GUÍA DE DISEÑO

CLOUDFLARE

Cloudflare One, nuestra plataforma SASE

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

ÍNDICE

Acerca de esta guía **3**

Transformación: comparación del antes y el después de Cloudflare **4**

- Conectividad segura, rápida, fiable y privada para cualquier usuario 5
- Conectividad y seguridad más sencillas de los recursos públicos 6-7
- Conectividad y seguridad más sencillas de los recursos privados 8-9
- Conectividad y seguridad más sencillas de cualquier recurso 10
- Una plataforma para facilitar la conectividad y seguridad 11

Caso de uso 1: Acceso seguro para aplicaciones web **12**

- Diseño heredado - resumen 13
- Diseño heredado - fallos de seguridad 14
- Diseño heredado - complementos de seguridad necesarios 15
- Diseño de Cloudflare One 16
- Diagramas comparativos 17
- Cuadros comparativos 18

Caso de uso 2: Filtrado de DNS **19**

- Diseño heredado - resumen 20
- Diseño heredado - fallos operativos 21
- Diseño heredado - requiere modificaciones en la red 22
- Diseño de Cloudflare One 23
- Diagramas comparativos 24
- Cuadros comparativos 25

Nota: Se añadirán más casos de uso

Acerca de esta guía

Esta guía de diseño está destinada a profesionales con un perfil técnico y proporciona ejemplos ilustrativos de cómo las organizaciones pueden simplificar y reforzar su arquitectura de red y seguridad con Cloudflare One, nuestra plataforma SASE. Cloudflare One agrupa los servicios de conectividad de red con los servicios de seguridad Zero Trust, todo ello desde la red global de Cloudflare.

La primera sección de esta guía de diseño se centra en la transformación y modernización integrales, ilustrando todos los posibles elementos de la conectividad y la seguridad alineados con la red de entrada, la red de salida y las aplicaciones antes y después de Cloudflare. Compara el enfoque del perímetro de seguridad centralizado heredado que depende de soluciones de varios proveedores con el enfoque de la red global de Cloudflare que aprovecha una arquitectura de plataforma modulable.

Las siguientes secciones analizan los casos de uso técnico más comunes. En primer lugar, exploraremos cómo se resuelve normalmente ese problema con un enfoque heredado y, después, cómo lo resuelve Cloudflare One con mayor eficiencia y experiencia.

Se han priorizado dos casos de uso en función de su popularidad entre los clientes, pero no representan en absoluto todo el alcance de las capacidades de Cloudflare One.

- Acceso seguro para aplicaciones web privadas y públicas
- Filtrado de DNS para empleados locales y remotos

Seguiremos ampliando esta guía con otros casos de uso, como el acceso seguro a redes privadas, la protección avanzada de datos y amenazas, etc.

Transformación: comparación del antes y el después de Cloudflare

Conectividad segura, rápida, fiable y privada para cualquier usuario

Cualquier usuario

Las organizaciones deben habilitar una conectividad segura, rápida, fiable y privada para dos grupos de usuarios.

Usuarios administrados son empleados que acceden a un recurso con un dispositivo corporativo o personal desde casa, la oficina o cualquier otro lugar.

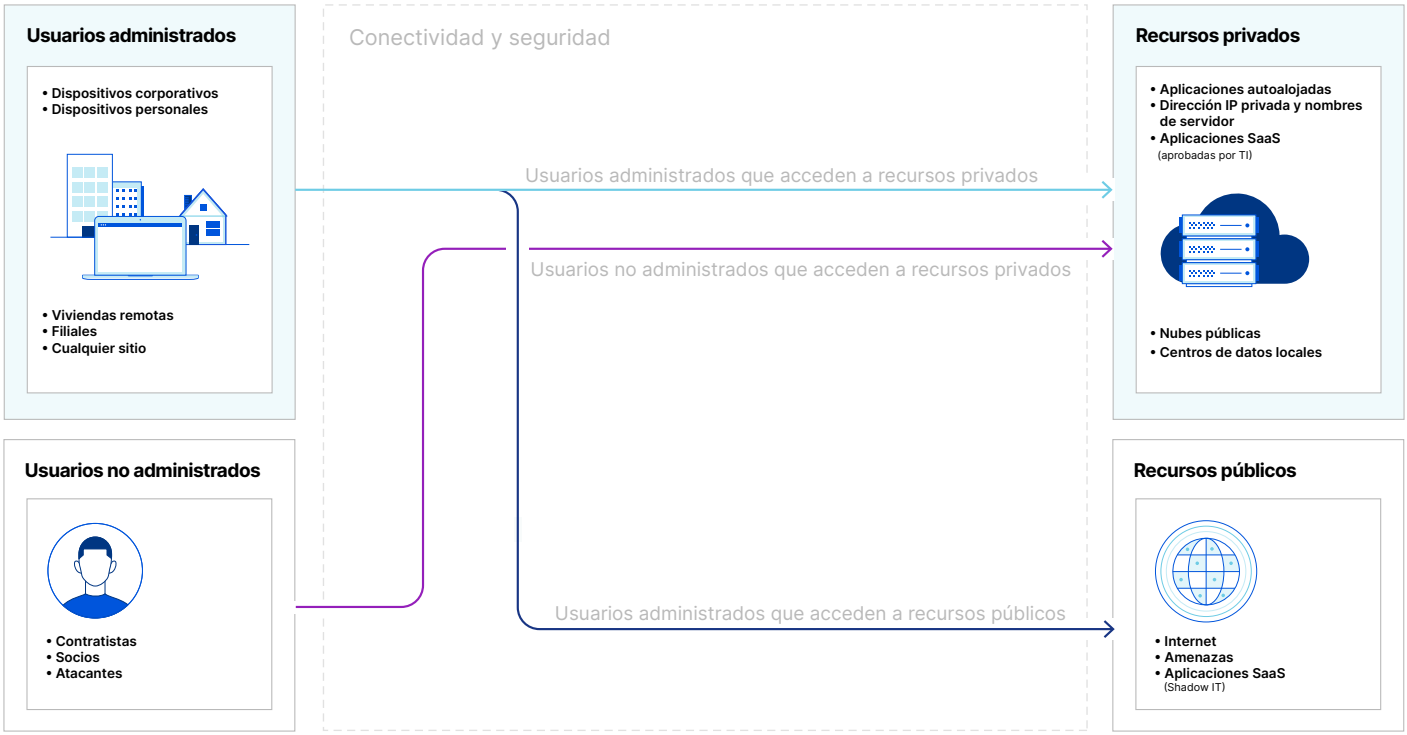
Usuarios no administrados incluyen a los contratistas o socios que están autorizados acceder a un recurso, pero también a los atacantes, que no lo están.

Cualquier recurso

Las organizaciones deben habilitar la gestión de acceso con protección de datos y amenazas para dos grupos de recursos.

Recursos privados incluyen aplicaciones autoalojadas y direcciones IP o nombres de servidor privados dentro de nubes públicas y centros de datos locales, además de aplicaciones SaaS aprobadas por los responsables informáticos.

Recursos públicos en Internet incluyen a las aplicaciones SaaS no autorizadas y amenazas.



Comparación de la conectividad y la seguridad antes y después de Cloudflare

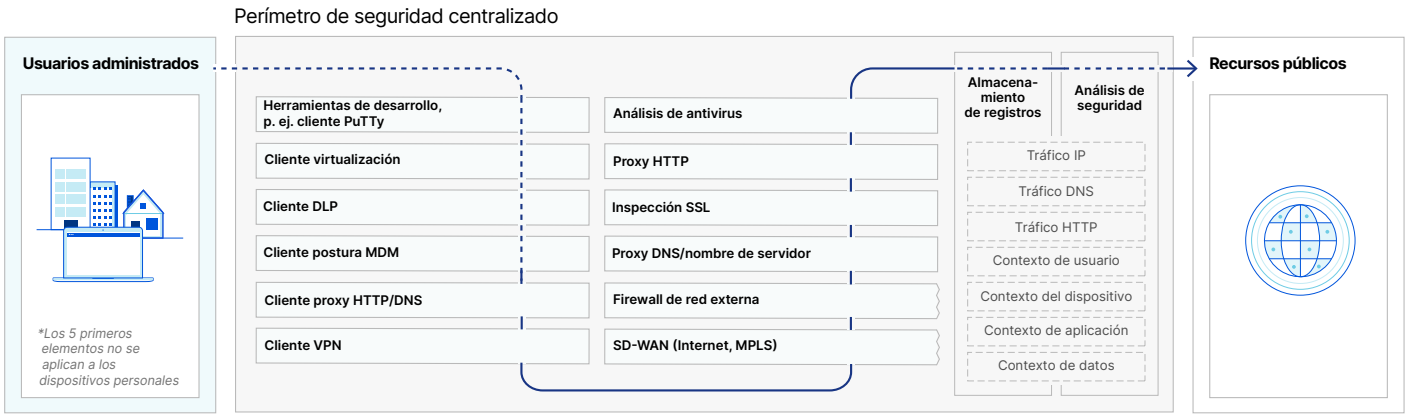
En las seis páginas siguientes, una serie de diagramas del antes y después detallarán todos los posibles elementos de conectividad y seguridad que tu organización necesita para que los usuarios administrados accedan a los recursos públicos y los usuarios administrados o no administrados accedan a los recursos privados.

El primer diagrama "antes" ilustra los dispositivos de red y el proceso de los puntos finales implementados en un perímetro de seguridad centralizado.

El segundo diagrama "después" ilustra los servicios de nube comparables a través de la red global de Cloudflare.

