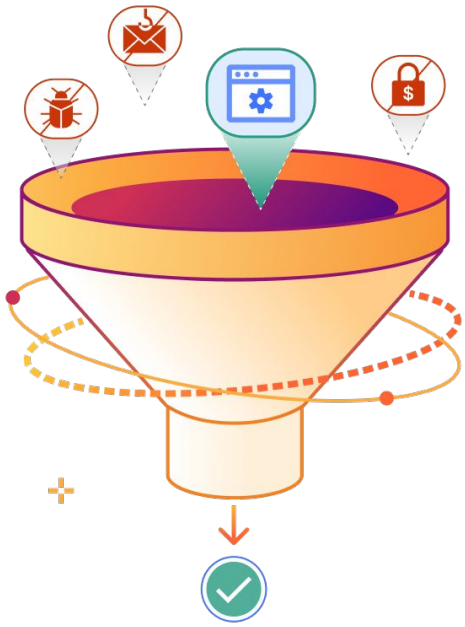
Puerta de enlace web segura (SWG)

Cloudflare Gateway, un servicio componible que forma parte de Cloudflare One, protege a los usuarios y los datos de las ciberamenazas a través del filtrado de Internet con reconocimiento de identidad.



Protección sencilla y moderna contra amenazas

Sustituye las complejas soluciones de seguridad web heredadas

Las ciberamenazas nos acechan por todos lados y siguen aprovechando las vulnerabilidades de la superficie de ataque en expansión de tu organización. La combinación de varias soluciones específicas (como la resolución DNS, las puertas de enlace web y los firewalls de red) solo aumenta el coste, la complejidad y el riesgo.

Cloudflare Gateway simplifica la seguridad con visibilidad y protección coherentes para acceder a Internet y a los recursos internos. Reduce el ciberriesgo con políticas de reconocimiento de identidad que ayudan a tu organización a:

- **Evitar las amenazas web** como el ransomware, el phishing, el comando y control y mucho más.
- **Controlar y supervisar el tráfico** de capas 4-7 con la aplicación de reglas de DNS, HTTP, red y aislamiento de navegador.
- **Aplicar políticas de uso aceptable** entre los usuarios remotos y presenciales.

En una arquitectura de paso único, el tráfico se verifica, filtra, inspecciona y aísla de las amenazas.

Empieza hoy con una solución SWG y avanza hacia el uso de servicios de seguridad en el perímetro (SSE) en el futuro

La modernización de los controles de SWG es el primer paso habitual hacia la consolidación de la seguridad, junto con una arquitectura SSE y la adopción de las prácticas recomendadas de Zero Trust.

Descubre ese recorrido con Cloudflare.

¿Por qué Cloudflare?

Seguridad unificada

1 red

y un plano de control para todos los servicios como la seguridad en el perímetro (SSE), la protección de aplicaciones web y las API (WAAP) y la seguridad del correo electrónico, entre otros.

Información sobre amenazas a gran escala

2 billones

de consultas DNS resueltas al día. Esta visibilidad en tiempo real de los dominios nuevos, recién vistos y peligrosos alimenta los modelos de detección de amenazas basados en la IA y el aprendizaje automático.

Plataforma creada para escalar

+310

ubicaciones de red en +120 países. Los clientes pueden ejecutar todas las funciones de SWG y Zero Trust/SSE en todas las ubicaciones, garantizando así una aplicación rápida y consistente en todo momento.

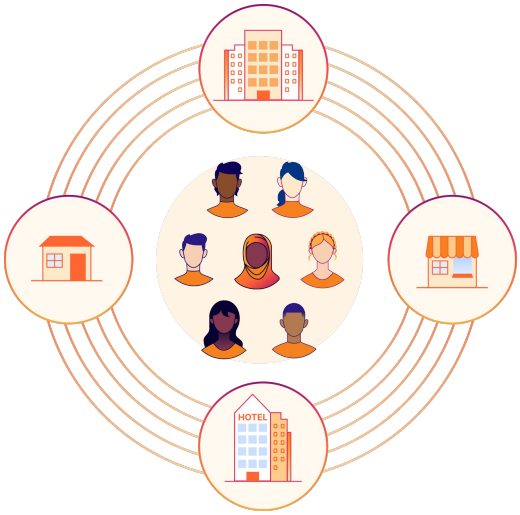
Caso de uso: Protección contra amenazas para usuarios remotos y presenciales

Problema

La modalidad de trabajo híbrido ha ampliado tu superficie de ataque, y los fallos de seguridad derivados de la gestión de herramientas dispares facilitan que el ransomware, el phishing y otras ciberamenazas afecten de manera negativa a tu bolsillo y a la reputación de tu marca.

