Linux Avanzado

Virtualització de Sistemes. VirtualBox

Instal·lació

VirtualBox és un excel·lent programari de virtualització que ens permet executar altres sistemes operatius com qualsevol distribució de Linux ,WindowsXP o Windows Vista en Ubuntu. A partir de la versió 1.5, VirtualBox integra el que s'anomenen finestres Seamless, és a dir, que els programes virtualitzats es mostren en el sistema operatiu com finestres corrents.

La pàgina web del programa és http://www.virtualbox.org/ i des d'ella ens podem baixar e instal·lar el programa per a Ubuntu.

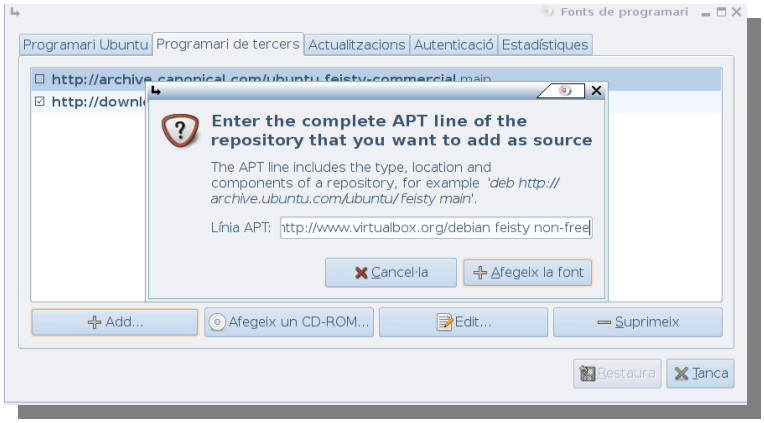
Aquest programa està en dos modalitats diferents, la versió lliure amb llicència GPL que no té suport de USB ni de RDP, i la versió que té suport de USB i pantalla Remota i no és lliure.

En la pàgina de http://www.virtualbox.org/ sols ens podem descarregar la versió no lliure i està en l'apartat downloads. Per a instal·lar-la ho podem fer de 2 formes, fent clic al damunt de i386 en "Ubuntu 7.04 ("Feisty Fawn") i386" i instal·lar-la amb el *gdebi*, o afegir el repositori de VirtualBox als nostres orígens de programari. Ambdós formes són correctes, però amb la segona no ens tindrem que preocupar d'assabentar-nos quan ha eixit una versió nova per a instal·lar-la.

La cadena que cal afegir per a Ubuntu Feisty tal com mostra la pàgina de Downloads és:

```
deb http://www.virtualbox.org/debian feisty non-free
```

I l'haurem d'afegir manualment a l'arxiu /etc/apt/sources.list o també emprant l'eina "Orígens del Programari" que es troba en "Sistema → Administració"



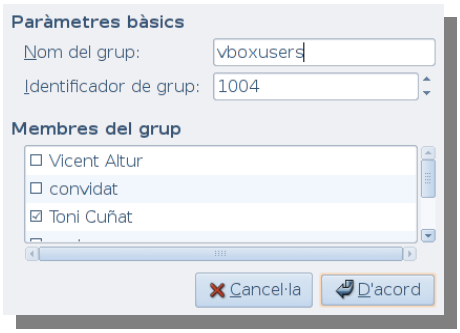
Ara simplement el podrem instal·lar amb el synaptic o des de la línia d'ordres:

```
sudo apt-get install virtualbox
```

Hem de tindre en compte, que et requereix acceptar una llicència d'ús (la versió no lliure), i que segurament estarà ocult en la finestra del progrés d'instal·lació del synaptic.

Per tal que funcione, el nostre usuari ha d'estar en el grup vboxusers, així que el podem afegir des de l'eina de gestió d'Usuaris i Grups en el menú d'administració. Una vegada hem accedit a aquesta

finestra hem de polsar al damunt de “Gestiona els Grups”, seleccionar el grup vboxusers i marcar propietats. Des d'aquesta finestra podrem afegir el nostre usuari al grup vboxusers.



També ho podem fer des de la línia d'ordres:

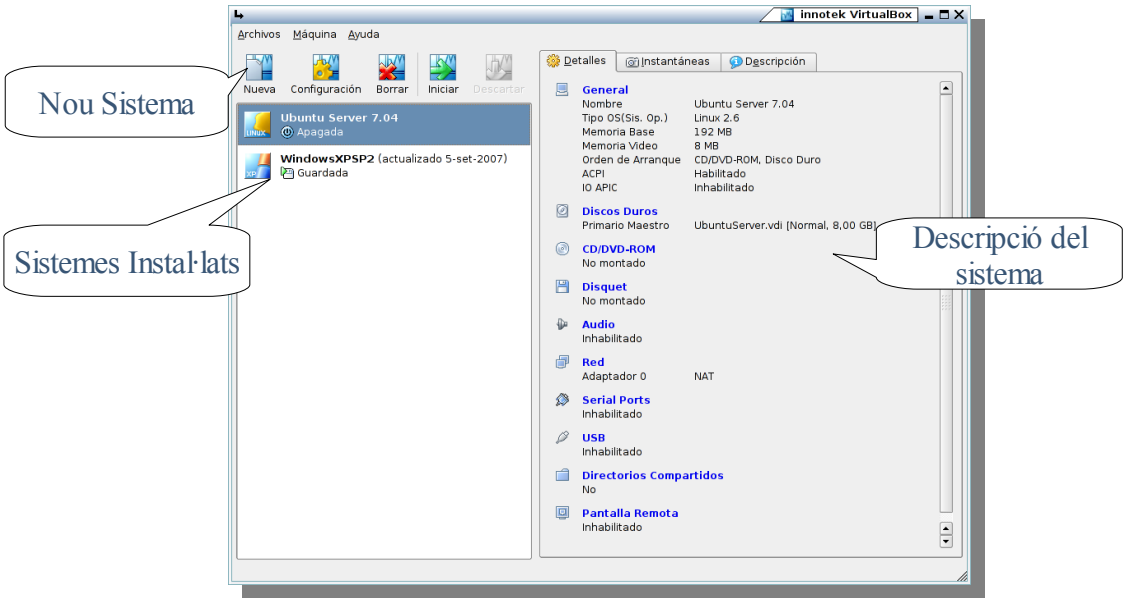
```
sudo usermod -G vboxusers -a el teu usuari
```

Caldrà tancar la sessió per a que els canvis de grup facen efecte.

També caldrà

Primeres passes

Per tal d'iniciar el VirtualBox ho podem fer des del menú Aplicacions → Eines del Sistema → Innotek VirtualBox. La pantalla que ens mostrarà serà semblant a aquesta:

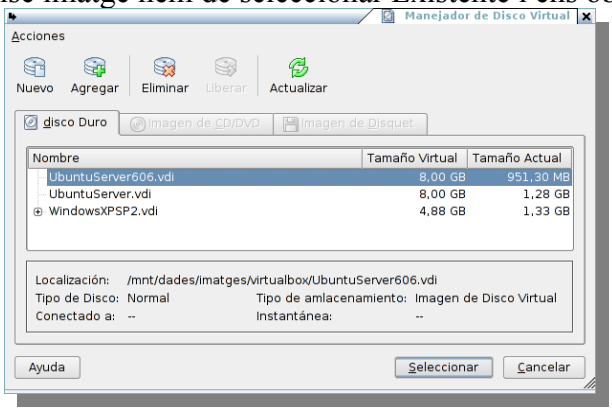


Per tal d'afegir una nova màquina, polsem el botó Nueva. Ens obrirà un assistent que ens ajudarà a configurar la màquina virtual pas per pas.

