ACTIVIDAD 3 - SERVIDOR PROXY TRANSPARENTE

Cristóbal Suárez Abad

SEGURIDAD Y ALTA DISPONIBILIDAD - 2º ASIR

Índice

- Usamos el proyecto de GNS3: **CSA_Actividad_01_Tema_06_Seguridad**

Actividad 3 - Servidor Proxy Transparente

Convertir un proxy manual en uno **transparente** es un paso muy común en entornos educativos y empresariales, ya que evita tener que configurar uno a uno los navegadores de los clientes.

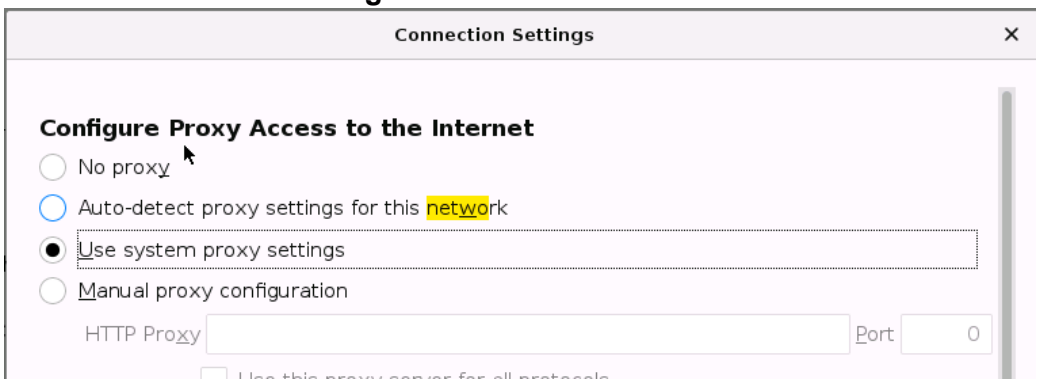
Usa la configuración de las actividades anteriores, para pasar de la configuración que ya tienes a una transparente, debes realizar estos **tres pasos fundamentales**:

1. Revertir la configuración en el Cliente

En un proxy transparente, el usuario no debe saber que el proxy existe.

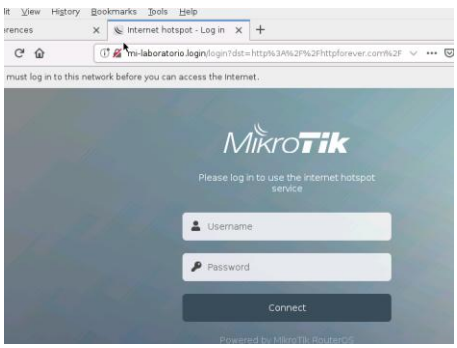
- **Acción:** Ve al navegador del cliente (Firefox en Webterm) y cambia la configuración de red de "Configuración manual del proxy" a **"Sin proxy"** o **"Usar la configuración del sistema"**.

Preferences → Networking



- **Resultado esperado:** El cliente intentará salir a internet directamente por el puerto 80 (HTTP).

Si intentamos entrar en una página “http” (puerto 80), nos rederigirá automáticamente al portal de autentificación del router Mikrotik.
http://httpforever.com/

