Antivirus e firewall (cortalumes)

Nesta sección veranse aspectos relacionados coa seguridade: antivirus e firewalls

Sumario

Antivirus

A incidencia dos virus en GNU/linux é moi baixa, por varias razóns:

- O número de usuarios é moi inferior ao de MS Windows. É máis produtivo facer un virus para este último.
- Tal e como esta deseñado GNU/Linux no que atinxe á seguridade de quen pode realizar as distintas tarefas, é máis difícil que se instale un virus.
- Ao ser software libre, todo o mundo pode analizar os programas que se instalan, salvo aqueles que non son software libre.

Pero aínda así, nada é infalible e menos en informática, por tanto nun futuro nunca se sabe o que pode chegar a ocorrer.

TAMÉN PODES VER...

Recoméndase a lectura dos seguintes artigos:

- http://www.wikilearning.com/tutorial/manual_faq_debian-porque_en_linux_no_hay_virus/6515-8
- http://www.quevidaesta.com/index.php/%C2%BFpor-que-no-hay-virus-en-linux-y-mac/2007/08/05/

Aínda así pódese instalar un antivirus para detectar e eliminar virus en soportes (Lapis USB, discos, etc) que puideran estar infectados por ser usados en equipos con MS Windows sen protección.

Os soportes e ficheiros que puideran estar infectados con virus para MS Windows non afectarán en absoluto ao sistema operativo GNU/Linux.

ClamAV

Este programa instálase xeralmente en servidores de correo, para que analice os adxuntos.

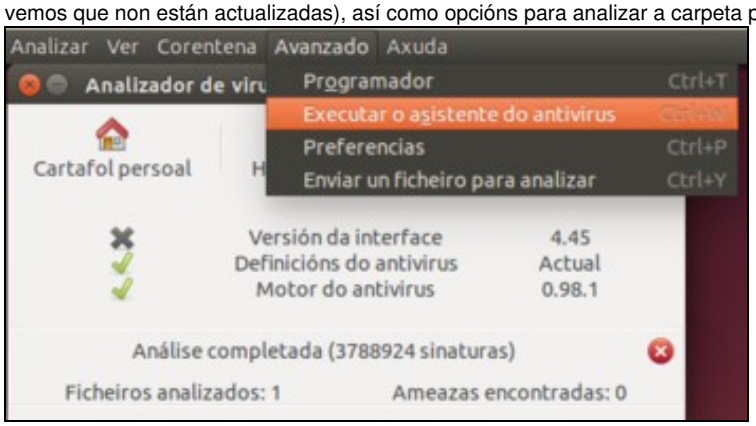
En Ubuntu podemos instalar o paquete **clamtk**, que é o interface gráfico para xestionar *ClamAv* . Ao instalalo xa se instala tamén ClamAv e o actualizador automático de firmas.

O programa está accesible a través do *Dash* como **ClamTK**

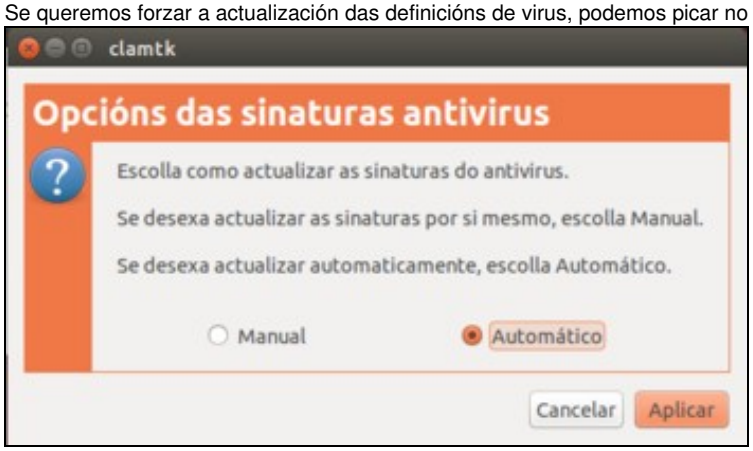
- Uso de ClamTK

- 

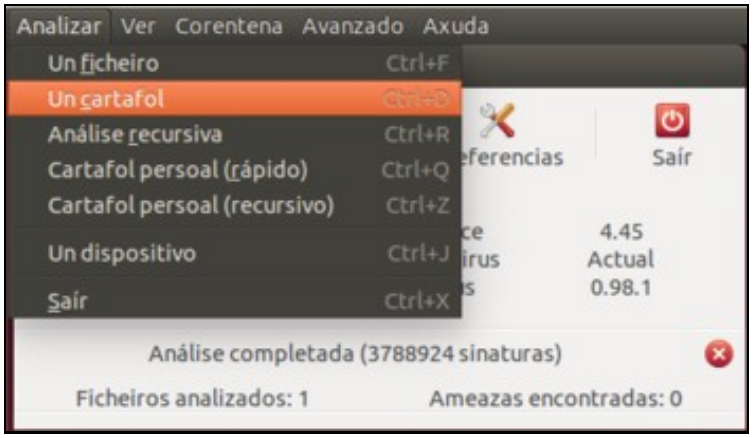
Iniciamos o programa, e podemos ver a ventá principal na que aparece o estado de actualización do programa e as definicións de virus (que vemos que non están actualizadas), así como opcións para analizar a carpeta persoal do usuario ou cambiar as preferencias do programa.

