



**Nombre de la materia:
Fundamento de telecomunicaciones**

**Nombre de la licenciatura:
SISTEMAS COMPUTACIONALES**

**Nombre del alumno(a):
ALAN GERARDO GIJON AGOSTO**

**Número de control:
18530390**

Nombre de la tarea: Investigación Proxy

Unidad #: nombre de la unidad:

**Nombre del profesor(a):
ING. ISMAEL JIMENEZ SANCHEZ**

Fecha:



Con la creciente necesidad de proteger nuestros datos ante la constante mirada de los intrusivos ISPs, además de agencias gubernamentales que quieren controlar cada vez más a los ciudadanos, el concepto de proxy ha comenzado a volverse cada vez más popular.

Si bien lo que se llama como servidor proxy popularmente es en realidad una tecnología que tiene décadas existiendo, se ha vuelto cada vez más una necesidad para muchas personas debido a múltiples necesidades relacionadas a la privacidad de los datos.

Algo importante a aclarar, es que un proxy no necesariamente está relacionado con lo que es un VPN, y menos aún con un VPS (algo aclarado en el artículo diferencias entre VPN vs VPS).

¿Qué es un Servidor Proxy?

Cuando nos aproximamos al término servidor proxy nos surgen dos interrogantes: la palabra servidor, como ya todos sabemos, hace alusión a un dispositivo de hardware o bien un software, que es utilizado para servir datos a cliente que le envían peticiones.

Un proxy por el otro lado, es simplemente un software intermediario, es decir, un punto intermedio que permite interconectar dos partes remotas en Internet. Un servidor proxy entonces, es un software o servicio de sistema que corre en un sistema operativo, y permite que una persona se conecte a él, para llegar a un destino X en Internet, o bien obtener información a través del proxy.

¿Cuándo necesito un Servidor Proxy?

Usar un servidor proxy puede depender de muchos factores, desde causas estrictamente ligadas a necesidades tecnológicas, a necesidades de cuidado de la información personal (anonimato). Veamos entonces los diferentes escenarios en los que se necesita un servidor proxy:



- Anonimato: es la razón número uno generalmente por las cuales las personas buscan servidores proxy. Debido a que el proxy impide que el origen se conecte al destino de forma directa vía HTTP/HTTPS, sirve para esconder nuestra dirección IP pública, tanto al navegar, como al realizar conexiones a servicios utilizando otros protocolos de Internet. Es junto con el hosting anónimo uno de los servicios más solicitados por los usuarios a los que les interesa proteger sus huellas en la red.
- Acceder a contenido restringido: si desde tu país no tienes disponible ciertos contenidos de Internet debido a censuras políticas por parte de gobiernos autoritarios (caso de Venezuela, Cuba, etc), lo ideal es usar un servidor proxy externo que te permitirá acceder al contenido sin restricciones.
- Balanceo de carga: este es otro de los motivos por los cuales los usuarios solicitan un servidor proxy, para usarlo como un balanceador de carga y así distribuir las peticiones de los visitantes de una web hacia otros servidores. En este caso, el servidor proxy en realidad se usa como un servidor de balanceo o balanceador de cargas. Sirve además como nodo central para controlar el ancho de banda usado por cada usuario, especialmente en redes corporativas para evitar abusos del uso de la red.
- Cache de recursos: otra de las grandes funciones que tienen los servidores proxy es permitirnos cachear contenido. Esto mejora mucho la respuesta de ciertos recursos que pedimos a Internet, cachándolos y así despachándose mucho más rápido que si establecemos la conexión directa.
- Mitigar ataques DDOS: existen muchas empresas que ofrecen servicios AntiDDOS a través de proxys, de esta forma permiten que una web esté protegida mientras ellos mitigan el ataque malicioso desde el proxy, y dirigen a los visitante legítimos hacia tu sitio web ubicado en el servidor web real detrás del proxy.

