

# Gestió del Servidor de Comunicacions Linkat

Revisió: Juny 2012 – 001GP  
[XTEC – Atenció a l'usuari](#)  
Guies de programari

El Servidor de Comunicacions és un ordinador destinat a gestionar i filtrar l'accés a Internet d'una xarxa local. El programari proxy (intermediari en anglès) instal·lat a l'ordinador intercepta la navegació dels clients de la xarxa per pàgines web. L'objectiu és augmentar la seguretat i el rendiment del tràfic de la xarxa.

## Índex

<b>1. Introducció .....</b>	<b>2</b>
1.1. Conceptes previs .....	2
1.2. L'eina Webim.....	3
<b>2. Gestió de l'ample de banda (Servidor Proxy Squid) .....</b>	<b>4</b>
2.1. Limitació d'ample de banda a pàgines web (Control d'Accés).....	4
2.2. Visualització de les pàgines visitades (Anàlisi de Registres Calamaris).....	6
2.3. Neteja i Reconstrucció del Cau.....	7
<b>3. Gestió del filtratge de continguts (Squidguard) .....</b>	<b>8</b>
3.1. Llistes negres genèriques (blacklists) .....	10
3.2. Afegir pàgines a la llista blanca de centre .....	11
3.3. Afegir pàgines a la llista negra de centre .....	12
<b>4. Altres informacions d'interès .....</b>	<b>13</b>
4.1. Usuaris.....	13
4.2. Còpies de seguretat.....	13
4.3. Servei de gestió remota.....	14
4.4. Recuperació a l'estat anterior .....	14

## 1. Introducció

### 1.1. Conceptes previs

El servidor de comunicacions és un ordinador que incorpora un programari que permet reduir el trànsit d'una xarxa local cap a Internet i gestionar l'accés dels usuaris/àries. Les funcions i serveis que afecten a tots els equips de la xarxa local que utilitzen aquest servidor per accedir a Internet més significatius són:

- Servidor intermediari (Proxy Cache - Squid) - Emmagatzema les pàgines web que visiten els equips de la xarxa i les desa, en un directori local del servidor. Evita transferències idèntiques d'informació entre servidors. L'objectiu és millorar la velocitat d'accés dels clients. Exemple: quan hi ha 10 clients que accedeixen a una pàgina web, el primer la descarrega d'Internet, i la resta la descarreguen del directori local.
- Control d'*ample de Banda*\* (Control d'accés - Squid) - Permet limitar l'ample de banda d'algunes pàgines web. Serveix perquè algunes pàgines web no col·lapsin el cap dalt de la línia. Exemple: les pàgines web com youtube.com i video.google.com tenen limitat l'ample de banda a 1 MB/s.
- Control de pàgines web visitades (Anàlisi de Registres Calamaris - Squid) - Mostra les pàgines web més visitades del centre i les que més ample de banda consumeixen. Exemple: la pàgina web youtube té poques visites i un alt percentatge de consum d'ample de banda.
- Llistes negres (Blacklists - SquidGuard) – Denega l'accés a un llistat de pàgines web de contingut inapropiat. El centre pot incloure pàgines web a aquest llistat. Exemple: les pàgines web com redtube.com i hackers.com ja estan bloquejades per defecte, el centre pot incloure tuenti.com o facebook.com.
- Llistes blanques (SquidGuard) – Assegura l'accés a un llistat de pàgines web. El centre pot incloure pàgines web a aquest llistat. Exemple: en el llistat de pàgines blanques es troben youtube.com i vimeo.com.

\* *L'ample de banda és la quantitat de informació o de dades que es pot transmetre per una connexió de xarxa en un període de temps. S'indica en bits per segons (bps), kilobits per segons (Kbps), o megabits per segons (Mbps).*

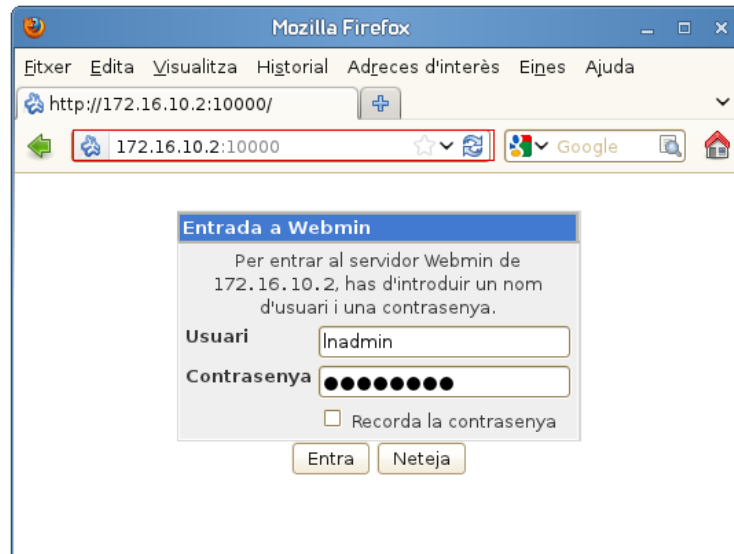
La instal·lació s'ha realitzat en un dels ordinadors preestablerts amb el SO linkat 11.4.