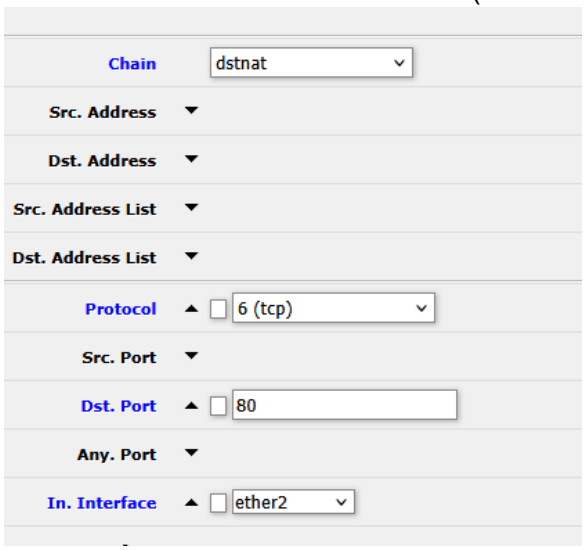


2. Crear la regla de redirección (NAT) en MikroTik

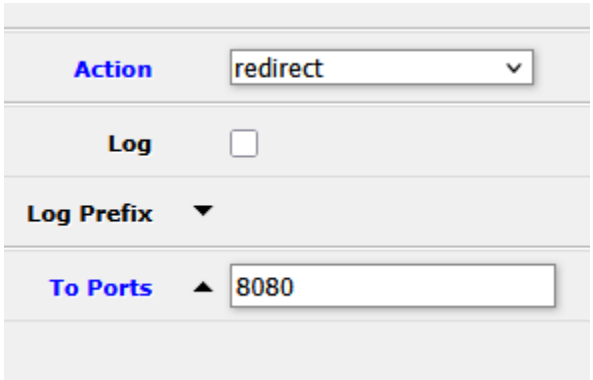
Debes decirle al router que todo el tráfico que venga de la LAN con destino a la web (puerto 80) sea interceptado y enviado al puerto donde escucha tu proxy (8080).

Pasos en WinBox:

1. Ve a **IP** -> **Firewall** -> Pestaña **NAT**.
2. Haz clic en el símbolo **+** para añadir una nueva regla.
3. En la pestaña **General**:
   - **Chain:** dstnat
   - **Protocol:** 6 (tcp)
   - **Dst. Port:** 80
   - **In. Interface:** ether2 (La interfaz de la LAN).



