Cómo Instalar y configurar un servidor completo guifi.net

¡¡¡¡ Documento en construcción !!!!

Servicios a instalar

Sistema base Debian o Ubuntu

Debian

La versión que vamos a instalar es la debian estable, a fecha 7/3/2010 es la 5.0.4, cuyo nombre en código es *lenny*. Se pueden encontrar instrucciones de instalación en http://www.debian.org/releases/stable/installmanual, para equipos actuales de 64 bits, seleccionar la opción AMD64.

Ubuntu

Utilizando el liveCD ...

Particionado del disco

Durante la instalación pedirá que indiquemos las particiones a realizar, el particionado depende de las necesidades y del equipo del que se disponga, como ejemplo en el servidor de `castello.guifi.net` con 160GBytes se ha realizado el siguiente particionado:

```
mperez@castello:~$ df -k
S.ficheros         Bloques de 1K   Usado    Dispon Uso% Montado en
/dev/sda1             28834716    677244  26692748   3% /
tmpfs                  1037436         0   1037436   0%
/lib/init/rw
udev                     10240       712      9528   7% /dev
tmpfs                  1037436         0   1037436   0% /dev/shm
/dev/sda6             57677500    184268  54563380   1% /copias
/dev/sda8             50980676   2537140  45853860   6% /home
/dev/sda5              3842376     73256   3573932   3% /tmp
/dev/sda2              4806936    703012   3859736  16% /var
/dev/sda7              4806904    351428   4211292   8%
/var/cache/apt
```

Actualizar el sistema

Una vez instalado conviene actualizar los paquetes utilizando el Gestor de Actualizaciones del entorno gráfico o desde una consola mediante las órdenes:

```
apt-get update
apt-get upgrade
```

Instalar el servidor ssh

Para poder conectarse por ssh remotamente hay que instalar el servidor

`apt-get install openssh-server`

Activar el forwarding permanente

Si el servidor tiene que actuar como router hay que activar el forwarding.

Editar el fichero `/etc/sysctl.conf` y poner:

`net.ipv4.ip_forward = 1`

normalmente esta linea estará comentada, hay que descomentarla.

Esto hace que el forwarding se active al arrancar, si sólo queremos hacer una prueba hay que hacer:

`echo "1" > /proc/sys/net/ipv4/ip_forward`

Cortafuegos

Instalar el siguiente script (adaptandolo si es necesario) en `/etc/network/if-up.d` con el nombre `firewall`

```
#!/bin/sh
IPTABLES=/sbin/iptables

  # 1) Definir la norma de cada cadena básica
  $IPTABLES -P INPUT ACCEPT
  $IPTABLES -P FORWARD ACCEPT
  $IPTABLES -P OUTPUT ACCEPT

  $IPTABLES -F

  #$IPTABLES -t nat -A POSTROUTING -o eth0 -j SNAT --to
10.228.130.162
  $IPTABLES -t nat -A POSTROUTING -s 192.168.1.0/24 -d 0.0.0.0/0 -
j SNAT --to 10.228.152.37

  # 2) Aceptar paquetes en estado establecido y relacionado
  $IPTABLES -A INPUT -i lo -j ACCEPT
  $IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT

  $IPTABLES -I INPUT -p icmp -j ACCEPT

  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 22 -j
ACCEPT
  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 25 -j
ACCEPT
  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 53 -j
ACCEPT
  $IPTABLES -A INPUT -m state --state NEW -p udp --dport 53 -j
ACCEPT
```

```
  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 80 -j
ACCEPT

  # Para el SNMP
  $IPTABLES -A INPUT -m state --state NEW -p udp --dport 161  -j
ACCEPT

  # Para quagga
  $IPTABLES  -A INPUT -p 89 -j ACCEPT

  $IPTABLES -A INPUT -j DROP
```

y hacerlo ejecutable

```
chmod 755 firewall
```

Para parar el firewall hay que ejecutar:

```
iptables -F
iptables -F -t nat
```

Webmin

Descargar el fichero http://sourceforge.net/projects/webadmin/files/webmin/1.510/webmin_1.510_all.deb/download o la versión que corresponda (mirar en http://webmin.com/)

```
dpkg --install webmin_1.510_all.deb
```

Si existen fallos de dependencias, ejecutar:

```
apt-get -f install
```

Ahora ya se puede acceder a webmin con un navegador en la dirección https://localhost:10000/ o por internet o guifi.net en la dirección del servidor.

