Cómo prevenir los ataques DDoS | Métodos y herramientas

La reducción de la superficie de ataque, la detección de amenazas en tiempo real y la mitigación de DDoS siempre activa pueden ayudar a prevenir los ataques antes de que lleguen a las infraestructuras y sistemas objetivo.

Objetivos de aprendizaje

Después de leer este artículo podrás:

- Explicar cómo funcionan los ataques DoS
- Explora las estrategias de prevención de ataques DDoS
- Descubre cómo Cloudflare ayuda a prevenir ataques

CONTENIDO RELACIONADO

¿Quieres saber más?

Copiar enlace del artículo

Descubre cómo funcionan los ataques DDoS

Un ataque de denegación de servicio distribuido (DDoS) interrumpe las operaciones de un servidor, servicio o red al inundarlo con tráfico de Internet no deseado. En el peor de los casos, estos ataques pueden interrumpir un sitio web o toda la red durante largos periodos de tiempo.

Los ataques DDoS funcionan dirigiendo tráfico malicioso a un objetivo a través de varios ordenadores o máquinas. A menudo, estas máquinas forman una botnet: un grupo de dispositivos que se han visto en riesgo por malware y pueden ser controlados por un único atacante. Otros ataques DDoS pueden implicar a varios atacantes o herramientas de ataque DDoS, como la aplicación de pruebas de estrés (por ejemplo, LOIC) o programas bajos y lentos (como Slowloris).

Los atacantes pueden utilizar una o más de las siguientes estrategias para realizar DDoS a sus objetivos:

1. Los **ataques de capa de aplicación**, también conocidos como *ataques DDoS de capa 7*, crean una denegación de servicio, abrumando el servidor y los recursos de red del objetivo con solicitudes HTTP que parecen legítimas.

2. Los **ataques de protocolo**, o *ataques de un estado de agotamiento*, sobrecargan los equipos y la infraestructura de la red al utilizar protocolos de capa 3 o 4 (por ejemplo,ICMP) para enviar una inundación de tráfico no deseado a su objetivo.

Los **ataques volumétricos** utilizan técnicas de amplificación —por ejemplo, implementando un botnet o explotando un protocolo de red común— para consumir todo el ancho de banda disponible del objetivo.

Para saber más sobre las tácticas empleadas en un ataque DDoS, lee ¿Qué es un ataque de denegación de servicio distribuido (DDoS)?

Cómo prevenir los ataques DDoS

Prevenir los ataques DDoS puede ser un reto, sobre todo en periodos de mucho tráfico o en una arquitectura de red vasta y distribuida. Una defensa contra amenazas DDoS verdaderamente proactiva depende de varios factores clave: reducción de superficie de ataque, monitorización de amenazas y herramientas escalables de mitigación de DDoS.

Métodos de prevención de DDoS

- **Reducción de superficie de ataque:** limitar la exposición a la superficie de ataque puede ayudar a minimizar el efecto de un ataque DDoS. Varios métodos para reducir esta exposición incluyen restringir el tráfico a ubicaciones específicas, implementar un compensador de cargas y bloquear la comunicación desde puertos, protocolos y aplicaciones obsoletos o no utilizados.

- **Difusión de red Anycast:** una red Anycast ayuda a aumentar la superficie de la red de una organización, para que pueda absorber más fácilmente los picos de tráfico volumétrico (y evitar interrupciones) al dispersar el tráfico por múltiples servidores distribuidos.

- **Monitoreo de amenazas adaptable y en tiempo real:** el monitoreo de registros puede ayudar a detectar posibles amenazas al analizar los patrones de tráfico de la red, al supervisar el pico de tráfico u otras actividades inusuales y al adaptarse para defenderse de solicitudes, protocolos y bloqueos de dirección IP anómalos o maliciosos.

- **Almacenamiento en caché:** un almacenamiento en caché almacena copias del contenido solicitado para que el servidor de origen atienda menos peticiones. Utilizar una red de entrega de contenido (CDN) para almacenar recursos en caché puede reducir la carga de los servidores de una organización y dificultar que se vean sobrecargados por solicitudes tanto legítimas como maliciosas.

- **Limitación de velocidad:** la limitación de velocidad restringe el volumen de tráfico de la red durante un periodo de tiempo determinado, lo que esencialmente impide que los servidores web se vean sobrecargados por peticiones procedentes de direcciones IP concretas. La limitación de velocidad se puede utilizar para evitar ataques DDoS que utilizan botnets para enviar contenido no deseado a un punto final con una cantidad anormal de solicitudes a la vez.

Herramientas de prevención de DDoS

- **Firewall de aplicaciones web (WAF):** un WAF ayuda a bloquear los ataques utilizando políticas personalizables para filtrar, inspeccionar y bloquear el tráfico HTTP malicioso entre la aplicación web e Internet. Con un WAF, las organizaciones pueden aplicar un modelo de seguridad positivo y negativo que controle el tráfico entrante de ubicaciones y direcciones IP específicas.

- **Mitigación de DDoS siempre activa:** un proveedor de mitigación de DDoS puede ayudar a prevenir los ataques DDoS analizando continuamente el tráfico de la red, aplicando cambios de política en respuesta a los patrones de ataque emergentes y proporcionando una red expansiva y confiable de centros de datos. Al evaluar los servicios de mitigación de DDoS basados en la nube, busca a un proveedor que ofrezca protección adaptable, escalable y siempre activa contra ataques volumétricos y sofisticados.

Para profundizar en las herramientas y estrategias de mitigación de DDoS, lee ¿Qué es la mitigación de DDoS?

Cómo Cloudflare ayuda a prevenir ataques DDoS

Cloudflare ofrece protección contra DDoS L3-7 integrada que ayuda a las organizaciones a supervisar, prevenir y mitigar los ataques antes de que lleguen a las aplicaciones, redes e infraestructuras objetivo. Algunas de las principales ventajas de nuestra defensa contra amenazas por capas son:

- Una red Anycast global que abarca más de 335 ciudades y 125 países en todo el mundo, capaz de absorber incluso los ataques DDoS más grandes
- Enrutamiento de tráfico y aceleración para ayudar a difundir el pico de tráfico por nuestra red y minimizar la latencia y la congestión
- Mitigación de DDoS siempre activa y automática que puede detectar y bloquear el tráfico malicioso, en menos de tres segundos
- Un WAF de próxima generación que ofrece limitación de velocidad avanzada, conjuntos de reglas personalizadas y prevención de amenazas flexible

¿Bajo ataque? Consigue protección contra DDoS inmediata a través de la línea de emergencia cibernética de Cloudflare.

Ataques DDoS

Herramientas para ataques DDoS

Glosario de DDoS

Navegación del centro de aprendizaje