- 

Se queremos forzar a actualización das definicións de virus, podemos picar no menú **Avanzado**->**Executar o asistente do antivirus**.

- 

Podemos escoller se actualizar as sinaturas de virus de forma manual ou automática. É preferible seleccionar esta última.

- 

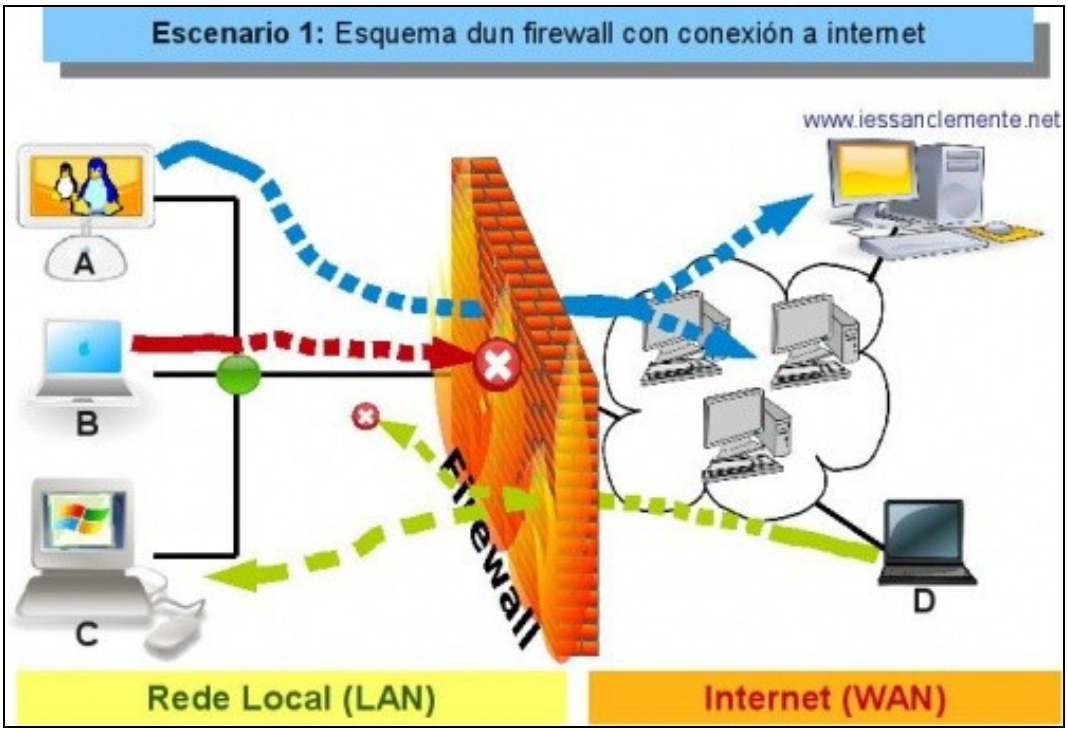
Agora xa veremos que a definición de virus está actualizada. O programa e moi sinxelo de usar e non imos detallar todas as opcións que ofrece. Simplemente indicar que para analizar unha carpeta, un ficheiro un dispositivo, etc, só hai que premer no menú **Analizar** e escoller o que corresponda. No menú **Avanzado-->Preferencias** pódese escoller que tipos de arquivos se desexan analizar.

Firewall

Un **firewall** (*Cortalumes ou devasa*) (En español, *cortafuegos*), permite protexer o ordenador fronte ataques externos e incluso controlar a que lugares se deixa realizar conexións e a cales non.

Un dispositivo firewall

Neste escenario o firewall é un dispositivo (pode ser un elemento hardware ou un ordenador configurado para tal fin), que recibe o nome de *firewall de subrede*:



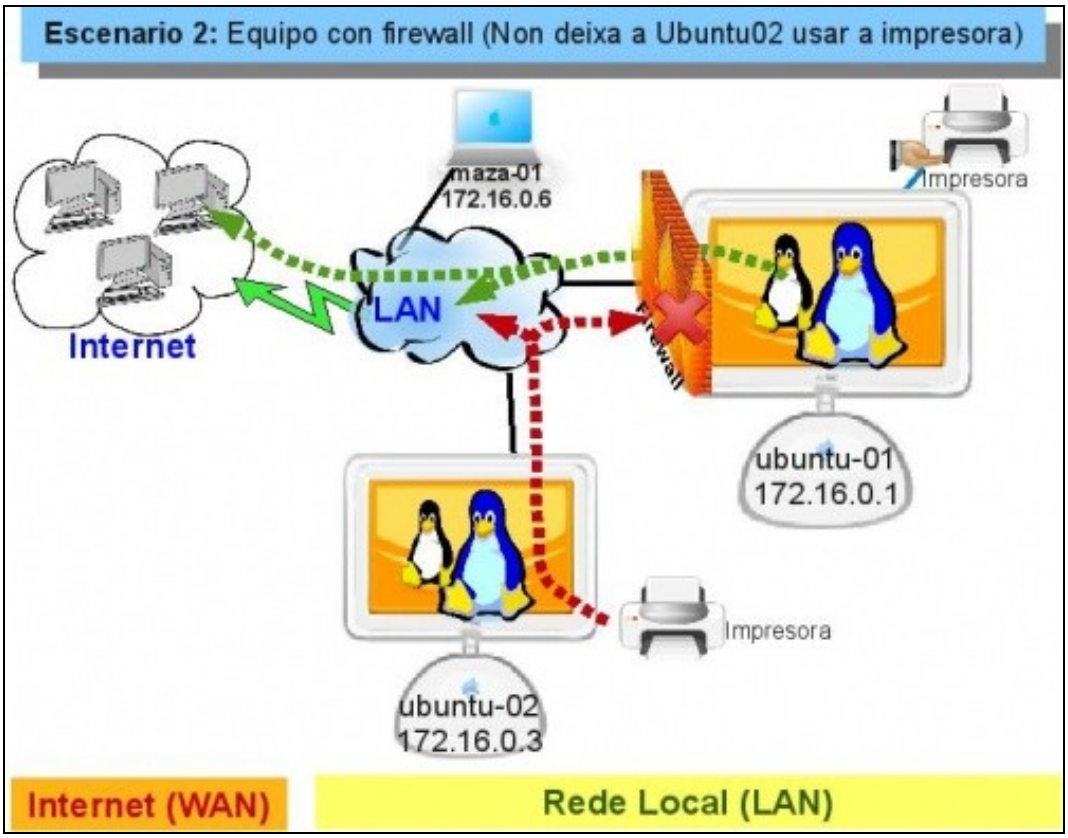
Neste escenario 1 o firewall é un dispositivo que controla as conexións que se poden establecer entre equipos da rede local e internet. Non controla as comunicacións entre os equipos locais (neste caso). Quen se pode comunicar con quen?:

- **Ordenador A:** pode comunicarse cos ordenadores locais B e C e con internet.
- **Ordenador B:** pode comunicarse cos ordenadores locais A e C, pero non con internet.
- **Ordenador C:** pode comunicarse cos ordenadores locais A e B, e non se sabe con internet.
- **Ordenador D:** poderá comunicarse con internet, pode comunicarse co equipo local C, pero non con A e B.

Que D se poida comunicar con C, non significa necesariamente o contrario. D inicia unha comunicación con C e o firewal autoriza que se comuniquen entre eles, pero ó mellor se a inicia C o firewall non lle deixa, depende de como se configure.

Un ordenador con firewall

Neste outro escenario, que será o que se implante no manual, un ordenador ten un cortalumes instalado e permítelle controlar as conexións entrantes e saíntes. Neste caso, o firewall recibe o nome de *firewall persoal*:



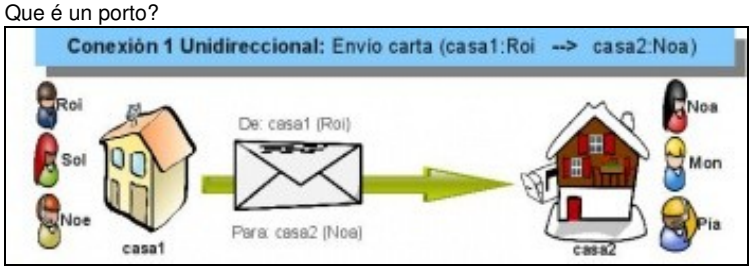
- **Ubuntu-01:** pode acceder á LAN e a Internet. Non deixa acceder ao servidor de impresoras.
- **Ubuntu-02:** non ten firewall, pode acceder a internet, pero non pode acceder ao servidor de impresoras de *ubuntu-01*.

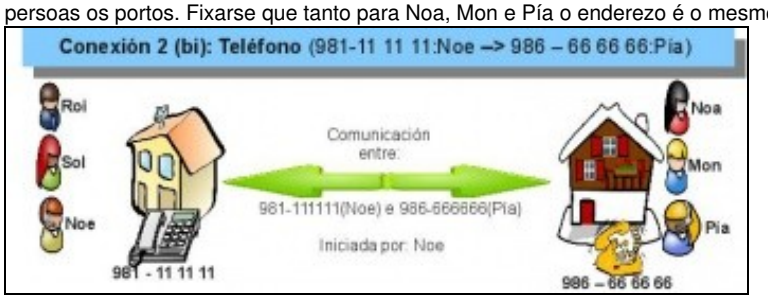
Concepto de conexión e portos

Toda conexión entre dous ordenadores identifícase polo par: (IP orixe:porto orixe <-> IP destino: Porto destino).

