

## GATEPROXY

Gateproxy is a simple proxy/firewall server for managing Pyme's LAN networks. 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. It can be implemented in physical servers or VMs, for greater flexibility and portability.

Gateproxy es un sencillo servidor proxy/firewall para administrar redes Pyme's LAN. 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. Puede ser implementado en servidores físicos o VMs, para mayor flexibilidad y portabilidad.

We thank all those who have contributed to this project / Agradecemos a todos aquellos que han contribuido a este proyecto



© 2023 [maravento](https://maravento.com) se distribuye bajo una [Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/).

### Disclaimer

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.

## TABLE OF CONTENTS / TABLA DE CONTENIDOS

START AND MINIMUM REQUIREMENTS.....	2
PACKAGES.....	3
PACKAGES.....	4
POST-INSTALL .....	8
FILES.....	16

## START AND MINIMUM REQUIREMENTS

GNU/Linux:	Ubuntu 22.04
Processor:	Intel compatible 1x GHz
Interfaces:	2: (Public and Local)
RAM:	4 GB reserved for Squid-Cache
HDD/SSD:	100 GB reserved for Squid-Cache
Language:	eng-spa
Internet:	High speed (recommended)



```

Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Bienvenido a GateProxy

Requisitos Minimos:
GNU/Linux:  Ubuntu 22.04.x x64
Processor:   Up to Intel 1x GHz
Interfaces:  Public and Local
RAM:         4 GB reserved for Squid-Cache
HDD/SSD:     100 GB reserved for Squid-Cache

Presione ENTER para iniciar o CTRL+C para abortar

```

Open the terminal, run the following command and follow the instructions on the screen / Abra el terminal, ejecute el siguiente comando y siga las instrucciones en pantalla:

```
wget -q -N https://github.com/maravento/gateproxy/raw/master/gateproxy.sh && sudo
chmod +x gateproxy.sh && sudo ./gateproxy.sh
```

At the end of the installation of all the selected modules (depending on your internet connection), the Gateproxy installation ends / Al finalizar la instalación de todos los módulos seleccionados (en dependencia de su conexión a internet) termina la instalación de Gateproxy.

```
Fin de la instalacion. "Presione ENTER para reiniciar..."
```


## PACKAGES

Step	Packages
Pre-Install	nala curl software-properties-common apt-transport-https aptitude net-tools mlocate plocate git git-gui gitk subversion gist systemd-timesyncd
Essential	gpated libfuse2 nfs-common ntfs-3g exfat-fuse tzdata tar p7zip p7zip-full p7zip-rar rar unrar unzip zip unace cabextract arj zlib1g-dev gawk gir1.2-gtop-2.0 gir1.2-xapp-1.0 javascript-common libjs-jquery libxapp1 rake ruby ruby-did-you-mean ruby-json ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit rubygems-integration xapps-common python3-pip libssl-dev libffi-dev python3-dev python3-venv idle3 python3-psutil geoip-database neofetch ppa-purge gdebi synaptic pm-utils sharutils wget dpkg pv libnotify-bin inotify-tools expect tcl-expect tree preload xsltproc debconf-utils mokutil uuid-dev libmnl-dev conntrack mesa-utils gcc make autoconf autoconf-archive autogen automake pkg-config deborphan perl lsof finger logrotate linux-firmware util-linux linux-tools-common build-essential module-assistant linux-headers-\$(uname -r) reiserfsprogs reiser4progs xfsprogs jfsutils dosfstools e2fsprogs hfsprogs hfsutils hfsplus mtools nilfs-tools f2fs-tools quota sshfs lvm2 attr jmpfs
Server	isc-dhcp-server php apache2 apache2-doc apache2-utils apache2-dev apache2-suexec-pristine libaprutil1 libaprutil1-dev squid squid-langpack webmin glances nbtscan libpcap-dev libasound2-dev libfontconfig1 sniffnet libcgi-session-perl libgd-gd2-perl lightsquid sarg fonts-liberation fonts-dejavu cockpit cockpit-storaged cockpit-networkmanager cockpit-packagekit cockpit-machines cockpit-sosreport virt-viewer ipset ddos ulogd2 rsyslog timeshift freefilesync
Samba with Recycle Bin and Audit (ask)	samba samba-common samba-common-bin smbclient winbind cifs-utils


## PACKAGES


### WEBMIN

Access <https://localhost:10000>

 **Webmin 1.791**  
 192.168.1.10

Please, sign in with your account to manage this server





☐ Remember me
 

Sign in

### Lightsquid

Access: <http://localhost/lightsquid/>

localhost/lightsquid/index.cgi
80% ☆

## Squid user access report

📅 Work Period: **Sep 2022**

**📅 Calendario**

Cambiar Fecha  
 2022  
 01 02 03 04 05 06 07 08 09 10 11 12

**📊 Ranking**

Top Sites	Total	Group
YEAR	YEAR	YEAR
MONTH	MONTH	MONTH

**📊 Estadísticas Generales**
HERRAMIENTAS

10 entradas
Buscar:

Date	Group	Users	Oversize	Bytes	Average	Hit %
30 Sep 2022	grp	64	51	2.7 G	43.7 M	7.33%
29 Sep 2022	grp	21	6	347.1 M	16.5 M	3.89%
<b>Total/Average:</b>		<b>42</b>	<b>28</b>	<b>3.1 G</b>	<b>30.1 M</b>	<b>5.61%</b>

Mostrando 1 de 2 de 2 entradas
Previous 1 Next

## SARG Monitor: (programmable reports)

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

Important:

Your server must register traffic before generating the first SARG report, otherwise no report will appear For the first time you must execute: / Su servidor debe registrar tráfico antes de generar el primer reporte de SARG, de lo contrario no aparecerá ningún reporte Por primera vez debe ejecutar:

```
sudo sarg-reports today
```

o

```
sudo sarg -f /etc/sarg/sarg.conf -l /var/log/squid/access.log
```

Or go to webmin, to the section "Servers" and then "Report Generator and Squid Analysis" and finally click "Generate report now". In the following image we see the daily SARG report of a computer on the local network. As an example, we have blocked Facebook and the report indicates this blocking with the message DENIED. To modify 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 with `sudo squid -k reconfigure` or run the script `sudo /etc/scr/serverload.sh` or from Webmin, in the System / Start and Stop section

O 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.txt` y añada el sitio que quiera autorizar de acuerdo a sus necesidades, guarde los cambios y reconfigure el squid con `sudo squid -k reconfigure` o ejecute el script `sudo /etc/scr/serverload.sh` o desde Webmin, en la sección de Sistema/ Arranque y Parada.

Domain	Bytes	Packets	Errors	Rate	Denied
ads-afreem.com	170	249,494	0.73%	100.00%	00:05:09 309,740 0.61%
static-tilt.com:443	26	236,124	0.70%	100.00%	00:01:23 19,210 0.19%
www.gateic.com:443	2	213,856	0.67%	100.00%	00:01:28 16,614 0.19%
fortis.gateic.com	14	209,576	0.61%	100.00%	00:00:36 36,238 0.07%
static-foodanddrink-eus.s-man.com	10	204,778	0.60%	100.00%	00:00:24 24,326 0.09%
es.yahoo.com:443	2	203,214	0.60%	100.00%	00:00:28 26,938 0.09%
www.mon.com	4	199,088	0.58%	100.00%	00:00:14 14,826 0.03%
u.dynad.net	12	165,484	0.48%	100.00%	00:00:29 29,274 0.08%
net.gateic.com:443	4	163,788	0.48%	100.00%	00:01:07 67,492 0.13%
clients.google.com:443	4	146,244	0.43%	100.00%	00:14:24 864,748 1.70%
cache-paek.google.com	32	138,024	0.40%	100.00%	00:00:00 0 0.00%
www.facebook.com:443	32	116,736	0.34%	100.00%	00:00:00 0 0.00%
static.googleusercontent.com:443	4	110,236	0.32%	100.00%	00:00:00 0 0.00%
login.live.com:443	14	109,176	0.32%	100.00%	00:01:42 102,336 0.20%
u.yimg.com:443	6	102,608	0.30%	100.00%	01:30:42 5,442,954 10.68%
www.quebaconagra.com	8	102,188	0.30%	100.00%	00:00:19 19,222 0.04%
www.youtube-nocookie.com:443	6	86,736	0.25%	100.00%	00:02:08 128,364 0.25%
gpx.aspreth.com	2	84,824	0.25%	100.00%	00:00:07 7,940 0.02%
analytics.mistatic.com	2	81,656	0.24%	100.00%	00:00:08 8,522 0.02%
www.youtube.com:443	22	80,164	0.23%	100.00%	00:00:00 0 0.00%
partner.googleadservices.com	2	69,656	0.20%	100.00%	00:00:07 7,834 0.02%
fortis.gateic.com:443	2	69,244	0.20%	100.00%	00:00:45 49,348 0.09%
gpx.googleads.com	2	66,856	0.20%	100.00%	00:00:08 6,074 0.01%
msn-d2-g.mistatic.com	20	64,904	0.19%	100.00%	00:00:42 42,204 0.08%
www.memadobres.com.co	4	64,688	0.19%	100.00%	00:00:09 9,398 0.02%
ctid.windowsupdate.com	16	60,488	0.18%	100.00%	00:00:00 0 0.00%

## DDoS Deflate

Protects the local network from DDoS attacks, banning internal IPs / Protege de ataques DDoS la red local, baneando IPs internas. Default: BAN\_LIMIT=180 BAN\_PERIOD=120

To modify ban time / Para modificar tiempo de baneo: `/usr/local/ddos/ddos.conf`

To exclude IPs from the ban / Para excluir IPs del baneo: /usr/local/ddos/ignore

Log: /usr/local/ddos/ddos.log

/usr/local/ddos/ddos.log

---

Últimas  líneas de

Mostrar sólo las líneas que contengan el texto

---

```

BANNED: 192.168.1.56 with 181 connections ()
WARNING: 179.58.3.7 with 124 connections (desarrollo.eduardono.com.)

Banned the following ip addresses on jue may 17 17:14:01 -05 2018
WARNING: 192.168.1.56 with 140 connections ()
WARNING: 204.11.58.39 with 79 connections (bh-48.webhostbox.net.)

Banned the following ip addresses on jue may 17 17:15:01 -05 2018
WARNING: 192.168.1.56 with 101 connections ()

Banned the following ip addresses on jue may 17 17:16:01 -05 2018
WARNING: 192.168.1.56 with 120 connections ()

Banned the following ip addresses on jue may 17 17:20:01 -05 2018
WARNING: 192.168.1.66 with 74 connections ()

Banned the following ip addresses on jue may 17 17:28:01 -05 2018
WARNING: 192.168.1.32 with 94 connections ()

Banned the following ip addresses on jue may 17 17:29:01 -05 2018
WARNING: 192.168.1.32 with 120 connections ()
WARNING: 52.184.182.228 with 91 connections ()

Banned the following ip addresses on jue may 17 17:33:01 -05 2018
WARNING: 192.168.1.38 with 175 connections ()
WARNING: 52.184.182.228 with 115 connections ()

Banned the following ip addresses on jue may 17 17:36:04 -05 2018
WARNING: 192.168.1.37 with 83 connections ()
    
```

Últimas  líneas de

Mostrar sólo las líneas que contengan el texto

---

## Shellinabox

Access: <https://localhost:4242>.

For more information read / Para más información lea [HERE](#)

```

← → ↻ ⚠ No seguro | https://localhost:4242
mstudio login: mstudio
Password:
Login incorrect
mstudio login: user
Password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Meltdown, Spectre and Ubuntu: What are the attack vectors,
   how the fixes work, and everything else you need to know
   - https://ubuntu.com/knownissues

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

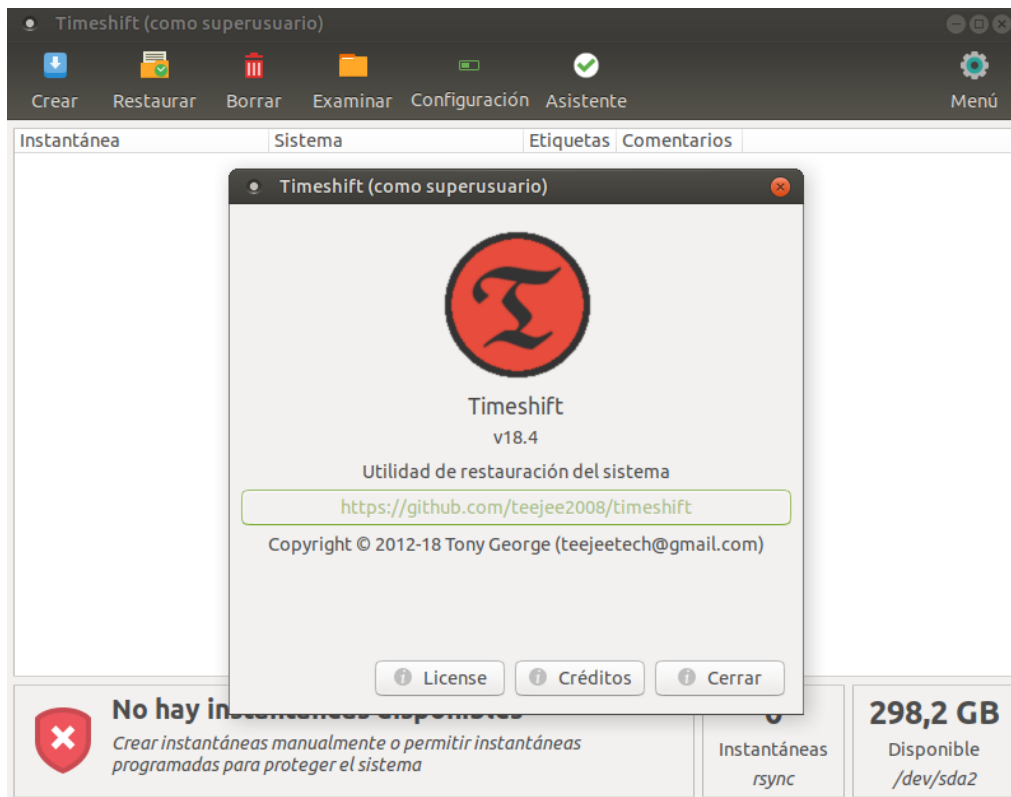
Pueden actualizarse 0 paquetes.
0 actualizaciones son de seguridad.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

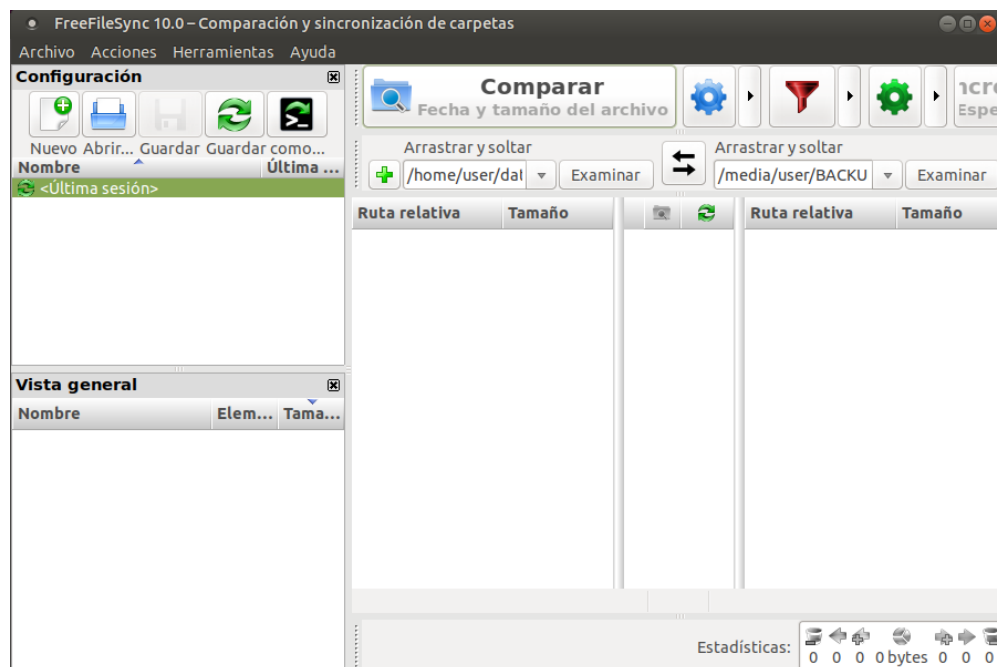
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

user@mstudio:~$ upgrade
[sudo] contraseña para user:
Ign:1 http://dl.google.com/linux/chrome/deb stable InRelease
Ign:2 http://download.webmin.com/download/repository sarge InRelease
Ign:3 http://dl.google.com/linux/chrome/deb stable InRelease
    
```

## Timeshift



## FreeFileSync





## POST-INSTALL

### DHCP

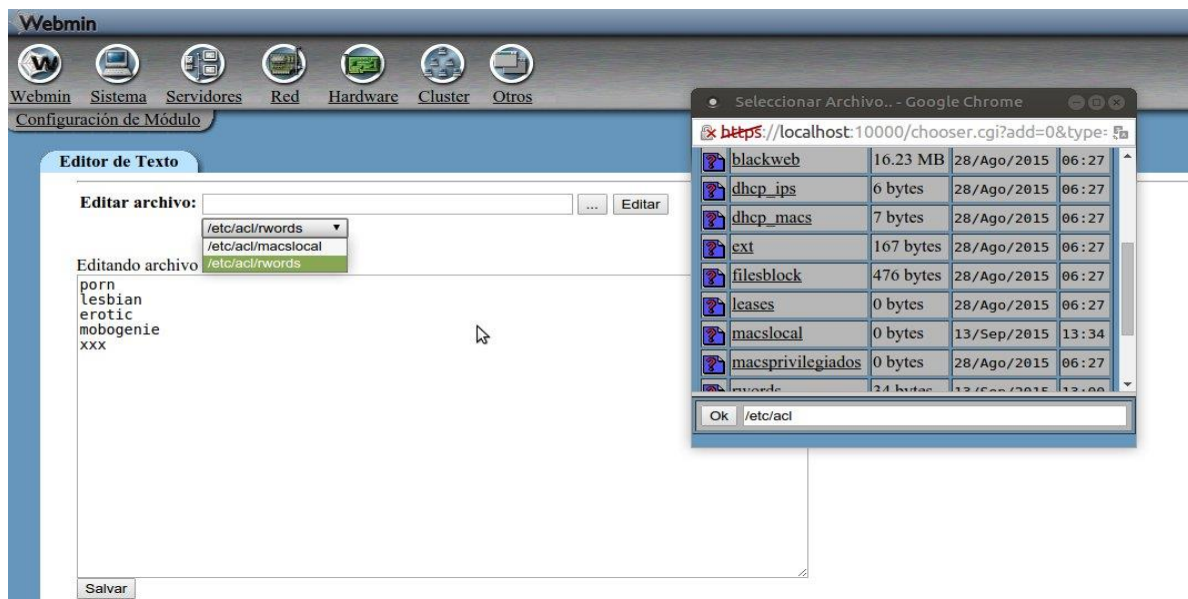
The DHCP server automatically leases IP addresses to all the terminals that enter its local network. The lease range is set by the `/etc/sr/leases.sh` script. You can increase or decrease this range by editing the script. The policy established by default is that all PCs, which the DHCP server leases an IP address, enter the local network denied, included in the `acl /etc/acl/blackdhcp.txt` with the format: / 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/sr/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.`

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

If after 20 minutes (this time can be adjusted in `crontab`) the server operator does not authorize the entry to the local network of the terminals in the `acl` in `/etc/acl/blackdhcp.txt`, the DHCP server will block them permanently and not will re-lease an IP address / Si pasados 20 minutos (este tiempo puede ser ajustado en `crontab`) 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.

To authorize entry to the local network of terminals, edit the `acl /etc/acl/blackdhcp.txt` and copy and paste the authorized terminal to the `acl` of your choice (see table ACLs). For more convenience you can install the webmin [Text-Editor](#) module (Webmin Configuration / Webmin Modules and load from ftp or http URL). / 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` de su preferencia (ver tabla ACLs). Para mayor comodidad puede instalar el módulo de webmin [Text-Editor](#) (Configuración de Webmin/Módulos de Webmin y cargar desde dirección URL ftp o http).



## BACKUP

The /etc/scr/bkconf script is used for backup. By default it includes the paths to the essential configuration files. You can edit it to add more files or change the backup path to your preferred destination (external media, the cloud, etc). You can change the periodicity of its execution in crontab (sudo crontab -e). By default it runs daily. / El script /etc/scr/bkconf se utiliza para realizar copias de seguridad. 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.

## Additional Ports / Puertos Adicionales

The iptables firewall comes by default with the essential ports open and the rest closed. If you want to include more ports for your local network (SMTP / SSMTP, POP3 / POP3S, IMAP / IMAPS, etc) edit the script (sudo nano /etc/scr/iptables.sh), and add or uncomment the ports you want to authorize for your local network.

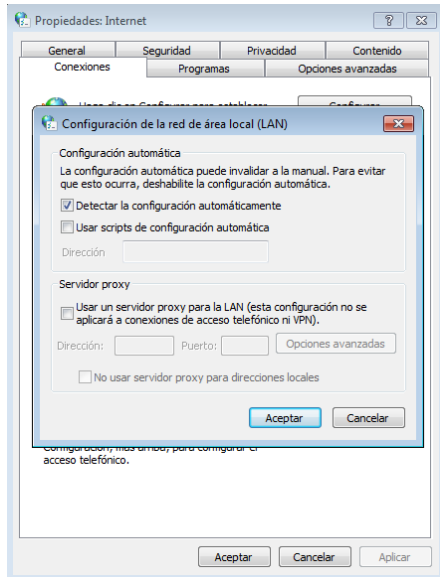
Additionally, the iptables firewall includes an Administration MAC (sysadmin), in case the sysadmin wants to administer the gateproxy server from another terminal. To do this edit the script /etc/scr/iptables.sh and replace the mac sysadmin with that of the administrator PC and you will have access to certain privileged 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/scr/iptables.sh), y agregue o descomente los puertos que quiera autorizar para su red local. Adicionalmente, el firewall iptables incluye una MAC de Administración (sysadmin), para el caso en que el sysadmin quiera administrar el servidor gateproxy desde otro terminal. Para esto edite el script /etc/scr/iptables.sh y reemplace la mac sysadmin por la del PC administrador y tendrá acceso a ciertos puertos privilegiados.

**sysadmin="XX:YY:ZZ:AA:BB:CC"**

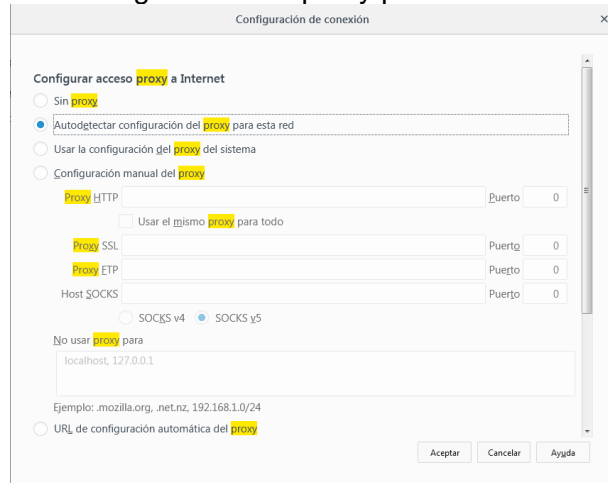
## PROXY

Gateproxy includes [Proxy Auto-Configuration \(PAC\)](#), which uses the DHCP method (option 252) and opens port 8000 in Apache2 for its disclosure. For its operation, you just have to make sure that the box " Automatically detect settings "and in Firefox (Quantum 63x or higher)" Auto-detect proxy settings for this network "(Chrome and Opera take IE settings). / Gateproxy trae incluido [Proxy Auto-Configuration \(PAC\)](#), el cual utiliza el método DHCP (opción 252) y abierto el puerto 8000 en Apache2 para su divulgación. Para su funcionamiento tan solo debe asegurarse que esté seleccionada en la configuración de IE la casilla "Detectar la configuración automáticamente" y en Firefox (Quantum 63x o superior) "Autodetectar configuración del proxy para esta red" (Chrome y Opera toman la configuración de IE).

## IE: Detectar la configuración automáticamente

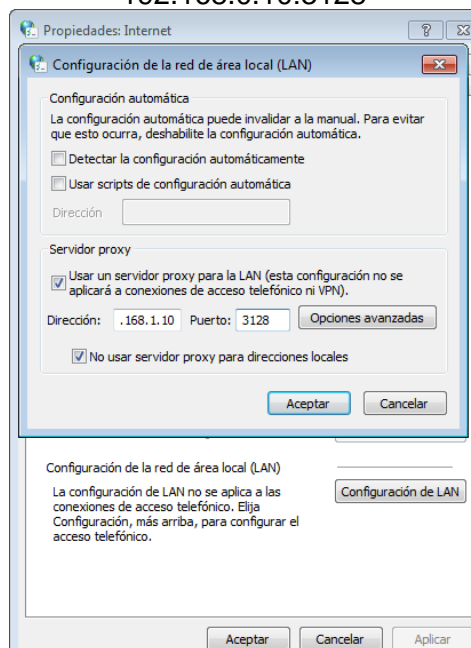


## Firefox 63x o superior: Autodetectar configuración del proxy para esta red

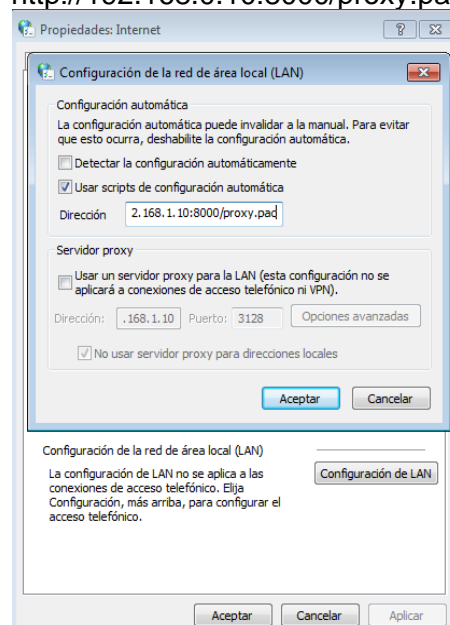


Please note that it is a Microsoft implementation, therefore it is not guaranteed to work in browsers other than IE (see [Browser-Support](#)). In this case, you must specify the url of the PAC or configure the proxy manually. / Tenga en cuenta que es una implementación de Microsoft, por tanto no se garantiza que funcione en otros navegadores diferentes a IE (consulte [Browser-Support](#)). En este caso deberá especificar la url del PAC o configurar el proxy manualmente.

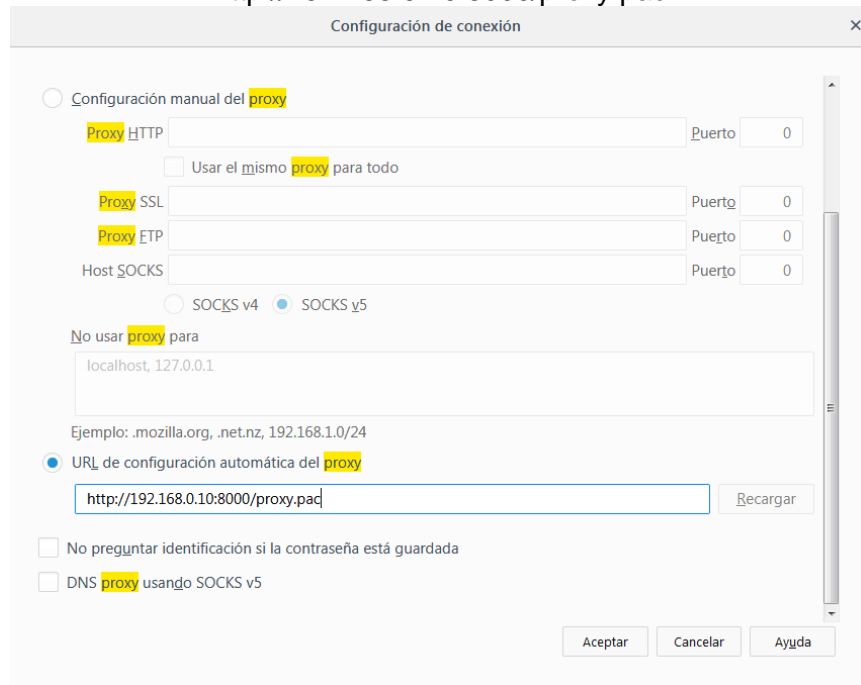
## Manual 192.168.0.10:3128



## URL PAC http://192.168.0.10:8000/proxy.pac



Firefox Mozilla (not required in 63 or higher / no es requerido en 63 o superior)  
http://192.168.0.10:8000/proxy.pac



To reduce compatibility issues, WPAD can replace the proxy IP with its NetBIOS name. To do this, modify the following parameters (replace Gateproxy with the netBIOS hostname of your server): / Para reducir problemas de compatibilidad WPAD puede reemplazar la IP del proxy por su nombre NetBIOS. Para hacerlo modifique los siguientes parámetros (reemplace Gateproxy por el nombre-host netBIOS de su servidor):

<b>Old: /etc/scr/leases.sh</b>	<b>New: /etc/init.d/leases.sh</b>
option wpad	option wpad
"http://192.168.0.10:8000/proxy.pac";	"http://gateproxy:8000/proxy.pac\";

Open NetBIOS ports (e.g.: NetBIOS and SAMBA): / Abrir puertos NetBIOS (ej: NetBIOS y SAMBA):

```
# SAMBA
$Iptables -A INPUT -s $local/$netmask -i $lan -m mac --mac-source $mac- -p tcp -m multiport --dports 137:139,445 -j ACCEPT
$Iptables -A INPUT -s $local/$netmask -i $lan -p udp -m multiport --dports 137:139,445 -j ACCEPT
```

If you want all connections to go through the proxy, including local ones, then the following modifications are recommended: / Si quiere que todas las conexiones pasen por el proxy, incluyendo las locales, entonces se recomienda realizar las siguientes modificaciones:

proxy.pac

<b>/var/www/html/wpap/proxy.pac</b>	<b>/var/www/html/wpap/proxy.pac</b>
function FindProxyForURL(url, host) {	function FindProxyForURL(url, host) {
// If the requested website is hosted within the internal network, send direct.	return "PROXY gateproxy:3128";
if (isPlainHostName(host)    shExpMatch(host, "*.local")	}

```

    isInNet(dnsResolve(host),
"192.168.0.0", "255.255.0.0") ||
    isInNet(dnsResolve(host),
"127.0.0.0", "255.255.255.0"))
    return "DIRECT";
    return "PROXY 192.168.0.10:3128";
}

```

Open local services and ports in squid.conf (replace servername with the name of your local server): / Abrir servicios locales y puertos en squid.conf (reemplace servername por el nombre de su servidor local):

#### **/etc/squid/squid.conf**

```

# example servername
acl servername_port port 8090
acl servername_ip dst 192.168.0.10
http_access allow servername_ip servername_port

```

Declare local service names in the hosts file / Declarar nombres de servicios locales en el archivo hosts

#### **Edite /etc/hosts**

```

127.0.0.1    localhost
127.0.1.1    gateproxy
192.168.0.10 servername

```

### ABOUT WPAD

Note that WPAD is vulnerable (someone can create a rogue wpad server) therefore it is not recommended to use it and instead you must configure browsers manually to point to the proxy. To disable WPAD, remove: / Tenga en cuenta que WPAD [es vulnerable](#) (alguien puede crear un [servidor wpad falso](#)) por tanto no se recomienda usarlo y en su lugar debe configurar los navegadores manualmente para apuntar al proxy. Para desactivar WPAD, elimine:

#### **FILES/DIR**

```

/var/www/html/wpad
/etc/apache2/sites-enabled/
/etc/apache2/ports.conf
/etc/scr/leases.sh
/etc/scr/iptables.sh

```

#### **RULES OR FILES**

```

proxy.pac
proxy.conf
Listen 8000
option wpad code 252 = text;
option wpad \"http://192.168.0.10:8000/proxy.pac\";
8000

```

### Squid-Cache Ports

If during the installation you decided to change the proxy port (by default 3128) you should choose an unreserved port (see the [list of ports](#)). / Si durante la instalación decidió cambiar el puerto del proxy (por default 3128) debe elegir un puerto no reservado (consulte el [listado de puertos](#)).

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

A transparent proxy is a security risk, as the cache can be poisoned with redirected requests. But there are devices that are not compatible with WPAD / PAC (devices with Android or other OS). To solve the connectivity of these devices, Gateproxy includes by default a transparent rule (in Squid and iptables), but it only applies to the mac-transparent ACL (see ACL table). However, keep in mind that squid-cache does not filter https connections (port

443) in transparent mode, therefore the https traffic of the devices included in this list will not be reflected in the Sarg, Sqstat, etc reports (eventually only http) , that is, they will not apply rules such as extension locks and other types of filtering included in squid, since https is an encrypted protocol. To counteract this scenario, Gateproxy brings an additional rule in the iptables firewall, to filter port 443, that is, allow https IPs to pass in the whiteip.txt acl and then the firewall closes this port. This rule is not active by default, as it can crash your system due to the amount of IP addresses that the firewall has to process for each request, so use it at your own risk. / Un proxy transparente es un riesgo de seguridad, ya que la cache puede ser envenenada con peticiones redireccionadas. Pero existen dispositivos que no son compatibles con WPAD/PAC (dispositivos con Android u otros SO). Para solucionar la conectividad de estos dispositivos, Gateproxy incluye por default una regla transparente (en Squid e iptables), pero únicamente aplica para la ACL mac-transparent (ver tabla ACL). Sin embargo, tenga en cuenta que squid-cache no filtra conexiones https (puerto 443) en modo transparente, por tanto el tráfico https de los equipos incluidos en esta lista no aparecerá reflejado en los reportes Sarg, Sqstat, etc (eventualmente solo http), o sea, no aplicarán reglas como bloqueos de extensiones y otros tipos de filtrado incluidos en squid, ya que https es un protocolo cifrado. Para contrarrestar este escenario, Gateproxy trae una regla adicional en el firewall iptables, para filtrar el puerto 443, o sea, permitir el paso de IPs https en la acl whiteip.txt y luego el firewall cierra este puerto. Esta regla no viene activa por defecto, ya que puede hacer colapsar su sistema, por la cantidad de direcciones IPs que tiene que procesar el firewall para cada petición, por tanto úsela bajo su propio riesgo.

#### [Blackip for Ipset](#)

IPset is not active by default, since this filtering consumes many resources and Squid already includes Whiteip. To activate it visit the [Blackip](#) project / IPset no viene activo por defecto, ya que este filtrado consume muchos recursos y Squid ya trae incluido Whiteip. Para activarlo visite el proyecto [Blackip](#)

#### Whiteip

It is recommended to only use the squid blocking rule (it is active by default in Squid): / Se recomienda utilizar solamente la regla de bloqueo de squid (viene activa por defecto en Squid):

```
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
```

The previous rule blocks all IPs by default, and only lets through the IPs found in the ACL /etc/acl/whiteip.txt and in /etc/acl/wextra.txt You can edit the latter manually and include the additional IPs. or CIDR ranges that you want to exclude, that are not in Whiteip / 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 y en /etc/acl/wextra.txt Puede editar esta última manualmente e incluirle las IPs adicionales o rangos CIDR que quiera excluir, que no estén en Whiteip.

#### SAMBA (PUBLIC SHARED, RECYCLING BIN, AND AUDIT / COMPARTIDA PUBLICA, PAPELERA DE RECICLAJE Y AUDITORIA)

File sharing on local networks is essential. To avoid the use of usb devices (and malware via usb) we recommend creating a "Public Shared Folder" to which only members of the local network will have access. By default the "Public Shared Folder" has restricted the storage of certain files (\*.mp3/\*.wmv/\*.wma/\*.mpg/\*.3gp/\*.mpeg/\*.mkv/\*.rmvb/\*.flv / \*.avi /., etc). If you want to modify it, edit /etc/samba/smb.conf and at the end you will find the



restrictions. The Recycle Bin (recycle directory) is hidden inside "Public Shared Folder". The files deleted by users and with the date of deletion will be stored there. It is scheduled to be emptied weekly (files older than 7 days). If you want to modify it, access the crontab (sudo crontab -e) and modify it according to your needs. / 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.

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

For monitoring the "Public Shared Folder", you can access the logs at: http://192.168.0.10:11900, which shows date and time of deletion, modification, reading, of directories and files. In the following example we have created a file called test.txt. The log shows the creation, display and deletion records of this file: / Para el seguimiento de la "Carpeta Compartida Pública", puede acceder a los registros en: http://192.168.0.10:11900, 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:

```
Feb 6 17:40:19 localhost smbdaudit: 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

By default these records are updated daily. If you want to disable or modify this option (you can do it in real time), enter the crontab and delete or modify the line: / 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 smbdaudit /var/log/syslog > /etc/smbdaudit/smbdaudit.log
```

To prevent this log from being flooded with records, by default it is flushed weekly by the crontab. It is not recommended that you modify this option / 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
```

You can also check the logs at /var/log/syslog or at / Igualmente puede consultar los registros en

/var/log/syslog | http://localhost:10100 o en : http://192.168.0.10:10100

## USB CONTROL

blackusb is an experimental script, which prevents personal data theft, malware, forensic tools, BadUSB (USB Rubber Ducky), etc. Generate a whitelist of usb / hid devices and block any other unauthorized insertion of unknown devices, using udev rules. It is a bash script that generates a white list of usb / hid devices and blocks any other unauthorized insertion of unknown devices, using udev rules / blackusb es un script experimental, que previene el robo de datos personales, malware, herramientas forenses, BadUSB (USB Rubber Ducky), etc. Genera una lista blanca de dispositivos usb/hid y bloquea cualquier otra inserción no autorizada de dispositivos desconocidos, usando reglas udev. Es un bash script que genera una lista blanca de dispositivos usb/hid y bloquea cualquier otra inserción no autorizada de dispositivos desconocidos, usando reglas udev

Howto use:

```
sudo /etc/scr/blackusb s
sudo /etc/scr/blackusb show
```

show	s	Shows connected devices / Muestra los dispositivos conectados
on	o	Enable blackusb and generate white list of connected USB devices / Activar blackusb y genera lista blanca de dispositivos USB conectados
eject	j	Choose a device from the list to eject or add entry / Elija un dispositivo de la lista para expulsarlo o agregar entrada
off	x	Temporarily disable blackusb / Desactiva temporalmente blackusb
gen	g	Generate or refresh device whitelist usb udev list / Genera o refresca lista blanca de dispositivos lista udev usb
del	D	Delete udev file containing usb devices whitelist / Elimina archivo udev que contiene lista blanca de dispositivos usb
edit	e	Manually edit udev rules / Edita manualmente las reglas udev

Paranoid Mode:

It consists of turning off your terminal when an unauthorized and / or unknown usb device is inserted, instead of blocking it. To activate it, manually edit the script and uncomment the line / Consiste en apagar su terminal cuando se inserte un dispositivo usb no autorizado y/o desconocido, en lugar de bloquearlo. Para activarlo, edite manualmente el script y descomente la línea

```
poweroff
```

## Logs

```
/var/log/blackusb.log
```

Ejemplo:

```
2017-07-06 12:34:10 blackusb triggered!
```

```
Unknown Device Blocked: SUBSYSTEM=="usb", ATTR{idVendor}=="0781",
ATTR{idProduct}=="5567", ATTR{serial}=="4C530799910104103543"
Cruzer Blade
```



## FILES

ACL

ACL (.txt)	Servicio	Uso
mac-unlimited	Squid, iptables	It includes the mac and IP of the computers with unlimited or administrative privileges (they do not go through the proxy or are subject to any restrictions). Reserved for administrators, switches, APs, etc. Use it with caution / Incluye las mac e IP de los equipos con privilegios ilimitados o de administración (no pasan por el proxy ni están sujetos a ninguna restricción). Reservado para administradores, switches, AP, etc. Úsela con precaución
mac-limited	Squid, iptables	It includes the mac and IP of the computers that will only be able to access the internet during limited hours. By default it comes into operation after hours (MON-FRI from 6:00 PM). You can change the schedule by editing the iptables.sh script. For the weekend, create the same rules with we = Sat, Sun / Incluye las mac e IP de los equipos que solo podrán acceder a internet en horario limitado. Por default entra en funcionamiento fuera de horario laboral (LUN-VIE a partir de las 6:00 PM). Puede cambiar el horario editando el script iptables.sh. Para fin de semana, cree las mismas reglas con we=Sat,Sun
mac-proxy	Squid, iptables	Includes mac- and IPs of the computers subject to total filtering (all firewall rules iptables and Squid proxy apply) / Incluye las mac- e IPs de los equipos sujetas a filtrado total (aplican todas las reglas de firewall iptables y proxy Squid)
mac-transparent	Squid, iptables	Only for non-WPAD compatible devices such as Android etc. This ACL only filters the http protocol (8080), it does not filter https (443), therefore the computers in this ACL may represent a security risk. See PROXY section / Solo para dispositivos no compatibles con WPAD, como Android, etc. Esta ACL solo filtra el protocolo http (8080), no filtra https (443), por tanto los equipos en esta ACL pueden representar un riesgo de seguridad. Consulte el apartado PROXY
blackdhcp	Iptables, dhcp	It contains all the terminals that are blocked by default on your local network. Terminals are blocked by default, until the operator removes them from this list / 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

User ACL (/etc/acl)

ACLs (.txt)	Servicio	Uso
blackdomains	squid	List to add domains to block / Lista para agregar dominios a bloquear
blackwords	squid	Blacklist blocking by words or phrases (can generate false positives) / Lista negra de bloqueo por palabras o frases (puede generar falsos positivos)
whitedomains	squid	List to add allowed domains. / Lista para agregar dominios permitidos.

System ACL (/etc/acl). No se recomienda la manipulación de estas listas

ACLs (.txt)	Servicio	Uso
whiteip	Ipset, Iptables, squid	White list of IPs (not editable) / Lista blanca de IPs (no editable)
wextra	Ipset, Iptables, squid	Whiteip companion list to exclude new ips / Lista complementaria de Whiteip para excluir nuevas ips
<a href="#">blackweb</a>	Squid	Domain blacklist / Lista negra de dominios
dhcp_ips	dhcp, iptables	System ACL for Leases / ACL de sistema para arrendamientos
dhcp_mac	dhcp, iptables	System ACL for Leases / ACL de sistema para arrendamientos
blackext	squid	Blacklist of url_regex extensions / Lista negra de extensiones url_regex
blackmime	squid	Blacklist of mime_type extensions / Lista negra de extensiones mime_type
ipsreserved	iptables	IANA anti-spoofing

SCRIPTS (etc/scr/)

script	task	Work
bkconf	week	Backup the server configuration files in the path of your choice / Realiza backup de los archivos de configuración del servidor en el path de su preferencia
cleaner.sh	daily	Delete temporary, encryptable.zone, Thumbs.db, old crash reports / Elimina temporales, encryptable.zone, Thumbs.db, informes de crash antiguos
iptables.sh	serverload.sh	Iptables firewall rules. / Reglas de firewall iptables
leases.sh	serverload.sh	DHCP server control
lock.sh	reboot	Prevents the execution of several instances of the same script / Evita que la ejecución de varias instancias de un mismo script
servicesload.sh	10 min	Keep an eye on essential server services. (isc-dhcp-server, Squid, Apache2, ntopng, redis-server, etc). If one falls, the script automatically picks it up / Vigila los servicios esenciales del servidor. (isc-dhcp-server,

		Squid, Apache2, ntopng, redis-server, etc). Si alguno cae, el script lo levanta automáticamente
blackusb	no	Protect your server from unauthorized usb devices. / Protege su servidor de dispositivos usb no autorizados.
serverload.sh	20 min	Start all servers / Inicia todos los servidores
bandata.sh	no	Data plan / Plan de datos
banip.sh	no	Block IP base don Ipset / Bloquea IP basado en Ipset

## FOLDERS

proxy	/var/www/html/wpad	Contains the proxy autoconfiguration files / Contiene los archivos de autoconfiguración del proxy wpad.dat, proxy.pac y wpad.da
acl	/etc/	Contains the system ACLs / Contiene las ACLs de sistema
scr	/etc/	Contains the gateproxy scripts / Contiene los scripts de gateproxy
add	/etc/scr/	Contains additional scripts / Contiene scripts adicionales