

WAN como servicio

Magic WAN simplifica la adopción de SASE con la conectividad universal

La evolución de las arquitecturas de red

Internet es la nueva red corporativa

Con el trabajo híbrido como la nueva normalidad y la migración de las aplicaciones a la nube, los equipos informáticos afrontan diversos desafíos:

- **Complejidad de la red:** el suministro MPLS y los ajustes de soluciones específicas requieren demasiado tiempo.
- **Vulnerabilidades de seguridad:** los usuarios distribuidos y los dispositivos personales suponen más riesgo para los datos corporativos.
- **Costos elevados:** los enlaces MPLS y las soluciones específicas de seguridad crean gastos innecesarios.
- **Experiencia de usuario deficiente:** el redireccionamiento del tráfico para aplicar las medidas de seguridad añade latencia.

Magic WAN simplifica la conectividad de red desde las filiales, las VPC multinube o los centros de datos a la plataforma SASE [Cloudflare One](#). Así, garantizamos una conectividad segura, eficaz y rentable para resolver los desafíos del trabajo híbrido y de las implementaciones multinube a los que se enfrentan los equipos de TI.

A diferencia de la red [MPLS](#), rígida y costosa, o de las excesivas implementaciones [SD-WAN](#) basadas en firewalls locales, Magic WAN adopta un enfoque "sucursal ligera, nube pesada" para mejorar o finalmente reemplazar tu arquitectura actual. Es más fácil de implementar, gestionar y utilizar, y se escala al ritmo de tus requisitos empresariales, todo ello con seguridad integrada.



Magic WAN conecta las ubicaciones de la red física o virtual con la plataforma SASE de Cloudflare. Los sitios físicos, incluyen, entre otros, filiales, plantas de producción, puntos de venta, oficinas centrales o centros de datos. Las ubicaciones virtuales pueden ser, por ejemplo, servicios de nube pública como AWS, Azure, GCP y OCI.



Mejor agilidad operativa

Gestiona de forma centralizada la seguridad y la conectividad de la red desde una única interfaz. Permite el acceso de tráfico en cuestión de minutos con la configuración Zero Touch.



Seguridad integrada, no adicional

Benefíciate de la protección contra DDoS nativa en la nube, el firewall de red y la funcionalidad SSE y Zero Trust, todo plenamente integrado y ofrecido como servicio.



Menores costos de red

Minimiza la ocupación de espacio de tus sucursales y migra las funciones de red a la nube para reducir la dependencia de costosas implementaciones MPLS o SD-WAN.

Principales casos de uso de Magic WAN

Optimizar la conectividad de la red

- ★ **Simplifica la conectividad de las filiales** — Sustituye un entramado de circuitos y dispositivos de red propios para dirigir de forma segura el tráfico entre las filiales y los centros de datos. Facilita la conectividad entre sitios en las distintas ubicaciones con Anycast IPsec.
- **Simplifica la conectividad híbrida y multinube** — Las organizaciones tienen aplicaciones en instancias en la nube de distintos proveedores (p. ej. AWS, GCP, Azure, Oracle, IBM) y centros de datos locales. Utiliza controles centralizados para dirigir y proteger el tráfico entre esta gran variedad de entornos.

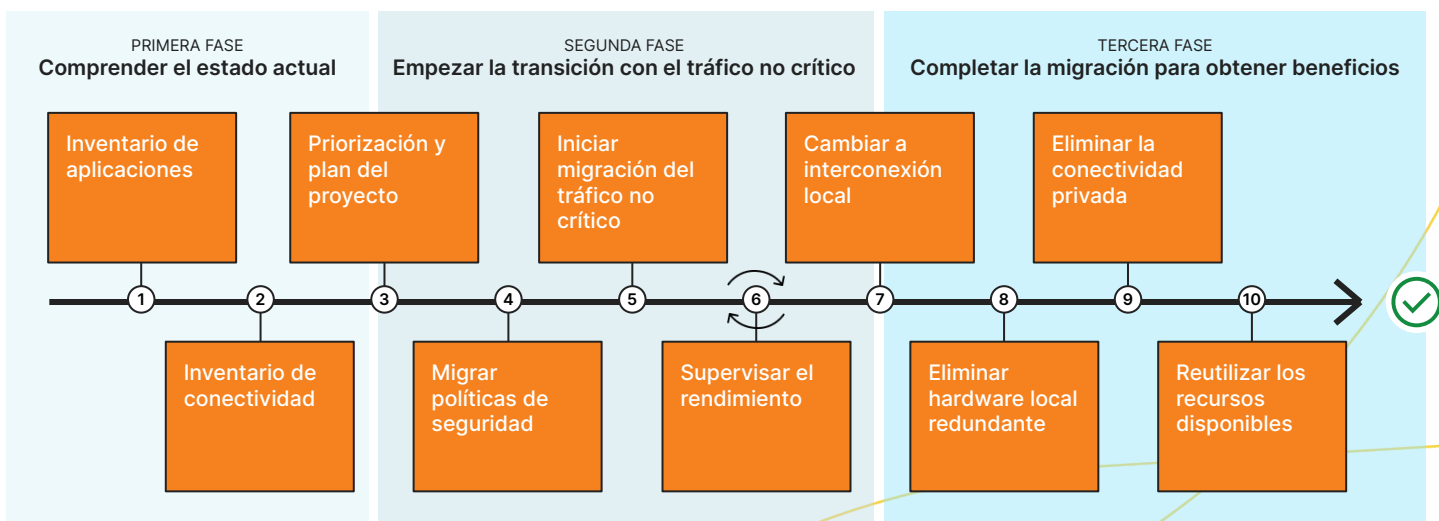
Mejorar la seguridad sin sacrificar el rendimiento

- **Protege la conectividad la WAN** — Aplica filtrado e inspecciones del tráfico entre las ubicaciones (filiales, centros de datos, etc.), y del tráfico hacia/desde esas ubicaciones (desde/hacia Internet global), añadiendo firewalls y controles SWG a WAN.
- **Escala el rendimiento de la WAN** — Las implementaciones MPLS han sido costosas de crear y lentas de escalar. La eliminación de MPLS y la adopción de una WAN en la nube ofrece una implementación más ágil y más económica con seguridad integrada.

Cómo abordar la implementación de Magic WAN

La transformación de la red es un proceso a largo plazo, durante el que lograrás pequeñas victorias

Magic WAN ofrece un rendimiento y una fiabilidad iguales a los de MPLS en la red pública de Internet a fin de proporcionar una ruta de migración desde las arquitecturas de red existentes. Empieza poco a poco con una prueba piloto de la migración del tráfico no crítico, y gradualmente descarga más tráfico a lo largo del tiempo. La combinación "sucursal ligera, nube pesada" de Cloudflare de conectividad de última milla y rendimiento, fiabilidad y seguridad de milla intermedia conecta y protege mejor el trabajo híbrido. Nuestra arquitectura nativa de Internet puede implementarse junto con las implementaciones SD-WAN existentes allí donde sea necesario o bien sustituir por completo la necesidad de nuevas implementaciones SD-WAN.



Comparación entre MPLS y SD-WAN

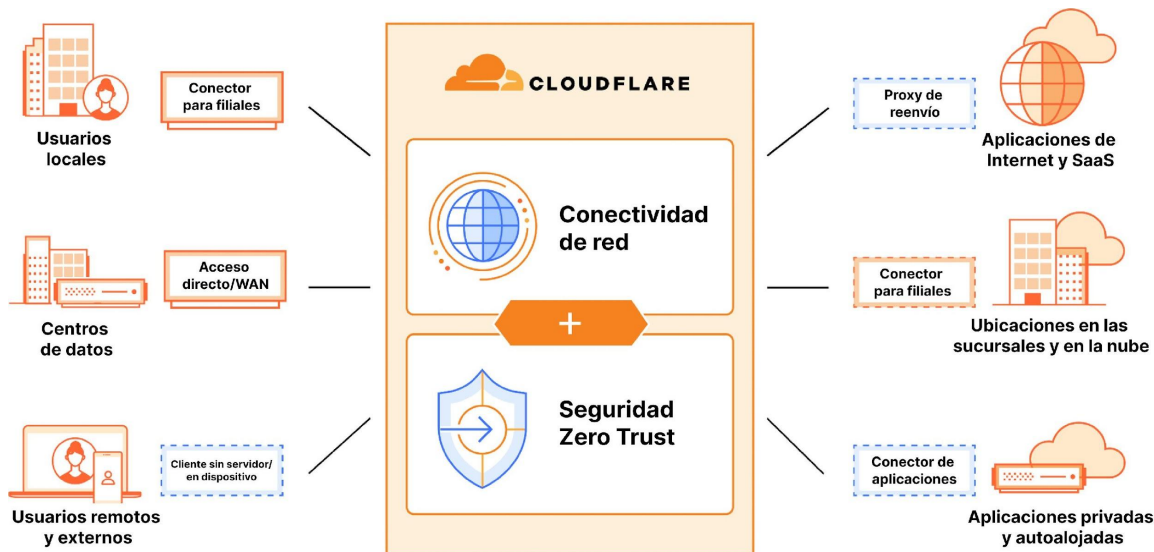
Tradicionalmente, las organizaciones han confiado en los circuitos MPLS para obtener una conectividad WAN eficaz y fiable. Con la migración de las aplicaciones a la nube y las opciones de trabajo más flexibles de los usuarios, este modelo está dejando de ser válido. A pesar de que el tráfico está cada vez más distribuido, los equipos de seguridad aún aplican mecanismos de control mediante ubicaciones de "interconexión" centralizadas, redirigiendo todo el tráfico a través de un entramado de dispositivos de seguridad. En concreto, dado que su costo aumenta para las implementaciones más grandes, MPLS no puede cubrir eficazmente las necesidades modernas.

Más recientemente, SD-WAN ayudó a mejorar las dificultades de la orquestación con interfaces web intuitivas y centralizadas, y se implementaron funciones de enrutamiento inteligente a nivel local a fin de mejorar la toma de decisiones instantánea acerca de cómo dirigir y definir el tráfico en la última milla. Sin embargo, los dispositivos SD-WAN aún no suelen tener controles de seguridad integrados, por lo tanto, para cubrir esta necesidad los equipos deben combinar una amalgama de herramientas de hardware, virtualizadas y en la nube. Aunque la promesa de la finalización de los contratos de MPLS llevó a las organizaciones a esperar una reducción de los costos, en general, no lo han conseguido. La razón: los costos de hardware nuevo, de licencias o de mantenimiento, o que finalmente no han podido sustituir MPLS debido a las deficiencias de seguridad y fiabilidad de SD-WAN.

La plataforma SASE de Cloudflare fusiona la seguridad y la red en nuestra conectividad cloud para entregar todo el tráfico mediante un enfoque "sucursal ligera, nube pesada", que permite a las organizaciones abandonar los circuitos privados heredados y utilizar nuestra red como una extensión de la suya propia. La gestión simplificada, el rendimiento fiable, la seguridad Zero Trust moderna y el menor costo total de propiedad solo son posibles si se combinan con un enfoque realmente nuevo: el que representa la arquitectura de diseño SASE para las organizaciones que están en proceso de modernización digital.

Aspecto	Ejemplo	Servicio MPLS/VPN	SD-WAN	SASE con Cloudflare One
Configuración	Configuración y gestión de sitios nuevos	MSP mediante solicitud de servicio	Orquestación y gestión simplificadas mediante controlador centralizado	Orquestación automatizada mediante el portal de SaaS; panel de control centralizado
Control del tráfico de la última milla	Equilibrio del tráfico, QoS y conmutación por error	Cubierto por los SLA de MPLS	Selección de mejor ruta disponible en dispositivo SD-WAN	Implementación local mínima para controlar la toma de decisiones locales
Control del tráfico de la milla intermedia	Direccionar el tráfico para sortear la congestión de la milla intermedia	Cubierto por los SLA de MPLS	"Túnel Spaghetti" y aún sin control de la milla intermedia	Gestión del tráfico y controles de redes troncales privadas integrados en la misma interfaz
Integración de la nube	Conectividad para la migración a la nube	Interconexión centralizada	Interconexión descentralizada	Conectividad nativa con interconexión de red en la nube
Seguridad	Filtrar el tráfico de Internet de entrada y salida para evitar malware	Amalgama de controles de hardware	Amalgama de controles de hardware y/o de software	Integración nativa con herramientas de seguridad de los usuarios, los datos, las aplicaciones y las redes
Costos	Maximizar el ROI de las inversiones de red	Costo alto del hardware y la conectividad	Costos de conectividad optimizados en detrimento de mayores costos de hardware y de software	Menores costos de hardware y de conectividad para maximizar el ROI

Acceso del tráfico a la plataforma SASE de Cloudflare



Magic WAN Connector facilita la conexión de tus ubicaciones de red a Cloudflare. Compra el software del conector para filiales preinstalado y configurado en un dispositivo de hardware certificado por Cloudflare para lograr la implementación más sencilla posible, o bien instala el software en dispositivos Linux físicos o virtuales en tu entorno.

