Acceso a la red Zero Trust con enrutamiento privado

Evita el movimiento lateral y reduce la dependencia de la VPN

Confiar en los controles en red (como las VPN y la restricción de la ubicación IP) para acceder a las aplicaciones puede aumentar tu superficie de ataque, limitar la visibilidad y frustrar a los usuarios finales. El acceso a la red Zero Trust de Cloudflare trabaja junto con tus proveedores de identidad y plataformas de protección de puntos de conexión para aplicar reglas Zero Trust de denegación por defecto, que limitan el acceso a las aplicaciones corporativas, los espacios de direcciones IP internas y los nombres de servidor. Permite que las conexiones de los usuarios sean más rápidas que una VPN gracias a nuestra inmensa red eficaz Anycast.

Desde que implementamos internamente el acceso a la red Zero Trust, Cloudflare se ha beneficiado de:

- Una reducción del 91 % en la superficie de ataque.[1]
- Un doble ahorro de costos al simplificar el trabajo de los equipos informáticos.
- Una reducción del 80 % en el tiempo destinado a atender incidencias relacionadas con la VPN.
- Un descenso del 70 % en el volumen de incidencias.
- Más de 300 horas anuales de productividad aprovechada durante el proceso de integración de nuevos empleados.

Lo que puedes hacer con Access

Proteger cualquier aplicación

Cloudflare es independiente de la identidad y de las aplicaciones, lo que te permite proteger cualquier aplicación, ya sea SaaS, en la nube o en un entorno local, con el proveedor de identidad de tu elección.

Conectar usuarios de manera flexible, con o sin cliente

Facilita las conexiones SSH y a las aplicaciones web sin software cliente ni configuraciones. Para aplicaciones no web, conexiones RDP y enrutamientos privados, utiliza un cliente integral en distintos casos de uso de acceso a Internet y a las aplicaciones.

Permitir la federación de identidades a través de varios proveedores de identidad

Integra todos tus proveedores de identidad corporativos (Okta, Azure AD, entre otros) en los procesos de migración, adquisición y acceso de usuarios de terceros más seguros. Activa códigos únicos para el acceso temporal, o incorpora proveedores de identidad social como LinkedIn y GitHub.

Restringir el movimiento lateral entre recursos corporativos

Aplica métodos de autenticación seguros y consistentes, incluso a aplicaciones heredadas con reglas de firewall de IP y Zero Trust.

Implementar métodos de acceso de acuerdo al dispositivo

Antes de conceder acceso a un recurso, evalúa las señales de postura del dispositivo, incluida la presencia del cliente Gateway, el número de serie y el certificado mTLS, para garantizar que solo los dispositivos conocidos y seguros puedan conectarse a tus recursos. Integra la postura del dispositivo de proveedores de la plataforma de protección de puntos de conexión (EPP), incluidos Crowdstrike, Carbon Black, Sentinel One y Tanium.

Registrar la actividad del usuario a través de cualquier aplicación

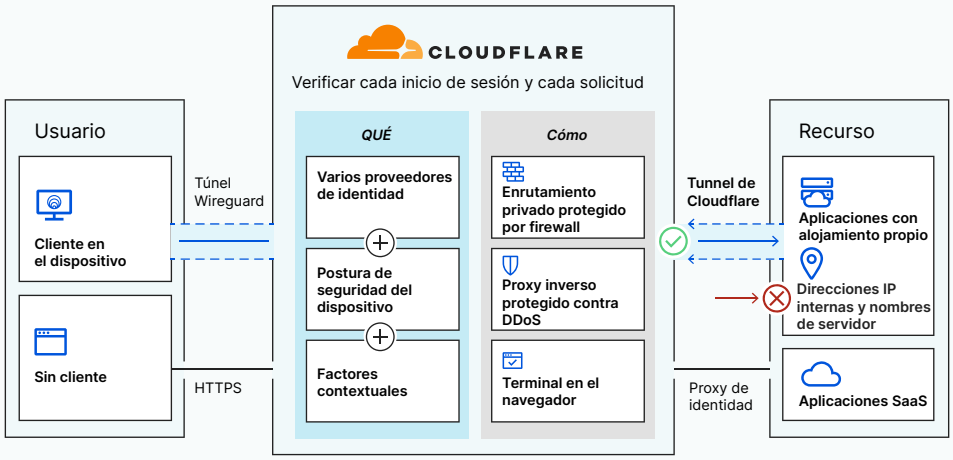
Registra todas las solicitudes que se haga en tus aplicaciones protegidas, no solo inicio y cierre sesión. Añade registros de actividad en Cloudflare o expórtalos a tu proveedor de SIEM.