- ✔ Se'ns presenta l'assistent i avancem (Siguiente)
- ✔ Posem el nom que li volem donar a la màquina virtual (Ubuntu 606 Server, en el nostre cas), i seleccionem el sistema (Linux 2.6)
- ✔ **Memòria:** És la memòria RAM que li anem a donar al nostre sistema hoste. En el nostre cas

amb 128 MB ja anirà bé.

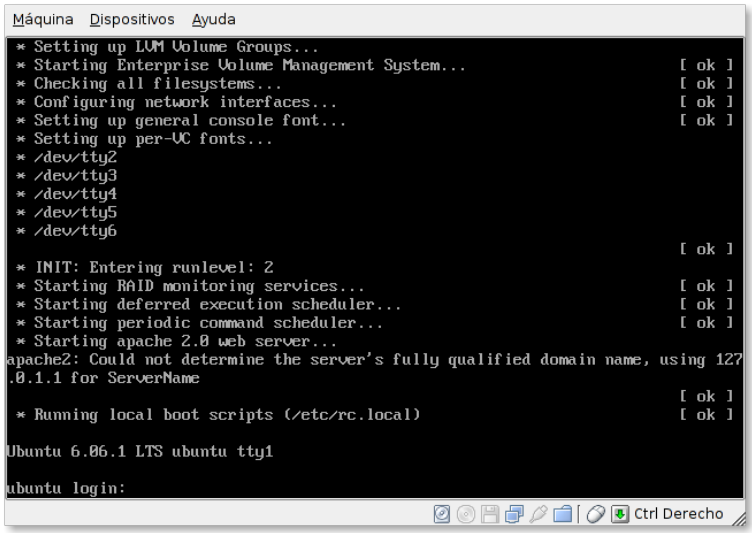
- ✔ **Disco Duro Virtual:** És una porció del nostre disc dur real on es va a instal·lar el sistema hoste i les seues aplicacions. Podem crear-ne un de nou Seleccionant Nuevo o emprar un ja creat amb antelació.
  - ✗ En el nostre cas emprarem una imatge de disc creada amb antelació, on ja ha estat instal·lat el Ubuntu Server 6.06.
  - ✗ Per a afegir el disc imatge hem de seleccionar Existente i ens obrirà una altra finestra.



  - ✗ Hem de polsar el boto Agregar per a escollir l'arxiu d'imatge de disc. Una vegada afegit a la llista de discs virtuals disponibles, sols cal seleccionar-lo.
- ✔ Per a acabar ens informa de la configuració bàsica.

Amb tot açò ja tenim una configuració bàsica de la màquina virtual, amb la que podrem iniciar-la prement el botó Iniciar.

Ens iniciarà una nova finestra on arrancarà el sistema que li hem configurat.



Configuracions Addicionals

Si hem creat una màquina nova per tal d'instal·lar un sistema nou en ella (en el nostre cas ja estava instal·lat) segurament haurem seleccionat l'opció de crear un nou disc imatge.

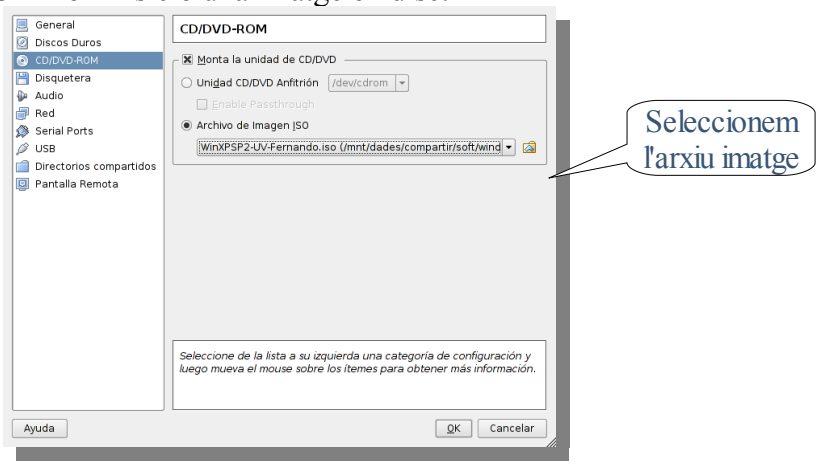
Haurem comprovat que si li donem a inicia la màquina no passa res e absolut, òbviament és degut a que no hi ha cap sistema en el disc que hem creat de nou.

El més habitual és tenir el sistema a instal·lar en CD, així que una vegada creat la configuració per al sistema nou, podem configurar més paràmetres com ara el CD d'on iniciarà el sistema.

Podem accedir a les preferències esteses mitjançant el botó configurar, o també accedir a certes parts de la configuració des de la pestanya Detalles.

Entre els paràmetres que podem configurar estan:

- ✔ General: On podrem canviar la RAM del sistema
- ✔ Discos Duros: On podrem seleccionar un o varies imatges de disc més.
- ✔ CD/DVD-Rom: Ací és on hem de configurar la imatge d'inici del sistema que vullgam instal·lar. Pot ser un CD-Rom físic o una imatge en disc.



- ✔ Disquetera i Audio, on respectivament podrem habilitar la disquetera i l'àudio.
- ✔ Red: Des d'ací podrem crear fins a 4 targetes ethernet virtuals. Hem de tenir seleccionat “Conectar a NAT” per a tindre accés a la xarxa des de la màquina virtual.
- ✔ Serial Ports i USB ens permet simular i passar dispositius serie/USB a la màquina hoste.
- ✔ Directorios compartidos: El que fa es crear un recurs compartit samba accessible des de la màquina hoste. També es pot accedir a un recurs compartir que es tinga en l'amfitrió amb antelació tenint en compte que la IP de l'amfitrió és 10.0.2.2, de forma que si hem creat un recurs que es diu “compartir” i el sistema hoste és Windows podrem connectar-nos amb:
  - ✗ \\10.0.2.2\compartir
- ✔ Pantalla remota permet l'accés des d'una altra màquina al VirtualBox emprant el protocol RDP.

Execució de Programari de Windows en Linux. Wine

Introducció

-Què és WINE? Segons la Wikipedia “és una reimplementació de la API de Win16 i Win32 per a sistemes operatius basats en Unix sota plataformes Intel. Permet l'execució de programes per a MS-DOS, Windows 3.11, Windows 95, Windows 98, Windows Em, Windows NT, Windows 2000 i Windows XP”

Com la API de Windows no està completament documentada, els és molt difícil implementar-la al 100%, amés que canvia depenent del sistema.

