Engineer

NAT

🔀 reescritura de direcciones IP al atravesar un router

Qué es

NAT, sigla inglesa de traducción de direcciones de red, consiste en reescribir direcciones IP en los paquetes que atraviesan un router, para que equipos numerados en un espacio de direcciones puedan comunicarse con otros numerados en otro. RFC 2663, el documento de 1999 que fijó el vocabulario, lo describe como la correspondencia de direcciones IP entre ámbitos, con el objetivo de un encaminamiento transparente: los equipos de ambos lados no deberían necesitar saber que ocurre.

La modalidad que casi todo el mundo conoce es la que RFC 3022, publicado en enero de 2001, llama NAT tradicional. El caso típico es una oficina pequeña o un hogar con una única dirección IP del proveedor; las máquinas detrás del router usan direcciones privadas de los bloques RFC 1918: 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16, que no se encaminan entre organizaciones. El router sustituye la dirección de origen de cada paquete saliente por la suya pública y deshace el cambio en las respuestas. NAT básico solo traduce direcciones: pueden salir simultáneamente tantos equipos internos como direcciones públicas haya en su conjunto. NAPT, traducción de direcciones y puertos de red, reescribe además el puerto TCP o UDP o el identificador ICMP; así permite compartir una dirección pública entre muchos equipos internos. RFC 3022 señala que Linux ofrecía NAT con el nombre IP masquerade, palabra que sus herramientas de cortafuegos siguen utilizando.

Cambiar una dirección invalida todo lo calculado a partir de ella; el router también debe corregirlo. RFC 3022 exige ajustar la suma de comprobación de la cabecera IP y las de TCP y UDP, porque estas cubren una pseudocabecera con las direcciones de origen y destino. Para entregar cada respuesta al equipo interno adecuado, el router mantiene una tabla de correspondencias: dirección y puerto internos a un lado, dirección y puerto externos al otro. Esa tabla es estado conservado en medio de la red y origina la mayoría de los problemas de NAT.

NAT tradicional funciona en una dirección. RFC 3022 describe sesiones salientes desde la red privada y solo permite tráfico en sentido contrario mediante correspondencias estáticas de direcciones para equipos elegidos de antemano. La idea también opera ahora un nivel por encima: RFC 6598, de abril de 2012, reservó 100.64.0.0/10 para NAT de operador, con el que se numeran los enlaces entre el NAT del proveedor y los equipos de sus clientes, que pueden volver a traducir.

Utilice el concepto en una decisión

Aplique «¿Qué es NAT?» 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

RFC 3022 expone con franqueza la contrapartida. Puede instalarse NAT sin cambiar equipos ni routers, pero elimina, en palabras del RFC, «el significado de extremo a extremo de una dirección IP» y lo compensa con más estado en la red. Casi todas sus consecuencias prácticas se derivan de esa frase.

Para un servidor, la dirección de origen de una conexión suele corresponder a un router con muchos equipos detrás, en lugar de a una sola máquina. Un bloqueo o un límite de frecuencia dirigido a un visitante alcanza a todos los que comparten esa dirección; una denuncia de abuso identifica al router, no al culpable. RFC 3022 plantea lo mismo desde dentro: ocultar las direcciones privadas, que considera una ventaja para la privacidad, también dificulta el diagnóstico, porque el router NAT oculta la dirección del equipo que ataca a otros o envía spam.

El estado también implica temporizadores. Una correspondencia solo existe mientras el router la recuerda. RFC 4787, un documento de buenas prácticas (Best Current Practice) de enero de 2007, exige que una correspondencia UDP siga siendo válida durante al menos dos minutos y recomienda cinco o más. RFC 5382, su equivalente TCP de octubre de 2008, fija 2 horas y 4 minutos para una conexión establecida pero inactiva: los mensajes de mantenimiento se envían cada dos horas de forma predeterminada y los cuatro minutos cubren los paquetes aún en tránsito. Son mínimos para los dispositivos que cumplen esos

documentos; no todos lo hacen. Una conexión inactiva durante más tiempo que el temporizador del dispositivo pierde su correspondencia y el siguiente paquete externo ya no tiene destino interno.

De ahí se derivan otras dos restricciones. RFC 3022 exige que todos los paquetes de una sesión atraviesen el mismo router NAT; si una red tiene varias salidas, considera esencial que los dispositivos NAT compartan una tabla de traducciones idéntica. Los protocolos que incluyen direcciones en la carga útil necesitan ayuda del dispositivo NAT, que solo puede prestarla mientras pueda leer esa carga.

Cómo se aplica en la práctica

En un router Linux, nftables realiza NAT en cadenas de tipo `nat`. Las reglas siguientes son una ilustración de este artículo, basada en los ejemplos NAT del manual nft(8). Aquí, 198.51.100.0/24 representa la red interna y 203.0.113.5, la dirección pública del router: ambas pertenecen a los rangos para documentación; una red interna real utilizaría normalmente uno de los bloques RFC 1918.

```
add table nat
add chain nat prerouting { type nat hook prerouting priority dstnat; }
add chain nat postrouting { type nat hook postrouting priority srcnat; }
add rule nat postrouting oif eth0 ip saddr 198.51.100.0/24 snat to 203.0.113.5
add rule nat prerouting iif eth0 tcp dport 443 dnat to 198.51.100.20
```

La primera regla es el caso cotidiano: los paquetes de la red interna que salen por eth0 reciben 203.0.113.5 como origen. Para una dirección pública dinámica, el manual ofrece `masquerade`, que usa la dirección que tenga en ese momento la interfaz de salida. La segunda regla crea una correspondencia estática inversa: las conexiones TCP que llegan a eth0 por el puerto 443 se dirigen a 198.51.100.20 en el interior. Bastan tan pocas reglas porque solo el primer paquete de una conexión atraviesa una cadena nat: su decisión se guarda en la entrada de seguimiento de conexiones y todos los paquetes posteriores se reescriben de la misma forma.

La otra cara es un equipo detrás de un NAT que no controla; WireGuard dispone de un ajuste para ese caso concreto. En esta segunda ilustración propia del artículo, un equipo interno mantiene abierto un túnel hacia un par externo:

```
[Peer]
PublicKey = <the outside peer's public key>
Endpoint = 192.0.2.44:51820
AllowedIPs = 192.0.2.128/25
PersistentKeepalive = 25
```

El manual wg(8) describe `PersistentKeepalive` como un intervalo de 1 a 65.535 segundos para enviar un paquete vacío autenticado y mantener el estado de conexión de un cortafuegos con estado o la correspondencia NAT. Propone 25 segundos para una interfaz detrás de NAT que rara vez envía datos por iniciativa propia y puede recibir tráfico en cualquier momento; el ajuste viene desactivado de forma predeterminada. El par externo no necesita nada especial: su `Endpoint` para este equipo se actualiza con la dirección y el puerto de origen más recientes de los paquetes correctamente autenticados, precisamente los asignados por NAT.

Los problemas de NAT suelen aparecer en túneles de este tipo. El portafolio describe ocho conexiones WireGuard e IPsec administradas y diagnosticadas entre 2022 y 2024, entre Google Cloud y sistemas Linux. La página explica que los túneles eran frágiles y difíciles de diagnosticar cuando caían; se corrigieron de raíz los problemas recurrentes de encaminamiento e intercambio de claves, en lugar de recurrir a reinicios, y después cesaron las interrupciones. No indica si NAT intervino: los dos ejemplos anteriores pertenecen a este artículo, no a aquel proyecto.

Dónde surgen los problemas

Conexiones inactivas que dejan de responder. Un túnel, una conexión a base de datos o un canal de notificaciones que no envía nada durante un tiempo pierde su correspondencia y se rompe sin que ninguno de los extremos lo haya cerrado. El síntoma parece aleatorio porque depende del tiempo de inactividad. Envíe mensajes de mantenimiento desde dentro a intervalos más cortos que el tiempo de caducidad más breve del recorrido, como hace `PersistentKeepalive` ; si administra el NAT, mantenga los temporizadores en los mínimos de RFC 4787 y RFC 5382 o por encima de ellos. RFC 4787 exige que los paquetes salientes renueven la correspondencia y advierte de que la renovación entrante permite a un atacante conservarla para siempre: debería renovarla el extremo interno.

