DOCUMENTO TÉCNICO

Cómo optimizar el rendimiento y la seguridad de un sitio web en China

Estrategias para aprovechar la economía digital masiva, compleja y en rápido crecimiento de China

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

Resumen ejecutivo

China es el país con mayor población conectada a Internet del mundo. Sin embargo, la complejidad de la red y la amenaza continuamente presente de ciberataques pueden dificultar el acceso a este mercado. Para ayudar a las organizaciones a superar estos obstáculos y optimizar mejor la experiencia de sus sitios web para los usuarios en China, Cloudflare ha ampliado fácilmente sus servicios de red de seguridad y rendimiento global a China.

Los desafíos de desarrollar un negocio digital en China

La vasta economía digital en rápido crecimiento de China convierte al país en un mercado atractivo para una variedad de negocios. Más de 1 000 millones de ciudadanos chinos están conectados a Internet , la población conectada a Internet más grande del mundo, y más de 812 millones de ellos realizaron una compra en línea en la primera mitad de 2021. En general, el gasto en línea se redujo ligeramente en ese periodo en comparación con años anteriores debido en gran parte a la mayor inestabilidad económica causada por la pandemia de la COVID-19. No obstante, la economía china siguió experimentando un crecimiento de dos dígitos después de la pandemia, mientras que el mercado del comercio electrónico creció un 12,5 % en 2020.

Al igual que con cualquier mercado regional, las empresas internacionales que operan en China deben adaptar sus servicios y experiencias en línea para satisfacer las expectativas locales. Desafortunadamente, las regulaciones de Internet, la infraestructura subyacente y el panorama de amenazas de China presentan una variedad de desafíos únicos que pueden dificultar que las empresas globales ofrezcan la calidad de experiencia que esperan los consumidores locales. Estos desafíos incluyen:

- Latencia causada por la fragmentación de las redes y deficiencia del intercambio de datos entre redes.
- Contrapartidas en términos de rendimiento del sitio web móvil.
- Ciberataques locales constantes.

Este documento explica esos desafíos en detalle, describe estrategias para superarlos y muestra cómo Cloudflare puede ayudar.

Latencia causada por los cuellos de botella de Internet y deficiencia del intercambio de datos entre redes

Al igual que muchos consumidores, los chinos tienen grandes expectativas en cuanto a experiencias digitales. Según un informe elaborado por HSBC, China lidera y domina el mercado del comercio electrónico en todo el mundo y, el análisis por países de business.com identifica al gigante asiático como el mayor mercado de comercio electrónico del mundo.

Lamentablemente, las organizaciones a menudo tienen dificultades para ofrecer a los usuarios en China sitios que funcionen de manera rápida y fiable.

Una de las razones son los cuellos de botella de la red. Todo el tráfico de Internet que entra y sale de China pasa por uno de los tres puntos de intercambio de Internet (IXP): en Pekín, Shanghái o Cantón. Durante los picos de tráfico, estos IXP se pueden saturar y aumentar de forma significativa los tiempos de carga de los sitios web alojados fuera de China. Una serie de pruebas determinó que la carga del sitio web de TED tardó por primera vez entre 8-38 segundos en Shanghái durante un pico de tráfico, en comparación con un rango de 5-8 segundos en Nueva York durante un periodo comparable.

Para evitar estos cuellos de botella, algunas empresas internacionales optan por alojar sus sitios web en centros de datos cerca de uno de los tres IXP de China, por ejemplo, Hong Kong, para estar cerca del IXP de Cantón, o en servidores dentro de las fronteras de China. Sin embargo, estos enfoques siguen viéndose amenazados por otro desafío importante de la red: un número limitado de proveedores de servicios de Internet (ISP) locales cuyo intercambio de datos entre redes es deficiente.

Es posible que las empresas que están familiarizadas con el panorama de Internet de China ya sepan que hay tres ISP estatales que dominan el mercado: China Telecom, China Mobile y China Unicom. Cada uno de estos ISP domina en una determinada parte del país. También participan en una interconexión comparativamente pequeña o la práctica de conectar redes independientes en los IXP. Un estudio de Mlytics de 2017 concluyó que la red con mayor interconexión en China solo estaba conectada a dos IXP, en comparación con 66 en Norteamérica y 71 en Europa.

Esto significa que incluso el tráfico de Internet a nivel nacional a menudo debe cubrir una distancia de red importante para recorrer un trayecto geográfico relativamente corto, lo que añade latencia para los usuarios finales.

