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

# Projecte Xarxipèlag

Documents tècnics

# Instal·lació i configuració d'un tallafoc per separar una xarxa experimental de la xarxa del centre

Rafel Cortès i Mora
rcortes@educacio.caib.es
Setembre 2005

# Instal·lació i configuració d'un tallafoc per separar una xarxa experimental de la xarxa del centre

## Índex de contingut



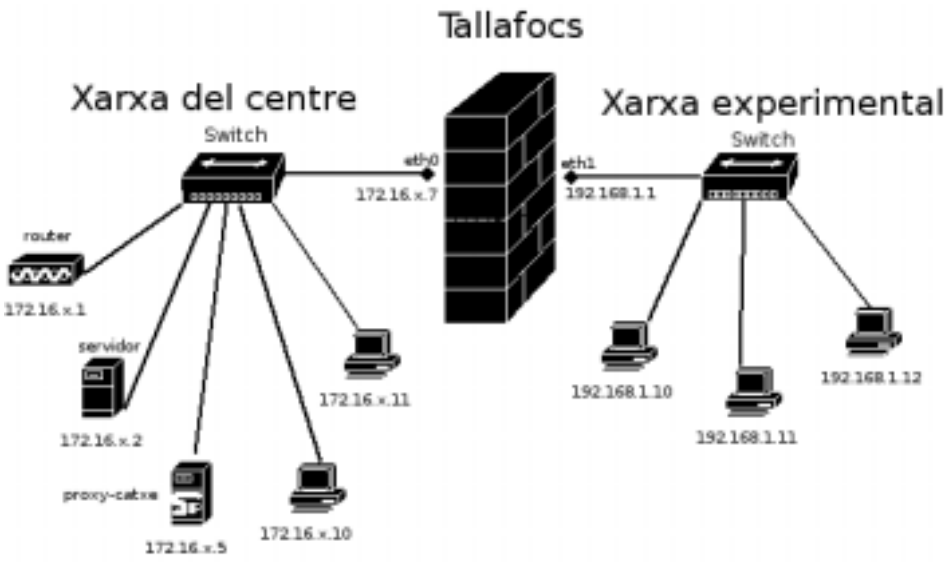
## INTRODUCCIÓ

Alguns centres, generalment IES, necessiten disposar d'una aula d'informàtica on no s'hi apliquin les polítiques restrictives de la xarxa del centre. Necessiten que els usuaris puguin iniciar sessions com a administradors, poder instal·lar i desinstal·lar aplicacions i, fins i tot, tenir capacitat per a reinstal·lar el sistema operatiu. Una d'aquestes situacions es genera en els centres que ofereixen mòduls de formació professional relacionats amb la informàtica. En aquests centres es fa imprescindible disposar d'una aula d'informàtica amb les característiques abans esmentades.

Aquesta proposta consisteix en instal·lar i configurar un tallafoc que separi una xarxa experimental de la xarxa del centre.

El tallafoc pot ser qualsevol *Pentium* II o superior amb dues targetes de xarxa. Una targeta s'ha de connectar a un *switch* de la xarxa del centre (millor si és el *switch* principal; el que té connectat el *router*) i l'altra s'haurà de connectar al *switch*/*hub* de la xarxa experimental.

La figura següent mostra la configuració de la xarxa amb el tallafoc instal·lat:




## FUNCIONALITAT

El tallafoc permetrà únicament les connexions següents:

| *Origen* | *Destinació* | *Connexions permeses* |
|---|---|---|
| Xarxa experimental | Internet | Permet només connexions http, https, ftp, pop3, smtp, telnet i ssh. |
| Xarxa experimental | Xarxa del centre | Només es permet fer ping; no es permet cap altra connexió. |
| Xarxa del centre | Xarxa experimental | No es permet cap connexió. |
| Xarxa del centre | Tallafoc | Només es permeten connexions des del servidor del centre i des de l'equip del coordinador de TIC. Des dels altres equips no es permet cap connexió. |
| Xarxa experimental | Tallafoc | No es permet cap connexió. |

## INSTAL·LACIÓ DEL TALLAFOC

### Suposicions

En aquest document suposarem que les adreces P de les xarxes són:

Xarxa del centre: 172.16.x.0/255.255.255.0

Xarxa experimental: 192.168.1.0/25.255.255.0

També suposarem que el dispositiu que està connectat amb la xarxa del centre és **eth0** i la seva adreça IP és 172.16.x.7. L'altra dispositiu **eth1** estarà connectat a la xarxa experimental i la seva adreça IP és 192.168.1.1

### Requeriments de maquinària

Qualsevol Pentium II o superior amb DUES interfícies de xarxa. També es pot fer la prova amb un Pentium I; caldrà veure el seu rendiment “in situ”.

