DOCUMENTO TÉCNICO

CLOUDFLARE

Introducción a SASE: Guía para proteger y optimizar tu infraestructura de red

SASE, o perímetro de servicio de acceso seguro, (en inglés, Secure Access Service Edge) simplifica la arquitectura de red tradicional incorporando servicios de seguridad y de red en una red global. Este documento analiza la evolución de la seguridad de la red que motivó el diseño de la arquitectura SASE, describe la oferta de servicios incluidos en una solución SASE y destaca una serie de pasos prácticos para su implementación.

INTRODUCCIÓN

SASE, término acuñado por Gartner en 2019, se posicionó al inicio como un avance fundamental en el proceso de transformación digital. Servicios de seguridad y de red con numerosas opciones personalizables se incorporaron sin problemas a la estructura de una plataforma global en la nube. Con una tasa de adopción del 20 % prevista para 2023, Gartner afirmó que la demanda de soluciones SASE "redefiniría la arquitectura de seguridad de redes y redes empresariales, y rediseñaría el panorama competitivo".[1]

Desde entonces, el término se ha extendido como la pólvora en el ámbito de la seguridad empresarial y de TI. La carrera de los proveedores de soluciones de seguridad de red y SD-WAN por posicionarse como líderes de SASE incorpora de manera precipitada un popurrí de servicios de seguridad y de red para empresas, cuyo enfoque se aproxima al marco SASE, si bien a menudo no lo abarca completamente.

La verdadera adopción de SASE va más allá de una combinación de soluciones específicas actuales, exige una revisión completa de la infraestructura de red empresarial. Mantener un perímetro de red sólido en las instalaciones ya no es suficiente para proteger a los trabajadores remotos y desplazados. Por otro lado, disponer de varios servicios de seguridad para proteger una infraestructura híbrida puede ser caro, complicar el trabajo de implementación y gestión de los equipos informáticos, y crear enormes brechas de seguridad.

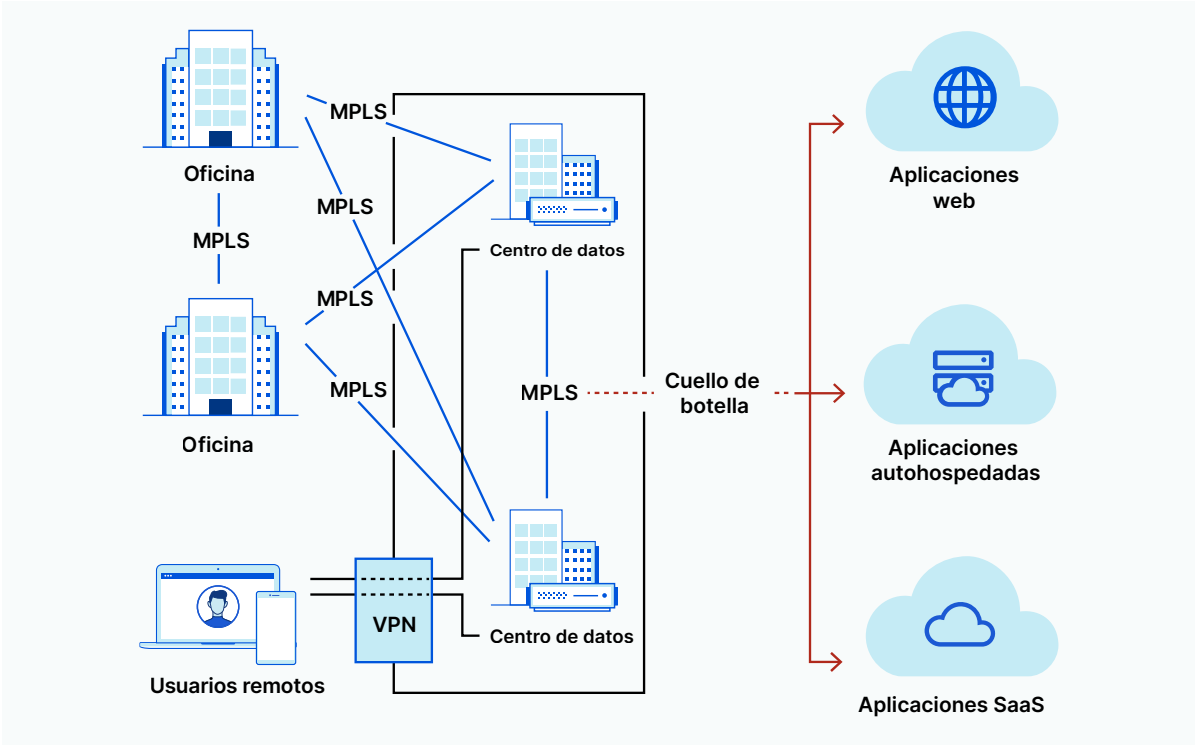
SASE aborda estos desafíos ya que cambia el perímetro de la red de los centros de datos centralizados al usuario. La consolidación de los servicios de red y de seguridad de la red que se ofrecen desde una única plataforma nativa de la nube, basada en los principios de Zero Trust, permite a SASE eliminar las brechas de seguridad entre servicios. Además, ofrece una mayor visibilidad de la actividad de la red a los informáticos y simplifica el proceso de migración a la nube.

