientas gráficas de MikroTik.

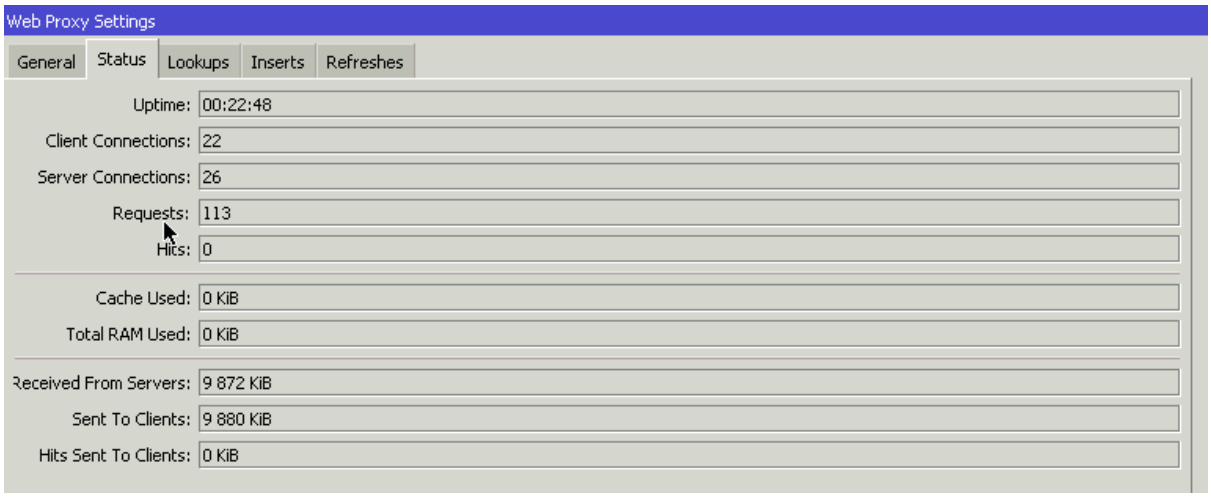
1. Mientras navegas frenéticamente en el cliente (abre varias pestañas: noticias, google, etc.), ve a MicroTik.
2. **Herramienta 1: Connections.**
    - Dentro de `IP -> Web Proxy`, ve a la pestaña **Connections**.
    - Observa las conexiones activas: verás la IP del cliente (`Src. Address`) y a qué servidores web está pidiendo datos (`Dst. Address`).



