Engineer

VPN

🖧 red lógicamente separada sobre infraestructura compartida

Qué es

Una VPN, abreviatura de virtual private network o red privada virtual, es un conjunto de túneles o rutas etiquetadas que permite a un grupo cerrado de máquinas comunicarse con sus propias direcciones y rutas, con independencia de las redes que atraviesen los paquetes. La terminología del IETF lo trata como una cuestión de separación, no de secreto: el grupo queda apartado de otros usuarios, y el cifrado se menciona como un añadido posible fuera del ámbito de los grupos de trabajo. En el uso cotidiano dominan dos formas. Una VPN entre sitios une redes completas, como una oficina y un proyecto en la nube, mediante una pasarela en cada extremo. Una VPN de acceso remoto conecta un portátil o teléfono con una red en la que no se encuentra físicamente.

Tecnologías muy distintas comparten el nombre. IPsec protege paquetes IP dentro de la pila de red de un equipo o una pasarela de seguridad y suele usar IKEv2 para negociar sus claves; es lo que admiten la mayoría de cortafuegos, routers y pasarelas gestionadas de nube. WireGuard es un túnel más reciente que aparece como una interfaz de red normal, viaja sobre UDP, identifica a cada par mediante una clave pública y ofrece deliberadamente un solo conjunto fijo de algoritmos de cifrado, en lugar de un menú que negociar. OpenVPN se ejecuta como proceso en espacio de usuario y establece sus claves con TLS. Las VPN de operadores basadas en BGP y MPLS separan a los clientes dentro de la red troncal del proveedor y, según su propia especificación, no ofrecen ninguna privacidad criptográfica. Cuando un contrato, un diagrama o un proveedor de cortafuegos dice VPN, conviene preguntar a cuál de estas tecnologías se refiere.

Utilice el concepto en una decisión

Aplique «¿Qué es una VPN?» 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 decisión que suele resolver una VPN es cómo comunicar dos lugares sin exponer en Internet el servicio que los une. Una base de datos que solo lee un flujo de otra nube, un panel interno de administración o un destino de copias de seguridad pueden escuchar públicamente tras un inicio de sesión, o hacerlo en una dirección privada accesible únicamente por el túnel. La segunda opción reduce a un puerto de pasarela lo que puede encontrar un escáner y sigue siendo una solución sencilla y bien conocida para enlaces entre sitios.

La siguiente pregunta es WireGuard o IPsec, y suele decidirla el extremo remoto. Si ese extremo es un cortafuegos dedicado, una pasarela gestionada de un proveedor de nube o el equipo de redes de un socio, a menudo solo se ofrece IPsec y la interoperabilidad pesa más que la elegancia. Si ambos extremos son máquinas Linux bajo su control, WireGuard se configura más deprisa y resulta más fácil de entender: un archivo breve por lado, una clave pública por par y una lista de direcciones desde las que cada par puede enviar. Su artículo de diseño cifra la implementación Linux en menos de 4.000 líneas de código, lo bastante pequeña para auditarla. Una configuración IPsec en Linux, en cambio, combina la transformación de paquetes del núcleo con un demonio aparte de intercambio de claves y una lista más larga de opciones que deben acordarse.

El coste de funcionamiento rara vez es el software, incluido en Linux y en la mayoría de los cortafuegos. El coste es la atención. Los túneles caen de noche, la renovación de claves falla horas después de que alguien cambie un ajuste en el otro extremo y el único síntoma es el silencio: entran paquetes y no vuelve nada. Un túnel merece el mismo trato que cualquier servicio de producción: su propia comprobación de salud, su propia alerta y una nota escrita que indique quién se ocupa de cada extremo.

Una VPN también puede ser la herramienta equivocada. Dar a cada empleado remoto un túnel completo hacia la oficina le concede acceso a toda una subred cuando solo necesitaba una aplicación, y, una vez conectado, todo en esa subred tiende a confiar en él. El acceso por aplicación, donde cada solicitud se autentica por separado y que suele venderse como confianza cero, encaja mejor cuando los usuarios son personas y los destinos son aplicaciones web. Las aplicaciones de

consumo que anuncian una VPN para proteger la privacidad son otra cosa: trasladan la confianza del proveedor de Internet a la empresa de VPN y pueden ocultar la IP de origen inicial a los sitios de destino, pero no garantizan por sí solas el anonimato.

Cómo se aplica en la práctica

Entre 2022 y 2024, el tráfico seguro entre Google Cloud y sistemas Linux locales pasó por ocho túneles WireGuard e IPsec, gestionados y diagnosticados como un conjunto. Habían sido frágiles y lentos de diagnosticar, y un túnel caído podía cortar la comunicación entre entornos. Su configuración se normalizó para que ninguno siguiera siendo un caso particular, se vigiló su estado y los problemas recurrentes de rutas e intercambio de claves se corrigieron de raíz, en vez de despejarse con un reinicio. Los ocho pasaron a funcionar de forma fiable y cesaron las incidencias recurrentes de conectividad.