SOBRE EL ORIGEN DE SASE - MODELO OBSOLETO

Para entender el cambio fundamental que representa SASE es importante analizar la evolución gradual de la infraestructura y seguridad de la red.

Antes de la adopción generalizada de la informática en la nube, los recursos corporativos, los datos y las aplicaciones se alojaban en instalaciones locales que estaban protegidas por firewalls de hardware y dispositivos DDoS. Los empleados de una oficina corporativa accedían a los recursos internos a través de conexiones privadas filtradas por firewalls de red. Los usuarios que se conectaban desde lugares remotos, en general, lo hacían a través de una VPN, propensa a la latencia, a una elevada sobrecarga para evitar la saturación y las vulnerabilidades de los parches, y a experiencias móviles deficientes.

La inquietud subyacente a esta configuración era la red pública, una herramienta que se creó ante todo para ser resistente, sin tener en cuenta las necesidades de rendimiento y seguridad de las empresas. Debido a que Internet había demostrado ser inherentemente vulnerable a los ataques, las organizaciones eligieron desarrollar sus propias redes privadas que protegían (a menudo, con poca eficacia) los datos, las aplicaciones y los recursos corporativos con cajas de firewall físicas y dispositivos DDoS, y redirigían todo el tráfico entrante a través de centros de datos centralizados para su inspección y filtrado.



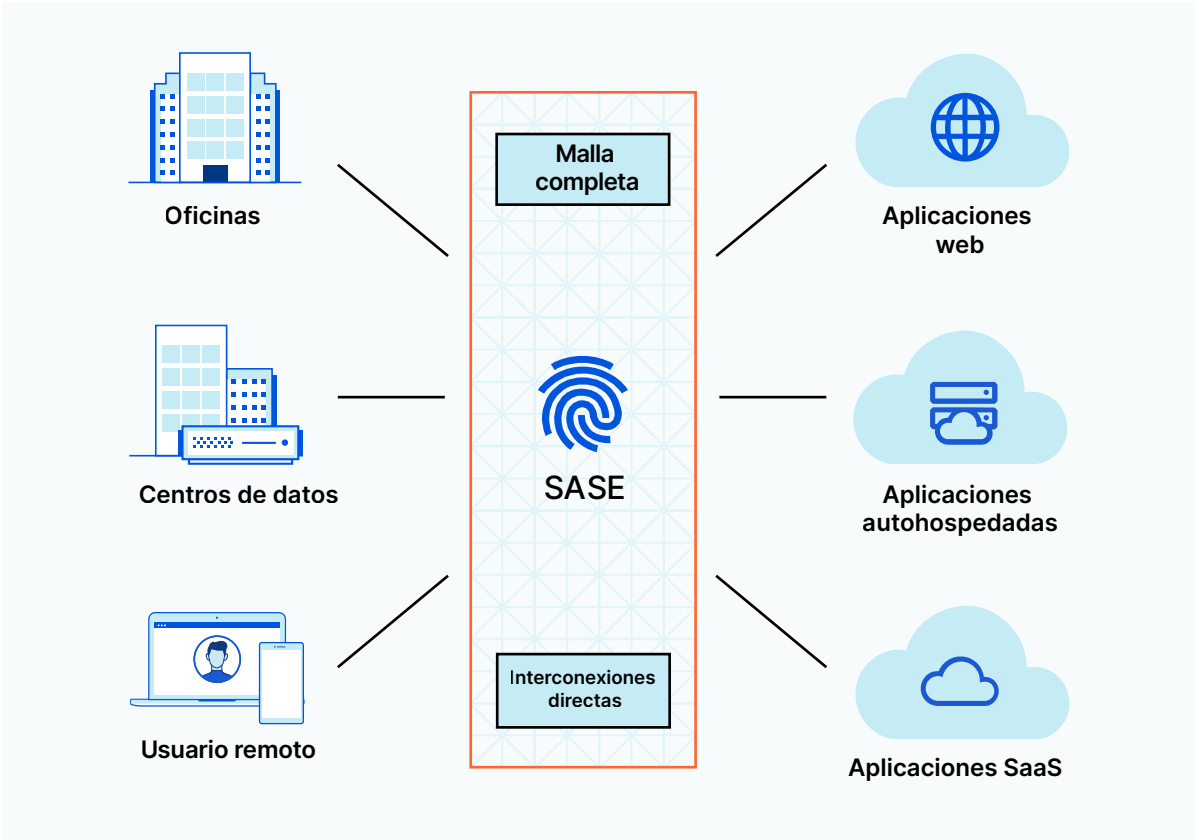
Este modelo de seguridad de red era caro y complejo, y seguía dejando a las organizaciones expuestas a fugas de datos y amenazas internas. Una vez que un atacante traspasaba el perímetro de la red, podía provocar daños importantes dentro de una organización mediante la propagación de ransomware, la apropiación de cuentas de usuarios[2] y el robo de valiosos datos de clientes.[3]

Con la llegada de los servicios en la nube y SaaS, las organizaciones tienen más libertad y flexibilidad para reinventar su infraestructura de red, ya que las aplicaciones, los datos y los empleados ya no necesitan estar solo en las instalaciones locales.

SOBRE LOS ORÍGENES DE SASE - NUEVO MODELO

Sin embargo, esa libertad viene acompañada de nuevos desafíos de seguridad. Los equipos informáticos tienen la tarea de proteger una combinación de servicios locales y en la nube, así como de proteger una fuerza laboral cada vez más desplazada y remota.[4] Lograrlo a menudo requiere mantener infraestructura cara y estratificar servicios de seguridad específicos de varios proveedores, cuya implementación y gestión puede ser lenta y difícil.

Es probable que la próxima evolución de la seguridad de la red no se parezca al hardware que protegía la infraestructura tradicional de red en estrella tipo hub-and-spoke o a las soluciones complejas que requerían una arquitectura de nube híbrida. En su lugar, será similar a un marco SASE, que consolida los servicios de red y seguridad, y los ofrece como un servicio integrado.



En lugar de depender de hardware ineficaz o parchear servicios de seguridad aislados, SASE ofrece un enfoque simplificado a la seguridad de la red. Reemplaza la complicada transmisión de datos por el perímetro de Internet, lo que permite a las empresas enrutar, inspeccionar y proteger el tráfico en un solo paso. Junto con la conectividad WAN de malla completa, las políticas de acceso Zero Trust y la protección contra amenazas a nivel de red, SASE elimina la necesidad de VPN heredadas y circuitos MPLS, además del firewall de hardware, el proxy y los dispositivos de protección contra DDoS, lo que otorga a las organizaciones más visibilidad y control sobre sus configuraciones de seguridad de red.

DEFINICIÓN DEL ALCANCE DE SASE - CAPACIDADES BÁSICAS

SASE es un modelo de seguridad en la nube que combina una red de área extensa (WAN) definida por software (SD) con servicios básicos de seguridad de red que entrega en el perímetro de la nube. La mayoría de las ofertas de soluciones SASE se caracterizan por tener cinco capacidades básicas:

Desarrollo y gestión de redes

Una red de área extensa definida por software (SD-WAN) permite a las organizaciones establecer redes corporativas privadas sin la ayuda de enrutadores de hardware ni circuitos de conmutación de etiquetas de protocolos múltiples (MPLS). Esta arquitectura virtual basada en software ofrece a las empresas una mayor flexibilidad, ya que crea y mantiene su infraestructura de red, aunque también comporta vulnerabilidades de seguridad integradas.

