kyndryl / CLOUDFLARE

DOCUMENTO TÉCNICO

La necesidad de la convergencia de la red y la seguridad

Contenido

Evolución de la red

Lo que "solía ser" es lo que sigue siendo para muchas organizaciones. Las redes se crearon para conectar un punto A con un punto B de forma muy controlada, estática y centrada en el hardware. Las redes eran responsables de la barrera de protección, o "foso", que rodeaba a la empresa, la cual contenía su infraestructura. Tal vez había sucursales y varios centros de datos, pero tú eras el único propietario y tenías el control total de la infraestructura y de la conectividad de punto a punto.

Tres tendencias principales han alterado esta arquitectura de red tan simple.

1. La adopción de la nube para el alojamiento de los procesos y las aplicaciones
2. Los usuarios remotos y móviles que trabajan desde cualquier lugar
3. Nuevas arquitecturas de datos con información que reside en el centro de datos, en dispositivos móviles, vinculada a servicios SaaS, en la nube

Como resultado, el perímetro tradicional ha desaparecido. Sin embargo, muchas organizaciones aún utilizan muchos elementos de la red tradicional, junto con los nuevos servicios de conectividad y las herramientas necesarias para conectar los usuarios remotos y las nubes. Esto crea una red fragmentada que es difícil de gestionar y no puede mantener el ritmo de una empresa digital actual.

Desafíos de la red

Las aplicaciones se desarrollan más rápido, pero el tiempo de comercialización y la agilidad se ven obstaculizados por la lentitud de los cambios en la red para adaptarse.

Los equipos están atrincherados en silos organizativos y técnicos que antes tenían sentido, pero que ahora frenan los cambios necesarios.

La red tradicional no puede actuar como un agente eficaz de aplicación de políticas.

La evolución orgánica de las tecnologías de red puede haber resuelto los problemas inmediatos. No obstante, la incorporación de soluciones específicas genera nuevos problemas de interoperabilidad y complejidad de gestión.

La red nunca se diseñó para ser inteligente. Era una forma de conectar un sitio a otro, un servidor a otro, un dispositivo a otro. Se ha producido cierta evolución con la definición por software y la abstracción de la capa de hardware para facilitar el cambio y hacer posibles características como la microsegmentación y SD-WAN. Sin embargo, la mayoría de las organizaciones se encuentran en una fase inicial de este proceso, que debería respaldar los objetivos de seguridad y estar más interrelacionado con ellos.

El estado de la seguridad y sus desafíos

Paralelamente, el trabajo de seguridad también ha crecido en complejidad. Además de la incorporación de la nube, las plantillas híbridas, los datos distribuidos y las aplicaciones que amplían exponencialmente la superficie de ataque y erosionan la visibilidad y el control, las ciberamenazas han crecido en volumen, velocidad y sofisticación.

La respuesta habitual a las amenazas emergentes es añadir una nueva herramienta que se centre en ese problema concreto. Esta "mejor" estrategia puede resolver los problemas inmediatos, pero aumenta la complejidad y la deuda técnica que se agrava con el tiempo. La seguridad se ha convertido en un trabajo ruidoso y repleto de herramientas. Se dedica experiencia a comprender y manejar las decenas de herramientas del arsenal y a filtrar alertas dispersas y sin priorizar, en lugar de instituir estrategias y marcos integrales para abordar de forma inteligente las amenazas potenciales y garantizar una recuperación rápida.

A esto hay que añadir la presión del cumplimiento y los nuevos niveles de rigurosidad necesarios para demostrar la ciberseguridad y la capacidad de recuperación a efectos de la responsabilidad a nivel ejecutivo, la respuesta a complejas auditorías y los requisitos de los seguros cibernéticos.

La visión: convergencia de la red y la seguridad

El estado de las redes es una combinación de red local heredada, focos de MPLS, oficinas remotas conectadas y conectividad personalizada a cada nube mediante herramientas nativas. Lo que se necesita es un lugar donde todos estos elementos puedan combinarse y generar un cambio de paradigma de superconectividad con seguridad. Porque no se trata solo de dónde procede una solicitud, sino de quién la remite.

Zero Trust y marcos de seguridad

Zero Trust supone un cambio de paradigma en la forma de considerar el rol de la red. En una red de "foso" tradicional, el guardia está en la puerta, pero una vez concedido el acceso, eres libre de recorrer el castillo sin restricciones. En una arquitectura Zero Trust, la suposición por defecto es que los usuarios, los dispositivos y la aplicación no deberían tener acceso a menos que se demuestre lo contrario. La suposición es que ya se ha producido una violación de la seguridad y que cada solicitud podría proceder de un actor malicioso. Este cambio de mentalidad permite a los equipos diseñar una red segura que abarque el centro de datos, la nube, el perímetro y los dispositivos y usuarios móviles, y que puede incluir componentes que no sean de tu propiedad o sobre los que no tengas el control. Podemos decir que Zero Trust es el único enfoque que te permite ampliar tu red a la nube y al perímetro de forma segura.

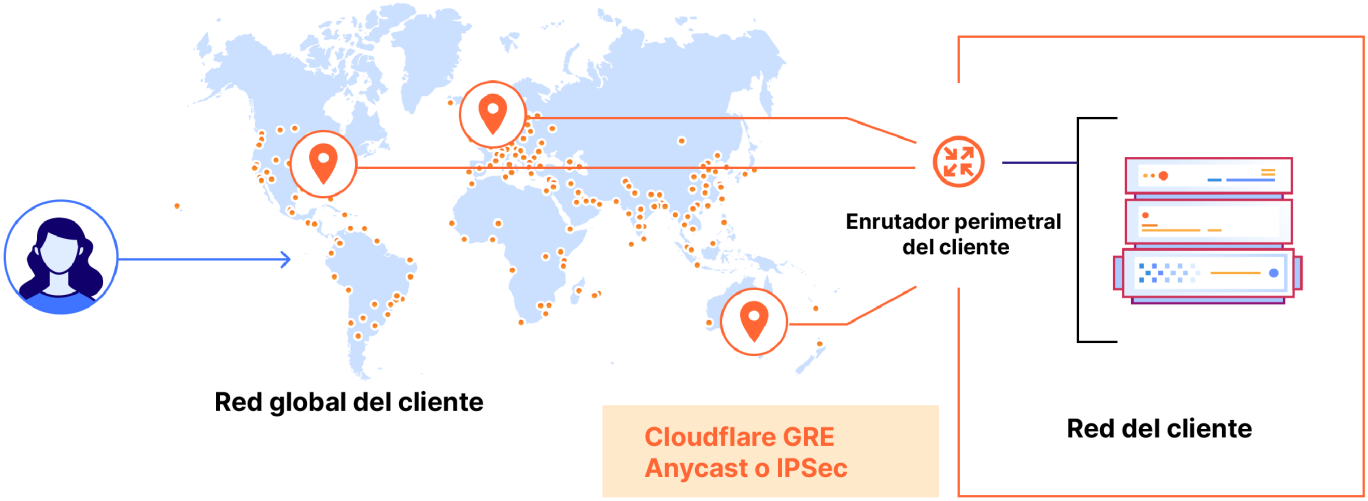
El cumplimiento con los marcos de seguridad, como NIST, complementa los esfuerzos del enfoque Zero Trust y puede proporcionar aún más rigurosidad para una estrategia de seguridad eficaz e integral.

El rol del enrutamiento Anycast

Un aspecto fundamental de este cambio de paradigma es la aplicación de permisos en el punto más cercano a la ubicación de entrada del tráfico a tu "gran conectividad cloud", y esa función la activa el **enrutamiento Anycast**. El enrutamiento Anycast permite una red superpuesta basada en una única dirección IP. Los usuarios remotos pueden conectarse al punto de entrada de la red superpuesta más cercano a ellos, y el enrutamiento Anycast interno elige la ruta más rápida o prioritaria para minimizar la latencia desde el perímetro de la red hasta el centro de datos o los recursos de la nube. El resultado son políticas simplificadas basadas en la identidad, escalabilidad, equilibrio de carga integrado y conectividad entre nubes.

