
Unidad 9-b: Servicio Proxy en Linux

Curso de Introducción a la administración de
servidores GNU/Linux

Centro de Formación Permanente
Universidad de Sevilla

Contenidos

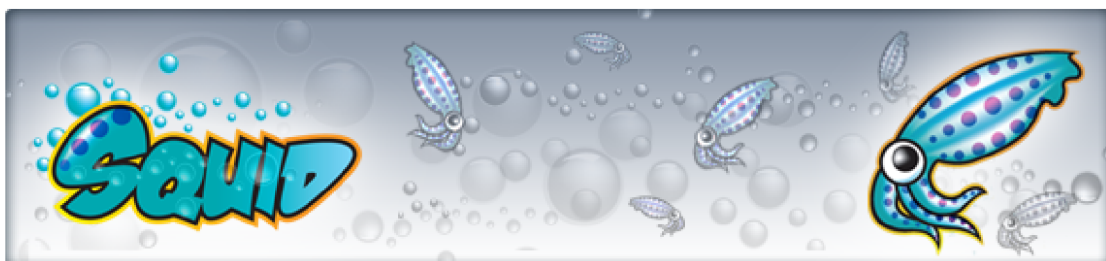
1. Introducción: Proxy y Squid
2. Instalación de Squid
3. Configuración de Squid
 - Configuración por defecto
 - Algunos Parámetros interesantes
 - Control de Acceso
 - Configuración avanzada
4. Proxy de anonimización: Tor

1. ¿Qué es un proxy?

- Proxy es un servidor por el que se pueden realizar peticiones de un determinado servicio de internet en nombre de otro, generalmente innacesible de otra forma.
- Sería un **intermediario** del cliente.
- El servicio más habitual por el que se accede con un proxy es la web (http y https) y el ftp. Para otros servicios se usa SOCKS [dante].
- Generalmente se aprovecha para introducir también una caché y ganar así velocidad y reducir el consumo de ancho de banda.

¿Qué es Squid?

- Squid es el servidor de proxy más usado
- Es un servidor de alto rendimiento para clientes web, ftp, gopher.
- Soporta SSL, resulta muy configurable, implementa un control de acceso e incluso se puede organizar jerárquicamente una red de proxy's.



2. Instalación de Squid

- Instalar el paquete **squid**
 - \$ sudo apt-get install squid
- El script de control es /etc/init.d/squid
 - Start
 - Stop
 - Restart
 - Reload
- Se lanza automáticamente una vez instalado

3. Configuración de Squid

- La configuración se realiza a través del fichero /etc/squid/squid.conf (sólo root)
- Los logs se guardan en /var/log/squid:
 - access.log
 - cache.log
 - store.log
 - Se rotan una vez al día, con “logrotate”
- La caché se guarda en /var/spool/squid
- El puerto para http por defecto es 3128, aunque muchas veces se usa el 8080.

Algunos parámetros interesantes

- `http_port [IP:]puerto` `/*:3128/`
- `https_port [IP:]puerto cert=cert.pm` `/ninguno/`
- `icp_port puerto` `/3130/`
- `cache_dir <tipo> <dir.>` `/var/spool/squid`
- `cache_mem <tamaño>` `/8 MB/`
- `maximum_object_size <tamaño>` `/4096 KB/`
- `acl` `/lista de control de acceso/`
- `http_access` `/permisos de acceso/`

Control de acceso

- El acceso se basa en listas de control de acceso (ACL) de la forma:
 - `acl <nombre_acl> <tipoacl> <cadenas>`
- Definidas las ACL, se permite o rechaza el acceso en función de cada ACL.
 - `http_access <allow|deny> <nombre_acl>`
- Ejemplo de configuración:

```
acl mi_empresa srcdomain midominio.com
http_access allow localhost
http_access allow mi_empresa
http_access deny all
```

Creando ACL's

- Los tipos de ACL más usados son:
 - src IP[/mask]
 - dst IP[/mask]
 - myip
 - arp MAC_address
 - srcdomain dte.us.es
 - dstdomain ...
 - dstdom_regex ...
 - time
 - url_regex ^http://...
 - Port 80 70 21 ...
 - Proto HTTP FTP
 - Method GET POST
 - Browser nombre