Filtrado del tráfico

Una puerta de enlace web segura (SWG) evita las amenazas cibernéticas y las fugas de datos mediante la filtración de contenido no deseado del tráfico web, el bloqueo del comportamiento de usuarios no autorizados y la aplicación de las políticas de seguridad de la empresa. Por lo general, incluye el filtrado de URL, la detección y el bloqueo del malware y el control de aplicaciones, entre otras funciones.

Protección de datos

Un agente de seguridad de acceso a la nube (CASB) realiza varias funciones de seguridad para los servicios alojados en la nube (p. ej., las aplicaciones SaaS, IaaS y PaaS). Los CASB estándar protegen los datos confidenciales a través del control de acceso y la prevención de la pérdida de datos, ayudan a detectar shadow IT y garantizan la conformidad de las regulaciones de privacidad de los datos.

Conexión de los usuarios con las aplicaciones

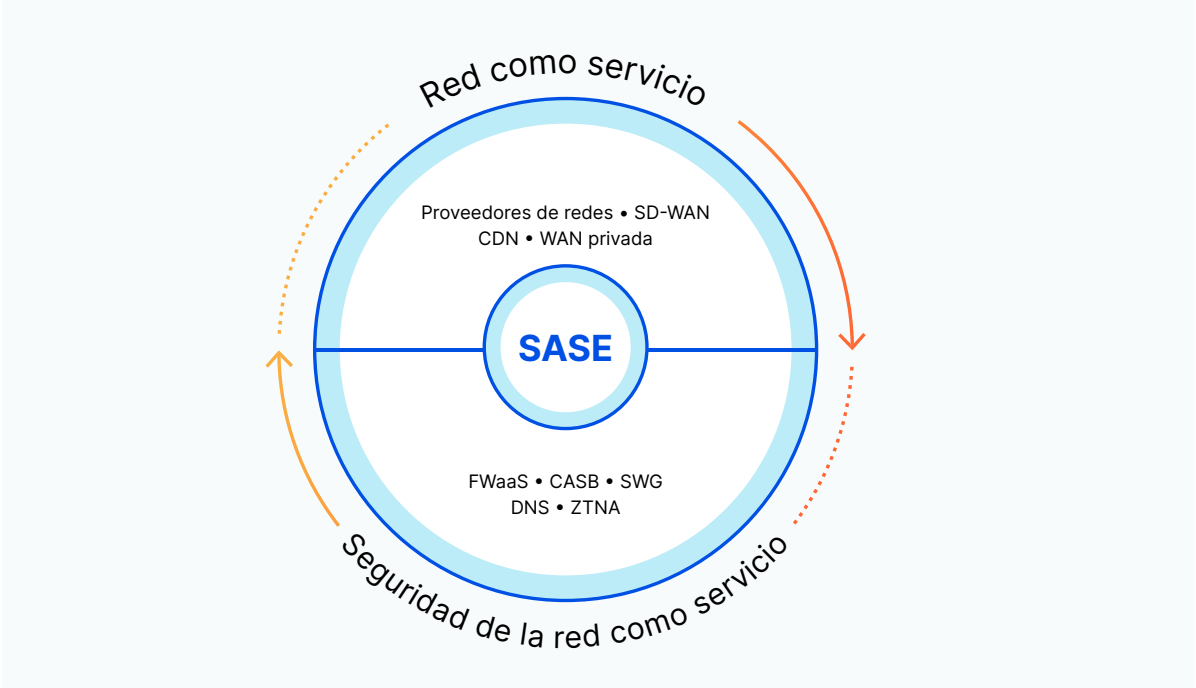
El acceso a la red Zero Trust (ZTNA) requiere la verificación en tiempo real de cada usuario a cada aplicación protegida, a fin de proteger los recursos internos y defenderse contra posibles fugas de datos. Con un enfoque "Zero Trust", se desconfía automáticamente de cualquier entidad hasta que se autentica su identidad, incluso si ya está dentro del perímetro de una red privada.

Protección de aplicaciones e infraestructura

Los firewalls en la nube (FWaaS) protegen la infraestructura y las aplicaciones en la nube de ataques cibernéticos a través de un conjunto de funciones de seguridad que incluyen el filtrado de la URL, la prevención de intrusiones y la administración de políticas uniformes.

