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 basat en Mandriva 2009 per separar una xarxa experimental de la xarxa del centre

Rafel Cortès Mora
Miquel Llobera Sancho
Damià Andreu Verger Vidal
Febrer 2009

Instal·lació i configuració d'un tallafoc basat en Mandriva 2009 per separar una xarxa experimental de la xarxa del centre

Índex de contingut

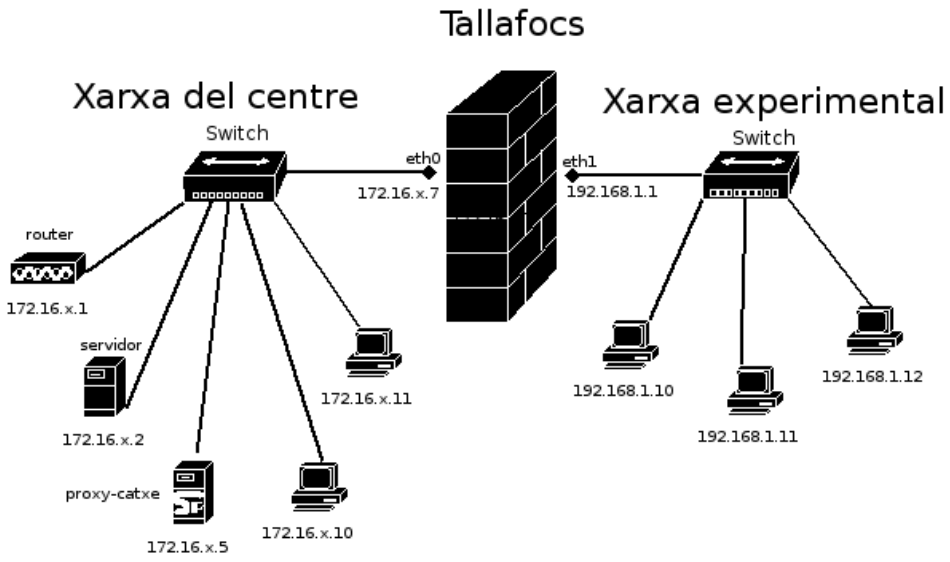
INTRODUCCIÓ

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 als 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 centcre	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 IP de les xarxes són:

Xarxa del centre: 10.216.x.0/255.255.255.y

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 10.216.x.8. 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.

Instal·lació del sistema operatiu

Per fer la instal·lació amb Mandriva 2009 és necessari disposar del DVD Mandriva Linux 2009 Free o bé dels dos CD de Mandriva Linux 2009 Free. Podeu trobar les imatges ISO del DVD i dels CD a ftp://ftp.rediris.es/pub/mirror/mandriva/iso/2009.0

L'ISO del DVD s'anomena *mandriva-linux-free-2009-dvd-i586.iso*

Els dos CD són: *mandriva-linux-free-2009-cdx-i586.iso*, per a x=1,2

Si l'ordinador on s'ha de realitzar la instal·lació disposa de lector de DVD es recomana emprar la instal·lació basada en aquest suport ja que la instal·lació per mitjà dels 2 CD té l'inconvenient de que requereix el canvi de CD unes quantes vegades.

També és necessari disposar del fitxer ***fwexpmdv09.txt*** que trobareu adjunt a aquest document. Per a poder emprar-lo durant la instal·lació és necessari guardar-lo a un disquet o a un llapis de memòria USB (si el PC on es realitza la instal·lació no disposa de disquetera).

- Iniciau la instal·lació amb el DVD o amb el CD 1 (cas de no disposar de lector de DVD).
- Triau *Install Mandriva Linux 2009 in your system*
- S'iniciarà la instal·lació. Si l'instal·lador apareix en mode text, reiniciau la instal·lació amb una resolució de 640 x 480 (la resolució de pantalla emprada per l'instal·lador es pot canviar prement F3 - F3).
- A la pantalla d'elecció d'idioma, triau *Europa* - *Català*
- Tot seguit acceptau l'*acord de llicència*
- Si al disc hi ha altres instal·lacions de Mandriva, l'instal·lador demana si es tracta d'una actualització o bé d'una instal·lació nova. Triau *Instal·lació* per indicar que voleu una instal·lació des de zero.
- El programa d'instal·lació demanarà les particions on s'ha d'instal·lar Linux. Triau *particionament personalitzat del disc*. Esborrau particions anteriors (si cal). En disposar d'espai suficient (amb 20Gb n'hi ha prou, encara que també es pot instal·lar amb menys), podeu usar l'assignació automàtica (*canvia al mode expert* i *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 la grandària recomanada és:

/	sistema (doble del proposat màx. 2Gb)
swap	intercanvi (espai proposat)
/usr	programes d'usuari (40% de l'espai restant, màx. 8GB)
/var	contingut variable (20%)
/tmp	temporal (20%)
/home	resta d'espai

  Fet – D'acord per confirmar l'escriptura de la taula de particions.
- El programa d'instal·lació demanarà quins suports d'instal·lació disposau (hauríeu de tenir o bé el DVD o bé els dos CD). Premeu *Següent*.
- Contestau *Cap* a la pregunta de si es disposa de més suports. Premeu *Següent*.
- A la pantalla de selecció de grups de paquets, triau *Instal·lació personalitzada*. *Següent*.
- El programa d'instal·lació demanarà la selecció de paquets a instal·lar. Marcau "Selecció individual de paquets" i premeu *Següent*.
- Tot seguit apareixerà la pantalla de selecció individual de paquets. No cal que en seleccioneu cap, sinó que introduïu el disquet que conté la llista de paquets a instal·lar a la disquetera i premeu sobre la icona que simbolitza un disquet. Si emprau un llapis USB, connectau-lo a la interfície USB. Si el programa no el detecta tornau a la passa anterior, connectau el llapis USB a

la interfície USB i tornau a prémer la icona del disquet.

- Escolliu l'opció *Carrega + D'acord* i després *Disquet (fd0)* per llegir la llista de paquets a instal·lar des del disquet. Si emprau un llapis USB, s'ha de fer doble clic sobre la unitat corresponent.
- Quan surti la llista de fitxers del disquet, seleccionau *fwexpmdv09.txt* (el fitxer que conté el llistat de paquets) i premeu *D'acord*
- Si el procés ha anat bé (no retorna cap error), hauran quedat seleccionats els paquets de la llista inclosa al fitxer *fwexpmdv09.txt.* Premeu *Instal·la* per iniciar la instal·lació. El programa d'instal·lació us avisarà que s'ha elegit la instal·lació del servidor *openssh-server* i demanarà confirmació per procedir a la instal·lació. Triau *Sí* i continuau. Com ja s'ha esmentat abans, si s'utilitzen CD, el programa d'instal·lació demanarà canvi de CD en bastants ocasions.
- Tot seguit, apareix la pantalla d'administrador d'usuaris. Entrau una contrasenya per a *root*. També, el programa d'instal·lació requereix la creació d'un usuari local diferent de *root*. Per unificar proposam anomenar aquest usuari *usulocal* (tant a nom real com a nom d'accés) amb contrasenya la mateixa que *root.*
- Carregador de l'arrencada. L'instal·lador demanarà on voleu instal·lar el carregador de l'arrencada (Mandriva 2009 instal·la el *Grub*). Normalment convendrà instal·lar el carregador al *primer sector de la unitat (MBR)*, però si es vol fer servir un altre carregador, com per exemple el GAG, serà necessari instal·lar el carregador al *primer sector de la partició de root*.
- A l'apartat Resum caldrà configurar, com a mínim, la xarxa, la targeta gràfica (normalment la targeta gràfica es detecta automàticament) i el rellotge.
- Per configurar la xarxa, s'ha d'especificar el següent:
  1. Connexió: triau *Ethernet*
  2. Els punts següents indiquen com configurar la interfície *eth0*, però com que a priori no sabem quina de les dues que ens surten per pantalla és, triau la primera de la llista. Més endavant podreu saber si heu configurat *eth0* o bé *eth1*.
  3. Configuració manual (ip estàtica)
  4. L'adreça IP de l'equip i la submàscara de la xarxa. Podem considerar el tallafoc com un servidor i, per tant, recomanam que li assigneu una IP dintre del rang de les deu primeres.
  5. La passarel·la o *gateway* (generalment, el *router* ADSL del centre).
  6. IP del servidor DNS (si teniu servidor Windows 2000 o 2003 com a controlador del domini, és necessari utilitzar-lo com a únic servidor DNS).
  7. El nom de l'ordinador 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; per exemple, una bona política per anomenar màquines és utilitzar el nom del sistema operatiu i el darrer nombre de l'adreça IP. Així, si l'adreça IP d'aquesta màquina és 10.216.x.8, i com que es tracta d'un servidor tallafoc (*firewall* en anglès), el podeu anomenar *fw8* o millor *fw8mdv09* si voleu especificar el sistema operatiu. El nom complet d'aquest sistema a un domini *curs.local* seria, respectivament, *fw8mdv09.curs.local*.
  8. Premeu *Següent*. Ara s'ha de configurar el control de la connexió:

     Permetre als usuaris administrar la connexió: NO

     Iniciar la connexió quan la màquina arranqui: SÍ.

9. Finalment, es demanarà si voleu iniciar la connexió ara. Triau SÍ i podrem comprovar-la.
10. És important que comproveu si la interfície configurada és l'*eth0* o l'*eth1*, ja que és necessari que sigui l'*eth0*. Canviau a mode consola prement *Ctrl-Alt-F2*, i executau la comanda ***ifconfig***. En cas que la comanda ifconfig no anàs bé una altre possibilitat es escriure la següent comanda

    ```
    ls /mnt/etc/sysconfig/network-scripts/ifcfg-et*
    ```

    Amb aquesta comanda la màquina ens contestarà si hem configurat eth0 o eth1

    Si la interfície configurada és l'*eth0* podeu continuar al punt següent (tornau a la pantalla corresponent a la instal·lació prement *Ctrl-Alt-F7*), en canvi si és l'*eth1* repetiu aquestes passes de configuració (*Ctrl-Alt-F7* i tornau al punt 2) però seleccionant ara la segona interfície de la llista.

