Engineer

Tor

Red que dirige el tráfico por repetidores de voluntarios

Qué es

Tor oculta quién se comunica con quién a quienes observan la red: hace pasar cada conexión por una cadena de máquinas para que ninguna conozca tanto el origen como el destino del tráfico. La cadena la elige el cliente, un programa llamado tor que se ejecuta en el propio ordenador del lector, y suele tener tres repetidores: uno de entrada, o guard, que el cliente reutiliza como acceso; uno intermedio; y uno de salida, que realiza la conexión final con el destino. El cliente construye ese circuito tramo a tramo y acuerda una clave distinta con cada repetidor; después envuelve cada fragmento de datos en una capa de cifrado por tramo. Cada repetidor elimina su propia capa y solo conoce al vecino anterior y al siguiente. Esas capas anidadas son la cebolla del título del artículo de diseño, The Second-Generation Onion Router. En el uso habitual, el conjunto de repetidores es la red Tor, tor en minúsculas es el programa y Tor Browser es el navegador preparado para utilizarlo.

Los datos viajan en celdas de tamaño fijo, de modo que un repetidor ve un flujo de bloques uniformes en lugar de la forma de los paquetes originales. Varios flujos TCP pueden compartir un circuito cuando sus requisitos de aislamiento son compatibles. El cliente construye circuitos tanto de antemano como bajo demanda y los retira según su antigüedad y uso; un flujo duradero puede permanecer en su circuito original, y algunas opciones de aislamiento permiten reutilizarlo durante más tiempo. Las aplicaciones acceden al cliente mediante un proxy SOCKS local y por esa vía solo viaja TCP; el artículo de diseño indica expresamente que no encapsula protocolos como UDP. Los repetidores los operan voluntarios, y cada uno publica un descriptor con sus claves, dirección, ancho de banda y política de salida; un pequeño grupo de autoridades de directorio vota cuáles incluir y firma el resultado como documento de consenso, que cada cliente obtiene antes de elegir una ruta.

Utilice el concepto en una decisión

Aplique «¿Qué es Tor?» 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

Para quien opera un sitio web público, Tor es, ante todo, algo que debe tener en cuenta sobre su público. Un lector que llega por Tor parece proceder de la dirección de un repetidor de salida en lugar de la suya, y la lista de repetidores es pública por diseño, porque cada cliente la necesita para elegir una ruta. Por tanto, un sitio puede reconocer el tráfico de Tor y tratarlo de otra manera. La posición del propio Tor Project es que los operadores tienen derecho a bloquearlo, aunque espera que no lo hagan. La decisión pendiente es qué hacer con esos lectores: atenderlos como a los demás, ralentizarlos, presentarles un desafío o darles una entrada que nunca abandone la red Tor, que es lo que ofrece una dirección onion.

Conviene precisar lo que promete Tor, porque su artículo de diseño enumera lo que queda fuera. No afirma derrotar a un observador que pueda vigilar ambos extremos de una conexión y comparar tiempos y volúmenes, y la documentación del proyecto añade que los investigadores no conocen ningún diseño práctico de baja latencia que lo consiga de forma fiable. El protocolo básico no oculta el propio uso de Tor; los puentes con transportes conectables añaden formas de disimular ese tráfico. Además, Tor no cifra el último tramo, desde el repetidor de salida hasta el destino: la aplicación necesita su propio cifrado para ese tramo.

Frente a una VPN, la confianza se distribuye de otra forma. Un proveedor de VPN ve tanto al usuario como el destino y se le pide que no mire. En Tor ningún repetidor ve ambos. En la mayoría de las rutas, las reglas de selección separan los repetidores de una misma familia declarada y evitan por defecto que compartan una subred IPv4 /16 o IPv6 /32; existen excepciones documentadas y límites de subred configurables. El precio es la latencia, ya que un circuito de salida normal atraviesa tres máquinas de voluntarios, por lo que las páginas ligeras que necesitan pocos viajes de ida y vuelta atienden mejor a quienes leen por Tor.

Ofrecer una dirección onion requiere un proceso tor y una clave privada que proteger, pero ningún puerto de entrada abierto, por lo que encaja en infraestructuras pequeñas.

Cómo se aplica en la práctica

El sitio de la empresa puede leerse por Tor. La página de línea de comandos publica la dirección onion junto a un comando `curl` que obtiene el texto Markdown mediante un cliente tor local. La dirección utiliza deliberadamente `http://` : una dirección onion de versión 3 codifica la clave pública de identidad del servicio junto a una suma de comprobación y un byte de versión. Tor autentica el servicio y cifra el circuito antes de que empiece HTTP. Para esa autenticación mediante la dirección onion no hace falta un certificado web público.