Se puede configurar el idioma de la interfaz de webmin en `Webmin –> Cambio de Idioma y Tema`

También se puede limitar el acceso en `Webmin –> Configuración de Webmin –> Control de Acceso a IP`

Si se ha puesto en marcha el cortafuegos y se quiere dar acceso desde fuera, hay que abrir el puerto 10000:

```
$IPTABLES -A INPUT -m state --state NEW -p tcp --dport 10000 -j
ACCEPT
```

Videotutorial para instalar webmin en ubuntu 11.4

Servidor web Apache

```
root@ftp2000-desktop:~# apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalaron de forma automática los siguientes paquetes y ya no
son necesarios.
```

```
  linux-headers-2.6.31-14 linux-headers-2.6.31-14-generic
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes extras:
  apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common
libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Paquetes sugeridos:
  apache2-doc apache2-suexec apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-mpm-worker apache2-utils apache2.2-bin
apache2.2-common libapr1 libaprutil1 libaprutil1-dbd-sqlite3
libaprutil1-ldap
0 actualizados, 9 se instalarán, 0 para eliminar y 0 no
actualizados.
Necesito descargar 2013kB de archivos.
Se utilizarán 6738kB de espacio de disco adicional después de esta
operación.
¿Desea continuar [S/n]?
Des:1 http://es.archive.ubuntu.com karmic/main libapr1 1.3.8-1
[116kB]
Des:2 http://es.archive.ubuntu.com karmic/main libaprutil1
1.3.9+dfsg-1ubuntu1 [91,1kB]

Des:3 http://es.archive.ubuntu.com karmic/main libaprutil1-dbd-
sqlite3 1.3.9+dfsg-1ubuntu1 [27,5kB]
Des:4 http://es.archive.ubuntu.com karmic/main libaprutil1-ldap
1.3.9+dfsg-1ubuntu1 [25,2kB]
Des:5 http://es.archive.ubuntu.com karmic-updates/main apache2.2-
bin 2.2.12-1ubuntu2.2 [1309kB]
Des:6 http://es.archive.ubuntu.com karmic-updates/main apache2-
utils 2.2.12-1ubuntu2.2 [155kB]
Des:7 http://es.archive.ubuntu.com karmic-updates/main apache2.2-
common 2.2.12-1ubuntu2.2 [285kB]
Des:8 http://es.archive.ubuntu.com karmic-updates/main apache2-
mpm-worker 2.2.12-1ubuntu2.2 [2314B]
Des:9 http://es.archive.ubuntu.com karmic-updates/main apache2
2.2.12-1ubuntu2.2 [1426B]
Descargados 2013kB en 18s (111kB/s)
Seleccionando el paquete libapr1 previamente no seleccionado.
(Leyendo la base de datos ...  00%
152401 ficheros y directorios instalados actualmente.)
Desempaquetando libapr1 (de .../libapr1_1.3.8-1_i386.deb) ...
Seleccionando el paquete libaprutil1 previamente no seleccionado.
Desempaquetando libaprutil1 (de .../libaprutil1_1.3.9+dfsg-
1ubuntu1_i386.deb) ...
Seleccionando el paquete libaprutil1-dbd-sqlite3 previamente no
seleccionado.
Desempaquetando libaprutil1-dbd-sqlite3 (de .../libaprutil1-dbd-
sqlite3_1.3.9+dfsg-1ubuntu1_i386.deb) ...
Seleccionando el paquete libaprutil1-ldap previamente no
seleccionado.
Desempaquetando libaprutil1-ldap (de .../libaprutil1-
ldap_1.3.9+dfsg-1ubuntu1_i386.deb) ...
```

```
Seleccionando el paquete apache2.2-bin previamente no
seleccionado.
Desempaquetando apache2.2-bin (de .../apache2.2-bin_2.2.12-
1ubuntu2.2_i386.deb) ...
Seleccionando el paquete apache2-utils previamente no
seleccionado.
Desempaquetando apache2-utils (de .../apache2-utils_2.2.12-
1ubuntu2.2_i386.deb) ...
Seleccionando el paquete apache2.2-common previamente no
seleccionado.
Desempaquetando apache2.2-common (de .../apache2.2-common_2.2.12-
1ubuntu2.2_all.deb) ...
Seleccionando el paquete apache2-mpm-worker previamente no
seleccionado.
Desempaquetando apache2-mpm-worker (de .../apache2-mpm-
worker_2.2.12-1ubuntu2.2_all.deb) ...
Seleccionando el paquete apache2 previamente no seleccionado.
Desempaquetando apache2 (de .../apache2_2.2.12-1ubuntu2.2_all.deb)
...
Procesando disparadores para man-db ...
Procesando disparadores para ufw ...
Procesando disparadores para ureadahead ...
Configurando libapr1 (1.3.8-1) ...

Configurando libaprutil1 (1.3.9+dfsg-1ubuntu1) ...

Configurando libaprutil1-dbd-sqlite3 (1.3.9+dfsg-1ubuntu1) ...
Configurando libaprutil1-ldap (1.3.9+dfsg-1ubuntu1) ...
Configurando apache2.2-bin (2.2.12-1ubuntu2.2) ...
Configurando apache2-utils (2.2.12-1ubuntu2.2) ...
Configurando apache2.2-common (2.2.12-1ubuntu2.2) ...
Enabling site default.
Enabling module alias.
Enabling module autoindex.
Enabling module dir.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module status.
Enabling module auth_basic.
Enabling module deflate.
Enabling module authz_default.
Enabling module authz_user.
Enabling module authz_groupfile.
Enabling module authn_file.
Enabling module authz_host.

Configurando apache2-mpm-worker (2.2.12-1ubuntu2.2) ...
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
```

```
[ OK ]

Configurando apache2 (2.2.12-1ubuntu2.2) ...

Procesando disparadores para libc-bin ...
ldconfig deferred processing now taking place
```

