Engineer

proxy

servidor que reenvía una petición en su nombre

Qué es

Un proxy es un programa situado entre un cliente y el servidor al que quiere llegar. Acepta la petición del cliente, hace su propia petición a la siguiente máquina y devuelve la respuesta. El cliente habla con el proxy y el proxy habla con el servidor, de modo que los dos extremos nunca comparten una conexión. Hay varios tipos de proxy, y la pregunta útil para cada uno es quién lo ha colocado ahí.

La propia especificación de HTTP, RFC 9110, distingue tres intermediarios habituales. Un proxy en sentido estricto es uno elegido por el cliente, normalmente mediante una configuración local, como un ajuste del navegador o una variable de entorno. Una pasarela, que el RFC también llama proxy inverso, se sitúa del lado del servidor: ante quien se conecta se comporta como el servidor de origen, mientras reenvía cada petición hacia uno o varios servidores que tiene detrás. Un túnel retransmite bytes entre dos conexiones sin interpretarlos y, una vez abierto, deja de participar en la conversación. El cliente lo solicita con el método CONNECT, indicando un host y un puerto, y después establece TLS de extremo a extremo a través de él. El RFC añade un cuarto tipo que nadie ha elegido: el proxy de interceptación, a menudo llamado proxy transparente, que redirige el tráfico saliente por el puerto 80 en el límite de una red, como hacen los puntos de acceso públicos y los cortafuegos corporativos.

Cada salto es una conexión independiente. El diagrama del RFC coloca tres intermediarios entre un navegador y un servidor de origen, lo que da cuatro conexiones, y ajustes como keep-alive o un tiempo de espera se aplican a una de esas conexiones cada vez. HTTP también exige que el proxy se identifique: debe añadir un campo de cabecera Via a cada mensaje que reenvía, y así es como un bucle o un intermediario inesperado aparece en una traza.

HTTP es solo una capa. Un proxy SOCKS, cuya versión 5 se especifica en el RFC 1928 de marzo de 1996, retransmite conexiones TCP y datagramas UDP sin leer su contenido, de modo que cualquier protocolo puede utilizarlo. Tor es un ejemplo conocido: de forma predeterminada escucha en el puerto 9050 las conexiones SOCKS de las aplicaciones locales.

Utilice el concepto en una decisión

Aplique «¿Qué es un proxy?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Wi-Fi, cortafuegos y acceso remoto configurados para trabajar desde cualquier lugar y permitir el acceso solo a las personas autorizadas.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. Administración de 30 VPS Ubuntu Linux — 30 servidores Linux administrados con recuperación planificada

Administración de 30 VPS Ubuntu Linux Póngase en contacto →

Por qué importa

Quien opera el proxy puede leer el tráfico. Con HTTP sin cifrar, eso significa todas las cabeceras y todos los cuerpos. A través de un túnel CONNECT ve el nombre del host y el puerto; el resto es TLS entre el cliente y el servidor. Un proxy inverso que termina TLS lo ve todo sin cifrar, y esa es su función, porque tiene que leer la petición para dirigirla. Por tanto, poner delante de un sitio el proxy inverso de otra empresa, que es lo que hace una red de distribución de contenidos, entrega a esa empresa la dirección de cada visitante y cada URL antes de que las vea el propio sitio. Puede ser una contrapartida adecuada para una tienda que sufre un ataque. Sigue siendo una decisión sobre privacidad, y la página de privacidad debería explicarla.

La segunda consecuencia es lo que averigua el servidor. El RFC 7239 explica la pérdida con claridad: detrás de un proxy, las peticiones parecen proceder de la dirección del proxy. Un registro, un límite de frecuencia, una lista de bloqueo o una lista de permitidos basada en la dirección del cliente ve entonces una única dirección para todo el mundo. La solución habitual es una cabecera que transmite la dirección original: el campo estándar Forwarded del RFC 7239 o el anterior X-Forwarded-For. La mayor parte de los problemas empieza al decidir en qué copia de esa cabecera confiar.

En tercer lugar, un proxy cambia el significado de un error. Un intermediario genera un 502 Bad Gateway o un 504 Gateway Timeout para informar sobre el servidor que tiene detrás: el proxy recibió una respuesta no válida o no recibió

ninguna a tiempo. Un 407 significa que el propio proxy exige credenciales antes de reenviar nada. Saber qué máquina generó el error es la mitad del diagnóstico.

En cuarto lugar, muchos proxies usan caché. El RFC 9111 llama caché compartida a la que guarda respuestas para más de un usuario, normalmente como parte de un intermediario. Hace que servir un sitio sea más rápido y barato, y también es el lugar donde una respuesta destinada a una persona puede llegar a otra.

