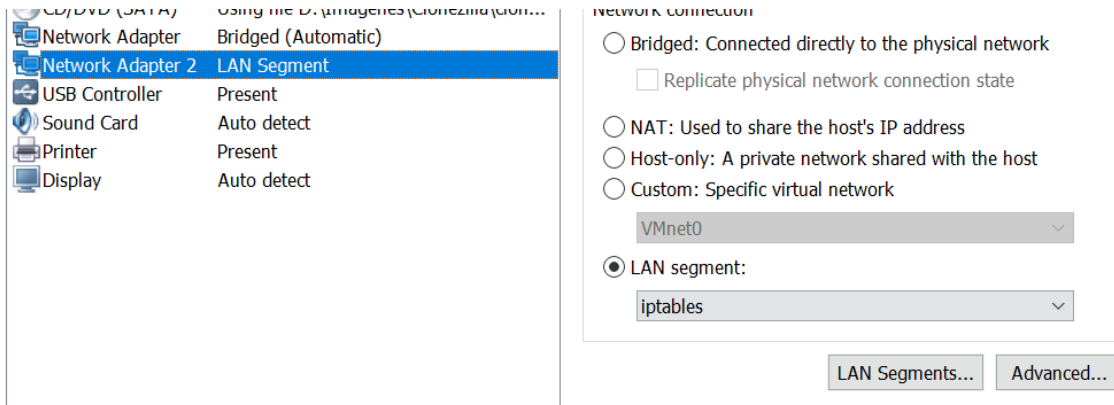


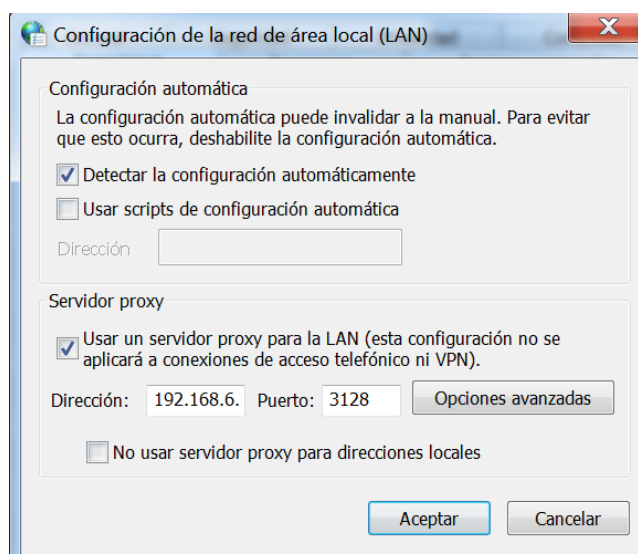
## Práctica – Proxy Squid - Linux

Configuración Básica de Squid:

1. Arranca una máquina Linux con dos adaptadores de red.



2. Uno debe ser adaptador Puente (network adapter 1) y el otro será una adaptador en el segmento LAN (network adapter 2), que habrá que configurar previamente (le daremos la IP 192.168.6.0 al segmento).
3. Arranca una máquina Windows conectada al segmento Lan.
4. Configura la dirección IP del segmento Lan.
5. Instala squid en Linux.
6. Modifica la configuración del Proxy en Windows para comprobar que el Squid funciona bien.
  - a. El puerto del proxy es 3128
  - b. La IP del servidor Proxy es la ip de la máquina Linux. **Ojo: El servidor Linux tiene 2 ips.**



## ERROR

### El URL solicitado no se ha podido conseguir

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://elpais.es/>

#### Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, consulte con su administrador del caché es [webmaster](#).

Generado Mon, 06 Feb 2017 10:22:26 GMT por ubuntu (squid/3.5.12)

Haz una copia de seguridad del fichero /etc/squid/squid.conf como squid.conf.bak usando el comando cp.

7. Añade las siguientes acl's y reglas en el fichero squid.conf:

```
#  
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS  
#  
  
#Declaraciones  
acl MIRED src 192.168.6.0/24  
  
#Reglas  
http_access allow MIRED
```

8. Comprueba que la máquina Windows VM puede conectar ahora a Internet. Si funciona, la configuración básica de squid está superada!!

