Engineer

Servicio onion

dirección que solo funciona a través de Tor

Qué es

Un servicio onion es un servidor al que los lectores acceden dentro de la red Tor mediante un nombre construido a partir de la propia clave pública del servidor, en lugar de un nombre DNS que apunte a una dirección IP. A menudo se habla simplemente de un onion; un demonio tor puede ejecutar varios servicios onion en paralelo, y la especificación sigue usando el nombre anterior, servicio oculto.

El nombre consta de 56 caracteres base32 seguidos de `.onion`. Una vez decodificado, ocupa 35 bytes: la clave de identidad ed25519 de 32 bytes del servicio, una suma de comprobación de dos bytes extraída de un hash SHA3-256 de esa clave y un byte de versión establecido en 3. Como ese byte va al final, todas las direcciones actuales terminan en la letra d. Nadie elige la etiqueta; es la clave expresada por escrito. Los nombres anteriores, de versión 2, tenían 16 caracteres extraídos de un hash SHA-1 de una clave RSA-1024, y tor dejó de admitirlos en la versión 0.4.6.1-alpha, en 2021.

Para acceder al servicio hacen falta dos lugares de encuentro. El servicio elige algunos nodos de retransmisión como puntos de introducción, mantiene circuitos abiertos hacia ellos y sube a nodos de directorio un descriptor firmado que los enumera. El descriptor se guarda bajo una clave cegada que cambia en cada período, y su cuerpo está cifrado, por lo que un nodo que lo almacene sin conocer la dirección no puede leer la lista. Un cliente que tenga la dirección obtiene el descriptor, comprueba la firma con la clave del nombre, elige un nodo como punto de encuentro y pide al servicio, a través de un punto de introducción, que se reúna allí. El servicio construye su propio circuito hasta ese nodo y completa la negociación, y el nodo une ambos circuitos. El recorrido cruza seis nodos, tres elegidos por cada lado, y ninguno de los extremos conoce la dirección IP del otro. Un modo opcional, hoy llamado descubrimiento restringido

y antes autorización de clientes, también cifra el descriptor para la clave de cada cliente autorizado, de modo que solo esos clientes conocen dónde están los puntos de introducción.

Utilice el concepto en una decisión

Aplique «¿Qué es un servicio onion?» 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

El nombre hace el trabajo que DNS y una autoridad de certificación comparten en un sitio normal, y no necesita ninguno de los dos. Verificar el descriptor y completar la negociación indica al cliente que está hablando con quien posee la clave privada que hay detrás de la dirección. El RFC 7686, que reserva `.onion` como nombre de dominio de uso especial, describe estos nombres como una combinación de localización y autenticación y extrae la consecuencia: un nombre onion no se puede registrar, asignar, transferir ni revocar. Poseer uno significa controlar el par de claves, nada más.

El cifrado procede del mismo diseño. El tráfico hacia un servicio onion nunca sale de la red Tor, así que no hay un nodo de salida en el otro extremo ni un último tramo en texto claro. Por tanto, una página con un simple `http://` en un onion viaja cifrada de extremo a extremo hasta un host cuya identidad el cliente comprobó con el nombre que escribió.

El servicio solo establece conexiones salientes, hacia sus puntos de introducción y cada punto de encuentro, por lo que no necesita ningún puerto entrante abierto y funciona detrás de NAT. Añadir un onion no cambia la lista de puertos abiertos del host.

Los lectores siguen teniendo que conocer la dirección. Un sitio puede anunciarla mediante una cabecera de respuesta `Onion-Location` , y Tor Browser muestra entonces un botón morado con forma de píldora en la barra de direcciones que lleva a la copia onion de la página. Tor Project impone tres condiciones: el valor debe ser una URL `http:` o `https:` con un host onion, la página que la envía

debe haber llegado por HTTPS y esa página no debe estar ya en un onion. Una etiqueta meta puede transmitir el mismo anuncio cuando no se pueden configurar cabeceras, pero sin la ruta, de modo que todas las páginas apuntan a una URL fija.

Cómo se aplica en la práctica

La publicación del espejo onion de la empresa bajo una dirección legible está descrita paso a paso. El demonio procede del propio paquete de la distribución, con su puerto de proxy de salida desactivado. La clave privada asociada a la dirección se generó fuera del host y nunca ha llegado al repositorio ni a un portátil; el rol se niega a sobrescribir una identidad que no generó, por lo que una clave colocada a mano se utiliza tal cual. La dirección es un valor declarado en el inventario, y cada ejecución de convergencia comprueba que el archivo de identidad del host coincide con él, de modo que una clave sustituida con una declaración sin actualizar detiene la ejecución. Ambos controles de secretos detectan el archivo de clave, después de que una medición mostrara que el patrón evidente para archivos de claves coincidía con una clave de despliegue y pasaba por alto esta.