Anycast es un método de direccionamiento y enrutamiento de red en el que las solicitudes entrantes se pueden dirigir a una variedad de ubicaciones o nodos diferentes.

Además, con el enrutamiento Anycast, te beneficias de alta disponibilidad y resiliencia integradas para las aplicaciones a través del enrutamiento inteligente, y ofreces una mayor resiliencia frente a un gran volumen de tráfico, la congestión de la red o ataques DDoS. La naturaleza distribuida y mórfica de las redes Anycast dificulta de forma innata la eficacia de los ataques DDoS y otros ataques automatizados.



La red y la seguridad convergen con las plataformas basadas en la nube

La nube inició una nueva era para las aplicaciones, permitiendo una aceleración extrema del desarrollo. Los ciclos de adquisición que duraban semanas e incluso meses se sustituyeron por "toques" en la nube listos para activar los recursos cuando fuera necesario para desarrollar, probar e implementar rápidamente las aplicaciones. Si bien el entorno de los desarrolladores se ha visto revolucionado, los dominios de red y seguridad están sintiendo ahora la presión de modernizarse y lograr una mayor agilidad.

Al consolidar los conjuntos de herramientas y migrar a una única plataforma, puedes crear una experiencia bajo demanda, más similar a la de la nube, con mayor visibilidad y nuevas oportunidades para la correlación y el análisis avanzado, todo lo cual amplía las perspectivas y revela problemas que aún no habías previsto o identificado. Reducirás el ruido general para los equipos del SOC y podrás responder mejor a incidentes reales en lugar de perseguir "fantasmas" en el sistema.

Ahora, cuando surge una nueva amenaza, la respuesta automática no debería ser adquirir otra herramienta especializada. Quieres asegurarte de que las nuevas herramientas son absolutamente necesarias y pueden conectarse a tu nuevo ecosistema de plataforma:

1

Evalúa qué ha cambiado, ya sea una nueva amenaza, una nueva vulnerabilidad o un nuevo vector desde el que te pueden atacar.

2

Tómate el tiempo necesario para comprender esa amenaza y asegúrate de que estás considerando herramientas que la aborden de forma eficaz.

3

Asegúrate de haber categorizado adecuadamente la nueva amenaza que ha aparecido en el sistema. ¿Es una amenaza de día cero? ¿Tienes una semana para aplicar la revisión? ¿Cuál es el verdadero nivel de vulnerabilidad? ¿Están configuradas tus herramientas para adaptarse? ¿Puedes simplemente aplicar una revisión a los sistemas o realmente necesitas una nueva herramienta?

4

Y luego, por último, decide que una nueva herramienta es realmente necesaria. Estratégicamente, selecciona una solución que esté integrada con un conjunto de herramientas existente o que tenga la capacidad de funcionar como API o que cumpla con CSF (con el marco NIST) de manera que se pueda integrar en la pila de supervisión existente y recibir valiosas señales a las que tu equipo pueda responder.

Si no cumples o tienes dificultades con cualquiera de estos pasos, puede indicar que necesitas echar un vistazo a tu entorno y comprender si hay vulnerabilidades en tu arquitectura, y esa es una conversación más importante que tener con los equipos multifuncionales.

Estos pasos te pueden ayudar a evitar la proliferación de nuevas herramientas y la deuda técnica que crea complejidad, dificulta la visibilidad y afecta a la postura de seguridad.

