Álvaro Almellones Fernández

PRÁCTICA 7 (almellonesfernandez-practica7)
U.D.4. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). PROXY APLICACIÓN WEB.

Antes de describir lo que hay que realizar se van a explicar una serie de normas a tener en cuenta para cada apartado que:

• Se deja al alumno que en cada ejercicio realice las capturas concluyentes que desee, pero **NUNCA** debe faltar:

- Fichero de configuración de squid que muestra lo que se desea probar.
- Evidencias de los contadores de las reglas relacionadas (PREROUTING, INPUT, y si la página envía a https FORWARD), para comprender por donde pasa los paquetes. (iptables -L -n – v –line number, iptables -t nat -L -n -v –line-number)
- La ejecución de comando wget/curl con las evidencias del número de respuesta (2??, 3??,4??), respuesta del proxy, reenvio a otras páginas ya sea por https o por qué el proxy nos envía a otro web.
- Las líneas del fichero access.log exactamente relacionada con esa comprobación, que evidencia la aceptación o denegación del mismo, y que tienen que coincidir con la anterior.

• Uso de squid -k parse para comprobar que no hay errores en la configuración de las directivas.

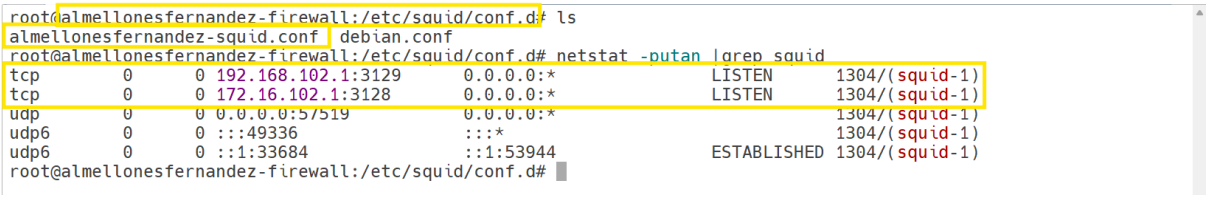
• **Para cada** HTTP_ACCESS y HTTP_REPLY_ACCESS tiene que haber un deny_info personalizado donde aparezca nombre alumno XXxx, número de clase del alumno, el nombre de la ACL que prohíbe y un texto que explica el motivo por el cual se deniega.

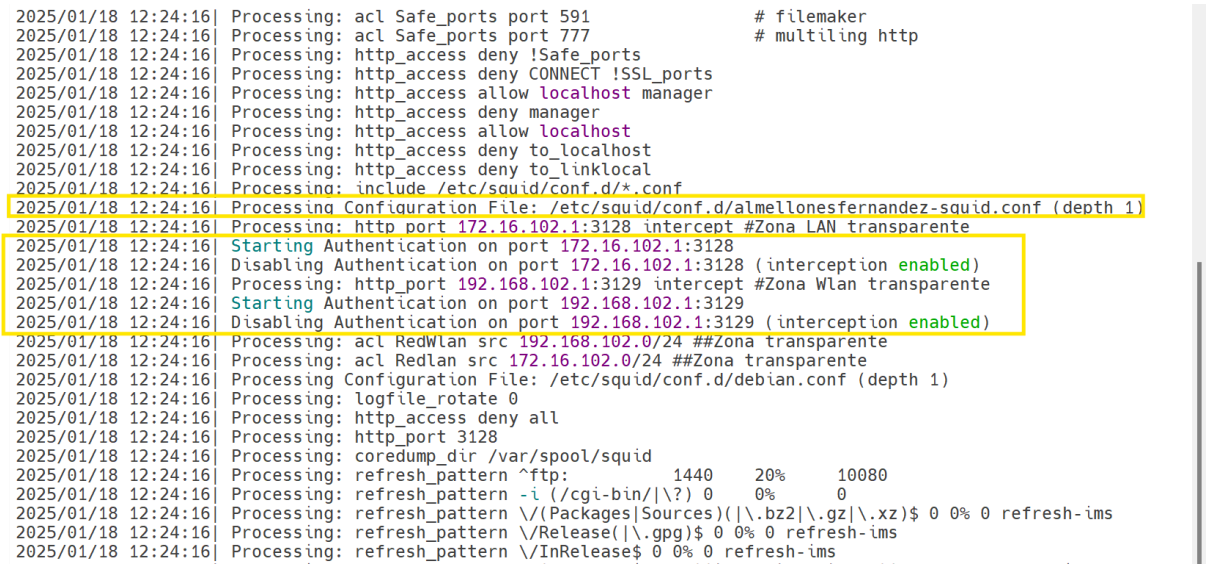
Álvaro Almellones Fernández

SEGURIDAD PERIMETRAL

1. **(2,5 puntos)** Instalaciones y configuraciones previas:

a) **(0,75 puntos)** Instalación del servicio squid, configuración en modo transparente para las dos zonas LAN (puerto 3128) y WLAN (3129), no realizando dicha configuración directamente sobre fichero squid.conf, si no en fichero en el directorio ".conf.d/XXxx-squid.conf". (netstat, systemctl, etc.)





b) **(0,5 puntos)** Adaptación del script del cortafuegos para prohibir la regla de FORWARD de http desde las dos zonas en modo DROP (esto lo haremos para tener la certeza de que no debe pasar nada por esa regla en todo el ejercicio) y para correcto funcionamiento para http en squid. En este momento no debería funcionar nada relacionado con http, ya que http_access deny all (única directiva configurada), lo cortaría todo, pero si con https.

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v --line-number
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REDIRECT   6    --  lan2   *       172.16.102.0/24      0.0.0.0/0            tcp dpt:80 redir por
ts 3128
2        0     0 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir por
ts 3129
3        0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.1
02.2:80
4        0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.
102.2:443
5        0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej N
ATP */ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 MASQUERADE  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ
a WAN */
2        0     0 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN
a WAN */
3        0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN
 a WAN */
root@almellonesfernandez-firewall:~/scripts#
```

```
root@almellonesfernandez-firewall:~/scripts# iptables -t filter -L -n -v --line-number
Chain INPUT (policy DROP 8 packets, 256 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
2       92  6416 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permit
ir SSH desde WAN */
3        1    28 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping des
de cualquier subred */
4        0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permit
ir SSH desde LAN */
5        0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permit
ir SSH desde DMZ */
6        0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3128 /* Zona
 LAN */
7        0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3129 /* Zona
 WLAN */
8        0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
ISHED /* Respuestas OUTPUT */
```

Álvaro Almellones Fernández

```
9        0     0 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
ISHED /* Respuesta WAN a DMZ */
10       0     0 DROP       6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:80
11       0     0 ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:443
12       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:53
13       0     0 ACCEPT     1    --  lan2   wan2    172.16.102.2         0.0.0.0/0
14       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:123
15       0     0 DROP       6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:80
16       0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:443
17       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:53
18       0     0 ACCEPT     1    --  lan2   wan2    172.16.102.3         0.0.0.0/0
19       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:123
20       0     0 DROP       6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:80
21       0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:443
22       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:53
23       0     0 ACCEPT     1    --  lan2   wan2    172.16.102.4         0.0.0.0/0
24       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:123
25       0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
ISHED /* Respuesta WAN a LAN */
26       0     0 DROP       6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
27       0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
28       0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
29       0     0 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
30       0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:123
31       0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
ISHED /* Respuesta WAN a WLAN */
32       0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
33       0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
34       0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
35       0     0 ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
```

```
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget http://google.com
--2025-01-18 12:10:00--  http://google.com/
Resolving google.com (google.com)... 142.250.200.110, 2a00:1450:4003:803::200e
Connecting to google.com (google.com)|142.250.200.110|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 12:10:01 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-intranet:~$ wget https://google.com
--2025-01-18 12:10:07--  https://google.com/
Resolving google.com (google.com)... 142.250.200.110, 2a00:1450:4003:803::200e
Connecting to google.com (google.com)|142.250.200.110|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/ [following]
--2025-01-18 12:10:10--  https://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.201.68, 2a00:1450:4003:80c::2004
Connecting to www.google.com (www.google.com)|142.250.201.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.7'

index.html.7                    [ <=>                                   ]  19,36K  --.-KB/s    in 0,03s

2025-01-18 12:10:10 (688 KB/s) - 'index.html.7' saved [19822]

almellonesfernandez@almellonesfernandez-us-intranet:~$
```

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget http://google.com
--2025-01-18 12:12:22--  http://google.com/
Resolving google.com (google.com)... 142.250.184.14, 2a00:1450:4003:803::200e
Connecting to google.com (google.com)|142.250.184.14|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 12:12:23 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-wlan:~$ wget https://google.com
--2025-01-18 12:12:34--  https://google.com/
Resolving google.com (google.com)... 142.250.184.14, 2a00:1450:4003:803::200e
Connecting to google.com (google.com)|142.250.184.14|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/ [following]
--2025-01-18 12:12:37--  https://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.17.4, 2a00:1450:4003:802::2004
Connecting to www.google.com (www.google.com)|172.217.17.4|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.2'

index.html.2                    [ <=>                                   ]  19,33K  --.-KB/s    in 0,001s

2025-01-18 12:12:38 (26,6 MB/s) - 'index.html.2' saved [19789]

almellonesfernandez@almellonesfernandez-us-wlan:~$
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v --line-number
Chain PREROUTING (policy ACCEPT 71 packets, 2982 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        1    60 REDIRECT   6    --  lan2   *       172.16.102.0/24      0.0.0.0/0            tcp dpt:80 redir por
ts 3128
2        1    60 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir por
ts 3129
3        0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.1
02.2:80
4        0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.
102.2:443
5        0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej N
ATP */ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 4 packets, 266 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 MASQUERADE  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ
a WAN */
2        7   472 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN
a WAN */
3       10   660 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN
 a WAN */
root@almellonesfernandez-firewall:~/scripts#
```

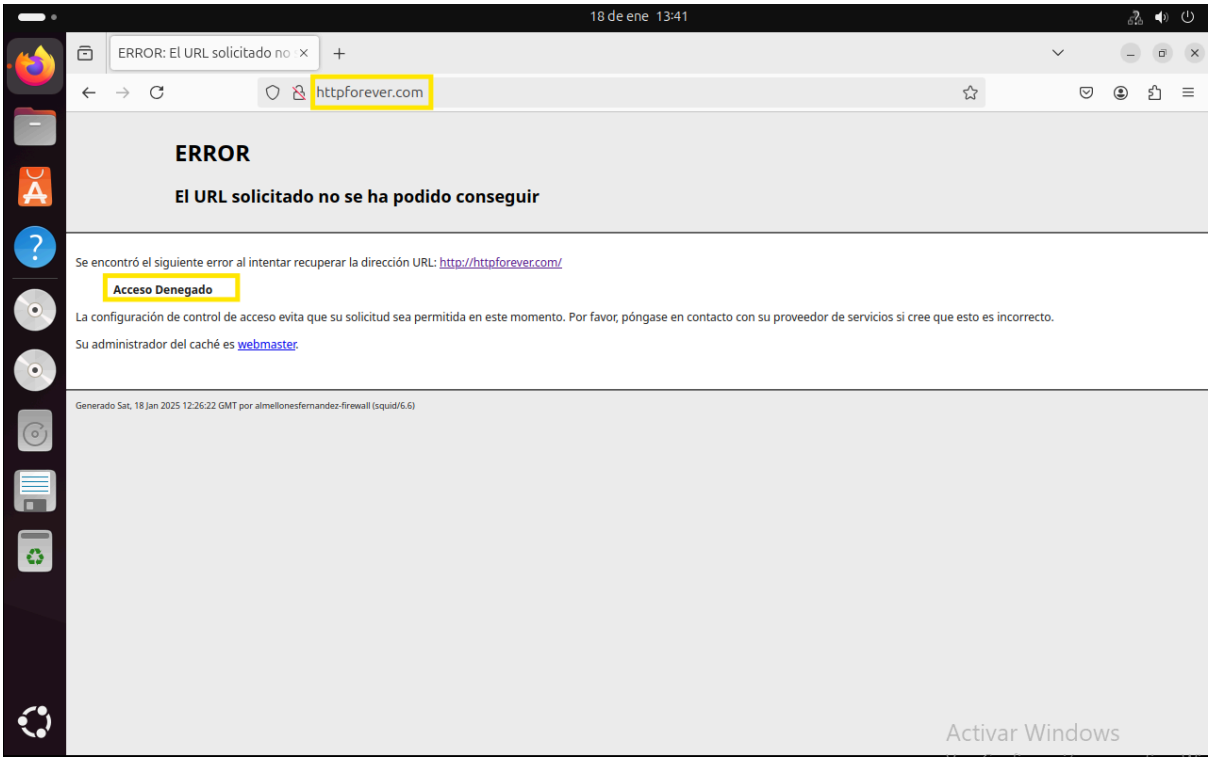
```
root@almellonesfernandez-firewall:~/scripts# iptables -t filter -L -n -v --line-number
Chain INPUT (policy DROP 56 packets, 1930 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        4   268 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
2      336 21424 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permit
ir SSH desde WAN */
3        5   140 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping des
de cualquier subred */
4        0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permit
ir SSH desde LAN */
5        0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permit
ir SSH desde DMZ */
6        7   497 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3128 /* Zona
 LAN */
7        8   549 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3129 /* Zona
 WLAN */
8     2871  257K ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
ISHED /* Respuestas OUTPUT */
```

```
10       0     0 DROP       6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:80
11      27  2738 ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:443
12       4   276 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:53
13       0     0 ACCEPT     1    --  lan2   wan2    172.16.102.2         0.0.0.0/0
14       1    76 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:123
15       0     0 DROP       6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:80
16       0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:443
17       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:53
18       0     0 ACCEPT     1    --  lan2   wan2    172.16.102.3         0.0.0.0/0
19       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:123
20       0     0 DROP       6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:80
21       0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:443
22       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:53
23       0     0 ACCEPT     1    --  lan2   wan2    172.16.102.4         0.0.0.0/0
24       0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:123
25      35 37951 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
ISHED /* Respuesta WAN a LAN */
26       0     0 DROP       6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
27      29  2818 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
28       8   540 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
29       0     0 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
30       0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:123
31      35 36569 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABL
ISHED /* Respuesta WAN a WLAN */
```