Instal·lació

Ubuntu ja porta en els seus repositoris el WINE, però en el nostre cas instal·larem des de la pàgina del wine una versió més actual, amés de que ens permetrà tenir el wine actualitzat en quan aparega una nova versió.

Ens disposem a anar a la web del projecte wine (http://www.winehq.org/) i des d'ahí al apartat de Downloads de Ubuntu (http://www.winehq.org/site/download-deb).

Ací ens diu com afegir-lo al repositori, des d'un terminal escrivim:

```
sudo wget http://wine.budgetdedicated.com/apt/sources.list.d/feisty.list -O /etc/apt/sources.list.d/winehq.list
```

(Ens serà més fàcil copiar-ho i pegar-ho des de la pàgina web)

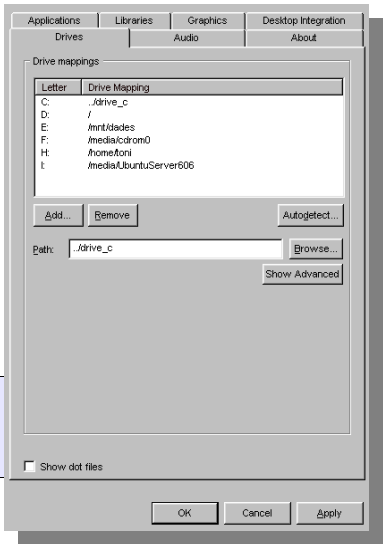
Si anem als “Orígens de programari” podrem comprovar que ja està afegit. Ara procedirem a instal·lar-lo des del synaptic (abans hem de refrescar per a que actualitze els origens de programari).

Configurar Wine

Encara que hem instal·lat WINE, no està configurat. Per tal de configurar-lo hem d'executar la ordre:

```
winecfg
```

El que ens obrirà una nova finestra on podem configurar certs paràmetres en general, com ara els discs que veurà l'aplicació executada amb wine.



Hem de tindre en compte que podem tenir també una configuració per a cada aplicació. Açò serà útil ja que depenent de l'aplicació ens caldrà tindre una configuració o una altra.

Habitualment, els programes més senzills funcionaran correctament amb la configuració per defecte, i sols caldrà executar winecfg i prémer el botó de OK.

Hem de tenir en compte que el procés de configuració crea un "mini entorn de Windows" en nostre "directori d'usuari "/.wine

```
toni@alabulie:~/.wine$ ls
dosdevices  drive_c  system.reg  userdef.reg  user.reg
```

drive_c és el que veurem com a disc dur C:\ en l'aplicació i on instal·larem habitualment els programes.

Una vegada hem configurat el wine amb el winecfg, ja podrem executar algunes aplicacions dissenyades per a Windows.

Per a executar una aplicació amb el wine podem escriure:

```
wine ruta/aplicació.exe
```

O també des del navegador d'arxius amb el botó de la dreta "Obre amb altra Aplicació" i escollir WINE.

Si tot ha anat bé podrem accedir a l'aplicació que hem instal·lat en ~/.wine/drive_c i executar-la des d'ahí.

En les versions més modernes del sistema, és habitual que apareguen les aplicacions instal·lades amb wine al menú Aplicacions → Wine

```
Exercici: Instal·lació d'una aplicació.

Instal·larem l'aplicació DVDSrink que serveix per a recomprimir pel·lícules
de DVD9 a DVD5. La podem baixar de:

http://dvd-shrink.softonic.com/

La descomprimim, i procedim a executar l'arxiu de setup.exe. Amb açò
tindrem aquesta aplicació instal·lada i funcional.
```

Avui en dia funcionen aplicacions tal com el Photoshop, Flash o Dreamweaver.

Instal·lació del Internet Explorer

Abans de procedir a instal·lar el Internet Explorer en Linux mitjançant el Wine, és convenient instal·lar les tipografies que venen per defecte amb Windows al nostre sistema, a tal de que es vegen les pàgines igual en Windows.

Amb açò matarem dos pardals d'un tir, ja que també estaran disponibles per al OpenOffice.org, de forma que quan ens passen un document de Microsoft Office tindrem una major compatibilitat.

El paquet que instal·la les fonts de Microsoft (a través de la Xarxa) és el msttcorefonts. Podem instal·lar-lo des de synaptic o mitjançant apt:

```
sudo apt-get install msttcorefonts
```

El que fa es baixar-se les fonts i instal·lar-les al sistema. Per problemes legals aquestes tipografíes no poden ser incloses en els repositoris/CD-Rom d'Ubuntu.

Una vegada instal·lades les fonts, procedirem a instal·lar el Internet Explorer. Per a tal cosa emprarem un script en bash que ens automatitza la feina, descarregant-se'l d'Internet i creant-li un entorn propi de wine. Aquest script el podem trobar en:

http://www.tatanka.com.br

On seleccionem l'idioma Español i el descarreguem des de:

http://www.tatanka.com.br/ies4linux/download.html

El descomprimim, i posteriorment l'executem

També podem executar el script que mostra en la pàgina que ho automatitza tot:

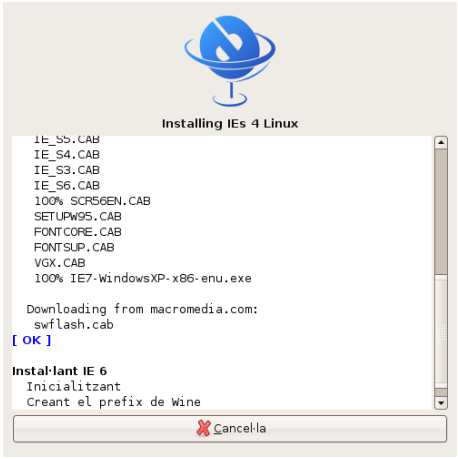
```
wget http://www.tatanka.com.br/ies4linux/downloads/ies4linux-latest.tar.gz
tar zxvf ies4linux-latest.tar.gz
cd ies4linux-*
./ies4linux
```

Les noves versions ja tenen suport d'interfície gràfica, i amés ens permetran instal·lar el Internet Explorer 7 (encara en fase de proves)

```
wget http://www.tatanka.com.br/ies4linux/downloads/ies4linux-
2.5beta6.tar.gz
tar zxvf ies4linux-2.5beta6.tar.gz
cd ies4linux-*
```

