

Squid e Iptables

Configuración y uso

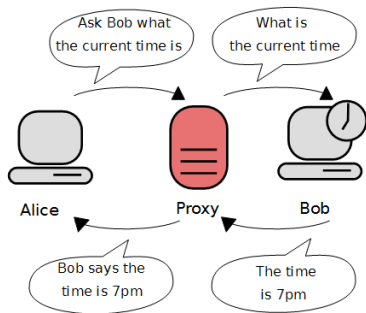
Carolina Alvarado Chavarría

UCR

2017

Proxy

- ▶ Squid es un proxy
- ▶ ¿Como funciona un proxy?



Squid



- ▶ ¿Como funciona el caché web?
- ▶ El bloqueo de paginas

Squid: Instalación y configuración

- Instalación con binario vs. código fuente
- Compilación
- Repositorio: squid3

```
caro@Link:~/Documents$ sudo apt-get install squid3
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  squidclient squid-cgi squid-purge resolvconf smbclient ufw winbind
The following NEW packages will be installed:
  squid3
0 upgraded, 1 newly installed, 0 to remove and 44 not upgraded.
Need to get 0 B/2,068 kB of archives.
After this operation, 6,577 kB of additional disk space will be used.
Selecting previously unselected package squid3.
(Reading database ... 170663 files and directories currently installed.)
Preparing to unpack .../squid3_3.4.8-6+deb8u4_amd64.deb ...
Unpacking squid3 (3.4.8-6+deb8u4) ...
Processing triggers for systemd (215-17+deb8u6) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up squid3 (3.4.8-6+deb8u4) ...
Creating Squid HTTP proxy 3.x spool directory structure
2017/04/25 22:19:29 kid1| Set Current Directory to /var/spool/squid3
2017/04/25 22:19:29 kid1| Creating missing swap directories
2017/04/25 22:19:29 kid1| No cache_dir stores are configured.
Processing triggers for systemd (215-17+deb8u6) ...
caro@Link:~/Documents$
```

Squid: ACL y puertos HTTP

- ▶ Puertos físicos vs. puertos virtuales
- ▶ Puertos predeterminados.
- ▶ Puerto 3128 o 8080



Squid: ACL y puertos HTTP

- ▶ ¿Que son las ACL?
- ▶ Access control lists
- ▶ ACL rápidas y lentas (src y dst)



Squid: Instalación y configuración

- ▶ Squid.conf
- ▶ Sintaxis del archivo de configuración
- ▶ Realizar archivos de texto con palabras prohibidas.