Solución

La solución SWG de Cloudflare ofrece seguridad web coherente a todos los usuarios remotos y presenciales. La mayoría de las organizaciones recurren como primer paso al filtrado de DNS para conseguir una rentabilidad rápida, antes de aplicar inspecciones y controles más exhaustivos en toda la actividad en Internet.



Primeros pasos

Envía primero el tráfico a la red de Cloudflare para la resolución DNS (y luego para la inspección completa de HTTP).

Aplica el filtrado de DNS por identidad / dispositivo de los usuarios remotos o por ubicación de oficina.

Usa una arquitectura de capas de control más precisa, incluidas reglas HTTP, de red y de aislamiento de navegador.

Implementa la seguridad del correo electrónico en la nube en modo en línea como MX, mediante API o ambas (modo múltiple).

Primero, protege la navegación de los usuarios dentro y fuera de la red

A continuación, añade una solución de seguridad del correo electrónico

Reduce el riesgo y mejora la productividad de los equipos

Implementación sencilla y flexible

Utiliza enrutadores de red para la resolución de DNS. Envía el tráfico de capa 3 a través de túneles GRE/IPsec, conector WAN o SD-WAN existente.

O implementa nuestro cliente de dispositivo para reenviar el tráfico mediante proxy.

Protección rápida y coherente

Inspección de paso único en toda nuestra red para una aplicación de políticas rápida y coherente en todas partes.

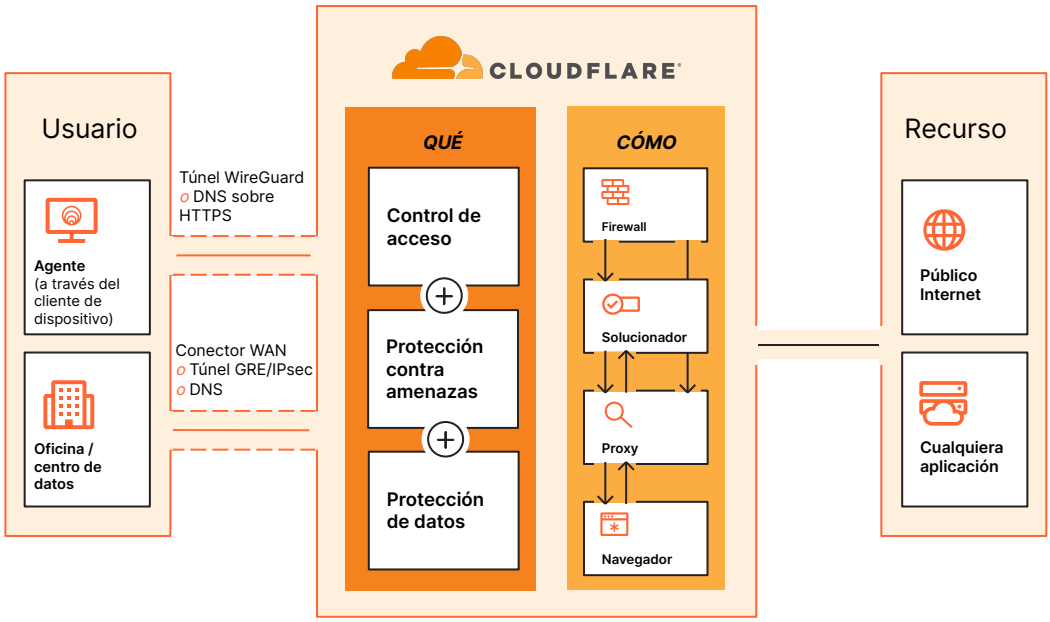
Se ha demostrado que nuestra solución es más rápida que las soluciones de proveedores como Zscaler, Netskope y Palo Alto Networks.

Acelera la adopción de Zero Trust

Un plano de control unificado con un solo gestor de políticas en todos los servicios SSE / SASE componibles.

Empieza con soluciones de seguridad web y correo electrónico y añade otros controles Zero Trust a tu propio ritmo.

Cómo funciona SWG



Simplifica la seguridad.

Aplica controles de firewall, de resolución, de proxy y de navegador tanto al tráfico interno como web.

Crea políticas desde un gestor de políticas.

Añade controles SSE a tu solución SWG

El redireccionamiento del tráfico mediante proxy a través de la solución SWG de Cloudflare permite a tu organización ampliar aún más los controles de seguridad y la visibilidad aprovechando las capacidades de nuestros servicios SSE integrados de forma nativa y componibles.

Protege la actividad web y de las aplicaciones con RBI

- Aísla los dispositivos locales del malware mediante la ejecución de todo el código del navegador en la red global de Cloudflare con baja latencia.
- Aísla las aplicaciones para proteger los datos con análisis DLP y controles del navegador (p. ej. bloquear, copiar y pegar, restringir carga/descarga, impresión), con o sin un cliente de dispositivo.

Protege los datos con soluciones CASB y DLP multimodo

- Evita las fugas de datos mediante la detección y el bloqueo de datos confidenciales en el tráfico HTTP(S) y en los archivos con perfiles predefinidos (p. ej. datos financieros / sanitarios) o personalizados (p. ej. coincidencia exacta de datos).
- Analiza las aplicaciones SaaS en busca de configuraciones erróneas con detecciones DLP integradas para datos confidenciales y adopta medidas prescriptivas para corregirlas.

Amplía las políticas de acceso de reconocimiento de identidad con ZTNA

- Aplica reglas Zero Trust que limitan el acceso a aplicaciones corporativas autoalojadas, aplicaciones SaaS y nombres de host o direcciones IP de redes privadas.
- Integra proveedores de soluciones de protección de identidad y de puntos finales y aplica comprobaciones de postura en las reglas de acceso a Internet y a las aplicaciones utilizando el mismo generador de reglas.

Aumenta la visibilidad

- Mantén registros de auditoría detallados en los dispositivos administrados y no administrados (en los planes de contratos, los registros DNS se almacenan durante 6 meses y los registros HTTP y de red durante 30 días)
- Envía los registros a tu SIEM preferido para fines de correlación y análisis más exhaustivos.

