Servidor Proxy Squid

Por: John A. Pérez B. ~ 20186748

Este tutorial es un extracto del siguiente video:

https://youtu.be/7Z2wVEj2mH0

Configuración

Primero instalamos el paquete squid con el comando
yum -y install squid

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~

```
[root@samba4 ~]# yum install -y squid
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
```

12:43 PM
11/4/2019

Right Ctrl

12:43 PM

Luego iniciamos el servicio y comprobamos su estado

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~

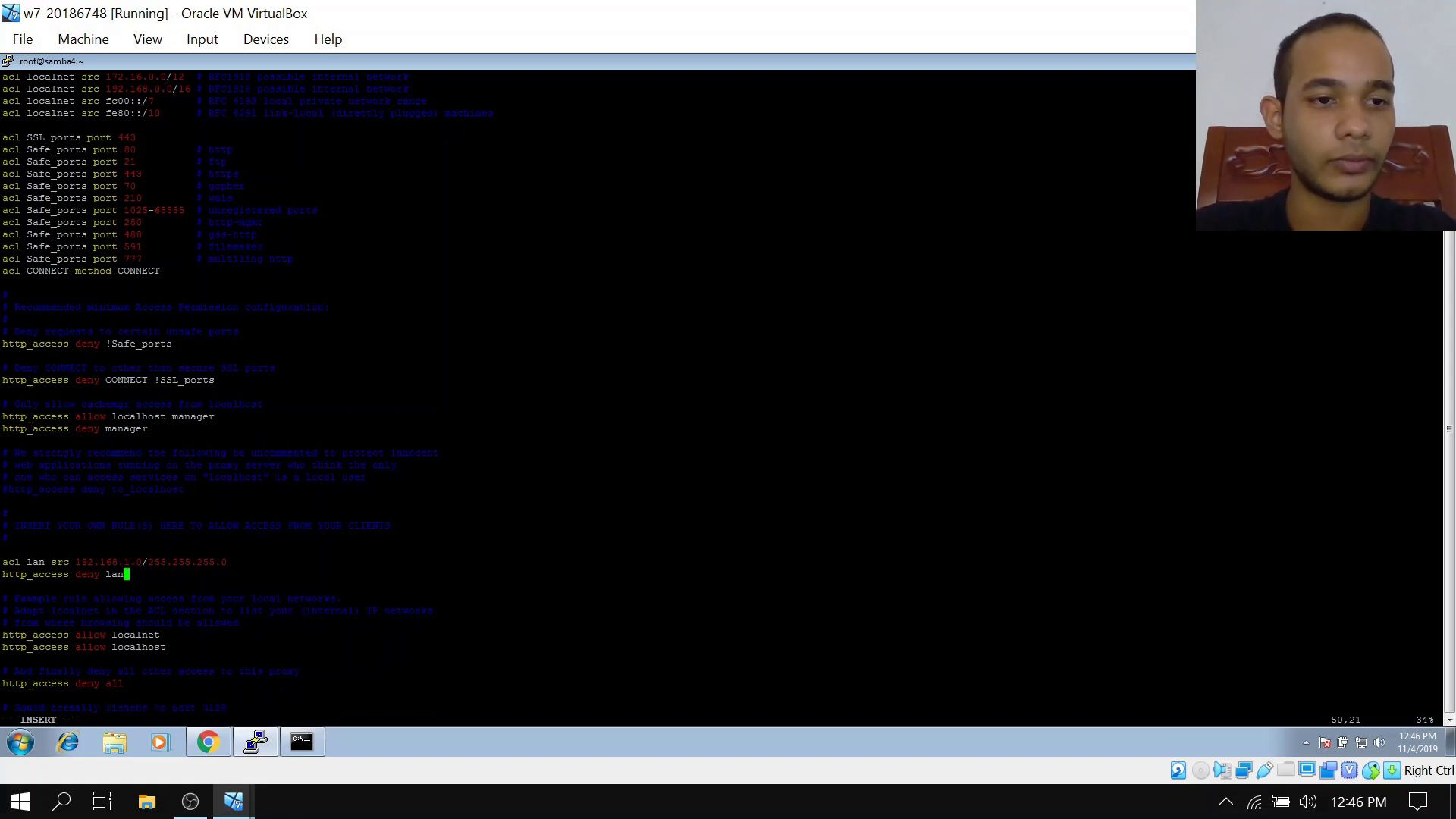
```
[root@samba4 ~]# systemctl start squid
[root@samba4 ~]# systemctl enable squid
[root@samba4 ~]# systemctl status squid
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-11-04 11:41:55 EST; 2min 25s ago
 Main PID: 4032 (squid)
   CGroup: /system.slice/squid.service
           ├─4032 /usr/sbin/squid -f /etc/squid/squid.conf
           ├─4034 (squid-1) -f /etc/squid/squid.conf
           └─4035 (logfile-daemon) /var/log/squid/access.log

Nov 04 11:41:55 samba4.centos.cc systemd[1]: Stopped Squid caching proxy.
Nov 04 11:41:55 samba4.centos.cc systemd[1]: Starting Squid caching proxy...
Nov 04 11:41:55 samba4.centos.cc systemd[1]: Started Squid caching proxy.
Nov 04 11:41:55 samba4.centos.cc squid[4032]: Squid Parent: will start 1 kids
Nov 04 11:41:55 samba4.centos.cc squid[4032]: Squid Parent: (squid-1) process 4034 started
[root@samba4 ~]#
```

12:44 PM
11/4/2019

Right Ctrl

12:44 PM

Accedemos al archivo de configuración **squid.conf** que se encuentra en el directorio **/etc/squid**, en este aplicaremos una regla para probar que todo funciona correctamente, y luego reiniciamos el servicio.


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(s) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl lan src 192.168.1.0/255.255.255.0
http_access deny lan
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access deny all
Squid normally listens to port 3128
-- INSERT --
50,21 34%
12:46 PM
11/4/2019
Right Ctrl
12:46 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~

```
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]#
```

12:46 PM
11/4/2019

Right Ctrl

12:46 PM

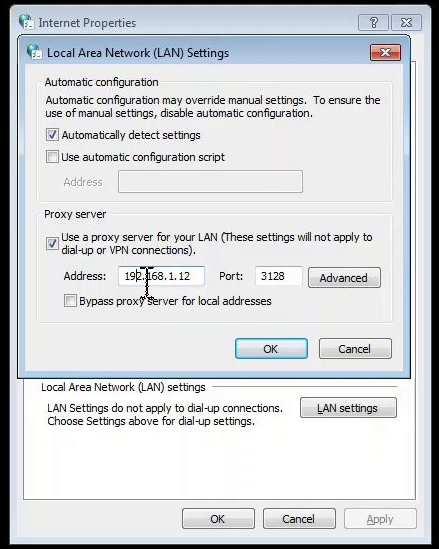
En el cliente nos vamos a las configuraciones de internet, podemos acceder simplemente colocando proxy como parametro de busqueda. En conecciones nos vamos a configuración de la LAN donde colocamos la ip del servidor y el puerto del proxy. Probamos la regla yendo al navegador y buscando una web

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~

```
[root@samba4 ~]#
```



12:46 PM
11/4/2019

Right Ctrl

12:46 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

www.google.com

google.com/search?q=google&rlz=1C1GCEU_enDO874DO874&oq=goog&aqs=chrome.0.69i59j69i57j69i60l2.819j0j7&sourceid=chrome&ie=UTF-8

This site can't be reached

The webpage at **https://www.google.com/search?q=google&rlz=1C1GCEU_enDO874DO874&oq=goog&aqs=chrome.0.69i59j69i57j69i60l2.819j0j7&sourceid=chrome&ie=UTF-8** might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED

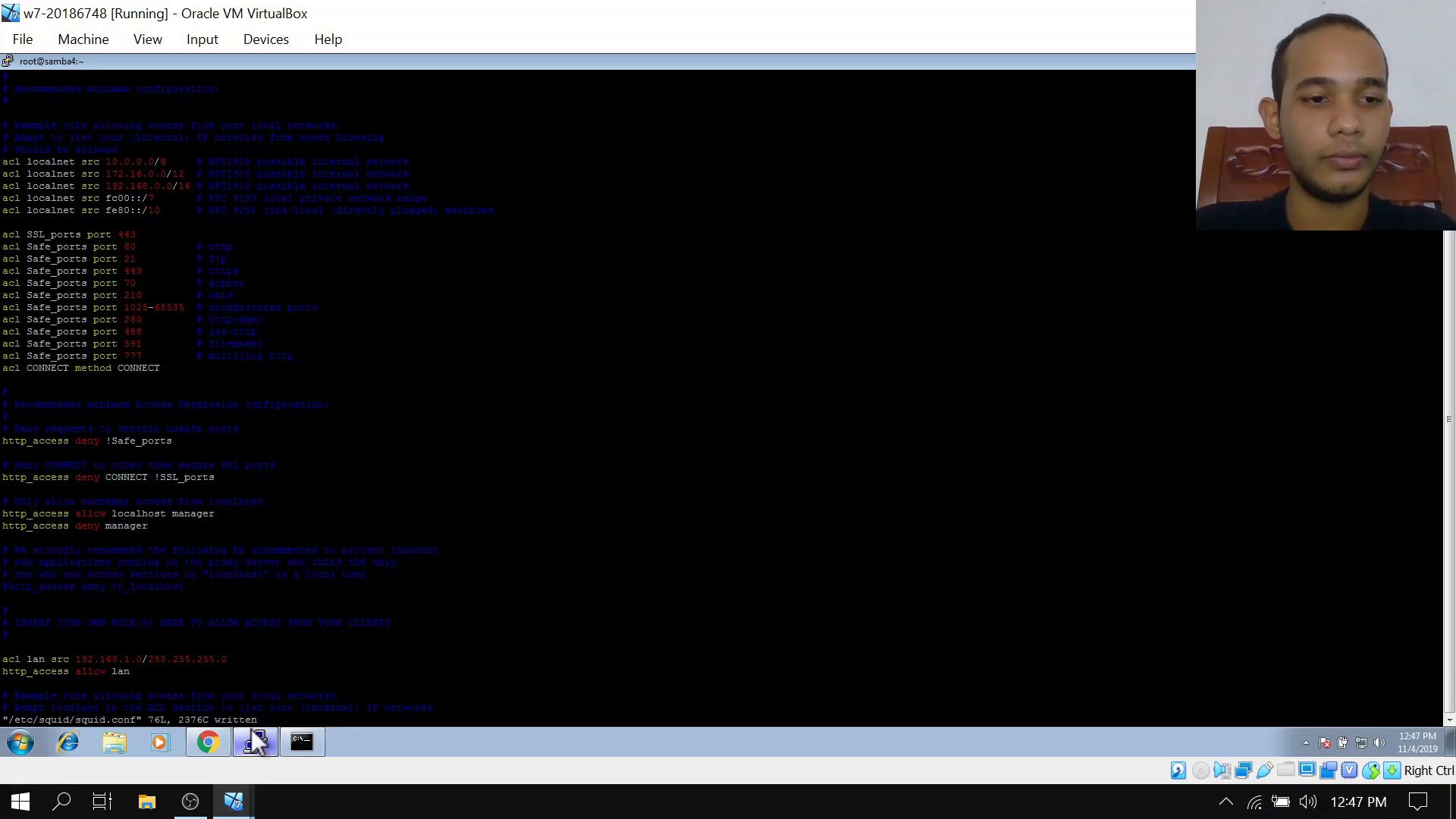
12:46 PM
11/4/2019

Right Ctrl

12:46 PM

Bloqueando y permitiendo redes

Para permitir una red colocamos una nueva lista de acceso **acl** con el nombre que queramos y luego establecemos la fuente **src** con la red que queremos bloquear luego en **http_access** permitimos con **allow** y colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
#
Recommended minimum configuration:
#
Example rule allowing access from your local networks.
Adapt to list your (internal) IP networks from where browsing
should be allowed
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(s) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl lan src 192.168.1.0/255.255.255.0
http_access allow lan
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
"/etc/squid/squid.conf" 76L, 2376C written
12:47 PM
11/4/2019
Right Ctrl
12:47 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

google - Buscar con Google

google.com/search?q=google&rlz=1C1GCEU_enDO874DO874&oq=goog&aqs=chrome.0.69i59j69i57j69i60l2.819j0j7&sourceid=chrome&ie=UTF-8

Google

google

Todos Imágenes Maps Videos Noticias Más Preferencias Herramientas

Cerca de 20,480,000,000 resultados (0.48 segundos)

Google
https://www.google.es
Collections · Even more from **Google** · Sign in. **Google**. ×. ×. REPORT THIS. CANCEL. OK. DELETE. **Google** offered in: español. Location unavailable - -.

Google
https://www.google.com › ...
Google. Búsqueda avanzadaHerramientas de idioma · Programas de publicidadTodo acerca de **GoogleGoogle**.com in English. © 2019 - Privacidad ...

Google Accounts: Sign in
https://accounts.google.com
Use your **Google** Account. Email or phone. Forgot email? Type the text you hear or see. Not your computer? Use Guest mode to sign in privately. Learn more.

Inicia sesión: Cuentas de Google
https://adssettings.google.com › authenticated
Utiliza tu cuenta de **Google**. Correo electrónico o teléfono. ¿Has olvidado tu correo electrónico? Escribe el texto que escuches o veas. ¿No es tu ordenador?

Google to acquire Fitbit - The Keyword
https://www.blog.google › agreement-with-fitbit ▾ Traducir esta página
hace 3 días - Today, we're announcing that **Google** has entered into a definitive agreement to acquire Fitbit, a leading wearables brand. We believe ...

Noticias destacadas

Google
Compañía

Google LLC es una compañía principal subsidiaria de la multinacional estadounidense Alphabet Inc., cuya especialización son los productos y servicios relacionados con Internet, software, dispositivos electrónicos y otras tecnologías. Wikipedia

Director ejecutivo: Sundar Pichai (2 de octubre de 2015–)
Tendencias

Fundación: 4 de septiembre de 1998, Menlo Park, California, Estados Unidos

Oficinas centrales: Mountain View, California, Estados Unidos

Organización principal: Alphabet Inc. (2015–)

Filiales: YouTube, Google.org, DoubleClick, AdMob, Nest Labs, MÁS

Fundadores: Larry Page, Serguéi Brin

También se buscó Ver 15 más

Instagram Twitter Yahoo! Netflix Amazon

Renuncia de responsabilidad Comentarios

Looking for results in English?
Change to English
Continuar usando español
Configuración del idioma

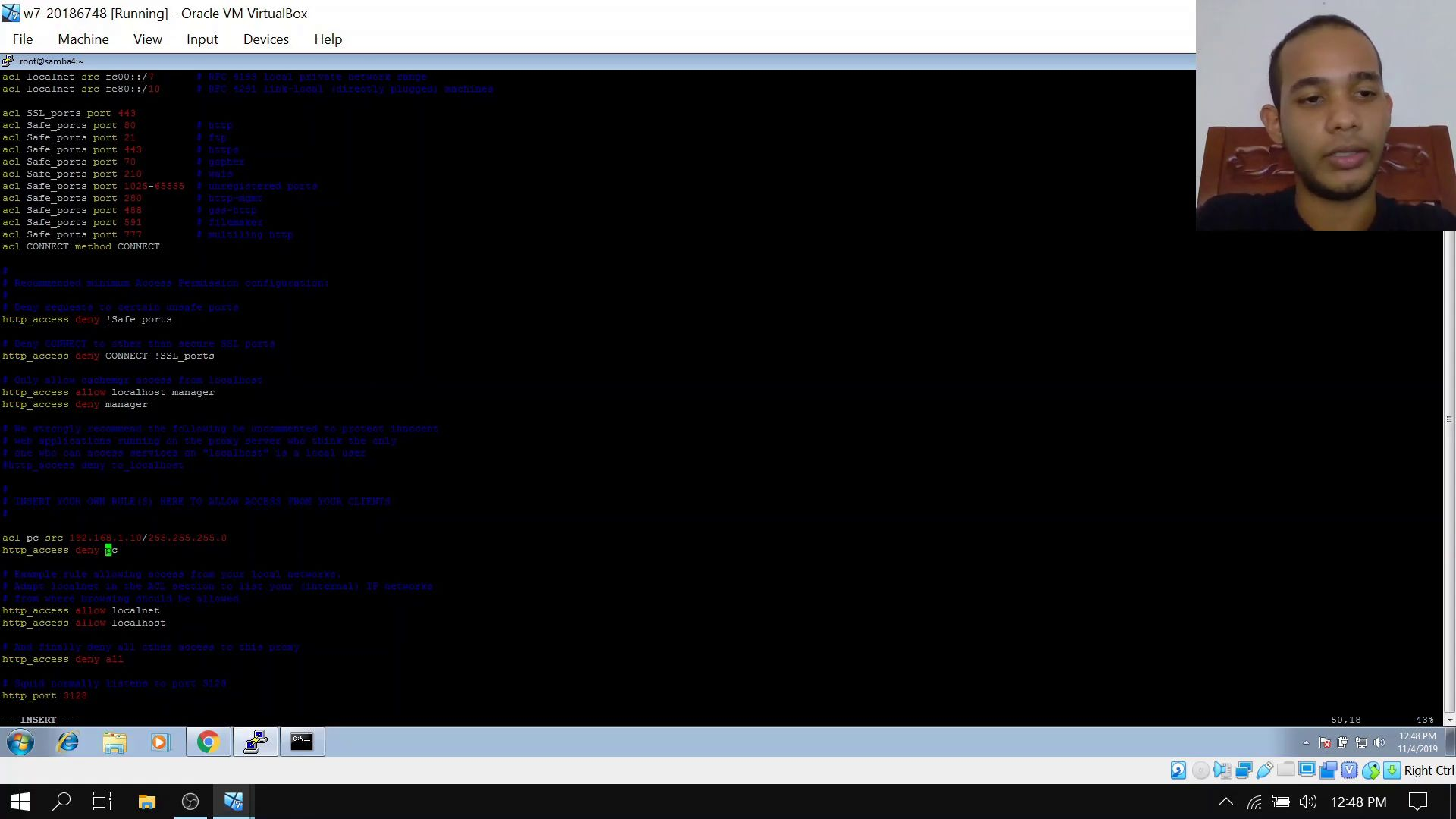
Waiting for www.google.com...

12:47 PM 11/4/2019

Right Ctrl

12:47 PM

Para bloquear una red colocamos una nueva lista de acceso **acl** con el nombre que queramos y luego establecemos la fuente **src** con la red que queremos bloquear luego en **http_access** negamos con **deny** y colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl pc src 192.168.1.10/255.255.255.0
http_access deny pc
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access deny all
Squid normally listens to port 3128
http_port 3128
-- INSERT --
50,18 43%
12:48 PM
11/4/2019
Right Ctrl
12:48 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

www.google.com

google.com/webhp?hl=es-419&sa=X&ved=0ahUKEwj5paqMgdHIAhUCyFkKHRK1D3IQPAgH

This site can't be reached

The webpage at **https://www.google.com/webhp?hl=es-419&sa=X&ved=0ahUKEwj5paqMgdHIAhUCyFkKHRK1D3IQPAgH** might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED

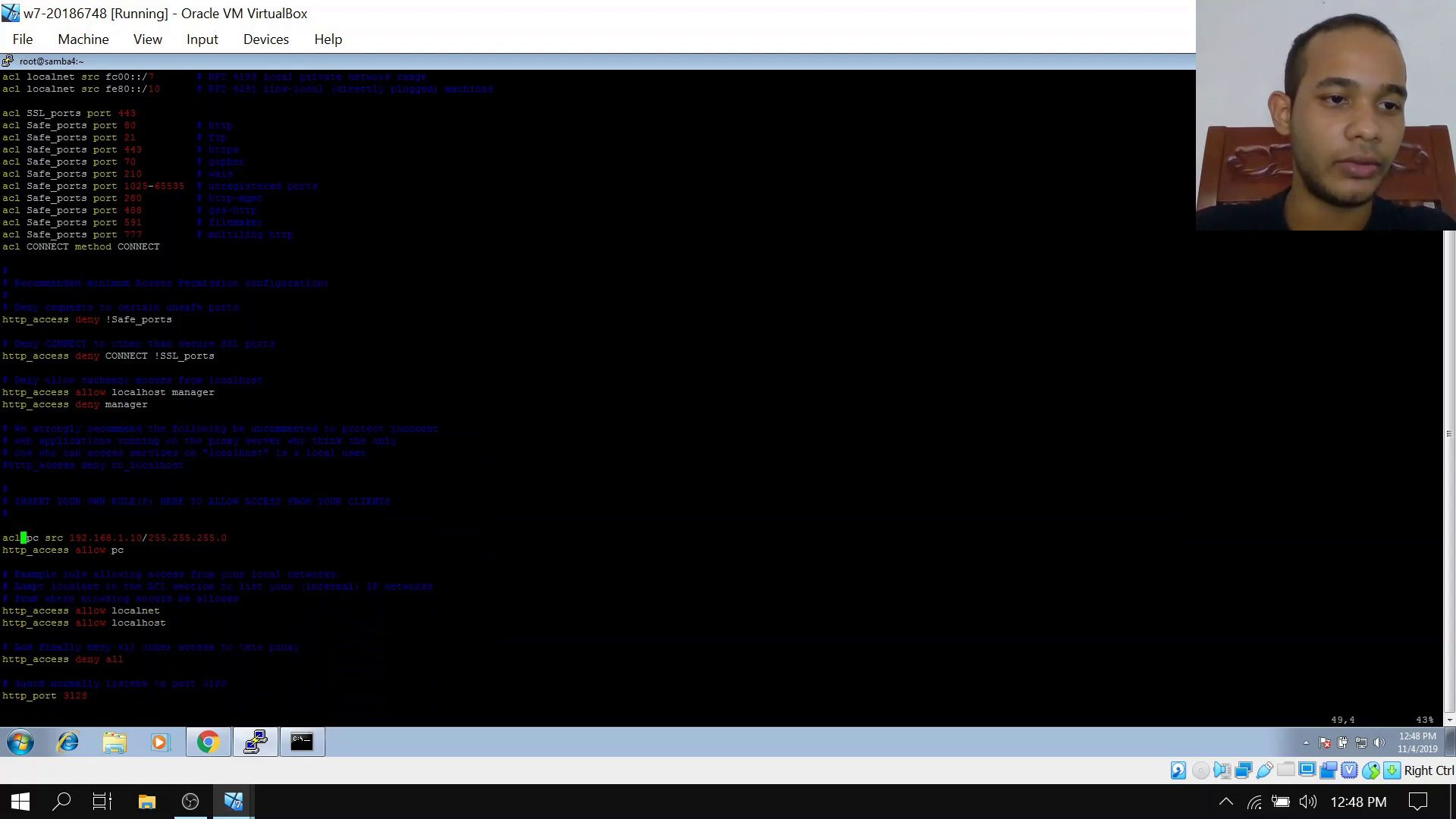
12:48 PM
11/4/2019

Right Ctrl

12:48 PM

Bloqueando y permitiendo equipos

Para permitir un equipo colocamos una nueva lista de acceso **acl** con el nombre que queramos y luego establecemos la fuente **src** con la ip de la queremos permitir, o, con **arp** establecemos su dirección mac. Luego en **http_access** permitimos con **allow** y colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
acl pc src 192.168.1.10/255.255.255.0
http_access allow pc
http_access allow localnet
http_access allow localhost
http_access deny all
http_port 3128
49,4 43%
12:48 PM
11/4/2019
Right Ctrl
12:48 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

www.google.com

google.com/webhp?hl=es-419&sa=X&ved=0ahUKEwj5paqMgdHIAhUCyFkKHRK1D3IQPAgH

This site can't be reached

The webpage at **https://www.google.com/webhp?hl=es-419&sa=X&ved=0ahUKEwj5paqMgdHIAhUCyFkKHRK1D3IQPAgH** might be temporarily down or it may have moved permanently to a new web address.

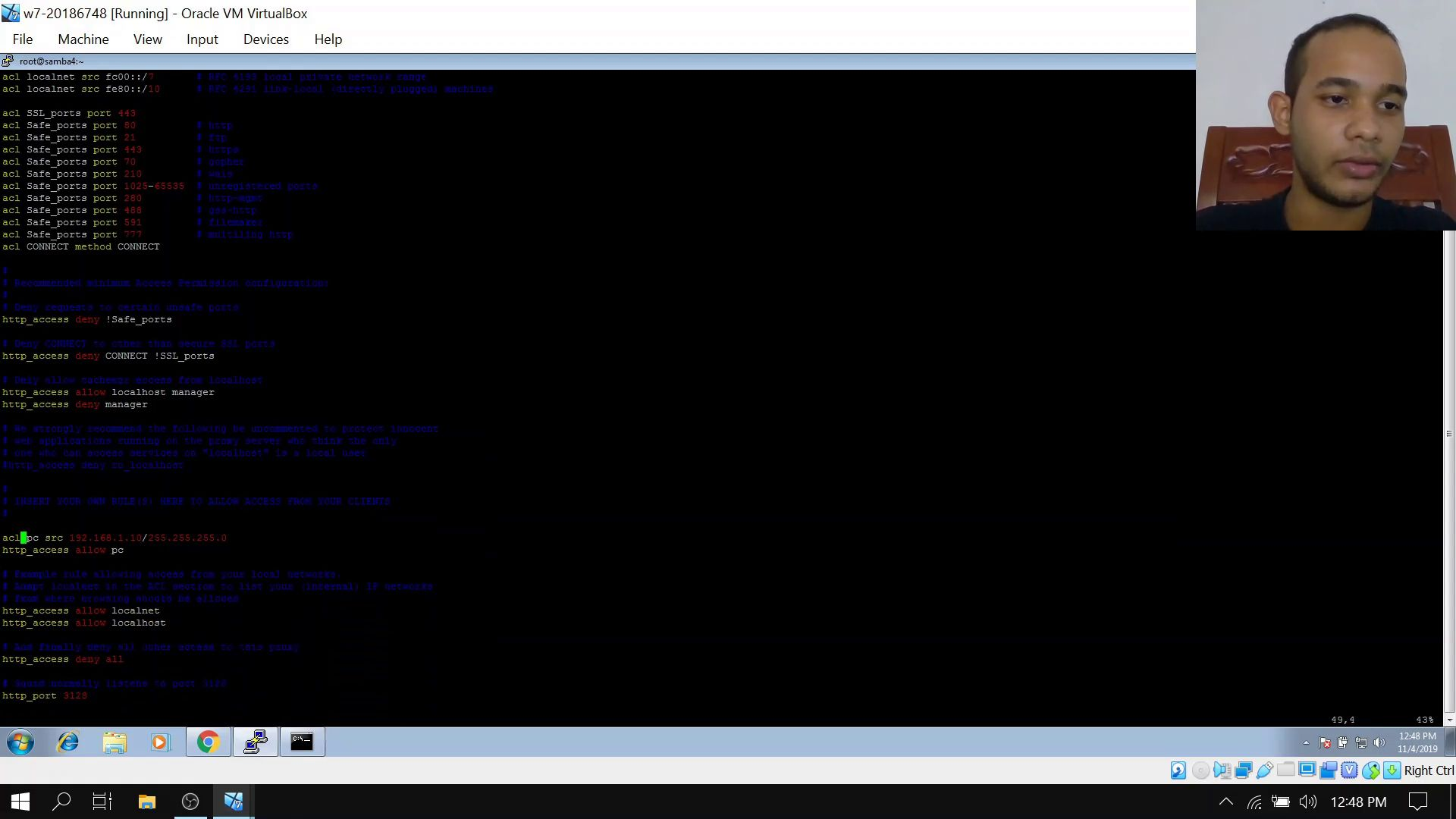
ERR_TUNNEL_CONNECTION_FAILED

12:48 PM
11/4/2019

Right Ctrl

12:48 PM

Para bloquear un equipo colocamos una nueva lista de acceso **acl** con el nombre que queramos y luego establecemos la fuente **src** con la ip de la queremos permitir, o, con **arp** establecemos su dirección mac. Luego en **http_access** negamos con **deny** y colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
acl pc src 192.168.1.10/255.255.255.0
http_access allow pc
http_access allow localnet
http_access allow localhost
http_access deny all
http_port 3128
49,4 43%
12:48 PM
11/4/2019
Right Ctrl
12:48 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Google

google.com/webhp?hl=es-419&sa=X&ved=0ahUKEwj5paqMgdHIAhUCyFkKHRK1D3IQPAgH

Google

Buscar con Google Me siento con suerte

República Dominicana

Publicidad Negocios Sobre Google Cómo funciona la Búsqueda Privacidad Condiciones Preferencias

Waiting for www.google.com...

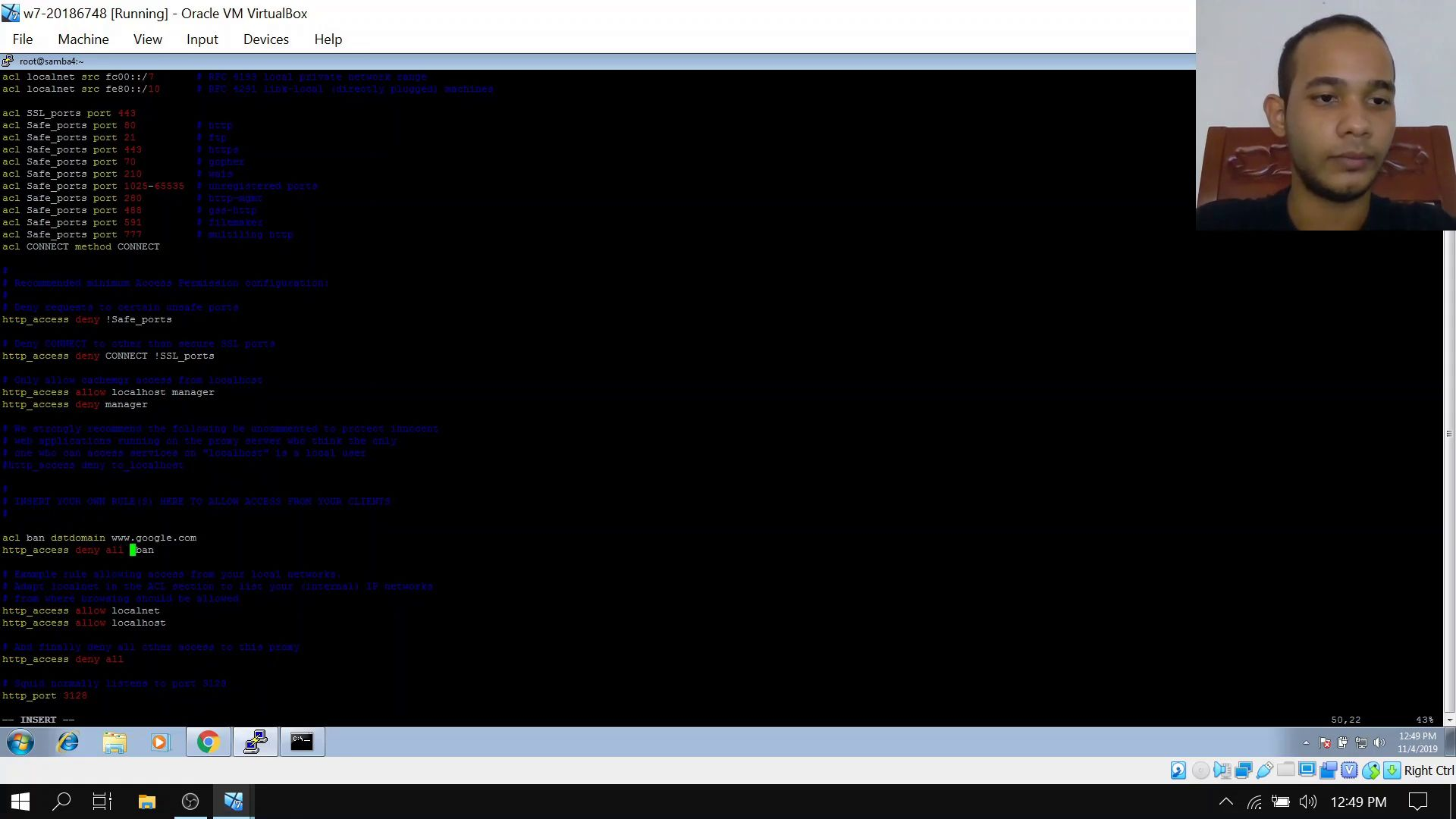
12:48 PM
11/4/2019

Right Ctrl

12:48 PM

Bloqueando y permitiendo páginas web

Para bloquear una web en específico colocamos una nueva lista de acceso **acl** con el nombre que queramos y con **dstdomain** colocamos la dirección web. Luego en **http_access** negamos con **deny** y colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl ban dstdomain www.google.com
http_access deny all ban
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access deny all
Squid normally listens to port 3128
http_port 3128
-- INSERT --
50,22 43%
12:49 PM
11/4/2019
Right Ctrl
12:49 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

DuckDuckGo — Privacy, simplifie

duckduckgo.com/?t=ht&natb=v193-6at&cp=atbdcc

DuckDuckGo

The search engine that doesn't track you. Help Spread DuckDuckGo!

www.google.com

google.com

This site can't be reached

The webpage at **https://www.google.com/** might be temporarily down or it may have moved permanently to a new web address.

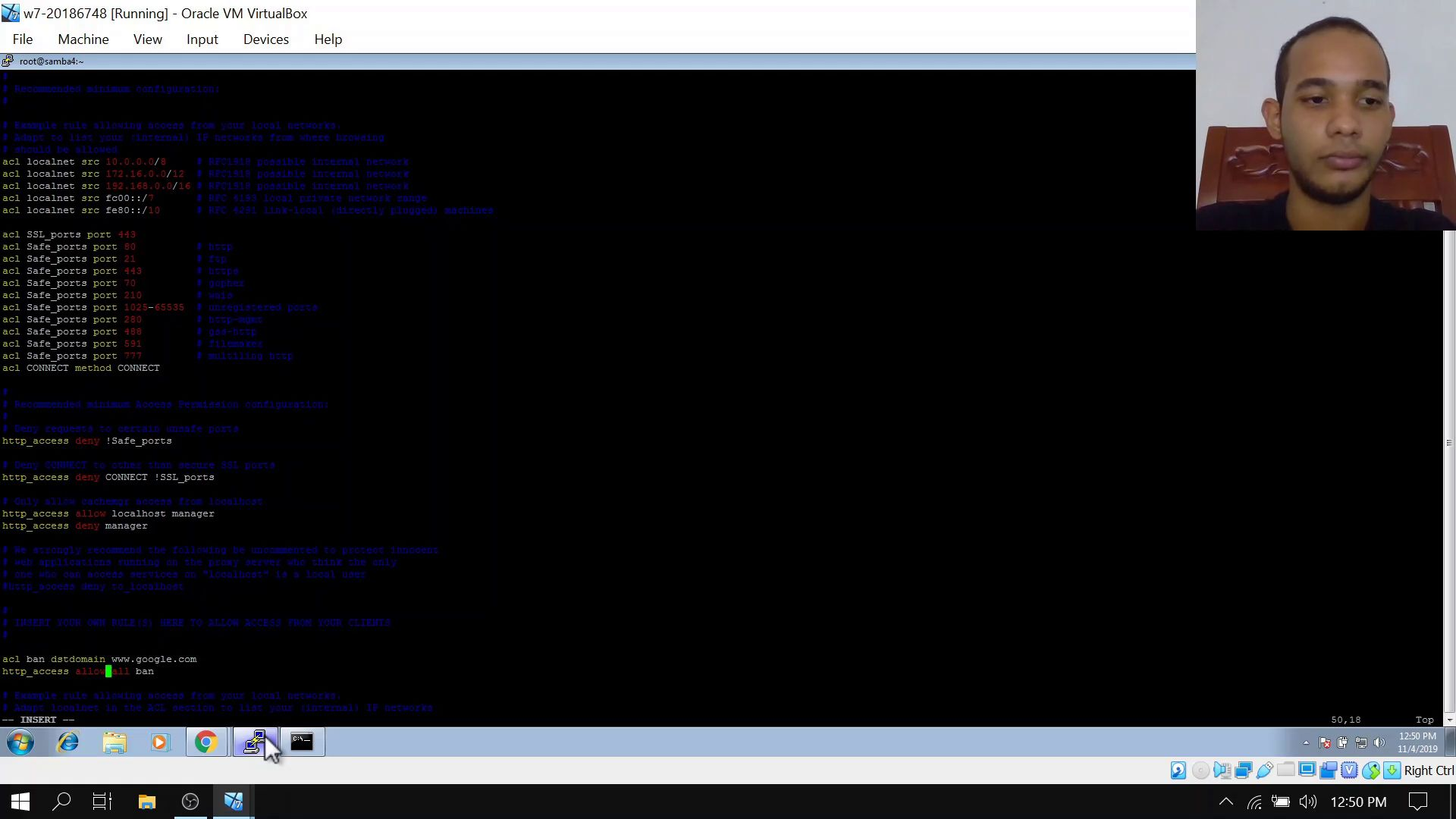
ERR_TUNNEL_CONNECTION_FAILED

12:49 PM
11/4/2019

Right Ctrl

12:49 PM

Para permitir una web en específico reemplazamos **deny** por **allow** en **http_access**, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
#
Recommended minimum configuration:
#
Example rule allowing access from your local networks.
Adapt to list your (internal) IP networks from where browsing
should be allowed
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(s) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl ban dstdomain www.google.com
http_access allow all ban
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
-- INSERT --
50,18 Top
12:50 PM
11/4/2019
Right Ctrl
12:50 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

DuckDuckGo — Privacy, simplifie

duckduckgo.com/?t=ht&natb=v193-6at&cp=atbdcc

DuckDuckGo

The search engine that doesn't track you. Help Spread DuckDuckGo!

Google

google.com

Trans

Google

Buscar con Google Me siento con suerte

Ofrecido por Google en: English

República Dominicana

Publicidad Negocios Sobre Google Cómo funciona la Búsqueda Privacidad Condiciones Preferencias

Waiting for cache...

12:50 PM
11/4/2019

Right Ctrl

12:50 PM

Bloqueando contenido

Para bloquear el contenido web colocamos una nueva lista de acceso **acl** con el nombre que queramos y con **urlpath_regex** colocamos el tipo de contenido como **\.[extensión]**. Luego en **http_access** negamos con **deny**, colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

acl img urlpath_regex \.jpg
http_access deny img

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256
```

50,16 56%

12:51 PM
11/4/2019

Right Ctrl

12:51 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Free Photos - Free Images - Free

Not secure | freedigitalphotos.net

freedigitalphotos.net

Log in Register

Home | Categories | Enter keyword(s) or image ID | SEARCH | Advanced search | Contact | CART - 0 Items

Free photos

Download free and premium stock photos and illustrations for websites, advertising materials, newspapers, magazines, ebooks, book covers and pages, music artwork, software applications and much more. All our free images are of high quality, produced by our community of professional stock photographers and digital illustrators.

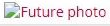
Royalty free photos for business and personal use

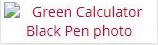
Our free photos and illustrations are ideal for business, personal and educational use. Every image is free, with an option to buy larger images at reasonable prices.

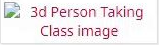
A huge range of free images!

We have a huge selection of photos and illustrations. Our most popular categories are pictures of people and business pictures.

POPULAR IMAGES







More popular images

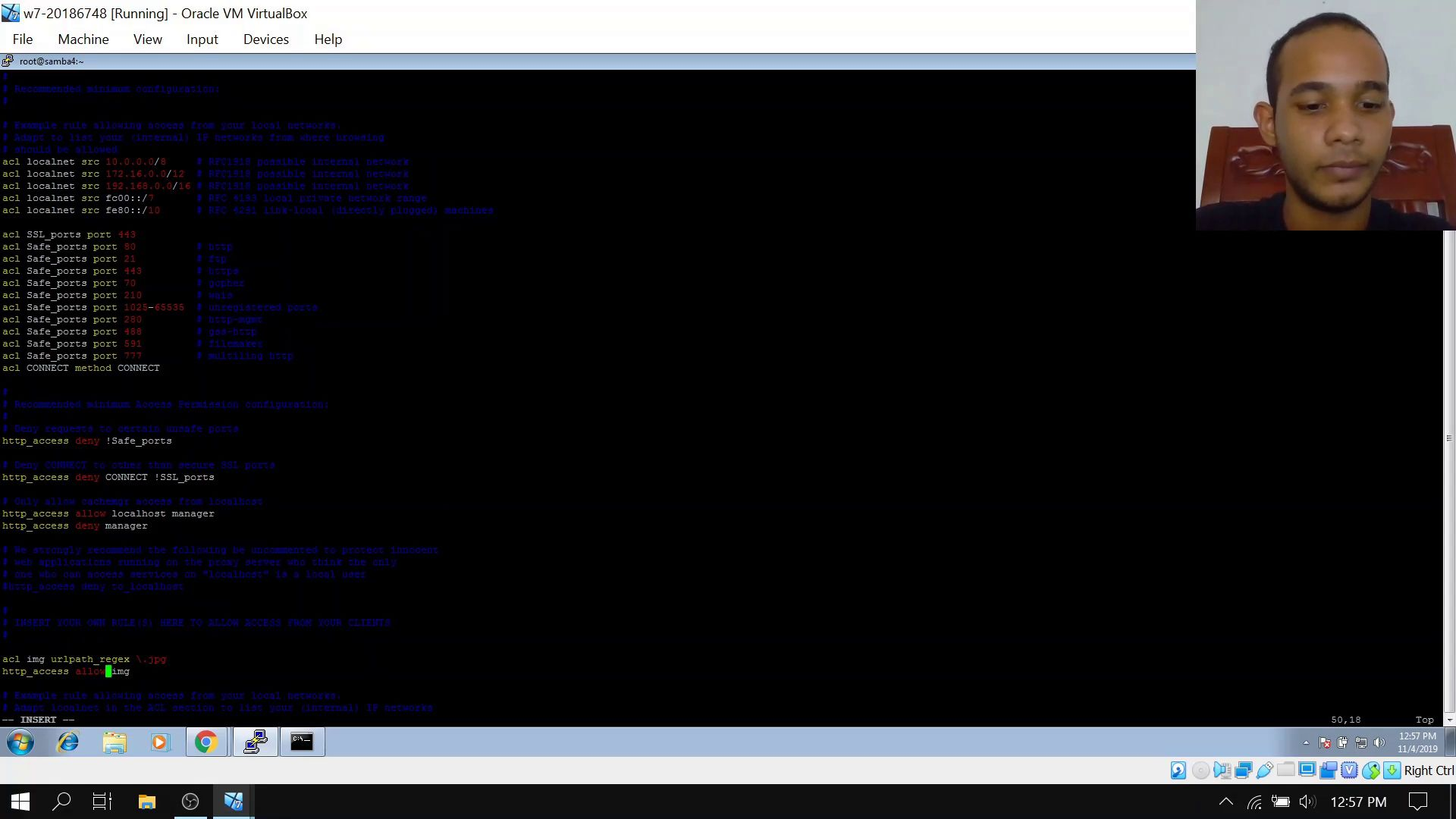
Establishing secure connection...

12:57 PM
11/4/2019

Right Ctrl

12:57 PM

Para permitir el contenido web reemplazamos **deny** por **allow** en **http_access**, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
#
Recommended minimum configuration:
#
Example rule allowing access from your local networks.
Adapt to list your (internal) IP networks from where browsing
should be allowed
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(s) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl img urlpath_regex \.jpg
http_access allow img
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
-- INSERT --
50,18 Top
12:57 PM
11/4/2019
Right Ctrl
12:57 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

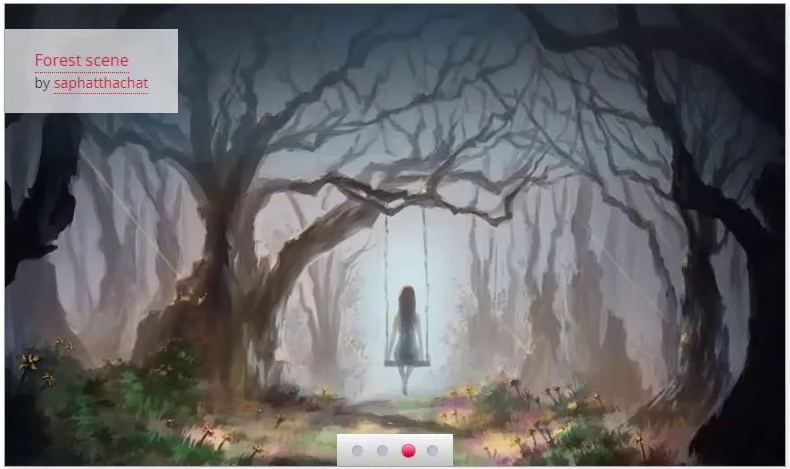
Free Photos - Free Images - Free

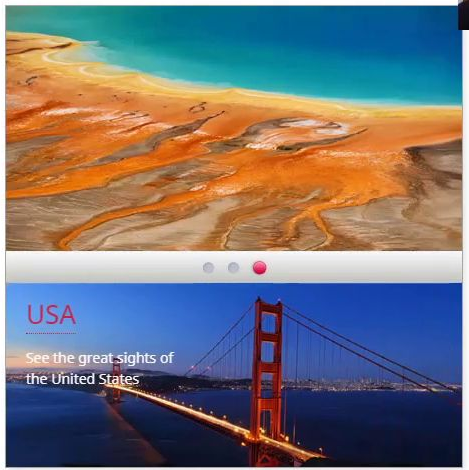
Not secure | freedigitalphotos.net

freedigitalphotos.net

Log in Register Like 29K

Home | Categories | Enter keyword(s) or image ID | SEARCH | Advanced search | Contact | CART - 0 Items





Free photos

Download free and premium stock photos and illustrations for websites, advertising materials, newspapers, magazines, ebooks, book covers and pages, music artwork, software applications and much more. All our free images are of high quality, produced by our community of professional stock photographers and digital illustrators.

Royalty free photos for business and personal use

Our free photos and illustrations are ideal for business, personal and educational use. Every image is free, with an option to buy larger images at reasonable prices.

A huge range of free images!

12:58 PM
11/4/2019

Right Ctrl

12:58 PM

Acceso por dia

Para bloquear el acceso a internet en dias especificos colocamos una nueva lista de acceso **acl** con el nombre que queramos y con **time** colocamos el o los días que se clasifican como **M T W H F S A** en el mismo orden. Luego en **http_access** negamos con **deny**, colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios

```
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

acl days time MTW
http_access deny days

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
"/etc/squid/squid.conf" 76L, 2356C written
```

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

www.google.com

google.com

This site can't be reached

The webpage at **https://www.google.com/** might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED

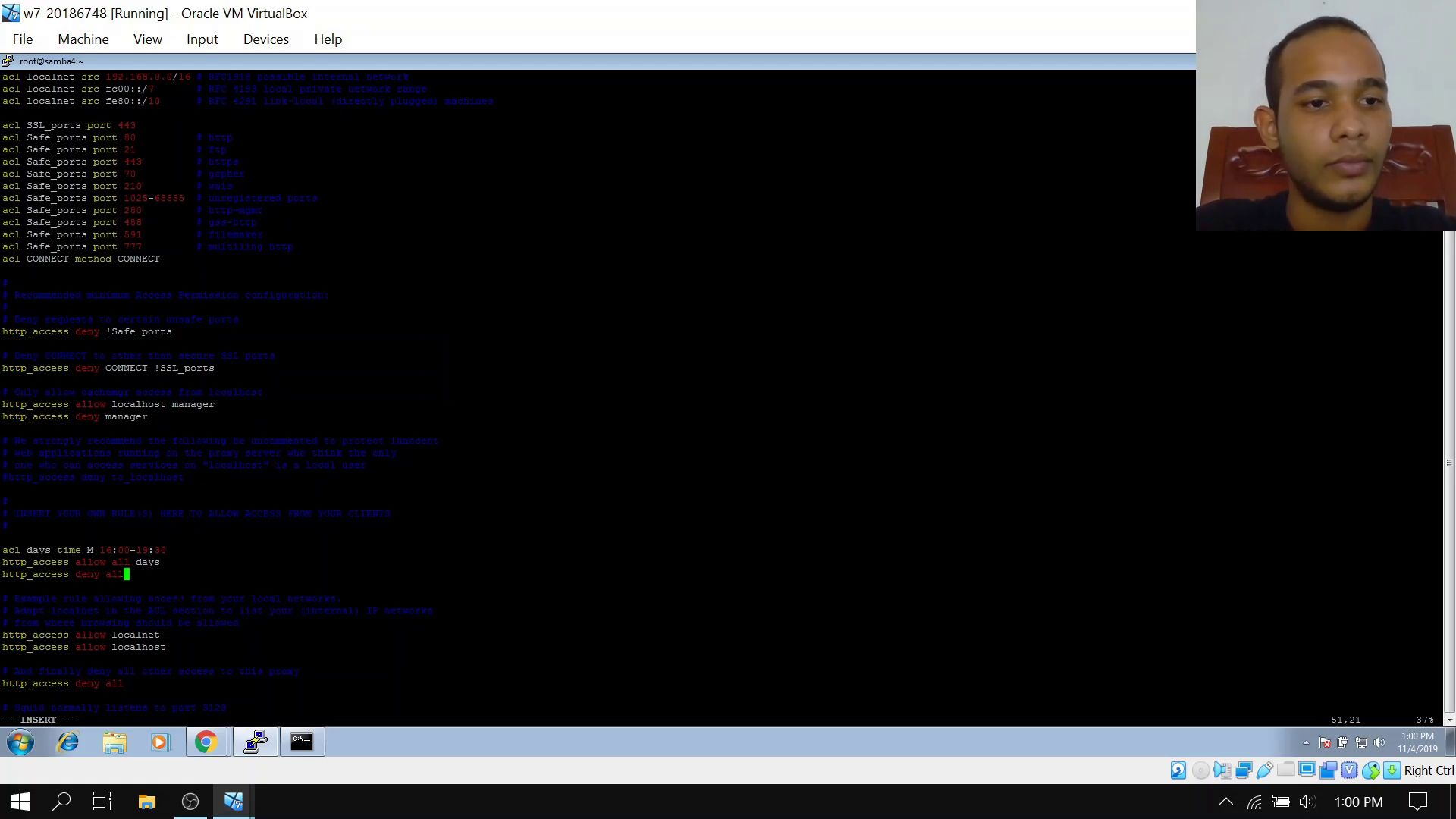
12:59 PM
11/4/2019

Right Ctrl

12:59 PM

Acceso por hora

Para bloquear o permitir el acceso a internet en horarios específicos colocamos una nueva lista de acceso **acl** con el nombre que queramos y con **time** establecemos un rango de tiempo en formato de 24 horas **00:00-23:59** Luego en **http_access** negamos o permitimos con **deny** o **allow** respectivamente, colocamos el nombre de la lista de acceso que acabamos de crear, y reiniciamos el servicio para aplicar los cambios


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(s) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl days time M 16:00-19:30
http_access allow all days
http_access deny all
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access deny all
Squid normally listens to port 3128
-- INSERT --
51,21 37%
1:00 PM
11/4/2019
Right Ctrl
1:00 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

www.google.com

google.com

This site can't be reached

The webpage at **https://www.google.com/** might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED

1:00 PM
11/4/2019

Right Ctrl

1:00 PM

Seguridad por usuario

Squid posee diversas herramientas para ser integradas con squid, estas se encuentran en el directorio **/usr/lib64/squid*,** en este caso usaremos la **basic_access_auth**

* El directorio lib en el que estas se encuentren puede variar dependiendo de la arquitectura de nuestro sistema

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~

```
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# ls /usr//lib64//squid/
basic_db_auth               basic_ncsa_auth   basic_radius_auth   basic_smb_lm_auth       digest_file_auth     ext_kerberos_ldap_group_acl  ext_unix_group_acl    log_file_daemon              ntlm_
basic_getpwnam_auth         basic_nis_auth    basic_sasl_auth     cachemgr.cgi            digest_ldap_auth     ext_ldap_group_acl           ext_wbinfo_group_acl  negotiate_kerberos_auth      ssl_crtd                  url_fake_rewrite.sh
basic_ldap_auth             basic_pam_auth    basic_smb_auth      cert_tool               diskd                ext_session_acl              helper-mux.pl         negotiate_kerberos_auth_test storeid_file_rewrite
basic_msnt_multi_domain_auth basic_pop3_auth  basic_smb_auth.sh  digest_edirectory_auth  ext_file_userip_acl  ext_time_quota_acl           log_db_daemon         ntlm_fake_auth               unlinkd
[root@samba4 ~]#
```

1:03 PM
11/4/2019

Right Ctrl

1:03 PM

En nuestro archivo de configuración **squid.conf** colocamos el parametro **auth_param basic program** donde colocamos la dirección del programa de autenticación y la dirección del archivo **.htpasswd** que crearemos más adelante, luego definimos un **realm**, y colocamos una nueva **acl** con **proxy_auth** como parámetro como **REQUIRED**, y generamos un nuevo **http_access** permitiendo esta nueva **acl**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~

```
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

auht_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/.htpasswd
auth_param basic realm Squid Basic Authentication
acl pass proxy_auth REQUIRED
http_access allow pass


# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid
```

-- INSERT -- 52,23 73%

1:06 PM
11/4/2019

Right Ctrl

1:06 PM

Por último creamos el archivo **.htpasswd** en el la ruta que colocamos en el **squid.conf**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:/etc/squid

```
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# systemctl restart squid
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# ls /usr//lib64//squid/
basic_db_auth               basic_ncsa_auth   basic_radius_auth  basic_smb_lm_auth       digest_file_auth     ext_kerberos_ldap_group_acl  ext_unix_group_acl    log_file_daemon              ntlm_
basic_getpwnam_auth         basic_nis_auth    basic_sasl_auth    cachemgr.cgi            digest_ldap_auth     ext_ldap_group_acl           ext_wbinfo_group_acl  negotiate_kerberos_auth      ssl_crtd              url_fake_rewrite.sh
basic_ldap_auth             basic_pam_auth    basic_smb_auth     cert_tool               diskd                ext_session_acl              helper-mux.pl         negotiate_kerberos_auth_test storeid_file_rewrite
basic_msnt_multi_domain_auth basic_pop3_auth  basic_smb_auth.sh  digest_edirectory_auth  ext_file_userip_acl  ext_time_quota_acl           log_db_daemon         ntlm_fake_auth               unlinkd
[root@samba4 ~]# vim /etc/se
securetty       security/       selinux/        services        sestatus.conf   setroubleshoot/ setuptool.d/
[root@samba4 ~]# vim /etc/squid/squid.conf
[root@samba4 ~]# cd /etc/squid/
[root@samba4 squid]# ls
banned.txt  cachemgr.conf  cachemgr.conf.default  errorpage.css  errorpage.css.default  mime.conf  mime.conf.default  squid.conf  squid.conf.backup  squid.conf.default  squid.conf.test  test
[root@samba4 squid]# touch .htpassw
```

1:06 PM
11/4/2019

Right Ctrl

1:06 PM

Con la herramienta **htpasswd** generamos un nuevo usuario dentro del archivo, para esto usamos **htpasswd -c [dirección del archivo] [usuario]**. Luego reiniciamos el servicio y en el cliente abrimos el navegador

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:/etc/squid

```
[root@samba4 squid]# htpassw -c .htpasswd test1
-bash: htpassw: command not found
[root@samba4 squid]# htpasswd -c .htpasswd test1
New password:
Re-type new password:
Adding password for user test1
[root@samba4 squid]#
```

1:07 PM
11/4/2019

Right Ctrl

1:07 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Untitled

Search Google or type a URL

Sign in

The proxy http://192.168.1.12:3128 requires a username and password.

Your connection to this site is not private

Username test1

Password ••••

Sign in Cancel

1:08 PM
11/4/2019

Right Ctrl

1:08 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Google

google.com

Google

Buscar con Google Me siento con suerte

Ofrecido por Google en: English

República Dominicana

Publicidad Negocios Sobre Google Cómo funciona la Búsqueda Privacidad Condiciones Preferencias

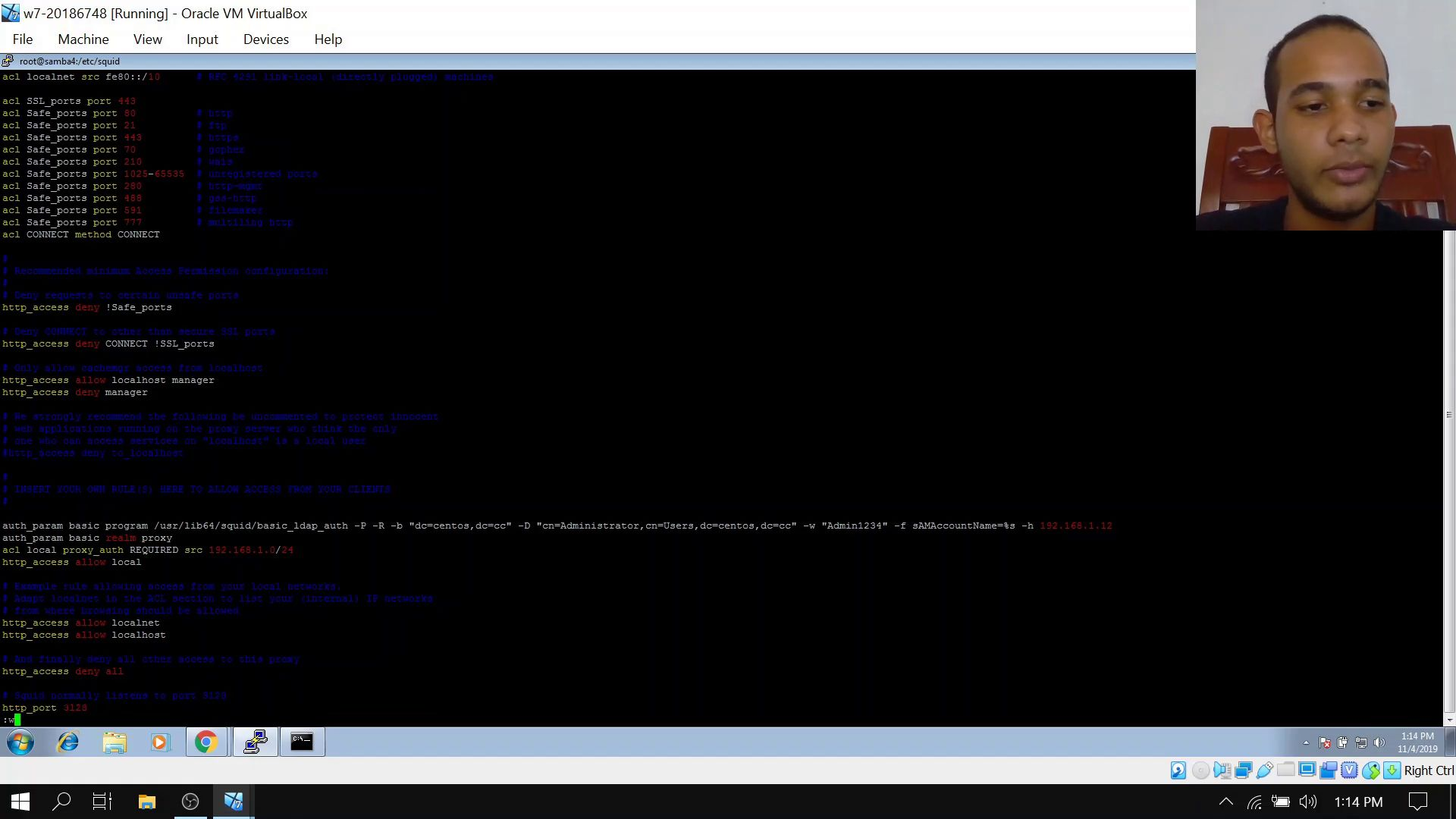
1:08 PM
11/4/2019

Right Ctrl

1:08 PM

Seguridad con Active Directory

Para establecer la autenticación con los usuarios de nuestro dominio con la herramienta ldap_auth, establecemos las opciones **-P -R -b** luego colocamos nuestro controlador de dominio cono **“dc=dominio,dc=com”** con la opción **-D** establecemos el nombre del administrador dentro del dominio**,** con la opción **-w** establecemos su contraseña y con **-h** la ip del controlador de dominio. Luego establecemos las mismas reglas que antes, y para aplicar los cambios reiniciamos el servicio


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:/etc/squid
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
auth_param basic program /usr/lib64/squid/basic_ldap_auth -P -R -b "dc=centos,dc=cc" -D "cn=Administrator,cn=Users,dc=centos,dc=cc" -w "Admin1234" -f sAMAccountName=%s -h 192.168.1.12
auth_param basic realm proxy
acl local_proxy_auth REQUIRED src 192.168.1.0/24
http_access allow local
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access deny all
Squid normally listens to port 3128
http_port 3128
:w
1:14 PM
11/4/2019
Right Ctrl
1:14 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Untitled

Search Google or type a URL

Sign in

The proxy http://192.168.1.[redacted]:3128 requires a username and password.

Your connection to this site is not private

Username

Password

Sign in Cancel

1:14 PM
11/4/2019

Right Ctrl

1:14 PM

Squid con sarg

Primero instalamos los paquetes que utilizaremos para compilar e implementar sarg.

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:/etc/squid

```
[root@samba4 squid]# yum install -y gcc gd gd-devel make perl-GD httpd
```

2:08 PM
11/4/2019

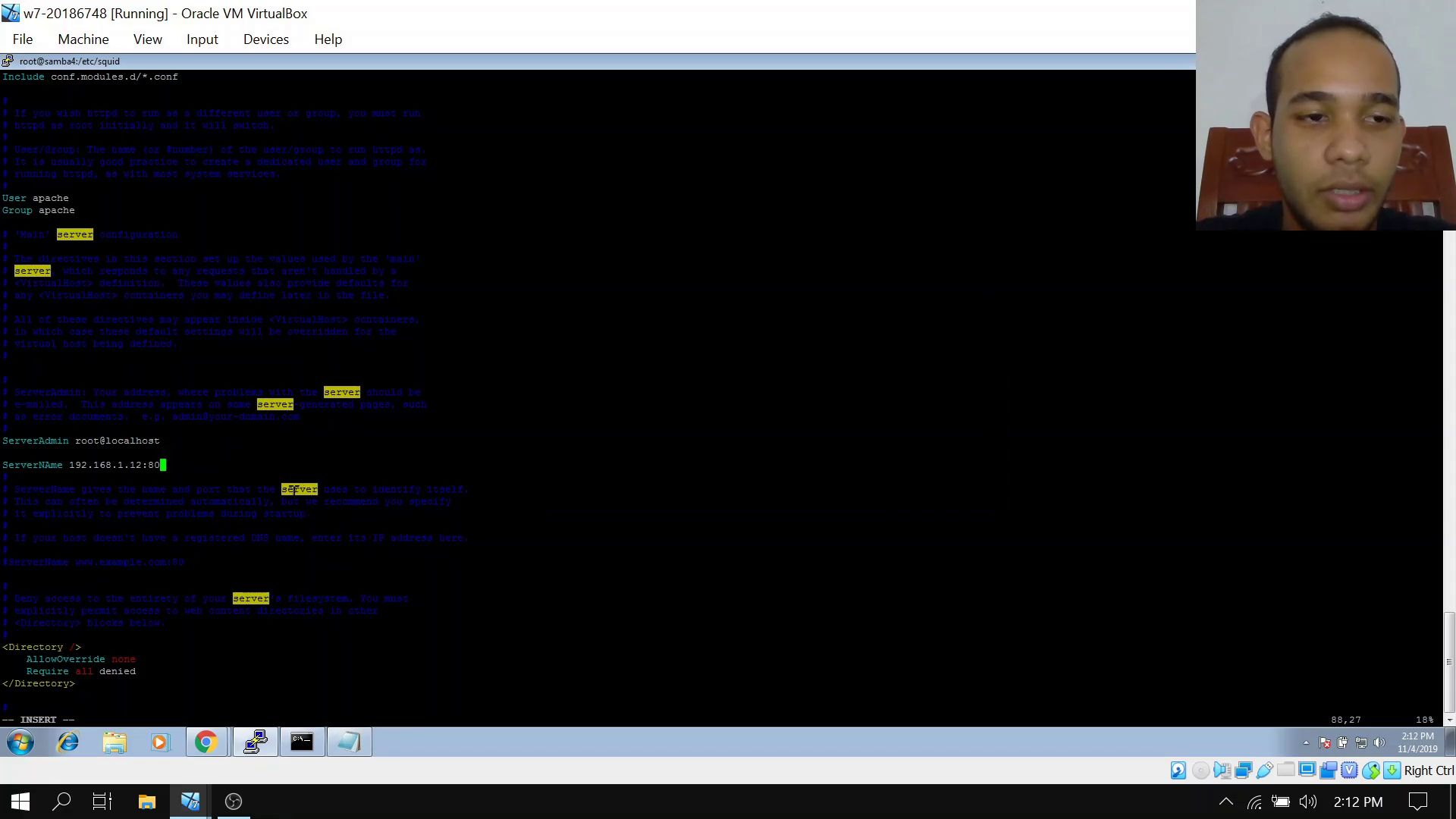
Right Ctrl

2:08 PM

Luego procedemos a configurar apache, donde primero iniciamos el servicio con **systemctl start httpd**

```
  Installing : libXext-1.3.3-3.el7.x86_64
  Installing : libXt-1.1.5-3.el7.x86_64
  Installing : libXpm-devel-3.5.12-1.el7.x86_64
  Installing : expat-devel-2.1.0-10.el7_3.x86_64
  Installing : fontconfig-devel-2.13.0-4.3.el7.x86_64
  Installing : mailcap-2.1.41-2.el7.noarch
  Installing : httpd-2.4.6-90.el7.centos.x86_64
  Installing : gd-devel-2.0.35-26.el7.x86_64
  Installing : perl-GD-2.49-3.el7.x86_64
  Verifying  : libXext-1.3.3-3.el7.x86_64
  Verifying  : fontconfig-2.13.0-4.3.el7.x86_64
  Verifying  : 2:libpng-devel-1.5.13-7.el7_2.x86_64
  Verifying  : mailcap-2.1.41-2.el7.noarch
  Verifying  : libjpeg-turbo-devel-1.2.90-8.el7.x86_64                    5/29
  Verifying  : httpd-2.4.6-90.el7.centos.x86_64                           6/29
  Verifying  : libXt-1.1.5-3.el7.x86_64                                   7/29
  Verifying  : libICE-1.0.9-9.el7.x86_64                                  8/29
  Verifying  : dejavu-fonts-common-2.33-6.el7.noarch                      9/29
  Verifying  : fontpackages-filesystem-1.44-8.el7.noarch                 10/29
  Verifying  : expat-devel-2.1.0-10.el7_3.x86_64                         11/29
  Verifying  : fontconfig-devel-2.13.0-4.3.el7.x86_64                    12/29
  Verifying  : perl-GD-2.49-3.el7.x86_64                                 13/29
  Verifying  : xorg-x11-proto-devel-2018.4-1.el7.noarch                  14/29
  Verifying  : libXpm-devel-3.5.12-1.el7.x86_64                          15/29
  Verifying  : libX11-1.6.7-2.el7.x86_64                                 16/29
  Verifying  : libX11-common-1.6.7-2.el7.noarch                          17/29
  Verifying  : libxcb-1.13-1.el7.x86_64                                  18/29
  Verifying  : freetype-devel-2.8-14.el7.x86_64                          19/29
  Verifying  : libXpm-3.5.12-1.el7.x86_64                                20/29
  Verifying  : libjpeg-turbo-1.2.90-8.el7.x86_64                         21/29
  Verifying  : gd-devel-2.0.35-26.el7.x86_64                             22/29
  Verifying  : dejavu-sans-fonts-2.33-6.el7.noarch                       23/29
  Verifying  : gd-2.0.35-26.el7.x86_64                                   24/29
  Verifying  : libxcb-devel-1.13-1.el7.x86_64                            25/29
  Verifying  : libXau-1.0.8-2.el7.x86_64                                 26/29
  Verifying  : libSM-1.2.2-2.el7.x86_64                                  27/29
  Verifying  : libX11-devel-1.6.7-2.el7.x86_64                           28/29
  Verifying  : libXau-devel-1.0.8-2.el7.x86_64                           29/29

Installed:
  gd.x86_64 0:2.0.35-26.el7                    gd-devel.x86_64 0:2.0.35-26.el7                    httpd.x86_64 0:2.4.6-90.el7.centos                    perl-GD.x86_64 0:2.49-3.el7

Dependency Installed:
  dejavu-fonts-common.noarch 0:2.33-6.el7          dejavu-sans-fonts.noarch 0:2.33-6.el7          expat-devel.x86_64 0:2.1.0-10.el7_3          fontconfig.x86_64 0:2.13.0-4.3.el7          fontconfig-devel.x86_64 0:2.13.0-4.3.el7
  fontpackages-filesystem.noarch 0:1.44-8.el7      freetype-devel.x86_64 0:2.8-14.el7             libICE.x86_64 0:1.0.9-9.el7                  libSM.x86_64 0:1.2.2-2.el7                  libX11.x86_64 0:1.6.7-2.el7
  libX11-common.noarch 0:1.6.7-2.el7               libX11-devel.x86_64 0:1.6.7-2.el7              libXau.x86_64 0:1.0.8-2.el7                  libXau-devel.x86_64 0:1.0.8-2.el7           libXext.x86_64 0:1.3.3-3.el7
  libXpm.x86_64 0:3.5.12-1.el7                     libXpm-devel.x86_64 0:3.5.12-1.el7             libXt.x86_64 0:1.1.5-3.el7                   libjpeg-turbo.x86_64 0:1.2.90-8.el7         libjpeg-turbo-devel.x86_64 0:1.2.90-8.el7
  libpng-devel.x86_64 2:1.5.13-7.el7_2             libxcb.x86_64 0:1.13-1.el7                     libxcb-devel.x86_64 0:1.13-1.el7             mailcap.noarch 0:2.1.41-2.el7               xorg-x11-proto-devel.noarch 0:2018.4-1.el7

Complete!
[root@samba4 squid]# systemctl start httpd
[root@samba4 squid]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@samba4 squid]#
```

En el archivo de configuración de colocamos la dirección de nuestro servidor como **ServerName**


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:/etc/squid
Include conf.modules.d/*.conf
User apache
Group apache
ServerAdmin root@localhost
ServerName 192.168.1.12:80
<Directory />
AllowOverride none
Require all denied
</Directory>
-- INSERT --
88,27 18%
2:12 PM
11/4/2019
Right Ctrl
2:12 PM

Luego permitimos el acceso en el puerto **80**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:/etc/squid

```
[root@samba4 squid]# firewall-cmd --add-port=80/tcp --zone=public --permanent
FirewallD is not running
[root@samba4 squid]# systemctl start firewalld
[root@samba4 squid]# firewall-cmd --add-port=80/tcp --zone=public --permanent
success
[root@samba4 squid]#
```

2:13 PM
11/4/2019

Right Ctrl

2:13 PM

Descargamos el paquete sarg para configurarlo en nuestro sistema con wget a través de la siguiente dirección web:

http://liquidtelecom.dl.sourceforge.net/project/sarg/sarg/sarg-2.3.10/sarg-2.3.10.tar.gz

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~/downloads

```
[root@samba4 downloads]# wget http://liquidtelecom.dl.sourceforge.net/project/sarg/sarg/sarg-2.3.10/sarg-2.3.10.tar.gz
--2019-11-04 13:13:28--  http://liquidtelecom.dl.sourceforge.net/project/sarg/sarg/sarg-2.3.10/sarg-2.3.10.tar.gz
Resolving liquidtelecom.dl.sourceforge.net (liquidtelecom.dl.sourceforge.net)...
```

2:13 PM
11/4/2019

Right Ctrl

2:13 PM

Con **tar -xvzf** desempaquetamos el archivo

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~/downloads

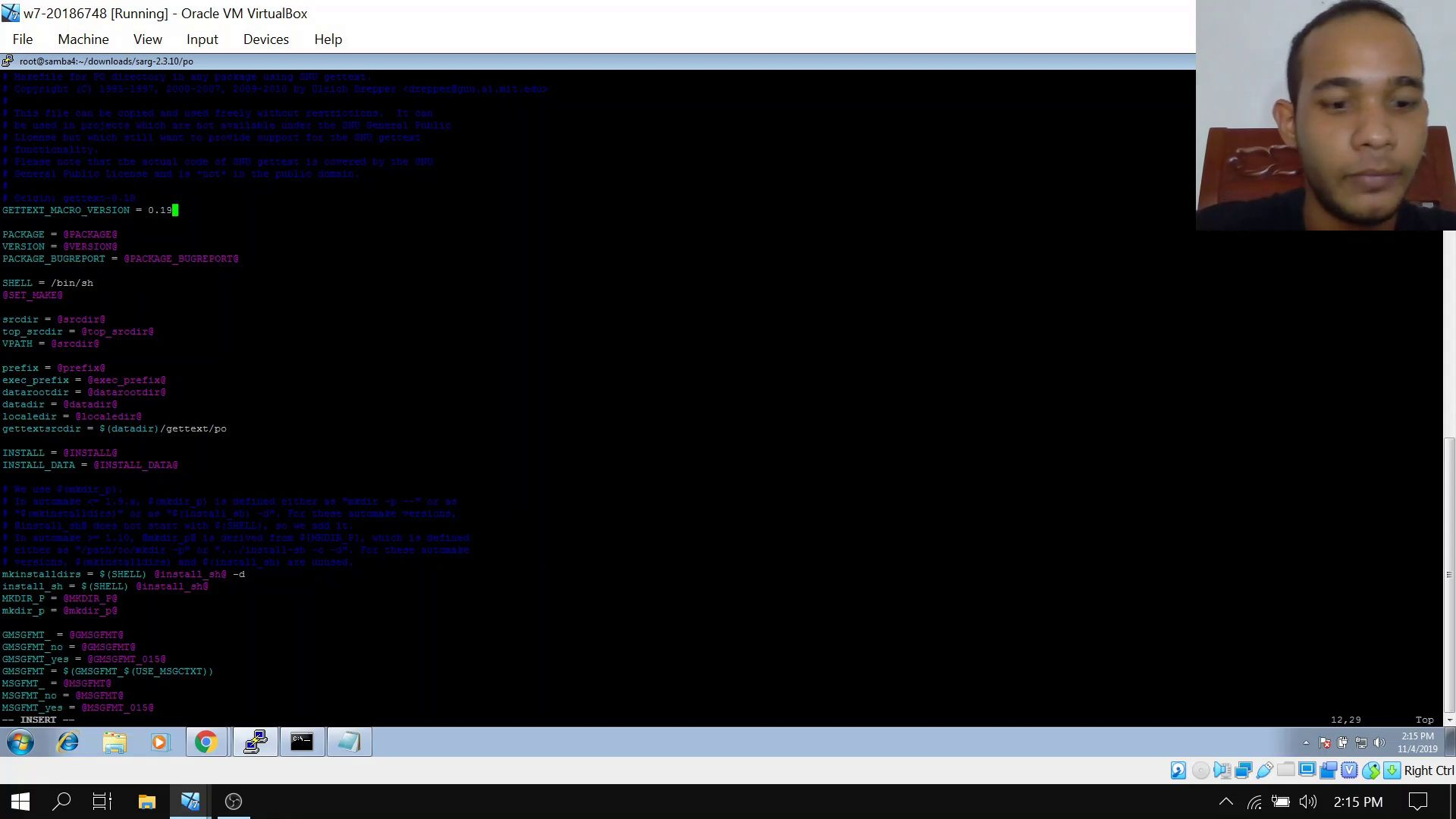
```
[root@samba4 downloads]# wget http://liquidtelecom.dl.sourceforge.net/project/sarg/sarg/sarg-2.3.10/sarg-2.3.10.tar.gz
--2019-11-04 13:13:28--  http://liquidtelecom.dl.sourceforge.net/project/sarg/sarg/sarg-2.3.10/sarg-2.3.10.tar.gz
Resolving liquidtelecom.dl.sourceforge.net (liquidtelecom.dl.sourceforge.net)... 197.155.77.8
Connecting to liquidtelecom.dl.sourceforge.net (liquidtelecom.dl.sourceforge.net)|197.155.77.8|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1270660 (1.2M) [application/x-gzip]
Saving to: 'sarg-2.3.10.tar.gz'

100%[==========================================================================================================================================================================================================>] 1,270,660   19.5KB/s   in 1m 3s

2019-11-04 13:14:34 (19.5 KB/s) - 'sarg-2.3.10.tar.gz' saved [1270660/1270660]

[root@samba4 downloads]# ls
dansguardian-2.12.0.3-1.3.x86_64.rpm  sarg-2.3.10.tar.gz
[root@samba4 downloads]# tart -xvzf sarg-2.3.10.tar.gz
-bash: tart: command not found
[root@samba4 downloads]# tar -xvzf sarg-2.3.10.tar.gz
```

2:15 PM
11/4/2019

Right Ctrl

2:15 PM

Dentro del directorio del archivo vamos al directorio **/po** y en el archivo **MakeFile.in.in** cambiamos la opción **SETTEXT_MACRO_VERSION** a **0.19**


w7-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@samba4:~/downloads/sarg-2.3.10/po
Makefile for PO directory in any package using GNU gettext.
Copyright (C) 1995-1997, 2000-2007, 2009-2010 by Ulrich Drepper <drepper@gnu.ai.mit.edu>
#
This file can be copied and used freely without restrictions. It can
be used in projects which are not available under the GNU General Public
License but which still want to provide support for the GNU gettext
functionality.
Please note that the actual code of GNU gettext is covered by the GNU
General Public License and is *not* in the public domain.
#
# Origin: gettext-0.18
GETTEXT_MACRO_VERSION = 0.19
PACKAGE = @PACKAGE@
VERSION = @VERSION@
PACKAGE_BUGREPORT = @PACKAGE_BUGREPORT@
SHELL = /bin/sh
@SET_MAKE@
srcdir = @srcdir@
top_srcdir = @top_srcdir@
VPATH = @srcdir@
prefix = @prefix@
exec_prefix = @exec_prefix@
datarootdir = @datarootdir@
datadir = @datadir@
localedir = @localedir@
gettextsrcdir = $(datadir)/gettext/po
INSTALL = @INSTALL@
INSTALL_DATA = @INSTALL_DATA@
# We use $(mkdir_p).
# In automake <= 1.9.x, $(mkdir_p) is defined either as "mkdir -p --" or as
# "$(mkinstalldirs)" or as "$(install_sh) -d". For these automake versions,
# $(install_sh) does not start with $(SHELL), so we add it.
# In automake >= 1.10, @mkdir_p@ is derived from ${MKDIR_P}, which is defined
# either as "/path/to/mkdir -p" or ".../install-sh -c -d". For these automake
# versions, $(mkinstalldirs) and $(install_sh) are unused.
mkinstalldirs = $(SHELL) @install_sh@ -d
install_sh = $(SHELL) @install_sh@
MKDIR_P = @MKDIR_P@
mkdir_p = @mkdir_p@
GMSGFMT_ = @GMSGFMT@
GMSGFMT_no = @GMSGFMT@
GMSGFMT_yes = @GMSGFMT_015@
GMSGFMT = $(GMSGFMT_$(USE_MSGCTXT))
MSGFMT_ = @MSGFMT@
MSGFMT_no = @MSGFMT@
MSGFMT_yes = @MSGFMT_015@
-- INSERT --
12,29 Top
2:15 PM
11/4/2019
Right Ctrl
2:15 PM

Comenzamos a compilar el archivo. Para esto primero configuramos el paquete con **./config** dentro del directorio de este, y luego con **make** y **make install** los configuramos e instalamos en nuestro sistema

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~/downloads/sarg-2.3.10

```
[root@samba4 downloads]# ls
dansguardian-2.12.0.3-1.3.x86_64.rpm  sarg-2.3.10  sarg-2.3.10.tar.gz
[root@samba4 downloads]# cd sarg-2.3.10/
[root@samba4 sarg-2.3.10]# ls
ABOUT-NLS     btree_cache.c   config.h      COPYING              datafile.c     DONATIONS   exclude_codes  html.c       ip2name.c       log.c         README        report.c          sarg.php
aclocal.m4    CHANGES         configure     css.c                decomp.c       download.c  fonts          images       ip2name_dns.c   longline.c    README_cmake  sarg.1            siteuser.c
auth.c        ChangeLog       configure.in  css.tpl              denied.c       Doxyfile    getconf.c      include      ip2name_exec.c  Makefile.in   realtime.c    sarg.conf         smartfilter.c
authfail.c    charset.c       CONTRIBUTORS  dansguardian_log.c   dichotomic.c   email.c     grepday.c      index.c      lastlog.c       po            redirector.c  sarg_htaccess     sort.c
BETA-TESTERS  CMakeLists.txt  convlog.c     dansguardian_report.c  documentation  exclude.c   htaccess       indexonly.c  LICENSE         PROGRAMMERS   repday.c      sarg_manpage.xml  sorttable
[root@samba4 sarg-2.3.10]# cd po/
[root@samba4 po]# ls
bg.gmo      ca.po      da.gmo  el.gmo             es.gmo  hu.gmo  insert-header.sin  ja.po     Makefile.in.in  pl.gmo      pt_BR.po  remove-potcdate.sin  Rules-quot  sk.po  tr.po      zh_CN.po
bg.po       ChangeLog  da.po   el.po              es.po   hu.po   it.gmo             LINGUAS   Makevars        pl.po       pt.gmo    ro.gmo               ru.po       sr.gmo  uk.gmo
boldquot.sed  cs.gmo   de.gmo  en@boldquot.header  fr.gmo  id.gmo  it.po              lv.gmo    nl.gmo          POTFILES.in  pt.po     ro.po                sarg.pot    sr.po   uk.po
ca.gmo      cs.po      de.po   en@quot.header      fr.po   id.po   ja.gmo             lv.po     nl.po           pt_BR.gmo   quot.sed  ru.gmo               sk.gmo      tr.gmo  zh_CN.gmo
[root@samba4 po]# vim Makefile.in.in
[root@samba4 po]# cd ..
[root@samba4 sarg-2.3.10]# ./configure
```

2:15 PM
11/4/2019

Right Ctrl

2:15 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@samba4:~/downloads/sarg-2.3.10

```
[root@samba4 sarg-2.3.10]# make && make install
gcc -std=gnu99 -c -I.  -DBINDIR=\"/usr/local/bin\" -DSYSCONFDIR=\"/usr/local/etc\" -DFONTDIR=\"/usr/local/share/sarg/fonts\" -DIMAGEDIR=\"/usr/local/share/sarg/images\" -DSARGPHPDIR=\"/var/www/html
\" -DPACKAGE_NAME=\"sarg\" -DPACKAGE_TARNAME=\"sarg\" -DPACKAGE_VERSION=\"2.3.10\" -DPACKAGE_STRING=\"sarg\ 2.3.10\" -DPACKAGE_BUGREPORT=\"\" -DPACKAGE_URL=\"\" -DHAVE_DIRENT_H=1 -DSTDC_HEADERS=1 -
-DHAVE_STDLIB_H=1 -DHAVE_STRING_H=1 -DHAVE_MEMORY_H=1 -DHAVE_STRINGS_H=1 -DHAVE_INTTYPES_H=1 -DHAVE_STDINT_H=1 -DHAVE_UNISTD_H=1 -DHAVE_STDIO_H=1 -DHAVE_STDLIB_H=1 -DHAVE_STRING_H=1 -DHAVE_STRINGS_
-DHAVE_UNISTD_H=1 -DHAVE_DIRENT_H=1 -DHAVE_SYS_TYPES_H=1 -DHAVE_SYS_SOCKET_H=1 -DHAVE_NETDB_H=1 -DHAVE_ARPA_INET_H=1 -DHAVE_NETINET_IN_H=1 -DHAVE_SYS_STAT_H=1 -DHAVE_CTYPE_H=1 -DHAVE_ERRNO_H=1 -DHA
-DHAVE_STDARG_H=1 -DHAVE_INTTYPES_H=1 -DHAVE_LIMITS_H=1 -DHAVE_LOCALE_H=1 -DHAVE_EXECINFO_H=1 -DHAVE_MATH_H=1 -DHAVE_LIBINTL_H=1 -DHAVE_LIBGEN_H=1 -DHAVE_STDBOOL_H=1 -DHAVE_GETOPT_H=1 -DHAVE_FCNTL_
AVE_GDFONTT_H=1 -DHAVE_GDFONTS_H=1 -DHAVE_GDFONTMB_H=1 -DHAVE_GDFONTG_H=1 -DHAVE_LDAP_H=1 -DHAVE_ICONV=1 -DICONV_CONST= -DHAVE_ICONV_H=1 -DHAVE_PCRE_H=1 -DENABLE_NLS=1 -DHAVE_GETTEXT=1 -DHAVE_DCGET
OURCE=1 -DHAVE_BZERO=1 -DHAVE_BACKTRACE=1 -DHAVE_SYMLINK=1 -DHAVE_LSTAT=1 -DHAVE_GETNAMEINFO=1 -DHAVE_GETADDRINFO=1 -DHAVE_MKSTEMP=1 -DSIZEOF_RLIM_T=8 -DRLIM_STRING=\"%lli\" -DHAVE__USR_SHARE_SGML_
 XSL=1 -DHAVE__USR_SHARE_SGML_DOCBOOK_XSL_STYLESHEETS_HTML_ONECHUNK_XSL=1 -g -O2 -Wall -Wno-sign-compare -Wextra -Wno-unused-parameter -Werror=implicit-function-declaration -Werror=format  util.c
```

2:16 PM
11/4/2019

Right Ctrl

2:16 PM

Una vez iniciamos **sarg** usamos el comando **sarg -x** para generar el reporte. Para acceder a este vamos al navegador y en la dirección que establecimos el el archivo de configuración del servidor web vamos al apartado **/squid-reports**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

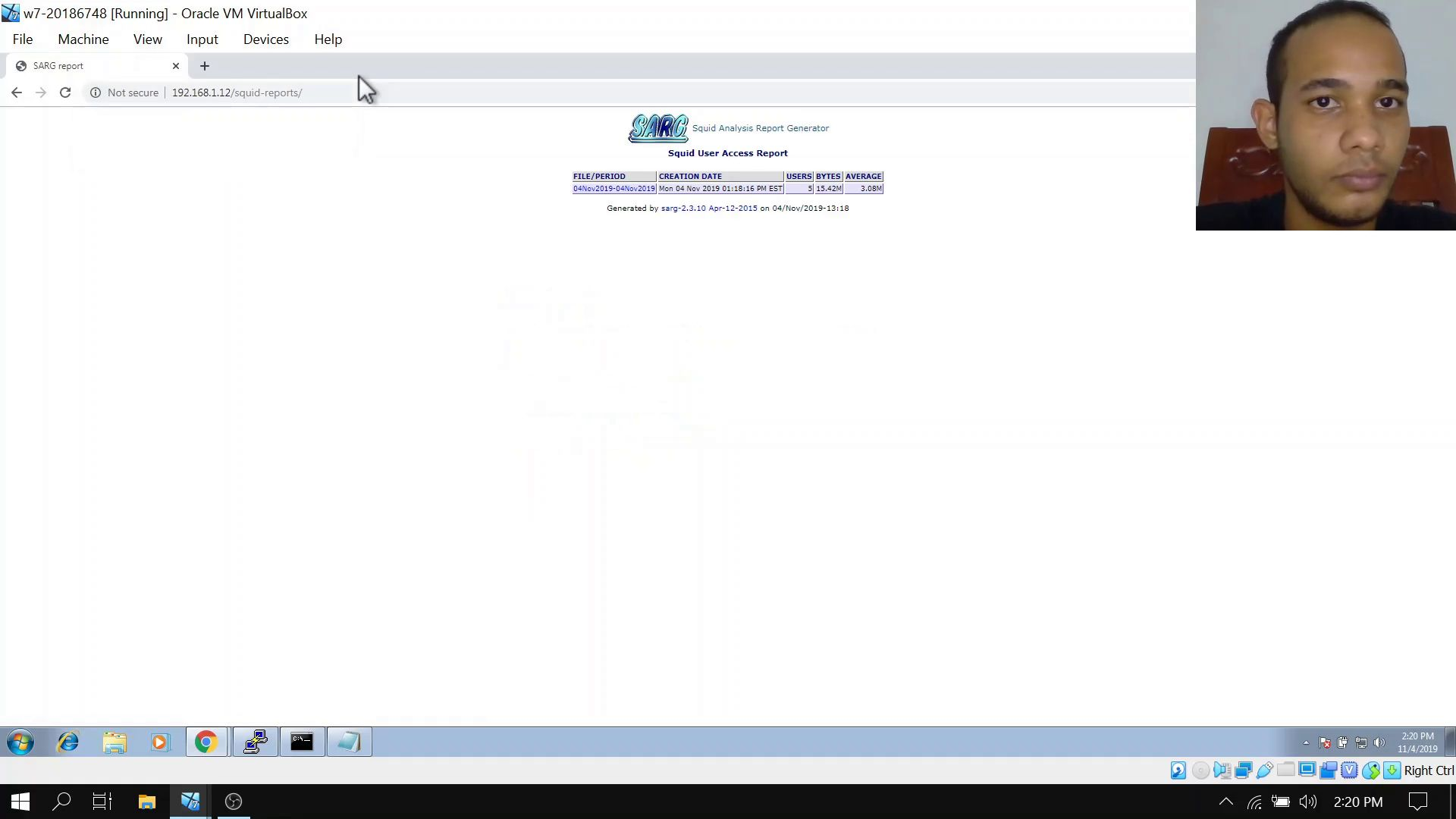
root@samba4:~/downloads/sarg-2.3.10

```
[root@samba4 sarg-2.3.10]# rm -f /usr/local/etc/sarg.conf
[root@samba4 sarg-2.3.10]# vim  /usr/local/etc/sarg.conf
[root@samba4 sarg-2.3.10]#
[root@samba4 sarg-2.3.10]# sarg -x
```

2:18 PM
11/4/2019

Right Ctrl

2:18 PM


w7-20186748 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
SARG report
Not secure
192.168.1.12/squid-reports/
Squid Analysis Report Generator
Squid User Access Report
FILE/PERIOD
CREATION DATE
USERS
BYTES
AVERAGE
04Nov2019-04Nov2019
Mon 04 Nov 2019 01:18:16 PM EST
5
15.42M
3.08M
Generated by sarg-2.3.10 Apr-12-2015 on 04/Nov/2019-13:18
2:20 PM
11/4/2019
Right Ctrl
2:20 PM

Una vez aquí tenemos acceso a todos los eventos del proxy, solo que se ofrecen más organizados y a través de una interfaz grafica

SARG report for 04 Nov 2019

Not secure | 192.168.1.12/squid-reports/04Nov2019-04Nov2019/index.html

Squid Analysis Report Generator

Squid User Access Report

Period: 04 Nov 2019
Sort: bytes, reverse
Top users

Top sites
Sites & Users
Denied accesses
Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		192.168.1.10	855	7.36M	47.76%	69.38%	30.62%	00:52:35	3.155.133	21.63%
2		127.0.0.1	125	4.07M	26.45%	99.99%	0.01%	02:11:53	7.913.533	54.26%
3		test1	26	2.82M	18.34%	100.00%	0.00%	00:53:18	3.198.120	21.93%
4		admin	24	1.07M	6.97%	99.77%	0.23%	00:04:37	277.113	1.90%
5		us	4	73.52K	0.48%	100.00%	0.00%	00:00:40	40.035	0.27%
		TO	**1.03K**	**15.42M**		**85.36%**	**14.64%**	**04:03:03**	**14.583.934**	
		AVERAGE	**206**	**3.08M**				**00:48:36**	**2.916.786**	

Generated by sarg-2.3.10 Apr-12-2015 on 04/Nov/2019-13:18

rpm.pbone.net	6	26.43K	0.36%	100.00%	0.00%	00:00:00	2	0.00%	DENIED
fonts.googleapis.com:443	6	21.90K	0.30%	100.00%	0.00%	00:01:15	75.794	2.40%	
adservice.google.com:443	6	19.27K	0.26%	100.00%	0.00%	00:05:04	304.558	9.65%	
ssl.gstatic.com:443	4	17.22K	0.23%	100.00%	0.00%	00:00:06	6.895	0.22%	
staticxx.facebook.com:443	1	16.65K	0.23%	100.00%	0.00%	00:00:05	5.457	0.17%	
improving.duckduckgo.com:443	4	15.28K	0.21%	100.00%	0.00%	00:00:01	1.177	0.04%	
img-cdn.hipertextual.com:443	1	14.08K	0.19%	100.00%	0.00%	00:00:02	2.390	0.08%	
tc.dataxpand.com:443	1	13.80K	0.19%	100.00%	0.00%	00:00:01	1.864	0.06%	
clientservices.googleapis.com:443	3	12.24K	0.17%	100.00%	0.00%	00:00:00	0	0.00%	DENIED
cdn.syndication.twimg.com:443	1	12.12K	0.16%	100.00%	0.00%	00:00:02	2.006	0.06%	
cdn.sstatic.net:443	4	12.04K	0.16%	100.00%	0.00%	00:00:32	32.865	1.04%	
cm.g.doubleclick.net:443	4	10.72K	0.15%	100.00%	0.00%	00:00:41	41.381	1.31%	
d.agkn.com:443	2	9.70K	0.13%	100.00%	0.00%	00:01:12	72.550	2.30%	
clientservices.googleapis.com	3	9.67K	0.13%	95.40%	4.60%	00:00:00	122	0.00%	DENIED
pixel.mathtag.com:443	1	8.69K	0.12%	100.00%	0.00%	00:00:00	750	0.02%	
googlec.om	2	8.65K	0.12%	0.00%	100.00%	00:00:00	833	0.03%	
facebook.com:443	3	8.41K	0.11%	100.00%	0.00%	00:02:10	130.869	4.15%	
r5---sn-ugpjvh-nq9s.gvt1.com	3	7.93K	0.11%	0.00%	100.00%	00:00:00	121	0.00%	
fbsbx.com:443	1	7.81K	0.11%	100.00%	0.00%	00:01:05	65.232	2.07%	
duckduckgo.com:443	1	7.50K	0.10%	100.00%	0.00%	00:01:40	100.517	3.19%	
ajax.cloudflare.com:443	1	7.42K	0.10%	100.00%	0.00%	00:00:02	2.389	0.08%	
trc.taboola.com:443	1	7.36K	0.10%	100.00%	0.00%	00:00:00	760	0.02%	
ads01.groovinads.com:443	1	6.90K	0.09%	100.00%	0.00%	00:00:00	412	0.01%	
beacon.walmart.com:443	1	6.39K	0.09%	100.00%	0.00%	00:00:35	35.791	1.13%	
static.xx.fbcdn.net:443	1	6.39K	0.09%	100.00%	0.00%	00:01:07	67.712	2.15%	
bcp.crwdcntrl.net:443	1	6.08K	0.08%	100.00%	0.00%	00:00:00	488	0.02%	
www.gravatar.com:443	1	5.74K	0.08%	100.00%	0.00%	00:00:00	154	0.00%	
image6.pubmatic.com:443	1	5.67K	0.08%	100.00%	0.00%	00:00:02	2.850	0.09%	
adservice.google.com.do:443	2	5.47K	0.07%	100.00%	0.00%	00:00:59	59.766	1.89%	
clients1.google.com:443	2	5.26K	0.07%	100.00%	0.00%	00:00:01	1.864	0.06%	
toplist.cz:443	1	5.13K	0.07%	100.00%	0.00%	00:00:09	9.060	0.29%	
id.google.com:443	1	5.04K	0.07%	100.00%	0.00%	00:00:01	1.253	0.04%	
update.googleapis.com	1	4.91K	0.07%	100.00%	0.00%	00:00:00	1	0.00%	DENIED
syndication.twitter.com:443	1	4.86K	0.07%	100.00%	0.00%	00:00:02	2.745	0.09%	
image2.pubmatic.com:443	1	4.69K	0.06%	100.00%	0.00%	00:00:00	635	0.02%	
apps.identrust.com	3	4.69K	0.06%	0.00%	100.00%	00:00:01	1.002	0.03%	
cms.analytics.yahoo.com:443	1	4.67K	0.06%	100.00%	0.00%	00:00:00	765	0.02%	
rtb.openx.net:443	2	4.58K	0.06%	100.00%	0.00%	00:00:03	3.187	0.10%	
toplist.sk:443	1	4.57K	0.06%	100.00%	0.00%	00:00:21	21.861	0.69%	
pixel.tapad.com:443	1	4.47K	0.06%	100.00%	0.00%	00:00:00	771	0.02%	
toplist.eu:443	1	4.35K	0.06%	100.00%	0.00%	00:00:44	44.558	1.41%	
chrome.google.com:443	1	4.34K	0.06%	100.00%	0.00%	00:00:12	12.372	0.39%	
stats.g.doubleclick.net:443	1	4.34K	0.06%	100.00%	0.00%	00:00:01	1.366	0.04%	

Proxy transparente

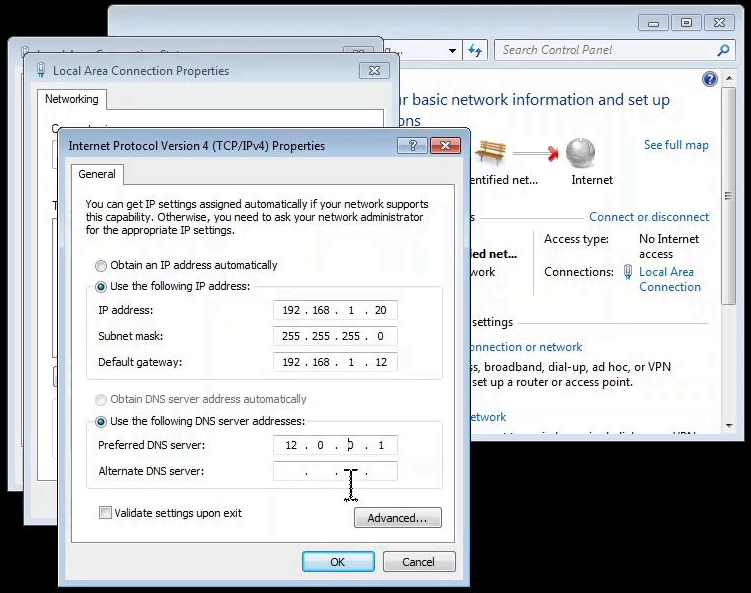
En el cliente colocamos como gateway la dirección de la interfaz de servidor conectada al la red local, y como dns el mismo de la interfaz wan del servidor

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
[root@localhost ~]#
```



8:42 PM
11/6/2019

Right Ctrl

8:42 PM

Para el proxy transparente enrutamos el tráfico de la interfaz de los clientes a la interfaz del servidor con el servidor proxy. Antes de enrutar debemos realizar ciertas verificaciones de configuración para que nuestros clientes aún cuenten con acceso a internet. primero en el archivo **/etc/sysconfig/network** nos aseguramos de que el **GATEWAY** sea el mismo que el de la interfaz que conectamos a internet

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
[root@localhost ~]# vim /etc/sysconfig/network
```

8:43 PM
11/6/2019

Right Ctrl

8:43 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
# Created by anaconda
NETWORKING=yes
HOSTNAME=nat
GATEWAY=12.0.0.1
~
~
~

"/etc/sysconfig/network" 4L, 67C                                    4,16          All
```

8:43 PM
11/6/2019

Right Ctrl

8:43 PM

Luego en el archivo **/etc/resolv.conf** nos nos aseguramos de que el **nameserver** sea el mismo que el de la interfaz que conectamos a internet

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
[root@localhost ~]# vim /etc/sysconfig/network
[root@localhost ~]# vim /etc/resolv.conf
```

8:43 PM
11/6/2019

Right Ctrl

8:43 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
# Generated by NetworkManager
nameserver 12.0.0.1
~
"/etc/resolv.conf" 2L, 50C                                        2,7          All
```

8:43 PM 11/6/2019

Right Ctrl

8:43 PM

Luego aplicamos las reglas de enrutamiento con las iptables, estas son:

iptables --table nat --append POSTROUTING --out-interface [interfaz wan] -j MASQUERADE

iptables --append FORWARD --in-interface [interfaz lan] -j ACCEPT

y activamos el routing con:

echo 1 > /proc/sys/net/ipv4/ip_forward

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
[root@localhost ~]# iptable --table nat --append POSTROUTING --out-interface enp0s3 -j MASQUERADE
-bash: iptable: command not found
[root@localhost ~]# iptables --table nat --append POSTROUTING --out-interface enp0s3 -j MASQUERADE
[root@localhost ~]# iptables --append FORWARD --in-interface enp0s10 -j ACCEPT
[root@localhost ~]#
```

8:45 PM
11/6/2019

Right Ctrl

8:45 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
[root@localhost ~]# iptable --table nat --append POSTROUTING --out-interface enp0s3 -j MASQUERADE
-bash: iptable: command not found
[root@localhost ~]# iptables --table nat --append POSTROUTING --out-interface enp0s3 -j MASQUERADE
[root@localhost ~]# iptables --append FORWARD --in-interface enp0s10 -j ACCEPT
[root@localhost ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
```

8:46 PM
11/6/2019

Right Ctrl

8:46 PM

En el archivo **/etc/squid/squid.conf** le colocamos la opción **transparent** al **http_port**, y reiniciamos el servicio **squid**

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
http_access allow all
http_port 3128 transparent
~
~
~

-- INSERT --                                                    2,27          All
```

8:47 PM
11/6/2019

Right Ctrl

8:47 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
[root@localhost ~]# vim /etc/squid/squid.conf
[root@localhost ~]# systemctl restart squid
[root@localhost ~]# systemctl status squid
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-11-06 19:47:47 EST; 7s ago
  Process: 2393 ExecStop=/usr/sbin/squid -k shutdown -f $SQUID_CONF (code=exited, status=0/SUCCESS)
  Process: 2400 ExecStart=/usr/sbin/squid $SQUID_OPTS -f $SQUID_CONF (code=exited, status=0/SUCCESS)
  Process: 2395 ExecStartPre=/usr/libexec/squid/cache_swap.sh (code=exited, status=0/SUCCESS)
 Main PID: 2402 (squid)
   CGroup: /system.slice/squid.service
           ├─2402 /usr/sbin/squid -f /etc/squid/squid.conf
           ├─2404 (squid-1) -f /etc/squid/squid.conf
           └─2405 (logfile-daemon) /var/log/squid/access.log

Nov 06 19:47:47 localhost.localdomain systemd[1]: Stopped Squid caching proxy.
Nov 06 19:47:47 localhost.localdomain systemd[1]: Starting Squid caching proxy...
Nov 06 19:47:47 localhost.localdomain systemd[1]: Started Squid caching proxy.
Nov 06 19:47:47 localhost.localdomain squid[2402]: Squid Parent: will start 1 kids
Nov 06 19:47:47 localhost.localdomain squid[2402]: Squid Parent: (squid-1) process 2404 started
[root@localhost ~]#
```

8:47 PM
11/6/2019

Right Ctrl

8:47 PM

Luego redireccionamos todo el tráfico web de ambas interfaces al puerto del proxy squid con:

**iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 **

-j REDIRECT --to-port 3128

**iptables -t nat -A PREROUTING -i enp0s10 -p tcp --dport 80 **

-j REDIRECT --to-port 3128

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
[root@localhost ~]#
[root@localhost ~]# iptables -t nat --append PREROUTING -i enp0s3 -p tcp --dport 80 \
>         -j REDIRECT --to-port 3128
[root@localhost ~]# iptables -t nat --append PREROUTING -i enp0s3 -p tcp --dport 80         -j REDIRECT --to-port 3128
```

8:48 PM
11/6/2019

Right Ctrl

8:48 PM

Podemos comprobar de que los clientes tienen acceso a internet accediendo a una página web

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Sites list | Scratchpads

Not secure | scratchpads.eu/explore/sites-list

Scratchpads
biodiversity online

contact us

Search this site Search across Scratchpads

Home Explore Support Develop About us

- Summary Statistics
- Scratchpads 2 statistics
- Sites list

Sites list

Website	Views	Pages	Users	Recent logins	Last change	DwCA
http://iczn.org	786 720	6 973	637	0	30.04.2019	No
http://wallacefund.info	539 818	538	4	0	01.09.2019	No
http://checklist.onlineflora.cn	335 713	44 953	2	0	01.12.2016	No
http://mosquito-taxonomic-inventory.info	195 271	5 081	1	0	03.09.2019	No
http://phthiraptera.info	147 729	43 074	30	2	17.10.2019	No
http://pistiaistyoryhma.myspecies.info	78 021	2 600	17	2	02.07.2019	No
http://eunops.org	76 135	990	102	0	27.10.2017	No
http://solanaceaesource.org	72 599	143 168	5	1	15.10.2019	Yes
http://seargentina.myspecies.info	57 105	26	1	0	10.09.2017	No
http://wallaceletters.info	55 369	168	37	0	02.08.2019	No
http://rbzs.myspecies.info	55 329	22	2	1	03.10.2018	No
http://sciaroidea.info	52 488	18 185	130	10	13.10.2019	Yes
http://fossilinsects.net	52 149	51 637	56	3	17.06.2019	No
http://avis.webapp.local	27 813	57 786	7	0	20.06.2015	No
http://weevil.myspecies.info	23 416	8 517	148	0	01.04.2015	No
http://milichiidae.info	17 099	10 500	26	1	21.07.2019	No
http://lonchaeidae.myspecies.info	15 869	543	30	1	06.10.2019	No
http://olivirv.myspecies.info	15 478	9 027	29	1	13.09.2019	No
http://westpalbees.myspecies.info	13 773	3 437	1	0	28.08.2015	No
http://araceae.e-monocot.org	13 005	3 763	31	0	05.05.2019	Yes
http://cyperaceae.e-monocot.org	12 033	3 871	61	0	12.09.2016	Yes
http://families.e-monocot.org	11 928	2 306	17	0	11.08.2014	Yes

8:49 PM 11/6/2019

Right Ctrl

8:49 PM

Para probar el proxy transparente aplicamos una regla negando todo el tráfico web.

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@localhost:~

```
http_access deny all
http_port 3128 transparent
~
-- INSERT --                                                    1,18          All
```

8:49 PM
11/6/2019

Right Ctrl

8:49 PM

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ERROR: The requested URL could

Not secure | scratchpads.eu/explore/sites-list

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://scratchpads.eu/explore/sites-list

Access Denied.

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

Your cache administrator is root.

Generated Thu, 07 Nov 2019 00:51:21 GMT by localhost.localdomain (squid/3.5.20)

8:51 PM
11/6/2019

Right Ctrl

8:51 PM

Como vemos el tráfico se ha bloqueado sin la necesidad de colocar el servidor proxy en las configuraciones de área local

w7-20186748 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ERROR: The requested URL could

Not secure | scratchpads.eu/explore/sites-list

ERROR

The requested URL could not be retrieved

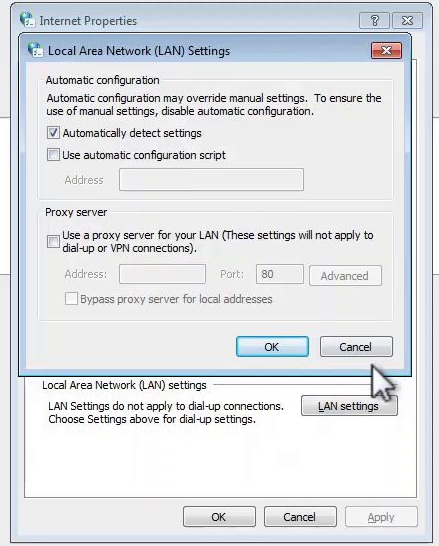
The following error was encountered while trying to retrieve the URL: http://scratchpads.eu/explore/sites-list

Access Denied.

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

Your cache administrator is root.

Generated Thu, 07 Nov 2019 00:52:43 GMT by localhost.localdomain (squid/3.5.20)



8:52 PM
11/6/2019

Right Ctrl

8:52 PM