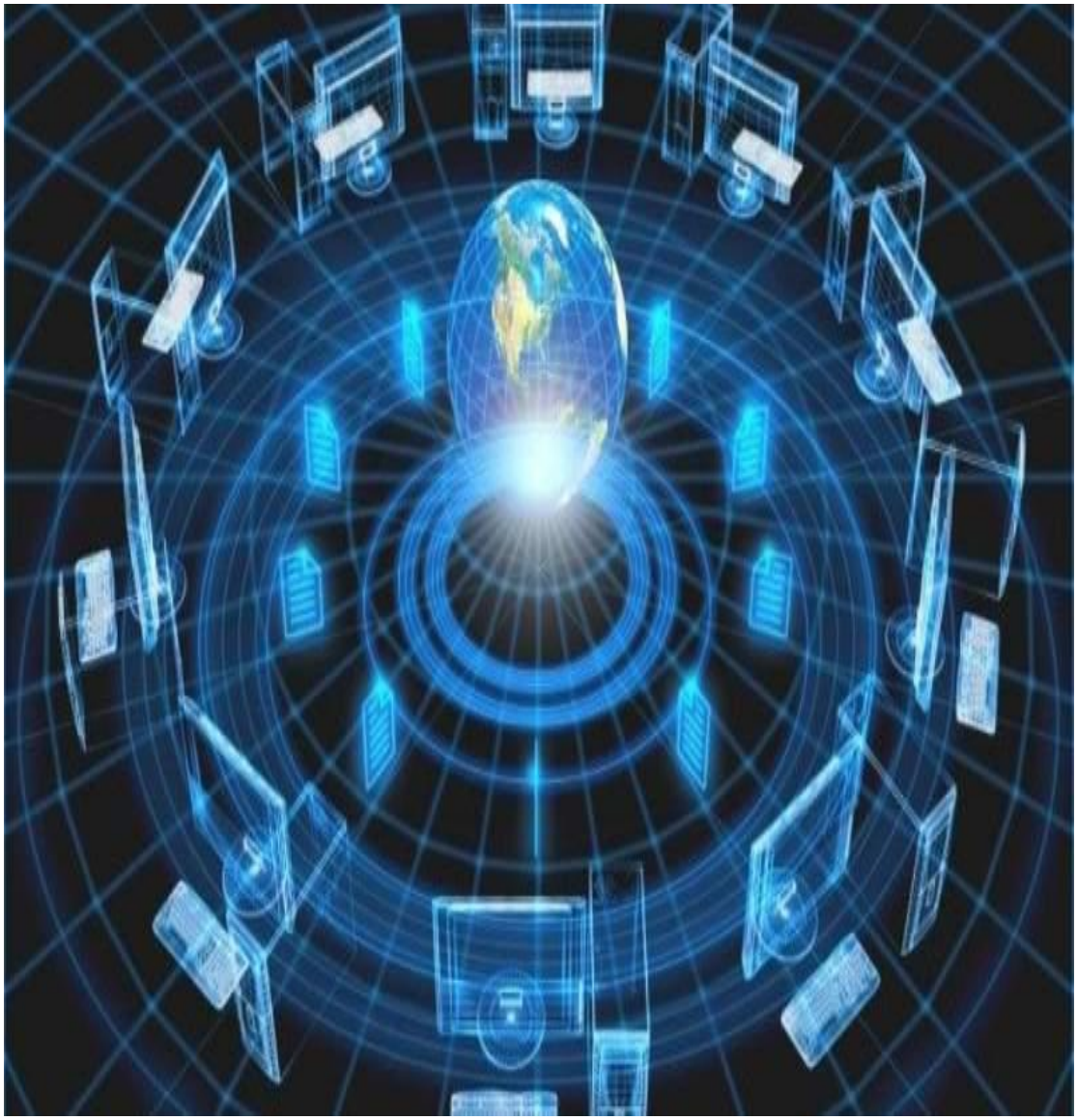

Investigar los tipos de proxy

IBARRA SABIDO JOSE MARIA | Fundamentos de Telecomunicaciones | 12-11-2020

¿Qué es un servidor proxy y qué significa?

Un servidor proxy es un equipo informático que actúa de intermediario entre un cliente de Internet y otro servidor. Es decir, cuando un usuario navega a través de un proxy, no se conecta directamente al servidor en el que se encuentra la información, sino que solicita el contenido a dicho intermediario, el cual se dirige al servidor principal y, posteriormente, devuelve la respuesta al cliente.

Por ejemplo, imaginemos un cliente A, un proxy B y un servidor C. A desea acceder a un recurso que hay en internet, como un sitio web, que está alojado en C. Al emplear un proxy, A le hará la petición a B y será B el encargado de trasladar esa solicitud a C. Más tarde, B le devolverá a. A la información pedida después de haberla obtenido de C. Por consiguiente, no existe una conexión directa entre el usuario y el servidor, y éste último desconoce el cliente que ha realizado la demanda.