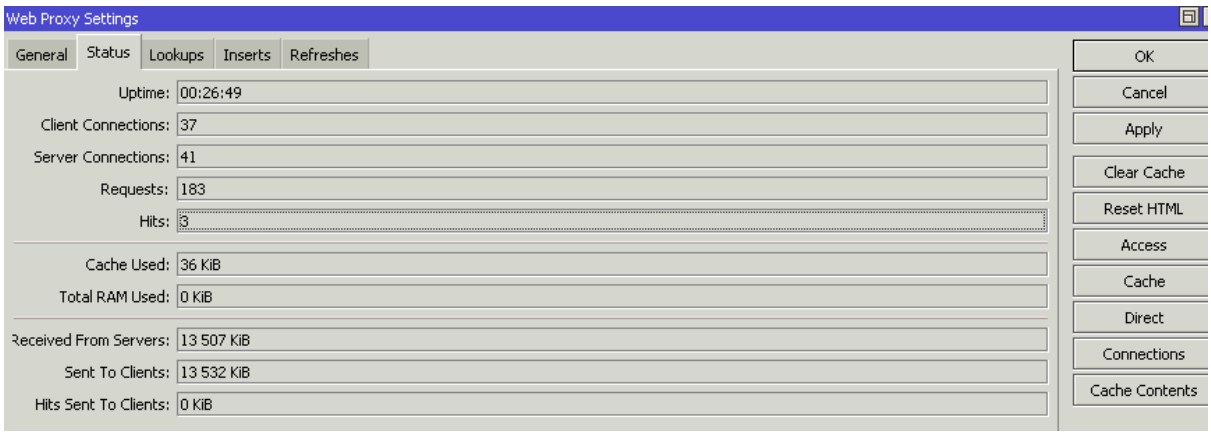
	Src. Address	Dst. Address	Last Prot...	State	Tx Bytes	Rx Bytes
S	216.239.34.36	192.168.10.253	unknown	rx body	1813 B	5.9 KiB
S	216.58.215.174	192.168.10.253	unknown	rx body	2510 B	9.3 KiB
S	216.58.209.67	0.0.0.0	HTTP/1.1	idle	1008 B	2204 B
C	192.168.10.253	142.250.185.4	HTTP/1.1	rx body	56.1 KiB	3435 B
C	192.168.10.253	142.250.184.4	HTTP/1.1	rx body	1358.2 KiB	49.3 KiB
C	192.168.10.253	0.0.0.0	unknown	idle	6.5 KiB	2666 B
C	192.168.10.253	142.250.200.131	HTTP/1.1	rx body	174.0 KiB	3261 B
C	192.168.10.253	188.114.96.5	HTTP/1.1	rx body	818.6 KiB	16.6 KiB
C	192.168.10.253	0.0.0.0	unknown	idle	4410 B	1778 B
C	192.168.10.253	142.250.200.98	HTTP/1.1	rx body	5.4 KiB	2204 B
C	192.168.10.253	142.250.184.14	HTTP/1.1	rx body	149.2 KiB	2109 B
C	192.168.10.253	142.251.142.131	HTTP/1.1	rx body	320.5 KiB	2741 B
C	192.168.10.253	142.250.200.113	HTTP/1.1	rx body	7.2 KiB	3712 B
C	192.168.10.253	142.250.200.136	HTTP/1.1	rx body	254.1 KiB	2223 B
C	192.168.10.253	172.217.17.14	HTTP/1.1	rx body	8.5 KiB	4284 B
C	192.168.10.253	0.0.0.0	unknown	idle	3307 B	1333 B
C	192.168.10.253	142.250.185.10	HTTP/1.1	rx body	11.1 KiB	2823 B
C	192.168.10.253	142.251.142.142	HTTP/1.1	rx body	9.1 KiB	2107 B
C	192.168.10.253	142.250.185.14	HTTP/1.1	rx body	26.5 KiB	1537 B
C	192.168.10.253	142.251.39.170	HTTP/1.1	rx body	14.3 KiB	2244 B
C	192.168.10.253	216.239.34.36	HTTP/1.1	rx body	5.9 KiB	2044 B
C	192.168.10.253	104.17.24.14	HTTP/1.1	rx body	6.6 KiB	1502 B
C	192.168.10.253	104.26.8.123	HTTP/1.1	rx body	6.4 KiB	1476 B
C	192.168.10.253	142.250.200.98	HTTP/1.1	rx body	348.7 KiB	1947 B
C	192.168.10.253	216.58.215.174	HTTP/1.1	rx body	9.4 KiB	2751 B
C	192.168.10.253	142.250.200.129	HTTP/1.1	rx body	19.3 KiB	1655 B
C	192.168.10.50	45.56.79.23	HTTP/1.1	waiting	0 B	363 B
S	188.114.96.5	192.168.10.253	unknown	rx body	16.4 KiB	818.6 KiB
S	172.217.168.163	0.0.0.0	HTTP/1.1	idle	504 B	1102 B
S	172.217.17.14	192.168.10.253	unknown	rx body	4079 B	8.5 KiB
S	142.251.142.142	192.168.10.253	unknown	rx body	1896 B	9.1 KiB
S	142.251.142.131	192.168.10.253	unknown	rx body	2532 B	320.5 KiB

3. **Herramienta 2: Status.**

   - Ve a la pestaña **Status**. Observa el contador de `Requests` (Peticiones) y `Hits` (Aciertos de caché).



   - *Pregunta:* Refresca una página 3 veces. ¿Aumenta el contador de "Cache Hits"? ¿Por qué?

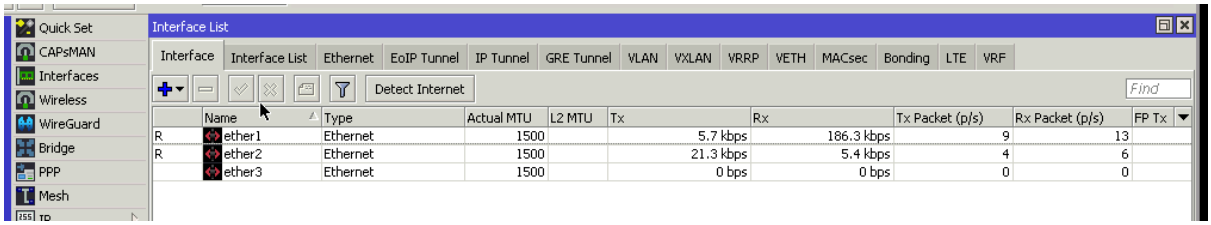


Si, porque el proxy guarda los datos de la página en su cache, permitiendo acelerar el acceso a la página.

