GOVERN DE LES ILLES BALEARS
Conselleria d'Educació i Cultura
Direcció General d'Administració Educativa

Projecte Educ@ib

Documents tècnics

Instal·lació i configuració d'un servidor proxy-catxé basat en Ubuntu 8.04 a les xarxes dels centres

Rafel Cortès i Mora
rcortes@educacio.caib.es
Juny 2009

Instal·lació i configuració d'un servidor proxy-catxé basat en Ubuntu 8.04

Índex de contingut

INTRODUCCIÓ

proxyautocfg és una utilitat per configurar automàticament un proxy-catxé segons la proposta desenvolupada en el document "*Instal·lació i i configuració del proxy-catxé Squid*". En concret, la utilitat realitza les següents tasques:

- Integra el servidor en el domini
- Estableix la seguretat en els accessos per xarxa
- Configura el proxy-catxé *Squid*
- Configura el filtre *squidGuard*
- Instal·la i configura la utilitat *iControl*
- Configura el tallafocs *iptables* blocant totes les connexions excepte les destinades als ports *http*, *https*, *pop3*, s*mtp*, *dns*, *ftp, ftp-data* i *ssh*. Es permeten els paquets *icmp* (ping).

Fent servir aquesta utilitat és molt senzill instal·lar i configurar un proxy-catxé a la xarxa del centre. Aquest document explica totes les passes que s'han de fer per tal d'instal·lar i configurar una màquina en el centre que realitzi les tasques de catxé de la xarxa, de filtratge de continguts i de tallafocs.

REQUERIMENTS PREVIS

Es necessari disposar del següent CD:

1. Ubuntu 8.04 Alternate CD

L'ISO del CD s'anomena *ubuntu-8.04.x-alternate-i386.iso*

Es pot trobar a ftp://ftp.rediris.es/sites/releases.ubuntu.com/releases/

INSTAL·LACIÓ DE LINUX

Iniciau la instal·lació amb el CD Ubuntu 8.04.x Alternate CD.

Triau l'idioma *Català* i pitjau <Enter>

Pitjau F4 (Modes) i escolliu "Instal·la un sistema de línia d'ordres" + <Enter>

Iniciau la instal·lació amb "Instal·la l'Ubuntu" +<Enter>

Seleccionau el país ("Espanya") + <Enter>

Començarà la detecció de maquinària, s'analitzarà el CD-Rom, es carregaran components addicionals i es detectarà la targeta de xarxa.

Cancel·lau la configuració automàtica de la xarxa amb DHCP. Pitjau <*Continua*> per configurar la xarxa manualment.

Introduïu l'adreça IP del servidor (usar un dels 10 primers nombre del rang d'IP del centre) i pitjau <Continua>

Introduïu la màscara de la xarxa del centre i pitjau <Continua>

Introduïu la passarel·la (l'adreça IP del *router*) i pitjau <Continua>

Introduïu l'adreça IP del servidor de noms (DNS). Normalment, l'adreça IP del servidor controlador del domini del centre. Pitjau <Continua>

Ara s'ha d'introduir el nom curt que volem posar al proxy. Es proposa identificar-lo fent servir l'abreviatura *px*, el darrer número de l'adreça IP i el nom i versió del sistema operatiu. Així, si s'assigna l'adreça 10.216.254.7 al servidor de terminals, es proposa anomenar el servidor com *px7ubt804.*

Tot seguit introduïu el nom complet del domini del centre. Per exemple, *curs.local*

En aquest punt es configurarà el rellotge. Triau *Madrid* com a localització dens el fus horari. <Enter>

Després s'executarà el mòdul de detecció de discs i particionat. Triau Guiat - Utilitza el disc sencer. S'emprarà una partició primària pel sistema i una partició lògica petita per intercanvi.

Confirmau els canvis en el disc.

El procés segueix amb amb el format de les particions i la instal·lació del sistema base.

Tot seguit, el programa d'instal·lació demana les dades de l'usuari que utilitzareu per administrar el sistema. Es recomana emprar el mot *ubtadmin* com a nom d'usuari. Com a nom complet introduïu, per exemple, *Administrador de l'Ubuntu*. Caldrà també entrar la contrasenya per aquest usuari *ubtadmin*.

S'iniciarà la configuració del gestor de paquets apt. El programa d'instal·lació demana si s'utilitza un servidor intermediari de HTTP. Per contestar que no, deixau en blanc la resposta i pitjau <Continua>

Tot seguit s'inicia la instal·lació del programari. En acabar, el programa d'instal·lació demana si el rellotge del sistema està configurat a UTC. Contestau <Sí>.

La instal·lació ha finalitzat. Es demana que es tregui el CD per arrencar de nou amb el sistema instal·lat.

Iniciau una sessió amb el compte de l'usuari *ubtadmin*.