ACL's por 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 443 563 # https, snews
acl SSL_ports port 873 # rsync
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
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
```

Accesos por defecto

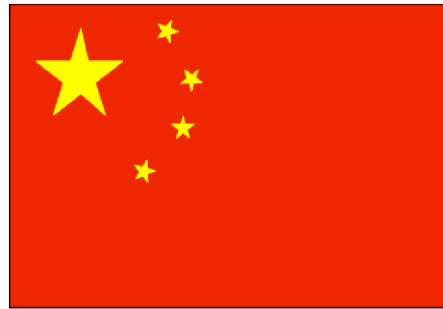
```
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Only allow purge requests from localhost
http_access allow purge localhost
http_access deny purge
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Only allow purge requests from localhost
http_access allow purge localhost
http_access deny purge
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
### PARA CONFIGURAR: #acl our_networks src 192.168.1.0/24 192.168.2.0/24
### PARA CONFIGURAR: #http_access allow our_networks
http_access allow localhost
### MUY IMPORTANTE: # And finally deny all other access to this proxy
http_access deny all
```

Configuración avanzada

- Squid tiene otras funciones avanzadas:
 - ICP: proxy's vecinos, para una red de proxy's
 - Acelerador del servidor web (httpd-accelerator)
 - Gestión avanzada del caché, división en discos, uso de RAID, políticas de reemplazo, ...
 - Opciones de logs, emulación del log de apache
 - Caché de DNS, resolución por programas externos
 - Autenticación del cliente del proxy
 - Controles de red, cabeceras http, timeouts, etc...
 - Anuncio del proxy como servicio público
 - Interfaz de estadísticas SNMP integrado

4. Proxy de anonimización

- Análisis de tráfico
- Email
- Web Browsing
- Censura del sistema (Firewall en China)
- Derecho a la privacidad



Proxy de anonimización

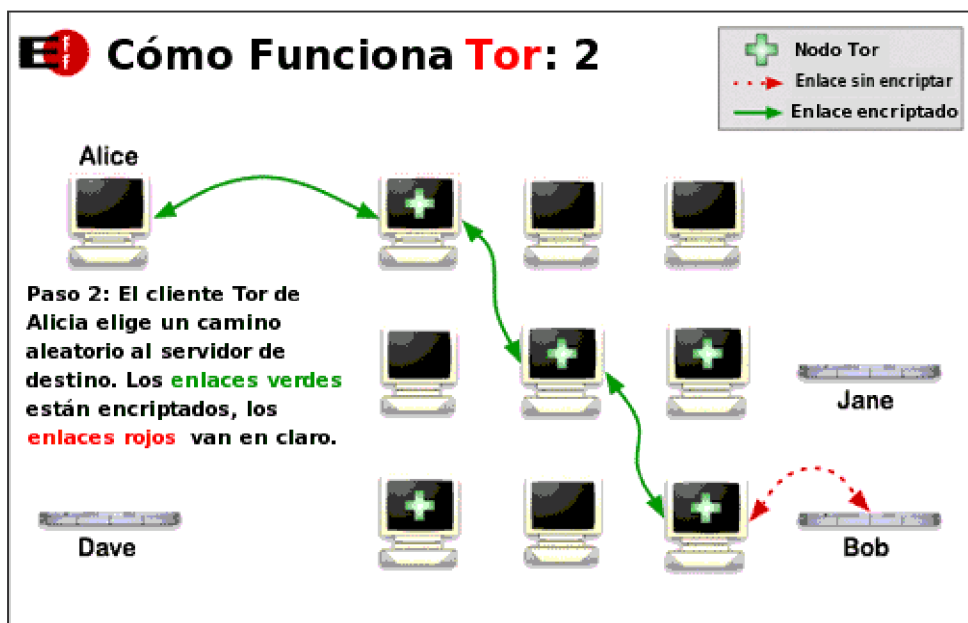
- TOR: The Onion Router
 - Capa de anonimización
 - Integración con Privoxy
 - Plugins para los principales navegadores
 - Incrementa el anonimato
 - No incrementa la privacidad
 - No es invulnerable
 - DNS leakage
 - Ataques fuente destino



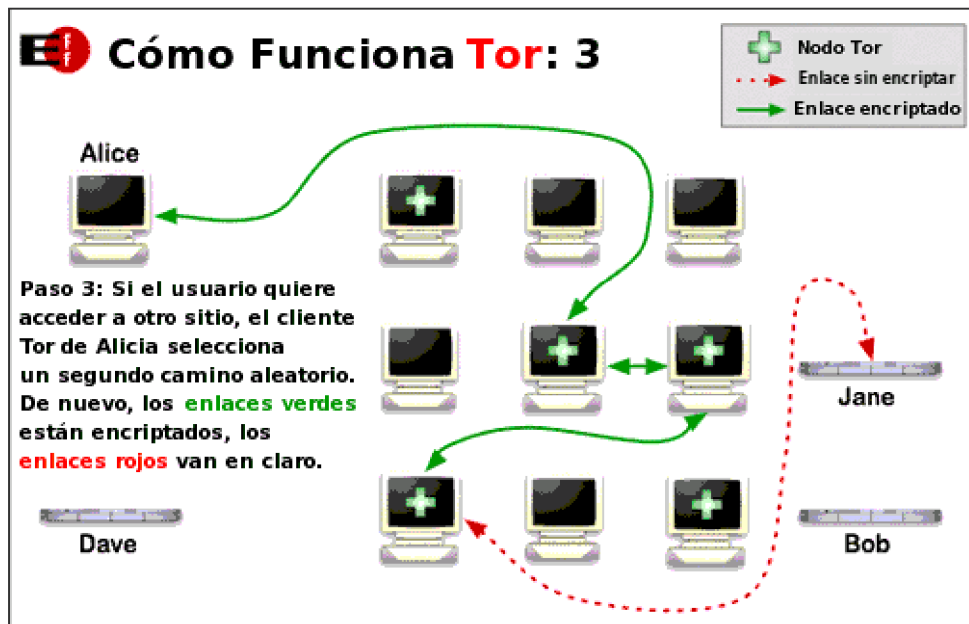
Proxy de anonimización



Proxy de anonimización



Proxy de anonimización



Proxy de anonimización

- Instalación de Tor, Privoxy y TorButton
 - `sudo apt-get install tor privoxy`
- Configuración de Privoxy
 - `sudo gedit /etc/privoxy/config/`
 - Añadir: `"forward-socks5 / localhost:9050 ."`
- Instalar la Extensión TorButton o similar