Parte de una familia de accesos flexibles en crecimiento

El primer paso para la adopción de [SASE](#) es la conexión: establecer una ruta segura desde tu red existente a la ubicación más cercana donde se pueden aplicar políticas de seguridad Zero Trust. Cloudflare ofrece un amplio conjunto de "accesos" para posibilitar esta conectividad. Estos incluyen las opciones de acceso basadas en cliente y sin cliente para los usuarios de trabajo híbrido, los túneles de capa de aplicación establecidos mediante la implementación de un daemon de software ligero, la conectividad de red con túneles GRE o IPsec habilitados para Anycast y la interconexión física o virtual tanto para centros de datos privados como para nubes públicas.

Para facilitar aún más este primer paso hacia SASE, Magic WAN Connector se puede implementar en cualquier red física o en la nube para proporcionar conectividad automática a la ubicación de la red de Cloudflare más cercana. Para ello, utiliza la conectividad de Internet de última milla existente y elimina la necesidad de que los equipos informáticos deban configurar manualmente los dispositivos de red para la conexión.

Funcionalidades del software y especificaciones del hardware

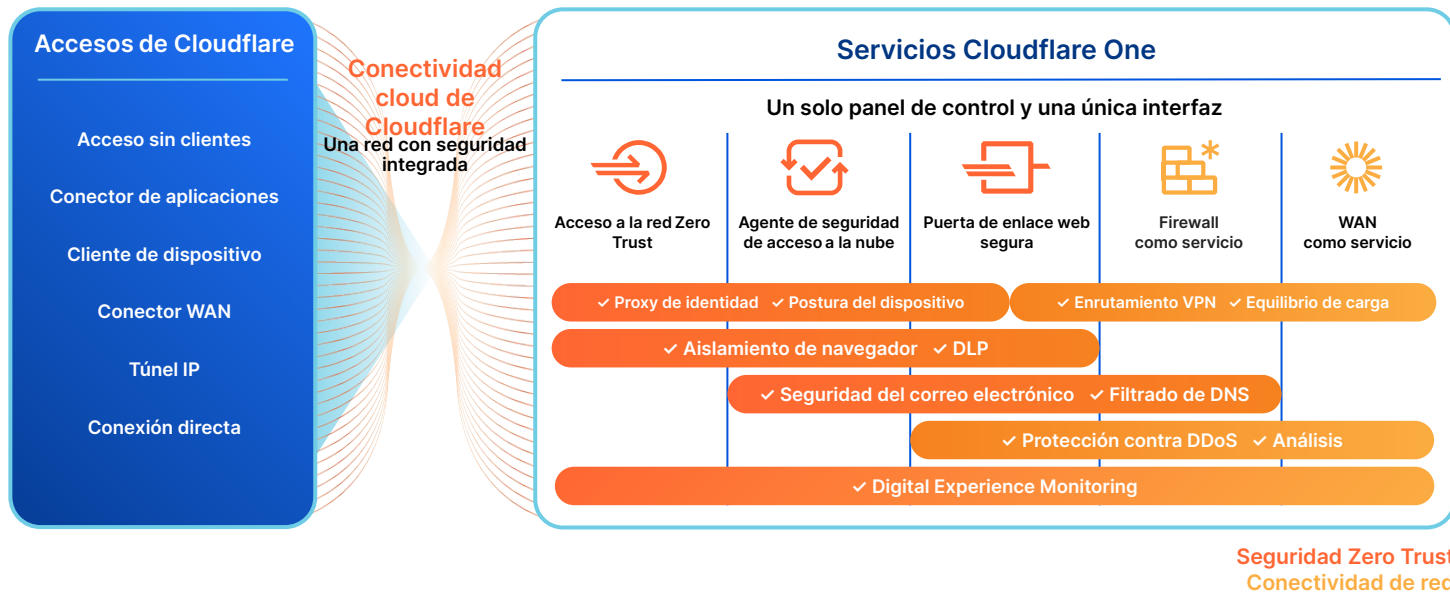
Funcionalidades del software de Magic WAN ¹	
Configuración del conector WAN	Se suministran dispositivo(s) local(es) del cliente (CPE) Zero-Touch y Plug and Play que se gestionan de forma centralizada mediante el panel de control/API de Cloudflare. Configura automáticamente túneles IPsec y rutas para dirigir el tráfico a la red de Cloudflare para lograr conectividad y seguridad. Actualizaciones automáticas del software a lo largo del tiempo (en la ventana de servicio que defina el cliente).
Configuración del sitio del conector WAN	Compatibilidad de WAN/LAN con las configuraciones de IP estática o DHCP existentes en cada sitio. Compatibilidad con las VLAN y la segmentación de red local.
Enfoque "sucursal ligera, nube pesada"	Equilibrio de carga y conmutación por error del conector WAN local en múltiples circuitos WAN según las comprobaciones de estado. Las funcionalidades SSE de Zero Trust y de firewall con mayor uso de recursos se suministran desde la conectividad cloud de Cloudflare en la milla intermedia.
Integración de terceros	Configura puntos finales de túnel Anycast IPsec o GRE con tus VPC en la nube existentes, como Amazon AWS Transit Gateway o el equipo local del cliente (CPE) como dispositivos de SD-WAN, firewall y enrutador. Configura rutas estáticas con el reenvío de paquetes ECMP a la red de Cloudflare.
Seguridad integrada	Integración de firewall y detección de intrusiones en la capa 3; completa integración con otras funcionalidades de SSE/seguridad y accesos como la puerta de enlace web segura en las capas 4-7, cliente de dispositivo, conector de aplicaciones, etc.
Visibilidad y control	Visibilidad/análisis para métricas de túneles, tráfico y dispositivos disponibles mediante el panel de control, la API, los registros o GraphQL. Control mediante el panel de control de Cloudflare, la API o Terraform.
Especificaciones de las opciones de hardware de Magic WAN Connector ²	
Especificaciones del dispositivo	• Puertos: (6× 1G Copper RJ45) + (2× 10G SFP+) + (2x USB 3.0 Tipo A) • Dimensiones: 8,1×7,9×2,0 pulgadas; 1,5RU; Peso: 1,3 kg • Opciones de montaje: colocación sobre escritorio, montaje en pared o montaje en bastidor (con bandeja) • TPM: 2.0, en todo el mundo, excepto China • CPU: Denverton 4 Núcleo C3558 • Unidad: M.2 120 SSD con eMMC Flash de 16 GB • RAM: DDR4 de 8 GB • WiFi y Bluetooth: 802.11ac, 2×2 MIMO, velocidad física máx.: 866,7 Mb/s • Ventilador: uno