En esos mismos años, una organización necesitaba datos de un almacén remoto situado tras una VPN IPsec. Para los seis flujos ETL/ELT que alimentaban Google BigQuery, el túnel era el primer eslabón: se establecieron conexiones seguras con el servidor protegido para obtener datos sin intervención. Después, tareas programadas descargaban archivos comprimidos con ficheros Parquet, CSV y .bak, los restauraban y preparaban en MSSQL y PostgreSQL y cargaban el resultado en BigQuery. Con un túnel que ya no esperaba a una persona, la ejecución completa duraba menos de 20 minutos frente a al menos tres horas de trabajo manual, y los datos se actualizaban cada día en vez de cada semana. La VPN es la parte menos visible del resultado y la que sostiene a las demás: un flujo que no puede llegar a su fuente se detiene en el primer paso, por bueno que sea el SQL que viene después.

Dónde surgen los problemas

Los paquetes grandes desaparecen y los pequeños pasan. Todo túnel añade cabeceras, así que el mayor paquete que cabe dentro es menor de lo que permite la ruta exterior. Un mensaje de datos WireGuard añade 32 bytes de sobrecarga fija antes de las cabeceras UDP e IP externas: unos 60 bytes en total sobre IPv4 y 80 sobre IPv6, además de cualquier relleno del paquete. Si la MTU del túnel es demasiado alta y la ruta descarta los mensajes ICMP que lo comunicarían, funcionan ping y el inicio de sesión SSH, pero se bloquean las transferencias de archivos y los intercambios TLS. Pruebe con un paquete de tamaño completo que no permita fragmentación y reduzca después la MTU de la interfaz o limite el tamaño de los segmentos TCP para que quepan.

```
# When each WireGuard peer last completed a handshake, as Unix time
wg show wg0 latest-handshakes
# A 1,420-byte packet that may not be fragmented on the way
ping -M do -s 1392 -c 3 10.0.0.2
# Which interface and route the kernel picks for a remote host
ip route get 10.20.0.5
```

Dos sitios eligieron las mismas direcciones. Rangos privados como 10.0.0.0/8 y 192.168.0.0/16 se reutilizan por todas partes. Unir dos redes que usan 10.0.0.0/24 deja al router sin forma de saber a qué lado va un paquete. Planifique los rangos antes del primer túnel o acepte traducir direcciones en un extremo, lo que complica cada línea de registro y cada regla de cortafuegos posteriores.

El túnel está activo, pero la ruta es incorrecta. Un par puede mostrar un intercambio de claves reciente mientras el tráfico sigue saliendo por la ruta predeterminada, porque falta la ruta a la subred remota o porque la lista de direcciones permitidas de WireGuard para ese par no la incluye. En IPsec, el equivalente son selectores de tráfico que difieren entre extremos. IKEv2 los reduce a la intersección o los rechaza con una notificación TS_UNACCEPTABLE, de modo que un túnel puede establecerse transportando menos de lo que pretendía cualquiera de los lados.

La renovación de claves falla mucho después del cambio. Ambos protocolos sustituyen las claves de sesión activas con el tiempo. Una discrepancia introducida en un extremo, como una propuesta editada o una clave rotada, puede manifestarse solo al sustituirse las claves actuales. WireGuard inicia una nueva sesión aproximadamente cada dos minutos mientras hay tráfico. Los tiempos de vigencia de IPsec se fijan mediante la política local de cada extremo y no tienen por qué coincidir. En WireGuard, interprete la antigüedad del último intercambio correcto junto con el tráfico previsto o las comprobaciones de salud: un intercambio antiguo de un par inactivo no demuestra por sí solo un fallo. Active la comprobación de actividad de IKEv2, conocida como dead peer detection, para que la pasarela detecte un par silencioso en lugar de seguir enviando a un agujero negro.

Estar conectado pasa a significar ser de confianza. En muchas configuraciones de acceso remoto, un portátil conectado a la VPN se trata como si estuviera en la oficina: una credencial robada da acceso a todo en esa subred. Filtre en la

pasarela qué puede alcanzar cada cliente VPN, mantenga la autenticación de los servicios que hay detrás y decida de forma deliberada si la resolución de nombres y el tráfico de Internet pasan por el túnel o lo rodean.

Lecturas adicionales

- RFC 4026, sección 3.10 — la definición genérica del IETF de una VPN y la nota que sitúa el cifrado fuera de los mandatos de los grupos de trabajo.
- WireGuard: Next Generation Kernel Network Tunnel — el artículo de diseño: rutas ligadas a claves, intercambio de claves y temporizadores que rigen su renovación.
- RFC 4301 — la arquitectura de seguridad para IP que sigue toda implementación IPsec.
- RFC 7296 — IKEv2, incluida la reducción de selectores de tráfico, las duraciones como política local y la comprobación de actividad.
- RFC 4364 — las VPN IP BGP/MPLS de operadores, con espacios de direcciones solapados y sin privacidad criptográfica.

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 una VPN?» 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/vpn/