Las reglas drop del puerto 80 no aumenta ya que antes se hace el prerouting al 3128 y 3129 demostrando así que pasa correctamente por el squid, además aumentan los contadores de las reglas input y prerouting de estos puertos

Además, se deben realizar evidencias con netstat, tcpdump e iptraf-ng, para

demostrar que existen conexiones **establecidas** en los puertos de escucha de squid.




```
root@almellonesfernandez-firewall:~/scripts# netstat -putan | grep ESTABLISHED | grep squid
tcp        0      0 172.16.102.1:3128       172.16.102.4:33130      ESTABLISHED 1272/(squid-1)
udp6       0      0 ::1:50018               ::1:41777               ESTABLISHED 1272/(squid-1)
root@almellonesfernandez-firewall:~/scripts#
```

c) **(0,25 puntos)** Deny_info personalizado para la **acl all** y evidencia de su funcionamiento.

```
  GNU nano 7.2                          almellonesfernandez-squid.conf
http_port 172.16.102.1:3128 intercept #Zona LAN transparente
http_port 192.168.102.1:3129 intercept #Zona Wlan transparente

acl RedWlan src 192.168.102.0/24 ##Zona transparente
acl Redlan src 172.16.102.0/24 ##Zona transparente

deny_info https://www.naughtydog.com/  all

#http_access allow RedWlan
#http_access allow Redlan
```

```
2025/01/18 14:08:27| Processing: acl Safe_ports port 777               # multiling http
2025/01/18 14:08:27| Processing: http_access deny !Safe_ports
2025/01/18 14:08:27| Processing: http_access deny CONNECT !SSL_ports
2025/01/18 14:08:27| Processing: http_access allow localhost manager
2025/01/18 14:08:27| Processing: http_access deny manager
2025/01/18 14:08:27| Processing: http_access allow localhost
2025/01/18 14:08:27| Processing: http_access deny to_localhost
2025/01/18 14:08:27| Processing: http_access deny to_linklocal
2025/01/18 14:08:27| Processing: include /etc/squid/conf.d/*.conf
2025/01/18 14:08:27| Processing Configuration File: /etc/squid/conf.d/almellonesfernandez-squid.conf (depth 1)
2025/01/18 14:08:27| Processing: http_port 172.16.102.1:3128 intercept #Zona LAN transparente
2025/01/18 14:08:27| Starting Authentication on port 172.16.102.1:3128
2025/01/18 14:08:27| Disabling Authentication on port 172.16.102.1:3128 (interception enabled)
2025/01/18 14:08:27| Processing: http_port 192.168.102.1:3129 intercept #Zona Wlan transparente
2025/01/18 14:08:27| Starting Authentication on port 192.168.102.1:3129
2025/01/18 14:08:27| Disabling Authentication on port 192.168.102.1:3129 (interception enabled)
2025/01/18 14:08:27| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/18 14:08:27| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/18 14:08:27| Processing: deny_info https://www.naughtydog.com/  all
2025/01/18 14:08:27| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 14:08:27| Processing: logfile_rotate 0
2025/01/18 14:08:27| Processing: http_access deny all
2025/01/18 14:08:27| Processing: http_port 3128
2025/01/18 14:08:27| Processing: coredump_dir /var/spool/squid
2025/01/18 14:08:27| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 14:08:27| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 14:08:27| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 14:08:27| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 14:08:27| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 14:08:27| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 14:08:27| Processing: refresh_pattern .               0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```



```
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget httpforever.com
--2025-01-18 13:06:22--  http://httpforever.com/
Resolving httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0::1f1:2000
Connecting to httpforever.com (httpforever.com)|146.190.62.39|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.naughtydog.com/ [following]
--2025-01-18 13:06:22--  https://www.naughtydog.com/
Resolving www.naughtydog.com (www.naughtydog.com)... 100.25.73.52
Connecting to www.naughtydog.com (www.naughtydog.com)|100.25.73.52|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.10'

index.html.10                   [  <=>                                  ]  43,30K   187KB/s    in 0,2s

2025-01-18 13:06:26 (187 KB/s) - 'index.html.10' saved [44344]

almellonesfernandez@almellonesfernandez-us-intranet:~$
```

d) **(0,25 puntos)** Personalizar la opción visible_hostname (proxyXXxx.es) y el fichero access.log (accessXXxx-squid.log) y evidencia de su funcionamiento.

```
  GNU nano 7.2                          almellonesfernandez-squid.conf
http_port 172.16.102.1:3128 intercept #Zona LAN transparente
http_port 192.168.102.1:3129 intercept #Zona Wlan transparente

acl RedWlan src 192.168.102.0/24 ##Zona transparente
acl Redlan src 172.16.102.0/24 ##Zona transparente

#deny_info https://www.naughtydog.com/  all

visible_hostname proxyAlmellonesfernandez.es
access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log

#http_access allow RedWlan
#http_access allow Redlan
```

Álvaro Almellones Fernández

```
2025/01/18 16:07:31| Processing: http_access deny !Safe_ports
2025/01/18 16:07:31| Processing: http_access deny CONNECT !SSL_ports
2025/01/18 16:07:31| Processing: http_access allow localhost manager
2025/01/18 16:07:31| Processing: http_access deny manager
2025/01/18 16:07:31| Processing: http_access allow localhost
2025/01/18 16:07:31| Processing: http_access deny to_localhost
2025/01/18 16:07:31| Processing: http_access deny to_linklocal
2025/01/18 16:07:31| Processing: include /etc/squid/conf.d/*.conf
2025/01/18 16:07:31| Processing Configuration File: /etc/squid/conf.d/almellonesfernandez-squid.conf (depth 1)
2025/01/18 16:07:31| Processing: http_port 172.16.102.1:3128 intercept #Zona LAN transparente
2025/01/18 16:07:31| Starting Authentication on port 172.16.102.1:3128
2025/01/18 16:07:31| Disabling Authentication on port 172.16.102.1:3128 (interception enabled)
2025/01/18 16:07:31| Processing: http_port 192.168.102.1:3129 intercept #Zona Wlan transparente
2025/01/18 16:07:31| Starting Authentication on port 192.168.102.1:3129
2025/01/18 16:07:31| Disabling Authentication on port 192.168.102.1:3129 (interception enabled)
2025/01/18 16:07:31| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/18 16:07:31| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/18 16:07:31| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/18 16:07:31| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/18 16:07:31| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 16:07:31| Processing: logfile_rotate 0
2025/01/18 16:07:31| Processing: http_access deny all
2025/01/18 16:07:31| Processing: http_port 3128
2025/01/18 16:07:31| Processing: coredump_dir /var/spool/squid
2025/01/18 16:07:31| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 16:07:31| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 16:07:31| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 16:07:31| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 16:07:31| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 16:07:31| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 16:07:31| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d# 
```



```
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget example.com
--2025-01-18 15:08:28--  http://example.com/
Resolving example.com (example.com)... 23.215.0.138, 23.192.228.84, 23.192.228.80, ...
Connecting to example.com (example.com)|23.215.0.138|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 15:08:28 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-intranet:~$ 
```

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget httpforever.com
--2025-01-18 15:08:46--  http://httpforever.com/
Resolving httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0::1f1:2000
Connecting to httpforever.com (httpforever.com)|146.190.62.39|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 15:08:46 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-wlan:~$ 
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall /etc/squid/conf.d# cat /var/log/squid/accessAlmellonesfernandez-squid.log
1737212497.948    303 172.16.102.2 TCP_DENIED/302 345 GET http://example.com/ - HIER_NONE/- text/html
1737212626.701     52 172.16.102.2 TCP_DENIED/403 3918 GET http://example.com/ - HIER_NONE/- text/html
1737212717.492    122 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737212719.075      0 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737212723.082      0 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737212731.956      0 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737212747.180      0 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737212908.958     25 172.16.102.2 TCP_DENIED/403 3918 GET http://example.com/ - HIER_NONE/- text/html
1737212926.552     87 192.168.102.2 TCP_DENIED/403 3931 GET http://httpforever.com/ - HIER_NONE/- text/html
1737213126.861     17 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737213128.700      0 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737213132.672      0 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737213140.626      0 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737213156.476      1 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737213188.443     27 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737213255.355   1069 172.16.102.4 TCP_DENIED/403 3892 GET http://connectivity-check.ubuntu.com/ - HIER_NONE/- tex
t/html
1737213287.099   5952 172.16.102.4 TCP_DENIED_ABORTED/403 0 GET http://detectportal.firefox.com/canonical.html - H
IER_NONE/- text/html
1737213287.318    154 172.16.102.4 TCP_DENIED/403 4291 GET http://detectportal.firefox.com/canonical.html - HIER_N
```


e) **(0,25 puntos)** Evidenciar de que no se deja rastros de la IP del cliente, únicamente desde la red. Reestablecer para que siempre guarde la IP del cliente web.

```
  GNU nano 7.2                          almellonesfernandez-squid.conf
http_port 172.16.102.1:3128 intercept #Zona LAN transparente
http_port 192.168.102.1:3129 intercept #Zona Wlan transparente

acl RedWlan src 192.168.102.0/24 ##Zona transparente
acl Redlan src 172.16.102.0/24 ##Zona transparente

#deny_info https://www.naughtydog.com/  all

visible_hostname proxyAlmellonesfernandez.es
access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
client_netmask 255.255.0.0
#http_access allow RedWlan
#http_access allow Redlan
```

```
2025/01/18 16:36:47| Processing: http_access deny CONNECT !SSL_ports
2025/01/18 16:36:47| Processing: http_access allow localhost manager
2025/01/18 16:36:47| Processing: http_access deny manager
2025/01/18 16:36:47| Processing: http_access allow localhost
2025/01/18 16:36:47| Processing: http_access deny to_localhost
2025/01/18 16:36:47| Processing: http_access deny to_linklocal
2025/01/18 16:36:47| Processing: include /etc/squid/conf.d/*.conf
2025/01/18 16:36:47| Processing Configuration File: /etc/squid/conf.d/almellonesfernandez-squid.conf (depth 1)
2025/01/18 16:36:47| Processing: http_port 172.16.102.1:3128 intercept #Zona LAN transparente
2025/01/18 16:36:47| Starting Authentication on port 172.16.102.1:3128
2025/01/18 16:36:47| Disabling Authentication on port 172.16.102.1:3128 (interception enabled)
2025/01/18 16:36:47| Processing: http_port 192.168.102.1:3129 intercept #Zona Wlan transparente
2025/01/18 16:36:47| Starting Authentication on port 192.168.102.1:3129
2025/01/18 16:36:47| Disabling Authentication on port 192.168.102.1:3129 (interception enabled)
2025/01/18 16:36:47| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/18 16:36:47| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/18 16:36:47| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/18 16:36:47| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/18 16:36:47| Processing: client_netmask 255.255.0.0
2025/01/18 16:36:47| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 16:36:47| Processing: logfile_rotate 0
2025/01/18 16:36:47| Processing: http_access deny all
2025/01/18 16:36:47| Processing: http_port 3128
2025/01/18 16:36:47| Processing: coredump_dir /var/spool/squid
2025/01/18 16:36:47| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 16:36:47| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 16:36:47| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 16:36:47| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 16:36:47| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
```

```
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget example.com
--2025-01-18 15:28:49--  http://example.com/
Resolving example.com (example.com)... 96.7.128.175, 23.215.0.138, 23.192.228.84, ...
Connecting to example.com (example.com)|96.7.128.175|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 15:28:49 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-intranet:~$
```

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget httpforever.com
--2025-01-18 15:29:00--  http://httpforever.com/
Resolving httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0::1f1:2000
Connecting to httpforever.com (httpforever.com)|146.190.62.39|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 15:29:01 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-wlan:~$
```

