ÍNDICE

1

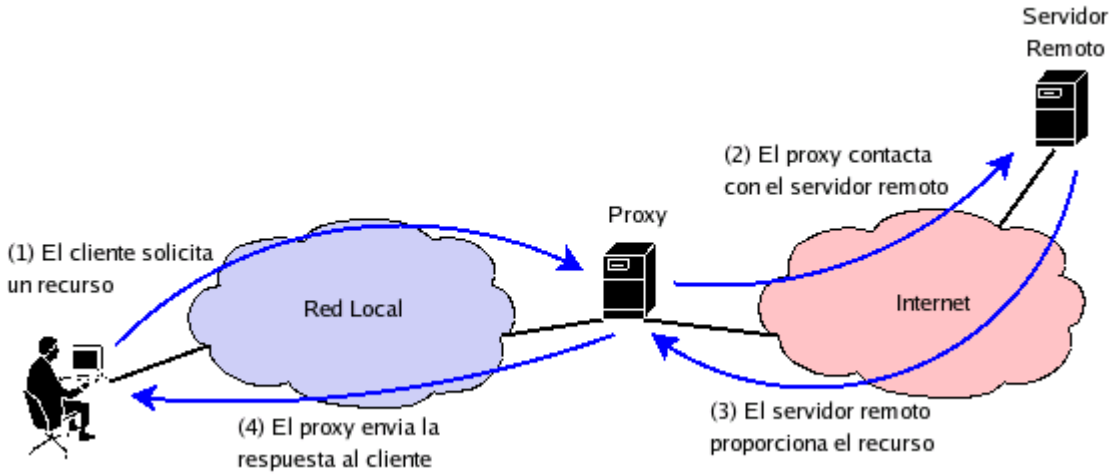
DEFINICIONES

1.1.- Proxy y cache

El servicio que permite a los usuarios realizar indirectamente conexiones a Internet es conocido como s*ervidor proxy*.

Un servidor proxy se situa entre la estacion cliente (el usuario) y el acceso a internet (ADSL, cable, Frame Relay...). El cliente se conecta al servidor proxy, solicita un recurso de Internet (una conexión, un fichero o cualquier otro recurso) y es el servidor proxy el encargado de solicitar ese recurso a Internet para proporcionárselo al cliente. La traducción de la palabra inglesa “proxy” viene a ser “*por poderes*”, es decir dejaremos que sea el servidor proxy el que se conecte a Internet por nosotros.

En algunos casos es posible que el proxy no se conecte a Internet para obtener el recurso solicitado sino que lo obtenga de una cache. El término *cache* es utilizado en el ámbito informático para designar un conjunto de datos replicando a los originales, residentes en un almacenamiento remoto: Cuando se accede por primera vez a un dato, se hace una copia en el caché, los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso aparente al dato sea menor.



