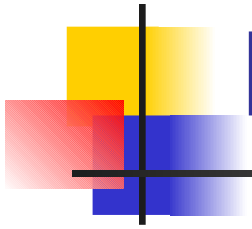
# SQUID

Prueba hecha en Ubuntu Feisty 7,04

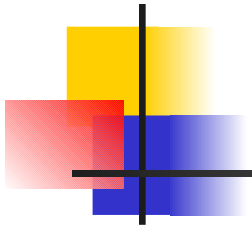
# Utilidades

- Controlar el acceso mediante IP
- Controlar el acceso mediante MAC
- Controlar el acceso en el horario permitido
- Controlar el acceso a paginas permitidas
- Asi como permito acceso puedo denegar acceso
- Autentificar a usuarios el acceso

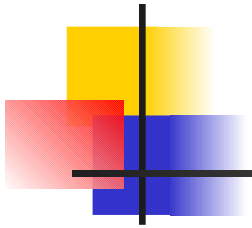
# Editando el archivo



- El archivo a editar es el “/etc/squid/squid.conf”
- http_port 3128 *seleccionamos el puerto*
- hierarchy_stoplist cgi-bin ? *(por defecto)*
- acl QUERY urlpath_regex cgi-bin \? *(por defecto)*



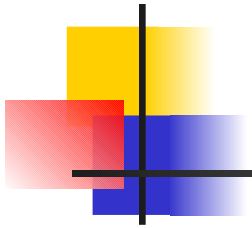
- cache deny QUERY *(por defecto)*
- acl apache rep_header Server ^Apache *(por defecto)*
- broken_vary_encoding allow apache *(por defecto)*



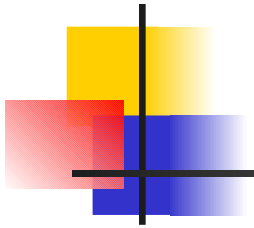
- cache_mem 128 MB *capacidad de RAM que usaremos para la cache*
- cache_dir ufs /var/spool/squid 200 16 256
- access_log /var/log/squid/access.log
- cache_log /var/log/squid/cache.log
- cache_store_log /var/log/squid/store.log
- hosts_file /etc/hosts

*Parametros para la autentificacion con NCSA*

- auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves
- auth_param basic children 5
- auth_param basic realm Squid proxy-caching web server
- auth_param basic credentialsttl 1 hours
- auth_param basic casesensitive on



- authenticate_cache_garbage_interval 1 hour
- authenticate_ttl 1 hour
- authenticate_ip_ttl 60 minutes *( indica el tiempo que un usuario se queda registrado en una ip.)*

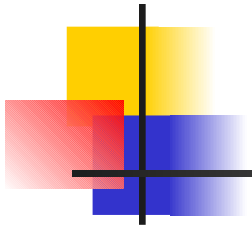


- refresh_pattern ^ftp:  1440 20% 10080
- refresh_pattern ^gopher: 1440  0%  1440
- refresh_pattern .  0 20%  4320

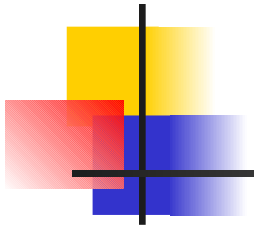
*(defecto)*

- acl all src 0.0.0.0/0.0.0.0
- acl manager proto cache_object
- acl localhost src 127.0.0.1/255.255.255.255
- acl to_localhost dst 127.0.0.0/8
- acl SSL_ports port 443 # https
- acl SSL_ports port 563 # snews
- acl SSL_ports port 873 # rsync
- acl Safe_ports port 80 # http
- acl Safe_ports port 21 # ftp

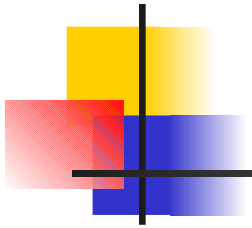
- acl Safe_ports port 443 # https
- acl Safe_ports port 70 # gopher
- acl Safe_ports port 210 # wais
- acl Safe_ports port 1025-65535 # unregistered ports
- acl Safe_ports port 280 # http-mgmt
- acl Safe_ports port 488 # gss-http
- acl Safe_ports port 591 # filemaker
- acl Safe_ports port 777 # multiling http
- acl Safe_ports port 631 # cups
- acl Safe_ports port 873 # rsync
- acl Safe_ports port 901 # SWAT
- acl purge method PURGE
- acl CONNECT method CONNECT



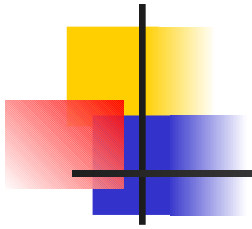
- http_access allow manager localhost
- http_access deny manager
- http_access allow purge localhost
- http_access deny purge
- http_access deny !Safe_ports
- http_access deny CONNECT !SSL_ports



- http_access allow localhost *permitir acceso al localhost*
- http_access allow password mired ! listanegra tiempop !nopag !extnegadas
  *permite loguearse con el NCSA a toda mired, menos los ip que esten en listanegra, en un tiempo dentro del rango de tiempop, menos a paginas url que esten en nopag, no podras bajar archivos con extensiones que esten dentro de extnegadas*
- http_access deny all *buena politica de seguridad al final negar todo*



- http_reply_access allow all
- icp_access allow all
- cache_mgr a20030520@pucp.edu.pe
- cachemgr_passwd 123 all
- coredump_dir /var/spool/squid



# Activamos el Firewall (Proxy Transparente)

```
# iptables –t nat –A PREROUTING –i eth0 –
  p tcp –dport 80 –j REDIRECT  --to-port
  3128
```

# Visualizar estadisticas

- Activar el APACHE: #service httpd start
- Copiar: /usr/share/doc/squid/cachemgr.cgi
  a
  /var/www/cgi-bin *(directorio root apache)*
- En los clientes:
  http://<ip_servidor>/cgi-bin/cachemgr.cgi

# Autentificacion de usuarios

- Para crear las claves usamos:

  #htpasswd –c /etc/squid/claves <login>

  *Con esto creamos automaticamente las claves encriptadas dentro del archvo claves*

# Contenido de arch claves

- cooljsh:IwoZm8kw93O.c
- yoni:mM6O5.NLcYYVg

*El formato es <user>:<psswd> en donde el password se encuentra encriptado*

# Contenido de arch extensiones

- \.iso$
- \.exe$

*Tipo de archivos que seran negados*

# Contenido de arch listanegra

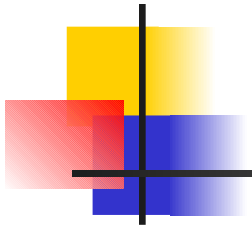
- 10.0.0.135
- 10.0.0.130

*En cada linea irá el IP el cual sera restringido o permitido para acceder a la web*

# Contenido de arch nopag

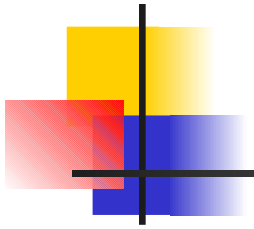
- ^http://www.peru.com
- ^http://www.yahoo.com

*Lista de url que seran bloqueados*



# CALAMARIS

visualizador de los .log



- cat access.log | calamaris -a -F html -> /var/www/calamaris/reporte.html

*-a todo el log*

*-F html la salida en formato html*

*la salida se guardara en el archivo reporte.html*

# Proxy Report

**Report period:** **13.Aug 07 10:34:39 - 13.Aug 07 16:35:37**

**Generated at:** 13.Aug 07 16:40:04

---

| Table of Content / Overview | | | |
|---|---|---|---|
| Summary | - | - | - |
| Incoming requests by method | most requested method | GET | 770 Requests |
| Incoming UDP-requests by status | - | - | no requests found |
| Incoming TCP-requests by status | most incoming request by status to | MISS | 661 Requests |
| Outgoing requests by status | most outgoing request to | DIRECT Fetch from Source | 671 Requests |
| Outgoing requests by destination | most requested destination | DIRECT | 671 Requests |
| Request-destinations by 2nd-level-domain | most requested 2nd-level-domain | *.pucp.edu.pe | 378 Requests |
| Request-destinations by toplevel-domain | most requested toplevel-domain | *.pe | 400 Requests |
| TCP-Request-protocol | most requested protocol | http: | 682 Requests |
| Requested content-type | most requested content-type | text/html | 273 Requests |
| Requested extensions | most requested extension | <dynamic> | 315 Requests |
| Incoming UDP-requests by host | - | - | no requests found |
| Incoming TCP-requests by host | most active host | 10.0.0.137 | 789 Requests |
| Size Distribution Diagram | most requested object_size | 100-999 | 479 Requests |
| Performance in 1 hour steps | most active day | 13.Aug 07 13:00 | 353 Requests |
| UDP-Request duration distribution in msec | - | - | no requests found |

# BlackList

- http://urlblacklist.com/cgi-bin/commercialdownload.pl?type=download&file=bigblacklist