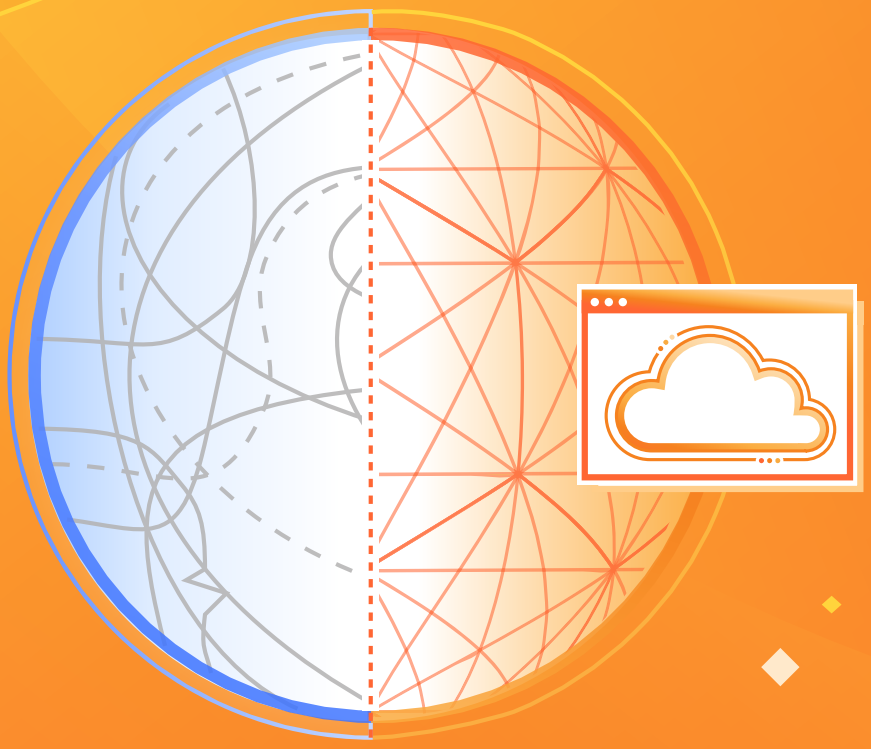
CLOUDFLARE

DOCUMENTO TÉCNICO

Cómo desarrollar una estrategia para modernizar tu red



Contenido

3 **Redes heredadas, un obstáculo para la modernización digital**

4 **Tu recorrido**

5 **Cuatro rutas clave del tráfico de red**

6 **Conectividad cloud de Cloudflare**

7 **Principales casos de uso para la modernización de la red**

7 Conectividad de filiales

8 Protege tu infraestructura accesible desde Internet

9 Simplifica tu red corporativa

9 Migración de zonas perimetrales (DMZ)

10 Sustitución de la tecnología VPN por una solución ZTNA

10 Eliminación de la confianza elevada en las redes LAN

10 Aceleración de la conectividad en los procesos de fusión y adquisición

11 Conecta y protege tus nubes

12 **Próximos pasos**

Redes heredadas, un obstáculo para la modernización digital

La agilidad es una ventaja crucial para sobresalir en un mundo en el que las condiciones empresariales pueden cambiar de forma repentina. Sin embargo, no es solo una cuestión de liderazgo y de decisión, la agilidad también depende de la capacidad de las organizaciones para ejecutar el cambio. Se deben crear sistemas flexibles con capacidad de adaptación, sin provocar fallos. Las empresas deben poder reorganizarse para adaptarse a nuevos modelos de ingresos, admitir nuevas aplicaciones y conectar a usuarios de todo el mundo.

La agilidad es uno de los resultados más deseados en los proyectos de modernización digital, mientras las organizaciones se reacondicionan para obtener ventajas competitivas. Esto es especialmente cierto si se tiene en cuenta el estado de la red empresarial tradicional, que desempeña un papel fundamental a la hora de proporcionar comunicaciones y facilitar la colaboración. La red empresarial se ha resistido obstinadamente al cambio, y con razón. Se diseñó para resistir los vaivenes del sistema, pero los cambios acarrean un precio muy alto y requieren grandes esfuerzos.