DEFINICIÓN DEL ALCANCE DE SASE - LAS MEJORES CAPACIDADES EN SU CATEGORÍA

Aunque una solución convencional de SASE incluye los cinco servicios detallados anteriormente, la lista es más un punto de partida que un conjunto estricto de requisitos. SASE, en su esencia, reúne dos capacidades fundamentales e independientes: arquitectura de red basada en software y servicios de seguridad en la nube. Más allá de eso, los proveedores pueden añadir o quitar servicios adicionales, según sea necesario.



Si bien la red SD-WAN ayuda a los clientes a gestionar el último paso de la conectividad de la red, no puede garantizar directamente la seguridad, el rendimiento y la fiabilidad del paso intermedio entre los usuarios y las aplicaciones. En el mejor de los casos, puede optimizar las conexiones de un extremo a otro utilizando varias redes globales y encadenando varios servicios de seguridad, un proceso que es difícil y caro. Un proveedor de SASE que haya desarrollado una WAN como servicio desde cero, con o sin SD-WAN, permite a los clientes gestionar solo una red global con seguridad, rendimiento y fiabilidad incorporados por defecto. Juntos, SWG, CASB y ZTNA reducen en gran medida los riesgos de seguridad, aunque dejan aún muchas brechas para la protección de datos y amenazas en todos los casos de uso. Un proveedor de SASE que ha desarrollado el aislamiento remoto del navegador desde cero para integrarse de forma nativa con SWG, CASB y ZTNA dentro de cada centro de datos elimina esas brechas.

VENTAJAS DE UN ENFOQUE SASE

La implementación de soluciones SASE, cuya evolución continúa, puede variar de manera considerable entre proveedores y organizaciones. La mayoría de las soluciones SASE, sin embargo, comparten varias ventajas fundamentales sobre las configuraciones de seguridad de las redes locales e híbridas:

Implementación simplificada

La consolidación de servicios de seguridad y red permite a SASE eliminar la necesidad de incorporar servicios basados en la nube, establecer dispositivos en las instalaciones e invertir tiempo, dinero y recursos internos para mantener ambos actualizados contra las últimas amenazas.

Gestión de políticas sencilla

SASE permite que las organizaciones establezcan, supervisen, ajusten y apliquen políticas de acceso sobre todas las ubicaciones, usuarios, dispositivos y aplicaciones. Los ataques y las amenazas entrantes se pueden identificar y mitigar desde un portal único, en lugar de tener que realizar de manera individual la supervisión y gestión de varias herramientas de seguridad de una sola función.

Acceso a la red basado en la identidad

SASE depende en gran medida de un modelo de seguridad Zero Trust, en el que la identidad del usuario y el acceso se conceden en función de una combinación de factores: ubicación del usuario, hora del día, estándares de seguridad de la empresa, políticas de conformidad y una evaluación continua de riesgo y confianza. Este nivel de seguridad, que representa un paso significativo con respecto a las, VPN que son demasiado permisivas e intrínsecamente vulnerables, protege contra las fugas de datos tanto externas como internas y otros ataques.

Disminución de la latencia

SASE reduce la latencia y optimiza el rendimiento al enrutar el tráfico de red a través de una amplia red perimetral en la que el tráfico se procesa lo más cerca posible del usuario. La optimización del enrutamiento puede ayudar a determinar la ruta de red más rápida en función de la congestión de la red y otros factores.

Red global

El marco SASE se erige sobre una red global única, lo que permite a las organizaciones ampliar su perímetro de red a cualquier usuario, sucursal, dispositivo o aplicación y obtener más visibilidad y control en toda su infraestructura de red.

INTRODUCCIÓN A SASE

Para aquellas empresas que han invertido tiempo, recursos y dinero en complejas configuraciones en entornos locales, que gestionan difíciles entramados de redes de servicios de seguridad en la nube, o siguen adaptándose al futuro del teletrabajo, la adopción de SASE puede parecer abrumadora, pero no tiene por qué serlo.

