MARAVENTO STUDIO

GATEPROXY

GATEPROXY

Instalación de GateProxy Server -Home & Business-

v1.0 Alpha

gateproxy.com

QUÉ ES GATEPROXY

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

El script de instalación y configuración es totalmente automatizado con una interacción mínima durante proceso. Puede ser personalizado y escalado de acuerdo a las necesidades del administrador u organización, sin que esto implique una excesiva intervención, reduciendo así la curva de aprendizaje.

Entre sus múltiples herramientas, se pueden mencionar un Proxy Cache, un Firewall, y muchas otras aplicaciones, en su mayoría libres, las cuales le brindan a su hogar u organización un nivel de seguridad y administración estándar para la protección y administración de las conexiones.

QUÉ NO ES GATEPROXY

Un nodo proxy para ocultar conexiones (similar a Tor, Ultrasurf, Psiphon, etc.)

LICENCIA

EXENCION DE RESPONSABILIDAD:

El script de instalación puede dañar su sistema si se usa incorrectamente. Úselo bajo su propio riesgo.

REQUISITOS MINIMOS:

GNU/Linux: Ubuntu 16.04.x (Xenial Xerus) LTS x64
Procesador: Intel compatible 1x GHz
RAM: 4GB
DD: 200 GB
Display: 1024 x 768 128Mb Video
Install: DVD/USB
Internet: Alta velocidad (recomendado)
Bash: 4.3x (verifique con echo $BASH_VERSION)
Desktop: Mate (Opcional)
HowTo: HowTo install Ubuntu/Debian with Mate Desktop

IMPORTANTE ANTES DE USAR

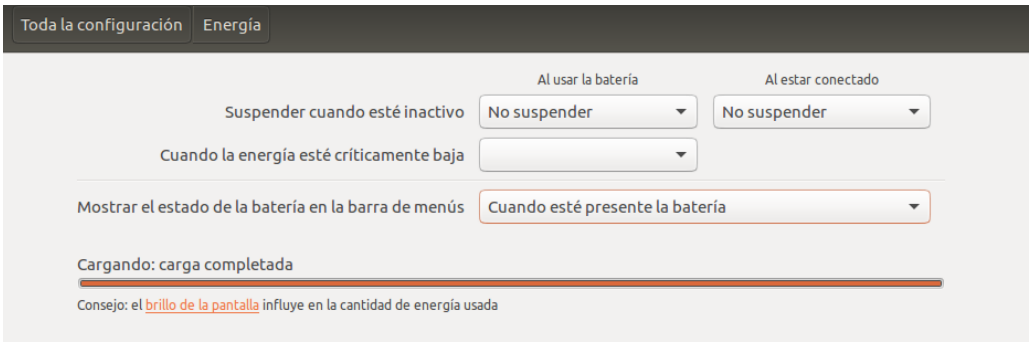
Nota: Algunas de las siguientes medidas no están incluidas en este proyecto

Haga copia de seguridad de sus archivos esenciales
Actualice su sistema y desinstale las app no 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
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); 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

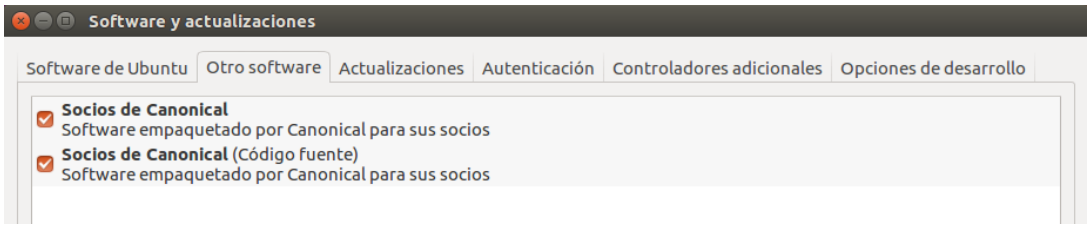
deshabilitarla; hacer copia de seguridad de su arranque con boot-repair u otra solución; auditar regularmente su servidor y red local con lynis, Sparta, o cualquier otra herramienta de su manejo, protegerse de los ataques de amplificación DNS con dns-iptables-rules y de los ataques DDoS con Bohatei y 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.), o cualquier otra medida que considere para prevenir intrusiones y mantener su sistema protegido
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
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

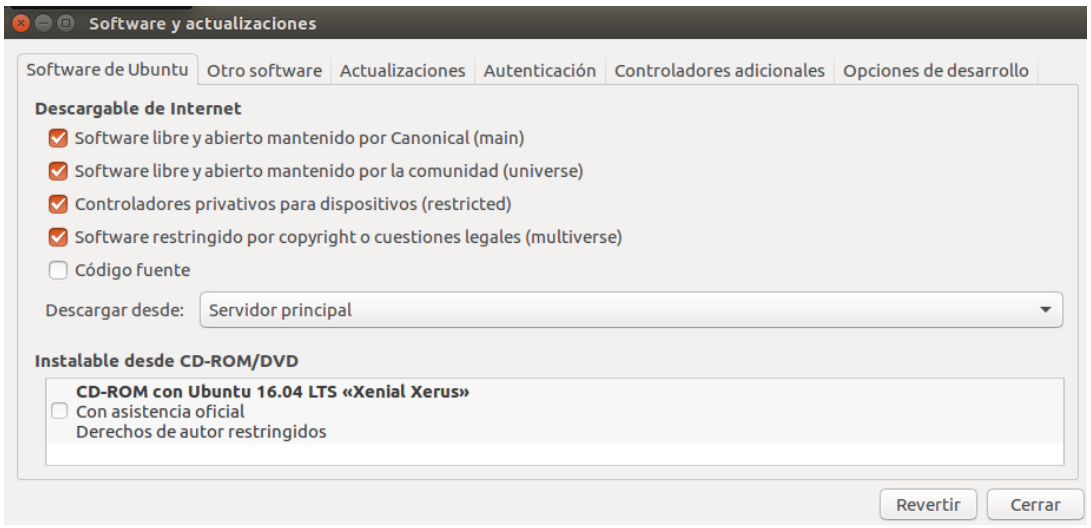
PRE-INSTALACION

Se recomienda que durante la instalación desactive el protector de pantalla y la energía



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





INSTALACION

Abra el terminal e instale las dependencias

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

Descargue el proyecto Gateproxy y ejecútelo **SIN PRIVILEGIOS "SUDO"**

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

VERIFICACION DE SISTEMA OPERATIVO

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.

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

VERIFICACION DE INTERFACES DE RED CON FORMATO 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

Nota: Este procedimiento solo aplica para interfaces ETH (no aplica para interfaces virtuales o WLan)
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.

```
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
```

Después de reiniciar, ejecute nuevamente el script de gateproxy

```
gateproxy/gateproxy.sh
```

Inicio de la instalación de Gateproxy

Al ejecutar el script le saldrá la pantalla de bienvenida

```
Bienvenido a la instalacion de GateProxy Home and Business v1.0 Alpha


Requisitos Mínimos:
GNU/Linux:    Ubuntu 16.04.x (Xenial Xerus) LTS x64
Procesador:   Intel compatible 1x GHz
RAM:          4GB
DD:           200 GB
Display:      1024 x 768 128Mb Video
Internet:     High Speed (esencial)
Desktop:      Mate (opcional)
Dependencias: sudo apt-get -y install git apt dpkg


Exención de responsabilidad:
Este script puede dañar su sistema si se usa incorrectamente.
Para mayor información, visite gateproxy.com y lea el HowTO


Presione ENTER para iniciar o CTRL+C para cancelar
```

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.

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

Elimine la carpeta gateproxy, descargue el proyecto nuevamente y ejecútelo

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

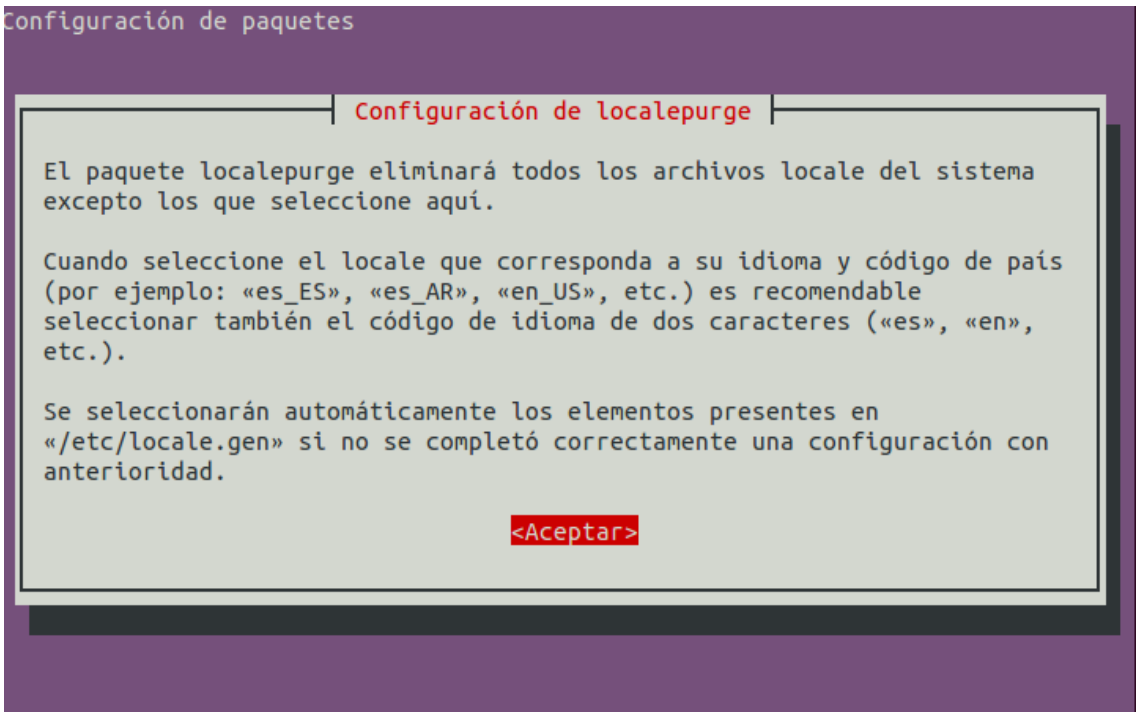
Si la suma coincide, el instalador le preguntará si quiere cambiar los parámetros por defecto que trae el proyecto GateProxy.

```
Parametros del servidor:
ip-port: 192.168.1.10:3128  mask: 255.255.255.0 or /24  dhcp: eth1
dns: 8.8.8.8,8.8.4.4  localnet: 192.168.1.0  broadcast: 192.168.1.255

Desea cambiar estos parametros? (s/n)
```

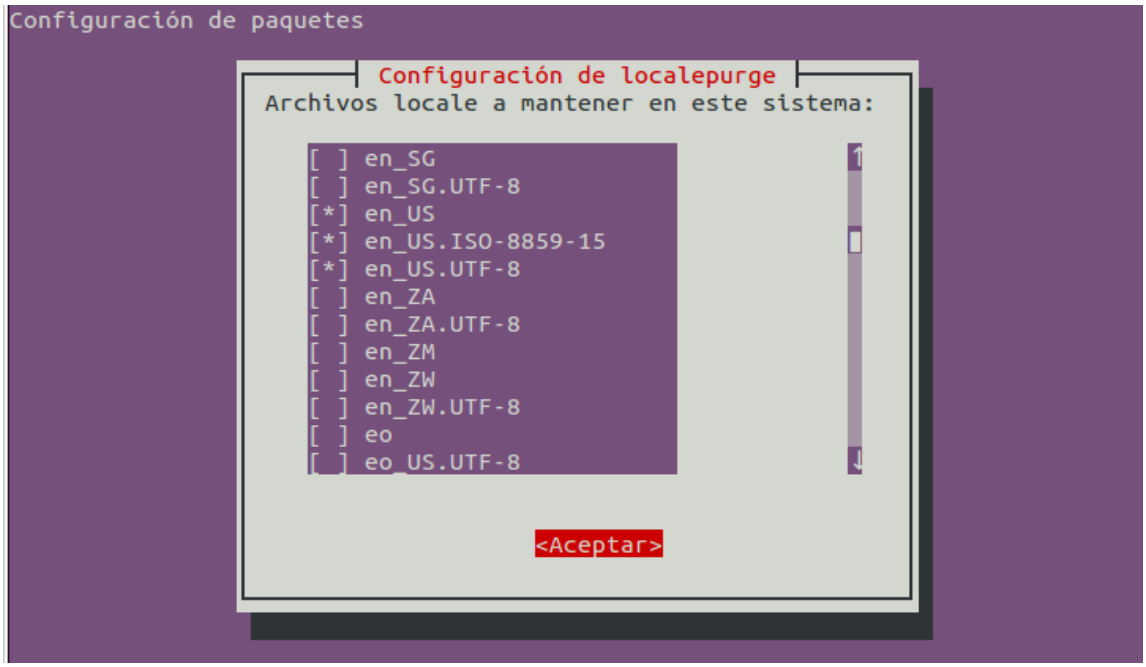
Al finalizar la configuración de los parámetros de red de su servidor, comenzará la instalación de paquetes. Asegúrese de tener una conexión de internet estable y de alta velocidad.

Instalación de Paquetes Esenciales

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).



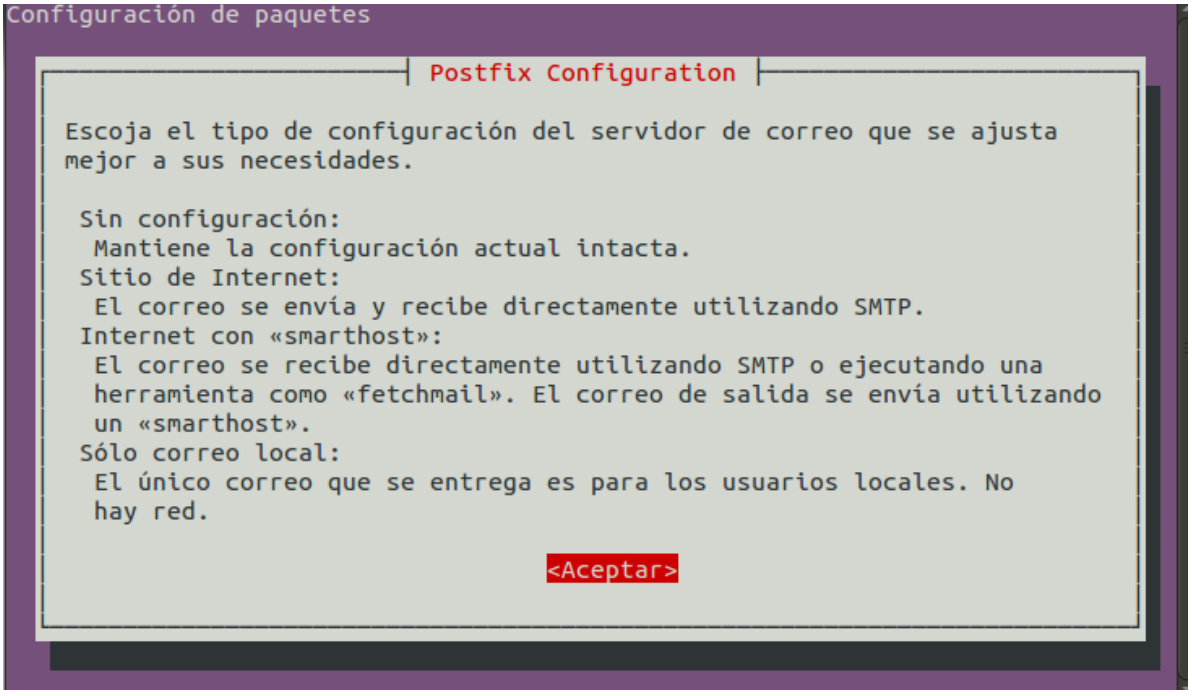
En la siguiente pantalla pulse "**Aceptar**" (Puede marcar más idiomas –no recomendado-)



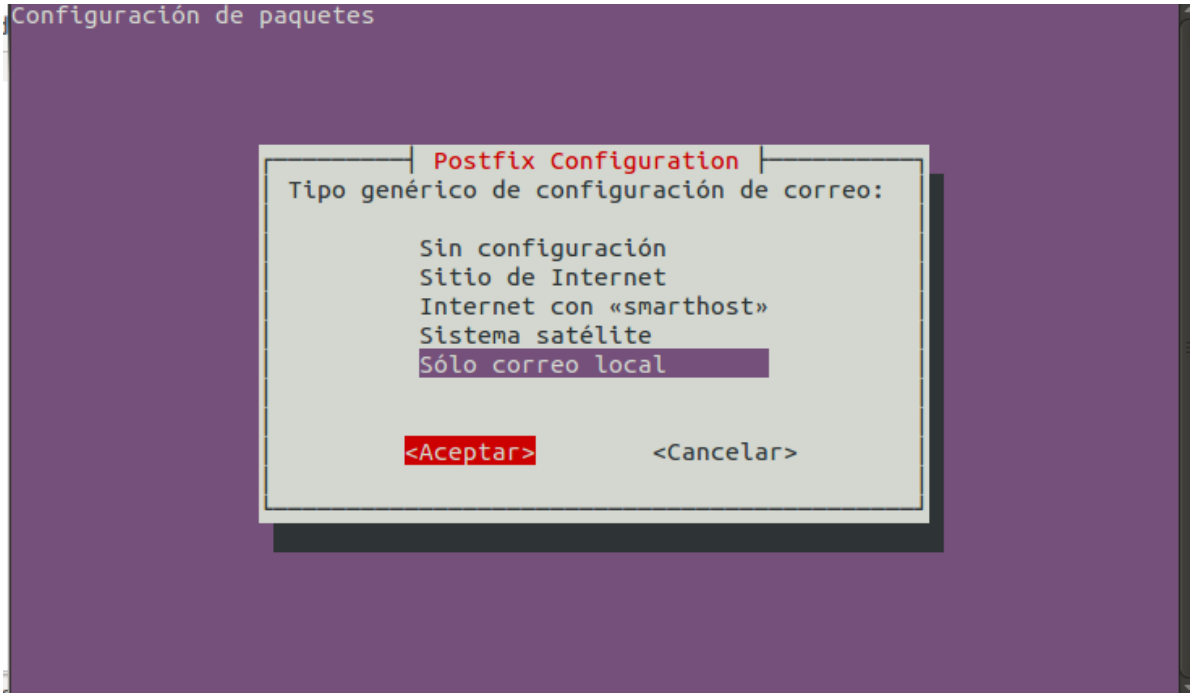
Elija "**Sí**"

Instalación de Mail Postfix en reemplazo de sendmail

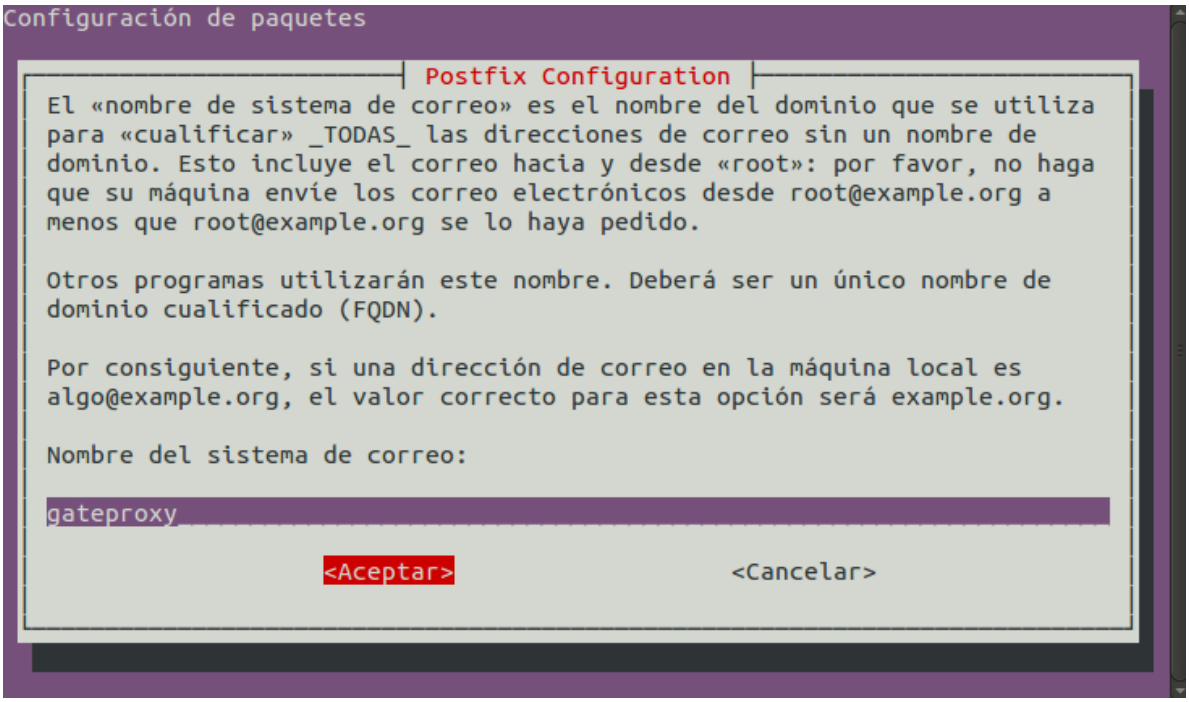
Si elige esta opción, pulse **Aceptar** en el siguiente recuadro



Configúrelo según sus necesidades. Puede dejarlo solo para correo local

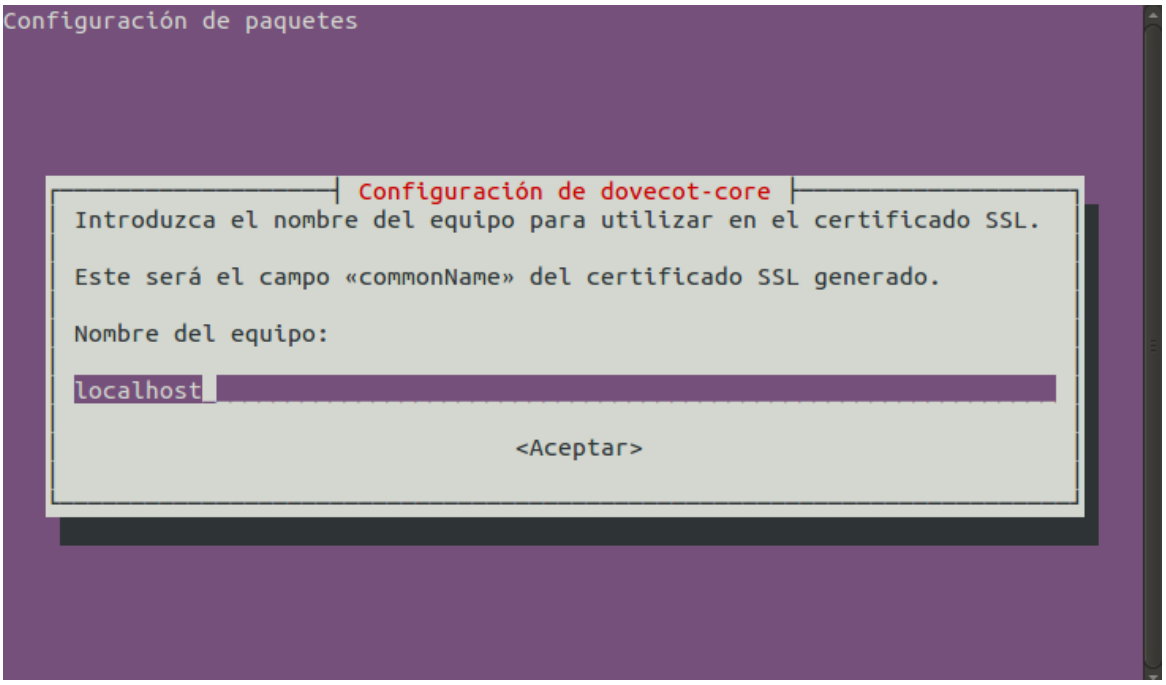


Escriba el nombre de su sistema (por seguridad no elija “gateproxy”)



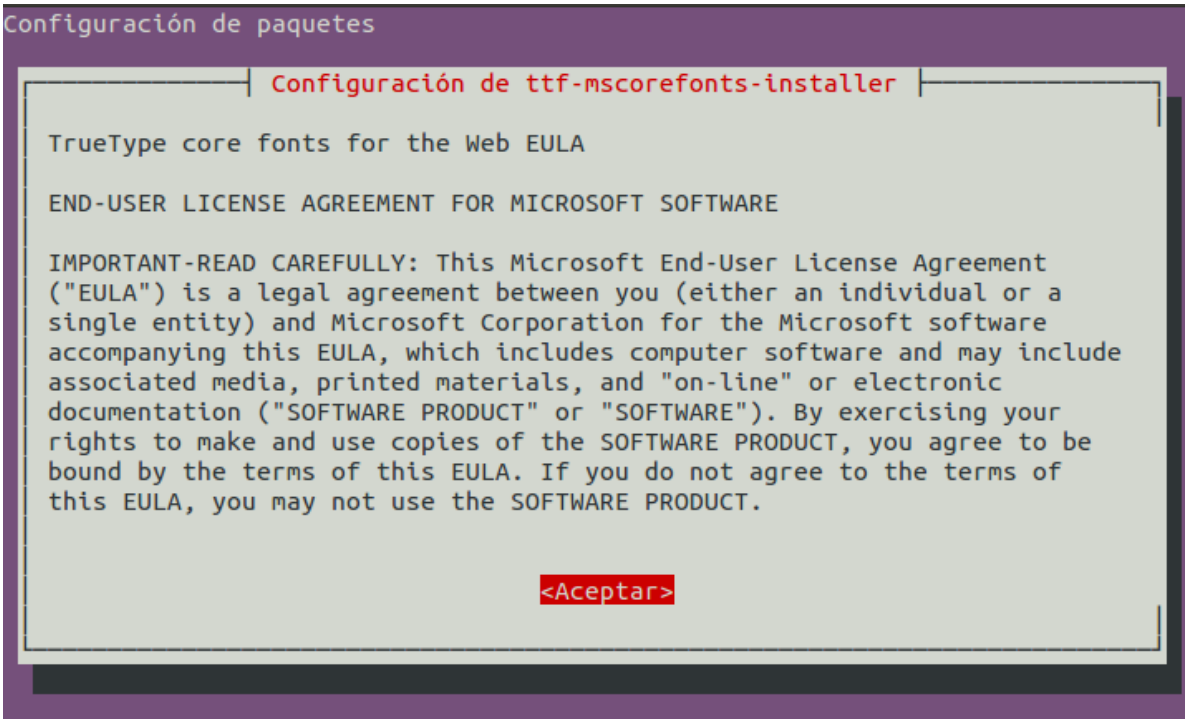
Puede elegir crear un certificado SSL autofirmado

Si generó un certificado, ponga el nombre y pulse **Aceptar**

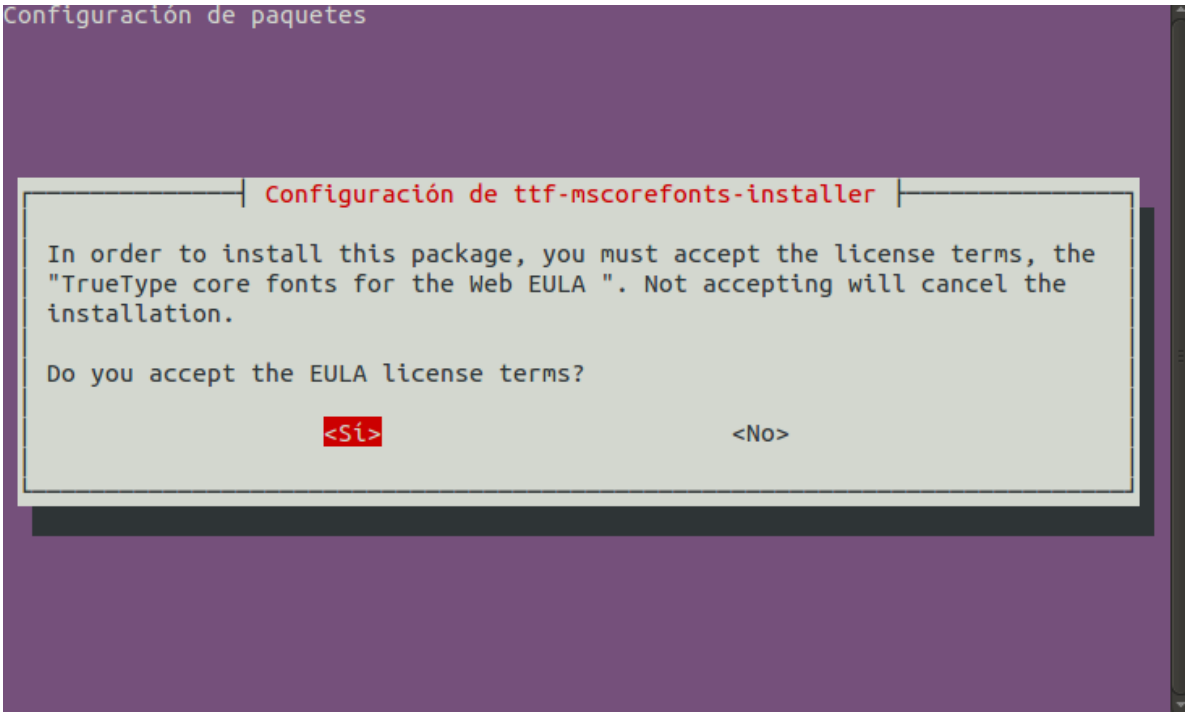


Durante el proceso de instalación, es posible que el script de instalación le pida en varias veces que ingrese su contraseña (de usuario)

Instalación de Fuentes Microsoft: pulse **Aceptar**.