### Instal·lació del sistema operatiu

Iniciau amb el primer CD de la distribució de Mandrake 9.1.

En el nivell de seguretat especificau *Alta*.

Demanarà en quina partició s'ha d'instal·lar Linux. Escolliu *particionament personalitzat – Canviar a mode Expert – Assigna automàticament – servidor* . Si el disc és gran, convé modificar la grandària de les particions. Per fer això s'han de suprimir i tornar-les a crear. L'ordre en què s'han de crear i l'espai proposat és:

| | |
|---|---|
| / | sistema (doble del proposat màx. 2Gb) |
| swap | intercanvi (espai proposat) |
| /usr | programes d'usuari (40% de l'espai restant) |
| /var | contingut variable (20%) |
| /tmp | temporal (20%) |
| /home | resta d'espai |

*Fet – D'acord* per confirmar l'escriptura de la taula de particions.

Quant a la selecció de paquets **és necessari** instal·lar, com a mínim, els següents (utilitzau *Selecció individual de paquets* per a precisar la selecció):

- Entorn gràfic:
  - NO és necessari. Si us hi trobau més còmodes, instal·lau GNOME. En tot cas, per estalviar recursos de màquina, es recomana que, un cop realitzada la configuració, es configuri Linux per arrencar en mode text. És a dir, quan funcioni el tallafoc és millor no iniciar el mode gràfic.
- Servidor:
  - Tallafoc/Encaminador:
    - iproute2
    - iptables
    - routed
  - Servidor d'ordinador de xarxa:
    - rfbdrake (només si s'ha instal·lat entorn gràfic)
    - OpenSSH (per poder treballar remotament amb el tallafoc)
- Estació de treball:
  - Ordinador de xarxa client:
    - samba-client (per si hem de connectar amb carpetes compartides)
  - Configuració (les opcions per defecte).
  - Eines de consola (les opcions per defecte. Si s'ha instal·lat GNOME, afegiu el paquet *gedit*).

En l'apartat de configuració de la xarxa, escolliu *Detecció automàtica*. Si va bé, detectarà les dues targetes de xarxa. Linux anomena aquests dispositius com a **eth0** i **eth1**. Triau Connexió LAN. Després s'haurà de configurar el protocol TCP/IP de cada una de les targetes:

**eth0** (el dispositiu que se connectarà a la xarxa del centre)

- Tipus protocol IP estàtic
- L'adreça IP dins la xarxa del centre (és un servidor, per tant, es recomana emprar una adreça del rang 172.16.x.3 – 172.16.x.9; (per exemple, 172.16.x.7) i la submàscara de la xarxa

(generalment, 255.255.255.0)

**eth1** (el dispositiu que se connectarà a la xarxa experimental)

- Tipus protocol IP estàtic
- L'adreça IP dins la xarxa experimental. El tallafoc actuarà com a porta d'enllaç de tots els equips de la xarxa experimental. Utilitzarem les adreces 192.168.1.0/255.255.255.0 per direccionar aquesta xarxa. El dispositiu eth1 del tallafoc serà el dispositiu 1 de la xarxa, és a dir, 192.168.1.1 Com a submàscara 255.255.255.0.

**Altres paràmetres**

- El nom de l'ordinador central és el nom complet que s'utilitzarà per identificar l'ordinador dins la xarxa. Aquest nom està format pel nom curt de l'equip més el nom del domini del centre. Convé que tengueu un criteri establert per identificar els equips del centre. Una bona política per anomenar màquines és utilitzar el darrer nombre de l'adreça IP. Així, si l'adreça IP d'aquesta màquina és 172.16.x.7, i com que es tracta d'un servidor tallafoc (firewall amb anglès), l'anomenarem *fw7*. El nom complet d'aquesta màquina en un domini *curs.local* és *fw7.curs.local.*
- El nom *zeroconf* és el nom curt és a dir, *fw7*.
- IP del servidor DNS (si teniu servidor Windows 2000, es recomana utilitzar-lo com a servidor DNS).
- El *gateway* o porta d'enllaç (la IP del *router* ).
- Dispositiu de la passarel·la: eth0

Si s'ha instal·lat entorn gràfic , és necessari configurar la targeta gràfica.