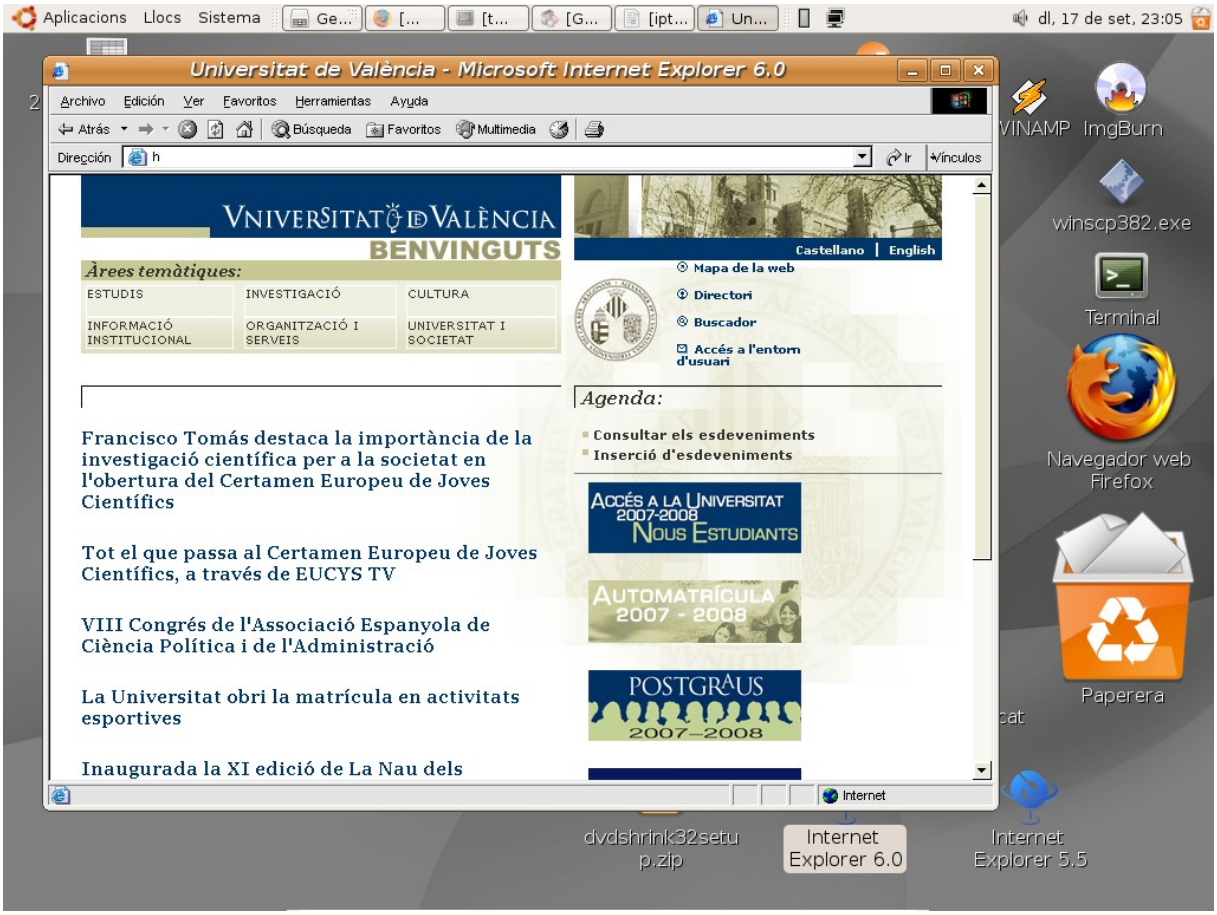
i hem d'executar el script passant-li paràmetres addicionals si volem que instal·le el motor del IE7:

```
./ies4linux –hack-ie7-proxy-settings
```



Si en les opcions avançades seleccionem IE7 ens instal·larà el Internet Explorer 6 i posteriorment el Internet Explorer 7. Encara que el que fa realment és instal·la el motor del IE7 en el IE6, i dona prou problemes.

> *També hem de tindre en compte que apart de poder executar aplicacions de windows desde Wine, podem instal·lar un sistema Windows en una màquina virtual i posteriorment instal·lar les aplicacions en la màquina virtual. Açò encara que té molta més compatibilitat que el wine, té com a desavantatges que consumeix més recursos i amés caldrà sumar el preu de la llicència del Sistema Windows instal·lat.*



Escalat de privilegis. Sudo

Tots els sistemes tipus Unix (com els BSD i Linux) posseeixen un superusuari (root) a través del qual es domina el sistema. Sens dubte açò pot ser un problema de seguretat, pot presentar-se la situació en la qual diverses persones estan treballant i han de realitzar algunes operacions que requereixen els drets del root, de manera que no queda altra opció que donar-li la preciosa contrasenya, cosa que és un perill.

També pot passar que al estar emprant el sistema en mode root ens enganyem amb alguna ordre i li fem malbé al sistema.

Algunes de les preguntes que més es repeteixen quan algú que no coneix Ubuntu ho instal·la per primera vegada tenen relació amb sudo:

- On està el compte de root?
- Necessite executar l'ordre "X" com root i no em funciona el su.

Per defecte a Ubuntu el compte de root esta bloquejat. Això significa que no ens podem autenticar com a superusuari. Durant la instal·lació Ubuntu dona permís a l'usuari principal per executar comandes com a superusuari mitjançant sudo.

Però, qué és sudo?

És programa que permet que usuaris o grups normals prenguen drets de root per a ordres específiques sense conèixer la contrasenya del root, de manera que puguen realitzar la seua labor sense posar en perill el sistema.

Aleshores, eixe usuari és root?

No, ni de bon tros, aquest usuari pot fer totes les tasques que fa root però sempre que mostre l'autorització. Hem de tindre en compte que:

- La contrasenya que cal introduir és la del usuari no la del superusuari (per aquesta raó no cal contrasenya de root a Ubuntu)
- La contrasenya es emmagatzemada per defecte durant 15 minuts. Passat aquest temps es necessari posar una altra vegada la contrasenya.
- La contrasenya no es mostra per pantalla ni tan sols amb els asteriscs!.
- Les aplicacions dels menús que necessitin permisos de superusuari preguntaran una contrasenya.
- Per a les aplicacions gràfiques cal utilitzar gksudo. Amb kde cal utilitzar kdesudo.

```
toni@europa:~$ gksudo synaptic
```

Avantatges de sudo

- L'instal·lador d'Ubuntu ha de fer menys preguntes
- Els usuaris no han de recordar una contrasenya extra
- Evita que els usuaris ho puguin fer tot per defecte. Abans de fer cap canvi important es pregunta una contrasenya. Això permet pensar en les conseqüències del que fem abans de fer-ho.
- Sudo afegeix un entrada en un fitxer de registre (/var/log/auth.log).
- El password de root no el sap ningú. Augmenta la seguretat ja que els atacants no poden utilitzar l'usuari root.
- Permet administrar de forma més granular els permisos dels usuaris i per tant la política de seguretat de ela màquina.

Configuració de Sudo

La configuració de sudo es troba a l'arxiu /etc/sudoers. En aquest fitxer s'indiquen els usuaris que tenen permís per executar sudo.

