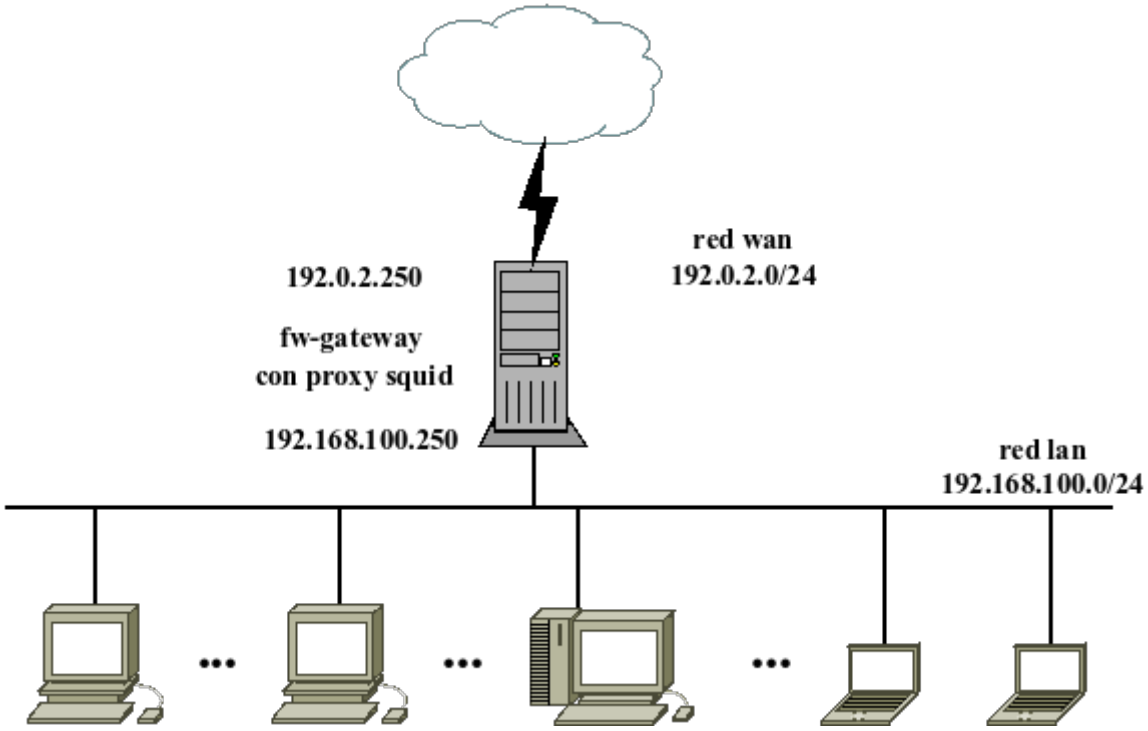
Squid en Ubuntu Linux

Dada la organización de la figura instala y configura el servidor proxy squid en el equipo Linux Ubuntu Server para establecer restricciones de acceso en base a los siguientes requerimientos:



Equipos administradores	de la .1 a la .3
Eq. trabajadores 1º turno	de la .4 a la .120
Eq. trabajadores 2º turno	de la .121 a la .140
Eq. trabajadores turno de noche	de la .141 a la .150
Eq. técnicos externos	de la .151 a la .160
Eq. pruebas	de la .161 a la .162

- La caché en disco será como mínimo de 3 GBytes y para la caché en memoria RAM se reservarán 300 MBytes. En ambos casos, no se guardarán archivos con un tamaño superior a los 100Kbytes.
- El servidor proxy registrará las solicitudes y rotará los logs cada 7 días.
- Los mensajes de error estarán en castellano por defecto.

Restricciones de tráfico:

- Los equipos de los administradores serán los únicos en poder gestionar el equipo fw-gateway vía ssh.
- Los equipos de los administradores saldrán a Internet por el proxy sin ningún tipo de restricciones.
- Con independencia de horarios y para el resto de usuarios del proxy:

  - Usando acl de tipo `dstdomain` crea una lista blanca donde se permite el acceso a cualquier sitio web de los dominios edu.xunta.es, edu.xunta.gal, sepe.es, amazon.es y a www.elmundo.es.
  - Usando acl de tipo `dstdom_regex` crea una lista negra donde se bloquea el acceso a cualquier sitio web de los dominios xunta.es, xunta.gal, elpais.com, lavozdegalicia.es, facebook, tuenti, microsoft, amazon y sitios torrent.
  - Usando acl de tipo `urlpath_regex` bloquea la descarga de torrents (p.e. desde los sitios web de descargar de Ubuntu) y páginas relativas a deportes.
- Los equipos de los trabajadores del 1º turno podrán visitar sitios web a través del proxy únicamente dentro de su horario de trabajo, que va de lunes a viernes de las 08:00 a las 15:00 horas. Usa acl de tipo `time`
- Los equipos de los trabajadores del 2º turno podrán visitar sitios web a través del proxy únicamente dentro de su horario de trabajo, que va de lunes a viernes de las 16:00 a las 20:00 horas y el sábado y domingo de 10:00 a 14:00.
- Los equipos de los trabajadores del turno de noche podrán visitar sitios web a través del proxy únicamente dentro de su horario de trabajo, que va de lunes a domingo de las 20:00 a las 04:00 horas.
- Los equipos de los técnicos externos saldrán a navegar usando el proxy como proxy transparente sin restricciones horarias.
- Los administradores tienen dos equipos de pruebas que pueden navegar por Internet con salida directa; es decir, sus comunicaciones no pasan por el proxy squid.
- Usando la regla de control de acceso `reply_body_max_size` limita el tamaño máximo de descarga de archivos a 20MBytes a todos, salvo a los administradores.
- Crea una acl asociada a un fichero donde se guarden todos los equipos baneados (que no pueden usar el proxy).
- Para las resoluciones DNS los equipos de la LAN y el propio Ubuntu Server emplearán los servidores 8.8.8.8 y 8.8.4.4.
- Únicamente se permite el tráfico estrictamente necesario para que el sistema funcione; por lo que, el resto de comunicaciones deben prohibirse.
- La IP asignada a la interfaz WAN del servidor Ubuntu se considera como una IP pública.
- Hay que crear las regras de filtrado/NAT para hacer que funcionen conjuntamente netfilter y squid.
- Justifica, aportando pruebas; por que, a pesar de estar permitido totalmente amazon.es y www.elmundo.es, esas páginas no se cargan correctamente.

How Squid Matches Access Rules

Recall that Squid uses OR logic when searching ACL elements. Any single value in an acl can cause a match.

It's the opposite for access rules, however. For http_access and the other rule sets, Squid uses AND logic. Consider this generic example:

access_list allow ACL1 ACL2 ACL3

For this rule to be a match, the request must match each of ACL1, ACL2, and ACL3. If any of those ACLs don't match the request, Squid stops searching this rule and proceeds to the next.

Within a single rule, you can optimize rule searching by putting least-likely-to-match ACLs first.

Instalación de squid

Ejecución del script de creación del escenario:

```
$ lxc ls -c n,4,s,l,P,m
+-------+-----------------------+---------+---------------------+----------+-------------+
| NAME  |          IPV4         |  STATE  |     LAST USED AT    | PROFILES | MEMORY USAGE |
+-------+-----------------------+---------+---------------------+----------+-------------+
| squid | 192.168.100.250 (eth1) | RUNNING | 2022/04/30 08:19 UTC | WAN-LAN  | 183.52MiB    |
|       | 192.0.2.250 (eth0)     |         |                     |          |              |
+-------+-----------------------+---------+---------------------+----------+-------------+
$ lxc exec squid -- su - ubuntu
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@squid:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
33: eth0@if34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen
1000
    link/ether 00:16:3e:e4:36:3a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.0.2.250/24 brd 192.0.2.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fee4:363a/64 scope link
       valid_lft forever preferred_lft forever
35: eth1@if36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen
1000
    link/ether 00:16:3e:c7:06:be brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.100.250/24 brd 192.168.100.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fec7:6be/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@squid:~$ ip route
default via 192.0.2.1 dev eth0 proto static
192.0.2.0/24 dev eth0 proto kernel scope link src 192.0.2.250
192.168.100.0/24 dev eth1 proto kernel scope link src 192.168.100.250
ubuntu@squid:~$ host www.edu.xunta.gal
www.edu.xunta.gal has address 85.91.64.65
```

Actualizar listado paquetes e instalación software:

```
ubuntu@squid:~$ sudo apt update
ubuntu@squid:~$ apt show squid
Package: squid
Version: 4.10-1ubuntu1.5
Priority: optional
Section: web
Origin: Ubuntu
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Original-Maintainer: Luigi Gangitano <luigi@debian.org>
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
Installed-Size: 8.809 kB
Provides: squid3
```

```
Pre-Depends: adduser
Depends: libc6 (>= 2.29), libcap2 (>= 1:2.10), libcom-err2 (>= 1.43.9), libcrypt1 (>= 1:4.1.0), libdb5.3, libecap3 (>= 1.0.1), libexpat1 (>= 2.0.1), libgcc-s1 (>= 3.0), libgnutls30 (>= 3.6.12), libgssapi-krb5-2 (>= 1.17), libkrb5-3 (>= 1.10+dfsg~), libldap-2.4-2 (>= 2.4.7), libltdl7 (>= 2.4.6), libnetfilter-conntrack3 (>= 1.0.7), libnettle7, libpam0g (>= 0.99.7.1), libsasl2-2 (>= 2.1.27+dfsg), libstdc++6 (>= 9), libxml2 (>= 2.7.4), netbase, logrotate (>= 3.5.4-1), squid-common (>= 4.10-1ubuntu1.5), lsb-base, libdbi-perl, ssl-cert
Recommends: libcap2-bin, ca-certificates
Suggests: squidclient, squid-cgi, squid-purge, resolvconf (>= 0.40), smbclient, ufw, winbind, apparmor
Homepage: http://www.squid-cache.org
Download-Size: 2.562 kB
APT-Sources: http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages
Description: Full featured Web Proxy cache (HTTP proxy)
 Squid is a high-performance proxy caching server for web clients, supporting
 FTP, gopher, ICY and HTTP data objects.

N: Hay 1 registro adicional. Utilice la opción «-a» para verlo.
ubuntu@squid:~$ sudo apt install squid
ubuntu@squid:~$ ls -lhF /etc/squid/
total 156K
drwxr-xr-x 2 root root    3 abr 30 10:26 conf.d/
-rw-r--r-- 1 root root 1,8K oct  4  2021 errorpage.css
-rw-r--r-- 1 root root 310K oct  4  2021 squid.conf
ubuntu@squid:~$ sudo mv /etc/squid/squid.conf /etc/squid/squid.conf.ORIGINAL
ubuntu@squid:~$ sudo nano /etc/squid/squid.conf
http_port 192.168.100.250:3128                ← socket escucha solicitudes proxy estándar
http_port 192.168.100.250:3129 intercept      ← socket escucha solicitudes proxy transparente

visible_hostname fw-gateway
cache_mgr admin@milxd.org
error_default_language es-es


cache_effective_user proxy
cache_effective_group proxy

access_log /var/log/squid/access.log          ← ficheros de log
cache_log /var/log/squid/cache.log
cache_store_log none
logfile_rotate 7                              ← rotación ficheros de log
debug_options rotate=7

cache_mem 300 MB                              ← tamaño caché en memoria RAM
maximum_object_size_in_memory 100 KB          ← tamaño máximo archivo en caché en memoria RAM
memory_replacement_policy heap GDSF
cache_replacement_policy heap LFUDA
cache_dir ufs /var/spool/squid 3072 16 256    ← tamaño caché en disco duro y directorios L1/L2
minimum_object_size 0 KB
maximum_object_size 100 KB                    ← tamaño máximo archivo en caché en disco duro
offline_mode off
cache_swap_low 90
cache_swap_high 95

refresh_pattern ^ftp:             1440   20%    10080
refresh_pattern ^gopher:   1440   0%     1440
refresh_pattern -i (/cgi-bin/|\?) 0      0%     0
refresh_pattern (Release|Packages(.gz)*)$      0       20%     2880
```

```
refresh_pattern .          0      20%    4320

acl localnet src 192.168.100.0/24            ← definición red lan
acl allsrc src all
acl safeports port 21 70 80 210 280 443 488 563 591 631 777 901  3128 3127 1025-65535
acl sslports port 443 563
acl connect method CONNECT

# Equipos
acl admin src 192.168.100.1-192.168.100.3
acl trabajadores_turno1 src 192.168.100.4-192.168.100.120
acl trabajadores_turno2 src 192.168.100.121-192.168.100.140
acl trabajadores_noche src 192.168.100.141-192.168.100.150
acl tecnicos src 192.168.100.151-192.168.100.160
acl banned_hosts src "/etc/squid/acls/banned_hosts.acl"
# Horarios
acl turno1 time MTWHF 08:00-15:00
acl turno2 time MTWHF 16:00-20:00
acl turno2 time AS 10:00-14:00
acl noche time 20:00-23:59
acl noche time 00:00-04:00
# Restricciones
acl lista_blanca dstdomain "/etc/squid/acls/whitelist.acl"
acl lista_negra dstdom_regex -i "/etc/squid/acls/blacklist.acl"
acl bloquear_torrent urlpath_regex -i torrent
acl bloquear_torrent urlpath_regex -i deportes
#acl deny_rep_mime_flashvideo rep_mime_type video/flv
#acl youtube_domains dstdomain .youtube.com .googlevideo.com .ytimg.com


#deny_info ERROR_BANNED banned_hosts
#deny_info ERROR_BLACKLIST blacklist

# Permitir/denegar en base a las access list
http_access deny !safeports
http_access deny connect !sslports

http_access deny banned_hosts
http_access allow admin
http_access allow lista_blanca
http_access deny lista_negra
http_access deny bloquear_torrent
#http_access deny youtube_domains

http_access allow trabajadores_turno1 turno1
http_access allow trabajadores_turno2 turno2
http_access allow trabajadores_noche noche
http_access allow tecnicos
http_access deny allsrc

reply_body_max_size 20 MB allsrc !admin

#http_reply_access deny deny_rep_mime_flashvideo
```

Creación de los ficheros de las acls:

```
ubuntu@squid:~$ sudo mkdir /etc/squid/acls
ubuntu@squid:~$ sudo nano /etc/squid/acls/banned_hosts.acl
```

```
192.168.100.161-192.168.100.255
ubuntu@squid:~$ sudo nano /etc/squid/acls/whitelist.acl
.edu.xunta.es
.edu.xunta.gal
.sepe.es
.amazon.es
www.elmundo.es
ubuntu@squid:~$ sudo nano /etc/squid/acls/blacklist.acl
xunta.es
xunta.gal
elpais.com
lavozdegalicia.es
facebook
tuenti
microsoft
amazon
torrent
```

Comprobación de que no hay errores en el archivo de configuración:

```
ubuntu@squid:~$ sudo squid -k parse
2022/04/30 11:11:35| Startup: Initializing Authentication Schemes ...
2022/04/30 11:11:35| Startup: Initialized Authentication Scheme 'basic'
2022/04/30 11:11:35| Startup: Initialized Authentication Scheme 'digest'
2022/04/30 11:11:35| Startup: Initialized Authentication Scheme 'negotiate'
2022/04/30 11:11:35| Startup: Initialized Authentication Scheme 'ntlm'
2022/04/30 11:11:35| Startup: Initialized Authentication.
2022/04/30 11:11:35| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2022/04/30 11:11:35| Processing: http_port 192.168.100.250:3128
2022/04/30 11:11:35| Processing: http_port 192.168.100.250:3129 intercept
2022/04/30 11:11:35| Starting Authentication on port 192.168.100.250:3129
2022/04/30 11:11:35| Disabling Authentication on port 192.168.100.250:3129 (interception enabled)
2022/04/30 11:11:35| Processing: visible_hostname fw-gateway
2022/04/30 11:11:35| Processing: cache_mgr admin@milxd.org
2022/04/30 11:11:35| Processing: error_default_language es-es
2022/04/30 11:11:35| Processing: cache_effective_user proxy
2022/04/30 11:11:35| Processing: cache_effective_group proxy
2022/04/30 11:11:35| Processing: access_log /var/log/squid/access.log
2022/04/30 11:11:35| Processing: cache_log /var/log/squid/cache.log
2022/04/30 11:11:35| Processing: cache_store_log none
2022/04/30 11:11:35| Processing: logfile_rotate 7
2022/04/30 11:11:35| Processing: debug_options rotate=7
2022/04/30 11:11:35| Processing: cache_mem 300 MB
2022/04/30 11:11:35| Processing: maximum_object_size_in_memory 100 KB
2022/04/30 11:11:35| Processing: memory_replacement_policy heap GDSF
2022/04/30 11:11:35| Processing: cache_replacement_policy heap LFUDA
2022/04/30 11:11:35| Processing: cache_dir ufs /var/spool/squid 3072 16 256
2022/04/30 11:11:35| Processing: minimum_object_size 0 KB
2022/04/30 11:11:35| Processing: maximum_object_size 100 KB
2022/04/30 11:11:35| Processing: offline_mode off
2022/04/30 11:11:35| Processing: cache_swap_low 90
2022/04/30 11:11:35| Processing: cache_swap_high 95
2022/04/30 11:11:35| Processing: refresh_pattern ^ftp:       1440   20%    10080
2022/04/30 11:11:35| Processing: refresh_pattern ^gopher:    1440   0%     1440
2022/04/30 11:11:35| Processing: refresh_pattern -i (/cgi-bin/|\?) 0      0%     0
2022/04/30 11:11:35| Processing: refresh_pattern (Release|Packages(.gz)*)$      0       20%     2880
2022/04/30 11:11:35| Processing: refresh_pattern .           0      20%    4320
2022/04/30 11:11:35| Processing: acl localnet src 192.168.100.0/24
```

```
2022/04/30 11:11:35| Processing: acl allsrc src all
2022/04/30 11:11:35| Processing: acl safeports port 21 70 80 210 280 443 488 563 591 631 777 901  3128
3127 1025-65535
2022/04/30 11:11:35| Processing: acl sslports port 443 563
2022/04/30 11:11:35| Processing: acl connect method CONNECT
2022/04/30 11:11:35| Processing: acl admin src 192.168.100.1-192.168.100.3
2022/04/30 11:11:35| Processing: acl trabajadores_turno1 src 192.168.100.4-192.168.100.120
2022/04/30 11:11:35| Processing: acl trabajadores_turno2 src 192.168.100.121-192.168.100.140
2022/04/30 11:11:35| Processing: acl trabajadores_noche src 192.168.100.141-192.168.100.150
2022/04/30 11:11:35| Processing: acl tecnicos src 192.168.100.151-192.168.100.160
2022/04/30 11:11:35| Processing: acl banned_hosts src "/etc/squid/acls/banned_hosts.acl"
2022/04/30 11:11:35| Processing: acl turno1 time MTWHF 08:00-15:00
2022/04/30 11:11:35| Processing: acl turno2 time MTWHF 16:00-20:00
2022/04/30 11:11:35| Processing: acl turno2 time AS 10:00-14:00
2022/04/30 11:11:35| Processing: acl noche time 20:00-23:59
2022/04/30 11:11:35| Processing: acl noche time 00:00-04:00
2022/04/30 11:11:35| Processing: acl lista_blanca dstdomain "/etc/squid/acls/whitelist.acl"
2022/04/30 11:11:35| Processing: acl lista_negra dstdom_regex -i "/etc/squid/acls/blacklist.acl"
2022/04/30 11:11:35| Processing: acl bloquear_torrent urlpath_regex -i torrent
2022/04/30 11:11:35| Processing: acl bloquear_torrent urlpath_regex -i deportes
2022/04/30 11:11:35| Processing: http_access deny !safeports
2022/04/30 11:11:35| Processing: http_access deny connect !sslports
2022/04/30 11:11:35| Processing: http_access deny banned_hosts
2022/04/30 11:11:35| Processing: http_access allow admin
2022/04/30 11:11:35| Processing: http_access allow lista_blanca
2022/04/30 11:11:35| Processing: http_access deny lista_negra
2022/04/30 11:11:35| Processing: http_access deny bloquear_torrent
2022/04/30 11:11:35| Processing: http_access allow trabajadores_turno1 turno1
2022/04/30 11:11:35| Processing: http_access allow trabajadores_turno2 turno2
2022/04/30 11:11:35| Processing: http_access allow trabajadores_noche noche
2022/04/30 11:11:35| Processing: http_access allow tecnicos
2022/04/30 11:11:35| Processing: http_access deny allsrc
2022/04/30 11:11:35| Processing: reply_body_max_size 20 MB allsrc !admin
2022/04/30 11:11:35| Initializing https:// proxy context
```