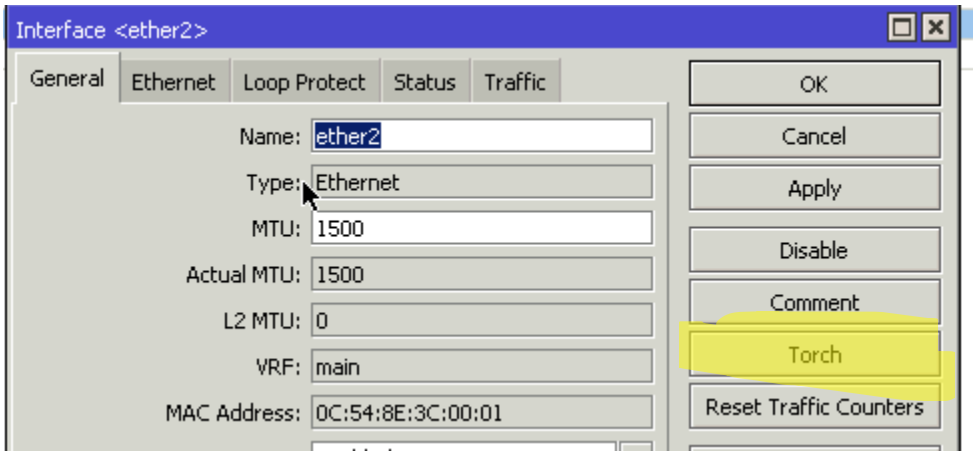
NOTA: En mi caso he tenido que usar una página “HTTP”, porque las “HTTPS” no subían el conteo.

4. **Herramienta 3: Torch (Monitor de Tráfico).**

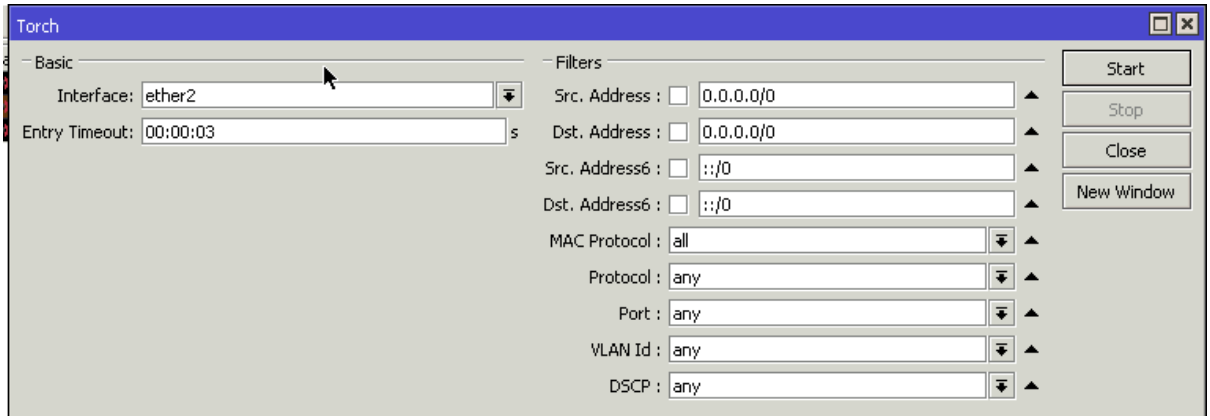
   - Ve al menú principal **Interfaces**.



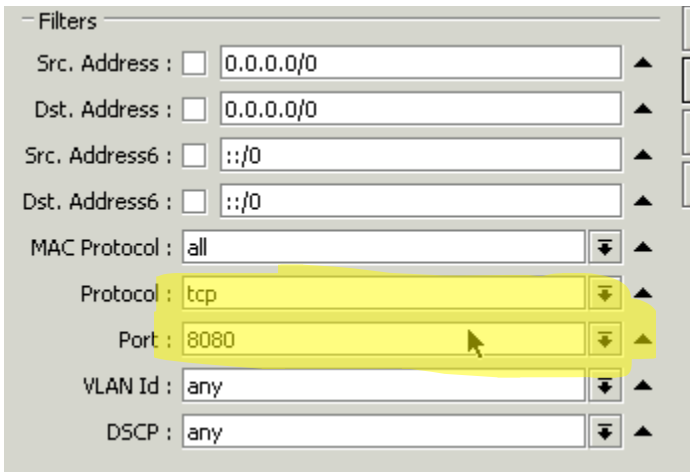
   - Doble clic en `ether2` (LAN) o clic derecho -> **Torch**.



   - Dale a **Start**.



- Filtra por Protocolo `6 (tcp)` y Puerto `8080`. Verás el consumo de ancho de banda en tiempo real del proxy.



En estos momentos, el cliente está accediendo a www.youtube.com