

Autenticación en el Proxy

y

Instalación de SARG

para informes

Nombre: Alejandro

Apellidos: Román Caballero

Curso: 2 ASIR

ÍNDICE

Como hacer proxy squid con autenticación	3
Como instalar SARG, reportes de SQUID	6

Como hacer proxy squid con autenticación

Primero instalaremos los servicios necesarios para esta práctica , para ello instalaremos el apache y squid.

Los comandos a ejecutar son :

apt update

apt install apache2

apt install squid

```
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/squid# apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
apache2 ya está en su versión más reciente (2.4.18-2ubuntu3.9).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 31 no actualizados.
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/squid# apt install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
squid ya está en su versión más reciente (3.5.12-1ubuntu7.6).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 31 no actualizados.
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/squid# █
```

Después de instalarlo crear un usuario para el squid para ello hacer el siguiente comando:

htpasswd -c /etc/squid/passwd alejandro

-c sirve para crear el archivo passwd si no está creado

Luego modificamos el archivo de configuración del squid, aunque antes hacemos una copia de seguridad al archivo de configuración del squid con el comando.

cp /etc/squid/squid.conf /etc/squid/squid.conf.back

Vaciamos el archivo de configuración que vamos a configurar :

```
echo "" > /etc/squid/squid.conf
```

Luego lo editamos:

```
nano squid.conf
```

```
http_port 3128  
cache_dir ufs /var/spool/squid 2000 16 256  
cache_mem 32 MB  
maximum_object_size_in_memory 256 MB  
access_log /var/log/squid/access.log  
cache_log /var/log/squid/cache.log  
auth_param basic program /usr/lib/squid/basic_ncsa_auth  
/etc/squid/users_passwd  
auth_param basic realm proxy  
acl auth_users proxy_auth REQUIRED  
  
http_access allow auth_users  
  
http_access deny all
```

Autenticación en el Proxy e Instalación de SARG para informes

```
GNU nano 2.5.3                               Archivo: squid.conf
http_port 3128

cache_dir ufs /var/spool/squid 2000 16 256

cache_mem 32 MB

maximum_object_size_in_memory 256 MB

access_log /var/log/squid/access.log

cache_log /var/log/squid/cache.log

auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/users_passwd

auth_param basic realm proxy

acl auth_users proxy_auth REQUIRED

http_access allow auth_users

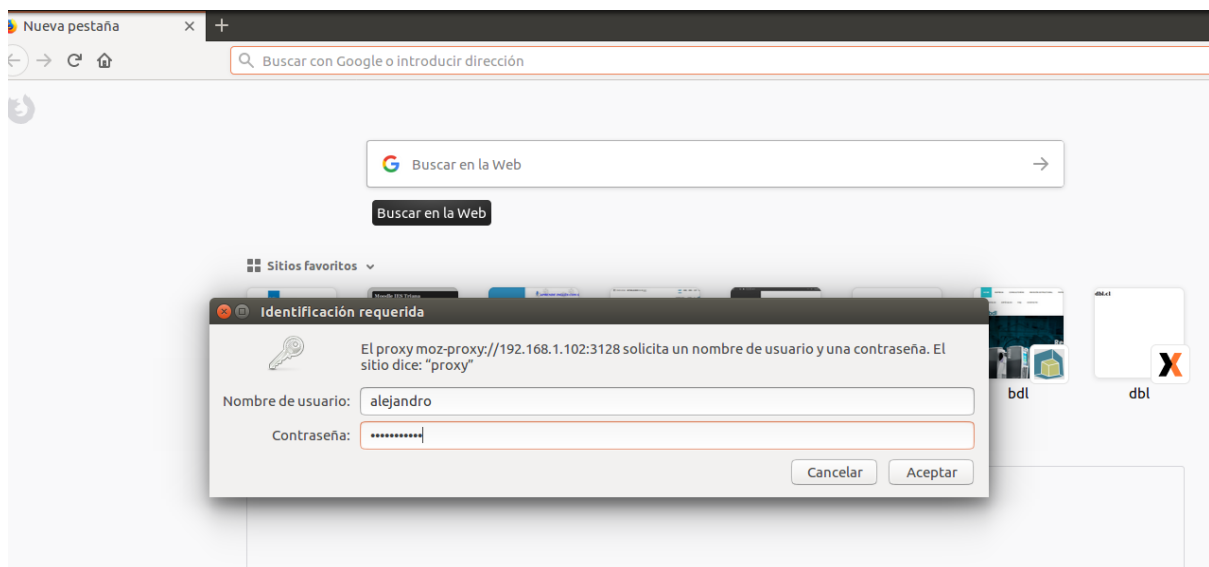
http_access deny all


#acl mak arp a0:48:1c:8f:18:90
#acl permiso1 dstdomain www.clafoti.com clafoti.com
#acl permiso2 dstdomain www.cajamagica.net cajamagica.net
#acl permisopdf rep_mime_type -i mime-type .pdf
#acl permisopost method post
#acl conexion maxconn 1


#http_access deny mak
#http_reply_access deny mak
#http_access allow permiso1
#http_access deny permiso2
#http_access deny permisopdf
#http_access deny permisopost
#http_access deny conexion
```

Por último reiniciamos el squid y comprobamos que funciona.

