

Restricións nas conexións a través do proxy

Sumario

- 1 Restricións das conexións en Squid
- 2 Restricións segundo o dominio de destino
- 3 Restricións segundo o tipo de ficheiro
- 4 Restricións segundo a hora da conexión

Restricións das conexións en Squid

- Squid é un servidor proxy moi completo, e abordar con profundidade as distintas opcións de configuración que permite excede con moito os obxectivos deste curso.
- Por iso, o que imos facer é ilustrar unha configuración básica das opcións de filtrado máis comúns, para amosar así as posibilidades máis relevantes que ofrece o servizo de proxy que non serían posibles por medio do enrutamento.

Restricións segundo o dominio de destino

- Como o servizo de proxy opera no nivel de aplicación, pode ler a cabeceira HTTP para ver a URL de destino da conexión. Isto permite a posibilidade de establecer restricións en función do dominio ao que o cliente se quere conectar:

- Restricións por dominio de destino



The screenshot shows a web interface for configuring Squid. It features a table with the following rows: 'Safe_ports' (Puerto URL), 'Safe_ports' (Puerto URL), 'CONNECT' (Método de Petición), and 'LAN' (Dirección de Cliente). Below the table, there is a button labeled 'Crear nueva ACL' and a dropdown menu labeled 'Nombre de Máquina de Servidor Web'. A mouse cursor is pointing at the 'Crear nueva ACL' button. At the bottom, there is a link labeled 'Regresar a índice squid'.

Na pestana de *Listas de control de acceso* da configuración do *Control de acceso* creamos unha nova ACL de tipo **Nome de máquina de servidor web**.




The screenshot shows the 'Crear ACL' form in the Squid configuration interface. The form has the following fields: 'Nombre ACL' (Facebook), 'Dominios' (www.facebook.com), and 'URL de Fallo'. Below these fields, there is a section for 'Almacenar ACL en archivo' with two radio buttons: 'Configuración Squid' (selected) and 'Separate file'. There is also a checkbox labeled '¿Usar sólo contenidos existentes del archivo?'. At the bottom, there is a 'Guardar' button and two links: 'Regresar a Lista ACL' and 'Regresar a índice'.


Podemos introducir os datos que se ven na imaxe para filtrar o dominio *www.facebook.com*.

- 

Unha vez creada a ACL imos a crear unha restrición sobre a mesma.

- 

Engadimos unha nova restrición.

- 

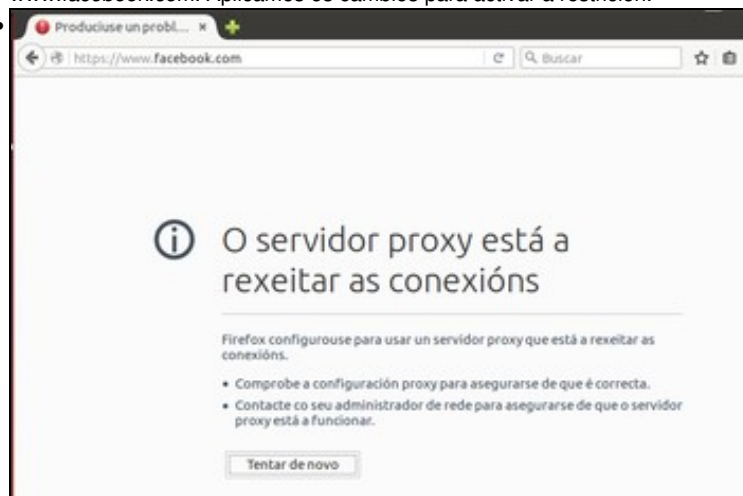
Neste caso, imos denegar as conexións ao dominio *www.facebook.com* seleccionando a ACL.



Vemos a restrición creada. Debemos colocala no lugar adecuado da táboa para que se execute.



Por exemplo, deixándoa na posición da imaxe, conseguiremos que os equipos da LAN poidan acceder a calquera dominio excepto *www.facebook.com*. Aplicamos os cambios para activar a restrición.