```
root@almellonesfernandez-firewall:/etc/squid/conf.d# tail -5 /var/log/squid/accessAlmellonesfernandez-squid.log
1737213524.582      0 172.16.102.4 TCP_DENIED/403 4291 GET http://detectportal.firefox.com/canonical.html - HIER_N
ONE/- text/html
1737213524.585      0 172.16.102.4 TCP_DENIED/403 4291 GET http://detectportal.firefox.com/canonical.html - HIER_N
ONE/- text/html
1737213524.587      0 172.16.102.4 TCP_DENIED/403 4291 GET http://detectportal.firefox.com/canonical.html - HIER_N
ONE/- text/html
1737214129.770     17 172.16.0.0 TCP_DENIED/403 3918 GET http://example.com/ - HIER_NONE/- text/html
1737214141.089     88 192.168.0.0 TCP_DENIED/403 3931 GET http://httpforever.com/ - HIER_NONE/- text/html
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

f) **(0,5 puntos)** Además configurar para que haya dos ficheros más de log, una con la opción combined (accessXXxx-combined.log) y uno con un formato realizado por vosotros con todas las opciones posibles (accessXXxx-personalizado.log).

```
root@almellonesfernandez-firewall:/var/log/squid# cd /etc/squid/
root@almellonesfernandez-firewall:/etc/squid# cd conf.d/
root@almellonesfernandez-firewall:/etc/squid/conf.d# cat almellonesfernandez-squid.conf |grep log
logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv %Sh/%<A %>Hs %<st %rm %ru %>a "%{
Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Álvaro Almellones Fernández

```
2025/01/18 16:50:53| Processing: http_access deny to_linklocal
2025/01/18 16:50:53| Processing: include /etc/squid/conf.d/*.conf
2025/01/18 16:50:53| Processing Configuration File: /etc/squid/conf.d/almellonesfernandez-squid.conf (depth 1)
2025/01/18 16:50:53| Processing: http_port 172.16.102.1:3128 intercept #Zona LAN transparente
2025/01/18 16:50:53| Starting Authentication on port 172.16.102.1:3128
2025/01/18 16:50:53| Disabling Authentication on port 172.16.102.1:3128 (interception enabled)
2025/01/18 16:50:53| Processing: http_port 192.168.102.1:3129 intercept #Zona Wlan transparente
2025/01/18 16:50:53| Starting Authentication on port 192.168.102.1:3129
2025/01/18 16:50:53| Disabling Authentication on port 192.168.102.1:3129 (interception enabled)
2025/01/18 16:50:53| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/18 16:50:53| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/18 16:50:53| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/18 16:50:53| Processing: logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv
%Sh/%<A %>Hs %<st %rm %ru %>a "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
2025/01/18 16:50:53| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/18 16:50:53| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/18 16:50:53| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/18 16:50:53| Processing: client_netmask 255.255.0.0
2025/01/18 16:50:53| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 16:50:53| Processing: logfile_rotate 0
2025/01/18 16:50:53| Processing: http_access deny all
2025/01/18 16:50:53| Processing: http_port 3128
2025/01/18 16:50:53| Processing: coredump_dir /var/spool/squid
2025/01/18 16:50:53| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 16:50:53| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 16:50:53| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 16:50:53| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 16:50:53| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 16:50:53| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 16:50:53| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/var/log/squid#
```



```
almellonesfernandez@almellonesfernandez-us-intranet ~$ wget example.com
--2025-01-18 15:49:08--  http://example.com/
Resolving example.com (example.com)... 23.192.228.84, 23.192.228.80, 96.7.128.198, ...
Connecting to example.com (example.com)|23.192.228.84|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 15:49:08 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-intranet:~$
```

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget httpforever.com
--2025-01-18 15:49:12--  http://httpforever.com/
Resolving httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0::1f1:2000
Connecting to httpforever.com (httpforever.com)|146.190.62.39|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-01-18 15:49:12 ERROR 403: Forbidden.

almellonesfernandez@almellonesfernandez-us-wlan:~$
```

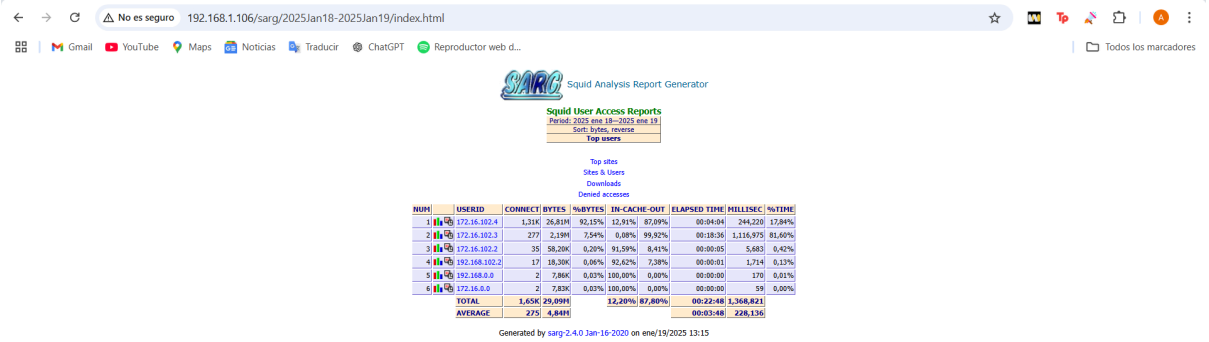
```
root@almellonesfernandez-firewall:/etc/squid/conf.d# cd /var/log/squid/
root@almellonesfernandez-firewall:/var/log/squid# ls
accessAlmellonesfernandez-combined.log       accessAlmellonesfernandez-squid.log  access.log.1  cache.log.1
accessAlmellonesfernandez-personalizado.log  access.log                           cache.log
root@almellonesfernandez-firewall:/var/log/squid# cat accessAlmellonesfernandez-combined.log
172.16.0.0 - - [18/Jan/2025:16:49:08 +0100] "GET http://example.com/ HTTP/1.1" 403 3918 "-" "Wget/1.21.4" TCP_DENI
ED:HIER_NONE
192.168.0.0 - - [18/Jan/2025:16:49:12 +0100] "GET http://httpforever.com/ HTTP/1.1" 403 3931 "-" "Wget/1.21.4" TCP
_DENIED:HIER_NONE
root@almellonesfernandez-firewall:/var/log/squid# cat accessAlmellonesfernandez-personalizado.log
1737215348 18/Jan/2025:15:49:08 172.16.0.0 - - - GET http://example.com/  HTTP/1.1 HIER_NONE/- 403 3918 GET http:/
/example.com/ 172.16.0.0 "-" "Wget/1.21.4" TCP_DENIED:HIER_NONE 42 18/Jan/2025:15:49:08 -
1737215352 18/Jan/2025:15:49:12 192.168.0.0 - - - GET http://httpforever.com/  HTTP/1.1 HIER_NONE/- 403 3931 GET h
ttp://httpforever.com/ 192.168.0.0 "-" "Wget/1.21.4" TCP_DENIED:HIER_NONE 82 18/Jan/2025:15:49:12 -
root@almellonesfernandez-firewall:/var/log/squid#
```

Álvaro Almellones Fernández

HERRAMIENTAS DE MONITORIZACIÓN

2. **(2 puntos, Investigación)** Realice la instalación y posterior configuración de 2 loganizadores de proxy web entre los siguientes:
a) Sarg.
b) Awstats.
c) Squid Analyzer.
d) Calamaris.
e) Fiddler
f) Burp Suite.

```
root@almellonesfernandez-firewall:/var/log/squid# calamaris -a accessAlmellonesfernandez-squid.log

 Proxy-Report

Report period: 18.Jan 25 16:01:37 - 18.Jan 25 16:49:12
Generated at: 18.Jan 25 17:08:17

# Summary
Calamaris statistics
------------------------------------------------------ --------------- ----------
lines parsed:                                                    lines         88
invalid lines:                                                   lines          0
parse time:                                                        sec          1
parse speed:                                                 lines/sec         88
------------------------------------------------------ --------------- ----------
Proxy statistics
------------------------------------------------------ --------------- ----------
Total amount:                                                 requests         88
unique hosts/users:                                              hosts          5
Total Bandwidth:                                                  Byte     341528
Proxy efficiency (HIT [kB/sec] / DIRECT [kB/sec]):              factor       0.00
Average speed increase:                                            %       0.00
TCP response time of 100% requests:                             msec        136
------------------------------------------------------ --------------- ----------
Cache statistics
------------------------------------------------------ --------------- ----------
Total amount cached:                                          requests          0
Request hit rate:                                                  %       0.00
Bandwidth savings:                                                Byte          0
Bandwidth savings in Percent (Byte hit rate):                      %       0.00
Average cached object size:                                       Byte          0
Average direct object size:                                       Byte       3881
```

***** Se realiza la instalación en este apartado para qué al realizar el ejercicio al completo, podáis recoger capturas de toda la información que está recogiendo cada loganizador, en función de la configuración de**

vuestra práctica.

**** Se recomienda un snapshot, con explicación de lo que hace.*

Muestre, aunque no se valorará.

Álvaro Almellones Fernández

SEGURIDAD PERIMETRAL

3. (2,5 puntos) Filtros HTTP_ACCESS BÁSICOS.

A continuación, se deja al alumno que elija los ejemplos, orden que tiene que tener las directivas http_access en el fichero de configuración y las capturas que desee para evidenciar directivas relacionadas con (deben funcionar todas a la vez, el enunciado está redactada de forma que vaya creciendo):

a) **(0,5 puntos)** Restricciones por la directiva url_regex por ciertas palabras en las dos subredes.

```
 GNU nano 7.2                              almellonesfernandez-squid.conf
http_port 172.16.102.1:3128 intercept #Zona LAN transparente
http_port 192.168.102.1:3129 intercept #Zona Wlan transparente

acl RedWlan src 192.168.102.0/24 ##Zona transparente
acl Redlan src 172.16.102.0/24 ##Zona transparente

#deny_info https://www.naughtydog.com/  all

visible_hostname proxyAlmellonesfernandez.es

logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv %Sh/%<A %>Hs %<st %rm %ru %>a "%>

access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato

#client_netmask 255.255.0.0

acl lista_url_prohibidas_aaf url_regex  mercadona bershka

http_access deny lista_url_prohibidas_aaf
deny_info https://www.game.es/  lista_url_prohibidas_aaf


http_access allow RedWlan
http_access allow Redlan


^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

```
2025/01/18 17:42:38| Starting Authentication on port 172.16.102.1:3128
2025/01/18 17:42:38| Disabling Authentication on port 172.16.102.1:3128 (interception enabled)
2025/01/18 17:42:38| Processing: http_port 192.168.102.1:3129 intercept #Zona Wlan transparente
2025/01/18 17:42:38| Starting Authentication on port 192.168.102.1:3129
2025/01/18 17:42:38| Disabling Authentication on port 192.168.102.1:3129 (interception enabled)
2025/01/18 17:42:38| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/18 17:42:38| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/18 17:42:38| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/18 17:42:38| Processing: logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv
%Sh/%<A %>Hs %<st %rm %ru %>a "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
2025/01/18 17:42:38| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/18 17:42:38| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/18 17:42:38| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/18 17:42:38| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka
2025/01/18 17:42:38| Processing: http_access deny lista_url_prohibidas_aaf
2025/01/18 17:42:38| Processing: deny_info https://www.game.es/  lista_url_prohibidas_aaf
2025/01/18 17:42:38| Processing: http_access allow RedWlan
2025/01/18 17:42:38| Processing: http_access allow Redlan
2025/01/18 17:42:38| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 17:42:38| Processing: logfile_rotate 0
2025/01/18 17:42:38| Processing: http_access deny all
2025/01/18 17:42:38| Processing: http_port 3128
2025/01/18 17:42:38| Processing: coredump_dir /var/spool/squid
2025/01/18 17:42:38| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 17:42:38| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 17:42:38| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 17:42:38| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 17:42:38| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 17:42:38| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 17:42:38| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

```
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget mercadona.com
--2025-01-18 16:40:24--  http://mercadona.com/
Resolving mercadona.com (mercadona.com)... 195.53.40.253
Connecting to mercadona.com (mercadona.com)|195.53.40.253|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.game.es/ [following]
--2025-01-18 16:40:24--  https://www.game.es/
Resolving www.game.es (www.game.es)... 212.170.159.195
Connecting to www.game.es (www.game.es)|212.170.159.195|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1281499 (1,2M) [text/html]
Saving to: 'index.html.19'

index.html.19               100%[=========================================>]   1,22M  7,48MB/s    in 0,2s

2025-01-18 16:40:24 (7,48 MB/s) - 'index.html.19' saved [1281499/1281499]

almellonesfernandez@almellonesfernandez-us-intranet:~$ wget bershka.com
--2025-01-18 16:40:27--  http://bershka.com/
Resolving bershka.com (bershka.com)... 2.20.253.160, 2.20.253.149, 2.20.253.163, ...
Connecting to bershka.com (bershka.com)|2.20.253.160|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.game.es/ [following]
--2025-01-18 16:40:27--  https://www.game.es/
Resolving www.game.es (www.game.es)... 212.170.159.195
Connecting to www.game.es (www.game.es)|212.170.159.195|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1281499 (1,2M) [text/html]
Saving to: 'index.html.20'

index.html.20               100%[=========================================>]   1,22M  7,11MB/s    in 0,2s
```



```
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget mercadona.com
--2025-01-18 16:40:51--  http://mercadona.com/
Resolving mercadona.com (mercadona.com)... 195.53.40.253
Connecting to mercadona.com (mercadona.com)|195.53.40.253|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.game.es/ [following]
--2025-01-18 16:40:52--  https://www.game.es/
Resolving www.game.es (www.game.es)... 212.170.159.195
Connecting to www.game.es (www.game.es)|212.170.159.195|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1281499 (1,2M) [text/html]
Saving to: 'index.html.5'

index.html.5                100%[=========================================>]   1,22M  --.-KB/s    in 0,1s

2025-01-18 16:40:52 (9,93 MB/s) - 'index.html.5' saved [1281499/1281499]

almellonesfernandez@almellonesfernandez-us-wlan:~$ wget bershka.com
--2025-01-18 16:40:54--  http://bershka.com/
Resolving bershka.com (bershka.com)... 2.18.40.147, 2.18.40.139, 2a02:26f0:b80:18::214:4415, ...
Connecting to bershka.com (bershka.com)|2.18.40.147|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.game.es/ [following]
--2025-01-18 16:40:55--  https://www.game.es/
Resolving www.game.es (www.game.es)... 212.170.159.195
Connecting to www.game.es (www.game.es)|212.170.159.195|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1281499 (1,2M) [text/html]
Saving to: 'index.html.6'

index.html.6                100%[=========================================>]   1,22M  7,02MB/s    in 0,2s
```


b) **(0,5 puntos)** Restricciones en el uso de los navegadores (user-agent) en las dos subredes

