CLOUDFLARE®

No se quede atrás

Mejore el rendimiento y la seguridad de su sitio de comercio electrónico para los consumidores de telefonía móvil

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Resumen ejecutivo

El móvil está en el punto de inflexión para convertirse en el canal más importante de las estrategias de comercio electrónico. El 25 % de los minoristas de Estados Unidos ya han averiguado cómo subir las tasas de conversión de móviles para lograr una cuota del mercado potencial sobreproporcional, en una carrera en la que los ganadores se lo llevan todo. Consiguen retener mejor a los usuarios y atraer vistas de producto ofreciendo sitios y aplicaciones de móviles rápidos y con alto grado de disponibilidad. Cloudflare puede ayudar a lograr los requisitos fundamentales ofreciendo:

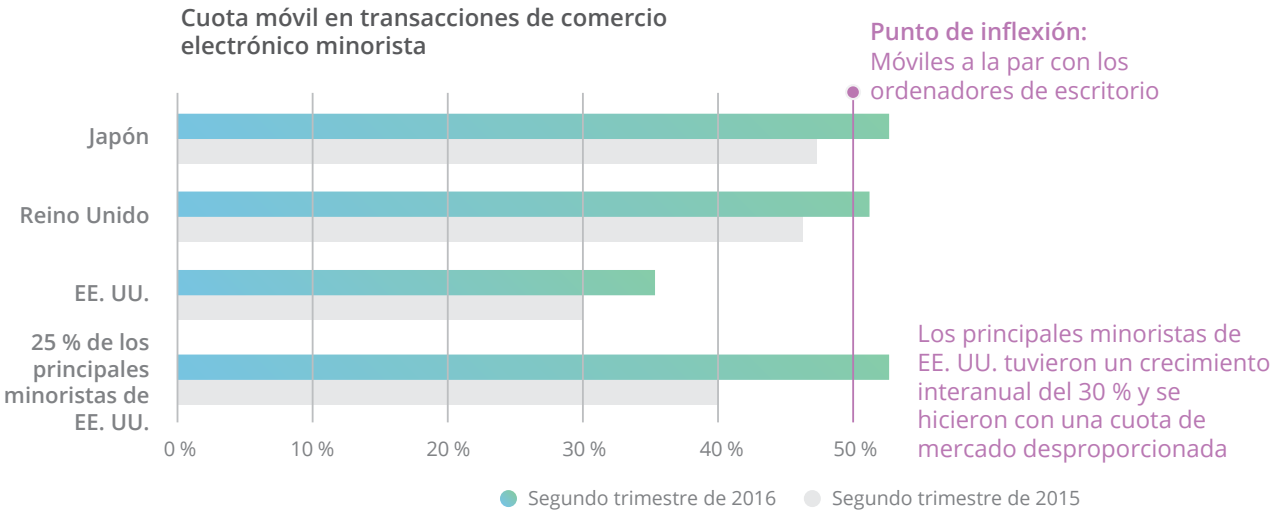
- Una de las redes de entrega de contenido más rápidas, basada en enrutamiento Anycast y la capacidad de almacenar contenido en caché físicamente cerca de los consumidores para reducir la latencia.
- Precios fijos predecibles.
- Optimización de código e imágenes de móvil, además de compatibilidad IPv6 para reducir la latencia en dispositivos móviles.
- Protección frente a ataques DDoS en capas 3, 4 y 7, y vulnerabilidades de aplicación en capa 7 para aumentar el tiempo de actividad.
- Cifrado correcto de alto rendimiento.

La configuración de Cloudflare para acceder a esas capacidades es un importante paso para que los proveedores de comercio electrónico mantengan sus sitios rápidos y seguros de forma proactiva en todo momento.

El comercio a través de móvil es un punto de inflexión

El comercio electrónico es emocionante: con un crecimiento anual del 14,6 % en 2015, y con un registro del enorme crecimiento en ventas minoristas del 36,2 % en Estados Unidos en el mismo año, superó con mucho al crecimiento del modelo de negocio "ladrillos y clics", que combina su presencia en línea y presencial. Todavía más impresionante es el crecimiento incluso más rápido del comercio a través de móvil. Este sector se encuentra ahora en un punto de inflexión: por primera vez, en el segundo trimestre de 2016 en Japón y Reino Unido, el porcentaje de transacciones de venta de comercio electrónico a través de móvil superaba el 50 %, adelantando, por lo tanto, a las transacciones de dispositivos de escritorio. En Estados Unidos el porcentaje de transacciones de comercio electrónico a través de móvil está creciendo a pasos agigantados con un 17 % anual, y aunque va a la zaga con un 35 % de transacciones, todo indica que alcanzará en breve a los países más avanzados.