Un servicio onion necesitaba espacio para un proceso tor en el host de servicios públicos de la empresa de septiembre de 2026: un solo núcleo con unos 464 MB de memoria utilizable que ya terminaba TLS para siete dominios y ejecutaba un servidor de repositorios git. El espacio para ese proceso se midió en lugar de debatirse, durante un día registrado de muestras en aquel host de 512 MB: la menor cantidad de memoria disponible observada fue de unos 310 MB de los 464, el uso de swap fue del 2,6 % y el procesador estuvo inactivo el 99,7 % del tiempo, así que Tor se añadió junto a lo demás.

El aviso de privacidad recoge la decisión de la empresa sobre contar lectores. Las aplicaciones Gemini y Gopher no mantienen registros de acceso, y sus contadores diarios solo registran el total agregado de solicitudes. Gopher también tiene un registro de conexiones del sistema operativo que contiene la dirección de origen; ese registro se elimina a los 30 días. En Tor, la empresa declara que no cuenta nada y no ofrece ninguna opción para activarlo. Es una decisión de privacidad del operador: Tor oculta la dirección de red de un lector, pero no impide que un servicio cuente solicitudes. El aviso dice que la empresa prefiere no saberlo a poder averiguarlo.

Dónde surgen los problemas

El nombre se resuelve fuera de Tor. Un programa que envía sus conexiones a un proxy SOCKS puede resolver antes el nombre de host por su cuenta mediante el resolvedor habitual, y esa consulta revela a la red local y al proveedor de DNS qué sitio se está visitando. La conexión viaja después por Tor, pero el destino ya se ha

filtrado. En `curl` la diferencia está en una sola opción: con `--socks5` el nombre se resuelve localmente; con `--socks5-hostname` se entrega al proxy y lo resuelve el repetidor de salida.

```
# Resolves the name locally, then connects through the proxy
curl -s --socks5 127.0.0.1:9050 https://example.org/
# Hands the name to tor; the exit relay looks it up
curl -s --socks5-hostname 127.0.0.1:9050 https://example.org/
```

Texto sin cifrar después de la salida. Tor cifra los tramos entre repetidores, pero no el último. El repetidor de salida abre una conexión TCP normal con el destino y envía lo que le haya dado la aplicación, por lo que un formulario de acceso enviado mediante HTTP sin cifrar puede leerlo tanto el operador de ese repetidor como cualquiera que esté en la red a partir de él. Sirva mediante HTTPS todo lo que salga de la red Tor. Un servicio onion evita el problema porque su tráfico nunca sale de ella.

Una dirección representa a muchos lectores. Los límites de frecuencia y los bloqueos basados en la dirección del cliente tratan a un repetidor de salida como un solo visitante, aunque muchas personas lo utilicen a la vez. Un límite ajustado para una persona deja fuera a todos aquellos cuyo circuito termine allí, y un bloqueo provocado por un usuario que abusa del servicio recae sobre todos. Decida expresamente cómo tratar las direcciones de salida, en lugar de dejarlo en manos de una regla genérica por dirección.

La identidad viaja dentro del circuito. Tor oculta la dirección de red y no interviene en lo que dice la aplicación. Iniciar sesión en una cuenta personal, una configuración de navegador distintiva o un documento que obtiene algo al abrirse vinculan la sesión con una persona, por muchos repetidores intermedios que haya. La documentación del proyecto señala que sigue siendo necesario eliminar información identificativa del tráfico de las aplicaciones en el lado del usuario; de eso se ocupa Tor Browser, a diferencia de un navegador normal configurado para utilizar el proxy.

Un repetidor de salida en una conexión doméstica. Los repetidores de entrada e intermedios rara vez reciben denuncias por abusos. Es en el de salida donde los destinos ven que se origina el tráfico, así que las denuncias y alguna consulta legal llegan a quien lo opera, y la guía de repetidores de Tor Project indica que no

debe operarse uno desde casa. Un voluntario con una única dirección doméstica puede operar un puente: un repetidor no incluido en el directorio público que la misma guía recomienda para esa situación.

Se espera que UDP funcione. Las llamadas de voz, muchos juegos y las herramientas que envían sus propias consultas DNS dependen de UDP, y Tor solo transporta flujos TCP. Esos programas no funcionan a través de él, y uno que no esté obligado a pasar por el proxy puede conectarse directamente fuera de Tor sin avisar.

Lecturas adicionales

- Especificaciones de Tor — especificaciones del protocolo, la selección de rutas, el directorio y los servicios onion reunidas en un lugar.
- Tor: The Second-Generation Onion Router — artículo de diseño: circuitos, celdas, políticas de salida y lista explícita de lo que el diseño no pretende conseguir.
- Especificación de rutas de Tor — cómo elige un cliente sus repetidores de entrada, intermedio y de salida, y qué repetidores no pueden compartir una ruta.
- Tipos de repetidores de la red Tor — repetidores de entrada, intermedios, de salida y puentes, con la exposición legal que supone cada uno para su operador.
- Cifrado HTTPS y Tor — vista interactiva de lo que ve quien escucha el tráfico con Tor, con HTTPS, con ambos y sin ninguno.

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 Tor?» 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/tor/