¹ Toda la información sobre las características de Magic WAN se encuentra en los [documentos de Cloudflare](#)

² Hardware con la certificación de Cloudflare y software de Magic WAN preinstalado: [Dell VEP 1425](#) vendido a través de socios (se proporciona con montaje en bastidor)

Conectividad de red y recorrido hacia SASE

La conectividad cloud de Cloudflare ofrece la simplicidad de implementación, la resiliencia de red y la velocidad de innovación necesarias para seguir a la vanguardia mientras consolidas productos específicos y los fusionas en una estrategia de TI unificada.



Cloudflare One permite a las organizaciones de cualquier tamaño llevar a cabo la [transición a SASE](#): conectar cualquier fuente y destino de tráfico a una red global segura, rápida y fiable donde se aplican todas las funciones de seguridad y el tráfico se optimiza hacia su destino, tanto si está en una red privada como en la red de Internet pública.

Independientemente de si deseas descargar el tráfico de implementaciones MPLS o SD-WAN consolidadas de tu organización o si abor das la transformación de la red por primera vez, Magic WAN puede ayudarte con la modernización. Cloudflare One brinda seguridad Zero Trust y WAN como servicio para ofrecer SASE como proveedor integral, pero también puede complementar una estrategia con distintos proveedores mediante sus componentes para ayudarte en el punto del recorrido donde te encuentres en la adopción de SASE.

Analicemos la conectividad de red para tu organización

Solicitar seminario



¿Necesitas más tiempo?

Más información sobre la [plataforma SASE de Cloudflare](#)