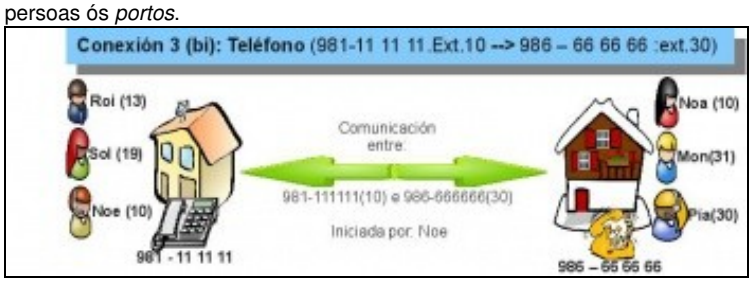
Pero que é o **porto**?

Obsérvese os seguintes exemplos:

- Que é un porto?
- 

  Neste exemplo Roi que vive na casa1 envía unha carta a Noa que vive na casa2. Cada casa ten un enderezo, pero non se comunica toda a casa1 con toda a casa2. Comunícase unha *entidade* da casa1 con outra *entidade* da casa2. Os enderezos serían as IPs dos equipos, e as persoas os portos. Fixarse que tanto para Noa, Mon e Pía o enderezo é o mesmo *Casa2*, pero cada un deles é unha persoa nese enderezo.
- 

Neste outro exemplo Noé que ten por teléfono 981-111111 fala con Pía que ten por teléfono 986-666666. Non todo o mundo que vive na casa con teléfono 981-111111 esta participando na chamada que se está realizando con Pía. Os teléfonos serían o equivalente ás *IPs* e as persoas ós *portos*.

- 

Derradeiro exemplo antes de chegar á explicación final. Se cada persoa nas casa ten unha extensión telefónica, pois Noe podería chamar a Pía indicando o 986-666666 e logo marcando a extensión 30. Cada persoa dentro da casa tería asignado un número de extensión. O teléfono sería o equivalente á *IP* e a extensión asignada a cada persoa sería o *porto*. Notar que en cada casa todo o mundo ten o mesmo número de teléfono pero extensión distinta. A conexión sería o par: (981-111111 Ext 10 <---> 986-666666 Ext 30)

Finalmente, cada ordenador ten unha IP, e ese ordenador executa aplicacións que precisan conectarse a outros ordenadores (skype, navegador, impresora compartida, etc, etc). Cada unha desas aplicacións terá un número asignado, ese número chámase **porto**. Agora ben, como se asignan eses números (portos) dentro de cada ordenador?.

Comecemos con *ubuntu-01* que é un servidor de distintos servizos: (impresoras compartidas, carpetas compartidas por SAMBA, servidor web). Cada servizo coñecido ten un porto un porto por defecto: así todo servidor web sempre estará atendendo as peticións no porto 80 (pódese cambiar). Deste xeito, cada vez que alguén se conecte ó servidor web de calquera ordenador, por defecto vai tratar de conectarse ó porto 80 do servidor.

Por tanto, cando se instala un servizo (web, samba, IPP -Internet Printing Protocol-, etc) este terá un ou varios portos asignados por defecto (observar os portos da imaxe) polos que recibir as peticións. Se se desexa pódese cambiar o porto asignado por defecto.

Como actúa *ubuntu-01*?, cando recibe unha petición, mira o porto para quen vai destinada e envía a petición ó servizo asignado a ese porto.

Imos agora con *ubuntu-02*: cando se abre un cliente (un navegador web, skype, etc) o sistema operativo asígnalle nese intre un porto dos que teña libres. Se por exemplo o navegador Firefox desexa conectarse ao servidor web de *ubuntu-01*, só debe poñer o nome (ou IP) do equipo de destino na barra de enderezos e non pon o porto de destino (80). Por que?, porque se supón que todo navegador web sempre fai ás peticións ao porto 80.

Que pasa se o servidor web está configurado para atender noutro porto?. O cliente debe especificalo na barra de enderezos, por exemplo http://172.16.0.1:631. Lembrar da sección anterior (Impresoras) que polo porto 631 estaba o servidor web que permite administrar as impresoras de *ubuntu-01*.

Neste exemplo a comunicación estase producindo entre (172.16.0.3:1000, 172.16.0.1:80).

Un firewall pode controlar a que equipos se poden realizar conexións e a que portos (servizos) deses equipos (poden ser a todos ou a algúns).