1a. Conectividad y seguridad más sencillas de los recursos públicos

Antes de Cloudflare



= Primera instancia del elemento ------ = Tráfico de red no enrutado/filtrado a través de estos elementos

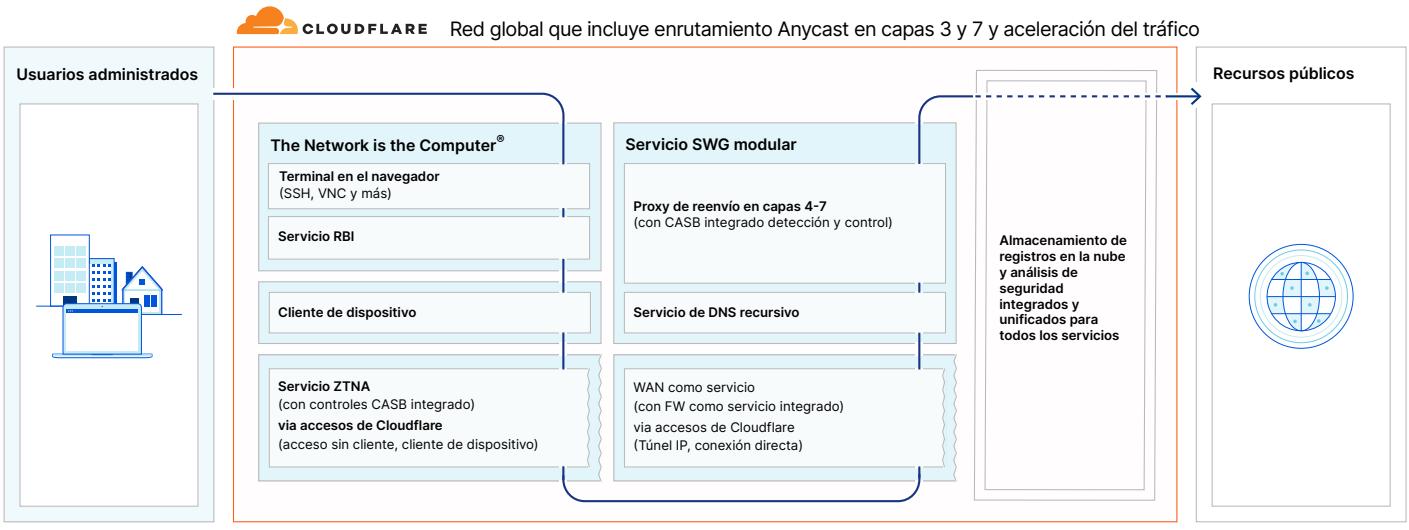
Usuarios administrados (para recursos públicos y privados)

Los equipos informáticos tenían que gestionar la conectividad y la seguridad de muchos clientes, o peor aún, no podían hacerlo para los dispositivos personales. Herramientas de desarrollo y VPN para el acceso privado. Proxy HTTP/DNS para el acceso público. Virtualización, DLP y MDM para una mejor protección.

Recursos públicos

Los equipos de seguridad dependían del cliente VPN o de la SD-WAN para enrutar el tráfico de los usuarios remotos o de la oficina a través del firewall de la red, el proxy DNS, la inspección SSL, el proxy HTTP y los dispositivos de análisis antivirus para proteger el acceso a los recursos públicos.

Después de Cloudflare



= Primera instancia del elemento ------ = Tráfico de red no enrutado/filtrado a través de estos elementos

Usuarios administrados (para recursos públicos y privados)

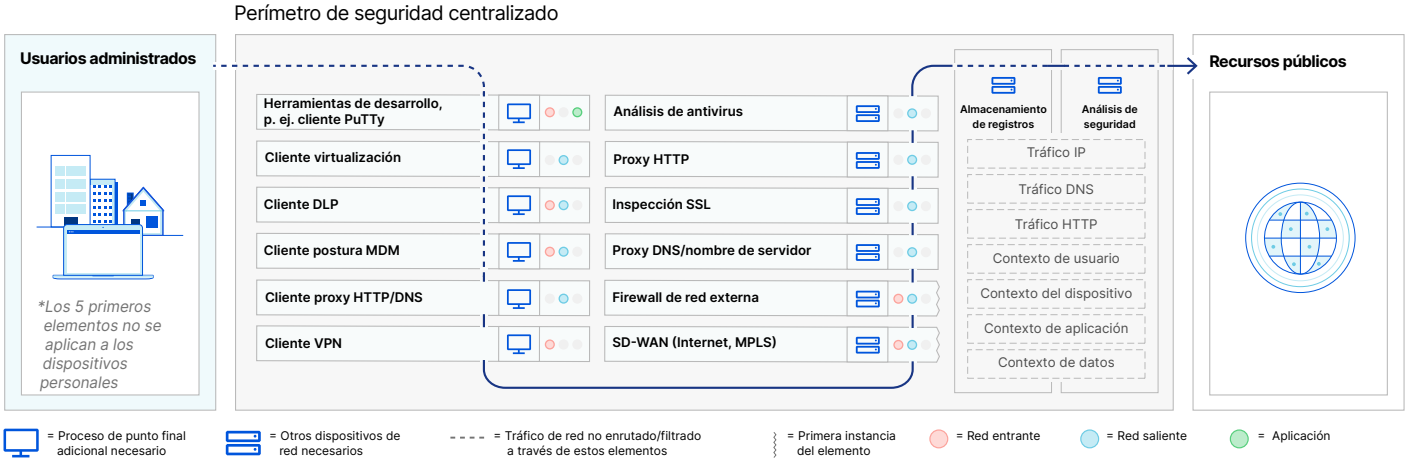
La red elimina muchas funciones del ordenador o computadora o un cliente consolida muchas funciones.

Recursos públicos

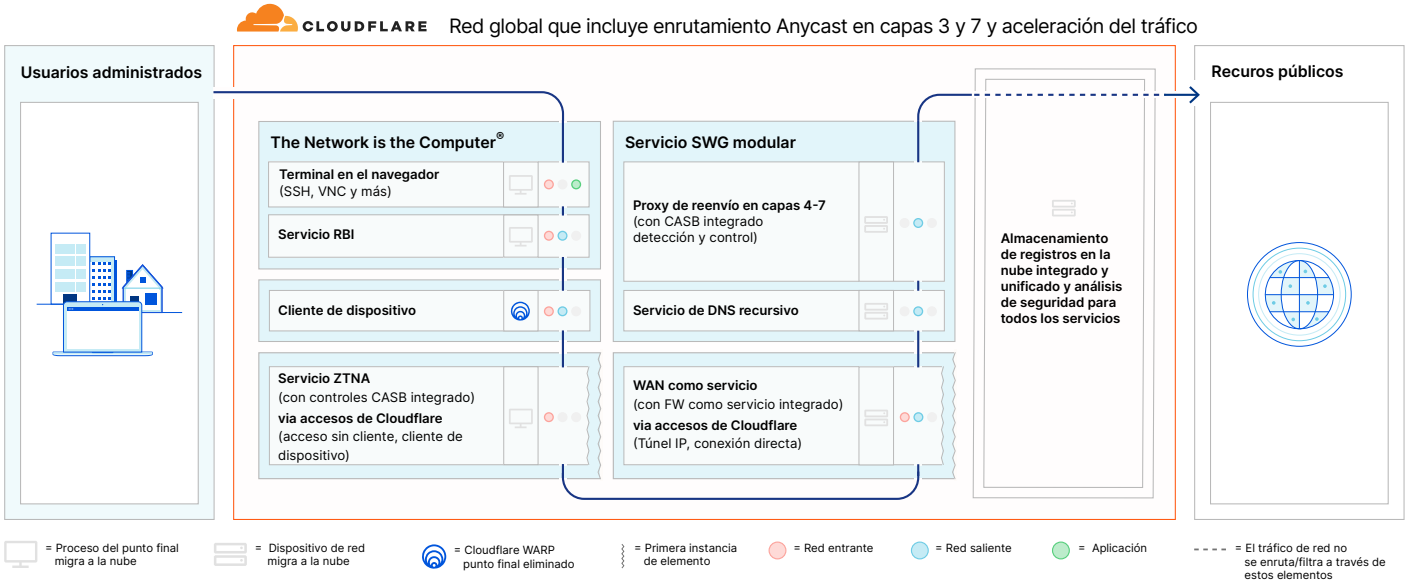
Nuestro servicio SWG (puerta de enlace web segura) modular inspecciona el tráfico en un único paso antes o después de implementar nuestra WAN como servicio y/o el servicio ZTNA con seguridad incorporada.

1b. Conectividad y seguridad más sencillas de los recursos públicos

Antes de Cloudflare



Después de Cloudflare



Servicios nativos de nube

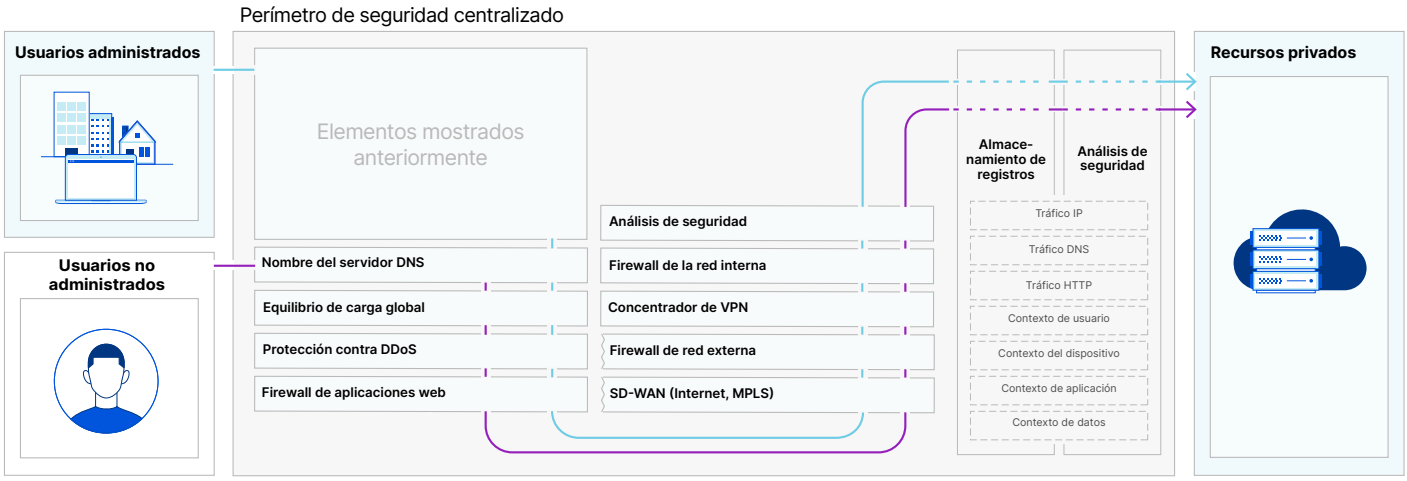
Se reducen los requisitos del proceso de los puntos finales y de los dispositivos de red.

Arquitectura modular

Las pilas de redes entrantes y salientes se unifican con la pila de aplicaciones para garantizar la seguridad y el rendimiento de un extremo a otro.

2a. Conectividad y seguridad de los recursos privados

Antes de Cloudflare



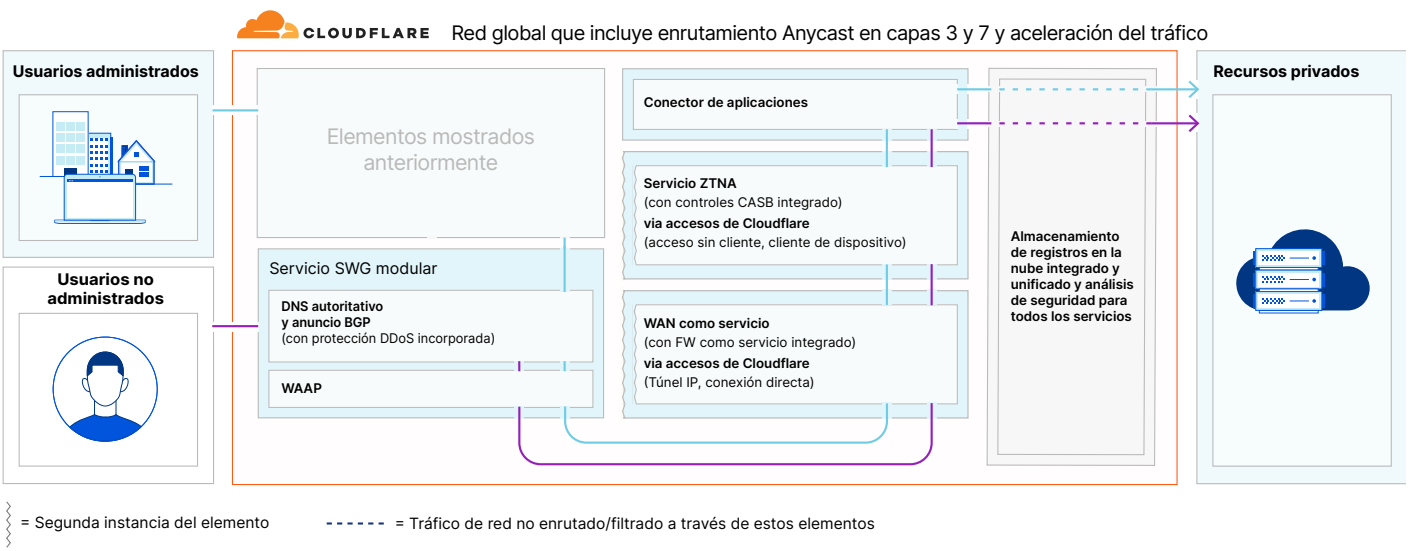
Usuarios no administrados

Los equipos de red tenían que gestionar la disponibilidad de los recursos privados anunciados públicamente a los contratistas y socios, y protegerse contra los ataques DDoS o la explotación de vulnerabilidades por parte de los atacantes.

Recursos privados (de usuarios administrados y no administrados)

Los equipos de seguridad dependían del cliente VPN o de la SD-WAN para enrutar el tráfico de los usuarios a través de los firewall de red, los concentradores VPN y los equilibradores de carga para garantizar el acceso a los recursos privados.

Después de Cloudflare



Usuarios no administrados

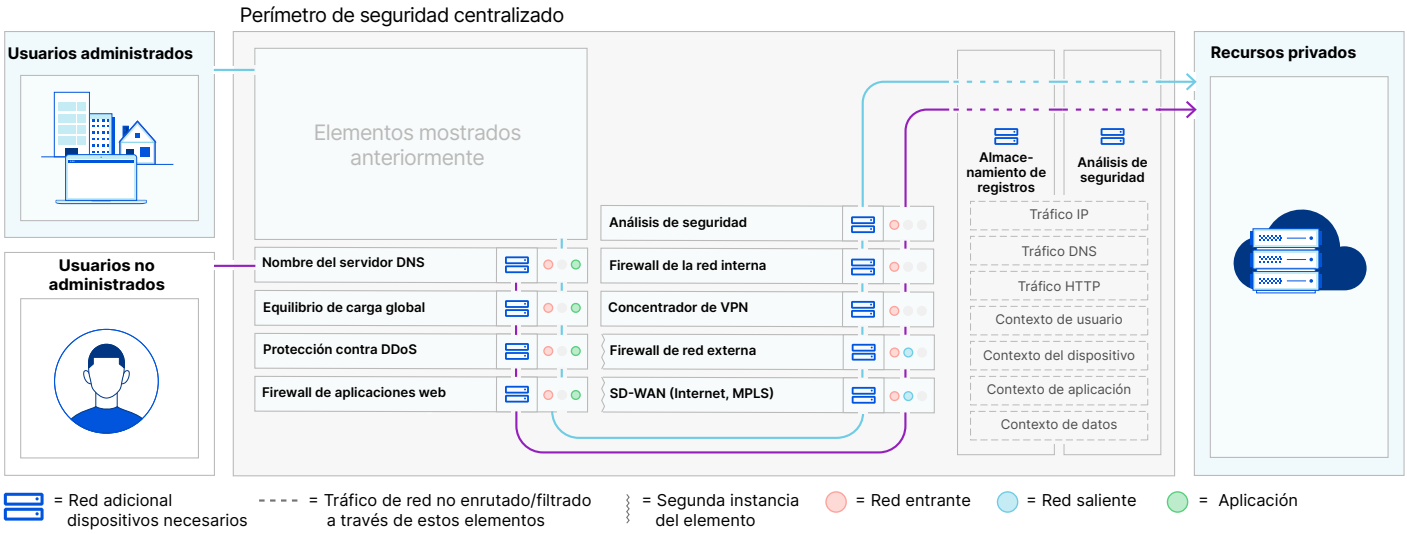
Nuestros servicios de red y aplicaciones modulares eliminan esta carga antes o después de adoptar nuestro servicio ZTNA o WAN como servicio con seguridad integrada.

Recursos privados (de usuarios administrados y no administrados)

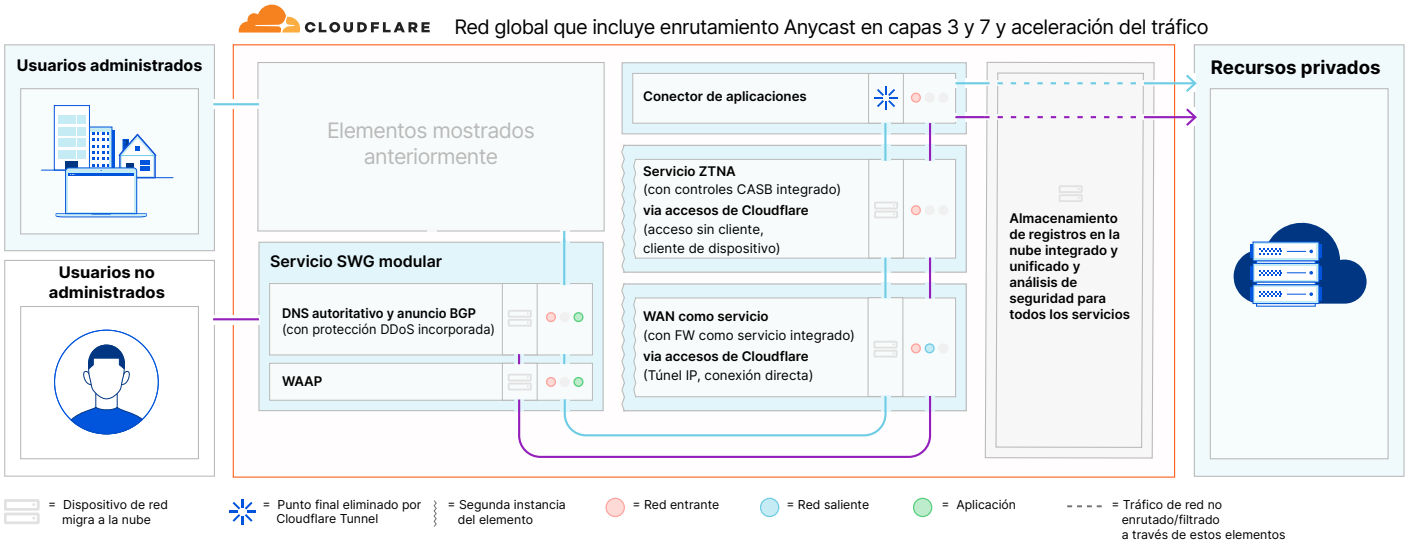
Nuestro servicio ZTNA y/o WAN como servicio con seguridad integrada simplifica el acceso mediante nuestro conector de aplicaciones.