A veces se pueden anticipar, porque se producen gradualmente, como los efectos de la nube en el centro de datos. En lo que respecta a las redes, las fuerzas exógenas del mercado impulsan cambios rápidos, a veces repentinos. Por ejemplo, la pandemia nos dejó enseñanzas sobre lo difícil que era para algunas empresas añadir capacidad para implementar con rapidez el teletrabajo, mantener la productividad de los empleados y gestionar los costes en vista del peaje de la inactividad de la red en las oficinas vacías.

A pesar de estas dificultades, también resultó evidente la capacidad de otras empresas no solo para adaptarse, sino también para progresar. No se trataba únicamente de la capacidad de los equipos directivos para tomar decisiones empresariales adecuadas, sino también de la capacidad de las empresas para transformar y ejecutar los procesos del negocio. Los directores de informática deben desarrollar estrategias para afrontar el cambio, modernizar el negocio para satisfacer las necesidades futuras y permitir que los equipos informáticos aceleren la transformación en lugar de frenarla.

Teniendo en cuenta las inversiones masivas que exigen las redes locales, la modernización no es una decisión sencilla. Para aprovechar plenamente las ventajas de la modernización de la red, es necesario examinar lo que hay que conseguir para definir lo que se debe cambiar.

Tu recorrido

Si consideras las prácticas recomendadas para diseñar tu red a lo largo de los años, te darás cuenta de que la complejidad existente obedece a una buena razón. Durante décadas, las organizaciones crearon y consolidaron sus redes añadiendo capas y capas de nueva tecnología. Cada generación de diseño de red, y cada nueva innovación, aumentaba la complejidad de la red. No existía la posibilidad de buscar la simplicidad, y a menudo la incorporación de nueva tecnología complicaba aún más la velocidad, la resiliencia y la seguridad.

Con los servicios de seguridad y redes en la nube, ahora estamos a la vanguardia del próximo cambio generacional en el diseño de redes empresariales. El uso de servicios en la nube como una extensión de la red permite a las organizaciones abordar nuevos casos de uso, ampliar su cobertura y proteger las aplicaciones mucho más allá del centro de datos. Representa una oportunidad para simplificar enormemente la red, porque la prestación de servicios se basa en la conexión de red existente con el punto de presencia (PoP) del proveedor de nube, sin interrumpir la conexión para incorporar nuevos dispositivos. La conexión entre la red local y el servicio en la nube sigue siendo la misma, si bien se incluyen y usan los servicios dentro del servicio en la nube.

El problema es que no todas las plataformas de red y seguridad en la nube se crean igual, y no siempre es fácil ver las diferencias entre unas y otras. Muchas tienen ventajas limitadas en el recorrido hacia la modernización. Para entender las diferencias, es necesario trazar tus objetivos de modernización de la red para evitar sustituir una fuente de complejidad por otra.

Cuatro rutas clave del tráfico de red

Cuando evalúes el alcance de tu proyecto de modernización de red, ten en cuenta que tu red abarca un amplio número de puntos de contacto, algunos de los cuales confluyen en la misma infraestructura (por ejemplo, el tráfico entrante o saliente o este-oeste que pasa a través de tu red principal), si bien otros operan fuera de la infraestructura (como tu conexión a la nube pública).

Tráfico entrante: algunas partes de la red están expuestas a Internet, de ahí que sea necesario proteger el acceso contra los intentos de incapacitar o vulnerar la empresa, sin impedir el paso del tráfico legítimo. Las defensas perimetrales tradicionales pueden verse desbordadas y requieren capacidades para hacer frente a los ataques de denegación de servicio distribuido.

Tráfico saliente: las conexiones a Internet y a las aplicaciones basadas en la nube requieren políticas que proporcionen protecciones para un uso empresarial seguro, como la protección contra amenazas y la filtración de datos. Dada la variabilidad de la ubicación de un usuario, las organizaciones han implementado una combinación de tecnologías de protección del tráfico saliente que incluyen dispositivos internos como firewalls (para cuando el usuario está en la red), solucionadores DNS, así como proxies basados en la nube como SWG y CASB (para cuando el usuario está en remoto).

