

Resumen

Instalación y
Configuración PROXY

Práctica 6

Alumno: León Gaspar, Juan Miguel

Clase: SMRD_B

Asignatura: Seguridad Informática

ÍNDICE

Resumen Instalación y Configuración Proxy

1-º PREGUNTA O PETICIÓN EN CLASE (BORRAR LO QUE NO VALGA)

Realizar la práctica en una red puntúa extra

Añadimos a los equipos a una misma red, con IP dentro del rango y a la máquina que tendrá el Proxy le damos una interfaz NAT.

Añadir un DNS a la máquina servidor, utilizando **sudo nano /etc/resolv.conf**

Creamos un script que permita a la máquina Linux, la que tiene la tarjeta NAT, enrutar los paquetes a Internet para el resto de equipos.

```
administrador@ubuntu1:~$ cat enrutar.sh
iptables -F
iptables -t nat -F

iptables -t nat -A POSTROUTING -j MASQUERADE

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

iptables-save
```

Le damos permisos.

```
miguelsor@miguelsor-VirtualBox:~$ sudo chmod 775 enrutar.sh
```

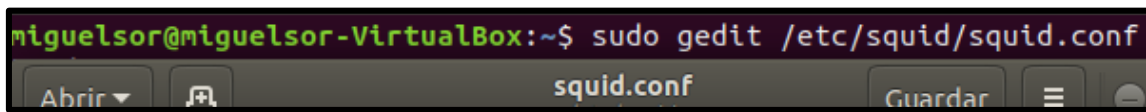
Ejecutamos el script.

```
miguelsor@miguelsor-VirtualBox:~$ sudo ./enrutar.sh
# Generated by iptables-save v1.6.1 on Tue Mar  2 01:52:23 2021
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
```

Instalamos squid3 para poder realizar la práctica Proxy

```
miguelsor@miguelsor-VirtualBox:~$ sudo apt-get install squid3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

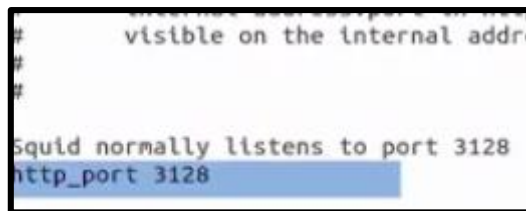
Utilizamos un comando o programa de edición, en este caso *nano*, al archivo localizado en la ruta `/etc/squid3/squid.conf`



ctrl+f para buscar entre todas las líneas.



Descomentamos una línea concreta, **# http_port 3128**, para comprobar que el puerto está a la escucha.



Podemos comprobar que el puerto está a la escucha desde otra máquina, utilizando el comando: **nmap IP_Máquina_Puerto_abierto**

Ejemplo → **nmap 192.168.1.1**

Descomentamos otra línea concreta, **# cache_mem 256 MB**

Buscamos otra línea para descomentar, **# cache_dir ufs /var/spool/squid3 100 16 256**

Modificamos el valor 100 por 300

Buscamos otra línea para descomentar, **# acl CONNECT method CONNECT**

Debajo de esta línea, escribimos la lista de control de acceso

→ **acl RED src 192.168.1.1/24**

y el archivo de denegación

→ **acl noway url_regex "/etc/squid3/noperm.txt"**



Una vez hecho lo anterior buscamos: **"#only-allow-chaemgr-Access-from-localhost"**

Añadimos las siguientes líneas:

- → **http_access deny noway => deniega todo lo que tenemos en noway**
- → **http_access allow Red =>**

ctrl+f para buscar la línea que comienza con *insert* y utilizar esas líneas en adelante para introducir nuestras reglas.

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# Example rule allowing access from your local networks
```

```
#
acl windows1 src 10.33.1.2/24
http_access deny windows1
```

Para declarar las diversas reglas con src se sigue una sintaxis concreta:

acl Nombre_único_ACL **src** IP_Concreta/Mascara_Red

Ejemplo→acl TODOS src 192.168.1.1/24

Para declarar una regla con src para un único equipo es:

acl Nombre_único_ACL **src** IP_del_Equipo

Ejemplo→acl PC1 src 192.168.1.100

Para declarar una regla con src para varios equipos es

acl Nombre_único_ACL **src** "etc/squid3/Nombre_archivo.txt"

Ejemplo→acl EQUIPOS src "etc/squid3/lista_de_ips.txt"

Para declarar una regla con http_acces se sigue una sintaxis concreta:

http_access **allow** Nombre_único_ACL

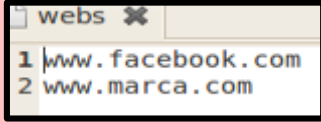
Ejemplo→http_access allow TODOS

Opciones → **allow** (permitir) **deny** (denegar)

Esto es muy importante, el permitir a toda la red el acceso siempre será nuestra última línea de configuración para evitar problemas.

Para validad y comprobar que el archivo de configuración es correcto usaremos el siguiente comando:

sudo squid3 -k reconfigure

Para configurar el control de acceso a páginas web, crearemos un archivo en la ruta /etc/squid3/
Ejemplo→ /etc/squid3/paginas.txt
En este archivo introduciremos las direcciones de las páginas web que queremos bloquear.

Creamos la declaración para identificarla y aplicarla, diferenciándola del resto.
Ejemplo→ acl WEBS url_regex "/etc/squid3/paginas.txt
Creamos la regla para la declaración anterior.
Ejemplo→ http_access deny WEBS PC1