Esperar que entren conexiones. NAT tradicional es saliente por diseño: un servicio de un equipo interno resulta inaccesible hasta que alguien crea una correspondencia estática. Añada una regla `dnat` para los puertos exactos que necesita el servicio o invierta la dirección y deje que el equipo interno se conecte hacia fuera, como en el mantenimiento anterior.

Falta de retorno interno, o hairpinning. Dos equipos internos que se comunican mediante la dirección externa de uno de ellos necesitan que NAT devuelva el paquete hacia dentro. RFC 4787 exige ese retorno y que el paquete devuelto presente la dirección y el puerto externos de origen. Pruebe deliberadamente ese recorrido; donde el dispositivo no lo admita, haga que los equipos internos usen la dirección interna.

Direcciones dentro de la carga útil. FTP es el caso clásico: RFC 2663 señala que su orden `PORT` y su respuesta `PASV` incluyen una dirección IP y un puerto como texto, que quedan incorrectos si NAT solo reescribe cabeceras. Los dispositivos NAT adaptan estos protocolos mediante una pasarela de nivel de aplicación, ALG; RFC 3022 considera la de FTP la más extendida. Una ALG debe leer la carga útil: el cifrado la inutiliza salvo que la pasarela tenga la clave. RFC 3022 añade que no puede darse por supuesto IPsec de extremo a extremo a través de NAT. Prefiera protocolos sin direcciones en la carga útil; si debe atravesar un NAT propio con uno antiguo, el manual nft(8) muestra un ayudante de seguimiento de conexiones para FTP.

Logs que solo identifican al router. Detrás de NAT, el log de acceso de un servidor registra la dirección compartida, insuficiente por sí sola para identificar un equipo interno. Registre junto a ella el puerto de origen y una marca de tiempo exacta; mantenga sincronizados los relojes para poder relacionar una reclamación sobre una conexión con la traducción del router.

Fragmentos con NAPT. Solo el primer fragmento de un paquete contiene la cabecera TCP o UDP. RFC 3022 advierte de que traducir fragmentos salientes con NAPT está condenado al fallo y de que dos equipos internos que envíen fragmentos con el mismo identificador al mismo destino pueden corromper ambas sesiones. Mantenga los paquetes lo bastante pequeños para atravesar todo el recorrido sin fragmentarse.

Tratar NAT como un cortafuegos. Es fácil confundir su carácter unidireccional con protección. RFC 4787 reconoce que NAT suele desplegarse con fines de seguridad, pero afirma que la forma de establecer correspondencias no influye

en ella: la determina por completo el filtrado, es decir, qué paquetes deja entrar. Escriba reglas de filtrado explícitas sobre lo permitido y acompañe cada regla `dnat` de otra que solo admita el tráfico previsto.

Lecturas adicionales

- RFC 3022: traductor de direcciones IP tradicional, NAT tradicional — la descripción de 2001 de NAT básico y NAPT, con una lista franca de sus costes.
- RFC 2663: terminología y consideraciones sobre NAT — el vocabulario, desde los ámbitos de direcciones hasta el encaminamiento transparente y las ALG.
- RFC 4787: requisitos de comportamiento de NAT para UDP unicast — cómo debería establecer correspondencias, aplicar caducidades y realizar el retorno interno del tráfico UDP.
- RFC 5382: requisitos de comportamiento de NAT para TCP — el equivalente TCP, incluidos los tiempos de inactividad de conexiones establecidas y en cierre.
- wg(8): establecer y consultar la configuración de interfaces WireGuard — el manual de WireGuard, con `PersistentKeepalive` y las recomendaciones para equipos detrás de NAT.
- nft(8): manual de nftables — la referencia de nftables, incluidas las cadenas nat y las sentencias `snat`, `dnat` y `masquerade`.

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 NAT?» 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/nat/