

Tuxinfo



/tuxinfo

@tuxinfo

una revista libre, para un mundo libre.

no.62

Guerra fría tecno mundial

Opinión

GNUPANEL 2.0

El Panel de Control de Hostíng LIBRE y Universal para sistemas GNU/Linux

La respuesta a la decepción celular

Opinión

Usando firewall en Fedora

TubeMate 2

Descargas de YouTube sin límites...

Soporte para múltiples productos

en Apache™ Bloodhound 0.7

Redes para las masas

Parte VI

Huayra Linux

Y un día las vacas volaron...



Me

Esta revista se publica bajo una licencia de **Creative Commons CC BY-SA 3.0**. Puedes copiar, distribuir, mostrar públicamente su contenido y hacer obras derivadas, siempre y cuando **a)** reconozcas los créditos de la obra y **b)** la compartas bajo la misma licencia.

Microsoft, Apple, Sun, Oracle, así como otras marcas comerciales mencionadas en esta revista son propiedad de sus respectivas empresas.

Dirección

Ariel M. Corgatelli

Corrección

Luis Luque

Oscar Reckziegel

Diseño de tapa

Martín Eschoyez

Diseño

Ariel M. Corgatelli

www

<http://www.tuxinfo.com.ar>

facebook

<http://www.facebook.com/tuxinfo>

email

info@tuxinfo.com.ar

twitter

[@tuxinfo](https://twitter.com/tuxinfo)

Como todos los meses, les brindamos un nuevo número de nuestra querida revista. En esta oportunidad tenemos como de costumbre mucha información para compartir y muy buenos artículos para leer.

Este mes sin dudas estuvo muy movido, más que nada en lo referido a movilidad y Android. En donde la gente de Google se definió directamente por la próxima versión, que llevará el nombre de Kikat, y será la versión 4.4. La cual va a ser la próxima alternativa de Google antes de la versión 5.0, tan esperada por sus promesas de innovación y soporte de hardware más humilde.

Sin dudas es una versión que va traer cambios pero no tantos tal cual se había previsto en relación a la utilización de equipos más básicos como se había prometido.

Por otro lado y de forma local tuvimos el desembarco de Google Street View, lo cual desató todo un tema de quejas en cuanto a la privacidad. El problema principal planteado fue que no había buenas condiciones de privacidad en cuanto a la forma en que la empresa maneja los datos. Y para rematarlo Google anunció que va a cambiar las políticas de privacidad de Google+, haciendo que los usuarios de alguna manera seamos "objetos publicitarios".

Y como para seguir con temas locales tenemos que se anunció de forma oficial la Distribución Open Source HuayraLinux. Estuvimos presentes con nuestras cámaras (ver video url).

En el mismo se hizo mucho hincapié en todo lo relacionado a los temas políticos del software en general. Lo destacable de la presentación es que se hizo mención de que la distribución Linux está basada en software libre, y no sobre estar compuesta

completamente por software libre, ya que posee porciones que no lo son. Con lo cual se dispuso el tema que veníamos hablando hace tiempo sobre la licencia y el código. Obviamente se explicó que el código fuente existente sólo es el que se basa en el software desarrollado por el equipo de Huayra, y el de las partes de este sistema operativo que sí lo son, lógicamente no de las otras.

Para cerrar la editorial y no entretenerlos más, les hago un pequeño resumen de los temas que vamos a tratar en la revista. Y por cierto agradecemos mucho el interés de nuestros lectores por cada nuevo número.

Opinión - Guerra fría tecno mundial; GNUPANEL 2.0: El Panel de Control de Hosting LIBRE y Universal para sistemas GNU/Linux; Usando firewall en Fedora;

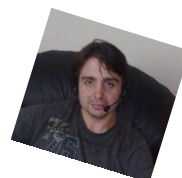
TubeMate 2 - Descargas de YouTube sin límites; Soporte para múltiples productos en Apache™ Bloodhound 0.7; Redes para las masas – Parte VI; Huayra, la distribución GNU/Linux del Estado Nacional Argentino, etc.

Y como todos los meses, repetimos la misma convocatoria en donde podemos tener más sugerencias de ustedes y así adaptar los contenidos de las notas a vuestras necesidades y preferencias, las mismas las podrán realizar en nuestros medios de contacto.

Fan page: <https://www.facebook.com/tuxinfo>
User Twitter: @tuxinfo

Mail de contacto: info@tuxinfo.com.ar

¡Sigán pasando la voz! Hay otro nuevo número de TuxInfo para descargar de forma gratuita.



Ariel M. Corgatelli
@arielmcorg

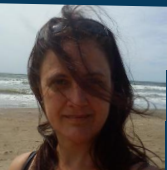
- 4. Soporte para múltiples productos en Apache™ Bloodhound 0.7.
- 12. Huayra, la distribución GNU/Linux del Estado Nacional Argentino.
- 15. La respuesta a la decepción celular.
- 16. TubeMate 2, Descargas de YouTube sin límites...
- 20. Usando firewallD en Fedora.
- 32. Guerra fría tecno mundial.
- 33. GNUPANEL 2.0: El panel de control de hosting LIBRE y universal.
- 35. Redes para las masas Parte VI.



Olemis
Lang



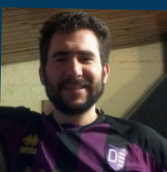
Juan M.
Dansa



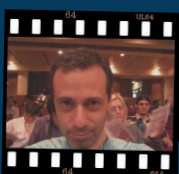
Maria
Eugenia
Nuñez



Hernan
Saltiel



Rino
Rondan



Claudio
de
Brasi





Soporte para múltiples productos en Apache™ Bloodhound 0.7

Por Olemis Lang

El quinto artículo de esta serie estará dedicado a la posibilidad de administrar múltiples productos en un solo servidor de Apache™ Bloodhound. Sin dudas es esta la característica más notable de este gestor de incidencias con respecto a su antecesor Trac, ya que en este último cada instancia permite manejar los datos de un único producto (o proyecto). Apache™ Bloodhound es un proyecto oficial de la Apache Software Foundation, hecho que reafirma su capacidad de ofrecer herramientas que fomenten las mejores prácticas en el área de gestión de proyectos.

Los artículos previos de esta serie (números 50, 51, 54) trataron acerca de algunas innovaciones en la interfaz de usuario que introdujo la versión 0.4.0. En el número 61 se describe la instalación (en Ubuntu 10.04) de la versión 0.7. Ésta es la última versión estable y por consiguiente es utilizada también en este artículo.

Creando múltiples productos con Bloodhound

No es objetivo de este artículo profundizar en todos los detalles técnicos de la solución para múltiples productos que ofrece Apache™ Bloodhound. Sin embargo es importante resaltar muy brevemente algunos puntos importantes para comprender todos los ejemplos que se presentarán a continuación.

Los usuarios de Trac que desean administrar varios proyectos independientes, sólo tienen la opción de instalar varias instancias, cada una con su base de datos independiente, su administración, usuarios, etc... Colocando varios entornos de Trac (i.e. environments) en una carpeta es posible configurar un servidor que publique en la web de una sola vez todos estos datos.

El mismo entorno (i.e. environment) de Trac sigue estando presente en Bloodhound, pero se le llama entorno global. De manera muy simplificada se puede decir que Apache™ Bloodhound ha añadido una columna product en (algunas de) las tablas que define Trac con el fin de almacenar la información de varios productos (proyectos) en una sola base de datos. Cada producto es independiente en el sentido de que tiene una identidad y datos propios. Este enfoque tiene varias ventajas entre las que se pueden mencionar las siguientes:

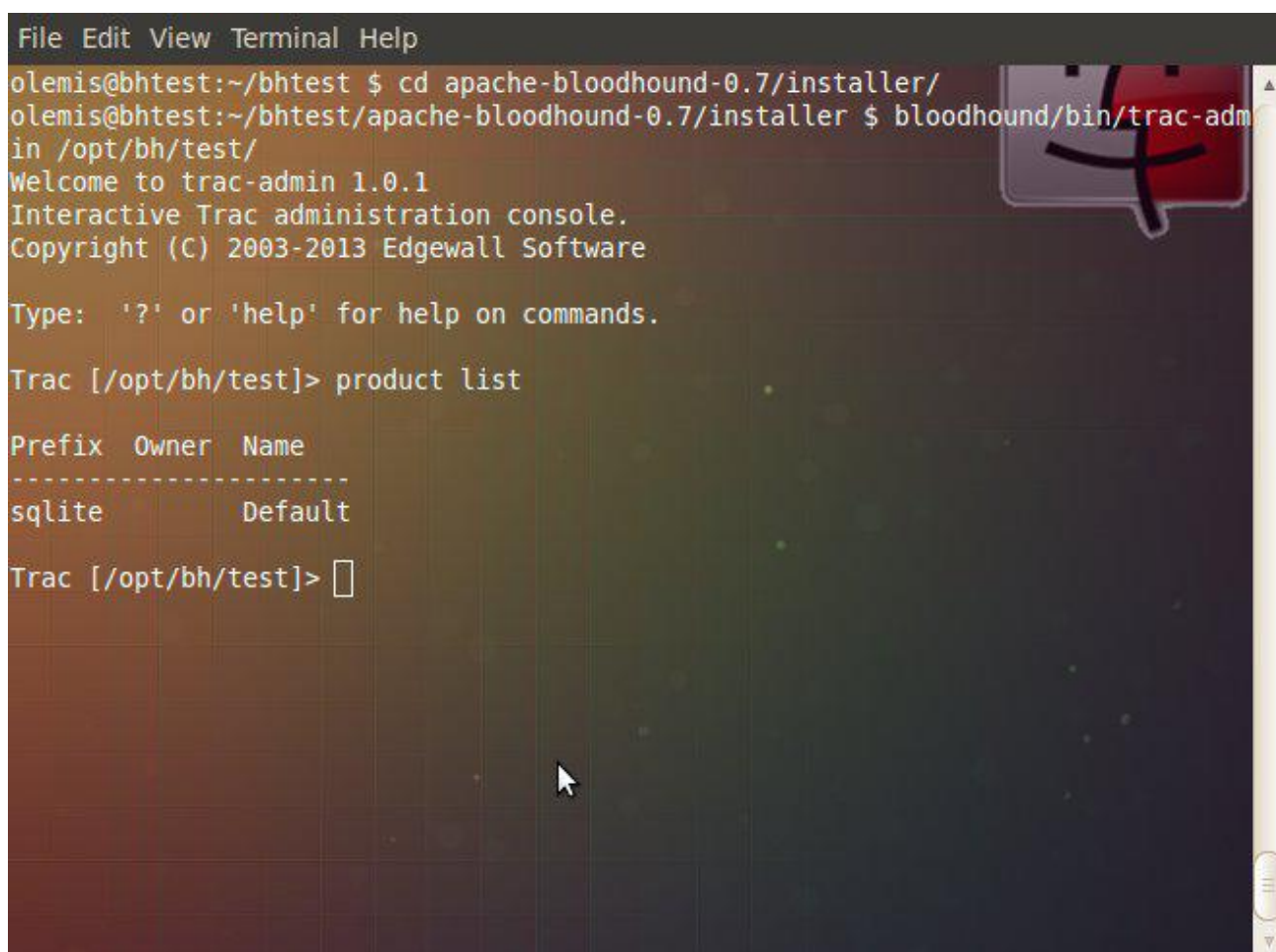
- Basta con una sola consulta para hacer operaciones sobre todos los datos de interés independientemente del producto donde hayan sido definidos.
- Se facilita la administración, búsqueda y análisis de datos.
- Se pueden establecer relaciones entre recursos que pertenecen a dos productos distintos.
- Se comparten los usuarios y sus sesiones para todos los productos definidos en una misma instancia.
- Es posible crear otros datos globales y compartirlos entre varios productos.
- Los reportes pueden reflejar el estado y progreso de varios productos.
- Es posible tener una copia diferente de un mismo recurso para cada producto, en caso de que esto sea apropiado.
- Los permisos se definen para cada producto de manera independiente.
- Se establece una diferencia entre los administradores del servicio (a.k.a. hostmaster) y los de los proyectos (i.e. un rol similar al de los webmasters o jefes de proyectos).
- Se centralizan las tareas de administración.

Entre otros temas, a lo largo de esta serie se ofrecerán ejemplos ilustrando cada uno de los puntos anteriores. El resto de este artículo está dedicado a la administración del sitio desde la consola con el comando `trac-admin`. Se continúa a partir de la instalación descrita en el número 61, por lo que es recomendado leer previamente ese artículo y familiarizarse con los pasos y las opciones de instalación utilizadas.

Creando nuevos productos

Los usuarios de Trac pueden realizar las tareas de administración del entorno del proyecto utilizando la herramienta `trac-admin`. Bloodhound añade varios comandos relacionados con los productos. Cada producto tiene los siguientes atributos :

- prefijo: identificador del producto (proyecto) e.g. `dataviz`.
- nombre: el nombre del producto e.g. `Bloodhound Data Visualization API`.
- descripción: texto que describe brevemente el propósito del producto.
- dueño: nombre de usuario del dueño del producto.



```
File Edit View Terminal Help
olemis@bhctest:~/bhctest $ cd apache-bloodhound-0.7/installer/
olemis@bhctest:~/bhctest/apache-bloodhound-0.7/installer $ bloodhound/bin/trac-admin
in /opt/bh/test/
Welcome to trac-admin 1.0.1
Interactive Trac administration console.
Copyright (C) 2003-2013 Edgewall Software

Type: '?' or 'help' for help on commands.

Trac [/opt/bh/test]> product list

Prefix  Owner  Name
-----
sqlite          Default

Trac [/opt/bh/test]> 
```

Para entrar en calor ejecutamos el script `trac-admin` creado en el environment virtual de Python donde se instaló Bloodhound. Como se puede apreciar el comando `product list` enumera los productos existentes inmediatamente después de la instalación. En el ejemplo se utiliza el entorno creado previamente con una base de datos SQLite. Note que el prefijo del producto coincide con el valor del parámetro `--default-product-prefix` especificado durante la instalación (ver artículo en TuxInfo 61).

```
File Edit View Terminal Help
Trac [/opt/bh/test]> help product
product add <prefix> <owner> <name>

    Add a new product

product admin <PREFIX> <admin command>

    Execute admin (sub-)command upon product resources

product chown <prefix> <owner>

    Change product ownership

product list

    Show available products

product remove <prefix>

    Remove/uninstall a product

product rename <prefix> <newname>

    Rename a product

Trac [/opt/bh/test]> █
```

Con ayuda del meta-comando help podemos ver todas las operaciones que se pueden realizar con los productos. Empecemos por lo básico.

```
File Edit View Terminal Help
Trac [/opt/bh/test]> product add prueba_tuxinfo olemis
                        "Pruebas para artículos de TuxInfo"
Trac [/opt/bh/test]> product list

Prefix      Owner      Name
-----
sqlite      Default
prueba_tuxinfo olemis  Pruebas para artículos de TuxInfo

Trac [/opt/bh/test]> █
```

Creamos otro producto prueba_tuxinfo que será utilizado en los ejemplos de la serie. Para ello se le suministra al comando product add el prefijo, el usuario del dueño del producto (i.e. olemis) y el nombre del producto.


```
File Edit View Terminal Help
Trac [/opt/bh/test]> product chown prueba_tuxinfo admin
Trac [/opt/bh/test]> product rename prueba_tuxinfo "Pruebas para TuxInfo"
Trac [/opt/bh/test]> product list

Prefix      Owner  Name
-----
sqlite      Default
prueba_tuxinfo admin  Pruebas para TuxInfo

Trac [/opt/bh/test]> █
```

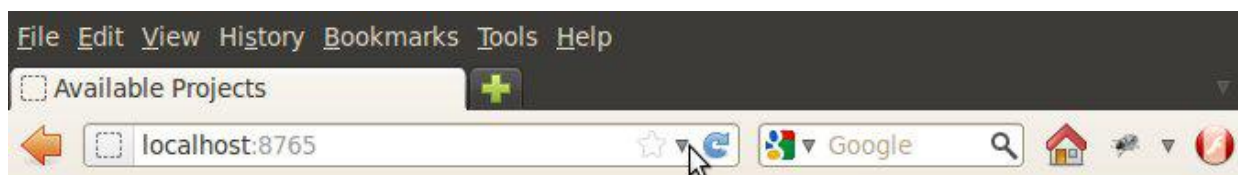
Sin embargo el usuario y el nombre del producto no son correctos, así que se rectifican esos datos utilizando los comandos `product chown` y `product rename`.

Creando productos a través de la interfaz web

También es posible crear un producto a través de la interfaz web.

