TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“tipos de proxy”

UNIDAD 2

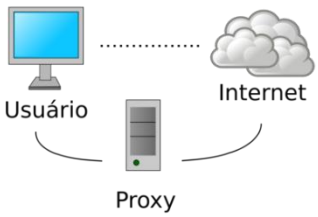
Proxy

Comúnmente un servidor proxy es un dispositivo que intercepta conexiones de red hechas desde un cliente a un servidor de destino. El significado básico más conocido de la palabra proxy es: función de algo que actúa como sustituto de otro. En otras palabras, un servidor proxy es un tipo específico de servidor de aplicaciones que direcciona solicitudes HTTP de clientes, a los servidores de contenido que realmente realizan el trabajo. Usualmente, un servidor proxy intercepta una conexión entre un dispositivo e Internet, manipulando la comunicación directa entre los dos puntos. También conocido como pasarela a nivel de capa de aplicación entre una red y otra de mayor escala (por ejemplo, Internet), un servidor proxy puede ser una aplicación o un dispositivo específico en una red, que filtra las transferencias de datos salientes y entrantes. La situación estratégica de punto intermedio, le permite ofrecer diversas funcionalidades a un servidor proxy: control de acceso, registro de trazas, restricción a determinados tipos de información y tráfico, mejoras de rendimiento, anonimato de la comunicación, caché web, entre otros. Dependiendo del contexto, la intermediación que realiza el proxy puede ser considerada tanto por usuarios, como por administradores y proveedores de servicios.

Existen dos clasificaciones de proxys atendiendo al objetivo de quien implemente su política de intermediación:

- proxy local: En este caso el que implementa la política es el mismo que hace la petición, por eso se denomina local. Suelen estar en el mismo dispositivo que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y establecer reglas de filtrado que aseguren, por ejemplo, que no se revela información privada.

- proxy de red: En esta implementación, quien establece las políticas del proxy es una entidad, y se aplica para todos los dispositivos que empleen su infraestructura de red; también suele denominarse proxy externo. Se utiliza fundamentalmente para implementar filtros, bloquear contenidos, control de tráfico, registro de trazas, entre otros.

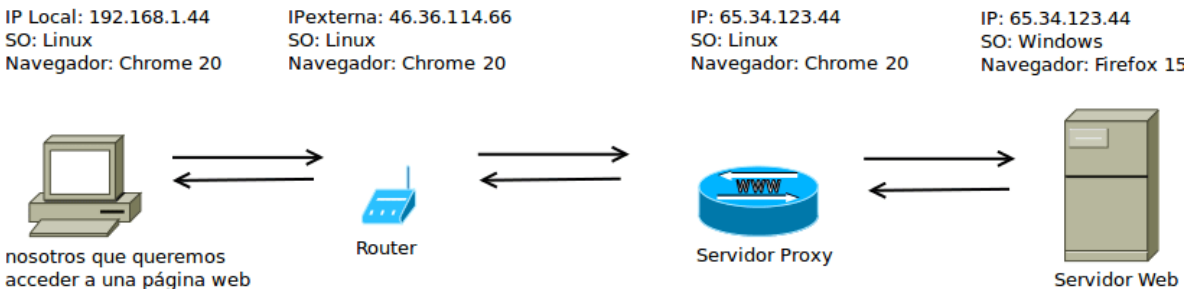


Funcionamiento

Un proxy permite a otros dispositivos 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 realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. Generalmente, un proxy es un punto intermedio entre un dispositivo de una red e Internet para acceder a algún recurso. Cuando se navega a través de un proxy, el cliente que realiza la solicitud en realidad no está accediendo directamente al servidor, sino que es el proxy quien accede a lo demandado, y devuelve el resultado de la petición. Es el servidor proxy quien se encarga de la traducción de las direcciones de red (NAT, Network Address Translation) también conocida como enmascaramiento IP.

Esto es lo que ocurre cuando varios dispositivos comparten una única conexión a Internet. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado, y generalmente una dirección IP única de salida hacia otra red o Internet; en ese sentido, el proxy es el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las respuestas recibidas a cada usuario interno que la solicitó. Esta situación es muy común en las empresas y domicilios con varios dispositivos en red y un solo acceso externo 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 los equipos no están expuestos a ataques directos desde el exterior. El servidor proxy, además, suele tener una memoria cache de almacenamiento, que guarda una copia de las páginas web que han sido visitadas, de manera que el primer acceso será físicamente al servidor de destino, mientras que los sucesivos, es el proxy quien comprueba si ya fue accedida con anterioridad (si se encuentra en su cache), y si no ha sido modificada en el servidor desde la última solicitud del proxy. En caso afirmativo, en lugar de solicitar de nuevo la página al servidor, envía al usuario la copia que tiene en la caché, lo que mejora notablemente el rendimiento o velocidad de la conexión a Internet de los equipos que están detrás del proxy.



Los servidores proxy tienen múltiples funciones, algunas de las más comunes son:

Interfaz entre la red interna y la pública (Internet): para controlar los accesos de los dispositivos de una red a Internet.

Control del ancho de banda: a los usuarios de una red pueden asignársele ciertos recursos, y un determinado ancho de banda disponible. Las tareas de control también incluyen la supervisión de la disponibilidad del servidor.

Protección contra ataques por la red: el servidor proxy se coloca entre el servidor de datos real y los usuarios. Las páginas WEB que trabajan con datos confidenciales de clientes, como las tiendas online, por ejemplo, a menudo utilizan esta solución para proteger sus servidores.

Registro en la red: los servidores proxy se utilizan habitualmente para registrar la actividad en la red; de este modo, se puede identificar más rápidamente el acceso mal intencionado.

