

UF3 TALLAFOCS I SERVIDORS INTERMEDIS

Servidors intermedis o proxy

El servidor proxy-cache

- Un servidor proxy s'encarrega de realitzar una petició en nom d'un client a un altre servidor mitjançant un protocol determinat.
- **Es tracta d'un programari que s'instal·la en un servidor i que serveix d'intermediari entre client i servidor.**
- També es coneix com servidor intermediari
 - El servidor fa d'intermediari per realitzar una acció en nom del client.
 - **La majoria dels proxys treballen amb el protocol HTTP.**

El servidor proxy-cache

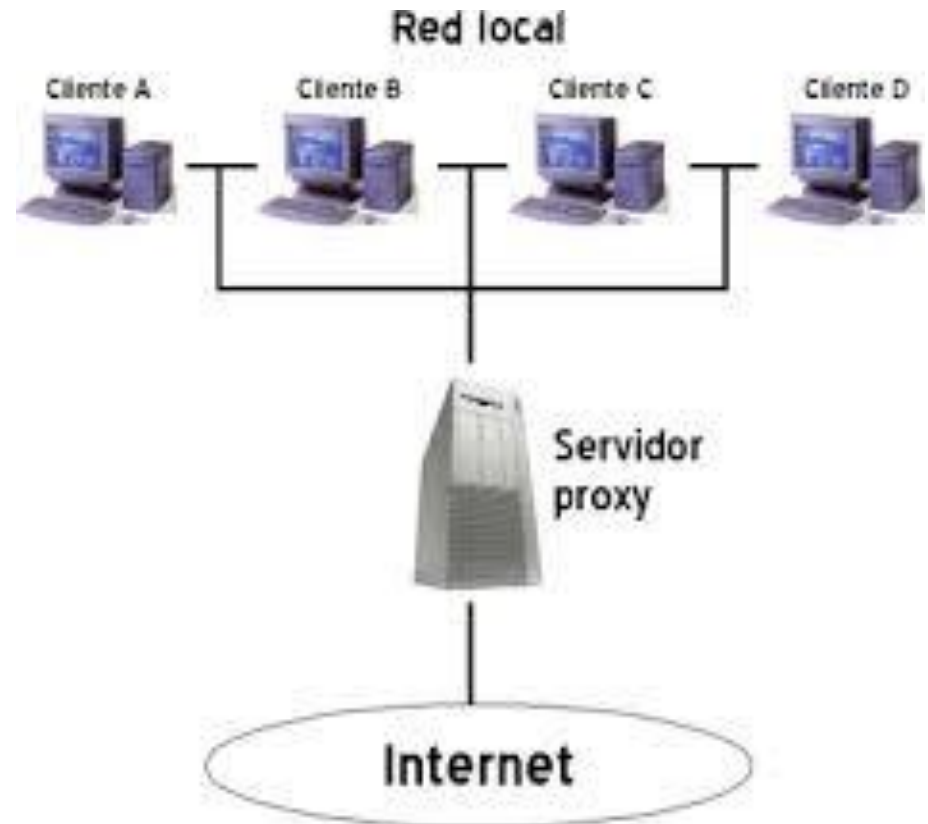


El servidor proxy-cache

- Un servidor proxy té com **objectiu** la **centralització del trànsit entre Internet i una LAN**
- **Actua com passarel·la a nivell d'aplicació**
 - Cadascun dels ordinadors de la xarxa local no té la **necessitat de disposar d'una connexió directa a Internet**
- **També s'utilitza per controlar els accessos no permesos desde Internet fins a la xarxa local**

El servidor proxy-cache

- El servidor proxy el que fa és transformar les adreces d'entrada i sortida.
- Quan un ordinador de la xarxa local fa una sol·licitud o petició web, el proxy el que fa és interceptar i processar aquesta sol·licitud.
- Així oculta l'adreça IP de l'ordinador real que ha fet la sol·licitud.
- En lloc de l'adreça IP de la màquina sol·licitant, surt la IP del servidor proxy.