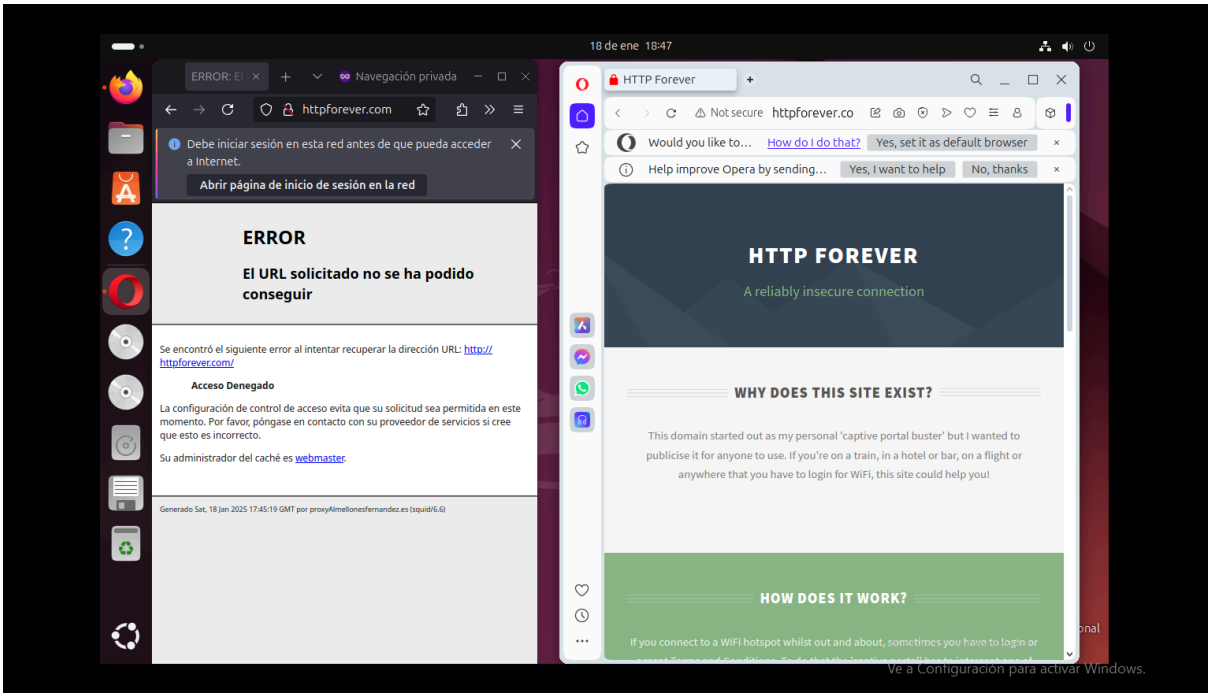
Álvaro Almellones Fernández

```
 GNU nano 7.2                              almellonesfernandez-squid.conf *
http_port 172.16.102.1:3128 intercept #Zona LAN transparente
http_port 192.168.102.1:3129 intercept #Zona Wlan transparente

acl RedWlan src 192.168.102.0/24 ##Zona transparente
acl Redlan src 172.16.102.0/24 ##Zona transparente

#deny_info https://www.naughtydog.com/  all

visible_hostname proxyAlmellonesfernandez.es

logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv %Sh/%<A %>Hs %<st %rm %ru %>a "%>

access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato

#client_netmask 255.255.0.0

acl lista_url_prohibidas_aaf url_regex  mercadona bershka
http_access deny lista_url_prohibidas_aaf
deny_info https://www.game.es/  lista_url_prohibidas_aaf

acl lista_Navegadores_prohibidos_aaf browser -i Firefox
http_access deny lista_Navegadores_prohibidos_aaf


http_access allow RedWlan

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```



```
2025/01/18 18:48:22| Processing: http_port 192.168.102.1:3129 intercept #Zona Wlan transparente
2025/01/18 18:48:22| Starting Authentication on port 192.168.102.1:3129
2025/01/18 18:48:22| Disabling Authentication on port 192.168.102.1:3129 (interception enabled)
2025/01/18 18:48:22| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/18 18:48:22| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/18 18:48:22| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/18 18:48:22| Processing: logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv
%Sh/%<A %>Hs %<st %rm %ru %>a "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
2025/01/18 18:48:22| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/18 18:48:22| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/18 18:48:22| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/18 18:48:22| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka
2025/01/18 18:48:22| Processing: http_access deny lista_url_prohibidas_aaf
2025/01/18 18:48:22| Processing: deny_info https://www.game.es/  lista_url_prohibidas_aaf
2025/01/18 18:48:22| Processing: acl lista_Navegadores_prohibidos_aaf browser -i Firefox
2025/01/18 18:48:22| Processing: http_access deny lista_Navegadores_prohibidos_aaf
2025/01/18 18:48:22| Processing: http_access allow RedWlan
2025/01/18 18:48:22| Processing: http_access allow Redlan
2025/01/18 18:48:22| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 18:48:22| Processing: logfile_rotate 0
2025/01/18 18:48:22| Processing: http_access deny all
2025/01/18 18:48:22| Processing: http_port 3128
2025/01/18 18:48:22| Processing: coredump_dir /var/spool/squid
2025/01/18 18:48:22| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 18:48:22| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 18:48:22| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 18:48:22| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 18:48:22| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 18:48:22| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 18:48:22| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Álvaro Almellones Fernández



c) **(0,5 puntos)** Restricciones en el uso de ciertos dominios en las dos subredes, a partir de un fichero de texto.

```
root@almellonesfernandez-firewall:/etc/squid/conf.d# cat almellonesfernandez-domain.txt
youtube.com
twitter.com

root@almellonesfernandez-firewall:/etc/squid/conf.d# cat almellonesfernandez-squid.conf | grep Dominio
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
http_access deny Lista_Dominios_Prohibidos_aaf
deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Álvaro Almellones Fernández

```
2025/01/18 19:11:15| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/18 19:11:15| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/18 19:11:15| Processing: logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv
%Sh/%<A %>Hs %<st %rm %ru %>a "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
2025/01/18 19:11:16| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/18 19:11:16| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/18 19:11:16| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/18 19:11:16| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka
2025/01/18 19:11:16| Processing: http_access deny lista_url_prohibidas_aaf
2025/01/18 19:11:16| Processing: deny_info https://www.game.es/  lista_url_prohibidas_aaf
2025/01/18 19:11:16| Processing: acl lista_Navegadores_prohibidos_aaf browser -i Firefox
2025/01/18 19:11:16| Processing: http_access deny lista_Navegadores_prohibidos_aaf
2025/01/18 19:11:16| Processing: acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernande
z-domain.txt"
2025/01/18 19:11:16| Processing: http_access deny Lista_Dominios_Prohibidos_aaf
2025/01/18 19:11:16| Processing: deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf
2025/01/18 19:11:16| Processing: http_access allow RedWlan
2025/01/18 19:11:16| Processing: http_access allow Redlan
2025/01/18 19:11:16| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 19:11:16| Processing: logfile_rotate 0
2025/01/18 19:11:16| Processing: http_access deny all
2025/01/18 19:11:16| Processing: http_port 3128
2025/01/18 19:11:16| Processing: coredump_dir /var/spool/squid
2025/01/18 19:11:16| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 19:11:16| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 19:11:16| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 19:11:16| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 19:11:16| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 19:11:16| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 19:11:16| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```



```
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget twitter.com
--2025-01-18 18:07:23--  http://twitter.com/
Resolving twitter.com (twitter.com)... 104.244.42.1
Connecting to twitter.com (twitter.com)|104.244.42.1|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.eroski.es/ [following]
--2025-01-18 18:07:23--  https://www.eroski.es/
Resolving www.eroski.es (www.eroski.es)... 159.60.134.230
Connecting to www.eroski.es (www.eroski.es)|159.60.134.230|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 316756 (309K) [text/html]
Saving to: 'index.html.23'

index.html.23               100%[=========================================>] 309,33K  --.-KB/s    in 0,07s

2025-01-18 18:07:23 (4,39 MB/s) - 'index.html.23' saved [316756/316756]

almellonesfernandez@almellonesfernandez-us-intranet:~$ wget youtube.com
--2025-01-18 18:08:19--  http://youtube.com/
Resolving youtube.com (youtube.com)... 172.217.17.14, 2a00:1450:4003:803::200e
Connecting to youtube.com (youtube.com)|172.217.17.14|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.eroski.es/ [following]
--2025-01-18 18:08:19--  https://www.eroski.es/
Resolving www.eroski.es (www.eroski.es)... 159.60.134.230
Connecting to www.eroski.es (www.eroski.es)|159.60.134.230|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 316756 (309K) [text/html]
Saving to: 'index.html.24'

index.html.24               100%[=========================================>] 309,33K  --.-KB/s    in 0,1s
```

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget twitter.com
--2025-01-18 18:08:41--  http://twitter.com/
Resolving twitter.com (twitter.com)... 104.244.42.1
Connecting to twitter.com (twitter.com)|104.244.42.1|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.eroski.es/ [following]
--2025-01-18 18:08:41--  https://www.eroski.es/
Resolving www.eroski.es (www.eroski.es)... 159.60.134.230
Connecting to www.eroski.es (www.eroski.es)|159.60.134.230|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 316756 (309K) [text/html]
Saving to: 'index.html.7'

index.html.7                100%[=========================================>] 309,33K  --.-KB/s    in 0,07s

2025-01-18 18:08:41 (4,59 MB/s) - 'index.html.7' saved [316756/316756]

almellonesfernandez@almellonesfernandez-us-wlan:~$ wget youtube.com
--2025-01-18 18:08:54--  http://youtube.com/
Resolving youtube.com (youtube.com)... 142.250.184.14, 2a00:1450:4003:811::200e
Connecting to youtube.com (youtube.com)|142.250.184.14|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.eroski.es/ [following]
--2025-01-18 18:08:54--  https://www.eroski.es/
Resolving www.eroski.es (www.eroski.es)... 159.60.134.230
Connecting to www.eroski.es (www.eroski.es)|159.60.134.230|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 316756 (309K) [text/html]
Saving to: 'index.html.8'

index.html.8                100%[=========================================>] 309,33K  --.-KB/s    in 0,08s
```


d) **(0,5 puntos, AND)** Se permitirá todas las restricciones anteriormente (a, b, c) a una determinada hora (a elegir por el alumno, que dependerá de cuando se realice el ejercicio) de que denominemos descanso, es decir en ese horario no se aplicará ninguna de las restricciones, pero **sólo** en la red LAN. Por tanto, en wlan en ese mismo rango de horas se debe cortar.