A continuación, detallamos cinco pasos prácticos que puedes seguir para empezar con SASE:

1. Protege a tus equipos remotos.

Implementa una solución ZTNA que te permitirá reducir la dependencia de tu VPN o incluso sustituirla, proteger los datos y recursos corporativos de las amenazas internas y externas, y mejorar la experiencia del usuario. La migración de tu puerta de enlace web segura, el firewall y los navegadores de los dispositivos al perímetro te permitirá filtrar, aislar e inspeccionar el tráfico evitando así el retorno a través de un centro de datos central.

2. Afianza las sucursales detrás de un perímetro en la nube.

Aplica una arquitectura Zero Trust a las sucursales para eliminar la necesidad de dispositivos de seguridad locales (gestión unificada de amenazas, etc.), cuyo mantenimiento puede resultar caro e ineficaz frente a un panorama de amenazas en rápida evolución.

3. Migra la protección contra DDoS al perímetro.

Pon fin a los dispositivos DDoS y protege las redes corporativas de los ataques con una protección DDoS nativa de la nube y de la capa de red que pueda detectar y mitigar las amenazas en tiempo real.

4. Migra las aplicaciones a la nube.

A medida que escala tu organización, migra las aplicaciones autohospedadas de tus centros de datos a la nube y asegúrate de aplicar políticas de seguridad de red coherentes en todo el tráfico.

5. Sustituye los dispositivos de seguridad locales por una aplicación de políticas unificada y nativa de la nube.

Reduce el coste y la complejidad del mantenimiento de los dispositivos de hardware de red migrando la aplicación de políticas al perímetro, donde puedes supervisar de una sola pasada y gestionar en un solo panel todo el tráfico, los patrones de ataque y las políticas de seguridad.

LA SOLUCIÓN SASE DE CLOUDFLARE ES CLOUDFLARE ONE

Cloudflare One es una plataforma de red como servicio Zero Trust que conecta dinámicamente los usuarios con los recursos corporativos mediante controles de seguridad basados en la identidad que se aplican cerca de los usuarios, estén donde estén.

Con los servicios de red de Cloudflare One, los equipos de infraestructura pueden:	**Con los servicios Zero Trust de Cloudflare One, los equipos de seguridad informática pueden:**
• Utilizar la red global de Cloudflare como su WAN. • Sustituir los dispositivos heredados por un firewall de red nativo de la nube. • Optimizar el rendimiento de las aplicaciones y la latencia del usuario final.	• Conectar a los usuarios con los recursos de manera sencilla y segura sin VPN. • Bloquear el movimiento lateral, el ransomware, el malware y la suplantación de identidad. • Mejorar la experiencia del usuario final y el trabajo administrativo, especialmente durante la integración.

¿Por qué Cloudflare?

Facilidad de implementación y gestión

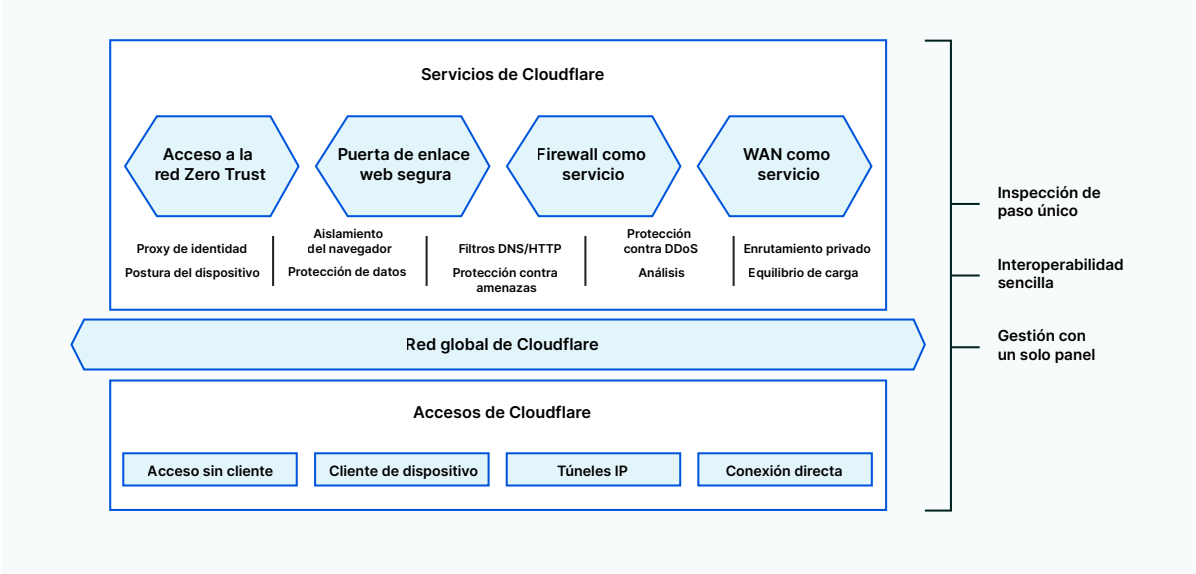
Todos los servicios de Cloudflare One se ejecutan en cada una de nuestras más de 250 ciudades en todo el mundo. Sin necesidad de integrar manualmente diferentes productos específicos mientras avanzas al modelo SASE.