Podemos comprobar dende un equipo cliente que non podemos conectarnos a *www.facebook.com*...



pero si a calquera outro dominio.

- 

Imos facer outra proba, creando unha ACL asociada ao dominio `.edu.xunta.es`. Este dominio afectaría a todos os servidores para os que o seu nome acabase por este nome de dominio.

- 

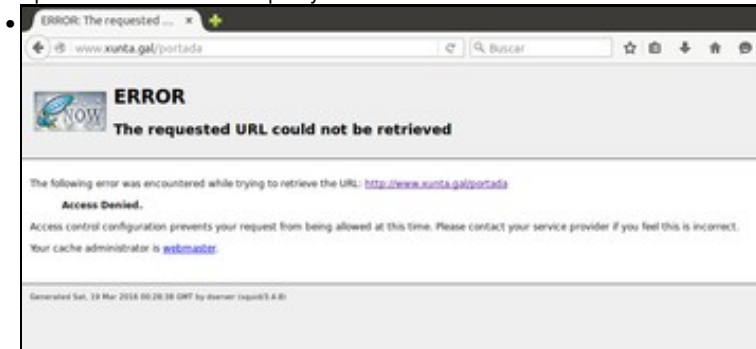
Na táboa de restricións do proxy, picamos sobre a restrición que permite o acceso a todos os equipos da LAN para editar a configuración desta restrición.

- 

Seleccionamos na lista de **Coincidir con ACLs** a ACL que acabamos de crear ademais da de LAN que xa estaba seleccionada. Vemos deste xeito que unha restrición pode asociarse a varias ACLs, e só encaixarán con ela as conexións que coincidan con todas esas ACLs. Por exemplo, agora só se permitirá a conexión dende a LAN ao dominio **.edu.xunta.es**



Aplicamos os cambios no proxy...



e podemos comprobar nun equipo cliente da LAN que non se permite o acceso a unha páxina dun dominio distinto a **edu.xunta.es**...



pero si ao portal da consellería.

Restricións segundo o tipo de ficheiro

- Outra opción que permite Squid é filtrar unha conexión polo **tipo MIME** do documento que devolve como resposta o servidor web. O tipo do documento vai indicado na cabeceira da resposta do HTTP.
- Existe una gran variedade de **tipos MIME dispoñibles**, para ficheiros de audio, imaxes, documentos PDF, vídeos, etc.
- A continuación imos mostrar un exemplo no que denegaremos a descarga de documentos PDF:
- Restricións segundo o tipo de ficheiro en Squid

- | | |
|-----------------|-----------------------------------|
| CONNECT | Método de Petición |
| LAN | Dirección de Cliente |
| Facebook | Nombre de Máquina de Servidor Web |
| Edu_Xunta | Nombre de Máquina de Servidor Web |
| Crear nueva ACL | Tipo MIME de Respuesta |

[Regresar a índice squid](#)

Creamos unha ACL de tipo **Tipo MIME de Respuesta**.

- Índice de Módulo

Aplicar Cambios

Para Squid

Crear ACL

Tipo MIME de Respuesta ACL

Nombre ACL

PDFs

Tipo MIME de Respuesta

application/pdf

URL de Fallo

Almacenar ACL en archivo

☒ Configuración Squid
 ☐ Separate file

☐ ¿Usar sólo contenidos existentes del archivo?

Guardar

[Regresar a Lista ACL](#) | [Regresar a índice](#)

Poñemos un nome para a ACL e como **Tipo MIME de resposta** introducimos o tipo que se corresponde cos documentos PDF, que sería **application/pdf**.