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM  
#  
visible_hostname Link  
acl bloqueadas url_regex "/etc/squid3/prohibidas"
```

Squid: Instalación y configuración

- ▶ El directorio de caché
- ▶ Caching selectivo

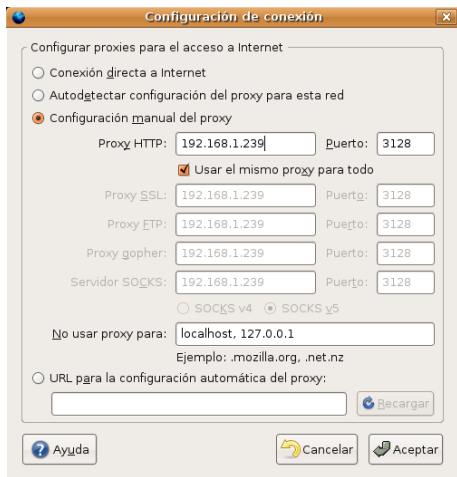


Squid: Instalación y configuración

- ▶ Refresh patterns
- ▶ Logging
- ▶ Archivos de registro, caché de accesos.

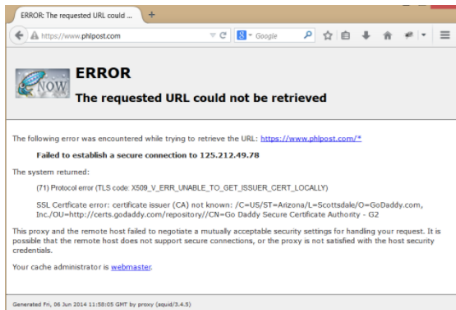


Squid: Configuración final



- ▶ Squid en navegador
- ▶ Firefox, chrome, explorer.
- ▶ /etc/init.d/squid3 restart

Squid: Paginas de error



- ▶ Pagina predeterminada
- ▶ /usr/share/squid3/errors/English
- ▶ Modificar utilizando html
- ▶ Se debe reiniciar de nuevo

Squid: Posibles dificultades

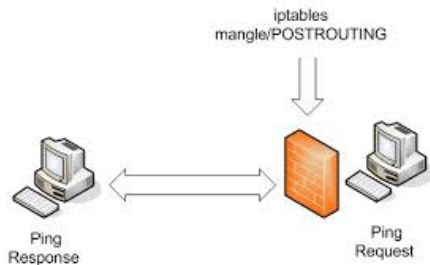
- ▶ Definir las ACL antes de denegarlas.
- ▶ Asegurarse de tener acceso por determinada ip
- ▶ Dificultad de no ser transparente
- ▶ Configurar cada navegador que se utilizará

Squid: Extras

- ▶ ¿Que es proxy transparente?
- ▶ Usar pi raspberry
- ▶ Almacenar logs en base de datos

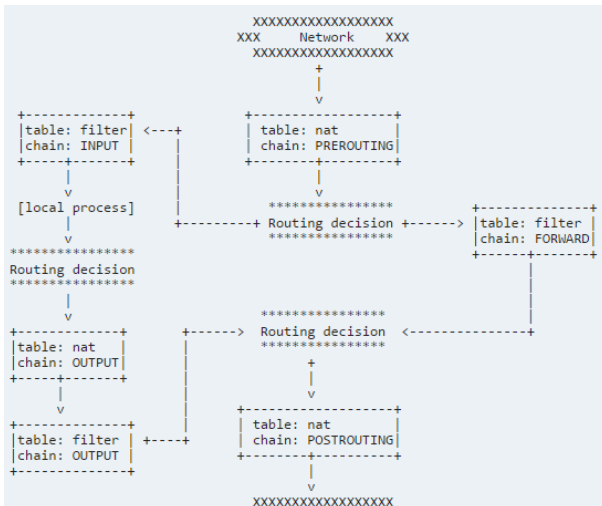
Iptables

- ▶ ¿Qué es iptables?
- ▶ Filtración de paquetes de entrada y salida.
- ▶ Pertence a Netfilter, firewall del kernel.



Iptables: Organización

- Internamente se divide en tablas, cadenas y reglas.



Iptables: Instalación y configuración

- ▶ Viene en el kernel pero se debe instalar paquete para utilización del usuario.
- ▶ Repositorio: iptables
- ▶ Una vez instalado se pueden crear nuevas reglas por medio de la terminal

```
caro@Link:~/Documents$ sudo apt-get install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  iptables
0 upgraded, 1 newly installed, 0 to remove and 44 not upgraded.
Need to get 277 kB of archives.
After this operation, 3,642 kB of additional disk space will be used.
Get:1 http://mirrors.ucr.ac.cr/debian/ jessie/main iptables amd64 1.4.21-2+b1 [277 kB]
Fetched 277 kB in 1s (158 kB/s)
Selecting previously unselected package iptables.
(Reading database ... 170587 files and directories currently installed.)
Preparing to unpack .../iptables_1.4.21-2+b1_amd64.deb ...
Unpacking iptables (1.4.21-2+b1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up iptables (1.4.21-2+b1) ...
Processing triggers for libc-bin (2.19-18+deb8u7) ...
caro@Link:~/Documents$
```


Iptables: Proxy transparente



- ▶ Se debe redireccionar el tráfico
- ▶ Se crea una regla
- ▶ Ahora el tráfico de red accesa el puerto donde esta squid escuchando

Virtualbox o Red de ordenadores

- ▶ Se puede utilizar squid en una red
- ▶ Para simularlo se puede utilizar una aplicación como virtualbox
- ▶ Se pueden controlar servidores en una red como en la universidad.
- ▶ El hecho que sea transparente permite pasar por el proxy sin conocimiento de los navegadores.

Conclusiones

- ▶ Utilizar un proxy como squid reduce el uso del ancho de banda.
- ▶ El caching permite disminuir el tiempo de carga de paginas web
- ▶ Con squid se pueden establecer reglas para el uso de la red además de monitorear el tráfico de cada usuario.
- ▶ Squid es una herramienta personalizable. Paginas de error, configuraciones de inicio, etc.

Conclusiones

- ▶ Un proxy transparente es más eficaz ya que elimina la necesidad de configurar cada navegador.
- ▶ Iptables es un firewall que permite controlar el tráfico tanto entrante como saliente.
- ▶ Las redes de varios servidores le encuentran una gran utilidad a el uso de un proxy transparente para controlar los derechos de cada cliente.