Sistemas operativos de redes

Cátedra: Sistemas Operativos de Redes.
Docente: Ing. Manuel de Jesús Flores.
Tema: Firewall de Red

Benitez Argueta jose Dimas ba02110776
Flores Martinez Jose Manue FM02110857
Garcia Pineda Osiris Stephani GP0211020

Que es ipetables. **Iptables** es un poderoso firewall integrado en el kernel de Linux y que forma parte del proyecto netfilter. **Iptables** puede ser configurado directamente, como también por medio de un frontend o una GUI. **iptables** es usado por IPv4, en tanto que ip6tables es usado para IPv6

Para que sirve la ipetables

iptables permite crear reglas que analizarán los paquetes de datos que entran, salen o pasan por nuestra máquina, y en función de las condiciones que establezcamos, tomaremos una decisión que normalmente será permitir o denegar que dicho paquete siga su curso

Squid es un servidor proxy para web con caché. Es una de las aplicaciones más populares y de referencia para esta función, software libre publicado bajo licencia GPL.

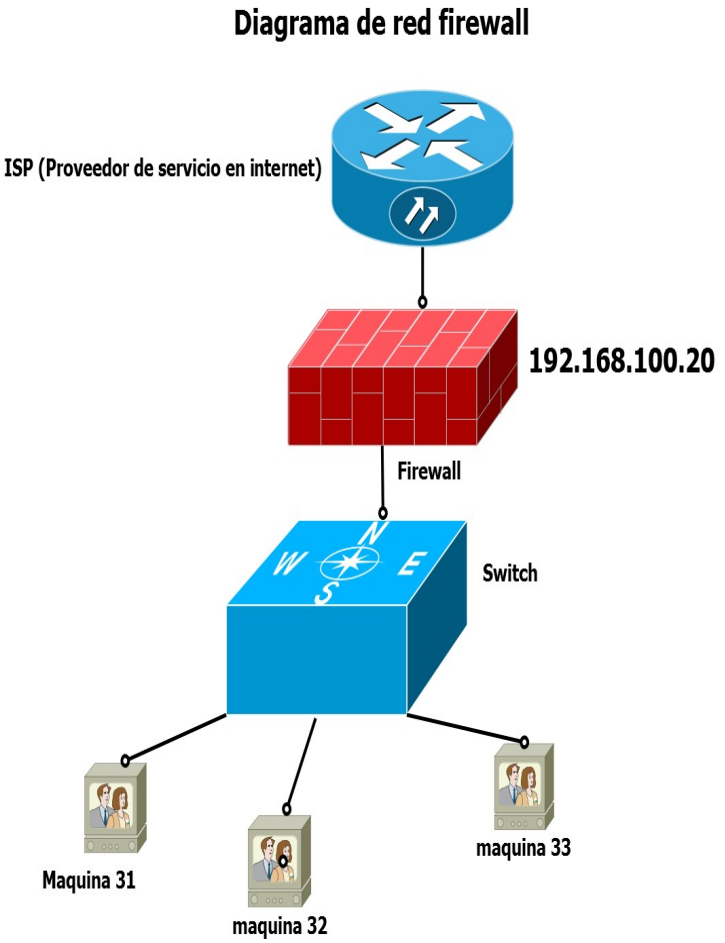
Para que sirve Squid es un servidor proxy para web con cache. Es una de las aplicaciones más populares y de referencia para esta función, software libre publicado bajo licencia gpl . Entre sus utilidades está la de mejorar el rendimiento de las conexiones de empresas y particulares a guardando en cache peticiones recurrentes a SERVIDORES WEB y DNS, acelerar el acceso a un servidor web determinado o añadir seguridad realizando filtrados de tráfico

Un **ACL** es una lista que especifica los permisos de los usuarios sobre un archivo, carpeta u otro objeto. Un **ACL** define cuales usuarios y cuales grupos pueden accesar y que tipo de operaciones pueden realizar una vez dentro.

Paea que sirve ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.

Imagen del firewall

Diagrama de red d



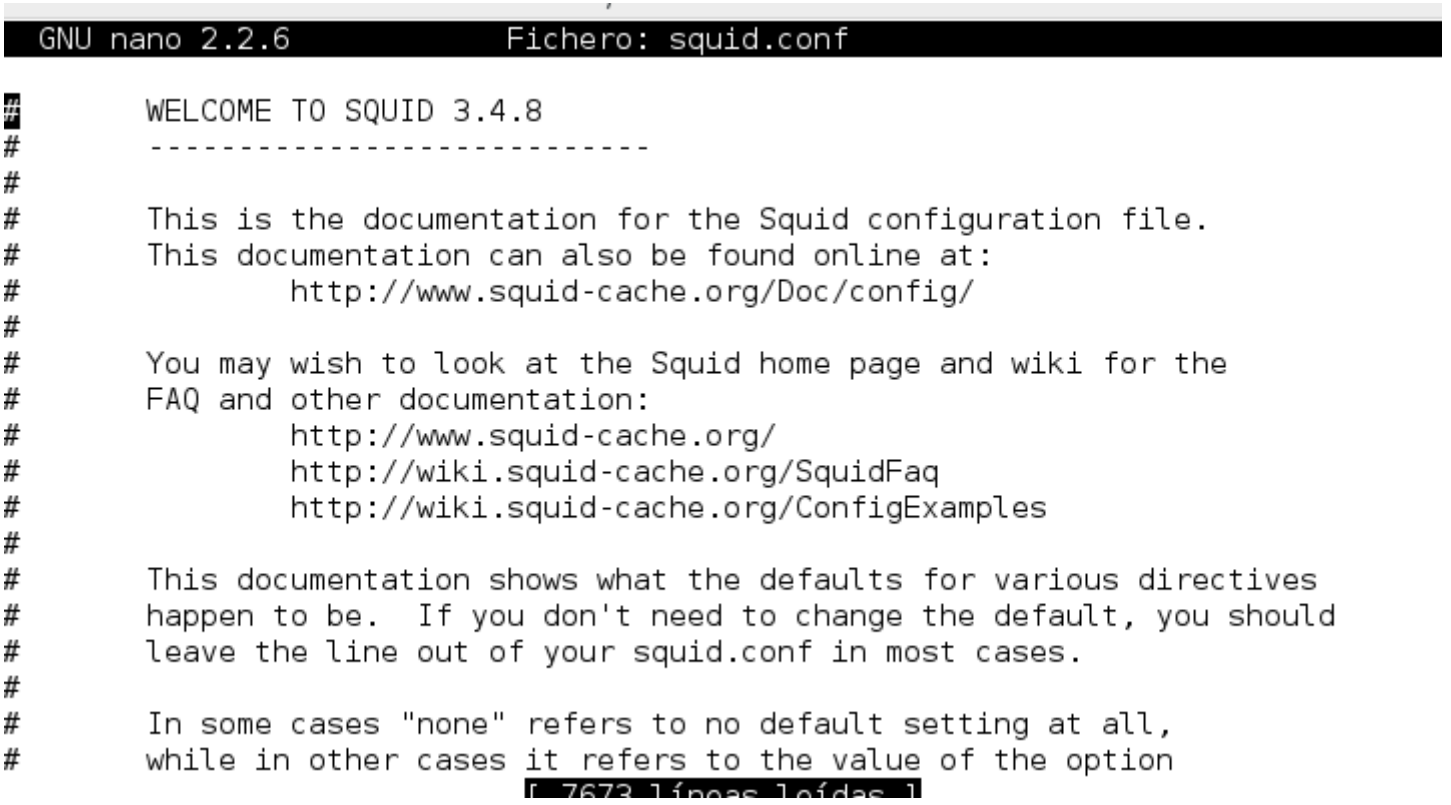
Accediendo a squis3

```
root@debian:/etc# cd squid3
root@debian:/etc/squid3# ls
errorpage.css  listas  msntauth.conf  squid.conf  squid.conf.copy  usuarios
root@debian:/etc/squid3#
```

Accediendo a listas

```
root@debian:/etc/squid3# cd listas
root@debian:/etc/squid3/listas# ls
dominios-denegados  expreg-denegadas  ip-denegadas
root@debian:/etc/squid3/listas#
```

Archivo de squids

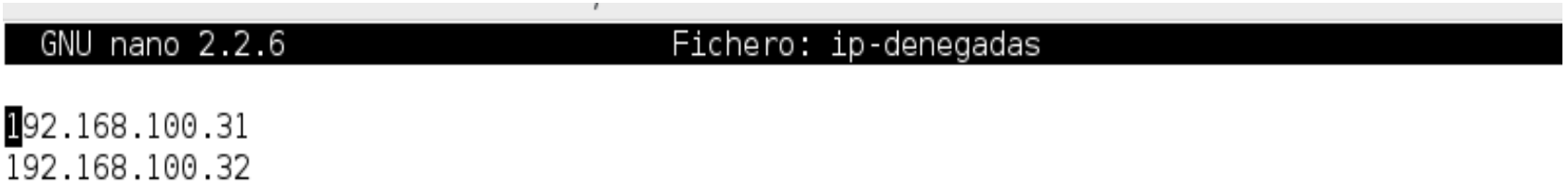


Configuracion de acl

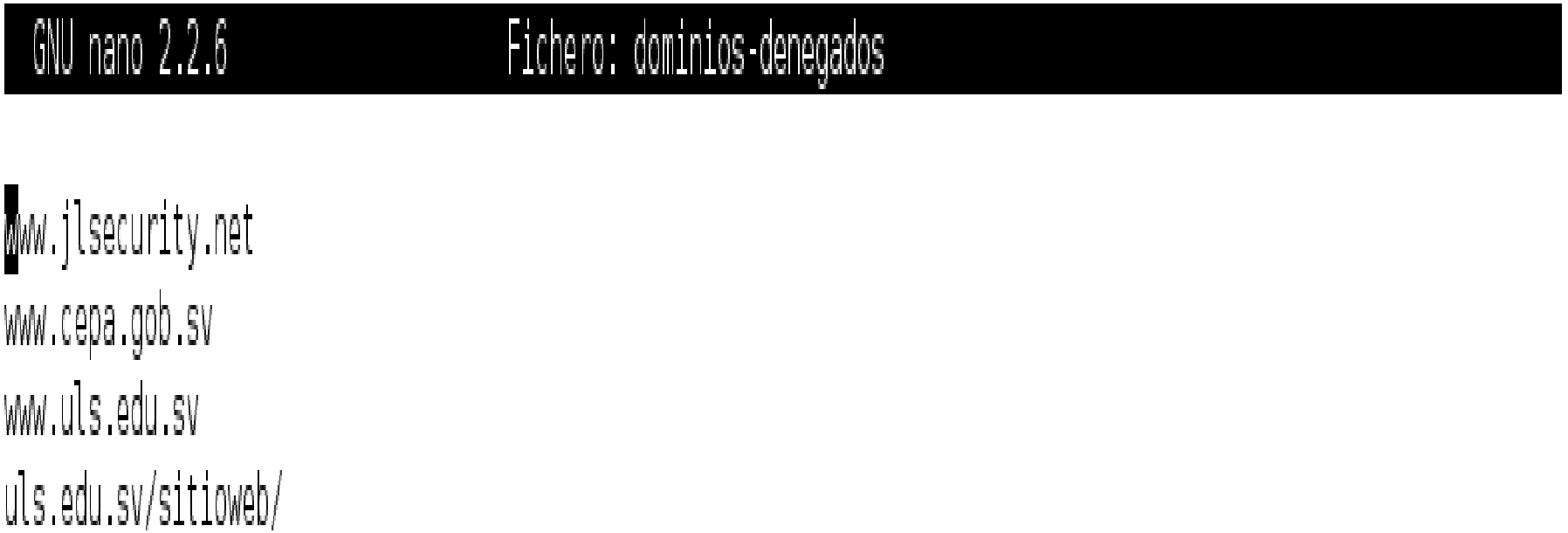
```
# By Manuel
http_port 3128
cache_mem 500 MB
cache_dir ufs /var/spool/squid 150 16 256
#Policy 1
acl red_local src 192.168.100.0/24
acl localhost src 127.0.0.1/32
#Policy 2
acl dominios-denegados dstdomain "/etc/squid3/listas/dominios-denegados"

#acl all src all
#http_access allow localhost
#http_access allow red_local !dominios-denegados
#Policy 3
acl expreg-denegadas url_regex "/etc/squid3/listas/expreg-denegadas"
#policy 4
acl sininternet src "/etc/squid3/listas/ip-denegadas"
http_access allow red_local !sininternet !expreg-denegadas !dominios-denegados
```

Bloqeo de ip


GNU nano 2.2.6
Fichero: ip-denegadas
192.168.100.31
192.168.100.32

Bloqueo de dominios



Bloqueo de contenido

Monitoreo de un cliente

```
root@debian:/etc/squid3/listas# tail -f /var/log/squid3/access.log
1447966167.528  24887 192.168.100.30 TCP_MISS/200 6831 CONNECT pges.solution.weborama.fr:443 - HIER_DIRECT/195.5
4.48.228 -
1447966167.532  34262 192.168.100.30 TCP_MISS/200 367 CONNECT r1---sn-upbvn8-n5al.googlevideo.com:443 - HIER_DIR
ECT/190.150.50.76 -
1447966170.183      0 192.168.100.30 TCP_MISS/503 0 CONNECT csc.beap.bc.yahoo.com:443 - HIER_NONE/- -
1447966170.629      0 192.168.100.30 TCP_MISS/503 0 CONNECT sb.scorecardresearch.com:443 - HIER_NONE/- -
1447966172.008    117 192.168.100.30 TCP_MISS/503 0 CONNECT y.analytics.yahoo.com:443 - HIER_NONE/- -
1447966172.462    283 192.168.100.30 TCP_MISS/503 0 CONNECT geo.query.yahoo.com:443 - HIER_NONE/- -
1447966173.126      0 192.168.100.30 TCP_MISS/503 0 CONNECT geo.query.yahoo.com:443 - HIER_NONE/- -
1447966173.585      0 192.168.100.30 TCP_MISS/503 0 CONNECT geo.query.yahoo.com:443 - HIER_NONE/- -
1447966173.638    364 192.168.100.30 TCP_MISS/503 0 CONNECT ads.yahoo.com:443 - HIER_NONE/- -
1447966177.137      0 192.168.100.30 TCP_MISS/503 0 CONNECT geo.query.yahoo.com:443 - HIER_NONE/- -
1447966183.204      0 192.168.100.30 TCP_MISS/503 0 CONNECT geo.query.yahoo.com:443 - HIER_NONE/- -
1447966187.283      0 192.168.100.30 TCP_MISS/503 0 CONNECT geo.query.yahoo.com:443 - HIER_NONE/- -
1447966206.229  73042 192.168.100.30 TCP_MISS/200 2278123 CONNECT r1---sn-upbvn8-n5al.googlevideo.com:443 - HIER
 DIRECT/190.150.50.76 -
```

Información de los bloqueos

```
manuel@debian:~$ su
Contraseña:
root@debian:/home/manuel# cd /etec/
bash: cd: /etec/: No existe el fichero o el directorio
root@debian:/home/manuel# cd /etc/
root@debian:/etc# cd squid3
root@debian:/etc/squid3# cd listas
root@debian:/etc/squid3/listas# ls
dominios-denegados  expreg-denegadas  ip-denegadas
root@debian:/etc/squid3/listas# nano ip-denegadas
root@debian:/etc/squid3/listas# nano dominios-denegados
root@debian:/etc/squid3/listas# nano expreg-denegadas
root@debian:/etc/squid3/listas#
root@debian:/etc/squid3/listas#
```

conclucion

- Como grupo de trabajo de sistema operativo de redes concluimos que el Firewall es necesario porque proporciona su seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa

•

Gracias por su atención