El cambio cultural

No hay ningún interruptor que accionar para lograr la convergencia de la red y la seguridad. Se trata de un proceso de transformación. Y como todos los procesos que llevan cierto tiempo, necesitas la aceptación de las partes interesadas, un camino hacia logros rápidos para mostrar el retorno de la inversión y una hoja de ruta para el éxito. Pero los equipos están atascados en el modo de extinción de incendios y no tienen tiempo para impulsar el cambio. Es posible que tampoco tengan la perspectiva para hacer realidad el cambio de paradigma necesario para abordar las redes y la seguridad de manera diferente.
Un tercero puede mostrarte el camino hacia tu visión, crear la hoja de ruta, identificar logros e hitos rápidos, y definir el proceso continuo basándose en las prácticas recomendadas y la experiencia adquirida ayudando a otras empresas como la tuya. Pueden ayudarte a abordar no solo las decisiones tecnológicas, sino también las personas y los procesos. Esto incluye ajustar o elevar los roles y redirigir los recursos a proyectos más estratégicos que impulsen los resultados empresariales.

Indicadores clave de rendimiento orientados a la empresa

En lugar de medir el éxito únicamente en función de métricas como el tiempo de actividad de la red, considera añadir indicadores clave de rendimiento más orientados a la empresa que se ajusten mejor a los objetivos de agilidad y del mercado.

- Tiempo de adquisición e integración de una empresa
- Tiempo de incorporación de un nuevo empleado
- Tiempo de lanzamiento de una nueva aplicación
- Tiempo de lanzamiento de un nuevo canal digital
- Evitar por completo incidentes cibernéticos que acaben siendo noticia
- Capacidad para limitar el daño de las amenazas: velocidad de detección de amenazas (MTTD), contención (MTTC) y recuperación (MTTR)
- Velocidad y cadencia de las actualizaciones de las revisiones
- Cumplimiento de los marcos del sector (como NIST)

Cloudflare y Kyndryl para servicios gestionados de transformación de la red

Los amplios servicios de asesoramiento informático de Kyndryl, además de la combinación de redes en la nube y seguridad de red a través de las soluciones de Cloudflare, ayudan a las organizaciones a superar las barreras tecnológicas para una transformación digital eficaz. Con nuestra colaboración, podemos guiar a los clientes en sus procesos integrales de modernización de la red, que pueden incluir las soluciones de WAN centradas en la nube y Cloudflare Zero Trust proporcionadas por Kyndryl.

Juntos, Cloudflare y Kyndryl ayudan a las empresas a:

Optimizar la estrategia multinube y directa a Internet y migrar las redes con total confianza.
Las empresas han migrado los datos a la nube y utilizan aplicaciones SaaS, pero utilizan hardware como su red. Cloudflare y Kyndryl se han asociado para ofrecer servicios de red al mercado empresarial. Cloudflare es la plataforma tecnológica y Kyndryl es el proveedor de servicios que guía a los clientes a lo largo de este proceso.

Reducir el gasto en dispositivos y enlaces de red privada y ahorrar a los equipos informáticos tareas manuales.
Proporcionamos a las empresas las mejores funciones de red y de seguridad perimetral necesarias para entornos de trabajo flexibles, y reducimos la deuda técnica y la arquitectura tradicional. Kyndryl asesora y ayuda en la gestión de la infraestructura informática a medida que las organizaciones modernizan sus redes y transfieren las cargas de trabajo a la plataforma de Cloudflare.

Acelerar la madurez digital y la modernización de la red.
Nuestra experiencia en redes flexibles en la nube con WAN gestionada centrada en la nube permite que las redes respondan a las necesidades informáticas en constante evolución y estén preparadas para lo que depare el futuro.

Ampliar la seguridad de la red a las oficinas y los centros de datos sustituyendo la WAN tradicional.
La ciberseguridad empresarial integral aborda los riesgos y los ataques desde cualquier ubicación y vector. Esto incluye tu WAN. La WAN gestionada permite a las organizaciones convertir todos sus recursos en soluciones nativas de nube y retirar el costoso hardware tradicional.

Más información

Para obtener más información sobre la asociación entre Cloudflare y Kyndryl, visita cloudflare.com o kyndryl.com.

kyndryl / CLOUDFLARE

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

REV:BDES-6064.10JUN2024