

## EJERCICIO 1

Crear un archivo de configuración para denegar el acceso a todos los equipos a la dirección `www.google.es`

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl no_permitido1 dstdomain www.google.es
http_access deny no_permitido1
```

## EJERCICIO 2

Crear un archivo de configuración que deniegue el acceso a las direcciones `www.google.es` y `www.alejandrox.com`

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl no_permitido1 dstdomain www.google.es www.alejandrox.com
http_access deny no_permitido1
```

En este caso el fichero de configuración es similar al caso anterior. Tan sólo hay que poner `www.alejandrox.com` después de `www.google.es` en la `acl no_permitido1`.

## EJERCICIO 3

Crea en tu carpeta personal un archivo llamado `no_permitidos` que contenga las direcciones de los tres siguientes dominios:

- `www.google.es`
- `http://es.yahoo.com/`
- `http://es.msn.com/`

Para crear este archivo puedes abrir el terminal (Aplicaciones/Accesorios/Terminal) y escribir:

- `gedit /home/nombre_de_usuario/no_permitidos.`

A continuación crea un archivo de configuración `squid.conf` que deniegue las conexiones a las direcciones que se encuentran en el archivo `no_permitidos`.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl no_permitido1 url_regex "/home/alex/no_permitidos"
http_access deny no_permitido1
```

## EJERCICIO 4

Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Crear un archivo de configuración squid.conf que permita el acceso a Squid a todos los ordenadores de la red y no lo permita a los restantes.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl totalared src 192.168.1.0/255.255.255.0
http_access allow totalared
http_access deny all
```

## EJERCICIO 5

Se dispone de una red de área local con dirección 192.168.1.0 y máscara 255.255.255.0. Se desea permitir el acceso a Squid a los ordenadores con las IP que están comprendidas en el rango 192.168.1.1 y 192.168.1.10 (ambas incluidas). Crea en tu directorio personal un fichero llamado ip\_permitidas que tenga estas direcciones (cada dirección en una línea diferente). A continuación indica que fichero de configuración para Squid crearías para permitir el acceso a Squid a todas estas direcciones y denegar el acceso a las restantes.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl red_local src "home/nombre_usuario/ip_permitidas"
http_access allow red_local
http_access deny all
```

## EJERCICIO 6

Deniega las conexiones a todos los equipos en horario de 18:00 a 21:00 horas.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl horario time 18:00-21:00
http_access deny horario
```

## EJERCICIO 7

Deniega las conexiones a todos los equipos en horario de 18:00 a 21:00 horas, pero sólo los lunes, martes y miércoles.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl horario time MTW 18:00-21:00
http_access deny horario
```

## EJERCICIO 8

Deniega el acceso a Squid al equipo con IP 192.168.1.5. Permite el resto de accesos a Squid.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl equipo5 src 192.168.1.5
http_access deny equipo5
```

## EJERCICIO 9

Deniega el acceso a Squid al equipo con IP 192.168.1.5 en horario de 18:00 a 21:00 horas. Permite el resto de accesos a Squid.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl equipo5 src 192.168.1.5
acl horario 18:00-21:00
http_access deny equipo5 horario
```

## EJERCICIO 10

Deniega el acceso a Squid al equipo con IP 192.168.1.5 en horario de 18:00 a 21:00 horas. Para el resto de equipos permitir el acceso sólo en horario de 10:00 a 14:00 horas. Se supone que los equipos pertenecen a la red 192.168.1.0 con máscara 255.255.255.0.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl red_local src 192.168.1.0/255.255.255.0.
acl equipo5 src 192.168.1.5
acl horario1 18:00-21:00
```

```
acl horario2 10:00-14:00
http_access deny equipo5 horario
http_access allow red_local horario
http_access deny all
```

## EJERCICIO 11

En el archivo `/etc/squid/permitidos` se tiene una lista de todas las direcciones IP de la red local. El equipo10 tiene la dirección IP 192.168.1.10. Se permite el acceso a Internet al equipo10 de lunes a miércoles de 9:00 a 14:00 horas. También se permite el acceso a los equipos de la red local de lunes a miércoles. Se prohíbe el acceso en el resto de casos.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl redlocal src "/etc/squid/permitidos"
acl equipo10 src 192.168.1.10
acl horario time MTWHF 9:00-14:00
acl horario2 time MTW
http_access allow equipo10 horario
http_access allow redlocal horario2
http_access deny all
```

## EJERCICIO 12

Restringe el acceso a todo el contenido con extensión `.mp3` a los ordenadores del aula.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl redlocal src 192.168.1.0/255.255.255.0
acl musica urlpath_regex \.mp3
http_access allow redlocal !musica
http_access deny all
```

## EJERCICIO 13

Restringe el acceso a todo el contenido con extensión `.mp3` a los ordenadores del aula en horario de 9:00 a 14:00 horas.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl redlocal src 192.168.1.0/255.255.255.0
acl musica urlpath_regex \.mp3
acl horario 9:00-14:00
http_access allow redlocal !musica
```

## EJERCICIO 14

A los equipos comprendidos en el rango de direcciones IP 192.168.1.1-192.168.1.5 se les quiere denegar el acceso a las páginas web que están en el archivo /etc/squid/sitios\_permitidos los fines de semana. Se supone que las direcciones de ese rango están en el archivo /etc/squid/permitidos. El resto de equipos de la red tienen acceso a todas las páginas pero no los fines de semana, en el que no tienen acceso a ninguna página.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl redlocal src 192.168.1.0/255.255.255.0
acl ip_permitidas src "/etc/squid/permitidos"
#La letra 'A' se corresponde con el sábado
acl horario time AS
acl sitios_permitidos url_regex "/etc/squid/permitidos"
http_access deny permitidas sitios_permitidos horario
```

## EJEMPLO-DEPARTAMENTO DE INFORMÁTICA

```
visible_hostname localhost
http_port 8080 transparent

icp_port 0
acl QUERY urlpath_regex cgi-bin \?
cache_mem 64 MB
maximum_object_size 128 MB
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
cache_dir ufs /var/spool/squid 4096 16 256
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log

refresh_pattern ^ftp:      1440 20% 10080
refresh_pattern ^gopher:  1440 0% 1440
refresh_pattern .         0 20% 4320

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl Puertos_SSL port 443 465 563 587 873 995 9666 10000
acl aula1 src 192.168.1.0/24
acl aula2 src 192.168.2.0/24
acl aula6 src 192.168.6.0/24
acl informaticabosco url_regex "/etc/squid/permitidos"
acl deniedsites url_regex -i "/etc/squid/prohibido" # gopher
acl msnmessenger req_mime_type -i ^application/x-msn-messenger$
acl macs arp "/etc/squid/mac_permitidas"
```

```
acl sitioshttps url_regex "/etc/squid/httpsPermitidos"  
acl mysql port 3306  
acl ALL_PUERTOS port 0-65535  
acl TRANSPARENTE_SSL_3128 port 3128
```

```
always_direct allow all
```

```
http_access allow macs  
http_access allow informaticabosco  
http_access allow Mysql_Carmen  
http_access deny deniedsites  
http_access deny msnmessenger  
http_access allow aula1  
http_access allow aula2  
http_access allow aula6  
http_access allow manager localhost  
http_access allow all CONNECT ALL_PUERTOS
```

```
cache_effective_user proxy  
cache_effective_group root
```

```
error_directory /usr/share/squid/errors/es  
coredump_dir /var/spool/squid
```

```
offline_mode on  
ie_refresh on  
cache deny aula2  
icp_access allow all  
http_reply_access allow all
```