2b. Conectividad y seguridad más sencillas de los recursos privados

Antes de Cloudflare



Después de Cloudflare



Servios nativos de nube

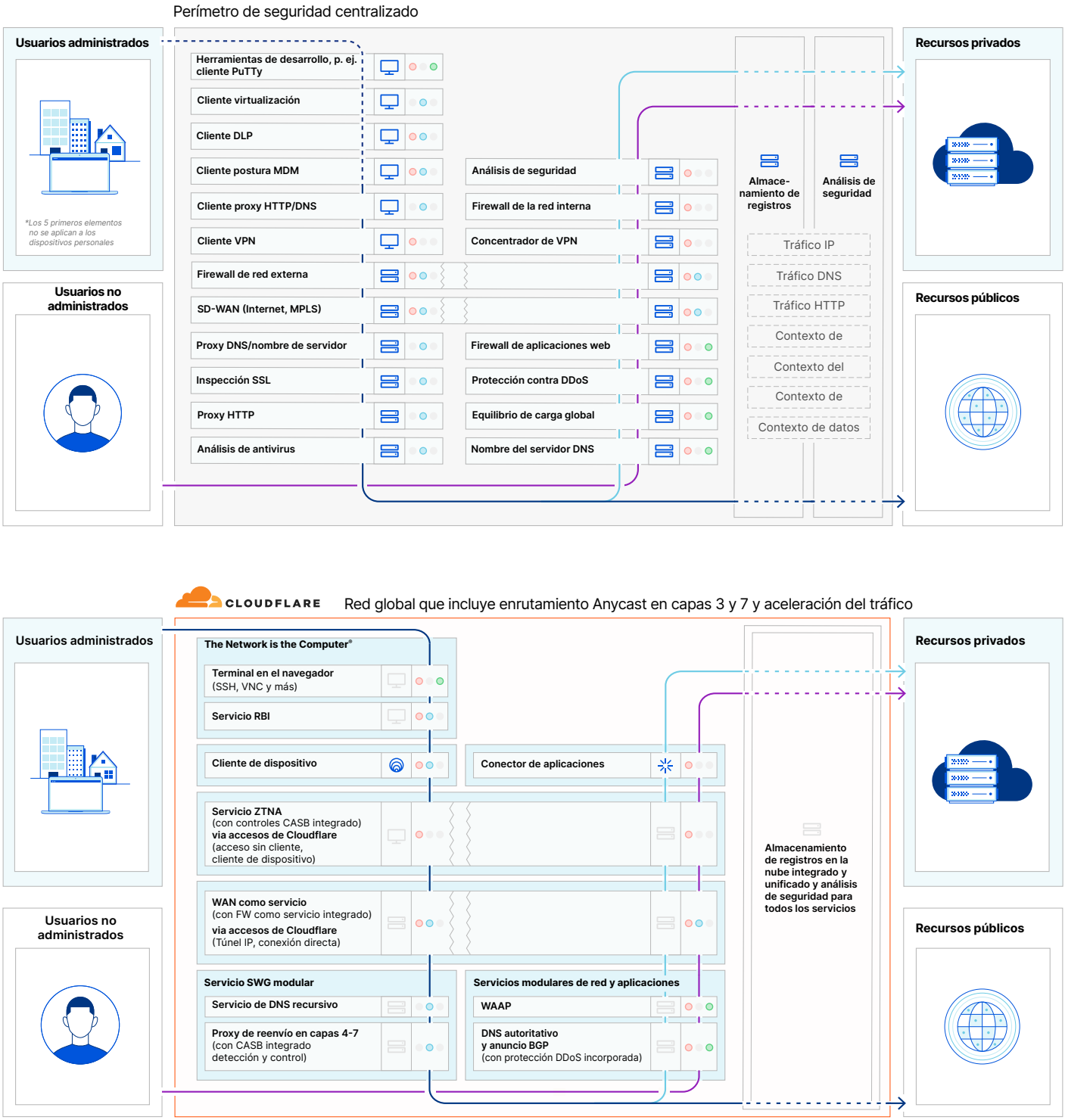
Se reducen los requisitos del proceso de los puntos finales y de los dispositivos de red.

Arquitectura modular

Las pilas de redes entrantes y salientes se unifican con la pila de aplicaciones para garantizar la seguridad y el rendimiento de un extremo a otro.

Conectividad y seguridad más sencillas de cualquier recurso

Esta vista combina los diagramas 1 y 2.



Después

Los elementos de conectividad y seguridad se reutilizan cuando cualquier usuario accede a cualquier recurso, lo que mejora la eficiencia y la experiencia. Además, nuestro servicio ZTNA y la WAN como servicio abarcan elementos que tradicionalmente gestionaban los equipos informáticos, de red y seguridad de manera independiente.

Una plataforma para facilitar la conectividad y la seguridad

Perímetro de seguridad centralizado frente a la red global de Cloudflare

Antes

Los equipos informáticos, de red y seguridad dependían de las soluciones de muchos proveedores, cada uno con una arquitectura diferente, de manera que las integraciones daban lugar a deficiencias de conectividad y seguridad con un rendimiento limitado.

Después

Todos los equipos aprovechan una plataforma con la misma arquitectura modular para eliminar las deficiencias y los impactos en el rendimiento. Nuestra plataforma se ejecuta en todas partes y se desarrolla para adaptarse a tu mundo, no al revés. Puedes implementar los servicios que desees, en cualquier secuencia, y seguirán funcionando juntos de manera uniforme.

Caso de uso 1:
Acceso seguro para aplicaciones web

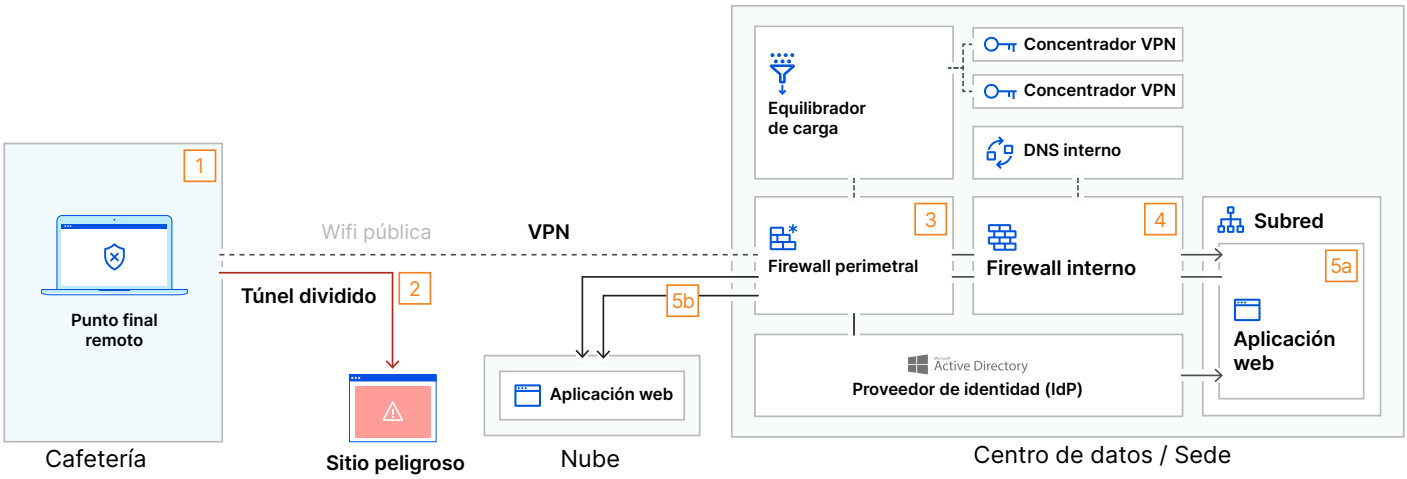
Diseño heredado - resumen

Este gráfico representa un método tradicional de proporcionar acceso remoto a las aplicaciones web. Aquí, un usuario remoto accede a recursos corporativos, concretamente a una aplicación web privada (autoalojada) y pública (basada en la nube).

Hemos incluido algunas de las medidas de seguridad más comunes que cualquier organización razonable tendría en vigor, incluido un firewall perimetral, un firewall interno para la segmentación y una VPN.

De izquierda a derecha, este escenario ilustra la duración de una sesión cuando un usuario se conecta desde una ubicación pública, un escenario en el que se basarán los siguientes gráficos de diseño.

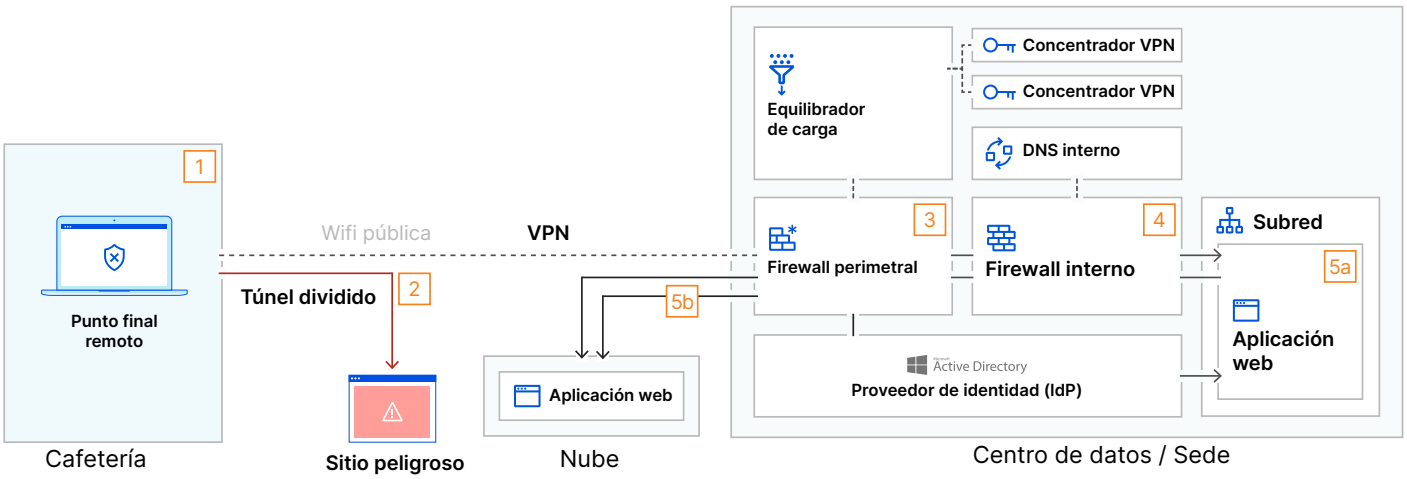
Nota: este gráfico solo representa los dispositivos, equipos y flujos de tráfico implicados en esta transacción de red específica y no representa una instantánea completa de todas las tecnologías que estarían presentes en una arquitectura de red heredada.



	Acción de red/seguridad
1	Un dispositivo remoto se conecta a los recursos corporativos a través de una wifi pública
2	El dispositivo remoto llega al perímetro corporativo a través de un cliente VPN, pero divide el resto del tráfico
3	La VPN termina en el firewall perimetral o en el concentrador de VPN detrás del firewall
4	La política del firewall concede al usuario remoto acceso a la subred con la aplicación web privada
5	El usuario accede a la aplicación web a través de la IP/URL privada **[5a]** o la URL pública **[5b]** tras autenticarse en el IDP5

Diseño heredado - fallos de seguridad

Este gráfico añade otra columna a la tabla que se muestra a continuación, en la que se destacan los problemas de fallos de seguridad que se asocian a cada paso específico de este escenario y que exponen a una organización a vulnerabilidades.