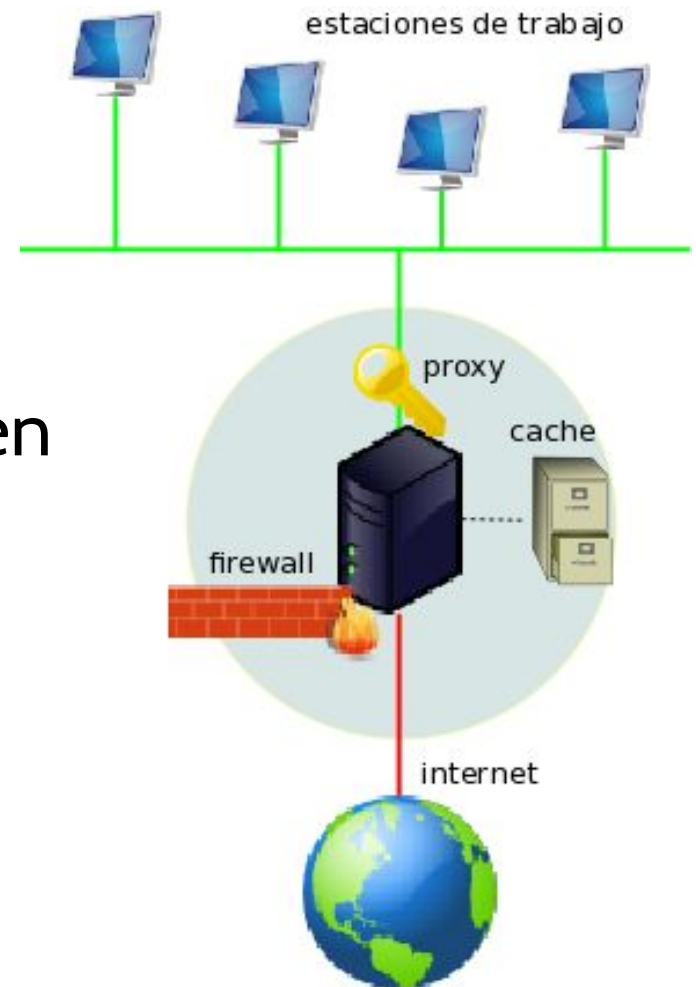


El servidor proxy-cache

- De normal, l'ordinador que fa de **servidor proxy té dues interfícies de xarxa.**
 - Un connectada a la xarxa local
 - Altra connectada a Internet
- Tots els paquets de la xarxa local, arriben al servidor proxy a través de la interfície local i son analitzats abans d'enviar-se a l'exterior a través de la interfície de xarxa

El servidor proxy-cache

- El servidor proxy també ofereix altres serveis com el de cache
 - Pot emmagatzemar en memòria cache les dades que gestiona.



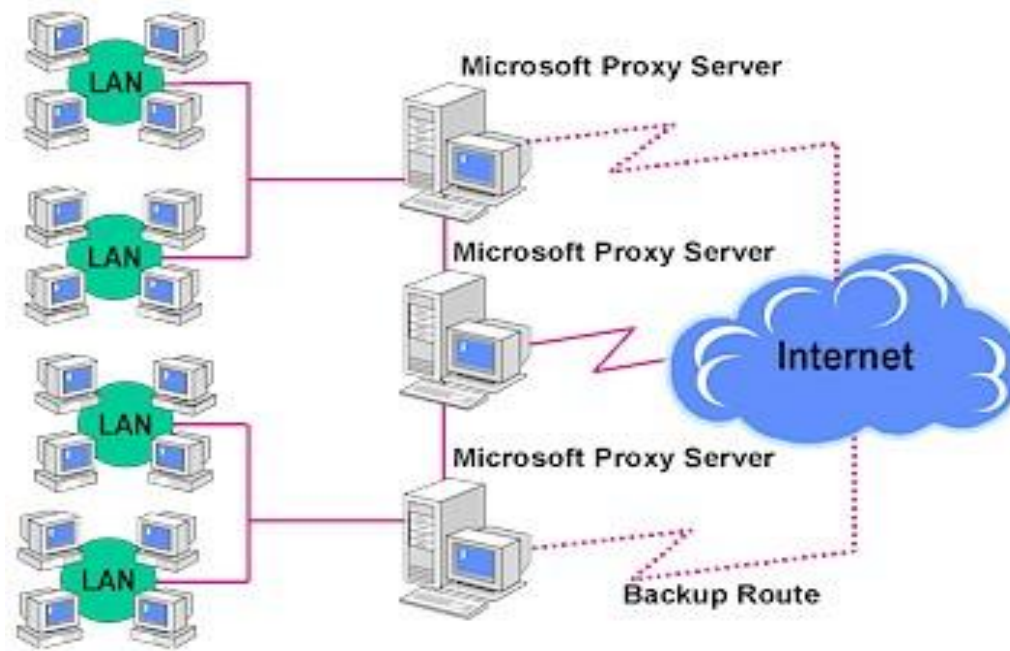
El servidor proxy-cache

- **Característiques:**

- Permeten l'accés web a màquines que no estan connectades directament a Internet
- Controlen l'accés web aplicant regles o normes
- Registren el trànsit web desde la xarxa local fins a l'exterior
- Controlen la seguretat i el contingut web visitat i descarregat per prevenir atacs de virus
- **Funcionen com cache de pàgines web:**
 - Emmagatzemen les pàgines web visitades pels usuaris per si altre usuari vol accedir.
 - En aquest cas és el servidor proxy qui serveix la pàgina directament a l'usuari sense que es tingui que tornar a connectar a Internet