Redes WAN: las redes WAN, así como los límites que cubren, incluidos el campus y las sucursales, se están rediseñando para dar soporte a las iniciativas que dan prioridad a la nube y a los dispositivos habilitados para IoT. Como tal, la topología de red tradicional está revirtiendo la red de retorno al centro de datos en favor de arquitecturas directas a Internet. Asimismo, los rápidos avances de las redes en estas áreas han incrementado la complejidad a la hora de incorporar la seguridad. En muchos casos, las rutas de tráfico interno siguen dependiendo de dispositivos de seguridad implementados en el perímetro, lo que impide el progreso transformador de la organización.

Conexiones a nubes públicas: a medida que las organizaciones desarrollan sus aplicaciones en entornos multinube, resulta cada vez más difícil establecer y mantener configuraciones de red y seguridad punto a punto. La configuración y la gestión de la red consumen tiempo y recursos — un tiempo que se podría emplear en el desarrollo de proyectos.

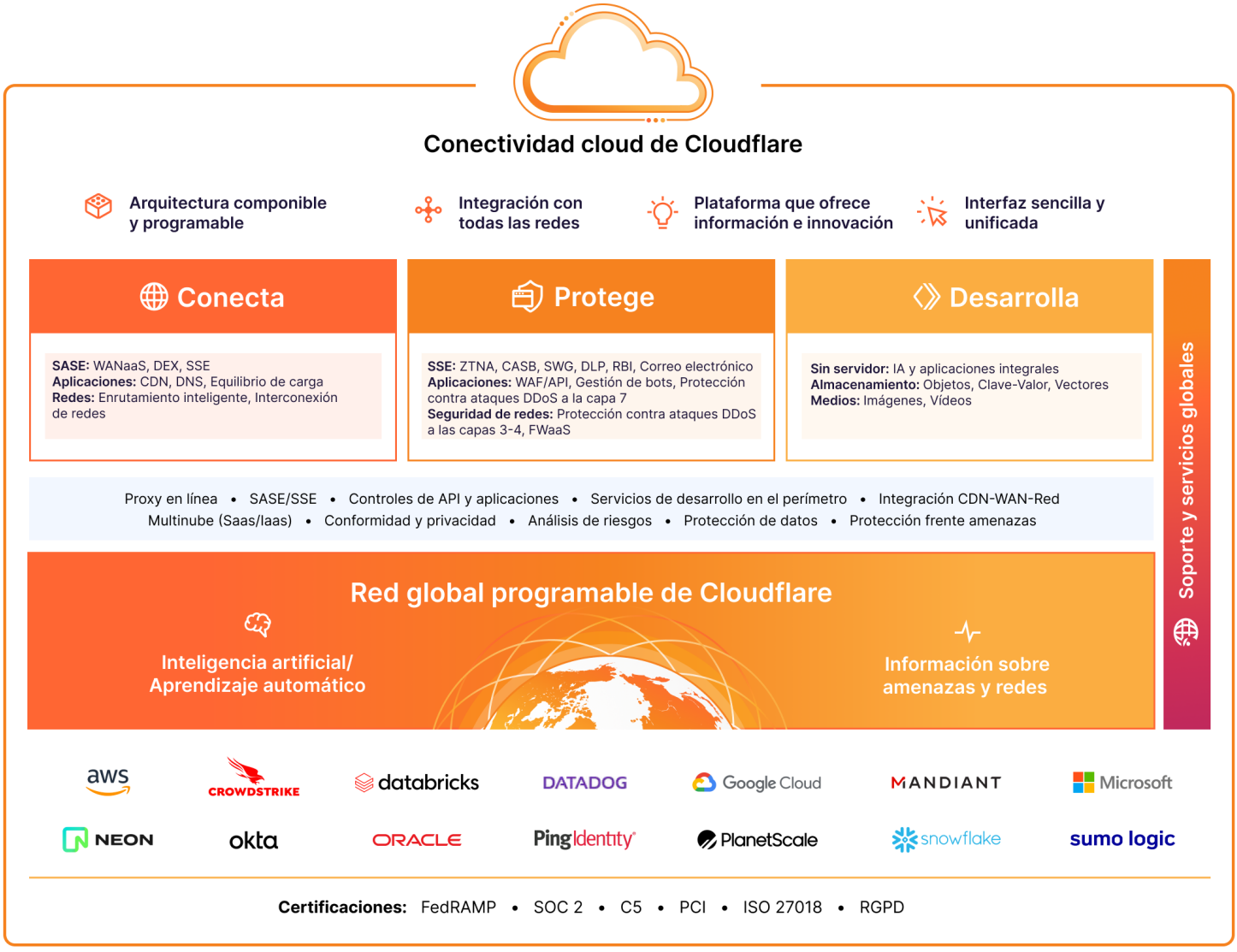
Cada una de estas rutas de tráfico tiene una serie de tecnologías que las organizaciones implementan en su red o usan de la nube. Dado que los proyectos de modernización tocan rutas de tráfico en numerosas direcciones, es necesario planificar el recorrido completo de la modernización de la red en las cuatro direcciones para evitar cometer un error de arquitectura que limite los beneficios de transformación alcanzables o requiera numerosas tecnologías dispares para abordar casos de uso sin resolver.

