cloudfresh CLOUDFLARE

Як запобігти DDoS-атаці залежно від типу

Зіткнення з DDoS-атаками може нагадувати мігрень. Однієї хвилини все гаразд, а наступної ви відчуваєте цифровий біль. Але знаєте що? Вам не обов'язково страждати через це. Ми розповімо вам про різні способи цих атак і, що більш важливо, про те, як ви можете нейтралізувати кожну з них і продовжити роботу вашого бізнесу.

01

DNS-флуд

Використовуйте Cloudflare DNS як основний або додатковий резолвер, а також увімкніть DNS Firewall або Magic Transit для покращеного захисту. Глобальна мережа Cloudflare фільтрує шкідливий або надмірний DNS-трафік, одночасно кешуючи та обслуговуючи запити, що надходять від законних користувачів. Вона обробляє десятки мільйонів DNS-запитів на секунду, автоматично блокуючи флуд до того, як він досягне вашого місця походження.

02

SYN-флуд

Розгорніть Cloudflare Magic Transit, щоб зупинити SYN-флуд на межі. Він використовує SYN-кукі, відстеження з'єднань і аналіз поведінки, щоб відокремити реальних користувачів від підроблених IP-адрес або шкідливого трафіку. Для додаткового захисту скеровуйте трафік через Cloudflare Spectrum (для TCP) або Cloudflare CDN/Web Application Firewall (для HTTP). Ці зворотні проксі запобігають прямому доступу до вашого джерела і блокують DDoS-трафік на основі TCP, перш ніж він завдасть шкоди.

03

UDP-флуд

Вам цікаво, як запобігти DDoS-атаці, яка надсилає UDP-трафік? Використовуйте Magic Transit або Spectrum, щоб виявити і відкинути його в режимі реального часу. Поєднайте їх із Magic Firewall, щоб застосувати інтелектуальне обмеження швидкості або повністю заблокувати небажані UDP-пакети та захистити свою інфраструктуру від об'ємних сплесків.

04

Teeworlds

Захистіть свої ігрові сервери за допомогою Cloudflare Spectrum або Magic Transit. Cloudflare автоматично відстежує та фільтрує DDoS-трафік, дозволяючи реальним гравцям підключатися до мережі. Для додаткового контролю використовуйте брандмауер Magic Firewall, щоб створити власні правила, які зупиняють атаки на рівні пакетів.

05

RIPv1

Вимкніть RIPv1 на всіх маршрутизаторах і перейдіть на RIPv2 з автентифікацією, якщо потрібна маршрутизація. Заблокуйте вхідний UDP-порт 520 із ненадійних мереж і відстежуйте незвичну активність маршрутизації, щоб завчасно виявити потенційні зловживання.

06

RDP

Використовуйте Magic Transit для блокування підробленого або шкідливого RDP-трафіку до того, як він потрапить до вас. Аби захистити віддалений доступ на рівні застосунків, перемістіть RDP за Cloudflare Gateway або Zero Trust Network Access (ZTNA), які вимагають автентифікації та допомагають запобігти зловживанню відкритими RDP-сервісами.

07

DemonBot

Як захиститися від DDoS-атак, що здійснюються через DemonBot? Зверніться до Magic Transit, який фільтрує масові флуди на рівнях 3 і 4. Cloudflare ідентифікує заражений трафік за допомогою аналізу в реальному часі та виявлення сигнатур. Для атак 7-го рівня використовуйте WAF і DDoS захист Cloudflare, щоб блокувати HTTP-флуд і зловживання з'єднаннями.

08

VxWorks Flood

Розгорніть Magic Transit для фільтрації DDoS-трафіку зі скомпрометованих пристроїв VxWorks. Cloudflare виявляє і блокує цей трафік за допомогою спеціальних евристик і відбитків у реальному часі. Для захисту на рівні застосунків використовуйте Cloudflare Gateway і WAF для захисту від зловживань на рівні протоколів.

Ніяких відмов: Ваш захист від DDoS виграє з Cloudfresh!

cloudfresh.com

hi@cloudfresh.com