- Índice de Módulo

Aplicar Cambios

Para Squid

Control de Acceso

[Ayuda...](#)
[Listas de control de Acceso](#)
[Restricciones Proxy](#)
[Restricciones ICP](#)
[Programas externos ACL](#)
[Reply proxy restrictions](#)

Añadir restricción proxy

Acción	ACLs	Mover
<input type="checkbox"/> Denegar	!Safe_ports	↓↑
<input type="checkbox"/> Denegar	CONNECT !SSL_ports	↓↑
<input type="checkbox"/> Permitir	localhost manager	↓↑
<input type="checkbox"/> Denegar	manager	↓↑
<input type="checkbox"/> Permitir	localhost	↓↑
<input type="checkbox"/> Denegar	Facebook	↓↑
<input type="checkbox"/> Permitir	LAN	↓↑
<input type="checkbox"/> Denegar	all	↑

Añadir restricción proxy

Delete Selected Restrictions

[Regresar a índice squid](#)

Coa ACL creada, imos á pestana de restricións proxy de resposta, xa que neste caso a restrición ímola facer por unha condición na resposta HTTP do servidor web ao que se conecta o cliente.

- Índice de Módulo

Aplicar Cambios

Para Squid

Control de Acceso

[Ayuda...](#)
[Listas de control de Acceso](#)
[Restricciones Proxy](#)
[Restricciones ICP](#)
[Programas externos ACL](#)
[Reply proxy restrictions](#)

No proxy reply restrictions defined

Añadir restricción proxy

[Regresar a índice squid](#)

Vemos que neste apartado non hai ningunha restrición creada. Imos crear unha nova.

Indice de Módulo

Create Proxy Reply Restriction

Proxy Reply Restriction

Acción ☐ Permitir ☒ Denegar

Coincidir con ACLs

- all
- SSL_ports
- Safe_ports
- CONNECT
- LAN
- Facebook
- Edu_Xunta
- PDFs

No coincidir con ACLs

- all
- SSL_ports
- Safe_ports
- CONNECT
- LAN
- Facebook
- Edu_Xunta
- PDFs

Salvar

[Regresar a Lista de ACL](#) | [Regresar a indice](#)

O que facemos na restrición é denegar as conexións que coincidan coa ACL que acabamos de crear.

Indice de Módulo

Control de Acceso

Aplicar Cambios
Parar Squid

Listas de control de Acceso: Restricciones Proxy Restricciones ICP Programas externos ACL Reply proxy restrictions

Añadir restricción proxy

Acción	ACLs	Mover
<input type="checkbox"/> Denegar	PDFs	

Añadir restricción proxy

Delete Selected Restrictions

[Regresar a índice squid](#)

Vemos na imaxe a restrición creada, e aplicamos os cambios para activala.

www.xunta.es/diario-oficial-galicia/mostrarcContenido-da/macha

DOG | Diario Oficial de Galicia

XUNTA DE GALICIA

Consulta de DOG - Datos Nº 54

Consulta de DOG

Nº 54

Viernes, 18 de marzo de 2016

I. Disposiciones xerais

II. Autoridades e persoal

- 41. Consellos
- 42. Nomeamentos
- 43. Substitucións

III. Outras disposicións

IV. Disposicións e concellos

V. Administración de xestión

VI. Anexos

- 44. Administracións autonómicas
- 45. Administración local
- 46. Outros anexos

[Servizo de Xestión DOG](#)

www.xunta.es/dog/Publicados/2016/20160318/indice54_gl.pdf

Para comprobar o efecto da restrición, dende un equipo cliente imos intentar descargar a versión en PDF dun DOG.

www.xunta.es/dog/Publicados/2016/20160318/indice54_gl.pdf

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://www.xunta.es/dog/Publicados/2016/20160318/indice54_gl.pdf

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](#).

Downloaded Sat, 19-Mar-2016 09:34:10 GMT by 80.100.1.10 (ip:80.100.1.10)

Na imaxe podemos ver a mensaxe que obteremos denegando o acceso a este documento.

Restricións segundo a hora da conexión

- Remataremos este apartado vendo como podemos restrinxir no proxy o acceso a Internet segundo a hora na que se produza as conexións:
- Restricións segundo a hora en Squid

Control de Acceso

Índice de Módulo | Ayuda | Aplicar Cambios | Pasar Squid

Listas de control de Acceso | Restricciones Proxy | Restricciones ICP | Programas externos ACL | Reply proxy restrictions

Nombre	Tipo	Coincidiendo con...
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	581
Safe_ports	Puerto URL	777
CONNECT	Método de Petición	CONNECT
LAN	Dirección de Cliente	172.16.0.0/16
Facebook	Nombre de Máquina de Servidor Web	www.facebook.com
Edu_Xunta	Nombre de Máquina de Servidor Web	edu.xunta.es
PDFs	Tipo MIME de Respuesta	application/pdf

Crear nueva ACL | Fecha y Hora

Regresar a índice squid

Creamos unha ACL de tipo de **Fecha e hora**.

Crear ACL

Índice de Módulo | Aplicar Cambios | Pasar Squid

Fecha y Hora ACL

Nombre ACL:

Días de la Semana: ☒ Todos ☐ Seleccionado...

Horas del Día: ☐ Todos a

URL de Fallo:

Almacenar ACL en archivo: ☒ Configuración Squid ☐ Separate file

☐ Usar sólo contenidos existentes del archivo?

Guardar

Regresar a Lista ACL | Regresar a índice

Poñemos un nome a ACL e o horario no que neste caso imos restrinxir o acceso a Internet.

Control de Acceso

Índice de Módulo | Ayuda | Aplicar Cambios | Pasar Squid

Listas de control de Acceso | Restricciones Proxy | Restricciones ICP | Programas externos ACL | Reply proxy restrictions

Nombre	Tipo	Coincidiendo con...
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	581
Safe_ports	Puerto URL	777
CONNECT	Método de Petición	CONNECT
LAN	Dirección de Cliente	172.16.0.0/16
Facebook	Nombre de Máquina de Servidor Web	www.facebook.com
Edu_Xunta	Nombre de Máquina de Servidor Web	edu.xunta.es
PDFs	Tipo MIME de Respuesta	application/pdf
Horario	Fecha y Hora	1:57-3:00

Crear nueva ACL | Autenticación Externa

Regresar a índice squid

Podemos ver na listaxe a ACL creada. Iremos á pestana de **Restricións proxy** para definir a restrición sobre ela.

Indice de Módulo

Crear Restricción de Proxy

Restricción de Proxy

Acción ☐ Permitir ☒ Denegar

Coincidir con ACLs

all (1)
SSL_ports (1)
Safe_ports (1)
CONNECT (1)
LAN (1)
Facebook (1)
Edu_Xunta (0)
PDFs (0)
Horario (0)

No coincidir con ACLs

all (1)
SSL_ports (1)
Safe_ports (1)
CONNECT (1)
LAN (1)
Facebook (1)
Edu_Xunta (0)
PDFs (0)
Horario (0)

[Regresar a Lista de ACL](#) | [Regresar a indice](#)

Creamos a restrición que denega as conexións que se produzan nese horario.

Indice de Módulo

Control de Acceso

Ayuda...

[Listas de control de Acceso](#) |
[Restricciones Proxy](#) |
[Restricciones ICP](#) |
[Programas externos ACL](#) |
[Reply proxy restrictions](#)

Añadir restricción proxy

Acción	ACLs	Mover
<input type="checkbox"/> Denegar	!Safe_ports	↓
<input type="checkbox"/> Denegar	CONNECT !SSL_ports	↓ ↑
<input type="checkbox"/> Permitir	localhost manager	↓ ↑
<input type="checkbox"/> Denegar	manager	↓ ↑
<input type="checkbox"/> Permitir	localhost	↓ ↑
<input type="checkbox"/> Denegar	Facebook	↓ ↑
<input type="checkbox"/> Denegar	Horario	↓ ↑
<input type="checkbox"/> Permitir	LAN	↓ ↑
<input type="checkbox"/> Denegar	all	↑

Añadir restricción proxy

[Regresar a indice squid](#)

E tras colocar a restrición na orde que corresponde na listaxe de restricións, aplicamos os cambios para activala.

www.xunta.es/diario-oficial-galicia/mostrarContenido.do?pagina

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://www.xunta.es/diario-oficial-galicia/mostrarContenido.do?>

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 Sat, 19 Mar 2016 00:57:04 GMT by server (squid/3.4.8)

Na imaxe podemos ver o resultado dun cliente que intenta conectarse no horario restrinxido.