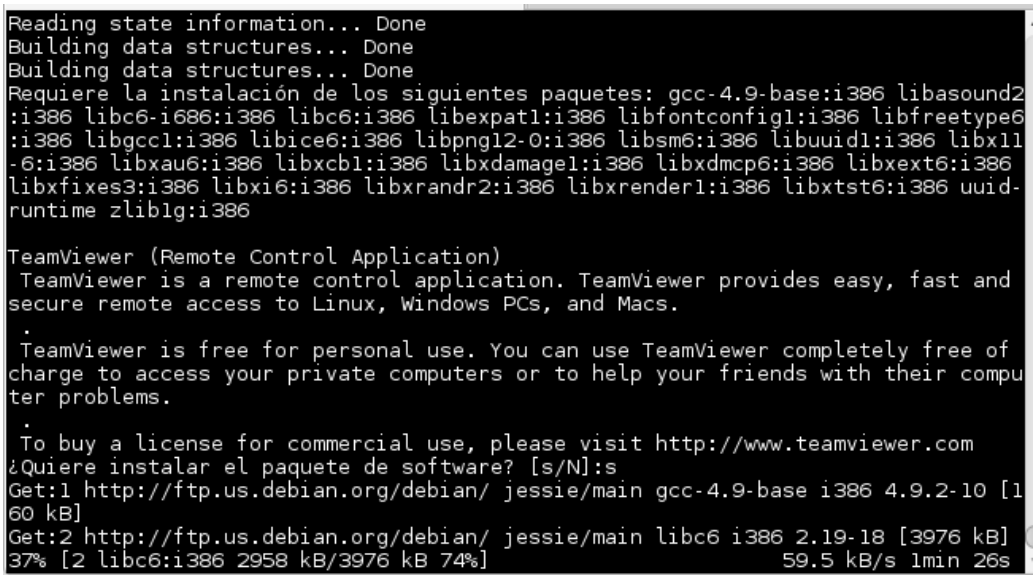


Y acepte los **términos de la Licencia EULA**



Instalación de Aplicaciones Opcionales

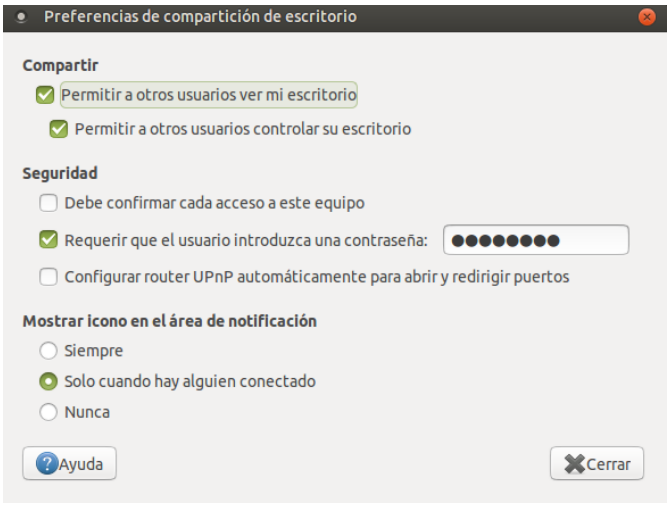
Si elige instalar los paquetes opcionales, (Mate Desktop, Gdiskdump, Teamviewer, VirtualBox Pack, VNC Remote Desktop, etc), para Teamviewer se le solicitará confirmación adicional para descarga e instalación:



Y autorización adicional para la descarga de las dependencias faltantes:

```
(Leyendo la base de datos ... 200650 ficheros o directorios instalados actualmen
te.)
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
```

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



Es obligatorio marcar estas opciones ya que VNC vino-server puede detenerse

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

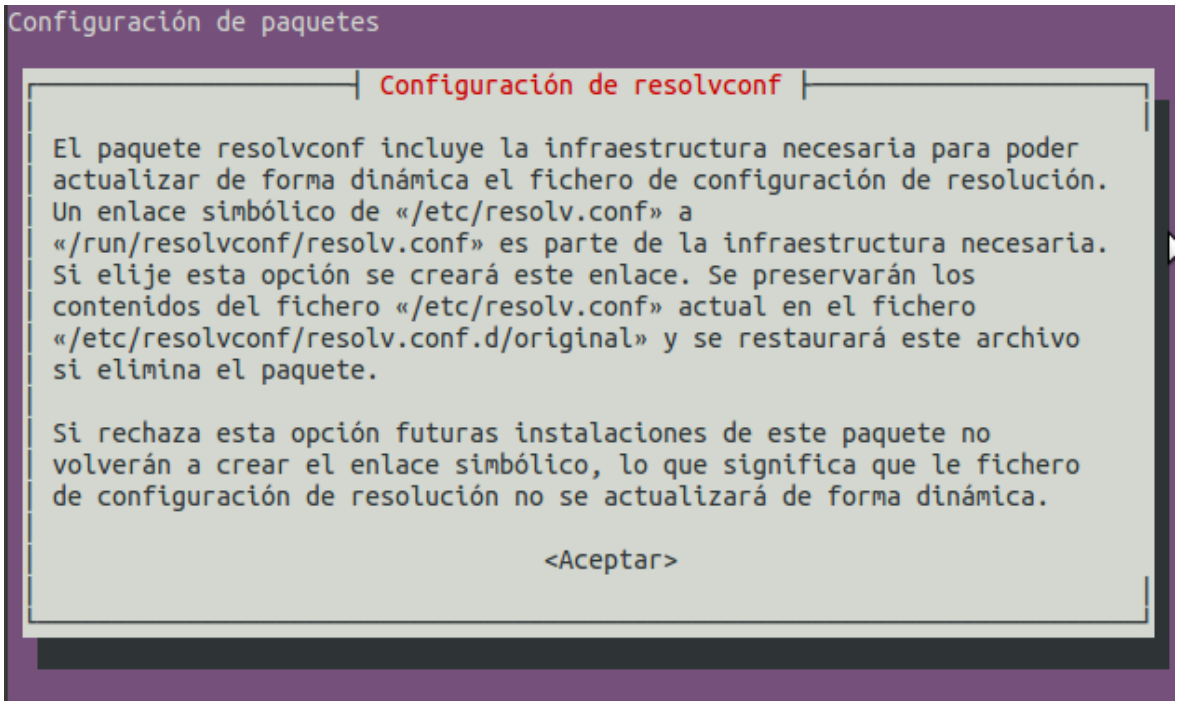
Nota Importante: El servidor VNC solo es accesible por el administrador (sysadmin). Si desea cambiar esto, edite el script **etc/init.d/iptables.sh** y descomente las reglas VNC y elimine las restricciones sobre los puertos 5900 y 5901. EL servidor VNC no viene activo por defecto. Para iniciarlo manualmente escriba en el terminal:

```
sudo /etc/init.d/vnc-server.sh start
```

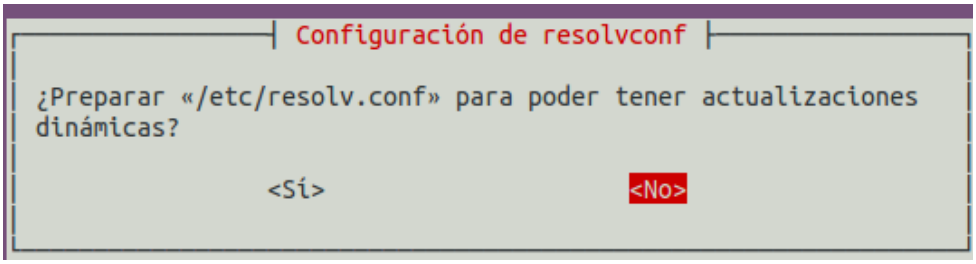
Instalación de Servidores y Modulos

Seguridad: Instalará Fail2ban, DDOS Deflate, Mod Security, OWASP, Evasive y Rootkitchk
Servidores: Instalará Squid, Apache2, DHCP
Reportes, Logs y Monitoreo: Instalará Ntop-ng, Sqstat, Sarg, Webalizer, Iptraf, Monitorix, Htop, Awstats, Logwatch, Logrotate, Ulogd2, Acct, logtail
DNS-Local: Instalará y configurará el servidor dnsmasq
Proxy: Activa la autoconfiguracion del proxy WPAD/PAC (opción 252 dhcp) o el Proxy Transparente (NAT 8080) con filtrado 443
Samba: Instala samba y activar carpeta compartida, con papelera y auditoria
Auditoria: Instalará Lynis, Nmap, Zenmap, Hping, Pipe Viewer, Arp Scan, SSl Scan wireless-tools, My traceroute, Networking toolkit, Byobu

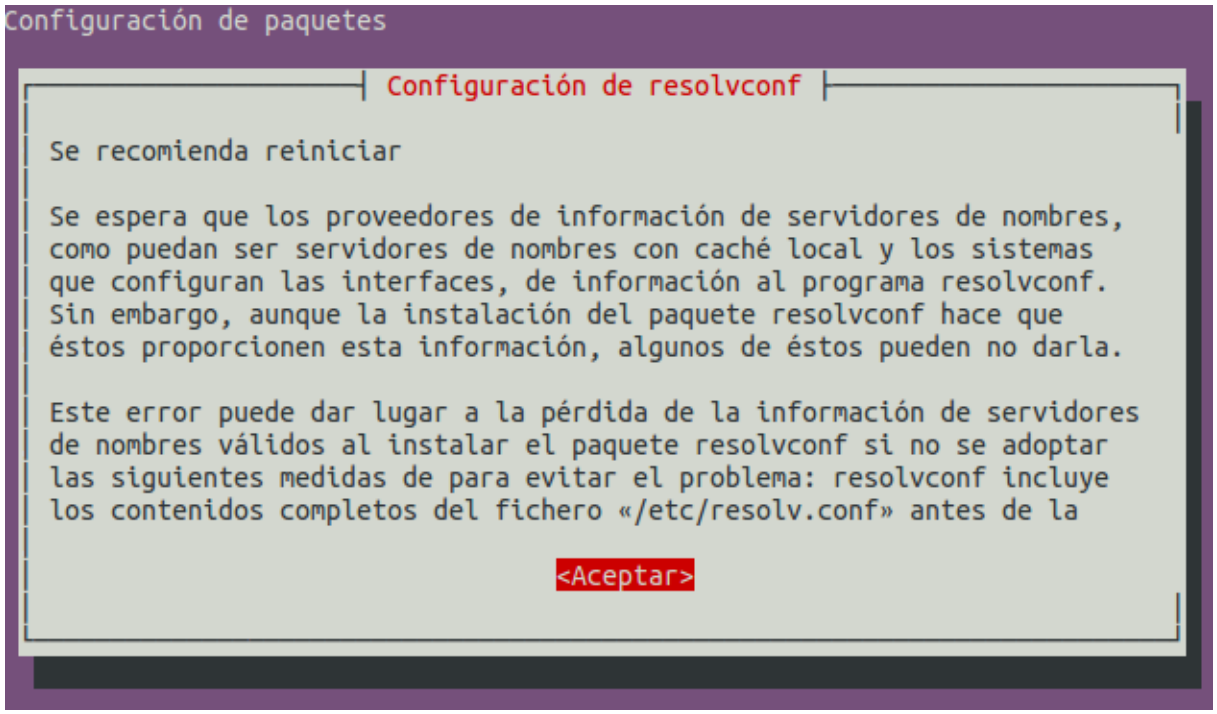
Resolv (no recomendado): Desactiva el mecanismo resolvconf y configura el antiguo resolv.conf (para ips dns estáticas). Si responde **SI** le saldrá la siguiente pantalla. Seleccione **Aceptar**



Seleccione **No**



Y finalmente seleccione **Aceptar**



Después de unos minutos (en dependencia de su conexión a internet) termina el script de instalación. Presione **ENTER** (y ponga la contraseña) para reiniciar el servidor.

PRELINK

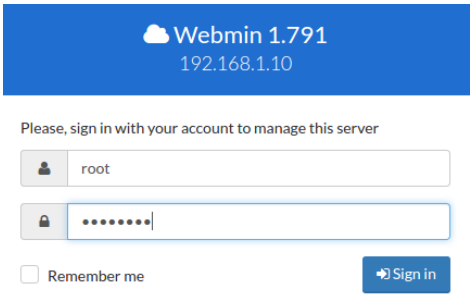
Al reiniciar, ejecutamos en el terminal el comando prelink, para acelerar el servidor

```
sudo prelink --all
```

Ha finalizado la instalación y configuración de **GATEPROXY Home & Business.**

Ahora reinicie nuevamente el servidor y configure los navegadores de su red local para que apunten al **proxy 192.168.1.10:3128 (o la IP que haya elegido para su servidor durante el proceso de instalación)**

ADMINISTRANDO EL SERVIDOR

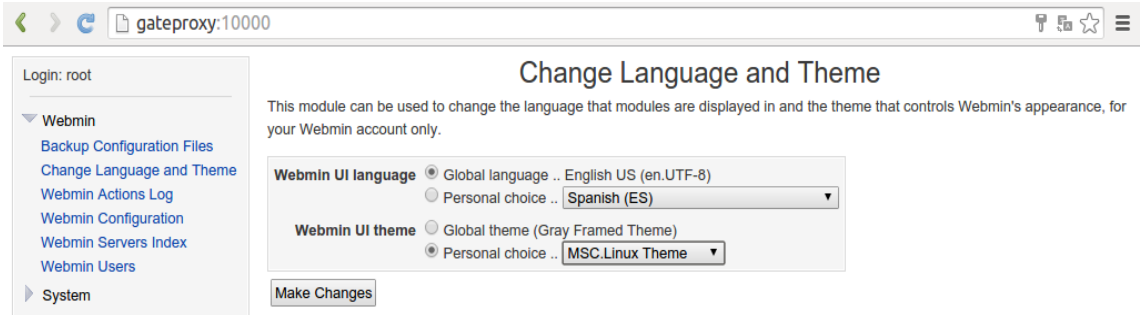


WEBMIN
Acceso https://localhost:10000 o
https://192.168.1.10:10000

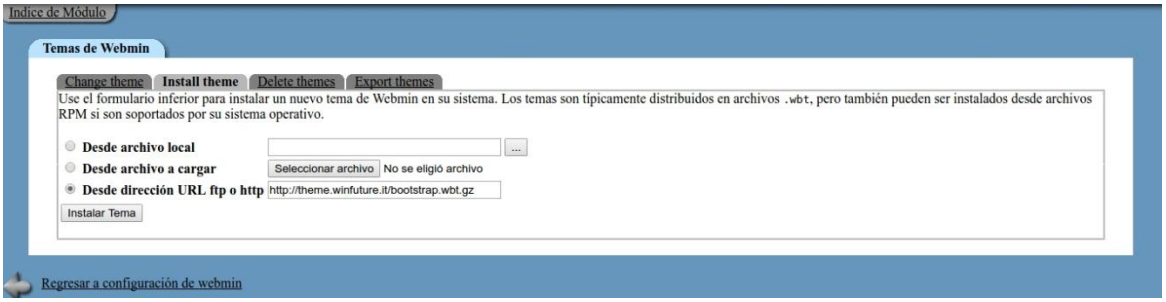
Ingrese al Webmin con el usuario **root y contraseña**. Si quiere cambiar la contraseña de **root** solamente para el acceso a webmin, ejecute en el terminal:
sudo /usr/share/webmin/changepass.pl /etc/webmin root nueva_contraseña.
Y el mensaje de respuesta deberá ser:
updated password of webmin user root

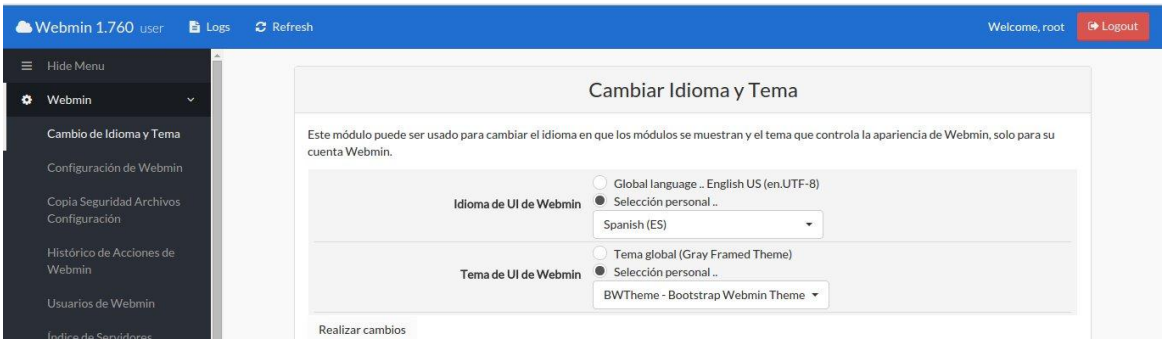
```
user@user:~$ sudo /usr/share/webmin/changepass.pl /etc/webmin root newpassword
Updated password of Webmin user root
```

Si quiere utilizar http en lugar de https, edite el archivo
/etc/webmin/miniserv.conf
y cambie el valor **SSL=1** a **SSL=0**
Puede cambiar el idioma y diseño de Webmin en "**Change Languaje and Theme**"



Si no le agradan los diseños predeterminados, puede utilizar externos, como Bootstrap





REPORTES, LOGS y MONITOREO DEL SERVIDOR

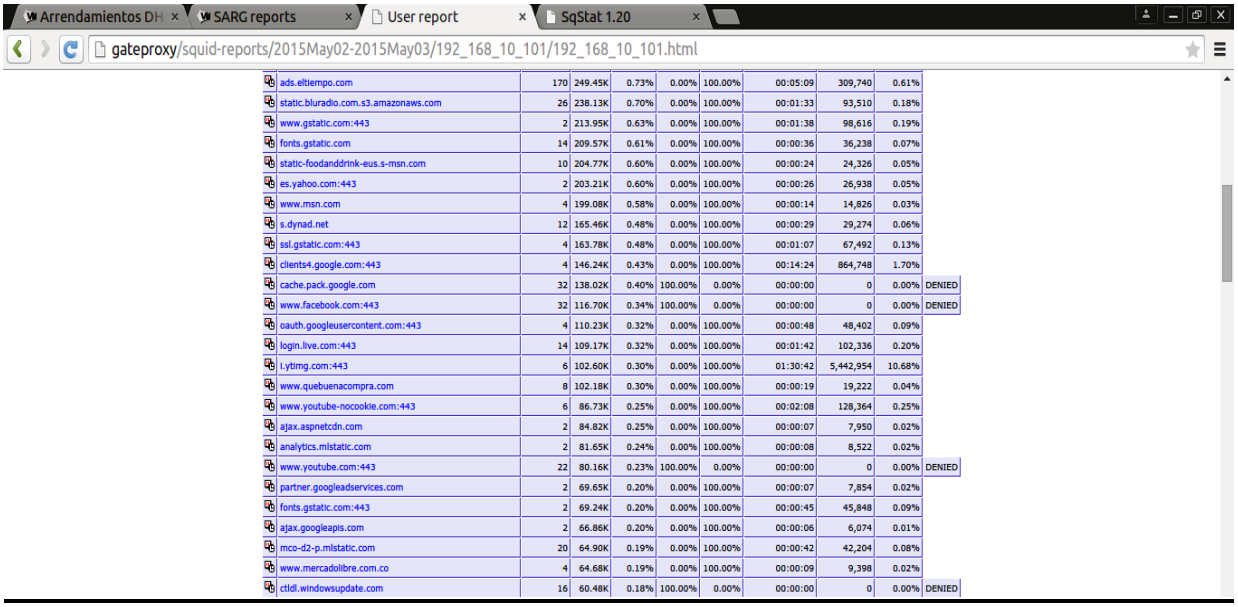
Si decidió instalar los Reportes, Logs y Monitoreo (Ntop-ng, Sqstat, Sarg, logwatch logrotate ulogd2, acct, webalizer, Munin, awstats, bandwidthd, Top Family, etc). Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache
Nota: Si quiere instalar más herramientas de monitoreo, visite el post 80 Linux Monitoring Tools for SysAdmins

SARG: (Tráfico programable)

Acceso: http://localhost/squid-reports/, http://gateproxy/squid-reports/, http://192.168.1.10:11500, o por Webmin (http://localhost:10000/sarg/)

Los reportes SARG se generan diariamente. Para generarlos manualmente, ejecute en el terminal **sudo sarg-reports today** o para mayor comodidad ingrese a webmin, a la sección “Servidores” y luego “Generador de Informes y Análisis de Squid” y finalmente pulse “Generar informe ahora”. 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** 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.

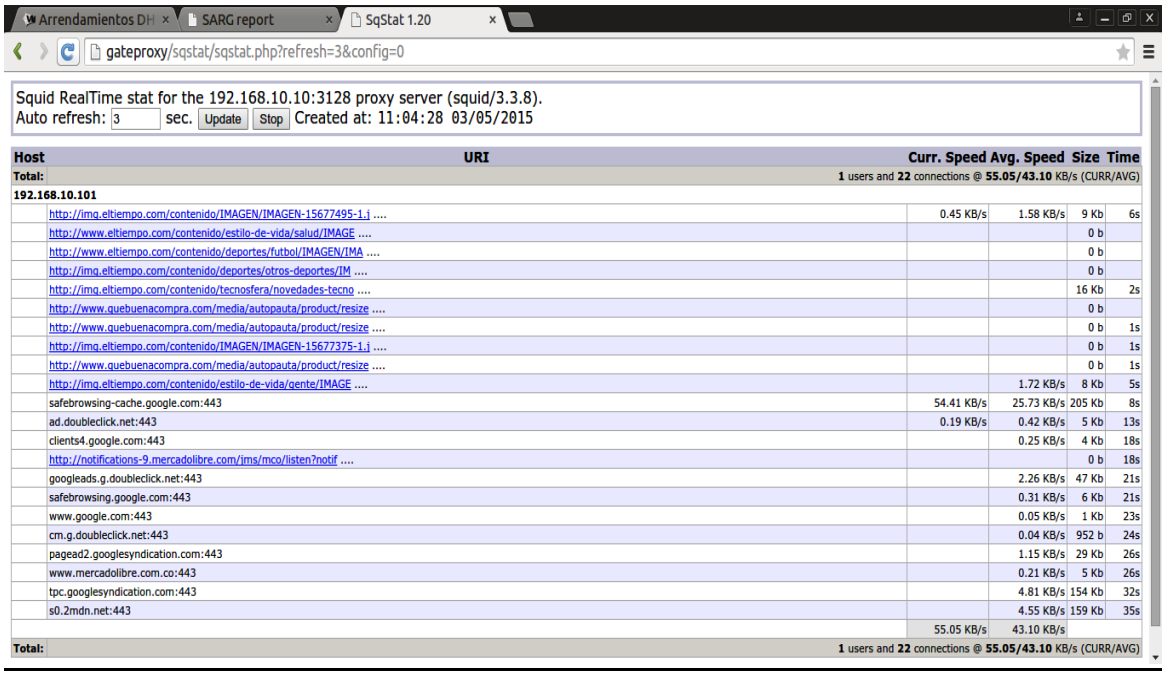


ads.eltiempo.com	170	249.45K	0.73%	0.00%	100.00%	00:05:09	309,740	0.61%
static.bluradio.com.s3.amazonaws.com	26	238.13K	0.70%	0.00%	100.00%	00:01:33	93,510	0.18%
www.gstatic.com:443	2	213.95K	0.63%	0.00%	100.00%	00:01:38	98,616	0.19%
fonts.gstatic.com	14	209.57K	0.61%	0.00%	100.00%	00:00:36	36,238	0.07%
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%	100.00%	0.00%	00:00:00	0	0.00% DENIED
www.facebook.com:443	32	116.70K	0.34%	100.00%	0.00%	00:00:00	0	0.00% DENIED
oauth.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%
i.ytimg.com:443	6	102.60K	0.30%	0.00%	100.00%	01:30:42	5,442,954	10.68%
www.quebuenacompra.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.mlstatic.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%	100.00%	0.00%	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.mlstatic.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%
ctldl.windowsupdate.com	16	60.48K	0.18%	100.00%	0.00%	00:00:00	0	0.00% DENIED

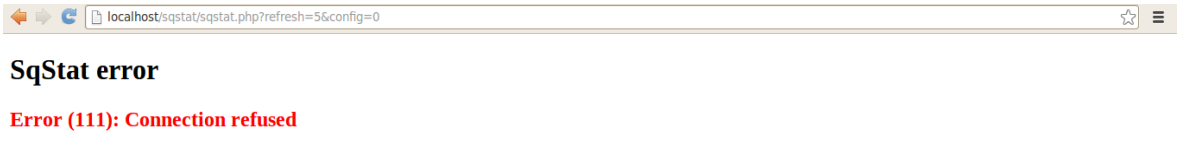
SQSTAT: (Tráfico en Tiempo real).

Acceso: http://gateproxy/sqstat/sqstat.php o http://localhost/sqstat/sqstat.php, o http://192.168.1.10/sqstat/sqstat.php

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



Nota: Tenga en cuenta que cada vez que reinicie **squid** (sudo service squid restart) o **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.



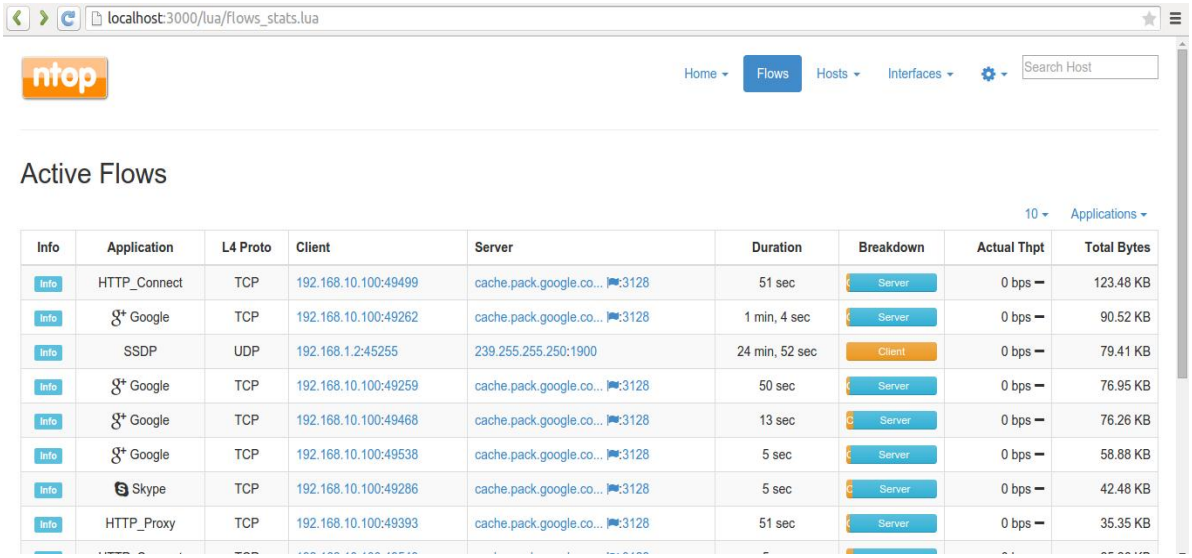
La solución es esperar un minuto y pulsar la tecla f5 para recargar la página.

NOTA: 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)**

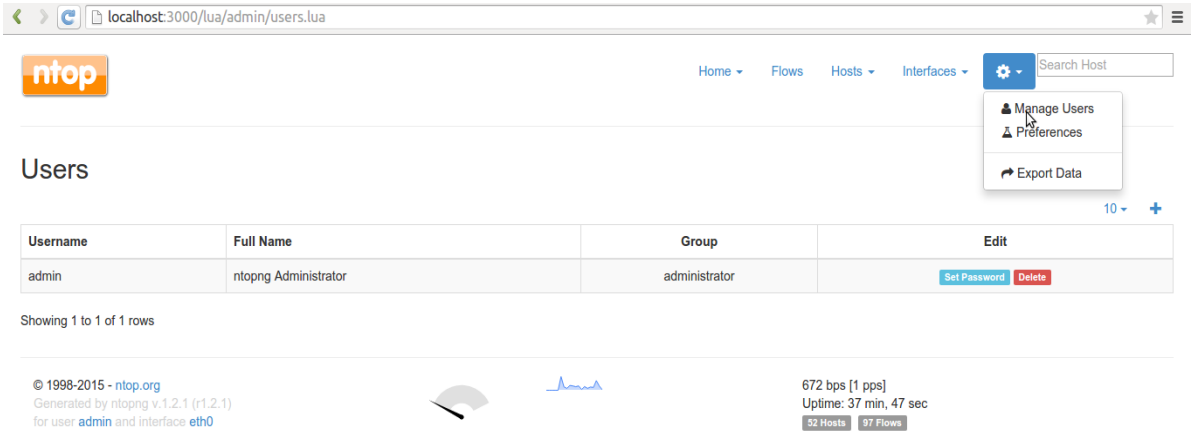
NTOP-NG (Opcional)

Acceso Notpng: http://localhost:3000, http://192.168.1.10:3000
usuario: **admin** pass: **admin**

Importante: **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



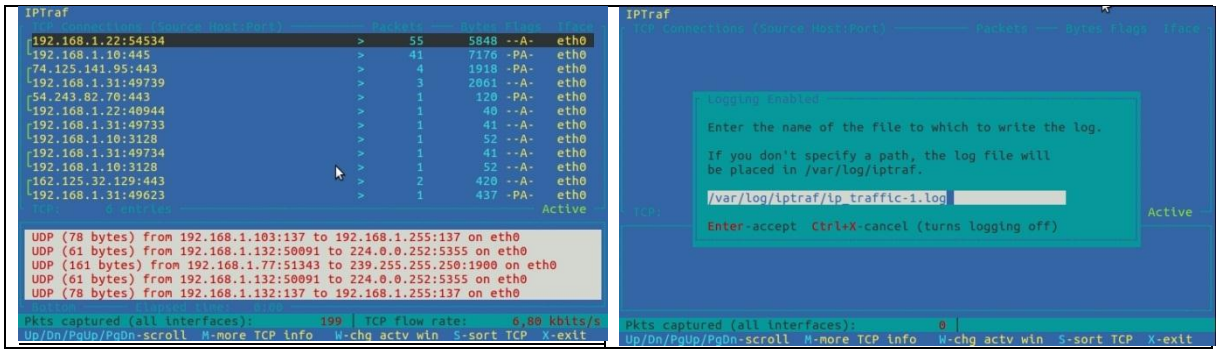
Para cambiar el pass por default, ingresamos a **Manage Users** y sobre el usuario **admin** seleccionamos **set password**



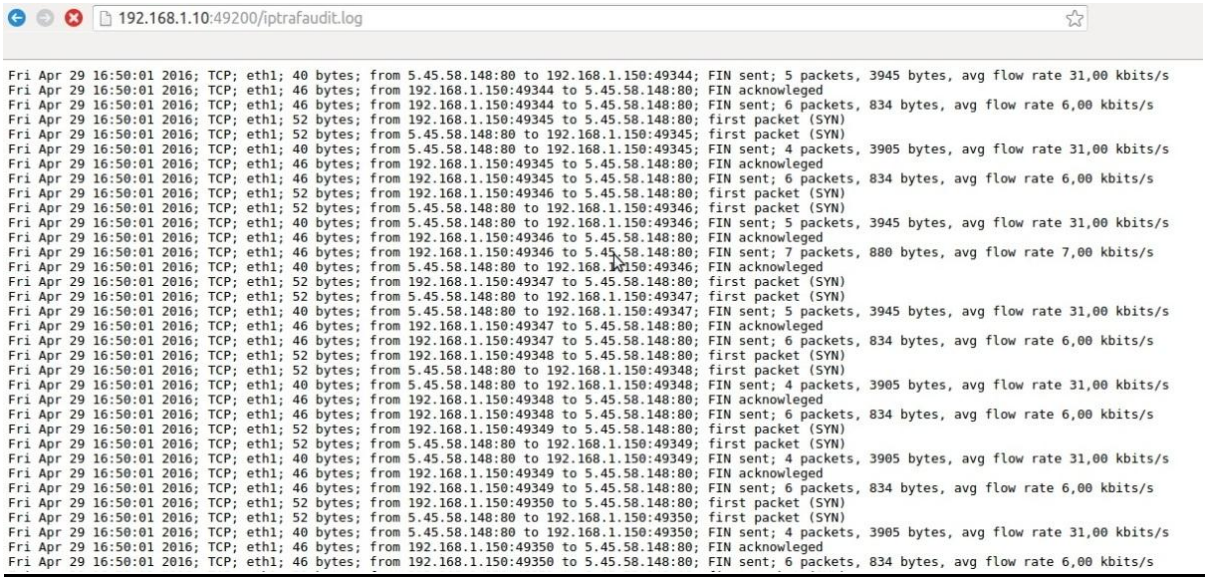
IPTRAF (Opcional)

Acceso **IPtraf**: Puede visualizarlo por terminal con **sudo iptraf** o por el navegador: http://localhost:11300 y http://192.168.1.10:11300
Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache

Iptraf consola



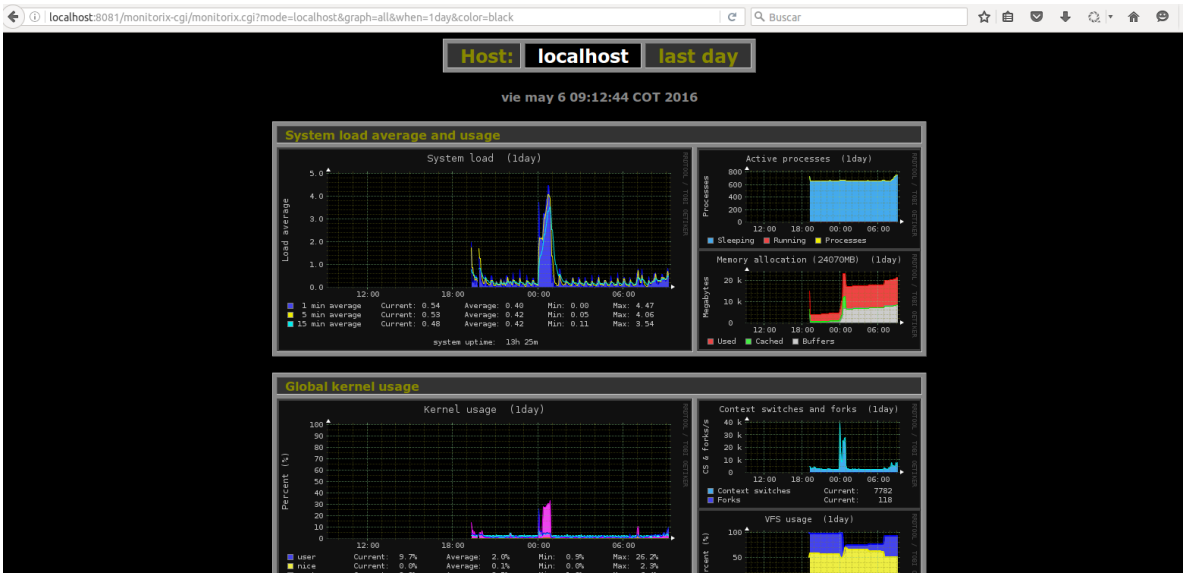
Logs IPtraf navegador



La visualización de los logs de IPtraf está programada en el cron para ejecutarse diariamente. Se visualizarán las últimas 50 líneas. Si quiere cambiar este comportamiento, ingrese al cron (**sudo crontab -e**), busque la línea y adáptela a sus necesidades. No se recomienda aumentar demasiado el número de líneas y la frecuencia
@daily tail -50 /var/log/iptraf/ip_traffic-1.log > /etc/iptrafaudit/iptrafaudit.log
Por ejemplo, ver en el navegador las últimas 100 líneas cada 2 minutos
***/10 * * * * tail -100 /var/log/iptraf/ip_traffic-1.log > /etc/iptrafaudit/iptrafaudit.log**

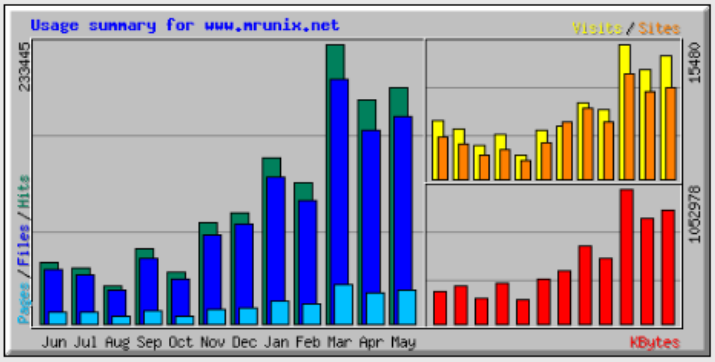
MONITORIX (Opcional)

Acceso: http://localhost:8081/monitorix/ o http://192.168.1.10:8081/monitorix/



Webalizer (Opcional)

Acceso: http://localhost:10000 o http://192.168.1.10:10000 (servidores/webalizer)



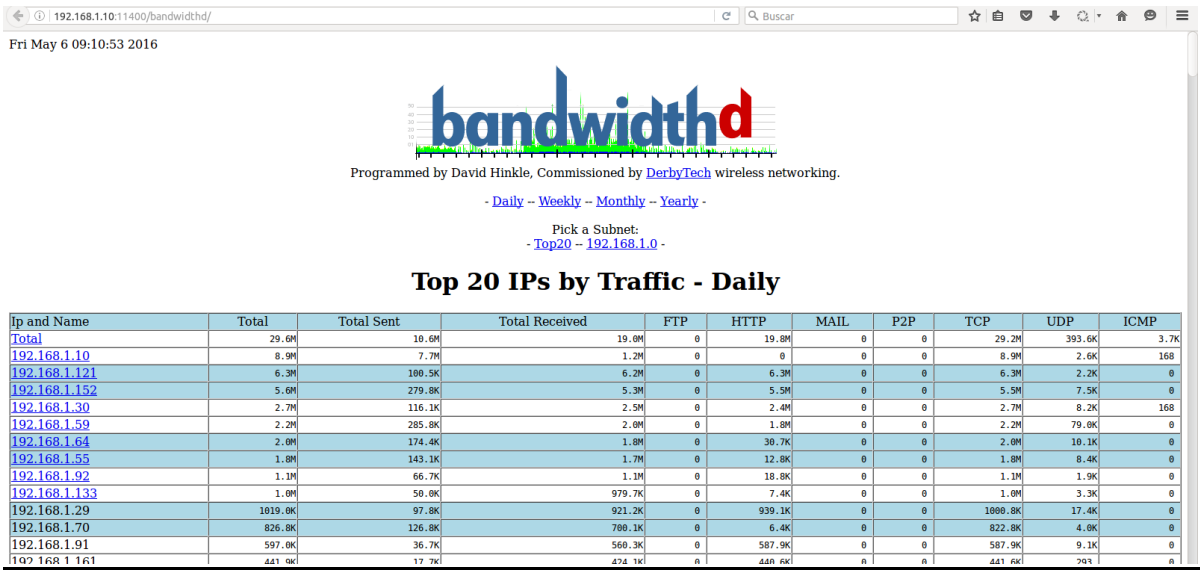
Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
May 1999	6377	5570	903	455	10484	884568	14119	28004	172671	197696
Apr 1999	6216	5394	858	419	10087	821968	12594	25758	161844	186504
Mar 1999	7530	6582	1046	499	12128	1052978	15480	32432	204059	233445
Feb 1999	4712	4128	656	321	6629	511793	8048	16419	103203	117816
Jan 1999	4470	3934	607	284	8079	605694	8808	18844	121980	138571
Dec 1998	2998	2673	411	197	6524	410110	6120	12769	82875	92951
Nov 1998	2910	2567	400	192	4260	346705	5588	11627	74468	84403
Oct 1998	3052	2668	457	202	2203	189253	2839	6399	37360	42738
Sep 1998	2072	1826	345	169	3475	314492	5075	10376	54807	62165
Aug 1998	1014	901	211	125	2693	196560	3890	6571	27958	31455
Jul 1998	1484	1325	302	184	4041	298225	5716	9383	41102	46019
Jun 1998	1707	1502	322	222	4809	251502	6675	9687	45077	51227
Totals						**5883848**	**94952**	**188269**	**1127404**	**1284990**

Bandwidthd (Opcional)

Las pantallas de configuración puede dejarlas por defecto, ya que prevalecerá la información de red que puso al comienzo de la instalación. Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache

Acceso: http://localhost:11400 o http://192.168.1.10:11400



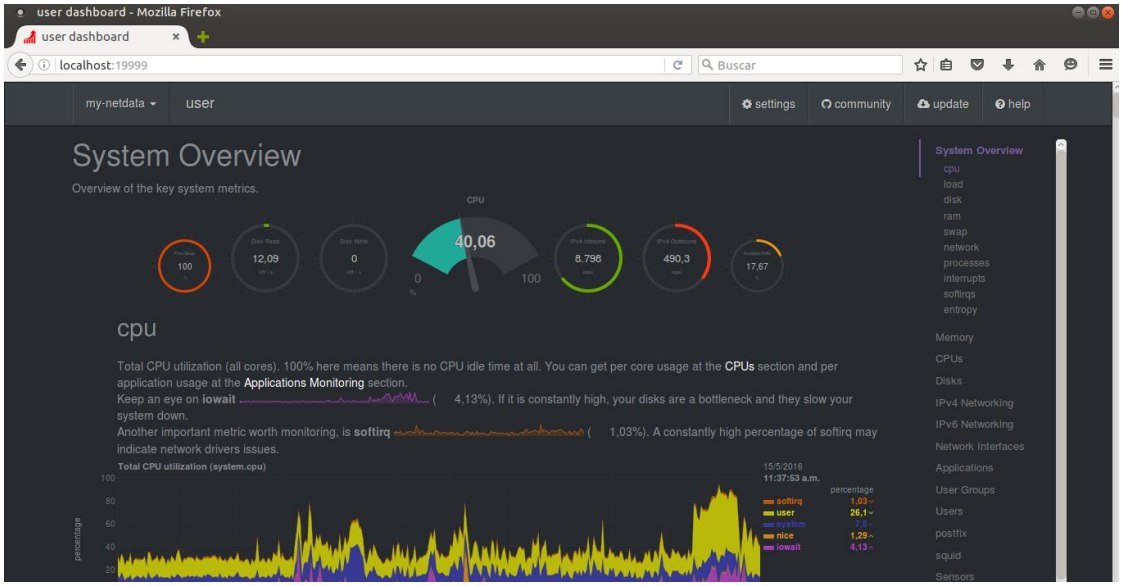
Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	MAIL	P2P	TCP	UDP	ICMP
Total	29.6M	10.6M	19.0M	0	19.8M	0	0	29.2M	393.6K	3.7K
192.168.1.10	8.9M	7.7M	1.2M	0	0	0	0	8.9M	2.6K	168
192.168.1.121	6.3M	100.5K	6.2M	0	6.3M	0	0	6.3M	2.2K	0
192.168.1.152	5.6M	279.8K	5.3M	0	5.5M	0	0	5.5M	7.5K	0
192.168.1.30	2.7M	116.1K	2.5M	0	2.4M	0	0	2.7M	8.2K	168
192.168.1.59	2.2M	285.8K	2.0M	0	1.8M	0	0	2.2M	79.0K	0
192.168.1.64	2.0M	174.4K	1.8M	0	30.7K	0	0	2.0M	10.1K	0
192.168.1.55	1.8M	143.1K	1.7M	0	12.8K	0	0	1.8M	8.4K	0
192.168.1.92	1.1M	66.7K	1.1M	0	18.8K	0	0	1.1M	1.9K	0
192.168.1.133	1.0M	50.0K	979.7K	0	7.4K	0	0	1.0M	3.3K	0
192.168.1.29	1019.0K	97.8K	921.2K	0	939.1K	0	0	1000.8K	17.4K	0
192.168.1.70	826.8K	126.8K	700.1K	0	6.4K	0	0	822.8K	4.0K	0
192.168.1.91	597.0K	36.7K	560.3K	0	587.9K	0	0	587.9K	9.1K	0
192.168.1.161	441.9K	17.7K	424.1K	0	440.6K	0	0	441.6K	293	0

NetData: Monitoreo de recursos del servidor (Opcional)

Durante la instalación presiones **Enter**

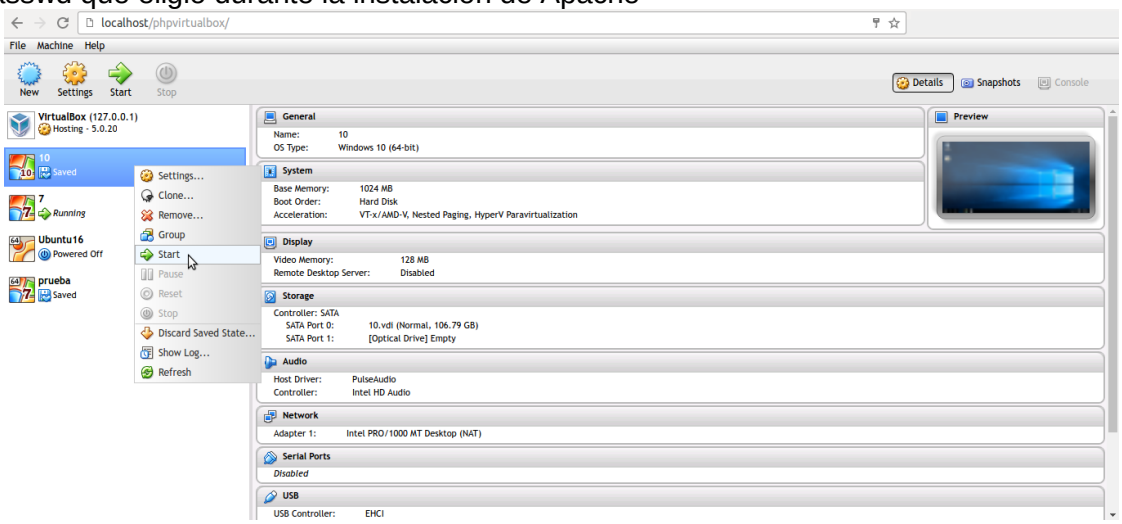
```
This installer allows you to change the installation path.
Press Control-C and run the same command with --help for help.

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

Acceso : http://localhost:19999/



PHPVIRTUALBOX: Acceso http:/192.168.1.10:11600

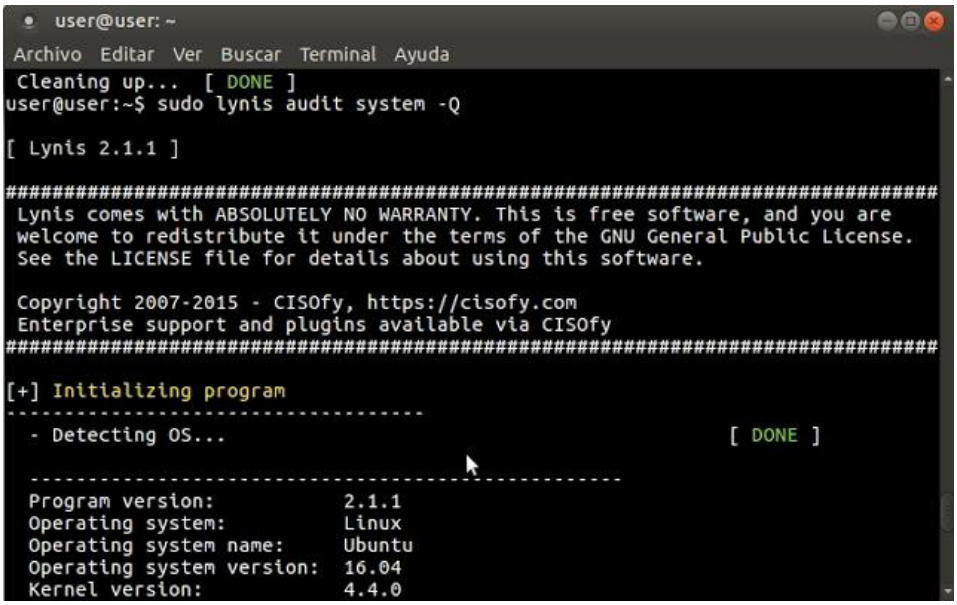
Si instaló **VirtualBox Pack**, puede **administrar sus VMs desde el navegador con phpvirtualbox**. Al ingresar por primera vez, debe le pedirá el usuario de su servidor y el passwd que eligió durante la instalación de Apache



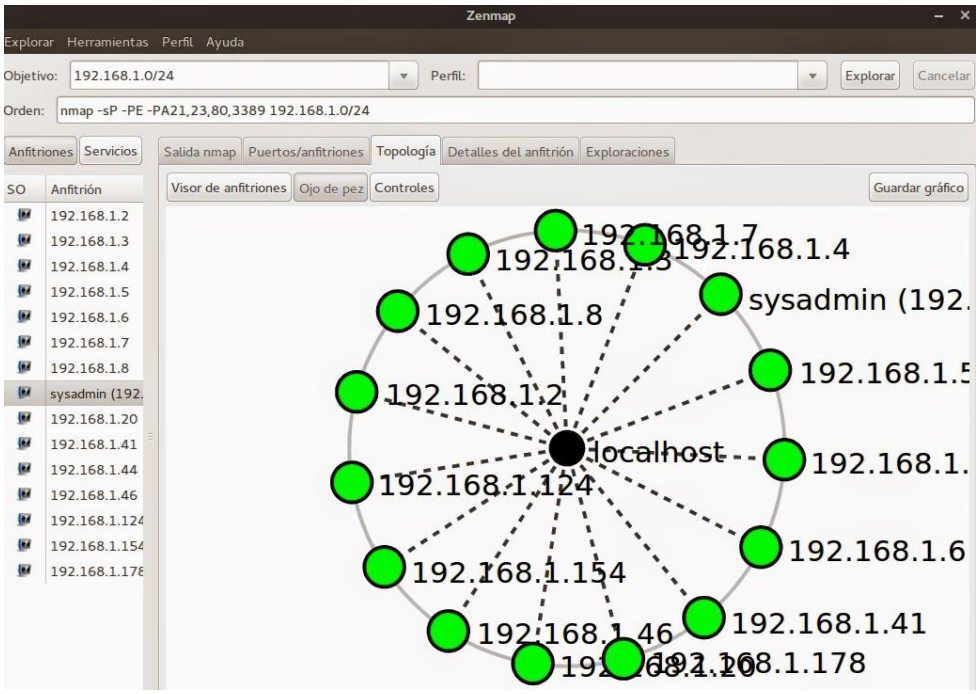
MODULOS DE AUDITORIA

Si decidió instalar los Módulos de Auditoria (Lynis, Nmap, Zenmap, Hping, Arp Scan, Pipe Viewer, Networking toolkit, wireless-tools, My traceroute, General Colorizer, byobu, sslscan), para acceder a estos debe ingresar su usuario (nombre del servidor) y password (solicitado durante la instalación)

Lynis: Para mayor información lea el post Auditoria de servidores Linux



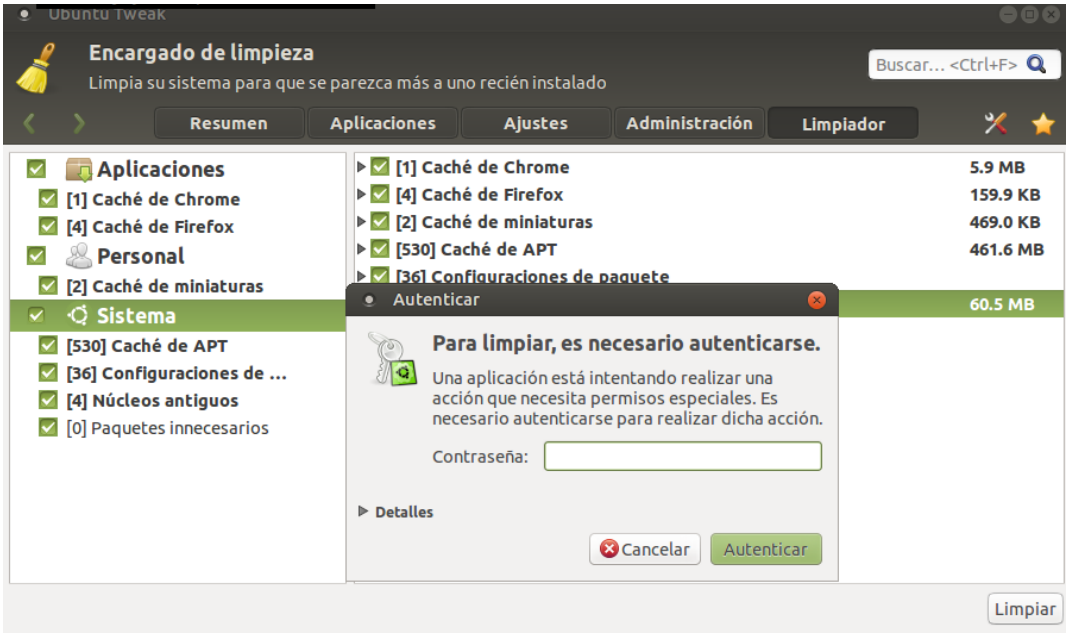
Zenmap/Npap: Para mayor información lea el post Control de Acceso



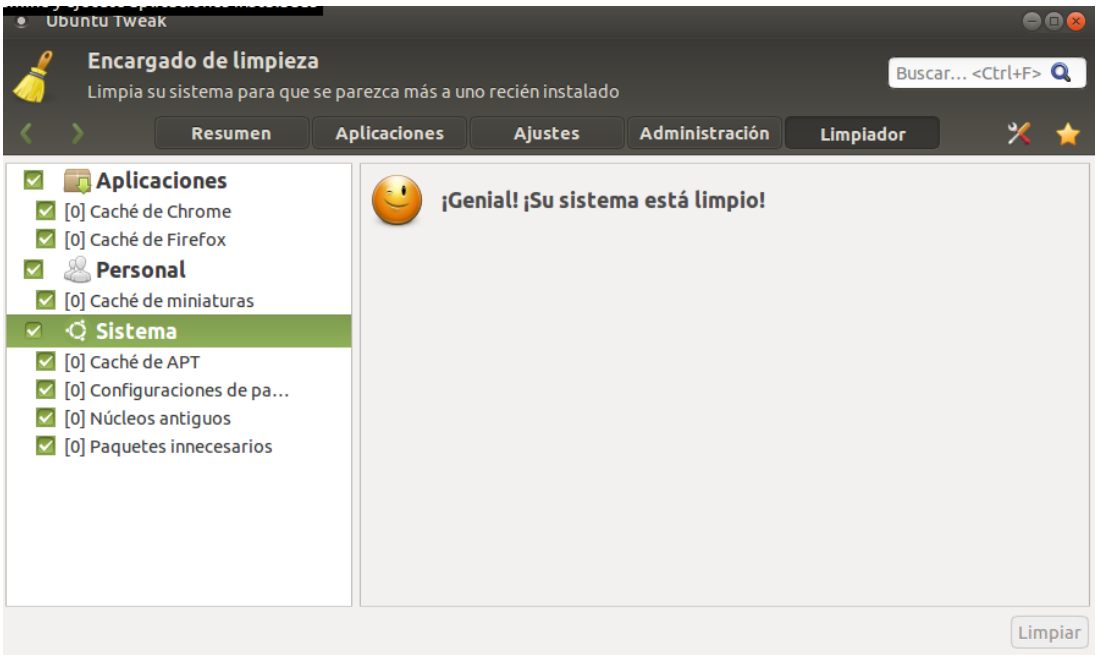
PASOS OPCIONALES (Solo para Ubuntu)

LIMPIEZA

El siguiente paso es realizar una limpieza del sistema. Para esto accedemos a **Sistemas/Administracion/Ubuntu Tweak.** Aquí seleccionaremos todas las casillas y pulsamos **Limpiar** (pedirá la contraseña)

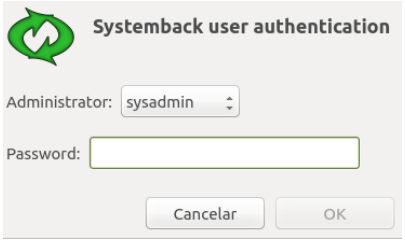


Al terminar debe salir el siguiente mensaje

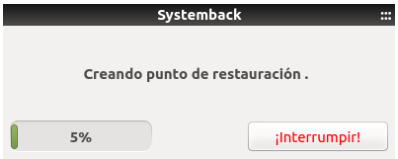


CREANDO PUNTO DE RESTAURACION

Para evitar cualquier situación con nuestro servidor, crearemos un punto de restauración. Para esto vamos a **Aplicaciones/Herramientas de Sistema/Systemback** e ingresamos la contraseña del sistema y pulsamos ok. Por defecto el programa almacena el punto en **/home**. Puede cambiarlo a una ubicación específica (no recomendado). El siguiente paso es pulsar **Crear nuevo**…



Y comenzará la creación del punto de restauración. Si se presentan fallas con alguna actualización o manipulación, puede restaurarlo ingresando nuevamente a la aplicación y eligiendo el punto de restauración



BACKUP DE PARTICION Y/O DISCO DURO

También puede realizar un Backup (usando técnicas de clonación) de su DD y/o partición, para posteriormente restaurarla en caso de desastres, con la herramienta GDiskDump, incluida en **Gateproxy**.

Para mayor información sobre copias de seguridad visite los posts:

Clonación Incremental y Clonación Virtual

POST-INSTALL

Contraseña: Crear la contraseña del usuario **root.** Para hacerlo escriba en el terminal **sudo su** y la contraseña. Luego escriba **passwd** y elija la contraseña **root** (dos veces), y finalmente escriba **exit**.

```
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
```

Si va a cambiar la contraseña del usuario**,** escriba en el terminal **sudo passwd** e ingrese la nueva contraseña (dos veces).

Ingreso de equipos a la red local y privilegios: 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 **leases.sh** (**/etc/init.d/leases.sh**). Puede aumentar o disminuir este rango, editando **leases.sh**.

La política establecida por defecto es que todos los PCs a los cuales el DHCP les arrienda una dirección IP entran a su red **denegados,** o sea son incluidos en una acl llamada **blackdhcp** (**/etc/acl/blackdhcp**) con el formato:

[a|b];dirección_mac;dirección_ip;nombre_host;fecha_introduccion. Ejemplo:

```
a;90:68:c3:20:00:00;192.168.1.102;USUARIO;1432768764;
```

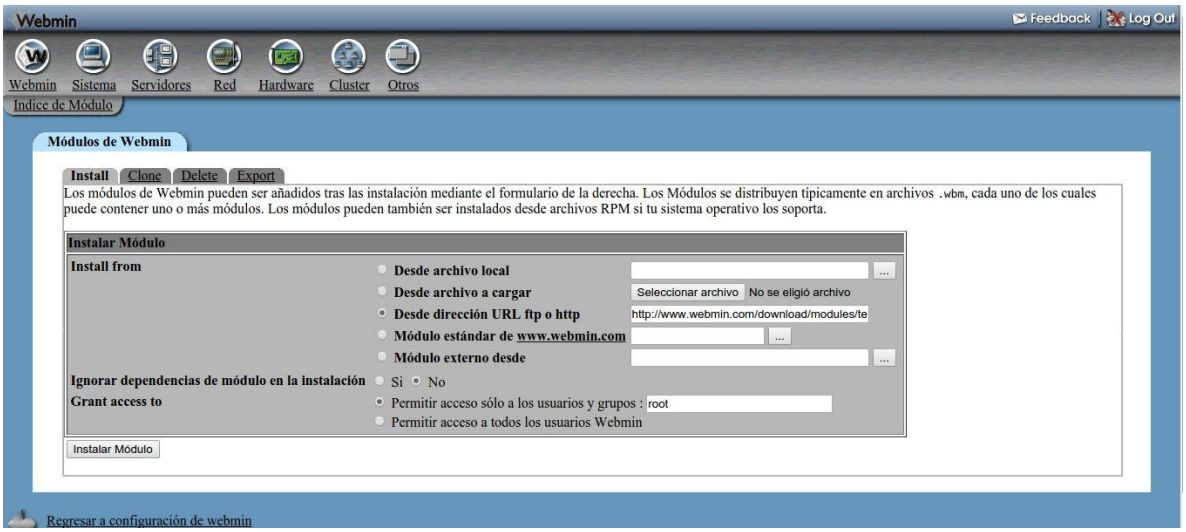
Si pasados en 5 minutos el operador del servidor no decide qué hacer con estos terminales entrantes, el servidor DHCP automáticamente no les volverá a arrendar una dirección IP.

Entonces, el operador del servidor deberá identificar cuál de estos terminales entrantes le va a autorizar la entrada definitiva a su red local. Para autorizarlos, **edite con privilegios sudo** la acl **/etc/acl/blackdhcp.txt** y **copie y pegue** el terminal autorizado a la acl **/etc/acl/macslocal.txt** (ver tabla **ACL INCLUIDAS**). Si quiere otorgarle altos privilegios a ciertos equipos (descargas, acceso ilimitado sin restricciones, etc) debe pegarlos acl /**etc/acl/macsprivilegiadas.txt.** Tenga en cuenta que la acl **macsprivilegiadas 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.

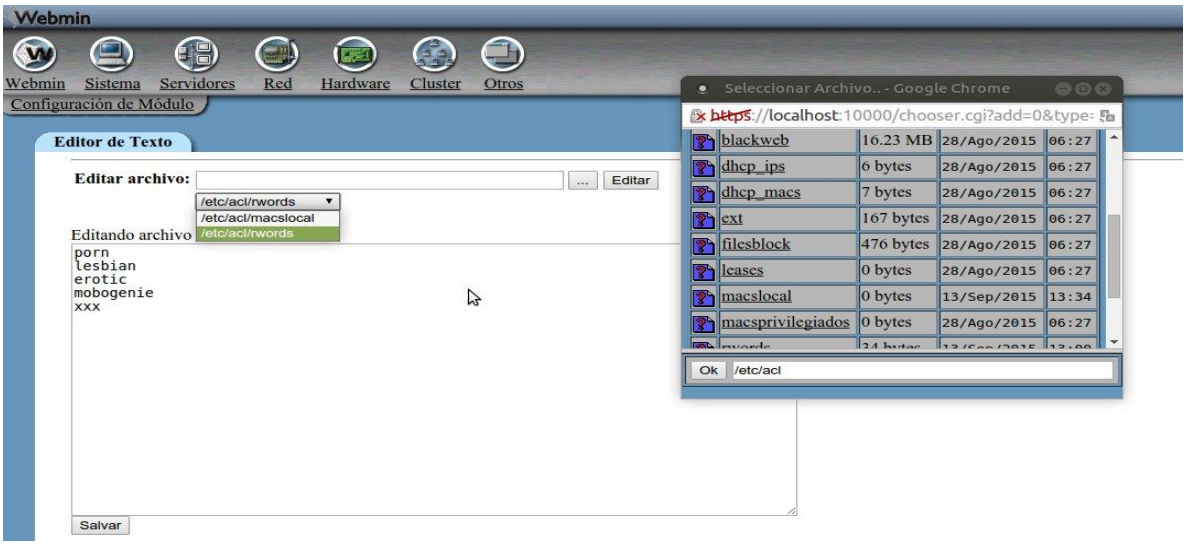
Puede agregar terminales manualmente, incluyéndolos en la acl **/etc/acl/macslocal.txt** o /**etc/acl/macsprivilegiadas.txt**, siguiendo el formato descrito anteriormente, pero, tenga en cuenta que el servidor amarra MAC+IP (y HOST como consulta), por tanto no debe utilizar ninguna IP, MAC o HOST asignado a otro terminal o generará conflictos. Es

importante aclarar que no puede haber terminales repetidos en la acl macslocal (vea la explicación en tabla **ACLS INCLUIDAS**)

Para mayor comodidad puede editar las ACLs mencionadas, ubicadas en **/etc/acl,** desde Webmin. Para esto ingrese a **Webmin,** pulse en **Configuración de Webmin** y luego en **Módulos de Webmin** y en **Desde dirección URL ftp o http** ingrese el enlace de Text Editor (http://www.webmin.com/download/modules/text-editor.wbm.gz)
y pulse **Instalar**. Ejemplo:



Esto instalará un editor de textos. Luego acceda al Webmin como **root**, y e ingrese a **Otros** y pulse en **Editor de Texto.** Ahí podrá abrir cada una de ACLs ubicadas en **/etc/acl**. Ahora, cada vez que necesite editar alguna, simplemente en el módulo **Editor de Texto,** en **Editar Archivo**, pulse el botón "**…**", se abrirá una ventana, seleccione la acl en **/etc/acl**, y pulse el botón **Editar** y finalmente **Salvar** para que quede guardada en el historial. La próxima vez que la necesite, estará disponible en el menú desplegable, como se muestra en la imagen:



Inicio automático y actividad de servicios esenciales: En la sección de **Sistema/Arranque y Parada** de **Webmin** se encuentran los servicios esenciales de su servidor (según los que haya elegido durante la instalación):
Isc-dhcp-server, squid, webmin, apache, dnsmasq, ntopng, redis-server, etc
Ejemplo de servicio dhcp inactivo:

☐	isc-dhcp-server	Dynamic Host Configuration Protocol Server	No	No

Ejemplo de servicio dhcp activos:

☐	isc-dhcp-server	Dynamic Host Configuration Protocol Server	Si	Si

Es irrelevante los cambios que haga en esta zona, debido a que el script vigilante **/etc/init.d/servicesreload.sh** (corre en el cron cada 3 minutos) es el encargado de supervisar que estos servicios se encuentren siempre activos y si por alguna razón caen o no están activos, los levanta y deja constancia en **/var/log/alert.log**

Backup de los archivos de configuración y ACLs: 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.

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.
Ingrese al terminal, acceda como **root** en la raíz a la carpeta “CDROM” y ejecute:
sh VBoxLinuxAdditions.run
Para Ubuntu, acceda a la carpeta VBOXADDITIONS_5XXXXX/ dentro de la carpeta “media” y ejecute:
sudo ./VBoxLinuxAdditions.run

Puertos adicionales
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**) o por webmin, busque la regla PORTS RULES y descomente los puertos que quiera autorizar para su red local.

Dirección MAC de administración: Si va a administrar el firewall iptables desde otro equipo que no sea el servidor, edite el script **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.
 # reemplace la mac de administración
sysadmin="b4:74:9f:93:00:00"

PROXY

Durante la instalación, el script de **GateProxy** le da la oportunidad de definir con qué tipo de proxy quiere trabajar:

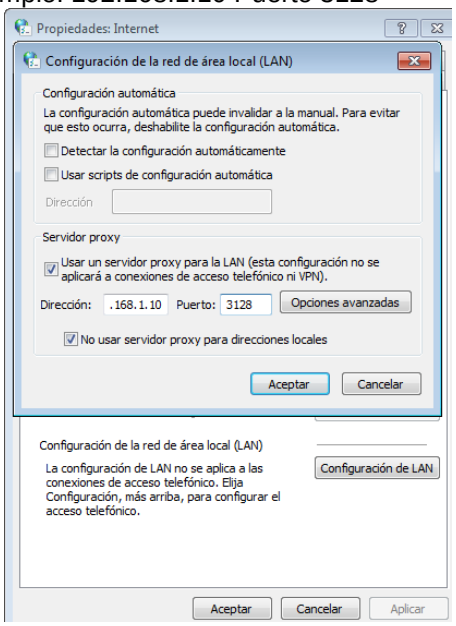
Proxy Transparente (NAT 8080) o Proxy No-Transparente (3128)

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

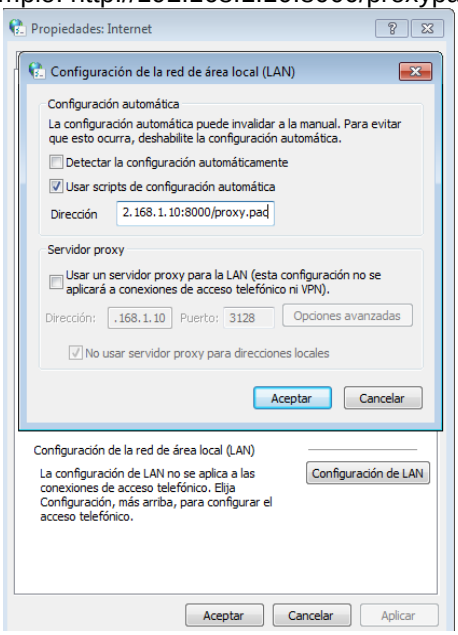
Manual

Panel de Control / Opciones de Internet / Conexiones / Configuración de LAN
Ingrese la ip y puerto de su servidor proxy.
Ejemplo: 192.168.1.10 Puerto 3128



Automático

Panel de Control / Opciones de Internet / Conexiones / Configuración de LAN
Ingrese la url del archivo de configuración
Ejemplo: http://192.168.1.10:8000/proxypac



Importante: El método manual es compatible todos los navegadores actuales, pero el método de configuración automática (WPAD/PAC) o por default, presenta muchas limitaciones, es vulnerable (se puede crear un servidor wpad falso) y no es compatible con todos los navegadores. Además, algunos navegadores (como Mozilla) no soportan DHCP WPAD y requieren de un servidor DNS para divulgar WPAD (puede consultar la tabla de compatibilidad en Browser-Support).

Si activó el proxy no-transparente y desea desactivar la autoconfiguración para realizarla manualmente, realice las siguientes acciones:

ARCHIVO/DIRECTORIO	ACCION (ELIMINAR O COMENTAR)
/etc/proxy	Eliminar
/etc/apache2/sites-enabled/proxy.conf	Eliminar
/etc/apache2/ports.conf	#Listen 8000
/etc/init.d/leases.sh	#option option-252 code 252 = text; #option option-252 \"http://192.168.1.10:8000/proxy.pac\";

Proxy Transparente NAT 8080 con filtrado IP 443 (**no recomendado**)

Un proxy transparente "*combina un servidor proxy con un cortafuegos (firewall) de manera que las conexiones son interceptadas y desviadas hacia el proxy sin necesidad de configuración en el cliente, y habitualmente sin que el propio usuario conozca de su existencia*." En otras palabras, no tendrá que configurar los navegadores de su red local para que apunten a la ip y puerto específico del proxy, sino que, con la configuración por default que traen (detección automática del proxy), podrán conectarse fácilmente; sin embargo debe tener en cuenta que esto puede implicar un riesgo en la seguridad, tanto para el servidor como para su red local.

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

Tenga en cuenta que el proxy squid no filtra conexiones https (puerto 443) en modo transparente y por tanto este tipo de tráfico no aparecerá reflejado en los reportes Sarg, Sqstat, etc (estos reportes solo mostrarán el tráfico http en modo transparente). Además, para las conexiones https no aplican reglas de squid de bloqueos de extensiones y otros tipos de filtrado, ya que las conexiones https son cifradas. Para el caso de proxy caché (no-transparente) squid solamente puede realizar bloqueos a urls https, gracias a la cláusula CONNECT y el tráfico https aparece en los reportes, siendo la única diferencia importante con el proxy no transparente. Para mayor información consulte el post Proxy

Nota: 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).

Las reglas transparentes incluidas iptables están diseñadas para permitir el paso solamente de las ips (https) o rangos de ips, contenidos en la acl whiteip y luego el firewall cierra el puerto 443 (sección 443 filter), sin embargo esto puede hacer que su firewall colapse, por la cantidad de ips que tiene que procesar para validar (incluidas en whiteip.txt). Por defecto viene comentada. Actívela bajo su propio riesgo.

```
for mac in $(awk -F";" '{print $2}' $route/macs*); do
        # PROXY ACCESS (LAN ---> PROXY ---> INTERNET Redirect to NAT proxyport)
        $iptables -t nat -A PREROUTING -s $local/$netmask -i $lan -p tcp --dport 80 -j REDIRECT
--to-port $proxyport2
        $iptables -A INPUT -s $local/$netmask -i $lan -p tcp --dport $proxyport2 -j ACCEPT
        # ACCEPT LAN --> INTERNET (Incluya los puertos que quiera permitir)
        #       https://www.iana.org/assignments/service-names-port-numbers/service-names-port-
numbers.txt
        $iptables -A FORWARD -s $local/$netmask -i $lan -p tcp -m multiport --dports 80,8080 -o
$internet -j ACCEPT

        # 443 Filter (Solo se permiten sitios https de la acl whiteip.txt)
        #for ip in $(sed '/#.*/d' $route/whiteip.txt); do
  #  if echo $ip | grep -q "-" >/dev/null; then
  #    $iptables -w -A FORWARD -s $local/$netmask -i $lan -o $internet -p tcp --dport 443 -m
iprange --dst-range "$ip" -j ACCEPT
        #  else
  #      $iptables -w -A FORWARD -s $local/$netmask -i $lan -o $internet -p tcp --dport 443 -d $ip
-j ACCEPT
        #  fi
  #done
done
$iptables -A INPUT -i $lan -p tcp --dport $proxyport2 -j DROP
$iptables -A FORWARD -p tcp -m multiport --dports 80,8080,443 -o $internet -j DROP
```

Proyecto Blackip for Ipset: Gateproxy incluye un script en **/etc/init.d/blackip.sh** que actualiza semanalmente y que descarga las bases de datos **geoip** para **iptables/ipset**. Tampoco viene activa por defecto la regla por defecto de Ipset en el script de Iptables.
Lo anterior se debe a que este tipo de filtrado consume muchos recursos de sistema.
Para activar la regla **Ipset**, edite el script de iptables (**/etc/init.d/iptables.sh**) y realice las siguientes modificaciones:
Si va a utilizar solamente la 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
# Descomente esta linea si desea bloquear paises enteros
#for ip in $(cat /etc/zones/{cn,ru}.zone /etc/acl/blackip); do
# Descomente esta linea si desea bloquear solo ips (recomendado)
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:

```
# Descomente esta linea si desea bloquear paises enteros
for ip in $(cat /etc/zones/{cn,ru}.zone /etc/acl/blackip); do
# Descomente esta linea si desea bloquear solo ips (recomendado)
# for ip in $(cat /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 (que viene activa por defecto):

```
# ips permitidas y restringidas
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/whiteips.txt**. Puede editar manualmente esta ACL e incluirle las IPs adicionales o rangos CIDR que quiera excluir.

Importante sobre filtrado por IP: El filtrado por ips en un proxy transparente no garantiza la protección de su red local. Por ejemplo, las direcciones ips usadas por youtube.com, son las mismas que regularmente utilizan otros servicios de Google, por lo tanto si bloquea estas ips, eventualmente puede comprometer los demás servicios de Google.
También hay que destacar que muchas de estas ips son dinámicas y pueden cambiar sin previo aviso, por lo que el operador deberá estar revisando constantemente los rangos autorizados en la acl **whiteip (aquí también se incluye el rango de la red local)**
El abuso de esta regla de filtrado por ips trae como consecuencia la ralentización de su servidor. Para mayor información visite el proyecto Blackip

DNS-LOCAL
Gateproxy ofrece la posibilidad de instalar servidor DNS-LOCAL (dnsmasq) durante el proceso de instalación, (Desea instalar el servidor DNS-LOCAL dnsmasq), sin embargo tenga en cuenta que su uso demandará gran cantidad de recursos de su sistema (no se

recomienda en VMs o en sistemas físicos con menos de 4 núcleos en el procesador y 16 GB RAM)
Si después de instalado desea desactivar el DNS-LOCAL para usar DNS-PUBLIC debe modificar los siguientes archivos de configuración:

ARCHIVO	EJEMPLOS DE REGLAS A MODIFICAR

/etc/init.d/iptables.sh	# DNS-LOCAL (cambiar a DNS-PUBLIC)
	dns="8.8.8.8 8.8.4.4"

/etc/squid/squid.conf	# DNS-LOCAL (cambiar a DNS-PUBLIC) dns_nameservers 8.8.8.8 8.8.4.4 # tcp_outgoing_address 192.168.1.10 # udp_outgoing_address 192.168.1.10
/etc/init.d/leases.sh	ServDNS=8.8.8.8,8.8.4.4

/etc/dnsmasq.conf	# DNS Settings (upstream servers)
	# server=/localnet/192.168.1.10
	server=8.8.8.8
	server=8.8.4.4

Por defecto, el servidor Dnsmasq no lee la información de /etc/hosts y de /etc/resolv.conf, para evitar posibles conflictos, sin embargo, si tiene configuraciones personalizadas en estos archivos, se recomienda activar su lectura realizando la siguiente acción:**ARCHIVO**	**EJEMPLOS DE REGLAS A MODIFICAR**
/etc/dnsmasq.conf	# 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)
Ante la oleada de virus transmitidos por dispositivos usb (pendrives, celulares conectados a usb de equipos, etc) se hace necesario dentro de la red local, tener una carpeta compartida pública para el intercambio de archivos y así evitar el contagio de malware vía usb.
Durante la instalación se le preguntará:
Desea instalar samba (carpeta compartida, papelera y auditoria)? (s/n)
En caso de que acepte, se instalará samba y todos los equipos de su red local tendrán acceso a esta carpeta. Puede conectarla como unidad de red, accediendo a su red local y haciendo doble click en el nombre de su servidor y ahí encontrará un directorio llamado "**compartida**".
Para evitar el mal uso de este directorio, hemos incluido unas restricciones a ciertos tipos de archivos, tales como /*.mp3/*.wmv/*.wma/*.mpg/*.3gp/*.mpeg/*.mkv/*.rmvb/*.flv/*.avi/. Si quiere cambiar este comportamiento puede editar el archivo de configuración de samba (**/etc/samba/smb.conf**) buscar al final del mismo, donde se encuentra declarada la

carpeta compartida, y hacerle los cambios que considere, en dependencia de sus necesidades.
Adicionalmente, se ha creado un directorio papelera de reciclaje (**recycle**), el cual está oculto a simple vista dentro del directorio **compartida** (debe seleccionar "ver archivos ocultos" para poder acceder) donde se almacenarán los archivos eliminados, ordenados por usuarios y con la fecha de la eliminación.
La papelera de reciclaje, está programada para ser vaciada semanalmente (archivos que tengan más de 7 días). Si quiere modificar este comportamiento, acceda al crontab (**sudo crontab –e**) y modifíquelo según sus necesidades.
@weekly find /home/tu_usuario/compartida/recycle/* -mtime +7 -exec rm {} \;
Por último, para un mayor seguimiento de esta carpeta pública, hemos habilitado por defecto el acceso a los registros de la misma (ej: http://192.168.1.10:11200)
Ahí podrá visualizar fecha y hora de eliminación, modificación, lectura, etc, tanto de directorios como de archivos.
En el siguiente ejemplo hemos creado un archivo llamado prueba.txt. El log muestra los registros de creación, previsualización y borrado de este archivo:

Ejemplo de smbdaudit.log

```
Feb  6 17:40:19 localhost smbd_audit: 192.168.1.41|user|compartida|pwrite|ok| prueba.txt
```

Nomenclatura de smbdaudit.log
mkdir: Creación de carpetas/directorios
rmdir: Borrado de carpetas/directorios
pread: Archivos abiertos (lectura)
pwrite: Nuevos ficheros (creados o subidos)
rename: Renombrado de archivos
unlink: Borrado de archivos
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**

SEGURIDAD ADICIONAL:
Dentro de la sección **PAQUETES OPCIONALES** el script de instalación contiene algunos módulos y aplicaciones de seguridad, pero no se encuentran activos o se encuentran parcialmente activos, como Fail2ban, Mod Security, OWASP, Evasive y Rootkit checkers, ya que para manejarlos el usuario debe tener conocimientos avanzados.
Si eligió instalarlos durante el proceso de instalación de Gateproxy y quiere activarlos, realice los siguientes cambios:
Mod Security: **Edite /etc/modsecurity/modsecurity.conf**, busque la variable **SecRuleEngine** y cámbiela de **DetectionOnly** a **On**.
Tenga presente que ModSecurity genera muchos falsos positivos y puede experimentar bloqueos y ralentización en la navegación de los usuarios y en el mismo servidor, sobre todo si accede a direcciones ip (127.0.0.1) o páginas localhost, etc. Para solucionarlo, deberá supervisar constantemente los logs de Apache (**tail /var/log/apache2/error.log**) para hacer los cambios que se indican y mejorar la seguridad de su red local. Si no sabe qué hacer ante los mensajes de **error.log** generados por ModSecurity, se recomienda

que deje ModSecurity por default, sin embargo esto dejará expuesto a Apache y la seguridad de su red local disminuirá. También puede monitorizar gráficamente el módulo de seguridad (ModSecurity), utilizando el aplicativo Waf-fle, (no incluido). Consulte la documentación.

Mod evasive: Este módulo 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.
Fail2ban: Este aplicativo viene por defecto con algunas reglas básicas activas, para la protección de apache, ssh, etc. Puede editarlo /etc/fail2ban/jail.conf para autorizar (cambiar **false** por **true**) algunas jaulas que vienen inactivas o puede agregar nuevas. Tenga presente que por cada cambio de **false** a **true** que realice en una jaula, esta debe tener su respectivo filtro y log debidamente configurado.
La alteración de estos archivos de configuración puede llevar al mal funcionamiento de su servidor.

Ayudas Adicionales
Puede crear su propia VM (vdi) con virtualbox o una imagen ISO de GateProxy LiveCD con Systemback o gdiskdump, ambas incluidas en Gateproxy. Para Systemback, consulte el tutorial linuxirun.com.
Puede recibir soporte (gratuito) visitando el portal gateproxy.com o la sección Help Desk para soporte personalizado (pago) y lo ayudaremos en el proceso de creación, configuración y/o migración de su servidor.

DIRECTORIOS

proxy	/etc/proxy	Directorio que contiene los archivos de autoconfiguración del proxy wpad.dat, proxy.pac y wdad.da
acl	/etc/acl	Directorio donde se encuentran todas las acls de sistema
scripts	/etc/init.d	Directorio donde se encuentran todos los scripts utilizados por gateproxy

SCRIPTS INCLUIDOS

Nombre	Ruta	Tarea/ Ejecución	Función
backup	/etc/init.d	semanal	Se encarga de realizar backup a la mayoría de los archivos de configuración del servidor. Los comprime en un zip y los guarda en **/home/tu_usuario/ backup.** Para cambiar esta ruta debe editar el script **/etc/init.d/backup**
cleaner.sh	/etc/init.d	diario	Se encarga de eliminar archivos encryptable.zone, Thumbs.db, informes de crash antiguos, limpia la ram y la swap
geoip.sh	/etc/init.d	semanal	Descarga la base de datos para **ntopng**
iptables.sh	/etc/init.d	Cada 10 min (aprox)	Contiene las reglas de firewall iptables
leases.sh	/etc/init.d	Cada 10 min (aprox)	Controla el servidor **DHCP**, por tanto el operador **NO** debe manipular el archivo **/etc/dhcp/dhcpd.conf.** Este script captura los arrendamientos del servidor **DHCP** y los inyecta al archivo de configuración **dhcpd.conf** y a la acl **blackdhcp.** Si el administrador del servidor no toma ninguna decisión (copiar de la acl **blackdhcp** a la acl **macslocal y macsprivilegiadas**) en el tiempo estipulado en la columna **tarea,** el script correrá nuevamente eliminando el terminal del **dhcpd.leases** y no le será arrendada ip nuevamente.
lock.sh	/etc/init.d	inicio	Evita que la ejecución de varias instancias de un mismo script
servicesreload.sh	/etc/init.d	Cada 10 min (aprox)	Vigila los servicios esenciales del servidor (isc-dhcp-server, Squid, Apache2, ntopng, redis-server, etc) y en caso de que alguno caiga, lo levanta
updatehour.sh	/etc/init.d	inicio	Actualiza y sincroniza la hora del servidor
vm	/etc/init.d	inicio	Inicia o detiene las VMs que tenga en su servidor (Virtualbox). Si quiere programar su vm para que sea la primera en iniciar y la última en cerrar (recomendado), edite /etc/init.d/vm y reemplace

			VMNAME="my_vm_name" por el nombre de su máquina
blackweb.sh	/etc/initd	semanal	Se encarga de actualizar semanalmente la lista de dominios bloqueados por default. Para mayor información visite el proyecto blackweb
blackip.sh	/etc/init.d	semanal	Se encarga de actualizar semanalmente la lista negra de IPs. Para mayor información visite el proyecto Blackip

ACLS INCLUIDAS

Nombre (.txt)	Ruta	Dependencia	Función
blackip	/etc/acl	Ipset/iptables	Contiene las ips o rangos de ips que el operador quiere bloquear. Si abusa de esta acl, incluyéndole muchos rangos, puede comprometer su sistema.
blackdhcp	/etc/acl	Iptables/dhcp	Contiene los terminales que entran por defecto bloqueados a su red local, hasta tanto el operador (administrador) del servidor no los saque de esta "lista negra" y los incluya en la acl **macslocal** o en la acl **macsprivilegiadas**
blackstring	/etc/acl	iptables	Contiene strings a bloquear (de programas proxy como ultrasurf, etc). Esta es una acl de sistema y no debe ser manipulada. Puede actualizarla en el post Firewall.
whiteip	/etc/acl	blackips.sh ipset/iptables squid	En esta acl contiene ips (o rangos de ips) "blancos". Sirve para excluir ips del bloqueo que realiza ipset en el firewall iptables. Si su proxy es transparente, también sirve para permitir el paso de estas ips por squid (proxy) e iptables (firewall) y el resto queda cerrado por default. Si desea autorizar el paso de alguna ip (http/s) de un sitio web (o rango de ips) hacia su red local, puede agregarlo manualmente en esta acl.
blackweb	/etc/acl	Squid	Esta es una acl de sistema y no debe ser manipulada. Contiene más de 2 millones de sitios web bloqueados. Está programada para actualizarse semanalmente. Para mayor información visite blackweb
blackdomains	/etc/acl	Squid	Esta acl hace exactamente lo mismo que **blackweb**, pero está diseñada para que el operador del servidor proxy pueda agregar manualmente NUEVOS sitios quiera bloquear **NO** incluidos en la acl **blackweb.**

dhcp_ips	/etc/acl	dhcp/iptables	Esta es una acl de sistema y no debe ser manipulada
dhcp_macs	/etc/acl	dhcp/iptables	Esta es una acl de sistema y no debe ser manipulada
blackext	/etc/acl	squid	Contiene una lista de las extensiones más usadas de archivos a bloquear, para impedir descargas de archivos con este tipo de extensiones en su red local por **url_regex**. Edítela agregue o quite extensiones. Por defecto se bloquean extensiones de multimedia, ejecutables, ransomware, entre otras
blackmime	/etc/acl	squid	Lo mismo que **blackext** pero por **mime_type.** Edítela y comente las extensiones que no vayan a ser objeto de bloqueo y puede agregar nuevas. Por defecto se bloquean una gran cantidad de extensiones.
macslocal	/etc/acl	dhcp/iptables	Contiene los terminales autorizados que el operador (administrador) del servidor permitió entrar a su red local, sin importar que tengan ip estáticas o dinámicas (ambas asignadas por dhcp). Los terminales se agregan manualmente.
macsprivilegiadas	/etc/acl	dhcp/iptables	Contiene los terminales autorizados que el operador (administrador) del servidor permitió entrar a la red local y que no están sujetos a restricciones, ya que no pasan por el firewall. Los terminales se agregan manualmente.
blackwords	/etc/acl	squid	Contiene un listado de palabras a bloquear en el squid. Por ejemplo, si algún usuario digita en el buscador la palabra porno o intenta ingresar a algún sitio que contenga esa palabra en la url, squid bloqueará el acceso. **Tenga especial cuidado en las palabras que incluye en esta acl o puede generar falsos positivos**.
whitedomains	/etc/acl	squid	Contiene la lista de exclusiones de dominios. Por default está vacía. Si su squid está bloqueando alguna página que quiera autorizar, la debe incluir en esta acl y reportar el incidente en el proyecto Blackweb
ipsreservadas	/etc/acl	iptables	Esta acl es de sistema y no debe ser modificada. Contiene ips anti-spoofing

PROBLEMAS CONOCIDOS

ERROR	DESCRIPCION DEL PROBLEMA	SOLUCION
El comando: sudo service networking restart no funciona	Afecta a Ubuntu	Ubuntu tiene un bug. Se recomienda utilizar ips estáticas. Sin embargo bajo su propio riesgo, puede usar la siguiente solución: Para apagar y levantar interfaces: **sudo ifdown eth0 && sudo ifup eth0** Para usar **sudo service networking restart** ejecute: **sudo apt-get install git** **sudo git clone https://github.com/metral/restore_networking.git** **cd restore_networking/** **sudo ./restore_networking.sh** **sudo service networking restart** networking stop/waiting networking start/running Para mayor información visite: Restore Networking
Modo Promiscuo	Las interfaces de red entran en modo promiscuo	No utilice tcpdump y wireshark (desinstalar)
DHCP Error Ip duplicate	El servidor dhcp en ocasiones asigna ips que ya se encuentran declaradas en el **dhcpd.conf**	Si son ip fijas, edite el archivo donde se encuentre el terminal en conflicto (macslocal o macsprivilegiadas) y cambie el número de ip a un rango por fuera del asignado en el dhcp, guarde cambios y reinicie. El rango dhcp está declarado en el script **/etc/init.d/leases.sh**. Por defecto es **192.168.1.100 a la 250**. Puede reducirlo o utilizar las IPs por debajo de la **.100** para ingresar terminales manualmente.
DNS no resuelve	Proxy incapaz de resolver peticiones a servidores internos. Solo se presenta en proxy manual. Si el proxy es transparente no se presenta este problema. ejemplo: http://nombre_host:8090/xxx/	En la configuración de los navegadores marcar la opción: "**no usar servidor proxy para direcciones locales**"
FATAL: Bungled /etc/squid/squid.c	Se detiene el squid	Comentar en el squid.conf las líneas relacionadas con qos

onf qos flows disable-preserve-miss		# qos_flows disable-preserve-miss Por defecto ya están comentadas estas líneas
fail2ban.filter : ERROR Unable to open /var/log/squid/access.log y auth.log	Fail2ban presenta problemas al acceder al log de squid access.log y auth.log	Reiniciar fail2ban sudo service fail2ban restart Aumente el número de jaulas. Por defecto el valor está en 256 /proc/sys/fs/inotify/max_user_instances Revise si ha activado alguna jaula adicional a las que trae jail.conf por defectos ya que pueden estar mal configuradas
fail2ban.actions.action: ERROR iptables (etc) fail2ban.jail: INFO Jail 'apache-overflows' stopped	Error de Fail2ban, relacionado con las jaulas e iptables, registrado en el log: **/var/log/fail2ban.log**	Reemplazar el comando **sudo service fail2ban restart** Por: **sudo service fail2ban stop && sleep 3 && sudo service fail2ban start**.
E: Sub-process /usr/bin/dpkg returned an error code (1)	Error al instalar un paquete	Abra el terminal, ingrese a /var/lib/dpkg/info Elimine todas las referencias al paquete con sudo rm –rf nombre_del_paquete sudo rm /var/cache/debconf/*.dat
W: No se podrán ignorar los privilegios para descargar mientras no se pueda acceder a «/var/lib/update-notifier/package-data-downloads/partial/arialb32.exe» con el usuario «_apt». -pkgAcquire::Run (13: Permiso denegado)	Error al instalar un paquete	Abra el terminal y elimine el contenido de /var/lib/update-notifier/package-data-downloads/partial/ con sudo rf *.*
VBoxNetFlt: Failed to allocate packet buffer, dropping the packet	Problemas con el buffer de Virtuabox. No afecta el funcionamiento de Virtualbox **/var/log/syslog**	**BUG. Pendiente de solucionar** https://code.launchpad.net/~mitya57/ubuntu/precise/virtualbox/4.1.12-dfsg-2ubuntu0.3/+merge/153346

Bugs

Aplicativo	Enlace	Descripción del problema	Nota
Psad	http://cipherdyne.org/psad/	Possible precedence issue with control flow operator at /usr/sbin/fwcheck_psad line 193	Retirado provisionalmente

AGRADECIMIENTOS

Agradecemos a todos aquellos que, directa o indirectamente, contribuyeron con la realización de este proyecto

http://www.novatoz.com
http://www.alterserv.com/foros/index.php
https://www.google.com
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://glx-dock.org/
http://gparted.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://ww.jose-linares.com
http://dasubipar.blogspot.com
http://www.joanemarti.com
http://arpon.sourceforge.net/
https://github.com/da667/Autosnort
https://www.bestvpn.com
http://wiki.syspass.org/es/instalar
https://klaver.it/linux/sysctl.conf
http://www.hackplayers.com