Fuente: http://es.wikipedia.org/w/index.php?title=Proxy&oldid=8001661

PROXY

Proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la de ***servidor proxy,*** que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, es decir, una única dirección IP.

La palabra proxy se usa en muchas situaciones, donde tiene un sentido intermedio:

a) ***Servidor proxy*** es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

- El más famoso es el ***servidor proxy de web (proxy)*** que intercepta la navegación de los clientes por páginas web por varios motivos: seguridad, rendimiento, anonimato, etc.
- También existen proxies para otros protocolos, como el ***proxy de FTP.***
- ***Proxy ARP*** puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

b) Proxy también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.

c) Un componente hardware también actúa como intermediario para otros (Por ejemplo: un teclado USB al que se conectan más dispositivos USB).

d) Fuera de informática, proxy puede ser una persona autorizada para actuar en representación de otra.

e) En una ***guerra proxy*** las dos potencias usan a terceros para el enfrentamiento directo.

Proxy tiene un significado general, aunque siempre es sinónimo de ***intermediario.*** También se puede traducir por ***delegado*** o ***apoderado.***

VENTAJAS

1. **Control.** Sólo el intermediario hace el trabajo real, por lo tanto, se pueden limitar y restringir los derechos de los usuarios y dar pérmisos sólo al proxy.
2. **Ahorro.** Sólo el proxy ha de estar equipado para hacer el trabajo real.
3. **Velocidad.** Si varios clientes van a pedir el mismo recurso, el proxy puede hacer ***caché:*** guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
4. **Filtrado.** El proxy puede negarse a responder peticiones si detecta que están prohibidas.
5. **Modificación.** Un proxy puede falsificar información o modificarla siguiendo un algoritmo.
6. **Anonimato.** Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo cuando hay que hacer necesariamente la identificación.

DESVENTAJAS

1. **Abuso.** Ha de controlar quién tiene acceso y quién no a sus servicios, trabajo que es muy difícil.

Fuente: http://es.wikipedia.org/w/index.php?title=Proxy&oldid=8001661

2. **Carga.** Un proxy hace el trabajo de muchos usuarios.
3. **Intromisión.** Es un paso entre origen y destino, y algunos usuarios no quieren pasar por él. Y menos si actúa como caché y guarda copias de los datos.
4. **Incoherencia.** Si actúa como caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente.
5. **Irregularidad.** Si un proxy representa a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre un emisor y un receptor (TCP/IP).

FUNCIONAMIENTO

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es proxy quien realiza la comunicación y traslada al resultado al equipo inicial. En algunos casos, esto se hace así porque no es posible la comunicación directa o porque proxy añade una funcionalidad adicional como mantener los resultados obtenidos (caché).

PROXY DE WEB / PROXY CACHÉ DE WEB

Proxy para una aplicación específica: el acceso a Web. Proporciona una caché para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo, libera la carga de los enlaces hacia Internet.

Funcionamiento

1. El cliente realiza una petición (p.e. mediante un navegador web) de un recurso de Internet (página web o archivo) especificado por una url.
2. Cuando el proxy caché recibe la petición, busca la url en su caché local. Si la encuentra, devuelve el documento inmediatamente, si no, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda una copia en su caché para futuras peticiones.

El caché utiliza un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de estos algoritmos son ***LRU (usado menos recientemente o Least Recently Used)*** y el ***LFU (usado menos frecuentemente o Least Frequently Used).***

Ejemplo:

Un cliente de ISP manda una petición a Google. La petición llega en un inicio al servidor Proxy que tiene el ISP, no va directamente a la dirección IP del dominio de Google. Esta página suele ser muy utilizada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta mucho menor en tiempo. Cuando el usuario crea una búsqueda, el servidor Proxy ya no es utilizado y el ISP envía su petición y el cliente recibe su respuesta desde Google.

Ventajas.

Fuente: http://es.wikipedia.org/w/index.php?title=Proxy&oldid=8001661

a) Ahorro de tráfico.- Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red.
b) Demanda a usuarios.- Puede cubrir a gran número de usuarios.
c) Filtrado de contenidos.- El servidor proxy puede hacer un filtrado de páginas o contenidos basándos e en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite.
d) Modificación de contenidos.- Basándose en la función de filtrado, protege la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies.

Desventajas.
a) Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.
b) El hecho de acceder a Internet a través de un Proxy, en vez de conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.

PROXIES TRANSPARENTES

Muchas organizaciones (empresas, colegios o familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché.

Un proxy transparente combina un servidor proxy con NAT de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente y sin que el cliente conozca de su existencia. Este es el tipo de proxy que utilizan los Proveedores de Servicios de Internet (ISP).

REVERSE PROXY

Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy.
Razones para instalar un “reverse proxy”.

a) Seguridad.- El servidor proxy es una capa adicional de defensa y protege los servidores web.
b) Cifrado / Aceleración SSL.- Cuando se crea un sitio web seguro, el cifrado SSL no la hace el servidor web, sino que es realizada por el “reverse proxy”, el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).
c) Distribución de Carga.- El reverse proxy puede distribuir la carga entre varios servidores web.
d) Caché de contenido estático.- Un reverse proxy puede descargar los servidores web almacenando contenido estático como imágenes y otro contenido gráfico.

Fuente: http://es.wikipedia.org/w/index.php?title=Proxy&oldid=8001661

PROXY NAT (NETWORK ADDRESS TRANSLATION) /ENMASCARAMIENTO

Un mecanismo para hacer de intermediario en una red es NAT.

La Traducción de Direcciones de Red (NAT, Network Address Translation) también es conocida como enmascaramientode Ips. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP con reescritas, sustituidas por otras (de ahí el enmascaramiento).

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la LAN los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a la única dirección pública para realizar las peticiones.

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los cortafuegos, y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador.