

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Copiar la estructura de sota, tantes vegades com sigui necessari

Lliura una captura amb el contingut de l'arxiu squid.conf on es mostrin les línies modificades (amb hores diferents a l'actual).

```

GNU nano 6.2 /etc/squid/squid.conf
acl Safe_ports port 280      # http-mgmt
acl Safe_ports port 488      # gss-http
acl Safe_ports port 591      # filemaker
acl Safe_ports port 777      # multiling http

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

http_access allow localhost manager
http_access deny manager

include /etc/squid/conf.d/*.conf

acl dominis-bloquejats dstdomain "/etc/squid/blacksites"
acl expressions-denegades url_regex "/etc/squid/blackwords"
acl arxius urlpath_regex "/etc/squid/blackfiles"
acl algunesHores time MWHF 12:00-15:00

#http_access deny arxius
#http_access deny expressions-denegades
http_access deny dominis-bloquejats algunesHores
http_access allow dominis-bloquejats

http_access allow localnet

http_access deny all


http_access allow localhost

http_port 3128

coredump_dir /var/spool/squid

dj. de febr. 06 13:00:07 romerorx@SYN:~$ _

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura del navegador del client on no es pot accedir a la web
(www.google.com)

```

-----
The following error was encountered while trying to retrieve the URL: http://google.com/
Access Denied.

Access control configuration prevents your request from being allowed at this time. Please
contact your service provider if you feel this is incorrect.

Your cache administrator is webmaster.
-----

Generated Thu, 06 Feb 2025 12:54:47 GMT by SYN (squid/5.9)

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.

Exiting via interrupt: 2
jue feb 06 12:54:51 zulema@PC2:~$

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura amb el contingut de l'arxiu squid.conf on es mostrin les línies modificades (amb hores incloent l'actual).

```

Archivo  Màquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2                                     /etc/squid/squid.conf
acl Safe_ports port 210                          # wais
acl Safe_ports port 1025-65535                   # unregistered ports
acl Safe_ports port 280                          # http-mgmt
acl Safe_ports port 488                          # gss-http
acl Safe_ports port 591                          # filemaker
acl Safe_ports port 777                          # multiling http

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

http_access allow localhost manager
http_access deny manager

include /etc/squid/conf.d/*.conf

acl dominis-bloquejats dstdomain "/etc/squid/blacksites"
acl expressions-denegades url_regex "/etc/squid/blackwords"
acl arxius urlpath_regex "/etc/squid/blackfiles"
acl algunesHores time MWHF 12:00-15:00

#http_access deny arxius
#http_access deny expressions-denegades
http_access allow dominis-bloquejats algunesHores
http_access deny dominis-bloquejats

http_access allow localnet

http_access deny all

http_access allow localhost

http_port 3128

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura del navegador del client on si es pot accedir a la web
(www.google.com)

```

Búsqueda Imágenes Maps Play YouTube Noticias Gmail Drive Más »
Historial web | Ajustes | Iniciar sesión

Google

-----
Buscar con Google  Voy a tener suerte  Búsqueda avanzada


Ofrecido por Google en: català galego euskara English

Publicidad  Soluciones Empresariales  Todo acerca de Google  Google.es

© 2025 - Privacidad - Términos

(NORMAL LINK) Use right-arrow or <return> to activate.
Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura de l'arxiu squid.conf on es mostri l'anterior configuració

```

GNU nano 6.2 /etc/squid/squid.conf
http_access deny manager

include /etc/squid/conf.d/*.conf

#acl dominis-bloquejats dstdomain "/etc/squid/blacksites"
#acl expressions-denegades url_regex "/etc/squid/blackwords"
#acl arxius urlpath_regex "/etc/squid/blackfiles"
#acl algunesHores time MWHF 12:00-15:00
acl ubuntuOS src 172.30.1.10

#http_access deny arxius
#http_access deny expressions-denegades
#http_access allow dominis-bloquejats algunesHores
#http_access deny dominis-bloquejats

http_access allow localnet !ubuntuOS

http_access deny all

#http_access allow localhost

#http_port 3128

coredump_dir /var/spool/squid

refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/(Release|\.pgp)$ 0 0% 0 refresh-ims
refresh_pattern \/(InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims

dj. de febr. 06 13:16:20 romerorx@SYN:~$ sudo nano /etc/squid/squid.conf_

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura del navegador del client mostrant que no pot accedir a cap pàgina. P.e www.duckduckgo.com (pàgina no filtrada anteriorment)

```

ERROR: The requested URL could not be retrieved

ERROR

The requested URL could not be retrieved

-----
The following error was encountered while trying to retrieve the URL: http://google.com/

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please
contact your service provider if you feel this is incorrect.

Your cache administrator is webmaster.
-----

Generated Thu, 06 Feb 2025 13:26:13 GMT by SYN (squid/5.9)

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura amb la modificació feta a l'arxiu squid.conf

```

GNU nano 6.2 /etc/squid/squid.conf

#acl dominis-bloquejats dstdomain "/etc/squid/blacksites"
#acl expressions-denegades url_regex "/etc/squid/blackwords"
#acl arxius urlpath_regex "/etc/squid/blackfiles"
#acl algunesHores time MWHF 12:00-15:00
acl ubuntuOS src 172.30.1.10

#http_access deny arxius
#http_access deny expressions-denegades
#http_access allow dominis-bloquejats algunesHores
#http_access deny dominis-bloquejats

http_access allow localnet !ubuntuOS

http_access deny all

#http_access allow localhost

http_port 3128

coredump_dir /var/spool/squid

refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0        0%        0
refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/(Release(|\.pgp)$ 0 0% 0 refresh-ims
refresh_pattern \/(InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .              0        20%     4320

error_directory /usr/share/squid/errors/Spanish

dj. de febr. 06 13:27:32 romerom@SYN:~$

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura del navegador del client on es mostra el missatge d'error (caldrà que verifiquis les ACLs per assegurar-te que llençarà l'error)

```

ERROR: El URL solicitado no se ha podido conseguir
ERROR
El URL solicitado no se ha podido conseguir
-----
Se encontró el siguiente error al intentar recuperar la dirección URL: http://google.com/
Acceso Denegado
La configuración de control de acceso evita que su solicitud sea permitida en este momento.
Por favor, póngase en contacto con su proveedor de servicios si cree que esto es
incorrecto.
Su administrador del caché es webmaster.
-----
Generado Thu, 06 Feb 2025 13:28:39 GMT por SYN (squid/5.9)

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list

```


	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

Lliura una captura de l'execució de cada tipus de comanda que has vist en aquest apartat (total 5). Recorda que això es realitza al servidor!

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

```

dj. de febr. 06 13:31:09 romeror@SYN:~$ sudo tail -f /var/log/squid/access.log
1738846943.917      0 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738846951.430      0 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738847027.332      1 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738847135.767     272 172.30.1.10 TCP_MISS/301 878 GET http://google.com/ - HIER_DIRECT/142.250.184.
174 text/html
1738847138.855     1066 172.30.1.10 TCP_MISS/200 3100 GET http://www.google.com/ - HIER_DIRECT/216.239
.38.120 text/html
1738847874.437     3686 172.30.1.10 TCP_MISS_ABORTED/000 0 GET http://duckduckgo.com/ - HIER_DIRECT/52
.142.124.215 -
1738847889.101      1 172.30.1.10 TCP_MEM_HIT/301 886 GET http://google.com/ - HIER_NONE/- text/html
1738847891.428     313 172.30.1.10 TCP_MISS/200 3102 GET http://www.google.com/ - HIER_DIRECT/216.58.
215.132 text/html
1738848373.426      9 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738848519.436      0 172.30.1.10 TCP_DENIED/403 3927 GET http://google.com/ - HIER_NONE/- text/html

```

```

dj. de febr. 06 13:32:06 romeror@SYN:~$ sudo tail -n 20 /var/log/squid/access.log
1738845016.784     335 172.30.1.10 TCP_MISS/403 5381 GET http://www.google.com.com/ - HIER_DIRECT/104
.26.4.148 text/html
1738845703.054     172 172.30.1.10 TCP_MISS/301 878 GET http://google.com/ - HIER_DIRECT/142.250.184.
174 text/html
1738845706.133     1066 172.30.1.10 TCP_MISS/200 3103 GET http://www.google.com/ - HIER_DIRECT/216.239
.38.120 text/html
1738845814.837     363 172.30.1.10 TCP_MISS/301 876 GET http://google.es/ - HIER_DIRECT/142.250.184.1
63 text/html
1738845820.115      0 172.30.1.10 TCP_MEM_HIT/301 886 GET http://google.com/ - HIER_NONE/- text/html
1738845979.268     125 172.30.1.10 TCP_MISS/301 878 GET http://google.com/ - HIER_DIRECT/142.250.184.
174 text/html
1738846487.574      9 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738846943.917      0 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738846951.430      0 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738847027.332      1 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738847135.767     272 172.30.1.10 TCP_MISS/301 878 GET http://google.com/ - HIER_DIRECT/142.250.184.
174 text/html
1738847138.855     1066 172.30.1.10 TCP_MISS/200 3100 GET http://www.google.com/ - HIER_DIRECT/216.239
.38.120 text/html
1738847874.437     3686 172.30.1.10 TCP_MISS_ABORTED/000 0 GET http://duckduckgo.com/ - HIER_DIRECT/52
.142.124.215 -
1738847889.101      1 172.30.1.10 TCP_MEM_HIT/301 886 GET http://google.com/ - HIER_NONE/- text/html
1738847891.428     313 172.30.1.10 TCP_MISS/200 3102 GET http://www.google.com/ - HIER_DIRECT/216.58.
215.132 text/html
1738848373.426      9 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738848519.436      0 172.30.1.10 TCP_DENIED/403 3927 GET http://google.com/ - HIER_NONE/- text/html
dj. de febr. 06 13:32:10 romeror@SYN:~$

```

	Institut Antoni Ballester Sistemes Microinformàtics i Xarxes. M7 - Serveis de Xarxa	«PROXY 3»	«Zulema Romero»	Curs: 24-25
---	---	-----------	-----------------	-------------

```

dj. de febr. 06 13:32:10 romerox@SYN:~$ sudo grep '172.30.1.10' /var/log/squid/access.log
1738845016.784      335 172.30.1.10 TCP_MISS/403 5381 GET http://www.google.com.com/ - HIER_DIRECT/104
.26.4.148 text/html
1738845703.054      172 172.30.1.10 TCP_MISS/301 878 GET http://google.com/ - HIER_DIRECT/142.250.184.
174 text/html
1738845706.133     1066 172.30.1.10 TCP_MISS/200 3103 GET http://www.google.com/ - HIER_DIRECT/216.239
.38.120 text/html
1738845814.837      363 172.30.1.10 TCP_MISS/301 876 GET http://google.es/ - HIER_DIRECT/142.250.184.1
63 text/html
1738845820.115        0 172.30.1.10 TCP_MEM_HIT/301 886 GET http://google.com/ - HIER_NONE/- text/html
1738845979.268     125 172.30.1.10 TCP_MISS/301 878 GET http://google.com/ - HIER_DIRECT/142.250.184.
174 text/html
1738846487.574        9 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738846943.917        0 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738846951.430        0 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738847027.332        1 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738847135.767     272 172.30.1.10 TCP_MISS/301 878 GET http://google.com/ - HIER_DIRECT/142.250.184.
174 text/html
1738847138.855     1066 172.30.1.10 TCP_MISS/200 3100 GET http://www.google.com/ - HIER_DIRECT/216.239
.38.120 text/html
1738847874.437     3686 172.30.1.10 TCP_MISS_ABORTED/000 0 GET http://duckduckgo.com/ - HIER_DIRECT/52
.142.124.215 -
1738847889.101        1 172.30.1.10 TCP_MEM_HIT/301 886 GET http://google.com/ - HIER_NONE/- text/html
1738847891.428     313 172.30.1.10 TCP_MISS/200 3102 GET http://www.google.com/ - HIER_DIRECT/216.58.
215.132 text/html
1738848373.426        9 172.30.1.10 TCP_DENIED/403 3918 GET http://google.com/ - HIER_NONE/- text/html
1738848519.436        0 172.30.1.10 TCP_DENIED/403 3927 GET http://google.com/ - HIER_NONE/- text/html
dj. de febr. 06 13:32:45 romerox@SYN:~$

```

```

dj. de febr. 06 13:35:15 romerox@SYN:~$ sudo awk '{print $3}' /var/log/squid/access.log | sort | uni
q -c | sort -nr
17 172.30.1.10
dj. de febr. 06 13:36:18 romerox@SYN:~$

```

```

dj. de febr. 06 13:36:18 romerox@SYN:~$ sudo awk '{print $7}' /var/log/squid/access.log | sort | uni
q -c | sort -nr | head -10
11 http://google.com/
3 http://www.google.com/
1 http://www.google.com.com/
1 http://google.es/
1 http://duckduckgo.com/
dj. de febr. 06 13:37:25 romerox@SYN:~$ _

```