---

Parametros a configurar:

1. El tamaño máximo de memoria del servidor que el squid utilizará como caché será 100 MB. (**cache\_mem**)
2. El tamaño del disco duro y la jerarquía de directorios será: caché de 90 Mb en el directorio por defecto, con 16 subdirectorios y 256 directorios por subdirectorio. (**cache\_dir ufs /var/spool/squid 90 16 256**)
3. Los mensajes de rechazar páginas por nuestras reglas ACL deben estar personalizados:  

```
# Send error pages in the clients preferred language  
error_directory /usr/share/squid/errors/Spanish
```
4. Para reiniciar el squid puedes usar:

```
sudo squid -k reconfigure
```

### **Configuración de acceso:**

Como ya sabemos, para crear una ACL para un sólo equipo, escribimos la siguiente regla:

```
acl <NOMBRE_ACL> src <IP_DEL_EQUIPO>
```

Ejemplo:


```
acl PC1 src 192.168.1.117
```

Por otro lado, si queremos crear un grupo de equipos, Squid nos permite crear un fichero con una lista de direcciones IP. Este fichero debe estar en la carpeta "/etc/squid/":

```
acl <NOMBRE_GRUPO_ACL> src "/etc/squid/<NOMBRE_ARCHIVO>"
```

Ejemplo:

```
acl PORTATILES src "/etc/squid/lista_portatiles.txt"
```



```
1 192.168.1.117
2 192.168.1.120
3 192.168.1.121
```

Una vez creado el ACL, puedes controlar el acceso a Internet de los equipos configurados usando:

```
http_access <allow/deny> <NOMBRE_ACL>
```

### **Configuración de acceso en el tiempo:**

Puedes controlar el acceso en periodos de tiempo, declarándolos primero como ACL:

```
acl <NOMBRE> time <DIAS> hh:mm-hh:mm
```

Days:

M – Monday

T – Tuesday

W – Wednesday

H – Thursday

F – Friday

A – Saturday

S – Sunday

Ejemplo:

**acl LABORAL\_MAÑANA time MTWHF 08:00-14:00**

Esta ACL nose puede poner en marcha sólo, sino que se tendrá que aplicar a un equipo o grupo de equipos:

**http\_access <allow/deny> LABORAL\_MAÑANA PC1**

Ejemplo:

```
641 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
642
643 #MIS REGLAS
644 #DECLARACIONES
645 acl TODOS src 192.168.1.0/24
646 acl PC1 src 192.168.1.117
647 acl LABORAL_MAÑANA time 08:00-14:00
648
649 #REGLAS
650 http_access deny LABORAL_MAÑANA PC1
651 http_access allow TODOS
652
```

### Configuración de acceso a páginas

Podemos crear un fichero con diferentes webs para incluirlas en una ACL dentro del fichero de configuración de squid (/etc/squid/squid.conf):

**acl <NOMBRE\_acl> url\_regex "/etc/squid/<nombre\_archivo>"**

Ejemplo:

**acl WEBS url\_regex "/etc/squid/webs"**

Esta ACL se usará con una http\_access:

**http\_access <allow/deny> WEBS PC1**

Ejemplo:

```
641 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
642
643 #MIS REGLAS
644 #DECLARACIONES
645 acl TODOS src 192.168.1.0/24
646 acl PC1 src 192.168.1.117
647 acl LABORAL_MAÑANA time 08:00-14:00
648 acl WEBS url_regex "/etc/squid3/webs"
649 |
650 #REGLAS
651 http_access deny WEBS PC1
652 http_access allow LABORAL_MAÑANA PC1
653 http_access allow TODOS
654
```

**Tareas:**

1. Crea un fichero con un grupo de ordenadores a los cuales no se les permita el acceso a Internet.
2. El resto de ordenadores podrá conectarse a Internet.
3. Comprueba que los puntos 1 y 2 funcionan. Puedes ir cambiando la IP de la máquina de Windows para hacer las pruebas. No olvides tomar capturas de pantalla.
4. Crea otro grupo de ordenadores a los cuales se les prohíba el acceso a Internet de 3 a 9 de la tarde los Lunes, miércoles y viernes.
5. Prueba con la máquina de Windows cambiando de nuevo la IP que este punto también funciona.
6. Crea otro grupo de equipos a los cuales no se les permita conectar con sitios web cuya URL contengan las palabras “sex” y “porn”.
7. Vuelve a comprobar que este punto funciona también.

**Crea el informe correspondiente a la práctica, y además entrega también tu fichero de configuración squid.conf**