Seguridad y velocidad consistentes en cualquier lugar del mundo

Todos los centros de datos de Cloudflare proporcionan enrutamiento e inspección del tráfico en un paso único, lo que permite ofrecer la misma protección a todos los usuarios de cualquier parte del mundo, todo ello sin perder velocidad a causa de la latencia o el "efecto tromboning".

Se conecta con lo que ya usas

Cloudflare gestiona la red más potente y conectada del mundo, y Cloudflare One es compatible con los proveedores de identidad, punto de conexión y nubes que utilizas. Facilidad de uso e integración inmediata.



LA SOLUCIÓN SASE DE CLOUDFLARE ES CLOUDFLARE ONE

Cloudflare One ofrece las capacidades de seguridad y conectividad que necesitas para conectar usuarios, aplicaciones y sucursales en el mundo del teletrabajo.

<table>
<tr><th colspan="2">Cloudflare One</th></tr>
<tr><td>Acceso a la red Zero Trust
Conecta a cualquier usuario con cualquier aplicación y red privada con más rapidez y seguridad que una VPN, aplicando reglas basadas en la identidad y el contexto limitando a la vez el movimiento lateral.

Capacidades principales de SASE:
• Conecta a los usuarios con las aplicaciones
• Protección de datos</td><td>WAN como servicio
Habilita la conectividad universal con rendimiento más rápido, seguridad incorporada y mayor resistencia sustituyendo tu arquitectura WAN tradicional por nuestra red troncal privada global.

Capacidad principal de SASE:
• Creación y gestión de redes</td></tr>
<tr><td>Puerta de enlace web segura
Bloquea amenazas de Internet conocidas o desconocidas, y controla fácilmente los flujos de datos, aplicando reglas de aislamiento de DNS, HTTP, red y navegador con inspección SSL ilimitada.

Capacidades principales de SASE:
• Filtrado e inspección del tráfico
• Protección de datos</td><td>Firewall como servicio
Controla el acceso, y bloquea los ataques DDoS y otras amenazas, aplicando reglas de inspección de estado en todo el tráfico entrante y saliente, manteniendo al mismo tiempo la agilidad del rendimiento.
Capacidad principal de SASE:
• Protección de aplicaciones e infraestructura</td></tr>
<tr><td colspan="2">Red global de Cloudflare
Nuestra red, que se encuentra a menos de 50 ms del 95 % de la población conectada a Internet, opera en más de 250 ciudades. Cuenta con una capacidad de más de 100 Tbps, más de 10.000 interconexiones y un acuerdo de nivel de servicio del 100% de tiempo activo.</td></tr>
<tr><td>Acceso sin cliente
Incorpora usuarios o dispositivos a tu empresa en cuestión de minutos, incluso usuarios externos o con dispositivos privados, usando un acceso seguro basado en el navegador a aplicaciones SaaS y autohospedadas, y no solo el protocolo HTTP.</td><td>Túneles IP
Integra subredes públicas y privadas completas a través de anuncios de ruta BGP Anycast con túneles GRE, o nuestro propio conector Tunnel en entornos de nube o locales.</td></tr>
<tr><td>Cliente de dispositivo
Integra dispositivos Windows, macOS, iOS, Android, ChromeOS y Linux para un acceso seguro basado en el cliente en cualquier aplicación, red privada o destino de Internet.</td><td>Conexión directa
Integra tu infraestructura de red física o virtualmente en más de 1.600 ubicaciones conjuntas, en lugar de hacerlo en la red pública de Internet, para lograr experiencias más seguras y fiables.</td></tr>
</table>

RESULTADOS EMPRESARIALES CON CLOUDFLARE ONE

↓91 %

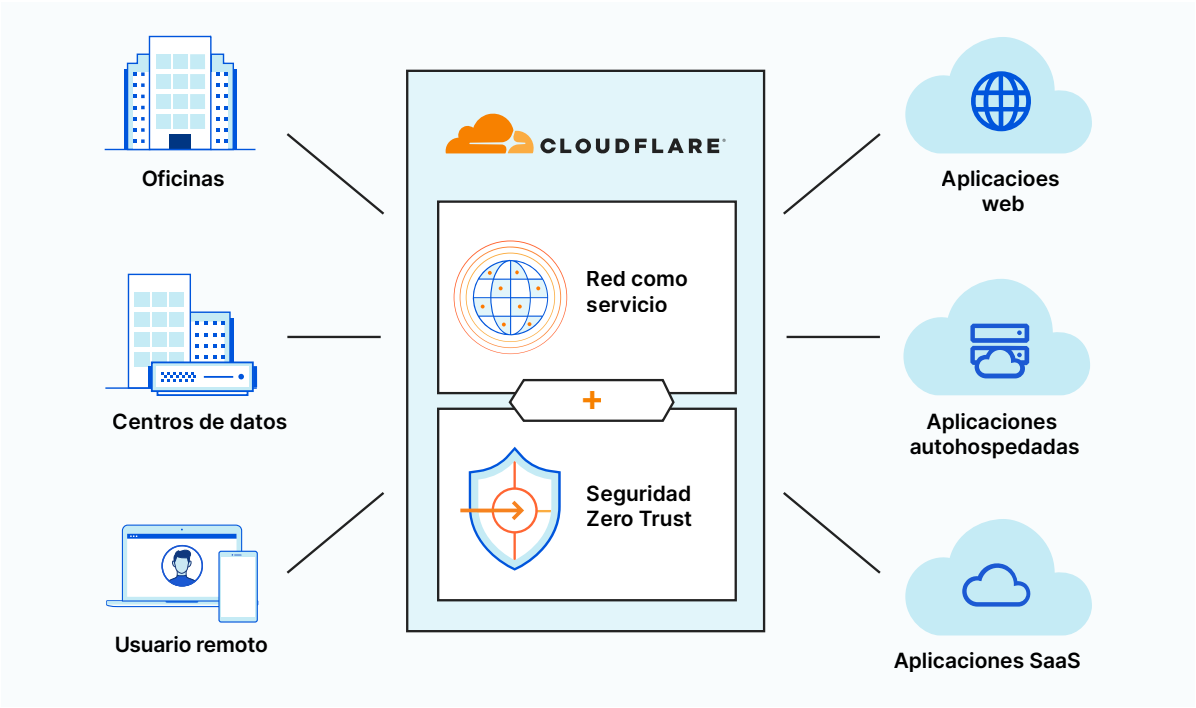
Reduce la superficie de ataque hasta un 91 % al aislar la navegación de alto riesgo de los usuarios y el acceso a aplicaciones desde las redes.

10 → 1

Disminuye el coste total de las operaciones y agiliza tu negocio combinando hasta 10 productos específicos en una plataforma.

↑60 %

Incorpora nuevos empleados y proveedores hasta un 60 % más rápido conectando a los usuarios con los recursos a través de Cloudflare en lugar de una VPN.



Más información sobre Cloudflare One

Haz clic aquí

REFERENCIAS

1. Gartner, “The Future of Network Security Is in the Cloud.” Analyst(s): Neil MacDonald, Lawrence Orans, Joe Skorupa. 30 de agosto de 2019. Gartner.

2. Twitter Inc. “An update on our security incident.” Twitter. Consultado el 27 de octubre de 2020.

3. Marriott International News Center. “Marriott International Notifies Guests of Property System Incident.” Marriott. Consultado el 27 de octubre de 2020.

4. Bursztynsky, Jessica. “Dropbox is the latest San Francisco tech company to make remote work permanent.” CNBC. CNBC. Consultado el 27 de octubre de 2020.