4. En la pestaña **Action**:
   - **Action:** redirect
   - **To Ports:** 8080

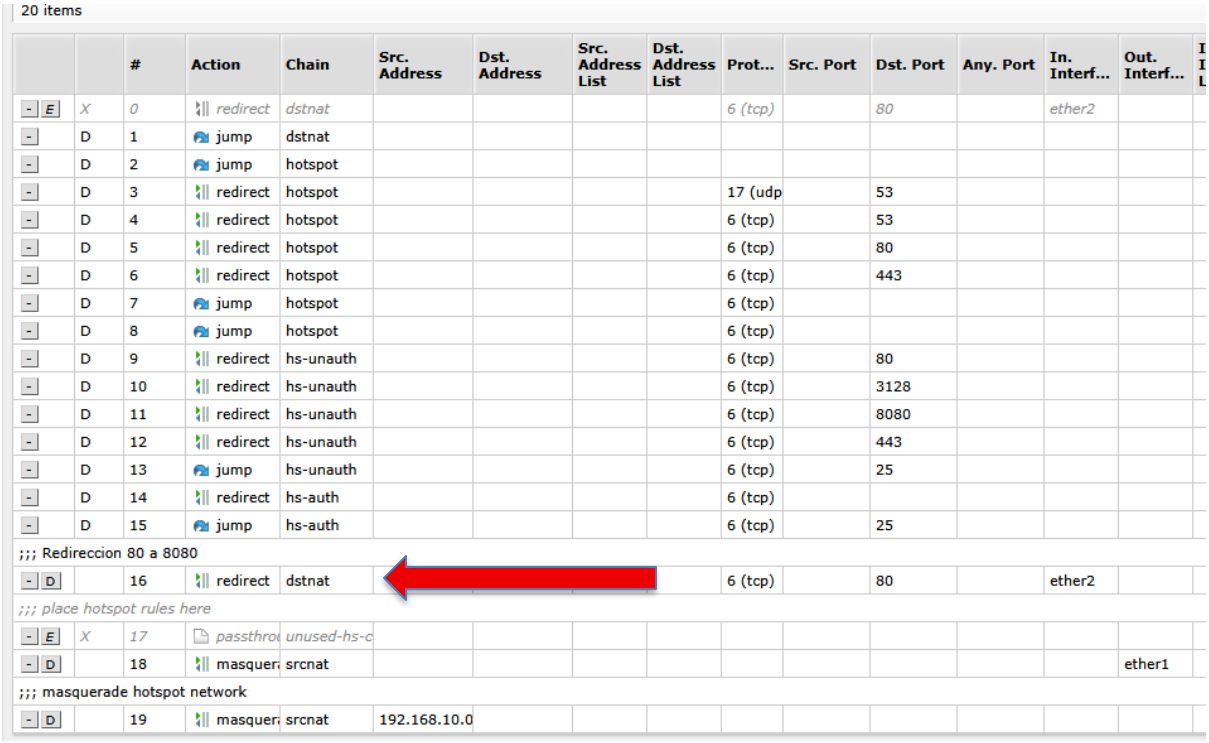


5. Haz clic en **OK**.

***Nota sobre HTTPS (Puerto 443): El Web Proxy de MikroTik es un proxy HTTP. La redirección transparente solo funcionará para sitios que usen el puerto 80. Hoy en día, la mayoría de las webs usan HTTPS (443). El tráfico HTTPS no se puede redireccionar de forma transparente tan fácilmente porque rompería el cifrado SSL (daría error de certificado).

¿Dónde colocamos la regla de redirección?

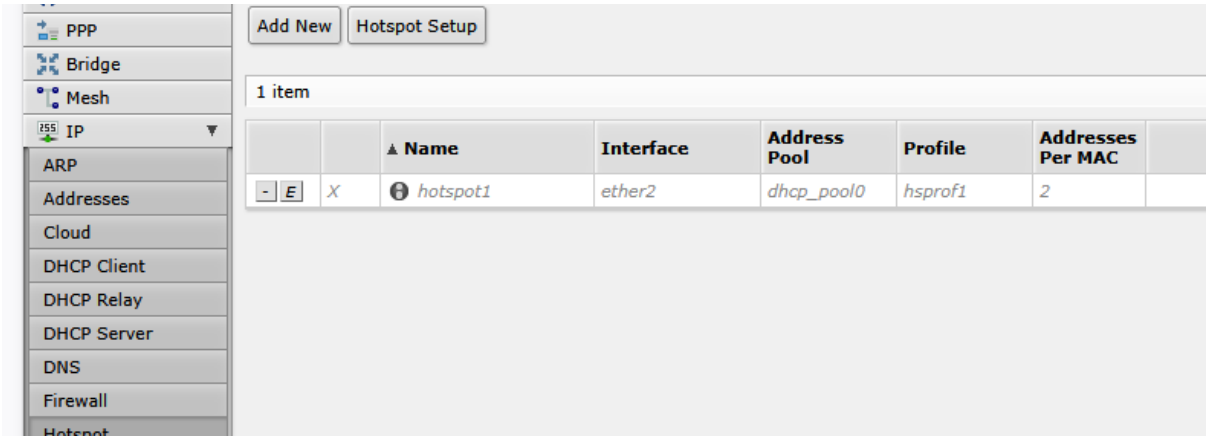
Justo debajo de las reglas dinámicas del Hotspot que gestionan la autenticación, si no, no podremos llegar nunca al portal del router Mikrotik.



20 items

		#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...
- E	X	0	redirect	dstnat					6 (tcp)		80		ether2	
-	D	1	jump	dstnat										
-	D	2	jump	hotspot										
-	D	3	redirect	hotspot					17 (udp		53			
-	D	4	redirect	hotspot					6 (tcp)		53			
-	D	5	redirect	hotspot					6 (tcp)		80			
-	D	6	redirect	hotspot					6 (tcp)		443			
-	D	7	jump	hotspot					6 (tcp)					
-	D	8	jump	hotspot					6 (tcp)					
-	D	9	redirect	hs-unauth					6 (tcp)		80			
-	D	10	redirect	hs-unauth					6 (tcp)		3128			
-	D	11	redirect	hs-unauth					6 (tcp)		8080			
-	D	12	redirect	hs-unauth					6 (tcp)		443			
-	D	13	jump	hs-unauth					6 (tcp)		25			
-	D	14	redirect	hs-auth					6 (tcp)					
-	D	15	jump	hs-auth					6 (tcp)		25			
;;; Redireccion 80 a 8080														
- D		16	redirect	dstnat					6 (tcp)		80		ether2	
;;; place hotspot rules here														
- E	X	17	passthro	unused-hs-c										
- D		18	masquer	srcnat										ether1
;;; masquerade hotspot network														
- D		19	masquer	srcnat	192.168.10.0									

¿Qué otra opción hay? Deshabilitar el HotSpot.