## 1.2. L'eina Webmin

L'eina **Webmin** permet gestionar els recursos del Servidor de Comunicacions, des de qualsevol ordinador del centre, a través d'un navegador web (exemple: Mozilla Firefox, Google Chrome, IE, ...)

✓ Per accedir a l'eina **Webim**, obriu un navegador web i escriviu l'adreça <http://172.16.10.2:10000>.

El responsable d'informàtica del centre disposa de l'usuari "Inadmin" per gestionar el servidor de comunicacions. La contrasenya d'aquest usuari es defineix durant la instal·lació del Servidor.





La pàgina principal de l'eina **Webmin** mostra, a la part central, la informació general del sistema: ús de la memòria virtual, ús de la CPU, espai en disc, ...


A la part esquerra de la pàgina es troben els mòduls que es poden configurar: **Servidor Proxy Squid** i **Squidguard**.

Identificació: Inadmin ← *Usuari d'entrada al webmin*

- ☑ Sistema
- ☑ Servidors
- ☑ Mòduls No utilitzats

Busca:

 Informació del Sistema  
 Surt



← *funcions disponibles*

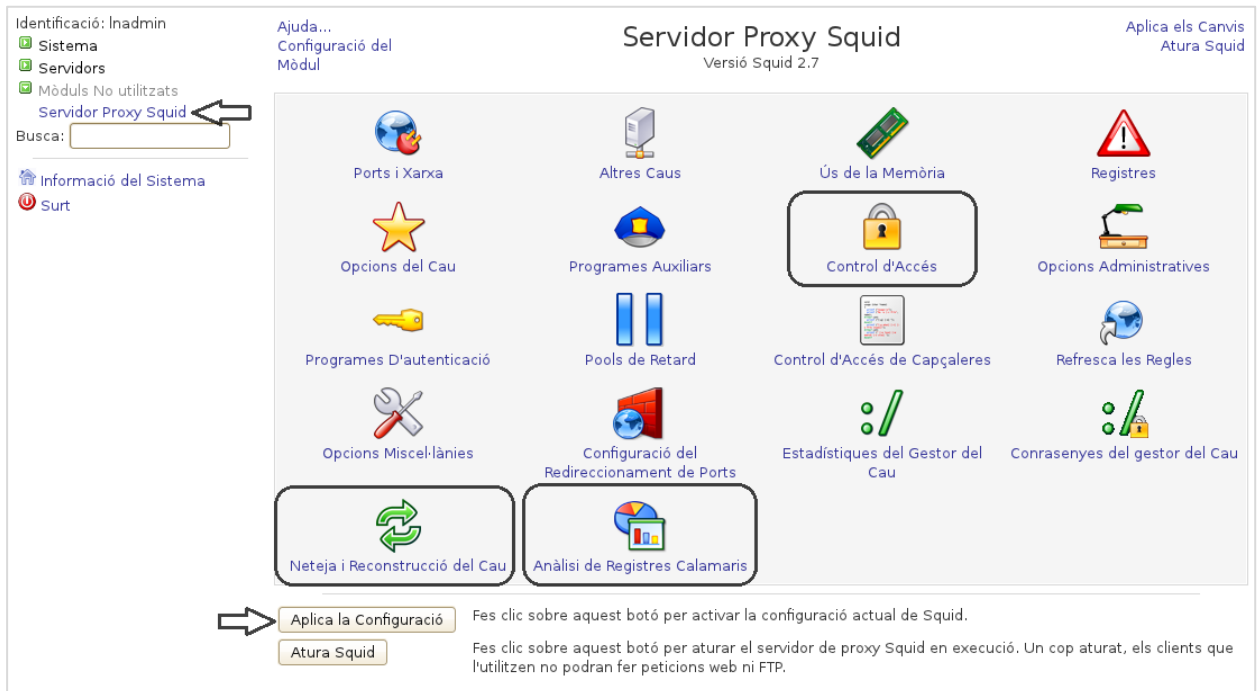
<b>Nom de host del sistema</b>	servidor-comunicacions
<b>Sistema operatiu</b>	SuSE Linux 11.4
<b>Versió Webmin</b>	1.570
<b>Hora del sistema</b>	Fri Jun 8 08:38:37 2012
<b>Nucli i CPU</b>	Linux 2.6.37.6-0.11-desktop a i686
<b>Informació del processador</b>	Pentium(R) Dual-Core CPU E6500 @ 2.93GHz, 2 nuclis
<b>En execució durant</b>	0 hores, 18 minuts
<b>Processos en execució</b>	111
<b>Càrrega mitjana de la CPU</b>	0.06 (1 min) 0.09 (5 mins) 0.07 (15 mins)
<b>Ús de la CPU</b>	0% usuari, 0% nucli, 0% E/S, 100% desocupada
<b>Memòria real</b>	1.88 GB total, 215.24 MB utilitzat
<b>Memòria virtual</b>	4 GB total, 0 bytes utilitzat
<b>Espai local en disc</b>	73.82 GB total, 3.43 GB utilitzat

*Informació del sistema* →

## 2. Gestió de l'ample de banda (Servidor Proxy Squid)

El mòdul **Servidor Proxy Squid** facilita la gestió de l'ample de banda de les connexions a internet. Ofereix les opcions següents:

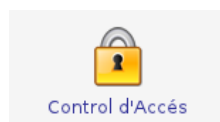
- Definició de les pàgines web on s'estableix el límit d'ample de banda. (mòdul **Control d'Accés**).
- Visualització de les pàgines web visitades i l'ample de banda consumit (mòdul **Anàlisi de Registres Calamaris**).
- Neteja de la memòria cau del servei proxy (mòdul **Neteja i Reconstrucció del Cau**).



### 2.1. Limitació d'ample de banda a pàgines web (Control d'Accés)

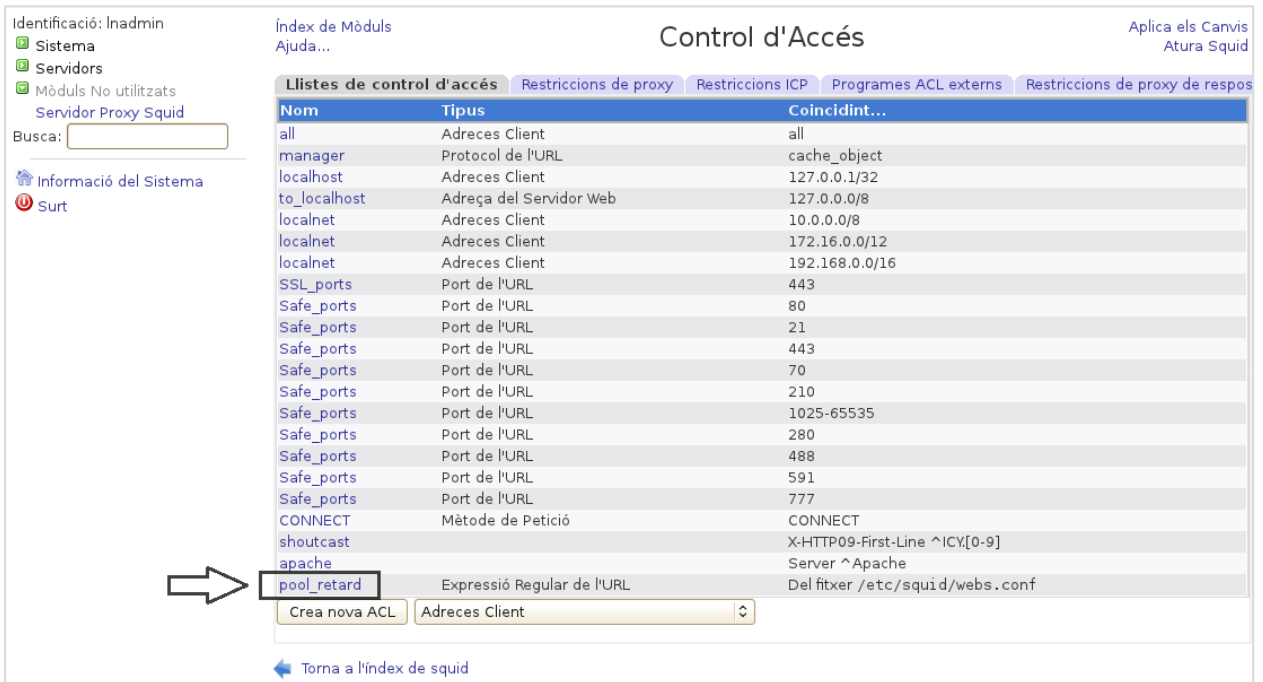
El mòdul de **Control d'accés** estableix les pàgines web que tenen limitat l'ample de banda, aquest límit pot servir per evitar el col·lapse de la línia del centre. Les pàgines web que més consum d'ample de banda requereixen són les que ofereixen vídeo en línia, com ara Youtube.

- ✓ Per accedir al mòdul cliqueu sobre la icona **Control d'Accés**.



La pàgina **Control d'Accés** mostra les llistes de control.

- ✓ Cliqueu sobre **pool\_retard** de la columna **Nom** per accedir a la pàgina **Edició d'ACL**.