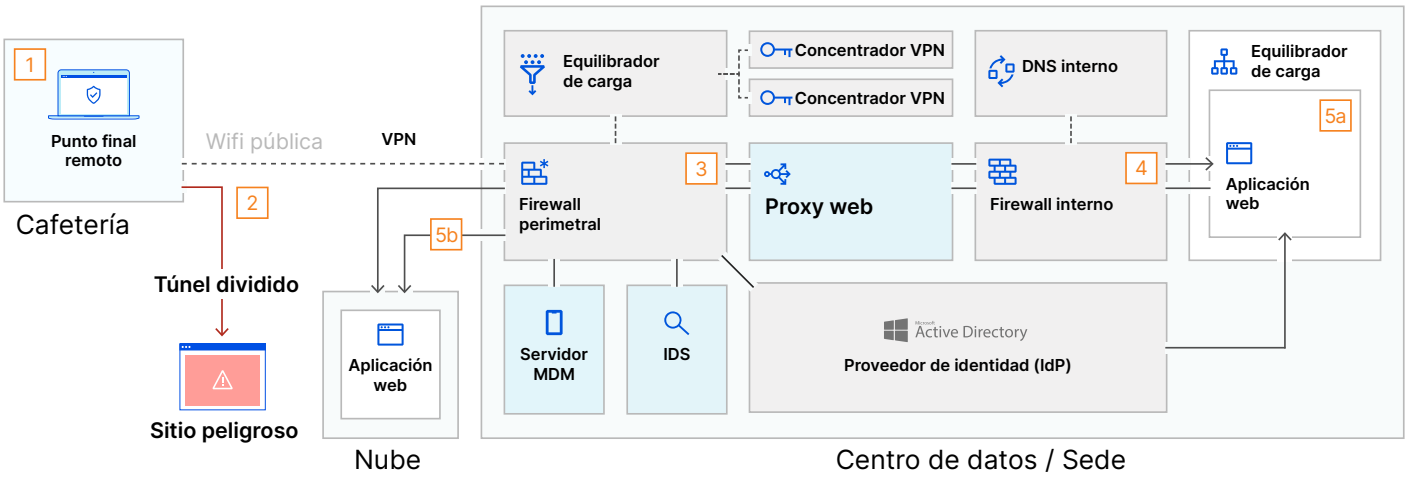


	Acción de red/seguridad	Solución heredada relevante	Fallo de diseño heredado
1	Un dispositivo remoto se conecta a los recursos corporativos a través de una wifi pública	Cliente VPN corporativo	Un dispositivo no seguro en una red wifi pública es un objetivo para los atacantes
2	El punto final remoto llega al perímetro corporativo a través del cliente VPN, pero divide el resto del tráfico	Cliente VPN corporativo	La seguridad específica de la VPN no protegerá el tráfico con túnel dividido
3	La VPN termina en el firewall perimetral o en el concentrador de VPN detrás del firewall	Equilibrador de carga Firewall perimetral Concentrador de VPN	Las reglas de FW/VPN entrantes pueden exponer puertos/protocolos a Internet, ampliando la superficie de ataque potencial
4	La política del firewall concede al usuario remoto acceso a la subred con la aplicación web privada	Firewall interno	El usuario tiene acceso a recursos fuera de su función laboral
5	El usuario accede a la aplicación web a través de la IP/URL privada **[5a]** o la URL pública **[5b]** tras autenticarse en el IdP	Directorio activo DNS interno (privado)	Si el punto final está en riesgo, la aplicación/red de la empresa también lo está.

Diseño heredado - complementos de seguridad necesarios

Para solucionar los defectos de diseño señalados en la página anterior, la organización debe modificar su arquitectura de red existente. Este gráfico añade otra columna a la tabla siguiente, en la que se detallan las soluciones típicas para proteger a los usuarios y los recursos.

La superposición de cada uno de los complementos de seguridad añade complejidad y costes de gestión continuos probablemente a través de varios proveedores del entorno heredado.



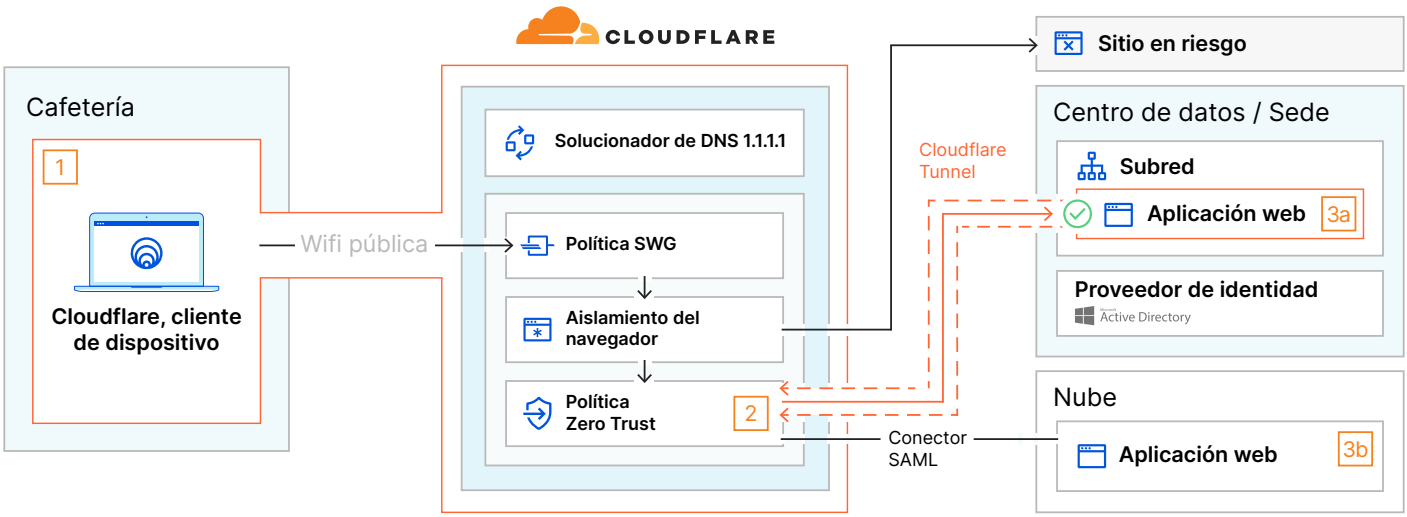
	Acción de red/seguridad	Solución heredada relevante	Fallo de diseño heredado	Complemento de seguridad necesario
1	Un dispositivo remoto se conecta a los recursos corporativos a través de una wifi pública	Cliente VPN corporativo	Un dispositivo no seguro en una red wifi pública es un objetivo para los atacantes	Plataforma de protección de puntos finales (EPP)
2	El dispositivo remoto llega al perímetro corporativo a través de un cliente VPN, pero divide el resto del tráfico	Cliente VPN corporativo	La seguridad específica de la VPN no protegerá el tráfico de túnel dividido	Desactivación del túnel dividido
3	La VPN termina en el firewall perimetral o en el concentrador de VPN detrás del firewall	Equilibrador de carga Firewall perimetral Concentrador de VPN	Las reglas de FW/VPN entrantes pueden exponer puertos/protocolos a Internet, ampliando la superficie de ataque potencial	Sistema de detección de intrusiones (IDS)
4	La política del firewall concede al usuario remoto acceso a la subred con la aplicación web privada	Firewall interno	El usuario tiene acceso a recursos fuera de su función laboral	Proxy web
5	El usuario accede a la aplicación web a través de la IP/URL privada **[5a]** o la URL pública **[5b]** tras autenticarse en el IDP5	Directorio activo DNS interno (privado)	Si el punto final está en riesgo, la aplicación/red de la empresa también lo está	Servidor de gestión de dispositivos móviles (MDM)

Diseño de Cloudflare One

Este gráfico destaca cómo una organización puede adoptar un enfoque más sencillo y eficiente para proteger el acceso a las aplicaciones mediante la implementación de Cloudflare One.

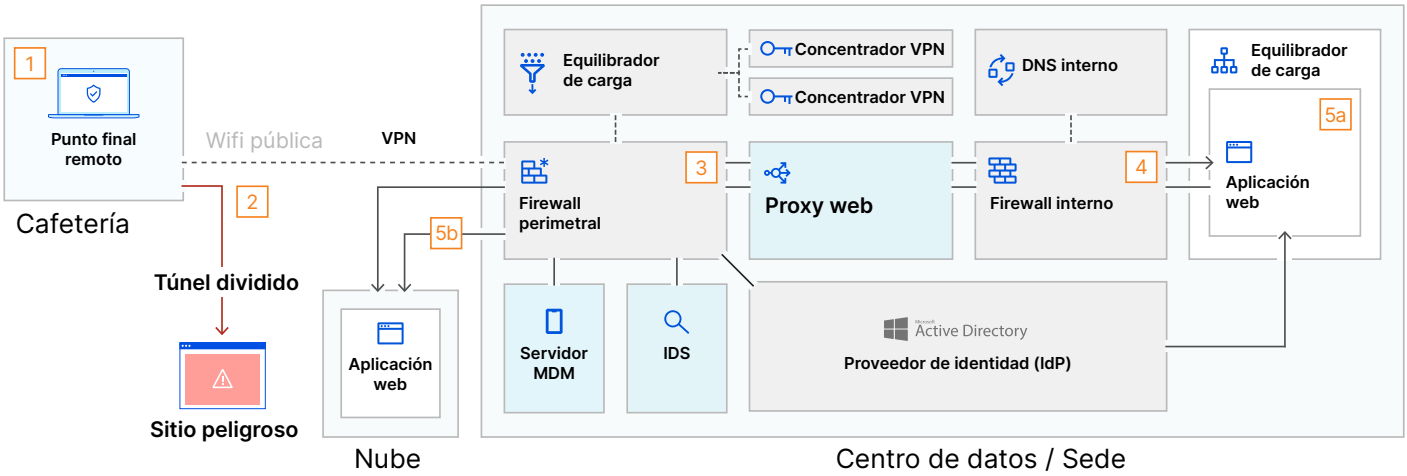
Aquí, gran parte de la arquitectura de red heredada mostrada anteriormente se descarga en Cloudflare, y muchos de los fallos de diseño existentes se corrigen sin necesidad de soluciones adicionales.

Con Cloudflare One, el tráfico entre el usuario remoto y los recursos de la organización se ejecuta a lo largo de la red global de Cloudflare con inspección de paso único. Todos los servicios que se muestran a continuación se ejecutan en todos los centros de datos de Cloudflare, ubicados en más de 250 ciudades en más de 100 países.