Parada, creación de caché L1/L2 y arranque:

```
ubuntu@squid:~$ sudo systemctl stop squid
ubuntu@squid:~$ sudo squid -z
2022/04/30 11:14:41 kid1| Creating missing swap directories
ubuntu@squid:~$ ls -lhF /var/spool/squid/
total 89K
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 00/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 01/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 02/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 03/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 04/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 05/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 06/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 07/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 08/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 09/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 0A/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 0B/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 0C/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 0D/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 0E/
drwxr-x--- 258 proxy proxy 258 abr 30 11:14 0F/
```

```
-rw-r-----   1 proxy proxy   0 abr 30 11:12 netdb.state
ubuntu@squid:~$ sudo systemctl start squid
ubuntu@squid:~$ ss -ltn
State                Recv-Q      Send-Q     Local Address:Port     Peer Address:Port   Process
LISTEN               0           4096       127.0.0.53%lo:53       0.0.0.0:*
LISTEN               0           128        0.0.0.0:22             0.0.0.0:*
LISTEN               0           256        192.168.100.250:3128   0.0.0.0:*
LISTEN               0           256        192.168.100.250:3129   0.0.0.0:*
LISTEN               0           128        [::]:22                [::]:*
```

Pruebas funcionamiento squid

Creación de un contenedor LXD que funcione como equipo cliente:

```
$ lxc launch ubuntu:f cliente -p LAN
$ lxc ls -c n,4,s,l,P,m
+---------+-------------------------+---------+---------------------+----------+--------------+
|  NAME   |          IPV4           |  STATE  |     LAST USED AT    | PROFILES | MEMORY USAGE |
+---------+-------------------------+---------+---------------------+----------+--------------+
| cliente | 192.168.100.137 (eth0)  | RUNNING | 2022/04/30 09:22 UTC | LAN      | 267.54MiB    |
+---------+-------------------------+---------+---------------------+----------+--------------+
| squid   | 192.168.100.250 (eth1)  | RUNNING | 2022/04/30 08:19 UTC | WAN-LAN  | 472.31MiB    |
|         | 192.0.2.250 (eth0)      |         |                      |          |              |
+---------+-------------------------+---------+---------------------+----------+--------------+
$ lxc exec cliente -- su - ubuntu
ubuntu@cliente:~$ sudo apt update
ubuntu@cliente:~$ sudo apt install firefox
```