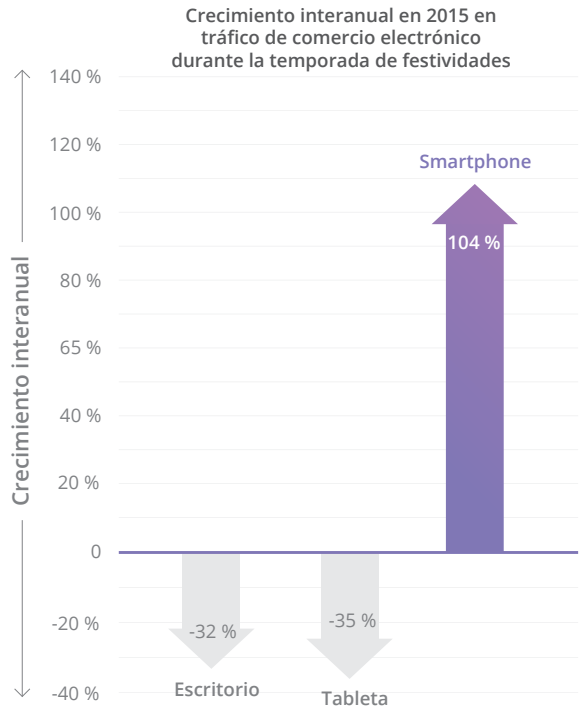
El cuartil principal de los minoristas de Estados Unidos ya está capitalizando esta tendencia proporcionando los mejores sitios y aplicaciones para móviles. Logran retener mejor a los usuarios y atraer vistas de producto, elevando sus tasas de conversión hasta un 90 % en comparación con el minorista emergente promedio. Como resultado están consiguiendo una sobreproporcional cuota del botín con un 52 % de sus ventas de comercio electrónico a través de móvil, lo que representa un impresionante crecimiento interanual del 30 %.

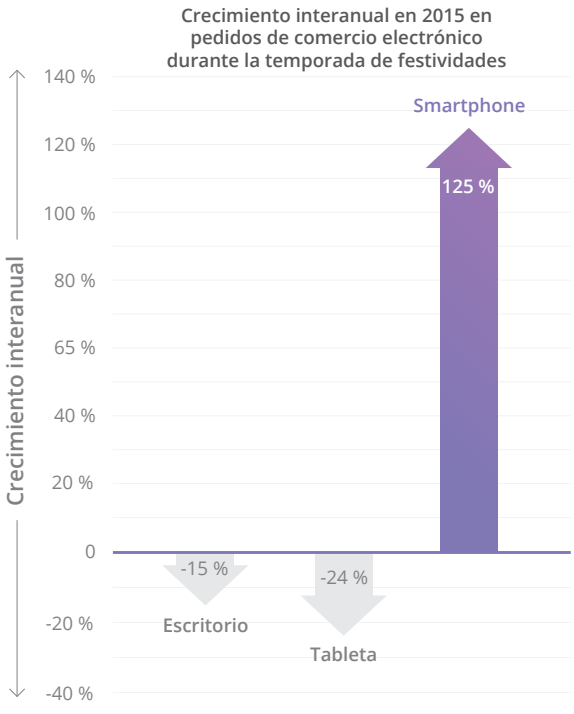


Sin duda alguna, el comercio a través de móvil se ha convertido en canal de venta y marketing clave. Los minoristas que ofrecen la mejor experiencia de móvil son los ganadores y conquistarán una cuota aún más dominante del mercado disponible.

Los móviles son de vital importancia para la temporada de compras navideñas

Las compras en línea en el periodo de Navidad (Cyber 5) batieron récords en 2015, con el Cyber Monday reclamando el título del día de mayor gasto en línea de la historia de Estados Unidos. Los teléfonos inteligentes jugaron un papel muy importante, protagonizando el 49 % del tráfico y el 27 % de los pedidos. Los pedidos y el tráfico de los teléfonos inteligentes crecieron en porcentajes increíbles, a diferencia de los pedidos y el tráfico de los dispositivos de escritorio y tabletas que, en consecuencia, redujeron su porcentaje.

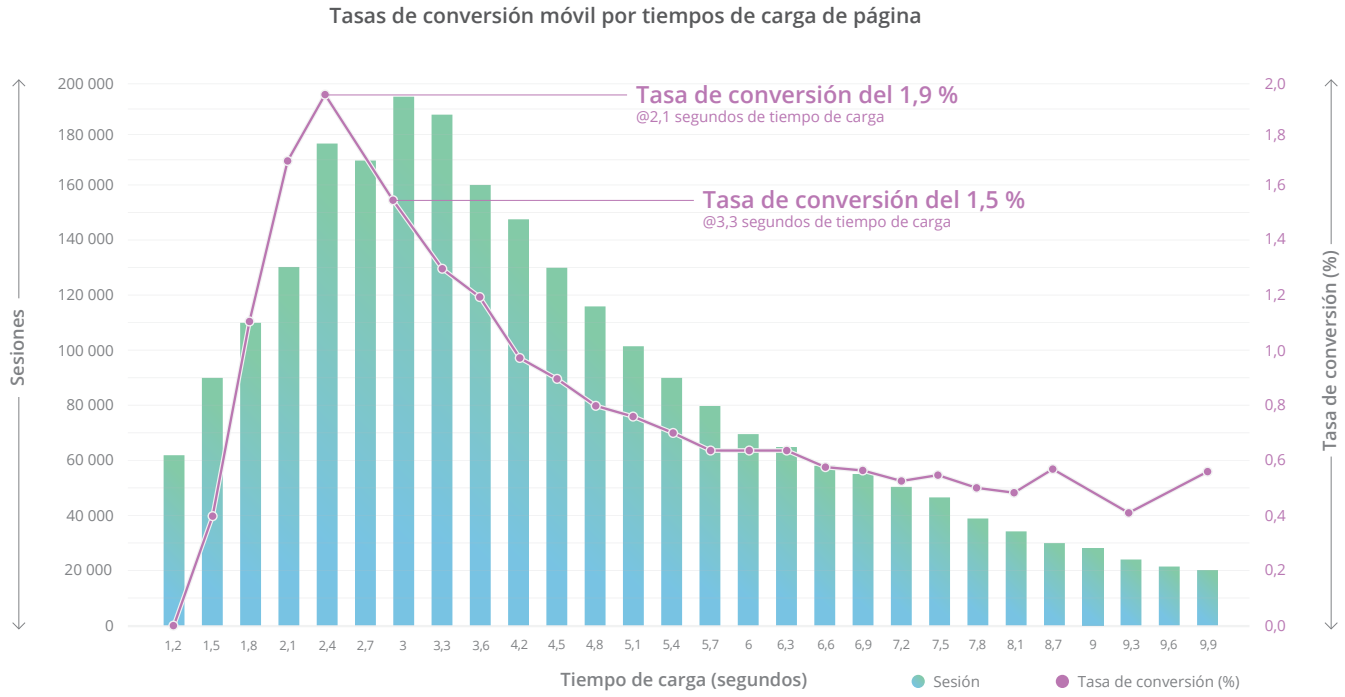




El periodo de compras Cyber 5 2015 demostró una vez más que los minoristas con la mejor experiencia de móvil se llevaron la mejor parte. Por ejemplo, Amazon creció un 24,1 % más en el periodo Cyber 5 2015 en comparación con el 2014. Todo apunta a que las próximas temporadas de Navidad, los minoristas de "ladrillos y clics" experimentarán más tráfico en línea que en tienda, convirtiéndose las transacciones de compra a través de móvil en un factor fundamental del crecimiento.

El impacto de la latencia y la disponibilidad en las tasas de conversión

Pero, ¿qué separa a los líderes de la manada? Los principales minoristas de comercio electrónico ofrecen los mejores sitios y aplicaciones móviles para aumentar sus tasas de conversión. Las tasas de conversión de móviles siguen siendo bajas y están directamente relacionadas con el rendimiento y la disponibilidad del sitio o la aplicación de móvil. Por ejemplo, la tasa de conversión de un minorista en línea líder alcanzó el 1,9 %, con un tiempo promedio de carga de página de 2,4 segundos. Solo un segundo de tiempo promedio de carga más lento de 3,3 segundos produjo una caída de la tasa de conversión en un 27 %.

