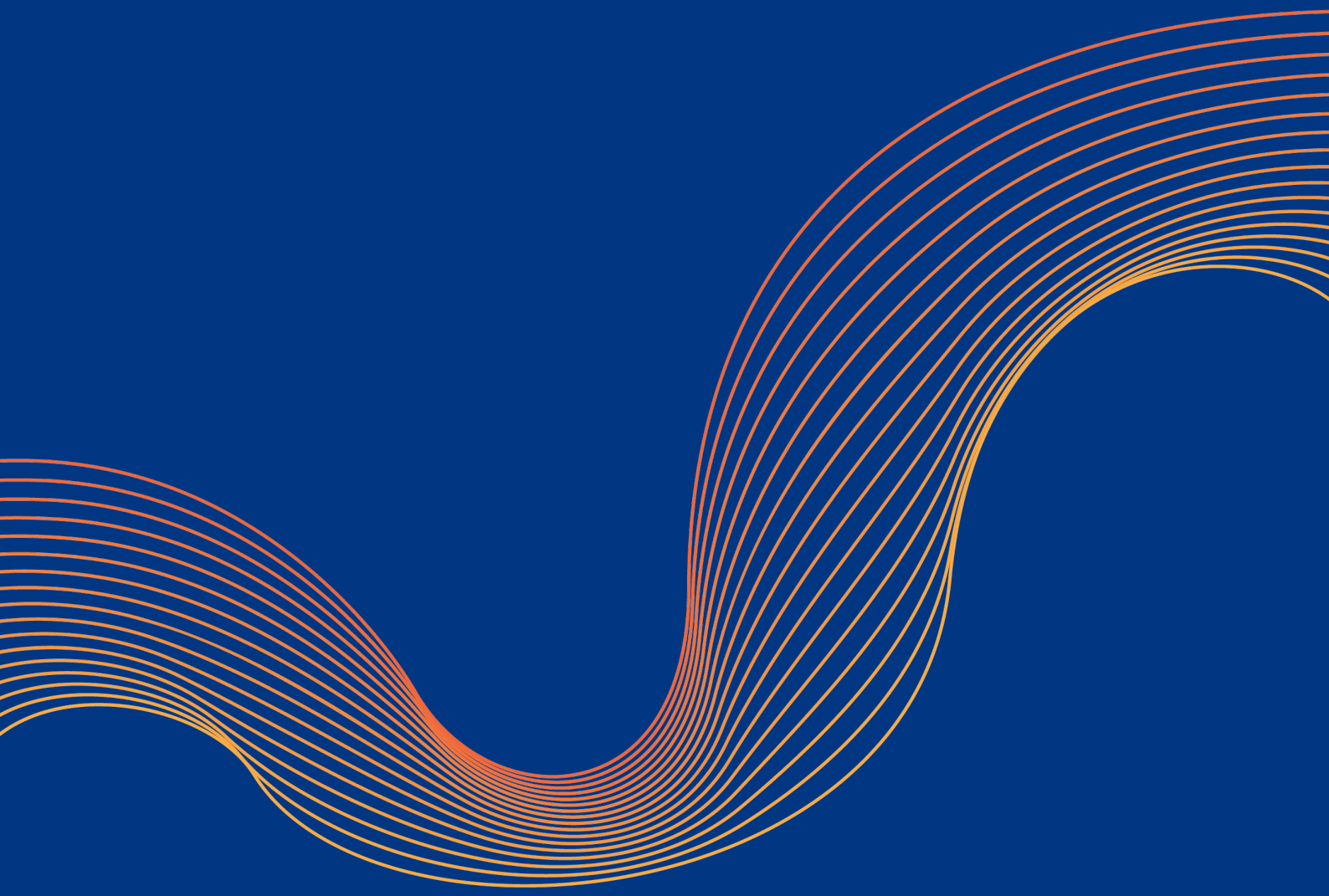
DOCUMENTO TÉCNICO

CLOUDFLARE

¿Pueden las soluciones de seguridad de ZTNA reemplazar tu VPN? Compara 3 enfoques de acceso remoto



+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com

ÍNDICE

INTRODUCCIÓN

Un acceso remoto seguro y eficiente es un instrumento para facilitar las actividades de las empresas, ya que impulsa la productividad de los usuarios remotos y reduce el tiempo que dedican los equipos informáticos a incorporar y mantener la conectividad entre usuarios y aplicaciones con agilidad y flexibilidad. Sin embargo, el acceso remoto sigue siendo un desafío para muchas organizaciones.

Hace tiempo, las VPN ofrecían una forma sencilla de comunicar a algunos usuarios remotos con las redes corporativas durante breves periodos de tiempo. Sin embargo, a medida que los empleados empezaron a estar más distribuidos y las organizaciones necesitaban mantener a los usuarios remotos conectados de forma segura durante periodos más largos, quedaron patentes las deficiencias de este enfoque, tales como la ralentización del rendimiento y el aumento de los riesgos de seguridad, así como los problemas de escalabilidad.

Conforme crecen las necesidades del acceso remoto, las organizaciones se alejan cada vez más de las implementaciones tradicionales de VPN, y optan por soluciones más seguras y eficaces. El acceso a la red Zero Trust (ZTNA) crea límites seguros en torno a aplicaciones específicas, direcciones IP privadas y nombres de servidor, y reemplazan las conexiones VPN que permiten de forma predeterminada por políticas de denegación por defecto que conceden acceso en función de la identidad y el contexto.

En 2020, las soluciones de ZTNA supusieron en torno al 5 % de todo el uso de acceso remoto. Debido a las limitaciones del acceso tradicional a las VPN y la necesidad de ofrecer un control de acceso y de sesión más preciso, se estima que esa cifra aumente hasta el 40 % en 2024.[1]

Si bien las soluciones de ZTNA ofrecen a las empresas varias ventajas claras, y funcionalidades adicionales, sobre las VPN, muchas organizaciones han considerado que es un sustituto incompleto de la infraestructura VPN. Sin embargo, a medida que las soluciones de ZTNA se vuelven más sólidas y las VPN más complejas, esa perspectiva va cambiando con rapidez. Este documento compara las VPN y las soluciones de acceso remoto de ZTNA para aclarar sus ventajas y limitaciones, al tiempo que pone en claro las consideraciones más importantes para los proyectos de migración. Además, explica cómo Cloudflare ofrece soluciones de ZTNA, y recomienda un conjunto de medidas para la transición de la infraestructura de VPN heredada a una conectividad Zero Trust más rápida y segura para los usuarios remotos.

[1] Riley, Steve, MacDonald, Neil, y Orans, Lawrence. "Market Guide for Zero Trust Network Access" (Guía de mercado para el acceso a la red Zero Trust). Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. Consultado el 21 de junio de 2021. Véase tabla 1 para más detalles.

ENFOQUE N.º 1: VPN HEREDADA

Durante décadas, las VPN han permitido a las organizaciones conectar a sus usuarios remotos a las redes corporativas con cierta privacidad y seguridad. En lugar de acceder a la información confidencial a través de la red de Internet pública, donde cualquier atacante podría espiar o robar datos, las VPN permiten a los usuarios acceder de forma segura a los recursos internos a través de una conexión cifrada.

Los dos modos más comunes de implementación de las VPN son las VPN basadas en el cliente y las redes SSL-VPN sin cliente. Cada una de ellas tiene sus propias ventajas y dificultades:

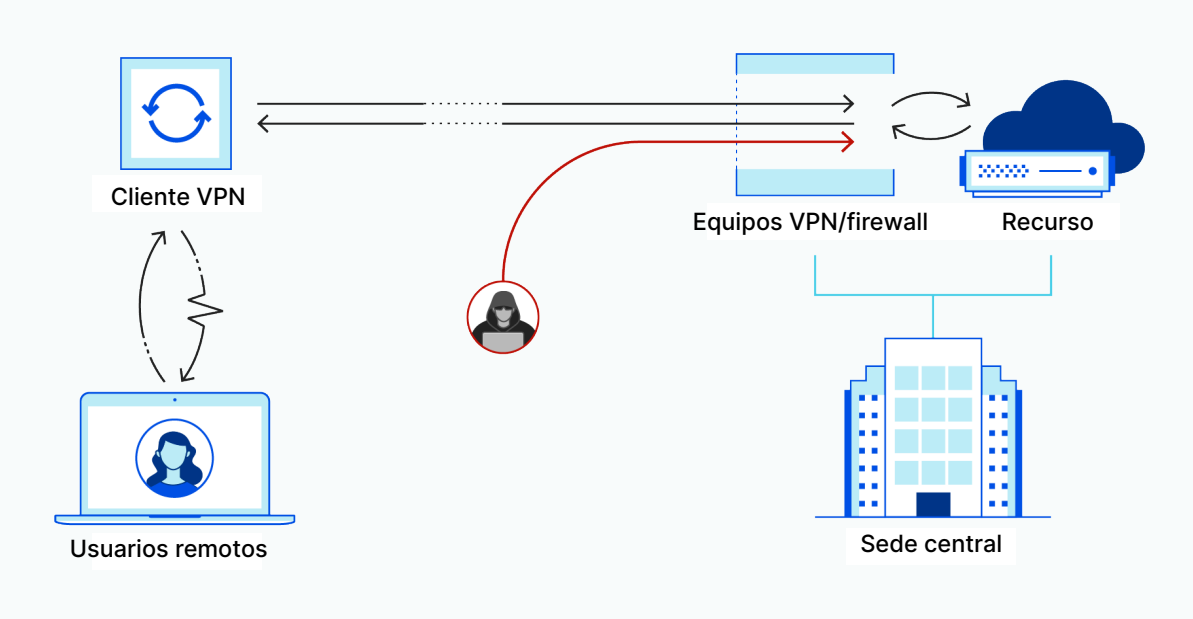
Las **VPN basadas en el cliente** conectan a los usuarios remotos a una red privada a través de un túnel cifrado. Esta conexión se establece a través de una aplicación de software, o cliente, que requiere que los usuarios se identifiquen una vez con un nombre de usuario y una contraseña para poder acceder a cualquier recurso de manera indefinida dentro de esa red.

Beneficio: una vez conectadas, el movimiento lateral libre facilita a los usuarios un acceso rápido a varios recursos mediante a aplicaciones y la conexión a servidores internos.

Desafíos:

- **No están diseñadas para perfiles itinerantes o usuarios de dispositivos móviles**. Cuando los usuarios se desplazan, tanto sus computadoras portátiles como sus dispositivos móviles se reconectan sin problema cuando las redes inalámbricas cambian de lugar. Sin embargo, los clientes VPN no pueden gestionar con eficacia estas reconexiones, lo que obliga a los usuarios a forzar repetidamente el cliente VPN para reiniciar y volver a aautenticar. Esto provoca una disminución de la productividad y un aumento de las solicitudes a TI.
- **Visibilidad deficiente.** Con este método, la infraestructura VPN termina el túnel encriptado del cliente VPN detrás del firewall interno del centro de datos. Aunque estas conexiones se registran, no hay registros centralizados específicos de la aplicación que revelen a qué aplicaciones han accedido los usuarios o las acciones que han realizado dentro de ellas.

Los **portales SSL-VPN sin cliente** permiten a unos pocos usuarios remotos conectarse a algunas aplicaciones en el navegador dentro de una red privada. Esta conexión es posible gracias a un servidor web integrado en el dispositivo de red que ejecuta el servicio VPN.	**Beneficio:** en lugar de utilizar un cliente en un dispositivo, cualquier navegador web puede utilizar el certificado SSL del portal para establecer una conexión HTTPS cifrada que admita a los proveedores en dispositivos no administrados. **Desafíos:** • **Problemas de seguridad.** La mayoría de las configuraciones de VPN dentro del centro de datos conceden acceso total a los usuarios, lo que supone un problema para las organizaciones que no quieren que personas que no son empleados, como los proveedores, obtengan acceso sin restricciones a recursos y aplicaciones confidenciales. • **No están diseñados para soportar muchos usuarios simultáneos.** A diferencia de los modernos servicios en la nube, el servidor web del portal no se puede escalar con flexibilidad para satisfacer una mayor demanda. En su lugar, hay que instalar más dispositivos de red y equilibrar la carga para escalar el portal, lo que suele ser caro, complejo e ineficaz, ya que se pueden desaprovechar el resto de las funcionalidades del dispositivo. • **Los portales SSL-VPN sin cliente exponen los puertos del firewall y los servidores web a ataques.** Para permitir que el servidor web que aloja el portal llegue a las aplicaciones internas, los administradores deben abrir los puertos del firewall de entrada, lo que los expone a los ataques externos. Tanto los puertos abiertos como el propio servidor web deben estar protegidos de ataques DDoS y de las aplicaciones web. Esto que exige una configuración más compleja y unos costes más elevados para asegurar este método de conectividad.



Si bien las VPN proporcionan un nivel básico de privacidad a los usuarios remotos, no se diseñaron contemplando la seguridad o la escalabilidad. Tradicionalmente, las organizaciones han utilizado las VPN para conectar a algunos usuarios remotos a la red corporativa durante breves periodos de tiempo. Sin embargo, a medida que el trabajo a distancia se hace más frecuente, los problemas de las VPN comienzan a multiplicarse:

- **Los usuarios se ven afectados por una ralentización del rendimiento.** Si la infraestructura de la VPN no tiene la capacidad de abordar el rendimiento del tráfico y las conexiones simultáneas creadas por sus usuarios, la conexión a Internet de estos últimos se ralentizará. Además, cuando las VPN están situadas a gran distancia tanto del usuario como del servidor de aplicaciones al que intentan acceder, el tiempo de recorrido resultante provoca problemas de latencia.
- **Las redes corporativas son vulnerables a los ataques.** Las VPN suelen utilizar un modelo de seguridad perimetral, en el que el usuario tiene acceso ilimitado a todos los recursos corporativos una vez que se conecta a la red. Al no contar con un método integrado para restringir el acceso a la infraestructura y los datos críticos, las organizaciones se ven obligadas a configurar servicios de seguridad caros y complejos, como firewalls de nueva generación y soluciones de control de acceso a la red, o se ven expuestas a movimientos laterales malintencionados, lo que se traduce en mayores fugas de datos.

El desafío de los servicios VPN alojados

Algunos proveedores han alojado el dispositivo de red que ejecuta el servicio VPN en la nube pública, donde se ejecuta como una máquina virtual en uno o varios centros de datos. La VPN puede o no estar integrada (o conectada en cadena) a otros servicios de seguridad.

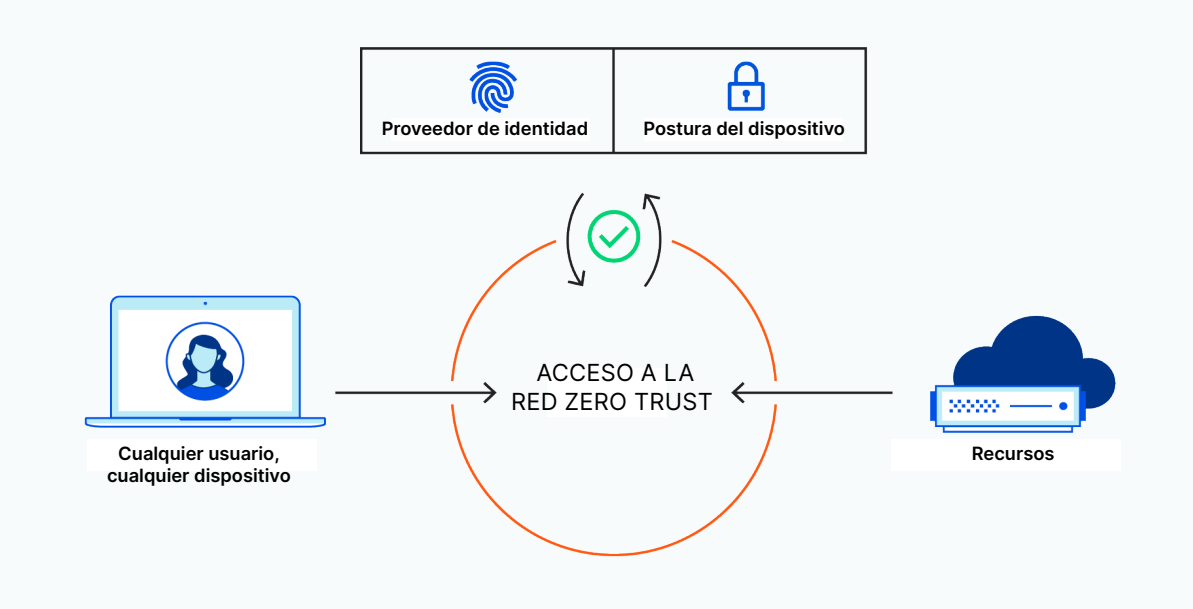
Alojar una VPN en la nube puede parecer que resuelve algunos de los problemas de escalabilidad inherentes a los dispositivos VPN de hardware. Sin embargo, al hacerlo también se plantean algunos problemas importantes de seguridad y escalabilidad.