La sintaxis de Sudoers

Sintaxis básica

```
usuari hoste = ordres
```

Aquesta sintaxi li diu a sudo que l'usuari, identificat com usuari i connectat a través del sistema hoste, pot executar qualsevol de les ordres llistades en **ordres** com usuari root. Un exemple més real podria ser més clarificador: permetre a l'usuari toni executar halt si està connectat des del sistema (i no a través de ssh):

```
toni localhost = /sbin/halt
```

Podríem crear un grup *apagar*, i permetre a tots els usuaris d'aquest grup que apagaren el sistema o el reiniciaren. La sintaxi per als grups és amb un % davant. Veguem un exemple:

```
%apagar localhost = /sbin/shutdown, /sbin/halt, /sbin/reboot
```

L'arxiu de sudoers està partit en tres seccions:

Les definicions de alies, les opcions per defecte i les regles d'accés. en el cas anterior, haguérem pogut fer un alias de les ordre per a apagar, a tal de podre-lo aprofitar en altres regles. Per Exemple:

```
Cmnd_Alias SHUTDOWN_CMDS = /sbin/shutdown, /sbin/halt, /sbin/reboot
```

%apagar localhost = SHUTDOWN_CMDS

Hi han quatre tipus d'alias diferents, dels quals acabem de veure'n un (Cmnd_alias) i son:

- Cmnd_Alias per a ordres
- User_Alias per a usuaris
- Runas_Alias per a usuaris privilegiats
- Host_Alias per a hosts

Existeix un alies especial, ALL, que s'utilitza per a englobar a totes les ordres, usuaris, usuaris privilegiats o hosts.

També és possible tenir un usuari per a executar una aplicació com altre usuari distint de root. Açò pot ser molt interessant si executa aplicacions com un usuari diferent (per exemple, apatxe per al servidor web). Per exemple, volem que l'usuari *toni* siga capaç d'executar apache com a usuari *www*

toni localhost = (www) /usr/bin/apache

Sols ens queda executar el apache (passant-li com a paràmetre -u nom_usuari):

```
sudo -u www /usr/bin/apache
```

Com hem vist abans, si ometem l'usuari privilegiat, executa l'ordre com a usuari root.

Anem doncs a veure la configuració que porta Ubuntu per defecte per a sudo. Caldrà doncs editar l'arxiu /etc/sudoers. És convenient editar-la amb l'ordre visudo, ja que aquesta bloqueja altres accesos al mateix arxiu. Escrivim *sudo visudo* des de la línea d'ordres:

```
# Cmnd alias specification
# Defaults
Defaults        !lecture,tty_tickets,!fqdn
# User privilege specification
root    ALL=(ALL) ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

Si ens fixem en la quinta línia (*root ALL=(ALL) ALL*) podem entendre que l'usuari root pot executar qualsevol aplicació, des de qualsevol màquina com a qualsevol usuari.

La última línia ens diu una cosa molt interessant, i és que tots els usuaris que estiguen en el grup *admin* podran executar qualsevol aplicació com a qualsevol usuari (per defecte root) des de qualsevol màquina connectada.

Açò és molt il·lustratiu, ja que permet a qualsevol usuari que estiga en el grup *admin* realitzar tasques d'administració, així doncs tenim un o varis administradors sense ser-ho realment.

Existeix una última possibilitat, i és poder eliminar la petició de contrasenya per a executar un o diversos comandos. Es tracta de les etiquetes NOPASSWD i PASSWD. Són opcionals i per defecte s'assumeix PASSWD.

```
usuari host = (usuariprivilegiat) NOPASSWD: ordre
```

Al igual que podem permetre escalar privilegis per a aplicacions, també podem impedir posant un ! davant de l'ordre. Exemple

```
toni      localhost = /usr/bin/passwd [a-zA-Z0-9_-]*, !/usr/bin/passwd root
```

Que permet canviar tots les contrasenyes excepte la de l'administrador.

Exercici:

Crea un usuari amb el teu nom i que no estiga en el grup *admin*.

-Permet a l'usuari reiniciar el sistema, però no li permetes apagar-lo.

-Permet a l'usuari afegir programes (apt-get, aptitude) sense que li demane contrasenya.

Firewall - Iptables

Introducció al filtrat amb IPTABLES

Al connectar-nos a Internet en les nostres cases, de forma explícita ens estem connectant, en AMBDÓS sentits. Mitjançant iptables, assolir certa protecció i seguretat. Noteu que un tallafocs no garanteix 100% de seguretat.

Iptables és una aplicació en línia d'ordres que gestiona el filtrat de paquets en sistemes Linux (kernels 2.4.x), sobre la base de les regles que hàgim definit. Iptables és molt més potent que el seu antecessor Ipchains (kernels 2.2.x).

Cap destacar que per a utilitzar iptables, és necessari tenir un kernel preparat per a aquest, i el mòdul iptables carregat.

Iptables s'encarrega de donar-li directives al kernel, sobre filtrat de paquets TCP/IP. Un paquet TCP/IP consta de diversos camps, amb informació addicional a les dades que es transmeten en si. No ve al cas descriure cadascun d'ells, sinó els quals considerarem mes rellevants, és a dir, aquells camps que mitjançant iptables, començarem a "vigilar". Exemple: adreça origen, adreça destinació, port origen, port de destinació, etc.

Com funciona?

L'estructura de Iptables és bàsicament una cua : quan un paquet arriba, aquest és validat contra cadascuna de les regles del firewall, en el moment que alguna regla casa (match) , s'executa l'acció que hagi estat definida en la regla (descartar el paquet, acceptarlo, enrutarlo, etc).

El kernel de linux posseeix (predefinides "de fàbrica") 3 cadenes (chains) de regles:

INPUT (Entrada), **FORWARD** (Reenviar) i **OUTPUT** (Eixida).

Cada paquet TCP/IP que ingressa/travessa/ix des de/cap a una màquina amb iptables funcionant, passarà per la cadena **INPUT**, **FORWARD** o **OUTPUT** respectivament. Les cadenes,no són mes que un llistat de regles, amb les quals controlem cadascun dels paquets que passen. Ara es preguntaren, que és una regla?.

Per a evitar les confusions, anem a simplificar la seua definició al màxim, i després mostrar-los alguns exemples. Una regla consta de 2 parts, i no és mes que una condició i una acció. Si es compleix la condició s'executa l'acció. Simple, veritat?

Una mica per a tenir en compte mes avant: si un paquet va travessar totes les regles d'una cadena, sense trobar coincidència, iptables es fixarà en la política per defecte d'aqueixa cadena (default policy).

Sintaxis de Iptables

L'estructura d'una ordre iptables és la següent :

