

Shockware Gaming S.A. | Crédito de Síntesi 2014

Proxy Squid3

Squid ACL, una solución para bloquear sitios con la finalidad de proteger la empresa...



Teoría

Un ACL es una definición de control de acceso, que en Squid se especifica mediante el parámetro acl según la siguiente sintaxis:

acl nombre_acl tipo_acl descripción ...

acl nombre_acl tipo_acl "archivo_de_descripciones" ...

Cuando usamos un "archivo_de_descripciones", cada descripción se corresponde con una línea del archivo.

Tipos de ACL

src

Especifica una dirección origen de una conexión en formato IP/máscara.

Por ejemplo, utilizaremos una acl de tipo src para especificar la red local:

acl red_local src 192.168.1.0/24

También podemos especificar rangos de direcciones mediante una acl de tipo src:

acl jefes src 192.168.1.10-192.168.1.25/32

dst

Especifica una dirección destino de una conexión en formato IP/máscara.

acl google_es dst 216.239.0.0/24

También podemos especificar hosts concretos mediante una acl de tipo dst:

acl google_es2 dst 216.239.59.104/32 216.239.39.104/32 216.239.57.104/32

Las definiciones son idénticas a las acl de tipo src salvo que se aplican al destino de las conexiones, no al origen.

srcdomain y dstdomain

Estos tipos de acl especifican un nombre de dominio.

En el caso de srcdomain es el dominio origen y se determina por resolución DNS inversa de la IP de la máquina, es decir, tendremos que tener bien configurado el DNS de la red local.

En el caso de dstdomain el nombre del dominio se comprueba con el dominio que se haya especificado en la petición de página web.

Por ejemplo:

acl google_com dstdomain google.com

srcdom_regex y dstdom_regex

Especifican una expresión regular que verifican los dominio origen o destino. La expresión regular hace distinción entre mayúsculas y minúsculas salvo que incluyamos la opción "-i" que evita dicha distinción.

Por ejemplo

acl google_todos dstdom_regex -i google\..*

Observamos como al incluir "-i" estamos indicando que no haga distinción entre mayúsculas y minúsculas.

time

Este tipo de acl permite especificar una franja horaria concreta dentro de una semana. La sintaxis es la siguientes

acl nombre_acl_horaria time [dias-abrev] [h1:m1-h2:m2]

Donde la abreviatura del día es:

S - Sunday (domingo)

M - Monday (lunes)

T - Tuesday (martes)

W - Wednesday (miércoles)

H - Thursday (jueves)

F - Friday (viernes)

A - Saturday (sábado)

además la primera hora especificada debe ser menor que la segunda, es decir h1:m1

tiene que ser menor que h2:m2

Por ejemplo

acl horario_laboral time M T W H F 8:00-15:00

Estaríamos especificando un horario de 8 a 15 y de lunes a viernes.

url_regex

Permite especificar expresiones regulares para comprobar una url completa, desde el http:// inicial.

Por ejemplo, vamos a establecer una acl que se verifique con todos los servidores cuyo nombre sea adserver:

url_regex serv_publicidad ^http://adserver.*

En otro ejemplo podemos ver una acl que verifique las peticiones de ficheros mp3:

url_regex ficheros_mp3 -i mp3\$

Nota: ver expresiones regulares

referer_regex

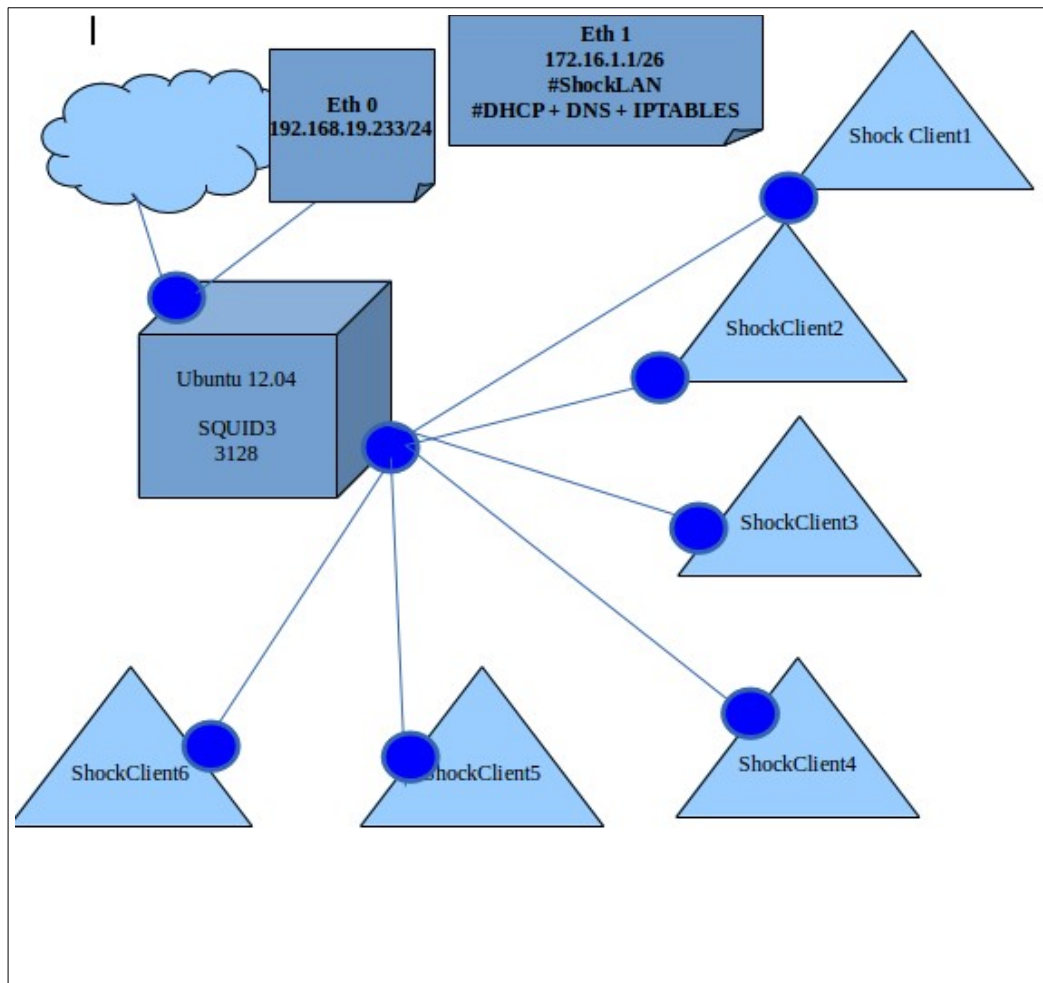
Define una acl que se comprueba con el enlace que se ha pulsado para acceder a una determinada página. Cada petición de una página web incluye la dirección donde se ha pulsado para acceder. Si escribimos la dirección en el navegador entonces estaremos haciendo una petición directa.

Por ejemplo vamos a establecer una acl para todas las páginas a las que hayamos accedido pulsando en una ventana de búsqueda de google:

acl pincha_google referer_regex http://www.google.*

Squid Proxy Transparente

http_port 3128 transparent [Línea 889]



Instalación y configuración PROXY SQUID

- apt-get update
- apt-get install squid3
- **Definimos ACLS**

```
# ACCESS CONTROLS
# -----

# IP del servidor local
acl localhost src 192.168.19.233

# IP del servidor2
acl servidor2 src 192.168.19.235

# Red Empresa Shockware Gaming
acl red-empresa src 172.16.1.2-172.16.1.40

# Cliente1 que serán los GERENTES de Shockware Gaming S.A. via MAC puesto que está activado DHCP.
acl cliente1 arp 08:00:27:f4:b9:8d

# Cliente2 que seremos los Informatico de Shockware Gaming S.A.via MAC puesto que está activado DHCP.
acl cliente2 arp 08:00:27:32:ed:2a

# Horario de trabajo
acl horario time MTWHF 14:00-22:00

# Cliente 4 (Windows) denegado a todas las paginas administrativas via MAC
acl cliente1 arp 08:00:27:8c:e5:45|

# Páginas web administrativas internas de Shockware Gaming S.A.
acl shockadmin dstdomain "/etc/squid3/shockadmin"
```

- **Habilitamos SQUID3 Transparente y empezamos a DENEGAR y PERMITIR.**

```
# Cliente 4 (Windows) denegado a todas las paginas administrativas via MAC
acl cliente4 arp 08:00:27:6f:b2:cf

# Páginas web administrativas internas de Shockware Gaming S.A.
acl shockadmin dstdomain "/etc/squid3/shockadmin"

# PRUEBAS PC4 DENEGACIÓN PÁGINAS Administrativas e Interinas|

http_access allow cliente4 !shockadmin
http_access deny cliente4

# -----

# DENEGAR Y PERMITIR

http_access allow servidor2
http_access allow localhost
http_access allow cliente1
http_access allow cliente2
http_access allow red-empresa horario
http_access deny all

# PROXY SQUID NO FUNCIONA CON HTTPS
```


- Las acls que definimos son:
 - Los clientes “red-empresa” podrán navegar de 2PM a 10PM excepto los GERENTES y los INFORMÁTICOS.
 - Puesto que tenemos DHCP hemos optado por hacer filtrado de dirección física MAC a esas excepciones, CLIENTE1 (Ub) y CLIENTE2 (Ub). Éstos no tendrán ninguna denegación.
 - Al cliente4, que serán el PC para el público que quiera ver nuestro catálogo y página web. Éstos solamente podrán acceder en las páginas FRONTEND (Joomla y PRESTASHOP) y no en las páginas internas y administrativas del SHOCKWARE-GAMING S.A.

- IPTABLES

Proxy ACL

```
iptables -t nat -A POSTROUTING -s 172.16.1.0/26 -o eth0 -j SNAT --to 192.168.19.233
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.19.233:3128
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

- Hay un problema con HTTPS con proxy SQUID Transparente:


 **Proxy http no filtra contenido por https**
« on: April 23, 2014, 05:26:49 pm »


Hola buenas a tod@s

Estoy configurando un proxy transparente de prueba en una 3.2 y todo lo que va por https no lo filtra.

Puede que sea ignorancia, que sera lo más seguro, pero ¿podéis filtrar dominios por https?

Muchas gracias y disculpad toda mi ignorancia.

 Logged


 **Re: Proxy http no filtra contenido por https**
« Reply #1 on: April 23, 2014, 05:51:40 pm »

Hola epc.


Te comento por mis conociminetos el proxy transparente solo escucha las peticiones del puerto 80 que es http, el trafico https sale por el puerto 443 que lo puedes bloquear desde el corta fuegos pero no vas a entrar a las paginas seguras de bancos y demas.

En mi trabajo tubimos el mismo problema y se decidio por configurar el proxy con puerto fijo y bloquear todo del corta fuego (menos calentura de cabeza y se termino el problema).

Saluda Djpablopol.

 Logged

<https://forum.zentyal.org/index.php?topic=21623.0>

<p>Joel Barrios Dueñas 21/05/13 10:40</p> <p>Admin</p>  <p>Estado: desconectado</p> <p>Identificado: 17/02/07 Mensajes: 1219</p>	<p>HTTPS no puede ser puesto en proxy transparente. HTTPS tiene que pasar por NAT en un esquema de proxy transparente. Por tanto en un esquema de proxy transparente el usuario puede brincar cualquier tipo de restricciones que tengas utilizando túneles SSL y a través de HTTPS, ejemplo: your-freedom y ultrasurf. En pocas palabras: con proxy transparente no puedes filtrar HTTPS a través de squid.</p> <p>En esquema de proxy no-transparente, que es lo que se hace hoy en día para poder filtrar sitios con HTTPS, donde sólo permites la salida a ciertos sitios con una lista blanca (solo se permite acceder a lo que esté en dicha lista), se puede filtrar con squid los contenidos que están disponibles a través de HTTPS y además hacer que programas como Your-freedom y ultrasurf dejen de funcionar.</p>
--	---

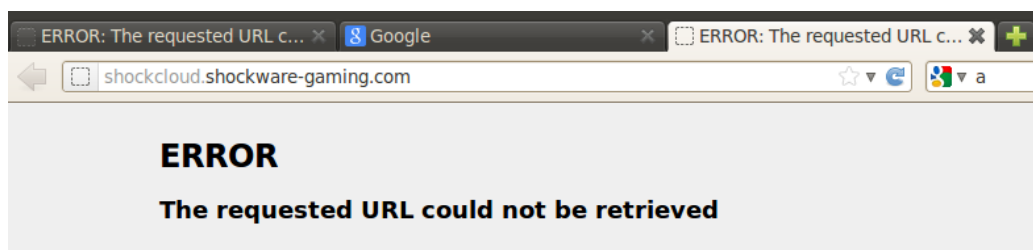
Perfil Correo Sitio Web Citar

- Esto hace que no podamos denegar las páginas administrativas e internas:
 - shockware-gaming.com/admin5166 → Pág BACKEND Prestashop
 - shockgamer.shockware-gaming.com/administrator → Pág BACKEND JOOMLA
 - shockopkm.shockware-gaming.com → OpenKM
 - shockmail... → Squirrel Mail Interno
 - shockcloud... → Cloud Computing Interno.

Como alternativa tenemos 3 Opciones para crear ACLs para el PC4.

Opción 1:

- Proxy Transparente: Denegamos shockmail ; shockcloud ; shockopkm.



The following error was encountered while trying to retrieve the URL: <http://shockcloud.shockware-gaming.com/>

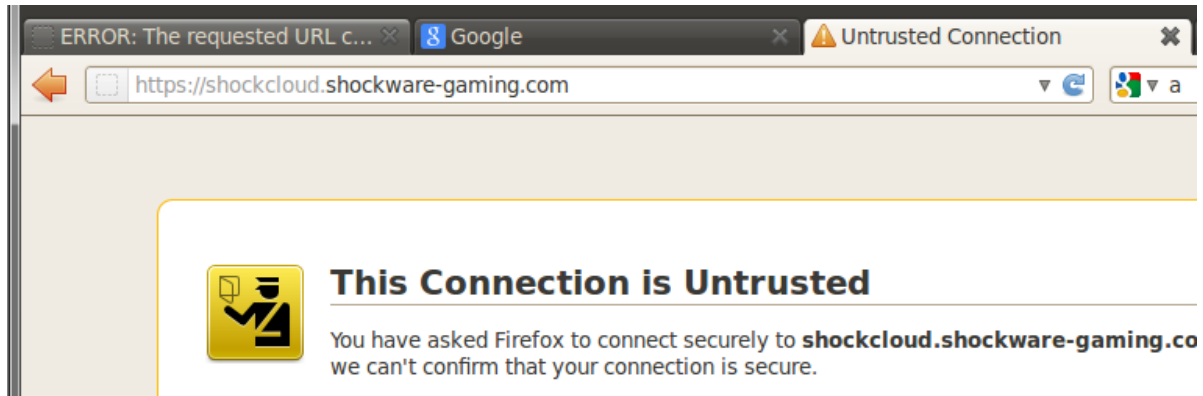
Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you f

Your cache administrator is [webmaster](#).

- Acreditación de usuarios vía APACHE2 en las carpetas de administración BACKEND.
- Si logran entrar vía HTTPS (Proxy Squid no bloquea HTTPS, entonces si entran...) en shockmail y derivados, se refuerza con acreditación de usuarios con un mensaje que dirá "Zona de administración Shockware Gaming S.A.: Identificarse primero". Si no logra

entrar entonces le denegará el servicio y acceso.



(Lo mismo para shockcloud.*)

- **Opción2**
 - Redirección proxy squid (Cada vez que intenten entrar en shockmail.* se le redirigirá a <http://shockware-gaming.com/blocked.html> como si fuera un squidguard pero en ProxySquid.

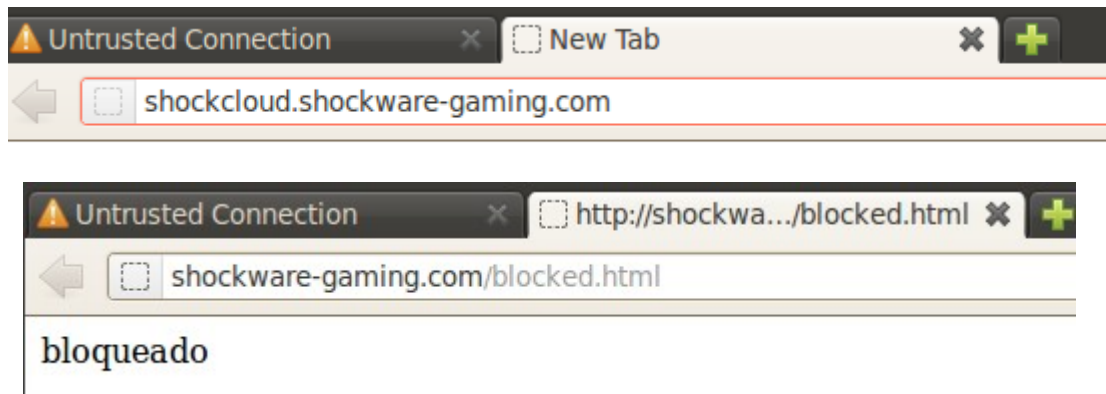
PRUEBAS

```
acl sites dstdomain shockmail.shockware-gaming.com
acl clienteesp arp 08:00:27:a5:c1:6a

deny_info http://shockware-gaming.com/blocked.html clienteesp

http_reply_access deny shockadmin clienteesp
http_access allow clienteesp
```


(En la imagen utilizamos el filtrado de MAC y las opciones deny_info y http_reply_access para la redirección proxy. Hemos denegado shockadmin "lista de sitios denegados" para el cliente "cliente4". CONCLUSIÓN: Cada vez que el cliente4 intente entrar en **shockcloud.shockware-gaming.com** le redigirá a **blocked.html**)



- Seguiremos utilizando la MAC del PC4 (Filtrado de MAC) puesto que va por DHCP y DNS automático.
- La redirección en los directorios BACKEND no se les puede redireccionar con el cuál se añadirán acreditación de usuarios.



• Opción3 Final (Descargado)

- Dejar configuración estática PC4: 172.16.1.41/26 + DNS y hacer las ACLs vía APACHE2.
- Con esto denegamos sólo a la IP del PC4 la entrada a shockware-gaming.com/admin5166 y a

shockgamer.shockware-gaming.com/administrator

- Todo lo demás denegado vía proxy + Acreditación de usuarios.
- **Conclusión:**
 - Modos de DENEGACIÓN vía filtrado de MAC:
 - Redirección PROXY SQUID Transparente vía blocked.html en el servidor + acreditación usuarios apache2 backend PRESTASHOP y JOOMLA (Y si entran por HTTPS también acreditación).
 - Denegación automática PROXY SQUID Transparente + Acreditación usuarios apache2 a todas las páginas menos en los FRONTEND de SGAMING S.A.
 - Sin filtrado de MAC:
 - Configuración estática PC4 + ACL vía apache2 en los BACKENDS + Acreditación usuarios apache2 vía https + Denegación proxy squid transparente sin https.

PRODECIMIENTO FINAL

- Como conclusión hemos hecho un mixto de las opciones que teníamos para crear ACLS en el ordenador PC4 vía filtrado MAC. Así construimos nuestro PROXY para el PC4.
1. Instalamos SQUID3.
 2. Abrimos las máquinas virtuales del servidor y el PC4.
 3. Definimos ACLs:



```
# ACCESS CONTROLS
# -----

# IP del servidor local
acl localhost src 192.168.19.233

# IP del servidor2
acl servidor2 src 192.168.19.235

# Red Empresa Shockware Gaming
acl red-empresa src 172.16.1.2-172.16.1.40

# Cliente1 que serán los GERENTES de Shockware Gaming S.A. via MAC puesto que está activado DHCP.
acl cliente1 arp 08:00:27:f4:b9:8d

# Cliente2 que seremos los Informatico de Shockware Gaming S.A.via MAC puesto que está activado DHCP.
acl cliente2 arp 08:00:27:32:ed:2a

# Horario de trabajo
acl horario time MTWHF 14:00-22:00

# Cliente 4 (Windows) denegado a todas las paginas administrativas via MAC
acl cliente1 arp 08:00:27:8c:e5:45|

# Páginas web administrativas internas de Shockware Gaming S.A.
acl shockadmin dstdomain "/etc/squid3/shockadmin"
```

4. Después hemos hecho las denegaciones:

```
# Cliente 4 (Windows) denegado a todas las paginas administrativas via MAC
acl cliente4 arp 08:00:27:6f:b2:cf

# Páginas web administrativas internas de Shockware Gaming S.A.
acl shockadmin dstdomain "/etc/squid3/shockadmin"

# PRUEBAS PC4 DENEGACIÓN PÁGINAS Administrativas e Interinas|

http_access allow cliente4 !shockadmin
http_access deny cliente4

# -----

# DENEGAR Y PERMITIR

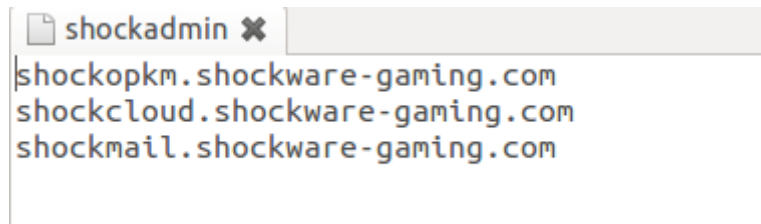
http_access allow servidor2
http_access allow localhost
http_access allow cliente1
http_access allow cliente2
http_access allow red-empresa horario
http_access deny all

# PROXY SQUID NO FUNCIONA CON HTTPS
```

5. Iptables

```
# Proxy ACL
iptables -t nat -A POSTROUTING -s 172.16.1.0/26 -o eth0 -j SNAT --to 192.168.19.233
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.19.233:3128
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

6. Creamos el archivo shockadmin

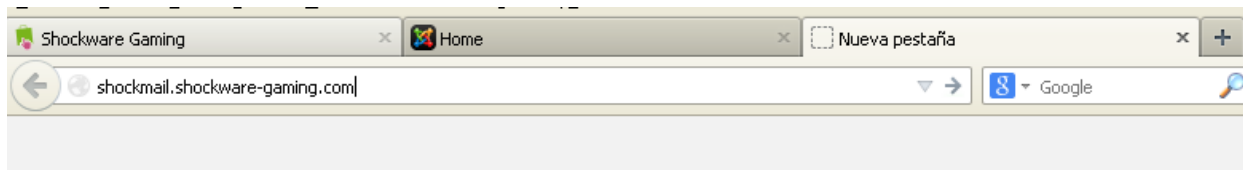


7. Hemos solucionado el ERROR de HTTPS Proxy Transparente utilizando métodos alternativos con APACHE2 y el propio PROXY.

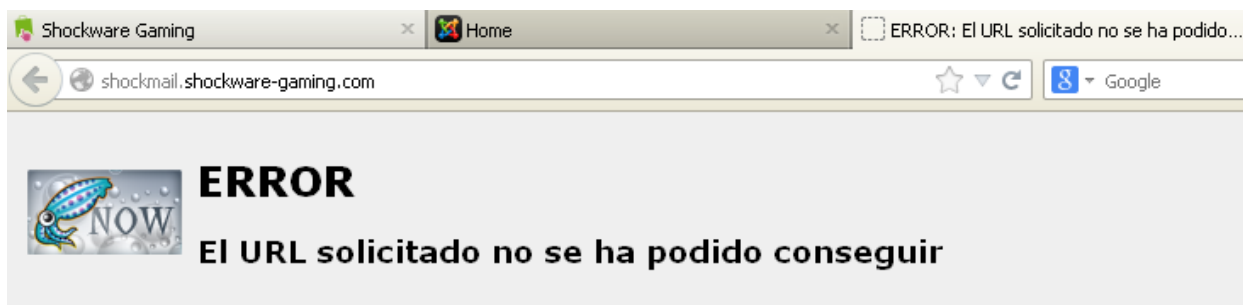
8. El PC4 utilizando filtrado de MAC hemos conseguido que deniegue las páginas. Los subdominios las podemos denegar con el proxy transparente en cambio los directorios no las podemos denegar, hay que hacerlo vía acreditación apache2. Especificarlo en el archivo default.

9. Reiniciamos squid3.

10. A continuación hemos probado primero las denegaciones con el PC4. Resultado:



11. ¿Funcionará?



Se encontró el siguiente error al intentar recuperar la dirección URL: <http://shockmail.shockware-gaming.com/>

Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con el proveedor de servicios si cree que esto es incorrecto.

Su administrador del caché es [webmaster](#).

12. Podemos observar que puede entrar en PRESTASHOP y en JOOMLA pero no en las páginas administrativas de la empresa.

13. Para la acreditación de usuarios hemos modificado el servicio APACHE2.

14. En los VIRTUALHOST 443 de SHOCKWARE-GAMING y SHOCKGAMER.SHOCKWARE-GAMING hemos añadido lo siguiente:

```
<Directory "/var/www/prestashop/admin5166">
    Options Indexes FollowSymlinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
    SSLRequireSSL
    AuthType Basic
    AuthName "Zona de administracion Shockware Gaming S.A.: Identificarse primero"
    AuthUserFile /var/www/.usuarios
    require valid-user
</Directory>
```

15. Dónde ponía Allow from all, intentamos añadir una ACL en APACHE2 que era Allow from all y "Deny from IP PC4". Pero no funcionó. Entonces optamos por acreditación de usuarios vía apache2 para esos directorios.

16. En la del JOOMLA.

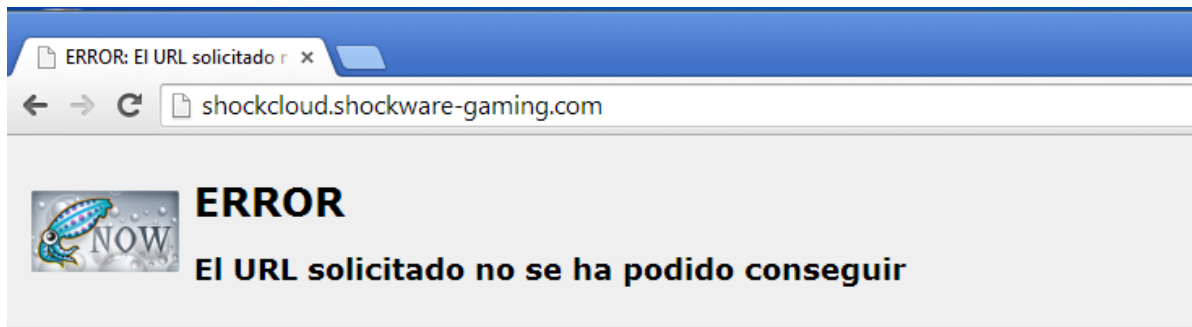
```
<Directory "/var/www/prestashop/admin5166">
    Options Indexes FollowSymlinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
    SSLRequireSSL
    AuthType Basic
    AuthName "Zona de administracion Shockware Gaming S.A.: Identificarse primero"
    AuthUserFile /var/www/.usuarios
    require valid-user
</Directory>
```

17. A continuación hemos ejecutado este comando `htpasswd -c /var/www/.usuarios shockgadmin ; PASSWD shockgadmin:S*****`.

18. A partir de aquí hemos reiniciado APACHE2 y hemos probado si funcionaba cada configuración establecida.

19. En PC4:

- Entrando en SHOCKMAIL o SHOCKCLOUD:



Se encontró el siguiente error al intentar recuperar la dirección URL: <http://shockcloud.shockware-gaming.com/>

Acceso Denegado

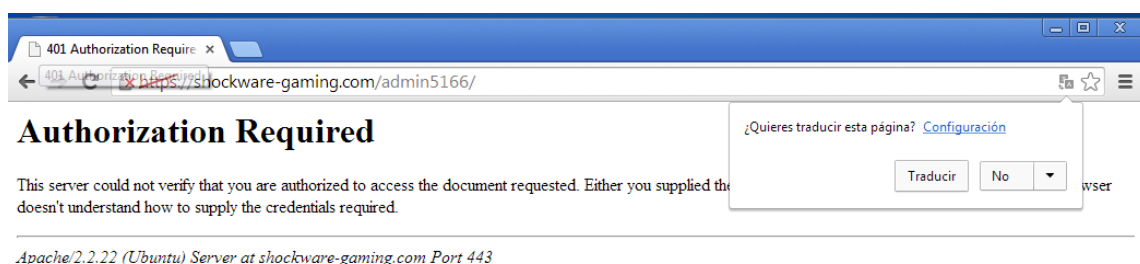
La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su administrador del caché para que cree que esto es incorrecto.

Su administrador del caché es [webmaster](#).

- Entrando en la zona administrativa de PRESTASHOP:



- Si fallase el intento: (No entraría)



- Entrando en SHOCKMAIL:



SQUIDGUARD

SquidGuard. Sistema de filtrado combinado de redireccionamiento web, y el plugin del controlador de acceso para Squid. Utiliza una lista negra "Blacklists" como base de datos para denegar o permitir sitios web al usuario. Su mayor utilidad es la prevención de dominios o URLs que contengan informaciones no deseadas o nada productivas en horario laboral.

Lista negra

Una lista negra "blacklists" en la computación, es una lista de dominios, URLs o direcciones de IP que deben ser restringidas por contener informaciones no adecuadas, en muchos casos por proveer Spam, Spyware, Hacking, Porn, etc.



1. **apt-get install squidguard**
2. Cambiamos los permisos de DB
chown -R proxy:proxy /var/lib/squidguard/db
3. Editamos el archivo squidguard.conf
gedit /etc/squid/squidGuard.conf
4. Esborrem el contingut i posem:

dbhome /var/lib/squidguard/db

logdir /var/log/squid

dest adv {

domainlist adv/domains

urllist adv/urls

}

dest porn {

domainlist porn/domains

urllist porn/urls

}

dest warez {

domainlist warez/domains

urllist warez/urls

}

acl {

default {

pass !adv !porn !warez all

redirect http://192.168.19.233/blocked.html

}

}

5. Creamos el archivo blocked.html en /var/www
6. Dentro de squid.conf ponemos: `url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf`
7. Hacemos el comando `squid3 -k reconfigure` y reiniciamos.
8. Entonces ejecutamos este comando para obtener el script: `wget http://www.shallalist.de/Downloads/shalla_update.sh`
9. Modificamos el script de la siguiente forma:

```
squidGuardpath="/usr/bin/squidGuard"
```

```
squidpath="/usr/sbin/squid3"
```

```
httpget="/usr/bin/wget"
```

```
tarpath="/bin/tar"
```

```
chownpath="/bin/chown"
```

```
dbhome="/var/lib/squidguard/db"      # like in squidGuard.conf
```

```
squidGuardowner="proxy:proxy"
```

```
#####
```

```
workdir="/tmp"
```

```
shallalist="http://www.shallalist.de/Downloads/shallalist.tar.gz"
```

10. Ejecutamos el SCRIPT:

```
root@shockwaregaming:/etc/squid3# sh shalla_update.sh
-2014-05-21 19:17:07-- http://www.shallalist.de/Downloads/shallalist.tar.gz
Resolviendo www.shallalist.de (www.shallalist.de)... 46.4.77.203
Conectando con www.shallalist.de (www.shallalist.de)[46.4.77.203]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 10179112 (9,7M) [application/x-gzip]
Grabando a: "/tmp/shallalist.tar.gz"
100%[=====] 10.179.112 2,99M/s en 3,6s
```

11. Compilamos con squidGuard -u -C all -d
12. Reiniciamos squid3 y hacemos squid3 -k reconfigure
13. Creamos el archivo blocked.html con este contenido:

URL Bloqueada por la empresa Shockware Gaming S.A.

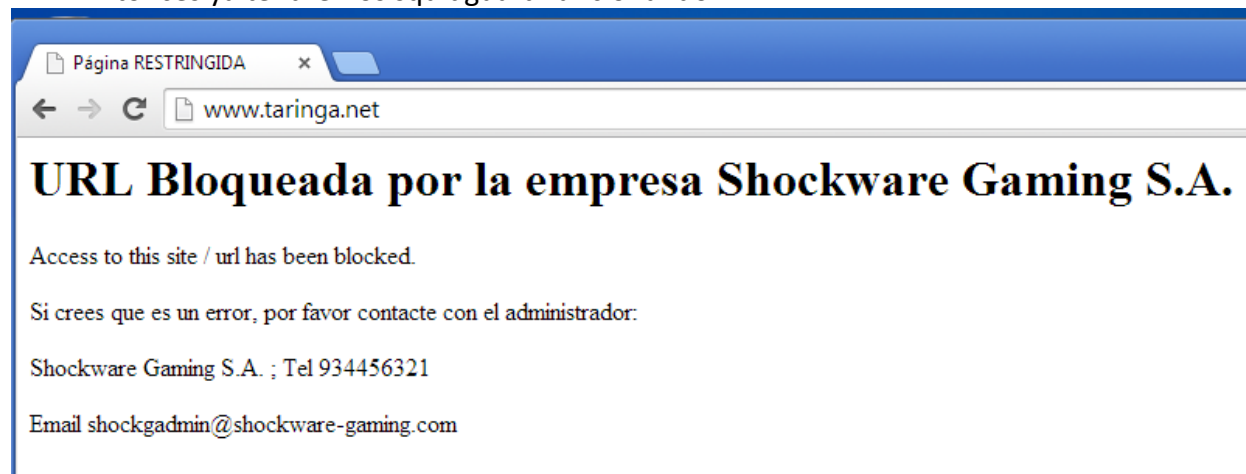
Access to this site / url has been blocked.

Si crees que es un error, por favor contacte con el administrador:

Shockware Gaming S.A. ; Tel 934456321

Email shockgadmin@shockware-gaming.com

14. Entonces ya tendremos squidguard funcionando.



15. Vemos que deniega todo tipo de blacklist: porno, warez y publicidad.