Falta hacer lo del certificado que indican en http://guifi.net/node/9502, ??? es necesario????

proxy cache / web cache

Siguiendo los pasos de http://guifi.net/node/9502 y http://guifi.net/ca/proxy.

```
root@ftp2000-desktop:~# apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalaron de forma automática los siguientes paquetes y ya no
son necesarios.
  linux-headers-2.6.31-14 linux-headers-2.6.31-14-generic
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes extras:
  squid-common squid-langpack
Paquetes sugeridos:
  squidclient squid-cgi logcheck-database resolvconf winbind
Se instalarán los siguientes paquetes NUEVOS:
  squid squid-common squid-langpack
0 actualizados, 3 se instalarán, 0 para eliminar y 0 no
actualizados.
Necesito descargar 1346kB de archivos.
Se utilizarán 8651kB de espacio de disco adicional después de esta
operación.
¿Desea continuar [S/n]?
Des:1 http://es.archive.ubuntu.com karmic/main squid-langpack
3.HEAD.20090706-1ubuntu1 [230kB]
Des:2 http://es.archive.ubuntu.com karmic-updates/main squid-
common 2.7.STABLE6-2ubuntu2.2 [352kB]

Des:3 http://es.archive.ubuntu.com karmic-updates/main squid
2.7.STABLE6-2ubuntu2.2 [764kB]
Descargados 1346kB en 17s (78,1kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete squid-langpack previamente no
seleccionado.
(Leyendo la base de datos ...  00%
152972 ficheros y directorios instalados actualmente.)
Desempaquetando squid-langpack (de .../squid-
langpack_3.HEAD.20090706-1ubuntu1_all.deb) ...
Seleccionando el paquete squid-common previamente no seleccionado.
Desempaquetando squid-common (de .../squid-common_2.7.STABLE6-
```