Capacidades de Cloudflare Gateway

Protección contra amenazas y acceso seguro	
Categorías de seguridad y aplicación	Protección integral contra ransomware, phishing, dominios DGA, tunelización de DNS, dominios nuevos y vistos recientemente, C2 y botnet, y otros riesgos de seguridad. Protección CASB en línea de 25 categorías de aplicación, incluida la IA.
Filtrado de DNS recursivo	Permite/bloquea/anula dominios y direcciones IP por categorías de seguridad o contenido. El filtrado de DNS se puede gestionar a través de nuestra API Tenant para la configuración de dominios principales y secundarios.
Filtrado e inspección de HTTP(S)	Controla el tráfico en función del origen, el destino, los dominios, los métodos HTTP, las URL y mucho más. La inspección HTTP 1/2/3 posibilita el análisis antivirus y DLP, los controles de archivos, la postura del dispositivo remoto, los inquilinos, el aislamiento del navegador y mucho más.
Inspección TLS 1.3 ilimitada	Inspección ilimitada de TLS 1.3 por defecto. Todo el tráfico HTTPS se descifra, se aplican políticas y las solicitudes se vuelven a encriptar con nuestro certificado o tu certificado personalizado, todo ello con una latencia líder en el mercado. Compatibilidad con los estándares DNS sobre TLS (DoT) y DNS sobre HTTP (DoH). Habilita solo conjuntos de encriptación compatibles con FIPS 140-2.
FWaaS de capa 4	Las políticas de red de capa 4 se aplican a todos los paquetes TCP/UDP públicos/privados para controlar el acceso a los recursos no HTTP por protocolo detectado, geolocalización, dominio SNI y más. Audita el tráfico SSH a través del puerto 22. (Funciones de FWaaS de capa 3 integradas en los servicios de red WAN).
Control antivirus	Analiza los archivos cargados/descargados de todos los tipos (PDF, ZIP, RAR, etc.) para la detección de virus.
Comprobaciones de identidad y postura del dispositivo	Establece políticas basadas en los principales proveedores de identidad corporativa, identidades sociales o estándares SAML y OIDC. Verifica la postura del dispositivo a través del cliente del dispositivo o de tu proveedor de solución de protección de puntos finales.
Información integrada sobre amenazas	La información sobre amenazas se basa en nuestros propios modelos de IA / aprendizaje automático y en fuentes de terceros. La información propia se deriva de la telemetría global como uno de los mayores soluciones de DNS autoritativo y recursivo (más de 2 billones de consultas/día). Nuestro rastreador web también indexa toda la web (más de 8000 millones de páginas) cada pocas semanas para identificar infraestructura de campaña emergente. También se admiten fuentes y firmas personalizadas (IPS , URL y dominios, entre otros).
Acceso de entrada y salida	
Con cliente de dispositivo	Reenvía el tráfico mediante proxy a través de nuestro cliente de dispositivo (WARP) por túneles completos de WireGuard o sobre DoH. Inscripción por cuenta propia o implementación a través de MDM. Habilita las comprobaciones de la postura del dispositivo. Detecta si el dispositivo está en la red.
Opciones sin cliente	Las opciones incluyen: consultas DNS enrutadas por la red desde las ubicaciones de los clientes, túneles Anycast GRE/IPsec, conector WAN , puntos finales de proxy a través de archivos PAC y aislamiento web sin cliente a través de una URL reescrita.
Compatibilidad IPv4 e IPv6	Todas las funciones disponibles para la conectividad IPv4 e IPv6 (ya sea solo IP6 o de doble pila).
Enrutamiento de tráfico	
Direcciones IP de salida dedicadas y políticas de salida	Rango dedicado de direcciones IP estáticas (IPv4 o IPv6) que se puede utilizar para incluir el tráfico en la lista de permitidos en función de la dirección IP de origen. Utiliza políticas de salida para seleccionar qué dirección IP de salida se utiliza, en función de atributos como la identidad, la geolocalización o la postura del dispositivo. Cada dirección IP de salida es única para una cuenta individual y no la utilizan otros clientes.
Políticas de resolución	Enruta las solicitudes DNS a solucionadores de DNS personalizados para llegar a dominios no enrutables públicamente, como los servicios de red privada y las aplicaciones internas. (Por defecto, las solicitudes de DNS utilizan la resolución DNS pública de Cloudflare, 1.1.1.1, una de las más rápidas y fiables del mundo).
Túnel dividido	Excluye / incluye direcciones IP o dominios para redes privadas o que se ejecutan junto con una VPN.
Visibilidad y extensibilidad	
Registro	Registro integral de todas las consultas DNS, paquetes de red de capa 4 y solicitudes HTTP inspeccionadas en cualquier puerto. Utiliza logpush o la API para la integración con las herramientas SIEM, de orquestación y de análisis existentes. Los administradores pueden optar por excluir o redactar la recopilación de información de identificación personal entre los usuarios.
Detección de Shadow IT	Monitoriza, revisa y aprueba los orígenes de redes privadas y aplicaciones SaaS que visitan tus usuarios finales a través de la solución de CASB en línea.
Personalización de páginas	Carga páginas de bloqueo HTTP personalizadas que se adapten a tu marca o transmite instrucciones para mejorar la experiencia del usuario.
Automatización	API intuitivas y proveedor Terraform disponibles para gestionar mediante programación todos los aspectos de una implementación Zero Trust / SSE. También ofrece compatibilidad de token de servicio sin usuario para servicios automatizados.

Cómo utilizan los clientes nuestra SWG

Cloudflare y Accenture protegen el acceso a Internet para la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de EE. UU.

+100 **agencias civiles de EE. UU.** protegen sus oficinas con la solución de filtrado DNS de Cloudflare

Más información

bouvet

Consultoría escandinava de informática y comunicaciones digitales

"Dependemos de Cloudflare para reducir nuestra superficie de ataque, proteger nuestros puertos, filtrar amenazas y mejorar nuestro tráfico".

- Victor Persson, jefe de operaciones de seguridad

Leer caso práctico

classmethod

Consultoría e integrador de nube japonés

4K **solicitudes bloqueadas por semana** a contenido de Internet peligroso y no deseado para cientos de empleados

Leer caso práctico

Ejemplo: Cloudflare vs. Zscaler

Criterios	Cloudflare Gateway	Zscaler Internet Access
Arquitectura	✓ Una plataforma en la nube, Un plano de control	✗ Muchas nubes fragmentadas, muchos planos de control
Interfaz de gestión	✓ Una interfaz para todos los SSE	✗ Distintas para SWG y ZTNA
Inspección de paso único	✓ SÍ para todos los servicios SSE	✗ NO
Compatibilidad únicamente con IPv6	✓ SÍ	✗ NO
SLA de tiempo activo	✓ 100 % para todos los servicios	✗ 99,999 % para la mayoría de los servicios 99,9 % para resolución DNS

Sigue comparando Cloudflare vs. Zscaler

Protección más rápida

13-58 %

más rápido con la puerta de enlace web segura (SWG)

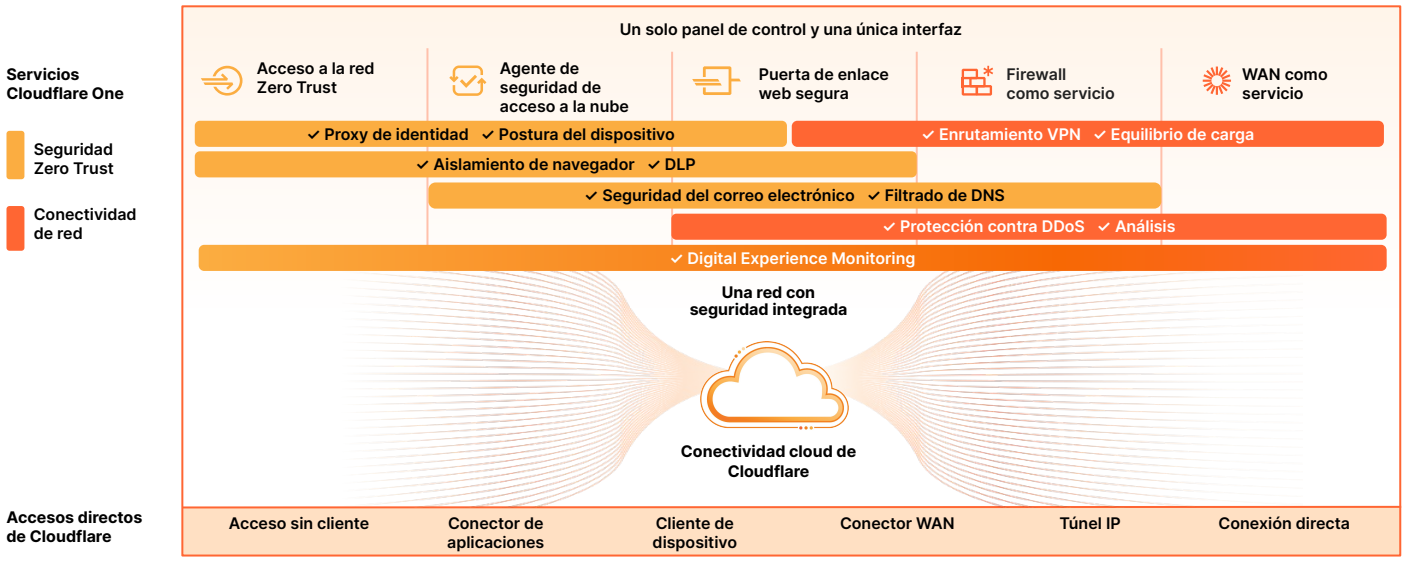
45-64 %

más rápido con el aislamiento remoto del navegador

Basado en pruebas propias y de terceros

Moderniza la seguridad con la plataforma SSE de Cloudflare

Cloudflare Gateway es un servicio componible que forma parte de Cloudflare One, nuestra plataforma SSE. Desarrolla desde tu SWG y amplía la visibilidad y los controles con las funciones de seguridad interoperables de Cloudflare One en entornos web, privados y SaaS.



Una plataforma unificada

- **Acceso seguro** mediante la verificación y la segmentación de cualquier usuario a cualquier recurso
- **Protección contra amenazas** que abarca todos los canales con información sobre amenazas y aprendizaje automático e IA basada en la red
- **Protección de datos** con mayor visibilidad y control de los datos en tránsito, en reposo y en uso

Una red programable

- **Más eficaz**, ya que simplifica la conectividad y la gestión de políticas
- **Mayor productividad** al garantizar una experiencia del usuario rápida, fiable y coherente en todas partes
- **Más ágil**, gracias a su capacidad para innovar rápidamente y satisfacer tus nuevos requisitos de seguridad

¿Necesitas más tiempo?

Si quieres más información, consulta nuestra arquitectura de referencia SASE, o comprueba cómo funciona en un recorrido interactivo por nuestra plataforma Zero Trust.