Protección DDoS con Cloudflare

La evolución de los ataques DDoS de hoy en día

2016

1 Tbps

Ataque de botnet de IoT de capa 7

El mayor ataque de capa 7 jamás visto con la botnet de IoT Mirai. El ataque fue volumétrico y utilizó los recursos de los servidores.

2014

400 Gbps

Ataque de amplificación NTP

Un atacante utilizó 4529 servidores NTP para amplificar un ataque desde un servidor origen de tan solo 87 Mbps.

2013

120 Gbps

Ataque DDoS de capas 3/4

El ataque a Spamhaus se consideró uno de los mayores en aquel momento y fue denominado «el ataque que casi acaba con Internet».

Los ataques de denegación de servicio distribuido (DDoS) están aumentando y se han convertido en complejos y abrumadores desafíos en materia de seguridad para las organizaciones. Aunque los ataques DDoS no son un fenómeno reciente, los métodos y recursos disponibles para dirigir y enmascarar dichos ataques han evolucionado considerablemente. Un hito en la evolución de los ataques DDoS fue la creación de la botnet Mirai; con esta botnet se infectaron más de 300 000 dispositivos enlazados al IoT, los cuales se usaron para generar el mayor ataque DDoS conocido actualmente, con picos de tráfico de ataque superiores a 1 Tbps de rendimiento. Los ataques de esa magnitud están empezando a ser lo habitual.

Los ataques DDoS no suelen ser eventos únicos y las víctimas sufren normalmente varios ataques durante el año. Según la experiencia de Cloudflare, cualquiera —organizaciones grandes y pequeñas— puede ser el objetivo. Aunque muchas jurisdicciones cuentan con leyes que penalizan los ataques DDoS, existen proveedores que ofrecen suscripciones de DDoS como servicio, algunas con precios realmente bajos, que van desde los 5 a los 10 dólares al mes.

La pérdida de beneficios es solo una de las muchas amenazas que este tipo de ataques representa para su sitio web o su negocio. Incluso el sitio web de Amazon (99 mil millones de dólares en ingresos al por menor en 2015) quedó fuera de servicio varias veces durante el pasado por razones desconocidas. Por ejemplo, en 2013 el sitio Amazon.com quedó fuera de servicio entre 15 y 45 minutos, lo que costó a la empresa pérdidas en ventas entre 1,8 y 5,3 millones, según las ventas promedio de la empresa de 117 882 dólares por minuto. Además, problemas como la inaccesibilidad al sitio conlleva pérdidas menos cuantificables, como la degradación de la marca y el deterioro de la satisfacción del cliente.

Una solución DDoS escalable y precisa

Una red global Anycast™ de 10 Tbps de Cloudflare es 10 veces mayor que el mayor ataque DDoS jamás registrado, lo que permite que todos los activos de Internet que se encuentren en la red de Cloudflare puedan soportar los ataques DDoS masivos actuales. La protección DDoS de Cloudflare para las capas 3, 4 y 7 está disponible como servicio en el perímetro de la red, igualando la escala de las amenazas de hoy en día, y puede utilizarse para mitigar ataques DDoS de todo tipo y tamaño. La limitación de la velocidad complementa la protección DDoS de Cloudflare al permitir una mitigación precisa de los ataques más sofisticados contra la capa de aplicación.

PROTECCIÓN CONTRA LOS ATAQUES DE CAPAS 3 Y 4

Los ataques de capa 3 y capa 4 son normalmente ataques volumétricos, tales como ataques DDoS de amplificación, DDoS de inundación y DDoS de inundación SYN. Aunque dichos ataques pueden desbordar la típica red de unidifusión, la red Anycast de Cloudflare aumenta intrínsecamente la superficie, dispersando el tráfico de ataque a los más de 102 centros de datos de Cloudflare y a un conjunto de interconexiones de ancho de banda con otras redes, para así absorber el tráfico de ataque.

Características de la protección DDoS

- Protección DDoS de las capas 3, 4 y 7
- Protección contra ataques DNS
- Bloqueo de amenazas específico con limitación de velocidad
- Seguridad predictiva con base de datos de reputación de IP

«Saber que no tenemos que preocuparnos por los ataques DDoS contra nuestra API y nuestros servidores de puerta de enlace nos da la tranquilidad que necesitamos para centrarnos en mejorar nuestros productos».

Jake Heinz, ingeniero de software de Discord

Red de Cloudflare

- Red global Anycast™ de más de 102 centros de datos
- 10 Tbps de rendimiento para absorber ataques volumétricos
- 6 millones de sitios de Internet
- Tarifa plana de ancho de banda

«Usamos Cloudflare porque las características de seguridad son excelentes, la CDN tiene un rendimiento muy alto y es muy práctico que estas soluciones vengan en un mismo paquete. Hace que sea más fácil gestionarlo todo y nos permite centrarnos en nuestra actividad principal».

Amanda Kleha GM, unidad de negocio en línea de Zendesk

PROTECCIÓN CONTRA LAS VULNERABILIDADES DE LA CAPA DE APLICACIÓN 7

Los ataques de capa 7 suelen ser, entre otros, los ataques de inyección SQL y de Cross Site Scripting (XSS), que pueden permitir que los atacantes accedan a los datos de los clientes o cualquier otro tipo de datos de la aplicación y los alteren. Cloudflare trata esas amenazas a través de su firewall de aplicaciones web (WAF). El WAF bloquea automáticamente las amenazas que se encuentran en el conjunto de reglas del OWASP Top 10, los conjuntos de reglas de aplicaciones de Cloudflare y las reglas personalizadas creadas por la comunidad o los clientes. Cloudflare ha podido proteger a sus clientes contra las principales vulnerabilidades de día cero, incluidas la vulnerabilidad Shellshock y el error de software Heartbleed.

LIMITACIÓN DE VELOCIDAD

Active la limitación de velocidad de Cloudflare para conseguir un control del tráfico específico que complemente la protección DDoS y los servicios de firewall de aplicaciones web (WAF). La limitación de velocidad protege ante ataques de denegación de servicio, intentos de contraseña por fuerza bruta y otros tipos de comportamientos abusivos dirigidos a la capa de aplicación. Configure umbrales de solicitud, defina respuestas personalizadas, tales como acciones de mitigación (desafíos o CAPTCHAS) o códigos de respuesta, y obtenga información analítica sobre los extremos de su sitio web, aplicación o API.

Seguridad predictiva

Cloudflare proporciona una plataforma de aprendizaje automático, donde se analiza el tráfico de red en tiempo real para detectar solicitudes anómalas o maliciosas. Una vez que se identifica un nuevo ataque, Cloudflare inicia automáticamente el bloqueo de ese tipo de ataque, tanto para el sitio web como para toda la comunidad. 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.

Tarifa plana de ancho de banda

Cloudflare proporciona protección DDoS ilimitada de nivel empresarial por una tarifa plana mensual. Cloudflare cree que los clientes no deberían ser penalizados por el aumento de tráfico de red asociado a un ataque DDoS. Con la protección DDoS de Cloudflare, los clientes contarán con la garantía de que su sitio web seguirá estando en línea y tendrán una facturación mensual fija.

Suscríbase a Cloudflare

Suscríbase a Cloudflare y active la limitación de velocidad para proteger su sitio web, aplicación o API ante los ataques DDoS, y al mismo tiempo, reducir la latencia y utilizar las últimas tecnologías web. La configuración es sencilla y normalmente no se necesitan más de 5 minutos para ponerla en marcha. Consulte los planes, que van desde el gratuito al Enterprise, en www.cloudflare.com.