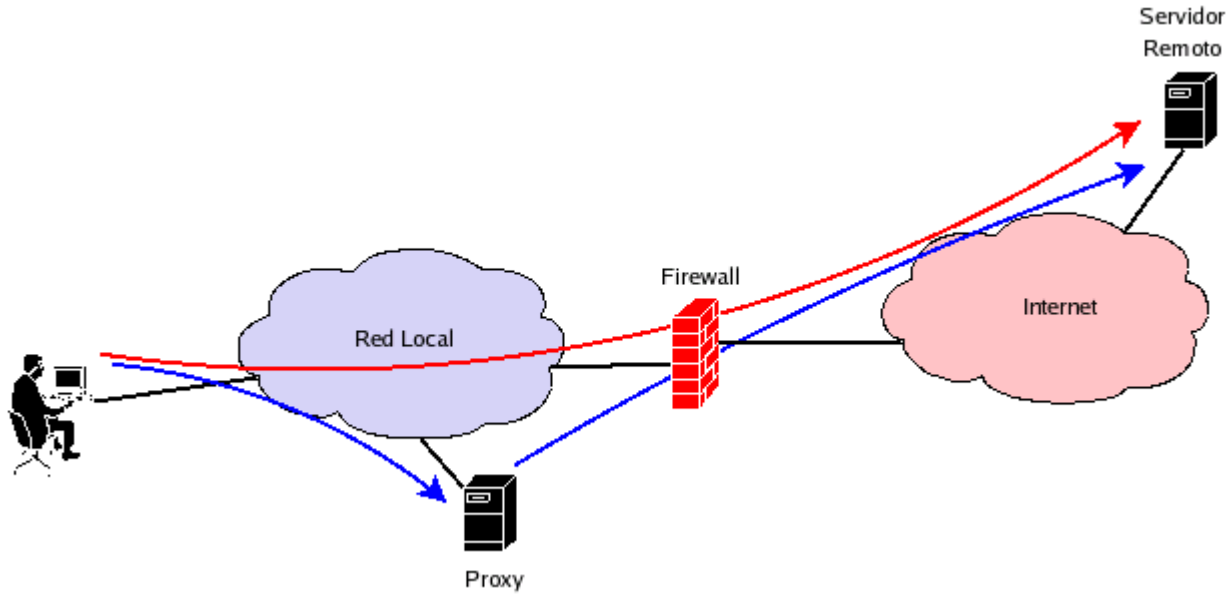
1.2.- Web proxy cache

Se dice que un servidor esta actuando como *web proxy cache* cuando almacena en su disco duro las páginas web descargadas de forma que, en próximas consultas, pueda acceder a ellas de forma muy rápida. De esta forma estamos optimizando el canal de acceso a Internet de la organización y mejoramos la sensación de navegación del usuario en momentos de ocupación importante de la línea.

Este tipo de proxy se suele usar en alguno de estos entornos:

- Cuando, por motivos de seguridad, no deseas permitir acceso libre a Internet a los usuarios pero se desea proporcionarles acceso a la web: se les proporciona a través del proxy.
- Cuando se desea optimizar el ancho de banda y acelerar la navegación para los usuarios. Por ejemplo, una oficina con muchos trabajadores que suelen visitar frecuentemente las mismas paginas.

Esta sería una posible estructura para impedir que los usuarios puedan acceder directamente a Internet:



1.3.- Proxy inverso

Un proxy inverso (o *reverse proxy*) es aquel que se sitúa cerca de uno o mas servidores web, de forma que es el proxy quien recibe las peticiones y las reenvía a los servidores web. Este tipo de proxy se suele usar en algunos de estos entornos:

- Para añadir seguridad a los servidores web: en ningún momento se accede directamente a ellos sino al proxy.
- Para balancear la carga de los servidores: el servidor proxy es el encargado de enviar las peticiones a aquellos servidores que estén mas descargados.
- Para descargar a los servidores webs de contenido estático como imágenes o documentos.
- En caso de sitios webs seguros se puede dejar al proxy que haga el encriptado de los datos y descargar así a los servidores web.

1.4.- Proxy transparente

Tal como hemos visto es posible usar un proxy para aplicar políticas de control de acceso a Internet. Normalmente esa configuración no es transparente: es necesario modificar el cliente para que use el proxy al acceder a Internet, de forma que es posible que un usuario modifique esa configuración.

Una configuración de proxy transparente hace que no sea necesaria modificación alguna en las máquinas clientes, eliminando el riesgo de que un usuario modifique dicha configuración a su antojo. El uso de un proxy transparente combina un servidor proxy con NAT, de forma que todas las conexiones son encaminadas a través del proxy sin la intervención de la máquina cliente.

2

Squid Web Proxy Cache

2.1.- Qué es Squid

Squid es un servidor proxy cache para clientes web que soportaFTP, gopher y HTTP.