Tipos de Servidores Proxy

- Servidor Proxy Web: se trata de un proxy basado en HTTP/HTTPS, donde el usuario accede a este servicio de la web, y desde allí puede usar el servidor proxy web intermediario para navegar por otras URLs. Así el usuario ingresa en el proxy web, indica la URL a donde quiere navegar, y el servidor proxy web devuelve el contenido.
- Servidor Proxy Transparente: un proxy transparente, también llamado proxy forzado, es un servidor que se encuentra como punto intermedio entre tu computadora en una red local, y el Internet. Lo que hace básicamente es tomar tu petición, y darle una redirección hacia el Internet sin modificar nada de ella. Por eso se le llama transparente, porque actúa como intermediario, pero no la modifica, es transparente.
- Servidor Proxy Cache: se trata de un servidor proxy que es utilizado como servidor intermedio entre una red y el Internet para cachear contenido, principalmente contenido de tipo estático como CSS, javascript, imágenes, vídeo o HTML. Esto permite acelerar el despacho de la información cuando los navegantes de la red acceden a Internet.
- Servidor Proxy Reverso o Reverse Proxy: un proxy reverso, o reverse proxy del inglés, es un tipo de servidor proxy que se usa para diferentes necesidades, entre las cuales se incluye: brindar acceso a Internet a usuarios de una red, balanceo de tráfico desde servidores web en el backend o proveer algún tipo de cache o despacho de ciertos archivos como lo son los estáticos.
- Servidor Proxy NAT: cuando hablamos de NAT proxy o proxy no-transparente, nos referimos a un servicio proxy que se usa principalmente para proteger la identidad de las verdaderas conexiones IP que acceden a Internet. Se usa de diferentes formas y con variadas configuraciones, pero la más típica y usada por los usuarios para tener anonimato es la llamada «masquerading», es decir, realizar un enmascaramiento de las conexiones.

Ventajas de un Proxy

Los servidores proxy tienen muchas ventajas, algunas de ellas los hacen una herramienta imprescindible para el trabajo diario de muchas personas:

- Guardar Cache: permiten el uso del servidor proxy como servidor cache, para despachar de forma más rápida ciertos tipos de contenidos en algunas redes donde están presentes. Gracias a esto se logran tiempos de carga de sitios webs realmente rápidos.
- Registro de logs: un servidor proxy permite guardar en sus archivos de datos todos los logs sobre lo que sucede en el tráfico que maneja, sea de entrada o de salida, podrás disponer de logs para ver lo que hacen los usuarios, todas las páginas cargadas por ellos, primeras visitas, re-carga de páginas, etc. En general, podrás ver qué hacen con su conexión a tu red.
- Filtración de sitios: el filtrado de sitios es una de las características más usadas por los servidores proxy empresariales, sobre todo para evitar que los empleados de una institución ingresen a redes sociales o páginas con contenidos que pueda distraerlos de su trabajo diario. También se puede configurar el filtrado para bloquear sitios potencialmente maliciosos que contengan malware o virus.
- Bloqueo de direcciones IP: con la característica del bloqueo de IP podrás bloquear tanto IPs internas de la red como IPs externas que accedan a ella, de esta forma tendrás siempre control sobre quién y cuándo ingresan al servidor proxy de tu red. Podrás aplicar bloqueos temporales o completos, dependiendo de tus necesidades.
- Autenticación: la autenticación es una de las cosas que ayudan muchísimo a mejorar la seguridad del proxy, y es simplemente un mecanismo de seguridad adicional que requiere autenticarte mediante un mecanismo de usuario y contraseña en la mayoría de los casos.
- Limitar el ancho de banda: en la mayoría de las empresas lo que se evita es el uso desbordado de ancho de banda, y para esto el servidor proxy ofrece excelentes características imponiendo límites a la cantidad de conexiones y

ancho de banda que se asigna a cada una de ellas, así evitarás lentitudes innecesarias por parte de una de las computadoras de la red.