- Per configurar la interfície de xarxa corresponent a la xarxa experimental, l'*eth1*, tornau a accedir a la configuració de xarxa i especificau el següent:
    1. Connexió: triau *Ethernet*
    2. Com que ara ja heu configurat l'*eth0*, ara heu de triar l'altra de la llista, es tracta de l'*eth1*.
    3. Configuració manual (ip estàtica)
    4. L'adreça IP dins la xarxa experimental i una submàscara de xarxa. Seguint l'exemple, 192.168.1.1/255.255.255.0
    5. La passarel·la o *gateway*: deixau-ho en blanc.
    6. IP del servidor DNS: deixau-ho en blanc.
    7. Nom de l'ordinador: introduïu el mateix que heu utilitzat quan heu configurat l'anterior interfície de xarxa.
    8. Premeu *Següent*. Ara s'ha de configurar el control de la connexió:

        Permetre als usuaris administrar la connexió: NO

        Iniciar la connexió quan la màquina arranqui: SÍ.
    9. Finalment, es demanarà si voleu iniciar la connexió ara. Triau SÍ i podrem comprovar-la.
    10. Per comprovar que heu configurat correctament les dues interfícies de xarxa, canviau a mode consola prement *Ctrl-Alt-F2*, i executau la comanda ***ifconfig***.

        En cas que la comanda ifconfig no anàs bé una altre possibilitat es escriure les següents comandes

        ```
        more /mnt/etc/sysconfig/network-scripts/ifcfg-eth0
        ```

        ```
        more /mnt/etc/sysconfig/network-scripts/ifcfg-eth1
        ```

        Heu de veure *eth0* (amb una IP de la xarxa vostra) i *eth1* (amb una IP de la xarxa experimental). Tornau a la pantalla corresponent a la instal·lació prement *Ctrl-Alt-F7.*
- Per configurar el rellotge, anau a *Fus horari – Configura* i triau *Madrid* com a zona horària. Després, marcau *Reloj interno puesto en hora UTC* i *Sincronització automàtica de l'hora (usant NTP)* i escolliu *Europa - Todos los servidores*.
- Nivell de seguretat: Alt
- Tallafoc, inhabilitau-ho: *Tallafoc - Configura* i seleccionau *Tot (sense tallafoc)*.
- Continuau amb la instal·lació. No és necessari actualitzar ara els paquets instal·lats; ja ho farem quan sigui necessari.

- Un cop acabada la instal·lació, extraieu el CD i el disquet, i reiniciau l'equip.

CONFIGURACIÓ DEL TALLAFOC

Iniciau una sessió amb el compte *root*.

Comprovau que teniu accés a internet executant

```
ping dweib.caib.es
```

Si no teniu accés repassau el contingut dels fitxers **ifcfg-eth0** i **ifcfg-eth1** que es troben a */etc/sysconfig/network-scripts* (vegeu el contingut dels fitxers que hem utilitzat a l'exemple)

/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
IPADDR=10.216.254.8
NETMASK=255.255.255.192
GATEWAY=10.216.254.1
ONBOOT=yes
METRIC=10
MII_NOT_SUPPORTED=no
USERCTL=no
DNS1=10.216.254.2
RESOLV_MODS=no
IPV6INIT=no
IPV6TO4INIT=no
```

/etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
IPADDR=192.168.1.1
NETMASK=255.255.255.0
ONBOOT=yes
METRIC=10
MII_NOT_SUPPORTED=no
USERCTL=no
RESOLV_MODS=no
IPV6INIT=no
IPV6TO4INIT=no
```

Fixau-vos que el fitxer *ifcfg-eth1* no conté ni `GATEWAY` ni `DNS1` (si les trobau eliminaules. Amb l'editor **vi** les línies s'eliminen prement dues vegades la tecla 'd')

Si necessitau fer-hi modificacions reiniciau després la xarxa amb:

```
/etc/init.d/network restart
```

Instal·lació de la utilitat fwexpautocfg

Configurau la font de programari educaib:

```
urpmi.addmedia educaib http://dweib.caib.es/rpms-educaib/mdv09 with media_info/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 emprant l'editor **vi**:

```
vi /root/fwexpautocfg/fwexpautocfg.conf
```

ip_eth0_lan_centre= Adreça IP de la targeta de xarxa connectada a la xarxa del centre (*10.216.x.8)*
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. (10.216.x.0)
sm_lan_centre= La submàscara de la xarxa del centre (255.255.255.y).
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 (*10.216.x.2 o 10.216.x.4)*
ip_administracio= Adreça IP de l'equip que s'utilitza habitualment per administrar la xarxa.

En acabar prem <*Esc*>. Guardau les modificacions pitjant ":w" i <*Enter*>. Per sortir ":q" i <*Enter*>

Ús d'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. Podeu fer servir l'ordre *cat* per visualitzar el contingut dels fitxers.

Un cop validat el test, 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 ALS 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).