```
iptables -t %[taula] -%[ADLF...] %[regla] %[criteri] -j %[acció]
```

-t %[taula]	Aquesta part de l'ordre especifica com és la taula en la qual volem afegir la regla. Existeixen 2 tipus de taules vàlides : **nat** i **filter**, sent **filter** la taula per defecte si és omesa en l'ordre. Nat es refereix a les connexions que seran modificades pel firewall, com per exemple, emmascarar connexions, realitzar redireccions de ports, etc. Filter és la taula on s'afegixen les relacionades amb el filtrat.
-%[AIRDLFZNXP] %[regla]	Hi ha 4 opcions bàsiques amb les quals es pot jugar en aquest apartat de l'ordre. Aquestes opcions bàsiques són les següents : ✔ A és per a afegir (Append) una regla. Regles vàlides són INPUT, FORWARD i OUTPUT. ✔ L és per a llistar les regles. ✔ F és per a esborrar totes les regles o en el cas de INPUT, FORWARD o OUTPUT siguen donats com argument s'esborraran les regles associades solament a aquesta classe. ✔ P establix la política per defecte del firewall. Per defecte és acceptar totes les connexions.
%[criteri]	Ací és on s'especificaran les característiques del tipus de paquet que casarà amb aquesta regla. Per a establir regles senzilles (regles stateless), podem operar amb les següents opcions : -s (ip/xarxa font), -d (ip/xarxa destinació), --sport (port font), --dport (port destinació), i -p (protocol). Un exemple de la sintaxi d'una ordre iptables senzilla podria ser aquesta (la part que es defineix el criteri de la regla està en negreta) : iptables -A FORWARD **-p %[protocol] -s %[ip/xarxa font] --sport %[port font] -d %[ip/xarxa destinació] --dport %[port destinació]** -j DROP
-j %[acció]	Ací establim que és el que cal fer amb el paquet. Les possibles opcions són : ACCEPT, REJECT, DROP, REDIRECT, LOG (existeixen més, però aquestes són les bàsiques). ACCEPT acceptarà el paquet. REJECT o DROP ho rebutjaran, la diferència entre ells resideix que DROP descartarà el paquet silenciosament i REJECT emetrà un paquet ICMP “Port Unreachable”, indicant que està tancat. REDIRECT redirigirà el paquet on s'indiqui en el criteri del comando i finalment... LOG ho registrarà per a la seva posterior anàlisi.

Per als exemples emprarem 2 equips:

europa amb IP 192.168.1.100 (és el nostre equip de referència, i on aplicarem les regles)

jupiter amb IP 192.168.1.1

Comencem amb Iptables!!!

Anem a veure com és l'estat de les nostres 3 cadenes principals (polítiques), llistant el que hi ha en elles. Per a això executem la següent ordre:

```
toni@europa:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Si l'eixida obtinguda no li sembla al que veuen ací dalt, significa que no teniu instal·lats els mòduls corresponents en el kernel, o que ja hi ha un tallafocs funcionant, o per a confondre'ls més: significa que ja es va executar un script probablement en l'inici del sistema on es carreguen les regles del tallafocs.

Suposant que l'eixida que van obtenir és igual a l'escrita ací dalt, la situació és la següent: vol dir que el tallafocs aquesta acceptant tots els paquets, o el que és el mateix, no filtra absolutament gens. Açò ens indica 2 coses:

- ✔ Les 3 cadenes (INPUT/FORWARD/OUTPUT) estan buides
- ✔ Les 3 cadenes tenen com política per defecte "ACCEPT".

És normal que al fer un ping a localhost (nosaltres mateixos) rebem resposta:

```
toni@europa:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.039 ms
(i així successivament...)
```

Anem a agregar una regla, per a entendre el funcionament:

```
sudo iptables -A INPUT -s 127.0.0.1 -j DROP
```

Què és açò? Simple:

-A = Agregar (append) la següent regla a la cadena INPUT: al rebre un paquet amb origen (-s) "127.0.0.1" i amb qualsevol destinació (ja que no ho especifiquem), enviarem aquest paquet (-j) a DROP (desapareixerà).

Què? No ha passat res, veritat? Segur? Llavors llistem altra vegada les regles que tenim carregades (et vas oblidar com es feia??)

```
toni@europa:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       0    --  localhost            anywhere
(...)
```

Notem que en la cadena INPUT, ens apareix una nova regla, la funció de la qual és impedir el tràfic d'entrada des de la nostra pròpia màquina. Podran notar que aquesta regla no és massa útil a les fins pràctiques, però si ho és per a exemplificar l'ús. I que és el que faltaria?

Comprovem el seu funcionament!! Per descomptat!!

```
toni@europa:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
(i es quedarà esperant una resposta que mai arribarà...)
```

El nostre tallafocs està invisible? Clar que no. De fet, veurem que des de qualsevol altre PC, fem ping sense problemes, i la nostra maquina li respon.

```
root@jupiter# ping europa
PING europa (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=64 time=1.2 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=1.0 ms
```

Amb la qual cosa, amb un simple ping, el nostre amic operador de jupiter pot notar la presència del nostre PC.

Restringint paquets provinents de l'exterior

Ja que el nostre tallafocs està filtrant els tots els paquets locals, i deixa passar els remots. Anem a canviar un poc les regles "del joc". Esborrem la regla que anteriorment agreguem:

```
sudo iptables -D INPUT -s localhost -j DROP
```

Açò s'assoleix amb l'opció "-D", i la resta, és la transcripció EXACTA de la regla que volem esborrar.

NOTA: coneixent que era l'única regla, haguérem assolit el mateix resultat escrivint:

```
sudo iptables -D INPUT 1.
```

Restringir l'accés a paquets amb protocol icmp (-p icmp) des de jupiter (192.168.1.1).

```
sudo iptables -A INPUT -p icmp -s 192.168.1.1 -j DROP
```

Ara, anem a llistar la nostra cadena INPUT:

```
toni@europa:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
```

```
target     prot opt source               destination
DROP       icmp --  jupiter             anywhere
(...)
```

Llest, ara qualsevol paquet icmp amb origen en 192.168.1.1 serà omés (DROP). Per això, quan el nostre amic curiós fa ping des de la seua màquina (jupiter) a la nostra, mai tindrà resposta..

```
root@jupiter # ping europa
PING europa (192.168.1.100): 56 data byte
```

Llest. Per al nostre amic de jupiter, la nostra màquina està invisible, per tant, vam assolir el nostre objectiu d'assegurar-la. Cert?

NOOO!!

Simplement el que hem fet es dir-li al nostre PC que no responga a un tipus específic de (en aquest cas ICMP), i sols des d'una màquina en concret.

Ara pensem el següent: que passa si en la nostra xarxa, hi han milers "d'amics curiosos"??. Agregarem una regla per a cadascun d'ells? Seria un treball bastant tediós, i poc eficient.

A més, un detall realment important: si bé totes aquestes regles, s'aplicaren sense problemes, i són correctes sintàcticament, és MOLT ACONSELLABLE seguir la filosofia de

"Tot el que no està EXPLICITAMENT permès, llavors està prohibit".

Com assolim açò? Com primer pas, establirem la política per defecte en DROP (descartar). Qualsevol paquet que circula per la cadena INPUT serà descartat (DROP) si no coincideix amb cap regla.

Buidem primer totes les cadenes amb l'opció -F (flush)

```
sudo iptables -F
sudo iptables -P INPUT DROP
```

Llistem el que tenim:

```
toni@europa:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
```

Encara que no tinguem cap regla, ningú va a poder accedir al nostre PC. Justament, qualsevol paquet que entra, és exposat a cada regla de la cadena (en el nostre cas la nostra cadena aquesta buida), al no trobar coincidències, la destinació del paquet, ho decideix la política de la cadena, o siga DROP.

El problema ací és que encara que nosaltres puguem realitzar connexions sortints, les respostes dels servidors seran descartades.

Podeu comprovar-ho intentat accedir a qualsevol pàgina web des del navegador.