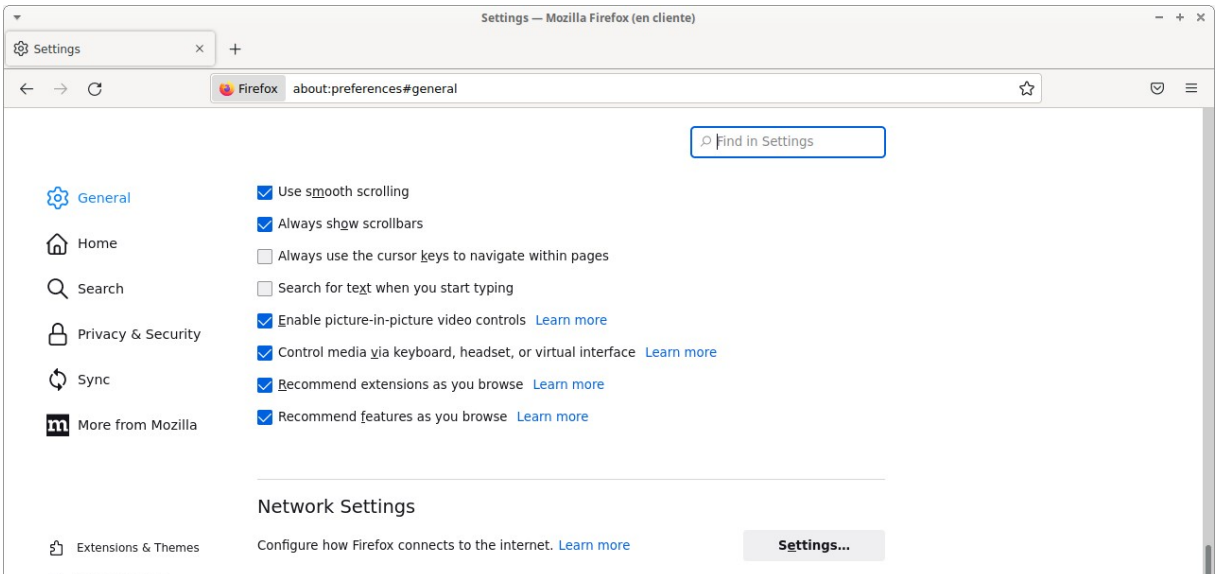
Preparación de ssh: acceso por contraseñas y X11 forwarding.

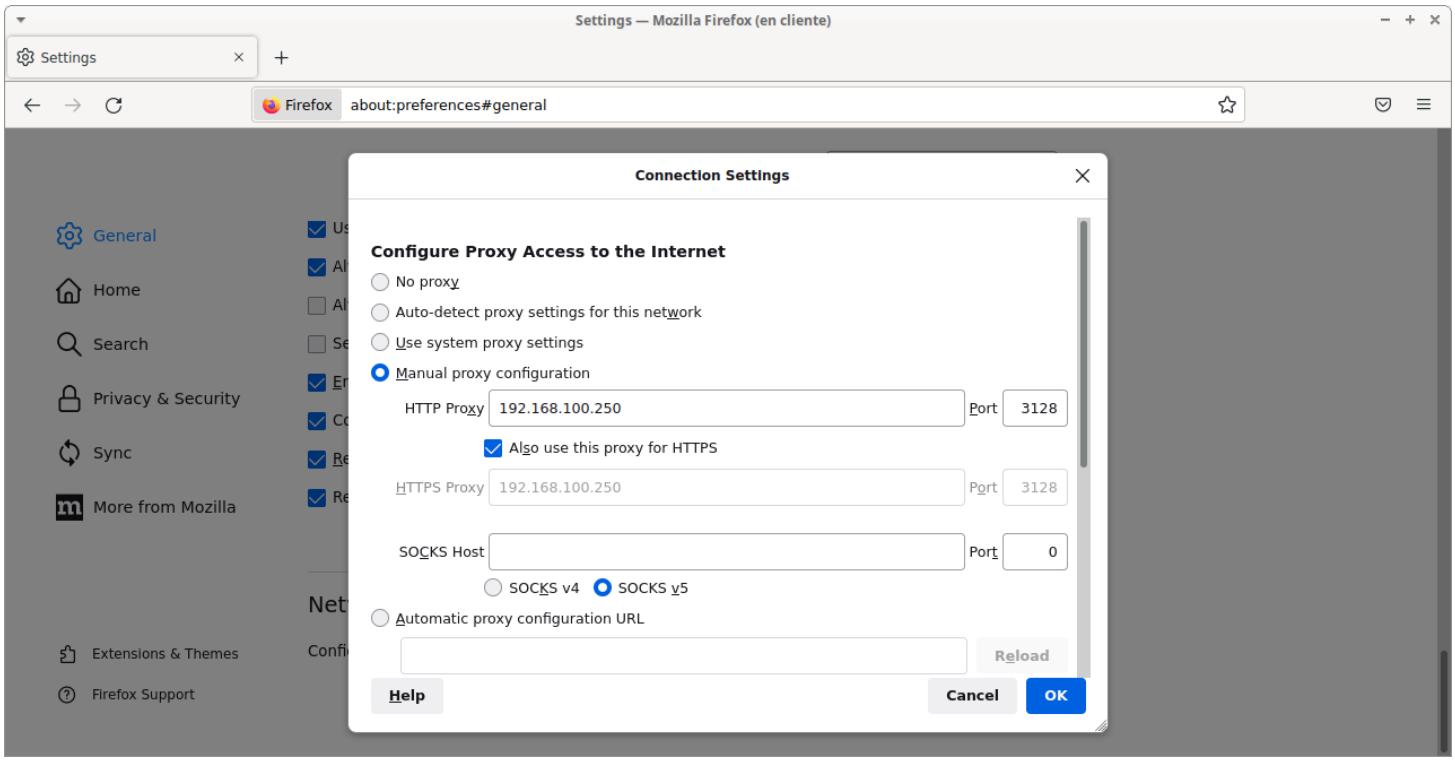
```
ubuntu@cliente:~$ passwd
New password:
Retype new password:
passwd: password updated successfully
ubuntu@cliente:~$ sudo nano /etc/ssh/sshd_config
PasswordAuthentication yes
X11Forwarding yes
ubuntu@cliente:~$ sudo systemctl restart sshd
```

Desde el equipo anfitrión:

```
manuel@x99:/$ ssh -X ubuntu@192.168.100.137
ubuntu@cliente:~$ firefox &
```