```
  GNU nano 7.2                          almellonesfernandez-squid.conf
logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv %Sh/%<A %>Hs %<st %rm %ru %>a "%

access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato

#client_netmask 255.255.0.0

acl lista_url_prohibidas_aaf url_regex  mercadona bershka
acl lista_Navegadores_prohibidos_aaf browser -i Firefox
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
acl Hora_Allow_All time 18:00-23:59

http_access allow Hora_Allow_All Redlan

http_access deny lista_url_prohibidas_aaf
deny_info https://www.game.es/  lista_url_prohibidas_aaf

http_access deny lista_Navegadores_prohibidos_aaf

http_access deny Lista_Dominios_Prohibidos_aaf
deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf

http_access allow Redlan Hora_Allow_All

http_access allow RedWlan
http_access allow Redlan
```

```
2025/01/18 20:13:52| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/18 20:13:52| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/18 20:13:52| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/18 20:13:52| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka
2025/01/18 20:13:52| Processing: acl lista_Navegadores_prohibidos_aaf browser -i Firefox
2025/01/18 20:13:52| Processing: acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernande
z-domain.txt"
2025/01/18 20:13:52| Processing: acl Hora_Allow_All time 18:00-23:59
2025/01/18 20:13:52| Processing: http_access allow Hora_Allow_All Redlan
2025/01/18 20:13:52| Processing: http_access deny lista_url_prohibidas_aaf
2025/01/18 20:13:52| Processing: deny_info https://www.game.es/  lista_url_prohibidas_aaf
2025/01/18 20:13:52| Processing: http_access deny lista_Navegadores_prohibidos_aaf
2025/01/18 20:13:52| Processing: http_access deny Lista_Dominios_Prohibidos_aaf
2025/01/18 20:13:52| Processing: deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf
2025/01/18 20:13:52| Processing: http_access allow Redlan Hora_Allow_All
2025/01/18 20:13:52| Processing: http_access allow RedWlan
2025/01/18 20:13:52| Processing: http_access allow Redlan
2025/01/18 20:13:52| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 20:13:52| Processing: logfile_rotate 0
2025/01/18 20:13:52| Processing: http_access deny all
2025/01/18 20:13:52| Processing: http_port 3128
2025/01/18 20:13:52| Processing: coredump_dir /var/spool/squid
2025/01/18 20:13:52| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 20:13:52| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 20:13:52| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 20:13:52| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 20:13:52| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 20:13:52| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 20:13:52| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

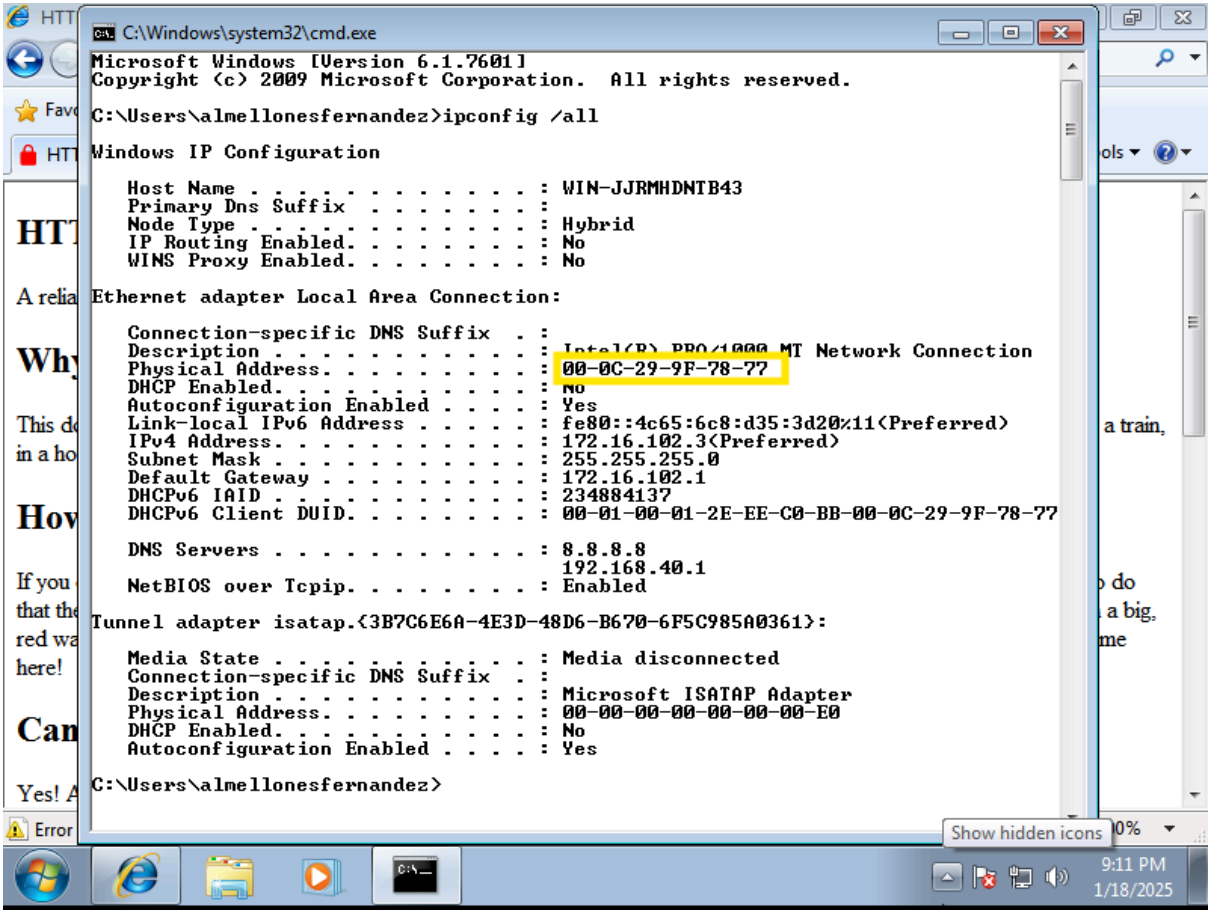


```
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget mercadona.com
--2025-01-18 19:11:01--  http://mercadona.com/
Resolving mercadona.com (mercadona.com)... 195.53.40.253
Connecting to mercadona.com (mercadona.com)|195.53.40.253|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.mercadona.com/ [following]
--2025-01-18 19:11:01--  https://www.mercadona.com/
Resolving www.mercadona.com (www.mercadona.com)... 23.200.66.163, 23.200.66.159, 2a02:26f0:980:a::6010:5697, ...
Connecting to www.mercadona.com (www.mercadona.com)|23.200.66.163|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10745 (10K) [text/html]
Saving to: 'index.html.29'

index.html.29               100%[=========================================>]  10,49K  --.-KB/s    in 0s

2025-01-18 19:11:01 (318 MB/s) - 'index.html.29' saved [10745/10745]

almellonesfernandez@almellonesfernandez-us-intranet:~$
```

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget mercadona.com
--2025-01-18 19:11:22--  http://mercadona.com/
Resolving mercadona.com (mercadona.com)... 195.53.40.253
Connecting to mercadona.com (mercadona.com)|195.53.40.253|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.game.es/ [following]
--2025-01-18 19:11:22--  https://www.game.es/
Resolving www.game.es (www.game.es)... 212.170.159.195
Connecting to www.game.es (www.game.es)|212.170.159.195|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1273851 (1,2M) [text/html]
Saving to: 'index.html.12'

index.html.12               100%[=========================================>]   1,21M  5,64MB/s    in 0,2s

2025-01-18 19:11:23 (5,64 MB/s) - 'index.html.12' saved [1273851/1273851]

almellonesfernandez@almellonesfernandez-us-wlan:~$
```

e) **(0,5 puntos)** Sin embargo para una MAC concreta (la de equipo Windows), siempre se podrá acceder a todo (no hay restricciones).

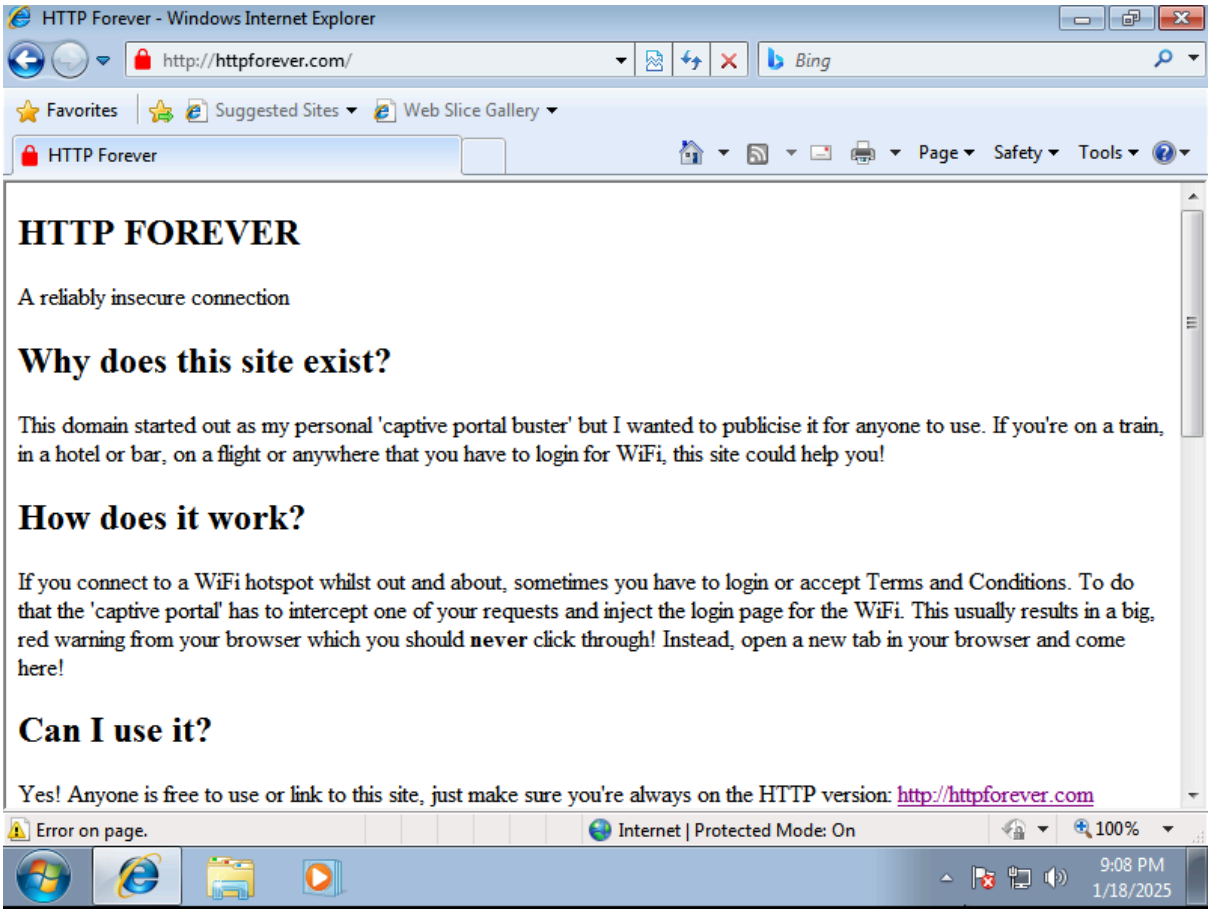
Álvaro Almellones Fernández




```
  GNU nano 7.2                          almellonesfernandez-squid.conf
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato

#client_netmask 255.255.0.0

acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
acl lista_Navegadores_prohibidos_aaf browser -i Firefox
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
acl Hora_Allow_All time 18:00-23:59
acl mac_Windows arp 00:0c:29:9f:78:77

http_access allow mac_Windows

http_access allow Hora_Allow_All Redlan

http_access deny lista_url_prohibidas_aaf
deny_info https://www.game.es/  lista_url_prohibidas_aaf

http_access deny lista_Navegadores_prohibidos_aaf

http_access deny Lista_Dominios_Prohibidos_aaf
deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf

http_access allow Redlan Hora_Allow_All

http_access allow RedWlan
http_access allow Redlan

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

Álvaro Almellones Fernández

```
2025/01/18 21:07:46| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/18 21:07:46| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/18 21:07:46| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
2025/01/18 21:07:46| Processing: acl lista_Navegadores_prohibidos_aaf browser -i Firefox
2025/01/18 21:07:46| Processing: acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernande
z-domain.txt"
2025/01/18 21:07:46| Processing: acl Hora_Allow_All time 18:00-23:59
2025/01/18 21:07:46| Processing: acl mac_Windows arp 00:0c:29:9f:78:77
2025/01/18 21:07:46| Processing: http_access allow mac_Windows
2025/01/18 21:07:46| Processing: http_access allow Hora_Allow_All Redlan
2025/01/18 21:07:46| Processing: http_access deny lista_url_prohibidas_aaf
2025/01/18 21:07:46| Processing: deny_info https://www.game.es/  lista_url_prohibidas_aaf
2025/01/18 21:07:46| Processing: http_access deny lista_Navegadores_prohibidos_aaf
2025/01/18 21:07:46| Processing: http_access deny Lista_Dominios_Prohibidos_aaf
2025/01/18 21:07:46| Processing: deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf
2025/01/18 21:07:46| Processing: http_access allow Redlan Hora_Allow_All
2025/01/18 21:07:46| Processing: http_access allow RedWlan
2025/01/18 21:07:46| Processing: http_access allow Redlan
2025/01/18 21:07:46| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/18 21:07:46| Processing: logfile_rotate 0
2025/01/18 21:07:46| Processing: http_access deny all
2025/01/18 21:07:46| Processing: http_port 3128
2025/01/18 21:07:46| Processing: coredump_dir /var/spool/squid
2025/01/18 21:07:46| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/18 21:07:46| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/18 21:07:46| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 21:07:46| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/18 21:07:46| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/18 21:07:46| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/18 21:07:46| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

para comprobarlo he añadido el http forever a la lista de url prohibidas porque por ser windows 7 el buscador no accede a algunas páginas por estar desactualizado

Álvaro Almellones Fernández

4. (1,5 puntos) OTROS Filtros HTTP_ACCESS y HTTP_REPLY_ACCESS

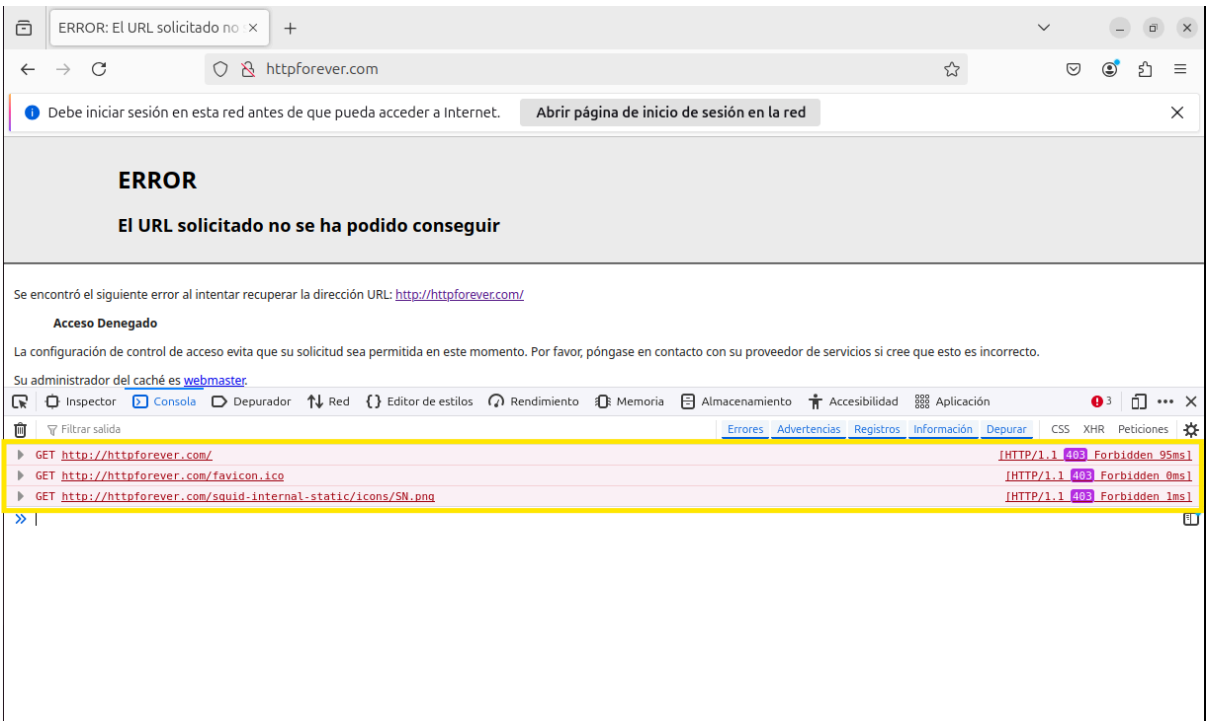
Las siguientes restricciones se pueden demostrar individualmente. Si no se indica nada se deja que el alumno decida el ejemplo de lo que se quiere restringir.

a) **(0,5 puntos)** Restricciones por la directiva method, por ejemplo, que no se permita paquetes mediante método GET. Se debe mostrar evidencias de lo que ocurre mediante FIREBUG o herramientas de desarrollador.

```
  GNU nano 7.2                          almellonesfernandez-squid.conf
#client_netmask 255.255.0.0

acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
acl lista_Navegadores_prohibidos_aaf browser -i Firefox
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
acl Hora_Allow_All time 18:00-19:00
acl mac_Windows arp 00:0c:29:9f:78:77
acl bloqueo_metodo_get method GET

http_access deny bloqueo_metodo_get


#http_access allow mac_Windows

#http_access allow Hora_Allow_All Redlan

#http_access deny lista_url_prohibidas_aaf
#deny_info https://www.game.es/  lista_url_prohibidas_aaf

#http_access deny lista_Navegadores_prohibidos_aaf

#http_access deny Lista_Dominios_Prohibidos_aaf
#deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf


http_access allow RedWlan
http_access allow Redlan

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

```
2025/01/19 11:12:30| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/19 11:12:30| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/19 11:12:30| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/19 11:12:30| Processing: logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv
%Sh/%<A %>Hs %<st %rm %ru %>a "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
2025/01/19 11:12:30| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/19 11:12:30| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/19 11:12:30| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/19 11:12:30| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
2025/01/19 11:12:30| Processing: acl lista_Navegadores_prohibidos_aaf browser -i Firefox
2025/01/19 11:12:30| Processing: acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernande
z-domain.txt"
2025/01/19 11:12:30| Processing: acl Hora_Allow_All time 18:00-19:00
2025/01/19 11:12:30| Processing: acl mac_Windows arp 00:0c:29:9f:78:77
2025/01/19 11:12:30| Processing: acl bloqueo_metodo_get method GET
2025/01/19 11:12:30| Processing: http_access deny bloqueo_metodo_get
2025/01/19 11:12:30| Processing: http_access allow RedWlan
2025/01/19 11:12:30| Processing: http_access allow Redlan
2025/01/19 11:12:30| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/19 11:12:30| Processing: logfile_rotate 0
2025/01/19 11:12:30| Processing: http_access deny all
2025/01/19 11:12:30| Processing: http_port 3128
2025/01/19 11:12:30| Processing: coredump_dir /var/spool/squid
2025/01/19 11:12:30| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/19 11:12:30| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/19 11:12:30| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 11:12:30| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/19 11:12:30| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/19 11:12:30| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 11:12:30| Processing: refresh_pattern .               0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Álvaro Almellones Fernández




```
root@almellonesfernandez-firewall:/var/log/squid# tail -5 accessAlmellonesfernandez-combined.log
172.16.102.4 - - [19/Jan/2025:11:15:47 +0100] "GET http://detectportal.firefox.com/canonical.html HTTP/1.1" 403 42
91 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0" TCP_DENIED:HIER_NONE
172.16.102.4 - - [19/Jan/2025:11:15:50 +0100] "GET http://detectportal.firefox.com/canonical.html HTTP/1.1" 403 42
91 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0" TCP_DENIED:HIER_NONE
172.16.102.4 - - [19/Jan/2025:11:15:53 +0100] "GET http://detectportal.firefox.com/canonical.html HTTP/1.1" 403 42
91 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0" TCP_DENIED:HIER_NONE
172.16.102.4 - - [19/Jan/2025:11:15:56 +0100] "GET http://detectportal.firefox.com/canonical.html HTTP/1.1" 403 42
91 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0" TCP_DENIED:HIER_NONE
172.16.102.4 - - [19/Jan/2025:11:15:59 +0100] "GET http://detectportal.firefox.com/canonical.html HTTP/1.1" 403 42
91 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0" TCP_DENIED:HIER_NONE
root@almellonesfernandez-firewall:/var/log/squid#
```

b) **(0,5 puntos)** Restricciones por la directiva browser.

```
  GNU nano 7.2                                almellonesfernandez-squid.conf
#client_netmask 255.255.0.0

acl lista_url_prohibidas_aaf url_regex  mercadona hershka httpforever
acl lista_Navegadores_prohibidos_aaf browser -i chrome
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
acl Hora_Allow_All time 18:00-19:00
acl mac_Windows arp 00:0c:29:9f:78:77
acl bloqueo_metodo_get method GET

#http_access deny bloqueo_metodo_get


#http_access allow mac_Windows

#http_access allow Hora_Allow_All Redlan

#http_access deny lista_url_prohibidas_aaf
#deny_info https://www.game.es/  lista_url_prohibidas_aaf

http_access deny lista_Navegadores_prohibidos_aaf

#http_access deny Lista_Dominios_Prohibidos_aaf
#deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf


http_access allow RedWlan
http_access allow Redlan

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

Álvaro Almellones Fernández

```
2025/01/19 11:54:48| Processing: acl RedWlan src 192.168.102.0/24 ##Zona transparente
2025/01/19 11:54:48| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/19 11:54:48| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/19 11:54:48| Processing: logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv
%Sh/%<A %>Hs %<st %rm %ru %>a "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
2025/01/19 11:54:48| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/19 11:54:48| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/19 11:54:48| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/19 11:54:48| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
2025/01/19 11:54:48| Processing: acl lista_Navegadores_prohibidos_aaf browser -i chrome
2025/01/19 11:54:48| Processing: acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernande
z-domain.txt"
2025/01/19 11:54:48| Processing: acl Hora_Allow_All time 18:00-19:00
2025/01/19 11:54:48| Processing: acl mac_Windows arp 00:0c:29:9f:78:77
2025/01/19 11:54:48| Processing: acl bloqueo_metodo_get method GET
2025/01/19 11:54:48| Processing: http_access deny lista_Navegadores_prohibidos_aaf
2025/01/19 11:54:48| Processing: http_access allow RedWlan
2025/01/19 11:54:48| Processing: http_access allow Redlan
2025/01/19 11:54:48| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/19 11:54:48| Processing: logfile_rotate 0
2025/01/19 11:54:48| Processing: http_access deny all
2025/01/19 11:54:48| Processing: http_port 3128
2025/01/19 11:54:48| Processing: coredump_dir /var/spool/squid
2025/01/19 11:54:48| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/19 11:54:48| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/19 11:54:48| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 11:54:48| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/19 11:54:48| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/19 11:54:48| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 11:54:48| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```



```
almellonesfernandez@almellonesfernandez-us-intranet:~$ curl -A "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:115.0
) Gecko/20100101 Firefox/115.0" http://example.com/
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helv
etica, Arial, sans-serif;

    }
    div {
```

```
almellonesfernandez@almellonesfernandez-us-intranet:~$ curl -A "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36" http://example.com/
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2021 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
 /*
 * Copyright (C) 1996-2023 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */

/*
 Stylesheet for Squid Error pages
 Adapted from design by Free CSS Templates
 http://www.freecsstemplates.org
 Released for free under a Creative Commons Attribution 2.5 License
*/

/* Page basics */
* {
        font-family: verdana, sans-serif;
}
```

Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ curl -A "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:115.0) Ge
cko/20100101 Firefox/115.0" http://example.com/
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helv
etica, Arial, sans-serif;
```