Per a solucionar açò, anem a agregar la següent regla:

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Per la qual deixem passar qualsevol paquet la connexió del qual ja s'ha establit (ESTABLISHED), o la connexió del qual és nova, però està relacionada a una connexió ja establida (RELATED), segons les man pages del iptables. Per enèsima vegada, llistem el que tenim en la nostra cadena INPUT!!

```
toni@europa:~$ sudo iptables -L INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     0    --  anywhere             anywhere            state
RELATED,ESTABLISHED
```

Amb la qual cosa, ningú podrà iniciar una connexió a la nostra maquina, llevat que especifiquem... Com veureu, per defecte tenim un DROP. Ara podem començar a permetre connexions. Accés local:

```
sudo iptables -A INPUT -i lo -j ACCEPT
```

-i lo : Amb açò especifique com interfície de xarxa a localhost (lo).

Si per exemple volem permetre accés al nostre PC d'un servei com per exemple el bittorrent (ports 6881-6889):

```
sudo iptables -A INPUT -p tcp --destination-port 6881:6999 -j ACCEPT
```

Consells útils i comentaris finals

Finalment, no apagueu encara la vostra màquina. Els canvis realitzats 'on-the-fly' a iptables, no queden guardats en cap arxiu, sinó que s'emmagatzemen en memòria, i com sabreu, al reiniciar, els canvis s'esborraran. Tingueu en compte els següents consells:

- ✔ Guardeu totes les vostres regles en un script bash, i amb comentaris explicant cada regla o grup de regles aplicades
- ✔ En cas d'executar el script automàticament a l'iniciar la màquina, considereu fer-lo abans d'alçar cap servei, o millor encara, abans d'alçar cap interfície de xarxa. No us preocupeu per les regles que fan referència a interfícies no alçades, igualment són acceptades per iptables.

Per a acabar, i com a mode ilustratiu, una regla de que no serveix per a filtrar, sino que fa NAT per a redireccionar un port.

Ordre	iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128.
Descripció	Redireccionar al port 3128 (proxy) tots els paquets que entren per eth1 i amb destinació port 80 (HTTP), d'aquesta manera aconseguim un proxy transparent.

Firewall - Firestarter

Ara que hem vist com configurar un filtrat bàsic amb iptables, procedirem a configurar el mateix amb l'eina gràfica Firestarter.

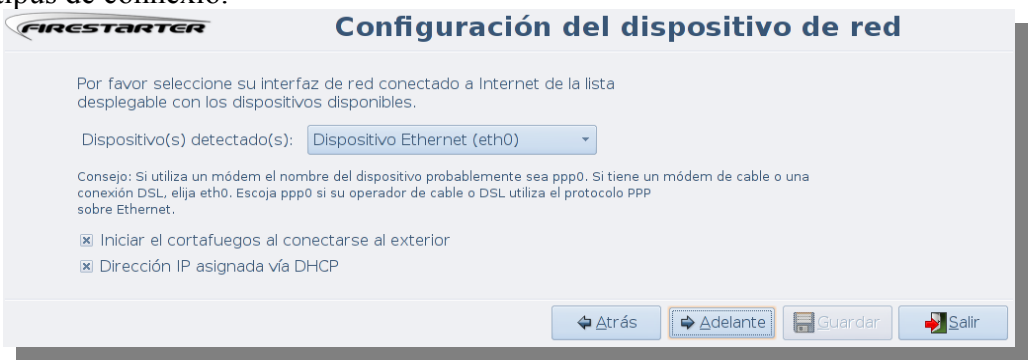
Firestarter no és més que una interfície gràfica per a iptables, de forma que configurar el tallafocs ens resulte més fàcil.

Instal·lació i configuració inicial

Per tal d'instal·lar-lo sols cal anar al gestor de paquets synaptic, o mitjançant el menú Aplicacions → Afegeix / Elimina i buscar Firestarter.

La primera vegada que arranquem el programa, se'ns mostra un assistent, amb el qual configurarem d'una manera bàsica el tallafocs.

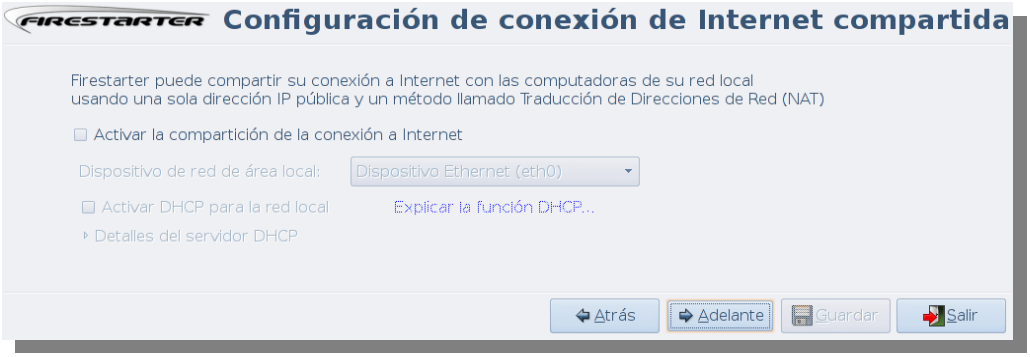
En aquesta finestra configurarem la interfície connectada a Internet, l'assistent detectarà automàticament totes la interfícies de xarxa, hauríem de seleccionar la qual està connectada directament a Internet. També tenim dues opcions les caselles de les quals podem marcar depenent del nostre tipus de connexió.



- ✔ Iniciar el tallafocs al connectar-se a l'exterior: Si no tenim connexió directa, podem usar aquesta opció perquè el tallafocs no aquest operatiu si no estem connectats, així mateix es reiniciarà en cas que perdem la connexió i tornem a reconnectar, ja siga manualment o automàticament.
- ✔ Adreça IP assignada via DHCP: Si la nostra connexió es configura d'aquesta manera, marcant aquesta casella aquesta connexió estarà permesa per defecte, però sempre podem deixar-la desmarcada i permetre aquesta connexió creant una regla que solament permeta la connexió al nostre servidor DHCP.

Si disposem d'una xarxa local i volem compartir la connexió o recursos entre el nostre PCs, podem activar-la des d'aquesta finestra. Lògicament hem de disposar de més d'una interfície de xarxa i la seleccionada en aquesta finestra deu ser diferent a la qual seleccionem en la finestra anterior.

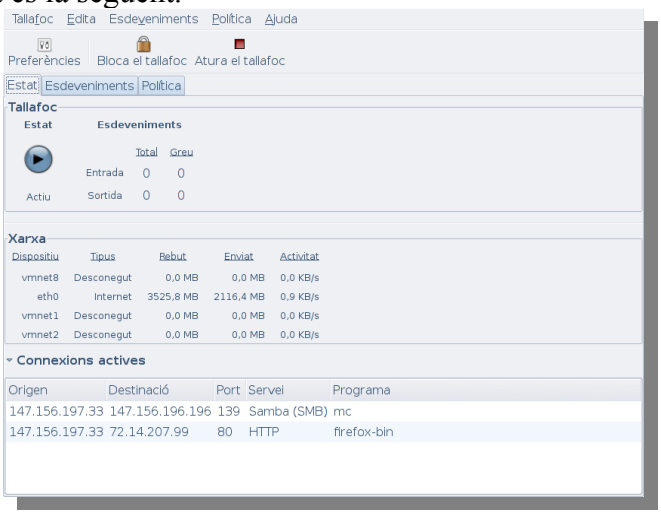
Si disposem d'un servidor DHCP per a no haver de configurar manualment tots els equips de la xarxa, podem habilitar aquesta connexió des d'ací.