Por ejemplo, piensa en una organización que aloja un firewall de última generación (NGFW) completo, que combina la VPN con un firewall y funciones de seguridad adicionales. Dado que el NGFW se ofrece como un servicio agrupado, es imposible escalar independientemente cualquier funcionalidad específica a pedido. Mejorar una función requiere la ampliación de todo el servicio. Para ello, hay que poner en marcha más máquinas virtuales con el fin de equilibrar la carga de una pequeña cantidad de procesos que se realiza en cada máquina virtual. Esto no solo es una solución poco práctica y compleja , sino que probablemente incurrirá en altos costes conforme las necesidades de acceso remoto de la organización sigan creciendo.

ENFOQUE N.º 2: ACCESO A LA RED ZERO TRUST

La seguridad Zero Trust sortea muchos de los retos inherentes a las VPN. Se basa en el principio de que no se puede confiar por defecto en ningún usuario o dispositivo dentro o fuera de una red. Para reducir el riesgo y el impacto de las fugas de datos, los ataques internos y otras amenazas, un enfoque Zero Trust:

- Autentica y registra cada inicio de sesión y solicitud.
- Exige una verificación estricta de todos los usuarios y dispositivos.
- Limita la información a la que puede acceder cada usuario y dispositivo en función de la identidad y el contexto.
- Añade un cifrado de un extremo a otro para aislar las aplicaciones y los datos dentro de la red.



Al igual que con las VPN, hay varias formas de configurar una solución ZTNA:

1. **ZTNA sin cliente (o iniciado por el servicio)** utiliza el navegador existente, en lugar de un cliente, para crear una conexión segura y autenticar los dispositivos de los usuarios. Tradicionalmente, ZTNA sin cliente se ha limitado a aplicaciones con protocolos HTTP/HTTPS, pero la compatibilidad está evolucionando con rapidez.[2]
   - **Beneficio:** ZTNA sin cliente utiliza una conexión de proxy inverso para impedir el acceso directo a las aplicaciones, y bloquea el acceso de los usuarios a aplicaciones y datos que no tienen permiso para ver, y permite a los administradores un mayor control y flexibilidad en la gestión.
2. **ZTNA basado en el cliente (o iniciado por el punto de conexión)** instala el software en un dispositivo de usuario antes de que pueda establecerse una conexión cifrada entre el agente controlador y las aplicaciones autorizadas.
   - **Beneficio:** ZTNA basado en el cliente permite a los administradores conocer mejor la postura del dispositivo, la ubicación y el contexto de riesgo de los usuarios que acceden a las aplicaciones, por lo que se pueden crear y aplicar políticas más granulares. Además, como este método no se limita a HTTP/HTTPS, se puede utilizar para acceder a una gama más amplia de aplicaciones no HTTP, como las que dependen de SSH, RDP, VNC, SMB y otras conexiones TCP.

[2] Desde junio de 2021, la solución de ZTNA de Cloudflare es compatible con el acceso sin cliente a aplicaciones SSH y VNC, y está previsto que sea compatible con RDP en el futuro.

Desafíos de la implementación de ZTNA

Si bien ZTNA ofrece claras ventajas sobre las VPN tradicionales, no es un enfoque que carezca de defectos para proteger el acceso a la red de los usuarios remotos. A medida que las empresas evalúan los pros y los contras de la adopción de Zero Trust, pueden encontrarse con uno o varios de los siguientes desafíos:

Las soluciones no son realmente nativas de la nube.

Si un proveedor no ofrece soluciones de ZTNA basadas en la nube, lo que significa que sus clientes tienen que implementar el software en sus propios centros de datos, los usuarios pierden ventajas clave, como la escalabilidad instantánea y el rendimiento ilimitado.

Puede que los proveedores no ofrezcan opciones de ZTNA basadas en el cliente y sin cliente.

Esto limita el valor para las organizaciones que necesitan conectar a los usuarios a aplicaciones que no son HTTP, como escritorios remotos, aplicaciones SSH o archivos compartidos.