Dentro de los servidores proxy, podemos hacer una distinción entre local o externo:

Proxy local. Integrado en el mismo ordenador que el cliente emplea para hacer sus peticiones, se utiliza para que el usuario mismo controle el tráfico y establezca reglas de filtrado de información.

Proxy externo. Situado en otra computadora diferente a la del cliente, se emplea para el bloqueo de contenidos o el control del tráfico, entre otros.

¿Para qué sirve un proxy?

Las funciones de un proxy se centran en controlar el acceso a Internet, registrar el tráfico y restringirlo en algunos casos, filtrar la información, mantener el anonimato de los clientes y mejorar el rendimiento de la red gracias al caché integrado. A continuación, detallamos cada una de ellas:

Controlar el acceso a Internet, ya que es el proxy el que realiza el trabajo real y, por tanto, puede incluso limitar los derechos de los usuarios y proporcionar permisos de forma discriminada.

Registrar el tráfico, que permite saber qué uso le dan los usuarios a la red. Esto es muy útil, por ejemplo, para conocer qué hacen los empleados de una empresa en Internet. Además, también es capaz de restringir el tráfico a determinados clientes.

Filtrar la información para no responder a aquellas solicitudes que el proxy detecte que están prohibidas o son peligrosas, como un malware. En este sentido, puede revisar, asimismo, el contenido que sale con el fin, por ejemplo, de evitar robo de información.

Mantener el anonimato de los clientes, pues el servidor final no conoce quién está haciendo la petición. Este aspecto incrementa la seguridad en Internet.

Mejorar el rendimiento de la red, gracias a la memoria caché que integra el proxy. En concreto, el contenido demandado por un usuario es almacenado en caché y, si vuelve a ser solicitado más tarde, el proxy se pone en contacto con el servidor principal y comprueba la posible modificación de la información desde la última petición. En caso de que haya permanecido inalterada, devuelve la respuesta desde su caché.

¿Cómo configurar un proxy?

La configuración de un servidor proxy varía en función del navegador utilizado por el usuario. Por este motivo, en ValorTop hemos escogido los tres principales: Internet Explorer, Mozilla Firefox y Google Chrome.

Internet Explorer. El usuario debe dirigirse a la sección de "Herramientas" del navegador y entrar en "Opciones de Internet". Una vez ahí, ha de situarse en la pestaña "Conexiones" y seleccionar "Configuración de LAN". Posteriormente, en los campos "Dirección" y "Puerto" tiene que introducir los datos correspondientes al proxy al que desea conectarse y, finalmente, deseleccionar todas las opciones menos "Usar un servidor proxy para la LAN [...]".

Google Chrome. Este navegador hace uso del proxy del sistema Internet Explorer, por lo que las instrucciones son las mismas que las explicadas anteriormente.

Mozilla Firefox. El navegante debe entrar en "Herramientas" y, seguidamente, en "Opciones", donde ha de pulsar el botón "Avanzado". Después, se selecciona la pestaña "Red" y, dentro de ella, "Configuración". En esta ventana es donde se introducen los datos de "Dirección" y "Puerto" del proxy y, para terminar, se hace clic en la opción "usar el mismo proxy para todo".

Tipos de proxy

Un proxy, dada la variada tipología, puede clasificarse de la siguiente forma:

Proxy web: es aquel que se encarga de proporcionar el acceso a la web con los protocolos HTTP y HTTPS. Se pueden emplear para reducir el tráfico, mejorar la seguridad, optimizar la velocidad de navegación y fortalecer el anonimato.

Proxy inverso: se encuentra en el alojamiento de uno o de más servidores web y se emplea, principalmente, por aquellas páginas y sitios web que desean controlar el tráfico, ya que este proxy controla a todos los usuarios que van a entrar en todos los servidores web a él vinculados.

Proxy NAT: su actividad se centra en la traducción y sustitución de las direcciones fuente o destino de los paquetes IP. Es decir, se encarga de traducir las direcciones privadas que emplean los usuarios en una única dirección pública, necesaria para el desarrollo de las solicitudes y la distribución de la información en función de las demandas.

Proxy transparente: su principal característica es que no requiere una configuración del navegador y, por tanto, los usuarios pueden desconocer su existencia. En especial, es empleado por las empresas para controlar el uso de Internet que hacen sus empleados, ya que incluso puede restringir el acceso a determinados sitios.

Proxy abierto: este intermediario acepta las peticiones que se hacen desde cualquier computadora, se encuentre o no conectada a su red.

Ventajas e inconvenientes de un proxy

Los puntos fuertes de estos servidores intermediarios son una mayor seguridad de Internet, anonimato de los usuarios, menor tiempo de configuración, mejor control por ser el proxy el que realiza todo el trabajo real, más velocidad de respuesta gracias al empleo de caché y eficiente filtrado de la información para esquivar aquellos contenidos prohibidos o peligrosos.

No obstante, un proxy también puede presentar algunas desventajas. Entre ellas, las más destacables son la carga de trabajo que acumula por la gran cantidad de usuarios, la posible intromisión entre un servidor y cliente cuando éste no quiere pasar por el intermediario y la probabilidad de existir de no estar actualizado adecuadamente debido a errores de caché.