Protege los flujos de trabajo DevOps

Conectividad Zero Trust para tus canales de integración y distribución continuas (CI/CD) y flujos de trabajo de servicio a servicio.

Acceso fácil y seguro para DevOps

Conectividad y seguridad tan ágiles como tus flujos de trabajo
Sabemos que la interacción compleja con el canal de integración y distribución continuas (CI/CD) es célebre por su agilidad. Por lo tanto, la conectividad y la seguridad que respaldan estos flujos de trabajo deben estar en consonancia. Sin embargo, los equipos de DevOps a menudo dependen de las VPN tradicionales para el acceso remoto a distintas herramientas operativas y de desarrollo.

Por qué las herramientas tradicionales de acceso remoto no son suficientes

Las VPN son intrínsecamente no seguras

No elijas las VPN para el acceso remoto. Son difíciles de gestionar y susceptibles a ser explotadas mediante vulnerabilidades conocidas o de día cero.

Los desarrolladores odian la fricción

La seguridad debe "simplemente funcionar", porque, sea cual sea el grupo de usuarios, los desarrolladores pueden encontrar soluciones creativas que permitan reducir la fricción en los flujos de trabajo.

Las herramientas heredadas no son ágiles

Es necesario dar cabida a los cambios puntuales de las políticas de seguridad, así como al acceso Zero Trust temporal que requieran los proveedores o el personal que intervenga en la respuesta a incidentes.

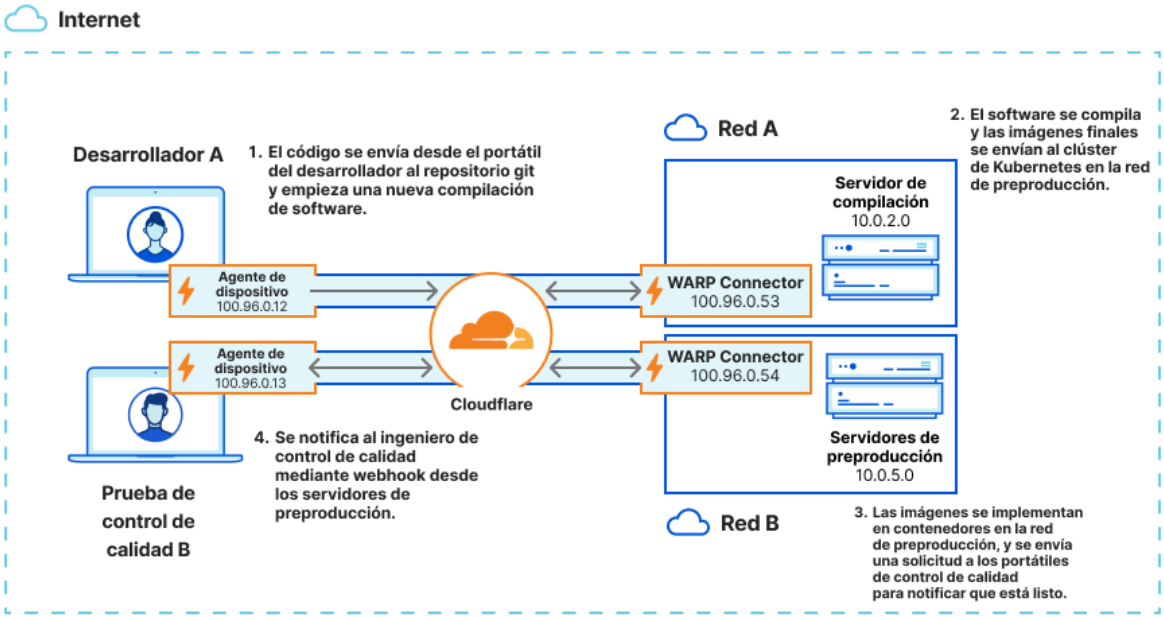
Ampliar a DevOps el acceso a la red Zero Trust

Conectividad de red en malla y tráfico bidireccional
El acceso a la red Zero Trust (ZTNA) funciona bien para el acceso seguro y con privilegio mínimo de los usuarios a las aplicaciones (incluidos los desarrolladores que acceden a los servidores SSH). Sin embargo, debe ir más allá para proteger los casos de uso de la red que implican tráfico bidireccional o iniciado por el servidor. Esto sigue una tendencia emergente que imagina un modelo de conectividad de red en malla superpuesto en las nubes, las VPC o los segmentos de red, sin depender de los enrutadores.

Para una conectividad verdaderamente universal, los clientes necesitan la flexibilidad necesaria para abordar todos sus casos de uso de acceso a las aplicaciones y de conectividad de la red. No todos los accesos a la red que ofrecen los proveedores SASE pueden ir más allá del tráfico iniciado por el cliente sin cambios del enrutamiento de red o desventajas de seguridad. Por lo tanto, las pretensiones acerca de una conectividad universal genérica pueden no ser lo que parecían en un principio.

Cómo puede ayudar Cloudflare

Cloudflare amplía el alcance del acceso a la red Zero Trust para garantizar que incluye todos los casos de uso de conectividad de los usuarios a las aplicaciones, así como las redes seguras punto a punto (P2P) y en malla para que las opciones de conectividad sean tan amplias y flexibles como sea posible. Los flujos de trabajo de servicio a servicio DevOps pueden ejecutarse eficazmente en la misma plataforma que proporciona el acceso a la red ZTNA, la sustitución de las VPN o SASE a nivel empresarial.



Cloudflare funciona como la herramienta que cohesiona la conectividad para todos los usuarios y recursos DevOps, independientemente del flujo de tráfico en cada paso. Esta misma tecnología, es decir, WARP Connector, permite a los administradores gestionar distintas redes privadas con rangos de direcciones IP que se solapan: VPC y RFC1918, admitir el tráfico iniciado por el servidor y la conectividad a las aplicaciones P2P (p. ej., tráfico SCCM, AD, VoIP y SIP) en las redes privadas existentes. También puede permitir desarrollar redes privadas P2P (p. ej., flujos de recursos CI/CD) y direccionar el tráfico de forma determinista. Asimismo, las organizaciones pueden automatizar la gestión de su plataforma SASE gracias al proveedor Terraform de Cloudflare.

Hablemos del acceso sencillo y seguro para tu organización

Solicitar seminario

CLOUDFLARE

¿Necesitas más tiempo?

Sigue leyendo en nuestra arquitectura de referencia SASE.