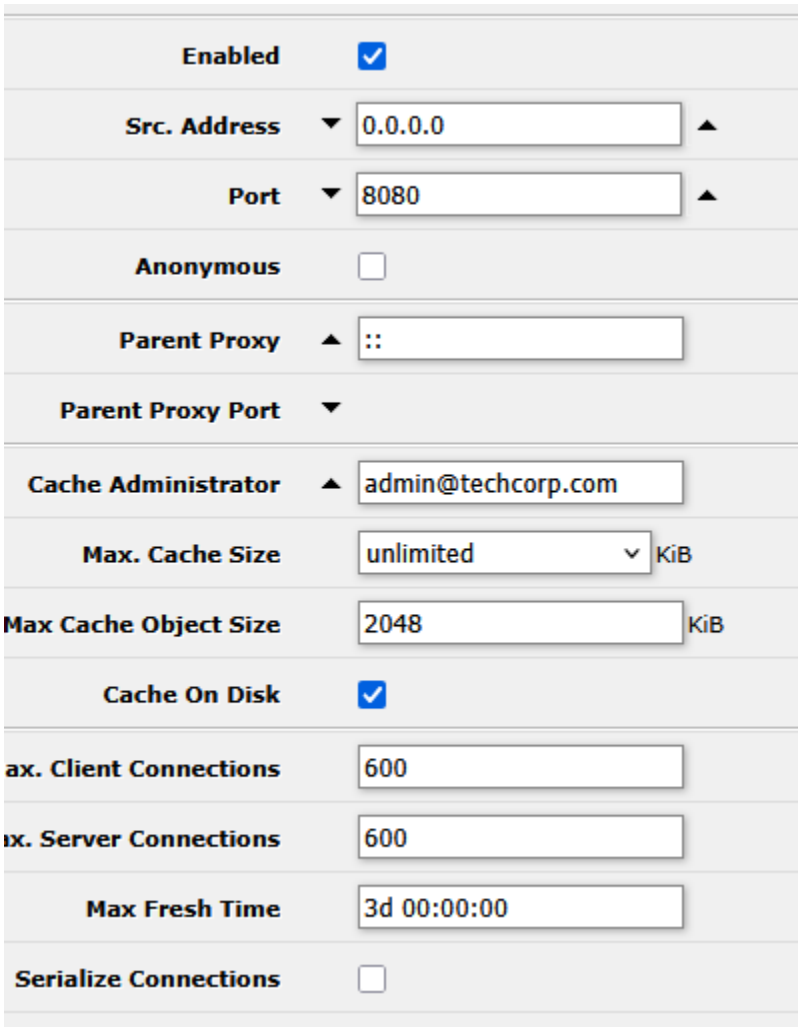


Así desaparecerán todas las reglas relacionadas con él y no nos pedirán credenciales.

3. Verificar que el Web Proxy tiene habilitada la opción

Asegúrate de que en la configuración que ya hiciste en la Fase 2, el proxy esté preparado para recibir estas peticiones:

1. Ve a **IP** -> **Web Proxy**.
2. Asegúrate de que la casilla **Enabled** está marcada.
3. El puerto debe ser el **8080** (el mismo que pusiste en la regla de NAT).