El servidor proxy-cache

- En una xarxa poden haver-hi més d'un servidor proxy
 - Aquests s'organitzen de manera jeràrquica



Els clients de cada xarxa, redrecen el trànsit web al seu servidor proxy més proper.

El servidor proxy-cache

- **Avantatges:**

- **Major velocitat de navegació.**

- Si la pàgina esta en cache, els clients poden accedir en un temps menor al contingut:

- <https://www.youtube.com/watch?v=TN6Yjy9OgmM>

- **Ús més eficient de la línia de connexió amb Internet.**

- Si la pàgina esta en cache, no s'accedeix a Internet a pel contingut. Es servit per la pròpia xarxa local

- **Tallafocs de continguts.**

- Fa funció de tallafocs, ja que és el proxy-cache qui es comunica amb l'exterior.
 - Augmenta la seguretat de l'usuari respecte al contingut al qual accedeix

El servidor proxy-cache

- **Avantatges:**
 - **Filtrat de serveis.**
 - Es pot indicar els serveis específics que es poden utilitzar (HTTP, FTP, etc)

El servidor proxy-cache

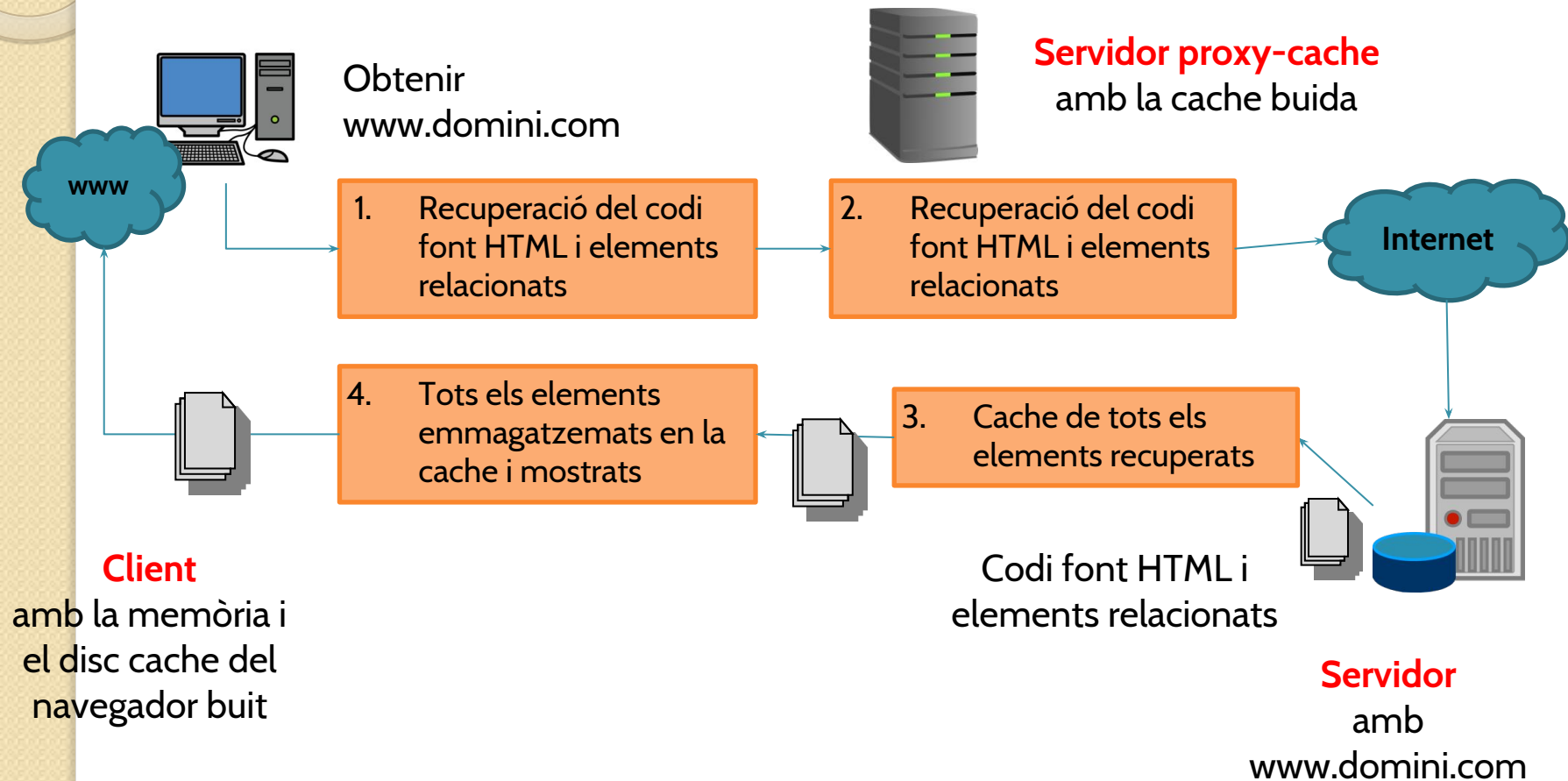
FUNCIONAMENT

1. El navegador web (client) demana accés a una pàgina web o demana un arxiu FTP
 - Com que el navegador està configurat per accedir a Internet a través del proxy, la petició la fa al servidor proxy-cache
2. El proxy-cache rep la petició i busca dins la seua memòria cache (disc dur) per si la pàgina ja ha estat sol·licitada per altre client

El servidor proxy-cache

3. **Si és la primera vegada** que es vol accedir al recurs, el servidor no la té la informació en cache
 - Llavors el servidor proxy reenvia la petició al servidor web que tingui el recurs
 - Aquest servidor web tornarà la informació demanada
 - A continuació el proxy emmagatzema la informació en cache i l'envia al navegador web (client) que la va sol·licitar

El servidor proxy-cache

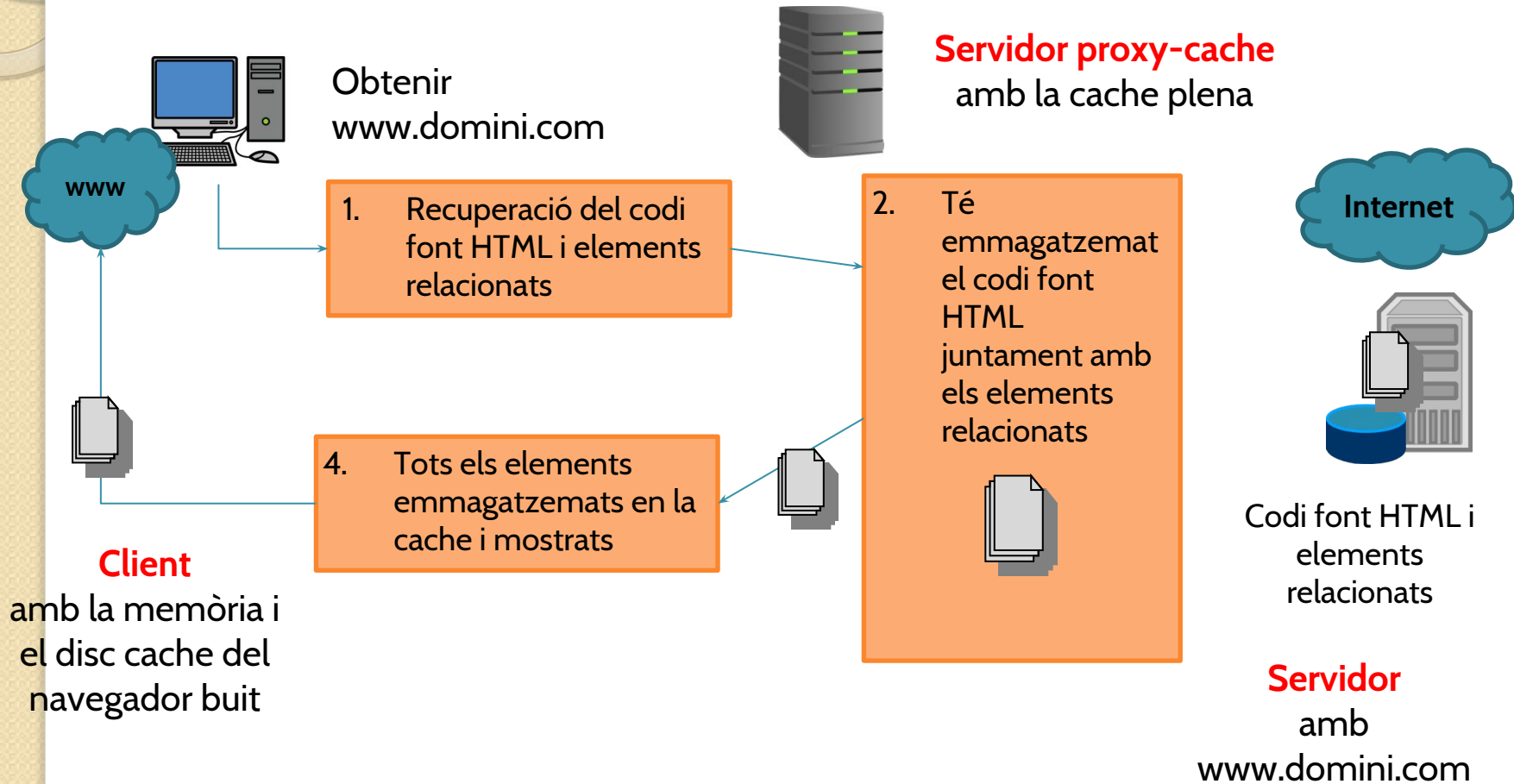


El servidor proxy-cache

4. Si el servidor ja té la informació, el proxy sol·licita al servidor web que li envii la capçalera de la pàgina o recurs

- A la **capçalera** verifica la data de creació de la pàgina i la data de l'última modificació
- A **continuació compara** les dates de la còpia que té a la seva cache amb les que envia el servidor i fa el següent:
 - Si la **informació no ha variat**, no se li demana més dades al servidor i el proxy envia directament al navegador web (client) la pàgina que té en cache
 - Si la **informació ha variat**, el proxy sol·licita la navegador web la nova versió de la informació i a continuació substitueix l'antiga que té en cache per la nova i finalment l'envia al navegador web (client)

El servidor proxy-cache



El servidor proxy-cache

- **SQUID**

- L'eina **Squid** és el servidor proxy-cache més estès entre les diferents distribucions Linux