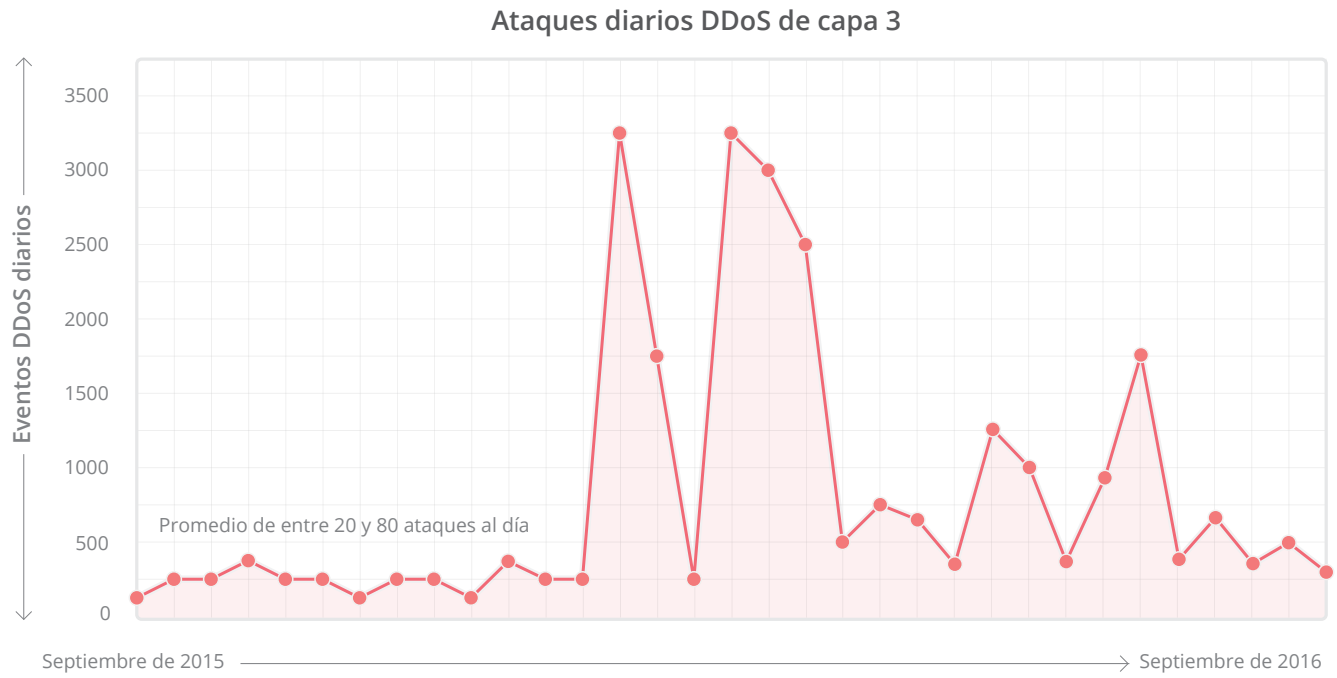


Existen muchos ejemplos del sector que ilustran la relación entre el rendimiento del sitio y la tasa de conversión.

- Amazon aumentó sus ingresos en un 1 % por cada 100 ms de reducción en latencia del sitio.
- Yahoo aumentó su tráfico en un 9 % por cada 400 ms de reducción en latencia del sitio.
- Walmart experimentó una fuerte disminución en la tasa de conversión cuando el tiempo promedio de carga aumentó de 1 a 4 segundos.

En general, Google informó que una latencia de sitio de 100 a 400 milisegundos tiene un impacto cuantificable en el comportamiento del consumidor, y un sitio que es 250 milisegundos más lento que el sitio de un competidor, tendrá una menor frecuencia de visitas.

Además de la latencia ocasionada por el propio sitio o aplicaciones, los ataques de denegación de servicio distribuido (DDoS) pueden inhabilitar totalmente el sitio. Cloudflare, que cuenta con casi el 10 % del tráfico de Internet de todo el mundo fluyendo a través de sus redes, puede filtrar y medir con precisión dichos ataques. En el último año, Cloudflare observó un crecimiento en la cantidad e intensidad de los ataques cada vez mayor, con hasta 1400 eventos de DDoS al día, un añadido de 400 Gbps de tráfico de entrada y ataques con 200 M de paquetes por segundo.



Normalmente, estos ataques no son eventos ocasionales y las víctimas son atacadas varias veces al año. Según la experiencia de Cloudflare, cualquier gran o pequeña empresa es susceptible de sufrir estos ataques. A pesar de que muchas jurisdicciones cuentan con normativas que establecen los ataques DDoS como ilegales, existen proveedores que ofrecen suscripciones para servicios de DDoS con un cargo mínimo de 5 o 10 USD al mes.