Configuració de la font de programari educaib

En primer lloc, és necessari instal·lar la clau pública per autenticar el repositori *Educaib.* Això suposa descarregar la clau i després instal·lar-la:

Per descarregar-la, obriu un terminal i executau:

```
cd $HOME
sudo wget http://weib.caib.es/ubt-educaib/educaib_key.asc
```

Ara, és necessari instal·lar la clau descarregada. Per això, executau:

```
sudo apt-key add educaib_key.asc
```

El sistema ha de contestar *OK*.

Un cop instal·lada la clau, s'ha d'afegir el repositori *Educaib* a les fonts de programari:

```
sudo nano /etc/apt/sources.list
```

Al final del fitxer afegiu la línia següent:

```
deb http://weib.caib.es/ubt-educaib ubt804 main
```

Guardau pitjant <*Ctrl-O*> + <*Enter*> i sortiu amb <*Ctrl-X*>

Instal·lació de la utilitat proxyautocfg

En primer lloc és necessari actualitzar les fonts de programari:

```
sudo apt-get update
```

Ara ja es pot instal·lar la utilitat:

```
sudo apt-get install proxyautocfg
```

Per satisfer les dependències, s'instal·laran uns 24 nous paquets.

Apareixerà un avís indicant la quantitat d'espai que s'emprarà. En acceptar (pitjant la tecla *s* + <*Enter*>), el sistema procedirà a la descarrega i instal·lació dels paquets.

És possible que apareixi una finestra per configurar el client kerberos. En concret demanarà el nom del servidor kerberos. Podeu deixar en blanc aquest nom ja que, després, *proxyautocfg* el configurarà automàticament.

La utilitat **proxyautocfg** s'instal·la a **/opt/proxyautocfg**

Descàrrega i instal·lació de les llistes negres gestionades per squidGuard

Executau:

```
cd $HOME
sudo wget http://dweib.caib.es/download/blacklists.tar.gz
sudo tar xzf blacklists.tar.gz
sudo rm -rf /var/lib/squidguard/db
sudo mv blacklists /var/lib/squidguard/db
```

Actualització del sistema

Executau

```
sudo apt-get upgrade
```

Reiniciau el sistema:

```
sudo shutdown -r now
```

Adaptació als paràmetres de la xarxa del centre

Editau el fitxer */opt/proxyautocfg/proxyautocfg.conf*

```
cd /opt/proxyautocfg
sudo nano proxyautocfg.conf
```

Modificau les variables segons els valors de la xarxa del centre:

ip_equip= Adreça IP del servidor proxy (l'equip que configurau) (*10.216.x.y)*

sm= Submàscara de xarxa.

ip_xarxa= Adreça IP de la xarxa del centre (*10.216.x.z*). El valor de *z* depèn de la subxarxa. Si aquesta és *255.255.255.0*, la *z* val 0. Si el centre està dins la Intranet i té les adreces IP normalitzades (que comencen amb 10.216), *z = r-1* essent *r* el darrer dígit de l'adreça IP del router.

nom_equip= Nom curt que heu assignat al proxy, per exemple *px7ubt804*

ip_servidor= Adreça IP del servidor controlador del domini

nom_servidor= Nom del servidor controlador del domini. A l'exemple: *scurs*

domini= Nom curt del domini de la xarxa del centre. A l'exemple:*curs*

dominic= El nom complet, segons el DNS, del domini del centre. A l'exemple *curs.local.* Alguns centres tenen el sufix *.local* mentre que altres no li tenen. Podeu consulta-ho en el servidor DNS del controlador del domini. Els dominis controlats per un Windows NT, no han d'afegir el sufix *.local*.

realm= El nom del domini tot en majúscules. Per exemple, *CURS.LOCAL*

nom_administrador= Nom de l'usuari administrador de domini. En el 99.99% dels cassos és *administrador*.

ip_administracio= Adreça IP de l'equip que s'utilitza habitualment per administrar la xarxa.

MB_catxe= nombre de Megabytes reservats per al catxé. Amb 5000 (aproximadament, 5Gb) ja està prou bé.

Guardau pitjant <*Ctrl-O*> + <*Enter*> i sortiu amb <*Ctrl-X*>

Execució de proxyautocfg

Convé fer una execució de prova:

```
sudo ./proxyautocfg -test
```

Es crearà una carpeta anomenada *output* amb els fitxers que la utilitat modifica. A més, dins aquesta carpeta trobareu un fitxer, anomenat ordres, amb el llistat de les comandes que s'executaran qua s'executi *proxyautocfg*. És convenient revisar una mica el contingut de *output* per comprovar si les modificacions es realitzaran correctament.

Un cop executada la prova amb resultat satisfactori, es pot procedir a l'execució definitiva:

```
sudo ./proxyautocfg
```

El procés demanarà la contrasenya de l'administrador del domini per tal d'integrar l'equip en el domini del centre. Si la integració ha anat bé, la resposta del sistema a la introducció de la contrasenya és: *Joined 'PX**UBT804' to realm 'nom del domini'*. Si no llegiu aquesta frase, alguna cosa ha fallat.