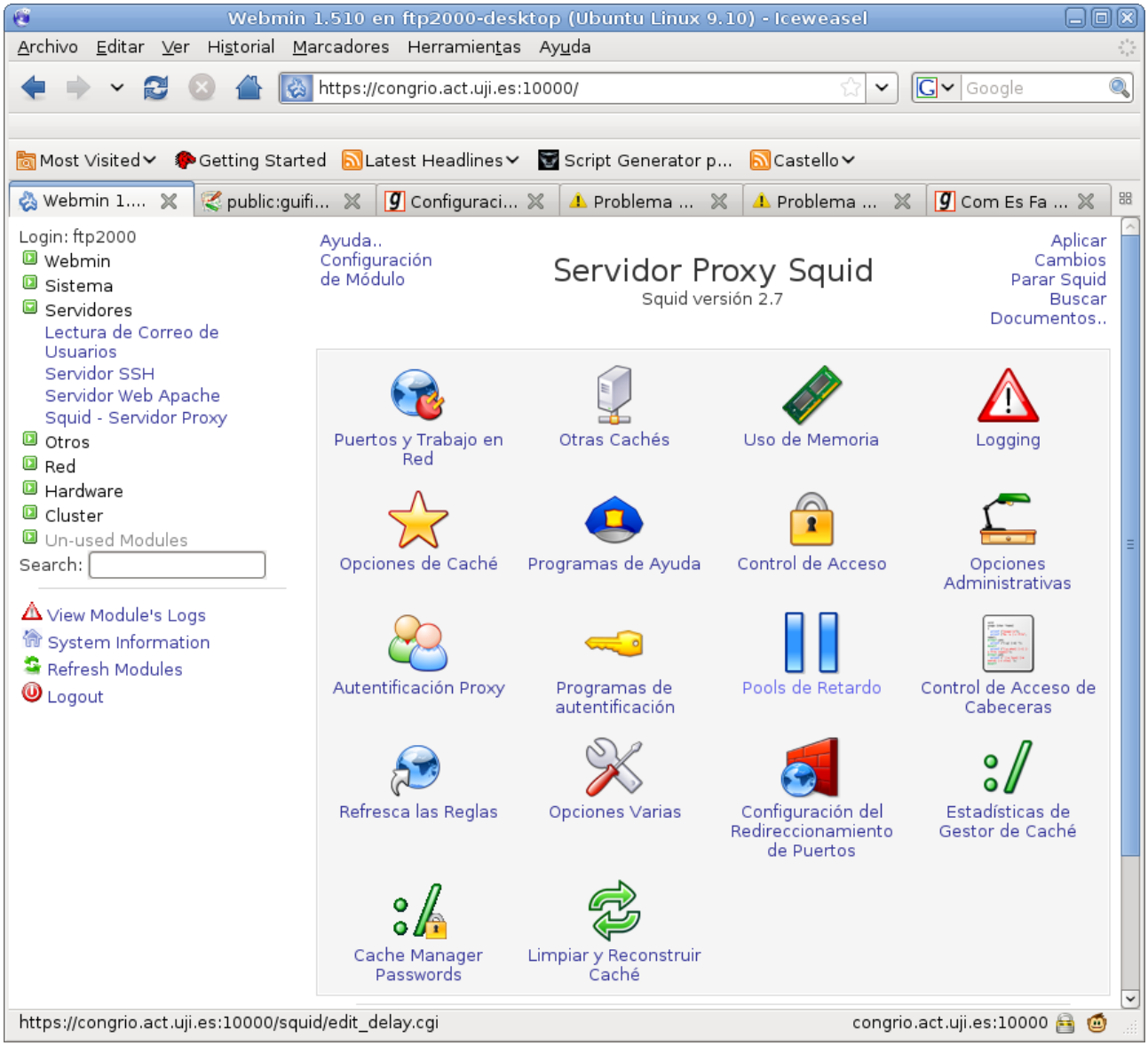
```
2ubuntu2.2_all.deb) ...
Seleccionando el paquete squid previamente no seleccionado.
Desempaquetando squid (de .../squid_2.7.STABLE6-
2ubuntu2.2_i386.deb) ...
Procesando disparadores para ureadahead ...
Procesando disparadores para man-db ...
Configurando squid-langpack (3.HEAD.20090706-1ubuntu1) ...
Configurando squid-common (2.7.STABLE6-2ubuntu2.2) ...

Configurando squid (2.7.STABLE6-2ubuntu2.2) ...
Creating squid spool directory structure
2010/03/18 14:01:15| Creating Swap Directories
 * Restarting Squid HTTP proxy squid
[ OK ]
```

Configuración utilizando webmin

Desde un terminal crear el directorio /usr/etc/passwd:

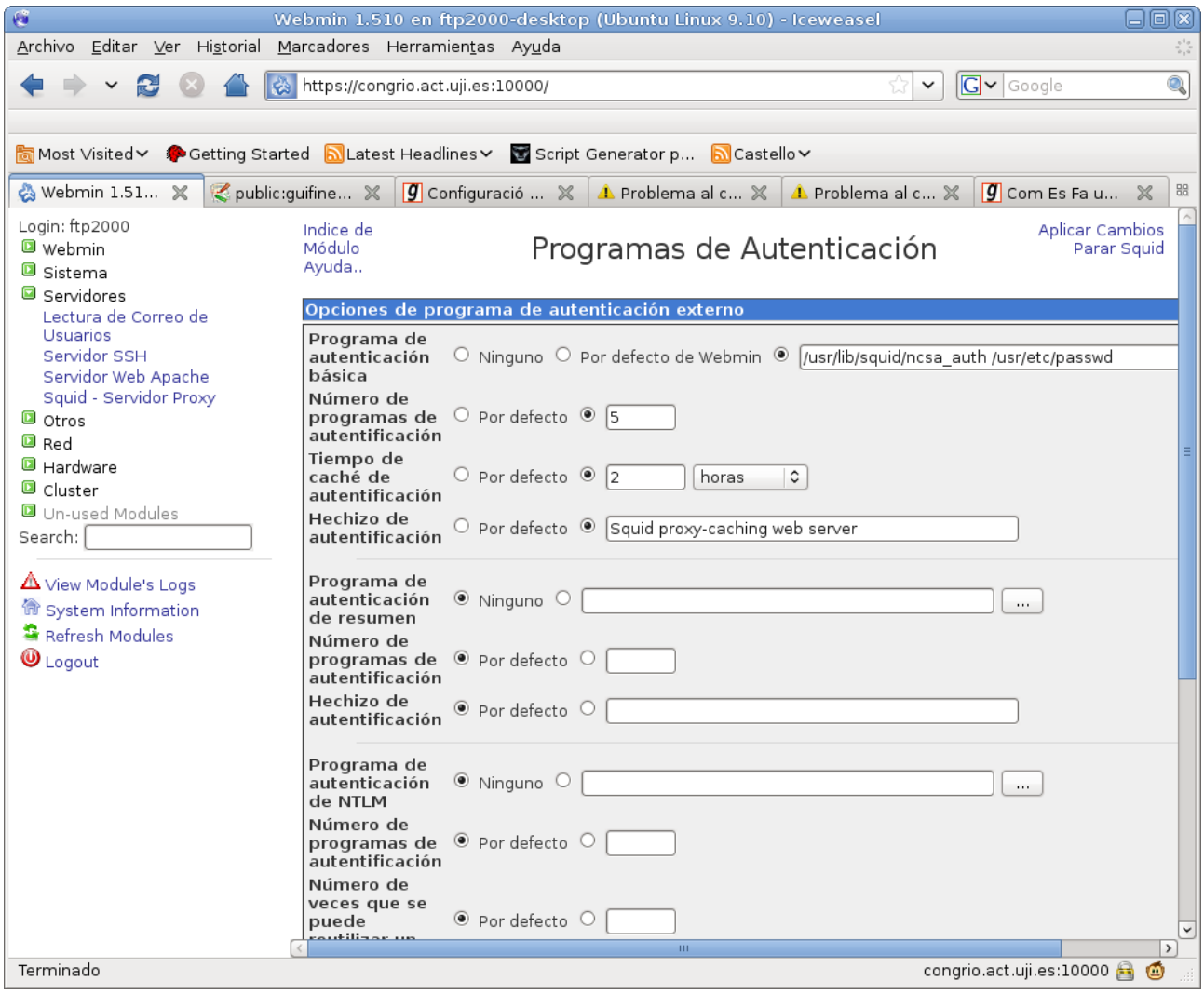
```
mkdir /usr/etc
touch /usr/etc/passwd
```

Acceder con el navegador a webmin en https://127.0.0.1:10000/ o https://ipDelServidor:10000/ y acceder a Servidores → Squid - Servidor Proxy. Si esta opción no aparece es porque no está actualizada la lista de módulos, seleccionando Refresh Modules debería aparecer