Incluso el sitio web de Amazon (con 99 mil millones de dólares en ingresos de ventas al por menor en 2015) sufrió varias caídas en el pasado por razones desconocidas. Por ejemplo, en el año 2013, Amazon.com se cayó durante unos 15-45 minutos, lo que le supuso un coste de entre 1,8 y 5,3 millones de dólares en pérdidas de venta, en base al promedio de ventas de la empresa de 117.882 millones USD por minuto. El coste de inactividad para los proveedores de comercio electrónico puede ser mucho mayor durante la época de Navidad. Por ejemplo, Amazon declaró obtener el 33 % de los ingresos anuales durante el cuarto trimestre de 2015 por la estacionalidad del negocio. Otros efectos de la inactividad del sistema incluyen el impacto negativo en la satisfacción del cliente, el posicionamiento en buscadores y las relaciones con los inversores.

En resumen, para los proveedores de comercio electrónico es fundamental mejorar las tasas de conversión, especialmente durante la temporada de Navidad y proporcionar sitios/aplicaciones ágiles que estén protegidos contra los ataques DDoS para mejorar el tiempo de actividad.

Tecnologías esenciales para sitios de móvil rápidos y seguros

Cloudflare puede ayudarle a acelerar y proteger sus sitios y aplicaciones de comercio electrónico sin añadir hardware, instalar software ni cambiar una sola línea de su código.

El primer paso es utilizar la red de entrega de contenido (CDN) de Cloudflare, una de las redes más grandes del mundo que gestiona más de 10 mil millones de solicitudes al mes. Esto supone casi el 10 % de todas las solicitudes de Internet de más de 2,5 mil millones de personas en todo el mundo. La CDN de Cloudflare está considerada como una de las más rápidas con un promedio de tiempos de respuesta de 34 ms (en EE. UU.) según los datos de Cedexis. Entre sus funciones clave se incluyen:

Enrutamiento basado en Anycast

Mientras la CDN de Cloudflare funciona con un esquema de enrutamiento denominado Anycast, la mayor parte de la internet de hoy en día sigue funcionando con un mecanismo denominado Unicast. Con Unicast, cada nodo de la red obtiene una dirección IP, que es única. Los routers mantienen un mapa de las direcciones IP del mundo para averiguar la ruta más corta a través de los distintos saltos de enlace hasta llegar al destino final. Sin embargo, el destino final podría estar en algún lugar del continente o en algún otro lugar del mundo, lo que requiere saltos de enlace adicionales, que aumentan la latencia. Con Anycast, el esquema de enrutamiento utilizado por Cloudflare, múltiples máquinas de la red CDN comparten la misma dirección IP, lo que permite a los routers enviar solicitudes directamente al servidor más cercano físicamente y reducir la latencia.

Almacenamiento de contenido en caché

La red Anycast de Cloudflare opera junto con el almacenamiento de contenido en caché. Una vez Anycast dirige una solicitud al servidor más cercano físicamente, se pone a disposición una copia del contenido almacenado en caché para el acceso en este servidor. La ventaja del almacenamiento en caché es que los objetos se pueden trasladar más cerca del solicitante, acelerando así su entrega y reduciendo la carga en el servidor web de origen. Cloudflare ofrece capacidad para el almacenamiento automático en caché de contenido estático y, con Railgun, añade un mecanismo para almacenar en caché contenido dinámico.

Cloudflare analiza el tráfico que pasa a través de los servidores de la CDN para encontrar las partes estáticas del sitio de origen. A continuación, el contenido estático se almacena en caché en la CDN durante un corto período de tiempo. Normalmente, el 66 % de contenido web es almacenable en caché (a través de "almacenamiento automático en caché de contenido estático") y el restante 34 % no almacenable en caché, por lo que debe obtenerse desde el servidor web de origen. Railgun está diseñado para acelerar la entrega de contenido que no se puede almacenar en caché, de manera que la totalidad de la web se convierte en almacenable. Funciona mediante el reconocimiento de que las páginas web no almacenables en caché no cambian de forma rápida, y la pequeña diferencia en los cambios entre las versiones de las páginas web pueden ser identificadas por servidores de la CDN de Cloudflare. A continuación, Cloudflare comprime los cambios con tasas de compresión de hasta el 99,6 % y los envía a través del enlace, logrando mejoras de rendimiento de hasta el 700 %. Railgun requiere la instalación de un componente de software por parte del servidor de origen.

> "A medida que el coste de ancho de banda sigue aumentando, disponer de una CDN como la de Cloudflare sirviendo imágenes en el borde a los usuarios es muy rentable y reduce la latencia para nuestros clientes de telefonía móvil".
>
> Chris Smith, director de comercio electrónico de Big 5 Sporting Goods

Precios fijos predecibles

Para ser parte de Internet, Cloudflare compra ancho de banda, conocido como tránsito, de una serie de proveedores. Cloudflare compra tránsito al por mayor en base a la capacidad utilizada en un mes determinado, pagando la utilización máxima durante un periodo de tiempo. Aunque la tarifa que paga Cloudflare varía considerablemente de una región a otra en todo el mundo, para mantener una tabla de precios sencilla, Cloudflare cobra a los clientes una tarifa fija, independientemente de donde se entregue el tráfico en todo el mundo. A diferencia de algunos servicios en la nube, que facturan por bits individuales entregados a través de una red, Cloudflare ofrece tarifas mensuales predecibles. Cloudflare continúa trabajando para reducir el precio de tránsito y el aumento de interconexión, a fin de ofrecer el mejor servicio posible al precio más bajo posible.

Optimización de código e imágenes

Con Polish, Mirage y Auto-Minify, Cloudflare proporciona una herramienta imbatible para reducir la latencia. Estas capacidades son especialmente importantes para los dispositivos móviles, que tienen anchos de banda limitados.

Polish elimina los metadatos y comprime las imágenes para reducir su tamaño. Polish se puede ejecutar en modo sin pérdidas, que elimina los excesos innecesarios del encabezado de la imagen y los metadatos sin eliminar ningún dato de la imagen. El tamaño promedio de archivo se reduce en un 21 %. Polish también se puede ejecutar en modo con pérdida, que en adición al modo sin pérdida, aplica un algoritmo de compresión a imágenes adecuadas. Las imágenes se mostrarán exactamente igual que antes, sin ninguna diferencia visual perceptible, pero los tamaños promedio de archivo se reducen en un 48 %. Las imágenes constituyen más del 50 % de los datos que componen un sitio web típico.

Mirage gestiona cómo las imágenes se cargan en los dispositivos móviles. Produce rápidamente la aparición de una página utilizable con la que los usuarios pueden interactuar, al tiempo que completa el resto de la página sin interrumpir la experiencia del usuario.

- Mirage utiliza la carga lenta diferida para dar prioridad a la carga de las imágenes que se encuentran en el área de visualización, es decir, las imágenes que en realidad muestra el navegador. A continuación, carga el resto de imágenes de la página, que no muestra el navegador, a medida que se necesitan o a medida que se vuelven disponibles recursos de red adicionales.

- Los dispositivos móviles requieren imágenes más pequeñas debido al tamaño de pantalla más pequeño. Mirage cambia el tamaño de una imagen en el servidor hasta tan solo el 1 % de la resolución completa de la imagen y envía la de tamaño reducido en primer lugar. Una vez que la página está presentada con las imágenes de tamaño reducido, estas se reemplazan por las versiones de máxima resolución. Las imágenes aparecen primero con baja calidad y luego adquieren un enfoque nítido.

- En lugar de iniciar una nueva solicitud para cada imagen, Mirage filtra todas las imágenes de la red de Cloudflare con una única solicitud. Esto significa que incluso una página con cientos de imágenes puede iniciar la presentación en el navegador con tan solo dos solicitudes. Incluso los usuarios con conexiones de móvil lentas pueden empezar a interactuar con la página de inmediato, en lugar de tener que esperar a que se carguen todas las imágenes con la resolución completa.

Auto Minify elimina sobre la marcha todos los caracteres innecesarios, es decir, el “espacio blanco”, de los archivos HTML, JavaScript y CSS, ahorrando un 20 % del tamaño de un archivo sin cambiar ninguna de las funcionalidades. La implementación de Cloudflare de Auto Minify es fácilmente 100 veces más rápida que el siguiente enfoque más próximo.