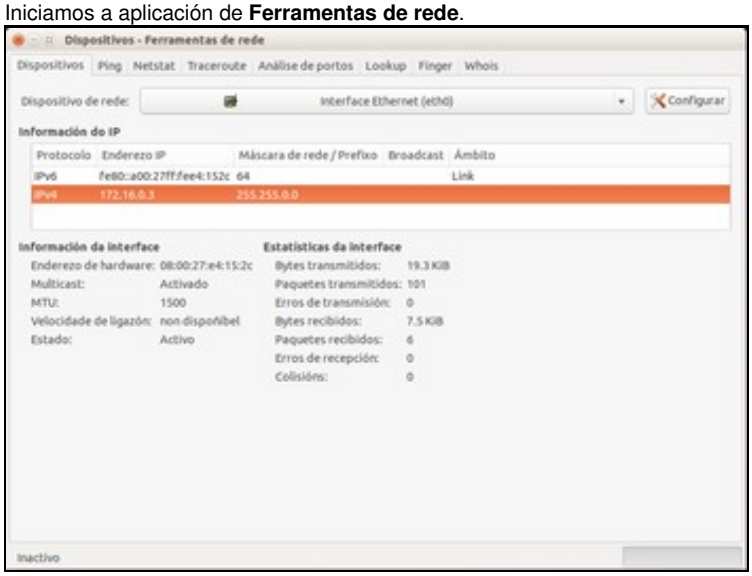
Análise de portos

É bo coñecer cales son os portos (servizos) que está dispoñibles nos nosos equipos.

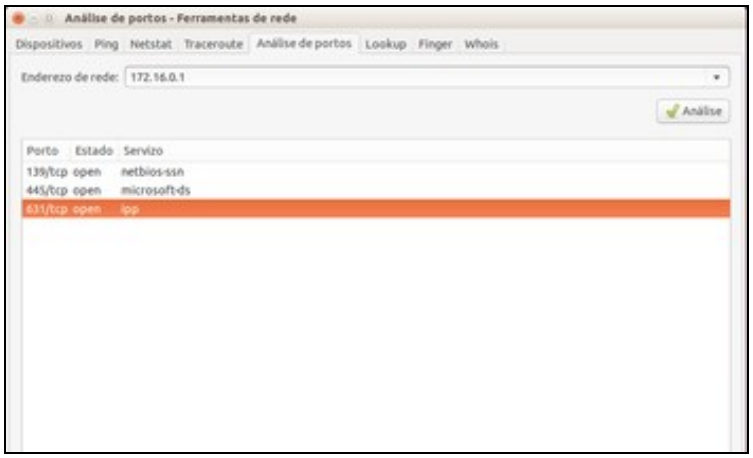
Para iso, en Ubuntu existe unha ferramenta que indica que portos (servizos) ten dispoñibles un ordenador.

- Análise de portos
- 

Co *Centro de Software de Ubuntu* instalamos o paquete de **Ferramentas de rede**.
- 

Iniciamos a aplicación de **Ferramentas de rede**.
- 

Pódese coñecer información sobre as tarxetas de rede e moitas cousas máis.

- 

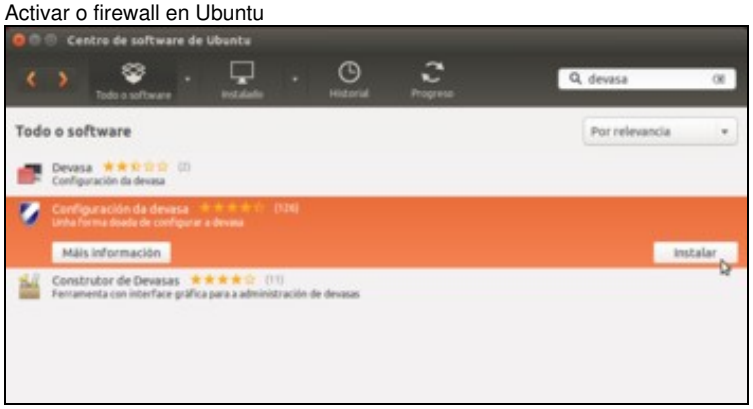
Pero neste caso interesa saber que portos ten abertos o equipo que ten a dirección IP 172.16.0.1: **139 e 445** para Samba (lembrar que trataba de simular o protocolo smb de Microsoft para compartir arquivos e impresoras por samba), **631**, IPP (Internet Printing Protocol, cando se comparten as impresoras nese equipo os demais equipos poderán chegar a elas a través dese porto).

Activar o firewall

O escenario que se vai seguir é o 2 e o esquema de conexión a cuarta, coa única diferenza de que o nome dos nosos equipos serán *uclient* e *uclient02* no canto de *ubuntu-01* e *ubuntu-02*.

Antes de nada indicar ao usuario que a instalación dun firewall pode cortar todas as conexións tanto saíntes como entrantes. O firewall que se vai instalar permite, por defecto, todas as conexións saíntes pero ningunha entrante (algo semellante ao escenario 2). Por tanto se ten un servidor de impresoras e outro samba (o feito anteriormente no manual), estes deixarán de ser accesibles dende a rede ate que se configure o firewall.

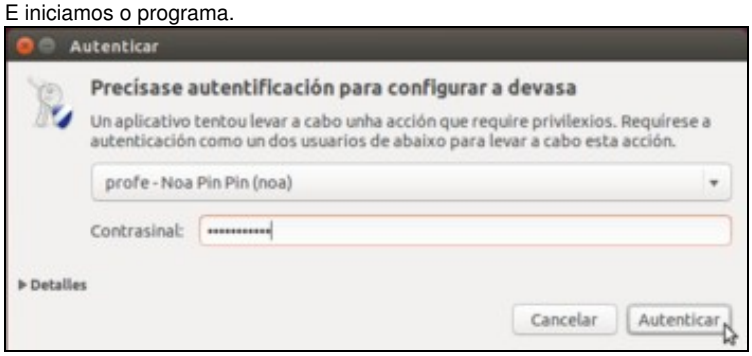
Como todo en GNU/Linux a configuración do Firewall reside nuns ficheiros de configuración. Existen varias ferramentas gráficas que permiten a manipulación deses arquivos; imos ver unha delas chamada *Gufw* (Que ven significando *Graphical Uncomplicated FireWall* ou *FireWall Gráfico Sinxelo*).

- Activar o firewall en Ubuntu
- 

Instalamos o paquete **Configuración da devasa**.

- 

E iniciamos o programa.

- 

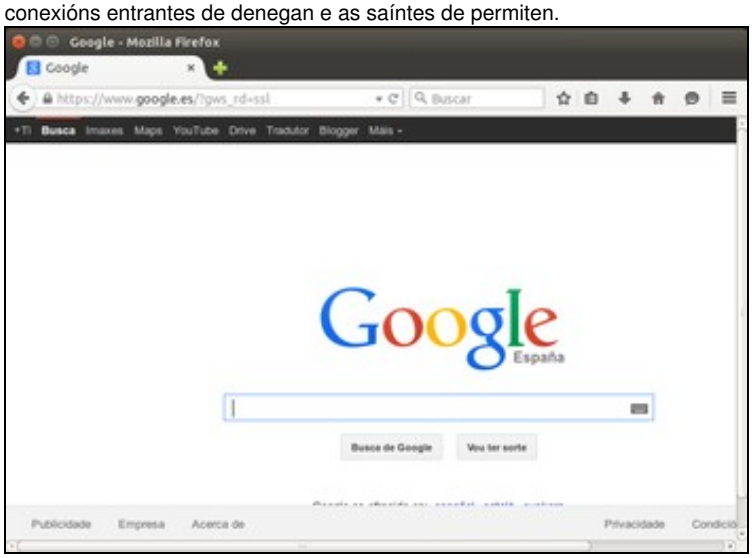
Dado que a xestión do firewall do sistema non é unha operación que poida facer calquera usuario, teremos que introducir o contrasinal de algún usuario con privilexios de administración.

- 

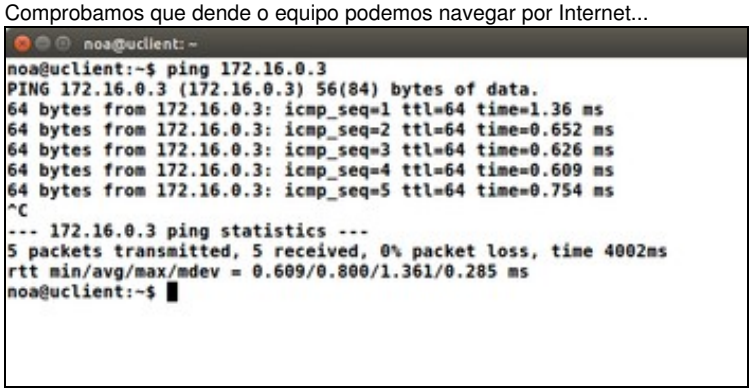
Atopámonos na ventá principal do programa. Na parte inferior podemos ver unha axuda para comezar a usar este programa, e na parte superior as opcións principais, entre as que se atopan o perfil de rede que queremos activar (logo explicaremos para que serven os perfís), e o estado do firewall que neste momento está desactivado.

- 

Simplemente picando sobre o interruptor do estado activamos o firewall, e podemos comprobar que as opcións por defecto son que as conexións entrantes de denegan e as saíntes de permiten.

- 

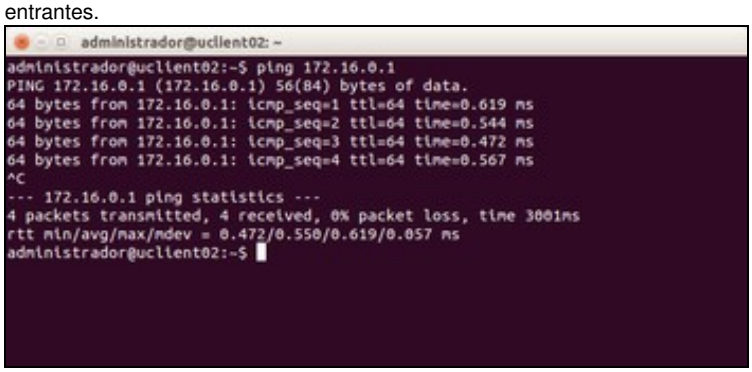
Comprobamos que dende o equipo podemos navegar por Internet...

- 

e facer *ping* a *uclient02*.

- 

Pero dende *uclient02* xa non podemos acceder aos portos que estaban abertos en *uclient*, porque agora o firewall denega esas conexións entrantes.