- <https://prezi.com/9oypbxb7w6wq/servidor-proxy-squid/>
- **Versió 3**
- Pot fer de proxy-cache amb els protocols HTTP, FTP i SSL
- Actua de proxy transparent i que es pot utilitzar com cache per a DNS
- La seva principal funció és la de suportar el protocol ICP (Internet Cache Protocol) que permet la integració i comunicació de servidors cache
- Pot establir jerarquies de proxys en cas de que es produeixi una errada

Proxy transparent

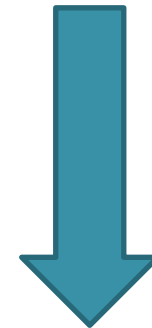
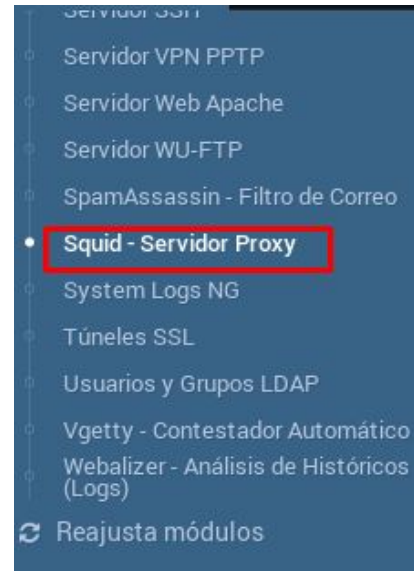
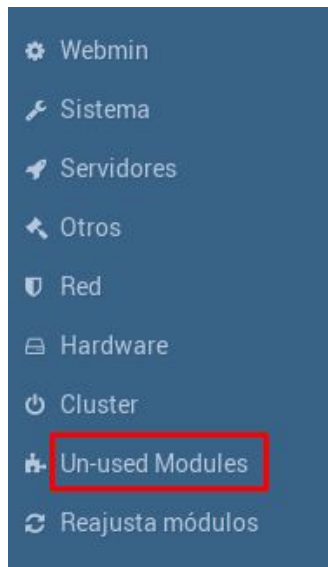
També conegut com proxy d'intercepció, proxy inline o proxy forçat, un proxy **transparent** intercepta la comunicació normal a la capa de xarxa sense requerir cap configuració de client especial. Els clients no necessiten ser conscients de l'existència del proxy. Normalment, un proxy transparent es troba entre el client i Internet, fent algunes de les funcions d'una passarel·la o un enrutador.