Identificació: Inadmin Aplica els Canvis  
Atura Squid

Sistema Índex de Mòduls  
 Servidors Ajuda...  
 Mòduls No utilitzats  
 Servidor Proxy Squid

Busca:

Informació del Sistema  
 Surt

### Control d'Accés

[Llistes de control d'accés](#) | [Restriccions de proxy](#) | [Restriccions ICP](#) | [Programes ACL externs](#) | [Restriccions de proxy de respos](#)

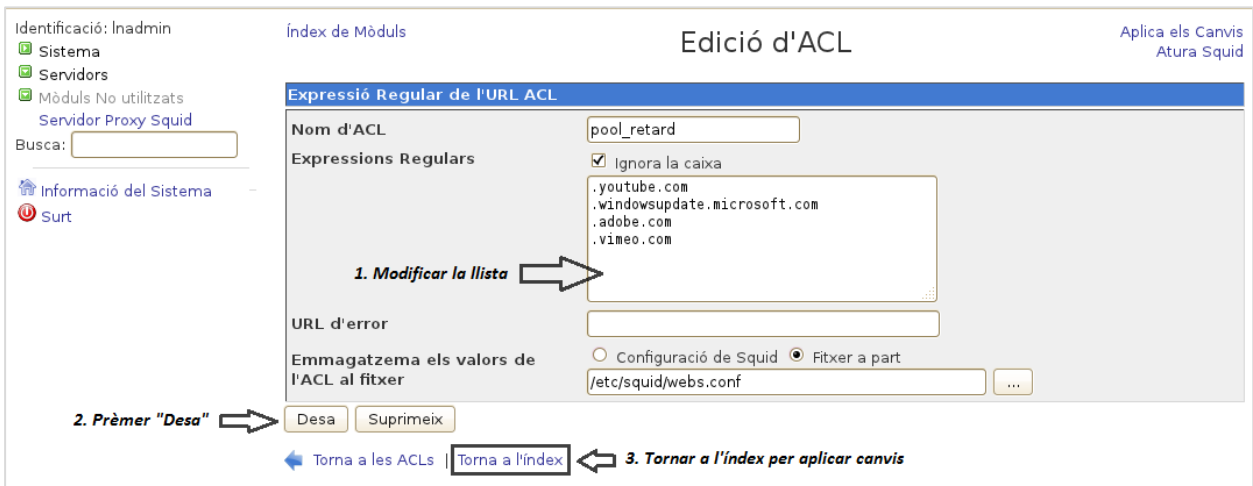
Nom	Típus	Coincidint...
all	Adreces Client	all
manager	Protocol de l'URL	cache_object
localhost	Adreces Client	127.0.0.1/32
to_localhost	Adreça del Servidor Web	127.0.0.0/8
localnet	Adreces Client	10.0.0.0/8
localnet	Adreces Client	172.16.0.0/12
localnet	Adreces Client	192.168.0.0/16
SSL_ports	Port de l'URL	443
Safe_ports	Port de l'URL	80
Safe_ports	Port de l'URL	21
Safe_ports	Port de l'URL	443
Safe_ports	Port de l'URL	70
Safe_ports	Port de l'URL	210
Safe_ports	Port de l'URL	1025-65535
Safe_ports	Port de l'URL	280
Safe_ports	Port de l'URL	488
Safe_ports	Port de l'URL	591
Safe_ports	Port de l'URL	777
CONNECT	Mètode de Petició	CONNECT
shoutcast		X-HTTP09-First-Line ^ICY[0-9]
apache		Server ^Apache
pool_retard	Expressió Regular de l'URL	Del fitxer /etc/squid/webs.conf

Adreces Client

[Torna a l'índex de squid](#)

A la pàgina **Edició d'ACL** es llisten els dominis, on es troben les pàgines web a les que s'aplica la limitació de l'ample de banda. Si es vol limitar l'ample de banda de l'adreça `www.domini.net`, s'ha d'afegir a la llista, sense les `www` amb el punt al davant: `.domini.net`

- ✓ Per fer efectius els canvis, feu clic al botó **Desa**.



Identificació: Inadmin Aplica els Canvis  
Atura Squid

Sistema Índex de Mòduls  
 Servidors Ajuda...  
 Mòduls No utilitzats  
 Servidor Proxy Squid

Busca:

Informació del Sistema  
 Surt

### Edició d'ACL

Expressió Regular de l'URL ACL

Nom d'ACL:

Ignora la caixa

Expressions Regulars:

**1. Modificar la llista** →

URL d'error:

Emmagatzema els valors de l'ACL al fitxer:  Configuració de Squid  Fitxer a part

**3. Tornar a l'índex per aplicar canvis**

- ✓ Accediu a la pàgina principal del **Servidor Proxy Squid** i feu clic al botó **Aplica** la configuració.

## 2.2. Visualització de les pàgines visitades (Anàlisi de Registres Calamaris)

El mòdul d'**Anàlisi de registres Calamaris** determina les pàgines web més visitades del centre i les que més ample de banda consumeixen. Aquesta informació ajuda a determinar quines pàgines web interessa afegir a la llista, de l'apartat anterior, on és limita l'ample de banda de les pàgines (**pool\_retard**) o denegar el seu accés.

- ✓ Per accedir al mòdul cliqueu sobre la icona **Anàlisi de registres Calamaris**.