Algunas características:

- Almacena en RAM los metadatos y los objetos muy consultados
- Guarda en cache las consultas DNS
- Soporta consultas de DNS no bloqueantes
- Soporta SSL
- Políticas de control de acceso
- Permite reescrituras de consultas
- Permite integración con dominios de Active Directory de Microsoft

2.2.- Sistemas operativos soportados

Estos son los sistemas operativos soportados a fecha de Marzo de 2005:

- Linux
- FreeBSD
- NetBSD
- OpenBSD
- BSDI
- MacOS X
- OSF / Digital Unix / Tru64
- IRIX
- SunOS / Solaris
- NeXTStep
- SCO Unix
- AIX
- HP-UX
- OS/2

Además existen algunos proyectos que proporcionan Squid para sistemas operativos Windows.

2.3.- Licencias de Squid

- Squid tiene copyleft por parte de la Universidad de California San Diego.
- Squid es software libre [1].
- Squid está licenciado bajo los términos de la licencia GNU GPL [2].

2.4.- Integración en dominios Microsoft

Una de las necesidades que tienen las organizaciones que trabajan con Active Directory de Microsoft es integrar la política de acceso a Internet (controlada desde el Proxy) con lo que tengan estructurado en el LDAP.

Mediante el uso de Samba es posible realizar una integración de Squid en dominios Microsoft de forma que podamos controlar que los usuarios que acceden a Internet son los proporcionados en una lista o, de forma mas óptima, los miembros de un grupo de usuarios de Active Directory.

Es importante destacar que dicha integración se comporta diferente si los clientes trabajan con un navegador u otro:

- Navegador propietario de Microsoft: al ser capaz de gestionar autenticación NTLM (NT Lan Manager) de forma que Samba puede obtener directamente el usuario autenticado en dominio que intenta acceder a Internet.
- Otros navegadores: al no disponer de la autenticación NTLM el proxy les solicitará su usuario y password de dominio para poder determinar si pertenecen o no al grupo de usuarios que pueden acceder a Internet.

Para realizar esta integración será necesario:

1. Descargar e instalar Samba 2.x o 3.x en el servidor que ejecuta Squid. A la hora de instalar es importante indicar a Samba que trabaje con *winbind*.

2. Configurar Samba indicándole el nombre de dominio Microsoft con el que tendrá que dialogar, así como los Domain Controlers de dicho dominio.

3. Configurar Squid para que use *ntlmauth* como sistema de autenticación de usuarios.

4. Meter la máquina en el dominio Microsoft.

3

Inspección de Contenidos

3.1.- En qué consiste

Es posible que nos interese proteger a los usuarios de contenido no deseado o, directamente, evitar que puedan acceder a contenido que no sea adecuado.

Para eso existen herramientas que inspeccionan el contenido que van a enviar (web, correo, etc...) al cliente y bloquean aquel que no es considerado adecuado.