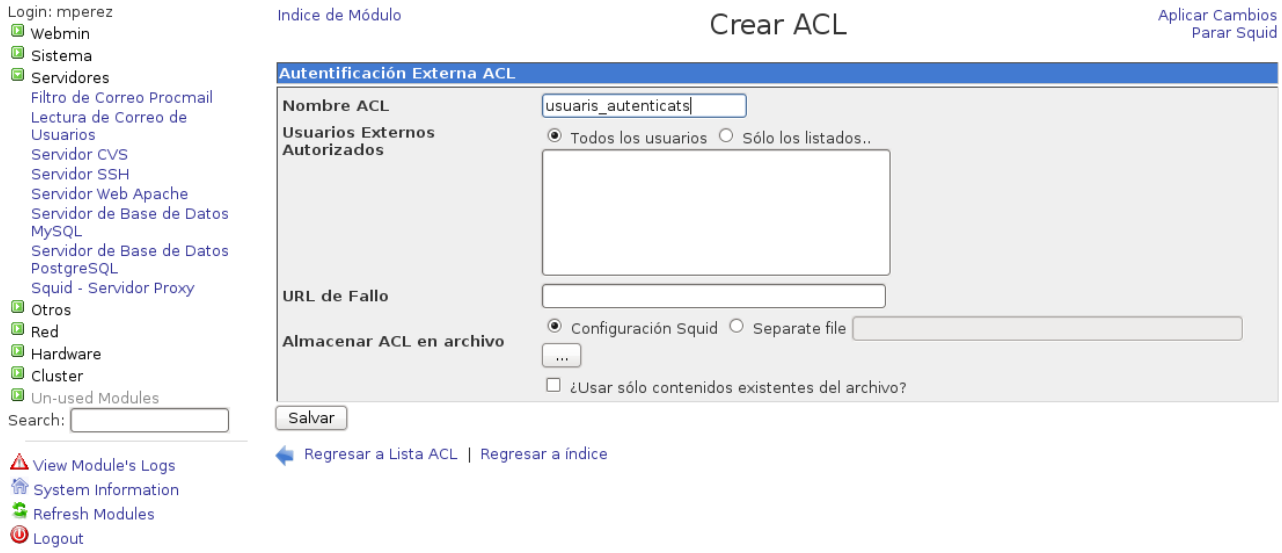
Seleccionar la opción `Programas de Autenticación` y poner los siguietes valores:

```
Programa de autenticación básica  /usr/lib/squid/ncsa_auth
/usr/etc/passwd
Número de programas de autentificación 5
Tiempo de caché de autentificación     2    horas
Hechizo de autentificación            Squid proxy-caching web
server
```

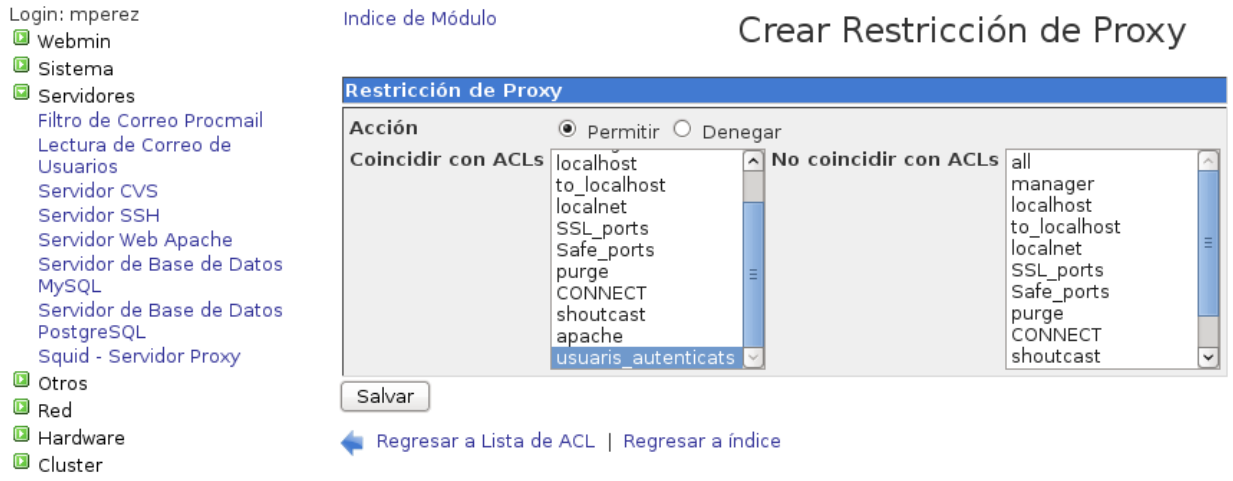


Al darle al botón `Salvar` se vuelve al meú de configuración de squid. Ahora hay que seleccionar la opción `Control de Acceso` y pulsar, en `Listas de control de acceso`, al final, el botón `Crear nueva ACL` de tipo `Autenticación externa`, como se indica en la siguiente figura:

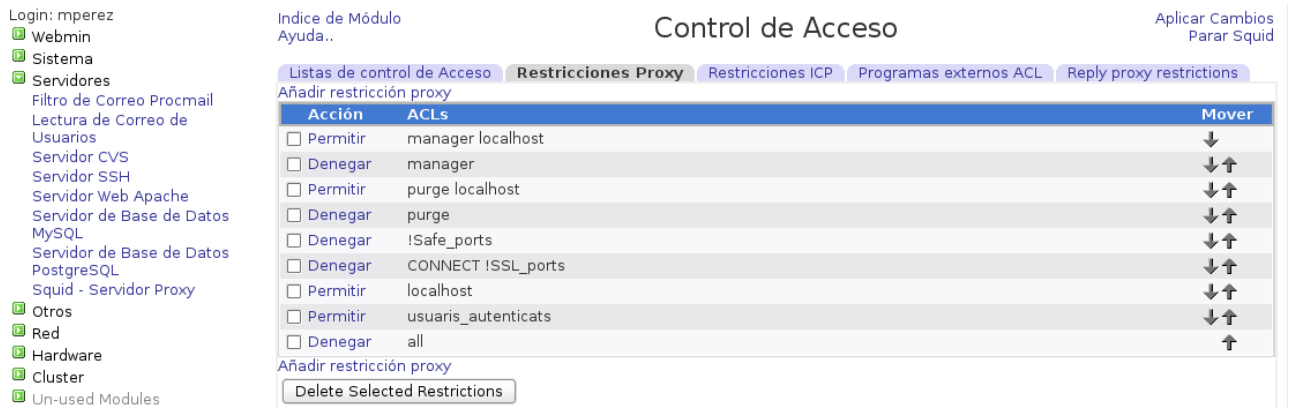
y en el menú `Autenticación externa`, poner en `Nombre ACL`: `usuaris_autenticats`



En la pestaña `Restricciones de proxy`, pulsar sobre `Añadir restricción proxy` y poner los valores que se indican en la figura y pulsar el botón `Salvar`



En la lista se ha de bajar la opción `Denegar all` a l'última posición, tal como se muestra en la figura



Por último hay que pulsar el enlace «Aplicar Cambios» que aparece en la parte superior derecha.

Otros

- QoS: tc??
- servidor de túneles: Openvpn
- Servidor voip y videoconferencia: Asterisk
- Servidor de gráficas guifi.net
- Autenticación: Free Radious
- DNS: PowerDNS?
- Copias de seguridad (sistema y logs): backup2l??
- enrutamiento: quagga
- SNMP (si el también hace de router, ha de enviar las gráficas).

Notas de instalación en servidores previos

Instalación de un servidor utilizando un ordenador viejo (portatil):

- El portátil está conectado por rj45 a un buffalo, dos nanos asociadas a dos APs (La Coma y el IESMiquelPeris) en modo bridge.
- Asociar cada nano con su ap y ponerla en modo bridge. Esto tiene algunos problemas, por ejemplo cuando un ordenador de la red interna pide una ip por dhcp, le puede contestar alguno de los APs de guifi.net y asignarle una IP. Por el momento lo soluciono dando ips fijas 
- Ponerle la ip del rango del AP al PC (si sólo tiene una interfaz hay que crearla como un alias). Hacerlo permanente en interfaces.

```
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see
interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

#iface eth0 inet dhcp
#auto eth0

auto eth0
iface eth0 inet static
address 192.168.1.157
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
```

```
post-up ifup eth0:2
pre-down ifdown eth0:2
post-up ifup eth0:3
pre-down ifdown eth0:3


iface eth0:2 inet static
address 10.228.152.37
netmask 255.255.255.224
network 10.228.152.32
broadcast 10.228.152.63
gateway 10.228.152.33


iface eth0:3 inet static
address 10.228.144.62
netmask 255.255.255.224
network 10.228.144.32
broadcast 10.228.144.63
```

las lineas

```
post-up ifup eth0:2
pre-down ifdown eth0:2
post-up ifup eth0:3
pre-down ifdown eth0:3
```

no son en principio necesarias, pero en algun caso no levanta los alias si no se ponen.