Compatibilidad con IPv6

Las mediciones de monitorización de usuarios reales de Facebook y Linkedin mostraron que los tiempos de carga de páginas de móviles a través de IPv6 son más de un 10 % más rápidos que a través de IPv4 en las 4 redes de telefonía móvil principales de Estados Unidos. Aunque la implementación de IPv6 es una actividad que conlleva varias décadas y sufre la percepción de parecer lenta, alrededor del 60 % de las solicitudes de Android y más del 20 % de las solicitudes de iPhone de las 4 redes de telefonía móvil principales Estados Unidos utiliza IPv6 en los sitios de doble apilado (a fecha de 05/04/2016). Cloudflare no solo ofrece soporte completo con IPv6, además de una puerta de enlace IPv6 a IPv4 desde 2012, sino que también facilita a los clientes la habilitación de este servicio con “un solo clic”. Si el servidor de origen es compatible con IPv6, los visitantes que llegan de una conexión IPv6 son transportados a través del protocolo de extremo-a-extremo. Si el servidor de origen solo es compatible con IPv4, Cloudflare aceptará un visitante a través de IPv6 y después, sin problemas, realizará una solicitud al servidor a través de IPv4. Además, si una aplicación que se ejecuta en el servidor de origen tiene un requisito difícil de ejecutar en IPv4, Cloudflare ofrece Pseudo IPv4. Esta opción, cada vez que se establece una conexión a través de IPv6, añade un encabezado HTTP a las solicitudes con una “pseudo” dirección IPv4.

Protección frente a DDoS en capas 3 y 4; resistencia de red Anycast con plataforma de aprendizaje automático

Además de utilizar la red de entrega de contenido (CDN) de Cloudflare, el siguiente paso es proteger el sitio o las aplicaciones contra ataques maliciosos para garantizar el tiempo de actividad. La protección avanzada de Cloudflare frente a DDoS, ofrecida como un servicio en el borde de la red, está a la altura de la sofisticación y el nivel de las amenazas y se utiliza para mitigar ataques DDoS de todas las formas y tamaños. Cloudflare impidió muchos de los mayores ataques DDoS, incluidos aquellos con más de 400 Gbps.

Los ataques DDoS en capas 3 y 4 son generalmente ataques volumétricos, tales como los ataques de amplificación DDoS, inundación DDoS e inundación DDOS SYN. Aunque estos ataques pueden devastar una red basada en unicast típica, la red basada en Anycast de Cloudflare aumenta inherentemente la superficie mediante la difusión del tráfico de ataque a cada uno de los más de 100 centros de datos de Cloudflare y a un conjunto diverso de interconexiones de gran ancho de banda con otras redes, para simplemente absorber el tráfico de ataque. Además, Cloudflare proporciona una plataforma de aprendizaje automático, en la que el tráfico de red se analiza en tiempo real para identificar las solicitudes anómalas o maliciosas. Una vez que se identifica un nuevo ataque, Cloudflare se inicia automáticamente para bloquear ese tipo de ataque, tanto en sitios web particulares como en toda la comunidad.

Incluso desde una punto de vista de costes, los ataques por lo general no afectan a Cloudflare: Cloudflare compra una cantidad significativa de ancho de banda al por mayor y paga el máximo de entrada y de salida del tráfico según el promedio de un mes. Puesto que Cloudflare actúa como un proxy de almacenamiento en caché, en circunstancias normales la salida siempre supera a la entrada en aproximadamente 4 a 5 veces. Cuando se produce un ataque, las dos líneas se acercan entre sí, pero rara vez un ataque es lo suficientemente grande como para aumentar los costes generales de ancho de banda de Cloudflare. Cloudflare transfiere este beneficio a sus clientes, que no soportan cargos adicionales por un aumento del tráfico de red a causa de un ataque DDoS.

A medida que Cloudflare continúe aumentando su red y su comunidad, se hará cada vez más difícil lanzar un ataque DDoS eficaz contra cualquiera de los usuarios de Cloudflare.

Protección frente a DDoS en capa 7; Rate Limiter con base de datos de reputación de IP

Al igual que los ataques volumétricos en capa 3 y 4, los ataques de denegación de servicio en capa 7 utilizan un gran volumen de solicitudes para evitar que los usuarios reales accedan a un sitio web. En los ataques de denegación de servicio en capa 7, una sola dirección IP realiza muchas solicitudes similares a los patrones de tráfico no malicioso y, por lo tanto, resultan difíciles de contrarrestar.

