CLOUDFLARE

RESUMEN DE SOLUCIÓN

Proteger los entornos de trabajo descentralizados

Protección coherente en un plano de control unificado para todas las solicitudes, desde cualquier ubicación

Migración de la seguridad a la nube

Reduce la complejidad y el riesgo en las oficinas con Cloudflare

Ahora que los empleados trabajan de forma remota y presencial, muchas organizaciones están reformulando la forma de proteger las oficinas hoy en día, tanto si dependen de dispositivos en centros de datos como si permiten el acceso directo y no seguro a Internet.

Su nuevo objetivo es ofrecer protección y experiencias coherentes a todos los usuarios dentro y fuera de la red. En la mayoría de los casos, esta misión exige alejar los controles de herramientas dispares como VPN, proxies web y firewalls, y dirigirlos hacia una única plataforma de seguridad en la nube.

Cloudflare ve a las organizaciones modernizando la seguridad de la oficina con dos casos de uso comunes.

> **Combina el acceso local y remoto en una única implementación para garantizar políticas coherentes y minimizar el número de proveedores necesarios. Implementa tecnología ZTNA para mejorar o sustituir la VPN tradicional y limitar la inversión en tecnología heredada.[1]**
>
> Gartner

Caso de uso recomendado:

Proteger el acceso a las aplicaciones con Zero Trust para sustituir las VPN

Aplica políticas granulares con reconocimiento de la identidad por aplicación, en lugar de permitir el movimiento lateral a través de la red corporativa.

- **Paso 1:** integra tu(s) proveedor(es) de identidad.
- **Paso 2**: protege cualquier aplicación web a través de un navegador.
- **Paso 3**: protege entornos SSH, VNC y RDP a través de un navegador.

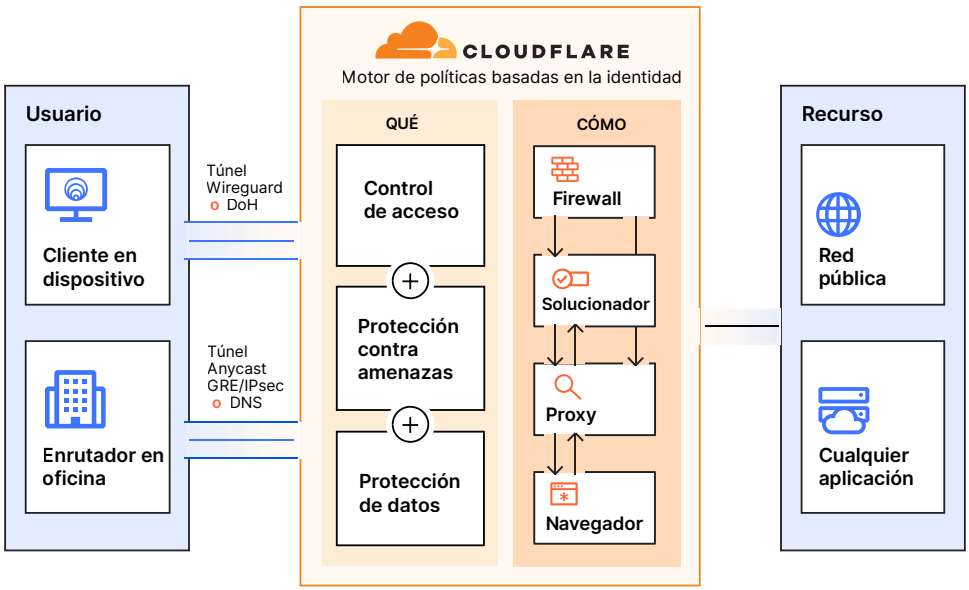
Caso de uso recomendado:

Filtrar el acceso a Internet para una seguridad coherente con una rentabilidad rápida

Protege primero a los usuarios presenciales con el filtrado DNS y, posteriormente, con inspecciones integrales en todas las ubicaciones. Se acabó el redireccionamiento del tráfico a través de dispositivos de seguridad locales en centros de datos.

- **Paso 1:** dirige el tráfico DNS a la red global de Cloudflare.
- **Paso 2**: configura el filtrado DNS basado en la ubicación para protegerte del ransomware, el phishing y otras amenazas de Internet.
- **Paso 3**: controla los flujos de datos aplicando reglas de HTTP, red y aislamiento de navegador con inspección TLS 1.3 ilimitada.

Funcionamiento



Implementación sin cliente para verificar el acceso y filtrar las consultas DNS desde las oficinas.

Implementación con el cliente de dispositivo de Cloudflare para conseguir mayor visibilidad y controles por usuario y dispositivo.

Figura 1: Verifica, filtra, aísla e inspecciona el tráfico local en un único paso con Cloudflare Zero Trust

Accesos flexibles desde cualquier origen

Empieza utilizando Cloudflare para la resolución de DNS a través de enrutadores de red. Con el tiempo, envía el tráfico de capa 3 a nuestra red global a través de tus túneles GRE o IPsec, o utiliza tu método de enrutamiento SD-WAN actual.

Como alternativa, implementa el cliente de Cloudflare para el filtrado y la inspección de DNS y HTTP en dispositivos administrados.

Aplicación rápida de políticas diseñada para escalar globalmente

Todas las funciones de seguridad, rendimiento y fiabilidad están diseñadas para ejecutarse en todos los servidores de todos los centros de datos en nuestras más de 275 ubicaciones en más de 100 países.

Nuestra escala de red significa que las protecciones se aplican siempre cerca de las oficinas y los usuarios finales, estén donde estén, a gran velocidad con inspección de paso único.

Otros casos de uso que investigar en los próximos 6-12 meses

Recupera el control sobre las aplicaciones SaaS

Descubre y mitiga los riesgos de los elementos de Shadow IT que los usuarios utilizan en las oficinas y en casa.

Evita las fugas de datos y el incumplimiento de normativas con políticas CASB activadas desde el mismo panel unificado de Cloudflare. Descubre cómo.

Elimina el tráfico MPLS

Sustituye las conexiones MPLS privadas, caras, obsoletas y lentas.

Simplifica la arquitectura WAN heredada utilizando la red global de Cloudflare para gestionar el tráfico entre sucursales, centros de datos y servicios de nube pública. Descubre cómo.

1. Gartner Hype Cycle for Network Security, 2021 | GARTNER y HYPE CYCLE son marcas comerciales registradas y marcas de servicio de Gartner, Inc. o sus filiales en los EE. UU. e internacionalmente, y se usan aquí con permiso. Todos los derechos reservados.

REV:BDES-6043.06AGO2024