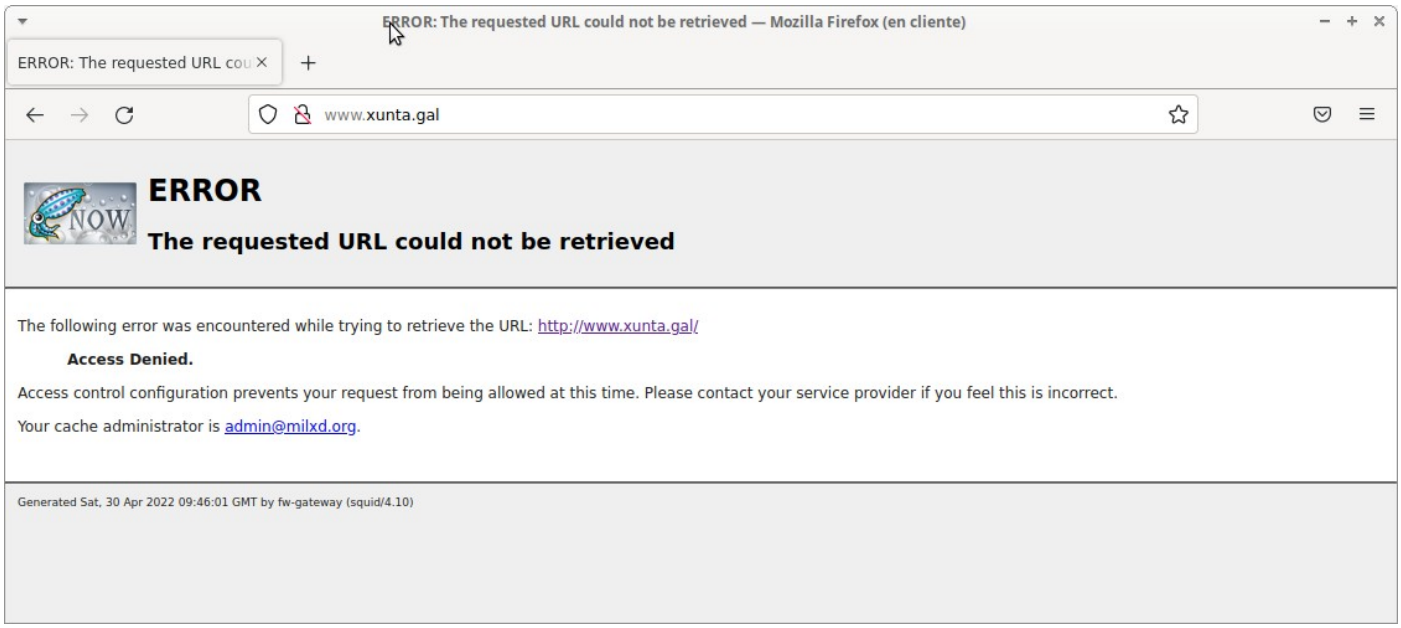
En la nueva ventana configurar el proxy en Firefox:





Se accede a www.edu.xunta.gal y xunta.gal:

```
1651311806.040     70 192.168.100.137 TCP_TUNNEL/200 39 CONNECT www.google.com:443 - HIER_DIRECT/142.250.185.4 -
1651311806.144     39 192.168.100.137 TCP_TUNNEL/200 39 CONNECT www.google.com:443 - HIER_DIRECT/142.250.185.4 -
1651311807.055     32 192.168.100.137 TCP_MISS/302 533 GET http://www.edu.xunta.gal/ - HIER_DIRECT/85.91.64.65 text/html
1651311807.081     20 192.168.100.137 TCP_MISS/200 16971 GET http://www.edu.xunta.gal/portal/ - HIER_DIRECT/85.91.64.65
text/html
1651311807.216      0 192.168.100.137 TCP_MISS_ABORTED/000 0 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_css/css__16296QiifbV8crkgBDfEDd7_r9v9fFxzxqUxT01fZK4__aJc2Hu2LbZJ
hyQhgSZdjf1vvqZjrwAEdWY2qINb_lMU__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.css - HIER_DIRECT/85.91.64.65 -
1651311823.118     29 192.168.100.137 TCP_MISS/200 17054 GET http://www.edu.xunta.gal/portal/ - HIER_DIRECT/85.91.64.65
text/html
1651311823.158     14 192.168.100.137 TCP_MISS/200 8551 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_css/css__16296QiifbV8crkgBDfEDd7_r9v9fFxzxqUxT01fZK4__aJc2Hu2LbZJ
hyQhgSZdjf1vvqZjrwAEdWY2qINb_lMU__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.css - HIER_DIRECT/85.91.64.65 text/css
1651311823.178     12 192.168.100.137 TCP_MISS/200 11098 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_js/js__txIUoBhNgCFMUUq3ki6DkrCRphW6uMPjds8i2p3um8w__echXbspW_7FN3
IHXbrOov97FjFSNJ5ZuSwp5RNbvXZI__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.js - HIER_DIRECT/85.91.64.65 text/javascript
1651311823.184     30 192.168.100.137 TCP_MISS/200 9228 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_js/js__rXB9yWbmntwzyHYOams4l2KPMachJRjzZZSuNab8cNc__DKYu2cvYgiI7U
ibSH4stPZAV-ESMtu5UsRK2VGHTuXg__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.js - HIER_DIRECT/85.91.64.65 text/javascript
1651311823.186     38 192.168.100.137 TCP_MISS/200 48851 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_css/css__rfGO4EV5xOCBQofSytHfjX9rXa_y9DyK8VqMq4vzetc__r3DMFN8QSmK
AeqXoh1z4gTtSFUaeqzds3j0AVEeN_Uk__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.css - HIER_DIRECT/85.91.64.65 text/css
1651311823.211     11 192.168.100.137 TCP_MISS/200 7459 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_js/js__iSK8eWjp8F_hPKFgRb60-V0D-
Nmtlbrnb_r4MsCxQIQ__d0hXpkRk3jS87HvKh27KLTSNfGC8XT0-ELWorzpwT30__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.js -
HIER_DIRECT/85.91.64.65 text/javascript
1651311823.225     11 192.168.100.137 TCP_MISS/200 4097 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_js/js__exncf12A-fQnkfFIUKO-U-_Ys6DjuuO3FF91EKxDz54__SKpZa9Nh-
NXZL84geNWqncfDMRS23CpA7LLOersk8l8__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.js - HIER_DIRECT/85.91.64.65
text/javascript
1651311823.233     18 192.168.100.137 TCP_MISS/200 18515 GET
http://www.edu.xunta.gal/portal/sites/web/files/advagg_js/js__26Q3JMXY8kwqzwj22_oEGJUcX3_yLAFgVxIwd7XJvVA__OIacvFxO5SVLD
qwzJyWaNPIaBm5ziEOJ64proy983dM__3k6z3hd6djWRfcR78WaGvyE56vxNdXFq9iJyZU7hOQ4.js - HIER_DIRECT/85.91.64.65 text/javascript
1651311823.329    179 192.168.100.137 TCP_MISS/200 33352 GET http://code.jquery.com/jquery-1.10.2.min.js -
HIER_DIRECT/69.16.175.10 application/javascript
1651311823.345     16 192.168.100.137 TCP_MISS/200 15024 GET http://www.edu.xunta.gal/portal/sites/web/files/css/cceu-
negativo.svg - HIER_DIRECT/85.91.64.65 image/svg+xml
```




```
1651311961.167      1 192.168.100.137 TCP_DENIED/403 4217 GET http://www.xunta.gal/ - HIER_NONE/- text/html
```