Cómo superar los cuellos de botella y la deficiencia del intercambio de datos entre redes

Ante estos desafíos de rendimiento web, muchas organizaciones globales con negocios en China optan por utilizar una red de entrega de contenido (CDN) para almacenar el contenido del sitio web estático (o no específico del usuario) en caché en los centros de datos cercanos a los usuarios finales, de modo que muchas de sus solicitudes no tengan que viajar hasta un servidor de origen. Las organizaciones deben considerar una CDN que:

- **Tenga una red grande y bien conectada**. Cuantos más centros de datos tenga una CDN, más cerca estará de los usuarios finales. Además, cuanto mejor sea la cobertura de los tres ISP principales de China, menos saltos de red tendrán que dar las solicitudes de los usuarios finales.
- **Tenga la capacidad de resolver consultas DNS dentro de China.** La resolución de DNS, el proceso por el cual los nombres de dominio se convierten en direcciones IP, puede añadir latencia si su tráfico debe viajar dentro y fuera de China, incluso si el contenido de otro sitio se almacena en caché localmente.
- **Minimice el código HTML, CSS y Javascript del sitio web.** Estos tipos de código son los componentes básicos de la mayoría de los sitios web, lo que indica a los navegadores de los usuarios finales cómo debería ser el sitio. La minificación es el proceso de eliminar caracteres innecesarios del código, disminuir su tamaño general y, por lo tanto, reducir el ancho de banda al atravesar una red. Cuanto menos ancho de banda, mayor velocidad de carga del sitio.
- **Use un código sin servidor en el perímetro de la red para crear reglas personalizadas para responder a las solicitudes.** El código sin servidor es un código que no se limita a un servidor en particular que un desarrollador controla. Cuando se ejecuta en el perímetro de la red, existe un código sin servidor en una gran red de centros de datos. Esto significa que el código puede aplicar de forma fácil y rápida reglas especiales al tráfico específico del usuario final. Por ejemplo, una organización podría escribir código sin servidor en una red basada en China que aplique reglas especiales para los usuarios de dispositivos móviles, para conexiones a Internet más lentas y muchos otros casos de uso.

La asociación de red de Cloudflare con JD Cloud, junto con nuestros servicios de rendimiento global, puede ayudar a superar tanto los cuellos de botella del tráfico como el intercambio de datos entre redes deficiente. Consulta la siguiente sección de este documento para descubrir cómo.

Ciberataques locales constantes

Como en cualquier región, los sitios web que operan en China tienen que hacer frente a una variedad de amenazas para la seguridad.

Una de esas amenazas son los ataques de denegación de servicio distribuido (DDoS), que saturan los servidores o la infraestructura de red con tanto tráfico basura que no pueden responder a solicitudes legítimas. Un informe elaborado por Talos Intelligence en 2017 reveló que los servicios nacionales de alquiler de DDoS, que permiten a los usuarios no expertos lanzar ataques fácilmente mediante una botnet existente de dispositivos infectados, se estaban expandiendo a gran velocidad en China.

Desde entonces, los organismos de seguridad chinos han cerrado varias botnets DDoS importantes, incluida una de 2019 que había infectado más de 200 000 dispositivos y lanzado ataques de hasta 200 GB/s. Sin embargo, otras botnets siguen estando activas, como DoubleGuns, cuyos atacantes seguían en libertad en el momento de la publicación de este documento.

Los sitios web en China también deben evitar los intentos de acceder a los datos privados y a los entornos de desarrollo. En 2018, los atacantes explotaron una vulnerabilidad en un marco popular de PHP en un intento por acceder a los servidores de más de 45 000 sitios web chinos. Los ataques al marco comenzaron menos de 24 horas después de que se anunciara su vulnerabilidad. Del mismo modo, en 2020, dos atacantes en China fueron acusados de acceder ilegalmente a cientos de redes privadas de empresas durante diez años, de nuevo aprovechando una variedad de vulnerabilidades de las aplicaciones web.

Además, es posible que las organizaciones que desean proteger los datos privados en China no puedan recurrir a su conjunto habitual de herramientas. La falta de estándares de encriptación modernos como TLS 1.3 y la indicación de nombre del servidor cifrada (ESNI) en las redes chinas aumenta las oportunidades para que los observadores no autorizados intercepten el tráfico.

Cómo defenderse de los ciberataques locales en China

El aumento de los ataques DDoS en todo el mundo ha hecho que los servicios de mitigación de DDoS y otras herramientas de seguridad de aplicaciones, como los firewalls de aplicaciones web (WAF), sean un requisito de seguridad fundamental para cualquier sitio web activo. China no es diferente. A la hora de buscar soluciones de protección de este tipo en este mercado, las organizaciones deben considerar:

- **Soluciones de mitigación de DDoS desde el perímetro de la red, en lugar de "centros de filtrado" limitados.** Aunque casi todos los servicios de mitigación de DDoS modernos operan en la nube, muchos dependen de un número limitado de centros de datos para filtrar el tráfico malintencionado. Retornar el tráfico a estos "centros de filtrado" para su inspección puede exigir saltos de red adicionales y, por lo tanto, causar latencia e interrupción a los usuarios, especialmente en China, con sus limitaciones de red. Para mitigar ataques DDoS sin afectar el rendimiento de Internet en China, las organizaciones deben considerar los servicios en la nube que ofrecen mitigación de DDoS en cada centro de datos del perímetro sin añadir saltos de red adicionales.
- **Limitación de velocidad para bloquear abusos.** Es esencial disponer de controles granulares que puedan mitigar los ataques DDoS de alta precisión a la capa 7, detener los abusos de las API para garantizar la disponibilidad, proteger la información sensible de los clientes contra los ataques de inicio de sesión brutos y proteger los servidores de origen para que no agoten recursos, todo ello evitando los costes imprevisibles a causa de picos de tráfico.

- **WAF que se actualiza de forma automática y rápida.** Los atacantes locales en China han demostrado su capacidad para aprovechar muy rápido las nuevas vulnerabilidades de las aplicaciones web. Es posible que las organizaciones deseen ser capaces de crear sus propias reglas WAF, pero no deben depender únicamente de su propia información de amenazas y capacidad para realizar actualizaciones. Deben considerar los firewalls de aplicaciones web que se actualizan automáticamente en función de un amplio grupo de amenazas observadas. Además, cuando la organización desea realizar sus propias actualizaciones de reglas, debe estar segura de que esos cambios se propaguen lo más rápido posible.
- **Opciones de cifrado personalizables.** Para proteger los datos en tránsito en ausencia de TLS 1.3 y ESNI, las organizaciones deben considerar servicios de seguridad que ofrezcan una gama más amplia de métodos de cifrado personalizables.

Los servicios de seguridad de Cloudflare, que están disponibles como parte de nuestra Red China, ofrecen mitigación de DDoS sin latencia y un WAF de actualización rápida que se basa en información global para detectar amenazas. Consulta la siguiente sección de este documento para obtener más información.

Cómo ayuda Cloudflare a los sitios web globales que operan en China

Cloudflare opera una red de centros de datos que abarca 200 ciudades globales en 100 países. El número de centros de datos en China era de 45 repartidos en 38 ciudades en marzo de 2022. Cada uno de estos centros de datos pueden ofrecer un amplio conjunto de servicios de seguridad, rendimiento y fiabilidad, como entrega de contenido, resolución de DNS, mitigación de DDoS, aplicación de WAF, ejecución de código sin servidor y mucho más. Dado que cada uno de estos servicios opera en cada centro de datos, pueden funcionar muy cerca de los usuarios finales, lo que ayuda a reducir la latencia y permite a nuestra red conseguir una visión detallada y actualizada de las amenazas y las condiciones de red más recientes. Además, las organizaciones pueden gestionar todos estos servicios desde un solo panel de control.

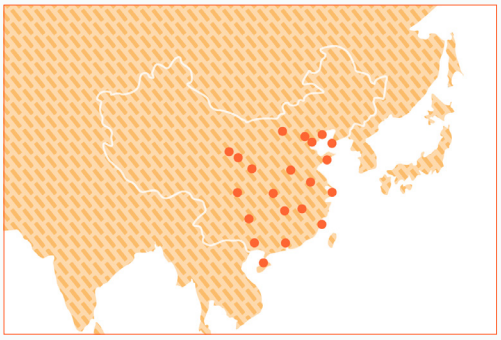
Cloudflare ha ayudado a distintas organizaciones a ofrecer experiencias de Internet seguras, rápidas y fiables para los visitantes que se encuentran en China desde 2015. Para mejorar aún más esos servicios, nos hemos asociado recientemente con JD Cloud, el brazo de tecnología inteligente en la nube de la potencia china de comercio electrónico JD.com.

Así es como esta red ayudará a las organizaciones a superar los desafíos descritos en la sección anterior.

Cómo ayuda Cloudflare a superar la latencia

Cloudflare y la red de JD Cloud en China ofrecen:

- **Argo Smart Routing:** la transmisión de datos del cliente al origen y viceversa puede añadir latencia. Con el almacenamiento en caché, el contenido estático puede evitar la congestión de la red, pero el contenido dinámico depende de la disponibilidad, la fiabilidad y el rendimiento de Internet. Esta dependencia puede ralentizar los tiempos de carga, los tiempos de espera, provocar desconexiones y degradar la experiencia del usuario final. **Argo Smart Routing** tiene una capacidad única de **detectar la congestión en tiempo real** y **dirigir el tráfico web** por las **rutas de red más rápidas y fiables**. Las solicitudes a la red de Cloudflare por parte de los clientes de Cloudflare y sus usuarios nos ayudan a entender cómo funcionan las diferentes partes de Internet en un momento dado. Argo Smart Routing utiliza los datos de tiempo que Cloudflare recopila para **dirigir el tráfico de forma dinámica por las rutas más rápidas de vuelta al origen**, aumentando el rendimiento. De media, Argo mejora un 30 % el rendimiento de los activos web. Y esto se traducirá posteriormente en un aumento de las ventas y la retención de clientes.
- **Almacenamiento en caché y servicio de contenido estático desde muchos centros de datos dentro de China**, lo que reduce la latencia y los tiempos de carga de páginas, independientemente de dónde se encuentren los usuarios finales. Nuestra red está estrechamente interconectada con todos los ISP chinos, lo que reduce el número de saltos de red que debe dar el tráfico.



Centros de datos en China continental

- **Resolución DNS opcional dentro de China**, que se traduce también en tiempos de respuesta más rápidos.
- La capacidad de **usar el protocolo de Internet versión 6** (IPv6), que permite un enrutamiento y procesamiento eficiente de los paquetes.
- La capacidad de **minimizar el código del sitio web** a través de nuestra función Minificador automático, que se puede activar fácilmente al marcar una casilla en el panel de control de Cloudflare.
- **Informática sin servidor** a través del servicio Cloudflare Workers, que opera en todos los centros de datos de nuestra red en China. Te permite responder a determinadas solicitudes de forma personalizada, aumentar las aplicaciones existentes, e incluso crear otras completamente nuevas sin necesidad de configurar o mantener infraestructura.

Cómo ayuda Cloudflare a abordar los constantes ciberataques locales

Los servicios de seguridad integrados en nuestra red de China permiten a las organizaciones:

- **Mitigar los ataques DDoS.** Cada uno de nuestros centros de datos en China puede mitigar los ataques, lo que le da a la red una inmensa capacidad para responder a los ataques más grandes sin perder solicitudes legítimas y sin depender de los centros de datos de Cloudflare en otras partes del mundo. Dado que la inspección de tráfico se realiza cerca de los usuarios finales, sus solicitudes se ahorran el largo proceso de retorno a un "centro de filtrado" potencialmente distante. Además, debido a los desafíos de la red en China, Cloudflare proporciona capacidades únicas de ingeniería de tráfico automatizado que permiten el reenrutamiento automático del ataque de tráfico. Todas estas funciones evitan que el rendimiento del tráfico legítimo dentro y fuera de China se vea afectado.
- **Proteger las vulnerabilidades de las aplicaciones web** con el WAF de Cloudflare. Además de detener los vectores de ataque conocidos gracias a los conjuntos de reglas administrados (como una implementación de reglas propias de OWASP y Cloudflare), el WAF utiliza un flujo continuo de información sobre amenazas de toda nuestra red para detener automáticamente las amenazas más recientes. Además, las organizaciones pueden crear fácilmente sus propias reglas y propagarlas por toda la red en cuestión de minutos. Las mejoras introducidas en 2021 permiten que WAF se implemente con mayor rapidez y escale sin esfuerzo para abarcar aún más tráfico. WAF también cuenta con conjuntos de reglas actualizados que proporcionan un mejor control separando el estado de la regla de la acción. Los usuarios pueden ahora disfrutar de una mejor navegación por las reglas mediante el filtrado avanzado, la edición masiva, las etiquetas de las reglas, etc.
- **Limitación de velocidad** se integra con nuestras reglas personalizadas del WAF y protege contra los ataques DDoS, los intentos de inicio de sesión por fuerza bruta, la sobrecarga del servidor de origen y otros tipos de abuso dirigidos a las API y las aplicaciones. Los usuarios pueden configurar umbrales, definir el tráfico, personalizar las respuestas y obtener información valiosa sobre URL específicas de sitios web, aplicaciones o puntos finales de la API.
- **Cifrar datos con TLS 1.2** y gestionar fácilmente sus propias certificaciones desde el panel de control de Cloudflare.

MÁS INFORMACIÓN

El servicio Red China de Cloudflare está disponible para los clientes suscritos al plan Enterprise de Cloudflare. Además, cumple plenamente con las leyes y normativas chinas, en las que una licencia válida de proveedor de contenidos de Internet (ICP) es un requisito obligatorio para incorporarse a la Red China.

Conforme la economía de Internet de China continúa creciendo, inevitablemente surgirán nuevos desafíos de seguridad y rendimiento. Los planes de Cloudflare para promover el crecimiento en China brinda a las empresas en nuestra red las herramientas para poder responder con rapidez a esos desafíos y seguir elevando los estándares para que las experiencias de usuario sean perfectas.

¡Llama a Cloudflare para empezar a optimizar tu presencia web en China hoy mismo!

Para obtener más información sobre la Red China de Cloudflare, visita cloudflare.com/network/china/ o contacta a tu representante de Cloudflare.