El protector de tráfico de Cloudflare, actualmente disponible mediante un programa de acceso temprano, controla el número de solicitudes que llegan a un sitio desde cada dirección IP e identifica sitios que están realizando demasiadas solicitudes por minuto. Una vez que se identifica una dirección IP sospechosa, el tráfico desde esta dirección IP se presenta como una página intersticial durante unos 5 segundos para realizar una serie de pruebas matemáticas. Si la solicitud no supera esta prueba, el protector de tráfico rebaja la reputación de ese IP y al tráfico proveniente de esta dirección se le mostrará una página de CAPTCHA en cada intento de acceso.

Cuando Cloudflare identifica una dirección IP que parece estar haciendo solicitudes maliciosas, se almacena en la base de datos de reputación de IP de Cloudflare. En base a una puntuación de amenaza, las solicitudes pueden pasar o se les puede presentar un CAPTCHA. Si falla el CAPTCHA y la dirección IP se identifica como maliciosa, la solicitud se bloquea en el borde de Cloudflare para toda la red, beneficiando a toda la comunidad de Cloudflare.

Ataques de vulnerabilidad de aplicaciones que no son DDoS en capa 7; firewall de aplicaciones web

Los ataques de aplicaciones en capa 7 son los más complicados y sofisticados. Imitando el uso normal de una aplicación, son capaces de superar la mayoría de servicios de protección de vulnerabilidad y equipos de mitigación de DDoS. Entre los tipos de ataque más comunes se incluyen la inyección de código SQL y la ejecución de comandos en sitios cruzados (XSS), que podría permitir a los atacantes el acceso directo a datos de clientes o cualquier otro tipo de aplicación.

Cloudflare contraataca las amenazas mediante su firewall de aplicaciones web (WAF). El WAF implementa el conjunto de reglas Core OWASP, que Cloudflare proporciona listo para su uso, además de reglas personalizadas creadas por la comunidad y los clientes. Una nueva regla generada por Cloudflare se propaga a todos los nodos de servidor de Cloudflare en 30 segundos y el WAF, por sí mismo, añade menos de 1 ms de latencia por solicitud, ofreciendo seguridad sin pérdida de rendimiento. De esta manera Cloudflare es capaz de proteger a sus clientes contra las principales vulnerabilidades de día cero, incluidas la vulnerabilidad Shellshock y el error Heartbleed.

"Nos tomamos el impacto de un ataque DDoS muy en serio. Incluso en los casos en que nuestro dominio sufrió un ataque DDoS, Cloudflare pudo protegerlo de forma rápida, ofreciendo una experiencia sin contratiempos para nuestros clientes. La ventaja más importante que nos proporciona Cloudflare es la tranquilidad de que alguien está controlando la red y que estás respaldado por un método para la mitigación de los ataques".

Chris Smith, director de comercio electrónico de Big 5 Sporting Goods

TLS 1.3 y HTTP/2 con Server Push

El cifrado es esencial para proporcionar una experiencia de compra fiable, pero las últimas mejoras de SSL pueden utilizarse para mejorar aún más el rendimiento. La seguridad de la capa de transporte (TLS) 1.3 no solo elimina las características de inseguridad de las anteriores versiones de TLS, también disminuye la latencia reduciendo el protocolo de ida y vuelta a la mitad. Cloudflare fue el primero en implementar la TLS 1.3 y contribuyó en gran medida al estándar. Cloudflare también fue el primero en implementar el HTTP/2, que solo funciona con TLS. El HTTP/2 aumenta el rendimiento, especialmente a nivel de latencia, percibido por el usuario durante el uso de un navegador. El HTTP/2 funciona en combinación con Server Push, con el que un servidor puede enviar recursos que el cliente aún no ha solicitado para acelerar el rendimiento percibido todavía más. El conjunto de TLS 1.3 y HTTP/2 con Server Push son solo dos ejemplos del continuo esfuerzo de Cloudflare para integrar nuevas tecnologías a su red.

Conclusiones

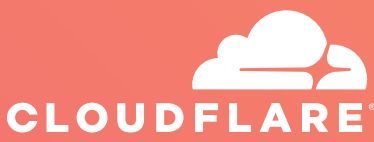
La contratación de Cloudflare mejorará el rendimiento de su sitio y aplicaciones de móvil al tiempo que los protege de ataques DDoS y vulnerabilidades de aplicaciones. La configuración es muy sencilla y solo tardará 5 minutos en ponerlo en marcha. Compruebe nuestros planes, que varían desde gratuitos hasta Enterprise en www.cloudflare.com.

Para obtener más información acerca de Cloudflare, póngase en contacto con nosotros.

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com