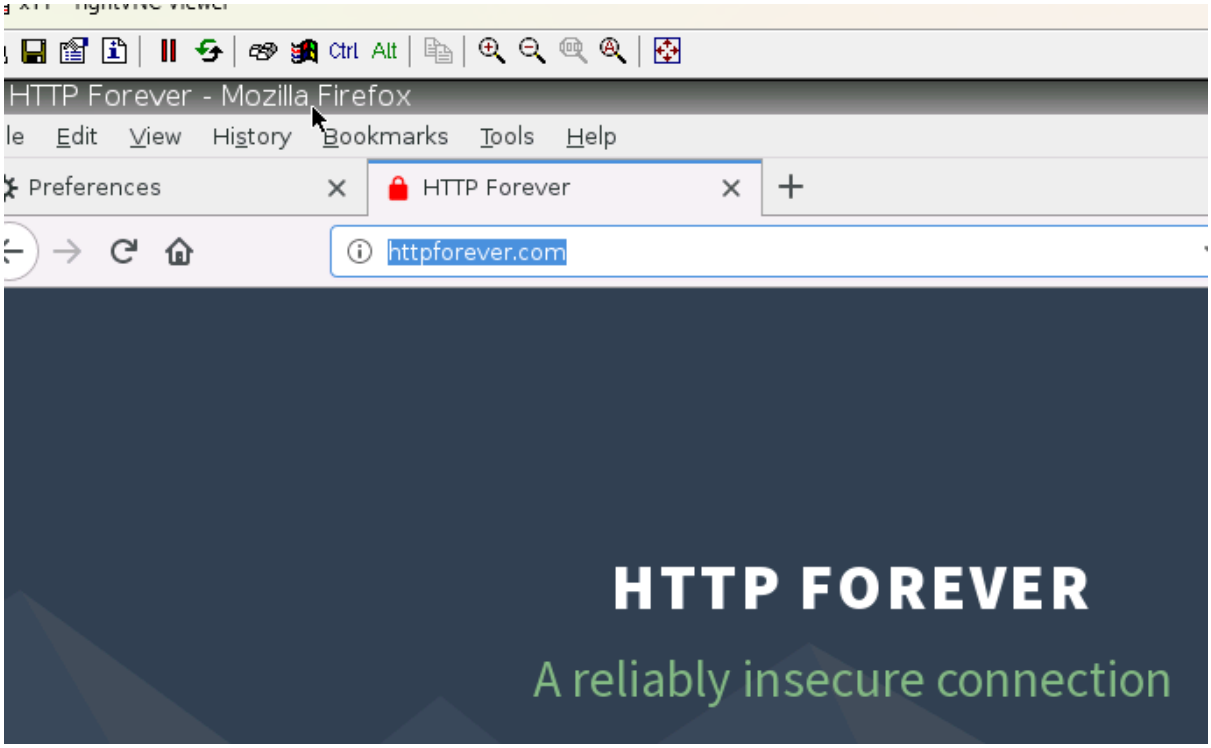


¿Cómo comprobar que funciona?

Para que tus alumnos verifiquen que realmente está pasando por el proxy sin haber configurado nada en el navegador:

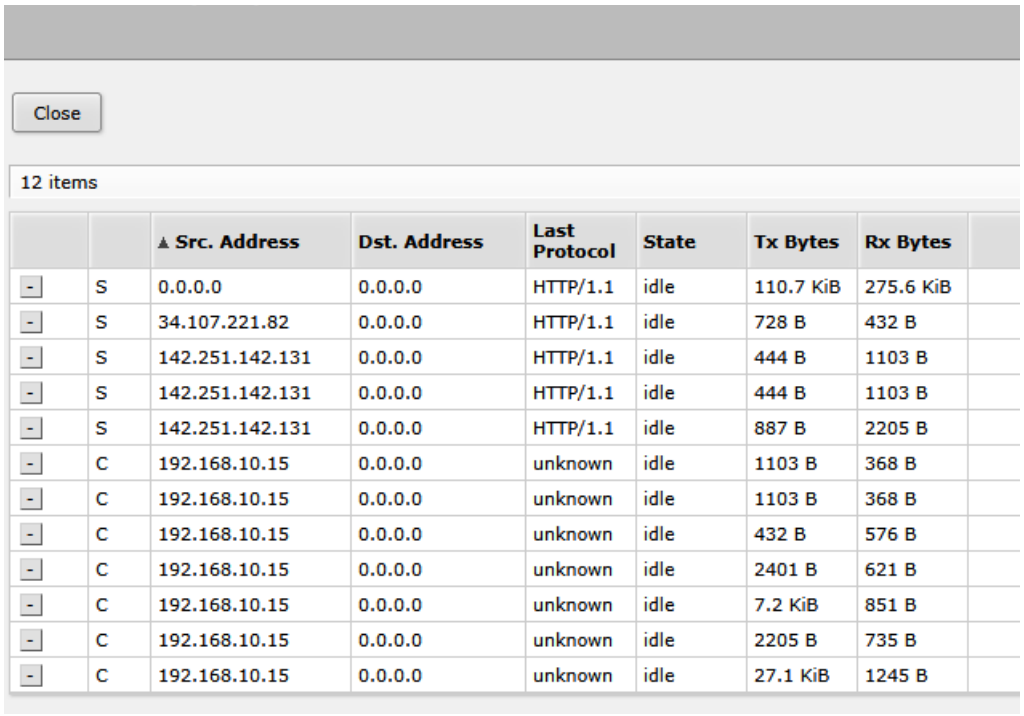
1. **Navegación:** Entra en una web que aún use HTTP (por ejemplo: http://neverssl.com o http://puchu.es).