Conectividad cloud de Cloudflare

Considera la conectividad cloud de Cloudflare para modernizar tus redes. Se ha diseñado en torno a una filosofía que propone el uso de una arquitectura programable y modular para brindar servicios de redes y de seguridad a tus usuarios y a tu infraestructura empresarial y aplicaciones en la nube. Por lo tanto, aborda tanto las necesidades actuales como futuras en tu recorrido hacia la modernización.

Con Cloudflare, puedes añadir funcionalidad y admitir nuevos casos de uso habilitando servicios, en vez de incorporando dispositivos. La conexión a un centro de datos Anycast de Cloudflare sigue siendo la misma, mientras configuras e implementas servicios desde la interfaz de gestión unificada para procesar el tráfico. Puedes abordar las necesidades actuales a la vez que pones en marcha la plataforma para admitir casos de uso futuros y respaldar todo tu recorrido de modernización de la red.

En lugar de crear una infraestructura global, utiliza la nuestra. Tu organización se beneficia de la velocidad ultrarrápida que se ofrece a través de la red global de Cloudflare. Nuestras conexiones directas con casi todos los proveedores de servicios y proveedores de soluciones en la nube permiten a nuestra red llegar al 95 % de los internautas a nivel global en aproximadamente 50 m/s.



Principales casos de uso para la modernización de la red

Para empezar, comienza con casos de uso que impacten en tu negocio y ofrezcan beneficios más significativos a tu organización. Estos casos de uso no tienen un orden concreto, ya que tus prioridades son exclusivas de tu empresa. Lo importante es abordar las necesidades a corto plazo y, al mismo tiempo, crear una arquitectura que te ayude en tu recorrido hacia la modernización de la red, sea cual sea el camino que tomes.

	Proyectos de modernización
Conectividad de filiales Reduce los costes, mejora la experiencia del usuario	• Migra de la red MPLS a la conectividad cloud • Migra de la red SD-WAN a la conectividad cloud
Protege tu infraestructura accesible desde Internet Prolonga la vida útil de las inversiones en firewall y DMZ	• Reduce la carga de los firewalls de red • Cambia la seguridad DMZ a la conectividad cloud
Simplifica tu red corporativa Implementa Zero Trust para mejorar la seguridad y reducir los gastos de capital	• Reduce/Elimina la DMZ • Sustituye la VPN por ZTNA • Elimina la confianza elevada en la LAN • Acelera la conectividad en los procesos de fusión y adquisición
Conecta y protege tus nubes Utiliza lo mejor de cada nube en tus aplicaciones	• Crea y protege tus aplicaciones • Usa los servicios para desarrolladores para centralizar las funciones básicas

Conectividad de filiales

Un componente importante de las redes WAN es conectar los sitios más pequeños, como filiales o tiendas, que dependen de la conexión de usuarios y dispositivos a las aplicaciones. Las arquitecturas tradicionales en estrella tipo hub-and-spoke conectaban los sitios con el centro de datos utilizando circuitos MPLS caros, pero con la creciente necesidad de admitir aplicaciones en la nube, cada vez más organizaciones utilizan arquitecturas directas a Internet con banda ancha.