[1]Cuando el acceso a la red Zero Trust se combina con la navegación por Internet

La diferencia de Cloudflare

- Nuestro **rendimiento inmejorable** agiliza las solicitudes con un enrutamiento optimizado y basado en datos de inteligencia a través de la red Anycast de Cloudflare. De media, se accede a las aplicaciones web un 30 % más rápido y el tiempo de ida y vuelta de las conexiones TCP se reduce un 17 %. Nuestra información se basa en el análisis de los datos de red de 25 millones de solicitudes HTTP por segundo y 39 000 nuevas conexiones TCP por segundo.
- Nuestra **gestión más sencilla** combina el acceso a la red Zero Trust (ZTNA), la puerta de enlace web segura (SGW), el aislamiento remoto del navegador (RBI), entre otras soluciones, en un único plano de control con una experiencia de administración que se ha desarrollado desde cero y, que por tanto, no hemos adquirido ni es resultado de una agrupación de varios proveedores.
- Nuestra **inspección de paso único** verifica, filtra, aísla e inspecciona el tráfico de forma rápida y consistente en todo el mundo, ya que todos los servicios de Cloudflare se implementan en cada centro de datos de nuestras más de 250 ubicaciones en todo el mundo.

Cómo funciona



En lugar de una VPN, los usuarios se conectan a los recursos corporativos a través de un cliente o navegador web. Conforme se enrutan y aceleran las solicitudes a través del perímetro de Cloudflare, se evalúan según las reglas Zero Trust que incorporan señales de proveedores de identidad, dispositivos y otros contextos. Anteriormente, el software RDP, los programas de visualización de archivos SMB y otros programas de clientes pesados requerían una VPN para una conexión de red privada. Sin embargo, hoy los equipos pueden enrutar de manera privada cualquier tráfico TCP o UDP a través de la red de Cloudflare donde se acelera, verifica y filtra en un paso único, optimizando así el rendimiento y la seguridad.

"Cloudflare Access evitó que tuviéramos que desarrollar nuestro propio sistema de administración de identidades y acceso (IAM). No tenemos que crear funciones de permiso de usuario en las aplicaciones que protege Access. Apostamos por un todo en uno. El acceso está abierto a toda la compañía".

Jim Tyrell
Director de infraestructura, Canva

"En Delivery Hero, siempre nos esforzamos por ofrecer una experiencia increíble a nuestros clientes. Cloudflare Access nos ayuda a hacer lo mismo para nuestros equipos internos. Les ofrece un entorno de trabajo seguro y elimina la necesidad de que una VPN acceda a todas nuestras aplicaciones en todo el mundo".

William Carminato
Director sénior de ingeniería, Delivery Hero

Integraciones de administración de identidades y acceso

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML OIDC

Integraciones de la plataforma de protección de puntos de conexión

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

Funciones principales

Política coherente	
Políticas personalizadas de acceso a aplicaciones, redes privadas e Internet	**Sin límite**
Autenticación a través de proveedores de identidad corporativos y sociales	✓
Postura del dispositivo con integraciones de terceros y Cloudflare	✓
Importación masiva basada en CSV de listas de números de serie de dispositivos corporativos	✓

Aumento de visibilidad	
Retención del registro de actividad	**6 meses**
Vistas detalladas del país estado y dispositivo en función de la identidad	✓
Envío de registros al almacenamiento en la nube o a los SIEM	✓

Conexión segura	
Conexiones cifradas basadas en el cliente a Internet (cliente WARP)	**Win, Mac, iOS, Android**
Acceso seguro sin cliente a aplicaciones autohospedadas y SaaS	✓
Conexiones privadas para aplicaciones autohospedadas, direcciones IP internas y nombres de servidor (Cloudflare Tunnel)	✓

Interoperabilidad sencilla	
Integraciones de gestión de puntos de conexión y movilidad	✓
Túnel dividido para conexión local o VPN	✓
Autoregistro de cliente para usuarios en dispositivos no administrados	✓
Iniciador de aplicaciones personalizable	✓
Autenticación que admite varios proveedores de identidad simultáneamente	✓
Conectores genéricos y personalizados que admiten los protocolos de identidad SAML y OIDC	✓
Autenticación basada en token para servicios automatizados	✓
Autorización basada en certificados para IoT y otros casos de uso de mTLS	✓

Sin afectar al rendimiento	
SLA de tiempo activo	**100 %**
Una de las redes más rápidas (a menos de 50 m/s de distancia de más de 250 PoP)	✓
El solucionador DNS más rápido que prioriza la privacidad (7-31 m/s a través de más de 250 PoP)	✓
Actualización ultrarrápida de políticas (menos de 500 m/s en más de 250 PoP)	✓
Navegador remoto ultrarrápido (sin inserción de píxeles - se ejecuta en nuestra red. Sin red de terceros)	**Complemento**

¿Te interesa saber más?

Visita www.cloudflare.com/es-la/products/zero-trust/access/ para abrir una cuenta. Gratis para un máximo de 50 usuarios.