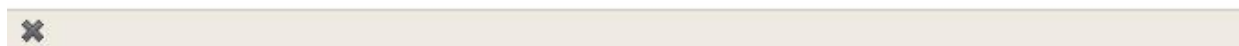
```
File Edit View Terminal Help
olemis@bhctest:~/bhctest/apache-bloodhound-0.7/installer $ bloodhound/bin/tracd
-e /opt/bh --port=8765
Server starting in PID 13675.
Serving on 0.0.0.0:8765 view at http://127.0.0.1:8765/
Using HTTP/1.1 protocol version
█
```

Iniciamos el servidor tracd como se muestra en la figura anterior.

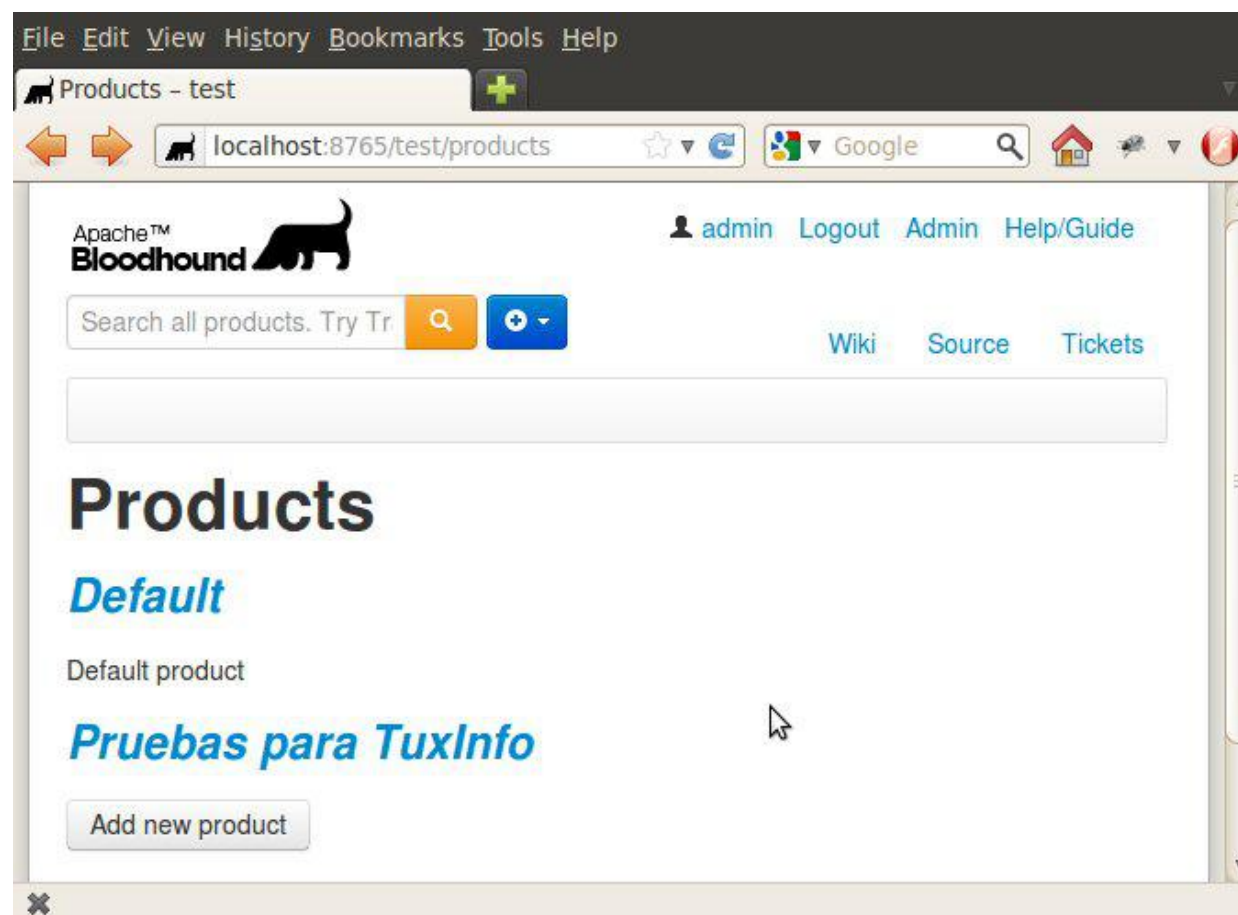


Available Projects

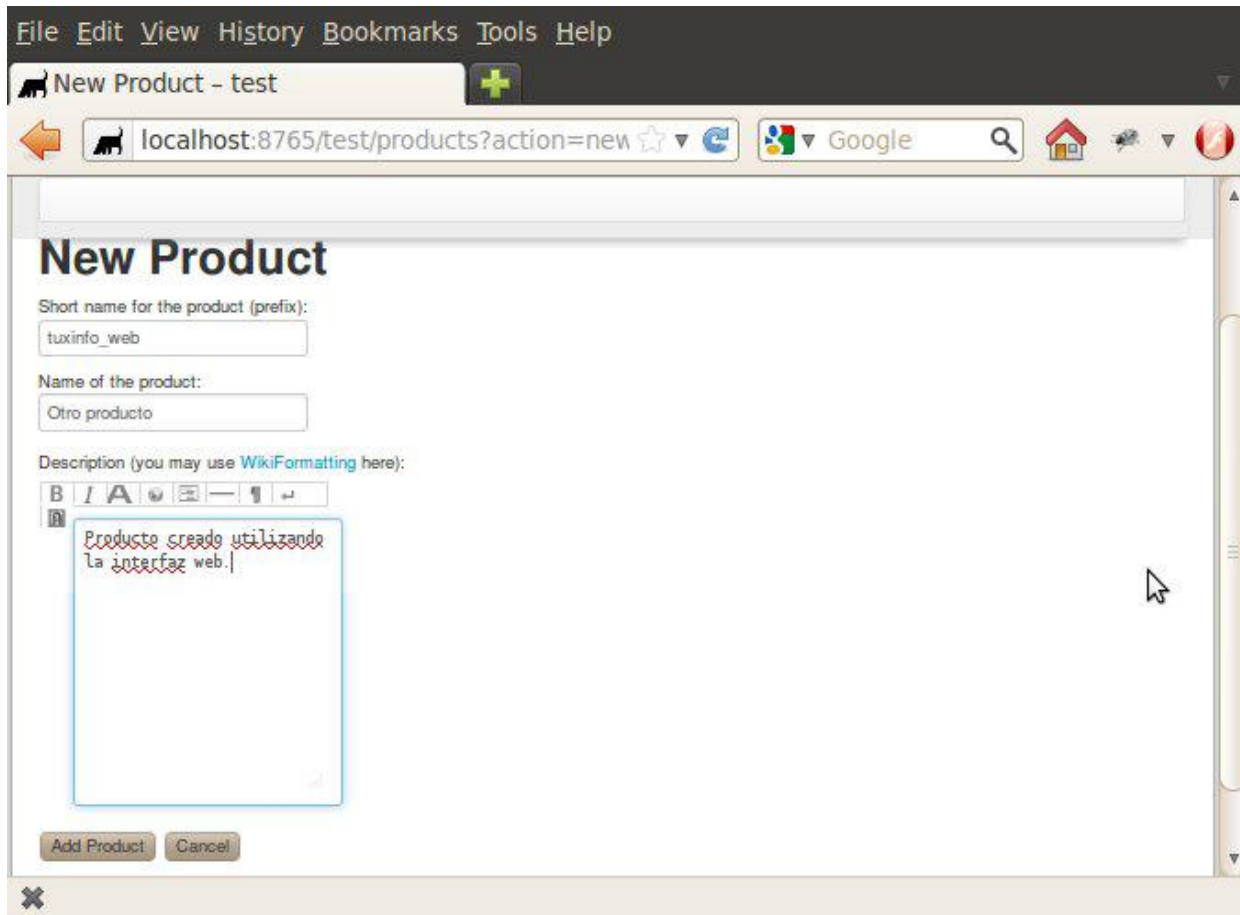
- [main](#)
- [test](#)



Al visitar la página <http://localhost:8765> vemos la lista de los entornos instalados. Es preciso recordar que el entorno main fue creado con una base de datos PostgreSQL, mientras que test utiliza una base de datos SQLite.



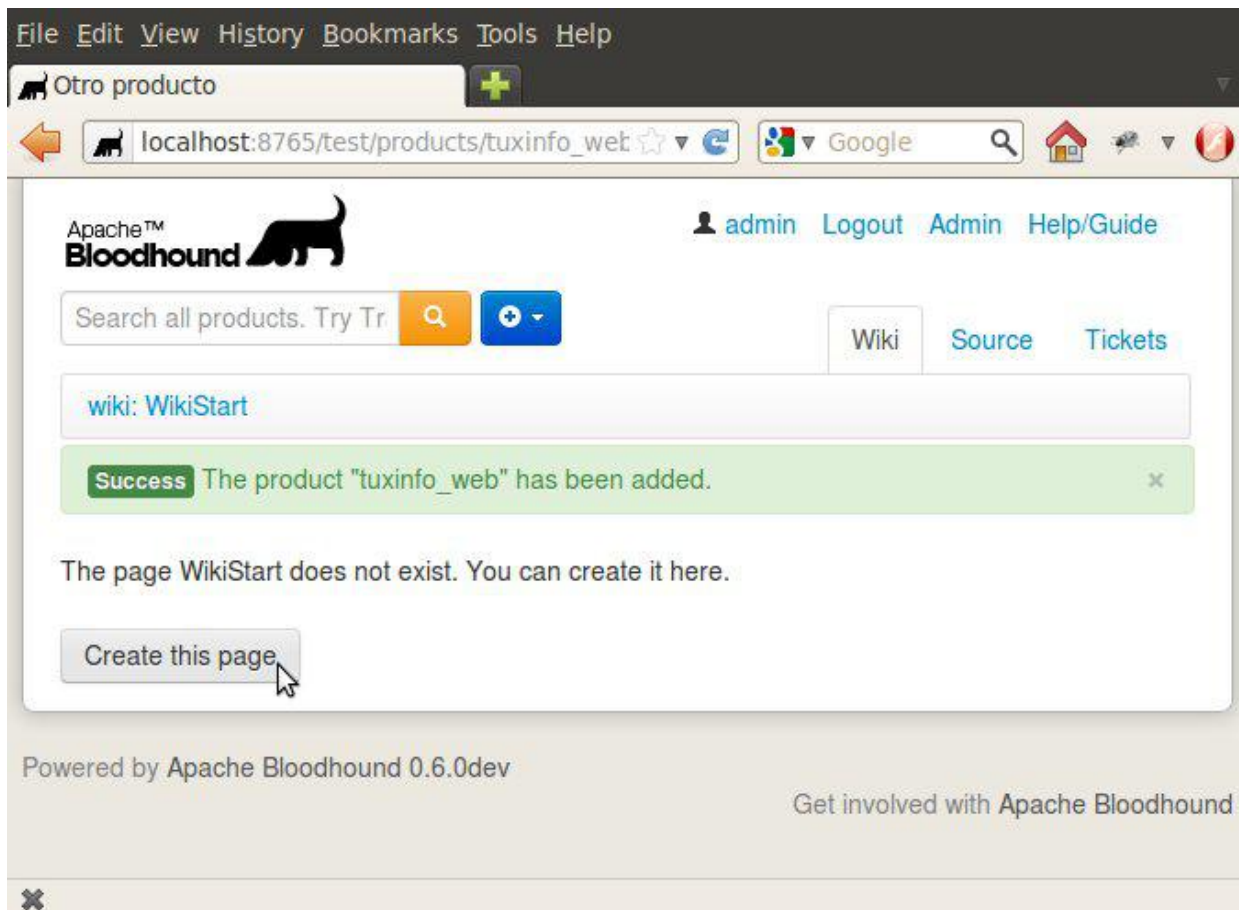
Al navegar a la URL <http://localhost:8765/test/products> aparece la lista de productos. Los usuarios con permisos pueden añadir un producto haciendo click en el botón Add new product.



The screenshot shows a web browser window with the address bar displaying `localhost:8765/test/products?action=new`. The page title is "New Product". The form contains the following fields and elements:

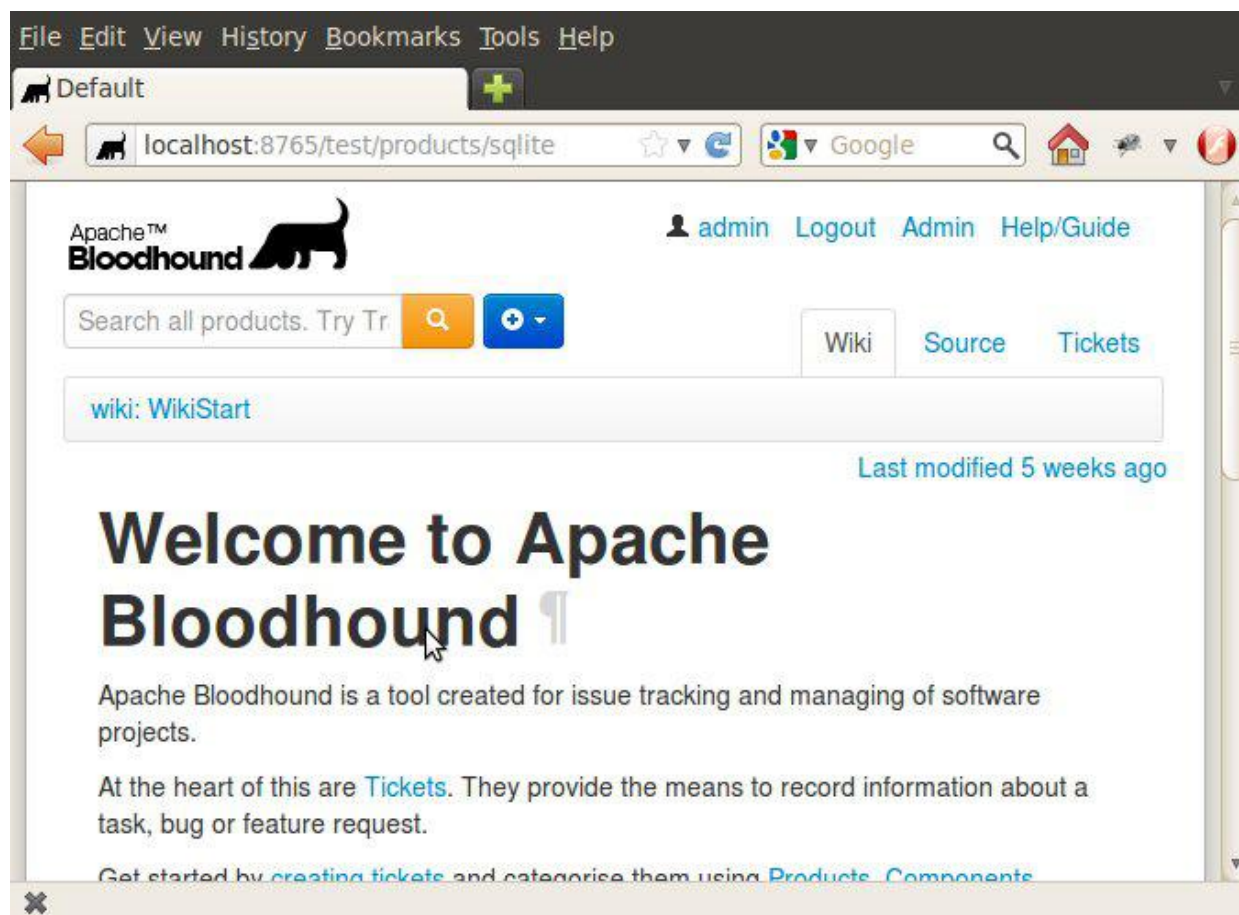
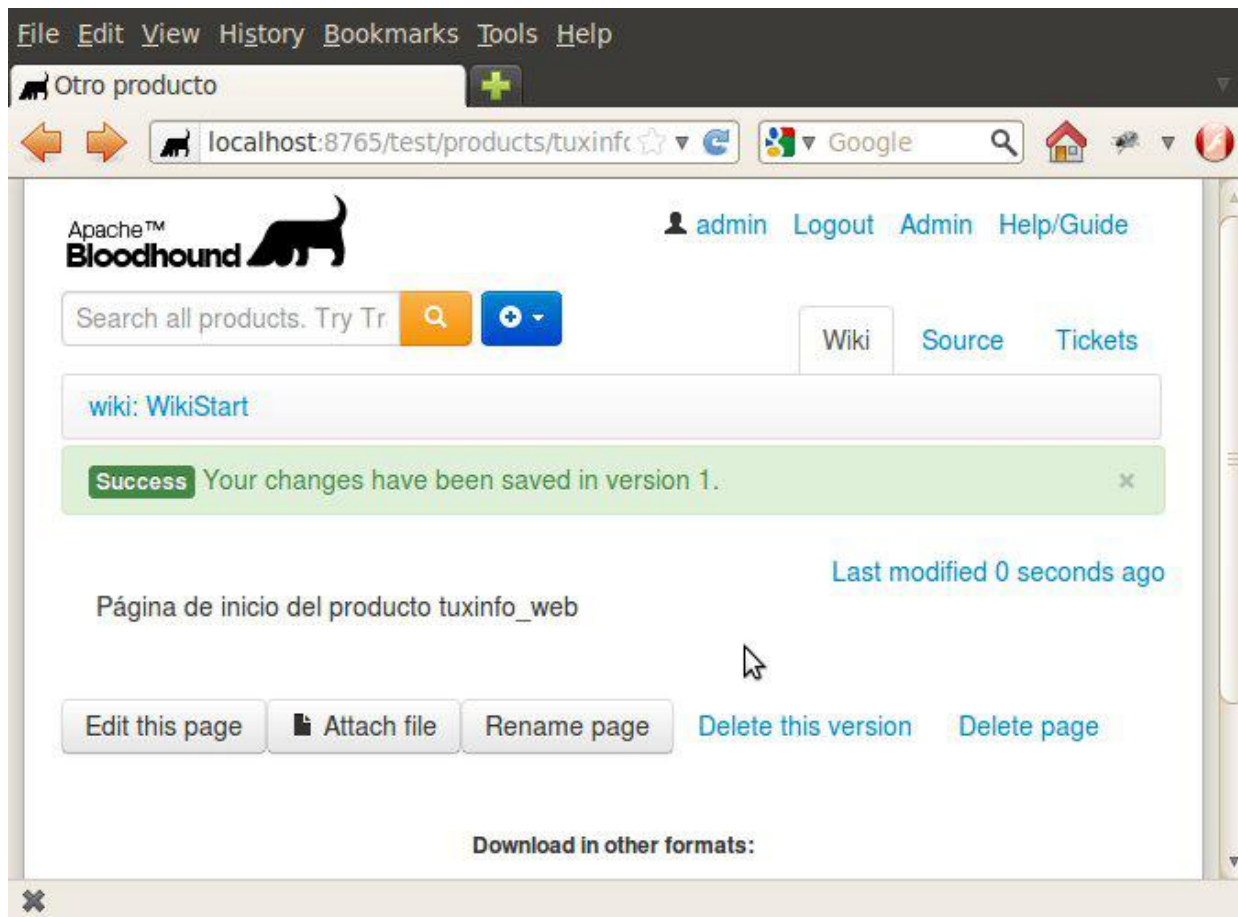
- Short name for the product (prefix):** A text input field containing "tuxinfo_web".
- Name of the product:** A text input field containing "Otro producto".
- Description (you may use WikiFormatting here):** A text area with a rich text editor toolbar. The description text is "Producto creado utilizando la interfaz web.".
- Buttons:** "Add Product" and "Cancel" buttons at the bottom left.