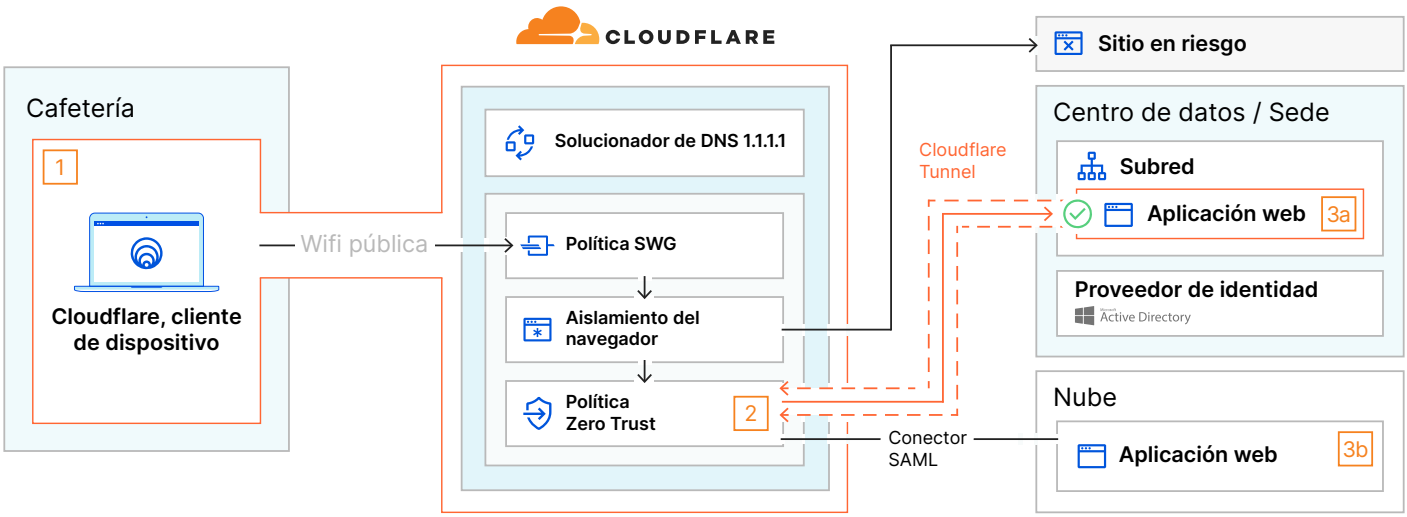


	Acción de red/seguridad	Elemento relevante de Cloudflare One	Corrección de fallos de diseño
1	Un dispositivo remoto se conecta a los recursos corporativos y a Internet a través de Cloudflare	Cliente de dispositivo de Cloudflare Política SWG Aislamiento del navegador	El cliente local de SWG permite a Cloudflare One filtrar el tráfico DNS/HTTP/red al dispositivo del usuario a través de la política de la puerta de enlace El aislamiento del navegador absorbe/aísla el impacto de los ataques exitosos de malware de sitios web
2	El usuario se somete a comprobaciones de postura de IdP y del dispositivo en Cloudflare	Política Zero Trust	La política Zero Trust realiza una comprobación de la postura del dispositivo antes de permitir el acceso, mitigando así el riesgo de dispositivos en riesgo La política Zero Trust autentifica al usuario en el recurso en lugar de en la red subyacente, lo que evita el movimiento lateral
3	Accede a la aplicación web [privada | pública] directamente a través de [Cloudflare Tunnel | Conector para SAML]	Cloudflare Tunnel Solucionador de DNS 1.1.1.1	Cloudflare Tunnel gestiona de forma segura una conexión con la aplicación web y elimina el uso de reglas de FW explícitas

Diseño heredado - complementos de seguridad necesarios



Diseño de Cloudflare One



Diseño heredado - complementos de seguridad necesarios

	Acción de red/seguridad	Solución heredada relevante	Fallo de diseño heredado	Complemento de seguridad necesario
1	Un dispositivo remoto se conecta a los recursos corporativos a través de una wifi pública	Cliente VPN corporativo	Un dispositivo no seguro en una red wifi pública es objetivo para los atacantes	Plataforma de protección de puntos finales (EPP)
2	El dispositivo remoto llega al perímetro corporativo a través de un cliente VPN, pero divide el resto del tráfico	Cliente VPN corporativo	La seguridad específica de la VPN no protegerá el tráfico de túnel dividido	Desactivación del túnel dividido
3	La VPN termina en el firewall perimetral o en el concentrador de VPN detrás del firewall	Equilibrador de carga Firewall perimetral Concentrador de VPN	Las reglas de FW/VPN entrantes pueden exponer puertos/protocolos a Internet, ampliando la superficie de ataque potencial	Sistema de detección de intrusiones (IDS)
4	La política del firewall concede al usuario remoto acceso a la subred con la aplicación web privada	Firewall interno	El usuario tiene acceso a recursos fuera de su función laboral	Proxy web
5	El usuario accede a la aplicación web a través de la IP/URL privada **[5a]** o la URL pública **[5b]** tras autenticarse en el IDP	Directorio activo DNS interno (privado)	Si el punto final está en riesgo, la aplicación/red de la empresa también lo está	Servidor de gestión de dispositivos móviles (MDM)

Diseño de Cloudflare One

	Acción de red/seguridad	Elemento relevante de Cloudflare One	Corrección de fallos de diseño
1	Un dispositivo remoto se conecta a los recursos corporativos y a Internet a través de Cloudflare	**Cliente de dispositivo de Cloudflare** **Política SWG** **Aislamiento del navegador**	El cliente local de SWG permite a Cloudflare One filtrar el tráfico DNS/HTTP/red al dispositivo del usuario a través de la política de la puerta de enlace. El aislamiento del navegador absorbe/aísla el impacto de los ataques exitosos de malware de los sitios web
2	El usuario se somete a comprobaciones de postura de IdP y del dispositivo en Cloudflare	**Política Zero Trust**	La política Zero Trust realiza una comprobación de la postura del dispositivo antes de permitir el acceso, mitigando así el riesgo de dispositivos en peligro La política Zero Trust autentifica al usuario en el recurso en lugar de en la red subyacente, lo que evita el movimiento lateral
3	Accede a la aplicación web [privada | pública] directamente a través de [Cloudflare Tunnel | Conector para SAML]	**Cloudflare Tunnel** **Solucionador de DNS 1.1.1.1**	Cloudflare Tunnel gestiona de forma segura una conexión con la aplicación web y elimina el uso de reglas de FW explícitas

Caso de Uso 2: Filtrado de DNS

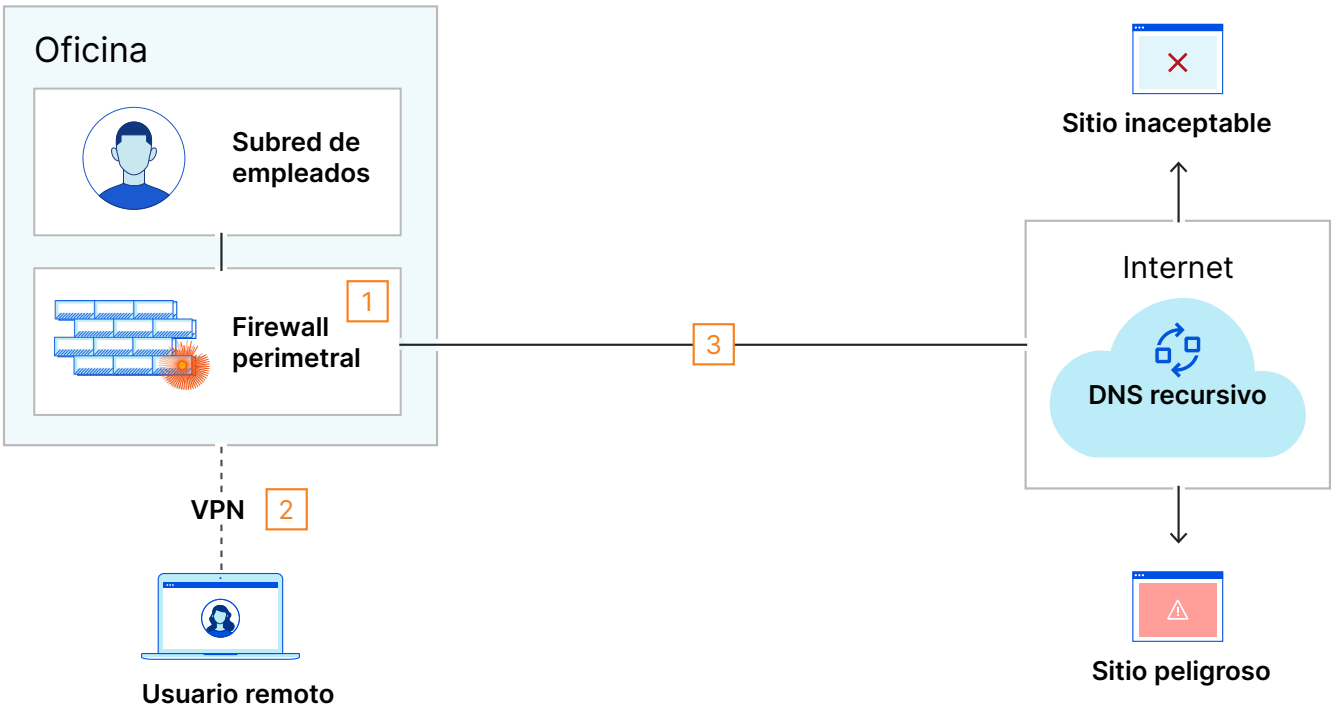
Diseño heredado - resumen

Este gráfico representa cómo las organizaciones implementan el filtrado de DNS para los usuarios que trabajan en oficinas y en remoto en un entorno heredado.

Por lo general, el filtrado de DNS para las organizaciones se lleva a cabo a través de las funciones integradas de las soluciones locales, como un firewall. Los usuarios remotos envían las solicitudes a través de este firewall primero redireccionado el tráfico a través de una VPN de túnel completo.

Para resolver los sitios web, la organización envía sus consultas DNS a un DNS recursivo (como el 8.8.8.8 de Google).

Nota: al igual que en otras secciones de esta guía, este entorno heredado no representa todas las tecnologías dentro de una oficina, solo las implicadas en este caso de uso específico.