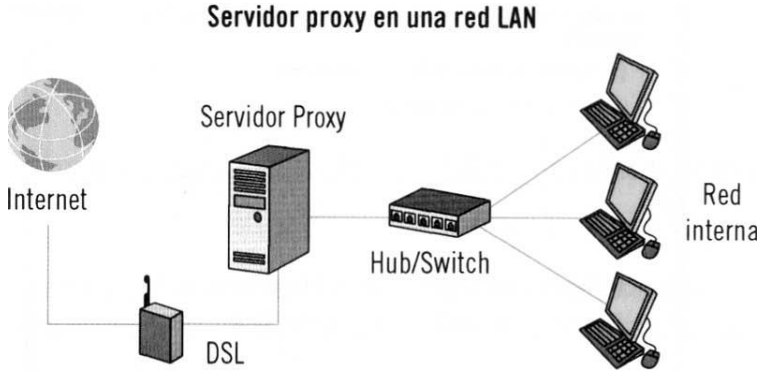
Tráfico anónimo: en Internet, el empleo de un proxy puede anonimizar una dirección IP y de esta manera evadir las restricciones sobre el acceso, por ejemplo, a un determinado sitio WEB.

Reducción de carga hacia el servidor real: un servidor proxy puede almacenar las peticiones que le han sido enviadas, y con ello entregar información solicitada sin causar una carga para el servidor de aplicaciones real; al mismo tiempo, el cliente solicitante recibe la información más rápidamente.

Bloqueo de contenido: en redes públicas, el acceso a Internet puede restringirse a través de un servidor proxy, y en este sentido limitar la navegación por los sitios WEB según su contenido, o en determinados horarios; además, las funciones de filtro también pueden incluir la eliminación de publicidad mientras se navega.

Ajuste de tiempo: un servidor proxy puede ajustar los tiempos de espera y los límites de duración de las solicitudes y respuestas para evitar el mal desempeño de la red. Además, puede personalizar el mensaje de negación de contenidos para las distintas restricciones.

v



Tipos de Proxys

Existen muchos tipos distintos de proxy, cada uno con funciones y características determinadas. A continuación, una pequeña lista con algunos de los más comunes:

Proxy WEB/caché WEB: es el tipo más común y se encarga del acceso a la WEB, enmascarando la dirección IP de los dispositivos de una red por la de él, ante la solicitud de un recurso en Internet. Además, proporciona el almacenamiento caché para 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 que libera la carga de los enlaces hacia Internet.

Proxy inverso: también conocido como reverse proxy, generalmente se configura junto con uno o varios servidores de aplicaciones que reciben peticiones desde Internet, para protegerlos, por ejemplo, de ataques de denegación de servicios. Todo el tráfico entrante de Internet y con destino de uno de esos servidores WEB pasa a través del proxy inverso, como capa adicional de seguridad; además, cuando se crea un sitio WEB seguro (HTTPS), habitualmente el cifrado no lo hace el mismo servidor WEB, sino que es realizado por el proxy. Del mismo modo, el proxy inverso puede realizar la distribución de cargas entre varios servidores WEB, reescribiendo las solicitudes externas en direcciones internas según sea el servidor donde se encuentre la información solicitada, así como almacenar contenido estático como imágenes o gráficos para acelerar la respuesta.

Proxy transparente: no requieren configuración por parte del cliente, aplicándose directamente a nivel de capa de red. Son utilizados generalmente por los Proveedores de Servicios de Internet (ISP) para filtrado WEB, entre otras cosas.

Proxy abierto: son servidores proxy que aceptan peticiones desde cualquier dispositivo, estén o no conectados a una misma red. En esta configuración el proxy ejecutará cualquier petición realizándola como si fuera propia. No son muy recomendados pues suelen emplearse como pasarela para el envío de correos spam, por lo que algunos servicios deniegan el acceso desde ellos.

Ventajas y Desventajas

En general, los proxys hacen posible:

El Control: solamente el intermediario hace el trabajo real, por tanto, se pueden limitar y restringir los derechos de los usuarios, y dar permisos únicamente al servidor proxy.

El Ahorro: solamente uno de los usuarios (el proxy) ha de estar preparado para hacer el trabajo real, o sea, disponer de los recursos y su configuración, en este caso, de la dirección IP externa de salida a Internet, por ejemplo.

La Velocidad: si varios clientes solicitan el mismo recurso, el proxy puede almacenar en caché la respuesta de una petición para devolverla directamente cuando otro usuario la necesite, de manera que se mejora el tiempo de respuesta.

La Demanda: puede cubrir a un gran número de usuarios, para solicitar, a través de él, determinados contenidos WEB.

El Filtrado: el proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

El Anonimato: Conectarse de forma anónima a un recurso externo sin revelar la dirección IP del cliente, pues se emplea la que es usada por el proxy para la obtención del recurso.

Por otra parte, también el empleo de proxys puede provocar:

No identificación: si todos los usuarios se identifican como uno solo, es difícil que el recurso accedido pueda diferenciarlos, pues todas las peticiones se realizan desde la misma dirección IP. Lo anterior en algunos escenarios puede representar un problema cuando se requiere necesariamente de una identificación real, o realizar operaciones avanzadas a través de algunos puertos o protocolos.

Intromisión: almacenar páginas y objetos que los clientes solicitan puede suponer una violación de la intimidad para algunos usuarios, sobre todo cuando se emplea el almacenamiento en caché y se guardan copias de los datos.

Incoherencia: al hacer uso del almacenamiento caché, las páginas WEB mostradas pueden no estar actualizadas si han sido modificadas desde la última carga que se realizó. Este problema en la actualidad se encuentra notablemente restringido, pues el proxy se conecta con el servidor remote para comprobar que la versión que tiene en el caché sigue siendo la más actualizada; no obstante, en ocasiones suele presentarse esa situación.