/etc/init.d/squid restart



Como instalar SARG, reportes de SQUID

Primero actualizamos los repositorios para poder instalar el sarg:

apt update

```
root@alejandro-HP-EliteDesk-800-G1-SFF:/home/alejandro# apt update
Ign:1 http://dl.google.com/linux/chrome/deb stable InRelease
Obj:2 http://dl.google.com/linux/chrome/deb stable Release
Obj:3 http://es.archive.ubuntu.com/ubuntu xenial InRelease
Des:4 http://es.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Obj:5 http://ppa.launchpad.net/ansible/ansible/ubuntu xenial InRelease
Obj:6 http://ppa.launchpad.net/webupd8team/java/ubuntu xenial InRelease
Obj:7 http://packages.microsoft.com/repos/vscode stable InRelease
Des:8 http://es.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Des:9 http://security.ubuntu.com/ubuntu xenial-security InRelease [107 kB]
Obj:10 https://download.docker.com/linux/ubuntu xenial InRelease
Des:11 https://mega.nz/linux/MEGAsync/xUbuntu_16.04 ./ InRelease [1.492 B]
Des:13 http://es.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [881 kB]
Des:14 http://es.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [783 kB]
Descargados 1.989 kB en 2s (685 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se pueden actualizar 32 paquetes. Ejecute «apt list --upgradable» para verlos.
```

Luego instalamos el sarg con el siguiente comando:

apt install sarg

```
root@alejandro-HP-EliteDesk-800-G1-SFF:/home/alejandro# apt install sarg
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  squidguard libapache2-mod-php5
Se instalarán los siguientes paquetes NUEVOS:
  sarg
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 32 no actualizados.
Se necesita descargar 145 kB de archivos.
[.....]
[.....]
[.....]
Seleccionando el paquete sarg previamente no seleccionado.....
(Leyendo la base de datos ... 265710 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../sarg_2.3.10-2_amd64.deb ...
Desempaquetando sarg (2.3.10-2) ...
Procesando disparadores para man-db (2.7.5-1) ...
Configurando sarg (2.3.10-2) ...
root@alejandro-HP-EliteDesk-800-G1-SFF:/home/alejandro#
```

Ahora nos metemos en la carpeta de configuración del xorg y miramos lo que tiene:

```
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/sarg# cd /etc/sarg/
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/sarg# ls
css.tpl  exclude_codes  exclude_hosts  exclude_users  sarg.conf  sarg-reports.conf  user_limit_block  usertab
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/sarg#
```

Editamos el `/etc/sarg/sarg.conf` para que sea así:

```
root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/sarg# nano /etc/sarg/sarg.conf

root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg
GNU nano 2.5.3 Archivo: /etc/sarg/sarg.co

# sarg.conf
#
# TAG: access_log file
#      Where is the access.log file
#      sarg -l file
#
access_log /var/log/squid/access.log

root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg
GNU nano 2.5.3 Archivo: /etc/sarg/sarg.co

#password none

# TAG: temporary_dir
#      Temporary directory name for work files
#      sarg -w dir
#
temporary_dir /tmp

# TAG: output_dir
#      The reports will be saved in that directory
#      sarg -o dir
#
output_dir /var/www/html/squid-reports
```

```
root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg
GNU nano 2.5.3 Archivo: /etc/sarg/s

#
exclude_hosts /etc/sarg/exclude_hosts

# TAG: useragent_log file
#       useragent.log file patch to generate useragent rep
#
#useragent_log none

# TAG: date_format
#       Date format in reports: e (European=dd/mm/yy), u (
#
date_format e
```

```
root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg
GNU nano 2.5.3 Archivo: /etc/sarg/sarg.conf

#
index yes

# TAG: index_tree date|file
#       How to generate the index.
#
index_tree file

# TAG: overwrite_report yes|no
#       yes - if report date already exist then will be overwritten.
#       no - if report date already exist then will be renamed to fi
#
overwrite_report yes
```

Generamos el informe:

Autenticación en el Proxy e Instalación de SARG para informes

```
root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg
root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg# sudo sarg -x
SARG: Init
SARG: Loading configuration from /etc/sarg/sarg.conf
SARG: Unknown option resolve_ip
SARG: Loading exclude host file from: /etc/sarg/exclude_hosts
SARG: Loading exclude file from: /etc/sarg/exclude_users
SARG: Deleting temporary directory "/tmp/sarg"
SARG: Parameters:
SARG:      Hostname or IP address (-a) =
SARG:      Useragent log (-b) =
SARG:      Exclude file (-c) = /etc/sarg/exclude_hosts
SARG:      Date from-until (-d) =
SARG:      Email address to send reports (-e) =
SARG:      Config file (-f) = /etc/sarg/sarg.conf
SARG:      Date format (-g) = Europe (dd/mm/yyyy)
SARG:      IP report (-i) = No
SARG:      Keep temporary files (-k) = No
SARG:      Input log (-l) = /var/log/squid/access.log
SARG:      Resolve IP Address (-n) = No
SARG:      Output dir (-o) = /var/www/html/squid-reports/
SARG: Use Ip Address instead of userid (-p) = No
SARG:      Accessed site (-s) =
SARG:      Time (-t) =
SARG:      User (-u) =
SARG:      Temporary dir (-w) = /tmp/sarg
SARG:      Debug messages (-x) = Yes
SARG:      Process messages (-z) = No
SARG: Previous reports to keep (--lastlog) = 0
SARG:
SARG: SARG version: 2.3.10 Apr-12-2015
SARG: Loading User table: /etc/sarg/usertab
SARG: Reading access log file: /var/log/squid/access.log
SARG: Records read: 41, written: 41, excluded: 0
SARG: Squid log format
SARG: Period: 16 nov 2018
SARG: Sorting log /tmp/sarg/192_168_1_102.user_unsort
SARG: Making file /tmp/sarg/192_168_1_102
SARG: Sorting log /tmp/sarg/alejandro.user_unsort
SARG: Making file /tmp/sarg/alejandro
SARG: (grepday) Fontname "/usr/share/fonts/truetype/ttf-dejavu/DejaVuSans.ttf" not found
root@alejandro-HP-EliteDesk-800-G1-SFF: /etc/sarg#
```

Da un fallo en el font , para arreglarlo ir al archivo de configuración del sarg.

Lo dejamos así:

```
GNU nano 2.5.3 Archivo: sarg.conf
# sarg.conf
#
# TAG: access_log file
# Where is the access.log file
# sarg -l file
#
access_log /var/log/squid/access.log
#
# TAG: graphs yes|no
# Use graphics where is possible.
# graph_days_bytes_bar_color blue|green|yellow|orange|brown|red
#
#graphs yes
#graph_days_bytes_bar_color orange
#
# TAG: graph_font
# The full path to the TTF font file to use to create the graphs. It is required
# if graphs is set to yes.
#
graph_font /usr/share/fonts/truetype/dejavu/DejaVuSans.ttf
#
# TAG: title
# Especifica el título para la página html.
#
title "Squid User Access Reports"
```

Lo volvemos a hacer y nos lo generará el informe.

```
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/sarg# /usr/bin/sarg
SARG: Unknown option resolve_ip
root@alejandro-HP-EliteDesk-800-G1-SFF:/etc/sarg#
```

Para verlo ir a: <http://localhost/squid-reports/>

Y podemos ver que sea a creado el informe:



SARG Squid Analysis Report Generator

Squid User Access Reports

Period: 16 nov 2018
Sort: bytes, reverse
Top users

Top sites
Sites & Users
Authentication Failures

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
1	 alejandro	73	447.07K	100,00%	89,28% 10,72%	00:25:11	1,511,245	100,00%
TOTAL		73	447.07K		89,28% 10,72%	00:25:11	1,511,245	
AVERAGE		73	447.07K			00:25:11	1,511,245	

Generated by [sarg-2.3.10](#) Apr-12-2015 on 16/nov/2018-09:10

Nos metemos en alejandro para verlo más detalladamente.

Aquí vemos el informe desglosado de los que está analizando del usuario alejandro.

Autenticación en el Proxy e Instalación de SARG para informes

Squid User Access Reports

Period: 16 nov 2018

User: alejandro

Sort: bytes, reverse

User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
 snippets.cdn.mozilla.net:443	2	230.53K	51,57%	100,00% 0,00%	00:01:55	115,932	7,67%
 ftp.mozilla.org:443	1	54.57K	12,21%	100,00% 0,00%	00:01:55	115,209	7,62%
 192.168.1.102	31	44.71K	10,00%	45,85% 54,15%	00:00:00	526	0,03%
 versioncheck-bg.addons.mozilla.org:443	6	31.76K	7,10%	100,00% 0,00%	00:06:09	369,607	24,46%
 incoming.telemetry.mozilla.org:443	6	22.15K	4,96%	100,00% 0,00%	00:06:06	366,911	24,28%
 ocsp.digicert.com	17	20.58K	4,60%	0,00% 100,00%	00:00:00	676	0,04%
 services.addons.mozilla.org:443	2	16.89K	3,78%	100,00% 0,00%	00:03:56	236,334	15,64%
 firefox.settings.services.mozilla.com:443	1	11.49K	2,57%	100,00% 0,00%	00:02:01	121,995	8,07%
 tiles.services.mozilla.com:443	2	6.61K	1,48%	100,00% 0,00%	00:02:01	121,720	8,05%
 aus5.mozilla.org:443	1	4.62K	1,03%	100,00% 0,00%	00:01:01	61,813	4,09%
 detectportal.firefox.com	4	3.13K	0,70%	0,00% 100,00%	00:00:00	522	0,03%
TOTAL	73	447.07K	100,00%	89,28% 10,72%	00:25:11	1,511,245	100,00%
AVERAGE	0	447.07K			00:25:11	1,511,245	100,00%

Generated by sarg-2.3.10 Apr-12-2015 on 16/nov/2018-09:10