- ✓ Cliqueu sobre **Request-destination by 2nd-level-domain**.

Identificació: lnadmin

- ☑ Sistema
- ☑ Servidors
- ☑ Mòduls No utilitzats

Servidor Proxy Squid

Busca:

[Informació del Sistema](#)

 Surt

[Índex de Mòduls](#)

## Anàlisi de Registres Calamaris

S'està limitant l'anàlisi a les darreres 50000 línies dels registres...

**Informe generat el 08/Jun/2012 08:58**

### Proxy Report

01.Jun 12 12:22:42 - 08.Jun 12 08:52:37

- Summary
- Incoming requests by method
- Incoming UDP-requests by status
- Incoming TCP-requests by status
- Outgoing requests by status
- Outgoing requests by destination
- **Request-destinations by 2nd-level-domain**
- Request-destinations by toplevel-domain
- TCP-Request-protocol
- Requested content-type
- Requested extensions
- Incoming UDP-requests by host
- Incoming TCP-requests by host
- Distribution Histogram
- Performance in 1 hour steps

L'informe d'anàlisi, que genera el programa **Calamaris**, mostra els dominis visitats ordenats per nombre decreixent de peticions (primera columna), el nombre de peticions fetes (segona columna), el percentatge total de peticions analitzades (tercera columna), la quantitat de dades descarregades (quarta columna) i el percentatge total de consum (cinquena columna).

Es recomana incloure a la llista on és limita l'ample de banda (**pool\_retard**), les pàgines web que reben poques visites (primera columna) i consumeixen un percentatge gran d'informació (cinquena columna).

destination	request	%	Byte	%	hit-%
*.windowsupdate.com	3785	29.26	83901274	37.54	0.00
*.telefonica.es	3231	24.98	2606694	1.17	0.00
*.pandasoftware.com	959	7.41	14084179	6.30	0.00
*.epimg.net	843	6.52	6755212	3.02	74.97
*.xtec.cat	645	4.99	28342175	12.68	50.70
*.edu365.cat	482	3.73	11205646	5.01	91.29
*.google.com	289	2.23	16525607	7.39	5.54
*.gencat.cat	216	1.67	1807960	0.81	19.44
*.yting.com	183	1.41	2396921	1.07	19.13
149.20.56.*	155	1.20	220100	0.10	0.00
*.google.es	145	1.12	2323511	1.04	9.66
<error>	140	1.08	194035	0.09	18.57
*.gstatic.com	123	0.95	1165547	0.52	26.02
*.youtube.com	113	0.87	17745403	7.94	5.31
*.prisacom.com	103	0.80	366222	0.16	3.88
*.planeo.com	81	0.63	779054	0.35	59.26
*.adobe.com	81	0.63	1235554	0.55	1.23
221.8.69.*	80	0.62	113600	0.05	0.00
xtec.cat	75	0.58	3200510	1.43	1.33

### 2.3. Neteja i Reconstrucció del Cau

Es aconsellable realitzar un neteja periòdica de la memòria cau, especialment quan es detecten errors durant la navegació, per exemple, que no es mostren les imatges de pàgines web recentment visitades.

- ✓ Accediu al mòdul **Servidor Proxy Squid** i a la secció **Neteja i Reconstrucció del Cau**.



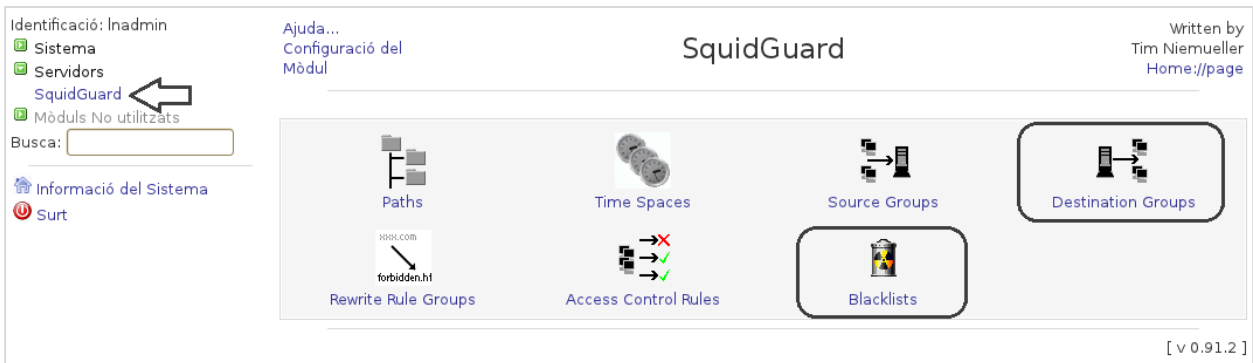
✓ Premeu el botó **Neteja i reconstrueix el cau**.



En acabar, s'ha buidat tota la memòria cau del servidor **proxy squid**.

### 3. Gestió del filtratge de continguts (Squidguard)

El mòdul de filtratge de contingut (**Squidguard**) autoritza o denega l'accés a determinades pàgines web mitjançant la seva inclusió a determinades llistes.



