Engineer

Proxy inverso

← servidor que recibe peticiones para un servicio web

Qué es

Un proxy inverso es un servidor que recibe peticiones en nombre de un servicio web. El navegador se conecta a la dirección pública, donde escucha el proxy. Este elige el servidor de origen al que reenviar la petición y entrega al navegador la respuesta que recibe. El servicio puede cambiar de máquina, de puerto o de dirección interna mientras los enlaces públicos siguen funcionando. El estándar de HTTP llama pasarela a este papel. Un proxy directo representa al cliente cuando este necesita contactar con otros destinos. El operador del sitio coloca el proxy inverso delante del servicio que ofrece.

Imagina una aplicación que carga la portada desde un servicio y el informe de `/api/informes/42` desde otro. El navegador pide ambos recursos al mismo dominio. El proxy puede leer la ruta de una petición HTTP y decidir a qué servicio enviarla. Si varias instancias pueden servir el mismo informe, el proxy también puede repartir entre ellas las peticiones. Esa tarea es el balanceo de carga. Una sola aplicación detrás del proxy ya permite separar su dirección interna del nombre que conocen los usuarios.

Algunos productos permiten pasar una conexión TCP cifrada directamente a otro servidor. Esta modalidad puede tomar decisiones con datos de la conexión o con campos visibles al iniciar TLS, cuando esos campos están disponibles. Para decidir por una ruta HTTP cifrada el componente necesita acceder al mensaje HTTP. Un diagrama útil identifica el punto donde termina la sesión TLS del navegador y muestra si empieza otra conexión cifrada hacia el origen.

Utilice el concepto en una decisión

Aplique «¿Qué es un proxy inverso?» 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

La entrada pública da al equipo un lugar donde decidir qué servicios quedan al alcance de los visitantes. El proxy puede gestionar el certificado del dominio, mientras que los servidores de aplicación solo admiten conexiones por una red privada. La entrada también puede aplicar límites de tamaño, gestionar redirecciones y registrar las peticiones. Cada ruta merece reglas adecuadas a su uso. Una carga de archivos requiere prever el tamaño de los cuerpos de petición, mientras que un flujo de eventos puede necesitar enviar cada parte de la respuesta sin acumularla.

El proxy forma parte del perímetro de confianza. Cuando termina la conexión TLS, puede ver lo que transmite, incluidas cookies, parámetros y datos enviados por el usuario. Una segunda conexión cifrada protege el tráfico de camino al servidor de origen. Su contenido sigue siendo accesible para quien administra el punto que lo descifra. Antes de describir cómo trata los datos un sitio, conviene decidir quién opera el proxy, qué registra y quién puede consultar esos registros.

El componente adicional también cambia el diagnóstico de errores. Una pasarela puede responder con `502` cuando recibe una respuesta inválida y con `504` cuando otra instancia tarda demasiado en responder. La aplicación puede generar sus propios errores. Busca la misma petición controlada en los registros de ambos lados. Anota qué estado devolvió cada uno y cuánto esperó. Si el origen no tiene constancia de la petición, investigar solo el código que atiende esa ruta difícilmente explica el fallo.

Cómo se aplica en la práctica

En su caso sobre la conciliación de la zona DNS como código, Engineer ApS documenta un proxy de CDN que llegó a funcionar y luego se desactivó. Al enviar el tráfico por la red del proveedor, este podía tratar la dirección de cada visitante y la URL solicitada antes que la propia empresa. En ese caso, la empresa dio más peso a la privacidad que a la protección adicional contra ataques. La zona DNS siguió disponible para control de versiones y auditoría. El ejemplo permite evaluar por separado quién resuelve un nombre y quién recibe la petición web.

En un entorno de pruebas, empieza por `/health` y `/api/informes/42?vista=resumen`. Anota el método y la ruta que recibe la aplicación. Comprueba la respuesta que ve el navegador y el esquema y el nombre de host de las redirecciones. Después cambia la dirección privada del servidor de informes y repite las dos peticiones al nombre público. Así se comprueba que los usuarios pueden seguir usando sus enlaces cuando cambia la infraestructura interna.

Abre dos sesiones con cuentas de prueba distintas antes de activar una caché compartida. Haz que cada cuenta reciba una marca inocua que la identifique y verifica qué respuesta llega en cada sesión. Por último, detén el servicio de origen deliberadamente en el entorno de pruebas. Mide cuánto tarda la respuesta de error y confirma que sabes encontrarla en los registros. Tendrás un ejemplo reproducible de cómo se manifiesta ese fallo.

Dónde surgen los problemas

Una petición procedente de Internet puede incluir su propia cabecera `Forwarded` o `X-Forwarded-For`. La aplicación necesita conocer los intermediarios de confianza antes de usar la dirección indicada en una cabecera. Elimina o sustituye los valores sin verificar al recibirlos y limita las conexiones directas al origen a los emisores previstos. Prueba con una dirección falsa. Revisa qué valor queda anotado y qué dirección emplea de verdad la aplicación para decidir permisos.

A veces las primeras señales son un bucle de redirección o un enlace que incluye un puerto interno. El navegador se conectó por HTTPS, pero la aplicación tomó el esquema de su conexión inmediata y construyó otra URL. Proporciona a la aplicación el esquema y el nombre público verificados y recorre el proceso completo de inicio de sesión. Comprueba enlaces de retorno y cookies. Si el proxy quita un prefijo de la ruta, prueba una ruta anidada con parámetros para observar exactamente qué cambió.

Un reintento tras un tiempo de espera agotado puede duplicar una operación. La aplicación podría registrar un pago antes de que la pasarela deje de esperar. Define cómo se reconocen las repeticiones antes de permitir reintentos automáticos en operaciones que cambian datos. En un entorno de pruebas, retrasa la respuesta una vez completada una operación controlada. Comprueba qué punto cierra la conexión y si los registros permiten saber qué intento realizó el trabajo.

Lecturas adicionales

- RFC 9110 sobre intermediarios HTTP define las funciones de proxy, pasarela y túnel.
- RFC 7239 sobre Forwarded describe la cabecera y sus implicaciones para la seguridad y la privacidad.
- Módulo HTTP de proxy de NGINX detalla las rutas, las cabeceras y los tiempos de espera.
- Directiva reverse_proxy de Caddy documenta la selección de servidores y el tratamiento de cabeceras reenviadas.
- Guía de proxy inverso de Apache HTTP Server muestra cómo una entrada pública sirve varias aplicaciones.

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 inverso?» 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/reverse-proxy/