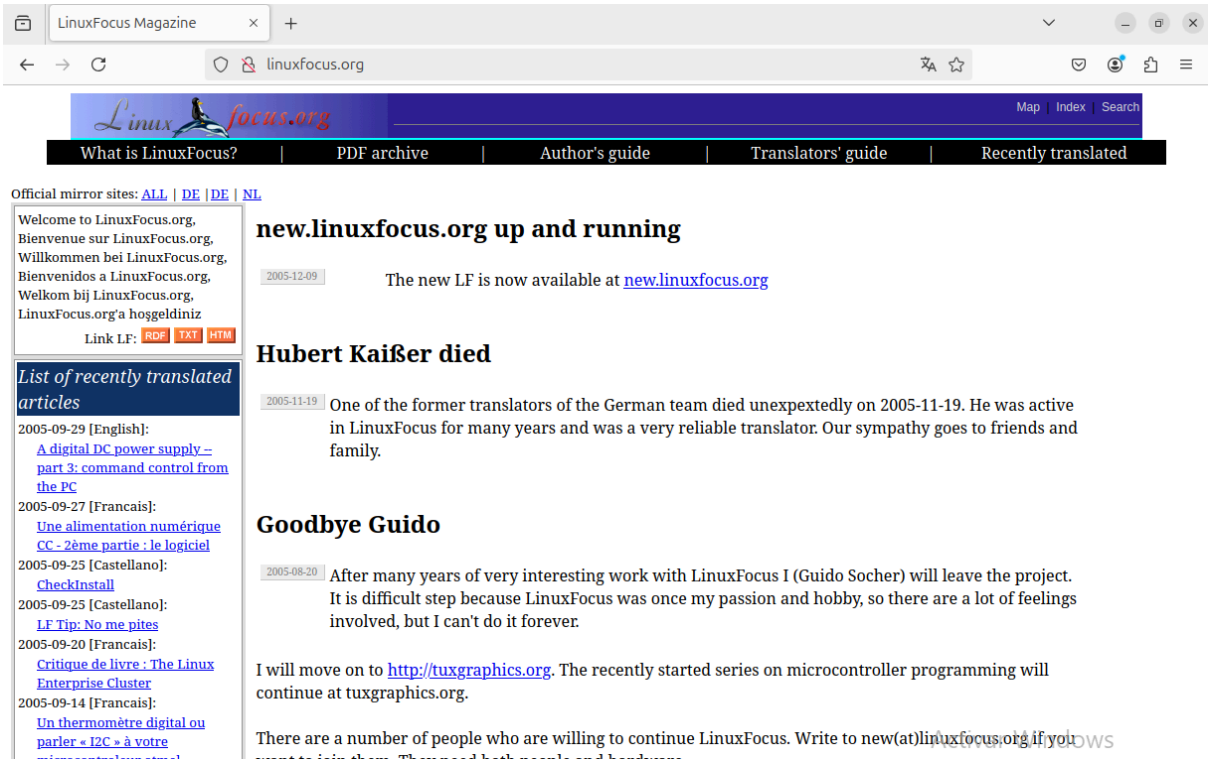
```
almellonesfernandez@almellonesfernandez-us-wlan:~$ curl -A "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36" http://httpforever.com/
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2021 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
 /*
 * Copyright (C) 1996-2023 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */

/*
 Stylesheet for Squid Error pages
 Adapted from design by Free CSS Templates
 http://www.freecsstemplates.org
 Released for free under a Creative Commons Attribution 2.5 License
*/

/* Page basics */
* {
        font-family: verdana, sans-serif;
```

```
root@almellonesfernandez-firewall:/etc/squid/conf.d# tail -4 /var/log/squid/accessAlmellonesfernandez-squid.log
1737283793.622      0 172.16.102.2 TCP_MEM_HIT/200 1637 GET http://example.com/ - HIER_NONE/- text/html
1737283835.725     17 172.16.102.2 TCP_DENIED/403 3983 GET http://example.com/ - HIER_NONE/- text/html
1737283893.035      0 192.168.102.2 TCP_MEM_HIT/200 1638 GET http://example.com/ - HIER_NONE/- text/html
1737283957.546     86 192.168.102.2 TCP_DENIED/403 3996 GET http://httpforever.com/ - HIER_NONE/- text/html
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Estoy usando curl porque estoy teniendo problemas para abrir muchas cosas en el desktop por tener poca ram

c) **(0,5 puntos)** Restricciones por la directiva rep_mime_type.

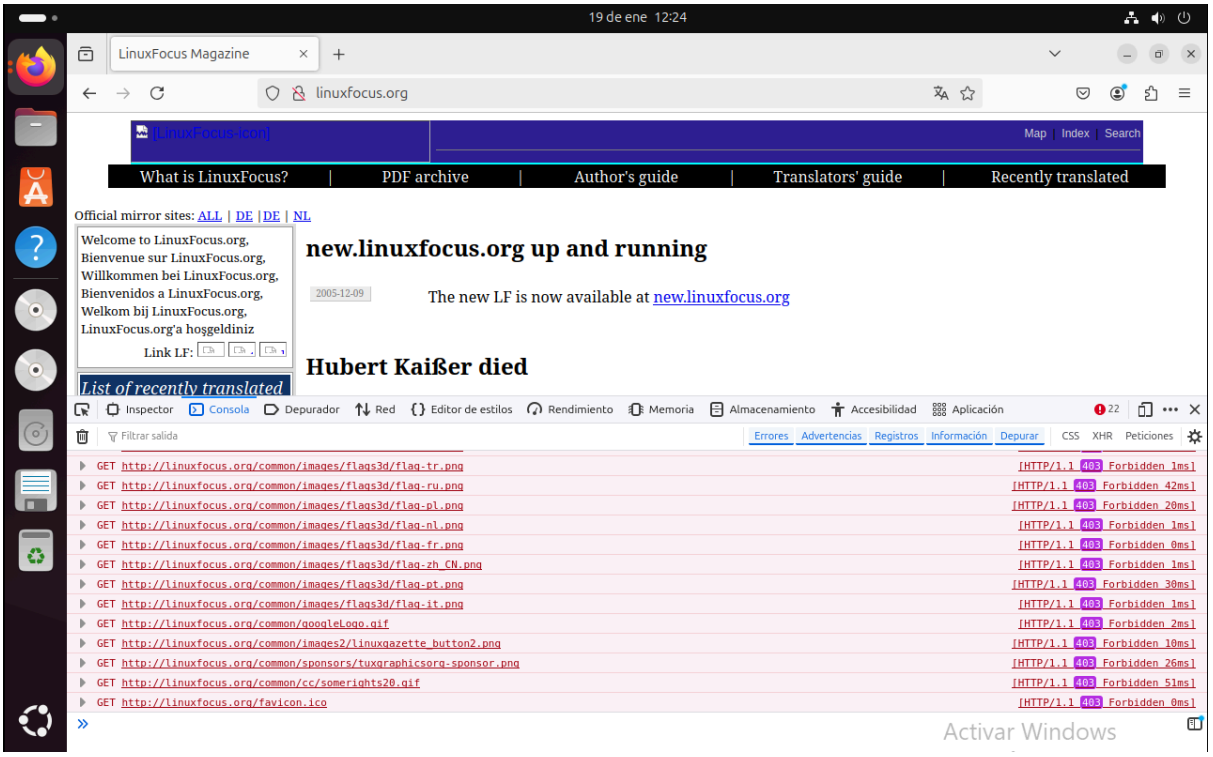
Álvaro Almellones Fernández




```
 GNU nano 7.2                    almellonesfernandez-squid.conf

acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
acl lista_Navegadores_prohibidos_aaf browser -i chrome
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
acl Hora_Allow_All time 18:00-19:00
acl mac_Windows arp 00:0c:29:9f:78:77
acl bloqueo_metodo_get method GET
acl bloqueo_imagenes rep_mime_type -i ^image/

http_reply_access deny bloqueo_imagenes
#http_access deny bloqueo_metodo_get


#http_access allow mac_Windows

#http_access allow Hora_Allow_All Redlan

#http_access deny lista_url_prohibidas_aaf
#deny_info https://www.game.es/  lista_url_prohibidas_aaf

#http_access deny lista_Navegadores_prohibidos_aaf

#http_access deny Lista_Dominios_Prohibidos_aaf
#deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf


http_access allow RedWlan
http_access allow Redlan

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```

Álvaro Almellones Fernández

```
2025/01/19 12:24:57| Processing: acl Redlan src 172.16.102.0/24 ##Zona transparente
2025/01/19 12:24:57| Processing: visible_hostname proxyAlmellonesfernandez.es
2025/01/19 12:24:57| Processing: logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv
%Sh/%<A %>Hs %<st %rm %ru %>a "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh %tr %tg %{Header}>h
2025/01/19 12:24:57| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
2025/01/19 12:24:57| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
2025/01/19 12:24:57| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/19 12:24:57| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
2025/01/19 12:24:57| Processing: acl lista_Navegadores_prohibidos_aaf browser -i chrome
2025/01/19 12:24:57| Processing: acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernande
z-domain.txt"
2025/01/19 12:24:57| Processing: acl Hora_Allow_All time 18:00-19:00
2025/01/19 12:24:57| Processing: acl mac_Windows arp 00:0c:29:9f:78:77
2025/01/19 12:24:57| Processing: acl bloqueo_metodo_get method GET
2025/01/19 12:24:57| Processing: acl bloqueo_imagenes rep_mime_type -i ^image/
2025/01/19 12:24:57| Processing: http_reply_access deny bloqueo_imagenes
2025/01/19 12:24:57| Processing: http_access allow RedWlan
2025/01/19 12:24:57| Processing: http_access allow Redlan
2025/01/19 12:24:57| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/19 12:24:57| Processing: logfile_rotate 0
2025/01/19 12:24:57| Processing: http_access deny all
2025/01/19 12:24:57| Processing: http_port 3128
2025/01/19 12:24:57| Processing: coredump_dir /var/spool/squid
2025/01/19 12:24:57| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/19 12:24:57| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/19 12:24:57| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 12:24:57| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/19 12:24:57| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/19 12:24:57| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 12:24:57| Processing: refresh_pattern .              0       20%     4320
```

Álvaro Almellones Fernández

5. (1,5 puntos) PROXY EN MODO TRANSPARENTE.

a) **(0,75 puntos)** Establezca ahora que en la zona LAN el proxy web funciona en modo no transparente y muestres las evidencias que crea necesario. No se olvide de realizar de que funciona correctamente la actualización en Ubuntu (apt-get).

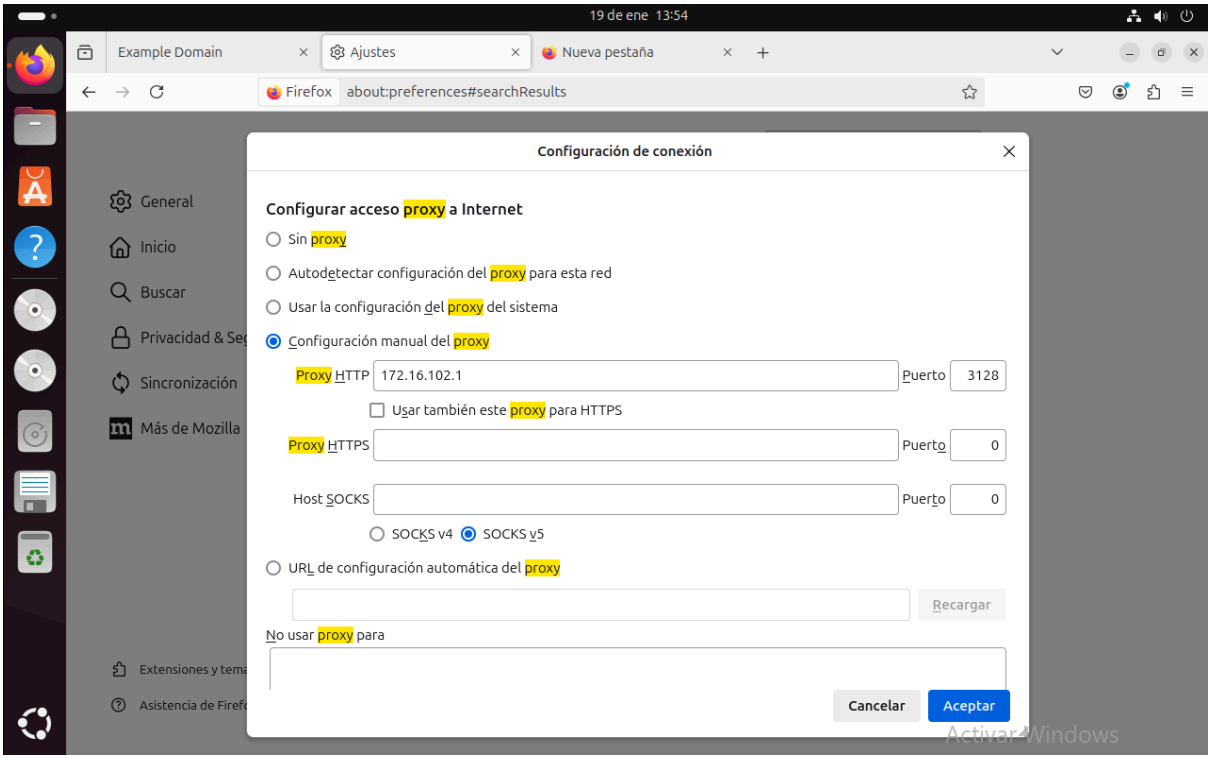
```
  GNU nano 7.2                          almellonesfernandez-squid.conf
http_port 172.16.102.1:3128  #Zona LAN no transparente
http_port 192.168.102.1:3129 intercept #Zona Wlan transparente

acl RedWlan src 192.168.102.0/24 ##Zona transparente
acl Redlan src 172.16.102.0/24 ##Zona transparente

#deny_info https://www.naughtydog.com/  all

visible_hostname proxyAlmellonesfernandez.es

logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv %Sh/%<A %>Hs %<st %rm %ru %>a "%>

access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato

#client_netmask 255.255.0.0

acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
acl lista_Navegadores_prohibidos_aaf browser -i chrome
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
acl Hora_Allow_All time 18:00-19:00
acl mac_Windows arp 00:0c:29:9f:78:77
acl bloqueo_metodo_get method GET
acl bloqueo_imagenes rep_mime_type -i ^image/

#http_reply_access deny bloqueo_imagenes
#http_access deny bloqueo_metodo_get
                                [ Read 45 lines ]
^G Help          ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit          ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo
```