Squid

- **Instal·lació d'squid en Debian**
 - Instal·leu squid amb la comanda següent
 - `apt-get install squid3`
 - A continuació aneu al seu directori de configuració `/etc/squid3` i visualitzeu el seu contingut
 - Feu una còpia de seguretat del fitxer de configuració d'squid per evitar futurs errors ja que el fitxer de configuració és molt extens
 - `cp squid.conf squid.conf.original`

El servidor proxy-cache

Intal.lació d'squid en Webmin



☆ Servidor Proxy Squid

El ejecutable Squid `squid3` no existe. Si tiene instalado Squid, ajuste su [configuración del módulo](#) para que utilice trayectorias correctas.

El paquete Squid - Servidor Proxy puede ser instalado automáticamente mediante Webmin. [Pulse aquí](#) para que sea descargado e instalado utilizando APT

☆ Instalar Paquete

Instalando paquete(s) mediante comando `apt-get -y -f install squid...`

```
Reading package lists...
Building dependency tree...
Reading state information...
```

El servidor proxy-cache



- **Configuració d'squid**
 - L'arxiu de configuració d'squid és `squid.conf`
 - Aquest fitxer esta dividit en diferents seccions
 - **Configurarem squid mitjançant Webmin**
 - A continuació explicarem les diferents seccions

<https://www.youtube.com/watch?v=ehraSdtUe4s&t=339s>

El servidor proxy-cache



- Configuració d'squid en Webmin

Webmin 1.780 en ns1 (Ubuntu Linux 14.04) - Mozilla Firefox

Webmin 1.780 en ns1 (Ubuntu ...

https://localhost:10000

Login: alicia

- Webmin
- Sistema
- Servidores
 - Configuración de Postfix
 - Lectura de Correo de Usuarios
 - Servidor de Base de Datos MySQL
 - Servidor de DNS BIND
 - Servidor Web Apache
 - Squid - Servidor Proxy**
 - Vsftpd
- Otros
- Red
- Hardware
- Cluster
- Un-used Modules

Search:

View Module's Logs

System Information

Refresh Modules

Configuración de Módulo

Servidor Proxy Squid

Su directorio de caché de Squid /var/spool/squid3 no ha sido inicializado. Esto tiene que realizarse antes de que Squid se ejecute.

Inicializar Caché como usuario Unix proxy



Puertos y Trabajo en Red



Otras Cachés



Uso de Memoria



Logging



Opciones de Caché



Programas de Ayuda



Control de Acceso



Opciones Administrativas



Programas de autenticación



Pools de Retardo



Control de Acceso de Cabeceras



Refresca las Reglas



Opciones Varias



Configuración del Redireccionamiento de Puertos



Estadísticas de Gestor de Caché



Cache Manager Passwords



Limpiar y Reconstruir Caché



Edit Configuration Files

Presione sobre este botón para activar la configuración actual de Squid.

El servidor proxy-cache



- Configuració d'squid en Webmin

Configuración de
Módulo

Servidor Proxy Squid

Su directorio de caché de Squid /var/spool/squid3 no ha sido inicializado. Esto tiene que realizarse antes de que Squid se ejecute.

Inicializar Caché como usuario Unix ...



Puertos y Trabajo en Red



Otras Cachés



Uso de Memoria



Logging



Opciones de Caché



Programas de Ayuda



Control de Acceso



Opciones Administrativas



Programas de autentificación



Pools de Retardo



Control de Acceso de Cabeceras



Refresca las Reglas



Opciones Varias



Configuración del
Redireccionamiento de Puertos



Estadísticas de Gestor de Caché



Cache Manager Passwords



Limpiar y Reconstruir Caché



Edit Configuration Files

El servidor proxy-cache



- **Configuració d'squid en Webmin**
 - Anem a veure cadascuna de les seccions del Webmin



- Executar com usuari/grup. Estableix usuari i grup.
`cache_effective_user proxy`
`cache_effective_group proxy`
- Adreça email de gestor de cache. El paràmetre `cache_mg` estableix l'adreça de direcció de correu
`cache_mg admin@domini.com`
- Nom de la màquina visible. Estableix el nom de la màquina amb la que s'anuncia la cache. Per defecte no s'assigna cat
`visible_hostname nomservidor`

El servidor proxy-cache



- **Configuració d'squid en webmin**
 - **Adreces i ports proxy**
 - Paràmetre `http_port` estableix el port o els ports on escolta squid
 - `default http_port: 3128`
 - `http_port: 8080`
 - Per defecte les peticions es realitzen a través del port 3128
 - També es fa ús d'altres com 8080 que és més fàcil de recordar
 - També podem associar squid a un IP en concret on es connectaria amb la xarxa local
 - `http_port 192.168.1.254:8080`



El servidor proxy-cache



Configuració d'squid en Webmin

- **Límit de l'ús de la memòria**
 - Paràmetre `cache_mem` determina la quantitat de RAM dedicada per emmagatzemar
 - **Per defecte es dediquen 256MB**
 - La quantitat de RAM depèn de l'espai disponible
 - `cache_mem 256MB`



El servidor proxy-cache



- **Configuració d'squid en Webmin**
 - **Directoris de cache**
 - El paràmetre `cache_dir` estableix la localització i el tamany de la cache en disc

```
cache_dir ufs /var/spool/squid 100 16 256
```



El servidor proxy-cache



- **Configuració d'squid en Webmin**
 - **Llistes de control d'accés**
 - El paràmetre ACL és molt important
 - Protegeix al servidor de connexions externes per evitar que es connectin clients desconeguts que saturin la connexió exterior
 - Protegeix als clients d'accessos a ports perillosos actuant com tallafocs contra possibles atacs desde la web
 - Estableix una jerarquia de caches
 - Estableix la xarxa com conjunt de treball o com màquines individuals



Control de Acceso

El servidor proxy-cache



- Configuració d'squid en webmin
 - Llistes de control d'accés

Indice de Módulo
Ayuda..

Control de Acceso

Aplicar Cambios
Parar 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	591
Safe_ports	Puerto URL	777
CONNECT	Método de Petición	CONNECT

Crear nueva ACL Autenticación Externa

Regresar a índice squid

El servidor proxy-cache



- **Configuració d'squid en Webmin**
 - **Llistes de control d'accés**
 - A continuació, a cada ACL creada se li assigna una regla de control d'accés - `http_access` – per a permetre o denegar les accions definides en l'ACL
 - Exemples de sintaxi d'ACL:

```
acl [nom_llista] src [components de la llista] - Adreça de client
acl [nom_llista] time marc horari - Data/hora
acl [nom_llista] srcdomain/dstdomain domain - Nom de la màquina
de servidor web
acl [nom_llista] url_regex patro - Expressió regular URL
acl [nom_llista] maxconn limit - Màximes connexions
```

El servidor proxy-cache



- **Configuració d'squid en Webmin**
 - **Llistes de control d'accés**
 - Es poden crear llistes de control per impedir l'accés desde el proxy a certes pàgines web, així com permetre o denegar la sortida a Internet durant certs dies de la setmana o un període de temps major.
 - Únicament s'ha de crear ACL que identifiqui diferents situacions o condicions

El servidor proxy-cache



- **Configuració d'squid en webmin**
 - **Llistes de control d'accés**
 - Restriccions proxy
 - El paràmetre `http_access` indica si es permet o es denega l'accés a squid per fer peticions HTTP.
 - Actua sempre sobre una llista de control d'accés

```
http_access [ deny | allow] [!] [llista control access]
```

Quan deneguem una condició particular dins d'una xarxa local, la corresponent línia `http_access` s'ha de col·locar abans de la línia que permet tot a la xarxa local

El servidor proxy-cache



- **Configuració d'squid en webmin**
 - **Llistes de control d'accés**
 - Restriccions ICP
 - El paràmetre `icp_access` indica si es permet o es denega la creació de jerarquies de cache basant-se en llistes de control d'accés

```
icp_access [ deny | allow] [!] [llista control access]
```

El servidor proxy-cache



- Configuració d'squid en webmin

- Login

- Dins d'aquesta secció, squid genera diversos arxius log en el directori `/var/log/squid3`
 - Son dedicats a la monitorització
 - La seua ruta és `/var/log/squid3`
 - `access.log` **emmagatzema peticions fetes al proxy.** Amb aquest fitxer podem extraure estadístiques.
 - Paràmetre `access_log`
 - `cache.log` **emmagatzema informació general del funcionament de la cache, errors, etc**
 - Paràmetre `cache_log`
 - `store.log` **emmagatzema informació referent a la gestió de la cache.** Entrades i sortides d'objectes a ella
 - Paràmetre `cache_store_log`