SD-WAN pretendía hacer más fiable la conectividad de red, pero tiene una relación imperfecta con la incorporación de seguridad. La mayoría de las arquitecturas SD-WAN se basan en dispositivos perimetrales pesados y firewalls locales para aplicar políticas de seguridad sobre la estructura SD-WAN, y solo utilizan la integración SSE/SASE para el tráfico saliente.

Utiliza la conectividad cloud de Cloudflare para conectar tus sucursales y apoyar tu ruta de migración completa, ya sea aumentando o sustituyendo los servicios heredados. Cloudflare utiliza una arquitectura basada en una filosofía de "perímetro ligero/nube pesada" para prestar servicios de red y seguridad. Facilita la conectividad entre ubicaciones de red (sucursales, tiendas o plantas de producción) con Cloudflare Magic WAN. Ofrece conectividad y enrutamiento seguros y eficaces para toda tu red corporativa, reduciendo los costes y la complejidad operativa. En cuanto a la seguridad, Cloudflare Magic Firewall se implementa fácilmente junto con Magic WAN, lo que te permite aplicar políticas de control de red tanto norte/sur como este/oeste a medida que el tráfico transita por la red de Cloudflare.

Protege tu infraestructura accesible desde Internet

La red de la empresa y la DMZ son direccionables, están expuestas a Internet y requieren medidas para impedir que los atacantes causen daños. En un mundo perfecto, los firewalls de red tradicionales podrían inspeccionar y eliminar todo el tráfico no deseado, pero cada firewall tiene capacidades limitadas (ancho de banda disponible, utilización/proceso, recuento de sesiones, etc.). El éxito del ataque es simplemente una cuestión de escala, es decir, si el atacante puede generar suficiente ruido para abrumar la capacidad de la empresa y operar a través de diferentes capas del protocolo de red.

No se trata solo del volumen de tráfico. Aceptar tráfico entrante abre la superficie de ataque al tráfico no autenticado/autenticado previamente. Un atacante puede explotar los fallos en aplicaciones y sistemas operativos sin tener una cuenta en el sistema. El relleno de credenciales o el uso de nombres de usuario/contraseñas conocidos de otras fugas también conllevan riesgos importantes. La aplicación de los principios Zero Trust a las aplicaciones en la DMZ permite a las organizaciones reducir la exposición a Internet, y eliminarla cuando sea posible.

Las organizaciones pueden mejorar la protección de su red aplicando principios de una estrategia de protección integral para absorber el tráfico malicioso desde un ordenador o red de la infraestructura de la organización accesible desde Internet. Cloudflare Magic Transit, que integra Magic Firewall y que se implementa a través de la red Anycast de Cloudflare, actúa como puerta de entrada a la organización, filtra el tráfico malicioso e innecesario y entrega solo el tráfico entrante legítimo.

Cuando los firewalls de red mitigan un ataque DDoS en un dispositivo, este aún tiene que procesar la conexión antes de poder eliminarla. Con Cloudflare, nuestra red difunde el prefijo del cliente, atrayendo así el tráfico que de otro modo se destinaría al firewall perimetral. De esta forma, estamos absorbiendo eficazmente el ataque DDoS al distribuir la carga por todos nuestros centros de datos. Los miembros de la botnet ven el PoP Anycast más cercano, que procesa el tráfico de acuerdo con las políticas de Magic Transit y Magic Firewall.

Simplifica tu red corporativa

La simplificación conlleva una serie de ventajas de modernización. Los equipos informáticos pueden hacer que la red sea más fiable si su diseño tiene menos componentes que puedan fallar, y más segura si adoptan un enfoque Zero Trust de denegación de todos los privilegios de acceso.

Para simplificar tu red, considera:

Migración de zonas perimetrales (DMZ)

Las DMZ de red son un quebradero de cabeza operativo, ya que son especialmente sensibles a las vulnerabilidades de día cero. Un atacante no necesita acceso a la red interna para comunicarse con los servidores de la DMZ, por lo que las organizaciones tienen que permanecer atentas para evitar vulnerabilidades y abusos.

Sin embargo, aunque las DMZ desempeñaron un papel importante en el pasado, ¿son necesarias hoy en día? La creación de redes a través de DMZ está perdiendo importancia, porque hay formas alternativas de crear y alojar aplicaciones.

