

Instituto Tecnológico de Cancún.

Investigación:

Tipos de proxy.

Kanxoc Ek Felix Gerardo.

Ismael Jiménez Sánchez.

Ingeniería en Sistemas Computacionales.

Fundamentos de Telecomunicaciones.

Noviembre 2020.

Proxy.

es un servidor (puede ser tanto un programa como un dispositivo físico) que actúa como un intermediario. Se sitúa entre la solicitud que realiza un cliente y otro servidor que da la respuesta. Si queremos acceder desde un móvil a un servidor de Internet donde está alojada una página web, un proxy puede actuar de intermediario.

Esto permite ganar más control de acceso, registrar el tráfico o incluso restringir determinados tipos de tráfico. De esta forma podremos mejorar en seguridad y también en rendimiento, así como tener anonimato al acceder a determinados servicios.

Una de las funciones más comunes para lo que los usuarios utilizan los proxys es para saltarse la restricción geográfica. Es decir, un proxy puede actuar como intermediarios y hacer que nuestra conexión aparezca en otro lugar. De esta forma podemos acceder a contenido disponible únicamente para un determinado país o poder ver contenido que no esté disponible en el nuestro.

Para que sirve un proxy.

En este caso, el proxy puede cumplir algunas de las siguientes funciones:

- **Control de acceso:** es posible que los administradores del servidor proxy permitan que ciertos usuarios tengan o no acceso a Internet a través de restricciones en su propio inicio de sesión o direcciones IP, proporcionando al entorno una capa adicional de protección.
- **Filtrado de contenido:** al estar en el medio del camino, el servidor también permite, o no, el acceso a ciertos sitios. Entre las reglas que se pueden aplicar están aquellas para bloquear sitios web específicos, pudiendo llegar a bloquear categorías completas.
- **Caché:** otro uso muy común para Web Proxies es hacer que realicen la función de caché. Esto hace que el proxy, después de acceder a una página, almacene el contenido de la misma en su sistema. Después de eso, las otras solicitudes a esta misma página no tendrán que ir a Internet, porque el contenido ya está almacenado en la memoria del proxy.

Estas son funciones ampliamente utilizadas de un servidor proxy web e ilustran un escenario de uso común para la mayoría de las empresas.

Proxy inverso

Otro uso muy común son los servidores de proxy inverso. En los ejemplos anteriores, el origen de la conexión siempre estuvo dentro de la red, pasaba por el proxy hasta Internet. En el caso del proxy inverso, el origen de las solicitudes está en Internet y busca acceder a un servidor dentro del entorno.

- **Equilibrio de carga:** debido a que la estructura del servidor proxy inverso le permite conectarse a varios servidores de destino, puede dirigir las solicitudes a cada uno de ellos sin sobrecargar ninguna. Como otra característica de seguridad, las solicitudes de Internet conocerán solo la dirección IP del proxy y no todos los servidores y páginas que tiene la compañía.
- **Caché:** como en el ejemplo de caché web, los servidores proxy también se utilizan para optimizar las solicitudes entre origen y destino. El servidor proxy inverso almacena elementos de página almacenados en servidores internos, buscando actualizaciones de contenido de vez en cuando, para que los servidores de página reciban incluso menos solicitudes de red, lo que les permite funcionar aún mejor.

Proxy para todos

No podemos hablar de proxy sin hablar de proxies gratuitos. Son páginas web, como <https://free-proxy-list.net/>, que proporcionan direcciones de servidores proxy en todo el mundo “absolutamente gratis”. Cualquier persona en Internet puede realizar la configuración adecuada en su navegador y utilizar el servidor ofrecido para navegar por la web.

Si la duda es para qué alguien puede querer esto, las respuestas son diversas. El uso de un proxy hace que todas las solicitudes sean hechas por el servidor proxy, no por tu enlace de Internet, eso hace que el proveedor de tu servicio a Internet (ISP) no sepa a qué destinos de Internet te estás dirigiendo.

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 del proxy.

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.

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.

Tipos de Proxy existentes.

Ahora bien, hay que tener en cuenta que existen diferentes tipos de proxys. Vamos a ver cuáles son los más comunes.

Proxy Web

Es el proxy que procesa las peticiones del cliente cuando intenta acceder a un sitio web. És el que hemos explicado en el esquema anterior.

Proxy Cache

Realiza casi las mismas funciones que el proxy web. Hace cache de las páginas que ya ha visitado cualquier cliente para servirlas directamente de los archivos que tiene guardados. Evita realizar peticiones de contenido que ya tiene guardado en cache.

Proxy Transparente

Son proxy que no hay que configurarlos directamente en el navegador web. Estos se aplican a nivel de red y no hace falta configurar nada en el cliente. Normalmente los utilizan los ISP para el filtrado de webs, entre otras funcionalidades.

Proxy Inverso

Realiza la función de un proxy web, pero de manera inversa. En este caso el proxy recibe todas las peticiones de muchos clientes y los entrega a un servidor. Se utiliza para proteger servidores web de ataques DDoS, hacer balanceos de carga, entre otras funciones.

Proxy NAT

Es un proxy a nivel de capa OSI más bajo. Se utiliza básicamente para enmascarar, ocultar o cambiar las IPs origen por una sola IP origen antes de realizar las peticiones.

Proxy abierto

Estos tipos de proxies están abiertos a todo tipo de conexiones y cualquier usuario puede utilizarlos. Si utilizas un servicio así, puede que los servidores te bloqueen porque detecten que están realizando SPAM, ya que no controlan quien se conecta.