La configuración puede ser compleja y requerir mucho tiempo.

Los proveedores que no ofrecen soporte para la organización y automatización de políticas (a través de herramientas como Terraform) pueden aumentar el trabajo manual de los administradores, además de la configuración que ya se realiza en un proveedor de identidad.

ENFOQUE DE CLOUDFLARE PARA EL ACCESO REMOTO

Proteger y escalar el acceso remoto debería ser un proceso eficiente, que no implique soluciones de seguridad engorrosas, que afecten al rendimiento o generen costes innecesarios. Cloudflare permite a los equipos gestionar todos los casos de uso del acceso remoto con las siguientes ventajas:

- **Incorporación fácil y sin riesgos para usuarios y administradores.** Cloudflare se integra fácilmente con los proveedores de identidad y las plataformas de protección de puntos de conexión existentes para aplicar políticas de Zero Trust que limitan el acceso a las aplicaciones y los recursos corporativos.
- **Flexibilidad para implementaciones de soluciones de ZTNA basadas en cliente y sin cliente.** Cloudflare ofrece soporte sin cliente para conexiones a aplicaciones web, SSH, VNC (y próximamente, RDP), y soporte basado en el cliente para aplicaciones no HTTP y enrutamiento privado a direcciones IP internas.

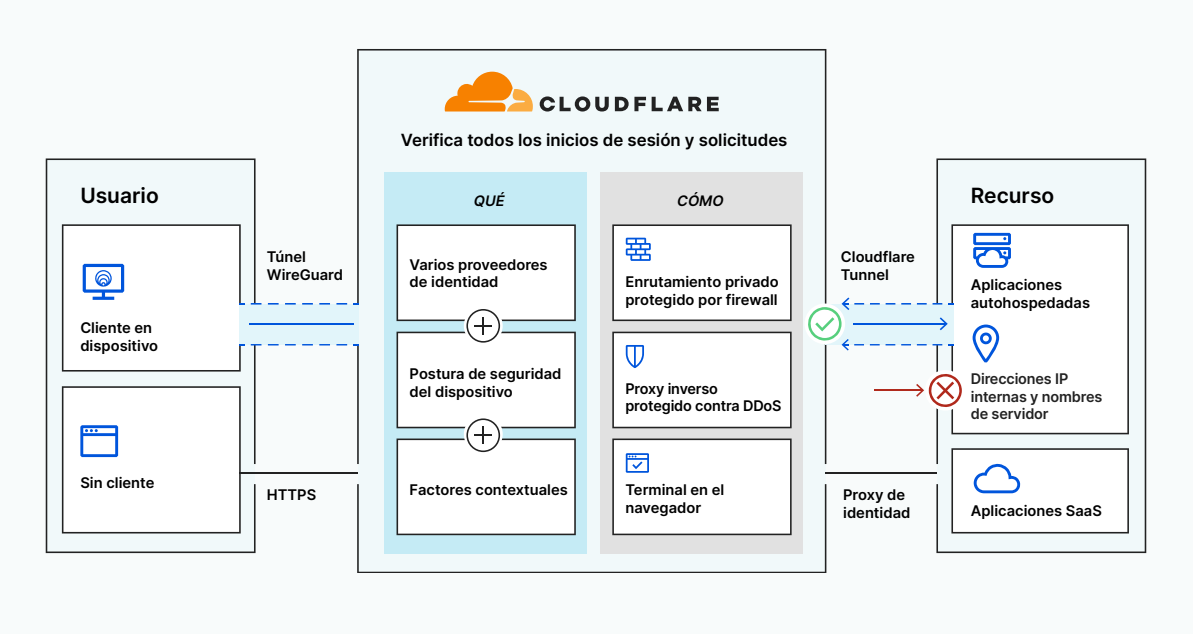


Tabla 1: Cómo aborda Cloudflare los desafíos del acceso remoto

⚠ Problema	✓ Solución	⚙ Implementación de Cloudflare
Dificultad para escalar	Red perimetral global	Los problemas de escalabilidad afectan tanto a las VPN como a los servicios ZTNA que no son nativos de la nube, lo que dificulta el acceso de los usuarios remotos a las aplicaciones y los datos. La red global Anycast de Cloudflare no solo acelera las conexiones de los usuarios respecto a una VPN, sino que también garantiza que todos los usuarios remotos puedan conectarse de forma segura y rápida a los recursos corporativos cuando lo necesiten, sin necesidad de que los administradores realicen largas configuraciones adicionales.