Entramos en http://httpforever.com/ que tarda menos en cargar.



2. **Monitorización:** En MikroTik, ve a **IP -> Web Proxy -> Connections**. Deberías ver aparecer la IP del cliente y la URL que está visitando en tiempo real, a pesar de que el navegador del cliente está configurado como "Sin Proxy".

El cliente es el **192.168.10.15**



Close

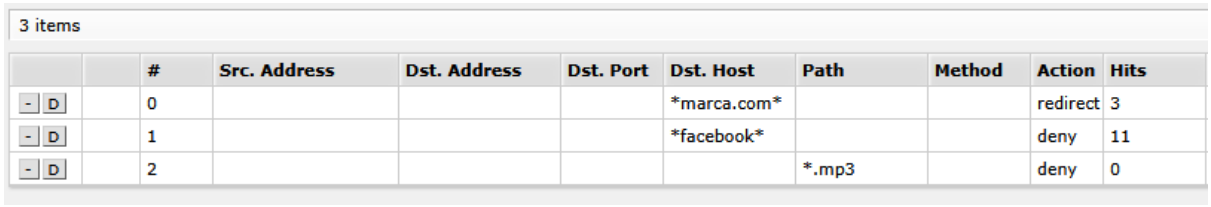
12 items

		Src. Address	Dst. Address	Last Protocol	State	Tx Bytes	Rx Bytes
-	S	0.0.0.0	0.0.0.0	HTTP/1.1	idle	110.7 KiB	275.6 KiB
-	S	34.107.221.82	0.0.0.0	HTTP/1.1	idle	728 B	432 B
-	S	142.251.142.131	0.0.0.0	HTTP/1.1	idle	444 B	1103 B
-	S	142.251.142.131	0.0.0.0	HTTP/1.1	idle	444 B	1103 B
-	S	142.251.142.131	0.0.0.0	HTTP/1.1	idle	887 B	2205 B
-	C	192.168.10.15	0.0.0.0	unknown	idle	1103 B	368 B
-	C	192.168.10.15	0.0.0.0	unknown	idle	1103 B	368 B
-	C	192.168.10.15	0.0.0.0	unknown	idle	432 B	576 B
-	C	192.168.10.15	0.0.0.0	unknown	idle	2401 B	621 B
-	C	192.168.10.15	0.0.0.0	unknown	idle	7.2 KiB	851 B
-	C	192.168.10.15	0.0.0.0	unknown	idle	2205 B	735 B
-	C	192.168.10.15	0.0.0.0	unknown	idle	27.1 KiB	1245 B

3. **Prueba de Bloqueo:** Intenta entrar en la web que bloqueaste en la Fase 3 (ej. http://www.marca.com). El router debería interceptar la petición y redirigirte a Disney o mostrarte el error, confirmando que el proxy está trabajando "en la sombra".

Nos fijamos en los “hits”, porque es difícil de mostrarlo a base de pantallazos.

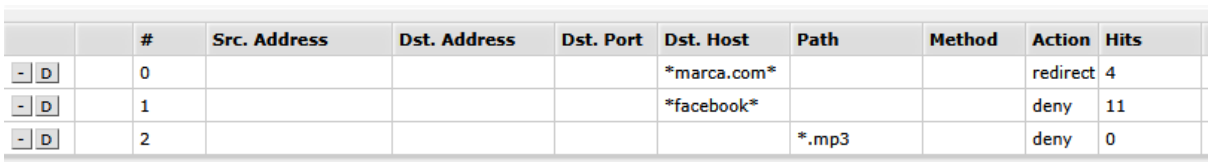
Web Proxy → Access:



3 items

		#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Hits
- D		0				*marca.com*			redirect	3
- D		1				*facebook*			deny	11
- D		2					*.mp3		deny	0

Ahora tiene un valor de “3”. Si ponemos “marca.com” en el navegador, nos redirige a disney.com



		#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Hits
- D		0				*marca.com*			redirect	4
- D		1				*facebook*			deny	11
- D		2					*.mp3		deny	0