



TECNOLOGICO
NACIONAL DE MEXICO



*INSTITUTO TECNOLÓGICO DE
CANCÚN*

*INGENIERIA EN SISTEMAS
COMPUTACIONALES*

*FUNDAMENTOS DE
TELECOMUNICACIONES*

INVESTIGACION SOBRE PROXY

Peraza Soberanis Gabriel Alfredo



TECNOLÓGICO
NACIONAL DE MÉXICO



¿Qué es proxy?

Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos. Siendo tú el cliente, esto quiere decir que el proxy recibe tus peticiones de acceder a una u otra página, y se encarga de transmitírselas al servidor de la web para que esta no sepa que lo estás haciendo tú.

Los proxys son utilizados muy a menudo para acceder a servicios que tienen bloqueado su contenido en determinado país. Por ejemplo, si una web no ofrece determinado contenido en tu país, pero sí en otro, haciéndote pasar por un internauta de ese otro país puedes acceder a él.

De esta manera, cuando vayas a visitar una página web, en vez de establecer una conexión directa entre tu navegador y ella puedes dar un rodeo y enviar y recibir los datos a través de este proxy. La página que visites no sabrá tu IP sino la del proxy, y podrás hacerte pasar por un internauta de otro país distinto al tuyo.

Como muchos de estos servicios de proxy bloquean también cookies, scripts y otros objetos que están alojados en las webs, también son útiles para poder navegar de una manera mucho más privada y anónima.

Lo mejor es desconfiar de los proxys web que no pertenezcan a empresas de seguridad o que muestren demasiada publicidad.

Por último, ten en cuenta que lo único que hace un servidor proxy es esconder tu IP. Esto quiere decir que no suelen eliminar ningún otro tipo de identificador adicional que pueda revelar tu identidad, por lo que, aunque tu IP esté oculta, alguien con acceso a tu red y los datos que transmites podría espiar tu tráfico.

Si quieres una seguridad mayor tendrás que ir a por una VPN. Las VPN o redes privadas virtuales se diferencian de los proxys sobre todo en que cifran todo el tráfico que pasa a través de ellas, algo que un proxy no hace. Por lo tanto, al cifrar los datos, aunque tus comunicaciones fuesen interceptadas por una agencia gubernamental u operadora no sería tan fácil obtener tus datos de navegación. Aunque claro, la eficacia de la VPN depende también de cual tengamos.



TECNOLÓGICO
NACIONAL DE MÉXICO



Tipos de servidores proxy web

Normal/Caché: El Web Proxy Caching actúa en el almacenamiento local de páginas web y archivos disponibles en servidores remotos, teniendo en cuenta que busca objetos primero en el sistema de almacenamiento local, ya sea en la memoria o en el disco. Así, al recibir la solicitud, el servidor accede al contenido y lo almacena para su uso futuro. En un próximo acceso, el proxy responde con el contenido almacenado, aumentando la velocidad de respuesta, ya que no se consume banda de internet.

Proxy Transparente: El Proxy Transparente es un modo de uso en el que no es necesario configurar el navegador de cada dispositivo, evitando sobrecargas administrativas. Ubicado entre el cliente y el internet, no requiere que el usuario de la máquina sea consciente de su existencia, pero permite que se lo configure de forma a no permitir el acceso a contenidos no adecuados a la política de uso de la empresa.

Este modelo actúa redireccionando el tráfico de red al servicio proxy, por lo que no puede confundirse con recursos complementarios de descubrimiento automático de proxy, como es el caso del WPAD/PAC. En estos, el proxy no es transparente, sólo el recurso de descubrimiento que se realiza, a menudo, sin la intervención del usuario.

Proxy Anónimo: Este tipo de proxy web permite realizar actividades en Internet de forma anónima. El acceso es realizado por el servicio de proxy, protegiendo la información de IP y ocultando la identificación del ordenador de origen. Es un gran obstáculo para las redes, pues a través de éstos, se hace posible el bypass de políticas de seguridad.

Aunque este tipo de proxy puede ser utilizado con fines legítimos, desafortunadamente la mayoría de los accesos son para burlar las políticas de seguridad existentes en las empresas. Otro aspecto importante es que esto termina siendo una fuente utilizada por criminales y mal intencionados para capturar información sensible de los usuarios.

Mientras el usuario está utilizando el servicio para burlar la seguridad local, puede automáticamente estar exponiendo información que genera un riesgo personal e incluso corporativo. Por lo tanto, mucho cuidado con este tipo de proxy.



TECNOLÓGICO
NACIONAL DE MÉXICO



Proxy reverso: También están los proxys reversos. Puede utilizarse para brindar acceso a Internet a un usuario en concreto dentro de la red, ofrecer algún tipo de caché o incluso actuar como firewall y ayudar a mejorar la seguridad.

Proxy NAT: Una opción más en cuanto a proxys es los proxys NAT. Principalmente se utilizan para enmascarar la identidad de los usuarios. Esconde la verdadera dirección IP para acceder a la red. Cuenta con variadas configuraciones.

En definitiva, estos son los principales tipos de proxys que podemos encontrarnos. Como vemos hay una variedad de opciones y cada uno de ellos puede tener un uso diferente de cara a los usuarios. Todos ellos actúan como intermediarios entre el usuario (dispositivo móvil, ordenador...) y un servidor. Pueden ayudar para mejorar la seguridad y privacidad, así como para obtener diferentes funciones a la hora de navegar por la red.