Compatibilidad deficiente con los dispositivos móviles	Clientes ligeros	Las VPN y las soluciones de ZTNA que utilizan los protocolos IPSec y SSL suelen tener un rendimiento deficiente en los dispositivos móviles. El cliente WARP de Cloudflare utiliza el protocolo Wireguard más moderno, que se ejecuta en el espacio de usuario para admitir un conjunto más amplio de opciones del SO con una experiencia de usuario más rápida que las opciones tradicionales. El cliente WARP de Cloudflare se puede configurar en dispositivos Windows, MacOS, iOS, Android y, próximamente, Linux.
Sin protección DDoS integrada o protección deficiente	Protección DDoS integrada líder en el sector	Sin protección DDoS integrada, las organizaciones a menudo se ven obligadas a conectar servicios de seguridad adicionales que pueden crear problemas de configuración, escalabilidad y desafíos de seguridad. La red de más de 67 Tbps de Cloudflare ofrece protección DDoS integrada para cualquier modo de ZTNA, y defiende a las redes contra los mayores ataques volumétricos.
Limitaciones de protocolos	Compatibilidad con aplicaciones no web	✓ Compatibilidad de modo: ZTNA sin cliente para aplicaciones SSH/VNC. ZTNA basado en cliente para el resto de las aplicaciones no web.
Sin firewall de red integrado	Firewall de red integrado	Conforme crecen las redes corporativas, también lo hace el conjunto de hardware de seguridad que las organizaciones tienen que compaginar, lo que afecta el coste, el rendimiento y la seguridad. Cloudflare permite a los administradores aplicar políticas de firewall de red en el perímetro lo que les proporciona un control detallado sobre los datos que tienen autorización para entrar y salir de su red y mejora la visibilidad de cómo fluye el tráfico a través de ella. ✓ Compatibilidad de modo: ZTNA basado en el cliente
Falta de control detallado	Puerta de enlace web segura (SWG) integrada	El uso no autorizado de las aplicaciones puede causar importantes problemas de seguridad a las organizaciones. Sin políticas rigurosas, los usuarios pueden acceder y alterar datos confidenciales y otros recursos corporativos. Al combinar ZTNA con SWG, Cloudflare permite a los administradores ejercer un control más detallado sobre los derechos de acceso de los usuarios y los dispositivos dentro de las aplicaciones, de modo que los usuarios y los grupos basados en roles solo tengan acceso a los recursos que necesitan. ✓ Compatibilidad de modo: ZTNA basado en el cliente