Durant el procés es recompilaran les llistes negres de l'SquidGuard (*Re-building SquidGuard db files ...)*. El procés és una mica lent, teniu paciència.

En acabar, es demanarà un reinici de l'equip. Un cop reiniciat, el proxy-catxé *Squid* + *squidGuard* + *iControl* + *iptables* estarà completament configurat.

Comprovació del correcte funcionament

Per comprovar el correcte funcionament del sistema podeu fer el següent:

1. Posau la IP del proxy com a porta d'enllaç per defecte d'un lloc de treball i navegau per Internet en aquest lloc de treball.
2. Visualitzau el contingut de */var/log/squid3/access.log*. Si el fitxer conté referències de la navegació anterior, vol dir que l'squid funciona.
3. Per comprovar l'*squidGuard*, executau *iControl* des d'un lloc de treball qualsevol (*http://adreça_ip_proxy/cgi-bin/iControl/iControl.cgi)*. Vos ha de demanar autenticació; introduïu administrador i la contrasenya de l'administrador del domini (inicialment aquest usuari és l'únic que té permisos per accedir a *iControl*).
4. Creau un nou origen i un nou destí, comprovau que podeu blocar, filtrar i permetre l'accés a Internet des del nou origen. Comprovau també que la navegació per llocs prohibits està restringida.
5. Per comprovar que s'han blocat totes les connexions excepte les destinades als ports *http*, *https*, *dns*, *pop3*, *smtp*, *ftp* i *ssh* podeu esperar la protesta d'un professor que usi habitualment eines tipus *eMule*. Podeu també comprovar que es permet fer ping (per exemple, *ping www.uoc.edu*).

Permisos d'accés a iControl

El control d'accés a la utilitat *iControl* es fa mitjançant el fitxer */usr/lib/cgi-bin/iControl/.htaccess*

En aquest fitxer s'ha d'especificar la llista de grups globals del domini els membres dels quals tendran accés a *iControl*. Aquesta llista s'introdueix amb l'ordre *Require group*. L'ordre que s'instal·la per defecte és:

```
Require group "Admins. del dominio"
```

Això vol dir que, inicialment, només els usuaris administradors del domini (grup *Admins. del dominio*) tendran accés a iControl.

Si volem que tots els professors també hi tenguin accés, s'haurà d'especificar:

```
Require group "Admins. del dominio" "profes"
```

Òbviament, s'ha suposat que *profes* és el nom del grup global de professors del centre.

Si el que volem és que només uns quants professors hi tenguin accés, recomanam crear un nou grup global en el domini i afegir a aquest grup els usuaris professors que han de gaudir d'accés a

iControl. Així, si anomenam icontrol a aquest nou grup, l'ordre *Require group* del fitxer .htaccess ha de quedar així:

```
Require group "Admins. del dominio" "icontrol"
```

ACTUALITZACIÓ DE LES LLISTES NEGRES

Actualment es poden trobar actualitzacions diàries de les llistes negres al servei FTP de la universitat de Toulouse (ftp.univ-tlse1.fr). Les llistes negres que s'han penjat a la Weib i que han servit per fer la instal·lació inicial del proxy s'han compilat a partir de aquestes llistes negres distribuïdes per la universitat de Toulouse. De tant en tant, també nosaltres penjarem en el weib llistes actualitzades. Per evitar haver de fer modificacions en el fitxer de configuració de l'squid Guard recomanam actualitzar les llistes negres emprant exclussivament les llistes publicades a la universitat de Tolouse o en el Weib. El procés de descàrrega i actualització és el següent:

```
cd $HOME
```

Parada de l'squid

```
sudo /etc/init.d/squid3 stop
```

Esborrar, si existeix, la darrera descàrrega:

```
sudo rm blacklists.tar.gz
sudo rm -rf blacklists
```

Descàrrega de les llistes

Si es fan servir les llistes de la universitat de Tolouse:

```
sudo wget ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz
```

Si es fan servir les llistes del Weib:

```
sudo wget http://dweib.caib.es/download/blacklists.tar.gz
```

Extracció

```
sudo tar xzf blacklists.tar.gz
```

Actualitza les llistes actuals

```
sudo cp -rf blacklists/* /var/lib/squidguard/db/
```

Recompilació de les llistes negres

```
sudo update-squidguard
```

Tornar a iniciar l'squid

```
sudo /etc/init.d/squid3 start
```

INFORMES SOBRE LA UTILITZACIÓ DEL PROXY-CATXÉ

Automàticament es generen informes diaris sobre la utilització del proxy i sobre les pàgines blocades per squidGuard. Els informes es poden consultar a la url *http://ip_proxy/squid-reports/*

Si es vol un informe del dia present, iniciau una sessió en el proxy-catxé amb el compte ubtadmin i executau:

```
sudo sarg-reports today
```

Ara, l'informe generat es podrà consultar a *http://ip_proxy/squid-reports/*