Iniciant Firestarter

Una vegada acabada la configuració mitjançant l'assistent, guardarem la configuració i eixirem d'aquest perquè s'inicie el programa.

També podem accedir a Firestarter des del menú Sistema → Administració → Firestarter, i la pantalla que ens mostrarà és la següent.

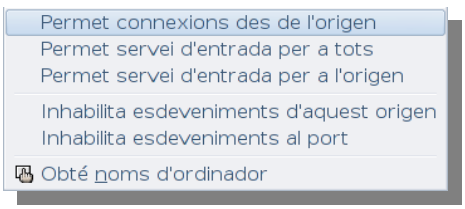


Des de la pestanya **ESTAT** podem veure tant l'estat del tallafocs, el tràfic per a cada dispositiu, així com les connexions actives.

Podem accedir al assistent d'abans des del menú Tallafoc, on amés podrem iniciar o aturar el tallafoc i blocar-lo.

En aturar el tallafoc es perden totes les regles que teníem (podeu comprovar-ho amb iptables).

Blocar el tallafocs el que fa és posar totes les polítiques per defecte a DROP (descartar). Comproveu-ho amb iptables).



En la següent pestanya, **Esdeveniments**, quedaran registrats tots els intents de connexió bloquejats pel tallafocs, excepte lògicament aquells que hem descartat mitjançant la nostra configuració.

Amb el botó dret al damunt d'una connexió blocada podrem afegir una regla.

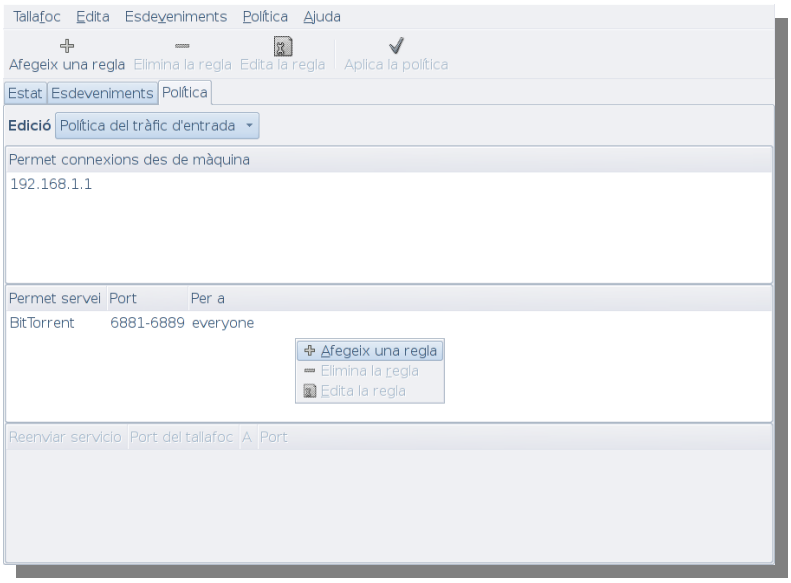
Afegint Regles

Per a afegir, esborrar o modificar regles, cal anar a la pestanya **Política**.

Des d'aquesta pestanya, definirem la política del tallafocs respecte a les connexions tant entrant com sortint, podent crear regles per a, depenent de la política triada, bloquejar o permetre tant ports com adreces IP.

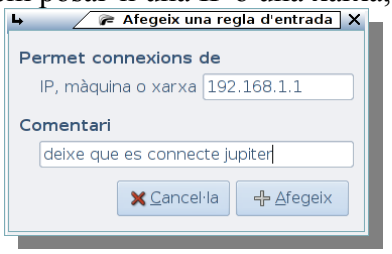
Política del tràfic d'entrada.

Per al Firestarter, la política del tràfic d'entrada prohibeix totes les connexions excepte les que estan permeses explícitament.



Podem permetre qualsevol tipus de connexió des d'un PC en concret, fent clic amb el botó de la dreta al damunt de la zona “permet connexions de la la màquina” i seleccionant “Afegeix una regla”.

Ens mostrarà una finestra on podem posar-li una IP o una xarxa, tal com mostra la figura.



En la part inferior, podem afegir una regla basada en ports/serveis. Al igual que en el cas anterior hem de fer clic amb el botó dret del ratolí al damunt d'aquesta àrea, per tal d'afegir, esborrar o modificar una regla.

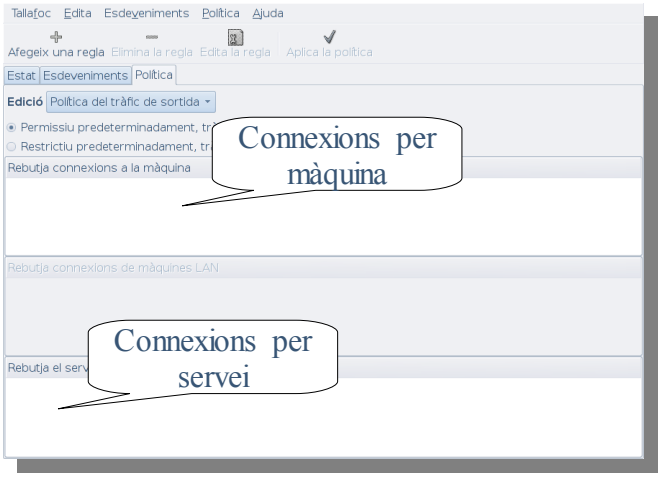
En el cas d'afegir una regla ens mostrarà la finestra següent.

Hem de tindre en compte que si el que volem és permetre l'accés a compartir arxius amb altres PC amb sistemes Windows, hem de permetre l'accés per “Samba (SMB)” , amés de tenir aquest servei habilitat.

Política del tràfic de sortida.

Al contrari de la política del tràfic d'entrada, existeixen dues polítiques diferents per al tràfic sortint.

- **Permissiu**: Tot el tràfic sortint està permès, solament els ports o adreces de la llista seran bloquejats.
- **Restrictiu**: Tot el tràfic sortint serà bloquejat, solament el tràfic entre els ports i adreces de la llista seran permesos.



Com podreu comprovar, d'aquesta forma es configura més fàcilment el tallafocs.

Recursos externs

Virtualizar un Sistema Windows XP.	http://alfonsoycia.blogspot.com/2007/06/virtualizar-sistemas-operativos.html
Wine a la wikipedia.	http://es.wikipedia.org/wiki/Wine
Pàgina web de Wine.	http://www.winehq.org/
Photoshop i Dreamweaver amb Wine.	http://tuxpepino.wordpress.com/2007/05/28/instalar-dreamweaver-y-photoshop-en-ubuntu/
Ies4linux	http://www.tatanka.com.br
Iniciación de sudo para bisoños	http://bulma.net/body.phtml?nIdNoticia=1779
Manual de Iptables	http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall.pdf