- Para las aplicaciones accesibles desde Internet, la migración de las cargas de trabajo a la nube pública tiene ventajas económicas y técnicas.
- Con SaaS, no es necesario ejecutar muchos tipos de aplicaciones públicas y privadas en infraestructuras gestionadas por el cliente.

Como tal, es pragmático desde el punto de vista de la seguridad y del diseño de la red empezar a pensar en cómo reducir o eliminar la necesidad de una DMZ. No solo tiene sentido desde un punto de vista operativo, sino que también simplifica enormemente la arquitectura al eliminar la infraestructura de red, como el firewall, el WAF y los equilibradores de carga que la protegen.

¿Qué ocurre con las aplicaciones privadas que se colocan en la DMZ para ampliar el acceso a empleados, socios y proveedores? Sería más seguro aislarlas en una red privada y ampliar el acceso a empleados y socios mediante el acceso a la red Zero Trust (ZTNA).

Con ZTNA, reduces eficazmente la superficie de ataque eliminando el tráfico de red entrante a la aplicación. ZTNA utiliza un acceso contextual y con intermediario a los recursos a través de la conectividad cloud de Cloudflare. De esta manera, se elimina la necesidad de abrir puertos en el firewall de la red y se proporciona al equipo de seguridad una visibilidad total sobre quién tiene acceso a qué recurso.

Sustitución de la tecnología VPN por una solución ZTNA

Los días de utilización de las VPN para acceder a las aplicaciones se están acabando. Desde el punto de vista del diseño de la red, no es práctico contener a los usuarios en un túnel muy largo para acceder a Internet y a la nube. También es una gran amenaza para la seguridad exponer a los usuarios (y puntos finales potencialmente en riesgo) a la red con una VPN.

El acceso a las aplicaciones tampoco es la única función de una VPN. Hay escenarios en los que las organizaciones necesitan una conectividad de red más amplia con un punto final, como con la administración de puntos finales y las comunicaciones iniciadas por el servidor. Estos casos de uso aprovechan tradicionalmente la conectividad de red de la VPN en ambas direcciones, y dejaron sin opciones a los primeros productos ZTNA del mercado. Sin alternativa, las organizaciones utilizaban ZTNA y VPN en paralelo.

Para modernizar la infraestructura de red, las organizaciones pueden consolidar las funciones con la solución ZTNA de Cloudflare. Esto se debe a que, con Cloudflare, las organizaciones pueden admitir tanto casos de uso clásicos de ZTNA como el tráfico iniciado por el servidor y el tráfico bidireccional. Estas funciones ayudan a las organizaciones a resolver sus necesidades de acceso a aplicaciones eliminando la VPN, y a promover mejoras de seguridad y la simplicidad.

Eliminación de la confianza elevada en las redes LAN

Con el trabajo híbrido, cada vez hay menos diferencias entre la forma de trabajar presencialmente en la oficina o en cualquier otra ubicación. De hecho, esto es especialmente cierto cuando los usuarios trabajan con frecuencia en redes públicas no fiables que se encuentran en cafeterías y espacios de trabajo compartidos.

En cierto modo, la red pública abierta es el arquetipo de Zero Trust: nadie tiene acceso privilegiado y nadie ni nada es digno de confianza. Si en principio puede funcionar en un espacio de trabajo compartido, en casa y en la cafetería, ¿por qué no puede eliminarse también la confianza en la red de la empresa?

La eliminación de la confianza no requiere avanzar en el diseño de la red, sino simplificarlo. En lugar de crear accesos con privilegios elevados para usuarios autenticados y utilizar políticas de red para abrir conexiones a los recursos, es mucho más seguro suponer que la red no es fiable. Con la expresión de la seguridad mediante SASE, las organizaciones pueden obtener el acceso a las aplicaciones que necesitan, con la seguridad adecuada para que sea seguro hacerlo, sin necesidad de ninguna presunción de confianza en la propia red. Un modelo Zero Trust no consiste en añadir confianza a la red, sino en eliminarla hasta alcanzar un estado mejor y más seguro, sin los permisos explícitos y excesivos del pasado.