Después de llenar los campos del formulario añadimos otro producto. El sistema muestra un mensaje de confirmación y nos lleva a la página de inicio del producto, que en este caso es la wiki.



The screenshot shows the Apache Bloodhound product page in a web browser. The address bar displays `localhost:8765/test/products/tuxinfo_web`. The page features the Apache Bloodhound logo and navigation links: "admin", "Logout", "Admin", and "Help/Guide". A search bar is present with the text "Search all products. Try Tr". Below the search bar, there are tabs for "Wiki", "Source", and "Tickets". A green success message box states: "Success The product 'tuxinfo_web' has been added." Below this, a message says: "The page WikiStart does not exist. You can create it here." A button labeled "Create this page" is visible, with a mouse cursor hovering over it. The footer of the page includes the text "Powered by Apache Bloodhound 0.6.0dev" and a link to "Get involved with Apache Bloodhound".

Con el fin de explicar la utilidad de los productos editamos esta página haciendo click en el botón Create this page e introduciendo un corto texto.



Observe la página de inicio del producto sqlite en <http://localhost:8765/test/products/sqlite>. Como es posible apreciar en la figura el navegador web muestra una wiki generada durante la instalación de Bloodhound. Si comparamos las dos últimas páginas se puede notar una diferencia importante. Observando la parte superior izquierda se puede constatar que ambas se llaman WikiStart, pero sus contenidos son diferentes. Podemos concluir entonces que cada producto tiene sus propias páginas wiki.

Conclusiones

Es posible utilizar el script trac-admin o la interfaz web para crear y administrar varios productos en una sola instancia. Todos los datos se guardan en una sola base de datos. Como resultado cada producto tiene su propio conjunto de páginas wiki.

No se pierda los próximos números de la revista TuxInfo si desea conocer todo lo que se puede lograr con los productos y las herramientas que ofrece el gestor de incidencias Apache™ Bloodhound.

Proyecto Bloodhound

Sitio web: <http://bloodhound.apache.org>

Lista de discusión: dev@bloodhound.apache.org

Gestor de incidencias <https://issues.apache.org/bloodhound>

Extensiones: <http://blood-hound.net>



Olemis Lang

olemis@gmail.com

Blog ES: <http://simelo-es.blogspot.com>

Blog EN: <http://simelo-en.blogspot.com>

Twitter: [@olemislc](https://twitter.com/olemislc)

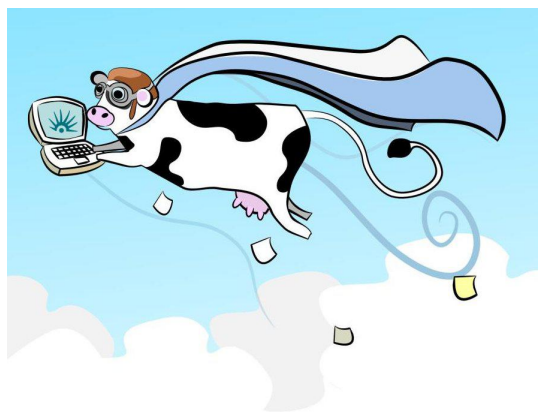
Recomendado: Popularidad de Python, septiembre 2013

<http://goo.gl/fb/tr0XB>



#RADIOGEEK
Podcast diario de
Tecnología

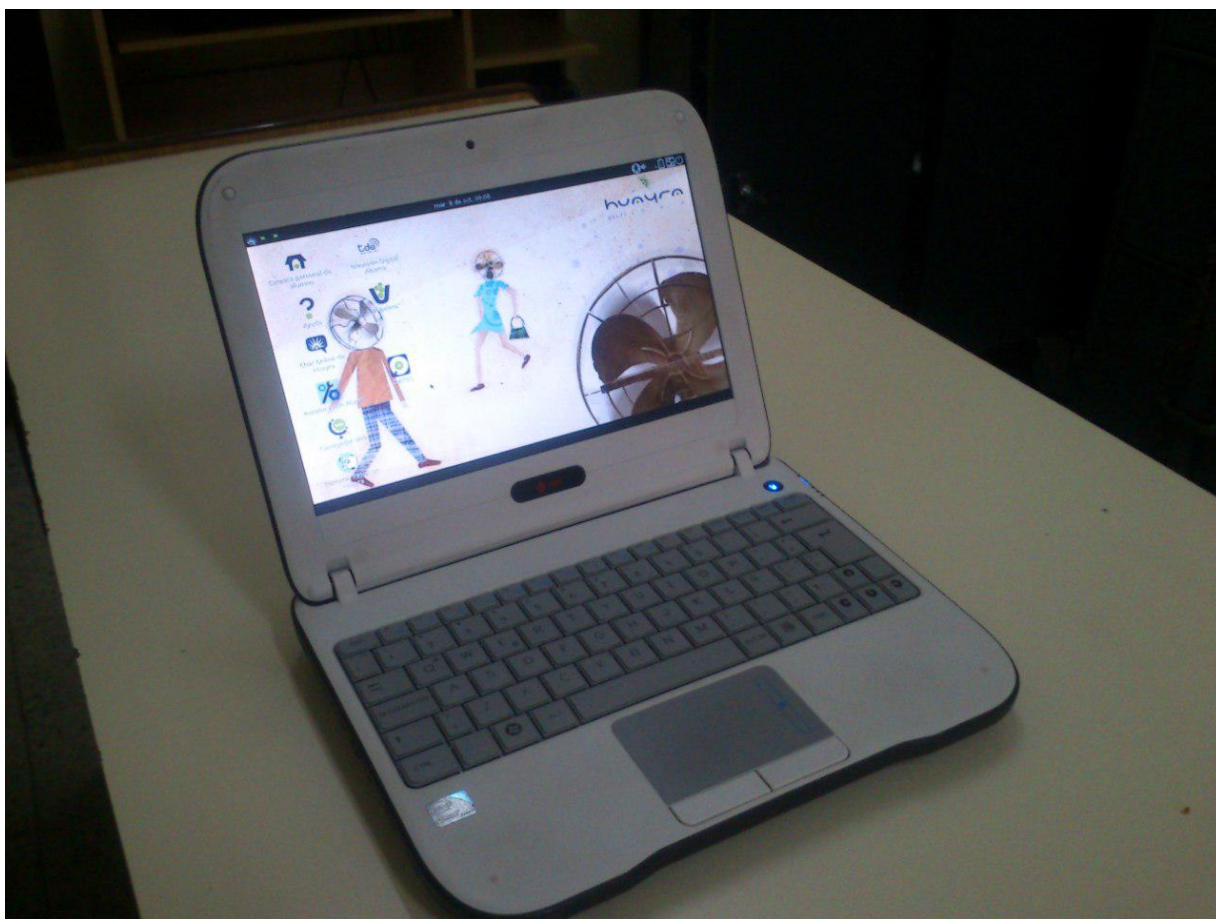
www.radiogEEK.ivoOX.com



Huayra, la distribución GNU/Linux del Estado Nacional Argentino

Por María Eugenia Núñez

En el año 2010, el Estado Nacional Argentino, comienza la implementación del Programa Conectar Igualdad entregando netbooks a docentes y alumnos de escuelas secundarias, especiales y de formación docente. Desde sus inicios, los equipos se ofrecen con dual boot: XP/Windows 7 y una distro GNU/Linux que fue cambiando con el transcurso de los años. La primera fue RXart, del que mucho se ha hablado porque nunca estuvo disponible ni siquiera la ISO (imagen descargable) para su descarga. Sólo se podía conocer lo que tenía a través de los listados de aplicaciones que ofrecía la empresa desarrolladora y nunca funcionó. Poco a poco, surgieron a lo largo y ancho del país docentes, que en forma individual, proponían instalaciones alternativas desde Arch Linux hasta distintas versiones de Ubuntu. El PCI tomó nota de esto y la distribución incluida en los equipos fue variando con el transcurso del tiempo.



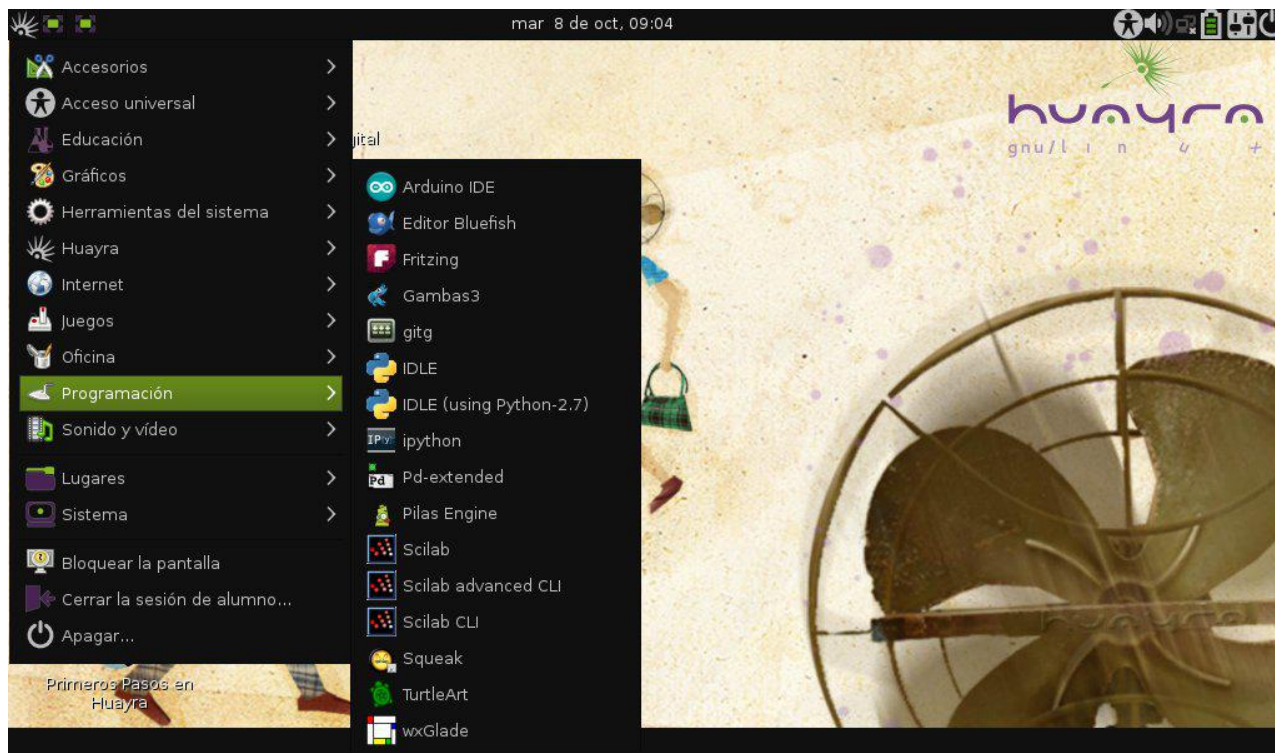
Desde el comienzo, distintas organizaciones y comunidades han sostenido la importancia de que los equipos entregados por el Estado Nacional utilicen Sistemas Operativos Libres. Hoy Huayra se presenta como la alternativa real al sistema operativo que domina el mercado y, por primera vez, es decisión del propio Estado desarrollar y darle prioridad de booteo, desde agosto del 2012, a un Sistema Operativo Libre.

Huayra es un sistema basado en Debian Wheezy, adaptado para ser accesible a alumnos acostumbrados a lidiar con Windows. A Debian, se le incorporó el entorno de escritorio Mate (fork de Gnome2), un repositorio de

aplicaciones propias y un diseño gráfico que lo identifica. Instalado en una netbook, Huayra tiene la estabilidad necesaria para que los usuarios descubran el mundo del Software Libre presentándose como el primer paso a otro tipo de cambios.

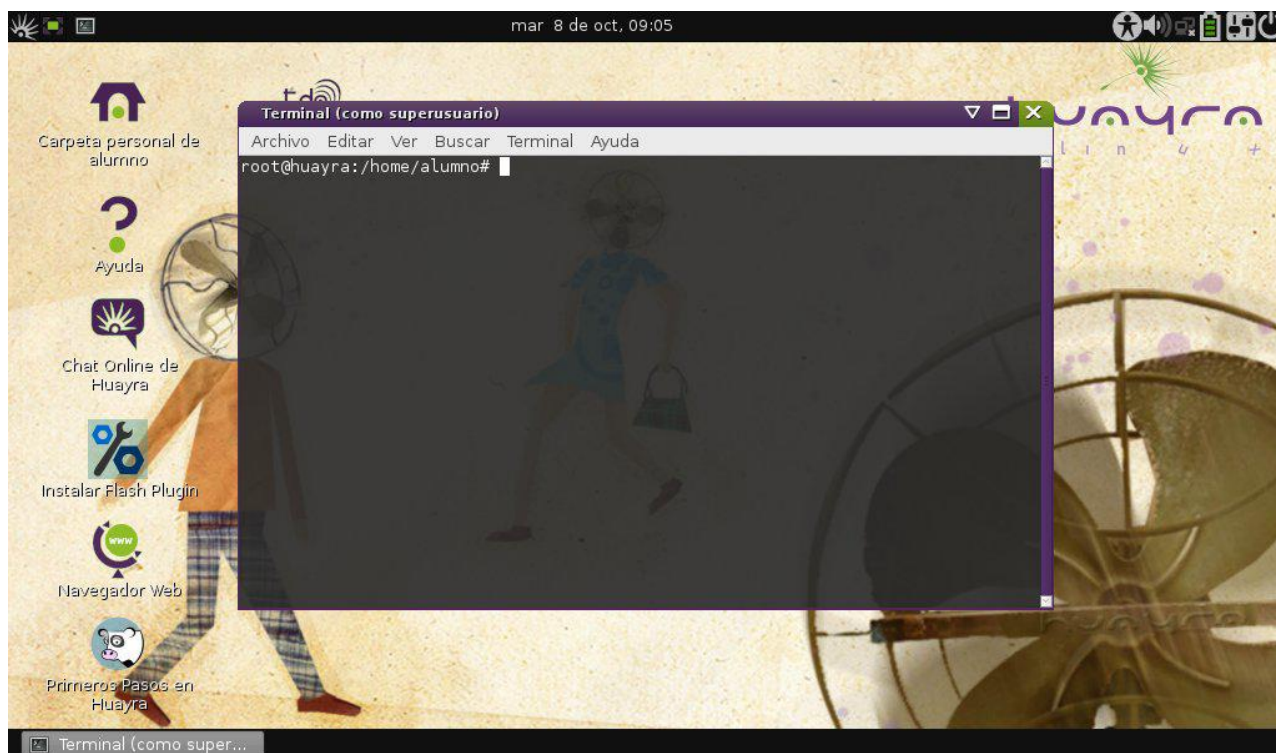


Desde el punto de vista del docente usuario de tecnología, tiene todo lo que se requiere de un Sistema Operativo pensado para el aula. Mate es un entorno gráfico amigable con una buena selección de herramientas para administrar el sistema. Permite instalaciones desde un Centro de Software, con programas como Synaptic y una terminal de root. Utiliza los repositorios estables de Debian y propios brindando la posibilidad de mantener el equipo actualizado.



La amplia variedad de aplicaciones disponibles permite, en principio, prescindir de instalaciones adicionales. Entre ellas encontraremos desde procesadores de texto hasta entornos de aproximación al desarrollo y la programación acordes a la edad de los alumnos destinatarios. En lo personal, destaco la buena elección que se hizo al no

modificar el entorno de escritorio pretendiendo que su aspecto general y menús se parezcan a otra cosa.



Al día de hoy fueron entregados cerca de 3.500.000 de equipos y gran parte de ellos no tienen instalado Huayra. Esto puede remediarse descargando la iso desde la página de Conectar Igualdad, instalarla en un pendrive para arrancar en modo live e instalarla en poco menos de 20 minutos. En la misma página encontramos un paquete deb que al ejecutarse realizará tareas tales como ocultar las particiones del Sistema de Recuperación y de Windows, montar la participación en la que se archivan los documentos (se trata de una partición NTFS ya que es utilizada desde ambos sistemas operativos), crea enlaces a las principales carpetas de almacenamiento y permite la instalación del plugin de flash. También recomienda la ejecución de comandos para actualizar todo el sistema.

Desde su presentación en sociedad el pasado 13 de septiembre, mucho hemos leído respecto de si Huayra puede ser considerado libre o no. La realidad es que el equipamiento entregado por el PCI desde sus comienzos tiene aproximadamente 30 modelos de netbooks diferentes. Esto significa una amplia variedad de hardware, mucho del cual no dispone de controladores y firmwares libres. Frente a esta situación existen sólo dos opciones: distribuir un SO que no pueda ser usado en todas las netbooks u otro que, contemplando las limitaciones del hardware, sea lo más libre posible. En lo personal y sin dudar, elijo la segunda opción ya que para trabajar en un aula es imprescindible un sistema estable, que no provoque pérdidas de tiempo con actualizaciones ni antivirus y, entre otras cosas, reconozca dispositivos externos sin instalaciones adicionales.

Falta todo un camino por recorrer y, mirando a futuro, no me cabe la menor duda de que el objetivo es lograr de Huayra un Sistema Operativo completamente libre que ni siquiera requiera de un TPM como seudo protección contra el robo. Esto solo se logrará con la continuidad de políticas de estado que persistan en el proyecto, brindando a todos los jóvenes igualdad de oportunidades para acceder a la alfabetización digital y tecnológica. El camino recorrido es bueno y lo mejor está aún por venir.



por **María Eugenia Núñez**
<http://www.demasiadoalup.com.ar/>
Eugenia Nuñez en G+
euge_nunez en twitter



La respuesta a la decepción celular

Por Claudio De Brasi

La decepción en términos informáticos es algo muy sufrido por los usuarios. Uno espera tales funciones de una máquina o Sistema Operativo y el mismo brinda una porción menor de esa función o ninguna. Muchas veces se tendía a solucionar estas faltas en los programas con algún otro complemento. Cambiar el sistema por una versión nueva (upgrade), Instalar un nuevo programa para cumplir con el fin esperado.

En la época actual esto se ha expandido a los teléfonos inteligentes. Pero los proveedores de dichos aparatos no les gusta que el usuario use mucho tiempo el teléfono, quieren que el usuario compre un aparato nuevo en forma constante. Por esto muchos usuarios no tienden a actualizar el teléfono más allá de cierto tiempo, sin importar las condiciones de hardware para ello.

Para tomar un ejemplo: Un teléfono que llega con sistema operativo Android 2.3.4 diseñado en 2011, pero salió a la venta en 2012, con una actualización "tardía" a fines 2012 a 4.0.4, (Cuando ya estaban los nuevos en 4.1), y para colmo el fabricante decidió no actualizar este modelo a 4.1. Para colmo de males un diseño 2012 con apenas 200 Mhz más de reloj e iguales características excepto la cámara, (Más chica), Si tiene esta actualización. Para mi gusto la "Obsolescencia programada" ya esta muy exagerada.

Otra decepción muy común es con los teléfonos que los proveedores de telefonía celular venden con herramientas de software propias del proveedor. Si uno compara el teléfono comprado directamente del fabricante se encuentra que el último anda más rápido y con menos cuelgues. Esto se debe a que el celular está sobrecargado de servicios.

En algunos casos los usuarios con más conocimiento empiezan por desinstalar o deshabilitar servicios que no se usan, que son redundantes, o peor, que sólo están para hacer publicidad. Otros recurren a medidas más extremas como cargar una nueva ROM al celular. Estas últimas no son tan recomendadas por los expertos en seguridad ya que no saben quién la elaboró ni qué cosas agregó o quitó. (La cuestión es que tampoco saben qué realizó el fabricante y el proveedor con el celular). aún así algún que otro usuario opta por el cambio. Para seguir con el ejemplo anterior. El teléfono que no se actualizó a 4.1 por el fabricante, hay ROM de Android versión 4.2.2 estable y están en versión alfa de la 4.3 y esperando 4.4 y 5.0.

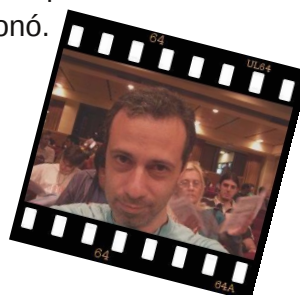
Una vez un fabricante de CPU's dijo que "Debían desarrollar no sólo el tener más transistores por pulgada, sino qué mejoras se puede hacer con ello. Ya que si no progresaban en ello algún competidor podría hacerlo mejor que ellos".

Uno de los grupos que hacían estas ROM ha decidido hacer punta, Cyanogenmod se ha lanzado como empresa Cyanogen Inc. y están brindando ROM propias, nuevos servicios y cosas que realmente abofetean a los fabricantes de celulares. Ya que mejoran los propios equipos de estos.

Al enterarme de esta noticia sólo la puedo comparar con 2 casos previos en la historia de la computación. Cuando Compaq ofreció una PC 100% compatible con IBM-PC. y cuando RedHat pasó a brindar S.O. igual de confiables y más baratos que SCO y con su código fuente.

Sea cual sea el caso, esta es una posible respuesta a la decepción celular. Pero, si un usuario llega a ella, es en gran parte porque el fabricante y el proveedor los decepcionó.

PD: Calma, paciencia, Esperar el estable y ver si la pileta tiene agua antes de tirarse a ella.



Claudio De Brasi.
@Doldraug



TubeMate 2

Descargas de YouTube sin límites...

Por Juan Manuel Dansa

Este mes he elegido esta excelente aplicación, la cual ya se encuentra en su versión 2; la misma nos permite la descarga de videos o audio desde YouTube.

Dentro de las novedades, podemos destacar el cambio de la interfaz a la tan conocida estilo HoLo la cual le da una excelente presencia y comodidad de uso gracias a la barra de opciones lateral. Otros puntos a destacar son la mejora en las descargas con soporte DailyMotion, Facebook, Youku, vídeos HTML5, pausar / reanudar (Wifi solamente), cambios en la lista de reproducción, motor de búsqueda más potente, lo que nos permite la búsqueda de archivos locales como de YouTube en forma manual o por voz.

Descarga e instalación

Para la descarga se recomienda siempre desde el sitio oficial <http://tubemate.net/>, en donde se encuentran los servidores autorizados para la descarga; tengamos en cuenta que la aplicación por la función que cumple no puede alojarse en el Play Store de Google. También nos encontramos que TubeMate 2 posee publicidad en forma de los tan conocidos banners, molestos para algunos y que en mi caso no interfieren ni me cambian la forma de usarlo. Un punto a destacar es que existe para su descarga de una versión para BlackBerry PlayBook con su correspondiente guía de instalación, pero en versión 1.05.55 de la aplicación.



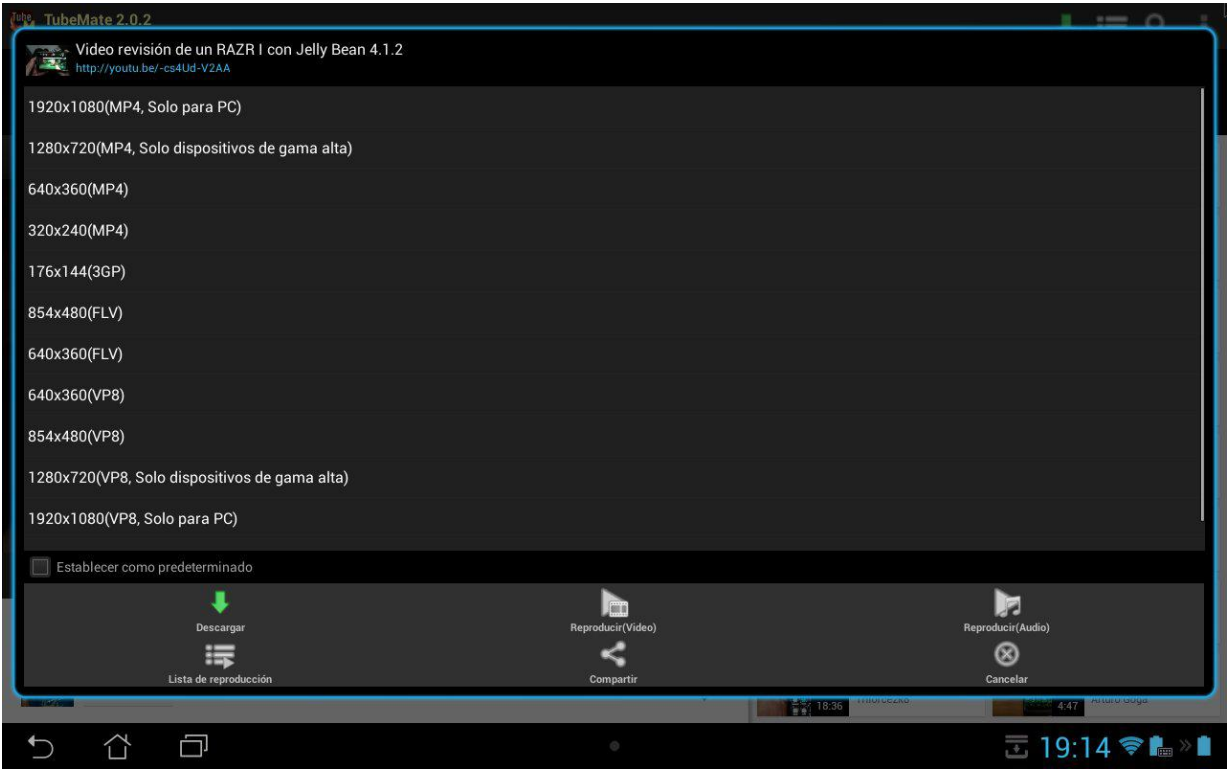
NOTA: Hay que tener en cuenta que esta aplicación fue durante un tiempo muy infectada, ya que la misma es muy conocida y famosa; por ende no descargarla por fuera del sitio oficial.

La instalación es muy sencilla, se instala como cualquier APK que se encuentre fuera del Play Store, simplemente habilitando los permisos para instalación en menú Seguridad y dentro de este tildando en Orígenes Desconocidos

(tener en cuenta que no todos los dispositivos poseen los mismos menús, por consiguiente deberán buscar la opción en otra ubicación).

Recorrido en algunas funciones...

TubeMate 2 se destaca por la descarga de videos de YouTube, los mismos en formato .mp4, 3GP, FLV o VP8, y lo más destacable es que podremos guardarlos en la definición que deseemos; cada video nos mostrará diferentes definiciones dependiendo de con cual haya sido subido.



Opciones de Descarga, diferentes definiciones y formatos.

Con respecto al audio, en el caso que sólo queramos este y no la parte visual, el mismo puede ser guardado en .mp3. Esta función no es el fuerte de la aplicación pero para una descarga de un audio de forma rápida cumple a la perfección.



*Opción
descarga
MP3*

Otra opción a tener en cuenta es la de poder ingresar a nuestra cuenta de YouTube y acceder a nuestros canales donde nos encontramos inscriptos, listas de reproducción, posibilidad de compartir, etc., muy similar a las funciones de YouTube nativas.

Dentro de las preferencias propias de la aplicación nos encontramos con la posibilidad de limitar la cantidad simultánea de descargas, múltiples conexiones para acelerar las mismas, descarga de los subtítulos en formato SMI si se encuentran en el idioma previamente predeterminado, poder elegir locación de donde llegarán los videos y audio, opción de utilizar el reproductor interno o no, y muchas otras que hacen de esta aplicación más que interesantes.

Opinión

En el mundo de Android las opciones son infinitas, desde modificar un Kernel hasta como en este caso aplicaciones fuera del Play Store de Google, que verdaderamente valen la pena. Mi experiencia con TubeMate es desde sus principios, ya que la necesidad de descarga de audio y video de YouTube siempre estuvo; un pro de esta aplicación es su constante actualización, lo que a su vez se transforma en su contra, ya que los avisos de actualización no siempre llegan y hay que dirigirse a su página para descargarla, pero vale la pena pasarse una vez por semana y verificar. El uso más importante en mi caso es bajar videos que luego no podré ver por falta de conexión, con la ventaja de poder elegir la definición y poder compartir el mismo con otra persona o bajarlo a un ordenador; por ende es una de mis aplicaciones favoritas que no me pueden faltar para acrecentar mi videoteca!. Mi puntaje: 9/10

La yapa...AppGratis



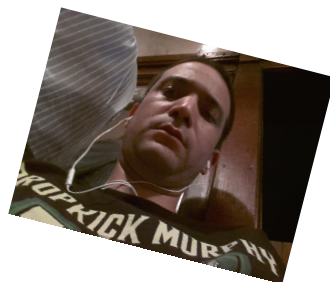
Esta aplicación fue muy famosa en su momento por ser expulsada del App Store de Apple, la misma se encuentra a cargo de Simon Dawlat quien fundó la aplicación en el año 2008; este culebrón informático potenció su fama y llevó a la aplicación al Play Store de Google, donde hoy en día la podemos encontrar y descargar gratuitamente. Y, ¿Cuál es su finalidad?... Su finalidad es irnos ofreciendo día a día una aplicación paga del Play Store de forma gratuita o con un descuento del 90%!! en la mayoría de los casos, posee un sistema de notificaciones que si lo deseamos día a día nos informará que ha salido una nueva aplicación.



La verdad, es muy jugosa AppGratis, ya que nos acerca aplicaciones o juegos de forma gratuita o con suculento descuento; en mi caso se ha transformado en parte fundamental del paquete de aplicaciones de mis dispositivos, ya sea tabletas o smartphones, el único inconveniente que veo es que en 10.1" queda, como es muchas veces costumbre en Android, estirada la pantalla y sólo se puede utilizar en forma vertical no aportando una versión para este tipo de tabletas; aunque en 7" es más tolerable.



Se puede descargar desde su página oficial: <http://appgratis.com/ar/android> o directamente desde el Play Store de Google: <https://play.google.com/store/apps/details?id=com.imediapp.appgratisv3>, así que a disfrutar de forma diaria con las sorpresas de AppGratis!!!!

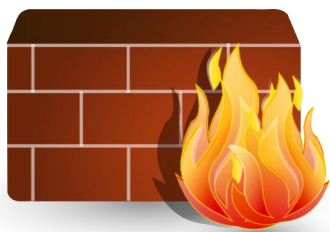


Juan Manuel Dansa (Amonal)
amonal88@gmail.com
twitter: @Amonal_
g+: Amonal Novell

**Curso de
ASTERISK VOIP
EXPERT**

Requiere conocimientos
básicos de Linux.

PROMOCIÓN HASTA AGOTAR VACANTES
Hasta 12 pagos con tarjeta de crédito.



Usando firewallD en Fedora

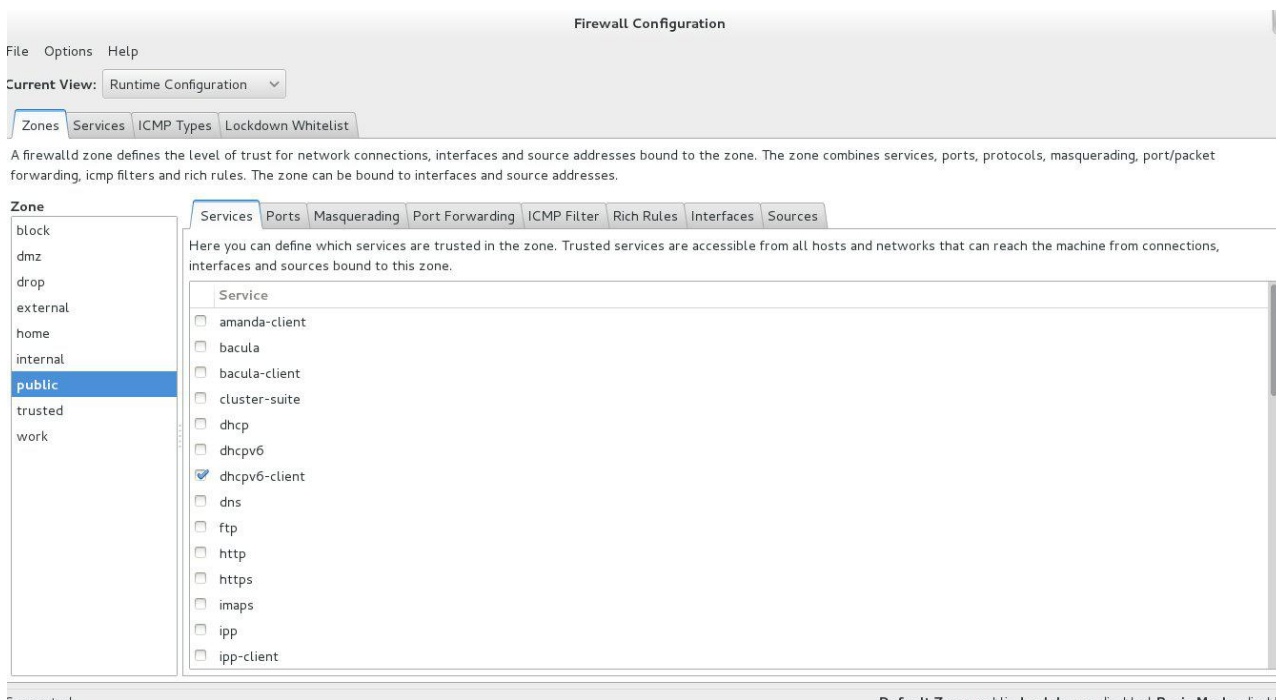
Por Rino Rondan

Vamos a hablar un poco acerca de algunas características de firewallD:

- * Reemplazo de iptables, iptables-ipv6, system-config-firewall
- * Totalmente Dinámico (evita el reinicio del servicio, módulos de netfilter)
- * El daemon que lo maneja aplica los cambios sin necesidad de ser reiniciado.
- * No toma las reglas que se cargan desde la línea de comando que no sean cargadas con sus herramientas
- * Utilización de D-BUS para obtener información acerca del firewall y sus estados.
- * Acepta modificaciones por medio de D-BUS utilizando métodos de autenticación con PolicyKit, por lo cual las aplicaciones, daemons o usuarios pueden interactuar con este por medio de D-BUS.
- * Integración con SELINUX
- * Permite configuraciones por un tiempo determinado
- * Configuración sobre servicios, puertos, protocolos, área segura de redes/interfaces/equipos, reenvío de paquetes/puertos, masquerading y icmp blocking entre otras cosas.
- * Implementación de zonas y servicios.

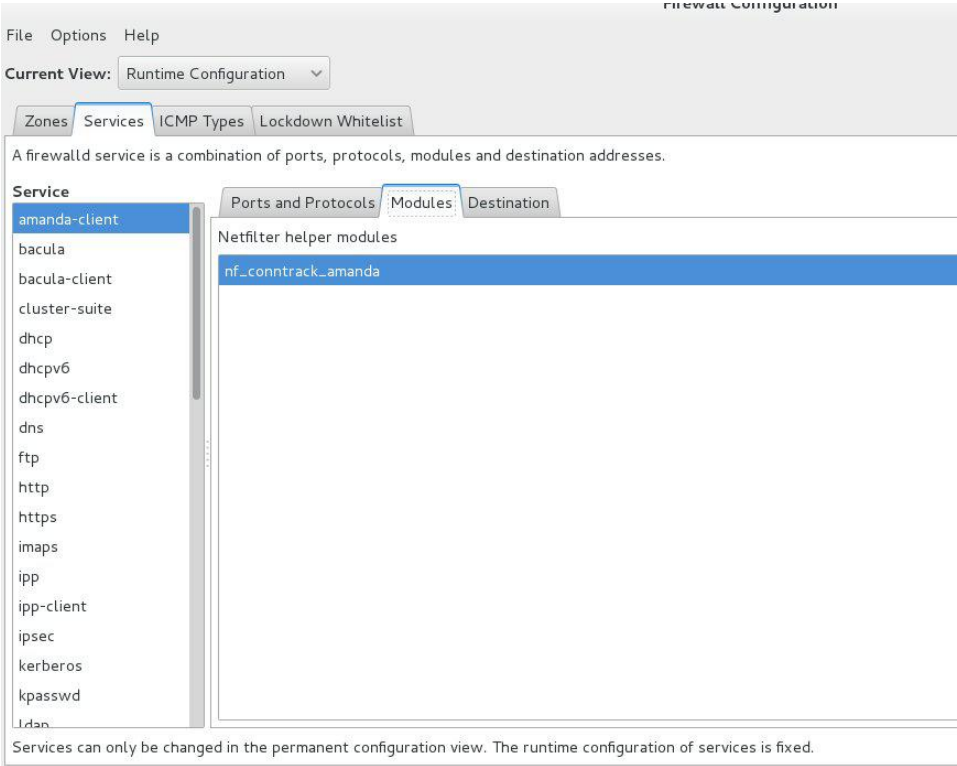
¿Qué es una zona?

Una zona de red define el nivel de confianza para las conexiones de red. Esta es una relación de uno a muchos, lo que significa que una conexión solo puede ser parte de una zona, pero una zona se puede utilizar para muchas conexiones de red.



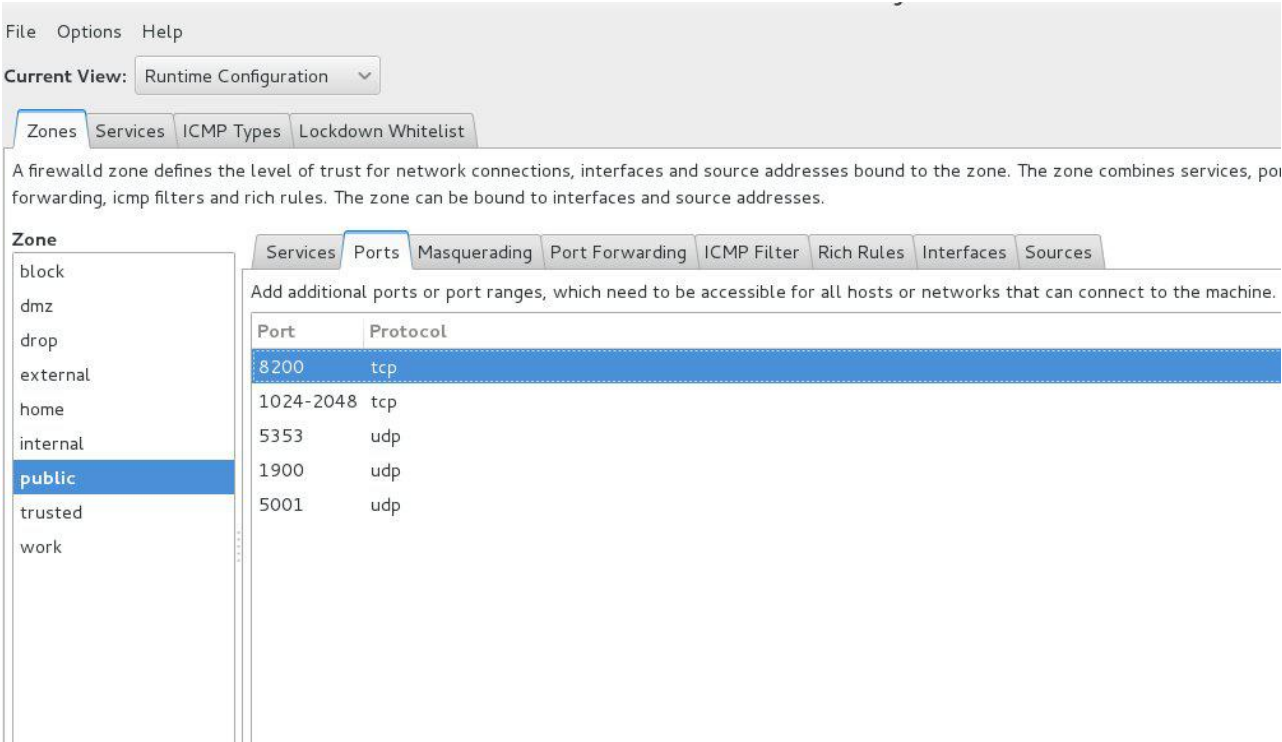
Servicios Predefinidos

Un servicio es una combinación de puerto y/o entradas de protocolo. Opcionalmente módulos auxiliares de netfilter se pueden agregar y también una dirección de destino IPv4 e IPv6.



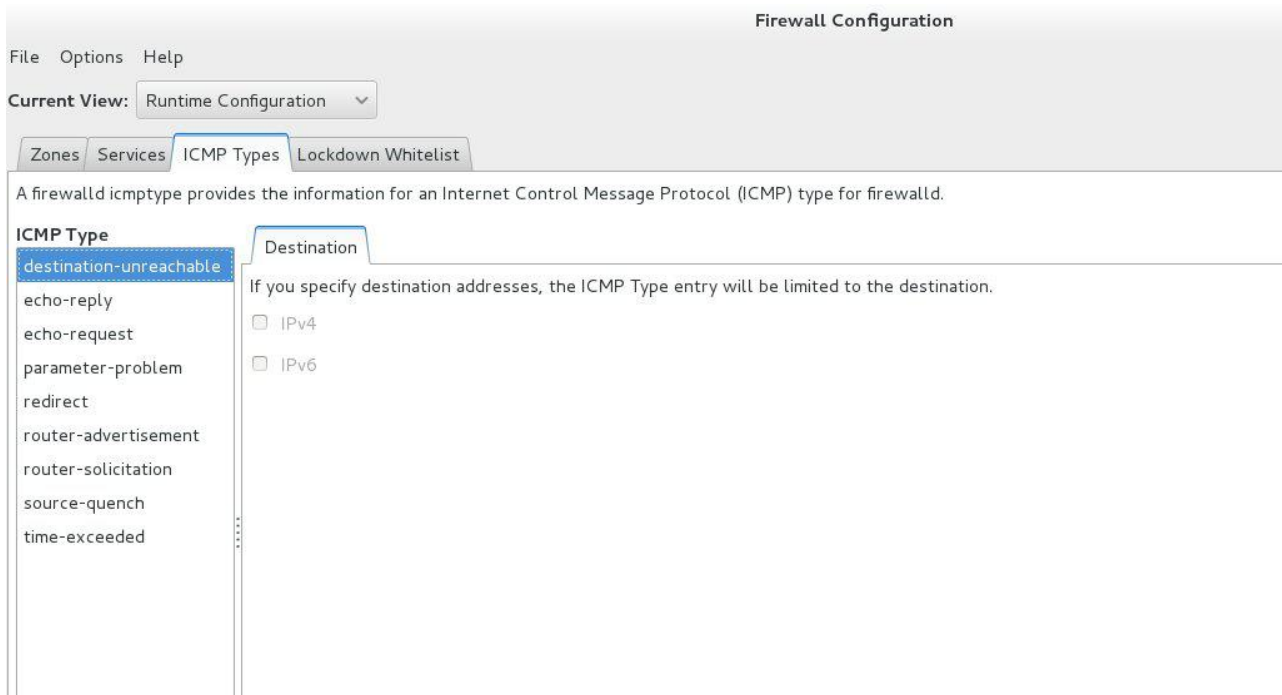
Puertos y protocolos

Definición de TCP o UDP, donde los puertos pueden ser un puerto único o un rango de puertos.



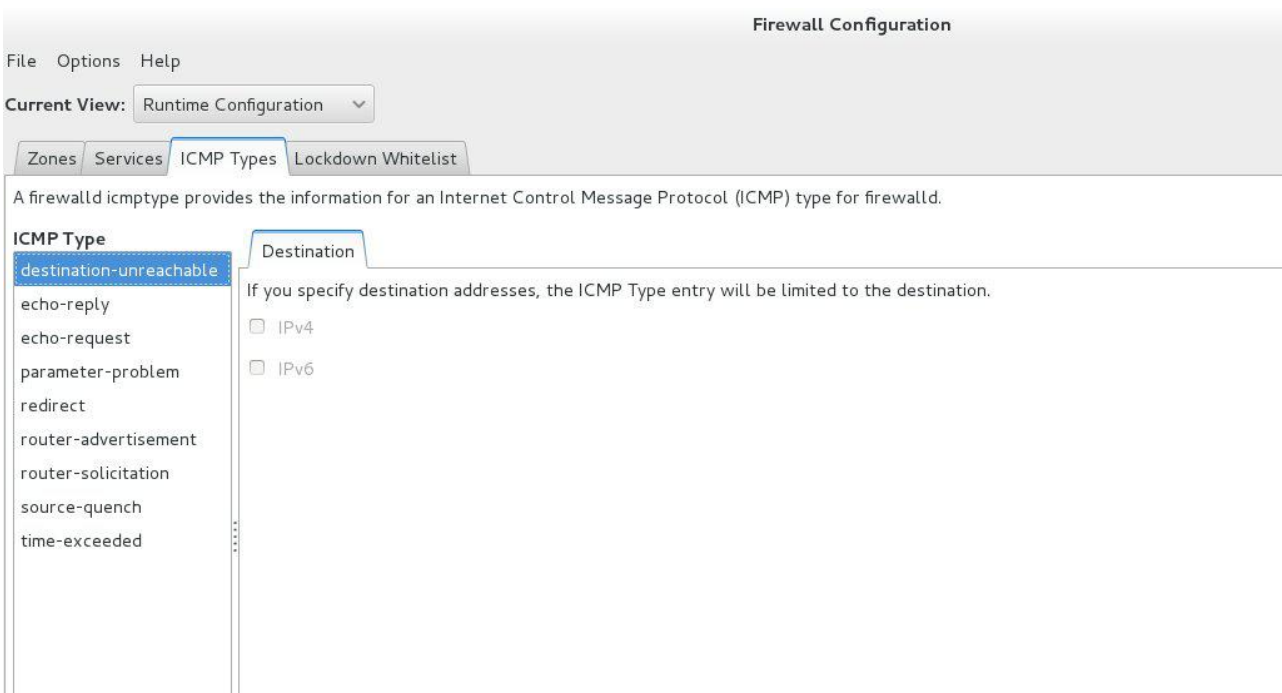
ICMP blocks

Selected Internet Control Message Protocol (ICMP) messages. Estos mensajes son solicitudes de información o son creados como respuesta a otras solicitudes o también respuestas para condiciones de error.



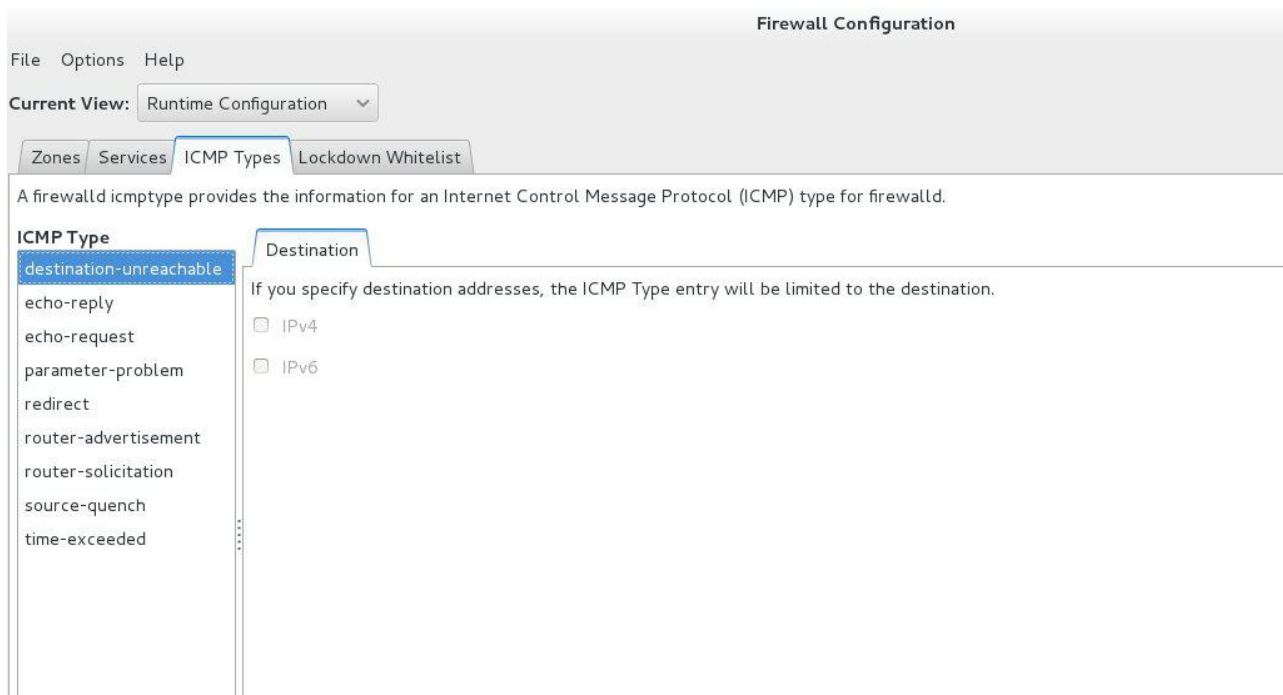
Masquerading (Enmascaramiento)

Las direcciones de la red privada son mapeadas detrás de una dirección IP pública. Ésta es una forma de traducción de direcciones.

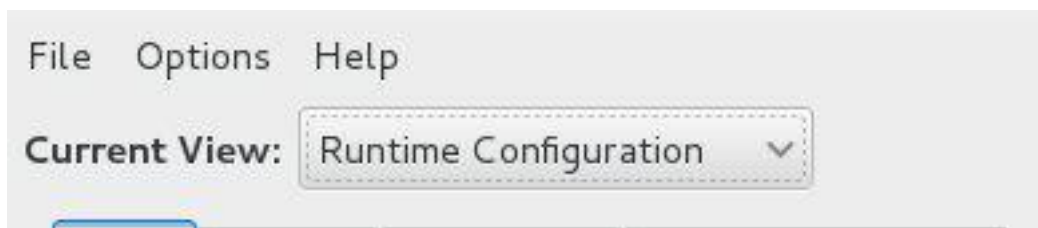


Forward ports

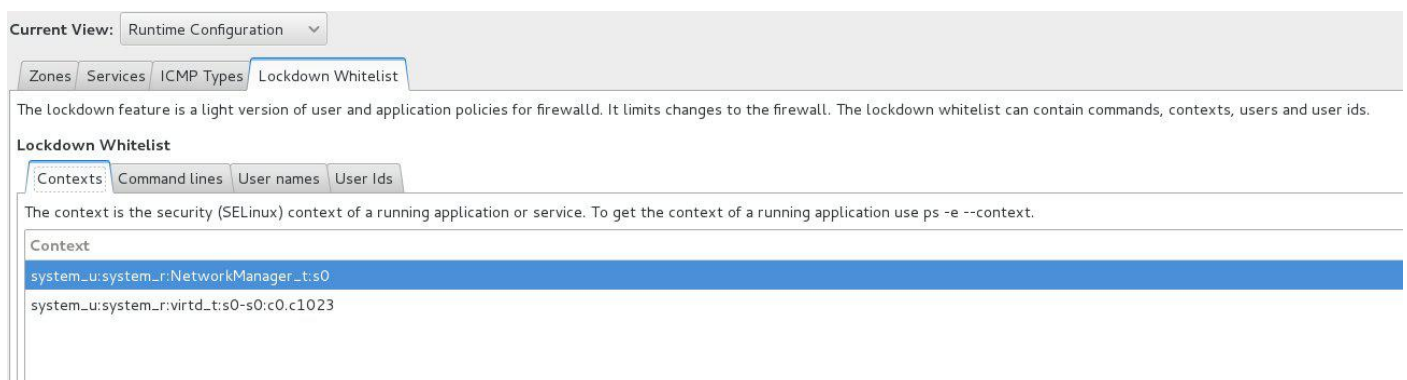
Un puerto está asignado a otro puerto y/o a otro host.



Podemos ver que se puede aplicar la configuración de una forma provisoria:



Podríamos cambiarlo a permanent para ver la configuración estable que es la persistente.



Un poco de seguridad aplicando diferentes políticas de usuarios.

¿Qué zonas se encuentran disponibles?

Estas son las zonas previstas por firewalld ordenados según el nivel de confianza predeterminado de las zonas desde no confianza a confianza:

drop (immutable)

Los paquetes de red entrantes se caen, no hay respuesta. Sólo las conexiones de red salientes son posibles.

block (immutable)

Las conexiones de red entrantes se rechazarán con un mensaje icmp-host—prohibited para IPv4 e icmp6-adm--prohibited para IPv6. Sólo las conexiones de red iniciadas dentro de este sistema son posibles.

public

Para el uso en las zonas públicas. Se basa en que no se confía en los otros equipos de la red para no dañar su equipo. Se aceptan conexiones entrantes sólo seleccionadas.

external

Para el uso en redes externas con enmascaramiento habilitado especialmente para los routers. Se basa en que no se confía en los otros equipos de la red para no dañar su equipo. Se aceptan conexiones entrantes sólo seleccionadas.

dmz

Para los equipos de la dmz que son de acceso público, con acceso limitado a la red interna. Se aceptan conexiones entrantes sólo seleccionadas.

work

Para su uso en áreas de trabajo. Se basa en que se confía en su mayoría en los otros equipos de la red. Se aceptan conexiones entrantes sólo seleccionados.

home

Para su uso en zonas de origen conocido. Usted confía en su mayoría en los otros equipos de la red. Se aceptan conexiones entrantes sólo seleccionadas.

internal

Para el uso en redes internas. Usted confía en su mayoría en los otros equipos de la red. Se aceptan conexiones entrantes sólo seleccionadas.

trusted (immutable)

Se aceptan todas las conexiones de red.

Ejemplo de como listar las zonas:

```
[root@localhost ~]# firewall-cmd --get-zones
work drop internal external trusted home dmz public block
[root@localhost ~]#
```

¿Qué zona se debe utilizar?

Una conexión de red Wi-Fi pública, por ejemplo, debe ser sobre todo de confianza, una conexión de red doméstica por cable debe ser bastante fiable. Seleccione la zona que mejor se adapte a la red que está utilizando. Para esto también es importante ir configurando nuestras zonas con las reglas que se adecuen mejor.

¿Cómo configurar o añadir zonas?

Para configurar o añadir zonas puede utilizar una de las interfaces firewalld (GUI, CLI). Se trata de las siguientes herramientas de configuración gráfica de firewall-config, la herramienta de línea de comandos firewall-cmd o la interfaz D-BUS. O bien, puede crear o copiar un archivo de la zona en uno de los directorios de configuración (/etc/firewalld/zones)

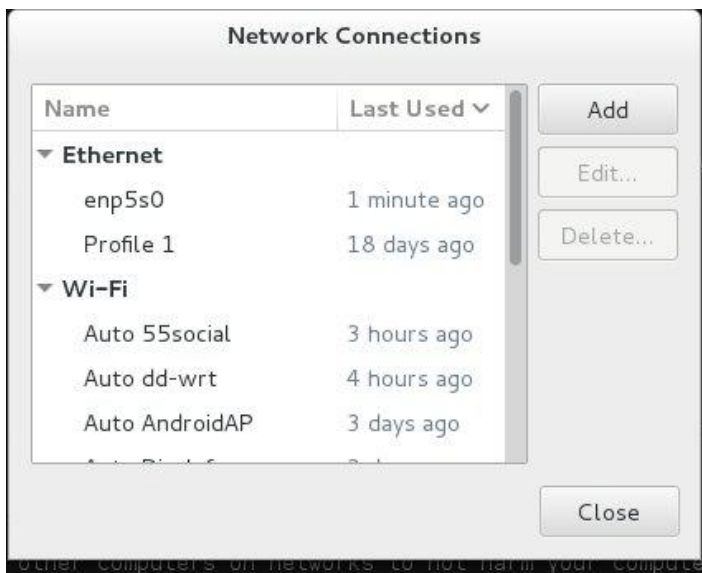
```
[root@localhost ~]# cat /etc/firewalld/zones/public.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Public</short>
  <description>For use in public areas. You do not trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.</description>
  <service name="mdns"/>
  <service name="dhcpv6-client"/>
  <service name="ssh"/>
  <port protocol="udp" port="5353"/>
  <port protocol="udp" port="1900"/>
  <port protocol="udp" port="5001"/>
  <port protocol="tcp" port="8200"/>
</zone>
[root@localhost ~]#
```

¿Cómo establecer o cambiar una zona de conexión?

La zona se almacena en el ifcfg de la conexión con la opción ZONE =. Si la opción se encuentra o está vacía, se utiliza el conjunto de la zona predeterminada en firewalld.

Si la conexión es controlada por NetworkManager, también puede utilizar nm-connection-editor para cambiar la zona.

```
[root@localhost network-scripts]# cat /etc/sysconfig/network-scripts/ifup-eth |grep -i ZONE
# Inform firewall which network zone (empty means default) this interface belongs to
/usr/bin/firewall-cmd --zone="${ZONE}" --change-interface="${DEVICE}" > /dev/null 2>&1
[root@localhost network-scripts]#
```



Las conexiones de red gestionadas por NetworkManager

El firewall no es capaz de manejar las conexiones de red con el nombre que aparece por NetworkManager, sólo puede manejar interfaces de red. Por lo tanto NetworkManager se comunica con firewalld para poner las interfaces de red relacionadas con las conexiones en las zonas definidas por el archivo de configuración (ifcfg) de la conexión



antes que la la conexión se establezca. Si la zona no se encuentra en el archivo de configuración, las interfaces se pondrán en el conjunto de la zona predeterminada de firewalld. Si la conexión tiene más de un interfaz, ambas serán suministradas a firewalld. También los cambios en los nombres de las interfaces se resolverán mediante NetworkManager y se suministran a firewalld.

Para simplificar se utilizarán esta conexión en relación con las zonas de ahora en adelante.

NetworkManager también se comunica con firewalld para eliminar las conexiones de las zonas si la conexión se cayó.

Si firewalld se inicia o reinicia por scripts systemd o init, firewalld notifica NetworkManager y las conexiones se añadirán a las zonas.

Ahora la parte divertida, la línea de comandos:

Instalación en Fedora

```
$ su - "yum install firewalld"
Desactive el antiguo servicio:
# systemctl disable iptables.service
# systemctl disable iptables6.service (ipv6 usualmente no habilitado)
Detenga los servicios antiguos iptables:
# systemctl stop iptables.service
# systemctl stop iptables6.service
Habilite el nuevo servicio.
# systemctl enable firewalld.service
Arranque firewalld:
# systemctl start firewalld
```

Algunos tips por ahora.

Arranque y parada con systemd

```
# systemctl start|stop|restart firewalld.service
# cat /lib/systemd/system/firewalld.service
[Unit]
Description=firewalld - dynamic firewall daemon
After=syslog.target
After=dbus.target
Before=network.target
Before=libvirtd.service
Before=NetworkManager.service
Conflicts=iptables.service ip6tables.service ebtables.service
```

```
[Service]
EnvironmentFile=-/etc/sysconfig/firewalld
ExecStart=/usr/sbin/firewalld --nofork $FIREWALLD_ARGS
ExecReload=/bin/kill -HUP $MAINPID
# supress to log debug and error output also to /var/log/messages
StandardOutput=null
StandardError=null
Type=dbus
BusName=org.fedoraproject.FirewallD1
```

[Install]

WantedBy=basic.target

Alias=dbus-org.fedoraproject.FirewallD1.service

Habilitando un servicio preconfigurado

```
# firewall-cmd --zone=public --add --service=nfs
```

Hacer esto no cambia la configuración persistente, sólo la configuración en ejecución.

Deshabilitando un servicio preconfigurado

```
# firewall-cmd --zone=public --remove --service ssh
```

Servicios disponibles

La instalación estándar de firewalld en Fedora incorpora una serie de servicios que se listan a continuación.

```
# ls -l /usr/lib/firewalld/services/
```

amanda-client.xml; bacula-client.xml; bacula.xml; cluster-suite.xml; dhcpv6-client.xml; dns.xml; ftp.xml; https.xml; http.xml; imaps.xml; ipp-client.xml; ipp.xml; ipsec.xml; libvirt-tls.xml; libvirt.xml; mdns.xml; nfs.xml; openvpn.xml; pop3s.xml; radius.xml; samba-client.xml; samba.xml; smtp.xml; ssh.xml; telnet.xml; tftp-client.xml; tftp.xml.

Agregar un nuevo servicio

Actualmente no hay una interfaz automática para hacerlo, pero no es tan difícil, es cosa de copiar y editar uno de estos archivos xml en /etc/firewalld/services.

```
# cp /usr/lib/firewalld/services/http.xml /etc/firewalld/services/hbci.xml
```

Para nombrar su servicio use como referencia /etc/services. Ahora toca editar el contenido hbci.xml.
/etc/firewalld/services/hbci.xml

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<service name="hbci">
```

```
  <short>HBCI - HomeBanking Computer Interface</short>
```

```
  <description>HBCI is a bank-independent online banking standard, developed by the German Central Banking Committee ZKA (Zentraler Kredit-Ausschuss). It is a publicly available specification that defines the communication between online banking applications and the credit institutes' servers. In Germany, roughly half of all banks offer online banking through HBCI, which are approximately 2000 banks. More and detailed information about HBCI can be found on our link page, and comments can be added on our LinuxWiki OpenHBCI Page (in German).</description>
```

```
  <port protocol="tcp" port="3000"/>
```

```
</service>
```

Debe recargar firewalld y poner en funcionamiento su nuevo servicio.

```
# systemctl restart firewalld.service
```

```
# firewall-cmd --zone=public --add --service=hbci
```

```
# iptables -L IN_ZONE_public_allow -n
```

Chain IN_ZONE_public_allow (1 references)

target	prot	opt	source	destination	
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:22 ctstate NEW
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:80 ctstate NEW
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:443 ctstate NEW
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:3000 ctstate NEW

```
<<< Nuevo servicio
```


Persistencia de los servicios

Una vez agregada el servicio a la configuración en ejecución es muy probable que desee hacer que dicha configuración resista un reinicio del sistema. Para lograrlo deberá modificar el archivo de zona correspondiente.

```
/lib/firewalld/zones/public.xml
<?xml version="1.0" encoding="utf-8"?>
<zone name="public">
  <short>Public</short>
  <description>For use in public areas. You do not trust the other computers on networks to
not harm your computer. Only selected incoming connections are accepted.</description>
  <service name="ssh"/>
  <service name="dhcpv6-client"/>
  <service name="http"/>
  <service name="https"/>
  <service name="hbc1"/>
</zone>
```

Más acerca del uso de zonas

Comenzando, incompleto

```
# firewall-cmd --get-default-zone
```

```
public
```

Varios ejemplos

Ver estado

```
# Más acerca del uso de zonas
```

Ver zona predeterminada

```
# firewall-cmd --get-default-zone
```

```
public
```

Ver zonas disponibles

```
# firewall-cmd --get-zones
```

```
work drop internal external trusted home dmz public block
```

Ver servicios disponibles

```
# firewall-cmd --get-services
```

```
cluster-suite kpasswd bacula-client smtp ipp radius mysql ms-wbt bacula transmission-client
ftp mdns samba pmproxy dhcpv6-client rpc-bind ldaps https ldap dhcp imaps samba-client vnc-
server http dns pmwebapi ntp kerberos telnet libvirt openvpn ssh pmwebapis pmcd ipsec
postgresql ipp-client proxy-dhcp amanda-client mounthd tftp-client dhcpv6 nfs tftp pop3s
libvirt-tls
```

Ver soporte ICMP

```
# firewall-cmd --get-icmptypes
```

```
redirect router-solicitation parameter-problem destination-unreachable echo-request echo-
reply source-quench time-exceeded router-advertisement
```

Ver las zonas en detalle

```
# firewall-cmd --list-all-zones
```

```
work
```

```
  interfaces:
```

```
  sources:
```

```
services: ipp-client mdns dhcpv6-client ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

drop

```
interfaces:
sources:
services:
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

internal

```
interfaces:
sources:
services: ipp-client mdns dhcpv6-client ssh samba-client
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

external

```
interfaces:
sources:
services: ssh
ports:
masquerade: yes
forward-ports:
icmp-blocks:
rich rules:
```

trusted

```
interfaces:
sources:
services:
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

home

```
interfaces:
sources:
services: ipp-client mdns dhcpv6-client ssh samba-client
```

```
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

dmz

```
interfaces:
sources:
services: ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

public (default, active)

```
interfaces: p1p1
sources:
services: mdns dhcpv6-client ssh
ports: 5353/udp 1024-2048/tcp
1900/udp 8200/tcp 5001/udp
masquerade: yes
forward-ports:
port=22:proto=tcp:toport=2233:t
oaddr=192.168.1.23
```

```
port=2345:proto=tcp:toport=2368
:toaddr=
icmp-blocks:
rich rules:
```

block

```
interfaces:
sources:
services:
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Ver zonas activas

```
# firewall-cmd --get-active-
zones
public
interfaces: p1p1
```

Algunas más que interpretando su sintaxis se comprende por sí sola.

```
# firewall-cmd --set-default-zone=<zone>
firewall-cmd --get-zone-of-interface=<interface>
firewall-cmd [--zone=<zone>] --add-interface=<interface>
firewall-cmd [--zone=<zone>] --change-interface=<interface>
firewall-cmd [--zone=<zone>] --remove-interface=<interface>
firewall-cmd [--zone=<zone>] --query-interface=<interface>
firewall-cmd [ --zone=<zone> ] --list-services
```

El viejo y querido modo te bloqueo todo

```
# firewall-cmd --enable-panic
firewall-cmd --disable-panic
firewall-cmd --query-panic
```

Habilitar un servicio en una zona por un tiempo

```
# firewall-cmd [--zone=<zone>] --add-service=<service> [--timeout=<seconds>]
```

Habilitar un cliente en una zona por un tiempo

```
# firewall-cmd --zone=home --add-service=ipp-client --timeout=60
```

Habilitar un servicio en la zona predeterminada

```
# firewall-cmd --add-service=http
```

Deshabilitar un servicio

```
# firewall-cmd [--zone=<zone>] --remove-service=<service>
```

Remover un servicio

```
# firewall-cmd --zone=home --remove-service=http
```

Consultar si un servicio esta en una zona

```
# firewall-cmd [--zone=<zone>] --query-service=<service>
```

Habilitar un protocolo/puerto en una zona

```
# firewall-cmd [--zone=<zone>] --add-port=<port>[-<port>]/<protocol> [--timeout=<seconds>]
```

Deshabilitarlo

```
# firewall-cmd [--zone=<zone>] --remove-port=<port>[-<port>]/<protocol>
```

Consultar si esta activo

```
# firewall-cmd [--zone=<zone>] --query-port=<port>[-<port>]/<protocol>
```

Habilitar masquerading

```
# firewall-cmd [--zone=<zone>] --add-masquerade
```

Deshabilitarlo

```
# firewall-cmd [--zone=<zone>] --remove-masquerade
```

Consultar

```
# firewall-cmd [--zone=<zone>] --query-masquerade
```


Habilitar port forwarding

```
# firewall-cmd [--zone=<zone>] --add-forward-port=port=<port>[-<port>]:proto=<protocol>
{ :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }
```

Deshabilitarlo

```
# firewall-cmd [--zone=<zone>] --remove-forward-port=port=<port>[-<port>]:proto=<protocol>
{ :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }
```

Consultar

```
# firewall-cmd [--zone=<zone>] --query-forward-port=port=<port>[-<port>]:proto=<protocol>
{ :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }
```

Para hacer los cambios permanentes:

Basta con hacer los mismos comandos de arriba pero con el flag `--permanent`, tener en cuenta que hay que hacer un reload o restart del servicio.

Para opciones más avanzadas les recomiendo mirar los links de referencia.



Rino Rondan
Fedora Ambassador
Fanático de Villa Dalmine

Links:

<https://fedoraproject.org/wiki/FirewallD>

<https://fedorahosted.org/firewalld/>

<https://fedoraproject.org/wiki/Features/firewalld-default>

<http://gomix.fedora-ve.org/projects/fedobetatest/wiki/Firewalld>

Zimbra™
Collaboration Suite
Linware
www.linware.com.ar
zimbra@linware.com.ar

En cualquier lugar, en cualquier máquina

Somos una empresa líder en soluciones OpenSource y contamos con más de 5 años de experiencia instalando servidores de colaboración Zimbra.

vmware®

Business Partner



zimbra@linware.com.ar

+54 (011) 60090219

+54 (351) 5891012

+56 (2) 5952714



Guerra fría tecno mundial

Por Claudio De Brasi

Se dice que en 1989 terminó la guerra fría entre EEUU y Rusia, OTAN vs, Bloque Soviético sería más acertado. Y es cierto hasta cierto punto.

Pero en realidad la guerra fría lo que hizo fue cambiar y mutar a otros estratos de la sociedad. Es llamativo que Internet apareciera al público justo después; originalmente como comunicación de los medios de defensa y posteriormente como comunicación de ideas científicas y académicas. Cuando se abrió el acceso al público en general, pronto se vio que la gente quería compartir casi todo. "Casi".

En el libro "Las Guerras del futuro" de Alvin Toffler, se dice que para que el pentágono supiera en tiempo real qué pasaba en la primera guerra del desierto, pasó por alto e ignoró cualquier regla, restricción de derechos de uso o patente. La consigna es clara, estar informado a cualquier costo.

Desde entonces las empresas de seguridad informática están en una "lucha" cuesta arriba contra las formas de filtración. Pero hay gente que desarrolla para espiar a quien sea y para quien quiera. Es llamativo que una empresa y gobiernos confíen en sistemas operativos de 2 empresas con base en EEUU. Particularmente si por omisión se deja habilitado el acceso remoto al equipo. Las redes sociales recaban demasiados datos de los usuarios y son el blanco de todo aquel que quiera recabar información de personas, empresas, corporaciones y organizaciones de gobierno.

Para colmo las empresas relacionadas con la tecnología con residencia en algunos países, están sujetas a las leyes de Inteligencia de esos países, (Leyes que no se dan a conocer al público en general), y que en muchos lugares se usan no sólo para la inteligencia de actividades extranjeras sino también de las internas. En varios países se observa y sigue a un grupo de ciudadanos por sus declaraciones en las redes sociales. Tanto Facebook por la cantidad verborragia como en Twitter por la inmediatez. WhatsApp pasa los mensajes por Canadá y EEUU, Line y ChatOn por sus respectivas sedes, etc. Todos pueden ser interceptados y si es necesario decodificados.

Por otra parte las empresas "privadas" que se dedican a espiar no discriminan de donde vienen los datos, los buscan y recolectan todos para cualquier cliente actual o futuro con métodos de los más diversos. AddWare, Spybots, Botnet, VPN públicas, servicios de almacenamiento de contenidos, etc. Hay muy pocos servicios realmente fiables, pero todos son susceptibles.

Ya no es la nueva guerra fría 2.0 en que las naciones del "Club Atómico" espiando a aquellas que intentan ingresar al mismo. Es algo mucho peor. Es una guerra fría de todos contra todos, donde no se sabe donde hay un lugar seguro o realmente neutral. Gobiernos, corporaciones, empresas, organizaciones y particulares. Todos contra todos. No importa qué nombre se le pongan a estas organizaciones de espionaje Echelon, Prismus, Proyecto X, etc, todos estamos afectados. Cualquier intento de mejorar la seguridad al público en general es perseguido. Por citar sólo un ejemplo, el de Phil Zimmermann, cuando PGP publicó el código fuente por eMail de EEUU a Europa, fue perseguido por más de 1 década.

El ojo ahora está sobre Kim Dotcom, y también sobre aquellos que decidieron difundir algunos temas de interés de las organizaciones de espionaje.

Una cosa notoria es lo poco que se han desarrollado la codificación comercial en los últimos 10 años. Prácticamente no hay avances. Para tener un ejemplo en cuenta: La segunda guerra mundial duró algo más de 6 años y se

desarrollaron más de 10 versiones de la máquina Enigma.

Hoy el avance es muchísimo más acelerado, pero muy estático en codificación. ¿Quién tiene interés en que siga tan quieto?. La respuesta es obvia, los que quieren seguir vigilando a todo el mundo.

Hoy día no se puede considerar seguro a ningún aparato que no se conozca todas sus funciones ya sea en Hardware como en Software, obviamente que el mismo se conecte a Internet. Y aún así no quita la posibilidad del espionaje remoto.

El mundo está sumido en una guerra fría tecno mundial. Y todos estamos en el campo de batalla ya sea como guerreros o como víctimas.

PD: En "El arte de guerra", el párrafo final dice que "La pieza más importante en la guerra son los espías", Más de 2000 años después, es más cierto que nunca.



Claudio De Brasi.
@Doldraug



GNUPANEL 2.0: El panel de control de hosting LIBRE y universal

GNUPanel es un panel de control de hosting desarrollado íntegramente en Argentina y publicado bajo licencia GPL. Originalmente nació para correr en servidores Debian y posteriormente también pudo instalarse sobre Ubuntu.

El proyecto se mantuvo activo con intermitencias desde su publicación y hacia fines de 2012 el equipo de desarrollo original comenzó a plantearse una reescritura completa del código para obtener una nueva versión del programa, incorporando mejoras de todo tipo.

Para reunir los recursos necesarios han optado por proponer un proyecto de financiación colectiva (crowdfunding) para ser lanzado en pocos días que permita completar el trabajo en un plazo de tres a cuatro meses.

¿Qué es GNUPanel 2.0?

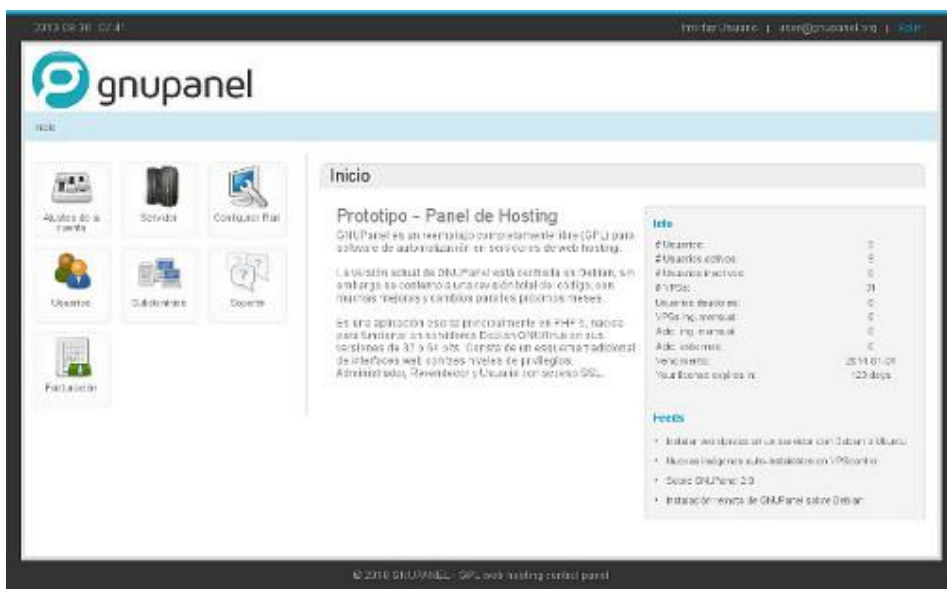
Es la reescritura total del código original de GNUPanel para obtener una versión superadora y muy flexible, apta para compartir en un repositorio y posibilitar el desarrollo de múltiples variantes.

La campaña de crowdfunding apunta a cumplir estos objetivos:

- Generar un paquete DEB de la aplicación para instalar mediante apt-get.
- Hacerlo adaptable a otras distribuciones muy populares (Ubuntu, CentOS, Fedora).
- Incluir soporte multiservidor y soporte IPv6.
- Dotarlo de una nueva interfaz gráfica editable
- Incluir un sistema de plugins para agregar funcionalidades.
- Asegurar que el código esté preparado para ajustarse a estándares GNU, con posibilidades de generalización para funcionar sobre otras distribuciones libres.

- Mejorar el sistema de tickets y módulos de pago integrados.

En resumen GNUPanel 2 se propone conformar una solución completa a las necesidades de web hosting sobre todo tipo de sistemas GNU/Linux para usuarios y empresas de todo el mundo.



Prototipo del nuevo aspecto para la versión 2.

La campaña de crowdfunding

En las campañas de Crowdfunding o financiación colectiva se propone un presupuesto y existen dos modalidades para tratar de alcanzar la meta: financiación flexible o fija.

En el primer caso los desarrolladores conservan los fondos acumulados aunque no lleguen a la meta.

Para este proyecto se optará por un esquema de financiación FIJA, un modelo también llamado “Todo o Nada”.

En el esquema “todo o nada” cada persona que decide co-financiar el proyecto sabe que el mismo se hará realidad dentro del plazo previsto porque si no se alcanza la meta, cada aporte es reembolsado en un 100% y la propia plataforma de Crowdfunding tampoco deduce su comisión.

Para ser co-financiador se pueden aportar distintas cantidades de dinero, desde 10 dólares hasta 500 o 1000. Lo más conveniente para todos es claramente la cooperación. Cientos o miles de usuarios aportando sumas de dinero muy pequeñas.

No es descabellado si se piensa en la cantidad de usuarios y pequeñas empresas que invierten cada mes entre 20 y 50 dólares en programas muy populares como CPanel, WHMCS, Clientexec, ClickDesk, Hyperspin y tantísimos otros.

Hay al menos 3 maneras de participar:

- Con una contribución económica acorde a tus posibilidades.
- Replicando la noticia por cuantos medios tengas a tu alcance.
- Visitando a diario el enlace del proyecto para aumentar su relevancia.

Aquellos que no pueden contribuir económicamente ayudarán mucho mencionando en foros o redes sociales el proyecto. O visitando a diario el enlace de la campaña.

Cuanta más actividad registre el proyecto mejor expuesto al público estará.

El proyecto estará en línea durante la primera semana de octubre y se puede obtener más información en el blog personal de Ricardo M. Alvarez, autor original de GNUPanel: <http://wp.geeklab.com.ar>.

[1] Ver <http://wp.geeklab.com.ar/gl/gnupanel/historia-breve/>

¿Por qué un código totalmente nuevo?

Durante el año 2007 hubo contactos con Richard Stallman para que GNUPanel fuera un verdadero paquete GNU, algo que lamentablemente no pudo llegar a gestarse [1].

El código originario (scripts, funciones, etc) contenía nombres y palabras en español por doquier. Esto dificultó la interacción con gente de la Free Software Foundation para su evaluación y adaptación a los estándares GNU.

La versión 2 del programa viene a cubrir este déficit y mucho más para liberar el potencial de este programa.



Redes para las masas

Parte VI

Por Hernan Saltiel

En las entregas anteriores hemos aprendido bastante sobre redes. Ya es hora de soltar la mano de la palabra “iniciados”, y volvernos “intermedios” o “avanzados”.

En este artículo armaremos un pequeño firewall, si bien no nos adentraremos demasiado en sus conceptos profundos (en un artículo anterior de esta misma revista expliqué cómo usar Shorewall y sus bondades), y jugaremos denegando y permitiendo puertos. Allá vamos, viajemos juntos por esta red llena de paquetes listos para ser descubiertos.

La virtualización que tanto nos gusta

En las entregas anteriores creamos máquinas virtuales y las interconectamos por medio de una red virtual interna para ver cómo ambas se comunican, y llegan a Internet. Hoy las usaremos para armar nuestro firewall y permitir o no la salida de determinados protocolos a la red de redes.

Entonces, antes que nada, encenderemos nuestra máquina virtual “firewall” (recordemos que la misma se encuentra creada en VirtualBox), que posee dos tarjetas de red: una con conexión a Internet a través de NAT, y la otra con acceso a la red interna que se conecta con el servidor virtual “centos1”.

Actualizaremos nuestra lista de paquetes, e instalaremos “shorewall”, siempre con la bella personalidad del usuario “root”:

```
# apt-get update && apt-get install shorewall
```

Ya instalado el paquete shorewall, encenderemos también nuestra máquina virtual “centos1”.

Ingresaremos a nuestro firewall, e intentaremos llegar a internet, por ejemplo, por medio de un “ping” a una dirección IP conocida, como es la 8.8.8.8 (uno de los servidores DNS de Google):

```
hecsa@firewall:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=63 time=161 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=63 time=160 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=63 time=161 ms
```



Efectivamente, llegamos sin problemas. Pero ¿qué nos ocurre cuando queremos llegar desde nuestro sistema “centos1”, que está conectado a una de las dos interfaces que posee el sistema “firewall”? Como imaginamos, no llegamos a ningún lugar. Nuestros paquetitos de red se han encontrado con la dura realidad que es el paredón que hemos puesto delante de ellos.

El motivo es sencillo. Si bien hemos instalado un paquete de software como lo es shorewall, aún no hemos configurado nada que permita que los paquetes de red pasen a través de él, ni que los enmascare. Si hay dudas sobre estos conceptos, releen los anteriores números de esta serie de redes. Si aún así siguen con dudas,

contáctenme. Claro está, háganlo sólo si vuestros paquetes de red pueden llegar al servidor de correo de vuestra preferencia.

Una paquetería

Entonces vamos a configurar shorewall para que permita todo lo que necesitamos, y se ejecute en el momento del inicio del servidor. Recordemos que todas estas configuraciones se harán con el usuario “root”, o con el comando “sudo”, y siempre con un editor de textos conocido, como puede ser “vi” o “emacs”. No descarto los editores gráficos, si bien está demostrado científicamente que el usar terminales en lugar de ventanas aumenta entre un 35,2 y un 43,7% las posibilidades de conseguir una pareja geek.

El primer archivo a tocar será /etc/shorewall/shorewall.conf, donde configuraremos por un lado IP Forwarding modificando la siguiente entrada:

```
IP_FORWARDING=Keep
```

...por:

```
IP_FORWARDING=Yes
```

Luego definiremos sus interfaces (como tenemos dos interfaces en el firewall, y el firewall en sí mismo, tendremos que asociarlas a las tres a lo que luego serán sus zonas, casi como si fueran sus nombres dentro del sistema) editando el archivo /etc/shorewall/interfaces, y dejando las siguientes entradas, considerando que eth0 está conectado a la WAN y eth1 a la LAN:

```
wan    eth0
lan    eth1
```

Configuraremos sus zonas para que se sepa que todas ellas corresponden a interfaces que utilizarán el protocolo IPv4. Para ello, tocaremos el archivo /etc/shorewall/zones, para que quede así:

```
fw      firewall
wan     ipv4
lan     ipv4
```

Ahora bien, haremos que todas las direcciones IP de la red secundaria del firewall (la red 10.200.200.0/24) puedan acceder a Internet enmascaradas. Para ello, tendremos que tocar el archivo /etc/shorewall/masq para que quede así:

```
eth0:0.0.0.0/0 10.200.200.0/0
```

Ahora, le avisaremos al paquete shorewall que ya se ha configurado, y que está listo para ser lanzado. Para ello, editaremos el archivo /etc/default/shorewall, cambiando la línea:

```
startup=0
```

...por:

```
startup=1
```

Ya con esto definido, llega el sagrado momento de relanzar el servicio que nos provee el paquete shorewall. Para

ello ejecutaremos:

```
# service shorewall restart
```

Veremos que aún podemos, desde el firewall, ejecutar el mismo “ping” de antes, con el mismo efecto:

```
hecsa@firewall:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=63 time=161 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=63 time=160 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=63 time=161 ms
```

La novedad es que desde ahora, podremos ejecutar también el mismo comando desde el servidor “centos1”, y llegar a destino. ¿Cómo es que logramos tal magia? Sencillo, ahora tenemos entre internet y centos1 un bloque que reenvía los paquetes de red, y los enmascara por nosotros.



Esto, que parece tan sencillo, nos permitirá, por ejemplo, poner detrás de una única conexión a internet una cantidad de máquinas tan grande como TCP/IP nos permita, utilizando direcciones internas, y permitiendo a todas tener salida a Internet. La familia internauta nunca estuvo tan feliz como en este día.

Ahora bien, ocurrirá que no deseamos que las máquinas utilicen cualquier protocolo, ya que puede que algún “abusador del ancho de banda” decida oprimir el botón “download” de varias páginas de internet en forma intempestiva. Para ello, comenzaremos permitiendo sólo el uso de DNS.

Ya lo sé, eso no nos servirá para mucho, ya que con sólo poder resolver un nombre no llegaremos muy lejos. Pero vamos por partes.

Lo primero que haremos es denegar todo tipo de comunicación tanto desde la zona “lan” como desde la “wan”, pero permitir cualquier tipo de comunicación desde la zona del mismo firewall.

Hay que tener especial cuidado cuando se hacen estas modificaciones en el mundo real, ya que si nuestra única conexión con el firewall es una terminal, y un SSH, por ejemplo, y cerramos todo tipo de comunicación, dejaremos dentro del grupo restringido al puerto 22 desde la WAN, ergo quedándonos afuera de nuestro propio sistema, y debiendo comprar boletos de autobús en el mejor de los casos para poder recuperarlo. Eso y un gasto inusual en psicólogos porque la pareja geek antes obtenida se marchará, sin remedio.

Para lograr nuestra política general, editaremos el archivo /etc/shorewall/policy, dejándolo de esta forma, notando que en todos los casos estamos solicitando que se guarde información de la acción que se tomó, y que ella se depositará en el archivo /var/log/kern.log:

```
fw      all    ACCEPT    info
wan     all    DROP      info
lan     all    DROP      info
```

Si relanzamos el servicio de shorewall como lo hemos hecho antes, e intentamos nuevamente ejecutar un “ping” desde nuestro servidor “centos1” hacia la dirección 8.8.8.8, veremos un mensaje interesante en el archivo /var/log/kern.log, que es donde estaremos logueando los eventos de shorewall a medida que se presenten (¿vieron esos campos del archivo /etc/shorewall/policy que decían “info”? Adivinen para qué sirven):

```
Oct  6 21:16:41 firewall kernel: [ 1051.159035] Shorewall:lan2wan:DROP:IN=eth1 O
UT=eth0 MAC=08:00:27:20:21:ba:08:00:27:62:96:80:08:00 SRC=10.200.200.2 DST=8.8.8
.8 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=22020 SE Q=111
```

```
Oct  6 21:16:42 firewall kernel: [ 1052.159677] Shorewall:lan2wan:DROP:IN=eth1 O
UT=eth0 MAC=08:00:27:20:21:ba:08:00:27:62:96:80:08:00 SRC=10.200.200.2 DST=8.8.8
.8 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=22020 SE Q=112
```

Estos mensajes nos están diciendo que ha habido un intento de parte de un paquete de ingresar por la interfaz eth1 y salir por la eth0, que el origen del paquete (SRC) es la dirección IP 10.200.200.2, que su destino (DST) es la dirección 8.8.8.8, y que usando una política entre la zona “lan” y la “wan”, se ha decidido descartarlo (DROP). El protocolo usado fue icmp (PROTO=ICMP).

Ahora, y para permitir el uso del puerto 53, normalmente de DNS, y en formato udp (¿necesitaríamos una orientación a la sesión para hacer una búsqueda en un servidor DNS? El primero que me mande la respuesta completa por mail se ganará una hermosa licuadora de mano), para lo cual amén de haber generado un archivo de políticas, generaremos uno de reglas particulares, el /etc/shorewall/rules, con el siguiente contenido, donde también hemos agregado el ping como aceptado:

```
ACCEPT      lan    wan    udp    53    -    -    # dns queries
ACCEPT      lan    wan    icmp   8     -    -    # ping
```

Luego de estas modificaciones, relanzaremos nuestro sistema shorewall, ejecutando nuevamente:

```
# service shorewall restart
```

Probemos ahora un ping a una dirección DNS, y veremos con gran alegría que nuestro sistema está funcionando como es debido. Analicemos nuevamente el mismo archivo /var/log/kern.log, y notemos la forma en la que los mensajes han cambiado:

```
Oct  6 21:18:51 firewall kernel: [ 941.022714] Shorewall:lan2wan:DROP:IN=eth1 O
UT=eth0 MAC=08:00:27:20:21:ba:08:00:27:62:96:80:08:00 SRC=10.200.200.2 DST=8.8.8
.8 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=22020 SE Q=1
Oct  6 21:18:52 firewall kernel: [ 942.025202] Shorewall:lan2wan:DROP:IN=eth1 O
UT=eth0 MAC=08:00:27:20:21:ba:08:00:27:62:96:80:08:00 SRC=10.200.200.2 DST=8.8.8
.8 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=22020 SE Q=2
```

Ahora bien, ¿qué pasa si intentamos ejecutar un comando de actualización en nuestro sistema “centos1”? Fallará miserablemente, porque no tenemos habilitado el puerto 80 y 443, ambos comúnmente utilizados para las comunicaciones via web. También lo podemos ver en el archivo /var/log/kern.log.

Nuevamente tocaremos nuestro archivo /etc/shorewall/rules, agregando las siguientes entradas:

```
ACCEPT      lan   wan   tcp   80    -    -    # Puerto 80 - Web
ACCEPT      lan   wan   tcp   443   -    -    # Puerto 443 - Web
```

Y como siempre, relanzaremos los servicios de shorewall como lo hemos hecho en el pasado.

Podremos ahora lanzar, en nuestro sistema “centos1”, comandos como ser “yum update”, notando con grata sonrisa que puede contactar sus servidores de actualizaciones con éxito.

Una luz al final del túnel

Intentemos salir al mundo desde nuestro servidor “centos1” mediante el uso de ssh. Claro está, primero tendremos que instalar en dicho equipo los clientes de ssh, ejecutando para ello:

```
# yum install openssh-clients
```

Una vez instalados, ejecutemos:

```
# ssh -l root 10.200.200.1
```

Efectivamente, el fracaso se ha logrado con éxito. No entramos ni en chiste a nuestro firewall, lo que nos deja tranquilos al saber que es seguro, e intranquilos al saber que no podemos ingresar. Veremos bonitos mensajes que nos avisan que nuestros paquetes han sido descartados en el archivo /var/log/kern.log. No los intepretaré, porque calculo que luego de la lectura anterior, usada para los paquetes icmp, ya ustedes mismos estarán en condiciones de hacerlo:

```
Oct  6 22:11:47 firewall kernel: [ 4356.516950] Shorewall:lan2wan:DROP:IN=eth1 O
UT=eth0 MAC=08:00:27:20:21:ba:08:00:27:62:96:80:08:00 SRC=10.200.200.2 DST=10.20
0.200.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=21130 DF PROTO=TCP SPT=38060 DPT=22 WINDOW=5840
RES=0x00 SYN URGP=0
```

```
Oct  6 22:11:51 firewall kernel: [ 4360.308174] Shorewall:lan2wan:DROP:IN=eth1 O
UT=eth0 MAC=08:00:27:20:21:ba:08:00:27:62:96:80:08:00 SRC=10.200.200.2 DST=10.20
0.200.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=11057 DF PROTO=TCP SPT=44297 DPT=22 WINDOW=5840
RES=0x00 SYN URGP=0
```

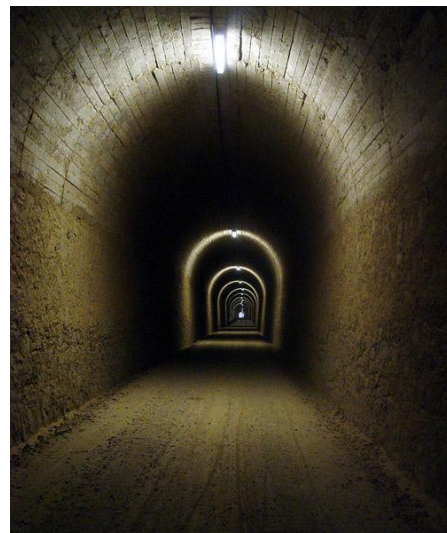
Agreguemos entonces una línea en nuestro archivo /etc/shorewall/rules, como la siguiente:

```
ACCEPT      lan   fw    tcp   22    -    -    # SSH al firewall1
```

Relancemos como de costumbre.

Esta línea nos estará diciendo que las conexiones al servidor SSH de nuestro firewall se podrán efectuar. ¿Pero de qué nos sirve eso, si no podemos llegar al mundo? De mucho, ahora veremos.

Una capacidad que tenemos con el subsistema de SSH es la de armar túneles, y por medio de ellos utilizar la capacidad de conectividad del sistema al que nos estamos conectando. Por ende, si nuestro firewall puede contactarse con el mundo en forma irrestricta, también podremos nosotros hacer lo mismo si sabemos cómo.



Para ello, el cliente SSH posee un argumento que puede especificarse de la siguiente forma: “-L puerto_local:dirección_IP_remota:puerto_remoto”.

Por ejemplo, si quisiéramos llegar mediante SSH a un sistema que tiene la dirección 10.100.100.2, claramente fuera de nuestra red, al cual no accedemos, pero al que sí puede acceder el firewall, podríamos configurar un puerto local en el “centos1” que sea suficientemente alto como para no romper nada en él, pero que nos permita lograr dicha conectividad. Supongamos el puerto 10022, que será redirigido al puerto 22 de la dirección IP 10.100.100.2. Si cometiéramos la locura de utilizar un puerto que localmente sirve para algo más, estaremos generando un conflicto, y como siempre en estos casos, hasta que alguien no se baje del caballo, la negociación no terminará.

Ejecutamos el siguiente comando, en el servidor “centos1”:

```
[root@centos1 ~]# ssh -l root -L 10022:10.100.100.2:22 10.200.200.1
The authenticity of host '10.200.200.1 (10.200.200.1)' can't be established.
RSA key fingerprint is 00:e0:43:b7:12:08:41:4b:8c:db:9b:d6:93:c7:8a:47.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.200.200.1' (RSA) to the list of known hosts.
root@10.200.200.1's password:
Linux firewall 3.2.0-4-486 #1 Debian 3.2.46-1 i686
...
```

En él estamos expresando que ingresaremos al sistema “firewall” (dirección IP 10.200.200.1) con el usuario root, y que luego haremos que cada vez que se invoque al puerto local 10022 del sistema “centos1”, se redirijan los paquetes de red al puerto 22 de la dirección IP 10.100.100.2. Ya sé, no parece sencillo, pero créanme que les va a solucionar los problemas muchas veces.

Ahora, ejecutaremos un pedido de conexión SSH local, al puerto 10022:

```
[root@centos1 ~]# ssh -l hecsa -p 10022 localhost
hecsa@localhost's password:
Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-31-generic i686)
 * Documentation:  https://help.ubuntu.com/
...
```

Nos encontramos, entonces, en el servidor de destino, al cual no podríamos haber llegado si hubiéramos intentado una conexión directa.

Esta técnica de armar túneles mediante el uso de SSH es muy usada cuando se desea levantar un ambiente “X” y sólo se posee una conexión SSH a un servidor que lo puede acceder, o cuando necesitamos una conexión VNC, por ejemplo. Les recomiendo profundamente que la prueben en todos los casos que deseen, y vean lo bien que funciona.

Cuando quieran armar un túnel para el protocolo “X”, específicamente, les comento que se puede utilizar el siguiente comando que resultará más sencillo de ejecutar:

```
# ssh -X -l <usuario> <dirección_IP>
```

Una vez dentro del equipo, verán que pueden ejecutar comandos que les mostrarán ventanas en sus máquinas locales como si realmente se estuvieran ejecutando en ellas. Casi magia, diría una amiga mía.

Epílogo

En esta serie de artículos hemos jugado y aprendido mucho sobre los elementos que todo buen sysadmin debe tener en su cabeza a la hora de configurar y diagnosticar problemas de redes. De aquí en más, la experiencia personal de cada uno definirá el camino que tomará según sus ganas de investigar.

Les recomiendo que ya que han configurado sus máquinas virtuales jueguen mucho con ellas aceptando y denegando puertos, abriendo programas como el “nmap” y verificando qué vulnerabilidades poseen en sus redes, armando servidores y ubicándolos en diferentes DMZs, y un largo e interminable etcétera que les dejo para que piensen.

Muchas gracias por habernos acompañado en este breve pero espero que útil cursillo de redes.

¡Hasta la próxima!



Hernán “HeCSa” Saltiel
AOSUG Leader
CaFeLUG Member
Twitter: @hcsaltiel
hsaltiel@gmail.com

<http://www.facebook.com/hcsaltiel>

<http://www.aosug.com.ar>



TUX **INFO**
WWW.TUXINFO.COM.AR