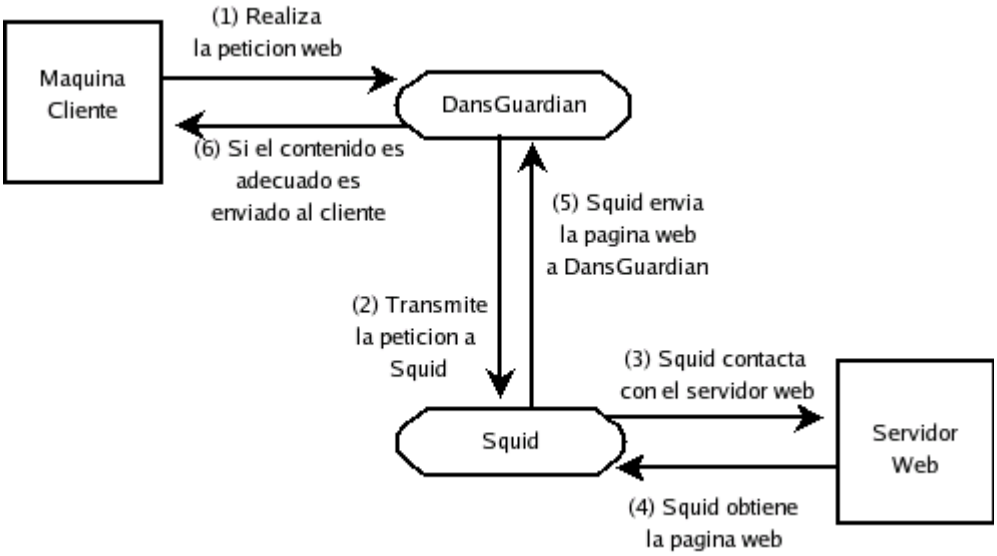
3.2.- DansGuardian

Es un filtro de contenido web que funciona sobre Linux, FreeBSD, OpenBSD, NetBSD, MacOS X, HP-UX y Solaris. Su filtrado no se basa simplemente en una lista negra de URLs sino:

- Buscando determinadas frases o patrones en el contenido web
- Filtrado de imágenes
- Filtrado de URLs

Para cualquier uso no comercial su licencia es GPL [2].

Se integra perfectamente con Squid: DansGuardian escucha en un puerto y reenvía las solicitudes de descarga a Squid. En función del contenido de la web le envía el contenido de dicha web al cliente o le muestra una página indicando que el contenido al que quería acceder no es considerado adecuado.



Para implantarlo en nuestra red simplemente deberemos de poner a DansGuardian como el proxy al que se conectan nuestros clientes y él será el encargado de comunicarse con Squid.

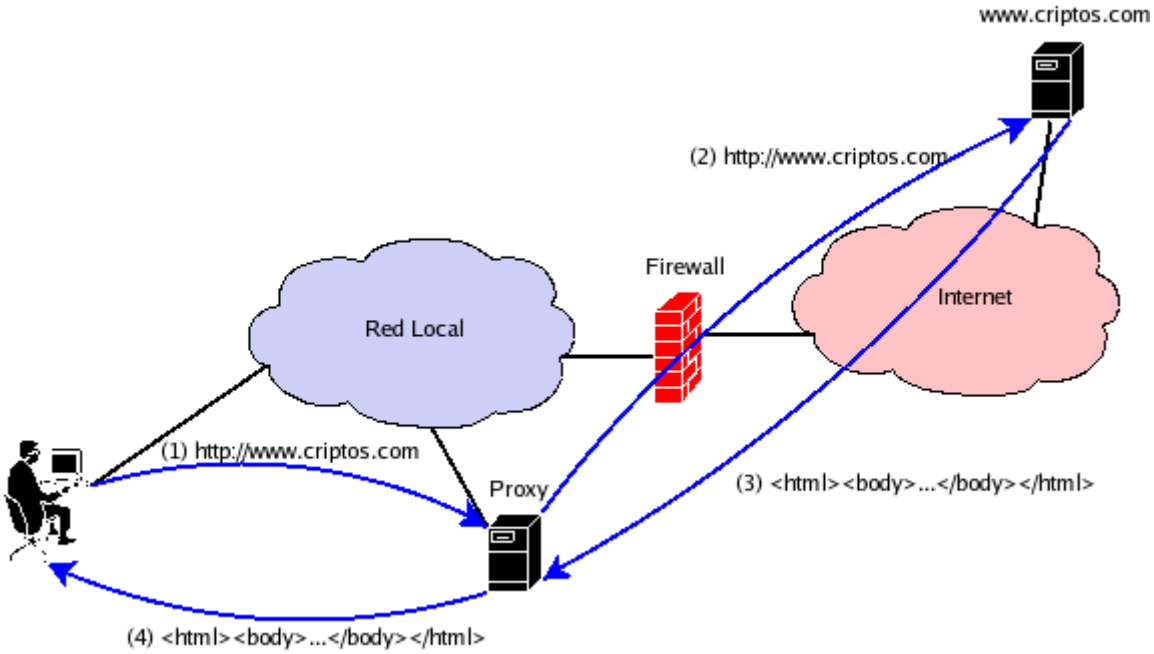
4

ESCENARIOS

4.1.- Squid como único proxy en nuestra red

Es la configuración básica pero probablemente la adecuada para muchas organizaciones:

- Se impide el acceso a Internet a todos los clientes.
- Se configuran los navegadores de las máquinas clientes para que accedan por nuestro proxy.
- Se concede a nuestro proxy permiso para acceder a los puertos HTTP/HTTPS de Internet.