- 

O que si funciona é o *ping* dende *uclient02* a *uclient*, xa que a ferramenta de xestión do firewall que estamos usando nunca denega este tipo de conexións.

Xestión dos perfís e configuración básica do firewall

A xestión máis básica do firewall consiste en indicar que queremos que faga coas conexións entrantes e coas saíntes, sen discernir entre as conexións que vaian a un porto do equipo e as que vaian a outro.

Pero é moi probable que non sempre nos interese o mesmo... Supoñamos que temos un portátil que usamos en casa pero que tamén usamos ás veces para conectarnos a Internet dende unha rede pública (unha biblioteca, cafetería, etc.). Pode ser que nel teñamos unha carpeta compartida que usamos para acceder dende un segundo equipo que temos en casa e compartir documentos entre eles, pero... quereríamos que esa carpeta fose accesible para os outros equipos cando nos conectamos á rede pública? Seguramente non nos faría gracia que outra persoa da cafetería entrase nesa carpeta na que temos documentos persoais, fotos, etc.

Isto poderíamos evitalo se para o acceso á carpeta é necesario introducir un nome de usuario con un contrasinal seguro, pero non estaría mal que o firewall xa evitase nese caso ese tipo de conexións. Pois para iso serven os perfís do firewall; poderíamos ter por exemplo un perfil de *Casa* no que o firewall está configurado para permitir a conexións entrantes, pero outro perfil *Público* configurado para que se deneguen. Iso si, teríamos que encargarnos de activar o perfil *Público* cando nos conectemos nunha rede pública e o de *Casa* cando queiramos acceder dende o outro equipo de casa á carpeta compartida. Ao activar un perfil, o firewall cargará automaticamente a configuración establecida para ese perfil.

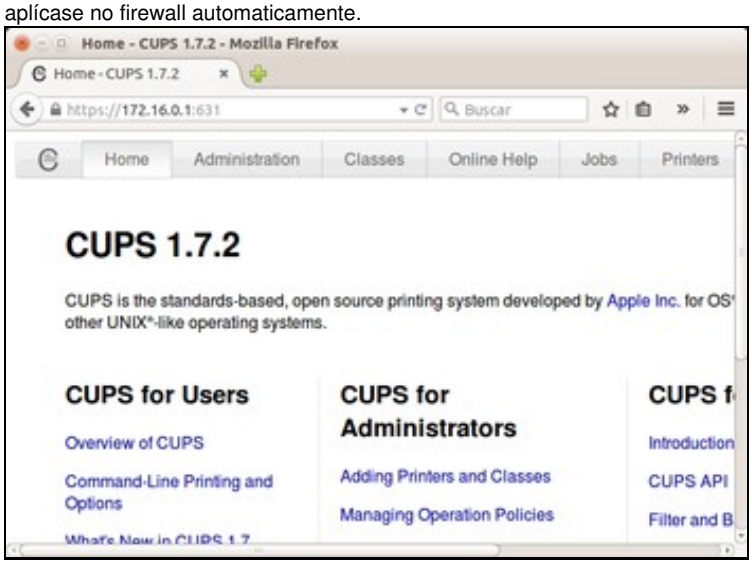
- Configuración básica do firewall e xestión dos perfís

- 

Antes de comezar a xogar con isto, véxase como dende *uclient02* non se pode acceder á xestión de impresoras web de *uclient*. O intento de conexión é rexeitado polo firewall.

- 

O primeiro que faremos é cambiar a configuración do firewall para as conexións entrantes, escollendo a opción de **Permitir**. O cambio aplícase no firewall automaticamente.

- 

Podemos comprobar dende *uclient02* que agora xa se pode acceder á xestión de impresoras. Tamén se podería acceder ás carpetas compartidas e todos os servizos de rede que poida estar executando *uclient*.

- 

Agora imos cambiar o perfil. Tiñamos activado o perfil de *Casa*, no que agora se permiten todo tipo de conexións (así dende os equipos da casa podemos acceder a todo neste equipo), e cambiamos ao perfil **Público**.

- 

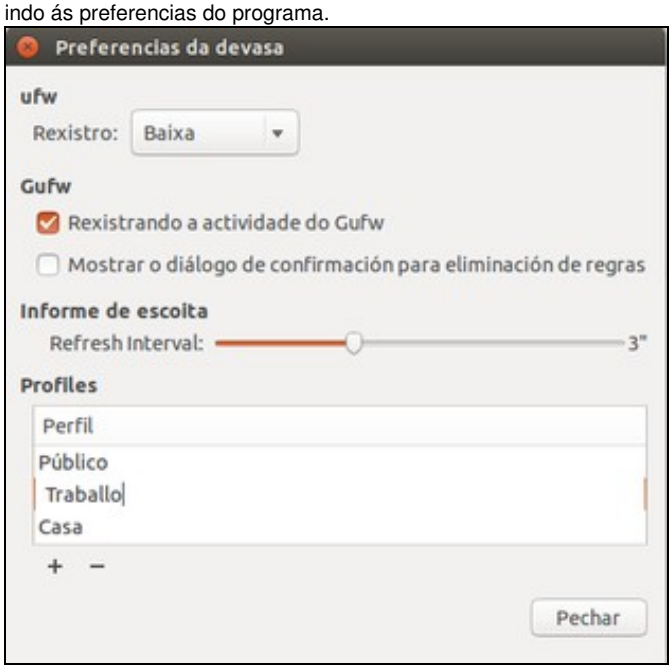
Ao escoller este perfil, a configuración para as conexións entrantes e saíntes cambia segundo o establecido no mesmo. Neste caso, a configuración por defecto para o perfil é rexeitar as conexións entrantes e permitir as saíntes, así que...