Monitoratge

- Hi ha diferents mètodes per monitoritzar l'activitat d'squid
- **Arxiu `/var/log/squid/cache.log`**
 - Podem visualitzar les línies en l'arxiu `cache.log`
 - Aquest arxiu ha de tenir permisos 660 per poder enregistrar la informació
 - Per visualitzar les últimes línies podem executar la comanda `tail`
 - `tail /var/log/squid/cache.log`
 - Si surten errors podem executar la mateixa comanda amb l'opció `-f`
 - `tail -f /var/log/squid/cache.log`

Monitoratge

- **Arxiu `/var/log/squid/access.log`**
 - Conté totes les peticions servides pel proxy als navegadors web (clients)
 - Si qualsevol client té problemes per accedir a Internet es pot consultar aquest fitxer amb la comanda
 - `more access.log | grep DENIED`
 - **Les línies que es mostren en aquest arxiu comencen per `TPC_` per indicar el tipus de peticions que s'estan fent**

Monitoratge

- Arxiu `/var/log/squid/access.log`

Codi	Descripció
TCP_HIT	Accés a un pàgina web que esta en cache i esta actualitzada
TCP_MISS	Accés a una pàgina web que no esta en la cache
TCP_REFRESH_MISS	Accés a una pàgina web que esta en cache però no esta actualitzada
TCP_DENIED	Accés a una pàgina web prohibida

Els codis de resultat de peticions més importants son **DIRECT** quan la pàgina web sol·licitada es du directament del servidor remot i **NONE** quan aquesta esta en cache del servidor proxy

Monitoratge

- **Calamaris: visor de logs**
 - Aquesta eina genera informes de l'activitat de la cache en format HTML i ASCII a partir dels fitxers log d'Squid
 - Per instal·lar-la executem la comanda
 - `apt-get install calamaris`
 - El seu arxiu de configuració és `/etc/calamaris/calamaris.conf`
 - Permet establir cada quant temps es realitzen els informes (diàriament, setmanal, mensual, etc)
 - Per defecte es fan de forma diària

Monitoratge

- **Calamaris: visor de logs**
 - Un cop instal·lat, podem veure desde Webmin els informes d'activitat del proxy Squid

Ayuda..
Configuración de Módulo

Servidor Proxy Squid
Squid versión 3.4

Aplicar Cambios
Parar Squid
Buscar Documentos..

The screenshot displays the Squid Proxy Server Webmin interface. At the top, there are links for 'Ayuda..', 'Configuración de Módulo', 'Servidor Proxy Squid', 'Squid versión 3.4', 'Aplicar Cambios', 'Parar Squid', and 'Buscar Documentos..'. The main area contains a grid of icons representing different configuration options:

- Puertos y Trabajo en Red
- Otras Cachés
- Uso de Memoria
- Logging
- Opciones de Caché
- Programas de Ayuda
- Control de Acceso
- Opciones Administrativas
- Programas de autenticación
- Pools de Retardo
- Control de Acceso de Cabeceras
- Refresca las Reglas
- Opciones Varias
- Configuración del Redireccionamiento de Puertos
- Estadísticas de Gestor de Caché
- Cache Manager Passwords
- Limpiar y Reconstruir Caché
- Análisis de Histórico de Calamaris** (highlighted with a red box)
- Edit Configuration Files

Aplicar la Configuración

Presione sobre este botón para activar la configuración actual de Squid.

Detener Squid

Presione sobre este botón para detener el servidor proxy Squid en ejecución. Una vez detenido, los clientes que lo utilizan no podran hacer peticiones web ni FTP.

Monitoratge

- Calamaris: visor de logs

 ☆ Análisis de Históricos de Calamaris

Limitando análisis a las 50000 últimas líneas de históricos...

Informe generado en 15/Mar/2017 12:37

Proxy Report

Report period: 14.Mar 17 17:02:48 - 15.Mar 17 11:46:56

Generated at: 15.Mar 17 12:37:54

Table of Content / Overview			
Summary	-	-	-
Incoming requests by method	most requested method	CONNECT	76 Requests
Incoming UDP-requests by status	-	-	no requests found
Incoming TCP-requests by status	most incoming request by status to	ERROR	59 Requests
Outgoing requests by status	most outgoing request to	DIRECT Fetch from Source	24 Requests
Outgoing requests by destination	most requested destination	DIRECT	24 Requests
Request-destinations by 2nd-level-domain	most requested 2nd-level-domain	<error>	57 Requests
Request-destinations by toplevel-domain	most requested toplevel-domain	<error>	57 Requests
TCP-Request-protocol	most requested protocol	<error>	57 Requests