Configuración de netfilter

Instalar ulogd2 e iptables-persistent

```
ubuntu@squid:~$ sudo apt update
ubuntu@squid:~$ sudo apt install ulogd2 iptables-persistent
```

Activar enrutamiento

```
ubuntu@squid:~$ sudo nano /etc/sysctl.conf
...
net.ipv4.ip_forward=1
...
ubuntu@squid:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
```

Trabajar con estados

```
ubuntu@squid:~$ sudo iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
ubuntu@squid:~$ sudo iptables -A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
ubuntu@squid:~$ sudo iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

Lazo cerrado

```
ubuntu@squid:~$ sudo iptables -A INPUT -i lo -m conntrack --ctstate NEW -j ACCEPT
ubuntu@squid:~$ sudo iptables -A OUTPUT -o lo -m conntrack --ctstate NEW -j ACCEPT
```

Administración fw-gateay por ssh

```
ubuntu@squid:~$ sudo iptables -N SSH
ubuntu@squid:~$ sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW -j SSH
ubuntu@squid:~$ sudo iptables -A SSH -s 192.168.100.1 -j ACCEPT
ubuntu@squid:~$ sudo iptables -A SSH -s 192.168.100.2 -j ACCEPT
ubuntu@squid:~$ sudo iptables -A SSH -s 192.168.100.3 -j ACCEPT
ubuntu@squid:~$ sudo iptables -A SSH -j NFLOG --nflog-prefix "iptables: SSH bloqueo"
ubuntu@squid:~$ sudo iptables -A SSH -j DROP
```

Tráfico DNS (fw-gateway y lan)

```
ubuntu@squid:~$ sudo iptables -N DNS
ubuntu@squid:~$ sudo iptables -A OUTPUT -p udp --dport 53 -m conntrack --ctstate NEW -j DNS
ubuntu@squid:~$ sudo iptables -A DNS -d 8.8.8.8 -j ACCEPT
ubuntu@squid:~$ sudo iptables -A DNS -d 8.8.4.4 -j ACCEPT
ubuntu@squid:~$ sudo iptables -A DNS -j NFLOG --nflog-prefix "iptables: DNS bloqueo"
ubuntu@squid:~$ sudo iptables -A DNS -j DROP
ubuntu@squid:~$ sudo iptables -A FORWARD -p udp --dport 53 -m iprange --src-range 192.168.100.1-192.168.100.162 -m conntrack --ctstate NEW -j DNS
```

SNAT para permitir salida a Internet a equipos LAN (dns, web para equipos pruebas y https para técnicos externos)

```
ubuntu@squid:~$ sudo iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -j SNAT --to-source 192.0.2.250
```

Tráfico hacia proxy estándar (puerto 3128/tcp)

```
ubuntu@squid:~$ sudo iptables -A INPUT -p tcp --dport 3128 -m iprange --src-range 192.168.100.1-192.168.100.150 -m conntrack --ctstate NEW -j ACCEPT
```

Tráfico técnicos externos: proxy transparente

```
ubuntu@squid:~$ sudo iptables -A FORWARD -p tcp --dport 443 -m iprange --src-range 192.168.100.151-192.168.100.160 -m conntrack --ctstate NEW -j ACCEPT
ubuntu@squid:~$ sudo iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -m iprange --src-range 192.168.100.151-192.168.100.160 -j DNAT --to-destination 192.168.100.250:3129
ubuntu@squid:~$ sudo iptables -A INPUT -i eth1 -p tcp --dport 3129 -m iprange --src-range 192.168.100.151-192.168.100.160 -m conntrack --ctstate NEW -j ACCEPT
```

Permitir a squid salir a Internet a buscar las páginas web

```
ubuntu@squid:~$ sudo iptables -A OUTPUT -p tcp -m multiport --dport 80,443 -m conntrack --ctstate NEW -j ACCEPT
```

Tráfico web equipos pruebas directo sin pasar por proxy

```
ubuntu@squid:~$ sudo iptables -A FORWARD -p tcp -m multiport --dports 80,443 -m iprange --src-range 192.168.100.161-192.168.100.162 -m conntrack --ctstate NEW -j ACCEPT
```

No Logging

```
ubuntu@squid:~$ sudo iptables -A INPUT -d 192.168.100.255 -j DROP
ubuntu@squid:~$ sudo iptables -A INPUT -d 192.0.2.255 -j DROP
```

```
ubuntu@squid:~$ sudo iptables -A INPUT -d 255.255.255.255 -j DROP
ubuntu@squid:~$ sudo iptables -A INPUT -d 224.0.0.0/4 -j DROP
```

Log Denied Rule y Clean Up

```
ubuntu@squid:~$ sudo iptables -A INPUT -j NFLOG --nflog-prefix "iptables: CleanUP Rule "
ubuntu@squid:~$ sudo iptables -A OUTPUT -j NFLOG --nflog-prefix "iptables: CleanUP Rule "
ubuntu@squid:~$ sudo iptables -A FORWARD -j NFLOG --nflog-prefix "iptables: CleanUP Rule "
ubuntu@squid:~$ sudo iptables -A INPUT -j DROP
ubuntu@squid:~$ sudo iptables -A OUTPUT -j DROP
ubuntu@squid:~$ sudo iptables -A FORWARD -j DROP
```

Ruleset

```
ubuntu@squid:~$ sudo iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
2    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            ctstate NEW
3    SSH        tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:22 ctstate NEW
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:3128 source IP range
192.168.100.1-192.168.100.150 ctstate NEW
5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:3129 source IP range
192.168.100.151-192.168.100.160 ctstate NEW
6    DROP       all  --  0.0.0.0/0            192.168.100.255
7    DROP       all  --  0.0.0.0/0            192.0.2.255
8    DROP       all  --  0.0.0.0/0            255.255.255.255
9    DROP       all  --  0.0.0.0/0            224.0.0.0/4
10   NFLOG      all  --  0.0.0.0/0            0.0.0.0/0            nflog-prefix  "iptables: CleanUP
Rule "
11   DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
2    DNS        udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53 source IP range
192.168.100.1-192.168.100.162 ctstate NEW
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:443 source IP range
192.168.100.151-192.168.100.160 ctstate NEW
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            multiport dports 80,443 source IP
range 192.168.100.161-192.168.100.162 ctstate NEW
5    NFLOG      all  --  0.0.0.0/0            0.0.0.0/0            nflog-prefix  "iptables: CleanUP
Rule "
6    DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
2    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            ctstate NEW
3    DNS        udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53 ctstate NEW
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            multiport dports 80,443 ctstate NEW
5    NFLOG      all  --  0.0.0.0/0            0.0.0.0/0            nflog-prefix  "iptables: CleanUP
Rule "
6    DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain DNS (2 references)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            8.8.8.8
2    ACCEPT     all  --  0.0.0.0/0            8.8.4.4
3    NFLOG      all  --  0.0.0.0/0            0.0.0.0/0            nflog-prefix  "iptables: DNS
bloqueo"
4    DROP       all  --  0.0.0.0/0            0.0.0.0/0
```

```
Chain SSH (1 references)
num  target     prot opt source               destination
1    ACCEPT     all  --  192.168.100.1        0.0.0.0/0
2    ACCEPT     all  --  192.168.100.2        0.0.0.0/0
3    ACCEPT     all  --  192.168.100.3        0.0.0.0/0
4    NFLOG      all  --  0.0.0.0/0            0.0.0.0/0            nflog-prefix  "iptables: SSH
bloqueo"
5    DROP       all  --  0.0.0.0/0            0.0.0.0/0
ubuntu@squid:~$ sudo iptables -t nat -L -n --line-numbers
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:80 source IP range
192.168.100.151-192.168.100.160 to:192.168.100.250:3129

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    SNAT       all  --  192.168.100.0/24     0.0.0.0/0            to:192.0.2.250
ubuntu@squid:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
ubuntu@squid:~$ sudo cat /etc/iptables/rules.v4
# Generated by iptables-save v1.8.4 on Sun May  1 10:40:36 2022
*nat
:PREROUTING ACCEPT [42:8092]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -i eth1 -p tcp -m tcp --dport 80 -m iprange --src-range 192.168.100.151-192.168.100.160 -
j DNAT --to-destination 192.168.100.250:3129
-A POSTROUTING -s 192.168.100.0/24 -j SNAT --to-source 192.0.2.250
COMMIT
# Completed on Sun May  1 10:40:36 2022
# Generated by iptables-save v1.8.4 on Sun May  1 10:40:36 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:DNS - [0:0]
:SSH - [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j SSH
-A INPUT -p tcp -m tcp --dport 3128 -m iprange --src-range 192.168.100.1-192.168.100.150 -m conntrack
--ctstate NEW -j ACCEPT
-A INPUT -i eth1 -p tcp -m tcp --dport 3129 -m iprange --src-range 192.168.100.151-192.168.100.160 -m
conntrack --ctstate NEW -j ACCEPT
-A INPUT -d 192.168.100.255/32 -j DROP
-A INPUT -d 192.0.2.255/32 -j DROP
-A INPUT -d 255.255.255.255/32 -j DROP
-A INPUT -d 224.0.0.0/4 -j DROP
```

```
-A INPUT -j NFLOG --nflog-prefix  "iptables: CleanUP Rule "
-A INPUT -j DROP
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p udp -m udp --dport 53 -m iprange --src-range 192.168.100.1-192.168.100.162 -m conntrack
--ctstate NEW -j DNS
-A FORWARD -p tcp -m tcp --dport 443 -m iprange --src-range 192.168.100.151-192.168.100.160 -m
conntrack --ctstate NEW -j ACCEPT
-A FORWARD -p tcp -m multiport --dports 80,443 -m iprange --src-range 192.168.100.161-192.168.100.162 -
m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -j NFLOG --nflog-prefix  "iptables: CleanUP Rule "
-A FORWARD -j DROP
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -m conntrack --ctstate NEW -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -m conntrack --ctstate NEW -j DNS
-A OUTPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate NEW -j ACCEPT
-A OUTPUT -j NFLOG --nflog-prefix  "iptables: CleanUP Rule "
-A OUTPUT -j DROP
-A DNS -d 8.8.8.8/32 -j ACCEPT
-A DNS -d 8.8.4.4/32 -j ACCEPT
-A DNS -j NFLOG --nflog-prefix  "iptables: DNS bloqueo"
-A DNS -j DROP
-A SSH -s 192.168.100.1/32 -j ACCEPT
-A SSH -s 192.168.100.2/32 -j ACCEPT
-A SSH -s 192.168.100.3/32 -j ACCEPT
-A SSH -j NFLOG --nflog-prefix  "iptables: SSH bloqueo"
-A SSH -j DROP
COMMIT
# Completed on Sun May  1 10:40:36 2022
```