Cómo se aplica en la práctica

En agosto de 2026, la empresa trasladó al repositorio su zona DNS de unos veinte registros y la concilió con la API de Cloudflare. Enviar el tráfico web a través de la CDN del proveedor como proxy inverso formó parte de ese trabajo, y después se desmontó por privacidad un proxy CDN que ya funcionaba delante del sitio. La objeción era su posición: la dirección de cada lector y cada ruta solicitada llegarían primero a un tercero, y para una empresa que dice a sus lectores que nadie los observa, eso pesaba más que la protección frente a ataques que proporcionaba.

Contar lectores a partir del registro de acceso que ya mantiene el servidor web, al mes siguiente, exigió tratar con proxies que la empresa no opera. El registro de acceso descarta siete cabeceras que transmiten la dirección de un cliente antes de escribir una línea. El codificador del registro copia las cabeceras sin cambios, de modo que, sin ese paso, se habría guardado la dirección sin enmascarar de un lector situado detrás de un proxy corporativo bajo un nombre de cabecera que la regla de enmascaramiento no contemplaba.

Cuando el sitio incorporó un espejo onion en Tor ese mismo mes, se desactivó en la configuración el puerto proxy del propio demonio Tor para el tráfico saliente. Se accede al servicio onion mediante circuitos que el demonio establece hacia fuera, por lo que publicar este espejo no requiere un puerto de Internet entrante adicional. Al tener desactivado su puerto de escucha SOCKS, este demonio Tor no ofrece un proxy de salida a las aplicaciones locales.

Dónde surgen los problemas

Todas las peticiones del registro proceden de la misma dirección. La aplicación está detrás de un proxy inverso y registra la dirección de la conexión que recibe, que es la del proxy. Un límite de frecuencia restringe entonces a todo el mundo a la vez, y un bloqueo generado por una herramienta de detección de intrusiones

bloquea el proxy, es decir, a todos los lectores. Haga que el proxy transmita la dirección del cliente en una cabecera y configure la aplicación para leer esa cabecera solo en conexiones procedentes de la propia dirección del proxy. En nginx, esa función corresponde a la directiva set_real_ip_from del módulo realip; la mayoría de los frameworks web tiene un ajuste equivalente de proxies de confianza.

Un cliente elige su propia dirección enviando una cabecera. La aplicación lee X-Forwarded-For en todas las peticiones, incluidas las que llegan directamente y las que ya traen un valor falsificado en la cabecera. El RFC 7239 especifica que cualquier nodo del recorrido, incluido el cliente, puede modificar el campo. Confíe únicamente en las entradas que haya añadido su propio proxy, contando desde la derecha, y haga que la aplicación escuche en la interfaz de bucle local o en una red privada para que el proxy sea la única vía de entrada.

El registro que se pretendía anonimizar conserva las direcciones completas. La dirección del cliente está enmascarada en el campo que alguien comprobó, pero la misma dirección viaja en Forwarded, X-Forwarded-For, X-Real-IP y cabeceras similares, y un sistema de registro que escribe el mapa de cabeceras tal como lo recibe las guarda completas. Enumere todas las cabeceras que puedan contener una dirección, descarte o enmascare cada una en el momento de escribir la línea y después envíe una petición de prueba y lea la línea en disco.

Las páginas devuelven 502 o 504 mientras el registro del backend no da señales del problema. El error lo ha generado el proxy. Un 502 significa que recibió una respuesta no válida: el backend estaba caído, escuchaba en otro puerto o hablaba HTTP sin cifrar donde el proxy esperaba TLS, o al revés. Un 504 significa que el backend tardó más que el tiempo de espera de lectura del proxy, que nginx fija de forma predeterminada en 60 segundos. Lea primero el registro de errores del proxy, porque identifica la dirección upstream a la que intentó acceder, y aumente el tiempo de espera solo para las rutas que se sabe que son lentas.

Un usuario ve la página de otro. Una caché compartida en un proxy o una red de contenidos guardó una respuesta personal, como una página de cuenta devuelta junto con una cookie de sesión, y la sirvió a la siguiente persona que pidió la misma URL. Marque cada respuesta específica de un usuario con Cache-Control: private; según el RFC 9111, una caché compartida no debe almacenar esa respuesta. Use no-store cuando no deba conservarse ninguna copia en ningún lugar y compruebe las cabeceras que devuelve realmente el proxy.

Lecturas adicionales

- RFC 9110, sección 3.7: intermediarios — Las definiciones de proxy, pasarela, túnel y proxy de interceptación.
- RFC 9110, sección 9.3.6: CONNECT — Cómo solicita un cliente al proxy que abra un túnel a un host y un puerto.
- RFC 7239: extensión HTTP Forwarded — La cabecera estándar para la dirección original del cliente, con sus advertencias.
- RFC 9111: almacenamiento en caché de HTTP — Cachés compartidas y privadas, y las directivas que las separan.
- RFC 1928: protocolo SOCKS versión 5 — El proxy independiente del protocolo que retransmite conexiones TCP y datagramas UDP.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es un proxy?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por **D.**

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/proxy/