Aceleración de la conectividad en los procesos de fusión y adquisición

Las organizaciones utilizan las fusiones y adquisiciones como herramienta para adquirir acceso a recursos y capacidades empresariales que de otro modo no estarían inmediatamente disponibles. Para aprovechar la oportunidad, las organizaciones deben actuar con rapidez para que la empresa integrada sea mejor que la suma de sus partes. Sin embargo, los equipos de informática no suelen ser capaces de actuar con rapidez, porque las aplicaciones y la infraestructura de red subyacente de dos organizaciones rara vez se engranan con facilidad.

Para acelerar la conectividad en los procesos de fusión y adquisición, las organizaciones pueden enfocar el acceso a las aplicaciones como una tarea independiente de la integración de redes. El calendario para diseñar una arquitectura de red convergente puede alargarse durante años, pero el acceso a las aplicaciones no tiene por qué depender de un hito tan lejano.

Esto se debe a que la situación en el día 1 es efectivamente un caso de uso Zero Trust, en el que los usuarios de confianza en redes no fiables siguen necesitando acceso a las aplicaciones. Amplía el acceso con Cloudflare One, que ofrece los medios para habilitar la conectividad en los procesos de fusiones y adquisiciones sin estar condicionada al acceso a redes convergentes.

Conecta y protege tus nubes

A medida que evoluciona el desarrollo de la nube, sus componentes serán beneficiosos para reutilizarse dentro de otra. Al igual que cada organización se convertirá en multinube de forma gradual, cada organización necesitará gestionar las conexiones a nubes públicas gradualmente. El desarrollo de aplicaciones tiende a ser tribal por naturaleza. Los equipos DevOps trabajan en diferentes partes de la organización y prefieren las herramientas con las que están más familiarizados. Sin embargo, el desarrollo de capacidades organizativas para gestionar la conectividad entre nubes es complejo, ya que el trabajo abarca conjuntos de herramientas desarrolladas sobre marcos totalmente distintos.

Otro aspecto de la complejidad de la multinube es el ámbito de la nube híbrida. La nube híbrida mezcla la nube privada en entornos locales con nubes privadas virtuales. Estas redes se desarrollan a veces con redes dedicadas, como AWS Direct Connect, que pueden ser caras y limitarse a una sola nube.
A medida que las organizaciones desarrollan aplicaciones multinube, no necesariamente quieren incurrir en los costes de una red dedicada para cada nube.

En lugar de crear redes y seguridad directamente de una aplicación a otra, utiliza las soluciones de Cloudflare para orquestar y conectar los servicios de red de las nubes públicas. Creemos que la conectividad cloud de Cloudflare desempeña un papel ideal en una arquitectura de este tipo, ya que está idealmente situada como tránsito para el tráfico que pasa entre nubes a través de nuestra vasta red. Con la incorporación de las capacidades de gestión de conexiones a la nube pública, ahora los clientes también pueden orquestar la configuración de la conectividad de la carga de trabajo a través de Cloudflare.

Nuestra red de nube pública va más allá de la mera orquestación de la tecnología y conexiones subyacentes, ya que ofrece servicios para desarrolladores, que están disponibles para crear e integrar aplicaciones multinube. La plataforma para desarrolladores te proporciona un completo ecosistema de tecnología básica desarrollado sobre código y estándares abiertos. Puedes elegir utilizar todos los elementos de la plataforma para desarrolladores o solo los que tú elijas, sin limitarte a los servicios concretos de una nube determinada.

Pasos siguientes

Para avanzar en tu recorrido hacia la modernización de la red, ponte en contacto con Cloudflare y deja que te ayudemos a desarrollar una estrategia. Hemos trabajado estrechamente con miles de clientes en la transición de su arquitectura a la conectividad cloud de Cloudflare.

Para más información, visita http://www.cloudflare.com

CLOUDFLARE

© 2024 Cloudflare, Inc. Todos los derechos reservados.
El logotipo de Cloudflare es una marca comercial de Cloudflare.
Todos los demás nombres de empresas y productos pueden ser marcas comerciales de las respectivas empresas a las que están asociados.

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

REV:BDES-5483.30ENE2024