A continuació es defineixen les llistes de menys a més autoritat:

- **Llistes negres genèriques (Blacklists)** - Denega l'accés a un llistat de pàgines web de contingut inapropiat. S'actualitzen automàticament cada dia. No són editables pel responsable d'informàtica del centre.
- **Llista blanca de centre** - Assegura l'accés a un llistat de pàgines webs tot i trobar-se al llistat de les Llistes negres genèriques (Blacklists). El responsable d'informàtica del centre pot editar aquesta llista.
- **Llista negra de centre** - Denega l'accés a un llistat de pàgines web de contingut inapropiat. El responsable d'informàtica del centre pot incloure pàgines que no es troben a les Llistes negres genèriques (Blacklists). Predomina sobre la llista blanca de centre.

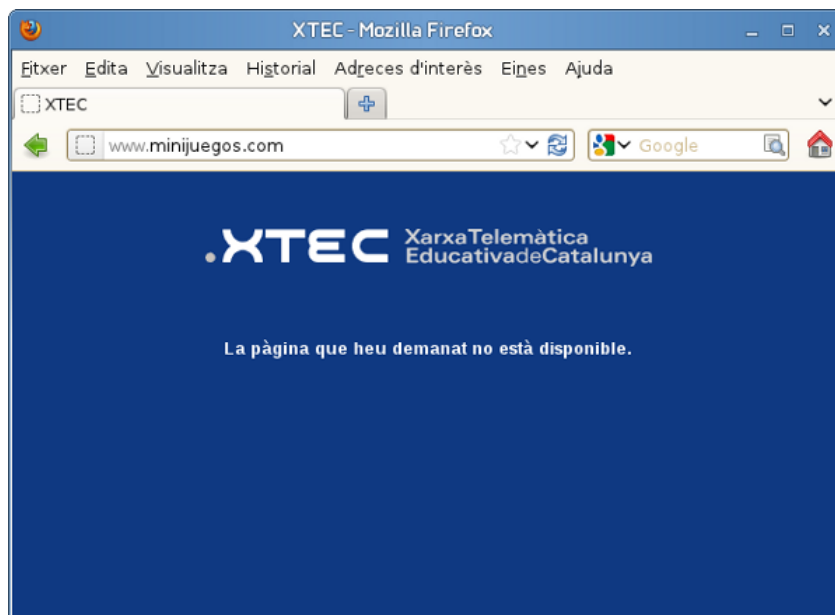
Si una pàgina web es troba simultàniament, a la **Llista blanca de centre** i a la **Llista negra de centre**, preval aquesta última i la pàgina web no és accessible. La **Llista blanca de centre** només té prioritat sobre les **Llistes negres genèriques (Blacklists)**.



El servidor de comunicacions mostra un missatge informatiu amb el fons taronja quan s'intenta visitar pàgines web que es troben a les **Llistes negres genèriques (Blacklists)** o a la **Llista negra de centre**.



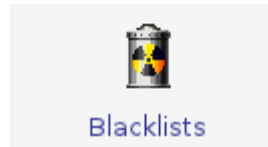
Existeix un altre filtre de continguts gestionat per la Xarxa Telemàtica Educativa de Catalunya (XTEC), el missatge informatiu d'aquest filtre és amb el fons de color blau. Les pàgines bloquejades per aquest filtre no es podran visualitzar afegint-les a la **Llista blanca de centre**.



### 3.1. Llistes negres genèriques (blacklists)

Les llistes negres genèriques (blacklists) s'actualitzen diàriament de forma automàtica i s'organitzen per temàtica (pornografia, violència, drogues, jocs, ...).

- ✓ Per veure les llistes negres genèriques cliqueu sobre la icona **Blacklists**.



- ✓ Seleccioneu una categoria (exemple: hacking)



- ✓ Premeu sobre **List All** per veure el contingut de la llista.

69.50.190.131	7sir7.com	80.53.249.38
80.80.15.28	80.80.15.30	81.177.26.26
83.149.65.117	abu-passwords.com	abx4.com
adultcomicworld.com	adultfreegals.com	adultpasswordcracks.com
allowstood.com	allpasswords.com	allteenmpgs.com
amateur-post.com	amateurpornsites.net	antionline.com
asianpornsites.net	asianxxxdatabase.com	astalavista.box.sk
backtrack-linux.org	bandit.org	banditpasswords.com
blackoutz-crew.de.gs	blackrosexxx.com	blog.chosun.com
bpics.com	busch-hacker.de	candoinet.com.br
cheatcodes.com	cheats.ru	chefcasimera.com
colibry-shells.com	controlpass.sexpikz.com	cowhigh.com
cracklib.net	cremepasswords.com	cultdeadcow.com
cyberpasses.com	darkflash.com	darknet.org.uk

No s'han de realitzar modificacions sobre aquestes llistes.