Un prefijo legible se puede encontrar, pero nunca elegir. Cada carácter adicional multiplica por 32 el esfuerzo de búsqueda esperado, por lo que las ocho letras de `engineer` requieren, de media, unos 1,1 billones de pares de claves. Retirar la dirección aleatoria con la que se publicó inicialmente el espejo exigió una transición por etapas, de modo que la dirección publicada siguió respondiendo durante todo el proceso. Un paso parecía definitivo y no lo era: la clave ya estaba en su sitio, la convergencia no notificó cambios y la nueva dirección siguió sin publicarse porque nada indicaba su directorio. Ahora el rol falla si encuentra en disco una identidad que ningún servicio menciona.

La página de créditos muestra la dirección completa, `engineer2ezpeji52ipphljcflzyhetvy5r6tnqubtq45nzlxxv6rsqd.onion`, junto a las de Gemini y Gopher. Las cuatro puertas de entrada comparten una carpeta de archivos y un despliegue, de modo que ninguna puede divergir de las demás, y el sitio normal envía `Onion-Location` para que Tor Browser ofrezca el onion sin que se solicite. Lo que ve la propia red del lector depende de la puerta: por Gopher, qué página se lee; por Gemini, qué dirección se solicitó; por el onion, ninguna de las dos cosas. El prefijo legible es una comodidad, no una prueba, así que lo que hay que comparar es la dirección completa.

La estructura de la dirección puede comprobarse sin conexión. Estas líneas la decodifican y vuelven a calcular la suma de comprobación, y ambas comparaciones imprimen `True`:

```
import base64
import hashlib

label = "engineer2ezpeji52ipphljcflzyhetvy5r6tnqubtq45nzlxxv6rsqd"
raw = base64.b32decode(label.upper())
key, checksum, version = raw[:32], raw[32:34], raw[34:]
digest = hashlib.sha3_256(b".onion checksum" + key + version).digest()
print(version == b"\x03", digest[:2] == checksum)
```

Una suma de comprobación válida muestra que la dirección está bien formada, no a quién pertenece. Esa parte procede de leerla en las propias páginas HTTPS de la empresa.

Dónde surgen los problemas

La clave es el único título de propiedad. Sin un registrador detrás del nombre, perder la clave privada significa perder la dirección, y una copia permite a otra persona responder en ella. La guía de configuración de Tor Project indica que los archivos de clave deben mantenerse privados y que debe hacerse una copia de seguridad de la clave si se pretende que el servicio perdure. Trátela como una clave de firma, no como configuración.

Leer solo las primeras letras. El RFC 7686 advierte de que un atacante puede encontrar claves cuyos nombres se parezcan al buscado y de que el riesgo aumenta porque los nombres no significan nada para una persona. Considera los nombres legibles, obtenidos con un esfuerzo de cómputo considerable, como una medida, pero un prefijo de ocho caracteres deja los otros 48 tan opacos como antes. Compare la dirección completa o acceda desde un marcador o un enlace en las propias páginas HTTPS del sitio.

El servidor revela su nombre. Tor oculta dónde se ejecuta el servicio, pero el software que hay detrás aún puede revelarlo. El RFC 7686 incluye entre las formas en que falla la protección que un servidor filtre su identidad en un mensaje de nivel de aplicación, y una página de error que muestre el nombre de

host real de la máquina es un ejemplo. La guía de configuración también recomienda pasar el tráfico al servidor web mediante un socket Unix en lugar de TCP, para que el servicio no quede expuesto en la red local:

```
HiddenServiceDir /var/lib/tor/my-website/
HiddenServicePort 80 unix:/var/run/tor/my-website.sock
```

Esto importa especialmente cuando la propia ubicación es el secreto.

El nombre llega a DNS. El software que no entiende Tor pregunta al resolvedor normal por un nombre onion, lo que revela a la red local y al proveedor de DNS qué onion se quería visitar. El RFC 7686 indica a ese software que falle sin hacer la consulta y a los servidores DNS que respondan que el nombre no existe. Entregue el nombre al cliente Tor en su lugar.

Un botón `Onion-Location` que nunca aparece. Una cabecera configurada solo en la redirección HTTP sin cifrar incumple la condición de HTTPS, y otra con una dirección mal escrita no lleva a los lectores a ningún sitio. Compruebe la cabecera de la respuesta HTTPS final.

Lecturas adicionales

- Especificación de encuentro de Tor, versión 3 — protocolo completo: claves de identidad y cegadas, descriptores, introducción y encuentro.
- Codificación de direcciones onion — fórmula que convierte una clave pública en un nombre de 56 caracteres, con direcciones de ejemplo.
- ¿Cómo funcionan los servicios onion? — recorrido paso a paso por los puntos de introducción, los descriptores y el encuentro.
- Configure su servicio onion — líneas de torrc, archivos que crea tor y recomendaciones sobre claves y filtraciones de ubicación.
- Onion-Location — configuración de cabeceras y etiquetas meta para Apache, Nginx y Caddy, y condiciones que debe cumplir la cabecera.
- RFC 7686 — por qué está reservado `.onion` y qué deben hacer con él los resolvedores, los operadores DNS y los registradores.

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 servicio onion?» 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/onion/