- Hacer NAT de la red privada:

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -d 0.0.0.0/0  -j SNAT --to 10.228.152.37
```

y hacerlo permanente (También se puede poner junto al firewall del punto posterior)

editar `/etc/network/interfaces` y poner las siguientes líneas al final:

```
iface eth0 inet static
      address 192.168.0.200
      netmask 255.255.255.0
      network 192.168.0.0
      post-up iptables -A POSTROUTING -t nat -j MASQUERADE -s 192.168.0.0/24
      post-up echo 1 > /proc/sys/net/ipv4/ip_forward
```

!!!Pendiente de probar!!!

- Firewall en el router (pendiente)

```
#!/bin/sh
IPTABLES=/sbin/iptables

  # 1) Definir la norma de cada cadena básica
  $IPTABLES -P INPUT ACCEPT
```

```
  $IPTABLES -P FORWARD ACCEPT
  $IPTABLES -P OUTPUT ACCEPT

  $IPTABLES -F

  #$IPTABLES -t nat -A POSTROUTING -o eth0 -j SNAT --to
10.228.130.162
  $IPTABLES -t nat -A POSTROUTING -s 192.168.1.0/24 -d 0.0.0.0/0 -
j SNAT --to 10.228.152.37

  # 2) Aceptar paquetes en estado establecido y relacionado
  $IPTABLES -A INPUT -i lo -j ACCEPT
  $IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT

  $IPTABLES -I INPUT -p icmp -j ACCEPT

  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 22 -j
ACCEPT
  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 25 -j
ACCEPT
  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 53 -j
ACCEPT
  $IPTABLES -A INPUT -m state --state NEW -p udp --dport 53 -j
ACCEPT
  $IPTABLES -A INPUT -m state --state NEW -p tcp --dport 80 -j
ACCEPT

  # Para el SNMP
  $IPTABLES -A INPUT -m state --state NEW -p udp --dport 161  -j
ACCEPT

  # Para quagga
  $IPTABLES  -A INPUT -p 89 -j ACCEPT

  $IPTABLES -A INPUT -j DROP
```

y hacerlo permanente.

- Instalar quagga, configurar el zebra y el ospf. El modo bridge de las nanos,

parece que sí que pasan los hellos pero no las rutas. Hay que definir que la red no es multicast e indocar los vecinos (ver http://wiki.quagga.net/index.php/Main/FAQ y http://wiki.quagga.net/index.php/Main/CfEx#toc9)

Ficheros en `/etc/quagga`:

```
coscoll:/etc/quagga# cat daemons
zebra=yes
bgpd=no
ospfd=yes
ospf6d=no
```

```
ripd=no
ripngd=no
isisd=no
```

```
coscoll:/etc/quagga# cat zebra.conf
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.1.1.1 2002/12/13 20:15:30 paul Exp $
!
hostname serradal.
password zebraaa
enable password zebraaa
!
! Interface's description.
!
!interface lo
! description test of desc.
!
!interface sit0
! multicast

interface eth0
  description virtual para el enlace con al coma

!
! Static default route sample.
!
!ip route 0.0.0.0/0 10.228.152.33
!

log file /var/log/quagga/zebra.log
```

```
coscoll:/etc/quagga# cat ospfd.conf
! -*- ospf -*-
!
! OSPFd sample configuration file
!
!
hostname serradal
password zebraaa
enable password zebraaa
!
interface eth0
!  ip ospf network point-to-point
   ip ospf network non-broadcast

router ospf
  ospf router-id 10.228.152.37
  network 10.228.152.32/27 area 0
  network 10.228.144.32/27 area 0
  neighbor 10.228.152.33
```

```
  neighbor 10.228.144.33
!
log file /var/log/quagga/ospf.log
```

- snmp: http://www.debian-administration.org/articles/366

Otros enlaces interesantes sobre snmp y herramientas de visualización:

http://www.debuntu.org/how-to-monitor-your-servers-with-snmp-and-cacti

http://edin.no-ip.com/content/snmp-rrdtool-cacti-debian-lenny-mini-howto

Enlaces

Tracedump:

```
newBaseSize: 12pt
newBaseSizeInPt: 12
```