Quito el intercept del http_port de Lan

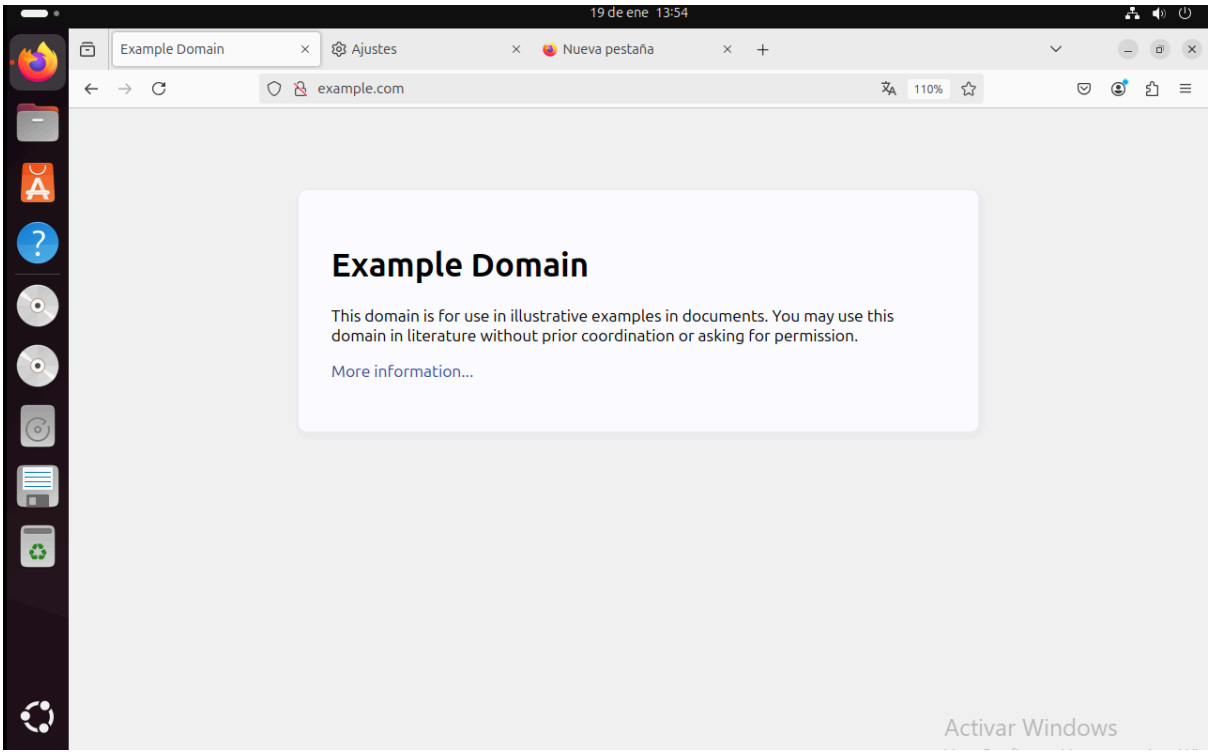
```
root@almellonesfernandez-firewall:/etc/squid/conf.d# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 44 packets, 2434 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir ports 31
29
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2
:443
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP *
/ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 17 packets, 1120 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ a WAN
 */
    3   216 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN a WAN
 */
    0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN a WA
N */
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Solo dejo el prerouting de wlan

Álvaro Almellones Fernández



Configuro el proxy en el navegador



Álvaro Almellones Fernández

```
root@almellonesfernandez-us-intranet:/etc/apt/apt.conf.d# cat 95proxies
Acquire::http::Proxy "http://172.16.102.1:3128";
root@almellonesfernandez-us-intranet:/etc/apt/apt.conf.d# apt  update
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Des:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Des:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Des:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [586 kB]
Des:6 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [114 kB]
Des:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7.252 B]
Des:8 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [572 kB]
Des:9 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [110 kB]
Des:10 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Des:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [800 kB]
Des:12 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [171 kB]
Des:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52,0 kB]
Des:14 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [12,4 kB]
```

b) **(0,75 puntos)** Configure proxy web para que solicite usuario/contraseña mediante htpasswd.

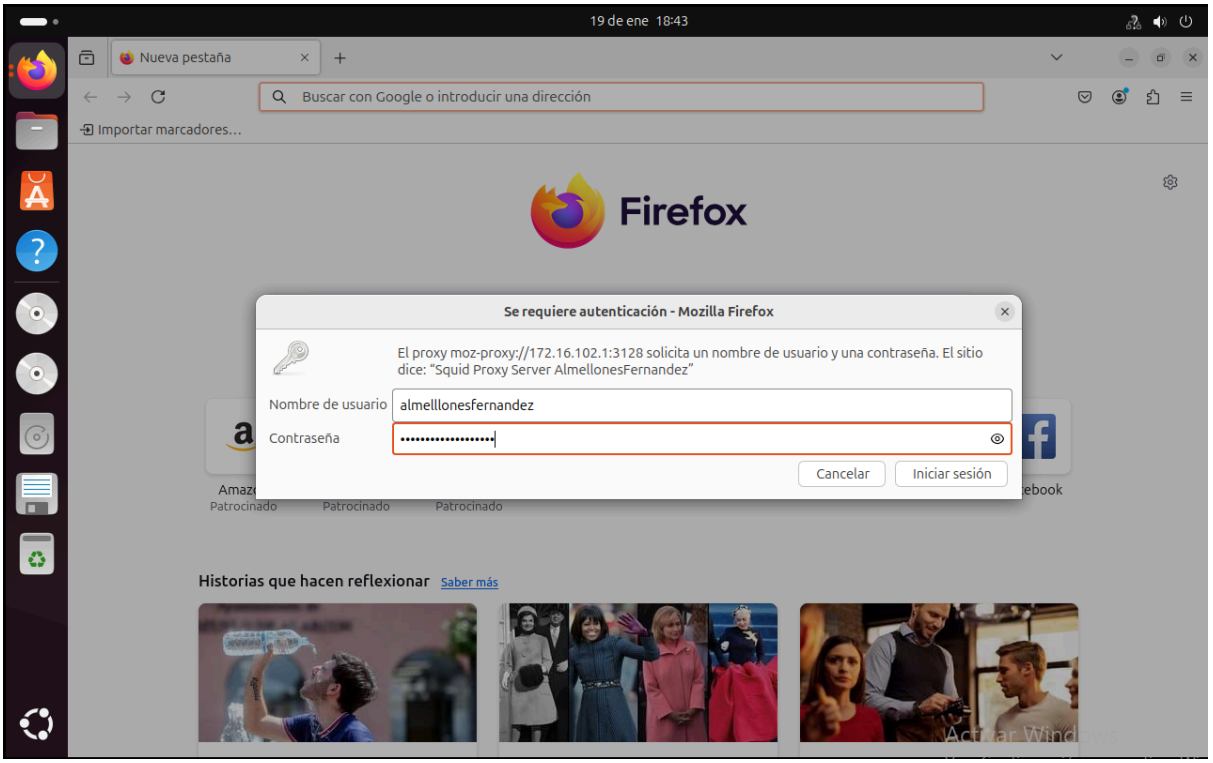
```
  GNU nano 7.2                          almellonesfernandez-squid.conf
visible_hostname proxyAlmellonesfernandez.es

logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv %Sh/%<A %>Hs %<st %rm %ru %>a "%>

access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato

#client_netmask 255.255.0.0

#auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/passwd  #Para usar usuarios de la máquina
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/hpasswd # Para usar usuarios en fichero de tex>
auth_param basic realm Squid Proxy Server AlmellonesFernandez
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off

acl authenticated proxy_auth REQUIRED
http_access allow authenticated

acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
acl lista_Navegadores_prohibidos_aaf browser -i chrome
acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernandez-domain.txt"
acl Hora_Allow_All time 18:00-19:00
acl mac_Windows arp 00:0c:29:9f:78:77
acl bloqueo_metodo_get method GET
acl bloqueo_imagenes rep_mime_type -i ^image/

#http_reply_access deny bloqueo_imagenes

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```



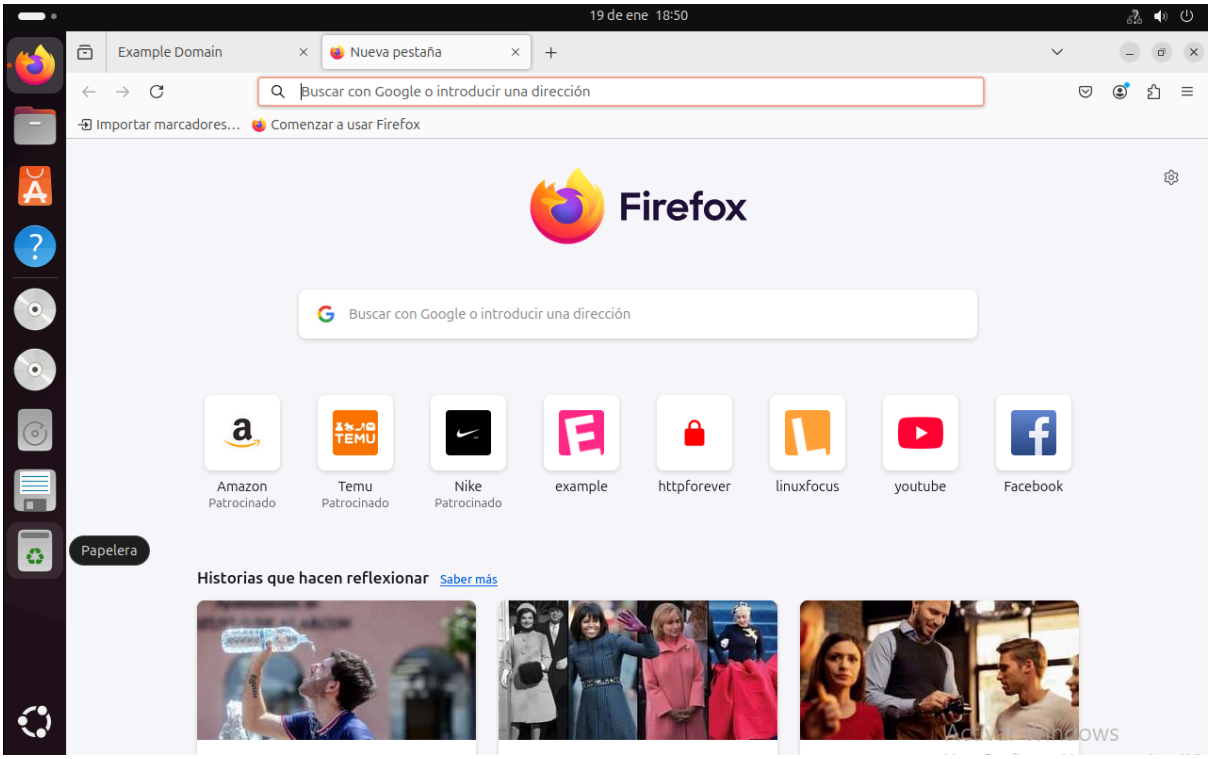
```
root@almellonesfernandez-firewall:/etc/squid/conf.d# htpasswd -c /etc/squid/hpasswd  almellonesfernandez
New password:
Re-type new password:
Adding password for user almellonesfernandez
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Álvaro Almellones Fernández

```
2025/01/19 18:47:33| Processing: access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log alme
llonesfernandez_formato
2025/01/19 18:47:33| Processing: auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/hpasswd # Para
 usar usuarios en fichero de texto
2025/01/19 18:47:33| Processing: auth_param basic realm Squid Proxy Server AlmellonesFernandez
2025/01/19 18:47:33| Processing: auth_param basic credentialsttl 2 hours
2025/01/19 18:47:33| Processing: auth_param basic casesensitive off
2025/01/19 18:47:33| Processing: acl authenticated proxy_auth REQUIRED
2025/01/19 18:47:33| Processing: http_access allow authenticated
2025/01/19 18:47:33| Processing: acl lista_url_prohibidas_aaf url_regex  mercadona bershka httpforever
2025/01/19 18:47:33| Processing: acl lista_Navegadores_prohibidos_aaf browser -i chrome
2025/01/19 18:47:33| Processing: acl Lista_Dominios_Prohibidos_aaf dstdomain "/etc/squid/conf.d/almellonesfernande
z-domain.txt"
2025/01/19 18:47:33| Processing: acl Hora_Allow_All time 18:00-19:00
2025/01/19 18:47:33| Processing: acl mac_Windows arp 00:0c:29:9f:78:77
2025/01/19 18:47:33| Processing: acl bloqueo_metodo_get method GET
2025/01/19 18:47:33| Processing: acl bloqueo_imagenes rep_mime_type -i ^image/
2025/01/19 18:47:33| Processing: http_access allow RedWlan
2025/01/19 18:47:33| Processing: http_access allow Redlan
2025/01/19 18:47:33| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/01/19 18:47:33| Processing: logfile_rotate 0
2025/01/19 18:47:33| Processing: http_access deny all
2025/01/19 18:47:33| Processing: http_port 3128
2025/01/19 18:47:33| Processing: coredump_dir /var/spool/squid
2025/01/19 18:47:33| Processing: refresh_pattern ^ftp:          1440    20%     10080
2025/01/19 18:47:33| Processing: refresh_pattern -i (/cgi-bin/|\?) 0    0%      0
2025/01/19 18:47:33| Processing: refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 18:47:33| Processing: refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
2025/01/19 18:47:33| Processing: refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
2025/01/19 18:47:33| Processing: refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
2025/01/19 18:47:33| Processing: refresh_pattern .              0       20%     4320
root@almellonesfernandez-firewall:/etc/squid/conf.d#
```

Álvaro Almellones Fernández



*** Una vez terminado este apartado número 5 reestablezca para que quede en modo no transparente.