- 

xa non podemos acceder ao equipo dende *uclient02*. Xa temos a configuración que pretendíamos, agora só queda seleccionar o perfil que nos interese segundo a confianza que teñamos na rede á que nos conectamos.

- 

Por defecto veñen creados tres perfís (*Casa*, *Oficina* e *Público*) pero podemos eliminar algún deles, crear novos perfís ou cambiarlles o nome indo ás preferencias do programa.

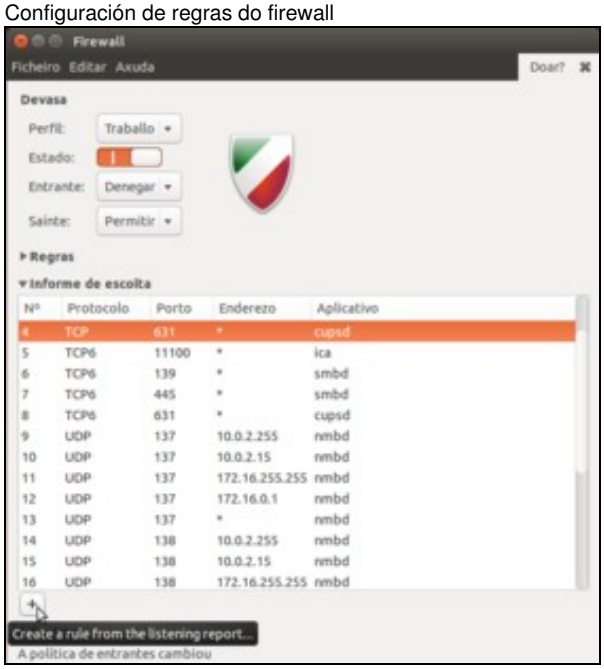
- 

Simplemente facendo clic sobre un perfil da lista podemos cambiar o seu nome, e cos botóns de **+** e **-** podemos crear e eliminar perfís respectivamente.

Configuración de regras do firewall

E xa para rematar, imos ver como facer unha configuración un chisco máis avanzada e precisa que o que fixemos ata o fe agora. Supoñamos que queremos que dende a rede se poida acceder a este equipo para imprimir, pero non entrar en carpetas que ten compartidas. Co que vimos ata agora, podemos decidir se permitimos conexións entrantes ao equipo ou non, pero non chegar a ese nivel de detalle.

Para conseguilo, teremos que configurar *regras* no firewall:

- Configuración de regras do firewall
- 

Se na ferramenta de configuración do firewall despregamos o apartado de **Informe de escoita** vánsenos mostrar os portos que ten abertos o equipo, que son número que identifican literais portas de entrada que o equipo ten abertas para prestar diversos servizos (impresoras, acceso a carpetas, etc.). Podemos atopar o porto número 631 que está asociado ao servizo de impresión; seleccionámolo e picamos no botón de **+**.

- 

Automaticamente créase unha regra cos datos necesarios para permitir a conexión a este servizo (fixarse que en *Política* está seleccionado *Permitir*). Tan só teremos que picar en **Engadir**.

- 

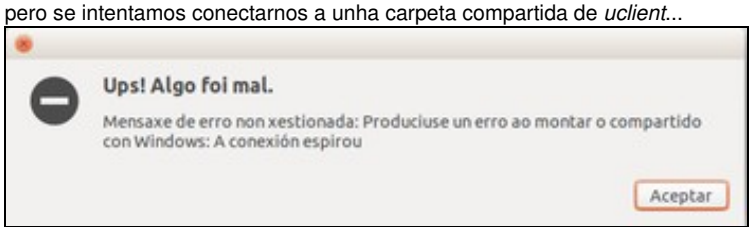
No apartado de regras aparece a regra que permite a conexión a ese porto. Polo tanto, coa configuración actual do firewall denegaranse todas as conexións entrantes **excepto** (as regras teñen prioridade sobre a configuración xeral das conexións) as que veñan dirixidas ao porto 631.

- 

Se probamos dende *uclient02*, podemos acceder a configuración de impresoras...

- 

pero se intentamos conectarnos a unha carpeta compartida de *uclient*...

- 

non imos poder. Fixarse en que a mensaxe de erro informa de que a conexión expirou, debido a que o firewall de *uclient* rexeita a conexión que está intentado establecerse dende *uclient02*.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez