

**MARAVENTO STUDIO**

**GATEPROXY**

## Licence

### GPL-3.0

This Project is educational purposes. Este proyecto es con fines educativos. Agradecemos a todos aquellos que han contribuido a este proyecto. We thank all those who contributed to this project. Special thanks to novatoz.com

## Disclaimer

Este script puede dañar su sistema si se usa incorrectamente. Úselo bajo su propio riesgo. This script can damage your system if used incorrectly. Use it at your own risk. HowTO Gateproxy

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.



© 2016 [gateproxy.com](http://gateproxy.com) por [maravento](http://maravento) se distribuye bajo una [Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/). Basada en una obra en [maravento](http://maravento). Permisos que vayan más allá de lo cubierto por esta licencia pueden encontrarse en [maravento](http://maravento).

## GATEPROXY SETUP

v1.0 Alpha  
[gateproxy.com](http://gateproxy.com)



### **QUÉ ES GATEPROXY / WHAT IS GATEPROXY**

Es un servidor, orientado a la administración de redes LAN, lo más intuitivo y desatendido Gateproxy es un servidor para administrar pequeñas y medianas redes LAN, lo más intuitivo y desatendido posible, apto para el manejo del usuario, sin importar si tiene o no un alto grado de conocimientos en GNU/Linux, generando así una mejor experiencia.

El script de instalación y configuración es totalmente automatizado y personalizable, de acuerdo a las necesidades del administrador u organización, con una interacción mínima durante proceso, reduciendo así la curva de aprendizaje. Puede ser implementado tanto en un servidor "físico", como en una VM, para mayor flexibilidad y portabilidad.



Gateproxy is a server for managing home & business LANs, and inattentive as intuitive as possible, suitable for handling user, regardless of whether it has a high degree of knowledge in GNU/Linux, thus creating a better experience.

The installation and configuration script is fully automated and customizable according to the needs of the administrator or organization, with minimal interaction during the process, thus reducing the learning curve. It can be implemented in either a "physical" server, such as in a VM, for greater flexibility and portability.

### **QUÉ NO ES GATEPROXY/ WHAT IS NOT GATEPROXY**

Un nodo o proxy, similar a Tor, Ultrasurf, Psiphon, etc.

A node or proxy, similar to Tor, Ultrasurf, Psiphon, etc.

## Requisitos Mínimos/Minimum requirements

GNU/Linux: [Ubuntu 16.04.x \(Xenial Xerus\) LTS x64](#)  
 Processor: Intel compatible 1x GHz  
 Interfaces: eth0, eth1  
 RAM: 4GB  
 DD: 200 GB  
 Internet: High speed (recommended)  
 Bash: 4.3x (check with echo \$BASH\_VERSION)  
 Desktop: Mate (Optional) [HowTo install Ubuntu/Debian with Mate Desktop](#)  
 Language: eng-spa

## IMPORTANT

Haga copia de seguridad de sus archivos esenciales y [cifrar el disco duro](#)

Back up your essential files and encrypt your hard drive

Actualice su sistema periódicamente y desinstale las app no esenciales (ejemplo: rhythmbox cheese vlc shotwell\* btrfs-tools sendmail libreoffice\*, etc)

Update your system and uninstall nonessential app esenciales (ejemplo: rhythmbox cheese vlc shotwell\* btrfs-tools sendmail libreoffice\*, etc)

Fortifique su política de seguridad: Verificar los permisos globales (find / -path /proc -prune -o -perm -2 ! -type l -ls) los archivos sin propietarios (find / -path /proc -prune -o -nouser -o -nogroup) y los que no tienen passwords (grep -v ':x:' /etc/passwd). Adicionalmente se recomienda fortificar su política de contraseñas y acceso, bien sea modificando los archivos de configuración relacionados o utilizando soluciones como [Syspass](#), entre otras. Por ejemplo, cambie su contraseña cada 30 días o menos, con un tiempo de gracia después de caducada de 5 días antes del bloqueo; no reutilice contraseñas; aumente su complejidad; admita un número máximo de intentos de acceso (3), ponga una contraseña en el arranque y grub; garantice la confidencialidad de los datos; el acceso concurrente; permita sólo credenciales certificadas y cualquier otra medida que considere necesaria para garantizar la seguridad de su servidor (Gateproxy incluye el paquete libpam-cracklib ([HowTo](#)))

Fortify your security policy: Check global permissions (find / -path /proc -prune -o -perm -2 ! -type l -ls) Unowned files (find / -path /proc, or -nouser -prune -o -nogroup) and those without passwords (grep -v ':x' /etc/passwd). Additionally we recommended fortifying your password policy and access, either by modifying the configuration files related or using solutions such as Syspass, among others. For example, change your password every 30 days or less, with a time of grace expired after 5 days before the blockade; do not reuse passwords; increase its complexity; support a maximum number of access attempts (3), put a password on boot and grub; ensure the confidentiality of data; concurrent access; allow only certified credentials and any other action deemed necessary to ensure the security of your server (Gateproxy includes package libpam-cracklib ([HowTo](#)))

Si su servidor va a estar expuesto a Internet, recomendamos protegerlo con soluciones de defensa perimetral, tales como IPS/IDS ([Snort con Snorby](#), [Barnyard2](#) o los script de instalación [Autosnort](#), [Maltrail](#), o lea el tutorial de instalación [AQUI](#)) (Gateproxy incluye un módulo experimental de IPS/IDS); [ArpON](#); instalar policycoreutils y verificar estado de selinux para activarlo (comandos sestatus, getenforce o system-config-selinux y setenforce enforcing o editar /etc/selinux/config) y verificar su compatibilidad con su servidor; comprobar los puertos abiertos innecesarios y cerrarlos (netstat -puerto); cambiar el puerto 22 ssh y otros puertos esenciales hacia puertos diferentes utilizando [portknocking](#); deshabilitar el inicio de sesión root; deshabilitar ipv6 si no se va a utilizar; cambiar la secuencia CTRL+ALT+SUPR (etc/inittab) o deshabilitarla; hacer copia de seguridad de su arranque con boot-repair u otra solución; auditar regularmente su servidor y red local con [lynis](#), [Sparta](#), o cualquier otra herramienta de su manejo, protegerse de los ataques de amplificación DNS con [dns-iptables-rules](#) y de los ataques DDoS con [Bohatei](#) y [ViewDDOS](#) derivar el tráfico por una [VPN segura](#) (OpenVPN/OpenSSL). Para la VPN puede utilizar el script de [Rosehosting Github](#) (lea los tutoriales de [DigitalOcean](#) y [rosehosting](#)), (Gateproxy incluye los paquetes OpenVPN y Open SSL) o cualquier otra medida que considere para prevenir intrusiones y mantener su sistema protegido

If your server will be exposed to the Internet, we recommend protecting with solutions perimeter such defense

as IPS / IDS (Snort with Snorby, Barnyard2 or installation script Autosnort, Maltrail, or read the installation tutorial [HERE](#)) (Gateproxy includes a experimental module IPS / IDS); Harpoon; polycycoreutils install and verify selinux status to activate (sestatus commands, getenforce or system-config-selinux and setenforce enforcing or edit / etc / selinux / config) and verify its compatibility with your server; check unnecessary ports open and closed (netstat-port); change the ssh port 22 and other essential ports to different ports using portknocking; disable root login; disable ipv6 if it will not be used; change the sequence CTRL + ALT + DEL (etc / inittab) or disable it; to back up your boot boot-repair or other solution; audited regularly your server and local network with Lynis, Sparta, or any other tool handling, protect from attacks by DNS amplification dnsmity and DDoS attacks with Bohatei and ViewDDOS derive traffic over a secure VPN ( OpenVPN / OpenSSL). For VPN you can use the script Rosehosting Github (read tutorials and rosehosting digitalocean.) (Gateproxy includes OpenVPN and OpenSSL packages) or any other measures deemed to prevent intrusions and keep your system protected

Es recomendable realizar una instalación desde 0 (en un sistema limpio), sin embargo el script de instalación de Gateproxy puede ser usado en servidores con configuraciones previas. Como medida de seguridad, el script hace backup de cada archivo de sistema a reemplazar. Si al terminar la instalación de GateProxy no obtiene los resultados esperados, o su servidor presenta fallas, puede restablecer la copia de seguridad del archivo afectado en la misma ruta donde se encuentra, con el formato bak

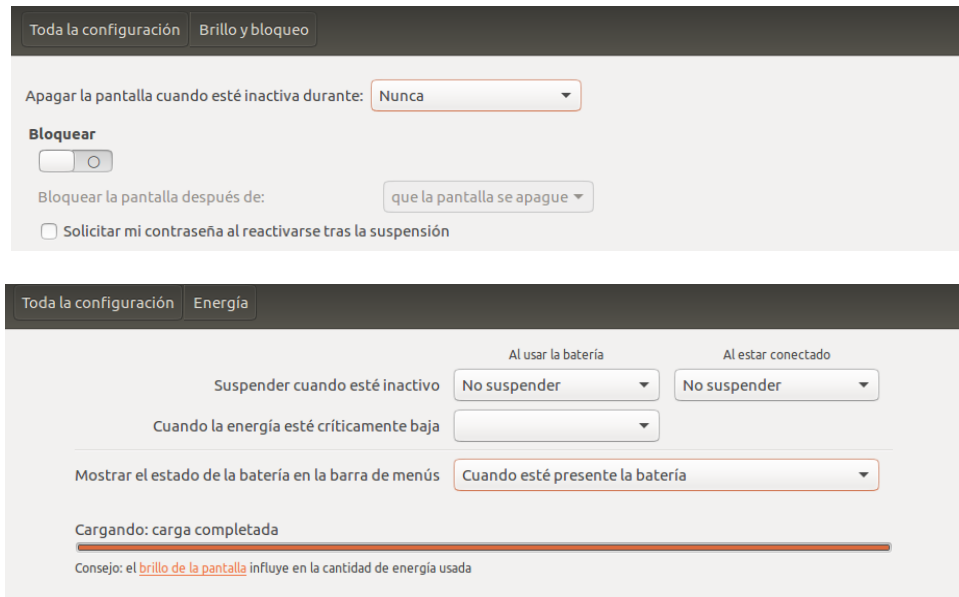
It is advisable to install from 0 (on a clean system), however the installation script Gateproxy can be used on servers with previous settings. As a safety precaution, the script makes backup of each file system to replace. If you finish installing GateProxy not get the expected results, or server should fail, you can restore the backup file affected in the same path where it is, with the format bak

En el presente tutorial hemos utilizado algunos nombres y contraseñas de ejemplo. Por razones de seguridad no deben ser utilizados en su servidor de producción

In this tutorial we used some names and passwords for example. For security reasons they should not be used in your production server

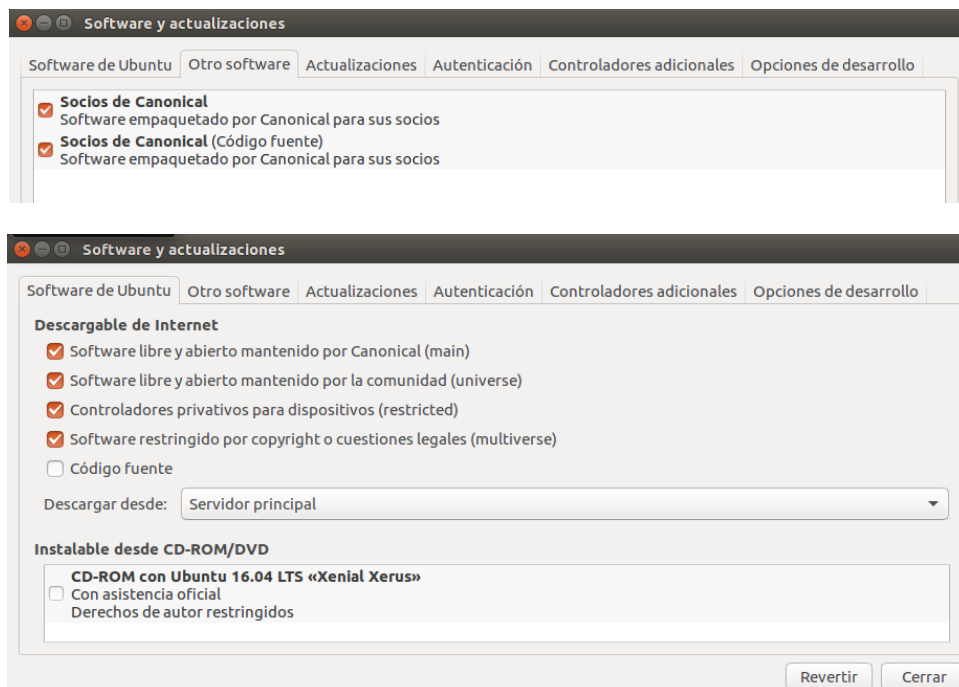
## PRE-INSTALL

Se recomienda que durante la instalación desactive el protector de pantalla y la energía  
It is recommended that during installation disables the screen saver and energy



Opcional: En **Software/Actualizaciones** marque **Servidor principal** y **Socios de Canonical** (pedirá contraseña) y elimine los repositorios que no vaya a utilizar.

Optional: In **Software/Updates** check **Partners Home Server and Canonical** (will ask password) and delete the repositories that are not using.



## INSTALL

Abra el terminal e instale las dependencias / Open the terminal and install dependencies

```
sudo apt-get -y install git dpkg apt
```

Descargue el proyecto Gateproxy y ejecútelo **sin privilegios “sudo”** / Download the Gateproxy project and run it **without privileges “sudo”**

```
git clone https://github.com/maravento/gateproxy
chmod +x gateproxy/gateproxy.sh && gateproxy/gateproxy.sh
```

## VERIFICACION DE SISTEMA OPERATIVO / CHECKING OF OPERATING SYSTEM

El script de instalación hará una verificación de su sistema operativo. Si todo es correcto iniciará la instalación continuará, de lo contrario el script abortará, indicando las causas.

The installation script will verify your operating system. If everything is correct you will begin the installation will continue, otherwise the script aborts, indicating the causes.

```
Sistema Operativo incorrecto. Instalacion abortada
Asegurese de tener instalado Ubuntu 16.04.x LTS x64
```

## VERIFICACION DE INTERFACES DE RED CON FORMATO ETH / CHECKING FORM NETWORK INTERFACES ETH

Gateproxy trabaja con eth, por tanto, el script verificará si tiene este formato en sus interfaces de red. Si es el caso, la instalación continuará, de lo contrario, ejecutará un comando para que conozca las direcciones MACs de sus interfaces de red.

En la siguiente imagen se muestran las direcciones MACs de las dos interfaces de red equivalentes a ETH0 (Publica) y ETH1 (Red Interna). Si tiene más interfaces debe agregarlas posteriormente. Y a continuación el script le pedirá que las introduzca, por lo tanto puede copiar y pegar. Una vez concluido, el script le solicitará que reinicie su servidor para que tome los cambios.

Gateproxy works with eth, therefore, the script will check whether this format on its network interfaces. If so, the installation will continue, otherwise, run a command to know the MAC addresses of network interfaces

In the next picture the MACs addresses of the two interfaces equivalent to ETH0 (Public) and ETH1 (internal network) network is. If you have more interfaces must add them later. And then the script will ask you to enter, so you can copy and paste. Once completed, the script prompts you to restart your server to make the changes.

```
Interfaces incorrectas

enp0s3   Link encap:Ethernet  direcciónHW 08:00:27:a1:fc:c1
enp0s8   Link encap:Ethernet  direcciónHW 08:00:27:53:44:62

Introduzca la MAC de la ETH0 publica (Ej: 00:00:00:00:00:00): 08:00:27:a1:fc:c1

Introduzca la MAC de la ETH1 Local (Ej: 11:11:11:11:11:11): 08:00:27:53:44:62

Reinicie su servidor y ejecute nuevamente Gateproxy
```



Reinicie y ejecute nuevamente el script / Restart and run script again

```
gateproxy/gateproxy.sh
```

### Inicio Gateproxy / Starting Gateproxy

```

Bienvenido a la instalacion de GateProxy Server v1.0
Welcome to installing GateProxy Server v1.0

Requisitos Mínimos / Minimum requirements:
GNU/Linux:      Ubuntu 16.04.x LTS x64
Processor:       Intel compatible 1x GHz
Interfaces:      eth0, eth1
RAM:             4GB
DD:             200 GB
Internet:        High Speed
Desktop:         Mate (optional)
Dependencies:    sudo apt-get -y install git apt dpkg

Exención de responsabilidad / Disclaimer:
Este script puede dañar su sistema si se usa incorrectamente
Para mayor información, visite gateproxy.com y lea el HowTO
This script can damage your system if used incorrectly
For more information, visit gateproxy.com and read the HowTO

Presione ENTER para iniciar o CTRL+C para cancelar
Press ENTER to start or CTRL+C to cancel

```

Al pulsar **Enter**, el instalador este verificara la suma (MD5). Si sale el mensaje: “**La suma no coincide**”, entonces la descarga fue corrupta. Debe revisar su conexión a internet y asegurarse de que sea de estable y rápida.

When you press Enter, the installer this will verify the sum (MD5). If you get the message: "The sum does not match" then the download was corrupt. You should check your internet connection and make sure it is stable and fast.

```

la suma no coincide
Verifique su conexion a internet y reinicie el script

```

```

git clone https://github.com/maravento/gateproxy
chmod +x gateproxy/gateproxy.sh && gateproxy/gateproxy.sh

```

El instalador le preguntará si quiere cambiar los parámetros por defecto que trae el proyecto GateProxy.

The installer will ask you to change the default settings that brings the GateProxy project.



```

Parametros del servidor:
ip 192.168.0.10, mask 255.255.255.0 /24, DNS 8.8.8.8,8.8.4.4, eth1
localnet 192.168.0.0, broadcast 192.168.0.255, rango-dhcp 100-250
Desea cambiar estos parametros? (s/n)

```

Al finalizar de configurar los parámetros de red, comenzará la instalación de paquetes. Asegúrese de tener una conexión de internet estable y de alta velocidad.

At the end of configuring network parameters it will begin installing packages. Make sure you have an internet connection stable and high speed.

### **La instalación de Gateproxy se divide en módulos o Packs / Gateproxy installation is divided into modules or packs**

#### **Essential:**

Instala una serie de aplicaciones necesarias que garantizan el funcionamiento mínimo de su servidor, tales como Apache, DHCP, PHP7, Squid, SSH, un Módulo de Reportes, Logs y Monitoreo, etc. También activa las reglas Squid Iptables, según el tipo de proxy que vaya a seleccionar. Se recomienda que elija NO (n) para activar el Proxy No-Transparente.

Installs a number of applications required to ensure the minimum performance of your server, such as Apache, DHCP, PHP7, Squid, SSH, Reporting Module, Logs and Monitoring, etc. Squid also enable Iptables rules, depending on the type of proxy you want to select. It is recommended that you choose NO (n) to activate the No-Transparent Proxy.

#### **Optional:**

Instala los paquetes / Install packages: Mate Desktop, Virtualbox Pack, gdiskdump, VNC server, Remote Desktop (Teamviewer-Remmina), y Samba (con carpeta compartida y papelera de reciclaje / with shared folder and recycle bin).

Si acepta la instalación, por cada paquete se le solicitará autorización / If you accept the installation, each packet will be asked authorization.

### **Encryption, Security, VPN, DNS and Audit Pack (Para Usuarios Avanzados / For Advanced users):**

Instala los paquetes / Install packages: Fail2Ban, DDOS Deflate, Mod Security, OWASP, Mod evasive, Rootkit checkers, Snort with Barnyard2, PulledPork, Snorby in Docker, ClamAV, libpam-cracklib, 2-Factor GoogleAuth, Veracrypt, Lynis, Nmap, Zenmap, ArpScan, SSLscan, cutter, python-nmap, Pipe Viewer, nbtscan, wireshark, Hping, tcpdump, dsniff, Byobu, My traceroute, Networking, toolkit, NetDiscover, wireless-tools, DNS-LOCAL, [4nonimizer](#), FruhoVPN, OpenVPN

Si acepta la instalación, por cada paquete se le solicitará autorización / If you accept the installation, each packet will be asked authorization

Dentro de este Pack encontramos algunos módulos experimentales. Instálelos bajo su propio riesgo / Within this pack are some experimental modules. Install at your own risk:

[Snort with Barnyard2, PulledPork, Snorby in Docker](#): Install IDS/IPS in Docker

DNS-LOCAL: Instala su propio servidor DNS (dnsmasq) y desactivar el nuevo mecanismo resolvconf y restaurar el antiguo resolv.conf para que pueda establecer sus DNS manualmente / Set up your own DNS (dnsmasq) server and disable the new resolvconf mechanism and restore the old resolv.conf so you can manually set your DNS.

VPN ([4nonimizer](#), FruhoVPN, OpenVPN): Derivar (o anonimizar) el tráfico por una VPN / Derive (or anonymous) traffic over a VPN

[BlackUSB](#): Este proyecto hace un inventario de los dispositivos usb conectados y activa la protección de puertos usb via udev, exceptuando la lista blanca de dispositivos preseleccionados, bloqueando el resto / This project makes an inventory of USB devices connected and active protection udev via USB ports, except the white shortlist devices, blocking the rest.

### **ANTES DE COMENZAR / BEFORE STARTING:**

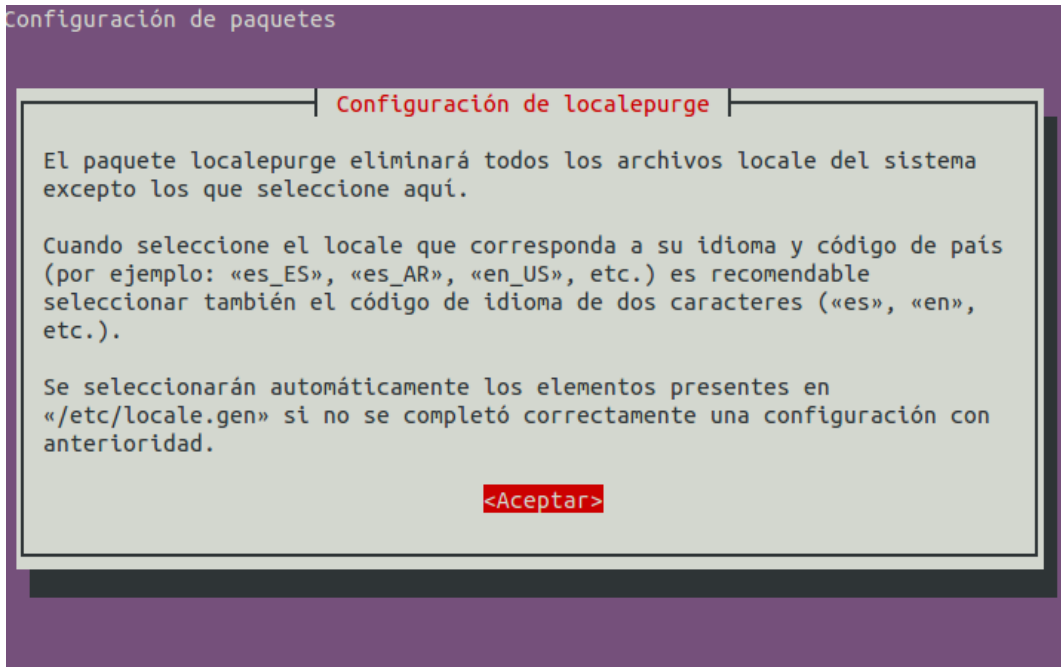
Durante el proceso de instalación el instalador le pedirá en varias veces que ingrese su contraseña (de usuario)

During the installation process the installer will ask several times to enter your password (user)

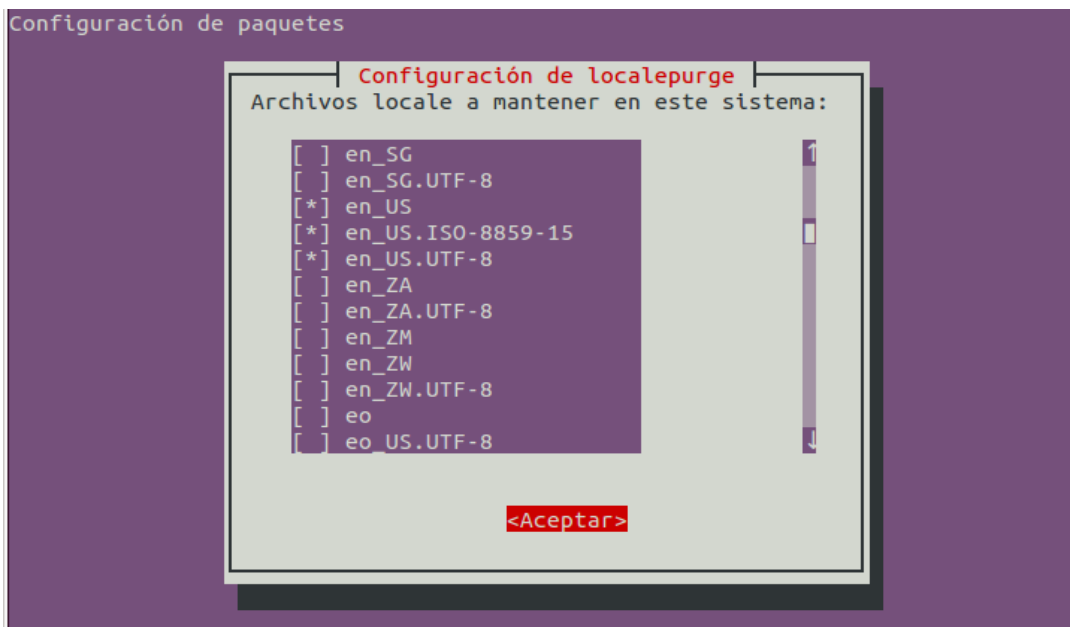
## ESSENTIAL PACK SETUP

Localepurge (opcional): Elimina idiomas innecesarios de su servidor. Elija **s** para instalarlo. Ya viene preconfigurado por defecto con los idiomas español (es) e inglés (en).

Remove unnecessary language of your server. I choose to install it. Already it comes pre-configured by default with the Spanish language (s) and English (en).

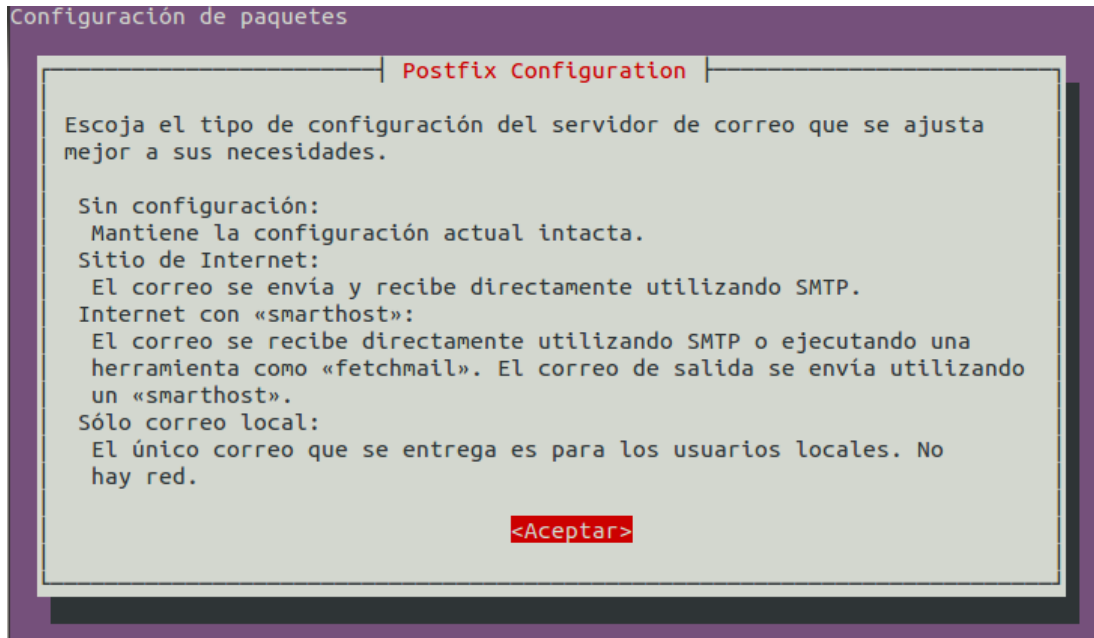


Pulse “**Aceptar**” / Click “**Accept**”

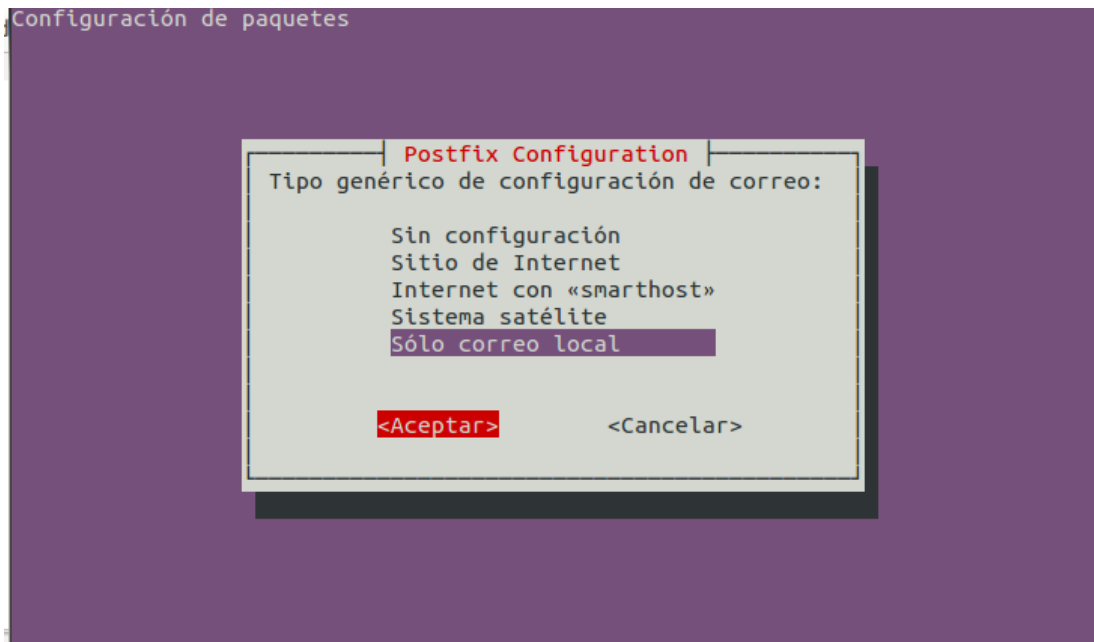


Postfix Mail (reemplazo de sendmail / sendmail replacement) ([HowTO](#))

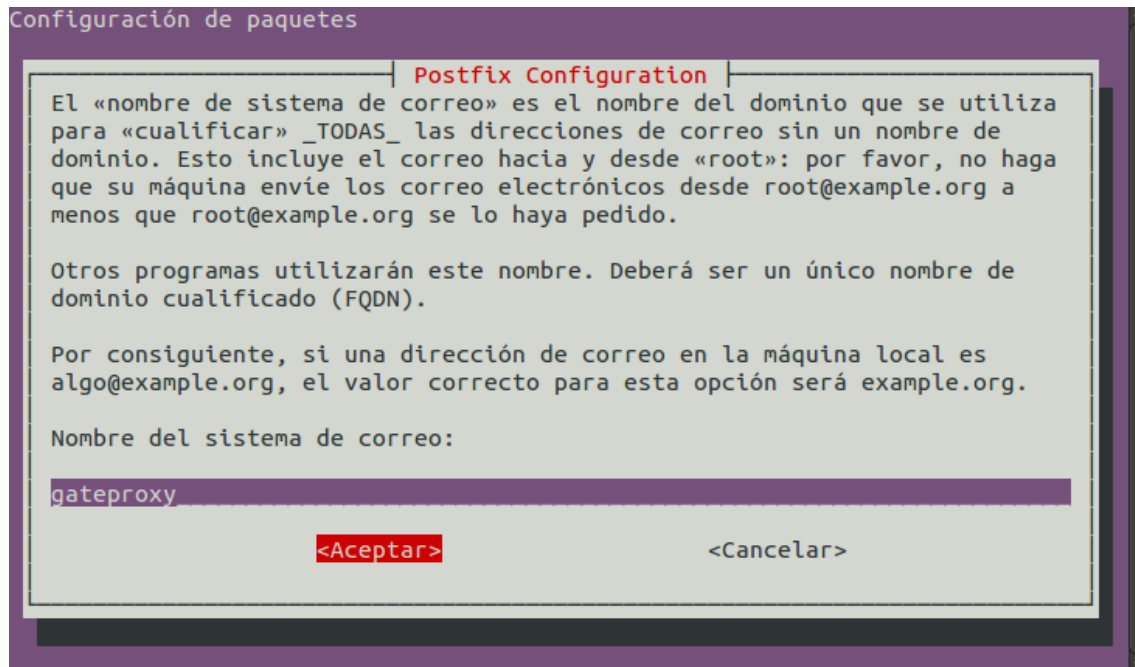
Si elige esta opción, pulse **Aceptar** en el siguiente recuadro / If you choose this option, click OK in the box below



Configúrelo según sus necesidades / Set it according to your needs



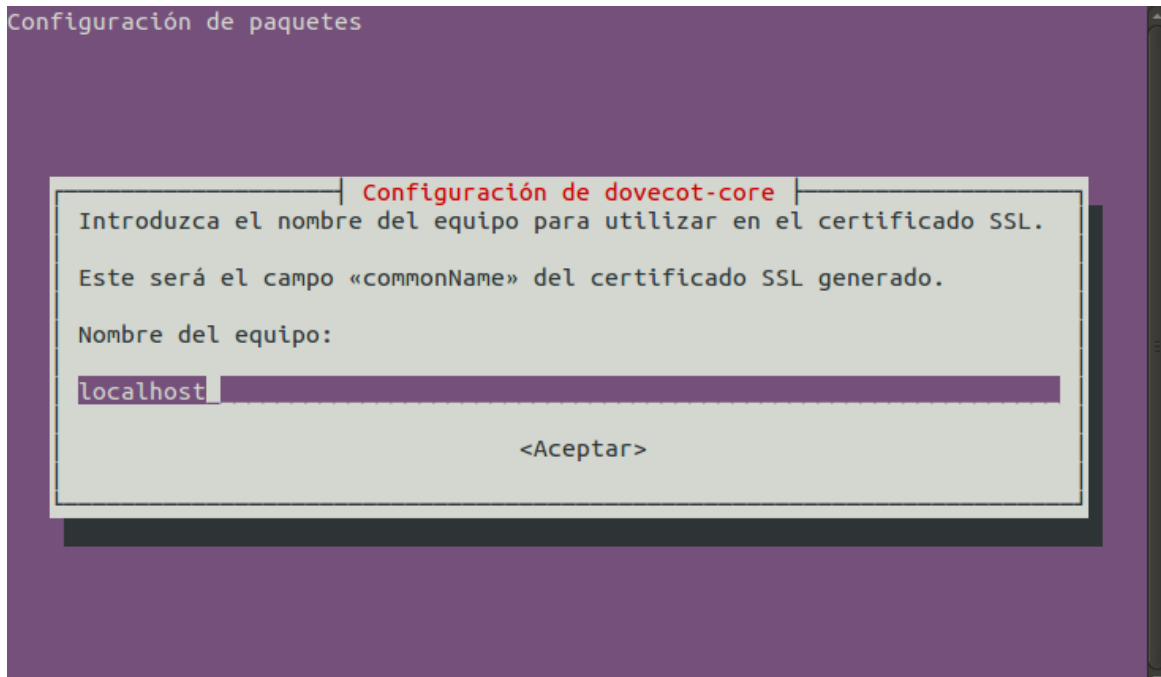
Escriba el nombre de su sistema (no elija "gateproxy") / Type the name of your system (not choose "gateproxy")



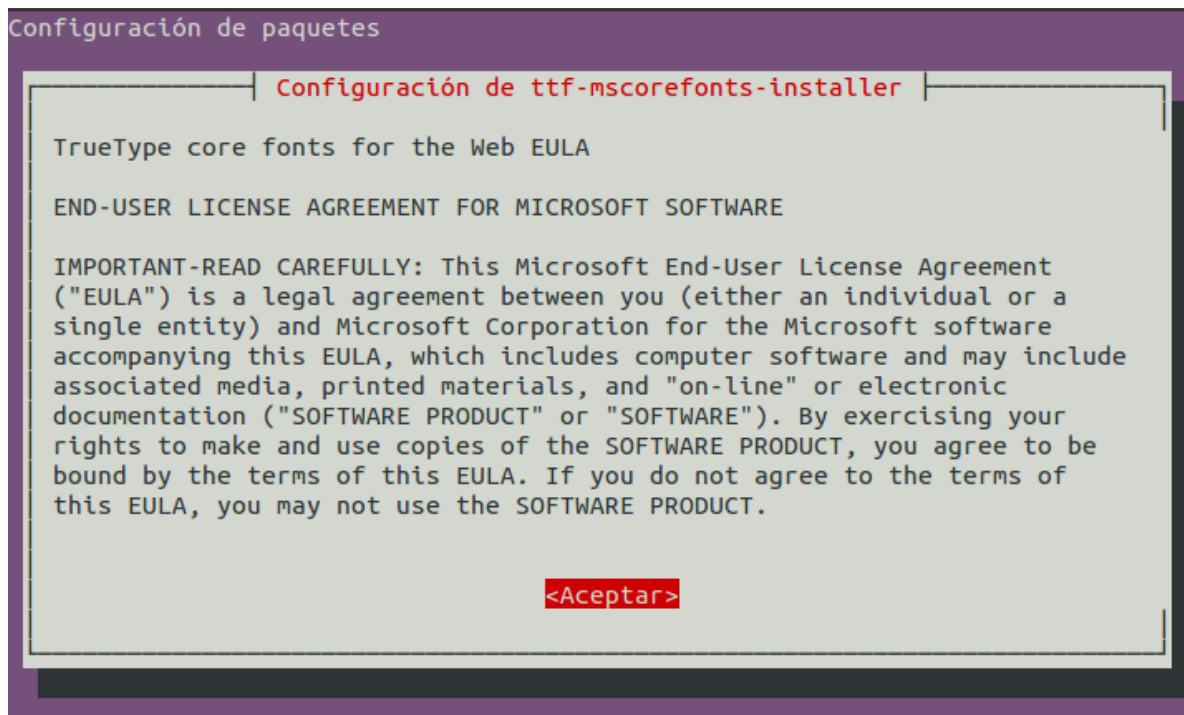
Seleccione **SI** / Select **YES**



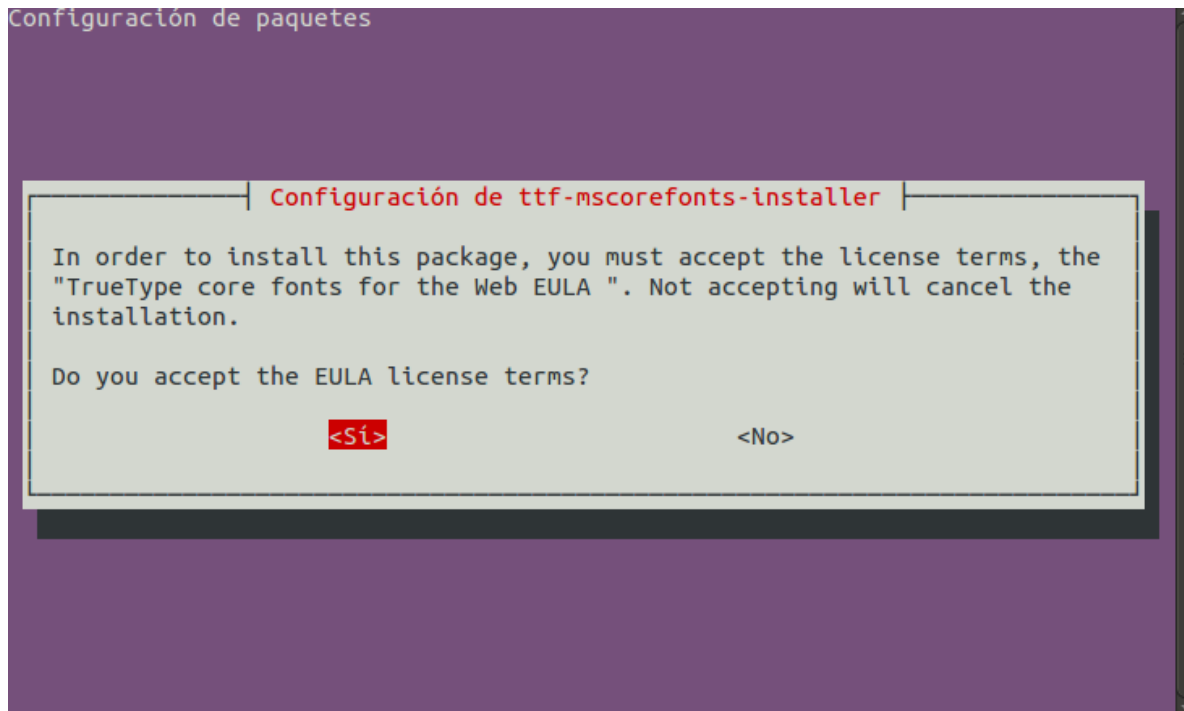
Seleccione **Aceptar** / Select **OK**



Microsoft Fonts pulse **Aceptar** /Select **Accept**



## Licencia EULA



[Teamviewer](#) le solicitará confirmación adicional / requesting additional information

```

Reading state information... Done
Building data structures... Done
Building data structures... Done
Requiere la instalación de los siguientes paquetes: gcc-4.9-base:i386 libasound2
:i386 libc6-i686:i386 libc6:i386 libexpat1:i386 libfontconfig1:i386 libfreetype6
:i386 libgcc1:i386 libice6:i386 libpng12-0:i386 libsm6:i386 libuuid1:i386 libx11
-6:i386 libxau6:i386 libxcb1:i386 libxdamage1:i386 libxdmcp6:i386 libxext6:i386
libxfixed3:i386 libxi6:i386 libxrandr2:i386 libxrender1:i386 libxtst6:i386 uuid-
runtime zlib1g:i386

TeamViewer (Remote Control Application)
TeamViewer is a remote control application. TeamViewer provides easy, fast and
secure remote access to Linux, Windows PCs, and Macs.

TeamViewer is free for personal use. You can use TeamViewer completely free of
charge to access your private computers or to help your friends with their compu
ter problems.

To buy a license for commercial use, please visit http://www.teamviewer.com
¿Quiere instalar el paquete de software? [s/N]:s
Get:1 http://ftp.us.debian.org/debian/ jessie/main gcc-4.9-base i386 4.9.2-10 [1
60 kB]
Get:2 http://ftp.us.debian.org/debian/ jessie/main libc6 i386 2.19-18 [3976 kB]
37% [2 libc6:i386 2958 kB/3976 kB 74%] 59.5 kB/s 1min 26s

```



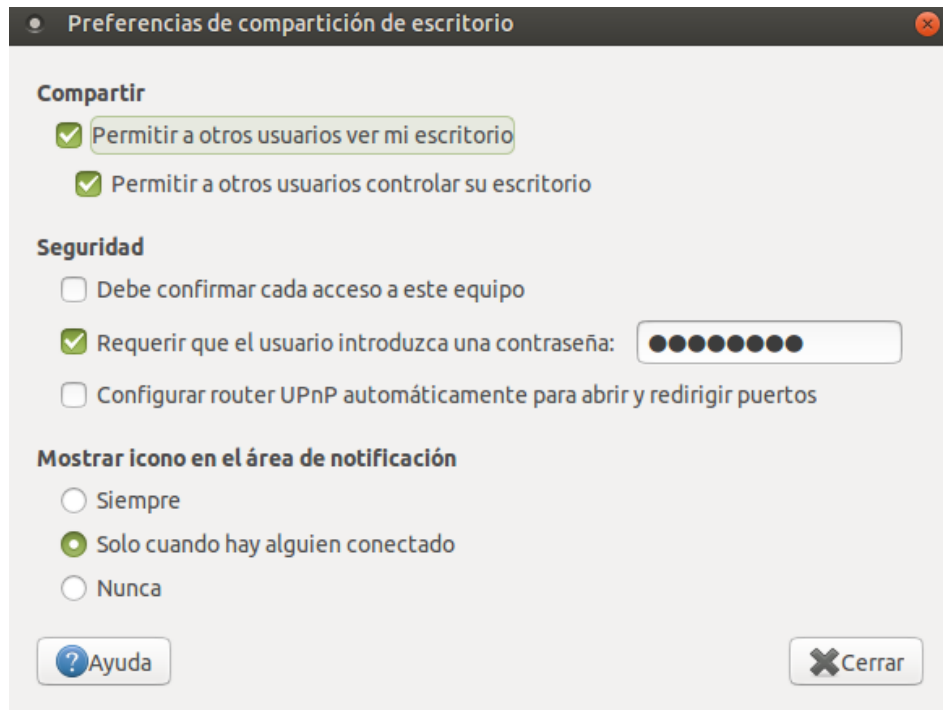
Y dependencias faltantes / And missing dependencies

```
(Leyendo la base de datos ... 200650 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar teamviewer_linux.deb ...
Desempaquetando teamviewer (10.0.35002) ...
dpkg: problemas de dependencias impiden la configuración de teamviewer:
 teamviewer depende de libjpeg8 | libjpeg62.

dpkg: error al procesar el paquete teamviewer (--install):
 problemas de dependencias - se deja sin configurar
Se encontraron errores al procesar:
 teamviewer
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Corrigiendo dependencias... Listo
Se instalarán los siguientes paquetes extras:
 libjpeg62-turbo:i386
Se instalarán los siguientes paquetes NUEVOS:
 libjpeg62-turbo:i386
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
1 no instalados del todo o eliminados.
Se necesita descargar 123 kB de archivos.
Se utilizarán 377 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

VNC Remote Desktop, se abrirá una ventana para que configure el escritorio remoto y pueda acceder desde una ubicación externa a su servidor.

A window will open to configure the remote desktop and can access from an external location to your server.



Es obligatorio marcar estas opciones ya que VNC vino-server puede detenerse / It is mandatory to mark these options as VNC vino-server may stop

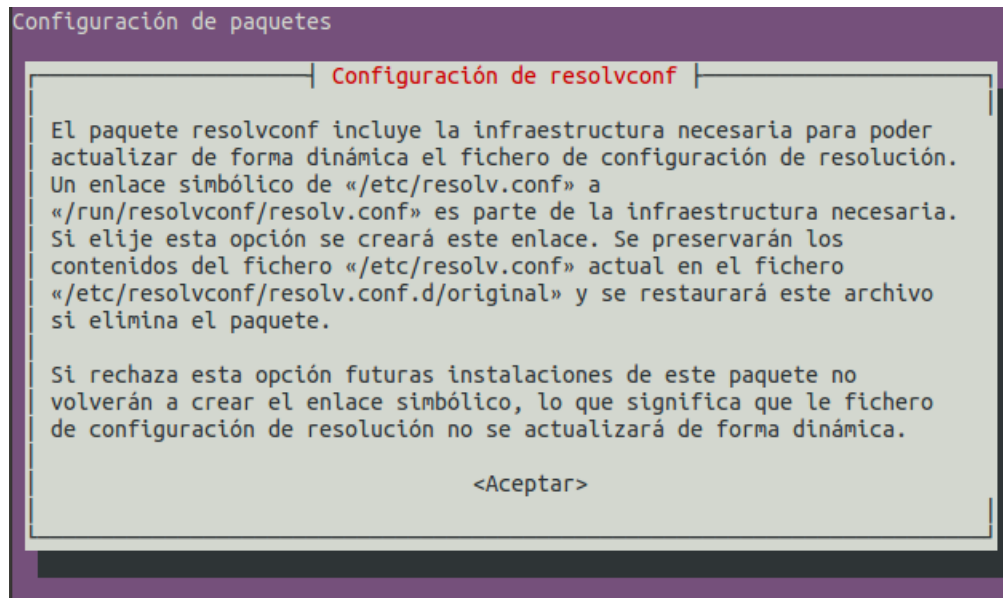
```
** (vino-server:993): WARNING **: The desktop sharing service is not enabled, so
it should not be run.
```

Important: Para activarlo edite `/etc/init.d/iptables.sh` y descomente las reglas VNC y elimine las restricciones sobre los puertos 5900 y 5901. EL servidor VNC no viene activo por defecto. Para iniciarlo manualmente escriba en el terminal: **sudo /etc/init.d/vnc-server.sh start**

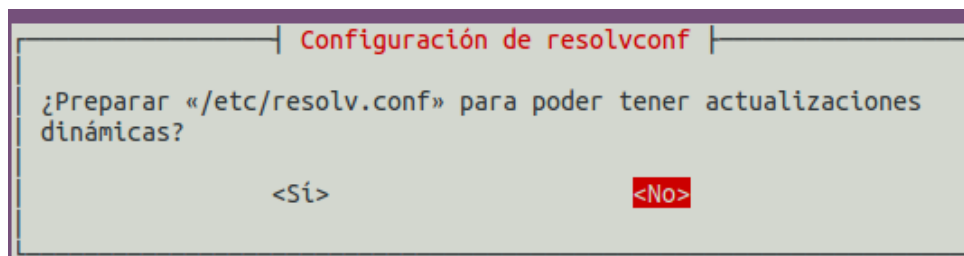
To activate `/etc/init.d/iptables.sh` edit and uncomment the VNC rules and remove restrictions on ports 5900 and 5901. The VNC server is not enabled by default. To start it manually type in the terminal: **sudo /etc/init.d/vnc-server.sh start**

### DNS-LOCAL

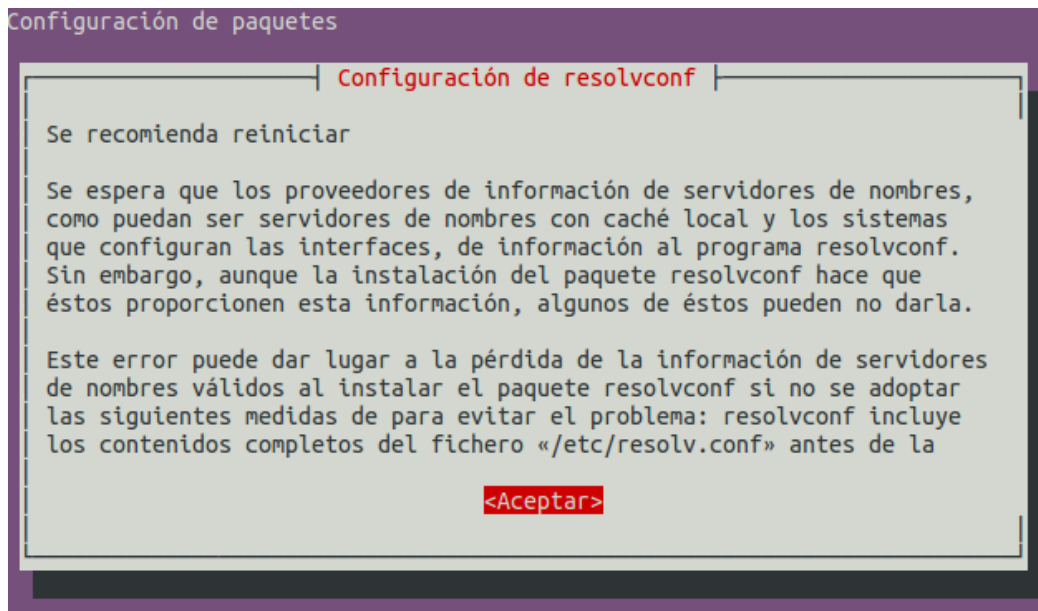
Desactiva el mecanismo resolvconf y configura el antiguo resolv.conf (dns estáticos). Si responde **SI** le saldrá la siguiente pantalla. Seleccione **Aceptar**  
Resolvconf mechanism disables and configures the old resolv.conf (static dns). If yes you will leave the following screen. Select **OK**



Seleccione **NO** / Select **NO**



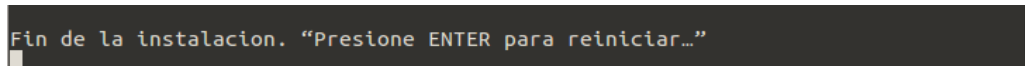
Seleccione **Aceptar** / Select **Accept**



Al finalizar la instalación de todos los módulos seleccionados (en dependencia de su conexión a internet) termina el script de instalación.

After installation of all selected modules (depending on your internet connection) terminates the installation script.

Presione **ENTER** para reiniciar el servidor / Press **ENTER** to restart the server.



Ha finalizado la instalación y configuración de **GATEPROXY**

You have completed the installation and configuration of **GATEPROXY**

### **PRELINK**

Al reiniciar por primera vez, ejecutamos en el terminal el comando prelink

When you restart for the first time in the terminal we run the prelink command

```
sudo prelink -all
```

## ADMINISTRANDO EL SERVIDOR

### WEBMIN

Access <https://localhost:10000> or <https://192.168.0.10:10000>

Ingresa al Webmin con el usuario **root** y **contraseña**. Si quiere cambiar la contraseña de **root** solamente para el acceso a webmin, ejecute en el terminal:

Login to Webmin with root user and password. If you want to change the root password only for access to webmin, run in the terminal:

```
sudo /usr/share/webmin/changepass.pl /etc/webmin root nueva_contraseña
```

Y la salida debe ser / And the output should be:

**updated password of webmin user root**

```
user@user:~$ sudo /usr/share/webmin/changepass.pl /etc/webmin root newpassword
Updated password of Webmin user root
```

Si quiere utilizar http en reemplazo de https, edite el archivo: / If you use http in lieu of https, edit the file:

**/etc/webmin/miniserv.conf**

y cambie el valor **SSL=1** a **SSL=0**

Puede cambiar el idioma y diseño de Webmin en: / You can change the language and design Webmin: **"Change Language and Theme"**

The image shows two parts of the Webmin interface. The top part is the login page for Webmin 1.791 on IP 192.168.1.10. It has a login form with fields for username (root) and password, a 'Remember me' checkbox, and a 'Sign in' button. The bottom part is the 'Change Language and Theme' module page. It has a sidebar with links like 'Webmin', 'Backup Configuration Files', 'Change Language and Theme', etc. The main content area shows settings for 'Webmin UI language' (Global language .. English US (en.UTF-8) selected, Personal choice .. Spanish (ES) available) and 'Webmin UI theme' (Global theme (Gray Framed Theme) selected, Personal choice .. MSC.Linux Theme available). There is a 'Make Changes' button at the bottom.

Puede usar diseños externos como: / You can use external designs such as:

### Bootstrap

The image shows the 'Temas de Webmin' (Webmin Themes) module page. It has a sidebar with 'Índice de Módulo' and 'Temas de Webmin'. The main content area has tabs for 'Change theme', 'Install theme', 'Delete themes', and 'Export themes'. The 'Install theme' tab is active. It contains instructions: 'Use the form below to install a new theme of Webmin in your system. Themes are typically distributed in .wbt files, but they can also be installed from RPM files if supported by your operating system.' Below the instructions are three radio buttons: 'Desde archivo local' (selected), 'Desde archivo a cargar' (with a 'Seleccionar archivo' button and 'No se eligió archivo' text), and 'Desde dirección URL ftp o http' (with a text input field containing 'http://theme.winfuture.it/bootstrap.wbt.gz'). There is an 'Instalar Tema' button at the bottom.



## REPORTES, LOGS y MONITOREO DEL SERVIDOR

Si instaló los Reportes, Logs y Monitoreo, al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache.

Si quiere instalar más herramientas de monitoreo, visite el post [80 Linux Monitoring Tools for SysAdmins](#)

If you installed Reports, Logs and Monitoring, entering for the first time, you will ask the user of your server and passwd you chose during the installation of Apache.

If you want to install more monitoring tools, and visit the post: [80 Linux Monitoring Tools for SysAdmins](#)

SARG: (programmable reports)

Access: <http://localhost/squid-reports/>, <http://gateproxy/squid-reports/>,  
<http://192.168.0.10:11500/>, o Webmin (<http://localhost:10000/sarg/>)

Los reportes SARG se generan diariamente. Para generarlos manualmente, ejecute en el terminal:

SARG reports are generated daily. To generate manually running on the terminal:

**`sudo sarg-reports today`**

O ingrese a webmin, a la sección “Servidores” y luego “Generador de Informes y Análisis de Squid” y finalmente pulse “Generar informe ahora”

Or login to webmin, to the "Servers" section and then "and Analysis Report Generator Squid" and finally click "Generate report now"

En la siguiente imagen vemos el reporte SARG diario de un equipo de la red local. A modo de ejemplo hemos bloqueado Facebook y el reporte indica dicho bloqueo con el mensaje **DENIED**. Para modificar este comportamiento, acceda a **/etc/acl/whitedomains.txt** y añada el sitio que quiera autorizar de acuerdo a sus necesidades, guarde los cambios y reconfigure el squid (**`sudo squid -k reconfigure`**) o desde Webmin, ingrese a la sección de **Sistema/Arranque y Parada** y reinicie squid. Es importante aclarar que primero su servidor debe registrar tráfico antes de generar el primer reporte de **SARG**, de lo contrario no aparecerá ningún reporte.

In the next picture we see the SARG daily report of a computer on the local network. As an example we have blocked Facebook and the report indicates that the message **DENIED** lock. To change this behavior, go to **/etc/acl/whitedomains.txt** and add the site you want to authorize according to your needs, save the changes and reconfigure the squid (**sudo squid -k reconfigure**) or from Webmin, go to the **System/start and stop** and restart squid. It is important to note that your server must register first traffic before generating the first report of **SARG**, otherwise no report will appear.

ads.eltiempo.com	170	249.45K	0.73%	0.00%	100.00%	00:05:09	309,740	0.61%	
static.bluradio.com.s3.amazonaws.com	26	238.13K	0.70%	0.00%	100.00%	00:01:33	93,510	0.18%	
www.gstatic.com:443	2	213.95K	0.63%	0.00%	100.00%	00:01:38	98,616	0.19%	
fonts.gstatic.com	14	209.57K	0.61%	0.00%	100.00%	00:00:36	36,238	0.07%	
static.foodanddrink-eus.s-msn.com	10	204.77K	0.60%	0.00%	100.00%	00:00:24	24,326	0.05%	
es.yahoo.com:443	2	203.21K	0.60%	0.00%	100.00%	00:00:26	26,938	0.05%	
www.msn.com	4	199.08K	0.58%	0.00%	100.00%	00:00:14	14,826	0.03%	
s.dynad.net	12	165.46K	0.48%	0.00%	100.00%	00:00:29	29,274	0.06%	
ssl.gstatic.com:443	4	163.78K	0.48%	0.00%	100.00%	00:01:07	67,492	0.13%	
clients4.google.com:443	4	146.24K	0.43%	0.00%	100.00%	00:14:24	864,748	1.70%	
cache.pack.google.com	32	138.02K	0.40%	0.00%	100.00%	00:00:00	0	0.00%	DENIED
www.facebook.com:443	32	116.70K	0.34%	0.00%	100.00%	00:00:00	0	0.00%	DENIED
cauth.googleusercontent.com:443	4	110.23K	0.32%	0.00%	100.00%	00:00:48	48,402	0.09%	
login.live.com:443	14	109.17K	0.32%	0.00%	100.00%	00:01:42	102,336	0.20%	
lytimg.com:443	6	102.60K	0.30%	0.00%	100.00%	01:30:42	5,442,954	10.68%	
www.quebuena compra.com	8	102.18K	0.30%	0.00%	100.00%	00:00:19	19,222	0.04%	
www.youtube-nocookie.com:443	6	86.73K	0.25%	0.00%	100.00%	00:02:08	128,364	0.25%	
ajax.aspnetcdn.com	2	84.82K	0.25%	0.00%	100.00%	00:00:07	7,950	0.02%	
analytics.mistatic.com	2	81.65K	0.24%	0.00%	100.00%	00:00:08	8,522	0.02%	
www.youtube.com:443	22	80.16K	0.23%	0.00%	100.00%	00:00:00	0	0.00%	DENIED
partner.googleadservices.com	2	69.65K	0.20%	0.00%	100.00%	00:00:07	7,854	0.02%	
fonts.gstatic.com:443	2	69.24K	0.20%	0.00%	100.00%	00:00:45	45,848	0.09%	
ajax.googleapis.com	2	66.86K	0.20%	0.00%	100.00%	00:00:06	6,074	0.01%	
mco-d2-p.mistatic.com	20	64.90K	0.19%	0.00%	100.00%	00:00:42	42,204	0.08%	
www.mercadolibre.com.co	4	64.68K	0.19%	0.00%	100.00%	00:00:09	9,398	0.02%	
ctidl.windowsupdate.com	16	60.48K	0.18%	0.00%	100.00%	00:00:00	0	0.00%	DENIED

### SQSTAT: (Tráfico en Tiempo real / Traffic in Real Time).

Access: <http://gateproxy/sqstat/sqstat.php> or <http://localhost/sqstat/sqstat.php>, or <http://192.168.0.10/sqstat/sqstat.php>

Para mayor seguridad, se recomienda que cambie la contraseña en **/var/www/html/sqstat/config.inc.php** (**\$cachemgr\_password[0]="tu\_usuario"**), y en **/etc/squid/squid.conf** (**cache\_mgr tu\_usuario** y **cachemgr\_passwd tu\_usuario all**). Ambas deben coincidir. Por defecto tienen el nombre de su servidor (**tu\_usuario**)

For added security, it is recommended to change the password in **/var/www/html/sqstat/config.inc.php** (**\$ cachemgr\_password [0] = "your\_username"**) and **/etc/squid/squid.conf** (**your\_username cache\_mgr** and **cachemgr\_passwd your\_username all**). Both must match. By default have the name of your server (**your\_username**)

La frecuencia de actualización por default es 0. Si quiere cambiarla, pulse el botón **stop**, luego en el recuadro de **Auto refresh** ponga la frecuencia de actualización en segundos y pulse **update**. Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache.

The refresh rate default is 0. If you want to change it, press the stop button, then the Auto refresh box set the refresh rate in seconds and press update. When entering for the first time, should the user of your server and passwd you chose during the installation of Apache will ask

Host	URI	Curr. Speed	Avg. Speed	Size	Time
<b>Total:</b> 1 users and 22 connections @ 55.05/43.10 KB/s (CURR/AVG)					
<b>192.168.10.101</b>					
http://img.eltiempo.com/contenido/IMAGEN/IMAGEN-15677495-1.j ...		0.45 KB/s	1.58 KB/s	9 Kb	6s
http://www.eltiempo.com/contenido/estilo-de-vida/salud/IMAGE ...				0 b	
http://www.eltiempo.com/contenido/deportes/futbol/IMAGEN/IMA ...				0 b	
http://img.eltiempo.com/contenido/deportes/otros-deportes/IM ...				0 b	
http://img.eltiempo.com/contenido/tecnosfera/novedades-tecno ...				16 Kb	2s
http://www.quebuena compra.com/media/autopauta/product/resize ...				0 b	
http://www.quebuena compra.com/media/autopauta/product/resize ...				0 b	1s
http://img.eltiempo.com/contenido/IMAGEN/IMAGEN-15677375-1.j ...				0 b	1s
http://www.quebuena compra.com/media/autopauta/product/resize ...				0 b	1s
http://img.eltiempo.com/contenido/estilo-de-vida/gente/IMAGE ...			1.72 KB/s	8 Kb	5s
safebrowsing-cache.google.com:443		54.41 KB/s	25.73 KB/s	205 Kb	8s
ad.doubleclick.net:443		0.19 KB/s	0.42 KB/s	5 Kb	13s
clients4.google.com:443			0.25 KB/s	4 Kb	18s
http://notifications-9.mercadolibre.com/jms/mco/listen?notif ...				0 b	18s
googleads.g.doubleclick.net:443			2.26 KB/s	47 Kb	21s
safebrowsing.google.com:443			0.31 KB/s	6 Kb	21s
www.google.com:443			0.05 KB/s	1 Kb	23s
cm.g.doubleclick.net:443			0.04 KB/s	952 b	24s
pagead2.googlesyndication.com:443			1.15 KB/s	29 Kb	26s
www.mercadolibre.com.co:443			0.21 KB/s	5 Kb	26s
tpc.googlesyndication.com:443			4.81 KB/s	154 Kb	32s
s0.2mdn.net:443			4.55 KB/s	159 Kb	35s
<b>Total:</b> 1 users and 22 connections @ 55.05/43.10 KB/s (CURR/AVG)					

Cada vez que reinicie **squid con apache (recomendado)** (sudo squid -k reconfigure | sudo invoke-rc.d apache2 reload), la comunicación con sqstat se perderá momentáneamente y aparecerá un mensaje de error.

Each time you restart **squid with Apached)** (sudo squid -k reconfigure | sudo invoke-rc.d apache2 reload), communication with SqStat be lost momentarily and an error message appears.



### SqStat error

**Error (111): Connection refused**

Espere un minuto y pulsar la tecla F5 para recargar la página / Wait one minute and press the F5 key to refresh the page.



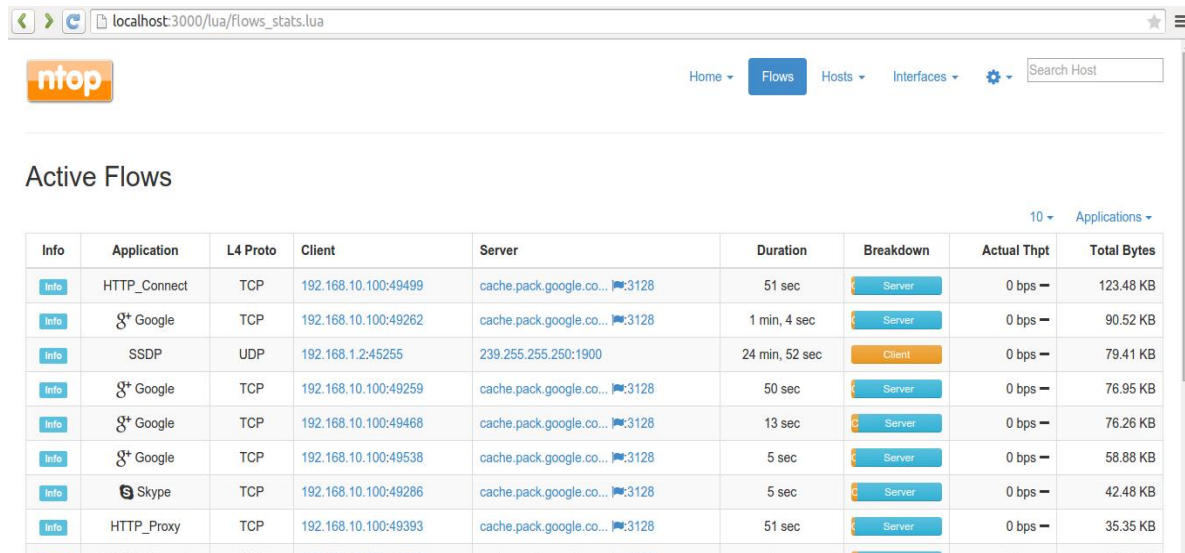
## NTOP-NG

Access: <http://localhost:3000>, <http://192.168.0.10:3000>

user: **admin** pass: **admin**

**NTopng** puede consumir gran cantidad de recursos de su servidor. Para saber el número de su adaptador de red y configurarlo, ejecute: **sudo ntopng -h**

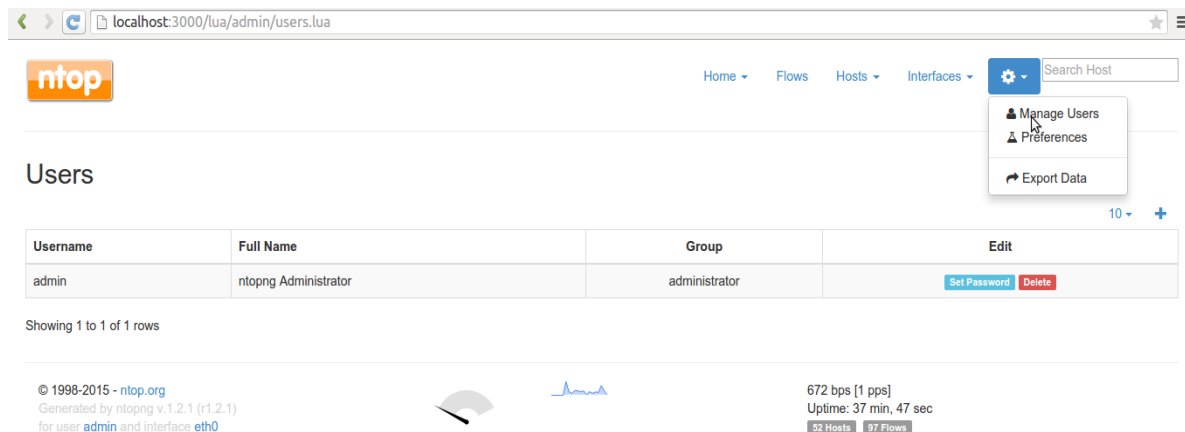
**NTopng** can consume lots of resources on your server. To know the number of your network adapter and configure, run: **sudo ntopng -h**



The screenshot shows the ntopng web interface at localhost:3000/ua/flows\_stats.lua. The 'Active Flows' section displays a table of network flows. The table has columns for Info, Application, L4 Proto, Client, Server, Duration, Breakdown, Actual Thpt, and Total Bytes. The flows listed include HTTP\_Connect, Google, SSDP, and Skype, all showing 0 bps and varying total bytes.

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes
Info	HTTP_Connect	TCP	192.168.10.100:49499	cache.pack.google.co...:3128	51 sec	Server	0 bps	123.48 KB
Info	Google	TCP	192.168.10.100:49262	cache.pack.google.co...:3128	1 min, 4 sec	Server	0 bps	90.52 KB
Info	SSDP	UDP	192.168.1.2:45255	239.255.255.250:1900	24 min, 52 sec	Client	0 bps	79.41 KB
Info	Google	TCP	192.168.10.100:49259	cache.pack.google.co...:3128	50 sec	Server	0 bps	76.95 KB
Info	Google	TCP	192.168.10.100:49468	cache.pack.google.co...:3128	13 sec	Server	0 bps	76.26 KB
Info	Google	TCP	192.168.10.100:49538	cache.pack.google.co...:3128	5 sec	Server	0 bps	58.88 KB
Info	Skype	TCP	192.168.10.100:49286	cache.pack.google.co...:3128	5 sec	Server	0 bps	42.48 KB
Info	HTTP_Proxy	TCP	192.168.10.100:49393	cache.pack.google.co...:3128	51 sec	Server	0 bps	35.35 KB

Change default pass: In **Manage Users** (user **admin**) select **set password**



The screenshot shows the ntopng web interface at localhost:3000/ua/admin/users.lua. The 'Users' section displays a table with one user, 'admin'. A dropdown menu is open, showing options: 'Manage Users', 'Preferences', and 'Export Data'. The 'admin' user row has buttons for 'Set Password' and 'Delete'.

Username	Full Name	Group	Edit
admin	ntopng Administrator	administrator	Set Password Delete

Showing 1 to 1 of 1 rows

© 1998-2015 - ntop.org  
Generated by ntopng v.1.2.1 (r1.2.1)  
for user admin and interface eth0

672 bps [1 pps]  
Uptime: 37 min, 47 sec  
52 Hosts 97 Flows

## IPTRAF

Access: **sudo iptraf** or <http://localhost:11300> or <http://192.168.0.10:11300>

Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache

When entering for the first time, should the user of your server and passwd you chose during the installation of Apache will ask

### Iptraf terminal

```

IPtraf
TCP connections (source host/port) ----- packets ----- bytes flags iface
192.168.1.22:54534 > 55 5848 --A- eth0
192.168.1.10:445 > 41 7176 -PA- eth0
74.125.141.95:443 > 4 1918 -PA- eth0
192.168.1.31:49739 > 3 2861 --A- eth0
54.243.82.70:443 > 1 120 -PA- eth0
192.168.1.22:40944 > 1 40 --A- eth0
192.168.1.31:49733 > 1 41 --A- eth0
192.168.1.10:3128 > 1 52 --A- eth0
192.168.1.31:49734 > 1 41 --A- eth0
192.168.1.10:3128 > 1 52 --A- eth0
162.125.32.129:443 > 2 420 --A- eth0
192.168.1.31:49623 > 1 437 -PA- eth0
TCP: 6 active
Active

UDP (78 bytes) from 192.168.1.103:137 to 192.168.1.255:137 on eth0
UDP (61 bytes) from 192.168.1.132:50091 to 224.0.0.252:5355 on eth0
UDP (161 bytes) from 192.168.1.77:51343 to 239.255.255.250:1900 on eth0
UDP (61 bytes) from 192.168.1.132:50091 to 224.0.0.252:5355 on eth0
UDP (78 bytes) from 192.168.1.132:137 to 192.168.1.255:137 on eth0

Pkts captured (all interfaces): 199 | TCP flow rate: 6,80 kbits/s
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit
  
```

### Logs IPtraf web

```

192.168.1.10:49200/iptrafaudit.log

Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49344; FIN sent; 5 packets, 3945 bytes, avg flow rate 31,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49344 to 5.45.58.148:80; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49344 to 5.45.58.148:80; FIN sent; 6 packets, 834 bytes, avg flow rate 6,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 192.168.1.150:49345 to 5.45.58.148:80; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 5.45.58.148:80 to 192.168.1.150:49345; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49345; FIN sent; 4 packets, 3905 bytes, avg flow rate 31,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49345 to 5.45.58.148:80; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49345 to 5.45.58.148:80; FIN sent; 6 packets, 834 bytes, avg flow rate 6,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 192.168.1.150:49346 to 5.45.58.148:80; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 5.45.58.148:80 to 192.168.1.150:49346; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49346; FIN sent; 5 packets, 3945 bytes, avg flow rate 31,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49346 to 5.45.58.148:80; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49346 to 5.45.58.148:80; FIN sent; 7 packets, 880 bytes, avg flow rate 7,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49346; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 192.168.1.150:49347 to 5.45.58.148:80; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 5.45.58.148:80 to 192.168.1.150:49347; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49347; FIN sent; 5 packets, 3945 bytes, avg flow rate 31,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49347 to 5.45.58.148:80; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49347 to 5.45.58.148:80; FIN sent; 6 packets, 834 bytes, avg flow rate 6,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 192.168.1.150:49348 to 5.45.58.148:80; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 5.45.58.148:80 to 192.168.1.150:49348; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49348; FIN sent; 4 packets, 3905 bytes, avg flow rate 31,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49348 to 5.45.58.148:80; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49348 to 5.45.58.148:80; FIN sent; 6 packets, 834 bytes, avg flow rate 6,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 192.168.1.150:49349 to 5.45.58.148:80; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49349; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 5.45.58.148:80 to 192.168.1.150:49349; FIN sent; 4 packets, 3905 bytes, avg flow rate 31,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49349 to 5.45.58.148:80; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49349 to 5.45.58.148:80; FIN sent; 6 packets, 834 bytes, avg flow rate 6,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 52 bytes; from 5.45.58.148:80 to 192.168.1.150:49350; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 40 bytes; from 5.45.58.148:80 to 192.168.1.150:49350; first packet (SYN)
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49350 to 5.45.58.148:80; FIN sent; 4 packets, 3905 bytes, avg flow rate 31,00 kbits/s
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49350 to 5.45.58.148:80; FIN acknowledged
Fri Apr 29 16:50:01 2016; TCP; eth1; 46 bytes; from 192.168.1.150:49350 to 5.45.58.148:80; FIN sent; 6 packets, 834 bytes, avg flow rate 6,00 kbits/s
  
```

logs de IPtraf cron task (50 lines)

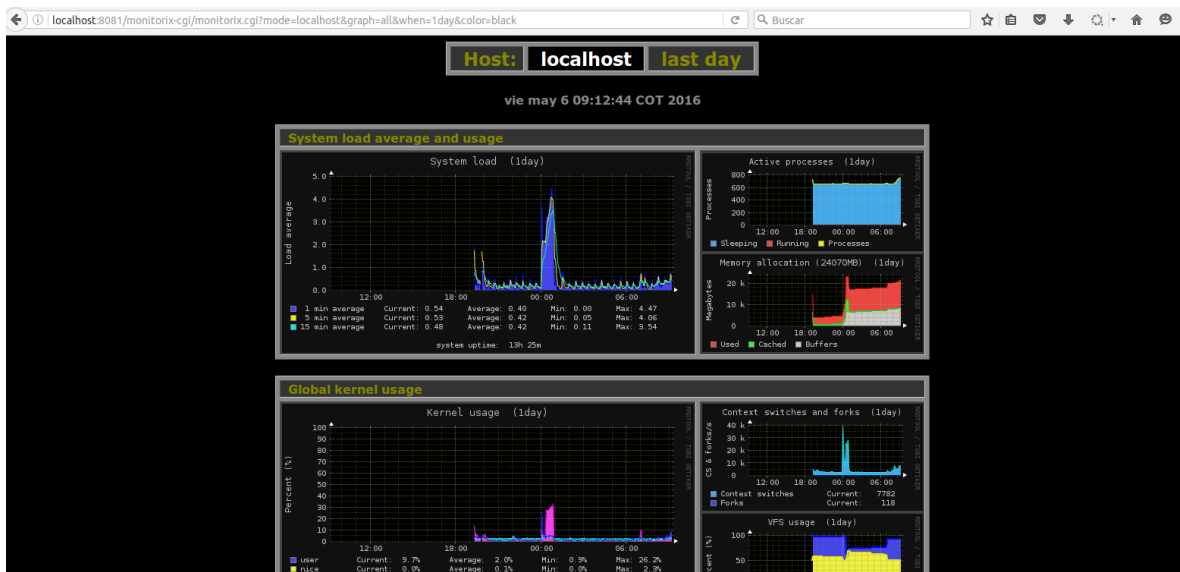
**@daily tail -50 /var/log/iptraf/ip\_traffic-1.log > /etc/iptrafaudit/iptrafaudit.log**

Para cambiarlo, por ejemplo ver las últimas 100 líneas cada 2 minutos / To change this, for example see the last 100 lines every 2 minutes

**\*10 \* \* \* tail -100 /var/log/iptraf/ip\_traffic-1.log > /etc/iptrafaudit/iptrafaudit.log**

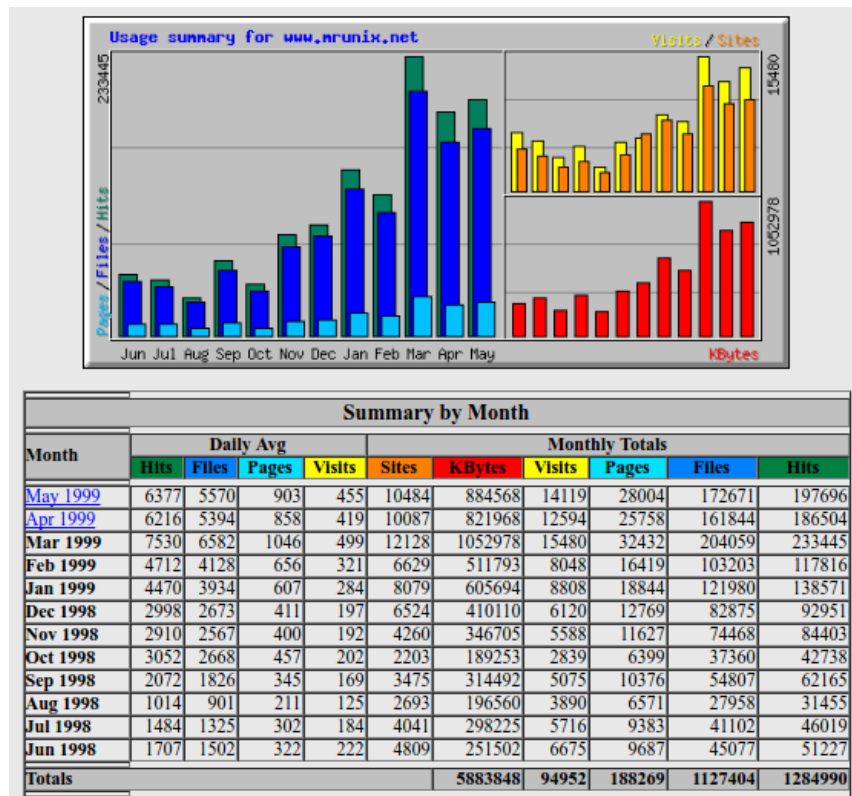
## MONITORIX

Access: <http://localhost:8081/monitorix/> or <http://192.168.0.10:8081/monitorix/>



## Webalizer

Access: <http://localhost:10000> or <http://192.168.0.10:10000> (servers/webalizer)



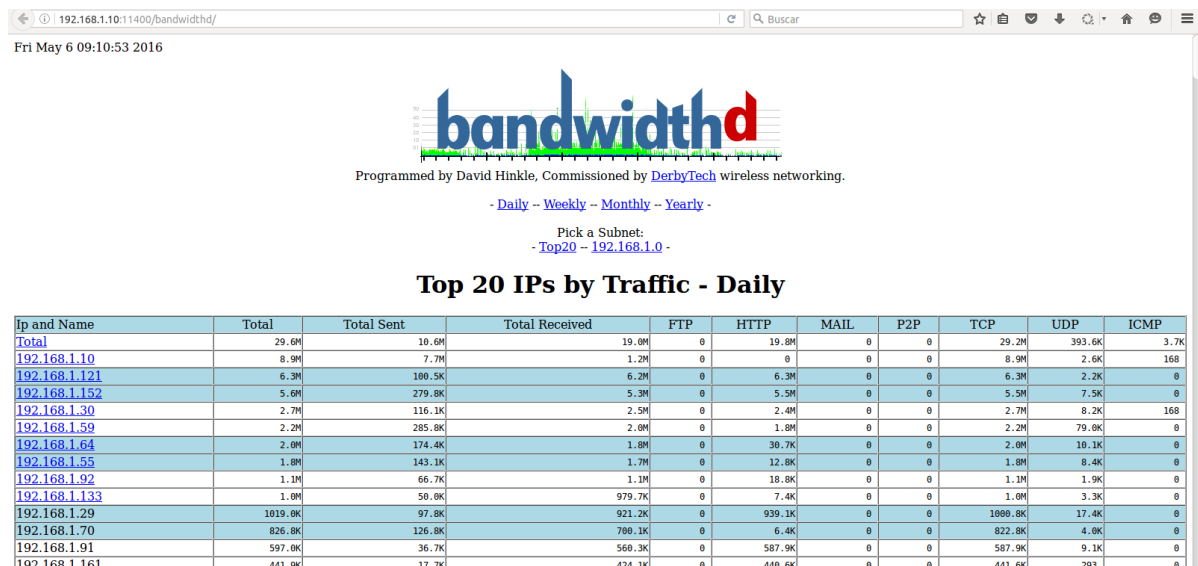
## Bandwidthd

Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache

When entering for the first time, should the user of your server and passwd you chose during the installation of Apache will ask



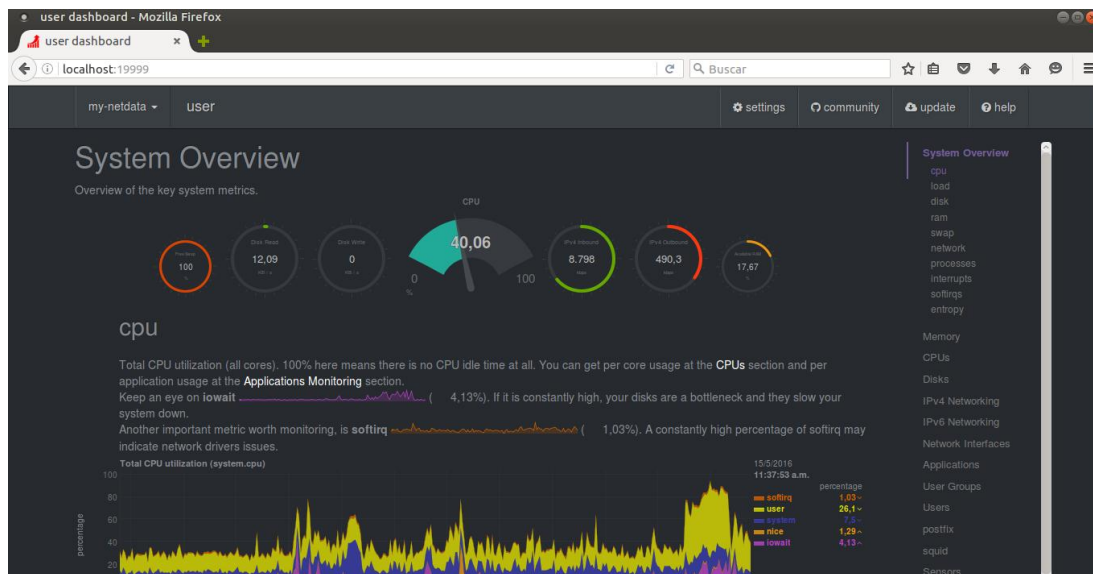
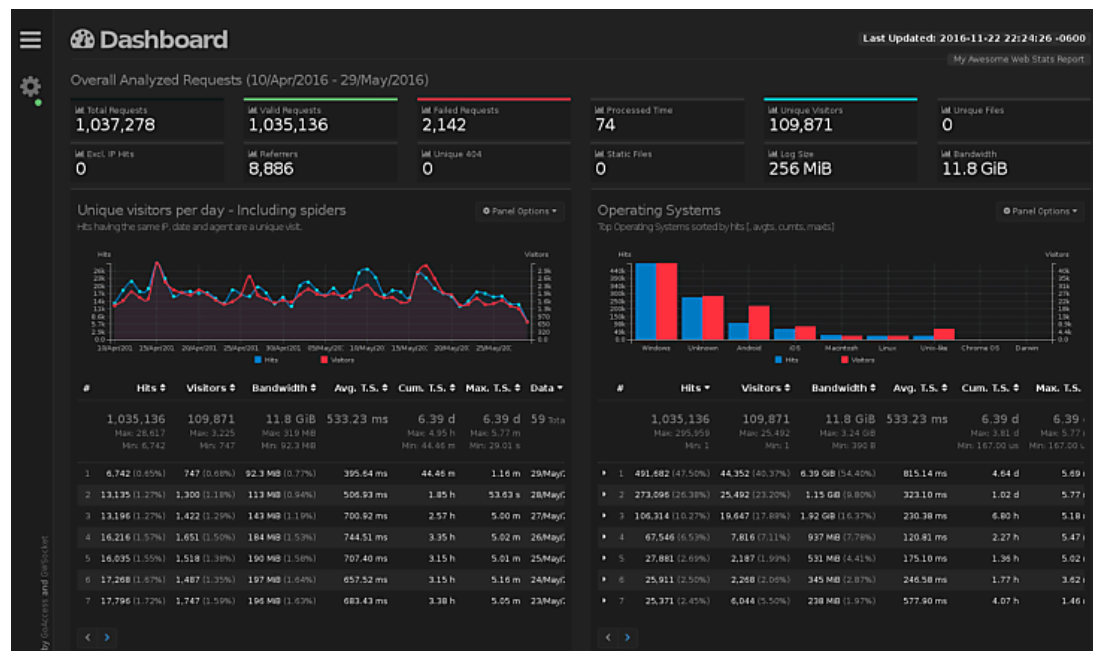
Access: <http://localhost:11400> or <http://192.168.0.10:11400>



NetData: (Server Resources / Recursos del Servidor)Press **Enter**

```
This installer allows you to change the installation path.
Press Control-C and run the same command with --help for help.

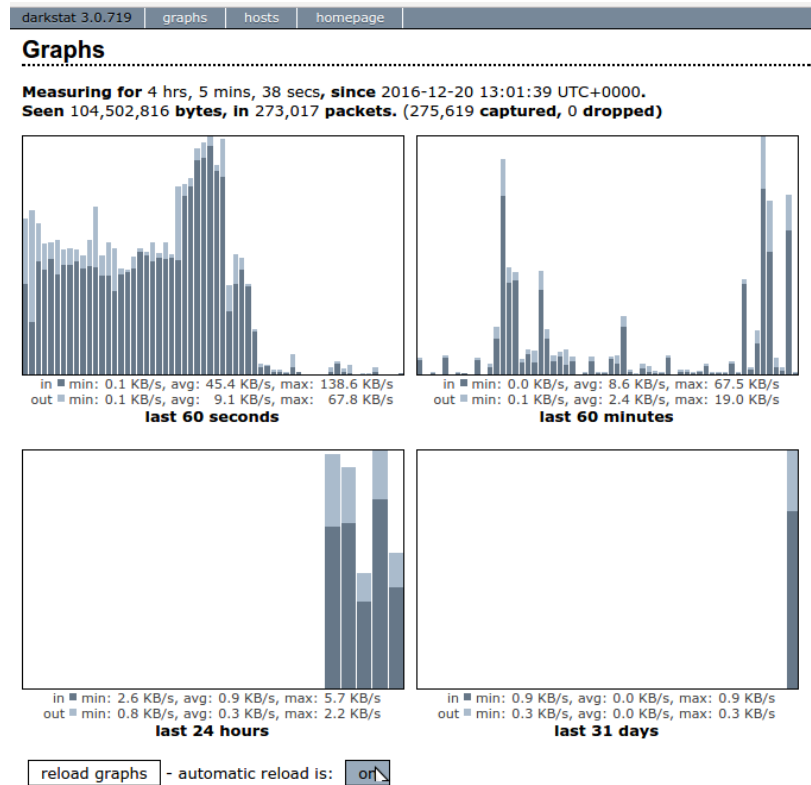
Press ENTER to build and install netdata to your system > |
```

Access: <http://localhost:19999/>Goaccess (Apache logs report) <http://localhost:11700/>



[Darkstat](http://localhost:666/) (host/net reports) <http://localhost:666/>

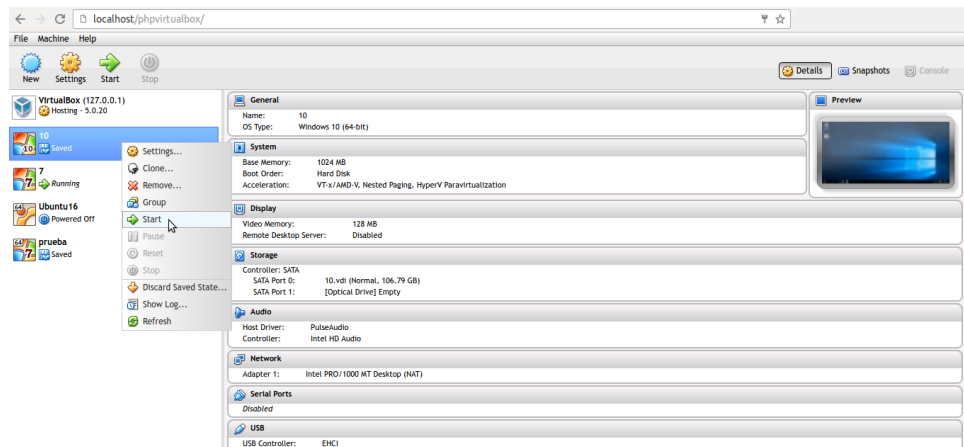
Active botón ON al final de la web para gráficos en tiempo real / Active button ON at the end of the web for real-time graphics



[PHPVIRTUALBOX](http://192.168.0.10:11600): Access <http://192.168.0.10:11600>

Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache

When entering for the first time, should the user of your server and passwd you chose during the installation of Apache will ask



## Encryption, Security, VPN, DNS and Audit Pack

Lynis: For more information read the post / Para mayor información lea el post [Auditoria de servidores Linux](#)

```

user@user: ~
Archivo Editar Ver Buscar Terminal Ayuda
Cleaning up... [ DONE ]
user@user:~$ sudo lynis audit system -Q

[ Lynis 2.1.1 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

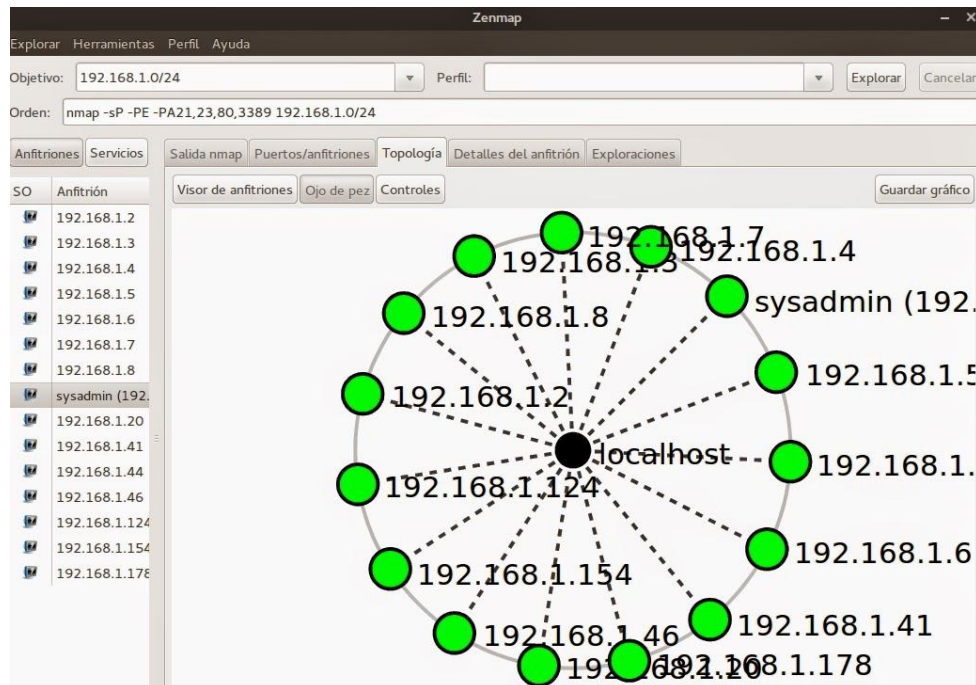
Copyright 2007-2015 - CISOfy, https://cisofy.com
Enterprise support and plugins available via CISOfy
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]

-----
Program version:      2.1.1
Operating system:     Linux
Operating system name: Ubuntu
Operating system version: 16.04
Kernel version:       4.4.0

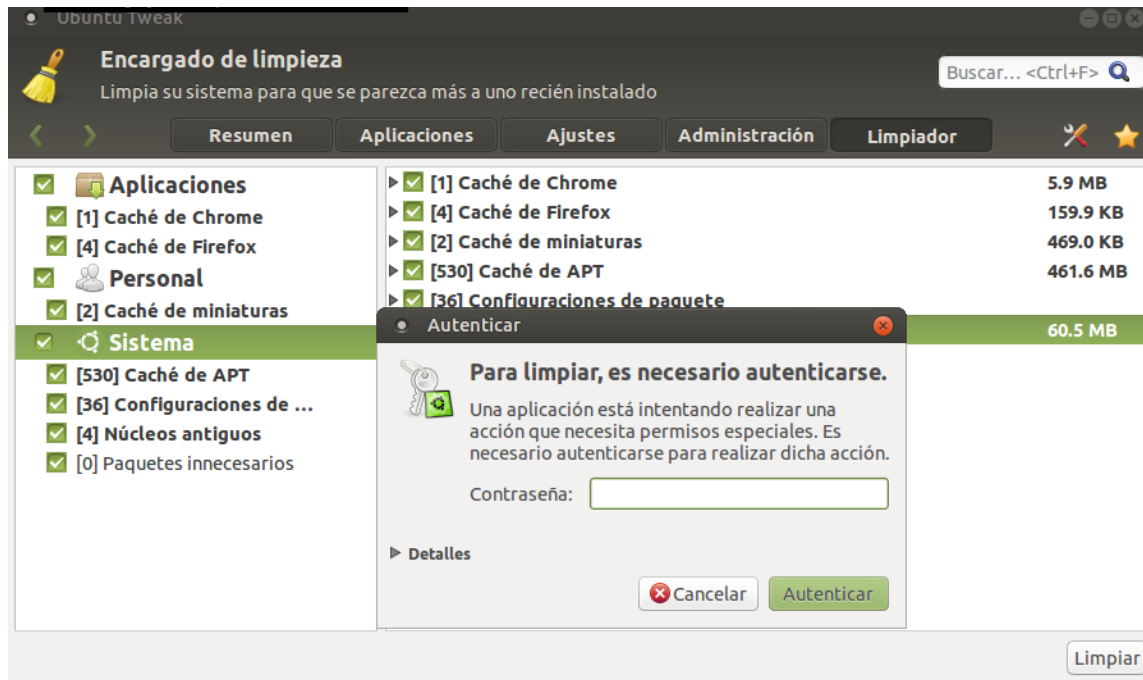
```

Zenmap/Nmap: For more information read the post / Para mayor información lea el post [Control de Acceso /Access Control](#)

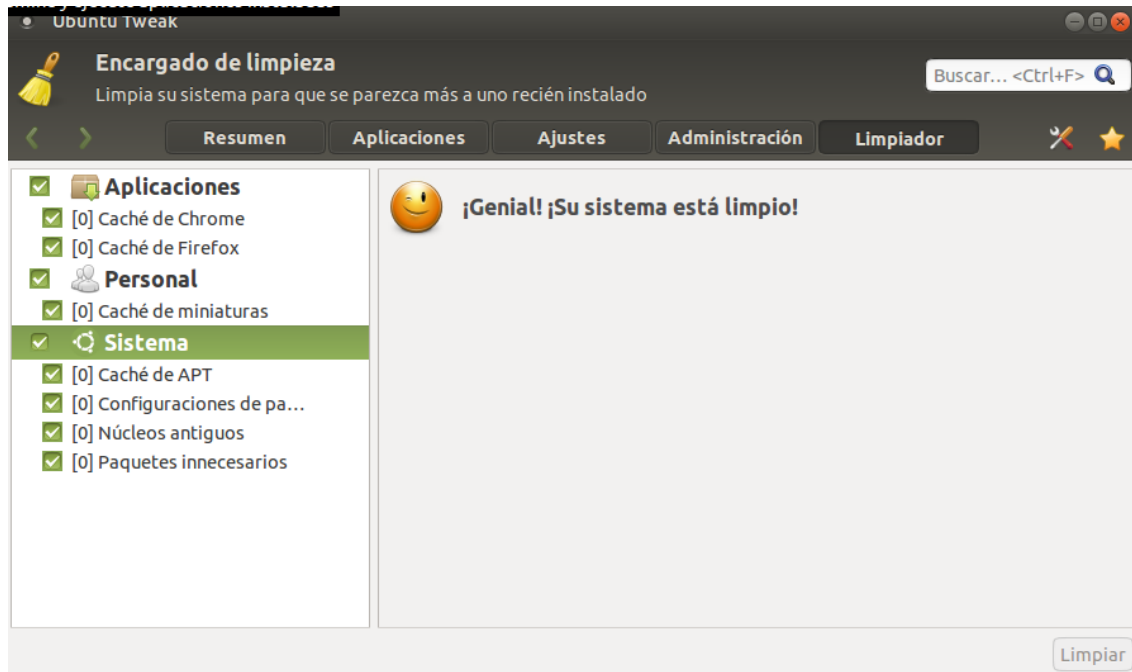




## OPCIONAL

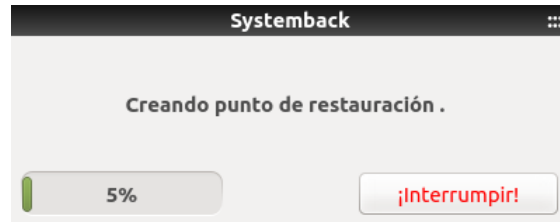
LIMPIEZA / CLEAN with **Ubuntu Tweak**

Clean Done



## CREANDO PUNTO DE RESTAURACION / RESTORE POINT

Creando un punto de restauración / Creating a restore point ...



## BACKUP HARD DRIVE/PARTITION

For more information read the post / Para mayor información visite los posts:

[Clonación Incremental](#) y [Clonación Virtual](#)



## POST-INSTALL

No olvide crear su contraseña root / Do not forget to create your root password.

```
sysadmin@gateproxy:~$ sudo su
[sudo] password for sysadmin:
root@gateproxy:/home/sysadmin# passwd
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@gateproxy:/home/sysadmin# exit
```

## Encryption

[libpam-cracklib](#): Debe tener en cuenta que los parámetros mínimos / You should note that the minimum parameters:

Longitud de la contraseña / Password Length	12 caracteres/ characters
Cambio de clave / Key change	3 diferencias (2 caracteres en mayúscula, 2 en minúscula, 2 dígitos y 2 símbolos) 3 Differences (2 characters uppercase, lowercase 2, 2 digits and 2 symbols)

Si quiere restablecer los valores por default o quiere fortificar aún más su contraseña, edite el archivo /etc/pam.d/common-password y modifique los valores de acuerdo a sus necesidades:

If you want to reset the default values or want further fortifying your password, edit the file /etc/pam.d/common-password and change the settings according to your needs:

**password requisite pam\_cracklib.so retry=3 minlen=12 difok=3 ucredit=-2 lcredit=-2 dcredit=-2 ocredit=-2**

retry	Número de intentos antes de que el sistema devuelva un error / Number of attempts before the system returns an error
minlen	Longitud mínima de contraseña / minimum password length
difok	Cambios de caracteres de la nueva contraseña en comparación con la anterior / Character changes the new password compared to the previous
ucredit	Cantidad de caracteres en mayúscula / Number of characters in uppercase
lcredit	Cantidad de caracteres en minúscula / Number of characters in lowercase
dcredit	Número de dígitos que debe tener la nueva contraseña / Number of digits that must have the new password
ocredit	Número de dígitos que debe tener la contraseña / Number of digits that must have the password

Ejemplo/Example:

ucredit=-3 (Significa que como mínimo debe tener 3 caracteres en mayúscula / It means that at least 3 characters must be uppercase)

ucredit=+3 (Significa que como máximo debe tener 3 caracteres en mayúscula / It means that a maximum of 3 characters should be uppercase)

Default values:

**password requisite pam\_cracklib.so retry=3 minlen=8 difok=3**

2FA (2-Factor Google Authentication): Para activarlo debe escribir en el terminal y seguir las instrucciones en pantalla. Si tiene alguna duda lea el [HowTO](#)

To activate it must write to the terminal and follow the onscreen instructions. If you have questions read the [HowTO](#)

google-authenticator

[Veracrypt](#). Para mayor información sobre cifrado con volúmenes de datos, lea el [HowTO](#) / For more information on encrypted data volumes, read the howto

### Ingreso de equipos a la red local y privilegios / Terminal income to the local network and privileges

El servidor DHCP, automáticamente, va arrendando direcciones IPs a todos los terminales que entren a su red local. El rango de arrendamiento lo establece el script `/etc/init.d/leases.sh`. Puede aumentar o disminuir este rango, editando el script. La política establecida por defecto es que todos los PCs, que el servidor DHCP les arrienda una dirección IP, entran a la red local denegados, incluidos en la acl `/etc/acl/blackdhcp.txt` con el formato:

`[a|b];dirección_mac;dirección_ip;nombre_host;fecha_introduccion.`

The DHCP server automatically goes leasing IP addresses to all terminals entering your local network. The range of lease established in `/etc/init.d/leases.sh` script. You can increase or decrease this range by editing the script. The default policy is that all PCs, the DHCP server will lease an IP address, enter the denied local network, including in the `/etc/acl/blackdhcp.txt` acl with the format:

`[a|b]; MAC address, IP address, host name, date introduction.`

Example:

`a;90:68:c3:20:00:00;192.168.0.102;USER;1432768764;`

Si pasados en 5 minutos el operador del servidor no autoriza la entrada a la red local de los terminales en la acl en `/etc/acl/blackdhcp.txt`, el servidor DHCP los bloqueará permanentemente y no les volverá a arrendar una dirección IP.

Para autorizar la entrada a la red local de terminales, edite la acl `/etc/acl/blackdhcp.txt` y **copie y pegue** el terminal autorizado a la acl `/etc/acl/macsllocal.txt` (ver tabla **ACL INCLUIDAS**). Para otorgarle altos privilegios a terminales (descargas, acceso ilimitado sin restricciones, etc) debe pegarlos en la acl `/etc/acl/macsunlimited.txt`.

If after 5 minutes the server operator does not authorize entry to the local network of terminals in the acl in `/etc/acl/blackdhcp.txt`, the DHCP server permanently blocked and will not return them to lease an IP address.

To authorize entry to the local network of terminals, edit the acl `/etc/acl/blackdhcp.txt` and copy and paste the acl `/etc/acl/macsllocal.txt` authorized the terminal (see table ACL INCLUDED). To grant high privileges to terminals (downloads, unlimited access without restrictions, etc) should paste them into the `/etc/acl/macsunlimited.txt` acl.

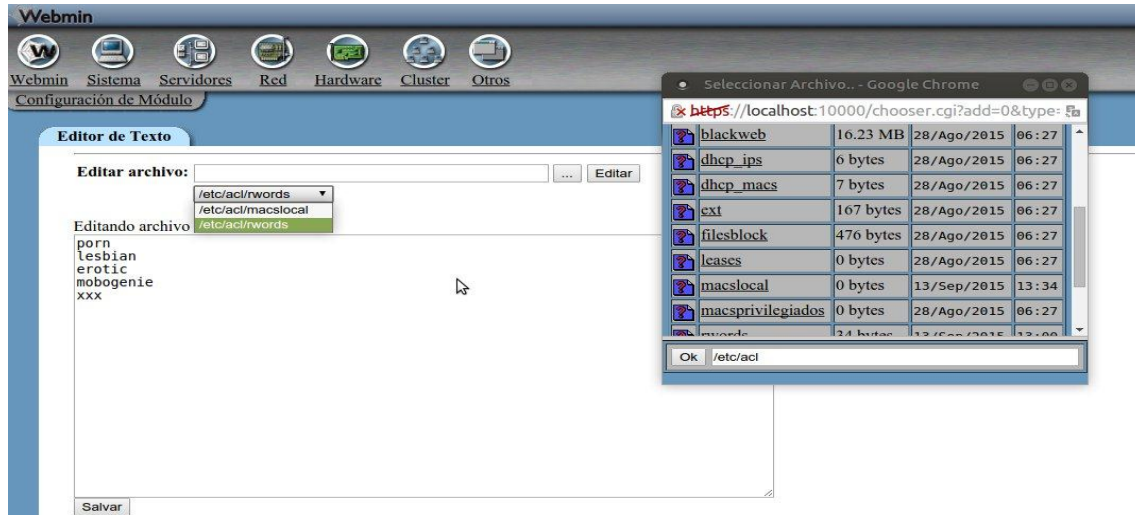
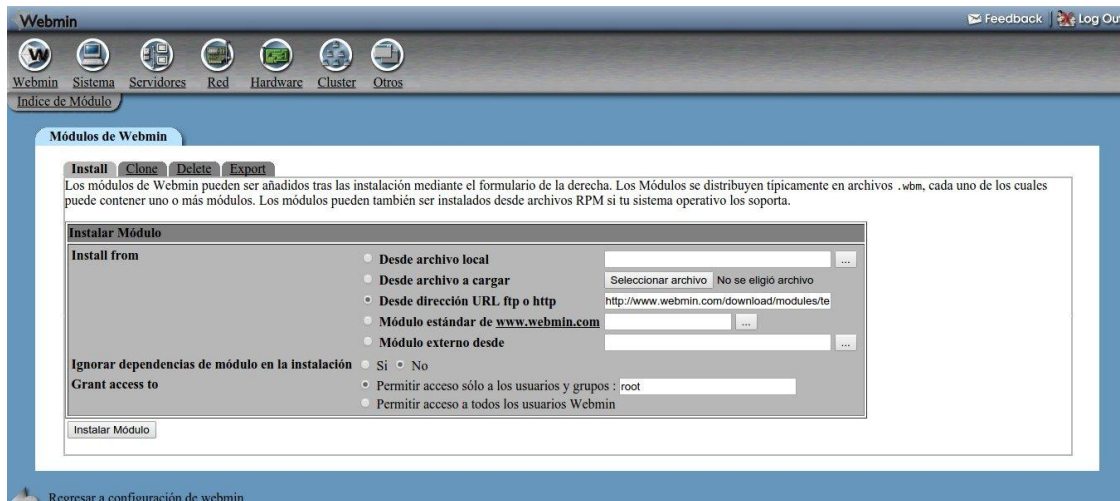
### **Important:**

La acl **macsunlimited** **NO PASA POR EL PROXY**, por tanto los equipos registrados en esta acl **pueden poner en riesgo la seguridad de su red local**. Sea precavido.

The acl mac unlimited bypasses the PROXY, so the teams registered in this acl can compromise the security of your local network at risk. Be cautious.

También puede editar las ACLs en Webmin, instalando el componente [Text-Editor](#) (Configuración de Webmin/Módulos de Webmin y cargar desde dirección URL ftp o http)

You can also edit the ACLs in Webmin, installing the Text-Editor component (Webmin Configuration / Webmin modules and load from URL ftp or http)



### Backup server configuration

El script **/etc/init.d/backup** se utiliza para realizar copias de seguridad. Por defecto guarda los archivos en la carpeta **/home/tu\_usuario/backup**.

Por defecto trae incluidos las rutas a los archivos de configuración esenciales. Puede editarlo para agregar más archivos o cambiar la ruta del backup hacia su destino preferido (soporte externo, la nube, etc). Puede cambiar la periodicidad de su ejecución en **crontab** (**sudo crontab -e**). Por defecto se ejecuta diariamente.

The **/etc/init.d/backup** script is used to perform backups. By default saves files in the **/home/your\_username/backup** folder.

By default it brings including routes to essential configuration files. You can edit it to add more files or change the path to your preferred destination backup (external support, cloud, etc). You can change the frequency of execution in crontab (sudo crontab -e). By default it runs daily.

#### VirtualBox Additions

Si usa una VM de VirtualBox para instalar GateProxy tenga presente que debe activar VBoxLinuxAdditions (Devices/Insert Guest Additions CD image...). Una vez hecho esto, le hará una pregunta de autoejecución, sin embargo no iniciará la instalación. Acceda a la carpeta VBOXADDITIONS\_5XXXXX/ dentro de "media" y ejecute:

If you use a VM VirtualBox to install GateProxy keep in mind that you must activate VBoxLinuxAdditions (Devices / Insert Guest Additions CD image ...). Once this is done, it will ask a question of self-executing, but will not start the installation. Access the VBOXADDITIONS\_5XXXXX / under "media" folder and run:

**sudo ./VBoxLinuxAdditions.run**

#### Puertos adicionales / additional ports

El firewall iptables, viene por defecto con los puertos esenciales abiertos y el resto cerrado. Si quiere incluir más puertos para su red local (SMTP/SSMTP, POP3/POP3S, IMAP/IMAPS, etc) edite el script (**sudo nano /etc/init.d/iptables.sh**), busque la regla PORTS RULES y descomente los puertos que quiera autorizar para su red local.

The iptables firewall, comes standard with the essential ports open and the rest closed. If you want to include more ports to your local network (SMTP / ssmtp, POP3 / POP3S, IMAP / IMAPS, etc) edit the script (sudo nano /etc/init.d/iptables.sh), locate the rule PORTS RULES and uncomment the ports you want to authorize to your local network.

#### Dirección MAC de administración / MAC address management

Si va a administrar el firewall iptables desde otro equipo que no sea el servidor, edite /etc/init.d/iptables.sh y reemplace la mac de ejemplo por la del PC administrador, el cual también tendrá acceso a ciertos puertos privilegiados.

If you're managing the iptables firewall from another computer than the server, edit **/etc/init.d/iptables.sh** and replace the mac example by the PC administrator, who also have access to certain privileged ports.

**sysadmin="b4:74:9f:93:00:00"**

#### PROXY

Durante la instalación, debe decidir con qué tipo de proxy quiere trabajar / During installation, you must decide what type of proxy wants to work:

**Proxy Transparent (NAT 8080) or Proxy No-Transparent (3128)**

Activacion del Proxy...

```
Seleccione 's' para activar Proxy Transparente (NAT 8080) con filtrado 443
Seleccione 'n' para activar Proxy No-Transparente (3128) con WPAD-PAC (s/n) █
```

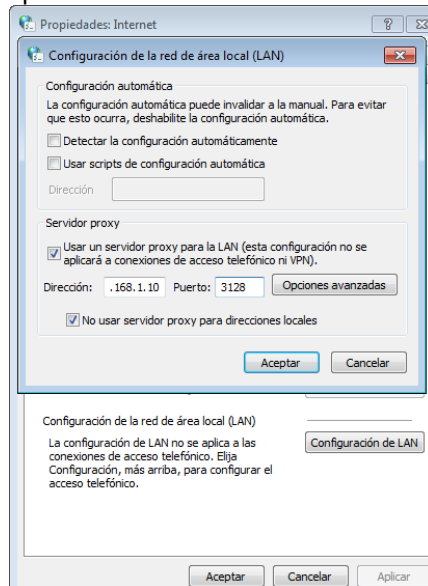
### Configuración del proxy en los navegadores de su red local / Proxy settings in browsers on your local network:

Hay 3 formas de hacerlo. Dejarlo por defecto (solo soportado por navegadores y sistemas operativos modernos), Manual y Automático

There are 3 ways to do it. Leave default (only supported by modern browsers and operating systems), Manual and Automatic

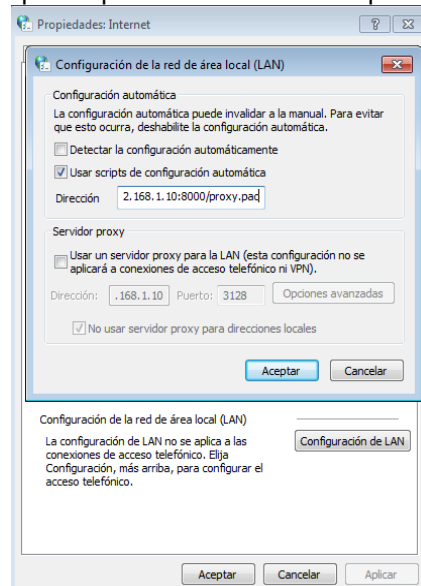
#### Manual

Example: 192.168.0.10: 3128



#### Automatic

Example: http://192.168.0.10:8000/proxypac



Tenga en cuenta que WPAD/PAC automático [es vulnerable](#) (se puede crear un [servidor wpad falso](#)) y no es compatible con todos los navegadores (Mozilla requiere adicionalmente servidor DNS para divulgar WPAD. Puede consultar la tabla de compatibilidad en [Browser-Support](#)).

Note that WPAD/PAC automatic is vulnerable (you can create a wpad fake server) and is not compatible with all browsers (Mozilla additionally requires DNS server to disclose WPAD. You can check the compatibility table in [Browser-Support](#)).

#### WPAD Control

FILES/DIR	RULES OR FILES
/etc/proxy	proxy.pac, wpad.da, wpad.dat
/etc/apache2/sites-enabled/	proxy.conf
/etc/apache2/ports.conf	#Listen 8000
/etc/init.d/leases.sh	#option option-252 code 252 = text; #option option-252 \"http://192.168.0.10:8000/proxy.pac\";
/etc/init.d/iptables.sh	8000

Si durante la instalación decidió cambiar el puerto del proxy no-transparente (por default 3128) debe elegir un puerto no reservado (consulte el [listado de puertos](#)).



If you chose during installation to change the port non-transparent proxy (by default 3128) must choose a port not reserved (see the [list of ports](#)).

#### Proxy Transparent NAT 8080 filter 443 (not recommended)

Un proxy transparente es un riesgo de seguridad, ya que la cache puede ser envenenada con peticiones redireccionadas. Para mayor información lea el post [Vulnerabilidad crítica de envenenamiento de caché en el servidor proxy Squid](#)

Tenga en cuenta que squid-cache no filtra conexiones https (puerto 443) en modo transparente, por tanto el tráfico https no aparecerá reflejado en los reportes Sarg, Sqstat, etc (solo http). Tampoco aplican reglas de squid-cache, como bloqueos de extensiones y otros tipos de filtrado, ya que https es cifrado. Para mayor información consulte el post [Proxy](#)

A transparent proxy is a security risk, since the cache can be poisoned with redirected requests. For more information read the post critical cache poisoning vulnerability in Squid proxy server

Note that squid-cache does not filter connections https (port 443) in transparent mode, so the traffic https not be reflected in the Sarg, SqStat, etc (only http) reports. Nor rules apply squid-cache, and locks extensions and other types of filtering, since https is encrypted. For more information see the post Proxy

#### Transparent Proxy Filter 443

El filtrado 443, consiste en permitir el paso de IPs https en la acl whiteip.txt y luego el firewall cierra el puerto 443. El uso de esta regla puede hacer colapsar su sistema, por la cantidad de ips que tiene que validar iptables. Usela con moderación

The filter 443 is to allow the passage of IPs https acl in whiteip.txt and then the firewall closes the port 443. Using this rule can bring down your system, the amount of ips you have to validate iptables. Use it sparingly

#### Blackip for Ipset

El script `/etc/init.d/blackip.sh` es el encargado de actualizar las bases de datos [geoip](#) y las Blacklist IPS para bloquear con [iptables/ipset](#).

IPset no viene activo por defecto, ya que este filtrado consume muchos recursos. Para activar la regla **ipset**, edite `/etc/init.d/iptables.sh`:

The `/etc/init.d/blackip.sh` script is responsible for updating the data bases geoip and IPS Blacklist to block with iptables/ipset.

Ipset is not enabled by default, since this filter consumes many resources. To activate the ipset rule, edit `/etc/init.d/iptables.sh`:

Si va a utilizar solamente la ACL `/etc/acl/blackip.txt`

If you are using only the ACL `/etc/acl/blackip.txt`

```
# BLACKZONE (select country to block and ip/range)
# http://www.ipdeny.com/ipblocks/
ipset=/sbin/ipset
$ipset -F
$ipset -N -! blackzone hash:net maxelem 1000000

for ip in $(cat /etc/acl/blackip.txt); do
```

```
$ipset -A blackzone $ip
done
$Iptables -A FORWARD -m set --match-set blackzone dst -j DROP
$Iptables -t mangle -A PREROUTING -m set --match-set blackzone src -j DROP
```

Si adicionalmente va a bloquear países enteros, cambie una línea por otra. En el ejemplo siguiente se muestra la línea bloqueando china y Rusia. Puede agregarle más países:

If additionally will block entire countries, change a line on the other. In the following example, the line blocking China and Russia is shown. You can add more countries

```
for ip in $(cat /etc/zones/{cn,ru}.zone /etc/acl/blackip.txt); do
```

Si no cuenta con muchos recursos de sistema, y activó el proxy no-transparente, se recomienda utilizar solamente la regla de bloqueo de squid (viene activa por defecto):

If you do not have many resources system and activate the non-transparent proxy, we recommend using only the blocking rule squid (is enabled by default):

```
acl whiteip dst "/etc/acl/whiteip.txt"
acl no_ip url_regex -i [0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}
http_access allow whiteip
http_access deny no_ip
```

La regla anterior bloquea por defecto todas las IPs, y solo deja pasar las IPs que se encuentren en la ACL **/etc/acl/whiteip.txt**. Puede editar manualmente esta ACL e incluirle las IPs adicionales o rangos CIDR que quiera excluir.

The above default rule blocks all IPs, and only let the IPs that are in the ACL **/etc/acl/whiteip.txt**. You can manually edit the ACL and include additional IPs or CIDR ranges you want to exclude.

#### Importante sobre filtrado por IP:

El filtrado por IPs en un proxy transparente no garantiza la protección de su red local. Por oytro lado, las direcciones usadas por [youtube.com](https://www.youtube.com), son las mismas que utilizan otros servicios de Google, por tanto, si bloquea estas IPs, puede comprometer los demás servicios de Google.

Tenga en cuenta que muchas de estas IPs son dinámicas y pueden cambiar sin previo aviso, por lo que deberá estar revisando constantemente los rangos autorizados en la acl **whiteip (aquí también debe incluir el rango de la red local)**

El abuso de esta regla puede traer como consecuencia la ralentización de su servidor. Para mayor información visite el proyecto [Blackip](#)

IP filtering by a transparent proxy does not guarantee protection of your local network. By oytro hand, the addresses used by youtube.com are the same using other Google services, therefore, if you block these IPs may compromise other Google services.

Note that many of these IPs are dynamic and can change without notice, so it must be constantly reviewing the acl whiteip authorized ranges (here must also include the range of the local network)

Abuse of this rule may result in slowing down your server. For more information visit the project [Blackip](#)

**DNS-LOCAL (Experimental)**

Gateproxy ofrece instalar servidor DNS-LOCAL ([dnsmasq](#)). Su uso demandará gran cantidad de recursos de su sistema

Si después de instalado, quiere desactivar DNS-LOCAL para cambiar a DNS-PUBLIC debe modificar los siguientes archivos de configuración:

Gateproxy offers to install DNS-LOCAL server ([dnsmasq](#)). Its use will require large amount of system resources

If after installation, you want to disable DNS-LOCAL to change to DNS-PUBLIC must modify the following configuration files:

CONF /SCRIPT	REGLAS / RULES
<b>/etc/init.d/iptables.sh</b>	dns="8.8.8.8 8.8.4.4"
<b>/etc/squid/squid.conf</b>	dns_nameservers 8.8.8.8 8.8.4.4 # tcp_outgoing_address 192.168.0.10 # udp_outgoing_address 192.168.0.10
<b>/etc/init.d/leases.sh</b>	ServDNS=8.8.8.8,8.8.4.4
<b>/etc/dnsmasq.conf</b>	# server=/localnet/192.168.0.10 server=8.8.8.8 server=8.8.4.4 # Use dnsmasq specific hosts file and resolv #no-hosts #no-resolv resolv-file=/etc/resolv.dnsmasq.conf

**SAMBA (COMPARTIDA PUBLICA, PAPELERA DE RECICLAJE Y AUDITORIA) (PUBLIC SHARED, RECYCLE BIN AND AUDIT)**

El intercambio de archivos en redes locales es esencial. Para evitar el uso de dispositivos usb (y el malware vía usb) recomendamos crear una “Carpeta Compartida Pública” a la cual solo tendrán acceso los integrantes de la red local.

Por defecto la “Carpeta Compartida Pública” tiene restringido el almacenamiento de ciertos archivos (\*.mp3/\*.wmv/\*.wma/\*.mpg/\*.3gp/\*.mpeg/\*.mkv/\*.rmvb/\*.flv/\*.avi/., etc)

Si desea modificarlo, edite **/etc/samba/smb.conf** y al final se encuentran las restricciones.

La Papelera de reciclaje (directorio recycle) se encuentra oculta dentro de “Carpeta Compartida Pública”. Ahí se almacenarán los archivos eliminados por los usuarios y con la fecha de la eliminación. Está programada para ser vaciada semanalmente (archivos que tengan más de 7 días). Si quiere modificarlo, acceda al crontab (**sudo crontab -e**) y modifíquelo según sus necesidades

The file sharing on local networks is essential. To avoid using USB devices (and malware via USB) recommend creating a "Public Shared Folder" to which only members have access to the local network.

By default the "Shared Folder Public" has restricted storage of certain files (\*.mp3/\*.wmv/\*.wma/\*.mpg/\*.3gp/\*.mpeg/\*.mkv/\*.rmvb/\*.flv / \*.avi /., etc)

If you want to modify, edit /etc/samba/smb.conf and end are restrictions.

The Recycle Bin (recycle directory) is hidden within "Public Shared Folder". That deleted by users and the date of removal files are stored. It is scheduled to be emptied weekly (files with more than 7 days). If you want to modify, access the crontab (sudo crontab -e) and modify it according to your needs

```
@weekly find /home/tu_usuario/compartida/recycle/* -mtime +7 -exec rm {} \;
```

Para el seguimiento de la “Carpeta Compartida Pública”, puede acceder a los registros en: <http://192.168.0.10:11200>, que muestra fecha y hora de eliminación, modificación, lectura, de directorios y archivos.

En el siguiente ejemplo hemos creado un archivo llamado **prueba.txt**. El log muestra los registros de creación, visualización y borrado de este archivo:

To track the "Public Shared Folder", you can access the records in: <http://192.168.0.10:11200>, showing date and time of deletion, modification, reading, directories and files.

In the following example we have created a file called test.txt. The log shows records creation, viewing and deleting this file:

```
Feb 6 17:40:19 localhost smbd_audit: 192.168.0.41[user|compartida|pwrite|ok| prueba.txt
```

#### Nomenclatura de / Nomenclature of: **smbdaudit.log**

mkdir	Creación de carpetas/directorios	Creating folders / directories
rmdir	Borrado de carpetas/directorios	Deleting folders / directories
pread	Archivos abiertos (lectura)	open files (reading)
pwrite	Nuevos ficheros (creados o subidos)	New files (created or uploaded)
rename	Renombrado de archivos	Renaming files
unlink	Borrado de archivos	Deleting files

Por defecto estos registros se actualizan diariamente. Si quiere deshabilitar o modificar esta opción (puede hacerlo en tiempo real), ingrese al crontab y elimine o modifique la línea: **@daily grep smbd\_audit /var/log/syslog > /etc/smbdaudit/smbdaudit.log**

Para evitar que este log se inunde de registros, por defecto es vaciado semanalmente por el crontab. No se recomienda que modifique esta opción.

```
@weekly cat /dev/null > /etc/smbdaudit/smbdaudit.log
```

Igualmente puede consultar todos los registros en **/var/log/syslog**

By default these records are updated daily. If you want to disable or modify this option (you can do in real time), enter the crontab and remove or modify the line:

```
@daily grep smbd_audit/var/log/syslog> /etc/smbdaudit/smbdaudit.log
```

To prevent this log record flooding, default is emptied weekly by the crontab. It is not recommended to modify this option.

```
@weekly cat /dev/null> /etc/smbdaudit/smbdaudit.log
```

You can also see all records in **/var/log/syslog**

### **CONTROL DE PUERTOS USB**

Protege su servidor de conexiones usb no autorizadas, creando una lista blanca con los dispositivos usb que quiera autorizar y bloquea el resto, dejando un log con registro de la intrusión en **/var/log/blackusb.log**

Generar lista de dispositivos usb autorizados (whitelist)

```
sudo /etc/init.d/blackusb gen
```

Eliminar lista de dispositivos usb autorizados (whitelist)

```
sudo /etc/init.d/blackusb del
```

Activar/Desactivar bloqueo

**sudo /etc/init.d/blackusb on (off)**

Mostrar lista de dispositivos usb conectados

**sudo /etc/init.d/blackusb show**

Apagar el servidor cuando se conecte una usb ilegal, descomente la línea:

**'poweroff'**

Para mayor información visite <https://github.com/maravento/blackusb>

Protect your server from unauthorized USB connections, creating a white list of USB devices you want to allow and blocks the rest, leaving a log record of the intrusion  
**/var/log/blackusb.log**

Generate list of authorized USB devices (whitelist)

**sudo /etc/init.d/blackusb gen**

Delete list of authorized USB devices (whitelist)

**sudo /etc/init.d/blackusb del**

Enable / Disable Lock

**sudo /etc/init.d/blackusb on (off)**

Show list of USB devices connected

**sudo /etc/init.d/blackusb show**

Shut down the server when an illegal usb, uncomment the line is connected:

**'Poweroff'**

For more information visit <https://github.com/maravento/blackusb>

## SECURITY PACK

Algunos paquetes incluidos en este Pack no se encuentran activos por default o se encuentran parcialmente activos (Fail2ban, Mod Security, OWASP, Evasive y Rootkit checkers), ya que para manejarlos, el usuario debe tener conocimientos avanzados. Si no está seguro, deje los valores por default.

Si quiere activarlos, realice los siguientes cambios:

Mod Security: **Edite /etc/modsecurity/modsecurity.conf**, busque, **SecRuleEngine** y cámbie **DetectionOnly** a **On**.

ModSecurity genera muchos falsos positivos y puede experimentar bloqueos (127.0.0.1 o localhost) y ralentización en la navegación. Para solucionarlo, deberá supervisar los logs de Apache (**tail /var/log/apache2/error.log**) para hacer los cambios que se sugieran.

Puede monitorizar gráficamente el módulo de seguridad (ModSecurity), utilizando el aplicativo [Waf-file](#), (no incluido). Consulte la [documentación](#)

Some packages included in this pack are not active by default or are partially active (Fail2ban, Mod Security, OWASP, Evasive and Rootkit checkers) as to handle, the user must have advanced knowledge. If you are unsure, leave the default values.

If you want to activate, make the following changes:

Mod Security: Edit **/etc/modsecurity/modsecurity.conf**, look, **SecRuleEngine** and change **DetectionOnly** to **On**.

ModSecurity generates many false positives and may experience blockages (127.0.0.1 or localhost) and deceleration in navigation. To fix this, you must monitor Apache logs (**tail /var/log/apache2/error.log**) to make the suggested changes.

You can graphically monitor the security module (ModSecurity) using the application [Waf-file](#), (not included). See the [documentation](#)

Mod\_evasive viene con una configuración predeterminada que excluye localhost. Si quiere incluir localhost, edite los archivos:

**/etc/apache2/mods-available/evasive.conf**

**/etc/apache2/mods-enabled/evasive.conf**

Y comente la línea: **DOSWhitelist 127.0.0.1**

Tenga en cuenta que este cambio puede afectar a algunos aplicativos webs que tenga alojados en su servidor, como sqstat, sarg, etc.

Mod\_evasive comes with a default configuration that excludes localhost. If you want to include localhost, edit the files:

**/etc/apache2/mods-available/evasive.conf**

**/etc/apache2/mods-enabled/evasive.conf**

And comment out the line: **DOSWhitelist 127.0.0.1**

Note that this change may affect some web applications that have hosted on your server, as SqStat, sarg, etc.

Fail2ban viene por defecto con algunas reglas básicas activas, para la protección de apache, ssh. Para agregar más protección, edítelo **/etc/fail2ban/jail.conf** y autorize (cambiar **false** por **true**) las jaulas que necesite o agregue nuevas.

Cada cambio (**false** a **true**) que realice en una jaula, debe tener su filtro y log configurado.

Fail2ban comes by default with some basic active rules for the protection of apache, ssh. To add more protection, edit **/etc/fail2ban/jail.conf** and authorizes (change **false** to **true**) cages need or add new.

Each change (**false** to **true**) to perform in a cage, you must have your filter and log set.

#### NIPS/NIDS in Docker (Experimental)

Este paquete instala [NIPS/NIDS Snort](#) con Barnyard2, PuledPork, Snorby, en un [Docker](#), para un mejor control de intrusiones (detección y prevención). Para mayor información visite el sitio del proyecto:

<https://github.com/amabrouki/snort>

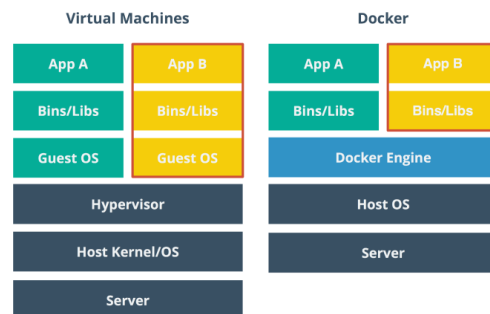
[HowTO para actualizar el Okicode](#)

This package installs [NIPS/NIDS Snort](#) with Barnyard2, PuledPork, Snorby in a [Docker](#), for better control (Intrusion detection and prevention).

For more information visit the project site:

<https://github.com/amabrouki/snort>

[Howto to update the Okicode](#)



## CONTENT OF GATEPROXY

## DIRECTORIOS/ DIRECTORIES

<b>proxy</b>	/etc/proxy	Contiene los archivos de autoconfiguración del proxy wpad.dat, proxy.pac y wdad.da It contains files proxy auto configuration wpad.dat, proxy.pac and wdad.da
<b>acl</b>	/etc/acl	Contiene las ACLs de sistema Contains ACLs system
<b>scripts</b>	/etc/init.d	Contiene los scripts utilizados por Gateproxy It contains the scripts used by gateproxy

## SCRIPTS

<b>script</b>	<b>path</b>	<b>task</b>	<b>Work</b>
<b>backup</b>	/etc/init.d	week	Realiza backup de los archivos de configuración del servidor en el path <b>/home/username/backup</b> . Make backup of the server configuration files in the path <b>/home/username/backup</b> .
<b>cleaner.sh</b>	/etc/init.d	daily	Elimina temporales, encryptable.zone, Thumbs.db, informes de crash antiguos, limpia la ram y la swap Delete temporary, encryptable.zone, Thumbs.db, old crash reports, clean the ram and swap
<b>geoip.sh</b>	/etc/init.d	week	Descarga la base de datos ntopng Database download ntopng
<b>iptables.sh</b>	/etc/init.d	10 min	Reglas de firewall iptables Iptables firewall rules
<b>leases.sh</b>	/etc/init.d	10 min	Controla el servidor DHCP DHCP server controls
<b>lock.sh</b>	/etc/init.d	start	Evita que la ejecución de varias instancias de un mismo script Prevents the execution of multiple instances of the same script
<b>servicesreload.sh</b>	/etc/init.d	10 min)	Vigila los servicios esenciales del servidor. (isc-dhcp-server, Squid, Apache2, ntopng, redis-server, etc). Si alguno cae, el script lo levanta automáticamente Watch essential services server. (Isc-dhcp-server, Squid, Apache2, ntopng, redis-server, etc). If one goes down, the script automatically lifts
<b>updatehour.sh</b>	/etc/init.d	start	Actualiza y sincroniza la hora del servidor Update and synchronize the server time
<b>vm</b>	/etc/init.d	start	Inicia o detiene las VMs que tenga en su servidor (Virtualbox). Edite /etc/init.d/vm y



			reemplaza VMNAME="my_vm_name" por el nombre de su máquina virtual Starts or stops the VMs you have on your server (Virtualbox). Edit /etc/init.d/vm and replace VMName = "my_vm_name" by the name of your virtual machine
<b>blackweb.sh</b>	/etc/initd	week	Actualiza la lista de dominios bloqueados. Para mayor información visite el proyecto <a href="#">blackweb</a> Updates the list of blocked domains. For more information visit the project blackweb
<b>blackip.sh</b>	/etc/init.d	week	Actualiza la lista de IPs bloqueadas para Ipset. Para mayor información visite el proyecto <a href="#">Blackip</a> Updates the list of blocked IPs for ipset. For more information visit the project Blackip
<b>whiteip.sh</b>	/etc/init.d	week	Actualiza la lista blanca de IPs para Squid. Para mayor información visite el proyecto <a href="#">whiteip</a> Updates the whitelist to Squid. For more information visit the project whiteip
<b>blackusb</b>	/etc/init.d	start	Protege su servidor de dispositivos usb no autorizados. Para mayor información visite el proyecto <a href="#">blackusb</a> Protect your server from unauthorized USB devices. For more information visit the project blackusb

## ACLS

ACL (.txt)	path	used in	Work
<b>blackip</b>	/etc/acl	Ipset/iptables	Lista negra de IPs para IPSET IPs blacklist
<b>blackdhcp</b>	/etc/acl	Iptables/dhcp	Contiene todos los terminales que entran por defecto bloqueados a su red local. Los terminales entran bloqueados por default, hasta que el operador los saque de esta lista It contains all terminals blocked entering default to your local network. Enter terminals blocked by default, until the operator's kick this list
<a href="#">blackstring</a>	/etc/acl	iptables	Contiene strings para bloquear programas anónimos (ultrasurf, etc). Para mayor información visite <a href="#">Blackstring</a> . It contains strings to block anonymous programs (ultrasurf, etc). For more information visit Blackstring.

<b>whiteip</b>	/etc/acl	Ipset/iptables/squid	Lista blanca de IPs para Squid y Iptables Whitelist for Squid and Iptables
<b><a href="#">blackweb</a></b>	/etc/acl	Squid	Lista negra de dominios. Para mayor información visite <a href="#">blackweb</a> Blacklist domains. For more information visit blackweb
<b>blackdomains</b>	/etc/acl	Squid	Lista negra de dominios para el usuario. Para mayor información visite <a href="#">blackweb</a> Blacklist domains for user. For more information visit blackweb
<b>dhcp_ips</b>	/etc/acl	dhcp/iptables	ACL de sistema y no debe ser manipulada ACL system and must not be manipulated
<b>dhcp_macs</b>	/etc/acl	dhcp/iptables	ACL de sistema y no debe ser manipulada ACL system and must not be manipulated
<b>blackext</b>	/etc/acl	squid	Lista negra de extensiones <b>url_regex</b> blacklist of extensions <b>url_regex</b>
<b>blackmime</b>	/etc/acl	squid	Lista negra de extensiones <b>mime_type</b> blacklist of extensions <b>mime_type</b>
<b>macslocal</b>	/etc/acl	dhcp/iptables	ACL que contiene las direcciones macs/ips de la red local ACL containing macs/ips addresses of local network
<b>macsunlimited</b>	/etc/acl	dhcp/iptables	ACL que contiene las direcciones macs/ips de la red local sin restricciones ACL containing macs/ips addresses of local network Without restrictions
<b>blackwords</b>	/etc/acl	squid	Lista negra de palabras. Esta ACL puede generar falsos positivos. Blacklist words. This ACL may produce false positives.
<b>whitedomains</b>	/etc/acl	squid	Lista blanca de dominios para el usuario. Para mayor información visite <a href="#">blackweb</a> Whitelist domains for user. For more information visit blackweb
<b>ipsreserved</b>	/etc/acl	iptables	Contiene ips anti-spoofing. ACL de sistema y no debe ser manipulada Contains IPs anti-spoofing. ACL system and must not be manipulated.

## PROBLEMAS CONOCIDOS/ KNOWN ISSUES

PROBLEM	SOLUTION
<b>sudo service networking restart</b> no funciona / does not work	Visit <a href="#">Restore Networking</a>
Las interfaces de red entran en modo promiscuo Network interfaces come into	Desinstale/ uninstall tcpdump y wireshark

promiscuous mode	
<b>DHCP Error Ip duplicate</b>	Modifique las ACLs macslocal y macsunlimited y cambie las direcciones IPs asignadas a los terminales, por fuera del rango DHCP modify ACLs macslocal and macsunlimited and change the IP addresses assigned to terminals outside the DHCP range
<b>DNS no resuelve</b> Example: http://localsite:8090	Modifique la configuración de los navegadores y marque la opción: <b>"no usar servidor proxy para direcciones locales"</b> Modify browser settings and check the option: <b>"Do not use proxy server for local addresses"</b>
<b>fail2ban.filter : ERROR Unable to open /var/log/squid/access.log and /var/log/squid/auth.log</b>	<b>sudo service fail2ban stop &amp;&amp; sleep 3 &amp;&amp; sudo service fail2ban start.</b> Aumente el número de jaulas (default 256) Increases the number of cages (default 256) /proc/sys/fs/inotify/max_user_instances Revise jail.conf ya que las jaulas pueden estar mal configuradas Check jail.conf as cages may be misconfigured
<b>fail2ban.actions.action: ERROR iptables (etc) fail2ban.jail: INFO Jail 'apache-overflows' stopped log: /var/log/fail2ban.log</b>	No utilice / Do not use: <b>sudo service fail2ban restart</b> Utilice:/ use: <b>sudo service fail2ban stop &amp;&amp; sleep 3 &amp;&amp; sudo service fail2ban start.</b>
<b>E: Sub-process /usr/bin/dpkg returned an error code (1)</b>	Ingrese a /var/lib/dpkg/info y elimine todas las referencias al paquete (sudo rm -rf paquete) Enter to /var/lib/dpkg/ info and delete all references to the package (sudo rm -rf package) sudo rm /var/cache/debconf/*.dat
<b>VBoxNetFlt: Failed to allocate packet buffer, dropping the packet</b>	<b>BUG</b> <a href="https://code.launchpad.net/~mitya57/ubuntu/precise/virtualbox/4.1.12-dfsg-2ubuntu0.3/+merge/153346">https://code.launchpad.net/~mitya57/ubuntu/precise/virtualbox/4.1.12-dfsg-2ubuntu0.3/+merge/153346</a>

### VM/ISO/Distro

Puede crear su propia VM (vdi) con virtualbox o una imagen ISO de **GateProxy LiveCD** con Systemback o gdiskump, ambas incluidas en **Gateproxy**. Para [Systemback](#), consulte [HowTO](#)

You can create your own VM (VDI) with virtualbox or LiveCD ISO image GateProxy with Systemback or gdiskump, both included in Gateproxy. To Systemback, see the tutorial [HowTO](#)

Agradecemos a todos aquellos que, directa o indirectamente, contribuyeron con la realización de este proyecto / We thank all those who directly or indirectly contributed to the realization of this project

<http://www.novatoz.com>  
<http://www.alterserv.com/foros/index.php>  
<http://www.pello.info>  
<https://ubuntu-mate.org/>  
<http://www.ubuntu.com/>  
<http://www.debian.org>  
<http://www.netfilter.org/>  
<http://www.squid-cache.org/>  
<https://www.isc.org/downloads/dhcp/>  
<https://www.apache.org/>  
<http://samm.kiev.ua/>  
<http://www.webmin.com/>  
<http://php.net/>  
<http://www.freefilesync.org/>  
<https://launchpad.net/systemback>  
<http://www.microsoft.com/>  
<http://bleachbit.sourceforge.net/>  
<https://www.perl.org/>  
<http://www.x.org/wiki/>  
<http://iptraf.seul.org/>  
<https://nmap.org>  
<http://qlx-dock.org/>  
<http://qparted.org/>  
<http://ubuntu-tweak.com/>  
<https://www.python.org/>  
<https://www.openssl.org/>  
<http://www.postfix.org/>  
<http://en.wikipedia.org/>  
<http://sourceforge.net/projects/sarg/>  
<http://www.thekelleys.org.uk/dnsmasq/doc.html>  
<http://www.atareao.es/ubuntu/acelerando-linux/>  
<http://openjdk.java.net/>  
<https://www.virtualbox.org/>  
<https://www.securitybydefault.com>  
<https://www.winrar.es/>  
<http://www.winzip.com/>  
<http://waf-fle.org/>  
<http://stackoverflow.com/>  
<http://blog.desdelinux.net/>  
<http://www.linuxirun.com/>  
<https://www.teamviewer.com/es/>  
<http://www.ntop.org/>  
<http://www.jose-linares.com>  
<http://dasubipar.blogspot.com>  
<http://www.ioanemarti.com>  
<http://arpon.sourceforge.net/>  
<https://github.com/da667/Autosnort>  
<https://github.com/SpiderLabs>  
<https://github.com/amabrouki>  
<https://github.com/firehol>  
<https://github.com/trpt>  
<https://www.bestvpn.com>  
<http://wiki.syspass.org/es/instalar>  
<https://klaver.it/linux/sysctl.conf>  
<http://www.hackplayers.com>  
<http://www.redeszone.net/>  
<https://www.linux.com/>  
<https://opensourceinside.blogspot.com.co>  
<https://unix4lyfe.org/darkstat/>  
<https://goaccess.io/>

© 2016 [gateproxy.com](http://gateproxy.com).