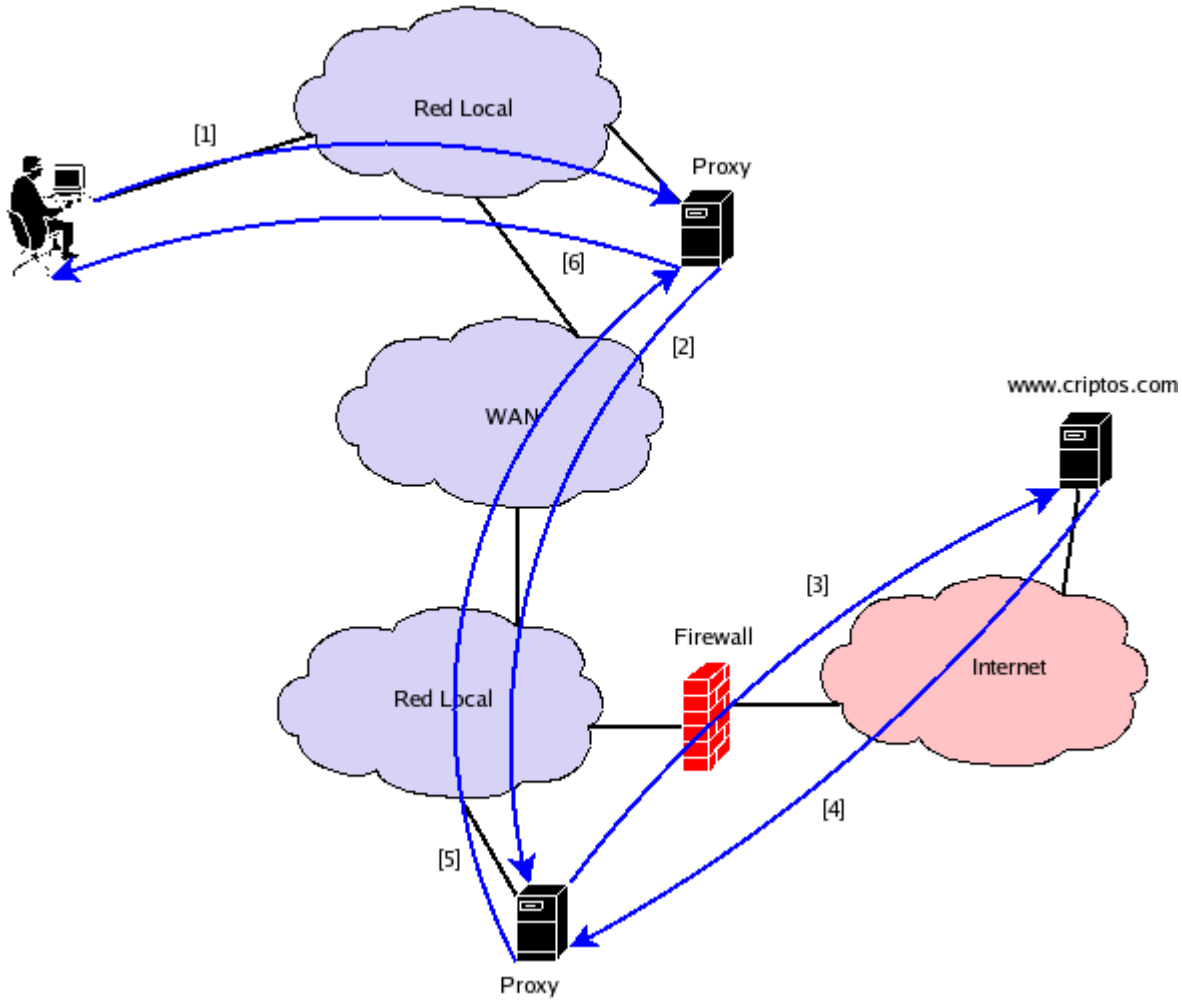


4.2.- Squid en una jerarquía de proxies en nuestra red

Esta característica será importante a la hora de integrar con DansGuardian y LDAP de Microsoft, consiste en:

- Se impide el acceso a Internet a todos los clientes.
- Se configuran los navegadores de las máquinas clientes para que accedan por nuestro proxy de segundo nivel.
- El proxy de segundo nivel se configura para que reenvíe las solicitudes a otro proxy que será el encargado de obtenerlas.
- Se concede al proxy de primer nivel permiso para acceder a los puertos HTTP/HTTPS de Internet.

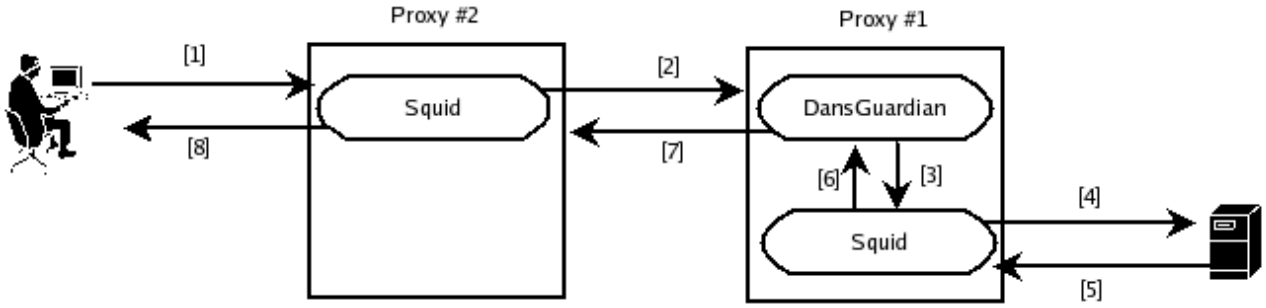
Esta estructura es útil si tenemos varias sedes conectadas con la central a través de lineas con poco caudal: poniendo un proxy en cada sede periférica estamos reduciendo el tráfico web entre esas sedes y la central.



4.3.- Squid con inspección de contenido

El problema con el que nos encontramos es que DansGuardian no gestiona autenticación NTLM, de forma que necesitamos hacerla con Squid pero sin perder la inspección de contenido. Una alternativa es:

- Montar un proxy de segundo nivel (con el que contactarán las máquinas cliente) sin DansGuardian, solo para evaluar si el usuario puede acceder o no a Internet (según sus privilegios de Active Directory).
- Montar un proxy de primer nivel con DansGuardian que haga la inspección de contenido



1. El cliente envía una solicitud web al Proxy#2. Éste evalúa si pertenece al grupo de usuarios de Active Directory con permisos para acceder.
2. Si pertenece a ese grupo envía la solicitud al DansGuardian del Proxy#1.
3. DansGuardian reenvía la petición al Squid de la misma máquina.
4. Squid se pone en contacto con el servidor web remoto.
5. El servidor web envía la página web a Squid.
6. Squid se la devuelve a DansGuardian
7. DansGuardian evalúa si el contenido es apto o no. Si es apto enviará la página web al Squid de Proxy#2, si no es apto enviará a dicho Squid una página informando de que esa web no es apta.
8. Squid de Proxy#2 envía al usuario el contenido remitido por DansGuardian de Proxy#1

5 REFERENCIAS

- Wikipedia:
  - http://en.wikipedia.org/wiki/Proxy_server
  - http://en.wikipedia.org/wiki/Squid_cache
- Squid Web Proxy Cache:
  - http://www.squid-cache.org/
- Acme Consulting:
  - http://www.acmeconsulting.it/SquidNT/
- Proyecto GNU:
  - [1] http://www.gnu.org/philosophy/free-sw.html
  - [2] http://www.gnu.org/copyleft/gpl.html
- DansGuardian:
  - http://dansguardian.org/