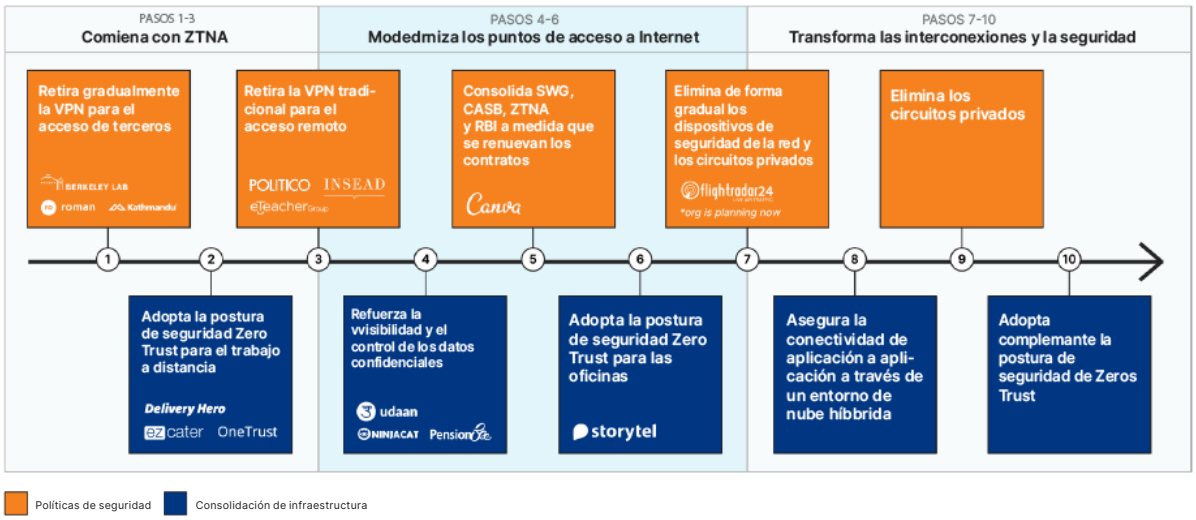
REEMPLAZA TU VPN HEREDADA POR EL ACCESO A LA RED ZERO TRUST

Para los responsables de seguridad, las promesas de Zero Trust pueden parecer vacías en el contexto de una larga y complicada transición a la seguridad sin VPN. Sin embargo, es posible reemplazar tu VPN por el acceso a la red Zero Trust sin impactar en la compatibilidad de protocolos o la funcionalidad.

La ruta de migración recomendada varía en función de las prioridades de la empresa que impulsen tu proyecto:

- Si tu prioridad es acelerar la conexión de las aplicaciones, implementa **ZTNA basado en el cliente para aplicaciones no web** en primer lugar.
- Si la mejora de la seguridad de las reglas de acceso a las aplicaciones es más importante, empieza por las **aplicaciones web**.

El reemplazo de tu VPN es solo el primer paso de una transformación completa de la red. Dado que la transición a un modelo SASE puede ser abrumadora, hemos especificado un recorrido común hacia la seguridad Zero Trust basado en el enfoque que han adoptado nuestros clientes:



Descubre cómo la plataforma Zero Trust de Cloudflare puede ayudarte a reducir la dependencia de tu VPN y, en última instancia, a reemplazarla.

Más información

Te mostramos una comparación real entre una VPN y la solución de ZTNA, y cómo Cloudflare Access mejora la seguridad para el acceso a las aplicaciones.

Ver demo

APÉNDICE

Moderniza los puntos de acceso a Internet

La implementación de ZTNA es un paso importante en la adopción de un modelo de perímetro de servicio de acceso seguro (SASE). **Cloudflare One** es una solución integral de red como servicio (NaaS) que simplifica y protege la red corporativa para equipos de todos los tamaños. Con Cloudflare One, las organizaciones pueden:

- **Adoptar el acceso Zero Trust.** Sustituye los amplios perímetros de seguridad por la verificación individual de cada solicitud a cada recurso. Aplica reglas de Zero trust en cada conexión a tus aplicaciones corporativas, sin importar dónde o quiénes sean tus usuarios.
- **Proteger el tráfico de Internet.** Cuando las amenazas en Internet avanzan con rapidez, las defensas que utilizas para detenerlas deben ser más proactivas. Cloudflare One protege a los usuarios remotos de las amenazas en Internet y aplica políticas que impiden que información valiosa salga de tu organización al aplicar el aislamiento del navegador Zero Trust en cualquier sitio, con una experiencia de usuario eficiente y rápida.
- **Proteger y conectar las oficinas y los centros de datos.** Las redes corporativas se han vuelto demasiado complejas, lo que significa que el tráfico de los usuarios a menudo tiene que dar varios saltos para llegar a donde tiene que ir. Con Cloudflare One, las empresas pueden proteger las oficinas y los centros de datos a través de una plataforma en la nube coherente y unificada.

Si quieres más información sobre Cloudflare One, no dejes de ver esta introducción y demostración de 10 minutos.

Transforma tu red

Próximamente, las soluciones de Zero Trust y WAN como servicio de Cloudflare convergerán en una sola, lo que permitirá a tus usuarios acceder a los recursos corporativos de forma estable, trabajen desde donde trabajen.

En la actualidad, tus productos VPN y WAN permiten a tus empleados acceder a recursos ubicados dentro de tu red corporativa privada, pero te obligan a gestionar la conectividad y las políticas de seguridad de forma diferente.

Ahora, Cloudflare ofrece un plano de control unificado, lo que te da más flexibilidad para aplicar las mismas políticas de seguridad Zero Trust a todos tus usuarios y lugares de trabajo sin necesidad de compaginar varios productos específicos.

Para más información, visita https://www.cloudflare.com/cloudflare-one/.