### 3.2. Afegir pàgines a la llista blanca de centre

La **llista blanca de centre** permet rectificar la restricció d'accés a una pàgina inclosa a les **l·listes negres genèriques (Blacklists)**.

- ✓ Per incloure pàgines web a la **llista blanca de centre**, accediu al mòdul **Destination Groups**.



- ✓ Cliqueu sobre la icona **llista\_blanca\_centre**.



Identificació: lnadmin Index de Mòduls Destination Groups Written by Tim Niemueller Home://page

Sistema  
Servidors  
SquidGuard  
Mòduls No utilitzats

Busca:

Informació del Sistema  
Surt

List of destination groups groups (Servers on the Web)

 llista_negra_centre	 llista_blanca_centre
--	---

Name for new destination group:

[Torna module index](#)

- ✓ Cliqueu sobre **Add Domain**.

Identificació: lnadmin Index de Mòduls Edit Destination Group Written by Tim Niemueller Home://page



Sistema  
Servidors  
SquidGuard  
Mòduls No utilitzats

Busca:

Informació del Sistema  
Surt

Domains for Destination group 'llista\_blanca\_centre'

vimeo.com	youtube.com
-----------	-------------

[ Add Domain ]  Afegir nous dominis  Dominis actuals de la llista blanca

URLs for Destination group 'llista\_blanca\_centre'

[ Add URL ]

Regular Expressions for Destination group 'llista\_blanca\_centre'

No regular expressions found for this destination group.

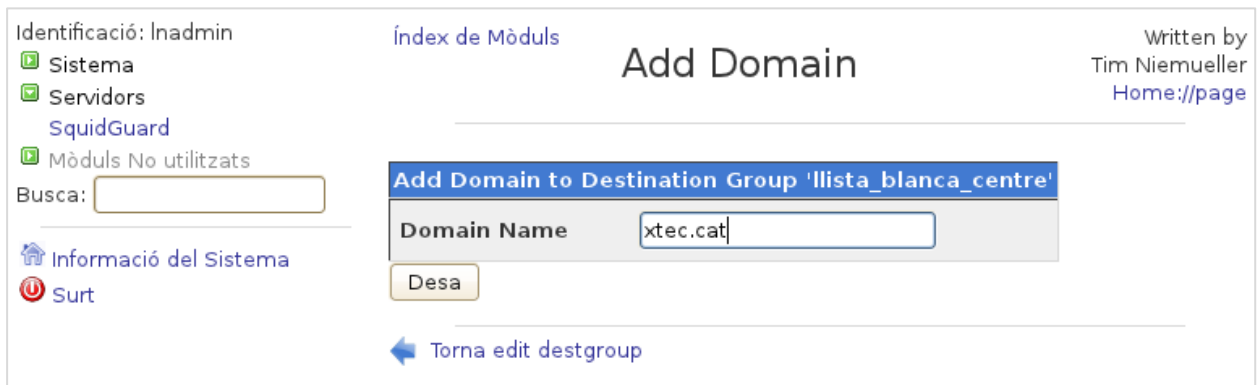
[ Add Expression ]

Timespace:

[ Delete Destination Group ]

[Torna list of destination groups](#)

- ✓ Afegiu el domini que es vol incloure a la llista i feu clic al botó **Desa**.



- ✓ Per fer efectius els canvis, accediu a la pàgina principal del **Servidor Proxy Squid** i cliqueu sobre el botó **Aplica la configuració**.

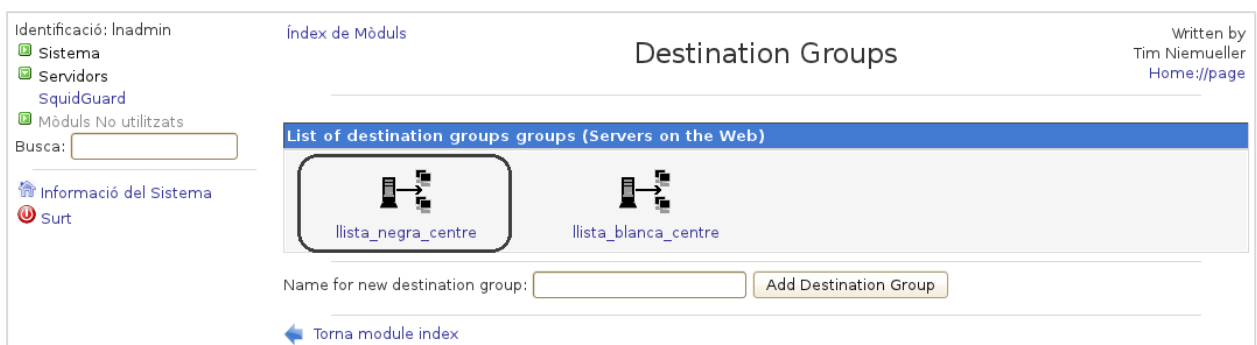
### 3.3. Afegir pàgines a la llista negra de centre

La **llista negra de centre** permet restringir l'accés a una pàgina independentment de la seva inclusió o no a la resta de llistes. Preval sobre els altres criteris.

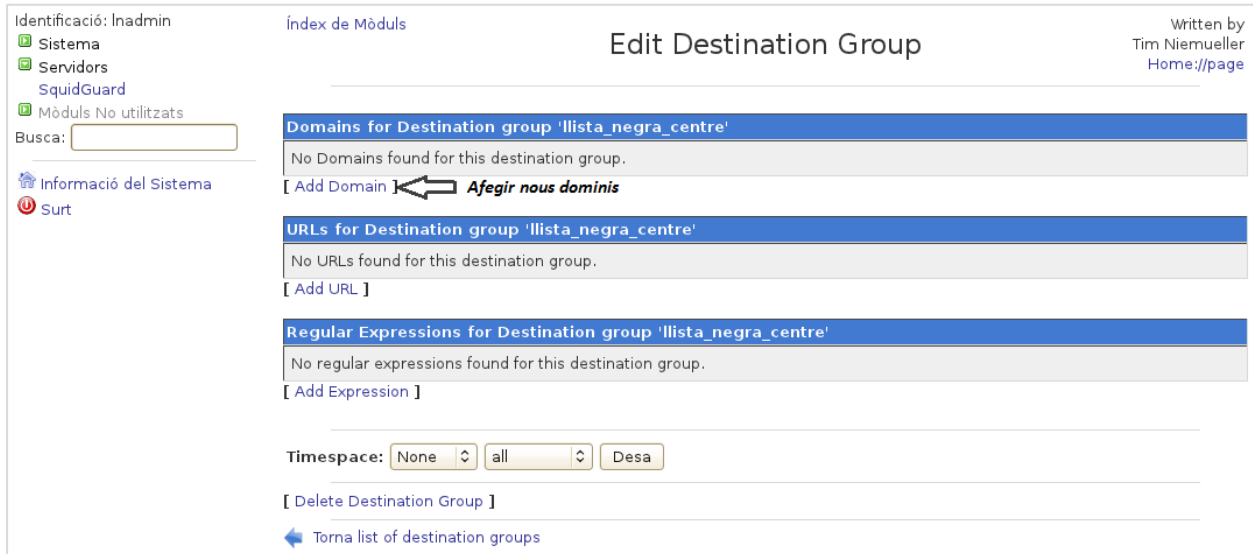
- ✓ Per incloure pàgines web a la **llista negra de centre**, accediu al mòdul **Squidguard** i cliqueu sobre la icona **Destination Groups**.



- ✓ Cliqueu sobre la icona **llista\_negra\_centre**.



✓ Cliqueu sobre **Add Domain**.



✓ Afegiu el domini que es vol incloure a la llista i feu clic al botó **Desa**.



✓ Per fer efectius els canvis, accediu a la pàgina principal del **Servidor Proxy Squid** i cliqueu sobre el botó **Aplica la configuració**.

## 4. Altres informacions d'interès

### 4.1. Usuaris

El servidor de comunicacions disposa de diversos usuaris per realitzar la seva gestió.

Nom	Descripció	Permisos	Accés
root	Administrador del sistema	Control total de l'equip	Gestió remota
gesrem	Servei gestió de remota	Control parcial de l'equip	Gestió remota
Inadmin	Responsable TIC del centre	Control parcial de l'equip	Responsable TIC del centre

### 4.2. Còpies de seguretat

En el procés d'instal·lació del servidor de comunicacions es realitza una còpia de seguretat dels fitxers de configuració sobre una carpeta del propi servidor. Es pot realitzar una segona còpia externa sobre un llapis USB del centre.

### 4.3. Servei de gestió remota

El servei de gestió remota ofereix assistència de suport tècnic en remot per tal d'ajudar als seus responsables TIC en les tasques de manteniment i gestió de l'equipament informàtic.

El servei de gestió remota pot realitzar les següents accions:

- a) Resoldre incidències que afecten al servidor, i com a conseqüència:
  - ✓ Restaurar una còpia de seguretat dels fitxers de configuració.
  - ✓ Instal·lar, eliminar i actualitzar programari
- b) Atendre peticions realitzades a través de l'espai de suport TIC com per exemple:
  - ✓ Modificar la configuració del servidor. Exemple: canvi d'adreces IP de les interfícies de xarxa.
  - ✓ Gestionar els límits d'ample de banda (Pools de retard / delay pools)
  - ✓ Afegir i treure routers
  - ✓ Ajustar el balanceig de càrrega (Pes aritmètic)

### 4.4. Recuperació a l'estat anterior

Per recuperar l'estat anterior a la instal·lació del servidor de comunicacions, desconnecteu els cables de xarxa del servidor de comunicacions i connecteu un cable de xarxa al/els routers amb el Switch principal.

A continuació, l'esquema mostra les connexions de xarxa entre els diferents elements abans i després de realitzar la instal·lació del servidor de comunicacions.