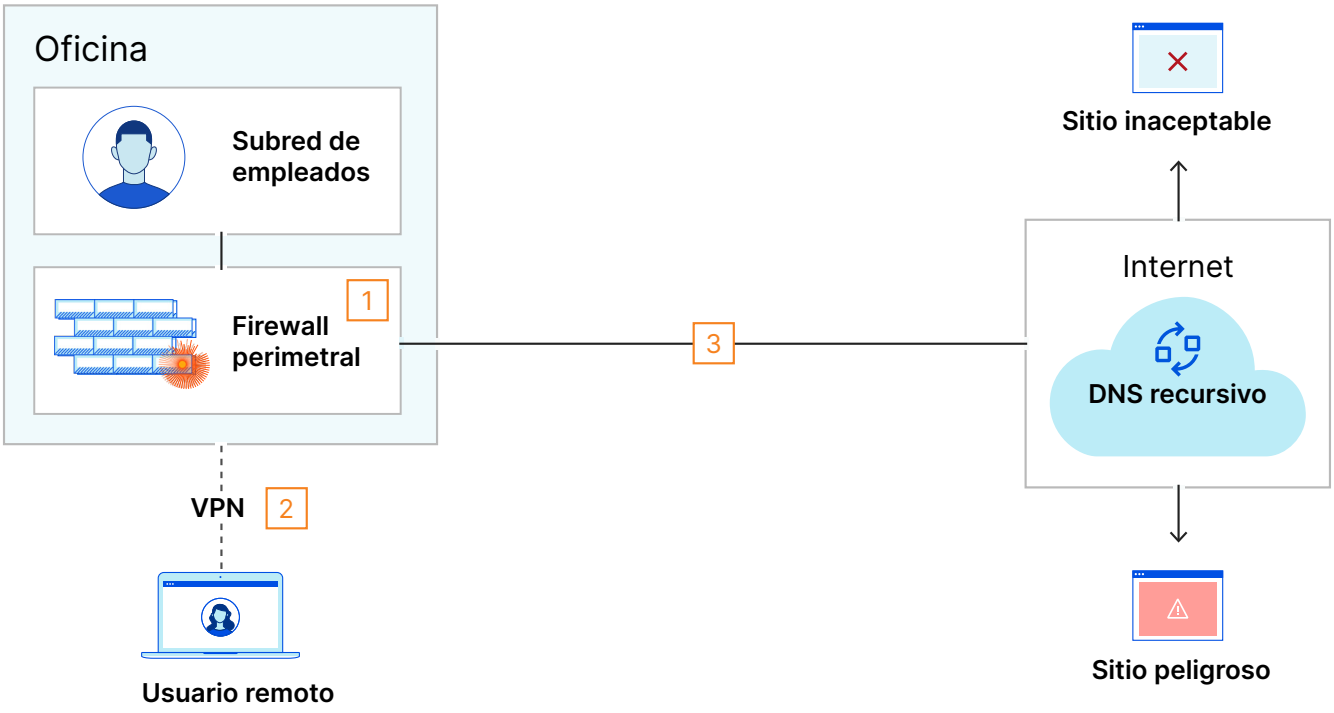
	Evento relacionado con el DNS
1	Se filtra el contenido de las soluciones de DNS de un usuario local por seguridad a través de la función incorporada en el firewall perimetral
2	Se filtran las solicitudes de DNS de un usuario local después de conectarse a la VPN de túnel completo de la organización
3	Las solicitudes de DNS salientes se transmiten sin cifrar

Diseño heredado - fallos operativos

El siguiente gráfico añade una columna a la tabla de abajo que articula los desafíos asociados con este diseño tradicional.

El reto más acuciante es que confiar en el hardware local para realizar el filtrado de DNS a escala acabará por provocar un cuello de botella en el rendimiento de todos los usuarios, especialmente cuando ese hardware también es responsable de otros servicios críticos (como la terminación de la VPN del usuario remoto).

Además, el envío de consultas DNS sin cifrado (que se produce por defecto) crea un nuevo vector de ataque con un riesgo desconocido.



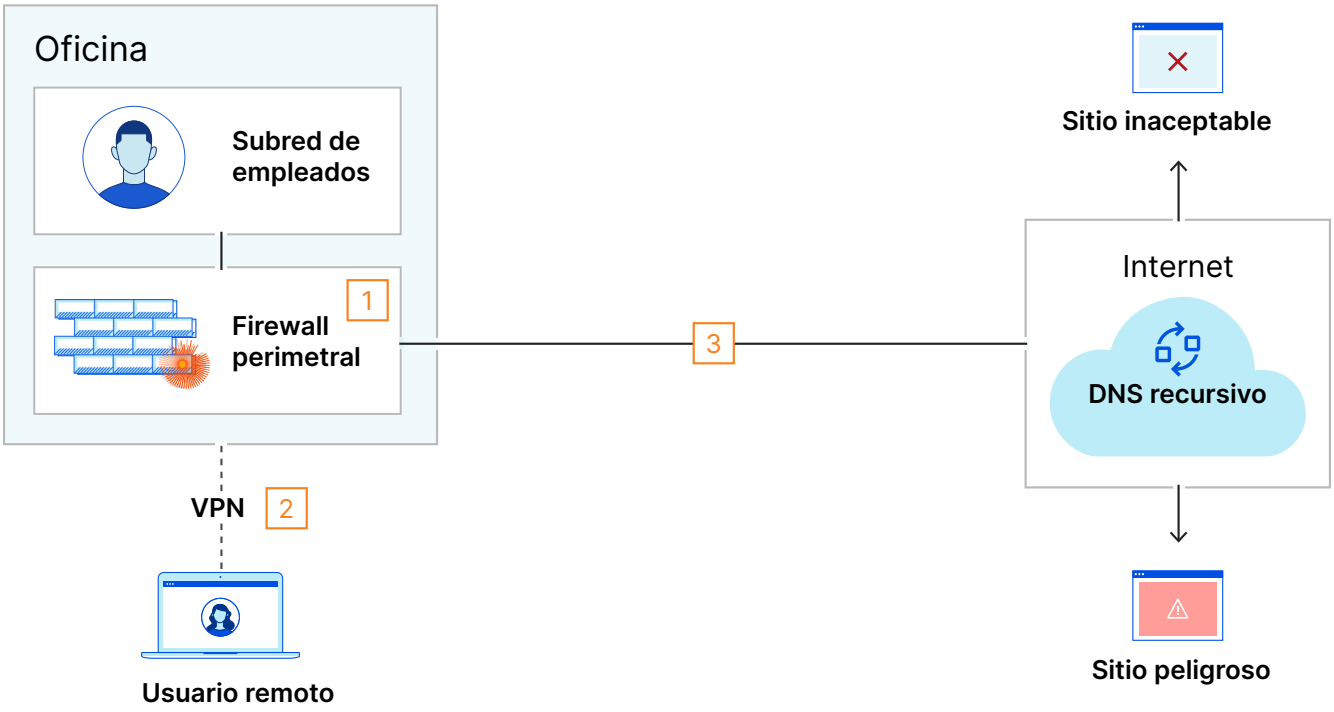
	Evento relacionado con el DNS	Elementos relevantes	Fallo de diseño
1	Se filtra el contenido de las soluciones de DNS de un usuario local por seguridad a través de la función incorporada en el firewall perimetral	Firewall perimetral	Depender del firewall perimetral para demasiadas operaciones esenciales puede impactar en el rendimiento de toda la organización
2	Se filtran las solicitudes de DNS de un usuario local después de conectarse a la VPN de túnel completo de la organización	Concentrador de VPN Firewall perimetral	Una VPN de túnel completo crea un "doble peaje" de paquetes de Internet, que puede impactar en el rendimiento para el tráfico de toda la organización a través del túnel
3	Las solicitudes de DNS salientes se transmiten sin cifrar	Puerto UDP 53	El DNS a través del puerto UDP 53 no está cifrado y, por tanto, no es privado. Cualquiera que lo vea puede reconocer el comportamiento web del usuario

Diseño heredado - requiere modificaciones en la red

Para solucionar los fallos de diseño señalados en la página anterior, la organización necesita ahora modificar su arquitectura de red existente. Este gráfico añade otra columna a la tabla de abajo, destacando las soluciones comunes con sus propios inconvenientes.

En este caso, la compra de nuevo hardware para gestionar más usuarios o aumentar el consumo de ancho de banda conllevará mayores inversiones y gastos operativos a la larga.

Las organizaciones que intentan escalar este enfoque por sí mismas a menudo se topan con problemas de crecimiento y, de hecho, muchas organizaciones evitan el filtrado de DNS por completo debido a estos problemas operativos.



	Evento relacionado con el DNS	Elementos relevantes	Fallo de diseño	Otras soluciones que no son de Cloudflare
1	Se filtra el contenido de las soluciones de DNS de un usuario local por seguridad a través de la función incorporada en el firewall perimetral	Firewall perimetral	Depender del firewall perimetral para demasiadas operaciones esenciales puede impactar en el rendimiento de toda la organización.	Filtrado DNS discreto
2	Se filtran las solicitudes de DNS de un usuario local después de conectarse a la VPN de túnel completo de la organización	Concentrador de VPN Firewall perimetral	Una VPN de túnel completo crea un "doble peaje" de paquetes de Internet, que puede impactar en el rendimiento para el tráfico de toda la organización a través del túnel	Aumentar el ancho de banda del ISP Mejora del hardware Habilitar el túnel dividido*
3	Las solicitudes de DNS salientes se transmiten sin cifrar	Puerto UDP 53	El DNS a través del puerto UDP 53 no está cifrado y, por tanto, no es privado. Cualquiera que lo vea puede reconocer el comportamiento web del usuario	DNS sobre TLS/HTTPS

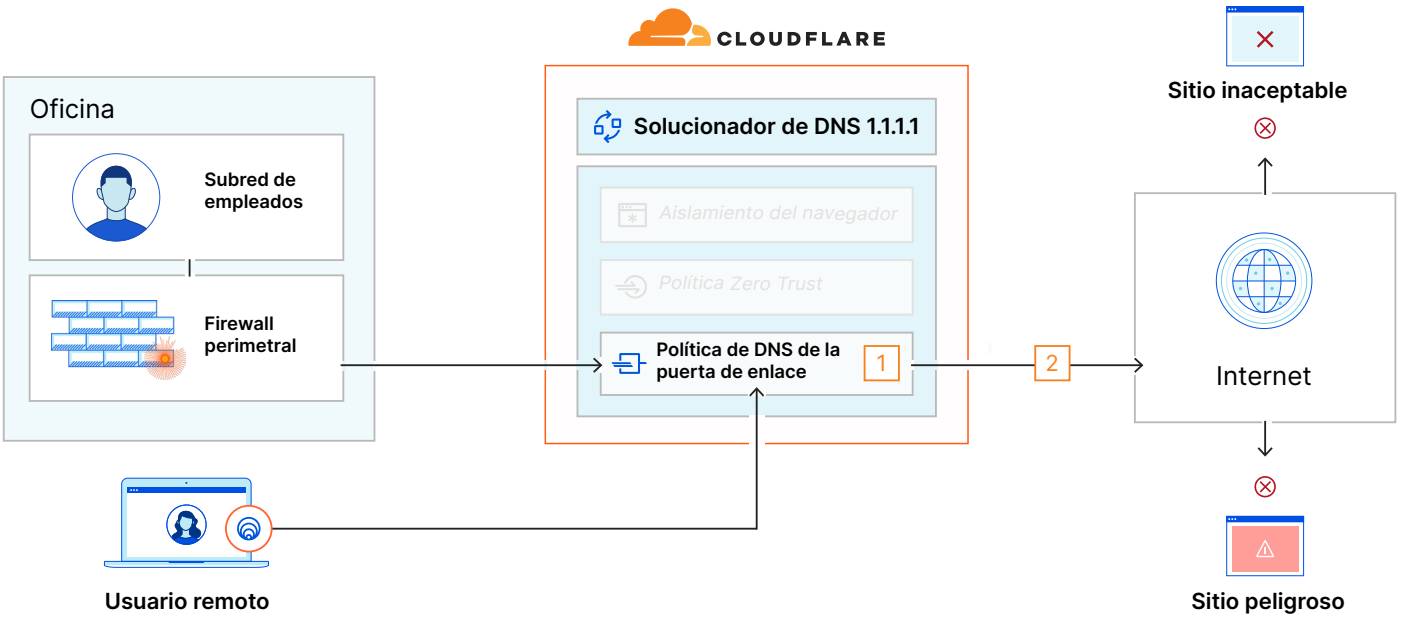
Diseño de Cloudflare One

Las organizaciones que implementan Cloudflare One dirigen su tráfico a la red global de Cloudflare y pueden realizar el filtrado de DNS para todos sus usuarios sin preocuparse de los límites operativos de su hardware local.

El filtrado de DNS de Cloudflare es fácil de implementar tanto para usuarios locales como remotos:

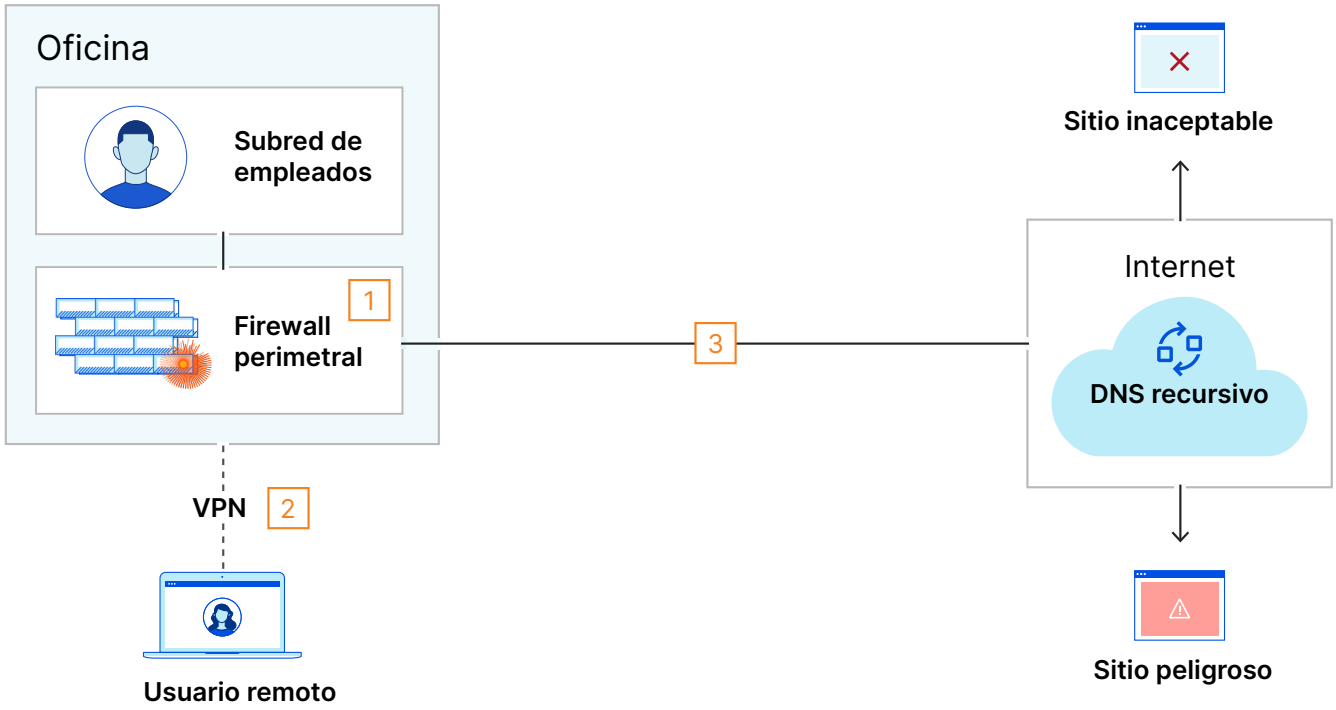
- El tráfico de los usuarios de la oficina se envía a Cloudflare basándose en la IP de salida del firewall perimetral.
- El tráfico de los usuarios remotos se envía a Cloudflare desde nuestro cliente de dispositivo.

Además, el solucionador de DNS de Cloudflare, 1.1.1.1, admite DNS sobre TLS/HTTPs, lo que resuelve el problema de seguridad detallado en el entorno heredado.

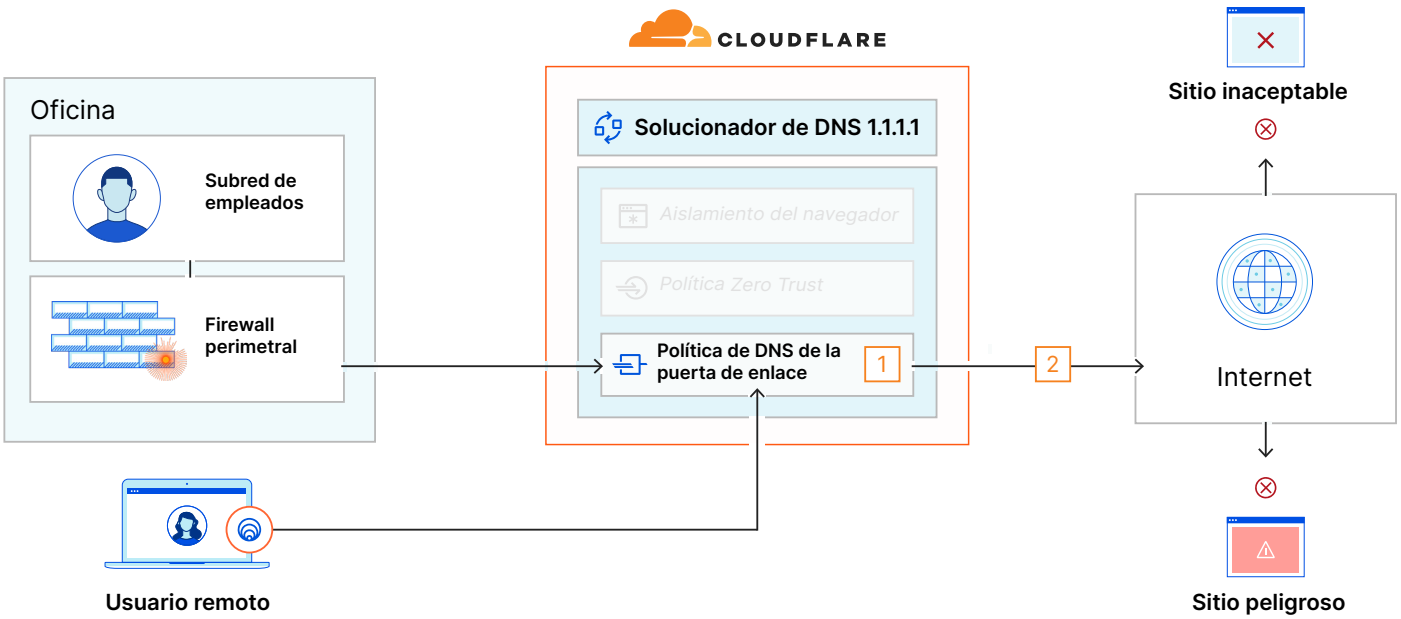


	Evento relacionado con el DNS	Elemento relevante de Cloudflare One	Corrección de fallos de diseño
1	Cloudflare filtra el contenido de las solicitudes de DNS tanto de los usuarios locales como remotos	SWG	Las políticas DNS de Gateway descargan el filtrado de DNS del hardware local (o lo proporcionan por primera vez)
2	Las solicitudes de DNS de la organización se cifran antes su envío	Solucionador de DNS 1.1.1.1	El solucionador de DNS 1.1.1.1 de Cloudflare admite DNS sobre TLS/HTTPs, lo que resuelve el problema de seguridad detallado en el entorno heredado

Diseño heredado



Diseño de Cloudflare One



Diseño heredado

	Evento relacionado con el DNS	Elementos relevantes	Fallo de diseño	Otras soluciones que no son de Cloudflare
1	Se filtra el contenido de las soluciones de DNS de un usuario local por seguridad a través de la función incorporada en el firewall perimetral	Firewall perimetral	Depender del firewall perimetral para demasiadas operaciones esenciales puede impactar en el rendimiento de toda la organización	Filtrado DNS discreto
2	Se filtran las solicitudes de DNS de un usuario local después de conectarse a la VPN de túnel completo de la organización	Concentrador de VPN Firewall perimetral	Una VPN de túnel completo crea un "doble peaje" de paquetes de Internet, que puede impactar en el rendimiento para el tráfico de toda la organización a través del túnel	Aumentar el ancho de banda del ISP Mejora del hardware Habilitar el túnel dividido*
3	Las solicitudes de DNS salientes se transmiten sin cifrar	Puerto UDP 53	El DNS a través del puerto UDP 53 no está cifrado y, por tanto, no es privado. Cualquiera que lo vea puede reconocer el comportamiento web del usuario	DNS sobre TLS/HTTPS

Diseño de Cloudflare One

	Evento relacionado con el DNS	Elemento relevante de Cloudflare One	Corrección de fallos de diseño
1	Cloudflare filtra el contenido de las solicitudes de DNS tanto de los usuarios locales como remotos	SWG	Las políticas DNS de Gateway descargan el filtrado DNS del hardware local (o lo proporcionan por primera vez)
2	Las solicitudes de DNS de la organización se cifran antes su envío	Solucionador de DNS 1.1.1.1	El solucionador de DNS 1.1.1.1 de Cloudflare admite DNS sobre TLS/HTTPs, lo que resuelve el problema de seguridad detallado en el entorno heredado