- Blacklists: las listas negras, también conocidas como blacklists en inglés, permiten crear un listado de sitios webs maliciosos, de esta forma se evitan tener incidentes de seguridad con sitios que tienen potenciales destructivos, o que no lucen muy confiables.
- Listas Negras. ¿Qué pasa con un sitio web malicioso al que alguien ingresó desde una red proxy?. Bueno, pues se va a la lista negra. Esta lista negra se conforma de todos los sitios a los que no estará permitido ingresar por distintas razones, es administrable y se pueden sacar sitios de ahí para su respectivo acceso, pero por ejemplo. Las redes sociales siempre se encuentran en la lista negra de muchas empresas y Youtube es el segundo que sufre de lo mismo.
- Anonimato: dependiendo de cómo se ofrezcan por el proveedor, pueden llegar a ser completamente anónimos, permitiéndote esconder tu IP de origen, los contenidos que navegas, etc. Aunque esto es un arma de doble filo, cuidado.

Desventajas del Servidor proxy

¿Los servidores proxy tienen algo malo o son tan bellos como parecen? La realidad es que tienen muchas desventajas también:

- Navegación más lenta: si bien por un lado ofrecen mecanismos de cache para acelerar la navegación, lo cierto es que muchas veces se obtiene el efecto contrario y la navegación con un proxy como intermediario lo hace todo mucho más lento, esto depende igualmente del proxy, su configuración, la red y el ISP final que maneja la salida a Internet, pero es cierto que es un escenario muchas veces visto.
- El 90% no son tan anónimos como dicen: esto de que los proxys son 100% anónimos no es tan así, hay muchas creencias de los usuarios que llevan a pensar que nadie podrá saber lo que hacen si usan un proxy, y la verdad es que si bien la IP y navegación se esconde en la mayoría de los casos, lo



cierto es que en casi todos los casos se guardan logs de todo lo que haces, que luego se usan con fines estadísticos, o que pueden llegar a entregarse a autoridades si lo solicitan. Ten cuidado si buscas anonimato, lo mejor en ese caso es que tú mismo crees un proxy, es lo único que te garantizará anonimato.

- Limitaciones de puertos y protocolos: muchas veces al salir a Internet por un proxy hace que no podamos usar muchos puertos o protocolos que usamos comúnmente en nuestras actividades diarias, tenlo en cuenta, estarás supeditado a lo que el proxy te permita hacer de acuerdo a su configuración.
- Cuidado con acceder a áreas privadas: si contratas cualquier proxy en Internet, no deberías usar usuarios y contraseñas, pues no sabes qué datos están guardando desde el proxy, incluso si todo está supuestamente encriptado por certificados de seguridad SSL. En los servidores proxy empresariales no suele pasar, pero igualmente cuidado por si acaso.

¿Cuál es el mejor servidor proxy para Linux?

Existen muchísimos tipos de servidores proxy que corren en servidores Linux (los recomendados por estabilidad y seguridad). Aquí te dejamos una lista de los más conocidos y que te recomendamos instalar en servidores Linux.

- Squid: probablemente el servidor proxy más conocido de la historia, soporta múltiples protocolos como HTTP, HTTPS, FTP, IMAP, SMTP, etc, además de cache, límite de conexiones, ancho de banda, etc.
- Polipo: este servidor proxy para Linux es realmente pequeño, pero a la vez poderoso. 100% software de código abierto, admite protocolos HTTP y DNS. Tiene una interfaz web para configurarlo, y puede usarse para filtrado y cache.
- Tiny Proxy: servidor proxy muy fácil de instalar con múltiples configuraciones, admite protocolos HTTP y HTTPS. Ofrece acceso a recursos restringidos, caching, interfaz web, bloqueo de IP, etc.



- Exa Proxy: a diferencia de los anteriores, este servidor proxy no está diseñado para el almacenamiento de cache, sino para filtrado de tráfico, blacklists y más, ofrece una GUI intuitiva.

Tipos de proxy

Existen muchos tipos de proxies y cada uno realiza unas funciones determinadas. A continuación os listamos y explicamos brevemente cada uno de ellos:

- Proxy Web

Es el proxy que procesa las peticiones del cliente cuando intenta acceder a un sitio web. Es 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.

Bibliografía:

<https://www.moving-it.net/proxy-que-es-un-proxy-tipos-de-proxy/>

<https://blog.infranetworking.com/servidor-proxy/>