Convé instal·lar el carregador d'arrencada (LILO) en el Master Boot Record (MBR).

També és interessant configurar l'ús horari. Si teniu configurat un servidor NTP a la xarxa del centre, l'opció recomanada és *Sincronització automàtica d'hora usant NTP*. En aquest cas, s'haurà d'especificar l'adreça IP del servidor NTP.

A la pregunta “A quins serveis voleu permetre la connexió des d'Internet” deixau marcat l'opció “*Tot (sense tallafoc)*”.

Finalitzada la instal·lació caldrà reiniciar l'equip.

## CONFIGURACIÓ DEL TALLAFOC

Iniciau una sessió amb el compte *root*.

### Instal·lació de la utilitat fwexpautocfg

Configurau la font de programari educaib:

```
urpmi.addmedia educaib http://weib.caib.es/rpms-educaib/mdk-9.1 with ./hdlist.cz
```

Un cop configurada, executau

```
urpmi fwexpautocfg
```

Es crearà un nou directori */root/fwexpautocfg* amb els arxius de la utilitat.

### Adaptació del fitxer fwexpautocfg.conf

Editau el fitxer */root/fwexpautocfg/fwexpautocfg.conf* i modificau les variables segons els valors de

la xarxa del centre (si no s'ha instal·lat l'entorn gràfic podeu emprar l'editor **vi**):

**ip_eth0_lan_centre=** Adreça IP de la targeta de xarxa connectada a la xarxa del centre (*172.16.x.7)*

**ip_eth1_lan_exp=** Adreça IP de la targeta de xarxa connectada a la xarxa experimental (*192.168.1.1)*

**ip_lan_centre=** L'adreça IP de la xarxa del centre. (172.16.x.0)

**sm_lan_centre=** La submàscara de la xarxa del centre (255.255.255.0).

**ip_lan_exp=** L'adreça IP de la xarxa experimental. (192.168.1.0)

**sm_lan_exp=** La submàscara de la xarxa experimental (255.255.255.0).

**ip_servidor=** Adreça IP del servidor controlador del domini (*172.16.x.2)*

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

### Ús de fwexpautocfg

Un cop adaptat el fitxer de configuració ja s'està en situació d'usar la utilitat *fwexpautocfg*.

La primera vegada convé fer una execució de prova:

```
cd /root/fwaexpautocfg
./fwexpautocfg -test
```

Es crearà una carpeta anomenada *output* amb els fitxers que la utilitat crea o modifica. És convenient revisar una mica el contingut d'*output* per comprovar si les modificacions es realitzaran correctament.

Un cop executada la prova amb resultat satisfactoris, ja es pot habilitar el tallafoc executant:

```
./fwexpautocfg -habilita
```

A partir d'ara el tallafoc farà la seva funció: tallarà les connexions prohibides i deixarà passar les acceptades.

El tallafoc es mantendrà habilitat fins i tot si la màquina es reinicia.

Per a deshabilitar-lo, caldrà executar:

```
./fwexpautocfg -deshabilita
```

Quan el tallafoc està deshabilitat, ho deixa passar TOT; deixa realitzar qualsevol connexió entre la xarxa experimental i la xarxa del centre.

## CONFIGURACIÓ DEL TCP/IP EN ELS EQUIPS DE LA XARXA EXPERIMENTAL

La xarxa experimental usa les adreces de la xarxa de classe C 192.168.1.0/255.255.255.0. Per tant, les dades per configurar un equip qualsevol d'aquesta xarxa són:

**Adreça IP**: 192.168.1.x (per x<>1)

**Submàscara de xarxa**: 255.255.255.0

**DNS**: caldrà utilitzar servidors DNS públics, de fora del centre. Per exemple, els de Terra (195.235.96.90 i 195.235.113.3).

**Passarel·la** (porta d'enllaç): 192.168.1.1 (és l'adreça IP de la interfície de xarxa del tallafoc que està connectada a la xarxa experimental).